



WiFi 6 Gateway Router with Bonded VDSL

Model # T3280V

User Manual



Table of Contents

1 Introduction	4
Package Contents	5
Minimum System Requirements	5
Features	5
Getting to Know the Gateway	6
Connecting the Gateway	9
2 Accessing the Home Screen	11
Accessing the Home Screen	11
Icon Bar	12
Connection Status	13
3 Checking the Gateway's Status	14
Accessing the Status Screens	14
Connection Status	15
Line 1/Line 2 Status	16
WAN Ethernet	17
Routing Table	17
Firewall Status	18
NAT Table	18
Wireless Status	19
Advanced Wireless Status	20
Wireless Monitor	20
Modem Utilization	21
LAN Status	21
ARP Table	22
Network Devices	22
Interface Statistics	23
Multicast Statistics	23
System Log	24
4 Configuring Wireless Settings	25
Accessing Wireless Settings	25
Basic Settings	26

Windstream T3280V Gateway

Advanced Settings	27
WPS	28
MAC Address Control	29
WDS	30
Band Steering	31
5 Configuring Firewall Settings	32
Accessing Firewall Settings	32
Firewall	33
IPv6 Firewall	34
Port Forwarding	35
Applications	36
DMZ Hosting	37
IPv6 DMZ Hosting	38
UPnP	39
5 Advanced Settings	40
Accessing the Advanced Setup Screens	40
Services Blocking	42
Website Blocking	42
Scheduling Access	43
Parental Controls	44
WAN IP Addressing	45
IPv6 WAN Settings	46
RFC1483 Transparent Bridge	47
LAN IP Settings	48
Static IP	49
IPv6 LAN Settings	50
DHCP Reservation	51
Dynamic DNS	52
DNS Host Mapping	53
IP QoS Upstream Settings	54
IP QoS Downstream Settings	55
IPv6 QoS	56
Remote GUI	57
Remote Telnet	57
Dynamic Routing	58
Admin Password	59
Storage Device Info	59

Windstream T3280V Gateway

Samba Configuration	60
Reboot	60
Restore Defaults	61
Upgrade Firmware	61
Check for New Firmware Link	62
Speed Test	62
Ping Test	63
Tcpdump Debug	64
Iperf Test	65
IPv6 Ping Test	66
Traceroute	67
IPv6 Traceroute	68
Time Zone	69
Language Settings	69
DNS Cache	70
IGMP Setting	71
Upgrade History	72
ALG	72
Tool Box	73
DLNA	73
xDSL Diagnostics	74
Print Server	75
GUI Setting to Activate VoIP	76
A Specifications	77
General	77
Wireless Operating Range	78
LED Indicators	78
Power Adapter	78
Environmental	79
Notices	80
Warranty	80
Important Safety Instructions	80
FCC Class B Equipment	81
Important Note on Wi-Fi	82
Contact Info	83

Introduction

Congratulations on purchasing the T3280V Wireless 11axBonded 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/LAN This 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.

Windstream T3280V Gateway

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. 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.

Introduction

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

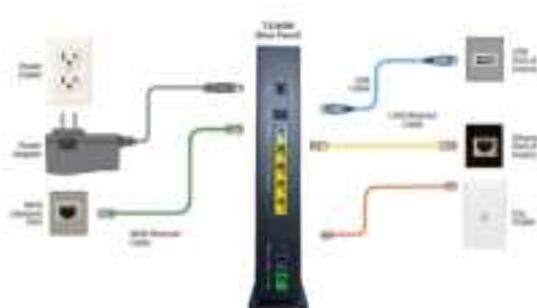
The USB port is used to connect the Gateway to a USB device.

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

Introduction

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.



2. The Gateway's Home screen appears.



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.

The screenshot displays the Home screen with three main sections: Summary, WAN Connection Status, Home Network, and Firewall.

Summary		Product Info		Login Status	
Internet Service Provider	Comcast	Model#	7120	You are currently logged in as root	
Version	2.0.0	Serial#	GC047099610	Logout	
Subscription Type	DSL 5M Fiber	MAC Address	8C:7E:30:3A:01		
DSL Link Up Time	8h	Device Version	7120-12.000.34		
Current Time	May 12 02:02:00	WAN Status	View Status		
	70%				

WAN Connection Status	
Link Type	Ethernet
Device MAC	8C:7E:30:3A:01
Router IP Address	192.168.1.1
Default GW	192.168.1.1
Default Gateway	192.168.1.1
Link Up Time Remaining	20:07:53
DNS Address #1	192.168.1.1
DNS Address #2	4.2.2.4

Home Network	
Internet	Connected 192.168.1.1
WiFi	Connected 192.168.1.1

Firewall	
UPnP Status	Enabled
Packet Filter	Enabled
Block Ping	Disabled

Diagnose & Login Required	
Ping	
Traceroute	
Website Ping	
Device Ping	
Factory Reset	
DOX Release/Reboot	

Checking the Gateway's Status

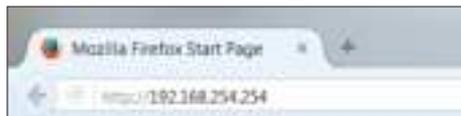
3

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:

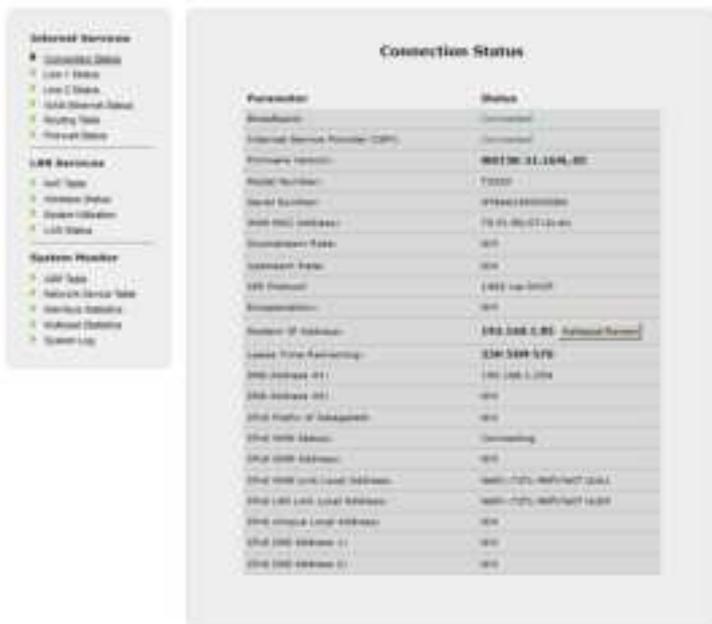
1. Open a Web browser. In the *Address* text box, type:
<http://192.168.254.254>
then press **Enter** on the keyboard.



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



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



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.

Checking the Gateway's Status

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** generates the *Line 2 Status* screen, which displays the connection parameters for the Gateway's *DSL Line 2* port.

Line 1 Status	
Connection	Status
Gateway Broadband	Disconnected
Gateway Status Provider	Disconnected
PPP Parameters	
Status	
Link Name	N/A
Link Type	N/A
Link State	Down
Link Speed	Down
Authentication Protocol	0
Session Time	0 Days, 00h:00m:00s
Remote Name	N/A
Remote Password	N/A
Remote Username	0 Days, 00h:00m:00s
PPP Mode	N/A
DSL Link	
Status	
DSL Link Name	0 Days, 00h:00m:00s
Name	N/A
Name of Link ID Name	N/A
Link ID Provider Name	N/A

Line 2 Status	
Connection	Status
DSL Provider	Disconnected
DSL Status Provider	Disconnected
PPP Parameters	
Status	
Link Name	N/A
Link Type	N/A
Link State	Down
Link Speed	Down
Authentication Protocol	0
Session Time	0 Days, 00h:00m:00s
Remote Name	N/A
Remote Password	N/A
Remote Username	0 Days, 00h:00m:00s
PPP Mode	N/A
DSL Link	
Status	
DSL Link Name	0 Days, 00h:00m:00s
Name	N/A
Name of Link ID Name	N/A
Link ID Provider Name	N/A

WAN Ethernet

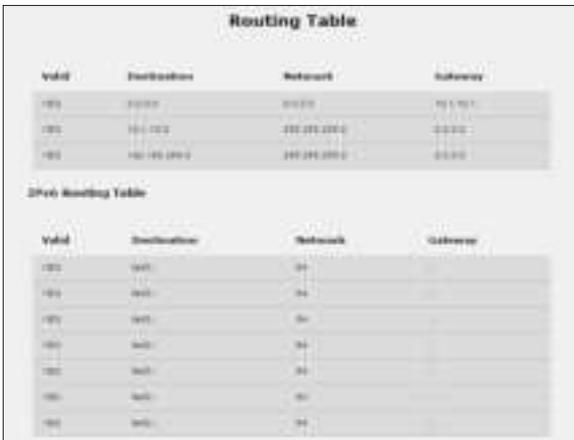
Click **WAN Ethernet Status** from any Status screen to generate the *WAN Ethernet Status* screen. This screen displays the Gateway's WAN (wide area network) parameters.



Parameter	Status
Connected	Connected
Gateway Service Provider	Connected
WAN Interface	7047636007-45000
IP Address	10.0.10.100
Default Mask	255.255.255.0
Default Gateway	10.0.10.1
Link Layer Name	001.230.499.190
WAN Speed	10,70,15,70,70,70,70,70
Operational System	30001
Serial Number	10204
Time Zone	EST (UTC-05:00)
System	Full
Link Speed	10000

Routing Table

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



Vcid	Destination	Network	Gateway
100	0.0.0.0	0.0.0.0	10.0.10.1
100	10.0.10.0	255.255.255.0	0.0.0.0
100	10.0.10.0/24	255.255.255.0	0.0.0.0

IPv6 Routing Table

Vcid	Destination	Network	Gateway
100	::	::	
100	::	::	
100	::	::	
100	::	::	
100	::	::	
100	::	::	

Wireless Status

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



The screenshot shows the 'Wireless Status' page. At the top, there is a 'Select SSID' dropdown menu with 'WiFi_1000000' selected. Below this is a note: 'The wireless network SSID of SSID Field may differ from this.' The main content is a table with two columns: 'Parameter' and 'Status'. The table lists various wireless settings and their current states. At the bottom of the page, there are three green buttons: 'Refresh Wireless Status', 'Refresh Wireless Parameters', and 'Refresh Wireless SSID'.

Parameter	Status
Radio	Enabled
SSID	Enabled
Security	Enabled
SSID	WiFi_1000000
Channel Selection	Auto
Channel	112
Wireless Network Type	WiFi (P) P2P
SSID Broadcast	Enabled
SSID Authentication	Disabled
Channel Width	Compatible Mode (802.11a+802.11n+802.11ac)
WPA State	Disabled
WPA Type	WPA2 PSK, WPA, and WPA3 PSK
WPA Key	Enabled
WPA Pre-Shared Key	Enabled
Wireless Network Name	WiFi
Wireless Network Password	0

[Refresh Wireless Status](#)
[Refresh Wireless Parameters](#)
[Refresh Wireless SSID](#)

Checking the Gateway's Status

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

Items	Values
ESSID	72 F1 94 07 8E 94
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:

Parameter	Status
Macaddr	72F194078E94
Mac	72 F1 94 07 8E 94
SSID	---
Connection Status	100 g
Priority used	28408
Planned Services	20180
Priority list	507
WPA user	1 of 10000
WPA2 group user	104
Disconnection	0/0

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 Sessions	1000/1000
Memory Usage	80%
Memory Status	OK
Recommended Action	None
Maximum Number of Sessions	1000
Used TCP Sessions	0
Used UDP Sessions	0
Modem Capabilities	OK
Power Cycle Sessions	0
Session Status	OK
Recommended Action	None

LAN Device Session Log		
Device Name	IP Address	No. of Open Sessions
 192.168.1.10	192.168.1.10	0

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	100Mbps	1000	1000
Ethernet	2	100Mbps/100Mbps	100	100
Ethernet	3	100Mbps/100Mbps	100	100
Ethernet	4	100Mbps/100Mbps	100	100
WiFi	1	100Mbps/100Mbps	100	100

Interface	Hostname	MAC Address	IP Address	Port	Connection Speed	Last Time Knowning
Ethernet	192.168.1.10	08:00:27:00:00:00	192.168.1.10	1	100Mbps	10/10/2010

Interface	MAC Address	IPv4 Subnet	IPv4 Address
-----------	-------------	-------------	--------------

Checking the Gateway's Status

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.



IP Address	HW Type	Flags	HW Address	Mask	Device
192.168.1.14	eth	0.0	00:0c:29:1c:14:14	-	eth0
192.168.1.1	eth	0.0	00:0c:29:1c:14:11	-	eth0

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

Build Screen: Enable Disable

Scan Interval: Minutes

Ethernet Devices:  00:20

Wireless Devices: 

 **Wireless**  00:20

 **Wireless**  00:20

Configuring Wireless Settings

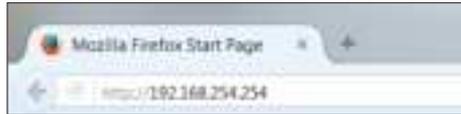
4

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.



Windstream T3280V 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 *Basic Settings* 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.

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**.

Configuring Wireless Settings

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.



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.



The screenshot shows the 'WPS (Wi-Fi Protected Setup)' configuration screen. At the top, it says 'WPS provides an easy and secure way to establish a wireless network by sharing the wireless key between the modem and wireless client.' Below this, there are two radio buttons for 'Frequency': '92' (selected) and '2.4G'. Underneath is a 'Select SSID' dropdown menu with 'WINS_70000E' selected. The screen is divided into two numbered steps: '1. Set the WPS state.' with radio buttons for 'Enable' and 'Disable' (selected), and '2. Click Apply to save changes.' with a green 'Apply' button.

Configuring Wireless Settings

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:

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: or

(Example MAC Address: 00:2D:e0:00:4E:00)

5. Click Apply to save changes.

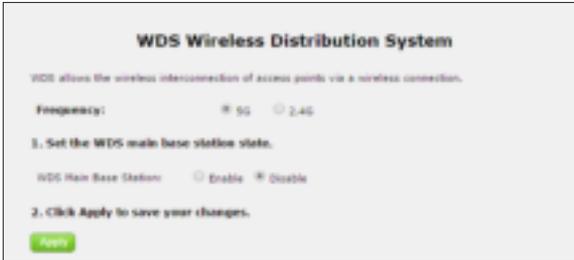
MAC Authentication Device List

DEVICE NAME	IP ADDRESS	MAC ADDRESS	ACCESS	EDIT
No Entries Defined				

Configuring Wireless Settings

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.

Apply

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.



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.



Configuring Firewall Settings

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 selected functionality may be lost.

1. Select the security mode state. When **enable** mode is enabled, the monitor will not respond to unsolicited WAN traffic, including ping.

Health 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:

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

Service	Service Type	Service Port	Traffic In	Traffic Out
SSH	Secure Shell	22 (Port 22) (TCP, UDP, ICMP, SCTP, DCCP)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
SSH	SSH	22	<input type="checkbox"/>	<input checked="" type="checkbox"/>
FTP	File Transfer	20, 21	<input type="checkbox"/>	<input checked="" type="checkbox"/>
FTS	Secure File Transfer	22	<input type="checkbox"/>	<input checked="" type="checkbox"/>
HTTP	HTTP	80	<input type="checkbox"/>	<input checked="" type="checkbox"/>
HTTPS	Web Services	443	<input type="checkbox"/>	<input checked="" type="checkbox"/>
SMTP	Secure Mail Services	25	<input type="checkbox"/>	<input checked="" type="checkbox"/>
SMTPS	Web Services	465	<input type="checkbox"/>	<input checked="" type="checkbox"/>
IMAP	Mail Services	143	<input type="checkbox"/>	<input checked="" type="checkbox"/>
IMAPS	Mail Services	993	<input 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:

LAN IP Address:

External (WAN) Start Port:

External (WAN) End Port:

Internal (LAN) Start Port:

Internal (LAN) End Port:

Protocol:

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 Forwarded ports to the selected IP address 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: all
Application: click on the table **Apply**

3. Click **Apply** to save changes.

Apply

Forwarded Applications List

SERVICE NAME	IP ADDRESS	APPLICATION FORWARDED	PORT
<small>No entries found</small>			

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 router's WAN IP address as its own. DMZ places the LAN device outside the firewall.

WARNING: Using a device as DMZ host creates a security risk by exposing the device to outside attacks.

1. Set the DMZ state:

DMZ Enable Disable

2. Select a device:

Select Device: Enter IP Address:

3. DMZ Times:

DMZ Times:

4. Click Apply to save changes.

DMZ Hosted Device

DEVICE NAME	IP ADDRESS	DMZ Times	EDIT
No DMZ Entries			

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

The screenshot shows the UPnP configuration page. At the top, it says "UPnP" and "Adjust the options below to enable or disable UPnP (Universal Plug and Play)". Below this, there are two main sections:

- 1. Set the UPnP state.**
 - UPnP: Enable Disable
 - UPnP Copy: Enable Disable
 - UPnP Profile: Keep only Load with
- 2. Click Apply to save changes.**

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

Advanced Settings

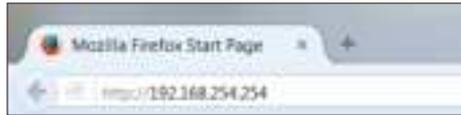
6

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.



Windstream T3280V Gateway

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



4. The Services Blocking screen appears.



Advanced Settings

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 a web interface titled "Website Blocking". Below the title, there is a sub-heading "Website Blocking" and two numbered instructions: "1. To block a specific website, enter the website address (such as www.abc.com) in the text box below." and "2. Click Apply to save changes." A text input field labeled "Website Address:" is provided. Below the instructions, there is a green "Apply" button. Underneath, the text "Blocked Websites" is displayed, followed by a table with two columns: "Website Blocked" and "EDIT". The table currently contains one row with the text "No Entries Default" centered under the "Website Blocked" column.

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 Dates allows the router to set a specific time period during which a computer on the network can access the internet.

1. Select Device.

Device Name: Enter MAC Address:

Manually enter the MAC address.

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

4 checked box specifies access allowed:

Sun Mon Tue Wed Thu Fri Sat

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

From: To:

4. Click Add to create device schedule.

Device Access Restrictions List

Device Name	MAC Address	Allowed Days	Allowed Times	1/01
<small>No Entries Defined</small>				

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.



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. Connect WAN interface to WAN Ethernet.

2. Select the ISP protocol below.

PPPoE

RFC 3493 via DHCP

RFC 3493 via Static IP

3. If your ISP Provider requires Host Name/Domain Name, enter it here.

Host Name:

Domain Name:

4. Select the DNS type.

Dynamic DNS Addresses (Default)

Static DNS Addresses

Primary DNS:

Secondary DNS:

5. Configure DUMP Proxy.

Enable

Disable

7. Enter the VLAN parameters.

VLAN ID: (0 - 4096)

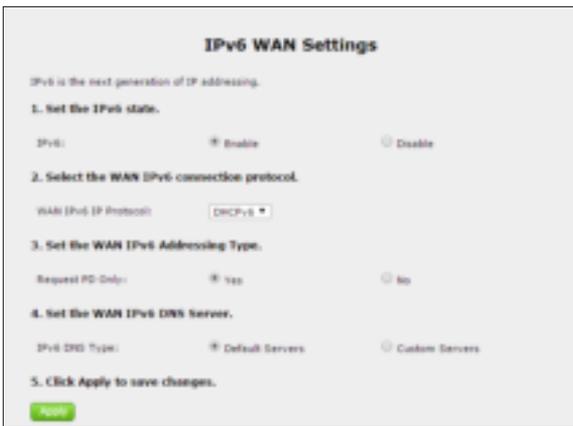
VLAN Priority: (0 - 7)

8. 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.



The screenshot shows the 'IPv6 WAN Settings' configuration screen. It includes a title, a brief introduction, and five numbered steps with corresponding radio button options and a dropdown menu. A green 'Apply' button is located at the bottom left.

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:

3. Set the WAN IPv6 Addressing Type.

Request PG 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 T3280V 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.

The screenshot shows the Windstream T3280V Gateway's configuration interface. At the top, there is a navigation bar with icons for Home, Status, Wireless Setup, Firewall, and Advanced Setup. The main content area is titled "WAN IP Address" and contains the following sections:

- Blocking/Filtering**
 - Services Blocking
 - Website Blocking
 - Subvending Access
 - Parental Controls
- IP Address**
 - WAN IP Addressing (selected)
 - IPv6 WAN Settings
 - LAN IP Settings
 - IPv6 LAN Settings
 - DHCP Reservation
 - Dynamic DNS
 - CN3 Host Mapping
- Security**
 - Admin Password
- Storage Service**
 - Storage Device Info
 - Samba Configuration
- Network Utilities**
 - Reboot
 - Restore Defaults
 - Upgrade Firmware
 - Check for new firmwares link
 - Speed Test
 - Ping Test
 - Topology Debug
 - Iperf Test
 - IPv6 Ping Test
 - Traceroute
 - IPv6 Traceroute
 - Time Zone
 - Language Settings
 - DNS Cache
 - IGMP Setting
 - Upgrade History
 - AIG
 - Tool Box
 - DHNA
 - xDSL Diagnostics

The "WAN IP Address" configuration page includes the following steps and options:

- Current WAN interface is WAN Ethernet.**
- Select the ISP protocol below.**
 - PPPoE
 - RFC 1483 Transparent Bridging
 - RFC 1483 via DHCP
 - RFC 1483 via Static IP
- Enter your PPP username and password.**
 - PPP Username:
 - PPP Password:
- Select the DNS type.**
 - Dynamic DNS Addresses (Default)
 - Static DNS Addresses
 - Primary DNS:
 - Secondary DNS:
- Configure IGMP Proxy.**
 - Enable
 - Disable
- Enter the VLAN parameters.**
 - VLAN ID: (-1 -- 4094)
 - VLAN Priority: (0 -- 7)
- Click Apply to save changes.**

A green "Apply" button is located at the bottom left of the configuration area.

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

Internet connectivity may be lost due to default LAN IP address of the device. You should modify the LAN IP address and DHCP server settings to avoid such issues. These changes will be implemented after a reboot of the device. Please refer to the instructions below.

1. To make changes, enter the new IP address or subnet mask of the router in the field below.

Public IP Address:

Public Subnet Mask:

2. Click Apply and Reboot to save your changes.

The router is configured with the LAN IP address to establish a local network.

3. Set the IP addressing values.

Starting IP Address:

End IP Address:

Subnet Mask:

4. Set the DHCP server lease time.

IP Lease Lease Time: Hours Hours Minutes

5. Set the DNS values.

Use DNS 1

DNS relay performed by address 192.168.234.2

DNS relay from WAN interface

Name server address:

Use DNS 2

DNS relay performed by address 192.168.234.2

DNS relay from WAN interface

Name server address:

6. Click Apply to save changes.

How to Set the T3280V 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.

The screenshot shows the Windstream T3280V Gateway's configuration interface. At the top, there is a green navigation bar with icons for Home, Status, Networking (selected), Services, and Administrative Status. The main content area is titled "WAN IP Address" and contains the following steps and fields:

- WAN IP Addressing** (Note: IP addressing on this screen must be done prior to creating a WAN.)
- 1. Connect WAN Interface to WAN Ethernet.**
- 2. Select the IP protocol below.**
 - DHCP
 - 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 Address (Default)
 - Static DNS addresses
 - Primary DNS:
 - Secondary DNS:
- 5. Configure NAT type.**
 - Enable
 - Disable
- 6. Enter the VLAN parameters.**
 - VLAN ID: (1 - 4094)
 - VLAN Priority: (0 - 7)
- 7. Click Apply to save changes.** (A green "Apply" button is visible at the bottom left of the main content area.)

On the left side of the screen, there is a sidebar menu with the following categories and items:

- Monitoring / Filtering**
 - Security Monitoring
 - Network Monitoring
 - Subsidiary Access
 - Routing Control
- IP Address**
 - WAN IP ADDRESSING** (Selected)
 - IPv4 IPv6 Settings
 - LAN IP Settings
 - IPv4 LAN Settings
 - IPv6 LAN Settings
 - DHCP Configuration
 - Dynamic DNS
 - DNS Host Mapping
- Security**
 - Access Placement
- Storage Settings**
 - Storage Overview
 - Access Configuration
- Network Utilities**
 - Router
 - Network Controls
 - Applicable Protocols
 - Check for new firmware (W)
 - Speed Test
 - Ping Test
 - Traceroute/Tracert
 - port Test
 - Port Ping Test
 - Forward
 - port Forward
 - Time Sync
 - Language Settings
 - QoS Config
 - QoS Setting
 - Upgrade Router
 - SLC
 - Tool Box
 - FAQ
 - 404 Error

Advanced Settings

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 interface. It includes a title, a brief description of IPv6, and four numbered steps for configuration. Step 1 involves selecting the LAN connection type. Step 2 involves setting addressing values, including prefix length, global address, LAN support, subnet mask, and router advertisement. Step 3 is for advanced settings, such as enabling DHCP. Step 4 is a final instruction to click 'Apply' to save changes. A green 'Apply' button is visible at the bottom left.

IPv6 LAN Settings

IPv6 is the next generation of IP addressing.

1. Set the IPv6 LAN connection type.

LAN Connection Type:

2. Set the IPv6 LAN addressing values.

Prefix length:

Global unicast address:

LAN Support: Enable IPv6 Support

Subnet Mask:

Router advertisement (offered): No (Default) Yes

3. Advanced setting.

Configured 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.

- Select MAC Address, or manually enter a MAC address.**
Select MAC Address: ▾
Manually Add MAC Address:
- Select an IP address to associate with a MAC address.**
IP Address: ▾
Manually Add IP Address:
- Click Apply to save changes.**

Advanced Settings

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 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. IPv4 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

Adding 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 performance and prevent your network from becoming overloaded. Refer to the 3.0 Setup to setup IP QoS.

I. Specify Classification Name and Order.

Traffic Class Name:

Rule Order:

II. Specify Classifications (Leave blank if criteria is not used for classification).

Input Interface:

Other Type:

Source IP address:

Source IP Mask:

Destination IP address:

Destination IP Mask:

III. Specify Classification Action.

Assign Classification Queue:

Mark Differentiated Service Code Point (DSCP):

Remark DSCP to priority code for VoIP (Rate priority):

Mark DSCP DSCP (only for VoIP Rate priority):

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) versus standard data traffic. Traffic sharing your network with QoS can also increase application performance and prevent your network from becoming overloaded. Follow Steps 1-3 below to setup IP QoS.

1. Specify Classification Name and Status

Traffic Class Name:

Run Status:

2. Specify Classification Name (Make it criteria to be used for classification)

Ingress Direction:

Filter 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 DSCP to priority (only for VoIP Same as throughput):

Remark CLAT (D-4004) (only for VoIP Same as throughput):

Downstream QoS Rules List

Advanced Settings

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
Egress 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 50540 for HTTPS access. If port 50540 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:
3. Set the remote management timeout.
Disable Remote Management After:
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:
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

RIP

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:

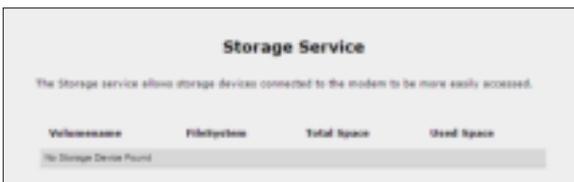
New Password:

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.

Volume Name	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.



The screenshot shows the 'Samba Configuration' screen. At the top, it says 'Samba Configuration'. Below that, there are two radio buttons: 'Enable' (selected) and 'Disable'. Underneath, there are four input fields: 'Samba Username:' with the value 'admin', 'Samba Password:' with masked characters '*****', 'Samba Share:' with a dropdown menu, and 'Workgroup:' with the value 'workgroup'. A green 'Next' button is located at the bottom left of the form area.

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. At the top, it says 'Reboot Modem'. Below that, there is a line of text: 'To restart the modem, click Reboot.' At the bottom, there is a button labeled 'Reboot Modem' with a green highlight on the right side.

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.



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.



Advanced Settings

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.



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.



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 by a specific test using the ping test below.

1. Select a DNS or IP address below.

URL or IP:

2. Select the packet size.

Packet Size (Bytes):

3. Select test.

Test Status
To Test Process

Ping Test Results:

REPLY FROM	BYTES	TIME	TTL
***	32B	34B	64B
***	32B	34B	64B
***	32B	34B	64B
***	32B	34B	64B

Ping Statistics:

PACKETS SENT	PACKETS RECEIVED	PACKETS LOSS	RX/RX%	RX/RX%	RX/RX% TRIP AVG
--------------	------------------	--------------	--------	--------	-----------------

Advanced Settings

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

- Select the interface to debug.**
Tcpdump Interface:
- Select the packet size to debug.**
Packet Size:
- Select the filename of debug file stored in the USB flash.**
File Name:
- Select the duration of debug.**
Tcpdump Timeout(Denials):

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 connection for throughput, latency.

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 ▾

remote addr: 100 Bytes

5. Select Transfer options.

Transfer Bytes: 1000 Bytes

Transfer Time: 10 seconds

6. Host.

URL or IP:

7. Select test.

Advanced Settings

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 feature.

1. Insert a IPv6 or IP address below:

IPv6 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
192...	128	0.00	64
192...	128	0.00	64
192...	128	0.00	64
192...	128	0.00	64

Ping Statistics:

Packets Sent	Packets Received	Packet Loss	Round Trip Minimum	Around Trip Maximum	Around Trip Average
100	100	0%	0.00	0.00	0.00

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
Not in Progress

Traceroute Results

Hop	Time 1	Time 2	Time 3	Host / IP Address
100	100	100	100	100
100	100	100	100	100
100	100	100	100	100
100	100	100	100	100
100	100	100	100	100

Advanced Settings

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

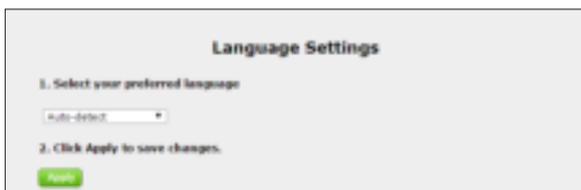
Time Zone

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.



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.



Advanced Settings

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 receive 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.

The screenshot shows the 'IGMP Configuration' screen with the following settings:

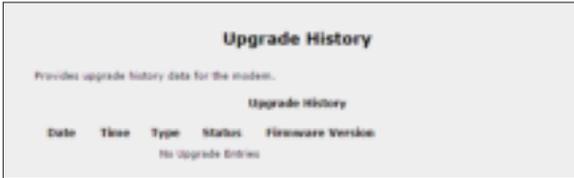
- IGMP Snooping**
 - IGMP Snooping Enable:
 - Standard Mode:
 - Blocking Mode:
- IGMP Protocol**
 - Default Version:
 - Query Interval:
 - Query Response Interval:
 - Load Member Query Interval:
 - Robustness Variable:
 - Maximum Multicast Groups:
 - Maximum Multicast Table Entries (for IGMPv2):
 - Maximum Multicast Group Members:
 - Fast Leave Enable:
 - IGMP to ILL (IGMP LAG) Multicast Enable:

A green 'Save' button is located at the bottom left of the configuration area.

Advanced Settings

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.



ALG

Click ALG from any Advanced Setup screen to generate the Firewall - ALG / Pass-Through screen. This screen allows the user to configure ALG settings 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, it says 'Tool Box' and provides a warning: 'Tool Box provides troubleshooting tools for the modem. Do not enable the Tool Box features unless you are a qualified network technician.' Below this, there are three numbered instructions: 1. Set the traffic type to mirror. 2. Select the port to be mirrored. 3. Click Apply to save changes. The first instruction is followed by a 'Traffic Type' dropdown menu with 'None' selected. The second instruction is followed by another 'Traffic Type' dropdown menu with 'None' selected. At the bottom left, there is a green 'Apply' button.

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, it says 'DLNA'. Below this, there are two numbered instructions: 1. Set the DLNA server state. 2. Click Apply to save changes. The first instruction is followed by a 'DLNA' section with two radio buttons: 'Disable' and 'Enable', with 'Enable' selected. Below the radio buttons is a 'Media Library Path' field with a text input box and a dropdown arrow. At the bottom left, there is a green 'Apply' button.

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.



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.



The screenshot shows a web-based configuration interface titled "Print Server". It contains the following elements:

- Section 1:** "1. Set the Print Server state." with a "Print Server:" label and two radio buttons: "Enable" (unselected) and "Disable" (selected).
- Form Fields:** Two text input fields labeled "Printer name:" and "Make and model:".
- Section 2:** "2. Click Apply to save changes." with a green "Apply" button.

Specifications



General

Model Number(s)

T3280V (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

0° C to 40° C (32°F to 104°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 comply 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



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 to 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.



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.

Federal Communications Commission (FCC) Interference Statement

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 generate, 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 to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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

(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

RF exposure warning

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 25 cm between the radiator & your body.