

MultiConnect[®] rCell 500 Series Router User Guide

MultiConnect® rCell 500 Series Router User Guide

Model: MTR5-LEU2

Part Number: S000589

Copyright

This publication may not be reproduced, in whole or in part, without the specific and express prior written permission signed by an executive officer of Multi-Tech Systems, Inc. All rights reserved. **Copyright © 2014 by Multi-Tech Systems, Inc.**

Multi-Tech Systems, Inc. makes no representations or warranties, whether express, implied or by estoppels, with respect to the content, information, material and recommendations herein and specifically disclaims any implied warranties of merchantability, fitness for any particular purpose and non-infringement.

Multi-Tech Systems, Inc. reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Multi-Tech Systems, Inc. to notify any person or organization of such revisions or changes.

Legal Notices

The Multi-Tech 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.

MULTI-TECH 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 MULTI-TECH WARRANT ANY CONNECTION OR ACCESSIBILITY TO ANY CELLULAR COMMUNICATIONS NETWORK. MULTI-TECH 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.

The Multi-Tech products and the final application of the Multi-Tech products should be thoroughly tested to ensure the functionality of the Multi-Tech 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 Multi-Tech product is integrated operates as intended and meets its requirements or the requirements of its direct or indirect customers. Multi-Tech 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 Multi-Tech 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.

Contacting Multi-Tech

Knowledge Base

The Knowledge Base provides immediate access to support information and resolutions for all Multi-Tech products. Visit <http://www.multitech.com/kb.go>.

Support Portal

To create an account and submit a support case directly to our technical support team, visit: <https://support.multitech.com>.

Support

Business Hours: M-F, 8am to 5pm CT

Country	By Email	By Phone
Europe, Middle East, Africa:	support@multitech.co.uk	+(44) 118 959 7774
U.S., Canada, all others:	support@multitech.com	(800) 972-2439 or (763) 717-5863

Warranty

To read the warranty statement for your product, visit www.multitech.com/warranty.go. For other warranty options, visit www.multitech.com/es.go.

World Headquarters

Multi-Tech Systems, Inc.

2205 Woodale Drive, Mounds View, MN 55112

Phone: (800) 328-9717 or (763) 785-3500

Fax (763) 785-9874

Contents

Product Overview	6
Package Contents	7
System Requirements	9
LED Indicators	10
Specifications	11
RF Specifications	13
Installing and Using the Router	14
Installing SIM Cards.....	14
Attaching Cables and Antennas	15
Using Setup Wizard.....	15
Basic Network	17
WAN Setup.....	17
Physical Interface	17
Internet Setup	17
WAN	18
4G WAN.....	18
Ethernet WAN	19
Static IP	19
Dynamic IP	19
PPP over Ethernet	19
PPTP	20
L2TP.....	20
LAN and VLAN Setup.....	21
Ethernet LAN.....	21
VLAN.....	21
Port-Based VLAN	21
Tag-Based VLAN	21
WiFi Setup	22
AP Router Mode.....	22
WDS Hybrid Mode	23
WDS Only Mode.....	24
Wireless Client List.....	25
Advanced Configuration.....	25
IPv6 Setup	25
Static IPv6.....	25
DHCPv6.....	26
PPPoE	26


6 to 4	26
6 in 4	27
NAT Setup	27
NAT Loopback	27
Virtual Server	27
Virtual Computers	27
Special AP	27
DMZ	28
Routing Setup	28
Static Routing	28
Dynamic Routing	28
Routing Information	28
Client/Server	28
Dynamic DNS	28
Serial Port	29
Port Configuration	29
Virtual COM	29
TCP Client Mode	29
TCP Server Mode	29
UDP Mode	30
RFC2217 Mode	30
Modbus	30
Advanced Network	32
Firewall	32
Packet Filters	32
URL Blocking	32
MAC Control	32
Options	33
Quality of Service	34
QoS Configuration	34
Rule-based QoS	34
Create a QoS Rule	34
VPN Setup	36
VPN-IPSec	36
Dynamic IP VPN	36
IPSec-IKE Setting	37
IPSec-Manual Setting	39
VPN-PPTP Server	39
VPN-PPTP Client	40
VPN-L2TP Server	40
VPN-L2TP Client	41

GRE Tunnel.....	41
Redundancy.....	42
VRRP.....	42
System Management.....	43
TR-069.....	43
SNMP.....	43
Applications.....	44
Mobile Application.....	44
SMS.....	44
Create Message.....	45
Inbox.....	45
System.....	46
System Information.....	46
System Status.....	46
Web Log.....	46
Syslog.....	46
Email Alert.....	46
System Tools.....	46
Change Password.....	46
FW Upgrade.....	47
System Time.....	47
Others.....	47
MMI.....	48
Web UI.....	48
Safety Warnings.....	49
Lithium Battery.....	49
Ethernet Ports.....	49
Radio Frequency (RF) Safety.....	49
Interference with Pacemakers and Other Medical Devices.....	50
Potential interference.....	50
Precautions for pacemaker wearers.....	50
Regulatory Information.....	51
EMC, Safety, and R&TTE Directive Compliance.....	51
Restriction of the Use of Hazardous Substances (RoHS).....	52
Waste Electrical and Electronic Equipment Statement.....	52
WEEE Directive.....	52
Instructions for Disposal of WEEE by Users in the European Union.....	52
Information on HS/TS Substances According to Chinese Standards.....	54
Information on HS/TS Substances According to Chinese Standards (in Chinese).....	55

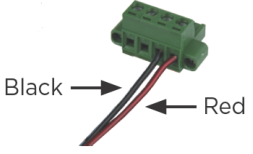

Product Overview

Thank you for purchasing the MultiConnect rCell 500 Series. The MultiConnect rCell 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	Description
	One MultiConnect rCell 500
	Two 4G Antennas
	Two WiFi Antennas
	One Power Adapter (DC12/2A). The maximum power consumption is 15.5W.
	One RJ-45 Cable
	One Console Cable
	Two Wall Mount Kits
	One DIN-Rail Bracket





PACKAGE CONTENTS

Contents	Description
 <p>Black → ← Red</p>	Power Port
	Four Rubber Feet

System Requirements


Network Requirements	<ul style="list-style-type: none">■ An Ethernet RJ-45 cable or DSL modem■ 4G cellular service subscription■ 802.11b/g/n wireless clients■ 10/100 Ethernet adapter
Configuration Utility Requirements	<ul style="list-style-type: none">■ Operating System Requirements<ul style="list-style-type: none">■ Windows®XP with SP2 or higher■ Macintosh■ Linux-based operating system■ Browser Requirements<ul style="list-style-type: none">■ Internet Explorer 9.0 or higher■ Chrome 2.0 or higher■ Firefox 3.0 or higher■ Safari 3.0 or higher

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 will choose power source 1 first. In this instance, the LED for power source 2 will remain OFF.
WLAN (WiFi)	WIFI	Continuously ON: Wireless radio is enabled. Flashing: Data packets are being transferred. OFF: Wireless radio is disabled.
SIM A		Continuously ON: SIM A is in use.
SIM B		Continuously ON: SIM B is in use.
LAN1 - LAN 4	E1 - E4	Continuously ON: Ethernet connection is established. Flashing: Data packets are being transferred.
High 4G Signal	HIGH	Continuously ON: Strong 4G signal strength.
Low 4G Signal	LOW	Continuously ON: Weak 4G signal strength.
USB	USB CELL	Continuously ON: USB device is attached.
Serial Port	SER.	Flashing: Serial data is being transferred.

Specifications

MTR5-LEU2

Category	Description
General	
Performance	LTE, HSPA+GSM/GPRS/EDGE
Frequency Bands	LTE FDD: B1/B2/B3/B5/B7/B8/B20 HSPA+ Band: 850/900/1900/2100 MHz GSM/GPRS/EDGE Band: 850/900/1800/1900 MHz
Radio	
Cellular	4G LTE Radio
Wi-Fi	802.11 b/g/n
Speed	
Packet Data	Up to 100 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
WiFi	Two Reverse polarity male SMA connector for Wi-Fi
SIM Holder	Two Mini-SIM, standard 1.8 V and 3 V SIM receptacle 
Power Requirements	
Voltage	9 V to 48 V DC
Physical Description	
Dimensions	Dimensions are shown in the section “Dimensions” that follows.
Weight	TBD
Environment	
Operating Temperature	-10° C to +60° C
Humidity	Relative humidity 15% to 93% non-condensing

Category	Description
Certifications, Compliance, Warranty	
EU Compliance	R&TTE
Safety Compliance	IEC 60950-1
Network Compliance	GCF
Warranty	Two years

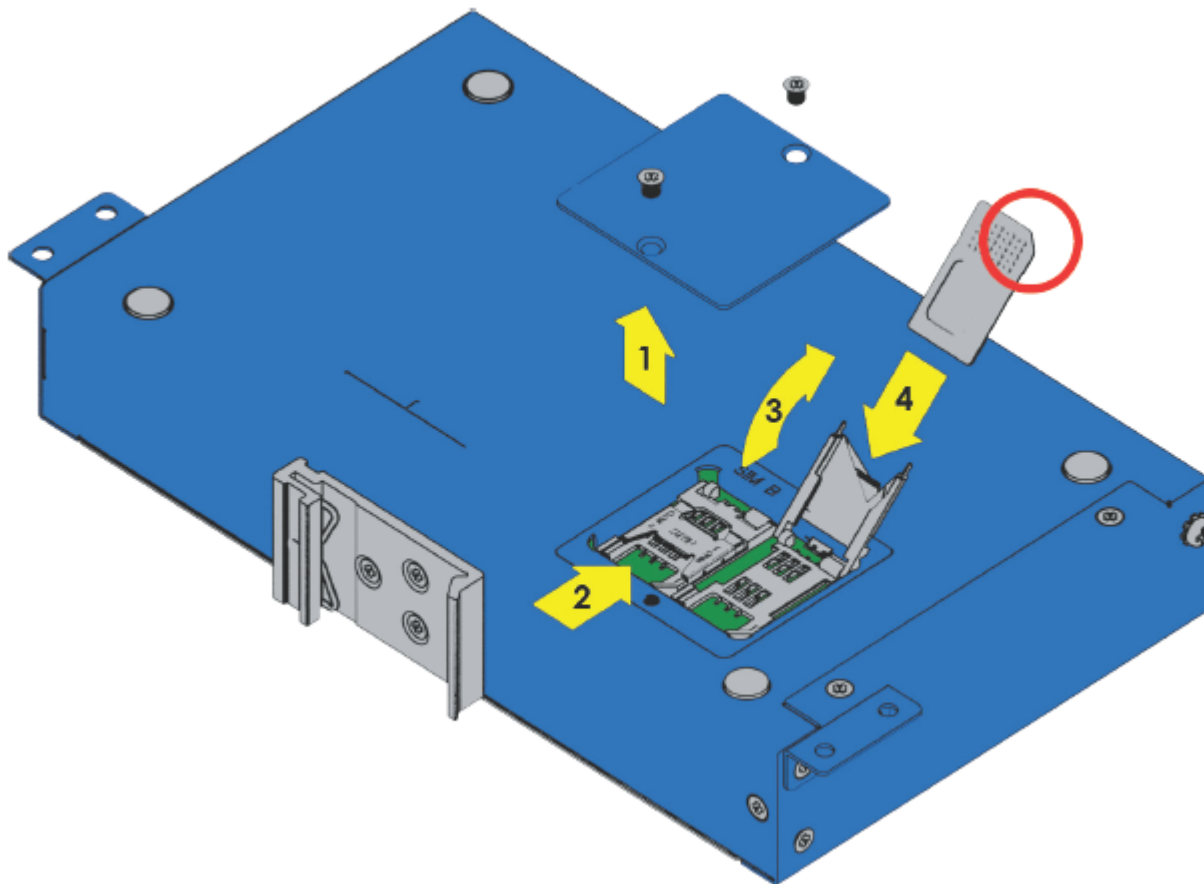
Note: The radio's performance may be affected at the temperature extremes. This is considered normal. There is no single cause for this function. It is the result of an interaction of several factors, such as the ambient temperature, the operating mode, and the transmit power.

RF Specifications

Operating Band	Tx	Rx
UMTS Band I	1920 MHz - 1980 MHz	2110 MHz - 2170 MHz
UMTS Band II	1850 MHz - 1910 MHz	1930 MHz - 1990 MHz
UMTS Band V	824 MHz - 849 MHz	869 MHz - 894 MHz
UMTS Band VIII	880 MHz - 915 MHz	925 MHz - 960 MHz
GSM 850	824 MHz - 849 MHz	869 MHz - 894 MHz
GSM 900	880 MHz - 915 MHz	925 MHz - 960 MHz
GSM 1800 (DCS)	1710 MHz - 1785 MHz	1805 MHz - 1880 MHz
GSM 1900 (PCS)	1850 MHz - 1910 MHz	1930 MHz - 1990 MHz
LTE Band I	1920 MHz - 1980 MHz	2110 MHz - 2170 MHz
LTE Band II	1850 MHz - 1910 MHz	1930 MHz - 1990 MHz
LTE Band III	1710 MHz - 1785 MHz	1805 MHz - 1880 MHz
LTE Band V	824 MHz - 849 MHz	869 MHz - 894 MHz
LTE Band VII	2500 MHz - 2570 MHz	2620 MHz - 2690 MHz
LTE Band VIII	880 MHz - 915 MHz	925 MHz - 960 MHz
LTE Band XX	832 MHz - 862 MHz	791 MHz - 821 MHz

Installing and Using the Router

Installing SIM Cards



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

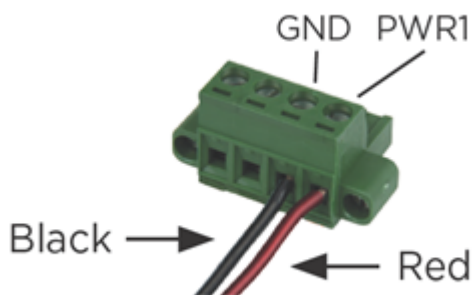
Note: Before installing or changing the SIM card, make sure the device is turned OFF and power is disconnected.

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 to the device's front panel by screwing them into the designated connectors.
2. Attach WiFi antennas to the device's 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.



Using Setup Wizard

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 is **admin**.

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 login password of the web UI. Click **Next**.
3. Select the correct **Time Zone**. Click **Next**.
4. Select the WAN type and address. Click **Next**.
5. Setup the LAN address and Subnet Mask. Click **Next**.
6. Setup WiFi connection. Click **Next**.
7. Verify that the Wifi Router Network setup summary is correct. Click **Apply**.
8. Apply and Restart.

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 1:** You can configure the fourth Ethernet port as a WAN. To setup, plug in the Ethernet cable from an external modem and follow UI setup.
- **3G/4G WAN 2:** There is one 3G/4G built in modem. To setup, insert SIM card and follow UI setup.
- **3G/4G WAN 3:** There is one USB port that supports a 3G/4G dongle. To setup, plug in the dongle and follow 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.

WAN 2: This interface is disabled by default. Click **Edit** to configure. There are three operation options for this interface.

WAN 3: This interface is disabled by default. Click **Edit** to configure. There are three operation options for this interface.

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.

Internet Setup

There are three 3G/4G WAN interfaces that you can setup individually. These interfaces support an ISP that provides LTE, HSPA+, HSPA, WCDMA, EDGE, GPRS data services, and xDSL or Cable connections with Dynamic IP, Static IP, PPPoE, PPTP, and L2TP connection types.

WAN Type	Description
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	IP Address is different each connection.
Static IP Address	IP Address is the same each connection.

WAN Type	Description
PPP over Ethernet (PPPoE)	Widely used for ADSL connections.
PPTP	This WAN type is used primarily in Russia.
L2TP	The WAN type is used primarily in Israel.

WAN

Click **Edit**, next to the WAN type you want view or configure.

- **Physical Interface:** Choose **Ethernet, 3G/4G, or USB 3G/4G**.
- **Operation Mode:** WAN-1 is set to **Always on**. Options are **Always on, Failover, or Disable** for other WAN connections.
- **Line Speed:** Manually set your upload and download Mbps.

4G WAN

1. Under the **Internet Setup** tab, click **Edit** for WAN-1.
2. Check to **Enable** Network Monitoring. Then **Save**.
3. On the **Physical Interface** tab, click **Edit** for WAN-2.
4. Under **Operation Mode**, choose **Failover** for WAN-1 from the dropdown list. Then **Save**.
5. On the **Internet Setup** tab, click **Edit** for WAN-2.
6. Set **WAN Type** as **3G/4G**.
7. For **Preferred SIM Card**, select **SIM-A**.
8. Under **Dial-up Profile**, choose either **Auto-detection** or **Manual-configuration**.
 - a. For **Manual Configuration** complete the following:
 - i. Select **Country**.
 - ii. Under **Service Providers**, choose appropriate **Service Provider** or **Others**.
 - iii. Manually enter in **APN, PIN Code (if needed), Dial Number, Account, and Password (if needed)**.
Note: If you chose a Service provider, some of the information will be automatically populated.
 - iv. Set **Authentication** to **Auto**.
 - v. **Primary** and **Secondary DNS** may be left blank. All other settings can be left at default.
 - vi. Click **Save**.
 - b. For **Auto-detection** enter **PIN Code (if needed)** and click **Save**.
9. Select **Status** from the menu on the left.
10. Select **Network status** from the list.
11. Verify that WAN-2 shows under WAN Interface IPv4 Network Status.

To Verify Cellular Failover/Fallback is working, complete the following:

1. While on the **Network Status** page, pull the primary WAN Ethernet cable from the E1/WAN interface.
2. Monitor WAN-2 connection status. It will go from **connecting** to **connected**.
Note: This will take approximately 45 seconds.
3. Plug back in the primary WAN Ethernet cable. The WAN-2 connection status will show **disconnected**.

Ethernet WAN

To access the Ethernet WAN settings, click **Internet Setup**. Click **Edit** next to the Ethernet WAN you want to configure.

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 appropriate IP address, subnet mask, and gateway address provided to you. The device will not accept IP addresses that are not in the correct format.

- **WAN IP Address:** Enter the provided IP Address.
- **WAN Subnet Mask:** Enter the provided subnet mask.
- **WAN Gateway:** Enter the gateway address.
- **Primary DNS:** Enter the primary DNS IP Address.
- **Secondary DNS:** Enter the secondary DNS. Can be left blank if your ISP doesn't supply one.
- **MTU:** The default value is 0 (Auto).
- **NAT:** Check to enable. If you enable, there will be no NAT mechanism between the LAN and WAN.
- **Network Monitoring:** Check to enable.
- **IGMP:** Choose Enable or Disable the IGMP snooping function. When enabled, the device will detect all IGMP messages exchanged. This prevents multicast flooding on an Ethernet link.
- **WAN IP Alias:** Some ISPs will provide a fixed IP address for management purposes, enter that into this field.

Dynamic IP

To configure a Dynamic IP the following fields are available:

- **Host Name:** This field is optional, but required by some ISPs.
- **ISP Registered MAC address:** Enter the registered MAC address, or click **Clone** to copy your PC's MAC address.
- **Connection Control:** Select the connection control scheme from the list. Options are: **Auto-Reconnect (Always on)**, **Connect-on-Demand**, and **Connect Manually**.
- **MTU:** The default value is 0 (Auto).
- **NAT:** Check to enable. If you enable, there will be no NAT mechanism between the LAN and WAN.
- **Network Monitoring:** Check to enable.
- **IGMP:** Choose to Enable or Disable the IGMP snooping function. When enabled, the device will detect all IGMP messages exchanged. This prevents multicast flooding on an Ethernet link.
- **WAN IP Alias:** Some ISPs will provide a fixed IP address for management purposes, enter that into this field.

PPP over Ethernet

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

- **IPv6 Dual Stack:** Check to enable. Enable this option if your ISP provides one IPv4 and one IPv6 address.
- **PPPoE Account:** Enter the account provided by your ISP.
- **PPPoE Password:** Enter the password provided by your ISP.
- **Primary DNS:** Enter the primary DNS IP Address.

- **Secondary DNS:** Enter the secondary DNS IP Address. Can be left blank if your ISP doesn't supply one.
- **Connection Control:** Select the connection control scheme from the list. Options are: **Auto-Reconnect (Always on), Connect-on-Demand, and Connect Manually.**
- **Service Name:** Your ISP may provide you with a specific service name when connecting with PPPoE.
- **Assigned IP Address:** Your ISP may provide you with a fixed IP address for this type of connection.
- **MTU:** The default value is 0 (Auto).
- **NAT:** Check to enable. If you enable, there will be no NAT mechanism between the LAN and WAN.
- **Network Monitoring:** Check to enable.
- **IGMP:** Choose to Enable or Disable the IGMP snooping function. When enabled, the device will detect all IGMP messages exchanged. This prevents multicast flooding on an Ethernet link
- **WAN IP Alias:** Some ISPs will provide a fixed IP address for management purposes, enter that into this field.

PPTP

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.

- **IP Mode:** Select the IP Mode assigned by your ISP. If you select **Static IP Address** you will need to enter the IP address, subnet mask, and gateway IP provided by your ISP.
- **Server IP Address/Name:** IP address of the PPTP server provided by your ISP.
- **PPTP Account:** Enter the account provided by your ISP.
- **PPTP Password:** Enter the password provided by your ISP.
- **Connection ID:** Enter the connection ID if required by your ISP.
- **Connection Control:** Select the connection control scheme from the list. **Auto-Reconnect (Always on), Connect-on-Demand, and Connect Manually** are the available options.
- **MTU:** The default value is 0 (Auto).
- **MPPE:** Enable this option to add encryption on transferred and received data packets.
- **NAT:** Check to enable. If you enable, there will be no NAT mechanism between the LAN and WAN.
- **Network Monitoring:** Check to enable.
- **IGMP:** Choose to Enable or Disable the IGMP snooping function. When enabled, the device will detect all IGMP messages exchanged. This prevents multicast flooding on an Ethernet link
- **WAN IP Alias:** Some ISPs will provide a fixed IP address for management purposes, enter that into this field.

L2TP

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

- **IP Mode:** Select the IP Mode assigned by your ISP. If you select **Static IP Address** you will need to enter the IP address, subnet mask, and gateway IP provided by your ISP.
- **Server IP Address/Name:** IP address of the L2TP server provided by your ISP.
- **L2TP Account:** Enter the account provided by your ISP.
- **L2TP Password:** Enter the password provided by your ISP.
- **Connection Control:** Select the connection control scheme from the list. Options are: **Auto-Reconnect (Always on), Connect-on-Demand, and Connect Manually.**

- **MTU:** The default value is 0 (Auto).
- **MPPE:** Enable this option to add encryption on transferred and received data packets.
- **NAT:** Check to enable. If you enable, there will be no NAT mechanism between the LAN and WAN.
- **Network Monitoring:** Check to enable.
- **IGMP:** Choose 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
- **WAN IP Alias:** Some ISPs will provide a fixed IP address for management purposes, enter that into this field.

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

- **IP Mode:** Static IP Address
- **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 this is changed, you will need to type in the new IP address into a browser to see the web UI.
- **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.

VLAN

The VLAN function allows you to divide a local network into "virtual LANs." In some cases, an ISP may need a router to support certain services. This device supports port-based VLAN and tag-based VLAN. You can 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 **Edit** next to the port you want to configure.

- **Type:** Select NAT or BRIDGE to identify if the packets are directly bridged to the WAN port or processed by a NAT mechanism.
- **LAN VID:** The ports with the same VID are in the same VLAN.
- **Tx TAG:** Select if the ISP requires a VLAN Tag with outgoing data.
- **DHCP Server:** Specify a DHCP server. This device provides up to four DHCP servers to handle requests from different VLANs.

Tag-Based VLAN

In a tag-based VLAN, groups are assigned tags and ports are no longer specifically assigned. To configure a tag-based VLAN, click **Edit** next to the VLAN you want to configure.

- **VLAN ID:** Specify a VLAN tag for this group. The ports with the same VID are in the same VLAN.
- **Internet Access:** Check to enable internet access.
- **Port:** Check the desired ports.

- **DHCP Server:** Specify a DHCP server. This device provides up to four DHCP servers to handle requests from different VLANs.

WiFi Setup

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

This device supports the following wireless operation modes: **AP Router Mode**, **WDS Hybrid Mode**, and **WDS Only Mode**.

AP Router Mode

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

- **WiFi Module:** Enables the wireless function.
- **WiFi Operation Mode:** Select AP Router Mode.
- **Green AP:** When there is no wireless traffic, enable Green AP to reduce power consumption.
- **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**.
- **Network ID (SSID) & Broadcast:** Network ID identifies the wireless LAN. Client stations can roam freely over this and other access points with the same Network ID. If the Broadcast option is unchecked, wireless clients can't find the gateway through a wireless network scan.
- **WLAN Partition:** Enabling this option separates the wireless clients so that they can't communication with each other, but can access the internet and other Ethernet LAN devices.
- **Channel:** The default radio channel number is set to **auto**. To reduce radio interference, choose a channel that is not used in your environment.
- **WiFi System:** The default setting is **B/G/N mixed**. You can also choose **N only** or **G/N Mixed**.
- **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 WiFi 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.
WPA	In this mode you have to 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 .
WPA2-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.

Authentication Type	Description
WPA2	In this mode you have to 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	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 and you have to specify the IP address and port number for the RADIUS server.

WDS Hybrid Mode

While acting as a wireless bridge, Wireless Router 1 and 2 can communicate with each other through WDS.

- **Lazy Mode:** Lazy mode automatically learns the MAC address of WDS peers. Not all APs can be set to enable Lazy mode simultaneously. There must be at least one AP with all WDS MAC addresses filled. Check to enable this option.
- **Green AP:** Enable this function to reduce the power consumption when there is no wireless traffic.
- **Time Schedule:** The wireless radio can be turned off according to a schedule rule. By default, the wireless radio is always turned on when the wireless module is enabled.
- **Network ID (SSID) & Broadcast:** The network ID is used to identify the WLAN. Client stations can roam freely over this device and other access points with the same Network ID. Check to enable Broadcast. If this is disabled, the wireless clients will not find this gateway through a wireless network scan.
- **WLAN Partition:** Check to enable the WLAN partition function to separate the wireless clients. When this is enabled, wireless clients can't communicate with each other, but they can access the Internet and other Ethernet LAN devices.
- **Channel:** The channel number needs to be the same as the channel number of the peer AP.
- **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 WiFi 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.
WPA	In this mode you have to 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 .
WPA2-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.

Authentication Type	Description
WPA2	In this mode you have to 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	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 and you have to specify the IP address and port number for the RADIUS server.

WDS Only Mode

The WDS function lets the access point act as a wireless LAN and rep

- **Lazy Mode:** Lazy mode automatically learns the MAC address of WDS peers. Not all APs can be set to enable Lazy mode simultaneously. There must be at least one AP with all WDS MAC addresses filled. Check to enable this option.
- **Green AP:** Enable this function to reduce the power consumption when there is no wireless traffic.
- **Channel:** The channel number needs to be the same as the channel number of the peer AP.
- **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 WiFi 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.
WPA	In this mode you have to 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 .
WPA2-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	In this mode you have to 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	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 and you have to specify the IP address and port number for the RADIUS server.

Wireless Client List

The Wireless Client List page you can see the connected wireless clients. You can 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.

- **Beacon Interval:** Beacons are broadcast packets that are sent by a wireless AP/router.
- **DTIM Interval:** When the wireless router has buffered a broadcast or multicast messages for clients, it sends a DTIM with a DTIM interval value.
- **RTS Threshold:** Adjusting the RTS threshold value can improve wireless performance if there is an excessive number of wireless packet collisions.
- **Fragmentation:** Wireless frames are divided into smaller units to improve performance in the presence of RF interference.
- **WMM:** WMM helps control latency and jitter when transmitting multimedia content over a wireless connection.
- **TX Rate:** Choose **Best** for auto-adjustment based on WiFi signal quality in the current environment.
- **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 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:

- **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 prefix length of the Subnet Mask.
 - **Default Gateway:** Enter the default gateway.
 - **Primary/Secondary DNS:** Add IPv6 primary and secondary DNS addresses.
- **LAN IPv6 address settings:** Enter the LAN IPv6 address and ignore the LAN IPv6 Link-Local address.
- **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 time period that the router broadcasts its router advertisements.

DHCPv6

When DHCPv6 is selected, do the following:

- **IPv6 DNS (WAN IPv6 address) Settings:** Choose **Obtain DNS Server address Automatically** or **Use the following DNS address**.
- **LAN IPv6 address settings:** Enter the LAN IPv6 address and ignore the LAN IPv6 Link-Local address.
- **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 time period that the router broadcasts its router advertisements.

PPPoE

When PPPoE is selected, do the following:

- **WAN IPv6 address settings:**
 - **Username:** Enter username provided by ISP.
 - **Password:** Enter password provided by ISP.
 - **Service Name:** Enter service name provided by ISP
 - **Reconnection Mode:** Leave setting as **AutoReconnect (always-on)**.
 - **MTU:** The default MTU value is 0 (auto).
- **LAN IPv6 address settings:** Enter the LAN IPv6 address and ignore the LAN IPv6 Link-Local address.
- **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 time period that the router broadcasts its router advertisements.

6 to 4

When 6 to 4 IPv6 is selected, do the following:

- **6 to 4 Settings:** Obtain IPv6 DNS automatically or set DNS address manually for both primary and secondary DNS.
- **LAN IPv6 address settings:** Enter the LAN IPv6 address and ignore the LAN IPv6 Link-Local address.
- **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 time period that the router broadcasts its router advertisements.

6 in 4

When 6 in 4 is selected, do the following:

- **6 in 4 Tunnel Settings:** Add remote/local IPv4 address and local IPv6 address, then set primary and secondary DNS addresses manually.
- **LAN IPv6 address setting:** LAN IPv6 address and LAN IPv6 Link-Local address
- **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 time 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. If you wish, 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 Server IP. Virtual Server can work with Scheduling Rules, and give user more flexibility on Access control. For the details, please refer to Scheduling 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.

- **Global IP:** Enter the global IP address assigned by your ISP.
- **Local IP:** Enter the local IP address of your LAN PC corresponding to the global IP address.
- **Enable:** Check this item to enable the Virtual Computer feature.

Special AP

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 the 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” to add the predefined setting to your list.

- **Trigger:** The outbound port number issued by the application.
- **Incoming Ports:** When the trigger packet is detected, the inbound packets sent to the specified port numbers are allowed to pass through the firewall.
- **Enable:** Check this item to enable the Special AP feature.

DMZ

DMZ (DeMilitarized Zone) Host is a host without the protection of 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 indicate that LAN computer as a DMZ host to solve this problem.

Note: This feature should be used only when needed.

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, then enable or disable by using the associated checkbox.

Dynamic Routing

Dynamic routing is used when there are lots of 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.
- **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.

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 particular network destinations. The routing table contains information about the topology of the network immediately around it. The routing information page 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 have to 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.

- **DDNS:** Check to enable.
- **Provider:** The DDNS provider supports service for you to bind your IP with a certain domain name.
- **Host Name:** Register a domain name to the DDNS provider.
- **Username/E-mail:** Enter username or e-mail based on the DDNS provider requirements.
- **Password/Key:** Enter password or key based on the DDNS provider requirements.

Serial Port

This device has one DB-9 male port used for serial communication. To use, connect an RS-232 or RS-485 serial device to an IP-based Ethernet LAN.

Port Configuration

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

- **Operation Mode:** Choose the purpose of the port. It can be Virtual COM or Modbus. To prevent unknown serial devices from connecting, you can 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 if you want to connect a device and communicate with it by this protocol.
- **Interface:** Choose RS-232 or RS-485
- **Baud Rate:** Set the baud rate (bps) of the serial port. The value can be 9600, 19200, 38400, 57600, or 115200.
- **Data Bits:** Choose 7 or 8 as the data bit.
- **Stop Bits:** Choose 1 or 2 as the stop bit.
- **Flow Control:** Choose RTS/CTS, DTS/DSR, or None for flow control.
- **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 established 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.

- **Operation Mode:** Choose TCP Client.
- **Connection Control:** To keep the connection with the TCP server all the time, choose Always On. To keep the connection only when transmitting data, choose ON-Demand.
- **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.
- **Alive Check Timeout:** The TCP connection will be terminated if it doesn't receive a response from the alive-check.
- **To Host:** Click Edit to enter IP address or FQDN of the remote host (TCP server).
- **Remote Port:** Enter the TCP port of the remote host.
- **Definition:** Check to enable the rule.

TCP Server Mode

In TCP Server Mode, a unique IP:Port address is provided on a TCP/IP network. This operation mode supports up to four simultaneous connections at the same time.

- **Operation Mode:** Choose TCP Client.
- **Listen Port:** Enter the listening port of the TCP connection.
- **Trust Type:** Choose **Allow All** to allow all TCP clients to connect. Choose **Specific IP** to allow certain TCP clients.
- **Max Connection:** Set the maximum number of concurrent TCP connections. Up to four connections can be established at the same time.
- **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.
- **Alive Check Timeout:** The TCP connection will be terminated if it doesn't receive a response from the alive-check.
- **Definition:** Check to enable the rule.

If choosing **Specific IP** in Trust Type, enter the IP address range of allowed TCP clients.

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.

- **Operation Mode:** Choose UDP.
- **Listen Port:** Enter the listening port of the UDP connection.
- **Host:** Click Edit to enter IP address range of remote UDP hosts.
- **Remote Port:** Enter the UDP port of peer UDP hosts.
- **Definition:** 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 host and serial device by mapping the IP:Port of the gateway's serial port to a local COM port on the host computer.

- **Operation Mode:** Choose RFC-23217.
- **Listen Port:** Enter the listening port of the connection.
- **Trust Type:** Choose **Allow All** to allow all hosts to connect. Choose **Specific IP** to allow certain hosts.
- **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.
- **Alive Check Timeout:** The TCP connection will be terminated if it doesn't receive a response from the alive-check.

Modbus

Modbus supports traditional RS-232/422/485 devices and recently developed Ethernet devices. It is used 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.

- **Operation Mode:** The Modbus Gateway enables conversions between serial and network Modbus protocols.

- **Serial Protocol:** Defines the protocol used on serial communication.
- **Listen Port:** Defines the TCP or UDP port that Masters connect to.
- **Serial Response Timeout:** If the serial side does not respond within a specific time, data is dropped and not transmitted.
- **Serial Timeout Retries:** If set to **0**, the gateway doesn't store TCP packets in the buffer. If 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.
- **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.
- **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.
- **Tx Delay:** The minimum amount of time after receiving a message before the next message can be sent out.
- **TCP Connection Idle Timeout:** Idle timeout, in seconds, for the Modbus /TCP connection. If no response within the time limit the connection is closed.
- **Maximum TCP Connection:** A maximum of four simultaneous Modbus /TCP connections is allowed.
- **Trusted IP Access:** Defines the IP that is allowed to connect to the gateway.
- **Modbus Priority:** Defines the priorities from specific IPs, Modbus IDs, or Function Codes.

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. You can select two filtering policies:

- Allow all to pass, except those match the specified rules.
- Deny all to pass, except those match the specified rules.

Enabling the Log Alert will record events that are blocked by these rules.

You can specify rules for each direction, inbound or outbound. For each rule, you can define the following:

- Source IP address or range. You can define a single IP address or a range of IP addresses. Leaving this empty implies all IP addresses.
- Destination IP address or range.
- Destination Port: You can define a single port or a range of ports.
- Protocol: TCP, UDP, or both.
- Use Rule Schedule #.

Each rule can be enabled or disabled individually.

URL Blocking

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

- **URL Blocking:** Check to enable URL Blocking.
- **Black List/White List:** Choose one of the following conditions:
 - Allow all to pass, except those match the specified rules.
 - Deny all to pass, except those match the specified rules.
- **Log Alert:** Check to enable Log Alert. This will record events that are blocked by these rules.
- **Invalid Access Web Redirection:** Users will see a specific webpage to know their access is blocked by a rule.
- **URL:** If any part of the website's URL matches the pre-defined word, the connection will be blocked. Up to 10 pre-defined words in a rule and each URL keyword separated by a comma can be entered.
- **Schedule:** The rule can be turned off according to a schedule rule.
- **Enable:** Check to enable each rule.

MAC Control

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

- **MAC Control:** Check to enable MAC Control.
- **Black List/White List:** Choose one of the following conditions:
 - Allow all to pass, except those match the specified rules.
 - Deny all to pass, except those match the specified rules.
- **Log Alert:** Check to enable Log Alert. This will record events that are blocked by these rules.
- **Known MAC from LAN PC List:** All connected clients and their MAC Address are displayed.
- **MAC Address:** Enter the MAC address of the local device.
- **Schedule:** The rule can be turned off according to a schedule rule.
- **Enable:** Check to enable each rule.

Options

- **Stealth Mode:** When enabled, the router will not respond to port scans from the WAN, thus making it less susceptible to discovery and attacks.
- **SPI ("Stateful Packet Inspection" also known as "dynamic packet filtering"):** helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through that session conforms to the protocol.
- **Discard PING from WAN Side:** When enabled, this gateway won't reply any ICMP request packet from WAN side.
- **Remote Administrator Host/Port:** This feature enables you to perform administration task from a certain remote host. If this feature is enabled, only the specified IP address can perform remote administration.

Quality of Service

QoS (Quality of Service) 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 WAN connection.

- **Bandwidth of Upstream:** Input the maximum bandwidth of uplink in Kbps.
- **Bandwidth of Downstream:** Input the maximum bandwidth of downlink in Kbps.
- **Flexible Bandwidth Management:** It is recommended you enable this option to exploit maximum bandwidth effectively.

Rule-based QoS

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

Create a QoS Rule

- **Rule:** Check this if you want to activate this rule after it's created.
- **Grouping:** There are two methods to define "who" will be managed, base on IP address or MAC address.

If creating a rule by IP address:

- **Grouping:** Choose IP from the list, and indicate single IP address or a segment IP range in following field.
- **Service:** Define the type of service that needs to be managed. There are four options for service recognition.
 - **DSCP:** DiffServ Code Point, as known as advanced TOS. You can choose this option if your local service gateway supports DSCP tags.
 - **Service Port:** Input a service port number or a segment of port range manually. You also need to indicate it's 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.
- **Control:** Set the corresponding control types for the selected service type.
 - **DSCP Marking:** This option is only available when DSCP is chosen in Service field. The purpose of this option is changing original DSCP tag to a new value. This option won't prioritize data packets.
 - **PRI:** Set priorities for data packets of selected hosts. The value is from 1 to 6. "1" is with highest priority, and "6" is with least 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.

- **SESSION:** This option is only available when Connection Sessions is chosen in Service field. The maximum number of session is 20000.
- **Direction:** Select the traffic direction to be applied for this rule.
- **Sharing Method:** This option is only available when MAXR, MINR, SESSION are chosen in Control field. If you want to apply the value of Control setting on each selected host, then you need select "Single".
- **Schedule:** The QoS rule can be turn off according to the schedule you specified. By default, it is always turned on when the rule is enabled.

If creating rule by MAC address:

- **Grouping:** Choose MAC from the list, and followed by a MAC address of selected host.
- **Control:** In this field, you will decide what action will be taken on those selected hosts. Set the corresponding control types for the selected service type.
 - **PRI:** Set priorities for data packets of selected hosts. The value is from 1 to 6. "1" is with highest priority, and "6" is with least 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.
 - **SESSION:** This option is only available when Connection Sessions is chosen in Service field. The maximum number of session is 20000.
- **Direction:** Select the traffic direction to be applied for this rule.
- **Sharing Method:** This option is only available when MAXR, MINR, SESSION are chosen in Control field. If you want to apply the value of Control setting on each selected host, then you need select "Single".
- **Schedule:** The QoS rule can be turn off according to the schedule you specified. By default, it is always turned on when the rule is enabled.

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-IPSec

- **VPN-IPSEC:** Check **Enable** to trigger the function of VPN-IPSEC.
- **Netbios over IPSEC:** Check to **Enable** to receive the Netbios from Network Neighborhood.
- **NAT Traversal:** Some NAT router will block IPSec packets if it doesn't support IPSec pass-through. If you connect to another NAT router which doesn't support IPSec pass-through at WAN side, you need to activate this option.
- **Max. number of tunnels:** The device supports up to 32 IPSec tunnels. You can define the required IPSec tunnel settings by clicking on the corresponding **Edit** button and then check the **Enable** box to enable it.
- **Dynamic IP VPN:** Enable it when you need remote mobile hosts build security tunnel with the Gateway. It is disabled by default. Click **Edit** to finish configuration.

Dynamic IP VPN

A VPN gateway can ignore IP information of client when using Dynamic VPN, so it is suitable for users to build VPN tunnel with VPN gateway from a remote mobile host.

- **Tunnel name:** Assign a name for this tunnel.
- **Local subnet:** This can be a host, a partial subnet, or the whole subnet of LAN site of local gateway.
- **Local Netmask:** The local netmask and associated local subnet can define a subnet domain for the devices connected via the VPN tunnel.
- **Phase 1 Key Life Time:** The value represents the life time of the key which is dedicated at Phase 1 between both end gateways.
- **Phase 2 Key Life Time:** The value represents the life time of the key which is dedicated at Phase 2 between both end gateways.
- **Encapsulation Protocol:** There are three protocols can be selected: ESP, AH, or ESP+AH.
- **PFS Group:** Configures Perfect Forward Secrecy for connections created with this IPSec transport profile by assigning a Diffie-Hellman prime modulus group. There are three groups can be selected: Group 1, Group 2, Group 5.
 - **Disable:** No PFS group.
 - **Group 1:** 768-bit Diffie-Hellman prime modulus group.
 - **Group 2:** 1024-bit Diffie-Hellman prime modulus group.
 - **Group 5:** 1536-bit Diffie-Hellman prime modulus group.
- **Preshare key:** The pre-shared key must be the same one for both VPN gateways and clients.
- **Remote ID:** The Type and Value of the local VPN gateway must be the same as the local ID of the remote VPN gateway.
- **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.

- **Dead Peer Detection:** This feature will detect if a remote VPN gateway still exists, indicate the interval between every detection, and assign value for timeout.
- **XAUTH:** 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. This function is suitable for remote mobile VPN clients. You can not only configure a VPN rule with a pre-shared key for all remote users, but you can also designate account / password for specific users that are permitted to establish VPN connection with VPN server.
 - **XAUTH - None:** Without Extended Authentication (xAuth).
 - **XAUTH - Server:** Check if the device behaves as a VPN server, and will validate the user information of VPN clients. You can click on "XAUTH Account" button at IPSec Setting main page to edit the permitted user account / password.
- **Set IKE Proposal:** Check to enable IKE proposals.
 - **Encryption:** There are five algorithms can be selected: DES, 3DES, AES-128, AES-192, and AES-256.
 - **Authentication:** There are two algorithms can be selected: SHA1 and MD5.
 - **DH Group:** There are three groups can be selected: Group 1 (MODP768), Group 2 (MODP1024), and Group 5 (MODP1536).
 - **Enable:** Check to enable the IKE Proposal with this rule.
- **Set IPSec Proposal:** Check to enable IPSec proposals.
 - **Encryption:** There are five algorithms can be selected: DES, 3DES, AES-128, AES-192, and AES-256. But when the encapsulation protocol is set to AH, you can choose Null without encryption.
 - **Authentication:** There are two algorithms can be selected: SHA1 and MD5. But none also can be selected here for IPSec proposal.
 - **Enable:** Check enable IPSec Proposal with this rule.

IPSec-IKE Setting

- **Tunnel name:** Assign a name for this tunnel.
- **Method:** There are IKE and Manual options. Choose IKE here.
- **Local subnet:** The subnet of LAN site of local VPN gateway. It can be a host, a partial subnet, or the whole subnet of LAN site of local gateway.
- **Local Netmask:** The local netmask and associated local subnet can define a subnet domain for the devices connected via the VPN tunnel.
- **Remote subnet:** The subnet of LAN site of remote VPN gateway. It can be a host, a partial subnet, or the whole subnet of LAN site of remote gateway.
- **Remote Netmask:** The remote netmask and associated remote subnet can define a subnet domain for the devices connected via the VPN tunnel.
- **Remote Gateway:** Enter the IP address of remote VPN gateway.
- **Phase 1 Key Life Time:** The value represents the life time of the key which is dedicated at Phase 1 between both end gateways.
- **Phase 2 Key Life Time:** The value represents the life time of the key which is dedicated at Phase 2 between both end gateways.
- **Encapsulation Protocol:** There are three protocols can be selected: ESP, AH, or ESP+AH.

- **PFS Group:** Configures Perfect Forward Secrecy for connections created with this IPSec transport profile by assigning a Diffie-Hellman prime modulus group. There are three groups can be selected: Group 1, Group 2, Group 5.
 - **Disable:** No PFS group.
 - **Group 1:** 768-bit Diffie-Hellman prime modulus group.
 - **Group 2:** 1024-bit Diffie-Hellman prime modulus group.
 - **Group 5:** 1536-bit Diffie-Hellman prime modulus group.
- **Aggressive Mode:** Enabling this mode will accelerate the establishing speed of VPN tunnel, but the device will suffer from less security. Hosts in both ends of the tunnel must support this mode so as to establish the tunnel properly.
- **Preshare key:** The first key that supports IKE mechanism of both VPN gateway and VPN client host for negotiating further security keys. The pre-shared key must be the same one for both VPN gateways and clients.
- **Connection Type:** There are three options for you to choose when the VPN tunnel will be established. You can choose “Connect-on-Demand”, “Auto Reconnect (always-on)”, or “Manually”.
- **Remote ID:** The Type and the Value of the local VPN gateway must be the same as the local ID of the remote VPN gateway.
- **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.
- **Dead Peer Detection:** This feature will detect if remote VPN gateway still exists. Indicate time of interval between every detection, and assigns value of timeout.
- **Dead Peer Detection:** This feature will detect if a remote VPN gateway still exists, indicate the interval between every detection, and assign value for timeout.
- **XAUTH:** 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. This function is suitable for remote mobile VPN clients. You can not only configure a VPN rule with a pre-shared key for all remote users, but you can also designate account / password for specific users that are permitted to establish VPN connection with VPN server.
 - **XAUTH - None:** Without Extended Authentication (xAuth).
 - **XAUTH - Server:** Check if the device behaves as a VPN server, and will validate the user information of VPN clients. You can click on "XAUTH Account" button at IPSec Setting main page to edit the permitted user account / password.
- **Set IKE Proposal:** Check to enable IKE proposals.
 - **Encryption:** There are five algorithms can be selected: DES, 3DES, AES-128, AES-192, and AES-256.
 - **Authentication:** There are two algorithms can be selected: SHA1 and MD5.
 - **DH Group:** There are three groups can be selected: Group 1 (MODP768), Group 2 (MODP1024), and Group 5 (MODP1536).
 - **Enable:** Check to enable the IKE Proposal with this rule.
- **Set IPSec Proposal:** Check to enable IPSec proposals.
 - **Encryption:** There are five algorithms can be selected: DES, 3DES, AES-128, AES-192, and AES-256. But when the encapsulation protocol is set to AH, you can choose Null without encryption.
 - **Authentication:** There are two algorithms can be selected: SHA1 and MD5. But none also can be selected here for IPSec proposal.

- **Enable:** Check enable IPsec Proposal with this rule.

IPSec-Manual Setting

- **Tunnel name:** Assign a name for this tunnel.
- **Method:** There are IKE and Manual options. Choose Manual here.
- **Local subnet:** The subnet of LAN site of local VPN gateway. It can be a host, a partial subnet, or the whole subnet of LAN site of local gateway.
- **Local Netmask:** The local netmask and associated local subnet can define a subnet domain for the devices connected via the VPN tunnel.
- **Remote subnet:** The subnet of LAN site of remote VPN gateway. It can be a host, a partial subnet, or the whole subnet of LAN site of remote gateway.
- **Remote Netmask:** The remote netmask and associated remote subnet can define a subnet domain for the devices connected via the VPN tunnel.
- **Remote Gateway:** Enter the IP address of remote VPN gateway.
- **Encapsulation Protocol:** There are two protocols can be selected: ESP or AH.
- **Outbound SPI:** SPI is an important parameter during hashing. Outbound SPI will be included in the outbound packet transmitted from local gateway. The value of outbound SPI should be set in hex formatted.
- **Inbound SPI:** Inbound SPI will be included in the inbound packet transmitted from WAN site of remote gateway. It will be used to de-hash the coming packet and check its integrity. The value of outbound SPI should be set in hex formatted.
- **Encryption Algorithm:** There are two algorithms can be selected: DES, or 3DES.
- **Encryption Key:** Encryption key is used by the encryption algorithm. Its length is 8 bytes if encryption algorithm is DES or 24 bytes if 3DES. The key value should be set in hex formatted.
- **Authentication Algorithm:** There are two algorithms can be selected: SHA1 or MD5.
- **Authentication Key:** Authentication key is used by the authentication algorithm. Its length is 16 bytes if authentication algorithm is MD5 or 20 bytes if SHA1. Certainly, its length will be 0 if no authentication algorithm is chosen. The key value should be set in hex formatted.

VPN-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.

- **VPN-PPTP Server:** Enable or Disable PPTP server function.
- **Server Virtual IP:** The IP address of PPTP server. This IP address should be different from IP address of L2TP server and LAN subnet of VPN gateway.
- **IP Pool Start Address:** This device will assign an IP address to remote PPTP client. This value indicates the beginning of IP pool.
- **IP Pool End Address:** This device will assign an IP address to remote PPTP client. This value indicates the end of IP pool.
- **Authentication Protocol:** Choose authentication protocol as PAP, CHAP, or MSCHAP(v1 or v2).

- **MPPE Encryption Mode:** Check to enable MPPE encryption. The MPPE needs to work with MSCHAP(v1 or v2) authentication.
- **Encryption Length:** Choose encryption length of MPPE encryption.
- **User Account:** Input up to 10 different user accounts for PPTP server.
- **Connection Status:** The connected PPTP user & connection information will be shown in this table.

VPN-PPTP Client

- **VPN-PPTP Client:** Enable or Disable PPTP client function.
- **User Account:** Input up to 10 different user accounts for PPTP client, define each user account settings by clicking on the corresponding **Edit** button, and check **Enable**.
- **Name:** The name of this rule.
- **Peer IP/Domain:** The IP address or Domain name of remote PPTP server.
- **User Name:** The user name which is provided by remote PPTP server.
- **Password:** The password which is provided by remote PPTP server.
- **Default Gateway:** You can check **Enable** to set this tunnel as the default gateway for WAN connection.
- **Peer Subnet:** The LAN subnet of remote PPTP server.
- **Connection Control:** There are three options for users to choose when the PPTP tunnel is established. Options are: **Connect-on-Demand**, **Auto Reconnect (always-on)**, or **Manual**.
- **Option:** Enable or disable MPPE and NAT function. If you enable MPPE, then this PPTP tunnel will be encrypted.
- **Authentication:** Enable if remote PPTP server requests it.
- **Authentication Protocol:** Choose authentication protocol as PAP, CHAP, or MSCHAP(v1 or v2). The protocol you choose must be supported by remote PPTP server.
- **LCP Echo Type:** Choose the appropriate connection keep alive.

VPN-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, MSCHAP(v1 and v2). Users can also enable MPPE encryption when using MSCHAP.

- **VPN-L2TP Server:** Enable or Disable L2TP server function.
- **L2TP Over IPsec:** L2TP over IPsec VPNs allow you to transport data over the Internet, while still maintaining a high level of security to protect data. Enter a Pre-sharekey when you use some devices to establish L2TP tunnels.
- **Server Virtual IP:** The IP address of L2TP server. This IP address should be different from IP address of PPTP server and LAN subnet of VPN gateway.
- **IP Pool Starting Address:** Device will assign an IP address to remote L2TP client. This value indicates the beginning of IP pool.
- **IP Pool Ending Address:** Device will assign an IP address to remote L2TP client. This value indicates the end of IP pool.
- **Authentication Protocol:** Choose authentication protocol as PAP, CHAP, or MSCHAP(v1 or v2).

- **MPPE Encryption Mode:** Check to enable MPPE encryption. The MPPE needs to work with MSCHAP(v1 or v2) authentication.
- **Encryption Length:** Choose encryption length of MPPE encryption.
- **User Account:** Input up to 10 different user accounts for L2TP server.
- **Connection Status:** The connected L2TP user & connection information will be shown in this table.

VPN-L2TP Client

- **VPN-L2TP Client:** Enable or Disable L2TP client function.
- **User Account:** You can input up to 10 different user accounts for L2TP client, define each user account settings by clicking on the corresponding **Edit** button and then check **Enable** to enable it.
- **Name:** The name of this rule.
- **Peer IP/Domain:** The IP address or Domain name of remote L2TP server.
- **User Name:** The user name which is provided by remote L2TP server.
- **Password:** The password which is provided by remote L2TP server.
- **Default Gateway:** You can check **Enable** to set this tunnel as the default gateway for WAN connection.
- **Peer Subnet:** The LAN subnet of remote L2TP server.
- **Connection Control:** There are three options for users to choose when the PPTP tunnel is established. Options are: **Connect-on-Demand, Auto Reconnect (always-on), or Manual.**
- **Option:** Enable or disable MPPE, NAT, and CCP function. If you enable MPPE, then this L2TP tunnel will be encrypted.
- **Authentication:** You need to enable this option if remote PPTP server requests it.
- **Authentication Protocol:** You can choose authentication protocol as PAP, CHAP, MSCHAP(v1), or MSCHAP(v2). The protocol you choose must be supported by remote L2TP server.
- **LCP Echo Type:** Choose the way to do connection keep alive.

GRE Tunnel

- **Default Gateway:** You can choose a tunnel as the default gateway for WAN connection.
- **Names:** The name of this GRE tunnel.
- **Tunnel IP:** Assign a virtual IP address of this tunnel.
- **Peer IP:** Enter the IP address of remote host that you want to connect.
- **Key:** Enter the password to establish GRE tunnel with remote host.
- **TTL:** Time-To-Live for packets. The value is within 1 to 255. If a packet passes number of TTL routers and still can't reach the destination, then this packet will be dropped.
- **Subnet:** Enter the local subnet of remote host. If a packet wants to go to this subnet, the GRE tunnel will be established automatically.
- **Enable:** Enable or Disable this GRE tunnel.

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.

- **Enable:** Enable or Disable the VRRP function.
- **Virtual Server ID:** Means Group ID. Specify the ID number of the virtual server.
- **Priority of Virtual Server:** Specify the priority to use in VRRP negotiations. Valid values are 1-254, and a larger value has higher priority.
- **Virtual Server IP Address:** Specify the IP address of the virtual server.

System Management

TR-069

- **TR-069:** Check to enable.

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.

- **Enable SNMP:** You can check “Local”, “Remote” or both to enable SNMP function. If “Local” is checked, this device will respond to the request from LAN. If “Remote” is checked, this device will respond to be request from WAN.
- **WAN Access IP Address:** If you want to limit the remote SNMP access to specific computer, please enter the PC’s IP address. The default value is 0.0.0.0, and it means that any internet connected computer can get some information of the device with SNMP protocol.
- **SNMP Version:** Supports SNMP V1, V2c, and V3.
- **Get Community:** The community of GetRequest that this device will respond. This is a text password mechanism that is used to weakly authenticate queries to agents of managed network devices.
- **Set Community:** The community of SetRequest that this device will accept.
- **SNMPv3 Settings: User 1/2:** This device supports up to two SNMP management accounts. You can specify the account permission as Read or Read/Write.
- **User 1/2 AUTH Mode:** Select MD5 or SHA as the method of password encryption for the specified level of access, or to disable authentication.
- **User 1/2 Privacy Mode:** You can configure the SNMP privacy mode. There are three modes for you to choose: “noAuthNoPriv” for both authentication and private key are not required, “authNoPriv” for no private key required, and “authPriv” for both authentication and private key required.
- **Username 1/2:** Use this field to identify the user name for the specified level of access.
- **Password 1/2:** Use this field to set the password for the specified level of access.
- **User 1/2 Priv Key:** Use this field to define the encryption key for the specified level of access.
- **Trap Event Receiver 1 ~ 4:** Enter the IP addresses or Domain Name of your SNMP Management PCs. You have to specify the IP address, so that the device can send SNMP Trap message to the management PCs consequently.

Applications

This device is equipped with a 3G/4G module as WAN interface, and it also provide the SMS feature for you to use.

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 to users to alert some events automatically.

Management Settings:

- **Remote Management via SMS:** Check this to enable this function.
- **Delete SMS for Remote Management:** This device will delete received SMS message that is for remote management purpose if enabling this option. This option can prevent storage space of SIM card from being occupied continuously. If SIM storage is full, this gateway can't receive any new SMS.
- **Security Key:** This security key will be used for authentication when this gateway receives SMS command. Users need to type this key first and then followed by a command. There should be a "blank" between key and command (e.g. 1234 reboot). If this field is empty, users just need to type command without adding any key information.

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

Command Settings:

- **Status:** When enabled you can send command "status" to query WAN connection status. For 3G/LTE WAN, router will send back WAN IP address, network name, network type, and connection time via SMS. For Ethernet WAN, router will send back WAN IP address and connection time via SMS.
- **Connect:** When enabled you can send command "connect" to start WAN connection. **Disconnect:** When enabled you can send command "disconnect" to disconnect WAN connection.

Note: If this gateway receives "disconnect" command from SMS, it won't try to connect again no matter WAN connection mode is set to auto-reconnect.

- **Reconnect:** When enabled you can send command "reconnect" to disconnect WAN connection, and start WAN connection again immediately.
- **Reboot:** When enabled you can send command "reboot" to restart router.

Notification Settings:

- **WAN Link Down:** When enabled this gateway will send a message to users if primary WAN connection is dropped.
- **WAN Link Up:** When enabled this gateway will send a message to users if WAN connection is established. This message will also include WAN IP address.
- **Secondary WAN is Up:** When enabled this gateway will send a message to users if secondary WAN is connected. This message will also include WAN IP address.
- **Secondary WAN is Down:** When enabled this gateway will send a message to users if secondary WAN is disconnected.

Access Control List Settings:

- **Access Control:** Users can decide which phone number can send commands to this gateway or receive notifications when enable this option.

- **Phone 1~5:** For security concern, this gateway won't deal with the command if that phone number is not in the list even the security key is correct. The phone number must be with the international prefix (i.e. +886939123456). You can also assign specific phone number can send command and/or also can receive notifications.

Create Message

Create a new SMS message. After finishing the content of message, and filling with phone number of receiver(s), you can press the "Send" button to send this message out. You can see "Send OK" if the new message has been sent successfully.

Inbox

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

- **Refresh:** You can press "Refresh" button to renew SMS lists.
- **Delete, Reply, Forward Messages:** After reading message, you can check the checkbox on the left of each message to delete, reply, or forward the message.

System

System information, system logs, use system tools for system update and do service scheduling and system administration setting are displayed.

System Information

System Information is displayed on this page.

System Status

Web Log

- **Log Types:** You can select the log types to be collected in the web log area. There are “System”, “Attacks”, “Drop”, and “Debug” types for you to select.
- **Web Log:** You can browse, refresh, download, and clear the log messages.

Syslog

This device can also export system logs to specific destination by means of syslog (UDP) and SMTP(TCP). With enabled Syslog function, this device will send log to a certain host periodically. You need to install a syslog utility on a host to receive syslog. The items you have to setup include:

- **IP Address for syslogd:** Host IP of destination where syslog will be sent to. Check Enable to enable this function.

Email Alert

This device can also export system logs via sending emails to specific recipients. The items you have to setup include:

- **Setting of Email alert:** Check if you want to enable Email alert (send syslog via email).
- **SMTP Server:** Port: Input the SMTP server IP and port, which are connected with ':'. If you do not specify port number, the default value is 25.
- **SMTP Username:** Enter the Username offered by your ISP.
- **SMTP Password:** Enter the password offered by your ISP.
- **E-mail Addresses:** The recipients are the ones who will receive these logs. You can assign more than 1 recipient, using ';' or ',' to separate these email addresses.
- **E-mail Subject:** The subject of email alert is optional.

System Tools

Change Password

You can change the System Password here. Click **Save** to store your settings or click **Undo** to give up the changes.

FW Upgrade

If new firmware is available, you can upgrade router firmware through the WEB GUI here. Press **Browse** to indicate the file name of new firmware, and then press **Upgrade** to start to upgrade new firmware on this device. If you want to upgrade a firmware which is from GPL policy, please check **Accept unofficial firmware**

Note: Do not turn off device until upgrade is complete.

System Time

- **Time Zone:** Select a time zone where this device located.
- **Auto-Synchronization:** Check **Enable** to enable this function.
- **Sync with Time Server:** Click on the button if you want to set Date and Time by NTP Protocol.
- **Sync with my PC:** Click on the button if you want to set Date and Time using the PC's Date and Time.

Others

In this section you can do system backup, reset to default, system reboot settings and Ping test.

- **Backup Setting:** You can backup your settings by clicking **Backup** and save it as a bin file. Once you want to restore these settings, click **Firmware Upgrade** and use the bin file you saved.
- **Reset to Default:** You can also reset this device to factory default settings by clicking **Reset**.
- **Reboot:** You can also reboot this device by clicking **Reboot**.
- **MAC Address for Wake-on-LAN:** Wake-on-LAN (WOL) is an Ethernet networking standard that allows a computer to be turned on or awakened by a network message.
- **Domain Name or IP address for Ping Test:** This allows you to configure an IP, and ping the device.
- **Domain Name or IP address for Traceroute:** Traceroute is a network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an IP network.

MMI

Web UI

You can enable and disable the HTTPS option for web administrator access in this section. Set UI administration time-out duration give remote administration host port in this page. When the host port is given please remember to check the enable box and save your settings.

Safety Warnings

Lithium Battery

- A lithium battery located within the product provides backup power for the timekeeping. This battery has an estimated life expectancy of ten years.
- When this battery starts to weaken, the date and time may be incorrect. If the battery fails, the board must be sent back to Multi-Tech Systems for battery replacement.
- Lithium cells and batteries are subject to the Provisions for International Transportation. Multi-Tech Systems, Inc. confirms that the Lithium batteries used in the Multi-Tech product(s) referenced in this manual comply with Special Provision 188 of the UN Model Regulations, Special Provision A45 of the ICAO-TI/IATA-DGR (Air), Special Provision 310 of the IMDG Code, and Special Provision 188 of the ADR and RID (Road and Rail Europe).

CAUTION: Risk of explosion if this battery is replaced by an incorrect type. Dispose of batteries according to instructions.

Attention: Pour réduire les risques d'incendie, utiliser uniquement des conducteurs de télécommunications 26 AWG au de section supérieure.

Ethernet Ports

CAUTION: Ethernet ports and command ports are not designed to be connected to a public telecommunication network. Ethernet is only designed to be connected within side plant. Routing to outside plant and or campus environments is prohibited.

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.
- Switch OFF your wireless device when in an aircraft. Using portable electronic devices in an aircraft may endanger aircraft operation, disrupt the cellular network, and is illegal. Failing to observe this restriction may lead to suspension or denial of cellular services to the offender, legal action, or both.
- Switch OFF your wireless device when around gasoline or diesel-fuel pumps and before filling your vehicle with fuel.
- Switch OFF your wireless device in hospitals and any other place where medical equipment may be in use.

Interference with Pacemakers and Other Medical Devices

Potential interference

Radiofrequency 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 the 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 the 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).

Regulatory Information

EMC, Safety, and R&TTE Directive Compliance



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

Council Directive 2004/108/EC of 15 December 2004 on the approximation of the laws of Member States relating to electromagnetic compatibility;

and

Council Directive 2006/95/EC of 12 December 2006 on the harmonization of the laws of Member States relating to electrical equipment designed for use within certain voltage limits;

and

Council Directive 1999/5/EC of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity.

Restriction of the Use of Hazardous Substances (RoHS)



Multi-Tech Systems, Inc

Certificate of Compliance

2011/65/EU

Multi-Tech Systems confirms that its embedded products comply with the chemical concentration limitations set forth in the directive 2011/65/EU of the European Parliament (Restriction of the use of certain Hazardous Substances in electrical and electronic equipment - RoHS).

These Multi-Tech products do not contain the following banned chemicals¹:

- Lead, [Pb] < 1000 PPM
- Mercury, [Hg] < 1000 PPM
- Hexavalent Chromium, [Cr+6] < 1000 PPM
- Cadmium, [Cd] < 100 PPM
- Polybrominated Biphenyl, [PBB] < 1000 PPM
- Polybrominated Diphenyl Ether, [PBDE] < 1000 PPM

Environmental considerations:

- Moisture Sensitivity Level (MSL) =1
- Maximum Soldering temperature = 260C (in SMT reflow oven)

¹Lead usage in some components is exempted by the following RoHS annex, therefore higher lead concentration would be found in some modules (>1000 PPM);

- Resistors containing lead in a glass or ceramic matrix compound.

Waste Electrical and Electronic Equipment Statement

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

WEEE Directive

The 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 Multi-Tech 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.

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, please contact your local city office, your household waste disposal service or where you purchased the product.

July, 2005



Information on HS/TS Substances According to Chinese Standards

In accordance with China's Administrative Measures on the Control of Pollution Caused by Electronic Information Products (EIP) # 39, also known as China RoHS, the following information is provided regarding the names and concentration levels of Toxic Substances (TS) or Hazardous Substances (HS) which may be contained in Multi-Tech Systems Inc. products relative to the EIP standards set by China's Ministry of Information Industry (MII).

Hazardous/Toxic Substance/Elements

Name of the Component	Lead (PB)	Mercury (Hg)	Cadmium (CD)	Hexavalent Chromium (CR6+)	Polybrominated Biphenyl (PBB)	Polybrominated Diphenyl Ether (PBDE)
Printed Circuit Boards	O	O	O	O	O	O
Resistors	X	O	O	O	O	O
Capacitors	X	O	O	O	O	O
Ferrite Beads	O	O	O	O	O	O
Relays/Opticals	O	O	O	O	O	O
ICs	O	O	O	O	O	O
Diodes/ Transistors	O	O	O	O	O	O
Oscillators and Crystals	X	O	O	O	O	O
Regulator	O	O	O	O	O	O
Voltage Sensor	O	O	O	O	O	O
Transformer	O	O	O	O	O	O
Speaker	O	O	O	O	O	O
Connectors	O	O	O	O	O	O
LEDs	O	O	O	O	O	O
Screws, Nuts, and other Hardware	X	O	O	O	O	O
AC-DC Power Supplies	O	O	O	O	O	O
Software /Documentation CDs	O	O	O	O	O	O
Booklets and Paperwork	O	O	O	O	O	O
Chassis	O	O	O	O	O	O

X Represents that the concentration of such hazardous/toxic substance in all the units of homogeneous material of such component is higher than the SJ/Txxx-2006 Requirements for Concentration Limits.

O Represents that no such substances are used or that the concentration is within the aforementioned limits.

Information on HS/TS Substances According to Chinese Standards (in Chinese)

依照中国标准的有毒有害物质信息

根据中华人民共和国信息产业部 (MII) 制定的电子信息产品 (EIP) 标准—中华人民共和国《电子信息产品污染控制管理办法》(第 39 号), 也称作中国 RoHS, 下表列出了 Multi-Tech Systems, Inc. 产品中可能含有的有毒物质 (TS) 或有害物质 (HS) 的名称及含量水平方面的信息。

有害/有毒物质/元素

成分名称	铅 (PB)	汞 (Hg)	镉 (CD)	六价铬 (CR6+)	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
印刷电路板	O	O	O	O	O	O
电阻器	X	O	O	O	O	O
电容器	X	O	O	O	O	O
铁氧体磁环	O	O	O	O	O	O
继电器/光学部件	O	O	O	O	O	O
ICs	O	O	O	O	O	O
二极管/晶体管	O	O	O	O	O	O
振荡器和晶振	X	O	O	O	O	O
调节器	O	O	O	O	O	O
电压传感器	O	O	O	O	O	O
变压器	O	O	O	O	O	O
扬声器	O	O	O	O	O	O
连接器	O	O	O	O	O	O
LEDs	O	O	O	O	O	O
螺丝、螺母以及其它五金件	X	O	O	O	O	O
交流-直流电源	O	O	O	O	O	O
软件/文档 CD	O	O	O	O	O	O
手册和纸页	O	O	O	O	O	O
底盘	O	O	O	O	O	O

X 表示所有使用类似材料的设备中有害/有毒物质的含量水平高于 SJ/Txxx-2006 限量要求。

O 表示不含该物质或者该物质的含量水平在上述限量要求之内。