



Wireless 11ac Bonded VDSL2 Modem Gateway with MoCA 2.0

Model # T3200M

User Guide

Table of Contents

Getting Started With the Gateway	4
Package Contents	5
Minimum System Requirements	5
Features	5
Getting to Know the Gateway	6
Connecting the Gateway	9
Accessing the Home Screen	11
Accessing the Home Screen	11
Icon Bar	13
Connection Status	13
Checking the Gateway's Status	14
Accessing the Status Screens	14
Connection Status	15
xDSL Status	16
WAN Ethernet	17
Routing Table	17
Firewall Status	18
NAT Table	19
Wireless Status	19
Modem Utilization	21
LAN Status	22
ARP Table	23
Interface Statistics	23
Multicast Statistics	24
System Log	24
Configuring Wireless Settings	25
Accessing Wireless Settings	25
Basic Settings	26
Advanced Settings	27
WPS	28
MAC Address Control	29
WDS	30

Table of Contents

Configuring Firewall Settings	31
Accessing Firewall Settings	31
Firewall	32
IPv6 Firewall	33
Port Forwarding	34
Applications	35
DMZ Hosting	36
IPv6 DMZ Hosting	37
UPnP	38
Advanced Settings	39
Accessing the Advanced Setup Screens	39
Services Blocking	40
Website Blocking	41
Scheduling Access	41
WAN IP Addressing	42
IPv6 WAN Settings	43
LAN IP Settings	44
IPv6 LAN Settings	45
DHCP Reservation	45
Dynamic DNS	46
DNS Host Mapping	47
Port Bridging	47
Admin Password	48
Storage Device Info	48
Samba Configuration	49
Voice Advanced Setting	49
Voice Basic Setting	50
Voice Debug Setting	51
Reboot	51
Restore Defaults	52
Check for New Firmware	52
Speed Test	53
Ping Test	54
Tcpdump Debug	55
Iperf Test	56
IPv6 Ping Test	57
Traceroute	58

Table of Contents

IPv6 Traceroute	58
Time Zone	59
Language Settings	59
DNS Cache	60
IGMP Setting	60
Upgrade History	61
SIP ALG	61
Tool Box	62
DLNA	62
xDSL Diagnostics	63
User's Manual	63
Specifications	64
General	64
Wireless Operating Range	65
LED Indicators	65
Environmental	65
Notices	66
Regulatory Compliance Notices	66
Modifications	66
GPL (General Public License)	67

Getting Started With the Gateway

1

Congratulations on purchasing the T3200M Wireless 11ac Bonded VDSL2 Modem Gateway with MoCA 2.0. The Gateway is a single platform device that supports universal WAN access, FTTN, FTTP, FTTB, or FTTP. With support for advanced 802.11ac 4x4 WiFi and bonded MoCA 2.0, the Gateway enables blazing fast HD video streaming, with multi-channel HD video throughput. The Gateway also offers an unprecedented level of security, helping protect your network resources. It has also been designed to deliver unparalleled WiFi performance, using dual-band WiFi supporting speeds up to 2.3 Gbps.



Package Contents

- Black Power adapter
- Yellow cable(Ethernet, 6ft.)
- White cable (Ethernet, 10ft.)
- Quick Start Guide
- Installation Guide
- Wall-mount template
- Vertical stand

Minimum System Requirements

- Active ADSL2+ service
- Computer with an 10 Mbps or 10/100/1000 Mbps Ethernet connection
- Microsoft Windows 10, 8, 7; Mac OS OS X+
- TCP/IP network protocol installed on each computer

Features

- ADSL2+, VDSL2, G.fast, and Fiber in a single CPE
- Dual Band WiFi delivering up to 2.3 Gbps with 802.11ac 4x4 5GHz and 802.11n 3x3 2.4GHz
- MoCA 2.0 with Channel Bonding and Turbo Mode
- Optimized for IPTV and Video over WiFi
- Integrated VoIP with 2 FXS Ports
- SFP cage for G.fast or EPON/GPON ONT modules

Getting to Know the Gateway

This section contains a quick description of the Gateway's lights, ports, and other features. The Gateway has several indicator lights (LEDs) and a button on its front panel, and a series of ports and switches on its rear panel.

Front Panel

The front panel of the Gateway features 2 LEDs (WAN and Wireless), and a WPS (Wireless Protected Setup) button.

WAN LED

The WAN LED illuminates when the Gateway is properly connected to a WAN Internet connection.

Wireless LED

The Wireless LED illuminates when the Gateway's wireless network is operating and properly configured.

WPS Button

The WPS button is used when connecting a wireless device to the Gateway's wireless network using WPS.

Introduction

Rear Panel

The rear panel of the Gateway features 14 ports, and a Reset button.



Power Port

The Power port is used to connect the Power cord (Model No. NBS40C120300VU, made by NetBit, or Model No. CDS036-W120U, made by Actiontec) to the Gateway.

Reset Button

Depressing the Reset button for 10 seconds will restore the Gateway's factory default settings. The reset process will start after releasing the button.

Coax Port

The Coax port is used to connect the Gateway to a coaxial connection via coaxial (MoCA) cable.

SFP Cage

The SFP cage is used to connect the Gateway to a service provider connection via optical fiber cable.

WAN Ethernet Port

The WAN Ethernet port is used to connect the Gateway to a WAN connection via an Ethernet cable.

LAN Ethernet Ports (4)

The LAN Ethernet ports are used to connect computers to the Gateway via Ethernet cable. The Ethernet ports are 10/100/1000 Mbps auto-sensing ports, and either a straight-through or crossover Ethernet cable can be used when connecting to the ports.

USB Ports (2)

The USB ports are used to connect the Gateway to a USB device.

DSL Ports (2)

The DSL ports are used to connect the Gateway to a DSL wall outlet via DSL cable.

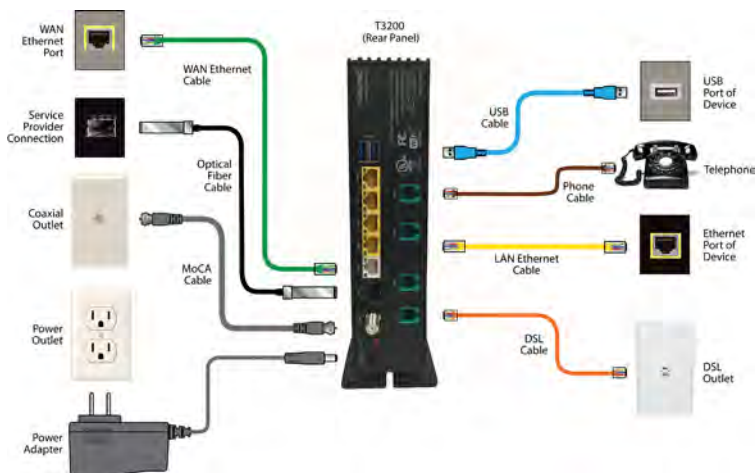
VoIP Ports (2)

The VoIP ports are used to connect the Gateway to a telephone or other communication device via phone cable.

WARNING! Do not unplug the Power cord from the Gateway during the reset process. Doing so may result in permanent damage to the Gateway.

Connecting the Gateway

There are many variables involved when connecting the Gateway, depending on the type of Internet service available. The figure below shows all of the possible connections available for the Gateway.



Connecting a Computer to the Gateway

To connect a computer to the Gateway to access the Gateway's graphical user interface (GUI):

1. Get the Gateway and black Power cord from the box.
2. Plug the black Power cord in the black port on the back of the Gateway and then into a power outlet.
3. Turn the Gateway on.
4. Plug the yellow Ethernet cable from the box into one of the four yellow Ethernet ports on the back of the Gateway.

Telus T3200M Gateway

5. Make sure the computer is powered on, then plug the other end of the yellow Ethernet cable into an Ethernet port on the computer.
6. Make sure at least the LED on the LAN port into which the Ethernet cable is plugged steadily green. This may take a few moments.
7. The computer should either be configured with a statically defined IP address and DNS address, or instructed to automatically obtain an IP address using the Network DHCP server. The Gateway is set up, by default, with an active DHCP server, and it is recommended to leave this setting as is.

Accessing the Home Screen

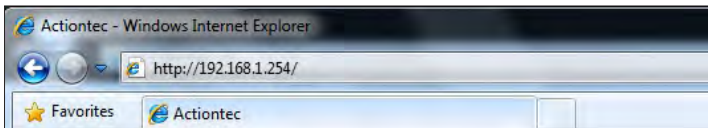
2

This chapter gives a short overview of the Home screen of the Gateway's graphical user interface (GUI).

Accessing the Home Screen

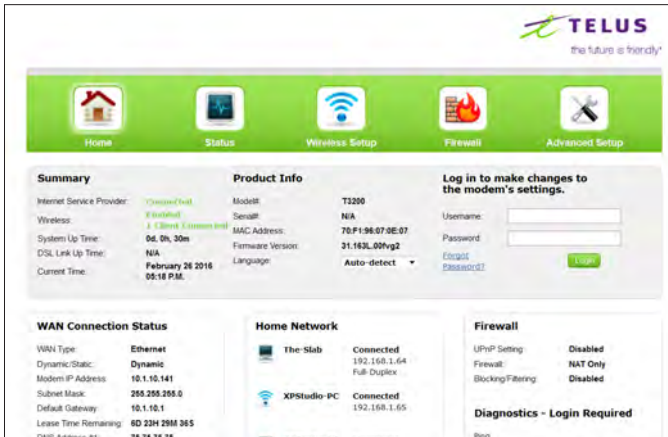
To access the Home screen:

1. Open a Web browser on computer connected, via Ethernet cable, to one of the Gateway's LAN ports. In the *Address* text box, type:
http://192.168.1.254
then press **Enter** on the keyboard.



Telus T3200M Gateway

- The Gateway's Home screen appears.



- Enter the username "admin" and the password found on the sticker on the back of the Gateway in the *Username* and *Password* text boxes at the top right side of the screen, then click **Login**.

Log in to make changes to the modem's settings.

Username:

Password:

[Forgot Password?](#)

The Gateway's GUI is now accessible.

Home Screen

Icon Bar

At the top of the Home screen is the Icon Bar. Here, you can quickly access the other four main sections of the Gateway's GUI by clicking on the appropriate icon: Status (see chapter x for more details); Wireless Setup (see chapter x for more details); Firewall (see chapter x for more details); Advanced Setup(see chapter x for more details). Clicking Home in any other screen generates the Home screen.



Connection Status

The bottom of the Home screen consists of connection and device information relating to the Gateway. There are no configurable options here.

Summary Internet Service Provider: Comcast-Net Wireless: Enabled System Up Time: 0d, 0h, 33m DSL Link Up Time: NA Current Time: February 26 2016 06:21 P.M.	Product Info Model#: T2209 Serial: GTB46040402228 MAC Address: 78:F1:96:07:0E:07 Firmware Version: 31.16L.00Vg2 Language: Auto-detect	Login Status You are currently logged in as admin Logout
WAN Connection Status WAN Type: Ethernet Dynamic/Static: Dynamic Modem IP Address: 10.1.10.141 Subnet Mask: 255.255.255.0 Default Gateway: 10.1.10.1 Lease Time Remaining: 6D 23H 26M 53S DNS Address #1: 75.75.75.75 DNS Address #2: 75.75.75.75	Home Network The Slab: Connected 192.168.1.64 Full-Duplex XPStudio-PC: Connected 192.168.1.65 XPStudio-PC: Connected 192.168.1.66	Firewall UPnP Setting: Disabled Firewall: NAT Only Blocking/Filtering: Disabled Diagnostics - Login Required Ping Traceroute Wireless Reset Device Reboot Factory Reset DHCP Release/Renew User's Manual
Wireless SSID: TELUS0225 Security: Enabled Security Type: WPA/WPA2-AES SSID: TELUS0225-5G		

Checking the Gateway's Status

3

This chapter explains the options available on the Status screens, which display information about the Gateway's network connections.

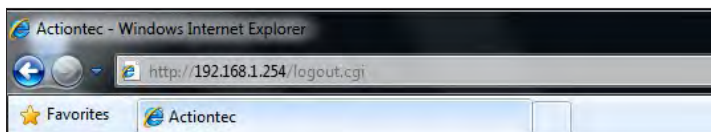
Accessing the Status Screens

To access the Gateway's Status screens:

1. Open a Web browser. In the *Address* text box, type:

<http://192.168.1.254>

then press **Enter** on the keyboard.



2. The Gateway's Main screen appears. Click the *Status* icon.

Status



3. The *Connection Status* screen appears.

The screenshot shows the 'Connection Status' screen. On the left is a sidebar menu with categories: 'Internet Services' (with 'Connection Status' selected), 'LAN Services', and 'System Monitor'. The main area displays a table of network parameters and their status.

Parameter	Status
Broadband:	Connected
Internet Service Provider (ISP):	Connected
Firmware Version:	31.163L.00lvq2
Model Number:	T3200
Serial Number:	GTBA6040460225
WAN MAC Address:	70:f1:96:07:9e:07
Downstream Rate:	N/A
Upstream Rate:	N/A
ISP Protocol:	1483 via DHCP
Encapsulation:	N/A
Modem IP Address:	10.1.10.141 Release/Renew
Lease Time Remaining:	6D 23H 24M 55S
DNS Address #1:	75.75.75.75
DNS Address #2:	75.75.76.76
IPv6 Prefix of Delegated:	N/A
IPv6 WAN Status:	Connecting
IPv6 WAN Address:	N/A
IPv6 WAN Link Local Address:	fe80::72f1:96ff:fe07:e07
IPv6 LAN Link Local Address:	fe80::72f1:96ff:fe07:e00
IPv6 Unique Local Address:	N/A
IPv6 DNS Address 1:	N/A
IPv6 DNS Address 2:	N/A

From here, all the Status screens can be accessed from the menu on the left.

Connection Status

Clicking Connection Status from any Status screen generates the *Connection Status* (see figure, above). Information concerning the devices connected to the Gateway's network, whether wired or wireless, is displayed here, along with the connected device's IP address, MAC address, and (if applicable) IPv6 address.

xDSL Status

Click **xDSL Status** from any Status screen to generate the *xDSL Status* screen. This screen displays the Gateway's DSL connection parameters.

xDSL Status	
Connection	
Telus Broadband	Disconnected
Internet Service Provider	Disconnected
PPP Parameter	
User Name	N/A
PPP Type	N/A
LCP State	DOWN
PCP State	DOWN
Authentication Failures	0
Session Time	0 Days, 00H:00M:00S
Packets Sent	N/A
Packets Received	N/A
Modem Uptime	0 Days, 00H:00M:00S
PPP Mode	N/A
DSL Link	
DSL Link Uptime	0 Days, 0H:0M:0S
Retrains	N/A
Retrains in Last 24 Hours	N/A
Loss of Power Link Failures	N/A
Loss of Signal Link Failure	N/A
Loss of Margin Link Failure	N/A

Status

WAN Ethernet

Click **WAN Ethernet** from any Status screen to generate the *WAN Ethernet Status* screen. This screen displays the Gateway's WAN (wide access network) parameters.

WAN Ethernet Status	
Parameter	Status
Broadband	Connected
Internet Service Provider	Connected
MAC Address:	70:f1:96:07:0e:07
IP Address:	10.1.10.141
Subnet Mask:	255.255.255.0
Default Gateway:	10.1.10.1
Lease Time Remaining	6D 23H 24M 2S
DNS Server:	75.75.75.75,75.75.76.76
Received Packets:	35561
Sent Packets:	26966
Time Span:	0 Days, 0H:35M:59S

Routing Table

Click **Routing Table** from any Status screen to generate the *Routing Table* screen. This screen displays the Gateway's routes.

Routing Table			
Valid	Destination	Netmask	Gateway
YES	0.0.0.0	0.0.0.0	10.1.10.1
YES	10.1.10.0	255.255.255.0	0.0.0.0
YES	169.254.1.0	255.255.255.248	0.0.0.0
YES	192.168.1.0	255.255.255.0	0.0.0.0

IPv6 Routing Table			
Valid	Destination	Netmask	Gateway
YES	:::0	64	-
YES	:::0	64	-
YES	:::0	64	-
YES	:::0	64	-
YES	:::0	64	-
YES	:::0	64	-
YES	:::0	64	-
YES	:::0	64	-

Firewall Status

Click **Firewall Status** from any Status screen to generate the *Firewall Status* screen. This screen displays parameters concerning the Gateway's firewall.

Firewall Status		
The list below displays all firewall settings modified from the factory default settings.		
Firewall Feature	LAN IP	Applied Rule
Applications	N/A	Default Feature Setting
Port Forwarding	N/A	Default Feature Setting
DMZ Hosting	N/A	Default Feature Setting
Firewall Settings	N/A	Default Feature Setting
NAT	N/A	NAT Enabled
UPnP	N/A	UPnP NAT Transversal Not Supported

NAT Table

Click **NAT Table** from any Status screen to generate the *NAT Table* screen. This screen displays the Gateway's WAN (wide access network) parameters.

NAT Table					
Protocol	Timeout	Source IP	Source Port	Destination IP	Destination Port
17	88	192.168.1.64	16403	24.130.151.160	16403
17	88	192.168.1.64	16403	17.156.127.223	16386
17	98	192.168.1.64	16403	17.156.127.222	16384
17	88	192.168.1.64	16403	17.156.127.222	16385
6	65	192.168.1.66	52090	205.206.163.40	80
6	74	192.168.1.66	52091	205.206.163.40	80
6	13	192.168.1.66	52081	205.206.163.40	80
6	13	192.168.1.66	52082	205.206.163.40	80

Status

Wireless Status

Click **Wireless Status** from any Status screen to generate the *WAN Ethernet Status* screen. This screen displays the Gateway's wireless network parameters.

Wireless Status

Select SSID

SSID: TELUS0225-5G

For wireless status, select SSID from drop-down list.

Parameter	Status
Radio:	Enabled
SSID:	Enabled
Security:	Enabled
SSID:	TELUS0225-5G
Channel Selection:	Auto
Channel:	44
Wireless Security Type:	WPA/WPA2 PSK
SSID Broadcast:	Enabled
MAC Authentication:	Disabled
Wireless Mode:	Compatible Mode (802.11a+802.11n+802.11ac)
WPS State:	Enabled
WPS Type:	AP PIN, PBC, End Device PIN
WMM QoS:	Enabled
WMM Power Save:	Enabled
Wireless Packets Sent:	13979
Wireless Packets Received:	7343

[Advanced Wireless Statistics](#) [HomeStatus Wireless Manager](#)

Wireless Status

Click **Advanced Wireless Statistics** from the bottom of the Wireless Status screen to generate the *Advanced Wireless Statistics* screen. This screen displays the Gateway's additional wireless network parameters.

Advanced Wireless Statistics

Frequency: 5G 2.4G

Display: BSSID Noise

BSSID Noise

Items	Values
BSSID	7D-F1-96-97-0E-06
Noise	-88 dBm

Wireless Monitor

Click **Modemstatus Wireless Monitor** from the bottom of the Wireless Status screen to generate the *Wireless Monitor* screen. This screen displays parameters for the clients connected to the Gateway's wireless network.

Wireless Monitor

Select Wireless Client




Wireless client: XPStudio-PC_F0:7B:CB:36:1D:96

Parameter	Status
Hostname	XPStudio-PC
MAC	F0:7B:CB:36:1D:96
RSSI	-40
Connection duration	775 s
Packets sent	26614
Packets Received	22162
Packets lost	507
PHY rate	1.0 Mbps
WMM power save	ON
Disconnection	N/A

Modem Utilization

Click **Modem Utilization** from any Status screen to generate the *Modem Utilization* screen. This screen displays statistics related to the Gateway's modem operation.

Modem Utilization	
Parameter	Status
Total Memory:	224MB RAM
Memory Used:	38%
Memory Status:	OK
Recommended Action:	NONE
Maximum Number of Sessions:	8192
LAN TCP Sessions:	1
LAN UDP Sessions:	3
Modem Sessions:	12
Total Open Sessions:	21
Session Status:	OK
Recommended Action:	NONE

LAN Device Session Log		
Device Name	IP Address	No. Of Open Session
 The-Slab	192.168.1.64	2
 XPStudio-PC	192.168.1.65	3
 XPStudio-PC	192.168.1.66	4

LAN Status

Click **LAN Status** from any Status screen to generate the *LAN Status* screen. This screen displays the Gateway's LAN (local area network) parameters.

LAN Status				
Interface	Port	Connection Speed	Packets Sent	Packets Received
Ethernet	1	1000M	4457	2697
Ethernet	2	DISCONNECTED	N/A	N/A
Ethernet	3	DISCONNECTED	N/A	N/A
Ethernet	4	DISCONNECTED	N/A	N/A
USB	1	undefined	undefined	undefined

Interface	Hostname	MAC Address	IP Address	Port	Connection Speed	Lease Time Remaining
Ethernet	XPSudio-PC	00:24:e8:82:99:6c	192.168.1.66	1	1000Mbps	23H 48M 37S

ARP Table

Click **ARP Table** from any Status screen to generate the *ARP Table* screen. This screen displays the Gateway's ARP (address resolution protocol) table.

ARP Table					
IP Address	HW Type	Flags	HW Address	Mask	Device
169.254.1.2	0x1	0x2	66:f1:96:07:0a:06	*	br0
192.168.1.66	0x1	0x2	00:24:e8:82:99:6c	*	br0
10.1.10.1	0x1	0x2	00:50:f1:80:00:00	*	swan0.1
192.168.1.65	0x1	0x2	80:7b:cb:36:1d:96	*	br0
192.168.1.64	0x1	0x2	60:8b:1d:6b:38:a1	*	br0

Interface Statistics

Click **Interface Statistics** from any Status screen to generate the *Estimated Interface Statistics* screen. This screen displays various statistics and parameters relating to the Gateway's connection interfaces.

Estimated Interface Statistics											
Interface	Connect Speed (Mbps)	Packets				Bytes (MB)			Bytes (MB) since Reset		
		Tx	Rx	Tx Errors	Rx Errors	Tx	Rx	dropped	Tx	Rx	dropped
E/WAN	Auto	27002	35673	0	0	3086880	36800231	0	3086880	36800231	0
XDSL	Auto	27002	35673	0	0	3086880	36800231	0	3086880	36800231	0
Eth LAN#1	1000M	4549	2731	0	0	1584974	582367	0	1584974	582367	0
Eth LAN#2	Disconnected	63	143	0	0	4316	38740	0	4316	38740	0
Eth LAN#3	Disconnected	0	0	0	0	0	0	0	0	0	0
Eth LAN#4	Disconnected	0	0	0	0	0	0	0	0	0	0
WiFi - 2.4G	405M	26758	20279	0	0	25992001	2334276	0	25992001	2334276	0
WiFi - 5G	1733M	14140	7343	0	0	12429270	889567	0	12429270	889567	0

Multicast Statistics

Click **Multicast Statistics** from any Status screen to generate the *Multicast Statistics* screen. This screen displays the Gateway's multicast statistics.

Multicast Statistics						
Channel	Joined Clients		Time Out Value			
	Host	IP	Days	Hour(s)	Minutes	Seconds
No Entries Defined						

System Log

Click **System Log** from any Status screen to generate the *System Log* screen. This screen displays the Gateway's system log, which keeps track of all events that occur on the Gateway.

System Log

1. Set the Firewall Log state.

Display firewall logs: Enable Disable

2. Click Apply to save changes.

Apply

TIME	SYSTEM	ACTION
2016/02/26 17:01:38	Kernel event	eth0 (Ext switch port: 3) (Logical Port: 11) Link UP 1000 mbps full duplex
2016/02/26 17:02:42	Kernel event	eth6 (Ext switch port: 3) (Logical Port: 11) Link DOWN
2016/02/26 17:04:46	Kernel event	eth1 (Ext switch port: 2) (Logical Port: 10) Link UP 1000 mbps full duplex
2016/02/26 17:05:01	Kernel event	eth1 (Ext switch port: 2) (Logical Port: 10) Link DOWN
2016/02/26 17:09:39	Kernel event	eth0 (Ext switch port: 3) (Logical Port: 11) Link UP 1000 mbps full duplex
2016/02/26 17:12:37	System event	Ethernet client disconnected_ip(192.168.1.64), mac(60:16:1d:6b:38:a1)
2016/02/26 17:12:50	System event	Ethernet client connected_ip(192.168.1.64), mac(60:16:1d:6b:38:a1)
2016/02/26 17:13:31	Kernel event	eth0 (Ext switch port: 3) (Logical Port: 11) Link DOWN
2016/02/26 17:14:17	System event	802.11 client connected_ip(192.168.1.66), mac(D7:c6:3e:3d:96)
2016/02/26 17:17:26	Kernel event	eth6 (Ext switch port: 3) (Logical Port: 11) Link UP 1000 mbps full duplex
2016/02/26 17:18:93	System event	Ethernet client connected_ip(192.168.1.66), mac(00:24:68:82:95:6c)
2016/02/26 17:21:45	System event	Ethernet client disconnected_ip(192.168.1.64), mac(60:16:1d:6b:38:a1)
2016/02/26 17:22:92	System event	Ethernet client connected_ip(192.168.1.64), mac(60:16:1d:6b:38:a1)

Auto Refresh Every 1 Minute Manual Refresh Refresh

Save Log As

Configuring Wireless Settings

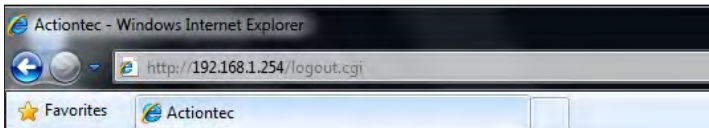
4

This chapter explains the options provided in the *Wireless Settings* section of the Gateway's firmware, including basic and advanced settings, and WPS.

Accessing Wireless Settings

To access the Wireless Settings screens:

1. Open a Web browser. In the *Address* text box, type:
<http://192.168.1.254>
then press **Enter** on the keyboard.

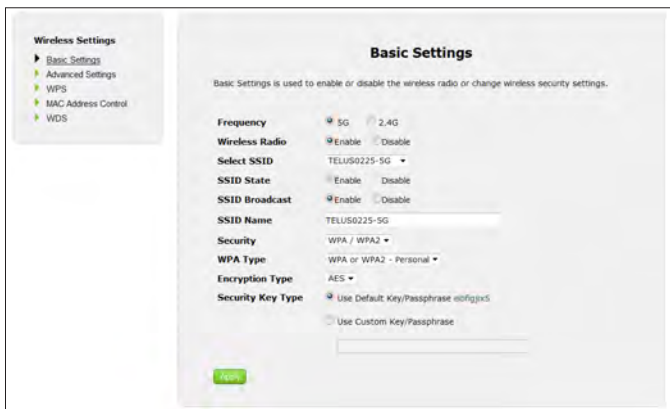


Telus T3200M Gateway

2. The Gateway's Main screen appears. Enter the user name and password, then click **Wireless Settings** from the row of icons at the top of the screen.



3. The *Wireless Status* screen appears, with a menu of other wireless options listed on the left side of the screen.



Basic Settings

Click **Basic Settings** from any *Wireless Settings* screen to generate the *Basic Settings* screen, as shown in the figure above. This screen displays a series of settings relating to the basic functionality of the Gateway's wireless network, including SSID (network name), frequency, and security.

Advanced Settings

Click **Advanced Settings** from any Wireless Settings screen to generate the *Advanced Settings* screen. This screen displays a series of settings relating to the advanced capabilities of the Gateway's wireless network, including compatibility mode, channel width, and WMM power save.

Advanced Settings

The modem supports high-speed wireless devices using the 802.11b/g/n protocol. Enable and tune 802.11b/g/n parameters as appropriate.

Frequency	<input checked="" type="radio"/> 5G <input type="radio"/> 2.4G
Compatibility Mode	5GHz (A,N,AC) ▾
Channel Width	80 MHz ▾
Control Channel	None ▾
MSDU Aggregation	MSDU Aggregation Disabled ▾
MPDU Aggregation	MPDU Aggregation Enabled ▾
WMM	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WMM Power Save	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel	Auto Detect ▾ <input type="button" value="Re-scan"/> Current Channel: 44
Wireless Power Level	100% ▾

WPS

Click **WPS** from any Wireless Settings screen to generate the *WPS (Wi-Fi Protected Setup)* screen, which allows the user to configure WPS by following the onscreen instructions.

WPS (Wi-Fi Protected Setup)

WPS provides an easy and secure way to establish a wireless network by sharing the wireless key between the modem and wireless client.

Frequency 5G 2.4G

1. Set the WPS state.

WPS: Enable Disable

2. Click Apply to save changes.

Connecting a device with WPS AP PIN

Current WPS AP PIN: **62052986**

Click Generate PIN to generate a new AP PIN:

Click Restore Default PIN to restore the default AP PIN:

Connecting a device with WPS PBC or End Device PIN

Push Button Configuration (PBC)

End Device PIN:

Insert End Device PIN:

Connect must be clicked within 120 seconds on client WPS device.

MAC Address Control

Click **MAC Address Control** from any Wireless Settings screen to generate the *Wireless MAC Authentication* screen, which allows the user to configure allow or deny access to the Gateway's wireless network using the MAC address of the wireless device. Follow the onscreen instructions to configure.

Wireless MAC Authentication

Limit access to the modem by using the MAC address of specific wireless devices.

Frequency 5G 2.4G

1. Select SSID from the pull down menu.
SSID: TELUS0225-5G ▾

2. Set MAC authentication state.
Mac Authentication: Enable Disable

3. Select Allow device list or Deny device list.

Allow device list: Denies all devices except those added in step 4.
 Deny device list: Allows all devices except those added in step 4.

4. Enter the MAC address of the wireless LAN device.

Select MAC Address: Manually Add MAC Address:
 or
(Sample MAC Address: 00:20:e0:00:41:00)

5. Click Apply to save changes.

MAC Authentication Device List

DEVICE NAME	IP ADDRESS	MAC ADDRESS	ACCESS	EDIT
No Entries Defined				

WDS

Click **WDS** from any Wireless Settings screen to generate the *WDS Wireless Distribution System* screen, which allows the user to configure the Gateway to allow wireless connections between access points. Follow the onscreen instructions to configure.

WDS Wireless Distribution System

WDS allows the wireless interconnection of access points via a wireless connection.

Frequency 5G 2.4G

1. Set the WDS main base station state.

WDS Main Base Station: Enable Disable

2. Click Apply to save your changes.

Configuring Firewall Settings

5

This chapter explains the options provided in the *Firewall* section of the Gateway's firmware, including setting up port forwarding and static NAT.

Accessing Firewall Settings

To access the Firewall screens:

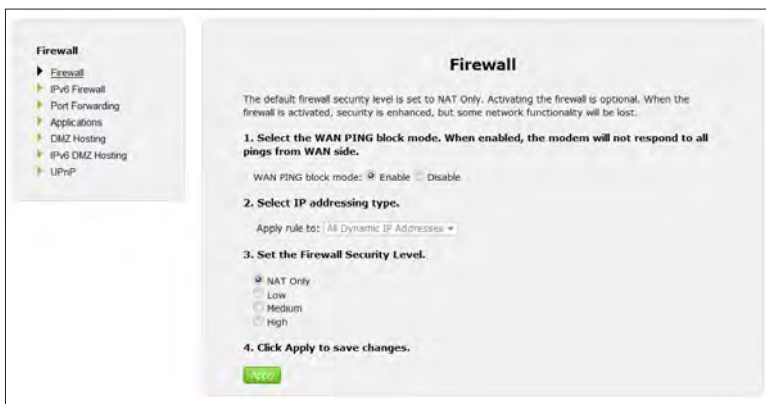
1. Open a Web browser. In the *Address* text box, type:
<http://192.168.1.254>
then press **Enter** on the keyboard.



The Gateway's Home screen appears. Click the *Firewall* icon.



2. The *Firewall* screen appears, with a menu of other wireless options listed on the left side of the screen.



Firewall

Click **General** from any Firewall Settings screen to generate the *Firewall* screen, as shown in the figure above. To set up, follow the onscreen instructions.

IPv6 Firewall

Click **IPv6 Firewall** from any Firewall Settings screen to generate the *IPv6 Firewall* screen. To set up, follow the onscreen instructions.

IPv6 Firewall

Activating the firewall is optional. When the firewall is activated, security is enhanced, but some network functionality may be lost.

1. Select the stealth mode state. When stealth mode is enabled, the modem will not respond to unsolicited WAN traffic, including pings..

Stealth Mode: Enable Disable

2. Select the IP address or IP addressing type to which the firewall rules will apply.

Addressing Type:

3. Set the Firewall Security Level.

Security Level:

[Create Rule](#)

4. Set the firewall table, below. Services checked are allowed. (optional)

Service	Service Type	Service Port	Traffic	Traffic
			In	Out
DirectX	Multimedia Control	2300 through 2400, 47824, 2300 through 2400 UDP, 6073 UDP	<input type="checkbox"/>	<input checked="" type="checkbox"/>
DNS	DNS	53	<input type="checkbox"/>	<input checked="" type="checkbox"/>
FTP	File Transfer	20, 21	<input type="checkbox"/>	<input checked="" type="checkbox"/>
FTPS	Secure File Transfer	990	<input type="checkbox"/>	<input checked="" type="checkbox"/>
H323	Video	1720	<input type="checkbox"/>	<input checked="" type="checkbox"/>
HTTP	Web Service	80	<input type="checkbox"/>	<input checked="" type="checkbox"/>
HTTPS	Secure Web Service	443	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ICMP Echo Request	Web Service	N/A	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ICMP Echo Reply	Web Service	N/A	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Port Forwarding

Click **Port Forwarding** from any Firewall screen to generate the *Port Forwarding* screen. Activating port forwarding allows the network to be exposed to the Internet in certain limited and controlled ways, enabling some applications to work from the local network (game, voice, and chat applications, for example), as well as allowing Internet access to servers in the local network. This screen allows you to configure the port forwarding settings of the Gateway. If changes are made in this screen, click **Apply** at the bottom of the screen to save them.

Port Forwarding

Enter ports or port ranges required to forward Internet applications to a LAN device below.

1. Set the LAN/WAN port and IP information.

Select LAN Device: Manually enter the IP address ▾

LAN IP Address:

External (WAN) Start Port:

External (WAN) End Port:

Internal (LAN) Start Port:

Internal (LAN) End Port:

Protocol: TCP ▾

2. Click Apply to save changes.

Applied Port Forwarding Rules

LAN START / END PORT	PROTOCOL	LAN IP ADDRESS	WAN START/END PORT	MODIFY	REMOVE
No Entries Defined					

Port forwarding settings should only be adjusted by experienced technical users who are extremely familiar with wireless networking concepts.

Applications

Click **Applications** from any Firewall screen to generate the *Applications* screen. This screen allows the user to designate certain applications to be forwarded, circumventing the usual firewall security settings. If changes are made in this screen, click **Apply** at the bottom of the screen to save them.

Applications

Applications forwards ports to the selected LAN device by application name.

1. Select Device.

Select Device: Enter IP Address:
Manually enter the IP address ▼

2. Select the application category, then the application to forward.

Application Category: ▼
Applications: ▼

3. Click Apply to save changes.

Forwarded Applications List:

DEVICE NAME	IP ADDRESS	APPLICATION FORWARDED	EDIT
No Entries Defined			

DMZ Hosting

Click **DMZ Hosting** from any Firewall screen to generate the *DMZ Hosting* screen. The DMZ host feature allows one device on the network to operate outside the firewall to use an Internet service that otherwise would be blocked, or to expose a networked device to all services without restriction or security. To activate, click in the *Enable* radio button, then enter the device's IP address in the appropriate text boxes.

DMZ Hosting

DMZ hosting enables a LAN device to use the modem's WAN IP address as its own. DMZ places the LAN device outside the firewall.

WARNING! Using a device in DMZ mode creates a security risk by exposing the device to outside intrusion.

1. Set the DMZ state.

DMZ: Enable Disable

2. Select a device.

Select Device: Enter IP Address:

3. Click Apply to save changes.

DMZ Hosted Device

DEVICE NAME	IP ADDRESS	EDIT
No Entries Defined		

Caution! A DMZ host is not protected by the firewall and may be vulnerable to attack. Designating a DMZ host may also put other computers in the local network at risk. When designating a DMZ host, consider the security implications and protect it if necessary.

IPv6 DMZ Hosting

Click **IPv6 DMZ Hosting** from any Firewall screen to generate the *IPv6 DMZ Hosting* screen. The DMZ host feature allows one device on the network to operate outside the firewall to use an Internet service that otherwise would be blocked, or to expose a networked device to all services without restriction or security. To activate, follow the onscreen instructions.

IPv6 DMZ Hosting

DMZ hosting enables a LAN device to use the modem's WAN IP address as its own. DMZ places the LAN device outside the firewall.

WARNING! Using a device in DMZ mode creates a security risk by exposing the device to outside intrusion.

1. Enter an IPv6 Address.

Enter The last 64 bits of IPv6 Address:

2. Click Apply to save changes.

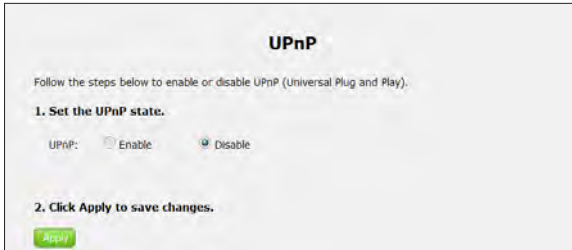
IPv6 DMZ Hosted Device

IP ADDRESS	EDIT
No Entries Defined	

Caution! A DMZ host is not protected by the firewall and may be vulnerable to attack. Designating a DMZ host may also put other computers in the local network at risk. When designating a DMZ host, consider the security implications and protect it if necessary.

UPnP

Click **UPnP** from any Firewall screen to generate the *UPnP* screen, which activates UPnP (Universal Plug and Play). To activate, click in the *Enable* radio button, then click **Apply**.



The screenshot shows a web interface for configuring UPnP. At the top, the title "UPnP" is centered. Below it, a line of text reads "Follow the steps below to enable or disable UPnP (Universal Plug and Play)." The first step is "1. Set the UPnP state." Underneath, the label "UPnP:" is followed by two radio buttons: "Enable" (which is currently selected) and "Disable". The second step is "2. Click Apply to save changes." At the bottom left, there is a green button labeled "Apply".

Advanced Settings

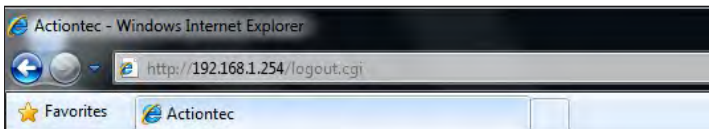
6

This chapter explains the options available with the Advanced Setup screens, which configure some of the more complex settings on the Gateway.

Accessing the Advanced Setup Screens

To access the Gateway's Advanced Setup screens:

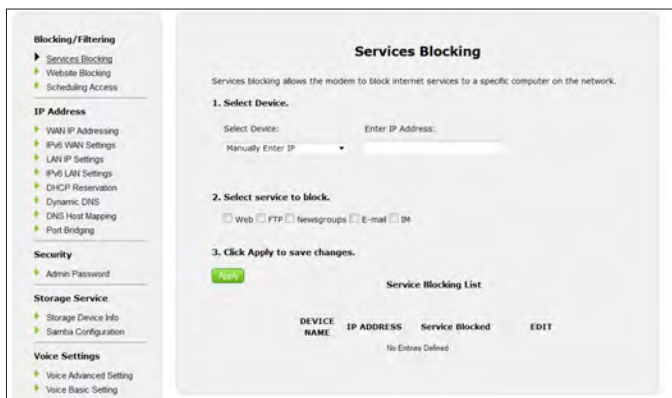
1. Open a Web browser. In the *Address* text box, type:
<http://192.168.1.254>
then press **Enter** on the keyboard.



2. The Gateway's Main screen appears. Click the *Advanced Setup* icon.



3. The *Services Blocking* screen appears.



From here, all the Advanced Setup screens can be accessed from the menu on the left.

Services Blocking

Click **Services Blocking** from any Advanced Setup screen to generate the *Services Blocking* screen (see the figure, above). This feature allows the user to block certain services from accessing the Gateway's network(s). Follow the onscreen instructions to configure.

Website Blocking

Click **Website Blocking** from any Advanced Setup screen to generate the *Website Blocking* screen. This feature allows the user to block certain websites from accessing the Gateway's network(s). Follow the onscreen instructions to configure.

The screenshot shows the 'Website Blocking' configuration interface. At the top, the title 'Website Blocking' is centered. Below it, the section 'Website Blocking' contains two numbered instructions: '1. To block a specific website, enter the website address (such as www.abcd.com) in the text box below.' and '2. Click Apply to save changes.' A text input field labeled 'Website Address:' is positioned below the first instruction. A green 'Apply' button is located below the second instruction. At the bottom of the screen, there is a section titled 'Blocked Websites' which contains a table with two columns: 'Website Blocked' and 'EDIT'. The table is currently empty, with the text 'No Entries Defined' centered below the columns.

Scheduling Access

Click **Scheduling Access** from any Advanced Setup screen to generate the *Scheduling Access* screen. This feature allows the user to schedule access to the Gateway's network(s) for certain devices. Follow the onscreen instructions to configure.

The screenshot shows the 'Scheduling Access' configuration interface. At the top, the title 'Scheduling Access' is centered. Below it, the text 'Schedule Rules allows the modem to set a specific time period during which a computer on the network can access the Internet.' is displayed. The section '1. Select Device.' contains two input fields: 'Select Device:' with a dropdown menu set to 'Manually enter the MAC Address' and 'Enter MAC Address:' with a text input field. The section '2. Select the days of the week to allow Internet access.' includes the instruction 'A checked box signifies access allowed.' and a row of seven checkboxes for the days of the week: SUN, MON, TUE, WED, THU, FRI, and SAT. The section '3. Select the time of day range from the drop-down list.' contains two dropdown menus: 'From: 12:00 PM' and 'To: 12:00 PM'.

WAN IP Addressing

Click **WAN IP Addressing** from any Advanced Setup screen to generate the *WAN IP Address* screen. This feature allows the user to set the protocol used by the ISP for Internet access. Follow the onscreen instructions to configure.

WAN IP Address

WAN IP Addressing sets the protocol used by your ISP for Internet access.

- 1. Current WAN interface is WAN Ethernet.**
- 2. Select the ISP protocol below.**
 - PPPoE
 - RFC 1483 via DHCP
 - RFC 1483 via Static IP
- 3. If your ISP Provider requires Host Name/Domain Name, enter it here.**

Host Name	home
Domain Name	telus
- 4. Select the DNS type.**
 - Dynamic DNS Addresses (Default)
 - Static DNS Addresses

Primary DNS:	Not Applicable
Secondary DNS:	Not Applicable
- 5. Configure IGMP Proxy.**
 - Enable
 - Disable
- 6. Click Apply to save changes.**

IPv6 WAN Settings

Click **IPv6 WAN Settings** from any Advanced Setup screen to generate the *IPv6 WAN Settings* screen. This feature allows the user to set the IPv6 protocol used by the ISP for Internet access. Follow the onscreen instructions to configure.

The screenshot shows the 'IPv6 WAN Settings' configuration page. At the top, it states 'IPv6 is the next generation of IP addressing.' Below this, there are five numbered steps for configuration:

- 1. Set the IPv6 state.**
IPv6: Enable Disable
- 2. Select the WAN IPv6 connection protocol.**
WAN IPv6 IP Protocol: DHCPv6 ▾
- 3. Set the WAN IPv6 Addressing Type.**
Request PD Only: Yes No
- 4. Set the WAN IPv6 DNS Server.**
IPv6 DNS Type: Default Servers Custom Servers
- 5. Click Apply to save changes.**

At the bottom left, there is a green 'Apply' button.

LAN IP Settings

Click **LAN IP Settings** from any Advanced Setup screen to generate the *LAN IP and DHCP Settings* screen. This feature allows the user to set LAN IP and DHCP server settings on the Gateway. Follow the onscreen instructions to configure.

LAN IP And DHCP Settings

Actiontec recommends that you keep the current default LAN IP address of the modem. Any changes made to the LAN IP address will reset some of the other settings on the modem. Do not proceed without understanding the technical impact of changing these settings.

1. To make changes, enter the new IP address or Subnet Mask of the modem in the field below.

Modem IP Address:	<input type="text" value="192.168.1.254"/>
Modem Subnet Mask:	<input type="text" value="255.255.255.0"/>

2. Click Apply and Reboot to save your changes.

The modem will automatically assign an IP address to each device in your network.

1. Set the IP addressing values.

Beginning IP Address:	<input type="text" value="192.168.1.64"/>
Ending IP Address:	<input type="text" value="192.168.1.253"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>

2. Set the DHCP server lease time.

DHCP Server Lease Time:	<input type="text" value="1"/> Day(s)	<input type="text" value="0"/> Hours	<input type="text" value="0"/> Minutes
-------------------------	---------------------------------------	--------------------------------------	--

IPv6 LAN Settings

Click **IPv6 LAN Settings** from any Advanced Setup screen to generate the *IPv6 LAN Settings* screen. This feature allows the user to set the IPv6 LAN IP settings on the Gateway. Follow the onscreen instructions to configure.

The screenshot shows the 'IPv6 LAN Settings' configuration page. At the top, it states 'IPv6 is the next generation of IP addressing.' Below this, there are three numbered steps: 1. 'Set the IPv6 LAN connection type.' with a dropdown menu set to 'Stateless'. 2. 'Set the IPv6 LAN addressing values.' with fields for 'Prefix Length', 'Link-Local Address' (fe80::72f1:96ff:fe07:e00), 'ULA Support' (radio buttons for 'Enable' and 'Disable', with 'Disable' selected), 'Subnet Number' (0), and 'Router Advertisement Lifetime' (30 Minute(s) (0 - 150)). 3. 'Click Apply to save changes.' with a green 'Apply' button at the bottom left.

DHCP Reservation

Click **DHCP Reservation** from any Advanced Setup screen to generate the *DHCP Reservation* screen. This feature allows the user to lease a permanent DHCP-allocated address to a client on the Gateway's network. Follow the onscreen instructions to configure.

The screenshot shows the 'DHCP Reservation' configuration page. It starts with the text 'DHCP reservation leases a permanent DHCP allocated address to a client.' followed by three numbered steps: 1. 'Select MAC Address, or manually enter a MAC address.' with a dropdown menu set to 'Manually enter the MAC Add' and an empty text input field below it. 2. 'Select an IP address to associate with a MAC address.' with a dropdown menu set to 'Manually enter the IP address' and an empty text input field below it. 3. 'Click Apply to save changes.' with a green 'Apply' button at the bottom left.

Dynamic DNS

Click **Dynamic DNS** from any Advanced Setup screen to generate the *Dynamic DNS* screen. This feature allows the user to associate the WAN IP address of the Gateway with a host name. Follow the onscreen instructions to configure.

Dynamic DNS

Dynamic DNS associates the WAN IP address of your modem with a host name. Dynamic DNS automatically updates DNS servers upon WAN IP address change.

1. Set the dynamic DNS state.

Dynamic DNS State: Enable Disable

2. Select the dynamic DNS provider.

Dynamic DNS provider:

3. Enter your username and password.

Username:

Password:

4. Enter the dynamic DNS host name.

Hostname:

5. Click Apply to save changes.

DNS Host Mapping

Click **DNS Host Mapping** from any Advanced Setup screen to generate the *Dynamic DNS* screen. This feature allows the user to create a static host name for a specified IP address. Follow the onscreen instructions to configure.

DNS Host Mapping

DNS host mapping creates a static host name for the specified IP address. WAN and LAN IP addresses are supported.

1. Enter the DNS host name.

DNS Host Name:

2. Enter the IP address.

IP Address:

3. Click Apply to save changes.

DNS Host Mapping List

DEVICE NAME	IP ADDRESS	DNS NAME	EDIT
No Entries Defined			

Port Bridging

Click **Port Bridging** from any Advanced Setup screen to generate the *Port Bridging* screen. This feature allows the user to create a port bridge on the Gateway. Follow the onscreen instructions to configure.

Port1 Bridge

1. Set the Port1 Bridge state.

Port1 Bridge: Enable Disable

2. Click Apply to save changes.

Admin Password

Click **Admin Password** from any Advanced Setup screen to generate the *Admin Password* screen. This feature allows the user to change the password for accessing the Gateway's graphical user interface. Follow the onscreen instructions to configure.

Admin Password

A strong password prevents outsiders from accessing the modem's web interface.
You will need to enter this password every time you access the modem's web interface.

1. Enter the old and new passwords.

Username:

Old Password:

New Password:

Confirm your password:

2. Click Apply to save changes.

Storage Device Info

Click **Storage Device Info** from any Advanced Setup screen to generate the *Storage Service* screen. This feature allows storage devices connected to the Gateway to be easily accessed. Any storage devices connected to the Gateway will be listed in the table at the bottom of the screen.

Storage Service

The Storage service allows storage devices connected to the modem to be more easily accessed.

Volumename	FileSystem	Total Space	Used Space
No Storage Device Found			

Samba Configuration

Click **Samba Configuration** from any Advanced Setup screen to generate the *Samba Configuration* screen. This feature allows the user to set up a Samba environment. Follow the onscreen instructions to configure.

Samba Configuration

File Sharing: Enable Disable

Samba Username: admin

Samba Password: *****

Device Name: [dropdown menu]

Workgroup: WORKGROUP

Voice Advanced Setting

Click **Voice Advanced Setting** from any Advanced Setup screen to generate the *Service VoIP - Advanced* screen. This feature allows the user to configure advanced VoIP settings on the Gateway. Follow the onscreen instructions to configure.

Service VoIP - Advanced

Global parameters: **Service Provider 0**

NOTE: For CallCtrl 1.10.x, this page displays activation status for each feature.
For CCTK 2.x, this page displays enable status for each feature, not configurable from keypad.

Enabled SIP Call Features	Account 0	Account 1	Activation Instructions
Call waiting	<input checked="" type="checkbox"/>	<input type="checkbox"/>	When enabled, dial *61 to activate, *60 to deactivate
Call forwarding number	<input type="text"/>	<input type="text"/>	
Forward unconditionally	<input checked="" type="checkbox"/>	<input type="checkbox"/>	When enabled, dial *71 to activate, *75 to deactivate
Forward on "busy"	<input checked="" type="checkbox"/>	<input type="checkbox"/>	When enabled, dial *71 to activate, *75 to deactivate
Forward on "no answer"	<input checked="" type="checkbox"/>	<input type="checkbox"/>	When enabled, dial *71 to activate, *75 to deactivate
MWI	<input type="checkbox"/>	<input type="checkbox"/>	
Call barring	<input checked="" type="checkbox"/>	<input type="checkbox"/>	When enabled, dial *85(PH)0*85(PH)1*85(PH)2 to deactivate/activate/activate per digitmap
Call barring pin	9999	<input type="text"/>	
Call barring digit map	<input type="text"/>	<input type="text"/>	
Warm line	<input checked="" type="checkbox"/>	<input type="checkbox"/>	When enabled, dial *70 to activate, *79 to deactivate
Warm line number	<input type="text"/>	<input type="text"/>	

Voice Basic Setting

Click **Voice Basic Setting** from any Advanced Setup screen to generate the *Service VoIP - Basic* screen. This feature allows the user to configure basic VoIP settings on the Gateway. Follow the onscreen instructions to configure.

Service VoIP - Basic

Global parameters | **Service Provider 0**

Enter the SIP parameters and click Start/Stop to save the parameters and start/stop the voice application.

Locale selection*: USA - NORTHAMERICA
(Note: Requires the SIP client to be stopped and then started to take affect.)

SIP domain name*:

Voip Dialplan Setting:

Use SIP Proxy.
SIP Proxy:
SIP Proxy port: 5060

Use SIP Outbound Proxy.
SIP Outbound Proxy:
SIP Outbound Proxy port: 5060

Use SIP Registrar.
SIP Registrar:
SIP Registrar port: 5060

Voice Debug Setting

Click **Voice Debug Setting** from any Advanced Setup screen to generate the *Service VoIP - Debug* screen. This feature allows the user to configure VoIP debug settings on the Gateway. Follow the onscreen instructions to configure.



The screenshot shows the 'Service VoIP - Debug' configuration page. At the top, it says 'Global parameters: Service Provider 0'. Below this, there are input fields for 'SIP log server IP Address*' and 'SIP log server port*'. The port is set to '0'. There are also dropdown menus for 'Line' (1 and 2), 'VAD support' (checked), 'Ingress gain' (0), and 'Egress gain' (0). At the bottom, there are three buttons: 'Start SIP Calls', 'Stop SIP Calls', and 'Apply'. A note at the bottom states: '* Changing this parameter for one service provider affects all other service providers.'

Reboot

Click **Reboot** from any Advanced Setup screen to generate the *Reboot* screen. Reboot the Gateway by clicking **Reboot**.



The screenshot shows the 'Reboot Modem' screen. It contains the text 'To reboot the modem, click Reboot..' and a button labeled 'Reboot Modem: Reboot'.

Restore Defaults

Click **Restore Defaults** from any Advanced Setup screen to generate the *Restore Defaults* screen. To restore certain settings on the Gateway, click the appropriate *Restore* button.



Check for New Firmware

Click **Check for New Firmware Link** from any Advanced Setup screen to generate the *Upgrade Firmware from Internet* screen. Follow the onscreen instructions to upgrade the firmware on the Gateway.



Speed Test

Click **Speed Test** from any Advanced Setup screen to generate the *Speed Test* screen. This screen allows the user to perform a speed test on the Gateway's Internet (or WAN) connection. Enter the URL for a speed test site, then click **Test**.

The screenshot shows the 'Speed Test' interface. At the top, it says 'Speed Test' and '1. Click "Test" to begin the speed test.' Below this is a text input field for the URL and a green 'Test' button. A table titled 'Speed Test Results' is displayed below the input field. The table has two columns: 'Test' and 'Results'. The 'Test' column lists various metrics, and the 'Results' column shows the corresponding values. The status 'NO TEST IN PROGRESS' is displayed in the Results column.

Test	Results
Train Rate Downstream:	1000Mbps
Train Rate Upstream:	1000Mbps
Test Status:	NO TEST IN PROGRESS
Average Downstream:	N/A
Average Upstream:	N/A
Ping Time:	N/A
MTU Size:	1500
MSS Size:	1460
TCP Connection:	Yes
RWIN Size:	87380
Do Not Fragment Bit:	Enabled

Ping Test

Click **Ping Test** from any Advanced Setup screen to generate the *Ping Test* screen. To perform a ping test on the Gateway, follow the onscreen instructions.

Ping Test

Test your Internet connectivity to a specific host using the ping test, below.

1. Insert a URL or IP address below.

URL or IP:

2. Select the packet size.

Packet Size (Bytes):

3. Select test.

Test Status
No Test in Progress

Ping Test Results:

REPLY FROM	BYTES	TIME	TTL
N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A

Ping Statistics:

PACKETS SENT	PACKETS RECEIVED	PACKETS LOSS	ROUND TRIP MIN	ROUND TRIP MAX	ROUND TRIP AVG
N/A	N/A	N/A	N/A	N/A	N/A

Tcpdump Debug

Click **Tcpdump Debug** from any Advanced Setup screen to generate the *Tcpdump Debug* screen. To perform a tcpdump debug on the Gateway, follow the onscreen instructions.

Tcpdump Debug

TCPDump will copy the packet capture (.pcap) file to the USB flash connected to the modem. Also, the CFE and wireless configuration files will be copied to the USB flash.

1. Select the interface to debug.

TCPDump Interface:

2. Select the packet size to dump.

Packet Size:

3. Select the filename of dump file stored in the USB Flash.

File Name:

4. Select the duration of Dump.

TCPDump Timeout(Seconds):

Test Status
No USB Flash is inserted
No TCPDump is in Progress

Iperf Test

Click **Iperf Test** from any Advanced Setup screen to generate the *Iperf Test* screen. To perform an iperf test on the Gateway, follow the onscreen instructions.

Iperf Test

Test your network situation for interface, below.

1. Select iperf Mode.

Client

2. Select port to listen or connect to.

port:

3. Select Report interval.

report interval: Seconds

4. Select protocol.

Protocol:

window size: Bytes

5. Select transmit options.

Transmit Bytes Bytes

Transmit Time Seconds

6. Host.

URL or IP:

IPv6 Ping Test

Click **IPv6 Ping Test** from any Advanced Setup screen to generate the *IPv6 PingTest* screen. To perform an IPv6 ping test on the Gateway, follow the onscreen instructions.

IPv6 Ping Test

Test the Modem's Internet connectivity to a specific host using the Ping Test, below.

1. Insert a URL or IP address below.

URL or IP:

2. Select the interface.

Interface Name:

3. Select the packet size.

Packet size (bytes):

4. Select test.

Ping test results

Reply From	Bytes	Time	TTL
N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A

Ping Statistics

Packets Sent	Packets Received	Packet Loss	Round Trip Minimum	Round Trip Maximum	Round Trip Average
N/A	N/A	N/A	N/A	N/A	N/A

Traceroute

Click **Traceroute** from any Advanced Setup screen to generate the *Traceroute* screen. To perform an route trace on the Gateway, follow the onscreen instructions.

Traceroute

Traceroute is used to determine the route taken by packets across a network.

1. Insert a URL or IP Address below.

URL or IP:

2. Select test.

Test Status
No Test in Progress

Traceroute Results:

Hop	Time 1	Time 2	Time 3	Host / IP Address
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A

IPv6 Traceroute

Click **IPv6 Traceroute** from any Advanced Setup screen to generate the *IPv6 Traceroute* screen. To perform an IPv6 route trace on the Gateway, follow the onscreen instructions.

IPv6 Traceroute

Traceroute is used to determine the route taken by packets across a network.

1. Enter a URL or IP address in the text box, below.

URL or IP:

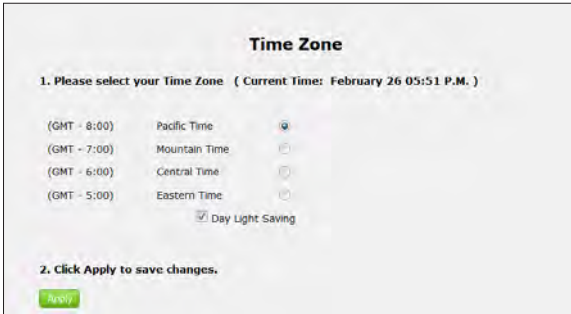
2. Select test.

Traceroute Results

Hop	Time 1	Time 2	Time 3	Host / IP Address
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A

Time Zone

Click **Time Zone** from any Advanced Setup screen to generate the *Time Zone* screen. Use this screen to set the time zone on the Gateway.



The screenshot shows a web interface titled "Time Zone". At the top, it says "1. Please select your Time Zone (Current Time: February 26 05:51 P.M.)". Below this, there are four radio button options: "Pacific Time" (GMT - 8:00), "Mountain Time" (GMT - 7:00), "Central Time" (GMT - 6:00), and "Eastern Time" (GMT - 5:00). The "Pacific Time" option is selected. There is also a checked checkbox for "Day Light Saving". At the bottom, it says "2. Click Apply to save changes." and there is a green "Apply" button.

Language Settings

Click **Language Settings** from any Advanced Setup screen to generate the *Language Settings* screen. Use this screen to set the language on the Gateway's graphical user interface.



The screenshot shows a web interface titled "Language Settings". It says "1. Select your preferred language" followed by a dropdown menu currently set to "Auto-detect". Below that, it says "2. Click Apply to save changes." and there is a green "Apply" button.

DNS Cache

Click **DNS Cache** from any Advanced Setup screen to generate the *DNS Cache* screen. Use this screen to set up a DNS cache on the Gateway.

DNS Cache

The modem provides DNS Caching ability. In most cases, DNS Caching allows a DNS Server to respond more quickly to multiple queries for the same domain or host.

Note: Although DNS Caching can resolve an Internet request more quickly, it also poses risks, such as DNS Poisoning.

1. Select Disable or Enable DNS Cache.

Disable (Recommended)

Enable

2. Click Apply to save changes.

IGMP Setting

Click **IGMP Setting** from any Advanced Setup screen to generate the *IGMP Setting* screen. Use this screen to set up IGMP processes on the Gateway.

IGMP Configuration

IGMP Snooping

IGMP Snooping Enable:

Standard Mode:

Blocking Mode:

IGMP Protocol

Default Version: version 2

Query Interval: 40

Query Response Interval: 10

Last Member Query Interval: 1

Robustness Value: 4

Maximum Multicast Groups: 128

Maximum Multicast Data Sources (for IGMPv3): 128

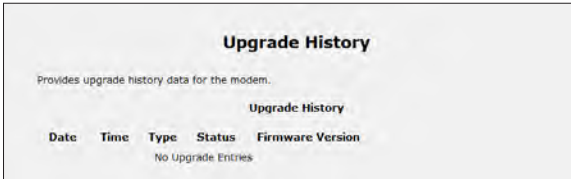
Maximum Multicast Group Members: 128

Fast Leave Enable:

LAN to LAN (Intra LAN) Multicast Enable:

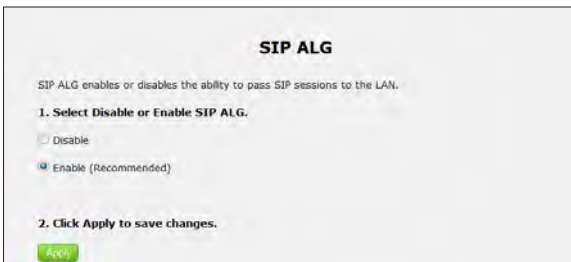
Upgrade History

Click **Upgrade History** from any Advanced Setup screen to generate the *Upgrade History* screen. This screen displays a list of firmware upgrades applied to the Gateway.



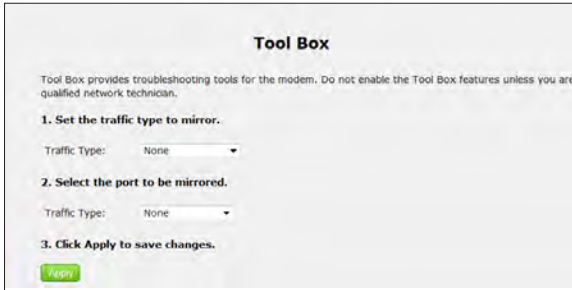
SIP ALG

Click **SIP ALG** from any Advanced Setup screen to generate the *SIP ALG* screen. This screen allows the user to configure SIP ALG on the Gateway.



Tool Box

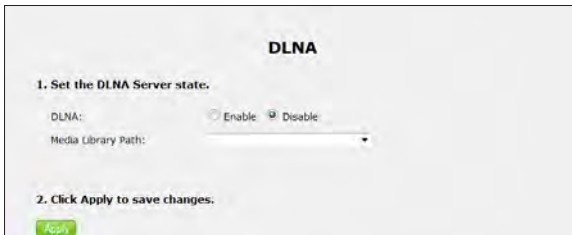
Click **Tool Box** from any Advanced Setup screen to generate the *Tool Box* screen. This screen allows the user to configure traffic and port mirroring on the Gateway.



The screenshot shows the 'Tool Box' configuration screen. At the top, the title 'Tool Box' is centered. Below the title, a paragraph of text reads: 'Tool Box provides troubleshooting tools for the modem. Do not enable the Tool Box features unless you are a qualified network technician.' There are three numbered steps: 1. 'Set the traffic type to mirror.' with a dropdown menu showing 'None'. 2. 'Select the port to be mirrored.' with a dropdown menu showing 'None'. 3. 'Click Apply to save changes.' with a green 'Apply' button at the bottom left.

DLNA

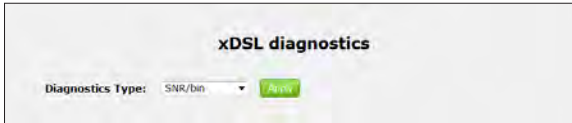
Click **DLNA** from any Advanced Setup screen to generate the *DLNA* screen. This screen allows the user to configure DLNA settings on the Gateway.



The screenshot shows the 'DLNA' configuration screen. At the top, the title 'DLNA' is centered. Below the title, there is a section '1. Set the DLNA Server state.' containing a 'DLNA:' label, two radio buttons for 'Enable' and 'Disable' (with 'Disable' selected), and a 'Media Library Path:' label with a dropdown menu. Below this is section '2. Click Apply to save changes.' with a green 'Apply' button at the bottom left.

xDSL Diagnostics

Click **xDSL diagnostics** from any Advanced Setup screen to generate the *DLNA* screen. This screen allows the user to select a type of diagnostics on the Gateway.



User's Manual

Click **xDSL diagnostics** from any Advanced Setup screen to view the Gateway's user manual.

Specifications



General

Model Number(s)

T3200M (Wireless 11ac Bonded VDSL2 Modem Gateway with MoCA 2.0)

Standards

IEEE 802.3 (10BaseT)
IEEE 802.3u (100BaseTX)
IEEE 802.11 b, g, n (Wireless)
G.dmt
G.lite
t1.413
RFC 1483, 2364, 2516

Protocol

LAN - CSMA/CD
WAN - PPP, DHCP, Static IP

WAN

VDSL2 interface

LAN

10/100/1000 RJ-45 switched ports

Speed

LAN Ethernet: 10/100/1000 Mbps auto-sensing
Wireless: 802.11n 300 Mbps optimal (see Wireless Operating Range for details)

Cabling Type

Ethernet 10BaseT: UTP/STP Category 3 or 5
Ethernet100BaseTX: UTP/STP Category 5

Wireless Operating Range

Indoors

Up to 91M (300 ft.) @ 300 Mbps

Outdoors

Up to 457M (1500 ft.) @ 300 Mbps

Topology

Star (Ethernet)

LED Indicators

WAN, Wireless, and WPS Push Button

Power Adapter

This device is supplied with one of two power adapters:

Adapter 1

Model No. - NBS40C120300VU

Input - 100-240V~, 50/60Hz, 1.0A

Output - 12.0V === 3.0A

Manufacturer - NetBit

Adapter 2

Model No. - CDS036-W120U

Input - 100-240V~, 50/60Hz, 1.0A

Output - 12.0V === 3.0A

Manufacturer - Actiontec

Environmental

Power

External, 12V DC, 3 A

Certifications

FCC Class B, FCC Class C (part 15, 68), CE Mark Commercial, UL

Operating Temperature

0° C to 45° C (32°F to 113°F)

Storage Temperature

-20°C to 70°C (-4°F to 158°F)

Operating Humidity

10% to 85% non-condensing

Storage Humidity

5% to 90% non-condensing

Notices

Warranty

This product has a one-year Limited Hardware Warranty and 90-day free software updates from date of purchase.

Local Law

This Limited Warranty Statement gives the customer specific legal rights. The customer may also have other rights, which vary from state to state in the United States, and from country to country elsewhere in the world.

To the extent that this Limited Warranty Statement is inconsistent with local law, this Statement shall be deemed modified to be consistent with such local law. Under such local law, certain disclaimers and limitations of this Warranty Statement may not apply to the customer.

Go to <http://www.actiontec.com/products/warranty.php> for more information.

Important Safety Instructions

Basic safety precautions should always be followed to reduce the risk of fire, electrical shock, and personal injury, including the following:

- Do not use this product near water – for example, near a bathtub, kitchen sink, laundry tub, or swimming pool, or in a wet basement; only clean with dry cloth.
- Do not block any ventilation openings. Install in accordance with the manufacturer's instructions. Do not install near any heat sources such as radiators, heat registers, stoves, or other apparatus including amplifiers that produce heat.
- Do not use the telephone to report a gas leak in the vicinity of the leak.
- Use only the power cord indicated in this manual.

Coaxial Cable

If applicable, the coaxial cable screen shield needs to be connected to the Earth at the building entrance per ANSI/NFPA 70, the National Electrical Code (NEC), in particular Section 820.93, “Grounding of Outer Conductive Shield of a Coaxial Cable,” or in accordance with local regulation.

FCC Class B Equipment

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference by implementing one or more of the following measures:

- Reorient or relocate the device;
- Increase the separation between the equipment and receiver;
- Consult the dealer or an experienced radio or television technician for help.

Modifications

The FCC requires the user to be notified that any changes or modifications made to this device that are not expressly approved by Actiontec Electronics, Inc, may void the user’s authority to operate the equipment.

Declaration of Conformity for Products Marked With the FCC Logo

This device complies with part 15 of the FCC. Operation is subject to the following two conditions:

1. This device may not cause harmful interference;
2. This device must accept any interference received, including interference that may cause undesired operation of the device.

Important Note on Wi-Fi

If applicable, this equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

The radio has been found to be compliant to the requirements set forth in CFR 47 Sections 2.1091, 15.247 (b) (4), 15.407 addressing RF Exposure from radio frequency devices as defined in Evaluating Compliance with FCC Guidelines for Human Exposure to Radio Frequency Electromagnetic Fields. The equipment should be installed more than 30 cm (~12 in.) from your body or nearby persons.

For product available in the USA market, only channel 1~11 can be operated. Selection of other channels is not possible.

The device could automatically discontinue transmission in case of absence of information to transmit, or operational failure. Note that this is not intended to prohibit transmission of control or signaling information or the use of repetitive codes where required by the technology.

The device for the band 5150-5250 MHz is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems.

The maximum antenna gain permitted for devices in the band 5725-5825 MHz shall comp with the e.i.r.p. limits specified for point-to-point and non point-to-point operation as appropriate.

The transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Contact Info

For questions regarding your product or the FCC declaration, contact:

Actiontec Electronics, Inc

760 North Mary Avenue, Sunnyvale, CA 94085, United States

Tel: (408) 752-7700

Fax: (408) 541-9003