

# ***CBV390SL5-X57***

***DOCSIS 3.1 Compliant  
EMTA Gateway with Wi-Fi 6 & 2.5Gb Ethernet  
User Manual***

***Revision 1.0  
March 2023***

# Table of Contents

<b>1. Introduction</b>	<b>6</b>
1.1 Features	6
1.2 System Requirement	6
1.3 Unpacking and Inspection	6
1.4 Safety Precautions	7
<b>2. Hardware Overview</b>	<b>8</b>
2.1 Front Panel and LEDs	8
2.2 Rear Panel and Hardware Connection	10
<b>3. Ethernet Installation</b>	<b>11</b>
<b>4. Web Management</b>	<b>12</b>
4.1 Enter Modem's IP Address	12
4.2 Gateway	13
4.2.1 At a Glance	13
4.2.2 Connection_Status	14
4.2.3 Connection_Network	14
4.2.4 Connection_Local IP Network	16
4.2.5 Connection_Wi-Fi	17
4.2.6 Connection_MTA_Line Status	18
4.3 Firewall	19
4.3.1 Firewall_IPv4	19
4.3.2 Firewall_IPv6	20
4.4 Software	21
4.5 Hardware	21
4.5.1 Hardware_System Hardware	21
4.5.2 Hardware_Wireless	22
4.6 Connected Devices	23
4.6.1 Connected Devices_Devices	23
4.7 Parental Control	24
4.7.1 Parental Control_Managed Sites	24
4.7.2 Parental Control_Managed Services	25
4.7.3 Parental Control_Managed Devices	26
4.7.4 Parental Control_Reports	27

4.8	Advanced .....	28
4.8.1	Advanced_Port Forwarding .....	28
4.8.2	Advanced_Port Triggering .....	29
4.8.3	Advanced_Remote Management.....	30
4.8.4	Advanced_DMZ.....	31
4.8.5	Advanced_Dynamic DNS.....	31
4.8.6	Advanced_Device Discovery.....	32
4.9	Troubleshooting.....	33
4.9.1	Troubleshooting_Logs.....	33
4.9.2	Troubleshooting_Diagnostic Tools .....	33
4.9.3	Troubleshooting_Reset/Restore Gateway.....	34
4.9.4	Troubleshooting_Change Password .....	35
<b>Appendix: Cable Modem Specification.....</b>		<b>36</b>

## **Note to CATV System 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."

## **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 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.

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.

**FCC Caution:** Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. The device is for indoor use only.

## **IMPORTANT NOTE:**

### **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 50cm between the radiator & your body

### **FCC RF Radiation Exposure Statement:**

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

## **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.

# 1. Introduction

The CBV390SL5-X57 is the integration of 4 ports switch and IEEE 802.11a/b/g/n/ac/ax wireless functionality, the CBV390SL5-X57 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.

## 1.1 Features

- DOCSIS 3.1 Compliant
- DOCSIS/EuroDOCSIS 3.0 Backwards Compatible
- PacketCable 2.0 and EuroPacketCable 1.5 Compliant
- DOCSIS 3.1 2x2 OFDM(A) Channels
- DOCSIS 3.0 32x8 Channel Bonding
- Switchable Diplexer
- Wi-Fi 6 4x4 for 2.4GHz and 5GHz
- 1-port 2.5Gb Ethernet
- 4-Port Gigabit Ethernet
- 2-Port FXS
- 1-Port USB 3.2 Gen1x1

## 1.2 System Requirement

- 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 CBV390SL5-X57
- 1 x Quick Installation Guide
- 1 x RJ-45 CAT 5e Cable
- 1 x 12V/3.5A Power Supply Adaptor

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



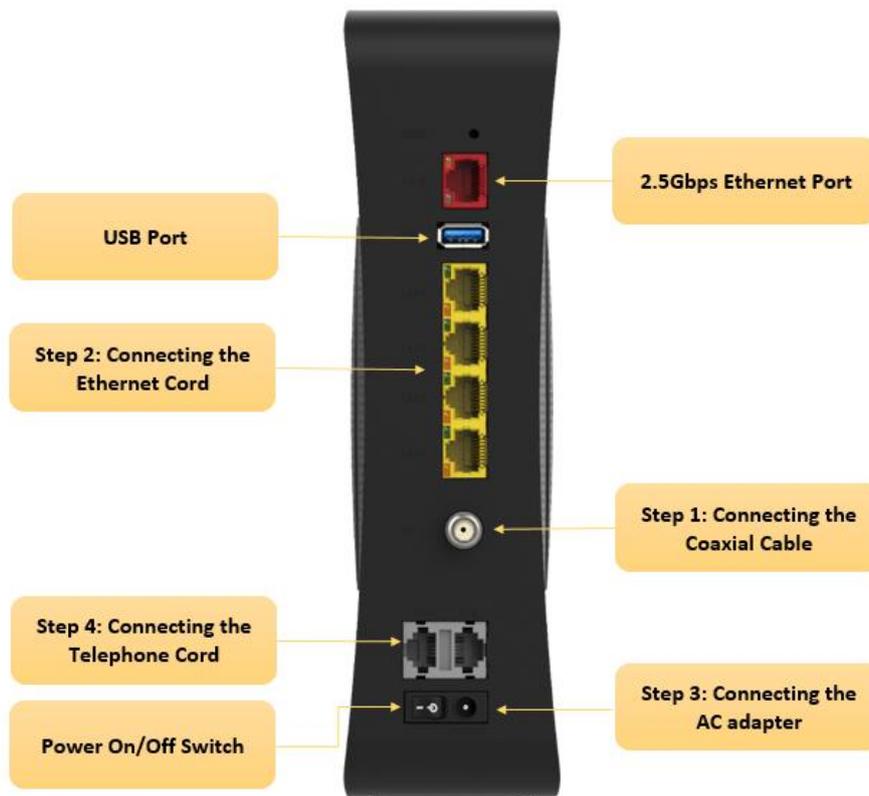
### 2.1 Front Panel and LEDs

There are 10 Light-Emitting-Diodes (LEDs) located on the front panel top to provide status information to the user.

NAME	COLOR	MODE	STATUS
POWER	Green	On	Power Connected
		Off	Power Failure or Disconnect
DS	Green	Blinking	Downstream Scanning
		On	Downstream Locked or W/DS Bonding
		Off	Cable Interface Idle
US	Green	Blinking	Upstream Scanning
		On	Upstream Locked or W/US Bonding
		Off	Cable Interface Idle
ONLINE	Green	Blinking	Registering
		On	Registering Finished
		Off	Cable Interface Idle

WLAN 2.4GHz	Green	On	Wireless Enable
		Blinking	Data Traffic Processing
		Off	Wireless Disable
WLAN 5GHz	Green	On	Wireless Enable
		Blinking	Data Traffic Processing
		Off	Wireless Disable
WPS	Green	Blinking	WPS Paring
		On	WPS Enabled
		Off	WPS Disabled
TEL1	Green	Blinking	TEL1 provisioning of off-hook
		On	TEL1 on-hook
		Off	TEL1 disabled
TEL2	Green	Blinking	TEL2 provisioning of off-hook
		On	TEL2 on-hook
		Off	TEL2 disabled
USB	Green	Blinking	USB Provisioning of Off-hook
		On	USB On-hook
		Off	USB Disabled

## 2.2 Rear Panel and Hardware Connection



**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.

**Step 2:** Connect the cable modem to a GbE Ethernet 10/100/1000 Mbps Network using a RJ-45 male-terminated Ethernet cable. This cable modem equips with four Ethernet ports, you can connect four PCs to the cable modem at the same time if necessary.

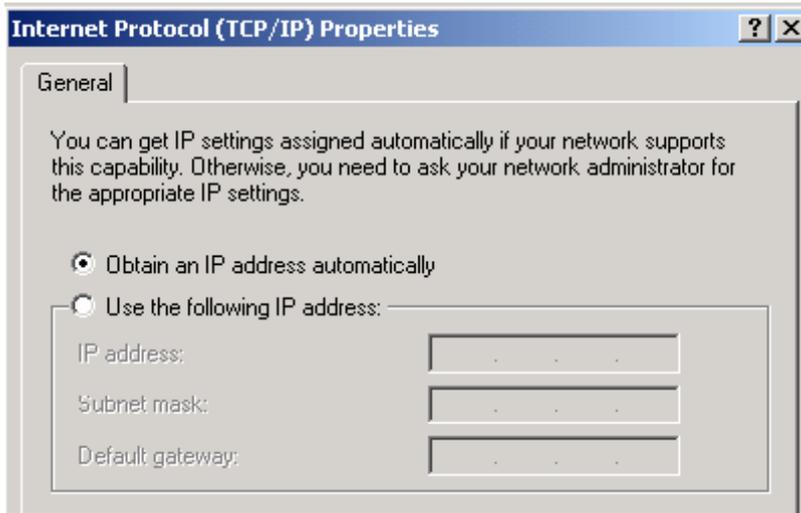
**Step 3:** Connect the AC Adapter to the cable modem by inserting the barrel- shaped connector into the mating power connector on the back of the cable modem. Exercise carefully to ensure the connectors are properly aligned prior to insertion and ensure the two connectors engage completely. The cable 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 4:** 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.

### 3. Ethernet Installation

The LAN port you are using is auto-negotiating 10/100Mbps (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.



Following is an example of configuring the TCP/IP Protocol on Windows 98 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.

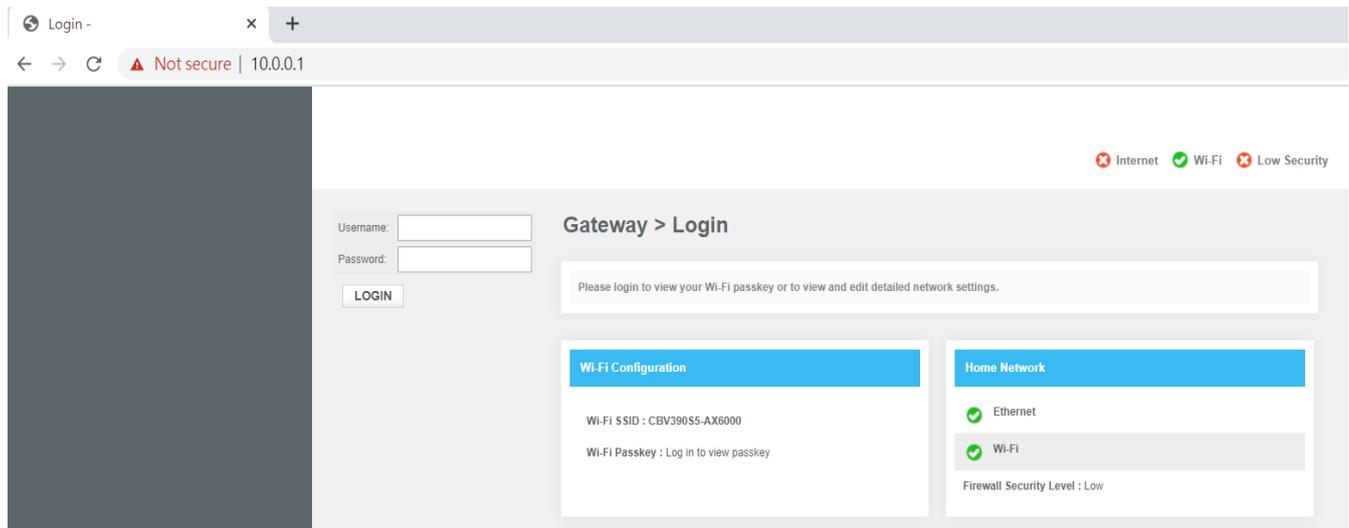
## 4. Web Management

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 CBV390SL5-X57.

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 CBV390SL5-X57 (e.g. 10.0.0.1) and press Enter.  
The Log In page appears. Type the user name (admin) and your password (password) in the respective fields.



3. There are five categories in this web management including Gateway, Connected Devices, Parental Control, Advanced, and Troubleshooting. The following sections describe their details.

## 4.2 Gateway

There are five sections under this category, including [At a Glance](#), [Connection](#), [Firewall](#), [Software](#), and [Hardware](#).

This page shows the summary of your network and connected devices.

### 4.2.1 At a Glance

This page shows the summary of your network and connected devices. Select [VIEW CONNECTED DEVICES](#) to manage devices connected to your network.

The screenshot displays the 'Gateway > At a Glance' page. On the left is a navigation menu with 'Gateway' selected, containing sub-items: 'At a Glance', 'Connection', 'Firewall', 'Software', 'Hardware', 'Connected Devices', 'Parental Control', 'Advanced', and 'Troubleshooting'. The main content area is titled 'Gateway > At a Glance' and includes a summary box with a 'more' link. Below this is the 'Wi-Fi Configuration' section showing 'Wi-Fi SSID : C8V39055-AX6000' and 'Wi-Fi Passkey: 1234567890'. A 'Bridge Mode' section has 'Enable' and 'Disable' buttons, with 'Disable' being active. The 'Home Network' section shows 'Ethernet' as active (green checkmark) and 'Wi-Fi' as inactive (red X). The 'Firewall Security Level : Low' is noted. The 'Connected Devices' section features a 'VIEW CONNECTED DEVICES' button.

## 4.2.2 Connection\_Status

This page shows the information about your network connections. To view and manage the settings of your local IP, Wi-Fi and Networks

The screenshot shows the 'Gateway > Connection > Status' page. On the left is a navigation menu with 'Gateway' selected, and sub-items: 'At a Glance', 'Connection', 'Status' (highlighted), 'Network', 'Local IP Network', 'Wi-Fi', 'Firewall', 'Software', 'Hardware', 'Connected Devices', 'Parental Control', 'Advanced', and 'Troubleshooting'. The main content area has a title 'Gateway > Connection > Status' and a subtitle 'View information about your network connections.' with a 'more' link. There are three main sections: 1. 'Local IP Network' (EDIT button): IP Address (IPv4): 10.0.0.1, Subnet mask: 255.255.255.0, DHCPv4 Server: Enabled, DHCPv4 Lease Time: 1 Week, Link Local Gateway Address (IPv6): fe80::10:18ff:fe38:7430, Global Gateway Address (IPv6):, Delegated prefix:, DHCPv6 Lease Time: 1 Week, IPv6 DNS:, No of Clients connected: 1. 2. 'Private Wi-Fi Network-CBV390S5-AX6000' (EDIT button): Wireless Network (Wi-Fi 2.4 GHz): Active, Supported Protocols: G,N, Security: WPA2-PSK (AES), No of Clients connected: 0. 3. 'Private Wi-Fi Network-CBV390S5-AX6000' (EDIT button): Wireless Network (Wi-Fi 5 GHz): Active, Supported Protocols: A,N,AC, Security: WPA2-PSK (AES), No of Clients connected: 0. Below these is a 'Network' (VIEW button) section: Internet: Inactive, WAN IP Address: 0.0.0.0, DHCP Client: Enabled, DHCP Expire Time: 0d:0h:1m.

## 4.2.3 Connection\_Network

View technical information related to your network connection.

View and manage the settings for your local IP, Wi-Fi and networks

The screenshot shows the 'Gateway > Connection > Network' page. The left navigation menu is the same as in the previous screenshot. The main content area has a title 'Gateway > Connection > Network' and a subtitle 'View technical information related to your network connection.' with a 'more' link. At the top, there is a 'Lock downstream' section with a value of '0' and a 'GOTO' button. Below is a 'Network' (VIEW button) section with the following details: Internet: Inactive, Local time: 2020-02-12 03:43:35, System Uptime: 0 days 0h: 5m: 58s, WAN IP Address (IPv4): 0.0.0.0, WAN Default Gateway Address (IPv4):, WAN IP Address (IPv6):, WAN Default Gateway Address (IPv6):, Delegated prefix (IPv6):, Primary DNS Server (IPv4):, Secondary DNS Server (IPv4):, Primary DNS Server (IPv6):, Secondary DNS Server (IPv6):, WAN Link Local Address (IPv6):, DHCP Client (IPv4): Enabled, DHCP Client (IPv6): Disabled, DHCP Lease Expire Time (IPv4): 0d:0h:1m, DHCP Lease Expire Time (IPv6): 0d:0h:0m, WAN MAC: FC:4A:E9:59:60:86, eMTA MAC: FC:4A:E9:59:60:85, CM MAC: FC:4A:E9:59:60:84.

### Initialization Procedure

Initialize Hardware:	Complete
Acquire Downstream Channel:	NotStarted
Upstream Ranging:	NotStarted
DHCP bound:	NotStarted
Set Time-of-Day:	NotStarted
Configuration File Download:	NotStarted
Registration:	NotStarted

Downstream	Channel Bonding Value
Index	0
Lock Status	Not locked
Frequency	0 MHz
SNR	0.0 dB
Power Level	-50.8 dBmV
Modulation	other

Upstream	Channel Bonding Value
Index	
Lock Status	
Frequency	
Symbol Rate	
Power Level	
Modulation	
Channel Type	

CM Error Codewords	
Unerrored Codewords	0
Correctable Codewords	0
Uncorrectable Codewords	0

## 4.2.4 Connection\_Local IP Network

Manage your home network settings.

Gateway address: Enter the IP address of the Gateway.

Subnet Mask: The subnet mask is associated with the IP address. Select the appropriate subnet mask based on the number of devices that will be connected to your network.

DHCP Beginning and Ending Addresses: The DHCP server in the Gateway allows the router to manage IP address assignment for the connected devices.

DHCP Lease time: The lease time is the length of time the Gateway offers an IP address to a connected device. The lease is renewed while it is connected to the network. After the time expires, the IP address is freed and may be assigned to any new device that connects to the Gateway.

The screenshot displays the 'Gateway > Connection > Local IP Configuration' page. On the left is a navigation menu with options: Gateway, At a Glance, Connection, Status, Network, Local IP Network (selected), Wi-Fi, Firewall, Software, Hardware, Connected Devices, Parental Control, Advanced, and Troubleshooting. The main content area is titled 'Gateway > Connection > Local IP Configuration' and includes a sub-header 'Manage your home network settings.' with a 'HELP' link. The IPv4 section contains: Gateway Address (10.0.0.1), Subnet Mask (255.255.255.0), DHCP Beginning Address (10.0.0.2), DHCP Ending Address (10.0.0.253), and DHCP Lease Time (1 Weeks). The IPv6 section contains: Link-Local Gateway Address (fe80::0:0:0:10:18ff:fe35:5f7), Global Gateway Address (empty), LAN IPv6 Address Assignment (checked for Stateless and Stateful), DHCPv6 Beginning Address (:::0:0:0:0:0:0:0001/64), DHCPv6 Ending Address (:::0:0:0:0:0:0:0:ffe/64), and DHCPv6 Lease Time (1 Weeks). Both sections have 'SAVE SETTINGS' and 'RESTORE DEFAULT SETTINGS' buttons.

## 4.2.5 Connection\_Wi-Fi

Manage your Wi-Fi connection settings.

Click EDIT next to the Network Name you'd like to modify its Wi-Fi network settings: Network Name (SSID), Mode, Security Mode, Channel, Network Password (Key), and Broadcasting feature.

MAC Filter Setting is specific to each Network Name (SSID). Select a MAC Filtering Mode.

Allow- All (Default): All wireless client stations can connect to the Gateway; no MAC filtering rules.

Allow: Only the devices in the "Wireless Control List" are allowed to connect to the Gateway.

Deny: Wireless devices in the "Wireless Control List" are not allowed to connect to the Gateway.

Wireless Control List: Displays the wireless devices (by Network Name and MAC Address) that were manually added or auto-learned.

Auto-Learned Wireless Devices are currently connected to the Gateway.

Manually-Added Wireless Devices: Enter a unique name and MAC address for the wireless device you want to manually add, then click ADD.

Band Steering: The device will connect to 5G by default if it supports both 2.4G and 5G,if you want to use 2.4G by default, please use different SSID.

The screenshot displays the 'Gateway > Connection > Wi-Fi' configuration page. On the left is a navigation menu with options like Gateway, Connection, Status, Network, Local IP Network, Wi-Fi, Firewall, Software, Hardware, Connected Devices, Parental Control, Advanced, and Troubleshooting. The main content area is titled 'Gateway > Connection > Wi-Fi' and includes a 'Manage your Wi-Fi connection settings.' link. It features two sections for network settings: 'Private Wi-Fi Network' and 'Guest Wi-Fi Network'. Each section contains a table with columns for Name, Frequency Band, MAC Address, and Security Mode, along with an 'EDIT' button for each entry. Below these is an 'ADD WI-FI PROTECTED SETUP (WPS) CLIENT' button. The 'MAC Filter Setting' section allows selecting an SSID (currently 'CBV390S5-AX6000') and a MAC Filtering Mode (currently 'Allow-All'). It also includes three tables: 'Wi-Fi Control List (up to 32 items)', 'Auto-Learned Wi-Fi Devices', and 'Manually-Added Wi-Fi Devices', each with columns for Device Name and MAC Address. An 'ADD' button is provided for the manually-added devices, and a 'SAVE FILTER SETTING' button is at the bottom.

Name	Frequency Band	MAC Address	Security Mode	
CBV390S5-AX6000	2.4GHz	FC:4A:E9:59:00:88	WPA2-PSK (AES)	EDIT
CBV390S5-AX6000	5GHz	FC:4A:E9:59:00:89	WPA2-PSK (AES)	EDIT

Name	Frequency Band	MAC Address	Security Mode	
CBV390S5-AX6000_GUEST_0_1	2.4 GHz	FE:4A:E9:59:00:89	Open (risky)	EDIT
CBV390S5-AX6000_GUEST_1_1	5 GHz	FE:4A:E9:59:00:8A	Open (risky)	EDIT

## 4.2.6 Connection\_MTA\_Line Status

Information related to the MTA Line Status

Hi admin • [Logout](#) • [Change Password](#)  
✔ Internet ✔ Wi-Fi ✘ Low Security

**Gateway > Connection > MTA > Line Status**

Information related to the MTA Line Status.

### MTA Line Status

Line 1 Status: On-Hook

Line 2 Status: On-Hook

- ▼ Gateway
  - At a Glance
- ▼ Connection
  - Status
  - Network
  - Local IP Network
  - Wi-Fi
  - ▼ MTA
    - Line Status**
  - ▶ Firewall
- Software
- ▶ Hardware
- ▶ Connected Devices
- ▶ Parental Control
- ▶ Advanced
- ▶ Troubleshooting

## 4.3 Firewall

Manage your firewall settings.

### 4.3.1 Firewall\_IPv4

Select a security level for details. If you're unfamiliar with firewall settings, keep the default security level, Minimum Security (Low).

**Maximum Security (High):** Blocks all applications, including voice applications (such as Gtalk, Skype) and P2P applications, but allows Internet, email, VPN, DNS, and iTunes services.

**Typical Security (Medium):** Blocks P2P applications and pings to the Gateway, but allows all other traffic.

**Minimum Security (Low):** No application or traffic is blocked. (Default setting)

**Custom security:** Block specific services.



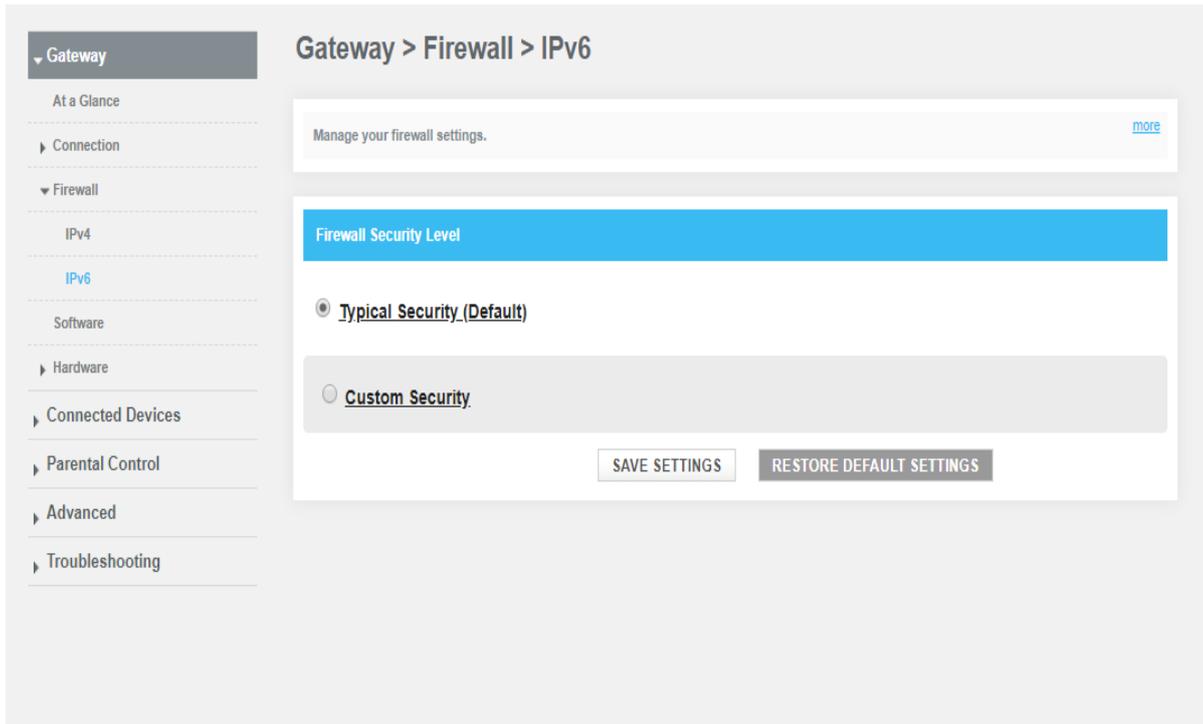
The screenshot shows the 'Gateway > Firewall > IPv4' settings page. On the left is a navigation menu with 'Gateway' selected, and sub-items: 'At a Glance', 'Connection', 'Firewall', 'IPv4', 'IPv6', 'Software', 'Hardware', 'Connected Devices', 'Parental Control', 'Advanced', and 'Troubleshooting'. The main content area has a breadcrumb 'Gateway > Firewall > IPv4' and a sub-header 'Manage your firewall settings.' with a 'more' link. Below this is a section titled 'Firewall Security Level' with four radio button options: 'Maximum Security (High)', 'Typical Security (Medium)', 'Minimum Security (Low)', and 'Custom Security'. The 'Minimum Security (Low)' option is selected. At the bottom are two buttons: 'SAVE SETTINGS' and 'RESTORE DEFAULT SETTINGS'.

### 4.3.2 Firewall\_IPv6

The Software Manage your firewall settings.

Select a security level for details. If you're unfamiliar with firewall settings, keep the default security level, Minimum Security (Low).

Typical Security (Default): Allows all traffic from home network to internet and blocks all unrelated traffic from internet to home network.



## 4.4 Software

View details about the Gateway's software.

You may need this information for troubleshooting assistance.

The screenshot shows a web interface for Gateway management. On the left is a navigation menu with 'Gateway' expanded, showing options like 'At a Glance', 'Connection', 'Firewall', 'Software', 'Hardware', 'Connected Devices', 'Parental Control', 'Advanced', and 'Troubleshooting'. The main content area is titled 'Gateway > Software'. It contains a summary box with the text 'View details about the Gateway's software.' and a 'more' link. Below this is a 'System Software Version' section with the following details:

BOOT Version:	5.0
Software Version:	CBV390S5-AX6000_0001_19331.S.001
Packet Cable:	1.5

## 4.5 Hardware

View information about the Gateway's hardware.

### 4.5.1 Hardware\_System Hardware

View information about the Gateway's hardware.

The screenshot shows a web interface for Gateway management. On the left is a navigation menu with 'Gateway' expanded, showing options like 'At a Glance', 'Connection', 'Firewall', 'Software', 'Hardware', 'Connected Devices', 'Parental Control', 'Advanced', and 'Troubleshooting'. The main content area is titled 'Gateway > Hardware > System Hardware'. It contains a summary box with the text 'View information about the Gateway's hardware.' and a 'more' link. Below this is a 'System Hardware' section with the following details:

Model:	BCM93390SMWVG2_V10
Vendor:	Castlenet.
Hardware Revision:	1.0
Serial Number:	RD122419001
Processor Speed:	751 MHz
DRAM Total Memory:	737 MB
DRAM Used Memory:	185 MB
DRAM Available Memory:	552 MB

## 4.5.2 Hardware\_Wireless

View information about the Gateway's wireless components.

Wi-Fi: The Gateway provides concurrent 2.4 GHz and 5 GHz for Wi-Fi connections.

The screenshot displays the 'Gateway > Hardware > Wireless' configuration page. On the left is a navigation menu with the following items: Gateway (selected), At a Glance, Connection, Firewall, Software, Hardware (expanded), System Hardware, **Wireless**, Connected Devices, Parental Control, Advanced, and Troubleshooting. The main content area is titled 'Gateway > Hardware > Wireless' and contains a summary box with the text 'View information about the Gateway's wireless components.' and a 'more' link. Below this are two panels for the Wi-Fi LAN ports:

Wi-Fi LAN port (2.4 GHZ)	Wi-Fi LAN port (5 GHZ)
Wi-Fi link status: Active	Wi-Fi link status: Active
MAC Address: FC:4A:E9:59:60:88	MAC Address: FC:4A:E9:59:60:89
System Uptime: 0 days 0h: 12m: 28s	System Uptime: 0 days 0h: 12m: 17s

## 4.6 Connected Devices

View information about devices currently connected to your network, as well as connection history.

### 4.6.1 Connected Devices\_Devices

Every device listed below was auto discovered via DHCP.

Online Devices are currently connected to your Gateway.

Offline Devices were once connected to your network, but not currently.

To block Internet access to a device connected to your Gateway, click the X button.

**Connected Devices > Devices**

View information about devices currently connected to your network, as well as connection history. [more](#)

**Prefer Private Connection**

**Online Devices-Private Network**

Host Name	DHCP/Reserved IP	RSSI Level	Connection
<a href="#">DESKTOP-RVE4C9U</a>	DHCP	NA	Ethernet

[EDIT](#) [X](#)

[ADD DEVICE WITH RESERVED IP](#)

**Offline Devices-Private Network**

Host Name	DHCP/Reserved IP	Connection
-----------	------------------	------------

[ADD WI-FI PROTECTED SETUP \(WPS\) CLIENT](#)

## 4.7 Parental Control

### 4.7.1 Parental Control\_Managed Sites

Manage access to specific websites by network devices.

Select Enable to manage sites, or Disable to turn off.

+ADD: Add a new website or keyword.

Blocked Sites: Deny access to specific websites (URLs).

Blocked Keywords: Deny access to websites containing specific words.

The Gateway will block connections to websites on all untrusted computers, based on the specified rules.

If you don't want restrictions for a particular computer, select Yes under Trusted Computers.

**Parental Control > Managed Sites**

Manage access to specific websites by network devices. [more](#)

**Managed Sites:**

**Blocked Sites**

URL	When
-----	------

**Blocked Keywords**

Keyword	When
---------	------

**Trusted Computers**

	Computer Name	IP	Trusted
1	DESKTOP-RVE4C9U	10.0.0.47/NA	<input type="button" value="No"/> <input type="button" value="Yes"/>

## 4.7.2 Parental Control\_Managed Services

Manage access to specific services and applications by network devices.  
Select Enable to manage services and applications, or Disable to turn off.

+ADD: Add to block a new service or application.

The Gateway will block services and applications on all untrusted computers, based on the specified rules. If you don't want restrictions for a particular computer, select Yes under Trusted Computers.

**Parental Control > Managed Services**

Manage access to specific services and applications by network devices. [more](#)

**Managed Services:**

**Blocked Services**

Services	TCP/UDP	Starting Port	Ending Port	When
----------	---------	---------------	-------------	------

**Trusted Computers**

	Computer Name	IP	Trusted
1	DESKTOP-RVE4C9U	10.0.0.47/NA	<input checked="" type="button" value="No"/> <input type="button" value="Yes"/>

### 4.7.3 Parental Control\_Managed Devices

Manage access by specific devices on your network.

Select Enable to manage network devices, or Disable to turn off.

Access Type: If you don't want your devices to be restricted, select Allow All. Then select +ADD BLOCKED DEVICE to add only the device you want to restrict.

If you want your devices to be restricted, select Block All. Click +ADD ALLOWED DEVICE to add the device you don't want to restrict.

The screenshot shows a web interface for "Parental Control > Managed Devices". On the left is a navigation menu with items: Gateway, Connected Devices, Parental Control (selected), Managed Sites, Managed Services, Managed Devices, Reports, Advanced, and Troubleshooting. The main content area has a title "Parental Control > Managed Devices" and a subtitle "Manage access by specific devices on your network." with a "more" link. Below this is a "Managed Devices" section with two rows of controls: "Managed Devices:" with "Enable" and "Disable" buttons, and "Access Type:" with "Allow All" and "Block All" buttons. At the bottom is a "Blocked Devices" section with a "+ ADD BLOCKED DEVICE" button and a table header with columns "Computer Name", "MAC Address", and "When Blocked".

## 4.7.4 Parental Control\_Reports

Generate, download, and print reports based on your parental controls.

The screenshot shows a web interface for generating parental control reports. On the left is a navigation sidebar with the following items: Gateway, Connected Devices, Parental Control (highlighted), Managed Sites, Managed Services, Managed Devices, Reports, Advanced, and Troubleshooting. The main content area is titled "Parental Control > Reports" and contains a sub-header "Generate, download, and print reports based on your parental controls." Below this is a "Report Filters" section with a blue header. It includes a "Report Type" dropdown menu set to "All", a "Time Frame" dropdown menu set to "Today", and a "GENERATE REPORT" button. Underneath is an "All Reports" section with a blue header and the text "Reports for Today". At the bottom of this section are "PRINT" and "DOWNLOAD" buttons.

## 4.8 Advanced

Manage external access to specific ports on your network.

### 4.8.1 Advanced\_Port Forwarding

Port forwarding permits communications from external hosts by forwarding them to a particular port.

Select Enable to manage external access to specific ports on your network.

Click +ADD SERVICE to add new port forwarding rules.

Port forwarding settings can affect the Gateway's performance.

**Advanced > Port Forwarding**

Manage external access to specific ports on your network. [more](#)

**Port Forwarding:**  Enable  Disable

**Port Forwarding** [+ ADD SERVICE](#)

Service Name	Type	Start Port	End Port	Server IPv4	Server IPv6	Active
--------------	------	------------	----------	-------------	-------------	--------

## 4.8.2 Advanced\_Port Triggering

Manage external access to specific ports on your network.

Port triggering monitors outbound traffic on your network. When traffic is detected on a particular outbound port, the Gateway remembers that computer's IP address, triggers the inbound port to accept the incoming traffic, and directs the communications to the same computer.

Select Enable to manage external access to specific ports on your network.

Click +ADD PORT TRIGGER to add new port triggering rules.

Port triggering settings can affect the Gateway's performance.

The screenshot shows the 'Advanced > Port Triggering' settings page. On the left is a navigation menu with categories: Gateway, Connected Devices, Parental Control, Advanced (selected), Port Forwarding, Port Triggering (highlighted), Remote Management, DMZ, Dynamic DNS, Device Discovery, and Troubleshooting. The main content area has a title 'Advanced > Port Triggering' and a subtitle 'Manage external access to specific ports on your network.' with a 'more' link. Below this, there is a 'Port Triggering:' label followed by two buttons: 'Enable' (highlighted in green) and 'Disable'. At the bottom, there is a blue header for a table titled 'Port Triggering' with a '+ ADD PORT TRIGGER' button. The table has five columns: 'Service Name', 'Service Type', 'Trigger Port(s)', 'Target port(s)', and 'Active'. The table is currently empty.

### 4.8.3 Advanced\_Remote Management

Remote Management allows the gateway to be remotely accessed by a customer account representative to perform troubleshooting or maintenance.

Remote Management can be used via HTTPS.

Enable the HTTPS option, then you can access your device from HTTP. For example, if the WAN IP address is 11.22.11.22, then you would use https://11.22.11.22

Select whether you would like to have Remote Management open to all Internet IP Addresses, an Internet IP Address range, or a single Internet IP Address.

The screenshot shows a web interface for configuring Remote Management. On the left is a navigation menu with categories: Gateway, Connected Devices, Parental Control, Advanced (selected), and Troubleshooting. The 'Advanced' section includes: Port Forwarding, Port Triggering, Remote Management (highlighted), DMZ, Dynamic DNS, and Device Discovery. The main content area is titled 'Advanced > Remote Management'. It contains a descriptive text box with a 'more' link. Below is a 'Remote Management' section with an 'HTTPS:' toggle set to 'Enable'. Underneath are fields for 'Remote Management Address (IPv4): 0.0.0.0' and 'Remote Management Address (IPv6):'. The 'Remote Access Allowed From' section has three radio button options: 'Single Computer' (with IPv4 and IPv6 address fields), 'Range Of IPs' (with Start and End IPv4 and IPv6 address fields), and 'Any Computer' (selected). A note below states: 'Note: This option will allow any computer on the Internet to access your network and may cause a security risk.' A 'SAVE' button is at the bottom.

## 4.8.4 Advanced\_DMZ

Configure DMZ to allow a single computer on your LAN to open all of its ports.

The screenshot shows the 'Advanced > DMZ' configuration page. On the left is a navigation menu with 'Advanced' selected. The main content area has a title 'Advanced > DMZ' and a subtitle 'Configure DMZ to allow a single computer on your LAN to open all of its ports.' Below this is a blue header 'DMZ'. The 'DMZ:' section has two buttons: 'Enable' (highlighted) and 'Disable'. The 'DMZ v4 Host:' section has four input boxes, each containing '0'. The 'DMZ v6 Host:' section has eight input boxes, each containing '0'. A 'SAVE' button is at the bottom.

## 4.8.5 Advanced\_Dynamic DNS

Configure the Gateway's router functionality as a Dynamic DNS client.

Service Provider: Dynamic DNS Service Provider Domain name

User Name: Name registered with the service provider

Password: Password registered with the service provider

Host Name: Host Name registered with the service provider

The screenshot shows the 'Advanced > Dynamic DNS' configuration page. On the left is a navigation menu with 'Advanced' selected. The main content area has a title 'Advanced > Dynamic DNS' and a subtitle 'Configure the Gateway's router functionality as a Dynamic DNS client.' Below this is a blue header 'Dynamic DNS' with a '+ ADD DDNS' button. The 'Dynamic DNS:' section has two buttons: 'Enable' (highlighted) and 'Disable'. Below is a table with columns: 'Service Provider', 'User Name', 'Password', and 'HostName(s)'. The table is currently empty.

## 4.8.6 Advanced\_Device Discovery

Manage UPnP network.

The UPnP enabled Gateway discovers all UPnP enabled client devices, such as network printers and laptops. Using UPnP, the ports are opened automatically for the appropriate services and applications. The UPnP devices will be auto configured in the network.

**Advertisement Period:** The Advertisement Period is how often the gateway will advertise (broadcast) its UPnP information.

**Time to Live:** Measured in hops for each UPnP packet sent. A hop is the number of steps an UPnP advertisement is allowed to propagate before disappearing.

**Zero Config:** Discovery protocol which allows devices, such as printers and computers, to connect to a network automatically.

The screenshot shows a web interface for configuring UPnP settings. On the left is a navigation menu with categories: Gateway, Connected Devices, Parental Control, Advanced (selected), Port Forwarding, Port Triggering, Remote Management, DMZ, Dynamic DNS, Device Discovery, and Troubleshooting. The main content area is titled "Advanced > Device Discovery". It contains a "Manage UPnP network." link with a "more" link. Below is a "Device Discovery" section with the following settings:

- UPnP:  Enable  Disable
- Advertisement Period:  minutes
- Time To Live:  hops
- Zero Config:  Enable  Disable

A "SAVE" button is located at the bottom of the configuration area.

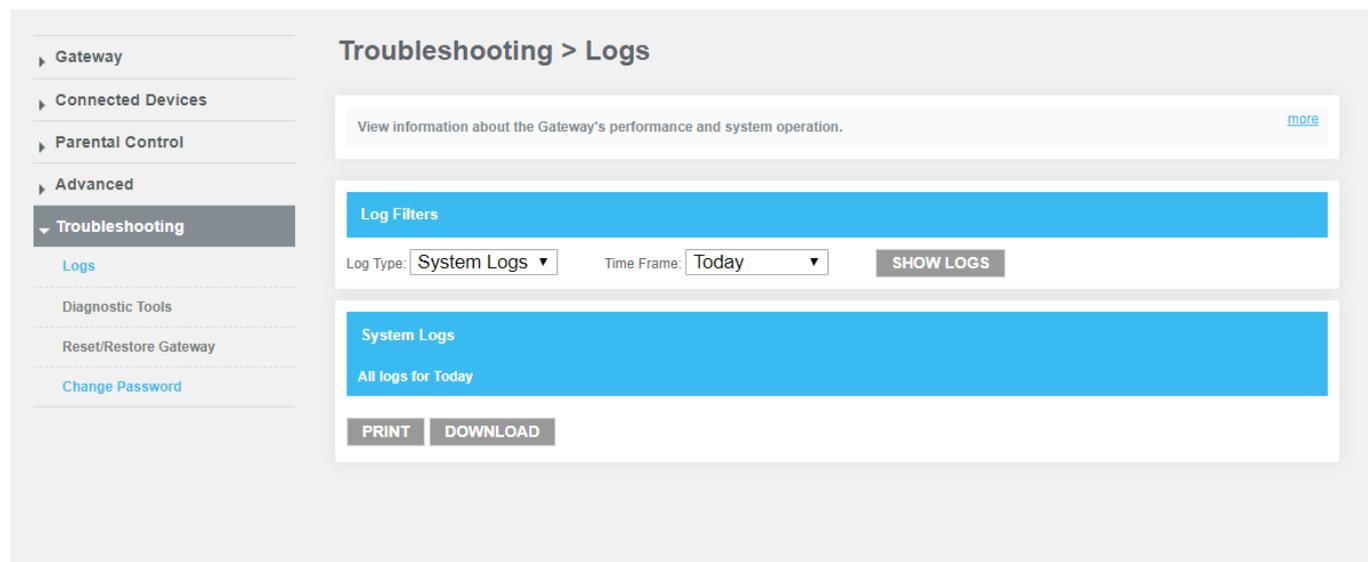
## 4.9 Troubleshooting

View information about the Gateway's performance and system operation.

### 4.9.1 Troubleshooting\_Logs

View information about the Gateway's performance and system operation.

Use the logs to troubleshoot issues and to identify potential security risks.



The screenshot displays the 'Troubleshooting > Logs' interface. On the left is a navigation menu with options: Gateway, Connected Devices, Parental Control, Advanced, Troubleshooting (selected), Logs, Diagnostic Tools, Reset/Restore Gateway, and Change Password. The main content area is titled 'Troubleshooting > Logs' and contains a summary box with the text 'View information about the Gateway's performance and system operation.' and a 'more' link. Below this is a 'Log Filters' section with 'Log Type' set to 'System Logs' and 'Time Frame' set to 'Today', accompanied by a 'SHOW LOGS' button. The main log area is titled 'System Logs' and shows 'All logs for Today', with 'PRINT' and 'DOWNLOAD' buttons at the bottom.

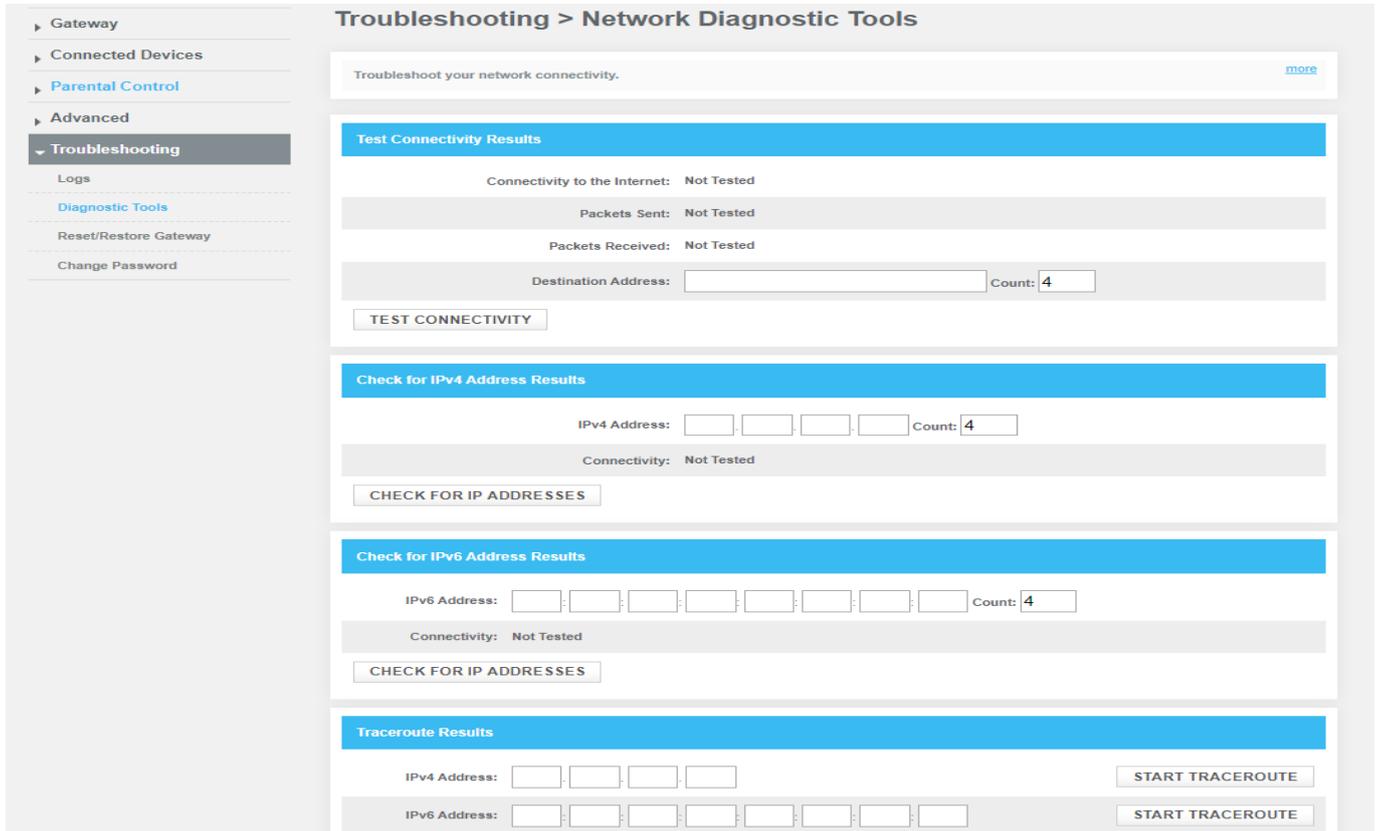
### 4.9.2 Troubleshooting\_Diagnostic Tools

Troubleshoot your network connectivity.

Test Connectivity Results: Checks your connectivity to the Internet.

Check IPv4 and IPv6 Address Results: Identifies accessibility to specific IP addresses.

Trace route Results: Displays the route of packets across an Internet Protocol (IP) network.

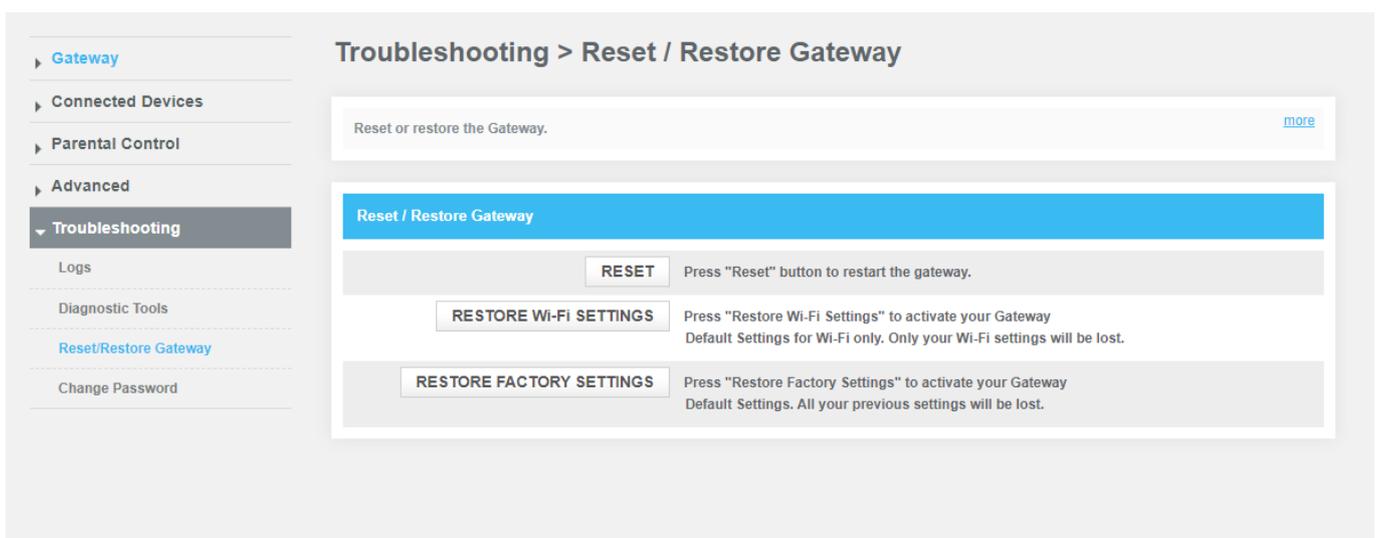


### 4.9.3 Troubleshooting\_Reset/Restore Gateway

Reset or restore the Gateway.

If you're having problems with the Gateway, click RESET to restart or RESTORE to the default factory settings.

CAUTION: RESTORE will erase all your settings (passwords, parental controls, firewall).



## 4.9.4 Troubleshooting\_Change Password

Periodically change your Admin Tool password to protect your network.

The screenshot shows a web interface for changing the Admin Tool password. On the left is a navigation menu with categories: Gateway, Connected Devices, Parental Control, Advanced, and Troubleshooting. Under Troubleshooting, there are links for Logs, Diagnostic Tools, Reset/Restore Gateway, and Change Password. The main content area is titled 'Troubleshooting > Change Password' and contains a warning message: 'Periodically change your Admin Tool password to protect your network.' Below this is a 'Password' section with three input fields: 'Current Password:', 'New Password:', and 'Re-enter New Password:'. There is also a checkbox for 'Show Typed Password:'. A note at the bottom states: 'Password Must be minimum 8 characters(Alphanumeric only). No spaces. Case sensitive.' At the bottom of the form are 'SAVE' and 'RESET' buttons.

**Troubleshooting > Change Password**

Periodically change your Admin Tool password to protect your network.

**Password**

Current Password:

New Password:

Re-enter New Password:

Show Typed Password:

Password Must be minimum 8 characters(Alphanumeric only). No spaces. Case sensitive.

**SAVE** **RESET**

# Appendix: Cable Modem Specification

**Table 1. RF Downstream Specification**

Parameter	Value
Frequency range	108-1002 / 258-1218 MHz switchable
Bonded Channels	DOCSIS 3.1: 2 (OFDM)
	DOCSIS 3.0: up to 32
Capture Bandwidth	1.2 GHz
Carrier Bandwidth	DOCSIS 3.1 : 192 MHz
	DOCSIS 3.0 : 6 MHz
	EuroDOCSIS 3.0 : 8 MHz
Modulation	DOCSIS 3.1 : 4096 QAM
	DOCSIS 3.0 : 1024 QAM
Data Rate	DOCSIS 3.1 : up to 5 Gbps
	DOCSIS 3.0 : up to 1.2 Gbps
	EuroDOCSIS 3.0 : 1.6 Gbps

**Table 2. RF Upstream Specification (DOCSIS)**

Parameter	Value
Frequency Range	5-85 / 5-204 MHz switchable
Bonded Channels	DOCSIS 3.1: 2 (OFDM)
	DOCSIS 3.0: up to 8
Modulation	4096 QAM (DOCSIS 3.1), 256 QAM, QPSK
Data Rate	DOCSIS 3.1 : up to 2 Gbps DOCSIS 3.0 : up to 200 Mbps

**Table 3. Electrical Specification**

Parameter	Measured Value	Notes
Input Voltage	12VDC/3.5A	
Power consumption	TBD	With AC adaptor

**Table 4. Physical Specification**

Parameter	Value
Size	205 mm (W) x 230mm(H) x 64.3 mm (L)
Weight	740 +/- 10g (device only)

**Table 5. Environmental Specification**

<b>Parameter</b>	<b>Value</b>
Operating Temperature	0 °C ~ +40 °C
Operating Relative Humidity	5% ~ 95% (Non-condensing)
Storage Temperature	-10 °C ~ +60 °C