

USER'S GUIDE



Hitron BVW-3653

VERSION 1.0
APRIL 2009

DEFAULT LOGIN DETAILS	
IP Address	192.168.0.1
Username	admin
Password	password



HitronTechnologies



ABOUT THIS USER'S GUIDE

INTENDED AUDIENCE

This manual is intended for people who want to configure the BVW-3653's features via its Graphical User Interface (GUI).

HOW TO USE THIS USER'S GUIDE

This manual contains information on each the BVW-3653's GUI screens, and describes how to use its various features.

- ▶ Use the **Introduction** (page 15) to see an overview of the topics covered in this manual.
- ▶ Use the **Table of Contents** (page 7), **List of Figures** (page 11) and **List of Tables** (page 13) to quickly find information about a particular GUI screen or topic.
- ▶ Use the **Index** (page 101) to find information on a specific keyword.
- ▶ Use the rest of this User's Guide to see in-depth descriptions of the BVW-3653's features.

RELATED DOCUMENTATION

- ▶ **Quick Installation Guide:** see this for information on getting your BVW-3653 up and running right away. It includes information on system requirements, package contents, the installation procedure, and basic troubleshooting tips.
- ▶ **Online Help:** each screen in the BVW-3653's Graphical User Interface (GUI) contains a **Help** button. Click this button to see additional information about configuring the screen.

DOCUMENT CONVENTIONS

This User's Guide uses various typographic conventions and styles to indicate content type:

▶ Bulleted paragraphs are used to list items, and to indicate options.

1 Numbered paragraphs indicate procedural steps.

NOTE: Notes provide additional information on a subject.



Warnings provide information about actions that could harm you or your device.

Product labels, field labels, field choices, etc. are in **bold** type. For example:

Select **UDP** to use the User Datagram Protocol.

A mouse click in the Graphical User Interface (GUI) is denoted by a right angle bracket (>). For example:

Click **Settings > Advanced Settings**.

means that you should click **Settings** in the GUI, then **Advanced settings**.

A key stroke is denoted by square brackets and uppercase text. For example:

Press [ENTER] to continue.

CUSTOMER SUPPORT

For technical assistance or other customer support issues, please consult your Hitron representative.

USER'S GUIDE FEEDBACK

Please send all User's Guide-related comments, questions or suggestions to info@carliletech.com. Thank you!

Written by Rick Carlile.

Copyright © 2010 Hitron Technologies. All rights reserved. All trademarks and registered trademarks used are the properties of their respective owners.

DISCLAIMER: The information in this User's Guide is accurate at the time of writing. This User's Guide is provided "as is" without express or implied warranty of any kind. Neither Hitron Technologies nor its agents assume any liability for inaccuracies in this User's Guide, or losses incurred by use or misuse of the information in this User's Guide.

TABLE OF CONTENTS

About This User's Guide	3
Table of Contents.....	7
List of Figures	11
List of Tables.....	13
Introduction.....	15
1.1 BVW-3653 Overview	15
1.1.1 Key Features	15
1.2 Hardware Connections	16
1.3 LEDs	18
1.4 IP Address Setup	20
1.4.1 Manual IP Address Setup	21
1.5 Logging into the BVW-3653	22
1.6 GUI Overview	23
1.7 Resetting the BVW-3653	23
Cable.....	25
2.1 Cable Overview	25
2.1.1 DOCSIS	25
2.1.2 IP Addresses and Subnets	25
2.1.2.1 IP Address Format	25
2.1.2.2 IP Address Assignment	25
2.1.2.3 Subnets	26
2.1.3 DHCP	27
2.1.4 DHCP Lease	28
2.1.5 MAC Addresses	28

2.1.6 Routing Mode	28
2.1.7 Configuration Files	29
2.1.8 Downstream and Upstream Transmissions	29
2.1.9 Cable Frequencies	29
2.1.10 Modulation	29
2.1.11 TDMA, FDMA and SCDMA	30
2.2 The System Info Screen	30
2.3 The Initialization Screen	32
2.4 The Status Screen	33
2.5 The Event Log Screen	35
2.6 The Password Screen	36
LAN	39
3.1 LAN Overview	39
3.1.1 Local Area Networks	39
3.1.2 LAN IP Addresses and Subnets	39
3.1.3 Domain Suffix	40
3.1.4 Debugging (Ping and Traceroute)	40
3.2 The LAN IP Screen	40
3.3 The Switch Setup Screen	42
3.4 The Debug Screen	43
3.5 The Backup Screen	44
Firewall	45
4.1 Firewall Overview	45
4.1.1 Firewall	45
4.1.2 Intrusion detection system	45
4.1.3 Ping	45
4.1.4 MAC Filtering	45
4.1.5 IP Filtering	46
4.1.6 Port Forwarding	46
4.1.7 Port Triggering	46
4.1.8 DMZ	46
4.2 The Firewall Options Screen	47
4.3 The MAC Filtering Screen	47
4.4 The IP Filtering Screen	50
4.4.1 Adding or Editing an IP Filtering Rule	51
4.5 The Forwarding Screen	53
4.5.1 Adding or Editing a Port Forwarding Rule	55
4.6 The Port Triggering Screen	56

4.6.1 Adding or Editing a Port Triggering Rule	58
4.7 The DMZ Setting Screen	60
4.8 The Local Logs Screen	60
Parental Control	63
5.1 Parental Control Overview	63
5.1.1 Website Blocking	63
5.2 The Web Site Blocking Screen	63
5.3 The Scheduling Screen	65
5.4 The Local Logs Screen	67
Wireless	69
6.1 Wireless Overview	69
6.1.1 Wireless Networking Basics	69
6.1.2 Architecture	69
6.1.3 Wireless Standards	69
6.1.4 Service Sets and SSIDs	70
6.1.5 Wireless Security	70
6.1.5.1 WPS	71
6.1.6 WMM	71
6.2 The Basic Screen	71
6.3 The Security Screen	74
6.4 The Access Control Screen	78
6.5 The Advanced Screen	80
6.5.1 Configuring WMM Parameters	86
EMTA	91
7.1 The Status Screen	91
7.2 The DHCP Screen	92
7.3 The QoS Screen	93
7.4 The Event Log Screen	95
Troubleshooting	97
Index	101

LIST OF FIGURES

FIGURE 1: Application Overview	15
FIGURE 2: Hardware Connections	17
FIGURE 3: LEDs	19
FIGURE 4: Login	22
FIGURE 5: GUI Overview	23
FIGURE 6: The Cable > System Info Screen	31
FIGURE 7: The Cable > Initialization Screen	32
FIGURE 8: The Cable > Status Screen	33
FIGURE 9: The Cable > Event Log Screen	36
FIGURE 10: The Cable > Password Screen	37
FIGURE 11: The LAN > LAN IP Screen	41
FIGURE 12: The LAN > Switch Setup Screen	42
FIGURE 13: The LAN > Debug Screen	43
FIGURE 14: The LAN > Backup Screen	44
FIGURE 15: The Firewall > Firewall Options Screen	47
FIGURE 16: The Firewall > MAC Filtering Screen	48
FIGURE 17: The Firewall > IP Filtering Screen	50
FIGURE 18: The Firewall > IP Filtering > Add/Edit Screen	52
FIGURE 19: The Firewall > Forwarding Screen	53
FIGURE 20: The Firewall > Forwarding > Add/Edit Screen	55
FIGURE 21: The Firewall > Port Triggering Screen	57
FIGURE 22: The Firewall > Port Triggering > Add/Edit Screen	58
FIGURE 23: The Firewall > DMZ Setting Screen	60
FIGURE 24: The Firewall > Local Logs Screen	61
FIGURE 25: The Parent Control > Web Site Blocking Screen	64
FIGURE 26: The Parent Control > Scheduling Screen	66
FIGURE 27: The Parent Control > Local Logs Screen	67
FIGURE 28: The Wireless > Basic Screen	72
FIGURE 29: WPS PIN	73
FIGURE 30: The Wireless > Security Screen	75
FIGURE 31: The Wireless > Access Control	79

FIGURE 32: The Wireless > Advanced Screen	81
FIGURE 33: The Wireless > Advanced > WMM Configuration Screen	86
FIGURE 34: The EMTA > Status Screen	91
FIGURE 35: The EMTA > DHCP Screen	92
FIGURE 36: The EMTA > QoS Screen	94
FIGURE 37: The EMTA > Event Log Screen	95

LIST OF TABLES

TABLE 1: Hardware Connections	18
TABLE 2: LEDs	19
TABLE 3: GUI Overview	23
TABLE 4: Private IP Address Ranges	26
TABLE 5: IP Address: Decimal and Binary	27
TABLE 6: Subnet Mask: Decimal and Binary	27
TABLE 7: The Cable > System Info Screen	31
TABLE 8: The Cable > Status Screen	34
TABLE 9: The Cable > Event Log Screen	36
TABLE 10: The Cable > Password Screen	37
TABLE 11: The LAN > LAN IP Screen	41
TABLE 12: The LAN > Switch Setup Screen	42
TABLE 13: The LAN > Debug Screen	43
TABLE 14: The LAN > Backup Screen	44
TABLE 15: The Firewall > Firewall Options Screen	47
TABLE 16: The Firewall > MAC Filtering Screen	48
TABLE 17: The Firewall > IP Filtering Screen	50
TABLE 18: The Firewall > IP Filtering > Add/Edit Screen	52
TABLE 19: The Firewall > Forwarding Screen	53
TABLE 20: The Firewall > Forwarding > Add/Edit Screen	55
TABLE 21: The Firewall > Port Triggering Screen	57
TABLE 22: The Firewall > Port Triggering > Add/Edit Screen	59
TABLE 23: The Firewall > DMZ Setting Screen	60
TABLE 24: The Firewall > Local Logs Screen	61
TABLE 25: The Parent Control > Web Site Blocking Screen	64
TABLE 26: The Parent Control > Scheduling Screen	66
TABLE 27: The Parental Control > Local Logs Screen	67
TABLE 28: The Wireless > Basic Screen	72
TABLE 29: The Wireless > Security Screen	75
TABLE 30: The Wireless > Access Control Screen	79
TABLE 31: The Wireless > Advanced Screen	82

TABLE 32: The Wireless > Advanced > WMM Configuration Screen	87
TABLE 33: The EMTA > Status Screen	91
TABLE 34: The EMTA > DHCP Screen	93
TABLE 35: The EMTA > QoS Screen	94
TABLE 36: The EMTA > Event Log Screen	95

1

INTRODUCTION

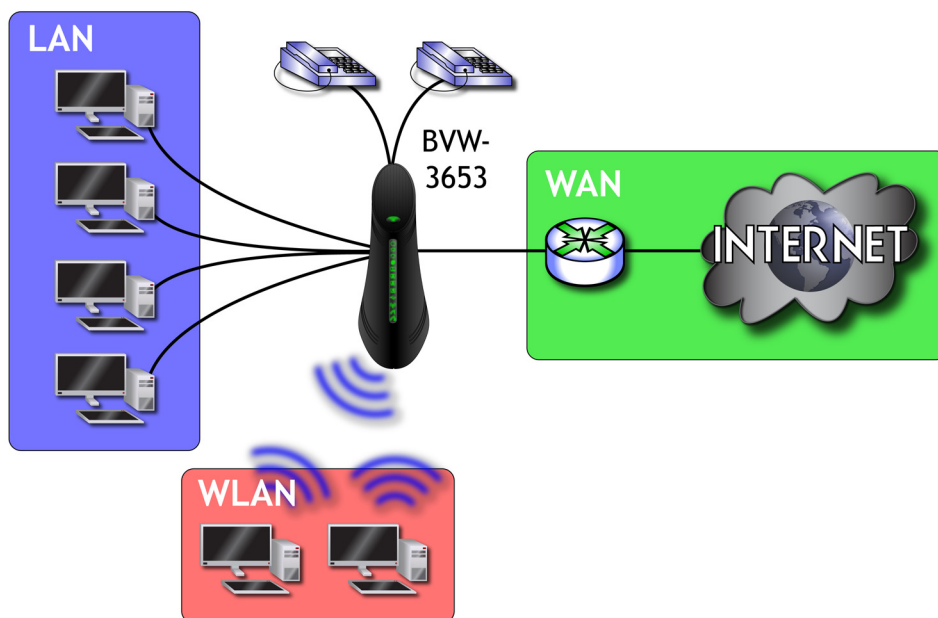
This chapter introduces the BVW-3653 and its GUI (Graphical User Interface).

1.1 BVW-3653 OVERVIEW

Your BVW-3653 is a voice-enabled cable modem and wireless access point that allows you to connect your computers, analog telephones, wireless devices, and other network devices to one another, and to the Internet via the cable connection.

Computers with a wired connection to the BVW-3653 are on the Local Area Network (LAN), computers with a wireless connection to the BVW-3653 are on the Wireless Local Area Network (WLAN) and the BVW-3653 connects to the service provider over the Wide Area Network (WAN).

FIGURE 1: Application Overview



1.1.1 KEY FEATURES

The BVW-3653 provides:

- ▶ Internet connection to cable modem service via **CATV** port (F-type RF connector)
- ▶ Voice over IP (VoIP) connection to your voice service provider.
- ▶ Local Area Network connection via four 10/100/1000 Mbps (megabits per second) Ethernet ports
- ▶ Dynamic Host Configuration Protocol (DHCP) for devices on the LAN
- ▶ LAN troubleshooting tools (Ping and Traceroute)
- ▶ IEEE 802.11b/g/n wireless MIMO (Multiple-In, Multiple-Out) networking, allowing speeds of up to 300Mbps
- ▶ Advanced wireless configuration features including Wifi MultiMedia (WMM) Quality of Service (Qos) setup, IGMP snooping,
- ▶ Wireless security: WEP, WPA-PSK and WPA2-PSK encryption, Wifi Protected Setup (WPS) push-button and PIN configuration, MAC filtering,
- ▶ Wired security: stateful inspection firewall with intrusion detection system, IP and MAC filtering, port forwarding and port triggering, De-Militarized Zone (DMZ) and event logging
- ▶ Parental control: scheduled website blocking and access logs
- ▶ Settings backup and restore
- ▶ Secure configuration interface, accessible by Web browser

1.2 HARDWARE CONNECTIONS

This section describes the BVW-3653's physical ports and buttons.

FIGURE 2: Hardware Connections

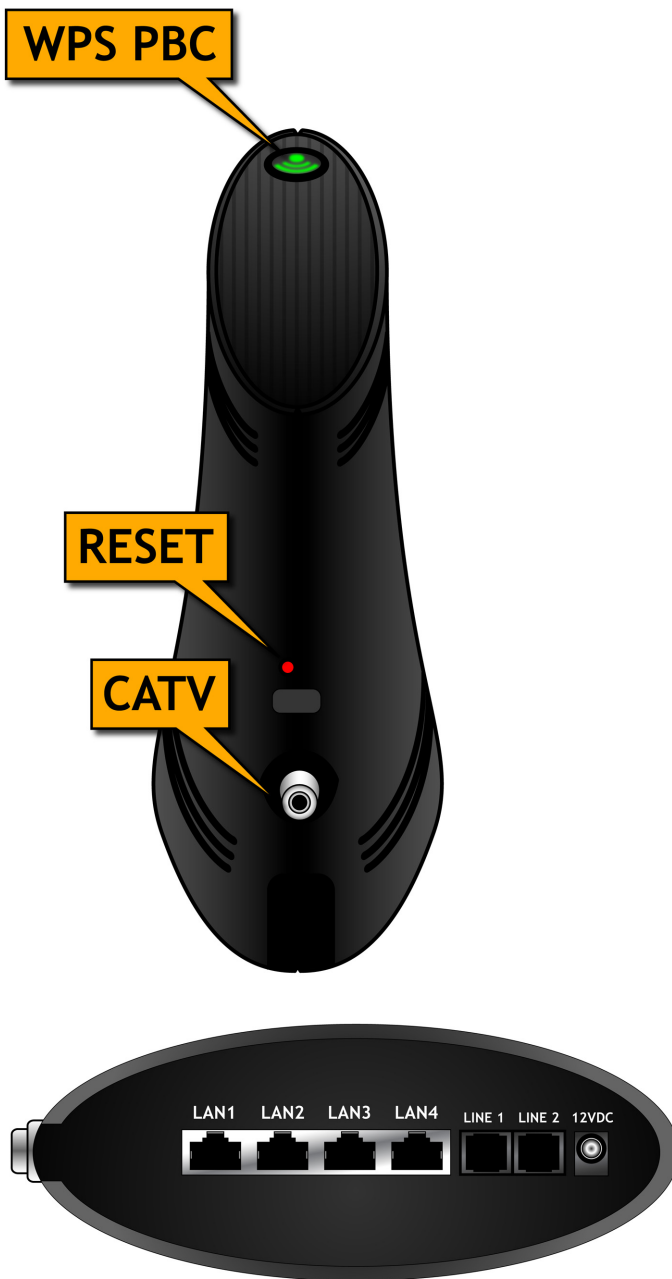



TABLE 1: Hardware Connections

WPS PBC	Press this button to begin the WiFi Protected Setup (WPS) Push-Button Configuration (PBC) procedure. Press the PBC button on your wireless clients in the coverage area within two minutes to enable them to join the wireless network. See WPS on page 71 for more information.
12VDC	Use this to connect to the 12v/2.0A power adapter that came with your BVW-3653.  NEVER use another power adapter with your BVW-3653. Doing so could harm your BVW-3653.
CATV	Use this to connect to the Internet via an F-type RF cable.
Reset	Use this button to reboot or reset your BVW-3653. ▶ Press the button and hold it for less than five seconds to reboot the BVW-3653. The BVW-3653 restarts, using your existing settings. ▶ Press the button and hold it for more than five seconds to delete all user-configured settings and restart the BVW-3653 using its factory default settings.
LAN1	Use these ports to connect your computers and other network devices, using Category 5 or 6 Ethernet cables with RJ45 connectors.
LAN2	
LAN3	
LAN4	
Line 1	Use these ports to connect your analog phones for VoIP services, using cables with RJ11 connectors.
Line 2	

1.3 LEDS

This section describes the BVW-3653's LEDs (lights).

FIGURE 3: LEDs



TABLE 2: LEDs







LED	STATUS	DESCRIPTION
Power 	On	The BVW-3653 is receiving power.
	Off	The BVW-3653 is not receiving power.

TABLE 2: LEDs

DS 	Blinking	The BVW-3653 is searching for a downstream frequency on the CATV connection.
	On	The BVW-3653 has successfully located and locked onto a downstream frequency on the CATV connection.
US 	Blinking	The BVW-3653 is searching for an upstream frequency on the CATV connection.
	On	The BVW-3653 has successfully located and locked onto an upstream frequency on the CATV connection.
Status 	Blinking	The BVW-3653's cable modem is registering with the service provider.
	On	The BVW-3653's cable modem has successfully registered with the service provider.
ETH 1~4 	Off	No device is connected to the relevant LAN port.
	Blinking (Yellow)	A device is connected to the relevant LAN port via a fast Ethernet link, and is transmitting or receiving data.
	Blinking (Blue)	A device is connected to the relevant LAN port via a gigabit ethernet link, and is transmitting or receiving data.
	On (Yellow)	A device is connected to the relevant LAN port via a fast ethernet link, but is not transmitting or receiving data.
	On (Blue)	A device is connected to the relevant LAN port via a gigabit ethernet link, but is not transmitting or receiving data.
Line 1 Line 2 	Off	No telephone is connected to the relevant Line port.
	Blinking	A telephone is connected to the relevant Line port, and is off-hook.
	On	A telephone is connected to the relevant Line port, and is on-hook.

1.4 IP ADDRESS SETUP

Before you log into the BVW-3653's GUI, your computer's IP address must be in the same subnet as the BVW-3653. This allows your computer to communicate with the BVW-3653.

NOTE: See IP Addresses and Subnets on page 25 for background information.

The BVW-3653 has a built-in DHCP server that, when active, assigns IP addresses to computers on the LAN. When the DHCP server is active, you can get an IP address automatically. The DHCP server is active by default.

If your computer is configured to get an IP address automatically, or if you are not sure, try to log in to the BVW-3653 (see [Logging into the BVW-3653](#) on page 22).

- ▶ If the login screen displays, your computer is already configured correctly.
- ▶ If the login screen does not display, either the BVW-3653's DHCP server is not active or your computer is not configured correctly. Follow the procedure in [Manual IP Address Setup](#) on page 21 and set your computer to get an IP address automatically. Try to log in again. If you cannot log in, follow the manual IP address setup procedure again, and set a specific IP address as shown. Try to log in again.

NOTE: If you still cannot see the login screen, your BVW-3653's IP settings may have been changed from their defaults. If you do not know the BVW-3653's new address, you should return it to its factory defaults. See [Resetting the BVW-3653](#) on page 23. Bear in mind that ALL user-configured settings are lost.

1.4.1 MANUAL IP ADDRESS SETUP

By default, your BVW-3653's local IP address is **192.168.0.1**. If your BVW-3653 is using the default IP address, you should set your computer's IP address to be between **192.168.0.2** and **192.168.0.255**.

NOTE: If your BVW-3653 DHCP server is active, set your computer to get an IP address automatically in step 5. The BVW-3653 assigns an IP address to your computer. The DHCP server is active by default.

Take the following steps to manually set up your computer's IP address to connect to the BVW-3653:

NOTE: This example uses Windows XP; the procedure for your operating system may be different.

- 1** Click **Start**, then click **Control Panel**.
- 2** In the window that displays, double-click **Network Connections**.
- 3** Right-click your network connection (usually **Local Area Connection**) and click **Properties**.
- 4** In the **General** tab's **This connection uses the following items** list, scroll down and select **Internet Protocol (TCP/IP)**. Click **Properties**.
- 5** You can get an IP address automatically, or specify one manually:

- ▶ If your BVW-3653's DHCP server is active, select **Get an IP address automatically**.
- ▶ If your BVW-3653's DHCP server is active, select **Use the following IP address**. In the **IP address** field, enter a value between **192.168.0.2** and **192.168.0.255** (default). In the **Subnet mask** field, enter **255.255.255.0** (default).

NOTE: If your BVW-3653 is not using the default IP address, enter an IP address and subnet mask that places your computer in the same subnet as the BVW-3653.

- 6** Click **OK**. The **Internet Protocol (TCP/IP)** window closes. In the **Local Area Connection Properties** window, click **OK**.

Your computer now obtains an IP address from the BVW-3653, or uses the IP address that you specified, and can communicate with the BVW-3653.

1.5 LOGGING INTO THE BVW-3653

Take the following steps to log into the BVW-3653's GUI.

NOTE: You can log into the BVW-3653's GUI via the wireless interface. However, it is strongly recommended that you configure the BVW-3653 via a wired connection on the LAN.

- 1** Open a browser window.
- 2** Enter the BVW-3653's IP address (default **192.168.0.1**) in the URL bar. The **Login** screen displays.

FIGURE 4: Login



The screenshot shows a login dialog box with a light gray background. At the top, it says "Please Enter login information:". Below this, there are two text input fields. The first is labeled "Username" and the second is labeled "Password". At the bottom of the dialog, there are two buttons: "login" and "cancel".

- 3** Enter the **Username** and **Password**. The default login username is **admin**, and the default password is **password**.

NOTE: The Username and Password are case-sensitive; "admin" is not the same as "Admin".

- 4 Click **Login**. The **Initialization** screen displays (see **The Initialization Screen** on page 32).

1.6 GUI OVERVIEW

This section describes the BVW-3653's GUI.

FIGURE 5: GUI Overview

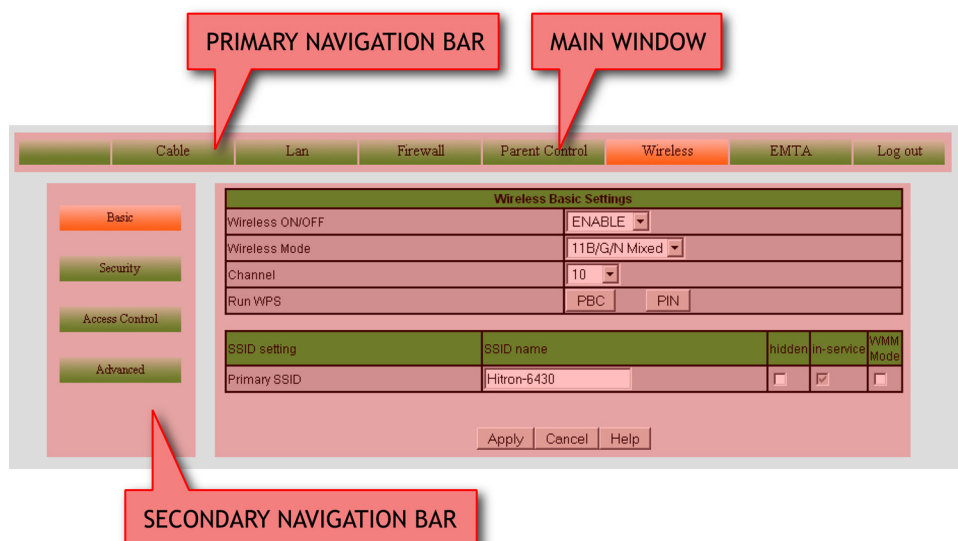


TABLE 3: GUI Overview

Primary Navigation Bar	Use this section to move from one part of the GUI to another.
Secondary Navigation Bar	Use this section to move from one related screen to another.
Main Window	Use this section to read information about your BVW-3653's configuration, and make configuration changes.

1.7 RESETTING THE BVW-3653

When you reset the BVW-3653 to its factory defaults, all user-configured settings are lost, and the BVW-3653 is returned to its initial configuration state.

- ▶ There are two ways to reset the BVW-3653:
- ▶ Press the **RESET** button on the BVW-3653, and hold it in for five seconds or longer.

Click **LAN > Backup**. In the screen that displays, click the **Factory Reset** button.

The BVW-3653 turns off and on again, using its factory default settings.

NOTE: Depending on your BVW-3653's previous configuration, you may need to re-configure your computer's IP settings; see IP Address Setup on page 20.



CABLE

This chapter describes the screens that display when you click **Cable** in the toolbar.

2.1 CABLE OVERVIEW

This section describes some of the concepts related to the **Cable** screens.

2.1.1 DOCSIS

The Data Over Cable Service Interface Specification (DOCSIS) is a telecommunications standard that defines the provision of data services (Internet access) over a traditional cable TV (CATV) network.

Your BVW-3653 supports DOCSIS version 3.0.

2.1.2 IP ADDRESSES AND SUBNETS

Every computer on the Internet must have a unique Internet Protocol (IP) address. The IP address works much like a street address, in that it identifies a specific location to which information is transmitted. No two computers on a network can have the same IP address.

2.1.2.1 IP ADDRESS FORMAT

IP addresses consist of four octets (8-bit numerical values) and are usually represented in decimal notation, for example **192.168.0.1**. In decimal notation, this means that each octet has a minimum value of 0 and a maximum value of 255.

An IP address carries two basic pieces of information: the “network number” (the address of the network as a whole, analogous to a street name) and the “host ID” (analogous to a house number) which identifies the specific computer (or other network device).

2.1.2.2 IP ADDRESS ASSIGNMENT

IP addresses can come from three places:

- ▶ The Internet Assigned Numbers Agency (IANA)

- ▶ Your Internet Service Provider
- ▶ You (or your network devices)

IANA is responsible for IP address allocation on a global scale, and your ISP assigns IP addresses to its customers. You should never attempt to define your own IP addresses on a public network, but you are free to do so on a private network.

In the case of the BVW-3653:

- ▶ The public network (Wide Area Network or WAN) is the link between the cable (CATV) connector and your Internet Service Provider. Your BVW-3653's IP address on this network is assigned by your service provider.
- ▶ The private network (in routing mode - see **Routing Mode** on page 28) is your Local Area Network (LAN) and Wireless Local Area Network (WLAN), if enabled. You are free to assign IP addresses to computers on the LAN and WLAN manually, or to allow the BVW-3653 to assign them automatically via DHCP (Dynamic Host Configuration Protocol). IANA has reserved the following blocks of IP addresses to be used for private networks only:

TABLE 4: Private IP Address Ranges

FROM...	...TO
10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

If you assign addresses manually, they must be within the BVW-3653's LAN subnet.

2.1.2.3 SUBNETS

A subnet (short for sub-network) is, as the name suggests, a separate section of a network, distinct from the main network of which it is a part. A subnet may contain all of the computers at one corporate local office, for example, while the main network includes several offices.

In order to define the extent of a subnet, and to differentiate it from the main network, a subnet mask is used. This "masks" the part of the IP address that refers to the main network, leaving the part of the IP address that refers to the sub-network.

Each subnet mask has 32 bits (binary digits), as does each IP address:

- ▶ A binary value of **1** in the subnet mask indicates that the corresponding bit in the IP address is part of the main network.
- ▶ A binary value of **0** in the subnet mask indicates that the corresponding bit in the IP address is part of the sub-network.

For example, the following table shows the IP address of a computer (**192.168.0.1**) expressed in decimal and binary (each cell in the table indicates one octet):

TABLE 5: IP Address: Decimal and Binary

192	168	0	1
11000000	10101000	00000000	00000001

The following table shows a subnet mask that “masks” the first twenty-four bits of the IP address, in both its decimal and binary notation.

TABLE 6: Subnet Mask: Decimal and Binary

255	255	255	0
11111111	11111111	11111111	00000000

This shows that in this subnet, the first three octets (**192.168.0**, in the example IP address) define the main network, and the final octet (**1**, in the example IP address) defines the computer's address on the subnet.

The decimal and binary notations give us the two common ways to write a subnet mask:

- ▶ **Decimal:** the subnet mask is written in the same fashion as the IP address: **255.255.255.0**, for example.
- ▶ **Binary:** the subnet mask is indicated after the IP address (preceded by a forward slash), specifying the number of binary digits that it masks. The subnet mask **255.255.255.0** masks the first twenty-four bits of the IP address, so it would be written as follows: **192.168.0.1/24**.

2.1.3 DHCP

The Dynamic Host Configuration Protocol, or DHCP, defines the process by which IP addresses can be assigned to computers and other networking devices automatically, from another device on the network. This device is known as a DHCP server, and provides addresses to all the DHCP client devices.

In order to receive an IP address via DHCP, a computer must first request one from the DHCP server (this is a broadcast request, meaning that it is sent out to the whole network, rather than just one IP address). The DHCP server hears the requests, and responds by assigning an IP address to the computer that requested it.

If a computer is not configured to request an IP address via DHCP, you must configure an IP address manually if you want to access other computers and devices on the network. See [IP Address Setup](#) on page 20 for more information.

By default, the BVW-3653 is a DHCP client on the WAN (the CATV connection). It broadcasts an IP address over the cable network, and receives one from the service provider. By default, the BVW-3653 is a DHCP server on the LAN; it provides IP addresses to computers on the LAN which request them.

2.1.4 DHCP LEASE

“DHCP lease” refers to the length of time for which a DHCP server allows a DHCP client to use an IP address. Usually, a DHCP client will request a DHCP lease renewal before the lease time is up, and can continue to use the IP address for an additional period. However, if the client does not request a renewal, the DHCP server stops allowing the client to use the IP address.

This is done to prevent IP addresses from being used up by computers that no longer require them, since the pool of available IP addresses is finite.

2.1.5 MAC ADDRESSES

Every network device possesses a Media Access Control (MAC) address. This is a unique alphanumeric code, given to the device at the factory, which in most cases cannot be changed (although some devices are capable of “MAC spoofing”, where they impersonate another device’s MAC address).

MAC addresses are the most reliable way of identifying network devices, since IP addresses tend to change over time (whether manually altered, or updated via DHCP).

Each MAC address displays as six groups of two hexadecimal digits separated by colons (or, occasionally, dashes) for example **00:AA:FF:1A:B5:74**.

NOTE: Each group of two hexadecimal digits is known as an “octet”, since it represents eight bits.

Bear in mind that a MAC address does not precisely represent a computer on your network (or elsewhere), it represents a network device, which may be part of a computer (or other device). For example, if a single computer has an Ethernet card (to connect to your BVW-3653 via one of the **LAN** ports) and also has a wireless card (to connect to your BVW-3653 over the wireless interface) the MAC addresses of the two cards will be different. In the case of the BVW-3653, each internal module (cable modem module, Ethernet module, wireless module, etc.) possesses its own MAC address.

2.1.6 ROUTING MODE

When your BVW-3653 is in routing mode, it acts as a gateway for computers on the LAN to access the Internet. The service provider assigns an IP address to the BVW-3653 on the WAN, and all traffic for LAN computers is sent to that IP address. The BVW-3653 assigns private IP addresses to LAN computers (when DHCP is active), and transmits the relevant traffic to each private IP address.

NOTE: When DHCP is not active on the BVW-3653 in routing mode, each computer on the LAN must be assigned an IP address in the BVW-3653’s subnet manually.

When the BVW-3653 is not in routing mode, the service provider assigns an IP address to each computer connected to the BVW-3653 directly. The BVW-3653 does not perform any routing operations, and traffic flows between the computers and the service provider.

Routing mode is not user-configurable; it is specified by the service provider in the BVW-3653's configuration file.

2.1.7 CONFIGURATION FILES

The BVW-3653's configuration (or config) file is a document that the BVW-3653 obtains automatically over the Internet from the service provider's server, which specifies the settings that the BVW-3653 should use. It contains a variety of settings that are not present in the user-configurable Graphical User Interface (GUI) and can be specified only by the service provider.

2.1.8 DOWNSTREAM AND UPSTREAM TRANSMISSIONS

The terms "downstream" and "upstream" refer to data traffic flows, and indicate the direction in which the traffic is traveling. "Downstream" refers to traffic from the service provider to the BVW-3653, and "upstream" refers to traffic from the BVW-3653 to the service provider.

2.1.9 CABLE FREQUENCIES

Just like radio transmissions, data transmissions over the cable network must exist on different frequencies in order to avoid interference between signals.

The data traffic band is separate from the TV band, and each data channel is separate from other data channels.

2.1.10 MODULATION

Transmissions over the cable network are based on a strong, high frequency periodic waveform known as the "carrier wave." This carrier wave is so called because it "carries" the data signal. The data signal itself is defined by variations in the carrier wave. The process of varying the carrier wave (in order to carry data signal information) is known as "modulation." The data signal is thus known as the "modulating signal."

Cable transmissions use a variety of methods to perform modulation (and the "decoding" of the received signal, or "demodulation"). The modulation methods defined in DOCSIS 3 are as follows:

- ▶ **QPSK:** Quadrature Phase-Shift Keying
- ▶ **QAM:** Quadrature Amplitude Modulation
- ▶ **QAM TCM:** Trellis modulated Quadrature Amplitude Modulation

In many cases, a number precedes the modulation type (for example **16 QAM**). This number refers to the complexity of modulation. The higher the number, the more data can be encoded in each symbol.

NOTE: In modulated signals, each distinct modulated character (for example, each audible tone produced by a modem for transmission over telephone lines) is known as a symbol.

Since more information can be represented by a single character, a higher number indicates a higher data transfer rate.

2.1.11 TDMA, FDMA AND SCDMA

Time Division Multiple Access (TDMA), Frequency Division Multiple Access (FDMA) and Synchronous Code Division Multiple Access (SCDMA) are channel access methods that allow multiple users to share the same frequency channel.

- ▶ TDMA allows multiple users to share the same frequency channel by splitting transmissions by time. Each user is allocated a number of time slots, and transmits during those time slots.
- ▶ FDMA allows multiple users to share the same frequency channel by assigning a frequency band within the existing channel to each user.
- ▶ SCDDMA allows multiple users to share the same frequency channel by assigning a unique orthogonal code to each user.

2.2 THE SYSTEM INFO SCREEN

Use this screen to see general information about your BVW-3653's hardware, its software, and its connection to the Internet.

NOTE: Most of the information that displays in this screen is for troubleshooting purposes only. However, you may need to use the MAC Address information when setting up your network.

Click **Cable > System Info**. The following screen displays.

FIGURE 6: The Cable > System Info Screen

This menu displays general information	
General Information	
Vendor identification:	Hitron Technologies
Model Name:	BVW-3653
DOCSIS main standard:	[test]
HW version:	1A
SW version:	1.4.0.1-SIP
Boot rom version:	PSPU-Boot(BBU) 1.0.1.7
MAC Address:	
RF MAC Address:	00:05:CA:5F:64:30
Ethernet MAC Address:	00:05:CA:5F:64:32
Mta MAC Address:	00:05:CA:5F:64:31
WAN MAC address(in routing mode)	00:05:CA:5F:64:33
Primary BSSID MAC address	00:05:CA:5F:64:38
System Time:	-----:--:--
System Uptime:	000 days 00h:26m:53s
Network Access:	Permitted

The following table describes the labels in this screen.

TABLE 7: The Cable > System Info Screen

General Information	
Vendor Identification	This displays the name of the company that supplied the BVW-3653.
Model Name	This displays the device's model name (BVW-3653).
DOCSIS Main Standard	This displays the version of the Data Over Cable Service Interface Specification (DOCSIS) standard to which the BVW-3653 complies.
HW Version	This displays the version number of the BVW-3653's physical hardware.
SW Version	This displays the version number of the software that controls the BVW-3653.
Boot ROM Version	This displays the version number of the program that controls the BVW-3653's boot procedure (in which the main software is loaded).
MAC Address	
RF MAC Address	This displays the Media Access Control (MAC) address of the BVW-3653's RF module. This is the module that connects to the Internet through the CATV connection.
Ethernet MAC Address	This displays the Media Access Control (MAC) address of the BVW-3653's Ethernet module. This is the module to which you connect through the LAN ports.
MTA MAC Address	This displays the Media Access Control (MAC) address of the BVW-3653's Multimedia Terminal Adapter (MTA) module.

TABLE 7: The Cable > System Info Screen (continued)

WAN MAC Address (in Routing Mode)	This displays the Media Access Control (MAC) address of the module that connects to the Internet through the CATV connection when the BVW-3653 is in routing mode.
Primary BSSID MAC Address	This displays the Media Access Control (MAC) address of the BVW-3653's Basic Service Set Identifier (BSSID). This is the MAC address of the wireless module to which wireless clients connect. NOTE: You may have additional BSSIDs, depending on your contract with your service provider.
System Time	This displays the current date and time.
System Uptime	This displays the number of days, hours, minutes and seconds since the BVW-3653 was last switched on or rebooted.
Network Access	This displays whether or not your service provider allows you to access the Internet over the CATV connection. ▶ Permitted displays if you can access the Internet. ▶ Denied displays if you cannot access the Internet.

2.3 THE INITIALIZATION SCREEN

This screen displays the steps successfully taken to connect to the Internet over the **CATV** connection.

Use this screen for troubleshooting purposes to ensure that the BVW-3653 has successfully connected to the Internet; if an error has occurred you can identify the stage at which the failure occurred.

NOTE: This screen displays when you first log in to the BVW-3653.

Click **Cable > Initialization**. The following screen displays.

FIGURE 7: The Cable > Initialization Screen

This menu displays the connectivity status of the modem and its boot state	
Modem Status	
HW init	Success
Find Downstream	Process...
Ranging	
DHCP	
Time of Day	
Download CM Config File	
Registration	
EAE status	Disable
BPI status	AUTH:start, TEK:start
Selected ISP index	0
Network Access	Permitted

For each step:

- ▶ **Process** displays when the BVW-3653 is attempting to complete a connection step.
- ▶ **Success** displays when the BVW-3653 has completed a connection step.

2.4 THE STATUS SCREEN

Use this screen to discover information about:

- ▶ The nature of the upstream and downstream connection between the BVW-3653 and the device to which it is connected through the **CATV** interface.
- ▶ IP details of the BVW-3653's WAN connection.
- ▶ Network devices attached to the BVW-3653.

You can also configure the BVW-3653's downstream center frequency.

Click **Cable > Status**. The following screen displays.

FIGURE 8: The Cable > Status Screen

This menu displays both upstream and downstream signal parameters and Attached Devices	
CM Configuration file name	[N/A]
Network Access	Permitted
Downstream	
Frequency to tune to:	627000000 Hz <input type="button" value="Apply"/>
Scanning start frequency:	999000000 Hz
Channel Frequency:	
Modulation:	
Signal strength:	
Signal noise ratio:	
Upstream	
Channel Id:	
Upstream Frequency:	
Upstream bandwidth:	
SCDMA mode:	
Transmission signal strength:	
Cable Modem IP Information	
IP Address:	0.0.0.1
Subnet Mask:	
Gateway IP:	
DHCP Lease Time:	D: -- H: -- M: -- S: --
System Time:	---:--:--:--:--:--
Attached Devices	
Attached Interface	Mac Address
MTA	00:05:CA:5F:64:31

The following table describes the labels in this screen.

TABLE 8: The Cable > Status Screen

CM Configuration File Name	This displays the name of the configuration file that the BVW-3653 downloaded from your service provider. This file provides the BVW-3653 with the service parameter data that it needs to perform its functions correctly.
Network Access	This displays whether or not your service provider allows you to access the Internet over the CATV connection. ▶ Permitted displays if you can access the Internet. ▶ Denied displays if you cannot access the Internet.
Downstream	
NOTE: The downstream signal is the signal transmitted to the BVW-3653.	
Frequency to Tune to	This displays the current center frequency in Hertz (Hz) over which data is transmitted to the BVW-3653 over the CATV interface. This is the frequency to which the BVW-3653 is locked in; it will only scan for another frequency if this frequency becomes unavailable. If you want the BVW-3653 to attempt to connect at a different frequency, enter it in the field and click Apply . NOTE: Do not change the frequency unless you have a good reason to do so.
Scanning Start Frequency	This displays the frequency in Hertz (Hz) at which the BVW-3653 begins scanning for a connection over the CATV interface (if a frequency is not already locked in).
Channel Frequency	This displays the actual frequency of each downstream data channel to which the BVW-3653 is connected.
Modulation	This displays the type of modulation that each downstream channel uses. Possible modulation types
Signal Strength	This displays the power of the signal of each downstream data channel to which the BVW-3653 is connected, in dBmV (decibels above/below 1 millivolt).
Signal Noise Ratio	This displays the Signal to Noise Ratio (SNR) of each downstream data channel to which the BVW-3653 is connected, in dB (decibels).
Upstream	
NOTE: The upstream signal is the signal transmitted from the BVW-3653.	
Channel ID	This displays the ID number of each channel on which the upstream signal is transmitted.
Upstream Frequency	This displays the frequency in Herz (Hz) of each upstream data channel to which the BVW-3653 is connected.

TABLE 8: The Cable > Status Screen (continued)

Upstream Bandwidth	This displays the bandwidth of each upstream data channel to which the BVW-3653 is connected (in Hertz).
SCDMA Mode	This displays the Synchronous Code Division Multiple Access (SCDMA) mode of each channel on which the upstream signal is transmitted.
Transmission Signal Strength	This displays the transmitted power of the signal of each upstream data channel to which the BVW-3653 is connected, in dBmV (decibels above/below 1 millivolt).
Cable Modem IP Information	
IP Address	This displays the BVW-3653's WAN IP address. This IP address is automatically assigned to the BVW-3653
Subnet Mask	This displays the BVW-3653's WAN subnet mask.
Gateway IP	This displays the IP address of the device to which the BVW-3653 is connected over the CATV interface.
DHCP Lease Time	This displays the time that elapses before your device's IP address lease expires, and a new IP address is assigned to it by the DHCP server.
System Time	This displays the current date and time.
Attached Devices	
Attached Interface	This displays the interface on which each network device is connected. NOTE: The MTA module always displays in this list.
MAC Address	This displays the Media Access Control (MAC) address of each connected network device.

2.5 THE EVENT LOG SCREEN

Use this screen to see information about unexpected system events that have occurred. The BVW-3653 creates a log entry for each event.

Click **Cable > Event Log**. The following screen displays.

FIGURE 9: The Cable > Event Log Screen

This menu displays the event logs of the modem

System Event Log				
Index	Date/Time	ID	Level	Text
1	01/01/70 00:41:50	cmstatus	warning	Lost MDD Timeout;CM-MAC=00:05:ca:5f:64:30;CMTS-MAC=00:10:29:37:54:38;CM-QOS=1.1;CM-VER=3.0;
2	01/01/70 00:41:50	cmstatus	warning	MDD message timeout;CM-MAC=00:05:ca:5f:64:30;CMTS-MAC=00:10:29:37:54:38;CM-QOS=1.1;CM-VER=3.0;
3	01/07/10 08:32:09	cmstatus	critical	SYNC Timing Synchronization failure - Loss of Sync;CM-MAC=00:05:ca:5f:64:30;CMTS-MAC=00:10:29:37:54:38;CM-QOS=1.1;CM-VER=3.0;
4	01/07/10 08:32:21	cmstatus	critical	Received Response to Broadcast Maintenance Request, But no Unicast Maintenance opportunities received - T4 time out;CM-MAC=00:05:ca:5f:64:30;CMTS-MAC=00:10:29:37:54:38;CM-QOS=1.1;CM-VER=3.0;

The following table describes the labels in this screen.

TABLE 9: The Cable > Event Log Screen

Index	This displays the incremental identification number assigned to the logged event.
Date/Time	This displays the date and time at which the event that triggered the log entry occurred.
ID	This displays cmstatus (cable modem status).
Level	This displays the severity level of the event that triggered the log entry. Possible levels (in order of severity) are: <ul style="list-style-type: none"> ▶ Error ▶ Warning ▶ Critical
Text	This displays automatically-generated specific information about the event that triggered the log entry.
Clear Log	Click this to remove all entries from the log. Deleted log entry data cannot be retrieved.
Help	Click this to see information about the fields in this screen.

2.6 THE PASSWORD SCREEN

Use this screen to change the password with which you log in to the BVW-3653.

NOTE: If you forget your password, you will need to reset the BVW-3653 to its factory defaults.

Click **Cable > Password**. The following screen displays.

FIGURE 10: The Cable > Password Screen

This menu displays the event logs of the modem

Modify Password	
Enter Current Password	<input type="text"/>
Enter New Password	<input type="text"/>
Re-enter New Password	<input type="text"/>
Password Idle Time	10 minutes
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>	

The following table describes the labels in this screen.

TABLE 10: The Cable > Password Screen

Enter Current Password	Enter the password with which you currently log into the BVW-3653
Enter New Password	Enter and re-enter the password you want to use to log into the BVW-3653.
Re-Enter New Password	
Password Idle Time	Enter the number of minutes of inactivity after which you should be automatically logged out of the BVW-3653. Once this period elapses, you will need to log in again.
Apply	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.



3

LAN

This chapter describes the screens that display when you click **LAN** in the toolbar.

3.1 LAN OVERVIEW

This section describes some of the concepts related to the **LAN** screens.

3.1.1 LOCAL AREA NETWORKS

A Local Area Network (LAN) is a network of computers and other devices that usually occupies a small physical area (a single building, for example). Your BVW-3653's LAN consists of all the computers and other networking devices connected to the **LAN 1~4** ports. This is your private network (in routing mode - see **Routing Mode** on page 28).

The LAN is a separate network from the Wide Area Network (WAN). In the case of the BVW-3653, the WAN refers to all computers and other devices available on the cable (**CATV**) connection.

By default, computers on the WAN cannot identify individual computers on the LAN; they can see only the BVW-3653. The BVW-3653 handles routing to and from individual computers on the LAN.

3.1.2 LAN IP ADDRESSES AND SUBNETS

IP addresses on the LAN are controlled either by the BVW-3653's built-in DHCP server (see **DHCP** on page 27), or by you (when you manually assign IP addresses to your computers).

For more information about IP addresses and subnets in general, see **IP Addresses and Subnets** on page 25.

3.1.3 DOMAIN SUFFIX

A domain is a location on a network, for instance **example.com**. On the Internet, domain names are mapped to the IP addresses to which they should refer by the Domain Name System. This allows you to enter “www.example.com” into your browser and reach the correct place on the Internet even if the IP address of the website’s server has changed.

Similarly, the BVW-3653 allows you to define a **Domain Suffix** to the LAN. When you enter the domain suffix into your browser, you can reach the BVW-3653 no matter what IP address it has on the LAN.

3.1.4 DEBUGGING (PING AND TRACEROUTE)

The BVW-3653 provides a couple of tools to allow you to perform network diagnostics on the LAN:

- ▶ Ping: this tool allows you to enter an IP address and see if a computer (or other network device) responds with that address on the network. The name comes from the pulse that submarine SONAR emits when scanning for underwater objects, since the process is rather similar. You can use this tool to see if an IP address is in use, or to discover if a device (whose IP address you know) is working properly.
- ▶ Traceroute: this tool allows you to see the route taken by data packets to get from the BVW-3653 to the destination you specify. You can use this tool to solve routing problems, or identify firewalls that may be blocking your access to a computer or service.

3.2 THE LAN IP SCREEN

Use this screen to:

- ▶ Configure the BVW-3653’s LAN IP address, subnet mask and domain suffix
- ▶ Configure the BVW-3653’s internal DHCP server
- ▶ See information about the network devices connected to the BVW-3653 on the LAN.

Click **LAN > LAN IP**. The following screen displays.

FIGURE 11: The LAN > LAN IP Screen

LAN Options	
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Domain Suffix	hitronhub.home

LAN DHCP	
Enable LAN DHCP	<input checked="" type="checkbox"/> Enabled
Lease Time	1 Week
DHCP Start IP	192.168.0.10
DHCP End IP	192.168.0.199

Host Name	IP Address	MAC Address	Type	Interface

The following table describes the labels in this screen.

TABLE 11: The LAN > LAN IP Screen

LAN Options	
IP Address	Use this field to define the IP address of the BVW-3653 on the LAN.
Subnet Mask	Use this field to define the LAN subnet. Use dotted decimal notation (for example, 255.255.255.0).
Domain Suffix	Use this field to define the domain that you can enter into a Web browser (instead of an IP address) to reach the BVW-3653 on the LAN. NOTE: The Domain Suffix is hitronhub.home by default.
LAN DHCP	
Enable LAN DHCP	Select this if you want the BVW-3653 to provide IP addresses to network devices on the LAN automatically. Deselect this if you already have a DHCP server on your LAN, or if you wish to assign IP addresses to your computers and other network devices manually.
Lease Time	Use this field to define the time after which the BVW-3653 renews the IP addresses of all the network devices connected to the BVW-3653 on the LAN (when DHCP is enabled).
DHCP Start IP	Use this field to specify the IP address at which the BVW-3653 begins assigning IP addresses to devices on the LAN (when DHCP is enabled).

TABLE 11: The LAN > LAN IP Screen (continued)

DHCP End IP	Use this field to specify the IP address at which the BVW-3653 stops assigning IP addresses to devices on the LAN (when DHCP is enabled). NOTE: Devices requesting IP addresses once the DHCP pool is exhausted are not assigned an IP address.
Host Name	This displays the name of each network device connected on the LAN.
IP Address	This displays the IP address of each network device connected on the LAN.
MAC Address	This displays the Media Access Control (MAC) address of each network device connected on the LAN.
Type	This displays whether the device's IP address was assigned by DHCP (DHCP-IP), or self-assigned .
Interface	This displays whether the device is connected on the LAN (Ethernet) or the WLAN (Wireless(x) , where x denotes the wireless mode; b , g or n).
Apply	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

3.3 THE SWITCH SETUP SCREEN

Use this screen to see information about the data rate and flow of each of the BVW-3653's **LAN** ports, and to activate or deactivate each port.

Click **LAN > Switch Setup**. The following screen displays.

FIGURE 12: The LAN > Switch Setup Screen

Port	Speed	Duplex	Active
1	100	full	✓ Active
2	10	half	✓ Active
3	10	half	✓ Active
4	10	half	✓ Active

The following table describes the labels in this screen.

TABLE 12: The LAN > Switch Setup Screen

Port	This displays the LAN port number.
Speed	This displays the maximum achievable data speed in megabits per second (MBPS).

TABLE 12: The LAN > Switch Setup Screen (continued)

Duplex	<ul style="list-style-type: none"> ▶ This displays Full when data can flow inbetween the BVW-3653 and the connected device in both directions simultaneously. ▶ This displays Half when data can flow inbetween the BVW-3653 and the connected device in only one direction at a time.
Active	<ul style="list-style-type: none"> ▶ Select a Port's checkbox to enable communications between the BVW-3653 and devices connected to the port. ▶ Deselect a Port's checkbox if you do not want to exchange data between the BVW-3653 and devices connected to the port.
Apply	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

3.4 THE DEBUG SCREEN

Use this screen to perform ping and traceroute tests on IP addresses or URLs.

Click **LAN > Debug**. The following screen displays.

FIGURE 13: The LAN > Debug Screen

The following table describes the labels in this screen.

TABLE 13: The LAN > Debug Screen

IP/URL	Enter the IP address or URL that you want to test.
Method	Select the type of test that you want to run on the IP/URL that you specified.
Run Test	Click this to perform the test.
Help	Click this to see information about the fields in this screen.

3.5 THE BACKUP SCREEN

Use this screen to back up your BVW-3653's settings to your computer, to load settings from a backup you created earlier, to reboot your BVW-3653, or to return it to its factory default settings.

Click **LAN > Backup**. The following screen displays.

FIGURE 14: The LAN > Backup Screen

This page is used for saving and restoring of end-user settable parameters to local PC using HTML. You can also reboot the device or reset all the settings back to the factory setting.

Backup/Restore Setting	
Backup Settings Locally	Backup
Restore Settings Locally	<input type="text"/> Choose... Restore
Reboot/Factory Reset	
Reboot	Reboot
Factory Reset	Factory Reset

Help

The following table describes the labels in this screen.

TABLE 14: The LAN > Backup Screen

Backup/Restore Setting	
Backup Settings Locally	Click this to create a backup of all your BVW-3653's settings on your computer.
Restore Settings Locally	Use these fields to return your BVW-3653's settings to those specified in a backup that you created earlier. Click Choose to select a backup, then click Restore to return your BVW-3653's settings to those specified in the backup.
Reboot/Factory Reset	
Reboot	Click this to restart your BVW-3653.
Factory Reset	Click this to return your BVW-3653 to its factory default settings. NOTE: When you do this, all your user-configured settings are lost, and cannot be retrieved.
Help	Click this to see information about the fields in this screen.

4

FIREWALL

This chapter describes the screens that display when you click **Firewall** in the toolbar.

4.1 FIREWALL OVERVIEW

This section describes some of the concepts related to the **Firewall** screens.

4.1.1 FIREWALL

The term “firewall” comes from a construction technique designed to prevent the spread of fire from one room to another. Similarly, your BVW-3653’s firewall prevents intrusion attempts and other undesirable activity originating from the WAN, keeping the computers on your LAN safe. You can also use filtering techniques to specify the computers and other devices you want to allow on the LAN, and prevent certain traffic from going from the LAN to the WAN.

4.1.2 INTRUSION DETECTION SYSTEM

An intrusion detection system monitors network activity, looking for policy violations, and malicious or suspicious activity. The BVW-3653’s intrusion detection system logs all such activity to the **Firewall > Local Logs** screen.

4.1.3 PING

The BVW-3653 allows you to use the ping utility on the LAN (in the **LAN > Debug** screen) and also on the WAN (in the **Firewall > Firewall Options** screen). For more information, see [Debugging \(Ping and Traceroute\)](#) on page 40.

4.1.4 MAC FILTERING

Every networking device has a unique Media Access Control (MAC) address that identifies it on the network. When you enable MAC address filtering on the BVW-3653’s firewall, you can set up a list of MAC addresses, and then specify whether you want to:

- ▶ Deny the devices on the list access to the BVW-3653 and the network (in which case all other devices can access the network)

or

- ▶ Allow the devices on the list to access the network (in which case no other devices can access the network)

4.1.5 IP FILTERING

IP filtering allows you to prevent computers on the LAN from sending certain types of data to the WAN. You can use this to prevent unwanted outgoing communications. Specify the IP address of the computer on the LAN from which you want to prevent communications, and specify the port range of the communications you want to prevent. The BVW-3653 discards outgoing data packets that match the criteria you specified.

4.1.6 PORT FORWARDING

Port forwarding allows a computer on your LAN to receive specific communications from the WAN. Typically, this is used to allow certain applications (such as gaming) through the firewall, for a specific computer on the LAN. Port forwarding is also commonly used for running a public HTTP server from a private network.

You can set up a port forwarding rule for each application for which you want to open ports in the firewall. When the BVW-3653 receives incoming traffic from the WAN with a destination port that matches a port forwarding rule, it forwards the traffic to the LAN IP address and port number specified in the port forwarding rule.

NOTE: For information on the ports you need to open for a particular application, consult that application's documentation.

4.1.7 PORT TRIGGERING

Port triggering is a means of automating port forwarding. The BVW-3653 scans outgoing traffic (from the LAN to the WAN) to see if any of the traffic's destination ports match those specified in the port triggering rules you configure. If any of the ports match, the BVW-3653 automatically opens the incoming ports specified in the rule, in anticipation of incoming traffic.

4.1.8 DMZ

In networking, the De-Militarized Zone (DMZ) is a part of your LAN that has been isolated from the rest of the LAN, and opened up to the WAN. The term comes from the military designation for a piece of territory, usually located between two opposing forces, that is isolated from both and occupied by neither.

4.2 THE FIREWALL OPTIONS SCREEN

Use this screen to turn firewall features on or off. You can enable or disable the BVW-3653's intrusion detection system, and allow or prevent responses to ICMP requests from the WAN.

Click **Firewall > Firewall Options**. The following screen displays.

FIGURE 15: The Firewall > Firewall Options Screen

Firewall Options	
Intrusion Detection System	<input type="checkbox"/> Disabled
Ping on WAN Interface	<input type="checkbox"/> Disabled

The following table describes the labels in this screen.

TABLE 15: The Firewall > Firewall Options Screen

Intrusion Detection System	<ul style="list-style-type: none"> ▶ Select this to turn the intrusion detection system off. ▶ Deselect this to turn the intrusion detection system on.
Ping on WAN Interface	<ul style="list-style-type: none"> ▶ Select this to prevent responses to ICMP requests originating from the WAN. ▶ Select this to allow responses to ICMP requests originating from the WAN.
Apply	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

4.3 THE MAC FILTERING SCREEN

Use this screen to configure Media Access Control (MAC) address filtering on the LAN.

NOTE: To configure MAC address filtering on the wireless network, see *The Access Control Screen* on page 78.

You can set the BVW-3653 to allow only certain devices to access the BVW-3653 and the network, or to deny certain devices access.

NOTE: To see a list of all the computers connected to the BVW-3653 on the LAN, click the **Connected Computers** button in the **Firewall > IP Filtering, Forwarding, Port Triggering** or **DMZ** screens.

Click **Firewall > MAC Filtering**. The following screen displays.

FIGURE 16: The Firewall > MAC Filtering Screen

Select the Mac Filter allows you to specify which computers to be blocked from accessing the Internet and your network.

Mac Filter Options		
The Mac Filter Table	Allow-All ▾	
Allow Table (up to 16 items)		
#	Device Name	
	MAC Address	
Delete		
Deny Table (up to 16 items)		
#	Device Name	
	MAC Address	
Delete		
Auto-Learned Lan Devices		
Device Name	MAC Address	Type
Manually-Added Lan Devices		
Device Name	MAC Address	Type
	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	<input type="radio"/> Allow <input type="radio"/> Deny
Add Cancel		
Apply Cancel Help		

The following table describes the labels in this screen.

TABLE 16: The Firewall > MAC Filtering Screen

MAC Filter Options	
The MAC Filter Table	Use this field to control whether the BVW-3653 performs MAC filtering. <ul style="list-style-type: none"> ▶ Select Allow-All to turn MAC filtering off. All devices may access the BVW-3653 and the network. ▶ Select Allow to permit only devices with the MAC addresses you set up in the Allow Table to access the BVW-3653 and the network. All other devices are denied access. ▶ Select Deny to permit all devices except those with the MAC addresses you set up in the Deny Table to access the BVW-3653 and the network. The specified devices are denied access.
Allow Table (up to 16 Items)	
#	This displays the index number assigned to the permitted device.

TABLE 16: The Firewall > MAC Filtering Screen (continued)



Device Name	This displays the name you gave to the permitted device.
MAC Address	This displays the MAC address of the permitted device.
Delete	Select a permitted device's radio button () and click this to remove the device from the list. The device may no longer access the BVW-3653 and the network. NOTE: Make sure you do not delete your management computer from the list; if you do so, you will need to log back in from another computer, or reset the BVW-3653.
Deny Table (up to 16 Items)	
Device Name	This displays the name you gave to the denied device.
MAC Address	This displays the MAC address of the denied device.
Delete	Select a denied device's radio button () and click this to remove the device from the list. The device may now access the BVW-3653 and the network.
Auto-Learned LAN Devices	
Device Name	This displays the name of each network device that has connected to the BVW-3653 on the LAN.
MAC Address	This displays the MAC address of each network device that has connected to the BVW-3653 on the LAN.
Type	Use this field to specify the list to which you want to add the device. ▶ Select Allow to add the device to the Allow Table . ▶ Select Deny to add the device to the Deny Table .
Manually-Added LAN Devices	
Device Name	Enter the name to associate with a network device that you want to permit or deny access to the BVW-3653 and the network. NOTE: This name is arbitrary, and does not affect functionality in any way.
MAC Address	Specify the MAC address of the network device that you want to permit or deny access to the BVW-3653 and the network.
Type	Use this field to specify the list to which you want to add the device. ▶ Select Allow to add the device to the Allow Table . ▶ Select Deny to add the device to the Deny Table .
Add	Click this to add the device to the list you specified.

TABLE 16: The Firewall > MAC Filtering Screen (continued)

Cancel	Click this to clear the Manually-Added LAN Devices fields.
Apply	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

4.4 THE IP FILTERING SCREEN

Use this screen to configure IP filtering. You can turn IP filtering on or off and configure new and existing IP filtering rules.

Click **Firewall > IP Filtering**. The following screen displays.

FIGURE 17: The Firewall > IP Filtering Screen

IP filtering is used to block certain outbound traffic which is destined to specific target port or port range from specific computers in the internal network. Traffic would be blocked according to the remote destination ports and the source IP addresses

IP Filtering Options

All IP Filtering rules Disabled

Select	#	Application Name	Port Range	Protocol	IP Address Range	Enable
<input type="button" value="add new"/> <input type="button" value="edit"/> <input type="button" value="delete"/>						

The following table describes the labels in this screen.

TABLE 17: The Firewall > IP Filtering Screen





All IP Filtering Rules	<p>Use this to turn IP filtering on or off.</p> <ul style="list-style-type: none"> ▶ Deselect the checkbox to enable IP filtering. ▶ Select the checkbox to disable IP filtering (default). <p>NOTE: You can add, edit or delete IP filtering rules only when this checkbox is deselected.</p>
Select	Select an IP filtering rule's radio button () before clicking Edit or Delete .
#	This displays the arbitrary identification number assigned to the IP filtering rule.
Application Name	This displays the arbitrary name you assigned to the rule when you create it.

TABLE 17: The Firewall > IP Filtering Screen (continued)

Port Range	This displays the start and end values of the ports to which communications from the specified IP addresses is not permitted.
Protocol	This displays the type of communications that are not permitted: <ul style="list-style-type: none"> ▶ TCP displays if communications via the Transmission Control Protocol are not permitted. ▶ UDP displays if communications via the User Datagram Protocol are not permitted. ▶ TCP/UDP displays if communications via the Transmission Control Protocol and the User Datagram Protocol are not permitted.
IP Address Range	This displays the start and end IP address from which communications to the specified ports are not permitted.
Enable	Use this field to turn each IP filtering rule on or off. <ul style="list-style-type: none"> ▶ Select this checkbox to enable the IP filtering rule. ▶ Deselect this checkbox to disable the IP filtering rule.
Add New	Click this to define a new IP filtering rule. See Adding or Editing an IP Filtering Rule on page 51 for information on the screen that displays.
Edit	Select an IP filtering rule's radio button () and click this to make changes to the rule. See Adding or Editing an IP Filtering Rule on page 51 for information on the screen that displays.
Delete	Select an IP filtering rule's radio button () and click this to remove the rule. The deleted rule's information cannot be retrieved.
Apply	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

4.4.1 ADDING OR EDITING AN IP FILTERING RULE

- ▶ To add a new IP filtering rule, click **Add** in the **Firewall > IP Filtering** screen.
- ▶ To edit an existing IP filtering rule, select the rule's radio button () in the **Firewall > IP Filtering** screen and click the **Edit** button.

The following screen displays.

FIGURE 18: The Firewall > IP Filtering > Add/Edit Screen

The following table describes the labels in this screen.

TABLE 18: The Firewall > IP Filtering > Add/Edit Screen

Application Name	Enter a name for the application that you want to block. NOTE: This name is arbitrary, and does not affect functionality in any way.
Port Range	Use these fields to specify the target port range to which communication should be blocked. Enter the start port number in the first field, and the end port number in the second field. To specify only a single port, enter its number in both fields.
Protocol	Use this field to specify whether the BVW-3653 should block communication via: <ul style="list-style-type: none"> ▶ Transmission Control Protocol (TCP) ▶ User Datagram Protocol (UDP) ▶ Both TCP and UDP. NOTE: If in doubt, leave this field at its default (Both).
IP Address Range	Use these fields to specify the range of local computers' IP addresses from which communications should be blocked. Enter the start IP address in the first field, and the end IP address in the second. To specify only a single IP address, enter it in both fields.
Connected Computers	Click this to see a list of the computers currently connected to the BVW-3653 on the LAN.
Back	Click this to return to the Firewall > IP filtering screen without saving your changes to the IP filtering rule.
Apply	Click this to save your changes to the fields in this screen.

TABLE 18: The Firewall > IP Filtering > Add/Edit Screen

Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

4.5 THE FORWARDING SCREEN

Use this screen to configure port forwarding between computers on the WAN and computers on the LAN. You can turn port forwarding on or off and configure new and existing port forwarding rules.

Click **Firewall > Forwarding**. The following screen displays.

FIGURE 19: The Firewall > Forwarding Screen

Forwarding is used to redirect the inbound traffic to the appropriate server(s) or specifically identified application(s) in the internal network. In the setting, the public ports are the target ports seen by the Internet world and the private ports are the target ports in the inside hosts to be translated by the device. The IP addresses are the hosts which host these private ports

Port Forwarding Options

All Port Forwarding rules Disabled

Select	#	Application Name	Port Range		Protocol	IP Address	Enable
			Public	Private			
<input type="button" value="add new"/> <input type="button" value="edit"/> <input type="button" value="delete"/>							

The following table describes the labels in this screen.

TABLE 19: The Firewall > Forwarding Screen




All Port Forwarding Rules	Use this field to turn port forwarding on or off. ▲ Select the checkbox to enable port forwarding. ▲ Deselect the checkbox to disable port forwarding.
Select	Select a port forwarding rule's radio button () before clicking Edit or Delete .
#	This displays the arbitrary identification number assigned to the port forwarding rule.
Application Name	This displays the arbitrary name you assigned to the rule when you created it.

TABLE 19: The Firewall > Forwarding Screen (continued)

Port Range	<p>These fields display the ports to which the rule applies:</p> <ul style="list-style-type: none"> ▶ The Public field displays the incoming port range. These are the ports on which the BVW-3653 received traffic from the originating host on the WAN. ▶ The Private field displays the port range to which the BVW-3653 forwards traffic to the device on the LAN.
Protocol	<p>This field displays the protocol or protocols to which this rule applies:</p> <ul style="list-style-type: none"> ▶ Transmission Control Protocol (TCP) ▶ User Datagram Protocol (UDP) ▶ Transmission Control Protocol and User Datagram Protocol (TCP/UDP) ▶ Generic Routing Encapsulation (GRE) ▶ Encapsulating Security Protocol (ESP)
IP Address	<p>This displays the IP address of the computer on the LAN to which traffic conforming to the Public Port Range and Protocol conditions is forwarded.</p>
Enable	<p>Use this field to turn each port forwarding rule on or off.</p> <ul style="list-style-type: none"> ▶ Select this checkbox to enable the port forwarding rule. ▶ Deselect this checkbox to disable the port forwarding rule.
Add New	<p>Click this to define a new port forwarding rule. See Adding or Editing a Port Forwarding Rule on page 55 for information on the screen that displays.</p>
Edit	<p>Select a port forwarding rule's radio button () and click this to make changes to the rule. See Adding or Editing a Port Forwarding Rule on page 55 for information on the screen that displays.</p>
Delete	<p>Select a port forwarding rule's radio button () and click this to remove the rule. The deleted rule's information cannot be retrieved.</p>
Apply	<p>Click this to save your changes to the fields in this screen.</p>
Cancel	<p>Click this to return the fields in this screen to their last-saved values without saving your changes.</p>
Help	<p>Click this to see information about the fields in this screen.</p>

4.5.1 ADDING OR EDITING A PORT FORWARDING RULE

- ▶ To add a new port forwarding rule, click **Add** in the **Firewall > Forwarding** screen.
- ▶ To edit an existing port forwarding rule, select the rule's radio button (☒) in the **Firewall > Forwarding** screen and click the **Edit** button.

The following screen displays.

FIGURE 20: The Firewall > Forwarding > Add/Edit Screen

The following table describes the labels in this screen.

TABLE 20: The Firewall > Forwarding > Add/Edit Screen

Application Name	Enter a name for the application for which you want to create the rule. NOTE: This name is arbitrary, and does not affect functionality in any way.
Public Port Range	Use these fields to specify the incoming port range. These are the ports on which the BVW-3653 received traffic from the originating host on the WAN. Enter the start port number in the first field, and the end port number in the second field. To specify only a single port, enter its number in both fields.
Private Port Range	Use these fields to specify the ports to which the received traffic should be forwarded. Enter the start port number in the first field. The number of ports must match that specified in the Public Port Range , so the BVW-3653 completes the second field automatically.

TABLE 20: The Firewall > Forwarding > Add/Edit Screen

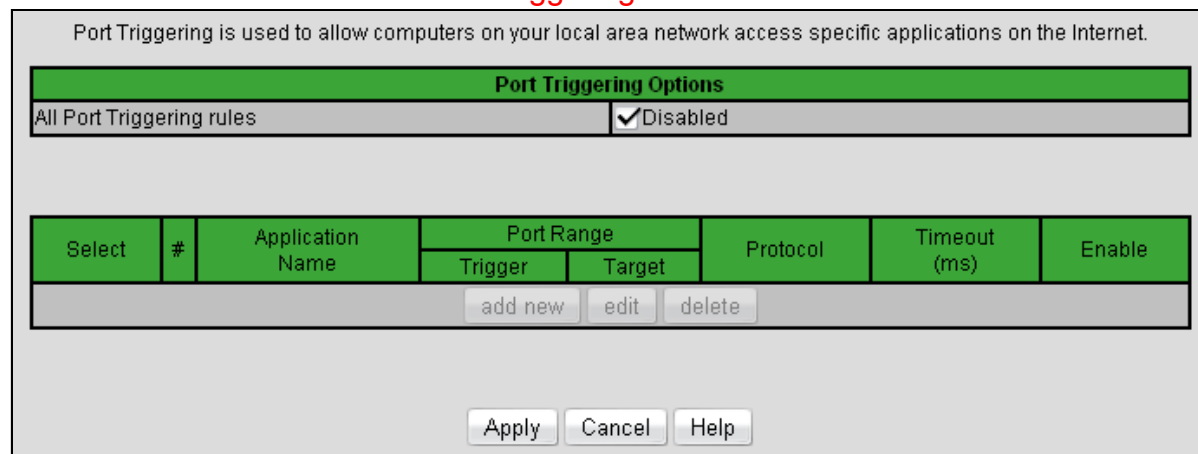
Protocol	Use this field to specify whether the BVW-3653 should forward traffic via: <ul style="list-style-type: none"> ▶ Transmission Control Protocol (TCP) ▶ User Datagram Protocol (UDP) ▶ Transmission Control Protocol and User Datagram Protocol (TCP/UDP) ▶ Generic Routing Encapsulation (GRE) ▶ Encapsulating Security Protocol (ESP) <p>NOTE: If in doubt, leave this field at its default (TCP/UDP).</p>
IP Address	Use this field to enter the IP address of the computer on the LAN to which you want to forward the traffic.
Connected Computers	Click this to see a list of the computers currently connected to the BVW-3653 on the LAN.
Back	Click this to return to the Firewall > Forwarding screen without saving your changes to the port forwarding rule.
Apply	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

4.6 THE PORT TRIGGERING SCREEN

Use this screen to configure port triggering. You can turn port triggering on or off and configure new and existing port triggering rules.

Click **Firewall > Port Triggering**. The following screen displays.

FIGURE 21: The Firewall > Port Triggering Screen



The following table describes the labels in this screen.

TABLE 21: The Firewall > Port Triggering Screen

All Port Triggering Rules	Use this field to turn port triggering on or off. <ul style="list-style-type: none"> ▶ Select the checkbox to enable port triggering. ▶ Deselect the checkbox to disable port triggering.
Select	Select a port triggering rule's radio button (☉) before clicking Edit or Delete .
#	This displays the arbitrary identification number assigned to the port triggering rule.
Application Name	This displays the arbitrary name you assigned to the rule when you created it.
Port Range	These fields display the ports to which the rule applies: <ul style="list-style-type: none"> ▶ The Trigger field displays the range of outgoing ports. When the BVW-3653 detects activity (outgoing traffic) on these ports from computers on the LAN, it automatically opens the Target ports. ▶ The Target field displays the range of triggered ports. These ports are opened automatically when the BVW-3653 detects activity on the Trigger ports from computers on the LAN.
Protocol	This displays the protocol of the port triggering rule.
Timeout (ms)	This displays the time (in milliseconds) after the BVW-3653 opens the Target ports that it should close them.
Enable	Use this field to turn each port triggering rule on or off. <ul style="list-style-type: none"> ▶ Select this checkbox to enable the port triggering rule. ▶ Deselect this checkbox to disable the port triggering rule.

TABLE 21: The Firewall > Port Triggering Screen

Add New	Click this to define a new port triggering rule. See Adding or Editing a Port Triggering Rule on page 58 for information on the screen that displays.
Edit	Select a port triggering rule's radio button (☑) and click this to make changes to the rule. See Adding or Editing a Port Triggering Rule on page 58 for information on the screen that displays.
Delete	Select a port triggering rule's radio button (☑) and click this to remove the rule. The deleted rule's information cannot be retrieved.
Apply	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

4.6.1 ADDING OR EDITING A PORT TRIGGERING RULE

- ▶ To add a new port triggering rule, click **Add** in the **Firewall > Port Triggering** screen.
- ▶ To edit an existing port triggering rule, select the rule's radio button (☑) in the **Firewall > Port Triggering** screen and click the **Edit** button.

The following screen displays.

FIGURE 22: The Firewall > Port Triggering > Add/Edit Screen

Port Triggering Add/Edit	
Application Name	<input type="text"/>
Trigger Port Range	<input type="text"/> ~ <input type="text"/>
Target Port Range	<input type="text"/> ~ <input type="text"/>
Protocol	Both ▾
Timeout (ms)	<input type="text"/>
<input type="button" value="Back"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>	

The following table describes the labels in this screen.

TABLE 22: The Firewall > Port Triggering > Add/Edit Screen

Application Name	<p>Enter a name for the application for which you want to create the rule.</p> <p>NOTE: This name is arbitrary, and does not affect functionality in any way.</p>
Trigger Port Range	<p>Use these fields to specify the trigger ports. When the BVW-3653 detects activity on any of these ports originating from a computer on the LAN, it automatically opens the Target ports in expectation of incoming traffic. Enter the start port number in the first field, and the end port number in the second field.</p> <p>To specify only a single port, enter its number in both fields.</p>
Target Port Range	<p>Use these fields to specify the target ports. The BVW-3653 opens these ports in expectation of incoming traffic whenever it detects activity on any of the Trigger ports. The incoming traffic is forwarded to these ports on the computer connected to the LAN.</p> <p>Enter the start port number in the first field, and the end port number in the second field.</p> <p>To specify only a single port, enter its number in both fields.</p>
Protocol	<p>Use this field to specify whether the BVW-3653 should activate this trigger when it detects activity via:</p> <ul style="list-style-type: none"> ▶ Transmission Control Protocol (TCP) ▶ User Datagram Protocol (UDP) ▶ Transmission Control Protocol and User Datagram Protocol (Both) <p>NOTE: If in doubt, leave this field at its default (Both).</p>
Timeout (ms)	<p>Enter the time (in milliseconds) after the BVW-3653 opens the Target ports that it should close them.</p>
Connected Computers	<p>Click this to see a list of the computers currently connected to the BVW-3653 on the LAN.</p>
Back	<p>Click this to return to the Firewall > Forwarding screen without saving your changes to the port forwarding rule.</p>
Apply	<p>Click this to save your changes to the fields in this screen.</p>
Cancel	<p>Click this to return the fields in this screen to their last-saved values without saving your changes.</p>
Help	<p>Click this to see information about the fields in this screen.</p>

4.7 THE DMZ SETTING SCREEN

Use this screen to configure your network's Demilitarized Zone (DMZ).

NOTE: Only one device can be on the DMZ at a time.

Click **Firewall > DMZ Setting**. The following screen displays.

FIGURE 23: The Firewall > DMZ Setting Screen

The following table describes the labels in this screen.

TABLE 23: The Firewall > DMZ Setting Screen

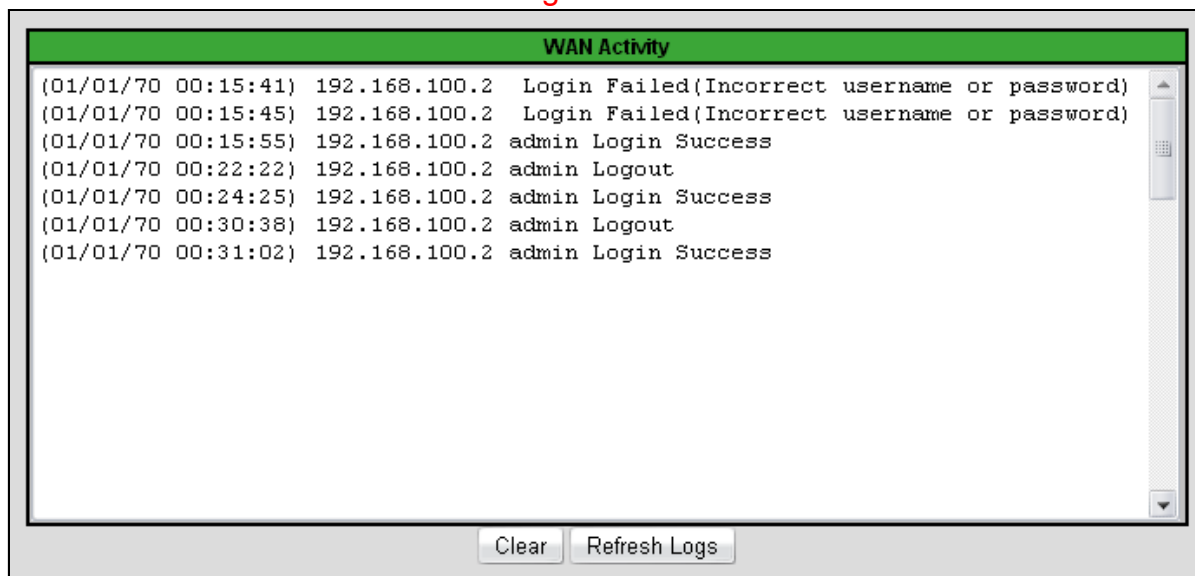
Enable DMZ Host	Use this field to turn the DMZ on or off. <ul style="list-style-type: none"> ▶ Select the checkbox to enable the DMZ. ▶ Deselect the checkbox to disable the DMZ. Computers that were previously in the DMZ are now on the LAN.
Connected Computers	Click this to see a list of the computers currently connected to the BVW-3653 on the LAN.
IP Address	Enter the IP address of the computer that you want to add to the DMZ.
Apply	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

4.8 THE LOCAL LOGS SCREEN

Use this screen to see information about firewall activity.

Click **Firewall > Local Logs**. The following screen displays.

FIGURE 24: The Firewall > Local Logs Screen



The following table describes the labels in this screen.

TABLE 24: The Firewall > Local Logs Screen

WAN Activity	This field displays information about firewall events in the following format: <ul style="list-style-type: none"> ▶ Date (DD/MM/YY) ▶ Time (HH:MM:SS) ▶ IP Address ▶ Event type
Clear	Click this to remove the log events. Deleted information cannot be retrieved.
Refresh Logs	Click this to reload the information in the WAN Activity list. Events that have occurred since you last refreshed the list display.

5

PARENTAL CONTROL

This chapter describes the screens that display when you click **Parent Control** in the toolbar.

5.1 PARENTAL CONTROL OVERVIEW

This section describes some of the concepts related to the **Parent Control** screens.

5.1.1 WEBSITE BLOCKING

The **Parent Control** screens allow you to block access from computers on the LAN to certain websites, or websites whose URLs (website addresses) contain the keywords you specify.

You can also specify “trusted” computers, which should be exempted from website blocking, and you can schedule website blocking so that it is only in effect at certain times (evenings and weekends, for example).

5.2 THE WEB SITE BLOCKING SCREEN

Use this screen to block access from the LAN to certain websites. You can also specify trusted computers, which are not subject to the blocking filter.

NOTE: To apply the blocking filter only at certain times, use the **Parent Control > Scheduling** screen.

Click **Parent Control > Web Site Blocking**. The following screen displays.

FIGURE 25: The Parent Control > Web Site Blocking Screen

Website blocking is used to restrict access to certain websites. You can block websites based on a keyword or specific website addresses. If you enter in a keyword, for instance "example", you would block many web sites that contain the word "example" in the address. These blocked sites would include "www.example.com", "www.example.net", and "www.example.org". If you enter a full web address - for instance, "www.exampleonline.com", you will only block this address.

Web Site Blocking Options	
Enable Web Site Blocking	<input type="checkbox"/> Enabled
New Key Word/URL Blocking	<input type="text"/> <input type="button" value="Add"/>
Blocked Key Words/URLs	<div style="border: 1px solid gray; height: 100px;"></div> <input type="button" value="Remove"/> <input type="button" value="Clear List"/>

Trusted Computers	
New Computer MAC Address	<input type="text"/> <input type="button" value="Add"/>
Trusted Computer List	<div style="border: 1px solid gray; height: 100px;"></div> <input type="button" value="connected computers"/> <input type="button" value="Remove"/> <input type="button" value="Clear List"/>

The following table describes the labels in this screen.

TABLE 25: The Parent Control > Web Site Blocking Screen

Web Site Blocking Options	
Enable Web Site Blocking	Use this field to turn web site blocking on or off. <ul style="list-style-type: none"> ▶ Select the checkbox to enable web site blocking. ▶ Deselect the checkbox to disable web site blocking.
New Key Word/URL Blocking	Use these fields to configure the websites to which users on the LAN are denied access: <ul style="list-style-type: none"> ▶ Enter a URL (for example, "www.example.com") to block access to that website only. ▶ Enter a keyword (for example, "example") to block access to all websites that contain the keyword in their URL (for example, "www.example.com", "www.example.org", "www.someotherwebsite.com/example" and so forth). Click Add to add the URL or keyword to the Blocked Key Words/URLs list.

TABLE 25: The Parent Control > Web Site Blocking Screen (continued)

Blocked Key Words/ URLs	This displays the list of websites and keywords to which users on the LAN are denied access. ▶ Select a URL or keyword and click Remove to delete it from the list. ▶ Click Clear List to delete all the URLs and keywords from the list.
Trusted Computers	
New Computer MAC Address	Enter a computer's Media Access Control (MAC) address and click Add to include it in the trusted computer list.
Trusted Computer List	This displays a list of the computers which are exempt from the website blocking filter, identified by their MAC addresses.
Connected Computers	Click this to see a list of the computers that are currently connected to the BVW-3653.
Remove	Select a computer's MAC address from the Connected Computers list and click this to delete it from the list.
Clear List	Click this to delete all the computers' MAC addresses from the list.
Apply	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

5.3 THE SCHEDULING SCREEN

Use this screen to control when the website blocking filter should be in effect.

NOTE: To configure the website blocking filter, use the **Parent Control > Web Site Blocking** screen.

Click **Parent Control > Scheduling**. The following screen displays.

FIGURE 26: The Parent Control > Scheduling Screen

Web Site Blocking Schedule allows you to apply your Web Site Blocking rules at different times of the day or week.

Days of the week	
Please select the days that you wish to apply Web Site Blocking settings to	
Everyday	<input checked="" type="checkbox"/>
Monday	<input checked="" type="checkbox"/>
Tuesday	<input checked="" type="checkbox"/>
Wednesday	<input checked="" type="checkbox"/>
Thursday	<input checked="" type="checkbox"/>
Friday	<input checked="" type="checkbox"/>
Saturday	<input checked="" type="checkbox"/>
Sunday	<input checked="" type="checkbox"/>

Time of the day	
Please select the hours of the day that you wish to apply Web Site Blocking settings to	
All Day	<input checked="" type="checkbox"/> Enabled

	Hour	Minute	
Start	12	0	AM ▾
End	12	0	AM ▾

The following table describes the labels in this screen.

TABLE 26: The Parent Control > Scheduling Screen

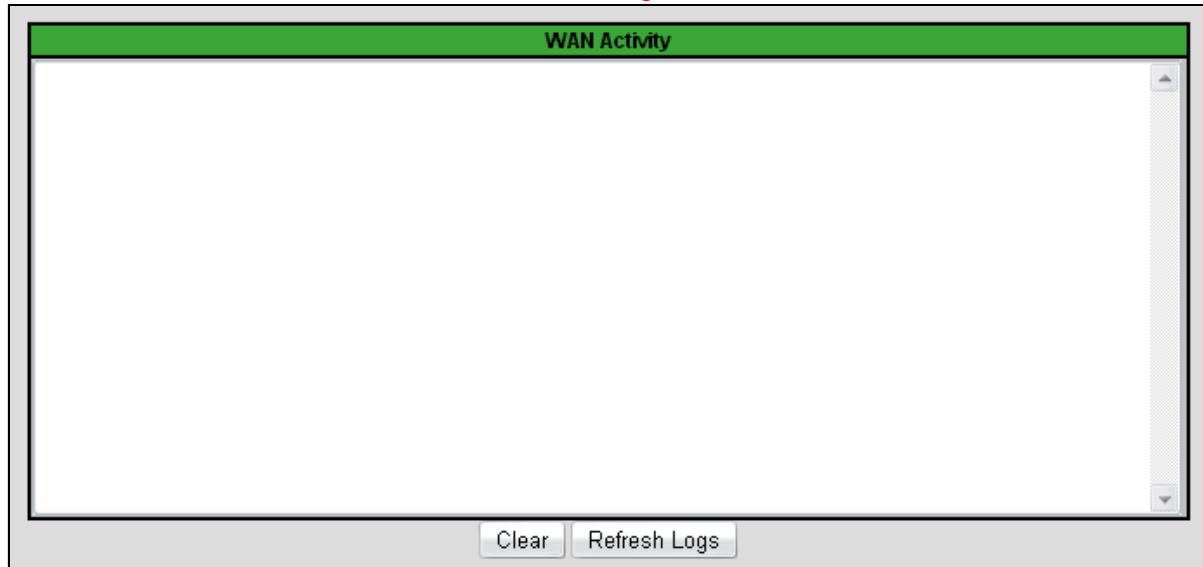
Days of the Week	Select the days of the week on which you want the website blocking filter to be in effect.
Time of Day	Use these fields to control the time that the website blocking filter should be in effect: <ul style="list-style-type: none"> ▶ Select All Day to apply the website blocking filter at all times. ▶ To apply the website blocking filter only at certain times of day, deselect All Day. Use the Start fields to define the time that the filter should come into effect, and use the End fields to define the time that the filter should cease being in effect.
Apply	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

5.4 THE LOCAL LOGS SCREEN

Use this screen to see information about events that have triggered the website blocking filter.

Click **Parent Control > Local Logs**. The following screen displays.

FIGURE 27: The Parent Control > Local Logs Screen



The following table describes the labels in this screen.

TABLE 27: The Parental Control > Local Logs Screen

WAN Activity	This field displays information about website blocking filter events in the following format: <ul style="list-style-type: none"> ▶ Date (DD/MM/YY) ▶ Time (HH:MM:SS) ▶ IP Address ▶ Event type
Clear	Click this to remove the log events. Deleted information cannot be retrieved.
Refresh Logs	Click this to reload the information in the WAN Activity list. Events that have occurred since you last refreshed the list display.

6

WIRELESS

This chapter describes the screens that display when you click **Wireless** in the toolbar.

6.1 WIRELESS OVERVIEW

This section describes some of the concepts related to the **Wireless** screens.

6.1.1 WIRELESS NETWORKING BASICS

Your BVW-3653's wireless network is part of the Local Area Network (LAN), known as the Wireless LAN (WLAN). The WLAN is a network of radio links between the BVW-3653 and the other computers and devices that connect to it.

6.1.2 ARCHITECTURE

The wireless network consists of two types of device: access points (APs) and clients.

- ▶ The access point controls the network, providing a wireless connection to each client.
- ▶ The wireless clients connect to the access point in order to receive a wireless connection to the WAN and the wired LAN.

The BVW-3653 is the access point, and the computers you connect to the BVW-3653 are the wireless clients.

6.1.3 WIRELESS STANDARDS

The way in which wireless devices communicate with one another is standardized by the Institute of Electrical and Electronics Engineers (IEEE). The IEEE standards pertaining to wireless LANs are identified by their 802.11 designation. There are a variety of WLAN standards, but the BVW-3653 supports the following (in order of adoption - old to new - and data transfer speeds - low to high):

- ▶ IEEE 802.11b
- ▶ IEEE 802.11g

- ▶ IEEE 802.11n

6.1.4 SERVICE SETS AND SSIDS

Each wireless network, including all the devices that comprise it, is known as a Service Set.

NOTE: Depending on its capabilities and configuration, a single wireless access point may control multiple Service Sets; this is often done to provide different service or security levels to different clients.

Each Service Set is identified by a Service Set Identifier (SSID). This is the name of the network. Wireless clients must know the SSID in order to be able to connect to the AP. You can configure the BVW-3653 to broadcast the SSID (in which case, any client who scans the airwaves can discover the SSID), or to “hide” the SSID (in which case it is not broadcast, and only users who already know the SSID can connect).

6.1.5 WIRELESS SECURITY

Radio is inherently an insecure medium, since it can be intercepted by anybody in the coverage area with a radio receiver. Therefore, a variety of techniques exist to control authentication (identifying who should be allowed to join the network) and encryption (signal scrambling so that only authenticated users can decode the transmitted data). The sophistication of each security method varies, as does its effectiveness. The BVW-3653 supports the following wireless security protocols (in order of effectiveness):

- ▶ **WEP** (the Wired Equivalency Protocol): this protocol uses a series of “keys” or data strings to authenticate the wireless client with the AP, and to encrypt data sent over the wireless link. WEP is a deprecated protocol, and should only be used when it is the only security standard supported by the wireless clients. WEP provides only a nominal level of security, since widely-available software exists that can break it in a matter of minutes.
- ▶ **WPA-PSK** (WiFi Protected Access - Pre-Shared Key): WPA was created to solve the inadequacies of WEP. There are two types of WPA: the “enterprise” version (known simply as WPA) requires the use of a central authentication database server, whereas the “personal” version (supported by the BVW-3653) allows users to authenticate using a “pre-shared key” or password instead. While WPA provides good security, it is still vulnerable to “brute force” password-guessing attempts (in which an attacker simply barrages the AP with join requests using different passwords), so for optimal security it is advised that you use a random password of thirteen characters or more, containing no “dictionary” words.
- ▶ **WPA2-PSK:** WPA2 is an improvement on WPA. The primary difference is that WPA uses the Temporal Key Integrity Protocol (TKIP) encryption standard (which has been shown to have certain possible weaknesses), whereas WPA2 uses the stronger Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP),

which has received the US government's seal of approval for communications up to the Top Secret security level. Since WPA2-PSK uses the same pre-shared key mechanism as WPA-PSK, the same caveat against using insecure or simple passwords applies.

6.1.5.1 WPS

WiFi-Protected Setup (WPS) is a standardized method of allowing wireless devices to quickly and easily join wireless networks, while maintaining a good level of security. The BVW-3653 provides two methods of WPS authentication:

- ▶ **Push-Button Configuration (PBC):** when the user presses the **PBC** button on the AP (either a physical button, or a virtual button in the GUI), any user of a wireless client that supports WPS can press the corresponding **PBC** button on the client within two minutes to join the network.
- ▶ **Personal Identification Number (PIN) Configuration:** all WPS-capable devices possess a PIN (usually to be found printed on a sticker on the device's housing). When you configure another device to use the same PIN, the two devices authenticate with one another.

Once authenticated, devices that have joined a network via WPS use the WPA2 security standard.

6.1.6 WMM

WiFi MultiMedia (WMM) is a Quality of Service (QoS) enhancement that allows prioritization of certain types of data over the wireless network. WMM provides four data type classifications (in priority order; highest to lowest):

- ▶ Voice
- ▶ Video
- ▶ Best effort
- ▶ Background

If you wish to improve the performance of voice and video (at the expense of other, less time-sensitive applications such as Internet browsing and FTP transfers), you can enable WMM. You can also edit the WMM QoS parameters, but are disadvised to do so unless you have an extremely good reason to make the changes.

6.2 THE BASIC SCREEN

Use this screen to configure your BVW-3653's basic wireless settings. You can turn the wireless module on or off, select the wireless mode and channel, run WPS and configure the wireless network's SSID.

Click **Wireless > Basic**. The following screen displays.

FIGURE 28: The Wireless > Basic Screen

Wireless Basic Settings				
Wireless ON/OFF	ENABLE ▾			
Wireless Mode	11B/G/N Mixed ▾			
Channel	auto ▾			
Run WPS	PBC PIN			
SSID setting	SSID name	hidden	in-service	WMM Mode
Primary SSID	Hitron-6430	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>				

The following table describes the labels in this screen.

TABLE 28: The Wireless > Basic Screen

Wireless Basic Settings	
Wireless ON/OFF	<p>Use this field to turn the wireless network on or off.</p> <ul style="list-style-type: none"> ▶ Select ENABLE to turn the wireless network on. ▶ Deselect DISABLE to turn the wireless network off.
Wireless Mode	<p>Select the type of wireless network that you want to use:</p> <ul style="list-style-type: none"> ▶ 11B/G Mixed: use IEEE 802.11b and 802.11n ▶ 11B Only: use IEEE 802.11b ▶ 11G Only: use IEEE 802.11g ▶ 11N Only: use IEEE 802.11n ▶ 11G/N Mixed: use IEEE 802.11g and 802.11N ▶ 11B/G/N Mixed: use IEEE 802.11b, 802.11g and 802.11N <p>NOTE: Only wireless clients that support the network protocol you select can connect to the wireless network. If in doubt, use 11B/G/N (default).</p>
Channel	<p>Select the wireless channel that you want to use, or select Auto to have the BVW-3653 select the optimum channel to use.</p> <p>NOTE: Use the Auto setting unless you have a specific reason to do otherwise.</p>

TABLE 28: The Wireless > Basic Screen (continued)

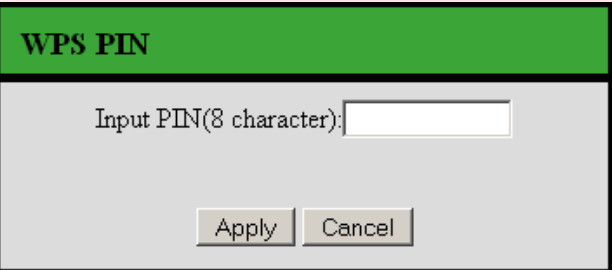
<p>Run WPS</p>	<p>Use these buttons to run Wifi Protected Setup (WPS):</p> <ul style="list-style-type: none"> ▶ Click the PBC button to begin the Push-Button Configuration process. You must then press the PBC button on your client wireless devices within two minutes in order to register them on your wireless network. ▶ Click the PIN button to begin the PIN configuration process. In the screen that displays, enter the WPS PIN that you want to use for the BVW-3653, or the WPS PIN of the client device you want to add to the network. <p>FIGURE 29: WPS PIN</p> 
<p>SSID Setting</p>	<p>This displays Primary SSID.</p> <p>NOTE: You may have additional BSSIDs, depending on your contract with your service provider.</p>
<p>SSID Name</p>	<p>Enter the name that you want to use for your wireless network. This is the name that identifies your network, and to which wireless clients connect.</p> <p>NOTE: It is suggested that you change the SSID from its default, for security reasons.</p>
<p>Hidden</p>	<p>Use this field to make your network visible or invisible to other wireless devices.</p> <ul style="list-style-type: none"> ▶ Select the checkbox if you do not want the BVW-3653 to broadcast the network name (SSID) to all wireless devices in the coverage area. Anyone who wants to connect to the network must know the SSID. ▶ Deselect the checkbox if you want your network name (SSID) to be public. Anyone with a wireless device in the coverage area can discover the SSID, and attempt to connect to the network.

TABLE 28: The Wireless > Basic Screen (continued)

In Service	<p>This field controls whether or not the SSID is in operation.</p> <p>NOTE: At the time of writing, this field is not user-configurable.</p>
WMM Mode	<p>Select the checkbox if you want to apply Wifi MultiMedia (WMM) Quality of Service (QoS) settings to this SSID.</p> <p>NOTE: Configure WMM settings in the Wireless > Advanced screen.</p>

6.3 THE SECURITY SCREEN

Use this screen to configure authentication and encryption on your wireless network.

NOTE: It is strongly recommended that you set up security on your network; otherwise, anyone in the radio coverage area can access your network.

Click **Wireless > Security**. The following screen displays.

FIGURE 30: The Wireless > Security Screen

Wireless Security	
SSID	Hitron-6430 ▾
Security Mode	WPA-Personal ▾

Wep Settings	
WEP Key Length	64 bit (10 hex digits) ▾ (length applies to all keys)
WEP Key 1	0000000000
WEP Key 2	0000000000
WEP Key 3	0000000000
WEP Key 4	0000000000
Default WEP Key	WEP Key 1 ▾
Authentication	Open System ▾

WPA_Personal	
WPA Mode	Auto (WPA-PSK or WPA2-PSK) ▾
Cipher type	AES ▾
Group Key Update Interval	3600 (seconds)
Pre-shared Key	defaultkey
Pre-Authentication	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

The following table describes the labels in this screen.

TABLE 29: The Wireless > Security Screen

Wireless Security	
SSID	Select the SSID for which you want to configure security. NOTE: At the time of writing, only one SSID is available.

TABLE 29: The Wireless > Security Screen (continued)

Security Mode	<p>Select the type of security that you want to use.</p> <ul style="list-style-type: none"> ▶ Select None to use no security. Anyone in the coverage area can enter your network. ▶ Select WEP to use the Wired Equivalent Privacy security protocol. ▶ Select WPA-Personal to use the WiFi Protected Access (Personal) security protocol. <p>NOTE: Due to inherent security vulnerabilities, it is suggested that you use WEP only if it is the only security protocol your wireless clients support. Under almost all circumstances, you should use WPA-Personal.</p>
<p>WEP Settings</p> <p>NOTE: These fields are only configurable when you select WEP from the Security Mode list.</p>	
WEP Key Length	<p>Use this field to specify the length of the security key used to allow wireless devices to join the network. The longer the key, the more secure it is.</p> <ul style="list-style-type: none"> ▶ Select 64-bit to use a ten-digit security key. ▶ Select 128-bit to use a twenty-six-digit security key.
WEP Key 1~4	<p>Use these fields to define the security keys that all wireless devices on the network must use to join the network.</p> <p>The BVW-3653 supports up to four WEP keys, of which you can select one as the default. You should input the same four keys, in the same order, in your network's wireless clients. Your BVW-3653 and your wireless clients can use different default keys, as long as all four keys are present and in the same order. If your wireless client supports only a single WEP key, use the BVW-3653's default key.</p> <p>Enter the keys in hexadecimal format (using the digits 0~9 and the letters A~F).</p>
Default WEP Key	<p>Select the number of the security key that you want the BVW-3653 to use as its default authentication key for transmissions.</p>

TABLE 29: The Wireless > Security Screen (continued)

Authentication	<p>Select the authentication mode that you want to use:</p> <ul style="list-style-type: none"> ▶ Select Open System to allow wireless clients to authenticate (identify themselves) to the BVW-3653 before presenting their security credentials (WEP keys). ▶ Select Shared Key to use the WEP key in the authentication process. When a client wants to associate, the BVW-3653 sends an unencrypted challenge message. The client must use the WEP key to encrypt the challenge message and return it to the BVW-3653, which then decrypts the message and compares the result with its original message. <p>Open System authentication is the more secure of the two authentication types, since while the Shared Key system appears more robust, it is possible to derive secure data by capturing the challenge messages.</p> <ul style="list-style-type: none"> ▶ Select Automatic to have the BVW-3653 choose the authentication method.
<p>WPA_Personal</p> <p>NOTE: These fields are only configurable when you select WPA-Personal from the Security Mode list.</p>	
WPA Mode	<p>Select the type of WPA security that you want to use:</p> <ul style="list-style-type: none"> ▶ Select WPA-PSK to use Wifi Protected Access (Pre-Shared Key) mode ▶ Select WPA2-PSK to use Wifi Protected Access 2 (Pre-Shared Key) mode ▶ Select Auto (WPA-PSK or WPA2-PSK) to allow clients operating in either mode to connect to the BVW-3653.
Cipher Type	<p>Select the type of encryption that you want to use:</p> <ul style="list-style-type: none"> ▶ Select TKIP to use the Temporal Key Integrity Protocol. ▶ Select AES to use the Advanced Encryption Standard. ▶ Select TKIP and AES to allow clients using either encryption type to connect to the BVW-3653.
Group Key Update Interval	<p>Enter the frequency (in seconds) with which you want the BVW-3653 to create new pre-shared keys, and issue them to the wireless client.</p>

TABLE 29: The Wireless > Security Screen (continued)

Pre-Shared Key	Enter the pre-shared key that you want to use for your wireless network. You will need to enter this key into your wireless clients in order to allow them to connect to the network.
Pre-Authentication	Use this field to allow pre-authentication (Enable) in WPA2, or deny pre-authentication requests (Disable). In preauthentication, a WPA2 wireless client can perform authentication with other wireless access points in its range when it is still connected to its current wireless access point. This allows mobile wireless clients to connect to new access points more quickly, permitting more efficient roaming.
Apply	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

6.4 THE ACCESS CONTROL SCREEN

Use this screen to configure Media Access Control (MAC) address filtering on the wireless network.

NOTE: To configure MAC address filtering on the wired LAN, see *The MAC Filtering Screen* on page 47.

You can set the BVW-3653 to allow only certain devices to access the BVW-3653 and the network wirelessly, or to deny certain devices access.

Click **Wireless > Access Control**. The following screen displays.


FIGURE 31: The Wireless > Access Control

The following table describes the labels in this screen.

TABLE 30: The Wireless > Access Control Screen

MAC Filtering	
SSID	Select the SSID for which you want to configure wireless access control. NOTE: At the time of writing, the BVW-3653 supports a single SSID.
MAC Filtering Mode	Use this field to control whether the BVW-3653 performs MAC filtering on the wireless network. <ul style="list-style-type: none"> ▶ Select Allow-All to turn MAC filtering off. All devices may access the BVW-3653 and the network wirelessly. ▶ Select Allow to permit only devices with the MAC addresses you set up in the Wireless Control List to access the BVW-3653 and the network wirelessly. All other devices are denied access. ▶ Select Deny to permit all devices except those with the MAC addresses you set up in the Wireless Control List to access the BVW-3653 and the network wirelessly. The specified devices are denied access.
Apply	Click this to save your changes in the MAC filtering section.
Wireless Control List (up to 16 Items)	

TABLE 30: The Wireless > Access Control Screen (continued)

# Index	This displays the index number assigned to the permitted or denied wireless device.
Device Name	This displays the name you gave to the permitted or denied wireless device.
MAC Address	This displays the MAC address of the permitted or denied wireless device.
Delete	Select a permitted or denied wireless device's radio button () and click this to remove the device from the list. The device may no longer access the BVW-3653 and the network.
Auto-Learned Wireless Devices	
Device Name	This displays the name of each network device that has connected to the BVW-3653 on the wireless network.
MAC Address	This displays the MAC address of each network device that has connected to the BVW-3653 on the wireless network.
Manually-Added Wireless Devices	
Device Name	Enter the name to associate with a network device that you want to permit or deny access to the BVW-3653 and the network wirelessly. NOTE: This name is arbitrary, and does not affect functionality in any way.
MAC Address	Specify the MAC address of the network device that you want to permit or deny access to the BVW-3653 and the network wirelessly.
Add	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

6.5 THE ADVANCED SCREEN

Click **Wireless > Advanced**. The following screen displays.

FIGURE 32: The Wireless > Advanced Screen

Wireless Advanced Settings	
BG Protection Mode	Always-Off ▾
IGMP Snooping	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
WMM Configuration	Configuration
HT Physical Mode	
Operating Mode	<input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field
Channel BandWidth	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40
Guard Interval	<input type="radio"/> long <input checked="" type="radio"/> short
MCS	Auto ▾
Reverse Direction Grant(RDG)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Extension Channel	2437MHz (Channel4) ▾
Aggregation MSDU(A-MSDU)	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Auto Block ACK	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Decline BA Request	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Other	
HT TxStream	2 ▾
HT RxStream	2 ▾
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>	

The following table describes the labels in this screen.

TABLE 31: The Wireless > Advanced Screen

Wireless Advanced Settings	
BG Protection Mode	<p>Use this field to configure IEEE 802.11b/g protection. Both 802.11b and 802.11g wireless communications occur at the same radio frequencies. When the BVW-3653 is wirelessly connected to 802.11b clients and 802.11g clients simultaneously, the performance of the link to 802.11g clients can deteriorate due to the presence of the 802.11b clients. Because 802.11b and 802.11g use different modulation techniques, 802.11b clients do not understand 802.11g's Request To Send (RTS) and Clear To Send (CTS) messages, which ensure that each wireless device transmits only when other devices are not transmitting.</p> <p>When B/G protection is active, the BVW-3653 prevents 802.11b clients transmitting over 802.11g transmissions by first transmitting an announcement (known as a CTS-to-Self) to 802.11b clients, stating that it intends to transmit to 802.11g clients.</p> <ul style="list-style-type: none"> ▶ Select Auto to have the BVW-3653 control whether B/G protection is active or not. ▶ Select Always-on to use B/G protection at all times. ▶ Select Always-off to never use B/G protection.
IGMP Snooping	<p>Use this field to turn Internet Group Management Protocol (IGMP) snooping on or off.</p> <p>IGMP is used to manage multicast groups. In multicast groups, data is transmitted to numerous IP addresses simultaneously. This is the most efficient method of providing the same data to many different recipients at the same time, since each data packet needs to be sent only once. Multicast groups are often used for Internet TV and real-time streaming applications such as online gaming.</p> <p>IGMP snooping allows the BVW-3653 to "snoop" or listen in on IGMP traffic, and to determine which computers on the LAN belong to which IGMP groups. By keeping lists of which computers belong to IGMP groups, the BVW-3653 can send the IGMP data to only those computers that have requested it, and can refrain from sending unsolicited multicast data. This can improve your connection to wireless clients.</p> <ul style="list-style-type: none"> ▶ Select Disable to turn IGMP snooping off. ▶ Select Enable to turn IGMP snooping on.

TABLE 31: The Wireless > Advanced Screen (continued)

WMM Configuration	<p>Click this to set up your Wifi Multimedia (WMM) Quality of Service (QoS) settings. See Configuring WMM Parameters on page 86 for information on the screen that displays.</p> <p>NOTE: Turn WMM on and off in the Wireless > Basic Settings screen.</p>
HT Physical Mode	
Operating Mode	<p>Use this field to configure how the BVW-3653 transmits in IEEE 802.11n mode.</p> <p>Greenfield mode, also known as High Throughput (HT) mode, assumes that there are no existing IEEE 802.11a/b/g stations using the same radio channel. In greenfield mode, the 802.11a/b/g stations are unable to tell when 802.11n transmissions are occurring. You should select this mode only if there are no 802.11a/b/g stations in your network (or other networks in your location). Otherwise these stations' wireless transmissions will interfere with your 802.11n transmissions. When no 802.11a/b/g stations are present, greenfield mode allows greater wireless network speeds, because the legacy messages (RTS, CTS and CTS-to-Self) do not need to be sent.</p> <p>Mixed mode, on the other hand, allows 802.11a/b/g stations to tell when 802.11n transmissions are occurring, by transmitting RTS, CTS and CTS-to-Self messages in a format the legacy stations can understand. You should select this option if you have 802.11a/b/g stations in your networks, or if there are other 802.11a/b/g networks in your area.</p>
Channel Bandwidth	<p>This field allows you to configure the width of the radio channel the BVW-3653 uses to communicate with its wireless clients (IEEE 802.11n only). Using the full 40MHz bandwidth can double your data speed.</p> <ul style="list-style-type: none"> ▶ Select 20 to only use a 20 megahertz band. ▶ Select 20/40 to use a 40 megahertz band when possible, and a 20 megahertz band when a 40MHz band is unavailable.

TABLE 31: The Wireless > Advanced Screen (continued)

Guard Interval	<p>In 802.11n networks, the guard interval is the amount of time that elapses between the transmission of symbols. This is to prevent Inter-Symbol Interference, or ISI, caused by echoes.</p> <p>NOTE: In modulated signals, each distinct modulated character (for example, each audible tone produced by a modem for transmission over telephone lines) is known as a symbol.</p> <ul style="list-style-type: none"> ▶ Select Long to use a long guard interval of 800 nanoseconds. ▶ Select Short to use a short guard interval of 400 nanoseconds.
MCS	<p>Use this field to configure the Modulation and Coding Scheme (MCS) that the BVW-3653 uses for IEEE 802.11n transmissions.</p> <p>The 802.11n protocol specifies 77 Modulation and Coding Schemes. Each MCS refers to a combination of a modulation technique, a coding rate, a guard interval, and a certain number of spatial streams. The BVW-3653 supports MCS 0~15, and 32.</p> <p>Select the MCS that you wish to use for 802.11n transmissions. If unsure, select Auto (default).</p>
Reverse Direction Grant (RDG)	<p>Use this field to configure Reverse Direction Grant in IEEE 802.11n transmissions.</p> <p>Each data transfer requires that the wireless station initiating the transfer acquires permission from the access point to perform the transfer. This is known as a transmission opportunity, or TXOP. Each TXOP is time-limited; the initiating station may transmit for only a certain length of time, and then must cease.</p> <p>Normally, if the receiving station wishes to return data to the initiating station, it must also acquire its own TXOP. However, when you enable Reverse Direction Grants, a wireless station that has already obtained a TXOP may issue a Reverse Direction Grant to the receiving station. This allows the receiving station to transmit data back to the initiating station for the remaining time specified in the original TXOP. It does not need to acquire its own TXOP.</p> <ul style="list-style-type: none"> ▶ Select Disable to disallow Reverse Direction Grants. ▶ Select Enable to allow Reverse Direction Grants.

TABLE 31: The Wireless > Advanced Screen (continued)

Extension Channel	<p>This field displays the secondary wireless radio channel that the BVW-3653 uses for channel bonding (combining two channels for faster data transfer) in IEEE 802.11n transmissions.</p> <p>NOTE: At the time of writing, you cannot select the Extension channel. It is selected automatically by the BVW-3653.</p>
Aggregation MSDU (A-MSDU)	<p>Use this field to control whether the BVW-3653 supports Aggregation MSDUs (A-MSDUs) in IEEE 802.11n transmissions.</p> <p>Each A-MSDU consists of multiple MSDUs, added together (aggregated) to create one large packet. This reduces the overhead associated with transmission, but can result in a reduced data rate if your network suffers from a high error rate since each lost A-MSDU will require retransmission.</p> <ul style="list-style-type: none"> ▶ Select Disable to not use A-MSDUs. ▶ Select Enable to use A-MSDUs.
Auto Block ACK	<p>Use this field to control how the BVW-3653 sends acknowledgement (ACK) requests in IEEE 802.11n transmissions.</p> <p>Normally, an ACK request is sent after every data or management frame in order to ensure that it has been received correctly. However, when you enable Auto Block ACK the BVW-3653 sends a burst of multiple frames together, and follows it with a single, block ACK request.</p> <ul style="list-style-type: none"> ▶ Select Disable to not use block ACKs. ▶ Select Enable to use block ACKs. <p>NOTE: Block ACK can increase your network's speed, as fewer ACK messages are sent. However, you should not use it if your network is prone to interference, since if the transmitting station needs to retransmit information, the required retransmission will be much longer.</p>
Decline BA Request	<p>Use this field to control how the BVW-3653 receives acknowledgement (ACK) requests in IEEE 802.11n transmissions.</p> <p>Select Disable to accept block ACK requests. The transmitting device may then send multiple data frames together, followed by the block ACK request.</p> <p>Select Enable to decline block ACK requests. The transmitting device must then follow each data frame with an ACK request in the traditional manner.</p>

TABLE 31: The Wireless > Advanced Screen (continued)

Other	
HT TxStream	Select the number of 802.11n radio transmitting channels (1 or 2) for High Throughput (HT) transmission.
HT RxStream	Select the number of 802.11n radio receiving channels (1 or 2) for High Throughput (HT) transmission.
Apply	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

6.5.1 CONFIGURING WMM PARAMETERS

To set up your BVW-3653's Wifi MultiMedia (WMM) Quality of Service (QoS) settings, click the **Configuration** button in the **Wireless > Advanced** screen. The following screen displays.

FIGURE 33: The Wireless > Advanced > WMM Configuration Screen

This page is used for WMM Configuration.

WMM Parameters of Access Point						
	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK	7	15	255	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI	1	7	15	94	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO	1	3	7	47	<input type="checkbox"/>	<input type="checkbox"/>

WMM Parameters of Station					
	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	255	0	<input type="checkbox"/>
AC_BK	7	15	255	0	<input type="checkbox"/>
AC_VI	2	7	15	94	<input type="checkbox"/>
AC_VO	2	3	7	47	<input type="checkbox"/>

NOTE: It is strongly recommended that you do not change the default values in this screen unless you have a good reason to do so.

The following table describes the labels in this screen.

TABLE 32: The Wireless > Advanced > WMM Configuration Screen

WMM Parameters of Access Point	
NOTE: This section controls the parameters of data transmitted from the BVW-3653 to the wireless clients.	
AC_BE	This row controls the Best Effort (BE) Access Category (AC)
AC_BK	This row controls the Background (BK) Access Category (AC)
AC_VI	This row controls the Video (VI) Access Category (AC)
AC_VO	This row controls the Voice (VO) Access Category (AC)
AIFSN	This column controls the Arbitration Inter-Frame Space Number for each Access Category. WMM gives the highest priority to the AC with the lowest AIFSN.
CWMin	This column controls the Contention Window Minimum for each Access Category. A smaller CWMin value increases priority for data of the relevant type. The contention window system is a mechanism for providing priority to important data on the wireless network. When a data collision occurs, each frame is assigned a random time to wait before attempting transmission again. This random time value is between zero and the data's CWMin value. If a collision occurs again, the time value is doubled, and transmission is attempted again. This continues until the time value reaches the CWMax value.
CWMax	This column controls the Contention Window Maximum for each Access Category. A smaller CWMin value decreases the access delay for data of the relevant type, but can result in more data collisions.
TXOP	This field defines the Transmission Opportunity (TXOP) length for each Access Category. This is the length of time during which the wireless device may to transmit over the wireless network, once it receives a transmission opportunity.
ACM	This field specifies whether Admission Control is Mandatory (ACM) for each Access Category. Select the checkbox to have the BVW-3653 control ACM.

TABLE 32: The Wireless > Advanced > WMM Configuration Screen

AckPolicy	<p>WMM defines two ACK policies: NormalAck and NoAck.</p> <ul style="list-style-type: none"> ▶ NormalAck: the recipient of a transmission acknowledges each received packet. ▶ NoAck: the recipient of a transmission does not acknowledge received packets. This can improve data throughput in situations where signal quality is excellent, but in other situations can cause a significant increase in lost packets. <p>Select the checkbox to use the NoAck policy.</p>
<p>WMM Parameters of Station</p> <p>NOTE: This section controls the parameters of data transmitted from the wireless clients to the BVW-3653.</p>	
AC_BE	This row controls the Best Effort (BE) Access Category (AC)
AC_BK	This row controls the Background (BK) Access Category (AC)
AC_VI	This row controls the Video (VI) Access Category (AC)
AC_VO	This row controls the Voice (VO) Access Category (AC)
AIFSN	This column controls the Arbitration Inter-Frame Space Number for each Access Category. WMM gives the highest priority to the AC with the lowest AIFSN.
CWMin	<p>This column controls the Contention Window Minimum for each Access Category. A smaller CWMin value increases priority for data of the relevant type.</p> <p>The contention window system is a mechanism for providing priority to important data on the wireless network. When a data collision occurs, each frame is assigned a random time to wait before attempting transmission again. This random time value is between zero and the data's CWMin value. If a collision occurs again, the time value is doubled, and transmission is attempted again. This continues until the time value reaches the CWMax value.</p>
CWMax	This column controls the Contention Window Maximum for each Access Category. A smaller CWMin value decreases the access delay for data of the relevant type, but can result in more data collisions.

TABLE 32: The Wireless > Advanced > WMM Configuration Screen

TXOP	This field defines the Transmission Opportunity (TXOP) length for each Access Category. This is the length of time during which the wireless device may to transmit over the wireless network, once it receives a transmission opportunity.
ACM	This field specifies whether Admission Control is Mandatory (ACM) for each Access Category. Select the checkbox to have the wireless client control ACM.

7

EMTA

This chapter describes the screens that display when you click **EMTA** in the toolbar. These screens display information about the BVW-3653's embedded Multimedia Terminal Adapter module.

NOTE: The fields in these screens are read-only, and are provided for troubleshooting purposes only.

7.1 THE STATUS SCREEN

Use this screen to see general information about the eMTA module.

Click **EMTA > Status**. The following screen displays.

FIGURE 34: The EMTA > Status Screen

This menu displays the eMTA general status	
Startup Procedure	
Telephony DHCP	[N/A]
Telephony Security	BASIC
Telephony TFTP	[Process...]
Telephony Call Server Registration	L1: [Fail]/L2:[Fail]
Telephony Registration Complete	[N/A]
SIP registration Status	
SIP registration timer	3600 s
MTA Line State	
Line1	[On-Hook]
Line2	[On-Hook]

The following table describes the labels in this screen.

TABLE 33: The EMTA > Status Screen

Startup Procedure	
Telephony DHCP	This field displays the status of the remote telephony DHCP server.
Telephony Security	This displays the type of security used for voice calls through the BVW-3653.

TABLE 33: The EMTA > Status Screen (continued)

Telephony TFTP	This field displays the status of the remote telephony TFTP server.
Telephony Call Server Registration	This field displays the status of the connection between each of the BVW-3653's phone lines and the remote call server.
Telephony Registration Complete	This field displays the overall status of voice call registration.
SIP Registration Status	
SIP Registration Timer	This field displays the number of seconds after which the BVW-3653 re-registers with the SIP (Session Initiation Protocol) server.
MTA Line State	
Line 1	These fields display the current status of each phone connected to the BVW-3653.
Line 2	

7.2 THE DHCP SCREEN

Use this screen to see information about the MTA module's connections to the service provider.

Click **EMTA > DHCP**. The following screen displays.

FIGURE 35: The EMTA > DHCP Screen

This menu displays the eMTA dhcp status	
Address information	
MTA MAC Address	00:05:CA:5F:64:31
MTA IP Address	0.0.0.0
Lease Parameters	
FQDN	
IP Address/Submask	0.0.0.0/[N/A]
Gateway	[N/A]
Bootfile	
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
Lease Timers	
Lease Time Remaining	D: 00 H: 00 M: 00 S: 07
Rebind Time Remaining	D: 00 H: 00 M: 00 S: 23
Renew Time Remaining	D: 00 H: 00 M: 00 S: 23
PacketCable DHCP option 122	
SNMP Entity (Sub-option 3)	
Kerberos Realm (Sub-option 6)	BASIC.1
Provisioning Timer (Sub-option 8)	[N/A]
© 2009 Hitron Technologies Inc.. All rights reserved.	

The following table describes the labels in this screen.

TABLE 34: The EMTA > DHCP Screen

Address Information	
MTA MAC Address	This field displays the Media Access Control (MAC) address of the Media Terminal Adapter (MTA) module.
MTA IP Address	This field displays the IP address of the MTA module.
Lease Parameters	
FQDN	This displays the Fully-Qualified Domain Name of the DHCP server from which the MTA module derives its IP address and subnet mask.
IP Address/Submask	This displays the MTA module's IP address and subnet mask, derived by DHCP.
Gateway	This displays the IP address of the MTA module's gateway on the WAN.
Bootfile	This displays the name of the file that controls the MTA module's boot process.
Primary DNS	This displays the IP address of the MTA module's primary Domain Name System (DNS) server.
Secondary DNS	This displays the IP address of the MTA module's secondary DNS server.
Lease Timers	
Lease Time Remaining	This displays the amount of time for which the MTA module's current DHCP lease is valid.
Rebind Time Remaining	This displays the amount of time until the MTA module attempts to obtain another IP address from another DHCP server, should lease renewal fail.
Renew Time Remaining	This displays the amount of time until the MTA module attempts to renew its DHCP lease with the current DHCP server.
Packet Cable DHCP Option 122	
NOTE: DHCP Option 122 is defined in RFC 3495.	
SNMP Entity (Sub-Option 3)	This displays the Telephony Service Provider's provisioning server address.
Kerberos Realm (Sub-Option 6)	This displays the TSP's Kerberos realm name.
Provisioning Timer (Sub-Option 8)	This displays the TSP's provisioning timer value.

7.3 THE QOS SCREEN

Click **EMTA > QoS**. The following screen displays.

FIGURE 36: The EMTA > QoS Screen

This menu displays the eMTA QoS and service flow status				
Error Codewords				
Unerrored Codewords			1	1 1
Correctable Codewords				
Uncorrectable Codewords	2010		45	43 45
Payload Header suppression				
PHS Status	OFF			
Service Flows				
SFID	Service Class Name	Direction	Primary Flow	Packets
Service Flow Failures				
Time	SFID	Failure Type		
Empty	Empty	Empty		

The following table describes the labels in this screen.

TABLE 35: The EMTA > QoS Screen

Error Codewords	
Unerrored Codewords	This displays information about the codewords received by the MTA module without error.
Correctable Codewords	This displays information about errored codewords received by the MTA and corrected.
Uncorrectable Codewords	This displays information about errored codewords received by the MTA that could not be corrected.
Payload Header Suppression	
PHS Status	This displays the status of Payload Header Suppression (PHS), also known as header compression and header suppression. PHS improves efficiency by removing redundant header information from voice data packets.
Service Flows	
SFID	This displays the DOCSIS Service Flow Identifier (SFID) for each current service flow. NOTE: Each connection requires two service flows: one for upstream traffic, the other for downstream.
Service Class Name	This displays the QoS profile name for each current service flow.
Direction	This displays whether the service flow carries upstream or downstream data.
Primary Flow	
Packets	This displays the number of packets that have been transmitted over each service flow.

TABLE 35: The EMTA > QoS Screen (continued)

Service Flow Failures	
Time	This displays the time at which the service flow failed.
SFID	This displays the Service Flow Identifier of each failed service flow.
Failure Type	This displays the cause of each service flow failure.

7.4 THE EVENT LOG SCREEN

Click **EMTA > Event Log**. The following screen displays.

FIGURE 37: The EMTA > Event Log Screen

This menu displays the eMTA log

Config file	
Config Filename	

MTA Event Log				
Index	Date/Time	Priority	ID	Text
1	01/07/10 08:26:36	critical	4000950903	Configuration File Error - Bad Format
2	01/07/10 08:26:36	error	4000950907	Configuration File Error- Misc.
3	01/07/10 08:26:36	critical	4000951502	Provisioning Complete - Fail

The following table describes the labels in this screen.

TABLE 36: The EMTA > Event Log Screen

Config File	
Config Filename	This displays the name of the configuration file (see Configuration Files on page 29).
MTA Event Log	
Index	This displays the arbitrary identifying number assigned to the log entry.
Date/Time	This displays the date and time at which the event that triggered the log entry occurred.
Priority	This displays the severity of the event that triggered the log entry.
ID	This displays the code number for the event type.
Text	This displays the event type.
Clear Log	Click this to remove all entries from the event log. Deleted information cannot be retrieved.



8


TROUBLESHOOTING

Use this section to solve common problems with the BVW-3653 and your network.

Problem: None of the LEDs Turn On

The BVW-3653 is not receiving power, or there is a fault with the device.

1 Ensure that you are using the correct power adaptor.

 **Using a power adaptor other than the one that came with your BVW-3653 can damage the BVW-3653.**

2 Ensure that the power adaptor is connected to the BVW-3653 and the wall socket (or other power source) correctly.

3 Ensure that the power source is functioning correctly. Replace any broken fuses or reset any tripped circuit breakers.

4 Disconnect and re-connect the power adaptor to the power source and the BVW-3653.

5 If none of the above steps solve the problem, consult your vendor.

Problem: One of the LEDs does not Display as Expected

1 Ensure that you understand the LED's normal behavior (see [LEDs](#) on page 18).

2 Ensure that the BVW-3653's hardware is connected correctly; see the Quick Installation Guide.

3 Disconnect and re-connect the power adaptor to the BVW-3653.

4 If none of the above steps solve the problem, consult your vendor.

Problem: I Forgot the BVW-3653's IP Address

- 1** The BVW-3653's default LAN IP address is **192.168.0.1**.
- 2** You can locate the BVW-3653's GUI by entering the LAN domain suffix into your browser's address bar (on a computer connected to the LAN). The default LAN domain suffix is **hitronhub.home**. See **The LAN IP Screen** on page 40 for more information.
- 3** Depending on your operating system and your network, you may be able to find the BVW-3653's IP address by looking up your computer's default gateway. To do this on (most) Windows machines, click **Start > Run**, enter "cmd", and then enter "ipconfig". Get the IP address of the **Default Gateway**, and enter it in your browser's address bar.
- 4** If you still cannot access the BVW-3653, you need to reset the BVW-3653. See **Resetting the BVW-3653** on page 23. All user-configured data is lost, and the BVW-3653 is returned to its default settings. If you previously backed-up a more recent version your BVW-3653's settings, you can now upload them to the BVW-3653; see **The Backup Screen** on page 44.

Problem: I Forgot the BVW-3653's Admin Username or Password

- 1** The default username is **admin**, and the default password is **password**.
- 2** If the default username and password do not work, you need to reset the BVW-3653. See **Resetting the BVW-3653** on page 23. All user-configured data is lost, and the BVW-3653 is returned to its default settings. If you previously backed-up a more recent version your BVW-3653's settings, you can now upload them to the BVW-3653; see **The Backup Screen** on page 44.

Problem: I Cannot Access the BVW-3653 or the Internet

- 1** Ensure that you are using the correct IP address for the BVW-3653.
- 2** Check your network's hardware connections, and that the BVW-3653's LEDs display correctly (see **LEDs** on page 18).
- 3** Make sure that your computer is on the same subnet as the BVW-3653; see **IP Address Setup** on page 20.
- 4** If you are attempting to connect over the wireless network, there may be a problem with the wireless connection. Connect via a **LAN** port instead.
- 5** If the above steps do not work, you need to reset the BVW-3653. See **Resetting the BVW-3653** on page 23. All user-configured data is lost, and the BVW-3653 is returned to its default settings. If you previously backed-up a more recent

version your BVW-3653's settings, you can now upload them to the BVW-3653; see [The Backup Screen](#) on page 44.

- 6 If the problem persists, contact your vendor.

Problem: I Cannot Access the Internet and the DS and US LEDs Keep Blinking

Your service provider may have disabled your Internet access; check the **Cable > System Info** screen's Network Access field (see [The System Info Screen](#) on page 30).

Problem: I Cannot Connect My Wireless Device

- 1 Ensure that your wireless client device is functioning properly, and is configured correctly. See the wireless client's documentation if unsure.
- 2 Ensure that the wireless client is within the BVW-3653's radio coverage area. Bear in mind that physical obstructions (walls, floors, trees, etc.) and electrical interference (other radio transmitters, microwave ovens, etc) reduce your BVW-3653's signal quality and coverage area.
- 3 Ensure that the BVW-3653 and the wireless client are set to use the same wireless mode and SSID (see [The Basic Screen](#) on page 71) and security settings (see [The Security Screen](#) on page 74).
- 4 Re-enter any security credentials (WEP keys, WPA(2)-PSK password, or WPS PIN).
- 5 If you are using WPS's PBC (push-button configuration) feature, ensure that you are pressing the button on the BVW-3653 and the button on the wireless client within 2 minutes of one another.

INDEX

Numbers

802.11b/g/n 16, 69, 72, 82, 83

A

access control 78
access logs 16
access point 15, 69
accounts, login 22
address, IP 20
address, IP, local 21
AP 15, 69
attached network devices 33
authentication 77

B

backup 44
backup and restore 16
bar, navigation 23
BG protection mode 82
buttons 16

C

cable connection 15
cable connection status 32
cable modem 15
CATV 16, 18, 25, 26
cipher type 77
clients, wireless 69
configuration file 29, 34
connection process 33
connection status, cable 32
conventions, document 3
customer support 4

D

debugging 40, 43
default 44
default IP address 21
default username and password 22
defaults 36, 44
De-Militarized Zone 46, 60
DHCP 16, 21, 27, 41, 92
DHCP lease 28
diagnostics 40
DMZ 46, 60
DMZ De-Militarized Zone 16
DNS 40
DOCSIS 25
document conventions 3
Domain Name System 40
domain suffix 40
downstream transmission 29
DS 20

E

eMTA 91
ETH 20
Ethernet 16
Ethernet cables 18
Ethernet port 21
event log 35, 95
event logging 16

F

factory defaults 36, 44
factory reset 18, 23
fast Ethernet 16
FDMA 30
firewall 45
forwarding, port 16, 46, 53
frequencies, cable 29
F-type RF connector 16, 18

G

gigabit Ethernet 16
Graphical User Interface 15
graphical user interface 15
GUI 15, 23
GUI overview 23

H

hardware 16
host ID 25

HT mode 83

I

IANA 25
ICMP 47
IEEE 802.11b/g/n 16, 69
IGMP 16
IGMP snooping 82
interface, user 15
intrusion detection 16, 45, 47
IP address 20, 21, 25, 39, 98
IP address lease 28
IP address renewal 28
IP address setup 20, 21
IP address, default 21
IP address, format 25
IP address, local 21
IP filtering 16, 46, 50
ISP 26

K

keyword blocking 64

L

LAN 15, 39, 69
LAN 1~4 18
LAN IP 40
LEDs 18, 97, 99
lights 18
Line 18
Line 1~2 18, 20
Local Area Network 15

local IP address 21
local logs 60, 67
log 35
log, event 95
logging in 22
login accounts 22
login screen 21
logs, access 16
logs, local 60, 67

M

MAC address 28
MAC address filtering 78
MAC filtering 16, 45, 47
main window 23
Media Access Control address 28
MIMO 16
modem 15
modulation 29
Multiple-In, Multiple-Out 16

N

navigation 23
navigation bar 23
network devices, attached 33
network diagnostics 40
network number 25
network, local 15
network, wide area 15
network, wireless 15

O

open system authentication 77
overview, GUI 23

P

parental control 16, 63
password 36, 98
password and username 22
PBC configuration 71
PIN configuration 16, 71
ping 16, 40, 43, 45, 47
port forwarding 16, 46, 53
port triggering 16, 56
port, Ethernet 21
ports 16
Power 18
pre-authentication 78
pre-shared key 78
private IP address 26
push-button configuration 16

Q

QAM 29
QAM TCM 29
QoS 16, 71, 93
QPSK 29
Quality of Service 16

R

radio coverage 74
 radio links 69
 reboot 44
 reset 18, 23
 restore and backup 16
 RF connector 16, 18
 RJ45 connectors 18
 routing mode 26, 28, 39
 rule, IP filtering 51
 rule, port forwarding 55

S

SCDMA 30
 scheduled website blocking 16
 scheduling 65
 security 74, 76
 security, wireless 16
 service set 70
 settings backup and restore 16
 shared key authentication 77
 SSID 70, 71
 Status 20
 status 33
 status, cable connection 32
 subnet 20, 21, 25, 39
 subnet, IP 20
 support, customer 4
 switch setup 42

T

TCP/IP 21
 TDMA 30
 traceroute 16, 40, 43
 triggering, port 16, 56

trusted computers 63

U

upstream transmission 29
 URL blocking 64
 US 20
 user interface 15
 username 98
 username and password 22

V

voice-enabled cable modem 15
 VoIP 16

W

WAN 15, 26
 WAN connection 33
 website blocking 63
 website blocking, scheduled 16
 WEP 16, 70
 Wide Area Network 15
 Wifi MultiMedia 16, 71
 Wifi Protected Setup 16, 71
 window, main 23
 Windows XP 21
 wired security 16
 wireless 69
 wireless access point 15
 wireless clients 69
 wireless connection 99
 Wireless Local Area Network 15
 wireless networking standards 69

wireless security 16, 70, 74, 76
wireless settings, basic 71
WLAN 15, 69
WMM 16, 71, 83, 86
WPA2 71
WPA2-PSK 16, 70
WPA-PSK 16, 70
WPS 16, 71, 76
WPS PBC 18

X

XP, Windows 21

