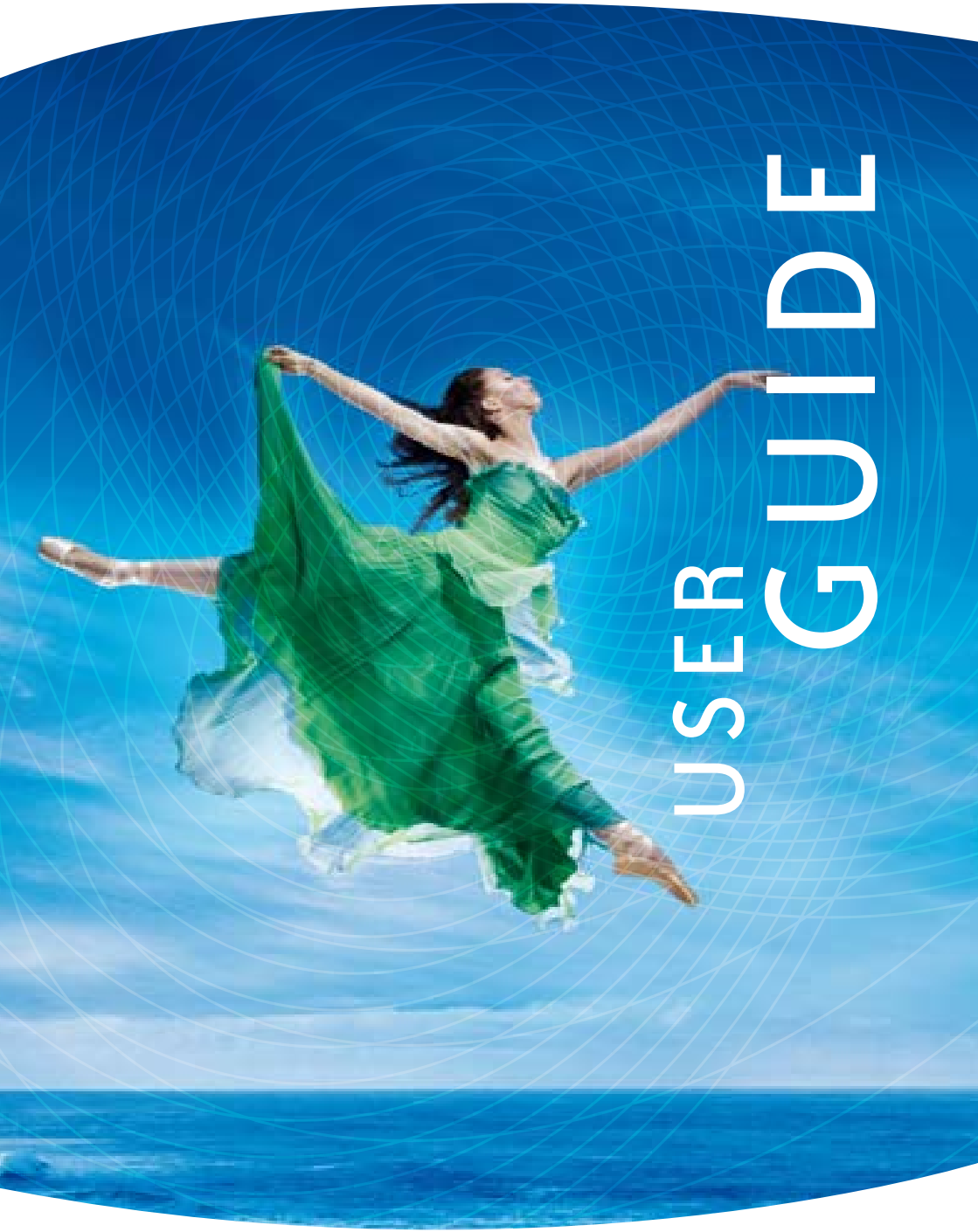

USER GUIDE

TABLE OF CONTENTS

1 – INTRODUCTION 5
1.1 FEATURES 6
1.2 PACKAGE CONTENTS 7
1.3 LED INDICATORS 8
1.4 PANELS 9

2 – QUICK SETUP (WITH USB KEY) 11
2.1 SETUP PROCEDURE 11

3 – ADVANCED SETUP (WITHOUT USB KEY) 13
3.1 SETUP PROCEDURE 13
3.2 TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL (TCP/IP) SETTINGS .. 13
3.3 DEFAULT SETTINGS 20
3.4 LOGIN PROCEDURE 21

WEB USER INTERFACE

4 –BASIC 23
4.1 WEB USER INTERFACE HOMEPAGE 23

5 – NEXT G™ SETTINGS 26
5.1 NEXT G™ SERVICE SETUP 26
5.1.1 PROFILE SETUP 26

6 – WI-FI 28
6.1 SETUP 29
6.2 SECURITY 31
6.3 CONFIGURATION 33
6.4 MEDIA ACCESS CONTROL (MAC) FILTER 36
6.5 WIRELESS BRIDGE 37
6.6 STATION INFO 38

7 – ADVANCED SETTINGS 40
7.1 LOCAL AREA NETWORK (LAN) 40
7.2 NETWORK ADDRESS TRANSLATION (NAT) 42
7.2.1 PORT FORWARDING 42
7.2.2 PORT TRIGGERING 44
7.2.3 DEMILITARIZED ZONE (DMZ) HOST 45
7.3 SECURITY 46
7.3.1 IP FILTERING 46
7.3.2 PARENTAL CONTROL 48

7.4 ROUTING 48
7.4.1 STATIC ROUTE 48
7.4.2 DYNAMIC ROUTE 49
7.5 DOMAIN NAME SYSTEM (DNS) 50
7.5.1 DOMAIN NAME SYSTEM (DNS) SERVER 50
7.5.2 DYNAMIC DOMAIN NAME SYSTEM (DYNAMIC DNS) 52
7.6 DEVICE SETTINGS 54
7.6.1 BACKUP SETTINGS 54
7.6.2 UPDATE SETTINGS 54
7.7 DEVICE SETTINGS 56
7.7.1 BACK UP SETTINGS 56
7.7.2 UPDATE SETTINGS 56
7.7.3 RESTORE DEFAULT 57
7.7.4 UPDATE FIRMWARE 58
7.8 ACCESS CONTROL 59
7.8.1 SERVICES 59
7.8.2 PASSWORDS 60
7.9 SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP) 61
7.10 SIMPLE NETWORK TIME PROTOCOL (SNTP) 62
7.11 USB SETTINGS 63
7.11.1 PRINT SERVER 63
7.11.2 USB STORAGE 73
7.12 SAVE AND REBOOT 77

8 – DIAGNOSTICS 79
8.1 DIAGNOSTICS 80
8.2 SYSTEM LOG 82
8.3 NEXT G™ STATUS 84
8.4 STATISTICS 86
8.4.1 LAN STATISTICS 86
8.4.2 NEXT G™ STATISTICS 86
8.5 ROUTE 87
8.6 ADDRESS RESOLUTION PROTOCOL (ARP) 88
8.7 DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) 89
8.8 PING 90

GETTING STARTED

INTRODUCTION

Welcome to BigPond Wireless Broadband – thanks for choosing us!

This guide is designed to help you get the most out of your BigPond Wireless Broadband experience. We're sure you're itching to get started, so don't feel that you have to study it all right away. However, it's important to read through the Quick Setup section to ensure you set up your BigPond Elite™ Wireless Broadband Network Gateway correctly. The rest will be there when you need it.

As a BigPond Wireless Broadband Member, you can now enjoy a huge range of internet services, including state of the art security options, great account tools, flexible plans, extra email features, worlds of 'unmetered' content, special shopping deals and lots more.

So let's get started.

Make a note of your BigPond email address and password. Remember, your email address is your username@bigpond.com. We suggest protecting your security by writing down an unmistakable clue rather than your actual password.

GETTING STARTED

1.1 FEATURES

- Combines Next G™ Broadband service, Wi-Fi and Ethernet gateway in one device
- Dual-band HSPA+/UMTS (850 / 2100 Mhz)
- Embedded multimode HSUPA/HSDPA/HSPA+/UMTS module
- 2 x USB 2.0 host ports
- WEP/WPA/WPA2 and 802.1x
- MAC address and IP filtering
- Static route functions
- DNS Proxy
- Integrated 802.11n AP (backward compatible with 802.11b/g)
- CLI command interface
- Web-based management
- Supports VPN Pass-through
- NAT/PAT
- DHCP Server/Relay/Client
- Configuration backup and restoration

1.2 PACKAGE CONTENTS

Your package contains the following:

- Bigpond Elite™ Wireless Broadband Network Gateway
- Printed Quick Start Guide
- USB key (Containing Bigpond Connection Manager and User Guide)
- Ethernet Cable
- Security Card
- Power Supply

1.3 LED INDICATORS

The LED indicators are explained in the table below.

LED	Icon	Color	Mode	Description
High		Blue	On	High signal strength
			Off	No activity, gateway powered off or on other signal strength
Med		Blue	On	Medium signal strength
			Off	No activity. The gateway is powered off or is currently using another signal strength
Low		Blue	On	Low signal strength
			Off	No activity. The gateway is powered off or is currently using another signal strength
3G	3G	Blue	On	Connection established with the 3G network
			Off	Either there is no activity, the Gateway is powered off, or there is no cable or no powered device connected to the associated port
			Blink	Connecting with 3G network
LAN 1~4	1	Blue	On	Powered device connected to the associated LAN port (includes devices with Wake-on-LAN capability where a slight voltage is supplied to an Ethernet connection)
			Off	No device connected or Connected device is off
			Blink	LAN activity present (traffic in either direction)
Internet	WWW	Blue	On	Internet connection established
			Off	No connection to the internet or gateway powered off
			Blink	Data is currently being transmitted through the Internet connection
Wi-Fi		Blue	On	Local Wi-Fi access to the Gateway is enabled and working
			Off	Local Wi-Fi access to the Gateway is disabled
			Blink	Data being transmitted or received over Wi-Fi.
POWER		Blue	On	Power on
			Off	Power off

1.4 PANELS

The rear and side panels shown below contain the ports for data and power connections.

(1) USIM card slot

(2) Four RJ-45 Ethernet LAN ports

(3) Reset button

(4) Power jack for DC power input (12VDC / 1.5A).

(5) External 3G SMA Connector (Optional)

Note: The Gateway will automatically select to use either the internal or external 3G antenna during power up based on whichever has the stronger signal. To switch between internal and external antenna, the Gateway may require a reboot

(6) USB1 Port

(7) USB2 Port

QUICK SETUP

QUICK SETUP

2.1 SETUP PROCEDURE (WITH USB KEY)

These steps explain how to quickly setup your Next G™ Gateway:

1: Insert your SIM card (until you hear a click) into the USIM slot on the rear of the Gateway.

2: Connect the yellow Ethernet cable to one of the yellow LAN ports found at the back of the Gateway.

3: Connect the other end of the yellow networking cable to the Ethernet port on your computer.

4: Connect the power adapter to the Power socket on the back of the Gateway.

5: Plug the power adapter into a wall socket and press the power button into the ON position.

6: Configure the Gateway through the Web User Interface (WUI).

NOTE: Chapters 4 through 8 explain how to set up and use the WUI

7: Save the Gateway configuration and reboot (see section 7.13).

ADVANCED
SETUP

ADVANCED SETUP

3.1 SETUP PROCEDURE (WITHOUT USB KEY)

These steps explain how to quickly setup your Next G™ Gateway:

1: Insert your SIM card (until you hear a click) into the USIM slot on the rear of the Gateway.

2: Connect the yellow Ethernet cable to one of the yellow LAN ports found at the back of the Gateway.

3: Connect the other end of the yellow networking cable to the Ethernet port on your computer.

4: Connect the power adapter to the Power socket on the back of the Gateway.

5: Plug the power adapter into a wall socket and press the power button into the ON position (depressed).

6: Configure the Gateway through the Web User Interface (WUI).

NOTE: Chapters 4 through 8 explain how to set up and use the WUI

7: Save the Gateway configuration and reboot (see section 7.13).

3.2 TCP/IP SETTINGS

It is likely that your computer will automatically obtain an IP Address and join the network.

This is because the Dynamic Host Configuration Protocol (DHCP) server (on the device) will start automatically when your Gateway powers up.

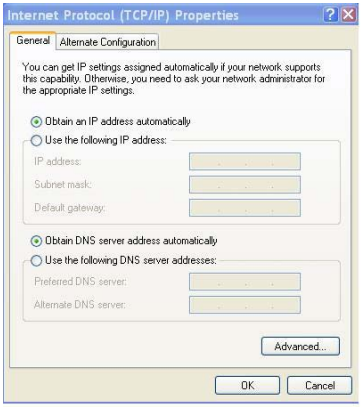
This automatic assignment requires that DHCP is configured on your computers. It is likely that this is already the case, but should you be required to configure this, please see the instructions on the following page.

WINDOWS XP

To access the dialog box that allows you to configure your network connection, click on Start > Control Panel > Network Connections. Then right mouse click on the Local Area Connection and select Properties. Select Internet Protocol (TCP/IP) then select Properties

DHCP MODE

You can set your PC to DHCP mode by selecting Obtain an IP address automatically in the dialog box shown below.



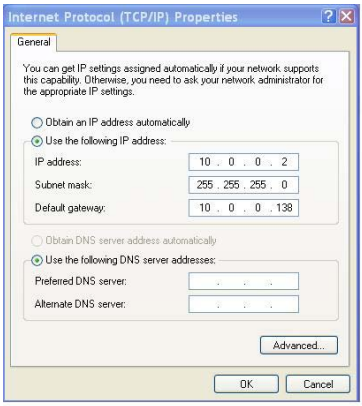
STATIC IP MODE

The following steps show how to assign a Static IP address to your PC using subnet 10.0.0.x.

1: Change the IP address to the domain of 10.0.0.x. (1<x<254) with subnet mask of 255.255.255.0.

2: Set the default gateway and DNS server to the gateway's IP address.

NOTE: The IP address of the gateway is 10.0.0.138. (Default), so the PC must be set with a different IP. In the case below, the PC's IP address is set as 10.0.0.2



3: Click Ok to submit the settings.

MACOSX 10.4

To access the dialog box that allows you to configure your network connection. Browse to the Apple menu and select System Preferences. From the System Preferences menu, click the Network icon and then select the Ethernet connection.

DHCP MODE

You can set your Mac to DHCP by selecting DHCP from the Configure drop down list. After clicking Apply, your Mac's IP Address will now be automatically assigned from the Gateway.

STATIC MODE

1. From the Configure drop down list, you can set your computer to Static IP mode by selecting the option Manually.

The following steps show how to assign a Static IP address to your Mac

2. Choose an IP address between 10.0.0.1 – 10.0.0.254 (Do not choose the Gateway IP of 10.0.0.138). enter this IP address into the field marked IP Address, and enter a Subnet Mask of 255.255.255.0

3. Set the Router and DNS server field to 10.0.0.138 (The gateway's IP address).

NOTE: The IP address of the gateway is 10.0.0.138. (default), so the computer must be set with a different IP to the gateway. In the case below, the PC's IP address is set as 10.0.0.2

4. Click Apply to submit the settings.

WINDOWS VISTA

To access the dialog box that allows you to configure your network connection, click on Start > Control Panel > Network Connections. Then right mouse click on the Local Area Connection and select Properties. Select Internet Protocol (TCP/IP) then select Properties

DHCP MODE

You can set your PC to DHCP mode by selecting Obtain an IP address automatically in the dialog box shown below.

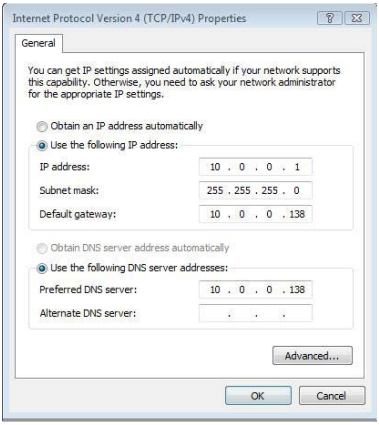
STATIC IP MODE

To configure your Gateway manually, your PC must have a static IP address within the Gateway's subnet. The following steps show how to assign a Static IP address to your PC using subnet 10.0.0.x.

1: Select Use the following IP Address. Choose an IP address between 10.0.0.1 – 10.0.0.254

NOTE: The Ip address of the gateway is 10.0.0.138. (default), so the PC must be set with a different Ip. In the case below, the PC's IP address is set as 10.0.0.1

2: Set the Router and DNS server field to 10.0.0.138 (The gateway's IP address).



3. Click Ok to apply the settings.

3.3 DEFAULT SETTINGS

The following are the default settings for the Gateway

- Local (LAN) access (username: admin, password: admin)
- Remote (WAN) access (username: support, password: support)
- User access (username: user, password: user)
- LAN IP address: 10.0.0.138
- Remote WAN access: disabled
- NAT and firewall: enabled
- Dynamic Host Configuration Protocol (DHCP) server on LAN interface: enabled

Technical Note:

During power on, the device initializes all settings to default values. It will then read the configuration profile from the permanent storage section of flash memory. The default attributes are overwritten when identical attributes with different values are configured. The configuration profile in permanent storage can be created via the web user interface or telnet user interface, or other management protocols. The factory default configuration can be restored either by pushing the reset button for more than five seconds until the power LED blinks or by clicking the Restore Default Configuration option in the Restore Default Settings screen (see section 7.7.3).

3.4 LOGIN PROCEDURE

To login to the web interface, follow the steps below:

NOTE: The default settings can be found in 3.3 Default Settings.

1: Open a web browser and enter the default IP address for the Gateway in the Web address field. In this case http://10.0.0.138

NOTE: For remote access, use the WAN IP address shown on the WUI Homepage screen and login with remote username and password.

2: A dialog box will appear, as illustrated below. enter the default username and password, as defined in section 3.3 Default Settings.

Click Ok to continue.

NOTE: The login password can be changed later (see 7.8.2 Passwords)

BASIC

BASIC

4.1 WEB USER INTERFACE HOMEPAGE

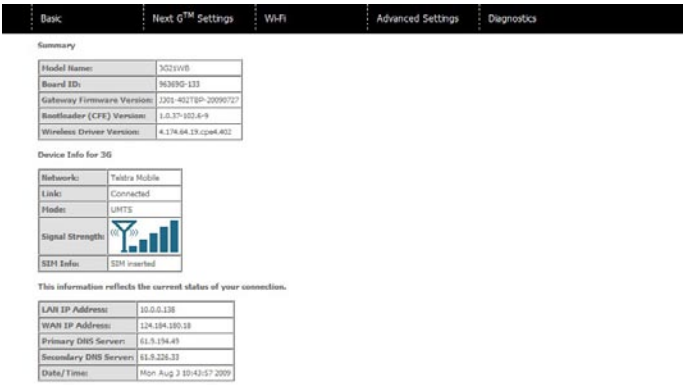
The web user interface (WUI) is divided into two window panels, the main menu (on the top) and the display screen (on the bottom). The main menu has the following options: Basic, Next G™ Settings, Wi-Fi, Advanced Settings and Diagnostics.

Selecting one of these options will open a submenu with more options. Basic is discussed below while subsequent chapters introduce the other main menu selections.

NOTE: The menu options available within the web user interface are based upon the device configuration and user privileges (i.e. local or remote).

BASIC / HOME

The Basic / Home screen is the WUI homepage and the first selection on the main menu. It provides information regarding the firmware, 3G, and IP configuration.



The following table provides further details.

Option	Description
Model Name	The model name of the device.
Board ID	The Hardware version of the device
Bootloader version	The bootloader version of the device.
Gateway Firmware version	The firmware version of the device.
Wireless driver version	The wireless driver version of the wireless module.
Network	The name of or other reference to the mobile network operator.
Link	Shows the connection status of the current Next G™ connection.
Mode	The radio access technique currently used to enable internet access. It can be HSUPA, HSDPA, UMTS, or Disconnected.
Signal strength	The mobile network (UMTS) signal quality available at the device location. This signal quality affects the performance of the unit. If two or more bars are green, the connection is usually acceptable.
SIM info	Shows the SIM card status on the device.
LAN IP Address	Shows the IP address for LAN interface.
WAN IP Address	Shows the IP address for WAN interface.
Primary DNS Server	Shows the IP address of the primary DNS server.
Secondary DNS server	Shows the IP address of the secondary DNS server.
Date/Time	The time according to the device's internal clock

NEXT GTM
SETTINGS

NEXT G™ SETTINGS

This menu includes Next G™ service Setup.

NOTE: Sections 8.3 and 8.4.2 also provide information about the Next G™ service.

5.1 NEXT G™ SERVICE SETUP

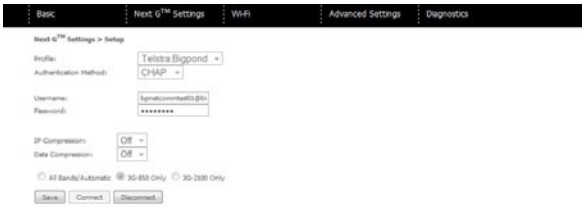
Select your Next G™ service settings according to predefined or custom profiles.

Setup instructions are provided in the following sections for your assistance.

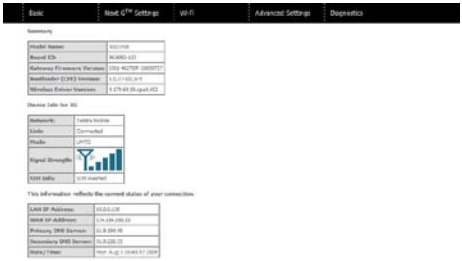
5.1.1 PROFILE SETUP

Bigpond will provide the information required to complete the first time setup instructions below. This includes profile, username and password. Only complete those steps for which you have information and skip the others.

1. If your SIM card is not inserted into the gateway, please turn the gateway off. Then insert the SIM and turn the gateway on.
2. Type the APN in the APN field. Authentication Method should be provided by Bigpond; or just leave it AUTO if not acquired. If you have not received the username and password, leave these fields empty.



3. Select IP compression and Data compression to be ON or OFF. By default they are set to off.
4. Click the Save button to save the new settings.
5. Press the Connect button to connect to Internet. The Device Info for 3G network box in the WUI Basic screen should indicate an active connection, as shown below. The 3G and Internet LEDs on the front panel of the Gateway should also be blinking.



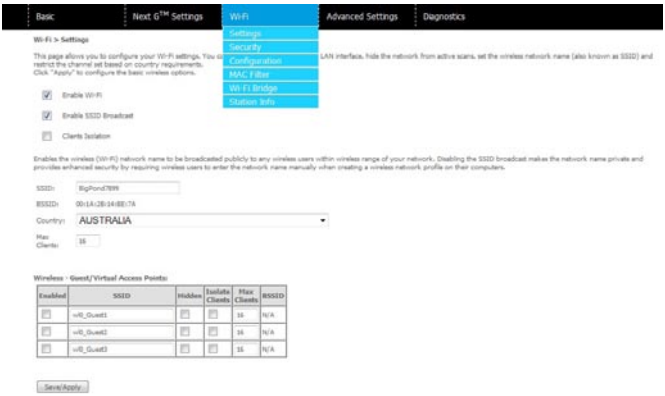
If the LEDs are off, then either your profile settings are incorrect, the SIM card is not working or the service network is unavailable. In either case, contact Technical Support for further instructions.

WI-FI

WI-FI

The Wi-Fi submenu provides access to Wireless Local Area Network (LAN) configuration settings including:

- Wireless network name
- Channel restrictions (based on country)
- Security
- Access point or bridging behaviour
- Station information



6.1 SETTINGS

This screen 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. The Wireless Guest Network function adds extra networking security when connecting to remote hosts.

Option	Description
Enable Wi-Fi	A checkbox that enables or disables the wireless LAN interface. When selected, the Web UI displays Hide Access point, SSID, and County settings. The default is Enable Wi-Fi.
Enable SSID Broadcast	Deselect Enable SSID Broadcast to protect the access point from detection by wireless active scans.
	To check AP status in Windows XP, open Network Connections from the Start Menu and select View Available Network Connections. If the access point is hidden, it will not be listed there. To connect a client to a hidden access point, the station must add the access point manually to its wireless configuration.
Clients Isolation	1. Prevents clients PC from seeing one another in My Network Places or Network Neighborhood.
	2. Prevents one wireless client communicating with another wireless client.
SSID	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.
	The naming conventions are: Minimum number of characters: 1, maximum number of characters: 32.
BSSID	The BSSID is a 48bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Medium Access Control) address of the AP (Access Point) and in Independent BSS or ad hoc networks, the BSSID is generated randomly.
Country	A drop-down menu that permits worldwide and specific national settings. Each county listed in the menu enforces specific regulations limiting channel range: US= worldwide, Japan=1-14, Jordan= 10-13, Israel= 1-13
Max Clients	The maximum number of clients that can access the router.
Wireless - Guest / Virtual Access Points	This router supports multiple SSIDs called Guest SSIDs or Virtual Access Points. To enable one or more Guest SSIDs select the radio buttons under the Enable heading. To hide a Guest SSID, select its radio button under the Hidden heading. Do the same for Isolate Client and Disable WMM Advertise functions. For a description of these two functions, see the entries for "Client Isolation" and "Disable WMM Advertise" in this table. Similarly, for Max Clients and BSSID headings, consult the matching entries in this table. NOTE: Remote wireless hosts are unable to scan Guest SSIDs.

6.2 SECURITY

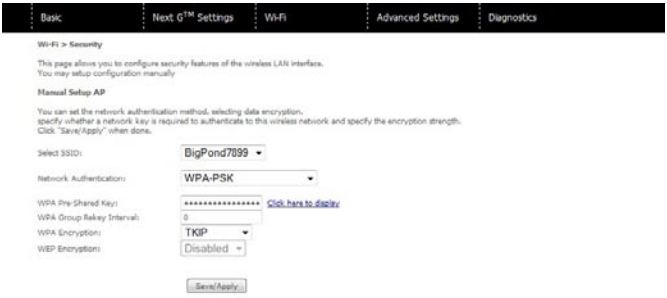
This Gateway includes a number of options to help provide a secure connection to the Next G™ Network.

Security features include:

- WEP / WPA / WPA2 data encryption
- SPI Firewall
- VPN Pass-Through
- MAC address IP filtering
- Authentication protocols – PAP / CHAP

You can authenticate or encrypt your service on the Wi-Fi Protected Access algorithm, which provides protection against unauthorized access such as eavesdropping.

The following screen appears when Security is selected. The Security page allows you to configure security features of your Gateway's wireless LAN interface. You can set the network authentication method, select data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.



Click Save/Apply to configure the wireless security options.

Option	Description
Select SSID	Your Service Set Identifier (SSID), sets your Wireless Network Name. You can connect multiple devices including Laptops, Desktop PCs and PDAs to your Wireless Gateway. To get additional devices connected, scan for a network, and locate the SSID shown on your Wireless Security Card. If the SSID does not match, access is denied.
Network Authentication	This option is used for authentication to the wireless network. Each authentication type has its own settings. For example, selecting 802.1X authentication will reveal the RADIUS Server IP address, Port and key fields.
WEP Encryption	This option indicates whether data sent over the network is encrypted. The same network key is used for data encryption and network authentication. Whilst four network keys can be defined, only one can be used at any one time.
Encryption Strength	This drop-down list box will display when WEP Encryption is enabled. The key strength is proportional to the number of binary bits comprising the key. This means that keys with a greater number of bits have a greater degree of security and are considerably more difficult to crack. Encryption strength can be set to either 64-bit or 128-bit. A 64-bit key is equivalent to 5 ASCII characters or 10 hexadecimal numbers. A 128-bit key contains 13 ASCII characters or 26 hexadecimal numbers. FYI: Each key contains a 24-bit header (an initiation vector) which enables parallel decoding of multiple streams of encrypted data.

6.3 CONFIGURATION

The following screen appears when you select Configuration. This screen allows you to control the advanced features of the Wireless Local Area Network (WLAN) interface:

- Select the channel which you wish to operate from
- Force the transmission rate to a particular speed
- Set the fragmentation threshold
- Set the RTS threshold
- Set the wake-up interval for clients in power-save mode
- Set the beacon interval for the access point
- Set Xpress mode
- Program short or long preambles

Click Save/Apply to set the advanced wireless configuration.

Option	Description
Band	The new amendment allows IEEE 802.11g units to fall back to speeds of 11 Mbps, so IEEE 802.11b and IEEE 802.11g devices can coexist in the same network. The two standards apply to the 2.4 GHz frequency band. IEEE 802.11g creates data-rate parity at 2.4 GHz with the IEEE 802.11a standard, which has a 54 Mbps rate at 5 GHz. (IEEE 802.11a has other differences compared to IEEE 802.11b or g, such as offering more channels.)
Channel	Drop-down menu that allows selection of a specific channel.
Auto Channel Timer (min)	Auto channel scan timer in minutes (0 to disable)
802.11n/EWC	With drop-down menu, "Auto" is for 11n and "Disable" is for 11g
Bandwidth	Drop-down menu specifies the following bandwidth: 20MHz and 40MHz.
Control Sideband	This is available for 40MHz. Drop-down menu allows selecting upper sideband or lower sideband
802.11n Rate	Drop-down menu specifies the following fixed rates. The maximum rate for bandwidth, 20MHz, is 130MHz and the maximum bandwidth, 40MHz, is 270MHz
802.11n Protection	It is similar as 802.11g protection. In Auto mode the router will use RTS/CTS to improve 802.11n performance in mixed 802.11n/ 802.11g/ 802.11b networks. Turn protection off to maximize 802.11n throughput under most conditions.
Support 802.11n client only	Drop-down menu allows selecting "On/Off". Choosing "On" allows the client with 11n only to connect, not for 11g or 11b; choosing "Off" allows the client with 11n/11g/11b to connect
54g Rate	Drop-down menu that specifies the following fixed rates: Auto: Default. Uses the 11 Mbps data rate when possible but drops to lower rates when necessary. 1 Mbps, 2Mbps, 5.5Mbps, or 11Mbps fixed rates. The appropriate setting is dependent on signal strength.
Multicast Rate	Setting multicast packet transmit rate.
Basic Rate	Setting basic transmit rate.
Fragmentation Threshold	A threshold, specified in bytes, that determines whether packets will be fragmented and at what size. On an 802.11 WLAN, packets that exceed the fragmentation threshold are fragmented, i.e., split into, smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value are not fragmented. Enter a value between 256 and 2346. If you experience a high packet error rate, try to slightly increase your Fragmentation Threshold. The value should remain at its default setting of 2346. Setting the Fragmentation Threshold too low may result in poor performance.
RTS Threshold	Request to Send, when set in bytes, specifies the packet size beyond which the WLAN Card invokes its RTS/CTS mechanism. Packets that exceed the specified RTS threshold trigger the RTS/CTS mechanism. The NIC transmits smaller packet without using RTS/CTS. The default setting of 2347 (maximum length) disables RTS Threshold.

Option	Description
DTIM Interval	Delivery Traffic Indication Message (DTIM), also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.
Beacon Interval	The amount of time between beacon transmissions. Each beacon transmission identifies the presence of an access point. By default, radio NICs passively scan all RF channels and listen for beacons coming from access points to find a suitable access point. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point). The entered value is represented in ms. Default is 100. Acceptable entry range is 1 to 0xffff (65535)
Global Max Clients	The device can support 4 SSID, and each SSID can set its own max clients, but it can't be bigger than Global max clients. "Global Max Clients" limits the total associated clients of the 4 SSID.
Xpress™ Technology	Xpress™ Technology is compliant with draft specifications of two planned wireless industry standards.
Transmit Power	The router will set different power output (by percentage) according to this selection.

6.4 MAC FILTER

This screen appears when Media Access Control (MAC) Filter is selected. This option allows access to be restricted based upon the unique 48-bit MAC address.

To add a MAC Address filter, click the Add button shown below.

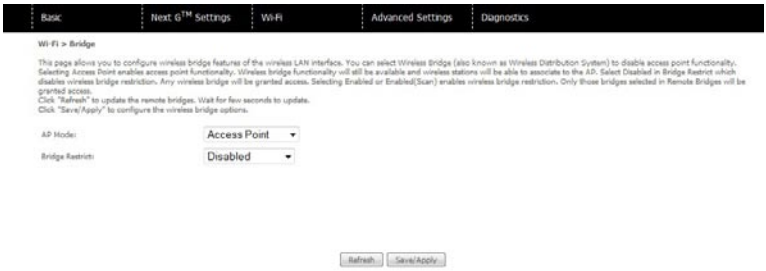
To delete a filter, select it from the table below and click the Remove button.

Option	Description
MAC Restrict Mode	Disabled – Disables MAC filtering Allow – Permits access for the specified MAC addresses. NOTE: Add a wireless device's MAC address before clicking the Allow radio button or else you will need to connect to the Gateway's web user interface using the supplied yellow Ethernet cable and add the wireless device's MAC address. Deny – Rejects access for the specified MAC addresses
MAC Address	Lists the MAC addresses subject to the MAC Restrict Mode. The Add button prompts an entry field that requires you type in a MAC address in a two- character, 6-byte convention: xx:xx:xx:xx:xx:xx where xx are hexadecimal numbers. A maximum of 60 MAC addresses can be added.

Enter the MAC address on the screen below and click Save/Apply.

6.5 WIRELESS BRIDGE

The following screen appears when selecting Wireless Bridge, and goes into a detailed explanation of how to configure wireless bridge features of the wireless LAN interface. Click Save/Apply to implement new configuration settings.



Option	Description
AP Mode	Selecting Wireless Bridge (Wireless Distribution System) disables Access Point (AP) functionality while selecting Access Point enables AP functionality. In Access Point mode, wireless bridge functionality will still be available and wireless stations will be able to associate to the AP.
Bridge Restrict	Selecting Disabled in Bridge Restrict disables Wireless Bridge restriction, which means that any wireless bridge will be granted access. Selecting enabled or enabled (Scan) allows wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access. Click Refresh to update the station list when Bridge Restrict is enabled.

6.6 STATION INFO

The following screen appears when you select Station Info, and shows authenticated wireless stations and their status. Click the Refresh button to update the list of stations in the WLAN

Option	Description
BSSID	The BSSID is a 48-bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Media Access Control) address of the AP (Access Point); and in Independent BSS or ad hoc networks, the BSSID is generated randomly.
Associated	Lists all the stations that are associated with the Access Point, along with the amount of time since packets were transferred to and from each station. If a station is idle for too long, it is removed from this list.
Authorized	Lists those devices with authorized access.

ADVANCED SETTINGS

ADVANCED SETTINGS

7.1 LOCAL AREA NETWORK (LAN)

This screen allows you to configure the Local Area Network (LAN) interface on your Gateway

See the field descriptions below for more details.

NOTE: If you change your gateway's IP address (first option on the chart), the installation software/ connection manager may not be able to communicate with the gateway. Please reset the gateway's IP address to 10.0.0.138 if this occurs.

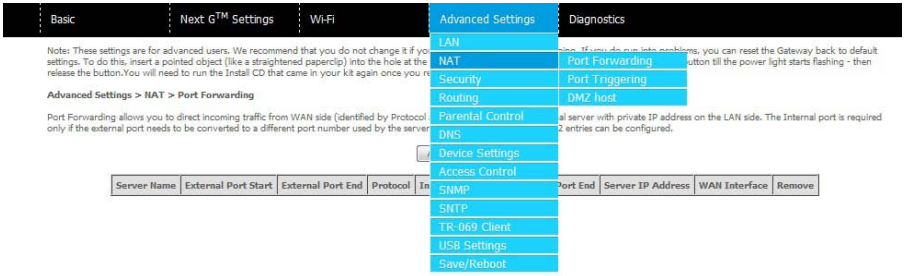
Option	Description
IP Address	Enter the IP address for the LAN interface
Subnet Mask	Enter the subnet mask for the LAN interface
Enable Internet Group Management Protocol (IGMP) Snooping	Enable by ticking the box Standard Mode: In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group. Blocking Mode: In blocking mode, the multicast data traffic will be blocked. When there are no client subscriptions to a multicast group, it will not flood to the bridge ports.
Enable NAT	To enable/disable Network Address Translation (NAT, please refer to 7.2 for NAT setting). By default NAT is enabled.
Enable UPnP	Tick the box to enable Universal Plug and Play
Dynamic Host Configuration Protocol (DHCP) Server	Select enable DHCP server and enter your starting and ending IP addresses and the lease time. This setting configures the gateway to automatically assign IP, default gateway and DNS server addresses to every DHCP client on your LAN
Static IP Lease List	To specify the IP address assigned through DHCP according to the MAC address of the hosts connected to the Gateway.
Enable DHCP Server Relay	To relay DHCP requests from the subnet with no DHCP server on it to a DHCP server on other subnets. DHCP Server Relay is disabled by default. To access enable DHCP relay, please un-tick NAT enable first, that means to disable NAT first, and then press save button. The enable DHCP server Relay option will then show up on the same page as below:

Configure a second IP address by ticking the checkbox shown below and enter the following information:

IP Address:	Enter the secondary IP address for the LAN interface.
Subnet Mask:	Enter the secondary subnet mask for the LAN interface.

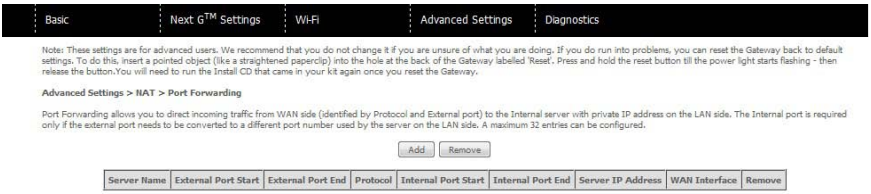
NOTE: The Save button saves new settings to allow continued configuration, while the Save/Reboot button not only saves new settings but also reboots the device to apply the new configuration (i.e. all new settings).

7.2 NETWORK ADDRESS TRANSLATION (NAT)



7.2.1 PORT FORWARDING

Port Forwarding allows you to direct incoming traffic from the Internet side (identified by Protocol and External port) to the internal server with a 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 of 32 entries can be configured.



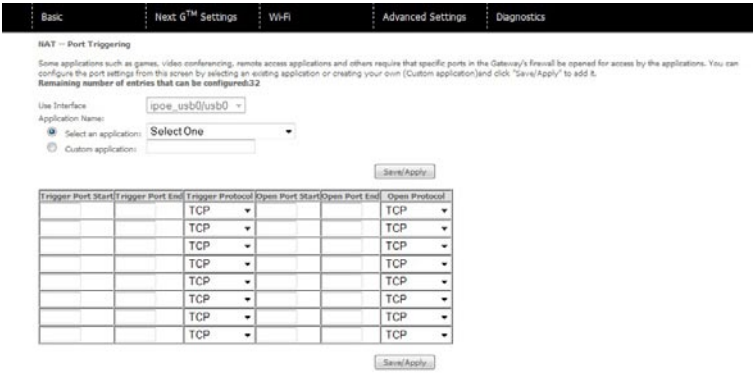
To add a Port Forwarding rule, click the Add button. The following screen will display.

Options	Description
Select a Service Or Custom Server	User should select the service from the list. Or create a custom server and enter a name for the server
Server IP Address	Enter the IP address for the server.
External Port Start	Enter the starting external port number (when you select Custom Server). When a service is selected the port ranges are automatically configured.
External Port End	Enter the ending external port number (when you select Custom Server). When a service is selected the port ranges are automatically configured.
Protocol	User can select from: TCP, TCP/UDP or UDP.
Internal Port Start	Enter the internal port starting number (when you select Custom Server). When a service is selected the port ranges are automatically configured
Internal Port End	Enter the internal port ending number (when you select Custom Server). When a service is selected the port ranges are automatically configured.

7.2.2 PORT TRIGGERING

Some applications require specific ports in the Gateway'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 Gateway 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

To add a Trigger Port, simply click the Add button. The following will be displayed.



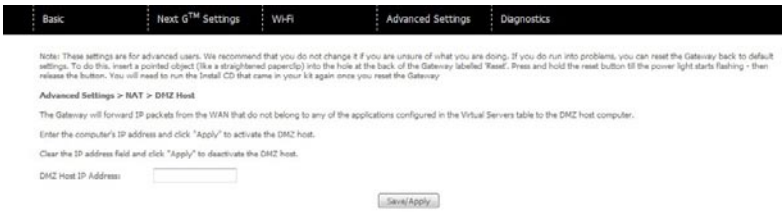
Options	Description
Select an Application or Custom Application	User should select the application from the list. or User can enter the name of their choice.
Trigger Port Start	Enter the starting trigger port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Trigger Port End	Enter the ending trigger port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Trigger Protocol	TCP, TCP/UDP or UDP.
Open Port Start	Enter the starting open port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Open Port End	Enter the ending open port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Open Protocol	TCP, TCP/UDP or UDP.

7.2.3 DEMILITARIZED (DMZ) HOST

Your Gateway 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.

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



7.3 SECURITY

Your Gateway can be secured with the IP Filtering function.

7.3.1 IP FILTERING

The IP Filtering screen sets filter rules that limit incoming and outgoing IP traffic. Multiple filter rules can be set with at least one limiting condition. All conditions must be fulfilled to allow individual IP packets to pass through the filter.

OUTGOING IP FILTER

The default setting for Outgoing traffic is ACCEPTED. Under this condition, all outgoing IP packets that match the filter rules will be BLOCKED.

To add a filtering rule, click the Add button. The following screen will display.

Options	Description
Filter Name	The filter rule label
Protocol	TCP, TCP/UDP, UDP or ICMP
Source IP address	Enter source IP address
Source Subnet Mask	Enter source subnet mask
Source Port (port or port:port)	Enter source port number or port range
Destination IP address	Enter destination IP address
Destination Subnet Mask	Enter destination subnet mask
Destination port (port or port:port)	Enter destination port number or range

Click Save/Apply to save and activate the filter.

INCOMING IP FILTER

The default setting for all Incoming traffic is BLOCKED. Under this condition only those incoming IP packets that match the filter rules will be ACCEPTED.

To add a filtering rule, click the Add button. The following screen will display.

Please refer to the Outgoing IP Filter table for field descriptions.

Click Save/Apply to save and activate the filter.

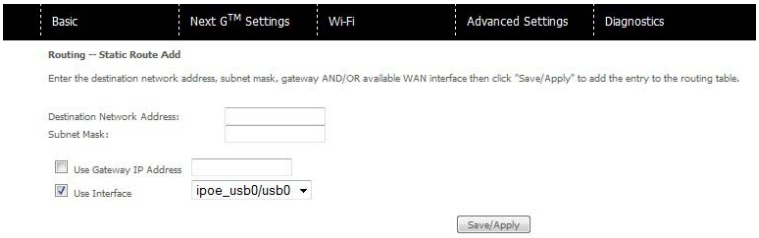
7.4 ROUTING

Static Route and Dynamic Route settings can be found in the Routing link as illustrated below.

7.4.1 STATIC ROUTE

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

Click the Add button to display the following screen.



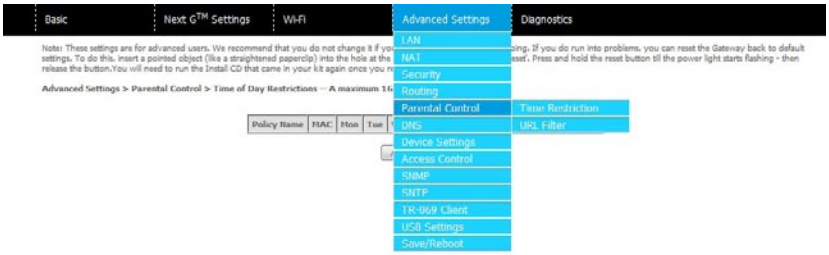
Enter Destination Network Address, Subnet Mask, Gateway IP Address and/or WAN Interface. Then click Save/Apply to add the entry to the routing table.

7.4.2 DYNAMIC ROUTE

To activate this option, select the enabled radio button for Global RIP Mode.

To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the enabled checkbox for that interface. Click Save/Apply to save the configuration and to start or stop dynamic routing.

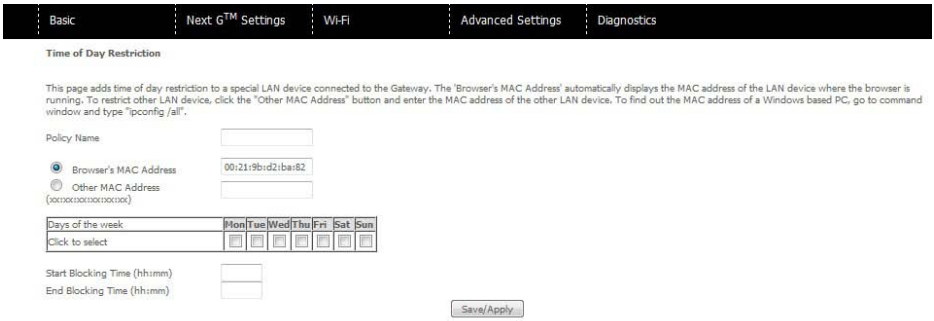
7.5 PARENTAL CONTROL



7.5.1 TIME RESTRICTION

Time Restriction allows you to restrict access from a device on your Local Area network (LAN) to the Internet through the Gateway on selected days at certain times. Make sure to activate the Internet Time server synchronization as described in section 7.10 SNTP, so that the scheduled times match your local time.

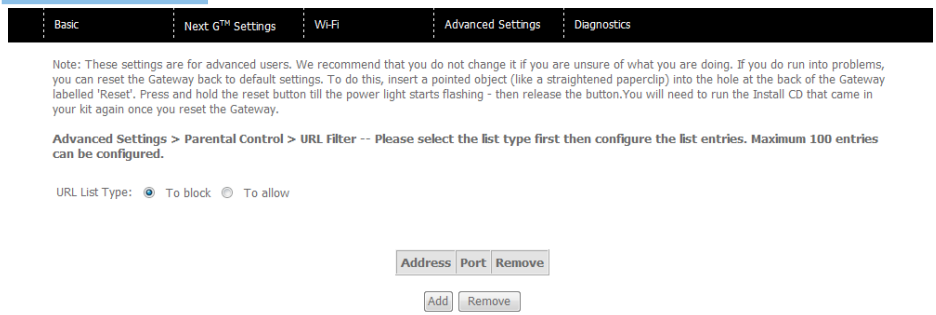
Click Add to display the following screen. Enter the MAC address of the device that you wish to restrict access for and select days of the week and times to apply the restriction



Complete the fields listed below and click Save/Apply to apply the settings.

Options	Description
User Name	A user-defined label for this restriction
Browser's MAC Address	Allows easy identification of MAC address of the computer running the Browser
Other MAC Address	MAC address of another LAN device
Days of the Week	Select one or more days for the restrictions to apply to.
Start Blocking Time	Enter the time you want the restriction to start
End Blocking Time	Enter the time you want the restriction to end

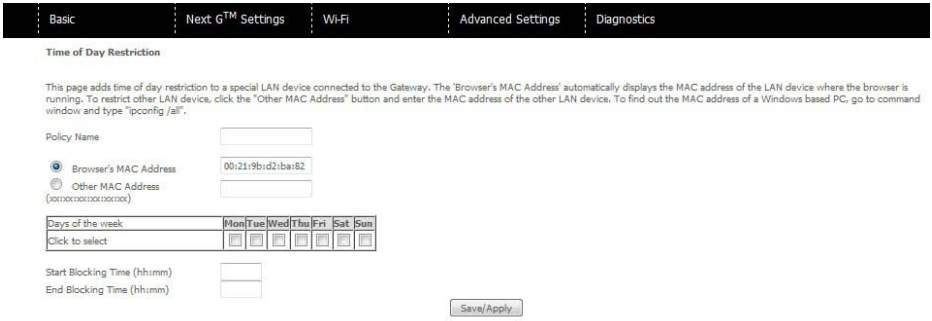
7.5.2 URL FILTER



The URL Filer allows you to restrict access from a device on your Local Area Network (LAN) to certain websites on the internet.

To use this feature, first select whether to Allow or Block the URL list. If Allow is selected, only the URL addresses listed in the table will be accessible to the computers on the LAN. If Block is selected, the URL addresses listed in the table will be blocked from computers on the LAN.

ADD URL ADDRESS



To add a URL address, click Add, then complete the fields listed below and click Save/Apply to apply the settings.

Options	Description
URL Address	Select either a URL address or a keyword to filter. (e.g. www.badwebsite.com)
Port Number	Either port 80 or port 8080 is accepted.

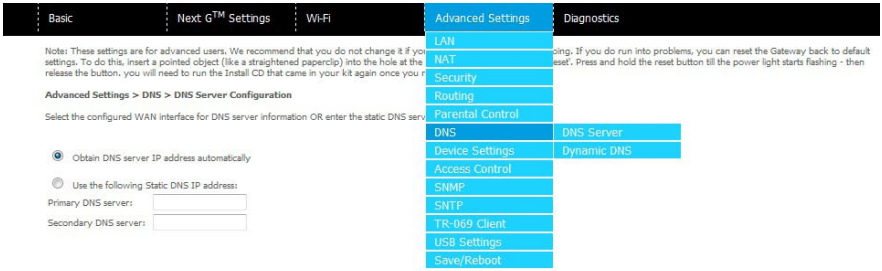
REMOVE URL ADDRESS

To remove a URL address, select the URL keyword you wish to remove, and click Remove.

7.6 DOMAIN NAME SERVER (DNS)

7.6.1 DNS SERVER CONFIGURATION

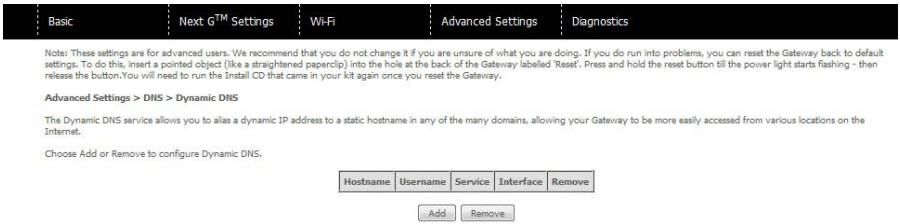
If Enable Automatic Assigned DNS is selected, this device will accept the first received DNS assignment from the Wide Area Network (WAN) interface during the connection process. Otherwise, you can enter the primary and optional secondary DNS server IP addresses. Click on Save to apply.



NOTE: Click the Save button to save the new configuration. To make the new configuration effective, reboot your Gateway.

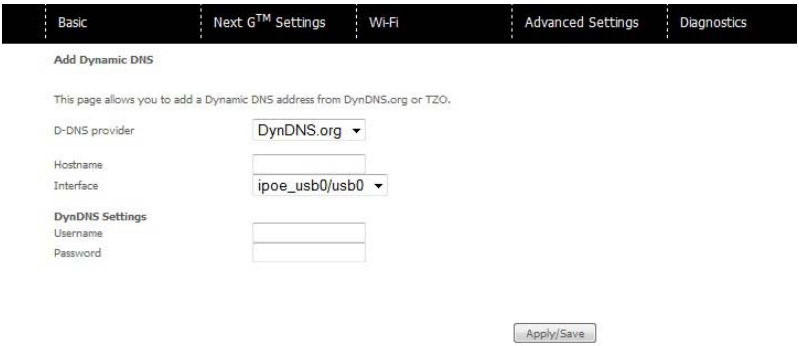
7.6.2 DYNAMIC DNS

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 gateway to be more easily accessed from various locations on the internet.



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

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



Options	Description
D-DNS provider	Select a dynamic DNS provider from the list.
Hostname	Enter the name for the dynamic DNS server.
Interface	Select the interface from the list.
Username	Enter the username for the dynamic DNS server.
Password	Enter the password for the dynamic DNS server.

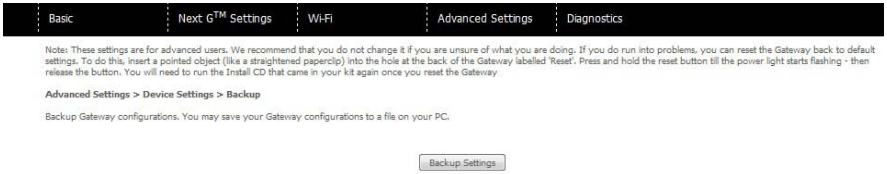
7.7 DEVICE SETTINGS

The Device Settings screens allow you to backup, retrieve and restore the default settings of your Gateway. It also provides a function for you to update your Gateway's settings.

7.7.1 BACKUP SETTINGS

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

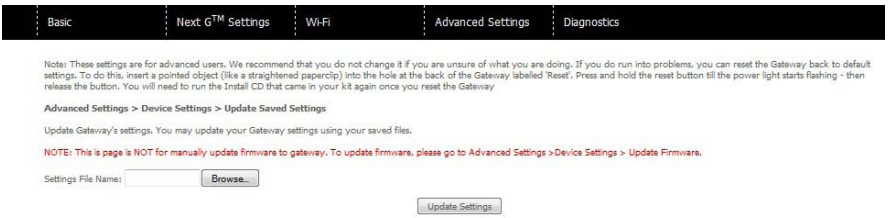
You will be prompted to define the location of a backup file to save to your PC.



7.7.2 UPDATE SETTINGS

The following screen appears when selecting Update from the submenu. By clicking on the

Browse button, you can locate a previously saved filename as the configuration backup file. Click on the Update settings to load it.



7.7.3 RESTORE DEFAULT

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

NOTE: The default settings can be found in section 3.3 Default Settings.

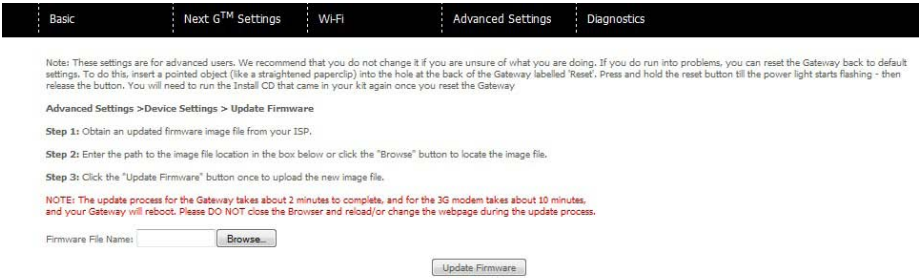
Once you have selected the Restore Default Settings button, the following screen will appear. Close the window and wait 2 minutes before reopening your browser. If required, reconfigure your computer's IP address to match your new configuration (see section 3.2 TCP/IP Settings for details)

After a successful reboot, the browser will return to the Device Info screen. If the browser does not refresh to the default screen, close and restart the browser.

NOTE: The Restore Default function has the same effect as the reset button. If the reset button is continuously pushed for more than 5 seconds (and not more than 12 seconds), the boot loader will erase the configuration settings saved on flash memory.

7.7.4 UPDATE FIRMWARE

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



1: Obtain an updated firmware image file

2: Enter the path and filename of the firmware image file in the Firmware File Name field or click the Browse button to locate the image file.

3: Click the Update Firmware button once to upload and install the file.

NOTE: The update process will take about 2 minutes to complete. The Gateway will reboot and the browser window will refresh to the default screen upon successful installation. It is recommended that you compare the Software Version at the top of the Basic screen (WUI homepage) with the firmware version installed, to confirm the installation was successful.

7.8 ACCESS CONTROL

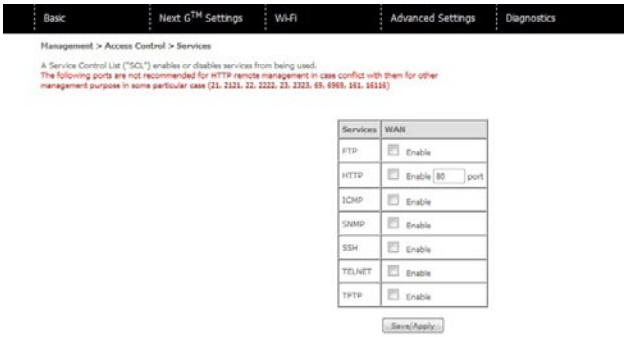
The Access Control option found in the Management drop down menu configures access related parameters in the following two areas:

- Services
- Passwords

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

7.8.1 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. These access services are available: FTP, HTTP, ICMP, SSH, TELNET, and TFTP. Click Save/Apply to continue.

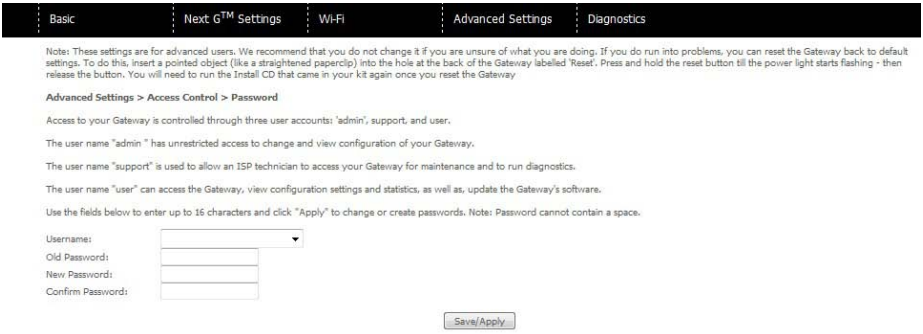


7.8.2 PASSWORDS

The Passwords option configures your account access password for your Gateway. 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 Save/Apply to continue.



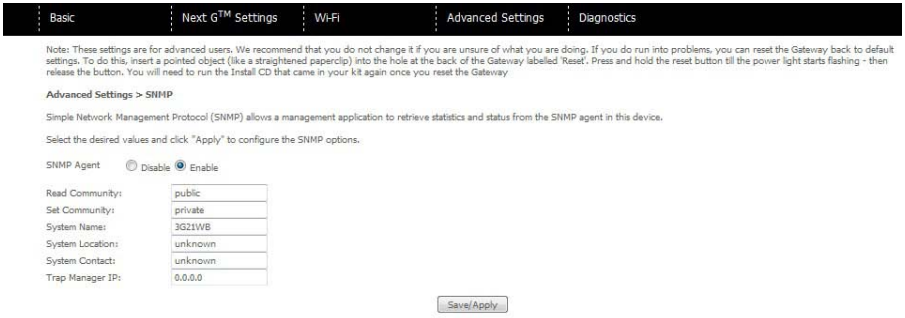
7.9 SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

The Simple Network Management Protocol (SNMP) allows a network administrator to monitor a network by retrieving settings on remote network devices. To do this, the administrator typically runs an SNMP management station program such as MIB browser on a local host to obtain information from the SNMP agent, in this case the 3G21WB (if SNMP enabled). An SNMP 'community' performs the function of authenticating SNMP traffic. A 'community name' acts as a password that is typically shared among SNMP agents and managers.

By default, SNMP agent is enabled on the gateway.

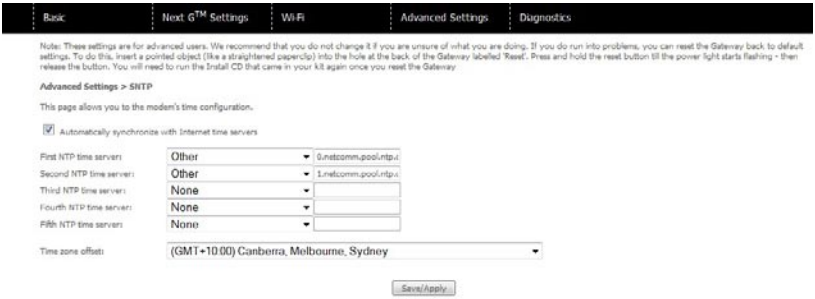
SETTING UP SNMP AGENT

1. Open a web browser (Ie/Firefox/Safari), type in LAN address of the gateway (http://10.0.0.138/ by default) to log into the web interface.
2. The login username and password by default is admin/admin.
3. Go to Advanced Settings > SNMP. Enable SNMP agent and set up all options according to the screenshot below.
4. Click Save/Apply to activate these settings.



7.10 SIMPLE NETWORK TIME PROTOCOL (SNTP)

This screen allows you to configure the time settings of your Gateway. To automatically synchronize with Internet time servers, tick the box as illustrated below.



The following options should now appear (see screenshot below):

Options	Description
First NTP time server:	Select the required server.
Second NTP time server:	Select second time server, if required.
Time zone offset:	Select the local time zone.

Configure these options and then click Save/Apply to activate.

NOTE: SNTP must be activated to use Parental Control (section 7.5).

7.11 USB SETTINGS

The USB Settings option found in the Advanced Settings drop down menu configures USB port related parameters in the following two areas:

- Print Server
- USB Storage

7.11.1 PRINT SERVER

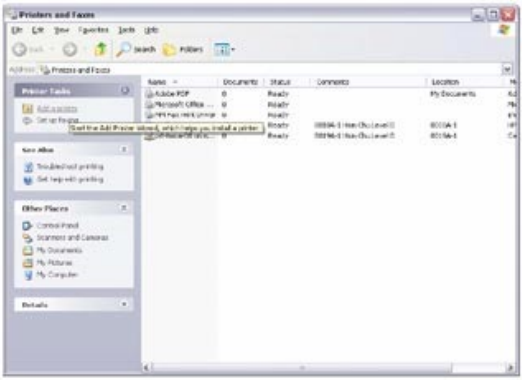
These steps explain the procedure for enabling the Print Server.

1: To enable the print server, Select Enable on-board print server checkbox and enter Printer name and Make and model

NOTE: The printer name can be any text string up to 40 characters. The Make and model can be any text string up to 128 characters.

FOR WINDOWS XP:

2: Go to the Printers and Faxes application in the Control Panel and select the Add a printer function (as located on the side menu below).



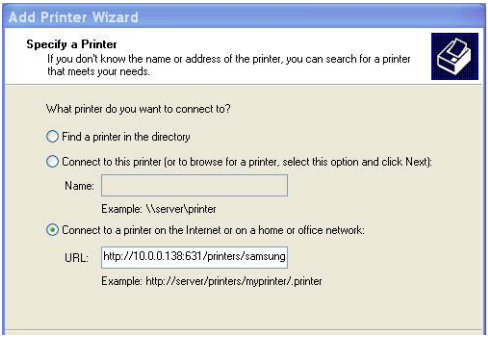
3: Click Next to continue, when you see the dialog box below.

4: Select Network Printer and click Next.

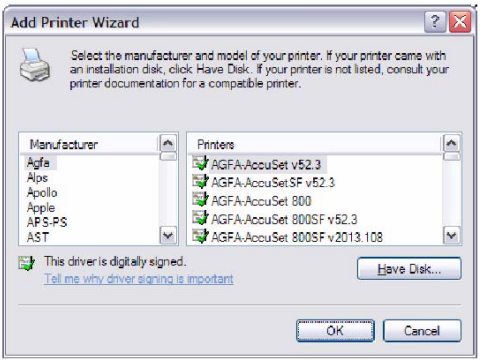
5: Select Connect to a printer on the Internet and enter your printer link.

(e.g. http://10.0.0.138:631/printers/printername) and click Next.

NOTE: the printer name must be the same name entered in the web user interface "printer server setting" as in step 1.



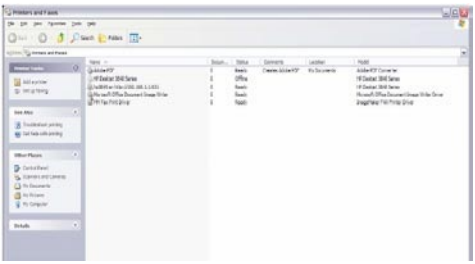
6: Click Have Disk and insert the printer driver CD.



7: Choose Yes or No for default printer setting and click Next.

8: Click “Finish”.

9: Check the status of printer from Windows Control Panel, printer window. Status should show as Ready.

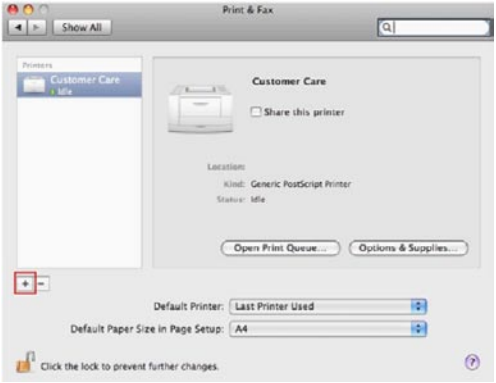


FOR MAC OSX:

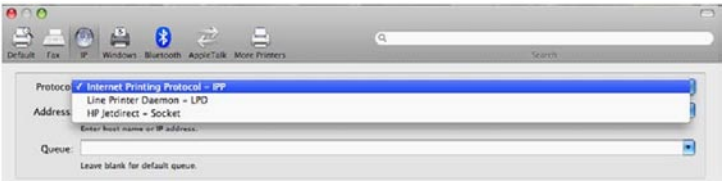
2. Browse to the Apple menu and select System Preferences. In the System Preferences menu click on Print & Fax.

3. With your Printer driver installed, please add your printer from the Printer & Fax menu.

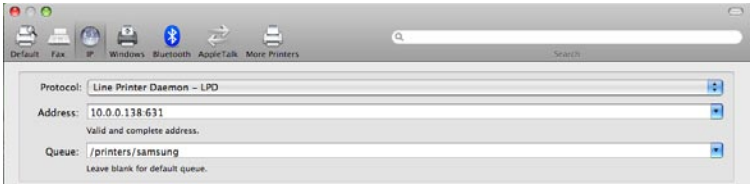
4. Click + to add your printer from the Print & Fax menu.



5. Select Internet Printing Protocol – IPP from the Protocol drop down list.



6. Type into the Address field “GatewayIPAddress:631” where GatewayIPAddress is the IP address of your Gateway (default: 10.0.0.138). See screenshot below for an example. Also enter into the Queue field “/printers/PrinterName”, where PrinterName is the name you gave your printer in step 1



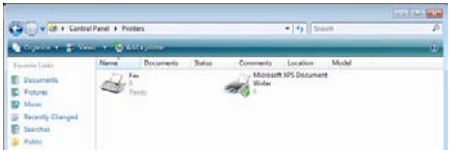
7. Select your printer from the Print Using drop down list.

8. Click Add and check the printer status.

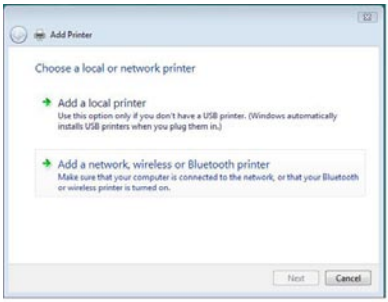
Print Server set up is now complete. You will now be able to print from common applications by selecting this printer from the Print dialogue box.

FOR WINDOWS VISTA

2. Go to the control panel, and select Printers. Once in the Printers page, click the Add a printer button as shown below.

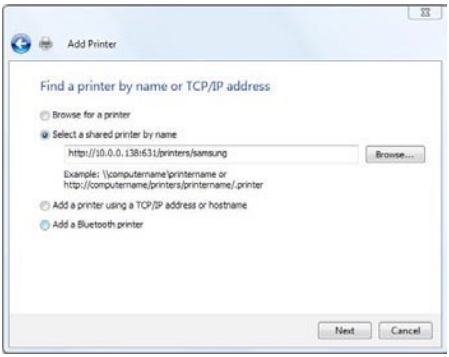


3. Select add a network, wireless or Bluetooth printer.

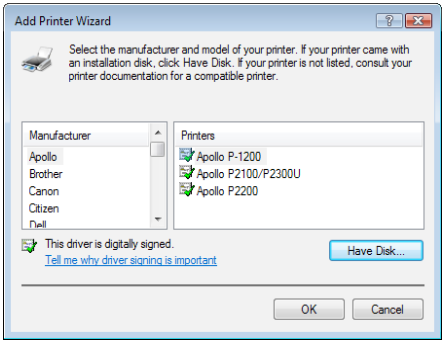


4. Click on the radio-button labeled Select a shared printer by name, and type "http://10.0.0.138:631/printers/PrinterName" in the box below. Click Next.

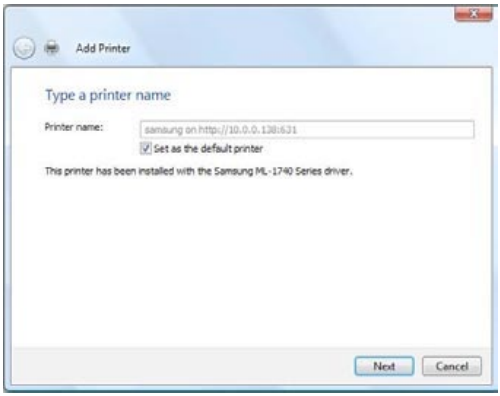
NOTE: The printername must be the same as the printer name entered in the Web User Interface during step 1



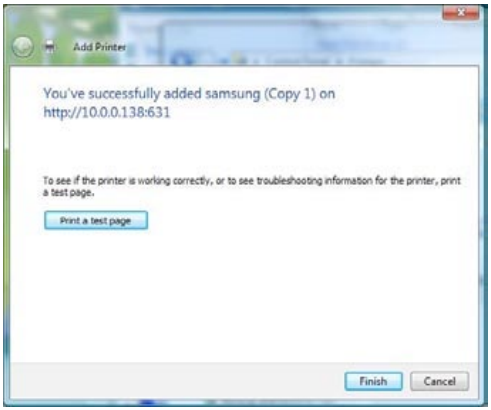
5. Next, select the driver that came with your printer. Browse through the list to select your printer driver, or click 'Have Disk' if you have your printer driver installation media.



6. Choose whether you want this printer to be the default printer, and then click Next.



7. Click Finish. Your device is now configured and ready for use.



7.11.2 USB STORAGE

The Bigpond Elite™ Wireless Broadband Network Gateway allows you to connect a USB storage device and share it with all of the users on the network.

By default, this feature is already enabled, so it is simply a matter of connecting your USB storage device and entering the appropriate network location.

If you wish to modify any of these features, the steps below explain the procedure for enabling the USB Storage.

1: Ensure that the Enable USB Storage checkbox is checked in the Web User Interface.

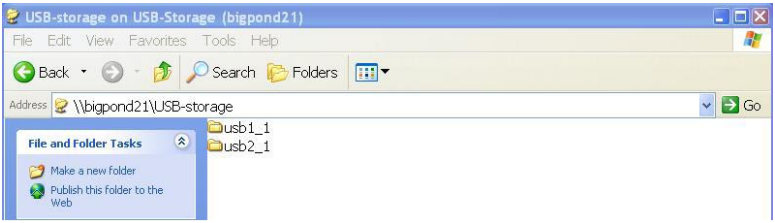
To do this, log into the device using the procedure found in Section 3.4 then select Advanced settings > USB settings > USB Storage from the menu along the top of the page. Enable USB Storage checkbox and enter the Gateway Name and USB Drive Name.

Field	Description
Gateway Name	The hostname of the Gateway device. This should only be modified if there are multiple Bigpond Elite™ Wireless Broadband Network Gateway's on your network. The default name is "BigPond21".
USB Drive Name	The name of USB drive. This should only be modified if there are multiple USB devices connected to your Bigpond EliteTM Wireless Broadband Network Gateway. The default name is "USB-Storage"

FOR WINDOWS XP:

2: Open a web-browser (such as Internet explorer, Firefox or Safari) and type in the address \\"GatewayName"\"USBDriveName"\ (e.g. \\Bigpond21\USB-Storage)

NOTE: There is no username and password required to access the USB drive, the user will be able to read/write the folder/files in the USB drive.



TO MAP THE USB STORAGE DRIVE

To enable easy access to the USB Storage Drive, you can map the network location. To do this, use the following steps:

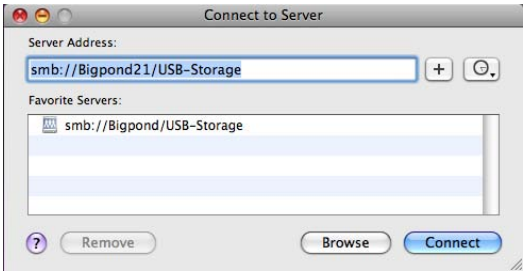
1. Click on the Start button and click My Computer
2. Clink on tools > Map network drive
3. In the Folder field, enter the address of the USB Storage Drive \\GatewayName\USBDriveName (e.g. \\Bigpond21\USB-Storage)
4. To access the USB Storage Drive in the future, you can simply double-click on the item in the My Computer menu

FOR MAC OSX:

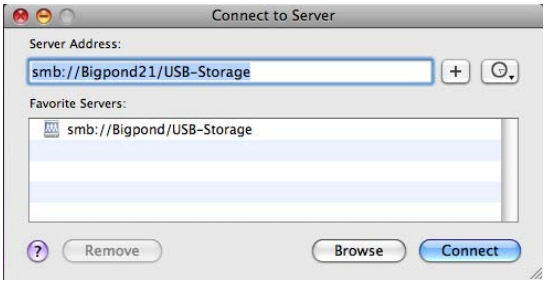
2. From the Finder, select the Go and then click Connect to Server

3. In the address field of the Connect to Server dialog, type in the address:

smb:// "GatewayName"/"USBDriveName" (e.g. smb://Bigpond21/USB-Storage)



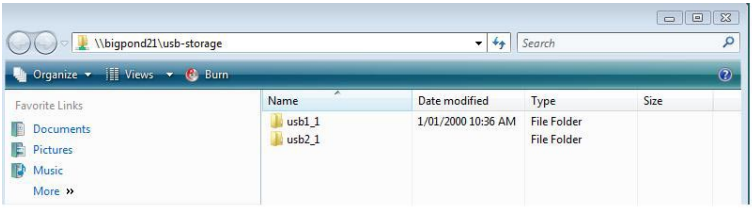
4. Click the + button to add this server to the list of Favourites and then click Connect



5. Select the Guest radio button and then click Connect

FOR WINDOWS VISTA

2. Open a web-browser (such as Internet explorer, Firefox or Safari)
3. Type in the address "\\GatewayName\USBDriveName\" (e.g. \\Bigpond21\USB-Storage)



NOTE: There is no username and password required to access the USB drive. Any network user will be able to read/write the folder/files in the USB drive.

TO MAP THE USB STORAGE DRIVE

To enable easy access to the USB Storage Drive, you can map the network location. To do this, use the following steps:

5. Click on the Start button and click Computer
6. Click the Map network drive button
7. In the Folder field, enter the address of the USB Storage Drive \\GatewayName\USBDriveName (e.g. \\Bigpond21\USB-Storage)
8. To access the USB Storage Drive in the future, you can simply double-click on the item in the Computer menu

7.12 SAVE AND REBOOT

This function saves the current configuration settings and reboots your Gateway.

NOTE1: 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.

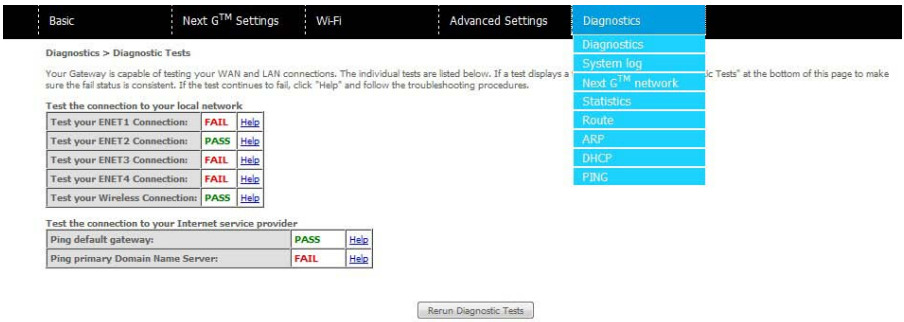
NOTE2: If you lose all access to your web user interface, simply press the reset button on the rear panel for 5-7 seconds to restore default settings.

DIAGNOSTICS

DIAGNOSTICS

The Diagnostics menu has the following submenus:

- Diagnostics
- System Log
- Next G™ Network
- Statistics
- Route
- ARP
- DHCP
- PING



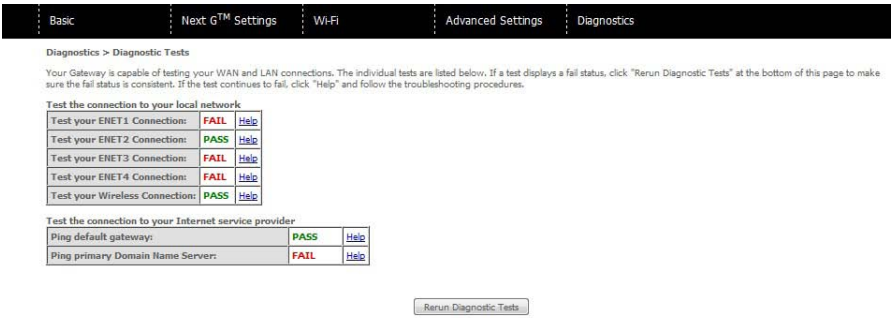
8.1 DIAGNOSTICS

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

2: Now click Re-run Diagnostic Tests at the bottom of the screen to re-test and confirm the error

3: If the test continues to fail, follow the troubleshooting procedures in the Help screen

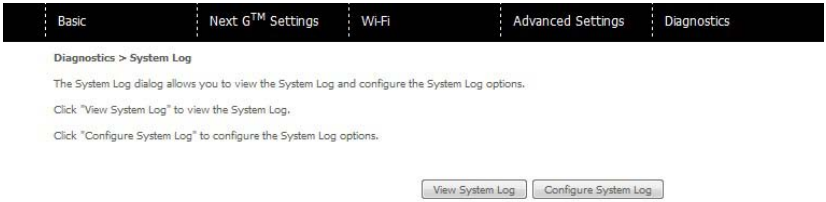


Name	Description
ENET Connection	Pass: Indicates that the Ethernet interface from your computer is connected to the LAN port of this Gateway.
	Fail: Indicates that the Gateway does not detect the Ethernet interface on your computer.
Wireless connection	Pass: Indicates that the wireless card is ON. Down: Indicates that the wireless card is OFF.
Ping Default Gateway	Pass: Indicates that the Gateway can communicate with the first entry point to the network. It is usually the IP address of the ISP's local Gateway.
	Fail: Indicates that the Gateway was unable to communicate with the first entry point on the network. It may not have an effect on your Internet connectivity. Therefore if this test fails but you are still able to access the Internet, there is no need to troubleshoot this issue.
Ping Primary Domain Name Server	Pass: Indicates that the Gateway can communicate with the primary Domain Name Server (DNS).
	Fail: Indicates that the Gateway was unable to communicate with the primary Domain Name Server (DNS). It may not have an effect on your Internet connectivity. Therefore if this test fails but you are still able to access the Internet, there is no need to troubleshoot this issue.

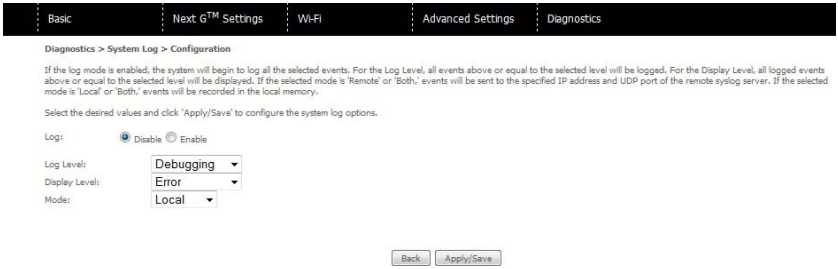
8.2 SYSTEM LOG

This function allows you to view system events and configure related options. Follow the steps below to enable and view the System Log.

1: Click Configure System Log to continue.

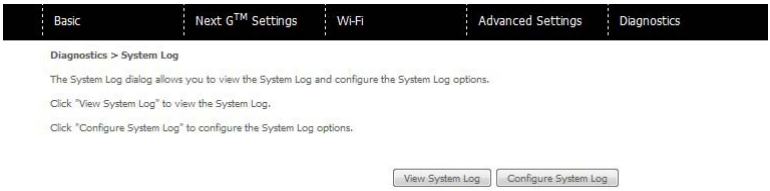


2: Select the system log options (see table below) and click Save/Apply.



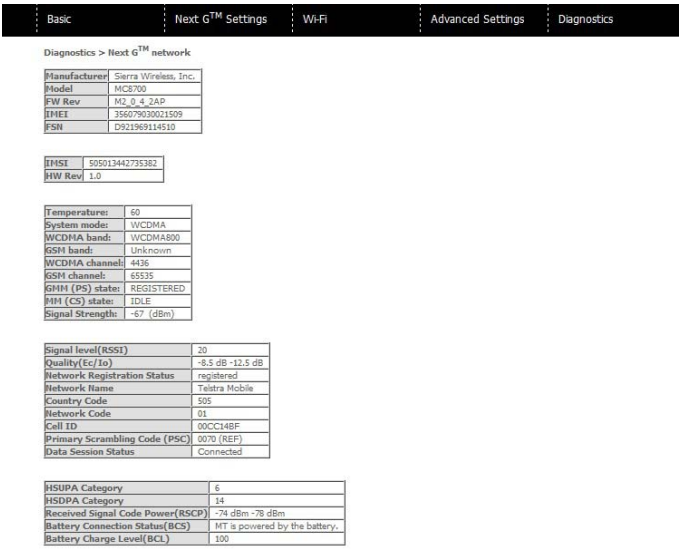
Name	Description
Log	Indicates whether the system is currently recording events. You can enable or disable event logging. By default, it is disabled.
Log level	Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the Gateway's SDRAM. When the log buffer is full, the newest event will wrap up to the top of the log buffer and overwrite the oldest event. By default, the log level is "Debugging", which is the lowest critical level. The log levels are defined as follows: Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level emergency level will be recorded. If the log level is set to error, only error and the level above will be logged.
Display Level	Allows you to select the logged events and displays on the View System Log window for events of this level and above to the highest emergency level.
Mode	Allows you to specify whether events should be stored in the local memory, be sent to a remote syslog server, or to both simultaneously. If remote mode is selected, the view system log will not be able to display events saved in the remote syslog server. When either Remote mode or Both mode is configured, the Web UI will prompt the you to enter the Server IP address and Server UDP port.

3: Click View System Log. The results are displayed as follows.

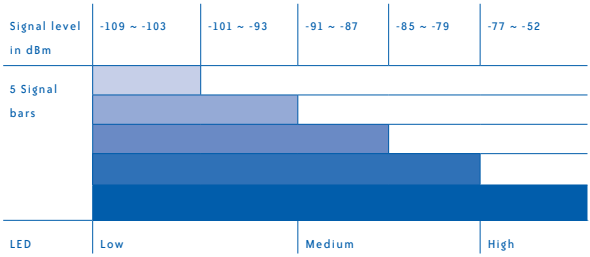


8.3 NEXT G™ NETWORK

Select this option for detailed status information on your Gateways 3G connection.



Consult the table on the next page for detailed field descriptions

Field	Description
Manufacturer	The manufacturer of the embedded 3G module.
Model	The model name of the embedded 3G module.
FW Rev.	The firmware version of the 3G module.
IMEI	The IMEI (International Mobile equipment Identity) is a 15 digit number that is used to identify a mobile device on a network.
FSN	Factory Serial Number of the 3G module.
IMSI	The IMSI (International Mobile Subscriber Identity) is a unique 15-digit number used to identify an individual user on a UMTS network.
HW Rev.	The hardware version of the 3G module.
Temperature	The temperature of the 3G module in degrees Celsius.
System Mode	WCDMA/Europe CMDA 2000 / America
WCDMA band	The 3G radio frequency band which supports dual-band UTMS/HSDPA/HSUPA frequencies (850/2100 MHz), IMT2000 is 2100 MHz, WCDMA800 is 850MHz
WCDMA channel	The 3G channel.
MM (CS) state	Circuit Switching state
Signal Strength	The 3G signal strength in dBm. 

8.4 STATISTICS

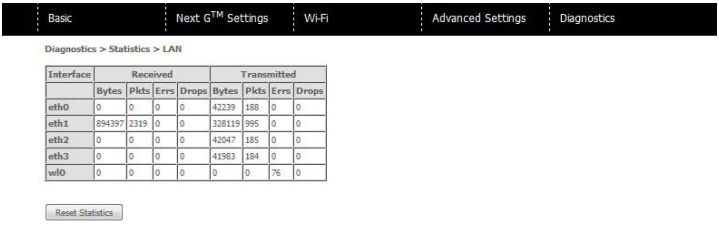
These screens provide detailed information for:

- Local Area Network (LAN) and Wireless Local Area Network (WLAN)
- 3G Interfaces

NOTE: These statistics page refresh every 15 seconds

8.4.1 LAN STATISTICS

This screen displays statistics for the Ethernet and Wireless LAN interfaces.



Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth0	0	0	0	0	42239	188	0	0
eth1	894397	2319	0	0	328119	995	0	0
eth2	0	0	0	0	42047	185	0	0
eth3	0	0	0	0	41983	184	0	0
wl0	0	0	0	0	0	0	76	0

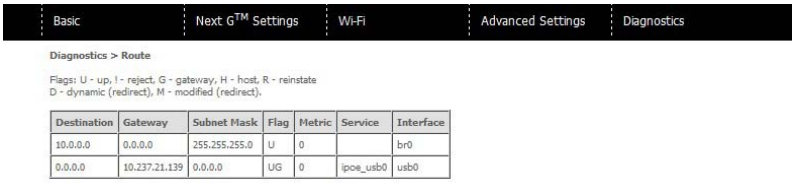
8.4.2 NEXT G™ STATISTICS

Click Next G™ network in the Statistics submenu to display the screen below.

Statistics of WAN	Inbound	Outbound
Octects	22784	771452
Packets	319	1121
Drops	0	0
Error	0	0

8.5 ROUTE

Select Route to display the paths the Gateway has found.



Field	Description
Destination	Destination network or destination host
Gateway	next hop IP address
Subnet Mask	Subnet mask of Destination
Flag	U: route is up
	!: reject route
	G: use gateway
	H: target is a host
	R: reinstate route for dynamic routing
	D: dynamically installed by daemon or redirect
	M: modified from routing daemon or redirect
Metric	The 'distance' to the target (usually counted in hops). It is not used by recent kernels, but may be needed by routing daemons.
Service	Shows the name for WAN connection
Interface	Shows connection interfaces

8.6 ARP

Click ARP to display the ARP information.

Field	Description
IP address	Shows IP address of host pc
Flags	Complete Incomplete Permanent Publish
HW Address	Shows the MAC address of host pc
Device	Shows the connection interface

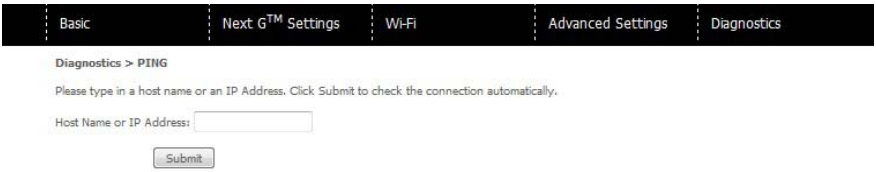
8.7 DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

Click DHCP to display the DHCP information.

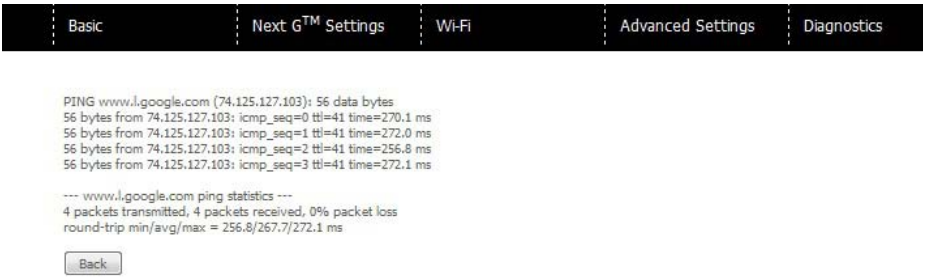
Field	Description
Hostname	Shows the device/host/Pc network name
MAC Address	Shows the Ethernet MAC address of the device/host/Pc
IP address	Shows IP address of device/host/Pc
Expires In	Shows how much time is left for each DHCP Lease

8.8 PING

The PING menu provides feedback of connection test to an IP address or a host name.



Input an IP address or a host name, e.g www.google.com and press Submit. The connection test result will be shown as below.



The above screen is showing a successful ping result.

TECHNICAL SUPPORT:
www.bigpond.com/help

BILLING AND ACCOUNT INFORMATION:
www.bigpond.com/mybigpond