User Manual

BEC MX-200(A)

Advanced Industrial
4G/LTE Router

TABLE OF CONTENTS

CHAPTER 5: TROUBLESHOOTING 146

APPENDIX: PRODUCT SUPPORT & CONTACT 148

CHAPTER 1: INTRODUCTION

Introduction to your Router

The BEC MX-200(A) Advanced Industrial 4G/LTE Router is a high performance fixed wireless platform enabling real-time 4G Cellular data connectivity for your existing serial devices and Ethernet network. The MX-200(A) provides a reliable and cost-effective alternative solution for business continuity. The platform can serve as the primary connection or backup connection when wired connections fail are unavailable or non-existent.

The MX-200(A) features two Gigabit Ethernet interfaces and a RS-232 Serial interface enabling wireless data connectivity for a broad range of applications and vertical machine-to-machine (M2M) market segments. Intelligent software supports configurable LAN/WAN options, embedded LTE module and enterprise level functionality such as: advanced security mechanisms, Quality of Service (QoS), SPI firewall, integrated VPN, auto failover for unparalleled uptime and network redundancy, and cloud-based management to extend visibility and control of devices remotely.

4G/LTE Mobility

To offer an advanced network solution that meets the growing demands of M2M services, MX-200(A) exclusively features dual WAN - load balance or auto-failover/failback to provide extraordinary, always-on internet connectivity.

Ultra-Compact and Lightweight Design

Designed for continuous operation in harsh environments, the MX-200(A) supports an extended operating temperature range from -4 to 140⁰ F (–20 to 60⁰ C) and a flexible input voltage range of 9-56V DC making it suitable for diverse environments and applications. To enable simple, reliable and efficient integration the ultra-compact, lightweight and low profile design incorporates highly flexible mounting options to ensure that the device and can be easily mounted discretely anywhere.

Secure VPN Connections

The MX-200(A) supports comprehensive and robust IPSec VPN (Virtual Private Network) protocols for business users to establish private encrypted tunnels over the public Internet to secure data transmission between headquarters and branch offices. It also supports VPN dial in from smart phones for secure remote Internet connection via your home broadband. With a built-in DES/3DES VPN accelerator, the router enhances IPSec VPN performance significantly.

IPv6 Supported

Internet Protocol version 6 (IPv6) is a version of the Internet Protocol that is designed to succeed IPv4. IPv6 has a vastly larger address space than IPv4. The router is already supporting IPv6, you can use it in IPv6 environment no need to change device. The dual-stack protocol implementation in an operating system is a fundamental IPv4-to-IPv6 transition technology. It implements IPv4 and IPv6

protocol stacks either independently or in a hybrid form. The hybrid form is commonly implemented in modern operating systems supporting IPv6.

Quick Start Wizard

Support a WEB GUI page to install this device quickly. With this wizard, simple steps will get you connected to the Internet immediately.

Firmware Upgradeable

Device can be upgraded to the latest firmware through the WEB based GUI.

Features & Specifications

- 4G/LTE and/or Ethernet IP broadband connectivity (3G Fallback optional)
- High performance SX antenna for increased coverage, signal reception and efficiency
- Gigabit Ethernet WAN (GbE WAN) for Cable/Fiber/xDSL high WAN throughput
- Gigabit Ethernet LAN
- IPv6 ready (IPv4/IPv6 dual stack)
- Secured IPSec VPN with powerful DES/ 3DES/ AES
- Secured PPTP VPN with Pap/ Chap/ MPPE authentication
- Secured L2TP VPN with Pap/Chap authentication
- Secured GRE VPN tunnel
- Firewall Security with DoS Preventing and Packet Filtering
- Quality of Service Control for traffic prioritization management
- Universal Plug and Play (UPnP) Compliance
- Ease of Use with Quick Installation Wizard
- Small form factor with multiple mounting options, easily installed by a single person
- Hardened enclosure with Industrial-graded components
- Designed to withstand hypothermia, heat and protect from shock, vibration, etc.

Availability and Resilience

- Dual-WAN Interfaces
- Auto fail-over and failback
- High performance external antennas

Network Protocols and Features

- IPv4, IPv6, IPv4 / IPv6 dual stack
- IP Tunnel IPv6 in IPv4 (6RD)
- IP Tunnel IPv4 in IPv6 (DS-Lite)
- NAT, static routing and RIP-1/2
- Universal Plug and Play (UPnP) compliant
- Dynamic Domain Name System (DDNS)
- Virtual server and DMZ
- SNTP, DNS relay
- IGMP proxy and IGMP snooping

- MLD proxy and MLD snooping
- Supports port-based Virtual LAN (VLAN)

Firewall

- Built-in NAT Firewall
- Stateful Packet Inspection (SPI)
- DoS attack prevention including Land Attack, Ping of Death, etc.
- Access control
- IP&MAC filter, URL Content Filter
- Password protection for system management
- VPN pass-through

Quality of Service Control

- Traffic prioritization management based-on Protocol, Port Number and IP Address (IPv4/ IPv6)

Virtual Private Network (VPN) (Optional)

- 8 IPSec VPN Tunnels
- 8 PPTP VPN Tunnels (Dial-in:4, Dial-out:4)
- 8 L2TP VPN Tunnels (Dial-in:4, Dial-out:4)
- GRE (up to 8 tunnels)
- OpenVPN (Server: 1 rule, Clients: 4)
- Embedded PPTP / L2TP / IPSec Client and Server
- IKE Key Management
- MPPE Encryption for PPTP
- IPSec DES, 3DES and AES encryption

Management

- Quick Installation wizard
- Web-based GUI for remote and local management (IPv4/IPv6)
- Firmware upgrades and configuration data upload and download via web-based GUI
- Supports DHCP server / client / relay
- Supports SNMP
- TR-069 supports remote management
- BECentral Cloud Management

Hardware Specifications

Physical interface

- 4G/LTE: Two(2) detachable antennas
- GPS: 1 detachable GPS antenna (optional)
- WAN: Cellular 4G/LTE (and/or ETH WAN Optional)
- RS-232 (DCE, DB-9): one (1) port
- Ethernet LAN: 2-port 10/100/1000Mbps, auto-crossover (MDI/ MDI-X) switch
- SIM Card: One (1) slot
- Reset Button
- Power Connector: 4-pin connectors
- LED Indicators: Power / Internet / LTE / Ethernet

Physical Specifications

- Dimensions (W*H*D): 4.29" x 1.17" x 3.43" (109mm x 29.7mm x 87mm)

Approves (MX-200)

PTCRB, CE, FCC

UL Safety

- Class I Division 2 (C1D2) Groups ABCD T4
- Power Rating: 9-56V DC, 1.34-0.22A
- Operating Temperature Range: -20° to +60° C (-4° to +140° F)

Attention	✓ BEC MX-200, THE EQUIPMENT, IS AN OPEN-TYPE DEVICE AND IS MEANT TO BE INSTALLED IN AN ENCLOSURE SUITABLE FOR THE ENVIRONMENT SUCH THAT THE EQUIPMENT IS ONLY ACCESSIBLE WITH THE USE OF A TOOL. ✓ BEC MX-200 IS SUITABLE FOR USE IN CLASS I, DIVISION 2, GROUPS A, B, C AND D HAZARDOUS LOCATIONS, OR NONHAZARDOUS LOCATIONS ONLY.
Warning	**EXPLOSION HAZARD** – DO NOT CONNECT OR DISCONNECT WHEN ENERGIZED. **AVERTISSEMENT** – RISQUE D'EXPLOSION. NE PAS BRANCHER NI DÉBRANCHER SOUS TENSION.

Application Diagrams

The MX-200(A) Advanced Industrial 4G/LTE VPN Router is ideal the ideal solution for Digital signage, Remote surveillance, Vending Machines, Retail Point-of-Sales (PoS), Remote patient care/maintenance services, SCADA, Metering applications and much more.

Industrial Industry:
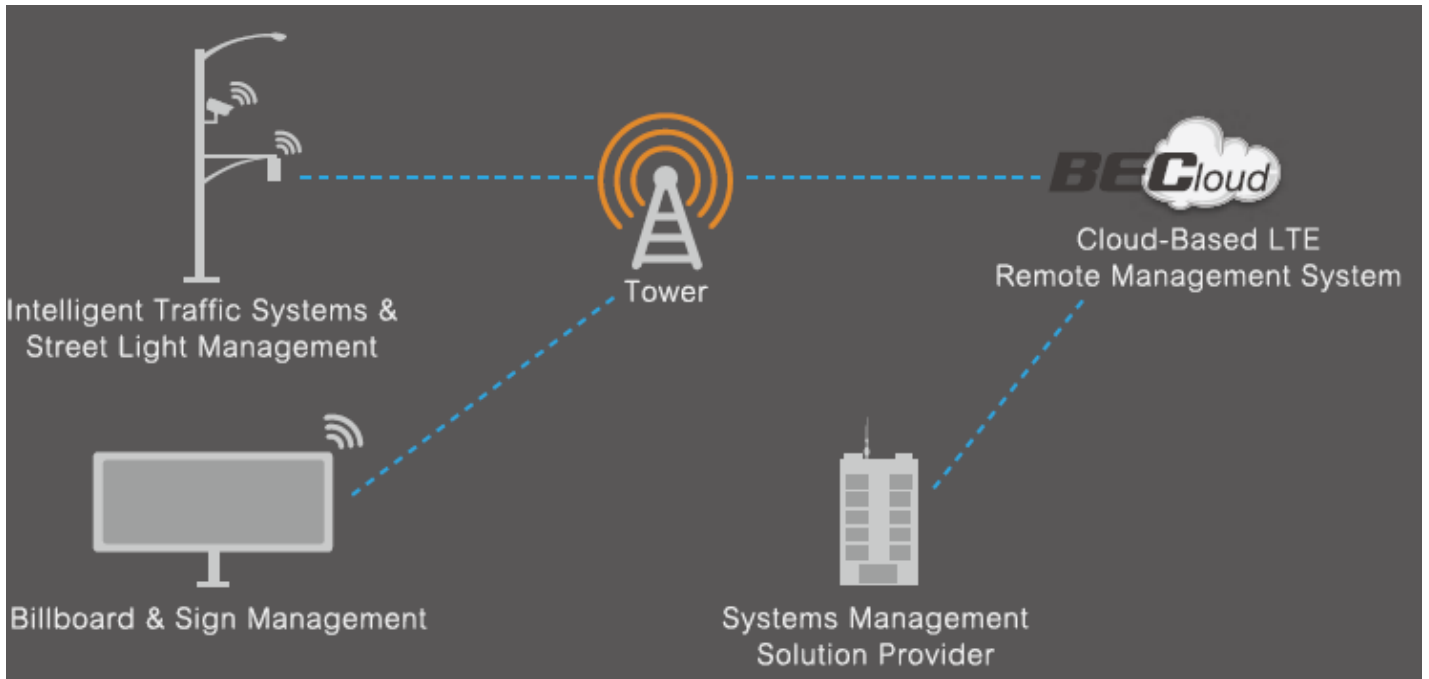
Power / Energy Industry:

CHAPTER 2: PRODUCT OVERVIEW

Important Note for Using This Router

✓ Do not use the router in high humidity or high temperature.

✓ Do not use the same power source for the MX-200(A) on other equipment.

Warning

✓ Do not open or repair the case yourself. If the device becomes too hot, turn off the power immediately and have it repaired at a qualified service center.

✓ Avoid using this product and all accessories outdoors.

✓ Place the router on a stable surface.

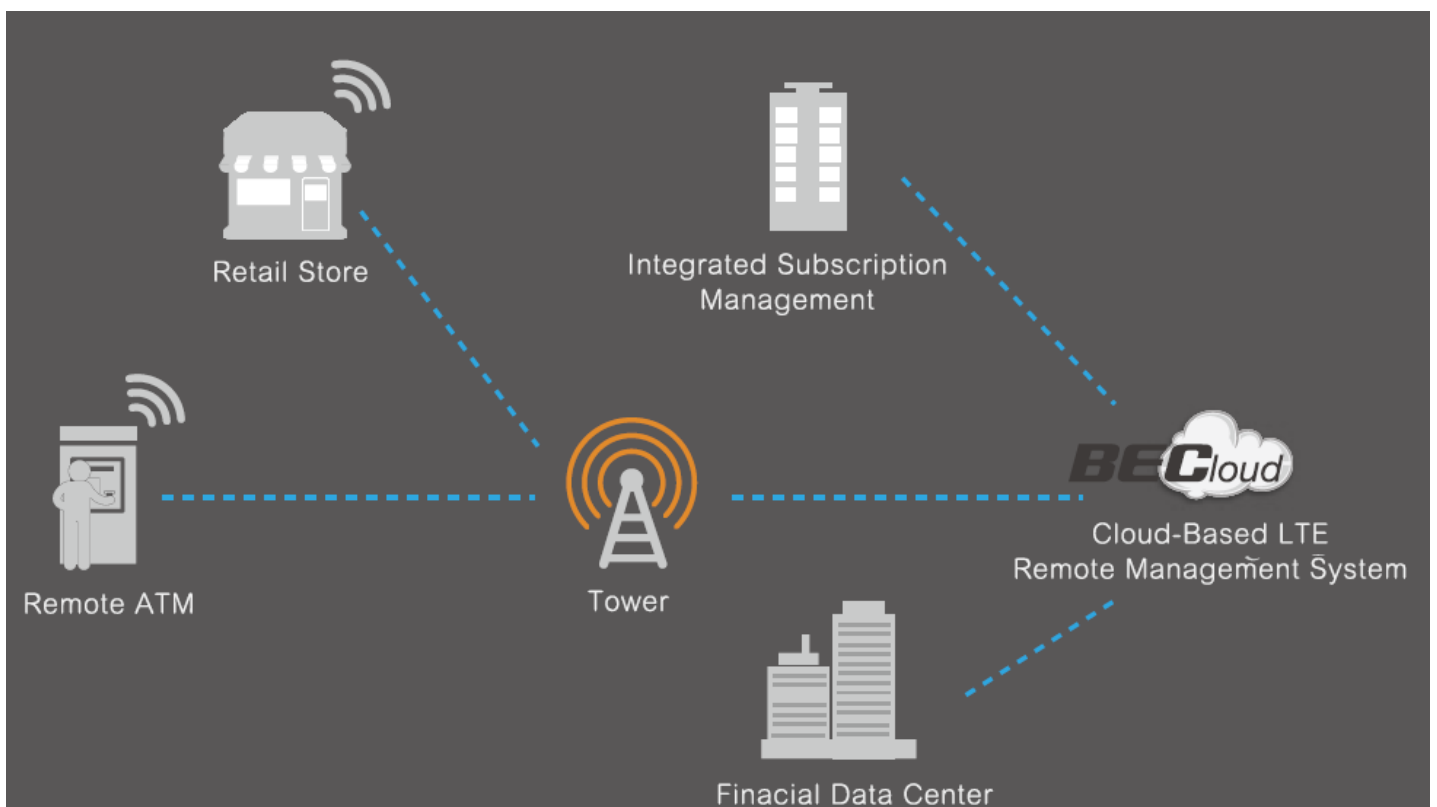✓ Only use the power adapter that comes with the package. Using a different voltage rating power adaptor may damage the router.

Attention

Package Contents

✓ BEC MX-200(A) M2M Router * 1

✓ CD containing the User Manual * 1

✓ Quick Installation Guide * 1

✓ DIN Rail Mounting Kit * 1

✓ Power Terminal Block 2-pin 3.5mm * 1

✓ Power Converter with 2-pin Terminal Block * 1

✓ DC Power Adapter, 12V 1.2A* 1

(Optional Accessories)

✓ 3G/4G Antennas

✓ Active GPS Antenna

✓ Ethernet (RJ-45) Cable

Device Description
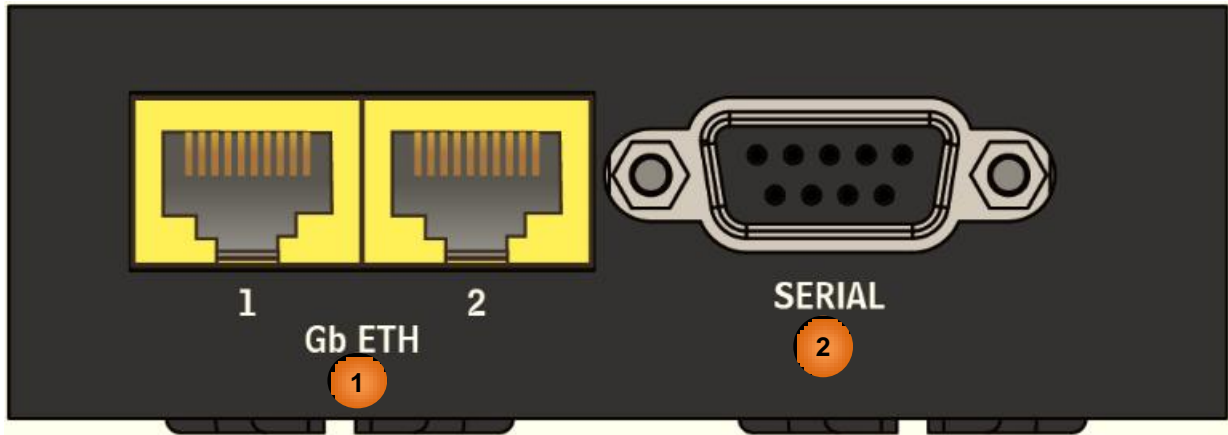
	INTERFACE	MEANING
1	**Gigabit Ethernet (LAN 1 ~ 2)**	**ETH1 is a LAN / WAN configurable port for broadband connectivity**
		Connect PCs, Laptops or any other office/home LAN devices with the supplied RJ-45 Ethernet cable (Cat-5 or Cat-5e) to any of those two LAN ports.
2	**SERIAL**	RS-232 serial port for machine connection and data collection
		Connect the male end of RS-232 serial data cable to the MX-200(A) and the other end to a machine or PC.

INTERFACE		MEANING
1	**WAN (MAIN/AUX)** **4G/LTE Antenna Connectors**	SMA female connectors. Manually screw the 3G/4G antennas tight to the female connectors for the Cellular Module
2	**GPS Antenna Connector**	SMA female connectors. Manually screw the GPS antenna tight to the connector
3	**RESET**	After the device is powered on, press it **6 seconds or above**: to restore to factory default settings (this is used when you cannot login to the router, e.g. forgot your password)
4	**POWER**	Attach the power terminal block, 2-pin 3.5mm, or the power converter with 2-pin terminal block here. **VCC** (Left Connector): Power - Red Wire to connect to the Positive (+) terminal of the power supply. **GND** (Right Connector): Ground – Black Wire to connect to the ground of the power supply

LEDS / INTERFACE			MEANING
1	**Gb ETH (1 & 2)** **(Gigabit Ethernet)**		**ETH #1 Can be configured to be WAN port for broadband connectivity**
		Green	**Ethernet LAN**: Connected to an Gigabit (1000Mbps) Ethernet device
			Ethernet WAN (ETH1 Only): Successfully connected with a broadband connection device
		Red	Transmission speed is at 10/100Mbps
		Blinking	Data being transmitted/received
		Off	No device is connected to the Ethernet port
2	**LTE** **(Received Signal** **Strength Indicator)**	Green	RSSI greater than -69 dBm. Excellent signal condition
		Green / Fast Flashing	RSSI from -81 to -69 dBm. Good signal condition
		Red / Fast Flashing	RSSI from -99 to -81 dBm. Fair signal condition
		Red / Slow Flashing	RSSI less than -99 dBm. Poor signal condition
		Red	No signal and the 4G LTE module is in service
		Off	No LTE module or LTE module fails
3	**Internet**	Green	IP connected and traffic is passing through the device
		Red	IP request failed
		Off	Either in bridged mode or WAN connection is not present
4	**Power**	Green	System ready
		Red	Boot failure
5	**SIM Card Slot**	N/A	Insert mini SIM card (2FF) with the gold contact facing down.
			Push mini SIM card (2FF) inwards to eject it
			* Power off the MX-200(A) before inserting or removing the SIM card

System Recovery Procedures

The purpose is to allow users to restore the MX-200(A) to its initial stage when the device is outage, upgraded to a wrong / broken firmware, cannot access to the GUI with wrong username and/or password, etc.

Step 1 – Configure your PC Network IP Address

Before performing the system recovery, assign this IP address and Netmask to your PC, **192.168.1.100** and **255.255.255.0** respectively.

Step 2 – Reset your MX-200(A) Device

2.1   Power off your MX-200(A)

2.2   Power on the MX-200(A) while pushing the RESET button with a small pointed object (such as paper clip, needle, toothpick, and etc.).

2.3   When the POWER LED turns RED, keep holding and pushing the RESET button until the INTERNET LED flashes in GREEN

Step 3 – Restore your MX-200(A) Device

With INTERNET light flashes green, MX-200(A) is in recovery mode and ready for a new Firmware.

3.1   Open a web browser and type the IP address, **192.168.1.1**, to access to the recovery page.

   NOTE: In the recovery mode, MX-200(A) will not respond to any PING or other requests.

3.2   Browse to the new Firmware image file then click Upload to start the upgrade process.

3.3   INTERNET LED turns red means the Firmware upgrade is in process.

   DO NOT power off or reboot the device, it would permanently damage your MX-200(A).

3.4   INTERNET LED turns green after the Firmware upgrade completed

3.5   Power cycle on & off to regain access to the MX-200(A).

Cabling

One of the most common causes of problems is bad cabling. Make sure that all connected devices are turned on. On the front panel of the product is a bank of LEDs. Verify that the LAN Link and LEDs are lit. If they are not, verify that you are using the proper cables.

CHAPTER 3: BASIC INSTALLATION

The router can be configured with your web browser. A web browser is included as a standard application in the following operating systems: Windows Vista / 7 / 8, Linux, Mac OS, etc. The product provides an easy and user-friendly interface for configuration.

PCs must have an Ethernet interface installed properly and be connected to the router either directly or through an external repeater hub, and have TCP/IP installed or configured to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The default IP address of the router is **192.168.1.254** and the subnet mask is **255.255.255.0** (i.e. any attached PC must be in the same subnet, and have an IP address in the range of 192.168.1.1 to 192.168.1.253). The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problems accessing the router's web interface it may also be advisable to **uninstall** any kind of software firewall on your PCs, as they can cause problems accessing the 192.168.1.254 IP address of the router. Users should make their own decisions on how to best protect their network.

Please follow the steps below for your PC's network environment installation. First of all, please check your PC's network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to your Windows-related or other operating system manuals.

> ⚠
> Any TCP/IP capable workstation can be used to communicate with or through the MX-200(A). To configure other types of workstations, please consult the manufacturer's documentation.
>
> ***Attention***

Network Configuration – IPv4

Configuring PC in Windows 10 (IPv4)

1. Click ⊞.

2. Click ⚙ Settings

3. Then click on **Network and Internet**.
    🌐

4. Under **Related settings,** select **Network and Sharing Center**

Related settings

Change adapter options

Change advanced sharing options

Network and Sharing Center

HomeGroup

Internet options

Windows Firewall
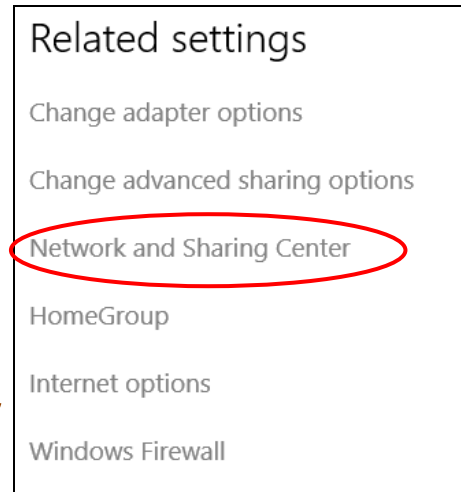
5. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.
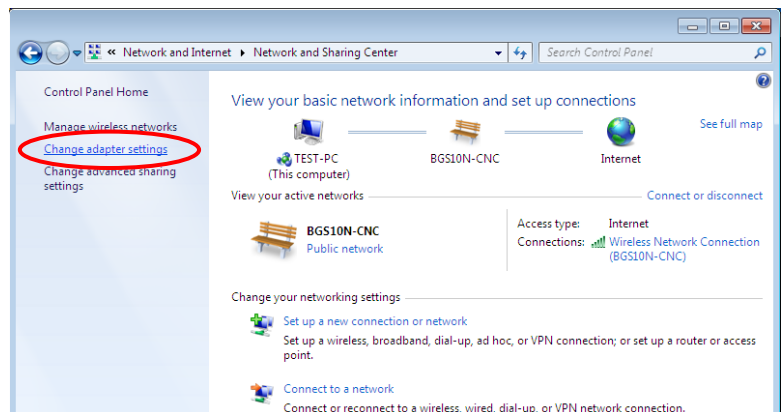
6. Select the **Local Area Connection**, and right click the icon to select **Properties**.
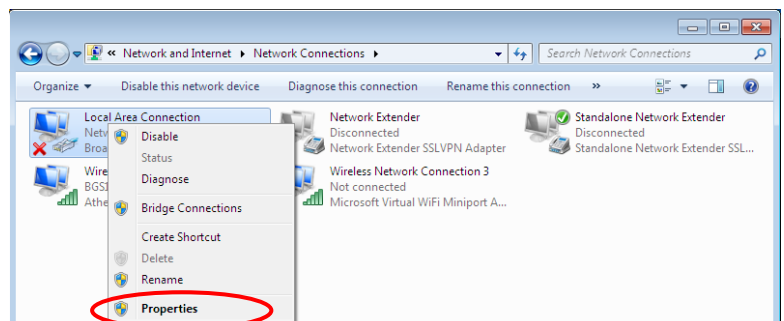
7. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.

8. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

9. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.

Configuring PC in Windows 7/8 (IPv4)

1. Go to **Start**. Click on **Control Panel**.
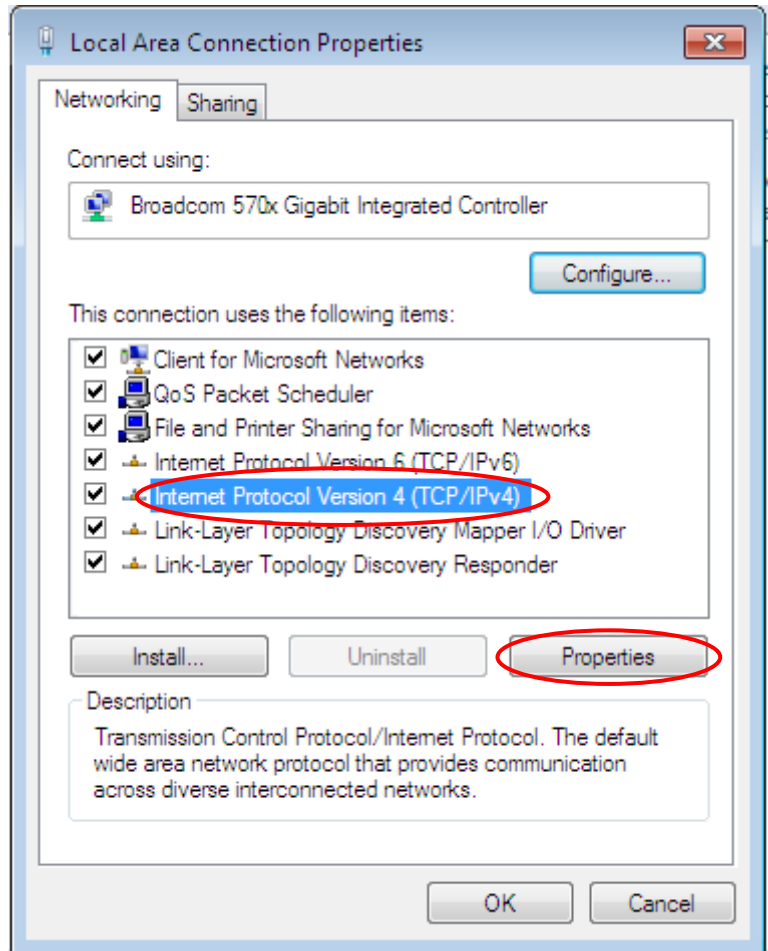
2. Then click on **Network and Internet**.

3. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.

4. Select the **Local Area Connection**, and right click the icon to select **Properties**.
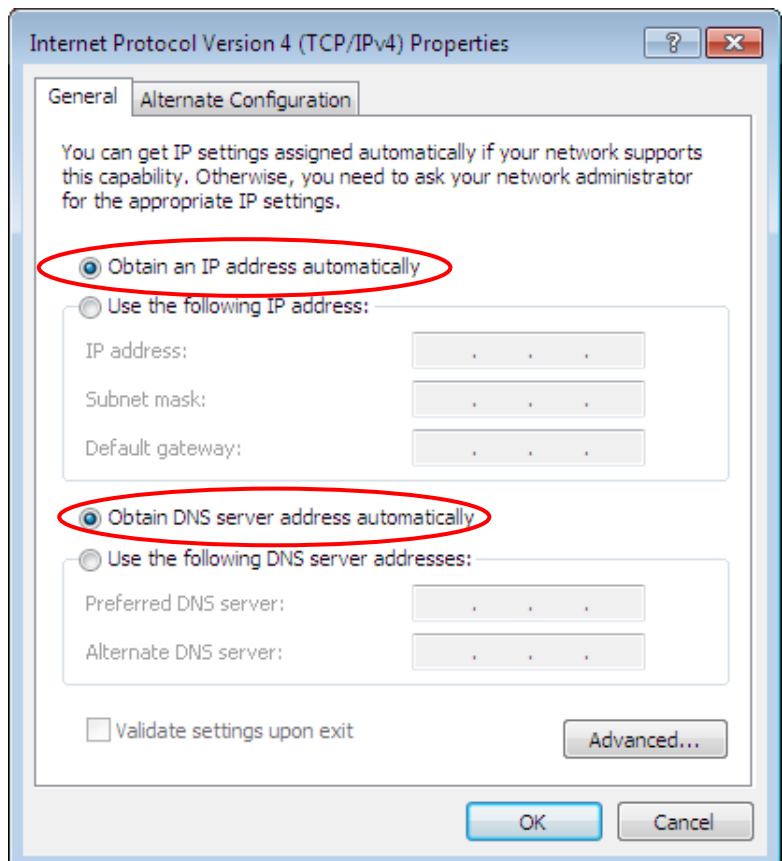
5. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.

Local Area Connection Properties

Networking | Sharing

Connect using:

📟 Broadcom 570x Gigabit Integrated Controller

Configure...

This connection uses the following items:

- ☑ 📟 Client for Microsoft Networks
- ☑ 📟 QoS Packet Scheduler
- ☑ 📟 File and Printer Sharing for Microsoft Networks
- ☑ 📟 Internet Protocol Version 6 (TCP/IPv6)
- ☑ 📟 Internet Protocol Version 4 (TCP/IPv4)
- ☑ 📟 Link-Layer Topology Discovery Mapper I/O Driver
- ☑ 📟 Link-Layer Topology Discovery Responder

Install... | Uninstall | Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
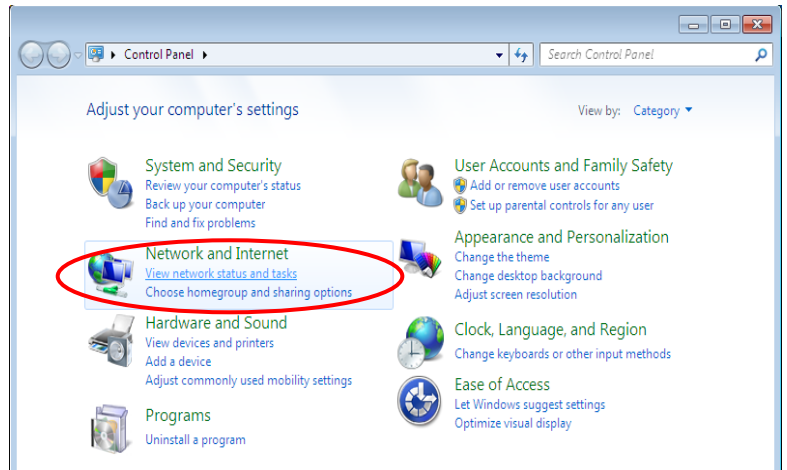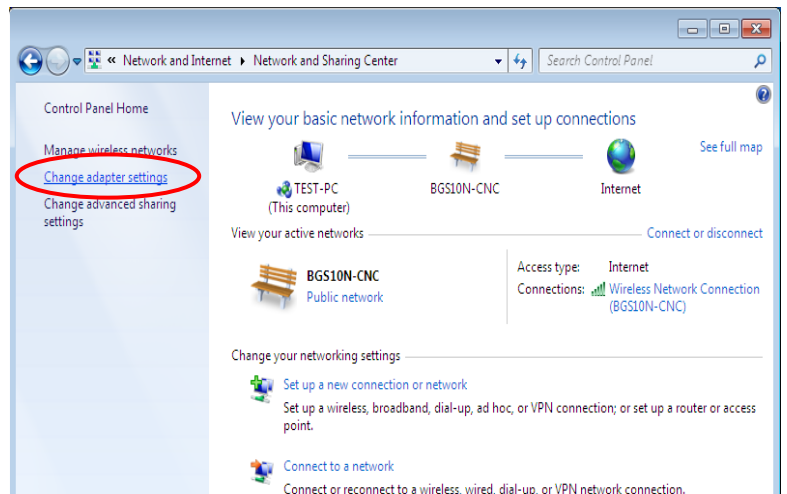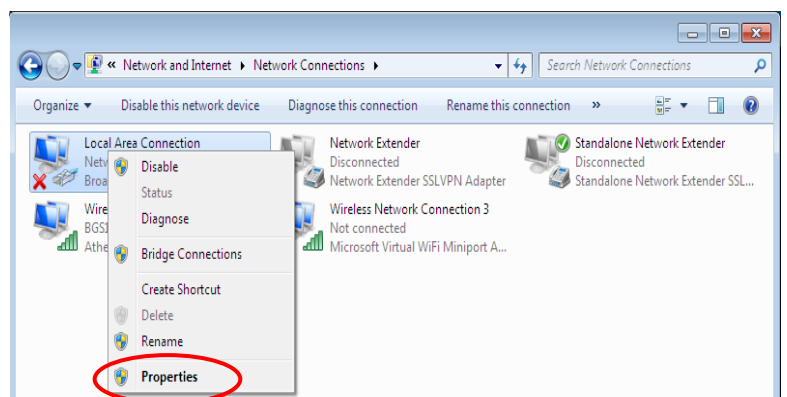
OK | Cancel

6. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.

Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

◉ Obtain an IP address automatically

◯ Use the following IP address:

IP address: ___.___.___

Subnet mask: ___.___.___

Default gateway: ___.___.___

◉ Obtain DNS server address automatically

◯ Use the following DNS server addresses:

Preferred DNS server: ___.___.___

Alternate DNS server: ___.___.___

☐ Validate settings upon exit

Advanced...

OK | Cancel

Configuring PC in Windows Vista (IPv4)

1. Go to **Start**. Click on **Network**.

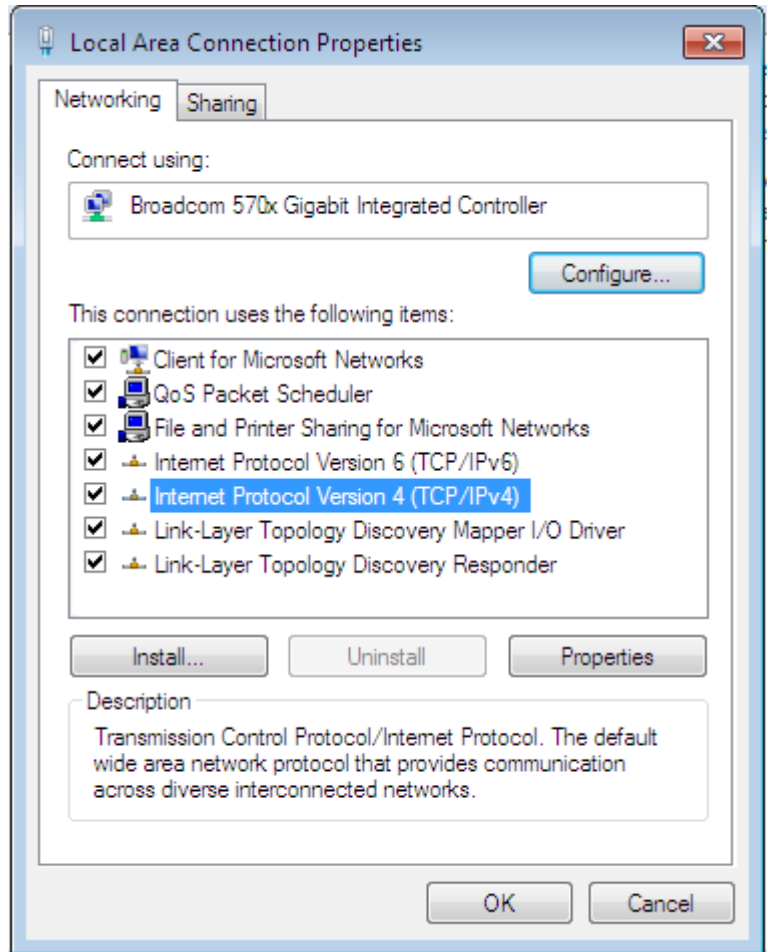2. Then click on **Network and Sharing Center** at the top bar.

3. When the **Network and Sharing Center** window pops up, select and click on **Manage network connections** on the left window pane.
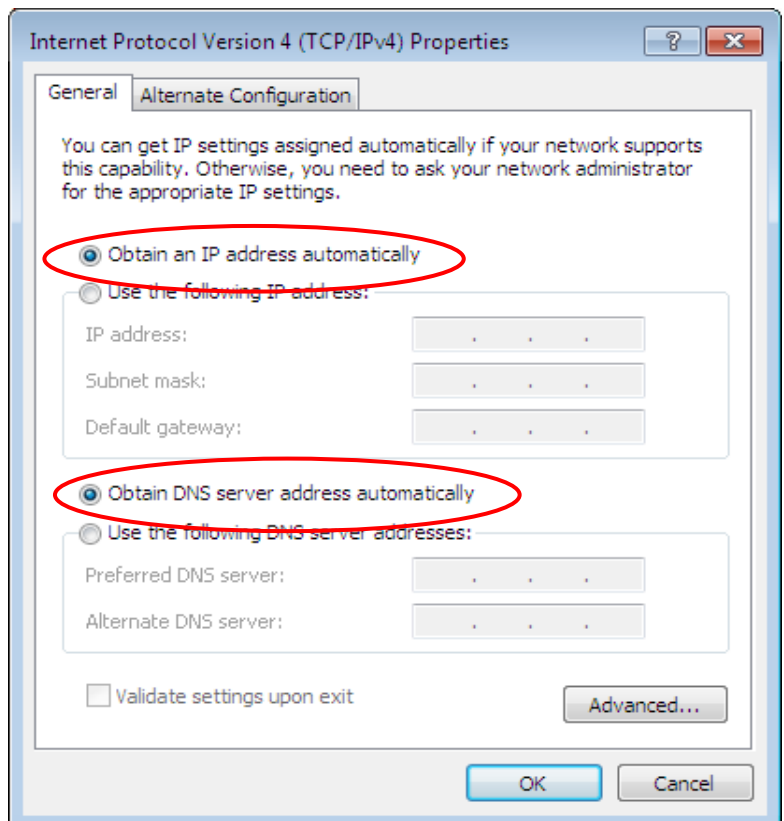
4. Select the **Local Area Connection**, and right click the icon to select **Properties**.

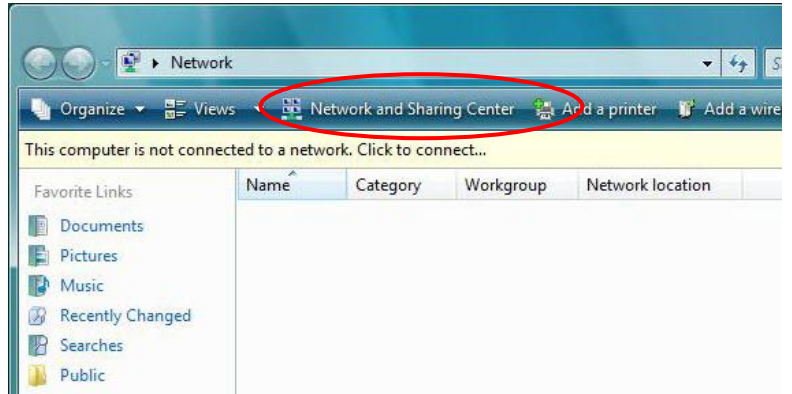**5.** Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.

6. In the **TCP/IPv4 properties** window, select the Obtain an **IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.

Network Configuration – IPv6

Configuring PC in Windows 10 (IPv6)

1. Click .

2. Click Settings

3. Then click on **Network and Internet**.

4. Under **Related settings,** select **Network and Sharing Center**

5. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.

6. Select the **Local Area Connection**, and right click the icon to select **Properties**.
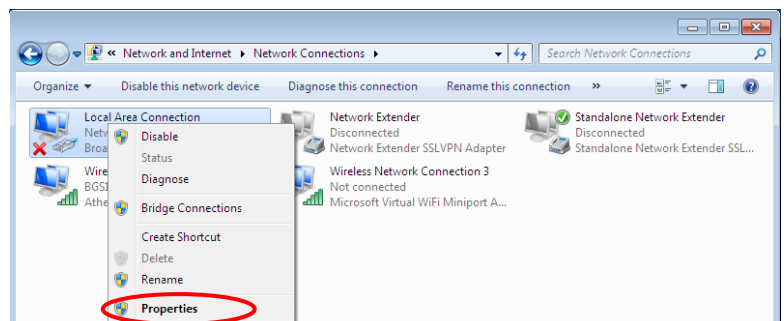
7. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**.
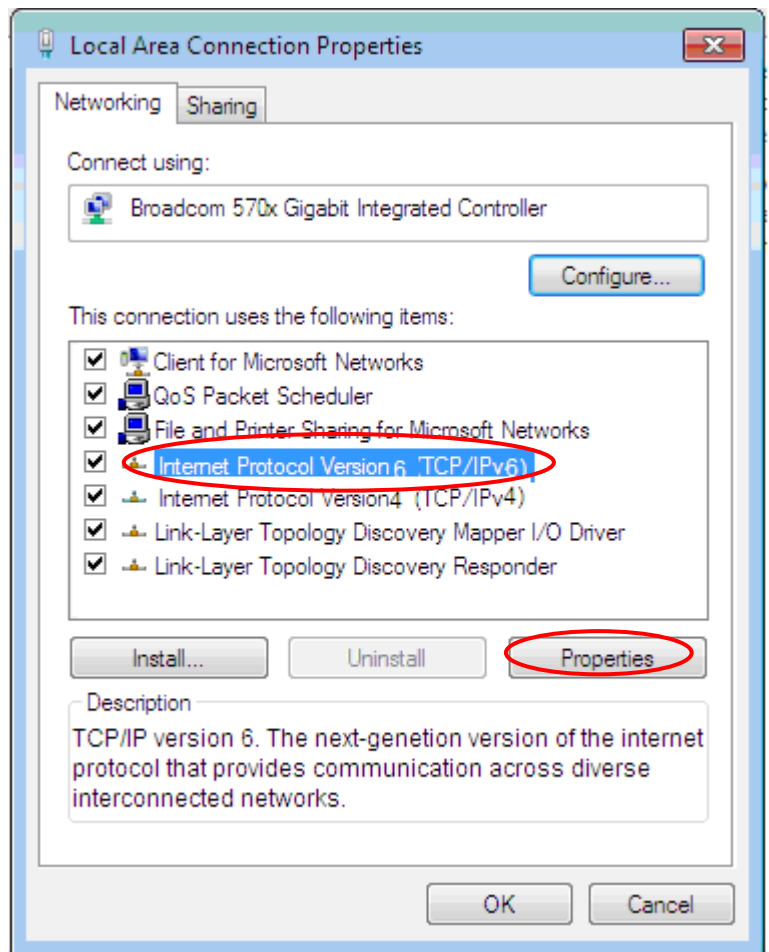
8. In the **TCP/IPv6 properties** window, select the **Obtain an IPv6 address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

9. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.
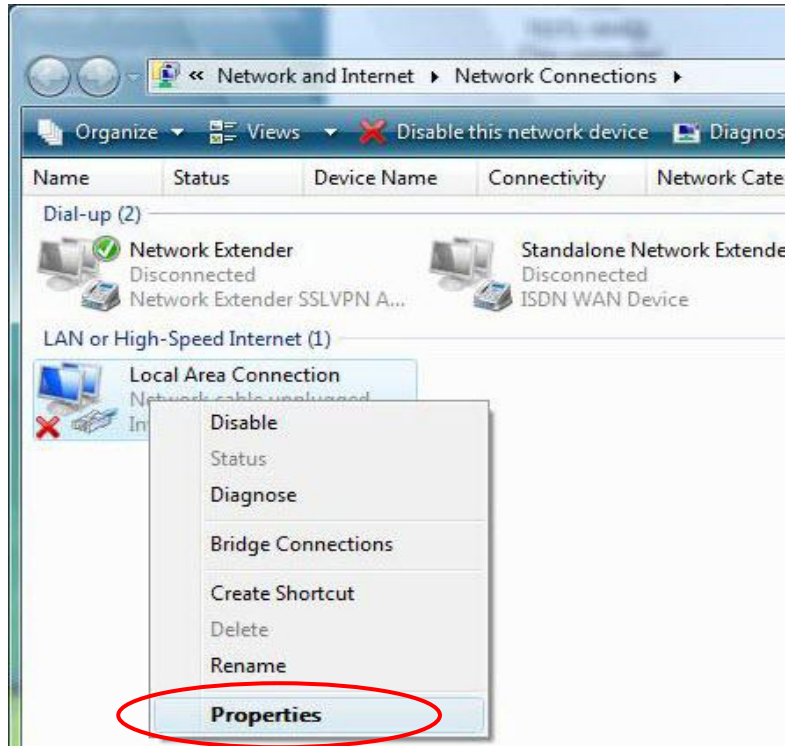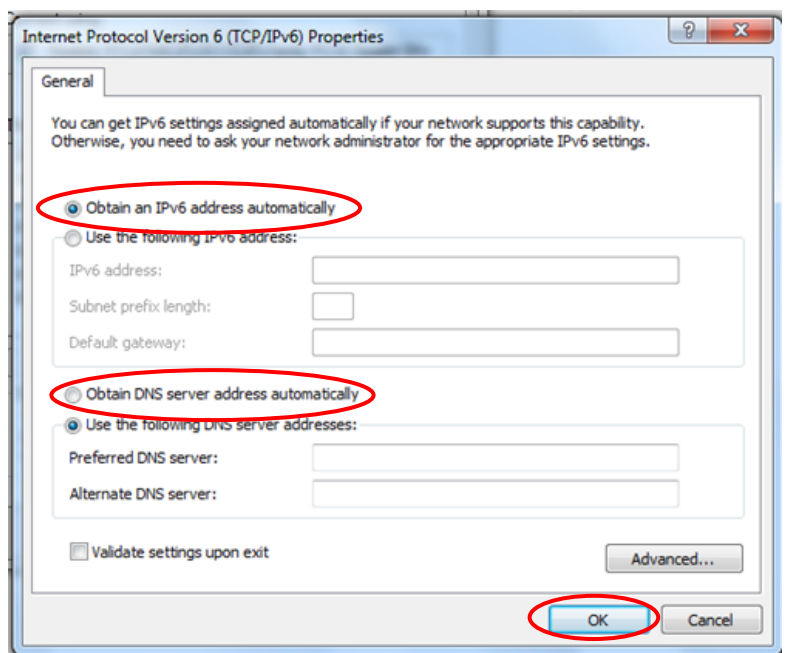
Configuring PC in Windows 7/8 (IPv6)

1. Go to **Start**. Click on **Control Panel**.
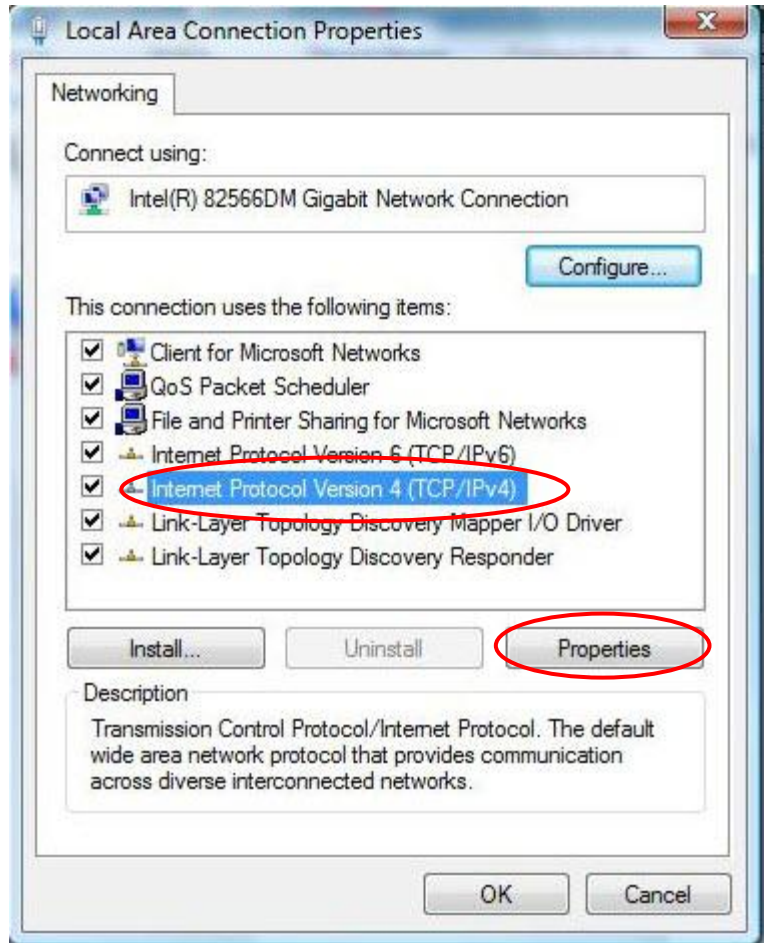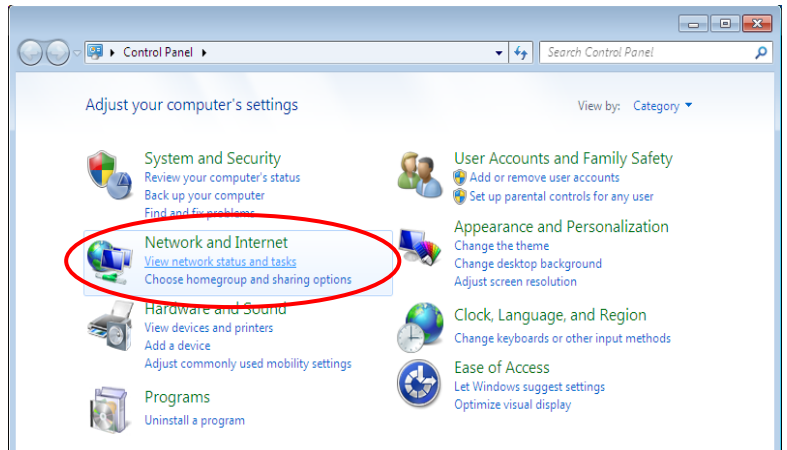

2. Then click on **Network and Internet**.

3. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.
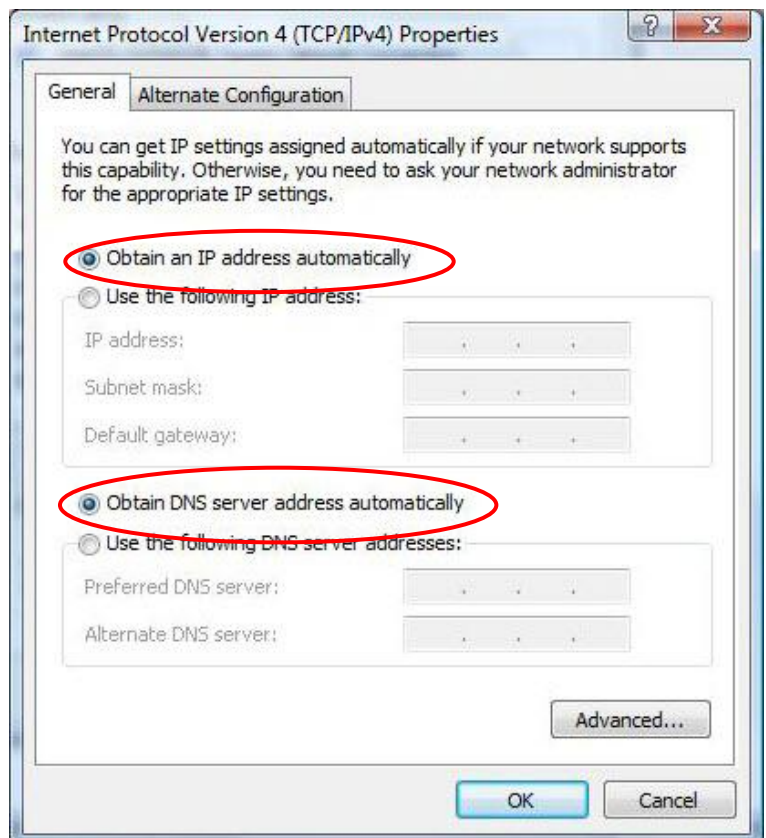

4. Select the **Local Area Connection**, and right click the icon to select **Properties**.

5. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**.
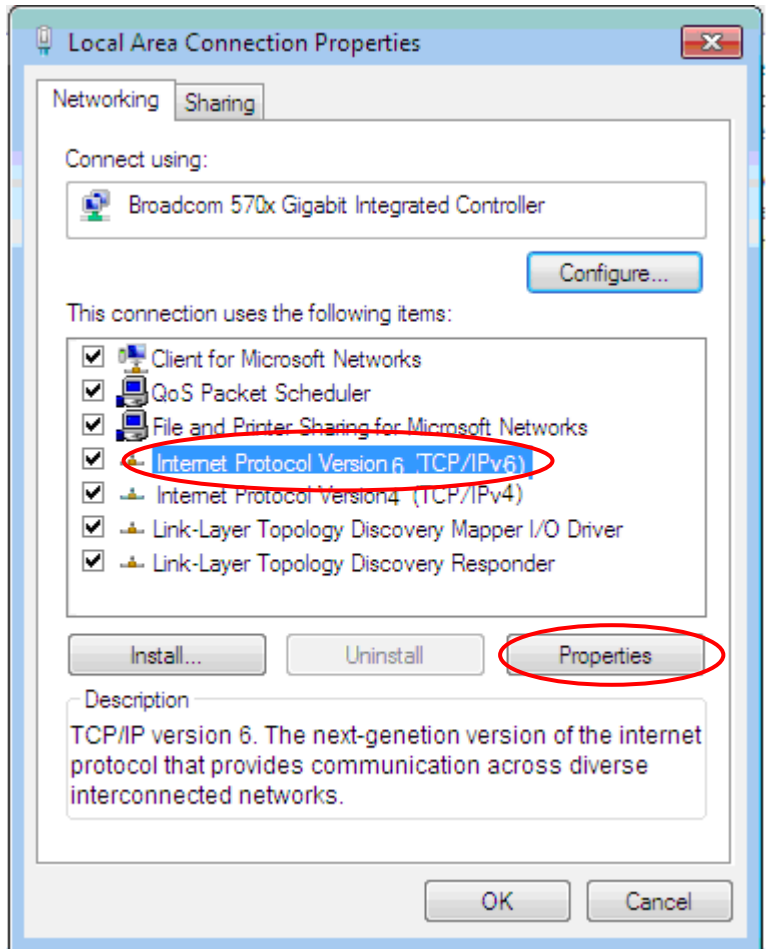
6. In the **TCP/IPv6 properties** window, select the **Obtain an IPv6 address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.

Configuring PC in Windows Vista (IPv6)

1. Go to **Start**. Click on **Network**.
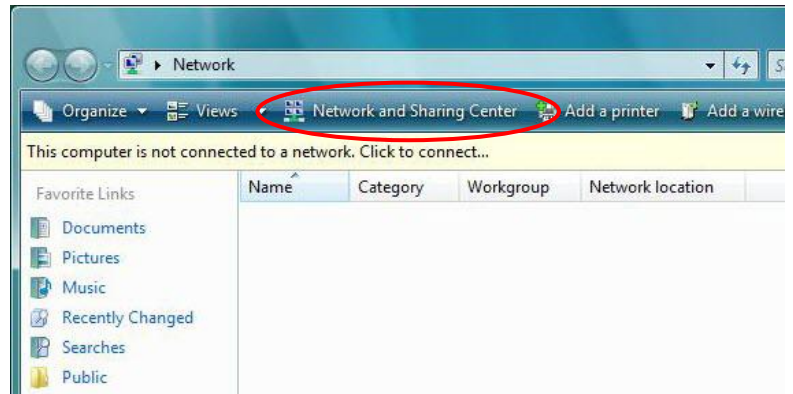
2. Then click on **Network and Sharing Center** at the top bar.

3. When the **Network and Sharing Center** window pops up, select and click on **Manage network connections** on the left window pane.

4. Select the **Local Area Connection**, and right click the icon to select **Properties**.
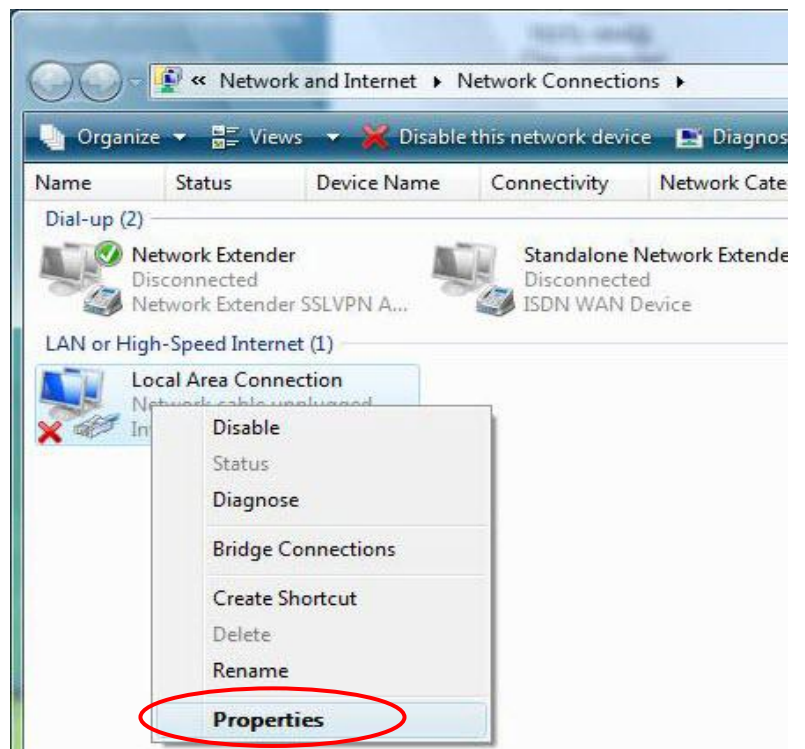
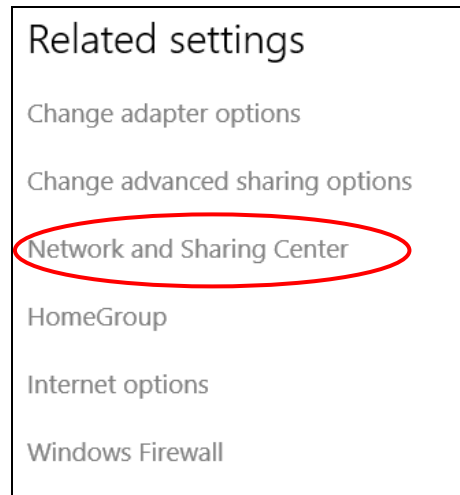5. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**.
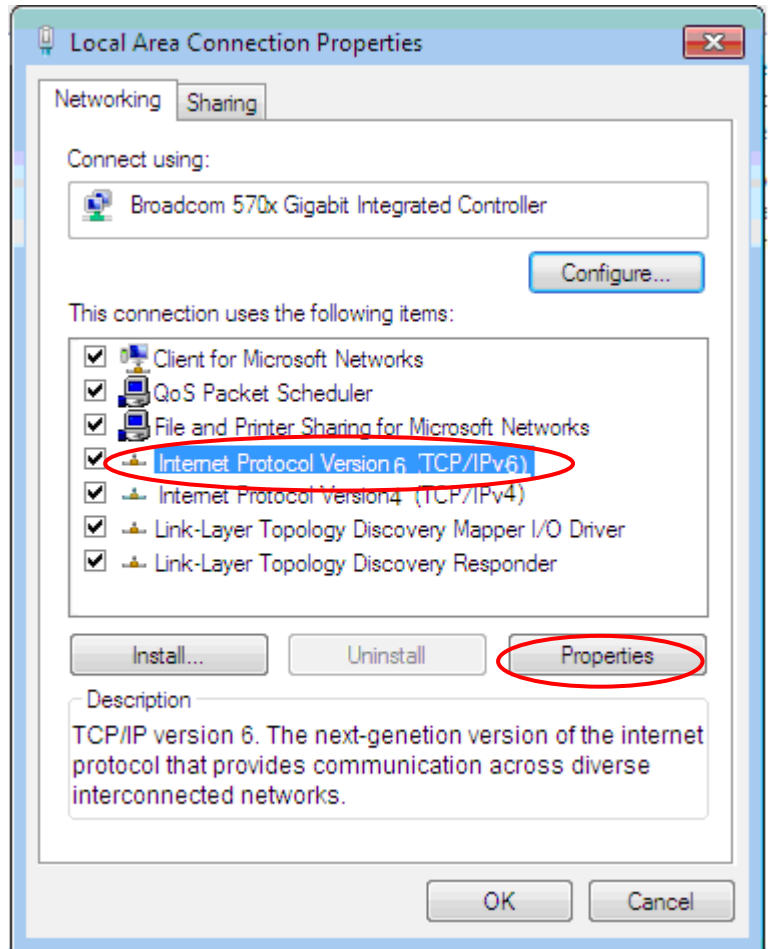
6. In the **TCP/IPv6 properties** window, select the Obtain an **IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

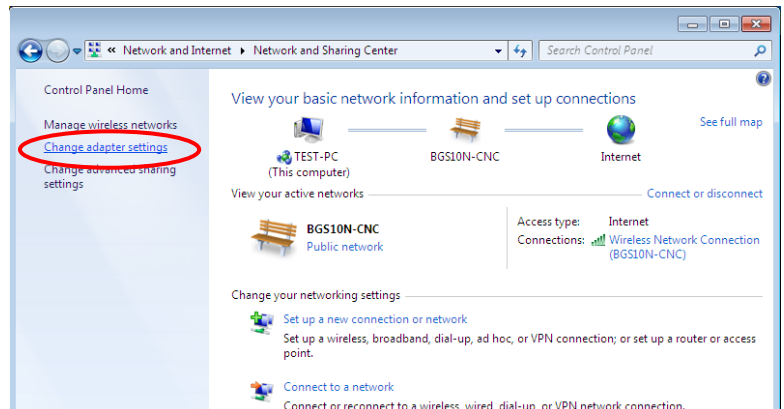7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.

Default Settings

Before configuring the router, you need to know the following default settings.

Web Interface: (Username and Password)

Administrator

✔   Username: admin

✔   Password: A unique12-digit password can be found on the device label.

User

✔   Username: user

✔   Password: user

> If you ever forget the username/password to login to the router, you may press the RESET button up to 6 seconds then release it to restore the factory default settings.
>
> **Caution**: After pressing the RESET button for more than 6 seconds then release it, to be sure you power cycle the device again.

Device LAN IP Settings

✔   IP Address: 192.168.1.254

✔   Subnet Mask: 255.255.255.0

DHCP Server:

✔   DHCP server is enabled.

✔   Start IP Address: 192.168.1.100

✔   IP pool counts: 100

CHAPTER 4: DEVICE CONFIGURATION

Login to your Device

Open your web browser, enter the IP address of your router, which by default is **192.168.1.254**, and click "**Go**", a user name and password window prompt appears.

The default username and password is **"admin"** and **"admin"** respectively for the **Administrator.**

For the **User** account, default username and password is "**user**" and "**user**".

NOTE: This username / password may vary by different Internet Service Providers.

Windows Security ✕

The server 192.168.1.254 is asking for your user name and password. The server reports that it is from MX-200.

Warning: Your user name and password will be sent using basic authentication on a connection that isn't secure.

	User name
	Password
	☐ Remember my credentials

OK   Cancel

Congratulations! You have successfully logged on to your MX-200(A)

Once you have logged on to your MX-200(A) via your web browser, you can begin to set it up according to your requirements. On the configuration homepage, the left navigation pane links you directly to the setup pages, which includes:

Section	Status	Quick Start (Wizard Setup)	Configuration
Sub-Items	Device Info System Status System Log 3G/4G-LTE Status Statistics DHCP Table IPSEC Status PPTP Status L2TP Status GRE Status OpenVPN Status ARP Table VRRP Status		**Interface Setup** - Internet - LAN - Loopback **Dual WAN** - General Setting - Outbound Load Balance - Protocol Binding **Advanced Setup** - Firewall - Routing - Dynamic Routing - NAT - VRRP - Static DNS - Time Schedule - Mail Alert - Serial **VPN** - IPSec - PPTP Server - PPTP Client - L2TP - GRE - OpenVPN Server - OpenVPN Client **Access Management** - Device Management - SNMP - Syslog - Universal Plug & Play - Dynamic DNS - Access Control - Packet Filter - CWMP (TR-069) - Parental Control - BECentral Management **Maintenance** - User Management - Certificate Management - Time Zone - Firmware & Configuration - System Restart - Auto Reboot - Diagnostic Tool

Please see the relevant sections of this manual for detailed instructions on how to configure your **MX-200(A)** device.

Status

Device Info

It provides brief status summary of the device.

▼ Device Information	
Model Name	MX-200
Firmware Version ▸	1.02.1.10
MAC Address	00:04:ed:98:76:54
Date-Time ▸	Fri Jan 2 01:59:11 UTC 1970
System Up Time	1 day 1 hour 59 mins

▼ Physical Port Status	
4G LTE -1	✗
EWAN	✗
Ethernet	✓

▼ WAN

Interface	Protocol	Connection	IP Address	Default Gateway
4G LTE -1 ▼	Dynamic IP	Not Connected	/	

▼ LAN

IP Address	Subnet Mask/Prefix Length	DHCP Server
192.168.1.254	255.255.255.0	Enable / 192.168.1.100~192.168.1.199 Enable / Stateless

Device Information

Model Name: Name of the router for identification purpose.

Firmware Version: Software version currently loaded in the router

MAC Address: A unique number that identifies the router

Data Time: Setup correct time on the **MX-200(A)** with your PC. Check on **Time Zone** section for more configuration information.

System Uptime: Display how long the **MX-200(A)** has been powered on.

Physical Port Status

Physical Port Status：Display available connection interfaces, WAN (3G/4G-LTE, EWAN) and LAN (Ethernet) are supported in the MX-200(A).

WAN

Interface: List current available WAN connections.

Protocol: Display selected WAN connection protocol

Connection: The current connection status.

IP Address: WAN port IP address.

Default Gateway: The IP address of the default gateway.

LAN

IP Address: LAN port IPv4 address.

Subnet Mask/Prefix Length: Display LAN port IP subnet mask of IPv4 and/or Prefix length of IPv6.

DHCP Server: Display LAN DHCP status of IPv4 and IPv6.

▸ **Enable / 192.168.1.100~199**: DHCPv4 server status on or off / DHCP IP range

▸ **Enable / Stateless**: DHCPv6 server status on or off / DHCPv6 server Type

System Status

Display device CPU and memory usage information

▼ System Status	
CPU	
Usage	1%
Memory	
Total	60520 kB
Free	32196 kB
Cached	9948 kB
Refresh	

CPU

Usage: Display the amount of CPU's processing capacity is being used in percentage (%). Higher the % rate may result in slow Internet loading, experiencing video lags, etc. To reduce high CPU consumption by resetting the device, power off and on, an easiest way to regain the service.

Memory

Total / Free / Cached (in Kbyte): Display the memory consumptions in kilobytes (kB).

System Log

In system log, you can check the operations status and any glitches to the router.
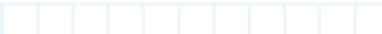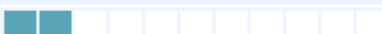
▼ System Log
Jan 1 00:00:31 syslogd started: BusyBox v1.00 (2015.12.28-02:11+0000) Jan 1 00:00:33 pptpd[1492]: MGR: Manager process started Jan 1 00:00:33 pptpd[1492]: MGR: Maximum of 100 connections available Jan 1 00:00:39 PPOELOGIN: bind service port Jan 1 00:00:39 PPOELOGIN: begin service loop Jan 1 00:00:39 syslog: [Hardware monitor]: START Jan 1 00:03:54 WEB: WEB user <admin> login
Refresh Backup

Refresh: Press this button to refresh the statistics.

Backup: Press to save the System log, log.cfg, to your computer / notebook.

3G/4G-LTE Status

It contains 3G/4G-LTE connection information.

▼ 4G/LTE Status	
Status	Up
Signal Strength	▮▮▮▮▮▮▮_ -62.00dbm
Signal Information	RSRP:-92.50 , RSRQ:-13.80 , SINR:11.90
Network Name	"Chunghwa Telecom"
Cell ID	81023501
Card IMEI	
Card IMSI	
Network Mode	LTE
Network Band	B3
Usage Allowance	
Amount used	☐☐☐☐☐☐☐☐☐☐☐☐☐☐ 0Hours of 720Hours
Billing period	▮▮☐☐☐☐☐☐☐☐☐☐☐☐ Day:6
[Clean] [Save]	
[Refresh]	

Status: The current status of the 3G/4G-LTE connection.

Signal Strength: The signal strength bar and dBm value indicates the current 3G/4G-LTE signal strength. The front panel 3G/4G-LTE Signal Strength LED indicates the signal strength as well.

Signal Information: Shows important LTE signal parameters such as RSRP (Reference Signal Receiving Power), RSRQ (Reference Signal Receiving Quality), SINR (Signal to Interference plus Noise Ratio).

‣ RSRP (Reference Signal Receiving Power): is the average power of all resource elements which carry cell-specified reference signals over the entire bandwidth.

‣ RSRQ (Reference Signal Receiving Quality): measures the signal strength and is calculated based on both RSRP and RSSI.

‣ RSSI (Received Signal Strength Indicator): parameter which provides information about total received wide-band power (measure in all symbols) including all interference and thermal noise. Please refer to the Device Description for details.

‣ SINR (Signal to Interference plus Noise Ratio): is also a measure of signal quality as well. It is widely used by the operators as it provides a clear relationship between RF conditions and throughput.

  NOTE: Some LTE modules do not provide this information.

Network Name: The name of the LTE network the router is connecting to.

Cell ID: The ID of base station that the device is connected to.

Physical Cell ID: Display the actual PCI (Physical Cell ID) that device is attached and to transfer the data.
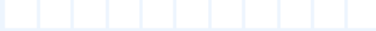
Card IMEI: The unique identification number that is used to identify the 3G/4G-LTE module.

Card IMSI: The international mobile subscriber identity used to uniquely identify the 3G/4G-LTE

module.

Network Mode / Band: Show the using network mode and LTE band.

Usage Allowance

Usage Allowance	
Amount used	0Hours of 720Hours
Billing period	Day:15

Clean | Save

Amount Used: Display the amount of mobile data used and remaining in current billing cycle.

Billing Cycle: Display the start date and number of days remaining in current billing cycle

Clean: Reset current saved mobile usage

Save: Click to save current mobile status to ROM

Refresh: Click to refresh the page.

Statistics

❖ **4G/LTE**

Take 4G/LTE as an example to describe the following connection transmission information.

▼ Statistics	
Traffic Statistics	
Interface	⦿ 3G/4G-LTE Status ◯ EWAN(LAN1) ◯ Ethernet
Transmit Statistics	
Transmit Frames of Current Connection	0
Transmit Bytes of Current Connection	0
Transmit Total Frames	0
Transmit Total Bytes	0
Receive Statistics	
Receive Frames of Current Connection	0
Receive Bytes of Current Connection	0
Receive Total Frames	0
Receive Total Bytes	0
Refresh	

Traffic Statistics

Interface: List all available network interfaces in the router. You are currently checking on the physical status of **3G or 4G/LTE** interface**.**

Transmit Statistics

Transmit Frames of Current Connection: Display the total number of 3G/4G/LTE frames transmitted until the latest second for the current connection.

Transmit Bytes of Current Connection: Display the total bytes transmitted till the latest second for the current connection for the current connection.

Transmit Total Frames: Display the total number of frames transmitted till the latest second since system is up.

Transmit Total Bytes: Display the total number of bytes transmitted until the latest second since system is up.

Receive Statistics

Receive Frames of Current Connection: Display the number of frames received until the latest second for the current connection.

Receive Bytes of Current Connection: Display the total bytes received till the latest second for the current connection.

Receive Total Frames: Display the total number of frames received until the latest second since system is up.

Receive Total Bytes: Display the total frames received till the latest second since system is up.

Refresh: Click to refresh the page.

❖ **EWAN (LAN1)**

▼ Statistics	
Traffic Statistics	
Interface	○ 3G/4G-LTE Status ◉ EWAN(LAN1) ○ Ethernet
Transmit Statistics	
Transmit Frames	0
Transmit Multicast Frames	0
Transmit Total Bytes	0
Transmit Collision	0
Transmit Error Frames	0
Receive Statistics	
Receive Frames	0
Receive Multicast Frame	0
Receive Total Bytes	0
Receive CRC Errors	0
Receive Under-size Frames	0
Refresh	

Traffic Statistics

Interface: List all available network interfaces in the router. You are currently checking on the physical status of the **EWAN (Ethernet #1)** port**.**

Transmit Statistics

Transmit Frames: Display the number of frames transmitted until the latest second.

Transmit Multicast Frames: Display the number of multicast frames transmitted until the latest second.

Transmit Total Bytes: Display the number of bytes transmitted until the latest second.

Transmit Collision: Numbers of collisions have occurred on this port.

Transmit Error Frames: Display the number of error packets on this port.

Receive Statistics

Receive Frames: Display the number of frames received until the latest second.

Receive Multicast Frames: Display the number of multicast frames received until the latest second.

Receive Total Bytes: Display the number of bytes received until the latest second.

Receive CRC Errors: Display the number of error packets on this port.

Receive Under-size Frames: Display the number of under-size frames received until the latest second.

Refresh: Click to refresh the page.

❖ **Ethernet**

Statistics	
Traffic Statistics	
Interface	○ 3G/4G-LTE Status ◉ EWAN(LAN1) ○ Ethernet
Transmit Statistics	
Transmit Frames	0
Transmit Multicast Frames	0
Transmit Total Bytes	0
Transmit Collision	0
Transmit Error Frames	0
Receive Statistics	
Receive Frames	0
Receive Multicast Frame	0
Receive Total Bytes	0
Receive CRC Errors	0
Receive Under-size Frames	0

Refresh

Traffic Statistics

Interface: List all available network interfaces in the router. You are currently checking on the physical status of the **Ethernet** port**.**

Transmit Statistics

Transmit Frames: Display the number of frames transmitted until the latest second.

Transmit Multicast Frames: Display the number of multicast frames transmitted until the latest second.

Transmit Total Bytes: Display the number of bytes transmitted until the latest second.

Transmit Collision: Numbers of collisions have occurred on this port.

Transmit Error Frames: Display the number of error packets on this port.

Receive Statistics

Receive Frames: Display the number of frames received until the latest second.

Receive Multicast Frames: Display the number of multicast frames received until the latest second.

Receive Total Bytes: Display the number of bytes received until the latest second.

Receive CRC Errors: Display the number of error packets on this port.

Receive Under-size Frames: Display the number of under-size frames received until the latest second.

Refresh: Click to refresh the page.

DHCP Table

DHCP table displays the devices connected to the router with clear information.

Index	Host Name	IP Address	MAC Address	Expire Time
1	Billion-HC-ee	192.168.1.101	00:C0:9F:D1:E1:CA	0days 23:36:1

Index #: The numeric indicator for devices using dynamic IP addresses.

Host Name: Display the hostname of the PC.

IP Address: The IP allocated to the device.

MAC Address: The MAC of the connected device.

Expire Time: The total remaining interval since the IP assignment to the PC.

IPSec Status

Index #: The numeric IPSec VPN tunnel/ rule.

Action: Display Connect or Drop the connection.

Connection Name: The profile name of the VPN connection/tunnel.

Active: Display Yes or No to indicate the profile is enabled or disabled.

Connection State: Display statuses of IPSec phase 1 and phase 2 connections.

Statistics: Display upstream/downstream traffic per session in KB. The value clears when session disconnects.

Remote Gateway: Display remote gateway IP address.

Remote Network: Display remote local IP address and Netmask.

Local Network: Display local IP address and Netmask.

Refresh: Click to refresh the page.

PPTP Status

❖ **PPTP Server**

▼PPTP Status					
PPTP Server					
Index	Connection Name	Active	Connection State	Connection Type	Assigned IP Address	Remote Network
1	HS-LL	Yes	Yes	Lan to Lan	192.168.1.2	192.168.0.0 / 255.255.255.0
PPTP Client					
Index	Connection Name	Active	Connection State	Connection Type	Server IP Address	Remote Network
Refresh					

Index #: The numeric PPTP VPN tunnel/ rule.

Connection Name: The profile name of the VPN connection/tunnel.

Active: Display Yes or No to indicate the profile is enabled or disabled.

Connection State: Display the VPN connection status.

Connection Type: Display if VPN connection is for single PC use (Remote Access) or multi-user use (LAN to LAN).

Assigned IP Address: Display the IP address assigned to the client by the PPTP Server.

Remote Network: Display the remote network and subnet mask in LAN to LAN PPTP connection.

Refresh: Click to refresh the page.

❖ **PPTP Client**

▼PPTP Status					
PPTP Server					
Index	Connection Name	Active	Connection State	Connection Type	Assigned IP Address	Remote Network
PPTP Client					
Index	Connection Name	Active	Connection State	Connection Type	Server IP Address	Remote Network
1	BC-LL	Yes	Yes	Lan to Lan	69.121.1.33	192.168.1.0 / 255.255.255.0
Refresh					

Index #: The numeric PPTP VPN tunnel/ rule.

Connection Name: The profile name of the VPN connection/tunnel.

Active: Display Yes or No to indicate the profile is enabled or disabled.

Connection State: Display Yes/No to indicate the VPN connection status.

Connection Type: Display if VPN connection is for single PC use (Remote Access) or multi-user use (LAN to LAN).

Server IP Address: Display the WAN IP address of remote PPTP Server.

Remote Network: Display the remote network address and subnet mask in LAN to LAN PPTP connection.

Refresh: Click to refresh the page.

L2TP Status

Index	Connection Name	Active	Connection State	Connection Mode	Connection Type	Tunnel Remote IP Address
1	HS-LL	Yes	Connected	Dial in	Lan to Lan	192.168.1.200

Refresh

Index #: The numeric L2TP VPN tunnel/rule indicator.

Connection Name: The profile name of the VPN connection/tunnel.

Active: Display Yes or No to indicate the profile is enabled or disabled.

Connection State: Display Yes/No to indicate the VPN connection status.

Connection Mode: Display if L2TP mode is a dial-in or dial-out.

Connection Type: Display if VPN connection is for single PC use (Remote Access) or multi-user use (LAN to LAN).

Tunnel Remote IP Address: Display the remote tunnel IP address.

Refresh: Click to refresh the page.

GRE Status

Index	Connection Name	Active	Connection State	Remote Gateway IP	Remote Network
1	GRE-0	Yes	Connected	69.121.1.30	192.168.0.0/255.255.255.0

Index #: The numerical GRE tunnel/rule indication.

Connection Name: The profile name of the VPN connection/tunnel.

Active: Display Yes or No to indicate the profile is enabled or disabled.

Connection State: Display Yes/No to indicate the VPN connection status.

Remote Gateway IP: Display the remote gateway IP address.

Remote Network: Display the remote local network IP address / Netmask.

OpenVPN Status

❖ **OpenVPN Server**

▼OpenVPN Status					
OpenVPN Server					
Index	Connection Name	Active	Service Port	Tunnel Network	Status
1	OpenVPN1	Yes	1194 /udp	192.168.100.0 /255.255.255.0	Ready
OpenVPN Client					
Index	Connection Name	Active	Remote Server	Status	Detail Info
Refresh					

Index #: The numeric OpenVPN tunnel/ rule.

Connection Name: The profile name of the VPN connection/tunnel.

Active: Display Yes or No to indicate the profile is enabled or disabled.

Service Port: Display the port/protocol (1194/udp) used for OpenVPN connection.

Tunnel Network: Display the virtual tunnel IP address and Netmask of the OpenVPN server.

Status: Display the status of the profile/rule

Refresh: Click to refresh the page.

❖ **OpenVPN Client**

▼OpenVPN Status					
OpenVPN Server					
Index	Connection Name	Active	Service Port	Tunnel Network	Status
OpenVPN Client					
Index	Connection Name	Active	Remote Server	Status	Detail Info
1	OpenVPN1	Yes	69.121.10.5:1194 /udp	Connected	Assigned IP: 192.168.100.2 Route: 192.168.100.0/255.255.255.0 192.168.5.0/255.255.255.0
Refresh					

Index #: The numeric OpenVPN tunnel/ rule.

Connection Name: The profile name of the VPN connection/tunnel.

Active: Display Yes or No to indicate the profile is enabled or disabled.

Remote Server: Display the remote server public IP address and used port/protocol for this connection.

Status: Display the status of the profile/rule

Detailed Info: Display detailed IP assignment and routing information of this VPN connection.

Refresh: Click to refresh the page.

ARP Table

ARP (Address Resolution Protocol) table displays a mapping IP address with a PC's MAC address.

▼ARP Table		
#	IP	MAC Address
1	192.168.1.11	f0:de:f1:31:68:77

#: The numeric table list indicator.

IP Address: It is the internal/local IP address to access to the network.

MAC Address: The MAC address of a device, e.g. PC, notebook, printer, etc., that is corresponded with the IP address.

VRRP Status

▼VRRP Status	
Current Status	N/A
Current Master	N/A

Current Status: Display current VRRP status, Master or Backup.

Current Master: Display the IP address of the Master

Quick Start

This is a useful and easy utility to help you to setup the router quickly and to connect to your ISP (Internet Service Provider) with only a few steps. It will guide you step by step to setup password, time zone, and WAN settings of your device. The Quick Start Wizard is a helpful guide for the first-time users to the device.

▼ **Quick Start**

The 'Quick Start' wizard will guide you to configure the device to connect to your ISP(Internet Service Provider).

Please follow the 'Quick Start' wizard step by step to configure the device. It will allow you to have Internet access within minutes.

Run Wizard

For detailed instructions on configuring WAN settings, see refer to the **Interface Setup** section.

▼ **Quick Start**

The Wizard will guide you through these five quick steps. Begin by clicking on NEXT.

Step 1. Set your new password

Step 2. Choose your time zone

Step 3. Set your internet connection

Step 4. Confirm the configuration and save it

Next

Click **NEXT** to move on to Step 1.

Step 1 – Password

Set new password of the "admin" account to access for router management. The default is "admin". Once changed, please use this new password next time when accessing to the router. Click **NEXT** to continue.

▼ **Quick Start - Password**

You may change the admin account password by entering in a new password. Click NEXT to continue.

| New Password | |
| Confirm Password | |

Back   Next

Step 2 – Time Zone

Choose your time zone. Click **NEXT** to continue.

▼ **Quick Start - Time Zone**

Select the appropriate time zone for your location and click NEXT to continue.

| Time Zone | (GMT-06:00) Central Time (US & Canada), Maxico City, Saskatchewan ▼ |

Back   Next

Step 3 – ISP Connection Type

Set up your Internet connection.

3.1 Select an appropriate WAN connection protocol then click **NEXT** to continue.

▼ Quick Start - ISP Connection Type

Select the WAN Interface and Internet Connection Type to connect to your ISP. Click NEXT to continue.

WAN Interface	4G/LTE ▼

Back Next

3.2(1) If selected **4G/LTE**

Input all relevant 3G/4G/LTE parameters from your cellular provider.

Click **Next** to continue.

▼ Quick Start - 4G/LTE

Enter the 3G information provided to you by your ISP. Click NEXT to continue.

TEL No.	*99***1#
APN	internet
PDN Type	● IPv4 ○ IPv4/IPv6 ○ IPv6
Authentication Protocol	Disable ▼
Username	
Password	
PIN	•••••
Keep Alive	○ Yes ● No
MTU	1428 (0 means use default:1500)

Back Next

3.2(2) If selected **EWAN (LAN1) / Static IP or PPPoE**, enter the static IP address or PPPoE account information provided by your ISP.

Click **NEXT** to continue.

▼ Quick Start - ISP Connection Type

Select the WAN Interface and Internet Connection Type to connect to your ISP. Click NEXT to continue.

WAN Interface	EWAN(LAN1) ▼

ISP
○ Dynamic IP Address (Select the WAN Interface and Internet Connection Type to connect to your ISP. Click **NEXT** to continue.)
○ Static IP Address (Choose this option to set static IP information provided to you by your ISP.)
● PPPoE (Choose this option if your ISP uses PPPoE..)

Back Next

Step 4 – Quick Start Completed

The Setup Wizard has completed. Click on BACK to make changes or correct mistakes. Click **NEXT** to save the current settings and complete the Quick Start setups.

▼ Quick Start - Quick Start Completed

Quick Start Completed !!

The Setup Wizard has completed. Click on BACK to modify changes or mistakes. Click NEXT to exit the Setup Wizard.

Back Next
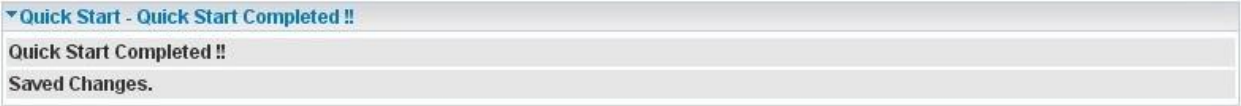
Go back to the **Status > Device Info** to view the status.

Device Configuration

Interface Setup

Here are the features under **Interface Setup: Internet**, **LAN** and **Loopback**

Internet

❖ 4G/LTE

▼ Internet	
WAN Interface	4G/LTE ▼
Status	◉ Activated ○ Deactivated
Usage Allowance ▸	☐ Enable
IP Pass-Through Mode	☐ Enable
LTE Antenna Diversity ▸	Enabled
Network Mode	Automatic ▼
PLMN Selection	Operator Numeric [ ] RAT [ ] Scan
TEL No.	*99***1#
Dual APN	Single APN ▼
APN	internet
PDN Type	◉ IPv4 ○ IPv4/IPv6 ○ IPv6
Authentication Protocol	Disable ▼
Username	[ ]
Password	[ ]
PIN	[ ]
Connection	◉ Always On (Recommended)
Keep Alive	○ Yes ◉ No
Keep Alive IP	[ ]
Default Route	◉ Yes ○ No
NAT	Enable ▼
MTU	1428 (0 means use default:1500)
Save	

WAN Interface: List all available WAN interfaces. (In this section, you have selected to use 4G/LTE)

Status: Choose Activated to enable the 4G/LTE connection.

Usage Allowance: Enable and click "**Usage Allowance**" for further setting configuration of your 4G/LTE data usage.

Usage Allowance

Mode: Include **Volume-based** and **Time-based** control.

- ▸ **Volume-based** include "only Download", "only Upload", and "Download and Upload" to limit the flow.

- ▸ **Time-based** control the flow by providing specific hours per month.

The billing period begins on: the beginning day of billing each month.

Over usage allowance action: Here are actions to perform when mobile data usage, defined in **Mode**, reached to its maximum.

- ▸ **None:** No action taken

- ▸ **Disconnect:** Disconnect mobile connection

- ▸ **Email Alert:** Send an e-mail alert and keep the mobile connection alive.

- ▸ **Email Alert and Disconnect:** Disconnect mobile connection after an alert e-mail is being sent.

Save the statistics to ROM:

- ▸ **Every one hour:** Activate the 3G/4G-LTE statistics on data usage and this info will get updated and saved to the internal memory (ROM) in every hour.

  Once the feature is turned on, you can see the amount of data used and how many days left before next billing cycle starts. Go to **Status >> 3G/4G-LTE Status** page for details.

  NOTE: This statistic information will get deleted after a factory reset.

- ▸ **Disable:** No action taken

LTE Mode*: Display current selected LTE frequency band. To change the band, please click "**LTE Mode**" link to access to the band selection page.

LTE Band

LTE Band: A list of available LTE bands to choose from.

LTE Antenna Diversity *: When **enabled**, the auxiliary antenna will be activated. With **disabled**, only the primary antenna is receiving and transmitting data. To change it, please click "**LTE Antenna Diversity**" link to access to the selection page.

LTE Antenna Diversity

To enable or disable the LTE antenna diversity feature.

* Feature is available with specific cellular module

IP Pass-through Mode: When **enabled**, MX-200(A) is in bridge mode that it does not obtain a WAN IP address; features such as routing capabilities, NAT, firewall, etc., are being disabled. The client router that is behind the MX-200(A) now obtains a WAN IP address. When **disabled**, MX-200(A) is in router mode that it handles a WAN IP address and all features become available.

Network Mode: There are 8 options of service standards: "Automatic", "UMTS 3G only", "GSM 2G Only", "UMTS 3G Preferred", "GSM 2G Preferred", "GSM and UMTS Only", "LTE Only", and "GSM, UMTS, LTE". If you are not sure which mode to use, you may select **Automatic** to auto detect the best mode for you.

PLMN (Public Land Mobile Network) Selection: Either manually enter the information or click **Scan** button to scanning all closest base stations in the area.**TEL No.:** The dial string to make a GPRS / 3G/4G-LTE user internetworking call. It may provide by your mobile service provider.

Dual APN *: Unit can support up to two (2) APNs. Select **Single** / **Dual** or a **different LTE/3G APN**.

‣ **APN (3G):** If select **LTE/3G with different APN,** enter the APN here.

* Feature is available with specific cellular module

APN: An APN is similar to a URL on the WWW, it is what the unit makes a GPRS / UMTS call. The service provider is able to attach anything to an APN to create a data connection, requirements for APNs varies between different service providers. Most service providers have an internet portal which they use to connect to a DHCP Server, thus giving you access to the internet i.e. some 3G operators use the APN 'internet' for their portal. The default value is "internet".

PDN Type: The IP type for PDN connections. Available types are **IPv4**, **IPv6**, and **IPv4v6**.

Authentication Protocol: Manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol). When using PAP, the password is sent unencrypted, while CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client.

Username/Password: Enter the username and password provided by your service provider. The username and password are case sensitive.

PIN: PIN stands for Personal Identification Number. A PIN code is a numeric value used in certain systems as a password to gain access, and authenticate. In mobile phones a PIN code locks the SIM

card until you enter the correct code. If you enter the PIN code incorrectly into the phone 3 times in a row, then the SIM card will be blocked and you will require a PUK code from your network/service provider.

Connection: Default set to Always on to keep an always-on 3G/4G-LTE connection.

Keep Alive / IP: Select **Yes** to keep the 3G/4G-LTE connection always on. Manually enter the Keep Alive IP Address to be used for ping operation to check if the connection is still on.

Default Route: Select **Yes** to use this interface as default route interface.

NAT: Select this option to Disabled/Enable the NAT (Network Address Translation) function. Enable NAT to grant multiples devices in LAN to access to the Internet through a single WAN IP.

When router's Internet configuration is finished successfully, you can go to the Status to check connection information.

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) an IP attempts to send through the interface. **0** means to use default MTU size, 1500byte.

Click **Save** to apply settings.

❖ **EWAN (LAN 1)**

Internet	
WAN Interface	EWAN(LAN1) ▾
Status	◯ Activated ● Deactivated
IPv4/IPv6	
IP Version	◯ IPv4 ● IPv4/IPv6 ◯ IPv6
ISP Connection Type	
ISP	◯ Dynamic IP Address ◯ Static IP Address ● PPPoE
802.1q Options	
802.1q	◯ Activated ● Deactivated
VLAN ID	0 (range: 0~4095)
PPPoE	
Username	
Password	
Bridge Interface for PPPoE	◯ Activated ● Deactivated
Connection Setting	
Connection	● Always On (Recommended) ◯ Connect Manually
TCP MSS Option	TCP MSS 0 bytes(0 means use default)
IP Options	
IP Common Options	
Default Route	● Yes ◯ No
TCP MTU Option	TCP MTU 0 bytes(0 means use default:1492)
IPv4 Options	
Get IP Address	◯ Static ● Dynamic
Static IP Address	0.0.0.0
IP Subnet Mask	0.0.0.0
Gateway	0.0.0.0
NAT	Enable ▾
Dynamic Route	RIP1 ▾ Direction None ▾
IGMP Proxy	◯ Enable ● Disable
IPv6 Options	
IPv6 Address	/
Obtain IPv6 DNS	● Enable ◯ Disable
Primary DNS	
Secondary DNS	
MLD Proxy	◯ Enable ● Disable
Save	

Status: Select to enable/activate or disable/deactivated the service.

IPv4/IPv6

IP Version: Choose **IPv4, IPv4/IPv6, IPv6** based on your environment. If you don't know which one to choose from, please choose IPv4/IPv6 instead.

ISP Connection Type:

ISP: Select the encapsulation type your ISP uses.

▸ **Dynamic IP:** Select this option if your ISP provides you an IP address automatically.

▸ **Static IP:** Select this option to set static IP information. You will need to enter in the Connection type, IP address, subnet mask, and gateway address, provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form. IP address from by four IP octets separated by a dot (xx.xx.xx.xx). The Router will not accept the IP address if it is not in this format.

▸ **PPPoE:** Select this option if your ISP requires you to use a PPPoE connection.

▸ **Bridge:** Select this mode if you want to use this device as an OSI Layer 2 device like a switch.

802.1q Options

802.1q: When activated, please enter a VLAN ID.

VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4095.

PPPoE (If selected PPPoE as WAN Connection Type; otherwise, skip this part)

Username: Enter the user name provided by your ISP.

Password: Enter the password provided by your ISP.

Bridge Interface for PPPoE: When "Activated", the device will gain WAN IP from your ISP with the PPPoE account. But if your PC is connected to the router working as a DHCP client, in this mode, the device acts as a NAT router; while if you dial up with the account within your PC, the device will then work as a bridge forwarding the PPPoE information to the PPPoE server and send the response to your PC, thus your PC gets a WAN IP working in the internet.

Connection Setting

Connection:

▸ **Always On:** Click on **Always On** to establish a PPPoE session during start up and to automatically re-establish the PPPoE session when disconnected by the ISP.

▸ **Connect Manually:** Select Connect Manually when you don't want the connection up all the time.

TCP MSS Option: Enter the maximum size of the data that TCP can send in a segment. Maximum Segment Size (MSS).

IP Options

IP Options	
IP Common Options	
Default Route	◉ Yes ○ No
TCP MTU Option	TCP MTU 0 bytes(0 means use default:1492)
IPv4 Options	
Get IP Address	○ Static ◉ Dynamic
Static IP Address	0.0.0.0
IP Subnet Mask	0.0.0.0
Gateway	0.0.0.0
NAT	Enable ▾
Dynamic Route	RIP1 ▾ Direction None ▾
IGMP Proxy	○ Enable ◉ Disable
IPv6 Options	
IPv6 Address	[ ] / [ ]
Obtain IPv6 DNS	◉ Enable ○ Disable
Primary DNS	[ ]
Secondary DNS	[ ]
MLD Proxy	○ Enable ◉ Disable

IP Common Options

Default Route: Select **Yes** to use this interface as default route interface.

TCP MTU Option: Enter the maximum packet that can be transmitted. Default MTU **0** means it is set to 1492 bytes.

IPv4 Options

Get IP Address: Choose Static or Dynamic

Static IP Address: If **Static** is selected in the above field, please enter the specific IP address you get from ISP and the following IP subnet mask and gateway address.

IP Subnet Mask: The default is 0.0.0.0. User can change it to other such as 255.255.255.0.Type the subnet mask assigned to you by your ISP (if given).

Gateway: Enter the specific gateway IP address you get from ISP.

NAT: Enable to allow MX-200(A) to assign private network IPs to all devices in the network for get Internet access.

Dynamic Route:

▸ **RIP Version:** (Routing Information protocol) Select this option to specify the RIP version, including RIP-1, RIP-2.

▸ **RIP Direction:** Select this option to specify the RIP direction.

- **None** is for disabling the RIP function.

- **Both** means the router will periodically send routing information and accept routing information then   incorporate into routing table.

- **IN only** means the router will only accept but will not send RIP packet.

- **OUT only** means the router will only send but will not accept RIP packet.

IGMP Proxy: IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group. Choose whether enable IGMP proxy.

IPv6 options (only when choose IPv4/IPv6 or just IPv6 in IP version field above):

IPv6 Address: Type the WAN IPv6 address from your ISP.

Obtain IPv6 DNS: Choose if you want to obtain DNS automatically.

Primary/Secondary: if you choose Disable in the Obtain IPv6 DNS field, please type the exactly primary and secondary DNS.

MLD Proxy: MLD (Multicast Listener Discovery Protocol) is to IPv6 just as IGMP to IPv4. It is a Multicast Management protocol for IPv6 multicast packets.

When router's Internet configuration is finished successfully, you can go to status to get the connection information.

Click **Save** to apply settings.

LAN

A Local Area Network (LAN) is a shared communication system to which many computers are attached and is limited to the immediate area, usually the same building or floor of a building.

LAN	
IPv4 Parameters	
IP Address	192.168.1.254
IP Subnet Mask	255.255.255.0
Alias IP Address	0.0.0.0 (0.0.0.0 means to close the alias ip)
Alias IP Subnet Mask	0.0.0.0
Snooping	○ Activated ● Deactivated
Dynamic Route	RIP1 ▼ Direction None ▼
DHCPv4 Server	
DHCPv4 Server	○ Disabled ● Enabled ○ Relay
Start IP	192.168.1.100
IP Pool Count	100
Lease Time	86400 seconds (0 sets to default value of 259200)
Physical Ports	☑ LAN1 ☑ LAN2
DNS Relay	● Automatically ○ Manually
Primary DNS	
Secondary DNS	
Option 66	
Option 160	
Fixed Host	
IP Address	
MAC Address	
IPv6 Parameters	
Interface Address/Prefix Length	/
DHCPv6 Server	
DHCPv6 Server	○ Disable ● Enable
DHCPv6 Server Type	● Stateless ○ Stateful
Start Interface ID	
End Interface ID	
Lease Time	seconds(0 sets to default value of 4800)
Router Advertisements	○ Disable ● Enable

Save

Fixed Host List			
Index	IP	MAC	Drop

IPv4 Parameters

IP Address: Enter the IP address of Router in dotted decimal notation, for example, 192.168.1.254 (factory default).

IP Subnet Mask: The default is 255.255.255.0. User can change it to other such as 255.255.255.128.

Alias IP Address: This is for local networks virtual IP interface. Specify an IP address on this virtual interface.

Alias IP Subnet Mask: Specify a subnet mask on this virtual interface.

IGMP Snooping: Select **Activated** to enable IGMP Snooping function. Without the IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic to be forwarded to all ports. With

IGMP snooping, multicast traffic of a group is only forwarded to ports that have members of that group.

Dynamic Route: Select the RIP version from RIP1 or RIP2.

DHCPv4 Server

DHCP (Dynamic Host Configuration Protocol) allows individual clients to obtain TCP/IP configuration at start-up from a server.

DHCPv4 Server	○ Disabled ● Enabled ○ Relay
Start IP	192.168.1.100
IP Pool Count	100
Lease Time	86400 seconds (0 sets to default value of 259200)
Physical Ports	☑ LAN1 ☑ LAN2
DNS Relay	● Automatically ○ Manually
Primary DNS	
Secondary DNS	
Option 66	
Option 160	

DHCPv4 Server: If set to **Enabled**, your MX-200(A) can assign IP addresses, default gateway and DNS servers to the DHCP client.

▸ If set to **Disabled**, the DHCP server will be disabled.

▸ If set to **Relay**, the MX-200(A) acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the Remote DHCP Server field in this case.

▸ When DHCP is used, the following items need to be set.

Start IP: This field specifies the first of the contiguous addresses in the IP address pool.

IP Pool Count: This field specifies the count of the IP address pool.

Lease Time: The current lease time of client.

Physical Ports: Select to determine if the DHCPv4 server is applicable to the specific port or ports. By default, all ports can obtain local IP from the DHCPv4 server.

DNS Relay:

▸ Select **Automatic** detection or

▸ **Manually** specific Primary and Secondary DNS IP addresses

Primary / Secondary DNS Server: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.

Option 66: Set the IP or hostname of the TFTP server for devices, like IPTV Set Box, to get configuration settings from the TFTP server.

Option 160: Set the IP or hostname of the TFTP server for devices, like IPTV Set Box, to get configuration settings from the TFTP server. (The option 160 is an extended feature in DHCP option, similar to option 66, but using http or https protocols.)

Fixed Host

In this field, users can map the specific IP (must in the DHCP IP pool) for some specific MAC, and this information can be listed in the following table.

Fixed Host	
IP Address	
MAC Address	

IP Address: Enter the specific IP. For example: 192.168.1.110.

MAC Address: Enter the responding MAC. For example: 00:0A:F7:45:6D:ED

When added, you can see the ones listed as showed below:

Fixed Host Listing			
Index	IP Address	MAC Address	Delete
1	192.168.1.110	00:04:ED:01:01:10	✖

IPv6 Parameters

The IPv6 address composes of two parts, thus, the prefix and the interface ID.

Interface Address/Prefix Length		/	

Interface Address / Prefix Length: Enter a static LAN IPv6 address. If you are not sure what to do with this field, please leave it empty as if contains false information it could result in LAN devices not being able to access other IPv6 device. Router will take the same WAN's prefix to LAN side if the field is empty.

DHCPv6 Server

DHCPv6 Server	○ Disable ● Enable
DHCPv6 Server Type	● Stateless ○ Stateful
Start Interface ID	
End Interface ID	
Lease Time	seconds(0 sets to default value of 4800)
Router Advertisements	○ Disable ● Enable

There are two methods to dynamically configure IPv6 address on hosts, **Stateless** and **Stateful**.

Stateless auto-configuration requires no manual configuration of hosts, minimal (if any) configuration of routers, and no additional servers. The stateless mechanism allows a host to generate its own addresses using a combination of locally available information (MAC address) and information (prefix) advertised by routers. Routers advertise prefixes that identify the subnet(s) associated with a link, while hosts generate an "interface identifier" that uniquely identifies an interface on a subnet. An address is formed by combining the two. When using stateless configuration, you needn't configure anything on the client.

Stateful configuration, for example using DHCPv6 (which resembles its counterpart DHCP in IPv4.) In the stateful auto configuration model, hosts obtain interface addresses and/or configuration information and parameters from a DHCPv6 server. The Server maintains a database that keeps track of which addresses have been assigned to which hosts.

DHCPv6 Server: Check whether to enable DHCPv6 server.

DHCPv6 Server Type: Select Stateless or Stateful. When DHCPv6 is enabled, this parameter is available.

▸ **Stateless:** If selected, the PCs in LAN are configured through RA mode, thus, the PCs in LAN are configured through RA mode, to obtain the prefix message and generate an address using a combination of locally available information (MAC address) and information (prefix) advertised by routers, but they can obtain such information like DNS from DHCPv6 Server.

▸ **Stateful:** If selected, the PCs in LAN will be configured like in IPv4 mode, thus obtain addresses and DNS information from DHCPv6 server.

Start interface ID: enter the start interface ID. The IPv6 address composed of two parts, thus, the prefix and the interface ID. Interface is like the Host ID compared to IPv4.

End interface ID: enter the end interface ID.

Leased Time (seconds): the leased time, similar to leased time in DHCPv4, is a time limit assigned to clients, when expires, the assigned ID will be recycled and reassigned.

Router Advertisement: Check to Enable or Disable the Issue Router Advertisement feature. This feature is to send Router Advertisement messages periodically which would multicast the IPv6 Prefix information (similar to v4 network number 192.168.1.0) to all LAN devices if the field is enabled. We suggest enabling this field.

Click **Save** to apply settings.

Loopback

Loopback interface is a widely known virtual interface, not the physical interface, on router and is highly robust and always up. The loopback interface has its own IP and subnet mask, often used for router management as Telnet management IP and involved in BGP as BGP Update-Source and OSPF as Router ID.

▼Loopback	
Loopback interface	○ Activated ● Deactivated
IP Address	127.0.0.1
IP Subnet Mask	255.0.0.0
Save	

IP Address: Enter a dedicated IP address for the loopback interface.

IP Subnet Mask: Enter the subnet mask for the loopback interface.

Click **Save** to apply settings.

Dual WAN

Dual WAN, is a feature to have two independent Internet connection connected concurrently, offers a reliable Internet connectivity and maximize bandwidth utilization for critical applications delivery.

General Setting

Mode: Select a mode then click **Save** to proceed.

❖ **Failover & Failback**

Auto failover/failback ensures always-online network connectivity. When primary WAN link (WAN1) fails, all traffic will switch over to the backup WAN (WAN2) seamlessly.

Again, when the primary link is restored, traffic will be handled over from WAN2 to WAN1.

General Setting	
Dual WAN Mode	
Mode	Failover & Failback ∨
WAN Port Service Detection Policy	
WAN1	4G/LTE ∨
WAN2	EWAN(LAN1) ∨
Keep Backup Interface Connected	Disable ∨
Minimun RSRP/RSSI	-105 / -90 dbm(-111~ -5 , 0:disable)
Connectivity Decision	Auto failover takes place after straight 3 consecutive failure in every 30 seconds.
Probe By Ping	☑ Enable
Ping Setting	○ Gateway ◉ Host 8.8.8.8 Timeout 3 ∨ seconds
Probe By Signal Strength	☑ Enable
Minimum RSRP/RSSI	-105 / -90 dbm(-111~ -5 , 0:disable)
Save	

WAN Port Service Detection Policy

WAN1 (Primary): Choose a desired WAN as the primary WAN Link from the list.

WAN2 (Backup): Choose a desired WAN as the backup WAN Link from the list.

Keep Backup Interface Connected: Select the following option whether to keep the backup WAN (WAN2) interface connected to the Internet.

▸ **Disable:** Inactivate this feature.

▸ **Always:** Keep the backup WAN (WAN2) interface always connected to the Internet

▸ **By Signal Strength:** Enable and initiate automatic backup WAN to connect to the Internet at all time until the RSRP / RSSI of primary WAN is greater than the Minimum RSRP / RSSI.

■ **Minimum RSRP / RSSI:** Set a minimum requirement for RSRP and RSSI for the primary WAN. Value range from -111 ~ -5. 0 means don't care/no need to check this value.

NOTE: Both the RSRP and RSSI cannot be 0 at the same time.

Connectivity Decision & Probe Cycle: Set a number of times and time in seconds to determine when to switch to the backup link (WAN2) when primary link (WAN1) fails and vice versa.

Example, *Auto failover takes place after straight **3** consecutive failures in every **30** seconds* meaning all traffic will hand over to backup link (WAN2) after primary link fails to response in total of 90 seconds, 30 seconds for 3 consecutive failures.

Note: Failover and Failback follow the same **Connectivity Decision & Probe Cycle** rule to failover from WAN1 to WAN2 or fallback from WAN2 to WAN1.

Failover/Fallback Rule Decisions:

1. **Probe by Ping:** Enable Ping to the gateway or an IP address

   ▸ **Gateway:** Internal system will wait for responses to the pings from the gateway of the WAN.

   ▸ **Host:** Internal system will wait for responses to the pings from a fixed IP address.

2. **Probe by Signal Strength:** Enable to measure the LTE signal strength

   ▸ **Minimum RSRP / RSSI:** Set a minimum requirement for RSRP and RSSI for initiating automatic WAN failback or failover procedures.

   The valid range is from <u>-111 ~ -5</u>. <u>0</u> means don't care/no need to check this value.

   NOTE: Both the RSRP and RSSI cannot be 0 at the same time.

Click **Save** to apply settings.

❖ **Load Balance**

Load balance aggregates the bandwidth of the two WAN links to optimize traffic distribution.

When primary link, WAN1, goes down, all traffic will be redirected to the backup, WAN2, to ensure service continuity.

▼ **General Setting**

Dual WAN Mode	
Mode	Load Balance ▼
WAN Port Service Detection Policy	
WAN1	4G/LTE ▼
WAN2	EWAN(LAN1) ▼
Service Detection	⦿ Enable ○ Disable
Connectivity Decision	Auto failover takes place after straight 3 consecutive failure in every 30 seconds.
Probe WAN1	○ Gateway ⦿ Host 8.8.8.8 Timeout 3 ▼ seconds
Probe WAN2	○ Gateway ⦿ Host 8.8.4.4
Save	

WAN Port Service Detection Policy

WAN1 (Primary): Choose a desired WAN as the primary WAN Link from the list.

WAN2 (Backup): Choose a desired WAN as the backup WAN Link from the list.

Service Detection: Enable to detect WAN connectivity automatically.

Connectivity Decision & Probe Cycle: Set a number of times and time in seconds to determine when to turn-off the Load Balancing service.

Example, *Disable Load Balance after straight* **3** *consecutive failures in every* **30** *seconds* meaning all traffic will hand over to backup link (WAN2) after primary link fails to response in total of 90 seconds, 30 seconds for 3 consecutive failures.

Deactivate Load Balance Decision:

    Probe Ping on WAN 1 / WAN2: Enable Ping to the gateway or an IP address

        ▸ **Gateway:** Internal system will wait for responses to the pings from the gateway of the WAN.

        ▸ **Host:** Internal system will wait for responses to the pings from a fixed IP address.

Click **Save** to apply settings

Outbound Load Balance

The connections are distributed over WAN1 and WAN2 so that it can utilize bandwidth of both WAN ports. With Outbound load balance, traffic may be routed to a faster link when one of the WAN links is slower or congested so that user gains better throughput and less delay.

User can distribute outbound traffic based on **Session Mechanism** or **IP Hash Mechanism**.

Base on Session Mechanism:

Balance by Session (Round Robin): Automatically assign requests/traffics to each WAN interface based on real-time WAN traffic-handling capacity.

OR

Balance by Session weight: Manually Balance session traffic based on a weight ratio.

Example: Session weight by 3:1 meaning forward 3 requests to WAN1 and 1 request to WAN2.

Base on IP Hash Mechanism:

Balance by weight: Use an IP hash to balance traffic based on a ratio. It is to guarantee requests from the same IP address get forward to the same WAN interface.

Click **Save** to apply settings

Protocol Binding

Protocol Binding lets you direct specific traffic to go out from a specific WAN port. Policies determine how specific types of internet traffic are routed, for example, traffic from a specific IP address is granted access to only one WAN port rather than using both of the WAN ports as with load balancing.

▼ Protocol Binding	
Rule Index	1 ∨
Active	⦿ Yes ◯ No
Bind Interface	WAN1 ∨ (Current WAN1 Mode: 4G/LTE , Current WAN2 Mode: EWAN)
Source IP Address	0.0.0.0 (0.0.0.0 means Don't care)
Subnet Mask	0.0.0.0
Port Number	0 (0 means Don't care)
Destination IP Address	0.0.0.0 (0.0.0.0 means Don't care)
Subnet Mask	0.0.0.0
Port Number	0 (0 means Don't care)
DSCP	0 (Value Range:0~64, 64 means Don't care)
Protocol	TCP ∨

Save   Delete

Protocol Binding List

#	Active	Interface	Source IP Address/Mask	Destination IP Address/Mask	Source Port	Destination Port	DSCP	Protocol

Rule Index: The numeric rule indicator. The maximum entry is up to 16.

Active: Click YES to activate the rule

Bind Interface: The dedicated WAN interface that guarantees to handle this traffic request.

Source IP Address: Enter the local network, known as source, IP address of the origin of a traffic/packet. **0.0.0.0** means any IP address in the network.

Subnet Mask: Enter the subnet of the source network.

Port Number: Enter the port number which defines the application.

Destination IP Address: Enter the destination / remote WAN IP address where the traffic/packet is going to. Enter **0.0.0.0** if no need to route to a specific IP address

Subnet Mask: Enter the subnet of the designation network.

Port Number: Enter the port number which defines the application.

DSCP: The DSCP value. Value Range from 0~64; **64** means any value/unspecified

Protocol: Select a protocol, TCP, UDP, ICMP, to use for this traffic.

Click **Save** to apply settings

Example:

All traffics from IP 192.168.1.100/255.255.255.0 with port 8080 will go through WAN1 interface.

The only time it would go through WAN2 interface is when WAN1 has no Internet connection.

Protocol Binding List

#	Active	Interface	Source IP Address/Mask	Destination IP Address/Mask	Source Port	Destination Port	DSCP	Protocol
1	Yes	WAN1	192.168.1.100/ 255.255.255.0	0.0.0.0/ 0.0.0.0	8080	0	0	TCP

Advanced Setup

Advanced configuration features provides advanced features, including **Firewall**, **Routing**, **Dynamic Routing**, **NAT**, **VRRP**, **Static DNS**, **Time Schedule**, **Mail Alert**, and **Serial**, for advanced users.

Firewall

Your router includes a firewall for helping to prevent attacks from hackers. In addition to this, when using NAT (Network Address Translation) the router acts as a "natural" Internet firewall, since all PCs on your LAN use private IP addresses that cannot be directly accessed from the Internet.

▼ Firewall	
Firewall	○ Enabled ● Disabled
SPI	○ Enabled ● Disabled
(WARNING: If You enabled SPI, all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.)	
Save	

Firewall: To automatically detect and block Denial of Service (DoS) attacks, such as Ping of Death, SYN Flood, Port Scan and Land Attack.

▸ **Enabled:** Activate your firewall function.

▸ **Disabled:** Deactivate the firewall function.

SPI: If you enabled SPI, all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.

▸ **Enabled:** Activate your SPI function.

▸ **Disabled:** Deactivate the SPI function.

Click **Save** to apply settings

Routing

This is static route feature. You are equipped with the capability to control the routing of all the traffic across your network. With each routing rule created, user can specifically assign the destination where the traffic will be routed to.

▼Routing Table

Index	Destination IP Address	Subnet Mask	Gateway IP Address	Metric	Interface	Edit	Drop
0	100.87.150.196	255.255.255.252	0.0.0.0	0	ppp12		
1	100.72.1.208	255.255.255.248	0.0.0.0	0	ppp11		
2	192.168.1.0	255.255.255.0	0.0.0.0	0	br0		
3	127.0.0.0	255.255.0.0	0.0.0.0	0	lo		
4	239.0.0.0	255.0.0.0	0.0.0.0	0	br0		
5	0.0.0.0	0.0.0.0	100.72.1.209	0	ppp11		

Add Route

Index #: The numeric route indicator.

Destination IP Address: IP address of the destination network

Subnet Mask: The subnet mask of destination network.

Gateway IP Address: IP address of the gateway or existing interface that this route uses.

Metric: It represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 1 and 15.

Interface: Media/channel selected to append the route.

Edit: Edit the route; this icon is not shown for system default route.

Drop: Drop the route; this icon is not shown for system default route.

Add Route

▼ Static Route

Destination IP Address	0.0.0.0
Destination Subnet Mask	0.0.0.0
Gateway IP Address / Interface	○ 0.0.0.0 ● 4G/LTE ▾
Metric	1

Save   Back

Destination IP Address: This is the destination subnet IP address.

Destination Subnet Mask: The subnet mask of destination network.

Gateway IP Address or Interface: This is the gateway IP address or existing interface to which packets are to be forwarded.

Metric: It represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 1 and 15.

Click **Save** to add this route

Dynamic Routing

The NAT (Network Address Translation) feature transforms a private IP into a public IP, allowing multiple users to access the internet through a single IP account, sharing the single IP address. NAT break the originally envisioned model of IP end-to-end connectivity across the internet so NAT can cause problems where IPSec/ PPTP encryption is applied or some application layer protocols such as SIP phones are located behind a NAT. And NAT makes it difficult for systems behind a NAT to accept incoming communications.

Open Shortest Path First (OSPF)

▼ OSPF		
OSPF	☐ Enable	
Rule Index	0 ▼	
Interface	EWAN(LAN1) ▼	
Area ID		
Save Delete		
OSPF Listing		
Index	Interface	Area ID

OSPF: Enable to activate OSPF routing.

Rule Index: The numeric route indicator. The maximum entry is up to <u>10</u>, ranging from 0 to 9.

Interface: Set the interface which runs the OSPF process (involved in OSPF routing). It can be WAN interfaces or established GRE tunnels.

Area ID: The OSPF area identifier. It is a decimal number in the range of 0-4294967295. Enter the area ID in which the interface belongs to. The area with area-id="0" is the backbone area.

If the router has networks in more than one area, then an area with area-id="0" (the backbone) must always be present. All other areas are connected to it. The backbone is responsible for distributing routing information between non-backbone areas. The backbone must be contiguous, i.e. there must be no disconnected segments. However, area border routers do not need to be physically connected to the backbone - connection to it may be simulated using a virtual link.

Border Gateway Protocol (BGP)

A standardized exterior gateway protocol (an uniquely TCP based inter-Autonomous System routing protocol) designed to allow setting up an inter-domain dynamic routing system that automatically updates routing tables of devices running BGP in case of network topology changes.

▼BGP				
BGP	☐ Enable			
As Number				
Rule Index	1 ▼			
Neighbor IP				
Neighbor As Number				
Allowas-in	☐ Enable			
Next-Hop-Self	☐ Enable			
Save Delete				
BGP Listing				
Index	Neighbor IP	Neighbor As Number		Allowas-in

BGP: Enable to activate BGP routing.

AS Number: Designate the AS number of local router. The AS number is used to identify the IBGP or EBGP your neighbor is running. The same AS number means the IBGP, and the different means EBGP.

Rule Index: The numeric route indicator. The maximum entry is up to 10, ranging from 0 to 9.

Neighbor IP: Enter the neighbor IP address.

Neighbor AS Number: Enter the neighbor AS number.

Allowas-in: Enable to allow inter-communication between devices in the same AS. If the local and neighbor AS number are the same, thus, an inter-AS communication, please enable the allowas-in. Otherwise, the router only support EBGP routing between different domains.

Next-Hop-Self: Enable to use the router's own loopback address as the next-hop address.

NAT

The NAT (Network Address Translation) feature transforms a private IP into a public IP, allowing multiple users to access the internet through a single IP account, sharing the single IP address. NAT break the originally envisioned model of IP end-to-end connectivity across the internet so NAT can cause problems where IPSec/ PPTP encryption is applied or some application layer protocols such as SIP phones are located behind a NAT. And NAT makes it difficult for systems behind a NAT to accept incoming communications.

▼ NAT	
NAT Status	Enable
ALG	
VPN Passthrough	⦿ Enabled ◯ Disabled
SIP ALG	⦿ Enabled ◯ Disabled
DMZ / Virtual Server	
Interface	4G/LTE ⌄
DMZ	▶ Edit
Virtual Server	▶ Edit

NAT Status: Enabled. (Disabled if WAN connection is in **BRIDGE** mode)

ALG

VPN Passthrough: VPN pass-through is a feature of routers which allows VPN client on a private network to establish outbound VPNs unhindered.

SIP ALG: Enable the SIP ALG when SIP phone needs ALG to pass through the NAT. Disable the SIP ALG when SIP phone includes NAT-Traversal algorithm.

DMZ / Virtual Server

Interface: Select a WAN interface connection to allow external access to your internal network.

Service Index: Associated to EWAN interface marking each EWAN service (0-7), to select which EWAN service the DMZ and Virtual server are applied to.

Click **DMZ** ▶ Edit or **Virtual Server** ▶ Edit to move on to set the DMZ or Virtual Server parameters, which are represented in the following scenario.

DMZ

NOTE: This feature disables automatically if WAN connection is in BRIDGE mode or NAT is being turned OFF.

The DMZ Host is a local computer which has all UDP and TCP ports exposed to the Internet. When setting an internal IP address as the DMZ Host, all incoming packets will be forwarded to this local host device. Packet filter or virtual server entries will take priority over forwarding internet packets to the DMZ host.

▼ DMZ	
DMZ for	Single IPs Account/ EWAN(LAN1)
DMZ	○ Enabled ● Disabled
DMZ Host IP Address	0.0.0.0

Save   Back

Except Ports

Port	
Protocol	TCP ▼
Description	Add

DMZ Export Ports Listing

Index	Description	Protocol	Port	Edit	Delete
1	N/A	N/A	N/A	📝	
2	N/A	N/A	N/A	📝	
3	N/A	N/A	N/A	📝	
4	N/A	N/A	N/A	📝	
5	N/A	N/A	N/A	📝	
6	N/A	N/A	N/A	📝	

DMZ for (via a WAN Interface): Allows outside network to connect in and communicate with internal LAN devices via a specific WAN interface.

DMZ:

▶   **Enabled:** Activate the DMZ function.

▶   **Disabled:** Deactivate the DMZ function.

DMZ Host IP Address: Give a static IP address to the DMZ Host when **Enabled** radio button is checked. Be aware that this IP will be exposed to the WAN/Internet.

Click **Save** to apply settings

Except Ports

Except Ports: Bypass UDP or/and TCP ports, in the list, being forwarded to the DMZ host.

Port: Enter port to be monitored.

Protocol: Enter the protocol to be monitored.

Description: Enter a description to this rule.

Example: Skip port 80 (UDP/TCP) in the list. All Incoming request to access to port 80 (Web GUI) will be forwarded to the embedded HTTP server of MX-200(A) instead of the DMZ host.

Click **Add** to add an entry to the Except Listing.

Virtual Server

NOTE: This feature disables automatically if WAN connection is in BRIDGE mode or NAT is being turned OFF.

Virtual Server is also known as Port Forwarding that allows MX-200(A) to direct incoming traffic to a specific device in the network.

Configure a virtual rule in MX-200(A) for remote users accessing services such as Web or FTP services via the public (WAN) IP address that can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network.

▼ Virtual Server	
Virtual Server for	4G/LTE
Protocol	TCP ▼
Start Port Number	21
End Port Number	21
Local IP Address	192.168.1.110
Start Port Number (Local)	21
End Port Number(Local)	21

Save   Back

Virtual Server Listing

Rule	Protocol	Start Port	End port	Local IP Address	Start Port Local	End Port Local	Edit	Drop
0	TCP	21	21	192.168.1.110	21	21	📝	❌
1	N/A	N/A	N/A	N/A	N/A	N/A	📝	
2	N/A	N/A	N/A	N/A	N/A	N/A	📝	
3	N/A	N/A	N/A	N/A	N/A	N/A	📝	
4	N/A	N/A	N/A	N/A	N/A	N/A	📝	
5	N/A	N/A	N/A	N/A	N/A	N/A	📝	
6	N/A	N/A	N/A	N/A	N/A	N/A	📝	
7	N/A	N/A	N/A	N/A	N/A	N/A	📝	
8	N/A	N/A	N/A	N/A	N/A	N/A	📝	
9	N/A	N/A	N/A	N/A	N/A	N/A	📝	
10	N/A	N/A	N/A	N/A	N/A	N/A	📝	

Virtual Server for: Indicate the related WAN interface to allow outside network to communicate with the internal LAN device.

Protocol: Choose the application protocol.

Start / End Port Number: Enter a port or port range you want to forward.

(Example: Start / End: 1000 or Start: 1000 & End: 2000).

The starting port must be greater than zero (0). The end port must be greater than or equal to the start port.

Local IP Address: Enter the server IP address in the network to receive the traffic/packets.

Start / End Port Number (Local): Enter the start / end port number of the local application (service).

Examples of well-known and registered port numbers are shown below. For further information, please see IANA's website at http://www.iana.org/assignments/port-numbers

Well-known and Registered Ports

Port Number	Protocol	Description
21	TCP	FTP Control
22	TCP & UDP	SSH Remote Login Protocol
23	TCP	Telnet
25	TCP	SMTP (Simple Mail Transfer Protocol)
53	TCP & UDP	DNS (Domain Name Server)
69	UDP	TFTP (Trivial File Transfer Protocol)
80	TCP	World Wide Web HTTP
110	TCP	POP3 (Post Office Protocol Version 3)
443	TCP & UDP	HTTPS
1503	TCP	T.120
1720	TCP	H.323
7070	UDP	RealAudio

Attention

Using port forwarding does have security implications, as outside users will be able to connect to PCs on your network. For this reason you are advised to use specific Virtual Server entries just for the ports your application requires, instead of using DMZ. As doing so will result in all connections from the WAN attempt to access to your public IP of the DMZ PC specified.

If you have disabled the NAT option in the WAN-ISP section, the Virtual Server function will hence be invalid.

If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign static IP address to each virtual server PC, with an address that does not fall into the range of IP addresses that are to be issued by the DHCP server. You can configure the virtual server IP address manually, but it must still be in the same subnet as the router.

Example: How to setup Port Forwarding for port 21 (FTP server)

If you have a FTP server in your LAN network and want others to access it through WAN.

Step 1: Assign a static IP to your local computer that is hosting the FTP server.

Step 2: Login to the Gateway and go to **Configuration / Advanced Setup / NAT / Virtual Server.**

FTP server uses TCP protocol with port 21.

Enter "21" to Start and End Port Number. The MX-200(A) will accept port 21 requests from WAN side.

Enter the static IP assigned to the local PC that is hosting the FTP server. Ex: 192.168.1.102

Enter "21" to Local Start and End Port number. The MX-200(A) will forward port 21 request from WAN to the specific LAN PC (Example: 192.168.1.102) in the network.

Step 3: Click **Save** to save settings.

▼ Virtual Server								
Virtual Server for		4G/LTE						
Protocol		TCP ⌄						
Start Port Number		21						
End Port Number		21						
Local IP Address		192.168.1.110						
Start Port Number (Local)		21						
End Port Number(Local)		21						

Save   Back

Virtual Server Listing

Rule	Protocol	Start Port	End port	Local IP Address	Start Port Local	End Port Local	Edit	Drop
0	TCP	21	21	192.168.1.110	21	21	📝	❌
1	N/A	N/A	N/A	N/A	N/A	N/A	📝	
2	N/A	N/A	N/A	N/A	N/A	N/A	📝	
3	N/A	N/A	N/A	N/A	N/A	N/A	📝	
4	N/A	N/A	N/A	N/A	N/A	N/A	📝	
5	N/A	N/A	N/A	N/A	N/A	N/A	📝	
6	N/A	N/A	N/A	N/A	N/A	N/A	📝	
7	N/A	N/A	N/A	N/A	N/A	N/A	📝	
8	N/A	N/A	N/A	N/A	N/A	N/A	📝	
9	N/A	N/A	N/A	N/A	N/A	N/A	📝	
10	N/A	N/A	N/A	N/A	N/A	N/A	📝	

VRRP

VRRP is designed to eliminate the single point of failure inherent in the static default routed environment. VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers in a LAN. The VRRP router controlling the IP address associated with a virtual router is called the Master, and forwards packets sent to these IP addresses. The election process provides dynamic fail-over in the forwarding responsibility should the Master become unavailable. Any of the virtual router's IP addresses in a LAN can then be used as the default first hop router by end-hosts. The advantage gained from using VRRP is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end-host.

▼VRRP	
VRRP	○ Activated ◉ Deactivated
VRID	1 (1~255)
Priority	100 (1~254)
Preempt Mode	◉ Activated ○ Deactivated
VRIP	192.168.1.253
Advertisement Period	1 (1~2147483647)
Save	

VRRP: Click to activate the feature.

VRID: Virtual Router Identifier, range from 1-255 (decimal). A master or backup router running the VRRP protocol may participate in one VRID instance.

Priority: Specifies the sending VRRP router's priority for the virtual router. Higher values equal higher priority. The priority value for the VRRP router that owns the IP address associated with the virtual router MUST be 255. VRRP routers backing up a virtual router MUST use priority values between 1 and 254. The default priority value for VRRP routers backing up a virtual router is 100. The priority value zero (0) has special meaning indicating that the current Master has stopped participating in VRRP. This is used to trigger Backup routers to quickly transition to Master without having to wait for the current Master to timeout.

Preempt Mode: When preempt mode is activated, a backup router always takes over the responsibility of the master router. When deactivated, the lower priority backup is left in the master state.

VRIP: An IP address which is associated with the virtual router.

Advertisement period: Indicates the time interval in seconds between advertisements. Default in 1 second.

Click **Save** to apply settings.

Static DNS

The Domain Name System (DNS) is a hierarchical naming system built on a distributed database for computers, services, or any resource connected to the Internet or a private network associates various information with domain names assigned to each of the participating entities. Most importantly, it translates domain names meaningful to humans into the numerical identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide.

An often-used analogy to explain the Domain Name System is that it serves as the phone book for the Internet by translating human-friendly computer hostnames into IP addresses. For example, the domain name www.example.com can be translated into the addresses 192.0.32.10 (IPv4).

▼Static DNS				
IP Address				
Domain Name				
Save				
Static DNS Listing				
Index	IP Address	Domain Name	Edit	Delete

IP Address: The IP address you are going to give a specific domain name.

Domain Name: The friendly domain name for the IP address.

Click **Save** to apply settings.

Time Schedule

The Time Schedule supports up to **16** timeslots which helps you to manage your Internet connection. In each time profile, you may schedule specific day(s) i.e. Monday through Sunday to restrict or allowing the usage of the Internet by users or applications.

This Time Schedule correlates closely with router's time, since router does not have a real time clock on board; it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server from the Internet.

▼Time Schedule								
Rule Index	0 ▼							
Rule Name	TimeSlot1							
		Mon.	Tues.	Wed.	Thur.	Fri.	Sat.	Sun.
Day of Week		☐	☐	☐	☐	☐	☐	☐
Start Time		00:00	00:00	00:00	00:00	00:00	00:00	00:00
End Time		00:00	00:00	00:00	00:00	00:00	00:00	00:00
Save								

Time Index: The rule indicator (0-15) for identifying each timeslot.

Name: User-defined identification for each time period.

Day of Week: Mon. to Sun. Specify the time interval for each timeslot from "Day of Week".

Start Time: The starting point of the interval for the timeslot, anytime in 00:00 – 24:00.

End Time: The ending point of the interval for the timeslot, anytime in 00:00 – 24:00.

Click **Save** to apply your settings.

Example, you can add a timeslot named "TimeSlot1" which features a period from 9:00 of Monday to 18:00 of Tuesday.

▼Time Schedule								
Rule Index	0 ▼							
Rule Name	TimeSlot1							
		Mon.	Tues.	Wed.	Thur.	Fri.	Sat.	Sun.
Day of Week		☑	☑	☐	☐	☐	☐	☐
Start Time		09:00	00:00	00:00	00:00	00:00	00:00	00:00
End Time		24:00	18:00	00:00	00:00	00:00	00:00	00:00
Save								

Another TimeSlot2 spanning from 09:00 to 18:00 of Wednesday

▼Time Schedule								
Rule Index	1 ▼							
Rule Name	TimeSlot2							
		Mon.	Tues.	Wed.	Thur.	Fri.	Sat.	Sun.
Day of Week		☐	☐	☑	☐	☐	☐	☐
Start Time		00:00	00:00	09:00	00:00	00:00	00:00	00:00
End Time		00:00	00:00	18:00	00:00	00:00	00:00	00:00
Save								

Mail Alert

Mail alert is designed to keep system administrator or other relevant personnel alerted of any unexpected events that might have occurred to the network computers or server for monitoring efficiency. With this alert system, appropriate solutions may be tackled to fix problems that may have arisen so that the server can be properly maintained.

▼ Mail Alert		
Server Information		
SMTP Server		
Username		
Password	•••••	
Sender's E-mail		(Must be XXX@yyy.zzz)
SSL/TLS	☐ Enable	
Port	25 (1~65535)	
Account Test		
WAN IP Change Alert		
Recipient's E-mail		(Must be XXX@yyy.zzz)
4G/LTE Usage Allowance		
Recipient's E-mail		(Must be XXX@yyy.zzz)
Apply		

Server Information

SMTP Server: Enter the SMTP server that you would like to use for sending emails.

Username: Enter the username of your email account to be used by the SMTP server.

Password: Enter the password of your email account.

Sender's Email: Enter your email address.

SSL/TLS: Check to whether to enable SSL encryption feature.

Port: the port, default is 25.

Account Test: Click the button to test the connectivity and feasibility to your sender's e-mail.

WAN IP Change Alert

Recipient's Email (WAN IP Change Alert): Enter a valid e-mail address to receive an alert message when WAN IP change has been detected.

Recipient's Email (3G/4G-LTE Usage Allowance): Enter a valid e-mail address to receive an alert message when the 3G or 4G/LTE over Usage Allowance occurs.

Click **Apply** button to save settings

Serial (RS-232 Console Port)

Here is the Serial RS-232 console configuration to connect with any existing industrial machine.

Serial	
General Settings	
Baud Rate	115200 ▾
Data Bits	8 bits ▾
Parity	None ▾
Stop Bits	1 bit ▾
Application	
Mode	Disabled ▾
Save	

General Settings

Baud Rate: Specify the desire baud rate (speed) run on this serial port

Data Bits: Specify the number of data bits contained in a frame

Parity: A simple form of error detection in a frame

Stop Bits: Specify the stop bits of a frame

Application

Mode: Select one of the mode from the list, **Disable / Modbus/TCP / TCP Server / TCP Client / Telnet Server / SSH Server.**

▸ **Disable:** Disable the serial port, RS-232.

▸ **Modbus/TCP:** Modbus is a master/slave communication uses IP over Ethernet to carry data between devices/machines

Mode	Modbus/TCP ▾
Port	502
Response Timeout	3000 ms

■ **Port:** Generally uses port 502, master and slave must use the same port. Specify port other than port 502.

■ **Response Timeout (ms):** Specify a response time-out in milliseconds. After the response timeout expires, default is in 3000ms (3 seconds), data transactions will get aborted.

Here are the possible causes for a timeout to occur:

• Serial connection errors between the MX-200(A) and the serial device

• Hardware issue with the Serial device

• Serial device response time is longer than the specified Response Timeout value. Increase the time-out value to see if it helps

▸ **TCP Server:**

Mode	TCP Server ⌄
Port	782
Empty Serial Buffer When TCP Connection is Established	◉ Yes ○ No
Data Packet Delimitier	○ Inter-character Time Gap 1000 msec(1~30000) ◉ Characters 0x0d0a ("0x"+Hex Code,e.g. "0x0d" or "0x0d0a")
TCP Idle Timeout	60 seconds (10~180)
Save	

- ■ **Port:** Use 782(tcp/udp), an unassigned port, for the TCP Server. Specify a tcp/udp port other than port 782.

- ■ **Empty Serial Buffer When TCP Connection is Established:** When TCP link connection is established, serial buffer will get deleted. Enable to empty the buffer after TCP connection is up.

- ■ **Data packet Delimiter:** A way to keep packets in tract.

  - ● **Inter-character Time Gap:** Default time is in 1000ms. After time has reached, serial data will be transmitted. Time range from 1 – 30000ms.

  - ● **Character Delimiter:** Default characters are 0x0d0a. Serial data will get transmitted when seeing the specified character(s), in this case, 0x0d0a. Valid characters "0x" + Hex code

- ■ **TCP Idle Timeout (Seconds):** Default time is in 60 seconds. Specify an idle time-out in seconds. After the timeout expires, meaning no data transmission within the defined time, serial connection will get aborted. Time range from 10 – 180 seconds

▸ **TCP Client:**

Mode	TCP Client ⌄
Remote Host Name / IP	
Port	782
Empty Serial Buffer When TCP Connection is Established	◉ Yes ○ No
Data Packet Delimitier	○ Inter-character Time Gap 1000 msec(1~30000) ◉ Characters 0x0d0a ("0x"+Hex Code,e.g. "0x0d" or "0x0d0a")
TCP Idle Timeout	60 seconds (10~180)
Save	

- ■ **Remote Host Name / IP:** Enter either TCP server's name or IP address.

- ■ **Port:** Generally uses port 782(tcp/udp). Specify tcp/udp port other than port 782.

- ■ **Empty Serial Buffer When TCP Connection is Established:** When TCP link connection is established, serial buffer will get deleted. Enable to empty the buffer after TCP connection is up.

- ■ **Data packet Delimiter:** A way to keep packets in tract.

  - ● **Inter-character Time Gap:** Default time is in 1000ms. After time has reached, serial

data will be transmitted. Time range from 1 – 30000ms.

- ● **Character Delimiter:** Default characters are 0x0d0a. Serial data will get transmitted when seeing the specified character(s), in this case, 0x0d0a. Valid characters "0x" + Hex code.

- ■ **TCP Idle Timeout (Seconds):** Default time is in 60 seconds. Specify an idle time-out in seconds. After the timeout expires, meaning no data transmission within the defined time, serial connection will get aborted. Time range from 10 – 180 seconds.

▸ **Telnet Server:**

Mode	Telnet Server ∨
Port	782
Save	

- ■ **Port:** Use 782(tcp/udp), an unassigned port. Specify a tcp/udp port other than port 782 for the Telnet server. Port 23 is being reserved, don't use this port.

Note: MX-200(A) uses port 23 as default port the embedded Telnet server.

▸ **SSH Server:**

Mode	SSH Server ∨
Port	782
Save	

- ■ **Port:** Use 782(tcp/udp), an unassigned port. Specify a tcp/udp port other than port 782 for the SSH server. Port 22 is being reserved, don't use this port.

Note: MX-200(A) uses port 22 as default port the embedded SSH server.

Click **Save** to apply settings

VPN

A **Virtual Private Network** (**VPN**) is a private network that interconnects remote (and often geographically separate) networks through primarily public communication infrastructures such as the Internet. VPNs provide security through tunneling protocols and security procedures such as encryption. For example, a VPN could be used to securely connect the branch offices of an organization to a Headquarter office network through the public Internet.

MX-200(A) supports **IPSec, PPTP, L2TP, GRE,** and **OpenVPN**.

IPSec

Internet Protocol Security (**IPSec**) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPSec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.

IPSec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite. It can be used in protecting data flows between a pair of security gateways (*network-to-network*), or between a security gateway and a host (*network-to-host*).

A total of 8 IPSec tunnels can be added.

Index	Connection Name	Active	Interface	Remote Gateway IP	Remote Network	Edit	Delete

▾ IPSec

IPSec Listing
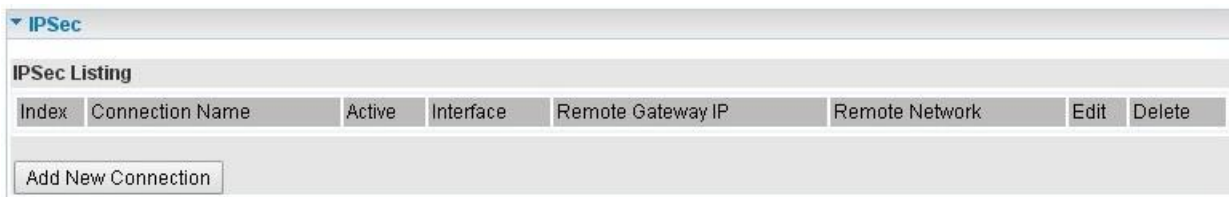
Add New Connection

Click **Add New Connection** to create a new IPSec profile.

IPSec Connection Setting

IPSec					
Connection Name					
Active	⦿ Yes ◯ No				
Interface	Auto ▾				
Remote Gateway IP		(0.0.0.0 means any)			
Local Access Range	Subnet ▾	Local IP Address	0.0.0.0	IP Subnetmask	0.0.0.0
Remote Access Range	Subnet ▾	Remote IP Address	0.0.0.0	IP Subnetmask	0.0.0.0
IKE Mode	Main ▾	Pre-Shared Key			
Local ID Type	Default (Local WAN IP) ▾	IDContent		*	
Remote ID Type	Default (Remote Gateway IP) ▾	IDContent		*	
IKE Proposal	Encryption Algorithm	DES ▾	Authentication Algorithm	MD5 ▾	
	Diffie-Hellman Group	MODP1024(DH2) ▾			
IPSec Proposal	⦿ ESP	◯ AH			
	Encryption Algorithm	DES ▾	Authentication Algorithm	MD5 ▾	
	Perfect Forward Secrecy	None ▾			
SA Lifetime	Phase 1 (IKE)	480 min(s)	Phase 2 (IPSec)	60 min(s)	
Keepalive	None ▾	PING to the IP(0.0.0.0:NEVER)	0.0.0.0	Interval	10 seconds
Disconnection Time after No Traffic	180 seconds (180 at least)				
Reconnection Time	3 min(s) (3 at least)				

Note * : FQDN with @ as first character means don't resolve domain name.

Note ** : (0-3600, 0 means NEVER)

Save   Back

Connection Name: Enter a description for this connection/profile.

Active: Yes to activate the connection.

Interface: Select a WAN interface to establish a tunnel with the remote VPN device. **Auto** allows system to automatically initiate a connection via current connected WAN interface.

Remote Gateway IP: The WAN IP address of the remote VPN device. Enter **0.0.0.0** for unknown remote WAN IP address – only the peer can initiate the tunnel connection.

Local Access Range: Set the IP address or subnet of the local network.

▸ **Single IP:** The IP address of the local host, for establishing an IPSec connection between a security gateway and a host (*network-to-host*).

▸ **Subnet:** The subnet of the local network, for establishing an IPSec tunnel between a pair of security gateways (*network-to-network*)

Remote Access Range: Set the IP address or subnet of the remote network.

▸ **Single IP:** The IP address of the local host, for establishing an IPSec connection between a security gateway and a host (network-to-host). If the remote peer is a host, select Single Address.

▸ **Subnet:** The subnet of the local network, for establishing an IPSec tunnel between a pair of security gateways (network-to-network), if the remote peer is a network, select Subnet.

IPSec Phase 1(IKE)

IKE Mode	Main ▼	Pre-Shared Key		
Local ID Type	Default (Local WAN IP) ▼	IDContent		*
Remote ID Type	Default (Remote Gateway IP) ▼	IDContent		*
IKE Proposal	Encryption Algorithm	DES ▼	Authentication Algorithm	MD5 ▼
	Diffie-Hellman Group	MODP1024(DH2) ▼		

IKE Mode: IKE, Internet Key Exchange, is the mechanism to negotiate and exchange parameters and keys between IPSec peers to establish security associations (SA). Select Main or Aggressive mode.

Pre-Shared Key: This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

Local ID Type / Remote ID Type: When the mode of IKE is aggressive, Local and Remote peers can be identified by other IDs.

IDContent: Enter IDContent the name you want to identify when the Local and Remote Type are Domain Name; Enter IDContent IP address you want to identify when the Local and Remote Type are IP addresses (IPv4 and IPv6 supported).

IKE Proposal & Encryption Algorithm: Select the encryption algorithm from the drop-down menu. There are several options: DES and AES (128, 192 and 256). 3DES and AES are more powerful but increase latency.

 ‣ **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.

 ‣ **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.

 ‣ **AES:** Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

Authentication Algorithm: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmission. There are 3 options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1, SHA256). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

 ‣ **MD5:** A one-way hashing algorithm that produces a 128−bit hash.

 ‣ **SHA1:** A one-way hashing algorithm that produces a 160−bit hash.

Diffie-Hellman Group: It is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). MODP stands for Modular Exponentiation Groups.

IPSec Phase 2(IPSec)

IPSec Proposal	◉ ESP	○ AH		
	Encryption Algorithm	DES ▼	Authentication Algorithm	MD5 ▼
	Perfect Forward Secrecy	None ▼		

IPSec Proposal: Select the IPSec security method. There are two methods of verifying the authentication information, AH (Authentication Header) and ESP (Encapsulating Security Payload).

Use ESP for greater security so that data will be encrypted and the data origin be authenticated but using AH data origin will only be authenticated but not encrypted.

Encryption Algorithm: Select the encryption algorithm from the drop-down menu. There are several options: DES and AES (128, 192 and 256). 3DES and AES are more powerful but increase latency.

> ‣ **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.

> ‣ **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.

> ‣ **AES:** Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

Authentication Algorithm: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmission. There are 3 options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1, SHA256). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

> ‣ **MD5:** A one-way hashing algorithm that produces a 128−bit hash.

> ‣ **SHA1:** A one-way hashing algorithm that produces a 160−bit hash.

Perfect Forward Secrecy: It is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). MODP stands for Modular Exponentiation Groups.

IPSec SA Lifetime

Phase 1 (IKE)SA Lifetime	480	min(s)	Phase 2 (IPSec)	60	min(s)

SA Lifetime: Specify the number of minutes that a Security Association (SA) will stay active before new encryption and authentication key will be exchanged. There are two kinds of SAs, IKE and IPSec. IKE negotiates and establishes SA on behalf of IPSec, and IKE SA is used by IKE.

> ‣ **Phase 1 (IKE):** To issue an initial connection request for a new VPN tunnel. The range can be from 5 to 15,000 minutes, and the default is 480 minutes.

> ‣ **Phase 2 (IPSec):** To negotiate and establish secure authentication. The range can be from 5 to 15,000 minutes, and the default is 60 minutes. A short SA time increases security by forcing the two parties to update the keys. However, every time the VPN tunnel re-negotiates, access through the tunnel will be temporarily disconnected.

IPSec Connection Keep Alive

Keepalive	None ▼		PING to the IP(0.0.0.0:NEVER)	0.0.0.0	Interval	10	seconds **
Disconnection Time after No Traffic	180	seconds (180 at least)					
Reconnection Time	3	min(s) (3 at least)					

Keep Alive:

> ‣ **None:** Disable. The system will not detect remote IPSec peer is still alive or lost. The remote peer will get disconnected after the interval, in seconds, is up.

> ‣ **PING:** This mode will detect the remote IPSec peer has lost or not by pinging specify IP address.

> ‣ **DPD:** Dead peer detection (DPD) is a keeping alive mechanism that enables the router to be

detected lively when the connection between the router and a remote IPSec peer has lost. Please be noted, it must be enabled on the both sites.

PING to the IP: It is able to IP Ping the remote PC with the specified IP address and alert when the connection fails. Once alter message is received, Router will drop this tunnel connection. Reestablish of this connection is required. Default setting is 0.0.0.0 which disables the function

Interval: This sets the time interval between Pings to the IP function to monitor the connection status. Default interval setting is 10 seconds. Time interval can be set from 0 to 3600 second, 0 second disables the function.

Ping to the IP	Interval (sec)	Ping to the IP Action
0.0.0.0	0	No
0.0.0.0	2000	No
xxx.xxx.xxx.xxx (A valid IP Address)	0	No
xxx.xxx.xxx.xxx(A valid IP Address)	2000	Yes, activate it in every 2000 second.

Disconnection Time after No Traffic: It is the NO Response time clock. When no traffic stage time is beyond the Disconnection time set, Router will automatically halt the tunnel connection and re-establish it base on the Reconnection Time set. 180 seconds is minimum time interval for this function.

Reconnection Time: It is the reconnecting time interval after NO TRAFFIC is initiated. 3 minutes is minimum time interval for this function.

Click **Save** to apply settings.

Examples: IPSec – Network (LAN) to Network (LAN)

Two of the MX-200(A) devices want to setup a secure IPSec VPN tunnel

NOTE: The IPSec Settings shall be consistent between the two routers.
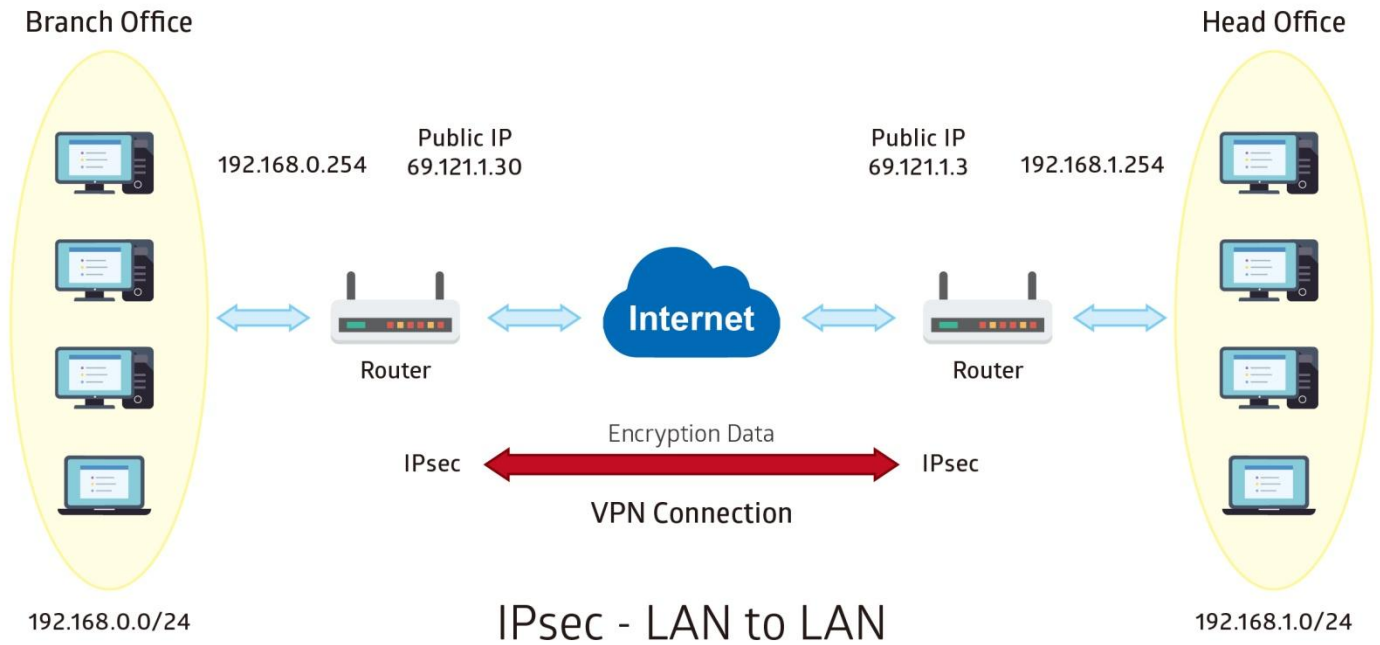
Headquarter office Side:

Configuration Settings		Description
Connection Name	H-to-B	Assigned name to this tunnel/profile
Remote Secure Gateway	69.121.1.30	IP address of the Branch office gateway
Access Network		
Local Access Range	Subnet	Headquarter office network
Local Network IP Address	192.168.1.0	
Local Network Netmask	255.255.255.0	
Remote Access Range	Subnet	Branch office network
Remote Network IP Address	192.168.0.0	
Remote Network Netmask	255.255.255.0	
IPSec Proposal		
IKE Mode	Main	Security Plan
Pre-Shared Key	1234567890	
Phase 1 Encryption	AES-128	
Phase 1 Authentication	SHA1	
Phase 1 Diffie-Hellman Group	MODP 1024(group2)	
Phase 2 Proposal	ESP	
Phase 2 Authentication	SHA1	
Phase 2 Encryption	3DES	
Prefer Forward Security	MODP 1024(group2)	

Branch Office Side:

Configuration Settings		Description
Connection Name	B-to-H	Assigned name to this tunnel/profile
Remote Secure Gateway	69.121.1.3	IP address of the Branch office gateway
Access Network		
Local Access Range	Subnet	Headquarter office network
Local Network IP Address	192.168.0.0	
Local Network Netmask	255.255.255.0	
Remote Access Range	Subnet	Branch office network
Remote Network IP Address	192.168.1.0	
Remote Network Netmask	255.255.255.0	
IPSec Proposal		
IKE Mode	Main	Security Plan
Pre-Shared Key	1234567890	
Phase 1 Encryption	AES-128	
Phase 1 Authentication	SHA1	
Phase 1 Diffie-Hellman Group	MODP 1024(group2)	
Phase 2 Proposal	ESP	
Phase 2 Authentication	SHA1	
Phase 2 Encryption	3DES	
Prefer Forward Security	MODP 1024(group2)	

Examples: IPSec – Remote Employee to MX-200(A) Connection

Router servers as VPN server, and host should install the IPSec client to connect to Headquarter office through IPSec VPN.
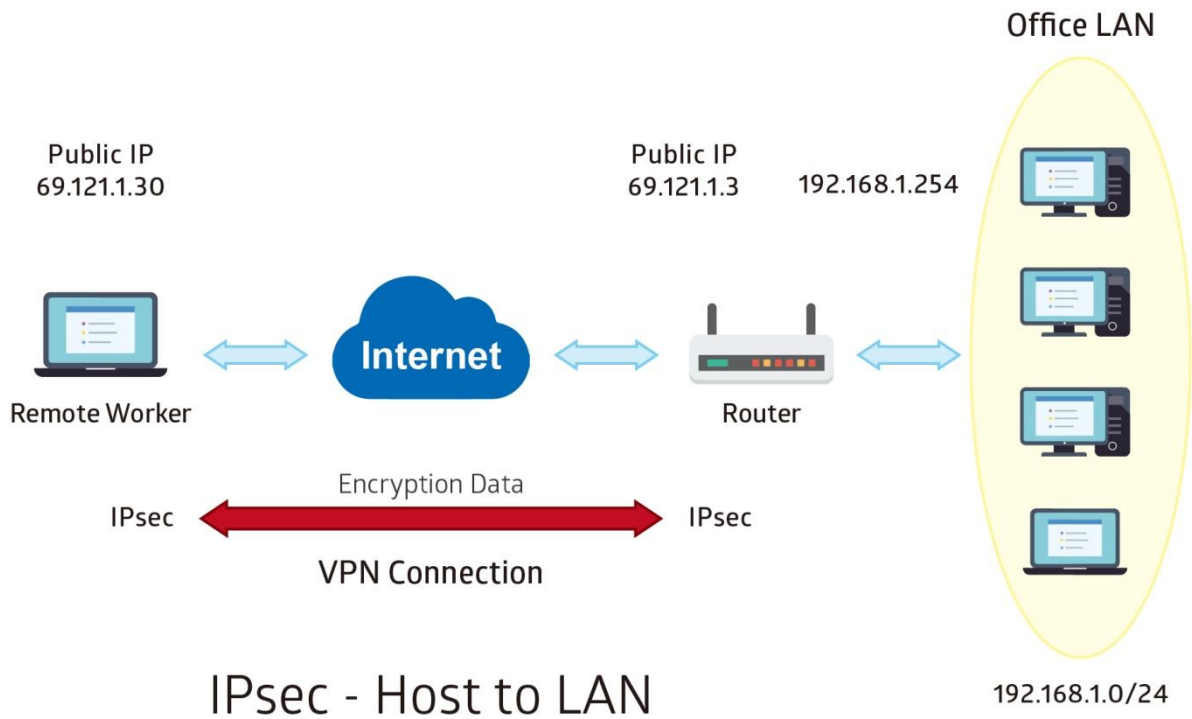
Headquarter office Side:

Configuration Settings		Description
Connection Name	H-to-H	Assigned name to this tunnel/profile
Remote Secure Gateway	69.121.1.30	IP address of the Branch office gateway
Access Network		
Local Access Range	Subnet	Headquarter office LAN network information
Local Network IP Address	192.168.1.0	
Local Network Netmask	255.255.255.0	
Remote Access Range	Signal IP	Remote worker IP address
Remote Network IP Address	69.121.1.30	
Remote Network Netmask	255.255.255.255	
IPSec Proposal		
IKE Mode	Main	Security Plan
Pre-Shared Key	1234567890	
Phase 1 Encryption	AES-128	
Phase 1 Authentication	SHA1	
Phase 1 Diffie-Hellman Group	MODP 1024(group2)	
Phase 2 Proposal	ESP	
Phase 2 Authentication	SHA1	
Phase 2 Encryption	3DES	
Prefer Forward Security	MODP 1024(group2)	

PPTP Server

The **Point-to-Point Tunneling Protocol** (PPTP) is a Layer2 tunneling protocol for implementing virtual private networks through IP network.

In the Microsoft implementation, the tunneled PPP traffic can be authenticated with PAP, CHAP, and Microsoft CHAP V1/V2 . The PPP payload is encrypted using Microsoft Point-to-Point Encryption (MPPE) when using MSCHAPv1/v2.

NOTE: 4 sessions for Client and 4 sessions for Server respectively.

▼ PPTP Server	
PPTP Server	○ Actived ● Deactived
Authentication Type	Chap/Pap ▼
Encryption Key Length	Auto ▼
Encryption Mode	Allow Stateless and Statefull ▼
CCP	● Yes ○ No
MS-DNS	192.168.1.254
Rule Index	1 ▼
Connection Name	
Active	○ Yes ● No
Username	
Password	•••••
Connection Type	Remote Access ▼
Private IP Address assigned to Dial-in User	
Remote Network IP Address	
Remote Network Netmask	
Save Delete	

PPTP Server Listing					
Index	Connection Name	Active	Username	Connection Type	Assigned IP Address

PPTP Server: Select **Activate / Deactivate** to enable or disable the PPTP Server.

Authentication Type: Pick an authentication type from the drop-down list. When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client. When passed the authentication with MS-CHAPv2, the MPPE encryption is supported.

Encryption Key Length: Auto, data encryption and key length, with 40-bit or 128-bit, is automatically negotiated when establish a connection. 128-bit keys provide strong stronger encryption than 40-bit keys.

Encryption Mode: The encryption key will be changed every 256 packets with Stateful mode. With Stateless mode, the key will be changed in each packet.

CCP (Compression Control Protocol): Enable to compress data to save bandwidth and increase data transfer speed.

MS-DNS: Assign a DNS server or use router default IP address to be the MS-DNS server IP address.

Rule Index: The numeric rule indicator for PPTP server. The maximum entry is up to 4.

Connection Name: Enter a description for this connection/profile.

Active: **Yes** to activate the account. PPTP server is waiting for the client to connect to this account.

Username / Password: Enter the username / password for this profile.

Connection Type: Select Remote Access for single user, Select LAN to LAN for remote gateway.

**Private IP Address Assigned to Dial-in User:** Specify the private IP address to be assigned to dial-in clients, and the IP should be in the same subnet as local LAN, but not occupied.

Remote Network IP Address: Enter the subnet IP of the remote LAN network.

Remote Network Netmask: Enter the Netmask of the remote LAN network.

Click **Save** to apply settings.

PPTP Client

Establish a PPTP tunnel over Internet to connect with a PPTP server.

A total of 4 PPTP Client sessions can be created.

▼PPTP Client	
Rule Index	1 ▼
Connection Name	
Active	○ Yes ● No
Authentication Type	Chap/Pap ▼
Encryption Key Length	Auto ▼
Encryption Mode	Allow Stateless or Statefull ▼
CCP	● Yes ○ No
Username	
Password	•••••
Connection Type	Remote Access ▼
Server IP Address	
Remote Network IP Address	
Remote Network Netmask	
Active as Default Route	☐ Enable
Save Delete	
PPTP Client Listing	

Index	Connection Name	Active	Username	Connection Type	Server IP Address

Rule Index: The numeric rule indicator for PPTP client. The maximum entry is up to 4.

Connection Name: Enter a description for this connection/profile.

Active: **Yes** to activate the account. PPTP server is waiting for the client to connect to this account.

Authentication Type: Pick an authentication type from the drop-down list. When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client. When passed the authentication with MS-CHAPv2, the MPPE encryption is supported.

Encryption Key Length: Auto, data encryption and key length, with 40-bit or 128-bit, is automatically negotiated when establish a connection. 128-bit keys provide strong stronger encryption than 40-bit keys.

Encryption Mode: The encryption key will be changed every 256 packets with Stateful mode. With Stateless mode, the key will be changed in each packet.

CCP (Compression Control Protocol): Enable to compress data to save bandwidth and increase data transfer speed.

Username / Password: Enter the username / password provided by the PPTP server/host.

Connection Type: Select Remote Access for single user, Select LAN to LAN for remote gateway.

Server Address: Enter the WAN IP address of the PPTP server.

Remote Network IP Address: Enter the subnet IP of the server/host LAN network.

Remote Network Netmask: Enter the Netmask of the server/host LAN network.

Click **Save** to apply settings.

Example: PPTP – Remote Employee Dial-in to MX-200(A)
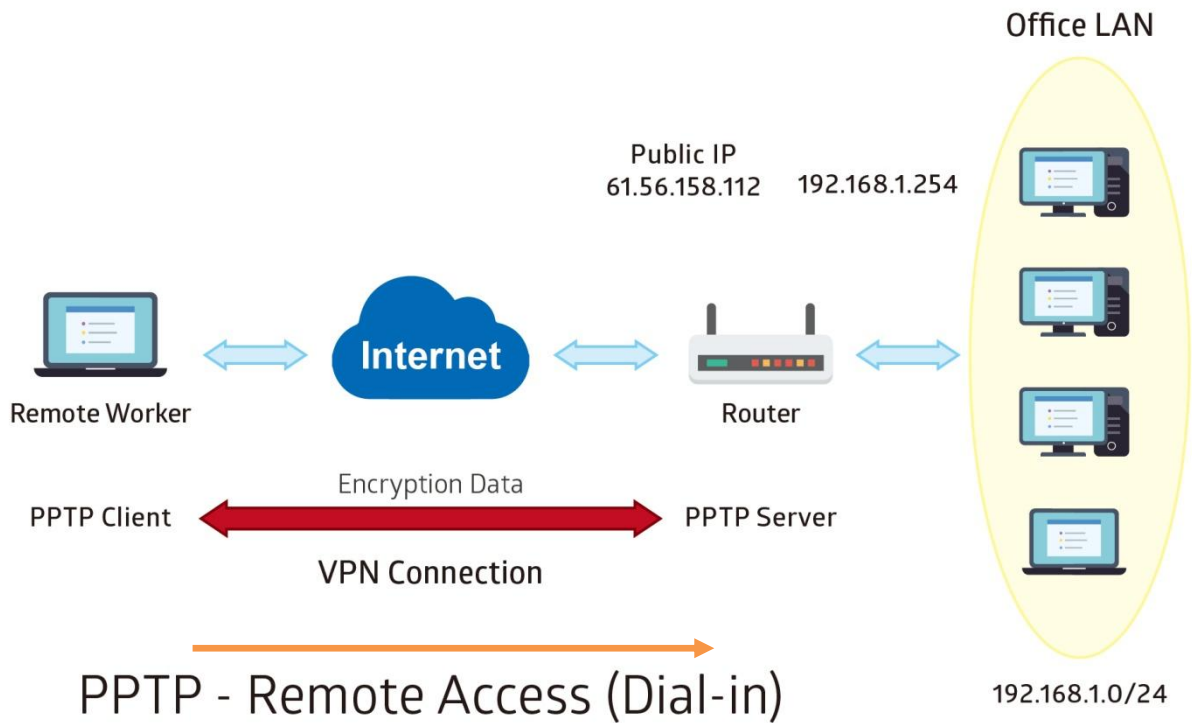
PPTP - Remote Access (Dial-in)

The input IP address 192.168.1.2 will be assigned to the remote worker. Please make sure this IP is not used in the Office LAN.

Configuration Settings		Description
Connection Name	HS-RA	Assigned name to this tunnel/profile
Authentication Type	MS-CHAPv2	Authentication type
Username	test	Credential created from the device to a
Password	test	PPTP client to dial-in to the network.
Connection Type	Remote Access	Remote access for a dial-in
Assigned IP	192.168.1.2	Local IP assigned to the dial-in client

▼ **PPTP Server**

PPTP Server	◉ Actived ○ Deactived
Authentication Type	MS-CHAPv2 ∨
Encryption Key Length	Auto ∨
Encryption Mode	Allow Stateless and Statefull ∨
CCP	◉ Yes ○ No
MS-DNS	192.168.1.254
Rule Index	1 ∨
Connection Name	HS-RA
Active	◉ Yes ○ No
Username	test
Password	••••
Connection Type	Remote Access ∨
Private IP Address assigned to Dial-in User	192.168.1.2
Remote Network IP Address	
Remote Network Netmask	

Save   Delete

PPTP Server Listing

Index	Connection Name	Active	Username	Connection Type	Assigned IP Address
1	HS-RA	Yes	test	Remote Access	192.168.1.2

Example: PPTP – Remote Employee Dial-out to MX-200(A)

A company's office establishes a PPTP VPN connection with a file server located at a separate location. The router is installed in the office, connected to a couple of PCs and Servers.
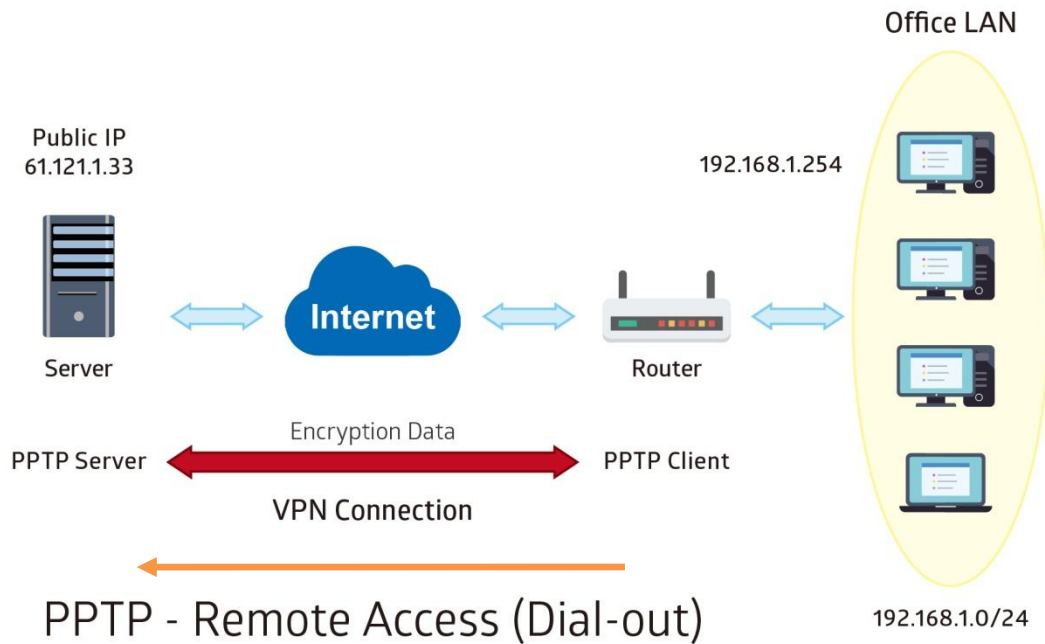
PPTP Server WAN IP address is 61.121.1.33 of the Headquarter office.

Configuration Settings		Description
Connection Name	HS-RA	Assigned name to this tunnel/profile
Authentication Type	MS-CHAPv2	Authentication type
Username	test	Credential assigned from the PPTP server
Password	test	for PPP client to dial-in to its network.
Connection Type	Remote Access	Remote access for a dial-in
Server IP	61.121.1.33	VPN server WAN IP address

▼PPTP Client	
Rule Index	1 ⌄
Connection Name	HS-RA
Active	⦿ Yes ○ No
Authentication Type	MS-CHAPv2 ⌄
Encryption Key Length	Auto ⌄
Encryption Mode	Allow Stateless or Statefull ⌄
CCP	⦿ Yes ○ No
Username	test
Password	•••••
Connection Type	Remote Access ⌄
Server IP Address	69.121.1.33
Remote Network IP Address	192.168.1.0
Remote Network Netmask	255.255.255.0
Active as Default Route	☐ Enable
Save Delete	

PPTP Client Listing

Index	Connection Name	Active	Username	Connection Type	Server IP Address
1	HS-RA	Yes	test	Remote Access	69.121.1.33

Example: PPTP – Network (LAN) to Network (LAN) Connection

The branch office establishes a PPTP VPN tunnel with Headquarter office to connect two private networks over the Internet. The routers are installed in the Headquarter office and branch offices accordingly.

NOTE: Both office LAN networks must be in **different subnets** with the LAN-LAN application.
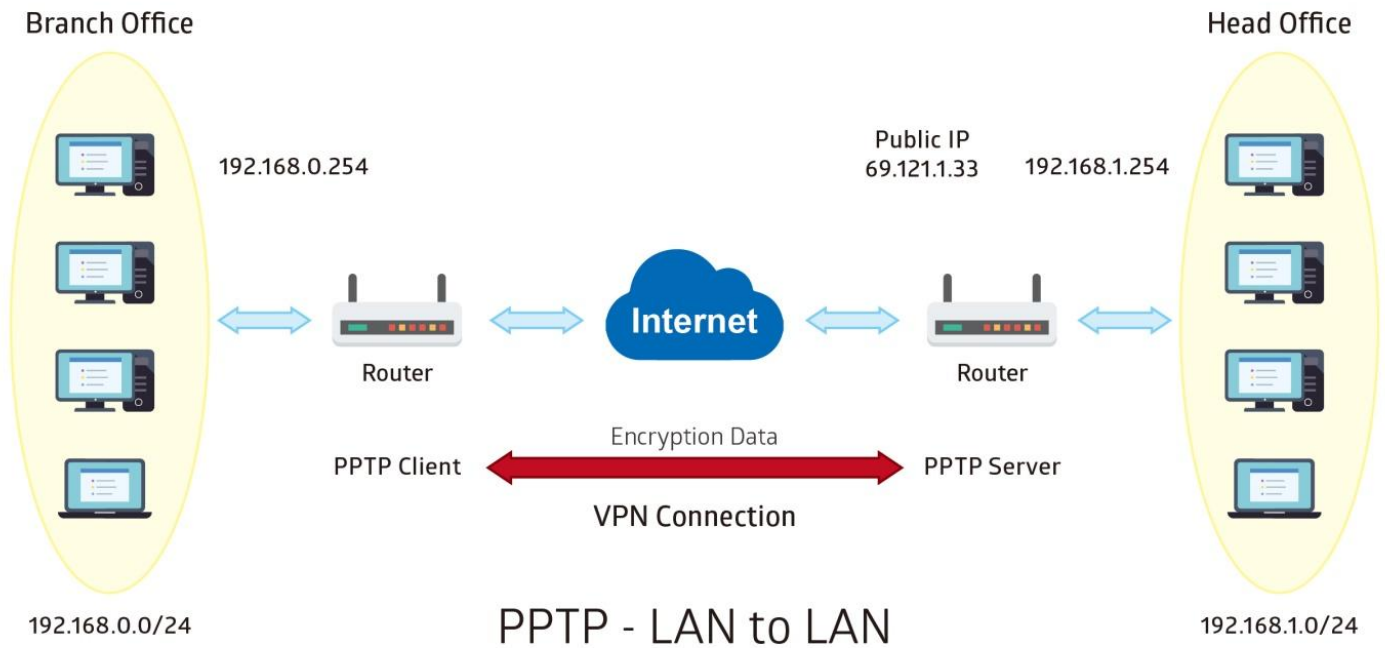
Configuring PPTP Server in the Headquarter office

The IP address 192.168.1.2 will be assigned to the router located in the branch office. Please make sure this IP is not used in the Headquarter office LAN.

Configuration Settings		Description
Connection Name	HS-LL	Assigned name to this tunnel/profile
Authentication Type	MS-CHAPv2	Authentication type
Username	test	Credential created for a PPTP client to dial-in to its local network.
Password	test	
Connection Type	LAN to LAN	LAN to LAN connection
Assigned IP	192.168.1.2	Local IP assigned to the dial-in client
Remote Network IP	129.168.0.0	Remote, Branch office, LAN network IP address and Netmask
Remote Network Netmask	255.255.255.0	

▼PPTP Server	
PPTP Server	⦿ Actived ◯ Deactived
Authentication Type	MS-CHAPv2 ⌄
Encryption Key Length	Auto ⌄
Encryption Mode	Allow Stateless and Statefull ⌄
CCP	⦿ Yes ◯ No
MS-DNS	192.168.1.254
Rule Index	1 ⌄
Connection Name	HS-LL
Active	⦿ Yes ◯ No
Username	test
Password	••••
Connection Type	LAN to LAN ⌄
Private IP Address assigned to Dial-in User	192.168.1.2
Remote Network IP Address	192.168.0.0
Remote Network Netmask	255.255.255.0

Save   Delete

PPTP Server Listing

Index	Connection Name	Active	Username	Connection Type	Assigned IP Address
1	HS-LL	Yes	test	Lan to Lan	192.168.1.2

Configuring PPTP Client in the Branch office

The IP address 69.1.121.33 is the Public IP address of the router located in Headquarter office.

Configuration Settings		Description
Connection Name	BC-LL	Assigned name to this tunnel/profile
Authentication Type	MS-CHAPv2	Authentication type
Username	test	Credential assigned from the Headquarter
Password	test	Server to dial-in.
Connection Type	LAN to LAN	LAN to LAN connection
Server IP	69.121.1.33	Headquarter Serve WAN IP address
Remote Network IP	129.168.1.0	Remote, Headquarter office, LAN network
Remote Network Netmask	255.255.255.0	IP address and Netmask

▼ **PPTP Client**

Rule Index	1 ▾
Connection Name	BC-LL
Active	⦿ Yes ○ No
Authentication Type	MS-CHAPv2 ▾
Encryption Key Length	Auto ▾
Encryption Mode	Allow Stateless or Statefull ▾
CCP	⦿ Yes ○ No
Username	test
Password	••••
Connection Type	LAN to LAN ▾
Server IP Address	69.121.1.33
Remote Network IP Address	192.168.1.0
Remote Network Netmask	255.255.255.0
Active as Default Route	☐ Enable

[Save] [Delete]

PPTP Client Listing

Index	Connection Name	Active	Username	Connection Type	Server IP Address
1	BC-LL	Yes	test	Lan to Lan	69.121.1.33

L2TP

L2TP, Layer 2 Tunneling Protocol is a tunneling protocol used to support virtual private networks (VPNs). It does not provide any encryption or confidentiality by itself; it relies on an encryption protocol that it passes within the tunnel to provide.

NOTE: 4 sessions for dial-in connections and 4 sessions for dial-out connections

Rule Index: The numeric rule indicator for L2TP. The maximum entry is up to 8 (4 dial-in and 4 dial-out profiles).

Connection Name: Enter a description for this connection/profile.

Active: To enable or disable this profile.

Connection Mode (Dial in)

Connection Mode: Select Dial In to operate as a L2TP server.

Authentication Type: Default in Chap/Pap (CHAP, Challenge Handshake Authentication Protocol. PAP, Password Authentication Protocol). If you want the router to determine the authentication type to use, or else manually specify PAP if you know which type the server is using (when acting as a client), or else the authentication type you want clients connecting to you to use (when acting as a server).

Username / Password (Server/Host): Enter the username / password for this profile.

Private IP Address Assigned to Dial-in User: The private IP to be assigned to dial-in user by L2TP

BEC MX-200(A) User Manual

server. The IP should be in the same subnet as local LAN, and should not be occupied.

Connection Mode (Dial out)

Connection Mode	Dial out ▼
Server IP Address	
Authentication Type	Chap/Pap ▼
Username	
Password	

Connection Mode: Choose Dial Out if you want your router to operate as a client (connecting to a remote L2TP Server, e.g., your office server).

Server IP Address: Enter the IP address of your VPN Server.

Authentication Type: Default is Chap/Pap (CHAP, Challenge Handshake Authentication Protocol. PAP, Password Authentication Protocol). If you want the router to determine the authentication type to use, or else manually specify PAP if you know which type the server is using (when acting as a client), or else the authentication type you want clients connecting to you to use (when acting as a server).

Username / Password (Client): Enter the username / password provide by the Server/Host.

Connection Type

▸ **Remote Access:** From a single user.

▸ **LAN to LAN:** Enter the peer network information, such as network address and Netmask.

Tunnel Authentication and Active

Tunnel Authentication	☐ Enable
Secret Password	
Local Host Name	
Remote Host Name	
Active as Default Route	☐ Enable

Tunnel Authentication: This enables router to authenticate both the L2TP remote and L2TP host. This is only valid when L2TP remote supports this feature.

Secret Password: The secure password length should be 16 characters which may include numbers and characters.

Local Host Name: Enter hostname of Local VPN device that is connected / established a VPN tunnel.

Remote Host Name: Enter hostname of remote VPN device. It is a tunnel identifier from the Remote VPN device matches with the Remote hostname provided. If remote hostname matches, tunnel will be connected; otherwise, it will be dropped.

Active as Default Route: Enabled to let the tunnel to be the default route for traffic, under this circumstance, all packets will be forwarded to this tunnel and routed to the next hop.

Click **Save** to apply settings.

Example: L2TP VPN – Remote Employee Dial-in to MX-200(A)

A remote worker establishes a L2TP VPN connection with the Headquarter office using Microsoft's VPN Adapter The router is installed in the Headquarter office, connected to a couple of PCs and Servers.

The input IP address 192.168.1.200 will be assigned to the remote worker. Please make sure this IP is not used in the Office LAN.

Configuration Settings		Description
Connection Name	HS-RA	Assigned name to this tunnel/profile
Connection Mode	Dial in	Operate as L2TP server
Authentication Type	Chap/Pap	Authentication type
Username	test	Credential from the device for remote
Password	test	client to dial-in to the network.
Assigned IP	192.168.1.200	An IP assigned to the dial in client
Connection Type	Remote Access	Remote access for dial in

Example: L2TP VPN – MX-200(A) Dial-out to a Server

A company's office establishes a L2TP VPN connection with a file server located at a separate location. The router is installed in the office, connected to a couple of PCs and Servers.
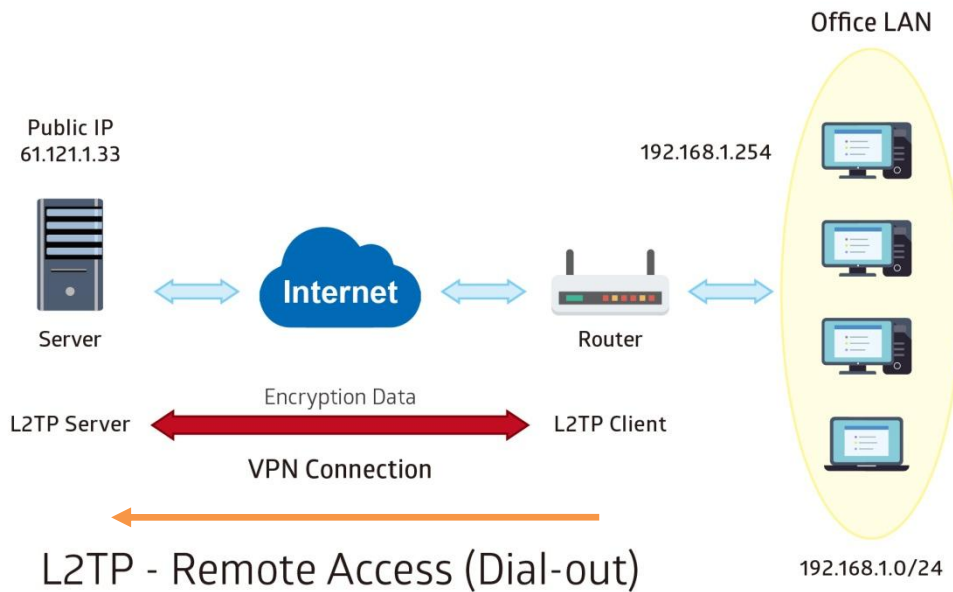
Item		Description
Connection Name	HC-RA	Assigned name to this tunnel/profile
Connection Mode	Dial out	Operate as L2TP client
Server IP	69.121.1.33	VPN server WAN IP address
Authentication Type	Chap/Pap	Authentication type
Username	test	Credential from the VPN Server for remote clients to dial-in to the network.
Password	test	
Connection Type	Remote Access	Remote access for dial out

Example: L2TP VPN – Network (LAN) to Network (LAN) Connection

The branch office establishes a L2TP VPN tunnel with Headquarter office to connect two private networks over the Internet. The routers are installed in the Headquarter office and branch office accordingly.

NOTE: Both office LAN networks must be in different subnets with the LAN-LAN application.

Configuring L2TP VPN Dial-in in the Headquarter office

The IP address 192.168.1.200 will be assigned to the router located in the branch office.

Item		Description
Connection Name	HS-LL	Assigned name to this tunnel/profile
Connection Mode	Dial in	Operate as L2TP server
Authentication Type	Chap/Pap	Authentication type
Username	Test	Credential for a PPTP client to dial-in to
Password	Test	the network.
Assigned IP	192.168.1.200	An IP assigned to the dial in client
Connection Type	LAN to LAN	LAN to LAN for dial in
Remote Network IP	129.168.0.0	Remote, Branch office, LAN network IP
Remote Network Netmask	255.255.255.0	address and Netmask

Configuring L2TP VPN Dial-out in the Branch office

The IP address 69.1.121.33 is the Public IP address of the router located in Headquarter office.

Item		Description
Connection Name	BC-LL	Assigned name to this tunnel/profile
Connection Mode	Dial out	Operate as L2TP client
Server IP	69.121.1.33	Dialed server IP
Authentication Type	Chap/Pap	Authentication type
Username	test	Credential from the PPTP server to dial-in
Password	test	to the network
Connection Type	LAN to LAN	LAN to LAN for dial out
Remote Network IP	129.168.1.0	Remote, Headquarter office, LAN network
Remote Network Netmask	255.255.255.0	IP address and Netmask

GRE Tunnel

Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocol packets inside virtual point-to-point links over an IP network.

NOTE: Up to 8 GRE tunnels supported.

GRE	
Rule Index	1 ∨
Connection Name	
Active	○ Yes ● No
Interface	EWAN(LAN1) ∨
Remote Gateway IP	0.0.0.0
Tunnel Local IP Address (Virtual Interface)	0.0.0.0
Tunnel Network Netmask (Virtual Interface)	0.0.0.0
Tunnel Remote IP Address (Virtual Interface)	0.0.0.0
Remote Network IP Address	0.0.0.0
Remote Network Netmask	0.0.0.0
Enable Keepalive	☐
Keepalive Retry Times	3
Keepalive Interval	5 Second(s)
MTU	1460
Active as Default Route	○ Yes ● No
IPSec	☐ Enable

Save   Delete

GRE Listing

Index	Connection Name	Active	Interface	Remote Gateway IP	Remote Network

Rule Index: The numeric rule indicator for GRE. The maximum entry is up to 8.

Connection Name: Enter a description for this connection/profile.

Active: Yes to activate this GRE profile.

Interface: Select a WAN interface to establish a tunnel with the remote VPN device.

Remote Gateway: Enter the remote GRE WAN IP address.

Tunnel Local IP Address & Remote IP address (Virtual Interface): Enter a virtual IP address for the local and peer network.

Tunnel Network Netmask (Virtual Interface): Enter the Netmask for this virtual interface.

NOTE: The virtual Local and Remote IP addresses must in **same subnet** and **cannot be existed or used** in both networks.

Remote Network IP Address Netmask: Enter remote LAN network IP address.

Remote Network Netmask: Enter remote LAN network Netmask.

Enable Keep-alive: Check the box to enable the keep-alive. The system will detect remote peer is still alive or lost. If no responses from the remote peer after certain times, **#-of-retry-time x interval**, the connection will get dropped.

Keep-alive Retry Times: Set the keep-alive retry times, default is 3.

Keep-alive Interval: Set the keep-alive Interval, unit in seconds. Default is 5 seconds.

Example: Keepalive retry time (3) x keepalive interval (5) = 15 seconds. If no responses for 15

seconds, GRE connection will get aborted.

MTU: Maximum Transmission Unit in byte. The size of the largest datagram (excluding media-specific headers) an IP attempts to send through the interface.

Active as Default Route: Select if to set the GRE tunnel as the default route.

IPSec: Click the checkbox to enable GRE tunnel over IPSec.

IPSec	☑ Enable
IKE Mode	Main ▼
IKE(IPSec) Local ID	Default (Local WAN IP) ▼
IKE(IPSec) Remote ID	Default (Remote Gateway IP) ▼
IKE(IPSec) Pre-Shared Key	

IKE Mode: IKE, Internet Key Exchange, is the mechanism to negotiate and exchange parameters and keys between IPSec peers to establish security associations (SA). Select Main or Aggressive mode.

IKE (IPSec) Local ID Type and **Remote ID Type:** When the mode of IKE is aggressive, Local and Remote peers can be identified by other IDs.

IKE (IPSec) Pre-Shared Key: This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

Click **Save** to apply settings.

Example: GRE VPN – Network (LAN) to Network (LAN) Connection

The branch office establishes a GRE VPN tunnel with Headquarter office to connect two private networks over the Internet. The routers are installed in the Headquarter office and branch office accordingly.

NOTE: Both office LAN networks must be in different subnets with the GRE VPN connection.
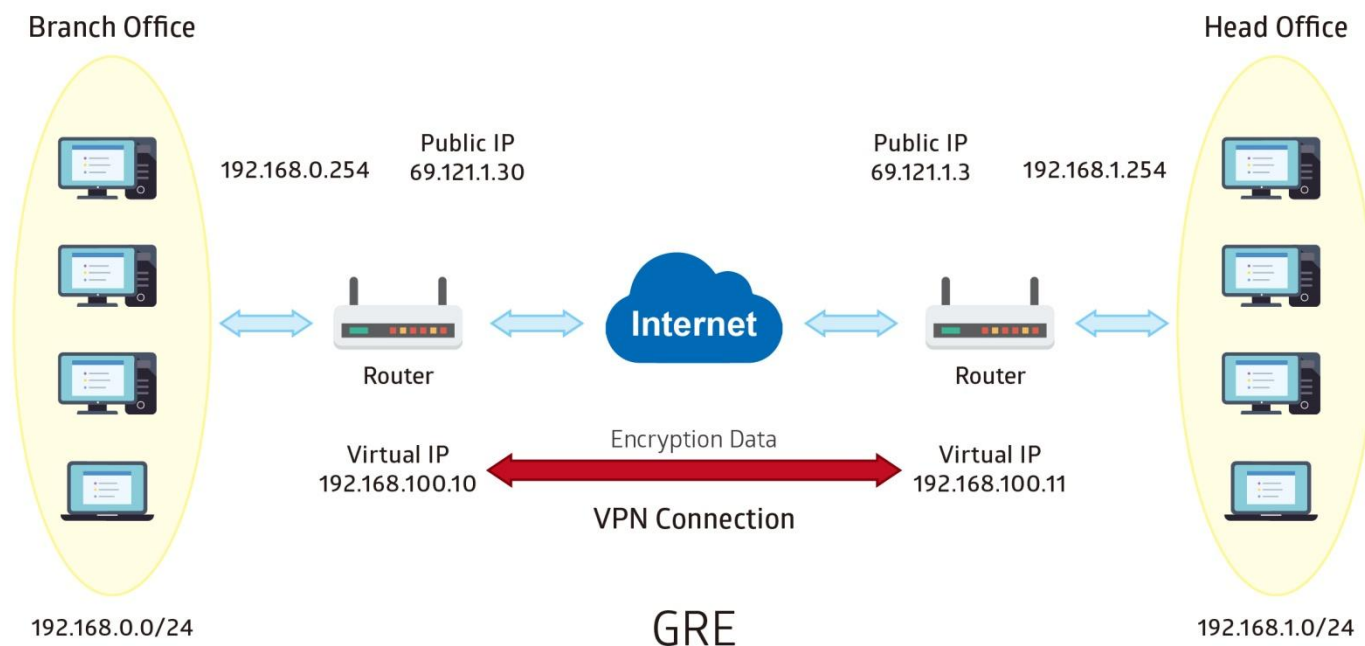
Configuring GRE connection in the Headquarter office

The IP address 69.1.121.30 is the Public IP address of the router located in branch office.

Item		Description
Connection Name	HS-LL	Assigned name to this tunnel/profile
Remote Gateway IP	69.121.1.30	WAN IP address of Branch office
Tunnel Local IP Address (Virtual Interface)	192.168.100.11	Local and remote virtual interface IP address must be in same Netmask.
Tunnel Remote IP Address (Virtual Interface)	192.168.100.10	
Tunnel Network Netmask (Virtual Interface)	255.255.255.0	Network Netmask of this virtual interface.
Remote Network IP/ Netmask	192.168.0.0/ 255.255.255.0	The remote, branch office, LAN network IP and Netmask.

Configuring GRE connection in the Branch office

The IP address 69.1.121.3 is the Public IP address of the router located in Headquarter office.

Item		Description
Connection Name	BC-LL	Assigned name to this tunnel/profile
Remote Gateway IP	69.121.1.3	WAN IP address of Headquarter office
Tunnel Local IP Address (Virtual Interface)	192.168.100.10	Local and remote virtual interface IP address must be in same Netmask.
Tunnel Remote IP Address (Virtual Interface)	192.168.100.11	
Tunnel Network Netmask (Virtual Interface)	255.255.255.0	Network Netmask of this virtual interface.
Remote Network IP/ Netmask	192.168.1.0/ 255.255.255.0	The remote, Headquarter office, LAN network IP and Netmask.

▼ GRE

Rule Index	1 ▼
Connection Name	BC-LL
Active	⦿ Yes ○ No
Interface	4G/LTE ▼
Remote Gateway IP	69.121.1.3
Tunnel Local IP Address (Virtual Interface)	192.168.100.10
Tunnel Network Netmask (Virtual Interface)	255.255.255.0
Tunnel Remote IP Address (Virtual Interface)	192.168.100.11
Remote Network IP Address	192.168.1.0
Remote Network Netmask	255.255.255.0
Enable Keepalive	☐
Keepalive Retry Times	3
Keepalive Interval	5 Second(s)
MTU	1460
Active as Default Route	○ Yes ⦿ No
IPSec	☐ Enable

[Save] [Delete]

GRE Listing

Index	Connection Name	Active	Interface	Remote Gateway IP	Remote Network
1	BC-LL	Yes	4G LTE	69.121.1.3	192.168.1.0/255.255.255.0

OpenVPN

OpenVPN is an open source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange. OpenVPN can run over User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) transports, multiplexing created SSL tunnels on a single TCP/UDP port. It is capable of traversing network address translation (NAT) and firewalls.

OpenVPN allows peers to authenticate each other using a pre-shared secret key, certificates, or username/password. Preshared secret key is the easiest, with certificate based being the most robust and feature-rich. It uses the OpenSSL encryption library extensively, allowing OpenVPN to use all the ciphers available in the OpenSSL package, as well as the SSLv3/TLSv1 protocol, and contains many security and control features.

It has integrated with OpenVPN package, allowing users to run OpenVPN in server or client mode from their network routers.

OpenVPN Server

NOTE: Up to 1 profile.

OpenVPN Server						
Rule Index	1 ∨					
Connection Name						
Active	○ Yes ● No					
Local Service Port	1194					
Tunnel Network (Virtual interface)						
IP Address		Netmask	255.255.255.0			
Local Access Range						
IP Address		Netmask	255.255.255.0			
Protocol	UDP ∨					
Local Certificate Index	Default ∨					
Trusted CA Index	Default ∨					
Cryptographic Suite						
Cipher	Default ∨	Hash	Default ∨			
Compression	Adaptive ∨					
Keepalive	☑ Enable	Interval	10	second(s)	Timeout	120 second(s)

Save   Delete

Rule Index: The numeric rule indicator for OpenVPN.

Connection Name: Enter a description for this connection/profile.

Active: Yes to activate this profile.

Local Service Port: Port 1194 is the default assigned port for OpenVPN

Tunnel Network (virtual Interface)

IP Address / Netmask: Enter a virtual IP address and Netmask for this tunnel.

NOTE: The virtual IP addresses **cannot be existed or used** in both networks.

Local Access Range

IP Address / Netmask: Enter local LAN network IP address and Netmask.

Protocol: OpenVPN can run over either UDP or TCP transports. Select the protocol.

Local Certificate / Trusted CA Index: OpenVPN mutually authenticate the server and client based on certificates and CA. Select a certificate and CA.

To import certificates and CAs, go to **Maintenance >> Certificate Management** to upload files. Otherwise, select **Default** certificate and CA.

Cryptographic Suite

Cipher: OpenVPN uses all the ciphers available in the OpenSSL package to encrypt both the data and channels. Select an encryption method.

Hash: To establish the integrity of the datagram and ensures it is not tampered with in transmission. There are options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1, SHA256). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

Compression: Choose **adaptive** to use the LZO compression library to compress the data stream.

Keepalive: Check the box to enable the keep-alive. The system will automatic send ping packet to remote peer to keep the tunnel active.

Interval: Set the keep-alive Interval, unit in seconds. Default is **10** seconds. Valid interval range is from **0 to 3600** seconds.

Timeout: Re-establish tunnel if no responses from peer network after timeout period expires. Default is 120 seconds.

Click **Save** to apply settings.

OpenVPN Client

OpenVPN client must match the VPN information / settings with the OpenVPN Server.

NOTE: Up to 4 tunnels supported.

Rule Index: The numeric rule indicator for OpenVPN. Maximum up to 4 profile/tunnels

Connection Name: Enter a description for this connection/profile.

Active: Yes to activate this profile.

Server IP Address or Domain Name: Enter OpenVPN Server's WAN IP address or Domain name.

Service Port: Port 1194 is the official assigned port number for OpenVPN

Active as Default Route: Choose **Yes** to let the OpenVPN tunnel/connection be the default route for traffic, under this circumstance, all outgoing packets will be forwarded to this tunnel and routed to the next hop.

Remote Subnet

IP Address / Netmask: Enter the LAN network IP address and Netmask of the OpenVPN Server.

Protocol: OpenVPN can run over either UDP or TCP transports. Select the protocol.

Local Certificate / Trusted CA Index: OpenVPN mutually authenticate the server and client based on certificates and CA. Select a certificate and CA.

To import certificates and CAs, go to **Maintenance >> Certificate Management** to upload files. Otherwise, select **Default** certificate and CA.

Cryptographic Suite

Cipher: OpenVPN uses all the ciphers available in the OpenSSL package to encrypt both the data and channels. Select an encryption method.

Hash: To establish the integrity of the datagram and ensures it is not tampered with in transmission. There are options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1, SHA256). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

Compression: Choose **adaptive** to use the LZO compression library to compress the data stream.

Keepalive: Check the box to enable the keep-alive. The system will automatic send ping packet to remote peer to keep the tunnel active.

Interval: Set the keep-alive Interval, unit in seconds. Default is **10** seconds. Valid interval range is from **0 to 3600** seconds.

Timeout: Re-establish tunnel if no responses from peer network after timeout period expires. Default is 120 seconds.

Click **Save** to apply settings.

Example: OpenVPN – Network (LAN) to Network (LAN) Connection

The Branch office establishes a tunnel with Headquarter office to connect two private networks over the OpenVPN.

NOTE: Both office LAN networks must be in different subnets with the GRE VPN connection.
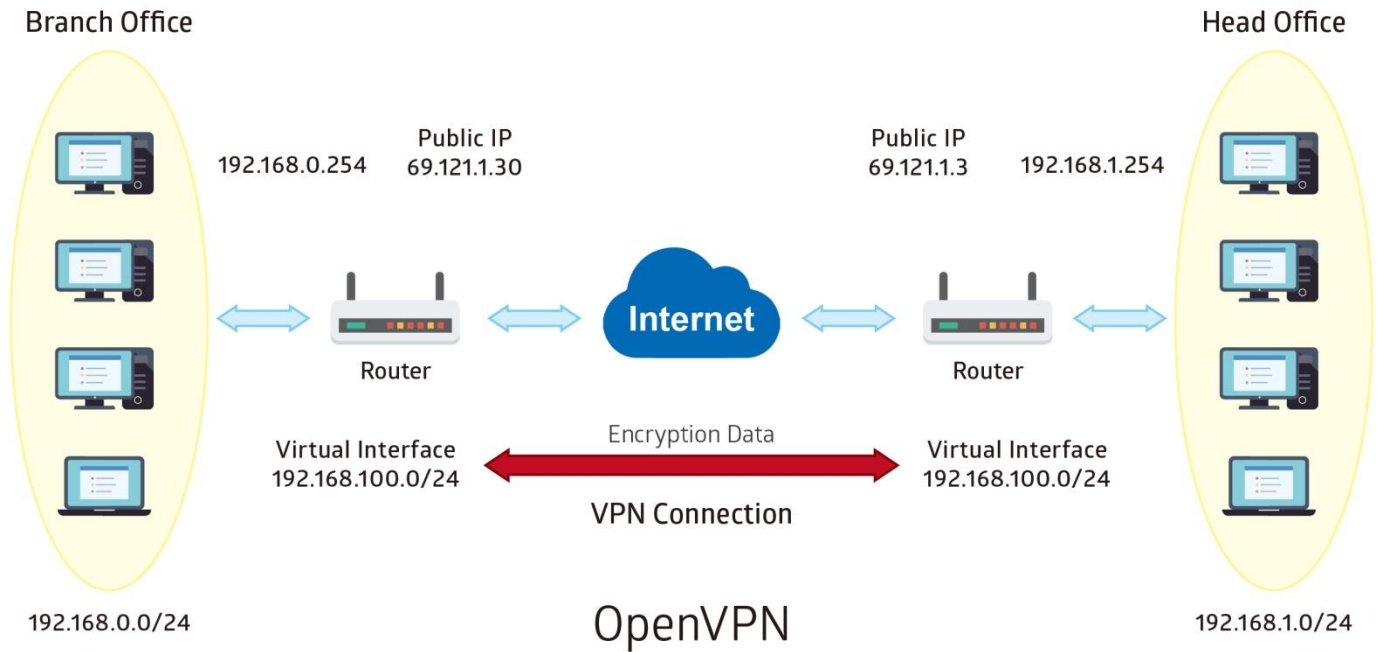
Configuring OpenVPN server in Headquarter office

The IP address 69.1.121.30 is the WAN IP address of the router located in the Branch office.

The OpenVPN tunnel network virtual interface is set to 192.168.100.0/24.

Item		Description
Connection Name	HS-LL	Assigned name to this tunnel/profile
Tunnel Network (Virtual Interface)	192.168.100.0/ 255.255.255.0	IP address & Netmask of the virtual tunnel.
Local Access Range	192.168.0.0/ 255.255.255.0	OpenVPN Server's local LAN network.

▼ OpenVPN Server

Rule Index	1 ▼
Connection Name	HS-LL
Active	⦿ Yes ○ No
Local Service Port	1194

Tunnel Network (Virtual interface)

IP Address	192.168.100.0	Netmask	255.255.255.0

Local Access Range

IP Address	192.168.0.0	Netmask	255.255.255.0
Protocol	UDP ▼		
Local Certificate Index	ServerLCA1 ▼		
Trusted CA Index	ServerTCA1 ▼		

Cryptographic Suite

Cipher	Default ▼	Hash	Default ▼
Compression	Adaptive ▼		
Keepalive	☑ Enable	Interval	10 second(s)	Timeout	120 second(s)

Save   Delete

Configuring OpenVPN client in Branch office

The IP address 69.1.121.3 is the WAN IP address of the router located in Headquarter office.

Item		Description
Connection Name	BC-LL	Assigned name to this tunnel/profile
Server IP Address	69.121.1.3	The WAN IP address of OpenVPN server.
Remote Subnet	192.168.0.0/ 255.255.255.0	Local LAN IP & Netmask of the Branch office

▼OpenVPN Client

Rule Index	1 ▾
Connection Name	BC-LL
Active	◉ Yes ○ No
Server IP Address or Domain Name	69.121.1.3 Port Number 1194
Active as Default Route	○ Yes ◉ No
Remote Subnet	
IP Address	192.168.0.0 Netmask 255.255.255.0
Protocol	UDP ▾
Local Certificate Index	ClientLCA1 ▾
Trusted CA Index	ClientTCA1 ▾
Cryptographic Suite	
Cipher	Default ▾ Hash Default ▾
Compression	Adaptive ▾
Keepalive	☑ Enable Interval 10 second(s) Timeout 120 second(s)

Save Delete

Access Management

Device Management

Device Host Name

Host Name: Enter the host name of the router. Default is **home.gateway**

Embedded Web Server

HTTP Port: It is the embedded web server (Web GUI) accessing port, default is **80**. It can be changed other port other than port 80, e.g. port 8080.

HTTPS Port: Similar to HTTP which is an unencrypted communication using port 80. HTTPS is encrypted by SSL using port 443 instead.

HTTPS Server Certificate Index: *HTTPS* known as HTTP-over-SSL tunnel protocol. Select a certificate to identify the system web server. When accessing to the web server (Web GUI), the browser will issue a warning page.

To import certificates, go to **Maintenance >> Certificate Management** to upload files. Otherwise, select **Default** certificate and CA.

Click **Save** to apply settings.

SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. The MX-200(A) serves as a SNMP agent that allows a manager station to manage and monitor the router through the network.

▼ SNMP	
SNMP	○ Activated ◉ Deactivated
Get Community	
Set Community	
Trap Manager IP	0.0.0.0
System Name	
System Location	
System Contact	
SNMPv3	
SNMPv3	○ Enable ◉ Disable
Username	
Access Permissions	Read Only ▼
Authentication Protocol	MD5 ▼
Authentication Key	(8~31 characters)
Privacy Protocol	DES ▼
Privacy Key	(8~31 characters)
Save	

SNMP: Activate to enable SNMP.

Get Community: Type the Get Community, which is the password for the incoming Get-and-GetNext requests from the management station.

Set Community: Type the Set Community, which is the password for incoming Set requests from the management station.

Trap Manager IP: Enter the IP of the server receiving the trap message (when some exception occurs) sent by this SNMP agent.

System Name / Location / Contact: String descriptions of the SNMP agent.

SNMPv3

SNMPv3: Enable to activate the SNMPv3.

User Name: Enter the name allowed to access the SNMP agent.

Access Permissions: Set the access permissions for the user; RO--read only and RW--read and writer.

Authentication Protocol: Select the authentication protocol, MD5 and SHA. SNMP agent can communicate with the manager station through authentication and encryption to secure the message exchange. Set the authentication and encryption information here and below.

Authentication Key: Set the authentication key, 8-31 characters.

Privacy Protocol: Select the privacy mode, DES and AES.

Privacy Key: Set the privacy key, 8-31 characters.

Click **Save** to apply settings.

Syslog

Use the Syslog to collect system event information to a remote log server.

▼ Syslog	
Remote System Log	○ Activated ● Deactivated
Server IP Address	0.0.0.0
Server UDP Port	514
Save	

Remote System Log: Select **Activated** to enable this feature

Server IP Address: Assign the remote log server IP address.

Server UDP Port: Assign the remote log server port, 514 is commonly used.

Click **Save** to apply settings.

Universal Plug & Play

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with control and data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems makes tasks such as port forwarding much easier by letting the application control the required settings, removing the need for the user to control advanced configuration of their device.

Both the user's Operating System and the relevant application must support UPnP in addition to the router.

▼ Universal Plug & Play	
UPnP	⦿ Activated ○ Deactivated
Auto-configured	○ Activated ⦿ Deactivated (by UPnP-enabled Application)
Save	

UPnP: Select this checkbox to activate UPnP. Be aware that anyone could use an UPnP application to open the web configuration's login screen without entering the MX-200(A)'s IP address

Auto-configured: Select this check box to allow UPnP-enabled applications to automatically configure the MX-200(A) so that they can communicate through the MX-200(A), for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.

Click **Save** to apply settings.

Dynamic DNS (DDNS)

The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your internet connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.

Here users can register different WAN interfaces with different DNS Providers.

If you do not have a DDNS account, please choose a DDNS Service Provider from the list then go to their website to create an account first.

▼Dynamic DNS	
Dynamic DNS	○ Activated ● Deactivated
Service Provider	www.dyndns.org (dynamic) ▼
My Host Name	
Username	
Password	
Wildcard support	○ Yes ● No
Period	25 Day(s) ▼
Save	

Dynamic DNS: Select this check box to activate Dynamic DNS.

Service Provider: Select from drop-down menu for the appropriate service provider, for example: www.dyndns.org.

My Host Name: Type the domain name assigned to your MX-200(A) by your Dynamic DNS provider.

Username / Password: Enter the user name and password of the account you created with this service provider.

Wildcard support: Select this check box to enable DYNDNS Wildcard.

Period: Set the time period on how often the MX-200(A) will update the DDNS server with your current external IP address.

Click **Save** to apply settings.

Example: How to register a DDNS account

If you do not have an account with Dynamic DNS, please go to www.dyndns.org to register an account first.

User *test1* register a Dynamic Domain Names in DDNS provider **http://www.dyndns.org/** .

DDNS: www.hometest.com using username/password test/test

Access Control

Access Control Listing allows you to determine which services/protocols can access the MX-200(A) interface from which computers. It is a management tool aimed to allow IPs (set in secure IP address) to access specified embedded applications (Web, etc., user can set) through some specified interface (LAN, WAN or both). User can have an elaborate understanding in the examples below.

The maximum number of entry is **16**.

▼ Access Control	
Access Control	⦿ Activated ○ Deactivated
Access Control Editing	
Rule Index	0 ▼
Active	⦿ Yes ○ No
Secure IP Address	0.0.0.0 ~ 0.0.0.0 (0.0.0.0 ~ 0.0.0.0 means all IPs)
Application	ALL ▼
Interface	LAN ▼
Save Delete	

Access Control Listing

Index	Active	Secure IP Address	Application	Interface
0	Yes	0.0.0.0-0.0.0.0	ALL	LAN
1	Yes	0.0.0.0-0.0.0.0	Ping	WAN

Access Control: Select whether to make Access Control function available.

Rule Index: The numeric rule indicator.

Active: Yes to activate the rule.

Secure IP Address: The default 0.0.0.0 allows any client to use this service to manage the MX-200(A). Type an IP address range to restrict access to the client(s) without a matching IP address.

Application: Choose a service that you want to all access to all the secure IP clients. The drop-down menu lists all the common used applications.

Interface: Select the access interface. Choices are **LAN**, **WAN** and **Both**.

Click **Save** to apply settings.

By default, the "Access Control" has **two default rules**.

Default Rule 1: (Index 1), a rule to allow only clients from LAN to have access to all embedded applications (Web, FTP, etc.). Under this situation, clients from WAN cannot access the router even from Ping.

Default Rule 2: (Index 2), an ACL rule to open Ping to WAN side.

Packet Filter

You can filter the packages by MAC address, IP address, Protocol, Port number and Application or URL.

❖ **Filter Type - IP & MAC Filter**

▼Packet Filter

Packet Filter	
Filter Type	IP & MAC Filter ▼

IP & MAC Filter Editing

Action	Black List ▼
Rule Index	1 ▼
Individual Active	○ Yes ● No
Interface	4G/LTE ▼
Direction	Both ▼
Type	IPv4 ▼
Source IP Address	0.0.0.0 (0.0.0.0 means Don't care)
Source Subnet Mask	0.0.0.0
Source Port Number	0 (0 means Don't care)
Destination IP Address	0.0.0.0 (0.0.0.0 means Don't care)
Destination Subnet Mask	0.0.0.0
Destination Port Number	0 (0 means Don't care)
DSCP	64 (Value Range:0~64, 64 means Don't care)
Protocol	Any ▼
Time Schedule	Always ▼

Save   Delete

IP & MAC Filter List

Index	Active	Interface	Direction	Source IP(IPv6) Address/Mask(Prefix)	Destination IP(IPv6) Address/Mask(Prefix)	Source MAC Address	Source Port	Destination Port	DSCP	Protocol

IP & MAC Filter Editing

Rule Index: The numeric rule indicator.

Individual Active: Yes to enable the rule.

Action: This is how to deal with the packets matching the rule. Allow please select White List or Black selecting Black List.

Interface: Select to determine which interface the rule will be applied to.

Direction: Select to determine whether the rule applies to outgoing packets, incoming packets or packets of both directions.

Type: Choose type of field you want to specify to monitor. Select "IPv4" for IPv4 address, port number and protocol. Select "IPv6" for IPv6 address, port number and protocol. Select "MAC" for MAC

address.

▸ **IPv4**

Source IP Address	0.0.0.0	(0.0.0.0 means Don't care)
Source Subnet Mask	0.0.0.0	
Source Port Number	0	(0 means Don't care)
Destination IP Address	0.0.0.0	(0.0.0.0 means Don't care)
Destination Subnet Mask	0.0.0.0	
Destination Port Number	0	(0 means Don't care)
DSCP	0	(Value Range:0~64, 64 means Don't care)
Protocol	TCP	

Source IP Address: The source IP address of packets to be monitored. 0.0.0.0 means "Don't care".

Source Subnet Mask: Enter the subnet mask of the source network.

Source Port Number: The source port number of packets to be monitored. 0 means "Don't care".

Destination IP Address: The destination IP address of packets to be monitored. 0.0.0.0 means "Don't care".

Destination Subnet Mask: Enter the subnet mask of the destination network.

Destination Port Number: This is the Port that defines the application. (E.g. HTTP is port 80.)

DSCP: DSCP: Differentiated Services Code Point, it is recommended that this option be configured by an advanced user or keep 0. (0 means Don't care.)

Protocol: Specify the packet type (TCP, UDP, ICMP, and ICMPv6) that the rule applies to.

▸ **IPv6**

Source IPv6 Address	0:0:0:0:0:0:0:0	(0:0:0:0:0:0:0:0 means Don't care)
Source IPv6 Prefix	32	
Source Port Number	0	(0 means Don't care)
Destination IPv6 Address	0:0:0:0:0:0:0:0	(0:0:0:0:0:0:0:0 means Don't care)
Destination IPv6 Prefix	32	
Destination Port Number	0	(0 means Don't care)
DSCP	0	(Value Range:0~64, 64 means Don't care)
Protocol	TCP	

Source IP (IPv6) Address/ Prefix: The source IP address or range of packets to be monitored.

Source Port Number: The source port number of packets to be monitored.

Destination IP (IPv6) Address/ Prefix: The destination subnet IP address.

Destination Port Number: This is the Port or Port Ranges that defines the application.

DSCP: show the set DSCP.

Protocol: It is the packet protocol type used by the application. Select either **TCP** or **UDP** or **ICMP or ICMPv6**

▸ **MAC**

Type	MAC ⌄
Source MAC Address	

Source MAC Address: show the MAC address of the rule applied.

Click **Save** to apply settings.

❖ **Filter Type- URL Filter**

URL Filter: Select **Activated** to enable URL Filter.

URL Filter Rule Index: The numeric rule indicator.

Individual Active: To give control to the specific URL access individually, for example, you want to prohibit access to www.yahoo.com, please first press Activated in "URL Filter" field, and also Yes in "Individual Active" field; if some time you want to allow access to this URL, you simply select No in individual active field. In a word, the command serves as a switch to the access of some specific URL with the filter on.

URL (Host): Specified URL which is prohibited from accessing.

Click **Save** to apply settings.

CWMP (TR-069)

CWMP, short for CPE WAN Management Protocol, also called TR069 is a Broadband Forum technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices. It defines an application layer protocol for remote management of end-user devices.

As a bidirectional SOAP/HTTP based protocol it can provides the communication between customer premises equipment (CPE) and Auto Configuration Server (ACS). It includes both a safe configuration and the control of other CPE management functions within an integrated framework. In the course of the booming broadband market, the number of different internet access possibilities grew as well (e.g. modems, routers, gateways, set-top box, VoIP-phones).At the same time the configuration of this equipment became more complicated –too complicated for end-users. For this reason, TR-069 was developed. It provides the possibility of auto configuration of the access types. Using TR-069 the terminals can get in contact with the Auto Configuration Servers (ACS) and establish the configuration automatically and let ACS configure CPE automatically.

▼ CWMP (TR-069)	
CWMP	○ Activated ● Deactivated
ACS Login Information	
URL	http://cpe.bectechnologies.com/comserver/node1/tr069
Username	testcpe
Password	ac5entry
Connection Request Information	
Path	
Username	conexant
Password	welcome
Periodic Inform Config	
Periodic Inform	● Activated ○ Deactivated
Interval	870
Bind Wan Interface	
Interface	Auto ▼
NATT Config	
NATT Server	
NATT Period	

Save

CWMP: Select activated to enable CWMP.

ACS Login Information

URL: Enter the ACS server login URL.

User Name: Specify the ACS User Name for ACS authentication to the connection from CPE.

Password: Enter the ACS server login password.

Connection Request Information

Path: Local path in HTTP URL for an ACS to make a Connection Request notification to the CPE.

Username: Username used to authenticate an ACS making a Connection Request to the CPE.

Password: Password used to authenticate an ACS making a Connection Request to the CPE.

Periodic Inform Config

Periodic Inform: Select Activated to authorize the router to send an Inform message to the ACS automatically.

Interval(s): Specify the inform interval time (sec) which CPE used to periodically send inform message to automatically connect to ACS. When the inform interval time arrives, the CPE will send inform message to automatically connect to ACS.

Bind WAN Interface

Interface: Specify any available or a single WAN interface to handle TR-069 requests.

NATT Config - This is a proprietary feature provided by BEC. May leave them in blank, no configuration is required.

NATT Server: By BEC administrator only.

NATT Period: By BEC administrator only.

Click **Save** to apply settings.

Parental Control

This feature provides Web content filtering offering safer and more reliable web surfing for users especially for parents to protect network security and control the contents for children at home.

To activate this feature, please log on to www.opendns.com to get an OpenDNS account first.

Parent Control Provider: Hosted by www.opendns.com

Parent Control: Enable the feature by clicking the **Activate**d

Host Name: It is the domain name of your OpenDNS. If you don't have one, please leave it blink.

Username / Password: Put down your OpenDNS account username and password

Click **Save** to apply settings.

BECentral Management

BECentral is a cloud based device management platform that provides operators with a comprehensive suite of services to manage devices in real-time.

▼BECentral Management	
BECentral Management	○ Activated ● Deactivated
BECentral Management URL	becentral.becloud.io
BECentral Management Port	48883
Organization ID	DEFAULT
Device Report Interval	480
Interface	ALL ▼
Save	

BECentral Management: Activate to enable the feature.

BECentral Management URL: Access path to the BECentral.

BECentral Management Port: Port listened by the BECentral.

Organization ID: Customer ID

Device Report Interval: Enter the interval time in seconds to send inform message periodically to the BECentral.

Interface: Specify any available or a single WAN interface to handle BECentral requests.

Maintenance

User Management

User Management provides the Administrator with the ability to grant access control and manage GUI login credentials for each user.

There are two access management levels, Administrator and User.

The default root account, Administrator (admin), has full access to all the features listed and ability to create other accounts with features to allow other users to access to. The User account is with limited access (specified by advanced users with admin account) to the GUI.

Total of **8** accounts can be created to grant access to manage the MX-200(A) via the web page.

❖ **Administrator Account**

admin/admin is the root/default account username and password.

NOTE: This username / password may vary by different Internet Service Providers.

Login using the Administrator account, you will have the full accessibility to manage & control your gateway device and can also create user accounts for others to control some of the open configuration settings.

▼ User Management	
User Account	
Index	1 ▾
Username	admin
New Password	•••••
Confirm Password	•••••
Save Delete	
User Account Listing	

Index	User Name
1	admin
2	user

User Setup

Index: The numeric account indicator. The maximum entry is up to 8 accounts.

User Name: Create account(s) user name for GUI management.

New Password: Enter a new password for this user account.

Confirmed Password: Re-enter the new password again; you must enter the password <u>exactly</u> the same as in the previous field

❖ **User Account**

user/user is the default user account username and password

NOTE: This username / password may vary by different Internet Service Providers.

User Management	
User Account	
Index	2 ▾
Username	user
New Password	••••
Confirm Password	••••
Web GUI Permission	
Guest Account	○ Enable ◉ Disable
Interface Setup	◉ Enable ○ Disable
Advanced Setup	◉ Enable ○ Disable
VPN Setup	◉ Enable ○ Disable
Access Management	◉ Enable ○ Disable
Maintenance	◉ Enable ○ Disable

Save   Delete

User Account Setup

Index #: The numeric account indicator. The maximum entry is up to 8.

Username: Create account(s) user name for GUI management.

New Password: Password for the user account.

Confirm Password: Re-enter the password.

Web GUI Permission

Guest Account: Enable to create this new guest account.

Interface Setup / Advanced Setup / VPN Setup / Access Management / Maintenance: Enable to grant this user access to these features.

When someone accesses to the MX-200(A) using this "user" account, he/she can only manage and configure the features that is pre-selected in **Web GUI Permission** for this account.

Click **Save** to apply settings.

Certificate Management

This feature is used for OpenVPN and HTTS Server authentication of the device using certificate. If the imported certificate doesn't match the authorized certificate with the Server then no access is allowed.

Local Certificate Listing			
Index	Certificate Name	Edit	Delete
1		📝	❌
2		📝	❌
Trusted CA Listing			
Index	Certificate Name	Edit	Delete
1		📝	❌
2		📝	❌

Edit: Click 📝 (Edit) to import a certificate.

Delete: Click ❌ (Delete) to remove the certificate from the list.

Local Certificate Listing

▼Local Certificate	
Index	1 ▼
Certificate Name	
	☐ PKCS12
Certificate File	Choose File No file chosen Upload (Please upload Certificate File.)
Private Key File	Choose File No file chosen Upload (Please upload Private Key File.)
Password	•••••
After clicked "Upload", please wait for 5 seconds and then click "Apply".	
Save Back	

Index #: The numeric account indicator. The maximum entry is up to 2.

Certificate Name: Description of the certificate.

PKCS12: Every certificate is accompanied by a private key. Upload both files if PKCS is disabled. Enable PKCS12 to put Certificate & Private Key in the same file, like *.p12, *.pfx.

Certificate File: Browse to locate the target certificate file on PC before uploading it.

Private Key File: Browse to locate the target file on PC before uploading it. If PKCS enabled, please ignore this setting.

Password: Enter the password if any, which is used to protect the private key. Otherwise, leave it empty.

Click **Apply** to save settings.

Trusted CA Listing

Trusted CA	
Index	1 ▾
CA Name	
CA Certificate File	Choose File No file chosen Upload (Please upload CA Certificate File.)
After clicked "Upload", please wait for 5 seconds and then click "Apply".	
Apply Back	

Index #: The numeric account indicator. The maximum entry is up to 2.

CA Name: Description of the CA.

CA Certificate File: Browse to locate the target certificate file on PC before uploading it.

Click **Apply** to save settings.

Time Zone

With default, MX-200(A) does not contain the correct local time and date.

There are several options to setup, maintain, and configure current local time/date on the MX-200(A). If you plan to use **Time Schedule** feature, it is extremely important you set up the Time Zone correctly.

▼ Time Zone	
Current Date/Time	N/A (Can't find NTP server)
Time Synchronization	
Synchronize time with	◉ NTP Server ○ PC's Clock ○ Manually
Time Zone	(GMT-06:00) Central Time (US & Canada), Maxico City, Saskatchewan ▾
Daylight Saving	○ Enabled ◉ Disabled
NTP Server Address	0.0.0.0 (0.0.0.0: Default Value)
Save	

Synchronize time with: Select the methods to synchronize the time.

‣ **NTP Server automatically:** To synchronize time with the SNTP servers to get the current time from an SNTP server outside your network then choose your local time zone. After a successful connection to the Internet, MX-200(A) will retrieve the correct local time from the SNTP server this is specified.

‣ **PC's Clock:** To synchronize time with the PC's clock.

‣ **Manually:** Select this to enter the SNMP server IP address manually.

◆ **Date:** Month / Date / Year. Month – 1 ~ 12 (January ~ December).

◆ **Time:** Hour: Minute: Second

Time Zone: Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).

Daylight Saving: Select this option if you use daylight savings time.

NTP Server Address: Enter the IP address of your time server. Check with your ISP/network administrator if you are unsure of this information.

Click **Save** to apply settings.

Firmware & Configuration

Firmware is the software that controls the hardware and provides all functionalities which are available in the GUI. This software may be improved and/or modified; your MX-200(A) provides an easy way to update the code to take advantage of the changes. .

To upgrade the firmware of the MX-200(A), you should download or copy the firmware to your local environment first. Click **"Choose File"** to specify the path of the firmware file. Then, click **"Upgrade"** to start upgrading process. After completing the firmware upgrade, the MX-200(A) will automatically restart and run the new firmware.

▼Firmware & Configuraiton	
Upgrade	● Firmware ○ Configuration
System Restart with	● Current Settings ○ Factory Default Settings
File	[Choose File] No file chosen
Backup Configuration	[Backup]
Status	
It might take several minutes, don't power off it during upgrading. Device will restart after the upgrade.	
[Upgrade]	

Upgrade: Choose Firmware or Configuration you want to update.

System Restart with:

▶ **Current Settings:** Restart the device with the current settings automatically when finishing upgrading.

▶ **Factory Default Settings:** Restart the device with factory default settings automatically when finishing upgrading.

File: Type in the location of the file you want to upload in this field or click **Browse** to find it.

Choose File: Click **"Choose File"** to find the configuration file or firmware file you want to upload. Remember that you must extract / decompress / unzip the .zip files before you can upload them.

Backup Configuration: Click **Backup** button to back up the current running configuration file and save it to your computer in the event that you need this configuration file to be restored back to your MX-200(A) device when making false configurations and want to restore to the original settings.

Upgrade: Click **"Upgrade"** to begin the upload process. This process may take up to two minutes.

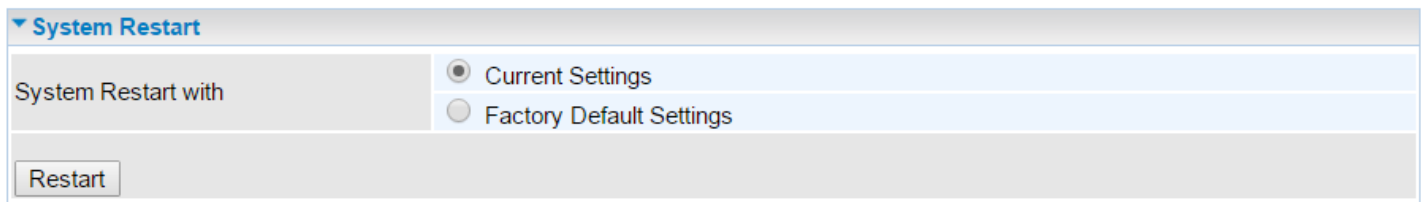| ▼Firmware Upgrade	
File upload succeeded, starting flash erasing and programming!!	
Progress	■■■
Percent	15 %

DO NOT turn off or power cycle the device while firmware upgrading is still in process.

Improper operation could damage your MX-200(A).

System Restart

Click **System Restart** with option **Current Settings** to reboot your router.

If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select **Factory Default Settings** to restore to factory default settings.

You may also restore your router to factory settings by holding the small Reset pinhole button on the back of your router in about more than 6s seconds whilst the router is turned on.

Auto Reboot

Schedule an automatic reboot for your MX-200(A) to ensure proper operation and best performance.

This reboot will only reboot with current configuration settings and not overwrite any existing settings.

Click **Save** to apply settings

Example: Schedule MX-200(A) to reboot at 10:00pm (22:00) every weekday (Monday thru Friday) and reboot at 9:00am on Saturday and Sunday.

Diagnostics Tool

The Diagnostic Test page shows the test results for the connectivity of the physical layer and protocol layer for both LAN and WAN sides.

3G/4G-LTE / EWAN (LAN1)

Ping other IP Address: Click **Yes** if you wish to ping other IP address rather than google.com

Click **START** to begin to diagnose the connection.

Trace Route is to display how many hops (also view the exact hops) the packet of data has to take to get to the destination.

Click **Yes**, enter the IP address or domain then **Start Trace Route**.

IP Address or Domain: Set the destination host (IP, domain name) to be traced.

Max TTL value: Set the max Time to live (TTL) value.

Shown as we "trace" www.billion.com below.

```
▼Trace www.billion.com

traceroute to www.billion.com (125.227.205.188), 16 hops max, 60 byte packets
 1  172.16.1.254 (172.16.1.254)  0.472 ms  0.488 ms  0.643 ms
 2  122.96.153.233 (122.96.153.233)  7.354 ms  7.517 ms  7.704 ms
 3  221.6.12.69 (221.6.12.69)  7.921 ms  8.108 ms  8.256 ms
 4  221.6.1.253 (221.6.1.253)  8.392 ms  8.544 ms *
 5  219.158.99.245 (219.158.99.245)  36.110 ms  36.839 ms  37.001 ms
 6  * * *
 7  * * 219.158.103.26 (219.158.103.26)  40.731 ms
 8  211.72.233.194 (211.72.233.194)  65.969 ms  66.040 ms  66.019 ms
 9  220.128.6.126 (220.128.6.126)  61.726 ms  61.831 ms  61.960 ms
10  220.128.11.170 (220.128.11.170)  61.543 ms  61.583 ms  65.127 ms
11  220.128.17.85 (220.128.17.85)  63.436 ms  62.133 ms  65.862 ms
12  220.128.17.229 (220.128.17.229)  64.695 ms  64.849 ms  65.063 ms
13  168.95.229.145 (168.95.229.145)  61.915 ms  60.715 ms  60.825 ms
14  * * *
15  * * *
16  * * *
```

LAN

▼Diagnostic Tool	
WAN Interface	LAN ▼
Testing Ethernet LAN Connection	**PASS**
Ping other IP Address or Domain ◉ Yes ○ No	**Skipped**
IP Address or Domain	N/A

Start

Ping other IP Address: Click **Yes** to ping any desired IP address or a domain.

Click **START** to begin to diagnose the connection.

Chapter 5: Troubleshooting

If your MX-200(A) is not functioning properly, you can refer to this chapter for simple troubleshooting before contacting your service provider support. This can save you time and effort but if symptoms persist, consult your service provider.

Problems with the Router

Problem	Suggested Action
None of the LEDs is on when you turn on the router	Check the connection between the router and the adapter. If the problem persists, most likely it is due to the malfunction of your hardware. Please contact your service provider or BEC for technical support.
You have forgotten your login username or password	Try the default username "admin" and password "admin". If this fails, you can restore your router to its factory settings by pressing the reset button on the device rear side.

Problem with LAN Interface

Problem	Suggested Action
Cannot PING any PC on LAN	Check the Ethernet LEDs on the front panel. The LED should be on for the port that has a PC connected. If it does not lit, check to see if the cable between your router and the PC is properly connected. Make sure you have first uninstalled your firewall program before troubleshooting.
	Verify that the IP address and the subnet mask are consistent for both the router and the workstations.

Recovery Procedures

Problem	Suggested Action
1. The front LEDs display incorrectly upgrade **2. Still cannot access to the router management interface after pressing the RESET button.** **3. Software / Firmware upgrade failure**	Before starting recovery process, please configure the IP address of the PC as 192.168.1.100 and proceed with the following step-by-step guide. 1. Power the router off. 2. Press reset button and power on the router, once the Power lights Red, keeping press reset button over 6 seconds. 3. Internet LED flashes Green, router entering recovery procedure and router's IP will reset to Emergency IP address (Say 192.168.1.1). 4. Open browser and access http://192.168.1.1 to upload the firmware. 5. Internet LED lit Red, and router starts to write firmware into flash. Please DO NOT power off the router at this step. 6. Internet LED lit Green when successfully upgrade firmware. 7. Power cycle off/on the MX-200(A)

Federal Communication Commission Interference Statement

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

* Reorient or relocate the receiving antenna.

* Increase the separation between the equipment and receiver.

* Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

* Consult the dealer or an experienced radio/TV technician for help.

FCC Caution:

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

(1) This device may not cause harmful interference

(2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. . This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

Co-location statement

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

V0141160