



# DVW3201B Advanced Wireless Voice Gateway

Firmware Version: 9.8.3012\_D1

## Subscriber User Guide



July 2012

[www.ubeeinteractive.com](http://www.ubeeinteractive.com)  
8085 S. Chester Street, Suite 200  
Englewood, CO 80112  
1.888.390.8233  
Sales (email): [amsales@ubeeinteractive.com](mailto:amsales@ubeeinteractive.com)  
Support (email) [amsupport@ubeeinteractive.com](mailto:amsupport@ubeeinteractive.com)

## Notices and Copyrights

Copyright 2012 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.

This device is Wi-Fi Alliance Certified.



# Contents

<b>1</b>	<b>Introduction.....</b>	<b>1</b>
1.1	Understanding Safety and Regulatory Information .....	2
1.1.1	Understanding Safety.....	2
1.1.2	Understanding Eco-Environmental Statements .....	2
1.1.3	Understanding Regulatory Statements .....	3
1.2	Understanding Connections and Applications .....	3
1.3	Requesting Support .....	3
1.4	Checking Device Package Components .....	4
1.5	Understanding the Device Rear Panel.....	5
1.6	Understanding Specifications, Standards, and Firmware .....	6
1.7	Understanding Default Values and Logins.....	8
1.8	Understanding LED Operations .....	8
1.8.1	Understanding the Device Front Panel .....	8
1.8.2	Understanding LED Behavior.....	9
<b>2</b>	<b>Installing the DVW3201B .....</b>	<b>11</b>
2.1	Setting Up and Connecting the DVW3201B .....	11
2.2	Connecting Devices to the Network .....	12
2.2.1	Connecting an Ethernet Device .....	12
2.2.2	Connecting a Wireless Device .....	13
2.2.3	Connecting a Telephone Line .....	14
2.3	Troubleshooting the Installation .....	14
<b>3</b>	<b>Using the Web User Interface .....</b>	<b>17</b>
3.1	Accessing the Web Interface .....	17
3.2	Logging Out of the Web Interface .....	18
3.3	Understanding Operation Modes and the Web User Interface .....	19
<b>4</b>	<b>Understanding the Modem Menu .....</b>	<b>21</b>
4.1	Using the Information Option .....	21
4.2	Using the Status Option .....	23
4.3	Using the Downstream Option .....	23
4.4	Using the Upstream Option .....	25
4.5	Using the Operation Config Option .....	26
4.6	Using the Event Log Option .....	27
4.7	Using the Battery Info Option.....	28
<b>5</b>	<b>Understanding the Gateway Menu .....</b>	<b>31</b>

5.1	Using the Gateway Information Option	32
5.2	Using the Setup Option	34
5.2.1	Viewing IPv6 Addresses in the Gateway Setup Option	36
5.2.2	Using the LAN IPv6 Option	36
5.3	Using the DHCP Option	37
5.4	Using the DHCP Static Lease Option	39
5.5	Using the Time Option	40
5.6	Using the Advanced Gateway Setup Options	41
5.7	Using the Advanced Gateway Setup MAC Filtering Option	44
5.8	Using the Advanced Gateway Setup IP Filtering Option	45
5.8.1	Using IP Filtering Best Practices	45
5.9	Using the Advanced Gateway Setup Port Filtering Option	46
5.10	Using the Advanced Gateway Setup Forwarding Option	47
5.10.1	Setting Up Port Forwarding for an Xbox Example	49
5.10.2	Viewing Port Maps	51
5.11	Using the Advanced Gateway Setup Port Triggering Option	51
5.12	Using the Advanced Gateway Settings Pass Through Option	53
5.13	Using the Advanced Gateway Settings DMZ Host Option	54
5.13.1	Using DMZ Host Best Practices	54
<b>6</b>	<b>Understanding the Wireless Menu</b>	<b>57</b>
6.1	Using the Wireless Radio Option	57
6.1.1	Scanning for Wireless Access Points (APs)	59
6.2	Using the Primary Network Option	61
6.2.1	Enabling a Closed Network	64
6.3	Using the Access Control Option	65
6.4	Deploying and Troubleshooting the Wireless Network	67
<b>7</b>	<b>Understanding the Firewall Menu</b>	<b>71</b>
7.1	Using the Content Filter Option	71
7.2	Using the Event Log Option	73
7.3	Using the Remote Log Option	74
<b>8</b>	<b>Understanding the Parental Control Menu</b>	<b>75</b>
8.1	Using the Parental Control User Setup Option	75
8.2	Using the Basic Option	77
8.3	Using the Tod Filter Option	79
8.4	Using the Event Log Option	80
<b>9</b>	<b>Understanding the Tools Menu</b>	<b>81</b>
9.1	Using the Ping Option	81
9.2	Using the Trace Route Option	82
9.3	Using the Client List Option	83
9.4	Using the Password Option	84
9.5	Using the User Defaults Option	85
<b>10</b>	<b>Glossary</b>	<b>87</b>

# 1 Introduction

Welcome to the Ubee family of data networking products. This guide is specific to the **DVW3201B** and serves the following purposes:

- ☐ Provides multiple system operators (MSOs) for cable systems with all information necessary to operationally stage, deploy, and support the DVW3201B.
- ☐ Provides the technical details needed to locally and remotely manage deployed devices. This can involve setting up configuration files, downloading the files to the device, and obtaining information from the device for support and troubleshooting.
- ☐ Defines all relevant device compliance standards and physical specifications.
- ☐ Provides information used by the following MSO entities:
  - ◆ Office of the CTO
  - ◆ Procurement, Network Engineering and Test Organizations
  - ◆ Physical & Environmental Engineers
  - ◆ Tech Ops
  - ◆ Installation and Repair
  - ◆ Customer Care
  - ◆ Training Organizations
- ☐ Provides installation instructions and device Web interface instructions for configuring/managing the device.



## Topics

**See the following topics:**

- ☐ [Understanding Safety and Regulatory Information on page 2](#)
- ☐ [Understanding Connections and Applications on page 3](#)
- ☐ [Requesting Support on page 3](#)
- ☐ [Checking Device Package Components on page 4](#)
- ☐ [Understanding the Device Rear Panel on page 5](#)
- ☐ [Understanding Specifications, Standards, and Firmware on page 6](#)
- ☐ [Understanding Default Values and Logins on page 8](#)
- ☐ [Understanding LED Operations on page 8](#)
- ☐ [Understanding the Device Front Panel on page 8](#)

## 1.1 Understanding Safety and Regulatory Information

The following information provides safety and regulatory standards to install, maintain, and use the DVW3201B Advanced Wireless Voice Gateway.

### 1.1.1 Understanding Safety



**WARNING:** The following information provides safety guidelines for anyone installing and maintaining the DVW3201B. 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:



Always 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, 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 the product. Use a soft dry cloth for cleaning.

Do not insert any sharp object 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 cord supplied with the device. Do not attach the power supply cable on building surfaces or floorings.

- ☐ Rest the power cable freely without any obstacles. Do not place heavy items on top of the power cable. Refrain from abusing, stepping on, or walking 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.
- ☐ To protect the equipment from overheating, do not block the slots and openings in the module housing that provide ventilation. Do not expose this device to direct sunlight. Do not place hot devices close to this device, as it may degrade it or cause damage.

### 1.1.2 Understanding Eco-Environmental Statements

The following eco-environmental statements apply to the DVW3201B.

#### **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](http://www.ubeeinteractive.com).

### 1.1.3 Understanding Regulatory Statements

The following regulatory statements apply to the DVW3201B.

#### Industry North America Statement:

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

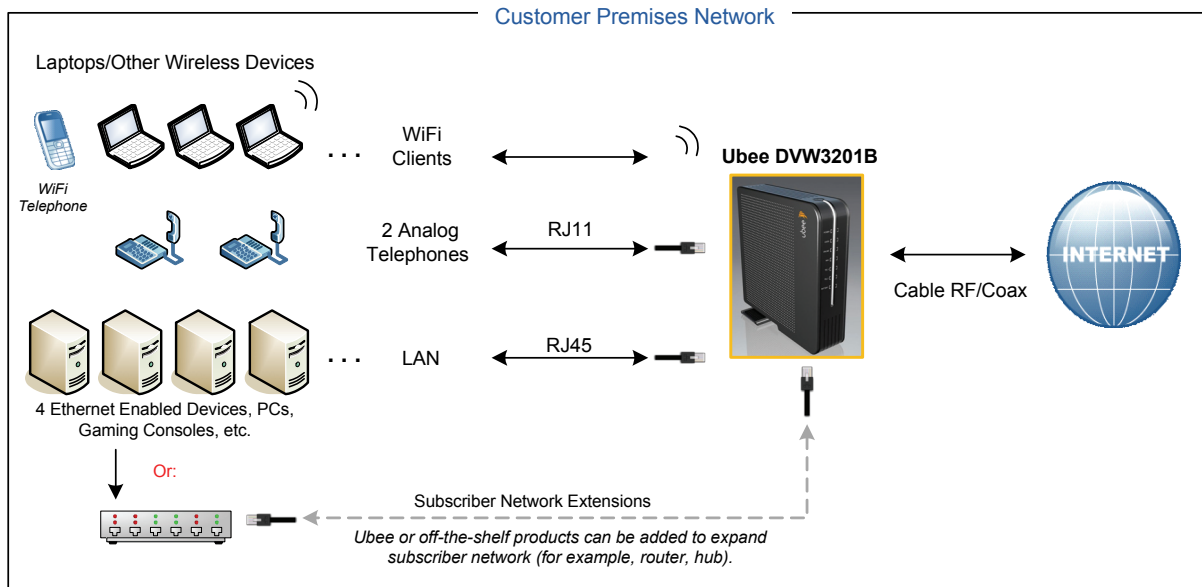
- (1) This device may not cause harmful interference.
- (2) This device must accept any interference received, including interference that may cause undesired operation.

#### 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 minimum distance 20cm between the radiator & your body. This device has been designed to operate with an antenna having a maximum gain of 2 dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry North America. The required antenna impedance is 50 ohms.

## 1.2 Understanding Connections and Applications

The following diagram illustrates the general connection topology and applications of the DVW3201B.



## 1.3 Requesting Support

Subscribers must contact their service provider for direct support. Device documentation support may be available at:

<http://www.ubeeinteractive.com>

## 1.4 Checking Device Package Components

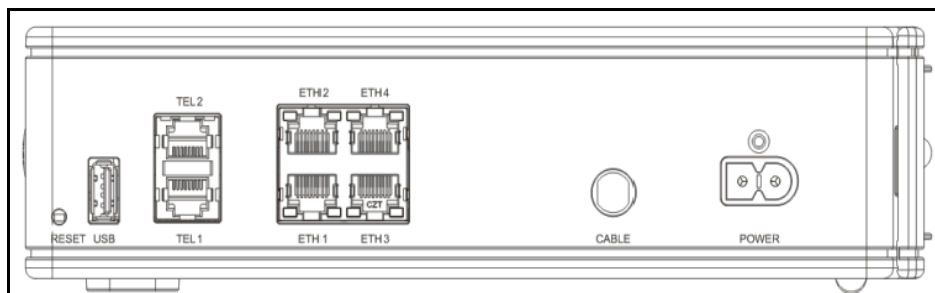
The package for the DVW3201B contains the following items:

Item	Description
	<p>1 - RJ45 Cable (Ethernet) Length ~ 6.0 ft RoHS &amp; UL compliant</p> <p><i>Sample image, actual appearance subject to change.</i></p>
	<p>1 - RJ11 Cable (Telephone)</p> <p><i>Sample image, actual appearance subject to change.</i></p>
	<p>1 - AC Power Cord 10A / 125V</p> <p><i>Sample image, actual appearance subject to change.</i></p>
 	<p>1 - Lithium-ion Battery Model: SMPCM9 Rating: 11.1V @ 2.55 Ah 28.305 Wh</p> <p>Battery supports continuous voice service during power outages, and provides up to 8.5 hours standby time, and 4 hours talk time with 2 lines offhook.</p> <p>Look for the <b>ONLY USE WITH DVW3201B</b> or <b>ONLY USE WITH DVW32xx</b> label on the bottom of the battery. Only use the SMPCM9 battery with this label in the DVW3201B.</p>



## 1.5 Understanding the Device Rear Panel

Review the following image and descriptions of the rear panel connections on the device.



Item	Description
<b>RESET</b>	Restores the default settings of the device including wireless and custom gateway settings. Use a pointed object to push down the reset button for 5-10 seconds until the power LED turns off. After the power LED turns off, release the button.
<b>USB</b>	Connects to some USB devices, such as computers and flash drives, if the USB connector is supported/enabled by the service provider.
<b>TEL1 TEL2</b>	Connects to a standard analog telephone using an RJ11 cable. Telephone service must be enabled through the service provider to use home telephony.
<b>ETH1 ETH2 ETH3 ETH4</b>	<p>Connects to Ethernet devices such as computers, gaming consoles, and/or routers/hubs using an RJ45 cable. Each ETH port on the back panel of the device has an LED to indicate its status when an Ethernet device is connected.</p> <p>When an Ethernet device, such as a computer, is connected to the cable modem the:</p> <ul style="list-style-type: none"> <li>♦ LED is <b>Orange</b> when connected at 10/100 Mbps speeds.</li> <li>♦ LED is <b>Green</b> when connected at 1000 speeds (Gigabit Ethernet).</li> <li>♦ LED blinks when data is being passed between the cable modem and the connected device.</li> </ul>
<b>CABLE</b>	Connects to the cable outlet (with the cable provided by your service provider), or a cable splitter connected to the cable outlet.
<b>POWER</b>	Connects the power adaptor to the device. Use only the power adaptor provided with the DVW3201B.
<b>BATTERY</b>	Houses the battery (located on the bottom of the device). The compartment can be opened to insert and replace the battery. Use only the battery marked for use with the DVW3201B. When inserting the battery into the housing, make sure the battery is inserted past the two clips on each side that hold the battery in place. The battery provides enough power to support voice service if the cable modem encounters a power failure from the wall power outlet at the subscriber's premises.

Item	Description
<b>WPS</b>	Connects a PIN-protected Wi-Fi device to the cable modem when the Wi-Fi Protected Setup method is used. When the WPS button is pushed or triggered through the device's Web UI, an LED on the top-front of the device flashes for four minutes until a PIN is entered from the wireless client, such as a laptop computer, that wants to connect. After a Wi-Fi client attaches successfully, the LED remains on for five minutes, and then turns off. Refer to <a href="#">Understanding the Wireless Menu on page 57</a> for more information.

## 1.6 Understanding Specifications, Standards, and Firmware

The following list provides the features and specifications of the DVW3201B.

### Interfaces and Standards

- ☐ Cable: F-Connector, Female, USB: 1 USB 2.0 host port
- ☐ LAN: 4 10/100/1000 Mbps RJ45 ports
- ☐ 2 RJ11 ports (telephony), PacketCable1.5 Certified/PacketCable 2.0 compliant
- ☐ DOCSIS 3.0/Euro DOCSIS 3.0 certified
- ☐ DOCSIS/Euro DOCSIS 1.0/ 1.1/2.0 certified
- ☐ CE/FCC Class B, ENERGY STAR® certified, WiFi Alliance certified
- ☐ Battery and Battery Port: The battery provides up to 8.5 hours standby time, 4 hours talk time with 2 lines off-hook, 1 US and 1 DS channel.



### Downstream\*

- ◆ Frequency Range: 88MHz ~ 1002MHz
- ◆ Modulation: 64 / 256 QAM, Channel B/W: 6 MHz
- ◆ Maximum Data Rate per Channel (up to 8 channels): DOCSIS = 30 Mbps (64 QAM), 42 Mbps (256 QAM), EuroDOCSIS = 41 Mbps (64 QAM), 55 Mbps (256 QAM)
- ◆ Total Max Bandwidth (8 Channels): DOCSIS = 343 (304) Mbps, EuroDOCSIS = 444 (400) Mbps
- ◆ Symbol Rate: 6952 Ksps
- ◆ RF Input Power: -15 to +15dBmV (64 QAM), -15 to +15dBmV (256 QAM)
- ◆ Input Impedance: 75 Ω

### Upstream\*

- ◆ Frequency Range: 5MHz ~ 42MHz
- ◆ Modulation A-TDMA: QPSK, 8, 16, 32, 64QAM, S-CMDA: QPSK, 8, 16, 32, 64, 128QAM

- ◆ Max Bandwidth of 4 Channels = 122.88 (108) Mbps, bandwidth per channel (up to 4 channels) = [QPSK 0.32 ~ 10.24 Mbps, 8 QAM 0.48 ~ 15.36 Mbps, 16 QAM 0.64 ~ 20.48 Mbps, 32 QAM 0.80 ~ 25.60 Mbps, 64 QAM 0.96 ~ 30.72 Mbps, 128 QAM/TCM 30.72 Mbps]
- ◆ Symbol Rate: 160, 320, 640, 1280, 2560, 5120 Ksps
- ◆ RF 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.

### Security and Network

- ◆ Supports 4 SSIDs, 802.11b/g/n compliant with link speeds up to 300 Mbps, 2Tx and 2Rx antennas
- ◆ 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
- ◆ DHCP Client/Server, Static IP network assignment, RIPv1/ v2, Ethernet 10/100/1000 BaseT, full-duplex auto-negotiate functionality, IPv4 and IPv6 support
- ◆ VPN Pass-Through and VPN End-Point Support (IPSec/L2TP/PPTP), TACACS or RADIUS Authentication

### Voice

- ◆ MGCP 1.0 / NCS 1.0 and SIP (RFC3261)
- ◆ 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

### Device Management

- ◆ Supports IEEE 802.11e Wi-Fi Multimedia (WMM) and UAPSD (power savings)
- ◆ DOCSIS, Web-Based, and XML Configuration
- ◆ Telnet Remote Management
- ◆ Firmware Upgrade via TFTP
- ◆ Configuration Backup and Restore
- ◆ SNMP Support

### Physical and Environmental

- ◆ Dimensions: 9" (230mm) x 8.9" (228mm) x 2.36" (60mm)
- ◆ Power: 10A / 125V
- ◆ Humidity: 5~90% (non-condensing)
- ◆ Operating Temperature: 32°F ~ 104°F (0°C ~ 40°C)

## 1.7 Understanding Default Values and Logins

The DVW3201B is pre-configured with the following parameters. Some regions may change default values using the cable modem or XML configuration file. Check with your provisioning team to determine the default values for your region.

**Local Port Address:** 192.168.100.1, Web Interface: http://192.168.100.1

**Operation Mode:** NAT Mode

**Subnet Mask:** 255.255.255.0

### Wireless Defaults:

- ◆ Primary SSID (subscriber-managed) = DVW3201B plus last 2 characters of the cable modem's MAC address with upper letters entered in upper case.

Example: **DVW3201BE3**

#### Note:

- ❖ If the subscriber changes the SSID, the device does not revert to this default SSID when the device is reset, except when a manual reset is performed through the Web UI (see [Understanding the Tools Menu on page 81](#)).
- ❖ The MAC address can be found on the device label or it can be found by opening an Internet browser window to the device. Refer to [Using the Information Option on page 21](#) for instructions.
- ◆ Encryption Method = **WPA2-PSK** with **AES** encryption
- ◆ WPA Pre-shared Key = DVW3201B plus the last 6 characters (3 octets) of the cable modem's MAC address (UPPER case, if letters).  
Example: **DVW3201B9822E3**
- ◆ WPS PIN = Randomly generated eight digit number
- ◆ Device Name: **UbeeAP**

### □ Standard User Web Interface Login:

Username: **user**

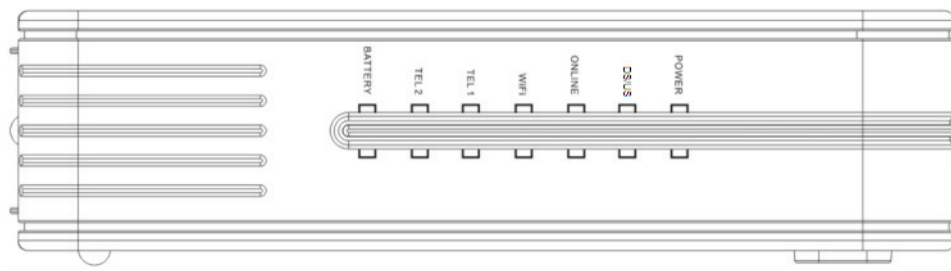
Password: **user**

## 1.8 Understanding LED Operations

The following section describes what the device LEDs indicate.

### 1.8.1 Understanding the Device Front Panel

The following image represents the front panel of the device. LED descriptions are provided in the following table.



## 1.8.2 Understanding LED Behavior

The following table summarizes the behavior of the device LEDs.

LED	Color	Description
<b>POWER</b>	White	<b>On</b> – Internal power-on completes successfully. <b>Blinks</b> – Power-on fails.
<b>DS/US</b>	White	<b>Blinks</b> – Initializing. <b>On</b> – Locked on to upstream (US) and downstream (DS) channels and registered OK. <b>Blinks</b> – Unable to register or lock. <b>Blinks</b> – When a firmware upgrade is in progress, the DS/US and TEL1 LEDs blink, first one then the other for a few seconds. Then DS/US and TEL1 and TEL2 LEDs blink in unison.
<b>ONLINE</b>	White	<b>Blinks</b> – Obtaining an IP address and configuration file. <b>On</b> – Configuration completes successfully.
<b>WiFi</b>	White	<b>On</b> – Wi-Fi is enabled. <b>Off</b> – Wi-Fi is disabled.
<b>TEL1 TEL2</b>	White	<b>On</b> – Telephone is on-hook. <b>Blinks</b> – Telephone is off-hook. <b>Blinks</b> – When a firmware upgrade is in progress, the DS/US and TEL1 LEDs blink, first one then the other for a few seconds. Then DS/US and TEL1 and TEL2 LEDs blink in unison.

LED	Color	Description
<b>BATTERY</b>	White	<p><b>On</b> – The battery is installed and AC power is on and properly functioning.</p> <p><b>Off</b> – If there is no AC power to the device, the Battery LED is Off, the Power LED flashes, and the TEL1 LED is On. All other LEDs are Off.</p> <p><b>Blinks</b> – If the battery is at low power level (30mins left).</p>
<b>Ethernet 1-4 (back panel)</b>	Orange/ Green	<p><b>On ORANGE</b> – When an Ethernet device is connected to the cable modem at 10/100 Mbps speeds,</p> <p><b>On GREEN</b> – When an Ethernet device is connected to the cable modem at 1000 speeds (Gigabit Ethernet).</p> <p><b>Blinks (in ORANGE or GREEN)</b> – When data is 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 DVW3201B using RJ45 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>
<b>WPS button (top of device)</b>	White	<p>Located on top of the cable modem, this button is used for the WiFi Protected Setup (WPS) method to connect a PIN-protected WiFi device to the cable modem.</p> <p>When a user pushes the WPS button or triggers WPS via the device's Web UI, an LED on the top-front of the device <b>blinks</b> for 4 minutes until a PIN is entered from the wireless client that wishes to connect (for example, a laptop computer). After a WiFi client attaches successfully, the LED remains <b>On</b> for 5 minutes, then turns <b>Off</b>. Refer to <a href="#">Understanding the Wireless Menu on page 57</a> for more information.</p>

			LED POSITION	LED1	LED2	LED3	LED4
			LED DESIGNATION/LABEL	POWER	US/DS	ONLINE	WiFi
eMTA INITIALIZATION	STEP	1	MTA DHCP	ON	ON	ON	
		2	MTA SNMP/TFTP	ON	ON	ON	
		3	RSIP	ON	ON	ON	
eMTA NORMAL OPERATION	AC POWER NORMAL (AC POWER IS ON)		On-Hook	ON	ON	ON = NETWORK AVAILABLE	ON
			Off-Hook			OFF = NETWORK NOT AVAILABLE	

## 2 Installing the DVW3201B

This chapter explains how to set up and connect the DVW3201B, connect additional devices, and troubleshoot the installation.



### Topics

See the following topics:

- ◆ [Setting Up and Connecting the DVW3201B on page 11](#)
- ◆ [Connecting Devices to the Network on page 12](#)
- ◆ [Troubleshooting the Installation on page 14](#)

### 2.1 Setting Up and Connecting the DVW3201B

Use the following instructions to set up and connect the DVW3201B. When the device is set up and connected, refer to [Accessing the Web Interface on page 17](#) to configure the device.

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

Typically, the service provider initially configures and connects the device. The installation steps are provided below if you wish to confirm the setup, or add devices to your network. Refer to [Connecting Devices to the Network on page 12](#).



### Steps

To set up the device:

1. Remove the contents from the device packaging.
2. Place the DVW3201B in the best location to connect to other devices, such as PCs or gaming consoles.
  - ◆ Place the wireless cable modem and wireless clients in open areas far away from transformers, heavy-duty motors, microwave ovens, refrigerators, fluorescent lights, and other manufacturing equipment. These items can impact wireless signals. A wireless signal can become weaker after it has passed through metal, concrete, brick, walls, or floors.
  - ◆ Place the device in a location that has an operating temperature of 0° C to 40° C (32° F to 104° F). Refer to [Understanding Safety and Regulatory Information on page 2](#) for more safety information.

3. Power on your PC. The PC must have an Ethernet network adaptor or Ethernet port and an Internet browser installed, such as Netscape or Internet Explorer. The following browsers are supported:
    - ◆ For Windows 2000, XP, Vista, Windows 7, 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 back of the cable modem and then to the power outlet.
  5. Insert the SMPCM9 battery into the battery housing on the bottom of the DVW3201B. Make sure the battery is inserted past the two clips on each side that hold the battery in place. The battery “clicks” into place when inserted properly. Use model SMPCM9 battery labeled: ONLY USE WITH DVW3201B.
  6. Connect the network cable included in the product package to your computer’s Ethernet port. Connect the other end to the ETH1, ETH2, ETH3, or ETH4 port to the cable modem.
  7. Connect a coaxial cable from the CABLE port on the device to the cable wall outlet, or to a cable splitter connected to the wall outlet.
  8. Connect an analog telephone if you will be using the device for telephone service to the TEL1 or TEL2 jack on the back panel of device. Use the supplied RJ11 telephone cable.
  9. Validate the network connection using the device LEDs to confirm operations:
    - ◆ The WiFi LED must be solidly lit.
    - ◆ The PWR, DS, US, and ONLINE LEDs are solidly lit.
- Refer to [Understanding LED Operations on page 8](#) for more information.

## 2.2 Connecting Devices to the Network

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

### 2.2.1 Connecting an Ethernet Device

You can connect up to three additional Ethernet devices to the DVW3201B.



#### Steps

##### To connect another Ethernet device to the network:

1. Connect the Ethernet cable from the Ethernet device (for example, a PC or gaming console) to an open Ethernet port on the back of the DVW3201B.
2. Use the device LEDs to confirm operations. Refer to [Understanding LED Operations on page 8](#) 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 14](#) for troubleshooting information.

### 2.2.2 Connecting a Wireless Device

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

Default values are shown in the steps below. Some regions may change default values using the cable modem or XML configuration file. Check with your provisioning team to determine the default values for your region.



#### Steps

##### To connect a wireless device to the cable modem:

1. Access the wireless networking feature on your wireless device. On a Windows computer, for example, double-click the **Wireless Network Connection** icon in the system tray (lower-right side of the Windows desktop).
2. Click **View Wireless Networks**. The device 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.
3. Double-click your **SSID** in the wireless networks window. The default SSID is the device name DVW3201B plus the last 2 characters of the cable modem's MAC address, with letters entered in upper case

Example: **DVW3201BE3**

**Notes:** You can find the MAC address on the device label or by opening an Internet browser window to the device. Refer to [Using the Information Option on page 21](#) for instructions. If the subscriber changes the SSID, the device does not revert to this default SSID upon any reset of the device, except in the case of a manual reset using the device's Web UI. See [Understanding the Tools Menu on page 81](#).

When prompted, enter the Network Key, which is the device name (DVW3201B) plus the last 6 characters (3 octets) of the cable modem's MAC address (UPPER case, if letters).

Example: **DVW3201B9822E3**

- ◆ If using WPS, enter the WPS personal identification number (PIN). The WPS PIN is a randomly-generated number found on the Wireless Primary Network screen. Refer to [Using the Primary Network Option on page 61](#).

**WPA-WPA2 AES** is the default encryption method.

4. Confirm connectivity by opening a Web browser and going to any Web site (for example, <http://www.wikipedia.org>) or access the Web interface for the DVW3201B.

**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 17](#).

If having wireless issues or questions, refer to [Deploying and Troubleshooting the Wireless Network on page 67](#).

### 2.2.3 Connecting a Telephone Line

You can connect up to two telephone lines to the DVW3201B to use the telephone (voice) features.

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

**Steps****To connect a telephone line:**

1. Connect an analog telephone to the TEL1 or TEL2 jack on the back panel of device using the supplied RJ11 telephone cable.
2. Pick up the telephone and listen for a dial tone.
3. Make a phone call and/or have someone call you to verify a successful connection.

## 2.3 Troubleshooting the Installation

Use the following tips to troubleshoot the installation.

☐ **None of the LEDs are on when I power on the DVW3201B.**

- ◆ Check the connection between the power outlet and the power adaptor. Verify the power outlet is energized and the power adaptor is connected to the power outlet.
- ◆ Check the connection between the power adaptor and the cable modem. Power off the cable modem and wait for 5 seconds and power on the modem again. If the problem still exists, there may be a hardware problem.

☐ **The ETH 1, 2, 3, or 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 cable modem.
- ◆ Check for a resource conflict (Windows users only):
  1. Right-click the **My Computer** icon 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 Adaptors field. If you see either one, you may have an interrupt request (IRQ) conflict. Refer to the manufacturer's documentation or your service provider for further assistance.
- ◆ Verify that TCP/IP is the default protocol for your network interface card.
  - ◆ Power cycle the cable modem by removing the power adaptor from the electrical outlet and plugging it back in. Wait for the cable modem to re-establish communications with your cable service provider.
- ❑ **Check General Connectivity Issues:**
- ◆ If your PC is connected to a hub or gateway, connect the PC directly into an Ethernet port on the cable modem.
  - ◆ If you are using a cable splitter, remove the splitter and connect the cable modem directly to the cable wall outlet. Wait for the cable modem to re-establish communications with the cable service provider.
  - ◆ Try a different cable. The Ethernet cable may be damaged.
- ❑ **The battery LED is not lit.**
- ◆ Verify you have the correct battery, model SMPCM9 labeled on the bottom of the battery: **ONLY USE WITH DVW3201B** or **ONLY USE WITH DVW32xx**.
  - ◆ Verify the battery is inserted correctly in the battery housing located on the bottom of the device. When inserting the battery into the housing, make sure the battery is inserted past the two clips on each side that hold the battery in place. The battery "clicks" into place when inserted properly.
- ❑ If none of these suggestions work, contact your cable service provider for further assistance.



## 3 Using the Web User Interface

The Web user interface (UI) for the DVW3201B is easy to use and allows you to view and configure several settings for your wireless gateway device. You can also validate the installation by accessing the Web user interface on the device.



### Topics

See the following topics:

- ◆ [Accessing the Web Interface on page 17](#)
- ◆ [Logging Out of the Web Interface on page 18](#)
- ◆ [Understanding Operation Modes and the Web User Interface on page 19](#)

### 3.1 Accessing the Web Interface

Access the Web user interface for the DVW3201B from a Web browser, such as Internet Explorer on a Windows computer.

Default values are shown in the steps below. Some regions may change default values using the cable modem or XML configuration file. Check with your provisioning team to determine the default values for your region.



### Steps

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 **<Enter>**.

<http://192.168.100.1>

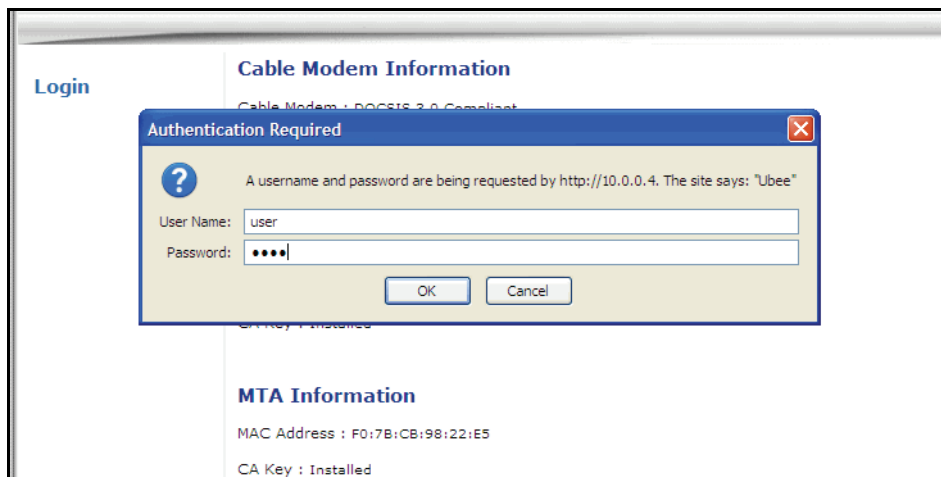
The Cable Modem Information screen displays general modem information about the device.

3. Click **Login** to access the Web interface.
4. At the login window, enter the user credentials:

- ◆ Standard subscriber Web interface login (enter in lower case letters):

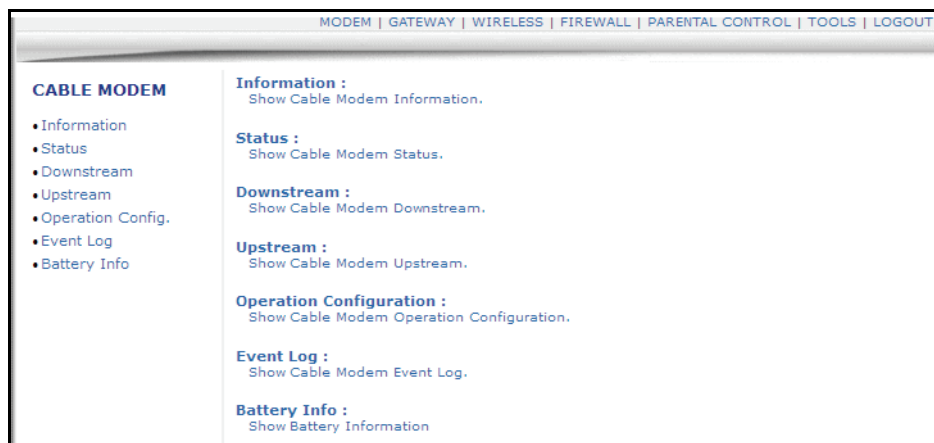
Username: **user**

Password: **user**



5. Click **OK**. The Cable Modem screen of the Web interface is displayed.

### Subscriber Options:



## 3.2 Logging Out of the Web Interface

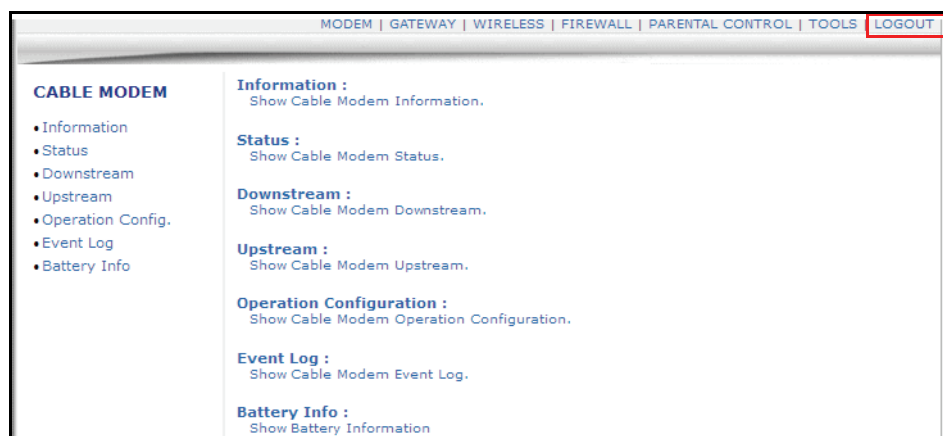
Log out when finished using the Web user interface.



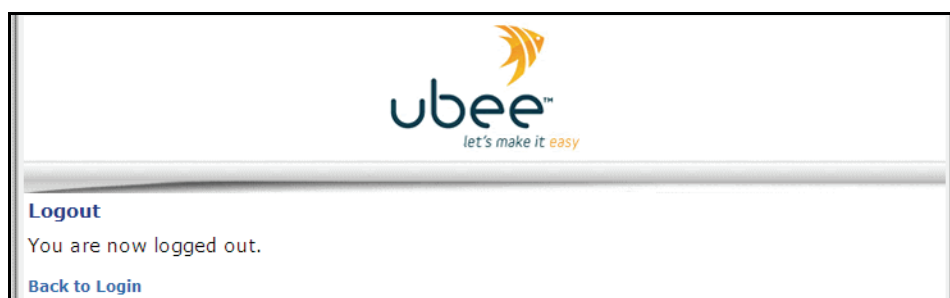
### Steps

#### To log out of the user interface:

1. Click **Logout** from the main menu.



The logout screen is displayed.



2. Click **Back to Login** to access the Login screen and begin a new user interface session.

### 3.3 Understanding Operation Modes and the Web User Interface

The DVW3201B provides four operation modes. Different options are available in the Web user interface depending on the mode and the type of user logged in. The operation mode is set from the Tools menu Operation Mode option.

#### Bridge

Provides a wireless side for a specific access point. Enables layer 2 protocols, in which (usually) one Public IP address is automatically assigned to the subscriber from the cable company's DHCP servers. In this mode, the first device to connect to a LAN or Wireless LAN interface gets the Public IP. Hint: Disable the wireless primary network SSID to ensure that only an Ethernet-based device (e.g., Home Router) gets the Public IP.

#### NAT

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.

**Router**

Operates in Router Mode for assigning Static Public IP addresses with RIP when this mode is enabled. DHCP, Firewall, and NAT functionality are disabled by default. When Route Mode is enabled, you can configure the device from the Web User Interface (UI) Routing screen, or through the Telnet Command Line Interface (CLI). Refer to [Using the Routing Setup Option on page 92](#) for more information.

**NAT Router**

Operates in NAT Router mode when enabled. Combines functionality found in both NAT and Router Modes. You can configure the device from the Web UI Routing screen or through the Telnet CLI. Refer to [Using the Routing Setup Option on page 92](#) for more information.

The following menus show the options available in each mode.

**Subscriber Web User Interface in Bridge Mode****Subscriber Web User Interface in NAT Mode****Subscriber Web User Interface in Router Mode****Subscriber Web User Interface in NAT Router Mode**



## 4 Understanding the Modem Menu

The **Modem** menu of the Web interface allows you to access information about the modem, such as status and battery information.



### Topics

See the following topics:

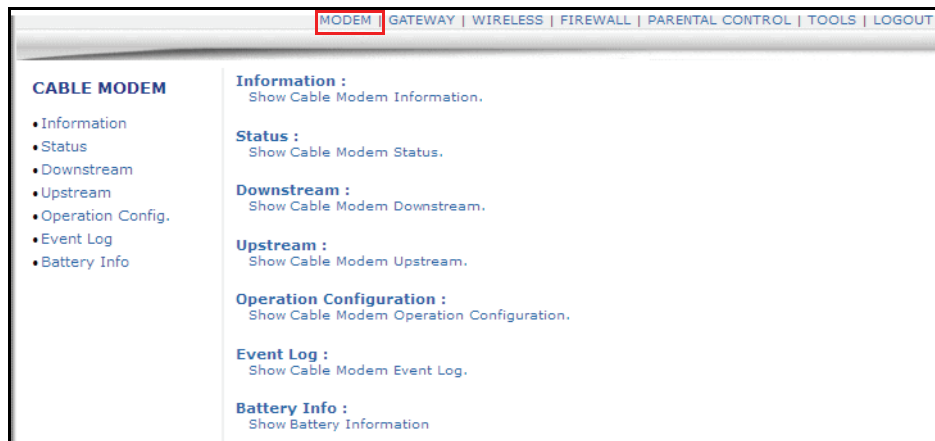
- ◆ [Using the Information Option on page 21](#)
- ◆ [Using the Status Option on page 23](#)
- ◆ [Using the Downstream Option on page 23](#)
- ◆ [Using the Upstream Option on page 25](#)
- ◆ [Using the Operation Config Option on page 26](#)
- ◆ [Using the Event Log Option on page 27](#)
- ◆ [Using the Battery Info Option on page 28](#)



### Steps

To access modem options:

1. Access the Web interface. Refer to [Accessing the Web Interface on page 17](#).
2. Click the **Modem** link from the top of the screen.



### 4.1 Using the Information Option

The **Information** option displays the device's internal software and hardware configuration.



## Steps

### To view modem information:

1. Click the **Modem** link from the top of the screen.
2. Click the **Information** link from the left side of the screen. Field explanations are listed below the following screen example.

Label	Description
<b>Cable Modem Information</b>	
<b>Cable Modem</b>	Defines the current DOCSIS standard of the device.
<b>MAC Address</b>	Defines the unique media access control (MAC) hardware address of the cable modem.
<b>Serial Number</b>	Defines the unique manufacturer serial number of the device.
<b>Boot Code Version</b>	Defines the boot software code version of the device.
<b>Software Version</b>	Defines the general software version of the device.
<b>Hardware Version</b>	Defines the internal version number that identifies the hardware design.
<b>CA Key</b>	Defines the certificate authority (CA) key. The device installs a CA key that is transferred from the service provider's server after the cable modem is authenticated. The key is used to secure communication between the service provider and the cable modem.
<b>MTA Information</b>	
<b>MAC Address</b>	Displays the MAC address for the MTA module (voice/telephony). The device has a unique MAC address, like the cable modem module.
<b>CA Key</b>	Displays the CA key for the MTA module (voice/telephony). The device installs a CA key that is transferred from the service provider after the cable modem is authenticated.

## 4.2 Using the Status Option

The **Status** screen displays the device's general connection information.



### Steps

#### To view modem status:

1. Click the **Modem** link from the top of the screen.
2. Click the **Status** link from the left side of the screen. Field explanations are listed below the following screen example.

MODEM | GATEWAY | WIRELESS | FIREWALL | PARENTAL CONTROL | TOOLS | LOGOUT

CABLE MODEM

- Information
- Status
- Downstream
- Upstream
- Operation Config.
- Event Log
- Battery Info

Cable Modem Status

Item	Status	Comments
Acquired Downstream Channel	321.000000 MHz	Primary Downstream Locked
Ranged Upstream Channel	25.400000 MHz	Success
CM Provisioning State	OK	Operational
MTA Provisioning State	Pass With Warnings	

Refresh

Label	Description
Acquired Downstream Channel	Displays the Downstream channel tat the cable modem is trying to lock to and its progress.
Ranged Upstream Channel	Displays the Upstream channel the cable modem is trying to lock to and its progress.
CM Provisioning State	Indicates the state of the device, operational or otherwise (for example, In Progress, Disabled).
MTA Provisioning State	Indicates the state of the voice portion (MTA) of the device, operational or otherwise (for example, In Progress).

## 4.3 Using the Downstream Option

The **Downstream** screen displays detailed information on the network traffic from the service provider to the local computer (downstream channels).



### Steps

#### To view downstream information:

1. Click the **Modem** link from the top of the screen.
2. Click the **Downstream** link from the left side of the screen. Field explanations are listed below the following screen example.

MODEM   GATEWAY   WIRELESS   FIREWALL   PARENTAL CONTROL   TOOLS   LOGOUT				
<b>CABLE MODEM</b>				
<ul style="list-style-type: none"> <li>• Information</li> <li>• Status</li> <li>• <b>Downstream</b></li> <li>• Upstream</li> <li>• Operation Config.</li> <li>• Event Log</li> <li>• Battery Info</li> </ul>				
<b>Cable Modem Downstream</b>				
	DS-1	DS-2	DS-3	DS-4
Frequency	321000000	303000000	309000000	315000000
Lock Status	Locked	Locked	Locked	Locked
Channel Id	2	3	4	1
Modulation	256QAM	256QAM	256QAM	256QAM
Symbol Rate (Msym/sec)	5.360537	5.360537	5.360537	5.360537
Interleave Depth	I=8 J=16	I=8 J=16	I=8 J=16	I=8 J=16
Power Level (dBmV)	1.4	1.2	0.9	1.5
RxMER (dB)	45.60	45.40	45.40	45.50
Correctable Codewords	0	0	0	0
Uncorrectable Codewords	0	0	0	0
	DS-5	DS-6	DS-7	DS-8
Frequency	-999	-999	-999	-999
Lock Status	Not-Locked	Not-Locked	Not-Locked	Not-Locked
Channel Id	N/A	N/A	N/A	N/A
Modulation	Unknown	Unknown	Unknown	Unknown
Symbol Rate (Msym/sec)	Unknown	Unknown	Unknown	Unknown
Interleave Depth	Unknown	Unknown	Unknown	Unknown
Power Level (dBmV)	-999	-999	-999	-999
RxMER (dB)	-999	-999	-999	-999
Correctable Codewords	0	0	0	0
Uncorrectable Codewords	0	0	0	0
<input type="button" value="Refresh"/>				

Label	Description
<b>DS-1 to DS-8</b>	Numbers the downstream channels.
<b>Frequency</b>	Displays the downstream channel frequency on which the cable modem is scanning.
<b>Lock Status</b>	Displays if the cable modem succeeded in locking to a downstream channel.
<b>Channel Id</b>	Displays the downstream channel ID.
<b>Modulation</b>	Displays the modulation method required for the downstream channel to lock on to by the cable modem. This method is determined by the service provider.
<b>Symbol Rate (Msym/sec)</b>	Displays the symbol rate. Current cable modem downstream symbol rates: <ul style="list-style-type: none"> <li>♦ QAM64 is 5056941 sym/sec</li> <li>♦ QAM256 is 5360537 sym/sec</li> </ul>
<b>Interleave Depth</b>	Displays the current cable modem downstream Interleave depth (4/8/16/32/64/128/other).
<b>Power Level (dBmV)</b>	Displays the receiver power level in millivolts after ranging process.

Label	Description
<b>RxMER (dB)</b>	Displays the Receiver Modulation Error Ratio used to quantify the performance of a digital radio receiver in a communications system using digital modulation.
<b>Correctable Codewords</b>	Displays the quantity of codewords which are correctable.
<b>Uncorrectable Codewords</b>	Displays the quantity of codewords which are not correctable.
<b>Refresh</b>	Updates the screen with the latest information.

## 4.4 Using the Upstream Option

The **Upstream** screen displays detailed information on the network traffic **from** the computer to the remote destination (upstream channels).



### Steps

To view upstream information:

1. Click the **Modem** link from the top of the screen.
2. Click the **Upstream** link from the left side of the screen. Field explanations are listed below the following screen example.

	US-1	US-2	US-3	US-4
<b>Channel Type</b>	1.1/2.0	N/A	N/A	N/A
<b>Channel Id</b>	1	N/A	N/A	N/A
<b>Frequency (HZ)</b>	25400000	N/A	N/A	N/A
<b>Ranging Status</b>	Success	N/A	N/A	N/A
<b>Modulation</b>	64QAM	N/A	N/A	N/A
<b>Symbol Rate (Ksym/sec)</b>	5120	N/A	N/A	N/A
<b>Mini-Slot Size</b>	2	N/A	N/A	N/A
<b>Power Level (dBmV)</b>	32.2	N/A	N/A	N/A
<b>T1 Timeouts</b>	0	N/A	N/A	N/A
<b>T2 Timeouts</b>	0	N/A	N/A	N/A
<b>T3 Timeouts</b>	0	N/A	N/A	N/A
<b>T4 Timeouts</b>	0	N/A	N/A	N/A

Label	Description
<b>US-1 to US-4</b>	Numbers the upstream channels.
<b>Channel Type</b>	Displays the channel type.
<b>Channel Id</b>	Displays the current cable modem upstream channel ID.
<b>Frequency (Hz)</b>	Displays the current cable modem upstream frequency in hertz.
<b>Ranging Status</b>	Displays the upstream ranging status.

Label	Description
<b>Modulation</b>	Displays the current cable modem upstream modulation type (QPSK/ QAM8 /QAM16/ QAM32/ QAM64/ QAM128/ QAM256).
<b>Symbol Rate (Ksym/sec)</b>	Displays the symbol rate.
<b>Upstream Mini-Slot Size</b>	Displays the current cable modem upstream mini-slot size in Timebase Ticks of 6.25.
<b>Power Level (dBmV)</b>	Displays the current cable modem upstream transmit power in decibel millivolts.
<b>T-1</b>	Displays DHCP time expiration.
<b>T-2</b>	Displays DHCP time expiration.
<b>T-3</b>	Displays range response (RNG-RSP) time expiration.
<b>T-4</b>	Displays range (RNG) time expiration.

## 4.5 Using the Operation Config Option

The **Operation Config** screen displays general information on the device's active operational capabilities.



### Steps

To view operation configuration information:

1. Click the **Modem** link from the top of the screen.
2. Click the **Operation Config** link from the left side of the screen. Field explanations are listed below the following screen example.

The screenshot shows the 'Cable Modem Operation Configuration' screen. The left sidebar has a 'CABLE MODEM' section with links: Information, Status, Downstream, Upstream, Event Log, and Battery Info. The 'Upstream' link is expanded, and 'Operation Config.' is highlighted. The main content area is titled 'Cable Modem Operation Configuration' and contains the following information:

General Configuration	
Network Access :	Allowed
Maximum Number of CPEs :	1
Baseline Privacy :	Disabled
DOCSIS Mode :	DOCSIS 3.0
Primary Downstream Service Flow	
SFID :	10614
Priority :	0
Max Traffic Rate :	0 bps
Max Traffic Burst :	3044 bytes
Max Concatenated Burst :	1522 bytes
Primary Upstream Service Flow	
SFID :	10613
Priority :	0
Max Traffic Rate :	0 bps
Max Traffic Burst :	3044 bytes
Max Concatenated Burst :	1522 bytes
Scheduling Type :	Best Effort

Label	Description
<b>General Configuration</b>	
<b>Network Access</b>	Displays the status of the cable modem. ♦ Denied – Connectivity is not established. ♦ Allowed – connectivity is established to the Internet.
<b>Maximum Number of CPEs</b>	Displays the maximum number of Ethernet devices that can be connected (LAN side) to access the network at the same time.
<b>Baseline Privacy</b>	Displays highlighted device configurations, such as PHS Enabled.
<b>DOCSIS Mode</b>	Displays the DOCSIS version of the device.
<b>Primary Downstream Service Flow</b>	
<b>SFID</b>	Displays the frequency ID of the downstream service flow.
<b>Priority</b>	Displays the priority level of the downstream service flow.
<b>Max Traffic Rate</b>	Displays the max data rate as enabled by the service provider.
<b>Max Traffic Burst</b>	Displays the max data rate as enabled by the service provider for downstream data bursts.
<b>Max Concatenated Burst</b>	Displays the max data rate per downstream burst.
<b>Primary Upstream Service Flow</b>	
<b>SFID</b>	Displays the frequency ID of the upstream service flow.
<b>Priority</b>	Displays the priority level of the upstream service flow.
<b>Max Traffic Rate</b>	Displays the max data rate as enabled by the service provider.
<b>Max Traffic Burst</b>	Displays the max data rate as enabled by the service provider for upstream data bursts.
<b>Max Concatenated Burst</b>	Displays the max data rate per upstream burst.
<b>Scheduling Type</b>	Displays the data scheduling type.

## 4.6 Using the Event Log Option

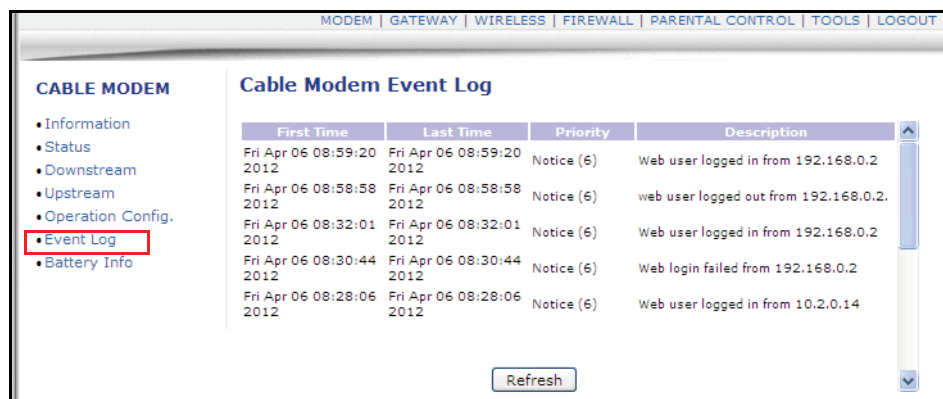
The **Event Log** screen displays log information that may be useful to diagnose operational issues with the device.



### Steps

#### To view event log information:

1. Click the **Modem** link from the top of the screen.
2. Click the **Event Log** link from the left side of the screen. Field explanations are listed below the following screen example.



Label	Description
<b>First Time</b>	Displays the time the event started.
<b>Last Time</b>	Displays the last time the event was last recorded.
<b>Priority</b>	Displays the event log severity.
<b>Description</b>	Displays a detailed description of the event log.
<b>Refresh</b>	Updates the event log record to its most current state when you click Refresh.

## 4.7 Using the Battery Info Option

The **Battery Info** screen displays current battery information, including estimated time remaining and current levels. In the event of a power loss, the battery provides:

- ☐ Up to 8.5 hours of standby time
- ☐ Four hours of talk time with two lines off-hook
- ☐ One upstream and one downstream channel

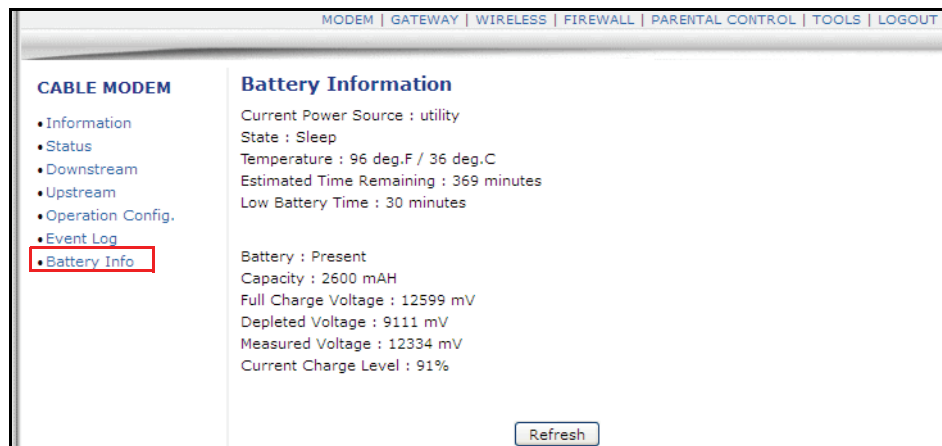


### Steps

#### To view battery information:

1. Click the **Modem** link from the top of the screen.
2. Click the **Battery Info** link from the left side of the screen. Field explanations are listed below the following screen example.





Label	Description
<b>Current Power Source</b>	Displays the power source for the device, such as Utility through the power cord or internal battery power.
<b>State</b>	Displays the status of the battery, such as Sleep or Idle.
<b>Temperature</b>	Displays the battery temperature in Fahrenheit and Celsius.
<b>Estimated Time Remaining</b>	Displays how much time is left on the battery in minutes.
<b>Low Battery Time</b>	Displays low battery time in minutes.
<b>Battery</b>	Displays if a battery is Present or Absent.
<b>Capacity</b>	Displays the battery capacity in milliampere-hours (mAH).
<b>Full Charge Voltage</b>	Displays voltage with a full charge in millivolts (mV).
<b>Depleted Voltage</b>	Displays voltage with a depleted charge in millivolts (mV).
<b>Measured Voltage</b>	Displays the measured voltage in millivolts (mV).
<b>Current Charge Level</b>	Displays charge level as percent charged.



## 5 Understanding the Gateway Menu

The Gateway functions provide the majority of configuration for the device including WAN IP addresses, LAN IP addresses, and DHCP. Advanced settings like MAC filtering and port forwarding are provided.



### Topics

See the following topics:

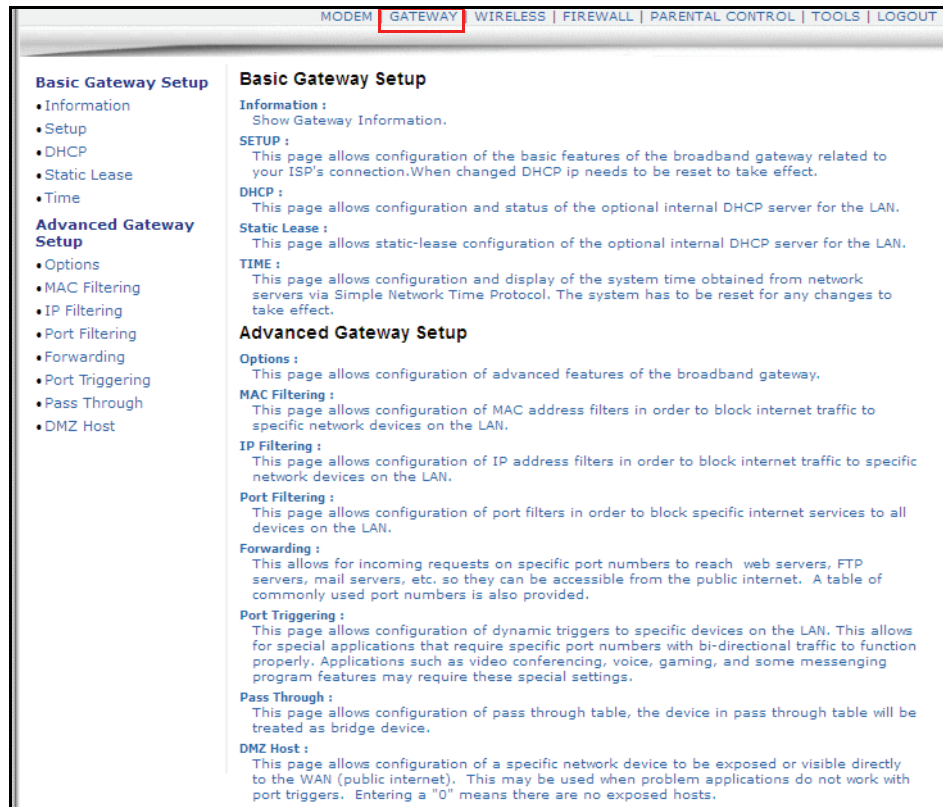
- ◆ [Using the Gateway Information Option on page 32](#)
- ◆ [Using the Setup Option on page 34](#)
- ◆ [Using the DHCP Option on page 37](#)
- ◆ [Using the DHCP Static Lease Option on page 39](#)
- ◆ [Using the Time Option on page 40](#)
- ◆ [Using the Advanced Gateway Setup Options on page 41](#)
- ◆ [Using the Advanced Gateway Setup MAC Filtering Option on page 44](#)
- ◆ [Using the Advanced Gateway Setup IP Filtering Option on page 45](#)
- ◆ [Using the Advanced Gateway Setup Port Filtering Option on page 46](#)
- ◆ [Using the Advanced Gateway Setup Forwarding Option on page 47](#)
- ◆ [Using the Advanced Gateway Setup Port Triggering Option on page 51](#)
- ◆ [Using the Advanced Gateway Settings Pass Through Option on page 53](#)
- ◆ [Using the Advanced Gateway Settings DMZ Host Option on page 54](#)



### Steps

To access the gateway menu:

1. Access the Web interface. Refer to [Accessing the Web Interface on page 17](#).
2. Click the **Gateway** link from the top of the screen.



## 5.1 Using the Gateway Information Option

The **Information** option allows you to view basic information for the device.



### Steps

To view gateway information:

1. Click the **Gateway** link from the top of the screen.
2. Click **Information**. **Information** fields are defined following this screen example.

MODEM | GATEWAY | WIRELESS | FIREWALL | PARENTAL CONTROL | TOOLS | LOGOUT

**Basic Gateway Setup**

- **Information**
- Setup
- DHCP
- Static Lease
- Time

**Advanced Gateway Setup**

- Options
- MAC Filtering
- IP Filtering
- Port Filtering
- Forwarding
- Port Triggering
- Pass Through
- DMZ Host

**Gateway - Information**

**INTERNET SETTINGS**

Gateway MAC Address: f0:7b:cb:98:22:e6  
 Internet IP Address: 10.2.0.7  
 Subnet Mask: 255.255.0.0  
 Default Gateway: 10.0.0.1  
 DNS: 65.106.1.196  
 65.106.7.196  
 192.168.250.251  
 DHCP Remaining Time: 0 days 21:42:37

**LOCAL SETTINGS**

Gateway IP Address: 192.168.0.1  
 Subnet Mask: 255.255.255.0  
 DHCP Server: Enabled  
 NAT : Enabled  
 Wireless Status : Enabled  
 Operating Mode: NAT mode  
 Private IP Range: 192.168.0.2 through 192.168.0.254  
 Public IP Range: 0.0.0.0 through 0.0.0.0  
 System Up-Time: 2 Hours 18 Minutes 20 Seconds

Label	Description
<b>Internet Settings</b>	
<b>Gateway MAC Address</b>	Displays the Media Access Control (MAC) address of the residential gateway.
<b>Internet IP Address</b>	Displays the Internet IP address obtained from the service provider.
<b>Subnet Mask</b>	Displays the subnet mask of the Internet IP address.
<b>Default Gateway</b>	Displays the default gateway IP address.
<b>DNS</b>	Displays the DNS server IP address.
<b>DHCP Remaining Time</b>	Displays the time remaining on the DHCP lease before it expires.
<b>Refresh</b>	Updates the information to its most current state when you click Refresh.
<b>Local Settings</b>	
<b>Gateway IP Address</b>	Displays the local IP address of the LAN interface.
<b>Subnet Mask</b>	Displays the subnet mask value.
<b>DHCP Server</b>	Displays the status of the DHCP sever feature (Enabled/Disabled).
<b>NAT</b>	Displays the status of the NAT feature (Enabled/Disabled).
<b>Wireless Status</b>	Displays the status of the wireless feature (Enabled/Disabled).
<b>Operating Mode</b>	Displays which mode the router is in (Bridge, Router, Gateway). <b>Note:</b> Firewall menu options are not available when the device is in Bridge mode.

Label	Description
<b>Private IP Range</b>	Displays the private IP address assigned to the DHCP client.
<b>Public IP Range</b>	Displays the Public IP DHCP Server Range.
<b>System Up-Time</b>	Displays the accumulated time since the last power cycle.

## 5.2 Using the Setup Option

The **Setup** option allows you to make basic configurations to the device.



### Steps

To configure gateway settings:

1. Click the **Gateway** link from the top of the screen.
2. Click **Setup** from the left side of the screen. The **Setup** fields are explained following this screen example.

Label	Description
<b>LAN</b>	
<b>IP Address</b>	Defines the local IP address, which is the default gateway address for all wired LAN hosts that connect to the DVW3201B.
<b>MAC Address</b>	Displays the LAN interface's hardware address.
<b>WAN</b>	
<b>IP Address</b>	Displays the current WAN public IP address obtained from the service provider.

Label	Description
<b>MAC Address</b>	Displays the WAN interface's hardware address.
<b>Duration</b>	Displays the accumulated time since successfully acquiring a WAN public IP address.
<b>Expires</b>	Displays the remaining time before the WAN IP address expires, if applicable.
<b>IPv4 DNS Servers</b>	Lists the DNS servers available on the network.
<b>Release WAN Lease</b>	Releases the WAN public IP address when clicked.
<b>Renew WAN Lease</b>	Renews the WAN IP address when clicked.
<b>WAN Connection Type</b>	<p>Selects the WAN connection type. For each type, different data entry is required, as explained below:</p> <ul style="list-style-type: none"> <li>♦ DHCP: The WAN interface is set to a DHCP client, and the IP address is assigned by the service provider's DHCP server.</li> <li>♦ Static IP: For Static IP, you must manually enter the IP address for the WAN interface.</li> <li>♦ PPTP (DHCP): For Point to Point Tunneling Protocol (PPTP), you must enter a username, password, and the PPTP server's IP address.</li> </ul>
<b>Host Name</b>	Defines the host name for the router. This may be required by some service providers.
<b>Domain Name</b>	Defines the domain for the router. This may be required by some service providers.
<b>IPv4 MTU Size</b>	Defines 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.
<b>Apply</b>	Saves all changes made in this screen when clicked.

## 5.2.1 Viewing IPv6 Addresses in the Gateway Setup Option

Additional IP addresses are needed to support the increase in Internet activity. Internet Protocol version 6 (IPv6) addressing is supported by the DVW3201B and displayed when the CMTS uses IPv6. The screen shot below displays an IPv6 address configuration in the Gateway Basic Setup option.

MODEM | GATEWAY | WIRELESS | VPN | ROUTING | FIREWALL | PARENTAL CONTROL | TOOLS | LOGOUT

**Basic Gateway Setup**

- Information
- **Setup**
- DHCP
- LAN IPv6
- Static Lease
- Time

**Advanced Gateway Setup**

- Options
- MAC Filtering
- IP Filtering
- Port Filtering
- Forwarding
- Port Triggering
- Pass Through
- DMZ Host

**Gateway - Basic Setup**

**Network Configuration**

**LAN**

IPv6 Address: 2011:7:1:1:f27b:cbff:fe98:1d7e/64  
fe80::f27b:cbff:fe98:1d7e/64

IPv6 Prefix: 2011:7:1:1::/64

IPv4 Address: 192.168.0.1

MAC Address: f0:7b:cb:98:1d:7e

**WAN**

IPv6 Address: fe80::f27b:cbff:fe98:1d7c/64  
2011:7:5f/128

IPv4 Address: 192.168.52.30

MAC Address: f0:7b:cb:98:22:e4

Duration: D: 01 H: 00 M: 00 S: 00

Expires: Thu Feb 02 01:04:03 2012

IPv4 DNS Servers: 65.106.1.196  
65.106.7.196

IPv6 DNS Servers: None

Release WAN Lease Renew WAN Lease

WAN Connection Type: DHCP

Host Name: (Required by some ISPs)

Domain Name: (Required by some ISPs)

IPv4 MTU Size: 0 (256-1500 octets, 0 = use default)

Apply

## 5.2.2 Using the LAN IPv6 Option

When the CMTS supports IPv6 address configuration, the LAN IPv6 option is available. The LAN IPv6 screen displays the assigned IP addresses which uses the Stateless Auto Configuration feature. Stateless Auto Configuration allows devices attached to an IPv6 network to connect to the Internet without requiring DHCP support.

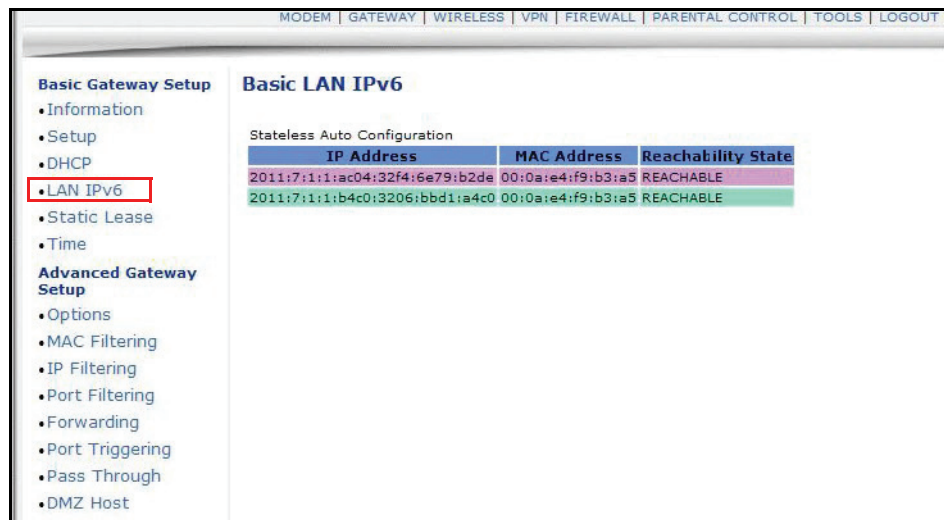


### Steps

#### To view assigned IPv6 addresses:

1. Click the **Gateway** link from the top of the screen.
2. Click **LAN IPv6** from the left side of the screen. The LAN IPv6 fields are explained following this screen example.





Label	Description
IP Address	Displays the IPv6 address of the connected device.
MAC Address	Displays the MAC address of the connected device.
Reachability State	Displays the status of the neighboring device. Reachable indicates the device can be contacted and configuration information can be obtained from the device.

## 5.3 Using the DHCP Option

The dynamic host configuration protocol (DHCP) option allows you to configure DHCP-specific behavior on the device.



### Steps

#### To configure DHCP settings:

1. Click the **Gateway** link from the top of the screen.
2. Click **DHCP** from the left side of the screen. The **DHCP** fields are explained following this screen example.

MODEM | GATEWAY | WIRELESS | FIREWALL | PARENTAL CONTROL | TOOLS | LOGOUT

**Basic Gateway Setup**

- Information
- Setup
- **DHCP**
- Static Lease
- Time

**Advanced Gateway Setup**

- Options
- MAC Filtering
- IP Filtering
- Port Filtering
- Forwarding
- Port Triggering
- Pass Through
- DMZ Host

**Gateway - DHCP**

DHCP Server ☒ Yes ☐ No

Starting Address Set

☒ Private Starting Address 192.168.0.2 (2~254) Number of CPEs 253

☐ Public Starting Address 0.0.0.0 (2~254) Number of CPEs 0

Lease Time 3600

DHCP Clients

MAC Address	IP Address	Subnet Mask	Duration	Expires	Select
00:25:B3:B9:C4:D6	192.168.0.2	255.255.255.0	D:00 H:01 M:00 S:00	Wed Mar 14 09:46:08 2012	<input type="radio"/>

Current System Time: Wed Mar 14 09:01:52 2012

Label	Description
<b>DHCP Server</b>	Enables (Yes) or disables (No) DHCP on the device. If No is selected, all the static DHCP rules in this screen are ignored.
<b>Private Starting Address</b>	Defines the starting private IP address for the pool of IP addresses that can be used by connecting clients. Private addresses are translated to public IPs to be used on the network.
<b>Public Starting Address</b>	Defines the starting public IP address. Public addresses can be recognized on the network.
<b>Number of CPEs</b>	Defines the maximum number of customer premises equipment (CPE) that can connect to the network through the DVW3201B.
<b>Lease Time</b>	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. <b>Note:</b> The default DHCP lease time is 3600 seconds and should be changed to <b>86400</b> seconds (24 hours). This helps resolve connectivity issues with some 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.

Label	Description
<b>Apply</b>	Applies and saves all changes when clicked.
<b>DHCP Clients</b>	Lists all DHCP clients currently connected to the device, either via an Ethernet link, or via a wireless connection. Each client is listed with the following information: <ul style="list-style-type: none"> <li>♦ MAC Address / IP Address / Subnet Mask</li> <li>♦ Duration / Expires: Duration displays the accumulated time since the client acquired the IP address. Expires is the time until the IP expires and must be recycled. If the IP address is reserved to a certain host, it shows STATIC IP ADDRESS.</li> <li>♦ Select: Reserves the current private IP address to be assigned to this host statically when selected.</li> </ul>
<b>Force Available</b>	Activates a selected rule in the DHCP Clients list and assigns IP addresses. Note: The Select button must be activated in the DHCP list.

## 5.4 Using the DHCP Static Lease Option

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

- ♦ [Using the Advanced Gateway Setup IP Filtering Option on page 45](#)
- ♦ [Using the Advanced Gateway Setup Port Filtering Option on page 46](#)
- ♦ [Using the Advanced Gateway Settings DMZ Host Option on page 54](#)



### Steps

#### To assign static IP addresses:

1. Click the **Gateway** link from the top of the screen.
2. Click **Static Lease** from the left side of the screen. The **Static Lease** fields are explained following this screen example.

**Note:** The following example shows the DHCP Static Lease option set up for a dual Xbox configuration.

MODEM | GATEWAY | WIRELESS | FIREWALL | PARENTAL CONTROL | TOOLS | LOGOUT

**Basic Gateway Setup**

- Information
- Setup
- DHCP
- **Static Lease**
- Time

**Advanced Gateway Setup**

- Options
- MAC Filtering
- IP Filtering
- Port Filtering
- Forwarding
- Port Triggering
- Pass Through
- DMZ Host

**Gateway - DHCP Static Lease**

Note: If some IP addresses turn to red color, you should check the DHCP pools!  
Current DHCP Server IP Ranges' information  
Private IP Range: 192.168.0.3 -- 192.168.0.253  
Public IP Range: 0.0.0.0 -- 0.0.0.0

Index	MAC Address	IP Address	Enabled	Clear
1.	f4 : ce : 46 : e3 : 96 : 91	192.168.0.11	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2.	00 : 22 : fa : 9c : 4d : b6	192.168.0.12	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>
4.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>
5.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>
6.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>
7.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>
8.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>

Apply

Label	Description
Index	Provides an index number for each client that connects to your network.
MAC Address	Defines the MAC address of the client to which you want to assign a static IP address.
IP Address	Defines an IP address to the specific client/host.
Enabled	Activates this rule when Enable is checked.
Clear	Deletes the rule when Clear is checked.
Apply	Saves all screen changes when clicked.

## 5.5 Using the Time Option

The **Time** option allows you to configure the system time obtained from network servers via Simple Network Time Protocol (SNTP). SNTP is a protocol for synchronizing the clocks of computing devices over networks. The device must be reset for changes to take effect.



### Steps

#### To configure system time:

1. Click the **Gateway** link from the top of the screen.
2. Click **Time** from the left side of the screen. The **Time** fields are explained following this screen example.

Label	Description
<b>Enable SNTP</b>	Enables (Yes) or disables (No) the SNTP feature.
<b>Current Time</b>	Displays the current system time.
<b>System Start Time</b>	Displays the accumulated time since the system was started.
<b>Time Server 1</b>	Defines the IP address or Domain name of the time server. Use the one provided or enter an alternative choice.
<b>Time Server 2</b>	Defines the IP address or Domain name of the time server. Use the one provided or enter an alternative choice.
<b>Time Server 3</b>	Defines the IP address or Domain name of the time server. Use the one provided or enter an alternative choice.
<b>Time Zone Offset</b>	Defines the time zone offset in hours and minutes from Greenwich MEan Time. For example: 8 hours means GMT +8, -1 hour means GMT -1.
<b>Apply</b>	Saves all screen changes when clicked.
<b>Reset Values</b>	Resets the screen to factory defaults when clicked.

## 5.6 Using the Advanced Gateway Setup Options

The **Options** selection allows you to define what networking protocols are enabled or disabled on the device. The network address translation application-level gateway (NAT ALG) settings provide additional security beyond the firewall.



### Steps

#### To enable or disable network protocols:

1. Click the **Gateway** link from the top of the screen.
2. Click **Options** from the left side of the screen. The **Options** fields are explained following this screen example.

MODEM | GATEWAY | WIRELESS | FIREWALL | PARENTAL CONTROL | TOOLS | LOGOUT

**Basic Gateway Setup**

- Information
- Setup
- DHCP
- Static Lease
- Time
- Advanced Gateway Setup**
  - **Options**
  - MAC Filtering
  - IP Filtering
  - Port Filtering
  - Forwarding
  - Port Triggering
  - Pass Through
  - DMZ Host

**Advanced Gateway - Options**

WAN Blocking ☐ Enable

Isec PassThrough ☒ Enable

PPTP PassThrough ☒ Enable

Multicast Enable ☐ Enable

UPnP Enable ☒ Enable

DNS Relay ☐ Enable

NAT ALG Status

RSVP ☒ Enable

FTP ☒ Enable

TFTP ☒ Enable

Kerb88 ☒ Enable

NetBios ☒ Enable

IKE ☒ Enable

RTSP ☒ Enable

Kerb1293 ☒ Enable

H225 ☒ Enable

PPTP ☒ Enable

MSN ☒ Enable

SIP ☒ Enable

ICQ ☒ Enable

IRC666x ☒ Enable

ICQTalk ☒ Enable

Net2Phone ☒ Enable

IRC7000 ☒ Enable

IRC8000 ☒ Enable

Apply

Label	Description
<b>WAN Blocking</b>	Blocks connection requests initialized from Internet users when enabled. WAN Blocking must be disabled to be able to PING the WAN gateway IP.
<b>Isec PassThrough</b>	Forces the router to redirect the IPsec request to the local host when enabled. NAT fails this attempt if Internet users initialize an IPsec VPN request to a host located behind the router.
<b>PPTP PassThrough</b>	Forces the router to redirect the PPTP request to the local host when enabled. Nat fails this attempt if Internet users initialize a PPTP VPN request to a host located behind the router.
<b>Multicast Enable</b>	Optimizes the bandwidth utilization compared with unicast (especially video streaming applications).
<b>UPnP Enable</b>	Activates Universal Plug and Play (UPnP) when enabled. A UPnP device can dynamically join a network, obtain an IP address, convey its 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.

Label	Description
<b>DNS Relay</b>	Allows the cable modem to act as the “relay” device. Each PC that wants to access a URL does not have to send a DNS request to a DNS server on the Internet. DNS is used to resolve a URL (Web site name) to an IP address. DNS Relay is typically used for commercial applications where each device/PC connected to the cable modem uses the DNS Relay address rather than going to a public DNS server hosted by an ISP to look-up a URL.
<b>NAT ALG Status</b> – Filters to allow (enable) or disallow (disable) protocols to pass through the DVW3201B to connected devices (computers, game consoles, and so on).	
<b>RSVP</b>	Enables or disables resource reservation protocol (RSVP). RSVP defines how applications reserve resources and how they free the reserved resources once they are no longer needed.
<b>FTP</b>	Enables or disables the file transfer protocol (FTP) used to transfer files from one host to another.
<b>TFTP</b>	Enables or disables the trivial file transfer protocol (TFTP) – a simpler protocol generally used for automated file transfers.
<b>Kerb88</b>	Enables or disables the Kerberos network authentication protocol which allow nodes to communicate over a non-secure network using “tickets” on port 88 to prove their identity to one another.
<b>NetBios</b>	Enables or disables the network basic input/output system (NetBIOS) services related to the OSI session layer. NetBIOS allows applications on separate computers to communicate over a LAN.
<b>IKE</b>	Enables or disables the network key exchange (IKE) protocol used to set up a security association (SA) in the IPsec protocol suite.
<b>RTSP</b>	Enables or disables the real time streaming protocol (RTSP) network control protocol used to establish and control media sessions between end points.
<b>Kerb1293</b>	Enables or disables the Kerberos network authentication protocol which allow nodes to communicate over a non-secure network using “tickets” on port 1293.
<b>H225</b>	Enables or disables the H.225 protocol used to define messages and procedures for call signalling, media packetization, and registration, admission, and status (RAS) functions.
<b>PPTP</b>	Enables or disables the point-to-point tunneling protocol (PPTP) used to implement a virtual private network.
<b>MSN</b>	Enables or disables the Microsoft network protocol used for instant messaging.

Label	Description
<b>SIP</b>	Enables or disables the session initiation protocol application layer gateway (SIP ALG). SIP ALG inspects protocol packets and formats SIP message headers and SDP body to ensure proper signaling. <b>Note:</b> Some hosted VoIP services prefer this function to be performed by their own session border controller (SBC) and require the SIP ALG to be disabled. Some IP-PBXs may require SIP ALG enabled.
<b>ICQ</b>	Enables or disables the ICQ instant messaging program.
<b>IRC666x</b>	Enables or disables the Internet relay chat (IRC) protocol used for text messaging.
<b>ICQTalk</b>	Enables or disables the ICQTalk instant messaging program.
<b>Net2Phone</b>	Enables or disables Net2Phone SIP VoIP.
<b>IRC7000</b>	Enable or disables the Internet relay chat protocol on TCP port 7000 used for text messaging and group forums.
<b>IRC8000</b>	Enable or disables the Internet relay chat protocol on UDP port 8000 used for text messaging and group forums.
<b>Apply</b>	Saves all screen changes when clicked.

## 5.7 Using the Advanced Gateway Setup MAC Filtering Option

The **MAC Filtering** option allows you to filter MAC addresses to block Internet traffic from specific network devices on the LAN. MAC filtering establishes a list and any host on this list is not able to access the network through the DVW3201B.



### Steps

#### To filter MAC addresses:

1. Go to **Tools>>Client List**. Your PC and other devices are listed. Note the MAC address of the devices that you want to deny Internet access. For more information, refer to [Using the Client List Option on page 83](#).

**Note:** Be sure all devices to which you potentially deny Internet access are connected to the DVW3201B network.

2. Click the **Gateway** link from the top of the screen.
3. Click **MAC Filtering** from the left side of the screen. The **MAC Filtering** fields are explained following this screen example.



Index	MAC Address	Clear
1.	00 : 25 : b4 : b8 : c4 : d4	<input type="checkbox"/>
2.	00 : 25 : b6 : b8 : c3 : e4	<input type="checkbox"/>
3.	00 : 00 : 00 : 00 : 00 : 00	<input type="checkbox"/>
4.	00 : 00 : 00 : 00 : 00 : 00	<input type="checkbox"/>
5.	00 : 00 : 00 : 00 : 00 : 00	<input type="checkbox"/>
6.	00 : 00 : 00 : 00 : 00 : 00	<input type="checkbox"/>
7.	00 : 00 : 00 : 00 : 00 : 00	<input type="checkbox"/>
8.	00 : 00 : 00 : 00 : 00 : 00	<input type="checkbox"/>
9.	00 : 00 : 00 : 00 : 00 : 00	<input type="checkbox"/>
10.	00 : 00 : 00 : 00 : 00 : 00	<input type="checkbox"/>

View Additional Rules: 1 to 10

Label	Description
<b>Index</b>	Assigns an index number to the rule.
<b>MAC Address</b>	Defines the MAC address to block.
<b>Clear</b>	Deletes the filtering rule when the Apply button is clicked and the Clear box is checked.
<b>View Additional Rules:</b>	Displays rules 11-20 when selected from the drop-down list, if they exist. A total of twenty rules are supported.
<b>Apply</b>	Saves all screen changes when clicked.

## 5.8 Using the Advanced Gateway Setup IP Filtering Option

The **IP Filtering** option allows you 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.

### 5.8.1 Using IP Filtering Best Practices

The following are best practices to set up IP filtering.

1. Make sure a PC is connected to the cable modem and both devices are powered on and functioning.
2. Log in to the cable modem Web user interface. Refer to [Accessing the Web Interface on page 17](#).
3. Go to **Tools>>Client List**. Your PC and other devices are listed. Note the MAC address and IP address of the devices to which you want to deny Internet access. For more information, refer to [Using the Client List Option on page 83](#).
4. Go to **Gateway>>Static Lease**. Enter the MAC address and IP address of devices to

which you want to deny Internet access. Click **Apply**. For more information, refer to [Using the DHCP Static Lease Option on page 39](#). A static lease ensures that the device always gets the same IP address. That way, if filtered, it gets filtered continuously. Otherwise, the IP address would change for the device and the filtering rule would not work.



### Note

You may also filter by the MAC address which does not require setting a static lease. Refer to [Using the Advanced Gateway Setup MAC Filtering Option on page 44](#).



### Steps

#### To filter IP addresses:

1. Click the **Gateway** link from the top of the screen.
2. Click **IP Filtering** from the left side of the screen. The **IP Filtering** fields are explained following this screen example.

Start Address	End Address	Enabled
192.168.0.4	192.168.0.4	<input checked="" type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>

Apply

Label	Description
<b>Start Address</b>	Defines the starting IP address to filter.
<b>End Address</b>	Defines the ending IP address to filter.
<b>Enabled</b>	Activates the rule when enabled is checked.
<b>Apply</b>	Saves all screen changes when clicked.

## 5.9 Using the Advanced Gateway Setup Port Filtering Option

The **Port Filtering** option allows you to configure port filters to block to all devices on the LAN Internet services that use specific ports.

For example, to prevent all Telnet access into and across your LAN, you would enter the **Start** and **End** ports to be 23, select Both for **Protocol**, and click the **Enabled** selection box.

Be careful using port filtering by port range as you may accidentally prevent traffic that should pass through your network (for example, http or email). To see what applications use each port, refer to [Using the Advanced Gateway Setup Forwarding Option on page 47](#) and click the **Port Map** button.



## Steps

### To configure port filters:

1. Click the **Gateway** link from the top of the screen.
2. Click **Port Filtering** from the left side of the screen. The **Port Filtering** fields are explained following this screen example.

The screenshot shows the 'Advanced Gateway - Port Filtering' configuration page. On the left is a sidebar with a tree view containing 'Basic Gateway Setup' (Information, Setup, DHCP, Static Lease, Time) and 'Advanced Gateway Setup' (Options, MAC Filtering, IP Filtering, Port Filtering, Forwarding, Port Triggering, Pass Through, DMZ Host). 'Port Filtering' is selected and highlighted with a red box. The main area contains a table titled 'Port Filtering' with the following structure:

Start Port	End Port	Protocol	Enabled
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>

An 'Apply' button is located at the bottom of the table.

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

## 5.10 Using the Advanced Gateway Setup Forwarding Option

Port forwarding settings may be needed to resolve issues when data is sent from a local host to the Internet, but the return path of expected data is not received by your local host. Or, you have an application or service running on your local network (on local host)

that cannot be accessed from the Internet directly (for example, a request to a local audio server). Port forwarding tells the cable modem to which computer on the local area network to send the data. Here are some examples:

- ☐ **Xbox/PlayStation** – Games/applications may require port forwarding.
- ☐ **Home Security Systems** – Security systems that use the Internet may require port forwarding.
- ☐ **Audio Servers/VoIP** – Audio and VoIP applications and services may require port forwarding to be fully enabled.



#### Note

If your host systems/applications do **not** have communications issues with the Internet, forwarding is **not** needed.

You need two major items of information to setup forwarding:

- ☐ The **IP address** of each local host system (for example, Xbox) for which you need to setup a port forwarding rule. See the discussion below for how to obtain IP addresses.
- ☐ The **port numbers** that a 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. You may also refer to <http://portforward.com> for more information.

The following tasks are recommended as best practices for setting up forwarding rules:

- a. Enable UPnP (Universal Plug and Play). This may resolve the issue you have without the need to set forwarding rules.
  - i. Access the Web interface of the cable modem, see [Accessing the Web Interface on page 17](#).
  - ii. Select **Gateway** from the top menu, then **Options** from the left menu.
  - iii. Select the option to enable UPnP.
  - iv. Test your local host/application (for example, Xbox) to determine correct functionality. If it is still not properly communicating, continue with forwarding.
- ☐ [Using the Client List Option on page 83](#) – Use this option to obtain the MAC and IP address of the internal host for which you are setting up a forwarding rule. You also need these for the following task.
- ☐ [Using the DHCP Static Lease Option on page 39](#) – Before setting up forwarding, we recommend that you 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, you should assign a static IP lease to that system to keep the IP from renewing and disrupting the forwarding rule.

### 5.10.1 Setting Up Port Forwarding for an Xbox Example:

To setup Port Forwarding, use the following procedure. See the following page for screen field definitions.



#### Steps

##### To set up port forwarding for an Xbox:

1. Click the **Gateway** link from the top of the screen.
2. Click **Forwarding** from the left side of the screen.

The following example shows how to setup a single Xbox running Modern Warfare 2. Since multiple ports are used for the Xbox and the Modern Warfare 2 game, a separate forwarding rule is set up for each port. (Multiple ports and forwarding rules may not be required for other applications.) Note the following:

- ◆ Enter the Xbox IP address in the Local IP field. Notice how the same IP is entered in 4 rows, one row for each port used by the Xbox.
- ◆ Define ports used by the Xbox in the Internal Port field. Define the same ports used by the Xbox in the External Port Start and End fields.
- ◆ You can set up applications/services to listen on one internal port. External Internet users who want to access that application, address it using an external port, such as an Audio server. In the screen example below, Internal Ports are the ports to which local servers listen. External Ports are the ports that the cable modem listens to from the WAN.
- ◆ Create Port Forwarding rules per port. Therefore, a rule set up for port 53 only works for port 53. A port can be used only by one program at a time.
- ◆ 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.

MODEM | GATEWAY | WIRELESS | FIREWALL | PARENTAL CONTROL | TOOLS | LOGOUT

**Basic Gateway Setup**

- Information
- Setup
- DHCP
- Static Lease
- Time

**Advanced Gateway Setup**

- Options
- MAC Filtering
- IP Filtering
- Port Filtering
- **Forwarding**
- Port Triggering
- Pass Through
- DMZ Host

### Advanced Gateway - Forwarding

Index	Internal			External			Protocol	Enabled
	Local IP	Start Port	End Port	Public Interface IP	Start Port	End Port		
1.	192.168.0.0	53	53	0.0.0.0	53	53	Both	<input checked="" type="checkbox"/>
2.	192.168.0.0	80	80	0.0.0.0	80	80	Both	<input checked="" type="checkbox"/>
3.	192.168.0.0	88	88	0.0.0.0	88	88	Both	<input checked="" type="checkbox"/>
4.	192.168.0.0	3074	3074	0.0.0.0	3074	3074	Both	<input checked="" type="checkbox"/>
5.	192.168.0.0	0	0	0.0.0.0	0	0	Both	<input type="checkbox"/>
6.	192.168.0.0	0	0	0.0.0.0	0	0	Both	<input type="checkbox"/>
7.	192.168.0.0	0	0	0.0.0.0	0	0	Both	<input type="checkbox"/>
8.	192.168.0.0	0	0	0.0.0.0	0	0	Both	<input type="checkbox"/>
9.	192.168.0.0	0	0	0.0.0.0	0	0	Both	<input type="checkbox"/>
10.	192.168.0.0	0	0	0.0.0.0	0	0	Both	<input type="checkbox"/>

View Additional Rules: 1 to 10

Apply Port Map

Label	Description
<b>Internal</b>	
<b>Index</b>	Displays the Index number of the rule.
<b>Local IP</b>	Defines the last digits of the IP address of the local LAN device to which the forwarding rule applies,. For example, an Xbox or PC.
<b>Start Port</b>	Defines the starting port number listened to by the server host located in your LAN.
<b>End Port</b>	Defines the ending port number listened to by the server host located in your LAN.
<b>External</b>	
<b>Public Interface IP</b>	Designates another router on the network through which to forward data. Normally, this field is not modified.
<b>Start Port</b>	Defines the port number to start the range of ports to publish to the Internet.
<b>End Port</b>	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.
<b>Protocol</b>	Selects the protocol type. Options are UDP, TCPIP, or Both.

<b>Enabled</b>	Enables this rule when checked.
<b>View Additional Rules</b>	Displays rules 11-20 when selected from the drop-down list, if they exist. A total of twenty rules are supported.
<b>Apply</b>	Saves all screen changes when clicked.
<b>Port Map</b>	Shows a list of common applications and their ports.

### 5.10.2 Viewing Port Maps

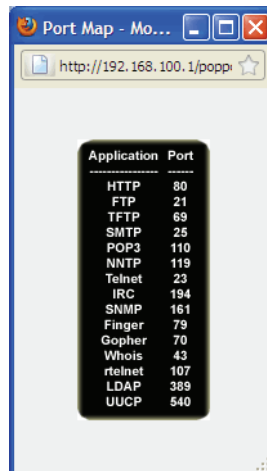
Port maps display a list of common applications and the port to which they are assigned. This option is available from the Forwarding screen.




#### Steps

To view assigned port maps:

1. On the Advanced Gateway - Forwarding screen, click **Port Map** at the bottom of the screen.
2. View the application names and pre-assigned port numbers.



3. Click  to close the Port Map window.

## 5.11 Using the Advanced Gateway Setup Port Triggering Option

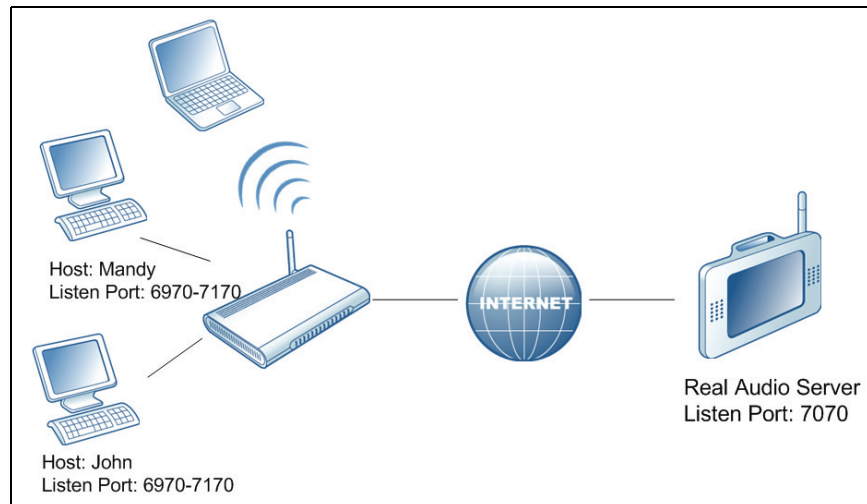
The **Port Triggering** option allows you to configure dynamic triggers to specific devices on the LAN. This allows for special applications that require specific port numbers with bi-directional traffic to function properly. Applications such as video conferencing, voice, gaming, and some messaging 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. With regular port forwarding, you set a forwarding rule to send a service to the IP address of a LAN side host. The problem is that port forwarding sends a service to a **single** LAN IP address.

With port triggering, we define two kinds of ports: Trigger Port and Target Port. Trigger port is the service request with a specific destination port number sent from a LAN side host. Target Port is the port this specific application requires a LAN host to listen to. Thus, the server returns responses to these ports.

For example:

1. John requests a file from the Real Audio server (port 7070). Port 7070 is a “trigger” port and causes the device to record John’s computer IP address. The DVW3201B associates John’s computer IP address with the “target” port range of 6970-7170.
2. The Real Audio server responds to a port number ranging between 6970-7170.
3. The DVW3201B forwards the traffic to John’s computer IP address.
4. Only John can connect to the Real Audio server until the connection is closed or times out.



## Steps

### To set up port triggering:

1. Click the **Gateway** link from the top of the screen.
2. Click **Port Triggering** from the left side of the screen. The **Port Triggering** fields are explained following this screen example.

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



The screenshot shows the 'Advanced Gateway - Port Triggering' configuration page. The left sidebar lists various settings, with 'Port Triggering' highlighted in red. The main area contains a table for configuring port triggering rules.

Port Triggering					
Trigger Range		Target Range		Protocol	Enable
Start Port	End Port	Start Port	End Port		
53	53	53	53	Both	<input checked="" type="checkbox"/>
80	80	80	80	UDP	<input checked="" type="checkbox"/>
88	88	88	88	TCP	<input checked="" type="checkbox"/>
3074	3074	3074	3074	Both	<input checked="" type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>

Apply

Label	Description
<b>Trigger Range</b>	Defines the trigger port or a range of ports that trigger the router to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
<b>Start Port</b>	Defines a port number or the starting port number in a range of port numbers.
<b>End Port</b>	Defines a port number or the ending port number in a range of port numbers.
<b>Target Range</b>	Defines a target range port or a range of ports a server on the WAN uses when it responds to service requests. The router forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
<b>Start Port</b>	Defines a port number or the starting port number in a range of port numbers.
<b>End Port</b>	Defines a port number or the ending port number in a range of port numbers.
<b>Protocol</b>	Defines the protocol type for this rule, UDP, TCP, or Both.
<b>Enable</b>	Activates this rule when checked.
<b>Apply</b>	Saves all screen changes when clicked.

## 5.12 Using the Advanced Gateway Settings Pass Through Option

The **Pass Through** option allows you to configure a pass through table. Devices in the pass through table are treated as bridge devices that store and forward data between LAN interconnections.



## Steps

### To set up a pass through table:

1. Click the **Gateway** link from the top of the screen.
2. Click **Pass Through** from the left side of the screen. The **Pass Through** fields are explained following this screen example.

Index	MAC Address	Clear
1.	00 : 25 : c1 : d2 : c4 : e3	<input type="checkbox"/>
2.	00 : 25 : b2 : e3 : c6 : 10	<input type="checkbox"/>
3.	00 : 00 : 00 : 00 : 00 : 00	<input type="checkbox"/>
4.	00 : 00 : 00 : 00 : 00 : 00	<input type="checkbox"/>
5.	00 : 00 : 00 : 00 : 00 : 00	<input type="checkbox"/>
6.	00 : 00 : 00 : 00 : 00 : 00	<input type="checkbox"/>
7.	00 : 00 : 00 : 00 : 00 : 00	<input type="checkbox"/>
8.	00 : 00 : 00 : 00 : 00 : 00	<input type="checkbox"/>

Apply

Label	Description
<b>Index</b>	Defines the index number of the pass through rule.
<b>MAC Address</b>	Defines the input host's MAC address.
<b>Clear</b>	Deletes this rule when checked and the Apply button is clicked.
<b>Apply</b>	Saves all screen changes when clicked.

## 5.13 Using the Advanced Gateway Settings DMZ Host Option

The **DMZ Host** option allows you to configure a host IP address to be exposed (visible) to the WAN (public Internet). This may be used when applications do not work with port triggers or other networking strategies.

### 5.13.1 Using DMZ Host Best Practices

The following instructions are best practices when adding a device into a DMZ.

1. Connect a PC to an Ethernet port on the DVW3201B. 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 DVW3201B.
3. Log in to the DVW3201B Web user interface.

4. Go to **Tools>>Client List**. Your PC and other devices are listed. Note the MAC address and IP address of the Home Gateway, VoIP Phone, or other device to put in the DMZ. For more information, refer to [Using the Client List Option on page 83](#).
5. Go to **Gateway>>Static Lease**. Enter the MAC address and IP address of a Home Gateway (or other device you wish to be in the DMZ).
6. Click **Apply**. For more information, refer to [Using the DHCP Static Lease Option on page 39](#). A static lease ensures that the device is assigned the same IP address so it is always available on the network, especially if devices are powered on/off or disconnected and reconnected.
7. Go to **Gateway > Advanced > DMZ Host**. Enter the IP address you just configured in the Static Lease section.
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).



## Steps

### To expose an IP address to the WAN:

1. Click the **Gateway** link from the top of the screen.
2. Click **DMZ Host** from the left side of the screen. The **DMZ Host** fields are explained following this screen example.

**Note:** The following example shows the DMZ Host set up for a dual Xbox configuration.

Label	Description
<b>DMZ Address</b>	Defines the IP address of the host to be exposed.
<b>Apply</b>	Saves all screen changes when clicked.



## 6 Understanding the Wireless Menu

This Wireless menu provides settings to configure a wireless network.



### Topics

See the following topics:

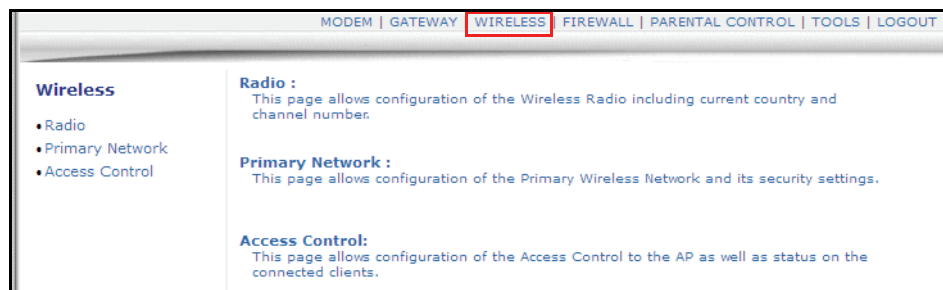
- ◆ [Using the Wireless Radio Option on page 57](#)
- ◆ [Using the Primary Network Option on page 61](#)
- ◆ [Using the Access Control Option on page 65](#)



### Steps

To access the wireless menu:

1. Access the Web interface. Refer to [Accessing the Web Interface on page 17](#).
2. Click the **Wireless** link from the top of the screen.



### 6.1 Using the Wireless Radio Option

The **Radio** option is used to configure the wireless radio, including the current country, channel number, and bandwidth control.



### Steps

To configure wireless operations:

1. Click the **Wireless** link at the top of the screen.
2. Click **Radio** from the left side of the screen. The **Radio** fields are explained following this screen example.

Label	Description
<b>Wireless Interfaces</b>	Displays the wireless name and MAC address.
<b>Wireless</b>	Displays the wireless radio's status, Enabled or Disabled.
<b>Country</b>	Defines the country where this device is used.
<b>Output Power</b>	Sets the percent of the Output Power for the radio.
<b>802.11 Band</b>	Defines the radio band as 2.4Ghz or 5 Ghz. <b>Note:</b> The distance coverage for 5Ghz is less than 2.4Ghz.
<b>802.11 n-Mode</b>	Sets the wireless networking standard. Select Auto to use 802.11 n mode when possible. This mode has a significant increase in the maximum raw OSI physical layer data rate from 54 Mbit/s to a maximum of 600 Mbit/s with the use of four spatial streams when at a channel width of 40 MHz.
<b>802.11 N Support Required</b>	Defines whether 802.11n support is required (on) or not (off). On forces the gateway to 802.11n mode and clients must support 802.11n.
<b>Bandwidth</b>	Sets the bandwidth to 20Mhz or 40Mhz. For 40 Mhz, set the sideband to lower or upper 20Mhz. 40 MHz channels double the channel width. This allows doubling the PHY data rate over a single 20 MHz channel.
<b>Sideband for Control Channel (40 Mhz only)</b>	Sets the sideband control to the lower or upper 20 MHz when the bandwidth is set to 40Mhz.
<b>Control Channel</b>	Selects a specific channel 1-11 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. For more information, refer to <a href="#">Selecting a Wireless Channel on page 70</a>

Label	Description
<b>Regulatory Mode</b>	Defines whether Regulatory Mode is set to off, 802.11d, or 802.11h.
<b>Pre-Network Radar Check</b>	Defines the number of seconds to check for radar on a channel before establishing a network. Current specs specify 60 seconds. Range 0-99. Zero disables checking. Designed so APs avoid channels that contain radar systems. Used for 802.11h only.
<b>In-Network Radar Check</b>	Defines the number of seconds to check for radar when switching to a new channel after a network has been established. Current specs specify 60 seconds. Range: 10-99. Cannot be disabled. Designed so APs avoid channels that contain radar systems. Used for 802.11h only.
<b>TPC Mitigation (dB)</b>	Defines the transmitter power control (TPC) mitigation setting as 0 (off), 2,3, or 4.
<b>OBSS Coexistence</b>	Enables or disables overlapping BSS coexistence.
<b>STBC Tx</b>	Sets the space-time block codes (STBCs) for the transmitting antenna.
<b>Apply</b>	Saves all screen changes when clicked.
<b>Restore Wireless Defaults</b>	Restores the factory default settings for wireless configurations when clicked.
<b>Scan Wireless APs</b>	Scans for other wireless access points and displays channel, encryption, SSID, RSSI levels, and other information.

### 6.1.1 Scanning for Wireless Access Points (APs)


You can search for wireless access points and display the results in a new window.



#### Steps

##### To search for wireless access points:

1. Click **Scan Wireless APs** at the bottom of the Wireless Radio screen. Results are displayed in a new window.



Nearby Wireless Access Points						
Network Name	Security Mode	Mode	PHY Mode	RSSI	Channel	BSSID
DVW3201B7B	WPA-PSK AES-CCMP TKIP	Managed	802.11n	-76 dBm	1	5c:ac:4c:23:d6:5c
UbeeDemo	WPA-PSK AES-CCMP TKIP	Managed	802.11n	-67 dBm	1	e0:91:53:59:2e:86
	WPA-PSK TKIP	Managed	802.11b/g	-57 dBm	1	5c:ac:4c:23:de:c8
DVW3201BE3	WPA-PSK AES-CCMP	Managed	802.11n	-57 dBm	11	18:f4:6a:b6:e9:97
Ubee	WPA-PSK TKIP	Managed	802.11n	-65 dBm	1	00:26:82:49:55:98
	WPA AES-CCMP	Managed	802.11n	-70 dBm	1	08:17:35:82:10:80
DVW3201B6B	WPA-PSK AES-CCMP	Managed	802.11n	-19 dBm	6	5c:ac:4c:a5:54:d6
71BE	NONE	Managed	802.11n	-48 dBm	11	c0:18:85:48:ab:30
cd78	WEP	Managed	802.11b/g	-81 dBm	1	00:22:69:0b:be:9a
093b	WEP	Managed	802.11n	-81 dBm	1	c0:f8:da:5d:9f:f2
DVW3201BE7	WPA-PSK AES-CCMP TKIP	Managed	802.11n	-78 dBm	1	5c:ac:4c:a5:55:73
UBEECHARTER	WPA-PSK AES-CCMP	Managed	802.11n	-84 dBm	1	90:4c:e5:6b:d4:64
ots-guest	WPA-PSK AES-CCMP	Managed	802.11b/g	-77 dBm	1	40:f4:ec:7e:ad:f2
HDMSDEMO	WPA-PSK TKIP AES-CCMP	Managed	802.11n	-59 dBm	6	00:26:82:22:1a:80
DVW3201B4C	WPA-PSK AES-CCMP	Managed	802.11n	-58 dBm	11	38:59:f9:ac:7c:39

2. Click **Refresh** to update the results.

Label	Description
<b>Network Name</b>	Displays the name of the wireless network (SSID) broadcast by the access point.
<b>Security Mode</b>	Displays the encryption method used.
<b>Mode</b>	<p>Displays the mode of the wireless access point: Possible modes are:</p> <ul style="list-style-type: none"> <li>♦ Master – Communicates with associated wireless cards that are in managed mode. Appears as a normal access point with an SSID and channel. Network communications, such as authentication, conflict, and duplicate packets are managed by the wireless card.</li> <li>♦ Managed – Communicates with an associated master, not directly with another managed AP. Wireless cards connect to the master network and change their channel to match. The master must accept the credentials of the managed network for it to be associated.</li> <li>♦ Ad-hoc – Communicates directly with another wireless network. Network cards must be in range and use the same name and channel.</li> <li>♦ Monitor – Communicates in observation mode and does not transmit. Can be used for troubleshooting wireless links or checking bandwidth usage in the area.</li> </ul>
<b>PHY Mode</b>	Displays the physical transceivers (PHY) layer method used.
<b>RSSI</b>	Displays the received signal strength (RSSI) of the wireless access points in range of the device. Lower negative numbers (for example, -1 to -65) indicate the access point is closer. Greater negative numbers (for example, -66 to -95) indicate the access point is farther away.
<b>Channel</b>	Displays the channel on which the wireless cable modem is operating.
<b>BSSID</b>	Displays the MAC address for the nearby wireless access points.



## 6.2 Using the Primary Network Option

The **Primary Network** option allows you to configure a variety of wireless security settings.



### Steps

To configure wireless security options:

1. Click the **Wireless** link from the top of the screen.
2. Click **Primary Network** from the left side of the screen. The **Primary Network** fields are explained following this screen example. **Note:** Wireless default values are discussed in [Understanding Default Values and Logins on page 8](#).

The screenshot displays the configuration page for the Ubee DVW3201BE3, specifically the **Wireless Primary Network** section. The interface includes a top navigation bar with links: MODEM, GATEWAY, WIRELESS, FIREWALL, PARENTAL CONTROL, TOOLS, and LOGOUT. On the left, a sidebar shows the **Wireless** menu with options: Radio, Primary Network (highlighted with a red box), and Access Control. The main content area is titled **Wireless Primary Network** and shows the MAC address DVW3201BE3 (18:F4:6A:B6:E9:97). The configuration is divided into several sections: **Primary Network** (with dropdowns for Primary Network, Network Name (SSID), Closed Network, AP Isolate, WPA, WPA-PSK, WPA2, WPA2-PSK, WPA/WPA2 Encryption, WPA Pre-Shared Key, RADIUS Server, RADIUS Port, RADIUS Key, Group Key Rotation Interval, WPA/WPA2 Re-auth Interval, WEP Encryption, Shared Key Authentication, 802.1x Authentication, Network Key 1-4, Current Network Key, and PassPhrase), **Automatic Security Configuration** (with WPS, WPS Config State, Device Name, and WPS Setup AP details), and **WPS Add Client** (with Add a client, Client PIN, and Authorized Client MAC fields). An **Apply** button is at the bottom.

Label	Description
<b>Primary Network</b>	Enables or disables the primary network.
<b>Network Name</b>	Allows you to define the unique SSID of the cable modem or accept the default. Refer to <a href="#">Understanding Default Values and Logins on page 8</a> for more information on the SSID.
<b>Closed Network</b>	Hides the selected SSID when enabled so it is not visible to wireless clients unless manually set up on the client. If disabled, the SSID is visible. Refer to <a href="#">Enabling a Closed Network on page 64</a> to set up a closed network.
<b>AP Isolate</b>	Prevents wireless client stations from communicating with each other when enabled.
<b>WPA</b>	Enables or disables the Wi-Fi Protected Access (WPA) security protocol. WPA is a subset of the IEEE 802.11i standard. Key differences between WPA and WEP are user authentication and improved data encryption. Setting WPA alone with a pre-shared key requires a RADIUS or TACACS server for authentication. This method is mostly used in large enterprise implementations.
<b>WPA-PSK</b>	Enables or disables WPA Pre-Shared Key (WPA-PSK). If you do not have an external RADIUS server, use WPA-PSK, which requires a single (identical) password entered into wireless gateway and wireless client. As long as the passwords match, a client is granted access to the wireless LAN. This is the default residential subscriber setting and uses TKIP encryption.
<b>WPA2</b>	Enables or disables WPA2. This advanced protocol is certified through Wi-Fi Alliance's WPA2 program and implements the mandatory elements of 802.11i. In particular, it has an AES-based algorithm (CCMP) that is considered fully secure. Setting WPA2 alone with a pre-shared key requires a RADIUS or TACACS server for authentication. This method is mostly used in large enterprise implementations.
<b>WPA2-PSK</b>	Enables or disables WPA2-PSK. If you do not have an external RADIUS server, use WPA2-PSK, which requires a single (identical) password entered into wireless gateway and wireless client. As long as the passwords match, a client is granted access to the wireless LAN. This is the recommended residential subscriber option. It is more secure than WPA-PSK and uses AES encryption.
<b>WPA/WPA2 Encryption</b>	Sets WPA/WPA2 encryption to AES or TKIP+AES. The default is AES.
<b>WPA Pre-Shared Key</b>	Displays (checked) or hides (unchecked) the WPA key. The encryption mechanisms for WPA and WPA-PSK are the same, except that WPA-PSK uses a simple common password instead of user-specific credentials. Refer to <a href="#">Understanding LED Operations on page 8</a> for the default value of the shared key.
<b>RADIUS Server</b>	Defines the IP address of the RADIUS server, if used.

Label	Description
<b>RADIUS Port</b>	Defines a RADIUS port number when WPA or 802.1x network authentication is selected.
<b>RADIUS Key</b>	Defines the RADIUS Key when WPA or 802.1x network authentication is selected.
<b>Group Key Rotation Interval</b>	Allows the device to generate the best possible random group key and update all the key-management capable stations periodically.
<b>WPA/WPA2 Re-auth Interval</b>	Sends a new group key to all clients at the specified interval for a wireless router (if using WPA-PSK key management) or RADIUS server (if using WPA key management). The re-keying process is the WPA equivalent of automatically changing the WEP key for a wireless access point and all stations in the WLAN on a periodic basis. Setting the WPA Group Key Update Timer is also supported in WPA-PSK mode.
<b>WEP Encryption</b>	Enables or disables WEP encryption. If you do not have wireless clients that can use WPA or WPA2, you can use WEP key encrypting. A higher bit key offers better security. WEP encryption scrambles the data transmitted between the wireless stations and the DVW3201B to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the DVW3201B must use the same WEP key. Data Encryption can be set to <b>WEP 128-bit</b> , <b>64-bit</b> , or <b>Disable</b> .
<b>Shared Key Authentication</b>	Defines Shared Key Authentication as optional or required. Shared Key is an authentication method used by wireless LANs, which follow the IEEE 802.11 standard. Wireless devices authenticate each other by using a secret key that is kept by both devices.
<b>802.1x Authentication</b>	Enables or disables 802.1x to authenticate wireless clients.
<b>Network Key 1-4</b>	Pre-defines up to 4 keys for 64-bit or 128-bit (64-bit keys require 10 hexadecimal digits) (128-bit key require 26 hexadecimal digits).
<b>Current Network Key</b>	Selects one of the four pre-defined keys as the current network key.
<b>Passphrase</b>	Sets the WEP encryption key by entering a word or group of printable characters in the Passphrase box and clicking Generate WEP keys. These characters are case sensitive.
<b>Generate WEP Keys</b>	Forces the device to generate 4 WEP keys automatically.
<b>Automatic Security Configuration</b> — Sets up WPS (Wi-Fi Protected Setup) for devices connecting to the wireless network.	
<b>WPS/Disabled</b>	Enables or disables WPS option. When enabled, the following additional fields are available:
<b>WPS Config State</b>	Defines if the WPS has been configured or not.
<b>Device Name</b>	Defines a name for this wireless cable modem for WPS.

Label	Description
<b>WPS Setup AP</b>	
<b>UUID</b>	Defines the universal unique identifier (UUID) for this access point.
<b>PIN</b>	Defines the Personal Identification Number for this access point.
<b>WPS Add Client</b>	
<b>Add a client</b>	Activates wireless protected setup (WPS) security on the device. To add a client: 1. Click Add a client. The WPS Add Client screen is displayed. 2. Click PUSH on the WPS Add Client screen. The WPS button is activated on the device, indicated by a flashing white light on top of the unit. 3. Press the WPS button on the device.
<b>Client PIN</b>	Defines a PIN number for client access.
<b>Authorized Client MAC</b>	Defines the MAC address of the authorized client.
<b>Apply</b>	Saves settings when clicked.

### 6.2.1 Enabling a Closed Network

You can enable the Closed Network option so the SSID cannot be broadcast or seen by others.



#### Steps

To enable a closed network:

1. Disable the WPS automatic security configuration.
2. Click **Apply**.
3. Access the pull down menu for the **Closed Network**.
4. Choose **Enabled** to enable a closed network.

**Wireless**

- Radio
- Primary Network
- Access Control
- Advanced
- Bridging
- Wifi Multimedia

**Wireless Primary Network**

DVW3201BE3 (18:F4:6A:B6:E9:97)

Primary Network: **Enabled** ▼

Network Name (SSID): DVW3201BE3

Closed Network: **Disabled** ▼

AP Isolate: **Enabled** ▼

WPA: **Disabled** ▼

WPA-PSK: **Disabled** ▼

WPA2: **Disabled** ▼

WPA2-PSK: **Enabled** ▼

Automatic Security Configuration: **Disabled** ▼

## 6.3 Using the Access Control Option

The **Access Control** option allows you to configure which clients can access your wireless network.



### Steps

#### To configure client access:

1. Click the **Wireless** link from the top of the screen.
2. Click **Access Control** from the left side of the screen. The **Access Control** fields are explained following this screen example.

The screenshot shows the web interface of the Ubee DVW3201B Advanced Wireless Voice Gateway. The top navigation bar includes links for MODEM, GATEWAY, WIRELESS, FIREWALL, PARENTAL CONTROL, TOOLS, and LOGOUT. The left sidebar shows a tree view under 'Wireless' with options for Radio, Primary Network, and Access Control (which is highlighted with a red box). The main content area is titled 'Wireless Access Control'. It features a 'Wireless Interface' dropdown menu set to 'DVW3201BE3 (18:F4:6A:B6:E9:97)'. Below this is a 'MAC Restrict Mode' dropdown menu set to 'Disabled'. There are eight input fields for 'MAC Addresses' arranged in two columns of four. An 'Apply' button is located below the input fields. At the bottom, there is a table titled 'Connected Clients' showing the status of connected devices.

MAC Address	Age(s)	RSSI(dBm)	IP Addr	Host Name	Mode	Speed (kbps)
00:27:10:8C:FE:F4	0	-41	192.168.0.4	your-s9279112e3	n	144445
00:21:00:83:99:47	9537	0			n	19500

Label	Description
Wireless Interface	Defines the network name for which you are setting access control parameters.
MAC Restrict Mode	<p>Controls wireless access to your network by MAC address.</p> <ul style="list-style-type: none"><li>♦ <b>Disabled</b> 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.</li><li>♦ <b>Allow</b> 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.</li><li>♦ <b>Deny</b> 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.</li></ul>

Label	Description
<b>MAC Addresses</b>	Defines the MAC addresses. Note: You may cut and paste MAC addresses from the connected clients list at the bottom of the screen.
<b>Apply</b>	Saves changes when clicked.
<b>Connected Clients</b>	<p>Lists wireless clients currently connected listed by MAC address.</p> <ul style="list-style-type: none"> <li>♦ <b>MAC Address</b> – Displays the MAC addresses entered in the MAC Addresses field (see above).</li> <li>♦ <b>Age(s)</b> – Displays the duration since the wireless client's polled values were sent to the device. The values include all information shown on this screen. The lower the number, the more current its data.</li> <li>♦ <b>RSSI(dBm)</b> – Displays the received signal strength from the device to the wireless cable modem. This value is commonly used to assist in troubleshooting wireless performance issues. A signal strength between 0dBm and -65dBm is considered optimal. Levels of -66dBm and lower (for example, -70, -80, etc.) have a downward impact on wireless data throughput. Refer to <a href="#">Deploying and Troubleshooting the Wireless Network on page 67</a> for more information.</li> <li>♦ <b>IP Address</b> – Displays the IP address assigned to this wireless client.</li> <li>♦ <b>Host Name</b> – Displays the host name of the wireless client.</li> <li>♦ <b>Mode</b> – Indicates the applicable 802.11a/b/g/n standard used by the connected client device.</li> <li>♦ <b>Speed (kbps)</b> – Displays the maximum theoretical link speed negotiated between the wireless gateway and the client, not including the overhead associated with encryption, and so on. For example, actual speeds with WEP encryption enabled are typically less than half of the negotiated link speed. TKIP encryption can also affect performance. AES is the most efficient and secure with the highest throughput possible. You can disable WMM if throughput on some client adaptors is adversely affected.</li> </ul>

## 6.4 Deploying and Troubleshooting the Wireless Network

This section provides the following information to help you understand, deploy, and troubleshoot your wireless environments:

- ❑ [Understanding Received Signal Strength on page 68](#)
- ❑ [Estimating Wireless Cable Modem to Wireless Client Distances on page 68](#)
- ❑ [Selecting a Wireless Channel on page 70](#)

## Understanding Received Signal Strength

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

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

To determine the received signal strength, refer to [Using the Access Control Option on page 65](#) and review the **RSSI** value. A receive signal strength indicator between 0 to -64 dBm is considered optimal. Levels of -67dBm and lower (for example, -70, -80, etc.) have a downward impact on wireless data throughput.

## 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.



### Steps

#### To determine wireless cable modem placement:

1. Connect a wireless client to the wireless cable modem. Refer to [Connecting Devices to the Network on page 12](#) if needed.
2. Place the wireless client at around one meter (three feet) away from the wireless cable modem.
3. Obtain the **RSSI** value for the connected client. Refer to [Using the Access Control Option on page 65](#). This value is used in the formula further below.
4. Use the following table to determine what materials the wireless signal must travel through to reach the desired wireless coverage distance.

**Attenuation Considerations at 2.4GHz**

Material	Attenuation
Connector/Cable	3.5dB
Free Space	.24dB / foot
Interior Drywall	3dB to 4dB
Cubicle Wall	2dB to 5dB
Wood Door (Hollow/Solid)	3dB to 4dB
Brick, Concrete Wall (Note 1)	6dB to 18db



Attenuation Considerations at 2.4GHz

Material	Attenuation
Glass Window (not tinted)	2dB to 3dB
Double Pane Coated Glass	13dB
Bullet Proof Glass	10dB
Steel / Fire Exit Door	13dB to 19dB
Human Body	3dB
Trees (Note 2)	.15dB / foot
<b>Note 1:</b> 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.	<b>Note 2:</b> The attenuation caused by trees varies significantly depending upon the shape and thickness of the foliage.

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

**Formula:**

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

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

**Example:**

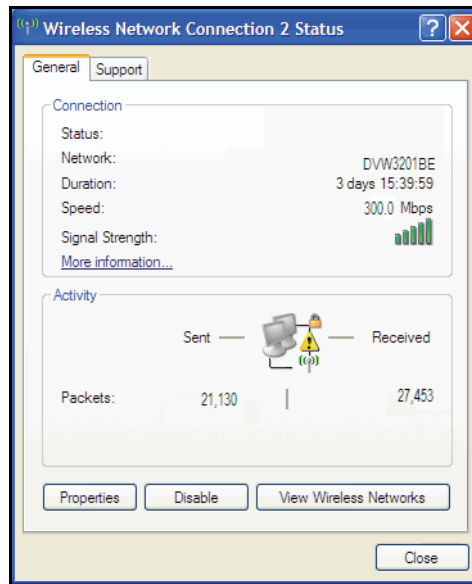
(-30dBm) - (-67dBm) = 37dBm (allowable free space loss for a 54Mbps connection)

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

6. Once you know the optimal feet distance between individual wireless clients and the wireless cable modem, you may resolve and prevent some performance issues.
7. To check the wireless signal strength and speed, use the following steps for a Windows computer connected wirelessly to the wireless cable modem. If the wireless computer is not connected, refer to [Connecting a Wireless Device on page 13](#).
- a. Double-click the Wireless networking icon in the system tray.



- b. Review the speed and signal strength in the Status window.



### Selecting a Wireless Channel

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

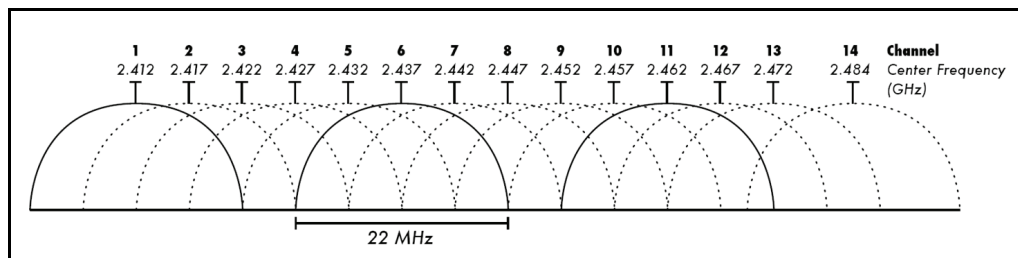
In some cases, you may want to segment your wireless traffic where a group of devices operates on one channel and another group operates on another channel, and so on. This is done by configuring the channel on each wireless access point individually (if you have multiples). If you have control over 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 Wireless Radio Option on page 57](#).

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

## 7 Understanding the Firewall Menu

This chapter provides instructions to configure the DVW3201B firewall to control what types of traffic are allowed on your network. The firewall can block certain Web-oriented cookies, java scripts, and pop-up windows. It is highly recommended the Firewall is left enabled at all times to protect against denial of service (DoS) attacks. Refer to [Using the Basic Option on page 77](#) to block Internet access to specific sites.

**Note:** Firewall menu options are not available when the device is in Bridge mode.



### Topics

See the following topics:

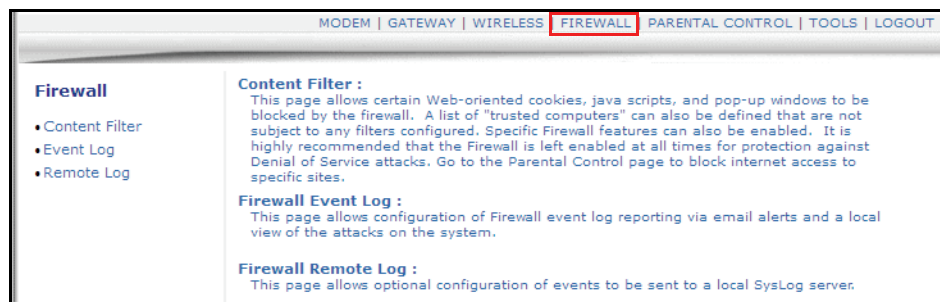
- ◆ [Using the Content Filter Option on page 71](#)
- ◆ [Using the Event Log Option on page 73](#)
- ◆ [Using the Remote Log Option on page 74](#)



### Steps

To access the firewall menu:

1. Access the Web interface. Refer to [Accessing the Web Interface on page 17](#).
2. Click the **Firewall** link from the top of the screen.



### 7.1 Using the Content Filter Option

The **Content Filter** option allows you to block certain Web-oriented cookies, java scripts, and pop-up windows.



### Steps

To filter Web content:

1. Click the **Firewall** link from the top of the screen.
2. Click **Content Filter** from the left side of the screen. The **Content Filter** fields are

explained following this screen example.

Firewall - Content Filter	
<b>Content Filter Settings</b>	
Filter Proxy	<input type="checkbox"/> Enable
Filter Cookies	<input type="checkbox"/> Enable
Filter Java Applets	<input type="checkbox"/> Enable
Filter ActiveX	<input type="checkbox"/> Enable
Filter Popup Windows	<input type="checkbox"/> Enable
<b>Firewall Settings</b>	
Block Fragmented IP Packets	<input type="checkbox"/> Enable
Port Scan Detection	<input checked="" type="checkbox"/> Enable
IP Flood Detection	<input type="checkbox"/> Enable
Firewall Protection	<input checked="" type="checkbox"/> Enable
Protection against incoming connection requests on routed subnet	<input type="checkbox"/> Enable
<input type="button" value="Apply"/>	

Label	Description
<b>Content Filter Settings</b>	
<b>Filter Proxy</b>	Acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN, it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
<b>Filter Cookies</b>	Stops Cookies from being stored on a connected computer's hard drive. Some Web servers use them to track usage and provide service based on an ID found in the Cookies.
<b>Filter Java Applets</b>	Stops Java applets from being launched on connected computers. Java is a programming language and development environment for building downloadable Web components or Internet and intranet business applications.
<b>Filter ActiveX</b>	Stops ActiveX applications from being launched on connected computers. ActiveX is a tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.
<b>Filter Popup Windows</b>	Stops popup windows when visiting some Websites.
<b>Firewall Settings</b>	
<b>Block Fragmented IP Packets</b>	Detects fragmented IP packets and blocks them.
<b>Port Scan Detection</b>	Detects port scan attacks.
<b>IP Flood Detection</b>	Detects IP flood attacks.

Label	Description
<b>Firewall Protection</b>	Activates the firewall function.
<b>Protection against incoming connection requests on routed subnet</b>	Protects all the routed subnets connected to the device.
<b>Apply</b>	Saves the configuration when clicked.

## 7.2 Using the Event Log Option

The **Event Log** option allows you to configure firewall event log reporting via email alerts and report on possible attacks on the system.



### Steps

To configure firewall event reporting:

1. Click the **Firewall** link from the top of the screen.
2. Click **Event Log** from the left side of the screen. The **Event Log** fields are explained following this screen example.

Label	Description
<b>Contact Email Address</b>	Defines the email address where you want to send the log.
<b>SMTP Server Name</b>	Defines the name of the SMTP server, such as smtp.example.com.
<b>SMTP Username</b>	Defines the username for the email address, such as contact@company.com.
<b>SMTP Password</b>	Defines the password for the email address.
<b>E-mail Alerts</b>	Enables or disables event log reporting.
<b>Apply</b>	Saves the settings and completes the setup.
<b>Email Log</b>	Sends the log to the specified email address.
<b>Clear Log</b>	Deletes the log.

## 7.3 Using the Remote Log Option

The **Remote Log** option allows you to configure events to be sent to a local SysLog server.



### Steps

#### To configure the firewall remote log:

1. Click the **Firewall** link from the top of the screen.
2. Click **Remote Log** from the left side of the screen. The **Remote Log** fields are explained following this screen example.

Label	Description
<b>Permitted Connections</b>	Logs all access attempts that are allowed by the firewall.
<b>Blocked Connections</b>	Logs all access attempts that are blocked by the firewall.
<b>Known Internet Attacks</b>	Logs all known attacks from the Internet.
<b>Product Configuration Events</b>	Logs when the DVW3201B is configured/modified by a user or administrator.
<b>SysLog server</b>	Defines the IP address of the Syslog server.
<b>Apply</b>	Saves the remote log configuration when clicked.

## 8 Understanding the Parental Control Menu

Parental Controls allow you to control Internet access for users on the DVW3201B network. Parental Controls provides the following features:

- ◆ Define user/password access.
- ◆ Block specific Web sites and Web sites based on keywords.
- ◆ Define the times users are allowed to access the Internet.
- ◆ View an event log to view Internet activity.



### Topics

See the following topics:

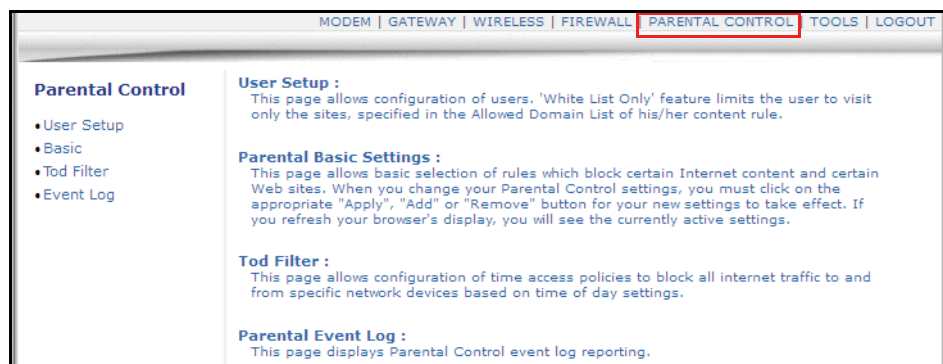
- ◆ [Using the Parental Control User Setup Option on page 75](#)
- ◆ [Using the Basic Option on page 77](#)
- ◆ [Using the Tod Filter Option on page 79](#)
- ◆ [Using the Event Log Option on page 80](#)



### Steps

To access the parental control menu:

1. Access the Web interface. Refer to [Accessing the Web Interface on page 17](#).
2. Click the **Parental Control** link from the top of the screen.



### 8.1 Using the Parental Control User Setup Option

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



## Steps

### To configure user accounts:

1. Click the **Parental Control** link from the top of the screen.
2. Click **User Setup** from the left side of the screen. The **User Setup** fields are explained following the screen example.

**Note:** To enable Parental Control, refer to [Using the Basic Option on page 77](#).

Label	Description
<b>Add User</b> <b>Remove User</b> <b>Enable</b>	Defines user accounts. <ul style="list-style-type: none"> <li>♦ To select an existing user, choose the user from the User Settings pop-up menu.</li> <li>♦ To add a new user, add the user name and click Add.</li> <li>♦ To activate the user, check Enable.</li> <li>♦ To remove a user, select the user from the pop-up menu and click Remove User.</li> </ul>
<b>Password</b>	Defines the password for this user. It is required when this user tries to access the Internet via the device.
<b>Re-Enter Password</b>	Checks the password with the re-entered password.
<b>Trusted User</b>	Defines the selected user as a trusted user when enabled is checked. The user is limited to timing and content when visiting the Internet, as defined in the following fields.
<b>Content Rule</b>	Selects from the pop-up menu an existing content rule that defines what kind of Websites the user can visit or not.



Label	Description
<b>White List Access Only</b>	Selects the White List Access option. If you have created a content rule that defines a black list and white list, select the White List Access Only checkbox to force the wireless modem to execute the policy for the selected user.
<b>Time Access Rule</b>	Selects a defined time access rule to apply to the selected user.
<b>Session Duration</b>	Allows you to enter a time in minutes for the user's session to expire. When the session expires, the user can log in again for the same session duration.
<b>Inactivity Time</b>	Allows you to enter the time out value when a user has no activity on the Internet. When the time expires, the user interface to the Internet is cancelled.
<b>Apply</b>	Saves all changes when clicked.
<b>Trusted Computers</b>	Defines the trusted hosts that can bypass the Parental Control Process.
<b>Add</b>	Adds the trusted host's MAC address entered in the given area and Add is clicked.
<b>Remove</b>	Removes a trusted computer from the list when it is highlighted and Remove is clicked.

## 8.2 Using the Basic Option

The **Basic** option allows you to select rules to block certain Internet content and Web sites. After you change your Parental Control settings, click the appropriate Apply, Add, or Remove button for your new settings to take effect. Refresh your browser's display to see the currently active settings.



### Steps

#### To filter Internet content and Web sites:

1. Click the **Parental Control** link from the top of the screen.
2. Click **Basic** from the left side of the screen. The **Basic** fields are explained following this screen example.

MODEM | GATEWAY | WIRELESS | FIREWALL | PARENTAL CONTROL | TOOLS | LOGOUT

**Parental Control**

- User Setup
- **Basic**
- Tod Filter
- Event Log

**Parental Control - Activation**

This box must be checked to turn on Parental Control ☐ Enable Parental Control

Apply

**Content Policy Configuration**

SmithFamily Add New Policy

**Content Policy List**

2. SmithFamily Remove Policy

**Keyword List**

anonymizer

Add Keyword Remove Keyword

**Blocked Domain List**

anonymizer.com

Add Domain Remove Domain

**Allowed Domain List**

ubee.com

Add Allowed Domain Remove Allowed Domain

Label	Description
<b>Enable Parental Control</b>	Activates the Parental Control feature when checked.
<b>Apply</b>	Saves all changes in the screen and activates Parental Control, if enabled.
<b>Content Policy Configuration</b>	
<b>Add New Policy</b>	Adds a policy to the Policy List. Enter the policy name and click Add New Policy.
<b>Content Policy List</b>	Lists existing policies you can choose to use.
<b>Remove Policy</b>	Deletes a policy from the list. Select the policy from the list and click Remove Policy.
<b>Keyword List</b>	Displays keywords you can use to block Web site addresses (URLs) containing those words.
<b>Add Keyword</b>	Adds a keyword to the keyword list. Enter the word in the field next to the Add Keyword button and click Add Keyword. The keyword is added to the list.
<b>Remove Keyword</b>	Removes a keyword from the keyword list. Select the keyword from the list, and click Remove Keyword.
<b>Blocked Domain List</b>	Displays Web domains (for example, unwanted.com) you can use to block access to those domains.
<b>Add Domain</b>	Adds a domain to the Allowed Domain List. Enter a domain, and click Add Domain.
<b>Remove Allowed Domain</b>	Removes a domain from the Allowed Domain List. Select the domain from the list, and click Remove Domain.

Label	Description
<b>Allowed Domain List</b>	Displays domains you can assign to users to visit only the sites allowed.
<b>Add Allowed Domain</b>	Adds allowed domains to the list. Enter the name and click Add Allowed Domain.
<b>Remove Allowed Domain</b>	Removes domain names from the list. Highlight the domain from the list and click Remove Allowed Domain.

## 8.3 Using the Tod Filter Option

The **Tod Filter** option allows the configuration of time-based access policies to block all Internet traffic at specified times.



### Steps

To configure time-of-day filters:

1. Click the **Parental Control** link from the top of the screen.
2. Click **Tod Filter** from the left side of the screen. The **Tod Filter** fields are explained following this screen example.

Label	Description
<b>Add New Policy</b>	Adds a new policy. Enter a policy name and click the Add New Policy button.
<b>Time Access Policy List</b>	Lists the existing policies in a drop-down list.
<b>Enabled</b>	Activates a policy. Select the policy from the drop-down list and check Enabled.
<b>Remove</b>	Deletes a policy. Select the policy from the drop-down list and click Remove.

Label	Description
<b>Days to Block</b>	Selects the days to block Internet access.
<b>Time to Block: All Day or by 24 hour clock time</b>	Defines the time to block. <ul style="list-style-type: none"> <li>♦ To block all day, check All Day to eliminate all access during the days selected.</li> <li>♦ To block a specific time, enter the time range in the fields provided in a 24 hour clock (00:00 - 24:00) format.</li> </ul>
<b>Apply</b>	Saves all changes when clicked.

## 8.4 Using the Event Log Option

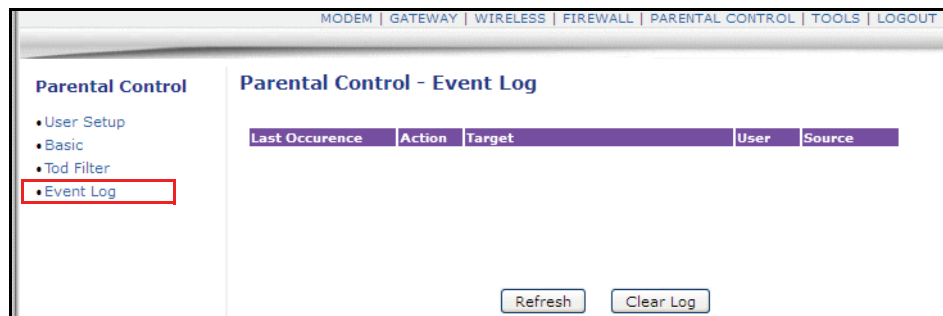
The **Event Log** option displays Parental Control event log reporting.



### Steps

To view the parental control event log:

1. Click the **Parental Control** link from the top of the screen.
2. Click **Event Log** from the left side of the screen. The **Event Log** fields are explained following this screen example.



Label	Description
<b>Last Occurrence</b>	Displays the time when the last event occurred.
<b>Action</b>	Displays what is done by parental control, including dropping or permitting access requests.
<b>Target</b>	Displays the destination IP address of a certain access request.
<b>User</b>	Displays the user who triggered this event log.
<b>Source</b>	Displays the source IP address of this event.
<b>Refresh/Clear Log</b>	Displays the event log. <ul style="list-style-type: none"> <li>♦ To update the log with the most current events, click Refresh.</li> <li>♦ To empty the displayed log entries, click Clear.</li> </ul>

## 9 Understanding the Tools Menu

This chapter instructs you how to use a variety of tools to evaluate and diagnose the DVW3201B.



### Topics

See the following topics:

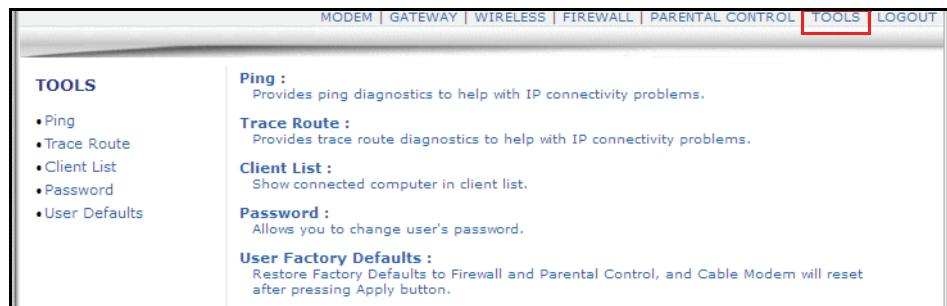
- ◆ [Using the Ping Option on page 81](#)
- ◆ [Using the Trace Route Option on page 82](#)
- ◆ [Using the Client List Option on page 83](#)
- ◆ [Using the Password Option on page 84](#)
- ◆ [Using the User Defaults Option on page 85](#)



### Steps

To access the tools menu:

1. Access the Web interface. Refer to [Using the Web User Interface on page 17](#).
2. Click the **Tools** link from the top of the screen.



### 9.1 Using the Ping Option

The **Ping** utility tests the 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.



### Steps

To test connectivity between devices:

1. Click the **Tools** link from the top of the screen.
2. Click **Ping** from the left side of the screen. The **Ping** fields are explained following this

screen example.

Label	Description
<b>Ping Test Parameters</b>	
<b>Ping Target</b>	Defines the IP address to which you want to send a ping.
<b>Ping Size</b>	Defines the packet size to send for the ping operation.
<b>No. of Pings</b>	Defines the number of ping commands to send to the ping target.
<b>Ping Interval</b>	Defines the interval between ping operations in milliseconds.
<b>Start Test/Abort Test/Clear Results</b>	Defines what you want to do. <ul style="list-style-type: none"> <li>♦ To start the test, click Start. Test</li> <li>♦ To cancel the test, click Abort Test.</li> <li>♦ To clear the displayed results, click Clear Results.</li> </ul>
<b>Results</b>	Displays the results of the ping test.
<b>Refresh</b>	Updates the results in the Results window. You must click the Refresh button to get the latest results.

## 9.2 Using the Trace Route Option

The Trace Route utility determines the IP addresses of the hosts on the path. By checking the Resolve host names box, Trace Route 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.



### Steps

**To trace host IP addresses along a route:**

1. Click the **Tools** link from the top of the screen.
2. Click **Trace Route** from the left side of the screen. The **Trace Route** fields are explained following this screen example.

MODEM | GATEWAY | WIRELESS | FIREWALL | PARENTAL CONTROL | TOOLS | LOGOUT

**TOOLS**

- Ping
- **Trace Route**
- Client List
- Password
- User Defaults

**Tools - Trace Route**

**Tracert Test Parameters**

Tracert Target :

MAX Hops :  Hops (1 ~ 50)

Time out :  ms (100 ~ 10000)

**Results**

Tracing route to [209.191.122.70]  
over a maximum of 30 hops:

1	10ms	10ms	10ms	10.2.0.1
2	690ms	*	40ms	209.191.122.70

Trace complete! ♦

To get an update of the results, you must select the REFRESH button above.

Label	Description
<b>Tracert Test Parameters</b>	
<b>Tracert Target</b>	Defines the specific IP address or domain (for example, yahoo.com) to which you want to trace a route.
<b>MAX Hops</b>	Defines the maximum number of hops. Hops are the number of routers that the trace route traverses.
<b>Time out</b>	Defines the time out interval (100–10000) in milliseconds.
<b>Start Test Abort Test Clear Results</b>	Defines what you want to do. <ul style="list-style-type: none"> <li>♦ To start the test, click Start Test.</li> <li>♦ To cancel the test, click Abort Test.</li> <li>♦ To clear the displayed results, click Clear Results.</li> </ul>
<b>Results</b>	Displays the results of the test. Once the traceroute is complete, an ordered list of hosts is displayed, the number of times the host answered, and how fast the host answered the probes.
<b>Refresh</b>	Updates the results in the Results window. You must click the Refresh button to get the latest results.

## 9.3 Using the Client List Option

The **Client List** option displays computers connected to the DVW3201B.



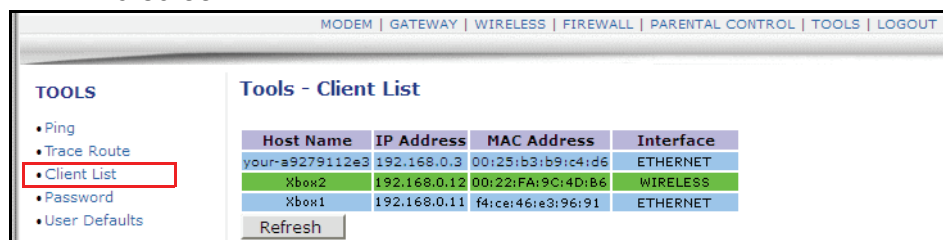
### Steps

**To view a list of computers connected to this device:**

1. Click the **Tools** link from the top of the screen.

- Click **Client List** from the left side of the screen. The **Client List** fields are explained following this screen example.

**Note** – Devices connected with an IPv6 IP address are shown in the Gateway–Setup–LAN IPv6 screen.



Label	Description
<b>Hostname</b>	Displays the hostname of the DHCP clients connected to the DVW3201B.
<b>IP Address</b>	Displays the IP address of the DHCP clients connected to the DVW3201B.
<b>MAC Address</b>	Displays the MAC address of the DHCP clients connected to the DVW3201B.
<b>Interface</b>	Displays the method of how clients are connected to the device (for example, ethernet LAN, Wireless).
<b>Refresh</b>	Refreshes the client list. This may be useful when testing network connectivity between connecting clients and the DVW3201B.

## 9.4 Using the Password Option

The **Password** option allows you to change the password for the **user** login on the DVW3201B. This login is used to access this web interface.



### Steps

**To change the password for the user login:**

- Click the **Tools** link from the top of the screen.
- Click **Password** from the left side of the screen. The **Password** fields are explained following this screen example.



Label	Description
<b>User Name</b>	Allows you to enter a new user name for the <b>user</b> account to this web interface of the DVW3201B. See <a href="#">Understanding Default Values and Logins on page 8</a> for more information on logins and defaults. Enter the new Password and re-enter the new password to confirm. Click Apply to save the changes.
<b>New Password</b>	Allows you to enter a new password for the user account.
<b>Confirm Password</b>	Allows you to re-enter the new password to confirm.
<b>Apply</b>	Saves all changes when clicked.

## 9.5 Using the User Defaults Option

The **User Defaults** option allows you to restore factory defaults to the Firewall and Parental Control settings. All other networking setting are not cleared and reset (for example, wireless settings).



### Note

Restoring factory defaults to the system resets the user login/password to the device. Refer to [Understanding Default Values and Logins on page 8](#) for the default values.

1. Click the **Tools** link from the top of the screen.
2. Click **User Defaults** from the left side of the screen. The **User Defaults** fields are explained following this screen example.

Label	Description
<b>Restore Factory Defaults to Firewall and Parental Control</b>	Restores settings to factory defaults. Select Yes to restore the device to default settings for the Firewall and Parental Control settings. This operation does not require a reset of the system.
<b>Reset The system</b>	Resets the system. Select Yes to power cycle the device.
<b>Apply</b>	Applies the options selected in this screen.

## 10 Glossary

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

### **Broadcast**

A packet sent to all devices on a network.

### **Cable Modem Termination System (CMTS)**

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 VoIP.

### **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.

### **Customer Premises Equipment (CPE)**

Equipment such as telephones, routers, and modems located at a subscribers location to enable customers 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.

### **Demilitarized Zone (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.

### **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.

### **Domain Name System (DNS)**

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.

**Dynamic Host Configuration Protocol (DHCP)**

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.

**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 and XNS.

**Firewall**

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

**Gateway**

A local device, usually a router, that connects hosts on a local network to other networks – sometimes with different incompatible communication protocols.

**Headend**

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

**Internet Protocol (IP)**

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.

**Internet Service Provider (ISP)**

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

### **Interval Usage Code (IUC)**

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.

### **Local Area Network (LAN)**

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.

### **Media Access Control (MAC) 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.

### **Megabits per Second (Mbps)**

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

### **Maximum Transmission Unit (MTU)**

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

### **Network Address Translation (NAT)**

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.

### **Network Basic Input Output System (NetBIOS)**

An application programming interface (API) that augments the DOS BIOS by adding special functions for LANs. Almost all Windows-based LANs for PCs are based on the NetBIOS.

### **Network Operations Center (NOC)**

A location that controls computer, television, or telecommunications networks. Large organizations usually have more than one network operations center to manage multiple networks.

### **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.

### **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.

### **Routing Information Protocol (RIP)**

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

**Router**

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

**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.

**Terminal Access Controller Access-Control System (TACACS)**

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

**Time Division Multiple Access (TDMA)**

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

**Transmission Control Protocol (TCP)**

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.

**Transmission Control Protocol/Internet Protocol (TCP/IP)**

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.

**Trivial File Transfer Protocol**

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

**Uniform Resource Identifier (URI)**

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

**Upstream**

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

**Uniform Resource Locator (URL)**

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

**Wide Area Network (WAN)**

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.

**Wi-Fi Protected Setup (WPS)**

A security protocol for wireless home networks. Created by the Wi-Fi Alliance, this protocol allows home users to easily set up wireless security and add new devices without needing to enter long passwords.

**Wireless Local Area Network (WLAN)**

A method that links two or more devices to provide a connection through an access point the wider Internet. Users can move within the local coverage area and stay connect to the network.

**Xerox Network Services (XNS)**

A protocol suite developed by Xerox that provides general purpose network communications, Internet routing, and packet delivery.

