TURBO 7 WIRELESS GATEWAY WITH VOICE (3G10WVT)

USER GUIDE

THANK YOU FOR PURCHASING A TELSTRA TURBO 7 WIRELESS GATEWAY WITH VOICE

PREFACE

The purpose of this manual is to provide you with detailed information on the installation, operation and application of your Turbo 7 Wireless Gateway with Voice

IMPORTANT NOTICE AND SAFETY PRECAUTION

- Before servicing or disassembling this equipment, always disconnect power from the device.
- Use an appropriate power supply, preferably the supplied power adapter, with an output of DC 12V 1.5A.
- Do not operate the device near flammable gas or fumes. Turn off the device when you are near a petrol station, fuel depot or chemical plant/depot. Operation of such equipment in potentially explosive atmospheres can represent a safety hazard.
- The device and antenna shall be used only with a minimum of 20 cm from the human body.
- The operation of this device may affect medical electronic devices, such as hearing aids and pacemakers.
- The Antennas must be connected to this product prior to connecting the telephone cord.
- The telephone cord must be disconnected prior to disconnecting the Antennas.

TABLE OF CONTENTS

1 – Introduction 6

1.1 Features 7

1.2 Package Contents 7

1.3 LED Indicators 8

1.4 Rear Panel 9

2 – Quick Setup 11

2.1 Setup Procedure 11

3 – Web user Interface 13

3.1 Default Settings 13

3.2 Transmission Control Protocol/Internet Protocol (TCP/IP) Settings 14

3.3 Login Procedure 18

3.4 Web User Interface Homepage 19

4 – Next G™ Settings 22

4.1 Next G™ Service Setup 22

4.1.1 Profile Setup 23

4.2 PIN Configuration 24

4.2.1 PIN Code Protection 24

4.2.2 PIN Code Change 26

5 – Wireless 28

5.1 Setup 29

5.2 Security 30

5.3 Configuration 32

5.4 Media Access Control (MAC) Filter 35

5.5 Wireless Bridge 36

5.6 Station Info 37

6 – Management 39

6.1 Device Settings 39

6.1.1 Backup Settings 39

6.1.2 Update Settings 40

6.1.3 Restore Default 40

6.1.4 Update Firmware 41

6.2 Access Control 42

6.2.1 Services 42

6.2.2 IP Addresses 43

6.2.3 Passwords 44

6.3 Configure SNMP agent on 3G10WVT 45
6.4 Simple Network Time Protocol (SNTP) 46
6.5 Save and Reboot 46

7 – Advanced setup 48
7.1 Local Area Network (LAN) 48
7.2 Network Address Translation (NAT) 50
7.2.1 Port Forwarding 50
7.2.2 Port Triggering 52
7.2.3 Demilitarized Zone (DMZ) Host 53
7.3 Security 54
7.3.1 IP Filtering 54
7.3.2 Parental Control 56
7.4 Routing 57
7.4.1 Default Gateway 57
7.4.2 Static Route 58
7.4.3 Dynamic Route 59
7.5 Domain Name System (DNS) 59
7.5.1 Domain Name System (DNS) Server 59
7.5.2 Dynamic Domain Name System (Dynamic DNS) 60

8 – Voice 62
8.1 Configuring your 3G10WVT for placing Voice Calls 62

9 – Status 64
9.1 Diagnostics 65
9.2 System Log 67
9.3 Next G™ Status 69
9.4 Statistics 72
9.4.1 LAN Statistics 72
9.4.2 Next G™ Statistics 73
9.5 Route 74
9.6 Address Resolution Protocol (ARP) 75
9.7 Dynamic Host Configuration Protocol (DHCP) 75
9.7 PING 76

Appendix A: Print Server 78

Appendix B: USB Storage 89

Appendix C: Command Line Interface (CLI) Commands Via Telnet 92

INTRODUCTION

INTRODUCTION

With the increasing popularity of the 3G standard worldwide, the Telstra Turbo 7 Wireless Gateway with Voice provides you with triple-band coverage through expanding cellular networks throughout the world.

By following the simple step-by-step instructions found on the Connection Manager USB key, you can share your connection with multiple wireless and wired devices using the Next G™ network.

The Gateway also provides state-of-the-art security features such as Wi-Fi Protected Access (WPA) data encryption, Firewall and Virtual Private Networks (VPN) pass through.

1.1 FEATURES

- The Telstra Turbo 7 Wireless Gateway with Voice allows you to share your Next G™ connection with multiple wireless or wired devices
- Provides you with worldwide coverage through triple-band HSUPA/HSDPA/UMTS (850 / 1900 / 2100MHz), quad-band EDGE/GSM (850 / 900 / 1800 / 1900 MHz)
- Embedded multi-mode HSUPA/HSDPA/UMTS/EDGE/GPRS/GSM module
- 1 x RJ11 port for voice calling over the Next G™ network via a connected standard Analogue Telephone (not included).
- Built-in USB 2.0 Print Server functionality
- Support for USB 2.0 Mass Storage device (NTFS, FAT 32)
- Integrated 802.11g/54Mbps AP (backward compatible with 802.11b)
- Wi-Fi Protected Access (WPA)/ Wi-Fi Protected Access 2 (WPA2) and 802.1x wireless encryption
- Static route/ Routing Information Protocol (RIP)/RIP v2 routing functions
- Media Access Control (MAC) address and IP filtering
- Network Address Translation (NAT) / Port Address Translation (PAT)
- Supports Universal Plug and Play (UPnP) and Internet Group Management Protocol (IGMP) snooping
- Supports Virtual Private Network (VPN) Pass-Through
- Dynamic Host Configuration Protocol (DHCP) Server/Relay/Client
- Domain Name System (DNS) Proxy and Dynamic Domain Name System (DDNS)
- Web-based Management
- Command Line Interface (CLI) via Telnet
- Configuration backup and restoration
- Remote configuration
- Gateway and Next G™ module firmware upgrade
- Supports half-bridging mode
- Supports Simple Network Management Protocol (SNMP)

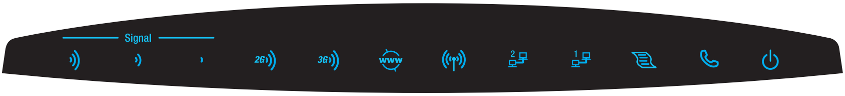
1.2 PACKAGE CONTENTS

Your package contains the following:

- Telstra Turbo 7 Wireless Gateway with Voice
- Printed Quick Start Guide
- USB Key (Containing Telstra Connection Manager and User Guide)
- Ethernet Cable
- Security Card
- 2 x 3G Antennas
- 1 x Wi-Fi Antenna
- Power Supply

1.3 LED INDICATORS

The LED indicators are shown in this illustration and followed by detailed explanations in the table below.

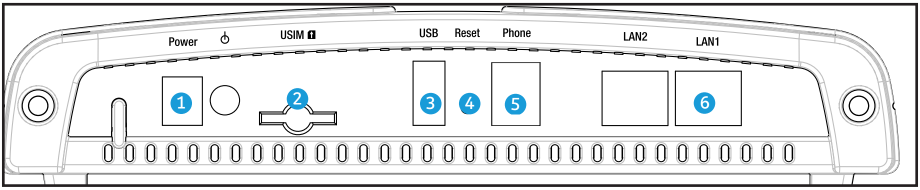


LED	Icon	Color	Mode	Description
POWER	⏻	Blue	On	Power on
			Off	Power off
Phone	☎	Blue	On	Phone line active
			Off	Phone line inactive or not connected
LAN 1~2	1 2	Blue	On	Powered device connected to the associated port (includes devices with wake-on-LAN capability where a slight voltage is supplied to an Ethernet connection)
			Off	No activity, modem powered off, no cable or no powered device connected to the associated port
			Blink	LAN activity present (traffic in either direction)
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.
Internet	www	Blue	Blink	Data is transmitted through Internet connection
			Off	No connection to the internet or gateway powered off
			On	Internet connection established
3G	3G	Blue	On	Connection established with 3G network
			Blink	Connecting with 3G network
			Off	No connection with UMTS cellular station, no activity, gateway powered off.
2G	2G	Blue	On	Connection established with 2G network
			Blink	Connecting to an EDGE, GPRS or GSM cellular station
			Off	No connection with EDGE, GPRS or GSM cellular station, no activity or gateway powered off.
Low	›	Blue	On	Low signal strength
			Off	No activity, gateway powered off or on other signal strength
Med	›)	Blue	On	Medium signal strength
			Off	No activity, gateway powered off or on other signal strength
High	›))	Blue	On	High signal strength
			Off	No activity, gateway powered off or on other signal strength

NOTE: The six LEDs on the left side of the top panel display (Low, Med, High, Internet, 3G, 2G) will cycle on and off if PIN code protection is activated. In this case, you should consult section 4.2.1 PIN Code Protection (page 21) for further instructions.

1.4 REAR PANEL

The rear panel contains the ports for data and power connections.



(1) Power jack for DC power input (12VDC / 1.5A)/Power button

(2) USIM card slot

(3) USB Port (For connecting a USB Printer or USB Storage Device)

(4) Reset button

(5) Phone Port (for Voice calls over the Next G™ Network)

(6) 2 RJ-45 Ethernet LAN ports

QUICK SETUP

QUICK SETUP

2.1 SETUP PROCEDURE (WITHOUT USB KEY)

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

1: Attach the two 3G antennas provided to the ports marked MAIN 3G and AUX 3G on the front of the gateway. The antennas should be screwed in a clockwise direction.

2: Attach the Wi-Fi antenna provided to the port marked WI-FI on the front of the Gateway. The antenna should be screwed in a clockwise direction.

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

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

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

6: If required, connect a standard Analogue Telephone (not included) to the port labeled "Phone" using a standard telephone cable (not included).

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

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

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

NOTE: Chapters 3 through 8 explain how to set up and use the WUI

10: Save the Gateway configuration and reboot (see section 6.5).

WEB USER INTERFACE

WEB USER INTERFACE

This section describes how to access the device via the web user interface using a web browser such as Microsoft Internet Explorer (version 5.0 or later), Mozilla Firefox or Safari.

3.1 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 6.1.3).

3.2 TCP/IP SETTINGS

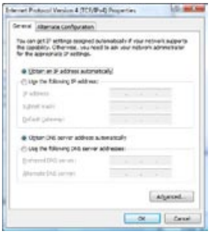
It is likely that your computer will automatically obtain an IP Address and join the network. This is because the Dynamic Host Configuration Protocol (DHCP) server (on the device) will start automatically when your Gateway powers up.

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 below.

WINDOWS XP

DHCP Mode

To set your PC for DHCP mode, check the Internet Protocol properties of your Local Area Connection. You can set your PC to DHCP mode by selecting Obtain an IP address automatically in the dialog box shown below.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

Advanced...

OK | Cancel

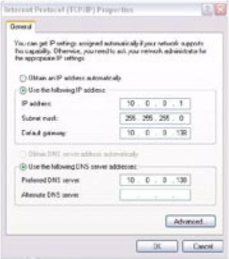
STATIC IP Mode

The following steps show how to configure your PC IP address using subnet 10.0.0.x. The following assumes you are running Windows XP.

1: From the Network Connections window, open Local Area Connection (You may also access this screen by double-clicking the Local Area Connection icon on your taskbar). Click the Properties button.

2: Select Internet Protocol (TCP/IP) and click the Properties button. The screen should now display as below. Change the IP address to the domain of 10.0.0.x. (1<x<254) with subnet mask of 255.255.255.0. 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 10.0.0.1



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 0 . 0 . 1

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 0 . 0 . 138

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 10 . 0 . 0 . 138

Alternate DNS server: . . .

Advanced...

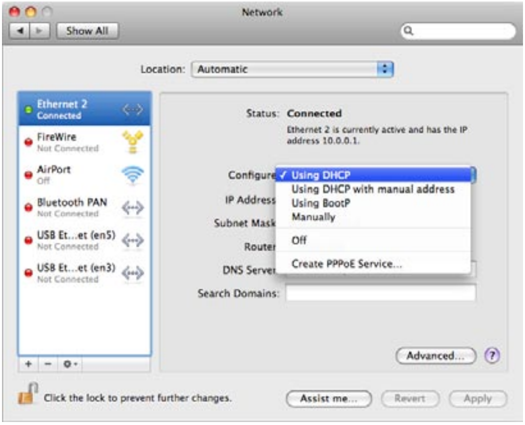
OK | Cancel

3: Click OK to submit the settings.

MAC OSX 10.4

DHCP Mode

To set your Apple Mac for DHCP mode, browse to the Apple menu and select System Preferences. In the System Preferences menu, click on the Network icon and select Ethernet. Next select Using DHCP from the Configure drop down list. After clicking Apply, your Mac's IP Address will now be automatically assigned from the Gateway.



Location: Automatic

Status: Connected

Ethernet 2 is currently active and has the IP address 10.0.0.1.

Configure: ✓ Using DHCP

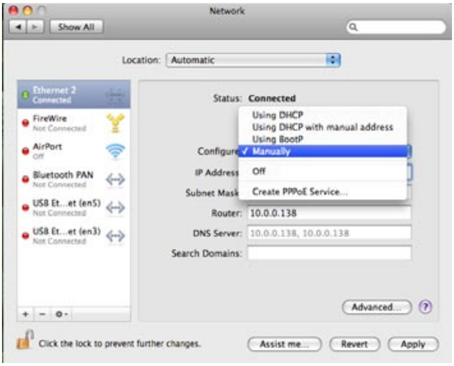
Click the lock to prevent further changes.

STATIC Mode

If you do not wish to use automatic assignment of IP Addresses and wish to configure your Gateway manually, your computer must have a static IP address within the Gateway's subnet. The following steps show how to configure your computer's IP address within the subnet 10.0.0.x

1. Browse to the Apple menu and select System Preferences. From the System Preferences, click the Network icon and select the Ethernet connection.

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



Location: Automatic

Status: Connected

Configure: ✓ Manually

Router: 10.0.0.138

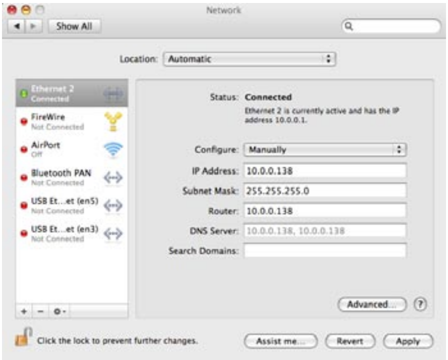
DNS Server: 10.0.0.138, 10.0.0.138

Search Domains:

3. 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

4. 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 10.0.0.1



Location: Automatic

Status: Connected

Ethernet 2 is currently active and has the IP address 10.0.0.1.

Configure: Manually

IP Address: 10.0.0.138

Subnet Mask: 255.255.255.0

Router: 10.0.0.138

DNS Server: 10.0.0.138, 10.0.0.138

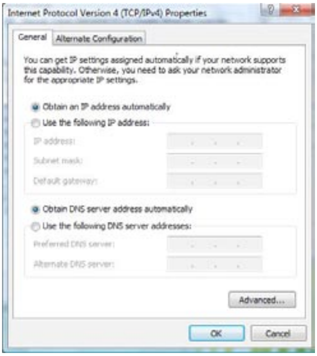
Search Domains:

5. Click Apply to submit the settings.

WINDOWS VISTA

DHCP Mode

To set your PC for DHCP mode, click properties of your Local Area Connection. You can set your PC to DHCP mode by selecting Obtain an IP address automatically in the dialog box shown below.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

STATIC IP Mode

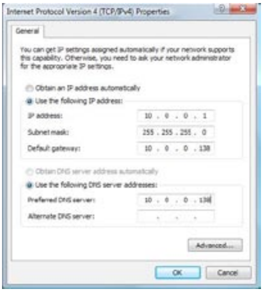
To configure your Gateway manually, your PC must have a static IP address within the Gateway's subnet. The following steps show how to configure your PC IP address using subnet 10.0.0.x. The following assumes you are running Windows Vista.

1: From the Network Connections window, open Local Area Connection (You may also access this screen by double-clicking the Local Area Connection icon on your taskbar). Click the Properties button.

2: Select Internet Protocol (TCP/IPv4) and click the Properties button. The screen should now display as below. 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

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 0 . 0 . 1

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 0 . 0 . 138

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 10 . 0 . 0 . 138

Alternate DNS server: . . .

3. Click OK to apply the settings.

3.3 LOGIN PROCEDURE

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

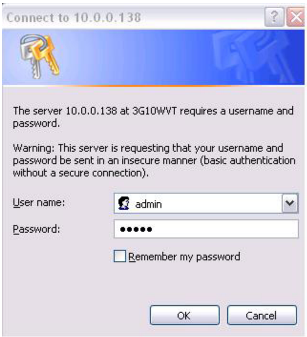
NOTE: The default settings can be found in 3.1 Default Settings.

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 3.1 Default Settings.

Click OK to continue.



Connect to 10.0.0.138

The server 10.0.0.138 at 3G10WVT requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

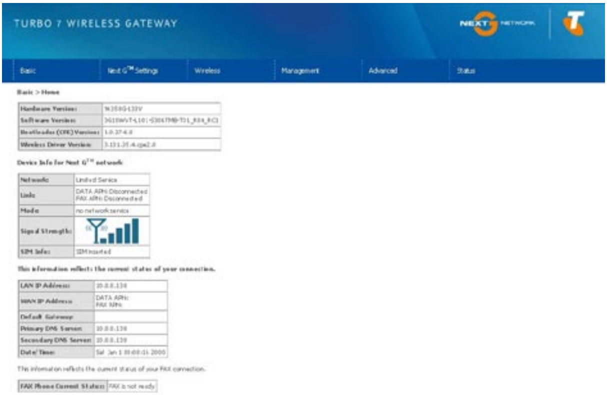
User name: admin

Password: •••••

□ Remember my password

NOTE: The login password can be changed later (see 6.2.3 Passwords)

3: After successfully logging in for the first time, you will reach this screen.



Basic > Home

Hardware Version:	W358G-133V
Software Version:	3G10WVT-L101-S306TMB-T01_R04_RC1
Bootloader (CFE) Version:	1.0.37-6.8
Wireless Driver Version:	3.131.35.4.cpe2.8

Device Info for Next G™ network

Network:	Limited Service
Link:	DATA APN: Disconnected FAX APN: Disconnected
Mode:	no network service
Signal Strength:	
SIM Info:	SIM inserted

This information reflects the current status of your connection.

LAN IP Address:	10.0.0.138
WAN IP Address:	DATA APN: FAX APN:
Default Gateway:	
Primary DNS Server:	10.0.0.138
Secondary DNS Server:	10.0.0.138
Date/ Time:	Sat Jan 1 00:00:01 2000

This information reflects the current status of your FAX connection.

FAX Phone Current Status:	FAX is not ready

3.4 WEB USER INTERFACE HOMEPAGE

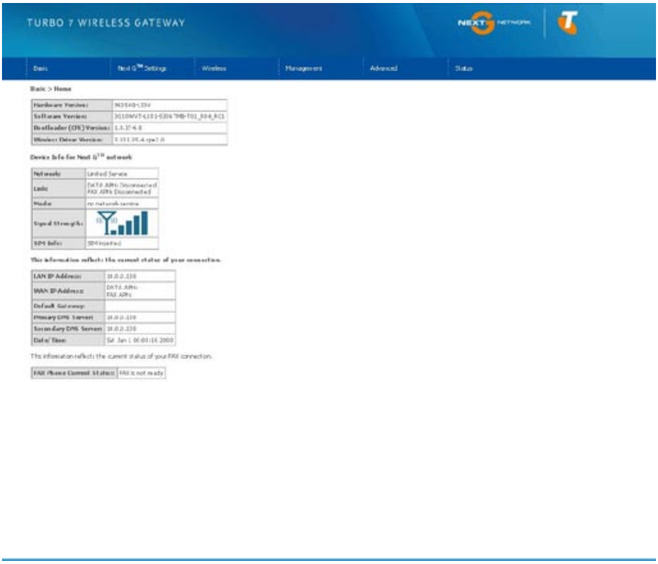
The web user interface (WUI) is divided into two window panels, the main menu (on the top) and the display screen (on the bottom). The main menu has the following options: Basic, Next G™ Settings, Wireless, Management, Advanced and Status.

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.



Basic > Home

Hardware Version:	[illegible]
Software Version:	3G10WVT-L101-S306TMB-T01_R04_RC1
Bootloader (CFE) Version:	[illegible]
Wireless Driver Version:	[illegible]

Device Info for Next G™ network

Network:	Limited Service
Link:	DATA APN: Disconnected FAX APN: Disconnected
Mode:	no network service
Signal Strength:	
SIM Info:	SIM inserted

This information reflects the current status of your connection.

LAN IP Address:	10.0.0.138
WAN IP Address:	DATA APN: FAX APN:
Default Gateway:	
Primary DNS Server:	10.0.0.138
Secondary DNS Server:	10.0.0.138
Date/Time:	Sat Jan 1 00:03:16 2000

This information reflects the current status of your FAX connection.

FAX Phone Current Status:	FAX is not ready

The following table provides further details.

Fields	Description
Software version	The software version of the device.
Hardware version	The Hardware version of the device
Bootloader version	The bootloader 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, EDGE, GPRS or Disconnected.
Signal strength	The mobile network (UMTS or GSM) 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.
Default Gateway	Shows the IP address of the default gateway for the 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 G™ SETTINGS

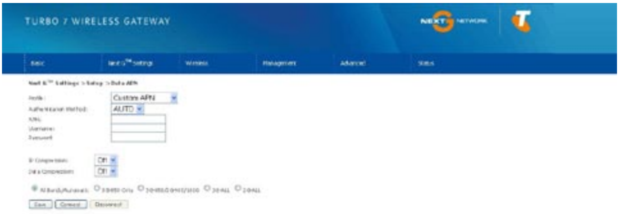
NEXT G™ SETTINGS

This menu includes Next G™ service Setup and PIN Configuration.

NOTE: Sections 9.3 and 9.4.2 also provide information about the Next G™ service.

4.1 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.



Next G™ Settings > Setup > Data APN

Profile : Custom APN
Authentication Method: AUTO
APN:
Username:
Password:

IP Compression: Off
Data Compression: Off

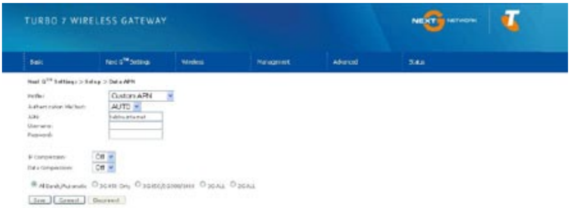
● All Bands/Automatic ○ 3G850 Only ○ 3G850/2G 900/1800 ○ 3G ALL ○ 2G ALL

4.1.1 Profile Setup

Telstra 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 Telstra; or just leave it AUTO if not acquired. If you have not received the username and password, leave these fields empty.



Next G™ Settings > Setup > Data APN

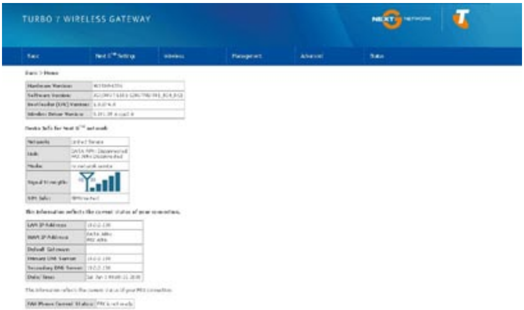
Profile: Custom APN
Authentication Method: AUTO
APN: telstra.internet
Username:
Password:

IP Compression: Off
Data Compression: Off

● All Bands/Automatic ○ 3G 850 Only ○ [illegible] ○ 2G ALL ○ 3G ALL

Save Connect Disconnect

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.



Basic > Home

Hardware Version:	[illegible]
Software Version:	[illegible]
Bootloader (CFE) Version:	[illegible]
Wireless Driver Version:	[illegible]

Device Info for Next G™ network

Network:	[illegible]
Link:	[illegible]
Mode:	[illegible]
Signal Strength:	
SIM Info:	[illegible]

This information reflects the current status of your connection.

LAN IP Address:	[illegible]
WAN IP Address:	[illegible]
Default Gateway:	
Primary DNS Server:	[illegible]
Secondary DNS Server:	[illegible]
Date/Time:	[illegible]

[illegible]

[illegible] Status:	[illegible]

.

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.

NOTE: If the LEDs light in an on/off pattern moving from left to right this indicates that your SIM is PIN Locked, please see PIN Lock Off on page 24 for instruction on how to fix this

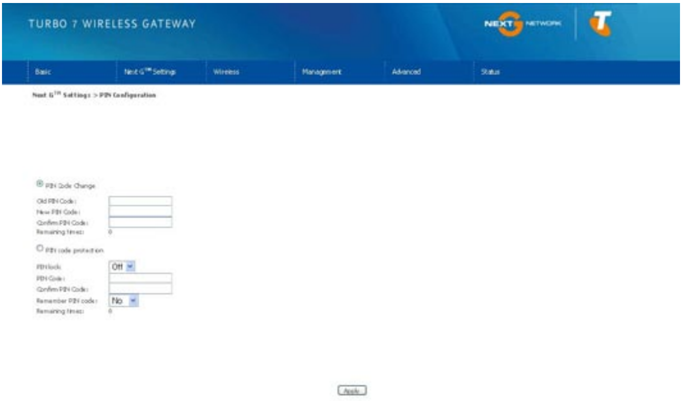
4.2 PIN CONFIGURATION

This screen allows for changes to the 3G SIM card PIN code protection settings.

NOTE: If you have entered the incorrect PIN 3 times, your SIM card will be locked for your security. Please call Telstra for assistance.

4.2.1 PIN Code Protection

PIN code protection prevents the use of a SIM card by unauthorized persons. To use the 3G internet service with this gateway however, the PIN code protection must be disabled. If the SIM card inserted into the Gateway is locked with a PIN code, the web user interface will display the following screen after login.



Next G™ Settings > PIN Configuration

● PIN Code Change

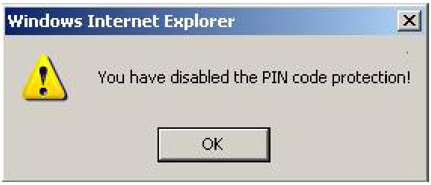
Old PIN Code:	
New PIN Code:	
Confirm PIN Code:	
Remaining times:	0

○ PIN code protection

PIN lock:	Off
PIN Code:	
Confirm PIN Code:	
Remember PIN code:	No
Remaining times:	0

PIN Lock Off

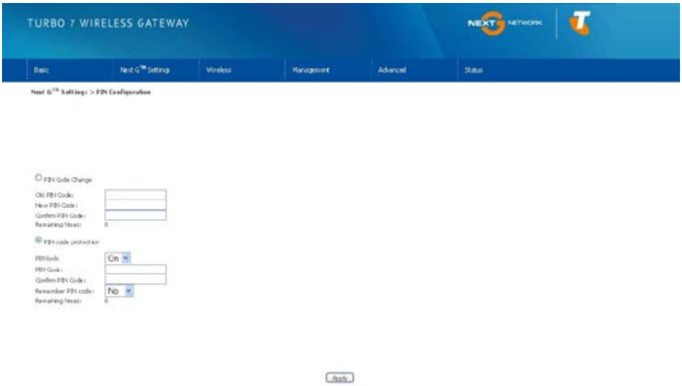
If you wish to connect to the Internet using a PIN locked SIM card, you must first turn PIN code protection Off. Select PIN lock Off, enter the PIN Code twice. Please keep in mind you only have 3 attempts before your SIM card is locked. The remaining attempts' number shows how many attempts left. Contact Telstra if you require assistance. You can select Remember PIN Code to ON so you don't need to input the PIN code every time when the gateway turns on. Afterwards, click Apply. The following dialog box should now appear.



You have disabled the PIN code protection!

PIN Lock On

After you are finished using your SIM card for Internet service, you may wish to lock it again. In this case, first go to the 3G Settings - PIN Configuration screen, as shown below. Select PIN lock ON, enter the PIN code twice. You can select Remember PIN code to Yes so you don't need to input the PIN code every time when the gateway turns on. Then click Save.



Next G™ Settings > PIN Configuration

○ PIN Code Change

Old PIN Code:

New PIN Code:

Confirm PIN Code:

Remaining times: 0

● PIN code protection

PIN lock: On

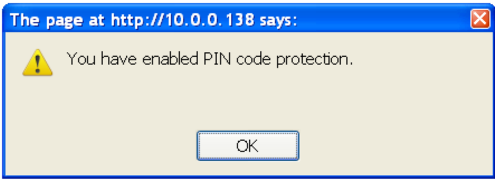
PIN Code:

Confirm PIN Code:

Remember PIN code: No

Remaining times: 0

After you do so, the following dialog box should appear.



The page at http://10.0.0.138 says:

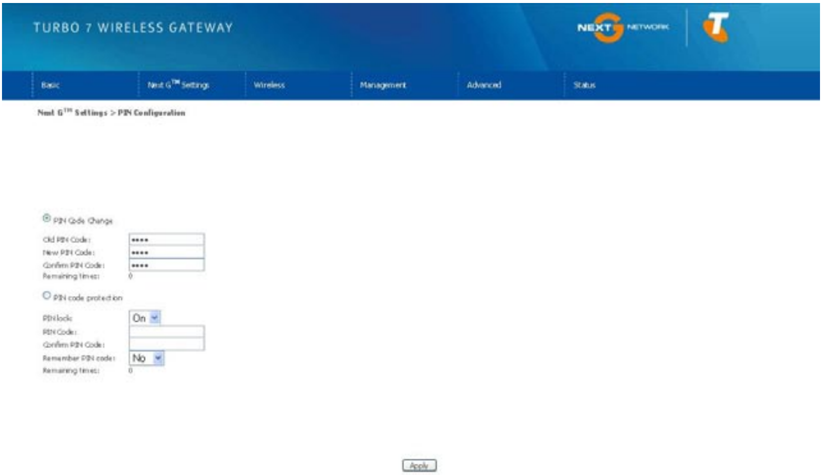
You have enabled PIN code protection.

You can now return your SIM card to your cellular phone or other mobile device.

4.2.2 PIN Code Change

If you wish to change your PIN code for greater security, enable the PIN Code protection. Go to the previous section and follow the procedure listed under PIN Lock On.

After locking the SIM card, select **PIN Code Change** and enter your Old and New PIN codes in the fields provided. Keep in mind you only have 3 attempts before your SIM card is locked. The remaining attempts' number shows how many attempts left. Contact Telstra if you require assistance. Afterwards, click Apply to activate the change.



Next G™ Settings > PIN Configuration

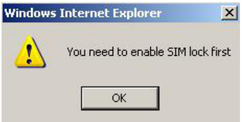
● PIN Code Change

Old PIN Code: ••••
New PIN Code: ••••
Confirm PIN Code: ••••
Remaining times: 0

○ PIN code protection

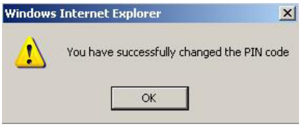
PIN lock: On
PIN Code:
Confirm PIN Code:
Remember PIN code: No
Remaining times: 0

NOTE: If you forget to change the PIN Code without first turning on PIN lock protection, you will see this dialog box as a helpful reminder.



You need to enable SIM lock first

NOTE: If your PIN Code change request was successful the following dialog box will display.



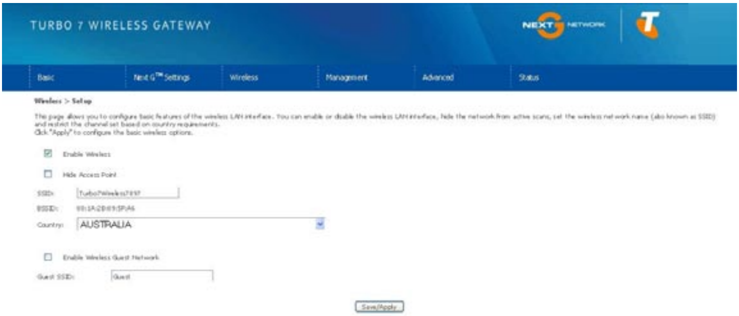
You have successfully changed the PIN code

WIRELESS

WIRELESS

The Wireless 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



Wireless > Setup

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" to configure the basic wireless options.

☑ Enable Wireless

□ Hide Access Point

SSID: Turbo7Wireless7897

BSSID: 00:1A:2B:03:5F:A6

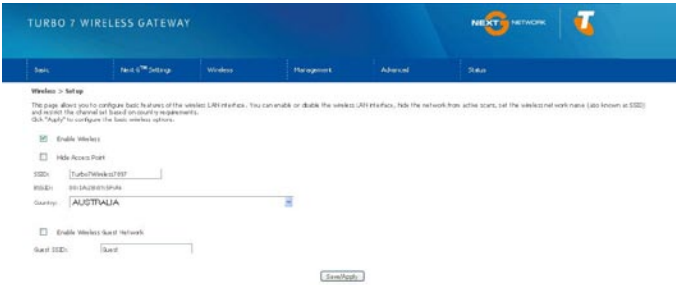
Country: AUSTRALIA

□ Enable Wireless Guest Network

Guest SSID: Guest

5.1 SETUP

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.



Wireless > Setup

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" to configure the basic wireless options.

☑ Enable Wireless

□ Hide Access Point

SSID: Turbo7Wireless7897

BSSID: [illegible]

Country: AUSTRALIA

□ Enable Wireless Guest Network

Guest SSID: Guest

Option	Description
Enable Wireless	A checkbox that enables (default) or disables the wireless LAN interface. When selected, the Web UI displays Hide Access point, SSID, BSSID and Country settings.
Hide Access Point	Select Hide Access Point 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.
SSID [1-32 characters]	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.
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 (Media 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.
Wireless Guest Network	The Guest SSID (Virtual Access Point) can be enabled by selecting the Enable Wireless Guest Network checkbox. Rename the Wireless Guest Network as you wish. NOTE: Remote wireless hosts cannot scan Guest SSIDs.

5.2 SECURITY

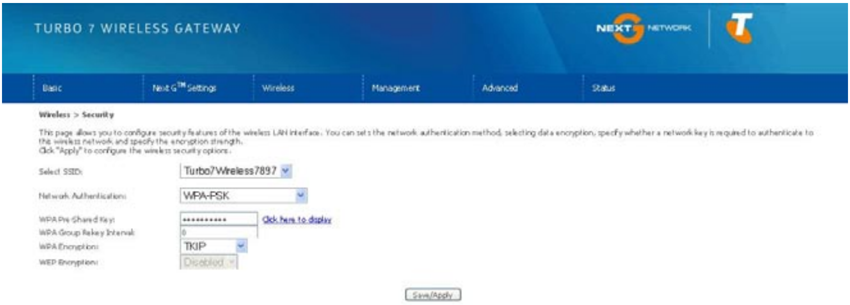
This Gateway includes a number of options to help provide a secure connection to the Next G™ Network.

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.

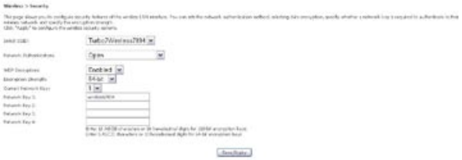
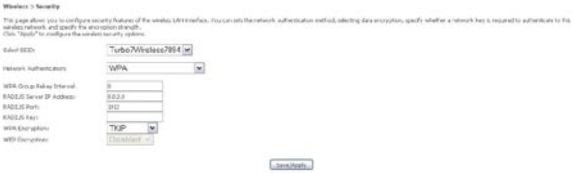
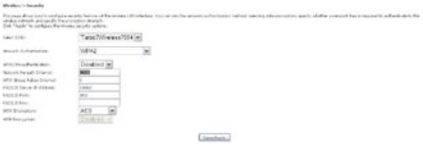


Wireless > Security

This page allows you to configure security features of the wireless LAN interface. You can sets the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to the wireless network and specify the encryption strength.
Click "Apply" to configure the wireless security options.

Select SSID:	Turbo7Wireless7897
Network Authentication:	WPA-PSK
WPA Pre-Shared Key:	**********
WPA Group Rekey Interval:	0
WPA Encryption:	TKIP
WEP Encryption:	Disabled

Click Save/Apply to configure the wireless security options.

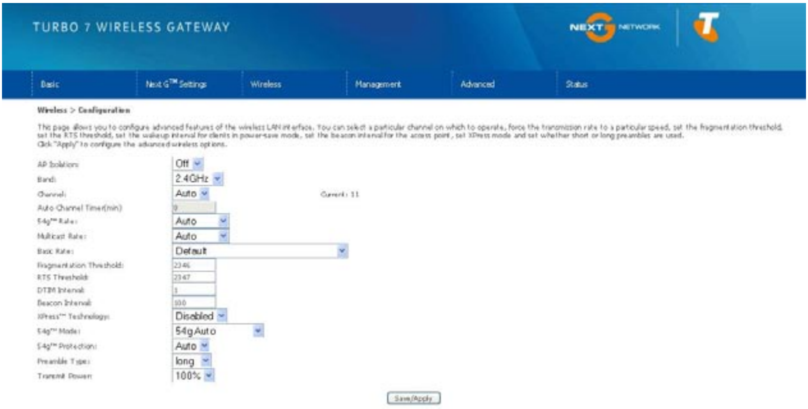
Select SSID	Your Service Set Identifier (SSID), sets your Wireless Network Name. You can connect multiple devices including Laptops, Desktop PCs and PDAs to your Wireless Gateway. To get additional devices connected, scan for a network, and locate the SSID shown on your Wireless Security Card. If the 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 as illustrated below. For example, selecting 802.1X authentication will reveal the RADIUS Server IP address, Port and Key fields. WEP Encryption will also be enabled.  Wireless > Security Select SSID: Turbo7Wireless7894 Network Authentication: Open WEP Encryption: Enabled Encryption Strength: 64-bit Current Network Key: 1 Network Key 1: Network Key 2: Network Key 3: Network Key 4: The settings for WPA authentication are shown below.  Wireless > Security This page allows you to configure security features of the wireless LAN interface. You can sets 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" to configure the wireless security options. Select SSID: Turbo7Wireless7894 Network Authentication: WPA WPA Group Rekey Interval: 0 RADIUS Server IP Address: 0.0.0.0 RADIUS Port: 1812 RADIUS Key: WPA Encryption: TKIP WEP Encryption: Disabled  Wireless > Security Select SSID: Turbo7Wireless7894 Network Authentication: WPA2 WPA2 Preauthentication: Disabled Network Re-auth Interval: WPA Group Rekey Interval: RADIUS Server IP Address: RADIUS Port: RADIUS Key: WPA Encryption: AES WEP Encryption: Disabled
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. Use the network key found in the drop down list.
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.

5.3 CONFIGURATION

The following screen appears when you select Configuration. This screen allows you to control the following 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.



Wireless > Configuration

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" to configure the advanced wireless options.

AP Isolation:	Off	
Band:	2.4GHz	
Channel:	Auto	Current: 11
Auto Channel Timer(min)	0	
54g™ Rate:	Auto	
Multicast Rate:	Auto	
Basic Rate:	Default	
Fragmentation Threshold:	2346	
RTS Threshold:	2347	
DTIM Interval:	1	
Beacon Interval:	100	
XPress™ Technology:	Disabled	
54g™ Mode:	54g Auto	
54g™ Protection:	Auto	
Preamble Type:	long	
Transmit Power:	100%	

Option	Description
AP Isolation	Select On or Off. By enabling this feature, wireless clients associated with the Access Point can be linked.
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	Allows selection of a specific channel (1-14) or Auto mode.
Auto Channel Timer (min)	The Auto Channel times the length it takes to scan in minutes.
54g Rate	In Auto (default) mode, your Gateway uses the maximum data rate and lowers the data rate dependent on the signal strength. The appropriate setting is dependent on signal strength. Other rates are discrete values between 1 to 54 Mbps.
Multicast Rate	Setting for multicast packet transmission rate. (1-54 Mbps)
Basic Rate	Sets basic transmission rate.
Fragmentation Threshold	A threshold (in bytes) determines whether packets will be fragmented and at what size. Packets that exceed the fragmentation threshold of an 802.11 WLAN will be split into smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value however are not fragmented. Values between 256 and 2346 can be entered but should remain at a default setting of 2346. Setting the Fragmentation Threshold too low may result in poor performance.
RTS Threshold	Request To Send (RTS) specifies the packet size that exceeds the specified RTS threshold, which then triggers the RTS/CTS mechanism. Smaller packets are sent without using RTS/CTS. The default setting of 2347 (max length) will disables the RTS Threshold.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown variable that informs 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 in is milliseconds. The default is 100 ms and the acceptable range is 1 – 65535. The beacon transmissions identify the presence of an access point. By default, network devices passively scan all RF channels listening for beacons coming from access points. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon.
Xpress™ Technology	Broadcom's Xpress™ Technology is compliant with draft specifications of two planned wireless industry standards. It has been designed to improve wireless network efficiency. Default is disabled.

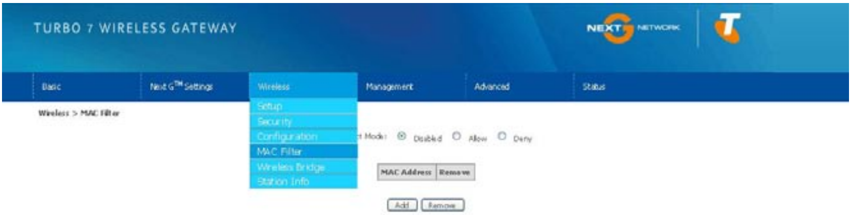
Option	Description
54g Mode	Select Auto mode for greatest compatibility. Select Performance mode for the fastest performance among 54g certified equipment. Select LRS mode if you are experiencing difficulty with legacy 802.11b equipment. If this does not work, you may also try 802.11b only mode.
54g Protection	In Auto mode, the gateway will use RTS/CTS to improve 802.11g performance in mixed 802.11g/802.11b networks. Turning protection Off will maximize 802.11g throughput under most conditions.
Preamble Type	Short preamble is intended for applications where maximum throughput is desired but it does not work with legacy equipment. Long preamble works with the current 1 and 2 Mbit/s DSSS specification as described in IEEE Std 802.11-1999
Transmit Power	Set the power output (by percentage) as desired.

5.4 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.



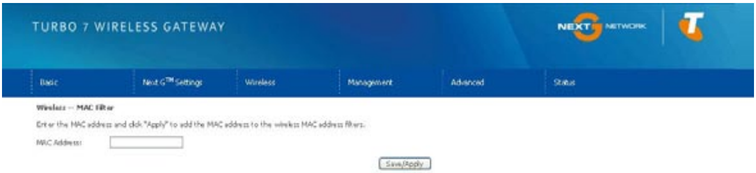
Wireless > MAC Filter

t Mode: ● Disabled ○ Allow ○ Deny

MAC Address	Remove

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.



Wireless -- MAC Filter

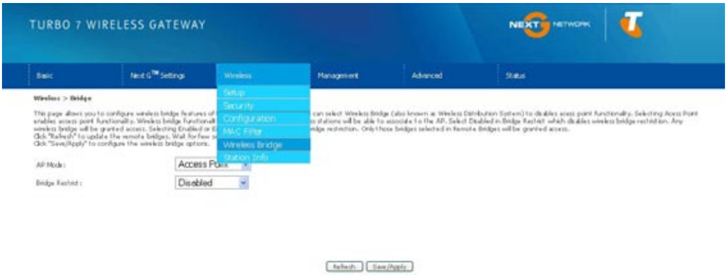
Enter the MAC address and click "Apply" to add the MAC address to the wireless MAC address filters.

MAC Address:

5.5 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.



Wireless > Bridge

This page allows you to configure wireless bridge features of
can select Wireless Bridge (also known as Wireless Distribution System) to disables acess point functionality. Selecting Acess Point
enables access point functionality. Wireless bridge functionalit
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 or E
idge restriction. Only those bridges selected in Remote Bridges will be granted access.
Click "Refresh" to update the remote bridges. Wait for few s
Click "Save/Apply" to configure the wireless bridge options.

AP Mode: Access Point

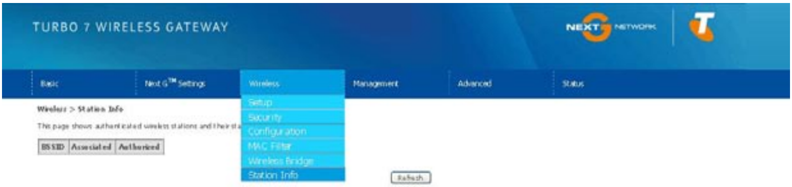
Bridge Restrict: Disabled

Feature	Options
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.

5.6 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.



Wireless > Station Info

This page shows authenticated wireless stations and their sta

BSSID	Associated	Authorized

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.

MANAGEMENT

MANAGEMENT

The Management menu has the following maintenance functions and processes:

6.1 Device Settings

6.2 Access Control

6.3 Simple Network Management Protocol (SNMP)

6.4 Simple Network Time Protocol (SNTP)

6.5 Save and Reboot

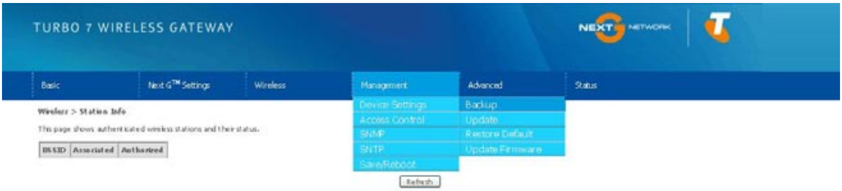
6.1 DEVICE SETTINGS

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.

6.1.1 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.



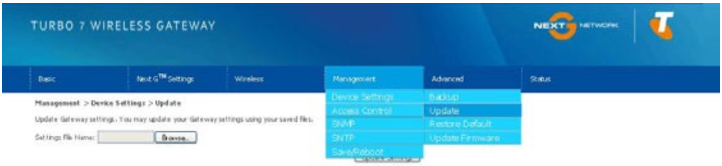
Wireless > Station Info

This page shows authenticated wireless stations and their status.

BSSID	Associated	Authorized

6.1.2 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.



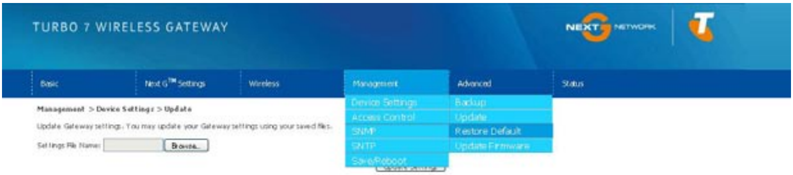
Management > Device Settings > Update

Update Gateway settings. You may update your Gateway settings using your saved files.

Settings File Name:

6.1.3 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.



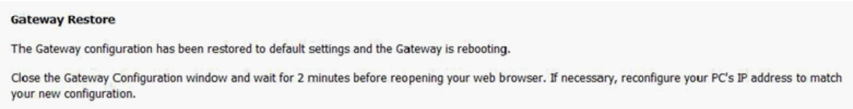
Management > Device Settings > Update

Update Gateway settings. You may update your Gateway settings using your saved files.

Settings File Name:

NOTE: The default settings can be found in section 3.1 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).



Gateway Restore

The Gateway configuration has been restored to default settings and the Gateway is rebooting.

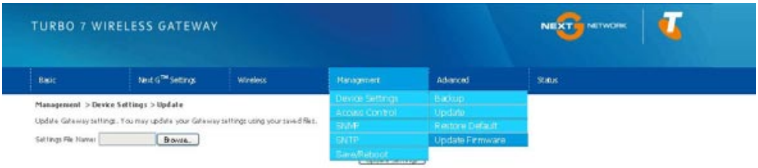
Close the Gateway Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

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.

6.1.4 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.



Management > Device Settings > Update

Update Gateway settings. You may update your Gateway settings using your saved files.

Settings File Name:

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.

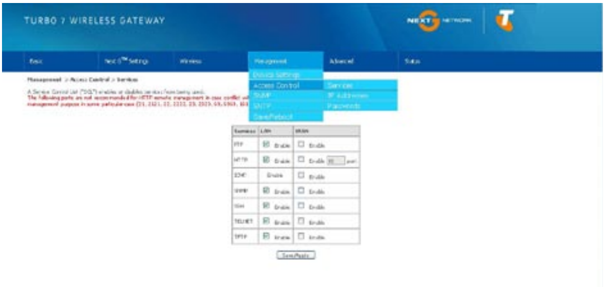
NOTE: The update process will take about 2 minutes to complete. The Gateway will reboot and the browser window will refresh to the default screen upon successful installation.
It is recommended that you compare the Software Version at the top of the Basic screen (WUI homepage) with the firmware version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

6.2 ACCESS CONTROL

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

- Services
- IP Addresses
- Passwords

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

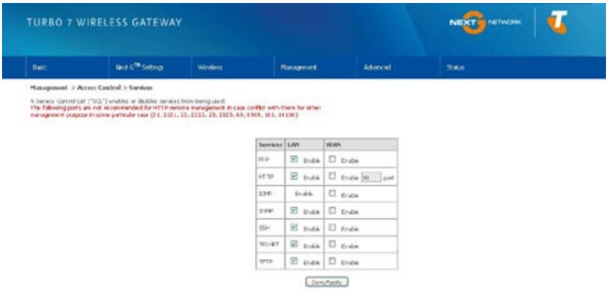


Management > Access Control > Services

Services	LAN	WAN
FTP	☑ Enable	☐ Enable
HTTP	☑ Enable	☐ Enable 80 port
ICMP	Enable	☐ Enable
SNMP	☑ Enable	☐ Enable
SSH	☑ Enable	☐ Enable
TELNET	☑ Enable	☐ Enable
TFTP	☑ Enable	☐ Enable

6.2.1 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.



Management > Access Control > Services

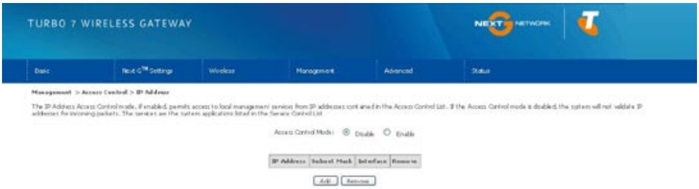
A Service Control List ("SCL") enables or disables services from being used.

The following ports are not recommended for HTTP remote management in case conflict with them for other management purpose in some particular case (21, 2121, 22, 2222, 23, 2323, 69, 6969, 161, 16116)

Services	LAN	WAN
FTP	☑ Enable	☐ Enable
HTTP	☑ Enable	☐ Enable 80 port
ICMP	Enable	☐ Enable
SNMP	☑ Enable	☐ Enable
SSH	☑ Enable	☐ Enable
TELNET	☑ Enable	☐ Enable
TFTP	☑ Enable	☐ Enable

6.2.2 IP Address

The IP Address option limits local access by IP address. When the Access Control Mode is enabled, only the IP addresses listed here can access the device. Before enabling Access Control Mode, add IP addresses with the Add button.



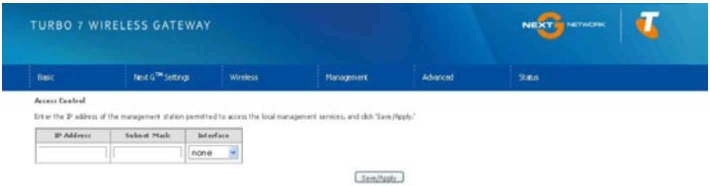
Management > Access Control > IP Address

The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List

Access Control Mode: ● Disable ○ Enable

IP Address	Subnet Mask	Interface	Remove

On this screen, enter the IP address Subnet Mask and the different interface for which you wish to allow permission. Click Save/Apply to continue.



Access Control

Enter the IP address of the management station permitted to access the local management services, and click 'Save/Apply.'

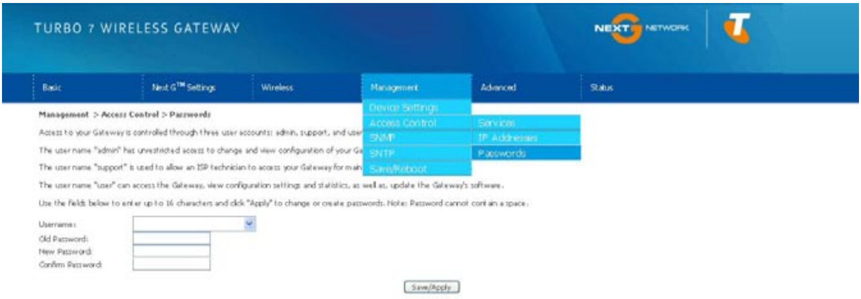
IP Address	Subnet Mask	Interface
		none

6.2.3 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.



Management > Access Control > Passwords

Access to your Gateway is controlled through three user accounts: admin, support, and user

The user name "admin" has unrestricted access to change and view configuration of your Ga

The user name "support" is used to allow an ISP technician to access your Gateway for main

The user name "user" can access the Gateway, view configuration settings and statistics, as well as, update the Gateway's software.

Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.

Username:
Old Password:
New Password:
Confirm Password:

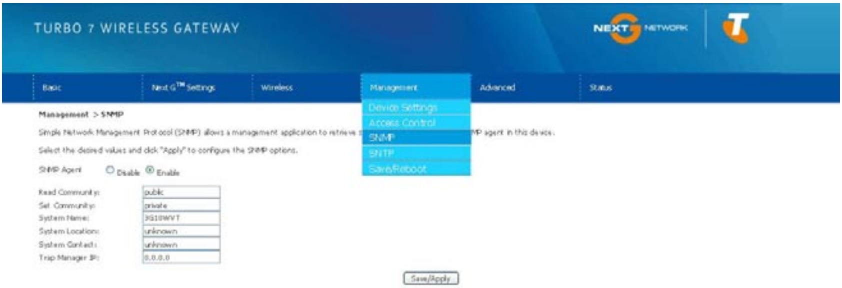
6.3 CONFIGURE SNMP AGENT ON THE 3G10WVT

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 3G10WVT (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.



Management > SNMP

Simple Network Management Protocol (SNMP) allows a management application to retrieve s MP agent in this device.

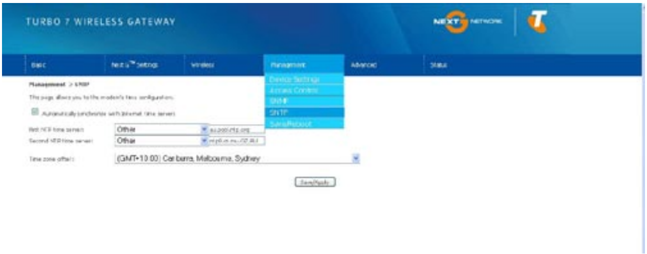
Select the desired values and click "Apply" to configure the SNMP options.

SNMP Agent ○ Disable ● Enable

Read Community:	public
Set Community:	private
System Name:	3G10WVT
System Location:	unknown
System Contact:	unknown
Trap Manager IP:	0.0.0.0

6.4 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.



Management > SNTP

This page allows you to the modem's time configuration.

□ Automatically synchronize with Internet time servers

First NTP time server: Other au.pool.ntp.org

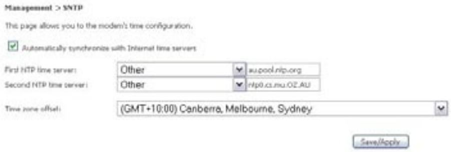
Second NTP time server: Other ntp0.cs.mu.OZ.AU

Time zone offset: (GMT+10:00) Canberra, Melbourne, Sydney

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

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.



Management > SNTP

This page allows you to the modem's time configuration.

☑ Automatically synchronize with Internet time servers

First NTP time server: Other au.pool.ntp.org

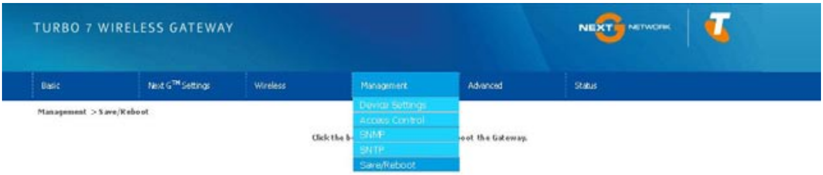
Second NTP time server: Other ntp0.cs.mu.OZ.AU

Time zone offset: (GMT+10:00) Canberra, Melbourne, Sydney

NOTE: SNTP must be activated to use Parental Control (section 7.3.2).

6.5 SAVE AND REBOOT

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



Management > Save/Reboot

Click the b… oot the Gateway.

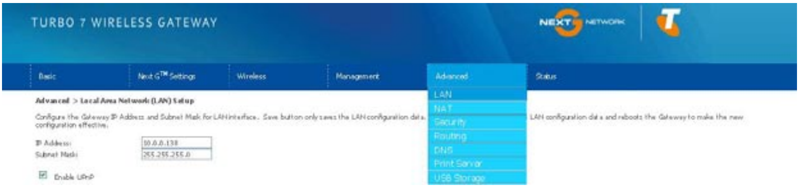
NOTE1: It may be necessary to reconfigure your TCP/IP settings to adjust for the new configuration. For example, if you disable the Dynamic Host Configuration Protocol (DHCP) server you will need to apply Static IP settings.

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.

ADVANCED SETUP

ADVANCED SETUP

This chapter explains advanced setup for your Gateway:



Advanced > Local Area Network (LAN) Setup

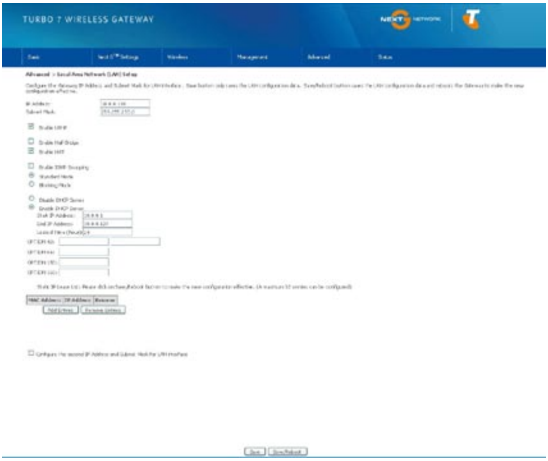
Configure the Gateway IP Address and Subnet Mask for LAN interface. Save button only saves the LAN configuration data. LAN configuration data and reboots the Gateway to make the new configuration effective.

IP Address: 10.0.0.138
Subnet Mask: 255.255.255.0

☑ Enable UPnP

7.1 LOCAL AREA NETWORK (LAN)

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



Advanced > Local Area Network (LAN) Setup

Configure the Gateway IP Address and Subnet Mask for LAN interface. Save button only saves the LAN configuration data. Save/Reboot button saves the LAN configuration data and reboots the Gateway to make the new configuration effective.

IP Address: 10.0.0.138
Subnet Mask: 255.255.255.0

☑ Enable UPnP

☐ Enable Half Bridge
☑ Enable NAT

☐ Enable IGMP Snooping
● Standard Mode
○ Blocking Mode

○ Disable DHCP Server
● Enable DHCP Server
Start IP Address: 10.0.0.1
End IP Address: 10.0.0.127
Leased Time (hour): 24
OPTION 42:
OPTION 44:
OPTION [illegible]:
OPTION [illegible]:

Static IP Lease List: Please click on Save/Reboot button to make the new configuration effective. (A maximum 32 entries can be configured)

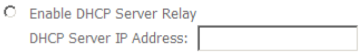
MAC Address	IP Address	Remove

☐ Configure the second IP Address and Subnet Mask for LAN interface

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 UPnP	Tick the box to enable Universal Plug and Play
Enable Half-Bridge	The Telstra Turbo 7 Wireless Gateway with Voice can be set up as a half-transparent bridge to cope with some special applications such as VPN pass-through. By default half-bridge is off. Please refer to Appendix B for more information.
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.
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
Enable NAT	To enable/disable Network Address Translation (NAT, please refer to 7.2 for NAT setting). By default NAT is enabled.
Option 42, 66,150,160	These options are used for special DHCP set up.
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:

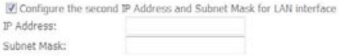


○ Enable DHCP Server Relay

DHCP Server IP Address:

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.



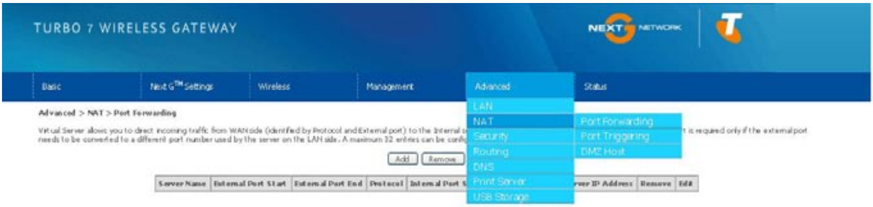
☑ Configure the second IP Address and Subnet Mask for LAN interface

IP Address:

Subnet Mask:

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)



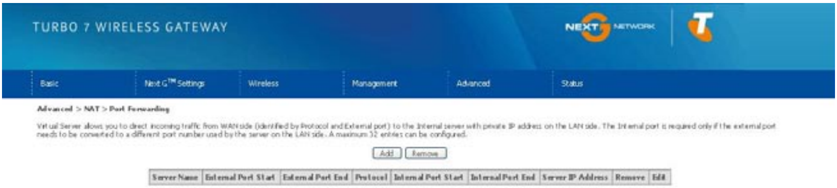
Advanced > NAT > Port Forwarding

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal s… t 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 confi…

Server Name	External Port Start	External Port End	Protocol	Internal Port S…	…ver IP Address	Remove	Edit

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.

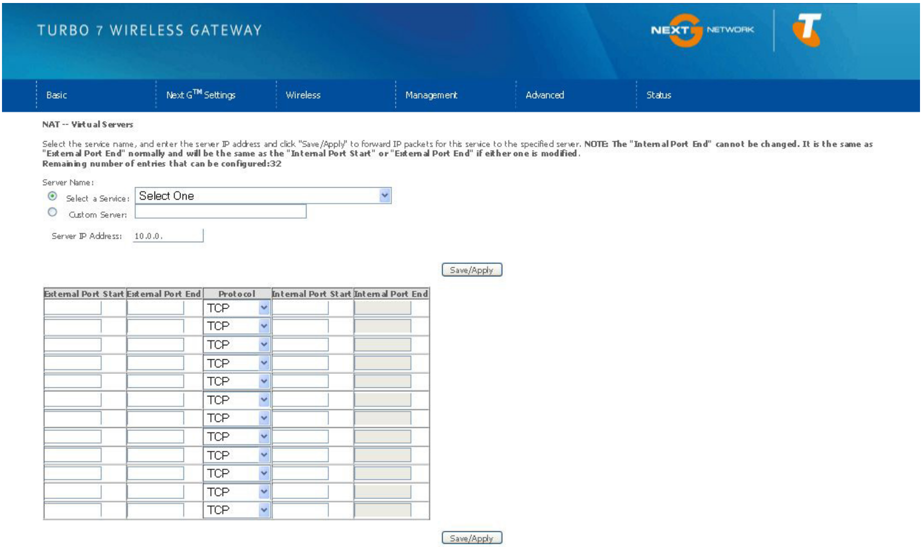


Advanced > NAT > Port Forwarding

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	Remove	Edit

To add a Virtual Server, click the Add button. The following screen will display.



NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Save/Apply" to forward IP packets for this service to the specified server. **NOTE: The "Internal Port End" cannot be changed. It is the same as "External Port End" normally and will be the same as the "Internal Port Start" or "External Port End" if either one is modified.**
Remaining number of entries that can be configured:32

Server Name:

● Select a Service: Select One

○ Custom Server:

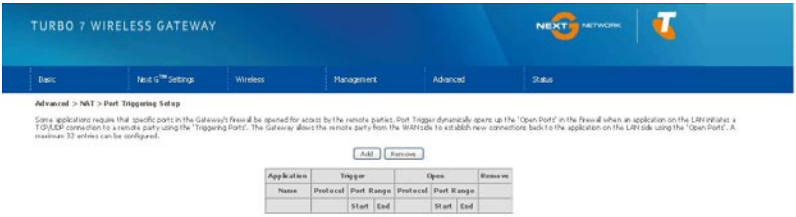
Server IP Address: 10.0.0.

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		

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.

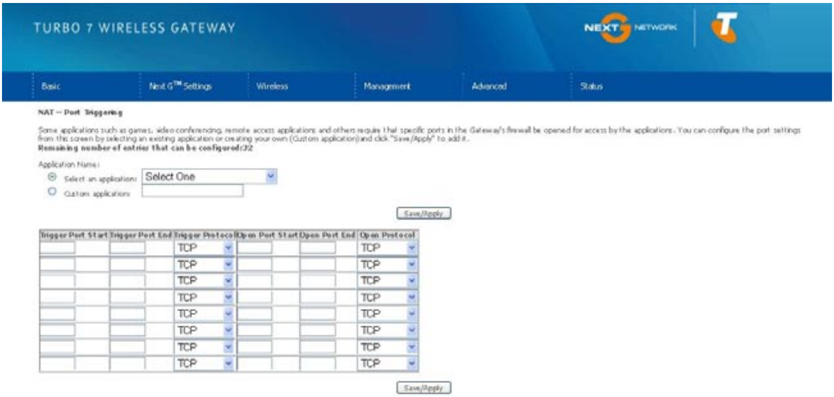


Advanced > NAT > Port Triggering Setup

Some applications require that specific ports in the Gateway'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 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.

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

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



NAT -- Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Gateway'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

Application Name:

● Select an application: Select One

○ Custom application:

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

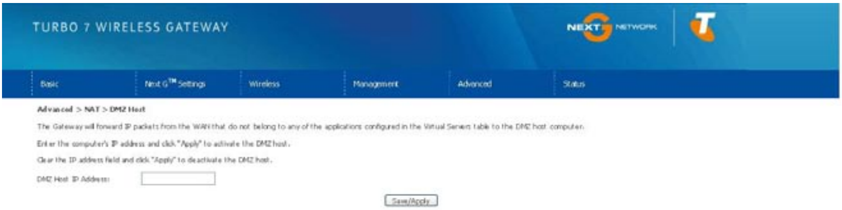
Options	Description
Select an Application **or** **Custom Application**	User should select the application from the list. or User can enter the name of their choice.
Trigger Port Start	Enter the starting trigger port number (when you select custom application). When an application is selected, the port 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.



Advanced > NAT > DMZ Host

The Gateway 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.

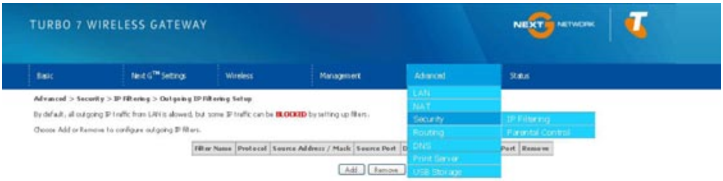
Enter the computer's IP address and click "Apply" to activate the DMZ host.

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

DMZ Host IP Address:

7.3 SECURITY

Your Gateway can be secured with **IP Filtering** or **Parental Control** functions.



Advanced > Security > IP Filtering > Outgoing IP Filtering Setup

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be BLOCKED by setting up filters.

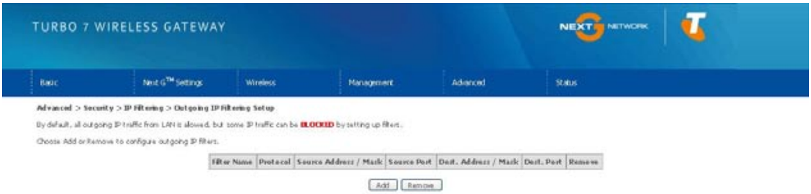
Choose Add or Remove to configure outgoing IP filters.

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**.



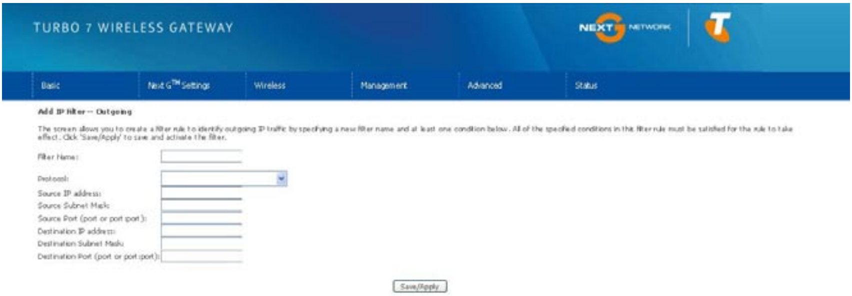
Advanced > Security > IP Filtering > Outgoing IP Filtering Setup

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be BLOCKED by setting up filters.

Choose Add or Remove to configure outgoing IP filters.

Filter Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove

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



Add IP Filter -- Outgoing

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

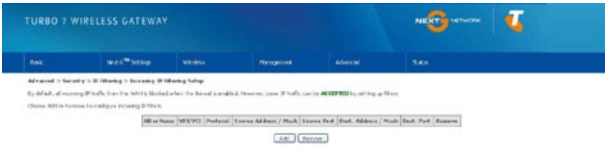
Destination Port (port or port:port):

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**.



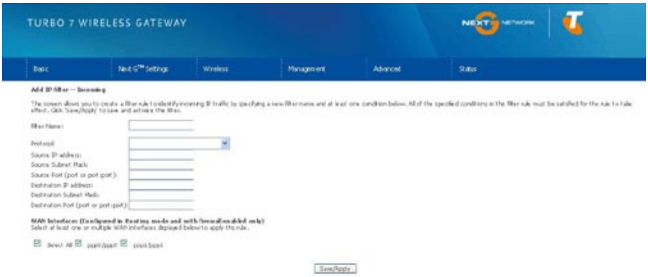
Advanced > Security > IP Filtering > Incoming IP Filtering Setup

By default, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	VPI/VCI	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove

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



Add IP Filter -- Incoming

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in the filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

WAN Interfaces (Configured in Routing mode and with firewall enabled only)

Select at least one or multiple WAN interfaces displayed below to apply this rule.

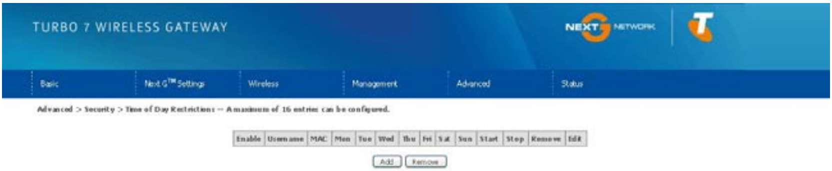
☑ Select All ☑ ppp0/ppp0 ☑ ppp1/ppp1

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

Click **Save/Apply** to save and activate the filter.

7.3.2 Parental Control

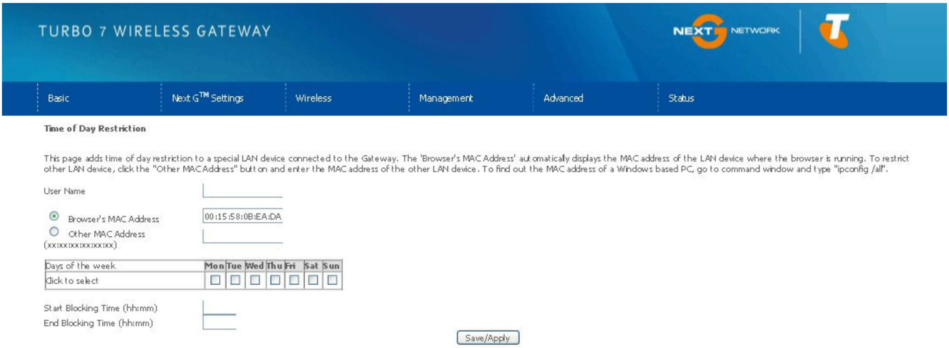
Parental Control allows you to restrict access from a device on your Local Area Network (LAN) to the Internet through the Gateway on selected days at certain times. Make sure to activate the Internet Time server synchronization as described in section 6.4 SNTP, so that the scheduled times match your local time.



Advanced > Security > Time of Day Restrictions -- A maximum of 16 entries can be configured.

Enable	Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove	Edit

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.



Time of Day Restriction

This page adds time of day restriction to a special LAN device connected to the Gateway. The 'Browser's MAC Address' automaticaly 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 00:15:58:0B:EA:DA

○ Other MAC Address (xx:xx:xx:xx:xx:xx)

Days of the week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select	□	□	□	□	□	□	□

Start Blocking Time (hh:mm)

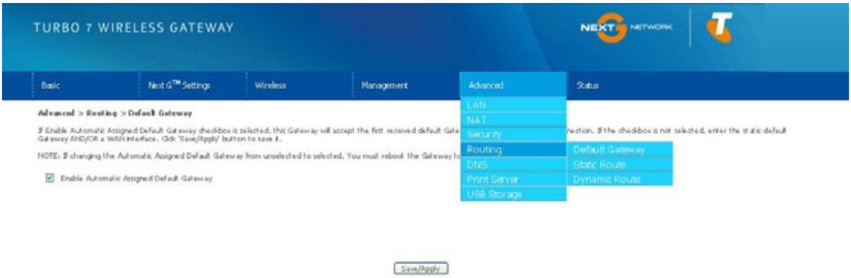
End Blocking Time (hh:mm)

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 more 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

7.4 ROUTING

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



Advanced > Routing > Default Gateway

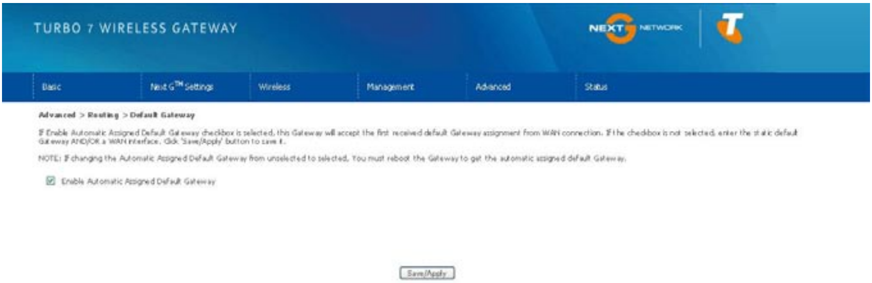
If Enable Automatic Assigned Default Gateway checkbox is selected, this Gateway will accept the first received default Gate… …nection. If the checkbox is not selected, enter the static default Gateway AND/OR a WAN interface. Click 'Save/Apply' button to save it.

NOTE: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the Gateway to…

☑ Enable Automatic Assigned Default Gateway

7.4.1 Default Gateway

If the **Enable Automatic Assigned Default Gateway** checkbox is selected, this device will accept a default Gateway assignment. If the checkbox is not selected, a field will appear allowing you to enter the static default gateway and/or WAN interface, then click **Save/Apply**.



Advanced > Routing > Default Gateway

If Enable Automatic Assigned Default Gateway checkbox is selected, this Gateway will accept the first received default Gateway assignment from WAN connection. If the checkbox is not selected, enter the static default Gateway AND/OR a WAN interface. Click 'Save/Apply' button to save it.

NOTE: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the Gateway to get the automatic assigned default Gateway.

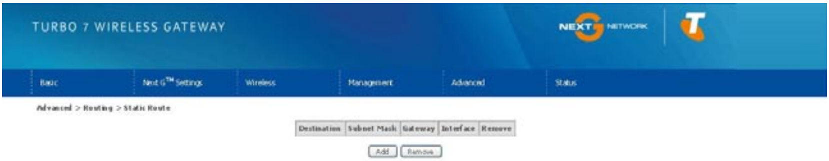
☑ Enable Automatic Assigned Default Gateway

NOTE: After enabling the Automatic Assigned Default Gateway, you must re-boot the Gateway to activate the assigned default Gateway.

7.4.2 Static Route

The Static Route screen displays the configured static routes.

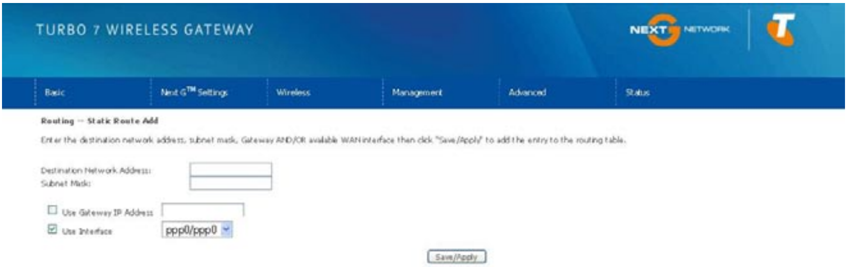
Click the Add or Remove buttons to change settings.



Advanced > Routing > Static Route

Destination	Subnet Mask	Gateway	Interface	Remove

Click the Add button to display the following screen.



Routing -- Static Route Add

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

Destination Network Address:

Subnet Mask:

□ Use Gateway IP Address

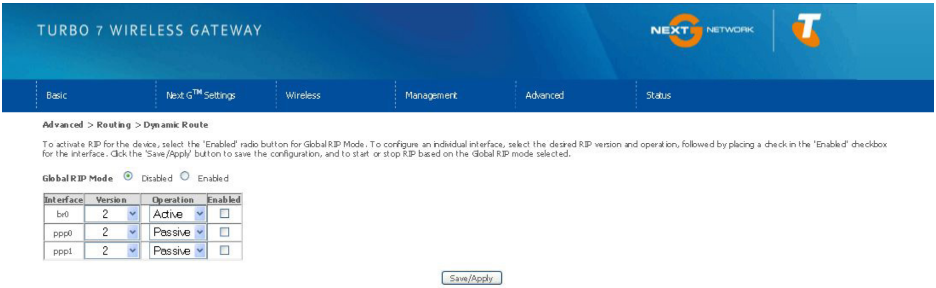
☑ Use Interface ppp0/ppp0

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.

7.4.3 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.



Advanced > Routing > Dynamic Route

To activate RIP for the device, 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 the interface. Click the 'Save/Apply' button to save the configuration, and to start or stop RIP based on the Global RIP mode selected.

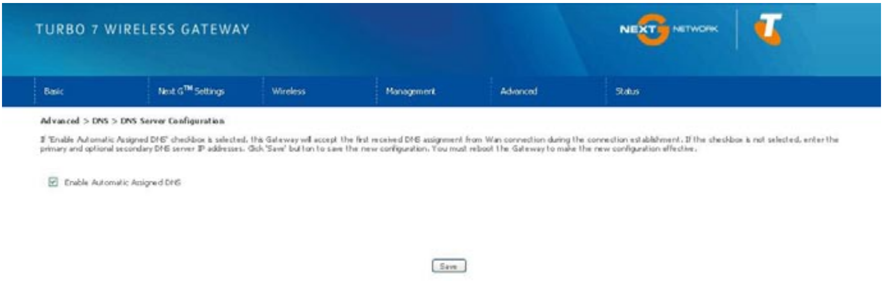
Global RIP Mode ● Disabled ○ Enabled

Interface	Version	Operation	Enabled
br0	2	Active	□
ppp0	2	Passive	□
ppp1	2	Passive	□

7.5 DOMAIN NAME SERVERS (DNS)

7.5.1 DNS Server Configuration

If the Enable Automatic Assigned DNS checkbox is selected, this device will accept the first received DNS assignment from the Wide Area Network (WAN) interface during the connection process. If the checkbox is not selected, a field will appear allowing you to enter the primary and optional secondary DNS server IP addresses. Click on **Save** to apply.



Advanced > DNS > DNS Server Configuration

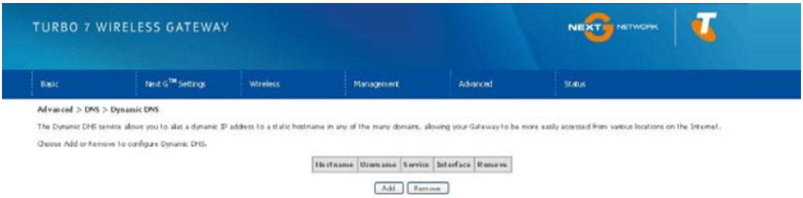
If 'Enable Automatic Assigned DNS' checkbox is selected, this Gateway will accept the first received DNS assignment from Wan connection during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click 'Save' button to save the new configuration. You must reboot the Gateway to make the new configuration effective.

☑ Enable Automatic Assigned DNS

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

7.5.2 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.



Advanced > DNS > Dynamic DNS

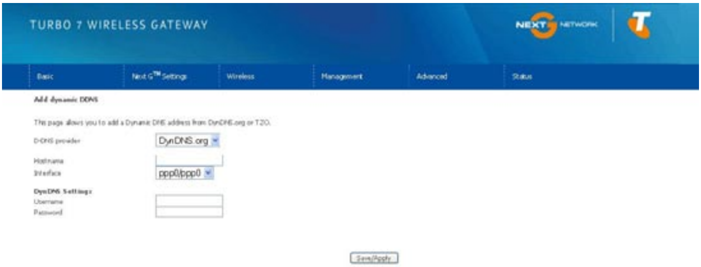
The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your Gateway to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove

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.



Add dynamic DDNS

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

D-DNS provider DynDNS.org

Hostname

Interface ppp0/ppp0

DynDNS Settings

Username

Password

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.

VOICE

VOICE

The Turbo 7 Wireless Gateway with Voice allows you to make telephone calls over the Next G™ network using a standard Analogue Telephone via the built in RJ-11 Phone port.

Please refer to the documentation provided by the manufacturer of your Analogue Telephone for help with the operation of your telephone.

8.1 CONFIGURING YOUR TURBO 7 WIRELESS GATEWAY FOR PLACING VOICE CALLS

Once your Gateway has been correctly configured to access the Next G™ network as outlined in Section 2.1 – Quick Setup, you can make and receive telephone calls after connecting your Analogue Telephone to the socket labeled Phone on the back of your Turbo 7 Wireless Gateway with Voice.

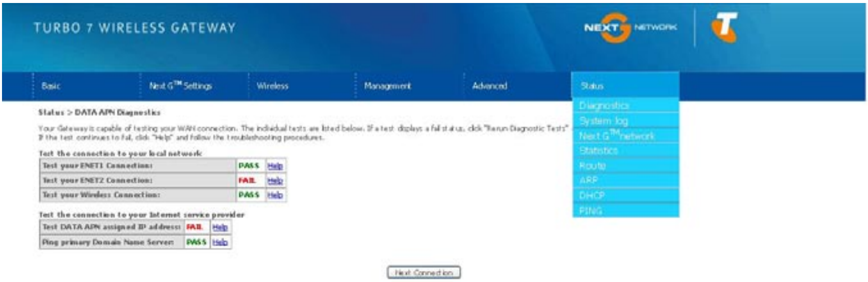
For voice calls over the Next G™ network, note that your SIM card needs to be provisioned for Voice Calling. Please consult with Telstra for verification. Also please note that any telephone calls placed using the Gateway will incur call usage charges at mobile call rates. Please contact Telstra for more information.

STATUS

STATUS

THE STATUS MENU HAS THE FOLLOWING SUBMENUS:

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



Status > DATA APN Diagnostics

Your Gateway is capable of testing your WAN connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network

Test your ENET1 Connection:	PASS	Help
Test your ENET2 Connection:	FAIL	Help
Test your Wireless Connection:	PASS	Help

Test the connection to your Internet service provider

Test DATA APN assigned IP address:	FAIL	Help
Ping primary Domain Name Server:	PASS	Help

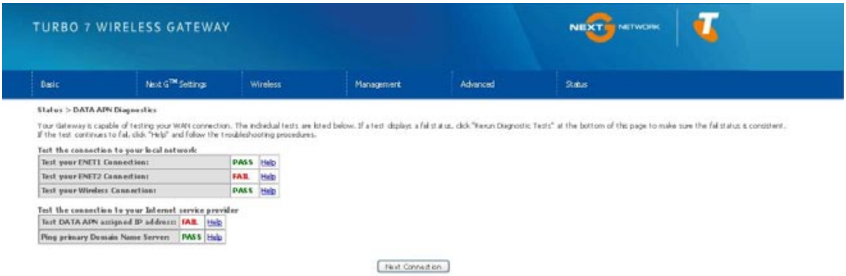
9.1 DIAGNOSTICS

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.



Status > DATA APN Diagnostics

Your Gateway is capable of testing your WAN connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of the 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 ENET1 Connection:	PASS	Help
Test your ENET2 Connection:	FAIL	Help
Test your Wireless Connection:	PASS	Help

Test the connection to your Internet service provider

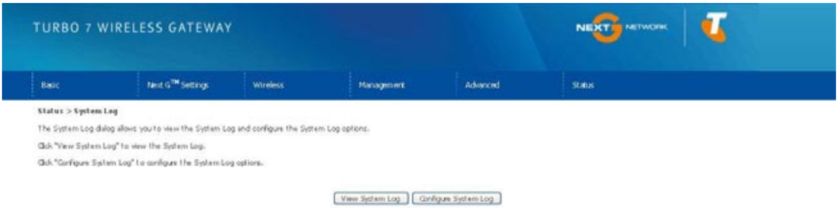
Test DATA APN assigned IP address:	FAIL	Help
Ping primary Domain Name Server:	PASS	Help

Test	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.

9.2 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.



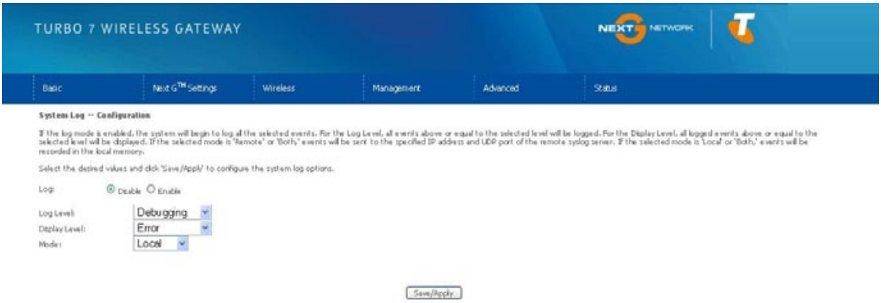
Status > System Log

The System Log dialog allows you to view the System Log and configure the System Log options.

Click "View System Log" to view the System Log.

Click "Configure System Log" to configure the System Log options.

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



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 'Save/Apply' to configure the system log options.

Log: ● Disable ○ Enable

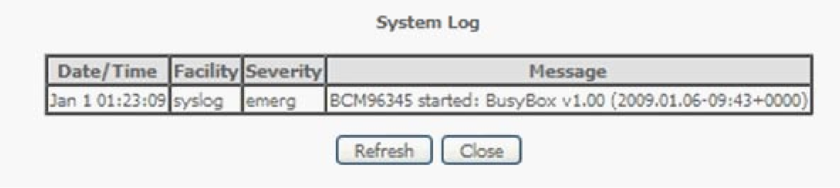
Log Level: Debugging

Display Level: Error

Mode: Local

Option	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.

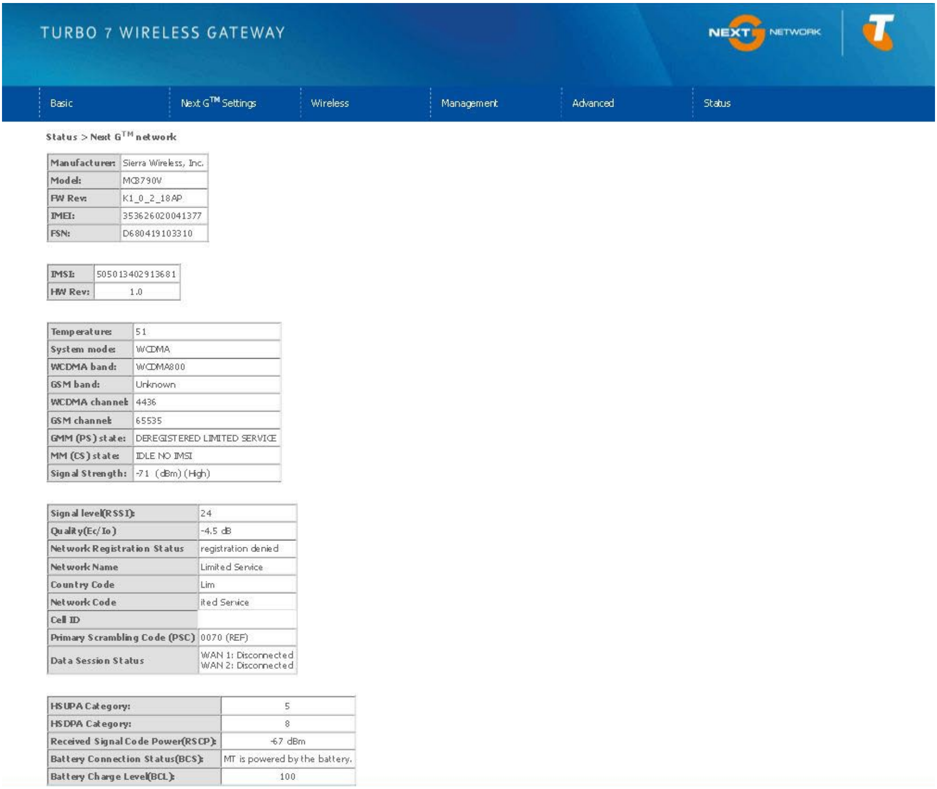


System Log

Date/Time	Facility	Severity	Message
Jan 1 01:23:09	syslog	emerg	BCM96345 started: BusyBox v1.00 (2009.01.06-09:43+0000)

9.3 NEXT G^{TM} STATUS

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



Status > Next G^{TM} network

Manufacturer:	Sierra Wireless, Inc.
Model:	MC8790V
FW Rev:	K1_0_2_18AP
IMEI:	353626020041377
FSN:	D680419103310

IMSI:	505013402913681
HW Rev:	1.0

Temperature:	51
System mode:	WCDMA
WCDMA band:	WCDMA800
GSM band:	Unknown
WCDMA channel:	4436
GSM channel:	65535
GMM (PS) state:	DEREGISTERED LIMITED SERVICE
MM (CS) state:	IDLE NO IMSI
Signal Strength:	-71 (dBm) (High)

Signal level(RSSI):	24
Quality(Ec/Io)	-4.5 dB
Network Registration Status	registration denied
Network Name	Limited Service
Country Code	Lim
Network Code	ited Service
Cell ID	
Primary Scrambling Code (PSC)	0070 (REF)
Data Session Status	WAN 1: Disconnected WAN 2: Disconnected

HSUPA Category:	5
HSDPA Category:	8
Received Signal Code Power(RSCP):	-67 dBm
Battery Connection Status(BCS):	MT is powered by the battery.
Battery Charge Level(BCL):	100

Consult the table on the next page for detailed field descriptions.

Status	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 GSM or 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 CDMA 2000 / America
WCDMA band	The 3G radio frequency band which supports tri-band UTMS/HSDPA/HSUPA frequencies (850/1900/2100 MHz), IMT2000 is 2100 MHz, WCDMA800 is 850 MHz, WCDMA1900 is 1900 MHz.
GSM band	The 2G radio frequency band which supports Quad-band GSM/GRPS frequencies, including GSM850, GSM900, DCS1800, PCS1900 with each number representing the respective frequency in MHz.
WCDMA channel	The 3G channel.
GSM channel	The 2G channel.
GSM (PS) state	Packet Switching state
MM (CS) state	Circuit Switching state
Signal Strength	The 3G/2G service signal strength in dBm.

Signal level in dBm	**-109 ~ -103**	**-101 ~ -93**	**-91 ~ -87**	**-85 ~ -79**	**-77 ~ -52**
5 Signal bars	▨				
	▨	▨			
	▨	▨	▨		
	▨	▨	▨	▨	
	▨	▨	▨	▨	▨
LED	**Low**		**Medium**		**High**

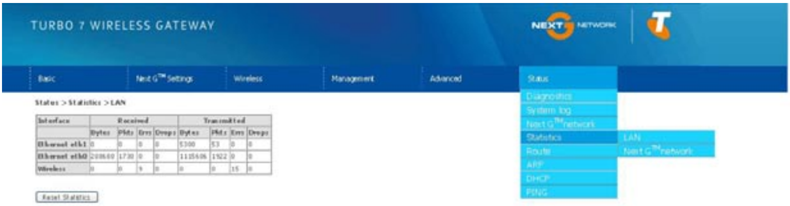
<table>
<tr><th>Status</th><th>Description</th></tr>
<tr><td><b>Signal Level (RSSI)</b></td><td>3G Radio Signal Strength Index
<table>
<tr><td><b>Value</b></td><td><b>2 ~ 5</b></td><td><b>6 ~ 10</b></td><td><b>11 ~ 13</b></td><td><b>14 ~ 17</b></td><td><b>18 ~ 31</b></td><td><b>99</b></td></tr>
<tr><td><b>Signal level in dBm</b></td><td><b>-109 ~ -103</b></td><td><b>-101 ~ -93</b></td><td><b>-91 ~ -87</b></td><td><b>-85 ~ -79</b></td><td><b>-77 ~ -52</b></td><td><b>unknown</b></td></tr>
<tr><td rowspan="5"><b>5 Signal bars</b></td><td>▨</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>▨</td><td>▨</td><td></td><td></td><td></td><td></td></tr>
<tr><td>▨</td><td>▨</td><td>▨</td><td></td><td></td><td></td></tr>
<tr><td>▨</td><td>▨</td><td>▨</td><td>▨</td><td></td><td></td></tr>
<tr><td>▨</td><td>▨</td><td>▨</td><td>▨</td><td>▨</td><td></td></tr>
<tr><td><b>LED</b></td><td colspan="2"><b>Low</b></td><td colspan="2"><b>Medium</b></td><td><b>High</b></td><td></td></tr>
</table>
</td></tr>
<tr><td><b>Quality (Ec/Io)</b></td><td>The total energy per chip per power density (Ec/Io) value of the active set's three strongest cells.</td></tr>
<tr><td><b>Network Registration Status</b></td><td>Should display as registered with a valid unlocked SIM card.</td></tr>
<tr><td><b>Network Name</b></td><td>The 3G internet Service Provider.</td></tr>
<tr><td><b>Country & Network Codes</b></td><td>Each country and network has a unique code.</td></tr>
<tr><td><b>Cell ID</b></td><td>The network information for the "serving" cell ID.</td></tr>
<tr><td><b>Primary Scrambling Code (PSC)</b></td><td>The PSC of the reference WCDMA cell</td></tr>
<tr><td><b>Data Session Status</b></td><td>Connected or Disconnected</td></tr>
<tr><td><b>HSUPA/HSDPA Categories</b></td><td>The HSUPA/HSDPA categories correspond to different data transmission rates with higher numbers generally indicating faster rates</td></tr>
<tr><td><b>Received Signal Code Power (RSCP)</b></td><td>The RSCP of the active set's three strongest cells</td></tr>
<tr><td><b>Battery Connection Status (BCS)</b></td><td>BCS of the MT (Mobile Termination)</td></tr>
<tr><td><b>Battery Charge Level (BCL)</b></td><td>BCL of the MT (Mobile Termination)</td></tr>
</table>

9.4 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.

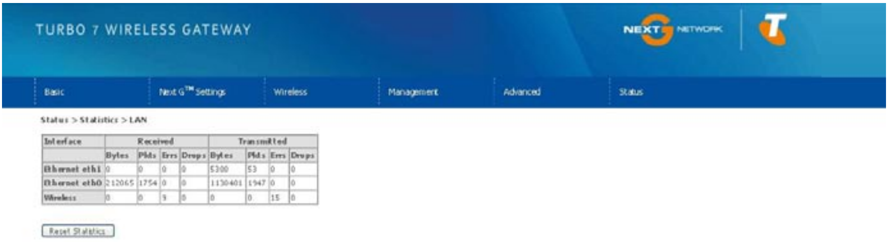


Status > Statistics > LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Ethernet eth1	0	0	0	0	5300	53	0	0
Ethernet eth0	208660	1730	0	0	1115606	1922	0	0
Wireless	0	0	9	0	0	0	15	0

9.4.1 LAN Statistics

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



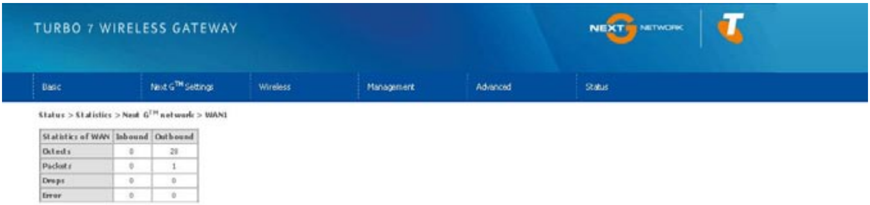
Status > Statistics > LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Ethernet eth1	0	0	0	0	5300	53	0	0
Ethernet eth0	212065	1754	0	0	1130401	1947	0	0
Wireless	0	0	9	0	0	0	15	0

Received/Transmitted	Bytes	Rx/TX (receive/transmit) packet in bytes
	Pkts	Rx/TX (receive/transmit) packets
	Errs	Rx/TX (receive/transmit) packets with errors
	Drops	Rx/TX (receive/transmit) packets dropped

9.4.2 Next G™ Statistics

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



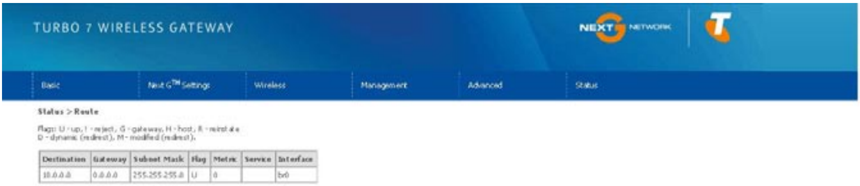
Status > Statistics > Next G™ network > WAN1

Statistics of WAN	Inbound	Outbound
Octets	0	28
Packets	0	1
Drops	0	0
Error	0	0

Service	Shows the service type	
Inbound	Octets	Number of received octets over the interface.
	Packets	Number of received packets over the interface.
	Drops	Received packets which are dropped.
	Error	Received packets which are errors.
Outbound	Octets	Number of Transmitted octets over the interface.
	Packets	Number of Transmitted packets over the interface.
	Drops	Transmitted packets which are dropped
	Error	Transmitted packets which are errors.

9.5 ROUTE

Select Route to display the paths the Gateway has found.



Status > Route

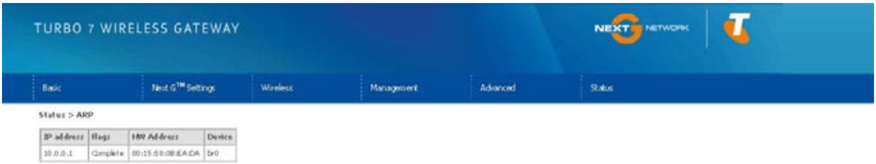
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
10.0.0.0	0.0.0.0	255.255.255.0	U	0		br0

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

9.6 ARP

Click ARP to display the ARP information.



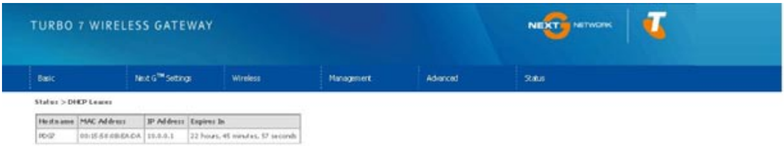
Status > ARP

IP address	Flags	HW Address	Device
10.0.0.1	Complete	00:15:58:0B:EA:DA	br0

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

9.7 DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

Click DHCP to display the DHCP information.



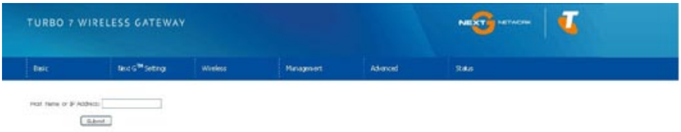
Status > DHCP Leases

Hostname	MAC Address	IP Address	Expires In
PC-07	00:15:58:0B:EA:DA	10.0.0.1	22 hours, 45 minutes, 57 seconds

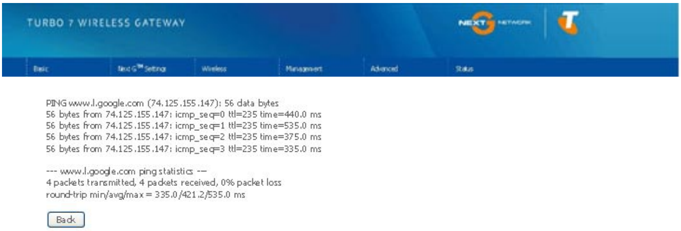
Field	Description
Hostname	Shows the device/host/PC network name
MAC Address	Shows the Ethernet MAC address of the device/host/PC
IP address	Shows IP address of device/host/PC
Expires In	Shows how much time is left for each DHCP Lease

9.8 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.



```
PING www.l.google.com (74.125.155.147): 56 data bytes
56 bytes from 74.125.155.147: icmp_seq=0 ttl=235 time=440.0 ms
56 bytes from 74.125.155.147: icmp_seq=1 ttl=235 time=535.0 ms
56 bytes from 74.125.155.147: icmp_seq=2 ttl=235 time=375.0 ms
56 bytes from 74.125.155.147: icmp_seq=3 ttl=235 time=335.0 ms

--- www.l.google.com ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 335.0/421.2/535.0 ms
```

The above screen is not showing successful ping result

APPENDICIES

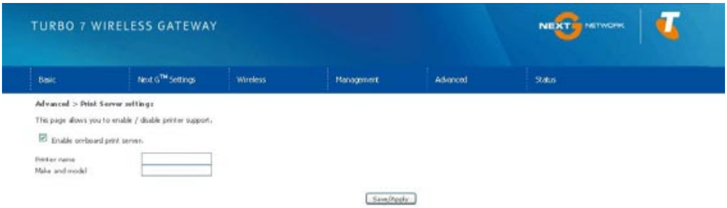
APPENDIX A: PRINT SERVER

These steps explain the procedure for enabling the Print Server.

1: Enable Print Server from the Advanced menu in the Web User Interface.

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.



Advanced > Print Server settings

This page allows you to enable / disable printer support.

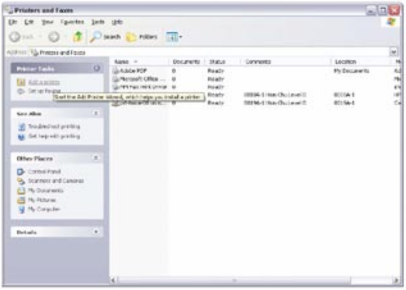
☑ Enable on-board print server.

Printer name

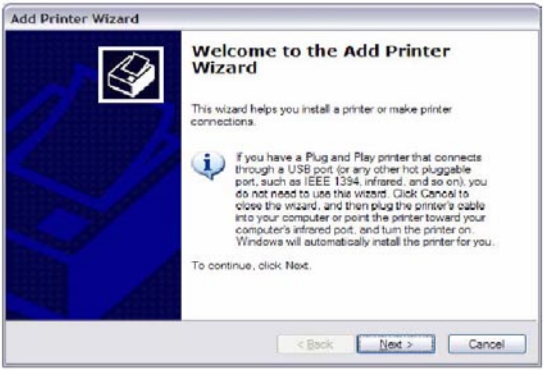
Make and model

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.


Add Printer Wizard

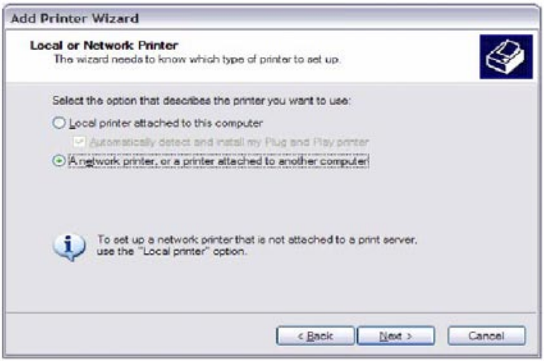
Welcome to the Add Printer Wizard

This wizard helps you install a printer or make printer connections.

If you have a Plug and Play printer that connects through a USB port (or any other hot pluggable port, such as IEEE 1394, infrared, and so on), you do not need to use this wizard. Click Cancel to close the wizard, and then plug the printer's cable into your computer or point the printer toward your computer's infrared port, and turn the printer on. Windows will automatically install the printer for you.

To continue, click Next.

4: Select Network Printer and click **Next**.


Add Printer Wizard

Local or Network Printer

The wizard needs to know which type of printer to set up.

Select the option that describes the printer you want to use:

○ Local printer attached to this computer

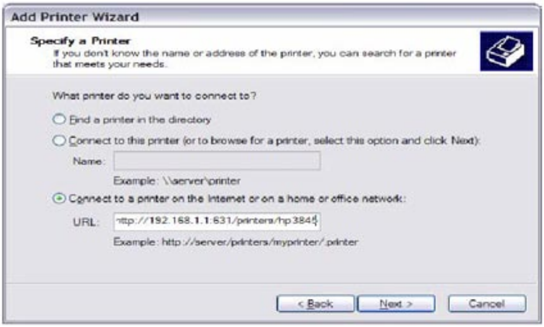
☑ Automatically detect and install my Plug and Play printer

● A network printer, or a printer attached to another computer

To set up a network printer that is not attached to a print server, use the "Local printer" option.

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.



Add Printer Wizard

Specify a Printer

If you don't know the name or address of the printer, you can search for a printer that meets your needs.

What printer do you want to connect to?

○ Find a printer in the directory

○ Connect to this printer (or to browse for a printer, select this option and click Next):

Name:

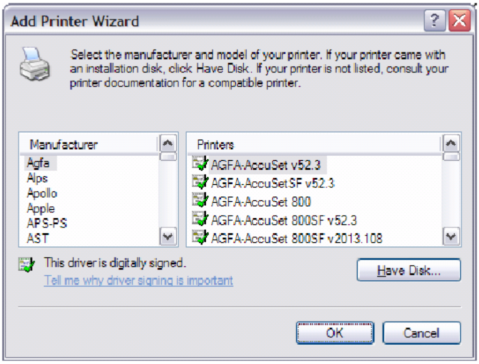
Example: \\server\printer

● Connect to a printer on the Internet or on a home or office network:

URL: http://192.168.1.1:631/printers/hp3845

Example: http://server/printers/myprinter/.printer

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



Add Printer Wizard

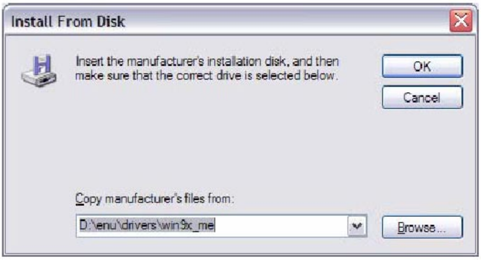
Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for a compatible printer.

Manufacturer	Printers
Agfa	AGFA-AccuSet v52.3
Alps	AGFA-AccuSet SF v52.3
Apollo	AGFA-AccuSet 800
Apple	AGFA-AccuSet 800SF v52.3
APS-PS	AGFA-AccuSet 800SF v2013.108
AST	

This driver is digitally signed.

Tell me why driver signing is important

7: Select driver file directory on CD-ROM and click **OK**.

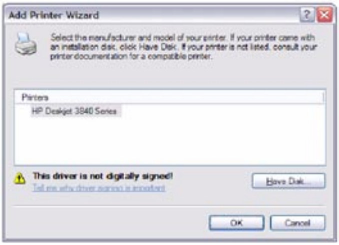


Insert the manufacturer's installation disk, and then make sure that the correct drive is selected below.

Copy manufacturer's files from:

D:\enu\drivers\win9x_me

8: Once the printer name appears, click **OK**.



Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for a compatible printer.

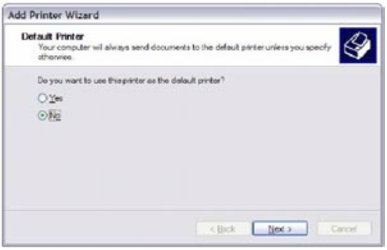
Printers

HP Deskjet 3840 Series

This driver is not digitally signed!

Tell me why driver signing is important

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



Default Printer

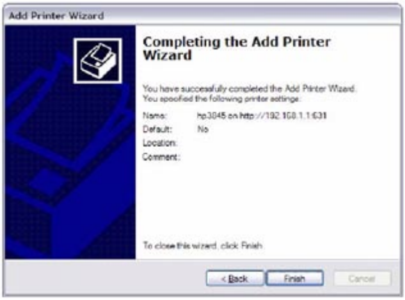
Your computer will always send documents to the default printer unless you specify otherwise.

Do you want to use this printer as the default printer?

○ Yes

● No

10: Click “**Finish**”.



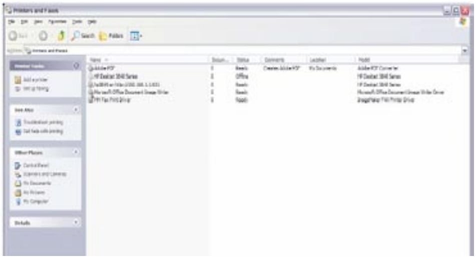
Completing the Add Printer Wizard

You have successfully completed the Add Printer Wizard.
You specified the following printer settings:

Name: hp3845 on http://192.168.1.1:631
Default: No
Location:
Comment:

To close this wizard, click Finish.

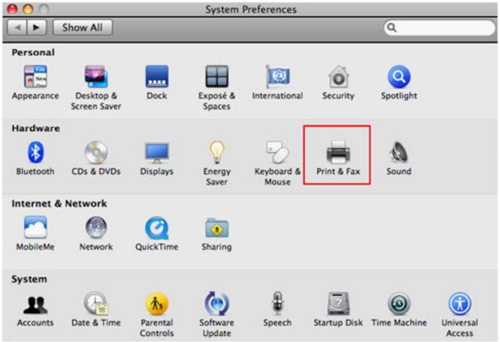
11: Check the status of printer from Windows Control Panel, printer window. Status should show as Ready.



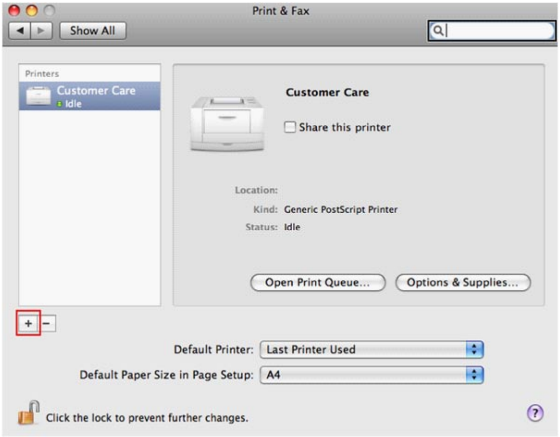
Name	Docum...	Status	Comments	Location	Model
Adobe PDF	0	Ready	Creates Adobe PDF	My Documents	Adobe PDF Converter
HP Deskjet 3840 Series	0	Offline			HP Deskjet 3840 Series
hp3845 on http://192.168.1.1:631	0	Ready			HP Deskjet 3840 Series
Microsoft Office Document Image Writer	0	Ready			Microsoft Office Document Image Writer Driver
[illegible]	0	Ready			[illegible]

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.



Customer Care

□ Share this printer

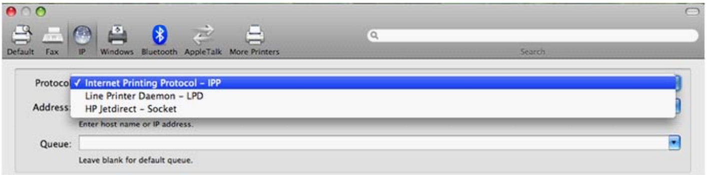
Location:
Kind: Generic PostScript Printer
Status: Idle

Default Printer: Last Printer Used

Default Paper Size in Page Setup: A4

Click the lock to prevent further changes.

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



Protocol: Internet Printing Protocol – IPP

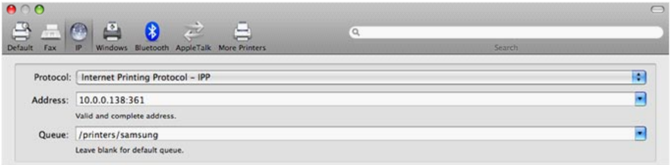
Address:

Enter host name or IP address.

Queue:

Leave blank for default queue.

6. Type into the Address field “GatewayIPAddress:361” 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 the initial step above.



Protocol: Internet Printing Protocol – IPP

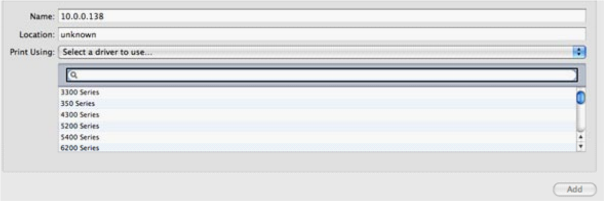
Address: 10.0.0.138:361

Valid and complete address.

Queue: /printers/samsung

Leave blank for default queue.

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

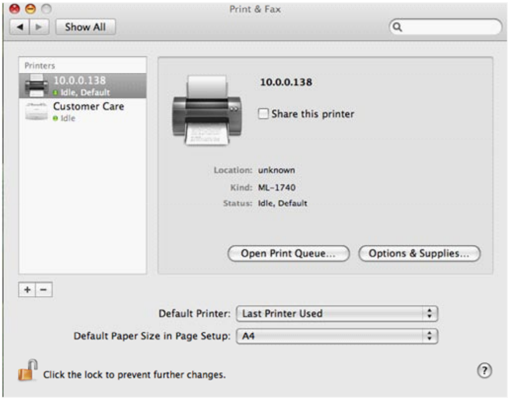


Name: 10.0.0.138

Location: unknown

Print Using: Select a driver to use...

8. Click Add and check the printer status.



10.0.0.138

☐ Share this printer

Location: unknown

Kind: ML-1740

Status: Idle, Default

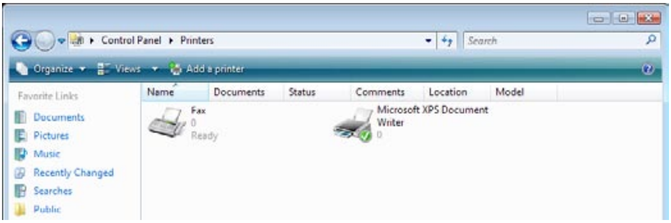
Default Printer: Last Printer Used

Default Paper Size in Page Setup: A4

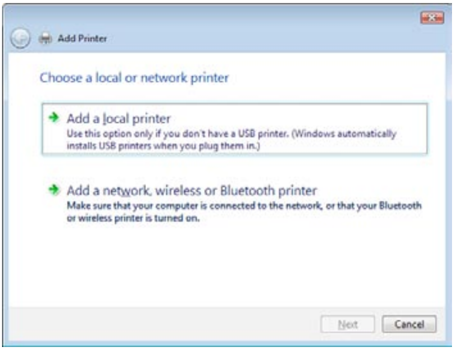
Print Server set up is now complete. You will now be able to print from common applications by selecting this printer from the Print dialogue box.

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.



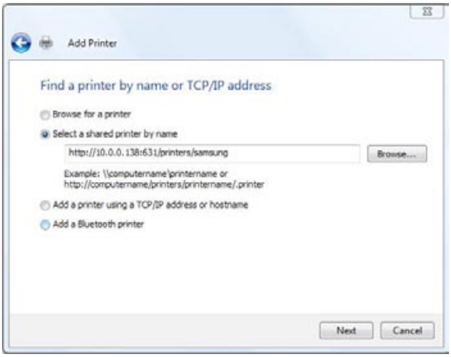
Choose a local or network printer

Add a local printer
Use this option only if you don't have a USB printer. (Windows automatically installs USB printers when you plug them in.)

Add a network, wireless or Bluetooth printer
Make sure that your computer is connected to the network, or that your Bluetooth or wireless printer is turned on.

4. Click on the radio-button labelled 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 above.



Find a printer by name or TCP/IP address

○ Browse for a printer

● Select a shared printer by name

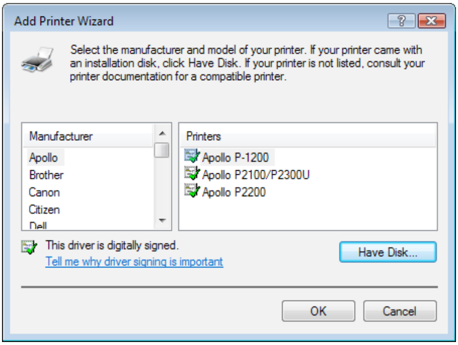
http://10.0.0.138:631/printers/samsung

Example: \\computername\printername or
http://computername/printers/printername/.printer

○ Add a printer using a TCP/IP address or hostname

○ Add a Bluetooth printer

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.

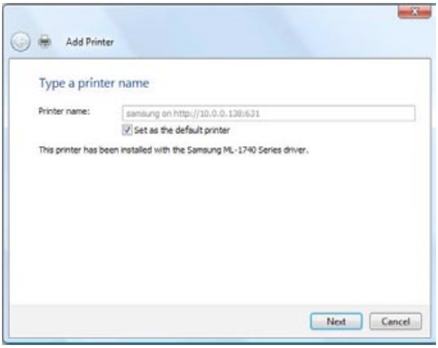


Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for a compatible printer.

Manufacturer	Printers
Apollo	Apollo P-1200
Brother	Apollo P2100/P2300U
Canon	Apollo P2200
Citizen	
Dell	

This driver is digitally signed.
Tell me why driver signing is important

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



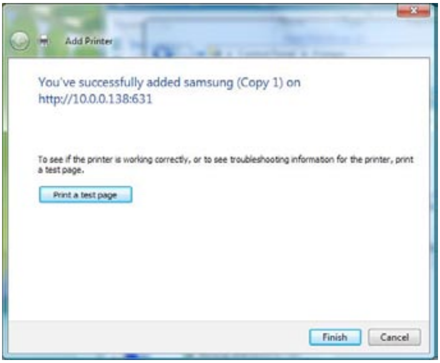
Type a printer name

Printer name: samsung on http://10.0.0.138:631

☑ Set as the default printer

This printer has been installed with the Samsung ML-1740 Series driver.

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



You've successfully added samsung (Copy 1) on http://10.0.0.138:631

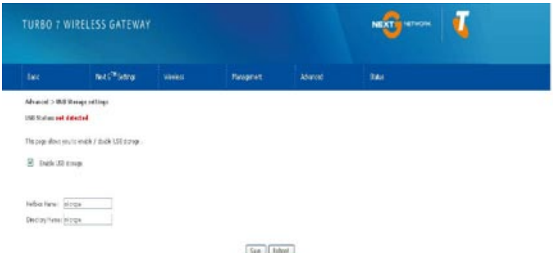
To see if the printer is working correctly, or to see troubleshooting information for the printer, print a test page.

APPENDIX B: USB STORAGE

These steps explain the procedure for enabling the USB Storage.

1: Enable Samba Server from Web User Interface.

Select Enable Samba checkbox and enter Netbios name and Directory Name

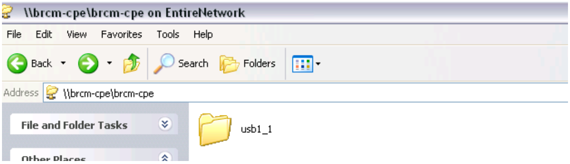


Field	Description
Netbios Name	It is the hostname of the PC
	The default name is “ntc-cpe”
Directory Name	The folder name of “root” directory.
	The default name is “ntc-cpe”

FOR WINDOWS XP:

2: Open a web-browser (such as Internet Explorer, Firefox or Safari) and type in the address. \\”NetbiosName”\”DirectoryName”\(eg. \\ntc-cpe\ntc-cpe)

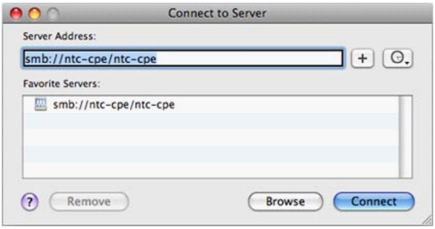
Note: There is no username and password required to access the USB drive, the user will be able to read/write the folder/files in the USB drive.



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:// "NetbiosName"/"DirectoryName" (eg smb://ntc-cpe/ntc-cpe)

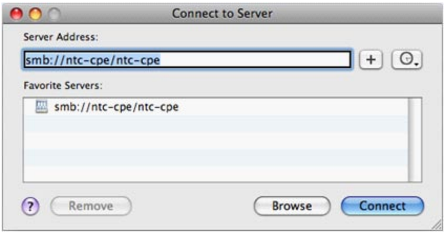


Connect to Server

Server Address: smb://ntc-cpe/ntc-cpe

Favorite Servers: smb://ntc-cpe/ntc-cpe

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

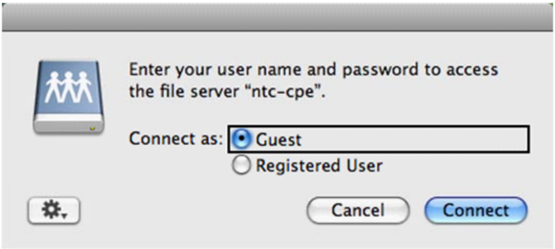


Connect to Server

Server Address: smb://ntc-cpe/ntc-cpe

Favorite Servers: smb://ntc-cpe/ntc-cpe

5. Select the Guest radio button and then click Connect

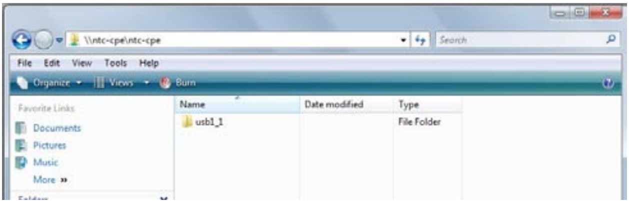


Enter your user name and password to access the file server "ntc-cpe".

Connect as: ● Guest
○ Registered User

FOR WINDOWS VISTA

1. Open a web-browser (such as Internet Explorer, Firefox or Safari)
2. Type in the address "\\NetbiosName\DirectoryName\"   (eg \\ntc-cpe\ntc-cpe)



\\ntc-cpe\ntc-cpe

Name	Date modified	Type
usb1_1		File Folder

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.

APPENDIX C:CLI COMMANDS VIA TELNET

Show all CLI commands

Description: List all available CLI commands that the 3G gateway supports.

Synopsis: help | ?

Example:

```
> help
?
help
logout
reboot
ddns
dumpcfg
arp
defaultgateway
dhcpserver
dns
lan
passwd
remoteaccess
restoredefault
route
save
ping
sntp
sysinfo
tftp
wlan
sierra
version
build
```

serialnumber

End the telnet session

Description: End the telnet session

Synopsis: logout

Example:

```
> logout
```

Reset/reboot device

Description: To reboot the gateway.

Synopsis: reboot

Example:

```
> reboot
```

Radio Signal Strength

Description: Display the 3G radio signal strength.

Synopsis: sierra show --signal

Example:

```
> sierra show --signal
signal: 23
```

Note: Signal value is explain in the table below

Radio Band

Description: Display the 3G band

Synopsis: sierra show --band

Example:

```
> sierra show --band
band: IMT2000
```

Note: IMT2000 is band 2100 and WCDMA800 is band 850

Connection status

Description: Display the 3G network connection status

Synopsis: sierra show –link
    sierra show --gstatus

Examples:

```
> sierra show --link
link: Connected
> sierra show --gstatus
Current Time: 450 Temperature: 45
Bootup Time: 1 Mode: ONLINE
System mode: WCDMA PS state: Attached
WCDMA band: WCDMA800 GSM band: Unknown
WCDMA channel: 4436 GSM channel: 65535
GMM (PS) state:REGISTERED NORMAL SERVICE
MM (CS) state: IDLE NORMAL SERVICE
WCDMA L1 State:L1M_FACH RRC State: CELL_FACH
RX level (dBm):-90
```

IMSI & IMEI read

Description: Display the IMSI and IMEI value

Synopsis: sierra show --imsi

    sierra show --imei

Example:

```
> sierra show --imsi
imsi: 466974800524867
> sierra show --imei
IMEI: 354219010024303
```

Network Information

- sierra show --hsdcat

Description: To indicate the current HSDPA category.

Synopsis: sierra show --hsdcat

Example:

```
> sierra show --hsdcat
!HSDCAT: 8
```

- sierra show --hsucat

Description: To indicate the current HSUPA category.

Synopsis: sierra show --hsucat

Example:

```
> sierra show --hsucat
!HSUCAT: 5
```

- sierra show --mode

Description: To report the current available and supported network technologies being used.

Synopsis: sierra show --mode

Example:

```
> sierra show --mode
mode: UMTS
```

(Valid values: "GSM", "GPRS", "EDGE", "UMTS", "HSDPA", "HSUPA")

- sierra show --registration

Description: To display the Network Registration Status, Country code and Network code.

Synopsis: sierra show --registration

Example:

```
> sierra show --registration
Network Name: Telstra Mobile
Country Code: 505
Network Code: 01
Registration Status: registered.
```

APN (Access Point Name) read and set

Description: Allows user to read and configure the APN on the 3G gateway. Commands include:

- sierra show --apn <profile>

Description: To display the APN value for custom APN profile.

Synopsis: sierra show [--apn <profile>]

<profile> 1:telstra.pcpack 2:telstra.datapack 3:telstra.internet 4:Custom APN

Example: Display the current APN for the profile Custom APN

```
> sierra show --apn 1
Profile1 APN: telstra.pcpack
```

- sierra set --apn <profile> <apn>

Description: To configure the APN value for custom APN profile.

Synopsis: sierra set [--apn <profile> <apn>]

    <profile> 4: Custom APN

Example: Set the Custom APN to test.test

```
> sierra set --apn 4 test.test
```

Authentication Method set and read

Description: To set and query authentication method (PAP/CHAP/AUTO) for PDP-IP packet data calls if the profile supports.

Synopsis: Authentication method set:

```
    sierra set --auth <profile> <method>
<profile> 4:Custom APN
<method> 0:AUTO 1:PAP 2:CHAP
```

```
    Authentication method read:
    sierra show --auth <profile>
 <profile> 4:Custom APN
```

Examples: Configure the customer profile to authentication PAP

```
> sierra set --auth 4 1
```

Display the current authentication requirement for the customer profile

```
> sierra show –auth 4
Profile4: "PAP"
```

Set Radio Band for APN profile

Description: To configure the frequency band for each APN profile.

Synopsis: sierra set [--band <profile> <band>]

```
    <profile> 1:telstra.pcpack  2:telstra.datapack  3:telstra.internet  4:Custom APN
<band> 0: auto  1: 3G-850 Only  2: 3G-850/2G-900/1800  3: 3G-ALL  4: 2G-ALL
```

Example:

Configure the customer profile to select frequency band automatically

```
> sierra set --band 4 0
> reboot
```

(Please reboot the gateway to make the change to take effect after configuring the band setting)

IP header/Data compression set and read

- sierra set --comp <profile> <type> <enable|disable>

Description: To enable or disable the IP header compression and data compression functions.

Synopsis: sierra set [--comp <profile> <type> <enable|disable>]

<profile> 1:telstra.pcpack 2:telstra.datapack 3:telstra.internet 4:Custom APN

<type> 0:IP HEADER 1:DATA

Example: Enable the IP header compression for Custom APN

```
> sierra set --comp 4 0 enable
```

- sierra show --comp <profile>

Description: To display the IP header or data compression status.

Synopsis: sierra show --comp <profile>

<profile> 1:telstra.pcpack 2:telstra.datapack 3:telstra.internet 4:Custom APN

Examples:

```
> sierra show --comp 1
Profile1: IPH is Off, DATA is Off
```

Connect / Disconnect PPP session

Description: To connect or disconnect the PPP session. The profile to be used to develop a connection is the latest configured by the sierra set command.

Synopsis: sierra set [--connection <connect ¦ disconnect> <num>]

<num> 0:First APN 1:Secondary APN

Examples: To connect the PPP session

```
>sierra set –connection connect
```

PIN code configuration

- sierra set --PIN-LOCK <enable|disable> <PIN code> <save>

Description: To enable or disable the PIN code protection and save to the SIM card.

Synopsis: sierra set [--PIN-LOCK <enable|disable> <PIN code>] <save>

Example: To enable the SIM PIN protection with PIN code 0000

```
> sierra set --PIN-LOCK enable 0000 save
```

- sierra set --PIN <PIN code> <save>

Description: To save the PIN code into gateway configuration settings.

Synopsis: sierra set [--PIN <PIN code> <save>]

Example: To save the PIN code 0000 into gateway configuration setting

```
> sierra set --PIN 0000 save
```

- sierra show --PIN-LOCK

Description: To display the PIN code protection status.

Synopsis: sierra show --PIN-LOCK

Example:

```
> sierra show --PIN-LOCK
PIN code protection is disabled
```

- sierra show --SIM

Description: To display the SIM card status.

Synopsis: sierra show --SIM

Example:

```
> sierra show --SIM
```

SIM inserted (SIM card is correctly inserted to the USIM slot)

SIM not inserted (SIM card is not inserted to the USIM slot)

USIM is PIN locked (SIM card is locked by the PIN code)

Incorrect SIM (a SIM card from other Internet service provider is inserted, SIM card can’t be recognized by the network)

PUK locked (SIM card is locked by the PUK code)

- sierra set --PIN-CHG <old PIN code> <new PIN code>

Description: Change the current PIN code to the new one.

Synopsis: sierra set [--PIN-CHG <old PIN code> <new PIN code>]

Example: Change the PIN code from 0000 to 1111

```
> sierra set --PIN-CHG 0000 1111
  changed the PIN code successfully
```

PUK code unlock

Description: Enter the new PUK code and configure the new PIN code when the modem is

PUK locked.

Synopsis: sierra set [--PUK <PUK key> <new PIN code>]

Examples: Unlock the modem with PUK key 11111111 and configure the PIN code as 0000

```
> sierra set --PUK 11111111 0000
PUK unlock successfully
The connection is up already!!
```

Wireless LAN mode set and read

Description: Allows user to configure the Wireless LAN interfaces on the 3G gateway.

This command can be use to configure basic feature, security feature, wireless bridge feature and MAC filter features of the wireless LAN interface.

Synopsis:

```
> wlan
wlan command usage :
wlan config [option]
wlan security [option]
wlan macfilter [option]
wlan wds [option]
wlan info [option]
wlan –help
```

Each option will be explained separately below.

Note: The settings changed from these commands take effect immediately and will be updated on the web page

1. Please enable the wireless BEFORE changing other wireless settings.

2. The wlan command will save the configuration into flash memory and the new settings will be saved.

Since the settings changed from wlan command take effect immediately, it is not recommended to modify the wireless settings through the Web UI at the same time.

Configure basic Wireless LAN features

Description: Configure basic wireless LAN features such as 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.

Synopsis:

```
wlan config [--enable <0|1>] [--hide <0|1>]
[--ssid <ssidStr>] [--country <countryStr>]
[--isolate <0|1>]
[--channel <channelVal>] [--rate <rateVal>]
[--mrate <rateVal>]
[--rts <rtsThreshold>] [--frag <fragThreshold>]
[--dtim <dtimInterval>] [--beacon <beaconInterval>]
[--xpress <on|off>] [--gmode <auto|performance|lrs|802.11b>]
[--gprotect <off|auto>] [--preamble <long|short>]
```

Options:

--enable <0|1>

Description: Enable or disable wireless LAN interface.

Valid value: 0 or 1

0 – disabled the wireless LAN interface.

1 – enabled the wireless LAN interface.

Default value: 1

--hide <0|1>

Description: Hide wireless LAN network name (SSID).

Valid value: 0 or 1

0 – not hide wireless LAN SSID.

1 – hide wireless LAN SSID

Default value: 0

--ssid <ssidStr>

Description: Set Wireless LAN network name (SSID).

Valid value: 32 characters string

--country <countryStr>

Description: Set Wireless LAN Country, only accept abbreviation.

Valid value: 2 or 3 characters string (AUSTRALIA is abbreviated to AU).

--isolate <0|1>

Description: Set wireless devices isolation. When enabled, wireless devices connected to the gateway will not be able to communicate to each other

Valid value: 0 or 1

0 – not isolate wireless devices.

1 – isolate wireless devices

Default value: 0

--channel <channelVal>

Description: Set the wireless LAN channel.

Valid value: 0~14

0 means auto select channel.

Default value: 0

--rate <rateVal>

Description: Set the wireless LAN data rate.

Valid value: 0, 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 (Mbps)

0 means auto

Default value: 0

--mrate <rateVal>

Description: Set the wireless LAN Multicast rate.

Valid value: 0, 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 (Mbps)

0 means auto

Default value: 0

--rts <rtsThreshold>

Description: Set the wireless LAN RTS threshold.

Valid value: 0~2347

Default value: 234

--frag <fragThreshold>

Description: Set the wireless LAN fragment threshold.

Valid value: 256~2346

Default value: 2346

--dtim <dtimInterval>

Description: Set the wireless LAN DTIM interval.

Valid value: 1~255

Default value: 1

--beacon <beaconInterval>

Description: Set the wireless LAN beacon interval.

Valid value: 1~65535

Default value: 100

--xpress <on|off>

Description: Enable or disable the xpress feature

Valid value: on / off

Default value: off

--gmode <auto|performance|lrs|802.11b>

Description: Set the wireless LAN G mode

Default value: auto

--gprotect <off|auto>

Description: Enable or disable the gprotect feature

Default value: auto

--preamble <long|short>

Description: Set the wireless LAN preamble

Default value: long

EXAMPLE 1:

User wants to enable the wireless LAN, configure the wireless LAN network name (SSID) as “TestAP”, configure wireless LAN channel to 5 and then hide the SSID:

```
wlan config --enable 1

wlan config --ssid “TestAP”

wlan config --channel 5 --hide 1
```

Or merge the above commands

```
wlan config --enable 1 --ssid “TestAP” --channel 5 --hide 1
```

Configure wireless LAN security

Description: Enable or disable and configure the wireless LAN security. This gateway supports different types of security such as: WEP, 802.1X, WPA and WPA2.

Synopsis:

```
wlan security open

[--wep <enabled|disabled>] [--keybit <64|128>]

[--nkey1 <keyStr>] [--nkey2 <keyStr>]

[--nkey3 <keyStr>] [--nkey4 <keyStr>]

[--keyidx <1|2|3|4>]

wlan security shared (wep have to enable)

[--wep <enabled|disabled>] [--keybit <64|128>]

[--nkey1 <keyStr>] [--nkey2 <keyStr>]

[--nkey3 <keyStr>] [--nkey4 <keyStr>]

[--keyidx <1|2|3|4>]

wlan security radius (wep have to enable)

[--rasip <serverIp>] [--raspt <portVal>] [--raskey <”raskeyStr”>]

[--wep <enabled|disabled>] [--keybit <64|128>]

[--nkey2 <keyStr>] [--nkey3 <keyStr>]

[--keyidx <2|3>]

wlan security wpa / wpa2 / wpa2mix

[--wlPreauth <0|1>] [--wlNetReauth <interval>]

[--wpaenc <tkip|aes|tkip+aes>] [--rekey <interval>]

[--rasip <serverIp>] [--raspt <portVal>] [--raskey <”raskeyStr”>]

[--wep <enabled|disabled>] [--keybit <64|128>]

[--nkey2 <keyStr>] [--nkey3 <keyStr>]

[--keyidx <2|3>]

wlan security psk / psk2 / psk2mix
```

[--wpaenc <tkip|aes|tkip+aes>] [--rekey <interval>]

[--pskey <"pskeyStr">]

[--wep <enabled|disabled>] [--keybit <64|128>]

[--nkey2 <keyStr>] [--nkey3 <keyStr>]

[--keyidx <2|3>]

Options:

--wep <enabled|disabled>

Description: enable or disable WEP encryption

--keybit <64|128>

Description: Set the WEP encryption strength

--nkey1 <keyStr>

--nkey2 <keyStr>

--nkey3 <keyStr>

--nkey4 <keyStr>

Description: Set the WEP key.

Note: 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys

--keyidx <1|2|3|4>

Description: Set the current WEP Key index.

--rasip <serverIp>

Description: Set the RADIUS server IP address.

--raspt <portVal>

Description: Set the RADIUS server port.

Valid value: 1~65535

Default value: 1812

--raskey <raskeyStr>

Description: Set the RADIUS Key.

Valid value: string of 79 characters.

--wpaenc <tkip|aes|tkip+aes>

Description: Set the WPA encryption

3G10WVT - HSPA 7.2Mbps Wi-Fi Gateway with Voice USER GUIDE

--rekey <interval>

Description: Set the Group Rekey Interval

Default value: 0

--pskey <"pskeyStr">

Description: Set the WPA Pre-Shared Key

Valid value: string of 8 ~ 63 characters.

Note: 1. wlPreauth can only be used with WPA2.

2. When using WPA-PSK or WPA2-PSK, WPA Pre-Shared Key (pskey) must be set first.

3. WEP MUST be enable when security is set to shared / 802.1X radius security mode.

4. WEP MUST be disable when security is set to WPA/WPA-PSK security mode

5. When setting keyidx to N for WEP key, ensure that the nkeyN field has a string value.

6. Always issue a complete security command. For example, once WEP is enabled, it will still be enabled even after changing the security mode, until the command "--wep disabled" is received by the gateway.

EXAMPLE 2:

After setting up the wireless configuration in example 1, the user wants to configure the wireless LAN security.

Scenario 1:

WPA2 with Radius server IP address of 172.16.2.199

wlan security wpa2 --rasip 172.16.2.199 --wlPreauth 1

Scenario 2:

WPA-PSK with "123456789" as the passkey.

wlan security psk --pskey "123456789" --wpaenc aes --wep disabled

Scenario 3:

802.1X with Radius server IP of 172.16.2.199 and RADIUS key as "whatever"

wlan security radius --rasip 172.16.2.199 --raskey "whatever" --wep enabled

CONFIGURE WIRELESS LAN MAC FILTER

Description: Enable, disable and configure the wireless LAN MAC filter feature. This feature enables the gateway to allow or deny connection from wireless client based on the MAC address.

Synopsis:

wlan macfilter [--mode <disabled|allow|deny>]

[--add <MACaddress>]

[--remove <MACaddress>]

Options:

--mode <disabled|allow|deny>

Description: Disable and set the wireless LAN MAC filter mode.

Valid Value:

Disabled: disable wireless LAN MAC filter

Allow: only allow access to wireless client with the MAC address listed in the gateway

Deny: allow all wireless client to connect unless the MAC address is listed in the gateway

Default Value: disabled

--add <MACaddress>

Description: add one MAC Address entry

--remove <MACaddress>

Description: remove one MAC Address entry

Note: The setting of the MAC filter takes effect immediately. When setting up this feature through the wireless interface, be careful of blocking the computer.

Changing the mode will make the MAC address list be reserved.

To see the list of MAC addresses, use the command "wlan info –macfilter".

EXAMPLE 3:

After Example 2, the user want to allow only wireless client with MAC address of 00:11:22:33:44:55 to be able to connect to the gateway

```
wlan macfilter --mode allow --add 00:11:22:33:44:55
```

Following the command above, if the user wants to deny wireless client with MAC address of 00:11:22:33:44:55 to be able to connect to the AP.

```
wlan macfilter --mode deny
```

Configure Wireless Bridge (Wireless Distribution System/WDS)

Description: configure the wireless bridge

Synopsis:

```
wlan wds [--mode <ap|wds>] [--restrict <enabled|disabled>]
[--rmac1 <MACaddress>] [--rmac2 <MACaddress>]
[--rmac3 <MACaddress>] [--rmac4 <MACaddress>]
```

Options:

--mode <ap|wds>

Description: configure wireless AP mode.

Default value: ap

--restrict <enabled|disabled>

Description: enable or disable bridge restrict mode.

Default value: disabled

--rmac1 <MACaddress>

--rmac2 <MACaddress>

--rmac3 <MACaddress>

--rmac4 <MACaddress>

Description: set remote bridge MAC address

Note: The "--restrict" option have to be enable before setting any restrict MAC address (--rmac1~4) or the restrict MAC address setting will be ignored.

The behavior of WDS is similar to connecting two or more AP using a hub. However, please be aware of the IP assignment to prevent assigning two or more hosts / STAs to the same IP address. To avoid IP address conflict, only enable DHCP server in one gateway and disable the other gateway DHCP server.

WDS CLI (command line interface) does NOT support Enable (Scan) mode in Bridge Restrict while using WUI (Web UI) does. When Bridge Restrict set to Enable (Scan) mode in WUI, the CLI will show Bridge Restrict disabled.

EXAMPLE 4:

After example 3, the user want to connect another AP which has DHCP disabled and the MAC address is 00:12:34:56:78:9a

```
wlan wds --mode wds --restrict enabled --rmac1 00:12:34:56:78:9a
```

Show wireless LAN interface configurations

Description: show the current configuration of the wireless LAN interface

Synopsis:

```
wlan info [--config] [--security]
[--macfilter] [--wds] [--station]
```

Options:

--config

Description: display the list of parameters from config option

Example:

```
> wlan info --config
Wlan Config Info :
Basic :
wlan config enable = 1
wlan config hide = 0
wlan config ssid = Series7Wireless7890
wlan config bssid = 00:11:22:33:44:56
wlan config country = AU
Advance :
wlan config isolate = 0
wlan config band = b
wlan config channel = 0
wlan config rate = 0
wlan config mrate = 0
wlan config brate = default
wlan config rts = 2347
wlan config frag = 2346
wlan config dtim = 1
wlan config beacon = 100
wlan config xpress = off
wlan config gmode = auto
wlan config gprotect = auto
wlan config preamble = long
```

3G10WVT - HSPA 7.2Mbps Wi-Fi Gateway with Voice USER GUIDE

--security

Description: display the list of parameters from security option

Example:

```
> wlan info --security
Wlan Security Info :
wlan security auth mode = psk
wlan security wpa = aes
wlan security wpaGTKRekey = 0
wlan security wpaPresharedKey = 1234567890
wlan security Wepstate = disabled
wlan security WepKeyBit = 128
wlan security WepKey2 =
wlan security WepKey3 =
wlan security WepCurrentKeyindex = 1
```

--macfilter

Description: display the list of parameters from macfilter option

Example:

```
> wlan info --macfilter
Wlan macfilter Info :
wlan macfilter mode = disabled
wlan macfilter entry :
```

--wds

Description: display the list of parameters from wds opiton

Example:

```
> wlan info --wds
Wlan wds Info :
wlan wds mode = ap
wlan wds restrict mode = disabled
```

--station

Description: display the list of authenticated wireless stations and their status

Example:

```
> --wlan info --station
--wlan info --station: not found
```

Configure Access Control

Description: to list and to configure access control from LAN & WAN.

(1) To set up the access control list.

Synopsis: remoteaccess service [--service <servicename>] <--interface <none|local|remote|both> >

<servicename>: FTP, HTTP, ICMP, TELNET, SSH, TFTP

<none|local|remote|both>:

- none: disable the service.
- local: enable the service at LAN side only
- remote: enable the service at WAN side only
- both: enable the service at both LAN and WAN sides.

(2) To add an entry of IP range that to be enable to manage the gateway. Subnet mask of 255.255.255.255 is for a host with the specific IP address.

Synopsis: remoteaccess iprange --add <IP address> <Subnet mask> <none|local|remote|both>

<none|local|remote|both>

- none: forbid the IP range to manage the 3G10WVT.
- local: permit the IP range to manage the 3G10WVT from LAN side only.
- remote: permit the IP range to manage the 3G10WVT from WAN side only.
- both: permit the IP range to manage the 3G10WVT from both LAN and WAN.

(3) To delete an entry of IP range that to be enable to manage the gateway.

Synopsis: remoteaccess iprange --remove <IP address> <Subnet mask>

(4)To enable or disable the all the IP ranges defined by command (2).

Synopsis: remoteaccess accesscontrolmode <--enable <0|1> >

* Argument --enable 1 is to enable the access list; argument --enable 0 is to disable the access list;. Please note (a) enabling access list mode is only for the case of at least one IP list is created; (b) after removing the last entry in the table, the access list mode will be disabled automatically. This is to avoid no IP being on the list when access mode is enabled; it will cause the gateway no being able to be managed by any IP address. The only solution under this circumstance is to reset 3G10WVTT gateway back to factory default by press the reset button on the back of the gateway for over 8 seconds.

(5) To display all current settings for remote access.

Synopsis: remoteaccess show

(6) To view the usage of "remoteacesss" command.

Synopsis: remoteaccess –help

config AP mode.

Default value : ap

--restrict <enabled|disabled>

config bridge restrict mode.

Default value : disabled

--rmac1 <MACaddress>

--rmac2 <MACaddress>

--rmac3 <MACaddress>

--rmac4 <MACaddress>

config remote bridge MAC address

NOTE 4:

You should enable the option - "restrict" before setting any restrict MAC address (setting --rmac1~4) or your restrict MAC address setting will be ignored.

After the version – C40_R01, the wireless driver – 3.91.15.0 supports both BCM4318 and BCM4306; Version - C39_R02 with the wireless driver - 3.61.13.0 supports only BCM4306;

The behavior of wds is similar to connect two or more AP using a hub, be aware of the IP assignment to prevent assigning two or more hosts / STAs to the same IP address. You could enable only one DHCP server in one gateway and disable all other's to avoid the conflict of the IP assignment.

WDS CLI does NOT support Enable(Scan) mode in Bridge Restrict while WEB does. If you set Bridge Restrict to Enable(Scan) mode, the CLI will show Bridge Restrict disabled.

EXAMPLE 4:

After example 3, we want to use wds to connect with the other AP which has disabled the DHCP server (NOTE 4) and has MAC address - 00:12:34:56:78:9a; we can achieve the goal using the following command.

```
wlan wds --mode wds --restrict enabled --rmac1 00:12:34:56:78:9a
```

info: Show the configurations of WLAN interface and the information of stations connected to this AP.

Options for the info command

```
wlan info [--config] [--security]
          [--macfilter] [--wds] [--station]
```

--config

list parameters of config command

--security

list parameters of security command

--macfilter

list parameters of macfilter command

--wds

list parameters of wds command

--station

list authenticated wireless stations and their status

NOTE 5:

You can use this command to view your wireless settings; no matter the settings are modified from web or CLI, the command will show the latest information for you.

EXAMPLE 5:

After example 4, if we forgot our ssid, we can view the ssid with the following command.

```
wlan info --config
```

--help: Display usage for WLAN interface.

Scenario 2 to configure AP with OPEN-disabled security:

```
wlan config --enable 1--ssid “WLAN_TLF” --hannel 8
wlan security open --wep disabled
```

Scenario 3 to configure AP with Shred-WEP security

```
wlan config --enable 1--ssid “WLAN_TLF” --hannel 8
wlan security shared --wep enabled --nkey1 1234567890123 --keyidx 1
```

Scenario 4 to configure AP with 802.1X security

```
wlan config --enable 1--ssid “WLAN_TLF” --hannel 8
wlan security radius --rasip 172.16.2.199 --raskey “whatever” --wep enabled
```

Scenario 5 to configure AP with WPA-PSK security

```
wlan config --enable 1--ssid “WLAN_TLF” --hannel 8
wlan security psk --pskey “123456789” --wpaenc aes
```

Scenario 6 to configure AP with WPA2 security

```
wlan config --enable 1--ssid “WLAN_TLF” --hannel 8
wlan security wpa2 --rasip 172.16.2.199 --wlPreauth 1
```

TECHNICAL SUPPORT:

Telstra Business Broadband:

1800 655 744