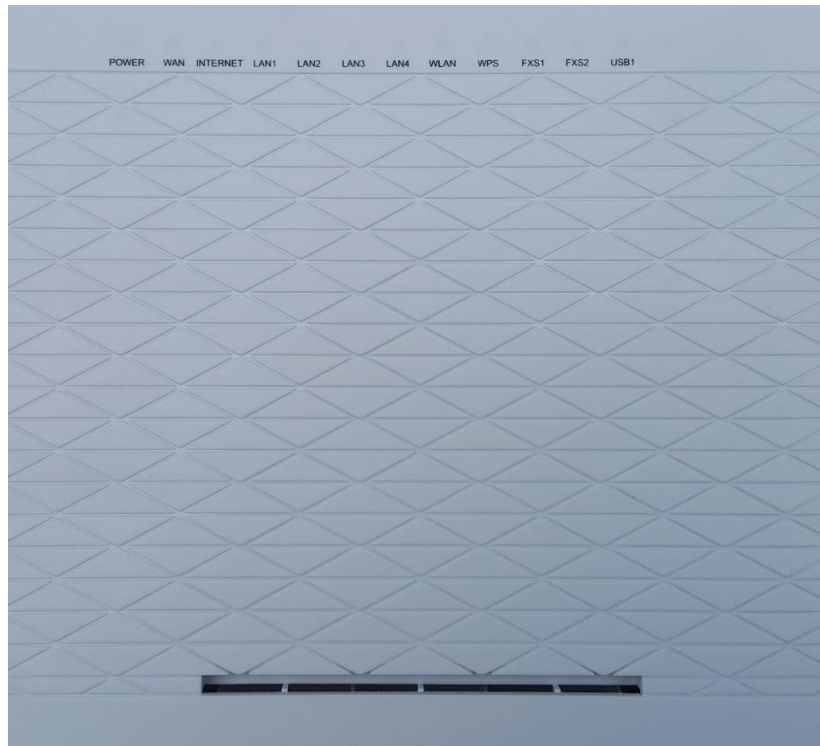


GIGABIT FIBRE ROUTER WITH VOICE



GF1V USER GUIDE

TABLE OF CONTENTS

Overview	4
Introduction.....	4
Target Users.....	4
Prerequisites	4
Notation.....	4
Product Introduction	5
Product Overview	5
Package Contents	5
Product Features	6
Physical Dimensions and Indicators	7
LED Indicators	7
Physical Dimensions.....	8
GF1V Default Settings	8
Interfaces	9
Rear	9
Safety and Product Care	11
Transport and Handling	11
Installation and Configuration of the GF1V	12
Placement of your GF1V.....	12
Avoid obstacles and interference	12
Cordless Phones	12
Choose the “Quietest” Channel for your Wireless Network.....	12
Hardware installation	13
Connecting via a cable.....	13
Connecting wirelessly	13
Web Based Configuration Interface	14
Device Info	14
Summary	14
WAN.....	15
Statistics	15
Route	16
ARP	16
DHCP	16
Advanced Setup	17
Layer2 Interface.....	17
WAN Service	18
LAN	20
NAT	21
Security	25
Parental Control.....	26
Quality of Service	27
Routing.....	29
DNS.....	31
UPnP	32
DNS Proxy.....	32
DLNA.....	33
Packet Acceleration	33
Storage Service	33
Interface Grouping.....	34
IP Tunnel	35
IPSec.....	36
Certificate	37
Power Management.....	37
Multicast (IGMP Configuration)	38

Wireless	39
Basic	39
Security	40
MAC Filter	40
Wireless Bridge	41
Advanced	41
Station Info	42
Voice	43
VoIP Status	43
SIP Basic Setting	43
SIP Advanced	44
SIP Extra Setting	46
SIP Debug Setting	47
Diagnostics	48
Diagnostics	48
Management	49
Settings	49
Update Settings	49
Restore Default	49
System Log	49
Access Control	50
Passwords	50
Services	51
Update Software	51
Save/Reboot	51
Additional Product Information	52
Establishing a wireless connection	52
Windows XP (Service Pack 3)	52
Windows Vista	52
Windows 7	52
Mac OSX 10.6	52
Troubleshooting	53
Using the indicator lights (LEDs) to Diagnose Problems	53
Quality of Service (QoS) configuration examples	54
Limiting the upstream rate	54
Limiting the downstream rate	55
Technical Data	56
Electrical Specifications	56
Environmental Specifications / Tolerances	56

OVERVIEW

INTRODUCTION

This manual provides information related to the installation, operation, and use of the GF1V.

TARGET USERS

The individual reading this manual is presumed to have a basic understanding of telecommunications terminology and concepts.

PREREQUISITES

Before continuing with the installation of your GF1V, please confirm that you comply with the minimum system requirements below.

- An active UFB connection.
- A Computer with Windows, Macintosh, or Linux-based operating systems with a working Ethernet adapter with TCP/IP Protocol installed.
- A Web Browser such as Internet Explorer, Google Chrome, Mozilla Firefox, Opera, Safari etc.
- Wireless Computer System Requirements:
Computer with a working 802.11b, 802.11g or 802.11n wireless adapter.

NOTATION

The following symbols are used in this manual:



Indicates a note requiring attention.



Indicates a note providing a warning.



Indicates a note providing useful information.

PRODUCT INTRODUCTION

PRODUCT OVERVIEW

- 1 x 10/100/1000 Gigabit Ethernet WAN port for connection to fibre services
- 4 x 10/100/1000 Gigabit Ethernet LAN ports for wired connections
- Wireless N300 Access Point for multiple high speed WiFi connections
- 2 x FXS ports for connecting a telephone to make VoIP calls
- 1 x USB host port – supports USB storage device for file sharing
- Built-in media server. Just add a USB hard drive
- IPv6 ready for the next generation IP addressing
- WPS button for simple setup of your wireless network

PACKAGE CONTENTS

The GF1V package consists of:

- 1 x Energy Imports GF1V WiFi Gigabit Fibre Router
- 1 x Quick start guide
- 2 x 1.5m RJ-45 Ethernet cable
- 1 x Power supply (12V/1A)
- 1 x RJ-11 Telephone cable

PRODUCT FEATURES

Utilising the Gigabit WAN port, you can connect to the Internet via a fibre service.

This router also includes 1 x USB host ports that can be used to connect USB devices so that their capabilities can be shared with all connected users. Connect a USB hard drive so that all files stored can be accessed and shared.

The included FXS ports can be used to connect standard telephones that will allow users to make calls over the Internet. By using a VoIP service, phone bills can be dramatically reduced.

All of these features can be shared with multiple users via the built-in wireless access point or the four Gigabit LAN Ethernet ports. The high speed Wireless N provides a signal strong enough to penetrate the far corners of a house and can connect all Wi-Fi enabled devices, such as laptops, smart phones, gaming consoles, tablets and PCs. The four Gigabit LAN Ethernet ports provide a wired connection that can be used to connect desktop computers, media devices or any Ethernet equipped product.



Note: Maximum wireless signal rate and coverage values are derived from IEEE Standard 802.11g and 802.11n specifications. Actual wireless speed and coverage are dependent on network and environmental conditions included but not limited to volume of network traffic, building materials and construction/layout.

PHYSICAL DIMENSIONS AND INDICATORS

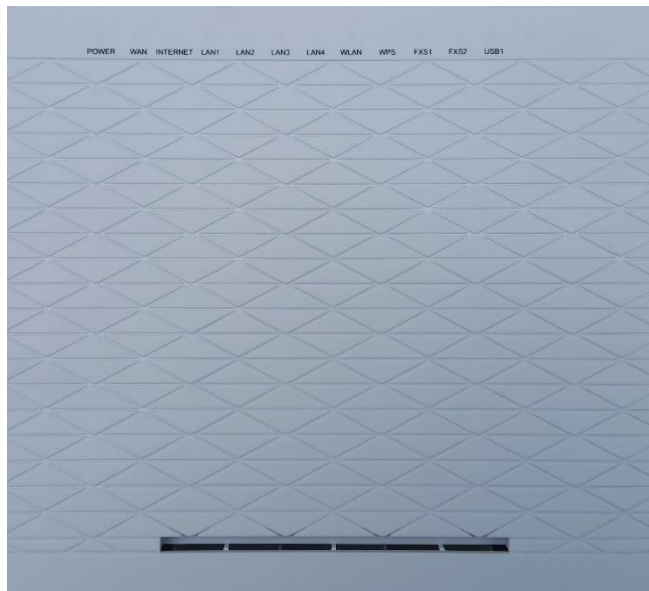
LED INDICATORS

The GF1V has been designed to be placed on a desktop. All of the cables exit from the rear for easy organization. The display is visible on the front of the GF1V to provide you with information about network activity and the device status. See below for an explanation of each of the indicator lights.

LED INDICATOR	COLOUR	DEFINITION
Power	Green	The GF1V is powered on and operating normally.
	Red	The GF1V is starting up.
	Red Blinking	The firmware is being upgraded.
	Off	The power is off.
Internet	Green	The GF1V is connected to an internet service.
	Red	Authentication on the broadband account has failed.
	Green Blinking	Data is being transmitted to or from the internet.
	Off	The GF1V is not connected to the internet.
WAN	Green	A device is connected to the Ethernet WAN port.
	Green Blinking	Data is being transmitted to or from the WAN.
	Off	No device is connected to the Ethernet WAN port.
Ethernet 1-4	Green	A device is connected to the Ethernet LAN port.
	Green Blinking	Data is being transmitted to or from the Ethernet LAN port.
	Off	No device is connected to the Ethernet LAN port.
WiFi	Green	WiFi is enabled.
	Green Blinking	Data is being transmitted to or from the Wireless interface.
	Off	WiFi is disabled.
WPS	Green	The client has successfully connected to the router.
	Green Blinking	The client is accessing the router via WPS.
	Off	WPS is disabled.
USB 1	Green	A USB hard drive is connected.
	Green Blinking	Data is being transmitted through the USB interface.
	Off	No USB hard drive is connected to the USB interface.
FXS1 – FXS2	Off	No handset is connected.
	Green	VoIP registration was successful.
	Green Blinking	The telephone is ready to make or receive a call.
	Green Blinking	The telephone is ringing.

PHYSICAL DIMENSIONS

The following page lists the physical dimensions of the GF1V.



170 mm (H) x 45 mm (D) x 190 mm (W)

GF1V DIMENSIONS	
Width	190 mm
Height	170 mm
Depth	45 mm
Weight	343 grams

GF1V DEFAULT SETTINGS

The following tables list the default settings for the GF1V.

LAN (MANAGEMENT)	
Static IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1

WIRELESS (WIFI)	
SSID	Slingshot Home WIFI
Security	WPA2-PSK (AES)
Security Key	The full MAC address

GF1V WEB INTERFACE ACCESS	
Username	admin
Password	Last 6 characters of MAC address

INTERFACES

REAR

The following interfaces are available on the GF1V:



INTERFACE	DESCRIPTION
TEL1 & TEL2	Connect regular analogue telephone handsets here to use them with a VoIP service.
LAN1 -4	Gigabit Ethernet LAN ports. Connect your Ethernet based devices to one of these ports for high-speed internet access.
WAN	Gigabit WAN port for connection to a WAN network.
Reset button	Factory Reset the device by holding the Reset button down for 3 seconds.
Power	Connection point for the included power adapter. Connect the power supply here.

LEFT



NUMBER	INTERFACE	DESCRIPTION
1	WPS	Activate the WPS function by holding the WPS button down for 3 seconds.
2	WLAN	Enable or disable the Wi-Fi radio by holding the Wi-Fi button down for 3 seconds.
3	USB	Connect an external USB hard drive here to use the NAS feature of the GF1V.
4	Power	Turns the GF1V on or off.

SAFETY AND PRODUCT CARE

With reference to unpacking, installation, use and maintenance of your electronic device, the following basic guidelines are recommended:

- Do not use or install this product near water to avoid fire or shock hazard. For example, near a bathtub, kitchen sink, laundry tub, or near a swimming pool. Also, do not expose the equipment to rain or damp areas (e.g. a wet basement).
- Do not connect the power supply cord on elevated surfaces. Allow it to lie freely. There should be no obstructions in its path and no heavy items should be placed on the cord. In addition, do not walk on, step on or mistreat the cord.
- To safeguard the equipment against overheating, make sure that all openings in the unit that offer exposure to air are unobstructed.

**WARNING**

Disconnect the power supply from the device before servicing.

TRANSPORT AND HANDLING

When transporting the GF1V, it is recommended to return the product in the original packaging. This ensures the product will not be damaged.



In the event the product needs to be returned, ensure it is securely packaged with appropriate padding to prevent damage during courier transport.

INSTALLATION AND CONFIGURATION OF THE GF1V

PLACEMENT OF YOUR GF1V

The wireless connection between your GF1V and your Wi-Fi devices will be stronger the closer your connected devices are to your GF1V. Your wireless connection and performance will degrade as the distance between your GF1V and connected devices increases. This may or may not be directly noticeable, and is greatly affected by the individual installation environment.

If you have concerns about your network's performance that might be related to range or obstruction factors, try moving the computer to a position between three to five meters from the GF1V in order to see if distance is the problem.



Note: While some of the items listed below can affect network performance, they will not prohibit your wireless network from functioning; if you are concerned that your network is not operating at its maximum effectiveness, this checklist may help.

If you experience difficulties connecting wirelessly between your Wi-Fi devices and your GF1V, please try the following steps:

- In multi-storey homes, place the GF1V on a floor that is as close to the centre of the home as possible. This may mean placing the GF1V on an upper floor.
- Try not to place the GF1V near a cordless telephone that operates at the same radio frequency as the GF1V (2.4GHz).

AVOID OBSTACLES AND INTERFERENCE

Avoid placing your GF1V near devices that may emit radio "noise," such as microwave ovens. Dense objects that can inhibit wireless communication include:

- Refrigerators
- Washers and/or dryers
- Metal cabinets
- Large aquariums
- Metallic-based, UV-tinted windows
- If your wireless signal seems weak in some spots, make sure that objects such as those listed above are not blocking the signal's path (between your devices and the GF1V).

CORDLESS PHONES

If the performance of your wireless network is impaired after considering the above issues, and you have a cordless phone:

- Try moving cordless phones away from your GF1V and your wireless-enabled computers.
- Unplug and remove the battery from any cordless phone that operates on the 2.4GHz band (check manufacturer's information). If this fixes the problem, your phone may be interfering with the GF1V.
- If your phone supports channel selection, change the channel on the phone to the farthest channel from your wireless network. For example, change the phone to channel 1 and move your GF1V to channel 11. See your phone's user manual for detailed instructions.
- If necessary, consider switching to a 900MHz or 5GHz cordless phone.

CHOOSE THE "QUIETEST" CHANNEL FOR YOUR WIRELESS NETWORK

In locations where homes or offices are close together, such as apartment buildings or office complexes, there may be wireless networks nearby that can conflict with your wireless network. Use the Site Survey capabilities found in the Wireless Utility of your wireless adapter to locate any other wireless networks that are available (see your wireless adapter's user manual), and switch your Router and computers to a channel as far away from other networks as possible.

Experiment with more than one of the available channels, in order to find the clearest connection and avoid interference from neighbouring cordless phones or other wireless devices.

HARDWARE INSTALLATION

1. Connect the power adapter to the Power socket on the back of the GF1V.
2. Plug the power adapter into the wall socket and switch on the power.
3. Wait approximately 60 seconds for the GF1V to power up.

CONNECTING VIA A CABLE

1. Connect the yellow Ethernet cable provided to one of the ports marked 'LAN' at the back of the GF1V.
2. Connect the other end of the yellow Ethernet cable to your computer.
3. Wait approximately 30 seconds for the connection to establish.
4. Open your Web browser, and enter <http://192.168.1.1> into the address bar and press enter.
5. Follow the steps to set up your GF1V.

CONNECTING WIRELESSLY

1. Ensure Wi-Fi is enabled on your device (e.g. computer/laptop/smartphone).
2. Scan for wireless networks in your area and connect to the network name that matches the Wireless network name configured on the GF1V. When prompted for your wireless security settings, enter the Wireless security key configured on the GF1V.
3. Wait approximately 30 seconds for the connection to establish.
4. Open your Web browser, and enter <http://192.168.1.1> into the address bar and press Enter.
5. Follow the steps to set up your GF1V.

WEB BASED CONFIGURATION INTERFACE

FIRST-TIME SETUP

Please note that the GF1V is configured to work out of the box for Slingshot UFB connections. No configuration is necessary. If you want to change any of the settings, please follow the steps below to configure your GF1V Wireless router via the web based menu.

Open your web browser (e.g. Internet Explorer/Firefox/Safari) and type <http://192.168.1.1/> into the address bar at the top of the window.

At the login screen, type admin in the username and the last 6 characters of the <MAC> address in the password field, then click the Login button.

DEVICE INFO

SUMMARY

When you log in to the router, the Device Info Summary page is displayed, providing a general overview of the status of the router and the WAN connection.

Device Info

Board ID:	WRV9200
Manufacturer:	Broadcom
Serial Number:	160520000259
Build Timestamp:	201605171937
Software Version:	4.12L.08
Bootloader (CFE) Version:	1.0.38-114.170
Wireless Driver Version:	6.30.163.23.cpe4.12L
Voice Service Version:	V2.4
Uptime:	0D 3H 3M 12S

This information reflects the current status of your WAN connection.

LAN IPv4 Address:	192.168.1.1
Default Gateway:	
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0
LAN IPv6 Address:	
Default IPv6 Gateway:	
Date/Time:	Sat Nov 19 03:03:03 2011

ITEM	DEFINITION
Serial Number	The unique set of numbers assigned to the routers for identification purposes.
Build Timestamp	The date and time that the software running on the router was published.
Software Version	The current firmware version installed on the router.
Boot Loader (CFE) Version	The current boot loader installed on the router.
Wireless Driver Version	The current wireless driver installed on the router.
Voice Service Version	The version of the software running the voice module.
Uptime	The number of days, hours and minutes that the router has been running.
LAN IPv4 Address	The current IPv4 address assigned to the router.
Default Gateway	The current default gateway of the WAN interface.
Primary DNS Server	The current primary DNS server in use
Secondary DNS Server	The current secondary DNS server in use.
LAN IPv6 Address	The current IPv6 IP address in use if assigned.
Default IPv6 Gateway	The current IPv6 default gateway if assigned.
Date/Time	The current date and time set on the router.

WAN

The WAN page shows more detailed information related to the WAN interface configuration, including the firewall status, IPv4 and IPv6 addresses of the router.

Interface	Description	Type	VlanMuxId	Igmp	NAT	Firewall	IPv4 Status	IPv6 Status	IPv4 Address	IPv6 Address	Connected Time	MAC Address
ppp0.1	SlingshotUFB.10	PPPoE	10	Enabled	Enabled	Enabled	Unconfigured	Unconfigured	0.0.0.0		/	00:00:00:00:00:00

ITEM	DEFINITION
Interface	The Interface of the WAN connection.
Description	The description of the WAN connection.
Type	The type of WAN connection.
VLAN Mux ID	Details the status of VLAN Mux ID.
IGMP	Details the status of IGMP on each WAN connection. IGMP is only used with IPv4 connections.
NAT	The NAT status of the WAN connection.
Firewall	The status of the router firewall across the WAN connection.
IPv4 Status	The status of the IPv4 WAN connection.
IPv6 Status	The status of the IPv6 WAN connection.
IPv4 Address	The current IP v4 address of the WAN connection.
IPv6 Address	The current IP v6 address of the WAN connection.

STATISTICS

LAN

The Statistics – LAN page shows detailed information about the number of bytes, packets, errors and dropped packets on each LAN interface in both directions of communication.

Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth2	0	8466	0	0	0	1780	0	0
eth1	0	0	0	0	0	0	0	0
eth0	0	0	0	0	0	0	0	0
eth3	0	0	0	0	0	0	0	0
wl0	0	0	0	0	0	0	0	0

Reset Statistics

INTERFACE	DESCRIPTION	
Received/Transmitted	Bytes	Rx/Tx (receive/transmit) packets in bytes.
	Packets	Rx/Tx (receive/transmit) packets.
	Errors	Rx/Tx (receive/transmit) packets with errors.
	Drops	Rx/Tx (receive/transmit) packets with drops.

WAN

The Statistics – WAN Service page shows detailed information about the number of bytes, packets, errors and dropped packets on the WAN interface in both directions of communication.

Statistics -- WAN

Interface	Description	Connected Time	Received				Transmitted			
			Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
ppp0.1	SlingshotUFB.10	/	0	0	0	0	0	0	0	0

Reset Statistics

INTERFACE		DESCRIPTION	
Received/Transmitted	Bytes	Rx/Tx (receive/transmit) packets in bytes.	
	Packets	Rx/Tx (receive/transmit) packets.	
	Errors	Rx/Tx (receive/transmit) packets with errors.	
	Drops	Rx/Tx (receive/transmit) packets with drops.	

ROUTE

The Route page displays any routes that the router has detected.

Device Info -- Route

Flags: U - up, I - reject, G - gateway, H - host, R - reinstate

D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0

ARP

Click ARP to display the ARP information.

This option can be used to determine which IP address / MAC address is assigned to a particular host. This can be useful when setting up URL filtering, Time of Day filtering or Static DHCP addressing.

Device Info -- ARP

IP address	Flags	HW Address	Device
192.168.1.69	Complete	d0:50:99:52:f2:f0	br0

DHCP

Click DHCP to display the DHCP information.

Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Connection Type	IP Address Assignment	Status	Expires In
Unknown	d0:50:99:52:f2:f0	192.168.1.69	Ethernet	Static	Active	0 seconds

You can use this to determine when a specific DHCP lease will expire, or to assist you with setting up Static DHCP addressing.

ADVANCED SETUP

LAYER2 INTERFACE

ETH INTERFACE

The ETH interface page allows you to add or remove ETH WAN interfaces. This is currently configured for Slingshot UFB requirements. Please do not change.

ETH WAN Interface Configuration

Choose Add, or Remove to configure ETH WAN interfaces.
Allow one ETH as layer 2 wan interface.

Name	Connection Mode	Remove
eth4/eth4	VlanMuxMode	<input type="checkbox"/>

WAN SERVICE

The WAN Service page displays the current Wide Area Network service setup and allows you to configure the router to connect to a larger network for Internet access. This is currently configured for Slingshot UFB requirements. Please do not change.

Wide Area Network (WAN) Service Setup
Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan802.1p	VlanMuxId	Igmp	NAT	Firewall	IPv4	IPv6	Mld	Remove	Edit	Action
ppp0.1	SlingshotUFB.10	PPPoE	0	10	Enabled	Enabled	Enabled	Enabled	Disabled	Disabled	<input type="checkbox"/>	<input type="button" value="edit"/>	<input type="button" value="Up"/>

To add a WAN service, click the Add button. Use the drop down list to select the layer 2 interface to use for the WAN service and click the Next button.

WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set

eth4/eth4

Select a WAN service type, enter a Service Description, enter the 802.1P Priority and 802.1 VLAN ID then click the Next button.

WAN Service Configuration

Select WAN service type:

☒ PPP over Ethernet (PPPoE)
☐ IP over Ethernet
☐ Bridging

Enter Service Description:

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

PPP OVER ETHERNET

Enter the details as required by your Internet Service Provider and click the Next button.

PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:
 PPP Password:
 PPPoE Service Name:
 Authentication Method:
 MTU[576-1492]:

☐ Config KeepAlive
☐ Enable Fullcone NAT
☐ Dial on demand (with idle timeout timer)

☒ Enable IPv4 for this service
☐ PPP IP extension
☐ Use Static IPv4 Address

☐ Enable IPv6 for this service
☐ Enable PPP Debug Mode
☐ Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

☐ Enable IGMP Multicast Proxy

IP OVER ETHERNET

Enter the details as required by your Internet Service Provider and click the Next button.

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
 Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode.
 If "Use the following Static IPv4/IPv6 address" is chosen, enter the WAN IPv4/IPv6 address, subnet mask/prefix Length and interface gateway.

☒ Enable IPv4 for this service

☒ Obtain an IP address automatically
☐ Use the following Static IP address

Option 55 Request List : (e.g:1,3,6,12)

Option 58 Renewal Time: (hour)

Option 59 Rebinding Time: (hour)

Option 60 Vendor ID:

Option 61 IAID: (8 hexadecimal digits)

Option 61 DUID: (hexadecimal digit)

Option 125:

☒ Disable ☐ Enable

☐ Enable IPv6 for this service

Select the NAT Translation settings as desired and click the Next button.

Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

☒ Enable NAT

☐ Enable Fullcone NAT

☒ Enable Firewall

Multicast Proxy

☐ Enable IGMP Multicast

BRIDGING

When you select bridging mode, a summary of the settings is displayed. Click Apply/Save to commit the settings.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	Bridge
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Use the arrow buttons to move the interfaces required to the list on the left. Click Next.

Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Selected Default Gateway Interfaces

eth4.1



Available Routed WAN Interfaces

ppp0.2

Back Next

Use the arrow buttons to move the interfaces required as DNS Server interfaces to the left. The interface highest on the list has the highest priority as a DNS server. Click Next to continue.

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces

eth4.1



Available WAN Interfaces

ppp0.2

Back Next

A summary of your settings is displayed. Click Apply/Save to commit your settings to the router.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	PPPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Back Apply/Save

LAN

IPv6 AUTOCONFIG

The IPv6 LAN Auto Configuration page allows you to configure settings pertaining to the IPv6 DHCP server.

IPv6 LAN Auto Configuration

Note:

1: Stateful DHCPv6 is supported based on the assumption of prefix length less than 64. Interface ID does NOT support ZERO COMPRESSION ":", Please enter the complete information. For example: Please enter "0:0:0:2" instead of "::2".

2: Unique local address must start with "fd". The prefix and the address must be in same network and the prefix length must be 64.

☐ Enable Unique Local Addresses And Prefix Advertisement

☐ Randomly Generate

☐ Statically Configure

Address: (e.g: fd80::1/64)

Prefix: (e.g: fd80::/64)

Preferred Life Time (hour):

Valid Life Time (hour):

IPv6 LAN Applications

☒ Enable DHCPv6 Server and RADVD

☒ Stateless

☐ Stateful

Start interface ID: 0:0:0:2

End interface ID: 0:0:0:254

Leased Time (hour): 24

☒ Enable MLD Snooping

☐ Standard Mode

☒ Blocking Mode

[Save/Apply](#)

OPTION	DEFINITION
Enable Unique Local Addresses and Prefix	Enable the use of unique local addresses. The router will advertise the IPv6 prefix to new devices on the network.
Randomly Generate	Randomly generates the unique local addresses and the prefix.
Statically Configure	Enter a static IPv6 address for the router if one has been assigned to you by your Internet Service Provider.
IPv6 LAN Applications	Enable IPv6 DHCP server
Enable DHCPv6 Server and RADVD	<p>The Router Advertisement Daemon (radvd) is an open-source software product that implements link-local advertisements of IPv6 router addresses and IPv6 routing prefixes using the Neighbor Discovery Protocol (NDP) as specified in RFC 2461. The Router Advertisement Daemon is used by system administrators in stateless auto-configuration methods of network hosts on Internet Protocol version 6 networks.</p> <p>When IPv6 hosts configure their network interfaces, they broadcast router solicitation (RS) requests onto the network to discover available routers. The radvd software answers requests with router advertisement (RA) messages. In addition, radvd periodically broadcasts RA packets to the attached link to update network hosts. The router advertisement messages contain the routing prefix used on the link, the link maximum transmission unit (MTU), and the address of the responsible default router.</p>
Stateless	IPv6 hosts can configure themselves automatically when connected to a routed IPv6 network using Internet Control Message Protocol version 6 (ICMPv6) router discovery messages. This type of configuration is suitable for small organizations and individuals. It allows each host to determine its address from the contents of received user advertisements. It makes use of the IEEE EUI-64 standard to define the network ID portion of the address.
Stateful	This configuration requires some human intervention as it makes use of the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) for installation and administration of nodes over a network. The DHCPv6 server maintains a list of nodes and the information about their state to know the availability of each IP address from the range specified by the network administrator.
Enable MLD Snooping	Select whether to enable or disable MLD Snooping on the router. The Multicast Listener Discovery (MLD) snooping function constrains the flooding of IPv6 multicast traffic on VLANs on the router.

NAT

VIRTUAL SERVERS

A virtual server allows you to direct incoming traffic from the WAN side to the Internal server with a private IP address on the LAN side.

NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address or Hostname	WAN Interface	LAN Loopback	Enable/Disable	Remove
-------------	---------------------	-------------------	----------	---------------------	-------------------	-------------------------------	---------------	--------------	----------------	--------

Click the Add button to add a virtual server.

NAT -- Virtual Servers

Select the service name, and enter the server IP address or hostname, and click "Apply/Save" to forward IP packets for this service to the specified server.
 NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".
 Remaining number of entries that can be configured: 32

Use Interface:

Service Name:

☒ Select a Service:

☐ Custom Service:

☐ Enable LAN Loopback

Server IP Address or Hostname:

Status:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		

FIELD	DESCRIPTION
Select a Service or custom Server	Select a pre-configured port forwarding rule or choose custom server to create your own port forwarding rule.
Server IP Address	Enter the IP address of the local server.
External Port Start	Enter the starting external port number (when custom server is selected). When a service is connected this field will be completed automatically.
External Port End	Enter the ending external port number (when custom server is selected). When a service is connected this field will be completed automatically.
Protocol	Options include TCP, UDP or TCP/UDP.
Internal Port Start	Enter the starting internal port number (when custom server is selected). When a service is connected this field will be completed automatically.
Internal Port End	Enter the ending internal port number (when custom server is selected). When a service is connected this field will be completed automatically.

Click Save/Apply to save your settings when you have finished creating virtual servers.

PORT TRIGGERING

Some applications require specific ports in the Router's firewall to be open for access by remote parties. Port Triggering opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'.

The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

NAT -- Port Triggering Setup

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

Application Name	Trigger			Open			WAN Interface	Remove
	Protocol	Port Range		Protocol	Port Range			
		Start	End		Start	End		

Add Remove

To add a Trigger Port, press the Add button.

NAT -- Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "Save/Apply" to add it. Remaining number of entries that can be configured: 32

Use Interface:

Application Name:

☒ Select an application:

☐ Custom application:

Apply/Save

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

Save/Apply

FIELD	DESCRIPTION
Select an Application or Custom Application	A user can select a pre-configured application from the list or select the Custom Application option to create custom application settings.
Trigger Port Start	Enter the starting trigger port number (when you select Custom Application). When an application is selected the port range values are automatically entered.
Trigger Port End	Enter the ending trigger port number (when you select Custom Application). When an application is selected the port range values are automatically entered.
Trigger Protocol	Options include TCP, UDP or TCP/UDP.
Open Port Start	Enter the starting open port number (when you select Custom Application). When an application is selected the port range values are automatically entered.
Open Port End	Enter the ending open port number (when you select Custom Application). When an application is selected the port range values are automatically entered.
Open Protocol	Options include TCP, UDP or TCP/UDP.

DMZ HOST

The GF1V will forward IP packets from the Wide Area Network (WAN) that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click Apply to activate the DMZ host. To deactivate the DMZ Host function clear the IP address field and press the Save/Apply button.

NAT -- DMZ Host

The Broadband Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click 'Apply' to activate the DMZ host.

Clear the IP address field and click 'Apply' to deactivate the DMZ host.

DMZ Host IP Address:

☐ Enable LAN Loopback

Apply/Save

SECURITY

FIREWALL

The GF1V has a firewall function which helps to keep you secure while allowing you to configure rules allowing certain types of data through.

Firewall Table

Firewall's Rule Table

enabled	IPVersion	PacketLength	DSCP/TC	Protocol	Action	RejectType	ConnType	TCP Flags	origIPAddress	origMask/ prefixLength	origPortRange	destIPAddress	destMask/ prefixLength	destPortRange	bytes	pkts
<input type="checkbox"/>																

To use the firewall feature, begin by clicking the Add Firewall button to create a firewall.

Firewall

a Firewall have a number of Rule which define the behavior of match item

name: interface type defaultaction

Then click the Add Rule button to create a rule for the firewall. Enter the rules that you require for the firewall and then click the Save&Apply button to commit the settings.

Enabled	<input type="checkbox"/>	PacketLength(FROM:TO)	<input type="text"/>	TC(0~255)	<input type="text"/>	DSCP	<input type="text"/>
IP Version	<input type="text" value="4"/>	Action	<input type="text" value="Permit"/>	RejectType	<input type="text"/>	IcmpType	<input type="text"/>
Protocol	<input type="text" value=""/>						
TCP Flags	<input type="checkbox"/> SYN <input type="checkbox"/> ACK <input type="checkbox"/> FIN <input type="checkbox"/> RST <input type="checkbox"/> URG <input type="checkbox"/> PSH						
origIPAddress:	<input type="text"/>	origMask/prefixLength	<input type="text"/>	origStartPort	<input type="text"/>	origEndPort	<input type="text"/>
destIPAddress:	<input type="text"/>	destMask/prefixLength	<input type="text"/>	destStartPort	<input type="text"/>	destEndPort	<input type="text"/>

PARENTAL CONTROL

The Parental Control feature allows you to take advanced measures to ensure the computers connected to the LAN are used only when and how you decide.

TIME RESTRICTION

This Parental Control function allows you to restrict access from a Local Area Network (LAN) connected device to an outside network through the router on selected days and at certain times. Make sure to activate the Internet Time server synchronization as described in the Management section, so that the scheduled times match your local time.

Access Time Restriction -- A maximum 16 entries can be configured.

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
<div style="text-align: center;"> <input type="button" value="Add"/> <input type="button" value="Remove"/> </div>											

Figure 1: Advanced - Parental Control – TimeRestriction

To add a time restriction rule, press the Add button. The following screen appears.

Access Time Restriction

This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the 'Other MAC Address' button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type 'ipconfig /all'.

User Name

☒ Browser's MAC Address

☐ Other MAC Address

(xx:xx:xx:xx:xx:xx)

Days of the week

Click to select ☐ ☐ ☐ ☐ ☐ ☐ ☐

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

Figure 2: Advanced - Parental Control - Add TimeRestriction

See the instructions below. Press the Apply/Save button to save a time restriction rule.

FIELD	DESCRIPTION
User Name	A user defined name for the time restriction rule.
Browser's MAC Address	The MAC address of the network card of the computer running the browser.
Other MAC Address	The MAC address of a second LAN device or network card.
Days of the Week	The days of the week for which the rules apply.
Start Blocking Time	The time of day when the restriction starts.
End blocking time	The time of day when the restriction ends.

Table 2: Advanced - Parental Control - Add Time Restriction Settings

URL FILTER

With the URL filter, you are able to add certain websites or URLs to a safe or blocked list. This will provide you added security to ensure any website you deem unsuitable will not be able to be seen by anyone who is accessing the Internet via the GF1V.

Select the 'To block' or 'To allow' option and then click Add to enter the URL you wish to add to the URL Filter list.

URL Filter -- Please select the list type first then configure the list entries.
Maximum 100 entries can be configured.

URL List Type: ☐ Black List ☐ White List

Address	Port	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>		

Figure 3: Advanced - Parental Control - URL Filter

Once you have chosen to add a URL to the list you will be prompted to enter the address. Simply type it in and select the Apply/Save button.

Parental Control -- URL Filter Add

Enter the URL address and port number then click 'Apply/Save' to add the entry to the URL filter.

URL Address:

Port Number: (Default 80 will be applied if leave blank.)

Figure 4: Advanced - Parental Control - Add URL Filter

QUALITY OF SERVICE

Quality of Service offers a defined level of performance in a data communications system - for example the ability to guarantee that video traffic is given priority over other network traffic to ensure that video streaming is not disrupted by other network traffic. This means that if you are streaming video and someone else in the house starts downloading a large file, the download won't disrupt the flow of video traffic.

QoS -- Queue Management Configuration

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.

Note: If Enable QoS checkbox is not selected, all QoS will be disabled for all interfaces.

Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.

☐ Enable QoS

Figure 5: Advanced - Enable QoS

To enable QoS select the Enable QoS checkbox, and set the Default DSCP (Differentiated Services Code Point) Mark. Then press the Apply/Save button.

QoS Queue

QoS Queue Setup

In ATM mode, maximum 16 queues can be configured.
 In PTM mode, maximum 8 queues can be configured.
 For each Ethernet interface, maximum 3 queues can be configured.
 To add a queue, click the **Add** button.
 To remove queues, check their remove-checkboxes, then click the **Remove** button.
 The **Enable** button will scan through every queues in the table. Queues with enable-checkbox checked will be enabled. Queues with enable-checkbox un-checked will be disabled.
 The enable-checkbox also shows status of the queue after page reload.
 If you disable WMM function in Wireless Page, queues related to wireless will not take effects

The QoS function has been disabled. Queues would not take effects.

Name	Key	Interface	Qid	Prec/Alg/Wght	DSL Latency	PTM Priority	Min Bit Rate(bps)	Shaping Rate(bps)	Burst Size(bytes)	Enable	Remove
WMM Voice Priority	1	wl0	0	1/SP						Enabled	
WMM Voice Priority	2	wl0	0	2/SP						Enabled	
WMM Video Priority	3	wl0	0	3/SP						Enabled	
WMM Video Priority	4	wl0	0	4/SP						Enabled	
WMM Best Effort	5	wl0	0	5/SP						Enabled	
WMM Background	6	wl0	0	6/SP						Enabled	
WMM Background	7	wl0	0	7/SP						Enabled	
WMM Best Effort	8	wl0	0	8/SP						Enabled	

Figure 6: Advanced - QoS Queue Setup

Click the Add button to add a QoS Queue. The following screen is displayed.

QoS Queue Configuration

This screen allows you to configure a QoS queue and add it to a selected layer2 interface.

Name:

Enable:

Interface:

Figure 7: Advanced - QoS - Add QoS Queue

The above screen allows you to configure a QoS queue entry and assign it to a specific network interface. Each of the queues can be configured for a specific precedence. The queue entry configured here will be used by the classifier to place ingress packets appropriately.

NOTE: Precedence level 1 relates to higher priority while precedence level 3 relates to lower priority.

QoS Classification

QoS Classification Setup -- maximum 32 rules can be configured.

To add a rule, click the **Add** button.
 To remove rules, check their remove-checkboxes, then click the **Remove** button.
 The **Enable** button will scan through every rules in the table. Rules with enable-checkbox checked will be enabled. Rules with enable-checkbox un-checked will be disabled.
 The enable-checkbox also shows status of the rule after page reload.
 If you disable WMM function in Wireless Page, classification related to wireless will not take effects

		CLASSIFICATION CRITERIA											CLASSIFICATION RESULTS							
Class Name	Order	Class Interface	Ethernet Type	Source MAC/Mask	Destination MAC/Mask	Source IP/Prefix Length	Destination IP/Prefix Length	Protocol	Source Port	Destination Port	DSCP Check	TC Check	802.1P Check	Queue Key	DSCP Mark	TC Mark	802.1P Mark	Rate Limit(kbps)	Enable	Remove

Figure 8: Advanced - QoS Classification Setup

Click the Add button to configure network traffic classes.

Add Network Traffic Class Rule

This screen creates a traffic class rule to classify the ingress traffic into a priority queue and optionally mark the DSCP or Ethernet priority of the packet. Click 'Apply/Save' to save and activate the rule.

Traffic Class Name:

Rule Order:

Rule Status:

Specify Classification Criteria (A blank criterion indicates it is not used for classification.)

Class Interface:

Ether Type:

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

Specify Classification Results (A blank value indicates no operation.)

Specify Class Queue (Required):

- Packets classified into a queue that exit through an interface for which the queue is not specified to exist, will instead egress to the default queue on the interface.

Mark 802.1p priority:

- Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits.
 - Class vlan packets egress to a non-vlan interface will have the packet p-bits re-marked by the class rule p-bits. No additional vlan tag is added.
 - Class non-vlan packets egress to a vlan interface will be tagged with the interface VID and the class rule p-bits.
 - Class vlan packets egress to a vlan interface will be additionally tagged with the packet VID, and the class rule p-bits.

Set Rate Limit: [Kbits/s]

Figure 9: Advanced - Add QoS Network Traffic Classification

The above screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header TOS (type of service) byte. A rule consists of a class name and at least one condition. All of the specified conditions in this classification rule must be satisfied for the rule to take effect.

Click the Apply/Save button to save and activate the rule.

ROUTING

The Default Gateway, Static Route and Policy Routing settings can be found in the Routing option of the Advanced menu.

DEFAULT GATEWAY

Select your preferred WAN interface from the available options.

Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Selected Default Gateway Interfaces

Available Routed WAN Interfaces

ppp0.1

TODO: IPV6 ***** Select a preferred wan interface as the system default IPv6 gateway.

Selected WAN Interface

Figure 10: Advanced - Routing - Default Gateway

STATIC ROUTE

The Static Route screen displays the configured static routes. Click the Add or Remove buttons to change settings.

Routing -- Static Route (A maximum 32 entries can be configured)

IP Version	DstIP/Mask	Gateway	Interface	Metric	Remove
<div> <div>Add</div> <div>Remove</div> </div>					

Figure 11: Advanced - Routing - Static Route

To add a static route rule, click the Add button. The following screen is displayed.

Routing -- Static Route Add

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click 'Apply/Save' to add the entry to the routing table.

IP Version: IPv4

Destination IP address/prefix length:

Interface:

Gateway IP Address:

(optional: metric number should be greater than or equal to zero)

Metric:

Apply/Save

Figure 12: Advanced - Routing - Add Static Route

Enter the Destination Network Address, Gateway IP Address and/or WAN Interface. Then click Apply/Save to add the entry to the routing table.

POLICY ROUTING

This function allows you to add policy rules to certain situations.

Policy Routing Setting -- A maximum 7 entries can be configured.

Policy Name	Source IP	LAN Port	WAN	Default GW	Remove
<div> <div>Add</div> <div>Remove</div> </div>					

Figure 13: Advanced - Routing - Policy Routing

Click the Add button to add a policy rule. The following screen is displayed.

Policy Routing Setup

Enter the policy name, policies, and WAN interface then click "Apply/Save" to add the entry to the policy routing table.
Note: If selected "IPv6" as WAN interface, default gateway must be configured.

Policy Name:

Physical LAN Port:

Source IP:

Use Interface: SlingshotUFB.10/ppp0.1

Default Gateway:

Apply/Save

Figure 14: Advanced - Routing - Add Policy Route

Enter the details into the provided fields. The table below describes each field.

FIELD	DESCRIPTION
Policy Name	A user defined name for the policy route.
Physical LAN Port	The LAN port to be used for the policy.
Source IP	The IP address of the LAN device involved with the policy.
Use Interface	Select the Interface that the policy will employ.
Default Gateway	Enter the gateway address.

DNS

DNS SERVER

This page allows you to enable automatic DNS settings detected from the Internet Service Provider or specify your own DNS server address manually.

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

☒ Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces

ppp0.1

->

<-

Available WAN Interfaces

☐ Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Figure 16: Advanced - DNS Server

DYNAMIC DNS

The Dynamic DNS service allows a dynamic IP address to be aliased to a static hostname in any of a selection of domains, allowing the router to be more easily accessed from various locations on the internet.

Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your Broadband Router to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove

Figure 17: Advanced - DNS - Dynamic DNS



Note: The Add/Remove buttons will be displayed only if the router has been assigned an IP address from the remote server.

To add a dynamic DNS service, click the Add button and the following screen will display.

Add Dynamic DNS

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

D-DNS provider

Hostname

Interface

DynDNS Settings

Username

Password

Figure 18: Advanced - DNS - Add Dynamic DNS Account

FIELD	DESCRIPTION
D-DNS Provider	Select the dynamic DNS provider from the list.
Host Name	The name of the dynamic DNS provider.
Interface	Select the interface from the list.
Username	Enter the Dynamic DNS account username.
Password	Enter the Dynamic DNS account password.

Table 3: Advanced - DNS - Add Dynamic DNS Account Settings

UPNP

Universal Plug and Play (UPnP) is a set of networking protocols that can allow networked devices, such as computers, printers, WiFi access points and mobile phones to automatically detect each other's presence on the network and establish functional network services for data sharing, communications, and entertainment.

UPnP Configuration

NOTE: UPnP is activated only when there is a live WAN service with NAT enabled.

☒ Enable UPnP

Figure 22: Advanced – UPnP

DNS PROXY

To enable DNS Proxy settings, select the corresponding checkbox and then enter the Host and Domain name, as in the example shown below. Click Apply/Save to continue.

DNS Proxy Configuration

☒ Enable DNS Proxy

Host name of the Broadband Router:

Domain name of the LAN network:

Figure 23: Advanced - DNS Proxy

The Host Name and Domain name are combined to form a unique label that is mapped to the router IP address. This can be used to access the user interface of the router with a local name rather than by using the router IP address.

DLNA

The DLNA page allows you to enable or disable and configure the digital media server. This means you can have digital media stored on an external USB hard drive connected to the GF1V and the router will make it accessible to other devices on your network.

Digital Media Server settings

This page allows you to enable / disable digital media server support.

☒ Enable on-board digital media server.

Interface Default ▾

Media Library Path /mnt/usb0_1

Apply/Save

Figure 24: Advanced - DLNA

Select Enable on-board digital media server and then use the drop down list to select the Interface. In the Media Library Path field, enter the path to the media. Click the Apply/Save button when you have finished.

PACKET ACCELERATION

Packet acceleration uses a number of methods to increase UFB WAN to LAN speeds. These can range from utilising locally terminated TCP connections to Fast Connection Setup.

Packet Acceleration

☒ Enable Packet Flow Accelerator

Apply/Save

Figure 25: Advanced - PacketAcceleration

Select to enable or disable Packet Acceleration and click Apply/Save to save the new packet acceleration configuration settings.

STORAGE SERVICE

The Storage Service options enable you to manage attached USB Storage devices and create accounts to access the data stored on the attached USB device.

STORAGE DEVICE INFO

The storage device info page displays information about the attached USB Storage device.

Storage Service

The Storage service allows you to use Storage devices with modem to be more easily accessed

Volume name	Physical Medium	File System	Total Space	Used Space
-------------	-----------------	-------------	-------------	------------

Figure 26: Advanced – Storage Service

USER ACCOUNTS

User accounts are used to restrict access to the attached USB Storage device.

To delete a User account entry, click the Remove checkbox next to the selected account entry and click Remove.

Click Add to create a user account.

Storage User Account Configuration

Choose Add, or Remove to configure User Accounts.

Username	Remove
----------	--------

Add Remove

Figure 27: Advanced – Storage Service – Storage User Account Configuration

Adding an account allows the creation of specific user accounts with a password to further control access permissions. To add an account, click the Add button and then enter the desired username and password for the account.

Storage User Account Setup

Please enter the username and password to be used for Network Attached Storage.
Username and Password must consists of [A-Z] or [a-z] or [0-9].

Username:

Password:

Confirm Password:

Apply/Save

Figure 28: Advanced – Storage Service – Storage User Account Setup

INTERFACE GROUPING

Port Mapping allows you to create groups composed of the various interfaces available in your router. These groups then act as separate networks.

To delete an Interface group entry, click the Remove checkbox next to the selected group entry and click Remove.

Interface Grouping -- A maximum 16 entries can be configured

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Group Name	Remove	WAN Interface	LAN Interfaces	Edit
Default		atm0.1	eth0	
			eth1	
			eth2	
			eth3	
			wl0	
			wl0.1	
			wl0.2	
			wl0.3	

Add Remove

Figure 29: Advanced - Interface Grouping

Click Add to create an Interface group.

Interface grouping Configuration

To create a new interface group:

1. Enter the Group name and the group name must be unique.
2. Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports.
3. Click Save/Apply button to make the changes effective immediately.

Group Name:

Grouped WAN Interfaces

Available WAN Interfaces

SlingshotUFB.10/ppp0.1

Grouped LAN Interfaces

Available LAN Interfaces

eth0
eth1
eth2
eth3
wl0
wl0.1
wl0.2
wl0.3

Apply/Save

Enter a group name and then use the arrow buttons to select which interfaces you wish to group. Click Apply/Save to save the Interface grouping configuration settings.

IP TUNNEL

The IP Tunnelling feature allows you to configure tunnelling of traffic between IPv6 and IPv4 networks.

IPv6inIPv4

IP Tunneling -- 6in4 Tunnel Configuration

Name	WAN	LAN	Dynamic	IPv4 Mask Length	6rd Prefix	Border Relay Address	Remove
<div> <div>Add</div> <div>Remove</div> </div>							

Figure 30: Advanced - IP Tunnel - IPv6inIPv4

Click the Add button to add a new tunnel.

IP Tunneling -- 6in4 Tunnel Configuration

Currently, only 6rd configuration is supported.

Tunnel Name:

Mechanism:

Associated WAN Interface:

Associated LAN Interface:

☒ Manual
 ☐ Automatic

IPv4 Mask Length:

6rd Prefix with Prefix Length:

Border Relay IPv4 Address:

Apply/Save

Figure 31: Advanced - IP Tunnel - IPv6inIPv4 - 6in4 Tunnel Configuration

IPv4inIPv6

IP Tunneling -- 4in6 Tunnel Configuration

Name	WAN	LAN	Dynamic	Remote Address	Remove
<div style="text-align: center;"> <input type="button" value="Add"/> <input type="button" value="Remove"/> </div>					

Figure 32: Advanced - IP Tunnel – IPv4inIPv6

Click the Add button to add a new tunnel.

IP Tunneling -- 4in6 Tunnel Configuration

Currently, only DS-Lite configuration is supported.

Tunnel Name:
 Mechanism: DS-Lite
 Associated WAN Interface:
 Associated LAN Interface: LAN/br0
☒ Manual ☐ Automatic
 Remote Address:

Figure 33: Advanced - IP Tunnel – IPv4inIPv6 - 4in6 Tunnel Configuration

IPSEC

The GF1V offers IPsec VPN tunnel functionality. To delete an IPsec entry, click the Remove checkbox next to the selected IPsec tunnel entry and click Remove.

Click Add to create a new IPsec tunnel connection.

IPSec Settings

IPSec Connection Name: new connection

Tunnel Mode: ESP

Remote IPSec Gateway Address (IPv4 address in dotted decimal): 0.0.0.0

Tunnel access from local IP addresses: Subnet

IP Address for VPN: 0.0.0.0

IP Subnetmask: 255.255.255.0

Tunnel access from remote IP addresses: Subnet

IP Address for VPN: 0.0.0.0

IP Subnetmask: 255.255.255.0

Key Exchange Method: Auto(IKE)

Authentication Method: Pre-Shared Key

Pre-Shared Key: key

Perfect Forward Secrecy: Disable

Advanced IKE Settings:

Figure 34: Advanced - IPsec

Enter the following parameters:

PARAMETER	DEFINITION
IPSec Connection Name	Enter a name to identify the IPsec tunnel
Tunnel Mode	Select the applicable IPsec tunnel mode
Remote IPSec Gateway	Enter the IP Address of the IPsec server to connect to
Tunnel access from Local	Select which remote addresses local IPsec connections are able to access
IP Address from VPN	Enter the IP Address to be used locally for the IPsec tunnel
Subnet mask for VPN	Enter the subnet mask to be used locally for the IPsec tunnel
Tunnel Access from Remote	Select which local addresses remote IPsec connections are able to access
IP Address for VPN	Enter the IP Address to be used on the remote end for the IPsec tunnel
Subnet mask for VPN	Enter the subnet mask to be used on the remote end for the IPsec tunnel
Key Exchange Method	Select the type of IPsec exchange is to be used on the IPsec tunnel
Authentication Method	Select the applicable authentication for the IPsec tunnel
Pre-Shared Key	Enter the pre-shared key (if applicable) to grant access to the IPsec tunnel
Perfect Forward Secrecy	Select to use Perfect Forward Secrecy during key exchange for the IPsec tunnel
Advanced IKE Settings	Configure advanced IKE settings for the IPsec tunnel such as the encryption method or key life time

After entering the required IPsec tunnel service settings, click Apply/Save to save the new IPsec Tunnel configuration settings.

CERTIFICATE LOCAL

Local Certificates

Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity.
Maximum 4 certificates can be stored.

Notice: Import and Remove Certificate need reboot the gateway

Name	In Use	Subject	Type	Action
Create Certificate Request		Import Certificate		

Figure 35: Advanced – Certificate - Local

TRUSTED CA

Trusted CA (Certificate Authority) Certificates

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates.
Maximum 4 certificates can be stored.

Notice: Import and Remove Certificate need reboot the gateway

Name	Subject	Type	Action
Import Certificate			

Figure 36: Advanced – Certificate – Trusted CA

POWER MANAGEMENT

The power management page enables you to control the green aspects of the GF1V.

You can enable or disable the power management features by selecting or unselecting the different power management functions as necessary and then click Apply to save these settings.

Power Management

This page allows control of Hardware modules to evaluate power consumption. Use the control buttons to select the desired option, click Apply and check the status response.

MIPS CPU Clock divider when Idle

☐ Enable Status: Disabled

Wait instruction when Idle

☒ Enable Status: Enabled

DRAM Self Refresh

☒ Enable Status: Enabled

Energy Efficient Ethernet

☒ Enable Status: Enabled

Ethernet Auto Power Down and Sleep

☒ Enable Status: Enabled

Number of ethernet interfaces:

Powered up: 0

Powered down: 5

Apply refresh

Figure 37: Advanced – Power Management

MULTICAST (IGMP CONFIGURATION)

The Internet Group Management Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships. IGMP is a protocol only used on the network between a host and the router. It allows a host to inform the router whenever that host needs to join or leave a particular multicast group. IGMP provides for more efficient allocation of resources when used with online gaming and video streaming.

IGMP Configuration

Enter IGMP protocol configuration fields if you want modify default values shown below.
NOTE: Query Interval is advised to no larger than 125s.

Default Version:

Query Interval (s):

Query Response Interval (1/10s):

Last Member Query Interval (1/10s):

Robustness Value:

Maximum Multicast Data Sources (for IGMPv3):

Fast Leave Enable: ☒

Membership Join Immediate (IPTV): ☐

MLD Configuration

Enter MLD protocol (IPv6 Multicast) configuration fields if you want modify default values shown below.

Default Version:

Query Interval (s):

Query Response Interval (1/10s):

Last Member Query Interval (1/10s):

Robustness Value:

Maximum Multicast Data Sources (for mldv2):

Fast Leave Enable: ☒

Figure 38: Advanced - IGMP Configuration

FIELD	DEFINITION
Default Version	The version IGMP in use by the router.
Query Interval	The hosts on the segment report their group membership in response to the router's queries. The query interval timer is also used to define the amount of time a router will store particular IGMP state if it does not hear any reports on the group. The query interval is the time in seconds between queries sent from the router to IGMP hosts.
Query Response Interval	When a host receives the query packet, it starts counting to a random value, less the maximum response time. When this timer expires, the host replies with a report, provided that no other host has responded yet. This accomplishes two purposes: a) Allows controlling the amount of IGMP reports sent during a time window. b) Engages the report suppression feature, which permits a host to suppress its own report and conserve bandwidth.
Last Member Query Interval	IGMP uses this value when router hears IGMP Leave report. This means that at least one host wants to leave the group. After router receives the Leave report, it checks that the interface is not configured for IGMP Immediate Leave (single-host on the segment) and if not, it sends out an out-of-sequence query.
Robustness Value	The robustness variable is a way of indicating how susceptible the subnet is to lost packets. IGMP can recover from robustness variable minus 1 lost IGMP packets. You can also click the scroll arrows to select a new setting. The robustness variable should be set to a value of 2 or greater. The default robustness variable value is 2.
Maximum Multicast Groups	The maximum number of multicast groups that the router can control at any one time.
Maximum Multicast Data Sources	The maximum number of data sources a multicast group can have.
Maximum Multicast Group Members	The maximum number of hosts a multicast group can have.
Fast Leave Enable	With IGMP fast-leave processing, which means that the router immediately removes the interface attached to a receiver upon receiving a Leave Group message from a IGMP host.

WIRELESS

BASIC

The Wireless Basic page allows you to enable the wireless network and configure its basic settings.

Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click 'Apply/Save' to configure the basic wireless options.

☒ Enable Wireless
☐ Enable Wireless Hotspot2.0 [WPA2 is required]
☐ Hide Access Point
☐ Clients Isolation
☐ Disable WMM Advertise
☒ Enable Wireless Multicast Forwarding (WMF)

SSID:
 BSSID:
 Country:
 Max Clients:

Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Isolate Clients	Enable WMM Advertise	Enable WMF	Enable HSPOT	Max Clients	BSSID
<input type="checkbox"/>	<input type="text" value="Slingshot 2 259"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	<input type="text" value="N/A"/>
<input type="checkbox"/>	<input type="text" value="Slingshot 3 259"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	<input type="text" value="N/A"/>
<input type="checkbox"/>	<input type="text" value="Slingshot 4 259"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	<input type="text" value="N/A"/>

Figure 39: Wireless - Basic

The following parameters are available:

PARAMETER	DEFINITION
Enable Wireless	Select to enable or disable the wireless network function
Hide Access Point	Select to hide or display the wireless network when an SSID scan is performed
Clients Isolation	Select to prevent clients on the wireless network being able to access each other
Disable WMM Advertise	Select to prevent the GF1V advertising its WMM function
Enable Multicast Forwarding (WMF)	Select to enable Wireless Multicast Forwarding. This can reduce latency and improve throughput for wireless clients
Max Clients	Enter the maximum number of wireless clients able to connect to the wireless network
Wireless Guest Network	Select to enable a separate Wireless Guest network, the same options are available for a Guest network as with the main system wireless network.

Click Apply/Save to save the new wireless configuration settings.

SECURITY

The GF1V supports all encryptions within the 802.11 standard. The factory default is WPA2-PSK. The GF1V also supports WPA, WPA-PSK, WPA2, WPA2-PSK. You can also select to enable WPS mode.

Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR:
through WiFi Protected Setup(WPS)
Note: When both STA PIN and Authorized MAC are empty, PBC is used. If Hide Access Point enabled or Mac filter list is empty with "allow" chosen, WPS2 will be disabled

WPS Setup

Enable WPS: Disabled ▾

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click 'Apply/Save' when done.

Select SSID: Slingshot Home WIFI 259 ▾

Network Authentication: WPA2 -PSK ▾

WPA/WAPI passphrase: ***** [Click here to display](#)

WPA Group Rekey Interval: 0

WPA/WAPI Encryption: AES ▾

Protect Management Frame: Disabled ▾

WEP Encryption: Disabled ▾

Apply/Save

Figure 40: Wireless -Security

The following parameters are available:

PARAMETER	DEFINITION
Enable WPS	Select to enable or disable the WPS function of the GF1V.
Select SSID	Select the SSID to apply the security settings to.
Network Authentication	Select the Wireless security type to use with the wireless network.
WPA/WAPI passphrase	Enter the security key to use with the wireless network.
WPA Group Rekey Interval	Enter the group rekey interval. This should not need to change.
WPA/WAPI Encryption	Select the type of encryption to use on the wireless network.
WEP Encryption	Select to utilise WEP encryption on the wireless network connection.

Click Apply/Save to save the new wireless security configuration settings.

MAC FILTER

MAC Filter allows you to add or remove the MAC Address of devices which will be allowed or denied access to the wireless network. First use the Select SSID drop down list to select the wireless network you wish to configure, then select to either allow or deny access to the MAC addresses listed.

Wireless -- MAC Filter

Select SSID: Slingshot Home WIFI 259 ▾

MAC Restrict Mode: ☒ Disabled ☐ Allow ☐ Deny

MAC Address Remove

Add Remove

Click Add to add a MAC Address Filter.

Wireless -- MAC Filter

Enter the MAC address and click 'Apply/Save' to add the MAC address to the wireless MAC address filters.

MAC Address:

Enter the MAC Address to be filtered and click Apply/Save to save the new MAC Address filter settings. To delete a MAC filter entry, click the Remove checkbox next to the selected filter entry and click Remove.

WIRELESS BRIDGE

Wireless Bridge allows you to configure the router's access point as a bridge.

Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access. Click "Refresh" to update the remote bridges. Wait for few seconds to update. Click "Apply/Save" to configure the wireless bridge options.

AP Mode:

Bridge Restrict:

Remote Bridges MAC Address:

Select the mode for the Wireless Access Point built into the GF1V. You can specify which wireless networks will be allowed to connect to the GF1V by using the 'Bridge Restrict' option and then entering the applicable MAC Addresses of the other wireless access points.

Click Apply/Save to save the new wireless bridge configuration settings.

ADVANCED

Advanced Wireless allows you to configure detailed wireless network settings such as the band, channel, bandwidth, transmit power and preamble settings.

Wireless -- Advanced

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used. Click 'Apply/Save' to configure the advanced wireless options.

Band:	<input type="button" value="2.4GHz"/>	
Channel:	<input type="button" value="Auto"/>	Current: 13 (interference: acceptable)
Auto Channel Timer(min)	<input type="text" value="0"/>	
802.11n/EWIC:	<input type="button" value="Auto"/>	
Bandwidth:	<input type="button" value="20MHz in Both Bands"/>	Current: 20MHz
Control Sideband:	<input type="button" value="Lower"/>	Current: N/A
802.11n Rate:	<input type="button" value="Auto"/>	
802.11n Protection:	<input type="button" value="Auto"/>	
Support 802.11n Client Only:	<input type="button" value="Off"/>	
RIFS Advertisement:	<input type="button" value="Off"/>	
OBSS Co-Existence:	<input type="button" value="Disable"/>	
RX Chain Power Save:	<input type="button" value="Disable"/>	Power Save status: Full Power
RX Chain Power Save Quiet Time:	<input type="text" value="10"/>	
RX Chain Power Save PPS:	<input type="text" value="10"/>	
54g Rate:	<input type="button" value="1 Mbps"/>	
Multicast Rate:	<input type="button" value="Auto"/>	
Basic Rate:	<input type="button" value="Default"/>	
Fragmentation Threshold:	<input type="text" value="2346"/>	
RTS Threshold:	<input type="text" value="2347"/>	
DTIM Interval:	<input type="text" value="1"/>	
Beacon Interval:	<input type="text" value="100"/>	
Global Max Clients:	<input type="text" value="16"/>	
XPress Technology:	<input type="button" value="Enable"/>	
Transmit Power:	<input type="button" value="100%"/>	
WMM(Wi-Fi Multimedia):	<input type="button" value="Enabled"/>	
WMM No Acknowledgement:	<input type="button" value="Disabled"/>	
WMM APSD:	<input type="button" value="Enabled"/>	

Click Apply/Save to save any changes to the wireless network settings configuration.

PARAMETER	DEFINITION
Band	You can select 2.4GHz or 5GHz.
Channel	Fill in the appropriate channel to correspond with your network settings. All devices in your wireless network must use the same channel in order to work correctly. This router supports auto channeling functionality.
Auto Channel Timer(min)	Specifies the timer of auto channelling.
802.11n/EWC	Select disable 802.11n or Auto.
Bandwidth	Select the bandwidth for the network. You can select 20MHz in Both Bands, 20MHz in 2.4G Band and 40MHz in 5G Band, or 40MHz in Both Bands.
Control Sideband	If you select 20MHz in Both Bands or 20MHz in 2.4G Band and 40MHz in 5G Band, the service of control sideband does not work. When you select 40MHz in Both Bands as the bandwidth, the following page appears. Then you can select Lower or Upper as the value of sideband. As the control sideband, when you select Lower, the channel is 1~7. When you select Upper, the channel is 5~11.
802.11nRate	Select the transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select Auto to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is Auto.
802.11nProtection	The 802.11n standards provide a protection method so 802.11b/g and 802.11n devices can co-exist in the same network without "speaking" at the same time.
Support 802.11n Client Only	Only stations that are configured in 802.11n mode can associate.
Multicast Rate	Select the multicast transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select Auto to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is Auto.
Basic Rate	Select the basic transmission rate ability for the AP.
Fragmentation Threshold	Packets that are larger than this threshold are fragmented into multiple packets. Try to increase the fragmentation threshold if you encounter high packet error rates. Do not set the threshold too low, since this can result in reduced networking performance.
RTS Threshold	This value should remain at its default setting of 2347. Should you encounter inconsistent data flow, only minor reductions are recommended. Should you encounter inconsistent data flow, only minor reduction of the default value, 2347, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of 2347.
DTIM Interval	(Delivery Traffic Indication Message) Enter a value between 1 and 255 for the Delivery Traffic Indication Message (DTIM.) A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.
Beacon Interval	A beacon is a packet of information that is sent from a connected device to all other devices where it announces its availability and readiness. A beacon interval is a period of time (sent with the beacon) before sending the beacon again. The beacon interval may be adjusted in milliseconds (ms). Default (100) is recommended.
XPress Technology	Select Enable or Disable. This is a special accelerating technology for IEEE802.11g. The default is Disabled.
Transmit Power	Adjust the transmission range here. This tool can be helpful for security purposes if you wish to limit the transmission range.
WMM (Wi-Fi Multimedia)	Select whether WMM is enable or disabled. Before you disable WMM, you should understand that all QoS queues or traffic classes relate to wireless do not take effects.
WMM No Acknowledgement	Select whether ACK in WMM packet. By default, the 'Ack Policy' for each access category is set to Disable, meaning that an acknowledge packet is returned for every packet received. This provides a more reliable transmission but increases traffic load, which decreases performance. To disable the acknowledgement can be useful for Voice, for example, where speed of transmission is important and packet loss is tolerable to a certain degree.
WMM APSD	APSD is short for automatic power save delivery, Selecting enable will make it has very low power consumption. WMM Power Save is an improvement to the 802.11e amendment adding advanced power management functionality to WMM.

STATION INFO

This page shows the MAC address of authenticated wireless stations that are connected to the GF1V and their status

Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

MAC	Associated	Authorized	SSID	Interface
-----	------------	------------	------	-----------

Refresh

VOICE

This section explains how to configure the VoIP settings of the GF1V.

VOIP STATUS

The Voice Status page displays the registration status of your SIP accounts and the total call time of each account.

Voice -- Voice Status

Account denial will display "Disabled", registered successfully will display "Up", and unregistered will display "Down".

SIP Account	call time	User Accounts	Registration Status
1	0:00:00		Down
2	0:00:00		Down

SIP BASIC SETTING

The SIP Settings page is where you enter your VOIP service settings as supplied by your VOIP service provider (VSP). If you are unsure about a specific setting or have not been supplied information for a particular field, please contact your VOIP service provider to verify if this setting is needed or not.

Voice -- SIP Basic Setting

Bound Interface Name: Any_WAN (Note: Requires vodsl restart to take affect)

Country : NZL - NEWZEALAND

sip local port(1-65535): 5060

SIP domain name*:

☐ Use SIP Proxy.

☐ Use SIP Outbound Proxy.

☐ Use SIP Registrar.

☐ Use SIP Proxy2.

☐ Use SIP Outbound Proxy2.

☐ Use SIP Registrar2.

SIP Account	0	1
Account Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Polarity Reverse Enable	<input type="checkbox"/>	<input type="checkbox"/>
Authentication name	<input type="text"/>	<input type="text"/>
Password	<input type="text"/>	<input type="text"/>
Cid Name	<input type="text"/>	<input type="text"/>
Cid Number	<input type="text"/>	<input type="text"/>

codec--line	ptime(ms)	priority	enable	codec--line	ptime(ms)	priority	enable
G711U	20	1 (1-100)	<input checked="" type="checkbox"/>	G711U	20	1 (1-100)	<input checked="" type="checkbox"/>
G711A	20	2 (1-100)	<input checked="" type="checkbox"/>	G711A	20	2 (1-100)	<input checked="" type="checkbox"/>
G729	20	3 (1-100)	<input checked="" type="checkbox"/>	G729	20	3 (1-100)	<input checked="" type="checkbox"/>
G723_63	30	4 (1-100)	<input checked="" type="checkbox"/>	G723_63	30	4 (1-100)	<input checked="" type="checkbox"/>
G726_24	20	5 (1-100)	<input checked="" type="checkbox"/>	G726_24	20	5 (1-100)	<input checked="" type="checkbox"/>
G726_32	20	6 (1-100)	<input checked="" type="checkbox"/>	G726_32	20	6 (1-100)	<input checked="" type="checkbox"/>
G726_16	20	7 (1-100)	<input checked="" type="checkbox"/>	G726_16	20	7 (1-100)	<input checked="" type="checkbox"/>
G726_40	20	8 (1-100)	<input checked="" type="checkbox"/>	G726_40	20	8 (1-100)	<input checked="" type="checkbox"/>
G722	20	9 (1-100)	<input checked="" type="checkbox"/>	G722	20	9 (1-100)	<input checked="" type="checkbox"/>

Apply

The individual fields shown above on the SIP Basic Settings page are explained in the following table.

OPTION	DEFINITION
Bound Interface Name	Select the Interface that the VoIP account will use to make a connection to the VoIP Service Provider.
SIP Local Port	Set the SIP local port of the gateway, the default value is 5060. SIP local port is the SIP UA (user agent) port.
SIP domain name	Enter the SIP domain name or IP address of your VoIP Service Provider here.
Use SIP Proxy	Select the checkbox of Use SIP Proxy, if your DSL router uses a SIP proxy. SIP proxy allows other parties to call DSL router through it. When it is selected, the following fields appear.
SIP Proxy	The IP address of the proxy.
SIP Proxy port	The port that this proxy is listening on. By default, the port value is 5060.
Use SIP Outbound Proxy	Some network service providers require the use of an outbound proxy. This is an additional proxy, through which all outgoing calls are directed. In some cases, the outbound proxy is placed alongside the firewall and it is the only way to let SIP traffic pass from the internal network to the Internet. When it is selected, the following fields appear.
SIP Outbound Proxy	The IP address of the outbound proxy.
SIP Outbound Proxy port	The port that the outbound proxy is listening on. By default, the port value is 5060.
Use SIP Registrar	Select this option if required by your VoIP Service Provider. Enter the SIP Proxy Domain Name and SIP Proxy Port which is typically 5060.
SIP Registrar	The IP address of the SIP registrar.
SIP Registrar port	The port that SIP registrar is listening on. By default, the port value is 5060.
Account Enabled	If it is unselected, the corresponding account is disabled. You can not use it to initiate or accept any call.
Polarity Reverse Enable	Enable or disable this function.
Authentication name	Set the user name of authentication.
Password	Set the password of authentication.
Cid Name	User name. It is the Display Name.
Cid Number	Set the caller number. It must be a number of 0~9.
Priority	The priority of codec is declined from up to down. Codecs define the method of relaying voice data. Different codecs have different characteristics, such as data compression and voice quality. For Example, G723 is a codec that uses compression, therefore, it is good for use where the bandwidth is limited but its voice quality is not good as other codecs, such as the G711. If you specify none of the codecs, using the default value showed in the above figure, the DSL router chooses the codec automatically.

After entering your VoIP settings press the Apply button. Select Management > Save/Reboot and press the Reboot button. Once the router restarts if there is a valid internet connection and the VoIP account settings are valid the VoIP service will start.

SIP ADVANCED

The SIP Advanced page allows you to configure settings that your VoIP service provider has enabled on your SIP account and if you have the appropriate call features and other functionality on your cordless or corded phone handsets.

Voice -- SIP Advanced Setting

Line	1	2
Call waiting	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Unconditionally Call forwarding number		
Busy Call forwarding number		
No Answer Call forwarding number		
Options Time	0	0
Forward unconditionally	<input type="checkbox"/>	<input type="checkbox"/>
Forward on "busy"	<input type="checkbox"/>	<input type="checkbox"/>
Forward on "no answer"	<input type="checkbox"/>	<input type="checkbox"/>
MWI	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Anonymous call blocking	<input type="checkbox"/>	<input type="checkbox"/>
Anonymous calling	<input type="checkbox"/>	<input type="checkbox"/>
Anonymous calling mode	Display anonymous	Display anonymous
DND	<input type="checkbox"/>	<input type="checkbox"/>
Enable Call Return	<input type="checkbox"/>	<input type="checkbox"/>
Call Transfer	<input type="checkbox"/>	<input type="checkbox"/>
Call conference	<input type="checkbox"/>	<input type="checkbox"/>
Warm Line	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Warm Line URI		
Warm Line Delay Timer	10	10

==Fax Setting==
 Fax Negotiate Mode: **Negotiate**

☒ Enable T38 support
☐ Enable vbd support
☐ Enable T38 redundancy support
☐ Enable vbd redundancy support

==Settings==
☐ Enable VAD support VAD mode in signal: **None**
☐ Enable Echo Cancellation
☐ Enable # To ASCII

==SIP Timer Setting==
 Registration Expire Timeout: 3600
 Session Expire Timeout: 1800
 Min Session Expire Time: 90 (need >= 90s)

==Digitmap Setting==
 Voip Dialplan Setting: [2-9]xxxxxxxx[034679]xx
 PSTN Prefix: 0 [Blank to turn off otherwise set a DTMF digit]

==Qos Setting==
 DSCP for SIP: **EF (101110)**
 DSCP for RTP: **EF (101110)**

==Payload Setting==
 RFC2198 Payload Value: 125 (range 97~127)
 Dtmf Relay setting: **RFC2833** payload value 120 (range 97~127)

==Call ID Setting==
 Caller ID send Delay Time: 600 (range 500~1500ms)
 Caller ID Message Type: **FSK_MDMF**
 FSK modulation Mode: **BellcoreGen**

==Transport Setting==
 SIP Transport protocol: **UDP**

==SIP Extends==
 PRACK (100rel): **SUPPORTED**

==Service Offer Setting==
 Complementary business modals: **Local model**

Apply

Figure 41: VoIP - Advanced - Service Provider

OPTION	DEFINITION
Line	Displays the line number you want to configure
Call Waiting	Select this option for your phone if your VoIP Service Provider has enabled Call Waiting on your SIP account.
Unconditionally Call forwarding number	Select this option if your VoIP Service Provider has enabled Call Forwarding on your SIP account and you wish to use this feature.
Busy Call Forwarding Number	Enter the phone number to forward a call to if it arrives while the line is busy.
No Answer Call forwarding number	Enter the phone number to forward a call to if the call is not answered.
Forward On "busy"	Select this option if your VoIP Service Provider has enabled Call Forwarding on your SIP account and you wish to use this feature.
Forward On "No Answer"	Select this option if your VoIP Service Provider has enabled Call Forwarding on your SIP account and you wish to use this feature.
MWI (Message Waiting Indicator)	Select this option if your VoIP Service Provider has enabled MWI (Message Waiting Indicator) on your SIP account and you wish to use this feature.
Anonymous Call Blocking	Select this option if your VoIP Service Provider has enabled Anonymous Call Blocking on your SIP account and you wish to use this feature.
Anonymous Calling	Select this option if your VoIP Service Provider has enabled Anonymous Calling on your SIP account and you wish to use this feature.

Anonymous calling mode	When set to Display anonymous, the modem hides your caller ID. When set to All anonymous, the modem hides both caller ID and the SIP URL of the originating call.
DND (Do Not Disturb)	Select this option if your VoIP Service Provider has enabled DND (Do Not Disturb) on your SIP account and you wish to use this feature.
Enable T38 Redundancy Support	Select this function if you wish to send or receive faxes via VoIP and have a fax machine capable of using the T38 fax over VoIP protocol.
Enable VBD redundancy support	Select this checkbox to use the feature.
Enable VAD support	Enables the Voice Activated Detection function of the modem.
Enable RTCP Flow Control	Select this checkbox to use the feature.
Enable Echo Cancellation	Select this checkbox to use the feature.
Enable #ToASCII	Select this checkbox to use the feature.
Enable Reinjection Function	Select this checkbox to use the feature.
RFC2198 Payload Value (range 97-127)	Enter the RFC2198 payload value that the valid range is 96 ~ 127.
Registration Expire Timeout	Enter the registration expire timeout.
Session Expire Time	The interval of dialog refreshing time.
Min Session Expire Time	The minimum interval of dialog refreshing time.
VoIP DialPlan Setting	Set the VoIP dial plan. If user-dialed number matches it, the number is processed by the DSL router immediately.
DSCP for SIP	Set the DSCP for SIP. You can select it from the drop-down list.
DSCP for RTP	Set the DSCP for RTP. You can select it from the drop-down list.
Dtmf Relay Setting	Set DTMF transmit method, which can be following values: – SIP Info: Use SIP INFO message to transmit DTMF digits. – RFC2833: Use RTP packet to encapsulate DTMF events, as specified in RFC 2833. – InBand: DTMF events are mixed with user voice in RTP packet.
SIP Transport Protocol	Select the transport protocol to use for SIP signaling. Note that the SIP proxy and registrar need to support the protocol you select.
Enable Local Supplementary Service	Select the checkbox to enable the supplementary service settings by the telephone set. If you deselect the checkbox, the supplementary service can not be set by the telephone set.

Table 4: VoIP - Advanced - Service Provider

SIP EXTRA SETTING

This page displays additional settings related to the SIP service.

Voice -- SIP Extra Settings

Line	1	2	
Dial tone time	15	15	10 ~ 20
Busy tone time	40	40	30 ~ 180
Inter digit time	5	5	1 ~ 5
Offhook warning tone time	60	60	30 ~ 180
Ringback tone time	80	80	30 ~ 180
T digit timer	4		
Short digit timer	4		

Apply

PARAMETER	DEFINITION
Dial tone time	Dial tone duration.
Busy tonetime	Busy tone duration.
Inter digit time	The valid range is 1 ~ 5.
Offhook warning tone time	Offhook warning tone duration.
Ringback tone time	Ringback tone duration.

SIP DEBUG SETTING

This page allows you to configure various settings regarding the logging levels of the SIP service.

Voice -- SIP Debug Setting

Vodsi Console Log Level:

System Log Level:

Protocol Stack Log Level:

Call Control Log Level:

Register Log Level:

DSP Log Level:

Tele Log Level:

Dialplan Log Level:

Restart Log Level:

==Master level control on modules: when debug the modules log level must be higher then master level ==

Master Level:

LOGIC:

PROVISION:

VOICE:

AGENT:

SIP log server IP Address*:

SIP log server port*:

Line	1	2
Ingress gain	<input type="text" value="0"/>	<input type="text" value="0"/>
Egress gain	<input type="text" value="0"/>	<input type="text" value="0"/>

OPTION	DEFINITION
SIP Log Server IP Address	Enter the IP address where the SIP Log data for the router's currently saved VoIP account settings will be sent to.
SIP Log Server port	Enter the port to be used for transmitting the SIP Log data for the router's currently saved VoIP account settings.
Ingress Gain	The incoming signal amplitude can be controlled with this field. Combined with the Egress gain a ratio can be expressed of input to output. The Ingress Gain setting can help improve the quality of the VoIP line, and can influence call volumes and help eliminate echoes.
Egress Gain	The outgoing signal amplitude can be controlled with this field. Combined with the Ingress gain a ratio can be expressed of input to output. The Egress Gain setting can help improve the quality of the VoIP line, and can influence call volumes and help eliminate echoes.

DIAGNOSTICS

This page is used to test the connection to your local network, and the connection to your Internet service provider. You may diagnose the connection by clicking the Test button or click the Test With OAM F4 button. If the test continues to fail, click Help and follow the troubleshooting procedures.

DIAGNOSTICS

The Diagnostics menu provides feedback on the connection status of the device. The individual tests are listed below. If a test displays a fail status:

1. Click on the Help link and follow the troubleshooting procedures in the Help screen that appears.
2. Now click Rerun Diagnostic Tests at the bottom of the screen to re-test and confirm the error.
3. If the test continues to fail, contact Technical Support.

br_0_0_35 Diagnostics

Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network

Test your eth0 Connection:	PASS	Help
Test your eth1 Connection:	FAIL	Help
Test your eth2 Connection:	FAIL	Help
Test your eth3 Connection:	FAIL	Help
Test your Wireless Connection:	PASS	Help

Test the connection to your DSL service provider

Test xDSL Synchronization:	FAIL	Help
Test ATM OAM F5 segment ping:	DISABLED	Help
Test ATM OAM F5 end-to-end ping:	DISABLED	Help

FIELD	DESCRIPTION
ethConnection	Pass: Indicates the Ethernet connection to your computer is connected to the LAN port of the router. Fail: Indicates that the router does not detect the Ethernet interface of your computer.
Test your Wireless Connection	Pass: Indicates that the wireless card is switched ON. Fail: Indicates that the wireless card is switched OFF.

MANAGEMENT

SETTINGS

The Settings screens allow you to back up, retrieve and restore the default settings of your Router. It also provides a function for you to update your router's firmware.

BACKUP

The following screen appears when Backup is selected. Click the Backup Settings button to save the current configuration settings.

You will be prompted for the location to save the backup file to on your PC.

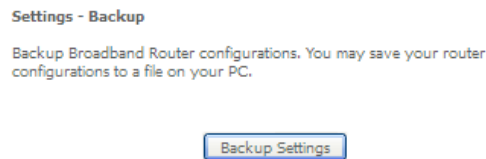
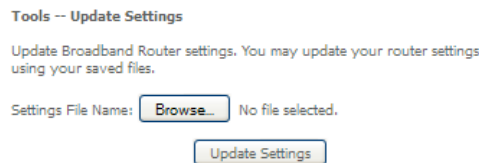


Figure 42: Management - Device Settings –Backup

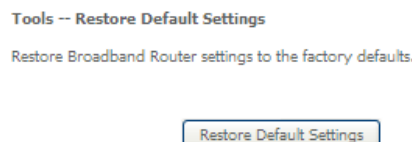
UPDATE SETTINGS

The following screen appears when selecting Update from the Settings submenu. By clicking on the Browse button, you can locate a previously saved filename as the configuration backup file. Click on the Update settings button to upload the selected file.



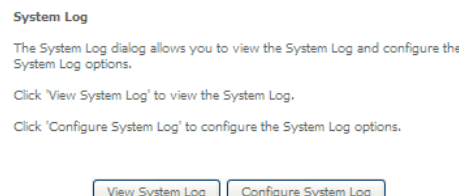
RESTORE DEFAULT

The following screen appears when selecting Restore Default from the Settings submenu. By clicking on the Restore Default Settings button, you can restore your Routers default firmware settings. To restore system settings, reboot your Router.



SYSTEM LOG

The System log page allows you to view the log of the router and configure the logging level also. To view the system log, click the View System Log button.



To configure the system log, click the Configure System Log button.

System Log -- Configuration

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Apply/Save' to configure the system log options.

Log: ☐ Disable ☒ Enable

Log Level:

Display Level:

Mode:

ACCESS CONTROL

The Access Control option found in the Management drop down menu configures access related parameters in the following three areas:

- Passwords
- Services Control

Access Control is used to control local and remote management settings for your router.

PASSWORDS

The Passwords option configures your account access password for your modem. Access to the device is limited to the following three user accounts:

- admin is to be used for local unrestricted access control
- support is to be used for remote maintenance of the device
- user is to be used to view information and update device firmware

Use the fields illustrated in the screen below to change or create your password. Passwords must be 16 characters or less with no spaces. Click the Apply/Save button after making any changes to continue.

Access Control -- Passwords

Access to your DSL router is controlled through three user accounts: admin, support and user .

The username "admin" has unrestricted access to change and view configuration of your DSL Router.

The username "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.

The username "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 15 characters and click 'Apply/Save' to change or create passwords. Note: Password cannot contain a space.

Username:

New Username:

Old Password:

New Password:

Confirm Password:

SERVICES

The Service Control List (SCL) allows you to enable or disable your Local Area Network (LAN) or Wide Area Network (WAN) services by ticking the checkbox as illustrated below. The following access services are available: FTP, HTTP, ICMP, SAMBA, SNMP, SSH, TELNET, and TFTP. Click the Apply/Save button after making any changes to continue.

Access Control -- Services

Services access control list (SCL) enable or disable the running services.

Services	LAN	LAN Port	WAN	Port
HTTP	<input checked="" type="checkbox"/> enable	80	<input type="checkbox"/> enable	80
TELNET	<input checked="" type="checkbox"/> enable	23	<input type="checkbox"/> enable	23
SSH	<input type="checkbox"/> enable	22	<input type="checkbox"/> enable	22
FTP	<input type="checkbox"/> enable	21	<input type="checkbox"/> enable	21
TFTP	<input type="checkbox"/> enable	69	<input type="checkbox"/> enable	69
ICMP	<input checked="" type="checkbox"/> enable	0	<input checked="" type="checkbox"/> enable	0
SAMBA	<input checked="" type="checkbox"/> enable	445	<input type="checkbox"/> enable	445

Apply/Save

UPDATE SOFTWARE

The following screen appears when selecting the Update Software option from the Management menu. By following this screen's steps, you can update your modem's firmware. Manual device upgrades from a locally stored file can also be performed using the following screen.

1. Obtain an updated software image file.
2. Enter the path and filename of the firmware image file in the Software File Name field or click the Browse button to locate the image file.
3. Click the Update Software button once to upload and install the file.

Tools -- Update Software

Step 1: Obtain an updated software image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the 'Browse' button to locate the image file.

Step 3: Click the 'Update Software' button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your Broadband Router will reboot.

Software File Name: No file selected.

SAVE/REBOOT

This option reboots the GF1V.

Click the button below to reboot the router.

Figure 43: Management - Reboot

NOTE 1: It may be necessary to reconfigure your TCP/IP settings to adjust for the new configuration. For example, if you disable the Dynamic Host Configuration Protocol (DHCP) server you will need to apply Static IP settings.

NOTE 2: If you lose all access to your web user interface, simply press the reset button on the rear panel for 3 seconds to restore default settings.

ADDITIONAL PRODUCT INFORMATION

ESTABLISHING A WIRELESS CONNECTION

WINDOWS XP (SERVICE PACK 3)

1. Open the Network Connections control panel (Start -> Control Panel -> Network Connections):
2. Right-click on your Wireless Network Connection and select View Available Wireless Networks:
3. Select the wireless network and click Connect.
4. Enter the network key.
5. The connection will show Connected.

WINDOWS VISTA

1. Open the Network and Sharing Center (Start > Control Panel > Network and Sharing center).
2. Click on "Connect to a network".
3. Choose "Connect to the Internet" and click on "Next".
4. Select the wireless network and click Connect.
5. Enter the network key.
6. Select the appropriate location. This will affect the firewall settings on the computer.
7. Click on both "Save this network" and "Start this connection automatically" and click "Next".

WINDOWS 7

1. Open the Network and Sharing Center (Start > Control Panel > Network and Sharing center).
2. Click on "Change Adapter settings" on the left-hand side.
3. Right-click on "Wireless Network Connection" and select "Connect / Disconnect".
4. Select the wireless network and click Connect.
5. Enter the network key.
6. You may then see a window that asks you to "Select a location for the 'wireless' network". Please select the "Home" location.
7. You may then see a window prompting you to setup a "HomeGroup". Click "Cancel" on this.
8. You can verify your wireless connection by clicking the "Wireless Signal" indicator in your system tray.
9. After clicking on this, you should see an entry matching the SSID of your GF1V with "Connected" next to it.

MAC OSX 10.6

1. Click on the Airport icon on the top right menu.
2. Select the wireless network and click Connect.
3. On the new window, select "Show Password", type in the network in the Password field and then click on OK.
4. To check the connection, click on the Airport icon and there should be a tick on the wireless network name.



Note: For other operating systems, or if you use a wireless adaptor utility to configure your wireless connection, please consult the wireless adapter documentation for instructions on establishing a wireless connection.

TROUBLESHOOTING

USING THE INDICATOR LIGHTS (LEDs) TO DIAGNOSE PROBLEMS

The LEDs are useful aides for finding possible problem causes.

POWER LED

The Power LED does not light up.

STEP	CORRECTIVE ACTION
1	Make sure that the GF1V power adaptor is connected to the device and plugged in to an appropriate power source. Use only the supplied power adaptor.
2	Check that the GF1V and the power source are both turned on and device is receiving sufficient power.
3	Turn the GF1V off and on.
4	If the error persists, you may have a hardware problem.

WEB CONFIGURATION

I cannot access the web configuration pages.

STEP	CORRECTIVE ACTION
1	Make sure you are using the correct IP address of the GF1V. You can check the IP address of the device from the Network Setup configuration page.
2	Check that you have enabled remote administration access. If you have configured an inbound packet filter, ensure your computer's IP address matches it.
3	Your computer's and the GF1V's IP addresses must be on the same subnet for LAN access. You can check the subnet in use by the router on the Network Setup page.
4	If you have changed the devices IP address, then enter the new one as the URL you enter into the address bar of your web browser.
5	If you are still not able to access the web configuration pages, reset the router to the factory default settings by pressing the reset button for 3 seconds and then releasing it. When the Power LED begins to blink, the defaults have been restored and the GF1V restarts. Navigate to 192.168.1.1 in your web browser and enter "admin" (without the quotes) as the username and the last 6 characters of the <MAC> address as the password.

The web configuration does not display properly.

STEP	CORRECTIVE ACTION
1	Delete the temporary web files and log in again. In Internet Explorer, click Tools, Internet Options and then click the Delete Files ... button. When a Delete Files window displays, select Delete all offline content and click OK. (Steps may vary depending on the version of your Internet browser.)

LOGIN USERNAME AND PASSWORD

I forgot my login username and/or password.

STEP	CORRECTIVE ACTION
1	Press the Reset button for 3 seconds, and then release it. When the Power LED begins to blink, the defaults have been restored and the GF1V restarts. You can now login with the factory default username and password "admin" (without the quotes) as the username and the last 6 characters of the <MAC> address as the password.
2	It is highly recommended to change the default username and password. Make sure you store the username and password in a safe place.

WLAN INTERFACE

I cannot access the GF1V from the WLAN or ping any computer on the WLAN.

STEP	CORRECTIVE ACTION
1	Check the Wi-Fi LED on the front of the unit and verify the WLAN is enabled as per the LED Indicator section.
2	If you are using a static IP address for the WLAN connection, make sure that the IP address and the subnet mask of the GF1V and your computer(s) are on the same subnet. You can check the routers configuration from the Network Setup page.

QUALITY OF SERVICE (QOS) CONFIGURATION EXAMPLES

LIMITING THE UPSTREAM RATE

- By default, a QoS queue is created when a WAN interface is created. On the QoS Queue page, enable the queue for eth4(WAN) interface and type in a name for the queue.

Limiting	33	eth4	1	1/SP						<input checked="" type="checkbox"/>	<input type="checkbox"/>
----------	----	------	---	------	--	--	--	--	--	-------------------------------------	--------------------------

- On the QoS Classification page, add a rule to limit the upstream rate, for example:

Classification Criteria:

Class Interface: LAN

Ether type: IP

Classification Results:

Class Queue: the queue that was enabled in Step 1

Set rate-limit: set according to your preference

Add Network Traffic Class Rule

This screen creates a traffic class rule to classify the ingress traffic into a priority queue and optionally mark the DSCP or Ethernet priority of the packet. Click 'Apply/Save' to save and activate the rule.

Traffic Class Name:	Upstream
Rule Order:	Last
Rule Status:	Disable

Specify Classification Criteria (A blank criterion indicates it is not used for classification.)

Class Interface:	LAN
Ether Type:	IP (0x800)
Source MAC Address:	
Source MAC Mask:	
Destination MAC Address:	
Destination MAC Mask:	
Source IP Address[/Mask]:	
Destination IP Address[/Mask]:	
Differentiated Service Code Point (DSCP) Check:	
Protocol:	

Specify Classification Results (A blank value indicates no operation.)

Specify Class Queue (Required): ppp0.1ð4(wan)&Key33&Pre1

- Packets classified into a queue that exit through an interface for which the queue is not specified to exist, will instead egress to the default queue on the interface.

Mark Differentiated Service Code Point (DSCP):

Mark 802.1p priority:

- Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits.
 - Class vlan packets egress to a non-vlan interface will have the packet p-bits re-marked by the class rule p-bits. No additional vlan tag is added.
 - Class non-vlan packets egress to a vlan interface will be tagged with the interface VID and the class rule p-bits.
 - Class vlan packets egress to a vlan interface will be additionally tagged with the packet VID, and the class rule p-bits.

Set Rate Limit: 800 [Kbits/s]

Apply/Save

- Click Apply/Save.

LIMITING THE DOWNSTREAM RATE

1. Navigate to the QoS Queue page to add a queue for the LAN interface, for example:

QoS Queue Configuration

This screen allows you to configure a QoS queue and add it to a selected layer2 interface.

Name:

Enable:

Interface:

Queue Precedence: (lower value, higher priority)

- The precedence list shows the scheduler algorithm for each precedence level.
 - Queues of equal precedence will be scheduled based on the algorithm.
 - Queues of unequal precedence will be scheduled based on SP.

2. On the QoS Classification page, add a rule to limit the downstream rate, for example:

Classification Criteria:

Class Interface: the appropriate WAN interface

Classification Results:

Class Queue: the queue that was created on Step 1

Set rate-limit: set according to your preference

Add Network Traffic Class Rule

This screen creates a traffic class rule to classify the ingress traffic into a priority queue and optionally mark the DSCP or Ethernet priority of the packet. Click 'Apply/Save' to save and activate the rule.

Traffic Class Name:

Rule Order:

Rule Status:

Specify Classification Criteria (A blank criterion indicates it is not used for classification.)

Class Interface:

Ether Type:

Source MAC Address:

Source IP Address/Mask:

Destination IP Address/Mask:

Protocol:

Specify Classification Results (A blank value indicates no operation.)

Specify Class Queue (Required):

- Packets classified into a queue that exit through an interface for which the queue is not specified to exist, will instead egress to the default queue on the interface.

Mark 802.1p priority:

- Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits.
 - Class vlan packets egress to a non-vlan interface will have the packet p-bits re-marked by the class rule p-bits. No additional vlan tag is added.
 - Class non-vlan packets egress to a vlan interface will be tagged with the interface VID and the class rule p-bits.
 - Class vlan packets egress to a vlan interface will be additionally tagged with the packet VID, and the class rule p-bits.

Set Rate Limit: x [Kbits/s]

3. Click Apply/ Save

The QoS Classification table looks like this:

QoS Classification Setup -- maximum 32 rules can be configured.

To add a rule, click the Add button.
 To remove rules, check their remove-checkboxes, then click the Remove button.
 The Enable button will scan through every rule in the table. Rules with enable-checkbox checked will be enabled. Rules with enable-checkbox un-checked will be disabled.
 The enable-checkbox also shows status of the rule after page reload.
 If you disable WMM function in Wireless Page, classification related to wireless will not take effects

		CLASSIFICATION CRITERIA												CLASSIFICATION RESULTS						
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ Prefix.length	DstIP/ Prefix.length	Proto	SrcPort	DstPort	DSCP Check	TC Check	802.1P Check	Queue Key	DSCP Mark	TC Mark	802.1P Mark	Rate Limit (Kbps)	Enable	Remove
Upstream	1	LAN	IP											33				800	<input type="checkbox"/>	<input type="checkbox"/>
Downstream	2	ppp0.1	IP											34				100	<input type="checkbox"/>	<input type="checkbox"/>
<div>AddEnableRemove</div>																				

TECHNICAL DATA

The following table lists the hardware specifications of the GF1V.

MODEL	GF1V
Ethernet WAN	1 x Gigabit WAN port (10/100/1000 Mbps)
Connectivity	4 x 10/100/1000 Mbps, 1 x WLAN
LED Indicators	Power, WAN, INTERNET, LAN 1-4, WLAN, WPS, FXS1, FXS2, USB.
Operating Temperature	Operating temperature: 0°C - 40°C, Humidity: 10%-90% non-condensing Storage temperature: -10°C - 70°C, Humidity: 0%-95% non-condensing
Power Input	12V DC - 1A
Dimensions & Weight	170 mm (H) x 45 mm (D) x 190 mm 343 grams

ELECTRICAL SPECIFICATIONS

It is recommended that the GF1V be powered by the supplied 12V DC, 1A power supply. A replacement power supply is available from the Energy Imports Online shop.

ENVIRONMENTAL SPECIFICATIONS / TOLERANCES

The GF1V housing enables it to operate over a wide variety of temperatures from 0°C - 40°C (operating temperature).