Ubee EVW32C

Advanced Wireless Voice Gateway

Firmware Version: 2.2.xxxx

Subscriber User Manual

March 2017

www.ubeeinteractive.com
Polarisavenue 77
2132 JH Hoofddorp
The Netherlands
+31(0)203038371
Sales (email): eusales@ubeeinteractive.com
Support (email): eusupport@ubeeinteractive.com

Notices and Copyrights

Ubee Interactive continuously improves its products and reserves the right to make changes to the product described in this document without notice. Ubee Interactive does not assume any liability that may occur due to the use of the product described in this document.

All trademarks mentioned in this document are the property of their respective owners.

This device is Wifi Alliance Certified:

Wi-Fi PROTECTED SETUP

Contents

1 Introduction

Welcome to the Ubee Interactive family of data networking products. This guide is specific to the **EVW32C Advanced Wireless Voice Gateway** for cable subscribers and serves the following purposes:

- Provides instructions on how to install, connect, and operate the EVW32C.
- Provides directions for accessing the Web User Interface (UI) for configuration and management of the device.
- Defines all relevant device compliance standards and physical specifications.

Topics

See the following topics:

1.1 Understanding Safety and Regulatory Information

Use the following information to better understand safety and regulatory standards to install, maintain, and use the EVW32C Advanced Wireless Voice Gateway.

1.1.1 Understanding Safety

WARNING: The following information provides safety guidelines for anyone installing and maintaining the EVW32C. Read all safety instructions in this guide before attempting to unpack, install, operate, or connect power to this product. Follow all instruction labels on the device itself. Comply with the following safety guidelines for proper operation of the device.

Follow basic safety precautions to reduce the risk of fire, electrical shock, and injury. To prevent fire or shock hazard, do not expose the unit to rain and moisture or install this product near water. Never spill any form of liquid on or into this product. Do not use liquid cleaners or aerosol cleaners on or close to this product. Clean with a soft dry cloth.

Do not insert sharp objects into the product’s module openings or empty slots. Doing so can accidentally damage its parts and/or cause electric shock.

Electrostatic discharge (ESD) can permanently damage semiconductor devices. Always follow ESD-prevention guidelines for equipment handling and storage.

Use only the power adapter supplied with the device. Do not attach the power supply cable to building surfaces or floorings.

- Rest the power adapter freely without any obstacles. Do not place heavy items on top of the power cable. Do not abuse, step, or walk on the cable.
- Do not place heavy objects on top of the device. Do not place the device on an unstable stand or table; the device can fall and become damaged.
- Do not block the slots and openings in the module housing that provide ventilation to prevent overheating the device. Do not expose this device to direct sunlight. Do not place hot devices close to this device; it may degrade it or cause damage.
- Place the device on a cool surface. Failure to do so may result in overheating which can cause damage to the unit or to furniture.

1.1.2 Understanding Eco-Environmental Statements

The following eco-environmental statements apply to the EVW32C.

Packaging Collection and Recovery Requirements:

This product should not be disposed of with household waste. Contact your city authorities for information on how electrical appliances can be recycled. For more information regarding collection and recovery of packaging and packaging waste within specific jurisdictions, contact Ubee Interactive at www.ubeeinteractive.com.

1.1.3 Regulatory Conformity

Ubee Interactive Corporation warrants that the EVW32C Advanced Wireless Voice Gateway meets the requirements for compliance in relation to the following directives:

- 2002/95/EC (The RoHS Directive) restricting the use of hazardous substances in all Electrical and Electric Equipment.
- 2002/96/EC (The WEEE Directive) preventing/reducing Waste Electrical and Electronic Equipment (WEEE).
- 2006/95/EC (The Low Voltage Directive) regulating all health and safety risks of electrical equipment operating within certain voltage ranges.
- 2004/108/EC (The Electromagnetic Compatibility Directive) ensuring that (i) electromagnetic emissions do not disturb radio and telecommunication or other equipment and (ii) the immunity of the products/equipment supplied to interference.
- 1999/5/EC (The R&TTE Directive) ensuring that radio communications and telecommunications terminal equipment (R&TTE) is safe and does not disturb radio services or other equipment.
- 2009/125/EC (The Eco Design Directive) establishing a framework for the setting of eco-design requirements for energy-using products as well as any relevant regulation made thereunder including, if appropriate, but not limited to the Standby Regulation (EC) No 1275/2008 with regard to eco-design requirements for standby

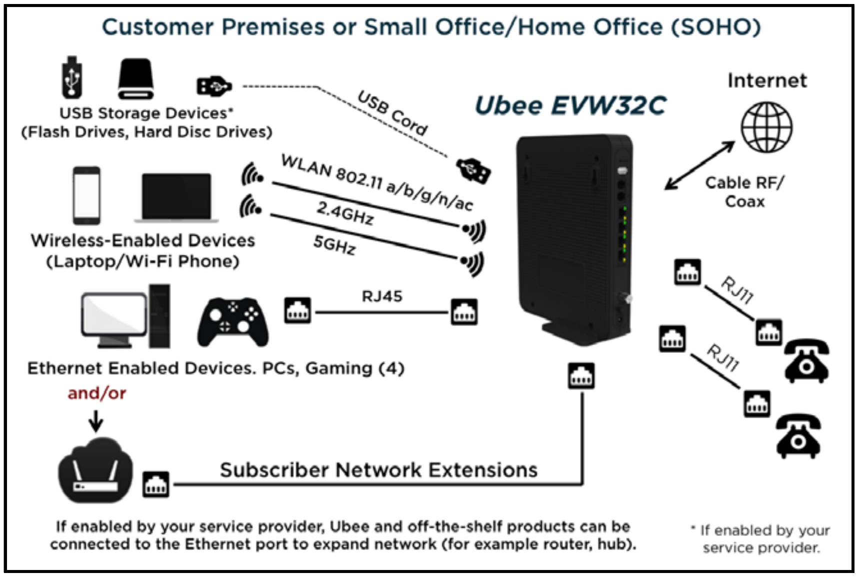
and off mode electric power consumption of electrical and electronic household and office equipment (The Standby Regulation) and regulation (278/2009) (The Power Supply Regulation).

The following standards apply:

- EN300328
- EN301893
- EN301489-1
- EN301489-17
- EN50385
- EN55022
- EN55024
- EN60950-1
- EN301893

1.2 Understanding Connections and Applications

The following diagram illustrates the general connection topology and applications of the EVW32C.


Customer Premises or Small Office/Home Office (SOHO)
USB Storage Devices*
(Flash Drives, Hard Disc Drives)
USB Cord
Ubee EVW32C
Internet
Cable RF/
Coax
WLAN 802.11 a/b/g/n/ac
2.4GHz
5GHz
Wireless-Enabled Devices
(Laptop/Wi-Fi Phone)
RJ45
RJ11
RJ11
Ethernet Enabled Devices. PCs, Gaming (4)
and/or
Subscriber Network Extensions
If enabled by your service provider, Ubee and off-the-shelf products can be connected to the Ethernet port to expand network (for example router, hub).
* If enabled by your service provider.

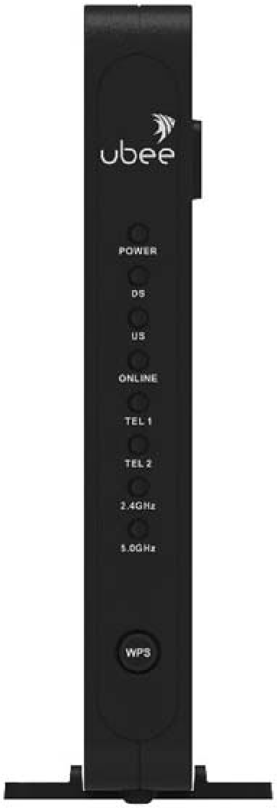
1.3 Checking Device Package Components

The package for the EVW32C contains the following items

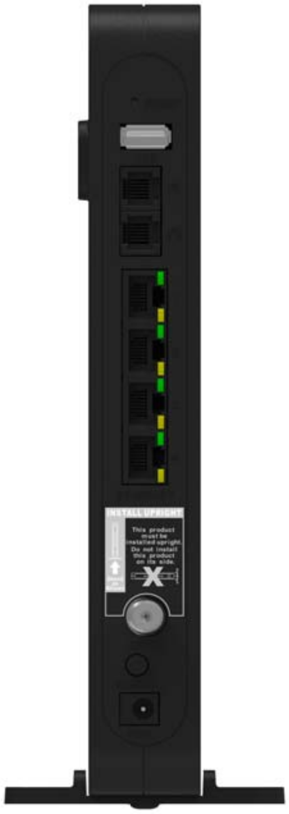
Item	Description
	1 - RJ45 Cable (Ethernet) Length ~ 6.0 ft RoHS & UL compliant *Sample image, actual appearance subject to change.*
	1 - RJ11 Cable (Telephony) *Sample image, actual appearance subject to change*
	1 - Power Adapter Input: 100-120VAC ~, 50-60Hz CE and UL Certified *Sample image, actual appearance subject to change.*

1.3.1 Understanding the Device Front and Rear Panels

The following images represent the device front and rear panels. Connection descriptions are provided in section 1.3.2., and LED descriptions are provided in section 1.3.3.



Front Panel


INSTALL UPRIGHT
This product must be installed upright. Do not install this product on its side.

Rear Panel

1.3.2 Understanding the Device Connections

The following table describes the connections on the device.

Item	Description
RESET	Restores the settings of the device including wireless and custom gateway settings. Use a pointed object to push down the reset button. To power cycle the device, hold for less than 5 seconds. To reset the device to factory defaults, hold for more than 5 seconds.
TEL1 / TEL2	Connects to standard telephones using an RJ11 cable. Telephone service must be enabled by your service provider.
ETHERNET 1-4	Connects to Ethernet devices such as computers, gaming consoles, and/or routers/hubs using an RJ45 cable. Each Ethernet port on the back panel of the device has 2 LEDs to indicate its status when an Ethernet device is connected.

Item	Description
CABLE RF	Connects to the cable outlet (with the cable provided by your service provider), or a cable splitter connected to the cable outlet.
ON / OFF	Switches the EVW32C on or off.
POWER	Connects the power adapter to the device. Use only the power adapter provided with the EVW32C.
USB PORT	USB 2.0 host port to support Linux applications for Ubee and 3rd party applications.
WPS	Located on front panel, this button is used for the WiFi Protected Setup (WPS) method to connect a PIN-protected WiFi device to the cable modem. Refer to Using the WPS Option on page 40 for more information.

1.3.3 Understanding LED Behavior

The following tables detail the behavior of the LEDs on both the front and rear panels of the EVW32C.

FRONT PANEL									
Position	**LED 1**	**LED 2**	**LED 3**	**LED 4**	**LED 5**	**LED 6**	**LED 7**	**LED 8**	**Button (Front Panel)**
Color	**Green**	**Green**	**Green**	**Green**	**Green**	**Green**	**Green**	**Green**	**Green**
Label	**POWER**	**DS**	**US**	**ONLINE**	**TEL 1**	**TEL 2**	**2.4GHZ**	**5.0GHz**	**WPS**
State:									
Power ON	**On**	**On**	**On**	**On**	**On**		Off	Off	Off
Self Test	N/A	N/A	N/A	N/A	N/A		N/A	N/A	N/A
Initialize Ethernet Switch	**On**	Blink	Blink	Blink	Off		Off	Off	Off
Initialize WLAN	**On**	Blink	Blink	Blink	Off		**On**	**On**	Off
Initialize Router	**On**	Blink	Blink	Blink	Off		**On**	**On**	Off
Downstream Search	**On**	Blink	Off	Off	Off		**On**	**On**	Off
Downstream Locked	**On**	**On**	Off	Off	Off		**On**	**On**	Off
Upstream Initial Ranging	**On**	**On**	Blink	Off	Off		**On**	**On**	Off

FRONT PANEL

Position	LED 1	LED 2	LED 3	LED 4	LED 5	LED 6	LED 7	LED 8	Button (Front Panel)
Registration	On	On	On	Flash	Off		On	On	Off
Registration OK **Network Access Enabled**	On	On	On	On	Off		On	On	Off
Registration OK **Network Access Disabled**	On	On	On	Off	Off		On	On	Off
Router Provisioning	On	On	On	Off	Off		On	On	Off
Attach device via WPS	On	On	On	On	Blink - VoIP registration On - VoIP registered		On	On	Off - WPS Stop Flash - WPS Start On - Attach Device
VoIP Registration	On	On	On	On	Blink		On/ strobe on link activity	On / strobe on link activity	Off
VoIP Registered	On	On	On	On	On		On/ strobe on link activity	On/ strobe on link activity	Off
VoIP Off-Hook	On	On	On	On	Blink		On / strobe on link activity	On/ strobe on link activity	Off
MTA is not provisioned	On	On	On	On	Off		On/ strobe on link activity	On / strobe on link activity	Off
TEL1 is provisioned but FXS2 is unused	On	On	On	On	On	Off	On/ strobe on link activity	On/ strobe on link activity	Off

REAR PANEL		
LED	**Color**	**Description**
ETHERNET 1-4	**Green/ Orange**	**On Green** – An Ethernet device is connected to the device at 1000 Mbps speeds (Gigabit Ethernet). **On Orange** – An Ethernet device is connected to the device at 10/100 Mbps speeds. **Flashes (in Green or Orange)** – When data is being passed between the cable modem and the connected device. The Ethernet ports are used to connect Ethernet devices such as computers, gaming consoles, and/or routers/hubs to the EVW32C using RJ-45 cables. Each Ethernet port on the back panel of the device has an LED to indicate its status when an Ethernet device is connected.

1.4 Understanding Specifications, Standards, and Firmware

The following list provides the features and specifications of the EVW32C.

Interfaces and Standards

- Cable: F-Connector, female
- LAN: 4 10/100/1000 Mbps RJ45 ports, auto-sensing MDI-X
- Telephony: 2 RJ-11 ports, PacketCable and EuroPacketCable 1.0/ 1.5/2.0 compatible, SIP RFC3261
- 1 USB 2.0 host port
- DOCSIS 3.0 and EuroDOCSIS 3.0 certified
- CE, EuP, RoHS, WEEE

Downstream*

- Frequency Range: 108MHz ~ 1002MHz, capture bandwidth: 1GHz
- Modulation: 64 / 256 QAM
- Channel Bandwidth: 8 MHz
- Maximum Data Rate per Channel (up to 24 channels): EuroDOCSIS = 41.71 Mbps (64 QAM), 55.62 Mbps (256 QAM)
- Total Max Bandwidth (24 Channels): EuroDOCSIS = 1029 Mbps
- Symbol Rate: 6.952 Msps (EuroDOCSIS)
- RF (cable) Input Power (one channel): -17 to +17dBmV
- Input Impedance: 75 Ω

Upstream*

- Frequency Range: 5MHz ~ 85MHz (EuroDOCSIS), 5MHz ~ 42MHz (DOCSIS), optional 5 to 65MHz upstream

- Modulation A-TDMA: QPSK, 8, 16, 32, 64QAM, S-CMDA: QPSK, 8, 16, 32, 64, 128QAM
- Data Rate: 0.32 to 30.72 Mbps per channel (8 channels)
- Symbol Rate: 160, 320, 640, 1280, 2560, 5120 Ksps
- RF (cable) Output Power (single channel): TDMA: +17dBmV to +61dBmV, S-CDMA: +17dBmV to +56dBmV
- RF (cable) Output Power per channel (2 channels bonded): TDMA: +17dBmV to +58dBmV, S-CDMA: +17dBmV to +53dBmV
- RF (cable) Output Power per channel (3 or 4 channels bonded): TDMA: +17dBmV to +55dBmV, S-CDMA: +17dBmV to +53dBmV
- RF (cable) Output Power per channel (5 or 8 channels bonded): TDMA: +17dBmV to +52dBmV, S-CDMA: +17dBmV to +53dBmV

*Actual speeds vary based on factors such as network configuration and service tier.

Security and Network

- Supports multiple SSIDs per radio, with dual band concurrent radios.
  - 5GHz band = 802.11a/b/g/n/ac compliant with link speeds up to 1300 Mbps, 3 Tx and 3 Rx antennas
  - 2.4GHz-band = 802.11a/b/g/n compliant with link speeds up to 300Mbps, 2 Tx and 2 Rx antennas
- 802.11ac Beam Forming focuses the signal toward each client, contracting the transmission so more data reaches targeted device
- DHCP client/server, static IP network assignment, RIPv1/ v2, Ethernet 10/100/1000 BaseT, full-duplex auto-negotiate functionality, IPv4 and IPv6 support
- NAT Firewall, MAC/IP/port filtering, parental/access control, stateful packet inspection (SPI), DoS attack protection, WPS (PIN and PBC)/ WPA/ WPA2/ WPA-PSK & 64/128-bit WEP encryption, WMM, 802.11e
- UPnP/DLNA
- VPN pass-through and end-point support (IPSec/L2TP/PPTP), TACACS or RADIUS authentication

Voice

- PacketCable and EuroPacketCable 1.5 (NCS) and 2.0 (IMS/SIP)
- Ring Voltage: 270 VAC, pk-pk (tip ring), Line Voltage Onhook: -48 Volts, Loop Current: 20mA / 41mA, Ring Capability: 2K ft., 5REN, Hook State: Signaling Loop Start
- Audio codecs: G.711. G.722, G.723, G.726, iLBC, BV16, G.728
- Caller ID basic and extended CLASS features
- DTMF Tone Detection, T.38 FAX Relay (G.711), Echo Cancellation (G.168) / Silence Suppression, Voice Active Detection and Comfort Noise Generation
- Modem support
- RTCP XR

Device Management

- Web-based user interface
- SNMP v1, v2c, v3

- Serial console (optional)
- Syslog
- WiFi radar
- Configuration backup and restore
- Spectrum analyzer
- TR-069 capable

Physical and Environmental

- Dimensions when positioned vertically: 182mm (D) x 237mm (H) x 80mm (W, including product stand)
- Weight: 800g
- Power: 12V / 2.5A
- Operating Temperature: 0°C ~ 40°C
- Storage Temperature: -10°C ~ 70°C
- Operating Humidity: 10~90% (non-condensing)

1.5 Understanding Default Values and Logins

The EVW32C is pre-configured with the default parameters for the Service Provider. Some regions may change default values using the cable modem or XML configuration file. Check with your provisioning team to determine the default values for your region.

Local Port Address: 192.168.100.1

Web Interface: http://192.168.100.1

Operation Mode: NAT Mode

Subnet Mask: 255.255.255.0

Wireless Defaults:

- Primary SSID (WiFi network name) = The last 6 characters of the cable modem MAC address. The SSIDs are the same for the 2.4GHz and 5GHz radio bands. The SSIDs are printed on the device label.
  - Example for a device with cable modem MAC address 68:14:01:24:A5:98 = **24A598**
  - If the subscriber changes the SSID, the device does not revert to this default SSID when the device is reset, except when a manual factory reset is performed through the Web UI.
  - The SSID can also be found on the WLAN Basic screen. Refer to Using the Basic Option on page 37.
- Encryption Method = Auto
- WPA Pre-shared Key = A unique key for each device, also called the network key, the wireless key, or the wireless password. The pre-shared key for the EVW32C is the 14 characters of the device serial number.

  Example Pre-Shared Key: EVW32C00000060

The password can be found on the WLAN Security screen. Refer to Using the Security Option on page 38. The pre-shared key can also be found on the device label. Refer to Understanding the Device Label on page 11.

- WPS PIN = The WPS (wireless protected setup) PIN is a randomly-generated number. Refer to Using the WPS Option on page 40.
- Device Name: UbeeAP

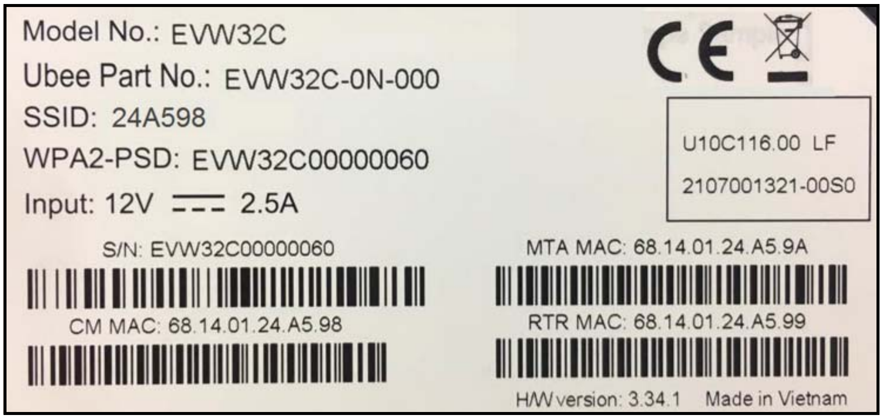
Login Default Value:

- User Web User Interface (UI) Login

  When you access the web user interface for the first time, you will be required to create a user name and password. Refer to Accessing the Web User Interface (UI) Locally on page 19 for detailed instructions.

1.6 Understanding the Device Label

The following is an example of the housing label for the EVW32C. Descriptions follow.



Model No.: EVW32C
Ubee Part No.: EVW32C-0N-000
SSID: 24A598
WPA2-PSD: EVW32C00000060
Input: 12V ⎓ 2.5A

U10C116.00 LF
2107001321-00S0

S/N: EVW32C00000060
MTA MAC: 68.14.01.24.A5.9A
CM MAC: 68.14.01.24.A5.98
RTR MAC: 68.14.01.24.A5.99
H/W version: 3.34.1 Made in Vietnam

Item	Description
Model No	Displays the device model number.
Ubee Part No	Displays the Ubee part number
SSID	Displays the SSID (service set identifier), or the wireless network name, for both the 2.4GHz and 5GHz wireless radio bands. The default is the last 6 characters of the cable modem MAC address. See Understanding Default Values and Logins on page 10 for more information.
WPA2-PSD	Displays the unique WPA pre-shared key for the device. It is also called the network key, the wireless key, or the wireless password. The default for both the 2.4 and 5GHz bands is the device serial number.
Input	Displays the power input.
S/N	Displays the serial number of the device.
CM MAC	Displays the cable modem MAC address of the device.

Item	Description
MTA MAC	Displays the MTA MAC address of the device.
RTR MAC	Displays the router MAC address of the device.
H/W version	Displays the internal version number that identifies the hardware design.
Made In	Displays the country in which the device was assembled.

2 Installing the EVW32C

Use the information in this chapter to set up and connect the EVW32C Advanced Wireless Voice Gateway, connect additional devices, and troubleshoot the installation.

Topics

See the following topics:

- Setting Up and Connecting the EVW32C on page 13
- Connecting Devices to the Network on page 15
- Troubleshooting the Installation on page 17

2.1 Setting Up and Connecting the EVW32C

Use the following instructions to set up and connect the EVW32C. When the device is set up and connected, refer to Accessing the Web User Interface (UI) Locally on page 19 to configure the device.

Important: Subscribers must contact their service provider to enable Internet access, wireless networking, and telephony (voice). In particular, voice service requires additional steps for the service provider including canceling the previous telephone provider service, porting the telephone number, and other tasks to minimize downtime during the transition.

Typically, the service provider initially configures and connects the device.

To set up the device:

1. Remove the contents from the device packaging.
2. Place the EVW32C in a central location, convenient for connecting to other devices, such as PCs or gaming consoles. Do not situate the wireless voice gateway on the floor.
   - Ensure the EVW32C is installed upright in a standing position so that the LED labels on the front panel of the device can be easily read. Affix the device stand to the bottom of the unit (included with the product) to ensure balance. Positioning your gateway horizontally or on it’s side affects the wireless performance dramatically, as the internal antennas won’t be able to propagate the wireless signal as designed.
   - Place the EVW32C and wireless clients in open areas far away from metal objects, transformers, heavy-duty motors, microwave ovens, refrigerators, fluorescent lights, and other manufacturing equipment. These items can impact wireless signals. A wireless signal can become weaker after it has passed through metal, concrete, brick, walls, or floors. For additional information on wireless signals, see Deploying and Troubleshooting the Wireless Network on page 42.

- Place the device in a location that has an operating temperature of 0˚C to 40˚C. Refer to Understanding Safety and Regulatory Information on page 1 for more safety information.

3. Power on your PC. The PC must have an Ethernet network adapter or Ethernet port and an Internet browser installed, such as Firefox or Internet Explorer. The following browsers are supported:
   - For Windows 2000, XP, Vista, Windows 8, Windows 7, Google Chrome, Firefox 1.07 and higher, Internet Explorer v7 and above.
   - For MAC OS X, 10.2, and higher: Firefox 1.07 and higher, Safari 1.x and higher.

4. Plug the power adapter included in the product package into a power outlet, and connect the other end to the PWR port on the back of the EVW32C.

5. Connect the Ethernet cable included in the product package to your computer's Ethernet port. Connect the other end to one of the ETHERNET ports on the back panel of the EVW32C.

6. Connect a coaxial cable (not included in the product packaging) from the CABLE port on the back of the device to the cable wall outlet, or to a cable splitter connected to the wall outlet.

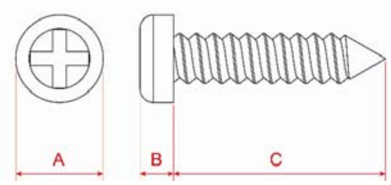
7. Connect an analog telephone (if you will be using the device for telephone service) to the TEL 1 or TEL 2 port on the back panel of the device. Use the supplied RJ-11 telephone cable for one of the telephones.

8. Validate the network connection using the device LEDs to confirm operations.
   - The 2.4GHz and 5GHz LEDs must be blinking or solidly lit.
   - The POWER, DS, US, and ONLINE LEDs are solidly lit.

   Refer to Understanding LED Behavior on page 6 for more information.

2.1.1 Wall Mount Installation

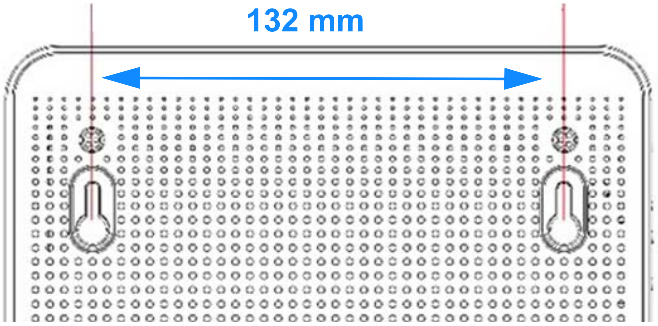
You can mount the EVW32C on a wall using the 2 mounting brackets on the side of the device. Two round or pan head screws are recommended. See the figure below.



Label	Size in Millimeters (mm)
A	7.2 +/- 0.5
B	2.6 +/- 0.15
C	19.0 +/- 1.2

To mount the EVW32C on a wall:

1. Install the two screws horizontally on a wall 132mm apart. See the figure below.



The screws should protrude from the wall so that you can fit the device between the head of the screw and the wall. If you install the screws in drywall, use hollow wall anchors to ensure the unit does not pull away from the wall due to prolonged strain from the cable and power connectors.

2. Mount the device on the wall.

2.2 Connecting Devices to the Network

Use the instructions below to connect network devices and validate device functionality.

See the following:

- Connecting an Ethernet Device on page 15
- Connecting a Wireless Device on page 16
- Connecting a Telephone Line on page 17

2.2.1 Connecting an Ethernet Device

You can connect up to three additional Ethernet devices to the EVW32C.

To connect another Ethernet device to the network:

1. Connect an Ethernet cable from the Ethernet device (for example, a PC or gaming console) to an open ETHERNET port on the back of the EVW32C.
2. Use the device LEDs to confirm operations. Refer to Understanding LED Behavior on page 6 for more information.
3. Open a Web browser and go to any Web site to validate network/Internet connectivity (for example, http://www.wikipedia.org).
4. If the connected device is a gaming console, perform any online task supported by the console (for example, log into the gaming server, play an online game, download content).

NOTE: Refer to Troubleshooting the Installation on page 17 for troubleshooting information.

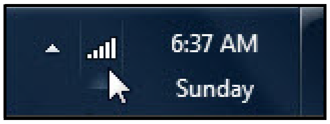
2.2.2 Connecting a Wireless Device

Use the following steps to connect a wireless device to the EVW32C (for example, a laptop computer).

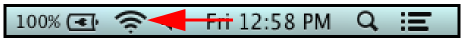
Default values are shown in the steps below.

To connect a wireless device to the EVW32C:

1. Access the wireless networking feature on your wireless device.
   - Windows Users: Double-click the Wireless Network Connection icon in the system tray (lower-right side of the Windows desktop). Click **View Wireless Networks**.



   - Mac Users: Click on the wireless icon on the right side of the top menu bar. All available wireless networks will appear in the drop-down menu.



2. The EVW32C is shipped with a default SSID. The SSID is the name of the wireless network broadcast from the device so that wireless clients can connect to it.
   - Double-click your **SSID** in the wireless networks window.
   - The SSID (WiFi network name) = The last 6 characters of the cable modem MAC address. The SSID is printed on the device label.
     - ❖ Example for a device with cable modem MAC address 68:14:01:24:A5:98:

       24A598.
     - ❖ Notes: If the subscriber changes the SSID, the device does not revert to this default SSID when the device is reset, except when a manual factory reset is performed through the Web UI.
   - When prompted, enter the network key, also called the WPA pre-shared key. This is a unique key for each device. The pre-shared key for the EVW32C is the same for both the 2.4GHz and 5GHz bands. The default password is the 14 characters of the device serial number. For example: **EVW32C00000060**. It can be found on the WLAN Security screen. Refer to Using the Security Option on page 38. The pre-shared key can also be found on the device label. Refer to Understanding the Device Label on page 11.
   - If using WPS, enter the WPS personal identification number (PIN). The WPS PIN is a randomly-generated number. Refer to Using the WPS Option on page 40
   - **AES** is the default encryption method.
3. Confirm connectivity by opening a Web browser and going to any Web site

(for example, http://www.wikipedia.org) or access the Web interface for the EVW32C.

NOTE: The Web interface allows you to customize the configurations and capabilities for the device. For a full explanation of all Web interface functions, refer to Using the Web User Interface on page 19.

If you have wireless issues or questions, refer to Deploying and Troubleshooting the Wireless Network on page 42.

2.2.3 Connecting a Telephone Line

You can connect up to two telephone lines to the EVW32C to use the telephone (voice) features.

Voice service must be enabled by the service provider. Voice service requires additional steps for the service provider including canceling the previous telephone provider service, porting the telephone number, and other tasks to minimize downtime during the transition.

To connect a telephone line:

1. Connect an analog telephone to the TEL 1 or TEL 2 jack on the back panel of the EVW32C using the supplied RJ-11 telephone cable.
2. Pick up the telephone line and listen for a dial tone.
3. Make a phone call and/or have someone call you to verify a successful connection.

2.3 Troubleshooting the Installation

Use the following tips to troubleshoot the installation.

❑ **None of the LEDs are on when I power on the EVW32C.**

- ♦ Verify the power outlet is energized and the power adapter is connected to the power outlet.
- ♦ Check the connection between the power adapter and the EVW32C. Power off the device and wait for 5 seconds and power it on again. If the problem still exists, there may be a hardware problem.

❑ **The ETHERNET LEDs on the back of the modem are not lit where Ethernet cables are connected.**

- ♦ Restart the computer so that it can re-establish a connection with the EVW32C.
- ♦ Check for a resource conflict (Windows users only):
  1. Right-click **My Computer** on your desktop and choose **Properties**.
  2. Choose the **Device Manager** tab and look for a yellow exclamation point or red **X** over the network interface card (NIC) in the Network Adapters field. If you see either one, you may have an interrupt request (IRQ) conflict. Refer to the manufacturer's documentation or ask your service provider for further assistance.
- ♦ Verify that TCP/IP is the default protocol for your network interface card.

- ♦ Power cycle the EVW32C by removing the power adapter from the electrical outlet and plugging it back in. Wait for the gateway to re-establish communications with your cable service provider.

❑ **Check General Connectivity Issues:**

- ♦ If your PC is connected to another hub or gateway, connect the PC directly into an Ethernet port on the EVW32C.
- ♦ If you are using a cable splitter, remove the splitter and connect the gateway directly to the cable wall outlet. Wait for it to re-establish communications with the cable service provider.
- ♦ Try a different cable. The Ethernet cable may be damaged.

3 Using the Web User Interface

The Web user interface (UI) for the EVW32C allows you to view and configure settings for the device. You can validate the installation by accessing the Web UI of the device.

Topics

See the following topics:

- Accessing the Web User Interface (UI) Locally on page 19
- Logging Out of the Web User Interface on page 21

3.1 Accessing the Web User Interface (UI) Locally

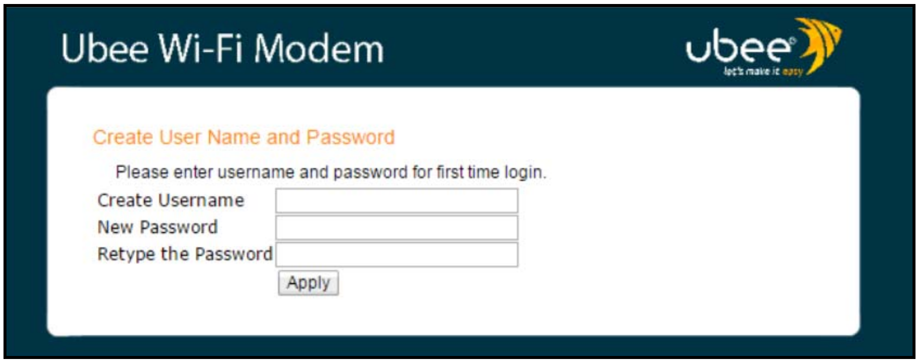
Access the Web UI for the EVW32C from a Web browser, such as Google Chrome on a Windows computer, or Safari on a Mac.

To access the Web user interface:

1. Launch an Internet browser, such as Google Chrome, from your computer.
2. Enter the following IP address in the address bar of the browser window and press the Enter key.

   `http://192.168.100.1`

3. When you access the web user interface for the first time, you will be required to create a user name and password.



Ubee Wi-Fi Modem

Create User Name and Password

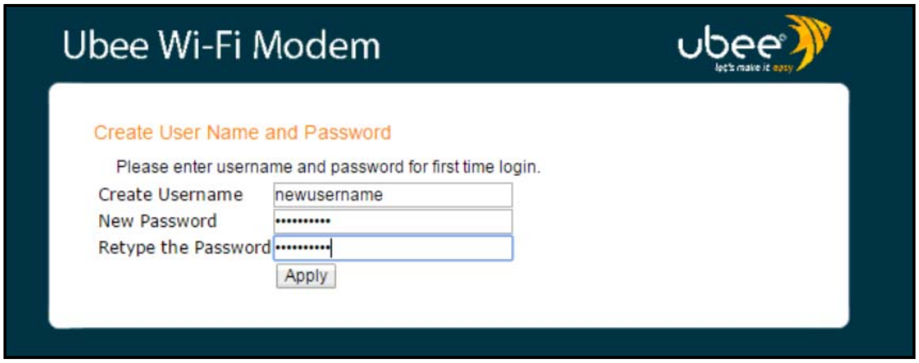
Please enter username and password for first time login.

Create Username

New Password

Retype the Password

4. Enter a Username and Password, then confirm the password by entering it again. Click the **Apply** button.



Ubee Wi-Fi Modem

Create User Name and Password

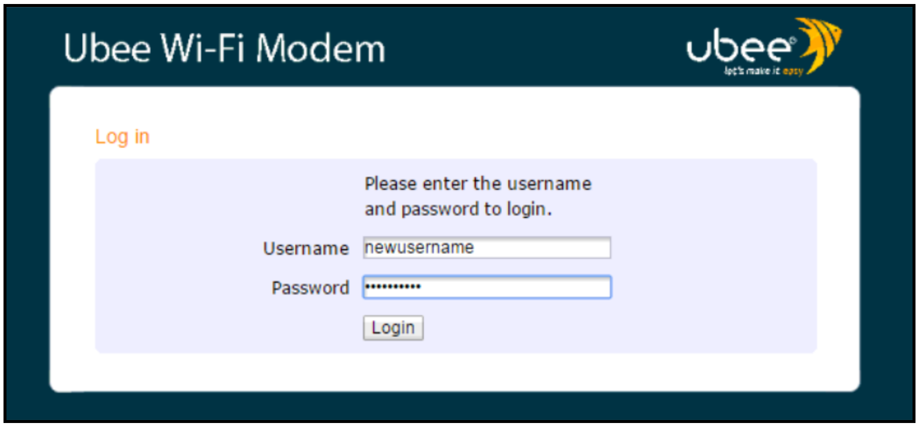
Please enter username and password for first time login.

Create Username: newusername

New Password: ••••••••••

Retype the Password: ••••••••••

5. After clicking **Apply**, the standard login screen appears. Enter the Username and Password you created in the previous step, then click **Login**.



Ubee Wi-Fi Modem

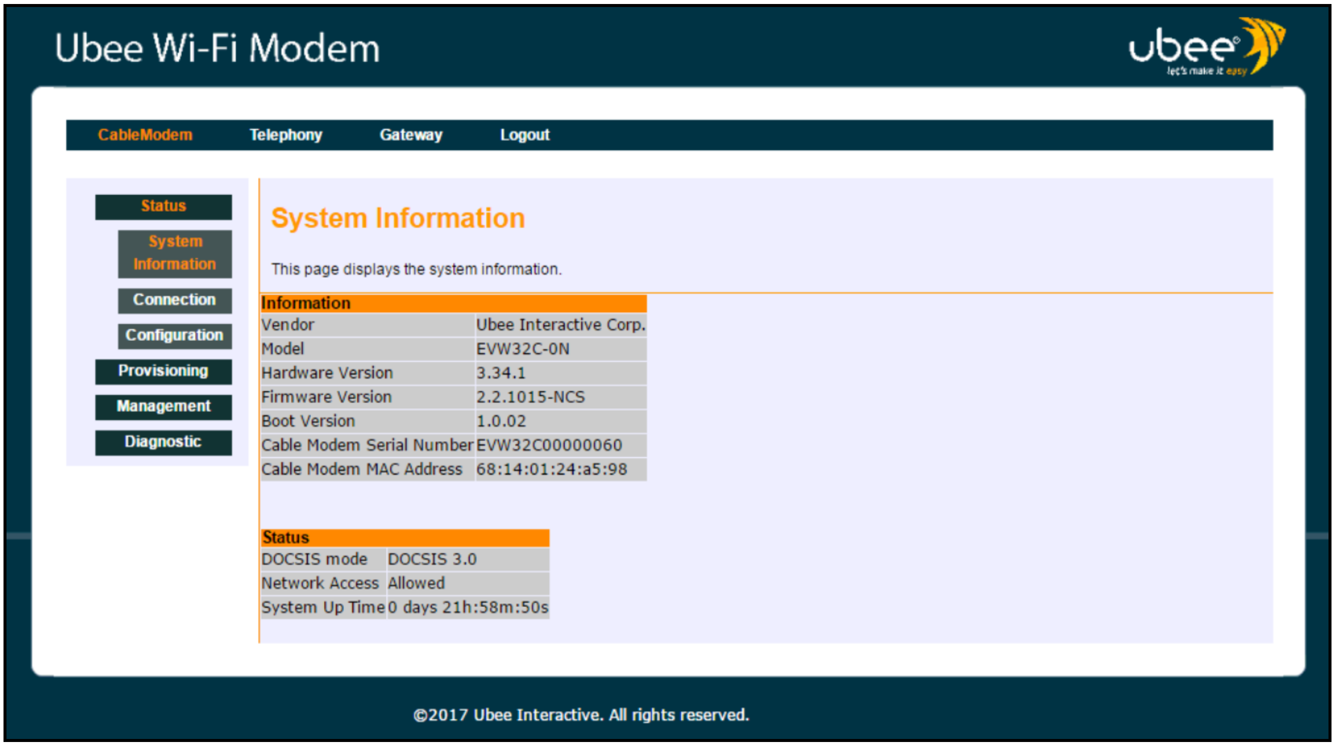
Log in

Please enter the username and password to login.

Username: newusername

Password: ••••••••••

The System Information screen (below) is displayed and provides basic information about the EVW32C. Refer to Using the System Information Option on page 22 for screen field descriptions.



System Information

This page displays the system information.

Information	
Vendor	Ubee Interactive Corp.
Model	EVW32C-0N
Hardware Version	3.34.1
Firmware Version	2.2.1015-NCS
Boot Version	1.0.02
Cable Modem Serial Number	EVW32C00000060
Cable Modem MAC Address	68:14:01:24:a5:98

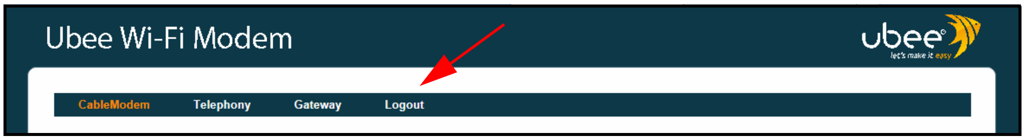
Status	
DOCSIS mode	DOCSIS 3.0
Network Access	Allowed
System Up Time	0 days 21h:58m:50s

©2017 Ubee Interactive. All rights reserved.

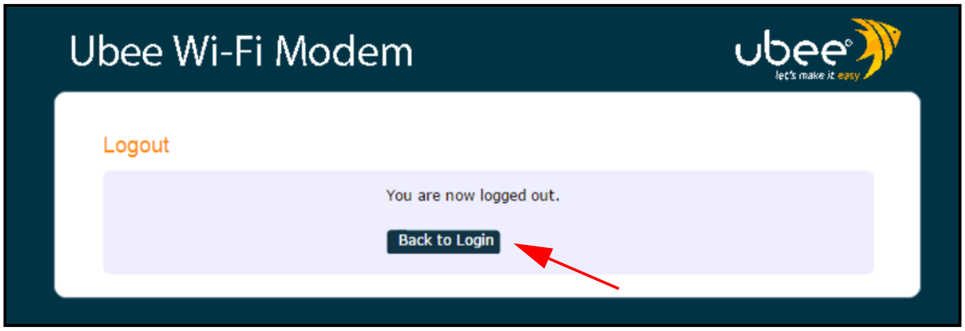
After clicking **Login**, the System Information screen (below) is displayed and provides basic information about the EVW32C. Refer to Using the System Information Option on page 22 for screen field descriptions.

3.2 Logging Out of the Web User Interface

To log out of the Web User Interface, click Logout on the top right of the menu bar.



The following screen appears and confirms you are logged out of the device and gives you the option to return to the login page.



You are now logged out.

4 Understanding the Cable Modem Menu

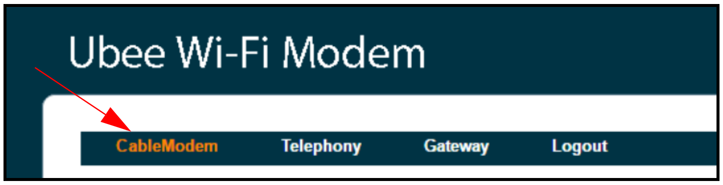
The **Cable Modem** menu of the Web user interface allows you to access information about the EVW32C, such as software version, and connection (downstream and upstream) status. It also allows you to change the username and password, and view cable modem provisioning information.

Topics

See the following topics:

To access cable modem options:

1. Access the Web user interface. Refer to Accessing the Web User Interface (UI) Locally on page 19.
2. Click **Cable Modem** from the main menu.



4.1 Using the Status Option

The **Status** option displays the device’s internal software and hardware configuration, and connection status (downstream and upstream). It also allows you to set the initial scan frequency, reboot the device or restore the device to factory default values.

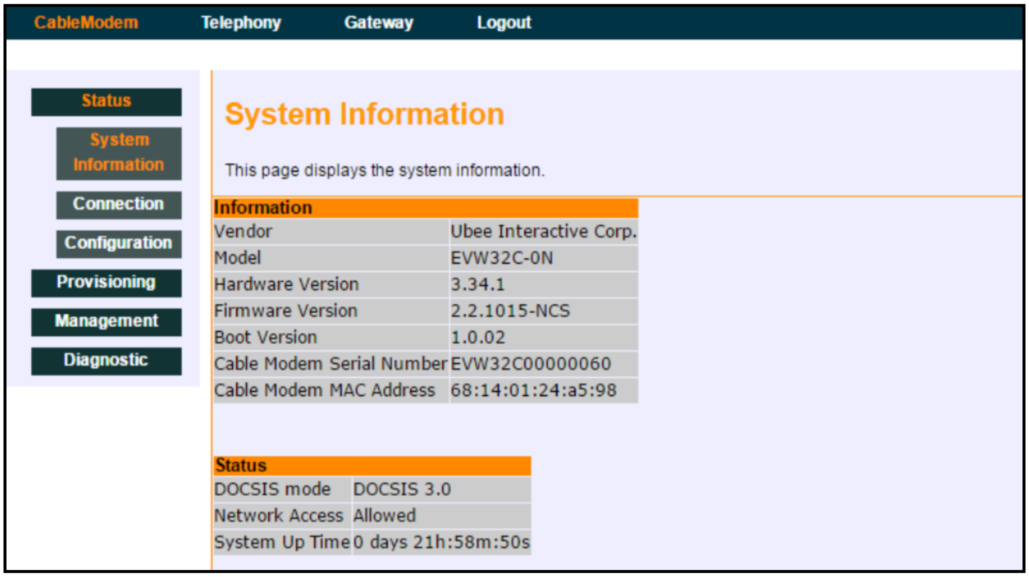
To view status information:

1. Click **Cable Modem** from the main menu.
2. Select **Status** from the left side menu.
3. The following sub-menu items are available for selection:
   - ♦ System Information

- ♦ Connection
- ♦ Configuration

4.1.1 Using the System Information Option

The System Information screen displays the EVW32C's internal software and hardware configuration. Field descriptions are listed below the screen example.



System Information

This page displays the system information.

Information	
Vendor	Ubee Interactive Corp.
Model	EVW32C-0N
Hardware Version	3.34.1
Firmware Version	2.2.1015-NCS
Boot Version	1.0.02
Cable Modem Serial Number	EVW32C00000060
Cable Modem MAC Address	68:14:01:24:a5:98

Status	
DOCSIS mode	DOCSIS 3.0
Network Access	Allowed
System Up Time	0 days 21h:58m:50s

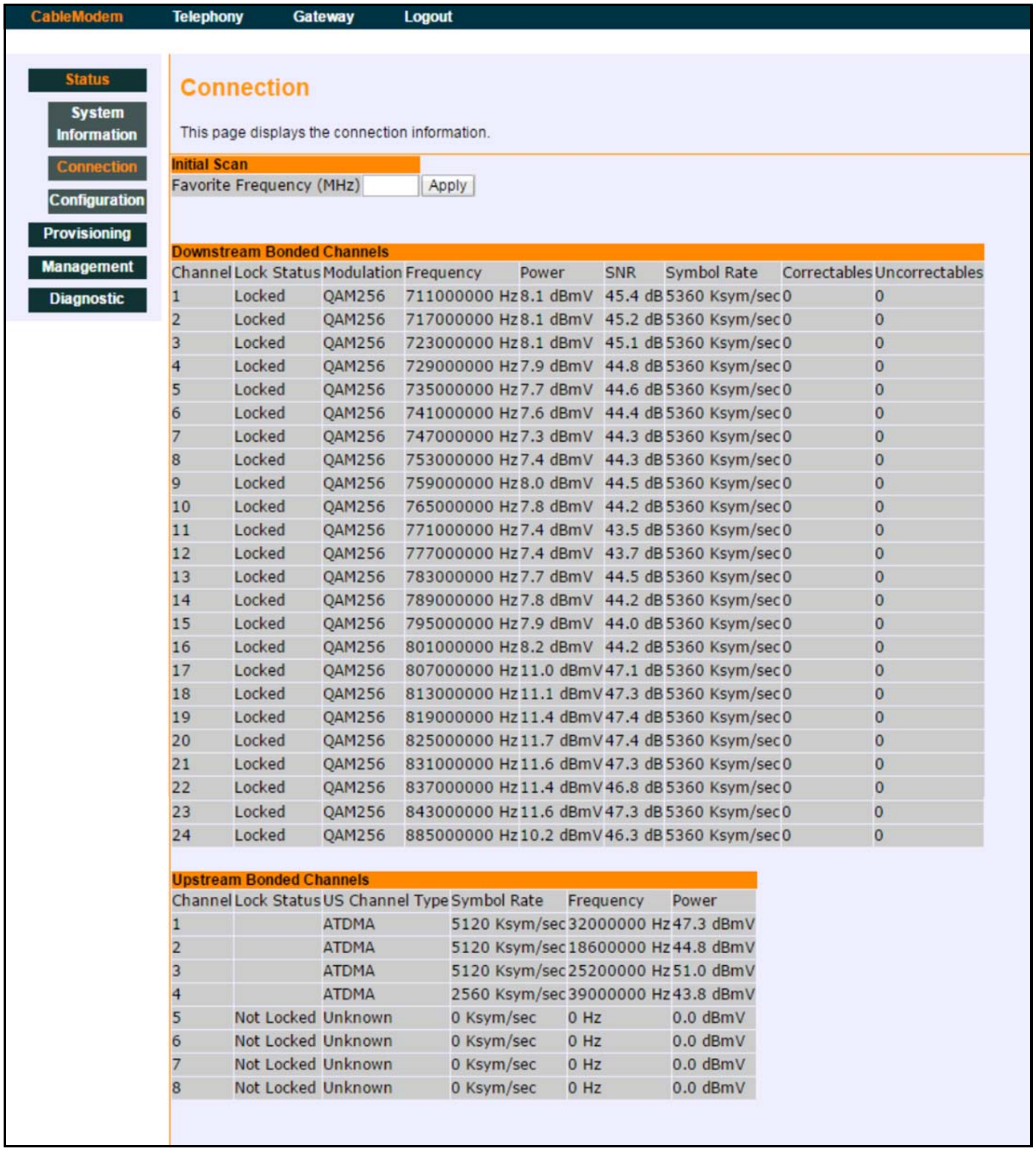
Label	Description
Information	
Vendor	Displays the device manufacturer (Ubee Interactive Corp.)
Model	Displays the device model number.
Hardware Version	Displays the internal version number that identifies the hardware design.
Firmware Version	Displays the firmware version of the device.
Boot Version	Displays the bootloader version.
Cable Modem Serial Number	Displays the unique manufacturer serial number of the device.
Cable Modem MAC Address	Displays the unique media access control (MAC) hardware address of the cable modem.
Status	
DOCSIS Mode	Displays the DOCSIS version of the device.
Network Access	Displays whether network access is allowed. When allowed, the user is allowed to access the network.
System Up Time	Displays how long the device has been connected.

4.1.2 Using the Connection Option

The **Connection** screen allows the user to set the favorite initial scan frequency, and displays information about connection status and downstream/upstream channel bonding statistics.

- **Downstream** displays detailed information on the network traffic from the service provider **to** the local computer (downstream channels).
- **Upstream** displays detailed information on the network traffic **from** the local computer to the remote destination (upstream channels).

Field descriptions are listed below the screen example.



Connection

This page displays the connection information.

Initial Scan

Favorite Frequency (MHz)

Downstream Bonded Channels

Channel	Lock Status	Modulation	Frequency	Power	SNR	Symbol Rate	Correctables	Uncorrectables
1	Locked	QAM256	711000000 Hz	8.1 dBmV	45.4 dB	5360 Ksym/sec	0	0
2	Locked	QAM256	717000000 Hz	8.1 dBmV	45.2 dB	5360 Ksym/sec	0	0
3	Locked	QAM256	723000000 Hz	8.1 dBmV	45.1 dB	5360 Ksym/sec	0	0
4	Locked	QAM256	729000000 Hz	7.9 dBmV	44.8 dB	5360 Ksym/sec	0	0
5	Locked	QAM256	735000000 Hz	7.7 dBmV	44.6 dB	5360 Ksym/sec	0	0
6	Locked	QAM256	741000000 Hz	7.6 dBmV	44.4 dB	5360 Ksym/sec	0	0
7	Locked	QAM256	747000000 Hz	7.3 dBmV	44.3 dB	5360 Ksym/sec	0	0
8	Locked	QAM256	753000000 Hz	7.4 dBmV	44.3 dB	5360 Ksym/sec	0	0
9	Locked	QAM256	759000000 Hz	8.0 dBmV	44.5 dB	5360 Ksym/sec	0	0
10	Locked	QAM256	765000000 Hz	7.8 dBmV	44.2 dB	5360 Ksym/sec	0	0
11	Locked	QAM256	771000000 Hz	7.4 dBmV	43.5 dB	5360 Ksym/sec	0	0
12	Locked	QAM256	777000000 Hz	7.4 dBmV	43.7 dB	5360 Ksym/sec	0	0
13	Locked	QAM256	783000000 Hz	7.7 dBmV	44.5 dB	5360 Ksym/sec	0	0
14	Locked	QAM256	789000000 Hz	7.8 dBmV	44.2 dB	5360 Ksym/sec	0	0
15	Locked	QAM256	795000000 Hz	7.9 dBmV	44.0 dB	5360 Ksym/sec	0	0
16	Locked	QAM256	801000000 Hz	8.2 dBmV	44.2 dB	5360 Ksym/sec	0	0
17	Locked	QAM256	807000000 Hz	11.0 dBmV	47.1 dB	5360 Ksym/sec	0	0
18	Locked	QAM256	813000000 Hz	11.1 dBmV	47.3 dB	5360 Ksym/sec	0	0
19	Locked	QAM256	819000000 Hz	11.4 dBmV	47.4 dB	5360 Ksym/sec	0	0
20	Locked	QAM256	825000000 Hz	11.7 dBmV	47.4 dB	5360 Ksym/sec	0	0
21	Locked	QAM256	831000000 Hz	11.6 dBmV	47.3 dB	5360 Ksym/sec	0	0
22	Locked	QAM256	837000000 Hz	11.4 dBmV	46.8 dB	5360 Ksym/sec	0	0
23	Locked	QAM256	843000000 Hz	11.6 dBmV	47.3 dB	5360 Ksym/sec	0	0
24	Locked	QAM256	885000000 Hz	10.2 dBmV	46.3 dB	5360 Ksym/sec	0	0

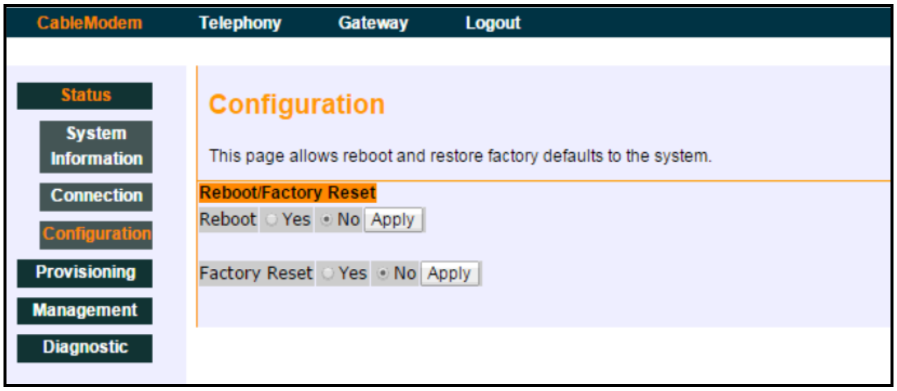
Upstream Bonded Channels

Channel	Lock Status	US Channel Type	Symbol Rate	Frequency	Power
1		ATDMA	5120 Ksym/sec	32000000 Hz	47.3 dBmV
2		ATDMA	5120 Ksym/sec	18600000 Hz	44.8 dBmV
3		ATDMA	5120 Ksym/sec	25200000 Hz	51.0 dBmV
4		ATDMA	2560 Ksym/sec	39000000 Hz	43.8 dBmV
5	Not Locked	Unknown	0 Ksym/sec	0 Hz	0.0 dBmV
6	Not Locked	Unknown	0 Ksym/sec	0 Hz	0.0 dBmV
7	Not Locked	Unknown	0 Ksym/sec	0 Hz	0.0 dBmV
8	Not Locked	Unknown	0 Ksym/sec	0 Hz	0.0 dBmV

Label	Description
Initial Scan	
Favorite Frequency (MHz)	Allows the user to enter a favorite frequency (in MHz) for the initial scan
Apply	Saves changes to the Favorite Frequency.
Downstream Bonded Channels	
Channel	Numbers the downstream channels.
Lock Status	Displays if the device is locked successfully to a downstream channel.
Modulation	Displays the modulation method required for the downstream channel to lock on to by the device. This method is determined by the service provider.
Frequency	Displays the downstream channel frequency on which the device is locked.
Power	Displays the receiver power level in decibel millivolts (dBmV) after ranging process.
SNR	Displays the signal-to-noise ratio (SNR) in decibels (dB), the desired signal level to the background noise level.
Symbol Rate	Displays the symbol rate in 1000 symbols per second.
Correctables	Displays the quantity of codewords which are correctable.
Uncorrectables	Displays the quantity of codewords which are uncorrectable.
Upstream Bonded Channels	
Channel	Numbers the upstream channels.
Lock Status	Displays if the EVW32C succeeded in locking to an upstream channel.
US Channel Type	Displays the channel type.
Symbol Rate	Displays the symbol rate in 1000 symbols per second.
Frequency	Displays the current upstream frequency in hertz.
Power	Displays the current upstream transmit power in decibel millivolts (dBmV).

4.1.3 Using the Configuration Option

The **Configuration** screen allows the user to reboot the device or restore the device to factory default values. Field descriptions follow the screen example.



Configuration

This page allows reboot and restore factory defaults to the system.

Reboot/Factory Reset

Reboot ○ Yes ● No Apply

Factory Reset ○ Yes ● No Apply

Label	Description
Reboot/Factory Reset	
Reboot	To reboot, or power cycle, the EVW32C, select **Yes**, then click **Apply**.
Factory Reset	To restore the device to factory default values, select **Yes**, then click **Apply**.

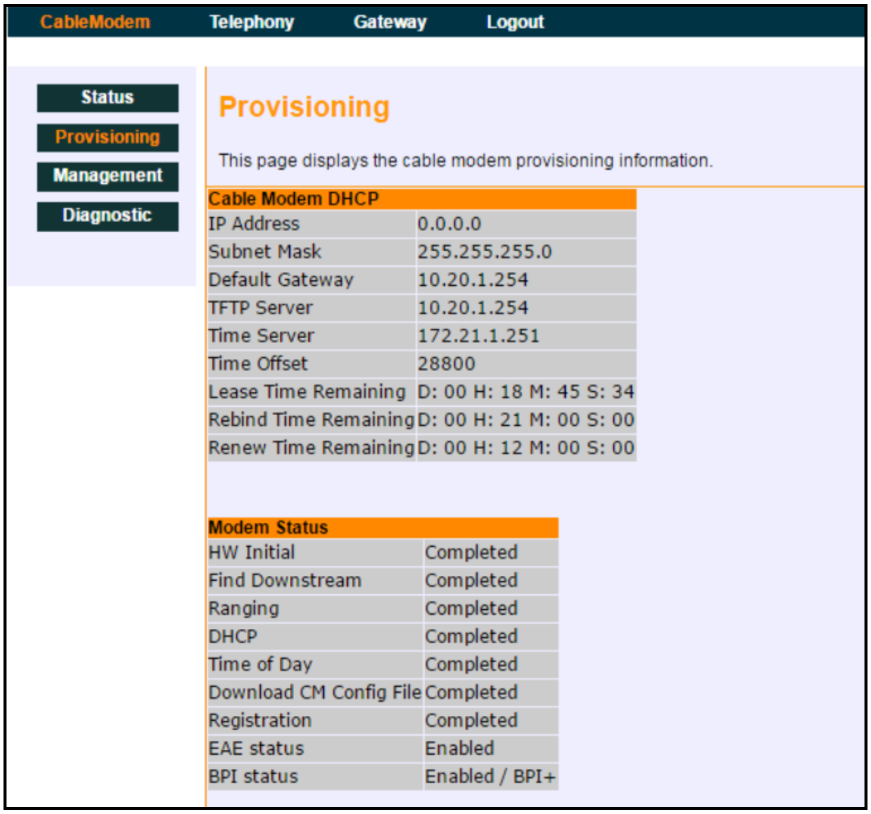
4.2 Using the Provisioning Option

Use the **Provisioning** option to view the cable modem provisioning options including the cable modem Dynamic Host Configuration Protocol (DHCP) and modem-status information.

To access the provisioning menu:

1. Click **Cable Modem** from the main menu.
2. Click **Provisioning** from the left side menu.

Field descriptions follow the screen example.



Provisioning

This page displays the cable modem provisioning information.

Cable Modem DHCP	
IP Address	0.0.0.0
Subnet Mask	255.255.255.0
Default Gateway	10.20.1.254
TFTP Server	10.20.1.254
Time Server	172.21.1.251
Time Offset	28800
Lease Time Remaining	D: 00 H: 18 M: 45 S: 34
Rebind Time Remaining	D: 00 H: 21 M: 00 S: 00
Renew Time Remaining	D: 00 H: 12 M: 00 S: 00

Modem Status	
HW Initial	Completed
Find Downstream	Completed
Ranging	Completed
DHCP	Completed
Time of Day	Completed
Download CM Config File	Completed
Registration	Completed
EAE status	Enabled
BPI status	Enabled / BPI+

Label	Description
Cable Modem DHCP	
IP Address	Displays the cable modem DHCP IP address.
Subnet Mask	Displays the subnet mask IP address.
Default Gateway	Displays the default gateway IP address.
TFTP Server	Displays the TFTP Server IP address.
Time Server	Displays the Time Server IP address.
Time Offset	Displays the time offset.
Lease Time Remaining	Defines the DHCP lease time duration in minutes between 1 and 71582788. A DHCP user's PC gets an IP address with a lease time. When the lease time expires, the PC must connect to the DHCP server and be issued a new, unused IP address.
Rebind Time Remaining	Displays the rebind time remaining in days, hours, minutes, and seconds.
Renew Time Remaining	Displays the renew time remaining in days, hours, minutes, and seconds.
Modem-Status	
HW Initial	Displays whether hardware initialization is completed.
Find Downstream	Displays whether finding a downstream channel is completed.
Ranging	Displays whether ranging is completed.

Label	Description
DHCP	Displays whether DHCP is completed.
Time of Day	Displays whether the time of day is completed.
Download CM Config File	Displays the name of the configuration file and if download was completed or not.
Registration	Displays whether device registration is completed.
EAE Status	Displays whether EAE (Early Authentication Encryption) is enabled or disabled.
BPI Status	Displays whether BPI (Baseline Privacy Interface) is enabled or disabled.

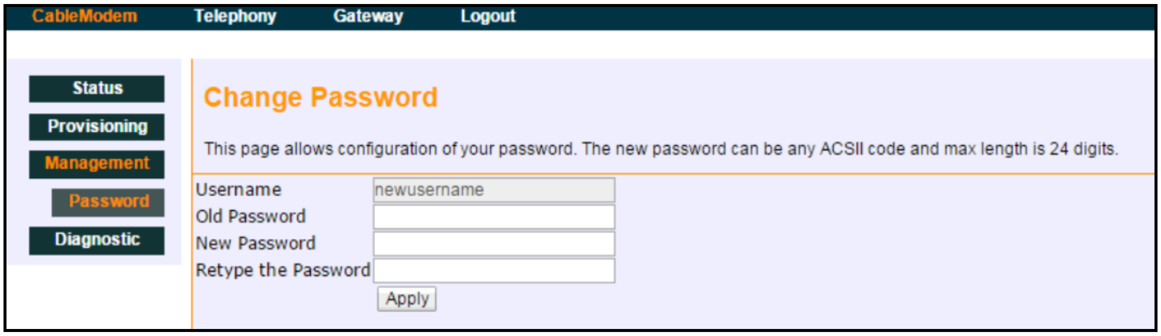
4.3 Using the Management Option

The Management menu allows you to set the device user name and password.

To access the management menu:

1. Click **Cable Modem** from the main menu.
2. Click **Management** from the left side menu.

The **Password** screen allows you to change the username and password for the EVW32C. Field descriptions are listed below the screen example.



Change Password

This page allows configuration of your password. The new password can be any ACSII code and max length is 24 digits.

Username: newusername
Old Password
New Password
Retype the Password

Label	Description
Username	Enter the new username.
Old Password	Enter the old password.
New Password	Enter the new password.
Retype the Password	Confirm the new password by retyping it here.
Apply	Saves changes.

4.4 Using the Diagnostic Option

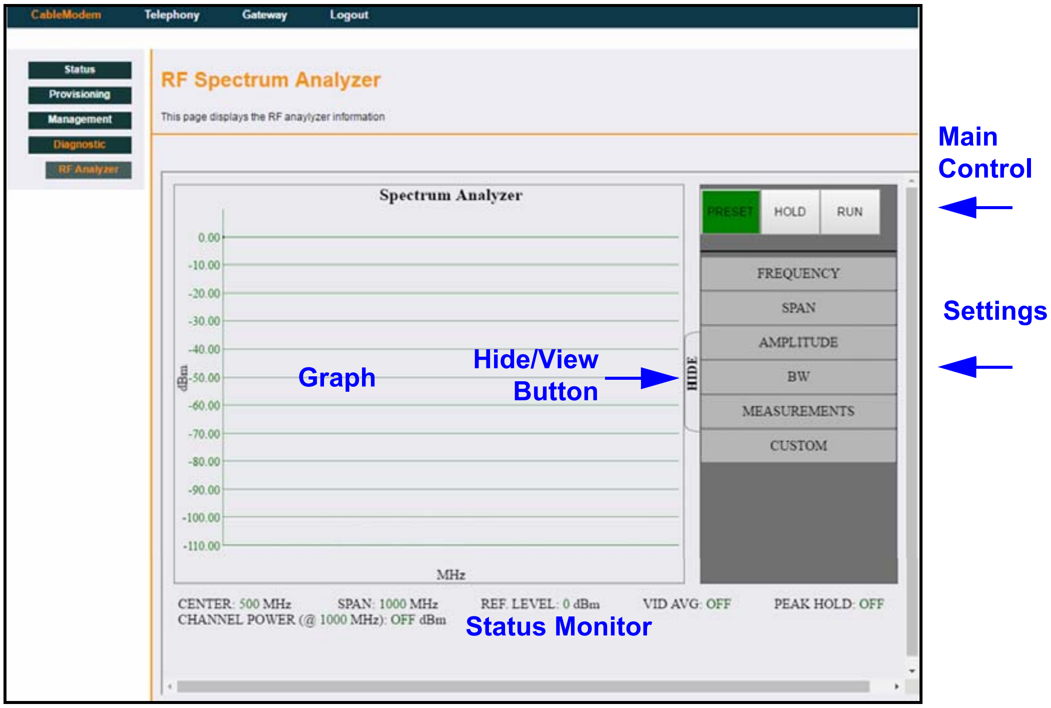
The Diagnostic option allows you to view RF Spectrum Analysis information. The spectrum analyzer can unobtrusively monitor the complete 1 GHz cable plant in real time without affecting user viewing or broadband data services on any video or data channels. This tool can be used by cable operators to reduce service calls allowing technicians to troubleshoot issues during an installation. After installations, it allows cable operators to collect RF diagnostics data from each unit to analyze and evaluate network health.

Note: To view spectrum analysis information, the web browser must support HTML5 and Websockets. Chrome and Safari will support it, but Internet Explorer will not.

To access the diagnostic menu:

1. Click **Cable Modem** from the main menu.
2. Click **Diagnostic** from the left side menu.

The **RF Analyzer** screen is displayed. Descriptions follow the screen shots below.



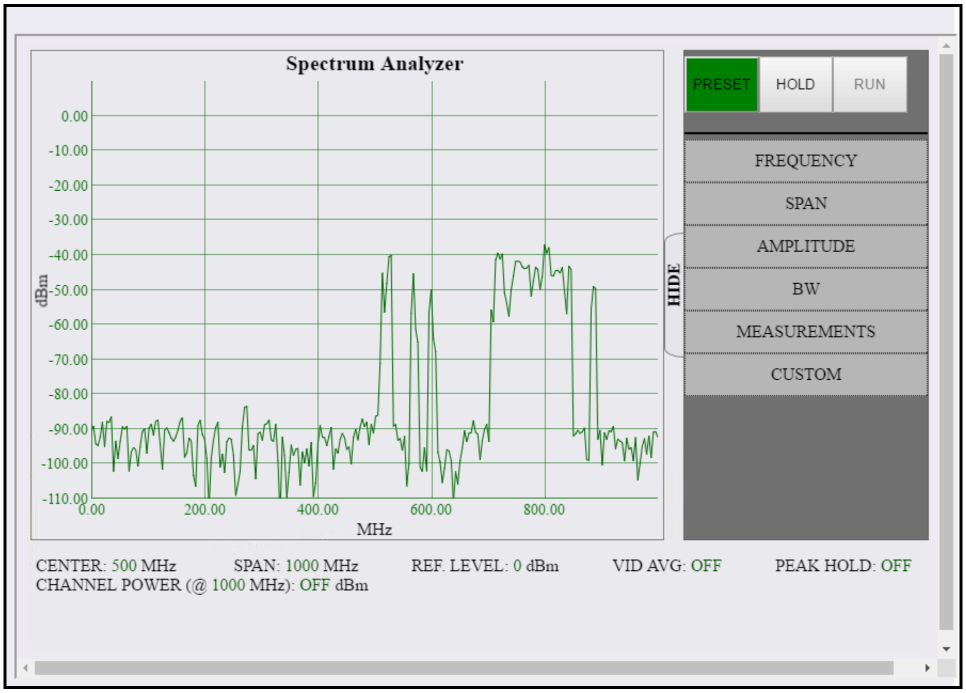
RF Spectrum Analyzer

This page displays the RF anaylyzer information

CENTER: 500 MHz SPAN: 1000 MHz REF. LEVEL: 0 dBm VID AVG: OFF PEAK HOLD: OFF
CHANNEL POWER (@ 1000 MHz): OFF dBm

Label	Description
Graph	This section is the main spectrum analyzer plot, which is where the data is displayed.
HIDE/VIEW Button	Click HIDE to shrink the right hand side controls and expand the graph to full width. Click VIEW to show the right hand side controls.
Main Control	This section contains the main buttons to start/stop the spectrum analyzer and to reset the setting back to the default settings. ♦ PRESET: Resets all the settings back to default values. ♦ HOLD: Stops the spectrum analyzer from running. ♦ RUN: Starts the spectrum analyzer.
Settings	This section contains all the supported settings for adjusting the plot or enabling features. ♦ FREQUENCY: Specifies the frequency (center, start, or stop) to monitor in terms of Hz. ♦ SPAN: Specifies how wide of a span to view in terms of Hz. ♦ AMPLITUDE: Sets the reference level (offset) of the input signal. ♦ BW: Bandwidth ♦ MEASUREMENTS:
Status Monitor	This section contains all the fields for supported measurements and current settings. ♦ CENTER ♦ SPAN ♦ REF LEVEL: Reference level ♦ VID AVG: Enable/Disable video averaging ♦ CHANNEL POWER: Specifies the span of the channel relative to the center frequency to measure power over.

The following screen shot shows the analyzer running.



CENTER: 500 MHz SPAN: 1000 MHz REF. LEVEL: 0 dBm VID AVG: OFF PEAK HOLD: OFF
CHANNEL POWER (@ 1000 MHz): OFF dBm

5 Understanding the Telephony Menu

The Telephony menu provides information regarding provisioning and line status for the EVW32C.

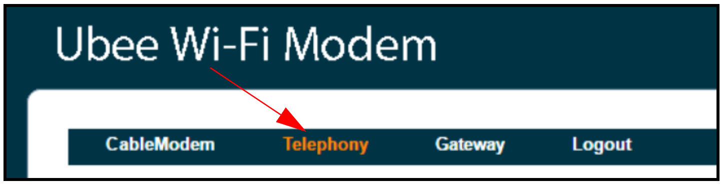
Topics

See the following topics:

- ♦ Using the Status Option on page 32

To access the telephony menu:

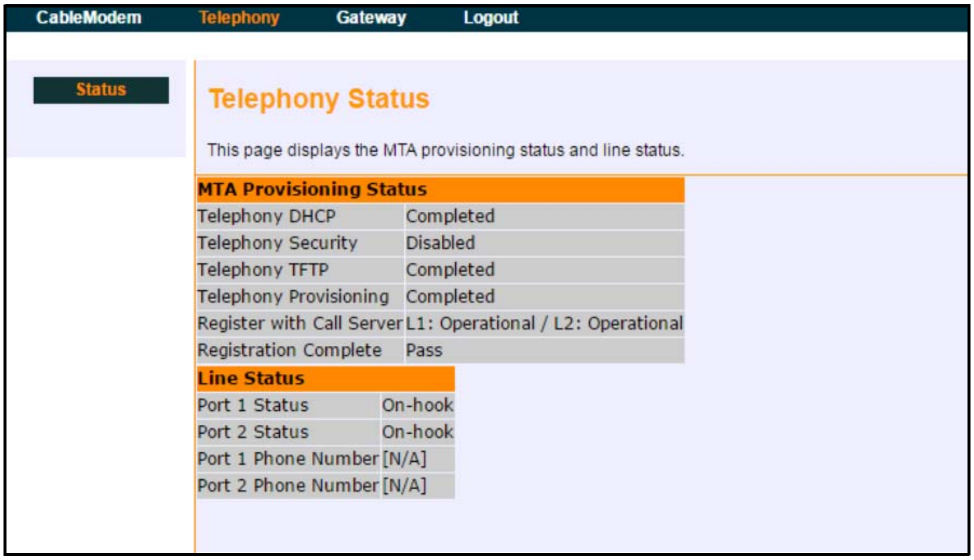
1. Access the Web interface. Refer to Accessing the Web User Interface (UI) Locally on page 19.
2. Click **Telephony** from the main menu.



3. The Status page is displayed.

5.1 Using the Status Option

The **Status** screen displays provisioning progress and MTA line status. Field descriptions follow the screen example.



Telephony Status

This page displays the MTA provisioning status and line status.

MTA Provisioning Status	
Telephony DHCP	Completed
Telephony Security	Disabled
Telephony TFTP	Completed
Telephony Provisioning	Completed
Register with Call Server	L1: Operational / L2: Operational
Registration Complete	Pass

Line Status	
Port 1 Status	On-hook
Port 2 Status	On-hook
Port 1 Phone Number	[N/A]
Port 2 Phone Number	[N/A]

Label	Description
MTA Provisioning Status	
Telephony DHCP	Displays whether the DHCP IP address has been registered.
Telephony Security	Displays the status of the security mode of the MTA (Enabled or Disabled).
Telephony TFTP	Displays whether the MTA's TFTP server registration is complete.
Telephony Provisioning	Displays whether telephony provisioning is complete.
Register with Call Server	Displays the status of the MTA's registration to the service provider's call server per line (Disconnected, Operational).
Registration Complete	Displays the completion status of the MTA registration.
Line Status	
Port 1 Status	Displays whether the telephone hooked up to port 1 is on-hook or off-hook
Port 2 Status	Displays whether the telephone hooked up to port 2 is on-hook or off-hook
Port 1 Phone Number	Displays the phone number associated with the telephone hooked up to port 1.
Port 2 Phone Number	Displays the phone number associated with the telephone hooked up to port 2.

6 Understanding the Gateway Menu

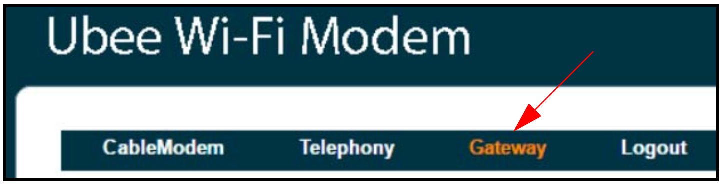
The Gateway menu provides the majority of the configuration options for the EVW32C. LAN, WAN, Firewall, VPN, Parental Control, and Wireless features are addressed.

Topics

See the following topics:

To access the Gateway menu:

1. Access the Web user interface. Refer to Accessing the Web User Interface (UI) Locally on page 19.
2. Click **Gateway** from the main menu.



3. The following sub-menu items are available for selection:
   - LAN
   - WAN
   - WLAN
   - Advanced
   - Management
   - VPN
   - Parental Control

6.1 Using the LAN Option

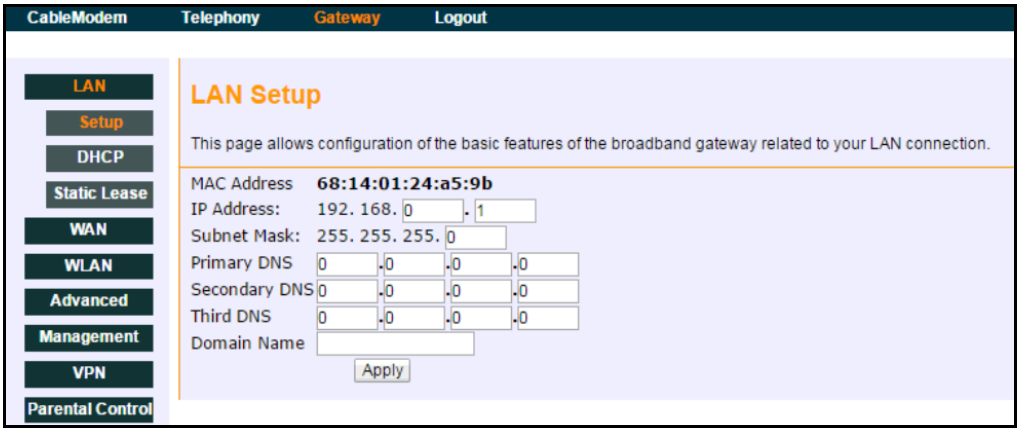
Use the **LAN** option to configure common gateway parameters and DHCP (dynamic host configuration protocol) behavior.

To configure LAN parameters:

1. Click **Gateway** from the main menu.
2. Click **LAN** from the left side.
3. The following sub-menu items are available for selection:
   - Setup
   - DHCP

6.1.1 Using the Setup Option

The LAN Setup screen allows you to configure basic features related to the LAN connection. Field descriptions are listed below the screen example.



LAN Setup

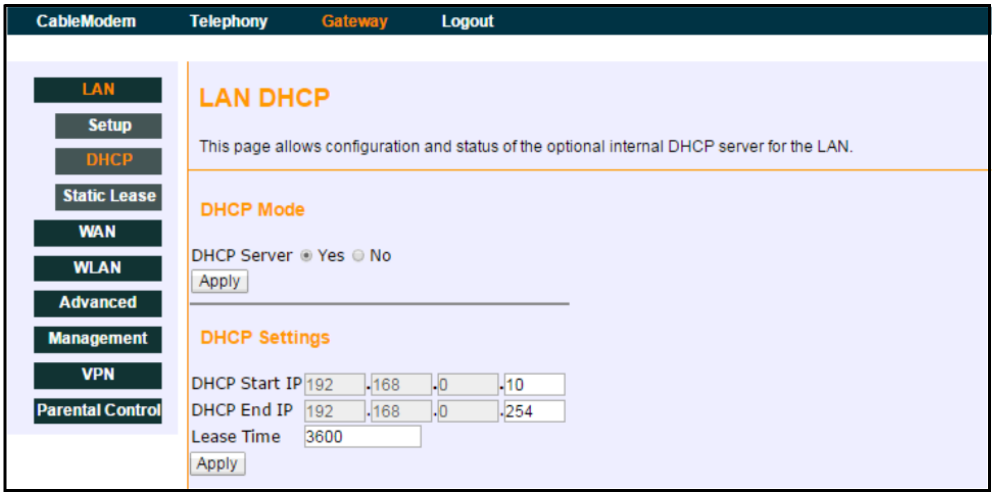
This page allows configuration of the basic features of the broadband gateway related to your LAN connection.

MAC Address 68:14:01:24:a5:9b
IP Address: 192. 168. 0 . 1
Subnet Mask: 255. 255. 255. 0
Primary DNS 0 .0 .0 .0
Secondary DNS 0 .0 .0 .0
Third DNS 0 .0 .0 .0
Domain Name

Label	Description
MAC Address	Displays the LAN interface's hardware address.
IP Address	Defines the local IP address, which is the default gateway address for all wired LAN hosts that connect to the EVW32C.
Subnet Mask	Displays the Subnet Mask for the LAN interface.
Primary DNS	Allows you to enter the Primary DNS (Domain Name Server) for the routed subnet.
Secondary DNS	Allows you to enter the Secondary DNS (Domain Name Server) for the routed subnet.
Third DNS	Allows you to enter the Third DNS (Domain Name Server) for the routed subnet.
Domain Name	Domain Name is a system that assigns addresses to Internet web servers. This may be required by domain name service providers.
Apply	Saves changes.

6.1.2 Using the DHCP Option

Use the **DHCP** option to configure dynamic host configuration protocol-specific behavior for the device. Field descriptions are listed below the screen example.



LAN DHCP

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

DHCP Mode

DHCP Server ● Yes ○ No

DHCP Settings

DHCP Start IP 192 .168 .0 .10
DHCP End IP 192 .168 .0 .254
Lease Time 3600

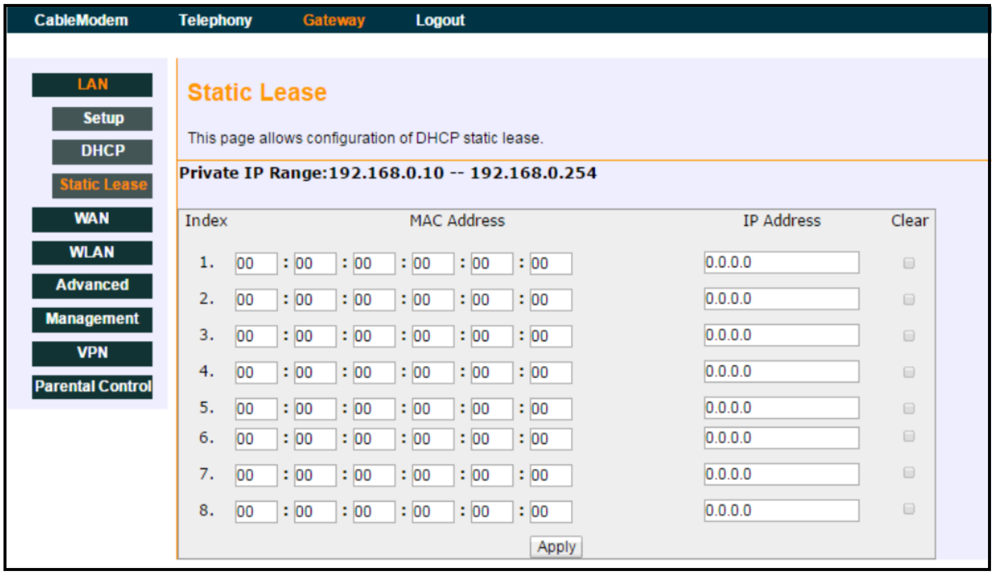
Label	Description
DHCP Mode	
DHCP Server	Enables (Yes) or disables (No) DHCP on the EVW32C. If No is selected, all the static DHCP settings on this screen are ignored.
Apply	Saves changes.
DHCP Settings	
DHCP Start IP	Defines the starting IP address for the pool of IP addresses that can be used by connecting clients.
DHCP End IP	Defines the last IP address that can be used by connecting clients.
Lease Time	Defines the DHCP lease time duration in minutes between 1 and 71582788. A DHCP user's PC gets an IPv4 address with a lease time. When the lease time expires, the PC must connect to the DHCP server and be issued a new, unused IPv4 address. **Note:** The default DHCP lease time is 3600 seconds and should be changed to **86400** seconds (24 hours). This helps resolve connectivity issues with some Mac and Windows 7 devices that turn off the network interface when they go into standby mode. This results in slow Web browsing until the device gets a new IPv4 address via DHCP.
Apply	Saves changes.

6.1.3 Using the Static Lease Option

Use the **Static Lease** option to assign IP addresses to clients on your network that do not change. A static lease ensures a specific device always gets the same IP address, especially if devices are powered on and off or disconnected and reconnects. This may be useful in a variety of networking scenarios where you need more control over the network and the clients that connect to it. Examples in which you may need to use a static lease include:

- Using the IP Filtering Option on page 59
- on page 60
- Using the DMZ Option on page 65

Field descriptions are listed below the screen example.



Static Lease

This page allows configuration of DHCP static lease.

Private IP Range:192.168.0.10 -- 192.168.0.254

Index	MAC Address	IP Address	Clear
1.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	□
2.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	□
3.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	□
4.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	□
5.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	□
6.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	□
7.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	□
8.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	□

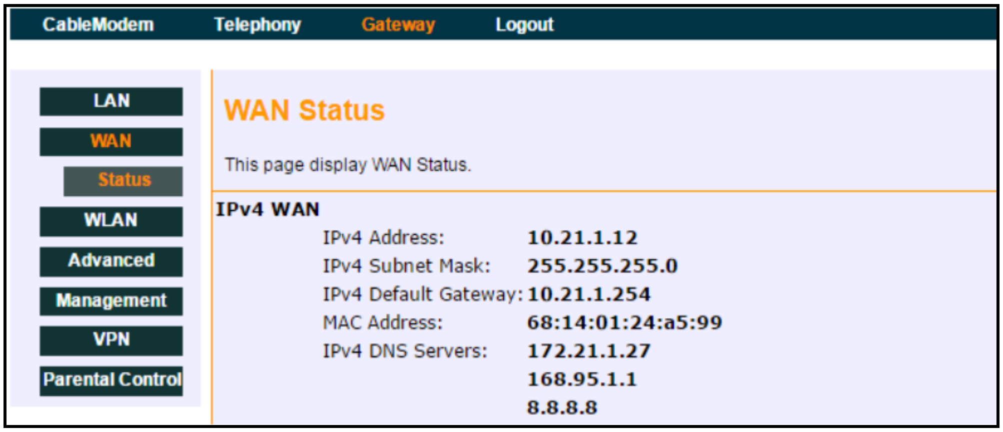
Label	Description
Index	Provides an index number for each client that connects to your network.
MAC Address	Allows you to enter the MAC address of the client to which you want to assign a static lease.
IP Address	Allows you to enter the IP address for the client.
Clear	Deletes the static lease when the Clear box is checked and **Apply** is selected.
Apply	Saves changes.

6.2 Using the WAN Option

Use the **WAN** option to view information regarding the WAN interface of the EVW32C.

To view WAN interface information:

1. Click **Gateway** from the main menu.
2. Click **WAN** from the left side.
3. The **WAN Status** screen is displayed. Field descriptions are listed below the screen example.



WAN Status

This page display WAN Status.

IPv4 WAN

IPv4 Address:	10.21.1.12
IPv4 Subnet Mask:	255.255.255.0
IPv4 Default Gateway:	10.21.1.254
MAC Address:	68:14:01:24:a5:99
IPv4 DNS Servers:	172.21.1.27 168.95.1.1 8.8.8.8

Label	Description
IPv4 WAN	
IPv4 Address	Displays the current WAN public IPv4 address obtained from the service provider.
IPv4 Subnet Mask	Displays the IPv4 subnet mask.
IPv4 Default Gateway	Displays the default IPv4 gateway.
MAC Address	Displays the WAN interface’s hardware address.
IPv4 DNS Servers	Lists the IPv4 DNS servers available on the network.

6.3 Using the WLAN Option

Use the WLAN (wireless local area network) option to configure wireless network settings. For assistance in deploying and troubleshooting the wireless network, refer to Deploying and Troubleshooting the Wireless Network on page 46.

To configure Wireless network settings:

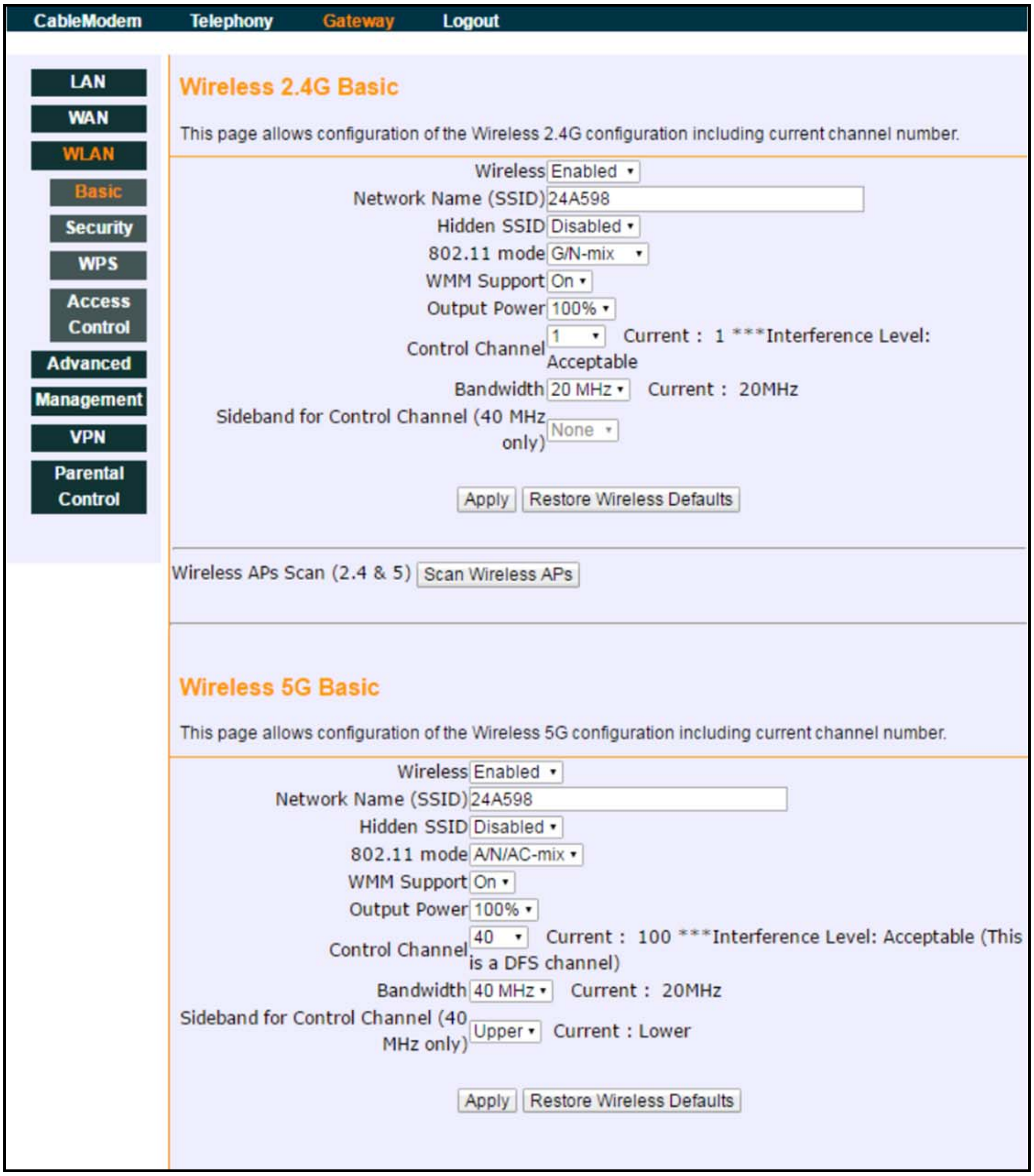
1. Click **Gateway** from the main menu.
2. Click **WLAN** from the left side menu.
3. The following sub-menu items are available for selection:
   - Basic
   - Security
   - WPS
   - Access Control

6.3.1 Using the Basic Option

The **Basic** option is used to configure both the 2.4GHz and 5GHz radios, including channel number, and bandwidth control.

IMPORTANT NOTE: The EVW32C is a *dual-band concurrent* wireless gateway, supporting operation of both the 2.4GHz and 5GHz radio bands simultaneously. Both radios are enabled by default.

Field descriptions are listed below the screen example.



Wireless 2.4G Basic

This page allows configuration of the Wireless 2.4G configuration including current channel number.

Wireless Enabled
Network Name (SSID) 24A598
Hidden SSID Disabled
802.11 mode G/N-mix
WMM Support On
Output Power 100%
Control Channel 1 Current : 1 ***Interference Level: Acceptable
Bandwidth 20 MHz Current : 20MHz
Sideband for Control Channel (40 MHz only) None

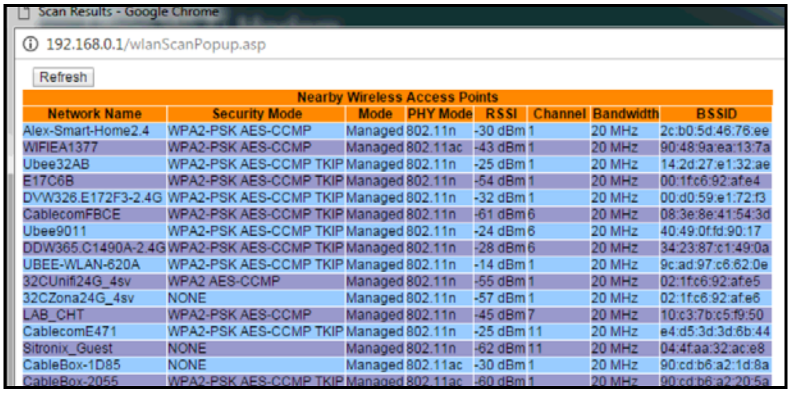
Wireless APs Scan (2.4 & 5)

Wireless 5G Basic

This page allows configuration of the Wireless 5G configuration including current channel number.

Wireless Enabled
Network Name (SSID) 24A598
Hidden SSID Disabled
802.11 mode A/N/AC-mix
WMM Support On
Output Power 100%
Control Channel 40 Current : 100 ***Interference Level: Acceptable (This is a DFS channel)
Bandwidth 40 MHz Current : 20MHz
Sideband for Control Channel (40 MHz only) Upper Current : Lower

Label	Description
The following fields are available for configuring either the 2.4GHz or the 5GHz radio:	
Wireless	Allows you to enable or disable the wireless radio. Both the 2.4GHz and 5GHz radios are enabled by default.
Network Name (SSID)	Displays the primary network name (SSID) to which client devices connect. It displays either the default SSID or a user defined SSID. The default SSID = The last 6 characters of the cable modem MAC address. To change the SSID to a personalized network name, highlight network name in the box, delete it, and enter a personalized network name. Click **Apply**.
Hidden SSID	When enabled, the SSID is not visible to wireless clients unless it is manually set up on the client. When disabled, the SSID is visible to wireless clients that wish to connect to the EVW32C.
802.11 mode	Sets the wireless networking standard. Select Auto to use 802.11 n mode when possible. This mode has a significant increase in the maximum raw OSI physical layer data rate from 54 Mbit/s to a maximum of 600 Mbit/s with the use of four spatial streams when at a channel width of 40 MHz. Options are: ♦ 2.4GHz: B/G/N-mix, G/N-mix, B/G-mix, N-only ♦ 5GHz: A/N/AC-mix, N/AC-mix, AC-only, A-only
WMM Support	When WMM (WiFi Multimedia) support is On, quality of service (QoS) is enabled to ensure the best service in your wireless network.
Output Power	Allows you to select the output power from the drop-down menu. Options are: 25%, 50%, 75%, 100%.
Control Channel	Selects a specific channel to deploy the wireless network. This allows you to set the operating frequency/channel depending on your particular region. Channel selection can have an impact on wireless networking performance. Control Channel is set to **Auto** by default. For more information, refer to Selecting a Wireless Channel on page 50. Options are: ♦ 2.4GHz: Auto, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 ♦ 5GHz: Auto, 40, 48, 56, 64, 104, 112, 120, 128, 136
Bandwidth	Sets the bandwidth to 20MHz or 40MHz. For 40 MHz, set the sideband to lower or upper 20MHz. 40 MHz channels double the channel width. This allows doubling the PHY data rate over a single 20 MHz channel. Options are: ♦ 2.4GHz: 20MHz, 40MHz ♦ 5GHz: 20MHz, 40MHz, 80MHz
Sideband for Control Channel	Only when using 40MHz Bandwidth should you choose the Lower or Upper 20MHz.

Label	Description
Apply	Saves all screen changes when clicked.
Restore Wireless Defaults	Restores the factory default settings for wireless configurations when clicked.
Wireless APs Scan (2.4 and 5)	When you click the **Scan Wireless APs** button, a pop-up window shows information about nearby wireless access points (example below). 

Scan Results - Google Chrome

192.168.0.1/wlanScanPopup.asp

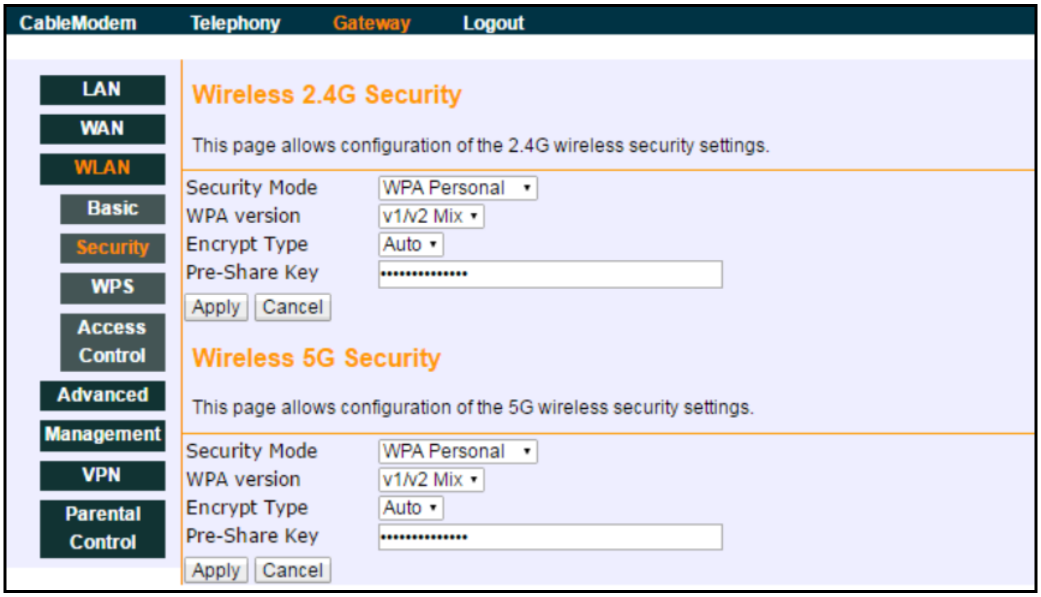
Nearby Wireless Access Points

Network Name	Security Mode	Mode	PHY Mode	RSSI	Channel	Bandwidth	BSSID
Alex-Smart-Home2.4	WPA2-PSK AES-CCMP	Managed	802.11n	-30 dBm	1	20 MHz	2c:b0:5d:46:76:ee
WIFIEA1377	WPA2-PSK AES-CCMP	Managed	802.11ac	-43 dBm	1	20 MHz	90:48:9a:ea:13:7a
Ubee32AB	WPA2-PSK AES-CCMP TKIP	Managed	802.11n	-25 dBm	1	20 MHz	14:2d:27:e1:32:ae
E17C6B	WPA2-PSK AES-CCMP TKIP	Managed	802.11n	-54 dBm	1	20 MHz	00:1f:c6:92:af:e4
DVW326.E172F3-2.4G	WPA2-PSK AES-CCMP TKIP	Managed	802.11n	-32 dBm	1	20 MHz	00:d0:59:e1:72:f3
CablecomFBCE	WPA2-PSK AES-CCMP TKIP	Managed	802.11n	-61 dBm	6	20 MHz	08:3e:8e:41:54:3d
Ubee9011	WPA2-PSK AES-CCMP TKIP	Managed	802.11n	-24 dBm	6	20 MHz	40:49:0f:fd:90:17
DDW365.C1490A-2.4G	WPA2-PSK AES-CCMP TKIP	Managed	802.11n	-28 dBm	6	20 MHz	34:23:87:c1:49:0a
UBEE-WLAN-620A	WPA2-PSK AES-CCMP TKIP	Managed	802.11n	-14 dBm	1	20 MHz	9c:ad:97:c6:62:0e
32CUnifi24G_4sv	WPA2 AES-CCMP	Managed	802.11n	-55 dBm	1	20 MHz	02:1f:c6:92:af:e5
32CZona24G_4sv	NONE	Managed	802.11n	-57 dBm	1	20 MHz	02:1f:c6:92:af:e6
LAB_CHT	WPA2-PSK AES-CCMP	Managed	802.11n	-45 dBm	7	20 MHz	10:c3:7b:c5:f9:50
CablecomE471	WPA2-PSK AES-CCMP TKIP	Managed	802.11n	-25 dBm	11	20 MHz	e4:d5:3d:3d:6b:44
Sitronix_Guest	NONE	Managed	802.11n	-62 dBm	11	20 MHz	04:4f:aa:32:ac:e8
CableBox-1D85	NONE	Managed	802.11ac	-30 dBm	1	20 MHz	90:cd:b6:a2:1d:8a
CableBox-2055	WPA2-PSK AES-CCMP TKIP	Managed	802.11ac	-60 dBm	1	20 MHz	90:cd:b6:a2:20:5a

6.3.2 Using the Security Option

Use the **Security** option to configure a variety of wireless security settings for both the 2.4GHz and 5GHz radio bands. For more information regarding wireless default values, see Understanding Default Values and Logins on page 10.

Field descriptions are listed below the screen example.



Wireless 2.4G Security

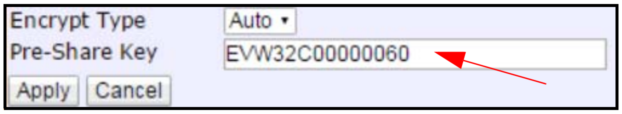
This page allows configuration of the 2.4G wireless security settings.

Security Mode	WPA Personal
WPA version	v1/v2 Mix
Encrypt Type	Auto
Pre-Share Key	••••••••••••••

Wireless 5G Security

This page allows configuration of the 5G wireless security settings.

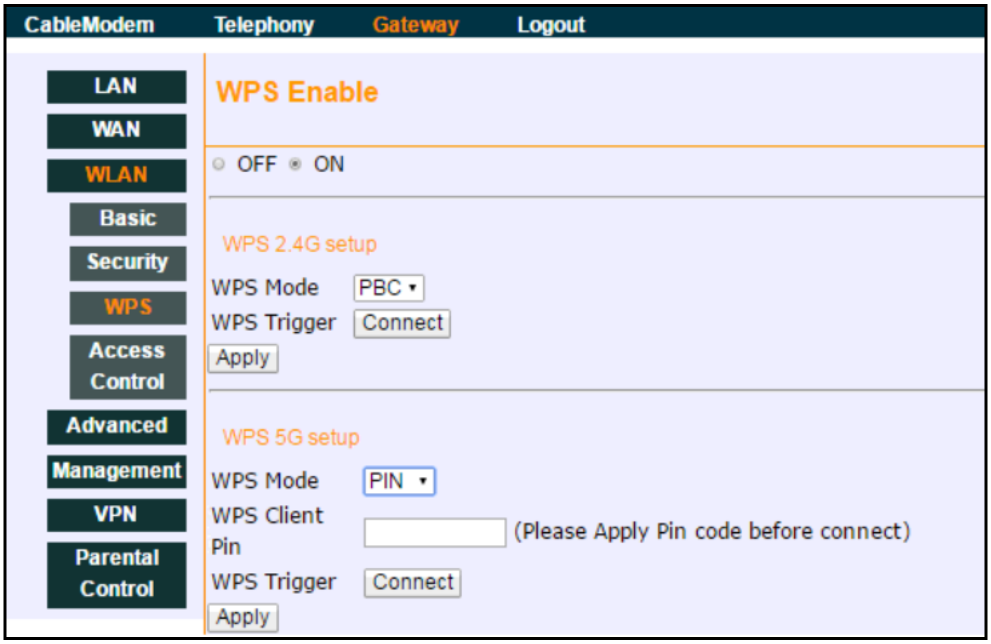
Security Mode	WPA Personal
WPA version	v1/v2 Mix
Encrypt Type	Auto
Pre-Share Key	••••••••••••••

Label	Description
The following fields are available for configuring security settings for either the 2.4GHz or the 5GHz radio:	
Security Mode	Allows selection of the security mode. Options are: ♦ Disable ♦ WEP 128 ♦ WEP 64 ♦ WPA Personal (default setting) ♦ WPA Enterprise
WPA version	Allows you to select the WPA version. Options are: ♦ Version 1 ♦ Version 2 ♦ v1/v2 Mix (default setting)
Encrypt Type	Allows you to select the Encryption type. Options are: ♦ TKIP ♦ AES ♦ Auto (default setting)
Pre-Share Key	Displays the Pre-Share Key when WPA or 802.1x network authentication is used. The pre-share key is a unique key for each device, also called the network key, the wireless key, or the wireless password. The pre-shared key for the EVW32C is the 14 characters of the device serial number. For example: **EVW32C00000060**. **Note:** the pre-share key is visible when you hover over the box next to "Pre-Share Key."  Encrypt Type: Auto ▾ Pre-Share Key: EVW32C00000060 To change the pre-share key (wireless password) to a personalized password, highlight the current password in the box, delete it, and enter a personalized password. Click **Apply**.
Apply	Saves changes.
Cancel	Cancels changes.

6.3.3 Using the WPS Option

Use the **WPS** option for automatic security configuration for devices connecting to the wireless network using WPS (Wi-Fi Protected Setup) without the need to know the encryption type, network name, or wireless network key. This screen allows configuration for both the 2.4GHz and 5GHz radios. Wireless default values are discussed in Understanding Default Values and Logins on page 10.

Field descriptions are listed below the screen example.



WPS Enable

○ OFF ● ON

WPS 2.4G setup

WPS Mode: PBC ▾

WPS Trigger: Connect

Apply

WPS 5G setup

WPS Mode: PIN ▾

WPS Client Pin: (Please Apply Pin code before connect)

WPS Trigger: Connect

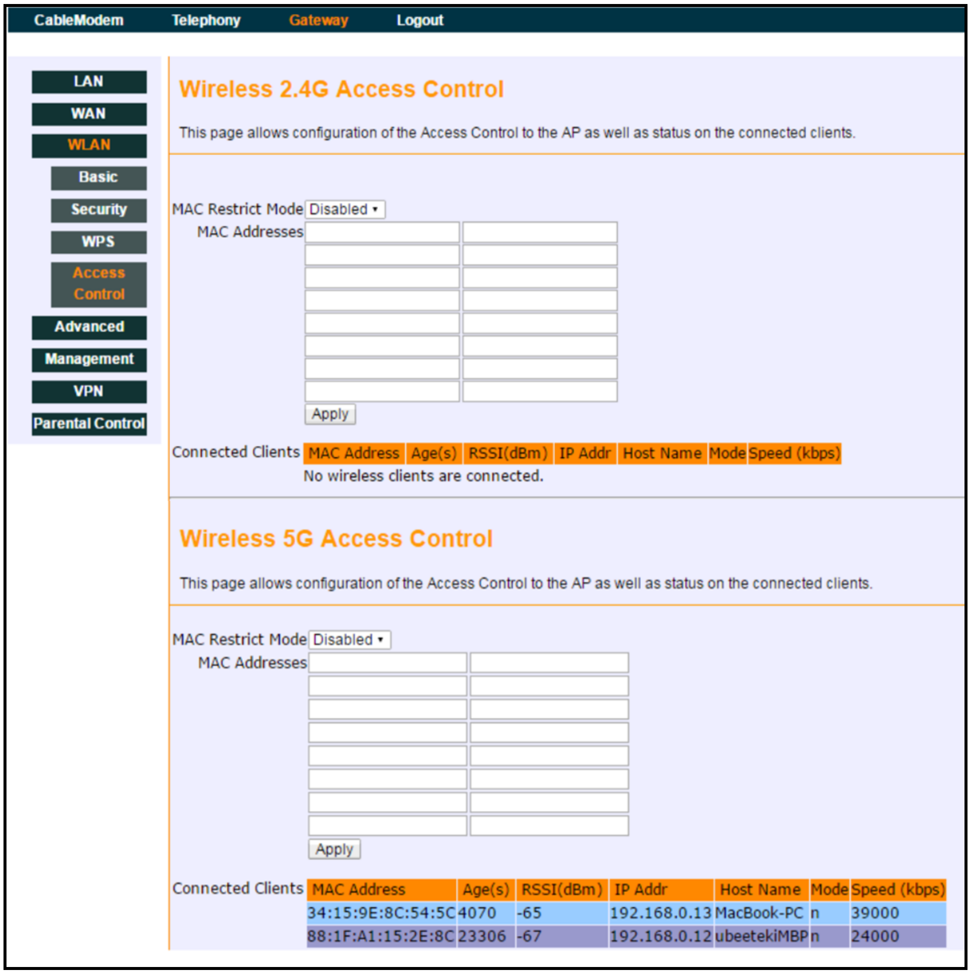
Apply

Label	Description
The following fields are available for configuring WPS settings for either the 2.4GHz or the 5GHz radio:	
WPS Enable	Check **ON** or **OFF** to enable or disable the WPS option.
WPS Mode	Allows you to choose between the 2 WPS modes: 1. PIN: User must enter the client WPS Pin. **Note:** When PIN is selected, the WPS Client Pin field will appear. 2. PBC (Push Button Configuration): A software or a hardware button is pushed on both the EVW32C and the wireless client that wishes to connect. Both devices are then in registration mode. This is the default setting.
WPS Client Pin	This field is only visible when PIN is selected as the WPS Mode. The connecting client's WPS Pin number must be entered in the space provided before clicking the Connect box.
WPS Trigger	Triggers connection to the client via WPS. The WPS Client Pin must be entered into the space provided before clicking the Connect box.
Apply	Saves changes.

6.3.4 Using the Access Control Option

Use the **Access Control** option to configure which clients can access either the 2.4GHz or 5GHz wireless networks. It also displays the status of currently connected clients.

Field descriptions are listed below the screen example.



Wireless 2.4G Access Control

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

MAC Restrict Mode Disabled

MAC Addresses

Connected Clients

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

No wireless clients are connected.

Wireless 5G Access Control

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

MAC Restrict Mode Disabled

MAC Addresses

Connected Clients

MAC Address	Age(s)	RSSI(dBm)	IP Addr	Host Name	Mode	Speed (kbps)
34:15:9E:8C:54:5C	4070	-65	192.168.0.13	MacBook-PC	n	39000
88:1F:A1:15:2E:8C	23306	-67	192.168.0.12	ubeetekiMBP	n	24000

Label	Description
The following fields are available for configuring Access Control settings for either the 2.4GHz or the 5GHz radio:	
MAC Restrict Mode	Controls wireless access to your network by MAC address. ♦ **Disabled** turns off MAC restrictions and allows any wireless client to connect to this device. However, if you use other security mechanisms for access to the wireless network, clients must still adhere to those restrictions. Disabled is the default setting. ♦ **Allow** creates a list of wireless clients that can connect to the wireless network. Enter the MAC addresses of these clients in the MAC Addresses fields. MAC addresses not on the list, are not allowed access to your wireless network. ♦ **Deny** creates a list of wireless clients that you do not want to have access to your wireless network. Enter the MAC addresses of these clients in the MAC Addresses fields.

Label	Description
MAC Addresses	Displays the MAC addresses. Note: You may cut and paste MAC addresses from the connected clients list at the bottom of the screen.
Apply	Saves changes when clicked.
Connected Clients	Lists wireless clients currently connected listed by MAC address. ♦ **MAC Address** – Displays the MAC addresses entered in the MAC Addresses field (see above). ♦ **Age(s)** – Displays the duration since the wireless client's polled values were sent to the device. The values include all information shown on this screen. The lower the number, the more current its data. ♦ **RSSI(dBm)** – Displays the received signal strength from the device to the wireless cable modem. This value is commonly used to assist in troubleshooting wireless performance issues. A signal strength between 0dBm and -65dBm is considered optimal. Levels of -66dBm and lower (for example, -70, -80, etc.) have a downward impact on wireless data throughput. Refer to Understanding Received Signal Strength on page 46 for more information. ♦ **IP Addr** – Displays the IP address assigned to this wireless client. ♦ **Host Name** – Displays the host name of the wireless client. ♦ **Mode** – Indicates the applicable 802.11a/b/g/n standard used by the connected client device. ♦ **Speed (kbps)** – Displays the maximum theoretical link speed negotiated between the wireless gateway and the client, not including the overhead associated with encryption, and so on. For example, actual speeds with WEP encryption enabled are typically less than half of the negotiated link speed. TKIP encryption can also affect performance. AES is the most efficient and secure with the highest throughput possible. You can disable WMM if throughput on some client adapters is adversely affected.

6.3.5 Deploying and Troubleshooting the Wireless Network

Use the information in this section to help you understand, deploy, and troubleshoot your wireless environments:

- Understanding Received Signal Strength on page 46
- Estimating Wireless Cable Modem to Wireless Client Distances on page 47
- Understanding the 2.4GHz and 5GHZ Bands on page 49
- Selecting a Wireless Channel on page 50

6.3.5.1 Understanding Received Signal Strength

Received signal strength (RSSI) is measured from connected wireless client devices to the wireless cable modem. This value can significantly impact wireless speeds/performance. It is determined by:

- Materials (for example, open air, concrete, trees)
- Distance between wireless clients and the wireless cable modem
- Wireless capabilities of the client devices

To determine the received signal strength, refer to Using the Access Control Option on page 44 and review the **RSSI** value. A receive signal strength indicator between 0 to -64 dBm is considered optimal. Levels of -67dBm and lower (for example, -70, -80, etc.) have a downward impact on wireless data throughput.

6.3.5.2 Estimating Wireless Cable Modem to Wireless Client Distances

The information in this section helps you to determine how far a wireless access point (the EVW32C) can be placed from wireless client devices. Environmental variances include the capabilities of wireless clients and the types of material through which the wireless signal must pass. When the EVW32C and wireless clients reach the distance threshold between each other, network performance degrades.

To determine wireless cable modem placement:

1. Connect a wireless client to the EVW32C. Refer to Connecting Devices to the Network on page 15 if needed.
2. Place the wireless client at around one meter (three feet) away from the EVW32C.
3. Obtain the **RSSI** value for the connected client. Refer to Using the Access Control Option on page 44. This value is used in the formula further below.
4. Use the following table to determine what materials the wireless signal must travel through to reach the desired wireless coverage distance.

Attenuation Considerations		
Material	**Attenuation**	
	2.4GHZ	**5GHz**
Free Space	0.24dB / foot	0.3dB / foot
Interior Drywall	3dB to 4dB	3dB to 5dB
Cubicle Wall	2dB to 5dB	4dB to 9dB
Wood Door (Hollow/Solid)	3dB to 4dB	6dB to 7dB
Brick, Concrete Wall (Note 1)	6dB to 18dB	10dB to 30dB
Glass Window (not tinted)	2dB to 3dB	6dB to 8dB
Double Pane Coated Glass	13dB	20dB
Bullet Proof Glass	10dB	20dB
Steel / Fire Exit Door	13dB to 19dB	25dB to 32dB
Human Body	3dB	6dB
Trees (Note 2)	0.15dB / foot	0.3dB / foot
Note 1: Different types of concrete materials are used in different parts of the world and the thickness and coating differ depending on whether it is used in floors, interior walls, or exterior walls. **Note 2**: The attenuation caused by trees varies significantly depending upon the shape and thickness of the foliage.		

5. Use the attenuation value from the materials table above in the following formula:

Formula:

(Transmit Power, **use -30dBm**) **–** (Receiver Sensitivity, **use RSSI value**) **=**
Allowable Free Space Loss

Allowable Free Space Loss ÷ Materials Attenuation Value **=**
Optimal Distance in Feet Between the EVW32C and a Wireless Client

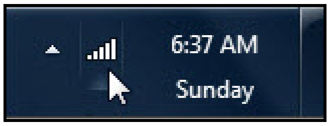
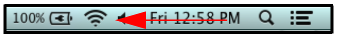
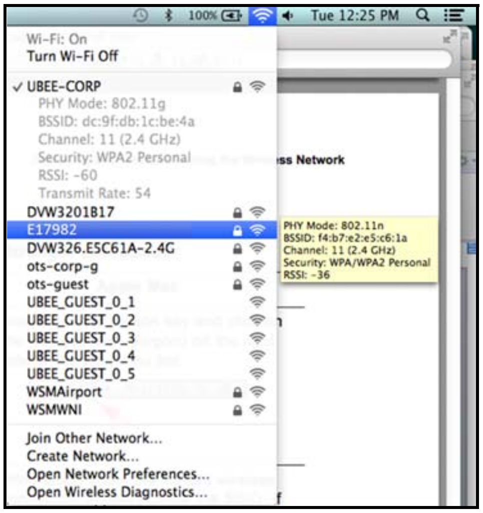
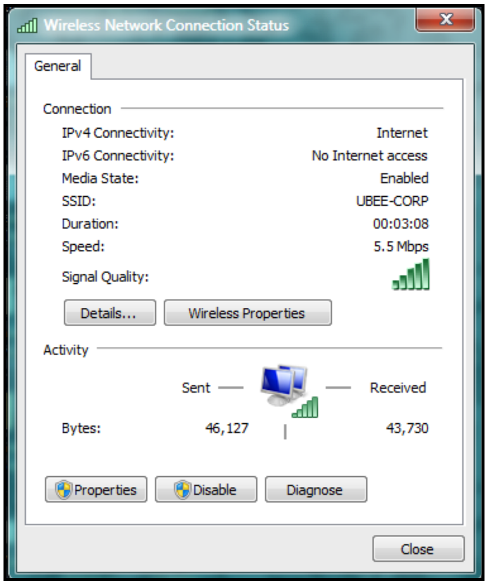
Example:

(-30dBm) **-** (-67dBm) **=** 37dBm (allowable free space loss for a 54Mbps connection)

37dBm ÷.24db/foot (for open space) **=** 154.16 feet

6. Once you know the optimal feet distance between individual wireless clients and the EVW32C, you may resolve and prevent some performance issues.

7. Check the wireless signal strength and speed of the computer connected via wireless to the EVW32C. Instructions for checking speeds are provided for both a Windows and Mac computer in the table below. If the wireless computer is not connected, refer to Connecting a Wireless Device on page 16.

Checking Wireless Signal Strength and Speed	
Windows PC	**Apple Mac**
1. Click the Wireless networking icon in the system tray to display a list of available wireless networks.  6:37 AM Sunday	1. Hold down the Option key and click on the wireless icon (Airport) on the right side of the top menu bar.  100% Fri 12:58 PM
2. Click “Open Network and Sharing Center,” then click “Wireless Network Connection.”	2. Information about the current wireless connection appears below the SSID. If you continue to hold the Option key and hover over any network, information about the connection is visible.  100% Tue 12:25 PM Wi-Fi: On Turn Wi-Fi Off ✓ UBEE-CORP PHY Mode: 802.11g BSSID: dc:9f:db:1c:be:4a Channel: 11 (2.4 GHz) Security: WPA2 Personal RSSI: -60 Transmit Rate: 54 DVW3201B17 E17982 DVW326.E5C61A-2.4G ots-corp-g ots-guest UBEE_GUEST_0_1 UBEE_GUEST_0_2 UBEE_GUEST_0_3 UBEE_GUEST_0_4 UBEE_GUEST_0_5 WSMAirport WSMWNI Join Other Network... Create Network... Open Network Preferences... Open Wireless Diagnostics... PHY Mode: 802.11n BSSID: f4:b7:e2:e5:c6:1a Channel: 11 (2.4 GHz) Security: WPA/WPA2 Personal RSSI: -36
3. Review the speed and signal strength in the Status window.  Wireless Network Connection Status General Connection IPv4 Connectivity: Internet IPv6 Connectivity: No Internet access Media State: Enabled SSID: UBEE-CORP Duration: 00:03:08 Speed: 5.5 Mbps Signal Quality: Details... Wireless Properties Activity Sent — — Received Bytes: 46,127 43,730 Properties Disable Diagnose Close	

6.3.5.3 Understanding the 2.4GHz and 5GHZ Bands

The EVW32C operates in both the 2.4GHZ and 5GHZ frequency bands simultaneously. This feature allows you to choose the best band for your device to ensure stability with your local and Internet connection.

The table below provides a comparison between the 2.4GHz and 5GHz bands.

Band	2.4GHz	5GHz
Channels	In the USA, channels 1-11 are used. There are 3 non-overlapping channels (1, 6, and 11). Auto channel should be selected to ensure that the channel with the least interference is used.	23 non-overlapping channels.
Standards	802.11b,g,n	802.11a,n,ac
Network Range	Wider range	Shorter Range
Interference	Higher, as many wireless devices such as cordless phones, microwave ovens, and computers use the 2.4GHz frequency.	Lower chance of picking up interference because fewer types of wireless devices use the 5GHz frequency.
Application	Recommended for simple Internet browsing and email, as these applications don't take too much bandwidth and work fine at a greater distance.	Recommended for applications that require uninterrupted throughput, like media streaming. The wider spectrum delivers better performance.
Note: If you want to use the 5GHz frequency, all wireless client adapters must support 5GHz.		

6.3.5.4 Selecting a Wireless Channel

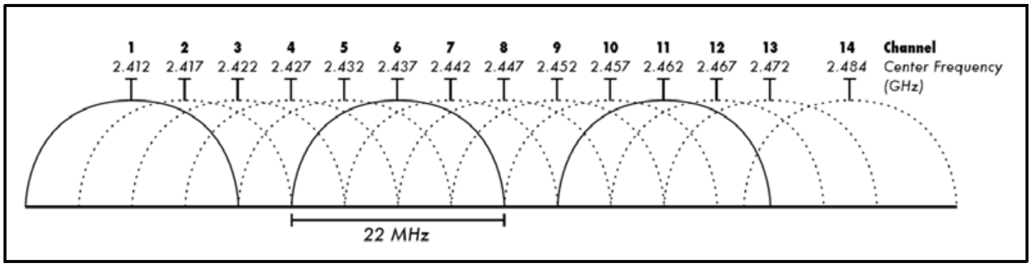
You may need to change the wireless channel on which the EVW32C operates when you are in computing, test, and other environments where several wireless access points may be operating in the 2.4GHz range.

In some cases, you may want to segment your wireless traffic where a group of devices operates on one channel and another group operates on another channel, and so on. This is done by configuring the channel on each wireless access point individually (if you have multiples). If you have control over only one wireless device in an environment where there may be several, you can change the wireless channel on your device to one that is not heavily used.

NOTE: To change the wireless broadcast channel, refer to Using the Basic Option on page 39.

2.4GHz Channels

The following diagram displays the 2.4GHz channels available in the Americas. Each available channel is 22MHz wide. Since channels overlap, it is best to choose channels that have the least overlap (typically 1, 6, and 11 in the Americas, and 1, 5, 9, and 13 in Europe). Overlapping channels can cause wireless network performance issues.



Source: Wikipedia.org, and IEEE article IEEE 802.11n-2009

5GHz Channels

The following table shows the 5GHz channel list and the corresponding frequencies.

Channel	GHz	Channel	GHz
36	5.180	108	5.540
40	5.200	112	5.560
44	5.220.	116	5.580
48	5.240	136	5.680
52	5.260	140	5.700
56	5.280	149	5.745
60	5.300	153	5.765
64	5.320	157	5.785
100	5.500	161	5.805
104	5.520	165	5.825

6.4 Using the Advanced Option

Use the **Advanced** option to configure advanced gateway setting such as MAC filtering and port forwarding.

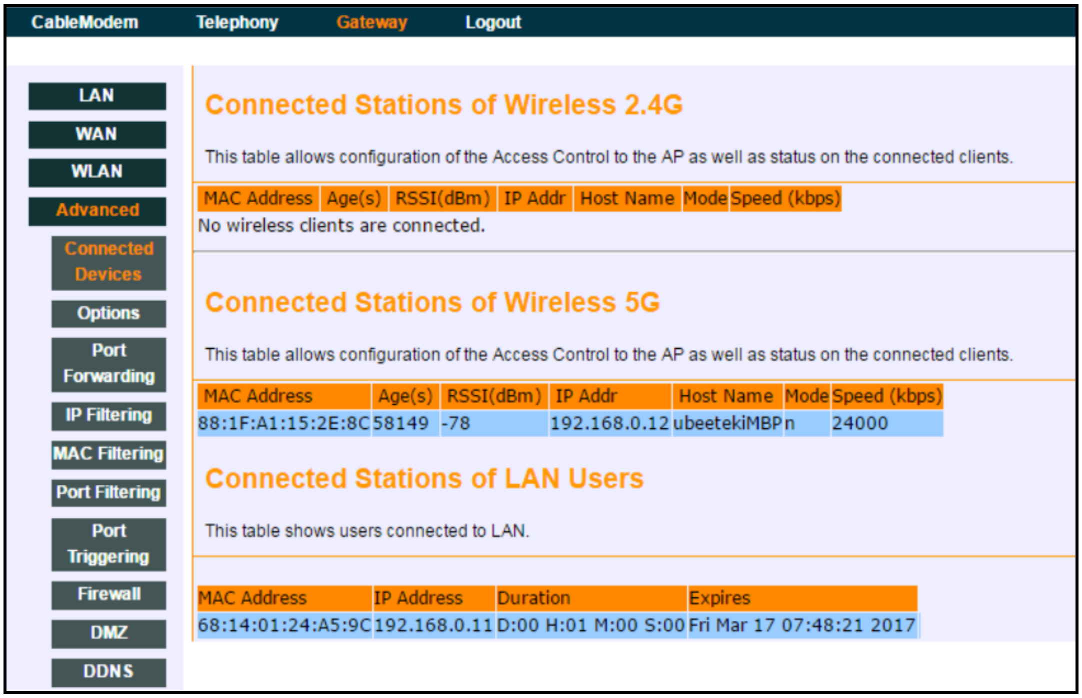
To configure Advanced gateway settings:

1. Click **Gateway** from the main menu.
2. Click **Advanced** from the left side.
3. The following sub-menu items are available for selection:
   - Connected Devices
   - Options
   - Port Forwarding
   - IP Filtering
   - MAC Filtering
   - Port Filtering

- Port Triggering
- Firewall
- DMZ
- DDNS

6.4.1 Using the Connected Devices Option

The Connected Devices screen displays information about devices currently connected to the EVW32C. Field descriptions are listed below the screen example.



Connected Stations of Wireless 2.4G

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

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

No wireless clients are connected.

Connected Stations of Wireless 5G

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

MAC Address	Age(s)	RSSI(dBm)	IP Addr	Host Name	Mode	Speed (kbps)
88:1F:A1:15:2E:8C	58149	-78	192.168.0.12	ubeetekiMBP	n	24000

Connected Stations of LAN Users

This table shows users connected to LAN.

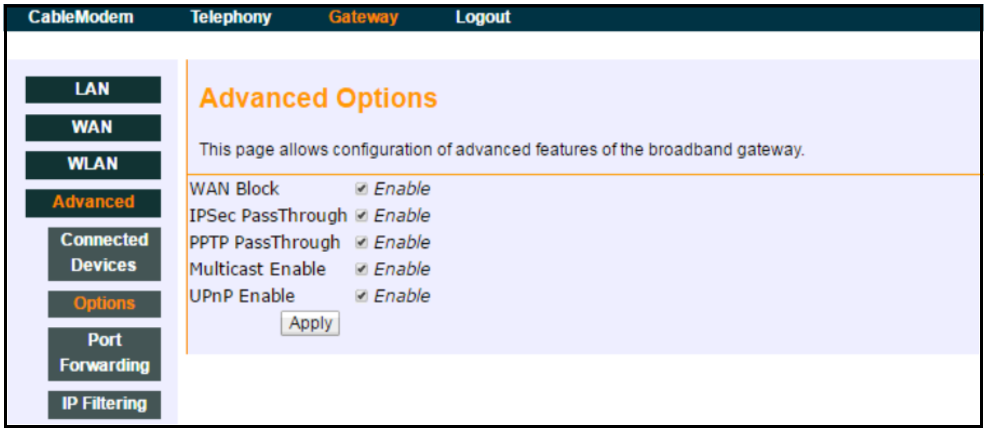
MAC Address	IP Address	Duration	Expires
68:14:01:24:A5:9C	192.168.0.11	D:00 H:01 M:00 S:00	Fri Mar 17 07:48:21 2017

Label	Description
Connected Stations of Wireless 2.4G Users	Displays information about clients currently connected to the 2.4GHz wireless radio.
MAC Address	Displays the MAC addresses of the connected client(s).
Age(s)	Displays the duration since the wireless client's polled values were sent to the device. The values include all information shown on this screen. The lower the number, the more current its data.
RSSI (dBm)	Displays the received signal strength from the device to the wireless cable modem. This value is commonly used to assist in troubleshooting wireless performance issues. A signal strength between 0dBm and -65dBm is considered optimal. Levels of -66dBm and lower (for example, -70, -80, etc.) have a downward impact on wireless data throughput. Refer to Understanding Received Signal Strength on page 46 for more information.
IP Addr	Displays the IP address assigned to this wireless client.
Host Name	Displays the host name of the wireless client.
Mode	Indicates the applicable 802.11a/b/g/n standard used by the connected client device.

Label	Description
Speed (kbps)	Displays the maximum theoretical link speed negotiated between the wireless gateway and the client, not including the overhead associated with encryption, and so on. For example, actual speeds with WEP encryption enabled are typically less than half of the negotiated link speed. TKIP encryption can also affect performance. AES is the most efficient and secure with the highest throughput possible. You can disable WMM if throughput on some client adapters is adversely affected.
Connected Stations of Wireless 5G Users	Displays information about clients currently connected to the 5GHz wireless radio.
MAC Address	Displays the MAC addresses of the connected client(s).
Age(s)	Displays the duration since the wireless client's polled values were sent to the device. The values include all information shown on this screen. The lower the number, the more current its data.
RSSI (dBm)	Displays the received signal strength from the device to the wireless cable modem. This value is commonly used to assist in troubleshooting wireless performance issues. A signal strength between 0dBm and -65dBm is considered optimal. Levels of -66dBm and lower (for example, -70, -80, etc.) have a downward impact on wireless data throughput. Refer to Understanding Received Signal Strength on page 46 for more information.
IP Addr	Displays the IP address assigned to this wireless client.
Host Name	Displays the host name of the wireless client.
Mode	Indicates the applicable 802.11a/b/g/n standard used by the connected client device.
Speed (kbps)	Displays the maximum theoretical link speed negotiated between the wireless gateway and the client, not including the overhead associated with encryption, and so on. For example, actual speeds with WEP encryption enabled are typically less than half of the negotiated link speed. TKIP encryption can also affect performance. AES is the most efficient and secure with the highest throughput possible. You can disable WMM if throughput on some client adapters is adversely affected.
Connected Stations of LAN Users	Displays information about users connected to the LAN.
MAC Address	Displays the MAC Address of the connected device(s).
IP Address	Displays the IP Address of the connected device(s).
Duration	Displays the accumulated time since the client acquired the IP address.
Expires	Displays the time until the IP address expires and must be recycled. If the IP address is reserved to a certain host, it shows STATIC IP ADDRESS.

6.4.2 Using the Options Option

The Options screen allows you to define which networking protocols are enabled or disabled on the device. The network address translation application (NAT ALG) settings provide additional security beyond the firewall. Field descriptions are listed below the screen example.



Advanced Options

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

WAN Block ☑ Enable
IPSec PassThrough ☑ Enable
PPTP PassThrough ☑ Enable
Multicast Enable ☑ Enable
UPnP Enable ☑ Enable

Apply

Label	Description
WAN Block	When enabled, WAN Block blocks PING access to the WAN public gateway IP address that is exposed to the Internet. When disabled, PING access is allowed to occur, which is necessary for the remote configuration of some VoIP phones (e.g. Cisco, Polycom, etc.).
IPsec Pass Through	When enabled, allows encrypted IPsec VPN traffic to pass through the router between the IPsec VPN Client application on the PC/Mac and the IPsec VPN Concentrator (e.g. Barracuda, Cisco, Juniper, etc.) for access to the “company VPN.”
PPTP Pass Through	When enabled, allows encrypted PPTP VPN traffic to pass through the router between the PPTP VPN Client application on the PC/Mac and the PPTP VPN Server (e.g. Windows Server 2013) for access to the “company VPN.”
Multicast Enable	Optimizes the bandwidth utilization compared with unicast (especially video streaming applications).
UPnP Enable	Activates Universal Plug and Play (UPnP). When enabled, a UPnP device can dynamically join a network, obtain an IP address, convey it’s capabilities, and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use. Gaming consoles and Web cameras are examples of devices that can use UPnP.
Apply	Saves changes.

6.4.3 Using the Port Forwarding Option

Forwarding tells the EVW32C to which computer on the local area network to send data. If your host systems or applications have communications issues with the Internet, you can use forwarding to resolve the following issues:

- ❑ Data is sent from a local host to the Internet, but the return path of expected data is not received by your local host.
- ❑ An application or service running on your local network (on local host) cannot be accessed from the Internet directly (for example, a request to a local audio server). Examples are:
  - ♦ Xbox/PlayStation – Games/applications
  - ♦ Home Security Systems – Security systems that use the Internet

- Audio Servers/VoIP – Audio and VoIP applications and services

See the following topics:

- Before Setting Up Forwarding on page 55
- Setting Up Forwarding on page 55
- Setting Up Port Forwarding for an Xbox Example on page 58

6.4.3.1 Before Setting Up Forwarding

Try the following options before you assign forwarding rules:

1. Enable Universal Plug and Play (UPnP). This may resolve the issue you have without setting up forwarding rules.

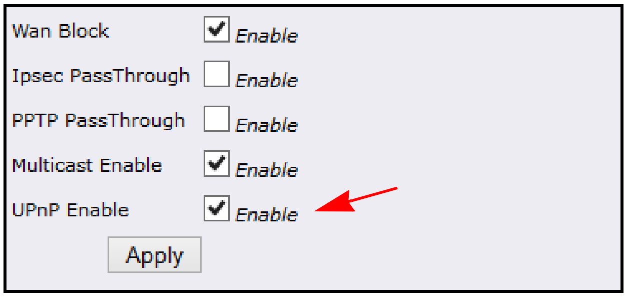
   a. Access the Web interface of the EVW32C, see Accessing the Web User Interface (UI) Locally on page 19.

   b. Click **Gateway** from the main menu.

   c. Click **Advanced** from the left menu.

   d. Click **Options** from the sub-menu.

   e. Check the **UPnP Enable** box.



Wan Block ☑ Enable
Ipsec PassThrough □ Enable
PPTP PassThrough □ Enable
Multicast Enable ☑ Enable
UPnP Enable ☑ Enable

   f. Click **Apply**.

   g. Test your local host or application such as your Xbox to see if it is functioning properly. Continue with port forwarding if the host or application is not communicating correctly.

2. Assign a Static IP lease to the client/host to which you are setting up forwarding. This way, the IP does not change and disrupt your forwarding rules. For example, if you are hosting a Web server in your internal network, and you wish to setup a forwarding rule for it, assign a static IP lease to that system to keep the IP from renewing and disrupting the forwarding rule.

   NOTE: To access a VPN, users must disable (uncheck) WAN Block and enable (check) both IPsec PassThrough and PPTP PassThrough.

6.4.3.2 Setting Up Forwarding

If the suggestions in Before Setting Up Forwarding on page 55 did not correct your communication problem, use port forwarding.

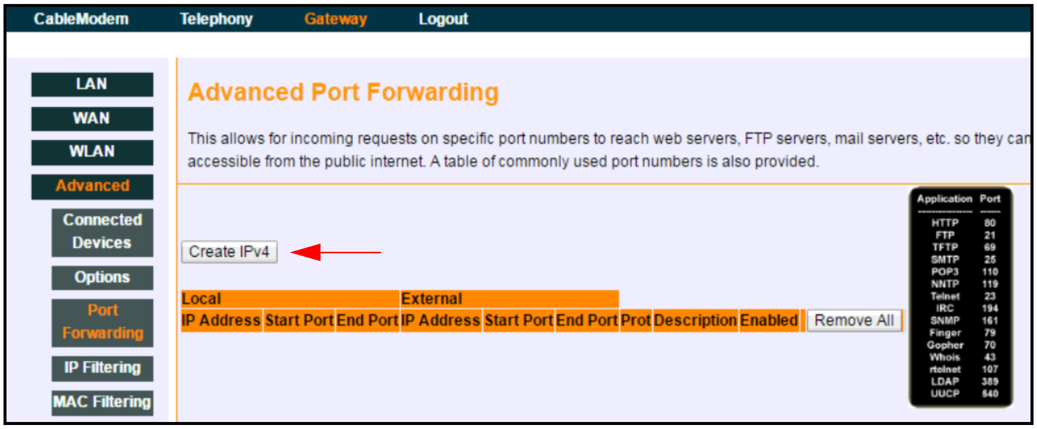
You need the following information to set up port forwarding:

- **IP address** of each local host system (for example, Xbox) for which you need to setup a port forwarding rule.
- **Port numbers** the local host's application listens to for incoming requests/data (for example, a game or other service). These port numbers should be available in the documentation associated with the application.

NOTE: For detailed information on port forwarding, including how to set it up for specific applications using specific network devices (for example, cable modems), refer to: http://portforward.com or consult your host device or application user manual.

To set up port forwarding:

1. On the Port Forwarding screen, click **Create IPv4**.



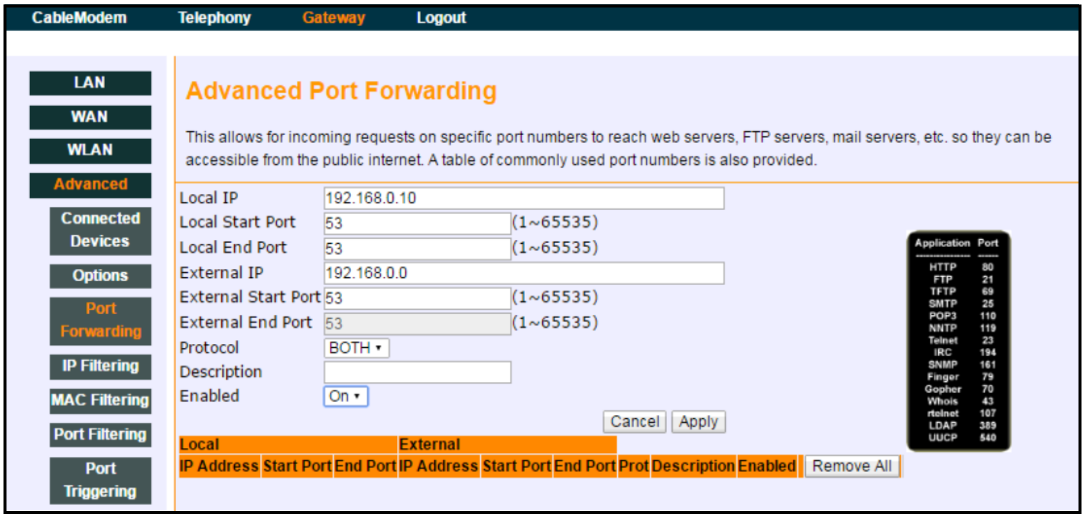
Advanced Port Forwarding

This allows for incoming requests on specific port numbers to reach web servers, FTP servers, mail servers, etc. so they car 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

2. Enter information in the forwarding fields as shown in the screen shot below. Field descriptions follow.



Advanced Port 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.

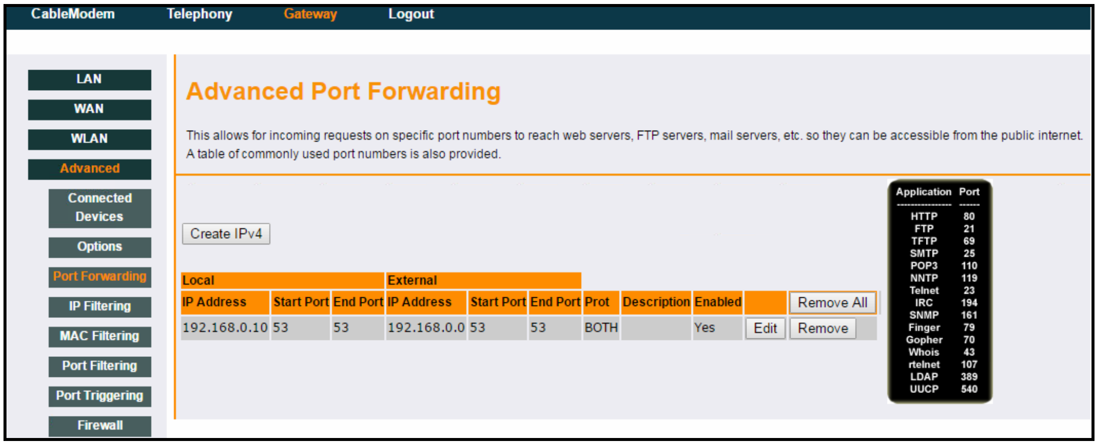
Local IP	192.168.0.10	
Local Start Port	53	(1~65535)
Local End Port	53	(1~65535)
External IP	192.168.0.0	
External Start Port	53	(1~65535)
External End Port	53	(1~65535)
Protocol	BOTH ▾	
Description		
Enabled	On ▾	

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

Label	Description
Local IP	Defines the IP address of the local LAN device to which the forwarding rule applies. For example, an Xbox or PC.
Local Start Port	Defines the starting port number listened to by the server host located in your LAN.
Local End Port	Defines the ending port number listened to by the server host located in your LAN.
External IP	Designates another router's IP address on the network through which to forward data.
External Start Port	Defines the port number to start the range of ports to publish to the Internet.
External End Port	Defines the port number to end the range of ports published to Internet. **Note:** Be very careful with ranges. Ports within a range are not usable by other applications that may require them. It is common and safer to enter the same port number as the start and end of the range.
Protocol	Selects the protocol type. Options are UDP, TCP, or BOTH.
Description	Specifies the forwarding rule name.
Enabled	Disables (Off) or enables (On) the forwarding rule.
Cancel	Stops the forwarding rule creation process and returns you to the previous Forwarding screen.
Apply	Saves changes.
Port Map	Shows a list of common applications and their ports.
Forwarding Table – Lists existing forwarding rules.	
Remove All	Deletes all entries in the forwarding table.

3. Click **Apply**. The forwarding rule is created and displayed in the table as shown below. Additional field descriptions follow.



Advanced Port 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	Remove All
192.168.0.10	53	53	192.168.0.0	53	53	BOTH		Yes	Edit Remove

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

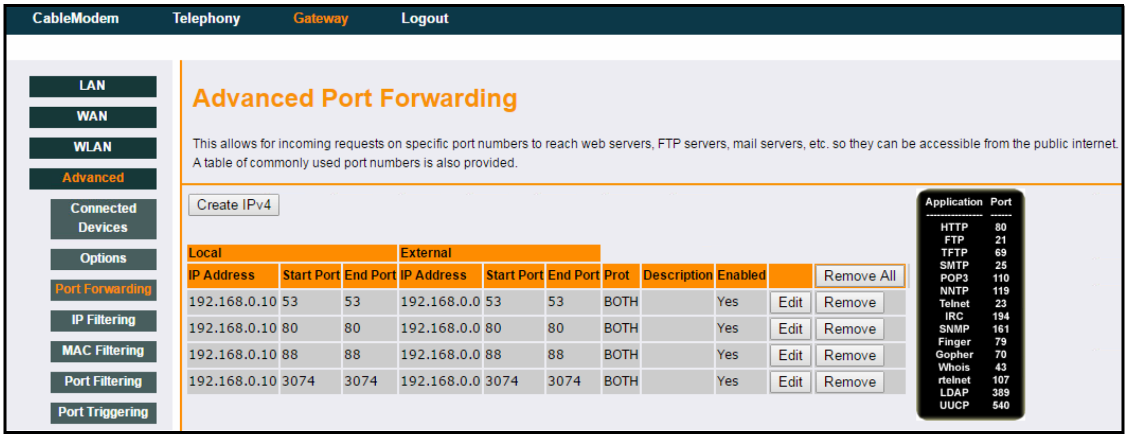
Label	Description
Remove All	Deletes all entries in the forwarding table.
Edit	Displays fields for the rule selected in order to change values.
Remove	Deletes the selected rule.

6.4.3.3 Setting Up Port Forwarding for an Xbox Example

The following is an example of how you would set up a single Xbox running Modern Warfare 2. Since multiple ports are used for the Xbox and the Modern Warfare 2 game, a separate forwarding rule is set for each port. Multiple ports and forwarding rules may not be required for other applications.

To set up port forwarding for an Xbox:

1. Click **Gateway** from the main menu.
2. Click **Advanced** from the left side menu.
3. Click **Port Forwarding** from the sub-menu.
4. Enter the Xbox IP address in the **Local IP** field.
5. Define ports used by the Xbox in the **Local Start Port** and **Local End Port** fields. Define the same ports used by the Xbox in the **External Start Port** and **External End Port** fields.
6. Create Port Forwarding rules per port. A rule set up for port 53 works for port 53. A port can be used only by one program at a time.



Advanced Port 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		Remove All
192.168.0.10	53	53	192.168.0.0	53	53	BOTH		Yes	Edit	Remove
192.168.0.10	80	80	192.168.0.0	80	80	BOTH		Yes	Edit	Remove
192.168.0.10	88	88	192.168.0.0	88	88	BOTH		Yes	Edit	Remove
192.168.0.10	3074	3074	192.168.0.0	3074	3074	BOTH		Yes	Edit	Remove

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

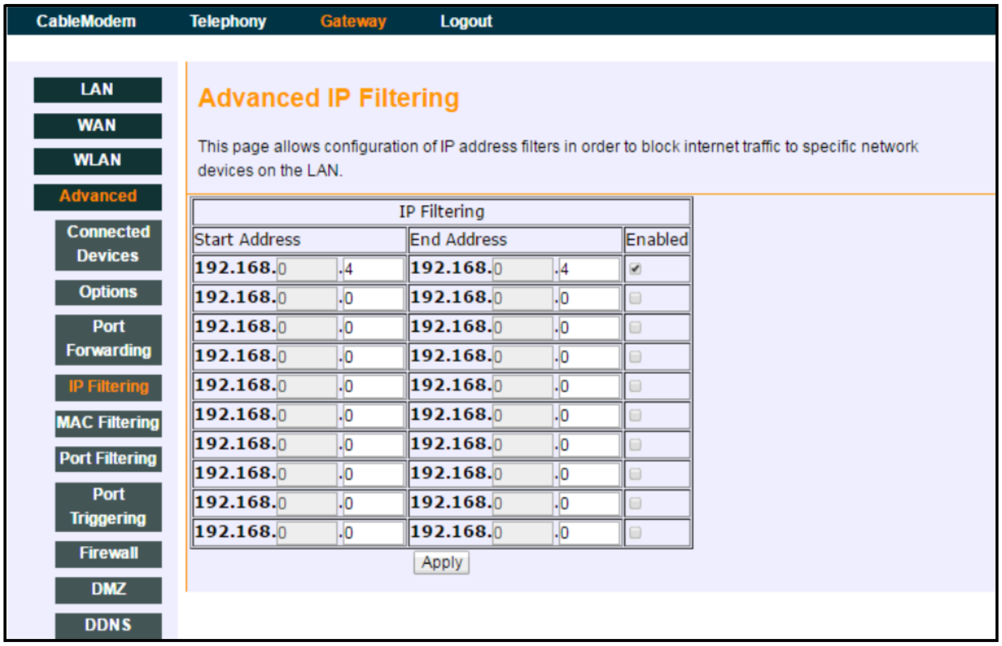
NOTE: You can set up applications/services to listen on one internal port. External Internet users who want to access that application, address it using an external port, such as an Audio server. Internal Ports are the ports to which local servers listen. External Ports are the ports that the cable modem listens to from the WAN.

6.4.4 Using the IP Filtering Option

Use the **IP Filtering** option to filter IP addresses to block Internet traffic to specific network devices on the LAN. Any host on this list is not accessible to Internet traffic.

NOTE: You may also filter by the MAC address which does not require setting a static lease. Refer to Using the MAC Filtering Option on page 59.

Field descriptions are listed below the screen example.



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 .4	192.168.0 .4	☑
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	☐

Label	Description
Start Address	Defines the starting IP address to block.
End Address	Defines the ending IP address to block.
Enabled	Activates the rule when enabled is checked.
Apply	Saves changes.

6.4.5 Using the MAC Filtering Option

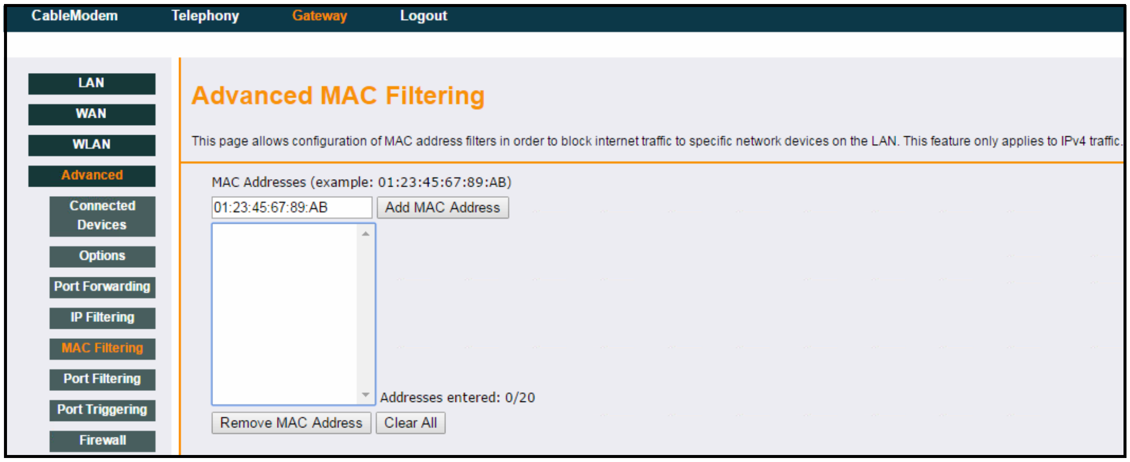
The **MAC Filtering** option allows you to filter MAC addresses to block Internet traffic from specific network devices on the LAN. MAC filtering establishes a list and any host on this list is not able to access the network through the EVW32C.

1. Note the MAC addresses of the devices that you want to deny Internet access.

   Be sure all devices to which you potentially deny Internet access are connected to the EVW32C network.

2. Enter the MAC address to block in the text box to the left of the **Add MAC Address** button.

3. Click the **Add MAC Address** button. The MAC address is displayed in the filtered MAC address list. Field descriptions are listed below the screen example.



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)

01:23:45:67:89:AB

Addresses entered: 0/20

Label	Description
MAC Addresses	Specifies the MAC address to block. Enter the MAC address in the field.
Add MAC Address	Adds a MAC address to the list of addresses to block.
Addresses entered: n/20	Displays the MAC addresses to be blocked. The number of MAC addresses entered is shown as 1/20 where 1 is the number of addresses in the list. You can filter up to twenty MAC addresses at one time.
Remove MAC Address	Deletes the selected MAC address from the list of addresses to be blocked.
Clear All	Removes all MAC addresses from the list.

6.4.6 Using the Port Filtering Option

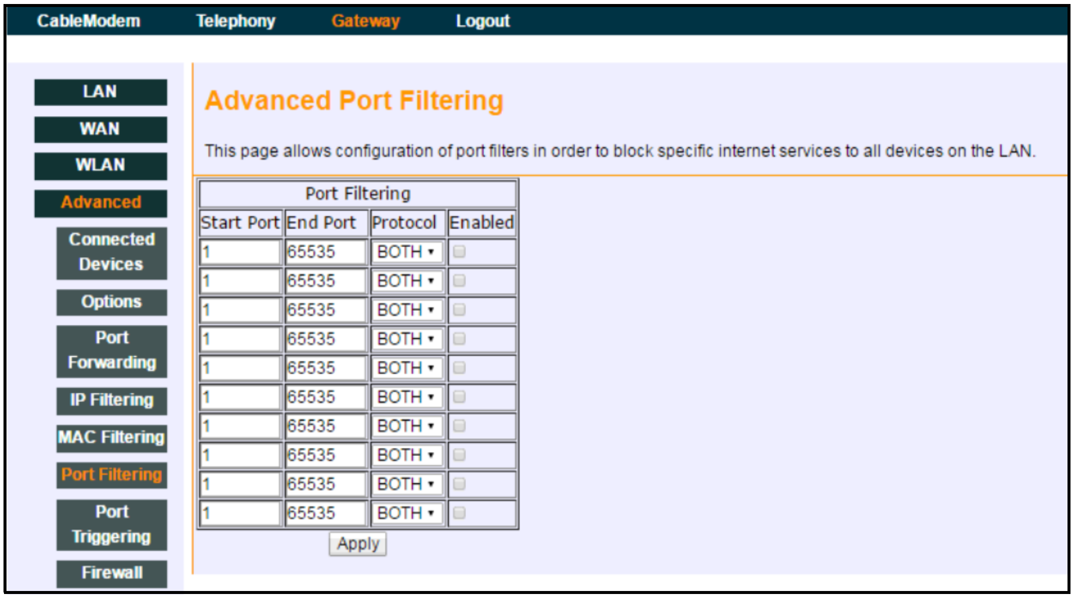
Use the **Port Filtering** option to configure port filters to block to all devices on the LAN Internet services that use the ports specified.

For example:

To prevent all Telnet access into and across your LAN:

1. Enter the **Start** and **End** ports to be 23.
2. Select **Both** for Protocol to include TCP and UDP.
3. Check **Enabled**.
4. Click **Apply**. Field descriptions are listed below the screen example.

NOTE: Use caution when assigning port filtering by port range. You may accidentally prevent traffic that should pass through your network, such as http or email. Pre-assigned application ports are displayed on the Forwarding screen. Refer to Using the Port Forwarding Option on page 54.



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 ▾	☐

Label	Description
Start Port	Defines the starting port number
End Port	Defines the ending port number.
Protocol	Selects the protocol type. Options are UDP, TCP, or Both.
Enabled	Activates the rule and filters out all traffic on the specified ports.
Apply	Saves changes.

6.4.7 Using the Port Triggering Option

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

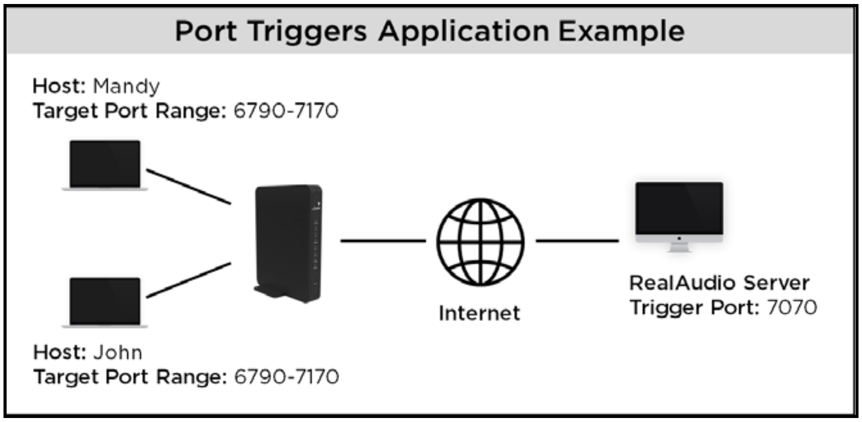
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. The difference between port forwarding and triggering is:

- Port forwarding sets a rule to send a service to a single LAN IP address.
- Port triggering defines two kinds of ports: trigger port and target port. The trigger port sends a service request from a LAN host to a specific destination port number. The port the LAN host is required to listen to by the application is called the target port. The server returns responses to these ports.

For example:

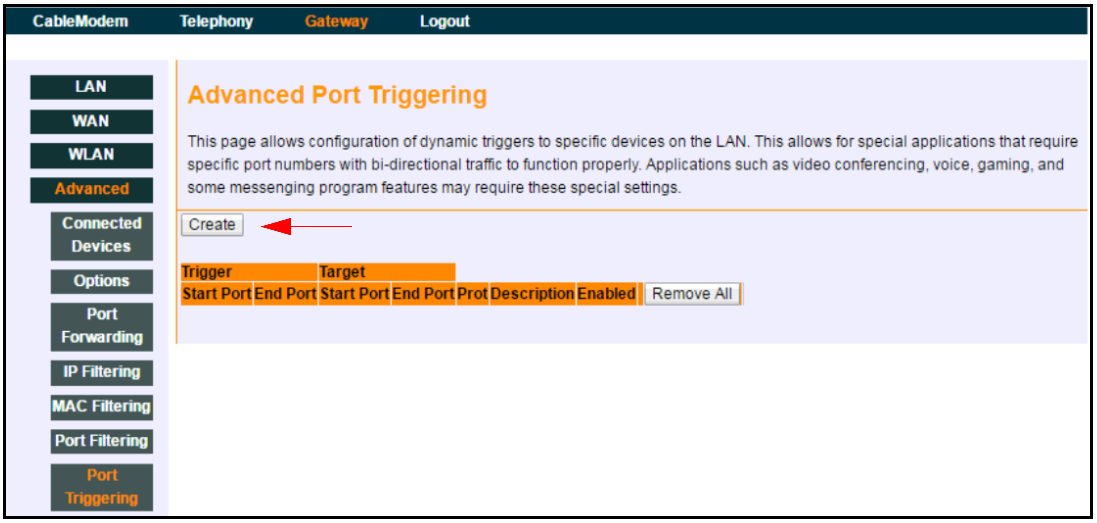
1. John requests a file from the Real Audio server (port 7070). Port 7070 is a “trigger” port and causes the device to record John’s computer IP address. The EVW32C associates John's computer IP address with the “target” port range of 6970-7170.
2. The Real Audio server responds to a port number ranging between 6970-7170.

3. The EVW32C forwards the traffic to John’s computer IP address.
4. Only John can connect to the Real Audio server until the connection is closed or expires.


Port Triggers Application Example
Host: Mandy
Target Port Range: 6790-7170
Internet
RealAudio Server
Trigger Port: 7070
Host: John
Target Port Range: 6790-7170

To set up port Triggering:

1. On the Port Triggering screen, click **Create**.

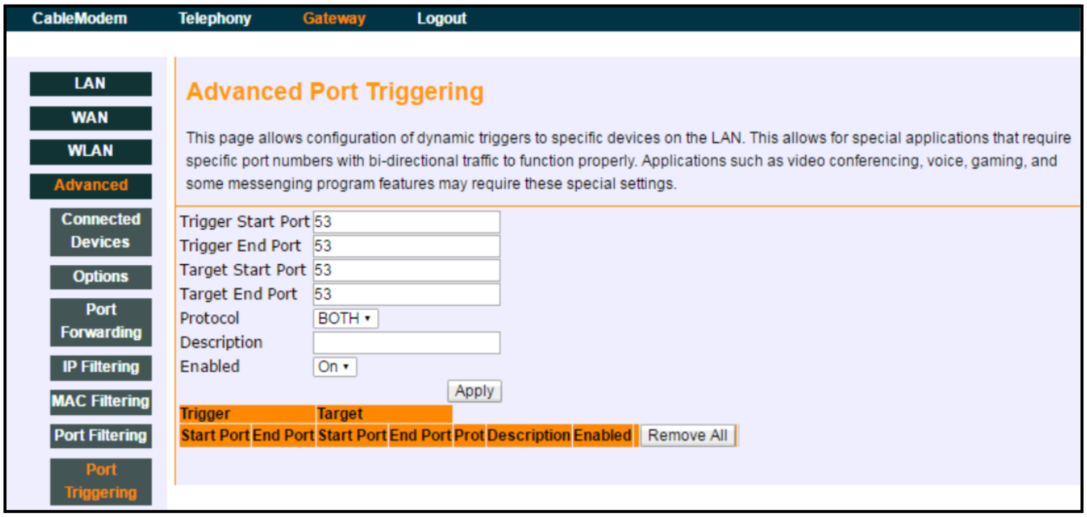


Advanced Port Triggering

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

2. Enter information in the forwarding fields as shown in the screen shot below. Field descriptions follow.



Advanced Port Triggering

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.

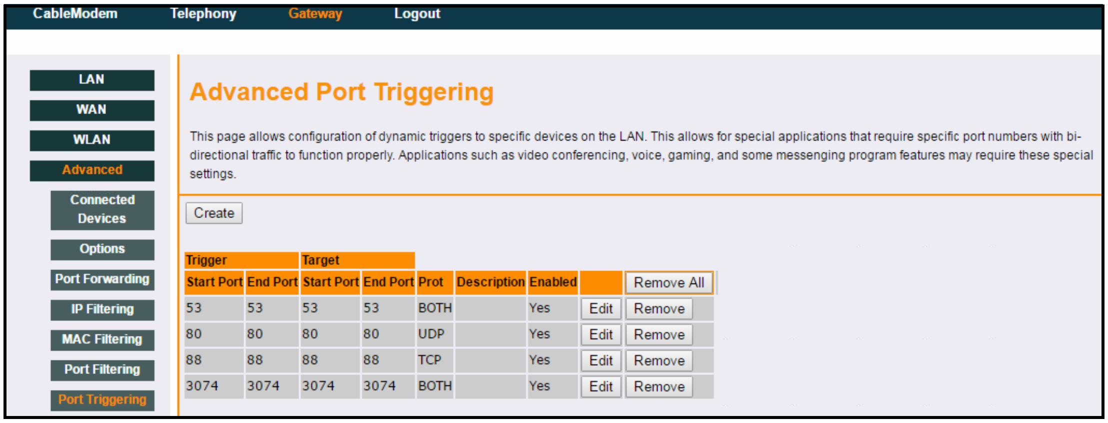
Trigger Start Port	53
Trigger End Port	53
Target Start Port	53
Target End Port	53
Protocol	BOTH ▾
Description	
Enabled	On ▾

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

Label	Description
Trigger Start Port	Allows you to enter a port number or the starting port number in a range of port numbers.
Trigger End Port	Allows you to enter a port number or the ending port number in a range of port numbers.
Target Start Port	Allows you to enter a port number or the starting port number in a range of port numbers.
Target End Port	Allows you to enter a port number or the ending port number in a range of port numbers.
Protocol	Allows you to enter the protocol type for this rule: UDP, TCP, or BOTH.
Description	Allows you to enter a name for the triggering rule.
Enabled	Disables (Off) or enables (On) the triggering rule.
Apply	Saves changes.
Remove All	Deletes all entries in the forwarding table.

3. Click **Apply**. The triggering rule is created and displayed in the table as shown below. Additional field descriptions follow.

The following example shows the Port Triggering option set up for a dual Xbox configuration.



Advanced Port Triggering

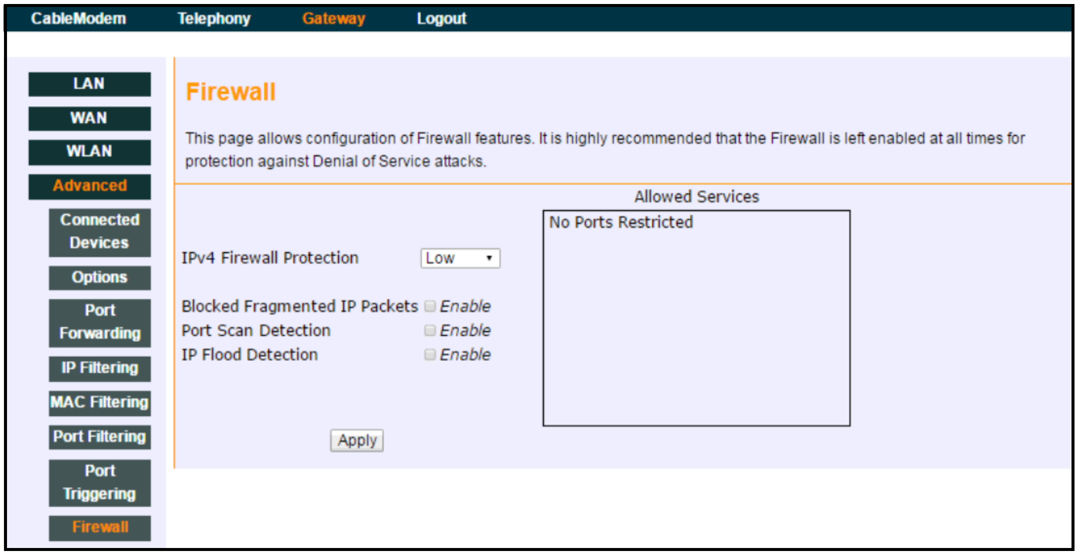
This page allows configuration of dynamic triggers to specific devices on the LAN. This allows for special applications that require specific port numbers with bi-directional traffic to function properly. Applications such as video conferencing, voice, gaming, and some messenging program features may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

Trigger		Target						
Start Port	End Port	Start Port	End Port	Prot	Description	Enabled		
53	53	53	53	BOTH		Yes	Edit	Remove
80	80	80	80	UDP		Yes	Edit	Remove
88	88	88	88	TCP		Yes	Edit	Remove
3074	3074	3074	3074	BOTH		Yes	Edit	Remove

Label	Description
Remove All	Deletes all entries in the forwarding table.
Edit	Displays fields for the rule selected in order to change values.
Remove	Deletes the selected rule.

6.4.8 Using the Firewall Option

Use these instructions to configure the EVW32C firewall settings to control what types of traffic are allowed on your network. The firewall can block certain Web-oriented cookies, Java scripts, and pop-up windows. It is highly recommended the Firewall is left enabled at all times to protect against denial of service (DoS) attacks.



Firewall

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.

IPv4 Firewall Protection: Low

Blocked Fragmented IP Packets □ Enable
Port Scan Detection □ Enable
IP Flood Detection □ Enable

Allowed Services
No Ports Restricted

Label	Description
IPv4 Firewall Protection	Defines the level of IPv4 protection. Choices are Off, Low, Medium, and High. The default is Low. Services are based on the protection level and displayed in the Allowed Services window.
Blocked Fragmented IP Packets	Detects fragmented IP packets and blocks them.
Port Scan Detection	Detects port scans that probe for available ports and potentially use these ports to detect weakness in the network.
IP Flood Detection	Detects IP flood attacks that send excessive information to the device, using up bandwidth.
Apply	Saves changes.

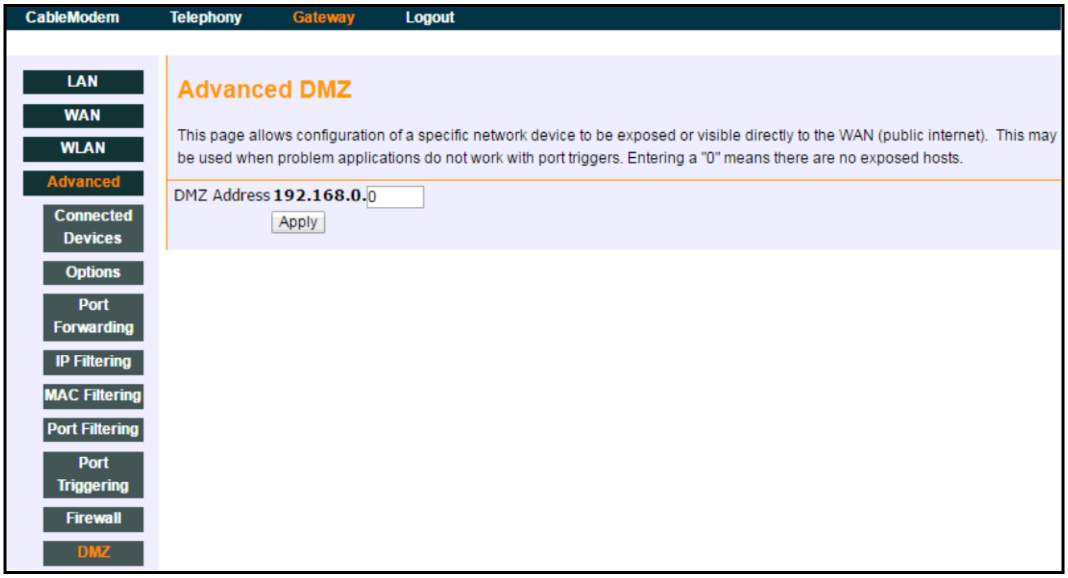
6.4.9 Using the DMZ Option

Use the DMZ (demilitarized zone) option to expose a host IP address to the WAN (public Internet). Putting a host in the DMZ outside the firewall is a quick and easy way to enable remote access and functionality of devices such as home routers, web cameras, VoIP phones, gaming consoles and other such devices without having to set up more complicated port forwarding or port triggering configurations.

To set up a DMZ host

1. Connect a PC to an Ethernet port on the EVW32C. Make sure both devices are powered on and functioning.
2. Connect a home gateway (or other device you wish to be in the DMZ) to an Ethernet port on the EVW32C.
3. Log in to the EVW32C Web user interface.
4. Click **Gateway** from the main menu.
5. Click **Advanced** from the left side menu.
6. Click **DMZ** under the Advanced options.
7. Enter the IP address of the home gateway or other device you wish to be exposed to the WAN.
8. Test the device to ensure Internet access is available and the device is functional. For example, connect to the Internet from a PC connected to the home gateway, or make a call from a VoIP phone.

Field descriptions follow the screen sample below.



Advanced DMZ

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.

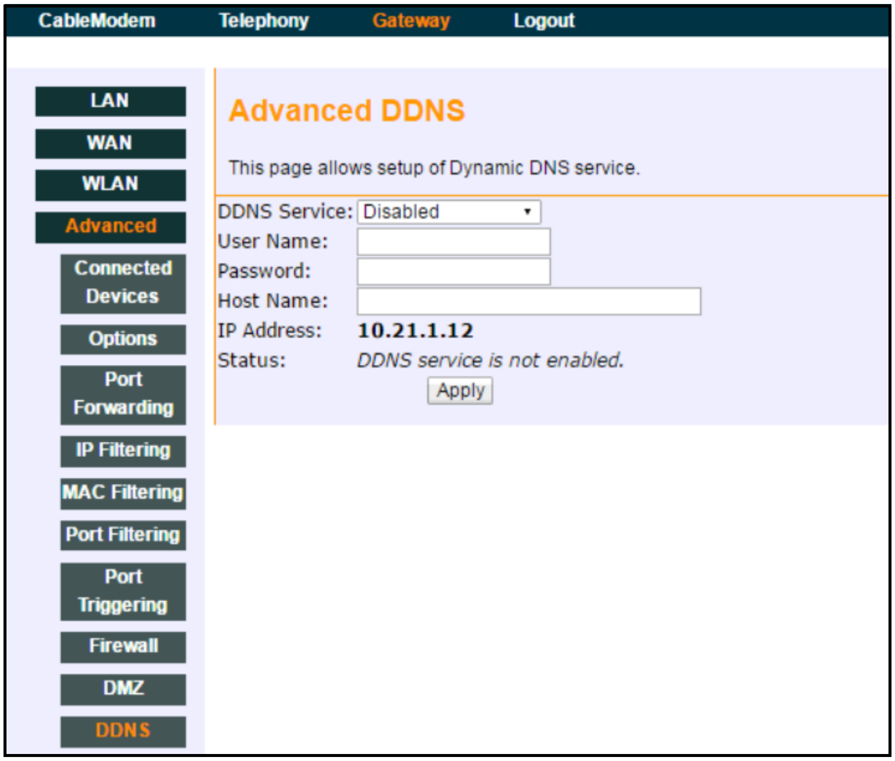
DMZ Address 192.168.0.0

Label	Description
DMZ Address	Defines the IP address of the host device to be exposed to the WAN.
Apply	Saves changes.

6.4.10 Using the DDNS Option

Use the dynamic domain name system (DDNS) to assign a changing IP address to a constant, pre-defined host name. The host can then be contacted by other hosts on the Internet, even if its IP address changes.

The DDNS service for the EVW32C Advanced Wireless Voice Gateway is provided through a third-party and can be purchased from Dynamic Network Services Inc. at www.dynDNS.com.



Advanced DDNS

This page allows setup of Dynamic DNS service.

DDNS Service: Disabled
User Name:
Password:
Host Name:
IP Address: 10.21.1.12
Status: *DDNS service is not enabled.*

Label	Description
DDNS Service	Allows you to enable or disable DDNS service. When enabled, this service is available from www.dynDNS.org.
User Name	Allows you to enter the user name for the DDNS account.
Password	Enter the password for the DDNS account.
Host Name	Allows you to enter a host name for the DDNS account.

Label	Description
IP Address	Displays the IP address for the DDNS account.
Status	Displays if the DDNS service is enabled or disabled.
Apply	Saves changes.

6.5 Using the Management Option

The Management menu allows you to backup the EVW32C configuration and restore the gateway to a previously saved configuration.

To access the management menu:

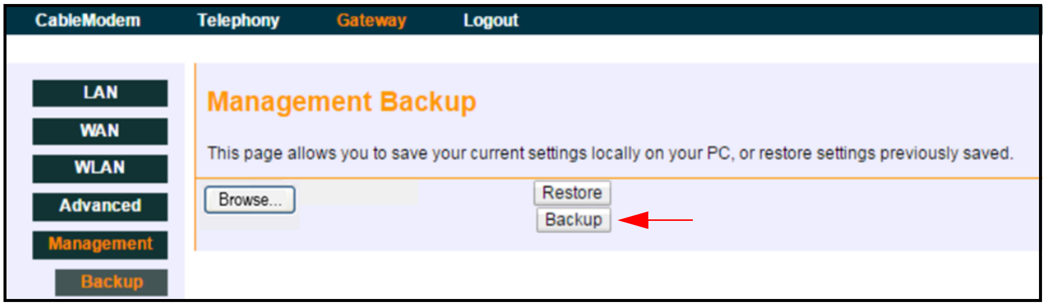
1. Click **Gateway** from the main menu.
2. Click **Management** from the left side menu.
3. The following sub-menu is available for selection:
   - Backup

6.5.1 Using the Backup Option

The Backup option let's you back up your device configuration or restore the EVW32C to a previously saved configuration.

6.5.1.1 Backing Up the Current Modem Configuration

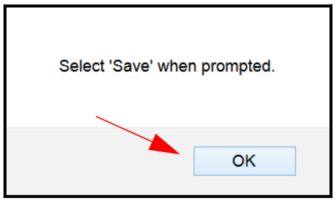
To backup and save the current modem configuration, click the **Backup** button.



Management Backup

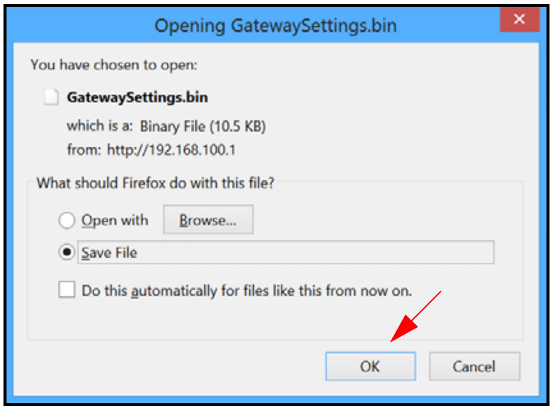
This page allows you to save your current settings locally on your PC, or restore settings previously saved.

A pop-up window appears instructing you to select 'Save' when prompted. Click '**OK**.'



Select 'Save' when prompted.

The following window appears, giving you the option to save the file. Click the ‘**Save File**’ option and click ‘**OK**’.


Opening GatewaySettings.bin

You have chosen to open:

GatewaySettings.bin

which is a: Binary File (10.5 KB)
from: http://192.168.100.1

What should Firefox do with this file?

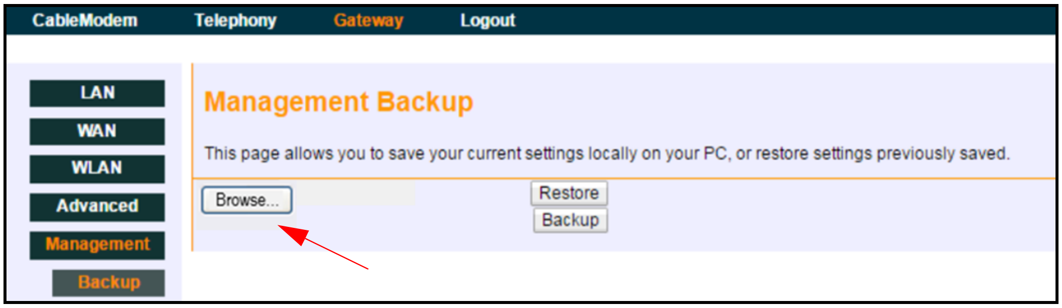
○ Open with
● Save File

□ Do this automatically for files like this from now on.

The file will be saved to your Downloads folder as a binary file (.bin) titled ‘GatewaySettings.bin.’

6.5.1.2 Restoring the EVW32C to a Previously Saved Configuration

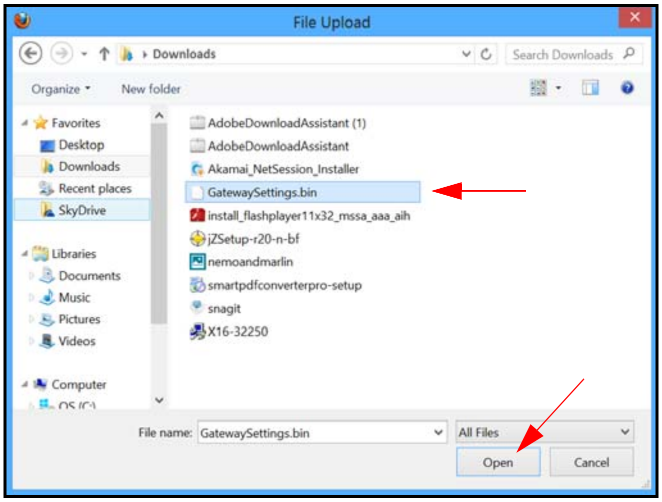
To restore the device to a previously saved configuration, click the **Browse** button.



Management Backup

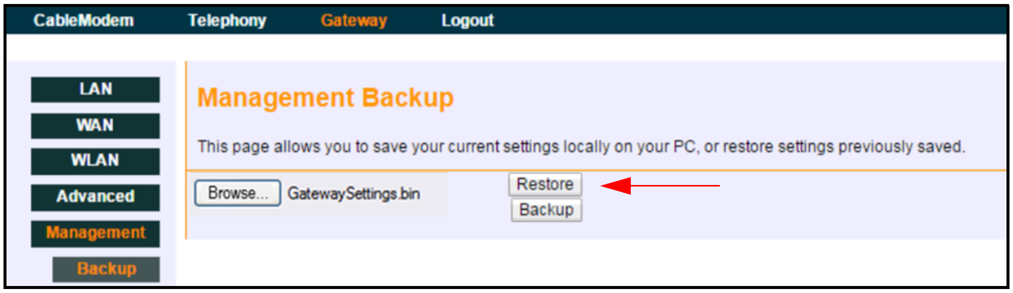
This page allows you to save your current settings locally on your PC, or restore settings previously saved.

The File Upload dialog box appears and allows you to select the previously saved backup file. Highlight the file and click ‘**Open**.’



File name: GatewaySettings.bin

The location for the backed up file appears to the right of the Browse button. Click the **Restore** button.

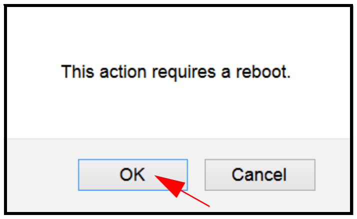


Management Backup

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

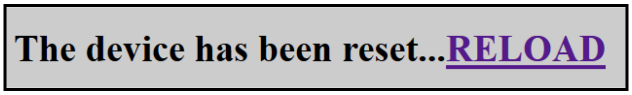
GatewaySettings.bin

You are advised that you will be required to reboot the device. Click ‘**OK**.’



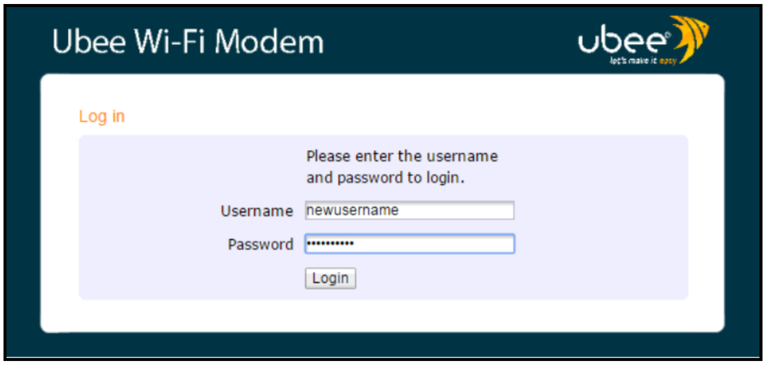
This action requires a reboot.

You are then notified that the device has been reset. Click ‘**RELOAD**’.



The device has been reset...RELOAD

You are then presented with the login screen for the EVW32C. Enter the username and password to return to the modem User Interface.



Please enter the username and password to login.

Username newusername

Password ••••••••••

6.6 Using the VPN Option

Use the VPN menu to configure virtual private tunnels (VPNs) for the EVW32C.

A VPN is a computer network that carries links between nodes by open connections over the Internet or virtual circuits instead of by physical wires. A common use of a VPN is when you want to connect to a computer at a remote location, such as from a branch office to a corporate office to share private data.

- ❑ **Internet Protocol Security (IPsec)** – A standards-based protocol suite used to secure IP communications. IPsec operates in the Internet layer (TCP/IP) to authenticate and encrypt each IP packet in a communication session.
- ❑ **VPN Tunnel** – A way to transmit data through a public network intended for use in a private network. Data is transmitted so that the routing points on the public network are unaware the transmission is part of a private network.

A VPN tunnel is established in two phases:

- ♦ Phase One – Establish an Internet key exchange (IKE) security association (SA) between the device and the remote IPsec router.
- ♦ Phase Two – Use the IKE SA to establish an IPsec SA through which the device and the remote IPsec router can send data securely between computers on the local and remote networks.

- ❑ **SA** – A security association is a contract that indicates what security parameters the device and the remote IPSec router use for each phase. An SA is the foundation of an IPsec VPN configuration.
- ❑ **IPsec Algorithms** – The AH and ESP protocols provide the authentication used to create a security association. Once the SA is established, you can begin to transport data securely.
  - ♦ **AH** – The authentication header protocol (RFC 2402) is designed for integrity, authentication, and resisting replays. In applications where confidentiality is not required or not sanctioned by government encryption restrictions, an AH can be used to ensure integrity. AH verifies information integrity and authenticates the originator, but does not protect against dissemination.

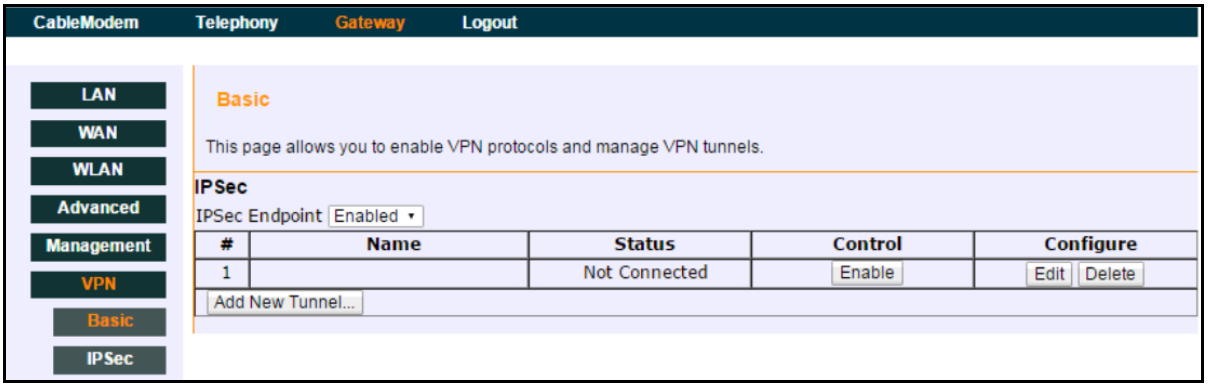
- **ESP** – The encapsulating security payload protocol (RFC 2406) provides encryption, as well as the services offered by AH. ESP authenticating properties do not include IP header information during the authentication process, whereas the AH protocol does. ESP is sufficient if only the upper layer protocols need to be authenticated. ESP also features payload padding which conceals the size of the packet being transmitted to further protect communications.

To configure VPN options:

1. Click **Gateway** from the main menu.
2. Click **VPN** from the left side menu.
3. The following sub-menu items are available for selection:
   - Basic
   - IPsec

6.6.1 Using the Basic Option

The **Basic** option displays an overview of the VPN settings. From this screen you can access configuration options for the selected VPN tunnel. Field descriptions are listed below the screen example.



Basic

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

IPSec

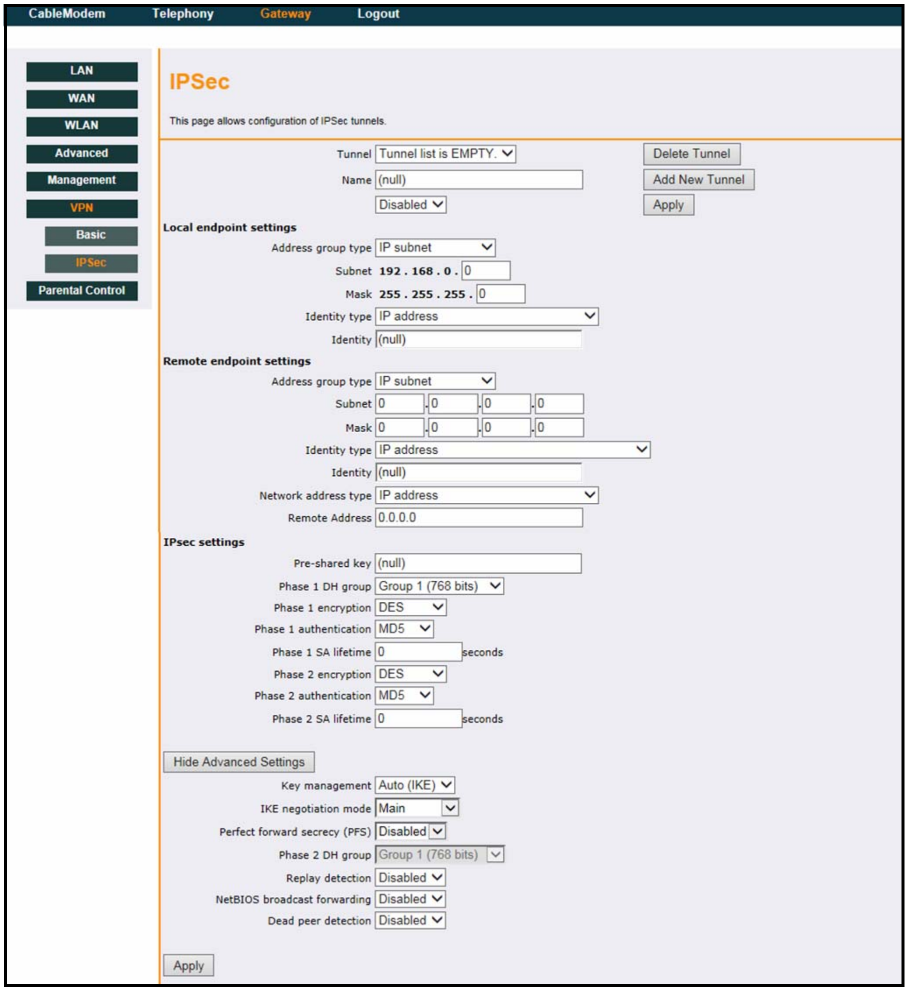
IPSec Endpoint Enabled

#	Name	Status	Control	Configure
1		Not Connected	Enable	Edit Delete

Label	Description
IPsec Endpoint	Enables or Disables Internet protocol security (IPsec) for the VPN service.
#	Displays an ID number for existing IPsec VPN tunnels.
Name	Displays the name of the IPsec VPN tunnel.
Status	Displays the status of the IPsec. Once an IPsec VPN connects successfully, the Status is Connected. Otherwise, it is set to Not connected.
Control	Displays when the user manually triggers an IPsec VPN connection request to the remote VPN gateway.
Configure	Allows you to edit or delete the IPsec configuration. ♦ **Edit** – Allows you to modify IPsec VPN parameters of this tunnel. ♦ **Delete** – Allows you to remove this IPsec VPN tunnel.
Add New Tunnel	Creates a new IPsec VPN tunnel and adds it to the IPsec list. Click **Edit** to modify its parameters.

6.6.2 Using the IPsec Option

The **IPsec** option allows you to configure a complete VPN. Field descriptions are listed below the screen example.



IPSec

This page allows configuration of IPSec tunnels.

Tunnel: Tunnel list is EMPTY.
Name: (null)
Disabled

Local endpoint settings

Address group type: IP subnet
Subnet: 192 . 168 . 0 . 0
Mask: 255 . 255 . 255 . 0
Identity type: IP address
Identity: (null)

Remote endpoint settings

Address group type: IP subnet
Subnet: 0 . 0 . 0 . 0
Mask: 0 . 0 . 0 . 0
Identity type: IP address
Identity: (null)
Network address type: IP address
Remote Address: 0.0.0.0

IPsec settings

Pre-shared key: (null)
Phase 1 DH group: Group 1 (768 bits)
Phase 1 encryption: DES
Phase 1 authentication: MD5
Phase 1 SA lifetime: 0 seconds
Phase 2 encryption: DES
Phase 2 authentication: MD5
Phase 2 SA lifetime: 0 seconds

Key management: Auto (IKE)
IKE negotiation mode: Main
Perfect forward secrecy (PFS): Disabled
Phase 2 DH group: Group 1 (768 bits)
Replay detection: Disabled
NetBIOS broadcast forwarding: Disabled
Dead peer detection: Disabled

Label	Description
Tunnel	Lists the number of the VPN tunnels available to edit. If no tunnels exist, the list shows, Tunnel list is EMPTY.
Name	Displays the name for the tunnel.
Enabled/Disabled	Enables or disables the VPN tunnel.
Delete Tunnel	Removes the selected VPN tunnel.
Add New Tunnel	Adds the new tunnel after a name is entered.
Apply	Enables or Disables the tunnel when you click Apply to save your changes.
Local endpoint settings	

Label	Description
Address group type	Configures the local network that will be protected by the IPsec VPN located on your device's LAN side. Choose the local address type: ♦ IP Subnet, to protect the whole subnet (default setting). ♦ Single IP address, to protect a single PC. ♦ IP address range, to protect several PCs.
Subnet	Defines the subnet.
Mask	Defines the subnet mask.
Identity type	Defines the identity type for this device: ♦ Automatically use WAN IP address ♦ IP address (default setting) ♦ Fully qualified domain name (FQDN) ♦ Email address (USER FQDN) In Main mode (see IKE negotiation mode on page 75), the identity type and content are encrypted to provide identity protection. The VPN concentrator can distinguish up to 30 different incoming SAs that have dynamic WAN IP addresses and connect from remote IPsec routers. You can select between five encryption algorithms (DES, 3DES, AES-128, AES-192 and AES-256), two authentication algorithms (MD5 and SHA1) and three key groups (DH1 and DH2, DH5) when you configure a VPN rule. The identity type and content act as an extra level of identification for incoming SAs. In Aggressive mode (see IKE negotiation mode on page 75), the VPN concentrator identifies incoming SAs by identity type and content (which are not encrypted) to distinguish between multiple rules for SAs that connect from remote IPsec routers that have dynamic WAN IP addresses.
Identity	Defines the value corresponding to the selected Identity type.
Remote endpoint settings	
Address group type	Defines the address group type: ♦ IP Subnet – protects the entire subnet. ♦ Single IP address – protects a single PC. ♦ IP address range – protects several PCs.
Subnet	Defines the subnet.
Mask	Defines the subnet mask.
Identity type	Defines the identity type to identity this device by: ♦ Automatically use WAN IP address ♦ IP address ♦ Fully qualified domain name (FQDN) ♦ Email address (USER FQDN)
Identity	Defines the value corresponding to the selected identity type.
Network address type	Defines the network address type: ♦ IP address, usually suitable for static public IP address (default setting). ♦ Fully Qualified Domain Name (FQDN), usually suitable for dynamic public IP address.

Label	Description
Remote address	Identifies the specific remote IPsec VPN gateway to which your device will initiate the IPsec VPN connection: ♦ Use the IP address value when an IP address is the Network Address Type. ♦ Use the FQDN if FQDN is selected.
IPsec settings	
Pre-shared key	Defines your pre-shared key. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called “pre-shared” because you have to share it with the other party before you can communicate with them over a secure connection.
Phase 1 DH group	Defines which Diffie-Hellman key group (DH*x*) you want to use for encryption keys: ♦ **DH1** – a 768-bit random number (default setting) ♦ **DH2** – a 1024-bit random number ♦ **DH5** – a 1536-bit random number
Phase 1 encryption	Defines which key size and encryption algorithm to use for data communications: ♦ **DES** – a 56-bit key with the DES encryption algorithm (default setting). ♦ **3DES** – a 168-bit key with the DES encryption algorithm. The EVW32C and the remote IPsec router must use the same algorithms and key, used to encrypt and decrypt the messages or to generate and verify a message authentication code. Longer keys require more processing power, resulting in increased latency and decreased throughput. ♦ **AES** – the Advanced Encryption Standard method of data encryption also uses a secret key. This implementation of AES applies a 128-bit key to 128-bit blocks of data. AES is faster than 3DES. You can choose **AES-128, AES-192, AES-256**.
Phase 1 authentication	Defines which hash algorithm to use to authenticate packet data in the IKE SA. ♦ **MD5** (message digest 5) produces a 128-bit digest to authenticate packet data (default setting). ♦ **SHA1** (secure hash algorithm) produces a 160-bit digest to authenticate packet data. SHA1 is generally considered stronger than MD5, but it is also slower.
Phase 1 SA lifetime	Defines the length of time (from 120 to 86400 seconds) before an IKE SA process renegotiates a key. A short SA lifetime increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates the keys, remote users are temporarily disconnected.
Phase 2 encryption	Defines the key size and encryption algorithm to use for data communications: ♦ **DES** – A 56-bit key with the DES encryption algorithm (default setting). ♦ **3DES** – A 168-bit key with the DES encryption algorithm device and the remote IPsec router must use the same algorithms and key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. Longer keys require more processing power, resulting in increased latency and decreased throughput. ♦ **AES** – The advanced encryption standard method of data encryption also uses a secret key. This implementation of AES applies a 128-bit key to 128-bit blocks of data. AES is faster than 3DES. You can choose **AES-128, AES-192, AES-256**.
Phase 2 authentication	Defines the hash algorithm to use to authenticate packet data in the IKE SA. Choices are **SHA1** and **MD5** (default setting). **SHA1** is generally considered stronger than **MD5**, but it is also slower.
Phase 2 SA lifetime	Defines the length of time (from 120 to 86400 seconds) before an IPsec SA process renegotiates keys.
Advanced Settings	

Label	Description
Key management	Defines the Auto (IKE) or Manual key configuration to set up a VPN. The default setting is Auto.
IKE negotiation mode	Determines how the security association (SA) is established for each connection through IKE negotiations. The choices are: ♦ **Main Mode** – Ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). This is the default setting. ♦ **Aggressive Mode** – Eliminates several steps when the communicating parties are negotiating authentication (phase 1). Quicker than Main Mode.
Perfect forward secrecy (PFS)	Enables or disables the perfect forward secret (PFS) option. This option is disabled by default in phase 2 IPsec SA setup to provide a faster IPsec setup, but is not very secure. Select DH1, DH2 or DH5 to enable PFS.
Phase 2 DH group	Defines which Diffie-Hellman key group (DH*x*) you want to use for encryption keys: ♦ **DH1** – a 768-bit random number ♦ **DH2** – a 1024-bit random number ♦ **DH5** – a 1536-bit random number
Replay detection	Enables or disables replay detection. As VPN setup is processing, the system can be vulnerable to denial of service (DOS) attacks. The IPsec receiver can detect and reject old or duplicate packets to protect against replay attacks.
NetBIOS broadcast forwarding	Provides the option to send NetBIOS packets through the VPN connection. NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to find other computers. It may sometimes be necessary to allow NetBIOS packets to pass through VPN tunnels to allow local computers to find computers on the remote network and vice versa.
Dead peer detection	Enables or disables dead peer detection. When enabled the device is forced to periodically detect if the remote IPsec gateway is available.
Apply	Saves changes.

6.7 Using the Parental Control Option

Parental controls allow you to control Internet access for users on the EVW32C network. The parental control menu enables you to:

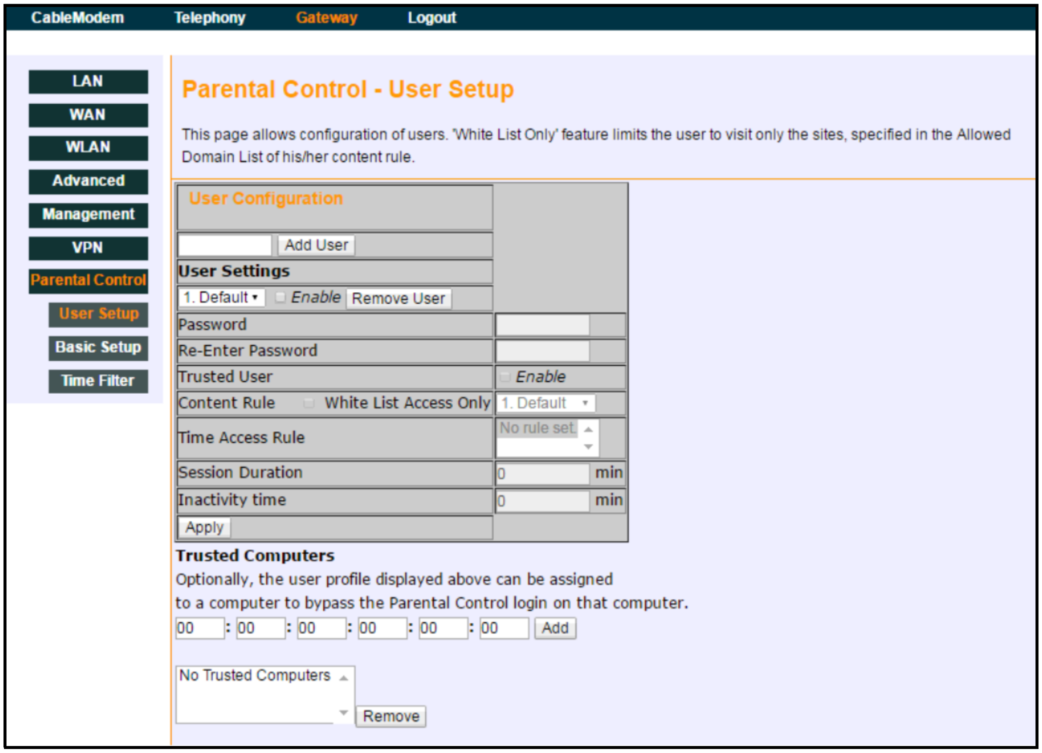
- ♦ Define username and password access
- ♦ Block specific Web sites based on keywords
- ♦ Define the days and times users are allowed to access the Internet

To access the Parental Control menu:

1. Click **Gateway** from the main menu.
2. Click **Parental Control** from the left side menu.
3. The following sub-menu items are available for selection:
    - ♦ User Setup
    - ♦ Basic Setup
    - ♦ Time Filter

6.7.1 Using the User Setup Option

The **User Setup** option allows you to configure which user accounts can or cannot connect to your wired or wireless network, and the parameters of each connection. Field descriptions are listed below the screen example.



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

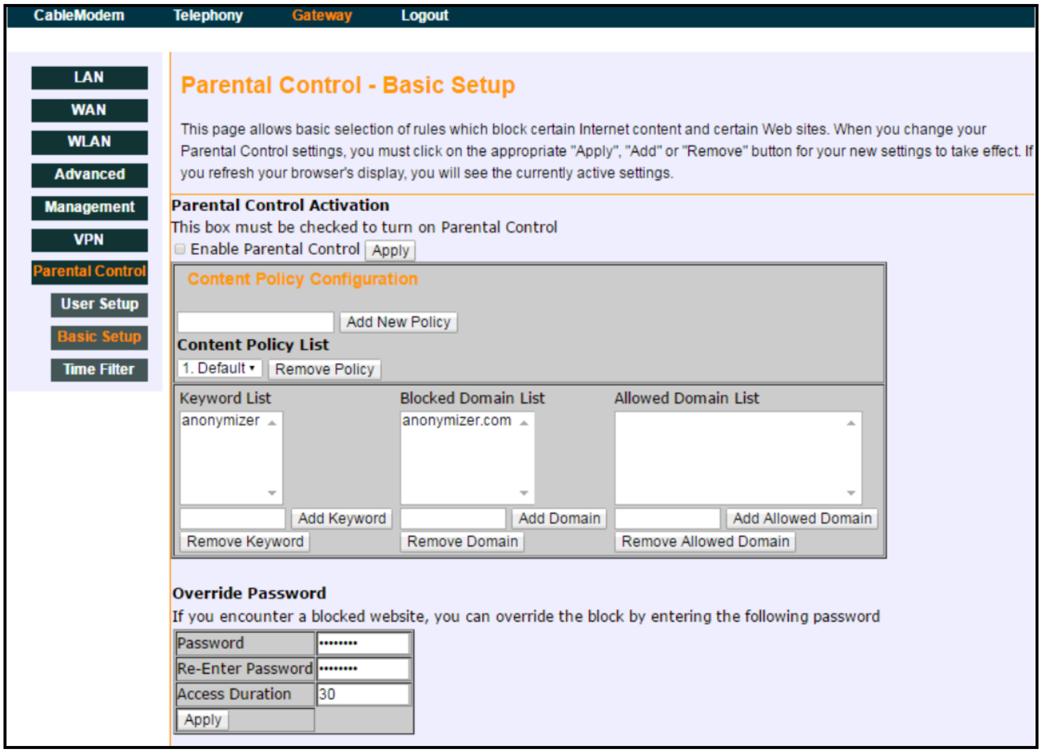
No Trusted Computers

Label	Description
User Configuration	
Add User **Remove User** **Enable**	Defines user accounts: ♦ To select an existing user, choose the user from the User Settings drop-down menu. ♦ To add a new user, enter the user name and click Add User. Note that the user name cannot contain any spaces. ♦ To activate the selected user, check Enable. ♦ To remove a user, select the user from the drop-down menu and click Remove User.
Password	Defines the password for the selected user. It is required for when the user attempts to access the Internet via the EVW32C.
Re-Enter Password	Confirm the password by re-entering it.
Trusted User	Each specified user may also be enabled as a “trusted user,” which means that person will have access to all Internet content regardless of filters that may be set up. This check box can be used as a simple override to grant a user full access while still being able to keep all of the previous settings stored and available.
Content Rule	Provides a drop-down list of existing content rules that define what kind of Websites the user can or cannot visit.

Label	Description
White List Access Only	Enables the White List Access Only option. If you have created a content rule that defines a black list and a white list, check the White List Access Only box to force the EVW32C to execute the policy for the selected user.
Time Access Rule	Selects a defined time access rule to apply to the selected user.
Session Duration	Allows you to enter a time in minutes for the user's session to expire. When the session expires, the user can log in again for the same session duration.
Inactivity Time	Allows you to enter the timeout value when a user has no activity on the Internet. When the time expires, the user interface to the Internet is canceled.
Apply	Saves all changes when clicked.
Trusted Computers	Defines the trusted hosts that can bypass the parental control process.
Add	Enter the trusted host's MAC address and click Add to enable a device as a trusted computer.
Remove	Removes a trusted computer from the list when it is highlighted and Remove is clicked.

6.7.2 Using the Basic Setup Option

The **Basic Setup** option allows you to enable parental control, and select rules to block certain Internet content and Web sites. After you change your parental control settings, click the appropriate Apply, Add or Remove buttons for your new settings to take effect. Refresh your browser's display to see the currently active settings. Field descriptions are listed below the screen example.



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 [Apply]

Content Policy Configuration

[Add New Policy]

Content Policy List

1. Default ▾ [Remove Policy]

Keyword List	Blocked Domain List	Allowed Domain List
anonymizer	anonymizer.com	
[Add Keyword]	[Add Domain]	[Add Allowed Domain]
[Remove Keyword]	[Remove Domain]	[Remove Allowed Domain]

Override Password

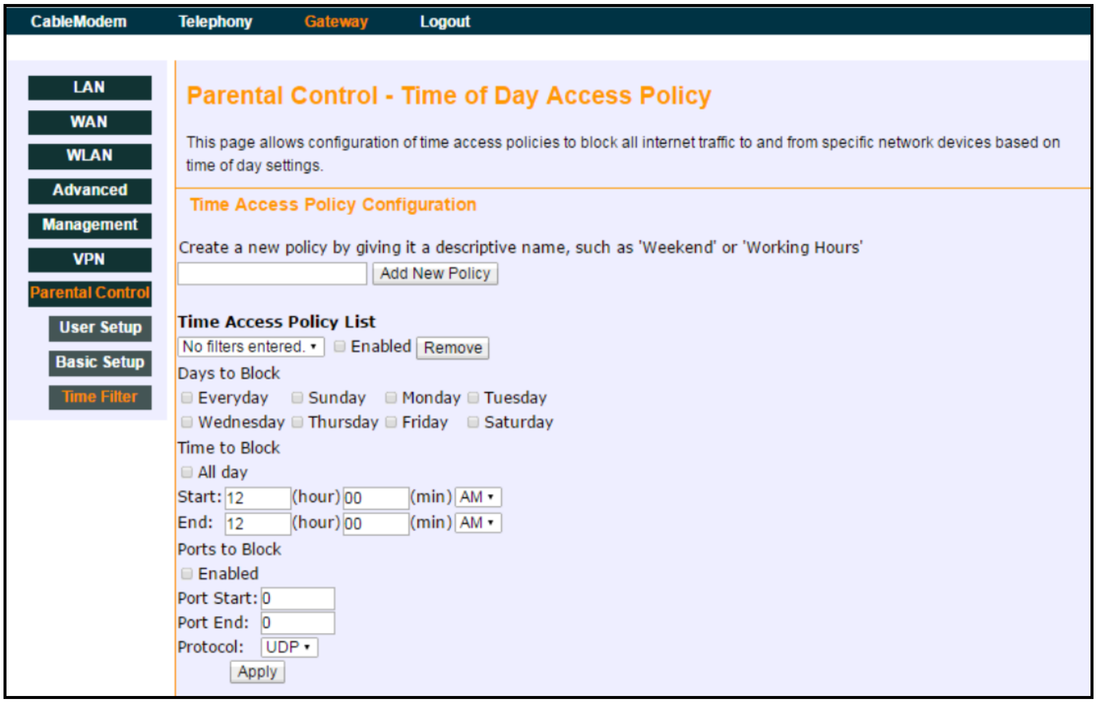
If you encounter a blocked website, you can override the block by entering the following password

Password	••••••••
Re-Enter Password	••••••••
Access Duration	30
[Apply]	

Label	Description
Enable Parental Control	Activates parental control when the box is checked and Apply is clicked.
Apply	Saves all changes in the screen and activates parental control if that box is checked.
Content Policy Configuration	
Add New Policy	Adds a policy to the Policy List. Enter the policy name and click Add New Policy. Note that the policy name cannot contain any spaces.
Content Policy List	Lists existing policies you can choose to use.
Remove Policy	Deletes a policy from the content policy list. Select the policy and click Remove Policy.
Keyword List	Displays keywords you can use to block Web site addresses (URLs) containing those words.
Add Keyword	Adds a keyword to the keyword list. Enter the word in the field provided and click Add Keyword. The keyword is then added to the list.
Remove Keyword	Removes a keyword from the list. Select the keyword and click the Remove Keyword button.
Blocked Domain List	Displays Web domains (for example, unwanted.com) you can use to block access to those domains.
Add Domain	Adds a domain to the blocked domain list. Enter a domain in the field provided and click Add Domain. The domain is then added to the list.
Remove Domain	Removes a domain from the blocked domain list. Select the domain and click the Remove Domain button.
Allowed Domain List	Displays Web domains (for example, safe.com) you can use to allow certain users access to only those domains.
Add Allowed Domain	Adds a domain to the allowed domain list. Enter a domain in the field provided and click Add Allowed Domain. The domain is then added to the list.
Remove Allowed Domain	Removes a domain from the allowed domain list. Select the domain and click the Remove Allowed Domain button.
Override Password	If you encounter a blocked website, you can override the block by entering a password.
Password	Enter a password for overriding blocked Web sites.
Re-Enter Password	Confirm the password by re-entering it here.
Access Duration	Allows you to set a time duration (in minutes) for access to the blocked site when the block has been overridden by entering the password.
Apply	Saves changes to the password and access duration time.

6.7.3 Using the Time Filter Option

Use the **Time Filter** option to configure time-based access policies to block all Internet access at certain times. Fields are explained following this screen example.



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'

Add New Policy

Time Access Policy List

No filters entered. ▾ □ Enabled Remove

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 ▾

Ports to Block

□ Enabled

Port Start: 0

Port End: 0

Protocol: UDP ▾

Apply

Label	Description
Time Access Policy Configuration	
Add New Policy	Adds a new time access policy. Enter a policy name and click the Add New Policy button.
Time Access Policy List	Displays the existing time access policies in a drop-down list.
Enabled	Activates a policy. Select the policy from the drop-down list and check Enabled.
Remove	Removes a policy. Select the policy from the drop-down list and click Remove.
Days to Block	Enables you to select the days to block Internet access.
Time to Block: All day or a specific time frame	Defines the times to block access: ♦ To block all day, check All Day to block access completely for the selected days. ♦ To block a specific time frame for the selected days, enter the Start time and the End time. Select AM or PM for each.
Ports to Block	Defines a port range to block if the Enabled box is checked. ♦ Port Start: Enter the starting port number to be blocked. ♦ End Port: Enter the ending port number to be blocked. ♦ Protocol: Select the protocol type. Options are UDP, TCP, or Both.
Apply	Saves all changes when clicked.