



Ubee UBC1301-AA00

DOCSIS 3.1 Advanced Voice Gateway

Firmware Version: 12.2.3101.20

Subscriber User Guide

March 2017

www.ubeeinteractive.com

9155 East Nichols Avenue, Suite 220
Centennial, CO 80112

Sales (email): amsales@ubeeinteractive.com

Support (email): amsupport@ubeeinteractive.com

Notices and Copyrights

Copyright 2017 Ubee Interactive. All rights reserved. This document contains proprietary information of Ubee and is not to be disclosed or used except in accordance with applicable agreements. This material is protected by the copyright laws of the United States and other countries. It may not be reproduced, distributed, or altered in any fashion by any entity (either internal or external to Ubee), except in accordance with applicable agreements, contracts, or licensing, without the express written consent of Ubee and the business management owner of the material.

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.



Contents

1	Introduction	1
1.1	Safety and Regulatory Information	1
1.1.1	Safety	1
1.1.2	Eco-Environmental Statements	2
1.1.3	Regulatory Statements	2
1.2	Application Example	3
1.3	Requesting Support	3
1.4	Device Package Components	4
1.5	Device Panels, Connections and LEDs	5
1.5.1	Device Front and Rear Panels	5
1.5.2	Device Connections	6
1.5.3	LED Behavior	6
1.6	Specifications, Standards, and Firmware	7
1.7	Default Values and Logins.	9
1.8	Device Label	10
2	Installing the UBC1301-AA00	12
2.1	Setting Up and Connecting the UBC1301-AA00	12
2.1.1	Wall Mount Installation	13
2.2	Connecting Devices to the Network	14
2.2.1	Connecting an Ethernet Device	14
2.2.2	Connecting a Telephone Line	15
2.2.3	Connecting a Wireless Device	15
2.3	Troubleshooting the Installation	16
3	Using the Web User Interface	18
3.1	Accessing the Web User Interface Locally	18
3.2	Logging Out of the Web User Interface	20

4	Understanding the Cable Modem Menu	22
4.1	Using the CM Info Option	22
4.1.1	Using the Status Option	22
4.1.2	Using the Connection Option	23
4.1.3	Using the Event Log Option	26
5	Understanding the Telephony Menu	28
5.1	Using the MTA Option	28
5.1.1	Using the Status Option	28
5.1.2	Using the DHCP Option	29
5.1.3	Using the QoS Option	31
5.1.4	Using the Provisioning Option	32
5.1.5	Using the Event Log Option	33
6	Understanding the Gateway Menu	34
6.1	Using the WAN Option	34
6.1.1	Using the Setup Option	35
6.1.2	Using the Operation Mode Option	36
6.2	Using the LAN Option	37
6.2.1	Using the DHCPv4 Option	37
6.2.2	Using the DHCPv6 Option	39
6.2.3	Using the DHCP Lease Option	41
6.3	Using the WLAN Option	41
6.3.1	Using the Basic Option	42
6.3.2	Using the Security Option	44
6.3.3	Using the WPS Option	45
6.3.4	Using the Access Control Option	46
6.3.5	Using the WMM Option	48
6.3.6	Deploying and Troubleshooting the Wireless Network	50
6.4	Using the Advanced Settings Options	54
6.4.1	Using the Options option	55
6.4.2	Using the Firewall option	56
6.4.3	Using the IP Filter Option	57
6.4.4	Using the MAC PassThrough Option	58

6.4.5	Using the MAC Filter Option	59
6.4.6	Using the Port Forwarding Option	61
6.4.7	Using the Port Trigger Option	64
6.4.8	Using the DMZ Option	67
6.4.9	Using the DDNS Option	68
6.4.10	Using the DNS Override Option	69
6.4.11	Using the NTP Option	70
6.5	Using the Parental Control Option	71
6.5.1	Using the ToD Filter Option	72
6.6	Using the Management Option	74
6.6.1	Using the Account Option	74
6.6.2	Using the Backup/Restore Option	75
6.6.3	Using the Factory Default Option	76
6.6.4	Using the Client List Option	77
6.7	Using the Diagnostics Option	78
6.7.1	Using the Tools Option	78
6.7.2	Using the Home Topology Option	80
7	Understanding the MoCA Menu	82
7.1	Using the MoCA Info Option	82
7.2	Using the Status Option	82
8	Understanding the Battery Menu	84
8.1	Using the Battery Info Option	84
8.1.1	Using the Controller Option	85
8.2	Using the UPS Option	86
8.3	Using the Interface Delay Option	86
9	Glossary	88

1 Introduction

Welcome to the Ubee family of data networking products. This guide is specific to the **UBC1301-AA00 Advanced Wireless Voice Gateway** for cable service provider subscribers and serves the following purposes:

- ❑ Provides instructions on how to install, connect, and operate the UBC1301-AA00.
- ❑ 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.
- ❑ Provides a glossary to define technical terms and acronyms. Refer to the [Glossary on page 88](#).



Topics

See the following topics:

- ◆ [Safety and Regulatory Information on page 1](#)
- ◆ [Application Example on page 3](#)
- ◆ [Requesting Support on page 3](#)
- ◆ [Device Package Components on page 4](#)
- ◆ [Device Panels, Connections and LEDs on page 5](#)
- ◆ [Specifications, Standards, and Firmware on page 7](#)
- ◆ [Default Values and Logins on page 9](#)
- ◆ [Device Label on page 10](#)

1.1 Safety and Regulatory Information

Use the following information to better understand safety and regulatory standards to install, maintain, and use the UBC1301-AA00 Advanced Wireless Voice Gateway.

1.1.1 Safety

WARNING: The following information provides safety guidelines for anyone installing and maintaining the UBC1301-AA00. 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 cable included with the device. Do not attach the power supply cable to building surfaces or floorings.

- ◆ Rest the power cable 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 furniture.

1.1.2 Eco-Environmental Statements

The following eco-environmental statements apply to the UBC1301-AA00.

Packaging Collection and Recovery Requirements:

Countries, states, localities, or other jurisdictions may require that systems be established for the return and/or collection of packaging waste from the consumer, or other end user, or from the waste stream. Additionally, reuse, recovery, and/or recycling targets for the return and/or collection of the packaging waste can be established. 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 Statements

The following regulatory statements apply to the UBC1301-AA00.

Industry North America Statement:

This device complies with RSS-210 of the Industry North America Rules. Operation is subject to the following two conditions:

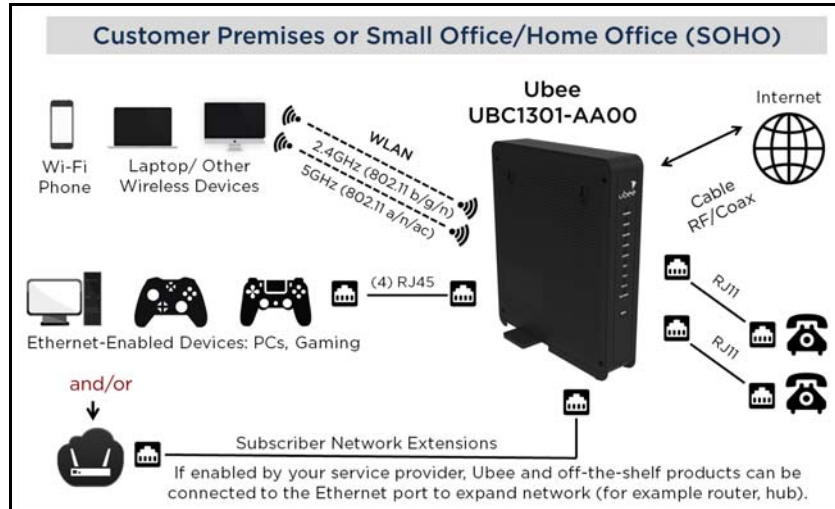
- (1) This device may not cause harmful interference.
- (2) This device must accept any interference received, including interference that may cause undesired operation.

Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between itself and your body. This device must not be co-located with or operating in conjunction with any other antenna or transmitter.

1.2 Application Example

The following diagram illustrates the general connection topology and applications of the UBC1301-AA00.






1.3 Requesting Support

Contact your service provider for direct support. Device documentation support may be available at:

<http://www.ubeeinteractive.com>

1.4 Device Package Components

The package for the UBC1301-AA00 contains the following items:

Item	Description
	<p>1 - RJ45 Cable (Ethernet) Length ~ 5.0 ft RoHS & UL compliant</p> <p><i>Sample image, actual appearance subject to change.</i></p>
	<p>1 - Power Cable Input: 100-120VAC, 60Hz, 1.2A Max. CE and UL Certified</p> <p><i>Sample image, actual appearance subject to change.</i></p>
	<p>1 - Battery</p> <p><i>NOTE:</i> <i>The battery is not included in the product packaging by default. You must contact your service provider to obtain a battery.</i></p> <p>Model: 13A0004A</p> <p>Battery supports continuous voice service during power outages, and provides up to 8 hours standby time, and 5 hours talk time with one line active. Actual performance is affected by battery age and operating environment.</p> <p>Battery must be fully charged prior to first use.</p>

1.5 Device Panels, Connections and LEDs

1.5.1 Device Front and Rear Panels

The following images represent the UBC1301-AA00 front and rear panels. Connection descriptions are provided in section 1.5.2., and LED descriptions are provided in section 1.5.3.



Front Panel

Rear Panel

1.5.2 Device Connections

The following table describes the connections on the rear panel of the UBC1301-AA00.


Item	Description
USB	Use to connect to USB enabled devices such as hard disk drives, and can be used for firmware upgrade.
RESET	To reset the device, use a pointed object like the end of a paper clip to push down the reset button. To power cycle the device, hold for less than 5 seconds. To reset to factory default settings, hold for more than 20 seconds. The UBC1301-AA00 will reset and reboot. Warning: Resetting to factory defaults will erase any and all settings you have configured and will restore to factory default settings.
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 an LED to indicate its status when an Ethernet device is connected.
CABLE	Connects to the cable outlet (with the cable provided by your service provider), or a cable splitter connected to the cable outlet.
TEL 1 TEL 2	Connects to standard telephones using an RJ11 cable. Telephone service must be enabled by your service provider.
POWER	Connects the power cable to the device. Use only the power cable provided with the UBC1301-AA00.

1.5.3 LED Behavior

The following tables summarize the behavior of the LEDs on both the front and rear panels of the UBC1301-AA00.

FRONT PANEL		
LED	Color	Description
POWER	Green	On – Internal power-on completed successfully. Flashes – Power-on failed. Note that the LED blinks briefly immediately after powering on the device.
DS/US (downstream/ upstream)	Green	Flashes – When DS and US scan is in progress. On – Locked to DS and US channels and registered OK, and when data is being passed. Flashes – When a firmware upgrade is in progress.
ONLINE	Green	Flashes – Obtaining an IP address and configuration file. On – Configuration completed successfully, network connected. Off – Network connect failed.
2.4G	Green	Flashes – 2.4GHz Wi-F- traffic is being passed. On – 2.4GHz Wi-F- is enabled. Off – 2.4GHz Wi-F- is disabled.
5G	Green	Flashes – 5GHz Wi-F- traffic is being passed. On – 5GHz Wi-F- is enabled. Off – 5GHz Wi-F- is disabled.
TEL1	Green	On – Telephony is enabled. Off – Telephony is not provisioned. Flashes – Call is in progress or EMTA is attempting to register.

FRONT PANEL		
LED	Color	Description
TEL2	Green	On – Telephony is enabled. Off – Telephony is not provisioned. Flashes – Call is in progress or EMTA is attempting to register.
MoCA	Green	On – Device is connected to a MoCA network. Off – Device is not connected to a MoCA network.
BATTERY	Green	On – Battery is installed an AC power is on. Off – No battery is installed. Flashes – When battery power level is low (30 minutes or less remaining).
WPS	White	When a user pushes the WPS button or triggers WPS via the web user interface, the WPS LED flashes for 4 minutes until the PIN is entered from the wireless client. After a Wi-Fi client attaches successfully, the LED remains on for 5 minutes, then turns off.

REAR PANEL		
LED	Color	Description
ETHERNET 1-4	Green/ Orange	<p>On Green – An Ethernet device is connected to the device at 1000 Mbps speeds (Gigabit Ethernet).</p> <p>On Orange – An Ethernet device is connected to the device at 10/100 Mbps speeds.</p> <p>Flashes (in Green or Orange) – When data is being passed between the cable modem and the connected device.</p> <p>The Ethernet ports are used to connect Ethernet devices such as computers, gaming consoles, and/or routers/hubs to the UBC1301-AA00 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.</p> 

1.6 Specifications, Standards, and Firmware

The following list provides the features and specifications of the UBC1301-AA00.

Interfaces and Standards

- ◆ Cable: F-Connector, female
- ◆ USB: 1 USB 3.0 host port
- ◆ LAN: (4) 10/100/1000 Mbps RJ45 ports
- ◆ Telephony: (2) RJ11 ports, PacketCable 1.5/2.0 compatible
- ◆ DOCSIS 3.1 certified
- ◆ DOCSIS 1.0/1.1/2.0/3.0 certified

- ◆ MoCA 2.0 enabled
- ◆ CE/FCC Class B, ENERGY STAR certified, Wi-Fi Alliance certified

Downstream*

- ◆ Frequency Range: 108MHz/1002MHz
- ◆ Capture Bandwidth: 1GHz
- ◆ Modulation: 64 or 256 QAM and OFDM: up to 4096 QAM
- ◆ Maximum DOCSIS 3.1 Data Rate: 2 x 192MHz OFDM channels provide capacity up to 5Gbps
- ◆ Maximum DOCSIS 3.0 Data Rate: 32 downstream channels provide speeds up to 1372Mbps
- ◆ Symbol Rate: 5361 Ksps
- ◆ RF (cable) Input Power: -15 to +15dBmV (64 QAM), -15 to +15dBmV (256 QAM)
- ◆ Input Impedance: 75 Ω

Upstream*

- ◆ Frequency Range: 5MHz - 42MHz/85MHz switchable
- ◆ Modulation: QPSK or 8/16/32/64/128 QAM and OFDMA: up to 4096 QAM
- ◆ Maximum DOCSIS 3.1 Data Rate: 2 x 96MHz OFDMA channels provide capacity up to 2Gbps
- ◆ Maximum DOCSIS 3.0 Data Rate: 8 upstream channels provide speeds up to 246Mbps
- ◆ Symbol Rate: 160, 320, 640, 1280, 2560, 5120 Ksps
- ◆ RF (cable) Output Power: TDMA/ATDMA: +8dBmV to +54dBmV (32/64 QAM).
ATDMA Only: +8dBmV to +55dBmV (8/16 QAM), +8dBmV to +58dBmV (QPSK).
S-CDMA: +8dBmV to +53dBmV (all modulations)

*Actual speeds vary based on factors including network configuration and speed.

Voice

- ◆ PacketCable 1.5 (NCS) OR 2.0 (IMS/SIP) compatible, based on the firmware version
- ◆ 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
- ◆ DTMF Tone Detection, T.38 Fax Relay (G.711), Echo Cancellation (G.168) / Silence Suppression, Voice Active Detection and Comfort Noise Generation
- ◆ G.722 codec, WB SLIC

Wireless, Security, and Network

- ◆ Dual-band concurrent, high power radios, supports 8 SSIDs per radio
- ◆ 802.11b/g/n/ac compliant with link speeds up to AC2400 (600Mbps at 2.4GHz + 1733Mbps at 5GHz)
- ◆ Beam forming technology and high powered amplifiers to extend range
- ◆ 4 Tx and 4 Rx antennas on each radio
- ◆ DHCP Client/Server, Static IP network assignment, RIPv1/v3, Ethernet 10/100/1000 Base-T, full duplex auto-negotiate functionality, IPv4 and IPv6 support

- ◆ NAT Firewall, MAC/IP/port filtering, parental control, stateful packet inspection (SPI), DoS attack protection, WPS/WPA/WPA2/WPA-PSK & 64/128-bit WEP encryption
- ◆ VPN pass-through and VPN end-point support (IPSec/T2TP/PPTP), TACACS or RADIUS authentication

Device Management

- ◆ Supports UAPSD (power savings)
- ◆ DOCSIS, Web-Based, and XML Configuration
- ◆ Telnet/SSH remote management
- ◆ Firmware upgrade via TFTP
- ◆ Configuration backup and restore
- ◆ SNMP v1, v2c, v3 support
- ◆ Syslog
- ◆ WiFi Radar
- ◆ Spectrum Analyzer
- ◆ TR-069 capable

Physical and Environmental

- ◆ Dimensions: 53 mm, 2.1" (W) x 286 mm, 11.25" (H) x 244 mm, 9.6" (D)
- ◆ Weight: 1200g (2.6 lb)
- ◆ Power: 100-120Vac, 60Hz, 1.2A, internal PSU
- ◆ Operating Temperature: 0°C ~ 45°C (32°F ~ 113°F)
- ◆ Humidity: 5~90% (non-condensing)
- ◆ **Optional** battery supports continuous voice service during power outages; up to 8 hours standby, 5 hours talk time with 1 line active. **Note:** Actual performance is affected by battery age and operating environment. **Note:** Battery must be fully charged prior to first use.

1.7 Default Values and Logins

The UBC1301-AA00 is pre-configured with the default parameters for your cable service provider.

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:

- ◆ Default wireless encryption is WPA2-PSK with AES.
- ◆ SSIDs (wireless network names) = "WIFI" plus the last 6 characters of the Cable Modem MAC address (in upper case) for the 2.4GHz radio band. "-5G" is added to the end for the 5GHz radio band. The SSIDs can be found on the device label.

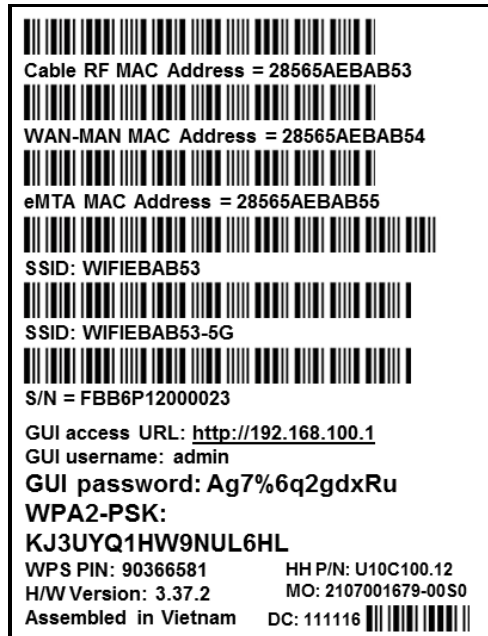
- ❖ Examples:
 1. 2.4GHz radio with Cable RF MAC address 28:56:5A:EB:AB:53.
SSID: WIFIEBAB53
 2. 5GHz radio with Cable RF MAC address 28:56:5A:EB:AB:53.
SSID: WIFIEBAB53-5G
- ❖ If you change the SSID, the device does not revert to the default value when the device is power cycled, but does revert to this default value if the device is reset to factory defaults.
- ◆ WPA Pre-shared Key (PSK) = a unique key for each device. Also called the network key or the wireless password. The default WPA pre-shared key is a randomly generated character string, 16 characters in length, and can be found on the device label.
 - ❖ Example WPA PSK: KJ3UYQ1HW9NUL6HL
- ◆ WPS PIN = The WPS PIN is a randomly generated number and is used to connect wireless clients via the Wireless Protected Setup (WPS) method. It can be found on the device label.
 - ❖ Example WPS PIN: 90366581

Login Default Value

- ◆ Standard User Web Interface Login
 - Username:** admin
 - Password:** Random password of 12 alpha-numeric characters (can be found on the device label)

1.8 Device Label

The following is an example of the housing label for the UBC1301-AA00. Descriptions are provided in the table below.



Label	Description
Cable RF MAC Address	Displays the MAC address of the RF interface of the device.
WAN-MAN MAC Address	Displays the MAC address of the cable home interface of the device.
eMTA MAC Address	Displays the eMTA (embedded multimedia terminal adapter) address of the device.
SSID	Displays the SSID for the 2.4GHz radio band. Also known as the wireless network name.
SSID	Displays the SSID for the 5GHz radio band. Also known as the wireless network name.
S/N	Displays the unique manufacturer serial number of the device.
GUI access URL	Displays the URL or web address to use when accessing the Web user interface for the device.
GUI username	Displays the user name to be entered when accessing the Web user interface for the device.
GUI password	Displays the random password to be entered when accessing the Web user interface for the device.
WPA2-PSK	Displays the WPA2 pre-shared key. Also known as the network key or the wireless password.
WPS PIN	Displays the randomly generated number that is used to connect wireless clients via the Wireless Protected Setup (WPS) method.
H/W Version	Displays the internal version number that identifies the hardware design.
Assembled in	Displays the country in which the device was assembled.
HH P/N	Displays the product number for the manufacturer.
MO	Displays the device internal manufacturing order number.
DC	The DC (date code) indicates the date of manufacture.

2 Installing the UBC1301-AA00

Use the information in this chapter to set up and connect the UBC1301-AA00, connect additional devices, and troubleshoot the installation.



Topics

See the following topics:

- ◆ [Setting Up and Connecting the UBC1301-AA00 on page 12](#)
- ◆ [Connecting Devices to the Network on page 14](#)
- ◆ [Troubleshooting the Installation on page 16](#)

2.1 Setting Up and Connecting the UBC1301-AA00

Use the following instructions to set up and connect the UBC1301-AA00. When the device is set up and connected, refer to [Accessing the Web User Interface Locally on page 18](#) to configure the device.

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

To set up the device:

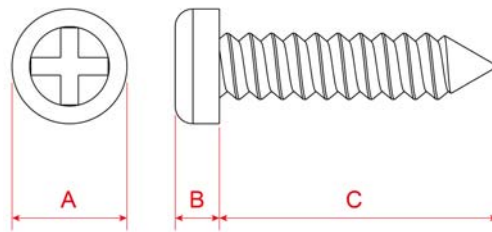
1. Remove the contents from the device packaging.
2. Place the UBC1301-AA00 in the best location to connect to other devices, such as PCs or gaming consoles.
 - ◆ Place the UBC1301-AA00 Advanced Wireless Voice Gateway and wireless clients in open areas far away from transformers, heavy-duty motors, microwave ovens, refrigerators, fluorescent lights, and manufacturing equipment. These items can adversely affect 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 50](#).
 - ◆ Place the device in a location that has an operating temperature of 0° C to 45° C (32° F to 113° F).
 - ◆ Regular operating altitude is 2000 m (6561 ft), and maximum operating altitude is 4500 m (14,760 ft).
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 10, Windows 8, Windows 7, Google Chrome, Firefox 1.07 and higher, Internet Explorer v7 and above, Netscape.
 - ◆ For MAC OS X, 10.2, and higher: Firefox 1.07 and higher, Safari 1.x and higher.

4. Connect the power cord included in the product package to the POWER port on the back of the cable modem and plug the other end into the power outlet.
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 UBC1301-AA00.
6. Connect a coaxial cable from the **CABLE** port on the back panel 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 TEL1 or TEL2 port on the back panel of the device. Use an RJ-11 telephone cable.
8. Validate the network connection using the device LEDs to confirm operations.
 - ◆ The PWR, DS/US, and ONLINE LEDs are solidly lit.

Refer to [LED Behavior on page 6](#) for more information.

2.1.1 Wall Mount Installation

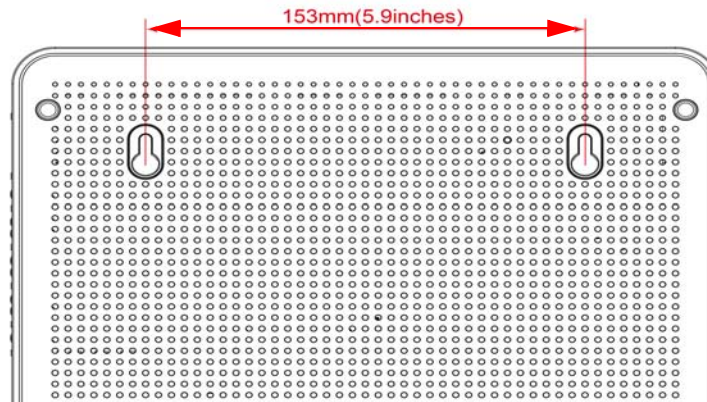
You can mount the UBC1301-AA00 on a wall using the 2 mounting brackets on the side of the device. Two round or pan head screws are recommended. See the figure below.



Label	Size in Millimeters (mm)
A	6.65 +/- 0.35
B	1.9 +/- 0.15
C	19.0 +/- 1.2

To mount the UBC1301-AA00 on a wall:

1. Install the two screws horizontally on a wall 5.9 inches (153 mm) 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 topics:

- ◆ [Connecting an Ethernet Device on page 14](#)
- ◆ [Connecting a Telephone Line on page 15](#)
- ◆ [Connecting a Wireless Device on page 15](#)

2.2.1 Connecting an Ethernet Device

You can connect up to three additional Ethernet devices to the UBC1301-AA00.

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 UBC1301-AA00.
2. Use the device LEDs to confirm operations. Refer to [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).

Refer to [Troubleshooting the Installation on page 16](#) for troubleshooting information.

2.2.2 Connecting a Telephone Line

You can connect up to two telephone lines to the UBC1301-AA00 to use the telephone (voice) features.

Voice service must be enabled by your 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 TEL1 or TEL2 jack on the back panel of the UBC1301-AA00 using an RJ11 telephone cable. Connect the other end to the telephone.
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.

2.2.3 Connecting a Wireless Device

Use the following steps to connect a wireless device (client) to the UBC1301-AA00 (for example a laptop computer).

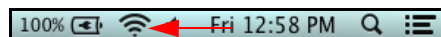
Default values are found in the steps below.

To connect a wireless device:

1. Access the wireless networking feature on your wireless device, and view available wireless networks.
 - ◆ 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 (Airport) on the right side of the top menu bar. All available wireless networks will appear in the drop-down menu.



2. The UBC1301-AA00 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 default SSID is "WIFI" plus the last 6 characters of the Cable Modem MAC address (in upper case) for the 2.4GHz radio band. "-5G" is added to the end for the 5GHz radio band.
 - ◆ SSID examples:
 1. 2.4G radio with Cable RF MAC address 28:56:5A:EB:AB:53.
2.4GHz SSID: WIFIEBAB53

2. 5G radio with Cable RF MAC address 28:56:5A:EB:AB:53.

5GHz SSID: WIFIEBAB53-5G

- ◆ **Notes:** You can find the Cable RF MAC address on the device label. If you change the SSID, the device does not revert to the default value when the device is power cycled, but does revert to this default value if the device is reset to factory defaults. See [Using the Basic Option on page 42](#).
 - ◆ When prompted, enter the network key, also called the pre-shared key (PSK). This is a unique key for each device. The pre-shared key for the UBC1301-AA00 The default WPA pre-shared key is a randomly generated character string, 16 characters in length, and can be found on the device label.
 - ❖ Pre-shared key example: KJ3UYQ1HW9NUL6HL
 - ◆ If using WPS, enter the WPS personal identification number (PIN). The WPS PIN is a randomly-generated number and is used to connect wireless clients via the Wireless Protected Setup (WPS) method. It can be found on the device label. Refer to [Using the WPS Option on page 45](#).
 - ◆ **Default Security and Encryption Methods:** WPA2-PSK with AES encryption.
3. Confirm connectivity by opening a Web browser on the wireless client device, and going to any Web site.

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 18](#).

4. If you have wireless issues or questions, refer to [Deploying and Troubleshooting the Wireless Network on page 50](#).

2.3 Troubleshooting the Installation

Use the following tips to troubleshoot the installation.

- ◆ None of the LEDs are on when I power on the UBC1301-AA00.
 - ❖ Check the connection between the power outlet and the power adapter. 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 UBC1301-AA00. Power off the unit and wait for 5 seconds and power it on again. If the problem still exists, there may be a hardware problem.
- ◆ The ETHERNET 1-4 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 UBC1301-AA00.
 - ❖ 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 UBC1301-AA00 by removing the power adapter from the electrical outlet and plugging it back in. Wait for the device 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 UBC1301-AA00.
 - ❖ 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.
- ◆ If none of these suggestions work, contact your service provider for further assistance.

3 Using the Web User Interface

The Web user interface (UI) for the UBC1301-AA00 is easy to access and allows you to view and configure settings for your wireless gateway device. You can validate the installation by accessing the Web user interface on the device.

- ◆ [Accessing the Web User Interface Locally on page 18](#)
- ◆ [Logging Out of the Web User Interface on page 20](#)

3.1 Accessing the Web User Interface Locally

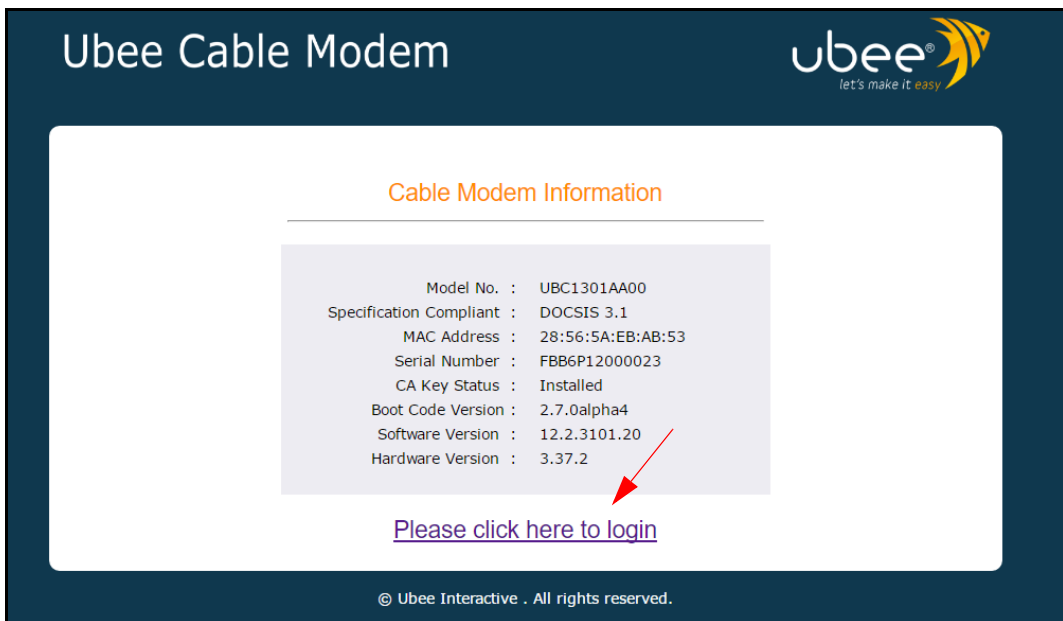
Access the Web user interface for the UBC1301-AA00 from a Web browser, such as Internet Explorer on a Windows computer. Default login values are shown in the steps below.

To access the Web user interface:

1. Launch an Internet browser, such as Internet Explorer, 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. The following screen appears and displays basic information about the UBC1301-AA00 Advanced Wireless Voice Gateway.
4. Click on **'Please click here to login.'**

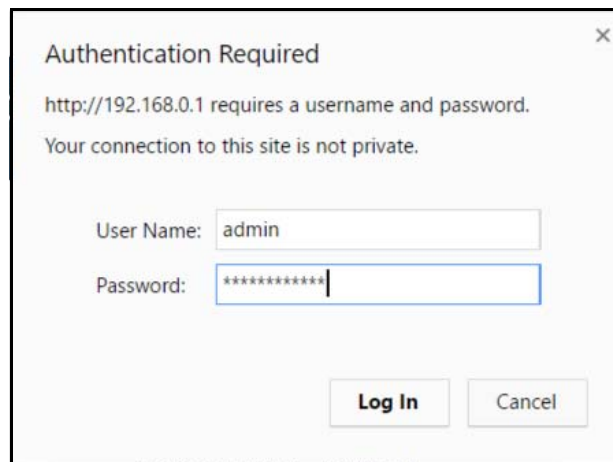


5. In the authentication dialog that appears, enter the username and password and click OK.

◆ **Standard User Web Interface Login:**

Username: admin

Password: Random password of 12 alpha-numeric characters (can be found on the device label)



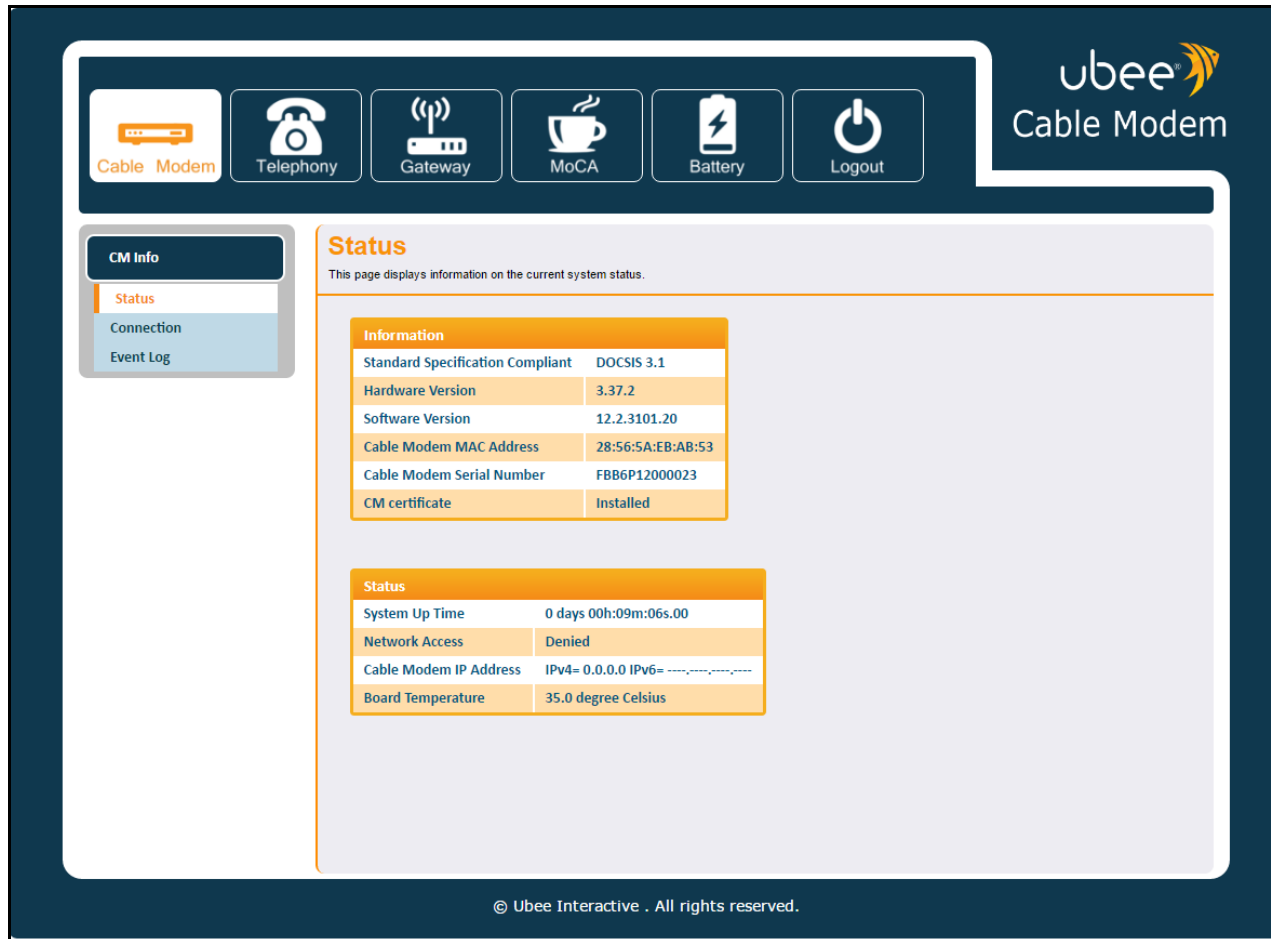
Authentication Required

http://192.168.0.1 requires a username and password.
Your connection to this site is not private.

User Name:

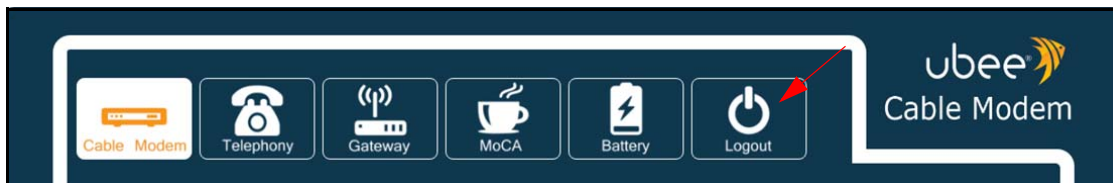
Password:

After logging in, the **Cable Modem Status** screen displays device information about the UBC1301-AA00. For screen field descriptions, refer to [Using the Status Option on page 22](#).




3.2 Logging Out of the Web User Interface

To log out of the UBC1301-AA00 web user interface, click the Logout icon on the main menu.



After logging out, you are returned to the login screen, where you can log back into the device by clicking on **'Please click here to login.'**

Ubee Cable Modem



Cable Modem Information

Model No. :	UBC1301AA00
Specification Compliant :	DOCSIS 3.1
MAC Address :	28:56:5A:EB:AB:53
Serial Number :	FBB6P12000023
CA Key Status :	Installed
Boot Code Version :	2.7.0alpha4
Software Version :	12.2.3101.20
Hardware Version :	3.37.2

[Please click here to login](#)

© Ubee Interactive . All rights reserved.

4 Understanding the Cable Modem Menu

The **Cable Modem** menu of the Web user interface allows you to access information about the UBC1301-AA00, such as software, uptime, CM hardware addresses, connection status and the event log.

To access the Web User Interface, refer to [Accessing the Web User Interface Locally on page 18](#).



Topics

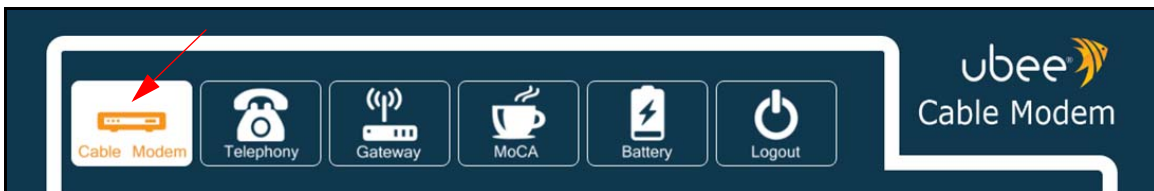
See the following topics:

- ◆ [Using the CM Info Option on page 22](#)

4.1 Using the CM Info Option

To access cable modem information:

1. Access the Web user interface. Refer to [Accessing the Web User Interface Locally on page 18](#).
2. Click **Cable Modem** from the top main menu.



3. Click **CM Info** (Cable Modem Information) from the left side menu. The following sub-menus are available:
 - ◆ [Using the Status Option on page 22](#)
 - ◆ [Using the Connection Option on page 23](#)
 - ◆ [Using the Event Log Option on page 26](#)

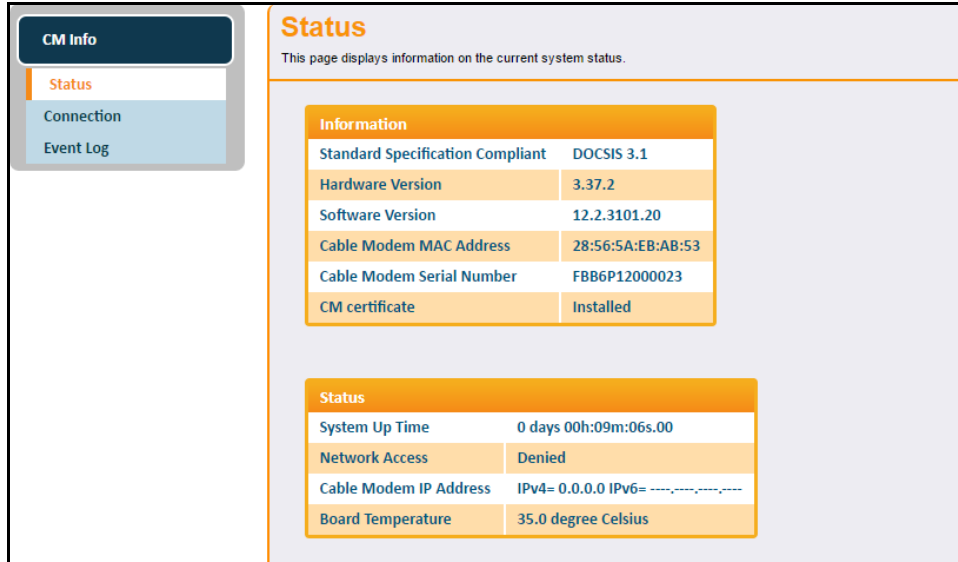
4.1.1 Using the Status Option

The **Status** option displays the device's software version, uptime, CM MAC and IP addresses.

To view device status information:

1. Click **CM Info** from the left side menu.
2. Click **Status** below CM Info.

Field descriptions follow the screen example.



Label	Description
Information	
Standard Specification Compliant	Defines the current DOCSIS standard supported by the UBC1301-AA00.
Hardware Version	Defines the internal version number that identifies the hardware design.
Software Version	Defines the firmware version of the device.
Cable Modem MAC Address	Defines the unique media access control (MAC) hardware address of the UBC1301-AA00.
Cable Modem Serial Number	Defines the unique manufacturer serial number of the device.
CM certificate	Indicates if the cable modem certificate is installed.
Status	
System Up Time	Displays how long the device has been connected.
Network Access	Defines if network access is enabled. When enabled, the user is allowed to access the network.
Cable Modem IP Address	Displays the IP address for the cable modem.
Board Temperature	If available, displays the temperature of the board.

4.1.2 Using the Connection Option

The **Connection** screen displays information about the device’s connection status and downstream and 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 computer to the remote destination (upstream channels).

To view connection information:

1. Click **CM Info** from the left side menu.
2. Click **Connection** under CM Info.

Please note that the following screen example shows the UBC1301-AA00 connected via *DOCSIS 3.0*. Field descriptions follow.

CM Info

Status

Connection

Event Log

Connection

This page displays information on the current system connection status.

CM IP Prov Mode: Honor MDD
Ethernet WAN Mode:
Bidirectional Forwarding Detection:
Current System Time: Tue Feb 7 12:51:26 2017

Startup Procedure

Procedure	Status	Comment
Acquire Downstream Channel	531000000	Locked
Connectivity State	OK	Operational
Boot State	OK	Operational
Configuration File	OK	UBC_D31_CVC.cfg
Security	Enabled	BPI+

CM Downstream Channel Info

Channel	Lock Status	Channel Type	Channel ID	Frequency	Width	Power	SNR	Modulation Profile ID	Correctables	Uncorrectables
1	Locked	SC-QAM Downstream	1	531000000 Hz	6000000 Hz	-12.1 dBmV	39.2 dB	QAM256	0	0
2	Locked	SC-QAM Downstream	2	537000000 Hz	6000000 Hz	-12 dBmV	39.2 dB	QAM256	0	0
3	Locked	SC-QAM Downstream	3	543000000 Hz	6000000 Hz	-12.3 dBmV	39.1 dB	QAM256	0	0
4	Locked	SC-QAM Downstream	4	549000000 Hz	6000000 Hz	-12.6 dBmV	39 dB	QAM256	0	0
5	Locked	SC-QAM Downstream	5	555000000 Hz	6000000 Hz	-12.7 dBmV	38.9 dB	QAM256	0	0
6	Locked	SC-QAM Downstream	6	561000000 Hz	6000000 Hz	-12.4 dBmV	39 dB	QAM256	0	0
7	Locked	SC-QAM Downstream	7	567000000 Hz	6000000 Hz	-12.6 dBmV	38.9 dB	QAM256	0	0
8	Locked	SC-QAM Downstream	8	573000000 Hz	6000000 Hz	-12.3 dBmV	38.9 dB	QAM256	0	0
9	Locked	SC-QAM Downstream	9	579000000 Hz	6000000 Hz	-12.3 dBmV	38.7 dB	QAM256	0	0
10	Locked	SC-QAM Downstream	10	585000000 Hz	6000000 Hz	-12.8 dBmV	38.8 dB	QAM256	0	0
11	Locked	SC-QAM Downstream	11	591000000 Hz	6000000 Hz	-13.3 dBmV	38.3 dB	QAM256	0	0
12	Locked	SC-QAM Downstream	12	597000000 Hz	6000000 Hz	-13.5 dBmV	38.1 dB	QAM256	0	0
13	Locked	SC-QAM Downstream	13	603000000 Hz	6000000 Hz	-13 dBmV	38.6 dB	QAM256	0	0
14	Locked	SC-QAM Downstream	14	609000000 Hz	6000000 Hz	-12.3 dBmV	39 dB	QAM256	0	0
15	Locked	SC-QAM Downstream	15	615000000 Hz	6000000 Hz	-12.1 dBmV	39 dB	QAM256	0	0
16	Locked	SC-QAM Downstream	16	621000000 Hz	6000000 Hz	-12.4 dBmV	38.8 dB	QAM256	0	0
17	Locked	SC-QAM Downstream	17	627000000 Hz	6000000 Hz	-13.4 dBmV	38.2 dB	QAM256	0	0

18	Locked	SC-QAM Downstream	18	633000000 Hz	6000000 Hz	-13.9 dBmV	37.9 dB	QAM256	0	0
19	Locked	SC-QAM Downstream	19	639000000 Hz	6000000 Hz	-14.4 dBmV	37.5 dB	QAM256	0	0
20	Locked	SC-QAM Downstream	20	645000000 Hz	6000000 Hz	-14 dBmV	37.7 dB	QAM256	0	0
21	Locked	SC-QAM Downstream	21	651000000 Hz	6000000 Hz	-13.6 dBmV	37.8 dB	QAM256	0	0
22	Locked	SC-QAM Downstream	22	657000000 Hz	6000000 Hz	-13.7 dBmV	37.6 dB	QAM256	0	0
23	Locked	SC-QAM Downstream	23	663000000 Hz	6000000 Hz	-14 dBmV	37.4 dB	QAM256	0	0
24	Locked	SC-QAM Downstream	24	669000000 Hz	6000000 Hz	-14.8 dBmV	36.8 dB	QAM256	0	0
25	Locked	OFDM Downstream	25	717000000 Hz	94000 kHz	-15.2 dBmV	35.0 dB	0 1	6777560	840

CM Upstream Channel Info							
Channel	Lock Status	Channel Type	Channel ID	Frequency	Width	Power	Modulation/Profile ID
1	Locked	ATDMA	77	301000000 Hz	6400000 Hz	54.5 dBmV	2
2	Locked	ATDMA	78	365000000 Hz	6400000 Hz	54 dBmV	2
3	Locked	ATDMA	79	237000000 Hz	6400000 Hz	54.3 dBmV	2
4	Locked	ATDMA	80	173000000 Hz	6400000 Hz	54 dBmV	2

CM IP info			
CM IP Address	Duration	Expires	
IPv4= 0.0.0.0 IPv6= 2001:558:4070:6:aa56:5aff:feeb:ab53	 	 	

Label	Description
Startup Procedure: (Procedure, Status, Comment)	
Acquire Downstream Channel	Displays the Downstream channel status and if the device has locked to a channel.
Connectivity State	Displays connection status and if the UBC1303-AA00 is operational.
Boot State	Displays the status on boot up and if the device is operational.
Configuration File	Provides the status and file name of the configuration file currently used by the UBC1303-AA00.
Security	Displays the status of the security settings: enabled/disabled.
CM Downstream Channel Info	
Channel	Numbers the downstream channels.
Lock Status	Displays if the device has locked successfully to a downstream channel.
Channel Type	Displays the channel type.
Channel ID	Displays the downstream channel ID.
Frequency	Displays the downstream channel frequency on which the UBC1303-AA00 is scanning.
Width	Displays the channel width.
Power	Displays the receiver power level in decibel millivolts (dBmV) after ranging process.
SNR	Displays the signal-to-noise ratio, the desired signal level to the background noise level.

Label	Description
Modulation Profile ID	Displays the modulation method required for the downstream channel to lock on to by device. This method is determined by the service provider.
Correctables	Displays the quantity of codewords which are correctable.
Uncorrectables	Displays the quantity of codewords which are not correctable.
CM Upstream Channel Info	
Channel	Numbers the upstream channels.
Lock Status	Displays if the device has locked successfully to an upstream channel.
Channel Type	Displays the channel type.
Channel ID	Displays the current upstream channel ID.
Frequency	Displays the current upstream frequency in hertz.
Width	Displays the channel width.
Power	Displays the current upstream transmit power in decibel millivolts (dBmV).
Modulation/Profile ID	Displays the modulation method required for the downstream channel to lock on to by the device. This method is determined by the service provider.
CM IP Info	
CM IP Address	Displays the UBC1303-AA00's IP address.
Duration	Displays the time the device has been active.
Expires	Displays when the cable modem's certificate expires.

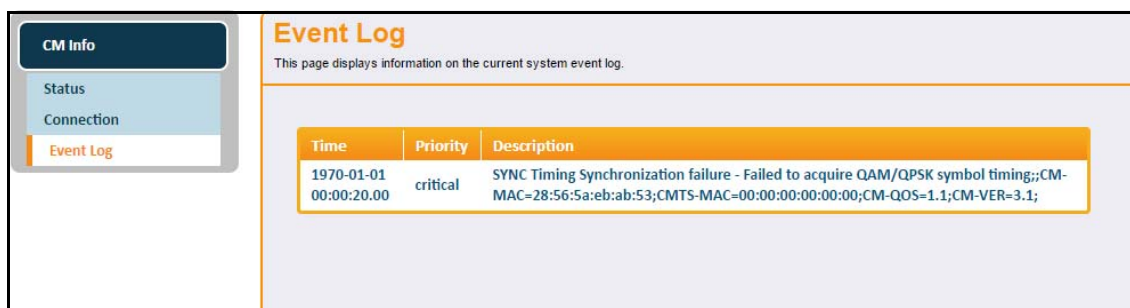
4.1.3 Using the Event Log Option

The **Event Log** option displays a log of events regarding the UBC1301-AA00's connection status.

To view event log information:

1. Click **CM Info** from the left side menu.
2. Click **Event Log** under CM Info.

Field descriptions are listed below the screen example.



Label	Description
Time	Displays the date and time of the event.
Priority	Displays the priority of the event.
Description	Describes the event.

5 Understanding the Telephony Menu

Telephony options provide settings for the voice functions of the UBC1301-AA00.

To access the Web User Interface, refer to [Accessing the Web User Interface Locally on page 18](#).



Topics

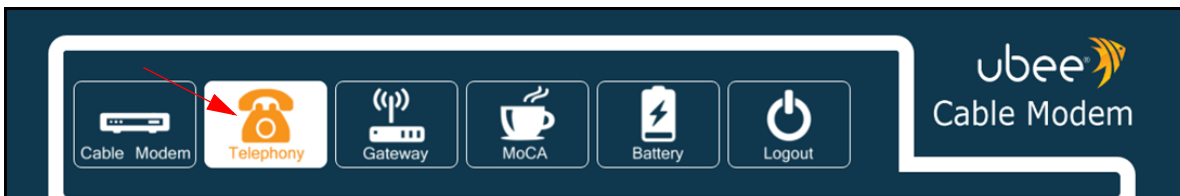
See the following topics:

- ◆ [Using the MTA Option on page 28](#)

5.1 Using the MTA Option

To access telephony information

1. Click **Telephony** from the top main menu.



2. Click **MTA** from the left side menu. The following sub-menus are available:

- ◆ [Using the Status Option on page 28](#)
- ◆ [Using the DHCP Option on page 29](#)
- ◆ [Using the QoS Option on page 31](#)
- ◆ [Using the Provisioning Option on page 32](#)
- ◆ [Using the Event Log Option on page 33](#)

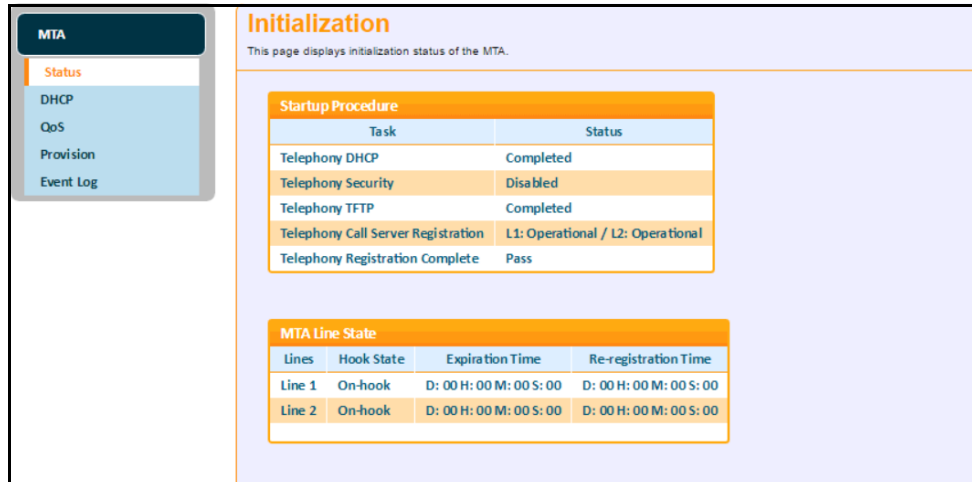
5.1.1 Using the Status Option

The **Status** option displays telephony startup procedure and line state information.

To view telephony status information:

1. Click **MTA** from the left side menu.
2. Click **Status** under MTA.

Field descriptions are listed below the screen example.



Label	Description
Startup Procedure	
Telephony DHCP	Displays the DHCP IP address of the MTA portion of the device.
Telephony Security	Displays the security mode of the MTA (Basic, Hybrid, or Security).
Telephony TFTP	Displays if the MTAs TFTP server is available.
Telephony Call Server Registration	Displays the status of the MTA's registration to the service provider's call server per line (Disconnected, Operational).
Telephony Registration Complete	Displays the completion status of the MTA registration (N/A, Operational).
MTA Line State	
Lines	Displays the telephone line connections: Line 1, Line 2.
Hook State	Displays if telephone is on-hook or off-hook.
Expiration Time	Displays the time the current connection registration expires.
Re-registration Time	Displays the time the current connection will re-register.

5.1.2 Using the DHCP Option

Use the **DHCP** (Dynamic Host Control Protocol) option to monitor the UBC1301-AA00 lease parameters, timers, and PacketCable DHCP Option 122.

To view DHCP status:

1. Click **MTA** from the left side menu.
2. Click **DHCP** under MTA.

Field descriptions are listed below the screen example.

MTA

Status

DHCP

QoS

Provision

Event Log

DHCP

This page displays DHCP status of the MTA.

Lease Parameters

FQDN	x1-6-90-cd-b6-a2-1d-87.mta.ubee.com
IP Address/Submask	10.32.1.50 / 255.255.255.0
Gateway	10.32.1.254
Bootfile	tftp://[172.21.1.251]/USMTA_Ubee.bin
Primary DNS	172.21.1.27
Secondary DNS	172.21.1.250

Lease Timers

Lease Time Remaining	D: 00 H: 23 M: 44 S: 03
Rebind Time Remaining	D: 00 H: 11 M: 44 S: 03
Renew Time Remaining	D: 00 H: 00 M: 00 S: 00

PacketCable DHCP Option 122

SNMP Entity (Sub-option 3)	x1-6-90-cd-b6-a2-1d-87.mta.ubee.com
Kerberos Realm (Sub-option 6)	BASIC.1
Provisioning Timer (Sub-option 8)	10

Label	Description
Lease Parameters	
FQDN	Displays the fully qualified domain name (FQDN), which specifies all the domain levels of the domain name system.
IP Address/Submask	Displays the IP address and submask of the telephone connection.
Gateway	Displays the gateway address.
Bootfile	Displays the location and file name of the file used to configure the telephony system.
Primary DNS	Displays the main domain name server.
Secondary DNS	Displays the secondary domain name server.
Lease Timers	
Lease Time Remaining	Displays the time left on the DHCP lease.
Rebind Time Remaining	Displays the time left on the rebinding lease. Rebinding is when the client tries to renew the DHCP lease on the same server before trying to connect to a new DHCP server.
Renew Time Remaining	Displays the time left before the DHCP lease renews.
PacketCable DHCP Option 122	
SNMP Entity (Sub-option 3)	Displays the SNMP entity
Kerberos Realm (Sub-option 6)	Displays the Kerberos domain name.
Provisioning Timer (Sub-option 8)	Displays the time interval for the provisioning flow to complete, if set.

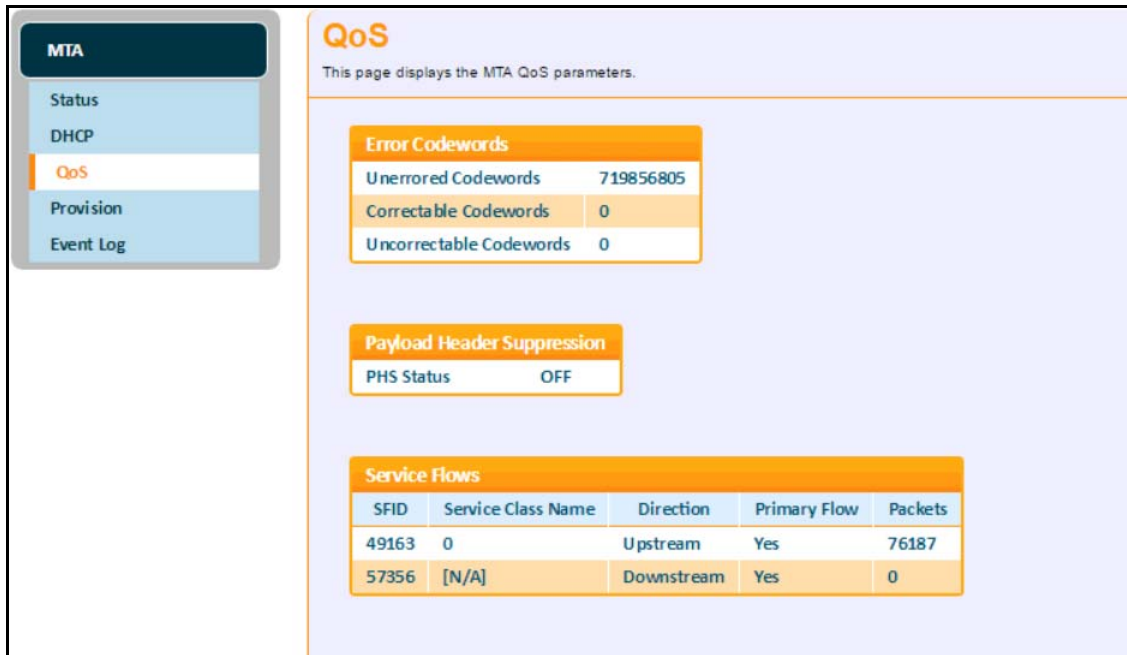
5.1.3 Using the QoS Option

Use the Quality of Service (QoS) option to monitor the UBC1301-AA00 error codewords, payload header suppression, and service flows.

To monitor QoS parameters:

1. Click **MTA** from the left side menu.
2. Click **QoS** under MTA.

Field descriptions are listed below the screen example.



Label	Description
Error Codewords	
Unerrored Codewords	Displays the number of codewords passed without error.
Correctable Codewords	Displays the number of codewords corrected.
Uncorrectable Codewords	Display the number of codewords that could not be corrected.
Payload Header Suppression	
PHS Status	Displays whether the payload header is suppressed (on) or not (off). When on, redundant information is not transmitted.
Service Flows	
SFID	Displays the service flow ID number.
Service Class Name	Displays the service class name string that the CMTS associates with a QoS parameter set.

Label	Description
Direction	Displays the direction of the data flow.
Primary Flow	Indicates if the SFID is a primary flow or not.
Packets	Displays the quantity of packets transported on a single SFID.

5.1.4 Using the Provisioning Option

Use the **Provisioning** option to view the MTA configuration file and enterprise MIB settings.

To view telephony provisioning details:

1. Click **MTA** from the left side menu.
2. Click **Provisioning** funder MTA.

Field descriptions are listed below the screen example.

The screenshot shows a web interface for MTA provisioning. On the left is a navigation menu with 'MTA' selected, containing links for Status, DHCP, QoS, Provision, and Event Log. The main content area is titled 'Provision' and includes a sub-section for 'MTA Config File' with fields for 'Filename' (N/A) and 'Contents'. Below this is a table of 'Enterprise MIBs' with columns for 'OID' and 'Value'.

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

Label	Description
MTA Config File	
Filename	Displays the config file being used.
Contents	Displays the current settings.
Enterprise MIBs	
OID	Displays the eMTA MIBs.
Value	Displays the current value of the MIBs.

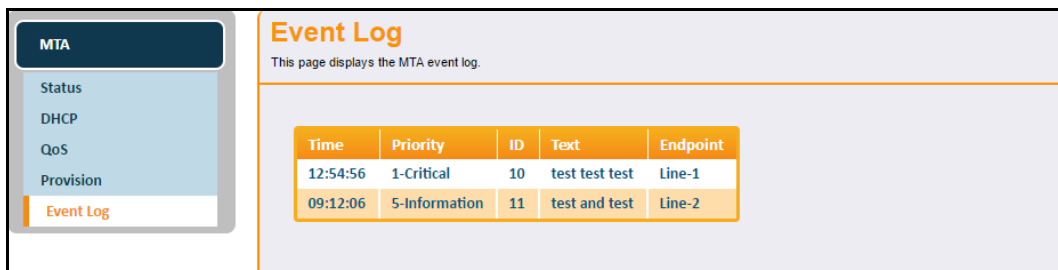
5.1.5 Using the Event Log Option

Use the Event Log to view events associated with the MTA.

To view the telephony event log:

1. Click **MTA** from the left side menu.
2. Click **Event Log** under MTA.

Field descriptions are listed below the screen example.



Label	Description
Time	Displays the time of the event.
Priority	Displays the priority level of the displayed event.
ID	Displays an identification number for the event.
Text	Defines the event with a detailed textual description.
Endpoint	Displays the endpoint name to which the event is related.

6 Understanding the Gateway Menu

The Gateway option provides the majority of configuration for the device including WAN and LAN setup, wireless settings, parental control, advanced gateway options such as MAC filtering and port forwarding, device diagnostics, and device management options.



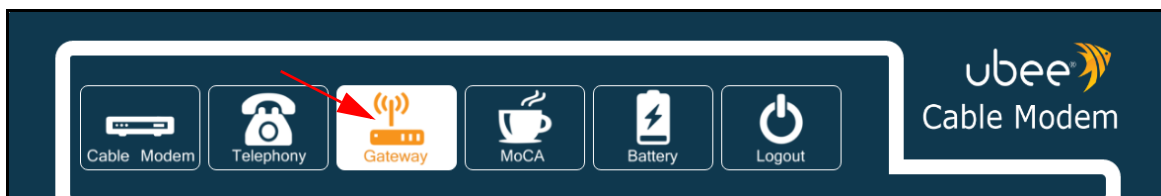
Topics

See the following topics:

- ◆ [Using the WAN Option on page 34](#)
- ◆ [Using the LAN Option on page 37](#)
- ◆ [Using the WLAN Option on page 41](#)
- ◆ [Using the Advanced Settings Options on page 54](#)
- ◆ [Using the Parental Control Option on page 71](#)
- ◆ [Using the Management Option on page 74](#)
- ◆ [Using the Diagnostics Option on page 78](#)

To access the gateway menu:

1. Access the Web user interface. Refer to [Accessing the Web User Interface Locally on page 18](#).
2. Click **Gateway** from the top main menu.



6.1 Using the WAN Option

Use the **WAN** option to view information regarding the WAN interface of the UBC1301-AA00.

To view WAN interface information:

1. Click **Gateway** from the main menu.
2. Click **WAN** on the left side menu.
3. The following sub-menus are available for selection:
 - ◆ [Using the Setup Option on page 35](#)
 - ◆ [Using the Operation Mode Option on page 36](#)

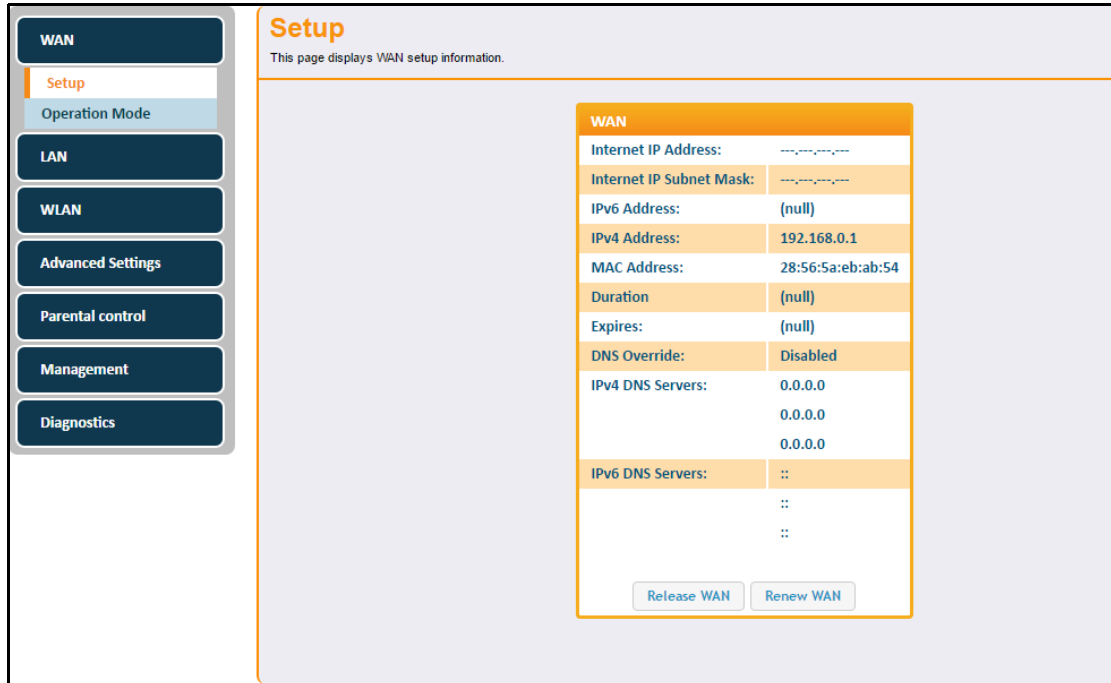
6.1.1 Using the Setup Option

The WAN Setup screen allows you to view information about the WAN interface.

To view WAN setup information:

1. Click **WAN** from the left side menu.
2. Click **Setup** under WAN.

Field descriptions are listed below the screen example.



Label	Description
WAN	
Internet IP Address	Displays the IP address for the Internet interface.
Internet IP Subnet Mask	Displays the IP subnet mask for the Internet interface.
IPv6 Address	Displays the current WAN public IPv6 address obtained from the service provider.
IPv4 Address	Displays the current WAN public IPv4 address obtained from the service provider.
MAC Address	Displays the WAN interface's hardware address.
Duration	Displays the accumulated time since successfully acquiring a WAN public IP address.
Expires	Displays the remaining time before the WAN IP address expires, if applicable.
DNS Override	Enable DNS Override to use specific host names and IP addresses instead of using DNS (Domain Name Servers) to translate host names into IP addresses.

Label	Description
IPv4 DNS Servers	Lists the IPv4 DNS servers available on the network.
IPv6 DNS Servers	Lists the IPv6 DNS servers available on the network.
Release WAN	Releases the WAN public IP address when clicked.
Renew WAN	Renews the WAN IP address when clicked.

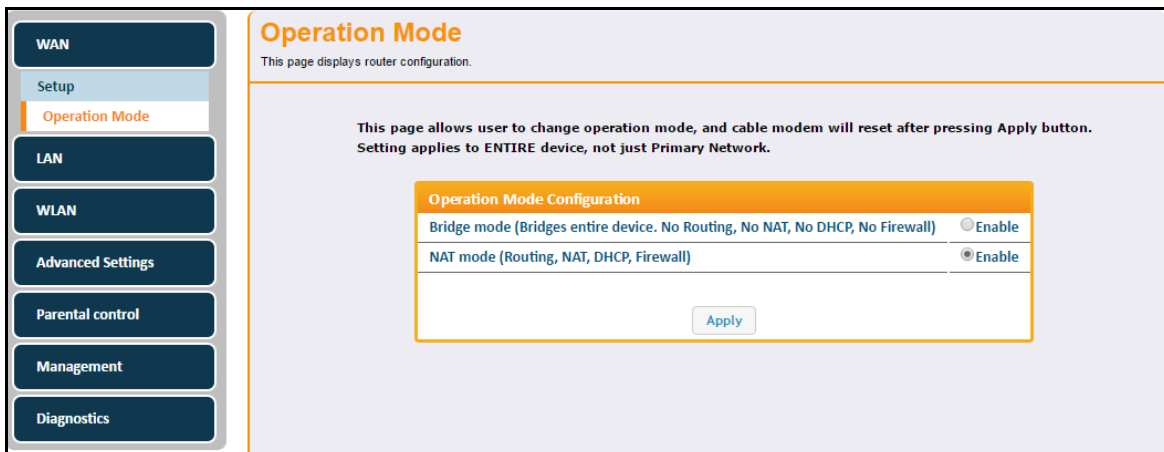
6.1.2 Using the Operation Mode Option

The WAN Operation Mode screen allows you to change the router operation mode.

To configure the router operation mode:

1. Click **WAN** from the left side menu.
2. Click **Operation Mode** under WAN.

Field descriptions are listed below the screen example.



Label	Description
Bridge mode	<p>Operates the device as a Bridge device when enabled. Bridge Mode can only be enabled when logged is an admin (vs. end user). Bridge Mode affects the entire device, meaning all networks become bridged. Only the Status and Wireless menus are visible when in Bridge mode.</p> <p>Note: If you place a device in Bridge mode, and only one public IP address has been provisioned for the customer premises equipment (CPE), i.e, a Home Router, consider disabling the Wireless SSID to avoid a wireless client inadvertently acquiring the single Public IP address assigned via DHCP.</p>
NAT mode	<p>Operates the device in network address translation (NAT) mode when enabled. NAT mode is selected by default and enables all gateway features of the UBC1303-AA00. NAT mode is the default operation mode when the device is reset to factory defaults.</p> <p>NAT mode provides a wireless access point that allows sharing a single Internet connection. Enables Layer 3 IP protocol, DHCP for private IP address assignment, NAT for network address and port translation, IP routing, firewall protection, and parental control features. Hint: All LAN and wireless LAN interfaces are on the same Private IP subnet, and are translated to a single Public IP address on the WAN gateway interface to the Internet.</p>
Apply	Applies the selected operation mode.

6.2 Using the LAN Option

Use the **LAN** option to view information regarding the LAN interfaces of the UBC1301-AA00.

To view LAN interface information:

1. Click **Gateway** from the main menu.
2. Click **LAN** on the left side menu.
3. The following sub-menus are available for selection:
 - ◆ [Using the DHCPv4 Option on page 37](#)
 - ◆ [Using the DHCPv6 Option on page 39](#)
 - ◆ [Using the DHCP Lease Option on page 41](#)

6.2.1 Using the DHCPv4 Option

The DHCPv4 screen allows you configure IPv4 DHCP (dynamic host configuration protocol) behavior.

To configure DHCPv4 settings:

1. Click **LAN** from the left side menu.
2. Click **DHCPv4** under LAN.

Field descriptions are listed below the screen example.

DHCPv4
This page displays LAN settings information.

Configure the Broadband Router IP Address and Subnet Mask for LAN interface. GroupName

IP Address:
 Subnet Mask:
 LAN firewall:

Enable UPnP
 SSDP Advertise Interval (second):

Disable DHCP Server
 Enable DHCP Server
 Start IP Address:
 End IP Address:
 Lease Time (second):

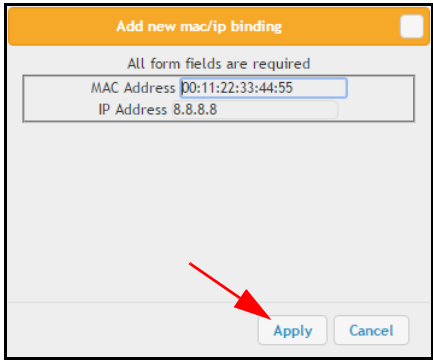
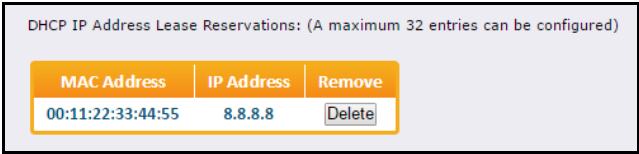
DHCP IP Address Lease Reservations: (A maximum 32 entries can be configured)

MAC Address	IP Address	Remove

Enable DHCP Server Relay
 DHCP Server IP Address:

MTU Size(256-1500):

Label	Description
GroupName	Enables you to select a group name from the drop-down menu.
IP Address	Displays the IP address of the broadband router LAN interface.
Subnet Mask	Displays the IP subnet mask for the LAN interface.
LAN Firewall	Allows you to enable or disable the firewall.
Enable UPnP	Check if you want to enable Universal Plug and Play. 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.
SSDP Advertise Interval	Allows you to set the time (in seconds) that SSDP (simple service discovery protocol) waits between advertising for discovery of UPnP devices on the network.
Disable DHCP Server	Check if you want to disable the use of a DHCP server.
Enable DHCP Server	Check if you want to enable the use of a DHCP server.
Start IP Address	Defines the starting IP address for the pool of IP addresses that can be used by connecting clients.
End IP Address	Defines the ending IP address for the pool of IP addresses that can be used by connecting clients.

Label	Description
<p>Lease Time</p>	<p>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. 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 printers, iMAC 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 IP address via DHCP.</p>
<p>Add Entries</p>	<p>Click the Add Entries button to add DHCP IPv4 Address Lease Reservations. The following pop-up window appears. Enter the MAC and IP addresses, then click Apply.</p>  <p>After clicking Apply, the lease reservation appears in the table as shown below.</p>  <p>To remove a DHCP IP lease, click the Delete button next to the entry in the table.</p>
<p>Enable DHCP Server Relay</p>	<p>Check the box to enable a host that forwards DHCP packets between clients and servers.</p>
<p>DHCP Server IP Address</p>	<p>Allows you to enter the IP Address for the DHCP Server Relay host.</p>
<p>MTU Size</p>	<p>Allows you to enter the maximum transmission unit (MTU) size. MTU defines the largest size of the packet or frame that the device can transfer (256-1500). If this is not given by your service provider, use 0 for the default.</p>
<p>Apply/Save</p>	<p>Saves all changes.</p>

6.2.2 Using the DHCPv6 Option

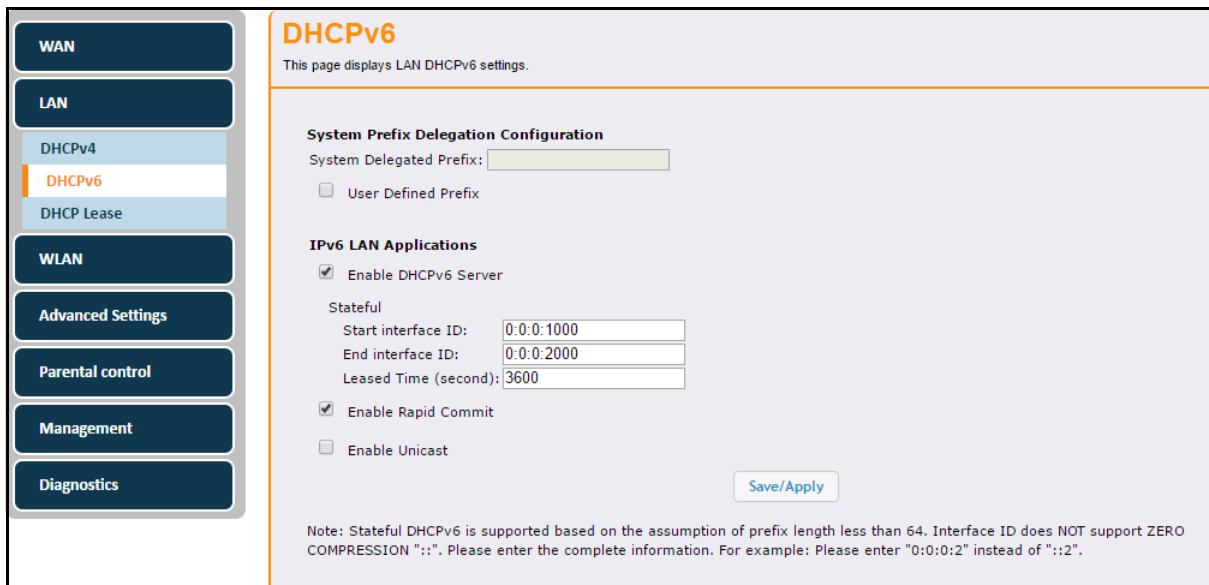
Use the **DHCPv6** option to configure IPv6 host IP addresses, IPv6 prefixes, and various configuration data required to operate in an IPv6 network.

To configure DHCPv6 settings:

1. Click **LAN** from the left side menu.

2. Click **DHCPv6** under LAN.

Field descriptions are listed below the screen example.



Label	Description
System Prefix Delegation Configuration	
System Delegated Prefix	This is the IPv6 prefix from the Setup Web UI, disabled (grayed out) by default. It is enabled buy the user defined prefix box below.
User defined prefix	Enables the System Delegated Prefix, which is disabled by default. Once enabled and Apply is clicked, the device restarts.
IPv6 LAN Applications	
Enable DHCPv6 Server	Enables the Ethernet Switch LAN Interface and Prefix.
Start interface ID	Allows you to enter the start Interface ID.
Start interface ID	Allows you to enter the end Interface ID.
Leased Time	<p>Defines the DHCPv6 lease time duration in minutes between 1 and 71582788. A DHCPv6 user’s PC gets an IPv6 address with a lease time. When the lease time expires, the PC must connect to the DHCPv6 server and be issued a new, unused IPv6 address.</p> <p>Note: The default DHCPv6 lease time is 3600. For optimum performance, it should be changes 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 IPv6 address via DHCPv6.</p>

Label	Description
Enable Rapid Commit	Enables Rapid Commit. When enabled, the server recognizes this option in Solicit messages sent from the DHCPv6 client. The server and client then use a two-message exchange (Solicit and Reply) to configure clients, rather than the default four-message exchange (Solicit, Advertise, Request, and Reply). This provides faster client configuration when networks are under heavy traffic loads.
Enable Unicast	Enables Unicast, which is disabled by default. Unicast transmission is defined to be between a single sender and a single user over a network.
Save/Apply	Saves changes.

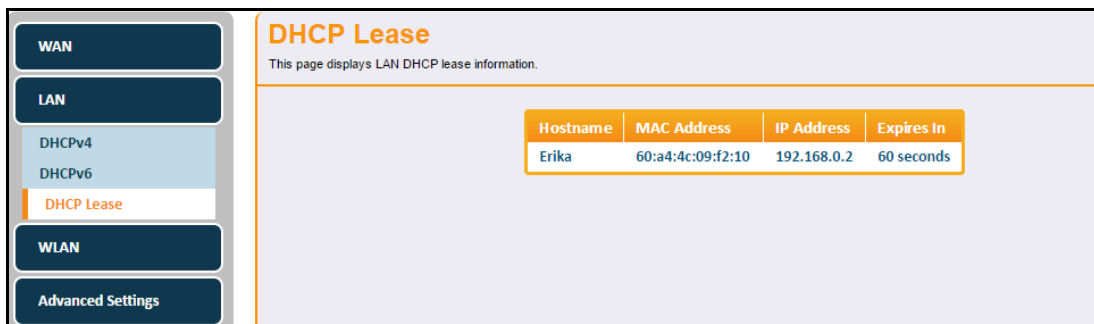
6.2.3 Using the DHCP Lease Option

Use the **DHCP Lease** option to view current LAN DHCP lease information.

To view DHCP lease settings:

1. Click **LAN** from the left side menu.
2. Click **DHCP Lease** under LAN.

Field descriptions are listed below the screen example.



Label	Description
Hostname	Displays the host name.
MAC Address	Displays the IP address of the client.
IP Address	Displays the MAC address of the client.
Expires in	Displays the time until the DHCP lease expires.

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 50](#).

To view and configure wireless information:

1. Click **Gateway** from the main menu.
2. Click **WLAN** on the left side menu.
3. The following sub-menus are available for selection:
 - ◆ [Using the Basic Option on page 42](#)
 - ◆ [Using the Security Option on page 44](#)
 - ◆ [Using the WPS Option on page 45](#)
 - ◆ [Using the Access Control Option on page 46](#)
 - ◆ [Using the WMM Option on page 48](#)

6.3.1 Using the Basic Option

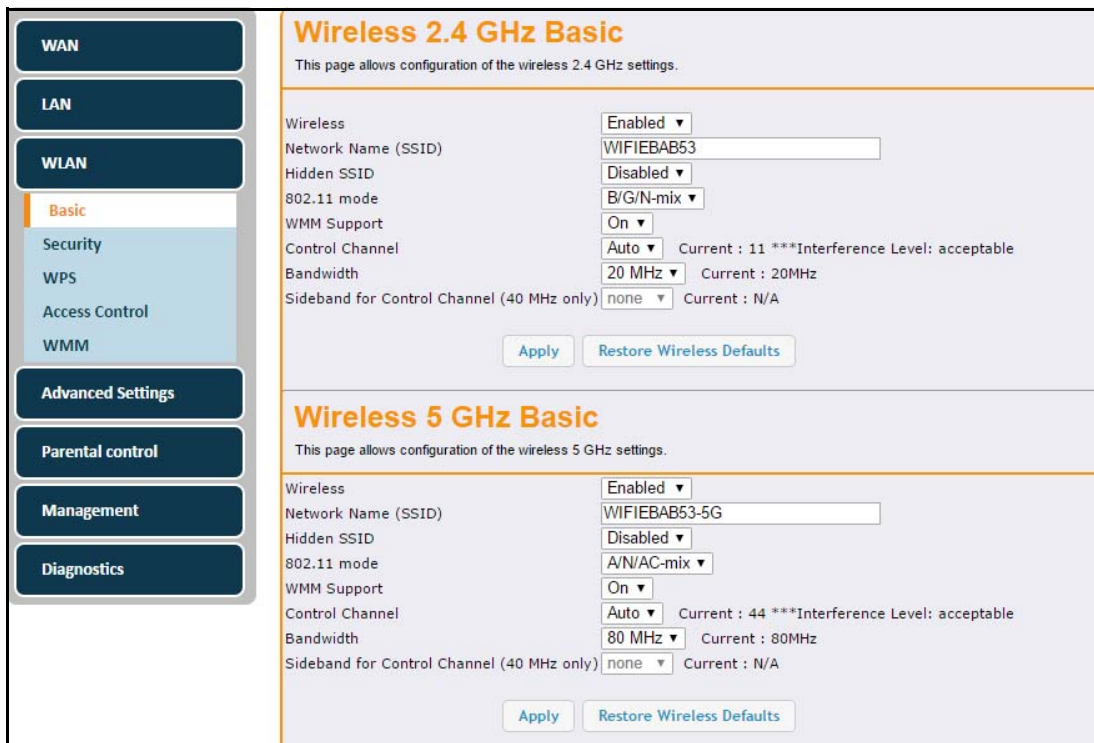
The WLAN **Basic** option allows you to configure basic settings for both the 2.4GHz and 5GHz radio bands, including channel number and bandwidth control. You can also change the SSID (wireless network name) here.

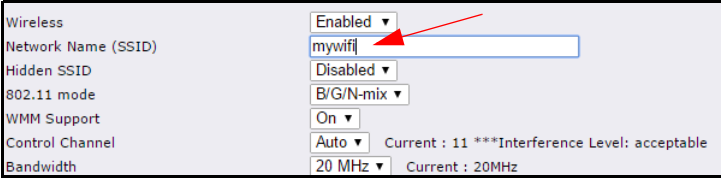
NOTE: The UBC1301-AA00 is a dual-band concurrent wireless gateway, supporting operation of both the 2.4GHz and 5GHz radio bands simultaneously. Both radios are enabled by default.

To configure basic wireless settings:

1. Click **WLAN** from the left side menu.
2. Click **Basic** under WLAN.

Field descriptions follow the screen example.



Label	Description
<p>The following fields are available for configuring the 2.4GHz and 5GHz radios.</p>	
<p>Wireless</p>	<p>Allows you to enable or disable the wireless radio. Both radios are enable by default.</p>
<p>Network Name (SSID)</p>	<p>Displays the wireless network name (SSID) to which client devices connect. It displays the default SSID.</p> <p>The default SSID for the UBC1301-AA00 is "WIFI" plus the last 6 characters of the Cable Modem MAC address (in upper case) for the 2.4GHz radio band. "-5G" is added to the end for the 5GHz radio band. The SSIDs can be found on the device label.</p> <p>If you want to change the device SSID, delete the default SSID and type in the name of your choice, then click Apply.</p> 
<p>Hidden SSID</p>	<p>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 wishing to connect to the UBC1303-AA00.</p>
<p>802.11 mode</p>	<p>Sets the wireless networking standard. Available modes for selection are:</p> <ul style="list-style-type: none"> ◆ 2.4GHz: B/G/N-mix (default), G/N-mix, B/G-mix, and N-only ◆ 5GHz: A/N/AC-mix (default), N/AC-mix, AC-only, A-only, N-only
<p>WMM Support</p>	<p>When WMM (WiFi Multimedia) support in on, quality of service (QoS) is enabled to ensure the best service in your wireless network.</p>
<p>Control Channel</p>	<p>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. The current channel number is displayed as well as the interference level. Available channels for selection are:</p> <ul style="list-style-type: none"> ◆ 2.4GHz: Auto, 1, 2, 3, 4, 5, 6, 7, 8, 9 ◆ 5GHz: Auto, 36, 52, 100, 116, 40, 56, 104, 120, 44, 60, 108, 124, 48, 64, 112, 128 <p>For more information regarding channels selection, refer to Selecting a Wireless Channel on page 53.</p>
<p>Bandwidth</p>	<p>Sets the channel bandwidth and displays the current channel bandwidth. Available bandwidths for selection are:</p> <ul style="list-style-type: none"> ◆ 2.4GHz: 20MHz, 40MHz ◆ 5GHz: 20MHz, 40MHz, 80MHz <p>NOTE:</p> <ul style="list-style-type: none"> ◆ 802.11b and 802.11g support 2.4GHz, 20MHz wide channels ◆ 802.11n supports 2.4GHz or 5GHz, 20MHz or 40MHz wide channels ◆ 802.11a supports 5GHz, 20MHz wide channels ◆ 802.11ac supports 5GHz, 20MHz, 40MHz or 80MHz wide channels

Label	Description
Sideband for Control Channel	Only when using 40MHz bandwidth should you choose the lower or upper 20MHz.
Apply	Saves changes.
Restore Wireless Defaults	Restores the factory default settings for wireless configurations when clicked.

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.

To configure wireless security:

1. Click **WLAN** from the left side menu.
2. Click **Security** under WLAN.

Field descriptions follow the screen example.



Label	Description
<p>The following fields are available for configuring the 2.4GHz and 5GHz radios.</p>	
<p>Security Mode</p>	<p>Allows selection of the security mode. Options available for selection for both radios are: WPA Personal, WPA Enterprise, Disable.</p>
<p>WPA version</p>	<p>Allows you to select the WPA version. Options available for selection for both radios are: v1/v2 Mix, Version 1, Version 2. WPA2-PSK is the most secure and most efficient. You should only enable WPA-PSK if you have a very old device that cannot support WPA2-PSK.</p> <p>NOTE: If you enable WPA-PSK, your device will be more vulnerable to attack, and your performance will suffer.</p>
<p>Encrypt Type</p>	<p>Allows you to select the encryption type. Options available for selection for both radios are: TKIP, AES, Auto.</p> <p>NOTE: AES is the most secure and efficient. You should only enable TKIP if you have a very old device that cannot support AES. TKIP will also compromise the security of your device, and will result in reduced throughput.</p>
<p>Pre-Share Key</p>	<p>Displays the pre-shared key when WPA or 802.1x network authentication is used. The pre -share key is a unique key for each device and is also called the network key or the wireless password. The default WPA pre-shared key is a randomly generated character string, 16 characters in length, and can be found on the device label. The default pre-share key is the same for both the 2.4GHz and 5GHz radios.</p> <p>NOTE: To be able to see the characters in the pre-share key (wireless password), click the Show Key button to the right side.</p> <p>If you want to change the pre-shared key, delete the default pre-shared key and type in the password of your choice, then click Apply.</p> <div data-bbox="553 1100 1273 1310" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> </div>
<p>Show Key</p>	<p>Check the Show Key box to see the pre-share key.</p>
<p>Protected Management Frame</p>	<p>When On is selected, this option allows you to increase the level of security when using WPA security modes.</p> <p>NOTE: Some printer manufacturers may not have implemented Protected Management Frames (PMF), which may result in connectivity problems. Disabling PMF may resolve the issue.</p>
<p>Apply</p>	<p>Saves changes.</p>
<p>Cancel</p>	<p>Cancels the changes.</p>

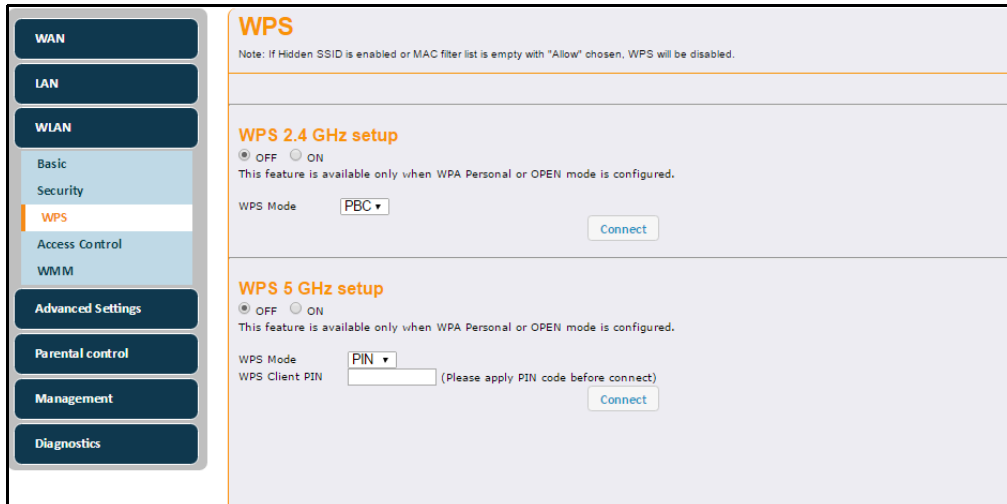
6.3.3 Using the WPS Option

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 (SSID), or pre-shared key.

To connect via WPS:

1. Click **WLAN** from the left side menu.
2. Click **WPS** under WLAN.

Field descriptions follow the screen example.



Label	Description
The following fields are available for configuring the 2.4GHz and 5GHz radios.	
WPS Enable	Check ON or OFF to enable or disable the WPS option.
WPS Mode	Allows you to choose between the 2 WPS modes: <ol style="list-style-type: none"> 1. PIN: User must enter the client WPS Pin. Note: When PIN is selected, the WPS Client Pin field will appear (as is shown in the WPS 5GHz setup section above). 2. PBC (Push Button Configuration): A software or hardware button is pushed on both the UBC1303-AA00 and the wireless client that wishes to connect. Both devices are then in registration mode.
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 button next to WPS Trigger.
Connect	Click the Connect button after entering the WPS Client Pin.

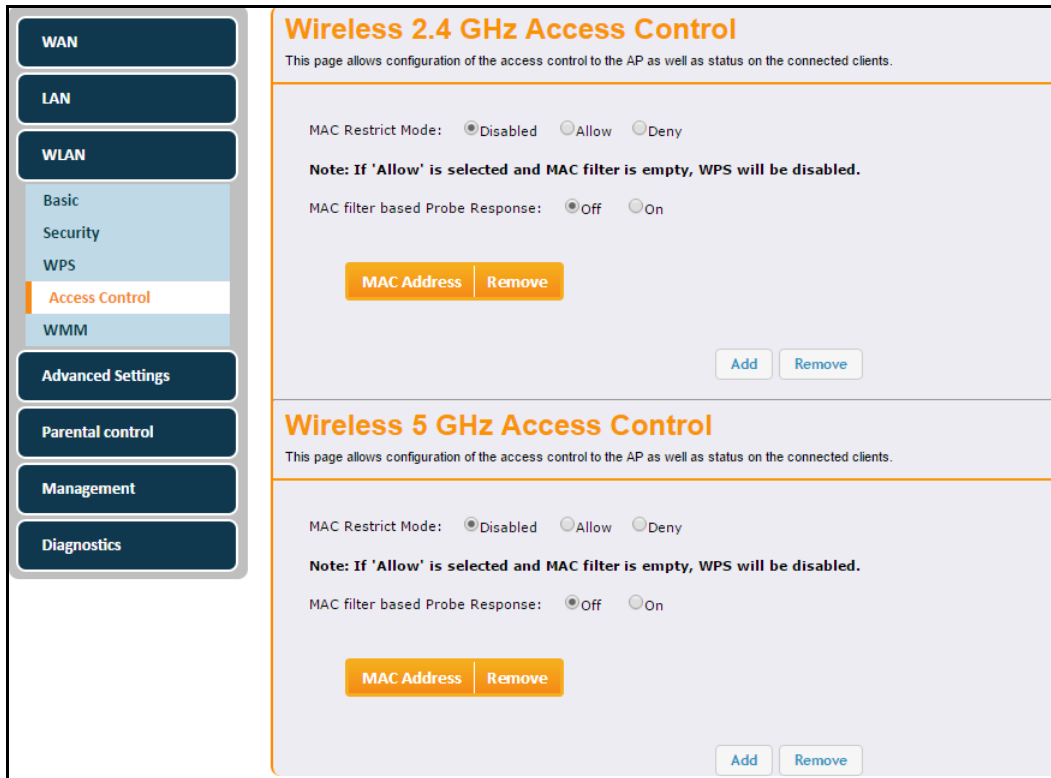
6.3.4 Using the Access Control Option

Use the **Access Control** option to configure which clients can access either the 2.4GHz or 5GHz wireless networks.

To configure wireless access:

1. Click **WLAN** from the left side menu.
2. Click **Access Control** under WLAN.

Descriptions follow the screen sample below.



Label	Description
<p>The following fields are available for configuring the 2.4GHz and 5GHz radios.</p>	
<p>MAC Restrict Mode</p>	<p>Controls wireless access to your network by MAC address.</p> <ul style="list-style-type: none"> ◆ 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. ◆ 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				
<p>MAC filter based Probe Response</p>	<p>Allows you to turn probe responses Off or On. Probe responses are sent to wireless stations that send out probe requests to discover wireless networks in their proximity.</p>				
<p>Add</p>	<p>Click the Add button to add MAC Addresses to the access control list. The pop-up window below appears.</p> <div data-bbox="711 405 1166 779" style="border: 1px solid black; padding: 5px; margin: 10px auto; width: fit-content;"> <p style="text-align: center; background-color: #f4a460; color: white; padding: 2px;">Add new mac to control list ✖</p> <p style="text-align: center; font-size: small;">All form fields are required</p> <p style="text-align: center;">MAC Address <input style="width: 100%;" type="text" value="00:11:22:33:44:55"/></p> <div style="text-align: right; padding-top: 10px;"> Apply Cancel </div> </div> <p>Enter the desired MAC Address in the field provided and click Apply. The added MAC address then appears in the table on the Access Control screen.</p> <div data-bbox="664 900 1213 1081" style="border: 1px solid black; padding: 5px; margin: 10px auto; width: fit-content;"> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #f4a460; color: white;">MAC Address</th> <th style="background-color: #f4a460; color: white;">Remove</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">00:11:22:33:44:55</td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> </tbody> </table> <div style="text-align: right; padding-top: 10px;"> Add Remove </div> </div>	MAC Address	Remove	00:11:22:33:44:55	<input type="checkbox"/>
MAC Address	Remove				
00:11:22:33:44:55	<input type="checkbox"/>				
<p>Remove</p>	<p>To remove a MAC address from the access control table, check the “Remove” box to the right of the MAC address, then click the Remove button at the bottom of the screen.</p>				

6.3.5 Using the WMM Option

Use the **WMM** (Wi-Fi Multimedia) option to enable quality of service (QoS) to ensure the best service in your wireless networks. WMM controls WLAN transmission priority on packets transmitted over the wireless network.

NOTE: Disabling WMM will break the 802.11n specification and result in speeds that tend toward a maximum speed of 54Mbps (802.11g max speeds).

To configure WMM:

1. Click **WLAN** from the left side menu.
2. Click **WMM** under WLAN.

Descriptions follow the screen sample below.

Label	Description
The following fields are available for configuring the 2.4GHz and 5GHz radios.	
Band Steering	Allows you to enable or disable band steering. Band Steering encourages dual-band capable wireless clients to connect to the less crowded 5GHz network, and leave the 2.4GHz network available for those clients who support 2.4GHz only. This helps improve Wi-Fi performance for all clients.
Airtime Fairness	Allows you to enable or disable airtime fairness. Airtime Fairness gives equal amounts of air time (instead of equal number of frames) to each wireless client regardless of its theoretical data rate. This will ensure higher download speed to faster devices when slower devices are connected to the same access point.
Traffic Scheduler	Allows you to enable or disable the traffic scheduler. Each AMPDU/NAR (Aggregated-MAC Packet Data Unit/Network Access Restriction) contributes to traffic independently when traffic is not enough. When we have more traffic to send than actual available bandwidth, each AMPDU/NAR contributes to the congestion, and all services get affected in an uncontrolled/unpredicted manner. The Traffic Schedule will control access to the common queue, so that we can control what to do when reaching over-capacity.

Label	Description
PS Pretend Retry Limit	Allows you to set the PS (Power Save) Pretend Retry Limit. Many times we consider that packet loss is due to a momentary problem that will resolve itself. PS pretend refers to the mechanism when we “pretend” that during a time period, the wireless station is doing power save. During this period, we stop sending traffic to this station and failing packets are recovered and saved to the power save queue. The retry limit is the number of times to do successive PS Pretend. The typically suggested value is around 5. In some cases, high values (10 or more) may be beneficial. A value of zero means the feature is disabled.
PS Pretend Threshold	Allows you to set the PS (Power Save) Pretend Threshold. PS pretend does not activate immediately on the first loss in threshold mode when a successive count of transmission failure reaches the threshold, then PS pretend activates. The packets prior to hitting the thresholds are lost. This offers a fix for dead link problems in multilink once the threshold is hit. With a value of 0 it is disabled. The suggested value is 5 or 10.
ACS Mode	Allows you to set the ACS (Auto Channel Selection) mode. Options are: <ul style="list-style-type: none"> ◆ SCA: Stable Channel Switching ◆ FCS: Fast Channel Switching
Apply/Save	Applies and saves changes.

6.3.6 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 50](#)
- ◆ [Estimating Wireless Cable Modem to Wireless Client Distances on page 50](#)
- ◆ [Understanding the 2.4GHz and 5GHz Bands on page 53](#)
- ◆ [Selecting a Wireless Channel on page 53](#)

6.3.6.1 Understanding Received Signal Strength

Received signal strength (RSSI) is measured from connected wireless client devices to the UBC1301-AA00. 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

6.3.6.2 Estimating Wireless Cable Modem to Wireless Client Distances

The information in this section helps you to determine how far a wireless cable modem 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 wireless cable modem and wireless clients reach the distance threshold between each other, network performance degrades.

To determine wireless gateway placement:

1. Connect a wireless client to the wireless UBC1301-AA00. Refer to [Connecting a Wireless Device on page 15](#) if needed.
2. Place the wireless client at around one meter (three feet) away from the UBC1301-AA00.
3. Obtain the **RSSI** value for the connected client. 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.
5. 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
<p>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.</p> <p>Note 2: The attenuation caused by trees varies significantly depending upon the shape and thickness of the foliage.</p>		

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

Formula:

$$(\text{Transmit Power, use } -30\text{dBm}) - (\text{Receiver Sensitivity, use RSSI value}) = \text{Allowable Free Space Loss}$$



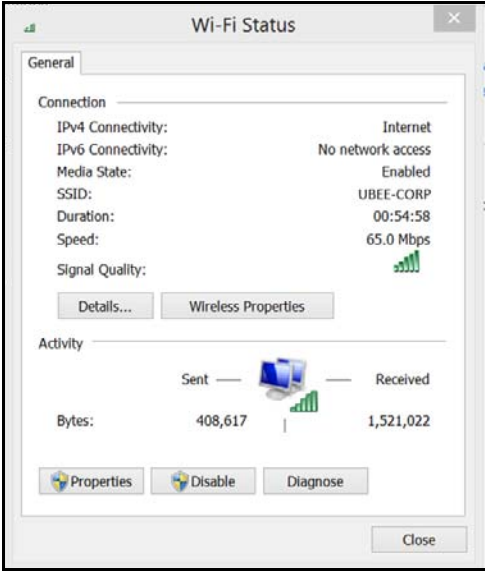
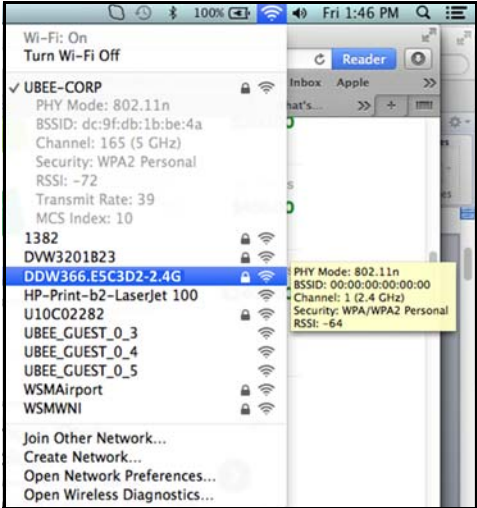
$$\text{Allowable Free Space Loss} \div \text{Materials Attenuation Value} = \text{Optimal Distance in Feet Between the UBC1301-AA00 and a Wireless Client}$$

Example:

$(-30\text{dBm}) - (-67\text{dBm}) = 37\text{dBm}$ (allowable free space loss for a 54Mbps connection)

$37\text{dBm} \div .24\text{db/foot}$ (for open space) = 154.16 feet

7. Once you know the optimal feet distance between individual wireless clients and the UBC1301-AA00, you may resolve and prevent some performance issues.
8. Check the wireless signal strength and speed of the computer connected wirelessly to the UBC1301-AA00. 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 15](#).

Checking Wireless Signal Strength and Speed	
Windows PC	Apple Mac
<p>1. Click the Wireless networking icon in the system tray to display a list of available wireless networks.</p> 	<p>1. Hold down the Option key and click on the wireless icon (Airport) on the right side of the top menu bar.</p> 
<p>2. Click "Open Network and Sharing Center," then click "Wireless Network Connection."</p>	<p>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.</p>
<p>3. Review the speed and signal strength in the Status window.</p> 	

6.3.6.3 Understanding the 2.4GHz and 5GHz Bands

The UBC1301-AA00 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
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.		

6.3.6.4 Selecting a Wireless Channel

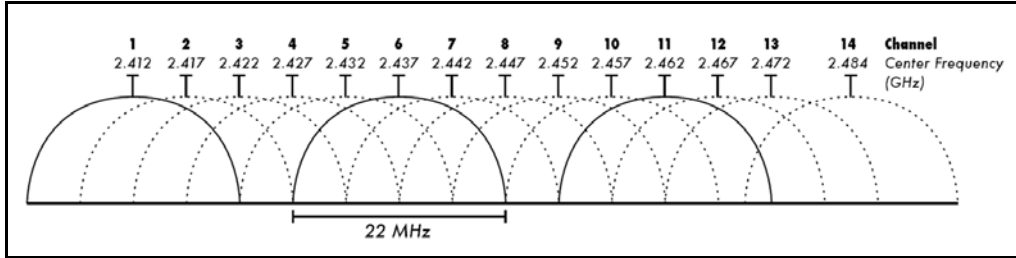
You may need to change the wireless channel on which the UBC1301-AA00 operates when you are in computing, test, and other environments where several wireless access points may be operating in the 2.4GHz range.

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 42](#).

2.4GHz Channels

The following diagram displays the 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 Settings Options

Advanced options provide many settings to configure your UBC1301-AA00.

To view Advanced Settings options:

1. Click **Gateway** from the main menu.
2. Click **Advanced Settings** on the left side menu.
3. The following sub-menus are available for selection:
 - ◆ [Using the Options option on page 55](#)
 - ◆ [Using the Firewall option on page 56](#)
 - ◆ [Using the IP Filter Option on page 57](#)
 - ◆ [Using the MAC PassThrough Option on page 58](#)

- ◆ Using the MAC Filter Option on page 59
- ◆ Using the Port Forwarding Option on page 61
- ◆ Using the Port Trigger Option on page 64
- ◆ Using the DMZ Option on page 67
- ◆ Using the DDNS Option on page 68
- ◆ Using the DNS Override Option on page 69
- ◆ Using the NTP Option on page 70

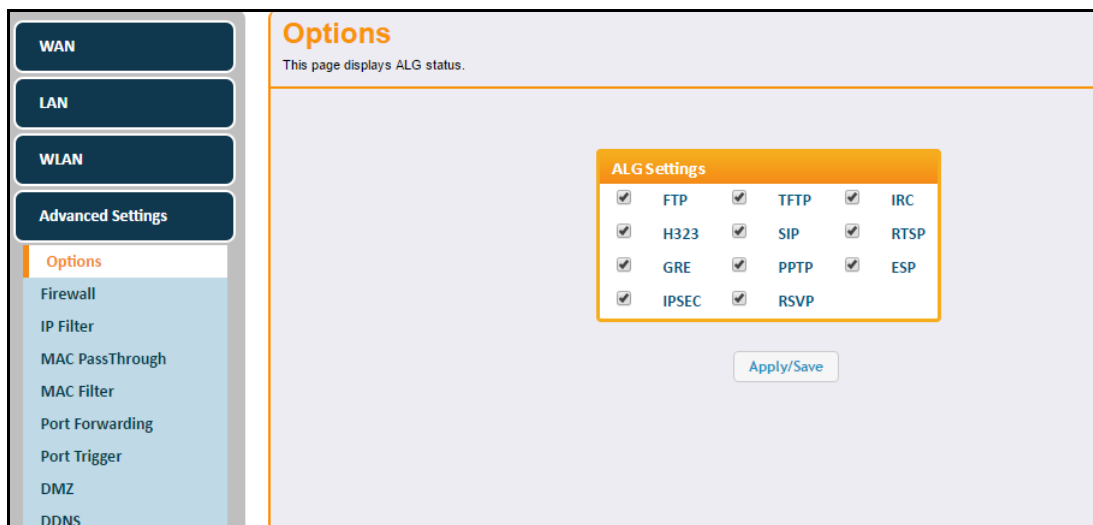
6.4.1 Using the Options option

The Options screen allows you to define which protocols are enabled or disabled on the ALG (Application Layer Gateway) of the device.

To configure ALG protocols:

1. Click **Advanced Settings** from the left side menu.
2. Click **Options** under Advanced Settings.

Field descriptions follow the screen example.



Label	Description
Settings	<p>Check the box next to each protocol to enable it:</p> <ul style="list-style-type: none"> ♦ FTP: Used to transfer files from one host to another. ♦ TFTP: Trivial file transfer protocol (TFTP) – a simpler protocol generally used for automated file transfers. ♦ IRC: Internet relay chat (IRC) protocol is used for text messaging. ♦ H323: A standard to promote compatibility in video conference transmissions over IP networks ♦ SIP: Session initiation protocol (SIP) inspects protocol packets and formats SIP message headers and SDP body to ensure proper signaling. Note: Some hosted VoIP services prefer this function to be performed by their own session border controller (SBC) and require the SIP to be disabled. Some IP-PBXs may require SIP enabled. ♦ RTSP: Real time streaming protocol (RTSP) network control protocol used to establish and control media sessions between end points. ♦ GRE: Generic route encapsulation. ♦ PPTP: Point-to-point tunneling protocol (PPTP) is used to implement a virtual private network. NOTE: If you have a Microsoft VPN client configured for access to your company network, be sure that PPTP is ENABLED. ♦ ESP: Encapsulating Security Payload. This feature helps ESP (IPsec encryption) work properly when using NAT. ♦ IPSEC: Allows encrypted IPsec VPN traffic to pass through the router between the IPsec VPN Client application on the PVC/Mac and the IPsec VPN Concentrator (e.g. Barracuda, Cisco, Juniper, etc.) for access to the “company VPN.” NOTE: If you have a Cisco AnyConnect VPN client or CheckPoint VPN client that supports IPsec, be sure that IPSEC is ENABLED. ♦ RSVP: Resource reservation protocol (RSVP) defines how applications reserve resources and how they free the reserved resources once they are no longer needed.
Apply/Save	Saves changes.

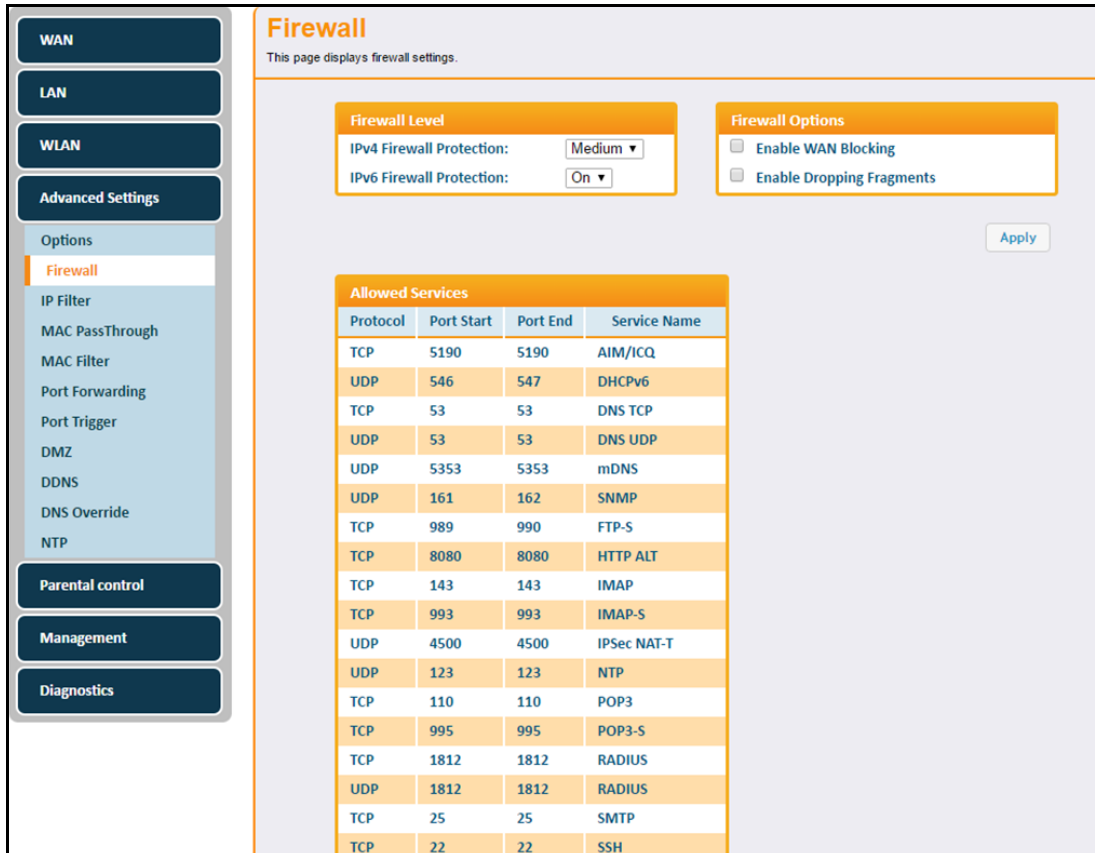
6.4.2 Using the Firewall option

The **Firewall** screen allows you to select firewall settings and enable firewall options.

To configure firewall settings:

1. Click **Advanced Settings** from the left side menu.
2. Click **Firewall** under Advanced Settings.

Field descriptions follow the screen example.



Label	Description
Firewall Level	
IPv4 Firewall Protection	Defines the level of IPv4 protection. Choices are Off, Low, Medium, High. Services are based on the protection level and are displayed in the Allowed Services section.
IPv6 Firewall Protection	Defines the level of IPv6 protection. Choices are On and Off. Services are based on the protection level and are displayed in the Allowed Services section.
Firewall Options	
Enable WAN Blocking	When enabled, WAN Blocking 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.).
Enable Dropping Fragments	When enabled, Dropping Fragments prevents all fragmented IP packets from passing through the firewall.
Allowed Services	Lists the allowed services based upon the selected firewall levels and options.
Apply	Saves changes.

6.4.3 Using the IP Filter Option

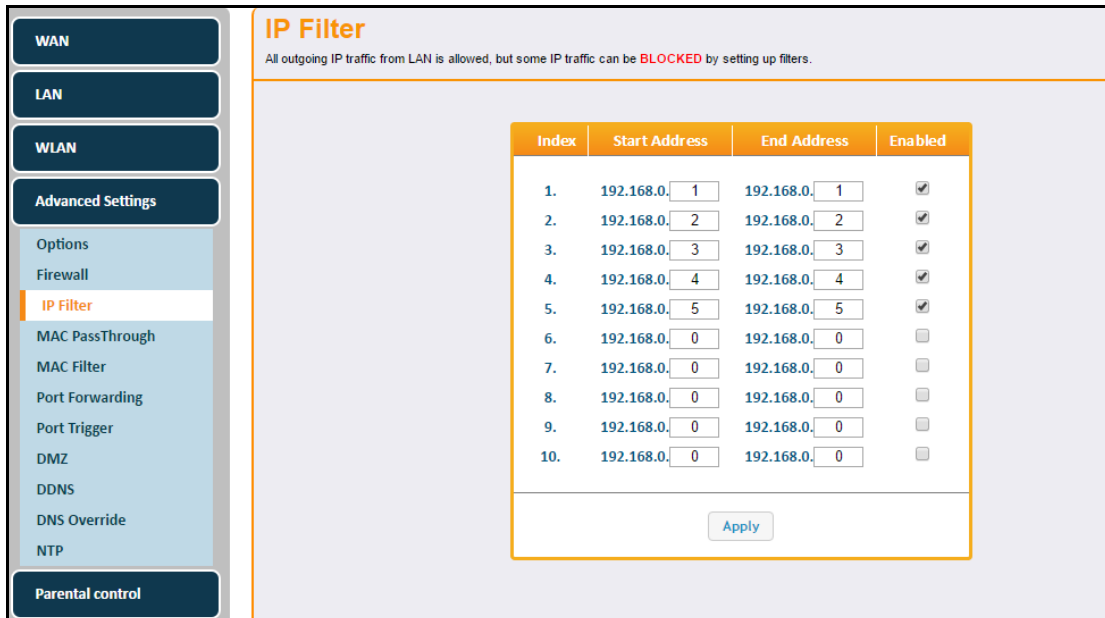
Use the **IP Filter** option to filter IP addresses to block Internet traffic to specific network devices on the LAN. Any host on this list is not accessible to Internet traffic.

NOTE: You may also filter by the MAC address which does not require setting a static lease. Refer to [Using the MAC Filter Option on page 59](#).

To set up IP Filters:

1. Click **Advanced Settings** from the left side menu.
2. Click **IP Filter** under Advanced Settings.

Field descriptions are listed below the screen example.



Label	Description
Index	Numbers the IP addresses to be blocked.
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.

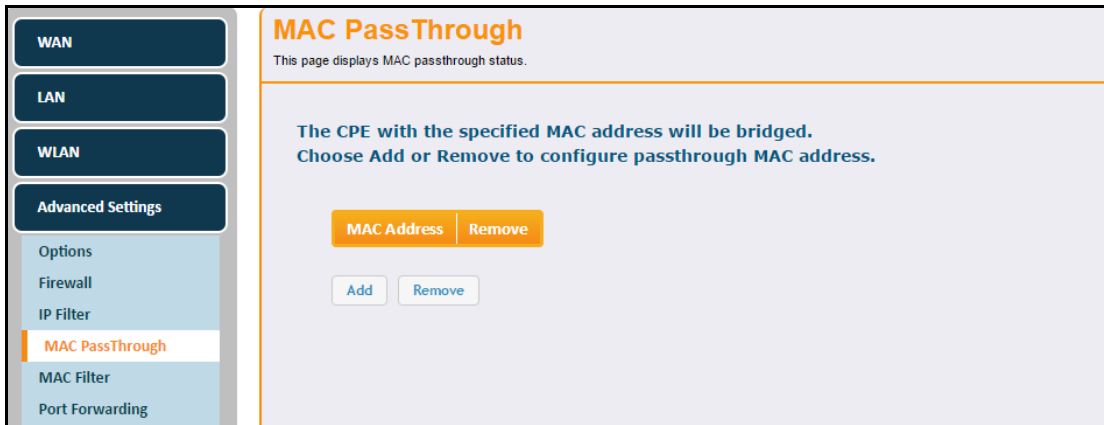
6.4.4 Using the MAC PassThrough Option

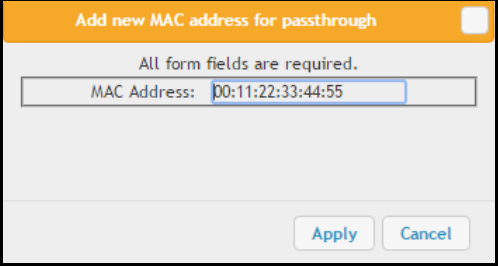
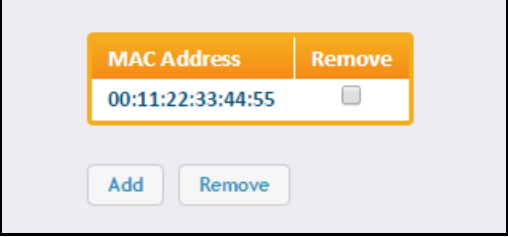
Use the **MAC PassThrough** option to configure a pass through table. Devices in the pass through table are treated as bridge devices, storing and forwarding data between LAN interconnections.

To configure a MAC PassThrough Address:

1. Click **Advanced Settings** from the left side menu.
2. Click **MAC PassThrough** under Advanced Settings.

Field descriptions are listed below the screen example.



Label	Description
<p>Add</p>	<p>Click the Add button to add MAC Addresses to the pass through table. The pop-up window below appears.</p>  <p>Enter the desired MAC Address in the field provided and click Apply. The added MAC address then appears in the table on the MAC PassThrough screen.</p> 
<p>Remove</p>	<p>To remove a MAC address from the passthrough table, check the “Remove” box to the right of the MAC address, then click the Remove button at the bottom of the screen.</p>
<p>Apply</p>	<p>Saves changes.</p>

6.4.5 Using the MAC Filter Option

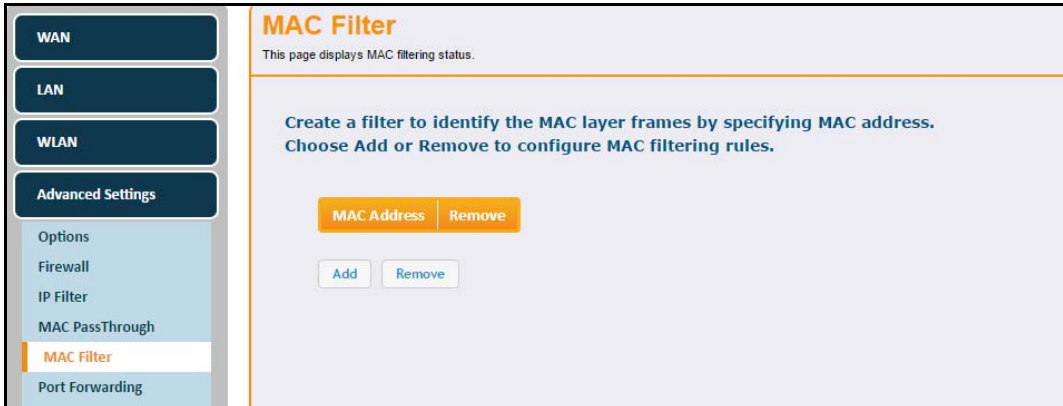
Use the **MAC Filter** option to filter MAC addresses to block Internet traffic from specific network devices on the LAN. MAC filtering establishes a list and any host on this list is not able to access the network through the UBC1301-AA00.

You must 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 UBC1301-AA00 network.

To configure a MAC Filter:

1. Click **Advanced Settings** from the left side menu.
2. Click **MAC Filter** under Advanced Settings.

Field descriptions are listed below the screen example.



Label	Description						
<p>Add</p>	<p>Click the Add button to add MAC Addresses to the MAC filter table. The pop-up window below appears.</p> <div data-bbox="659 1087 1133 1346" style="border: 1px solid black; padding: 5px; margin: 10px auto; width: fit-content;"> <p style="text-align: center; background-color: #f4a460; padding: 2px;">Add new mac filter ✖</p> <p style="text-align: center; font-size: small;">All form fields are required.</p> <p style="text-align: center;">MAC Address: <input style="width: 150px;" type="text" value="00:11:22:33:44:55"/></p> <p style="text-align: right; padding-top: 10px;"> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> </p> </div> <p>Enter the desired MAC Address in the field provided and click Apply. The added MAC address then appears in the table on the MAC Filtering screen.</p> <div data-bbox="719 1438 1073 1644" style="border: 1px solid black; padding: 5px; margin: 10px auto; width: fit-content;"> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="background-color: #f4a460; padding: 2px;">MAC Address</td> <td style="background-color: #f4a460; padding: 2px;">Remove</td> </tr> <tr> <td style="padding: 2px;">00:11:22:33:44:55</td> <td style="text-align: center; padding: 2px;"><input type="checkbox"/></td> </tr> <tr> <td colspan="2" style="padding-top: 10px; text-align: center;"> <input type="button" value="Add"/> <input type="button" value="Remove"/> </td> </tr> </table> </div>	MAC Address	Remove	00:11:22:33:44:55	<input type="checkbox"/>	<input type="button" value="Add"/> <input type="button" value="Remove"/>	
MAC Address	Remove						
00:11:22:33:44:55	<input type="checkbox"/>						
<input type="button" value="Add"/> <input type="button" value="Remove"/>							

6.4.6 Using the Port Forwarding Option

Forwarding tells the UBC1301-AA00 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

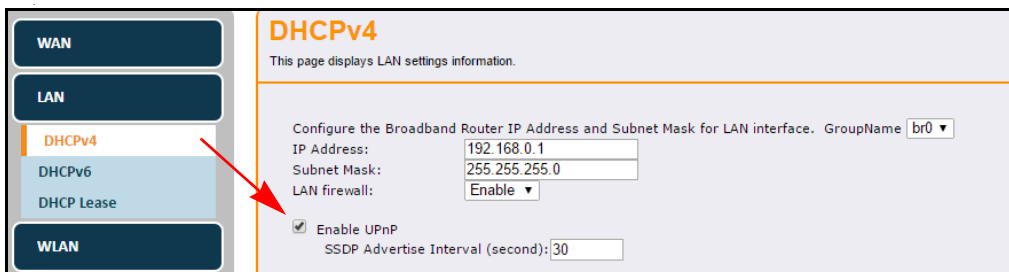
See the following topics:

- ◆ [Before Setting Up Forwarding on page 61](#)
- ◆ [Setting Up Forwarding on page 62](#)

6.4.6.1 Before Setting Up Forwarding

Try the following options before you assign forwarding rules:

1. Enable Universal Plug and Play (UPnP) on the [Using the DHCPv4 Option on page 37](#). This may resolve the issue you have without setting up forwarding rules.
 - a. Access the Web interface of the UBC1301-AA00, see [Accessing the Web User Interface Locally on page 18](#).
 - b. Click **Gateway** from the top main menu.
 - c. Click **LAN** from the left menu.
 - d. Click **DHCPv4** under the LAN menu
 - e. Check the **Enable UPnP** box



- 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.

6.4.6.2 Setting Up Forwarding

If the suggestions in [Before Setting Up Forwarding on page 61](#) did not correct your communication problem, use port forwarding.

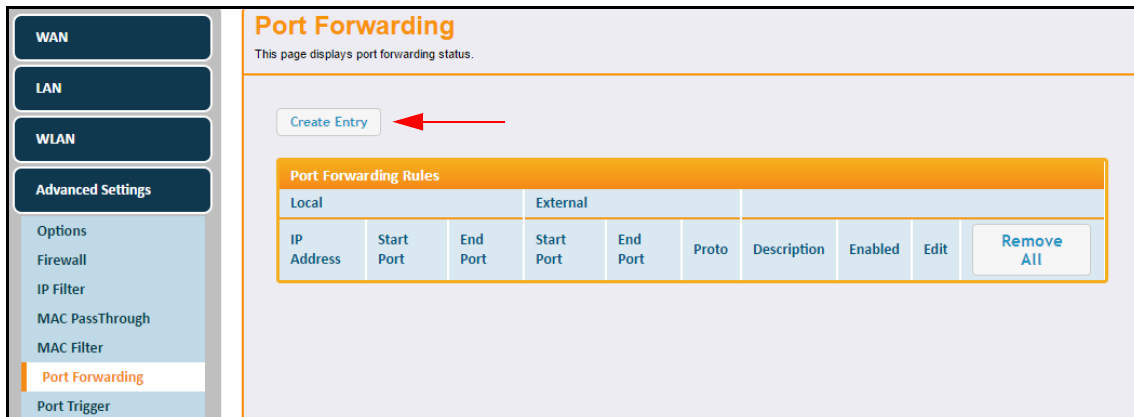
You need the following information to set up port forwarding:

- ◆ **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.

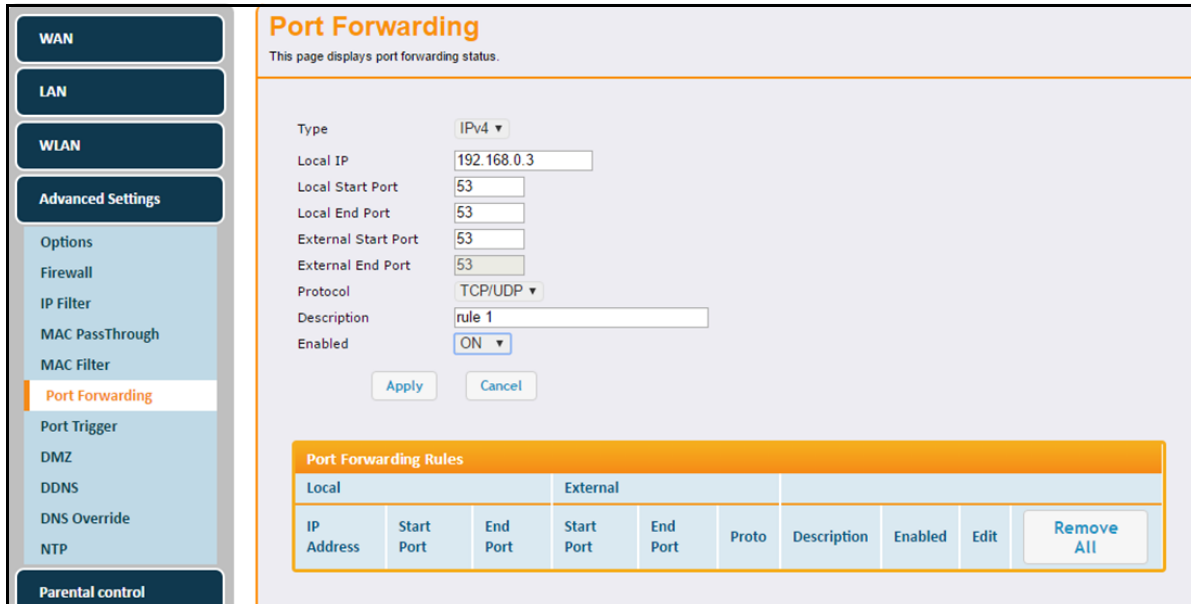
NOTE: For detailed information on port forwarding, including how to set it up for specific applications using specific network devices (for example, cable modems), refer to: <http://portforward.com> or consult your host device or application user manual.

To set up Port Forwarding:

1. Click **Advanced Settings** from the left side menu.
2. Click **Port Forwarding** under Advanced Settings.
3. Click the **Create Entry** button to begin setting up port forwarding.



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



Label	Description
Type	Allows you to select either IPv4 or IPv6.
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 Point	Defines the ending port number listened to by the server host located in your LAN.
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 TCP, UDP or TCP/UDP.
Description	Specifies the forwarding rule name.
Enabled	Disables (Off) or enables (On) the forwarding rule.
Apply	Saves the forwarding rule.
Cancel	Cancel the rule.

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

Create Entry

Port Forwarding Rules									
Local			External						
IP Address	Start Port	End Port	Start Port	End Port	Proto	Description	Enabled	Edit	Remove All
192.168.0.3	53	53	53	53	TCP/UDP	rule 1	Yes	Edit	Remove

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

6.4.6.3 Setting Up Port Forwarding for an Xbox

The following is an example of how to 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 configured for each port. Multiple ports and forwarding rules may not be required for other applications.

WAN

LAN

WLAN

Advanced Settings

- Options
- Firewall
- IP Filter
- MAC PassThrough
- MAC Filter
- Port Forwarding**
- Port Trigger

Port Forwarding
This page displays port forwarding status.

Create Entry

Port Forwarding Rules									
Local			External						
IP Address	Start Port	End Port	Start Port	End Port	Proto	Description	Enabled	Edit	Remove All
192.168.0.3	53	53	53	53	TCP/UDP	rule 1	Yes	Edit	Remove
192.168.0.4	80	80	80	80	TCP/UDP	rule 2	Yes	Edit	Remove
192.168.0.5	88	88	88	88	TCP/UDP	rule 2	Yes	Edit	Remove
192.168.0.8	3074	3074	3074	3074	TCP/UDP	rule 4	Yes	Edit	Remove

6.4.7 Using the Port Trigger Option

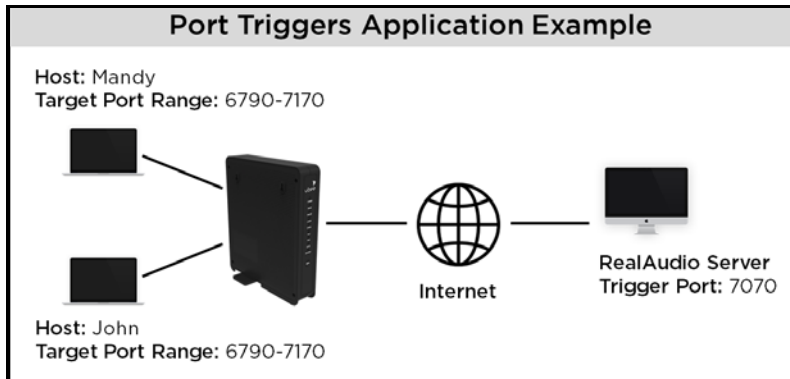
Port Triggers define dynamic triggers for specific devices on the LAN. This allows special applications that require specific port numbers with bi-directional traffic to function properly. Applications such as video conferencing, voice, gaming, and some messaging program features may require these special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

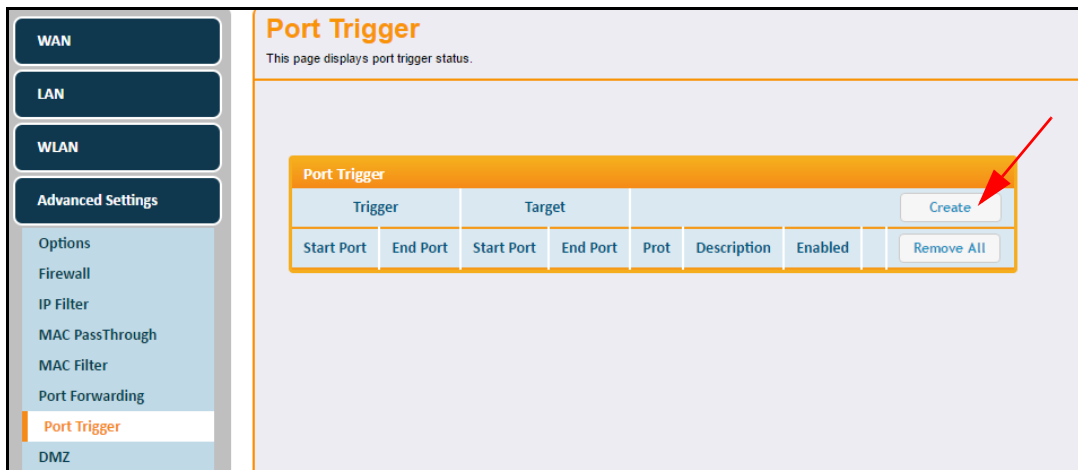
For example:

1. John requests a file from the RealAudio server (port 7070). Port 7070 is a “trigger” port and causes the device to record John’s computer IP address. The UBC1301-AA00 associates John’s computer IP address with the “target” port range of 6970-7170.
2. The RealAudio server responds to a port number ranging between 6970-7170.
3. The UBC1301-AA00 forwards the traffic to John’s computer IP address.
4. Only John can connect to the RealAudio server until the connection is closed or expires.

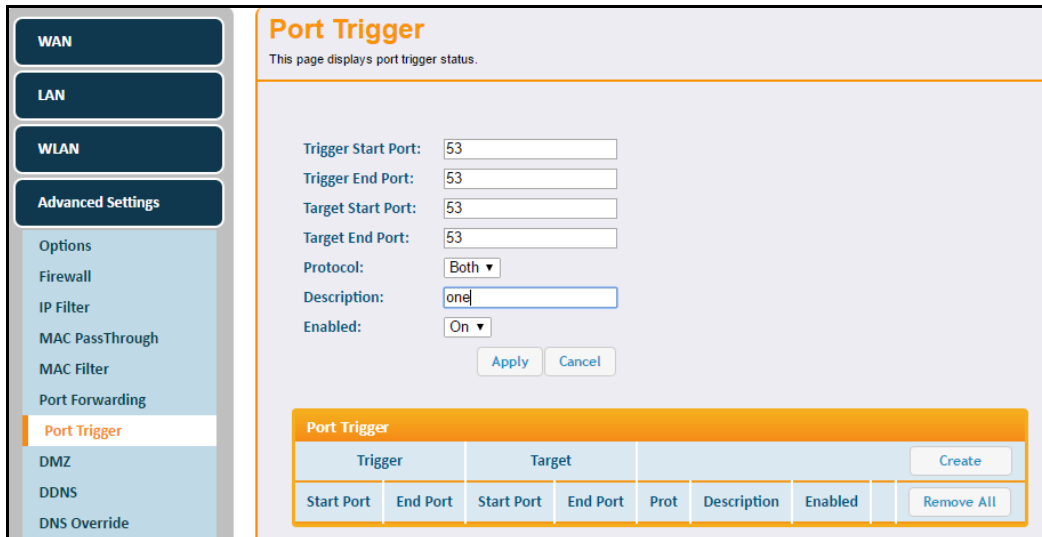


To set up Port Triggers:

1. Click **Advanced Settings** from the left side menu.
2. Click **Port Trigger** under Advanced Settings.
3. Click the **Create** button to begin setting up port triggers.

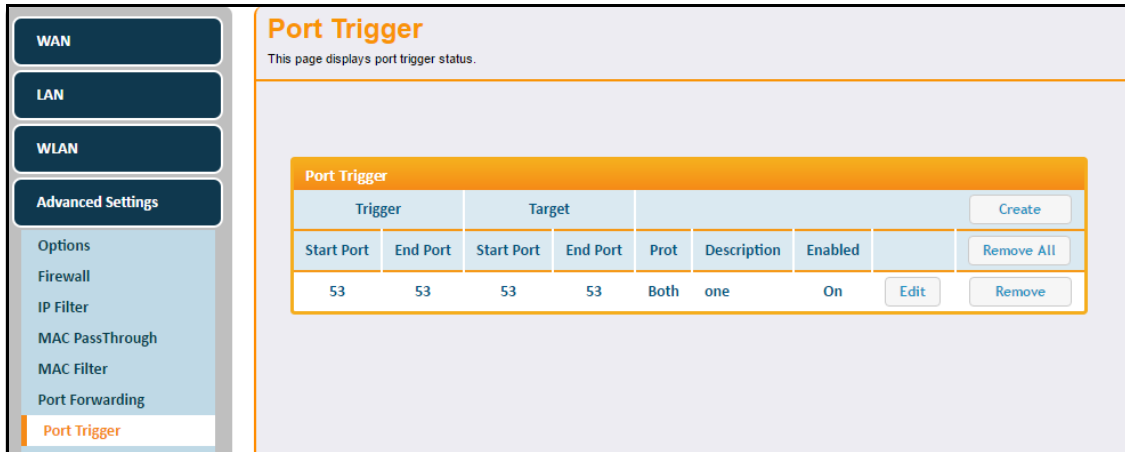


4. Enter information in the port trigger fields as shown in the screen shot below. Field descriptions follow.



Label	Description
Trigger Start Port	Defines a port number or the starting port number in a range of port numbers.
Trigger End Port	Defines a port number or the ending port number in a range of port numbers.
Target Start Port	Defines a port number or the starting port number in a range of port numbers.
Target End Port	Defines a port number or the ending port number in a range of port numbers.
Protocol	Defines the protocol type for this rule, UDP, TCP, or Both.
Description	Names the triggering rule.
Enabled	Enables (on) or disables (off) the triggering rule.
Apply	Saves the triggering rule.
Cancel	Cancels the triggering rule.

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



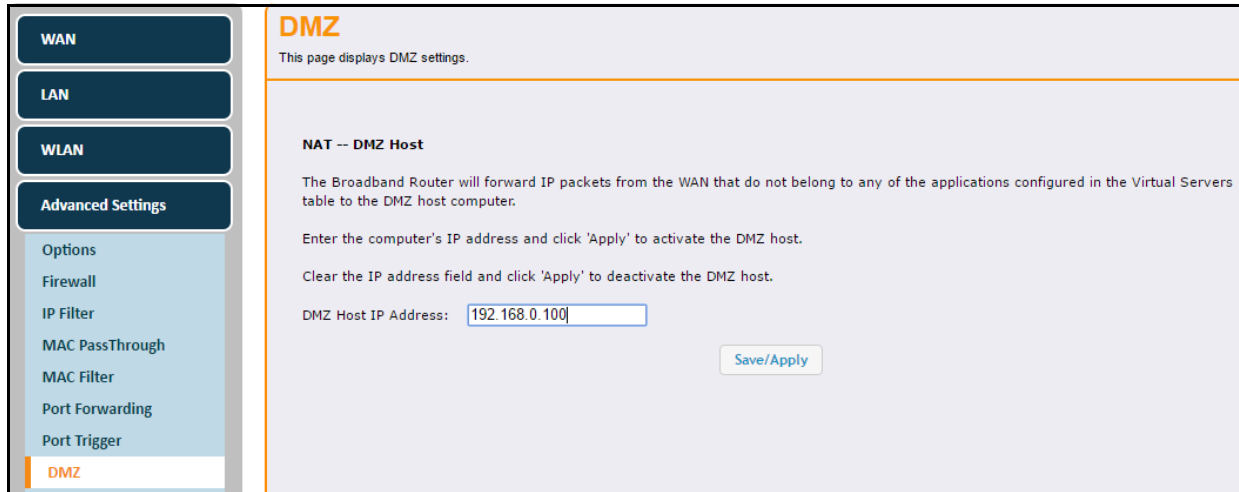
Label	Description
Edit	Displays fields for the rule selected in order to change values.
Remove All	Deletes all entries in the forwarding table.
Remove	Deletes the selected rule.

6.4.8 Using the DMZ Option

Use the **DMZ** (Demilitarized Zone) option to expose a host IP address to the WAN (public Internet). A **DMZ** allows one IP address (or computer) to be placed in between the firewall and the Internet (usually for gaming and video conferencing). This allows risky, open access to the Internet. You can use this option when applications do not work with port triggers or other networking strategies.

To set up a DMZ host:

1. Connect a PC to an Ethernet port on the UBC1301-AA00. 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 UBC1301-AA00.
3. Log in to the UBC1301-AA00 Web user interface.
4. Click **Gateway** from the top main menu.
5. Click **Advanced Settings** from the left side menu.
6. Click **DMZ** under Advanced Settings.
7. Enter the DMZ Host IP address in the appropriate field.
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 calls from a VoIP phone.



Label	Description
DMZ Host IP Address	Allows you to enter the IP address of the host to be exposed.
Save/Apply	Saves changes.

6.4.9 Using the DDNS Option

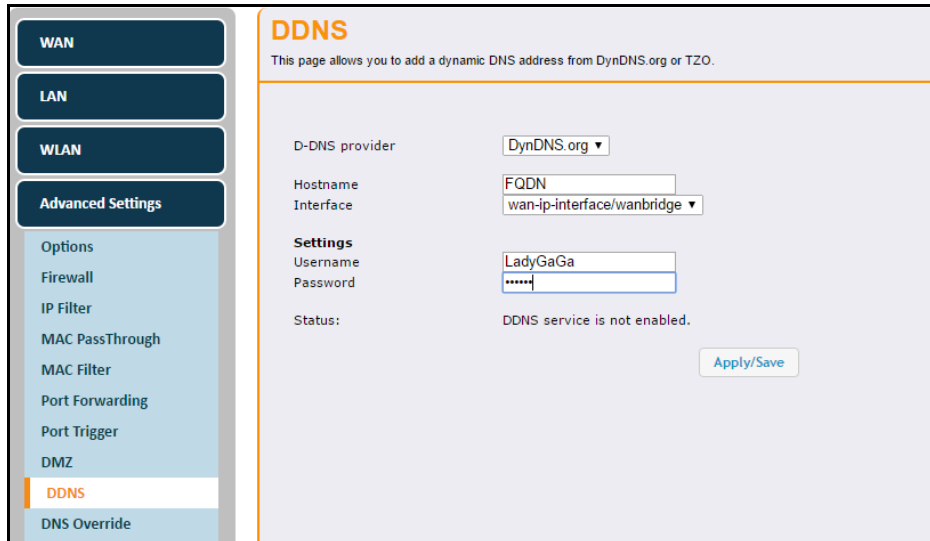
Use the **DDNS** (dynamic domain name system) to assign a changing IP address to a constant pre-defined host name. The host can then be contacted by other hosts on the Internet, even if its IP address changes.

The DDNS service for the UBC1301-AA00 is provided through third-parties and can be purchased from: Dynamic Network Services Inc. at www.dynDNS.com, or TZO at www.tzo.com.

To add a DDNS Address:

1. Click **Advanced Settings** from the left side menu.
2. Click **DDNS** under Advanced Settings.

Field descriptions are listed below the screen example.



Label	Description
D-DNS provider	Enables selection of the DDNS provider. Options are www.dynDNS.org and TZO.
Hostname	Allows you to enter a host name for the DDNS account.
Interface	Displays the interface for the DDNS account.
User Name	Allows you to enter a user name for the DDNS account.
Password	Allows you to enter a password for the DDNS account.
Status	Displays whether DDNS service is enabled.
Apply/Save	Saves changes.

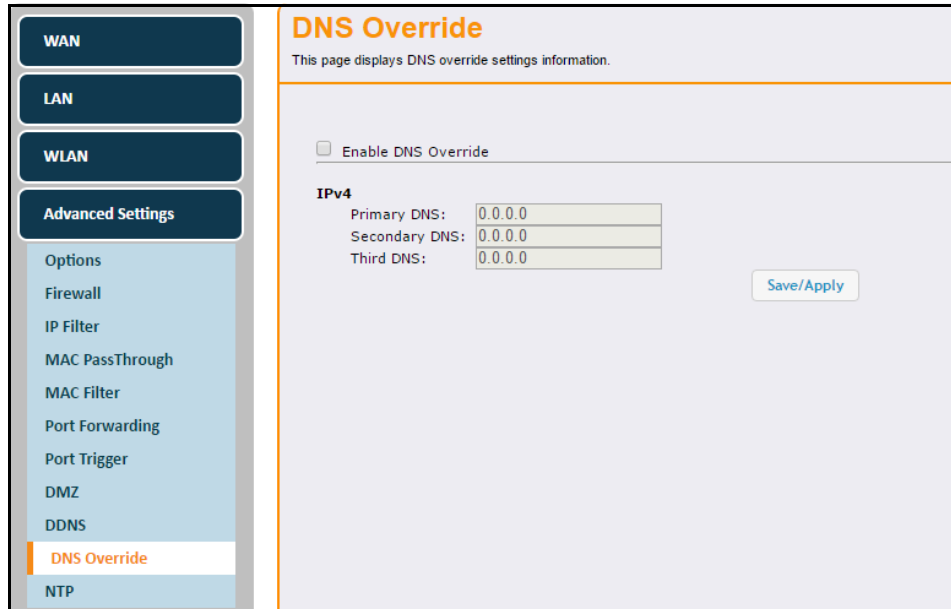
6.4.10 Using the DNS Override Option

The DNS Override option allows you to specify host IP addresses to use instead of using Domain Name System (DNS) servers to translate host names into IP addresses.

To configure DNS Overrides:

1. Click **Advanced Settings** from the left side menu.
2. Click **DNS Override** under Advanced Settings.

Field descriptions are listed below the screen example.



Label	Description
Enable DNS Override	Click the box to enable DNS Override.
IPv4	
Primary DNS	Enter the IP address for the primary DNS.
Secondary DNS	Enter the IP address for the secondary DNS.
Third DNS	Enter the IP address for the third DNS.
Save/Apply	Saves changes.

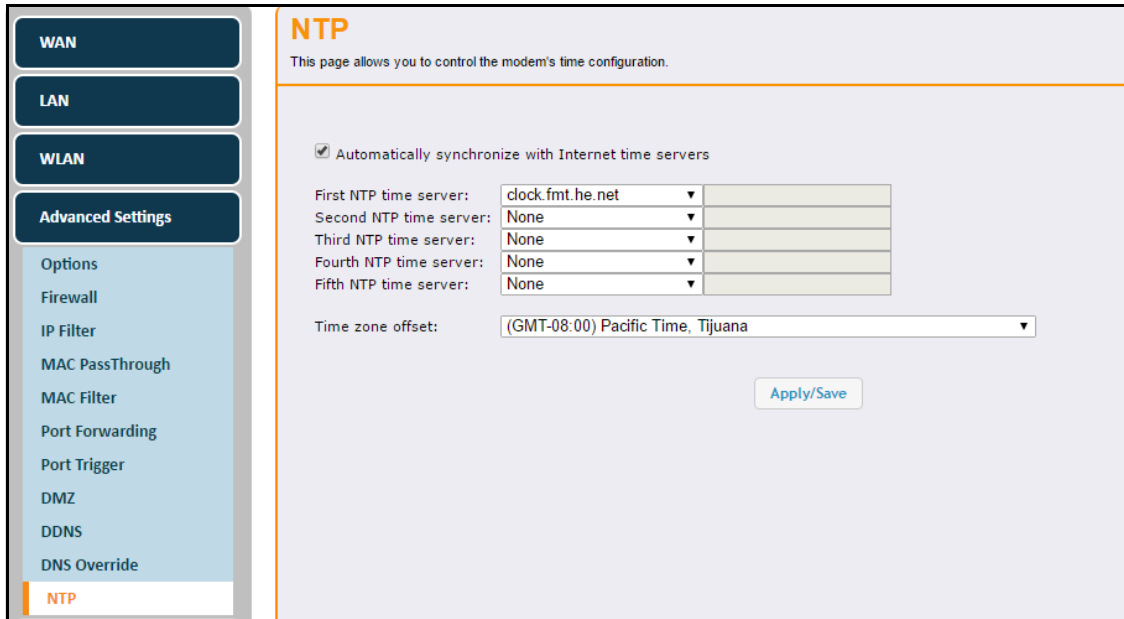
6.4.11 Using the NTP Option


The **NTP (Network Time Protocol)** option lets you set the UBC1301-AA00 to automatically synchronize with Internet Time servers via Simple Network Time Protocol (SNTP). SNTP is a protocol for synchronizing the clocks of computing devices over networks.

To synchronize with Internet Time:

1. Click **Advanced Settings** from the left side menu.
2. Click **NTP** under Advanced Settings.

Field descriptions are listed below the screen sample.



Label	Description
Automatically synchronize with Internet time servers	Check the box to automatically synchronize with Internet time servers. The Time Server and Time Zone Offset fields are only visible after checking the box to enable.
First - Fifth NTP time Servers	Select the NTP server from the drop-down menus to select the first, second, third, fourth, and fifth time servers. Options for each are: 
Time zone offset	Select the appropriate time zone from the drop-down menu.
Apply/Save	Applies the changes.

6.5 Using the Parental Control Option

Use the **Parental Control** option to configure access policies for the UBC1301-AA00.

To configure Parental Control Options:

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

◆ [Using the ToD Filter Option on page 72](#)

6.5.1 Using the ToD Filter Option

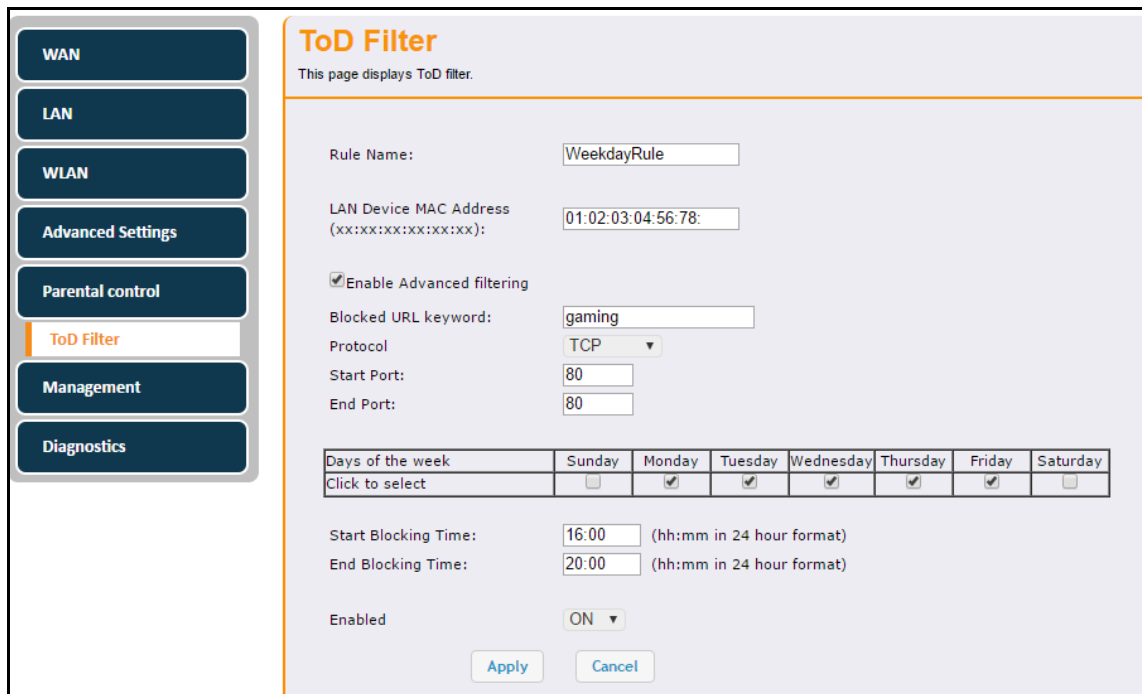
Use the **ToD (Time of Day) Filter** option to configure time-based access policies to block or allow access to specific Internet sites.

To set up Time of Day Filters:

1. Click **Parental Control** from the left side menu.
2. Click **ToD Filter** under Parental Control.
3. Click the **Create Entry** button to begin setting up time of day filters.



4. Enter information in the Time of Day Filter fields as shown in the screen shot below. Field descriptions follow.



Label	Description
Rule Name	Allows you to name the access rule.
LAN Device MAC Address	Enter the MAC address to be blocked or allowed.
Enable Advanced Filtering	Check the box to enable advanced time of day filtering. When this box is checked, the next 4 fields are available.
Blocked URL Keyword	Enter a URL or keyword to be blocked.
Protocol	Select the protocol type. Options are UDP, TCP, or Both.
Start Port	Enter the starting port number to be blocked or allowed.
End Port	Enter the ending port number to be blocked or allowed.
Days of the Week	Select the days to block Internet access.
Start Blocking Time	Enter the time (in 24-hour format) to start blocking Internet access on the days selected above.
End Blocking Time	Enter the time (in 24-hour format) to end blocking Internet access on the days selected above.
Enabled	Activates a policy when On is selected.
Apply	Applies the rule.
Cancel	Cancel the rule.

- Click **Apply**. The Time of Day rule is created and displayed in the table as shown below. Additional field descriptions follow.

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

6.6 Using the Management Option

Use the **Management** option to change the device user name and password, backup or restore the device configuration, and reset the device to factory default settings.

To configure Management Options:

1. Click **Gateway** from the main menu.
2. Click **Management** on the left side menu.
3. The following sub-menu is available for selection:
 - ◆ [Using the Account Option on page 74](#)
 - ◆ [Using the Backup/Restore Option on page 75](#)
 - ◆ [Using the Factory Default Option on page 76](#)
 - ◆ [Using the Client List Option on page 77](#)

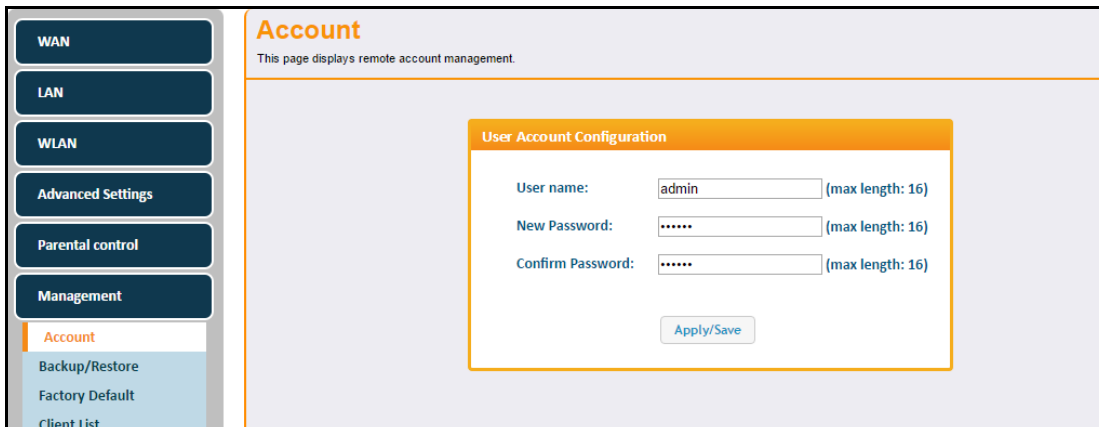
6.6.1 Using the Account Option

Use the **Account** option to change the user name and password for access to the UBC1301-AA00. Field descriptions are listed below the screen example.

To change the user name and password:

1. Click **Management** from the left side menu.
2. Click **Account** under Management.

Field descriptions are listed below the screen example.



Label	Description
User name	Enter the new User name.
New Password	Enter the new Password.
Confirm Password	Confirm the new Password.
Apply/Save	Saves the changes.

6.6.2 Using the Backup/Restore Option

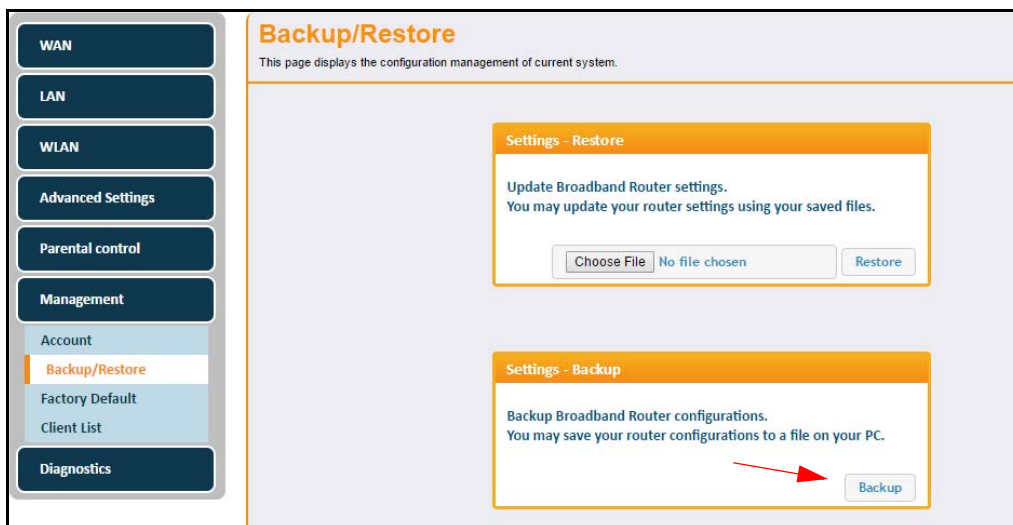
The Backup option lets you backup your gateway configuration or restore the UBC1301-AA00 to a previously saved configuration.

To back up or restore the gateway configuration:

1. Click **Management** from the left side menu.
2. Click **Backup/Restore** under Management.

6.6.2.1 Backing Up the Current Configuration

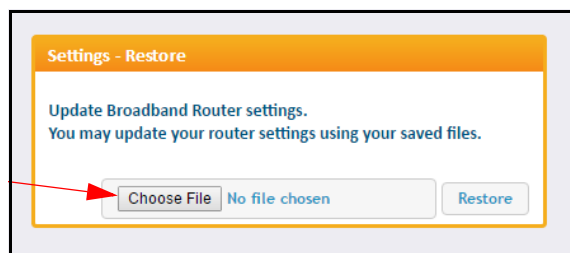
To backup and save the current device configuration, click the **Backup** button.



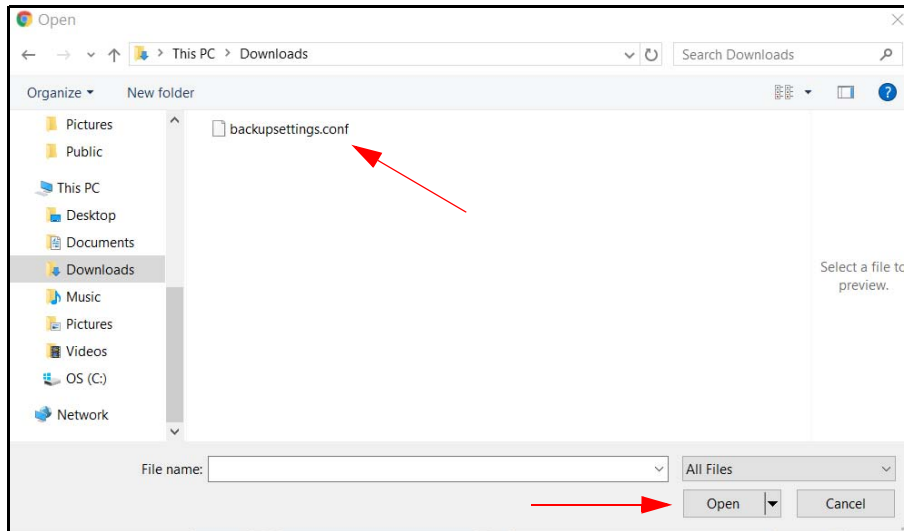
The file will be saved to your Downloads folder titled '**GatewaySettings.conf.**'

6.6.2.2 Restoring the UBC1301-AA00 to a Previously Saved Configuration

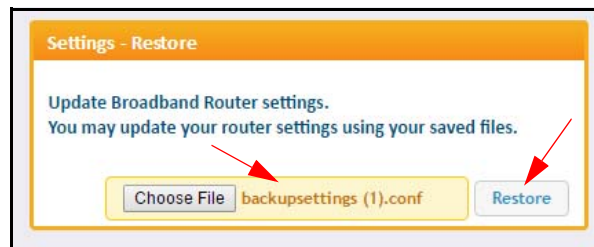
To restore the device to a previously saved configuration, click the **Choose File** button.



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



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



Your device will then reboot.

You are then presented with the login screen. Enter the Username and Password to return to the User Interface. Refer to [Accessing the Web User Interface Locally on page 18](#).

6.6.3 Using the Factory Default Option

The Factory Default option allows you to restore the UBC1301-AA00 to the factory default settings.

To reset the device to factory settings:

1. Click **Management** from the left side menu.
2. Click **Factory Default** under Management.

Field descriptions follow the screen example.



Label	Description
Restore User Defaults	Restores settings to factory defaults. Select the Yes button to restore the entire device to factory default settings.
Reset the System	Resets the system. Select the Yes button to power cycle the device.
Apply	Applies the changes.

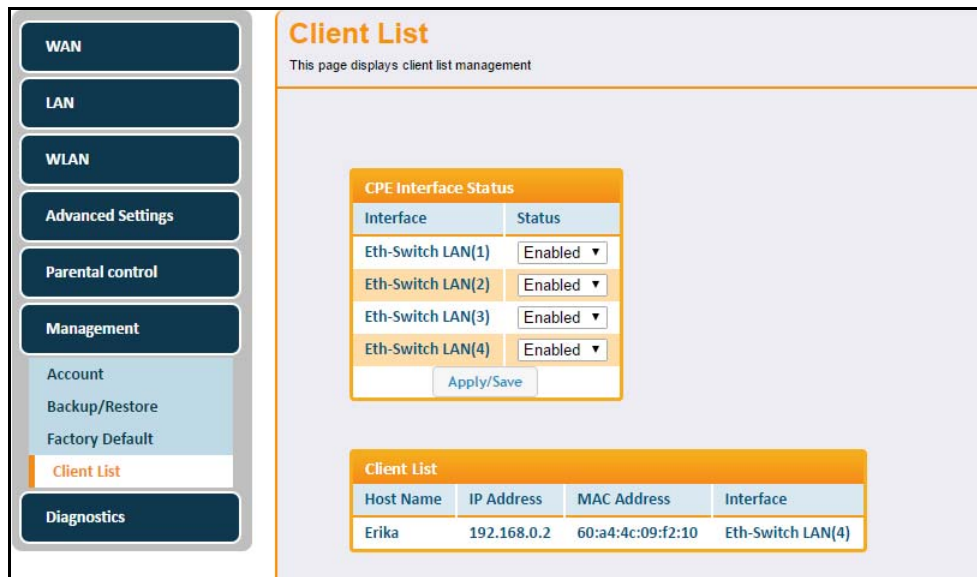
6.6.4 Using the Client List Option

The Client List screen displays computers and devices connected to the UBC1301-AA00.

To view connected devices:

1. Click **Management** from the left side menu.
2. Click **Client List** under Management.

Field descriptions follow the screen example.



Label	Description
CPE Interface Status	
Interface	Displays the interface of the UBC1301-AA00.
Status	Allows you to enable or disable the CPE interface. Choose the option from the drop-down menu.
Apply/Save	Applies and saves the changes.
Client List	
Host Name	Displays the name of the device connected to the UBC1301-AA00.
IP Address	Displays the IP Address of the device connected to the UBC1301-AA00.
MAC Address	Displays the MAC Address of the device connected to the UBC1301-AA00.
Interface	Displays the method of how the client is connected to the device (for example, Ethernet LAN or WiFi).

6.7 Using the Diagnostics Option

Use the **Diagnostics** option to test network connectivity and view the current network topology.

To use Diagnostic Tools and view Network Topology:

1. Click **Gateway** from the main menu.
2. Click **Diagnostics** on the left side menu.
3. The following sub-menus are available for selection:
 - ◆ [Using the Tools Option on page 78](#)
 - ◆ [Using the Home Topology Option on page 80](#)

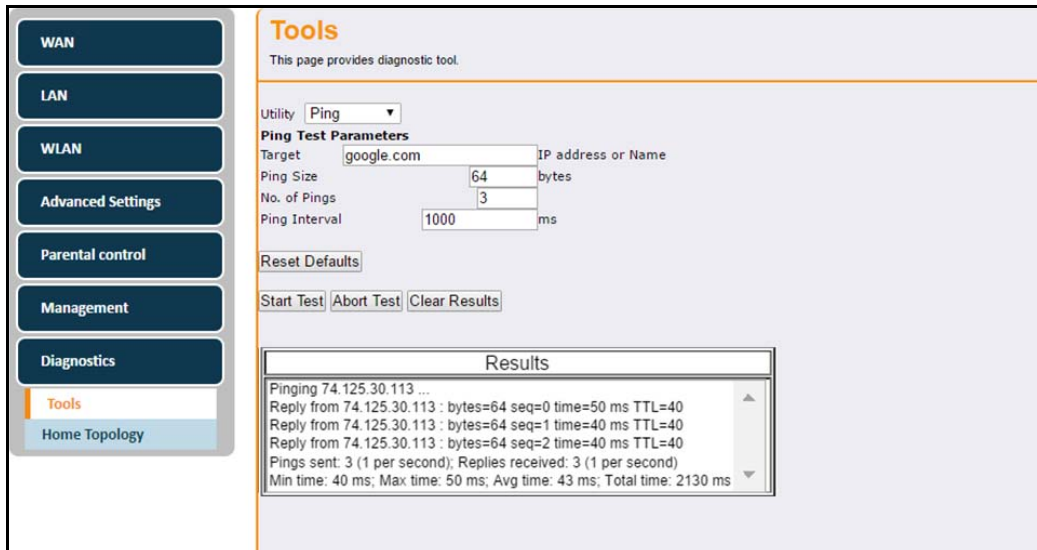
6.7.1 Using the Tools Option

Use the **Tools** option to test network connectivity. Two utilities are available: Ping and Traceroute.

6.7.1.1 Using the Ping Option

Use the **Ping** utility to test network connectivity between devices by sending a test message to a specific device. You can also confirm the size of data sent is the same as the size of data received.

1. Choose **Ping** from the drop-down menu.
2. Enter a target IP address or URL name to ping in the space provided.
3. Enter new parameters or accept the default values.
4. Click **Start Test**. Field description follow the example below.



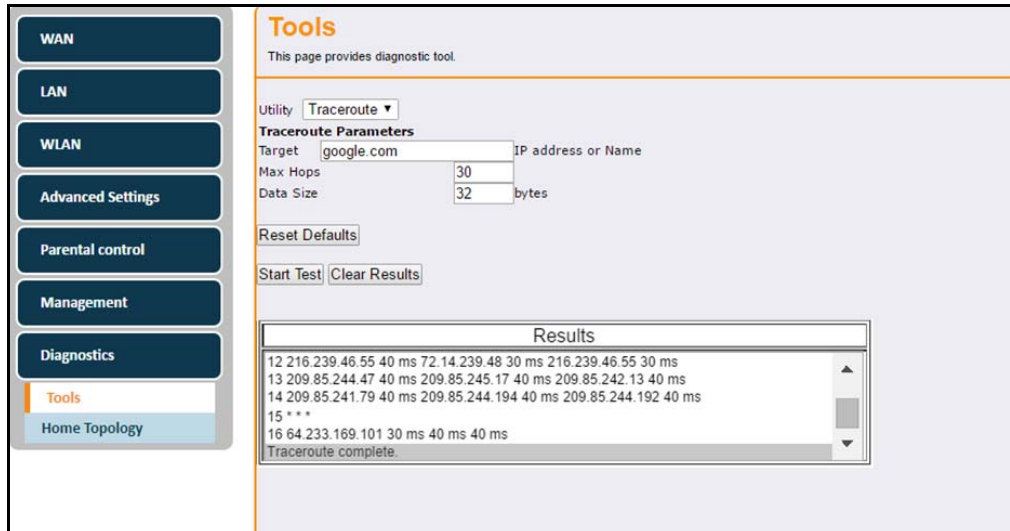
Label	Description
Utility	Provides a drop-down menu to choose Ping or Traceroute.
Ping Test Parameters	
Target	Enter the IP address or URL name to which you want to send a ping.
Ping Size	Defines the packet size (bytes of data) to send for the ping operation. The default is 64.
No. of Pings	Defines the number of ping commands to send to the ping target. Default is 3 pings.
Ping Interval	Defines the interval between ping operations in milliseconds.
Reset Defaults	Resets the Ping Test Parameters to the default values when pressed.
Start Test Abort Test Clear Results	Defines what action to take: <ul style="list-style-type: none"> ◆ Start Test begins the ping. ◆ Abort Test stops the ping. ◆ Clear Results deletes the previous test results in the Results table.
Results	Displays the results of the ping test.

6.7.1.2 Using the Traceroute Option

The **Traceroute** utility determines the IP addresses of hosts in the network path. By checking the Resolve Host names box, Traceroute tries to find which name matches the address. Some hosts have no names, and might still be shown as IP addresses, even if this option is active.

1. Choose **Traceroute** from the Utility drop-down menu.
2. Enter a target IP address or URL name of which to trace a route.
3. Enter new parameter values or accept the default values.

4. Click **Start Test**. Field descriptions are listed below the screen example.



Label	Description
Utility	Provides a drop-down menu to choose Ping or Traceroute.
Traceroute Parameters	
Target	Defines the specific IP address or domain (for example, google.com) to which you want to trace a route.
Max Hops	Defines the maximum number of hops. Hops are the number of routers the traceroute traverses. Default is 255.
Data Size	Defines the data size to send for the traceroute operation. Default is 32 bytes.
Base Port	Defines the destination port number. Default is 33434.
Resolve Host	Enable (on) or disables (off) this option. When checked, traceroute tries to find the name that matches the IP address. Default is Off.
Reset Defaults	Resets the Traceroute Parameters to the default values.
Start Test Clear Results	Defines what you want to do. <ul style="list-style-type: none"> ◆ Start Test begins the traceroute. ◆ Clear Results deletes previous test results in the Results table.
Results	Displays the results of the trace.

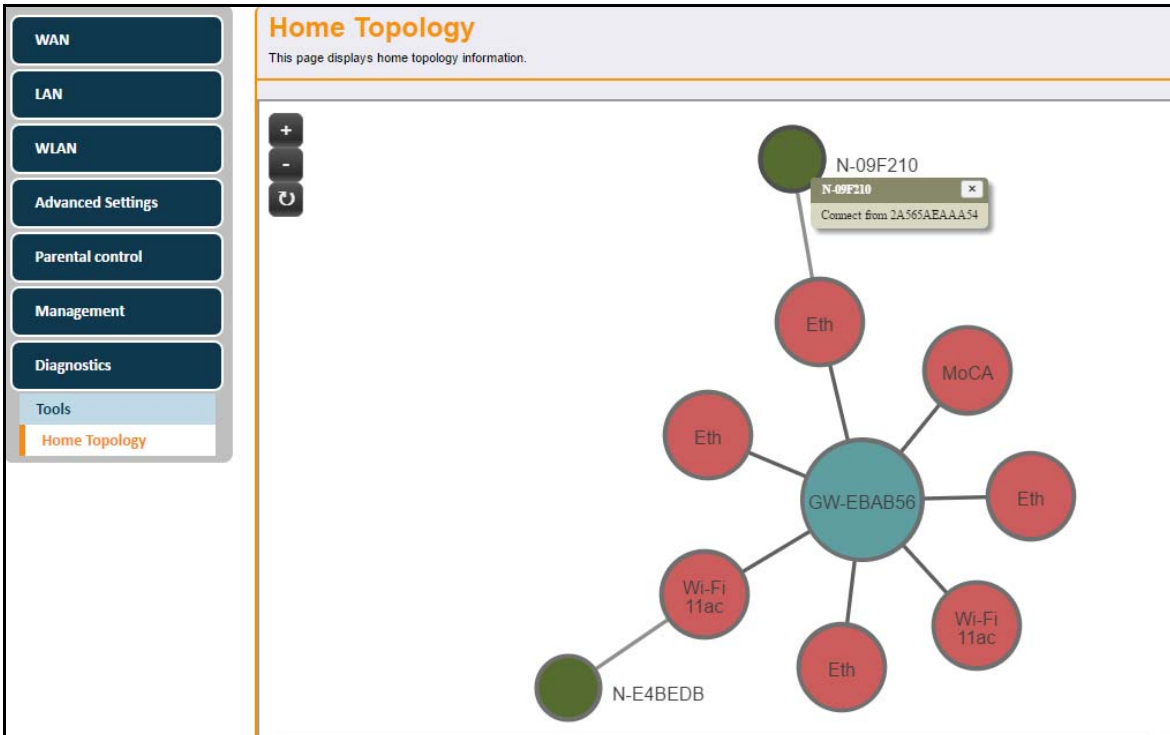
6.7.2 Using the Home Topology Option

Use the **Home Topology** option to view the current wireless network connections for the UBC1301-AA00 Advanced Wireless Voice Gateway.

In the following screen example:

- ◆ The **BLUE** node in the middle indicates the UBC1301-AA00.

- ◆ The **GREEN** nodes indicate stations connected to the UBC1301-AA00 (devices connected to the Ethernet and the wireless interfaces). The nodes are annotated by the last 6 characters of the interface with which they are connected to the access point (the UBC1301-AA00).
- ◆ The nodes in **RED** indicate the WiFi and Ethernet interfaces of the UBC1301-AA00.
- ◆ The lines indicate the connections between the interfaces.
- ◆ When you hover over a node, it displays the MAC addresses of the connected devices (the gray pop-up window in the below example).



7 Understanding the MoCA Menu

The **MoCA** menu of the Web user interface displays information about the MoCA status of the UBC1301-AA00. MoCA (Multimedia over Coax Alliance) technology is a standard that enables the distribution of high quality digital multimedia content throughout the home over existing coaxial cabling.

MoCA is a terrific technology that offers extended LAN support over a different set of frequencies on your home cable network. MoCA connected devices will be on the same LAN subnet as the Ethernet ports and Wireless Primary Networks.

IMPORTANT NOTE: Always consult your Cable Service Provider before enabling MoCA to be sure that the Point Of Entry Filter is properly installed and there is no conflict with another MoCA service.



Topics

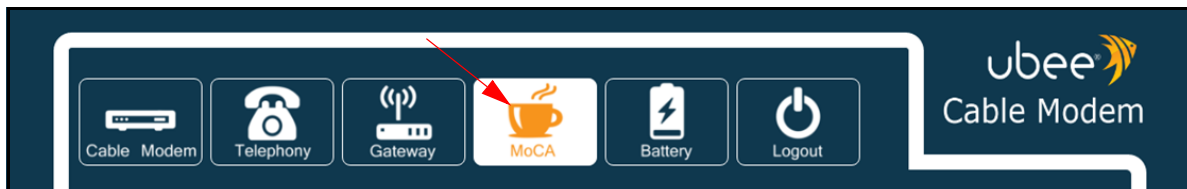
See the following topics:

- ◆ [Using the Status Option on page 82](#)

7.1 Using the MoCA Info Option

To access MoCA information:

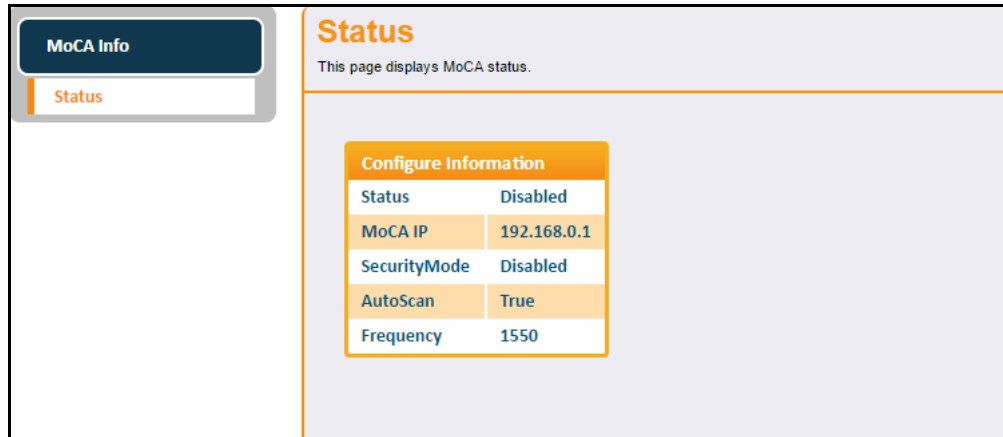
1. Access the Web user interface. Refer to [Accessing the Web User Interface Locally on page 18](#).
2. Click **MoCA** from the top main menu.



3. Click **MoCA Info** from the left side menu. The following sub-menus are available:
 - ◆ [Using the Status Option on page 82](#)

7.2 Using the Status Option

The **Status** option allows you to view the MoCA status of the UBC1301-AA00. Field descriptions are listed below the screen example.



Label	Description
Configure Information	
Status	Indicates whether MoCA is enabled or disabled.
MoCA IP	Displays the UBC1301-AA00 Gateway IP address, accessed via the MoCA interface.
Security Mode	Enabled means MoCA traffic is encrypted. Disabled means MoCA traffic is not encrypted.
Auto Scan	If true, the UBC1301-AA00 auto scans the MoCA frequency range to find an existing MoCA network. If one is not found, then the UBC1301-AA00 will become the Network Coordinator of its own MoCA network.
Frequency	Displays the current MoCA frequency seen by the UBC1301-AA00.

8 Understanding the Battery Menu

The **Battery** menu of the Web user interface allows you to access information about the battery, including estimated time remaining and current levels.

NOTE: The battery is optional, and is not included in the device packaging by default. You must contact your service provider to obtain a battery.

In the event of a power loss, the battery provides:

- ◆ Up to 8 hours of standby time
- ◆ Five (5) hours of talk time with 1 line active
- ◆ One upstream and 1 downstream channel

NOTE: Actual battery performance is affected by battery age and operating environment.



Topics

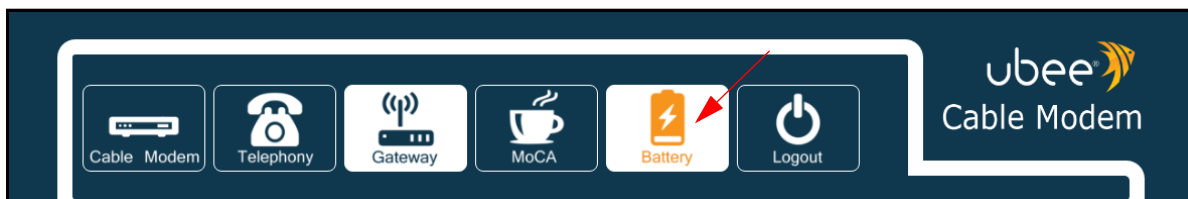
See the following topics:

- ◆ [Using the Battery Info Option on page 84](#)

8.1 Using the Battery Info Option

To access battery information:

1. Access the Web user interface. Refer to [Accessing the Web User Interface Locally on page 18](#).
2. Click **Battery** from the top main menu.



3. Click **Battery Info** from the left side menu. The following sub-menus are available:
 - ◆ [Using the Controller Option on page 85](#)
 - ◆ [Using the UPS Option on page 86](#)
 - ◆ [Using the Interface Delay Option on page 86](#)

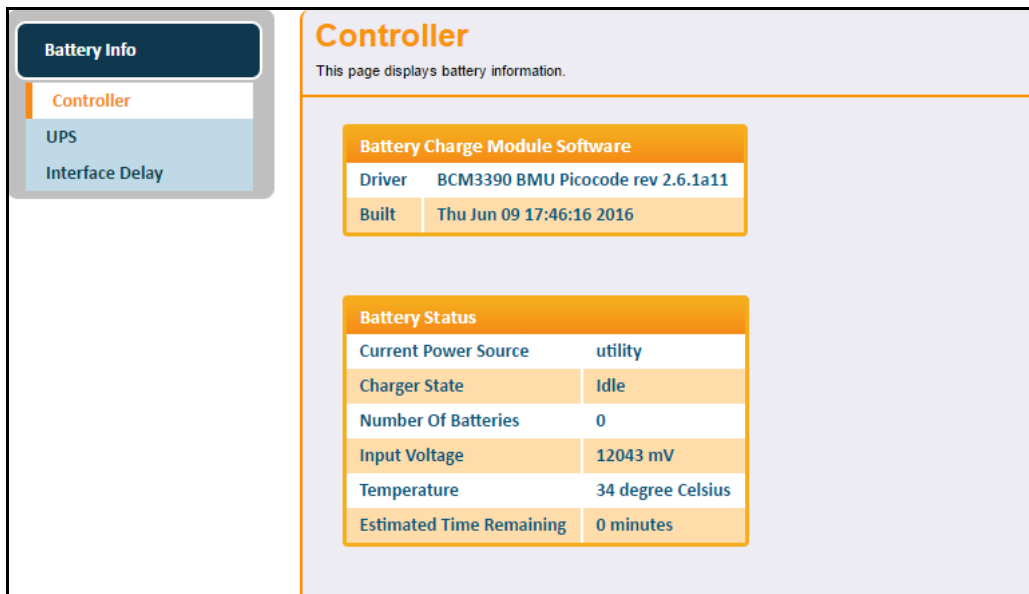
8.1.1 Using the Controller Option

The **Controller** option displays current battery information.

To view controller information:

1. Click **Battery** from the main menu.
2. Click **Battery Info** from the left side menu.
3. Click **Controller** below Battery Info.

Field descriptions follow the screen example.



Label	Description
Battery Charge Module Software	
Driver	Displays the driver used in the software.
Built	Indicates the date and time the battery was manufactured.
Battery Status	
Current Power Source	Displays the current power source for the device, such as utility through the power cord or internal battery power.
Charger State	Displays the status of the battery such as sleep or idle.
Number of Batteries	Indicated the number of batteries installed in the UBC1301-AA00.
Input Voltage	Displays the input voltage in millivolts (mV).
Temperature	Displays the battery temperature in Celsius.
Estimated Time Remaining	Displays how much time is left on the battery in minutes.

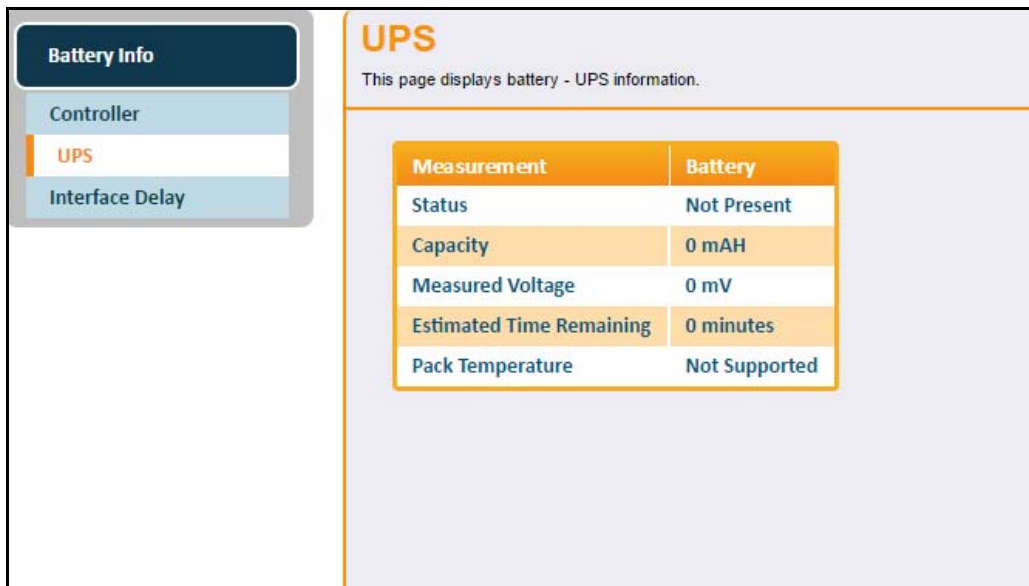
8.2 Using the UPS Option

The **UPS** option displays information about the uninterrupted power supply.

To view UPS information:

1. Click **Battery** from the main menu.
2. Click **Battery Info** from the left side menu.
3. Click **UPS** below Battery Info.

Field descriptions follow the screen example.



Label	Description
Measurement	
Status	Displays the current status of the battery.
Capacity	Displays the capacity of the battery.
Measured Voltage	Displays the current voltage of the battery.
Estimated Time Remaining	Displays how much time is left on the battery in minutes.
Pack Temperature	Displays the battery temperature in Celsius.

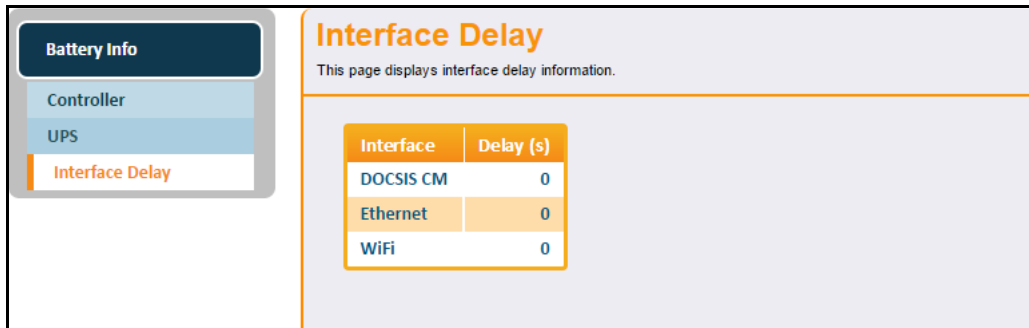
8.3 Using the Interface Delay Option

The **Interface Delay** option displays the length of time each interface will be active before being turned off when the device is operating on battery power.

To view Interface delay information:

1. Click **Battery** from the main menu.
2. Click **Battery Info** from the left side menu.
3. Click **Interface Delay** below Battery Info.

Field descriptions follow the screen example.



Label	Description
Interface	
DOCSIS CM	Displays the length of time in seconds the DOCSIS CM interface will be active before being turned off when the device is operating on battery power.
Ethernet	Displays the length of time in seconds the Ethernet interface will be active before being turned off when the device is operating on battery power.
WiFi	Displays the length of time in seconds the WiFi interface will be active before being turned off when the device is operating on battery power.

9 Glossary

This chapter defines terms used in this guide and in the industry.

ALG (Application-Level Gateway)

A type of security device that acts on behalf of the application servers on a network, hiding the servers themselves from traffic that might be malicious.

Broadcast

A packet sent to all devices on a network.

BSS (Basic Service Sets)

A basic service set is the fundamental building block of an 802.11 wireless local area network. The overlapping BSS problem refers to a situation where two or more systems, unrelated to each other are in close enough proximity to hear each other physically. Overlapping BSS may degrade the network performance severely.

Channel Bonding

A computer networking configuration where two or more network interfaces are combined on a host computer for redundancy or increased throughput. Data is transmitted over these channels as if they are one channel.

CMTS (Cable Modem Termination System)

Typically located in the cable company's headend, the CMTS is equipment that provides high-speed data services to subscribers, such as cable Internet and Voice over IP (VoIP).

CPE (Customer Premises Equipment)

Equipment such as telephones, routers, and modems located at a user's location to enable access to communication services.

Default Gateway

The routing device used to forward all traffic that is not addressed to a computer on the local subnet.

DHCP (Dynamic Host Configuration Protocol)

A protocol that centrally automates the assignment of IP addresses in a network. Using the Internet's set of protocols (TCP/IP), each machine that can connect to the Internet needs a unique IP address. For example, when the service provider sets up computer users with a connection to the Internet, an IP address is assigned to each machine. DHCP lets the service provider distribute IP addresses and automatically sends a new IP address when a computer is plugged in to the high-speed Internet network. DHCP uses the concept of a "lease" or amount of time an IP address is valid for a computer. Lease times can vary.

DMZ (Demilitarized Zone)

Allows one IP address (or computer) to be placed in between the firewall and the Internet (usually for gaming and video conferencing). This allows risky, open access to the Internet.

DOCSIS (Data Over Cable Service Interface Specification)

An International telecommunications standard that permits the addition of high-speed data transfer over an existing cable TV system.

Domain

A subnetwork comprised of a group of clients and servers under the control of one security database.

Domain Name

A descriptive name for an address or group of addresses on the Internet. Domain names are in the form of a registered entity name plus one of a number of predefined top-level suffixes, such as .com, .edu, .org.

DoS (Denial of Service) Attack

An attempt to make a machine or network resources unavailable to its intended users.

DNS (Domain Name System)

An Internet service that locates and translates domain names into IP addresses. Because domain names are alphabetic, they are easier to remember. However, the Internet is based on IP addresses. Every time you use a domain name, a DNS service translates the name into the corresponding IP address. The DNS system is actually its own network. If one DNS server does not know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Downstream

A term to describe the direction of data from the network service provider to the customer.

DTIM (Delivery Traffic Indication Message)

Informs clients about the presence of buffered broadcast data on the access point.

Ethernet

A standard network protocol that specifies how data is placed on and retrieved from a common transmission medium. It forms the underlying transport vehicle used by several upper-level protocols, including TCP/IP, HTTP, and FTP.

Firewall

A highly effective method to block unsolicited traffic from outside the connected computers in your gateway and local network.

FTP (File Transfer Protocol)

A network protocol used to transfer files from one host to another over a TCP-based network.

Gateway

A local device, usually a router, that connects hosts on a local network to other networks – sometimes with different incompatible communication protocols. The UBC1301-AA00 is an example of a gateway.

Headend

A main facility to process and distribute Internet communication signals. Headend may also refer to cable television signals and power line communication facilities.

ICQ

A free instant-messaging utility introduced by Mirabilis in 1996.

IKE (Internet Key Exchange)

A protocol used to ensure security for VPN negotiation and remote host or network access.

IP (Internet Protocol)

The method or protocol by which data is sent from one computer to another on the Internet. It is a standard set of rules, procedures, or conventions relating to the format and timing of data transmission between two computers that they must accept and use to understand each other. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.

IP Address

In the most widely installed level of the IP today, an IP address is a 32-bit binary digit number that identifies each sender or receiver of information that is sent in packet form across the Internet. When you request a Web page or send an e-mail, the IP part of TCP/IP includes your IP address. IP sends your IP address to the IP address obtained by looking up the domain name in the URL you requested or in the e-mail address to which you are sending a note. A dynamic IP address is an IP address that is automatically assigned to a client station in a TCP/IP network, typically by a DHCP server.

IPsec (Internet Protocol Security)

A protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.

IRC (Internet Relay Chat)

A system that facilitates the transfer of messages in the form of text.

ISP (Internet Service Provider)

A company that provides individuals and companies access to the Internet and other related services.

IUC (Interval Usage Code)

Interval usage codes define different profiles for upstream burst profiles to use for the data. IUCs are sent to the cable modem from the CMTS to tell the device important characteristics to use for the burst, such as modulation type, preamble length, and so on.

Kerberos

A network authentication protocol which works on the basis of “tickets” to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.

LAN (Local Area Network)

A group of computers and associated devices such as printers and servers that share a common communication line and other resources within a small geographic area.

MAC (Media Access Control Address)

A unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level. Usually written in the form 01:23:45:67:89:ab.

Mbps (Megabits per Second)

A unit of measurement for data transmission that represents one million bits per second.

MTU (Maximum Transmission Unit)

The size in bytes of the largest packet that can be sent or received.

NAT (Network Address Translation)

A technique by which several hosts or computers share a single IP address for access to the Internet. NAT enables a LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic, and provides a type of firewall by hiding internal IP addresses.

NetBios (Network Basic Input/Output System)

A program that allows applications on different computers to communicate within a local area network.

Net2Phone

A software/services company whose principal line of business is SIP-based and PacketCable-based voice over IP.

Packet

A block of information sent over a network. A packet typically contains a source and destination network address, some protocol and length information, a block of data, and a checksum.

PPTP (Point-to-Point Tunneling Protocol)

A method for ensuring secure communication between virtual private networks.

Ranging

A process in which a cable modem sends a range request at a power of 8 dBmV (very low power). If it does not receive a range response from the CMTS, the cable modem re-transmits the range request at a 3 dB higher power level and continues the process until a range response is received.

Router

A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.

RIP (Routing Information Protocol)

A protocol in which routers periodically exchange information with one another to determine minimum-distance paths between sources and destinations.

RSVP (Resource Reservation Protocol)

A set of communication rules that allows channels or paths on the Internet to be reserved for the multicast transmission of video and other high-bandwidth messages.

RTSP (Real Time Streaming Protocol)

A protocol used in the transfer of real-time streaming media such as audio and video.

SIP (Session Initiation Protocol)

A signaling communications protocol that is widely used for controlling multimedia communications sessions such as voice and video over Internet Protocol networks.

SNR (Signal-to-Noise Ratio)

A measure that compares the level of a desired signal to the level of background noise.

SNTP (Simple Network Time Protocol)

A protocol for synthesizing the clocks of computing devices over networks.

STBC (Space-Time Block Code)

A technique used in wireless communications to transmit multiple copies of a data stream across a number of antennas.

Subnet

A portion of a network that shares a common address component. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix. For example, all devices with IP addresses that start with 10.1.10 would be part of the same subnet. IP networks are divided using a subnet mask.

Subnet Mask

Combined with the IP address, the IP subnet mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router. A number that explains which part of an IP address comprises the network address and which part is the host address on that network.

Telnet

A network protocol used on the Internet or a local area network. Provides bi-directional interactive text-oriented communications using a virtual terminal connection.

TACACS (Terminal Access Controller Access-Control System)

A remote authentication protocol used to communicate with an authentication server to determine if the user is allowed to access the network.

TCP (Transmission Control Protocol)

A method (protocol) used with the IP to send data in the form of message units (datagrams) between network devices over a LAN or WAN. While IP handles the actual delivery of the data (routing), TCP keeps track of the individual units of data (packets) that a message is divided into for efficient delivery over the network. TCP requires the receiver of a packet to return an acknowledgment of receipt to the sender of the packet.

TCP/IP (Transmission Control Protocol/Internet Protocol)

The basic communication language or set of protocols to communicate over a network (developed specifically for the Internet). TCP/IP defines a suite or group of protocols.

TDMA (Time Division Multiple Access)

A method in which cable modems must time-share the upstream channel because there are many cable modems and only one upstream channel frequency.

TFTP (Trivial File Transfer Protocol)

A file transfer protocol used to transfer automatically configuration or boot files.

TPC (Transmit Power Control)

Sometimes called Dynamic Power Control (DPC), TPC is a mechanism used in radio communications to reduce the power of a radio transmitter to the minimum necessary to maintain the link with a certain quality. It is used to avoid interference with other devices and/or to extend battery life.

UDP (User Datagram Protocol)

A communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol.

UPNP (Universal Plug and Play)

A set of networking protocols that permits networked devices to seamlessly discover each other's presence on the network to enable data sharing, communications, and entertainment.

Upstream

A term to describe the direction of data from the customer to the network service provider.

URI (Uniform Resource Identifier)

A string of characters used to identify a name or a resource on the Internet.

URL (Uniform Resource Locator)

A uniform resource identifier (URI) that specifies where a known resource is available and how to retrieve it.

WAN (Wide Area Network)

A long-distance link or computer network that spans a relatively large geographical area that connects remotely located LANs. Typically, a WAN consists of two or more LANs. The Internet is a large WAN.

XML (Extensible Markup Language)

A markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine readable.

XPress™

XPress™ is a standards-based frame-bursting approach to improve 802.11g wireless LAN performance developed by Broadcom.