technicolor

FEEL THE WONDER

TECHNICOLOR WIRELESS GATEWAY - CGM4231

OPERATIONS GUIDE

Version - Draft 1.1

Revision History

Revision	Date	Description
Draft 1.0	1/8/2018	Initial draft

Table of Contents

1 Introduction

This document provides information on the Technicolor 4231 Wireless Gateway to Technicolor's service provider customers. The audience for this document includes those personnel who are tasked with deploying, maintaining, and servicing this device as well as those who provide answers to questions from end users.

2 Technicolor Wireless Gateway

The Technicolor Wireless Gateway (Wireless Gateway) meets industry standards for DOCSIS 3.1 high-speed data connectivity along with reliable digital telephone service. The Technicolor Wireless Gateway delivers data, voice and wired (Ethernet) or wireless (Wi-Fi) gateway capabilities to connect a variety of devices at home or SOHO small home office that supports high speed data access and voice services in one device.

Front Panel View

The following image represents the Wireless Gateway.

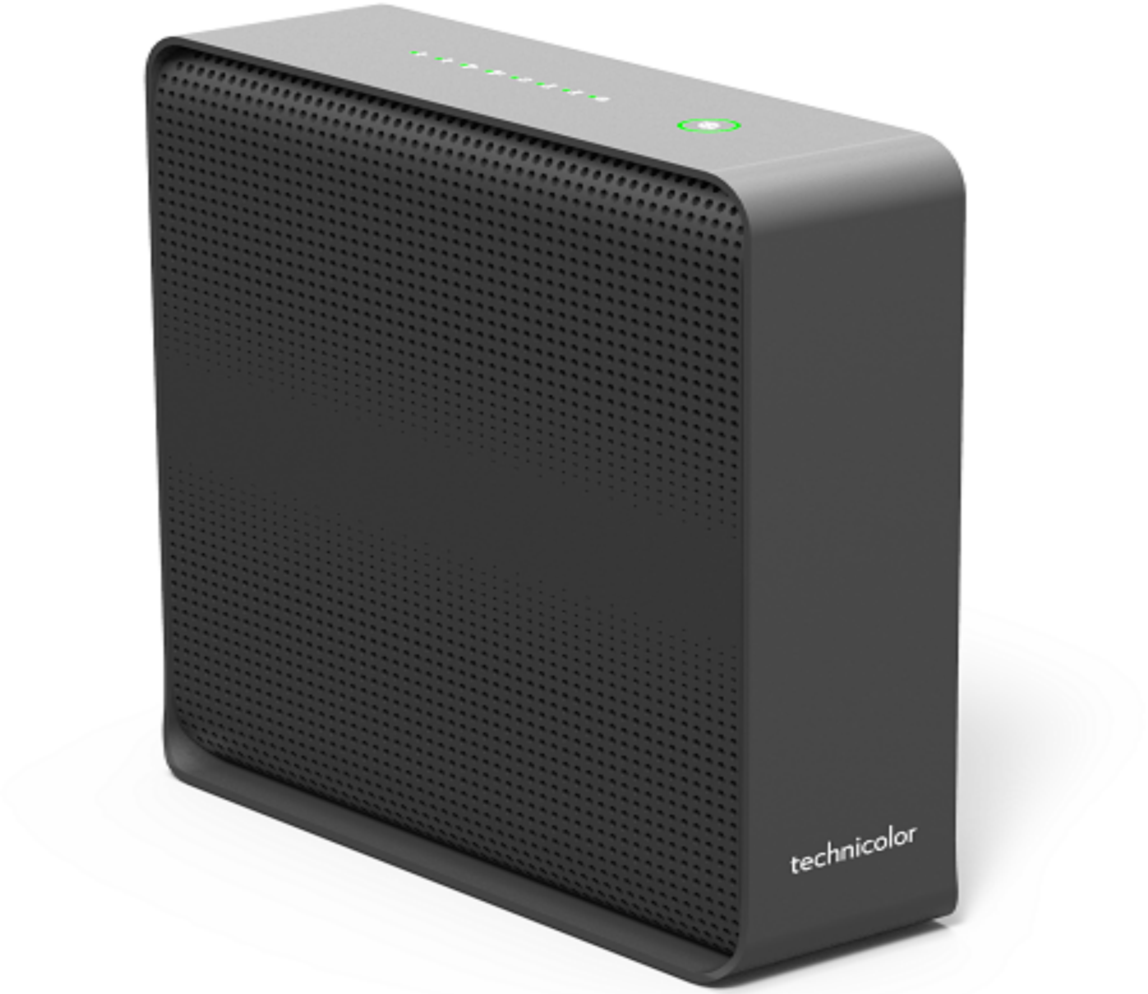


Figure 2.1

Top Panel View and LED Operations

The following image represents the front panel view of the Wireless Gateway

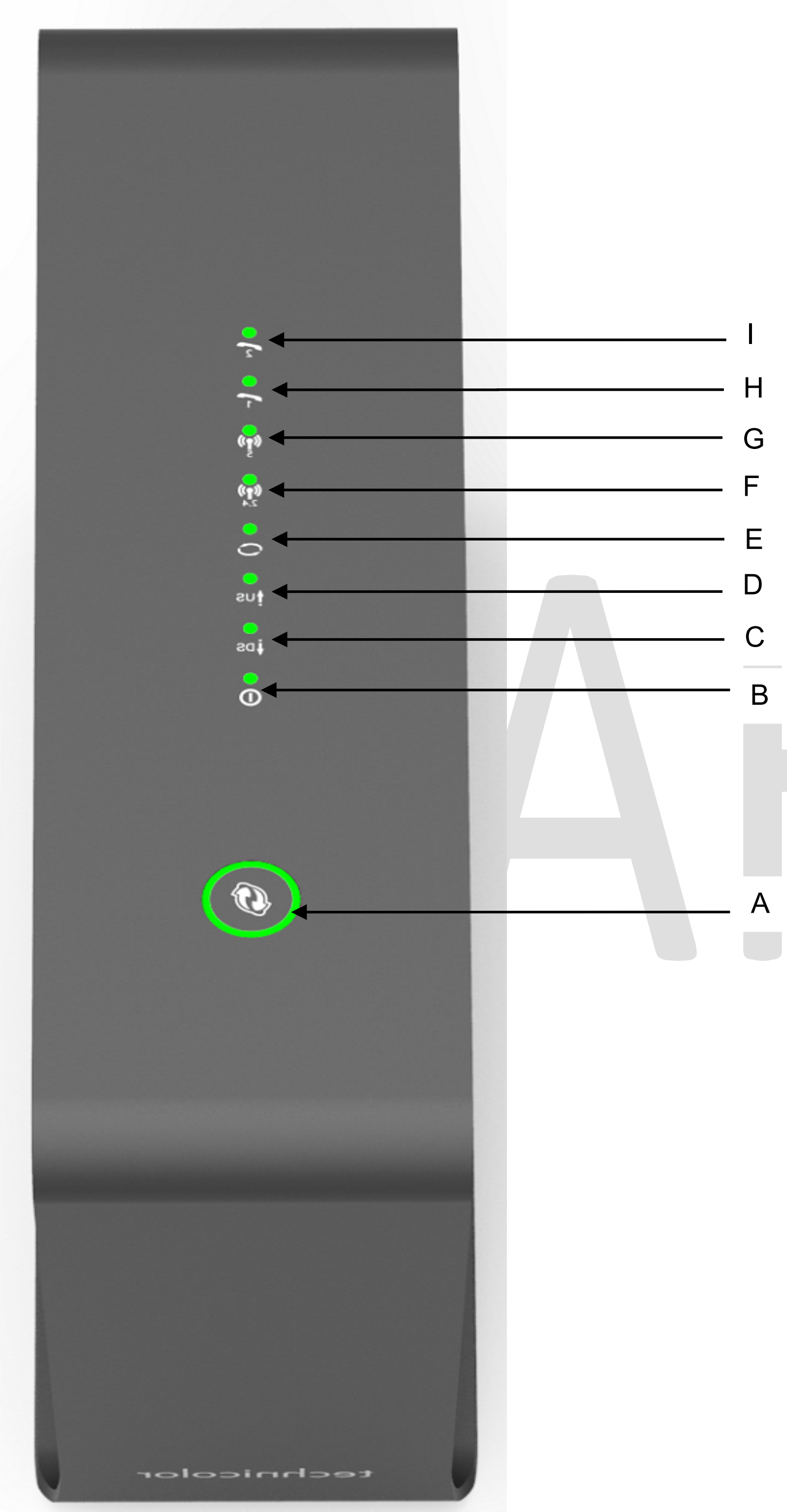


Figure 2.2

WPS Button (item A)

Wi-Fi Protected Setup (WPS) support, including an HW push button to activate WPS for simplified and secure wireless setup.

State	Description
Solid on	Wi-Fi Protected Setup (WPS) support, including an HW push button to activate WPS for simplified and secure wireless setup
Off	WPS setup not active

Power LED (item B)

State	Description
Solid on	Main Power Supply (12volt, 4.5 Amp.). DUT is on Main Power Supply.
Blinking	Slow Blink - MoCA is enabled, Fast Blink – MoCA enabled and MoCA client connected
Off	Power –Off

Downstream (DS) LED (item C)

State	Description
Solid on	Down Stream channel locked
Off	Power-Off
Flashing with US LED off	Searching for downstream signal
Flashing with US LED on	Partial service mode
Both US and DS Flashing	Software upgrade in progress

UP stream LED (US) (item D)

State	Description
Solid on	UP stream channel locked
Off	Power-Off
Flashing with DS Led off	Attempting to communicate with the CMTS
Flashing with US Led on	Partial service mode
Both US and DS Flashing	Software upgrade in progress

Online LED (item E)

State	Description
Solid on	Modem provisioning complete
Flashing slow	Attempting DHCP
Flashing fast	Attempting TFTP and final registration with CMTS
Very slow blink	Network access disabled by configuration file
Off	Not connected to your service provider's network

2.4 GHz Wi-Fi LED (item F)

State	Description
Blinking	Data is being transferred over the wireless connection. Wi-Fi is connected.
Off	Wi-Fi access point is not enabled

5 GHz Wi-Fi LED (item G)

State	Description
Blinking	Data is being transferred over the wireless connection. Wi-Fi is connected.
Off	Wi-Fi access point is not enabled

Telephone Line 1 led (item H)

State	Description
Solid on	Telephone Service on line -1 is enabled
Blinking	Telephone line 1 is connected to telephone and is operational
Flashing	Line two off (EMTA DHCP)
Both lines Blinking	Device registering with call agent
Off	Line 1 is not connected to phone or not operational

Telephone Line 2 led (item I)

State	Description
Solid on	Telephone Service on line -2 is enabled
Blinking	Telephone line 2 is connected to telephone and is operational
Flashing	Line one off (EMTA DHCP)
Both lines Blinking	Device registering with call agent
Off	Line 2 is not connected to phone or not operational.

Back panel

The following image shows the back of the Wireless Gateway.

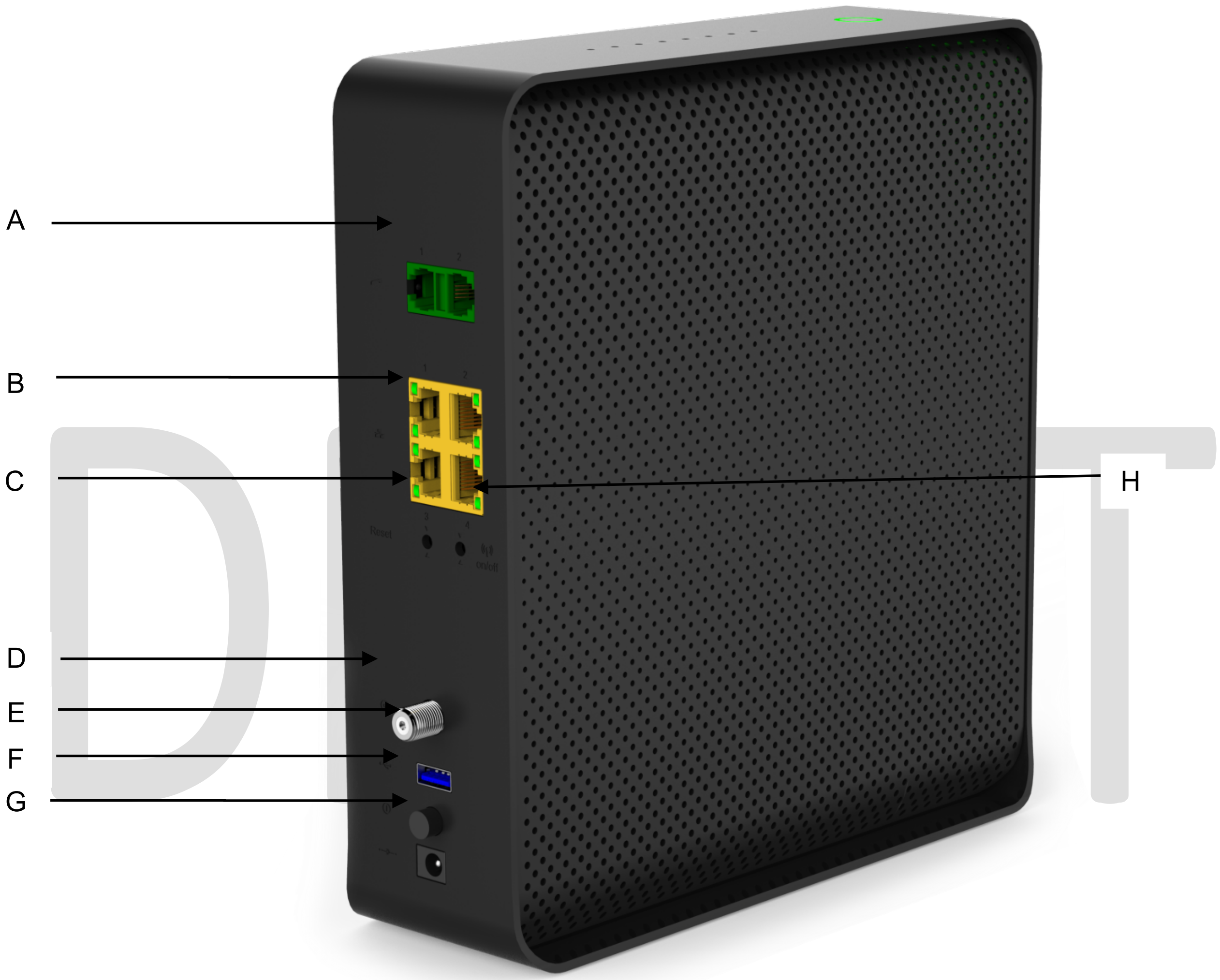


Figure 2.3

Tel ports (item A)

Two-line embedded digital voice adapter for wired telephony service.

Ethernet switch (item B)

Four 1000/100/10BASE-T Ethernet ports to provide wired connectivity. Each Ethernet port has two LEDs:

LED	LED Status	Description

Left LED (Green)	Solid on	Connected to a Gigabit Ethernet device
	Blinking	Connected to a Gigabit Ethernet device and sending/receiving data
	Off	Not connected to a Gigabit Ethernet device
Right LED (Amber)	Solid on	Connected to a 1000Mbps/100Mbps/10Mbps device
	Blinking	Connected to a 1000Mbps/100Mbps/10Mbps device and sending/receiving data
	Off	Not connected to a 100Mbps/10Mbps device

Reset Button (item C)

Press on the Reset button to reset the box.

Note:

Press and hold the reset button for more than 6 seconds to restore the gateway to factory settings.

Cable port (item D)

Compliance with DOCSIS 3.0, 3.1 standards along with PacketCable™ and EuroPacketCable™ specifications to deliver high-end performance and reliability.

USB port (item E)

USB interface provides full access for advanced user

Technicolor Wireless Gateway does not support USB printing. Refer section

Power Switch (item F)

The power switch (Turn-On/Off) allows you to turn-on and turn-off the box.

Power inlet (item G)

The power inlet (Power) allows you to connect the power cord.

Wi-Fi Turn –On/Off Switch (item H)

The Wi-Fi switch (Turn-On/Off) allows you to turn-on and turn-off the Wi-Fi.

Bottom panel

The following image depicts the bottom panel view of the Wireless Gateway.

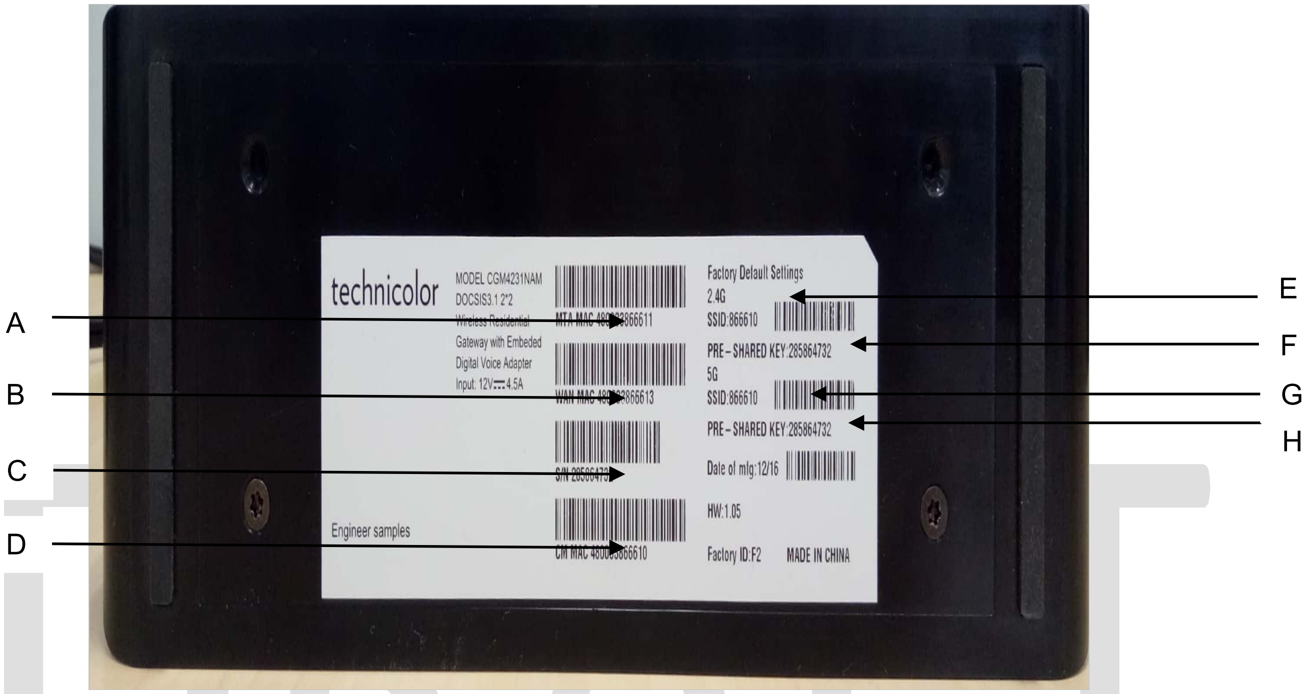


Figure 2.4

Product label: - The label on the bottom of the Gateway contains the following information about your Gateway:

MTA MAC No. (Item A)

MTA MAC No of Device. It is of the following format:

MTA MAC –X XXXXXXXXXXX

WAN MAC No. (Item B)

WAN MAC No of Device. It is of the following format:

WAN MAC –X XXXXXXXXXXX

Serial Number of Device (Item C)

S/N of Device. It is of the following format:

S/N –X XXXX XXXX

CM MAC No. (Item D)

CM MAC No of Device. It is of the following format:

CM MAC –X XXXXXXXXXXX

2.4 GHz SSID (Item E)

Network Name (SSID) is the network name of the 2.4 GHz access point and is of the following format:

2.4 GHz

SSID: X XXXXX

PRE- SHARED KEY of Device FOR 2.4 GHz (Item F)

PRE- SHARED KEY of Device. It is of the following format:

PRE - SHARED KEY –X XXXXXXXX

5 GHz SSID (Item G)

Network Name (SSID) is the network name of the 5 GHz access point and is of the following format:

5 GHz

SSID: X XXXXX

PRE- SHARED KEY of Device FOR 5 GHz (item H)

PRE- SHARED KEY of Device. It is of the following format:

PRE - SHARED KEY –X XXXXXXXX

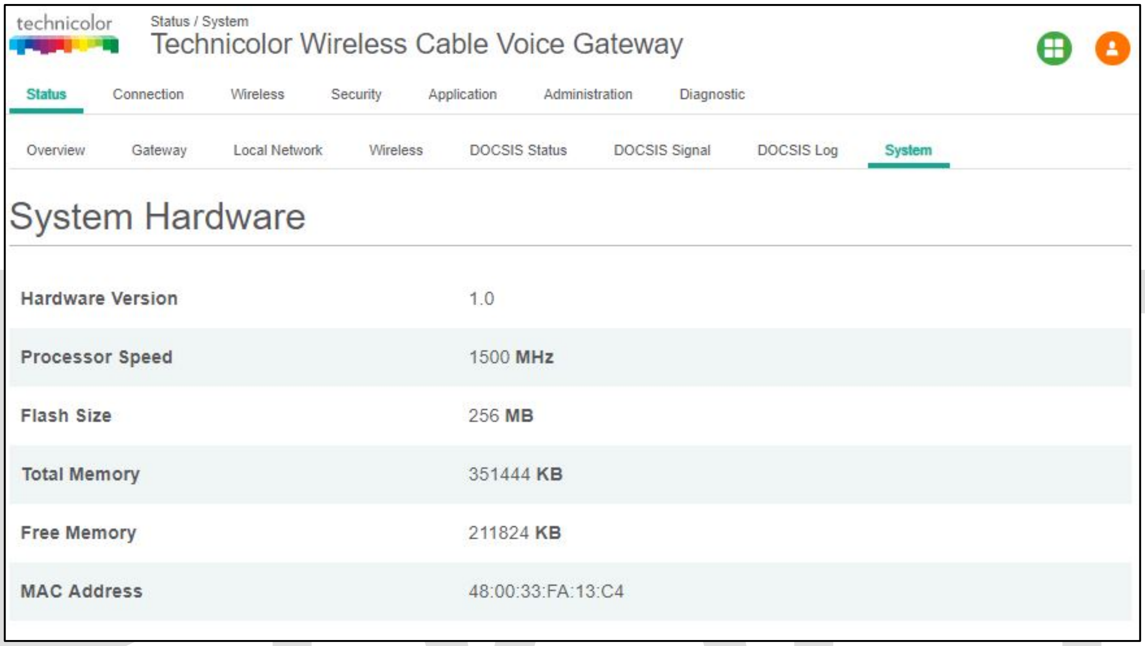
Other Features Details

- Compliance with DOCSIS 3.0, 3.1 standards along with Packet Cable™ and Euro Packet Cable™ specifications to deliver high-end performance and reliability
- Two-line embedded digital voice adapter for wired telephony service
- Up to two 802.11 radios for the dual-band concurrent operation with up to eight SSIDs per radio
- Wi-Fi Protected Setup TM (WPS) support, including an HW push button to activate WPS for simplified and secure wireless setup
- User configurable Parental Control blocks access to undesirable Internet sites
- Advanced firewall technology deters hackers and protects the home network from unauthorized access
- Attractive compact design that allows for horizontal, or wall-mounted operation
- Color-coded interface ports and corresponding cables to simplify installation and setup

- DOCSIS-8 compliant LED labeling and behavior provides a user and technician friendly method to check operational status and act as a troubleshooting tool
- Automatic software upgrades by the service provider
- TR-069 Compliant Remote Management Capabilities

2.1 System Information

The following WebUI page of the Wireless Gateway provides the hardware and software version information of the product.



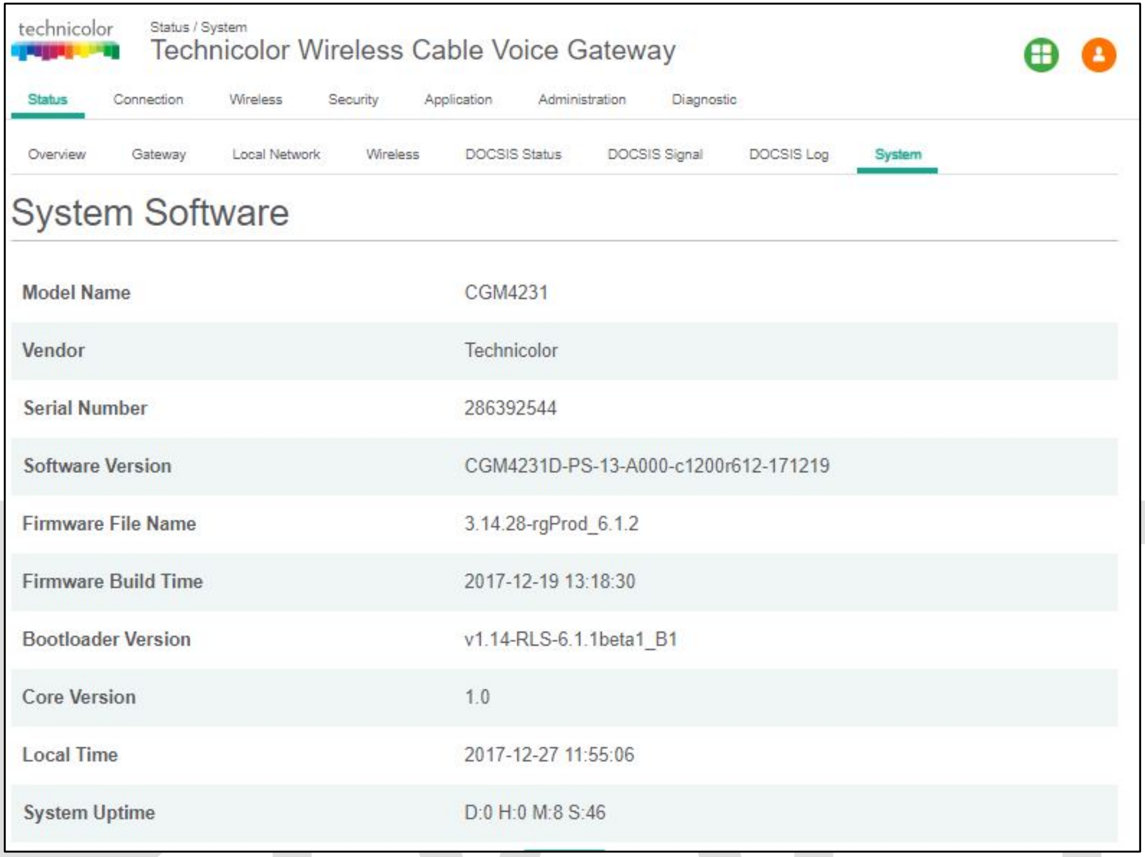
System Hardware

Hardware Version	1.0
Processor Speed	1500 MHz
Flash Size	256 MB
Total Memory	351444 KB
Free Memory	211824 KB
MAC Address	48:00:33:FA:13:C4

Figure 2.5

Software File Name and Revisions

The data shown in the table below provides the information about the firmware of your Wireless Gateway:



System Software

Model Name	CGM4231
Vendor	Technicolor
Serial Number	286392544
Software Version	CGM4231D-PS-13-A000-c1200r612-171219
Firmware File Name	3.14.28-rgProd_6.1.2
Firmware Build Time	2017-12-19 13:18:30
Bootloader Version	v1.14-RLS-6.1.1beta1_B1
Core Version	1.0
Local Time	2017-12-27 11:55:06
System Uptime	D:0 H:0 M:8 S:46

Figure 2.6

3 Initial Configuration and Setup

The Technicolor Wireless Gateway is configured using the Web UI

3.1 Accessing the WebUI

Procedure

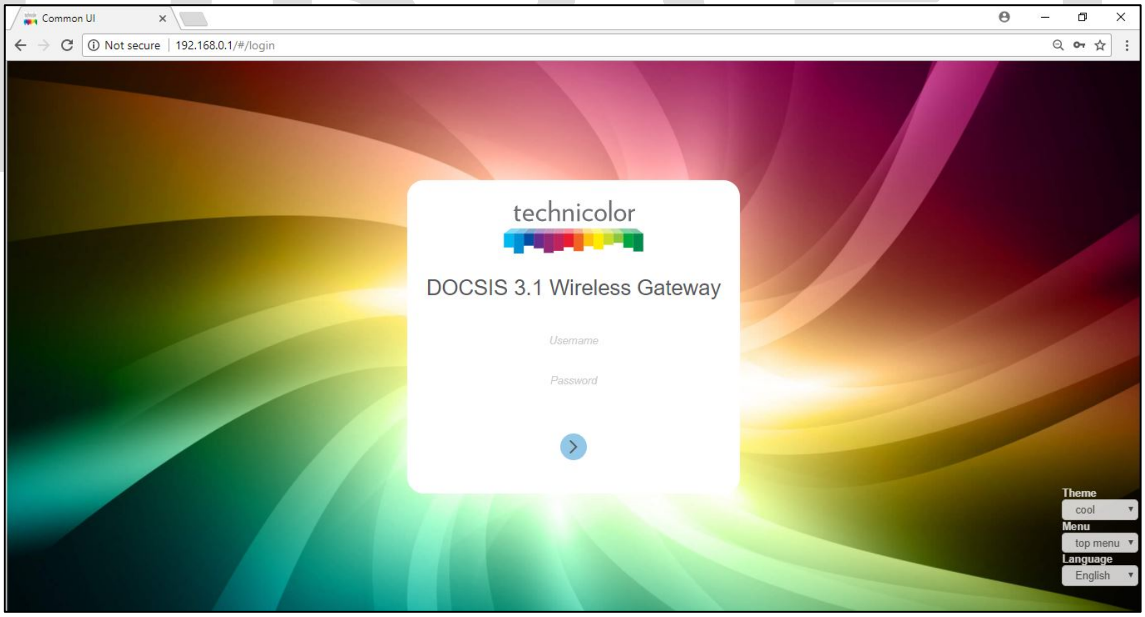
There are 3 interfaces for the user/operator to connect to on the CGM4231:

- LAN (Default URL 192.168.0.1 on LAN side)
- Cable Modem (CM IP on the WAN side)
- eRouter (eRouter IP on the WAN side)

Apart from these 3 interfaces, there are 2 user levels, Home User and Advanced User.

When the user connects to the WebUI, the page prompts the user enter the username and password. There is no user name and password set on default for the home user. On boot-up, the user can login to the WebUI by pressing <ENTER> and the user will be directed to a page to set the user name and password. After doing so, the user is directed again to the login page to login to the system with new credentials.

For the advanced user, the user name is admin and the password would be the generated password of the day.



Theme
cool
Menu
top menu
Language
English

Figure 3.1

The various pages on the WebUI may be accessible once the credentials are accepted.

4 WebUI Guide

Table 4.1 below describes the webpages available for the Home user (Advanced Access) in online and offline states.

Top Tab	Webpage (sub-tab)	On-line	Off-line
Status	Overview	✓	✓
	Gateway	✓	✓
	Local Network	✓	✓
	Wireless	✓	✓
	DOCSIS Status	✓	✓
	DOCSIS Signal	✓	✓
	DOCSIS Log	✓	✓
	System	✓	✓
Connection	Devices	✓	✓
	LAN	✓	✓
	WAN	✓	✓
	MoCA	✓	✓
	Routing	✓	✓
	Modem	✓	✓
	MTA	✓	✓
	Network Time	✓	✓
Wireless	Radio	✓	✓
	Security	✓	✓
	Advanced	✓	✓
	Guest Network	✓	✓
	MAC Control	✓	✓
	WPS	✓	✓
	QoS	✓	✓
Security	Firewall	✓	✓
	IP Filter	✓	✓
	Device Filter	✓	✓
	Site Filter	✓	✓
	Service Filter	✓	✓
	VPN	✓	✓
	Email Settings	✓	✓

	Report	✓	✓
Application	Port Forward	✓	✓
	Port Trigger	✓	✓
	DDNS	✓	✓
	DMZ	✓	✓
`	UPnP	✓	✓
	IP Passthrough	✓	✓
	Media	✓	✓
Administration	User	✓	✓
	Remote Access	✓	✓
	Backup and Restore	✓	✓
	Reboot and Reset	✓	✓
	Historical Consumption		
	Troubleshooting	✓	✓
	Remote Log	✓	✓
Diagnostics	System	✓	✓
	Interface	✓	✓
	Network	✓	✓
	Wireless	✓	✓
	Clients	✓	✓
	Internet	✓	✓
	Self-Test	✓	✓

Table – 4.1

Table 4.2 below describes the Webpages available for the Advanced User (Basic access) in online and offline states.

Top Tab	Webpage (sub-tab)	OnLine	OFFLine
Status	Overview	✓	✓
	Gateway	✓	✓
	Local Network	✓	✓
	Wireless	✓	✓
	DOCSIS Status	✓	✓
	DOCSIS Signal	✓	✓
	DOCSIS Log	✓	✓
	System	✓	✓

Table – 4.2

5 Status Pages

5.1 Overview

Status Tab / Overview
The Overview page under the Status tab provides the high level view of the Wireless Gateway. It displays the connections on the Wi-Fi, LAN and Guest Wi-Fi networks.

- **Main Wi-Fi** Displays the connected Wi-Fi (WLAN) Clients with their Host Name and IP address.
- **Network** Displays the connected Wired (LAN) Clients with their Host Name and IP address.
- **Guest Wi-Fi** Displays the clients connected to Guest Wi-Fi.

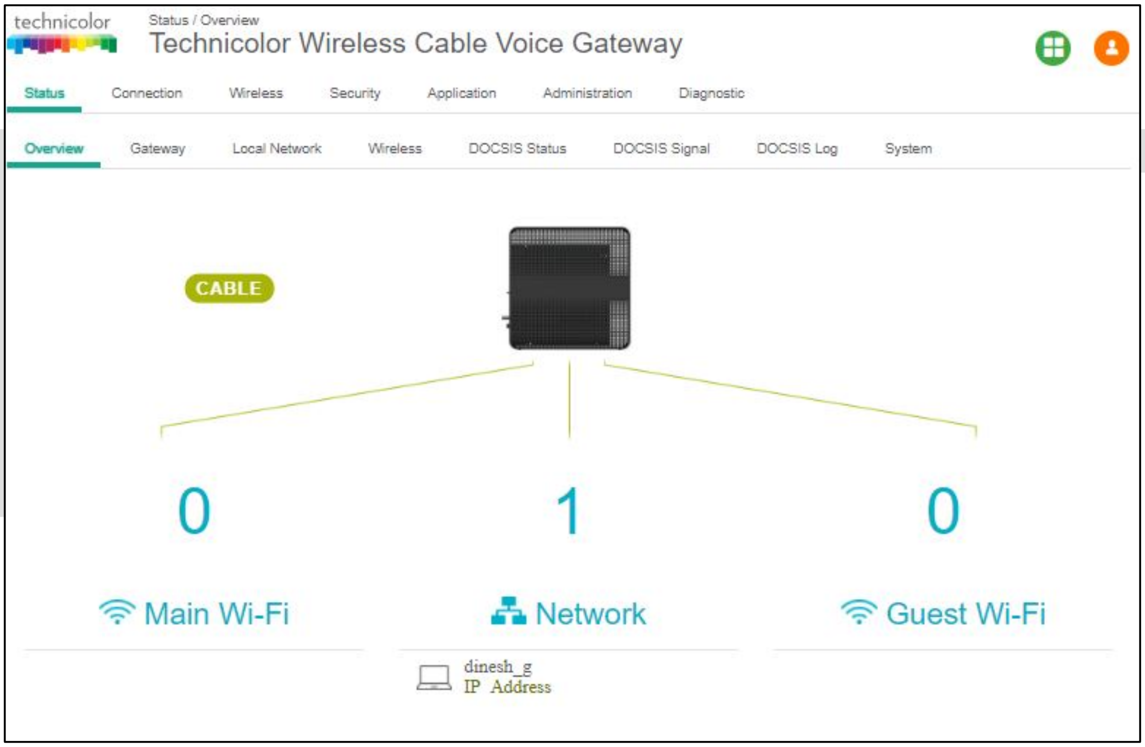
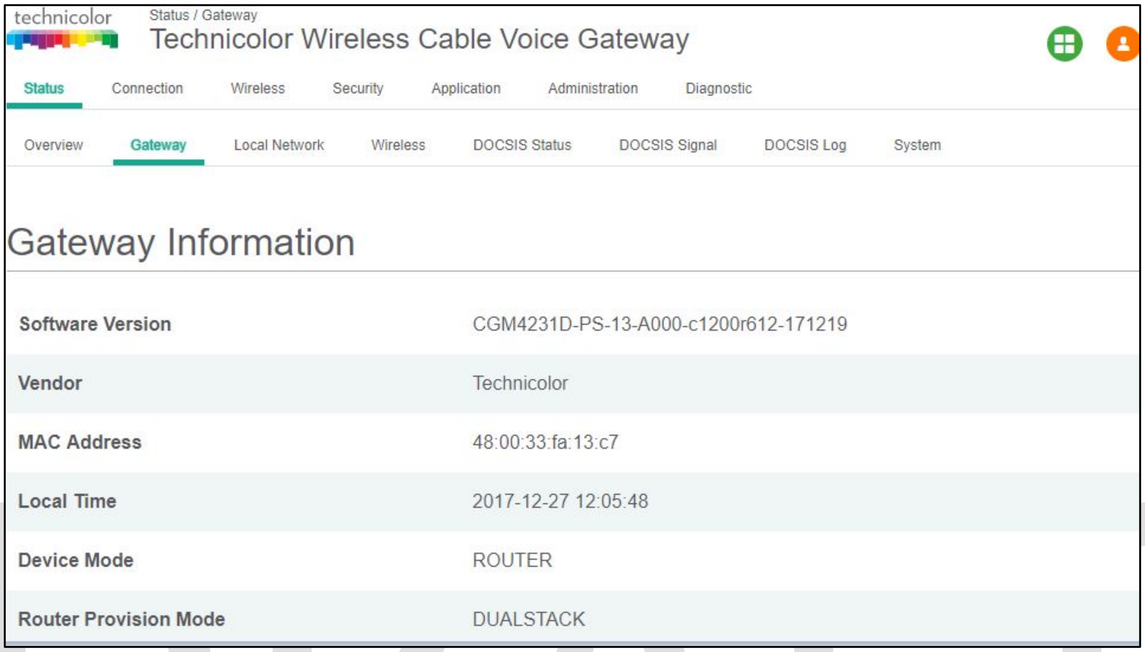


Figure 5.1

5.2 Gateway

Status Tab / Gateway
Click on the Status tab then click on Gateway. The page displays Gateway information and the IP Network information.

The Gateway Information section shows the Software Version, Vendor Name, eRouter MAC address, Device Mode, Router Provision Mode and Local Time set in the device as shown below:

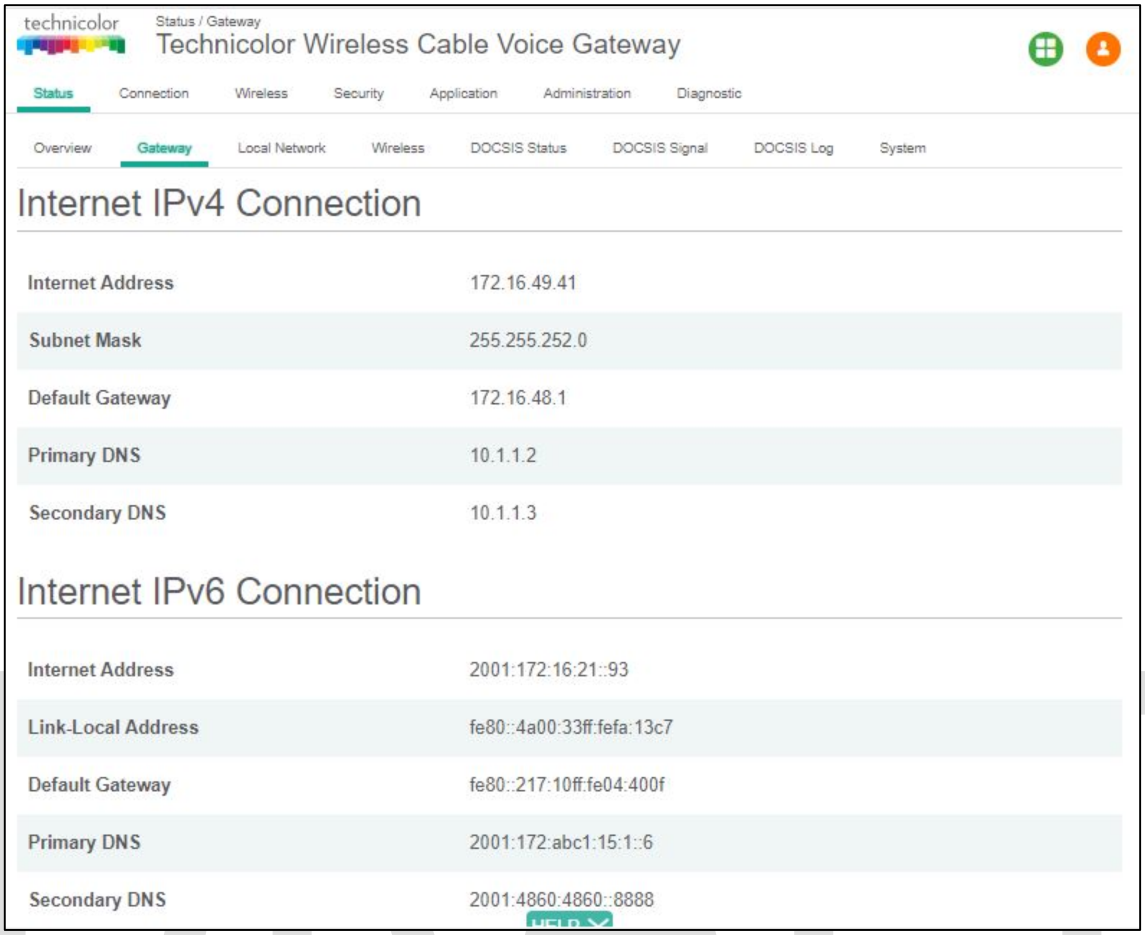


Gateway Information

Software Version	CGM4231D-PS-13-A000-c1200r612-171219
Vendor	Technicolor
MAC Address	48:00:33:fa:13:c7
Local Time	2017-12-27 12:05:48
Device Mode	ROUTER
Router Provision Mode	DUALSTACK

Figure 5.2

The IP connectivity information provided in the page includes eRouter IP Address, Subnet Mask, DNS and default Gateway Information for the IPv4 and IPv6 connections. The details are displayed as given below:



Internet IPv4 Connection

Internet Address	172.16.49.41
Subnet Mask	255.255.252.0
Default Gateway	172.16.48.1
Primary DNS	10.1.1.2
Secondary DNS	10.1.1.3

Internet IPv6 Connection

Internet Address	2001:172:16:21::93
Link-Local Address	fe80::4a00:33ff:fefa:13c7
Default Gateway	fe80::217:10ff:fe04:400f
Primary DNS	2001:172:abc1:15:1::6
Secondary DNS	2001:4860:4860::8888

Figure 5.3

5.3 Local Network

Status Tab / Local Network
Click on the Status tab then click on Local Network. The Local Network page will display the LAN information seen by the user.

LAN Information:

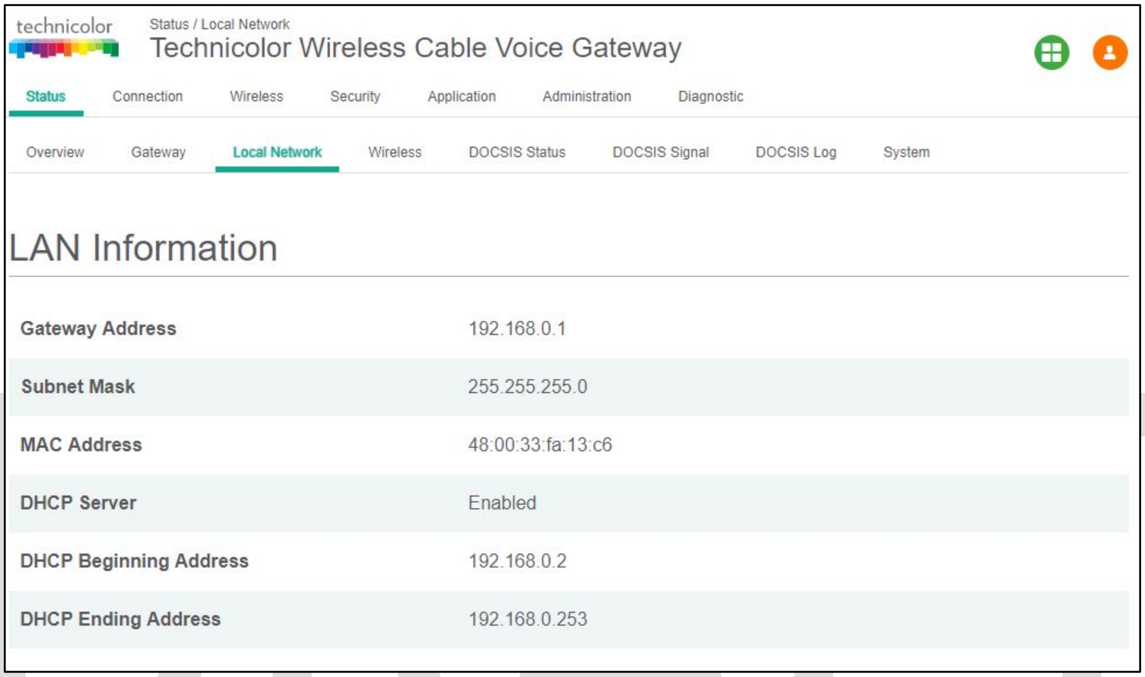
This section displays the configuration of DHCP addresses for the home user on the LAN side; Information such as the Gateway Address, Subnet Mask, MAC Address, DHCP Server, DHCP Beginning Address and DHCP Ending Address are displayed here.

DHCP Clients:
The connected clients to the gateway either via Ethernet or Wi-Fi will be displayed in this table.

ARP Table:
The ARP Table section displays ARP information about connected clients. When a client is configured for static IP, the static option will be shown as Yes.

SLAAC Table Information:

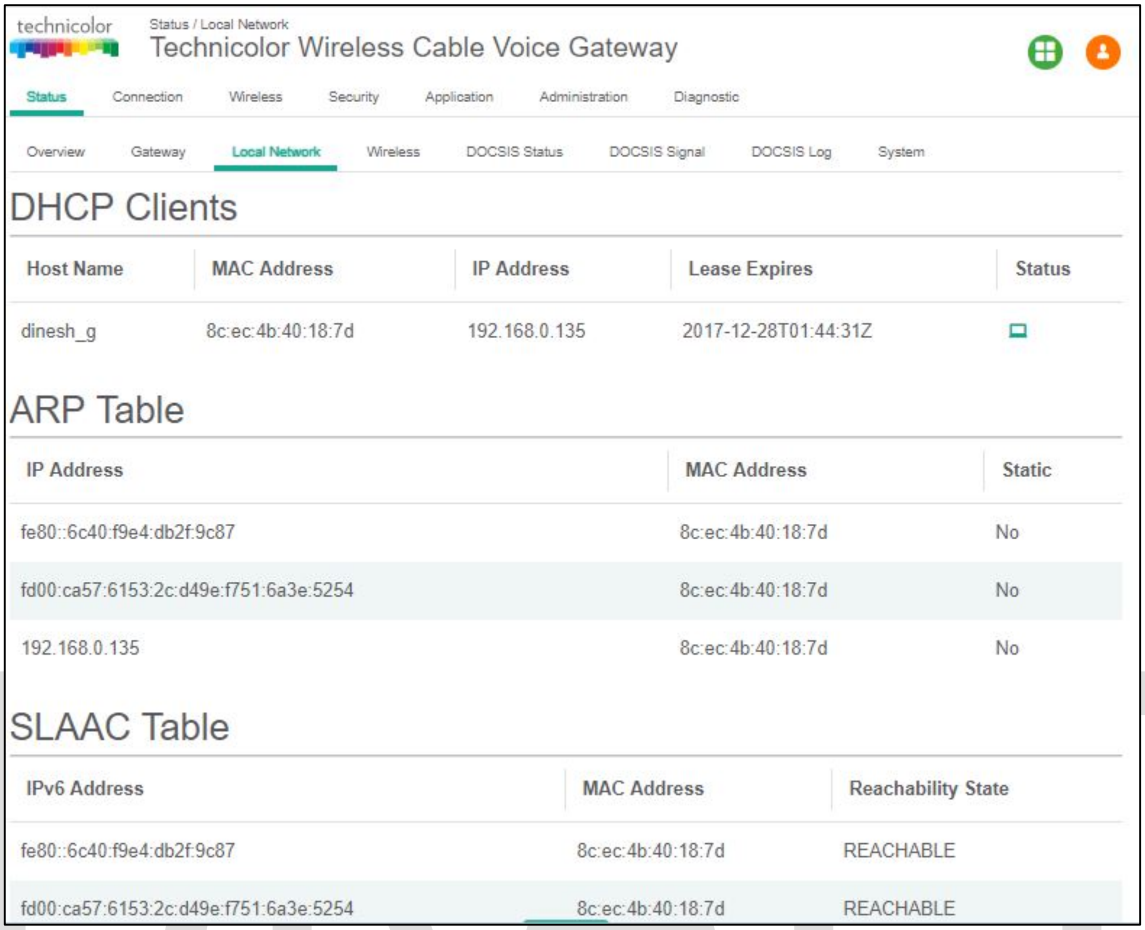
Stateless Auto Configuration (SLAAC) is a feature offered by the IPv6 protocol. It allows the various devices attached to an IPv6 network to connect to the Internet using the Stateless Auto Configuration without requiring any intermediate IP support in the form of a DHCP server. The SLAAC Table section displays details about IPv6 Address, the corresponding MAC Address and Reachability States information.



LAN Information

Gateway Address	192.168.0.1
Subnet Mask	255.255.255.0
MAC Address	48:00:33:fa:13:c6
DHCP Server	Enabled
DHCP Beginning Address	192.168.0.2
DHCP Ending Address	192.168.0.253

Figure 5.4



DHCP Clients

Host Name	MAC Address	IP Address	Lease Expires	Status
dinesh_g	8c:ec:4b:40:18:7d	192.168.0.135	2017-12-28T01:44:31Z	💻

ARP Table

IP Address	MAC Address	Static
fe80::6c40:f9e4:db2f:9c87	8c:ec:4b:40:18:7d	No
fd00:ca57:6153:2c:d49e:f751:6a3e:5254	8c:ec:4b:40:18:7d	No
192.168.0.135	8c:ec:4b:40:18:7d	No

SLAAC Table

IPv6 Address	MAC Address	Reachability State
fe80::6c40:f9e4:db2f:9c87	8c:ec:4b:40:18:7d	REACHABLE
fd00:ca57:6153:2c:d49e:f751:6a3e:5254	8c:ec:4b:40:18:7d	REACHABLE

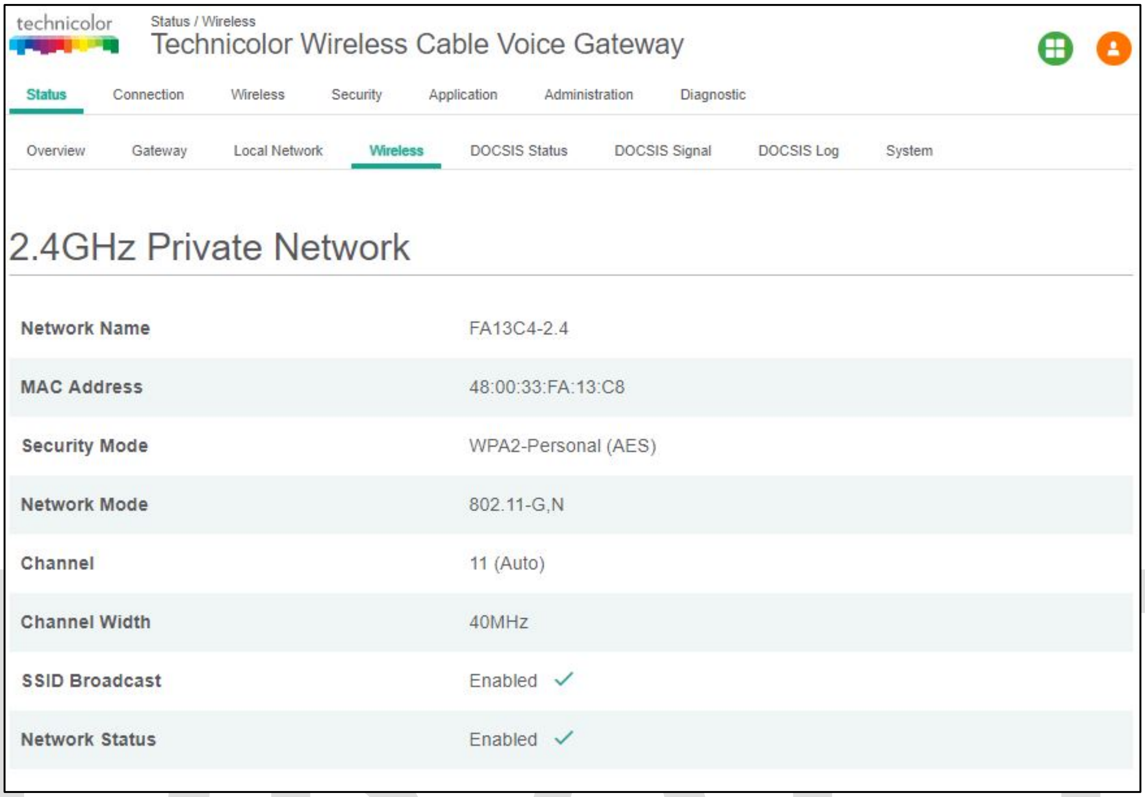
Figure 5.5

When in IPv6 mode or Dual Stack mode, the DHCP Client table includes IPv6 related status and type information.

5.4 Wireless Status

Status Tab / Wireless
Click on the Status tab then click on the Wireless tab. The page provides wireless network information, including the Network Name (SSID), MAC Address, Security Mode, Network Mode, Channel, Channel Width, SSID Broadcast and Network Status for 2.4 GHz and 5 GHz.

2.4GHz Network information:

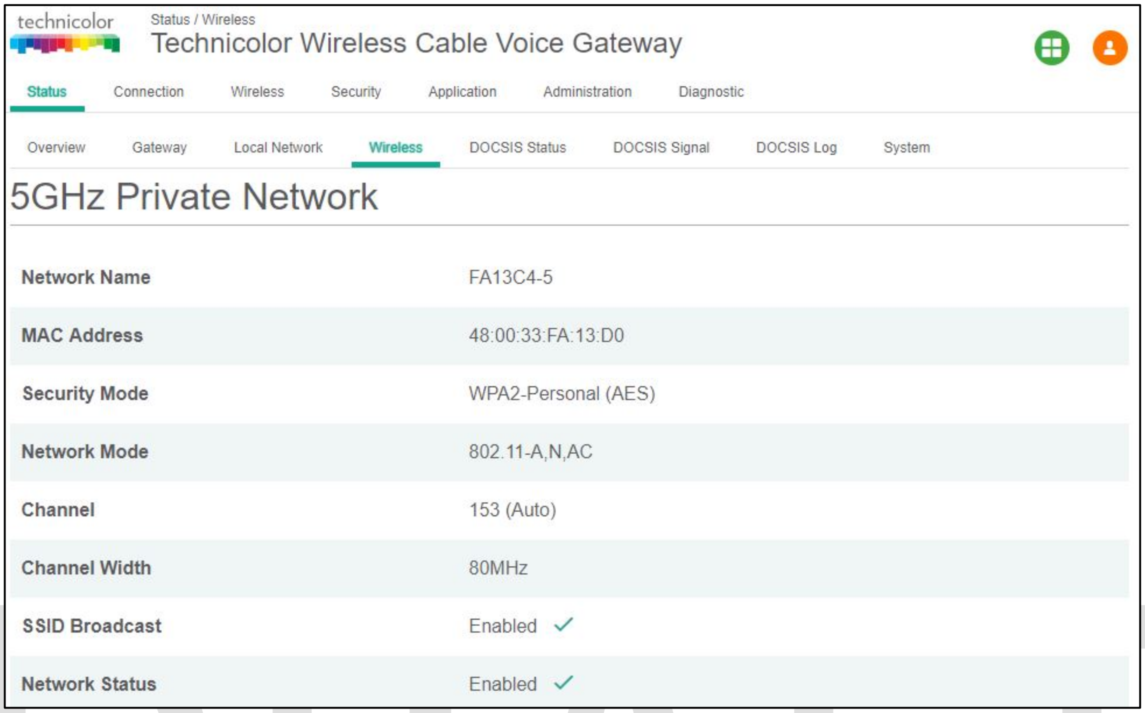


2.4GHz Private Network

Network Name	FA13C4-2.4
MAC Address	48:00:33:FA:13:C8
Security Mode	WPA2-Personal (AES)
Network Mode	802.11-G,N
Channel	11 (Auto)
Channel Width	40MHz
SSID Broadcast	Enabled ✓
Network Status	Enabled ✓

Figure 5.6

5GHz Network Information:



5GHz Private Network

Network Name	FA13C4-5
MAC Address	48:00:33:FA:13:D0
Security Mode	WPA2-Personal (AES)
Network Mode	802.11-A,N,AC
Channel	153 (Auto)
Channel Width	80MHz
SSID Broadcast	Enabled ✓
Network Status	Enabled ✓

Figure 5.7

5.5 DOCSIS Status

Status Tab / DOCSIS Status
Click on Status tab, and then click on DOCSIS Status. DOCSIS Status page explains the network connectivity and Cable Modem status. The following information is displayed:

Cable Modem Parameters:
This section displays information about the RF upstream Bonding, including CM Status, Active Time, IPv6 Address, IPv4 Address, Subnet Mask, IP Gateway, TFTP Server, Time Server, Time Offset, DHCP Lease Time, DHCP Rebind Time and DHCP Renew.

- CM Status – possible states are Below are the possible states for a cable modem other, notReady, notSynchronized, phySynchronized, usParametersAcquired, rangingComplete, ipComplete, todEstablished, securityEstablished, paramTransferComplete, registrationComplete, operational and accessDenied.
- Active time - The time since the network management portion of the system was last re-initialized.

Ethernet List:
This section displays information about the Ethernet List with Interface Name, Link Status, Link Speed and Link Duplex.

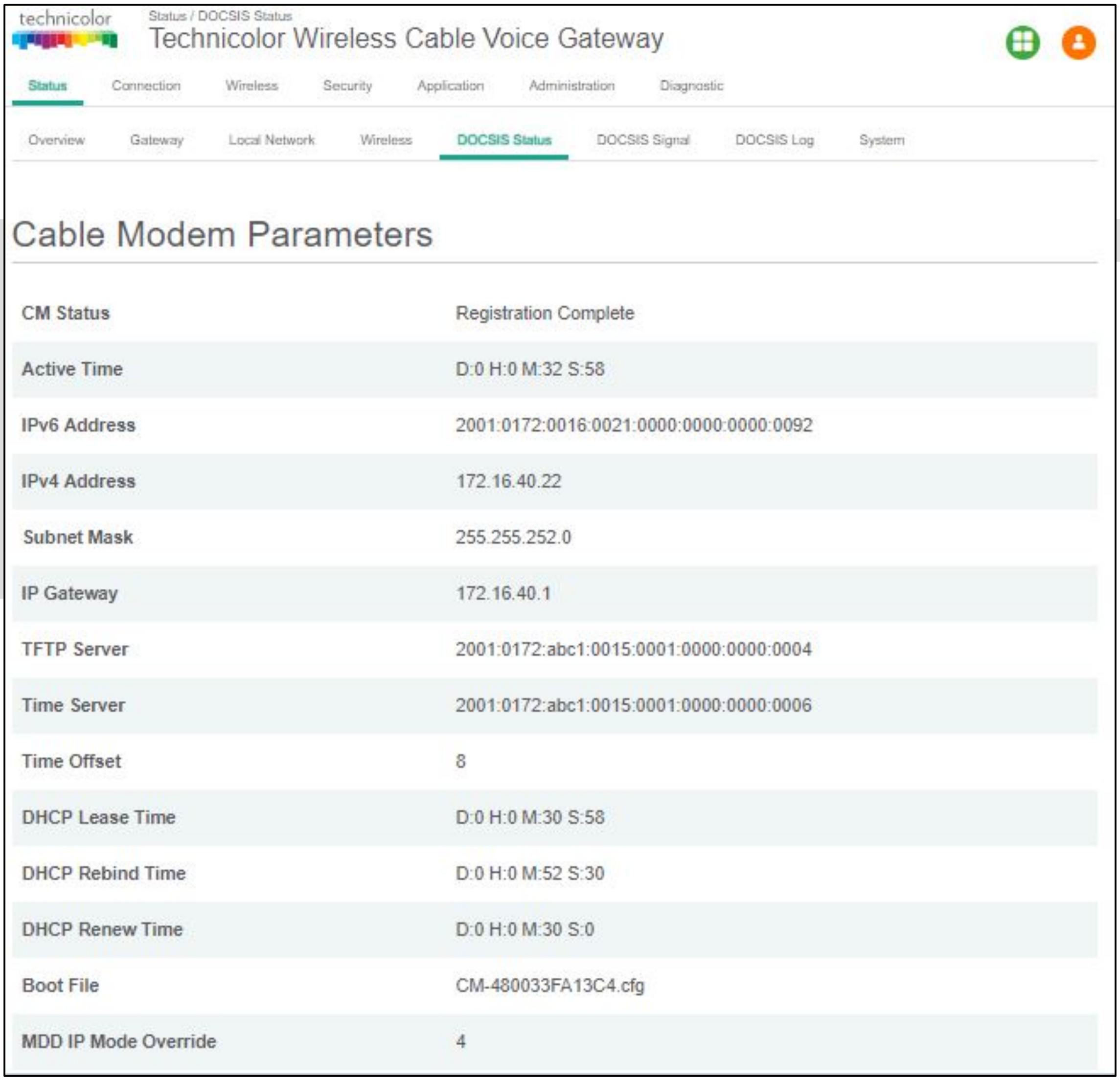
- Interface name displays Displays the port number in general (Ethernet 1 / Ethernet 2, etc.)

- Link Status - If there is any activity on the Link (Any Device connected) it shows "UP", else it will be "DOWN"
- Link Speed and Link Duplex - Speed of 10/100/1000 and is it half duplex, full duplex or Auto

CPE List:

- This section displays CPE List - displays information about the CPE List with IP Address (IPv4 and/or IPv6) and HW Address

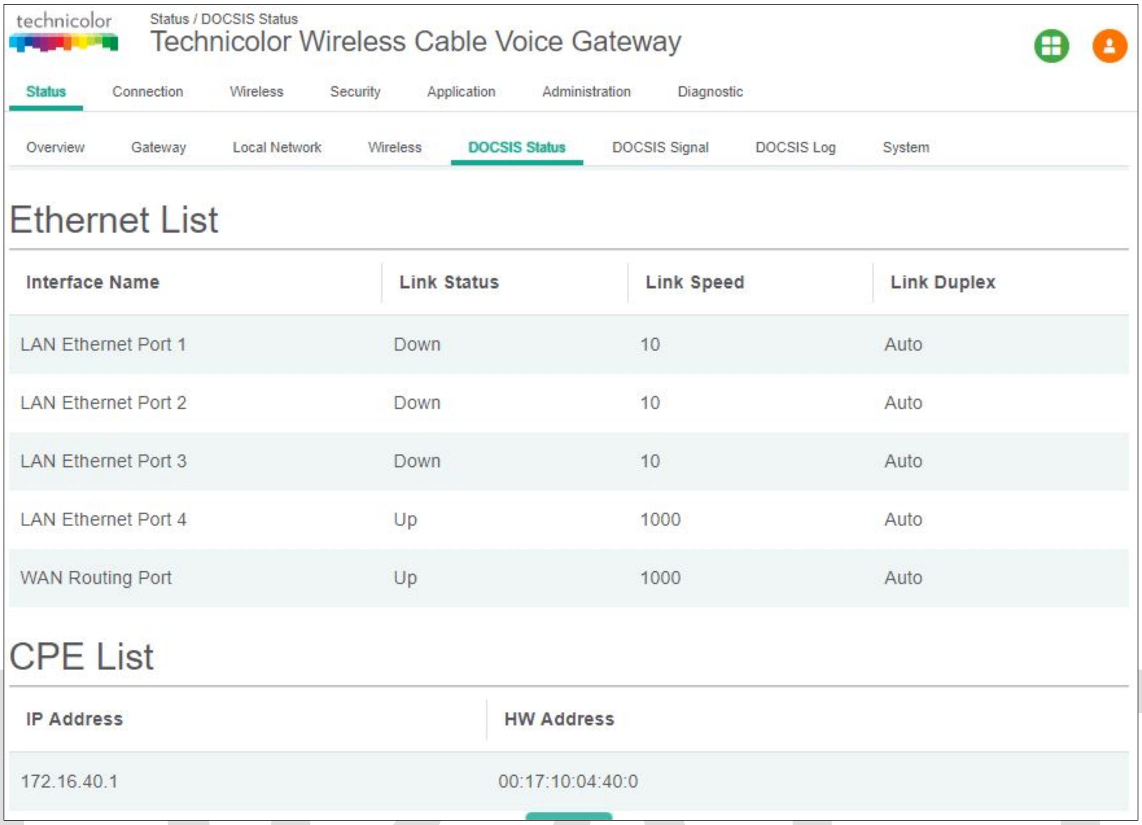
The following figures provide these details displayed in the page:



Cable Modem Parameters

CM Status	Registration Complete
Active Time	D:0 H:0 M:32 S:58
IPv6 Address	2001:0172:0016:0021:0000:0000:0000:0092
IPv4 Address	172.16.40.22
Subnet Mask	255.255.252.0
IP Gateway	172.16.40.1
TFTP Server	2001:0172:abc1:0015:0001:0000:0000:0004
Time Server	2001:0172:abc1:0015:0001:0000:0000:0006
Time Offset	8
DHCP Lease Time	D:0 H:0 M:30 S:58
DHCP Rebind Time	D:0 H:0 M:52 S:30
DHCP Renew Time	D:0 H:0 M:30 S:0
Boot File	CM-480033FA13C4.cfg
MDD IP Mode Override	4

Figure 5.8



Ethernet List

Interface Name	Link Status	Link Speed	Link Duplex
LAN Ethernet Port 1	Down	10	Auto
LAN Ethernet Port 2	Down	10	Auto
LAN Ethernet Port 3	Down	10	Auto
LAN Ethernet Port 4	Up	1000	Auto
WAN Routing Port	Up	1000	Auto

CPE List

IP Address	HW Address
172.16.40.1	00:17:10:04:40:0

Figure 5.9

5.6 DOCSIS Signal

Status Tab / DOCSIS Signal
Click on the Status tab then click on DOCSIS Signal. The DOCSIS Signal page displays the plant information on which the modem is connected.

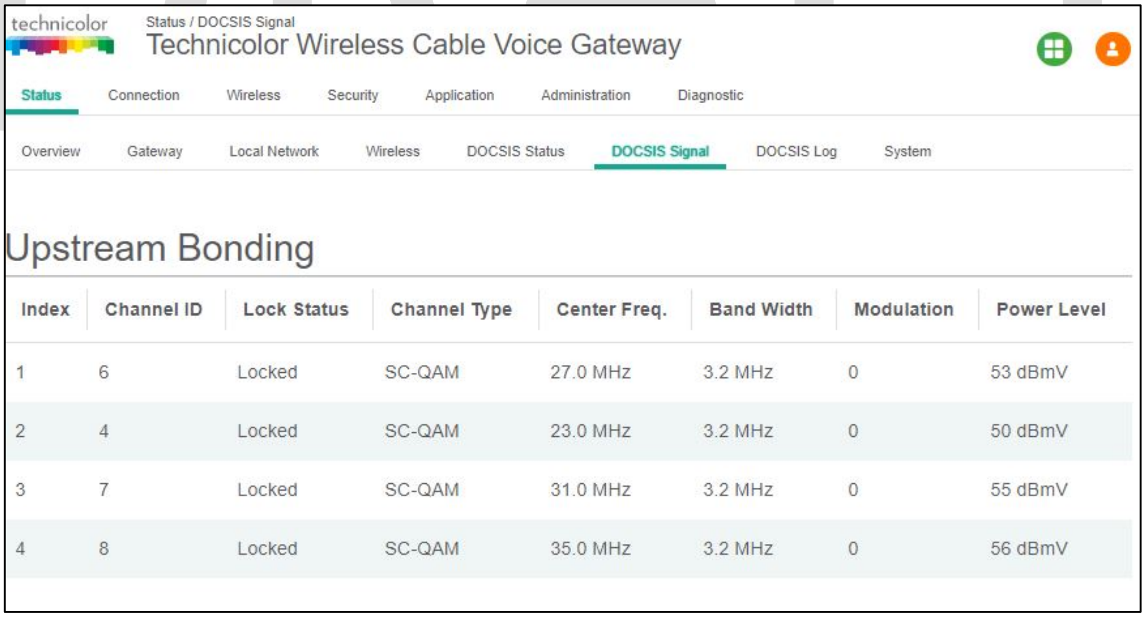
Upstream Bonding:
This section displays information about RF upstream Bonding, including upstream channel ID, Upstream Lock Status, Channel Type, Centre Freq., Band Width, Modulation, and Power Level (Tx Power level at gateway for the particular channel).

- Upstream Bonding - Number of channels locked to upstream which can be used for upstream data transfer
- Upstream channel ID - The CMTS identification of the upstream channel
- Upstream Lock Status - Displays Locked if QAM and FEC are locked (indicates that the channel is usable)
- Upstream Channel Type - Displays if it is a SC-QAM channel (Phy type 3) or a OFDMA channel (Phy type 5)
- Upstream Centre Frequency - The center of the frequency band associated with this upstream interface. Displays 0 if the frequency is undefined or unknown.
- Upstream Band Width -The bandwidth of this upstream interface as configured on the CMTS (Generally 1.6MHz, 3.2Mhz or 6.4MHz)

- Upstream Modulation - Displays the modulation used on upstream ATDMA, TDMA, SCDMA or MTDMA
- Upstream Power Level - Transmit power level at which the cable modem is transmitting on the respective channel

Downstream Bonding:
This section displays information about the RF downstream bonding with downstream channel ID, Downstream Lock status, Downstream Bond Status, Downstream Channel Type, Downstream Centre Freq., Downstream Band Width, Modulation, Power Level (Rx power level at the gateway for the specific channel) and SNR Level.

- Downstream Channel Id - The Cable Modem Termination System identification of the downstream channel within this particular MAC interface. If the interface is down, displays the most current value. If the downstream channel ID is unknown, 0 is displayed.
- Downstream Lock Status - Displays Locked if QAM and FEC are locked (indicates that the channel is usable)
- Downstream Bonding - Number of channels locked to downstream which can be used for downstream data transfer
- Downstream Channel Type - Displays if it is a SC-QAM channel or a OFDM channel
- Downstream Centre Frequency - The center of the downstream frequency associated with this channel
- Downstream Band Width - The bandwidth of this downstream channel. Most implementations are expected to support a channel width of 6 MHz (North America).
- Downstream Channel Modulation - The modulation type associated with this downstream channel. If the interface is down, it displays "unknown", else it will be either QAM64 or QAM256 based on CMTS configuration

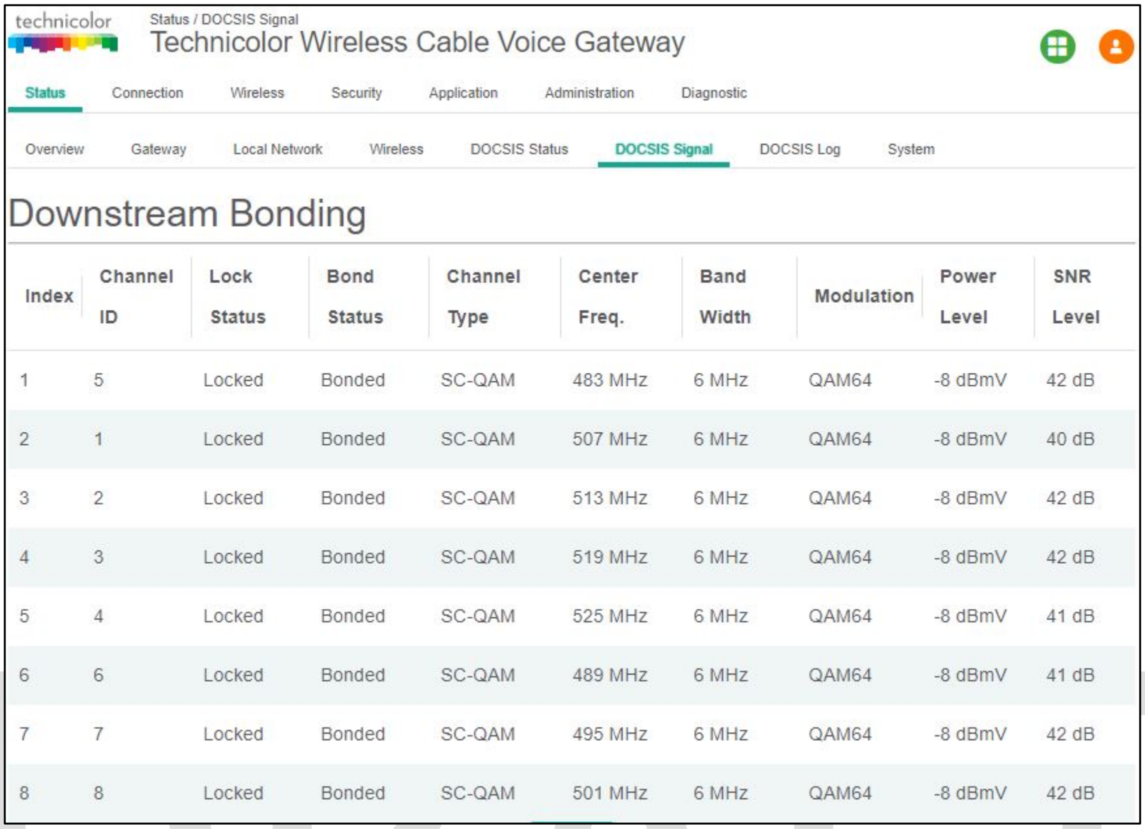


Technicolor Wireless Cable Voice Gateway

Upstream Bonding

Index	Channel ID	Lock Status	Channel Type	Center Freq.	Band Width	Modulation	Power Level
1	6	Locked	SC-QAM	27.0 MHz	3.2 MHz	0	53 dBmV
2	4	Locked	SC-QAM	23.0 MHz	3.2 MHz	0	50 dBmV
3	7	Locked	SC-QAM	31.0 MHz	3.2 MHz	0	55 dBmV
4	8	Locked	SC-QAM	35.0 MHz	3.2 MHz	0	56 dBmV

Figure 5.10



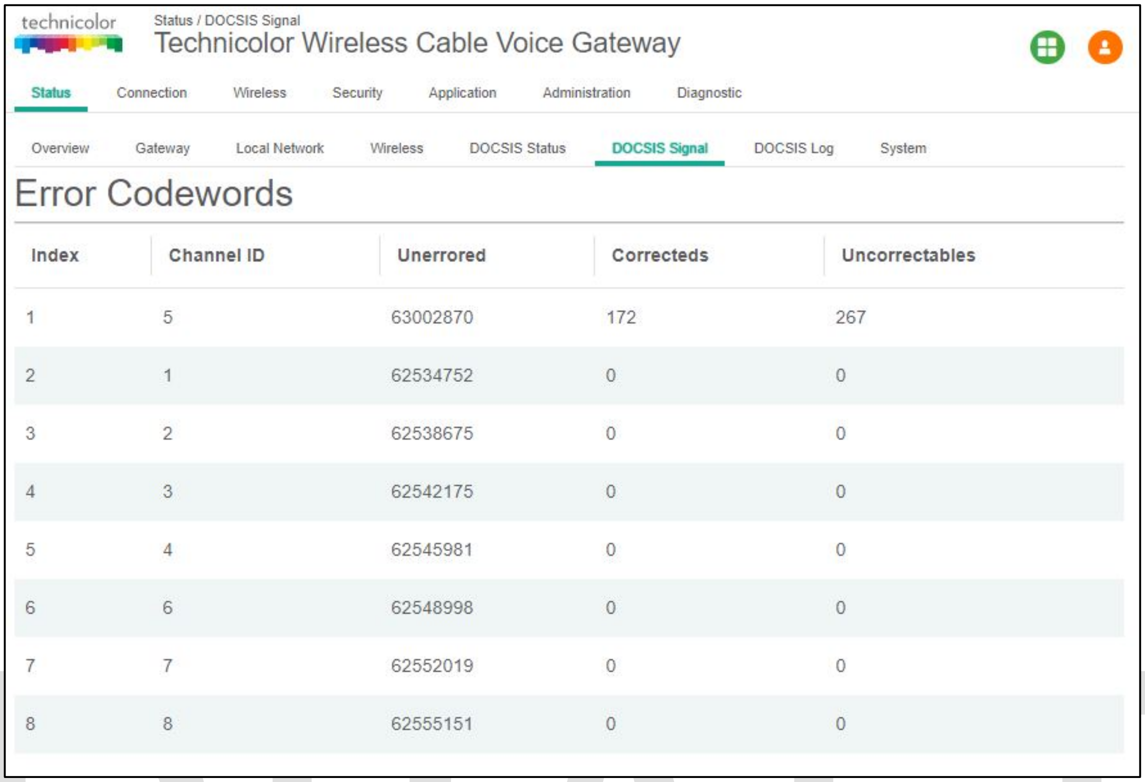
Downstream Bonding

Index	Channel ID	Lock Status	Bond Status	Channel Type	Center Freq.	Band Width	Modulation	Power Level	SNR Level
1	5	Locked	Bonded	SC-QAM	483 MHz	6 MHz	QAM64	-8 dBmV	42 dB
2	1	Locked	Bonded	SC-QAM	507 MHz	6 MHz	QAM64	-8 dBmV	40 dB
3	2	Locked	Bonded	SC-QAM	513 MHz	6 MHz	QAM64	-8 dBmV	42 dB
4	3	Locked	Bonded	SC-QAM	519 MHz	6 MHz	QAM64	-8 dBmV	42 dB
5	4	Locked	Bonded	SC-QAM	525 MHz	6 MHz	QAM64	-8 dBmV	41 dB
6	6	Locked	Bonded	SC-QAM	489 MHz	6 MHz	QAM64	-8 dBmV	41 dB
7	7	Locked	Bonded	SC-QAM	495 MHz	6 MHz	QAM64	-8 dBmV	42 dB
8	8	Locked	Bonded	SC-QAM	501 MHz	6 MHz	QAM64	-8 dBmV	42 dB

Figure 5.11

Error Codewords:

This section displays Error Codewords, the information about the Channel ID, Unerrored, Correcteds and Uncorrectables.



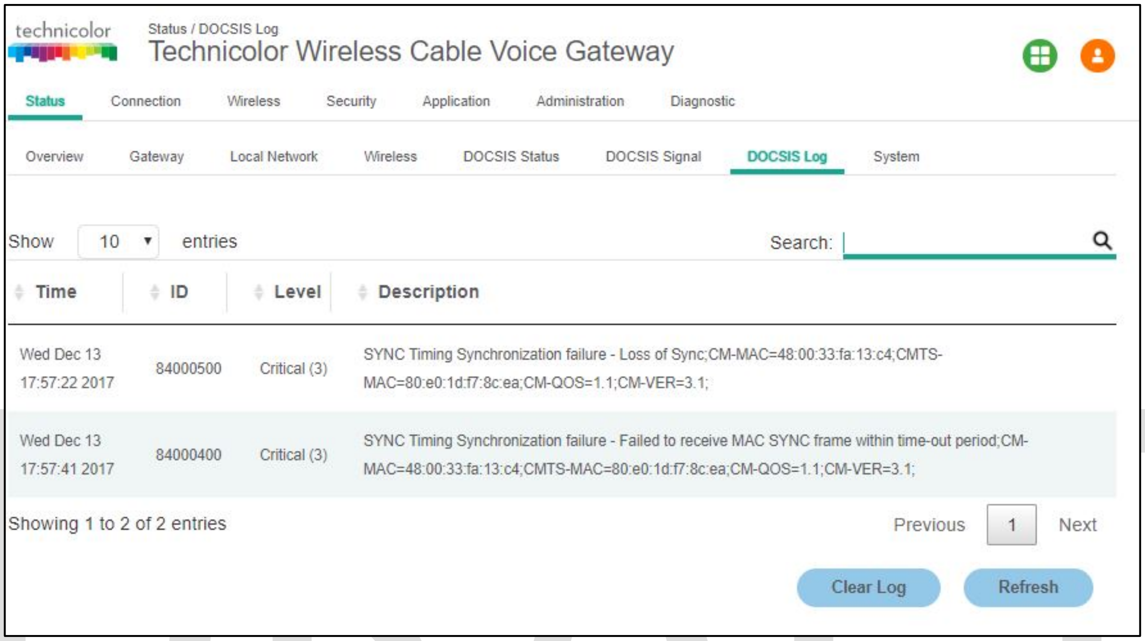
Error Codewords

Index	Channel ID	Unerrored	Correcteds	Uncorrectables
1	5	63002870	172	267
2	1	62534752	0	0
3	2	62538675	0	0
4	3	62542175	0	0
5	4	62545981	0	0
6	6	62548998	0	0
7	7	62552019	0	0
8	8	62555151	0	0

Figure 5.12

5.7 DOCSIS Log

Status Tab / DOCSIS Log
Click on the Status tab then click on DOCSIS Log. The page displays information about the DOCSIS Log including Time, ID, Level and Description for the entries. The number of entries to be listed can be selected from the drop down menu corresponding to the “Show entries” field.



Time	ID	Level	Description
Wed Dec 13 17:57:22 2017	84000500	Critical (3)	SYNC Timing Synchronization failure - Loss of Sync;CM-MAC=48:00:33:fa:13:c4;CMTS-MAC=80:e0:1d:f7:8c:ea;CM-QOS=1.1;CM-VER=3.1;
Wed Dec 13 17:57:41 2017	84000400	Critical (3)	SYNC Timing Synchronization failure - Failed to receive MAC SYNC frame within time-out period;CM-MAC=48:00:33:fa:13:c4;CMTS-MAC=80:e0:1d:f7:8c:ea;CM-QOS=1.1;CM-VER=3.1;

Showing 1 to 2 of 2 entries

Figure 5.13

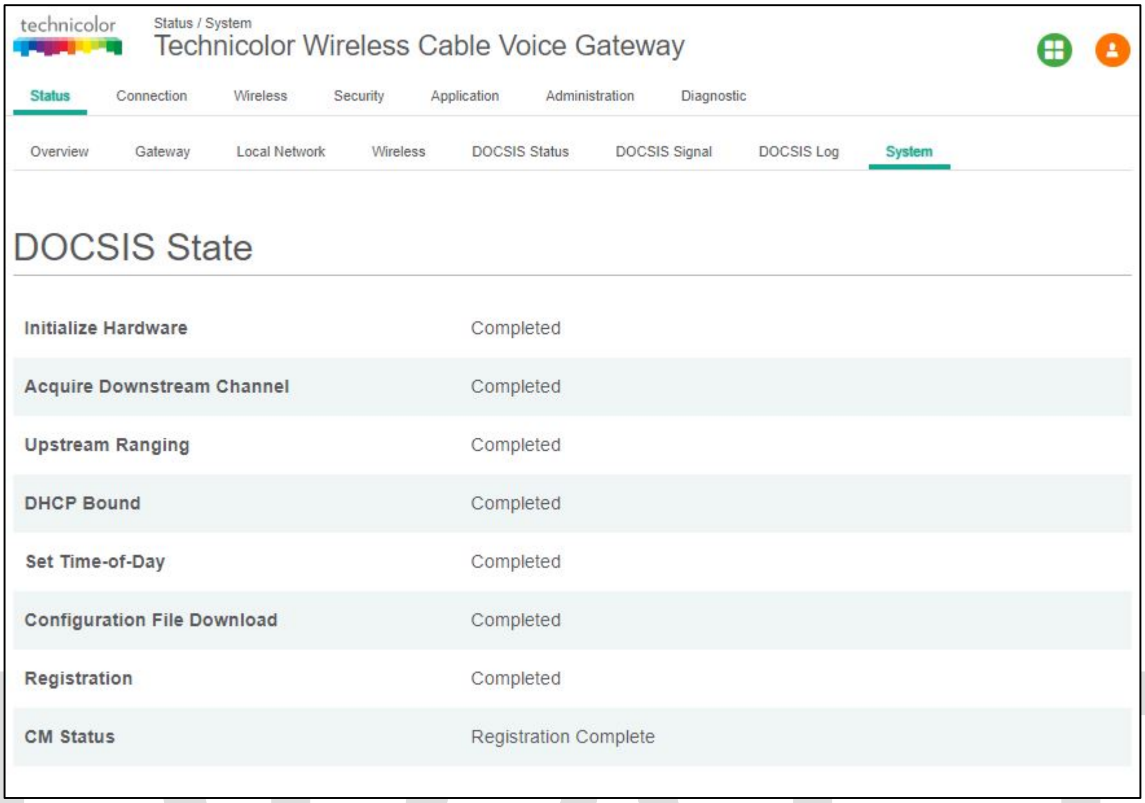
5.8 System

Status Tab / System
Click on the Status tab then click on System. This page displays further information on the DOCSIS connection, system software and hardware configuration.

DOCSIS State:
This section displays information about the DOCSIS State including Initialize Hardware, Acquire Downstream Channel, Upstream Ranging, DHCP Bound, Set Time-of-Day, Configuration File Download, Registration and CM Status.

System Software:
This section displays information about the System Software including Model Name, Vendor, Serial Number, Software Version, Firmware File Name, Firmware Build Time, Bootloader Version, Core Version, Local Time and System Uptime.

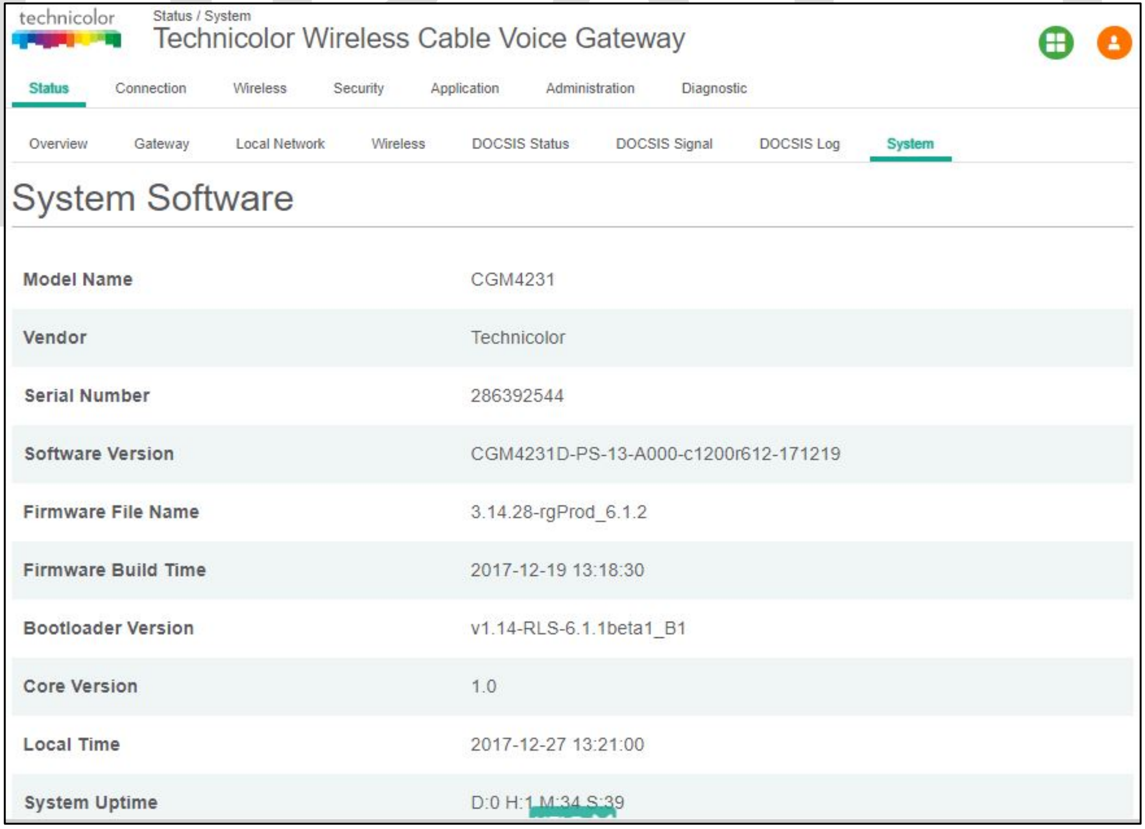
System Hardware:
This section displays information about the System Hardware including Hardware Version, Processor Speed, Flash Size, Total Memory and MAC Address.



DOCSIS State

Initialize Hardware	Completed
Acquire Downstream Channel	Completed
Upstream Ranging	Completed
DHCP Bound	Completed
Set Time-of-Day	Completed
Configuration File Download	Completed
Registration	Completed
CM Status	Registration Complete

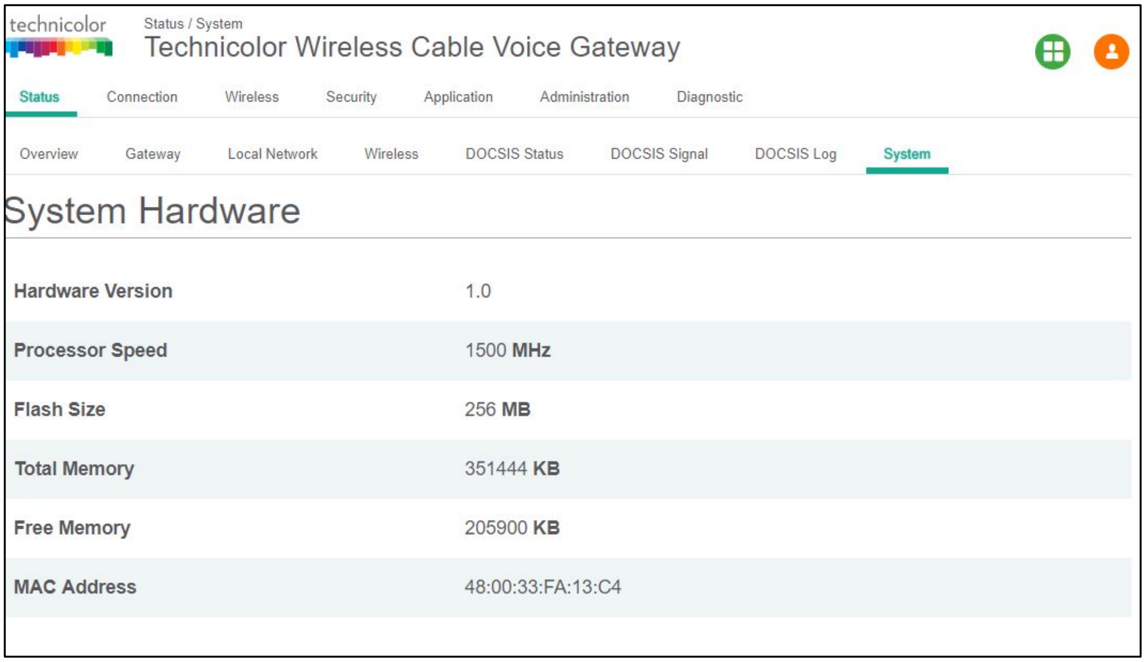
Figure 5.14



System Software

Model Name	CGM4231
Vendor	Technicolor
Serial Number	286392544
Software Version	CGM4231D-PS-13-A000-c1200r612-171219
Firmware File Name	3.14.28-rgProd_6.1.2
Firmware Build Time	2017-12-19 13:18:30
Bootloader Version	v1.14-RLS-6.1.1beta1_B1
Core Version	1.0
Local Time	2017-12-27 13:21:00
System Uptime	D:0 H:1 M:34 S:39

Figure 5.15



System Hardware

Hardware Version	1.0
Processor Speed	1500 MHz
Flash Size	256 MB
Total Memory	351444 KB
Free Memory	205900 KB
MAC Address	48:00:33:FA:13:C4

Figure 5.16

6 Connection

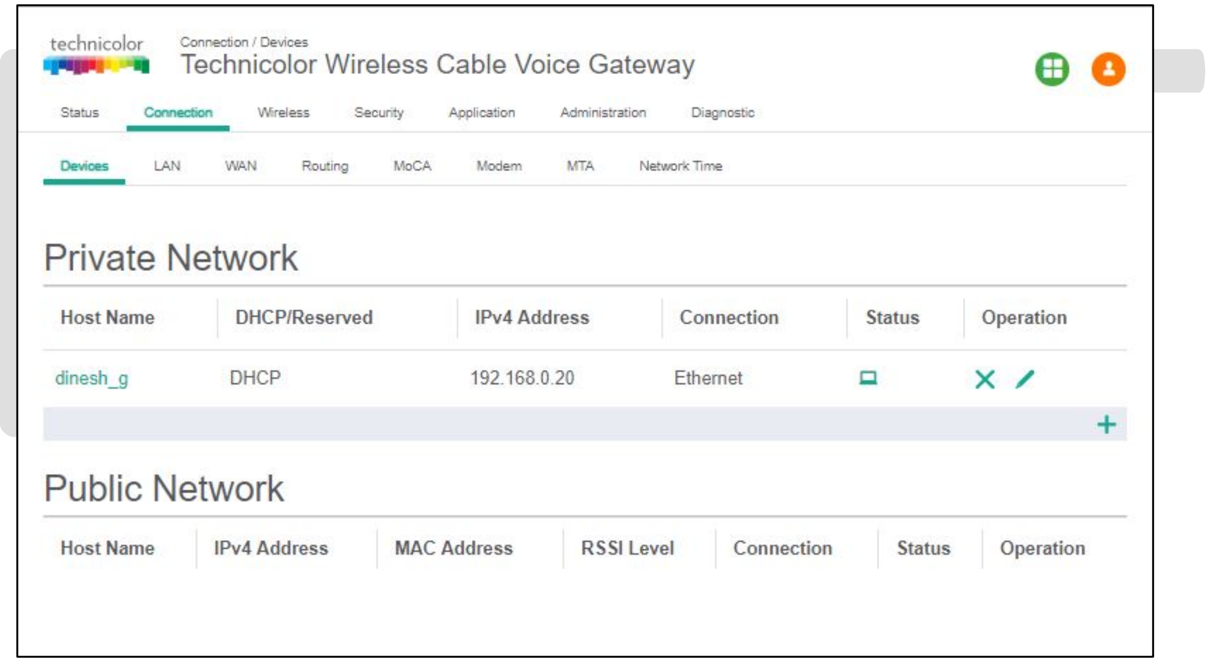
The following is a list of pages that are only visible to an Advanced User with specific credentials.

6.1 Devices

Connection Tab / Devices

The Connection/Device page displays all the clients that are connected to the private and the public/guest network. The page also displays the details of the connected device like Interface type, connection type, device name and the IP Address.

Click on Connection tab then click on Devices in the Web UI. The devices page appears populated with the information below:



Private Network

Host Name	DHCP/Reserved	IPv4 Address	Connection	Status	Operation
dinesh_g	DHCP	192.168.0.20	Ethernet	💻	✕ ✎

Public Network

Host Name	IPv4 Address	MAC Address	RSSI Level	Connection	Status	Operation

Figure 6.1

6.2 LAN

Connection Tab / LAN

Click on the Status tab then click on Local Network. The page displays details about the LAN configuration. The page also provides options to configure the LAN connections.

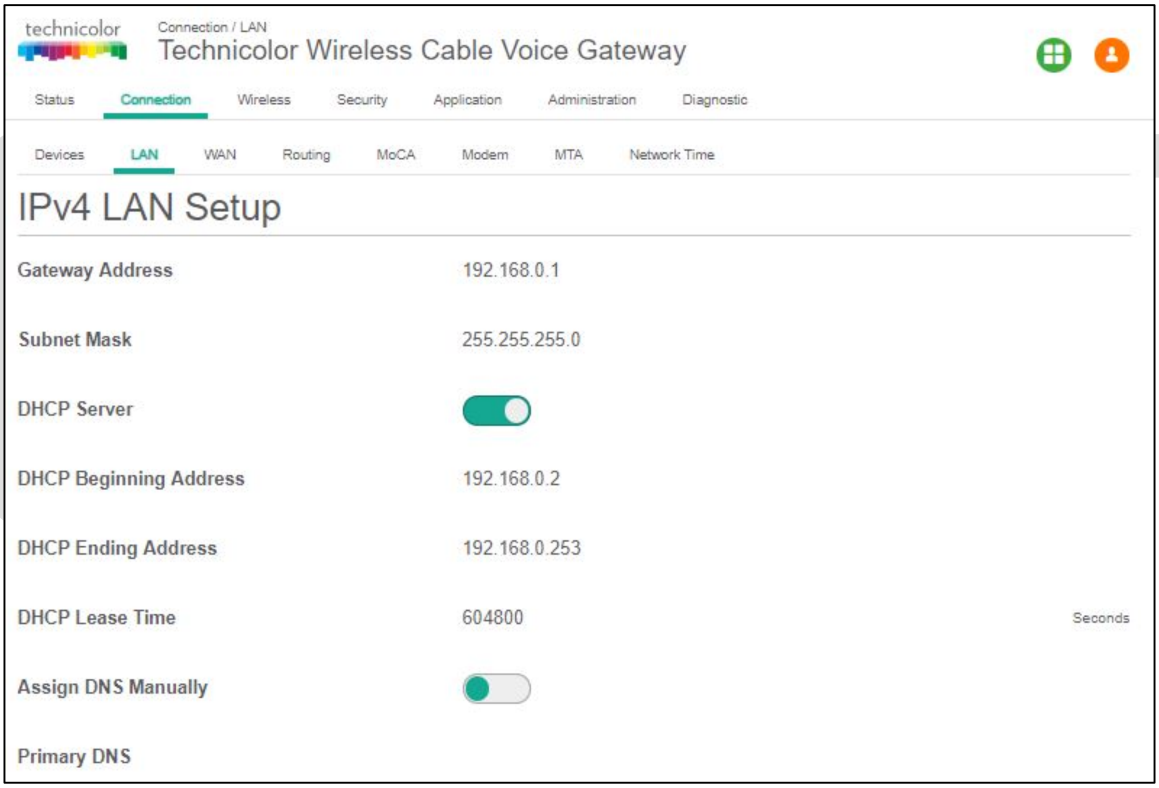
LAN Information:

The LAN Information section on the Local Network page displays details about the Gateway Address, Subnet Mask, DHCP details (Server, DHCP Beginning Address and DHCP Ending Address) and DNS details.

Clients connected to the LAN side, which are connected via wired or wireless, get IP addresses from the DHCP server running on the gateway. The beginning and end IP address define how many clients can be connected to the gateway (or the number of valid IP addresses that can be assigned). The gateway address of 192.168.0.1 is the default IP address; it is user configurable.

The user can modify the LAN configuration including the number of IP addresses. If a client needs to be assigned with a static address, the user has to select the static IP option and enter the MAC address of the client that needs the static IP address.

The life time of the DHCP address is defined in the DHCP lease time and again it is user configurable. By default, the lease time is 86400 seconds.



IPv4 LAN Setup

Gateway Address	192.168.0.1
Subnet Mask	255.255.255.0
DHCP Server	●
DHCP Beginning Address	192.168.0.2
DHCP Ending Address	192.168.0.253
DHCP Lease Time	604800 Seconds
Assign DNS Manually	○
Primary DNS	

Figure 6.2

6.2.1 LAN Setup

By default, the DHCP server of the Wireless Gateway is enabled to distribute IP addresses to LAN client devices. To have a wireless Home gateway, the DHCP server is enabled to distribute the IP Address starting from the range that is provisioned in Starting IP Address going up to the Maximum number of DHCP users. Lease Time and Time Zones are provisioned for DHCP Parameters. The LAN IP address default setup is192.168.x.x and the Mask is 255.255.255.0

6.2.1.1 Procedure to set SNMP LAN Settings

The following MIBs are used to configure the LAN settings:

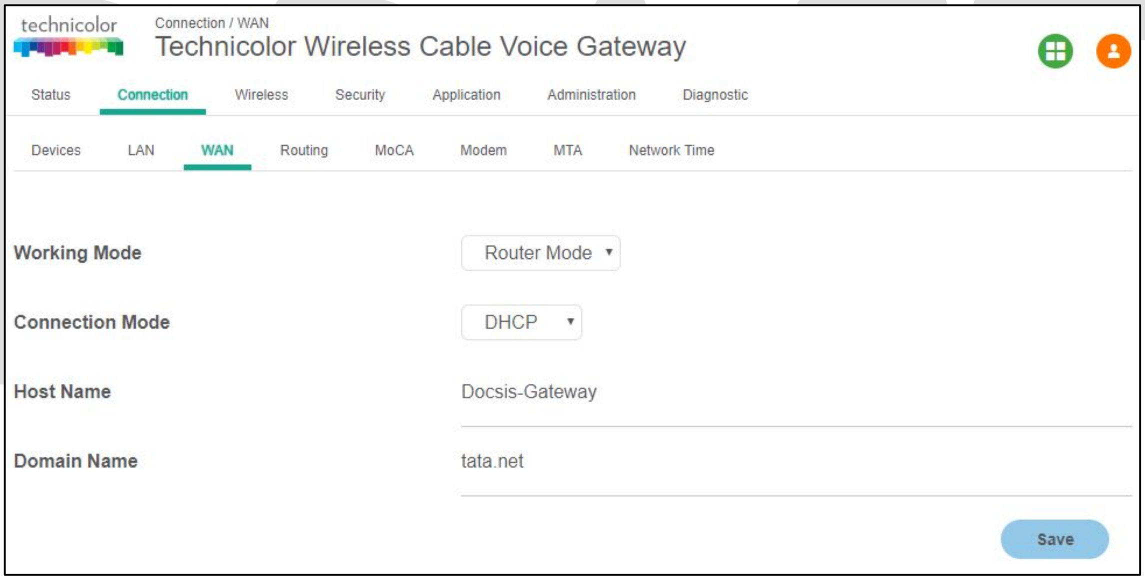
- **tchRgIpMgmtLanSubnetMask**
- **tchRgIpMgmtLanGateway**
- **tchRgIpMgmtLanDhcpServer**
- **tchRgIpMgmtLanDhcpServerPoolStart**
- **tchRgIpMgmtLanDhcpServerPoolEnd**
- **tchRgIpMgmtLanDhcpServerLeaseTime**
- **tchRgIpMgmtDnsServerIp**

6.3 WAN

6.3.1 User Provisioning of WAN

Connection Tab / WAN

Click on the Connection tab then click on the WAN tab. The page displays WAN configuration information. The page also allows the setting of WAN configuration - Working Mode (Router Mode, Bridged Mode), Connection Mode (DHCP, Static IP), Host Name and Domain Name.



Working Mode: Router Mode ▾

Connection Mode: DHCP ▾

Host Name: Docsis-Gateway

Domain Name: tata.net

Figure 6.3

When the Gateway WAN provisioning is enabled with DHCP, IPv4 and IPv6 DHCP client on the gateway will initiate DHCP request to get the eRouter / WAN IP for the gateway. In case of DHCP v6, the eRouter IP is obtained from the MSO network through IP Prefix delegation.

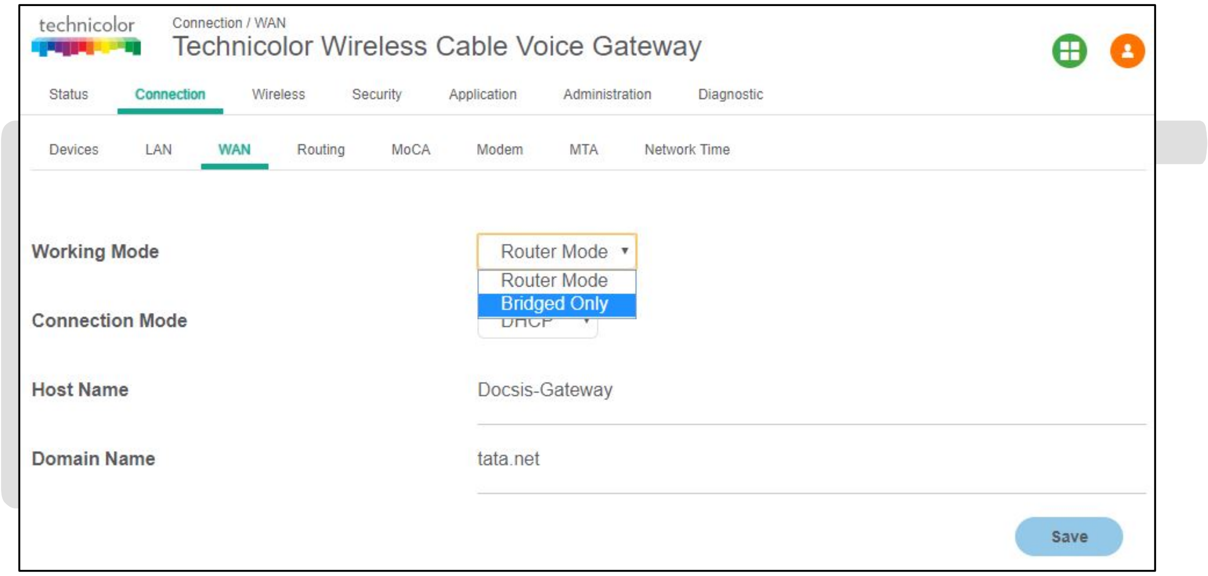
6.3.1.1 Working Mode

The Gateway can be configured to operate in Bridge or Router mode using this drop-down tab, which allows specific configuration of the device to Router or Bridge Mode for access and security.

In Router mode, routing functionality is enabled in the gateway, the DHCP server runs and all the LAN and Wi-Fi clients can obtain private, LAN IP addresses via DHCP. The NAT functionality in the gateway translates the private IP to the eRouter IP for external Internet access. When the gateway is provisioned with dualstack, then DHCP v6 and v4 servers would run in the gateway for the LAN clients.

In Bridge mode, the routing functionality is disabled (DHCP and NAT functionalities are similarly disabled). All LAN clients receive public IPs from the MSO. The Wi-Fi network is disabled in Bridge mode.

Router Mode:
If in Bridge mode and Router Mode is selected, the Gateway will reboot automatically and operate in Router Mode after reboot. Routing functionality is enabled with Wi-Fi and LAN set to active. The management IP address will change LAN configuration (such as from x.x.x.x to y.y.y.y. For instance, it may change from 10.0.0.1 to 192.168.0.1.)



Technicolor Wireless Cable Voice Gateway

Working Mode: Router Mode

Connection Mode: DHCP

Host Name: Docsis-Gateway

Domain Name: tata.net

Figure 6.4

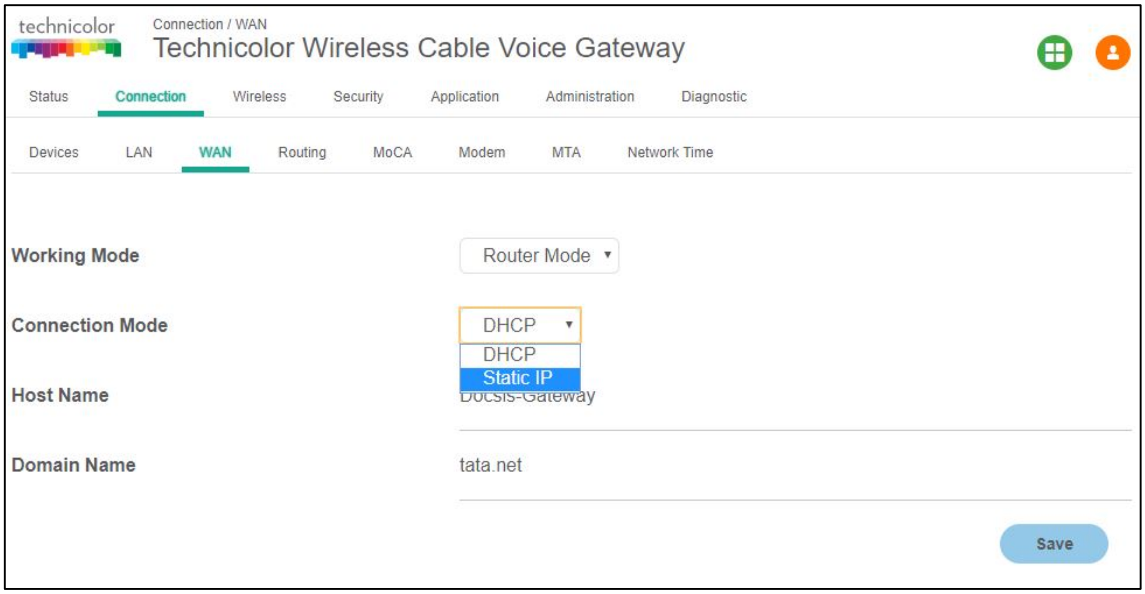
Bridge Mode:
If in Router Mode and Bridge Mode option is selected, the Gateway will reboot automatically and operate in Bridge Mode after reboot. The routing functionality, Wi-Fi and LAN ports 2, 3, and 4 will be disabled. Only LAN port 1 will remain active. The management IP address will change to 192.168.100.1.

NB. The Gateway will revert to Router mode upon factory reset via rear panel switch.

6.3.1.2 Connection Mode

There are 2 connection modes possible – DHCP or Static IP. When DHCP is selected, the WAN IP (eRouter IP) is configured automatically by the MSO DHCP Server.

In case of static IP, the details (IP address, Subnet Mask, Default Gateway, DNS configuration, MTU, etc.) needs to be obtained from the MSO and entered through the WebUI.



Working Mode: Router Mode

Connection Mode: DHCP

Host Name: Docsis-Gateway

Domain Name: tata.net

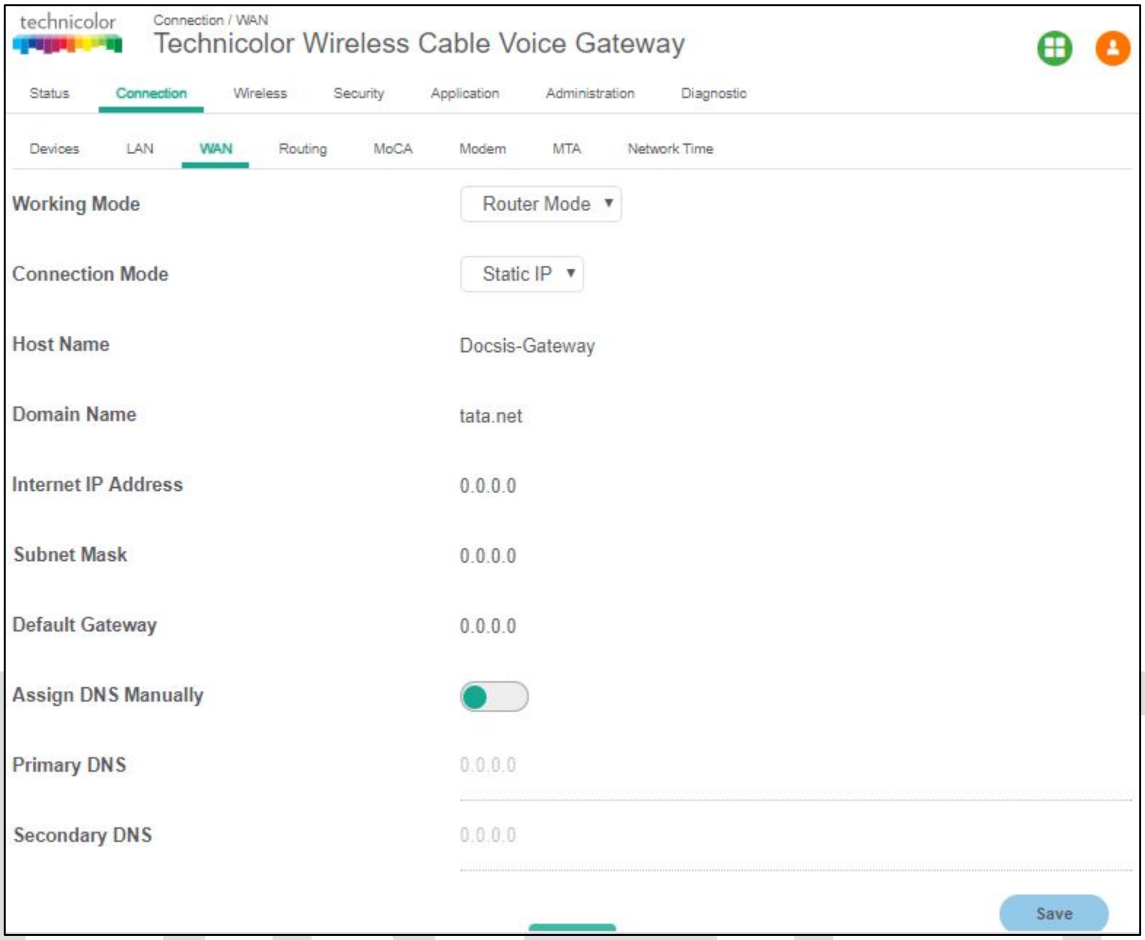
Figure 6.5

Provisioning WAN IP through DHCP (only for router mode)

When the WAN Connection Mode is selected as DHCP, no more user settings will be available to configure WAN IP. The WAN side will receive an IP address as per the rules specified in the DHCP configuration of the MSO/ISP.

Provisioning with Static IP

The Static IP for WAN interface is provided by the Service Provider.



Technicolor Wireless Cable Voice Gateway

Working Mode: Router Mode ▾

Connection Mode: Static IP ▾

Host Name: Docsis-Gateway

Domain Name: tata.net

Internet IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Default Gateway: 0.0.0.0

Assign DNS Manually: ●

Primary DNS: 0.0.0.0

Secondary DNS: 0.0.0.0

Figure 6.6

While configuring the Connection Mode as Static IP, the user needs to configure the following:

Internet IP Address
The Gateway's public IP address, as seen from the Internet.

Subnet Mask
The Gateway's Subnet Mask.

Default Gateway
The default gateway of the Service Provider’s router.

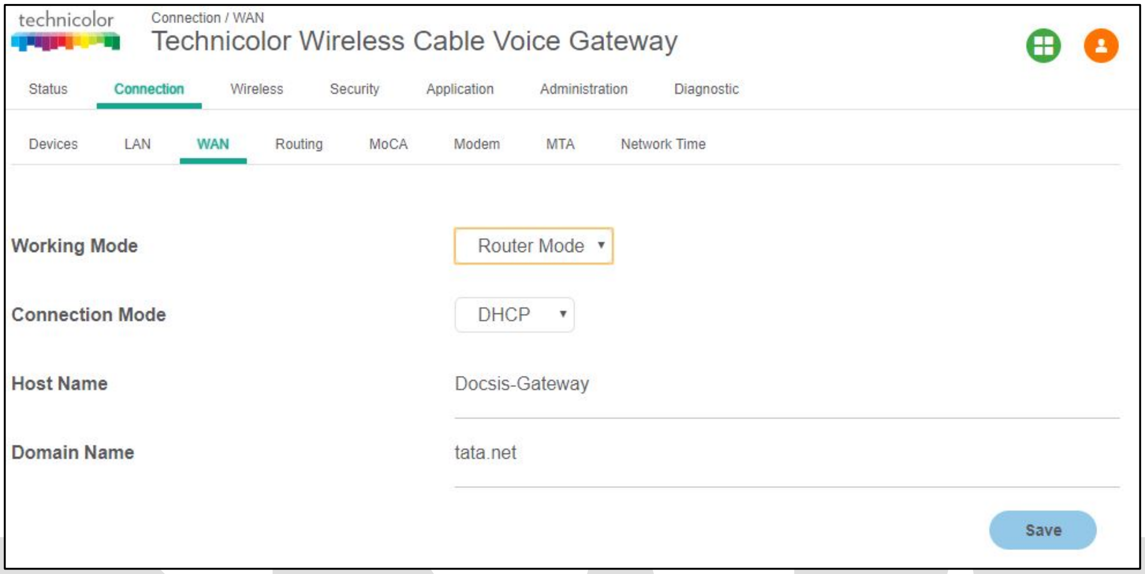
Primary DNS (Required) and **Secondary DNS** (Optional)
The DNS (Domain Name System) server IPaddress(es) that are to be used with the Wireless Gateway in order that client devices may perform name resolution.

6.3.1.3 Host Name (Optional)

The Host Name field is optional but may be required by some Service Providers. The default host name is the model number of the device.

6.3.1.4 Domain Name (Optional)

Enter in the local domain name for the network.



Working Mode: Router Mode

Connection Mode: DHCP

Host Name: Docsis-Gateway

Domain Name: tata.net

Figure 6.7

Setting the values of different parameters (Working mode, Connection Mode, Host name, Domain name):

- Click on the corresponding drop down menu and select the required values
- Press Save

6.3.2 SNMP Provisioning for WAN

tchRgIpMgmtWanMode determines whether the WAN IP address is assigned by a DHCP server from the Provisioning servers in the headend or assigned statically by the user or going to use a Dual IP. When Dual IP is select, the second IP stack is used for user options.

In case of Static Assignment use **tchRgIpMgmtWanAddrStatic** to fill in the details.

tchRgIpMgmtWanMtu & **tchRgIpMgmtWanTtl** can be optionally set.

tchRgIpMgmtWanDualIpAddr is where the second IP can be filled in and

tchRgIpMgmtWanDualIpRipAdvertised RIP advertised for the access.

tchRgIpMgmtWanAddrBackupDefGw is the default gateway used when the Modem is offline.

User Access MIBS defined in CM MIB set should control the Username & Password to Change. Remote Web access MIBs are also added in CM MIBs for User access.

6.3.3 Dual Stack Router

In dual stack configuration, eRouter will have both an IPv4 and IPv6 address. The gateway can support a mix of devices that support IPV4 and IPv6. To set eRouter in Dual IP stack (IPv4 and IPv6), set TLV 202 to Dual or set rdkbRgDeviceMode to dualstack(5).

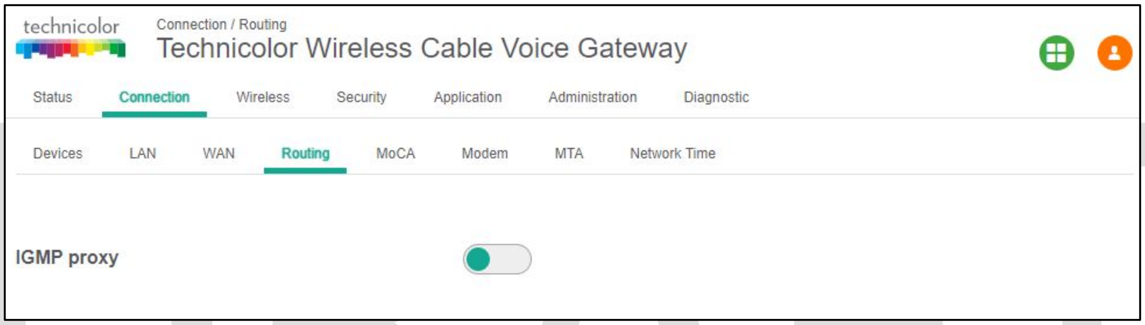
6.4 Routing

The routing view enables the user to configure RIP. IGMP Proxy can also be enabled or disabled from this view.

Connection Tab / Routing
Click on the Connection tab then click on Routing. This page displays Routing setup information for RIP. Here, IGMP Proxy can be displayed and set.

6.4.1 Enable / Disable IGMP Proxy

IGMP Proxy is used to enable multicast feature support. Users can enable or disable the IGMP Proxy using by selecting the button on the page.



IGMP proxy

Figure 6.8

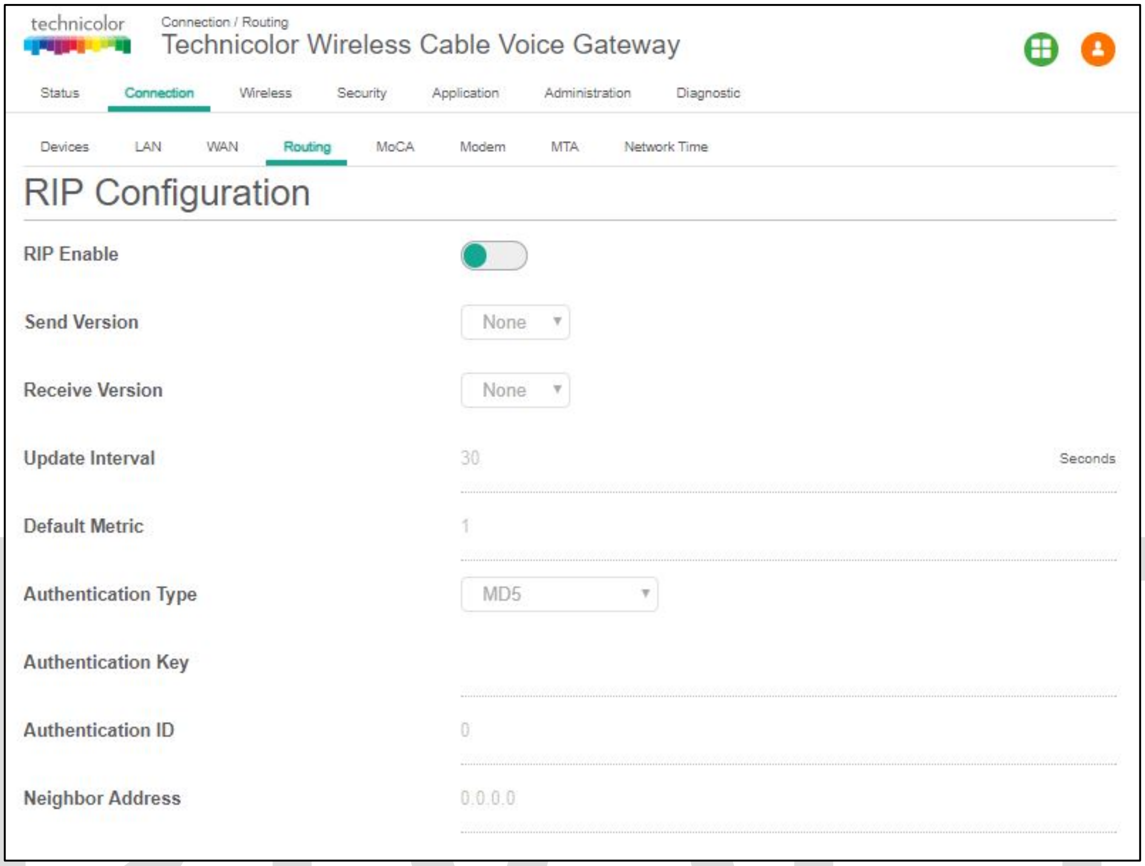
6.4.2 RIP

The Routing Information Protocol (RIP) defines a way for routers, which connect networks using the Internet Protocol (IP), to share information about how to route traffic among networks. RIP is classified by the Internet Engineering Task Force (IETF) as an Interior Gateway Protocol (IGP), one of several protocols for routers moving traffic around within a larger autonomous system network -- e.g., a single enterprise's network that may be comprised of many separate local area networks (LANs) linked through routers. To configure the RIP feature, the user needs to provide the following information:

- RIP (enable disable),
- Send Version(Version 2 recommended)
- Receive Version (Version 2 recommended)
- Update Interval (duration between route updates – default 30 seconds)
- Default Metric
- Authentication Type
- Authentication Key
- Authentication ID
- Neighbour Address (Next hop address)

Connection Tab / Routing

Click on the Connection tab then click on the Routing tab. The gateway will display the information below.



RIP Configuration

RIP Enable

Send Version: None

Receive Version: None

Update Interval: 30 Seconds

Default Metric: 1

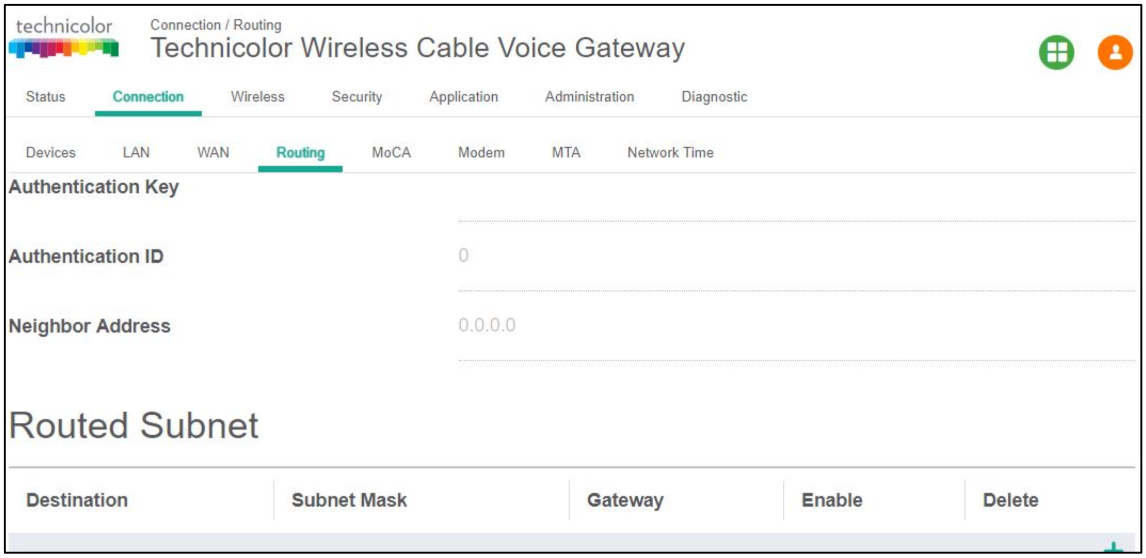
Authentication Type: MD5

Authentication Key

Authentication ID: 0

Neighbor Address: 0.0.0.0

Figure 6.9



Authentication Key

Authentication ID: 0

Neighbor Address: 0.0.0.0

Routed Subnet

Destination	Subnet Mask	Gateway	Enable	Delete

Figure 6.10

In order to change the configuration, the user needs to click on the parameters and change the values appropriately and press the save button provided in the page.

6.4.3 SNMP Provisioning for Routing

Router Advance Feature can be configured with following MIB
tchCmWebAccessUserIfLevel int 100 → For Router Advance feature

MaxCPE settings (specific to CM config file)

RIPv2 would advertise Primary LAN (LAN.32) NETWORK

tchRgRipMd5KeyId: Not implemented
tchRgRipInterval: Available
tchRgRipDestIpAddressType: Available
tchRgRipDestIpAddress: Available

LAN.32 in routed mode with Public IP address /30 ranges with NAT disabled

tchRgIpMgmtLanMode: Available
tchRgIpMgmtLanNetwork: Available
tchRgIpMgmtLanSubnetMask: Available
tchRgIpMgmtLanGateway: Available
tchRgIpMgmtLanNapt: Available

Wireless Gateway obtains its WAN IP address dynamically or through dual IP
Note: Not Available Currently

In case the customer network is behind a router (Example with Customer Router), Customer subnet needs to be advertised back to the IP backbone network (Static Configuration).

tchRgIpMgmtStaticRouteNetwork: Available
tchRgIpMgmtStaticRouteSubnetMask: Available
tchRgIpMgmtStaticRouteGateway: Available
tchRgIpMgmtStaticRouteRipAdvertise: Available
tchRgIpMgmtStaticRouteRowStatus: Available

6.5 MoCA

The CGM4231 Wireless Gateway includes a MoCA interface, enabling the extension of the LAN network via coaxial wiring to which the Wireless Gateway is connected.

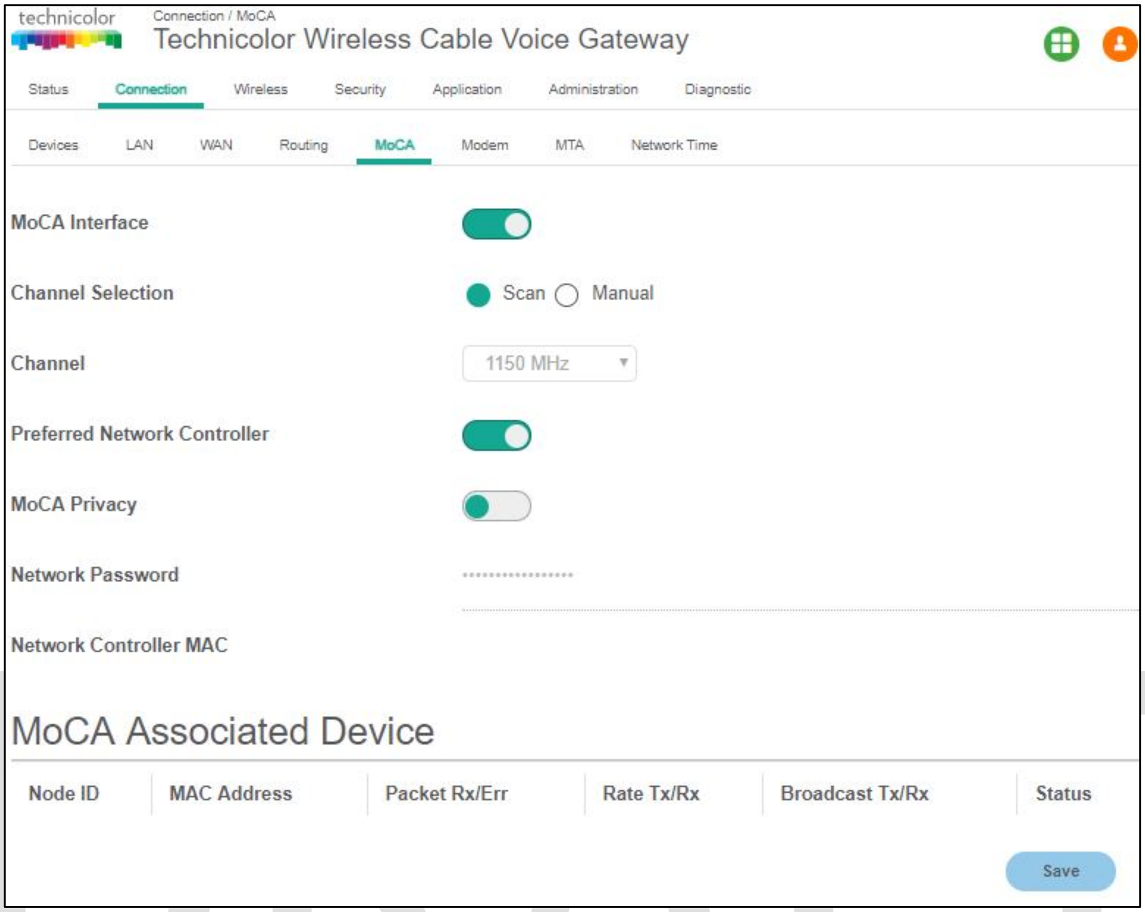
6.5.1 User Provisioning for MoCA

The MoCA feature of the Wireless Gateway may be configured via the MoCA page, accessible from the Connection tab of the homepage. From here, the following may be configured, depicted in figure 6.11 below.

- MoCA interface enable/disable via the “MoCA Interface” option
- MoCA channel selection may be configured to scan or manual. If manual is selected, the channel may be configured by selecting the center frequency from the drop-down box which because active upon selecting the manual option.
- Preferred network controller influences which MoCA device in the MoCA network controls the MoCA network.
- MoCA privacy controls whether the MoCA network is encrypted. If this setting is enabled, all MoCA devices on the network must be configured to use the same network password.
- The network controller MAC shows the MAC address of the MoCA device currently in control of the network.

MoCA Associated Device Table

This table displays the list of currently connected MoCA devices and connection status including Node ID, MAC Address, Packet Rx/Err, Rate Tx/Rx, Broadcast Tx/Rx and Status.



MoCA Interface

Channel Selection ● Scan ○ Manual

Channel 1150 MHz

Preferred Network Controller

MoCA Privacy

Network Password ••••••••••••••••••

Network Controller MAC

MoCA Associated Device

Node ID	MAC Address	Packet Rx/Err	Rate Tx/Rx	Broadcast Tx/Rx	Status

Figure 6.11

6.5.2 SNMP Provisioning for MoCA

SNMP provisioning is available to configure the MoCA interface of the Wireless Gateway, as well as to allow retrieval of related statistics. Most of the SNMP MIBs for the MoCA interface are defined within the MoCA module associated with the MOC MIB file included as part of the software release package for all MoCA enabled devices. Support has also been added for key MIB objects from the standard MoCA11 MIB file. This file can be provided upon request. The following are some configuration and statistics MIB objects available for use. All MIBs listed are read-write unless otherwise noted (ensure the appropriate instance is added to the end of each below MIB that references a table entry as noted before setting or reading). For additional MIB objects, refer to the above mentioned MIB definition file included with your software release package.

tchMocaDevEnable takes an integer value as an input, where“1” means the interface is enabled (default) and “0” means disabled.

tchMocaDevEncryptionEnable takes and integer value as an input, where “1” means MoCA Link Security is enabled (default) and “0” means disabled.

tchMocaDevEncryptionPassword takes an octet string as a value and defines the MoCA link security password which must be the password for each attached node.

tchMocaDevChannelScanning takes an integer value as an input where “1” means the MoCA interface will automatically scan and select the best available channel (default) and “0” means channel scanning is disabled requiring the MIB to be set.

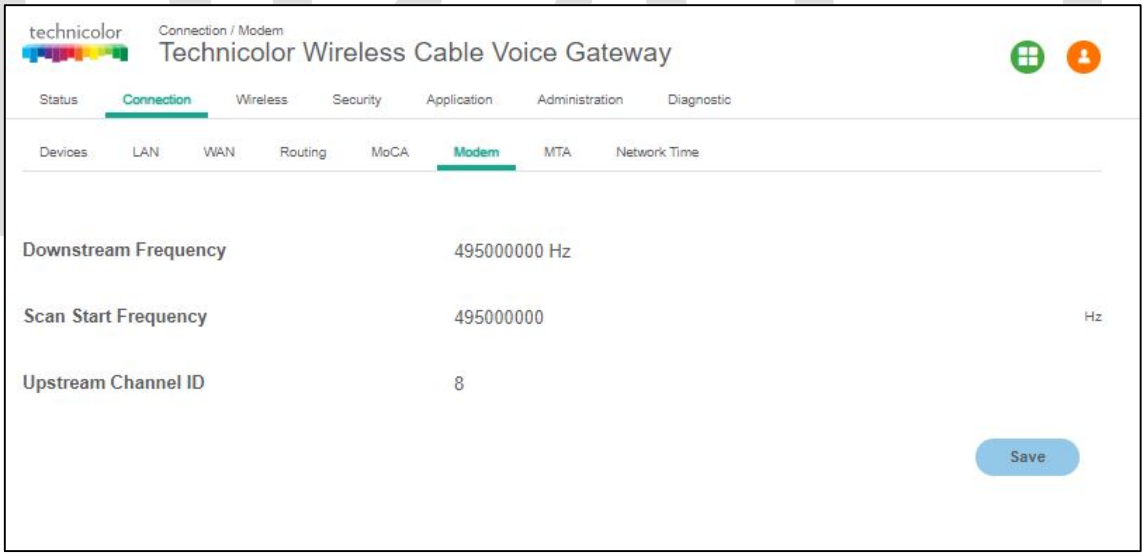
tchMocaDevChannelMask takes a channel list of bits as input that defines the channel or channels the device should scan and is only applicable if tchMocaDevChannelScanning is disabled.

6.6 Modem

Connection Tab / Modem

Click on the Connection tab then click on the Modem tab. The gateway will display the various modem parameters:

- The **Downstream Frequency** is the frequency at which the modem is locked with the CMTS during channel scan
- **Scan Start Frequency** is the frequency at which the modem tries to lock first (This frequency was saved as favorite channel, where the modem was able to connect last time).
- **Upstream Channel ID** is shows locked Upstream Channel Id for Cable Modem.



Downstream Frequency 495000000 Hz

Scan Start Frequency 495000000 Hz

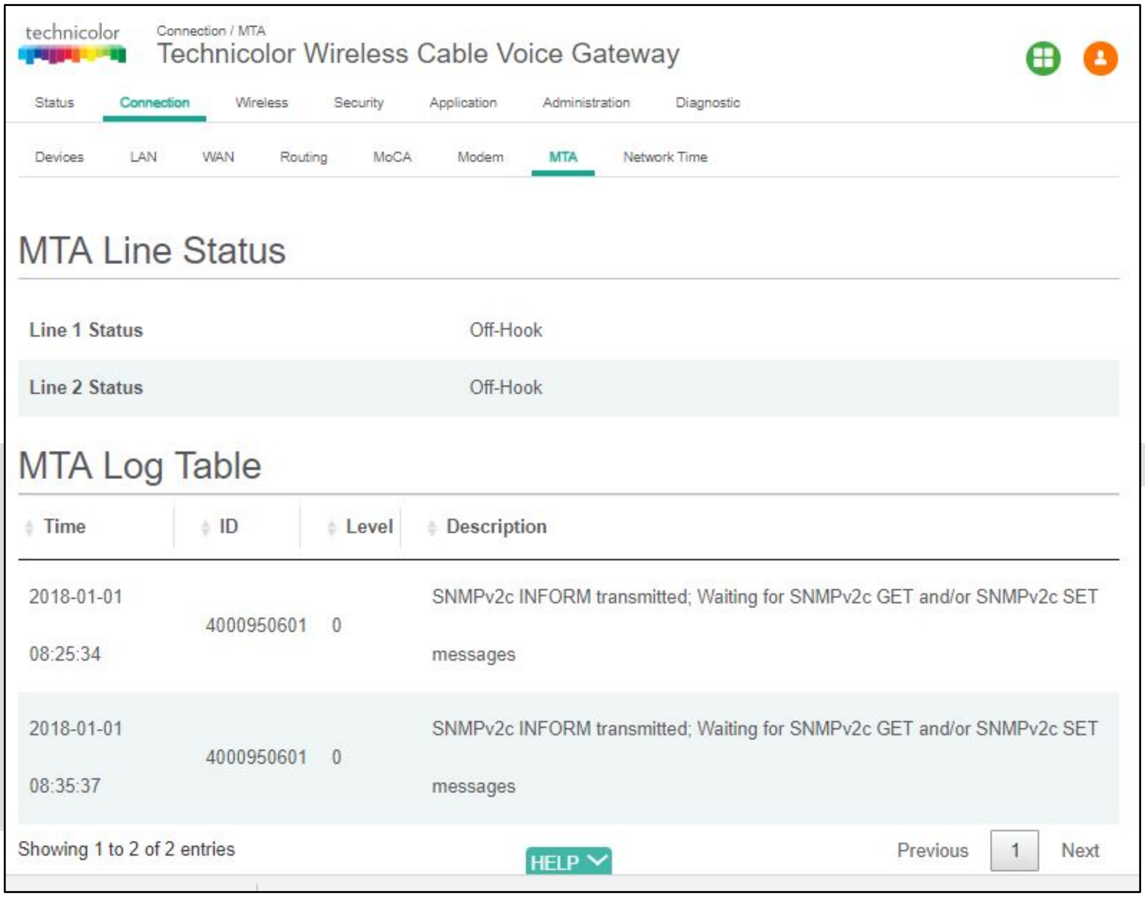
Upstream Channel ID 8

Figure 6.12

6.7 MTA

Connection Tab / MTA

Click on the Connection tab then click on the MTA. The MTA page will display the MTA line status and events logged on MTA line status as displayed below.



MTA Line Status

Line 1 Status	Off-Hook
Line 2 Status	Off-Hook

MTA Log Table

Time	ID	Level	Description
2018-01-01 08:25:34	4000950601	0	SNMPv2c INFORM transmitted; Waiting for SNMPv2c GET and/or SNMPv2c SET messages
2018-01-01 08:35:37	4000950601	0	SNMPv2c INFORM transmitted; Waiting for SNMPv2c GET and/or SNMPv2c SET messages

Showing 1 to 2 of 2 entries

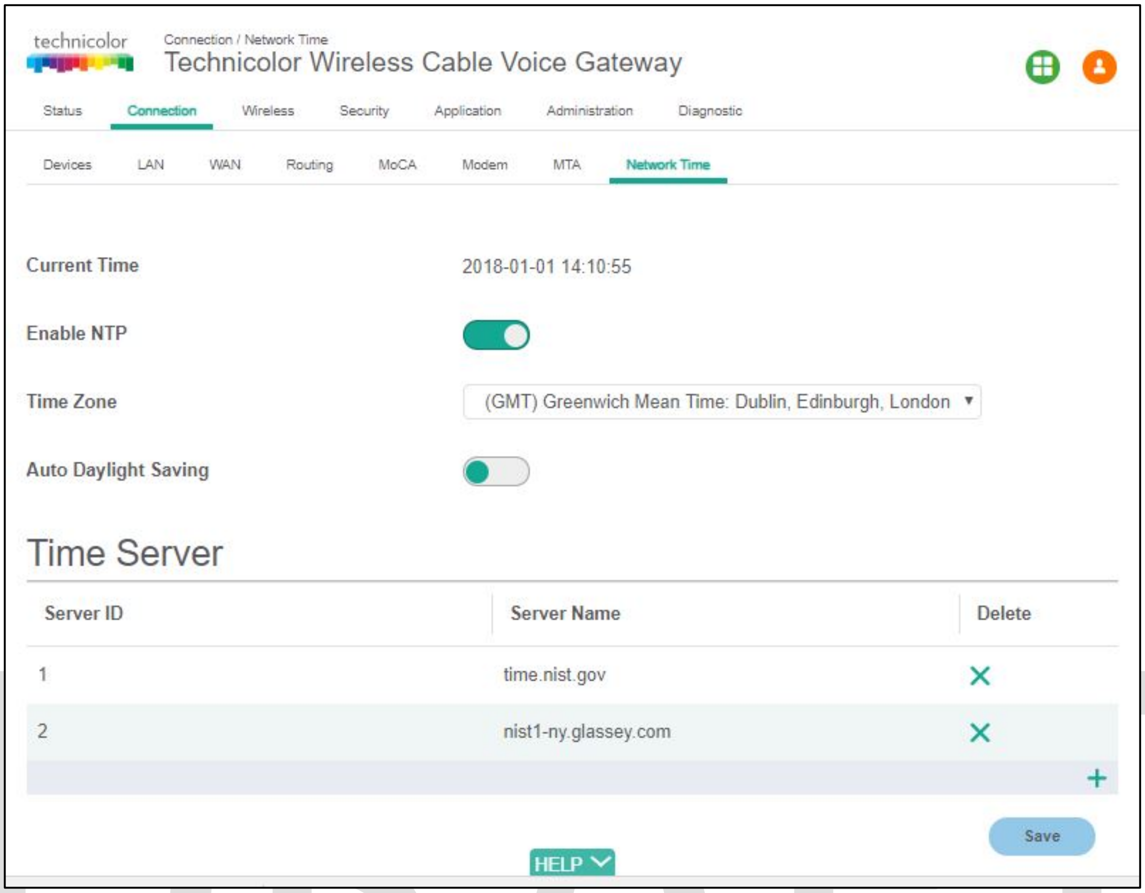
Previous 1 Next

Figure 6.13

6.8 Network Time

Connection Tab / Network Time

Click on the Connection tab then click on the Network Time tab. The network time page will display the various parameters related to current time, NTP server, etc. Options to configure Auto Daylight Saving and Time Zone are provided in this view.



Technicolor Wireless Cable Voice Gateway

Current Time: 2018-01-01 14:10:55

Enable NTP: ●

Time Zone: (GMT) Greenwich Mean Time: Dublin, Edinburgh, London ▾

Auto Daylight Saving: ○

Time Server

Server ID	Server Name	Delete
1	time.nist.gov	✕
2	nist1-ny.glassey.com	✕
		+

Figure 6.14

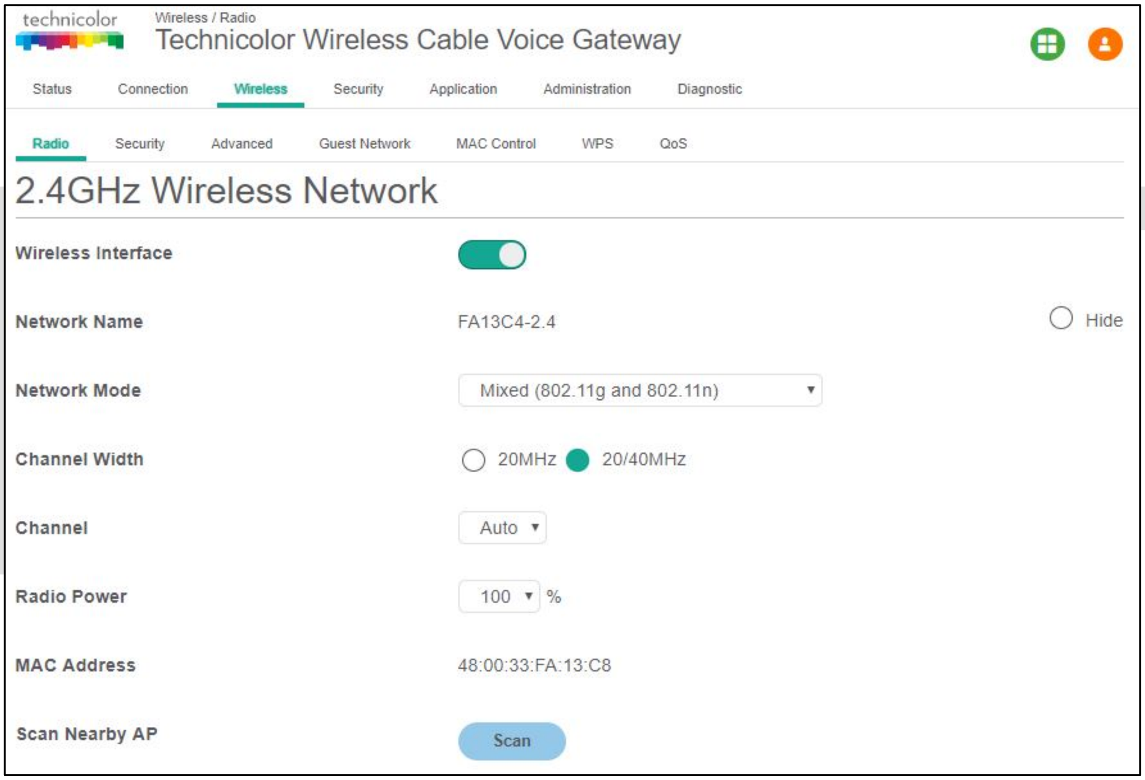
The user can change the configurations and press the Save button in the page to change these parameters.

7 Wireless

The CGM4231 Wireless Gateway also serves as an 802.11 wireless access point (AP). This section contains the essential wireless configuration items required to configure the wireless network.

7.1 Radio

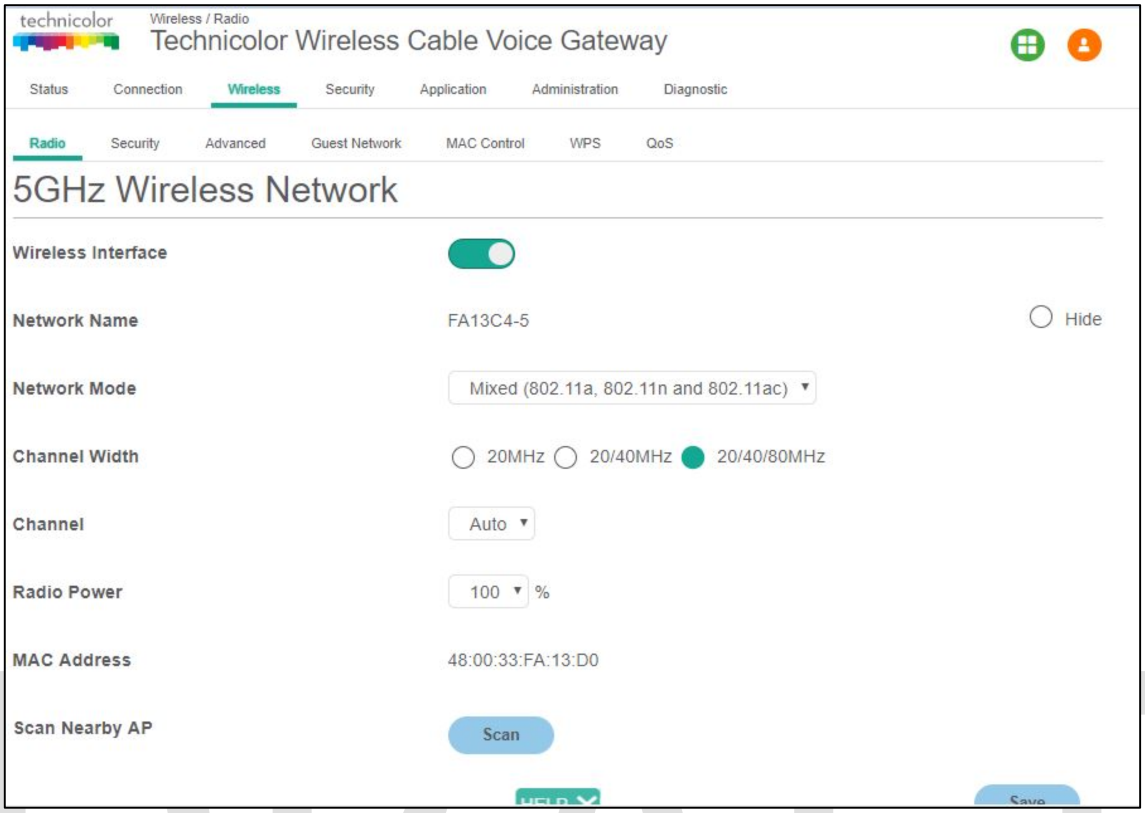
Wireless Tab / Radio
Click on the Wireless tab then click on the Radio tab. The page displays Radio setup information at 2.4 GHz and 5 GHz. Here user can set and display Wireless Network (2.4 GHz and 5 GHz) information as for Wireless Interface, Network Name, Network Mode, Channel Width, Channel, MAC Address, Scan Nearby AP.



2.4GHz Wireless Network

Wireless Interface	On
Network Name	FA13C4-2.4 ○ Hide
Network Mode	Mixed (802.11g and 802.11n)
Channel Width	○ 20MHz ● 20/40MHz
Channel	Auto
Radio Power	100 %
MAC Address	48:00:33:FA:13:C8
Scan Nearby AP	Scan

Figure 7.1



Wireless Interface	●
Network Name	FA13C4-5 ○ Hide
Network Mode	Mixed (802.11a, 802.11n and 802.11ac) ▾
Channel Width	○ 20MHz ○ 20/40MHz ● 20/40/80MHz
Channel	Auto ▾
Radio Power	100 ▾ %
MAC Address	48:00:33:FA:13:D0
Scan Nearby AP	Scan

Figure 7.2

7.1.1 User Provisioning for Radio

Wireless Interface:
You can enable or disable the wireless interface with the option “Wireless Interface” in this page.

Network Name:
Network name can either be set or displayed under this option, User can also hide network name by selecting the hide option.

Network Mode:
Network Mode determines which 802.11 wireless protocols will be supported by the wireless card.
Network mode has different option available according to Wireless interface:

1. For 2.4 GHz: 802.11b only, 802.11g only, 802.11n only, Mixed (802.11b and 802.11g), Mixed (802.11g and 802.11n), Mixed (802.11b, 802.11g and 802.11n).
2. For 5 GHz: 802.11a only, 802.11n only, 802.11ac only, Mixed (802.11a and 802.11n) and Mixed (802.11a, 802.11n and 802.11ac).

Channel Width:
User can select Channel width manually from any of these three options:

1. 20 MHz
2. 20/40 MHz
3. 20/40/80 MHz

Note:

1. Option 2. 20/40 MHz is possible in 2.4 GHz or 5 GHz wireless interface but only when Network mode include 802.11n or 802.11ac, is not possible with selection of only 802.11 b/ 802.11g /802.11a mode.
2. Option 3. 20/40/80 MHz is only possible with 5 GHz and network mode includes 802.11 ac.

Channel:
User can select any channel from the available drop down list or can select the gateway to operate in AUTO mode where the gateway will automatically select the best channel for the location in which it is installed. AUTO mode is the recommended setting so in order that the gateway may continuously scan and select the channel with lesser interference and congenstion from neighboring wireless networks.

Radio Power:
User can select Radio power from Radio Power drop down list.

MAC Address:
Mac address is reflected by this tab.

Scan Nearby AP:
The Scan button provides a mechanism for the AP to scan neighbouring APs and provides various statistics on neighbours.

7.1.2 SNMP Provisioning for Radio

tchRgdot11nExtMode selects the network mode.

tchRgdot11nExtBandWidth selects the channel width for 802.11n operation.

tchRgdot11nExtSideBand - This is for N cards only.

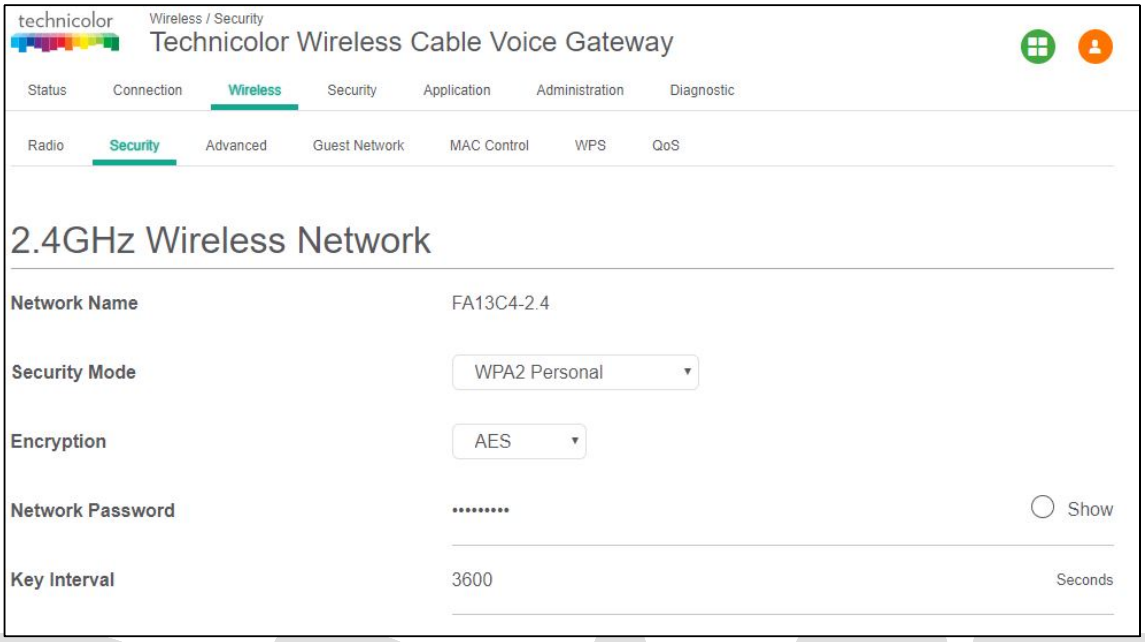
tchRgDot11ExtCurrenannelselects the channel. The list of the available channels depends on the radio capabilities and country code.

tchRgDot11BssSsid sets the network name (SSID), Controls and reflects the service set identifier.

tchRgDot11BssClosedNetwork controls whether the network name (SSID) will be hidden in the beacon frames or not

7.2 Security

Wireless Tab / Security
Click on the Wireless tab then click on Security tab. The page displays radio setup information at 2.4 GHz and 5 GHz. Here the user can set and display Wireless Network (2.4 GHz and 5 GHz) information including the Network Name, Security Mode, Encryption, Network Password, and Key Interval.



Technicolor Wireless Cable Voice Gateway

2.4GHz Wireless Network

Network Name FA13C4-2.4

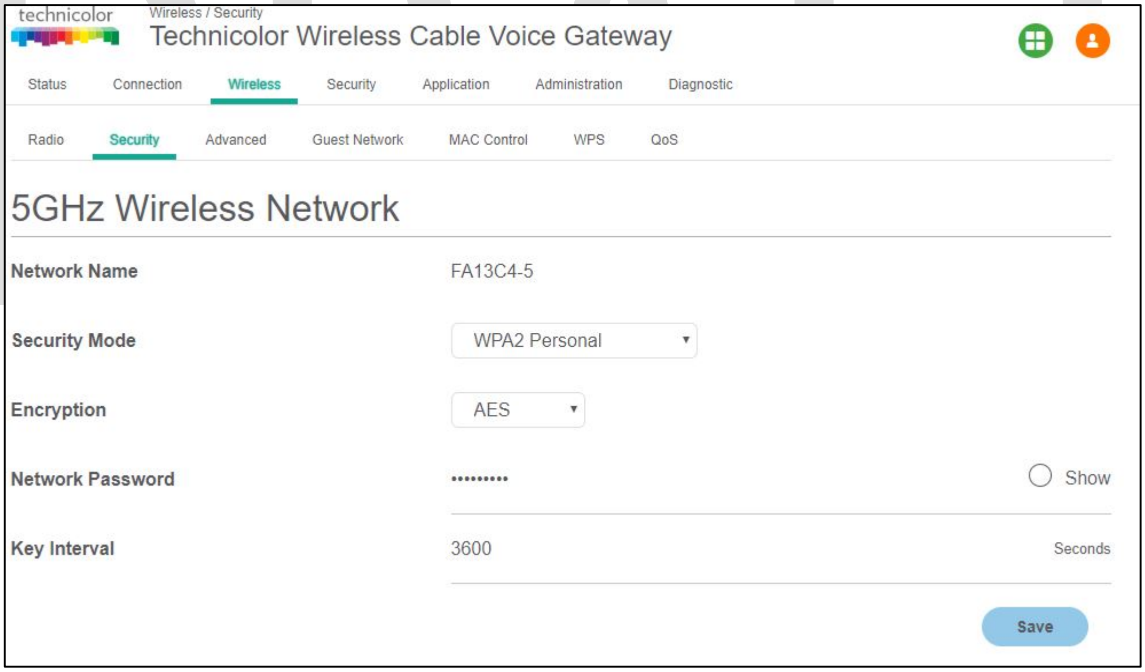
Security Mode WPA2 Personal

Encryption AES

Network Password •••••••••

Key Interval 3600 Seconds

Figure 7.3



Technicolor Wireless Cable Voice Gateway

5GHz Wireless Network

Network Name FA13C4-5

Security Mode WPA2 Personal

Encryption AES

Network Password •••••••••

Key Interval 3600 Seconds

Figure 7.4

7.2.1 User Provisioning for Wireless Security

Network Name:
Network name will only be displayed here. The User cannot make any changes under this tab.

Security Mode:
The User can select security mode from available drop down menu for 2.4 GHz: Open, WEP 64, WEP 128, WPA2 Personal, WPA or WPA2 Personal for 5.0 GHz: Open, WPA2 personal, WPA or WPA2 Personal.

Recommended setting is WPA2 personal.

Encryption:
Encryption mode changes according to selection of security mode. So the user doesn't have to worry about correct encryption type for their security mode. For example, if security mode WPA2 Personal is selected, only AES encryption may be configured. Similarly if it is WPA or WPA2 personal, AES or TKIP encryption mode may be configured.

Network Password:
User can select whatever password they like of their choice but only when it meets the requirement of encryption type.

1. Open: No password needed
2. WEP 64: need at least 5 ASCII characters or 10 Hex digits.
3. WEP 128: need at least 13 ASCII characters or 26 Hex digits
4. WPA2 Personal: at least 8 characters.
5. WPA or WPA2 Personal: at least 8 characters.

Key Interval:
User can make a choice what network key rotational value they want, in general it comes with 3600 sec, but user can choose between range 1- 999999.

Note: Don't forget to hit Save tab at bottom of page after making any changes.

7.2.2 SNMP Provisioning for Wireless Security

tchRgDot11BssSecurityMode sets the security mode for the selected SSID.

tchRgDot11WepEncryptionMode sets the key length for WEP.

tchRgDot11WepPassPhrase sets the passphrase for WEP.

tchRgDot11Wep64BitKeyValue sets each 40/64-bit WEP key.

tchRgDot11Wep128BitKeyValue sets each 104/128-bit WEP key.

tchRgDot11WepDefaultKey sets the default WEP key.

tchRgDot11WpaAlgorithm sets the encryption for WPA.

tchRgDot11WpaPreSharedKey sets the passphrase or PSK for WPA.

tchRgDot11WpaGroupRekeyInterval sets the rekeying interval for WPA.

tchRgDot11RadiusAddress sets the IP address of the RADIUS server.

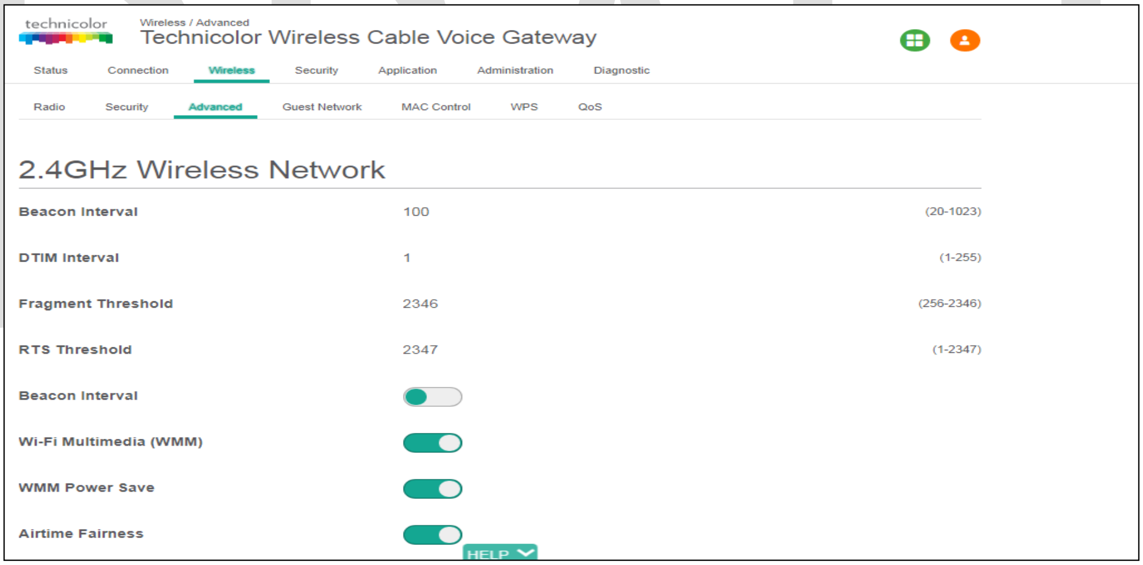
tchRgDot11RadiusPort sets the UDP port of the RADIUS server.

tchRgDot11RadiusKey sets the RADIUS key.

tchRgDot11RadiusReAuthInterval sets the rekeying interval for RADIUS

7.3 Advanced

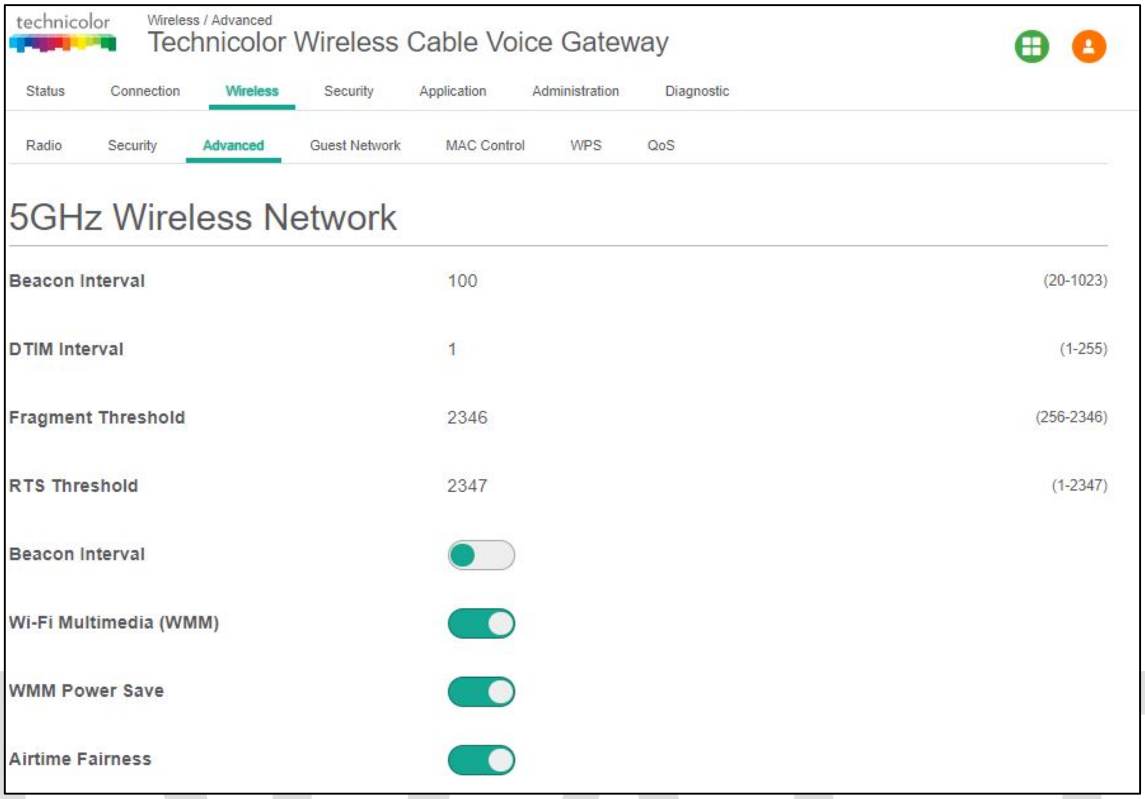
Wireless Tab / Advanced
Click on the Wireless tab then click on the Advanced tab. The page displays advanced wireless setup information of the 2.4 GHz and 5 GHz wireless networks including Beacon Interval, Fragment Threshold, RTS Threshold, Wi-Fi Multimedia (WMM), WMM Power Save Airtime Fairness and Band Steering Settings: - Band Steering Status, Band Steering RSSIThreshold 2.4G, and Band Steering RSSIThreshold 5G.



2.4GHz Wireless Network

Beacon Interval	100	(20-1023)
DTIM Interval	1	(1-255)
Fragment Threshold	2346	(256-2346)
RTS Threshold	2347	(1-2347)
Beacon Interval	○	
Wi-Fi Multimedia (WMM)	●	
WMM Power Save	●	
Airtime Fairness	●	

Figure 7.5



Technicolor Wireless Cable Voice Gateway

5GHz Wireless Network

Beacon Interval	100	(20-1023)
DTIM Interval	1	(1-255)
Fragment Threshold	2346	(256-2346)
RTS Threshold	2347	(1-2347)
Beacon Interval	○	
Wi-Fi Multimedia (WMM)	●	
WMM Power Save	●	
Airtime Fairness	●	

Figure 7.6

7.3.1 User provisioning for Advanced Wireless

This screen is used to set up the advanced wireless functions. These settings should only be adjusted by an expert administrator as incorrect setting can reduce wireless performance.

Beacon Interval:
The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast, by the device to synchronize the wireless network. The default value is 100; user can select any other value between 23 to1023.

DTIM Interval:
This value indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field, informing client of the next window for listening to broadcast and multicast messages. When the device has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients use the DTIM value to wake up and hear the beacons to receive the broadcast and multicast messages. The default value is 1; user can select any other value from 1 to 255.

Fragmentation Threshold:
This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most

cases, it should remain at its default value of 2346, user can select other value in range between 256 -2346.

RTS Threshold:
Should you encounter inconsistent data flow, only minor reduction of the default value, 2347, is recommended. If a network packet is smaller than the pre-set RTS Threshold size, the RTS/CTS mechanism will not be enabled. The device sends Request to Send (RTS) frames to a specific receiving station and negotiates the transmission of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of 2347; user can select other value in range between 1 and 2347.

Beacon Interval:
The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast, by the device to synchronize the wireless network. User has choice to enable or disable it, by corresponding toggle button. Recommended to leave it enabled.

Wi-Fi Multimedia (WMM):
This feature maintains priority between different traffic types such as audio, video, voice and background traffic. This is done using QOS WMM feature which in turn increases throughput. User has option available to disable it through toggle button but again will impact throughput rates.

WMM Power Save:
This feature helps devices to conserve battery life. Recommended to leave it enabled, but again if needed user has option disable it.

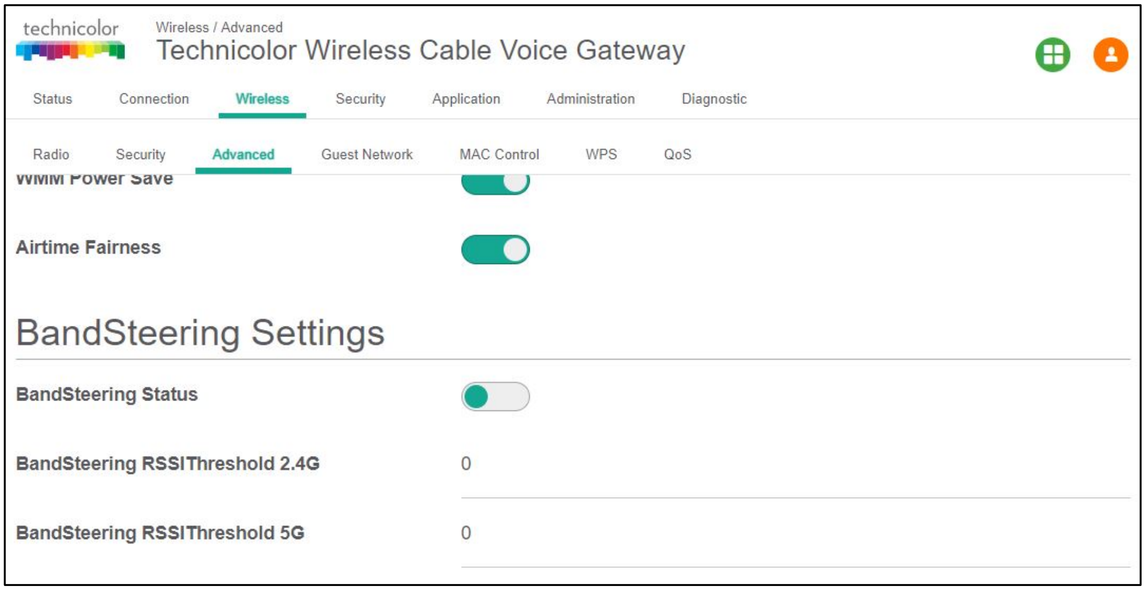
Airtime Fairness:
This feature comes handy in mixed environment of slow and fast devices, giving each client equal access to air time, this again leads to faster download speeds and high throughputs but user has option to disable it.

7.3.1.1 Band Steering Settings

Band Steering detects clients capable of 5 GHz operation and steers them to that frequency which leaves the more crowded 2.4 GHz band available for legacy clients. This helps improve end user experience by reducing channel utilization, especially in high density environments. Band steering can ensure that they achieve their maximum performance without being bottlenecked by legacy 802.11b/g clients.

Band Steering is based upon the clients RSSI threshold value. A minimum threshold value is configured in the WebUI. When the threshold is reached, the clients are automatically steered.

The following screen provides the setup for Band Steering feature. The user can set the required threshold values in this view.



WMM Power Save

Airtime Fairness

BandSteering Settings

BandSteering Status

BandSteering RSSIThreshold 2.4G 0

BandSteering RSSIThreshold 5G 0

Figure 7.7

7.3.2 SNMP Provisioning for Advanced Wireless

tchRgdot11nExtPhyRate sets the transmission rate.

tchRgdot11ExtCtsProtectionEnablesets the CTS protection mode.

tchRgDot11ExtBeaconIntervalsets the beacon interval.

tchRgDot11ExtDTIMIntervalsets the DTIM interval.

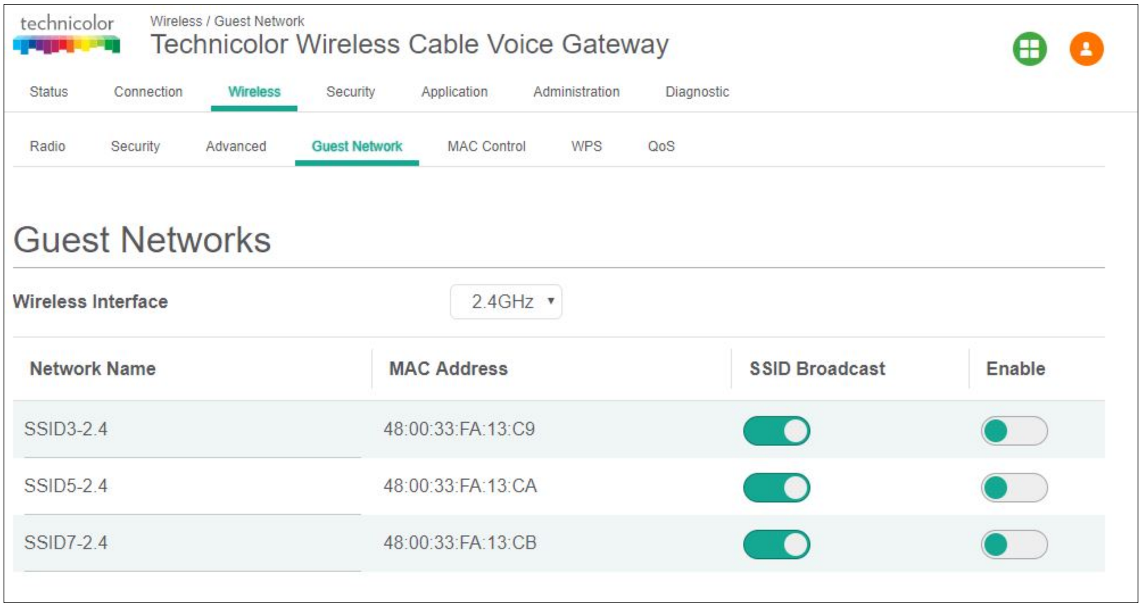
tchRgDot11ExtFragThreshsets the fragmentation threshold.

7.4 Guest Network

Wireless Tab / Guest Network

Click on the Wireless tab then click on the Guest Network tab. The page displays Guest Network and Guest LAN Settings. Here, user can enable, set and display Guest Network (2.4 GHz and 5 GHz) parameters such as the Network Name, MAC Address, and SSID Broadcast.

Under Guest LAN settings setup, the user can set and display Guest LAN parameters such as the Network Name, Security Mode, DHCP Server, IP Address, Subnet Mask, DHCP Beginning Address, DHCP Ending Address, and DHCP Lease Times for 2.4 and 5 GHz networks.

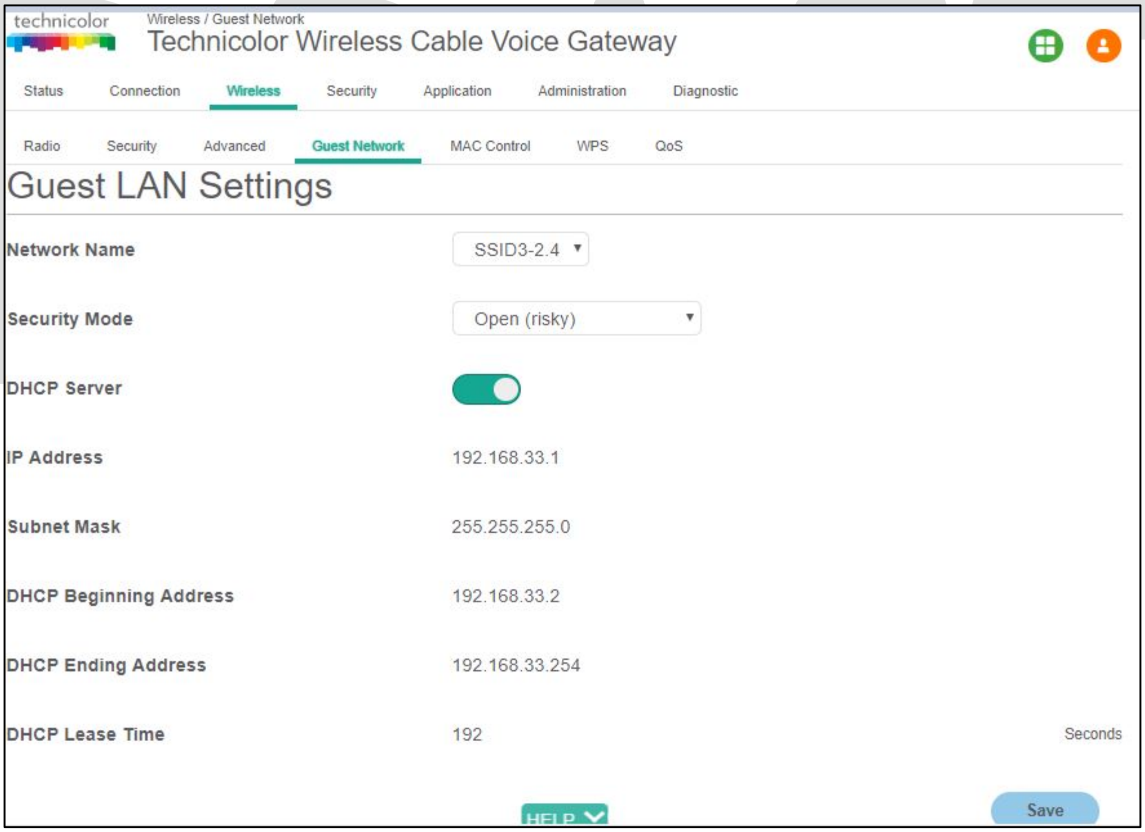


Guest Networks

Wireless Interface: 2.4GHz

Network Name	MAC Address	SSID Broadcast	Enable
SSID3-2.4	48:00:33:FA:13:C9	☑	☐
SSID5-2.4	48:00:33:FA:13:CA	☑	☐
SSID7-2.4	48:00:33:FA:13:CB	☑	☐

Figure 7.8



Guest LAN Settings

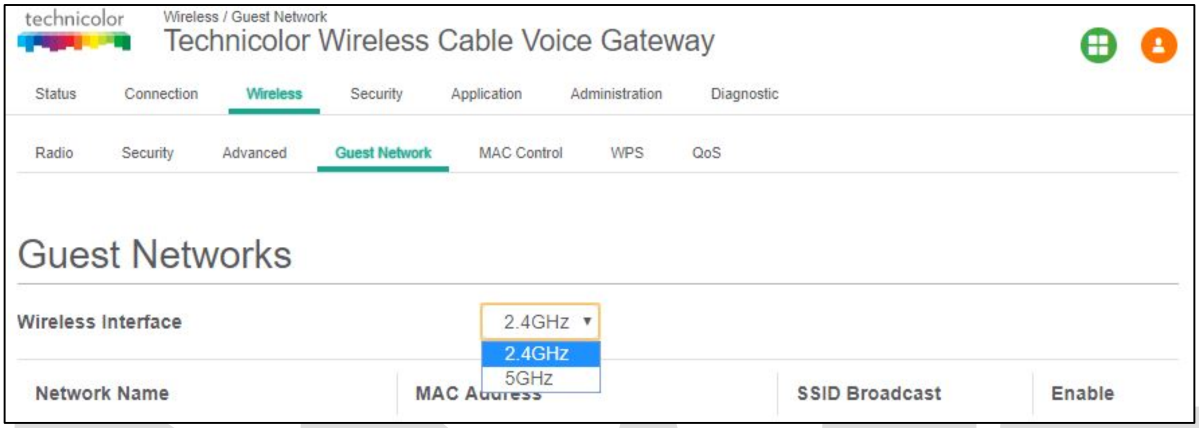
Network Name	SSID3-2.4
Security Mode	Open (risky)
DHCP Server	☑
IP Address	192.168.33.1
Subnet Mask	255.255.255.0
DHCP Beginning Address	192.168.33.2
DHCP Ending Address	192.168.33.254
DHCP Lease Time	192 Seconds

Figure 7.9

7.4.1 User Provisioning for Guest Network

7.4.1.1 Guest Network:

Wireless Interface:
This tab gives user option to make select wireless interface 2.4 GHz or 5 GHz guest networks.



Wireless Interface: 2.4GHz

Figure 7.10

Network Name:
Don’t get confused from previous (on Radio tab) network name, Network name here is for Guest Network. User can change default “SSID3- 2.4” from XXXXX under Network Name column.

MAC Address:
User can’t change MAC address it is available only for display information.

SSID Broadcast:
User can enable or disable this feature by toggle button provided under SSID Broadcast; this is similar to Network name hide feature Radio tab.

Enable:
User can again enable or disable the any required Guest SSID by this toggle button.

7.4.1.2 Guest LAN Settings:

Network Name:
Here user can get drop down menu on basis of selection in above wireless interface tab. If 2.4 GHz is selected in Wireless interface tab then it will show all 2.4 GHz Guest SSID. User can select and set / changes accordingly. Similarly for 5 GHz.

Security Mode:
Please refer 7.2.1 Security tab, settings are same.

DHCP Server:

When enabled, the gateway automatically assigns IP addresses. If disabled, parameters can be configured manually.

Note: Don't forget to hit Save button after all changes are made.

7.4.2 SNMP Provisioning for Guest Network

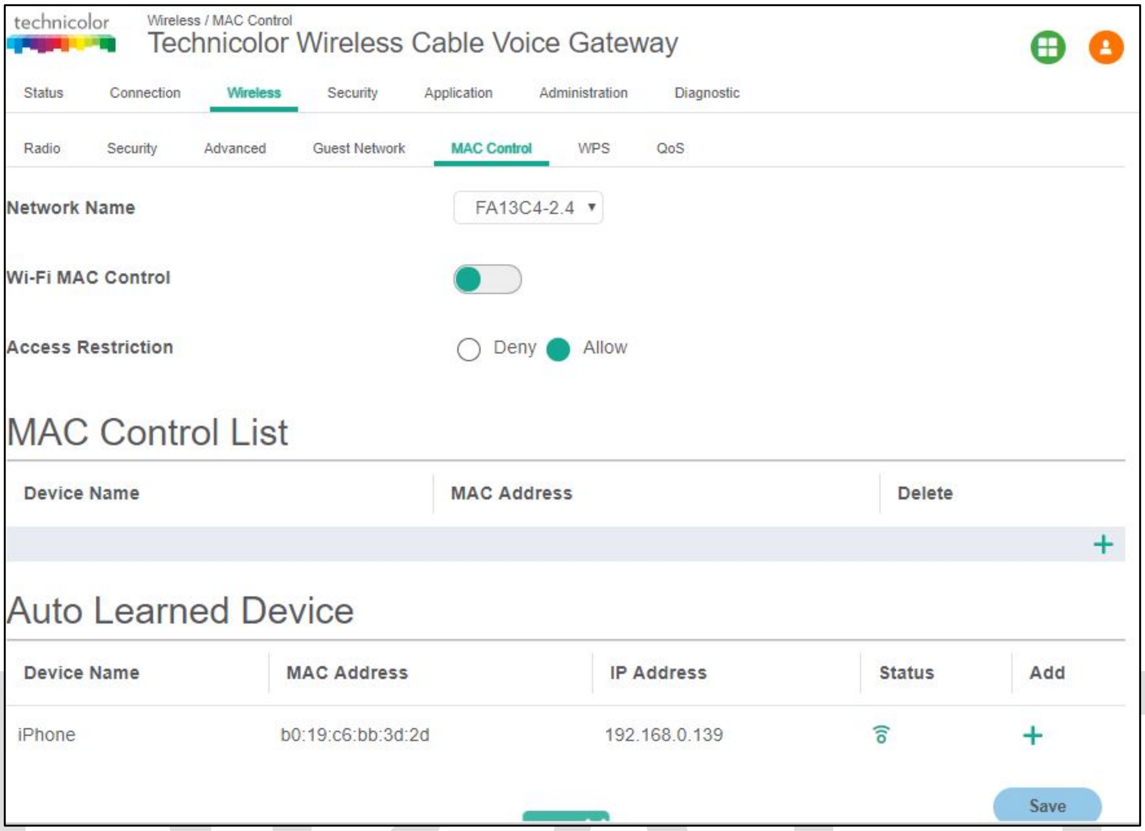
The following MIBs provide the control over the web pages:
tchRgDot11MbssUserControl
tchRgDot11MbssAdminControl

The following MIBs provide configuration settings for the SSID and DHCP lease parameters:
tchRgDot11Bss,
tchRgDot11Privacy
tchRgIpMgmtLanTable
tchRgIpMgmtLanDhcpServerTable

7.5 MAC Control

Wireless access can be filtered by using the MAC addresses of the clients that are connected to Wi-Fi.

Wireless Tab / MAC Control
Click on the Wireless tab then click on MAC Control tab. The page displays MAC Control setup information. Here the user can set and display Network Name, Wi-Fi MAC Control, Access Restriction, MAC Control List (Device Name, MAC Address, Delete), Auto Learned Device (Device Name, MAC Address, IP Address, Status, Add).



Network Name: FA13C4-2.4 ▾

Wi-Fi MAC Control: ●

Access Restriction: ○ Deny ● Allow

MAC Control List

Device Name	MAC Address	Delete
		+

Auto Learned Device

Device Name	MAC Address	IP Address	Status	Add
iPhone	b0:19:c6:bb:3d:2d	192.168.0.139	ᯤ	+

Figure 7.11

7.5.1 User Provisioning for MAC Control

7.5.1.1 Network Name

Network name can be selected from the Drop down menu.

7.5.1.2 Wi-Fi MAC Control

Wi-Fi MAC Control can be enabled by the selection that option.

7.5.1.3 Access Restrictions

Select the Deny or Allow button to block or permit the MAC addresses listed to access the wireless network.

7.5.1.4 MAC Control List

The gateway can manage the network access of select client devices if they are entered in this list using that device's MAC address.

Click the Add button to add to the list. Add the required details in the entries and click Save to add them into the control list.

7.5.1.5 Auto Learned Device

Auto learned devices are the Wi-Fi clients that are discovered by the gateway. The user can add them to the MAC control list by selecting the add option in the screen.

7.5.2 SNMP Provisioning for MAC Control

tchRgDot11BssAccessMode enables/disables MAC Control and specifies the access restriction mode. Note that in a dual-band concurrent model, the primary SSIDs of both first and second radios share the object with the instance 32.

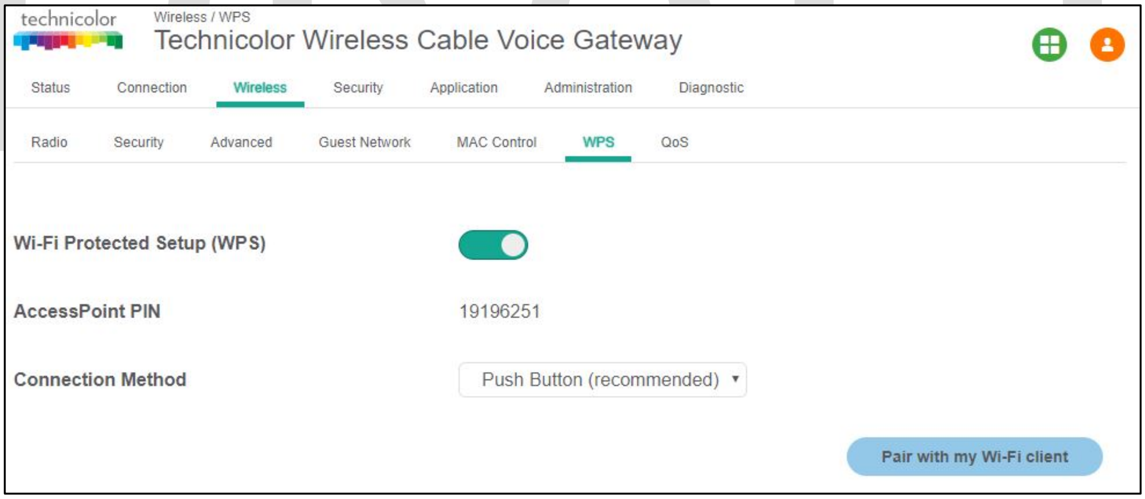
tchRgDot11ClientStation shows the MAC address of each connected wireless client.

7.6 WPS

Wi-Fi Protected Setup (previously called Wi-Fi Simple Config) is an optional certification program developed by the Wi-Fi Alliance designed to ease set up of security-enabled Wi-Fi networks at home and small office environment. Wi-Fi Protected Setup supports methods (pushing a button or entering a PIN into a wizard-type application)

The objective of this protocol is to make Gateways and Client's device connectivity easy for user.

Wireless Tab / WPS
Click on the Wireless tab, and then click on the WPS control tab. The page displays WPS setup information. Here user can set and display WPS parameters including the Access Point PIN and Connection Method (Push Button/ PIN Number).



Wireless / WPS

Technicolor Wireless Cable Voice Gateway

Wi-Fi Protected Setup (WPS) ●

AccessPoint PIN 19196251

Connection Method Push Button (recommended) ▾

Figure 7.12

7.6.1 User Provisioning for WPS

Wi-Fi Protected Setup (WPS):
User can change the WPS feature status in this option.

Access Point PIN
This is random number generated by gateway and this PIN is used for verification at the client devices.

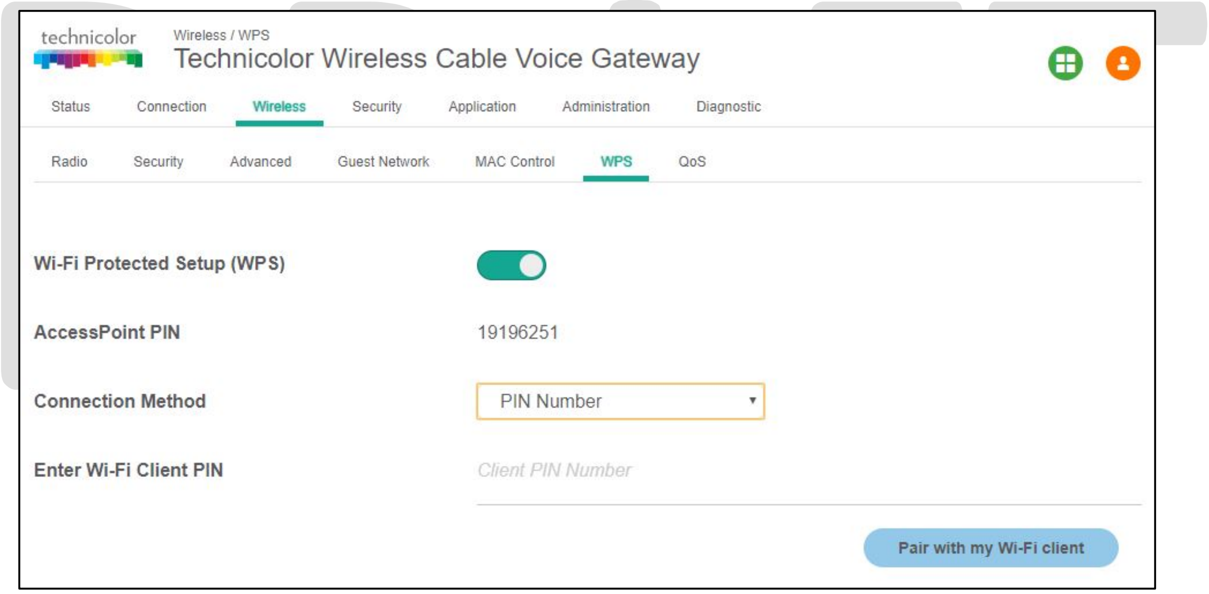
Connection Method:
Connection method has 2 options - Push Button or PIN Number.

Push Button:
User can either push the Hardware button available on front panel of gateway. Look for sign
Software tab available on Wireless Gateway WebUI saying “Pair with my client”.

To start WPS operation user needs to press HW/SW PBC button/ on Gateway and within 60 sec on Client’s device, User can observe WPS LED starts flashing as soon as HW/SW PBC button is pressed. This is indication that WPS process is initiated.

Personal Identification Number (PIN) method:

When user decides to go through connection method via PIN number, the user is prompted to enter the Wi Fi Client PIN.



Wi-Fi Protected Setup (WPS)

AccessPoint PIN 19196251

Connection Method PIN Number

Enter Wi-Fi Client PIN Client PIN Number

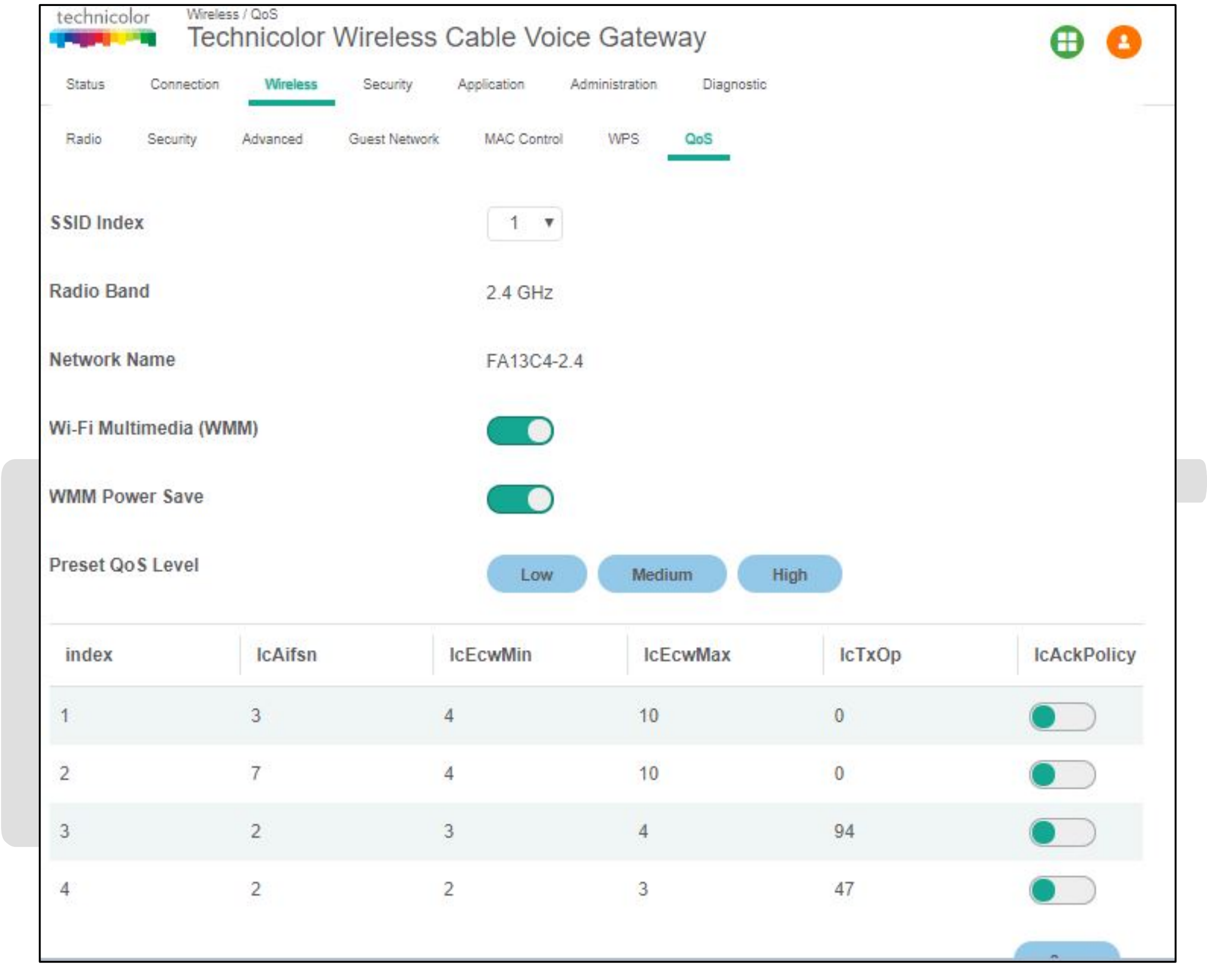
Figure 7.13

7.7 QOS

By default, networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped. Implementing QoS in wireless LAN makes network performance more predictable and bandwidth utilization more effective.

Note: When QoS is enabled, the device uses Wi-Fi Multimedia (WMM) mode by default.

Wireless Tab / QoS
Click on the Wireless tab then click on the QOS tab. The page displays QoS setup information. Here, the user can set and display SSID Index, Radio Band, Network Name, Wi-Fi Multimedia (WMM), WMM Power Save, Preset QoS Level (Low, Medium and High),Index, IcAifsn, IcEcwMin, IcEcwMax, IcTxOp , IcAckPolicy.



SSID Index: 1 ▼

Radio Band: 2.4 GHz

Network Name: FA13C4-2.4

Wi-Fi Multimedia (WMM): ●

WMM Power Save: ●

Preset QoS Level

index	IcAifsn	IcEcwMin	IcEcwMax	IcTxOp	IcAckPolicy
1	3	4	10	0	○
2	7	4	10	0	○
3	2	3	4	94	○
4	2	2	3	47	○

Figure 7.14

7.7.1 User Provisioning for QOS

SSID Index:
User can select any number from the drop down list. Where 1 represents 2.4 GHz and 2 represents 5 GHz and other numbers will be assigned to Guest SSID.

Radio Band:
This tab only displays which Wireless band is selected, dependent on selection of SSID Index.

Network Name:
This again depends on SSID index selection and will reflect selected number associated Network name.

Wi- Fi Multimedia and WMM Power Save:
Please refer section 7.3.1

Note: Recommended not to change anything under this tab, any wrong changes will lead to degradation in gateway performance.

7.7.2 SNMP Provisioning for QOS

tchRgDot11ExtWmm enables or disables WMM.
tchRgDot11ExtWmmNoAck enables or disables the no acknowledgement feature for WMM.

8 Security

Security settings in the security page allow blocking or selectively allowing different types of data through the router from the WAN to the LAN. Additionally, the settings allow the device's firewall to be enabled or disabled.

- Java Applets, Cookies, ActiveX controls, Popup Windows, and Proxies can be blocked using this page. Firewall Protection turns on the Stateful Packet Inspection (SPI) firewall features.
- Block Fragmented IP packets prevents all fragmented IP packets from passing through the firewall.
- Port Scan Detection detects and blocks port scan activity originating on both the LAN and WAN.
- IP Flood Detection detects and blocks packet floods originating on both the LAN and WAN.

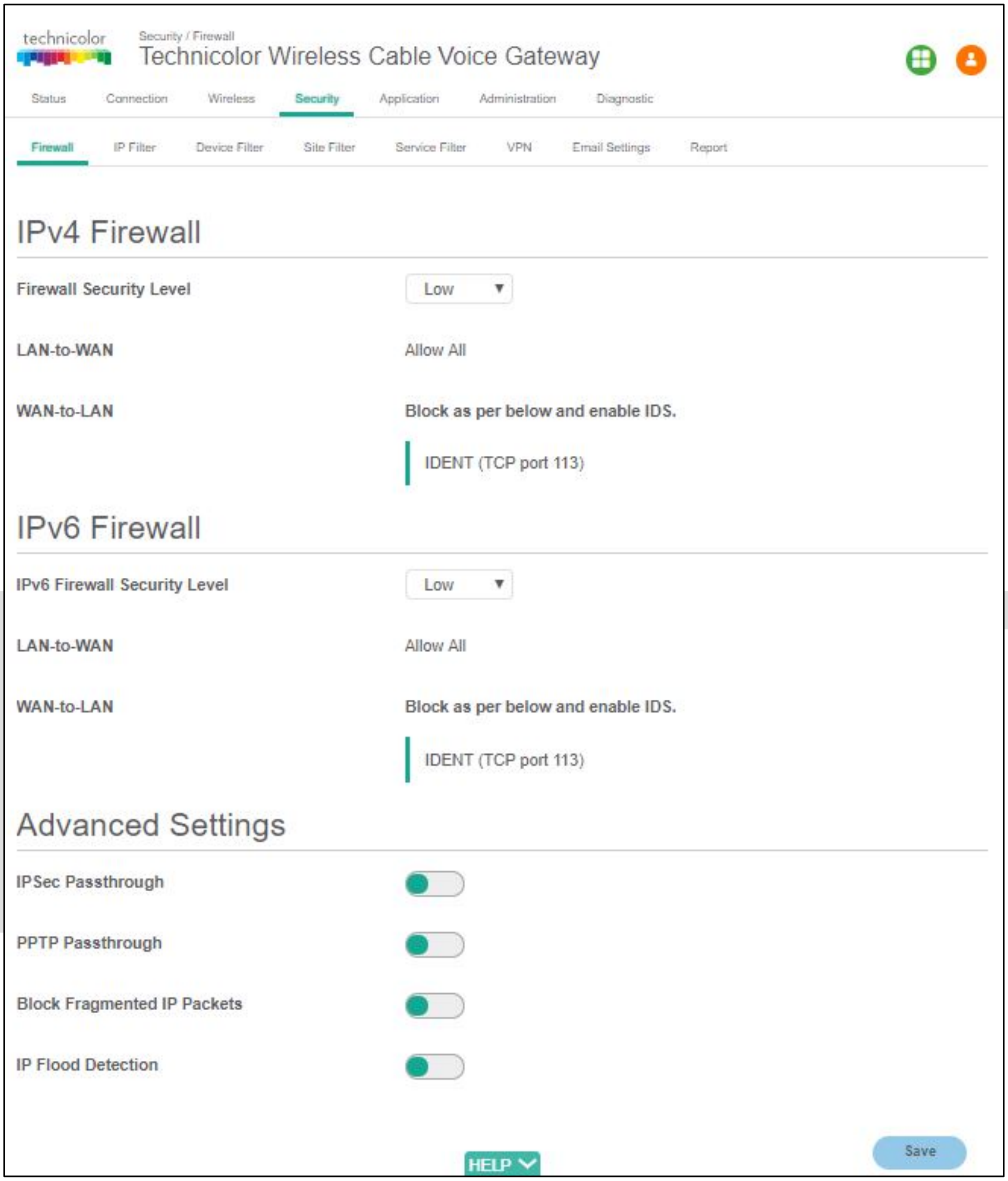
8.1 Firewall

8.1.1 User Provisioning for Firewall

Security Tab / Firewall
Click on the Security tab, and then click on Firewall tab. The page displays Firewall setup information. Here user can set and display:

IPv4 Firewall: Firewall Security Level, LAN – to – WAN, WAN – to - LAN
IPv6 Firewall: IPv6 Firewall Security Level, LAN – to – WAN, WAN – to - LAN
Advanced Settings:

- IPSec Passthrough (Allows or prevents an IPsec VPN client that is connected to the gateway to connect to a remote IPsec VPN connection)
- PPTP Passthrough (Allows or prevents a PPTP VPN client that is connected to the gateway to connect to a remote PPTP VPN connection.
- Block Fragmented IP Packets (Prevents or allows all fragmented IP Packets from passing through the firewall)
- IP Flood Detection (Protects against massive number of packets being sent to the router for overwhelming it, such as a Denial of Service attack)



IPv4 Firewall

Firewall Security Level: Low

LAN-to-WAN: Allow All

WAN-to-LAN: Block as per below and enable IDS.

IDENT (TCP port 113)

IPv6 Firewall

IPv6 Firewall Security Level: Low

LAN-to-WAN: Allow All

WAN-to-LAN: Block as per below and enable IDS.

IDENT (TCP port 113)

Advanced Settings

IPSec Passthrough

PPTP Passthrough

Block Fragmented IP Packets

IP Flood Detection

Figure 8.1

The following table explains the traffic restrictions while setting the firewall level to various levels – High, Medium, Low and Off.

Firewall level	Restrictions on inbound traffic	Restrictions on outbound traffic	Remarks
High	All unsolicited inbound traffic is blocked, and Intrusion Detection is enabled.	All traffic except the following are restricted: • HTTP and HTTPS (TCP	Both inbound and outbound traffic are restricted

		ports 80, 443) • DNS (TCP/UDP port 53) • NTP (UDP ports 119, 123) • Email (TCP ports 25, 110, 143, 465, 587, 993, 995) • VPN (GRE, UDP port 500, TCP port 1723) • iTunes (TCP port 3689)	
Medium	Inbound traffic is blocked for the following services: • IDENT protocol (TCP port 113) • ICMP request • Peer-to-Peer applications • Kazaa (TCP/UDP port 1214) • BitTorrent (TCP ports 6881-6999) • Gnutella (TCP/UDP port 6346) • Vuze (TCP ports 49152-65534) Intrusion Detection is enabled in the Medium operating level. All other inbound traffic is allowed by the firewall. Please note that unsolicited inbound traffic will not be forwarded to devices on your home network unless they match a port forwarding / triggering rule, or a DMZ host has been configured.	No restrictions - Outbound connections are allowed by the firewall regardless of the service or port(s) being used for the connection.	
Low	Inbound traffic is blocked for the following services: • IDENT protocol (TCP port 113) Intrusion Detection is enabled in the Low operating level. All other inbound traffic is allowed by the firewall. Please note that unsolicited inbound traffic will not be forwarded to devices on your home network unless they match a port forwarding / triggering rule, or a DMZ host has been configured.	No restrictions - outbound connections are allowed by the firewall regardless of the service or port(s) being used for the connection.	
Off	No restrictions	No restrictions	Firewall configuration is disabled.

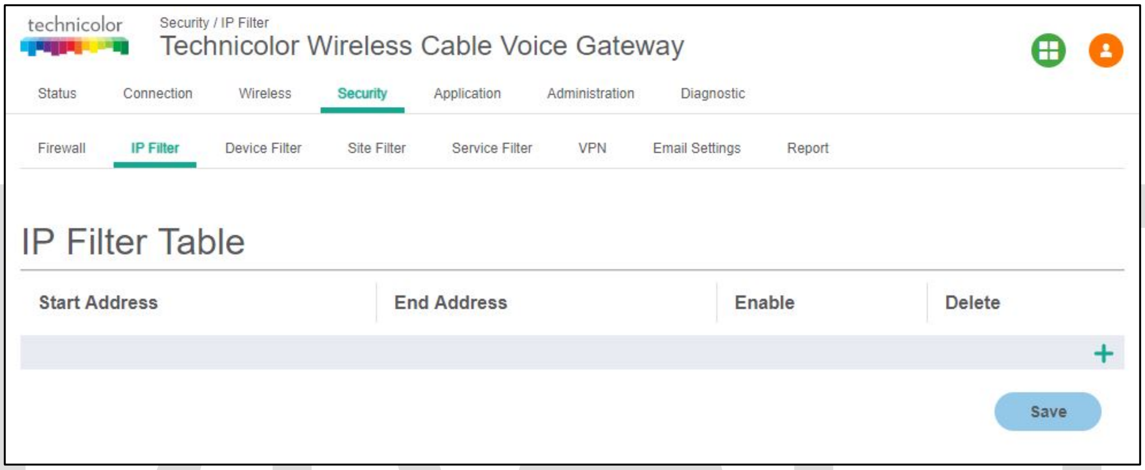
8.1.2 SNMP Provisioning for Firewall

tchRgFirewallProtection will allow low, medium and high options.

8.2 IP Filter

IP filters allow users to block certain IP addresses being assigned to the clients. Those IP addresses may be reserved for other purposes. To activate the IP address filter, provide the IP address range, click Enable and then click Save Settings.

Security Tab / IP Filter
This page displays IP Filter Table information. Here, user can set and display Start Address, End Address, Enable and Delete for IP Filter.



IP Filter Table

Start Address	End Address	Enable	Delete

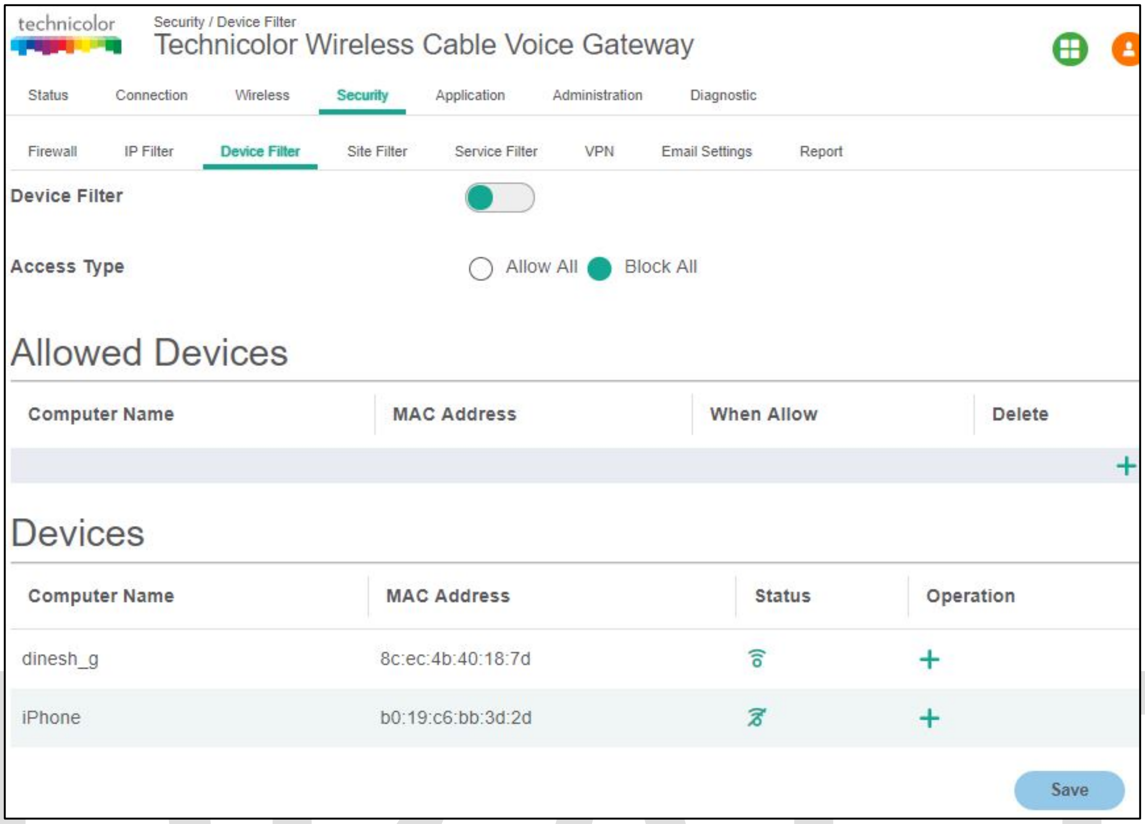
Figure 8.2

8.3 Device Filter

Device Filter page is used to allow or block devices connecting to the router, for both LAN and Wi Fi clients. The devices are allowed or blocked with respect to their MAC address, which is added in the allowed devices list in this page. User can add devices through auto learnt devices under devices list or add a device manually under the Allowed Devices list.

Security Tab / Device Filter
Click on the Security tab then click on Device Filter tab. The page displays following Device Filter setup information, which can be viewed and set by user. The following options are displayed:

- Device Filter - (Enabled / Disabled)
- Access Type - (Allow All / Block All)
- Blocked Devices - (Computer Name, MAC Address, Allow, Delete)
- Devices – List of Auto Learnt devices (Name, MAC Address, Status, Operation)



Technicolor Wireless Cable Voice Gateway

Device Filter ●

Access Type ○ Allow All ● Block All

Allowed Devices

Computer Name	MAC Address	When Allow	Delete
			+

Devices

Computer Name	MAC Address	Status	Operation
dinesh_g	8c:ec:4b:40:18:7d	ᯤ	+
iPhone	b0:19:c6:bb:3d:2d	ᯤ	+

Figure 8.3

Enable Device Filter

Device Filter can be enabled with Access type either Block All devices or Allow All devices status

- **Block All -** When Block all option is selected, all the devices in the Blocked Devices would be blocked from connecting to the router.
- **Allow All -** When Allow All option is selected, all the devices in the Blocked Devices would be allowed to connect to the router.

8.3.1 SNMP Provisioning for Device Filter

- **tchRgFirewallMacFilterIndex** - Main Index
- **tchRgFirewallMacFilterRowStatus -** To Add/delete and view the rows
- **tchRgFirewallMacFilterAddress** - To Add a MAC Address
- **tchRgFirewallMacFilterAlwaysBlock -** To Set device Filter to "Always Block"
- **tchRgFirewallMacFilterBlockStartTime -** To Set the Start time of the Time Interval Based blocking
- **tchRgFirewallMacFilterBlockEndTime -** To set the End time of the Time Interval based blocking
- **tchRgFirewallMacFilterBlockDays -** To Set the Days filter for Day based blocking.

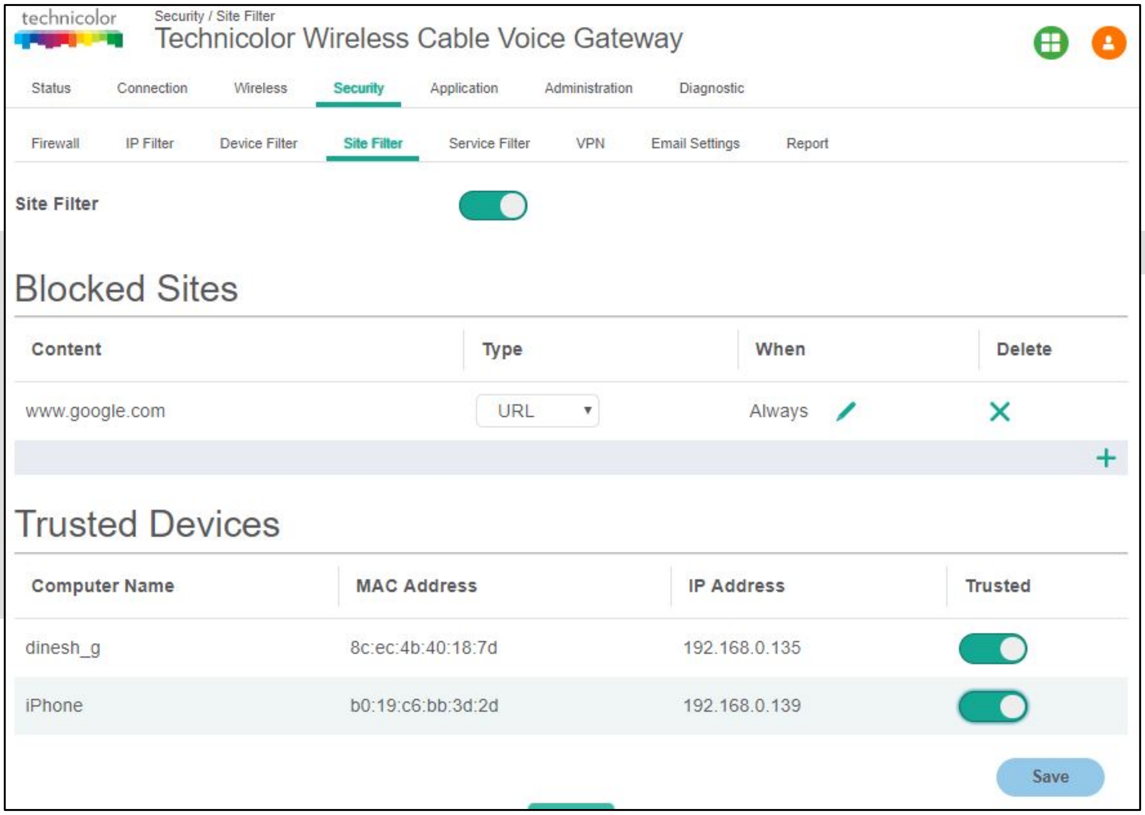
8.4 Site Filter

Site Filter page is used to block websites based on user necessities. User can add the desired website under the Blocked sites and the added website will be blocked for both LAN and WLAN devices, which are connected through the router.

Security Tab / Site Filter

Click on the Security tab then click on Site Filter tab. This page displays following Site Filter setup information which can be viewed and set by user:

- Site Filter Status: (Enabled / Disabled)
- Blocked Sites: (Content, Type, When, Delete)
- Trusted Devices: (Computer Name, MAC Address, IP Address, Trusted)



Site Filter ●

Blocked Sites

Content	Type	When	Delete
www.google.com	URL ▾	Always	✕

Trusted Devices

Computer Name	MAC Address	IP Address	Trusted
dinesh_g	8c:ec:4b:40:18:7d	192.168.0.135	●
iPhone	b0:19:c6:bb:3d:2d	192.168.0.139	●

Figure 8.4

The filter would be applied to all the devices in the trusted list. The user can edit/modify the filter setting to block the sites always, block on specific day, specific time, etc. The user also can remove the sites from the trusted devices list to remove the filter option for them.

The user needs to edit and press the Save button in the page to set the desired configuration.

8.4.1 SNMP Provisioning for Site Filter

Following MIBs are used to provision the Site Filter feature:

- **tchRgFirewallUrlKeywordFilterIndex** - Main Index

- **tchRgFirewallUrlKeywordFilterRowStatus** -To Add/delete and view the rows
- **tchRgFirewallUrlKeywordFilterMethod** - To Set the filter method as Keyword Filter or URL Filter
- **tchRgFirewallUrlKeywordFilterMatch** - To set the desired URL for blocking
- **tchRgFirewallUrlKeywordFilterAlwaysBlock** - To Set Filter to "Always Block"
- **tchRgFirewallUrlKeywordFilterBlockStartTime** - To Set the Start time of the Time Interval Based blocking
- **tchRgFirewallUrlKeywordFilterBlockEndTime** - To set the End time of the Time Interval based blocking
- **tchRgFirewallUrlKeywordFilterBlockDays** - To Set the Days filter for Day based blocking

8.5 Service Filter

The Service Filter page is used to block certain service requests coming from the WAN to LAN devices connected through the router. User can block the desired service port range by adding it to Blocked services

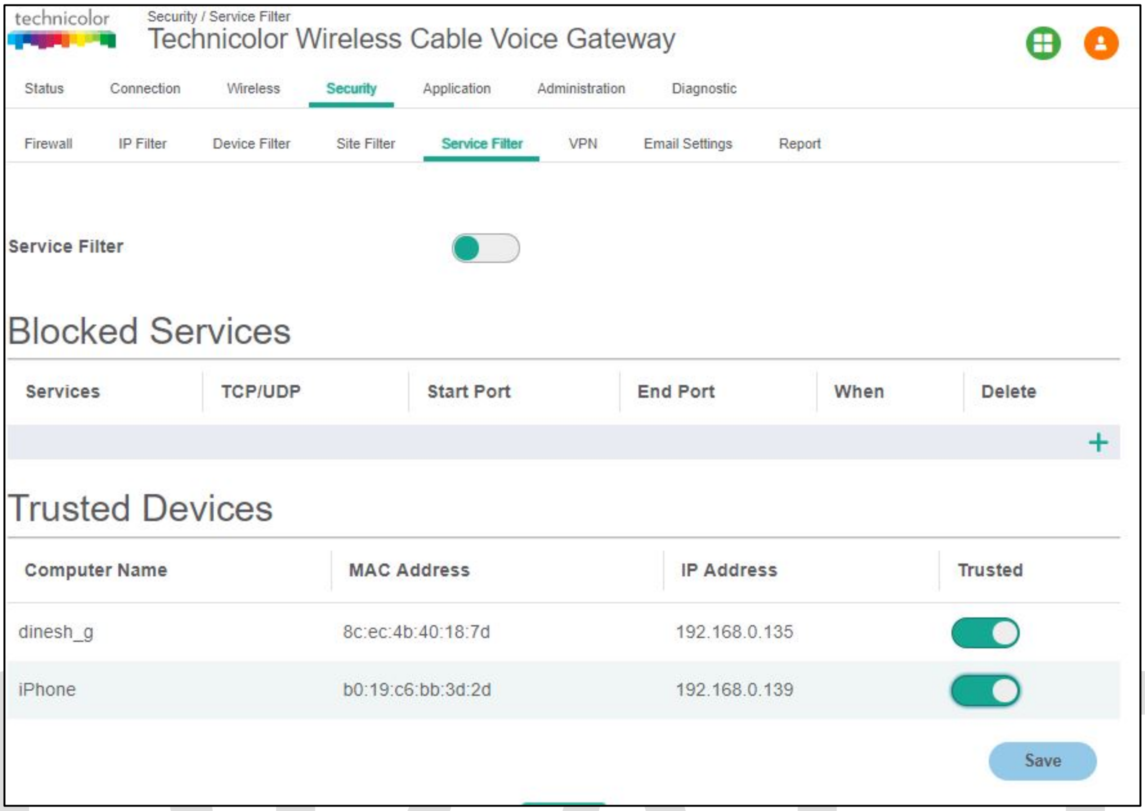
Security Tab / Service Filter
Click on Security tab then click on Service Filter tab. The page displays following Service Filter setup information, which can be viewed and modified by user.

Service Filter Status
Blocked Services: The specific traffic / service that are blocked using the Service Filter. This could be protocols or port numbers. (Services, TCP/UDP, Start Port, End Port, Time, and Delete)
Trusted Devices: These devices can be exempted from applying the Service filter for them. (Computer Name, MAC Address, IP Address and Trusted).

Enable Service Filter
Service Filter can be enabled with either disabled or enabled Trusted Devices, as shown in the figures below. The status can be enabled by clicking on the corresponding button.

Enable Service Filter with Trusted Device Disable:
Enable Service Filter with Trusted Devices Disabled

The following screen shows the list of trusted devices (without service filter feature enabled).



Service Filter: Off

Blocked Services

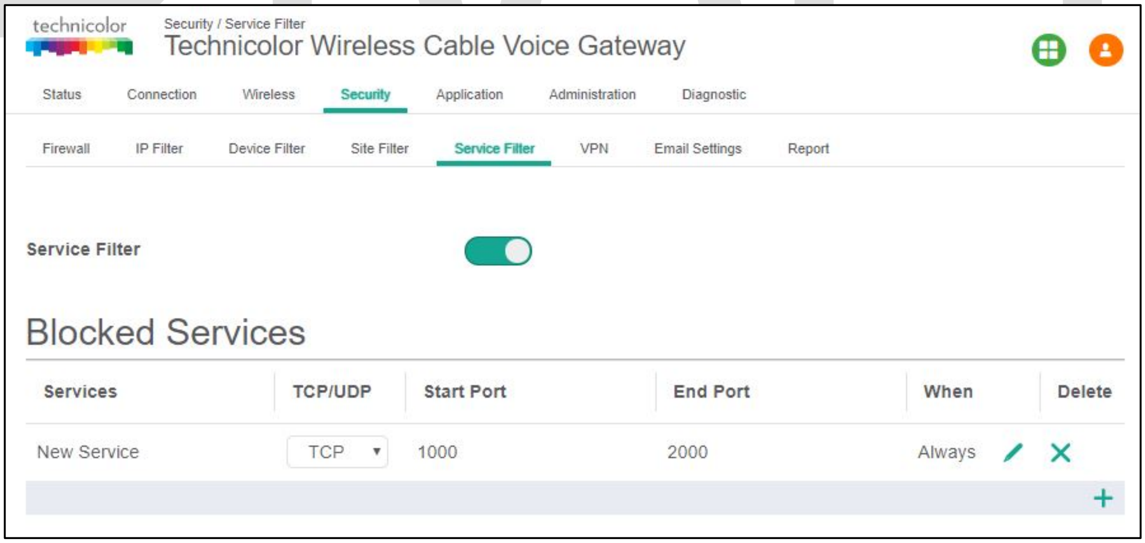
Services	TCP/UDP	Start Port	End Port	When	Delete

Trusted Devices

Computer Name	MAC Address	IP Address	Trusted
dinesh_g	8c:ec:4b:40:18:7d	192.168.0.135	On
iPhone	b0:19:c6:bb:3d:2d	192.168.0.139	On

Figure 8.5

The user can add a service filter by pressing the + option and providing the specific service, port number ranges and the time range for the filter action. The following screen shows a specific service filter being enabled:



Service Filter: On

Blocked Services

Services	TCP/UDP	Start Port	End Port	When	Delete
New Service	TCP	1000	2000	Always	✎ ✕

Figure 8.6

The user can edit / modify the service filters to change the duration for the filter to be active (day of the week, time of the day, etc.).

8.5.1 SNMP Provisioning for Service Filter

Following MIBs implements the Service Filter functions:

- **tchRgFirewallPortFilterIndex** - Main Index
- **tchRgFirewallPortFilterRowStatus -** To Add/delete and view the rows
- **tchRgFirewallPortFilterPortStart** - To set Start Port Number
- **tchRgFirewallPortFilterPortEnd** - To set End Port Number
- **tchRgFirewallPortFilterProto** - To set the desired Protocol
- **tchRgFirewallPortFilterAlwaysBlock -** To set permission to always block
- **tchRgFirewallPortFilterBlockStartTime** - To Set the Start time of the Time Interval Based blocking
- **tchRgFirewallPortFilterBlockEndTime -** To set the End time of the Time Interval based blocking
- **tchRgFirewallPortFilterBlockDays -** To Set the Days filter for Day based blocking

8.6 VPN Settings

This feature is used in cases where the Wireless Gateway acts as the VPN end point and all the machines connected to the LAN side want to be on the enterprise private network. This is mainly used in B2B (Business-2-Business) applications.

For the Wireless Gateway to act as a VPN end point, the user needs to configure a VPN tunnel on the Wireless Gateway. This can be done from the Security / VPN page. Enter the details of the local subnet and the remote subnet including the VPN gateway and security parameters for IPSEC (Key Exchange Method, Encryption, Authentication, Pre-shared key. etc.). Obtain these details from the network administrator (of the enterprise you are connecting to) before setting up the VPN tunnel.

8.6.1 User Provisioning for VPN Settings

Security Tab / VPN

Click on Security tab then click on VPN tab. The page displays VPN setup information. Here the user can set and display VPN information.

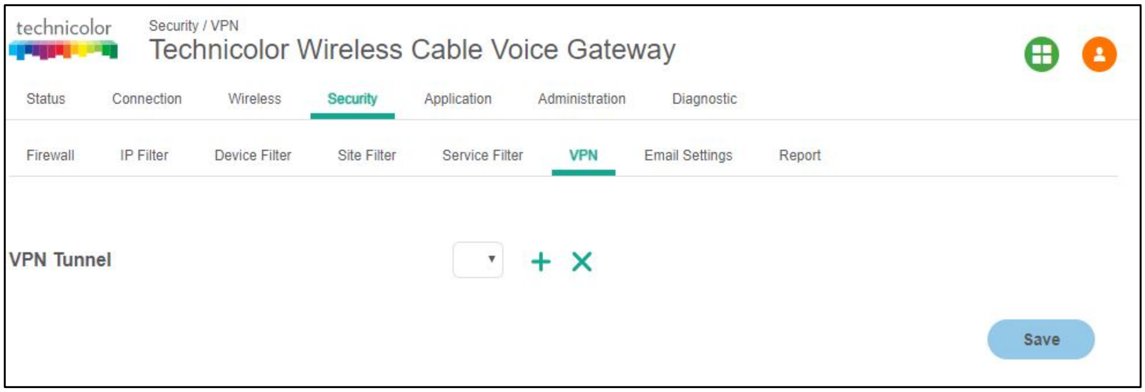
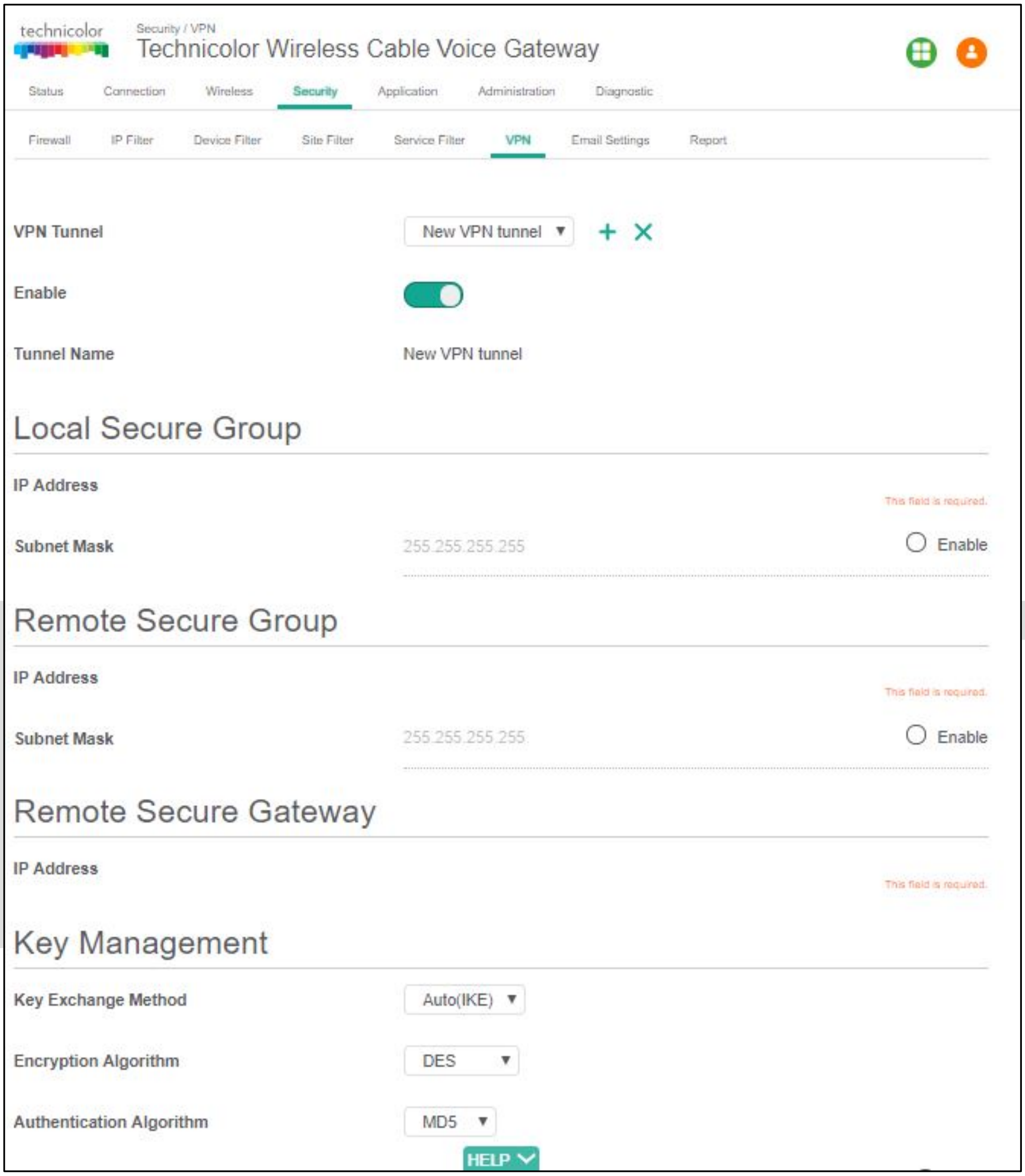


Figure 8.7

The user can configure the VPN Tunnel details by clicking on '+' symbol corresponding to the VPN Tunnel option. The page will show the following information:

- Enable (Option to enable VPN),
- Tunnel Name (Name of the tunnel to be created between endpoints)
- Local Secure Group: - (IP Address, Subnet Mask)
- Remote Secure Group: - (IP Address, Subnet Mask)
- Remote Secure Gateway: - (IP Address)
- Key Management: - (Key Exchange Method, Encryption Algorithm, Authentication
- Algorithm, Pre –Shared Key, Key Life Time)



Technicolor Wireless Cable Voice Gateway

VPN Tunnel New VPN tunnel ▾ + ✕

Enable

Tunnel Name New VPN tunnel

Local Secure Group

IP Address

This field is required.

Subnet Mask 255.255.255.255 ○ Enable

Remote Secure Group

IP Address

This field is required.

Subnet Mask 255.255.255.255 ○ Enable

Remote Secure Gateway

IP Address

This field is required.

Key Management

Key Exchange Method Auto(IKE) ▾

Encryption Algorithm DES ▾

Authentication Algorithm MD5 ▾

Figure 8.8

VPN Tunnel **Select Tunnel Entry:** Select a tunnel to configure.
+ Button: Click this button to create a new tunnel.
'X' Button: Click this button to delete all settings for the selected tunnel.

Enable To Enable VPN Tunnel

Tunnel Name: Enter a name for this tunnel, such as London Office.

Local Secure Group Select the local LAN user(s) that can use this VPN tunnel. This may be a single IP address or sub--network. Note that the Local Secure Group must match the remote gateway's

Remote Secure Group.

IP Address:

Enter the IP address on the local network.

Subnet Mask:

If the Subnet option is selected, enter the mask to determine the IP Addresses on the local network.

Remote Secure Group

Select the remote LAN user(s) behind the remote gateway who can use this VPN tunnel. This may be a single IP address, a sub--network, or any addresses. If Any is set, the Gateway acts as a responder and accepts requests from any remote user. Note that the Remote Secure Group must match the remote gateway's Local Secure Group.

IP Address:

Enter the IP address on the remote network.

Subnet Mask:

If the Subnet option is selected, enter the mask to determine the IP addresses on the remote network.

Remote Secure Gateway

Select the desired option, IP Address.,

Key Management

Key Exchange Method:

The device supports both automatic and manual key management.

When automatic key management is selected, Internet Key Exchange (IKE) protocols are used to negotiate key material for Security Association (SA). If manual key management is selected, no key negotiation is needed. Basically, manual key management is used in small static environments or for troubleshooting purposes.

Note that both sides must use the same key management method.

Encryption Algorithm:

The Encryption method determines the length of the key used to Encrypt/decrypt ESP packets. Note that both sides must use the Same method.

Available Options are DES, 3DES, AES-128, AES-129, AES-256

Authentication Algorithm:

The Authentication method authenticates the Encapsulating Security

Payload (ESP) packets. Select MD5 or SHA. Notice that both sides (VPN Endpoints) must use the same method.

MD5: A one--way hashing algorithm that produces a 128--bitdigests

SHA1: A one--way hashing algorithm that produces a 160--bitdigests

Pre-Shared Key:

IKE uses the Pre--Shared Key to authenticate the remote

IKE peer. Both character and hexadecimal values are acceptable in this field, e.g.,

My_@123 or 0x4d795f40313233. Note that both sides must use the same Pre--Shared Key.

Key Lifetime:

This field specifies the lifetime of the IKE generated key. If the time expires, a new key will be renegotiated automatically. The Key

Lifetime may range from 300 to 100,000,000 seconds. The default lifetime is 3600 seconds.

Enable:

To Enable the Key Management.

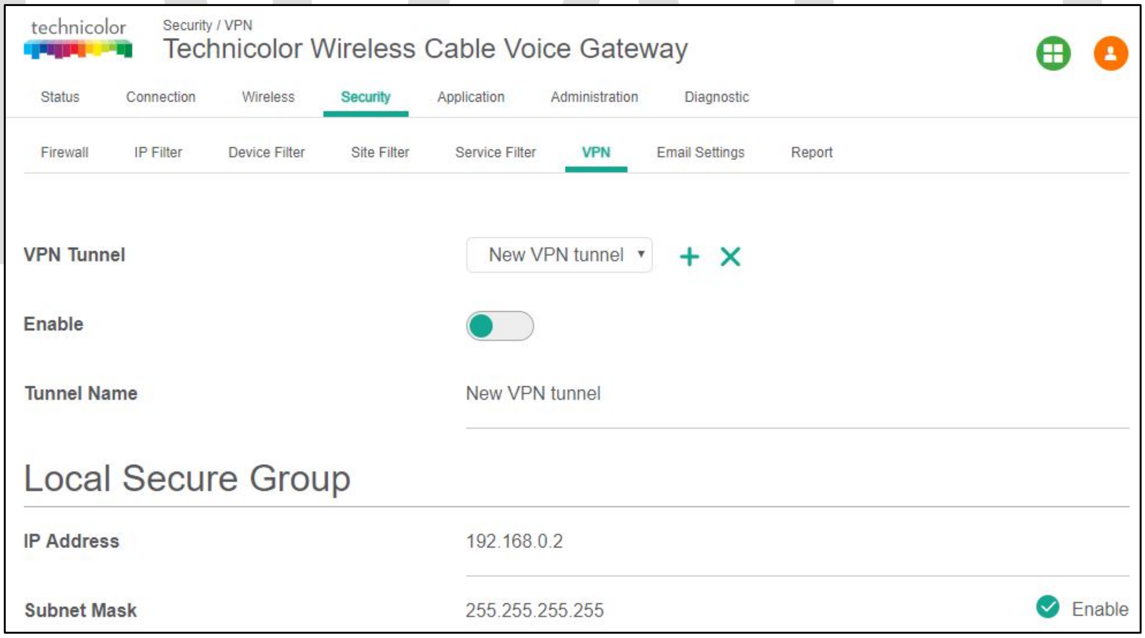
Tunnel Name:

This field specifies Tunnel Name.

Setting the values of different parameters:

- Click on the parameter and change the values in valid range
- Select the corresponding button
- Click on the corresponding drop down menu and select the required values
- Press Save

Below figures shows the value settings for different parameters.



VPN Tunnel: New VPN tunnel ▾

Enable: ●

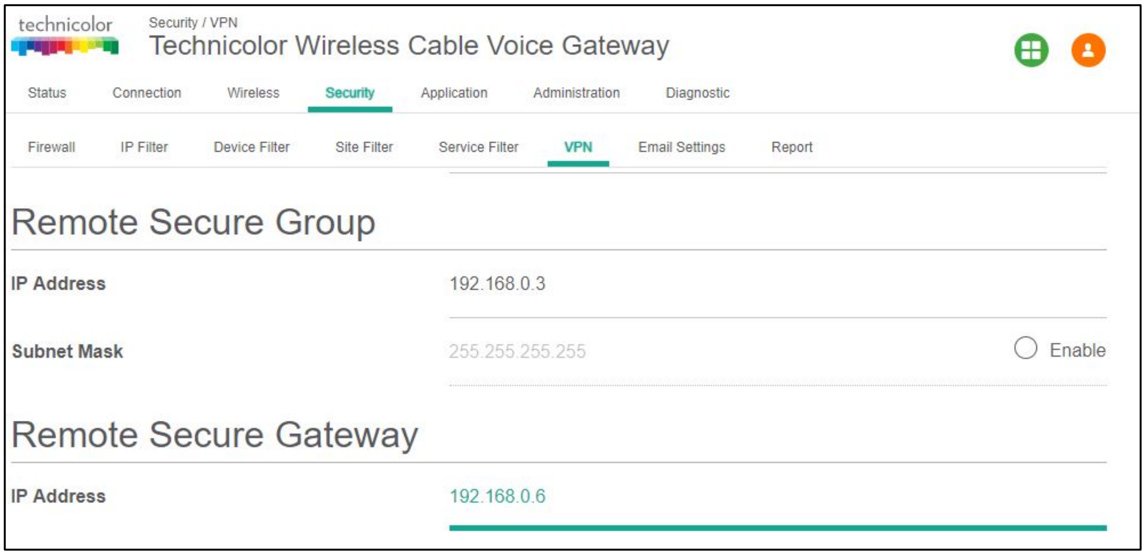
Tunnel Name: New VPN tunnel

Local Secure Group

IP Address: 192.168.0.2

Subnet Mask: 255.255.255.255 ✓ Enable

Figure 8.9



Remote Secure Group

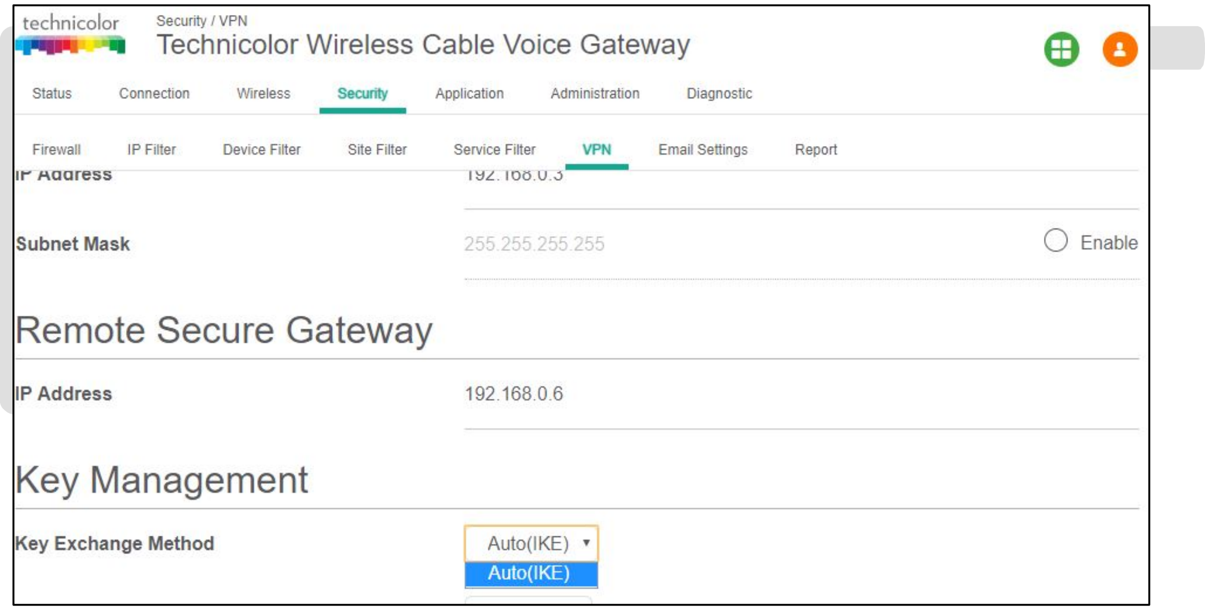
IP Address 192.168.0.3

Subnet Mask 255.255.255.255 ○ Enable

Remote Secure Gateway

IP Address 192.168.0.6

Figure 8.10



IP Address 192.168.0.3

Subnet Mask 255.255.255.255 ○ Enable

Remote Secure Gateway

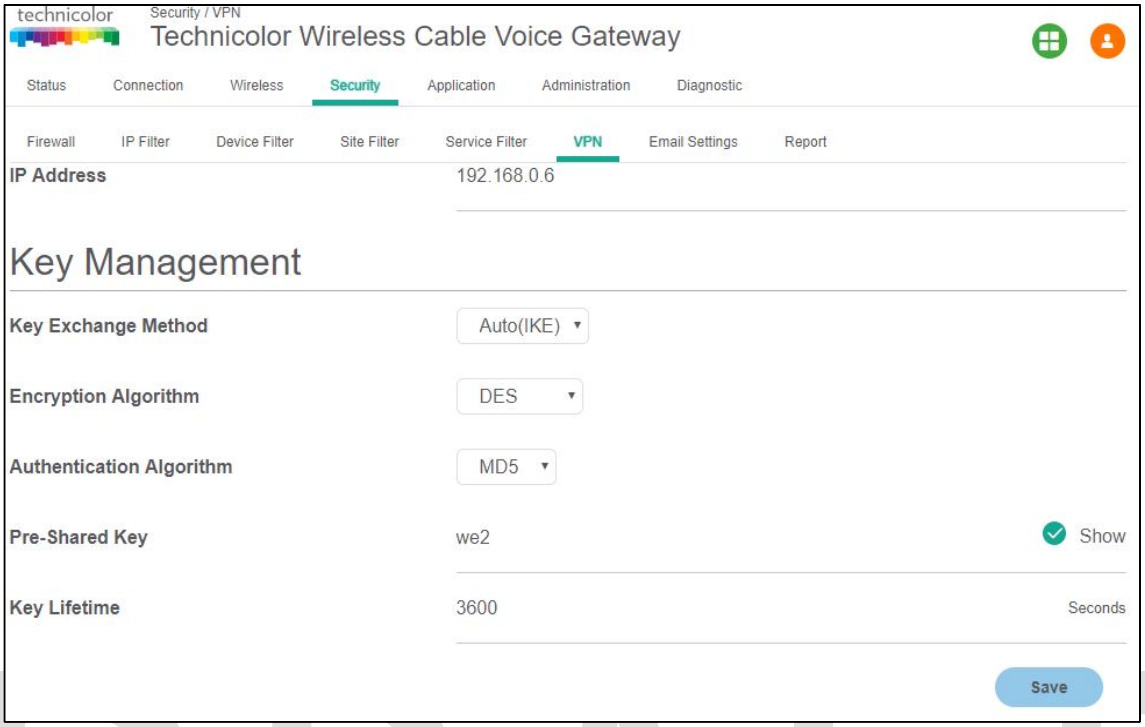
IP Address 192.168.0.6

Key Management

Key Exchange Method Auto(IKE) ▾

Auto(IKE)

Figure 8.11



IP Address 192.168.0.6

Key Management

Key Exchange Method: Auto(IKE)

Encryption Algorithm: DES

Authentication Algorithm: MD5

Pre-Shared Key: we2 ✓ Show

Key Lifetime: 3600 Seconds

Figure 8.12

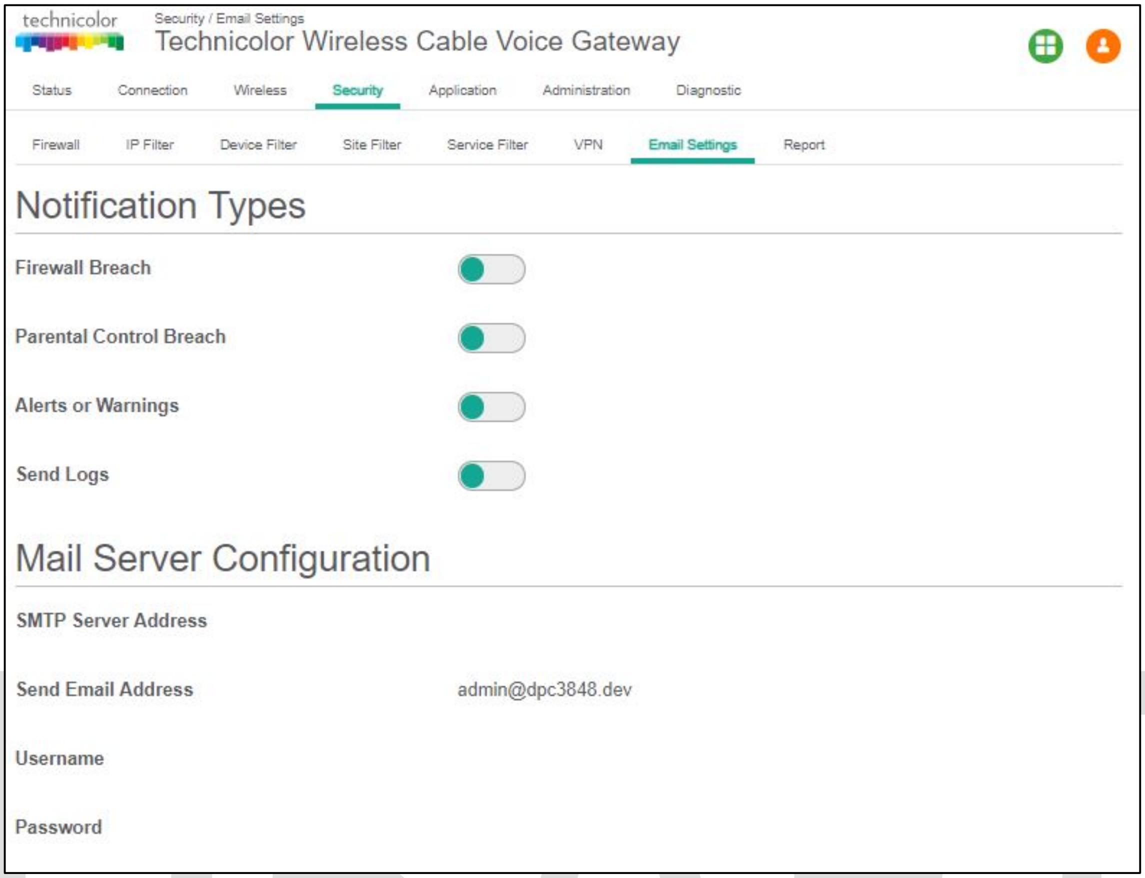
8.7 Email Settings

This page is used to create email based notifications for security events. The user can configure the email server, the notifications to be forwarded to the server and the email address of the recipient through this page.

Security Tab / Email Settings

Click on Security tab then click on Email settings tab. The page displays Email settings information which can be viewed and modified by the user. The following information will be displayed.

- Recipient Email
- Notification Types - (Firewall Breach, Parental Control Breach, Alerts or Warnings, Send Logs)
- Mail Server Configuration - (SMTP Server Address, Send Email Address, Username and Password)



Notification Types

Firewall Breach

Parental Control Breach

Alerts or Warnings

Send Logs

Mail Server Configuration

SMTP Server Address

Send Email Address admin@dpc3848.dev

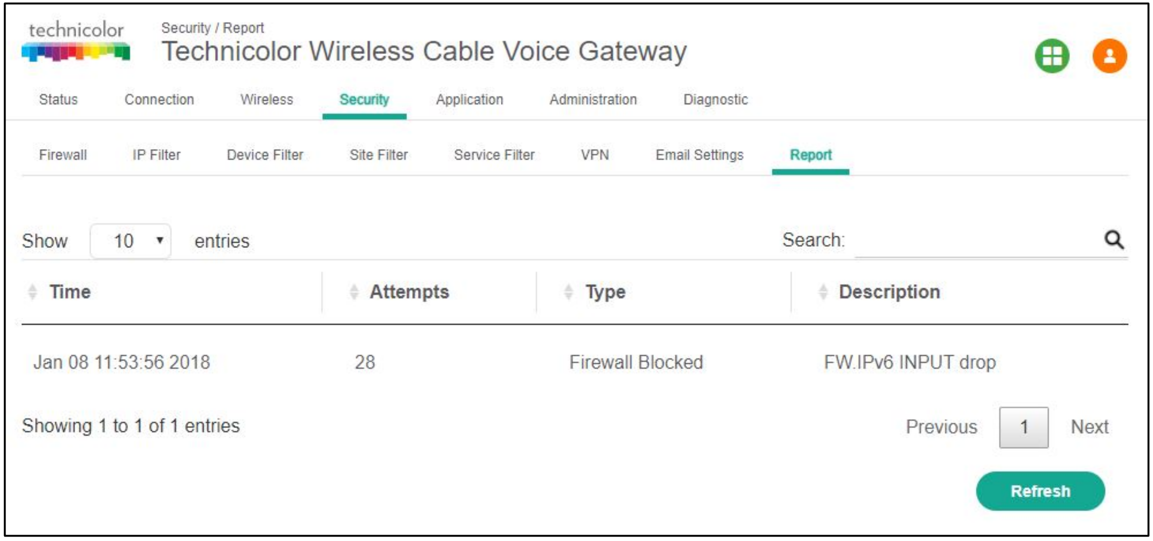
Username

Password

Figure 8.13

8.8 Reports

To display security events, select the Security tab in the Gateway page and then select Report tab. Device Filter logs, Site Filter logs, Service Filter logs and Email Settings logs, and Firewall Logs will be displayed as shown below:



Time	Attempts	Type	Description
Jan 08 11:53:56 2018	28	Firewall Blocked	FW.IPv6 INPUT drop

Showing 1 to 1 of 1 entries

Figure 8.14

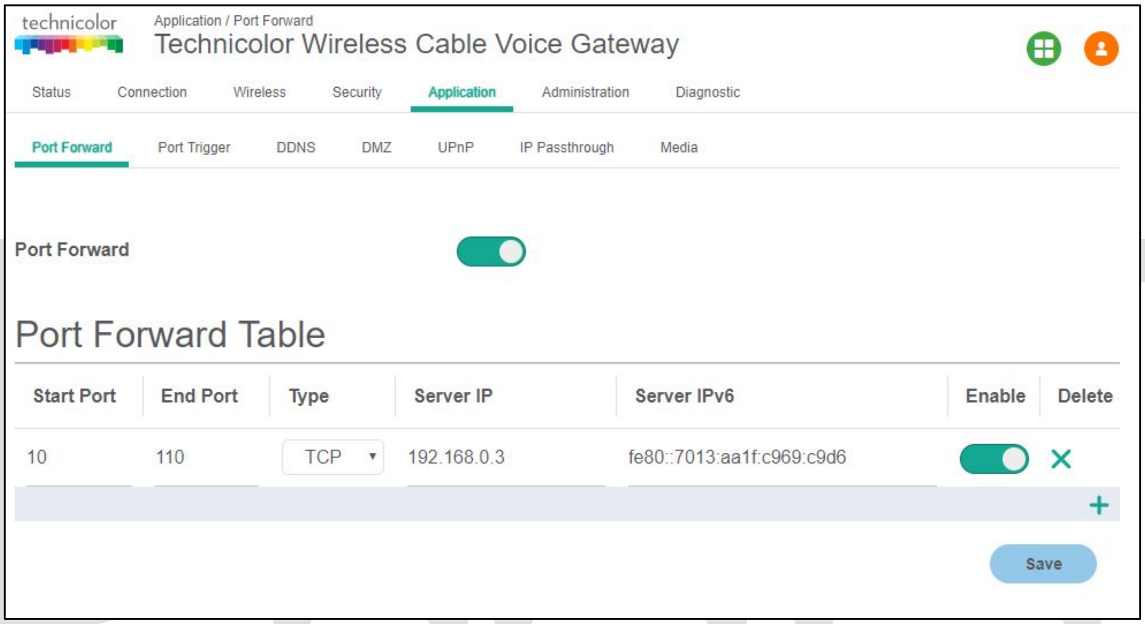
9 Application

9.1 Port Forward

Port Forwarding is commonly used to run a publicly accessible server on the LAN by specifying the mapping of TCP/UDP ports to a local PC.

Application Tab / Port Forward

Click on the Application tab then click on the Port Forward settings tab. This page displays Port Forward information. Here user can display and set Port Forward Table details. (Start Port, End Port, Type, Service IP, Service IPv6, Enable and Delete)



Port Forward ●

Port Forward Table

Start Port	End Port	Type	Server IP	Server IPv6	Enable	Delete
10	110	TCP	192.168.0.3	fe80::7013:aa1f:c969:c9d6	●	✕

Figure 9.1

To specify a mapping, enter the range of port numbers that should be forwarded locally, and the IP address to which traffic to those ports should be sent. If only a single port specification is desired, enter the same port number in the start and end locations for that IP address.

Setting the values of different parameters:

- Click on the parameter and change the values in valid range
- Select the corresponding button
- Click on the corresponding drop down menu and select the required values
- Press Save

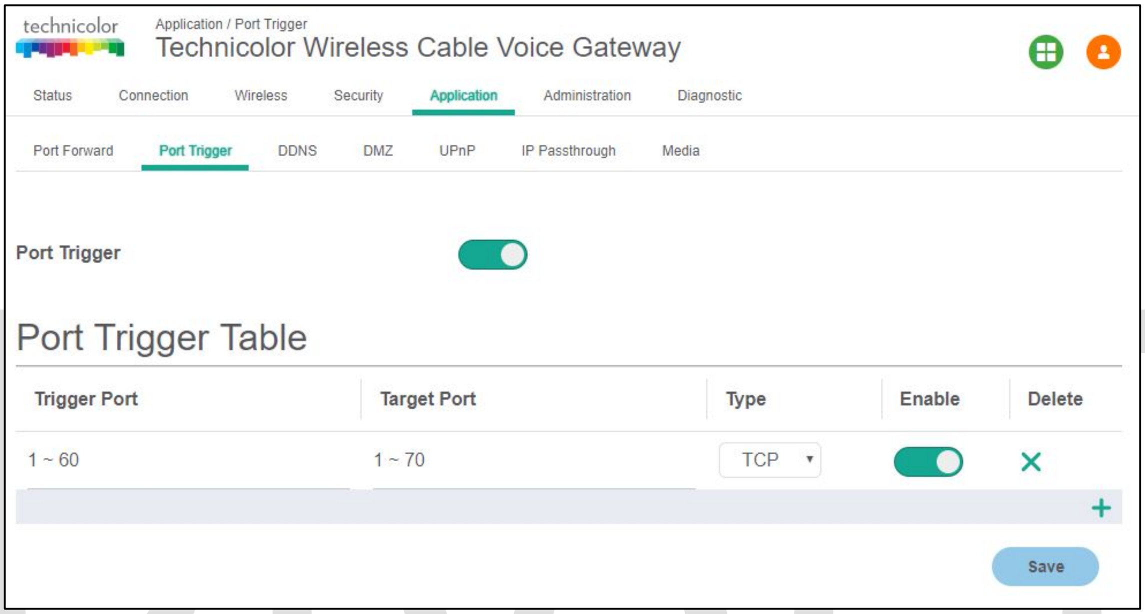
9.2 Port Trigger

Port Triggers are similar to Port Forwarding except that they are not static ports held open all the time. When the Technicolor Wireless Gateway detects outgoing data on a specific IP port number set in the Trigger Range, the resulting ports set in the Target Range are opened for incoming (or sometimes referred to as bi-directional ports) data. If no outgoing traffic is detected on the Trigger Range ports for 10 minutes, the Target Range ports will close.

This is a safer method for opening specific ports for special applications (e.g. video conferencing programs, interactive gaming, file transfer in chat programs, etc.) because they are dynamically triggered and not held open constantly or erroneously left open via the router administrator and exposed for potential hackers to discover.

Application Tab / Port Trigger

Click on the Application tab then click on Port Trigger settings tab. This page displays Port Trigger setup information (Trigger Port, Target Port, Type, Enable and Delete). In this view, the user can set/change the Port Trigger configuration



Port Trigger: on

Port Trigger Table

Trigger Port	Target Port	Type	Enable	Delete
1 ~ 60	1 ~ 70	TCP	on	✕

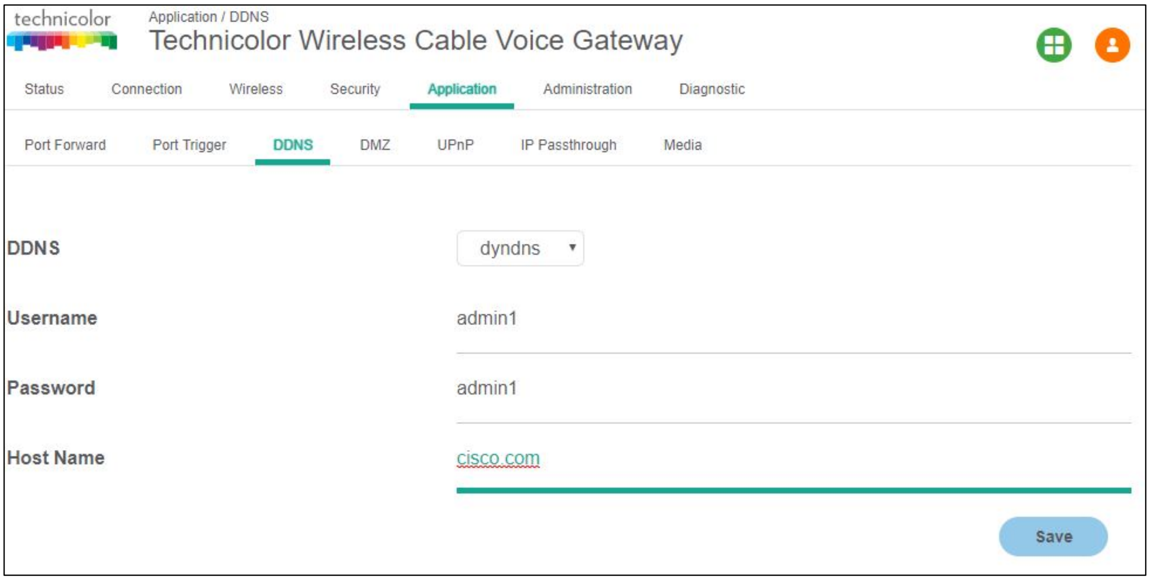
Figure 9.2

9.3 DDNS

Dynamic DNS (DDNS) allows a dynamic IP address to be aliased to a static, pre-defined host name so that the host can be easily contacted by other hosts on the internet even if its IP address changes. The Technicolor Wireless Gateway supports a dynamic DNS client compatible with the Dynamic DNS service (http://www.dyndns.com/). Since implementation of DDNS the service has switched from a free service to a paid service. A paid account is now required to use this feature. Technicolor is evaluating other dynamic DNS options for future implementation.

Application Tab/ DDNS

Click on the Application tab then click on DDNS tab. This page displays DDNS setup information. Here, user can set and display DDNS (Disable, DynDns.org, TZO.com, Changeip.com, and Freedns.afraid.com), Username, Password and Hostname.



DDNS dyndns

Username admin1

Password admin1

Host Name cisco.com

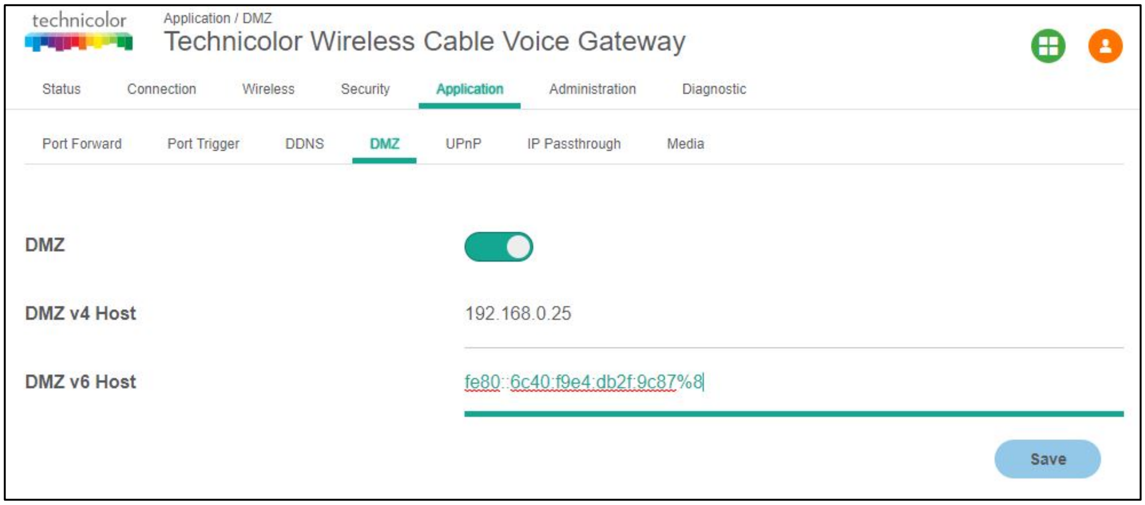
Figure 9.3

9.4 DMZ

The DMZ feature exposes the network user to the Internet for using special-purpose services such as Internet Gaming or Video Conferencing. DMZ hosting forwards all the ports at the same time to one computer. The Port Range Forwarding feature is more secure because it only opens the ports the user want to have opened, while DMZ hosting opens all the ports of one computer, exposing the computer to the Internet. This is generally used if PCs are running specific applications that use random unknown port numbers and do not function correctly with specific port triggers or port forwarding setups. It is advisable not to have any PCs/Servers as DMZ hosts because of exposure to the public internet which results from this configuration. Remember to disable this setting if this is enabled temporarily for any specific application.

Any computer whose port is being forwarded must have its DHCP client function disabled and should have a static IP address assigned to it because its IP address may change when it is using the DHCP function.

Application Tab/ DMZ
Click on Application tab then click on DMZ tab. This page displays DMZ setup information. Here a user can set and display DMZ parameters including DMZ enable and DMZ v4 and v6 Host addresses.



DMZ ●

DMZ v4 Host 192.168.0.25

DMZ v6 Host fe80::6c40:f9e4:db2f:9c87%8

Figure 9.4

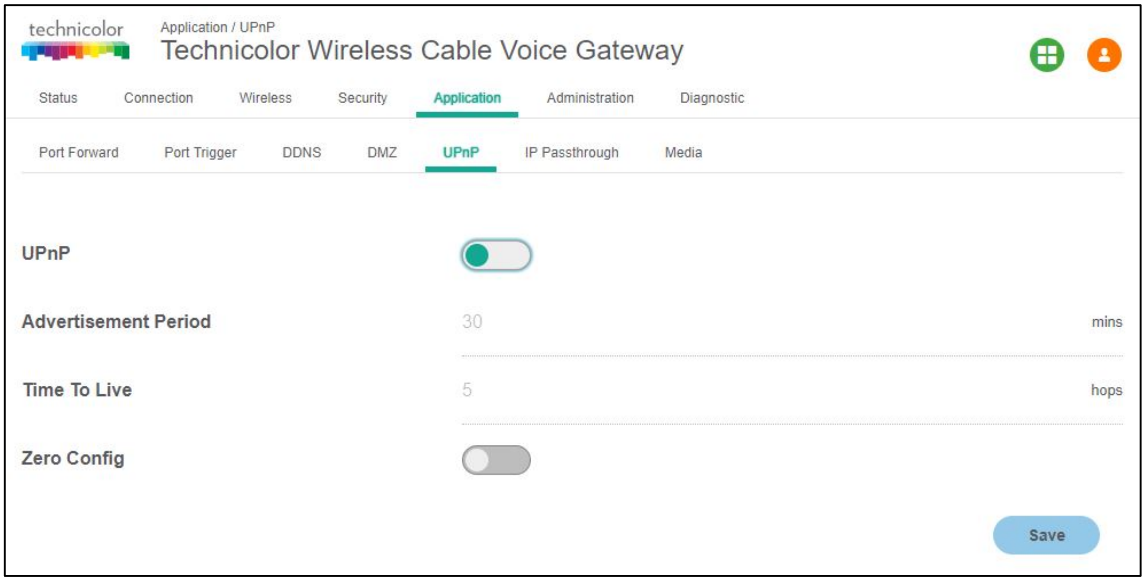
9.4.1 SNMP Provisioning for DMZ

For DMZ Host IP address set the following MIB: **tchRgFirewallDmzAddress**.
For all firewall MIBS set the **tchRgFirewallApplySettings** to 1 to take effect

9.5 UPNP

Universal Plug and Play (UPnP) allows client devices to automatically configure the device for various Internet applications, such as gaming and video conferencing. This protocol messaging over the LAN can be enabled or disabled.

Application Tab / UPnP
Click on the Application tab, and then click on UPnP tab. The page displays UPnP setup information. Here, user can enable or disable UPnP and alter parameters such as the Advertisement Period, Time to Live, and Zero Config.



UPnP ●

Advertisement Period 30 mins

Time To Live 5 hops

Zero Config ○

Figure 9.5

9.5.1 User Provisioning of UPnP

Users can Enable/Disable UPnP using the UPnP button option. While enabling the features, the parameters, Advertisement Period, TTL and Zero Config can be appropriately configured and saved.

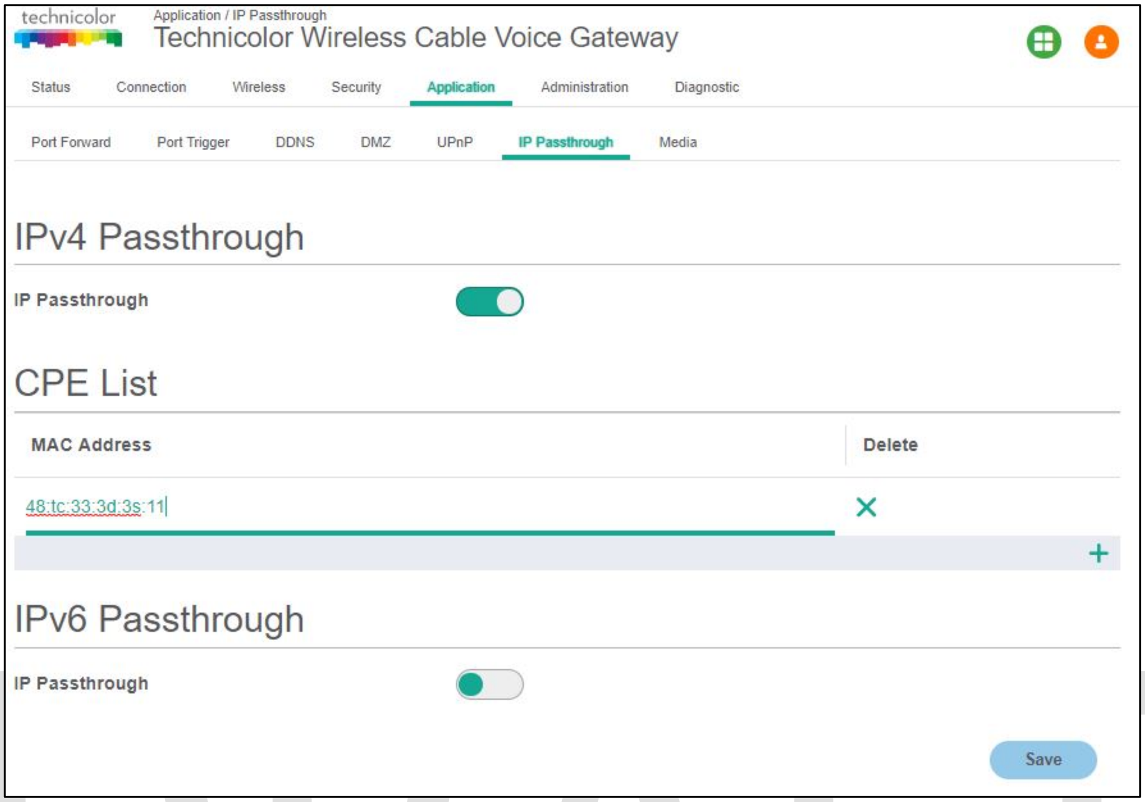
9.5.2 SNMP Provisioning for UPNP

The UPnP feature is controlled via **tchRgIpMgmtLanUpnp**. Since the MIB is a table for different SSID, UPnP configuration is supported on all primary as well as secondary SSIDs.

9.6 IP Passthrough

The IP Passthrough feature allows a device on the LAN to have the gateway's public address assigned to it. This configuration is often times suitable for a customer desiring to connect third party equipment to the internet.

Application Tab/ IP Passthrough
Click on the Application tab, and then click on IP Passthrough tab. The page displays setting up information IP Passthrough. Here, the user set and display IPv4 Passthrough, CPE List (MAC Address), IPv6 Passthrough.



IPv4 Passthrough

IP Passthrough: ●

CPE List

MAC Address	Delete
48:tc:33:3d:3s:11	✕

+

IPv6 Passthrough

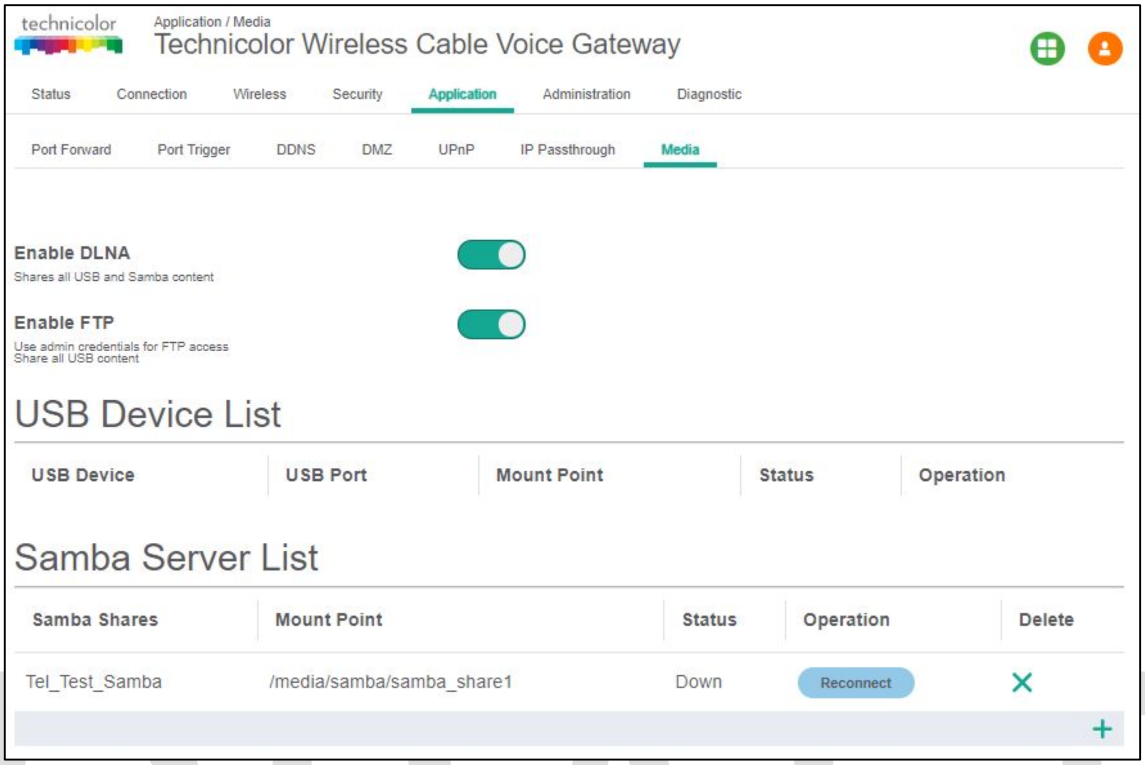
IP Passthrough: ○

Figure 9.6

9.7 Media

This page displays Media setup information. Here, we can set and display Enable DLNA, Enable FTP, USB Device List and Samba Server List.

Application Tab/ Media
Click on the Application tab, and then click on Media tab. The Gateway page appears populated with the information below:



Enable DLNA

Shares all USB and Samba content

Enable FTP

Use admin credentials for FTP access
Share all USB content

USB Device List

USB Device	USB Port	Mount Point	Status	Operation

Samba Server List

Samba Shares	Mount Point	Status	Operation	Delete
Tel_Test_Samba	/media/samba/samba_share1	Down	Reconnect	✕

Figure 9.7

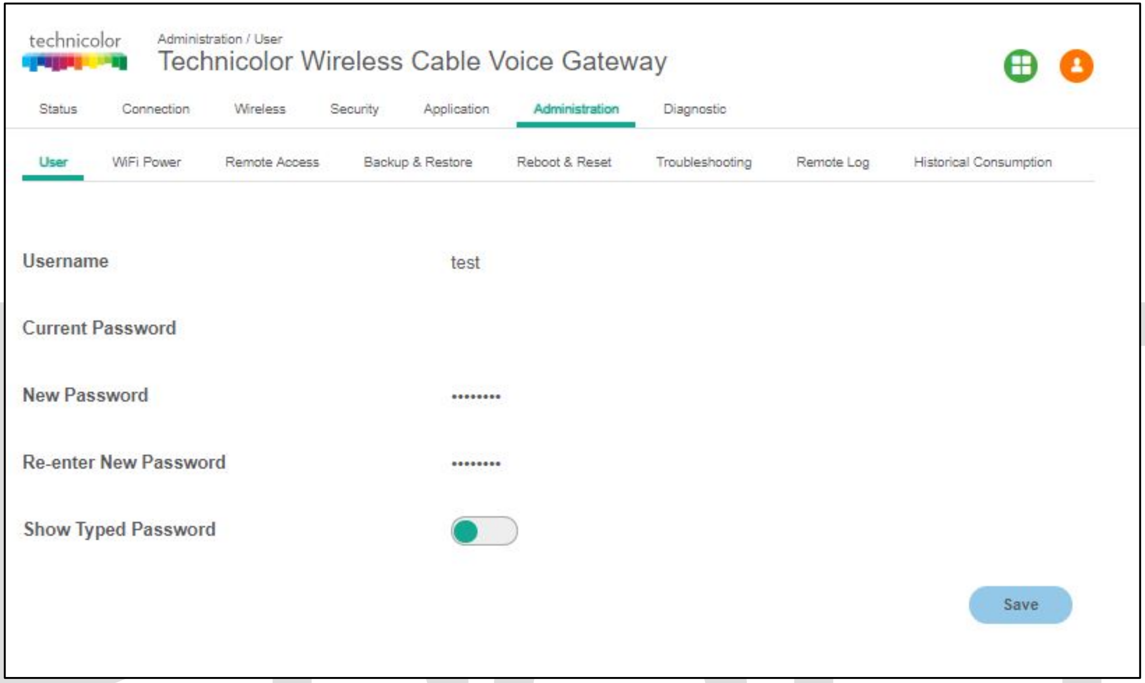
10 Administration

10.1 User

Administration / User

We have two users for this box **Home-User** and the **Adv-User**. When logged in as Home-User via WebUI, the page provides options to change the default username and the password.

Click on the Administration tab and then the User tab. The page appears with the information below. The user name and password can be entered into the various fields and changed.



Username test

Current Password

New Password ••••••••

Re-enter New Password ••••••••

Show Typed Password

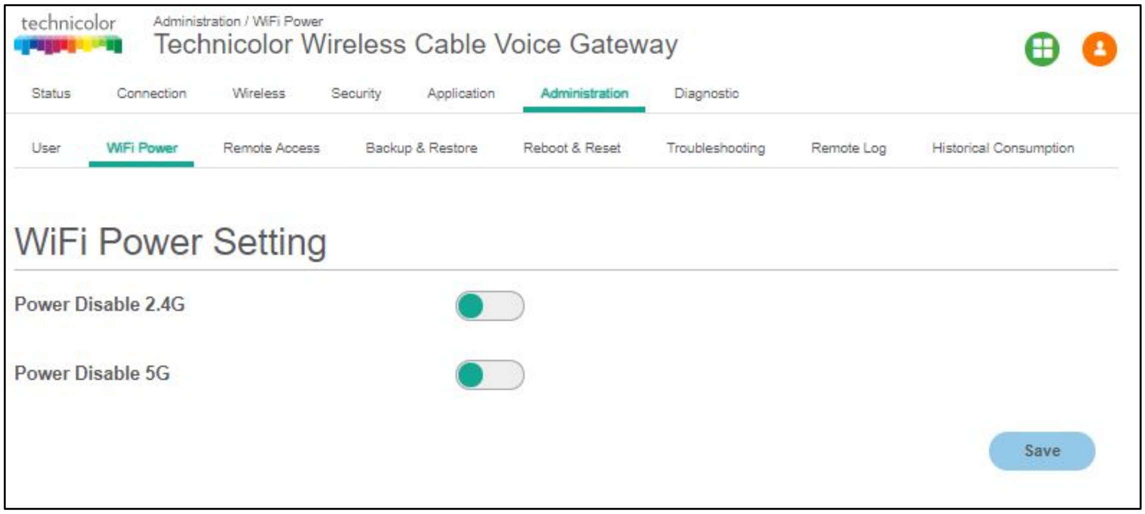
Figure 10.1

10.2 WiFi Power

This page provides the user an option to turn off and turn on the radio power for the 2.4GHz and 5GHz radios.

Administration / WiFi Power

Click on the Administration tab and then the WiFi Power tab. The page appears with the information below:


Administration / WiFi Power

Technicolor Wireless Cable Voice Gateway

WiFi Power Setting

Power Disable 2.4G

Power Disable 5G

Figure 10.2

The user can change the WiFi power setting by enabling or disabling the options provided in the screen.

10.3 Remote Access

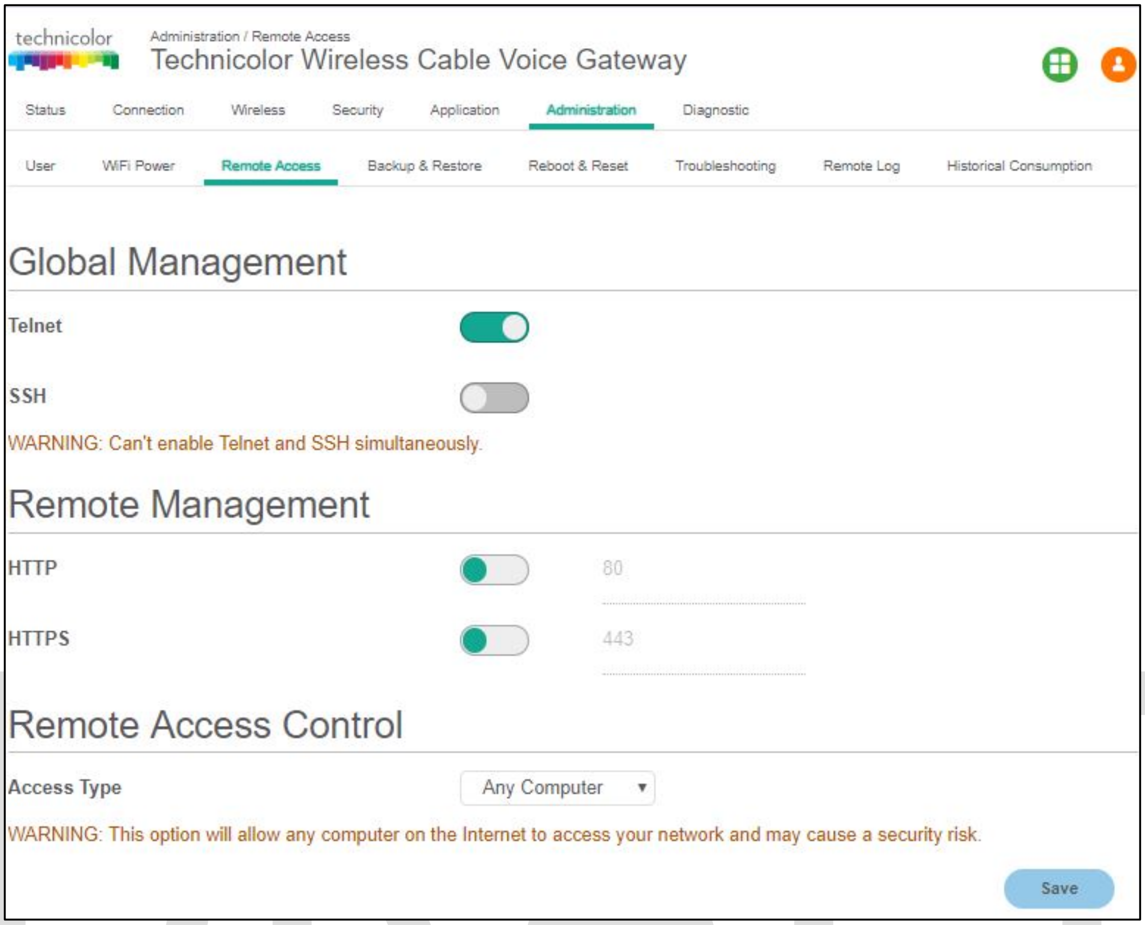
Administration / Remote Access

The Administration/Remote Access page can be accessed when logged in as Home-User (This page is not seen when logged in as Advanced User).

When Telnet is Enabled the Box can be remotely accessed via CM IP. Telnet and SSH cannot be enabled at the same time, either of these can be enabled at a given point of time. A remote terminal can establish a SSH session with the box if the SSH radio button is enabled. The HTTP and HTTPS can be enabled/disabled to allow/limit the WebUI access over corresponding communication protocol.

The options selected under the Global Management and the Remote Management can be applied to a single computer, range of computers or any computer by selecting the corresponding options provided against the Access Type.

Click on the Administration tab and then the Remote Access tab. The page appears with the information below:



Global Management

Telnet: ● On

SSH: ○ Off

WARNING: Can't enable Telnet and SSH simultaneously.

Remote Management

HTTP: ○ Off 80

HTTPS: ○ Off 443

Remote Access Control

Access Type: Any Computer ▾

WARNING: This option will allow any computer on the Internet to access your network and may cause a security risk.

Figure 10.3

10.3.1 SNMP Provisioning for Remote Management

Below are the MIBs used for Remote Management configuration:

- **tchRgDeviceRemoteWebAccessEnable**
- **tchRgDeviceRemoteWebAccessPort**

10.4 Backup & Restore

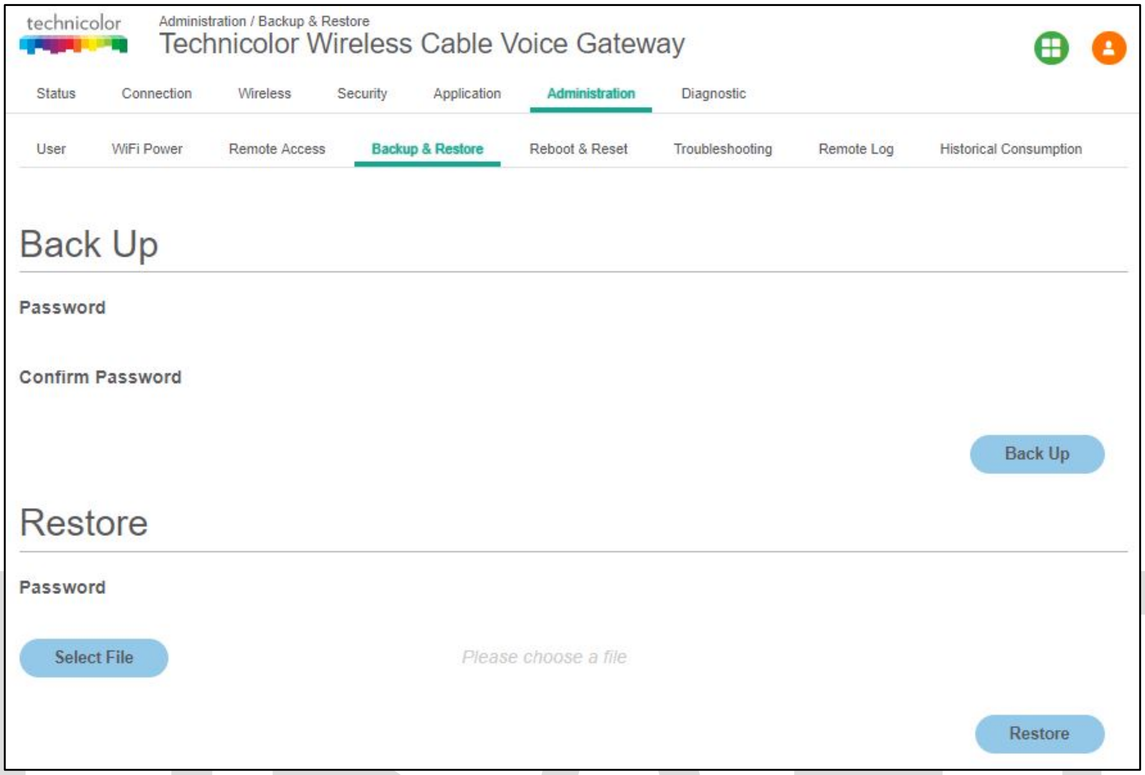
The backup feature saves the current gateway configuration to a local PC. These settings can be restored later if a configuration needs to be restored, or to recover from changes that have had an undesirable effect.

To backup the current configuration, click Backup and follow the prompts. To restore a previous configuration, click Browse and use the navigation window to locate the local backup file. The default filename is in the format MM_DD_YYYY.gwc. Note that this file is encrypted. When the file has been located, click Restore to restore the settings. When the settings are restored, the device will reboot to the restored settings.

10.4.1 User Provisioning for Backup & Restore

Administration Tab / Backup & Restore
Click on the Administration tab and then the Backup & Restore tab. This page displays Backup & Restore setup information.

The user can back up the configuration data to a specific file or restore the already backed up data from a file.



Back Up

Password

Confirm Password

Restore

Password

Please choose a file

Figure 10.4

10.4.2 SNMP Provisioning for Backup & Restore

tchRgDeviceConfigBackup MIB set is used for this**.**
tchRgDevConfBackupServerType defined as IPv4 for future usage.
tchRgDevConfBackupServer - The address of the TFTP server used for Wireless Gateway config download or upload. If the TFTP server is unknown, return 0.0.0.0.
tchRgDevConfBackupOperStatus InProgress(1) indicates that a TFTP download or upload is underway, Complete(2) indicates that the last download or upload is successful, failed(3) indicates that the last attempted download or upload is failed.
tchRgDevConfBackupAdminStatus. If set to download(1), the device will initiate a TFTP Wireless Gateway config file download using remoteProvisionFilename. If set to upload(2), the device will initiate a TFTP Wireless Gateway config file upload to remoteProvisionServer. The filename will be the same as remoteProvisionFilename. At initial start-up, this object has the default value of download(1).

10.5 Reboot & Reset

Administration Tab / Reboot & Reset
Click on the Administration tab and then the Reboot & Reset tab. The page displays Reboot and Reset options:

Reboot

- Reboot Wi-Fi module
- Reboot Wi-Fi Router
- Reboot System

Reset

- Reset User Name & Password
- Reset Wi-Fi Setting
- Reset Factory Settings.

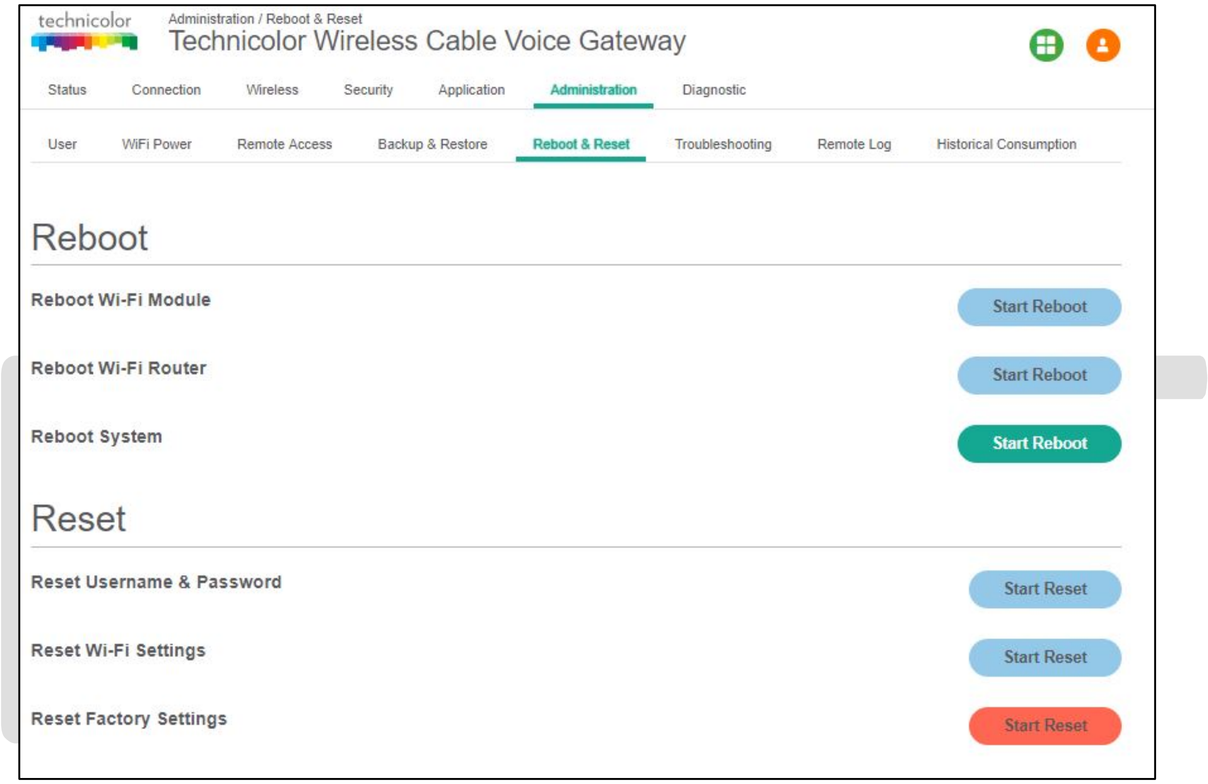


Figure 10.5

User can Reboot and Reset the settings by selecting the corresponding button.

10.5.1 SNMP Provisioning for Factory Settings

This will be controlled by the MIB **tchcmAPFactoryReset**. It can be set with a sequence of values to activate a remote factory reset. This is the same as a sustained (3 seconds or more) reset switch. Reading this object always returns false (2).

10.6 Restarting the Device

It is possible to restart the Gateway from WebUI. This can be done from Administration -> Reboot & Reset Tab, by clicking on the Reboot System option.

10.6.1 SNMP Provisioning for Restarting the Device

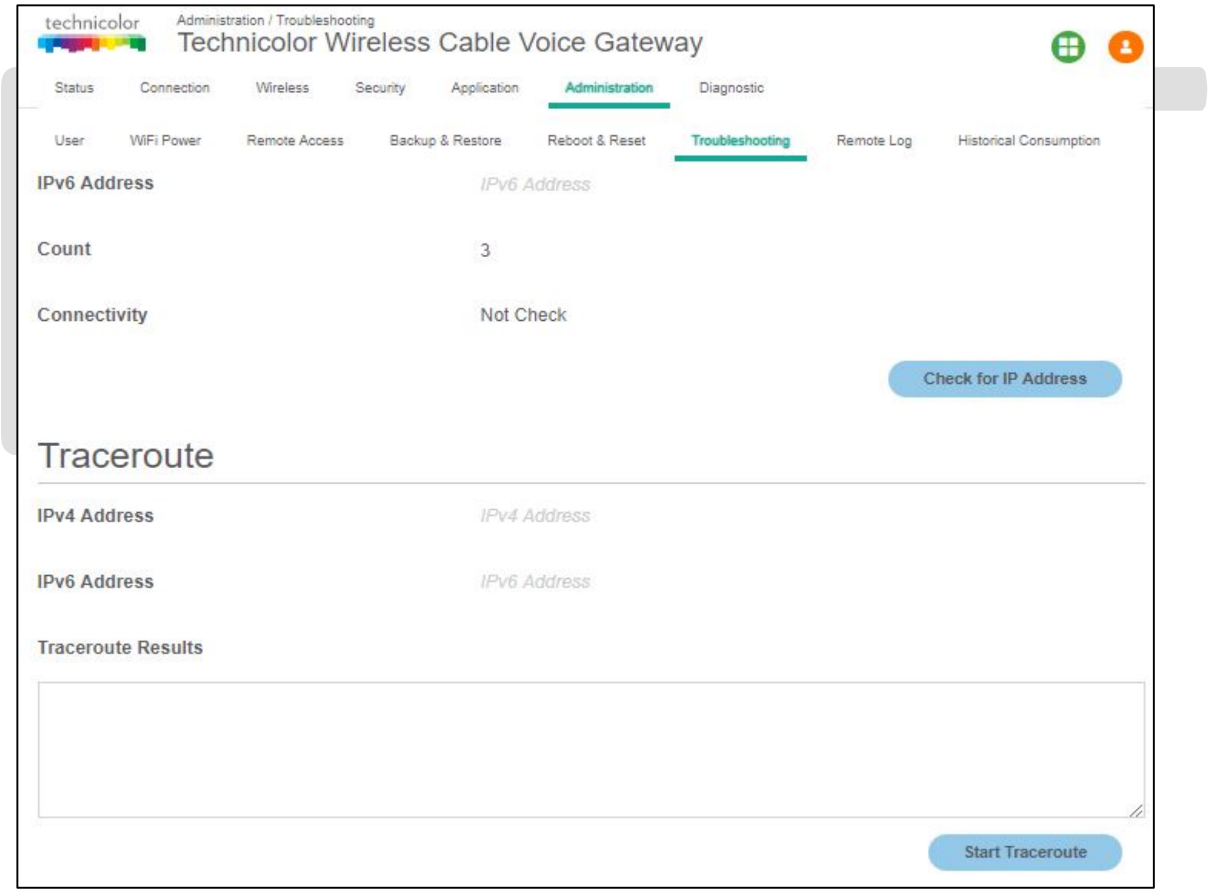
This will be controlled by

- **tchRgDeviceFactoryReset** -This MIB is used for performing a Factory Reset on the device
- **tchRgDeviceReset** - This MIB is used to restart the device

10.7 Trouble Shooting

Ping and Traceroute are the trouble shooting features available in the Troubleshooting options. This can be done for both the IPv4 and IPv6 networks.

Administration / Trouble Shooting
Click on the Administration tab then click on the Trouble Shooting tab. The page provides views for running ping (to check the network connectivity to a particular IPv4 or IPv6 address) and traceroot (for displaying the route/path and measuring transit delays of packets across the network.



IPv6 Address: IPv6 Address

Count: 3

Connectivity: Not Check

Traceroute

IPv4 Address: IPv4 Address

IPv6 Address: IPv6 Address

Traceroute Results

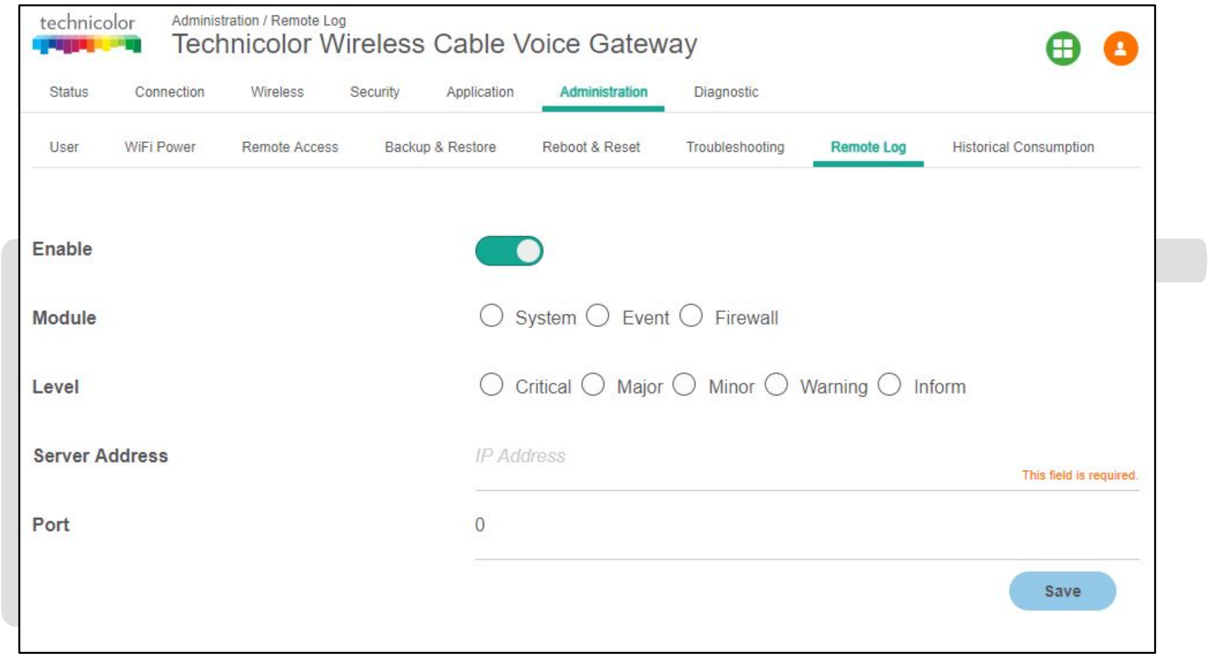
Figure 10.6

10.8 Remote Log

Remote Log view provides an option to add a log server and specify the kind of logs (including log levels) needed for any particular troubleshooting.

Administration / Remote Log
Click on the Administration tab then click on the Remote Log tab. The current logging configurations – module & log levels – would be displayed.

The User can modify the modules (System, Event, and Firewall) for logging and the log levels (Critical, Major, Minor, Warning and Inform) to be logged and save the configuration for future logging. The logging server details also need to be entered.



Enable	●
Module	○ System ○ Event ○ Firewall
Level	○ Critical ○ Major ○ Minor ○ Warning ○ Inform
Server Address	IP Address This field is required.
Port	0

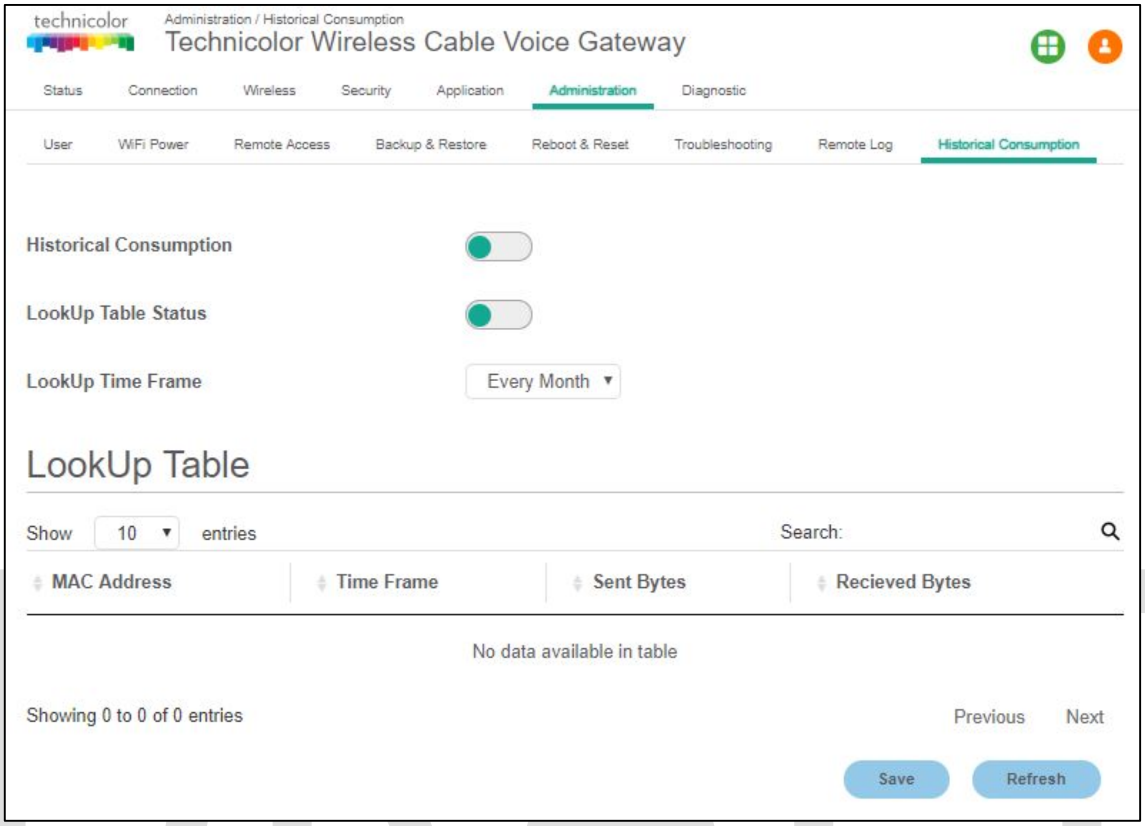
Figure 10.7

10.9 Historical Consumption

The Administration / Historical Consumption page provides the data consumption statistics on hour/day/monthly basis i.e. as selected against the Lookup Time Frame tab.

Administration / Historical Consumption
Click on the Administration tab then click on the Historical Consumption tab. The page displays the various options to configure the feature.

Once the feature is configured, against each of the devices (MAC Address), the LookUp Table displays the send and received bytes for the period configured as Lookup Time Frame. The User has to enable both the Historical Consumption option and the LookUp Table Status option to get this statistics. The Lookup Time Frame can be configured for every hour, every day or every month.



Historical Consumption ●

LookUp Table Status ●

LookUp Time Frame: Every Month ▾

LookUp Table

Show 10 ▾ entries

Search:

MAC Address	Time Frame	Sent Bytes	Recieved Bytes
No data available in table			

Showing 0 to 0 of 0 entries

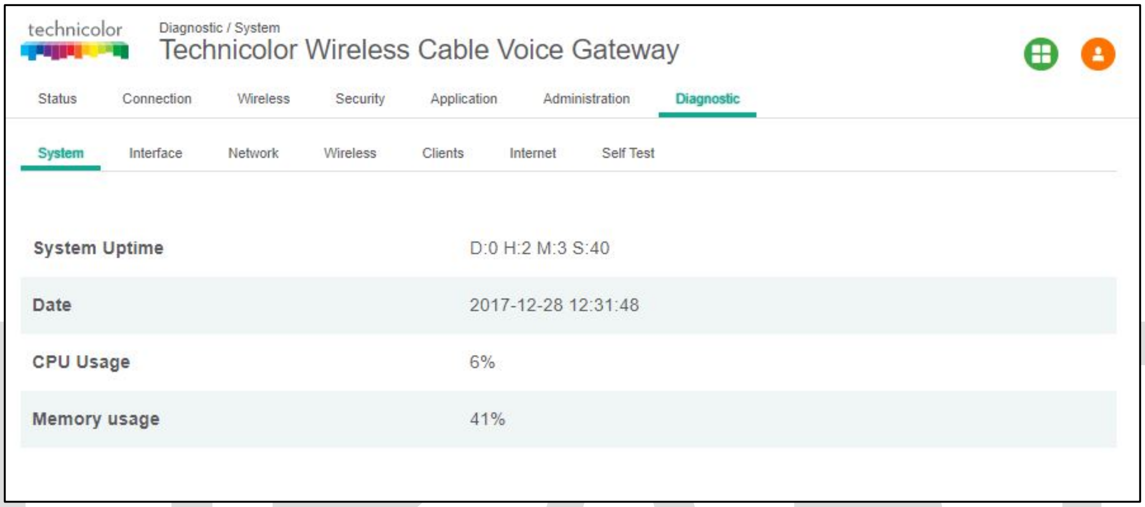
Figure 10.8

11 Diagnostics

This section provides details about the various diagnostic features built in CGM4231.

11.1 System

This page displays the System status details. The details shown are System Up-time, Resource usage such as CPU and memory.

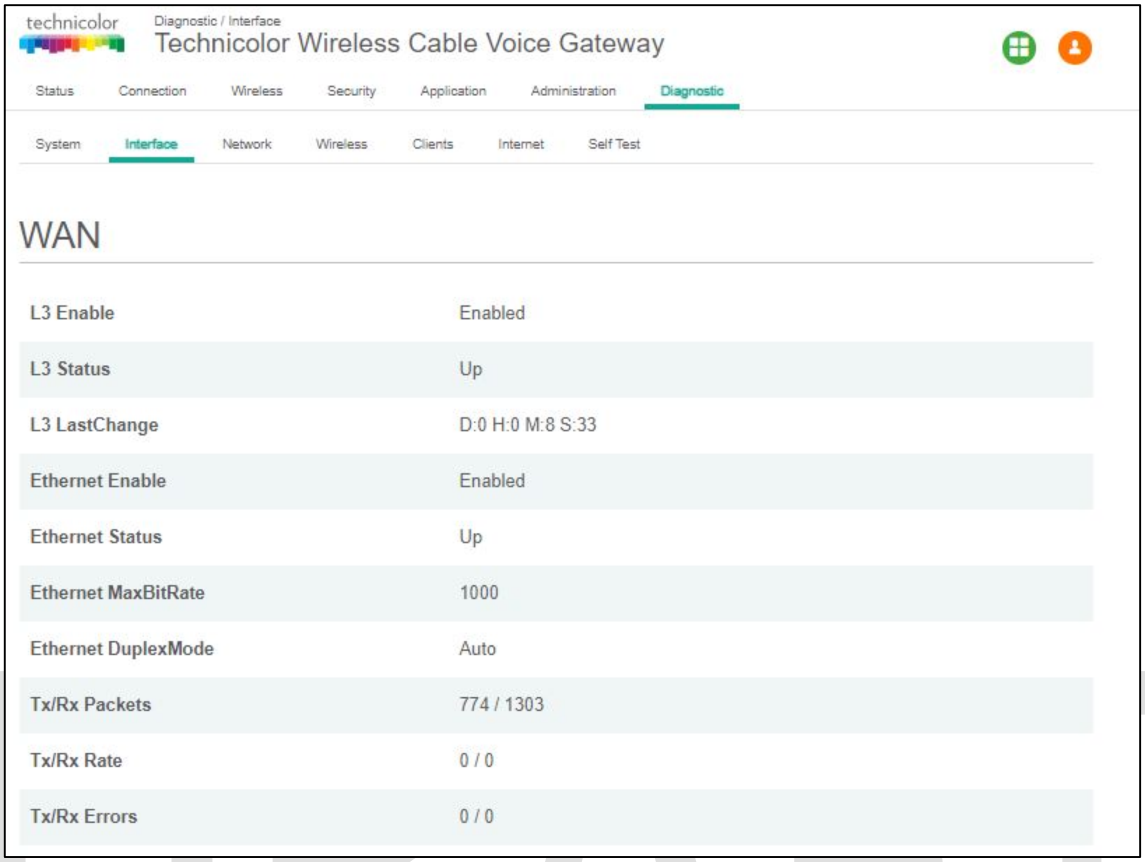


System Uptime	D:0 H:2 M:3 S:40
Date	2017-12-28 12:31:48
CPU Usage	6%
Memory usage	41%

Figure 11.1

11.2 Interface

Diagnostic Tab / Interface
This page displays the up/down status, various configurations, data traffic and error information for various interfaces in the system (WAN, LAN and Wi Fi). The figures below provide specific screenshots for each of these interfaces:

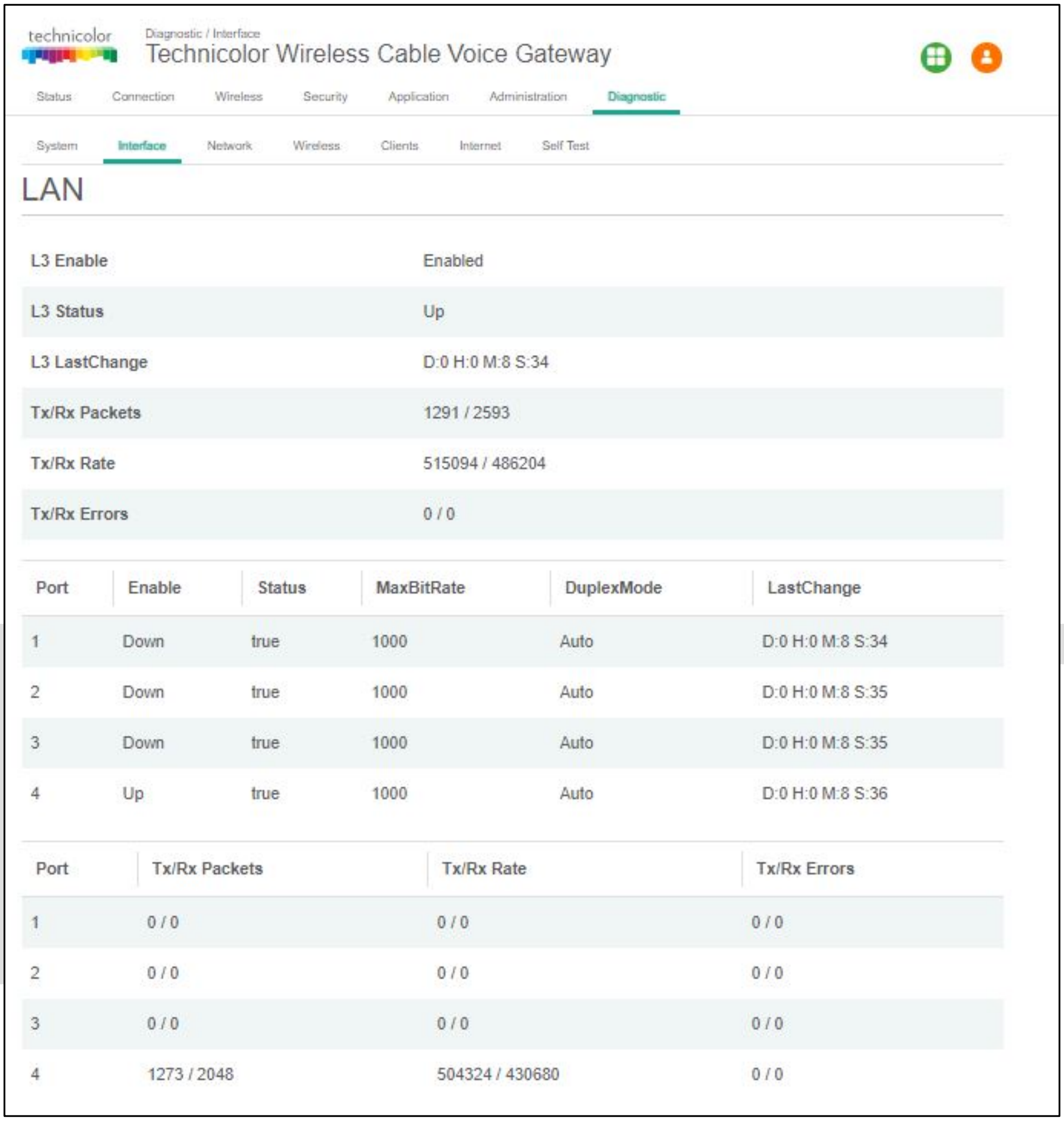


Technicolor Wireless Cable Voice Gateway

WAN

L3 Enable	Enabled
L3 Status	Up
L3 LastChange	D:0 H:0 M:8 S:33
Ethernet Enable	Enabled
Ethernet Status	Up
Ethernet MaxBitRate	1000
Ethernet DuplexMode	Auto
Tx/Rx Packets	774 / 1303
Tx/Rx Rate	0 / 0
Tx/Rx Errors	0 / 0

Figure 11.2



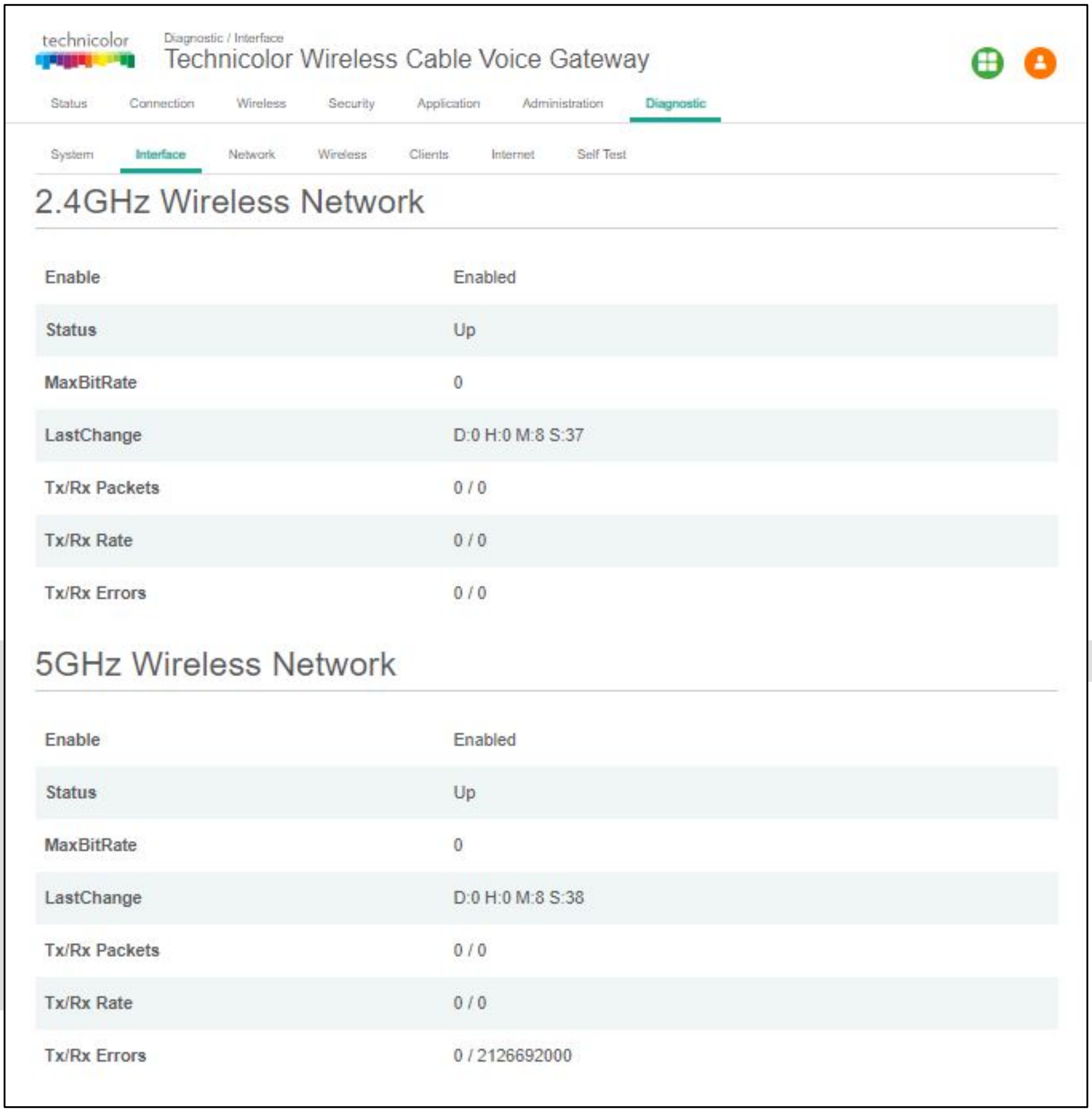
LAN

L3 Enable	Enabled
L3 Status	Up
L3 LastChange	D:0 H:0 M:8 S:34
Tx/Rx Packets	1291 / 2593
Tx/Rx Rate	515094 / 486204
Tx/Rx Errors	0 / 0

Port	Enable	Status	MaxBitRate	DuplexMode	LastChange
1	Down	true	1000	Auto	D:0 H:0 M:8 S:34
2	Down	true	1000	Auto	D:0 H:0 M:8 S:35
3	Down	true	1000	Auto	D:0 H:0 M:8 S:35
4	Up	true	1000	Auto	D:0 H:0 M:8 S:36

Port	Tx/Rx Packets	Tx/Rx Rate	Tx/Rx Errors
1	0 / 0	0 / 0	0 / 0
2	0 / 0	0 / 0	0 / 0
3	0 / 0	0 / 0	0 / 0
4	1273 / 2048	504324 / 430680	0 / 0

Figure 11.3



2.4GHz Wireless Network

Enable	Enabled
Status	Up
MaxBitRate	0
LastChange	D:0 H:0 M:8 S:37
Tx/Rx Packets	0 / 0
Tx/Rx Rate	0 / 0
Tx/Rx Errors	0 / 0

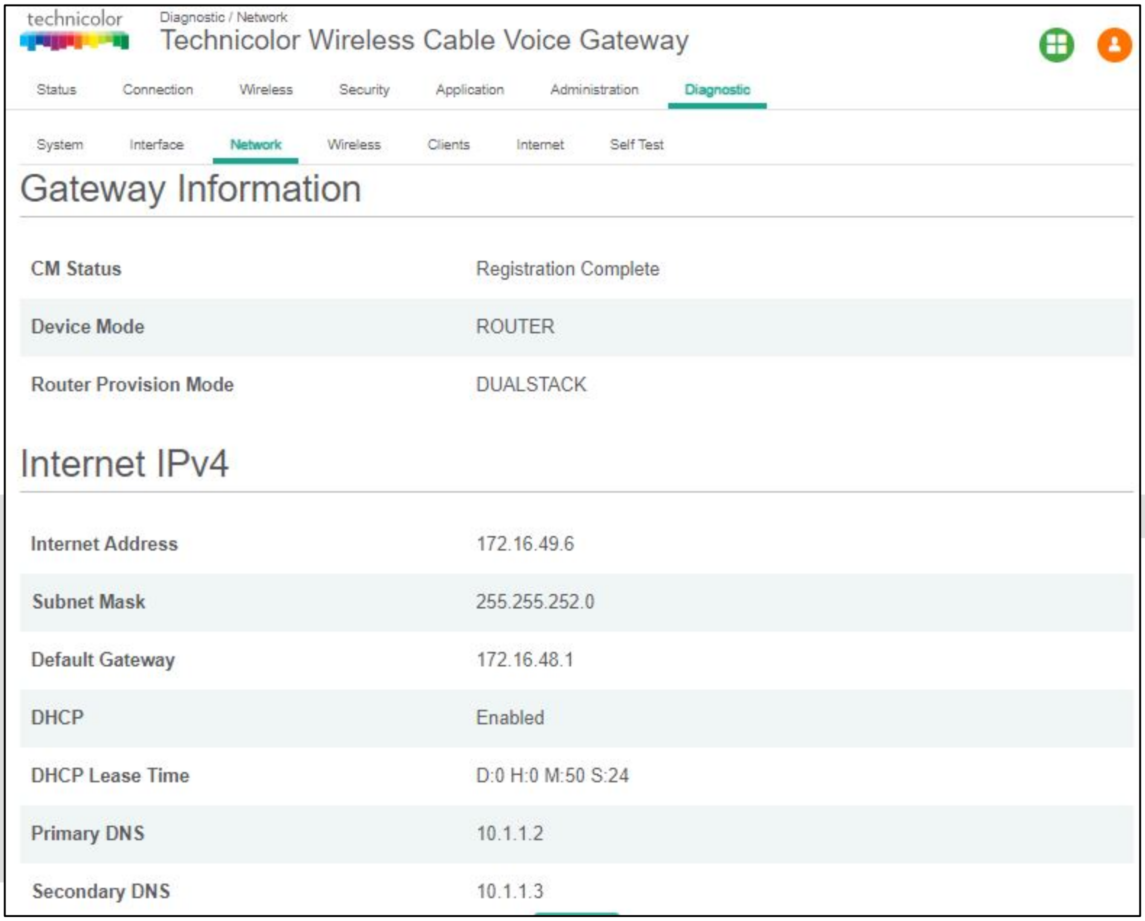
5GHz Wireless Network

Enable	Enabled
Status	Up
MaxBitRate	0
LastChange	D:0 H:0 M:8 S:38
Tx/Rx Packets	0 / 0
Tx/Rx Rate	0 / 0
Tx/Rx Errors	0 / 2126692000

Figure 11.4

11.3 Network

This section provides the gateway information, LAN network data for IPv4 and IPv6 networks. The figures mainly provide the configuration status for LAN side configurations.



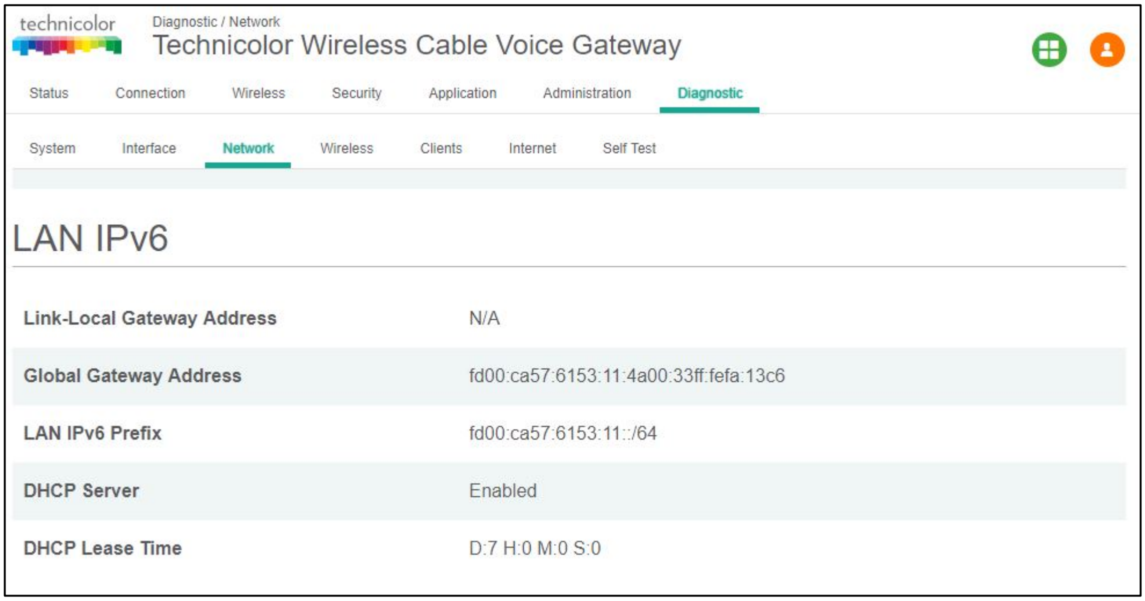
Gateway Information

CM Status	Registration Complete
Device Mode	ROUTER
Router Provision Mode	DUALSTACK

Internet IPv4

Internet Address	172.16.49.6
Subnet Mask	255.255.252.0
Default Gateway	172.16.48.1
DHCP	Enabled
DHCP Lease Time	D:0 H:0 M:50 S:24
Primary DNS	10.1.1.2
Secondary DNS	10.1.1.3

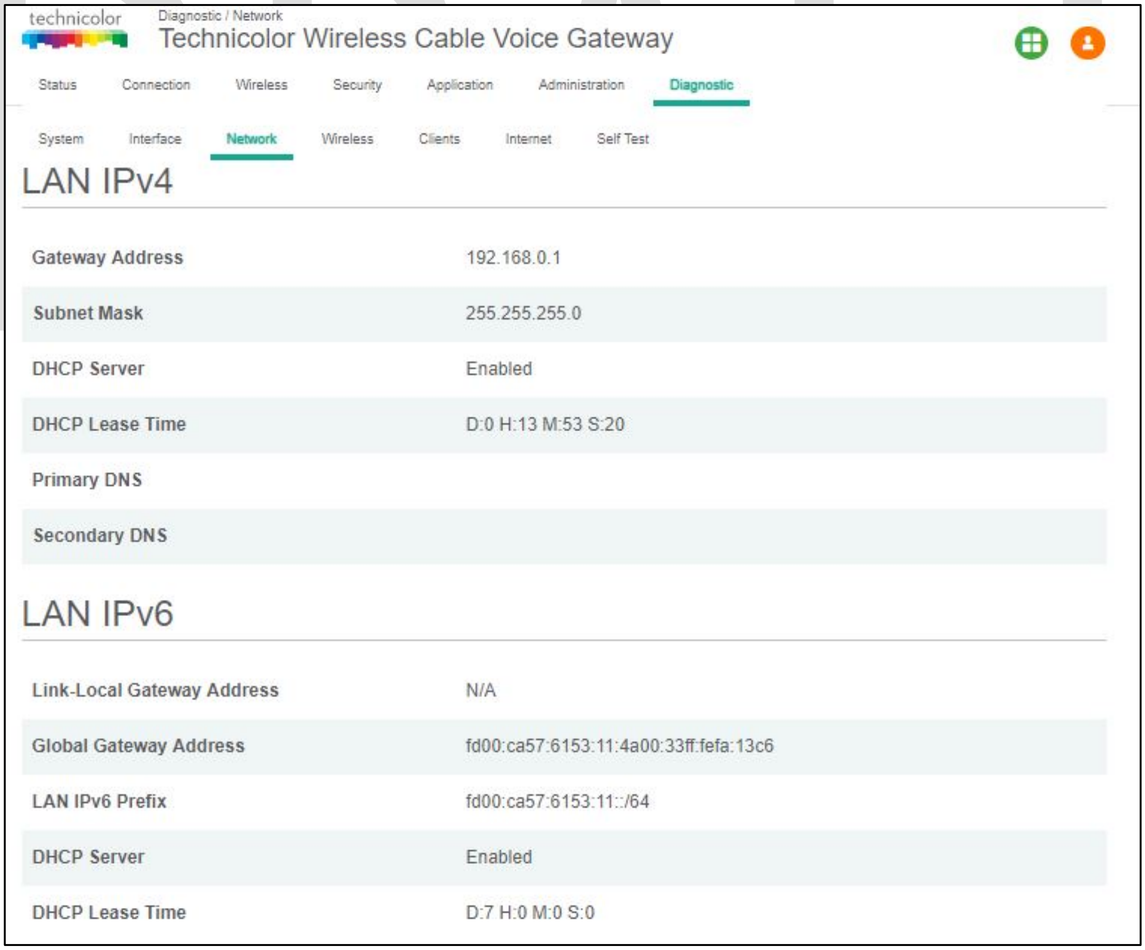
Figure 11.5



LAN IPv6

Link-Local Gateway Address	N/A
Global Gateway Address	fd00:ca57:6153:11:4a00:33ff:fefa:13c6
LAN IPv6 Prefix	fd00:ca57:6153:11::/64
DHCP Server	Enabled
DHCP Lease Time	D:7 H:0 M:0 S:0

Figure 11.6



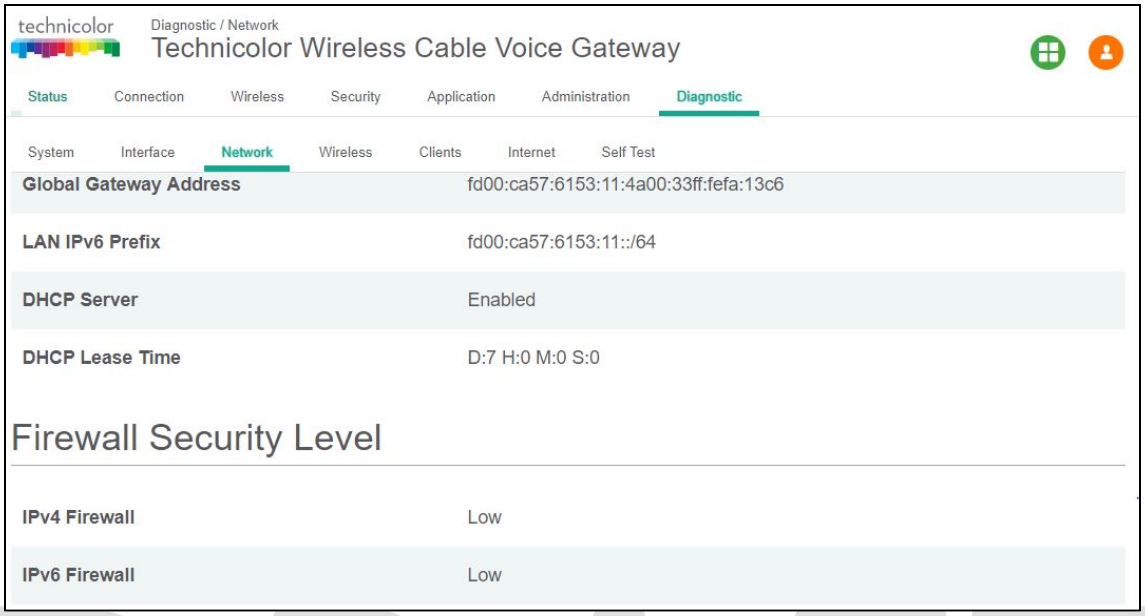
LAN IPv4

Gateway Address	192.168.0.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled
DHCP Lease Time	D:0 H:13 M:53 S:20
Primary DNS	
Secondary DNS	

LAN IPv6

Link-Local Gateway Address	N/A
Global Gateway Address	fd00:ca57:6153:11:4a00:33ff:fefa:13c6
LAN IPv6 Prefix	fd00:ca57:6153:11::/64
DHCP Server	Enabled
DHCP Lease Time	D:7 H:0 M:0 S:0

Figure 11.7



Technicolor Wireless Cable Voice Gateway

Global Gateway Address	fd00:ca57:6153:11:4a00:33ff:fefa:13c6
LAN IPv6 Prefix	fd00:ca57:6153:11::/64
DHCP Server	Enabled
DHCP Lease Time	D:7 H:0 M:0 S:0

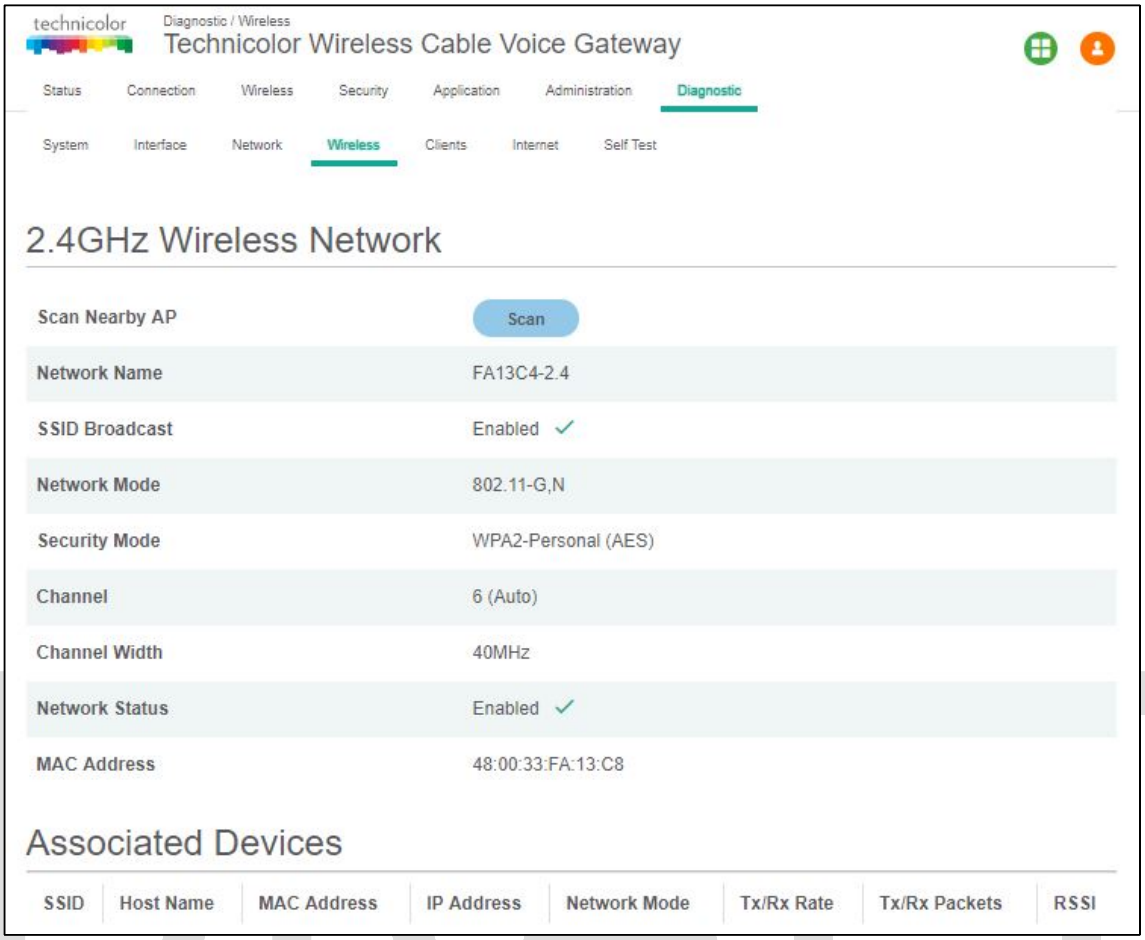
Firewall Security Level

IPv4 Firewall	Low
IPv6 Firewall	Low

Figure 11.8

11.4 Wireless

This section provides the Wi Fi network data for 2.4GHz and 5 GHz networks. The figure provides configuration information such as Network Name, Wi Fi MAC address, network mode, channel bandwidth, channel numbers, security mode, and SSID broadcast status (enabled/disabled).



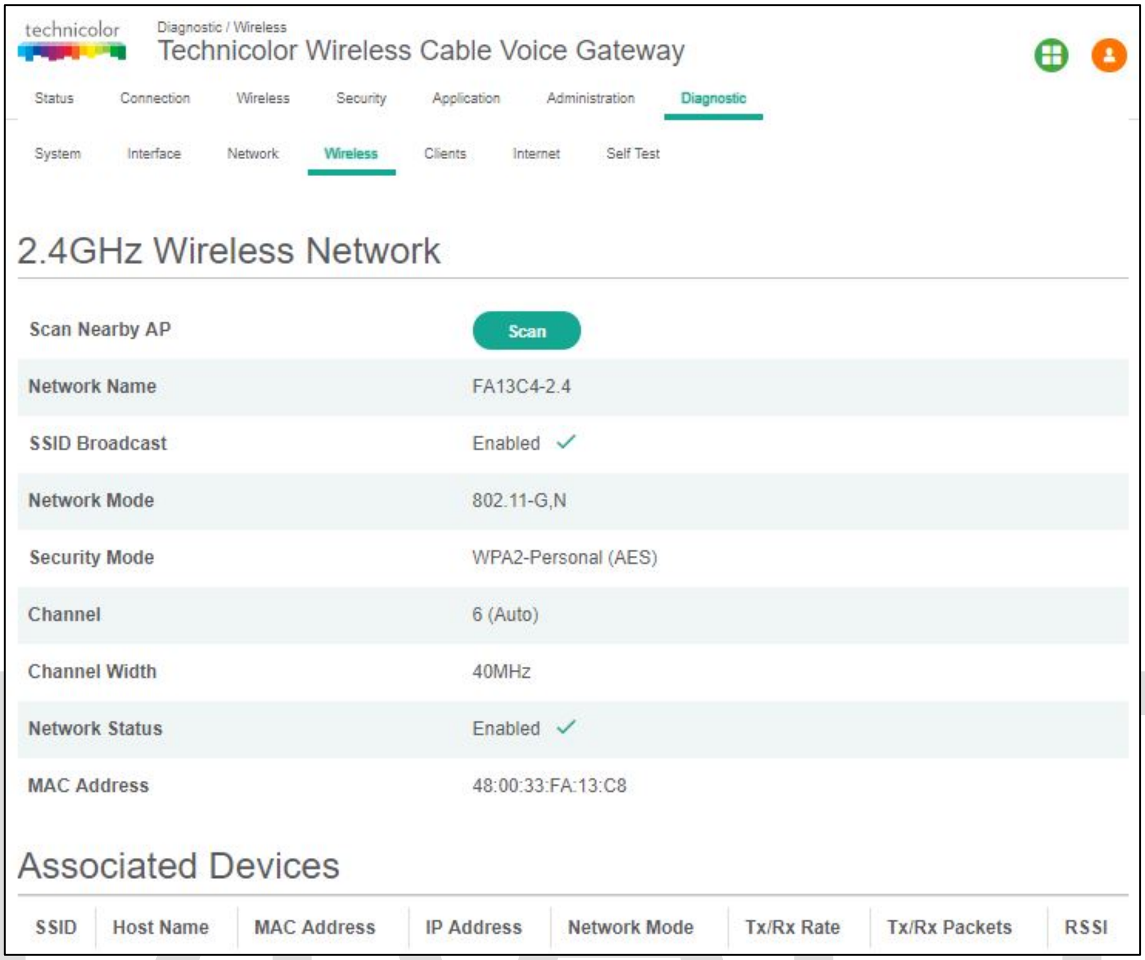
2.4GHz Wireless Network

Scan Nearby AP	Scan
Network Name	FA13C4-2.4
SSID Broadcast	Enabled ✓
Network Mode	802.11-G,N
Security Mode	WPA2-Personal (AES)
Channel	6 (Auto)
Channel Width	40MHz
Network Status	Enabled ✓
MAC Address	48:00:33:FA:13:C8

Associated Devices

SSID	Host Name	MAC Address	IP Address	Network Mode	Tx/Rx Rate	Tx/Rx Packets	RSSI

Figure 11.9



Technicolor Wireless Cable Voice Gateway

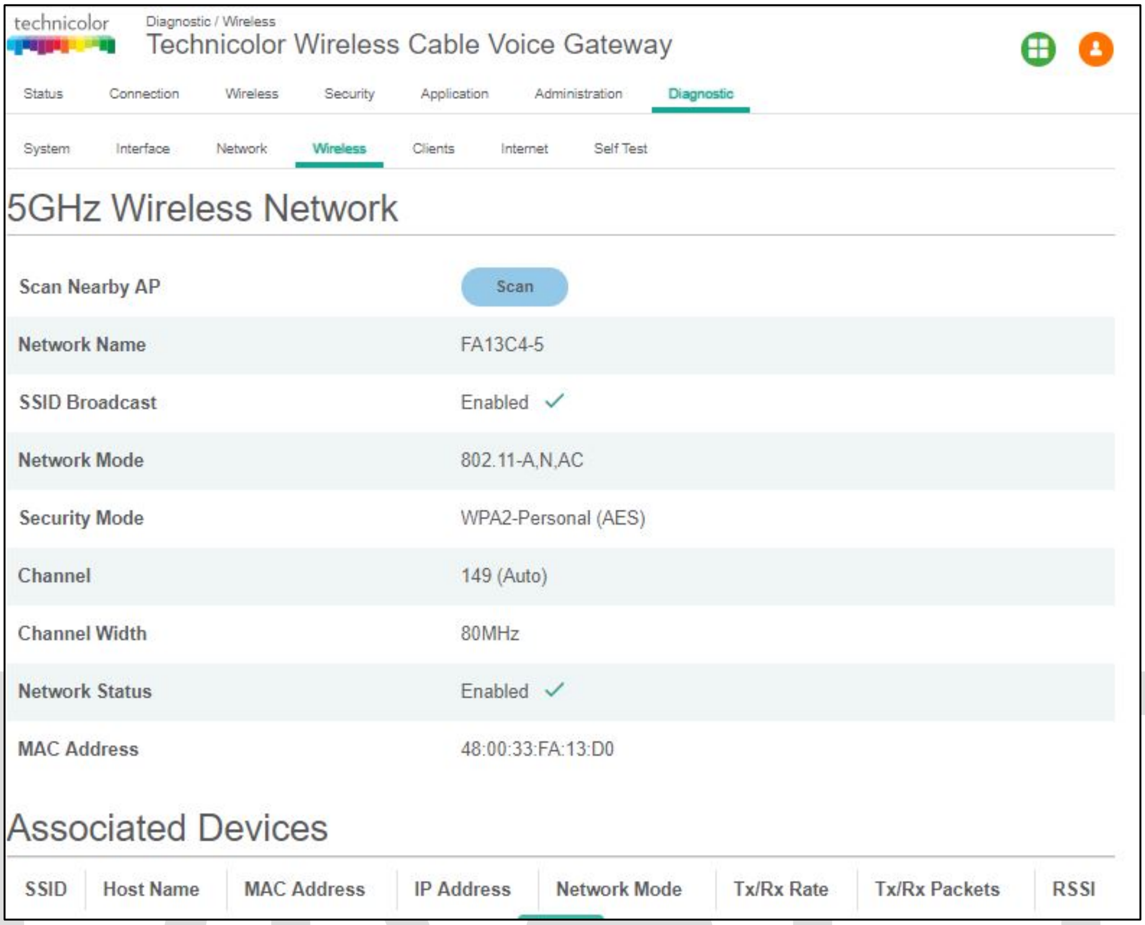
2.4GHz Wireless Network

Scan Nearby AP	Scan
Network Name	FA13C4-2.4
SSID Broadcast	Enabled ✓
Network Mode	802.11-G,N
Security Mode	WPA2-Personal (AES)
Channel	6 (Auto)
Channel Width	40MHz
Network Status	Enabled ✓
MAC Address	48:00:33:FA:13:C8

Associated Devices

SSID	Host Name	MAC Address	IP Address	Network Mode	Tx/Rx Rate	Tx/Rx Packets	RSSI

Figure 11.10



5GHz Wireless Network

Scan Nearby AP	Scan
Network Name	FA13C4-5
SSID Broadcast	Enabled ✓
Network Mode	802.11-A,N,AC
Security Mode	WPA2-Personal (AES)
Channel	149 (Auto)
Channel Width	80MHz
Network Status	Enabled ✓
MAC Address	48:00:33:FA:13:D0

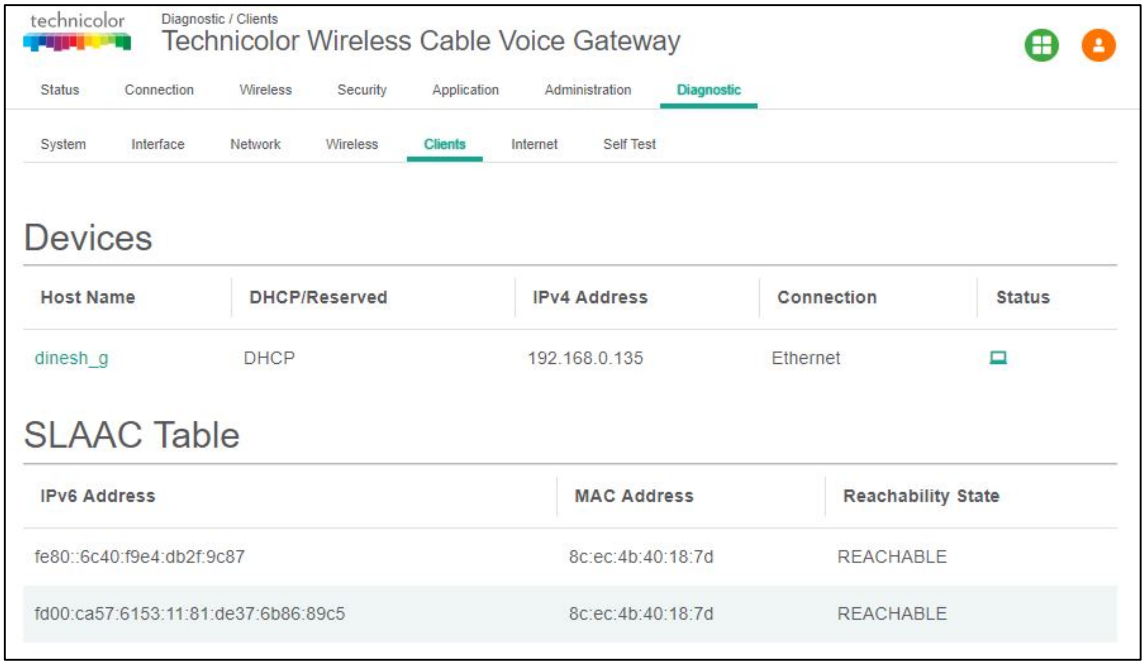
Associated Devices

SSID	Host Name	MAC Address	IP Address	Network Mode	Tx/Rx Rate	Tx/Rx Packets	RSSI

Figure 11.11

11.5 Clients

This page provides data for different clients (LAN and Wi Fi) connected to the gateway and the details of the network connectivity (IP address, DHCP status, LAN/Wi Fi and Status) of the clients connected.



Devices

Host Name	DHCP/Reserved	IPv4 Address	Connection	Status
dinesh_g	DHCP	192.168.0.135	Ethernet	💻

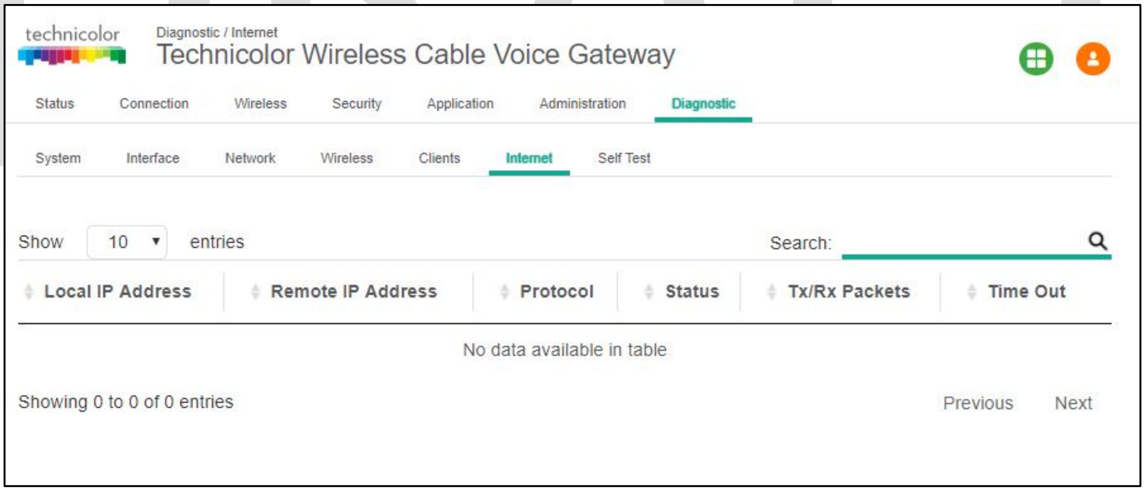
SLAAC Table

IPv6 Address	MAC Address	Reachability State
fe80::6c40:f9e4:db2f:9c87	8c:ec:4b:40:18:7d	REACHABLE
fd00:ca57:6153:11:81:de37:6b86:89c5	8c:ec:4b:40:18:7d	REACHABLE

Figure 11.12

11.6 Internet

This page provides the data traffic information (Protocol, Tx / Rx packet information, IP timeouts, etc.) for the LAN clients with remote internet access.



Show 10 ▾ entries Search:

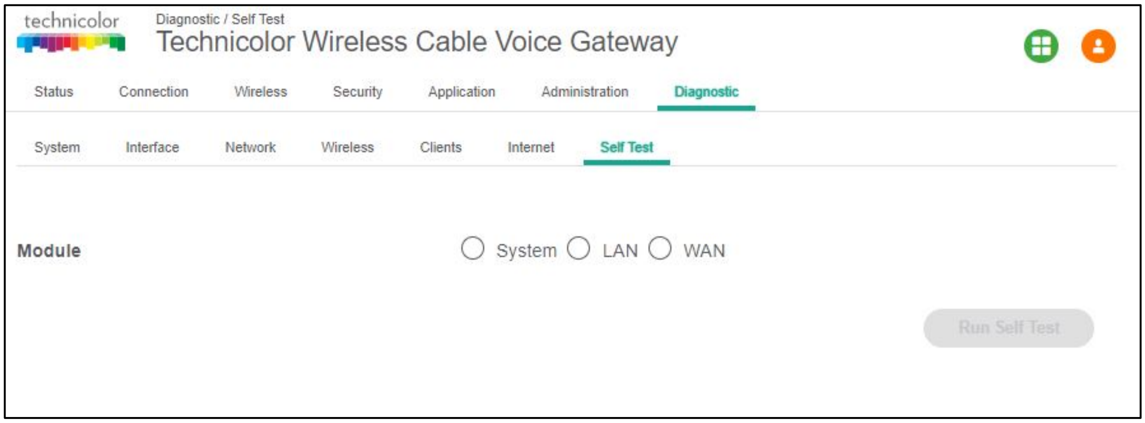
Local IP Address	Remote IP Address	Protocol	Status	Tx/Rx Packets	Time Out
No data available in table					

Showing 0 to 0 of 0 entries

Figure 11.13

11.7 Self Test

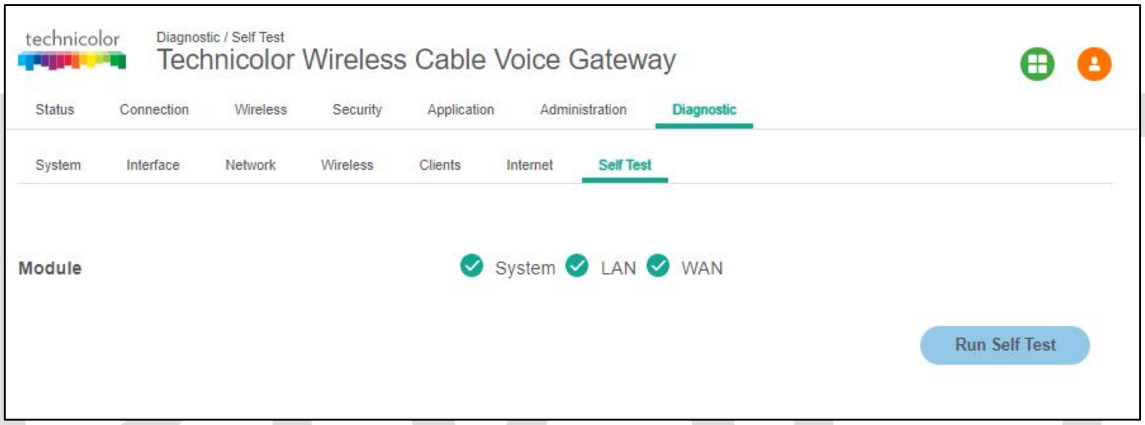
This page provides an option to run self tests for System, LAN and WAN modules. The page appears populated with the information below:



Module ○ System ○ LAN ○ WAN

Figure 11.14

User can run self test by selecting the module and clicking on Run Self-Test button Shown below:



Module ✓ System ✓ LAN ✓ WAN

Figure 11.15

12 Isolation

By default, the Technicolor Wireless Gateway allows traffic to pass freely between CPE devices on the same logical network. This behavior may not be desirable in certain types of deployments where devices associating with the Wireless Gateway may belong to different persons/households (examples: public hotspots, hotels, and multi-dwelling units). For these deployments, the appropriate isolation modes should be enabled. This feature causes the Wireless Gateway to block traffic sent between CPE devices.

12.1 User Provisioning for Isolation

No user provisioning is available for this feature. This feature must be provisioned by the operator using SNMP.

12.2 SNMP Provisioning for Isolation

Isolation can be configured separately for any, and all of the following types of traffic:

- Traffic in which both the source and destination addresses are reachable via the same primary or secondary BSSID (WLAN-WLAN traffic)

Isolation for WLAN-WLAN traffic:
Isolation for WLAN-WLAN traffic is controlled via the ***tchRgDot11BssApIsolation*** MIB object. This is an interface-specific MIB which must be appended with the appropriate interface index of the BSSID that is being configured for isolation.

Index	Interface
32	**Primary BSSID**
33	**Secondary BSSID #1**
34	**Secondary BSSID #2**
35	**Secondary BSSID #3**
36	**Secondary BSSID #4**
37	**Secondary BSSID #5**
38	**Secondary BSSID #6**
39	**Secondary BSSID #7**

This means that different BSSIDs may have different isolation settings. For example, it is possible to leave isolation disabled on the primary BSSID, while setting up a secondary BSSID for hotspot services that has isolation enabled.

The default setting for this MIB is integer 0 (disabled) for all SSIDs. To enable WLAN-WLAN traffic isolation, set this MIB to 1 (enabled).

This setting is effective in the device configuration file as well as when set via SNMP (If set via SNMP, the setting will persist across device reboots). If SNMP is used, setting ***tchRgDot11ApplySettings*** to true (1) is required for the change to take effect (as is the case with other ***tchRgDot11*** MIB settings when set via SNMP).

Example:

To provision complete isolation between Ethernet ports and the primary SSID, The following would be added to the CM config file:

```
SnmpMibObjecttchRgDeviceLanLanIsolation.0 Integer 1; /* enable */

SnmpMibObjecttchRgDeviceLanWlanIsolation.0 Integer 1; /* enable */

SnmpMibObjecttchRgDot11BssApIsolation.32 Integer 1; /* enable */
```

13 TR-069

TR-069 (Technical Report 069) is a method to remotely and securely manage CPE configuration from a central Auto Configuration Server or ACS. The following figure shows a simple and typical deployment layout. The ACS simply needs to be network accessible by the eRouter interface.

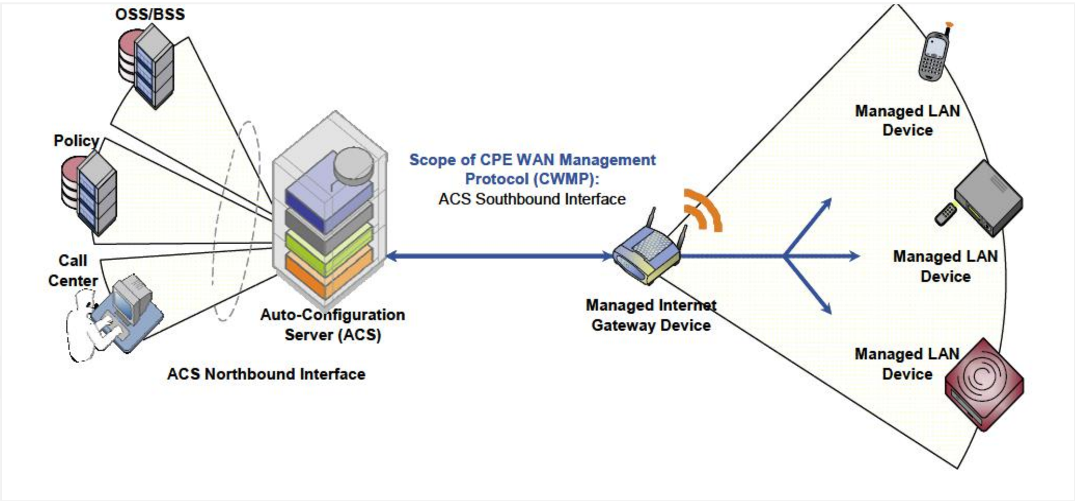


Figure 13.1

To configure TR-069, tchTR069ClientMode should be set to enable (1) and tchTR069ClientAcsUrl should point to the ACS server (e.g. http://myacs.acs.lab.sa). tchTR069ClientAllowDocsisConfig must be set to enable (1) to reconfigure any TR-069 parameters including the ACS URL above.

During the initial device check-in and configuration with the ACS, the server will populate the tchTR069ClientCrUsername and tchTR069ClientCrPassword fields. The client device identifier can also be set as either MAC or serial number when registering to the ACS server.

13.1 User Provisioning for TR-069

The user does not configure TR-069 as it is meant for remote management by the service operator from the auto configuration server.

13.2 SNMP Provisioning for TR-069

tchTR069ClientModeshould be set to enable (1) (TR-069 is disabled by default).

tchTR069ClientAcsUrlshould be set to the ACS IP address or FQDN.

tchTR069ClientAllowDocsisConfigshould be set to enable (1) for TR-69 to be reconfigured(this MIB is enabled by default).

tchTR069ClientAcsUsername –user name for ACS association

tchTR069ClientAcsPassword –password for ACS association

Optional configuration MIBs are:

tchTR069ClientPeriodicInformto enable inform messages to be sent back to the ACS periodically, refreshing the device data (this MIB is enabled by default)

tchTR069ClientPeriodicInformIntervalto set the time interval between inform messages in seconds (3600, or one hour by default).

14 Appendix1: Web User Interface Control

MSO administrators can control the display/modification of certain WebUI pages / sections / fields by enabling the appropriate bits in the **tchCmWebAccessReadPages** and **tchCMWebAccessWritePages**. The table below explains what is controlled by each bit:

Bitmap	Top tab	Bottom tab	Section	Field(s)/Pop-ups
bridgeRouterMode(0)	Administration	Management	Gateway Setup(WAN)	Working Mode

docsisSignal(1)
docsisStatus(2)
	Status
	Status
		DOCSIS Signal
		DOCSIS Status		

docsisLog(3)	Status	DOCSIS Signal		
timeUseNtp(4) *	Setup	LAN Setup	Network Setup (LAN)	NTP Enable
timeZone(5)	Setup	LAN Setup	Network Setup (LAN)	Time Zone Daylight Saving Time
timeDst(6)	Setup	LAN Setup	Network Setup (LAN)	Automatically adjust DST
timeServer(7)*	Setup	LAN Setup	Network Setup (LAN)	
lanIp(8)	Setup	LAN Setup	LAN Gateway IP	Local IP Address Subnet Mask
lanDhcpEnable(9)	Setup	LAN Setup	Network Setup (LAN)	DHCP Server
lanDhcpScope(10)	Setup	LAN Setup	Network Setup (LAN)	Starting IP Address Maximum Number of DHCP Users
lanDhcpLeaseTime(11)	Setup	LAN Setup	Network Setup (LAN)	Client Lease Time
lanDhcpDns(12)	Setup	LAN Setup	Network Setup (LAN)	LAN 1 Static DNS 1 LAN 1 Static DNS 2 LAN 1 Static DNS 3

Bitmap	Top tab	Bottom tab	Section	Field(s)/Pop-ups
lanDhcpWins(13)+				
lanFixedCpe(14)	Setup	LAN Setup	Network Setup (LAN)	Connected Device Summary Pre-assigned DHCP IP Addresses Also the associated pop-ups
wanStaticIp(15)	Administration	Management	Gateway Setup(WAN)	Internet IP address Subnet Mask Default Gateway (When Static IP is selected as Connection Mode)
wanDns(16)	Administration	Management	Gateway Setup(WAN)	Primary DNS Secondary DNS (When Static IP is selected as Connection Mode)
wanMtu(17)	Administration	Management	Gateway Setup(WAN)	MTU
wanHostDomainNames (18)	Administration	Management	Gateway Setup(WAN)	Host Name Domain Name (When Static IP is selected as Connection Mode)
resetModem(19)+	Administration	Device Restart		
resetFactoryDefaults(20)	Administration	Factory Defaults		
backupConfigToPc(21)+	Administration	Backup and Restore		
ddns(22)	Setup	DDNS		

Bitmap	Top tab	Bottom tab	Section	Field(s)/Pop-ups
wanBlocking(23)	Security	Firewall	Block WAN Requests	Block Anonymous Internet Requests
ipsecPassthrough(24)	Security	VPN Passthrough		IP Sec Passthrough
pptpPassthrough(25)	Security	VPN Passthrough		PPTP Passthrough
remoteManagement(26)	Administration	Management	Gateway Access	Remote Management Management Port
upnpEnable(28)	Administration	Management	UPnP	UPnP
ipFiltering(29)	Access Restrictions	IP Filter		
macFiltering(30)	Access Restrictions	MAC Address Filter		
portFiltering(31)	Applications and Gaming	Port Filter		
portForwarding(32)	Applications and Gaming	Port Range Forwarding		
portTriggers(33)	Applications and Gaming	Port Range Triggering		
dmz(34)	Applications and Gaming	DMZ		
vpnTermination(35)	Security	VPN		
staticRoute(36)+	Connection	WAN		

Bitmap	Top tab	Bottom tab	Section	Field(s)/Pop-ups
portScanDetection(43)	Security	Firewall	Filters	Block Port Scan Detection
ipFloodDetection(44)	Security	Firewall	Filters	Block IP Flood Detection
firewallProtection(45)	Security	Firewall	Firewall	SPI Firewall Protection
firewallEventLogging(46)+	Administration	Reporting		
parentalControl(47)	Access Restriction	Basic Rules Time of Day Rules User Setup Local Log		
wireless2p4SSID(48)	Wireless	Radio Settings	Basic Settings	Radio Band
wireless2p4ABGNMode(49)	Wireless	Radio Settings	Basic Settings	Network Mode
wireless2p4SSID(50)	Setup Wireless	Quick Setup Radio Settings	Wireless Network	Network Name (SSID) Network Name (SSID)
wireless2p4BroadcastSSID(51)	Wireless	Radio Settings		Broadcast SSID
wireless2p4Channel(52)	Wireless	Radio Settings		Standard Channel
wireless2p4ChannelWidth(53)	Wireless	Radio Settings		Channel Width
wireless2p4Security(54)	Wireless	Wireless Security		
wireless2p4Wps(55)	Wireless	WPS		all fields
wireless2p4Advanced(56)	Wireless	Advanced Settings		all fields
wireless2p4AccessControl(57) +	Wireless	MAC Control		all fields
wireless2p4Bridging(58) +	Wireless			
wireless2p4Wmm(59)	Wireless	QoS	Quality of Service	WMM Support
wireless2p4AckEnable(60)	Wireless	QoS	Quality of Service	No ACK

Bitmap	Top tab	Bottom tab	Section	Field(s)/Pop-ups
wireless5Enable(61)**				
wireless5ABGNMode(62) **	Wireless	Radio Settings		Network Mode
wireless5SSID(63) **	Setup Wireless	Quick Setup Radio Settings	Wireless Network	Network Name (SSID) Network Name (SSID)
wireless5BroadcastSSID(64) **	Wireless	Radio Settings		SSID Broadcast
wireless5Channel(65) **	Wireless	Radio Settings		Channel
wireless5ChannelWidth(66) **	Wireless	Radio Settings		Channel Width
wireless5Security(67) **	Wireless	Wireless Security		All fields
wireless5Wps(68) **	Wireless	WPS		all fields
wireless5Advanced(69) **	Wireless	Advanced Settings		All fields
wireless5AccessControl(70) ** +	Wireless	MAC Control		All fields
wireless5Bridging(71) ** +	Wireless			
wreless5Wmm(72) **	Wireless	QoS	Quality of Service	WMM Support
wireless5AckEnable(73) **	Wireless	QoS	Quality of Service	No ACK
ping(74)	Administration	Diagnostics		
igmpProxy(75)	Administration	Management	IGMP Proxy	IGMP

* - These bits are no longer available in GA but they are still available in some customer specific releases. ** - These bits will be available only on a model with 2.4GHz and 5GHz support.

+ - These bits are not supported currently.

These should be encoded as a hex string. Presently these will be represented by 20 hex digits each of which encapsulates 4 bits. The MSB of this hex string would be bit zero and LSB would be bit 79 though (we currently have defined onlyup to bit 76).

Examples:

- tchCmWebAccessReadPages = 0x10000000000000000000 tchCmWebAccessWritePages = 0x10000000000000000000 This would mean only bit 3 (docsisLog) is enabled (0001).

- tchCmWebAccessReadPages = 0x00000000000000000030 tchCmWebAccessWritePages = 0x00000000000000000030 This means bits 74(ping) and 75(igmpProxy) are enabled.

- tchCmWebAccessReadPages = 0x0fffffffffffffffffc0 and tchCmWebAccessWritePages = 0x0fffffffffffffffffc0

  The pages that will not be displayed in this case are: bridgeRouterMode(0), docsisSignal(1), docsisStatus(2), docsisLog(3) and ping(74), igmpProxy(75).

15 Appendix2: A Sample CM Config File

```
Main
{
        NetworkAccess 1;
        MaxCPE 8;
        SnmpMibObject iso.3.6.1.4.1.4491.2.1.20.1.31.1.1.2 Integer 4; /*OID:
.1.3.6.1.4.1.4491.2.1.20.1.31.1.1.2*/
        UsServiceFlow
        {
                UsServiceFlowRef 1;
                QosParamSetType 7;
                TrafficPriority 1;
                MaxTrafficBurst 1000000;
                MaxConcatenatedBurst 8000;
                SchedulingType 2;
        }
        DsServiceFlow
        {
                DsServiceFlowRef 2;
                QosParamSetType 7;
                TrafficPriority 0;
                MaxTrafficBurst 1000000;
        }
        BaselinePrivacy
        {
                AuthTimeout 10;
                ReAuthTimeout 10;
                AuthGraceTime 600;
                OperTimeout 10;
                ReKeyTimeout 10;
                TEKGraceTime 600;
                AuthRejectTimeout 60;
                SAMapWaitTimeout 1;
                SAMapMaxRetries 4;
        }
        GlobalPrivacyEnable 1;
        GenericTLVTlvCode 202 TlvLength 3 TlvValue0x010103  ;
        SNMPv1v2cCoexistence
        {
                SNMPv1v2cCommunityName public;
                SNMPv1v2cTransportAddrAccess
                {
                        SNMPv1v2cTransportAddr 0x000000000000;
                        SNMPv1v2cTransportAddrMask 0x000000000000;
                }
                        SNMPv1v2cTransportAddrAccess
                        {
                                SNMPv1v2cTransportAddr
0x000000000000000000000000000000000000;
                                SNMPv1v2cTransportAddrMask
0x000000000000000000000000000000000000;
                        }
                        SNMPv1v2cAccessViewType 2;
                        SNMPv1v2cAccessViewName docsisManagerView;
        }
        SNMPv1v2cCoexistence
        {
                SNMPv1v2cCommunityName private;
                SNMPv1v2cTransportAddrAccess
                {
                        SNMPv1v2cTransportAddr 0x000000000000;
                        SNMPv1v2cTransportAddrMask 0x000000000000;
                }
                SNMPv1v2cTransportAddrAccess
                {
                        SNMPv1v2cTransportAddr 0x000000000000000000000000000000000000;
                        SNMPv1v2cTransportAddrMask 0x000000000000000000000000000000000000;
                }
                SNMPv1v2cAccessViewType 2;
                SNMPv1v2cAccessViewName docsisManagerView;
        }
        SNMPCPEAccessControl 1;
        GenericTLVTlvCode 81 TlvLength 254 TlvValue
0x3082095806092A864886F70D010702A0820949308209450201013100300B06092A864886F70D010701A08
2092B3082053A30820322A00302010202104C9016B68537234E49B5F48592DEB8A9300D06092A864886F70D
01010B05003066310B3009060355040613025553311230100603550040A13094361626C654C6162733112301
0060355040B1309526F6F742043413031312F302D06035504031326436162C654C61627320526F6F742043
657274696669636174696F6E20417574686F72697479301E170D313431303238303030303030305A170D34393
130323732333539395A3064310B300906035504061302555331123010060355040A130943  ;
        GenericTLVTlvCode 81 TlvLength 254 TlvValue
0x61626C654C6162733111300F060355040B1308435643204341303131312E302C06035504031325436162C6
54C61627320435643204365727469666963617496F6E20417574686F72697479308201A2300D06092A8648
86F70D01010105000382018F003082018A0282018100B15F2E0D5B2322477EA31A2B11F43DA2A0D898FEB36
E5B7D56444367E3D3098FDA55D138E8F34CC13C1FCBDC06BD3D98B89A2BDF4E1842EB95184565304E16E230
AC61C5F89A447C6D9DEFB042A9AB24ADBBF7BD40432B3974BE634C8BD1FAA4F957CF25324A4DB63C8D65FBA
11760C26EBF4F424D2E197A4EAFD0DAF82243A56C3CE4F64F4F66E69F976BFF612AE8621067  ;
        GenericTLVTlvCode 81 TlvLength 254 TlvValue
0x2DCD018503566A26764F6E371FBEF2DD0DE034045E26B11DE453057263BDD87173F31F73381A1783E88A1
B851712A2969604A4E2E9D26694BC692D824C5824A78AE924A4180D9E7B93516F03CD3FBC0C462DC8E28C94
38045876DC7E50F0B2CDF14123169FABA0B6F0F289E977179D742D53C4542016DA2279F4DEDEF18AF4C4479
13BD53D0AC21D1E75EFE7B2053070C731D8E787DCA424E284419986786AC6471D19CC9F5F135EB484392DD2
3E6A738F1C7D125E96DF66147200F3944A72D88944C22454083E4C50AF0DDA4E2F435F5BD8EB2030F875E3E
386E5272F91F4F8206522151509CFE719BA54EC233F0203010001A3663064300E0603551D0F  ;
        GenericTLVTlvCode 81 TlvLength 254 TlvValue
0x0101FF040403020106301206035551D130101FF040830060101FF020100301D0603551D0E041604143147D
1E559A52F3B89F8FFB9F9046D67DC32DA67301F0603551D2304183016801491BBEB58DDF1885F79B891E007
C380AD9D19CA4A300D06092A864886F70D01010B05000382020100C2449C998F91FEC1EABC75F4F155B3E0D
B4A6BC99016BCD08D4410900A5B87CACDA2F692D0F6988C1443C3EA738ED561D08B0FBB47CADE8CA3AC70CA
00854247118242D406A5F36C99C06333A5CC6F5F3B2903316E09C8120CE6419657E71BEE4C5217860074A7D
F07371CC1C44BD9FC36258AE7FC87BD5A55CFB525AF1EDA4287D6F80FCE3FC1EEA72B7C6580  ;
        GenericTLVTlvCode 81 TlvLength 254 TlvValue
0xEE672F9945C9FBA77A561636E23DA158DBCE59FC883155C6415DB1E57C2D42376EB4A398BB20C9F16741F
E102EF81604FC3F9F6558FE6705318424A3AD9A3087D0CE40C5E5FC006B11BC9999349398B207B6493C82A8
8926A33B7489DD0722981A430ADCBBACAA079028F8CDB8D7FBF90DD30087ACC461A5FC498CA9472743BAFF0
7C70BD6BFF6B4B672E018C7338162DFEDFFB7E4BF937B67B76BA17DDD25180D8335E2E690D85F2940AF491B
5187A6832ABD3BDA91B15076CDF0A77F90C336AE53E0E98742F6924DA81DFB9A5A63823DF8986208D2C950D
1D8D5A4B3DB12BD2F0E0E90AC0C1939914886FF2E5362228815792050BDD596841979FC4E94  ;
        GenericTLVTlvCode 81 TlvLength 254 TlvValue
0xCE53D7EA1021EB4878DCC573AA63CFD7916FC9488C48D8AA92BFDC27DB17284590CF59670D754C56547DA
33E127D2BA3532EFC36CA6B2E6B43A4852361911533097C6F6457091F52A81F7D64657C3C324649E9EC8620
25C96A5086634AE0188B90C57C84007ED5A3DBB19CCCD3BCECA202694AC7AB308203E930820251A00302010
202053207081982300D06092A864886F70D01010B05003064310B3009060355040613025553311230100603
55040A13094361626C654C6162733111300F060355040B1308435643204341303131312E302C0603550403132
54361626C654C61627320435643204365727469666963617496F6E20417574686F72697479  ;
        GenericTLVTlvCode 81 TlvLength 254 TlvValue
0x301E170D3135313130353230323933315A170D3235313130353230323933315A304B310B3009060355040
61302555331143012060355040A130B546563686E69636F6C6F72312630240603550403131D436F64652056
65726966696361746F6E20436572746966696361746530820122300D06092A864886F70D0101010500038
2010F003082010A0282010100DA442A638232C6100895373FE2735900176EBCA11206A3170E68C70658F91C
6B4B97EA3C7FDC378893C3043A676DC4FCDB94C08F1C46290E9E8E6485FFFEE676D1F44DC8669FF32AC90FA
478B778DA740AA9C55D13F01520A1CC37BFAD7A19A81E4EB92DDC23E31F9C7BAF7A19841C39  ;
```

```
	GenericTLVTlvCode 81 TlvLength 254 TlvValue
0xEEBC3041FFFD0551CD17BB6C009104E66066EEE078AD44037363B9E9863AAE75CEF6575372201F5C4C17D
631FB741B346A820F13F4149759924C71CE00C5B5B0F170854C916566B433BCA74FB301CBF7CAE2CB51AAE8
8BE42F6E2632D6401B5F2743FBAD75BFBFDD0809C30A44BF0AF11B328197E179B850445C488EB88E9ED21BB
68C12AF2F3BEF740B71F8EFAB916D0203010001A33B303930160603551D250101FF040C300A06082B060105
05070303301F0603551D23041830168014314 7D1E559A52F3B89F8FFB9F9046D67DC32DA67300D06092A864
886F70D01010B05000382018100313061 37D1F2F9F2FEE89DE641F711126C25225EC748A84C  ;
	GenericTLVTlvCode 81 TlvLength 254 TlvValue
0x16F4134B55C1536174D0D1A6503DF487D354376D79CCEAF7CF2701797252DE610356E8A2DAFC73D80917D
D48133C8CF86137B7D70C330A283ED2050DF8179821DE5E3080AC7587CE8FCE8660618D4B9333F4E40BBB93
9D1F381868C20A63063126BD93A0578F609307779795AC2BECE2B6B260B033D110903CB4D1D607D38953019
B54BF687298741A81E500743C92281B36C7B47E41D176EC75B4F06B418A70EB5F8F615EBBBE9A6E97DEF3D1
57425CA483021DC0BA1687072C102C7F9313294F505D609E6A261246B091789CB61352086CA4C97B6BDE729
E24B5E6A0588680B9F46508195810FEB7CD2F590E6FD6A43269FC5B1002CBF9B25483885232  ;
	GenericTLVTlvCode 81 TlvLength 110 TlvValue
0xC51A002A3DB4E8B16B27AB904DA2DADDA496C792EF04957E09F9E8BC0E4D00397A55223FC9D9653C6F188
65E16DB6B68FC58292EFD26B313F048DE52A42F2C961104A13D2A224D23D90706F70AD7B139716F5EB3E159
5B1D3EB6D42022D285E83289963DC23F839B4329A1003100  ;
	SnmpMibObject iso.3.6.1.4.1.46366.4292.79.2.3.3.1.5.32 Gauge32 50000; /*OID:
.1.3.6.1.4.1.46366.4292.79.2.3.3.1.5.32*/
	SnmpMibObject iso.3.6.1.4.1.46366.4292.78.1.1001.1.0 Integer 1; /*OID:
.1.3.6.1.4.1.46366.4292.78.1.1001.1.0*/
	SnmpMibObject iso.3.6.1.4.1.46366.4292.78.1.1001.2.0 HexString 0x80; /*OID:
.1.3.6.1.4.1.46366.4292.78.1.1001.2.0*/
	SnmpMibObject iso.3.6.1.4.1.46366.4292.78.1.1001.3.0 String "Technicolor" ;
/*OID: .1.3.6.1.4.1.46366.4292.78.1.1001.3.0*/
	SnmpMibObject iso.3.6.1.4.1.46366.4292.78.1.1001.4.0 String "mdc" ; /*OID:
.1.3.6.1.4.1.46366.4292.78.1.1001.4.0*/
	SnmpMibObject iso.3.6.1.4.1.46366.4292.78.1.1001.5.0 Integer 0; /*OID:
.1.3.6.1.4.1.46366.4292.78.1.1001.5.0*/
/*CmMic 0x63F53A9CDFE69EA0C01C2AA1F56557C5*/
/*CmtsMic 0xEAE5074EF8D8437012308843D2E37D83*/
}
```

16 Abbreviations and Acronyms

This guide uses the following terms:

Abbreviation	Expansion
AP	Access Point
CTS	Clear To Send protection mode
DTIM Interval	Delivery Traffic Indication Message
MoCA	Multimedia over Coax Alliance
PMIP	Proxy Mobile Internet Protocol
RTS	Request to Send Threshold
SNMP	Simple Network Management Protocol
softGRE	Soft Generic Routing Encapsulation
STA	Station- A wireless Station
WDS	Wireless Distribution System
WPS	Wi-Fi Protected Setup

technicolor

FEEL THE WONDER

Technicolor Worldwide

Headquarters

1, Rue Jeanne d’Arc

92443 Issy-les-Moulineaux, France

T +33 (0)1 41 86 50 00

F +33 (0)1 41 86 56 15

technicolor.com

Specifications subject to change without notice.