

WiFi 6 Gateway Router with Bonded VDSL

Model # T3280



0535-0137-000

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

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 Q0S	56
Remote GUI	57
Remote Telnet	57
Dynamic Routing	58
Admin Password	59
Storage Device Info	59

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
A Specifications	76
General	76
Wireless Operating Range	77
LED Indicators	77
Power Adapter	77
Environmental	78
Notices	79
Warranty	79
Important Safety Instructions	79
FCC Class B Equipment	80
Important Note on Wi-Fi	81
Contact Info	82

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

Introduction

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. 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 autosensing ports, and either a straight-through or crossover Ethernet cable can be used when connecting to the ports.

USB Port

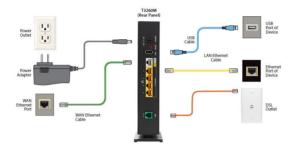
The USB port is used to connect the Gateway to a USB device.

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

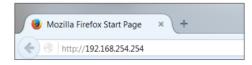
This chapter gives a short overview of the Home screen of the Gateway's graphical user interface (GUI).

Accessing the Home Screen

To access the Home screen:

 Open a Web browser on computer connected, via Ethernet cable, to one of the Gateway's LAN ports. In the *Address* text box, type: <u>http://192.168.254.254</u>

then press **Enter** on the keyboard.



2. The Gateway's Home screen appears.

				windstream.
Home	Statu:	y Wirele	ss Setup	Firewall Advanced Setup
Summary Internet Service Provider: Wireless: System Up Time: DSL Link Up Time: Current Time:	Connected Enabled 1 Client Connected 0d, 0h, 18m	Product Info Model#: Serial#: MAC Address: Firmware Version: Language:	T3260 GCBA8100100020 9C:1E:95:03:AC:81 T3260:32:165L:34 Auto-detect	Login Status You are currently logged in as: root Log not
Dynamic/Static: I Modem IP Address: Subnet Mask: Default Gateway: Lease Time Remaining: DNS Address #1:	Ethernet Dynamic 192.168.0.17 255.255.255.0 192.168.0.1	Home Network	Connected 192.168.254.50 Connected 192.168.254.64	Firewall UPhP Seting: Esabled Firewalt: Medium Biocolog/Filenig: Disabled Diagnostics - Login Required Prog
Wireless SmartSteering™: SSID 2.4G + 5G	4.2.2.4 Enabled WIN 100020			Traceroute Wireless Reset Device Reboot Factory Rest DHCP Release/Renew
Security:	Enabled WPA2-AES			

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.

	Product Inf	0		Login S	Status	
Connected Enabled 1 Client Connected 0d, 0h, 18m NA May 15 2020 02:56 RM.		n:	T3260 GCBA8100100020 9C:1E:95:03:AC:81 T3260-32:165L.34 Auto-detect v		_	root
Status	Home N	etwork		F	irewall	
Ethernet Dynamic 192.168.0.17 255.255.255.0			Connected 192.168.254.50 Connected	F	irewall:	Enabled Medium Disabled
192.168.0.1 23H 57M 5S 192.168.0.1	÷		192.168.254.64		-	ogin Required
4.2.2.4				v	Vireless Reset	
Enabled				F	actory Reset	w
WIN_100020 Enabled NVPA2-AES						
	Enabled 1 Client Connected od, 0n, 18m NA May 15 2020 02:56 PM. Status	Connected Model#: Enabled Serial#: 1 Clent Connected MAC Address: MA Address: Firmware Versio Language: Status	Connected Uodel#: Enabled Serial: 1 Cleat Connected MAC Address: WA May 15 2020 02:56 Class Connected MAC Address: Firmware Version: WA May 15 2020 02:56 Class Connected MAC Address: Firmware Version: WA May 15 2020 02:56 Class Connected MAC Address: Firmware Version: WA Language: L	Connected Model#: 73260 Enabled MAC Adverse: GCBA10010020 JCLent Connected MAC Adverse: GCBA102010020 MA May 15 2020 02:56 Firmware Version: J3260 32:165.134 Auto-detect Improve Version: Auto-detect Status Improve Version: 192:163.254.50 Status Improve Version: 192:163.254.50 Status Improve Version: 192:163.254.64 Status Improve Version: Improve Version: Status Improve Version:	Connected Model#: T3280 You are of GCRA8100100020 Intent Connected MAC Address: GCRA8100100020 MA Emmode Version: T3280 S2.168.124 MA May 15 2020 02:56 Language: Auto-detect → Status Home Network 192.168.254.50 Status Improve Version: 192.168.254.50 Status Phone Connected 192.168.0.1 192.168.254.64 Improve Version: Status Improve Version: 192.168.254.64 Status Improve Version: Improve Version: Status Improve Connected 192.168.254.64 Status Improve Version: Improve Version: Status Improve Connected 192.168.254.64 Status Improve Version: Improve Version: Status Improve Connected Improve Version: Status Improve Version: Improve Version: Status Improve Connected Improve Version: Status Improve Version: Improve Version: Status Improve Version: Improve Version: Status Improve Version: Improve Version: Improve Version: Improve Version: Improve Version: Improve Ve	Connected Model#: T3260 You are currently logged in as Indext Connected Status GCRAB100100020 Connected NA Firmware Version: T3260 Connected May 15 2020 02:56 Firmware Version: T3260-02:56 Connected Status Home Network Firmware Version: T3260-02:56 Status Image: Auto-detect WIP 5 billing: Status Image: Image: Connected Status Image: Image: Connected Status Image: Image: Connected Status Image: Image: Connected Status Image: Image: Image: Status Image: Image: Connected Status Image: Image: Image: Status Image: Image: Image: Status Image: Image: Connected Status: Image: Image: Image: Status: Image: Image: Image: Status: Image: Image: Image: Status: Image: Image: Image: Status: Image: Image: Image:

Checking the Gateway's Status



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

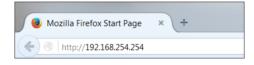
Accessing the Status Screens

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 Line 1 Status					
Line 2 Status WAN Ethernet Status	Parameter	Status			
Routing Table	Broadband:	Connected			
Firewall Status	Internet Service Provider (ISP):	Connected			
AN Services	Firmware Version:	WST3K-31.164L.05			
NAT Table	Model Number:	Т3200			
Wireless Status	Serial Number:	GTBA6190500086			
Modem Utilization LAN Status	WAN MAC Address:	70:f1:96:07:2c:b1			
	Downstream Rate:	N/A			
ystem Monitor	Upstream Rate:	N/A			
ARP Table Network Device Table	ISP Protocol	1483 via DHCP			
Interface Statistics	Encapsulation:	N/A			
Multicast Statistics System Log	Modem IP Address:	192.168.1.85 Release/Renew			
System Log	Lease Time Remaining:	23H 56M 575			
	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				
РРР Туре:	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				
Modern Uptime:	0 Days, 00H:00M:005				
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 Douar Link Esiliuras	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:	75.75.75.75.75.76.76			
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		
YES	192.168.254.0	255.255.255.0	0.0.0.0		
Pv6 Routin Valid		Netmask	Gateway		
Vo Routin Valid	ng Table Destination	Netmask 64	Gateway		
Valid	Destination				
Valid YES	Destination fe80::	04			
Valid YES YES	Destination fe80:: fe80::	04 04			
Valid YES YES YES	Destination fe80:: fe80:: fe80::	84 84 84			
Valid YES YES YES	Destination fe80:: fe80:: fe80:: fe80::	84 84 84 84			

Firewall Status

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

		Firew	all Status
The list belo	w displays all firewall	settings modif	fied 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	218.58.194.208	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	
0	24	192.108.254.04	49013	216.58.195.78	443	
17	16	192.168.254.64	123	40.78.58.209	123	
8	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	
8	22	192.168.254.64	49572	218.58.193.78	443	
8	21590	192.168.254.64	49670	218.58.194.174	443	
8	21	192.168.254.64	49602	216.58.195.78	443	
6	24	192.168.254.64	49577	216.58.194.206	443	
0	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.

Select SSID	
SSID:	WIN5_700005 T
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 Statistics	

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	9 5G 0 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	Sta	tus		
Total Memory:	1921	MB RAM		
Memory Used:	50%	6		
Memory Status:	ок			
Recommended Action:	NON	Æ		
Maximum Number of Sessions:	1800	00		
LAN TCP Sessions:	2			
LAN UDP Sessions:	0			
Modem Sessions:	11			
Total Open Sessions:	14			
Session Status:	ок			
Recommended Action:	NON	E		
AN 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.

		LA	N Status			
Interface	Port	Cor Spe	nnection eed	Packet		Packets Received
Ethernet	1	100	юм	32593		19887
Ethernet	2	DIS	CONNECTED	N/A		N/A
Ethernet	3	DIS	CONNECTED	N/A		N/A
Ethernet	4	DIS	CONNECTED	N/A		N/A
MOCA	1	DIS	CONNECTED	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	192.108.254.04	1	1000Mbps	23H 45M 10S
Interface	MAC Add	ress IPv6 G	UAddress		IPv6 LLAddr	ess

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 T	able		
IP Address	HW Type	Flags	HW Address	Mask	Device
192.108.254.04	0×1	0×2	00:24:e8:82:99:6c	•	br0
10.1.10.1	0×1	0×2	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 Sc	an:	Enable	🔘 Disable	e
Scan In	terval:	10		Minutes
Wireles	t Devices: 1 s Devices: 0 (PStudio-PC	00:24:e8:82:99:6c		
	Ethernet 192.168.254.64	Port 1 - 1000 Mbps Fu 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	Packets	,			Bytes (MB)			Bytes (MB) since I	Reset	
intenace	(Mbps)	тх	Rx	Tx Errors	Rx Errors	тх	Rx	dropped	тх	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.



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
Set the Firewall Lo	g state.	
Display firewall logs:	Enable	Disable
Click Apply to save	changes.	
pply		
TIME	SYSTEM	ACTION
970/01/01 00:00:16	Kernel event	lis3lv02d: unknown sensor type 0xFF
970/01/01 00:00:18	Kernel event	hub 2-0:1.0: over-ourrent condition on port
970/01/01 00:00:18	Kernel event	eth4 (Ext switch port: 4) (Logical Port: 12) Link UP 1000 mbps full duple
970/01/01 00:00:16	Kernel event	eth4 (Ext switch port: 5) (Logical Port: 13) Link UP 1000 mbps full duple
970/01/01 00:00:18	Kernel event	Skipping Link UP - one of other LAG member is already UP <0x1000
970/01/01 00:00:16	Kernel event	hub 3-0:1.0: over-ourrent condition on port
970/01/01 00:00:18	Kernel event	hub 4-0:1.0: over-ourrent condition
970/01/01 00:00:16	Kemel event	eth0 (Ext switch port: 3) (Logical Port: 11) Link DOWN
970/01/01 00:00:17	Syslog event	Wireless init enabled
970/01/01 00:00:19	Kernel event	XdslMediaSearch: INIT_S received start event, media(0
970/01/01 00:00:19	Kernel event	eth0 (Ext switch port: 3) (Logical Port: 11) Link UP 1000 mbps full duple
970/01/01 00:00:20	Kernel event	ewan0 (Int switch port: 0) (Logical Port: 0) Link UP 1000 mbps full duple
970/01/01 00:00:22	Kernel event	eth0 (Ext switch port: 3) (Logical Port: 11) Link DOWN
970/01/01 00:00:24	Kernel event	eth0 (Ext switch port: 3) (Logical Port: 11) Link UP 1000 mbps full duple
	Kernel	SIOCSDMZ go

Configuring Wireless Settings

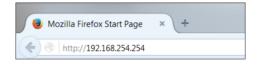


This chapter explains the options provided in the *Wireless Settings* section of the Gateway's firmware, including basic and advanced settings, and WPS.

Accessing Wireless Settings

To access the Wireless Settings screens:

 Open a Web browser. In the *Address* text box, type: <u>http://192.168.254.254</u> 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.

Wireless Settings Basic Settings Advanced Settings WPS MAC Address Control	Basic Settings is used to	Basic Settings enable or disable the wireless radio or change wireless security settings.
WDS	Frequency	® 5G
Band Steering	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 T
	Security Key Type	Use Default Key/Passphrase g52ye22jgj
		Use Custom Key/Passphrase
	Apply	

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 Cattings						
	Advanced Settings						
The modem supports high-speed 802.11b/g/n parameters as appro	wireless devices using the 802.11b/g/n protocol. Enable and tune opriate.						
Frequency	● 5G						
Compatibility Mode	SGHz (A,N,AC) ▼						
Channel Width	80 MHz 🔻						
Control Channel	None 🔻						
MSDU Aggregation	MSDU Aggregation Disabled 🔻						
MPDU Aggregation	MPDU Aggregation Enabled 🔻						
WMM	Enable O Disable						
WMM Power Save	Enable Disable						
Channel	Auto Detect Re-scan Current Channel: 132						
Scheduled Optimization	🔍 Enable 🔹 Disable						
Wireless Power Level	100% •						
Apply							

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.

w	PS (Wi-Fi Protected Setup)				
	WPS provides an easy and secure way to establish a wireless network by sharing the wireless key between the modern and wireless client.				
Frequency:	• 5G				
Select SSID	WIN5_700005 •				
1. Set the WPS state.					
WPS: O Enable Disable					
2. Click Apply to save changes.					
Apply					

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.

w	ireless MAC Au	uthentication		
Limit access to the modem I	y using the MAC address	of specific wireless devi	ces.	
Frequency:	● 5G 0 2.40	3		
1. Select SSID from the	pull down menu.			
SSID: WIN5_700005	T			
2. Set MAC authentication	n state.			
Mac Authentication: 🔘 Er	able 🖲 Disable			
3. Select Allow device li	t or Deny device list.			
Allow device list	Denies all devices exc	ept those added in step (4.	
Deny device list	Allows all devices exc	ept those added in step 4	ι.	
4. Enter the MAC addres	5 of the wireless LAN	device.		
Select MAC Address:	Manually	Add MAC Address:		
Manually Enter MAC	▼ or			
	(Sample M	IAC Address: 00:20:e0:00:4	1:00)	
5. Click Apply to save ch	anges.			
Apply	MAC Authentic	ation Device List		
DEVICE NA	1E IP ADDRESS	MAC ADDRESS	ACCESS	EDI
	No Entries D	efined		

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:	
1. Set the WDS main base station state.	
WDS Main Base Station: O Enable O 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

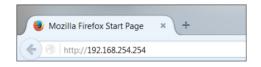


This chapter explains the options provided in the *Firewall* section of the Gateway's firmware, including setting up port forwarding and static NAT.

Accessing Firewall Settings

To access the Firewall screens:

 Open a Web browser. In the *Address* text box, type: <u>http://192.168.254.254</u> 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.

<u>II</u> rewall		curity level is set to NAT	rewall Only. Activating the firewall is optic		n the
Providency Hosting DMZ Hosting anced DMZ anced IPv6 DMZ P	1. Select the WAN is pings from WAN sid WAN PING block mo 2. Select IP addres Apply rule to: All C 3. Set the Firewall NAT Only Low MAT Only High	PING block mode. Wi de: O Enable ® Disable sing type.	some network functionality will be la		ond to all
	Note: If a check appears	in a box, that service is all	owed.		
	Service	Service Type	Service Port	Traffic	Traffic
			Service Fore	In	Out
	DirectX	Multimedia Control	2300-2400, 47624, 2300-2400 UDP, 6073 UDP	In	Out 🕑
	DirectX DNS	Multimedia Control	2300-2400, 47624, 2300-2400 UDP.		
			2300-2400. 47624. 2300-2400 UDP. 6073 UDP		
	DNS	DNS	2300-2400, 47624, 2300-2400 UDP, 6073 UDP 53		*
	DNS FTP	DNS File Transfer	2300-2400, 47624, 2300-2400 UDP, 0073 UDP 53 20, 21		\$ \$
	DNS FTP FTPS	DNS File Transfer Secure File Transfer	2300-2400, 47824, 2300-2400 UDP, 6073 UDP 53 20, 21 990		9 9 9 9
	DNS FTP FTPS H323	DNS File Transfer Secure File Transfer Video	2300-2400, 47824, 2300-2400 UDP, 6073 UDP 53 20, 21 990 1720	×	8 8 8 8
	DNS FTP FTPS H323 HTTP	DNS File Transfer Secure File Transfer Video Web Service	2300-3400, 47624, 2300-2400 UDP, 53 20, 21 690 1720 80		8 8 8 8 8
	DNS FTP FTPS H323 HTTP HTTPS	DNS File Transfer Secure File Transfer Video Web Service Secure Web Service	2300-2400, 47624, 2300-2400 UDP, 0073 UDP 53 20, 21 690 1720 80 443		8 8 8 8 8 8 8 8
	DNS FTP FTPS H323 HTTP HTTPS ICMP Echo Request	DNS File Transfer Secure File Transfer Video Web Service Secure Web Service Web Service	2300-2400, 47624, 2300-2400 UDP 0073 UDP 83 20, 21 990 1720 80 443 NA		8 8 8 8 8 8 8 8 8
	DNS FTP H323 HTTP HTTPS ICMP Echo Request ICMP Echo Repy	DNS File Transfer Secure File Transfer Video Web Service Web Service Web Service	2300-2400, 47524, 2300-2400 UCP, 4573 UCP 3 20, 21 600 1720 80 443 NA NA	8	8 8 8 8 8 8 8 8 8 8 8 8 8
	DNS FTP FTPS HITP HITPS ICMP Echo Request ICMP Echo Reply ICMP TTL Expire	DNS File Transfer Secure File Transfer Video Web Service Vieb Service Vieb Service Vieb Service	2300-2400, 47624, 2300-2400 UGP, 6073 UGP 05 20, 21 600 1720 80 443 NA NA NA NA	8	8 8 8 8 8 8 8 8 8 8
	DNS FTP FTPS H323 HTTP HTTPS ICMP Exho Repy ICMP The Exho Repy ICMP The Exho Repy ICMP The Exho Repy	DNS File Transfer Secure File Transfer Video Web Service Secure Vieb Service Web Service Vieb Service Vieb Service	2300-2400, 47624, 2300-2400 UCP, 63 20, 21 600 1720 80 443 NA NA NA NA	X X X	* * * * * * * * *
	DNS FTP H223 HTTPS ILCMP Exho Request ICMP This Expre ICMP This Expre ICMP This Expre ICMP This Expre	DNS File Transfer Secure File Transfer Video Veb Service Secure Web Service Veb Service Veb Service Meb Service Mail Service	2300-2400, 47024, 2300-2400 UDP, 4003 UDP 50 20, 21 000 1720 80 443 NA NA NA NA NA NA 143	8 8 8 .	* * * * * * * * * *
	DNS FTP FTPS H223 HTTP ICMP Echo Request ICMP Echo Request ICMP TTL Expire ICMP TTL expire ICMP TTL expire ICMP TTL expire ICMP TTL expire ICMP TTL expire	DNS File Transfer Secure File Transfer Viels Service Web Service Viels Service Viels Service Viels Service Viels Service Mail Service	2300-2400, 47524, 2300-2400 UDP, 4057 UDP 50 20, 21 60 1720 80 443 NA NA NA NA NA NA NA NA NA NA NA NA NA	× × × ×	
	DNS FTP FTPS H323 HTTP ICMP Excho Reguest ICMP Excho Reguest ICMP Trace route ICMP Trace route ICMP Trace route ICMP Trace route ICMP Trace route ICMP Trace route	DNS File Transfer Secure File Transfer Video Video Service Video Service Video Service Video Service Video Service Video Service Mali Service Remote Printing	2300-2400, 47624, 2300-2400 UCP, 63 20, 21 900 1720 80 443 NA NA NA NA NA NA 143 633		
	DNS FTP F123 HTTP HTTPS ICMP Exho Request ICMP TTL Expire ICMP	DNS File Transfer Secure File Transfer Vielo Service Vielo Service Vielo Service Vielo Service Vielo Service Mail Service Remote Printig VPN Service	2300-2400, 47024, 5300-2400 UDP, 6073 UDP 50 20, 21 600 443 NA NA NA NA NA 143 603 631 50, 51-500 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.

	TDv6	Firewall		
	IPVO	Filewall		
Activating the firewall i functionality may be lo		vall is activated, security is enhan	ced, but s	ome network
	n mode state. When st ated WAN traffic, inclu	ealth mode is enabled, the m iding pings	odem w	ill not
Stealth Mode:	🖲 Enable 🔍 Disa	ible		
2. Select the IP add	ress or IP addressing	type to which the firewall ru	les will a	apply.
Addressing Type:	All Dynamic IP Ad	dresses 🔻		
3. Set the Firewall S	Security Level.			
Security Level:	Medium 🔻			
CreateRule				
4. Set the firewall t	able, below. Services	checked are allowed. (option	al)	
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		1
FTPS	Secure File Transfer	990		
H323	Video	1720		1
HTTP	Web Service	80		1
HTTPS	Secure Web Service	443		1
ICMP Echo Request	Web Service	N/A		1
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
nter ports or port ranges requ	ired to forward Internet applications to a LAN device below.
. Set the LAN/WAN port a	and IP information.
Select LAN Device:	Manually enter the IP address T
LAN IP Address:	
External (WAN) Start Port:	
External (WAN) End Port:	
Internal (LAN) Start Port:	
Internal (LAN) End Port:	
Protocol:	TCP V
. Click Apply to save chan	nges.
Apply	
	Applied Port Forwarding Rules
LAN START/ END	TOCOL LAN IP WAN START/END MODIFY REMOVE
PORT	ADDRESS PORT HODIFY REMOVE

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: Enter IP Address: Manually enter the IP address ▼				
2. Select the application category, then the application to forward.				
Application Category: All Applications: Alien vs Predator View Rule				
3. Click Apply to save changes. Apply				
Forwarded Applications List:				
DEVICE IP APPLICATION EDIT NAME ADDRESS 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 Host	ing	
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 de	vice in DMZ mo	de creates a securi	y risk by exposing t	he device to outside
1. Set the DMZ sta	te.			
DMZ: 🔍 Enable 🖲	Disable			
2. Select a device.				
Select Device:		Enter IP Addres	s:	
Manually Enter IP	٣			
3. DMZ Timer.				
DMZ timer: 0				
4. Click Apply to save changes.				
Apply DMZ Hosted Device				
D	EVICE 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.

IF	Pv6 DMZ Hos	ting	
DMZ hosting enables a LAN device to LAN device outside the firewall.	use the modem's WAM	N IP address as its own. DMZ places t	he
WARNING! Using a device in DMZ mod intrusion.	de creates a security r	risk by exposing the device to outside	
1.Enter an Ipv6 Address.			
Enter The last 64 bits of Ipv6 Addr	ess: No PD get fro	om wan side	
Click Apply to save changes.			
Арріу	Ipv6 DMZ Hoste	d Device	
	IP ADDRESS	EDIT	

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	Follow the steps below to enable or disable UPnP (Universal Plug and Play).			
1. Set the UPr	1. Set the UPnP state.			
UPnP:	Enable	O Disable		
UPnp Log:	Enable	• Disable		
UPnP Mode:	Read only	Read write		
2. Click Apply	2. Click Apply to save changes.			
Apply				

Advanced Settings



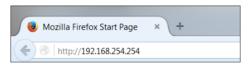
This chapter explains the options available with the Advanced Setup screens, which configure some of the more complex settings on the Gateway.

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.



4. The Services Blocking screen appears.

Services Blocking	Services Blocking
Website Blocking	Services blocking allows the modern to block internet services to a specific computer on the network
Scheduling Access	
Parental Controls	1. Select Device.
IP Address	Select Device: Enter IP Address:
WAN IP Addressing	Manually Enter IP
IPv6 WAN Settings	
LAN IP Settings	
IPv6 LAN Settings	
DHCP Reservation	2. Select service to block.
Dynamic DNS	
DNS Host Mapping	· Way - FIF - Heway ways - Emilian - In
Security	3. Click Apply to save changes.
Admin Password	Apply Service Blocking List
Storage Service	Service biocking List
Storage Device Info	
 Samba Configuration 	DEVICE IP ADDRESS Service Blocked EDIT
	NAME No Entries Defined
Modem Utilities	
Reboot	
Restore Defaults	
Upgrade Firmware	
Check for new firmware link	
Speed Test	
Ping Test	
Topdump Debug	
Iperl Test	
IPv6 Ping Test	
Traceroute	
IPv6 Traceroute	
Time Zone	
Language Settings	
DNS Cache	
IGMP Setting	
Upgrade History	
▶ ALG	
Tool Box	
DLNA	
xDSL Diagnostics	

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 Def	ned			

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		
	ules allows the modem to set a specific time period during which a computer on the n access the Internet.		
1. Select	Device.		
Select E Manua	Nevice: Enter MAC Address:		
2. Select	the days of the week to allow Internet access.		
A check	ed box signifies access allowed.		
SUN SUN	MON UUE 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 A	4. Click Add to create device schedule. Add		
	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:				
 Tag some devices as CHILD. Create time restrictions for all CHILD devices. Create webgage 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:				
 Select a target device. Create time restrictions for that particular device. Create webpage restrictions for that particular device. 				
The controls per device take priority over the CHILD controls. Update Tag Disable				
Client Device MAC Address Control Tag Internet Access Controls Parental Controls				
XPStudio-PC 00:24:e6:82:99:6c 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
AN IP Addressing sets	the protocol used by your ISP for Internet access.
L. Current WAN inte	erface is WAN Ethernet.
2. Select the ISP pro	otocol below.
O PPPoE	
RFC 1483 via DHCF	Ρ
🔘 RFC 1483 via Stati	ic IP
3. If your ISP Provid	der requires Host Name/Domain Name, enter it here.
Host Name	home
Domain Name	Home
I. Select the DNS ty	pe.
Dynamic DNS Addr	resses (Default)
Static DNS Address	ses
Primary DNS:	Not Applicable
Secondary DNS:	Not Applicable
5. Configure IGMP P	Proxy.
Enable	
O Disable	
	arameters.
 Enter the VLAN pa 	
VLAN ID:	-1 (-1 4094)
	-1 (-1 4094) 0 (0 7)
VLAN ID:	0 (0 7)

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 Setti	ngs			
IPv6 is the next generation of	IP addressing.				
1. Set the IPv6 state.					
IPv6:	Enable	O Disable			
2. Select the WAN IPv6 co	onnection protocol.				
WAN IPv6 IP Protocol:	DHCPv6 V				
3. Set the WAN IPv6 Addr	ressing 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 cha	5. Click Apply to save changes.				
Apply					

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.

	windstream.		
1	Status Wireless Satup Prenall Advanced Satup		
Blocking/Filtering			
Services Blocking	WAN IP Address		
Website Blocking	WAR IP Addressing sets the pretocol used by your ISP for Internet eccess.		
 Exheduling Access Parental Controls 			
	L. Current WAN Interface is WAN Ethernet.		
IP Address	2. Select the ISP protocol below.		
Weiv IP Addressing IPv6 W/M Sellings	Creeke		
 LAN IP Settings 	9 BPC 1483 Transported Bridging		
P IPVS LAN Scillings	C MC SHID VA DHCP		
DHOP Reservation	C BPC 3483 via Stolie IP		
 Dynamic DNS DNS HeatMapping 			
- Detaimationalphing	3. Enfor your PVP username and password.		
Security			
Admin Passwerd	PPP Userwarnen Bild Applicable		
Storege Service	PPP Passwards enterteretere		
Bierage Device Infe	4. Select the DHS type.		
Samba Configuration	4. Select the UNS type. ^(I) Dynamic OVS Addresses (Default)		
Nodem Utilities	 Dynamic Unic Addresses Static DAG Addresses 		
Retort			
 Reafore Defaults 	Primary DWS: Not Applicable		
Upgrade Fintewark	Secondary DWS: Dist Applicable		
Check for new firmware link			
 Speed Test Ping Test 	5. Configure IGMP Proay.		
 Topitump Debug 	ff Endle		
IperlTeat	f titable		
Prevenue Sea	0. Faller the VLAN parameters.		
Traceroute IPV6 Traceroute			
Time Zone			
Longuage Dellings	VLAN Priority: (0 - 7)		
 DNS Cache KMP Setting 	7. Click Apply to save changes.		
 Kally Setting Upgrade History 	Rept/		
* ALC			
Teal Bas			
 DUNA xDSL Diagnostics 			

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			
Actiontes recommends that you keep the current default LAN IP address of the modern. Any changes mode to the IAN IP address will react annual the other self-upp on the modern. Dated proceed without understanding the technical impact of changing these settings.			
1. To make changes, en field below.	ter the new TP address or Subnet Mask of the modem in the		
Podem IF Address:	102.169.254.254		
Modem Subnet Hask:	255.255.255.0		
2. Click Apply and Reboo	ot to save your changes.		
Apply and Reboot			
The modem will automatical	ly assign an IF address to each device in your network.		
1. Set the TP addressing) values.		
Deginning IP Address:	192.168.054.64		
Ending IP Address:	192,150,254,250		
Saluel Mask:	255.255.255.0		
 Set the DHCP server I DHCP Server Lease Time 			
3. Set the DNS values.			
DVS Nerver 1:			
DNS relay performed			
DNS directly from WAN connection			
Statustly Assumed 192.106.254.254 DNs Server 2:			
DNS berver 2: ONS relay performed by Gateway (Default)			
DNS directly from WA	Nennesten		
O Statically Assigned			
4. Click Apply to save ch	onges.		
Apply			

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.

<image/>		windstream.
<form> Bucking/Fittering Senders Blocking Person Profile Profile Person Senders Blocking Profile Person Senders Blocking Person Profile Person Senders Blocking Person Person Person Senders Blocking Person Person Senders Blocking Person Person</form>		🖪 🛜 👪 🔀
Services Blocking Wakine Blocking Weakine Blocking WAN IP Addressing sets the protocol used by your ISP for interment access. Parental Controls Lournent WAN interface is WAN Ethernet. Parental Controls Lournent WAN interface is WAN Ethernet. Parental Controls Lournent WAN interface is WAN Ethernet. Parental Controls Controls Prode Controls		Status Wireless Setup Firewall Advanced Setup
Services Blocking WAR IP Addressi Wath IP Addressi WAR IP Addressi Scheduling Access - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Storage Control Kondo - Select the DNS type. Parental Controls - Controls conter withinke Pa		
Services Blocking WAR IP Addressi Wath IP Addressi WAR IP Addressi Scheduling Access - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Parental Controls - Current WAN interface is WAN Ethernet. Storage Control Kondo - Select the DNS type. Parental Controls - Controls conter withinke Pa		
Sended Blocking Wateries Blocking Weater Blocking Wateries Blocking Scheddling Access Parental Controls Parental Controls 1. Current WAN interface is WAN Ethernet. Parental Controls 1. Current WAN interface is WAN Ethernet. Parental Controls 2. Select the ISP protocol below. Wateries Blocking © PPPod Prod UM Settings © PPPod Pod UM Settings © PPC 1483 Transparent Bindging Pod UM Settings © PPC 1483 via Static IP Dynamic DNS Other Prose Storage Service Submet Hask Storage Service Dynamic DNS Addresses Storage Service © Dynamic DNS Addresses (Defauk) Storage Service © Dynamic DNS Addresses (Defauk) Storage Teal © Dynamic DNS Addresses Ping Teal © Enable Prog Teal <td< td=""><td>Blocking/Filtering</td><td></td></td<>	Blocking/Filtering	
Scheduling Access Parential Controls Parential Controls Parential Controls IC unrent WAN interface is WAN Ethemet. Scheduling Access IV MAN Paddressing I WAN IP Addressing I WAN IP Addressing (DMA MAR BARNAR) I WAN IP Addressing I WAN	Services Blocking	WAN IP Address
	Website Blocking	
		WAN IP Addressing sets the protocol used by your ISP for Internet access.
WMLIP Addressing ^O PPPod I Mod WAN Settings ^O ECC 1483 Transparent Bindging I LAN PS ettings ^O ECC 1483 Transparent Bindging I Mod LAN Settings ^O ECC 1483 Transparent Bindging I Mod LAN Settings ^O ECC 1483 Transparent Bindging D DHOP Reservation ^O ECC 1483 Transparent Bindging Storage Service ^O ECC 1483 Transparent Bindging Admin Password ^{IP} Storage Service ^O Dynamic DNS Addresses Storage Service ^O Dynamic DNS Addresses Static DHS Addresses (Default) ^O Static DNS Addresses Opgrade Firmware ^O Dynamic DNS Addresses Pring Test ^O Static DNS Addresses Pring Test ^O Disable Pring Testing ^O Disable	Parental Controls	1. Current WAN interface is WAN Ethernet.
WMLIP Addressing ^O PPPod I Mod WAN Settings ^O ECC 1483 Transparent Bindging I LAN PS ettings ^O ECC 1483 Transparent Bindging I Mod LAN Settings ^O ECC 1483 Transparent Bindging I Mod LAN Settings ^O ECC 1483 Transparent Bindging D DHOP Reservation ^O ECC 1483 Transparent Bindging Storage Service ^O ECC 1483 Transparent Bindging Admin Password ^{IP} Storage Service ^O Dynamic DNS Addresses Storage Service ^O Dynamic DNS Addresses Static DHS Addresses (Default) ^O Static DNS Addresses Opgrade Firmware ^O Dynamic DNS Addresses Pring Test ^O Static DNS Addresses Pring Test ^O Disable Pring Testing ^O Disable	ID Address	3 Salact the TSD protocol below
Involution Involution Involution <td></td> <td></td>		
L MC Mass Presentation I Prod LMS Settings I Prod LMS Settings D DARS Presentation D DARS Device Mark D Dres Device Mark		
Pot LMS Settings C BrC 1483 via DHCP Public PReservation C BrC 1483 via DHCP Dynamic DNS C BrC 1483 via Static IP Dynamic DNS Storage Service Admin Password IP Storage Service Submet Hask Storage Service Submet Hask Storage Service Default Gateway Address Storage Service Dynamic DNS Addresses (Default) Restore Dtatuits C Dynamic DNS Addresses (Default) Restore Dtatuits Primary DNS: Spect Tat Primary DNS: Pring Test Storage Settings Pring Test C Datable Pring Test C Disable Imore Transmole VLAN Discrity: Imore Transmole VLAN Discrity: Upgnde History VLAN Discrity: Upgnde History C C Clock Apply to save changes. VLAN Priority: 0 Ubroade History VLAN Priority: Upgnde History C Click Apply to save changes. ALG VLAN		C RFC 1483 Transparent Bridging
DHCP Reservation IP Dirth Plassword 3. Select the 1P Type. Admin Password IP Admin Password IP Storage Service Submet Mask Storage Service Dafault Gateway Address Storage Service Dafault Gateway Address Storage Service Dafault Gateway Address Storage Service Dafault Gateway Addresse Storage Service Dafault Gateway Addresses Storage Service © Dynamic DNS Addresses Rebot © Static DNS Addresses Pugrade Firmware Primary DNS: Spece Test Secondary DNS: Spece Test © Datable Prog Test C Configure 1GMP Proxy. Topdump Debug G Enable Traceroule C Datable Traceroule C Datable Traceroule C Datable Traceroule VLAN Priority: Time Zone VLAN Discrete Language Settings VLAN Discrete Language Settings VLAN Discrete Language Settings VLAN Priority: Upprid Setting C Click Apply to sav		C RFC 1483 via DHCP
Dynamic DNS Disable Dynamic DNS Security Admin Password Storage Service Stora		G DEC 1483 via Static ID
> DNS Host Mapping 3. Select the IP Type. Scrinity µ > Admin Plassword µ > Storage Service □ubret Mask > Storage Necks Mo □rfault Gateway Address > Stanse Configuration		
Security IP Admin Password IP Storage Service Submet Mask Storage Service Default Gateway Address Stabase Configuration A. Select the DNS type. Nodem Utilities C Dynamic DNS Addresses (Default) Restore Defaults G Static DNS Addresses Upgnade Firmare Primary DNS: Specifies Secondary DNS: Storage Setting S. Configure IGMP Proxy. Ingel Test G Enable Ingel Test C Enable Index Setting VLAN IDI Index Setting VLAN IDI Upgnde History Q (0 + 7) Ubgnde History C Click Apply to save changes. A.C VLAN		
Security IP Admin Password IP Storage Service Submet Mask Storage Service Default Gateway Address Stabase Configuration A. Select the DNS type. Nodem Utilities C Dynamic DNS Addresses (Default) Restore Defaults G Static DNS Addresses Upgnade Firmare Primary DNS: Specifies Secondary DNS: Storage Setting S. Configure IGMP Proxy. Ingel Test G Enable Ingel Test C Enable Index Setting VLAN IDI Index Setting VLAN IDI Upgnde History Q (0 + 7) Ubgnde History C Click Apply to save changes. A.C VLAN		3. Select the IP Type
Armm Picks word Submet Mask Storage Service Default Gateway Address Stanige Device Mo Default Gateway Address Samba Configuration 4. Select the DNS type. Modern Utilities C Dynamic DNS Addresses Restorio Dravitis C Dynamic DNS Addresses Vigrade Firmmare Primary DNS: Speed Test Secondary DNS: Speed Test C Dable Prof Test C Dable	Security	
Storage Service Default Gateway Address > Standa Configuration A. Select the DNS type. Modem Utilities © Dynamic DNS Addresses (Default) > Rebot © Static DNS Addresses > Upgrade Firmare Primary DNS: > Ping Test Secondary DNS: > Ipod Test © Enable > Traceroule 6. Eater the VLAN parameters. > Time Zone OLAN Priority: > Language Settion VLAN ID: > DMS Cache VLAN Priority: > Upgrade Hutory 7. Click Apply to save changes. > ALG AcDV > Tool Box AcDV	Admin Password	1P
Straige Device Mo Default Gateway Address Samba Configuration 4. Select the DNS type. Modem Utilities © Dynamic DNS Addresses (Default) Rebot © Static DNS Addresses (Default) Restore Ordants © Static DNS Addresses (Default) Upgrade Firmmare Primary DNS: Speed Test Secondary DNS: Topdump Debug 5. Configure IGMP Proxy. Ipof Test © Enable Prof Test © Disable Ipof Test © Disable Imagraphic Setting VLAN ID: Language Setting VLAN ID: Upgrade History 7. Click Apply to save changes. ALG Valor Topio float Vector		Subnet Mask
A. Select the DNS type. Modem Utilities C Dynamic DNS Addresses (Default) Rebot C Static DNS Addresses (Default) Pactors Defaults Primary DNS: Upgrade Firmmare Primary DNS: Deck or new Immune link Geoodmary DNS: Ping Test C Disable Topdump Debug S. Configure IGMP Proxy. Ipof Test C Disable Tracorouls C Disable Tracorouls C Disable Tracorouls VLAN ID: DNS Coche VLAN ID: Upgrade Hitory C Click Apply to save changes. ALG ALG Top Box Apply		Default Gateway Address
Nodem Utilities C Dynamic DNS Addresses (Default) Reboot Static DNS Addresses (Default) Restore Defaults Static DNS Addresses Upgnade Firmare Primary DNS: Speed rat Secondary DNS: Ingel Test Secondary DNS: Ingel Test C Enable Upgnade History C Enable Upgnade History Q (1 - 40941) Ubgnade History Q (1 - 7) Udgrade History C Click Apply to save changes. ALC Vol Box Ubgrade History C Click Apply to save changes. ALC Vol Box	Samba Configuration	
Rebot Image: DNS Addresses (Default) Restore Defaults Image: DNS Addresses Restore Defaults Image: DNS Addresses Upgrade Firmare Primary DNS: Depade Firmare Secondary DNS: Pring Test Image: DNS Addresses Topdomp Debug S. Configure 1GMP Proxy. Ipped First Image: DNS Addresses Image: DNS Addresses Image: DNS Addresses Image: DNS Cache Image: DNS Addresses Image: DNS Cache Image: DNS Cache Image: DNS Cache Image: DNS Cache Image: DNS Cache Image: DNS Cache Imag		4. Select the DNS type.
Restore Dufaults ** Static DVA Addresses Upgrade Firmware Primary DNS: Other:K tore withmose link Secondary DNS: Spece Test Secondary DNS: Pring Test Secondary DNS: Topdump Debug S. Configure IGMP Proxy. Inder Test @ Enable Prof Test C Disable Traceroule S. Easter the VLAN parameters. Time Zone VLAN ID: Tanguage Setting VLAN ID: UAP Setting UAN Priority: UBP Setting VLAN Priority: VLAN Priority: Q (0 ~ 7) UBP Setting VLAN Priority: VLAN Priority: D (0 ~ 7) UBP Setting VLAN Priority: VLAN Priority: D (0 ~ 7) UDPAGE C Disable		Ø Dynamic DNS Addresses (Default)
Restore Ordautis Primary DNS: Upgrade Firmmare Primary DNS: Speed Test Secondary DNS: Pring Test Secondary DNS: Topdomp Debug 5. Configure XGMP Proxy. Topdomp Debug Genable Ipof Test Genable IPing Test C Disable Traceroule 6. Eater the VLAN parameters. Time Zone C Language Setting Upgrade Flatory VLAN ID: Language Setting VLAN Priority: Upgrade Flatory 7. Click Apply to save changes. ALG Apply Tool Box Option		G Static DNS Addresses
Check for new firmware link Secondary DNS: Prog Test Topdump Debug Prof Test Traceroule Traceroul		
Speed Test Secondary DNS: Ping Test Configure IGMP Proxy. Topdump Debug S. Configure IGMP Proxy. Ipof Test © Enable IPof Ping Test © Disable IPof Ping Test © Disable IPof Traceroute S. Enter the VLAN parameters. Time Zone VLAN ID: Imaginge Setting VLAN ID: Upprode History C. Click Apply to save changes. ALG Apply Top Idex		Primary DNS:
Pang Test S. Configure 1GHP Proxy. Topdomp Debug G Enable Ipof Test G Enable Ipof Pring Test C Disable Traceroule G. Enter the VLAN parameters. Time Zone VLAN ID: I Language Settings VLAN ID: DNS Cache VLAN Priority: Upgrade History C. Click Apply to save changes. ALG Apply Tool Box Apply		Secondary DNS:
Topdump Debug 5. Configure IGMP Proxy. Topdump Debug G Enable Traderoids G Enable Traderoids C Disable Traderoids G Enable Traderoids C Disable Traderoids G Enable Traderoids C Disable Traderoids G Enter the VLAN parameters. Time Zone VLAN ID: DNS Cachel VLAN Priority: UBMP Setting C Click Apply to save changes. ALG ALG Tool Box Apply		
I liger Test		5. Configure IGMP Proxy.
Tracerouls Classes IPvd Tracerouls 6. Enter the VLAN parameters. Time Zone Classes Language Settings VLAN ID: DNS Osche VLAN Priority: Upprode History Click Apply to save changes. ALC Toto Ibox DDNS		@ Enable
Traceroule 6. Enter the VLAN parameters. IPA Traceroule 6. Enter the VLAN parameters. Time Zone VLAN ID: Language Settings VLAN ID: DNS Osche VLAN Pointly: UABP Setting 0 Upgrade History 7. Click Apply to save changes. ALG Apply Tool Box Apply	IPv6 Ping Test	Cincella
Time Zone 6. Eater the VLAN parameters. Language Settings VLAN ID: -1 (-1 4094) DNS Osche VLAN ID: 0 (0 7) Halff Setting 0 (0 7) (-1 4094) Upprade History 7. Click Apply to save changes.	Traceroute	- Chapter
Time Zone VLAN ID: 1 (-1 ~ 4094) Language settings VLAN ID: 0 (0 ~ 7) IGMP Setting 0 (0 ~ 7) (0 ~ 7) Idpract Hotory 0 (0 ~ 7) (0 ~ 7) Idpract Hotory 7. Click Apply to save changes. ALG ALG Apply Apply Idpract Hotory DLNA Idpract Hotory Idpract Hotory Idpract Hotory		6. Enter the VLAN parameters.
DNS Cache VLAN Priority: 0 (0 ~~ 7) Highth Setting VLAN Priority: 0 (0 ~~ 7) Upgrade History 7. Click Apply to save changes. ALG Apply Total Bax Apply DUN Click Apply to save changes.		
IGMP Setting IGMP Setting Upgrade History ALG Tool Box Tool Box DUNA		
Upgrade History Z. Click Apply to save changes. ALG Tool Box DUNA		VLAN Priority: 0 (0 7)
ALG ALG ADD ADD		
Tool Box Apply DLNA		7. Click Apply to save changes.
DLNA		Apply
▶ xDSL Diagnostics		
	xDSL Diagnostics	

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 a	addressing.	
1. Set the IPv6 LAN connecti	on type.	
LAN Connection Type:	Stateless 🔻	
2. Set the IPv6 LAN addressi	ng 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 change	:5.	
Apply		

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	
HCP reservation leases a p	ermanent DHCP allocated address to a client.	
L. Select MAC Address, o	r manually enter a MAC address.	
Select MAC Address:	Manually enter the MAC Adi 🔻	
Manually Add MAC Address:		
,	to associate with a MAC address.	
2. Select an IP address t		
,	to associate with a MAC address.	
2. Select an IP address t IP Address:	to associate with a MAC address.	

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
	e WAN IP address of your modem with a host name. Dynamic DNS servers upon WAN IP address change.
1. Set the dynamic DNS	state.
Dynamic DNS State:	Enable Disable
2. Select the dynamic D	NS provider.
Dynamic DNS provider:	dyndns.com
3. Enter your username	and password.
Username:	
Password:	
4. Enter the dynamic DM	45 host name.
Hostname:	
5. Click Apply to save ch	langes.
Apply	

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.

DI	DNS Host Mapping			
DNS host mapping creates a static ho supported.	st name for the specified IP	address. WAN and LAN	IP addresses are	
1. Enter the DNS host name.				
DNS Host Name:				
2. Enter the IP address.				
IP Address:				
3. Click Apply to save changes.				
Apply				
	DNS Host Mapping List			
DEVICE NAME	IP ADDRESS No Entries Defined	DNS NAME	EDIT	

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.

1P QoS U	pstream Settings
before standard data traffic. Traffic shaping	prioritization of certain types of traffic (such as VoIP) your network with QoS can also increase application n becoming overloaded. Follow Steps 1-3 below to setup
1. Specify Classification Name and O	rder.
Traffic Class Name:	
Rule Order:	Last T
2. Specify Classifications (leave blan	k if criteria is not used for classification).
Ingress Interface:	LAN V
Ether Type:	T
Source MAC Address:	
Source MAC Mask:	
Destination MAC Address:	
Destination MAC Mask:	
3. Specify Classification Action.	
Assign Classification Queue:	T
Mark Differentiated Service Code Point (DSCP):	
Remark 802.1p priority (only for VLAN frame passthrough):	T
Retag VLAN ID [0-4094] (only for VLAN frame passthrough):	
Apply	

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.

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 O	rder.		
Traffic Class Name:			
Rule Order:	Last T		
2. Specify Classifications (leave blan	k if criteria is not used for classification).		
Ingress Interface:	WAN		
Ether Type:	T		
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):	T		
Remark 802.1p priority (only for VLAN frame passthrough):	τ		
Retag VLAN ID [0-4094] (only for VLAN frame passthrough):			

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 Oos	Settings		
	IPv6 QoS Settings IP QoS prioritizes traffic types (such as VoIP) before standard data traffic. Traffic shaping your network wit OoS can increase application performance and prevent your network from becoming overloaded.			
1. Set the QoS state				
QoS:	C Enable	O Disable		
2. Set the QoS direc	tion.			
QoS Direction:	Upstream	O Downstream		
Ingress Interface:	LAN V			
3. Set the QoS para	neters below.			
Rule Name:				
Mark Traffic Class:		۲		
Queue Priority:	Priority 1			
4. Set the IP tag.				
IP Tag:	All IP Address	O Define IP Address		
5. Click Apply to sav	e changes.			
Apply				
	QoS R	ule List		
Name Priority IP Tag	Name Priority IPTag 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 HTPS 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 modern remotely you will need to use https:// followed by the modern 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.		
Apply		

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: O Enable 🖲 Disable		
Local Telnet: O Enable 🖲 Disable		
2. Set the idle disconnect time below.		
Idle Disconnect After: 30 Minutes *		
3. Click Apply to save changes.		
Apply		

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.

Dumannia Dauting (DTD)	
Dynamic Routing (RIP)	
If a device is set up behind the modem in the network, consult the documentation that came with t device to see what kind of Dynamic Routing is required.	1e
1. Select the dynamic routing type.	
O Version 1	
O Version 2	
• off	
2. Click Apply to save changes.	
Apply	

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 ne	w passwords.			
Username:	admin			
Old Password:				
New Password:				
Confirm your password	:			
2. Click Apply to save o	2. Click Apply to save changes.			
Apply				

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.

The Storage service allows s	storage devices con	nnected 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:	T
Workgroup:	WORKGROUP
Apply	

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: Reboot	

Restore Defaults

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

	Restore Defaults	
To restore del	ault 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.
Browse
3. Click Upgrade Firmware to begin the upgrade.
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	
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.

Spe	ed Test
-	
1. Click "Test" to begin the speed test.	
URL:	
Test	
Speed Te	est 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 T	est			
Test your Inte	ernet connectiv	vity to a speci	fic host using	the ping test,	below.		
1. Insert a	URL or IP ad	dress below	<i>ı</i> .				
URL or IP:				_			
UKE OF IF.							
2. Select th	e packet size	÷.					
Packet Size	(Bytes): 32	2					
Tucket Size	(b)(c3).						
3. Select te	st.						
Test							
			Test Stat	us			
			Test Stat				
			No Test in Prop	press			
		P		press			
		F REPLY FROM	No Test in Pro	press	BYTES	TIME	πι
			No Test in Pro	press	BYTES N/A	TIME N/A	TTL N/A
		REPLY FROM N/A N/A	No Test in Pro	press	N/A N/A	N/A N/A	N/A N/A
		REPLY FROM N/A N/A N/A	No Test in Pro	press	N/A N/A N/A	N/A N/A N/A	N/A N/A N/A
		REPLY FROM N/A N/A	No Test in Pro	press	N/A N/A	N/A N/A	N/A N/A
		REPLY FROM N/A N/A N/A	No Test in Pro	sults:	N/A N/A N/A	N/A N/A N/A	N/A N/A N/A
		REPLY FROM N/A N/A N/A	No Test in Proj	sults:	N/A N/A N/A	N/A N/A N/A	N/A N/A N/A

Tcpdump Debug

Click Tcpdump Debug from any Advanced Setup screen to generate the Tcpdump Debug screen. 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.

	Tan duman Dahuan	
	Tcpdump Debug	
	et capture (pcap) file to the USB flash connecte ration files will be copied to the USB flash.	d to the modem. Also,
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	
Test		

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.

	Iper	f Test
Test your network situ	ation for interface, below.	
1. Select iperf Mode		
Client V		
2. Select port to list	en or connect to.	
port:	5001	
3. Select Report int	erval.	
report interval:	10	Seconds
4. Select protocol.		
Protocol:	TCP V	
window size:	16K	Bytes
5. Select transmit o	ptions.	
OTransmit Bytes	800M	Bytes
Transmit Time	10	Seconds
6. Host.		
URL or IP:		
7. Select test.		
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.

		IP	v6 Ping	Test		
Test the Mode	em's Internet c	onnectivity to	a specific ho	st using the Pin	g Test, below.	
1. Insert a	URL or IP ad	dress below	ı.			
URL or IP:						
2. Select th	e interface.					
Interface Na	ime:	None 🔻				
3. Select th	e packet size					
Packet size	(bytes):	32				
4. Select te	st.					
Test			Ping test	results		
Rep	oly 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 Statis	tics		
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.

		Т	raceroute	
Tracorouto i	s used to deter	ning the couts to	ken by packets acr	ross a potwork
riacerouter	s used to deteri	nine the route ta	ken by packets at	loss a network.
1. Insert a	URL or IP Ac	ldress below.		
URL or IP:				
ORL OF IP:				
2. Select to	est.			
Test				
			Test Status	
		N	o Test in Progress	
		Trac	eroute Results:	
Нор	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.

			IP	/6 Tracerout
Traceroute	is used to	determine	the route	taken by packets acr
1. Enter a	URL or I	P addres	s in the I	ext box, below.
URL or IP:				
2. Select	test.			
_				
Test				
			т	raceroute Results
Нор	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

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.

1. Please select your Time Zone (Current Time: September 12 07:07				
(GMT - 8:00)	Pacific Time			
(GMT - 7:00)	Mountain Time	•		
(GMT - 6:00)	Central Time	0		
(GMT - 5:00)	Eastern Time	۲		
	🕑 Day	Light Saving		

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.
Apply

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 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.
Apply

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	0		
Blocking Mode	۲		
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:	8		

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.

			Upg	jrade History
Provides (upgrade his	story data	for the mod	em. Jpgrade History
Date	Time	Type No Up	Status Igrade Entrie:	Firmware Version

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:	C Enable	Disable			
H323:	Enable	Disable			
TFTP:	Enable	Disable			
IRC:	Enable	Disable			
PPTP:	Enable	Disable			
RTSP:	Enable	Disable			
SIP:	Enable	Disable			
Apply					

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 provide qualified network	s troubleshooting tools for the modem. Do not enable the Tool Box features unless you are technician.
1. Set the traff	ic type to mirror.
Traffic Type:	None
2. Select the p	ort to be mirrored.
Traffic Type:	None
3. Click Apply t	o save changes.
Apply	

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	ate.	
DLNA:	C Enable	
Media Library Path:	T	
2. Click Apply to save ch	nges.	
Apply		

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.

	Print Server				
1. Set the Print Serv	er state.				
Print Server:	O Enable				
Printer name:					
Make and model:					
2. Click Apply to save	e changes.				
Apply					

Specifications



General

Model Number(s)

T3280 (Wireless 11ax Bonded VDSL2 Modem Gateway)

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. - CDS036-W120U **Input** - 100-240V~, 50/60Hz, 1.0A **Output** - 12.0V === 2.0A **Manufacturer** - Actiontec

Specifications

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 45° C (32°F to 113°F)

Storage Temperature

-20°C to 70°C (-4°F to 158°F)

Operating Humidity

10% to 85% non-condensing

Storage Humidity

5% to 90% non-condensing

Notices

Warranty

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

Local Law

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

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

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

Important Safety Instructions

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

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

Coaxial Cable

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

FCC Class B Equipment

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

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

Modifications

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

Declaration of Conformity for Products Marked With the FCC Logo

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

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

Important Note on Wi-Fi

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

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

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

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

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

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

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

Contact Info

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

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