Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Draft 1.0</td>
<td>1/8/2018</td>
<td>Initial draft</td>
</tr>
</tbody>
</table>
# Table of Contents

1. Introduction

2. Technicolor Wireless Gateway
   2.1 System Information

3. Initial Configuration and Setup
   3.1 Accessing the WebUI

4. WebUI Guide

5. Status Pages
   5.1 Overview
   5.2 Gateway
   5.3 Local Network
   5.4 Wireless Status
   5.5 DOCSIS Status
   5.6 DOCSIS Signal
   5.7 DOCSIS Log
   5.8 System

6. Connection
   6.1 Devices
   6.2 LAN
      6.2.1 LAN Setup
   6.3 WAN
      6.3.1 User Provisioning of WAN
      6.3.2 SNMP Provisioning for WAN
      6.3.3 Dual Stack Router
   6.4 Routing
      6.4.1 Enable / Disable IGMP Proxy
      6.4.2 RIP
      6.4.3 SNMP Provisioning for Routing
   6.5 MoCA
      6.5.1 User Provisioning for MoCA
      6.5.2 SNMP Provisioning for MoCA
   6.6 Modem
   6.7 MTA
   6.8 Network Time

7. Wireless

1/8/2018 Proprietary and Confidential - Technicolor
7.1 Radio..............................................................................................................52
  7.1.1 User Provisioning for Radio.........................................................................53
  7.1.2 SNMP Provisioning for Radio ......................................................................54
7.2 Security ..............................................................................................................54
  7.2.1 User Provisioning for Wireless Security......................................................55
  7.2.2 SNMP Provisioning for Wireless Security ....................................................56
7.3 Advanced ............................................................................................................57
  7.3.1 User Provisioning for Advanced Wireless....................................................58
  7.3.2 SNMP Provisioning for Advanced Wireless..................................................60
7.4 Guest Network ....................................................................................................60
  7.4.1 User Provisioning for Guest Network...........................................................62
  7.4.2 SNMP Provisioning for Guest Network.........................................................63
7.5 MAC Control ......................................................................................................63
  7.5.1 User Provisioning for MAC Control..............................................................64
  7.5.2 SNMP Provisioning for MAC Control...........................................................65
7.6 WPS ....................................................................................................................65
  7.6.1 User Provisioning for WPS ...........................................................................65
7.7 QOS .....................................................................................................................66
  7.7.1 User Provisioning for QOS ...........................................................................67
  7.7.2 SNMP Provisioning for QOS .......................................................................68
8 Security ..................................................................................................................69
  8.1 Firewall ............................................................................................................69
    8.1.1 User Provisioning for Firewall .................................................................69
    8.1.2 SNMP Provisioning for Firewall ..............................................................72
  8.2 IP Filter .............................................................................................................72
  8.3 Device Filter ....................................................................................................72
    8.3.1 SNMP Provisioning for Device Filter.........................................................73
  8.4 Site Filter ..........................................................................................................74
    8.4.1 SNMP Provisioning for Site Filter..............................................................74
  8.5 Service Filter ....................................................................................................75
    8.5.1 SNMP Provisioning for Service Filter.........................................................77
  8.6 VPN Settings ....................................................................................................77
    8.6.1 User Provisioning for VPN Settings...........................................................77
  8.7 Email Settings ..................................................................................................83
  8.8 Reports .............................................................................................................84
9 Application .............................................................................................................85
9.1 Port Forward ................................................................. 85
9.2 Port Trigger ................................................................. 85
9.3 DDNS ........................................................................... 86
9.4 DMZ ............................................................................ 87
  9.4.1 SNMP Provisioning for DMZ ........................................ 88
9.5 UPnP ............................................................................ 88
  9.5.1 User Provisioning of UPnP ........................................ 89
  9.5.2 SNMP Provisioning for UPNP ..................................... 89
9.6 IP Passthrough ............................................................. 89
9.7 Media ......................................................................... 90
10 Administration ............................................................... 92
  10.1 User .......................................................................... 92
  10.2 WiFi Power ............................................................... 92
  10.3 Remote Access .......................................................... 93
  10.3.1 SNMP Provisioning for Remote Management .............. 94
  10.4 Backup & Restore ....................................................... 94
    10.4.1 User Provisioning for Backup & Restore ..................... 94
    10.4.2 SNMP Provisioning for Backup & Restore .................. 95
  10.5 Reboot & Reset .......................................................... 95
    10.5.1 SNMP Provisioning for Factory Settings ................... 96
  10.6 Restarting the Device .................................................. 96
    10.6.1 SNMP Provisioning for Restarting the Device ............ 97
  10.7 Trouble Shooting ....................................................... 97
  10.8 Remote Log ............................................................... 98
  10.9 Historical Consumption .............................................. 98
11 Diagnostics ................................................................. 100
  11.1 System ..................................................................... 100
  11.2 Interface ................................................................. 100
  11.3 Network .................................................................... 104
  11.4 Wireless ................................................................. 106
  11.5 Clients ..................................................................... 109
  11.6 Internet ................................................................. 110
  11.7 Self Test .................................................................... 110
12 Isolation ........................................................................ 112
  12.1 User Provisioning for Isolation .................................... 112
  12.2 SNMP Provisioning for Isolation ................................. 112

1/8/2018 Proprietary and Confidential - Technicolor
13 TR-069 .................................................................................................................. 114
13.1 User Provisioning for TR-069 ........................................................................ 114
13.2 SNMP Provisioning for TR-069 ..................................................................... 114
14 Appendix1: Web User Interface Control ........................................................... 116
15 Appendix2: A Sample CM Config File ............................................................. 122
16 Abbreviations and Acronyms ......................................................................... 125
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.

![Image of 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.

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solid on</td>
<td>Wi-Fi Protected Setup (WPS) support, including an HW push button to activate WPS for simplified and secure wireless setup</td>
</tr>
<tr>
<td>Off</td>
<td>WPS setup not active</td>
</tr>
</tbody>
</table>

**Power LED (item B)**

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solid on</td>
<td>Main Power Supply (12volt, 4.5 Amp.). DUT is on Main Power Supply.</td>
</tr>
<tr>
<td>Blinking</td>
<td>Slow Blink - MoCA is enabled, Fast Blink – MoCA enabled and MoCA client connected</td>
</tr>
<tr>
<td>Off</td>
<td>Power –Off</td>
</tr>
</tbody>
</table>

**Downstream (DS) LED (item C)**

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solid on</td>
<td>Down Stream channel locked</td>
</tr>
<tr>
<td>Off</td>
<td>Power-Off</td>
</tr>
<tr>
<td>Flashing with US LED off</td>
<td>Searching for downstream signal</td>
</tr>
<tr>
<td>Flashing with US LED on</td>
<td>Partial service mode</td>
</tr>
<tr>
<td>Both US and DS Flashing</td>
<td>Software upgrade in progress</td>
</tr>
</tbody>
</table>
### UP stream LED (US) (item D)

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solid on</td>
<td>UP stream channel locked</td>
</tr>
<tr>
<td>Off</td>
<td>Power-Off</td>
</tr>
<tr>
<td>Flashing with DS Led off</td>
<td>Attempting to communicate with the CMTS</td>
</tr>
<tr>
<td>Flashing with US Led on</td>
<td>Partial service mode</td>
</tr>
<tr>
<td>Both US and DS Flashing</td>
<td>Software upgrade in progress</td>
</tr>
</tbody>
</table>

### Online LED (item E)

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solid on</td>
<td>Modem provisioning complete</td>
</tr>
<tr>
<td>Flashing slow</td>
<td>Attempting DHCP</td>
</tr>
<tr>
<td>Flashing fast</td>
<td>Attempting TFTP and final registration with CMTS</td>
</tr>
<tr>
<td>Very slow blink</td>
<td>Network access disabled by configuration file</td>
</tr>
<tr>
<td>Off</td>
<td>Not connected to your service provider’s network</td>
</tr>
</tbody>
</table>

### 2.4 GHz Wi-Fi LED (item F)

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blinking</td>
<td>Data is being transferred over the wireless connection. Wi-Fi is connected.</td>
</tr>
<tr>
<td>Off</td>
<td>Wi-Fi access point is not enabled</td>
</tr>
</tbody>
</table>

### 5 GHz Wi-Fi LED (item G)

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blinking</td>
<td>Data is being transferred over the wireless connection. Wi-Fi is connected.</td>
</tr>
<tr>
<td>Off</td>
<td>Wi-Fi access point is not enabled</td>
</tr>
</tbody>
</table>
### Telephone Line 1 led (item H)

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

### Telephone Line 2 led (item I)

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solid on</td>
<td>Telephone Service on line -2 is enabled</td>
</tr>
<tr>
<td>Blinking</td>
<td>Telephone line 2 is connected to telephone and is operational</td>
</tr>
<tr>
<td>Flashing</td>
<td>Line one off (EMTA DHCP)</td>
</tr>
<tr>
<td>Both lines Blinking</td>
<td>Device registering with call agent</td>
</tr>
<tr>
<td>Off</td>
<td>Line 2 is not connected to phone or not operational.</td>
</tr>
</tbody>
</table>
**Back panel**
The following image shows the back of the Wireless Gateway.

![Back panel image]

**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:

<table>
<thead>
<tr>
<th>LED</th>
<th>LED Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F</td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 2.3
**Left LED**
*Green*
<table>
<thead>
<tr>
<th>Solid on</th>
<th>Connected to a Gigabit Ethernet device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blinking</td>
<td>Connected to a Gigabit Ethernet device and sending/receiving data</td>
</tr>
<tr>
<td>Off</td>
<td>Not connected to a Gigabit Ethernet device</td>
</tr>
</tbody>
</table>

**Right LED**
*Amber*
<table>
<thead>
<tr>
<th>Solid on</th>
<th>Connected to a 1000Mbps/100Mbps/10Mbps device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blinking</td>
<td>Connected to a 1000Mbps/100Mbps/10Mbps device and sending/receiving data</td>
</tr>
<tr>
<td>Off</td>
<td>Not connected to a 100Mbps/10Mbps device</td>
</tr>
</tbody>
</table>

**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.

![Bottom panel view of the Wireless Gateway](image)

**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.
Software File Name and Revisions

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

![System Software Table]

**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.

![Image of WebUI login page]

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.

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

Table – 4.2

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

<table>
<thead>
<tr>
<th>Application</th>
<th>Report</th>
<th>✓</th>
<th>✓</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Port Forward</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Application</td>
<td>Port Trigger</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Application</td>
<td>DDNS</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Application</td>
<td>DMZ</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Application</td>
<td>UPnP</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Application</td>
<td>IP Passthrough</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Application</td>
<td>Media</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

| Administration | User | ✓ | ✓ |
| Administration | Remote Access | ✓ | ✓ |
| Administration | Backup and Restore | ✓ | ✓ |
| Administration | Reboot and Reset | ✓ | ✓ |
| Administration | Historical Consumption | ✓ | ✓ |
| Administration | Troubleshooting | ✓ | ✓ |
| Administration | Remote Log | ✓ | ✓ |

| Diagnostics | System | ✓ | ✓ |
| Diagnostics | Interface | ✓ | ✓ |
| Diagnostics | Network | ✓ | ✓ |
| Diagnostics | Wireless | ✓ | ✓ |
| Diagnostics | Clients | ✓ | ✓ |
| Diagnostics | Internet | ✓ | ✓ |
| Diagnostics | Self-Test | ✓ | ✓ |

Table – 4.1
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.

![Diagram of Gateway Status Tab](image)

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 Table]

**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:
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](image)

*Figure 5.4*
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:

![Technicolor Wireless Cable Voice Gateway](image)

2.4GHz Private Network

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Name</td>
<td>FA13C4:2.4</td>
</tr>
<tr>
<td>MAC Address</td>
<td>48:00:33:FA:13:C8</td>
</tr>
<tr>
<td>Security Mode</td>
<td>WPA2-Personal (AES)</td>
</tr>
<tr>
<td>Network Mode</td>
<td>802.11-G-N</td>
</tr>
<tr>
<td>Channel</td>
<td>11 (Auto)</td>
</tr>
<tr>
<td>Channel Width</td>
<td>40MHz</td>
</tr>
<tr>
<td>SSID Broadcast</td>
<td>Enabled</td>
</tr>
<tr>
<td>Network Status</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Figure 5.6
5GHz Network Information:

![Technicolor Wireless Cable Voice Gateway](image)

5GHz Private Network

<table>
<thead>
<tr>
<th>Network Name</th>
<th>FA13C4-5</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>48:00:33:FA:13:D0</td>
</tr>
<tr>
<td>Security Mode</td>
<td>WPA2-Personal (AES)</td>
</tr>
<tr>
<td>Network Mode</td>
<td>802.11-A,N,AC</td>
</tr>
<tr>
<td>Channel</td>
<td>153 (Auto)</td>
</tr>
<tr>
<td>Channel Width</td>
<td>80MHz</td>
</tr>
<tr>
<td>SSID Broadcast</td>
<td>Enabled</td>
</tr>
<tr>
<td>Network Status</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

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:

Figure 5.8
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** - Transmits 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

![Figure 5.10](image-url)
Error Codewords:
This section displays Error Codewords, the information about the Channel ID, Unerrored, Correcteds and Uncorrectables.
### Error Codewords

<table>
<thead>
<tr>
<th>Index</th>
<th>Channel ID</th>
<th>Unerrored</th>
<th>Correcteds</th>
<th>Uncorrectables</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5</td>
<td>63002670</td>
<td>172</td>
<td>267</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>62534752</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>62538675</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>62542175</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>62545981</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>62546990</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>62552019</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>62555151</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**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.

![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.
Figure 5.16

The image shows a screenshot of the System Hardware section of a Technicolor Wireless Cable Voice Gateway.

- **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
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:

![Image of Device Page]

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:

1/8/2018  Proprietary and Confidential - Technicolor  37
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](image)

**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 is 192.168.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:
- tchRglpMgmtLanSubnetMask
- tchRglpMgmtLanGateway
- tchRglpMgmtLanDhcpServer
- tchRglpMgmtLanDhcpServerPoolStart
- tchRglpMgmtLanDhcpServerPoolEnd
- tchRglpMgmtLanDhcpServerLeaseTime
- tchRglpMgmtDnsServerIp

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.

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.)

**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.
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.
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 IP address(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.

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

**tchRglpMgmtWanMode** 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 **tchRglpMgmtWanAddrStatic** to fill in the details.

**tchRglpMgmtWanMtu** & **tchRglpMgmtWanTtl** can be optionally set.

**tchRglpMgmtWanDualIpAddr** is where the second IP can be filled in and **tchRglpMgmtWanDualIpRipAdvertised** RIP advertised for the access.

**tchRglpMgmtWanAddrBackupDefGw** 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.

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.

![Figure 6.9](image)

![Figure 6.10](image)
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

```
tchRglpMgmtLanMode: Available
tchRglpMgmtLanNetwork: Available
tchRglpMgmtLanSubnetMask: Available
tchRglpMgmtLanGateway: Available
tchRglpMgmtLanNapt: 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).

```
tchRglpMgmtStaticRouteNetwork: Available
tchRglpMgmtStaticRouteSubnetMask: Available
tchRglpMgmtStaticRouteGateway: Available
tchRglpMgmtStaticRouteRipAdvertise: Available
tchRglpMgmtStaticRouteRowStatus: 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 becomes 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.
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.

![Technicolor Wireless Cable Voice Gateway](image)

**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 Status Screenshot](image)

**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.
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.

![Figure 7.1](image)
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 congestion 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.
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

- **tchgDot11BssSecurityMode** sets the security mode for the selected SSID.
- **tchgDot11WepEncryptionMode** sets the key length for WEP.
- **tchgDot11WepPassPhrase** sets the passphrase for WEP.
- **tchgDot11Wep64BitKeyValue** sets each 40/64-bit WEP key.
- **tchgDot11Wep128BitKeyValue** sets each 104/128-bit WEP key.
- **tchgDot11WepDefaultKey** sets the default WEP key.
- **tchgDot11WpaAlgorithm** sets the encryption for WPA.
- **tchgDot11WpaPreSharedKey** 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.

![Image](image_url)
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 to 1023.

**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.
7.3.2 **SNMP Provisioning for Advanced Wireless**

*tchRgdot11nExtPhyRate* sets the transmission rate.

*tchRgdot11ExtCtsProtectionEnable* sets the CTS protection mode.

*tchRgDot11ExtBeaconInterval* sets the beacon interval.

*tchRgDot11ExtDTIMInterval* sets the DTIM interval.

*tchRgDot11ExtFragThresh* sets 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.
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.

![Technicolor Wireless Cable Voice Gateway](image)

**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:
1/8/2018
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
- tchRgpMgmtLanTable
- tchRgpMgmtLanDhcpServerTable

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).
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).

![Technicolor Wireless Cable Voice Gateway](image)

**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.

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, IcAifs, IcEcwMin, IcEcwMax, IcTxOp, IcAckPolicy.

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

<table>
<thead>
<tr>
<th>Firewall level</th>
<th>Restrictions on inbound traffic</th>
<th>Restrictions on outbound traffic</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>All unsolicited inbound traffic is blocked, and Intrusion Detection is enabled.</td>
<td>All traffic except the following are restricted: • HTTP and HTTPS (TCP)</td>
<td>Both inbound and outbound traffic are restricted</td>
</tr>
</tbody>
</table>
| 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](image)

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)
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)

![Figure 8.4](image)

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 the 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).
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:

Figure 8.5

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.).

Figure 8.6
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.
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)
**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.

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.

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.

![Figure 8.9](image-url)
### Figure 8.10

#### Remote Secure Group

<table>
<thead>
<tr>
<th>IP Address</th>
<th>192.168.0.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.255</td>
</tr>
</tbody>
</table>

#### Remote Secure Gateway

<table>
<thead>
<tr>
<th>IP Address</th>
<th>192.168.0.6</th>
</tr>
</thead>
</table>

---

### Figure 8.11

#### Remote Secure Gateway

<table>
<thead>
<tr>
<th>IP Address</th>
<th>192.168.0.6</th>
</tr>
</thead>
</table>

#### Key Management

- **Key Exchange Method**
  - Auto(IKE)
  - Auto(IKE)
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)
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:
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)

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 Table](image)

**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.
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.
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.
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 `tchRglpMgmtLanUpnp`. 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.
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:
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.

![User Administration](image)

**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:
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:
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.

![Figure 10.4](image)

### 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.

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).

![Figure 10.6](image-url)
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.

![Remote Log Configuration](image)

**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.
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 status details](image)

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:
**WAN**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>L3 Enable</td>
<td>Enabled</td>
</tr>
<tr>
<td>L3 Status</td>
<td>Up</td>
</tr>
<tr>
<td>L3 LastChange</td>
<td>D:0 H:0 M:0 S:33</td>
</tr>
<tr>
<td>Ethernet Enable</td>
<td>Enabled</td>
</tr>
<tr>
<td>Ethernet Status</td>
<td>Up</td>
</tr>
<tr>
<td>Ethernet MaxBitRate</td>
<td>1000</td>
</tr>
<tr>
<td>Ethernet DuplexMode</td>
<td>Auto</td>
</tr>
<tr>
<td>Tx/Rx Packets</td>
<td>774 / 1303</td>
</tr>
<tr>
<td>Tx/Rx Rate</td>
<td>0 / 0</td>
</tr>
<tr>
<td>Tx/Rx Errors</td>
<td>0 / 0</td>
</tr>
</tbody>
</table>

*Figure 11.2*
Figure 11.3

```plaintext
<table>
<thead>
<tr>
<th>Port</th>
<th>Enable</th>
<th>Status</th>
<th>MaxBitRate</th>
<th>DuplexMode</th>
<th>LastChange</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Down</td>
<td>true</td>
<td>1000</td>
<td>Auto</td>
<td>10/00/03:03:34</td>
</tr>
<tr>
<td>2</td>
<td>Down</td>
<td>true</td>
<td>1000</td>
<td>Auto</td>
<td>10/00/03:35</td>
</tr>
<tr>
<td>3</td>
<td>Down</td>
<td>true</td>
<td>1000</td>
<td>Auto</td>
<td>10/00/03:35</td>
</tr>
<tr>
<td>4</td>
<td>Up</td>
<td>true</td>
<td>1000</td>
<td>Auto</td>
<td>10/00/03:36</td>
</tr>
</tbody>
</table>
```

```plaintext
<table>
<thead>
<tr>
<th>Port</th>
<th>Tx/Rx Packets</th>
<th>Tx/Rx Rate</th>
<th>Tx/Rx Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0 / 0</td>
<td>0 / 0</td>
<td>0 / 0</td>
</tr>
<tr>
<td>2</td>
<td>0 / 0</td>
<td>0 / 0</td>
<td>0 / 0</td>
</tr>
<tr>
<td>3</td>
<td>0 / 0</td>
<td>0 / 0</td>
<td>0 / 0</td>
</tr>
<tr>
<td>4</td>
<td>1273 / 2048</td>
<td>504324 / 430680</td>
<td>0 / 0</td>
</tr>
</tbody>
</table>
```
### 2.4GHz Wireless Network

<table>
<thead>
<tr>
<th>Enable</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Up</td>
</tr>
<tr>
<td>MaxBitRate</td>
<td>0</td>
</tr>
<tr>
<td>LastChange</td>
<td>0:0:0:0:0:0:0:37</td>
</tr>
<tr>
<td>Tx/Rx Packets</td>
<td>0/0</td>
</tr>
<tr>
<td>Tx/Rx Rate</td>
<td>0/0</td>
</tr>
<tr>
<td>Tx/Rx Errors</td>
<td>0/0</td>
</tr>
</tbody>
</table>

### 5GHz Wireless Network

<table>
<thead>
<tr>
<th>Enable</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Up</td>
</tr>
<tr>
<td>MaxBitRate</td>
<td>0</td>
</tr>
<tr>
<td>LastChange</td>
<td>0:0:0:0:0:0:0:33</td>
</tr>
<tr>
<td>Tx/Rx Packets</td>
<td>0/0</td>
</tr>
<tr>
<td>Tx/Rx Rate</td>
<td>0/0</td>
</tr>
<tr>
<td>Tx/Rx Errors</td>
<td>0/213682000</td>
</tr>
</tbody>
</table>

![Figure 11.4](image-url)
### 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](image)

**Figure 11.5**
**Figure 11.6**

<table>
<thead>
<tr>
<th>LAN IPv6</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Link-Local Gateway Address</td>
<td>N/A</td>
</tr>
<tr>
<td>Global Gateway Address</td>
<td>fd00:ca57:0153:11:4a00:33ff:fe0a:13c6</td>
</tr>
<tr>
<td>LAN IPv6 Prefix</td>
<td>fd00:ca57:0153:11::/64</td>
</tr>
<tr>
<td>DHCP Server</td>
<td>Enabled</td>
</tr>
<tr>
<td>DHCP Lease Time</td>
<td>D:7 H:0 M:0 S:0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LAN IPv4</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway Address</td>
<td>192.168.0.1</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>DHCP Server</td>
<td>Enabled</td>
</tr>
<tr>
<td>DHCP Lease Time</td>
<td>D:0 H:13 M:53 S:20</td>
</tr>
<tr>
<td>Primary DNS</td>
<td></td>
</tr>
<tr>
<td>Secondary DNS</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LAN IPv6</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Link-Local Gateway Address</td>
<td>N/A</td>
</tr>
<tr>
<td>Global Gateway Address</td>
<td>fd00:ca57:0153:11:4a00:33ff:fe0a:13c6</td>
</tr>
<tr>
<td>LAN IPv6 Prefix</td>
<td>fd00:ca57:0153:11::/64</td>
</tr>
<tr>
<td>DHCP Server</td>
<td>Enabled</td>
</tr>
<tr>
<td>DHCP Lease Time</td>
<td>D:7 H:0 M:0 S:0</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Name</td>
<td>FA13C4-2.4</td>
</tr>
<tr>
<td>SSID Broadcast</td>
<td>Enabled</td>
</tr>
<tr>
<td>Network Mode</td>
<td>802.11-0:N</td>
</tr>
<tr>
<td>Security Mode</td>
<td>WPA2-Personal (AES)</td>
</tr>
<tr>
<td>Channel</td>
<td>6 (Auto)</td>
</tr>
<tr>
<td>Channel Width</td>
<td>40MHz</td>
</tr>
<tr>
<td>Network Status</td>
<td>Enabled</td>
</tr>
<tr>
<td>MAC Address</td>
<td>48:00:33:FA:13:C8</td>
</tr>
</tbody>
</table>

Associated Devices

<table>
<thead>
<tr>
<th>SSID</th>
<th>Host Name</th>
<th>MAC Address</th>
<th>IP Address</th>
<th>Network Mode</th>
<th>Tx/Rx Rate</th>
<th>Tx/Rx Packets</th>
<th>RSSI</th>
</tr>
</thead>
</table>

**Figure 11.9**
2.4GHz Wireless Network

Scan Nearby AP

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

<table>
<thead>
<tr>
<th>SSID</th>
<th>Host Name</th>
<th>MAC Address</th>
<th>IP Address</th>
<th>Network Mode</th>
<th>Tx/Rx Ratio</th>
<th>Tx/Rx Packets</th>
<th>RSSI</th>
</tr>
</thead>
</table>

Figure 11.10
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.
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.

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

<table>
<thead>
<tr>
<th>Index</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
<td>Primary BSSID</td>
</tr>
<tr>
<td>33</td>
<td>Secondary BSSID #1</td>
</tr>
<tr>
<td>34</td>
<td>Secondary BSSID #2</td>
</tr>
<tr>
<td>35</td>
<td>Secondary BSSID #3</td>
</tr>
<tr>
<td>36</td>
<td>Secondary BSSID #4</td>
</tr>
<tr>
<td>37</td>
<td>Secondary BSSID #5</td>
</tr>
<tr>
<td>38</td>
<td>Secondary BSSID #6</td>
</tr>
<tr>
<td>39</td>
<td>Secondary BSSID #7</td>
</tr>
</tbody>
</table>

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:

```plaintext
SnmpMibObject tchRg DeviceLanLanIsolation.0 Integer 1; /* enable */
SnmpMibObject tchRg DeviceLanWlanIsolation.0 Integer 1; /* enable */
SnmpMibObject tchRg Dot11BssAplIsolation.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.

![Deployment Diagram]

Figure 13.1

To configure TR-069, \texttt{tchTR069ClientMode} should be set to enable (1) and \texttt{tchTR069ClientAcsUrl} should point to the ACS server (e.g. http://myacs.acs.lab.sa). \texttt{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 \texttt{tchTR069ClientCrUsername} and \texttt{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

\texttt{tchTR069ClientMode} should be set to enable (1) (TR-069 is disabled by default).

\texttt{tchTR069ClientAcsUrl} should be set to the ACS IP address or FQDN.
tchTR069ClientAllowDocsisConfig should be set to enable (1) for TR-69 to be reconfigured (this MIB is enabled by default).

- **tchTR069ClientAcsUsername** — username for ACS association
- **tchTR069ClientAcsPassword** — password for ACS association

Optional configuration MIBs are:
- **tchTR069ClientPeriodicInform** to enable inform messages to be sent back to the ACS periodically, refreshing the device data (this MIB is enabled by default)
- **tchTR069ClientPeriodicInformInterval** to 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:

<table>
<thead>
<tr>
<th>Bitmap</th>
<th>Top tab</th>
<th>Bottom tab</th>
<th>Section</th>
<th>Field(s)/Pop-ups</th>
</tr>
</thead>
<tbody>
<tr>
<td>bridgeRouterMode(0)</td>
<td>Administration</td>
<td>Management</td>
<td>Gateway Setup(WAN)</td>
<td>Working Mode</td>
</tr>
<tr>
<td>docsisSignal(1)</td>
<td>Status</td>
<td>Status</td>
<td>DOCSIS Signal</td>
<td></td>
</tr>
<tr>
<td>docsisStatus(2)</td>
<td>Status</td>
<td>DOCSIS Status</td>
<td></td>
<td></td>
</tr>
<tr>
<td>docsisLog(3)</td>
<td>Status</td>
<td>DOCSIS Signal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeUseNtp(4) *</td>
<td>Setup</td>
<td>LAN Setup</td>
<td>Network Setup (LAN)</td>
<td>NTP Enable</td>
</tr>
<tr>
<td>timeZone(5)</td>
<td>Setup</td>
<td>LAN Setup</td>
<td>Network Setup (LAN)</td>
<td>Time Zone</td>
</tr>
<tr>
<td>timeDst(6)</td>
<td>Setup</td>
<td>LAN Setup</td>
<td>Network Setup (LAN)</td>
<td>Automatically adjust DST</td>
</tr>
<tr>
<td>timeServer(7)*</td>
<td>Setup</td>
<td>LAN Setup</td>
<td>Network Setup (LAN)</td>
<td></td>
</tr>
<tr>
<td>lanIp(8)</td>
<td>Setup</td>
<td>LAN Setup</td>
<td>LAN Gateway IP</td>
<td>Local IP Address</td>
</tr>
<tr>
<td>lanIpEnable(9)</td>
<td>Setup</td>
<td>LAN Setup</td>
<td>Network Setup (LAN)</td>
<td>DHCP Server</td>
</tr>
<tr>
<td>lanIpScope(10)</td>
<td>Setup</td>
<td>LAN Setup</td>
<td>Network Setup (LAN)</td>
<td>Starting IP Address Maximum Number of DHCP Users</td>
</tr>
<tr>
<td>lanIpDhcpLeaseTime(11)</td>
<td>Setup</td>
<td>LAN Setup</td>
<td>Network Setup (LAN)</td>
<td>Client Lease Time</td>
</tr>
<tr>
<td>lanIpDhcpDns(12)</td>
<td>Setup</td>
<td>LAN Setup</td>
<td>Network Setup (LAN)</td>
<td>LAN 1 Static DNS 1 LAN 1 Static DNS 2 LAN 1 Static DNS 3</td>
</tr>
<tr>
<td>Bitmap</td>
<td>Top tab</td>
<td>Bottom tab</td>
<td>Section</td>
<td>Field(s)/Pop-ups</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td>------------------</td>
<td>----------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>lanDhcpWins(13)+</td>
<td></td>
<td></td>
<td>Network Setup (LAN)</td>
<td>Connected Device Summary Pre-assigned DHCP IP Addresses Also the associated pop-ups</td>
</tr>
<tr>
<td>lanFixedCpe(14)</td>
<td>Setup</td>
<td>LAN Setup</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Connected Device Summary</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Pre-assigned DHCP IP Addresses</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Also the associated pop-ups</td>
<td></td>
</tr>
<tr>
<td>wanStaticIp(15)</td>
<td>Administration</td>
<td>Management</td>
<td>Gateway Setup(WAN)</td>
<td>Internet IP address Subnet Mask Default Gateway (When Static IP is selected as Connection Mode)</td>
</tr>
<tr>
<td>wanDns(16)</td>
<td>Administration</td>
<td>Management</td>
<td>Gateway Setup(WAN)</td>
<td>Primary DNS Subnet Mask Default Gateway (When Static IP is selected as Connection Mode)</td>
</tr>
<tr>
<td>wanMtu(17)</td>
<td>Administration</td>
<td>Management</td>
<td>Gateway Setup(WAN)</td>
<td>MTU</td>
</tr>
<tr>
<td>wanHostDomainNames(18)</td>
<td>Administration</td>
<td>Management</td>
<td>Gateway Setup(WAN)</td>
<td>Host Name Domain Name (When Static IP is selected as Connection Mode)</td>
</tr>
<tr>
<td>resetModem(19)+</td>
<td>Administration</td>
<td>Device Restart</td>
<td></td>
<td></td>
</tr>
<tr>
<td>resetFactoryDefaults(20)</td>
<td>Administration</td>
<td>Factory Defaults</td>
<td></td>
<td></td>
</tr>
<tr>
<td>backupConfigToPc(21)+</td>
<td>Administration</td>
<td>Backup and Restore</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ddns(22)</td>
<td>Setup</td>
<td></td>
<td></td>
<td>DDNS</td>
</tr>
<tr>
<td>Bitmap</td>
<td>Top tab</td>
<td>Bottom tab</td>
<td>Section</td>
<td>Field(s)/Pop-ups</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------</td>
<td>------------</td>
<td>------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>wanBlocking(23)</td>
<td>Security</td>
<td>Firewall</td>
<td>Block WAN Requests</td>
<td>Block Anonymous Internet Requests</td>
</tr>
<tr>
<td>ipsecPassthrough(24)</td>
<td>Security</td>
<td>VPN Passthrough</td>
<td>IP Sec Passthrough</td>
<td></td>
</tr>
<tr>
<td>pptpPassthrough(25)</td>
<td>Security</td>
<td>VPN Passthrough</td>
<td>PPTP Passthrough</td>
<td></td>
</tr>
<tr>
<td>remoteManagement(26)</td>
<td>Administration</td>
<td>Management</td>
<td>Gateway Access</td>
<td>Remote Management Management Port</td>
</tr>
<tr>
<td>upnpEnable(28)</td>
<td>Administration</td>
<td>Management</td>
<td>UPnP</td>
<td>UPnP</td>
</tr>
<tr>
<td>ipFiltering(29)</td>
<td>Access Restrictions</td>
<td>IP Filter</td>
<td>IP Filter</td>
<td></td>
</tr>
<tr>
<td>macFiltering(30)</td>
<td>Access Restrictions</td>
<td>MAC Address Filter</td>
<td>MAC Address Filter</td>
<td></td>
</tr>
<tr>
<td>portFiltering(31)</td>
<td>Applications and Gaming</td>
<td>Port Filter</td>
<td>Port Filter</td>
<td></td>
</tr>
<tr>
<td>portForwarding(32)</td>
<td>Applications and Gaming</td>
<td>Port Range Forwarding</td>
<td>Port Range Forwarding</td>
<td></td>
</tr>
<tr>
<td>portTriggers(33)</td>
<td>Applications and Gaming</td>
<td>Port Range Triggering</td>
<td>Port Range Triggering</td>
<td></td>
</tr>
<tr>
<td>dmz(34)</td>
<td>Applications and Gaming</td>
<td>DMZ</td>
<td>DMZ</td>
<td></td>
</tr>
<tr>
<td>vpnTermination(35)</td>
<td>Security</td>
<td>VPN</td>
<td>VPN</td>
<td></td>
</tr>
<tr>
<td>staticRoute(36)+</td>
<td>Connection</td>
<td>WAN</td>
<td>WAN</td>
<td></td>
</tr>
<tr>
<td>Bitmap</td>
<td>Top tab</td>
<td>Bottom tab</td>
<td>Section</td>
<td>Field(s)/Pop-ups</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------</td>
<td>--------------</td>
<td>-------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>portScanDetection(43)</td>
<td>Security</td>
<td>Firewall</td>
<td>Filters</td>
<td>Block Port Scan Detection</td>
</tr>
<tr>
<td>ipFloodDetection(44)</td>
<td>Security</td>
<td>Firewall</td>
<td>Filters</td>
<td>Block IP Flood Detection</td>
</tr>
<tr>
<td>firewallProtection(45)</td>
<td>Security</td>
<td>Firewall</td>
<td>Firewall</td>
<td>SPI Firewall Protection</td>
</tr>
<tr>
<td>firewallEventLogging(46)+</td>
<td>Administration</td>
<td>Reporting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>parentalControl(47)</td>
<td>Access</td>
<td>Basic Rules</td>
<td>Time of Day</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Restriction</td>
<td>Rules</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>User Setup</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wireless2p4SSID(48)</td>
<td>Wireless</td>
<td>Radio Settings</td>
<td>Basic Settings</td>
<td>Radio Band</td>
</tr>
<tr>
<td>wireless2p4ABGNMode(49)</td>
<td>Wireless</td>
<td>Radio Settings</td>
<td>Basic Settings</td>
<td>Network Mode</td>
</tr>
<tr>
<td>wireless2p4SSID(50)</td>
<td>Setup</td>
<td>Quick Setup</td>
<td>Wireless Network</td>
<td>Network Name (SSID)</td>
</tr>
<tr>
<td></td>
<td>Wireless</td>
<td>Radio Settings</td>
<td></td>
<td>Network Name (SSID)</td>
</tr>
<tr>
<td>wireless2p4BroadcastSSID(51)</td>
<td>Wireless</td>
<td>Radio Settings</td>
<td>Broadcast SSID</td>
<td></td>
</tr>
<tr>
<td>wireless2p4Channel(52)</td>
<td>Wireless</td>
<td>Radio Settings</td>
<td>Standard Channel</td>
<td></td>
</tr>
<tr>
<td>wireless2p4ChannelWidth(53)</td>
<td>Wireless</td>
<td>Radio Settings</td>
<td>Channel Width</td>
<td></td>
</tr>
<tr>
<td>wireless2p4Security(54)</td>
<td>Wireless</td>
<td>Wireless Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wireless2p4Wps(55)</td>
<td>Wireless</td>
<td>WPS</td>
<td>all fields</td>
<td></td>
</tr>
<tr>
<td>wireless2p4Advanced(56)</td>
<td>Wireless</td>
<td>Advanced Settings</td>
<td>all fields</td>
<td></td>
</tr>
<tr>
<td>wireless2p4AccessControl(57)+</td>
<td>Wireless</td>
<td>MAC Control</td>
<td>all fields</td>
<td></td>
</tr>
<tr>
<td>wireless2p4Bridging(58)+</td>
<td>Wireless</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>wireless2p4Wmm(59)</td>
<td>Wireless</td>
<td>QoS</td>
<td>Quality of Service</td>
<td>WMM Support</td>
</tr>
<tr>
<td>wireless2p4AckEnable(60)</td>
<td>Wireless</td>
<td>QoS</td>
<td>Quality of Service</td>
<td>No ACK</td>
</tr>
<tr>
<td>Bitmap</td>
<td>Top tab</td>
<td>Bottom tab</td>
<td>Section</td>
<td>Field(s)/Pop-ups</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------</td>
<td>------------------</td>
<td>------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>wireless5Enable(61)**</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>wireless5ABGNMode(62) **</td>
<td>Wireless</td>
<td>Radio Settings</td>
<td>Network Mode</td>
<td></td>
</tr>
<tr>
<td>wireless5SSID(63) **</td>
<td>Setup</td>
<td>Quick Setup</td>
<td>Wireless Network</td>
<td>Network Name (SSID)</td>
</tr>
<tr>
<td></td>
<td>Wireless</td>
<td>Radio Settings</td>
<td></td>
<td>Network Name (SSID)</td>
</tr>
<tr>
<td>wireless5BroadcastSSID(64) **</td>
<td>Wireless</td>
<td>Radio Settings</td>
<td>SSID Broadcast</td>
<td></td>
</tr>
<tr>
<td>wireless5Channel(65) **</td>
<td>Wireless</td>
<td>Radio Settings</td>
<td>Channel</td>
<td></td>
</tr>
<tr>
<td>wireless5ChannelWidth(66) **</td>
<td>Wireless</td>
<td>Radio Settings</td>
<td>Channel Width</td>
<td></td>
</tr>
<tr>
<td>wireless5Security(67) **</td>
<td>Wireless</td>
<td>Wireless Security</td>
<td>All fields</td>
<td></td>
</tr>
<tr>
<td>wireless5Wps(68) **</td>
<td>Wireless</td>
<td>WPS</td>
<td>all fields</td>
<td></td>
</tr>
<tr>
<td>wireless5Advanced(69) **</td>
<td>Wireless</td>
<td>Advanced Settings</td>
<td>All fields</td>
<td></td>
</tr>
<tr>
<td>wireless5AccessControl(70) ** +</td>
<td>Wireless</td>
<td>MAC Control</td>
<td>All fields</td>
<td></td>
</tr>
<tr>
<td>wireless5Bridging(71) ** +</td>
<td>Wireless</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>wireless5Wmm(72) **</td>
<td>Wireless</td>
<td>QoS</td>
<td>Quality of Service</td>
<td>WMM Support</td>
</tr>
<tr>
<td>wireless5AckEnable(73) **</td>
<td>Wireless</td>
<td>QoS</td>
<td>Quality of Service</td>
<td>No ACK</td>
</tr>
<tr>
<td>ping(74)</td>
<td>Administration</td>
<td>Diagnostics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>igmpProxy(75)</td>
<td>Administration</td>
<td>Management</td>
<td>IGMP Proxy</td>
<td>IGMP</td>
</tr>
</tbody>
</table>

* - 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 only up to bit 76).

Examples:
- \text{tchCmWebAccessReadPages} = 0x10000000000000000000 \\
\text{tchCmWebAccessWritePages} = 0x10000000000000000000 \\
This would mean only bit 3 (docsisLog) is enabled (0001).

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

- \text{tchCmWebAccessReadPages} = 0xfffffffffffffffc0 \\
\text{tchCmWebAccessWritePages} = 0xfffffffffffffffc0 \\
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;
    GenericTLV1lvCode 202 TlvLength 3 TlvValue0x010103
    SNMPv1v2cCoexistence
    {
        SNMPv1v2cCommunityName public;
        SNMPv1v2cTransportAddrAccess
        {
            SNMPv1v2cTransportAddr 0x0000000000000000;
            SNMPv1v2cTransportAddrMask 0x0000000000000000;
        }
        SNMPv1v2cTransportAddrAccess
        {
            SNMPv1v2cTransportAddr 0x00000000000000000000000000000000;
            SNMPv1v2cTransportAddrMask 0x00000000000000000000000000000000;
        }
        SNMPv1v2cAccessViewType 2;
        SNMPv1v2cAccessViewName docsisManagerView;
    }
    SNMPv1v2cCoexistence
    {
        SNMPv1v2cCommunityName private;
        SNMPv1v2cTransportAddrAccess
        {
            SNMPv1v2cTransportAddr 0x00000000000000000000000000000000;
            SNMPv1v2cTransportAddrMask 0x00000000000000000000000000000000;
        }
        SNMPv1v2cAccessViewType 2;
        SNMPv1v2cAccessViewName docsisManagerView;
    }
}
GenericTLVTLVCode 81 TlvLength 254 TlvValue
0xEEBC3041FFFD0551CD17BB6C009104E66066EEE078AD44037363B9E9863AAE75CEF6575372201F5C4C17D631FB741B346A820F13F4149759924C71CE00C5B5B0FF170B54C916568B433BCA74FB301CBF7CAE2CB51AAE88EE42F6E2362D401B5F2743FBAD755BFBD0809C3A044BF0AF1B328197E179B85044C488EE889E9ED21BB68C12AF2F3BEF740B71F8EFA9160D0203010001A33B303930160603551D250101F040C30A0A60820B6010505703030F7063551D26301801680143147DE55A52F389F8FF8F9046D67DC32DA67300D6092A864886F70D0100B50003820180031306137DF2F92FE89DE641F711126C25225EC748A84C;

GenericTLVTLVCode 81 TlvLength 254 TlvValue
0x16F4134B55C1536174DD1A6503DF487D354376D79CCEAF7CF2701797252DE610356E8A2DAFC73D80917DD48133C8CF86137BDD7C330A23ED205DF8179821DE5E3080AC7587CE8C6E660618D49333F4E40BB93D1F38186C20A6306316DB93A0578F609307779795AC2BCE2E2B6260B3DD11903CB4D1D60738953019B54BF687298741A81E500743C92281B36C74BB4E41D76EC75B4F06B418A70EB5F8615EBBEB9A697DEF3D15742CA483021DC0A1687072C102C7F9313294F505D60E6A261246B0917989CB61352086CA4C7B6BE729E24B5E6A058B680BF46508195810EFEB7CD2F590E6FD6A43269FC5B1002CBF9B2548385232;

GenericTLVTLVCode 81 TlvLength 110 TlvValue
0xC51A002A3D4B5B6B27AB904A2DADA846C792EF04957E09F98EC0D0397A55223FC9D9653C6F186E16DB6B68FC58292EF2DB313048DE52A4F2FC961104A132A2242D39076F70AD7B139716F5EB3E1595B1D3EB6D42022D2258E328963DC23F839B4329A1003100; 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.3.6.1.4.1.46366.4292.78.1.1001.0 Integer 1; /*OID: .1.3.6.1.4.1.46366.4292.78.1.1001.0*/
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 0x6F5F3A9CDEFE69EA0C012AA1F5657C5*/
/*CmMic 0xE8E5074E80D73012808432D3783*/
16 Abbreviations and Acronyms

This guide uses the following terms:

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