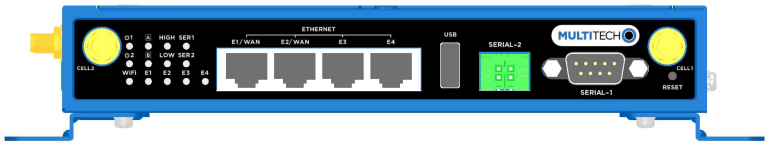
MULTITECH



rCell 500 R2 Series Router

User Guide

rCell 500 R2 Series Router User Guide

Model: MTR5-xxx.R2

Document Part Number: S000589 Rev 5.0

Copyright

Trademarks

Legal Notices

The MultiTech products are not designed, manufactured, or intended for use, and should not be used, or sold or re-sold for use, in connection with applications requiring fail-safe performance or in applications where the failure of the products would reasonably be expected to result in personal injury or death, significant property damage, or serious physical or environmental damage. Examples of such use include life support machines or other life preserving medical devices or systems, air traffic control or aircraft navigation or communications systems, control equipment for nuclear facilities, or missile, nuclear, biological, or chemical weapons or other military applications ("Restricted Applications"). Use of the products in such Restricted Applications is at the user's sole risk and liability.

MULTITECH DOES NOT WARRANT THAT THE TRANSMISSION OF DATA BY A PRODUCT OVER A CELLULAR COMMUNICATIONS NETWORK WILL BE UNINTERRUPTED, TIMELY, SECURE, OR ERROR FREE, NOR DOES MULTITECH WARRANT ANY CONNECTION OR ACCESSIBILITY TO ANY CELLULAR COMMUNICATIONS NETWORK. MULTITECH WILL HAVE NO LIABILITY FOR ANY LOSSES, DAMAGES, OBLIGATIONS, PENALTIES, DEFICIENCIES, LIABILITIES, COSTS, OR EXPENSES (INCLUDING WITHOUT LIMITATION REASONABLE ATTORNEYS FEES) RELATED TO TEMPORARY INABILITY TO ACCESS A CELLULAR COMMUNICATIONS NETWORK USING THE PRODUCTS.

MULTITECH DOES NOT WARRANT THAT THE TRANSMISSION OF DATA BY A PRODUCT OVER A WIRELESS COMMUNICATIONS NETWORK WILL BE UNINTERRUPTED, TIMELY, SECURE, OR ERROR FREE, NOR DOES MULTITECH WARRANT ANY CONNECTION OR ACCESSIBILITY TO ANY WIRELESS COMMUNICATIONS NETWORK. MULTITECH WILL HAVE NO LIABILITY FOR ANY LOSSES, DAMAGES, OBLIGATIONS, PENALTIES, DEFICIENCIES, LIABILITIES, COSTS, OR EXPENSES (INCLUDING WITHOUT LIMITATION REASONABLE ATTORNEYS FEES) RELATED TO TEMPORARY INABILITY TO ACCESS A WIRELESS COMMUNICATIONS NETWORK USING THE PRODUCTS.

The MultiTech products and the final application of the MultiTech products should be thoroughly tested to ensure the functionality of the MultiTech products as used in the final application. The designer, manufacturer, and reseller has the sole responsibility of ensuring that any end-user product into which the MultiTech product is integrated operates as intended and meets its requirements or the requirements of its direct or indirect customers. MultiTech has no responsibility whatsoever for the integration, configuration, testing, validation, verification, installation, upgrade, support, or maintenance of such end-user product, or for any liabilities, damages, costs, or expenses associated therewith, except to the extent agreed upon in a signed written document. To the extent MultiTech provides any comments or suggested changes related to the application of its products, such comments or suggested changes is performed only as a courtesy and without any representation or warranty whatsoever.

Disclaimers

Information in this document is subject to change without notice and does not represent a commitment on the part of Multi-Tech Systems, Inc. Multi-Tech Systems, Inc. provides this document "as is," without warranty of any kind, expressed or implied, including, but not limited to, the implied warranties of fitness or merchantability for a particular purpose. Multi-Tech Systems, Inc. may make improvements and/or changes in this manual or in the product(s) and/or the software described in this manual at any time.

Contents

1 About the rCell 500

This guide describes the rCell 500 R2 Series Router. The rCell R2 500 offers secure data communication between different types of devices. It features redundant power supplies and dual SIM capability for a more reliable connection

Package Contents

Contents	Quantity
rCell 500 R2	1
Power adapter	1
Power terminal block connector	1
Power blade	1
Wi-Fi antennas	2
Cellular antennas	2
Serial terminal block connector	1
Ethernet cable	1
Mounting brackets (wall mounting and DIN rail)	3
Rubber feet	4
Quick start guide	1

2 Safety Instructions

Operation Safety

CAUTION: Read all instructions and safety information before installing or using this device.

ATTENTION: Lisez toutes les instructions et consignes de sécurité avant d'installer ou d'utiliser cet appareil.

- Follow all local laws, regulations, and rules for operating a wireless device.
- Use the device security features to block unauthorized use and theft.
- Unless otherwise noted, antennas are not approved for outdoor use. Do not extend any antenna outside of any building, dwelling, or campus.
- Do not attempt to disassemble the device. There are no user-serviceable parts inside.
- Do not misuse the device. Follow instructions on proper operation and only use as intended. Misuse could make the device inoperable, damage the device or other equipment, or harm users.
- Do not apply excessive pressure or place unnecessary weight on the device. This could result in damage to the device or harm to users.
- Do not use this device in explosive or hazardous environments unless the model is specifically approved for such use. The device may cause sparks. Sparks in explosive areas could cause an explosion or fire that may result in property damage, severe injury, or death.
- Do not expose the device to any extreme environment where the temperature or humidity is high. Such exposure could result in damage to the device or cause a fire. See the device specifications for recommended operating temperature and humidity.
- Do not expose the device to water, rain, or other liquids. It is not waterproof. Exposure to liquids could result in damage to the device.
- Using accessories, such as antennas, that MultiTech has not authorized or that are not compliant with the device accessory specifications may invalidate the warranty.

If the device is not working properly, contact MultiTech technical support.

Power Supply Caution

CAUTION: Do not replace the power supply with one designed for another product; doing so can damage the modem and void your warranty. Adapter shall be installed near the equipment and shall be easily accessible.

ATTENTION: Pour garantir une protection continue contre les risques d'incendie, remplacez les fusibles uniquement par des fusibles du même type et du même calibre. L'adaptateur doit être installé à proximité de l'appareil et doit être facilement accessible.

VORSICHT: Ersetzen Sie das Netzteil nicht durch ein Netzteil, das für ein anderes Produkt vorgesehen ist. Andernfalls kann das Modem beschädigt werden und Ihre Garantie erlischt. Der Adapter muss in der Nähe des Geräts installiert und leicht zugänglich sein.

Vehicle Safety

When using your device in a vehicle:

- Do not use this device while driving.
- Respect local regulations on the use of cellular devices in vehicles.
- If incorrectly installed in a vehicle, operating the wireless device could interfere with the vehicle's electronics. To avoid such problems, use qualified personnel to install the device. The installer should verify that the vehicle electronics are protected from interference.
- Using an alert device to operate a vehicle's lights or horn is not permitted on public roads.
- UL evaluated this device for use in ordinary locations only. UL did *not* evaluate this device for installation in a vehicle or other outdoor locations. UL certification does not apply or extend to use in vehicles or outdoor applications.

Ethernet Ports

CAUTION: Ethernet ports and command ports are not designed to be connected to a public telecommunication network or used outside a building or campus.

⚠ **ATTENTION**: Les ports Ethernet et les ports de commande ne sont pas conçus pour être connectés à un réseau de télécommunication public ni utilisés à l'extérieur du bâtiment ou du campus.

FCC, EU, and Industry Canada RF Exposure Compliance

The antenna intended for use with this unit meets the requirements for mobile operating configurations and for fixed mounted operations, as defined in 2.1091 of the FCC rules for satisfying RF exposure compliance. This device also meets the European RF exposure requirements of EN 62311. If an alternate antenna is used, consult user documentation for required antenna specifications.

Compliance of the device with the FCC, EU, and IC rules regarding RF Exposure was established and is given with the maximum antenna gain as specified elsewhere in this document for a minimum distance of 20 cm between the devices radiating structures (the antenna) and the body of users. Qualification for distances closer than 20 cm (portable operation) would require recertification.

Wireless devices could generate radiation. Other nearby electronic devices, like microwave ovens, may also generate additional radiation to the user, causing a higher level of RF exposure.

Radio Frequency (RF) Safety

Due to the possibility of radio frequency (RF) interference, it is important that you follow any special regulations regarding the use of radio equipment. Follow the safety advice given below.

- Operating your device close to other electronic equipment may cause interference if the equipment is inadequately protected. Observe any warning signs and manufacturers' recommendations.
- Different industries and businesses restrict the use of cellular devices. Respect restrictions on the use of radio equipment in fuel depots, chemical plants, or where blasting operations are in process. Follow restrictions for any environment where you operate the device.

- Do not place the antenna outdoors.
- Turn off your wireless device when in an aircraft. Using portable electronic devices in an aircraft may endanger aircraft operation, disrupt the cellular network, and may be illegal. Failing to observe this restriction may lead to suspension or denial of cellular services to the offender, legal action, or both.
- Turn off your wireless device when around gasoline or diesel-fuel pumps and before filling your vehicle with fuel.
- Turn off your wireless device in hospitals and any other place where medical equipment may be in use.

Sécurité relative aux appareils à radiofréquence (RF)

À cause du risque d'interférences de radiofréquence (RF), il est important de respecter toutes les réglementations spéciales relatives aux équipements radio. Suivez les conseils de sécurité ci-dessous.

- Utiliser l'appareil à proximité d'autres équipements électroniques peut causer des interférences si les équipements ne sont pas bien protégés. Respectez tous les panneaux d'avertissement et les recommandations du fabricant.
- Certains secteurs industriels et certaines entreprises limitent l'utilisation des appareils cellulaires. Respectez ces restrictions relatives aux équipements radio dans les dépôts de carburant, dans les usines de produits chimiques, ou dans les zones où des dynamitages sont en cours. Suivez les restrictions relatives à chaque type d'environnement où vous utiliserez l'appareil.
- Ne placez pas l'antenne en extérieur.
- Éteignez votre appareil sans fil dans les avions. L'utilisation d'appareils électroniques portables en avion est illégale: elle peut fortement perturber le fonctionnement de l'appareil et désactiver le réseau cellulaires. S'il ne respecte pas cette consigne, le responsable peut voir son accès aux services cellulaires suspendu ou interdit, peut être poursuivi en justice, ou les deux.
- Éteignez votre appareil sans fil à proximité des pompes à essence ou de diesel avant de remplir le réservoir de votre véhicule de carburant.
- Éteignez votre appareil sans fil dans les hôpitaux ou dans toutes les zones où des appareils médicaux sont susceptibles d'être utilisés.

Interference with Pacemakers and Other Medical Devices

Radio frequency energy (RF) from cellular devices can interact with some electronic devices. This is electromagnetic interference (EMI). The FDA helped develop a detailed test method to measure EMI of implanted cardiac pacemakers and defibrillators from cellular devices. This test method is part of the Association for the Advancement of Medical Instrumentation (AAMI) standard. This standard allows manufacturers to ensure that cardiac pacemakers and defibrillators are safe from cellular device EMI.

The FDA continues to monitor cellular devices for interactions with other medical devices. If harmful interference occurs, the FDA will assess the interference and work to resolve the problem.

Precautions for Pacemaker Wearers

If EMI occurs, it could affect a pacemaker in one of three ways:

- Stop the pacemaker from delivering the stimulating pulses that regulate the heart's rhythm.
- Cause the pacemaker to deliver pulses irregularly.
- Cause the pacemaker to ignore the heart’s own rhythm and deliver pulses at a fixed rate.

Based on current research, cellular devices do not pose a significant health problem for most pacemaker wearers. However, people with pacemakers may want to take simple precautions to be sure that their device doesn't cause a problem.

- Keep the device on the opposite side of the body from the pacemaker to add extra distance between the pacemaker and the device.
- Avoid placing a turned-on device next to the pacemaker (for example, don’t carry the device in a shirt or jacket pocket directly over the pacemaker).

3 Specifications

MTR5-LEU2

Category	Description
General	
Performance	LTE, WCDMA, GSM/GPRS/EDGE
Frequency Bands	MTR5-LEU2-B04.R2 ▪ 4G-LTE/FDD: B1, B3, B7, B8, B20, B28A, TDD: B38, B40, B41 ▪ 3G-WCDMA: B1, B8 ▪ 2G-GSM/GPRS/EDGE Band: 900/1800 MHz
	MTR5-L12G2-B04.R2 ▪ 4G-LTE/TDD: B42, B43, B48 (CBRS)
Radio	
Cellular	MTR5-LEU2-B04.R2 - 4G LTE Radio with 3G/2G fallback
	MTR5-L12G2-B04.R2 – 4G LTE only Radio with CBRS band
Wi-Fi	802.11 b/g/n/a/ac
4G Speed	
Packet Data[1]	MTR5-LEU2-B04.R2: Up to 150 Mbps downlink / 50 Mbps uplink
	MTR5-L12G2-B04.R2: Up to 300 Mbps downlink / 50 Mbps uplink
SMS	
SMS	Point-to-Point Messaging
	Mobile-Terminated SMS
	Mobile-Originated SMS
Connectors	
Cellular	Two Female SMA connectors for cellular
Wi-Fi	Two Reverse polarity male SMA connector for Wi-Fi
SIM Holder	Two Mini-SIM 2FF, standard 1.8 V and 3 V SIM receptacle
Power Requirements	
Voltage	9 V to 48 VDC
Physical Description	
Dimensions	187mm x 110mm x 31mm
Weight	0.72Kg
Environment	
Operating Temperature[2]	-20° C to +60° C

Category	Description
Humidity	Relative humidity 15% to 93% non-condensing
Certifications, Compliance, Warranty	
EU Compliance	CE RED Radio (MTR5-LEU2-B04.R2 model only)
Safety Compliance	IEC 60950-1 (MTR5-LEU2-B04.R2 model only)
Network Compliance	GCF (MTR5-LEU2-B04.R2 model only)
FCC Compliance	FCC Part 15 and Part 96 CBRS (MTR5-L12G2-B04.R2 model only)
Warranty	Two years

[1]The radio's performance may be affected at the temperature extremes. This is considered normal. There is no single cause for this function. It is the result of an interaction of several factors, such as the ambient temperature, the operating mode, and the transmit power.

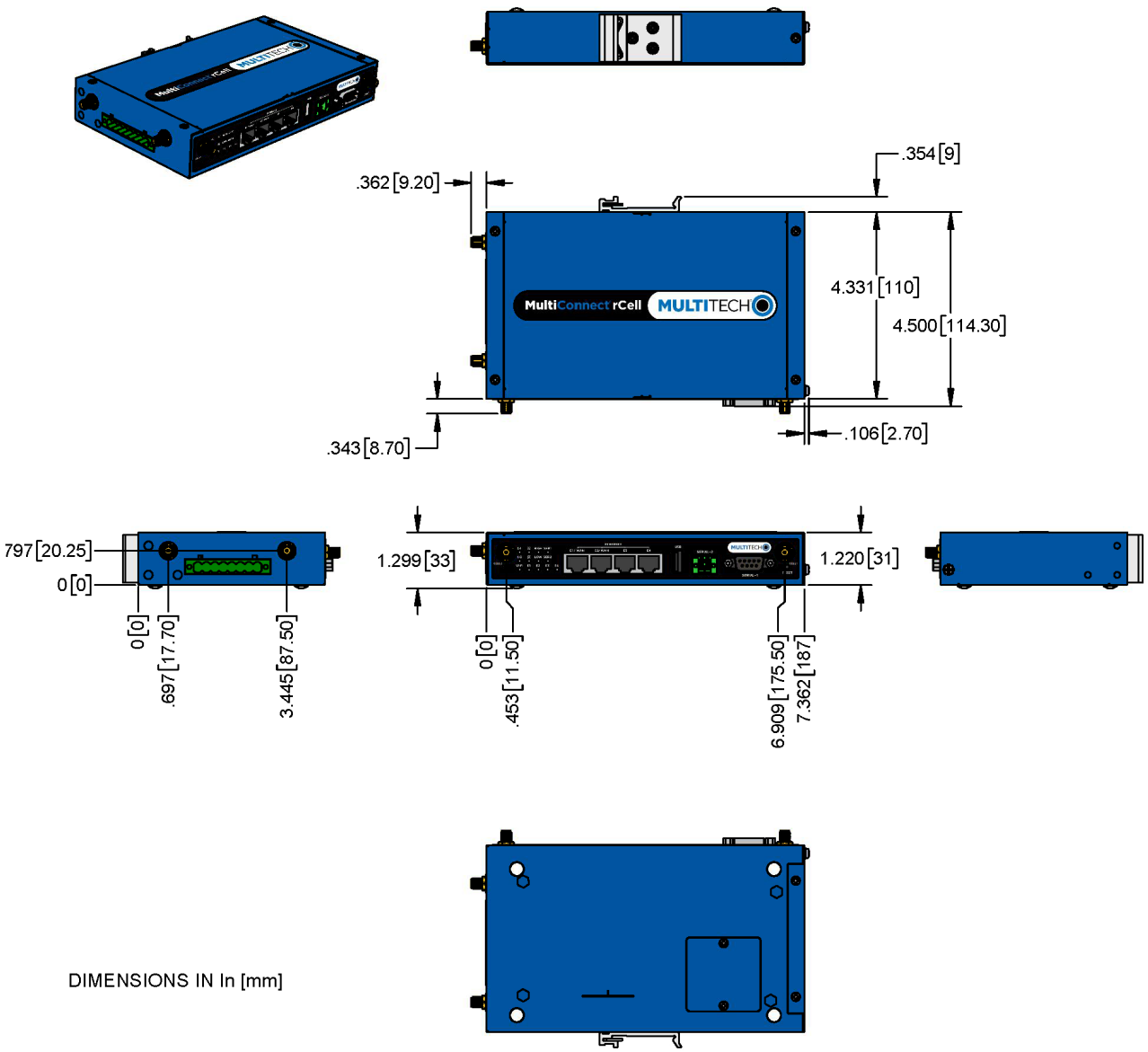
[2]UL Recognized @0° C to 40° C, Limited by DC Power Supply.

RF Specifications

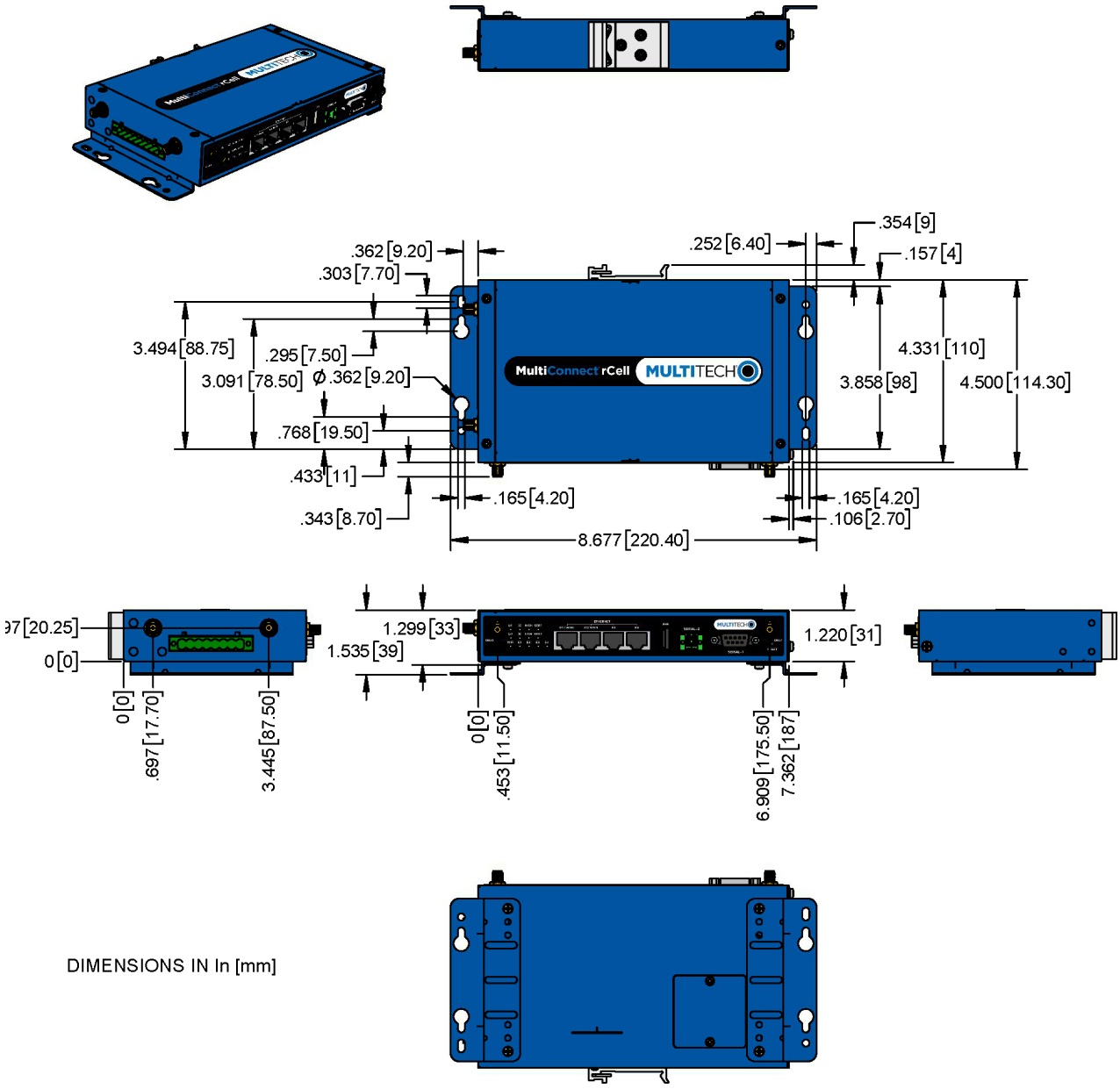
Operating Band	Tx	Rx
UMTS Band 1	1920 MHz - 1980 MHz	2110 MHz - 2170 MHz
UMTS Band 8	880 MHz - 915 MHz	925 MHz - 960 MHz
GSM 900	880 MHz - 915 MHz	925 MHz - 960 MHz
GSM 1800 (DCS)	1710 MHz - 1785 MHz	1805 MHz - 1880 MHz
LTE Band 1	1920 MHz - 1980 MHz	2110 MHz - 2170 MHz
LTE Band 3	1710 MHz - 1785 MHz	1805 MHz - 1880 MHz
LTE Band 7	2500 MHz - 2570 MHz	2620 MHz - 2690 MHz
LTE Band 8	880 MHz - 915 MHz	925 MHz - 960 MHz
LTE Band 20	832 MHz - 862 MHz	791 MHz - 821 MHz
LTE Band 28A	703MHz - 748 MHz	758MHz - 803 MHz
LTE Band 38	2570 MHz – 2620 MHz	2570 MHz – 2620 MHz
LTE Band 40	2300 MHz – 2400 MHz	2300 MHz – 2400 MHz
LTE Band 41	2496 MHz – 2690 MHz	2496 MHz – 2690 MHz
LTE Band 42	3400MHz - 3600 MHz	3400MHz - 3600 MHz
LTE Band 43	3600MHz - 3800 MHz	3600MHz - 3800 MHz
LTE Band 48	3550MHz - 3700 MHz	3550 MHz - 3700 MHz

Device Dimensions

The device dimensions in millimeters (mm).



The device dimensions with mounting brackets in millimeters (mm).



DIMENSIONS IN In [mm]

System Requirements

Network Requirements	▪ An Ethernet RJ-45 cable or DSL modem ▪ 4G cellular service subscription ▪ 802.11 b/g/n/a/ac Wi-Fi wireless ▪ Ethernet connection

Configuration Utility Requirements	▪ Operating System Requirements
	  ▪ Windows®10 or higher
	  ▪ Macintosh OS
	  ▪ Linux-based operating system
	▪ Browser Requirements
	  ▪ Microsoft Edge
	  ▪ Chrome
	  ▪ Firefox
	  ▪ Safari

LED Indicators

Indicator	Label	Description
Power Source 1		**Continuously ON:** Device is powered by source 1.
Power Source 2		**Continuously ON:** Device is powered by source 2. **Note:** If both power source 1 and 2 are connected, the device chooses power source 1 first. In this instance, the LED for power source 2 remains OFF.
WLAN (Wi-Fi)	**WIFI**	**Continuously ON:** Wi-Fi radio is enabled. **Flashing:** Data packets are being transferred.
		OFF: Wi-Fi radio is disabled.
SIM A		**Continuously ON:** SIM A is in use. **Flashing:** SIM card detected.
SIM B		**Continuously ON:** SIM B is in use. . **Flashing:** SIM card detected
LAN1 - LAN 4	**E1 - E4**	**Continuously ON:** Ethernet connection is established. **Flashing:** Data packets are being transferred.
High Cellular Signal	**HIGH**	**Continuously ON:** Strong cellular signal strength.
Low Cellular Signal	**LOW**	**Continuously ON:** Weak cellular signal strength.
USB	**USB CELL**	**Continuously ON:** USB device is attached.
Serial Port 1	**SER1**	**Continuously ON:** TCP connection is active. **Flashing:** Serial data is being transferred.
Serial Port 2	**SER2**	**Continuously ON:** TCP connection is active **Flashing:** Serial data is being transferred.

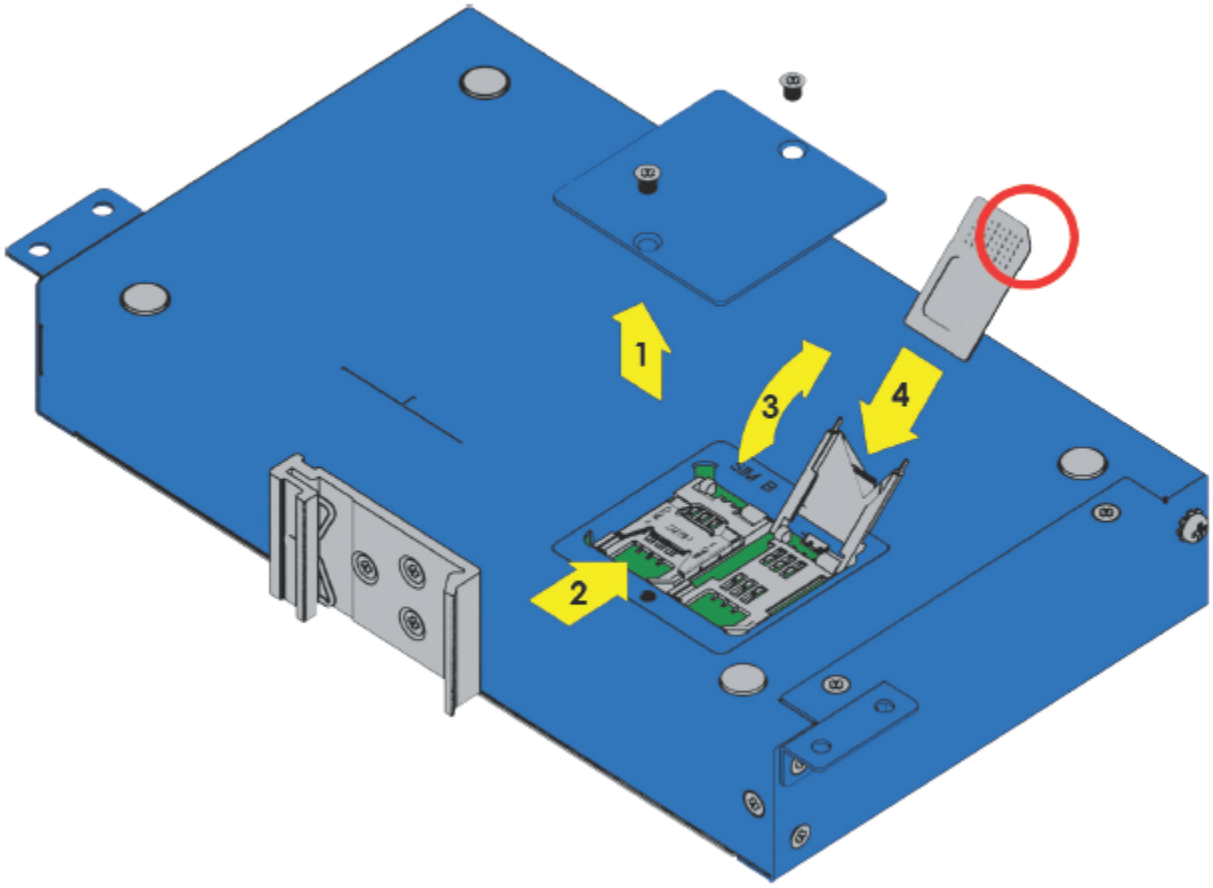
Using DeviceHQ for Device Management

DeviceHQ is a cloud-based device management tool for remote monitoring, upgrades, and configuring devices. For information on creating and using a DeviceHQ account, go to the http://www.multitech.net/developer/software/devicehq/.

Note: **If you are not using DeviceHQ** as the management system, disable DeviceHQ as the management system within the software. Once the Setup Wizard has been completed, from the left menu select **Basic Network > System Management** then deselect the "Enable" box on the top row of the configuration table.

4 Installation

Installing SIM Cards



The SIM card slots are located on the bottom of the device.

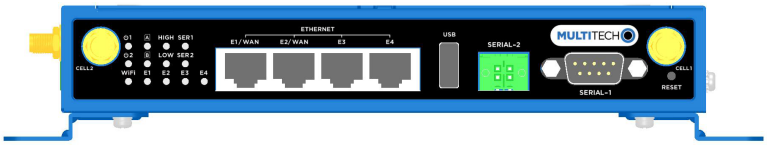
Note: Before installing or changing the SIM card, make sure the device is turned OFF and power is disconnected.

1. Unscrew and remove SIM card cover.
2. Slide SIM card socket toward hinge to unlock.
3. Lift up SIM holder and insert SIM card, making sure notch is lined up correctly.
4. Lay SIM holder down.
5. Slide SIM socket away from hinge to lock.
6. Replace SIM card cover.

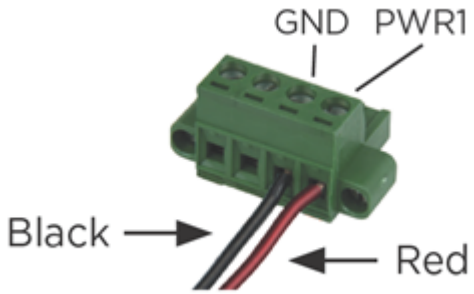
Attaching Cables and Antennas

1. Attach 4G antennas.
   - For the **MTR5-LEU2-B04.R2**: Attach 4G antennas to the device's front panel by screwing them into the designated connectors.
   - For the **MTR5-L12G2-B04.R2**: Attach 4G antennas to the device's right-side panel by screwing them into the designated connectors.
2. Attach Wi-Fi antennas to the device's left-side panel by screwing them into the designated connectors.
3. Attach cables to their corresponding ports on the device's front panel.

   Note: During configuration use ports E2 to E4 only. **DO NOT attach Ethernet cable to E1/WAN port.**



4. Attach red wire on the power cable to PWR1 and the black wire to the GND for PWR1 on the power port on the device's side panel.


GND
PWR1
Black
Red

Using Setup Wizard

If you are using a 3G/4G network, verify SIM card has been installed before starting setup. Configure this device using the web UI. To access the web UI, enter the IP Address into your browser. The default IP Address is 192.168.2.1. If this has been changed, type in the new IP Address. On the login page, type the administrator password and click **Login**.

Note: The default administrator username and password are **admin**. During the first login, the system requires you to set a new password.

After logging in, select the appropriate language. From the menu on the left, click **Wizard**.

1. To start the Wizard, click **Next**.
2. Change the web UI login password. Click **Next**. (We strongly recommend changing the default password.)
3. Select the correct **Time Zone**. Click **Next**. If auto detection does not work, click **Detect Again**, and select manually.
4. Select the WAN type and address. For fixed line, choose **Ethernet WAN**. Click **Next**.
    - If you select **Ethernet (Static IP Address)**, input all your ISP-provided addresses (fixed IP address). Click **Next**.
    - If you select **Ethernet (Dynamic IP Address)**, leave input blank if not required. If your ISP requires input, enter host name or registered MAC addresses. Click **Next**.
    - If you select **Ethernet (PPPoE or PPP over Ethernet)**, input account and password from your ISP. Use for ADSL for WAN connection. Click **Next**.
    - If you select **Ethernet (PPTP)**, input dial-up information if your ISP requests it. Click **Next**.
    - If you select **Ethernet (L2TP)**, input dial-up information if your ISP requests it. Click **Next**.
    - If you select **3G/4G** , choose **Auto-Detection** or **Manual Configuration** and enter 3G/4G network settings. Click **Next**
5. Enter **LAN IP address** and **Subnet Mask**. Click **Next**.
6. Setup Wi-Fi connection. Change the gateway's **SSID**, **Channel Number**, **Authentication**, and **Encryption Algorithm**. We strongly recommend adding authentication and encryption for security. Otherwise, accept the default settings. Click **Next**.
7. Verify the new Wi-Fi settings are correct. Click **Apply**.
8. Click **Apply** and **Restart**.

VPN Setup Wizard

The VPN setup wizard guides you step by step in creating profiles for IPSec, PPTP, or L2TP VPN connections. IPSec and GRE are each able to support up to 16 connections.

1. To start setup, click **Next**.
2. Select **VPN connection**. Choose **IPSec**, **PPTP**, **L2TP**, or **GRE**. Click **Next**.

- If you choose **IPSec,** select **Site to Site** for office to office or **Dynamic VPN** for remote access to office. For other options, go to **Advanced Network > VPN**. Input required network information. Click **Next**.
- If you choose **PPTP**, select **Client** to connect device to another PPTP server or **Server** to have other PPTP clients connect to the device. Click **Next**.
  - If you choose **PPTP Client**, enter tunnel name, IP/FQDN of PPTP server, username/password, authentication, and MPPE options. Verify these settings are accepted by the PPTP server or it will reject the connection. Click **Next**.
  - If you choose **PPTP Server**, selection options for authentication and MPPE. Create username and password for one PPTP client. To create additional usernames and passwords, select **Advanced Network > VPN > PPTP** to add more. Click **Next**.
- If you choose **L2TP**, select from **Client** for the device to connect to another L2TP server or **Server** for other L2TP clients to connect to the device. Click **Next**.
  - If you choose **L2TP Client**, enter tunnel name, IP/FQDN of L2TP server, username/password, authentication, and MPPE options. Verify that the L2TP server accepts these settings or it will reject the connection. Click **Next**.
  - If you choose **PPTP Server**, selection options for authentication and MPPE. Create username and password for one L2TP client. To create additional usernames and passwords, select **Advanced Network > VPN > L2TP** to add more. Click **Next**.

  If you choose **GRE**, enter GRE tunnel name, remote IP address, key and default gateway/remote subnet. Click **Next**.

3. Verify all settings are correct. Click **Apply**.

Status

The status window shows different kinds of system status: Network Status, Wi-Fi Status, LAN Client List, Firewall Status, VPN Status, and OpenVPN status.

Network Status

- **WAN Interface IPv4 Network Status:** This shows the current status of all the WAN interfaces that are set up with IPv4 addresses. Click **Edit** to configure the WAN internet settings.
- **WAN Interface IPv6 Network Status:** This shows the current status of all the WAN interfaces that are set up with IPv6 addresses. Click **Edit** to configure the WAN IPv6 settings.
- **LAN Interface Status:** This shows the current status of the LAN interface. Click **Edit** IPv4 or IPv6 to configure LAN interface settings.
- **3G/4G Modem Status:** This shows the current status of the 3G/4G mobile WAN interfaces. Click **Details** to view details of the cellular radio and network information. Click **Scan** button to perform Cellular site survey. This takes a minimum of five minutes to perform. Avoid any interruption when site survey is in progress. Click **Lite View, Full View, or Download** to see the cellular site survey scan results. Only newer hardware will have the Cellular site survey feature.

- **Internet Traffic Statistics:** This shows the amount of data being sent and received on all the WAN interfaces.
- **Data Usage Monitoring:** This shows the amount of data being sent and received periodically on 3G/4G mobile WAN interface.

Wi-Fi Status

- **Wi-Fi Virtual AP List:** This shows the current status of all the Virtual Wi-Fi access point. Click **Edit** to configure the virtual Wi-Fi access point settings.
- **Wi-Fi Traffic Statistics:** This shows the amount of data being sent and received on all the virtual Wi-Fi access point. Click **Refresh** to see the latest amount of data usage. Click **Reset** to start counting data from 0.

LAN Client List

- **LAN Client List:** This shows a list of all the current Ethernet and Wi-Fi client devices that are detected and active on the LAN and Wi-Fi interfaces.

Firewall Status

- **Packet Filters:** This shows all the detected contents that match with configured packet filter rules that have logging alert enabled. Click **Edit** to configure packet filter settings.
- **URL Blocking:** This shows all the detected contents that match with configured URL blocking rules that have logging alert enabled. Click **Edit** to configure URL blocking settings.
- **MAC Control:** This shows all the blocked MAC addresses that match with configured MAC Control rules that have logging alert enabled. Click **Edit** to configure MAC control settings.
- **IPS:** This shows all the detected contents that match with configured IPS (Intrusion Prevention System) rules that have logging alert enabled. Click **Edit** to configure IPS settings.
- **Options:** This shows status of Stealth Mode, SPI, Discard Ping from WAN, and Remote Administrator Management. Click **Edit** to configure settings.

VPN Status

- **IPSec Status:** This shows the status of all the active VPN IPSec tunnels. Click **Edit** to configure VPN IPsec settings.
- **OpenVPN Client Status:** This shows the status of all the active OpenVPN Client tunnels. Click **Edit** to configure OpenVPN Client settings.
- **OpenVPN Server Status:** This shows the status of all the active OpenVPN Server tunnels. Click **Edit** to configure OpenVPN Server settings.
- **L2TP Server Status:** This shows the status of all the active VPN L2TP Server tunnels. Click **Edit** to configure VPN L2TP Server settings.
- **L2TP Client Status:** This shows the status of all the active VPN L2TP Client tunnels. Click **Edit** to configure VPN L2TP Client settings.
- **PPTP Server Status:** This shows the status of all the active VPN PPTP Server tunnels. Click **Edit** to configure VPN PPTP Server settings.
- **PPTP Client Status:** This shows the status of all the active VPN PPTP Client tunnels. Click **Edit** to configure VPN PPTP Client settings.

5 Basic Network

Basic Network

WAN Setup

This device has three WAN interfaces to support different WAN connections. Configure these individually to maximize Internet connection setup.

- **Ethernet WAN:** Configure the **E1 or E2 Ethernet port** as a WAN. To setup, plug in the Ethernet cable from an external modem and follow UI setup.
- **Internal 3G/4G WAN:** There is one 3G/4G built-in modem. Check that the power is off before removing or inserting the SIM card. To set up, insert SIM card and follow UI setup.
- **Wi-Fi WISP WAN:** You can configure Wi-Fi as a client to connect to an external Wi-Fi access point. Follow the UI setup.

Physical Interface

Click **Edit** for each WAN interface to view the detailed physical interface settings. This interface allows you to configure the settings.

- **WAN 1:** This interface is in **Always On** mode and is the primary Internet connection. Click **Edit** to configure interface settings. This WAN 1 link is used as highest priority when handling outbound traffic.
- **WAN 2:** This interface is disabled by default. Click **Edit** to configure. There are three operation options for this interface. This WAN 2 link is used as second highest priority when handling outbound traffic.
- **WAN 3:** This interface is disabled by default. Click **Edit** to configure. There are three operation options for this interface. This WAN 3 link is used as lowest priority when handling outbound traffic.

Each WAN Physical interface can be configured as Ethernet, internal 3G/4G, external USB 3G/4G, or Wi-Fi client.

View WAN Interface

1. Select **WAN interface** from the available list. WAN items include **Ethernet**, **3G/4G**, and **Wi-Fi**.
    - To use RJ45 port as primary internet connection, select **Ethernet**.
    - To use embedded 3G/4G modem as primary internet connection, select **3G/4G**.
    - To use the MTD-H5 as primary internet connection, select **USB 3G/4G**.
    - To use Wi-Fi as primary internet connection, select **Wi-Fi**.
2. Operation mode includes three options:
    - **Always on:** Set this to be active all the time. Two or more internet connections are established simultaneously. Outgoing data will be transferred through these connections based on load balance policies. This mode is suitable for high bandwidth requirements such as video streaming.

- **Failover:** Set this to be a backup WAN connection. This WAN interface won't be active until other connections have failed. You must specify both the failover or primary connection and the fallback or backup connection. (For example, if WAN-1 connection is broken, the gateway tries to failover the connection to WAN-2 automatically. When WAN-1 connection becomes available again, the internet connection switchws back to WAN-1 automatically. This gateway supports seamless failover to shorten switch time between WAN interface failover and fallback. If an interface serves as a seamless failover WAN, the WAN connection will be activated after the system has operated normally, even without data flow in it. When the primary connection is broken, fast switching data flow to the WAN interface is the major concern for seamless failover.)

  Note: Your ISP will charge the connection fee even if **Operation mode** is set to seamless failover.

- **Disable:** Deactivate this WAN interface.

3. **VLAN Tagging:** If your ISP requires a VLAN tag to be inserted into the WAN packets, enable this setting. Input the specified tag value. Click **Save**.

Operation Mode	Description
Always-On	WAN 1 and 2 connect at the same time. Two internet connections are established simultaneously and outgoing data is transferred through both based on load balance policies.
Failover	If the WAN 1 connection is broken, the device will failover to WAN 2 automatically. When the WAN 1 connection is reestablished, the connection automatically switches back to WAN 1.
Disable	Disables WAN 2 or 3.

Internet Setup

You must configure **Internet Setup** for each physical interface. There are three WAN interfaces that you can setup individually. These interfaces support an ISP that provides LTE, WCDMA, GSM data services, and Wi-Fi, xDSL or cable connections with Dynamic IP, Static IP, PPPoE, PPTP, and L2TP connection types.

WAN Type	Description
3G/4G	Supports LTE/3G/2G depending on specifications. **Note:** If the data plan is not a flat rate, set the **Connection Control** mode to **Connect-on-Demand** or **Manual**.
Dynamic IP Address	Use for cable modem or fiber optic (VDSL) modem. Assigned IP Address is different with each connection.
Static IP Address	Use when you receive a fixed IP Address.
PPP over Ethernet (PPPoE)	Widely used for ADSL connections.
PPTP	This WAN requires the ISP to host a PPTP server.
L2TP	This WAN requires the ISP to host an L2TP server.

Internet Setup for 3G/4G WAN

To configure **3G/4G WAN settings**, Click **Edit** .

1. **WAN Type:** Choose **3G/4G** from the drop-down list.
2. **Preferred SIM Card:** Choose from options: **SIM-A, SIM-B, SIM-A First,** or **SIM-B First** for **3G/4G connection**. This device has two SIM card slots with four options. **SIM-A First** is default and used to connect to the mobile system for data transferring. The device tries to connect using the SIM-A card first. If the connection is broken, the device switches to SIM-B card automatically. The system will not switch back to SIM-A card unless the SIM-B connection is also broken. Either continues for data transferring when current connection is still alive. The same conditions apply for **SIM-B First** option. For **SIM-A** or **SIM-B**, the specified SIM card is the only one used for negotiation parameters between the device and mobile base station. Find SIM Configuration for all options beneath the **3G/4G WAN Type** configuration window.
3. **Dial-up Profile:** Use information given by your 3G/4G data service provider to setup connection including APN, dialed number and account or password. Choose from **Manual-configuration** or **Auto-detection** for profile. If you choose **SIM-A First** or **SIM-B First** for **Preferred SIM Card**, input dial-up profile for SIM-A and SIM-B respectively.
4. **PIN Code:** If your card needs to be unlocked before making a data connection, enter the SIM card PIN code.
5. **Account, Password:** Enter the ISP-provided Account/Password.
6. **Authentication:** Choose **Auto**, **PAP**, or **CHAP** according to your ISP's authentication approach. Use **Auto** if unsure.
7. **Primary/Secondary DNS:** Enter IP address of Domain Name Server. Most ISPs assign them automatically.
8. **Roaming:** Enables or disables roaming on cellular data network.
9. **Data Usage Monitor:** Controls how much data is allowed for the 3G/4G connection during a defined period. This avoids data overage charges from your ISP.
10. **Connection Control:** Set WAN connection to be **Always On**, **Connect On Demand**, or **Connect Manually**.
11. **Time Schedule:** Set WAN connection to be active for a certain period. Select **Always** available or **By Schedule** for connection method. If you choose **By Schedule**, add a new schedule at **System > Scheduling**.
12. **MTU:** Maximum Transmit Unit. Different WAN connections have different values. If unsure, use default value of 0 (Auto).
13. **NAT:** Enables or disables NAT mechanism between LAN and WAN interfaces. Default is enabled.
14. **AT Command:** Enables or disables AT command mode via TCP port. Cellular connection will be inactive in this mode
15. **Init String 1 to 4:** Set up extra custom AT command string sent to internal LTE radio before making data connection.
16. **Cellular consecutive fails times:** Number of times that it fails to obtain cellular connection will cause modem to auto reset/restart.

17. **Network Monitoring (keep alive):** Monitor WAN interface connection status. As a result, the system can prevent the embedded cellular radio from auto-timeout and disconnects after a period of inactivity. Check **Enable**.
18. **Data Load Check:** If there is no data activity on the WAN link for a configured period, it will automatically reset and reconnect on the cellular WAN link.
19. **Check Interval:** Indicate how often to send keep alive packet or to perform data load check.
20. **Target1/Target2:** Set host for keep alive checking including **DNS1, DNS2,** or **Other** host (input IP address manually).
21. **System Watchdog:** Monitor overall WAN connection and auto reboot when WAN connection detected with no reply from keep alive check.
22. **IGMP:** Enable or disable multicast traffic. Choose Auto mode or select by the option list of **IGMP v1, IGMP v2, IGMP v3,** and **Auto**.
23. **WAN IP Alias:** Some ISPs will provide another fixed IP address for management purposes. Enter this IP address.
24. **Network Scan Configuration (only available on certain devices):** Set up 3G/LTE cellular network scan (usually automatic). Manual scan is used for problem diagnosis.
25. Select **Network Status** from the list.
    a. **Physical Interface:** Indicate which 3G/LTE modem is used for network scan. **SIM Status** indicates which SIM card is used for Network Scan.
    b. **Network Type:** Set network scan type. You can choose **2G only or prefer, 3G only or prefer, LTE only or prefer**, or **Auto**.
    c. **Scan Approach:** Choose **Auto**, or **Manually**. If you choose **Manually**, click **Scan** to scan cellular network nearby and select your network provider. Click **Apply**.

Note: Incorrect settings may cause 3G/LTE connection problems.

Internet Setup for Ethernet WAN

1. To access Ethernet WAN settings, click **Internet Setup**.
2. Click **Edit** next to the Ethernet WAN you want to configure.
3. WAN types available are **Dynamic IP**, **Static IP**, **PPPoE**, **PPTP**, and **L2TP**.

Static IP

Use this option if your ISP provides a fixed IP address. Enter the ISP-provided IP address, subnet mask, and gateway address. The device rejects IP addresses that are not in the correct format.

1. **WAN IP Address:** Enter the provided IP Address.
2. **WAN Subnet Mask:** Enter the provided subnet mask.
3. **WAN Gateway:** Enter the provided gateway address.
4. **Primary DNS:** Enter the primary DNS IP Address.
5. **Secondary DNS:** Enter the secondary DNS. This can be left blank if your ISP doesn't supply one.

6. **MTU:** The default value is 0 (Auto).
7. **NAT:** Check to enable. If you enable, there will be no NAT mechanism between the LAN and WAN.
8. **Network Monitoring (keep alive):** Monitor WAN interface connection status. As a result, the system can prevent the WAN connection from auto-timeout and disconnects after a period of inactivity. Check **Enable**.
9. **Data Load Check:** If there is no data activity on the WAN link for a configured period, it will automatically reset and reconnect on the mobile WAN link.
10. **Check Interval:** Indicate how often to send keep-alive packet or to perform data load check.
11. **Target1/Target2:** Set host for keep alive checking including **DNS1, DNS2,** or **Other** host (input IP address manually).
12. **System Watchdog:** Monitor overall WAN connection and auto reboot when WAN connection detected with no reply from keep alive check.
13. **IGMP:** Choose **Enable** or **Disable** the IGMP snooping function. When enabled, the device detects all IGMP exchanged messages. This prevents multicast flooding on an Ethernet link.
14. **WAN IP Alias:** Some ISPs provide a fixed IP address for management purposes. If so, enter this address.

Dynamic IP

To configure a Dynamic IP the following fields are available:

1. **Host Name:** This field is optional. It may be required by some ISPs.
2. **ISP Registered MAC address:** Enter the registered MAC address or click **Clone** to copy your PC's MAC address.
3. **Connection Control:** Select the connection control scheme from the list. Options are: **Auto-Reconnect (Always on), Connect-on-Demand, and Connect Manually**.
4. **MTU:** The default value is 0 (Auto).
5. **NAT:** Check to enable. If you enable, there will be no NAT mechanism between the LAN and WAN.
6. **Network Monitoring (keep alive):** Monitor WAN interface connection status. As a result, the system can prevent the WAN connection from auto-timeout and disconnects after a period of inactivity. Check **Enable**.
7. **Data Load Check:** If there is no data activity on the WAN link for a configured period, it will automatically reset and reconnect on the mobile WAN link.
8. **Check Interval:** Indicate how often to send keep-alive packet or to perform data load check.
9. **Target1/Target2:** Set host for keep alive checking including **DNS1, DNS2,** or **Other** host (input IP address manually).
10. **System Watchdog:** Monitor overall WAN connection and auto reboot when WAN connection detected with no reply from keep alive check.
11. **IGMP:** Choose to **Enable** or **Disable** the IGMP snooping function. When enabled, the device will detect all IGMP exchanged messages. This prevents multicast flooding on an Ethernet link.

12. **WAN IP Alias:** Some ISPs provide a fixed IP address for management purposes. If so, enter this address.

PPP over Ethernet (PPPoE)

Select this option when your ISP requires a PPPoE connection. This is typically used for ADSL services.

1. **IPv6 Dual Stack:** Check to enable. Enable this option if your ISP provides one IPv4 and one IPv6 address.
2. **PPPoE Account:** Enter the ISP-provided account.
3. **PPPoE Password:** Enter the ISP-provided password.
4. **Primary DNS:** Enter the primary DNS IP Address.
5. **Secondary DNS:** Enter the secondary DNS IP Address. Can be left blank if your ISP doesn't supply one.
6. **Connection Control:** Select the connection control scheme from the list. Options are: **Auto-Reconnect (Always on), Connect-on-Demand, and Connect Manually**.
7. **Service Name:** Your ISP may provide you with a specific service name when connecting with PPPoE.
8. **Assigned IP Address:** Your ISP may provide you with a fixed IP address for this type of connection.
9. **MTU:** The default value is 0 (Auto).
10. **NAT:** Check to enable. If you enable, there will be no NAT mechanism between the LAN and WAN.
11. **Network Monitoring (keep alive):** Monitor WAN interface connection status. As a result, the system can prevent the WAN connection from auto-timeout and disconnects after a period of inactivity. Check **Enable**.
12. **Data Load Check:** If there is no data activity on the WAN link for a configured period, it will automatically reset and reconnect on the mobile WAN link.
13. **Check Interval:** Indicate how often to send keep-alive packet or to perform data load check.
14. **Target1/Target2:** Set host for keep alive checking including **DNS1, DNS2,** or **Other** host (input IP address manually).
15. **System Watchdog:** Monitor overall WAN connection and auto reboot when WAN connection detected with no reply from keep alive check.
16. **IGMP:** Choose to **Enable** or **Disable** the IGMP snooping function. When enabled, the device will detect all IGMP messaged exchanged. This prevents multicast flooding on an Ethernet link.
17. **WAN IP Alias:** Some ISPs will provide a fixed IP address for management purposes. If so, enter this address.

PPTP Client

Select Point-to-Point Tunneling Protocol (PPTP) when your ISP uses this type of connection. The ISP will provide you with a username and password.

1. **IP Mode:** Select the IP Mode assigned by your ISP. If you select **Static IP Address**, enter the ISP-provided IP address, subnet mask, and gateway IP.
2. **Server IP Address/Name:** The ISP-provided IP address of the PPTP server.
3. **PPTP Account:** Enter the ISP-provided account.
4. **PPTP Password:** Enter the ISP-provided password.
5. **Connection ID:** Enter the ISP-required connection ID (if required).
6. **Connection Control:** Choose the connection control scheme from the list. **Auto-Reconnect (Always on), Connect-on-Demand, and Connect Manually** are the available options.
7. **MTU:** The default value is 0 (Auto).
8. **MPPE:** Enable this option to add encryption on transferred and received data packets.
9. **NAT:** Check to enable. If enabled, there will be no NAT mechanism between the LAN and WAN.
10. **Network Monitoring (keep alive):** Monitor WAN interface connection status. As a result, the system can prevent the WAN connection from auto-timeout and disconnects after a period of inactivity. Check **Enable**.
11. **Data Load Check:** If there is no data activity on the WAN link for a configured period, it will automatically reset and reconnect on the mobile WAN link.
12. **Check Interval:** Indicate how often to send keep alive packet or to perform data load check.
13. **Target1/Target2:** Set host for keep alive checking including **DNS1, DNS2,** or **Other** host (input IP address manually).
14. **System Watchdog:** Monitor overall WAN connection and auto reboot when WAN connection detected with no reply from keep alive check.
15. **IGMP:** Choose to **Enable** or **Disable** the IGMP snooping function. When enabled, the device will detect all IGMP messaged exchanged. This prevents multicast flooding on an Ethernet link.
16. **WAN IP Alias:** Some ISPs will provide a fixed IP address for management purposes. If so, enter this address.

L2TP Client

Choose Layer 2 Tunneling Protocol (L2TP) if your ISP uses this type of connection. Your ISP will provide you with a username and password.

1. **IP Mode:** Select the IP Mode assigned by your ISP. If you select **Static IP Address**, enter the ISP-provided IP address, subnet mask, and gateway IP.
2. **Server IP Address/Name:** The ISP-provided IP address of the L2TP server .
3. **L2TP Account:** Enter the ISP-provided enter the account.
4. **L2TP Password:** Enter the ISP-provided password.
5. **Connection Control:** Select the connection control scheme from the list. Options are: **Auto-Reconnect (Always on), Connect-on-Demand, and Connect Manually**.
6. **MTU:** The default value is 0 (Auto).
7. **MPPE:** Enable this option to add encryption for transferred and received data packets.

8. **NAT:** Check to enable. If you enable, there is no NAT mechanism between the LAN and WAN.
9. **Network Monitoring (keep alive):** Monitor WAN interface connection status. As a result, the system can prevent the WAN connection from auto-timeout and disconnects after a period of inactivity. Check **Enable**.
10. **Data Load Check:** If there is no data activity on the WAN link for a configured period, it will automatically reset and reconnect on the mobile WAN link.
11. **Check Interval:** Indicate how often to send keep alive packet or to perform data load check.
12. **Target1/Target2:** Set host for keep alive checking including **DNS1, DNS2,** or **Other** host (input IP address manually).
13. **System Watchdog:** monitor overall WAN connection and auto reboot when WAN connection detected with no reply from Keep alive check.
14. **IGMP:** Choose **Enable** or **Disable** the IGMP snooping function. When enabled, the device detects all IGMP messages exchanged. This prevents multicast flooding on an Ethernet link.
15. **WAN IP Alias:** Some ISPs provide a fixed IP address for management purposes. If so, enter this address.

Internet Setup for Wi-Fi WISP WAN

1. To access the Wi-Fi WISP (Wireless Internet Service Provider) WAN settings, click **Internet Setup**.
2. Click **Edit** next to the WAN you want to configure.
3. Select **WISP** as **WAN type**.
    - **Connection Control:** Setup WAN connection to be **Always On**, **Connect On Demand,** or **Connect Manually**.
    - **Connect to AP:** Scan and select external **Wi-Fi AP** available for connection.
    - **Network Monitoring (keep alive):** Choose preferred settings to monitor the connection status of WAN interface. The system continuously evaluates the need to disconnect, reconnect, or failover to the backup WAN.
    - **Data Load Check:** If there is no data activity on the WAN link for a configured period, it will automatically reset and reconnect on the mobile WAN link.
    - **Check Interval:** Indicate how often to send keep alive packet or to perform data load check.
    - **Target1/Target2:** Set host for keep alive checking including **DNS1, DNS2,** or **Other** host (input IP address manually).
    - **System Watchdog:** Monitor overall WAN connection and auto reboot when WAN connection detected with no reply from keep alive check.

APN Profile List

APN Profile List This device supports multiple APN profiles for setting up cellular WAN connection. When cellular WAN is selected to use APN profile list, it will try each APN that is configured until a valid cellular connection is made.

Click **Add** or **Delete** to create and remove APN settings for SIM A or B.

1. **Profile Name:** Enter the name of the APN profile.
2. **APN:** Enter APN name that is assigned to SIM account.
3. **Account, Password:** Enter the ISP-provided Account/Password.
4. **Authentication:** Choose Auto, PAP, or CHAP according to your ISP's authentication approach. Use **Auto** if unsure.
5. **Priority:** Each APN will need to assign a priority, 1 is top priority.
6. **Profile:** Enable or Disable this APN profile.

Load Balance

This device supports a multi-WAN, load balancing function when multiple WAN interfaces are set as active. Load balance manages the outbound traffic to maximize available bandwidth on multiple WAN links.

If multiple WANs are active, click **Enable**. If not, click **Disable**.

Load Balance Strategy: If you enabled this function, configure a load balancing strategy for the outbound traffic. The three strategies include: **By Smart Weight**, **By Priority**, and **By User Policy**.

- **By Smart Weight:** The device will automatically allocate outbound traffic to each WAN interface.
- **By Priority:** Specify the outbound traffic percentage for each WAN interface. The function will follow these settings to allocate proper connection traffic for each WAN to access the internet.
- **By User Policy:** Create the active policies one by one. Click **Add** to create each load balance policy.

Manage outbound traffic flows and force specific traffic through a designated WAN interface. For those not covered by **User Policy** rules, the device will allocate the WAN interface by applying **Smart Weight** simultaneously.

1. **Source IP Address**: Enter the expected Source IP Address for the load balance policy. Choose one from **Any**, **Subnet**, **IP Range,** or **Single IP** and specify its value. If you don't want to specify an IP address, use **Any**.
2. **Destination IP Address**: Enter the expected Destination IP Address for the load balance policy. Choose one from **Any**, **Subnet**, **IP Range**, **Single IP**, or **Domain Name** and specify its value. If you don't want to specify an IP address, use **Any**.
3. **Destination Port**: Enter the expected Destination Port number for the load balance policy. Choose one from **All**, **Port Range**, **Single Port**, or **Well-known Applications** and specify its value. If you don't want to specify a port, use **All**.
4. **WAN Interface**: Select the WAN interface for accessing the Internet if all the above source and destination criteria are matched for the outbound traffic.
5. **Policy**: **Enable** or **Disable** this user policy.

LAN and VLAN Setup

This device has four Ethernet LAN ports to connect devices. VLAN function is also available to organize your local networks.

Ethernet LAN

1. **Site Name:** Enter the site name to uniquely identify the site/modem during installation. Both the main login screen and web UI display this site name.
2. **LAN IP Address:** Enter in the LAN's IP address. This IP address must be used as the computer's default gateway. This is also the IP address of the web UI. If you change this, type in the new IP address into a browser to see the web UI.
3. **Subnet Mask:** Enter the LAN's subnet mask. This defines how many clients are allowed in one network or subnet. The default subnet is 255.255.255.0 and allows for a maximum of 254 IP addresses in the subnet.
4. **ICMP:** Internet Control Message Protocol (LAN device keep alive) keeps LAN devices from disconnect or timeout due to inactivity (user-defined time interval).
    a. To use this function, check **Enable**.
    b. Enter the **IP address** for two LAN devices.
    c. Enter the **Time interval**.
    d. Click **Save**.

VLAN

The VLAN function allows you to divide a local network into virtual LANs. In some cases, the network needs multiple LANs with support certain services. This device supports port-based VLAN and tag-based VLAN. Select either operation mode and configure accordingly.

Port-Based VLAN

A port-based VLAN is a group of ports on an Ethernet switch or router that form a logical Ethernet segment. This device supports four LAN ports and up to eight virtual APs. By default, all LAN and virtual APs belong to one VLAN. This VLAN is a NAT network, all local device IP addresses are allocated by DHCP server 1. To divide them into different VLANs, click **Add** next to the port you want to configure.

1. **VLAN ID:** Enter unique VLAN ID from 6 to 4091.
2. **VLAN Tagging:** Enable or Disable VLAN Tagging with outgoing data.
3. **Type:** Select **NAT** or **BRIDGE** to identify if the packets are directly bridged to the WAN port or processed by a NAT mechanism.
4. **Port Members:** Check the desired ports to be part of the VLAN.
5. **LAN to Join:** Select preconfigured DHCP server to be used by the VLAN.
6. **WAN & WAN VID to Join:** Specify the WAN links to be used by the VLAN.
7. **Configure DHCP server information:** Enter DHCP server information such as Server Relay, Server Name, IP Pool, Lease Time, Domain Name, Primary DNS, Secondary DNS, Primary WINS, and Secondary WINS.

8. **Enable:** Enables or Disables this VLAN.

Tag-Based VLAN

In a tag-based VLAN, groups which have assigned tags and ports are no longer specifically assigned. To configure a tag-based VLAN, click **Add** to create a new VLAN to setup.

1. **VLAN ID:** Specify this group's VLAN tag. Enter unique VLAN ID 6 to 4091.
2. **Internet Access:** Check to enable internet access.
3. **Port:** Check the desired ports to be part of the VLAN.
4. **DHCP Server:** Specify a preconfigured DHCP server that VLAN will get its IP addresses."

Port Speed

The port speed function configures the Ethernet ports to a fixed speed.

1. **Speed Mode:** Select Auto, 10, 100, or 1000 for the Ethernet ports.
2. **Duplex Mode:** Select Auto, Half, or Full duplex for the Ethernet ports.

Port Setup

The port setup function configures the Ethernet ports to be enabled/disabled.

- **Enable / Disable:** Select Enable or Disable for the Ethernet port.

Wi-Fi Setup

The Wi-Fi settings allow you to set the wireless LAN configuration. Once the configurations is complete, your device will be ready to support your local Wi-Fi devices.

This device supports the following wireless operation modes: **AP Router Mode** .

2.4GHz and 5GHz AP Router Mode

This mode allows you to connect wired and wireless devices with NAT. In this mode, the gateway is a Wi-Fi AP and a hotspot. With NAT, all wireless clients don't need public IP addresses. The following settings are available under Wi-Fi configuration for AP Router Mode:

- **Wi-Fi Module:** Enables the wireless function.
- **Channel:** The default radio channel number is set to Auto. To reduce radio interference, choose a channel that is not used in your environment.
- **Wi-Fi System:**
    - For **2.4Ghz** the default setting is **b/g/n** mixed. You can also choose **b only**, **g only**, **n only**, **b/g Mixed**, or **g/n Mixed**.
    - For **5Ghz** the default setting is **a/n/ac**. You can also choose **n only**, **a only**, or **a/n Mixed**.
- **Wi-Fi Operation Mode:** AP Router Mode only.
- **Green AP:** When there is no wireless traffic, enable **Green AP** to reduce power consumption.

- **VAP Isolation:** Enabling this option separates the wireless clients so they can't communicate with each other but can access the internet and other Ethernet LAN devices
- **Time Schedule:** The wireless radio can be turned off on a schedule. By default, it is always on when the wireless module is enabled. To add a schedule rule, go to **System > Scheduling**.
- **Add VAP:** Click **Add** to add Wi-Fi virtual AP. Up to 8 VAP can be added. Each VAP can be set up with unique network SSID identifies the wireless LAN. If the Broadcast option is unchecked, wireless clients can't find the gateway through a wireless network scan.
- **SSID:** Enter Wi-Fi unique network SSID identifies the wireless LAN.
- **Max. STA:** Enable and enter number Wi-Fi of clients allow to connect.
- **Authentication and Encryption:** Select one of the following authentications to secure your wireless network:

Authentication Type	Description
Open	This mode consists of two communications, an authentication request by the client and an authentication response from the AP/router. In this mode, only **None** or **WEP** are available for encryption type.
Shared	Both stations in a shared authentication must have the same shared key or passphrase. This key must be manually set on both the client and the AP/router.
Auto	Automatically sets the appropriate authentication method based on the Wi-Fi client.
WPA-PSK	The available encryption types for this authentication are **TKIP**, **AES**, or **TKIP/AES**. In this mode, you don't need an additional RADIUS server for user authentication.
WPA2 (802.11x)	In this mode, specify the IP address and port number for the RADIUS server. The key value is shared by the device and RADIUS server. The available encryption modes are **TKIP**, **AES** , or **TKIP/AES**.
WPA-PSK/WPA2-PSK	This mode is used when some clients only support WPA-PSK and others use WPA2- PSK. You don't need an additional RADIUS server for user authentication.
WPA/WPA2 (802.11x)	This mode is used when some clients only support WPA and others use WPA2. The key value is shared by the device and RADIUS server. Specify the RADIUS server IP address and port number.

- **STA Isolation:** Enables or Disables to isolate the Wi-Fi clients that are connected to VAP.
- **Broadcast SSID:** Enables or Disables to broadcast or hide SSID.
- **Enable:** Enables or Disables VAP.

Wireless Client List

The Wireless Client List displays the connected wireless clients. Choose to see all connected clients or only clients on a specific AP.

Advanced Configuration

Advanced wireless setup is used to optimize the wireless performance under the specific installation environment.

1. **Operation Band:** Select 2.4G or 5G Wi-Fi band.
2. **Beacon Interval:** Beacons are broadcast packets that are sent by a wireless AP/router.
3. **DTIM Interval:** Delivery Traffic Indication Message Interval. When the wireless router has buffered a broadcast or multicast message for clients, it sends a DTIM with a DTIM interval value.
4. **RTS Threshold:** Adjust the Request to Send Threshold value and you can improve wireless performance if there is an excessive number of wireless packet collisions.
5. **Fragmentation:** Wireless frames are divided into smaller units to improve performance in the presence of RF interference.
6. **WMM:** Wi-Fi Multimedia helps control latency and jitter when transmitting multimedia content over a wireless connection.
7. **Short GI:** Wi-Fi Short GI (Short Guard Interval) is a feature that reduces the time gap between transmitted data symbols to increase throughput and data rates.
8. **TX Rate:** Choose **Best** for auto-adjustment based on Wi-Fi signal quality in the current environment.
9. **RF Bandwidth:** Choose Auto for auto bandwidth or set fixed bandwidth to HT20 or HT40
10. **Transmit Power:** You can lower the power ratio to prevent transmissions from reaching beyond your corporate/home office or designated wireless area.

IPv6 Setup

IPv6 is a version of the Internet Protocol (IP) intended to succeed IPv4. IPv6 implements additional features do not present in IPv4. It simplified aspects of address assignment, network renumbering, and router announcements. This device supports **Static IPv6**, **DHCPv6**, **PPPoE**, **6 to 4**, and **6 in 4** connection types. Confirm with your ISP what type of IPv6 is supported before you proceed with IPv6 setup.

Note: IPv6 isn't supported when WAN type is 3G/4G.

Static IPv6

When setting up Static IPv6, do the following and then click **Save**:

1. **WAN IPv6 address settings:**
   - **IPv6 address:** Enter the IPv6 address. IPv6 addresses are 128 bits, the address space is larger than IPv4.

     Note: An example of an IPv6 address is "2001:0db8:85a3:0000:000:8a2e:0370:7334"
   - **Subnet Prefix Length:** Enter the **Subnet Mask** prefix length.
   - **Default Gateway:** Enter the default gateway.
   - **Primary/Secondary DNS:** Add IPv6 primary and secondary DNS addresses.
   - **MLB Snooping:** Disable or Enable handling IPv6 multicast data.
2. **LAN Configuration:** Enter the LAN IPv6 address and ignore the LAN IPv6 Link-Local address.

3. **Address auto-configuration:**
    - **Auto-configuration: Disable** or **Enable** auto-configuration.
    - **Auto-configuration type:** Select **Stateless** or **Stateful** (Dynamic IPv6).
    - **Router Advertisement Lifetime:** Each router periodically multicasts a Router Advertisement from each of its interfaces, announcing the IP address(es) of that interface. Use this option to set the time period that the router broadcasts its router advertisements.

DHCPv6

When DHCPv6 is selected, do the following and then click **Save**:

1. **DNS:** Choose Obtain DNS Server address Automatically or Use Specific DNS address.
2. **LAN Configuration:** Enter the LAN IPv6 address and ignore the LAN IPv6 Link-Local address.
3. **Address auto-configuration settings:**
    - **Auto-configuration: Disable** or **Enable** auto-configuration.
    - **Auto-configuration type:** Select **Stateless** or **Stateful** (Dynamic IPv6).
    - **Router Advertisement Lifetime:** Each router periodically multicasts a Router Advertisement from each of its interfaces, announcing the IP address(es) of that interface. Use this option to set the period that the router broadcasts its router advertisements.

PPPoEv6

When PPPoE is selected, do the following and then click **Save**:

1. **PPPoEv6 WAN Type Configuration::**
    - **Account:** Enter the ISP-provided username.
    - **Password:** Enter the ISP-provided password.
    - **Service Name:** Enter the ISP-provided service name.
    - **Connection Control:** Leave setting as Auto Reconnect (always-on).
    - **MTU:** The default MTU value is 0 (auto).
    - **MLB Snooping:** Disable or Enable handling IPv6 multicast data.
2. **LAN Configuration:** Enter the LAN IPv6 address and ignore the LAN IPv6 Link-Local address.
3. **Address auto-configuration settings:**
    - **Auto-configuration: Disable** or **Enable** auto-configuration.
    - **Auto-configuration type:** Select **Stateless** or **Stateful** (Dynamic IPv6).
    - **Router Advertisement Lifetime:** Each router periodically multicasts a Router Advertisement from each of its interfaces, announcing the IP address(es) of that interface. Use this option to set the period that the router broadcasts its router advertisements.

NAT Setup

NAT Loopback

Allows you to access the WAN IP address from inside your home or office network.

Virtual Server

The NAT firewall filters out unrecognized packets to protect your Intranet, so all hosts behind this device are invisible to the outside world. You can make some of them accessible by enabling the **Virtual Server Mapping**. A virtual server is defined as a **Service Port**, and all requests to this port will be redirected to the computer specified by the LAN Server IP. **Virtual Server** can work with Scheduling Rules and give user more flexibility on Access control.

For details, refer to **Scheduling Rule**.

1. **Public Port:** Select pre-defined or enter user-defined service port.
2. **Server IP:** Enter the local server IP address of your LAN PC.
3. **Private Port:** Enter service port. Commonly same as public port.
4. **Protocol:** Select Both, TCP or UDP.
5. **Time Schedule:** Select Always or pre-defined time schedule in Schedule Rule setting.
6. **Rule:** Check to enable this rule.

Virtual Computers

Virtual Computer enables you to use the original NAT feature, and allows you to setup the one-to-one mapping of multiple global IP address and local IP address.

1. **Global IP:** Enter the assigned global IP address.
2. **Local IP:** Enter the local IP address of your LAN PC corresponding to the global IP address.
3. **Enable:** Check to enable this feature.

Special AP & ALG

Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with a pure NAT router. The **Special Applications** feature allows some of these applications to work with this product. If this mechanism of **Special Applications** fails to make an application work, try setting your computer as the DMZ host instead.

This device provides some predefined settings. Select your application and click **Copy to** add the predefined setting to your list.

1. **Trigger:** The application-issued outbound port number.
2. **Incoming Ports:** When the trigger packet is detected, the inbound packets sent to the specified port numbers are allowed to pass through the firewall.
3. **Time Schedule:** Select Always or pre-defined time schedule in Schedule Rule setting.

4. **Enable:** Check this item to enable this feature.

DMZ

DMZ (Demilitarized Zone) Host is a host without the protection of a firewall. It allows a computer to be exposed to unrestricted 2-way communication for Internet games, Video conferencing, Internet telephony, and other special applications. If a specific application is blocked by NAT mechanism, you can designate that LAN computer as a DMZ host to solve this problem.

Note: This feature should be used only when necessary.

Routing Setup

If there is more than one router and subnet, enable routing function to allow packets to find proper routing paths and allow different subnets to communicate with each other.

Static Routing

For static routing, you can specify up to 32 routing rules. These rules allow you to determine which physical interface addresses are being utilized for outgoing data. For each rule, enter the destination IP address, subnet mask, gateway, and hop. Check **Enable** or **Disable**. Click **Add** to create new static routing rule.

- **Destination IP:** Enter the IP address / subnet that requires routing.
- **Subnet Mask:** Enter IP subnet mask for the above IP address / subnet.
- **Gateway IP:** Enter gateway IP address that destination IP / subnet will be forwarded to.
- **Metric:** Enter metric number for the static route.
- **Rule:** Disable or Enable this rule.

Dynamic Routing

Dynamic routing is used when there are many subnets in your network. This device supports RIPv1/RIPv2, OSPF, and BGP dynamic routing protocols.

- **Routing Information Protocol (RIP):** This protocol will exchange information about destinations for computing routes throughout the network. Only select RIPv2 if you have different subnets in your network.
- **OSPF:** This is an interior gateway protocol that routes IP packets solely within a single routing domain.
    - **OSPF:** Disable or Enable OSPF feature.
    - **Router ID:** Enter unique router ID assign to this router on OSPF protocol.
    - **Authentication:** Select and Enter authentication method.
    - **Backbone Subnet:** Enter backbone subnet on OSPF protocol.
    - **OSPF Area List:** Click **Add** to create custom OSPF area rule with area subnet and ID.
- **BGP:** Border Gateway Protocol is the protocol backing the core routing decisions on the Internet. It maintains a table of IP networks which designate network reachability among autonomous systems.

- **BGP:** Disable or Enable BGP feature.
- **ASN:** Enter ASN number assign to this router on BGP protocol.
- **Router ID:** Enter unique router ID assign to this router on OSPF protocol.
- **BGP Network List:** Click **Add** to create custom BGP network list with IP subnet / netmask.
- **BGP Neighbor List:** Click **Add** to create custom BGP neighbor list with neighbor IP and Remote ASN.

Routing Information

A routing table, or routing information base (RIB), is a data table stored in a router or networked computer that lists the routes to other network destinations. The routing table contains information about the topology of the network immediately around it. This function displays the routing table maintained by this device. It is generated according to your network configuration.

Client/Server

Dynamic DNS

To host a server on a changing IP address, you must use dynamic domain name service (DDNS). DDNS maps the name of your host to the current IP address, which changes each time you connect to your ISP. Before you enable Dynamic DNS, you need to register an account on one of the DDNS servers in the Provider list.

1. **DDNS: Disable** or **Enable** this feature.
2. **Provider:** The DDNS provider supports service for you to bind your IP with a certain domain name.
3. **Host Name:** Register a domain name to the DDNS provider.
4. **Username/E-mail:** Enter username or e-mail based on the DDNS provider requirements.
5. **Password/Key:** Enter password or key based on the DDNS provider requirements.

DHCP Server

The gateway supports up to 4 DHCP servers to serve the DHCP requests from different VLAN groups.

There are two additional options to show the DHCP client list and the fixed mapping between MAC address and IP address of local client hosts.

To add or edit one DHCP server configuration click **Add** next to **DHCP Server List** or **Edit** at the end of DHCP server information.

1. **DHCP Server:** Enter unique DHCP server name.
2. **LAN IP Address:** Specify the local IP address of the enabled DHCP Server. It's the LAN IP address of this gateway for DHCP-n server. Normally, this IP address will be also the default gateway of local computers and devices.
3. **Subnet Mask:** Select the subnet mask for the specific DHCP-n server. Subnet Mask defines how many clients are allowed in one network or subnet. The default subnet mask is 255.255.255.0/24,

and it means maximum 254 IP addresses are allowed in this subnet. However, one of them is occupied by LAN IP address of this gateway. There is a maximum of 253 clients allowed in the LAN network. See available options for subnet mask below.

4. **IP Pool Starting / Ending Address:** Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. Specify the starting/ending address of the IP address pool.

   Note: The number of IP addresses in this IP pool must be less than the maximum number of subnet networks according to the subnet mask you set.

5. **Lease Time:** DHCP lease time to the DHCP client.
6. **Domain Name:** Optional. This information will be passed to the clients.
7. **Primary DNS/Secondary DNS:** Optional. Assign the DNS Servers.
8. **Primary WINS/Secondary WINS:** Optional. Assign the WINS Servers.
9. **Gateway:** Optional. This would be the alternate Gateway IP address. Assign another gateway to your local computer when the DHCP server offers an IP address. For example, this gateway assigns an IP address to a local computer but the computer accesses the Internet through another gateway.
10. **Server: Enable** if you want the DHCP server active or **Disable.**

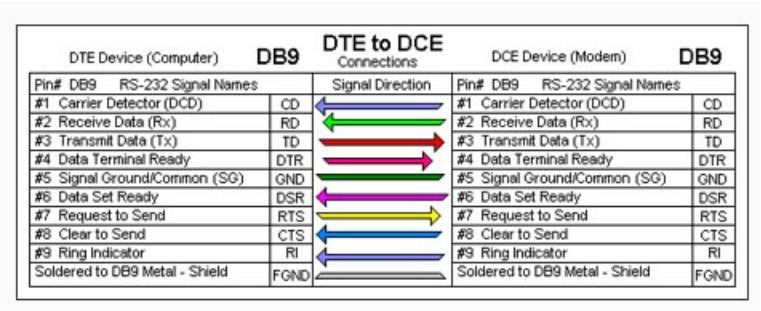
Fixed Mapping

Click **Fixed Mapping** at the bottom of the DHCP server list. Specify an IP address assigned to a local device (MAC address) so that the DHCP Server will always handout the same IP address to the same local device every time.

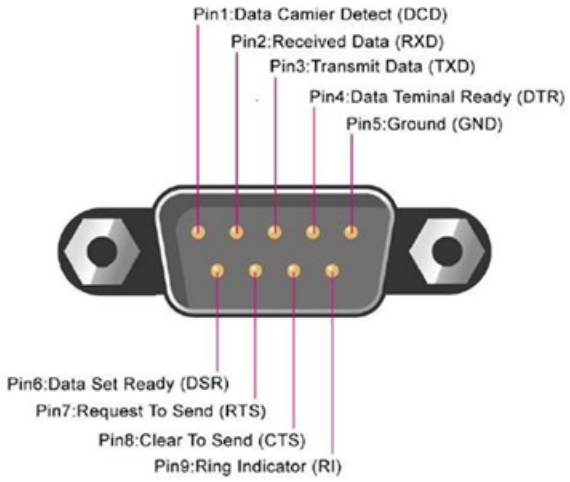
Serial Port

This device has one DB-9 male port (DTE interface) used for serial communication. To use, connect an RS-232 serial device to an IP-based Ethernet LAN. It also has one terminal block serial port with a three-wire RS232 or RS485 interface.

Serial port 1 - DB9 RS232 pinout (DTE interface)



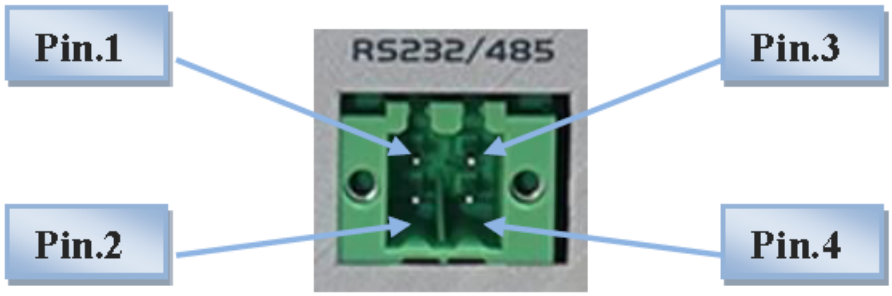
RS232 Pinout



	Pin1	Pin2	Pin3	Pin4	Pin5	Pin6	Pin7	Pin8	Pin9
RS-232	DCD	RXD	TXD	DTR	GND	DSR	RTS	CTS	RI

Serial Port 2 - Three-wires terminal block RS232 / RS485 pinout

Terminal Block Pin



	Pin1	Pin2	Pin3	Pin4
RS-232 (Lite)	RXD	GND	TXD	GND
RS-485	DATA-		DATA+	

Serial Port 1 Configuration (DB-9)

The DB9 serial port is a 9 pins RS232 DTE interface. The port can be set up as Paknet or virtual Com with TCP client, TCP server, UDP or RFC-2217 to access the external RS232 serial device on the DB9 serial port.

Before using a Virtual COM or Paknet, configure the DB-9 male port first.

1. **Operation Mode:** Choose the purpose of the port. It can be **Virtual COM** or **Paknet**. To prevent unknown serial devices from connecting, disable this option.
    - **Virtual COM:** Create a virtual COM port on a PC/Host and provide access to serial devices connected to the IDG gateway.
    - **Paknet:** This protocol and service is part of the old legacy Vodafone network that is widely use with RTU. Choose this option to connect a device and communicate with it using this protocol.
2. **Interface:** Choose **RS-232** only.
3. **Baud Rate:** Set the baud rate (bps) of the serial port. The value can be **1200** to **115200**.
4. **Data Bits:** Choose **7** or **8** as the data bit.
5. **Stop Bits:** Choose **1** or **2** as the stop bit.
6. **Flow Control:** Choose **RTS/CTS** or **None**.
7. **Parity:** Choose **Odd** or **Even**.

Virtual COM

Create a virtual COM port on a PC/Host and provide access to serial devices connected to the IDG gateway. Users can access, control, and manage serial devices through the Internet no matter where they are located.

TCP Client Mode

In TCP Client Mode, a TCP connection to a pre-defined host computer is active when serial data arrives. After the data has been transferred, it is disconnected from the host computer by using the TCP alive check or idle timeout settings.

1. **Operation Mode:** Choose **TCP Client**.
2. **Connection Control:** To keep the connection with the remote TCP server all the time, choose **Always On.** To keep the connection only when transmitting data, choose **ON-Demand**.
3. **Connection Idle Timeout:** The TCP connection will be terminated if it idles longer than this timeout setting. This is only available if the **Connection Control** is set to **ON-Demand**.
4. **Alive Check Timeout:** The TCP connection will be terminated if it doesn't receive a response from the alive check. This is only available if the **Connection Control** is set to **ON-Demand**.
5. **Data Packing:**
    - Data buffer Length: process and send data over IP after serial data buffer length is received. 0 sends data immediately without waiting.
    - Delimiter Character 1: process and send data over IP when the last character in the serial data stream matches. Check enable and enter Hex value for the character to activate this function.
    - Delimiter Character 2: process and send data over IP when the last TWO characters in the serial data stream matches. Check enable and enter Hex value for the character to activate this function.

- Data Timeout Transmit: process and send data over IP based on configured time value, when the serial port has received the data for configured time, it processes and sends the data. Value range is 1 to 1000ms, 0 is disable.

6. **Legal IP / FQDN Host:** Click **Edit** to enter the remote host IP address of FQDN (Fully Qualified Domain Name). The remote host is the TCP server.
   - **To Host:** Enter the remote host IP address.
   - **Remote Port:** Enter the remote host TCP port.
   - **Enable:** Check to enable the rule.

TCP Server Mode

In TCP Server Mode, remote TCP client connects to router WAN IP with a unique TCP Port number to send / receive serial data. This operation mode supports up to four simultaneous connections at the same time.

1. **Operation Mode:** Choose **TCP Server.**
2. **Listen Port:** Enter the listening port of the TCP connection.
3. **Trust Type:** Choose **Allow All** to allow all TCP clients to connect. Choose **Specific IP** to allow certain remote TCP clients and enter the IP address range of allowed remote TCP clients.
4. **Max Connection:** Set the maximum number of concurrent TCP connections. Up to four connections can be established at the same time.
5. **Connection Idle Timeout:** The TCP connection will be terminated if it idles longer then this timeout setting. This is only available if the Connection Control is set to **ON-Demand.**
6. **Alive Check Timeout:** The TCP connection will be terminated if it doesn't receive a response from the alive check.
7. **Data Packing:**
   - Data buffer Length: process and send data over IP after serial data buffer length is received. 0 sends data immediately without waiting.
   - Delimiter Character 1: process and send data over IP when the last character in the serial data stream matches. Check enable and enter Hex value for the character to activate this function.
   - Delimiter Character 2: process and send data over IP when the last TWO characters in the serial data stream matches. Check enable and enter Hex value for the character to activate this function.
   - Data Timeout Transmit: process and send data over IP based on configured time value, when the serial port has received the data for configured time, it processes and sends the data. Value range is 1 to 1000ms, 0 is disable.

UDP Mode

In UDP mode, you can multicast data from the serial device to multiple host computers. The serial device can receive data from multiple host computers. This mode is ideal for message display applications. This operation mode supports only one connection.

1. **Operation Mode:** Choose **UDP**.

2. **Listen Port:** Enter the listening port of the UDP connection.
3. **Host:** Click **Edit** to enter IP address range of remote UDP hosts.
    - **Host:** Enter the UDP port of peer UDP host.
    - **Remote Port:** Enter the UDP port of peer UDP hosts.
    - **Enable:** Check to enable the rule.

RFC2217 Mode

In this mode, a standard driver provides Virtual COM function. Any third-party driver that supports RFC2217 can be used to implement Virtual COM on the gateway. The driver establishes a transparent connection between the host and the serial device by mapping the IP: Port of the gateway's serial port to a local COM port on the host computer.

1. **Operation Mode:** Choose **RFC-2217**.
2. **Listen Port:** Enter the connection listening TCP port.
3. **Trust Type:** Choose **Allow All** to allow all hosts to connect. Choose **Specific IP** to allow certain hosts.
4. **Connection Idle Timeout:** The TCP connection will be terminated if it idles longer than this timeout setting. This is only available if the **Connection Control** is set to **ON-Demand**.
5. **Alive Check Timeout:** The TCP connection will be terminated if it doesn't receive a response from the alive check.

Paknet

This protocol and service is part of an old legacy Vodafone network that is widely used with RTU. This device supports a very minimum emulation set of the Paknet protocol. Make sure to check and test your device for compatibility with this Paknet emulation before deployment. This allows an RS232 device to communicate using legacy Paknet protocol and then convert to IP data. Use this feature to establish master-slave/client-server communication between an RS232 device to/from IP remote servers.

1. **Server Listen Port:** Defines TCP port that the remote IP server can connect to when device is set up to answer call.
2. **Remote IP:** Defines remote server IP address that device connects to when it is originating call. Defines TCP port that remote IP server connects to when device is set up to answer call.
3. **Remote Port:** Defines remote server IP port that the device connects to when it is originating call. Defines remote server IP address that device connects to when it is originating call. Defines TCP port that remote IP server connects to when device is set up to answer call.
4. **Secondary Remote IP:** Defines secondary remote server IP address that the device connects to when it is originating call.
5. **Secondary Remote Port:** Defines secondary remote server IP port that the device connects to when it is originating call.
6. **DTR Turn Off Time:** Defines how long to turn off DTR signal during TCP disconnect.
7. **Dialing Characters:** Defines dialing string to match when the device originates call. The string must match with the device string before TCP establishes a connection to the remote IP server.

8. **Data Timeout Transmit:** Process and send serial data over IP based on configured time value. When the serial port has received the data for the configured time, it processes and sends the data. Value range is 1 to 1000ms. 0 is disable.
9. **Connection Idle Timeout:** The TCP connection will be terminated if it idles longer than this timeout setting in second.
10. **Check DCD Status:** Check DCD signal in order to reset everything and start from the beginning of Paknet command mode.

Serial Port 2 Configuration (Terminal block)

The terminal block serial port is a three-wires (TXD, RXD and GND) RS232 or RS485 half-duplex interface. The port can be set up as Modbus or virtual Com with TCP client, TCP server or UDP to access the external RS232 / RS485 serial device connected to the terminal block serial port.

1. **Operation Mode:** Choose the purpose of the port. It can be Virtual COM or Paknet. To prevent unknown serial devices from connecting, disable this option.
    - **Virtual COM:** Create a virtual COM port on a PC/Host and provide access to serial devices connected to the IDG gateway.
    - **Modbus:** This protocol is widely used on meters. Choose this option to connect a device and communicate with it using this protocol.
2. **Interface:** Choose **RS-232** or **RS-485**.
3. **Baud Rate:** Set the baud rate (bps) of the serial port. The value can be **1200 to 115200**.
4. **Data Bits:** Choose **7** or **8** as the data bit.
5. **Stop Bits:** Choose **1** or **2** as the stop bit.
6. **Parity:** Choose **Odd** or **Even**.

Virtual COM

Create a virtual COM port on a PC/Host and provide access to serial devices connected to the IDG gateway. Users can access, control, and manage serial devices through the Internet no matter where they are located.

TCP Client Mode

In TCP Client Mode, a TCP connection to a pre-defined host computer is active when serial data arrives. After the data has been transferred, it is disconnected from the host computer by using the TCP alive check or idle timeout settings.

1. **Operation Mode:** Choose **TCP Client**.
2. **Connection Control:** To keep the connection with remote TCP server all the time, choose **Always On**. To keep the connection only when transmitting data, choose **ON-Demand.**
3. **Connection Idle Timeout:** The TCP connection will be terminated if it idles longer than this timeout setting. This is only available if the **Connection Control** is set to **ON-Demand**.
4. **Alive Check Timeout:** The TCP connection will be terminated if it doesn't receive a response from the alive check. This is only available if the **Connection Control** is set to **ON-Demand**.

5. **Data Packing:**
    - **Data Buffer Length:** process and send data over IP after serial data buffer length is received. 0 sends data immediately without waiting.
    - **Delimiter Character 1:** process and send data over IP when the last character in the serial data stream matches. Check enable and enter Hex value for the character to activate this function.
    - **Delimiter Character 2:** process and send data over IP when the last TWO characters in the serial data stream matches. Check enable and enter Hex value for the character to activate this function.
    - **Data Timeout Transmit:** process and send data over IP based on configured time value, when the serial port has received the data for configured time, it processes and sends the data. Value range is 1 to 1000ms, 0 is disable.
6. **Legal IP / FQDN Host:** Click **Edit** to enter the remote host IP address of FQDN (Fully Qualified Domain Name). The remote host is the TCP server.
    - **To Host:** Enter the remote host IP address.
    - **Remote Port:** Enter the remote host TCP port.
    - **Enable:** Check to enable the rule.

TCP Server Mode

In TCP Server Mode, remote TCP client connects to router WAN IP with a unique TCP Port number to send / receive serial data. This operation mode supports up to four simultaneous connections at the same time.

1. **Operation Mode**: Choose **TCP Server.**
2. **Listen Port:** Enter the listening port of the TCP connection.
3. **Trust Type:** Choose **Allow All** to allow all TCP clients to connect. Choose **Specific IP** to allow certain remote TCP clients and enter the IP address range of allowed remote TCP clients.
4. **Max Connection:** Set the maximum number of concurrent TCP connections. Up to four connections can be established at the same time.
5. **Connection Idle Timeout:** The TCP connection will be terminated if it idles longer then this timeout setting. This is only available if the Connection Control is set to **ON-Demand**.
6. **Alive Check Timeout**: The TCP connection will be terminated if it doesn't receive a response from the alive check.
7. **Data Packing:**
    - **Data Buffer Length:** process and send data over IP after serial data buffer length is received. 0 sends data immediately without waiting.
    - **Delimiter Character 1:** process and send data over IP when the last character in the serial data stream matches. Check enable and enter Hex value for the character to activate this function.
    - **Delimiter Character 2:** process and send data over IP when the last TWO characters in the serial data stream matches. Check enable and enter Hex value for the character to activate this function.

- **Data Timeout Transmit:** process and send data over IP based on configured time value, when the serial port has received the data for configured time, it processes and sends the data. Value range is 1 to 1000ms, 0 is disable.

8. **Legal IP / FQDN Host:** Click **Edit** to enter the remote host IP address of FQDN (Fully Qualified Domain Name). The remote host is the TCP server.
    - **To Host:** Enter the remote host IP address.
    - **Remote Port:** Enter the remote host TCP port.
    - **Enable:** Check to enable the rule.

UDP Mode

In UDP mode, you can multicast data from the serial device to multiple host computers. The serial device can receive data from multiple host computers. This mode is ideal for message display applications. This operation mode supports only one connection.

1. **Operation Mode:** Choose **UDP.**
2. **Listen Port:** Enter the listening port of the UDP connection.
3. **Host:** Click **Edit** to enter IP address range of remote UDP host.
    - **Host:** Enter the UDP port of peer UDP host.
    - **Remote Port:** Enter the UDP port of peer UDP host.
    - **Enable:** Check to enable the rule.

Modbus

Modbus supports traditional RS-232/485 devices and recently developed Ethernet devices. Use this feature to establish master-slave/client-server communication between intelligent devices. Modbus networks can automatically and intelligently translate between Modbus TCP (Ethernet) and Modbus ASCII/RTU (serial) protocols, allowing Ethernet-based PLCs to control instruments over RS-485 without additional programming. All devices connected to a single serial port must use the same protocol.

1. **Operation Mode:** The Modbus Gateway enables conversions between serial and network Modbus protocols.
2. **Serial Protocol:** Defines the RTU or ASCII protocol used on serial communication.
3. **Listen Port:** Defines the TCP or UDP port that Master connects to.
4. **Serial Response Timeout:** If the serial side does not respond within a specific time, data is dropped and not transmitted.
5. **Serial Timeout Retries:** If set to 0, the gateway doesn't store TCP packets in the buffer. If it is set to greater than 0, the gateway stores TCP packets in the buffer and retries for the specified time when the Modbus device on the serial side doesn't respond.
6. **0Bh Exception:** When the Modbus slave device doesn't respond before timeout, the 0Bh exception code is transmitted to the master that initiated the message.
7. **Serial Message Buffering:** When enabled, the gateway will buffer TCP up to 32 requests. If disabled, the gateway will respond with a 06h if it has a message out on the port with no response.

8. **Tx Delay:** The minimum amount of time after receiving a message before the next message can be sent out.
9. **TCP Connection Idle Timeout:** Idle timeout, in seconds, for the Modbus /TCP connection. If no response within the time limit, the connection is closed.
10. **Maximum TCP Connection:** A maximum of four simultaneous Modbus /TCP connections is allowed.
11. **TCP Keep-alive:** Disable or Enable TCP keep alive.
12. **Trusted IP Access:** Defines the IP that is allowed to connect to the gateway.
13. **Modbus Priority:** Defines the priorities from specific IPs, Modbus IDs, or Function Codes

6 Advanced Network

Advanced Network

This device supports advanced network features, such as Firewall, QoS, Security, Redundancy, and Management.

Firewall

The firewall function includes Packet Filters, URL Blocking, MAC control, and Options.

Packet Filters

Packet filters include outbound and inbound filters. This enables you to control what packets are allowed to pass through the router.

1. **Packet Filters:** Enable or Disable packet filter rules.
2. **Black List / White List:** Select Allow or Deny to pass except those matching the specified rules.
3. **Log Alert:** Enable or Disable the Log Alert will record events that are matched by these rules.
4. **Packet Filter List:** Add or Delete.
    - **Rule Name:** Enter unique rule name.
    - **From Interface:** Select LAN or WAN interface when data is from.
    - **To Interface:** Select LAN or WAN interface when data is to.
    - **Source IP address or range:** Define packet source IP, it is a single IP address or a range of IP addresses. Leaving this empty implies all IP addresses.
    - **Destination IP address or range:** Define packet destination IP, it is a single IP address or a range of IP addresses. Leaving this empty implies all IP addresses.
    - **Destination Port:** You can define a single port or a range of ports.
    - **Protocol:** TCP, UDP, TCP/UDP, Any.
    - **Time Schedule:** Rule can be turned off according to a time schedule defined rule.
    - **Rule: Enable** or **Disable** this packet filter rule.

URL Blocking (HTTP only)

URL blocking blocks websites containing pre-defined keywords. This feature filters both domain input suffix and keywords.

1. **URL Blocking:** Enable or Disable URL Blocking rules.
2. **Black List/White List:** Select Allow or Deny to pass except those matching the specified rules.
3. **Log Alert:** Enable or Disable the Log Alert. This records events that match these rules.
4. **URL Blocking Rule List:** Add or Delete.
    - **URL / Domain Name / Keyword:** Enter HTTP URL, domain name or keyword in URL.
    - **Destination Port:** You can define a single port or a range of ports.

- **Time Schedule:** Rule can be turned off according to a time schedule defined rule.
- **Rule:** Enable or Disable this URL Blocking rule.

MAC Control

Mac Control allows you to assign different access rights for different users based on a device's MAC address.

1. **MAC Control:** Enable or Disable **MAC Control**.
2. **Black List/White List:** Select Allow or Deny to pass except those matching the specified rules.
3. **Log Alert:** Enable or Disable the Log Alert. This records events that match these rules.
4. **Known MAC from LAN PC List:** Displays all connected clients and their MAC Addresses so you can copy to clipboard.
5. **MAC Control Rule List:** Add or Delete
    - **Rule Name:** Enter unique rule name.
    - **MAC Address:** Enter the device MAC address to filter.
    - **Schedule:** Rule can be turned off according to a time schedule defined rule.
    - **Enable:** Check to enable each rule.

IPS (Intrusion Prevention Systems)

IPS (Intrusion Prevention Systems) are network security appliances that monitor network and/or system activities for malicious activity. The main functions of IPS are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it. Some intrusion prevention items need a Threshold parameter to work properly. Enable the **Log Alert** so the system records Intrusion events when detected.

1. **IPS:** Check to enable **IPS**.
2. **Log Alert:** Check to enable **Log Alert**. This records intrusion events that are detected by IPS.
3. **Intrusion Prevention check boxes:** Check to enable each of the IPS activity to be filtered.

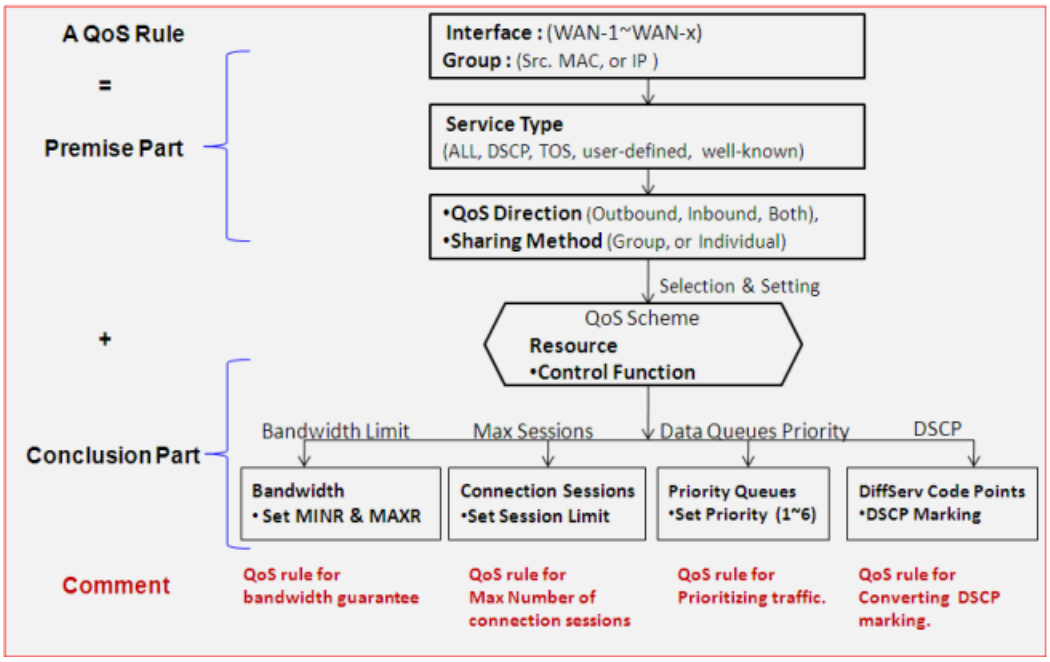
Options

1. **Stealth Mode:** When enabled, the router will not respond to port scans from the WAN. This makes the router less susceptible to discovery and attacks.
2. **SPI** (**Stateful Packet Inspection** also known as dynamic packet filtering): helps to prevent cyberattacks by tracking more states per session. It validates that the traffic passing through that session conforms to the protocol.
3. **Discard PING from WAN Side:** When enabled, this gateway won't reply to any ICMP request packet from the WAN side.
4. **HTTP:** Setup and allow HTTP web UI access via LAN and/or WAN. Setup and allow the web UI to use a custom HTTP TCP port and restrict remote WAN IPs accessing the web UI from the internet.

5. **HTTPS:** Setup and allow HTTPS web UI access via LAN and/or WAN. Setup and allow the web UI to use a custom HTTPS TCP port and restrict remote WAN IPs accessing the web UI from the internet.
6. **TCP Alive:** Allow a local/remote TCP client to perform a TCP keep alive check to the LAN/WAN IPs using a configurable TCP port.

Quality of Service

Quality of Service (QoS) prioritizes incoming data and prevents data loss due to factors such as jitter, delay, and dropping. QoS helps to prioritize data as it enters your router. By attaching special identification marks or headers to incoming packets, QoS determines which queue the packets enter, based on priority.



QoS Configuration

Before QoS can work correctly, this gateway needs to know available bandwidth of the WAN connection.

1. **Total Priority Queues of All WANs:** Input the maximum number of priority queues to manage QoS.
2. **WAN Interface:** Select the WAN interface.
3. **Bandwidth of Upstream:** Input the maximum bandwidth of uplink in Kbps or Mbps.
4. **Bandwidth of Downstream:** Input the maximum bandwidth of downlink in Kbps or Mbps.
5. **Total Connection Sessions:** Input the maximum IP connection sessions allow

Rule-based QoS

This gateway provides many flexible rules for you to set QoS policies.

1. **Rule-Based QoS:** Check to activate this rule after it's created.

2. **Flexible Bandwidth Management:** It is recommended you enable this option to exploit maximum bandwidth effectively.

Create a Rule-Based QoS Rule

Click **Add** to create a new rule

1. **Interface:** Choose WAN interface for the rule.
2. **Grouping:** Choose **Src MAC Address** or **IP address** from the list and indicate single IP address or a segment IP range in the following field.
3. **Service:** Select the type of service that needs to be managed. There are four options for service recognition.
    - **DSCP**: **DiffServ Code Point** (aka advanced TOS). Select this option if your local service gateway supports DSCP tags.
    - **Service Port:** Input a service port number or a segment of port range manually. Also indicate TCP or UDP service.
    - **Pre-defined Application profiles:** This option is similar to **Service Port** but lists many well-known services for your reference.
    - **Connection Sessions:** Choose this option if you want to limit connection sessions on those selected hosts.
4. **Resource:** Select the type of service that needs to be managed. There are four options Bandwidth, Connection Sessions, Priority Queues and DiffServ Code Points.
5. **Control:** Set the corresponding control types for the selected service type.
    - **DSCP Marking:** This option is only available when DSCP is chosen in the Service field. The purpose of this option is changing original DSCP tag to a new value. This option won't prioritize data packets.
    - **Set Priority:** Set priorities for data packets of selected hosts. The value is from **1** to **6**. **1** is highest priority and **6** is lowest priority.
    - **MAXR:** Indicate the maximum bandwidth for selected hosts. The measurement unit can be Kbps or Mbps.
    - **MINR:** Indicate the minimum bandwidth for selected hosts. The measurement unit can be Kbps or Mbps.
    - **Set Session Limitation:** This option is only available when you choose **Connection Sessions** in the **Service** field. The maximum number of sessions is **20000**.
6. **QoS Direction:** Select the traffic direction Outbound, Inbound or Both to apply for this rule.
7. **Sharing Method:** This option is only available when you choose MAXR, MINR, SESSION in the Control field. If you want to apply the value of the Control setting on each selected host, then select Single.
8. **Time Schedule:** According to the schedule you specify, the QoS rule can be turned off. The default is on when you enable the rule.
9. **Enable:** Enable or Disable this rule.

Cellular QoS Resource

This feature defines typical cellular bandwidth in Kbps or Mbps for the 2G, 3G and 4G connections.

VPN Setup

A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security, and management policies of a private network.

- **VPN: Enable** or **Disable** the main VPN function.

IPSec

1. **IPSEC:** Check to **Enable** or **Disable** this function.
2. **Max. Concurrent IPSec Tunnels:** The device can support up to 16 IPSec tunnels.

Dynamic VPN List

A VPN gateway can ignore IP information of client when using Dynamic VPN. This function builds a VPN tunnel with the VPN gateway from a remote mobile host.

1. **Tunnel: Enable** or **Disable** this tunnel.
2. **Tunnel name:** Assign a name for this tunnel.
3. **Interface:** Select WAN interface for this tunnel.
4. **Tunnel Scenario:** Select mode for this tunnel.
5. **Encapsulation Protocol:** Select ESP or AH protocol for this tunnel.
6. **IKE Version: I**KE version v1 only for this tunnel.
7. **Local subnet:** This can be a host, a partial subnet, or the whole subnet of a LAN site on the local gateway.
8. **Local Netmask:** The local netmask and associated local subnet can define a subnet domain for the devices connected via the VPN tunnel.
9. **Key Management:** The pre-shared key must be the same one for both VPN gateways and clients.
10. **Local ID:** The Type and the Value of the local VPN gateway must be the same as the Remote ID of the remote VPN gateway.
11. **Remote ID:** The Type and Value of the local VPN gateway must be the same as the local ID of the remote VPN gateway.
12. **Negotiation Mode:** Only main mode is supported.
13. **X-Auth:** For the extended authentication function (XAUTH), the VPN client (or initiator) needs to provide additional user information to the remote VPN server (or VPN gateway). The VPN server would reject the connect request from VPN clients because of invalid user information, even though the pre-shared key is correct. Use this function for remote mobile VPN clients. Configure

a VPN rule with a pre-shared key for all remote users and designate an account/password for specific users permitted to establish a VPN connection with the VPN server.

- **None:** Without Extended Authentication (xAuth).
- **Server:** Device behaves as a VPN server and validates the user information.
- **Client:** Device behaves as a VPN client. Enter user account and password to authenticate with remote VPN server

14. **Dead Peer Detection:** This feature detects if a remote VPN gateway still exists. Indicate the interval between every detection and assign the value for timeout.
15. **IKE Phase 1 Key Life Time:** The value represents the lifetime of the key which is dedicated at Phase 1 between both end gateways.
16. **IKE Proposal Definition:** Define up to four proposals during IKE negotiation.
    - **Encryption:** Choose from algorithms including **DES, 3DES, AES-128, AES-192,** and **AES- 256.**
    - **Authentication:** Choose from algorithms: **None, MD5, SHA1,** and **SHA2-256.**
    - **DH Group:** Choose from groups: **None, Group 1, 2, 5, 14, 15, 16, 17,** and **18.**
    - **Enable:** Check to enable the proposal.
17. **IPSec Phase 2 Key Life Time:** The value represents the lifetime of the key which is dedicated at Phase 2 between both end gateways.
18. **IPSec Proposal Definition:** Define up to four proposals during IPSec negotiation.
    - **Encryption:** Choose from algorithms including **DES, 3DES, AES-128, AES-192,** and **AES- 256.**
    - **Authentication:** Choose from algorithms: **None, MD5, SHA1,** and **SHA2-256.**
    - **PFS Group:** Choose from groups: **None, Group 1, 2, 5, 14, 15, 16, 17,** and **18.**
    - **Enable:** Check to enable the proposal.

IPSec Tunnel List

1. **Tunnel: Enable** or **Disable** this tunnel.
2. **Tunnel Name:** Assign a name for this tunnel.
3. **Interface:** Select WAN interface for this tunnel.
4. **Tunnel Scenario:** Select mode for this tunnel.
5. **Tunnel TCP MSS:** Select **Auto** or **Manual** and enter **TCP MSS** value.
6. **ICMP Keep Alive: Enable** or **Disable** ping keep alive and enter maximum fail time, interval, and IPs.
7. **Encapsulation Protocol:** Select **ESP** or **AH** protocol for this tunnel.
8. **IKE Version:** Select IKE version **v1** or **v2** for this tunnel.
9. **Local subnet list:** Setup and add all local subnets that need to travel over this tunnel.
10. **Remote subnet list:** Setup and add all remote subnets that need to travel over this tunnel.
11. **Remote Gateway:** Enter the IP address of the remote VPN gateway.

12. **Key Management:** The pre-shared key must be the same one for both VPN gateways and clients.
13. **Local ID:** The Type and the Value of the local VPN gateway must be the same as the Remote ID of the remote VPN gateway.
14. **Remote ID:** The Type and Value of the local VPN gateway must be the same as the local ID of the remote VPN gateway.
15. **Negotiation Mode:** Only main mode is supported.
16. **X-Auth:** For the extended authentication function (XAUTH), the VPN client (or initiator) needs to provide additional user information to the remote VPN server (or VPN gateway). The VPN server would reject the connect request from VPN clients because of invalid user information, even though the pre-shared key is correct. Use this function for remote mobile VPN clients. Configure a VPN rule with a pre-shared key for all remote users and designate an account/password for specific users permitted to establish a VPN connection with the VPN server
    - **None:** Without Extended Authentication (xAuth).
    - **Server:** Device behaves as a VPN server and validates the user information.
    - **Client:** Device behaves as a VPN client. Enter user account and password to authenticate with remote VPN server
17. **Dead Peer Detection:** This feature detects if a remote VPN gateway still exists. Indicate the interval between every detection and assign the value for timeout.
18. **IKE Phase 1 Key Life Time:** The value represents the lifetime of the key which is dedicated at Phase 1 between both end gateways.
19. **IKE Proposal Definition:** Define up to four proposals during IKE negotiation.
    - **Encryption:** Choose from algorithms including **DES, 3DES, AES-128, AES-192,** and **AES- 256.**
    - **Authentication:** Choose from algorithms: **None, MD5, SHA1,** and **SHA2-256.**
    - **DH Group:** Choose from groups: **None, Group 1, 2, 5, 14, 15, 16, 17,** and **18.**
    - **Enable:** Check to enable the proposal.
20. **IPSec Phase 2 Key Life Time:** The value represents the lifetime of the key which is dedicated at Phase 2 between both end gateways.
21. **IPSec Proposal Definition:** Define up to four proposals during IPSec negotiation.
    - **Encryption:** Choose from algorithms including **DES, 3DES, AES-128, AES-192,** and **AES- 256.**
    - **Authentication:** Choose from algorithms: **None, MD5, SHA1,** and **SHA2-256.**
    - **PFS Group:** Choose from groups: **None, Group 1, 2, 5, 14, 15, 16, 17,** and **18.**
    - **Enable:** Check to enable the proposal.

PPTP

PPTP Server

The VPN gateway can behave as a PPTP server and allows remote hosts to access LAN servers behind the PPTP server. The device can support three authentication methods: PAP, CHAP, and MSCHAP(v1 and v2). Users can also enable MPPE encryption when using MSCHAP.

1. **PPTP Server:** Check to **Enable** or **Disable** this function.
2. **Client / Server:** Select **Server** mode.
3. **PPTP Server: Enable** or **Disable** PPTP server.
4. **Server Virtual IP:** The IP address of PPTP server. This IP address should be different from IP address of the L2TP server and the LAN subnet of the VPN gateway.
5. **IP Pool Start Address:** This device assigns an IP address to the remote PPTP client. This value indicates the beginning of the IP pool.
6. **IP Pool End Address:** This device assigns an IP address to the remote PPTP client. This value indicates the end of the IP pool.
7. **Authentication Protocol:** Choose from three protocols: **PAP, CHAP ,**or **MSCHAP(v1 or v2)**.
8. **MPPE Encryption:** Check to enable and select 40, 56 or 128bits. The MPPE needs to work with MSCHAP (v1 or v2) authentication.
9. **Encryption Length:** Choose length of MPPE encryption.
10. **PPTP Server Status:** Displays all the active PPTP clients that are connected to the PPTP server.
11. **User Account:** Add username and password to allow connection to this PPTP server.

PPTP Client

1. **PPTP Client:** Check to **Enable** or **Disable** this function.
2. **Client / Server:** Select **Server** mode.
3. **PPTP Server: Enable** or **Disable** PPTP server.
4. **PPT Client List & Status:** Select Add, Delete and Refresh
    - **Tunnel Name:** The name of this rule.
    - **Interface:** Select WAN interface for this PPTP client to use.
    - **Remote IP/FQDN:** The IP address or Domain name of the remote PPTP server.
    - **User Name:** This is the PPTP server-provided user name.
    - **Password:** This is the PPTP server-provided password.
    - **Default Gateway/Remote Subnet:** Select and set this tunnel as the default gateway for the WAN connection. Or remote LAN subnet of the remote PPTP server.
    - **Authentication Protocol:** Choose from the following protocols: **PAP, CHAP,** or **MSCHAP(v1 or v2)**. The protocol you choose must be supported by remote PPTP server.
    - **MPPE Encryption:** Check to enable and select **40, 56,** or **128** bits. The MPPE needs to work with MSCHAP (v1 or v2) authentication.

- **NAT Before Tunneling: Enable** or **Disable** NAT before sending data over the PPTP tunnel.
- **LCP Echo Type:** Choose the appropriate connection keep alive.
- **Tunnel: Enable** if remote PPTP server requests it.

L2TP

L2TP Server

The VPN gateway can behave as a L2TP server and allows remote hosts to access LAN servers behind the L2TP server. The device can support three authentication methods: PAP, CHAP and MSCHAP(v1 and v2). Users can also enable MPPE encryption when using MSCHAP.

1. **L2TP Server:** Check to **Enable** or **Disable** this function.
2. **Client / Server:** Select **Server** mode.
3. **L2TP Client:** Check to **Enable** or **Disable** this function.
4. **Interface:** Select WAN interface for this L2TP server to use.
5. **L2TP over IPsec: Enable** or **Disable** and enter pre-shared key to authenticate with remote server.
6. **Server Virtual IP:** The IP address of L2TP server. This IP address should be different from IP address of the L2TP server and the LAN subnet of the VPN gateway.
7. **IP Pool Start Address:** This device assigns an IP address to the remote L2TP client. This value indicates the beginning of the IP pool.
8. **IP Pool End Address:** This device assigns an IP address to the remote L2TP client. This value indicates the end of the IP pool.
9. **Authentication Protocol:** Choose from three protocols: **PAP, CHAP,** or **MSCHAP (v1 or v2).**
10. **MPPE Encryption:** Check to enable and select **40, 56,** or **128** bits. The MPPE needs to work with MSCHAP (v1 or v2) authentication.
11. **Server Port:** Enter TCP port number L2TP server will be listening.
12. **L2TP Server Status:** Displays all the active L2TP clients that are connected to the L2TP server.
13. **User Account List:** Add username and password to allow connection to this L2TP server.

L2TP Client

1. **L2TP** Check to **Enable** or **Disable** this function.
2. **Client / Server:** Select **Client** mode.
3. **L2TP Client:** Check to **Enable** or **Disable** this function.
4. **L2TP Client List & Status:** Select Add, Delete and Refresh
    - **Tunnel Name:** The name of this client.
    - **Interface:** Select WAN interface for this PPTP client to use.
    - **L2TP Over IPsec: Enable** or **Disable.** Enter pre-shared key to authenticate with remote server.

- **Remote LNS IP/FQDN:** The IP address or Domain name of the remote PPTP server.
- **MTU:** Enter MTU value.
- **Remote LNS Port:** Enter remote TCP port number that remote LNS server is listening.
- **User Name:** This is the L2TP server-provided username.
- **Password:** This is the L2TP server-provided password.
- **Tunneling Password:** This is optional tunneling L2TP server-provided password.
- **Remote Subnet:** Enter remote LAN subnet of the remote L2TP server.
- **Authentication Protocol:** Choose from the following protocols: **PAP, CHAP,** or **MSCHAP (v1 or v2).** The protocol you choose must be supported by remote PPTP server.
- **MPPE Encryption:** Check to enable and select **40, 56,** or **128** bits. The MPPE needs to work with MSCHAP (v1 or v2) authentication.
- **NAT Before Tunneling:** Enable / Disable NAT before sending data over the PPTP tunnel.
- **LCP Echo Type:** Choose the appropriate connection keep alive type.
- **Service Port:** Enter TCP port number remote server is listening to.
- **Tunnel: Enable** or **Disable** this L2TP client tunnel.

GRE Tunnel

GRE Tunnel

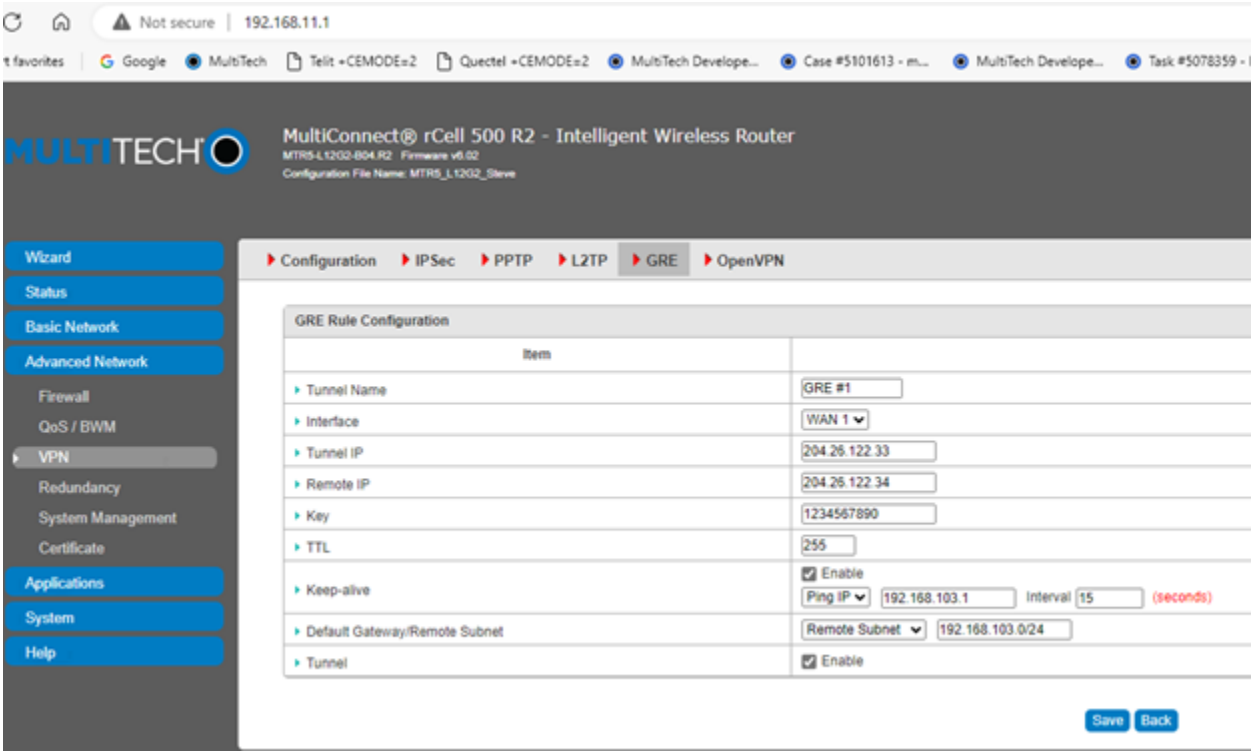
1. **GRE Tunnel:** Check to **Enable** or **Disable** this function.
2. **Default Gateway:** You can choose a tunnel as the default gateway for WAN connection.
3. **Tunnel Name:** The name of this GRE tunnel.
4. **Interface:** Choose a tunnel WAN interface.
5. **Operation Mode:** Choose a tunnel operation mode.
6. **Tunnel IP:** Assign a tunnel virtual IP address.
7. **Remote IP:** Enter the remote host IP address that you want to connect.
8. **Key:** Enter the password to establish the GRE tunnel with the remote host.
9. **TTL:** Time-To-Live for packets. The value is within **1** to **255**. If a packet passes a number of TTL routers and still can't reach the destination, the packet is dropped.
10. **Keep-alive:** Sending periodic data traffic in order to keep the tunnel active.
11. **Default Gateway/Remote Subnet:** Use default gateway or enter the remote host local subnet. If a packet wants to go to this subnet, the GRE tunnel is established automatically.
12. **DMVPN Spoke:** Check to Enable or Disable this function.
13. **IPsec Pre-shared Key:** Enter ipsec pre-shared key for use with the GRE tunnel.
14. **IPsec NAT Traversal:** Check to Enable or Disable this function.
15. **Ipsec Encapsulation Mode:** Select Transport or Tunnel mode.

16. **Tunnel:** Check to Enable or Disable the GRE tunnel.

GRE Tunnel Example

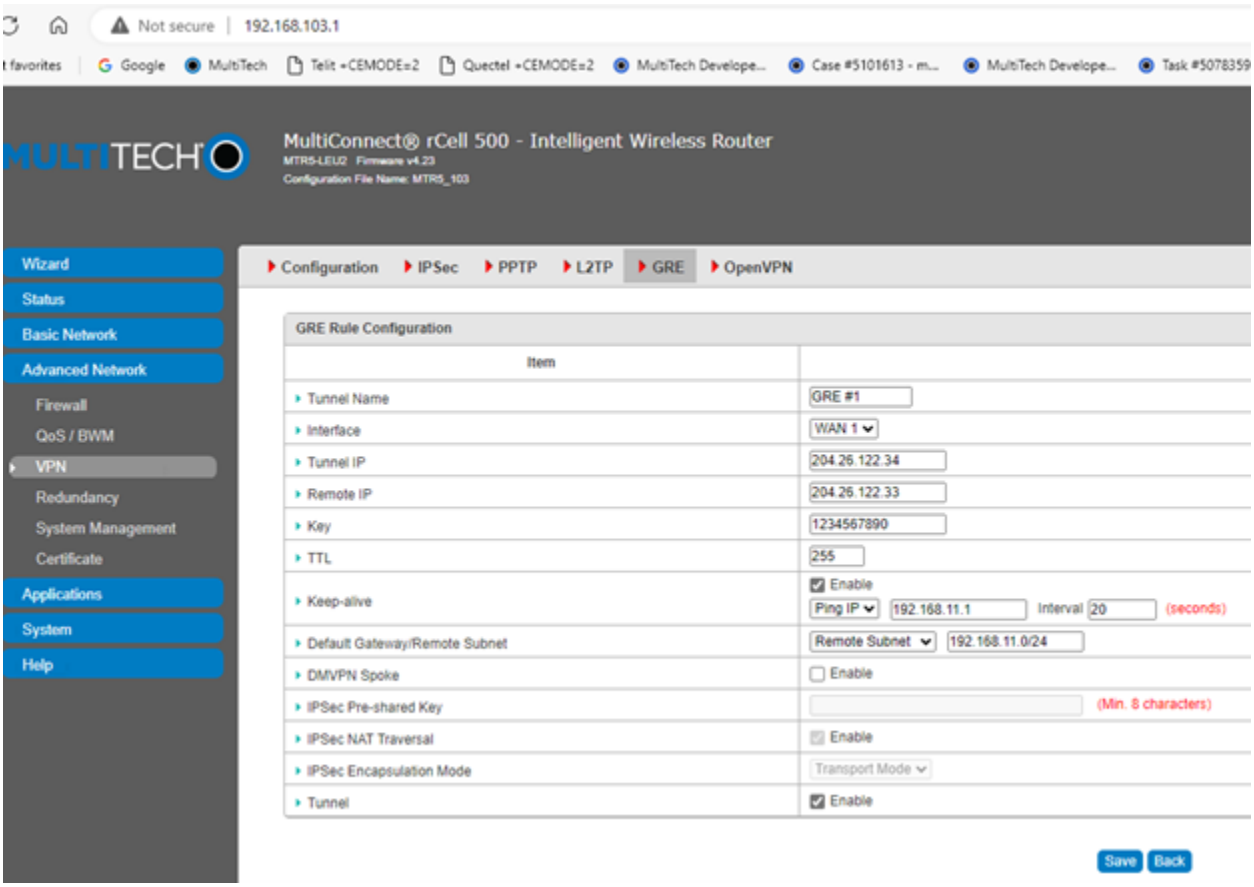
In MTR5 #1:

1. **Management IP address:** 192.168.11.1
2. **WAN port:** 204.26.122.33 / 24
3. **WAN Gateway:** 204.26.122.1 **GRE:** GRE#1; WAN 1; Tunnel IP: 204.26.122.33;
4. Remote IP: 204.26.122.34; Key: 1234567890; TTL: 255; Default G./ Remote Subn:192.168.103.0/24; keep-alive: enable, Ping IP 192.168.103.1, 15s; Tunnel: enable



In MTR5 #2:

1. **Management IP address:** 192.168.103.1
2. **WAN port:** 204.26.122.34 / 24
3. **WAN Gateway:** 204.26.122.1 /24
4. **GRE:** GRE#1; WAN 1; Tunnel IP: 204.26.122.34; Remote IP: 204.26.122.33; Key: 1234567890; TTL: 255; Default G./ Remote Subn:192.168.11.0/24; Keep-alive: enable, Ping IP 192.168.11.1, 20s interval; Tunnel: enable



MTR5#2 PC connected to MTR5 #2 has IP 192.168.103.100

- PC can successfully ping itself at 192.168.103.100
- PC can successfully ping Mgt LAN IP 192.168.103.1
- PC can successfully ping MTR5#1 WAN Port 204.26.122.34
- PC can successfully ping MTR5#2 WAN Port 204.26.122.33
- PC can successfully ping MTR5#2 LAN Mgt IP 192.168.11.1
- PC can successfully bring up browser and access 192.168.11.1 MTR5#2 Web administration.

MTR5#1 PC connected to MTR5 #1 has IP 192.168.11.198

- PC can successfully ping itself at 192.168.11.198
- PC can successfully ping Mgt LAN IP 192.168.11.1
- PC can successfully ping MTR5#1 WAN Port 204.26.122.33
- PC can successfully ping MTR5#2 WAN Port 204.26.122.34
- PC can successfully ping MTR5#1 LAN Mgt IP 192.168.103.1
- PC can successfully bring up browser and access 192.168.103.1 MTR5#1 Web administration.

OpenVPN

OpenVPN

1. **OpenVPN:** Check to **Enable** or **Disable** this function.
2. **Server / Client:** Select the WAN interface that the tunnel should use.

OpenVPN Client Setup

1. **OpenVPN Client Name:** Enter the name description for the tunnel.
2. **Interface:** Select the WAN interface that the tunnel should use.
3. **Protocol:** Select **TCP** or **UDP** protocol and enter Port number used to set up the tunnel.
4. **Tunnel Device:** Select tunnel type **TUN** or **TAP**.
5. **Remote IP/FQDN:** Enter remote server **IP** or **FQDN**.
6. **Remote Subnet:** Enter remote **subnet** and **netmask**.
7. **Authentication Mode:** Select **TLS** or **Static Key**.
    - **TLS:** Specify the certificates.
    - **Static Key:** Specify local IP, remote IP and static key used to set up the tunnel.
8. **Encryption Cipher:** Select Encryption type.
    - Blowfish
    - AES-256
    - AES-192
    - AES-128
    - None
9. **Hash Algorithm:** Select Hash Algorithm type.
    - SHA-1
    - MD5
    - MD4
    - SHA2-256
    - SHA2-512
    - None
10. **LZO Compression:** Select LZO compression type.
    - Adaptive
    - Yes
    - No
    - No Adaptive
11. Advanced Configuration: Check box to show advanced settings.

- **TLS Cipher:** If you require a high level of security, then set this parameter manually to prevent a version rollback attack in which a man-in-the-middle attacker tries to force two peers in to negotiate to the lowest level of security that they both support.
- **TLS Auth. Key:** Enter TLS authentication key.
- **User Name:** Username for authentication with remote OpenVPN server.
- **Password:** Password for authentication with remote OpenVPN server.
- **NAT:** Check the box to enable NAT for this tunnel.
- **Bridge TAP to:** Specify this setting to bridge the TAP interface to a certain local network interface or VLAN. Note: Bridge TAP will be available only when TAP is chosen in Tunnel Scenario and NAT is unchecked.
- **Firewall Protection:** Check the box to activate the Firewall Protection function. Note: Firewall Protection will be available only when NAT is enabled.
- **Client IP Address:** Specify the virtual IP Address for the OpenVPN Client. It can be Dynamic IP/Static IP.
- **Tunnel MTU:** Specify the value of Tunnel MTU. Value Range: 0 ~ 1500.
- **Tunnel UDP Fragment:** Specify the value of Tunnel UDP Fragment. Value Range: 0 ~ 1500. Note: Tunnel UDP Fragment will be available only when UDP is chosen in Protocol.
- **nsCertType Verification:** Check the Enable box to activate the nsCerType Verification function. Note: nsCerType Verification will be available only when TLS is chosen in Authorization Mode.
- **Redirect Internet Traffic:** Check the box to redirect and route all traffics over the tunnel.
- **TLS Renegotiation Time (seconds):** Specify the time interval of TLS Renegotiation Time. Value Range: -1 ~ 86400.
- **Connection Retry:** Specify the time interval of Connection Retry. The default -1 means that there is no need to execute connection retry. Value Range: -1 ~ 86400, and -1 means no retry is required.
- **DNS:** Specify the setting DNS. It can be Automatically/Manually.
- **Additional Configuration:** Additional OpenVPN server commands to be executed.

12. **Tunnel: Enable** or **Disable** this tunnel.

OpenVPN Server Setup

1. **OpenVPN Server:** Check box to enable server function.
2. **Protocol:** Select **TCP** or **UDP** protocol and enter port number used to set up the tunnel.
3. **Port:** Enter **TCP** or **UDP** port number that the tunnel uses to communicate.
4. **Tunnel Device:** Select tunnel type **TUN** or **TAP**.
5. **Authentication Mode:** Select **TLS** or **Static** key.
6. **Server Virtual ID:** Specify the Server Virtual IP address. Value Range: The IP format is 10.y.0.0, the range of y is 1~254.

   Note: Server Virtual IP will be available only when TLS is chosen in Authorization Mode.

7. **DHCP Proxy Mode:** Check the **Enable** box to activate the DHCP-Proxy Mode.

   Note: DHCP-Proxy Mode will be available only when TAP is chosen in Tunnel Device.

8. **IP Pool:** Specify the virtual IP pool setting for the OpenVPN server. You must specify the Starting Address and Ending Address as the IP address pool for the OpenVPN clients.

   Note: IP Pool will be available only when TAP is chosen in Tunnel Device and DHCP-Proxy Mode is unchecked (disabled).

9. **Gateway:** Specify the Gateway setting for the OpenVPN server. It will be assigned to the connected OpenVPN clients.

   Note: Gateway will be available only when TAP is chosen in Tunnel Device and DHCP- Proxy Mode is unchecked (disabled).

10. **Netmask:** Specify the Netmask setting for the OpenVPN server. It will be assigned to the connected OpenVPN clients. Value Range: 255.255.255.0/24 (only support class C).

    Note: Netmask will be available when TAP is chosen in Tunnel Device and DHCP-Proxy Mode is unchecked (disabled).

    Netmask will also be available when TUN is chosen in Tunnel Device.

11. **Encryption Cipher:** Select Encryption type.
    - Blowfish
    - AES-256
    - AES-192
    - AES-128
    - None

12. **Hash Algorithm:** Select Hash Algorithm type.
    - SHA-1
    - MD5
    - MD4
    - SHA2-256
    - SHA2-512
    - None

13. **LZO Compression:** Select LZO compression type.
    - Adaptive
    - Yes
    - No
    - No Adaptive

14. **Advanced Configuration:** Check box to show advanced settings.
    - **TLS Cipher:** If you require a high level of security, then you may want to set this parameter manually to prevent a version rollback attack in which a man-in-the-middle attacker tries to force two peers to negotiate to the lowest level of security that they both support.

- **TLS Auth. Key:** Enter TLS authentication key. Note: TLS authentication key will be available only when TLS is selected in Authorization Mode.
- **Redirect Default Gateway:** Remote client will have all traffics routed through the tunnel.
- **Client to Client:** Enable tells OpenVPN to internally route client-to-client traffic.
- **Duplicate CN:** Allow multiple clients with the same common name to concurrently connect.
- **Tunnel MTU:** Set MTU value for the tunnel.
- **Tunnel UDP Fragment:** Set UDP fragment value for the tunnel.
- **Tunnel UDP MSS-Fix:** Enable UDP MSS-Fix for the tunnel.
- **CDD-Dir Default File:** Server will execute the CCD-Dir Default File to save the settings as a client default.
- **Client Connection Script:** Server will execute the script after clients make connections.
- **Additional Configuration:** Additional OpenVPN server commands to be executed.

Redundancy

VRRP

The Virtual Router Redundancy Protocol (VRRP) is a computer networking protocol that allows a backup router or switch to automatically take over if the primary (master) router or switch fails. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP network.

1. **VRRP: Enable** or **Disable** this function.
2. **Virtual Server ID** (Group ID): Specify the VRRP virtual server ID number.
3. **Priority of Virtual Server:** Specify the priority to use in VRRP negotiations. Valid values are **1-254**. Larger values get higher priority.
4. **Virtual Server IP Address:** Specify the virtual server IP address.

System Management

TR-069

TR-069 (Technical Report 069) is a Broadband Forum technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices such as this gateway device. As a bidirectional SOAP/HTTP-based protocol, it provides the communication between customer-premises equipment (CPE) and TR-069 Auto Configuration Servers (ACS).

1. **TR-069:** Check to enable.
2. **Interface:** Select the WAN interface that TR-069 traffics will go out on.
3. **Contact your Service Provider:** TR-069 is a customized feature which is available depending on your Service Provider. They must be compatible with TR-069 to use it. Work with your Service

Provider to ensure proper set up of TR-069. Contact them directly with related questions or issues.

SNMP

Simple Network Management Protocol (SNMP) is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

1. **Enable SNMP**: Choose from **Local LAN** and/or **Remote WAN** to enable SNMP function. If Local is checked, this device will respond to the request from a LAN. If Remote is checked, this device will respond to a request from a WAN.
2. **SNMP Version:** Supports SNMP V1, V2c, and V3.
3. **Get Community:** The community of Get Request that this device will respond. This is a text password mechanism that is used to weakly authenticate queries to agents of managed network devices.
4. **Set Community:** The community of Set Request that this device will accept.
5. **Trap Event Receiver 1 to 4:** Enter the IP addresses or Domain Name of your SNMP Management PCs. You need to specify the IP address so the device can send SNMP Trap messages to the management PCs.
6. **WAN Access IP Address:** If you want to limit the remote SNMP access to a specific computer, enter the computer's IP address. The default value is 0.0.0.0 which means any internet connected computer can get the information of the device with the SNMP protocol.
7. **SNMPv3 Settings: User 1 to 5:** This device supports up to four SNMP management accounts. You can specify the account permission as **Read** or **Read/Write**.
    - **Username 1 to 5:** Use this field to identify the username for the specified access level.
    - **Password 1 to 5:** Use this field to set the password for the specified access level.
    - **Authentication 1 to 5:** Choose authentication options for the specified access level: **MD5** or **SHA-1**.
    - **Encryption 1 to 5:** CDES encryption is fixed.
    - **Privacy Mode 1 to 5:** Configure the SNMP privacy mode. Choose from the following options: **noAuthNoPriv** where both authentication and private key are not required, **authNoPriv** where no private key is required, or **authPriv** where both authentication and private key are required.
    - **Privacy Key 1 to 5:** Use this field to define the privacy key for the specified access level when privacy mode is set to **authPriv**.
    - **Authority 1 to 5:** Use this field to define the read or read/write access level.
    - **Enable 1 to 5: Enable** or **Disable** this user for access.

CLI (command line interface)

A command-line interface (CLI) is a means for debugging and troubleshooting the user (or client) issues. The interface is usually implemented with a command line shell. This shell is a program that accepts commands as text input and converts commands to the appropriate operating system functions. Programs with command-line interfaces are generally easier to automate via scripting. The device

supports both Telnet and SSH CLI with default service port 23 and 22 respectively. It also accepts commands from both the LAN and WAN sides.

1. **CLI:** Check LAN and/or WAN to allow CLI access.
2. **Connection Type:** Check Telnet and/or SSH to allow CLI access and specify TCP port number.

DeviceHQ™ (Device Management)

DeviceHQ can monitor and reboot the device, plus perform remote software and configuration updates. Before configuring your device to work with DeviceHQ, you must register for an account and request Device API support at https://www.devicehq.com.

To configure your device to use DeviceHQ:

1. **DeviceHQ: Enable** or **Disable** to use DeviceHQ device management service..
2. **Server Name:** Enter www.devicehq.com for the DeviceHQ server URL.
3. **Server Port:** Enter 443 for HTTPS.
4. **API Secret:** Find this information in your DeviceHQ account. Characters are case sensitive.
5. **API Auth Token:** Find this information in your DeviceHQ account. Characters are case sensitive.
6. **Check-in Interval:** How often the device will check into DeviceHQ. Default is 240 minutes.
7. Click **Save.**

   Note: Click **Check In To DeviceHQ** button to perform manually check into DeviceHQ as soon as possible. WAN connection must be active and have full internet access for check-in to be successful.

Certificate

In cryptography, a public key certificate (also known as a digital certificate or identity certificate or identity certificate) is an electronic document used to prove ownership of a public key. The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified that the certificate's contents are genuine. If the signature is valid and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner.[1]

In a typical public-key infrastructure (PKI) scheme, the signer is a certificate authority (CA). A CA is usually a company such as VeriSign which charges customers to issue certificates for it. In a web of trust scheme, the signer is either the key's owner (a self-signed certificate) or other users ("endorsements") whom the person examining the certificate might know and trust. The device also plays as a CA role.

Certificates are an important component of Transport Layer Security (TLS, previously called SSL), where they prevent an attacker from impersonating a secure website or other server. They are used in other important applications such as email encryption and code signing. Here, certificates can be used in IPSec or OpenVPN tunneling for user authentication.

Configuration

The configuration setting allows the user to create a Root Certificate Authority (CA) certificate and configure to set enable of SCEP. Root CA is the top-most certificate of the tree; its private key is used to "sign" other certificates.

When **Generate** is applied, the **Root CA Certificate Configuration** screen appears. The required information for the root CA includes name, key, subject name, and validity.

Field	Requirements	Definition
Name	String format. Can be any text. Required field.	Enter a root certificate name. It will be a certificate file name.
Key	Required field.	Specifies the key attributes of the certificate. ▪ **Key Type** sets public-key cryptosystems and currently only supports RSA. ▪ **Key Length** sets the size of the key used in a cryptographic algorithm, measured in bits. ▪ **Digest Algorithm** sets the identifier in the signature algorithm certificate identifier.
Subject name	Required field.	▪ **Country (C)** is the two-letter ISO code for the country where your organization is located. ▪ **State (ST)** is the state where your organization is located. ▪ **Location (L)** is the location of your organization. ▪ **Organization (O)** is the name of your organization. ▪ **Organization Unit (OU)** is the name of your organization unit. ▪ **Common Name (CN)** is the name of your organization. ▪ **Email** is the email of your organization, including the suffix (.com, .net or other).
Validity Period	Required field.	Specifies the validity period of the certificate.
SCEP	Unchecked by default.	Check **Enable** to activate **SCEP**.
Automatically re-enroll aging certificates	Unchecked by default.	When **SCEP** is activated, check **Enable** to activate this function. This will automatically check which certificate is aging and activate the SCEP function to re-enroll automatically.
Save	N/A	Click **Save** to save the settings.
Undo	N/A	Click **Undo** to cancel the settings.

My Certificates

My Certificate includes a Local Certificate List. The Local Certificate List shows all generated certificates by the root CA for the gateway. It also stores the generated Certificate Signing Requests (CSR) which will be signed by other external CAs. The signed certificates can be imported as the local ones of the gateway.

The My Certificate setting allows a user to create local certificates. On the My Certificate page, there are two configuration windows for the My Certificate function. The Local Certificate List window shows the stored certificates or CSRs for representing the gateway. The Local Certificate Configuration window lets

you fill in the required information for a corresponding certificate to be generated by itself, or corresponding CSR to be signed by other CAs.

When **Add** is applied, the **Local Certificate Configuration** screen will appear. The required information for the certificate or CSR includes the name, key, and subject name. It is a certificate if the **Self-signed** box is checked; otherwise, it is a CSR.

Field	Requirements	Definition
Name	String format. Can be any text. Required field.	Enter a certificate name. It will be a certificate file name. If Self-Signed is checked, it will be signed by root CA. If Self-signed is not checked, it will generate a certificate signing request (CSR).
Key	Required field.	Specifies the key attributes of the certificate. ■ **Key Type** sets public-key cryptosystems and currently only supports RSA. ■ **Key Length** sets the size of the key used in a cryptographic algorithm, measured in bits. Key length can be 512, 768, 1024, 1536, 2048. ■ **Digest Algorithm** sets the identifier in the signature algorithm certificate identifier. Digest Algorithm can be MD5/SHA-1.
Subject name	Required field.	■ **Country (C)** is the two-letter ISO code for the country where your organization is located. ■ **State (ST)** is the state where your organization is located. ■ **Location (L)** is the location of your organization. ■ **Organization (O)** is the name of your organization. ■ **Organization Unit (OU)** is the name of your organization unit. ■ **Common Name (CN)** is the name of your organization. ■ **Email** is the email of your organization, including the suffix (.com, .net or other).
Extra attributes	Required field.	Specifies the extra information for generating a certificate. ■ **Challenge Password:** The password that you can use to request certificate revocation in the future. ■ **Unstructured Name:** For additional information.

Field	Requirements	Definition
SCEP Enrollment	Unchecked by default.	Specifies the information of SCEP. To generate a certificate signing request that is then signed by the SCEP server online, check **Enable**. Select a SCEP server to identify the SCEP server for use. Find server information in External Servers. Navigate to **Object Definition** > **External Server** > **External Server**. Click **Add Object** to generate. Select a **CA Certificate** to identify which certificate is accepted by SCEP server for authentication. It is generated in **Trusted Certificates**. If required, select a **CA Encryption Certificate** to identify which certificate is accepted by the SCEP server for encryption data information. It is generated in **Trusted Certificates**. Enter an optional **CA Identifier** to identify which CA is used for signing certificates.
Save	N/A	Click **Save** to save the settings.
Back	N/A	Click **Back** to return to the previous page.

When **Import** is applied, an **Import** screen appears. You can import a certificate from an existing certificate file or directly paste a PEM encoded string as the certificate.

Field	Requirements	Definition
Import	Required field.	Select a file from the computer, then click **Apply** to import the specified certificate file to the gateway.
PEM Encoded	String format. Can be any text. Required field.	Alternative to importing a certificate. Copy and paste the PEM encoded certificate string, then click **Apply** to import the certificate to the gateway.
Apply	N/A	Click **Apply** to import the certificate.
Cancel	N/A	Click **Cancel** to discard the Import operation and return to the **My Certificates** page.

Trusted Certificates

Trusted Certificate includes Trusted CA Certificate List, Trusted Client Certificate List, and Trusted Client Key List. The Trusted CA Certificate List places the certificates of external trusted CAs. The Trusted Client Certificate List places the others' certificates that you trust. The Trusted Client Key List places the others' keys that you trust.

Import Trusted CA Certificate

When **Import** is applied, a Trusted CA Import screen appears. You can import a Trusted CA certificate from an existing certificate file, or directly paste a PEM encoded string as the certificate.

Field	Requirements	Definition
Import from a File	Required field.	Select a CA Certificate file from the computer, then click **Apply** to import the specified CA certificate file to the gateway.
Import from a PEM	String format. Can be any text. Required field.	Alternative to importing a CA certificate. Copy and paste the PEM encoded CA certificate string, then click **Apply** to import the specified CA certificate to the gateway.
Apply	N/A	Click **Apply** to import the certificate.
Cancel	N/A	Click **Cancel** to discard the Import operation and return to the **My Certificates** page.

Instead of importing a Trusted CA certificate with mentioned approaches, you can also get the CA certificate from the SECP server.

If **SCEP** is enabled (Refer to **Object Definition** > **Certificate** > **Configuration**), you can click **Get CA** button, a Get CA Configuration screen will appear.

Field	Requirements	Definition
SCEP Server	Required field.	Select **SCEP Server** to identify the SCEP server for use. The server detailed information is specified in External Servers. Go to **Object Definition** > **External Server** > **External Server**. Click **Add Object** to generate.
CA Identifier	String format. Can be any text.	Fill in optional **CA Identifier** to identify which CA is used for signing certificates.
Save	N/A	Click **Save** to save the settings.
Close	N/A	Click **Close** to return to the **Trusted Certificates** page.

Import Trusted Client Certificate

When **Import** is applied, a **Trusted Client Certificate Import** screen will appear. You can import a Trusted Client Certificate from an existing certificate file, or directly paste a PEM encoded string as the certificate.

Field	Requirements	Definition
Import from a file	Required field.	Select a certificate file from the computer and click **Apply** to import the specified certificate file to the gateway.
Import from a PEM	String format. Can be any text. Required field.	Alternative to importing a certificate. Copy and paste the PEM encoded certificate string and click **Apply** to import the specified certificate to the gateway.
Apply	N/A	Click **Apply** to import the certificate.
Cancel	N/A	Click **Cancel** to discard the import operation and return to the **Trusted Certificates** page.

Import Trusted Client Key

When **Import** is applied, a **Trusted Client Key Import** screen will appear. You can import a Trusted Client Key from an existing file, or directly paste a PEM encoded string as the key.

Field	Requirements	Definition
Import from a file	Required field.	Select a certificate key file from the computer and click **Apply** to import the specified key file to the gateway.
Import from a PEM	String format. Can be any text. Required field.	Alternative to importing a certificate key. Copy and paste the PEM encoded certificate key string and click **Apply** to import the specified certificate key to the gateway.
Apply	N/A	Click **Apply** to import the certificate.
Cancel	N/A	Click **Cancel** to discard the import operation and return to the **Trusted Certificates** page.

Issue Certificates

When you have a Certificate Signing Request (CSR) that needs to be certificated by the root CA of the device, you can issue the request here and let Root CA sign it. There are two approaches to issue a certificate: 1) from a CSR file importing from the managing PC, or 2) copy and paste the CSR codes into gateway's web-based utility. After completing one of these options, click **Sign.**

If the gateway signs a CSR successfully, the **Signed Certificate View** window shows the resulted certificate contents. In addition, click **Download** to download the certificate to a file in the managing PC.

Import and Issue Certificate

Field	Requirements	Definition
Certificate Signing Request (CSR) Import from a File	Required field	Select a certificate signing request file from your computer for importing to the gateway.
Certificate Signing Request (CSR) Import from a PEM	String format. Can be any text. Required field.	Copy and paste the certificate signing request PEM encoded certificate to the gateway.
Sign	N/A	Click **Sign** to issue the imported certificate by the root CA.

7 Applications

This device is equipped with a 3G/4G module as a WAN interface. It also provides an SMS feature and SMS management.

Mobile Application

SMS

Users can send certain SMS to this gateway to activate some actions, such as connect, disconnect, reconnect WAN connection, or reboot the system. The gateway can also send SMS alerts to users about some events automatically.

Configuration:

1. **Physical Interface:** Indicate which 3G/LTE modem is used for SMS feature.
2. **SMS:** Indicate which SIM card is used for SMS feature.
3. **SMS Storage:** Choose storage for SMS messages. This gateway only supports **SIM Card Only** for SMS storage.

Alert Rule List: This gateway can forward receive SMS message automatically via Alert rule. Press Add and enter details below to add a new rule.

1. **From Phone Number:** Indicate the sender's phone number.
2. **Alert Approach:** Decide the way to forward the message. You can forward to another phone number, an email address, or a syslog server.
3. **Destination:** Enter the receiver's phone number if you select **Auto-forward**, an email address if choosing **By Email** or enter the syslog IP address if you choose **Syslog**.
4. **Enable:** Click **Enable**.

SMS Summary: You can compose a new SMS message and check received SMS messages on this gateway.

1. **Unread SMS:** Indicates number of unread SMS messages.
2. **Received SMS:** Indicates number of total received SMS messages.
3. **Remaining SMS:** Indicates number of new messages that can be received based on SMS storage limit.

Create New SMS Message

1. Click **Create New SMS Message**.
2. Enter message content and phone number(s) of the receiver(s).
3. Click **Send** .
    - System displays **Send OK** message when successfully sent.

Read New SMS Message

You can read, delete, reply, and forward messages in the inbox section.

1. **Refresh:** Click **Refresh** to renew SMS lists.
2. **Delete, Reply, Forward Messages**: After reading message(s), check to the right of targeted message(s) to delete, reply, or forward.

Remote Management

Management Settings:

1. **Remote Management via SMS:** Check to enable this function.
2. **Delete SMS for Remote Management:** Enable to delete received SMS message for remote management purpose. This option can help manage SIM card storage space preventing messages from filling it up. If SIM storage is full, this gateway can't receive any new SMS.
3. **Security Key:** This security key will be used for authentication when this gateway receives an SMS command. Type this key first and then a command. There should be a blank space between the key and the command (e.g., 1234 reboot). If this field is empty, enter the command without adding any key information.

   Note: If the security key is empty, access control needs to be activated.

Command Settings:

1. **Status:** When enabled, send the **Status** command which queries the WAN connection status. For 3G/LTE WAN, the router will send back the WAN IP address, network name, network type, and connection time via SMS. For Ethernet WAN, the router will send back the WAN IP address and connection time via SMS.
2. **Connect:** When enabled, send the **Connect** command to start the WAN connection.
3. **Disconnect:** When enabled, send **Disconnect** command to disconnect the WAN connection.

   Note: If this gateway receives a **Disconnect** command from SMS, it won't try to connect again no matter if the WAN connection mode is set to auto-reconnect.
4. **Reconnect:** When enabled, send the **Reconnect** command to disconnect and restart the WAN connection again immediately.
5. **Reboot:** When enabled, send the **Reboot** command to restart the router. After the device receives this reboot command, it replies with an SMS message to the sender.

Notification Settings:

1. **WAN Link Up:** When enabled, this gateway will send a message to users if the WAN connection is established. This message will also include the WAN IP address.
2. **WAN Link Down:** When enabled, this gateway sends a message to users if the primary WAN connection is dropped.
3. **Data Allowance:** When enabled, this gateway will send a message to users when cellular WAN data allowance usage is reached.

Access Control List Settings:

1. **Access Control:** Users can decide which phone number sends commands to this gateway or receives notifications when enabling this option.
2. **Phone 1 to 5:** For security, this gateway ignores a command if the phone number is not in the list (even if the security key is correct). The phone number must contain the international prefix or country code (i.e. + +1234567890). You can assign specific phone numbers that can send commands and/or receive notifications.
3. **Phone Range 1 to 4:** Allow setup with a range of phone numbers for the SMS management function only. The range of numbers can be specified between 17630000000 and 17639999999. This allows any mobile numbers starting with 1763xxxxxxx to send SMS management commands to the modem.

Captive Portal

Captive Portal Configuration

This gateway supports the Captive Portal function via external cloud service provider www.hotspotsystem.com. This feature allows you to configure a public Wi-Fi hotspot with user authentication and usage management. First, obtain all the external RADIUS (Remote Authentication Dial in User Service) server and external UAM (Universal Access Method) server information from your service provider in order to configure this feature. Also, verify that you have one account and password for user authentication to access the Internet.

External Captive Portal

Before enabling external Captive Portal function, go to **System > External Servers** to define external server objects like the RADIUS server and UAM server.

1. **Captive Portal:** Enable this function.
2. **WAN Interface:** Select the WAN interface for accessing external servers for user authentication and Internet access
3. **LAN Subnet:** Select the VLAN group (Intranet) that users need to be authenticated before Internet surfing. DHCP-1 means that the server can assign its IP address dynamically for each host of the VLAN group.
4. **Authentication Server**: Select a RADIUS Server from the predefined list in **System > External Server**.
5. **UAM Server:** Enable and select a predefined external UAM server from the list in **System > External Server**.

Note: When you enable this feature, all internet packets from hosts using new MAC addresses in the dedicated VLAN group will be forwarded to the gateway's Captive Portal Website.

Digital IO

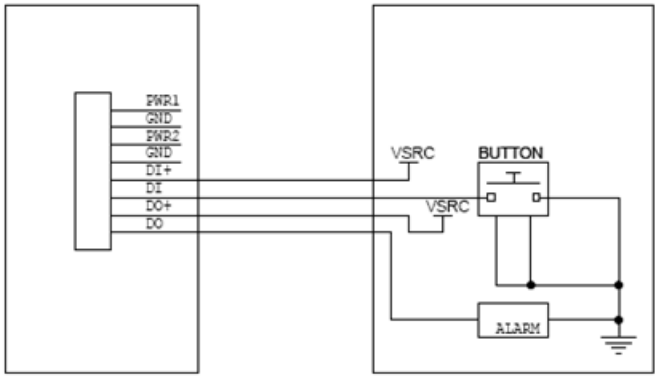
This gateway can setup notifying events to send SMS or Email when digital input is trigger. It can manage events using SMS or digital input to trigger and set digital output.

Digital IO Hardware Specification

There are a DI (digital input) and a DO (digital output) port together with power terminal block. Refer to following specification to connect DI and DO devices.

Mode		
Digital Input	Trigger Voltage (high)	Logic level 1: 5V~30V
	Normal Voltage (low)	Logic level 0: 0V~2V
Digital Output	Voltage (Relay Mode)	Depends on external device maximum voltage is 30V
	Maximum Current	1A

Example of Digital IO Connection diagram



Configuration

1. **Event Management: Enable** or **Disable** digital input and output events.
2. **SMS Account List:** Create SMS phone numbers that will be used for managing events and notifying events.
3. **Email Service List:** Create email addresses that will be used for digital input notifying events.
4. **Digital Input (DI) Profile List:** Create and define digital input profiles for notifying events.
   - **DI Profile Name:** Enter digital input profile name.
   - **Description:** Enter description for this profile.
   - **DI Source:** Only one digital input source available.
   - **Normal Level:** Select low or high for the normal level.
   - **Signal Active Time:** Enter input signal change active time in seconds before trigger an event.
   - **Profile: Enable** or **Disable** this profile.

5. **Digital Output (DO) Profile List:** Create and define digital output profiles for managing events.
    - **DO Profile Name:** Enter digital output profile name.
    - **Description:** Enter description for this profile.
    - **DO Source:** Only one digital output source available.
    - **Normal Level:** Select low or high for the normal level.
    - **Total Signal Period:** Enter the total time in ms that output signal needs to be active.
    - **Repeat & Counter:** Enable repeat and how many times to repeat the active output signal.
    - **Duty Cycle:** Enter percentage of the Total Signal period time need to be active.
    - **Profile: Enable** or **Disable** this profile.

Managing Events

1. **Managing Events: Enable** or **Disable** digital output managing events.
2. **Managing Event List:** Click **Add** to create and define digital output signal for managing event.
    - **Event Name:** Enter event name.
    - **Event:** Select event based on **SMS** or **Digital Input**. For SMS, enter mobile phone number. For Digital Input, select digital input profile defined in main event configuration.
    - **Trigger Type:** Set to **Once** only when SMS is selected. Set to **Period** when Digital Input is selected.
    - **Description:** Enter description for this event.
    - **Action:** Enable digital output action and select the digital output profile defined in main event configuration.
    - **Managing Event: Enable** or **Disable** this managing event.

Notifying Events

1. **Notifying Events: Enable or Disable** digital input notifying events.
2. **Notifying Event List:** Click **Add** to create and define digital input signal for notifying event.
    - **Event Name:** Enter event name.
    - **Event:** Only input trigger based one Digital Input.
    - **Trigger Type:** Select how digital input signal is detected, it is based on period of one time only. If it is period, then define the interval time.
    - **Description:** Enter description for this event.
    - **Delay to Send:** when digital input is detected, delay the configured time in seconds before sending the notifying event.
    - **Action:** Check and enable SMS and / or Email Alert for the notifying event.
    - **Time Schedule:** Select Always or pre-defined time schedule in Schedule Rule setting.
    - **Notifying Event: Enable** or **Disable** this notifying event.

Digital Output

1. **TCP Server:** Enable or Disable digitaloutput as TCP server.
2. **TCP Port number:**Enter TCP port number for server to listen to.
3. **Command String:** string should have format :DOA 1, 50
   - :DOA means digital output
   - 1 means relay number 1
   - 50 is the relay on time in units of 20 ms, so 50 means the relay should be on for 1 second. If the message is :DOA,1,100 instead, then the relay should be on for 2 seconds instead.

8 Operation

System Related

This section includes system information, system logs, system tools (like firmware updates), scheduling, and external server setup.

Change Password

Admin Account Configuration

1. Enter a new **Username** for the Web UI and CLI login to replace the default username, “admin.”
2. Type in your old and new **Password**.
3. Click **Save** to store your settings or click **Undo** to give up your changes.

User Account Confirmation

1. Enter a new **Username** for the user account with limited web UI login to replace the default username, “guest.”
2. Type in your new **Password**.
3. Click **Save** to store your settings or click **Undo** to give up your changes.

Others

Others option allows you to set:

1. **Web administration timeout** when there are no activities on web user interface.
2. **Hardware Watchdog** option to **Enable** or **Disable** internal hardware watchdog lockup detection.

System Information

This section displays System information for WAN interface, current date / time, and Device Serial number

System Status

Options to View log, email log or send log to external syslog server.

1. **Web Log:** Check and enable the type of logs.
2. **Email Alert:** Check to **Enable** email alert.
    - **Server List:** Select configured email server from the **External Servers** list.
    - **E-mail Addresses:** Enter the email addresses of log recipients. Assign multiple recipients by separating each address with a semicolon (;) or comma (,).
    - **E-mail Subject:** Enter email subject title.
    - **Syslogd:** Check and enable logging to the external configured syslog server.

3. **Log to Storage:**
    - **Enable:** Check to enable logging to internal or external USB storage.
    - **Select Device:** Select internal or external USB device to store log files.
    - **Log File name:** Define log filename to use when saving log files.
    - **Split File:** Check to enable split log file based on define file size in KB or MB.
    - **Interval:** Check and define time interval to save the log file.
    - **Max number of log files:** Enter the maximum number of log files to be saved in storage.
    - **Download log file:** Click to download all the saved log files.
    - **Clear Logs:** Clear all saved log files and start over.
    - **Log type Category:** Enter email subject title.
4. Click **Save** to store the settings.

System Tools

Options to setup System Time, perform Firmware Upgrade, Ping Test, Trace Route Test, Reboot or Schedule Reboot, Reset to factory default, Wake up on LAN and Backup configuration settings.

1. **System Time:** Configure time zone and select sync current time and date with external time server or local PC time.
2. **Firmware Upgrade:** Perform firmware upgrade by select local firmware BIN file.

   Note: To check the current firmware version, refer to the top of the page after login.
3. **Ping Test:** Perform ping test to specified Host IP address via LAN or WAN interface.
4. **Tracert Test:** Perform trace route test to specified Host IP address via LAN or WAN interface.
5. **Reboot:** Select reboot now or set a time for auto reboot to occur.
6. **Reset to Default:** Reset all settings back to factory default.
7. **Backup or Restore Configuration Settings:** Enter the config name that will be used when backup configuration file is perform. Click **Configuration Restore** and select configuration file on local PC to restore.

Packet Analyzer

The Packet Analyzer can capture network packets and depending on user settings and can be used for troubleshooting network issues. User can specify LAN or WAN interfaces to capture packets and filter by setting rules. Captured packets can be downloaded and view using the Wireshark application.

Field	Requirements	Definition
Packet Analyzer	Unchecked by default.	Check **Enable** to activate the Packet Analyzer.
File Name	Enter capture file name to be used. For example: <**Interface**>_<**Date**>_<**index**>.	Enter the file name to save the captured packets in log storage. The extension file name is .pcap.

Field	Requirements	Definition
File Size	Enter file size to capture.	Maximum filed size is 5MB. Select LAN or WAN interface and click downward to save file to local PC.
Packet Interface	Check interface box.	At least one interface is required, but multiple selections are also accepted.
Save	N/A	Click **Save** to save the configuration.

Once you have enabled the Packet Analyzer function on specific interfaces, you can further specify some filter rules to capture the packets that matched the rules.

Field	Requirements	Description
Filter	Optional	Check **Enable** to activate the Capture Filter function.
Source MACs	Optional	Define the filter rule with Source MACs, which means the source MAC address of packets. ■ Packets that match the rule will be captured. ■ Up to 10 MACs are supported, but they must be separated with a semicolon. For example: AA:BB:CC:DD:EE:FF; 11:22:33:44:55:66
Source IPs	Optional	Define the filter rule with Source IPs, which means the source IP address of packets. ■ Packets that match the rule will be captured. ■ Up to 10 IPs are supported, but they must be separated with a semicolon. For example: 192.168.1.1; 192.168.1.2
Source Ports	Optional	Define the filter rule with **Source Ports**, the source port of packets. ■ The packets will be captured when they match any port in the rule. ■ Up to 10 ports are supported, but they must be separated with a semicolon. For example: 80; 50 ■ Value range: 1 ~ 65535
Destination MACs	Optional	Define the filter rule with **Destination MACs**, the destination MAC address of packets. ■ Packets that match the rule will be captured. Up to 10 MACs are supported, but they must be separated with a semicolon. For example: AA:BB:CC:DD:EE:FF; 11:22:33:44:55:66 ■ The packets will be captured when they match any one MAC in the rule.

Field	Requirements	Description
Destination IPs	Optional	Define the filter rule with **Destination IPs**, the destination IP address of packets. ▪ Packets that match the rule will be captured. ▪ Up to 10 IPs are supported, but they must be separated with a semicolon. For example: 192.168.1.1; 192.168.1.2 ▪ The packets will be captured when match any one IP in the rule.
Destination Ports	Optional	Define the filter rule with **Destination Ports**, the destination port of packets. ▪ The packets will be captured when they match any port in the rule. ▪ Up to 10 ports are supported, but they must be separated with a semicolon. For example: 80; 53 ▪ **Value Range:** 1 ~ 65535

Scheduling

1. **Enable** schedule function and setup rule with time range for each schedule. The rule can be used in many other functions such as schedule reboot, schedule filtering, schedule WAN connectivity, etc.
2. Click **Save** to store all the scheduled settings .

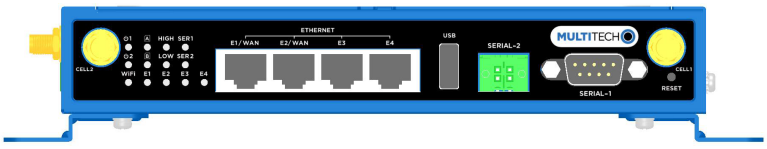
External Servers

1. Configure external server for the different types of services such as email server, syslog server, or captive portal Radius and UAM server. These servers can be used with other functions such as **Email alert**, **syslog, digital IO events**, and **Captive Portal**.
2. Click **Save** to store all the server settings.

Reset the Device

Prerequisite: A pin, paperclip, or similar thin object that can fit into the reset hole.

The following is the default condition for the RESET button on the device. You can program a change to the behavior of the button if needed.



To reset the device:

1. Find the hole labeled RESET. The Reset button is recessed into the case.

2. Use the pin to press and release the Reset button as follows:
   - To reset to factory settings, press Reset for 20 seconds or longer:
     a. The device restarts in factory default setup mode. The system automatically removes all user accounts.
     b. Enter a default username admin and password admin to create your new administrative password.

9 Disposal

Instructions for Disposal of WEEE by Users in the European Union

The symbol shown below is on the product or on its packaging, which indicates that this product must not be disposed of with other waste. Instead, it is the user's responsibility to dispose of their waste equipment by handing it over to a designated collection point for the recycling of waste electrical and electronic equipment. The separate collection and recycling of your waste equipment at the time of disposal will help to conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment. For more information about where you can drop off your waste equipment for recycling, contact your local city office, your household waste disposal service or where you purchased the product.

July, 2005

10 Regulatory Information

FCC 47 CFR Part 15 Regulation Class B Devices

(For model MTR5-L12G2-B04.R2 only)

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

FCC Interference Notice

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

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

EMC, Safety, and Radio Equipment Directive (RED) Compliance

(For model MTR5-LEU2-B04.R2 only)

CE The CE mark is affixed to this product to confirm compliance with the following European Community Directives:

Environmental Notices

EU WEEE Directive

Note: This statement may be used in documentation for your final product applications.

The Waste from Electrical and Electronic Equipment (WEEE) Directive places an obligation on EU-based manufacturers, distributors, retailers, and importers to take back electronics products at the end of their useful life. A sister directive, ROHS (Restriction of Hazardous Substances) complements the WEEE

Directive by banning the presence of specific hazardous substances in the products at the design phase. The WEEE Directive covers all MultiTech products imported into the EU as of August 13, 2005. EU-based manufacturers, distributors, retailers and importers are obliged to finance the costs of recovery from municipal collection points, reuse, and recycling of specified percentages per the WEEE requirements.

EU RoHS 3 Directive

MultiTech confirms that all products comply with the chemical concentration limitations set forth in the Restriction of Hazardous Substances in Electrical and Electronic Equipment (RoHS 3) regulations for CE and UKCA, following the standard EN IEC 63000:2018.

For the current Certificate of Compliance for Hazardous Substances and additional regulatory documents, go to https://multitech.com/approvals-and-certifications/.

Warranty

To read the warranty statement for your product, go to https://www.multitech.com/warranty.

Contact Information

General Information	info@multitech.com https://multitech.com/contact-us/
Sales	+1 (763) 785-3500 sales@multitech.com
Technical Support Portal	+1 (763) 717-5863 https://support.multitech.com
Website	www.multitech.com
World Headquarters	2205 Woodale Drive Mounds View, MN 55112 USA