CBV383Z4S-N300 DOCSIS 3.0 EMTA/Router with Wireless-N

Revision 1.0
Jan 2014

FCC Statement

This device complies with Class B Part 15 of the FCC Rules. The device generates, uses and can radiate radio frequency energy and, if not installed and used as instructed, may cause harmful interference to radio communication. Only Coaxial cables are to be used with this device in order to ensure compliance with FCC emissions limits. Accessories connected to this device by the user must comply with FCC Class B limits. The manufacturer is not responsible for any interference which results from use of improper cables, or which results from unauthorized changes or modifications to the device. "A Minimum 26 AWG Line Core should be used for connection to the cable modem"

Warranty

Items sold by manufacturer/distributor/agent, hereinafter called "Seller", are warranted only as follows: Except as noted below Seller will correct, either by repair or replacement at its option, any defect of material or workmanship which develops within one year after delivery of the item to the original Buyer provided that evaluation and inspection by Seller discloses that such defect developed under normal and proper use. Repaired or replaced items will be further warranted for the unexpired term of their original warranty. All items claimed defective must be returned to Seller, transportation charges prepaid, and will be returned to the Buyer with transportation charges collect unless evaluation proves the item to be defective and that the Seller is responsible for the defect. In that case, Seller will return to Buyer with transportation charge prepaid. Seller may elect to evaluate and repair defective items at the Buyer's site. Seller may charge Buyer a fee (including travel expenses, if needed) to cover the cost of evaluation if the evaluation shows that the items are not defective or that they are defective for reasons beyond the scope of this warranty.

The Seller makes no warranty concerning components or accessories not manufactured by it. However, in the event of failure of such a part, Seller will give reasonable assistance to Buyer in obtaining from the manufacturer whatever adjustment is reasonable in light of the manufacturer's own warranty. Seller will not assume expense or liability for repairs made outside the factory by other than Seller's employees without Seller's written consent.

SELLER IS NOT RESPONSIBLE FOR DAMAGE TO ANY ASSOCIATED EQUIPMENT, NOR WILL SELLER BE HELD LIABLE FOR INCIDENTAL, CONSEQUENTIAL, OR OTHER

DAMAGES. THIS WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES EXPRESSED OR IMPLIED INCLUDING THE IMPLIED WARRANTY OF "MERCHANTABILITY" AND "FITNESS FOR PARTICULAR PURPOSE."

Trademarks

All trademarks are the property of their respective owners.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation.

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

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.

Non-modification Statement:

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

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Limited Channels fixed for use in the US:

IEEE 802.11b or 802.11g or 802.11n(HT20) operation of this product in the U.S. is firmware-limited to Channel 1 through 11. IEEE 802.11n(HT40) operation of this product in the U.S. is firmware-limited to Channel 3 through 9.

Canada-Industry Canada (IC)

Operation is subject to the following two conditions:

this device may not cause interference and
this device must accept any interference, including interference that may cause undesired operation of the device.

IMPORTANT NOTE:

IC Radiation Exposure Statement:
This equipment with IC radiation exposure limits set forth for an uncontrolled environment. To maintain compliance with IC RF exposure compliance requirements, please follow operation instruction as documented in this manual.

Warranty

Items sold by manufacturer/distributor/agent, hereinafter called "Seller", are warranted only as follows: Except as noted below Seller will correct, either by repair or replacement at its option, any defect of material or workmanship which develops within one year after delivery of the item to the original Buyer provided that evaluation and inspection by Seller discloses that such defect developed under normal and proper use. Repaired or replaced items will be further warranted for the unexpired term of their original warranty. All items claimed defective must be returned to Seller, transportation charges prepaid, and will be returned to the Buyer with transportation charges collect unless evaluation proves the item to be defective and that the Seller is responsible for the defect. In that case, Seller will return to Buyer with transportation charge prepaid. Seller may elect to evaluate and repair defective items at the Buyer's site. Seller may charge Buyer a fee (including travel expenses, if needed) to cover the cost of evaluation if the evaluation shows that the items are not defective or that they are defective for reasons beyond the scope of this warranty.

The Seller makes no warranty concerning components or accessories not manufactured by it. However, in the event of failure of such a part, Seller will give reasonable assistance to Buyer in obtaining from the manufacturer whatever adjustment is reasonable in light of the manufacturer's own warranty. Seller will not assume expense or liability for repairs made outside the factory by other than Seller's employees without Seller's written consent.

SELLER IS NOT RESPONSIBLE FOR DAMAGE TO ANY ASSOCIATED EQUIPMENT, NOR WILL SELLER BE HELD LIABLE FOR INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES. THIS WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES EXPRESSED OR IMPLIED INCLUDING THE IMPLIED WARRANTY OF "MERCHANTABILITY" AND "FITNESS FOR PARTICULAR PURPOSE."

Note to CATV Sysrem Installer

"The EUT must be bonding the screen of the coaxial cable to the earth at the building entrance per ANSI/NFPA 70, the National Electrical Code (NEC), in particular Section 820.93, Grounding of Outer Conductive Shield of a Coaxial Cable.”

Trademarks

All trademarks are the property of their respective owners.

Table of Contents

1. Introduction

The CBV383Z4S-N300 is a Voice over IP Wireless Residential Gateway integrated with Cable Modem which allows you implement your VoIP phone call directly through Cable Modem Broadband Network service with its built-in PacketCable 1.5 and DOCSIS/EURODOCSIS 2.0 / 3.0 compliant specification.

Equipped with two standard phone ports, CBV383Z4S-N300 could easily provide end-users low-cost, long-distance calling, faxing, and a host of advanced service including CBV383Z4S-N300 -to-Phone, Phone-to-CBV383Z4S-N300

And with the integration of 4 ports switch and IEEE 802.11n wireless functionality, the CBV383Z4S-N300 could also be used as a Wireless Cable Modem Residential Gateway in your home or small office. The ability to route data information into your broadband network could help you easily extend your local network via wire or wireless.

The CBV383Z4S-N300 is MGCP/SIP compliant and has been tested with most major VoIP Softswitch vendors' Call Management systems. And it also has voice support that includes hardware based Quality of Service (QoS), voice compression with popular voice CODES G.711, echo cancellation, dynamic latency (jitter) buffers, silence suppression, and comfort noise generator.

1.1 Features

- PacketCable 1.5 standard compliant
- DOCSIS /EURODOCSIS 2.0 / 3.0 standard compliant.
- Support PacketCable MGCP (Media Gateway Control Protocol)
- SIP (Session Initiation Protocol) compliant
- 4 standard RJ45 connector for GbE Ethernet with auto-negotiation MDIX functions
- Two Rj11 Foreign Exchange Station (FXS) ports for IP telephony
- QoS enhancement
- MSO SNMPv3 remote network management
- Provide MIBs DOCSIS 1.0/1.1/2.0/3.0
- Support simultaneous voice and data communications
- Echo Cancellation
- Voice Active Detection (VAD)
- Comfort Noise Generation (CNG)
- Web Browser Management auto detect network status
- Build-in IEEE802.11n module as AP with miniPCI form factor

1.2 System Requirements

- IBM Compatible, Macintosh or other workstation supports TCP/IP protocol.
- An Ethernet port supports GbE Ethernet connection.
- Subscribed to a Cable Television company for Cable Modem services.

1.3 Unpacking and Inspection

Included in the kit is the following:

- 1 x EMTA CBV383Z4S-N300
- 1 x Quick Installation Guide
- 1 x RJ-45 CAT 5 Cable
- 1 x 12V/1.5A Power Supply Adaptor
- 1 x 6P4C Telephone Cord

If any of above items lost or damaged, please contact your retailer or ISP for assistance.

1.4 Safety Precautions

For your protection, observe the following safety precautions when setting up and using your equipment. Failure to observe these precautions can result in serious personal injury and damage to your equipment.

- Make sure the voltages and frequency of the power outlet matches the electrical rating labels on the AC Adapter.
- Do not place any object on top of the device or force it into a confined space.
- Never push objects of any kind through openings in the casing. Dangerous voltages may be present. Conductive foreign objects could produce a short circuit that could cause fire, electrical shock, or damage to the equipment.
- Whenever there is danger of lightning, disconnect the power cable and the Hybrid-Fiber Coax cable from the cable modem to prevent damage to the unit. The use of an AC protection device will not completely protect the cable modem product from damage caused from the transmission across the Hybrid-Fiber Coax network.

2. Hardware Overview

2.1 Front Panel and LEDs

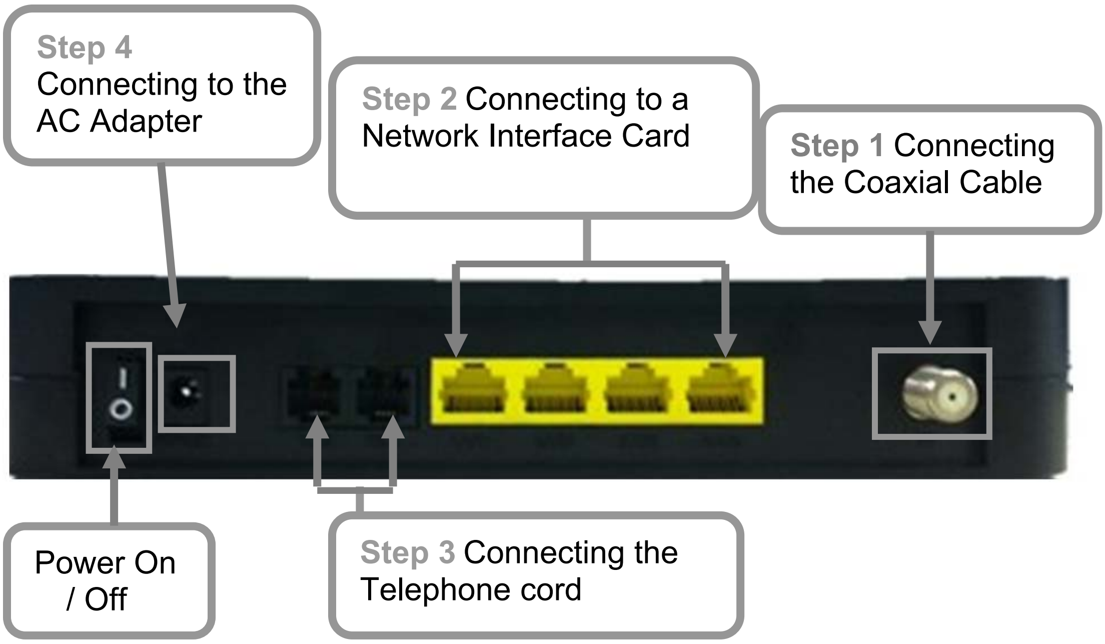
There are ten Light-Emitting-Diodes (LEDs) located on the front panel top provide status information to the user.

NAME	COLOR	MODE	STATUS
PWR	Green	On	DC Power is connected
		Off	No DC Power connected
DS	Green	Blinking	Downstream scanning
		On	Downstream locked
		Off	Cable interface idle or W/DS bonding
	Orange	On	W/DS locked
		Off	W/DS disabled
US	Green	Blinking	Upstream scanning
		On	Upstream locked
		Off	Cable interface idle or W/US bonding
	Orange	On	W/US locked
		Off	W/US disabled
ONLINE	Green	Blinking	CM provisioning
		On	CM On-line
		Off	CM Off-line
LAN	Green	Blinking	Data in traffic
		On	ETH device connected (GbE mode)
		Off	No ETH device connected

	Orange	Blinking	Data in traffic
		On	ETH device connected (FE mode)
		Off	No ETH device connected
WLAN 2.4GHz	Green	On	WiFi enable
		Off	WiFi disable
		Blinking	Data in traffic
		Blinking	WPS in paring
		ON	WPS enabled
		Off	WPS disabled
		On	TEL1 on-hook
		Off	TEL1 disable
		blinking	TEL1 provisioning or off-hook
		On	TEL2 on-hook
		Off	TEL2 disable
		blinking	TEL2 provisioning or off-hook

2.2 Rear Panel and Hardware Connection

This chapter describes the proper steps for connecting your cable modem. Please be sure to follow the steps in the sequence outlined below. Failure to do so could result in improper operation or failure of your cable modem.


Step 4 Connecting to the AC Adapter
Step 2 Connecting to a Network Interface Card
Step 1 Connecting the Coaxial Cable
Power On / Off
Step 3 Connecting the Telephone cord

Step 1:
Connect a cable by feeding the F-connector on the back of the cable modem. Ensure the center conductor of the 75 ohm coaxial cable is inserted directly into the center of the F-connector. Secure the coaxial cable by carefully threading the outer shell of the coaxial cable connector onto the F-connector in a clockwise direction until tight. Be careful not to over-tighten the connector or you may damage either the connector or the cable modem.

Step2: Connect the cable modem to an GbE Ethernet 10/100/1000 Mbps Network using a RJ-45 male-terminated Ethernet cable. This cable modem equips with two Ethernet ports, you can connect two PCs to the cable modem at the same time if necessary.

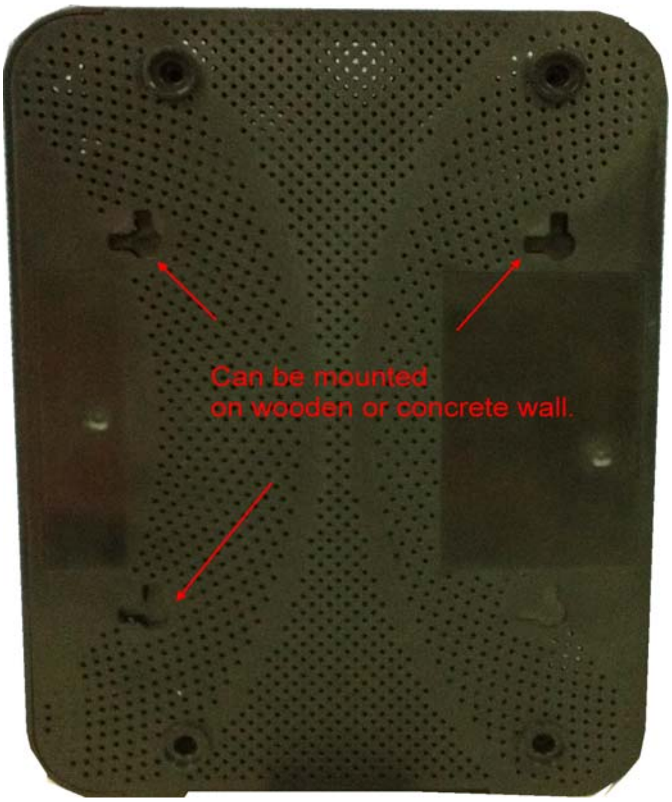
Step 3: Connect the telephone sets to TEL1 and TEL2. Use RJ-11 telephone line to connect TEL1/TEL2 port on the cable modem and telephone socket on telephone.

Step 4: Connect the AC Adapter to the cable modem by inserting the barrel-shaped connector into the mating power connector on the back of the cable modem. Exercise carefully to ensure the connectors are properly aligned prior to insertion and ensure the two connectors engage completely. The cable modem is shipped with an AC adapter. Remember to use only power adapter that came with the cable modem. Other power adapters might have voltages that are not correct for your particular cable modem. Using a power adapter with the wrong voltage can damage the cable modem.

Step 5: Adjust the antenna if necessary.

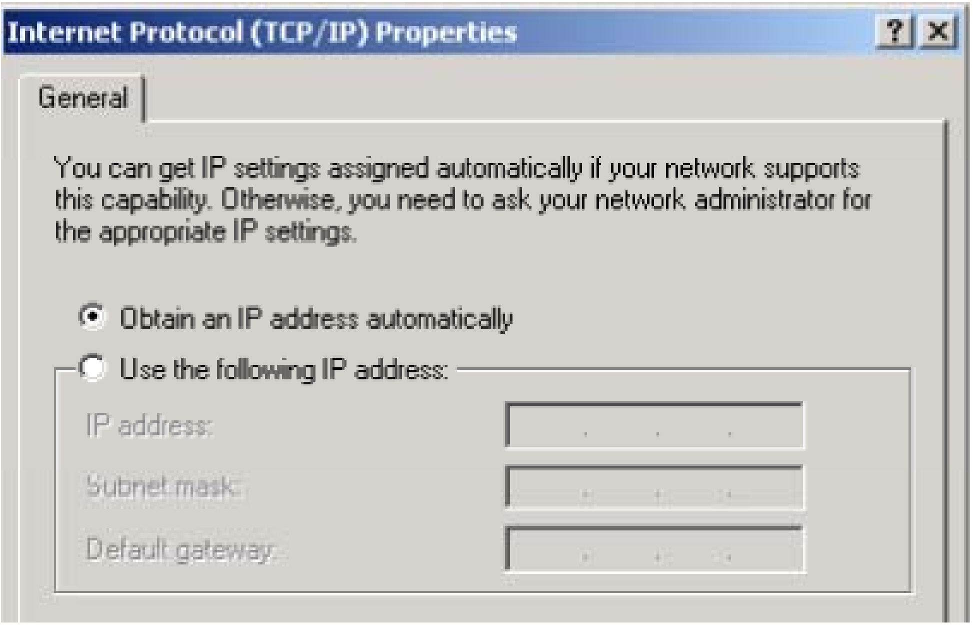
Step 6: The screen of the coaxial cable is intended to be connected to earth in the building installation.

Step 7: Wall-Mounting the EMTA
This product can be mounted on wooden or concrete wall, There are two holes in the lower case , you can use the screw（Diameter of stainless steel screw is about 3mm-3.5mm ） to mount it.



3. Ethernet Installation

The LAN port you are using is auto-negotiating 10/100/1000Mbps (Switch) Ethernet Interface. You can use the Ethernet port to connect to the Internet with an Ethernet network device such as NIC/Hub/Switch through RJ45. Before you connect to and install the cable modem, please set the IP address to "Obtain an IP address automatically" as below and do ensure the TCP/IP protocol is installed on your system and configured correctly in your PC.



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: . . .

Following is an example of configuring the TCP/IP Protocol on Windows Operating Systems:

1. Click **Start→Settings→Control Panel**. Double click on the **Network** icon click **Properties**.
2. A list of installed network components appears. Look for an entry named TCP/IP. This entry may be followed by an arrow and a description of the NIC hardware device installed in the computer. If you don't see "TCP/IP" listed anywhere in the "The following network components are installed" box, click the **Add** button, choose **Protocol**, and click the **Add** button. Select "Microsoft" as the manufacturer and then scroll down in the list on the right to find "TCP/IP". If you see "TCP/IP" listed, proceed to step 4.
3. Click the **OK** button. You will be prompted to insert the Windows 98 installation/upgrade CD.
4. Scroll down in the box until you find a line that says "TCP/IP -> " followed by the name of your Ethernet adapter. Click on **Properties** and choose "Obtain an address automatically" which means that your PC has been configured to use DHCP (Dynamic Host Configuration Protocol).
5. Click **OK**.

Congratulations! You have successfully set up your cable modem.

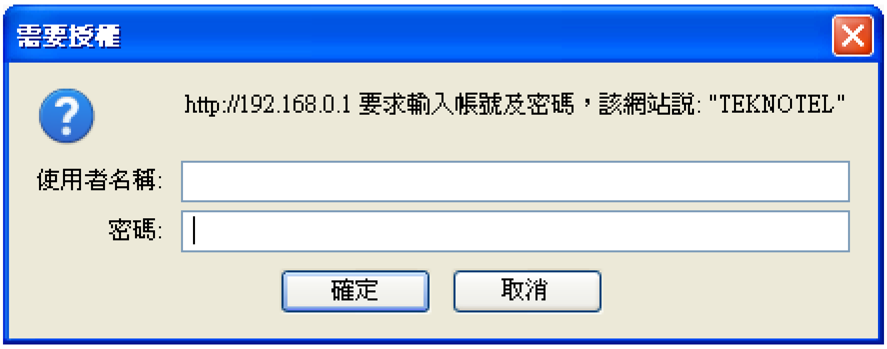
4. Web Management

For easy-changing the default setting or quick-checking diagnostics for troubleshooting, a Web-based GUI is built-in for your access.

4.1 Enter Modem's IP address

Use the following procedures to login to your CBV383Z4S-N300 .

1. Open your web browser.
   You may get an error message. This is normal. Continue on to the next step.
2. Type the default IP address of the CBV383Z4S-N300 (e.g. **192.168.0.1**) and press Enter.



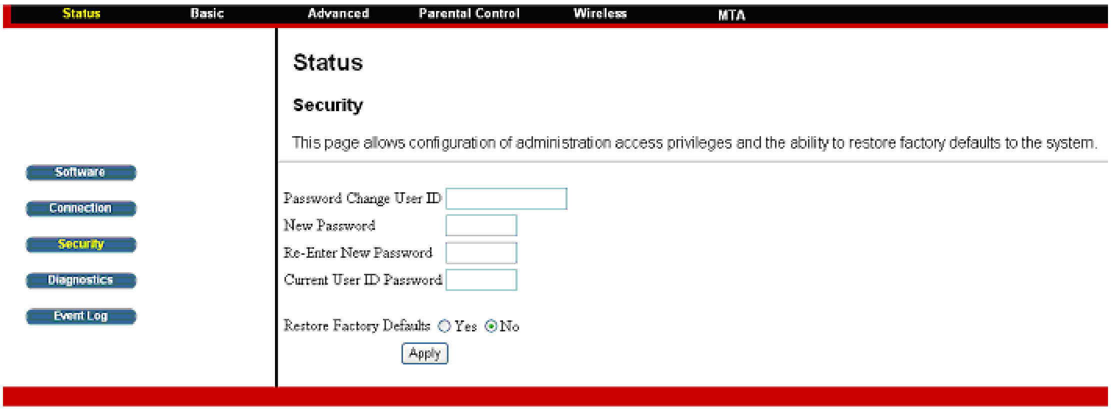
需要授權

http://192.168.0.1 要求輸入帳號及密碼，該網站說: "TEKNOTEL"

使用者名稱:

密碼:

3. The Log In page appears. Type the user name (**admin**) and your password (**password**) in the respective fields.



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

Restore Factory Defaults ○ Yes ● No

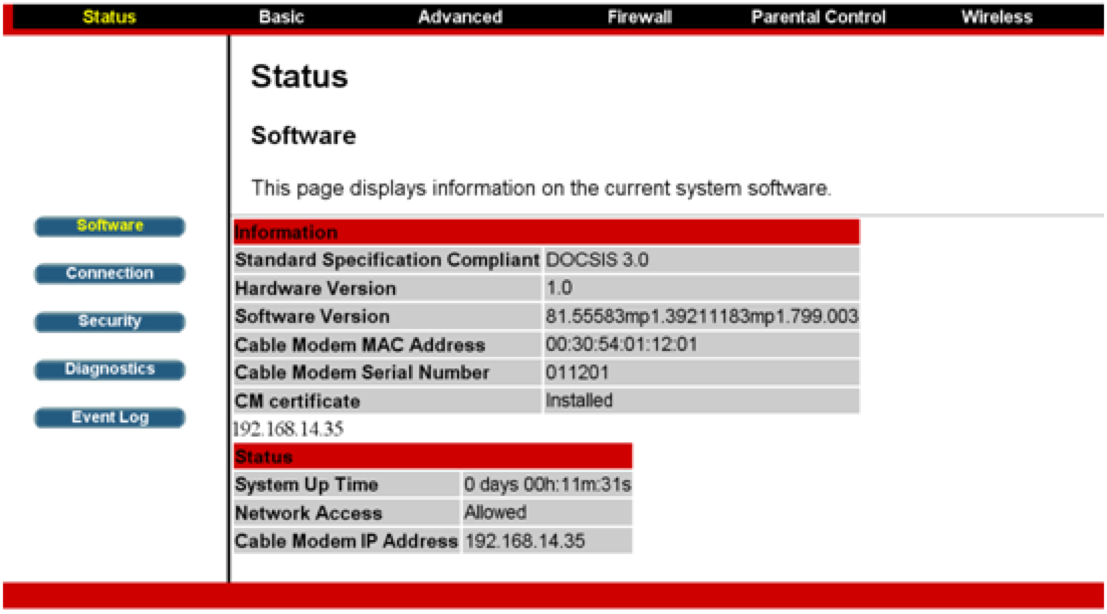
There are seven categories in this web management including Status, Basic, Advanced and Firewall. The following sections describe their details.

4.2 Status

The Status page shows hardware and software information about the CBV383Z4S-N300 that may be useful to your cable service provider.

4.2.1 Software Status

The Software page shows how long the CBV383Z4S-N300 has operated since last being powered up, and some key information the CBV383Z4S-N300 received during the initialization process with your cable service provider.



Status

Software

This page displays information on the current system software.

Information	
Standard Specification Compliant	DOCSIS 3.0
Hardware Version	1.0
Software Version	81.55583mp1.39211183mp1.799.003
Cable Modem MAC Address	00:30:54:01:12:01
Cable Modem Serial Number	011201
CM certificate	Installed

192.168.14.35

Status	
System Up Time	0 days 00h:11m:31s
Network Access	Allowed
Cable Modem IP Address	192.168.14.35

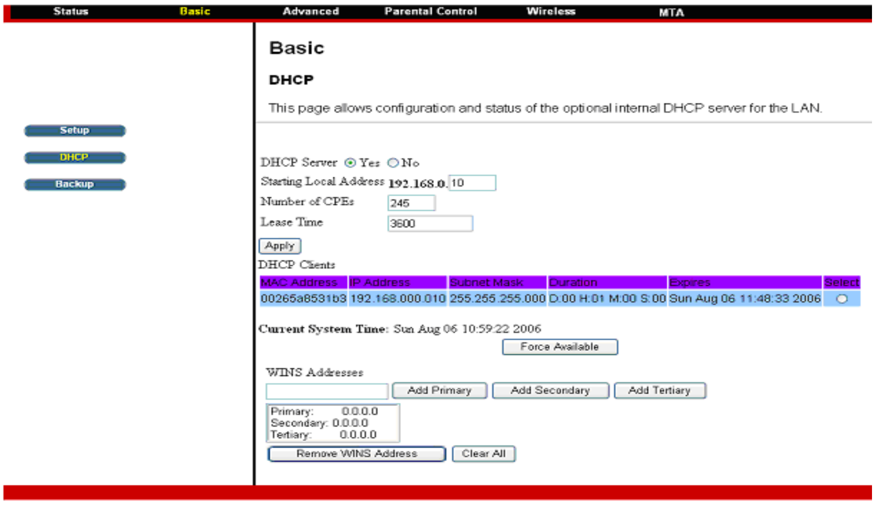
If Network Access shows "Allowed," then your cable service provider has configured the CBV383Z4S-N300 to have Internet connectivity. If Network Access shows otherwise, you may not have Internet access, and please contact your cable service provider for assistance.

4.3 Basic

The Basic page contains the basic features of CBV383Z4S-N300 including Setup, DHCP and Backup

4.3.1 DHCP

The DHCP page allows you to activate/deactivate the DHCP server function of the CBV383Z4S-N300 , and, if the DHCP server is activated, to see DHCP leases it has provided.



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

Apply

DHCP Clients

MAC Address	IP Address	Subnet Mask	Duration	Expires	Select
00265a8531b3	192.168.000.010	255.255.255.000	D:00 H:01 M:00 S:00	Sun Aug 06 11:48:33 2006	○

Current System Time: Sun Aug 06 10:59:22 2006

Force Available

WINS Addresses

Add Primary Add Secondary Add Tertiary

Primary: 0.0.0.0
Secondary: 0.0.0.0
Tertiary: 0.0.0.0

Remove WINS Address Clear All

With this function activated, your cable service provider's DHCP server provides one IP address for the CBV383Z4S-N300 , and the CBV383Z4S-N300 's DHCP server provides IP addresses, starting at the address you set in **Starting Local Address** field, to your PCs. A DHCP server leases an IP address with an expiration time.

To set the maximum number of PCs to which the CBV383Z4S-N300 will issue IP addresses, enter it in the **Number of CPEs** box and then click **Apply**. (CPE is another term sometimes used for PC.)

The table on the bottom of this page shows the information of DHCP clients including the IP and MAC addresses of each PC. Since MAC addresses are unique and permanently fixed into hardware, you can identify any PC listed by its MAC address. The CBV38Z4C provides leases for 3600 seconds (default), and has an automatic renewal mechanism that will keep extending a lease as long as the associated PC remains active.

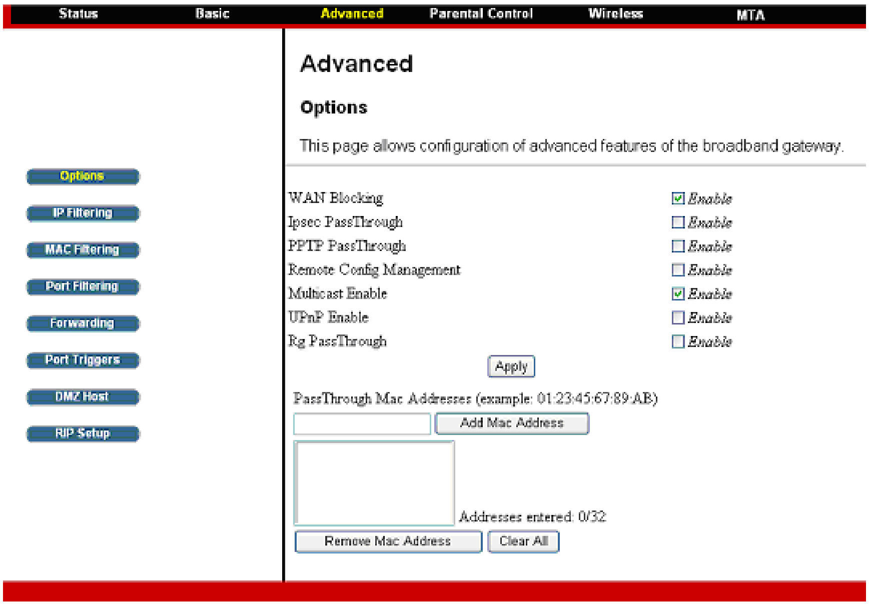
You can cancel an IP address lease by selecting it in the DHCP Client Lease Info list and then clicking the **Force Available** button. If you do this, you may have to perform a DHCP Renew on that PC, so it can obtain a new lease.

4.4 Advanced

The Advanced page allows you to enable/disable some advanced features of the CBV383Z4S-N300 .

4.4.1 Options

The Options page allows you to enable/disable some advanced features supported by CBV383Z4S-N300 .



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*
Rg PassThrough	□ *Enable*

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

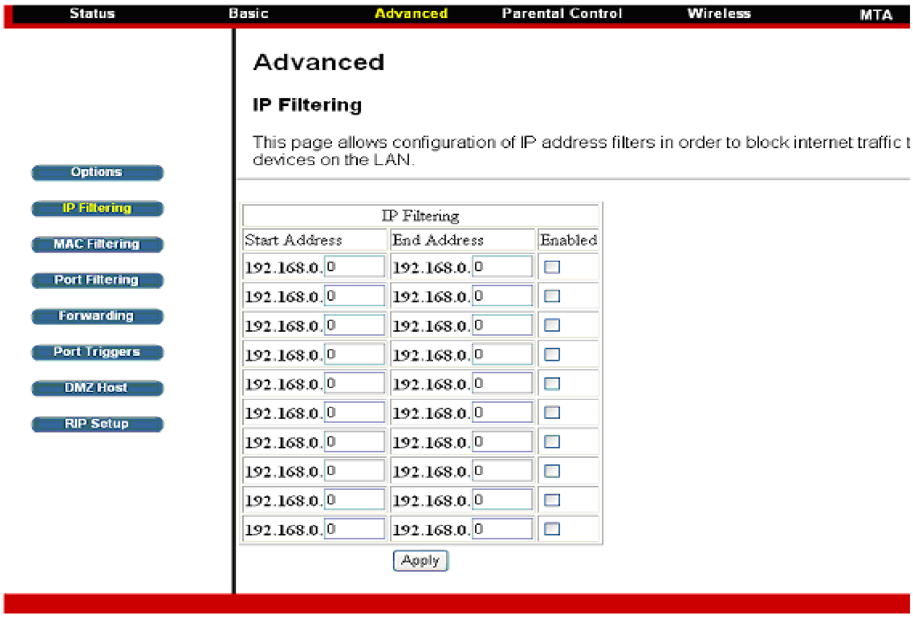
Addresses entered: 0/32

Check the option you want to use and click **Apply** button to enable the function(s).

- **WAN Blocking:** To prevent others on the WAN side from being able to ping your CBV383Z4S-N300 . With WAN Blocking on, your CBV383Z4S-N300 will not respond to pings it receives, effectively “hiding” your gateway.
- **Ipsec PassThrough:** To enable IpSec type packets to pass through between WAN and LAN.
- **PPTP PassThrough:** To enable PPTP type packets to pass through between WAN and LAN.
- **Remote Config Management:** To make the Web Management pages of your CBV383Z4S-N300 accessible from the WAN side. Page access is limited to only those who know the CBV383Z4S-N300 access password you set in the **Status--Security** page.
  When accessing the CBV383Z4S-N300 from a remote location, you must use HTTP port 8080 and your IP address. This is the "WAN IP address" that appears at the **Basic--Setup** page. For example, if this IP address were 211.20.15.28, you would navigate to http:// 211.20.15.28:8080 to reach the CBV383Z4S-N300 ’s Web Management page from a remote location.
- **Multicast Enable:** To enable multicast traffic to pass through between WAN and LAN. You may need to enable this to see some types of broadcast streaming and content on the Internet, such as webcasting of a popular live event.
- **UPnP Enable:** UPnP (Universal Plug and Play) offers pervasive peer-to-peer network connectivity of PCs of all form factors, intelligent appliances, and wireless devices. UPnP architecture leverages TCP/IP and the Web to enable seamless proximity networking in addition to control and data transfer among networked devices in the home, office, and everywhere in between.

4.4.2 IP Filtering

The IP Filtering page enables you to enter the IP address ranges of PCs on your LAN that you don't permit to have outbound access ability to the WAN. These PCs can still communicate with each other on your LAN, but packets they originate to WAN addresses are blocked by the CBV383Z4S-N300 .



Advanced

IP Filtering

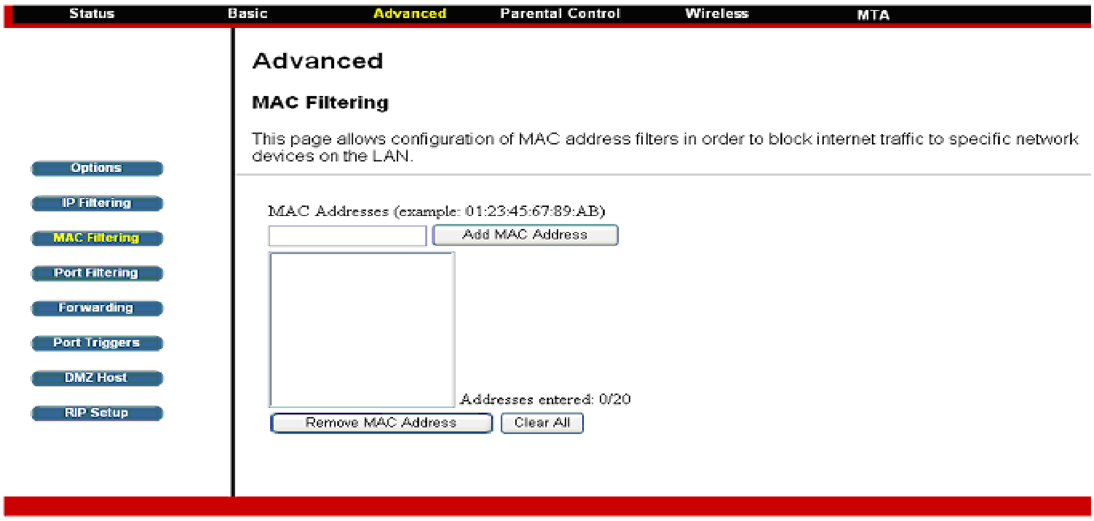
This page allows configuration of IP address filters in order to block internet traffic t devices on the LAN.

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	□

To enable IP Filtering feature of CBV383Z4S-N300 , check the **Enable** box and click **Apply** button.

4.4.3 MAC Filtering

The MAC Filtering page enables you to enter the MAC address of specific PCs on your LAN that you don't permit to have outbound access ability to the WAN. These PCs can still communicate with each other through the CBV383Z4S-N300 , but packets they send to WAN addresses are blocked.



Advanced

MAC Filtering

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

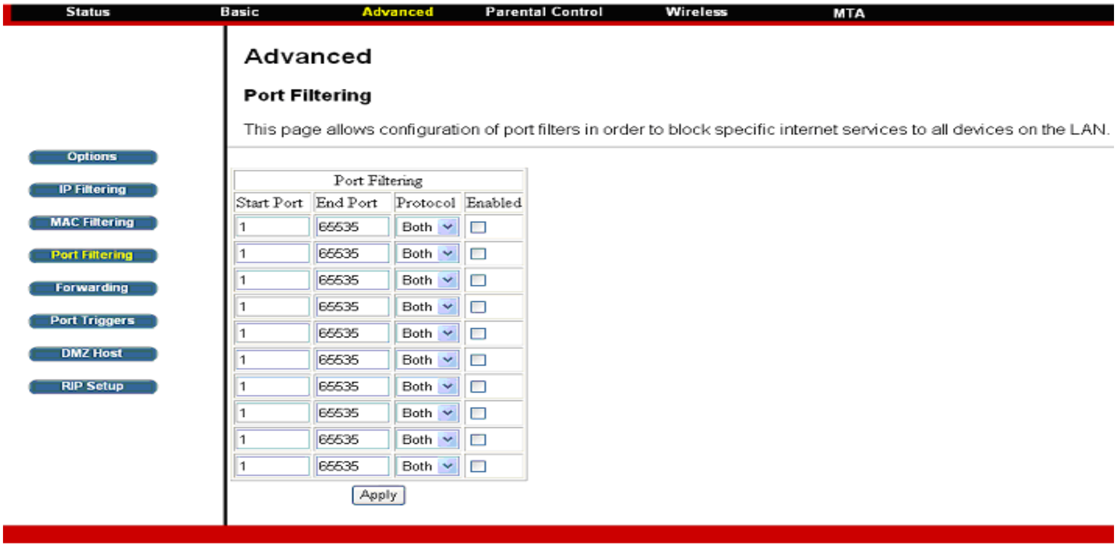
MAC Addresses (example: 01:23:45:67:89:AB)

Addresses entered: 0/20

To enable MAC filtering feature of CBV383Z4S-N300 , enter the MAC address of the LAN device and click **Apply** button.

4.4.4 Port Filtering

The Port Filtering page allows you to enter ranges of destination ports (applications) that you don't want your LAN PCs to send packets to. Any packets your LAN PCs send to these destination ports will be blocked. For example, you could block access to worldwide web browsing (HTTP port 80) but still allow email service (SMTP port 25 and POP3 port 110).



Advanced

Port Filtering

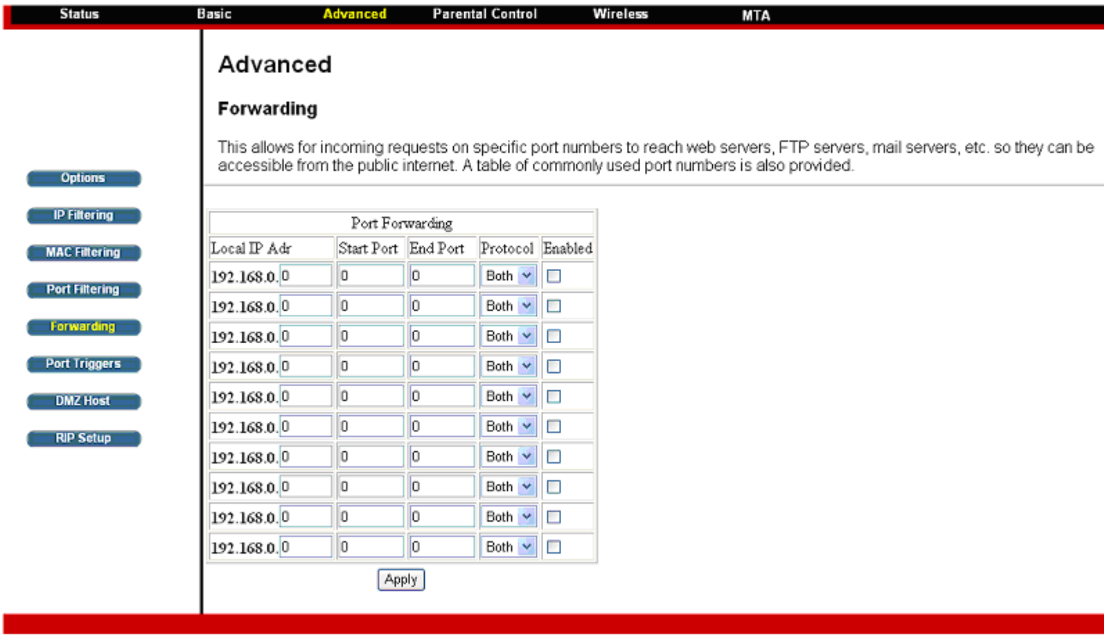
This page allows configuration of port filters in order to block specific internet services to all devices on the LAN.

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	□

To enable port filtering, enter the **Start port** and **End port** for each range. Then select its protocol form the drop-down list and check the **Enable** box, and click **Apply** button. To block only one port, set both Start and End ports the same.

4.4.5 Forwarding

For communications between LAN and WAN, the CBV383Z4S-N300 normally only allows you to originate an IP connection with a PC on the WAN; it will ignore attempts of the WAN PC to originate a connection onto your PC. This protects you from malicious attacks from outsiders. However, sometimes you may wish for anyone outside to be able to originate a connection to a particular PC on your LAN if the destination port (application) matches one you specify.
The Forwarding page allows you to specify up to 10 rules.



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.

Port Forwarding

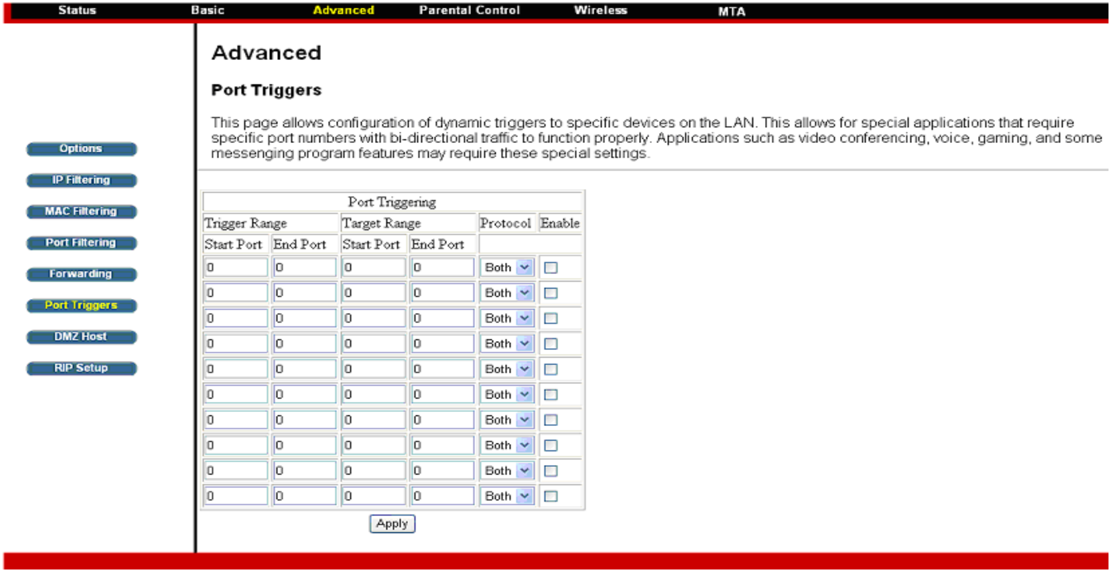
Local IP Adr	Start Port	End Port	Protocol	Enabled
192.168.0. 0	0	0	Both	□
192.168.0. 0	0	0	Both	□
192.168.0. 0	0	0	Both	□
192.168.0. 0	0	0	Both	□
192.168.0. 0	0	0	Both	□
192.168.0. 0	0	0	Both	□
192.168.0. 0	0	0	Both	□
192.168.0. 0	0	0	Both	□
192.168.0. 0	0	0	Both	□
192.168.0. 0	0	0	Both	□

Using the Port Forwarding page, you can provide local services (web servers, FTP servers, mail servers, etc) for people on the Internet or play Internet games. A table of commonly used port numbers is also provided.

4.4.6 Port Triggers

The Port Triggers page allows you to configure 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.

Port Triggering is an elegant mechanism that does the forwarding for you, each time you play the game.
You can specify up to 10 port ranges on which to trigger.



Advanced

Port Triggers

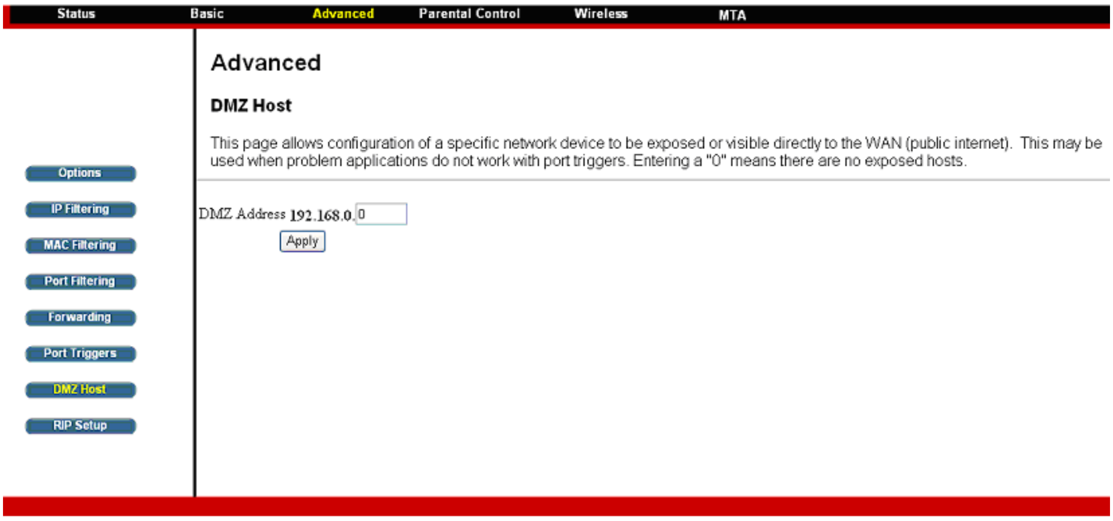
This page allows configuration of dynamic triggers to specific devices on the LAN. This allows for special applications that require specific port numbers with bi-directional traffic to function properly. Applications such as video conferencing, voice, gaming, and some messenging program features may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

Port Triggering

Trigger Range		Target Range		Protocol	Enable
Start Port	End Port	Start Port	End Port		
0	0	0	0	Both	□
0	0	0	0	Both	□
0	0	0	0	Both	□
0	0	0	0	Both	□
0	0	0	0	Both	□
0	0	0	0	Both	□
0	0	0	0	Both	□
0	0	0	0	Both	□
0	0	0	0	Both	□
0	0	0	0	Both	□

4.4.7 DMZ Host

The DMZ page allows you to configure a specific network device to be exposed or visible directly to the WAN (public Internet). Setting a host on your local network as demilitarized zone (DMZ) forwards any network traffic that is not redirected to another host via the port forwarding feature to the IP address of the host (PC). This designates one PC on your LAN that should be left accessible to all PCs from the WAN side for all ports. For example, if you locate a HTTP server on this machine, anyone will be able to access that HTTP server by using your CBV383Z4S-N300 's IP address as the destination. This may be used when problem applications do not work with port triggers. The setting of "0" indicates NO DMZ PC.



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

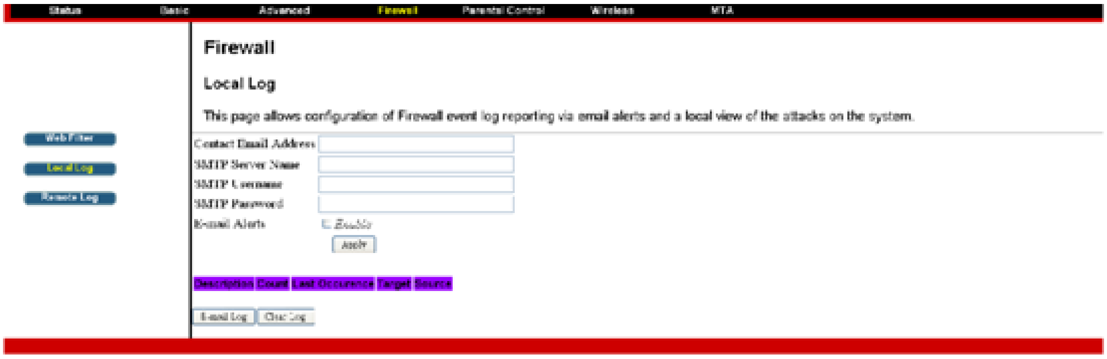
Apply

4.5 Firewall

The CBV383Z4S-N300 provides built-in firewall functions, enabling you to protect the system against denial of service (DoS) attacks and other unwelcome or malicious accesses to your LAN.

4.5.1 Local Log

The Local Log page allows you to configure the firewall event log reported via email alert, and these attack records are also visible in the table on the bottom of this 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

Apply

Description	Count	Last Occurence	Target	Source

E-mail Log Clear Log

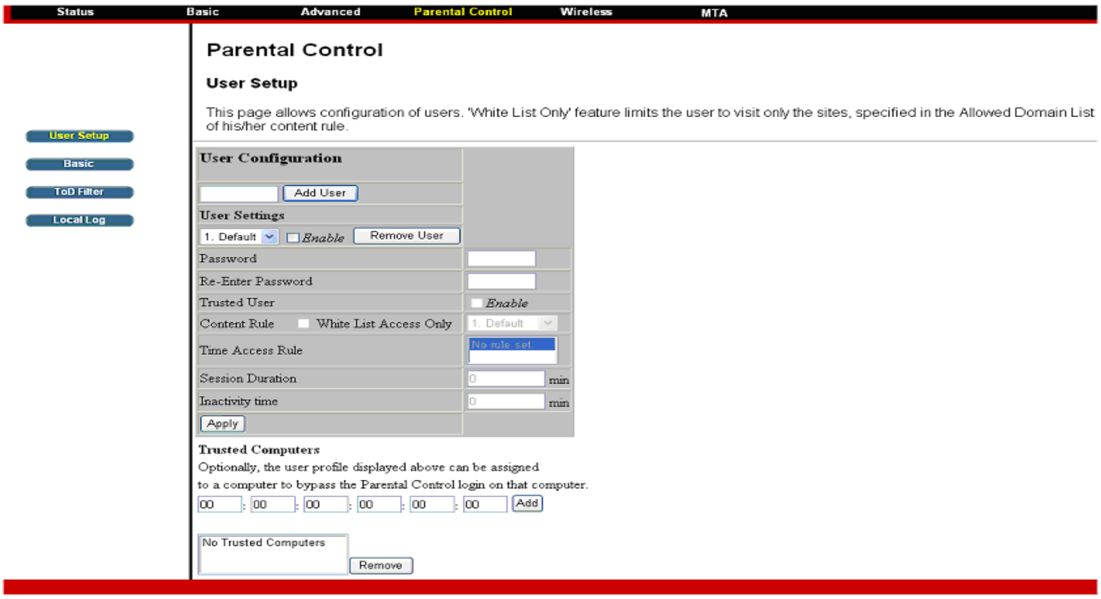
Specifies the e-mail address and its SMTP of the administrators who should receive notices of any attempted firewall violations. Type the addresses in standard Internet e-mail address format, for example, yourname@onecompany.com. Then check the **Enable** box to enable the alert feature.

Click **E-mail Log** to immediately send the email log. Click **Clear Log** to clear the table of entries for a fresh start.

4.6 Parental Control

4.6.1 User Setup

This page allows configuration of users. "White List Only" feature limits the user to visit only the sites, specified in the Allowed Domain List of his/her content rule.



Parental Control

User Setup

This page allows configuration of users. 'White List Only' feature limits the user to visit only the sites, specified in the Allowed Domain List of his/her content rule.

User Configuration

User Settings

1. Default □ Enable

Password	
Re-Enter Password	
Trusted User	□ Enable
Content Rule □ White List Access Only	1. Default
Time Access Rule	No rule set.
Session Duration	0 min
Inactivity time	0 min

Trusted Computers

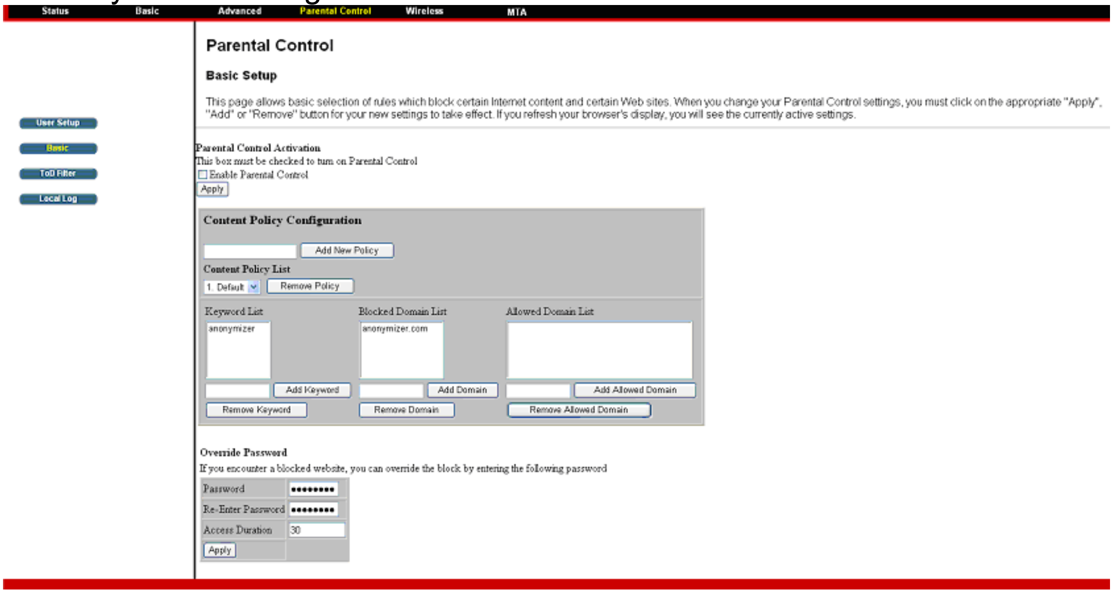
Optionally, the user profile displayed above can be assigned to a computer to bypass the Parental Control login on that computer.

00 : 00 : 00 : 00 : 00 : 00

No Trusted Computers

4.6.2 Basic Setup

This page allows basic selections of rules which block certain Internet content and certain Web sites. When you change your Parental Control settings, you must click on the appropriate "Apply", "Add" or "Remove" button for your new setting to take effect. If you refresh your browser's display, you will see the currently active settings.



Parental Control

Basic Setup

This page allows basic selection of rules which block certain Internet content and certain Web sites. When you change your Parental Control settings, you must click on the appropriate "Apply", "Add" or "Remove" button for your new settings to take effect. If you refresh your browser's display, you will see the currently active settings.

Parental Control Activation

This box must be checked to turn on Parental Control

□ Enable Parental Control

Content Policy Configuration

Content Policy List

1. Default

Keyword List	Blocked Domain List	Allowed Domain List
anonymizer	anonymizer.com	

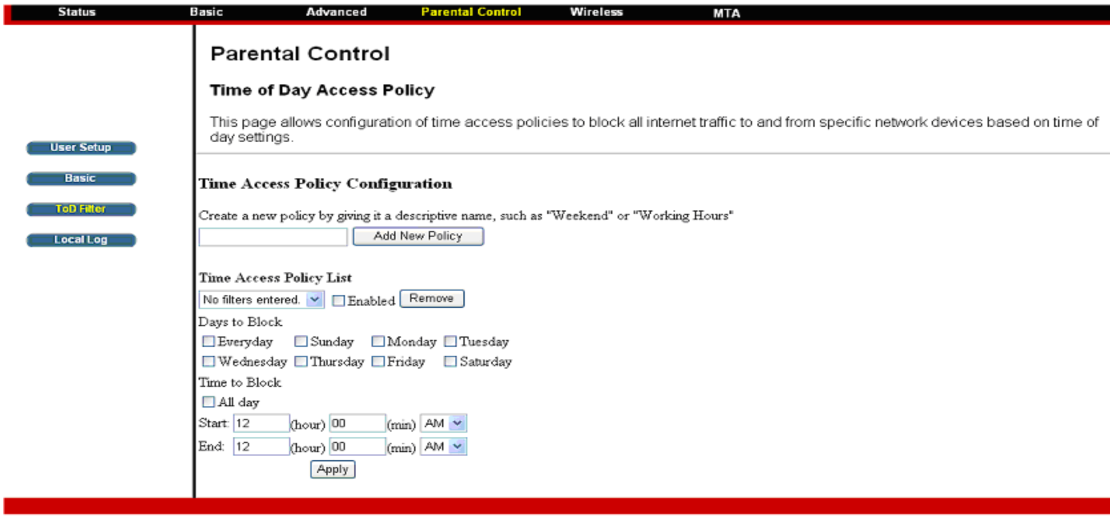
Override Password

If you encounter a blocked website, you can override the block by entering the following password

Password	●●●●●●●●
Re-Enter Password	●●●●●●●●
Access Duration	30

4.6.3 Time of Day Access Policy

This page allows configuration of time access policies to block all internet traffic to and from specific network devices based on time of day setting.



Parental Control

Time of Day Access Policy

This page allows configuration of time access policies to block all internet traffic to and from specific network devices based on time of day settings.

Time Access Policy Configuration

Create a new policy by giving it a descriptive name, such as "Weekend" or "Working Hours"

Time Access Policy List

No filters entered. □ Enabled

Days to Block

□ Everyday □ Sunday □ Monday □ Tuesday
□ Wednesday □ Thursday □ Friday □ Saturday

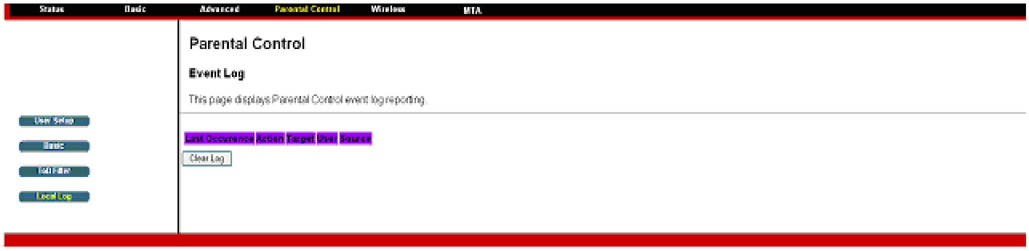
Time to Block

□ All day

Start: 12 (hour) 00 (min) AM
End: 12 (hour) 00 (min) AM

4.6.4 Event Log

This page displays Parental Control event log reporting.



Parental Control

Event Log

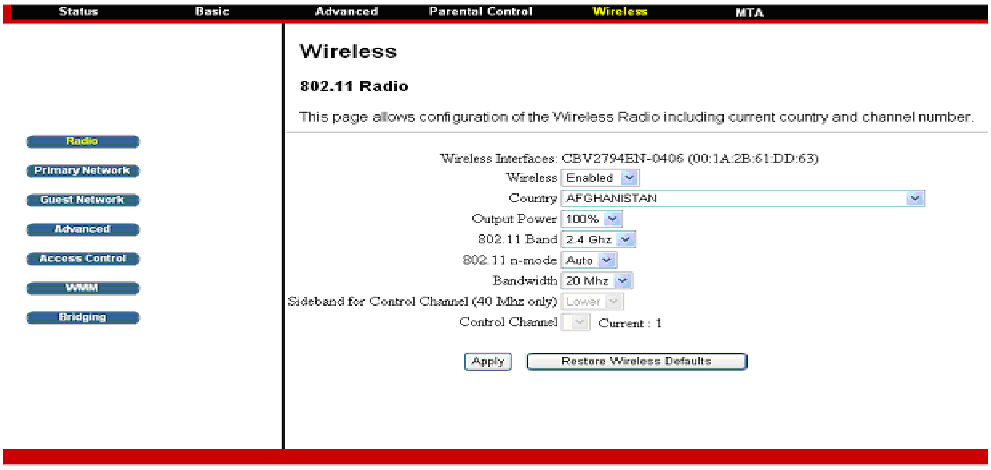
This page displays Parental Control event log reporting.

Last Occurence	Action	Target	User	Source

4.7 Wireless

4.7.1 Radio

The Wireless Connection Stage Configuration of the Wireless Radio includes current country and channel number.



Wireless

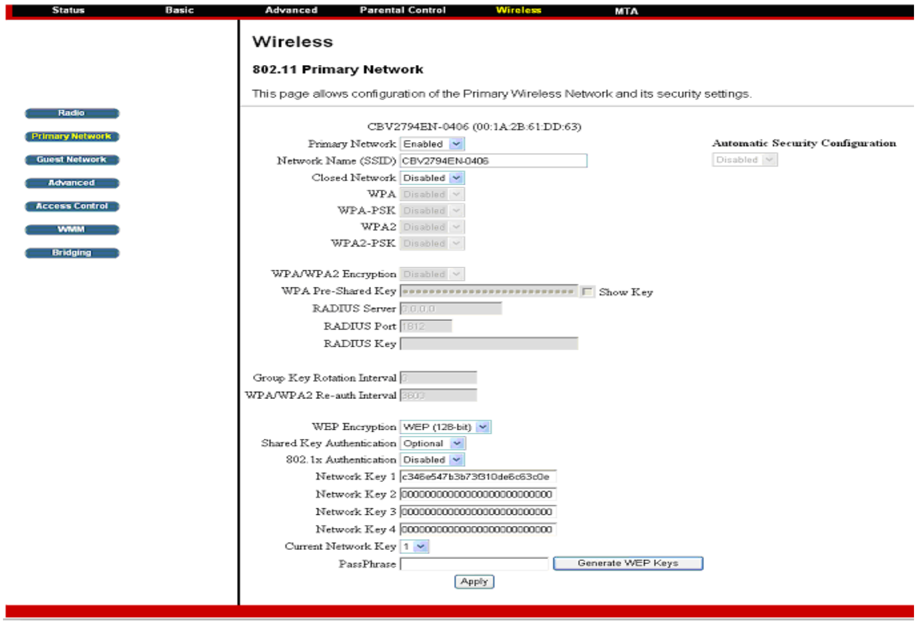
802.11 Radio

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

Wireless Interfaces: CBV2794EN-0406 (00:1A:2B:61:DD:63)
Wireless Enabled
Country AFGHANISTAN
Output Power 100%
802.11 Band 2.4 Ghz
802.11 n-mode Auto
Bandwidth 20 Mhz
Sideband for Control Channel (40 Mhz only) Lower
Control Channel Current : 1

4.7.2 802.11 Primary Network

The 802.11 Primary Network allows configuration of the Primary Wireless Network and its security settings.



Wireless

802.11 Primary Network

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

CBV2794EN-0406 (00:1A:2B:61:DD:63)

Primary Network: Enabled
Network Name (SSID): CBV2794EN-0406
Closed Network: Disabled
WPA: Disabled
WPA-PSK: Disabled
WPA2: Disabled
WPA2-PSK: Disabled

Automatic Security Configuration: Disabled

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

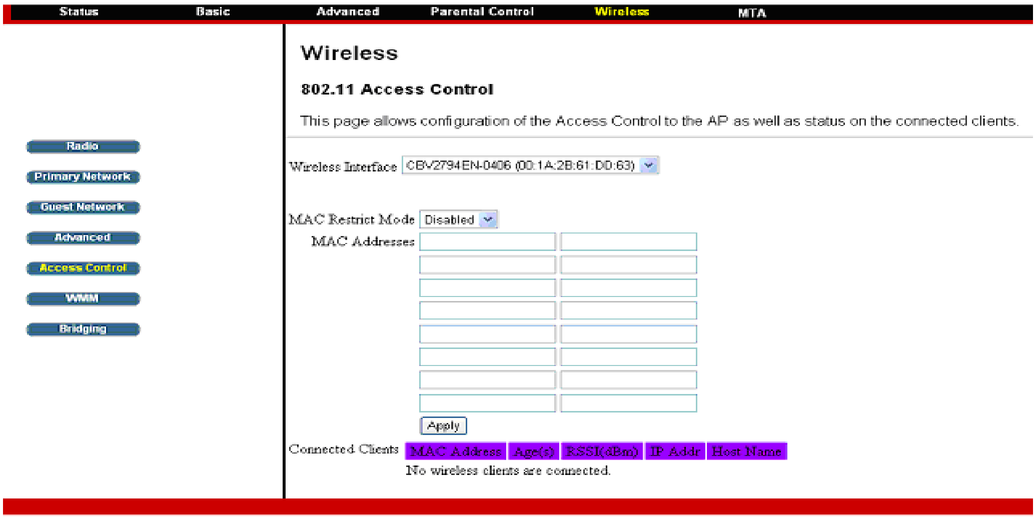
Group Key Rotation Interval: 0
WPA/WPA2 Re-auth Interval: 3600

WEP Encryption: WEP (128-bit)
Shared Key Authentication: Optional
802.1x Authentication: Disabled
Network Key 1: c346e547b3b73f310de6c63c0e
Network Key 2: 00000000000000000000000000
Network Key 3: 00000000000000000000000000
Network Key 4: 00000000000000000000000000
Current Network Key: 1
PassPhrase: [Generate WEP Keys]

[Apply]

4.7.3 Access Control

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



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: CBV2794EN-0406 (00:1A:2B:61:DD:63)

MAC Restrict Mode: Disabled
MAC Addresses:

[Apply]

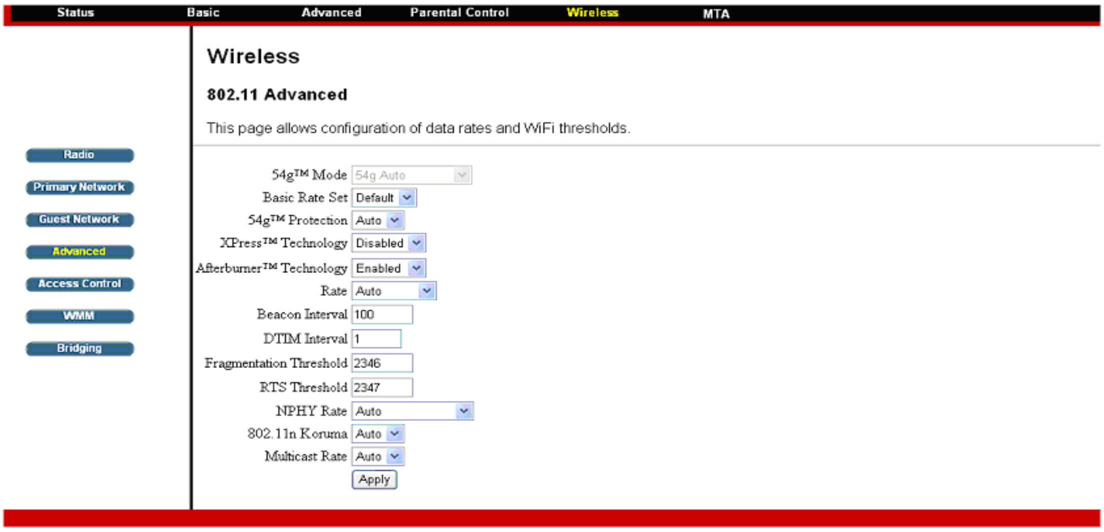
Connected Clients

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

No wireless clients are connected.

4.7.4 Advanced

This page allows configuration of data rates and WiFi thresholds.



Wireless

802.11 Advanced

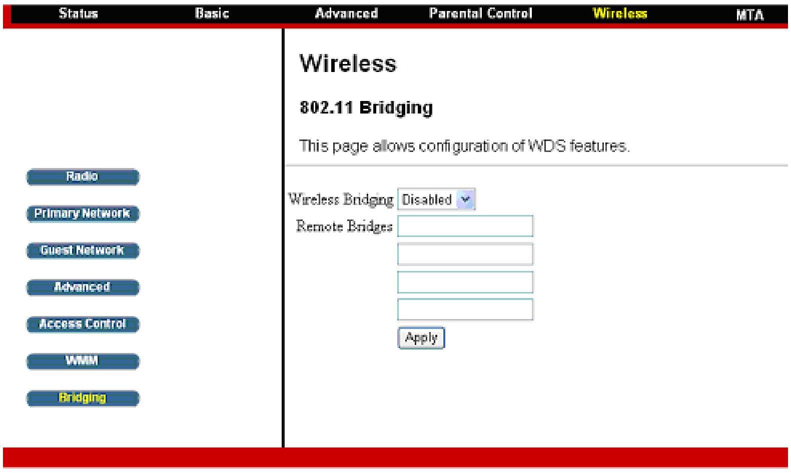
This page allows configuration of data rates and WiFi thresholds.

54g™ Mode	54g Auto
Basic Rate Set	Default
54g™ Protection	Auto
XPress™ Technology	Disabled
Afterburner™ Technology	Enabled
Rate	Auto
Beacon Interval	100
DTIM Interval	1
Fragmentation Threshold	2346
RTS Threshold	2347
NPHY Rate	Auto
802.11n Koruma	Auto
Multicast Rate	Auto

Apply

4.7.5 Bridging

This page allows configuration of WDS features.



Wireless

802.11 Bridging

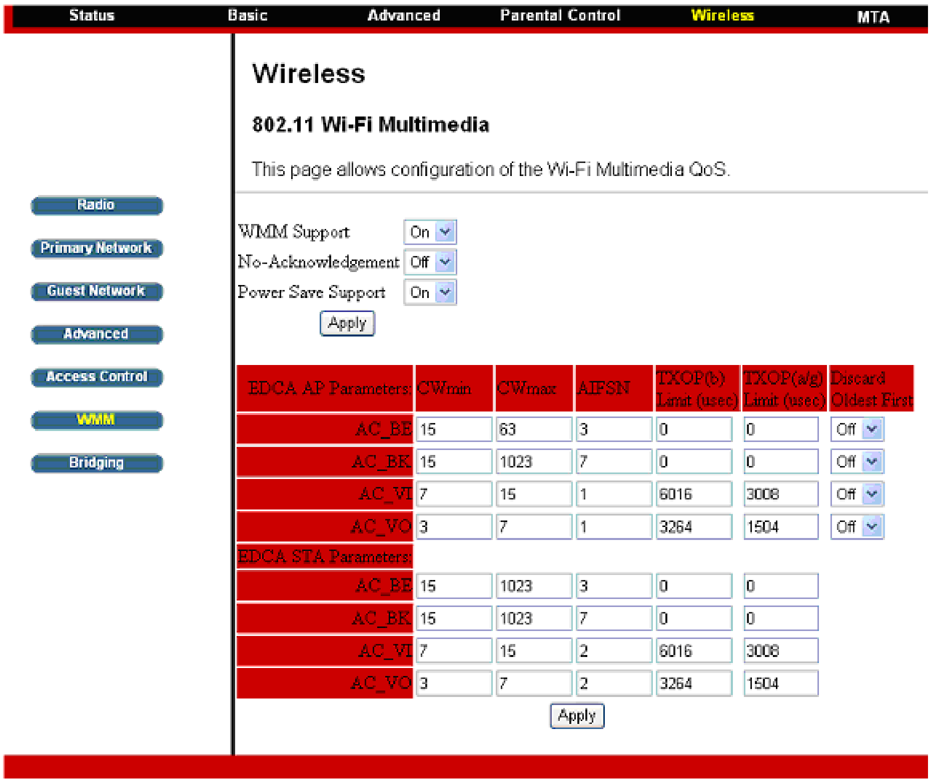
This page allows configuration of WDS features.

Wireless Bridging	Disabled
Remote Bridges	

Apply

4.7.6 WMM

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



Wireless

802.11 Wi-Fi Multimedia

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

WMM Support	On
No-Acknowledgement	Off
Power Save Support	On

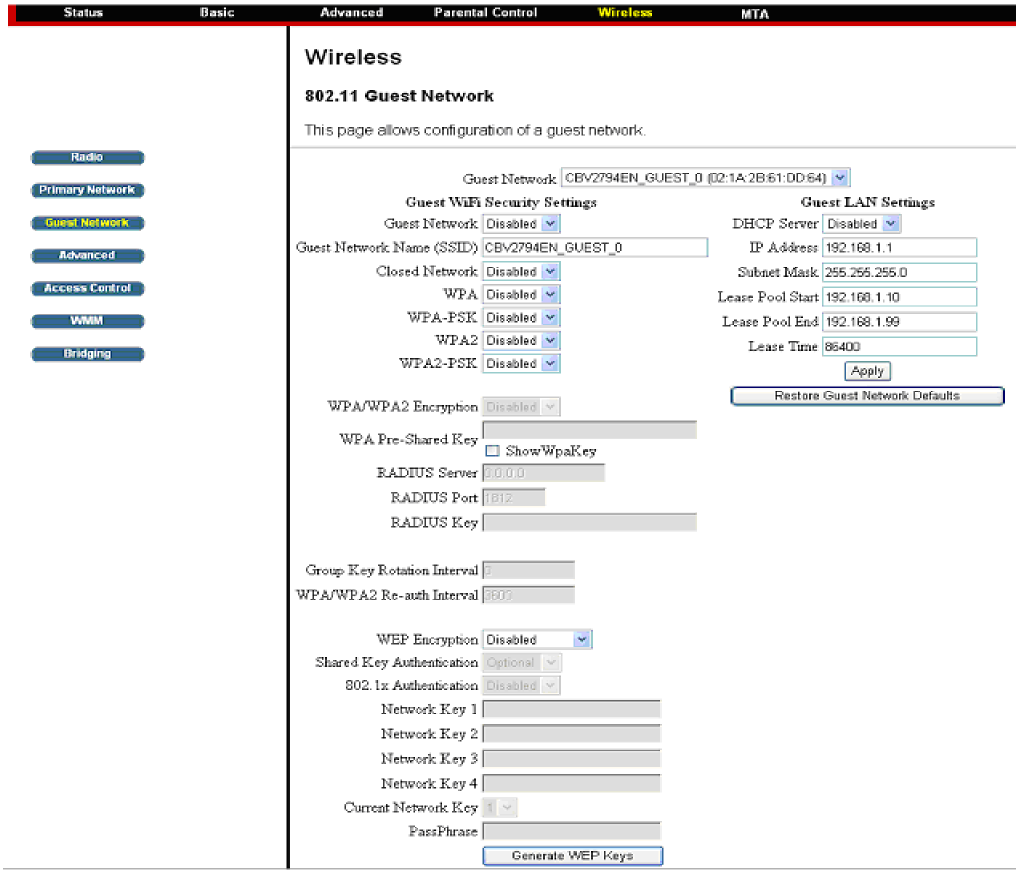
Apply

EDCA AP Parameters:	CWmin	CWmax	AIFSN	TXOP(b) Limit (usec)	TXOP(a/g) Limit (usec)	Discard Oldest First
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	

Apply

4.7.7 Guest Network

This page allows configuration of a guest network..



Wireless

802.11 Guest Network

This page allows configuration of a guest network.

Guest Network CBV2794EN_GUEST_0 (02:1A:2B:61:0D:64)

Guest WiFi Security Settings

Guest Network	Disabled
Guest Network Name (SSID)	CBV2794EN_GUEST_0
Closed Network	Disabled
WPA	Disabled
WPA-PSK	Disabled
WPA2	Disabled
WPA2-PSK	Disabled
WPA/WPA2 Encryption	Disabled
WPA Pre-Shared Key	
	□ ShowWpaKey
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	

Generate WEP Keys

Guest LAN Settings

DHCP Server	Disabled
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

Apply

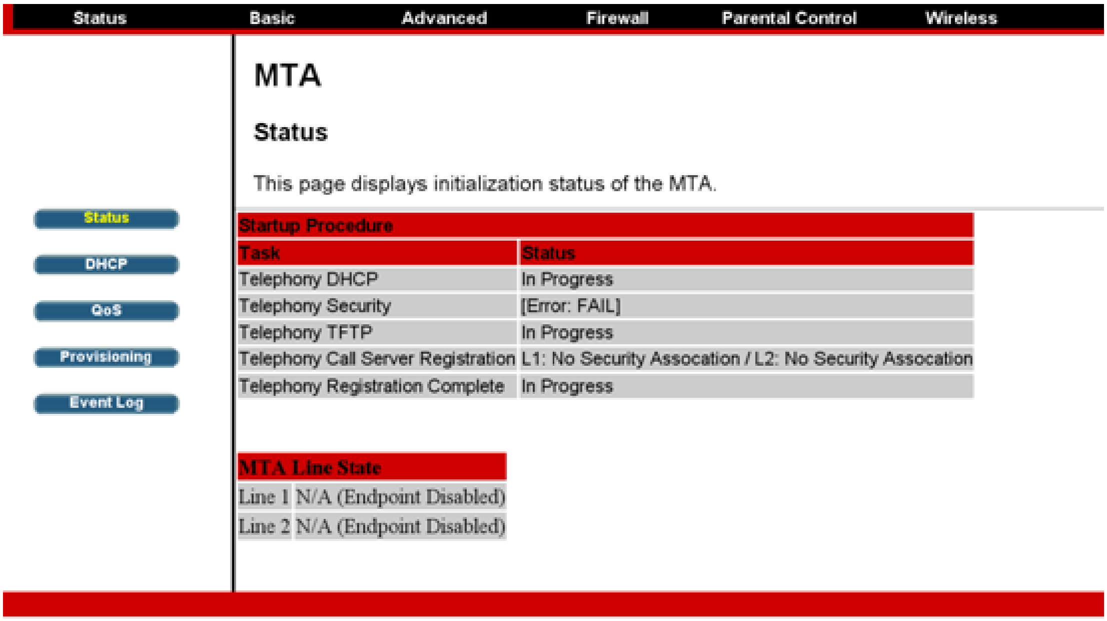
Restore Guest Network Defaults

4.8 MTA

Section MTA has 5 sub-items, which indicate the status of MTA. These information can help you to understand the parameters of MTA operation.

4.8.1 Status

This page displays initialization status of the MTA.



MTA

Status

This page displays initialization status of the MTA.

Startup Procedure	
Task	Status
Telephony DHCP	In Progress
Telephony Security	[Error: FAIL]
Telephony TFTP	In Progress
Telephony Call Server Registration	L1: No Security Assocation / L2: No Security Assocation
Telephony Registration Complete	In Progress

MTA Line State	
Line 1	N/A (Endpoint Disabled)
Line 2	N/A (Endpoint Disabled)

Appendix: Cable Modem Specification

Table 1. RF Downstream Specification (DOCSIS)

Parameter	Value	Notes
Frequency range	88 MHz to 860 MHz +/- 30 kHz	
Demodulation	64QAM. 256QAM	
Input power range	-15 dBmV to +15 dBmV	One Channel
Symbol Rate	5.056941 Msym/sec (30 Mbps) 5.360537 Msym/sec (43 Mbps)	64QAM 256QAM
Bandwidth	6 MHz	
Total Input Power	<30 dBmV	
Input Impedance	75 Ohms	

Table 2. RF Upstream Specification (DOCSIS)

Parameter	Value	
Frequency Range	5 MHz to 85 MHz	
Modulation	QPSK, 8QAM, 16QAM, 32QAM, 64QAM, 128QAM, 256QAM (SCDMA only)	
Symbol Rate	**TDMA**: 160K, 320K, 640K, 1280K, 2560K, 5120Ksym/sec **S-CDMA**: 1280K, 2560K, 5120Ksym/sec	
Bandwidth	**TDMA:** 200K, 400K, 800K, 1600K, 3200K, 6400KHz S-CDMA: 1600K, 3200K, 6400KHz	
Output power	TDMA	QPSK: 8 ~ 58 dBmV 8/16QAM: 8 ~ 55 dBmV 32/64QAM: 8 ~ 54 dBmV
	S-CDMA	QPSK, 8/16/32/64/128QAM: 8 ~ 53 dBmV
Output Impedance	75 Ohms	

Table 3. RF Downstream Specification (for EuroDOCSIS system)

Parameter	Value	Notes
Frequency Range	108 MHz to 862 MHz	
Demodulation	64QAM. 256QAM	
Input power range	+13dBmV to -17dBmV (65QAM) +17dBmV to -13dBmV (256QAM)	
Symbol Rate	056941 Msym/sec (30 Mbps) 5.360537 Msym/sec (43 Mbps)	64QAM 256QAM
Bandwidth	8MHz	
Total Input Power	<30 dBmV	
Input Impedance	75 Ohms	

Table 4. RF Upstream Specification (for EuroDOCSIS system)

Parameter	Value	
Frequency Range	5 MHz to 65 MHz	
Modulation	QPSK, 8QAM, 16QAM, 32QAM, 64QAM, 128QAM (TCM only)	
Symbol Rate	**TDMA**: 160K, 320K, 640K, 1280K, 2560K, 5120Ksym/sec **S-CDMA**: 1280K, 2560K, 5120Ksym/sec	
Bandwidth	**TDMA**: 200K, 400K, 800K, 1600K, 3200K, 6400KHz **S-CDMA**: 1600K, 3200K, 6400KHz	
Output power	TDMA	QPSK: 8 ~ 58 dBmV 8/16QAM: 8 ~ 55 dBmV 32/64QAM: 8 ~ 54 dBmV
	S-CDMA	QPSK, 8/16/32/64/128QAM: 8 ~ 53 dBmV
Output Impedance	75 Ohms	

Table 5. Electrical Specification

Parameter	Measured Value	Notes
Input Voltage	12VDC/2A	
Power consumption	< 9.5W	With AC adaptor

Table 6. Physical Specification

Parameter	Value
Size	160 mm (L) x 36mm(H) x 212 mm (W)
Weight	520g +/- 10g (Modem only)

Table 7. Environmental Specification

Parameter	Value
Operating Temperature	0 °C to +40 °C
Operating Relative Humidity	10% to 90% (Non-condensing)
Operating Altitude	-100 to +7,000 feet
Storage Temperature	-10 °C to +60 °C