Actiontec®

WiFi 6 Gateway Router with Bonded VDSL

Model # T3280

User Manual

Table of Contents

Introduction 1

Congratulations on purchasing the T3280 Wireless 11ax Bonded VDSL2 Modem Gateway. The Gateway is a single platform device that supports universal WAN access, FTTN, FTTdp, FTTB, or FTTP. With support for advanced 802.11ax 4x4 WiFi, 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 3.55 Gbps.

Package Contents

- Black Power adapter
- Yellow cable (Ethernet, 6 ft.)
- White cable (Ethernet, 10 ft.)
- 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, WAN Ethernet and Fiber in a single CPE
- Dual Band WiFi delivering up to 3.55 Gbps with 802.11ax 4x4 5GHz and 802.11ax 3x3 2.4GHz
- Optimized for IPTV and Video over WiFi

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 12 LEDs, and a WPS (Wireless Protected Setup) button.

Power
The Power LED brights green when the unit is powered up.

DSL 1
The DSL 1 LED brights green when the DSL 1 is synchronized.

DSL 2
The DSL 2 LED brights green when the DSL 2 is synchronized.

Internet
The Internet LED illuminates green when the Gateway is properly connected to a WAN Internet connection.WAN/LANThis LED brights green when there is an active Ethernet cable connected to the WAN port, and it blinks with traffic activity.

Ethernet 1
This LED brights green when there is an active Ethernet cable connected to the LAN port #1, and it blinks with traffic activity.

Ethernet 2
This LED brights green when there is an active Ethernet cable connected to the LAN port #2, and it blinks with traffic activity.

Ethernet 3
This LED brights green when there is an active Ethernet cable connected to the LAN port #3, and it blinks with traffic activity.

Ethernet 4
This LED brights green when there is an active Ethernet cable connected to the LAN port #4, and it blinks with traffic activity.

USB

This LED brights green when there is an active device connected to the USB port.

Wi-Fi 2.4G

This LED brights green when the Gateway's radio is operating in the 2.4GHz band.

Wi-Fi 5G

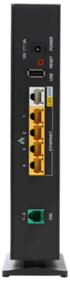
This LED brights green when the Gateway's radio is operating in the 5GHz band.

WPS Button

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

Rear Panel

The rear panel of the Gateway features 8 ports, and a Reset button.



Power Port

The Power port is used to connect the Power cord (Model No. CDS024T-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.

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

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 Port

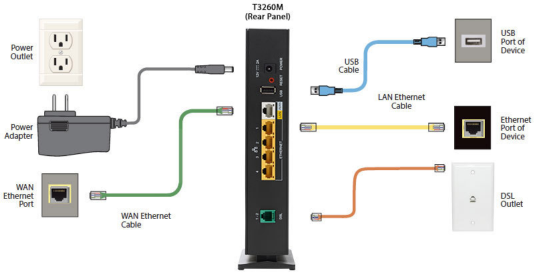
The USB port is used to connect the Gateway to a USB device.

DSL Port

The DSL port is used to connect the Gateway to a DSL wall outlet via DSL cable.

Connecting the Gateway

There are many variables involved when connecting the Gateway, depending on the type of Internet service available. The figure below shows 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. Plug the yellow Ethernet cable from the box into one of the four yellow Ethernet ports on the back of the Gateway.
4. Make sure the computer is powered on, then plug the other end of the yellow Ethernet cable into an Ethernet port on the computer.
5. Make sure that the LED on the LAN port into which the Ethernet cable is plugged glows steadily green. This may take a few moments.
6. 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.

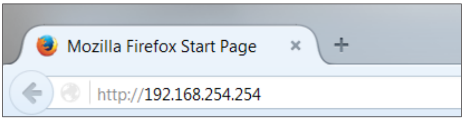
Accessing the Home Screen 2

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

Accessing the Home Screen

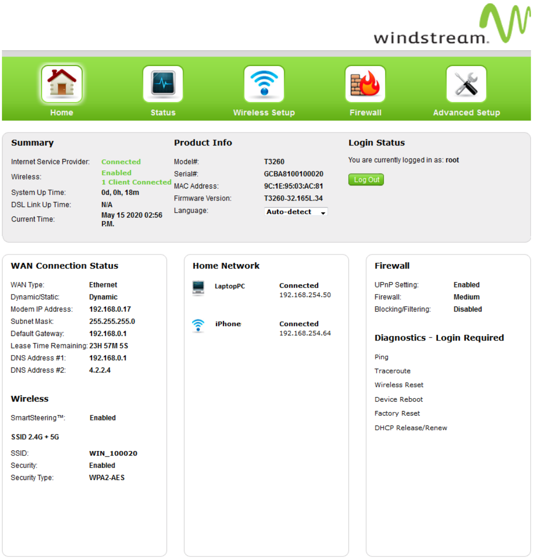
To access the Home screen:

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://192.168.254.254
   then press **Enter** on the keyboard.



http://192.168.254.254

2. The Gateway's Home screen appears.



Summary

Internet Service Provider:	Connected
Wireless:	Enabled 1 Client Connected
System Up Time:	0d, 0h, 18m
DSL Link Up Time:	N/A
Current Time:	May 15 2020 02:56 P.M.

Product Info

Model#:	T3260
Serial#:	GCBA8100100020
MAC Address:	9C:1E:95:03:AC:81
Firmware Version:	T3260-32.165L.34
Language:	Auto-detect

Login Status

You are currently logged in as: root

Log Out

WAN Connection Status

WAN Type:	Ethernet
Dynamic/Static:	Dynamic
Modem IP Address:	192.168.0.17
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.0.1
Lease Time Remaining:	23H 57M 5S
DNS Address #1:	192.168.0.1
DNS Address #2:	4.2.2.4

Wireless

SmartSteering™:	Enabled

SSID 2.4G + 5G

SSID:	WIN_100020
Security:	Enabled
Security Type:	WPA2-AES

Home Network

LaptopPC	Connected 192.168.254.50
iPhone	Connected 192.168.254.64

Firewall

UPnP Setting:	Enabled
Firewall:	Medium
Blocking/Filtering:	Disabled

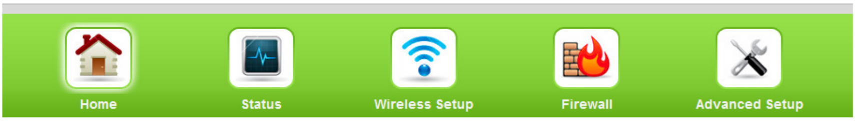
Diagnostics - Login Required

Ping
Traceroute
Wireless Reset
Device Reboot
Factory Reset
DHCP Release/Renew

The Gateway's GUI is now accessible.

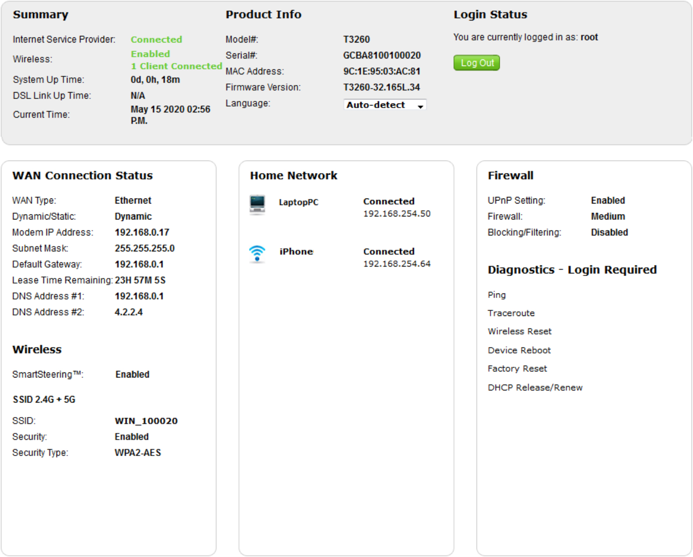
Icon Bar

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 3 for more details); Wireless Setup (see chapter 4 for more details); Firewall (see chapter 5 for more details); Advanced Setup (see chapter 6 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:	Connected
Wireless:	Enabled 1 Client Connected
System Up Time:	0d, 0h, 18m
DSL Link Up Time:	N/A
Current Time:	May 15 2020 02:56 P.M.

Product Info

Model#:	T3260
Serial#:	GCBA8100100020
MAC Address:	9C:1E:95:03:AC:81
Firmware Version:	T3260-32.165L.34
Language:	Auto-detect

Login Status

You are currently logged in as: **root**

WAN Connection Status

WAN Type:	Ethernet
Dynamic/Static:	Dynamic
Modem IP Address:	192.168.0.17
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.0.1
Lease Time Remaining:	23H 57M 5S
DNS Address #1:	192.168.0.1
DNS Address #2:	4.2.2.4

Wireless

SmartSteering™:	Enabled

SSID 2.4G + 5G

SSID:	WIN_100020
Security:	Enabled
Security Type:	WPA2-AES

Home Network

LaptopPC	Connected 192.168.254.50
iPhone	Connected 192.168.254.64

Firewall

UPnP Setting:	Enabled
Firewall:	Medium
Blocking/Filtering:	Disabled

Diagnostics - Login Required

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.

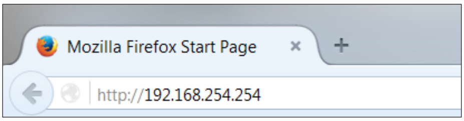
Accessing the Status Screens

To access the Gateway's Status screens:

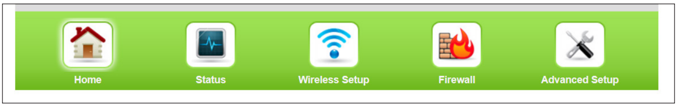
1. Open a Web browser. In the *Address* text box, type:

   http://192.168.254.254

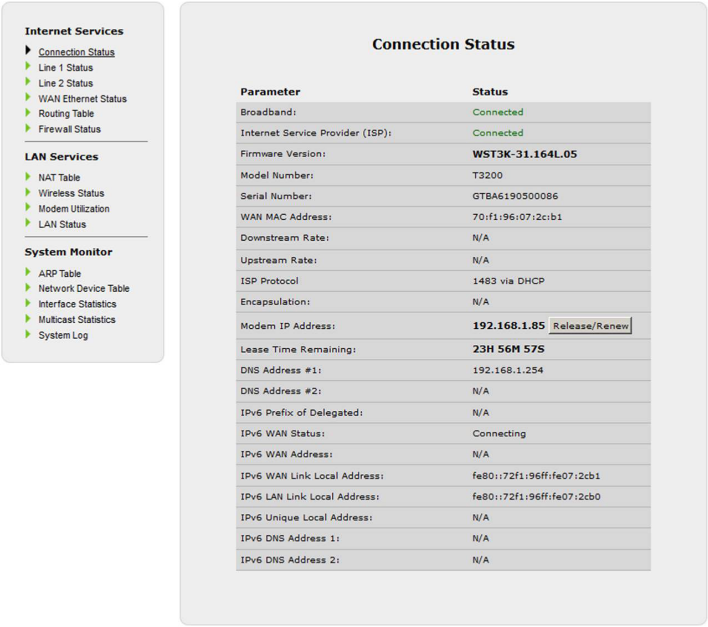
   then press **Enter** on the keyboard.



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



3. The *Connection Status* screen appears. “Connection Status” is under the “Internet Service” group.



Connection Status

Parameter	Status
Broadband:	Connected
Internet Service Provider (ISP):	Connected
Firmware Version:	**WST3K-31.164L.05**
Model Number:	T3200
Serial Number:	GTBA6190500086
WAN MAC Address:	70:f1:96:07:2c:b1
Downstream Rate:	N/A
Upstream Rate:	N/A
ISP Protocol	1483 via DHCP
Encapsulation:	N/A
Modem IP Address:	**192.168.1.85**
Lease Time Remaining:	**23H 56M 57S**
DNS Address #1:	192.168.1.254
DNS Address #2:	N/A
IPv6 Prefix of Delegated:	N/A
IPv6 WAN Status:	Connecting
IPv6 WAN Address:	N/A
IPv6 WAN Link Local Address:	fe80::72f1:96ff:fe07:2cb1
IPv6 LAN Link Local Address:	fe80::72f1:96ff:fe07:2cb0
IPv6 Unique Local Address:	N/A
IPv6 DNS Address 1:	N/A
IPv6 DNS Address 2:	N/A

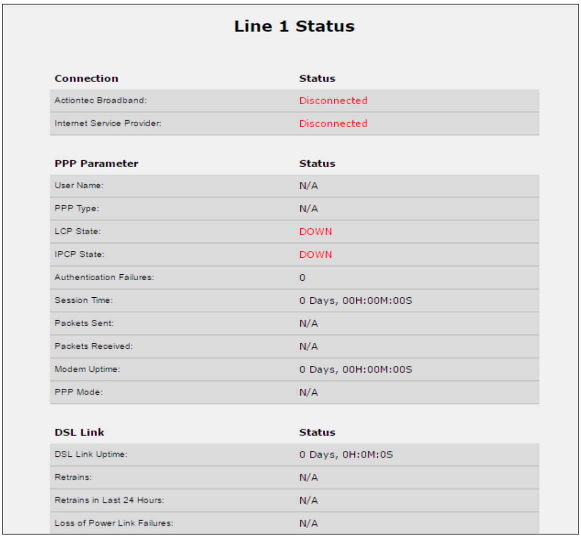
From here, all the Status screens can be accessed from the menu on the left.

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.

Line 1/Line 2 Status

Click **Line 1 Status** from any Status screen to generate the *Line 1 Status* screen. This screen displays the Gateway's DSL connection parameters for *DSL Line 1* port. Clicking **Line 2 Status** genreates the *Line 2 Status* screen, which displays the connection parameters for the Gateway's *DSL Line 2* port.

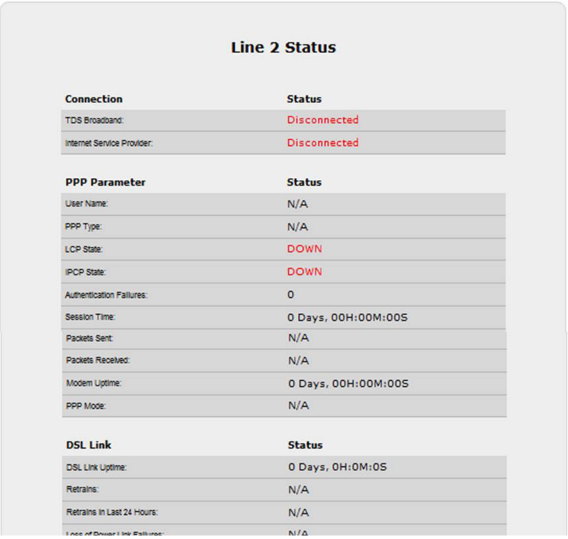


Line 1 Status

Connection	Status
Actiontec Broadband:	Disconnected
Internet Service Provider:	Disconnected

PPP Parameter	Status
User Name:	N/A
PPP Type:	N/A
LCP State:	DOWN
IPCP 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	Status
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



Line 2 Status

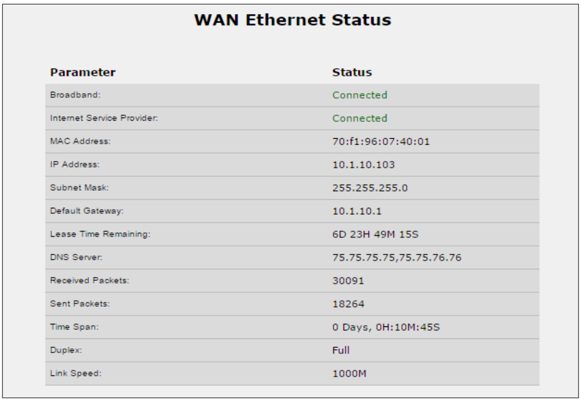
Connection	Status
TDS Broadband:	Disconnected
Internet Service Provider:	Disconnected

PPP Parameter	Status
User Name:	N/A
PPP Type:	N/A
LCP State:	DOWN
IPCP 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	Status
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

WAN Ethernet

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

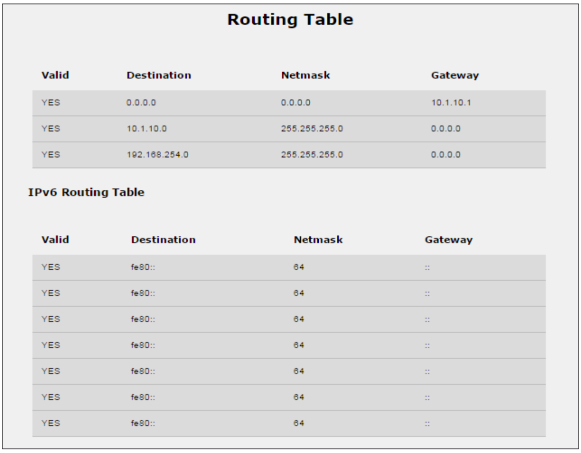


WAN Ethernet Status

Parameter	Status
Broadband:	Connected
Internet Service Provider:	Connected
MAC Address:	70:f1:96:07:40:01
IP Address:	10.1.10.103
Subnet Mask:	255.255.255.0
Default Gateway:	10.1.10.1
Lease Time Remaining:	6D 23H 49M 15S
DNS Server:	75.75.75.75,75.75.76.76
Received Packets:	30091
Sent Packets:	18264
Time Span:	0 Days, 0H:10M:45S
Duplex:	Full
Link Speed:	1000M

Routing Table

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



Routing Table

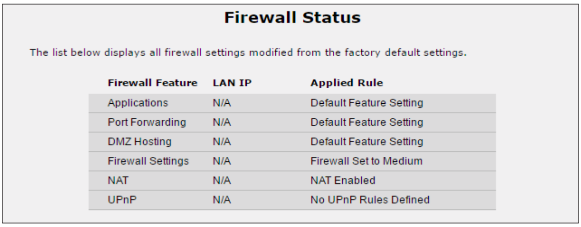
Valid	Destination	Netmask	Gateway
YES	0.0.0.0	0.0.0.0	10.1.10.1
YES	10.1.10.0	255.255.255.0	0.0.0.0
YES	192.168.254.0	255.255.255.0	0.0.0.0

IPv6 Routing Table

Valid	Destination	Netmask	Gateway
YES	fe80::	64	::
YES	fe80::	64	::
YES	fe80::	64	::
YES	fe80::	64	::
YES	fe80::	64	::
YES	fe80::	64	::
YES	fe80::	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.



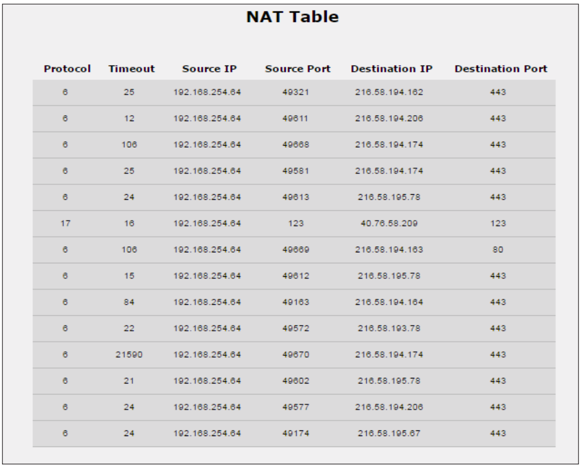
Firewall Status

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	Firewall Set to Medium
NAT	N/A	NAT Enabled
UPnP	N/A	No UPnP Rules Defined

NAT Table

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

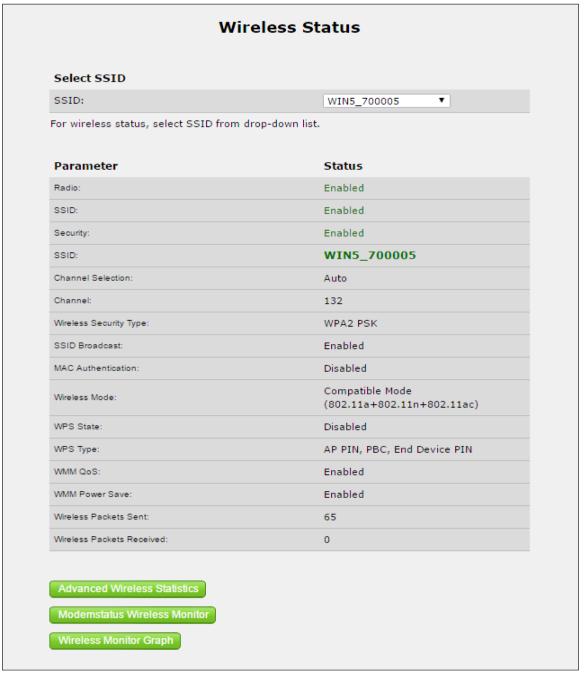


NAT Table

Protocol	Timeout	Source IP	Source Port	Destination IP	Destination Port
6	25	192.168.254.64	49321	216.58.194.162	443
6	12	192.168.254.64	49611	216.58.194.206	443
6	106	192.168.254.64	49668	216.58.194.174	443
6	25	192.168.254.64	49581	216.58.194.174	443
6	24	192.168.254.64	49613	216.58.195.78	443
17	16	192.168.254.64	123	40.76.58.209	123
6	106	192.168.254.64	49669	216.58.194.163	80
6	15	192.168.254.64	49612	216.58.195.78	443
6	84	192.168.254.64	49163	216.58.194.164	443
6	22	192.168.254.64	49572	216.58.193.78	443
6	21590	192.168.254.64	49670	216.58.194.174	443
6	21	192.168.254.64	49602	216.58.195.78	443
6	24	192.168.254.64	49577	216.58.194.206	443
6	24	192.168.254.64	49174	216.58.195.67	443

Wireless Status

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



Wireless Status

Select SSID

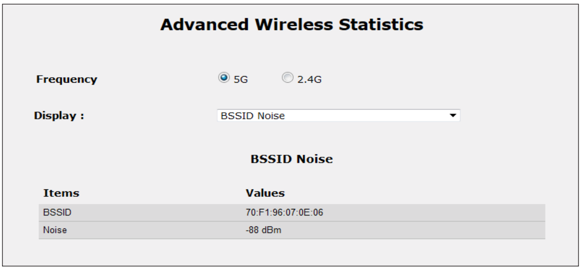
SSID:	WIN5_700005 ▾

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

Parameter	Status
Radio:	Enabled
SSID:	Enabled
Security:	Enabled
SSID:	**WIN5_700005**
Channel Selection:	Auto
Channel:	132
Wireless Security Type:	WPA2 PSK
SSID Broadcast:	Enabled
MAC Authentication:	Disabled
Wireless Mode:	Compatible Mode (802.11a+802.11n+802.11ac)
WPS State:	Disabled
WPS Type:	AP PIN, PBC, End Device PIN
WMM QoS:	Enabled
WMM Power Save:	Enabled
Wireless Packets Sent:	65
Wireless Packets Received:	0

Advanced 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

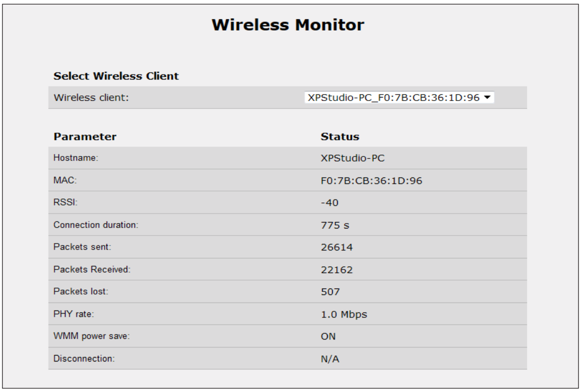
Display : BSSID Noise

BSSID Noise

Items	Values
BSSID	70:F1:96:07:0E: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

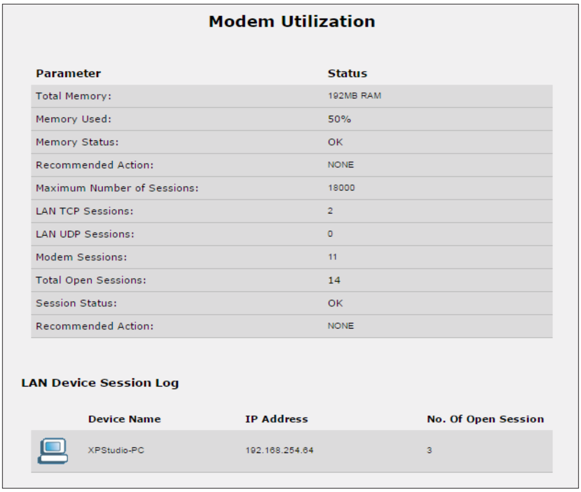
Select Wireless Client

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

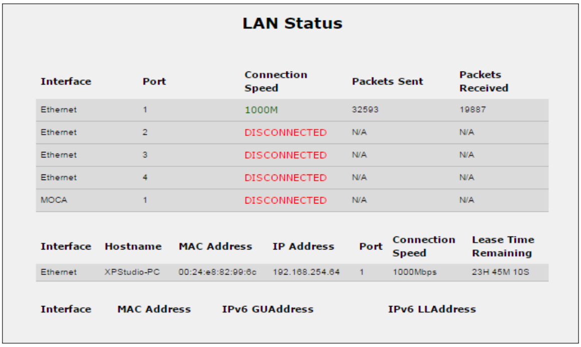
Parameter	Status
Total Memory:	192MB RAM
Memory Used:	50%
Memory Status:	OK
Recommended Action:	NONE
Maximum Number of Sessions:	18000
LAN TCP Sessions:	2
LAN UDP Sessions:	0
Modem Sessions:	11
Total Open Sessions:	14
Session Status:	OK
Recommended Action:	NONE

LAN Device Session Log

	Device Name	IP Address	No. Of Open Session
	XPStudio-PC	192.168.254.64	3

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

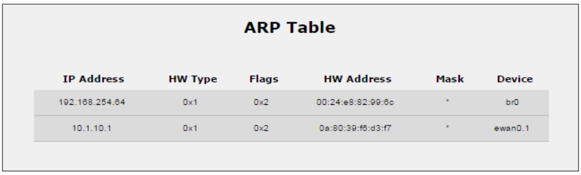
Interface	Port	Connection Speed	Packets Sent	Packets Received
Ethernet	1	1000M	32593	19887
Ethernet	2	DISCONNECTED	N/A	N/A
Ethernet	3	DISCONNECTED	N/A	N/A
Ethernet	4	DISCONNECTED	N/A	N/A
MOCA	1	DISCONNECTED	N/A	N/A

Interface	Hostname	MAC Address	IP Address	Port	Connection Speed	Lease Time Remaining
Ethernet	XPStudio-PC	00:24:e8:82:99:6c	192.168.254.64	1	1000Mbps	23H 45M 10S

Interface	MAC Address	IPv6 GUAddress	IPv6 LLAddress

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.

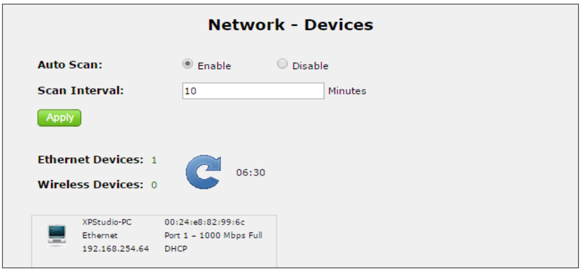


ARP Table

IP Address	HW Type	Flags	HW Address	Mask	Device
192.168.254.64	0x1	0x2	00:24:e8:82:99:6c	*	br0
10.1.10.1	0x1	0x2	0a:80:39:f6:d3:f7	*	ewan0.1

Network Devices

Click **Network Device Table** (underneath System Monitor) from any Status screen to generate the *Network - Devices* screen. This screen allows the user to scan the Gateway's networks for new devices at a selected time interval.



Network - Devices

Auto Scan: ● Enable ○ Disable

Scan Interval: 10 Minutes

Ethernet Devices: 1

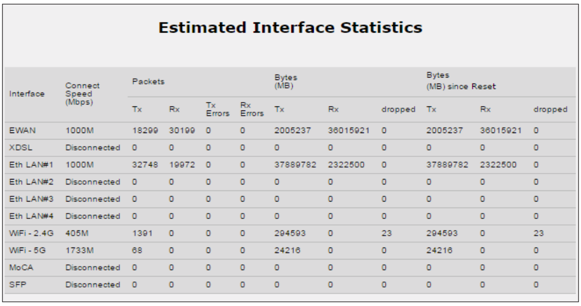
Wireless Devices: 0

06:30

XPStudio-PC 00:24:e8:82:99:6c
Ethernet Port 1 – 1000 Mbps Full
192.168.254.64 DHCP

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.

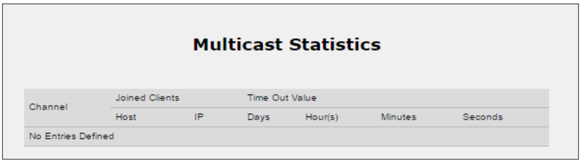


Estimated Interface Statistics

Interface	Connect Speed (Mbps)	Packets				Bytes (MB)			Bytes (MB) since Reset		
		Tx	Rx	Tx Errors	Rx Errors	Tx	Rx	dropped	Tx	Rx	dropped
EWAN	1000M	18299	30199	0	0	2005237	36015921	0	2005237	36015921	0
XDSL	Disconnected	0	0	0	0	0	0	0	0	0	0
Eth LAN#1	1000M	32748	19972	0	0	37889782	2322500	0	37889782	2322500	0
Eth LAN#2	Disconnected	0	0	0	0	0	0	0	0	0	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	1391	0	0	0	294593	0	23	294593	0	23
WiFi - 5G	1733M	68	0	0	0	24216	0	0	24216	0	0
MoCA	Disconnected	0	0	0	0	0	0	0	0	0	0
SFP	Disconnected	0	0	0	0	0	0	0	0	0	0

Multicast Statistics

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

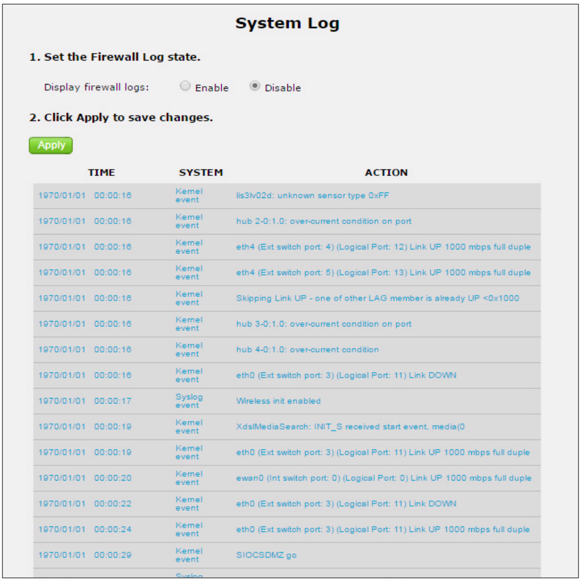


Multicast Statistics

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.

TIME	SYSTEM	ACTION
1970/01/01 00:00:16	Kernel event	lis3lv02d: unknown sensor type 0xFF
1970/01/01 00:00:16	Kernel event	hub 2-0:1.0: over-current condition on port
1970/01/01 00:00:16	Kernel event	eth4 (Ext switch port: 4) (Logical Port: 12) Link UP 1000 mbps full duple
1970/01/01 00:00:16	Kernel event	eth4 (Ext switch port: 5) (Logical Port: 13) Link UP 1000 mbps full duple
1970/01/01 00:00:16	Kernel event	Skipping Link UP - one of other LAG member is already UP <0x1000
1970/01/01 00:00:16	Kernel event	hub 3-0:1.0: over-current condition on port
1970/01/01 00:00:16	Kernel event	hub 4-0:1.0: over-current condition
1970/01/01 00:00:16	Kernel event	eth0 (Ext switch port: 3) (Logical Port: 11) Link DOWN
1970/01/01 00:00:17	Syslog event	Wireless init enabled
1970/01/01 00:00:19	Kernel event	XdslMediaSearch: INIT_S received start event, media(0
1970/01/01 00:00:19	Kernel event	eth0 (Ext switch port: 3) (Logical Port: 11) Link UP 1000 mbps full duple
1970/01/01 00:00:20	Kernel event	ewan0 (Int switch port: 0) (Logical Port: 0) Link UP 1000 mbps full duple
1970/01/01 00:00:22	Kernel event	eth0 (Ext switch port: 3) (Logical Port: 11) Link DOWN
1970/01/01 00:00:24	Kernel event	eth0 (Ext switch port: 3) (Logical Port: 11) Link UP 1000 mbps full duple
1970/01/01 00:00:29	Kernel event	SIOCSDMZ go
	Syslog	

Configuring Wireless Settings

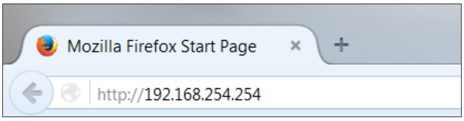
4

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

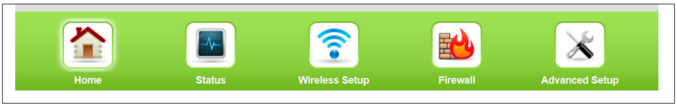
Accessing Wireless Settings

To access the Wireless Settings screens:

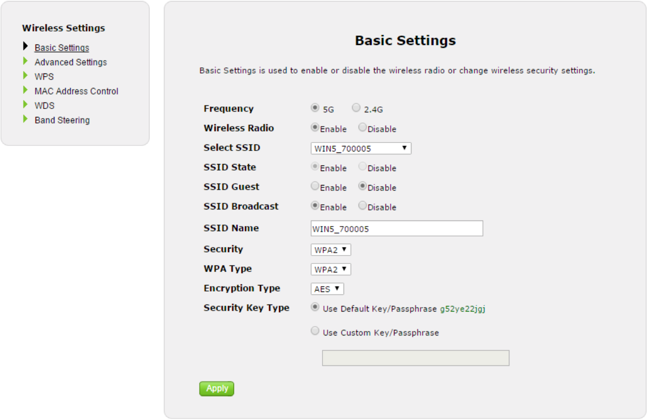
1. Open a Web browser. In the *Address* text box, type:
   http://192.168.254.254
   then press **Enter** on the keyboard.



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 *Basic Settings* screen appears, with a menu of other wireless options listed on the left side of the screen.



Basic Settings

Basic Settings is used to enable or disable the wireless radio or change wireless security settings.

Frequency ● 5G ○ 2.4G
Wireless Radio ● Enable ○ Disable
Select SSID WIN5_700005
SSID State ● Enable ○ Disable
SSID Guest ○ Enable ● Disable
SSID Broadcast ● Enable ○ Disable
SSID Name WIN5_700005
Security WPA2
WPA Type WPA2
Encryption Type AES
Security Key Type ● Use Default Key/Passphrase g52ye22jgj
○ Use Custom Key/Passphrase

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.

Changing the Wireless Network Name (SSID)

To change the name of the Gateway's wireless network, enter the new name in the *SSID Name* text box in the *Basic Settings* screen, then click **Apply**.

Changing the Wireless Key/Passphrase

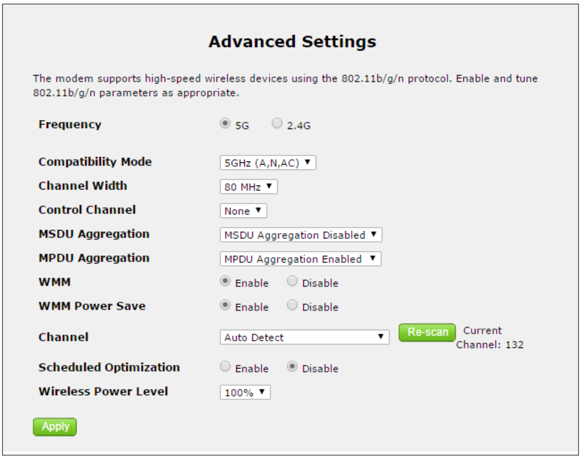
To change the passphrase for the Gateway's wireless SSID, at the Security Key Type, press the button for Use Custom Key/Passphrase, enter the desired Wireless Key/ Passphrase in the text box, then click Apply.

Enabling SSID Guest Option

Enabling this option in the *Basic Settings* screen allows guest users to access the Gateway's wireless Internet connection, while preventing these users from accessing other wireless devices, including network printers or other unsecured network devices. To enable, click in the *Enable* button next to *SSID Guest*, then click **Apply**.

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.



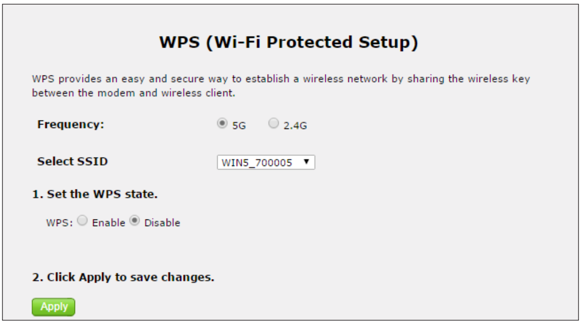
Advanced Settings

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	● 5G ○ 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	● Enable ○ Disable
WMM Power Save	● Enable ○ Disable
Channel	Auto Detect ▾ Re-scan Current Channel: 132
Scheduled Optimization	○ Enable ● Disable
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

Select SSID WIN5_700005 ▼

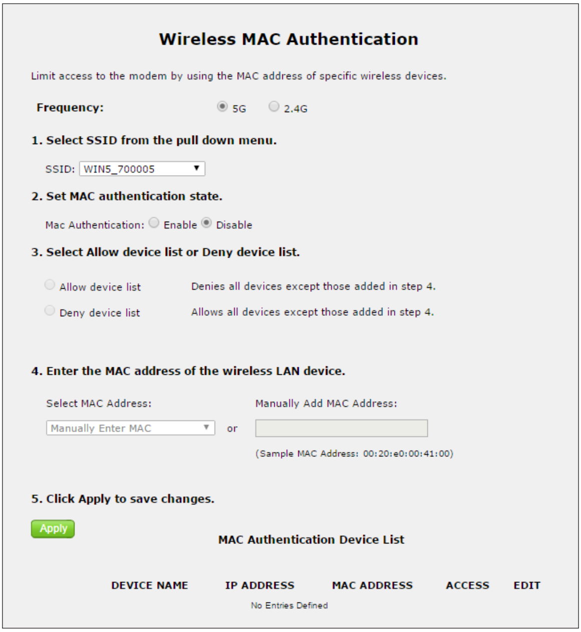
1. Set the WPS state.

WPS: ○ Enable ● Disable

2. Click Apply to save changes.

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. *(Note: this feature only works if Band Steering is DISABLED.)* 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: WIN5_700005 ▾

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 Enter MAC ▾ or Manually Add MAC Address:

(Sample MAC Address: 00:20:e0:00:41:00)

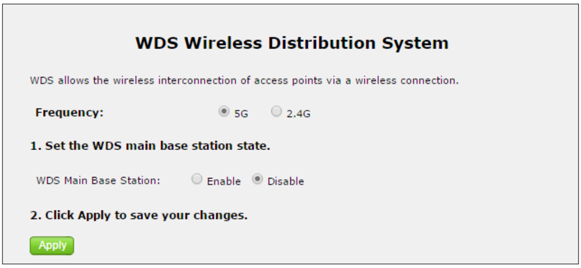
5. Click Apply to save changes.

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 interconnection of access points via a wireless connection. 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

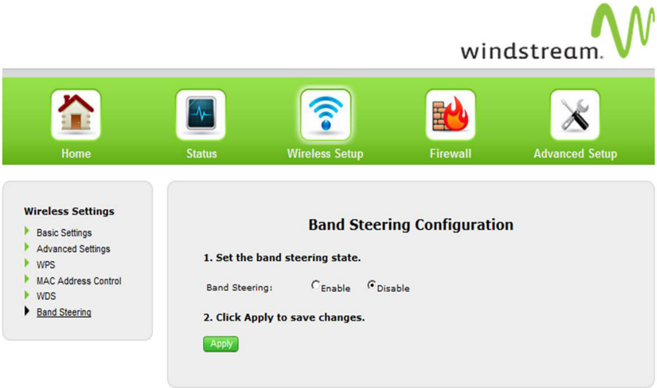
1. Set the WDS main base station state.

WDS Main Base Station: ○ Enable ● Disable

2. Click Apply to save your changes.

Band Steering

Click **Band Steering** from any Wireless Settings screen to generate the *Band Steering Configuration* screen, which allows the user to configure the Gateway to automatically connect 2.4GHz and 5GHz wireless devices to the appropriate wireless network bandwidth. Also, this screen can be used to assign a certain wireless network and/or bandwidth to a particular wireless device. Follow the onscreen instructions to configure.



Band Steering Configuration

1. Set the band steering state.

Band Steering: ○Enable ●Disable

2. Click Apply to save changes.

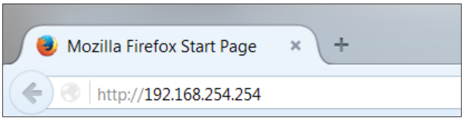
Configuring Firewall Settings 5

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

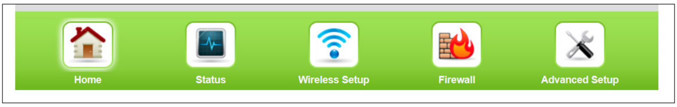
Accessing Firewall Settings

To access the Firewall screens:

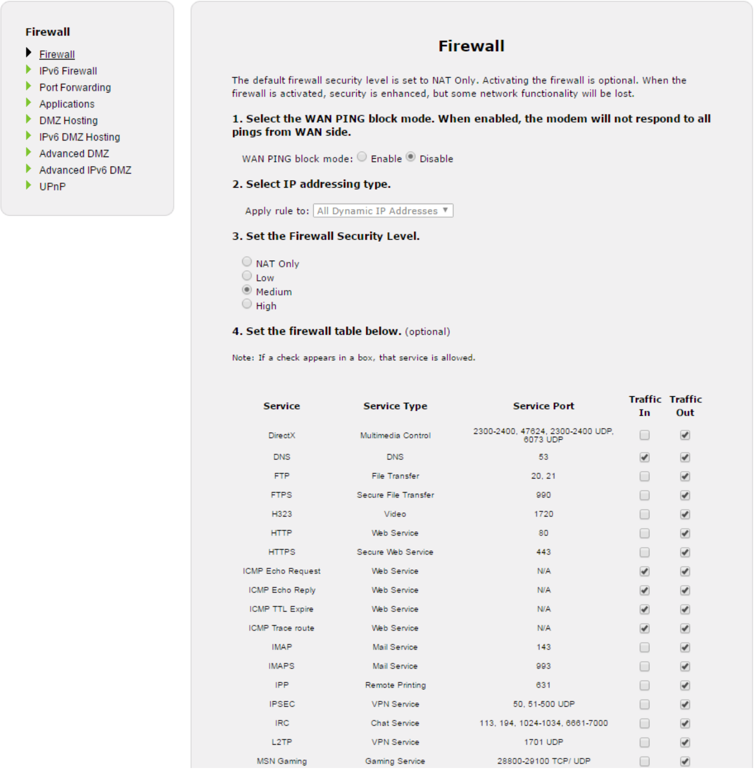
1. Open a Web browser. In the *Address* text box, type:
   http://192.168.254.254
   then press **Enter** on the keyboard.



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

The default firewall security level is set to NAT Only. Activating the firewall is optional. When the firewall is activated, security is enhanced, but some network functionality will be lost.

1. Select the WAN PING block mode. When enabled, the modem will not respond to all pings from WAN side.

WAN PING block mode: ○ Enable ● Disable

2. Select IP addressing type.

Apply rule to: All Dynamic IP Addresses ▾

3. Set the Firewall Security Level.

○ NAT Only
○ Low
● Medium
○ High

4. Set the firewall table below. (optional)

Note: If a check appears in a box, that service is allowed.

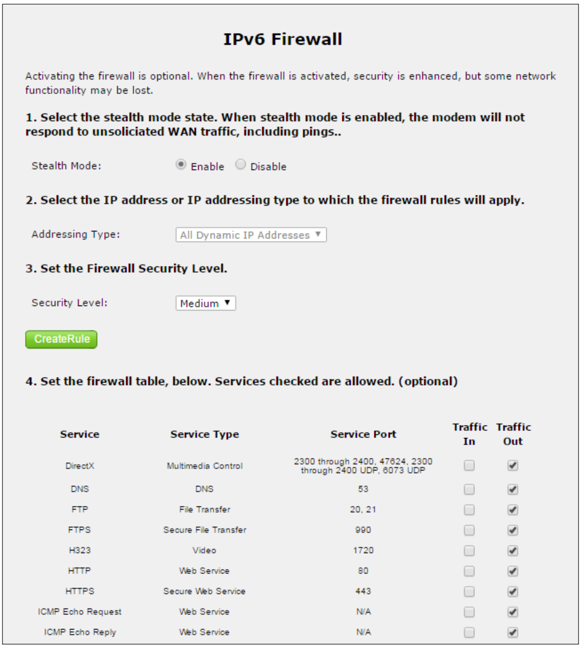
Service	Service Type	Service Port	Traffic In	Traffic Out
DirectX	Multimedia Control	2300-2400, 47624, 2300-2400 UDP, 6073 UDP	□	☑
DNS	DNS	53	☑	☑
FTP	File Transfer	20, 21	□	☑
FTPS	Secure File Transfer	990	□	☑
H323	Video	1720	□	☑
HTTP	Web Service	80	□	☑
HTTPS	Secure Web Service	443	□	☑
ICMP Echo Request	Web Service	N/A	☑	☑
ICMP Echo Reply	Web Service	N/A	☑	☑
ICMP TTL Expire	Web Service	N/A	☑	☑
ICMP Trace route	Web Service	N/A	☑	☑
IMAP	Mail Service	143	□	☑
IMAPS	Mail Service	993	□	☑
IPP	Remote Printing	631	□	☑
IPSEC	VPN Service	50, 51-500 UDP	□	☑
IRC	Chat Service	113, 194, 1024-1034, 6661-7000	□	☑
L2TP	VPN Service	1701 UDP	□	☑
MSN Gaming	Gaming Service	28800-29100 TCP/ UDP	□	☑

Firewall

Click **General** from any Firewall Settings screen to generate the *Firewall* screen, as shown in the figure above. To configure basic settings of the Gateway's firewall, 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: All Dynamic IP Addresses ▼

3. Set the Firewall Security Level.

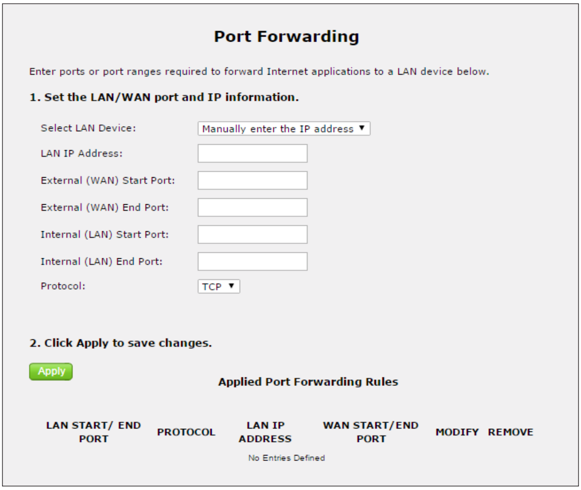
Security Level: Medium ▼

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

Service	Service Type	Service Port	Traffic In	Traffic Out
DirectX	Multimedia Control	2300 through 2400, 47624, 2300 through 2400 UDP, 6073 UDP	□	☑
DNS	DNS	53	□	☑
FTP	File Transfer	20, 21	□	☑
FTPS	Secure File Transfer	990	□	☑
H323	Video	1720	□	☑
HTTP	Web Service	80	□	☑
HTTPS	Secure Web Service	443	□	☑
ICMP Echo Request	Web Service	N/A	□	☑
ICMP Echo Reply	Web Service	N/A	□	☑

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.

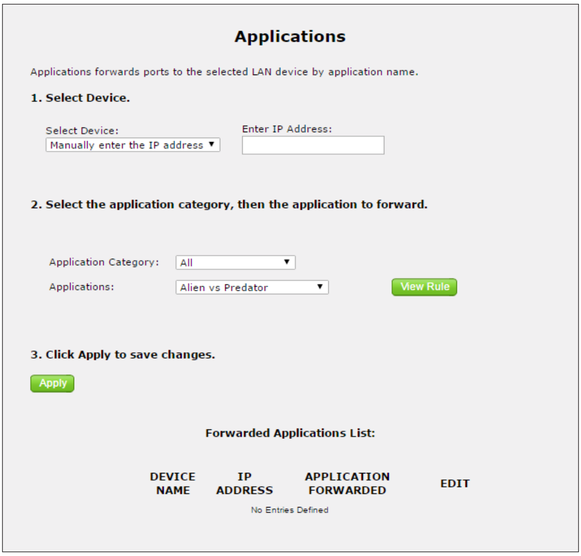
Applied Port Forwarding Rules

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 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: Manually enter the IP address

Enter IP Address:

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

Application Category: All

Applications: Alien vs Predator

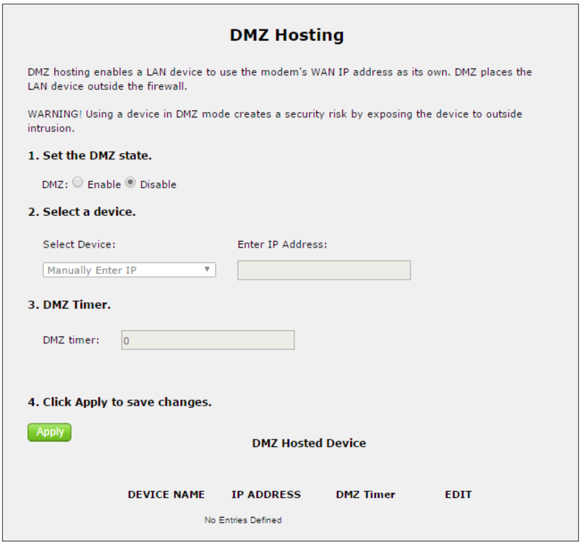
3. Click Apply to save changes.

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: Manually Enter IP

Enter IP Address:

3. DMZ Timer.

DMZ timer: 0

4. Click Apply to save changes.

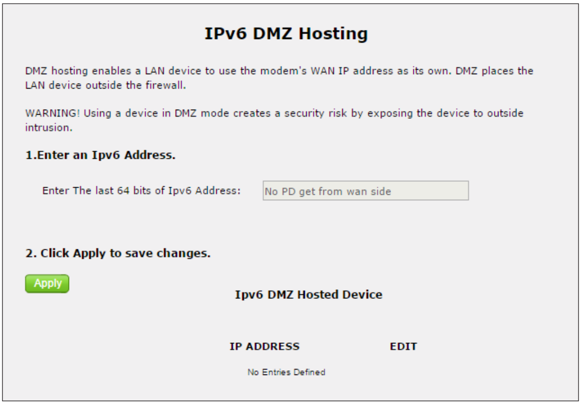
DMZ Hosted Device

DEVICE NAME	IP ADDRESS	DMZ Timer	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: No PD get from wan side

2. Click Apply to save changes.

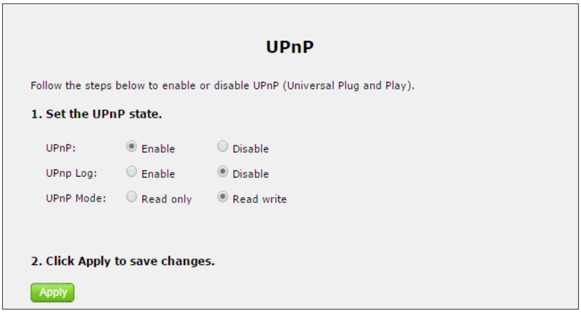
Ipv6 DMZ Hosted Device

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, set the preferred UPnP options, then click **Apply**.



UPnP

Follow the steps below to enable or disable UPnP (Universal Plug and Play).

1. Set the UPnP state.

UPnP:	● Enable	○ Disable
UPnp Log:	○ Enable	● Disable
UPnP Mode:	○ Read only	● Read write

2. Click Apply to save changes.

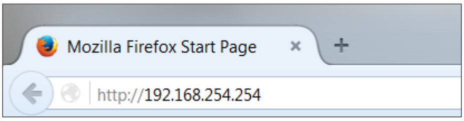
Advanced Settings 6

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

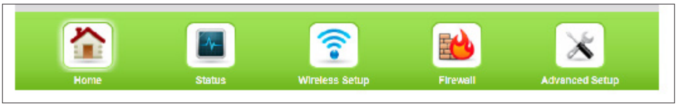
Accessing the Advanced Setup Screens

To access the Gateway's Advanced Setup screens:

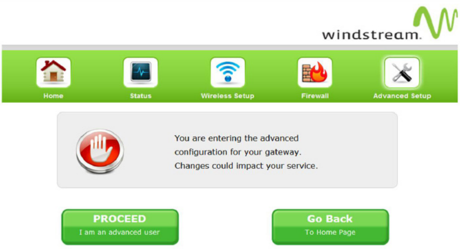
1. Open a Web browser. In the Address text box, type:
   http://192.168.254.254
   then press Enter on the keyboard.



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

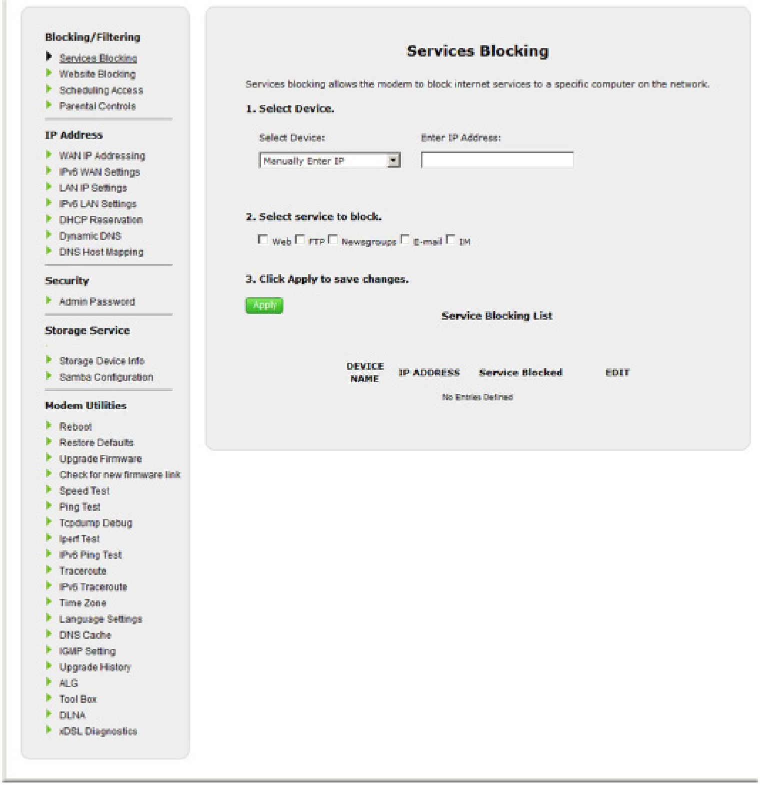


3. A WARNING screen appears. Technicians can click PROCEED to configure the Advanced Settings of the gateway.



You are entering the advanced configuration for your gateway. Changes could impact your service.

4. The Services Blocking screen appears.



Services Blocking

Services blocking allows the modem to block internet services to a specific computer on the network.

1. Select Device.

Select Device: Manually Enter IP

Enter IP Address:

2. Select service to block.

□ Web □ FTP □ Newsgroups □ E-mail □ IM

3. Click Apply to save changes.

Service Blocking List

DEVICE NAME	IP ADDRESS	Service Blocked	EDIT
	No Entries Defined		

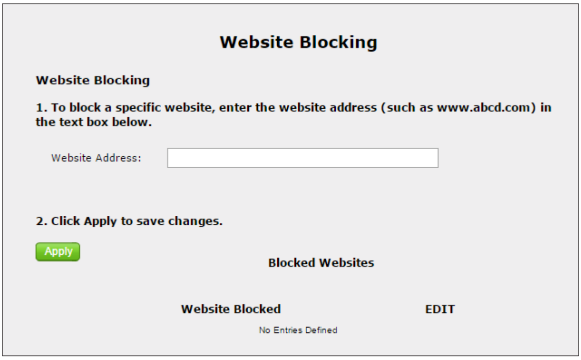
From here, all the Advanced Setup screens can be accessed from the menu on the left.

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.



Website Blocking

Website Blocking

1. To block a specific website, enter the website address (such as www.abcd.com) in the text box below.

Website Address:

2. Click Apply to save changes.

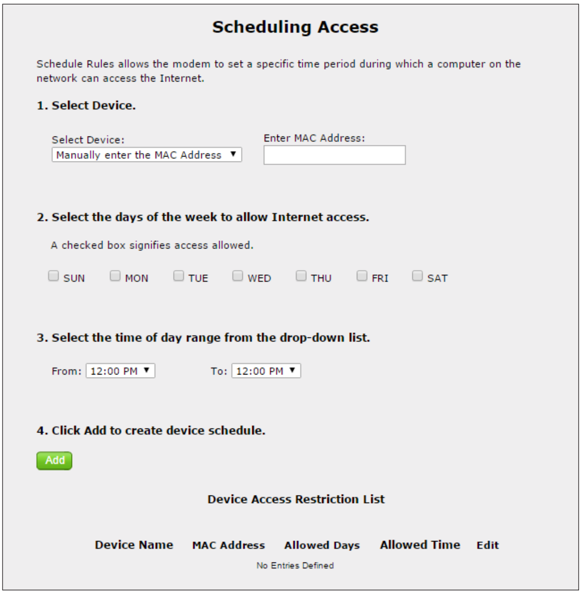
Apply

Blocked Websites

Website Blocked	EDIT
No Entries Defined	

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.



Scheduling Access

Schedule Rules allows the modem to set a specific time period during which a computer on the network can access the Internet.

1. Select Device.

Select Device: Manually enter the MAC Address ▼

Enter MAC Address:

2. Select the days of the week to allow Internet access.

A checked box signifies access allowed.

□ SUN □ MON □ TUE □ WED □ THU □ FRI □ SAT

3. Select the time of day range from the drop-down list.

From: 12:00 PM ▼ To: 12:00 PM ▼

4. Click Add to create device schedule.

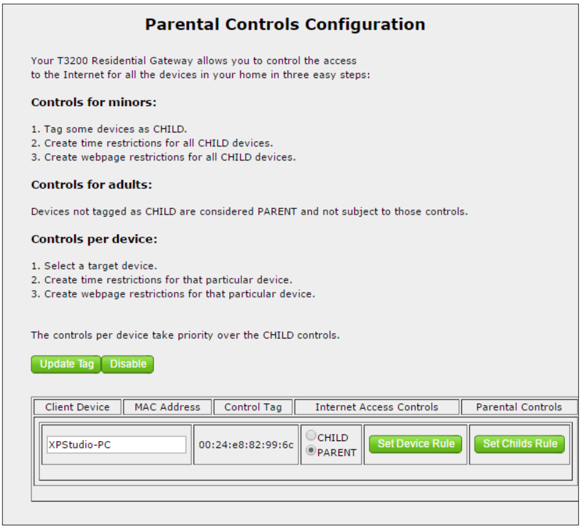
Device Access Restriction List

Device Name	MAC Address	Allowed Days	Allowed Time	Edit

No Entries Defined

Parental Controls

Click Parental Controls from any Advanced Setup screen to generate the Parental Controls Configuration screen. This feature allows the user to allow or prevent access to certain websites for devices on the Gateway's network. Follow the onscreen instructions to configure.



Parental Controls Configuration

Your T3200 Residential Gateway allows you to control the access to the Internet for all the devices in your home in three easy steps:

Controls for minors:

1. Tag some devices as CHILD.
2. Create time restrictions for all CHILD devices.
3. Create webpage restrictions for all CHILD devices.

Controls for adults:

Devices not tagged as CHILD are considered PARENT and not subject to those controls.

Controls per device:

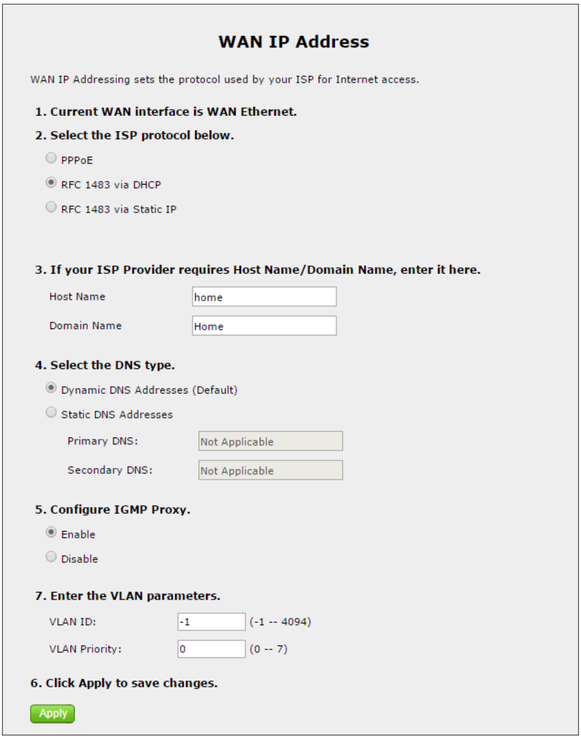
1. Select a target device.
2. Create time restrictions for that particular device.
3. Create webpage restrictions for that particular device.

The controls per device take priority over the CHILD controls.

Client Device	MAC Address	Control Tag	Internet Access Controls	Parental Controls
XPStudio-PC	00:24:e8:82:99:6c	○ CHILD ● PARENT	Set Device Rule	Set Childs Rule

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	Home

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

7. Enter the VLAN parameters.

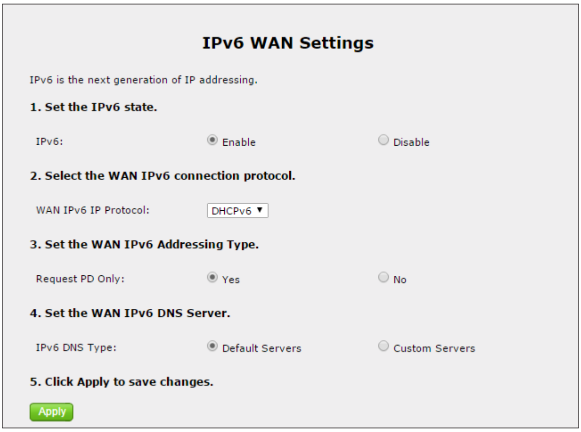
VLAN ID:	-1	(-1 -- 4094)
VLAN Priority:	0	(0 -- 7)

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.

> WARNING: This setting should be configured by experienced network technicians only, since any changes could affect the Gateway's IPv6 service.



IPv6 WAN Settings

IPv6 is the next generation of IP addressing.

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

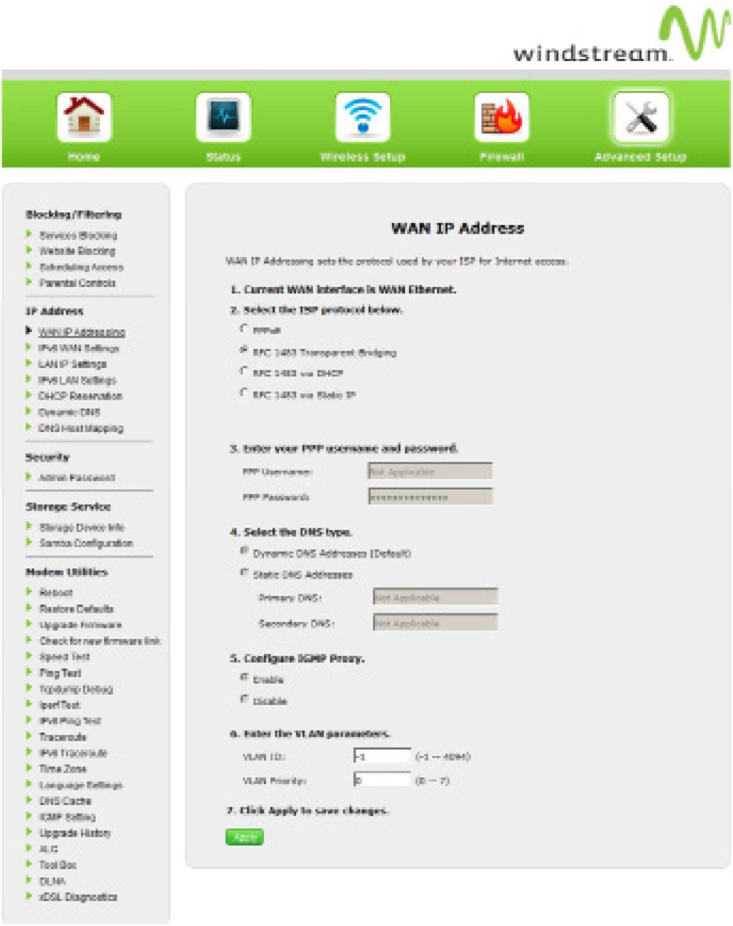
4. Set the WAN IPv6 DNS Server.

IPv6 DNS Type: ● Default Servers ○ Custom Servers

5. Click Apply to save changes.

How to Set the T3280 to RFC1483 Transparent Bridge

From the WAN IP Address screen, select RFC 1483 Transparent Bridging and click Apply. The gateway will allow the WAN IP address to pass-through to the device connected to LAN Port 1 Only.



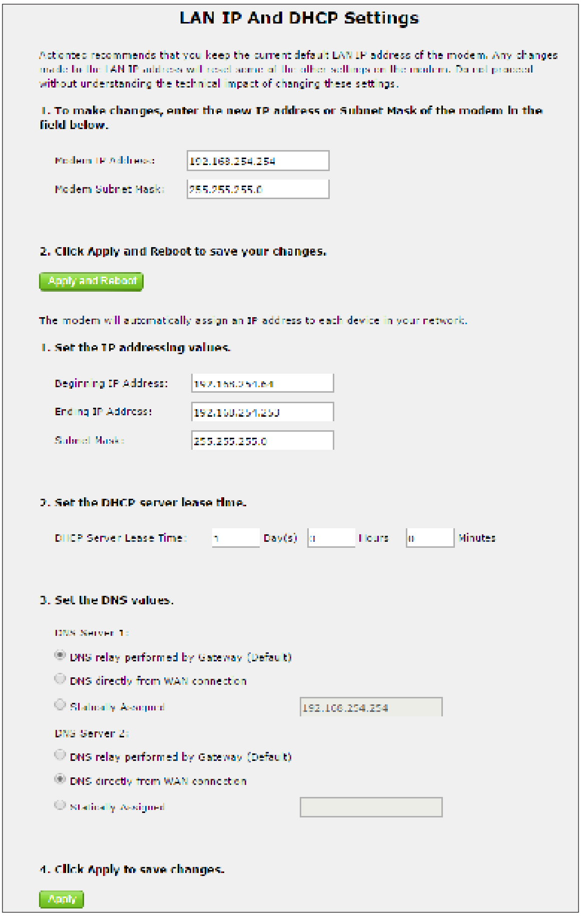
WAN IP Address

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 Transparent Bridging
   - ○ RFC 1483 via DHCP
   - ○ RFC 1483 via Static IP
3. Enter your PPP username and password.
   - PPP Username: Not Applicable
   - PPP Password: ••••••••••••••
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. Enter the VLAN parameters.
   - VLAN ID: -1 (-1 -- 4094)
   - VLAN Priority: 0 (0 -- 7)
7. Click Apply to save changes.

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: 192.168.254.254

Modem Subnet Mask: 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: 192.168.254.64

Ending IP Address: 192.168.254.253

Subnet Mask: 255.255.255.0

2. Set the DHCP server lease time.

DHCP Server Lease Time: 1 Day(s) 0 Hours 0 Minutes

3. Set the DNS values.

DNS Server 1:

● DNS relay performed by Gateway (Default)

○ DNS directly from WAN connection

○ Statically Assigned 192.168.254.254

DNS Server 2:

○ DNS relay performed by Gateway (Default)

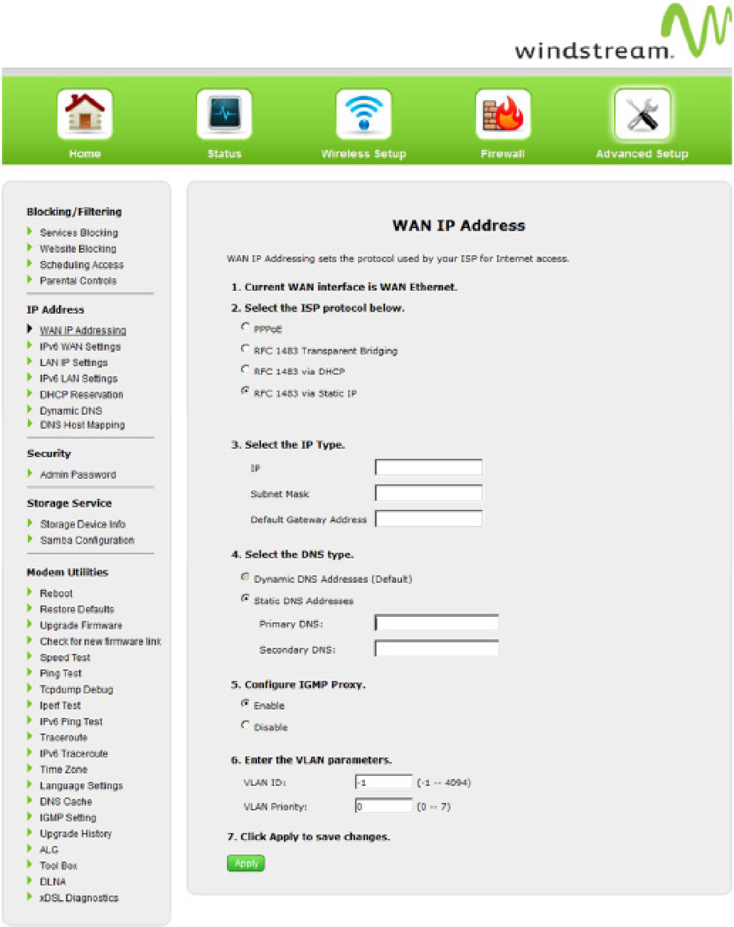
● DNS directly from WAN connection

○ Statically Assigned

4. Click Apply to save changes.

How to Manually Set the T3280 for Static IP

From the WAN IP Address screen, select RFC 1483 via Static IP. Enter the IP address to be assigned to the Gateway, the subnet mask and the IP Address of the Default Gateway. Click Apply.



WAN IP Address

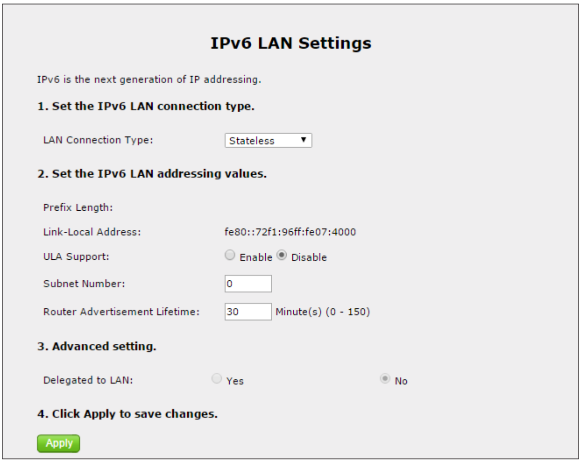
WAN IP Addressing sets the protocol used by your ISP for Internet access.

1. Current WAN interface is WAN Ethernet.
2. Select the ISP protocol below.
   - ○ PPPoE
   - ○ RFC 1483 Transparent Bridging
   - ○ RFC 1483 via DHCP
   - ● RFC 1483 via Static IP
3. Select the IP Type.
   - IP
   - Subnet Mask
   - Default Gateway Address
4. Select the DNS type.
   - ○ Dynamic DNS Addresses (Default)
   - ● Static DNS Addresses
   - Primary DNS:
   - Secondary DNS:
5. Configure IGMP Proxy.
   - ● Enable
   - ○ Disable
6. Enter the VLAN parameters.
   - VLAN ID: -1 (-1 -- 4094)
   - VLAN Priority: 0 (0 -- 7)
7. Click Apply to save changes.

Apply

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.



IPv6 LAN Settings

IPv6 is the next generation of IP addressing.

1. Set the IPv6 LAN connection type.

LAN Connection Type: Stateless ▼

2. Set the IPv6 LAN addressing values.

Prefix Length:

Link-Local Address: fe80::72f1:96ff:fe07:4000

ULA Support: ○ Enable ● Disable

Subnet Number: 0

Router Advertisement Lifetime: 30 Minute(s) (0 - 150)

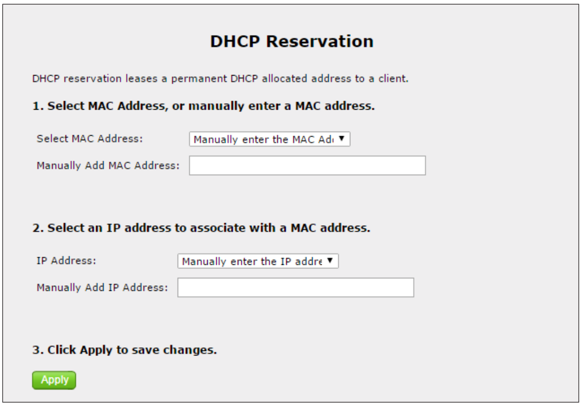
3. Advanced setting.

Delegated to LAN: ○ Yes ● No

4. Click Apply to save changes.

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.



DHCP Reservation

DHCP reservation leases a permanent DHCP allocated address to a client.

1. Select MAC Address, or manually enter a MAC address.

Select MAC Address: Manually enter the MAC Ad

Manually Add MAC Address:

2. Select an IP address to associate with a MAC address.

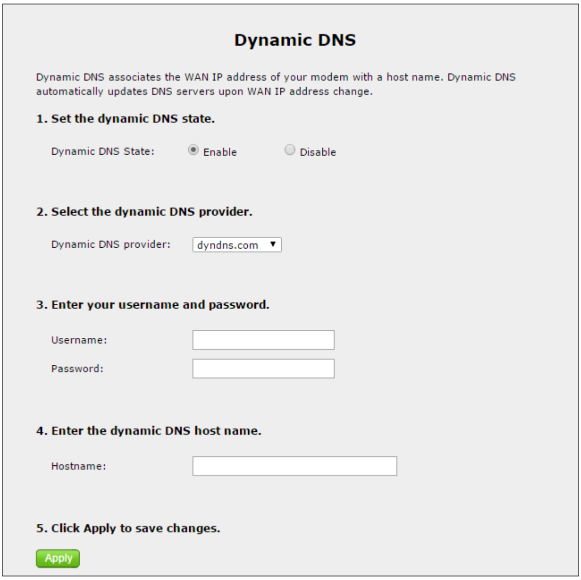
IP Address: Manually enter the IP addre

Manually Add IP Address:

3. Click Apply to save changes.

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: dyndns.com ▼

3. Enter your username and password.

Username:

Password:

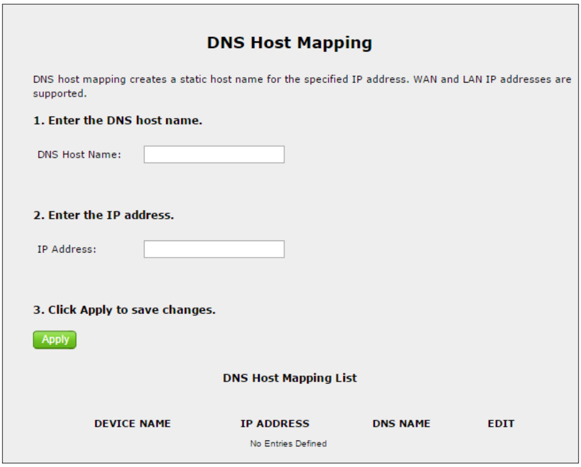
4. Enter the dynamic DNS host name.

Hostname:

5. Click Apply to save changes.

DNS Host Mapping

Click DNS Host Mapping from any Advanced Setup screen to generate the DNS Host Mapping 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:

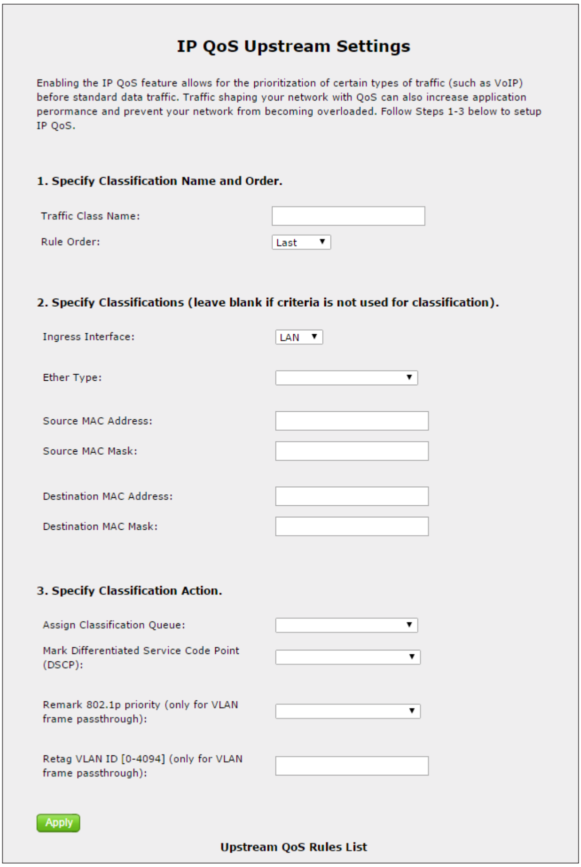
3. Click Apply to save changes.

DNS Host Mapping List

DEVICE NAME	IP ADDRESS	DNS NAME	EDIT
	No Entries Defined		

IP QoS Upstream Settings

Log in as root to generate the IP QoS Upstream Settings screen. This feature allows the user to prioritize certain types of upstream data traffic over standard upstream data traffic. Follow the onscreen instructions to configure.



IP QoS Upstream Settings

Enabling the IP QoS feature allows for the prioritization of certain types of traffic (such as VoIP) before standard data traffic. Traffic shaping your network with QoS can also increase application peromance and prevent your network from becoming overloaded. Follow Steps 1-3 below to setup IP QoS.

1. Specify Classification Name and Order.

Traffic Class Name:

Rule Order: Last

2. Specify Classifications (leave blank if criteria is not used for classification).

Ingress Interface: LAN

Ether Type:

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

3. Specify Classification Action.

Assign Classification Queue:

Mark Differentiated Service Code Point (DSCP):

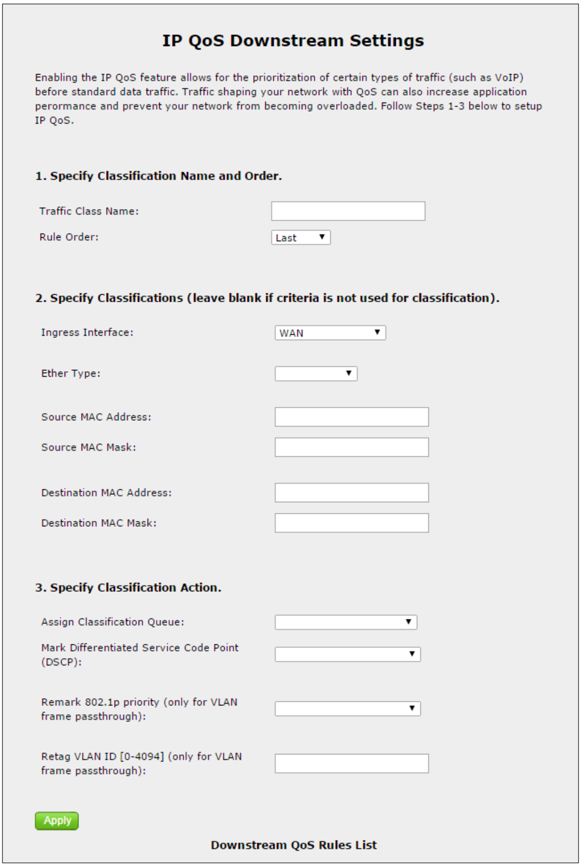
Remark 802.1p priority (only for VLAN frame passthrough):

Retag VLAN ID [0-4094] (only for VLAN frame passthrough):

Upstream QoS Rules List

IP QoS Downstream Settings

Log in as root to generate the IP QoS Downstream Settings screen. This feature allows the user to prioritize certain types of downstream data traffic over standard downstream data traffic. Follow the onscreen instructions to configure.



IP QoS Downstream Settings

Enabling the IP QoS feature allows for the prioritization of certain types of traffic (such as VoIP) before standard data traffic. Traffic shaping your network with QoS can also increase application perormance and prevent your network from becoming overloaded. Follow Steps 1-3 below to setup IP QoS.

1. Specify Classification Name and Order.

Traffic Class Name:

Rule Order: Last

2. Specify Classifications (leave blank if criteria is not used for classification).

Ingress Interface: WAN

Ether Type:

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

3. Specify Classification Action.

Assign Classification Queue:

Mark Differentiated Service Code Point (DSCP):

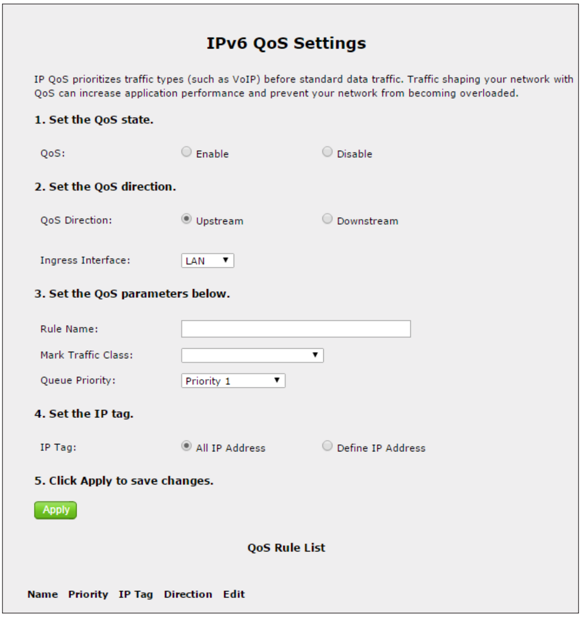
Remark 802.1p priority (only for VLAN frame passthrough):

Retag VLAN ID [0-4094] (only for VLAN frame passthrough):

Downstream QoS Rules List

IPv6 QoS

Log in as root to generate the IPv6 QoS Settings screen. This feature allows the user to prioritize certain types of IPv6 data traffic over standard IPv6 data traffic. Follow the onscreen instructions to configure.



IPv6 QoS Settings

IP QoS prioritizes traffic types (such as VoIP) before standard data traffic. Traffic shaping your network with QoS can increase application performance and prevent your network from becoming overloaded.

1. Set the QoS state.

QoS: ○ Enable ○ Disable

2. Set the QoS direction.

QoS Direction: ● Upstream ○ Downstream

Ingress Interface: LAN ▼

3. Set the QoS parameters below.

Rule Name:

Mark Traffic Class: ▼

Queue Priority: Priority 1 ▼

4. Set the IP tag.

IP Tag: ● All IP Address ○ Define IP Address

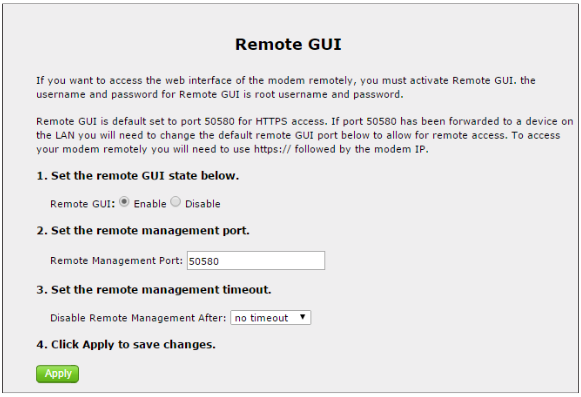
5. Click Apply to save changes.

QoS Rule List

Name	Priority	IP Tag	Direction	Edit

Remote GUI

Log in as root to generate the Remote GUI screen. This feature allows the user to access the Gateway's graphical user interface from a remote location. Follow the onscreen instructions to configure.



Remote GUI

If you want to access the web interface of the modem remotely, you must activate Remote GUI. the username and password for Remote GUI is root username and password.

Remote GUI is default set to port 50580 for HTTPS access. If port 50580 has been forwarded to a device on the LAN you will need to change the default remote GUI port below to allow for remote access. To access your modem remotely you will need to use https:// followed by the modem IP.

1. Set the remote GUI state below.

Remote GUI: ● Enable ○ Disable

2. Set the remote management port.

Remote Management Port: 50580

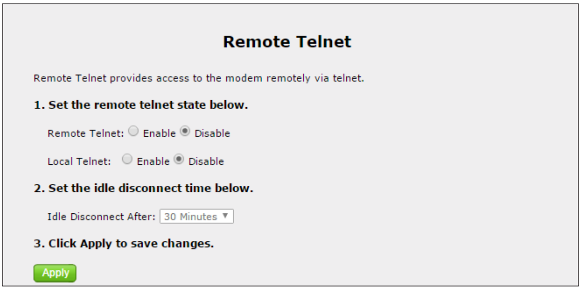
3. Set the remote management timeout.

Disable Remote Management After: no timeout ▼

4. Click Apply to save changes.

Remote Telnet

Log in as root to generate the Remote Telnet screen. This feature allows the user to access the Gateway from a remote location via telnet. Follow the onscreen instructions to configure.



Remote Telnet

Remote Telnet provides access to the modem remotely via telnet.

1. Set the remote telnet state below.

Remote Telnet: ○ Enable ● Disable

Local Telnet: ○ Enable ● Disable

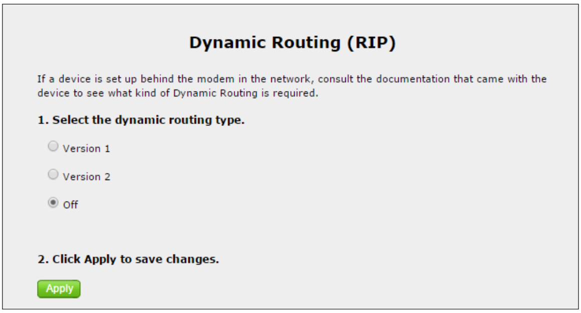
2. Set the idle disconnect time below.

Idle Disconnect After: 30 Minutes ▼

3. Click Apply to save changes.

Dynamic Routing

Click Dynamic Routing from any Advanced Setup screen to generate the Dynamic Routing (RIP) screen. This feature allows the user to set up the Gateway on the network behind a modem using dynamic routing. Follow the onscreen instructions to configure.



Dynamic Routing (RIP)

If a device is set up behind the modem in the network, consult the documentation that came with the device to see what kind of Dynamic Routing is required.

1. Select the dynamic routing type.

○ Version 1

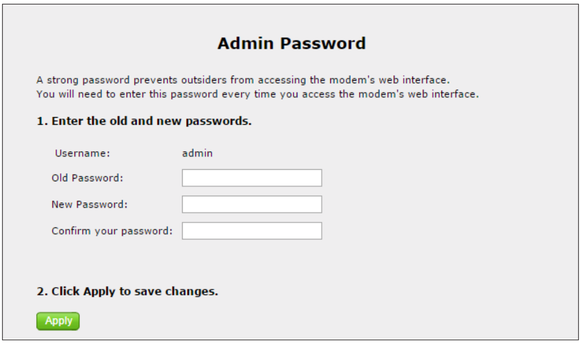
○ Version 2

● Off

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.

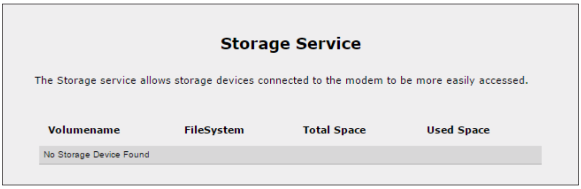
1. Enter the old and new passwords.

Username: admin
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.



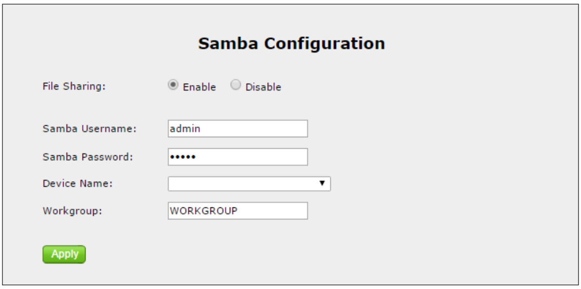
Storage Service

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

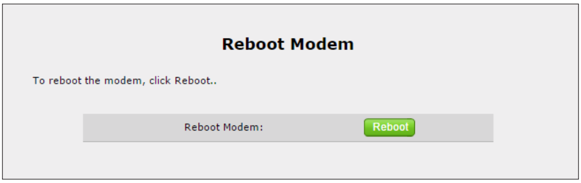
Samba Password: •••••

Device Name:

Workgroup: WORKGROUP

Reboot

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



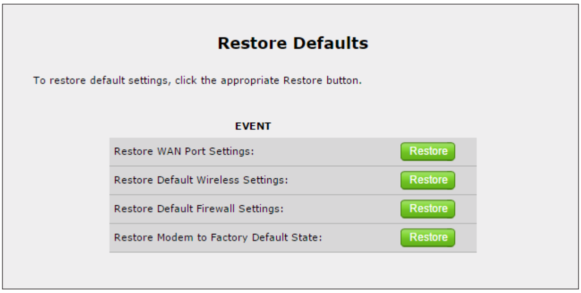
Reboot Modem

To reboot the modem, click Reboot..

Reboot Modem:

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.



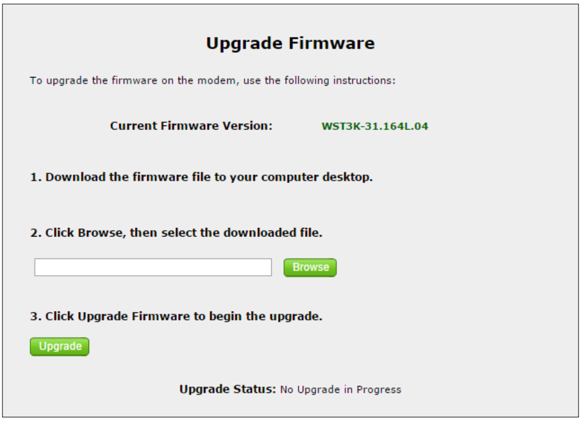
Restore Defaults

To restore default settings, click the appropriate Restore button.

EVENT	
Restore WAN Port Settings:	Restore
Restore Default Wireless Settings:	Restore
Restore Default Firewall Settings:	Restore
Restore Modem to Factory Default State:	Restore

Upgrade Firmware

Click Upgrade Firmware from any Advanced Setup screen to generate the Upgrade Firmware screen. To upgrade the Gateway's firmware, follow the onscreen instructions.



Upgrade Firmware

To upgrade the firmware on the modem, use the following instructions:

Current Firmware Version: WST3K-31.164L.04

1. Download the firmware file to your computer desktop.

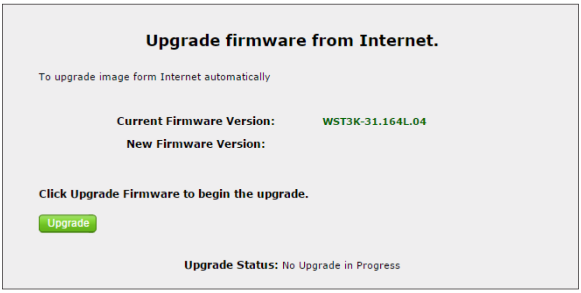
2. Click Browse, then select the downloaded file.

3. Click Upgrade Firmware to begin the upgrade.

Upgrade Status: No Upgrade in Progress

Check for New Firmware Link

Click **Check for new firmware link** from any Advanced Setup screen to generate the **Upgrade firmware from Internet** screen. To upgrade the Gateway's firmware from the Internet automatically, click **Upgrade**.



Upgrade firmware from Internet.

To upgrade image form Internet automatically

Current Firmware Version: WST3K-31.164L.04

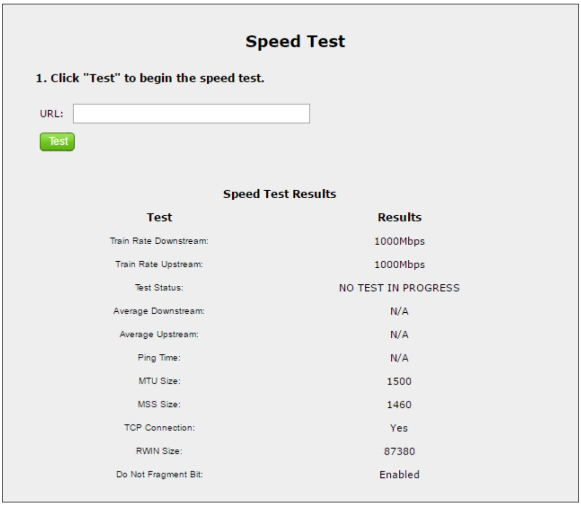
New Firmware Version:

Click Upgrade Firmware to begin the upgrade.

Upgrade Status: No Upgrade in Progress

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 server at a speed test site, then click **Test**.



Speed Test

1. Click "Test" to begin the speed test.

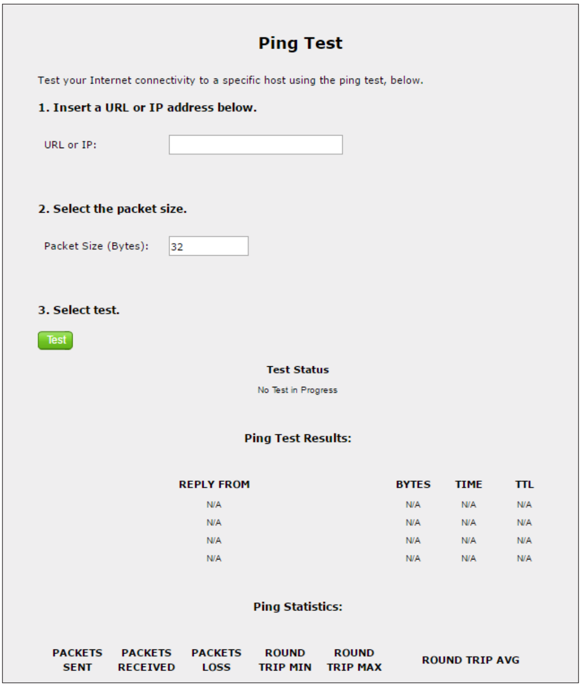
URL:

Speed Test Results

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): 32

3. Select test.

Test Status

No Test in Progress

Ping Test Results:

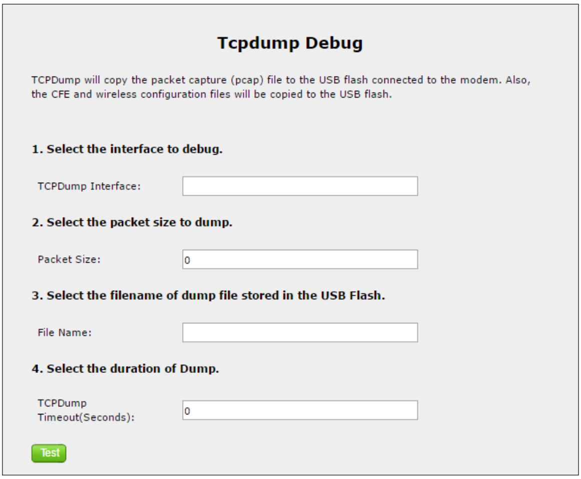
REPLY FROM	BYTES	TIME	TTL
N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A

Ping Statistics:

PACKETS SENT	PACKETS RECEIVED	PACKETS LOSS	ROUND TRIP MIN	ROUND TRIP MAX	ROUND TRIP AVG

Tcpdump Debug

Click Tcpdump Debug from any Advanced Setup screen to generate the Tcpdump Debug screen. This screen allows the user to copy the packet capture file to a USB flash drive connected to the Gateway, along with the CFE and wireless configuration files, for debugging purposes. Follow the onscreen instructions to complete.



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: 0

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

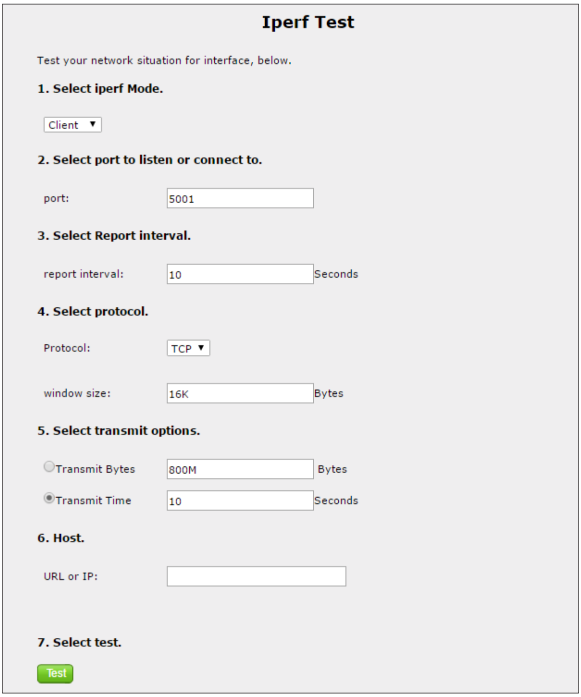
File Name:

4. Select the duration of Dump.

TCPDump Timeout(Seconds): 0

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: 5001

3. Select Report interval.

report interval: 10 Seconds

4. Select protocol.

Protocol: TCP ▼

window size: 16K Bytes

5. Select transmit options.

○ Transmit Bytes 800M Bytes

● Transmit Time 10 Seconds

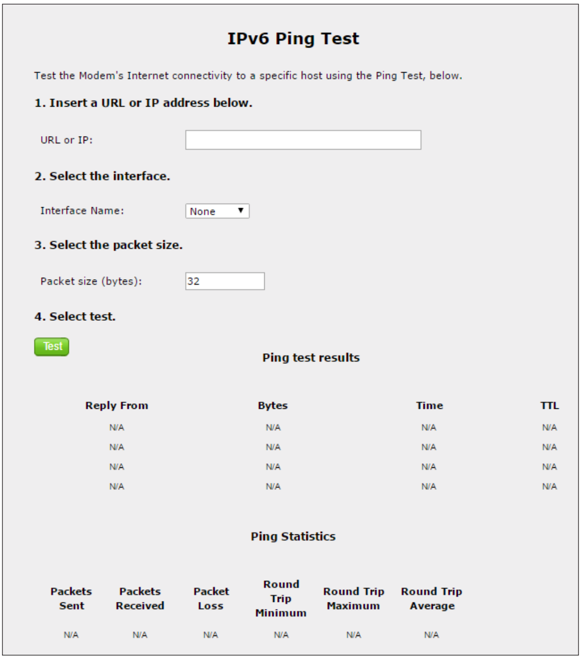
6. Host.

URL or IP:

7. Select test.

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: None

3. Select the packet size.

Packet size (bytes): 32

4. Select test.

Ping test results

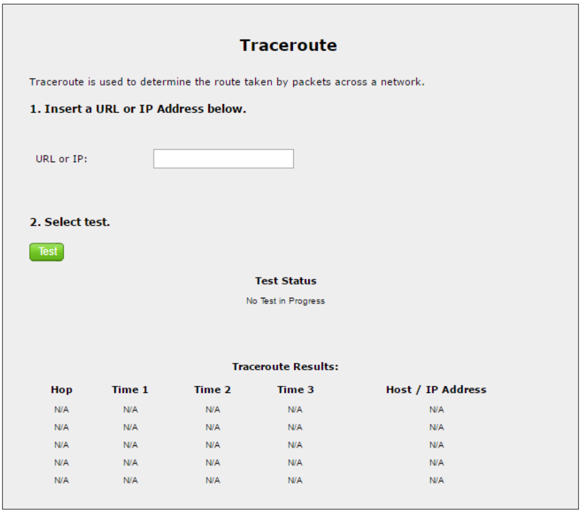
Reply From	Bytes	Time	TTL
N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A

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

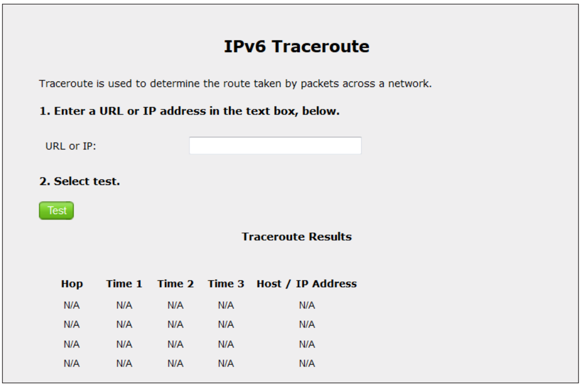
No Test in Progress

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:

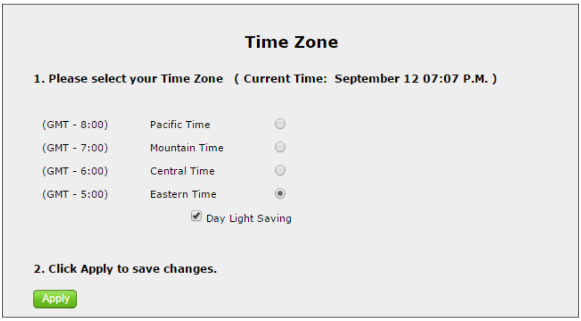
2. Select test.

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.



Time Zone

1. Please select your Time Zone (Current Time: September 12 07:07 P.M.)

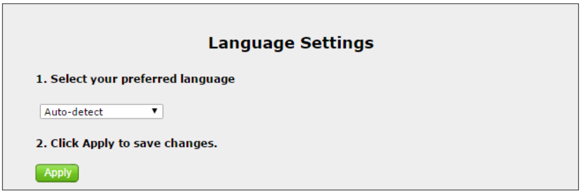
(GMT - 8:00)	Pacific Time	○
(GMT - 7:00)	Mountain Time	○
(GMT - 6:00)	Central Time	○
(GMT - 5:00)	Eastern Time	●

☑ Day Light Saving

2. Click Apply to save changes.

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.



Language Settings

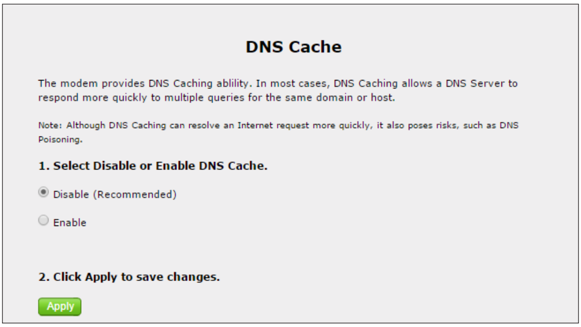
1. Select your preferred language

Auto-detect ▼

2. Click Apply to save changes.

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 ablility. 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.

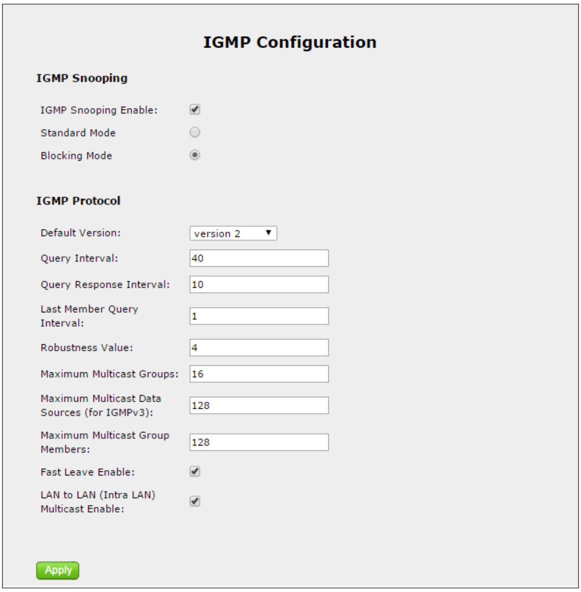
● Disable (Recommended)

○ Enable

2. Click Apply to save changes.

IGMP Setting

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



IGMP Configuration

IGMP Snooping

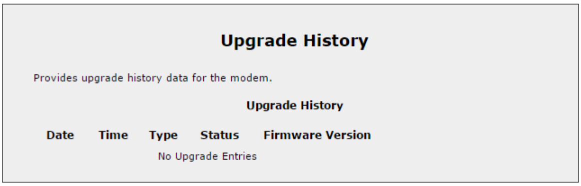
IGMP Snooping Enable: ☑
Standard Mode ○
Blocking Mode ●

IGMP Protocol

Default Version: version 2 ▼
Query Interval: 40
Query Response Interval: 10
Last Member Query Interval: 1
Robustness Value: 4
Maximum Multicast Groups: 16
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.



Upgrade History

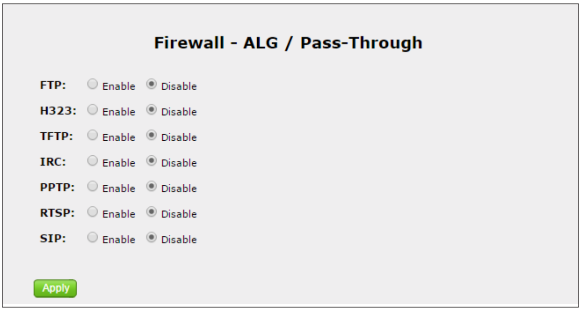
Provides upgrade history data for the modem.

Upgrade History

Date	Time	Type	Status	Firmware Version
No Upgrade Entries				

ALG

Click ALG from any Advanced Setup screen to generate the Firwall - ALG / Pass-Through screen. This screen allows the user to configure ALG settings on the Gateway.

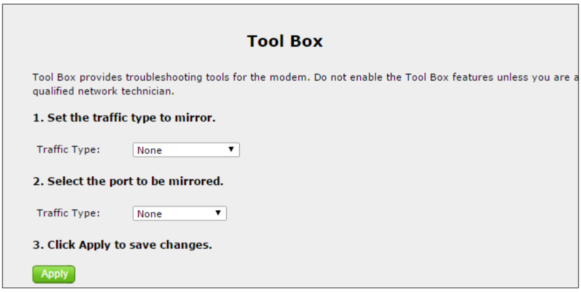


Firewall - ALG / Pass-Through

FTP:	○ Enable	● Disable
H323:	○ Enable	● Disable
TFTP:	○ Enable	● Disable
IRC:	○ Enable	● Disable
PPTP:	○ Enable	● Disable
RTSP:	○ Enable	● Disable
SIP:	○ Enable	● Disable

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.



Tool Box

Tool Box provides troubleshooting tools for the modem. Do not enable the Tool Box features unless you are a qualified network technician.

1. Set the traffic type to mirror.

Traffic Type: None ▼

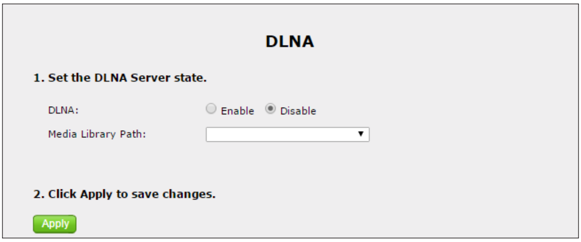
2. Select the port to be mirrored.

Traffic Type: None ▼

3. Click Apply to save changes.

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.



DLNA

1. Set the DLNA Server state.

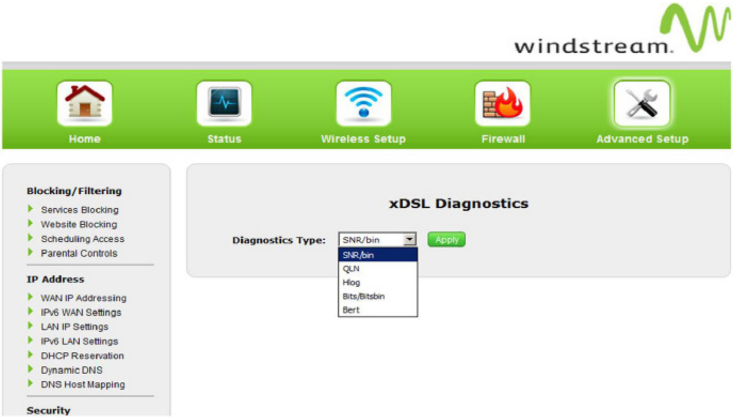
DLNA: ○ Enable ● Disable

Media Library Path: ▼

2. Click Apply to save changes.

xDSL Diagnostics

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

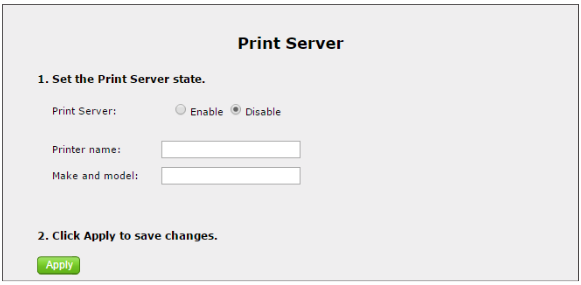


xDSL Diagnostics

Diagnostics Type: SNR/bin

Print Server

Click Print Server from any Advanced Setup screen to generate the Print Server screen. This screen allows the user to select and configure a print server for the Gateway's network.



Print Server

1. Set the Print Server state.

Print Server: ○ Enable ● Disable

Printer name:

Make and model:

2. Click Apply to save changes.

Specifications

A

General

Model Number(s)

T3280 (WiFi 6 Gateway Router with Bonded VDSL)

Standards

IEEE 802.3 (10BaseT)
IEEE 802.3u (100BaseTX) IEEE
802.11 b, g, n, ac, ax (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: 802.11a, b, g, n, ac, ax; 900 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

Model No. - CDS024T-W120U
Input - 120VAC, 50/60Hz, 0.58A
Output - 12.0VDC, 2.0A
Manufacturer - Actiontec

Environmental

Power

External, 12V DC, 2A

Certifications

FCC Part 15 Class B, Class C and E, FCC Part 68, UL

Operating Temperature

0º C to 45º C (32ºF to 113ºF)

Storage Temperature

-20ºC to 70ºC (-4ºF to 158ºF)

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
3301 Olcott St, Santa Clara, CA 95054, United States
Tel: (408) 752-7700

Actiontec®

FCC Part 68 User Manual Information Agreement

This equipment complies with Part 68 of the FCC rules. Located on the equipment is a label that contains, among other information, the ACTA registration number and ringer equivalence number (REN.) If requested, this information must be provided to the telephone company.

The REN is used to determine the quantity of devices which may be connected to the telephone line. Excessive REN's on the telephone line may result in the devices not ringing in response to an incoming call. In most, but not all areas, the sum of the REN's should not exceed five (5.0). To be certain of the number of devices that may be connected to the line, as determined by the total REN's contact the telephone company to determine the maximum REN for the calling area.

This equipment cannot be used on the telephone company-provided coin service. Connection to Party Line Service is subject to State Tariffs.

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. If advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right the file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make the necessary modifications in order to maintain uninterrupted service.

Actiontec®

If trouble is experienced with this equipment, please contact:

Company Name: Actiontec Electronics, Inc.
Address: 3301 Olcott St., Santa Clara, CA 95054, USA
TEL: 408-752-7700
FAX: 408-732-0087

If the trouble is causing harm to the telephone network, the telephone company may request you to remove the equipment from the network until the problem is resolved.

This equipment uses the following USOC jacks: RJ14

It is recommended that the customer install an AC surge arrester in the AC outlet to which this device is connected. This is to avoid damaging the equipment caused by local lightening strikes and other electrical surges.