User ManualF

BEC MX-210NP-R17AF

4G/LTE Broadband Router with PoE

Last revised: J, 2019
Version release: v1.01

Copyright Notice

Copyright@ 2017 BEC Technologies Inc. All rights reserved.

BEC Technologies reserves the right to change and make improvement to this manual at any time without prior notice.

No part of this document may be reproduced, copied, transmitted in any form or by any means without prior written permission from BEC Technologies, Inc.

Support Contact Information

Contact Support: http://bectechnologies.net/support/.

Telephone: +1 972 422 0877

TABLE OF CONTENTS

COPYRIGHT NOTICE 1

SUPPORT CONTACT INFORMATION 1

CHAPTER 1: INTRODUCTION 1

INTRODUCTION TO YOUR ROUTER.....1

FEATURES & SPECIFICATIONS 3

HARDWARE SPECIFICATIONS 5

CHAPTER 2: PRODUCT OVERVIEW.....6

IMPORTANT NOTE FOR USING THIS ROUTER 6

PACKAGE CONTENTS.....6

DEVICE DESCRIPTION 7

Front Panel LEDs.....7

Rear Panel Connectors 8

SYSTEM RECOVERY PROCEDURES.....9

CABLING 9

CHAPTER 3: BASIC INSTALLATION 10

NETWORK CONFIGURATION – IPV4..... 11

Configuring PC in Windows 10 (IPv4) 11

Configuring PC in Windows 7/8 (IPv4).....13

Configuring PC in Windows Vista (IPv4) 15

NETWORK CONFIGURATION – IPV6..... 17

Configuring PC in Windows 10 (IPv6) 17

Configuring PC in Windows 7/8 (IPv6).....19

Configuring PC in Windows Vista (IPv6) 21

DEFAULT SETTINGS 23

CHAPTER 4: DEVICE CONFIGURATION 24

LOGIN TO YOUR DEVICE **24**

STATUS **26**

Device Info 26
System Status 28
System Log 28
4G/LTE Status 29
Wireless Status 31
Statistics 32
DHCP Table 36
ARP Table 36
VRRP Status 36

QUICK START **37**

DEVICE CONFIGURATION **40**

Interface Setup 40
Internet *40*
LAN *48*
Wireless *52*
Wireless MAC Filter *56*
Loopback *57*
Dual WAN 58
General Setting *58*
Outbound Load Balance *62*
Protocol Binding *63*
Advanced Setup 65
Firewall *65*
Routing *66*
NAT *67*
VRRP *72*
Static DNS *73*
QoS *74*
Time Schedule *76*
Mail Alert *77*
Access Management 78
Device Management *78*
SNMP *79*
Syslog *81*
Universal Plug & Play *82*
Dynamic DNS (DDNS) *83*

Access Control *85*
Packet Filter *87*
CWMP (TR-069) *91*
Parental Control *93*
BECentral Management *94*
Maintenance 95
User Management *95*
Certificate Management *97*
Time Zone *99*
Firmware & Configuration *100*
System Restart *101*
Auto Reboot *102*
Diagnostics Tool *103*

CHAPTER 5: TROUBLESHOOTING 106

Problems with the Router 106
Problem with LAN Interface 106
Recovery Procedures 107

APPENDIX: PRODUCT SUPPORT & CONTACT 108

CHAPTER 1: INTRODUCTION

Introduction to your Router

The BEC MX-210NP-R17AF 4G/LTE 11n with PoE Router is a compact, affordable and high-performance fixed 4G/LTE Router incorporated 11n technology and offers flexible options such as dual-WAN failover by seamless connecting to other Internet Service Provider to avert internet downtown, redundant power source for safe & quick power installation via one of the versatile LAN/PoE-PD ports and secure network connection and data privacy with VPN encryption capabilities to provide a reliable and cost-effective alternative solution for business continuity.

4G/LTE Mobility

The MX-210NP-R17AF is a classic 4G/LTE router with dual WAN interfaces for redundancy or seamless failover between mobile carrier network and the wireline, an interchangeable Gigabit Ethernet LAN/WAN, to ensure continuous Internet connectivity.

Seamless Wi-Fi Coverage

The MX-210NP-R17AF integrates a 802.11n access point supporting data rates of up to 300Mbps. Security functionality includes: WEP 64/128 bit, WPA, WPA2 (PSK, TKIP and AES, 802.1X, SSID broadcast disable and wireless MAC address filtering and MSSID with Client Isolation to enhance the level of transmission security and access control over the Wireless LAN. The router also supports the Wi-Fi Protected Setup (WPS) standard, allowing users to establish a secure wireless network by simply pushing a button. If the network requires wider coverage, the built-in Wireless Distribution System (WDS) repeater function allows users to expand the wireless network without the need for anyexternal wires or cables.

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.

24/7 Cloud Management and Network Visibility

Remote monitoring, management and control of devices in real-time is essential for IoT networking devices, M2M and critical applications. The BECentral®, BEC's Cloud Based Remote Management, is a comprehensive device management platform designed to minimize deployment, lower support expenses and maximize the operational efficiency and profitability of the operator.

Features & Specifications

- 4G/LTE and/or Ethernet IP broadband connectivity
- High performance SX antenna for increased coverage, signal reception and efficiency
- Versatile Gigabit LAN & Ethernet WAN (GbE WAN) for Cable/Fiber/xDSL high WAN throughput
- Verstalile Gigabit LAN & PoE
- 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

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)

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
- WAN: Cellular 4G/LTE (and/or ETH WAN Optional)
- Ethernet LAN: 2-port 10/100/1000Mbps, auto-crossover (MDI/ MDI-X) switch
- SIM Card: One (1) slot
- Reset Button
- Power Source: DC or PoE
- LED Indicators: Power / Internet / LTE / Ethernet

Physical Specifications

- Dimensions (W*H*D): 5.19" x 1.38" x 3.71" (132mm x 35mm x 94mm)

CHAPTER 2: PRODUCT OVERVIEW

Important Note for Using This Router

Warning

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

Do not use the same power source for the MX-210NP-R17AF on other equipment.

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.

Attention

- ✓ 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.

Package Contents

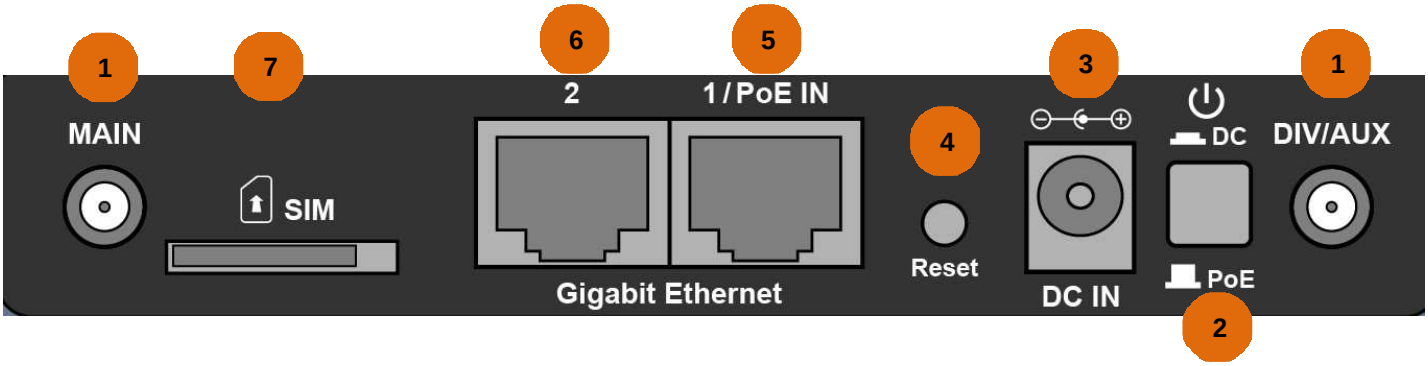
- ✓ BEC MX-210NP-R17AF Router * 1
- ✓ Quick Installation Guide * 1
- ✓ RJ-45 Ethernet cable *1
- ✓ DC Power Adapter, 12V 1.2A* 1

Device Description

Front Panel LEDs

LED	STATUS	DESCRIPTION
Power	Green	System is up and ready
	Red	Boot failure
Ethernet Port LAN 1 ~ 2	Green	Transmission speed is at Gigabit speed (1000Mbps)
	Orange	Transmission speed is at 10/100Mbps
	Blinking	Data being transmitted/received
Wireless	Green	Wireless connection established
	Green blinking	Data being transmitted / received
	Orange	WPS configuration is in progress
LTE (Received Signal Strength Indicator)	Green	RSSI greater than -69 dBm. Excellent signal condition
	Green Flashing quickly	RSSI from -81 to -69 dBm. Good signal condition
	Orange Flashing quickly	RSSI from -99 to -81 dBm. Fair signal condition.
	Orange Flashing slowly	RSSI less than -99 dBm. Poor signal condition.
	Orange	No signal and the cellular module is in service
	Off	No LTE module or LTE module fails
	Green & Orange	MX-210NP-R17AF is either in debug mode or in upgrading firmwere process
Internet	Green	IP address has received, and traffic is passing thru the device.
	Red	IP address request has failed.
	Off	MX-210NP-R17AF is either in bridged mode or WAN connection not ready.

Rear Panel Connectors



INTERFACE		MEANING
1	**4G/LTE Antenna Connectors (Main/Aux)**	SMA female connectors. Manually screw the cellular antennas tight to the female connectors. Connect to **Main** if decide to use one antenna instead of two.
2	**Power Source**	Power ON/OFF switch **(1) <u>with Power Switch ON:</u>** power up by the supplied DC power adapter **(2) <u>with Power Switch OFF:</u>** power up by the PoE battery unit
3	**Power Jack (DC IN)**	Connect the supplied Power Adapter to this jack.
4	**Rest**	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)
5	**Gigabit Ethernet (LAN 1 / PoE)**	**Ethernet LAN**: Connected to an Gigabit (1000Mbps) Ethernet device **Ethernet PoE**: Connect with a 802.3at Gb PoE injector to provide power to the MX-210NP-R17AF
6	**Gigabit Ethernet (LAN 1 / EWAN)**	**Ethernet LAN**: Connected to an Gigabit (1000Mbps) Ethernet device **Ethernet WAN**: Software configurable in the GUI. Connected with a broadband connection device
7	**SIM Card Slot**	Insert the mini SIM card (2FF) with the gold contact facing down. Push the mini SIM card (2FF) inwards to eject it * Power off the MX-210NP-R17AF before inserting or removing the SIM card(s)

System Recovery Procedures

The purpose is to allow users to restore the MX-210NP-R17AF 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-210NP-R17AF

2.1 Power off your MX-210NP-R17AF

2.2 Power on the MX-210NP-R17AF while pushing the RESET button with a small pointed object (such as paper clip, needle, toothpick, 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-210NP-R17AF

With INTERNET light flashes green, MX-210NP-R17AF 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-210NP-R17AF 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 MMX-210NP-R17AF

3.4 INTERNET LED turns green after the Firmware upgrade completed

3.5 Power cycle on & off to regain access to the MX-210NP-R17AF

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. Check your PC's network components first. 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.

Attention

Any TCP/IP capable workstation can be used to communicate with or through the MX-210NP-R17AF. To configure other types of workstations, please consult the manufacturer's documentation.

Network Configuration – IPv4

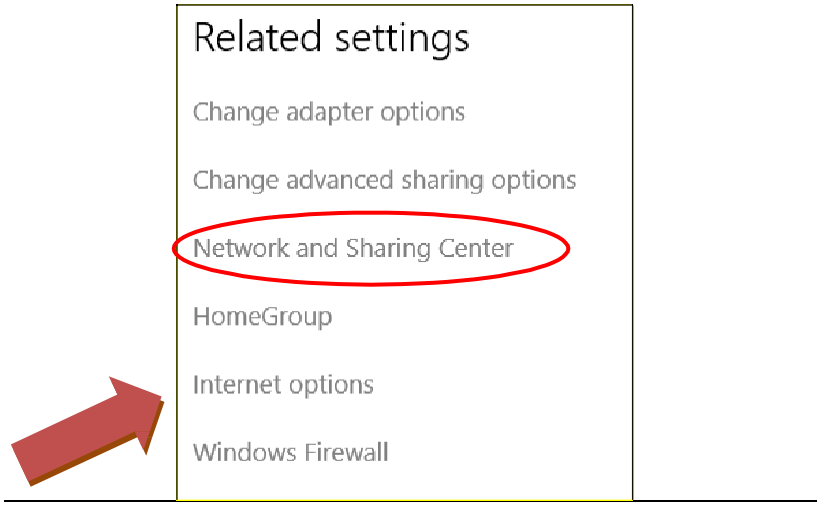
Configuring PC in Windows 10 (IPv4)

1. Click .

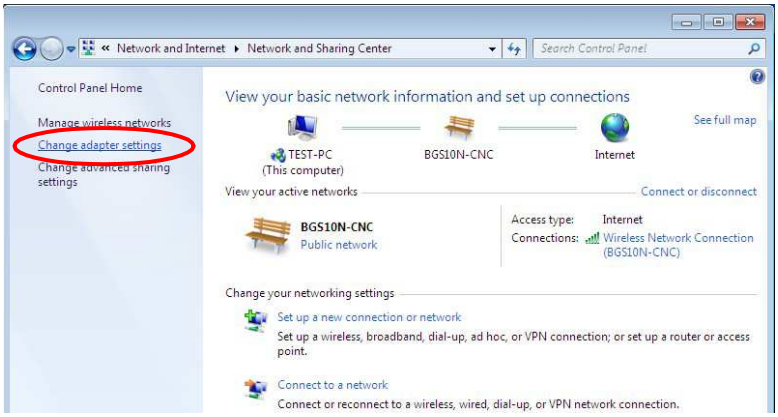
2. Click Settings

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

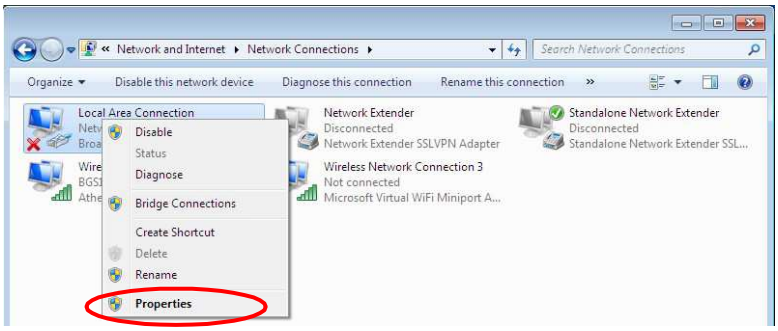
4. Under **Related settings,** select **Network and Sharing Center**



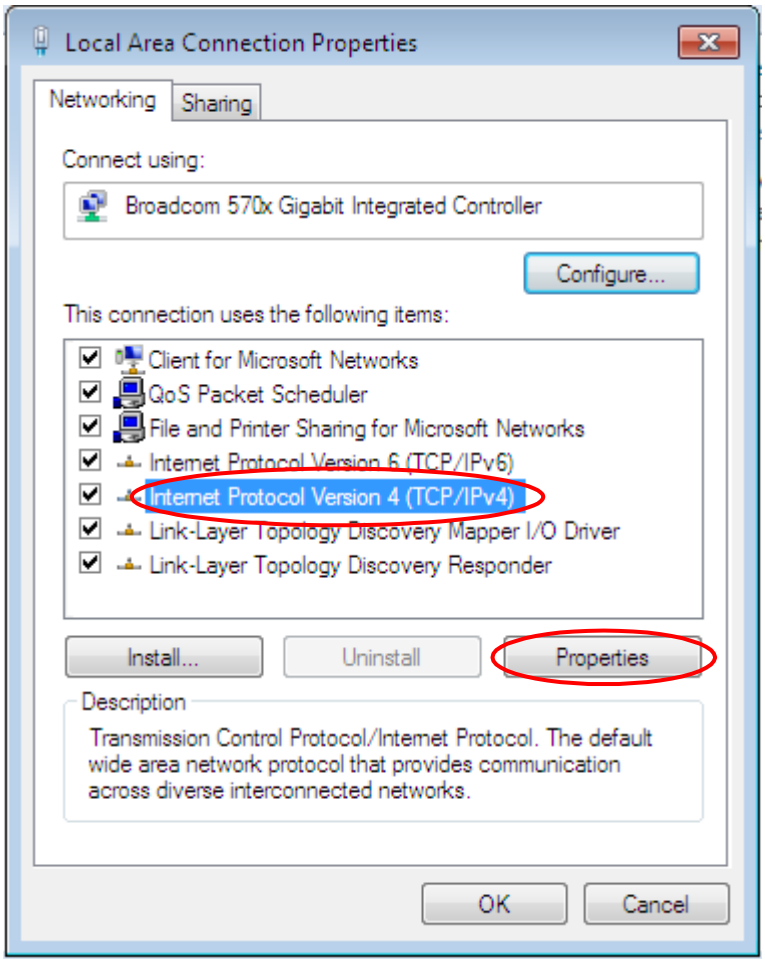
5. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



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

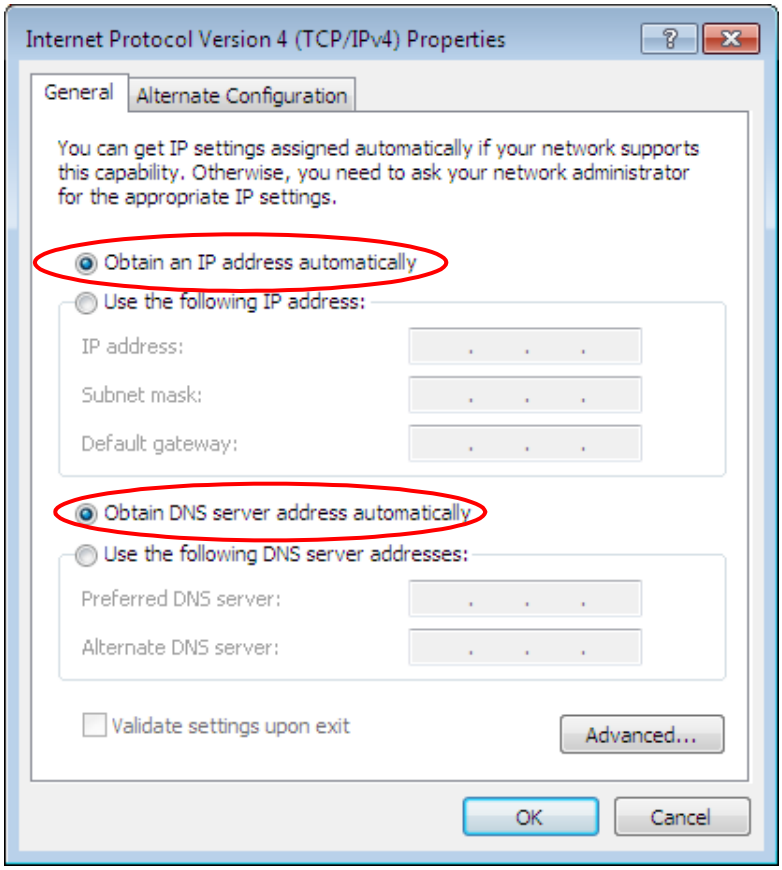


7. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.



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.

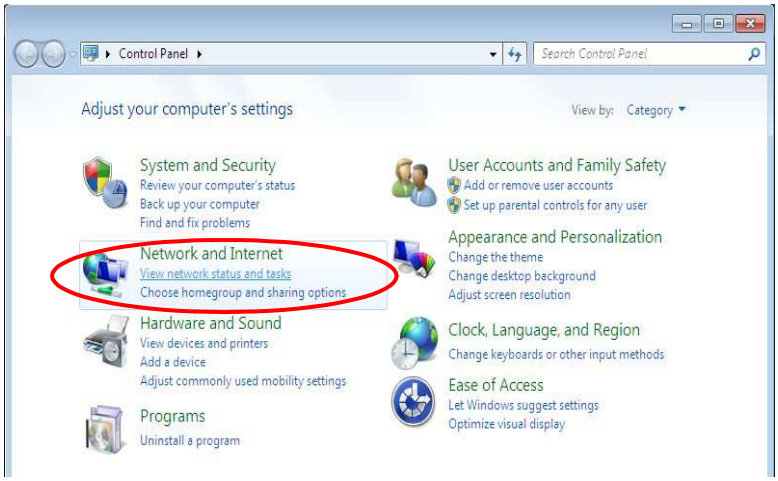
9. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



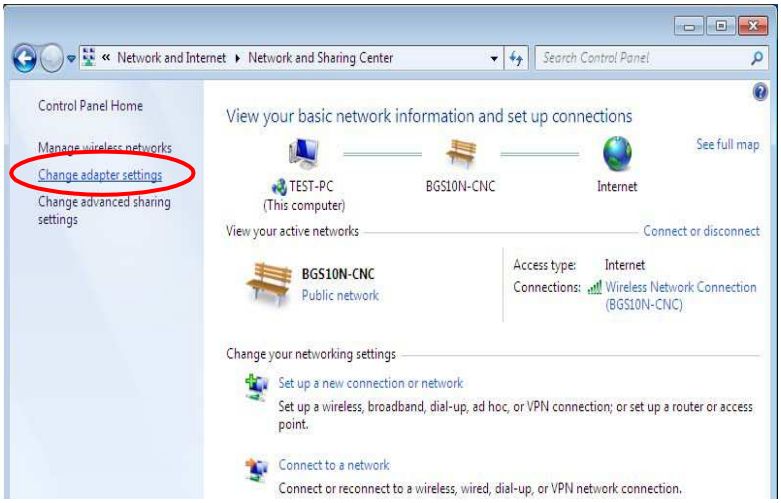
Configuring PC in Windows 7/8 (IPv4)

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

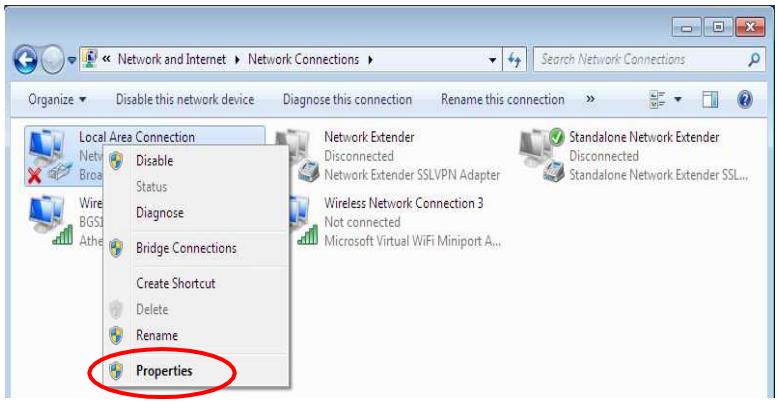
2. Then click on **Network and Internet**.



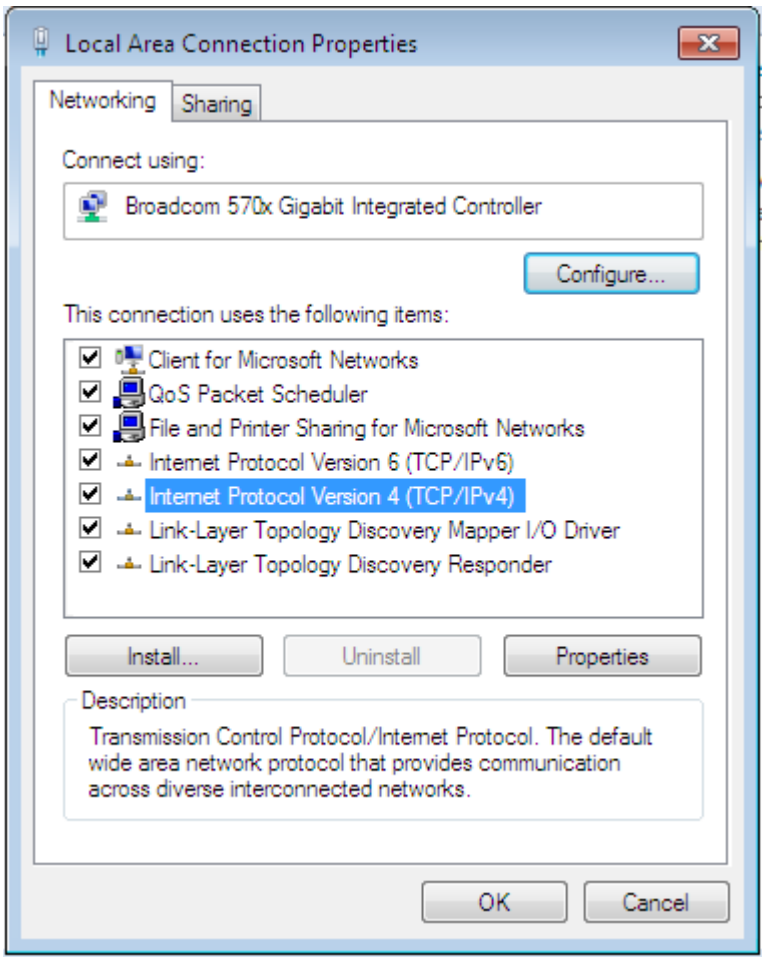
3. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



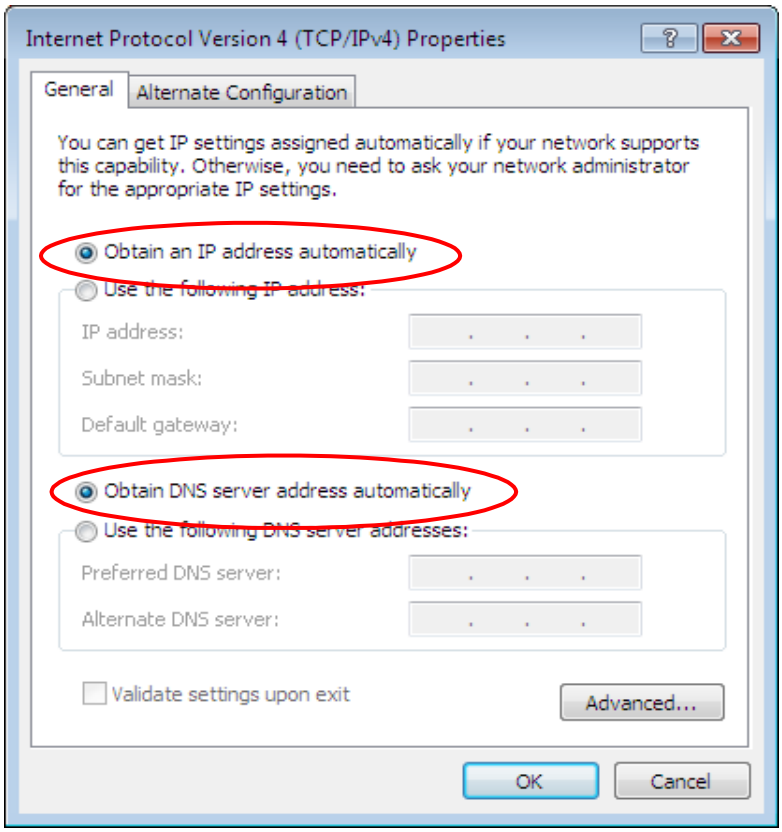
4. Select the **Local Area Connection**, and right click the icon to select **Properties**.



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



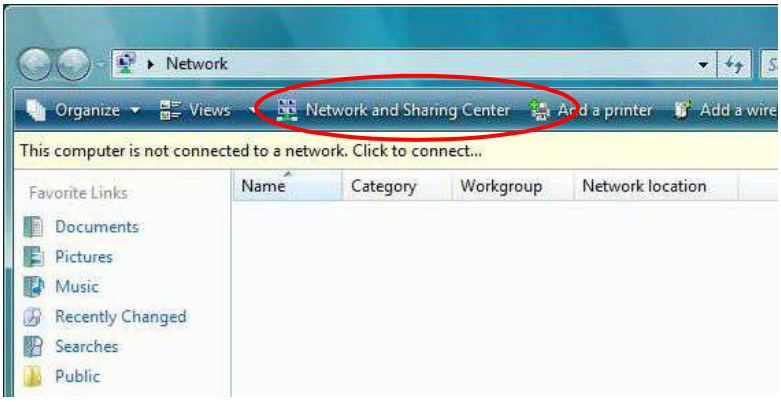
6. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



Configuring PC in Windows Vista (IPv4)

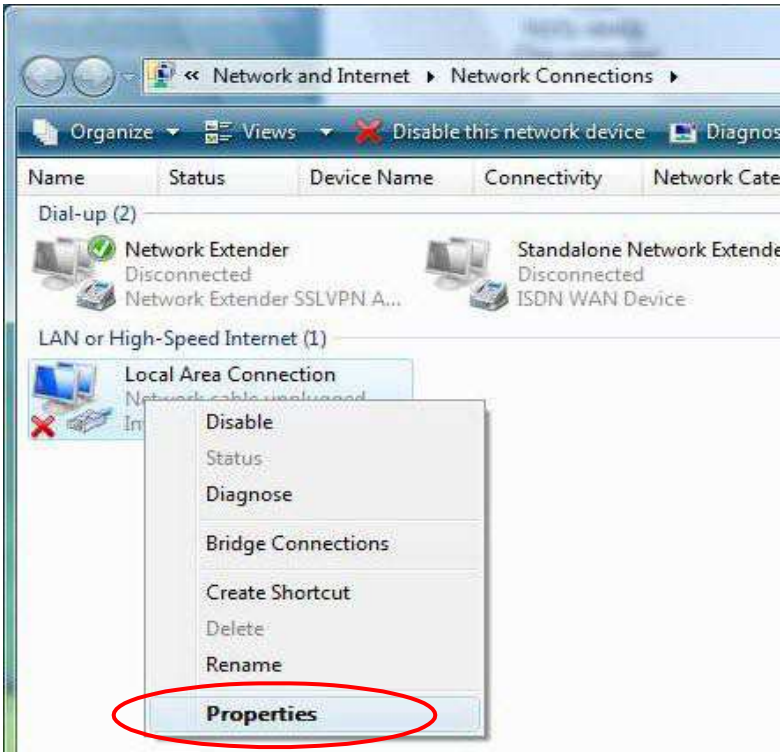
1. Go to **Start**. Click on **Network**.

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

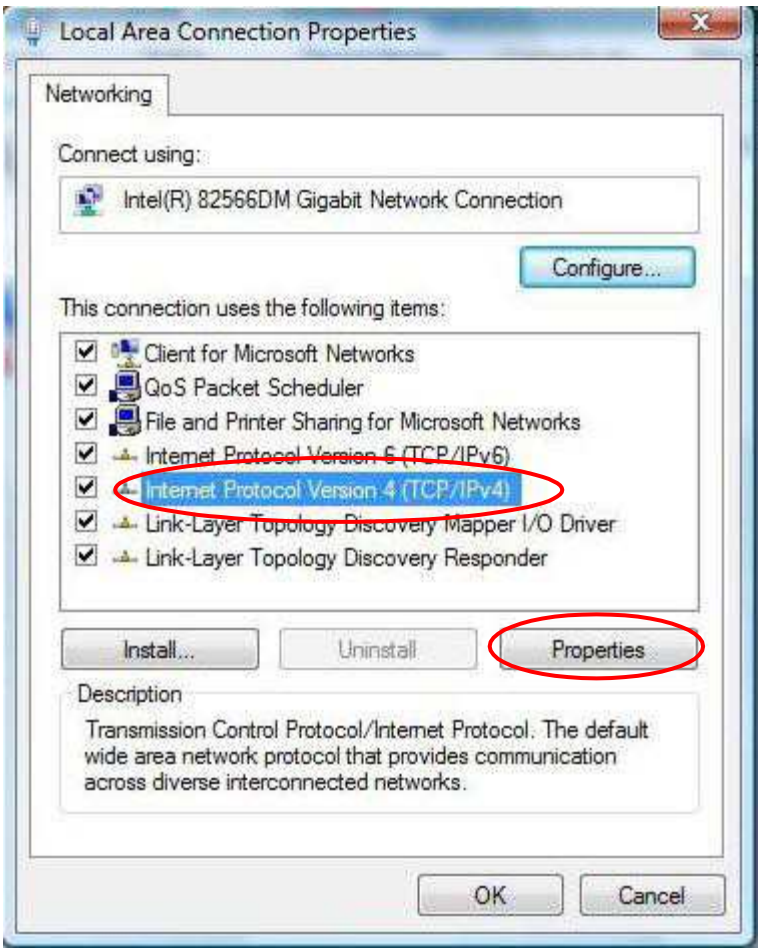


3. When the **Network and Sharing Center** window pops up, select and click on **Manage network connections** on the left window pane.

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

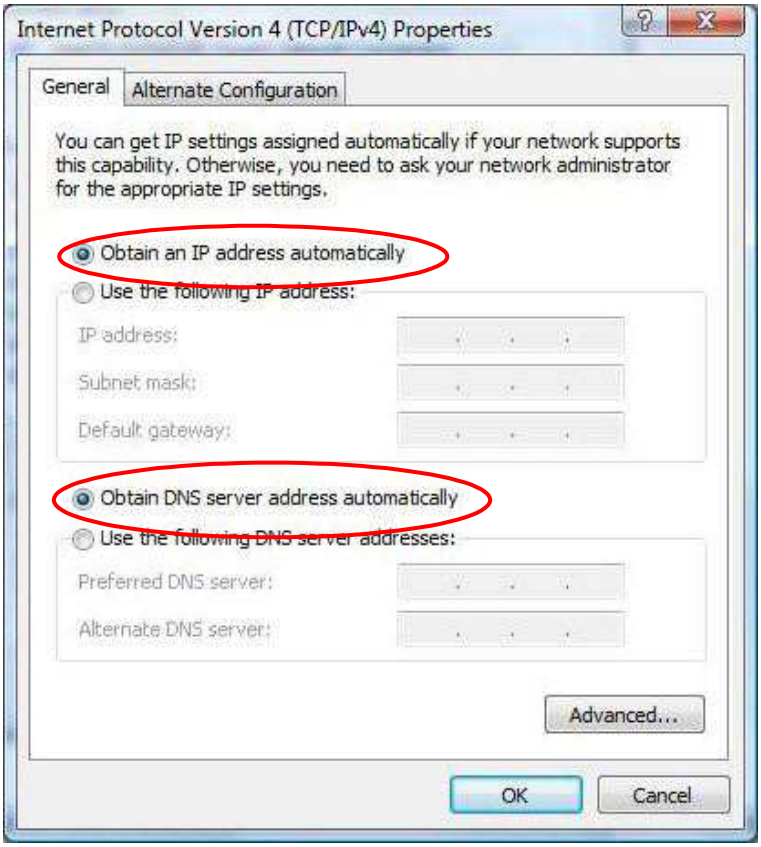


5. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.



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

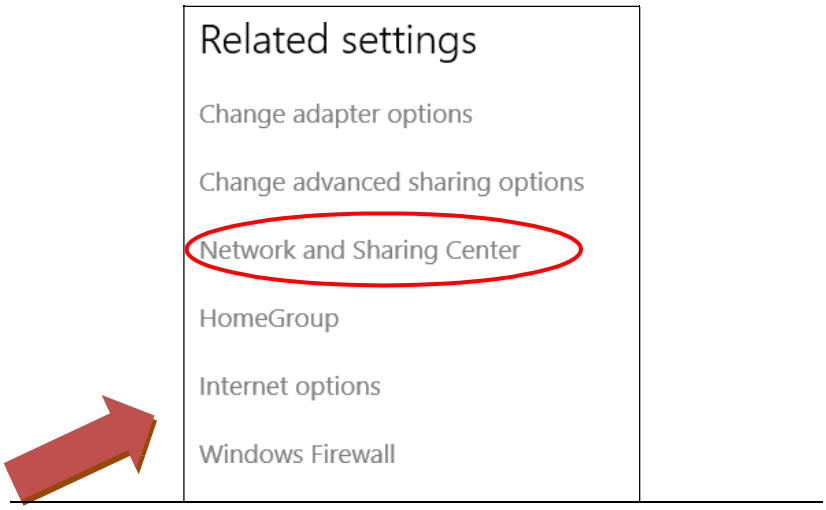
Configuring PC in Windows 10 (IPv6)

1. Click .

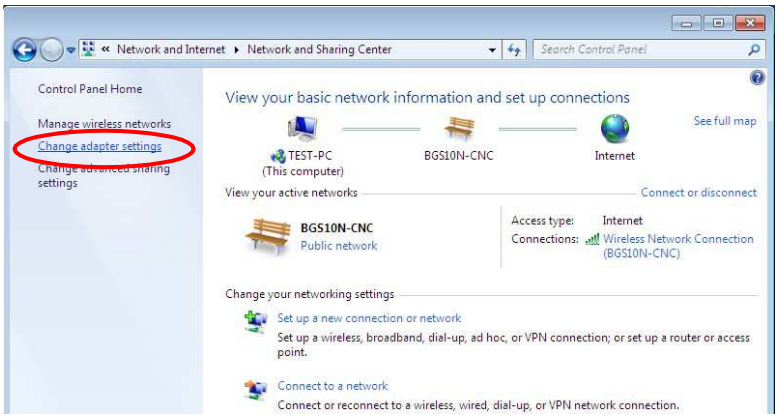
2. Click Settings

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

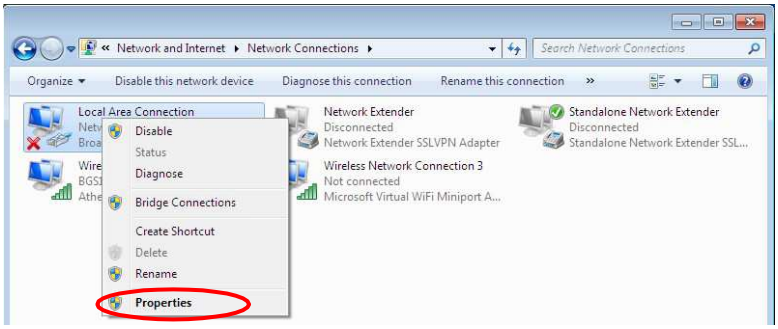
4. Under **Related settings,** select **Network and Sharing Center**



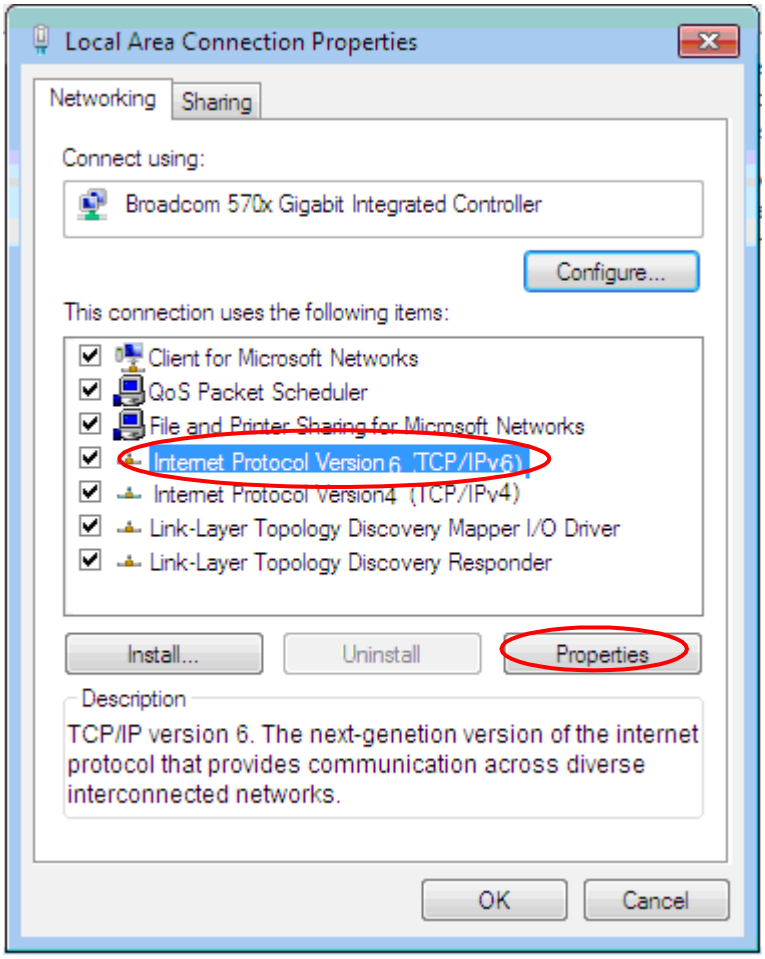
5. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



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

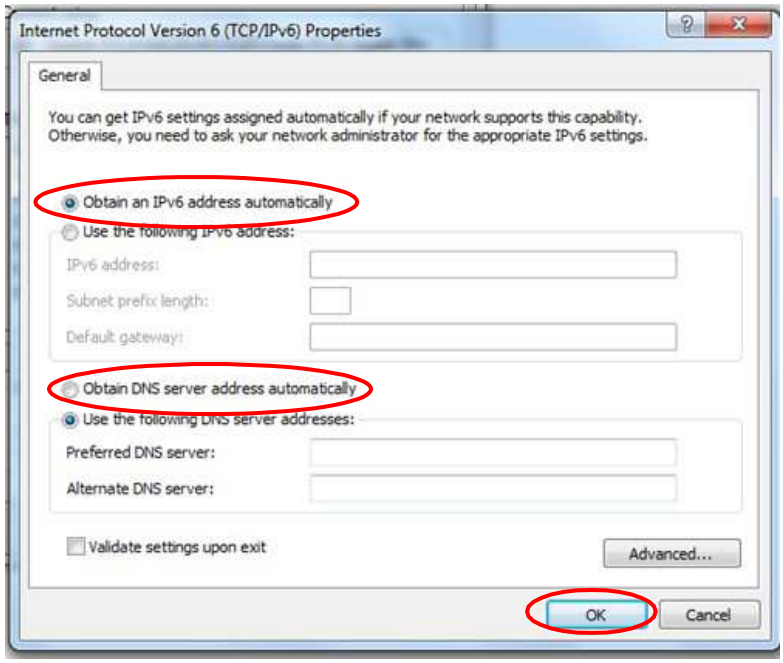


7. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**.



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.

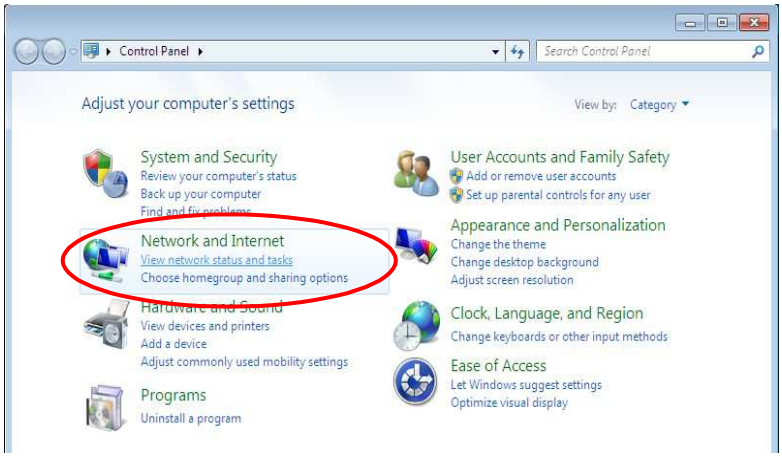
9. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



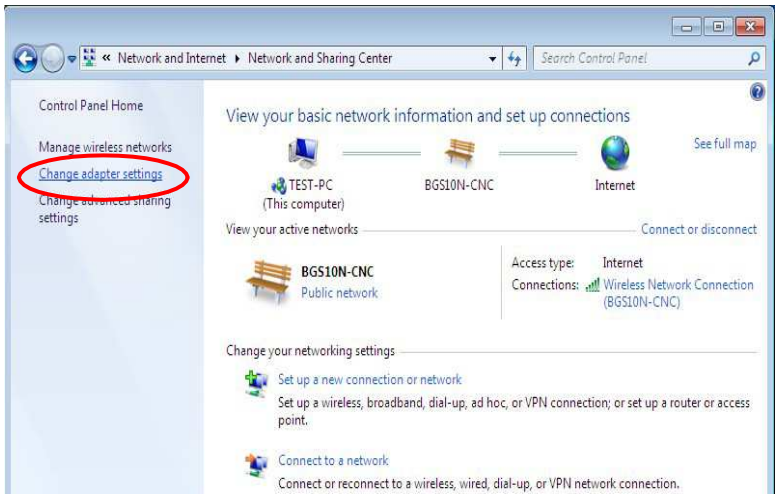
Configuring PC in Windows 7/8 (IPv6)

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

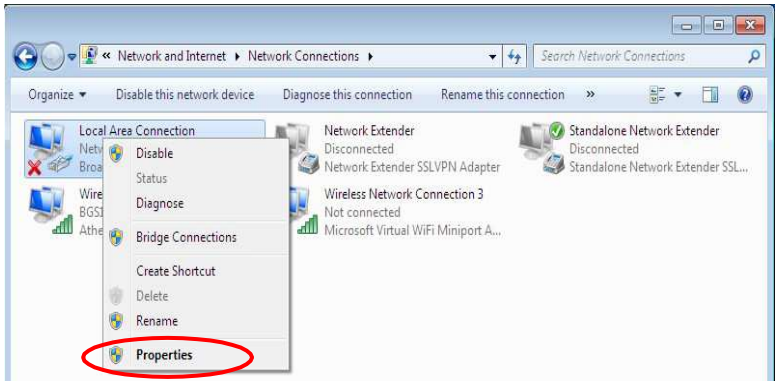
2. Then click on **Network and Internet**.



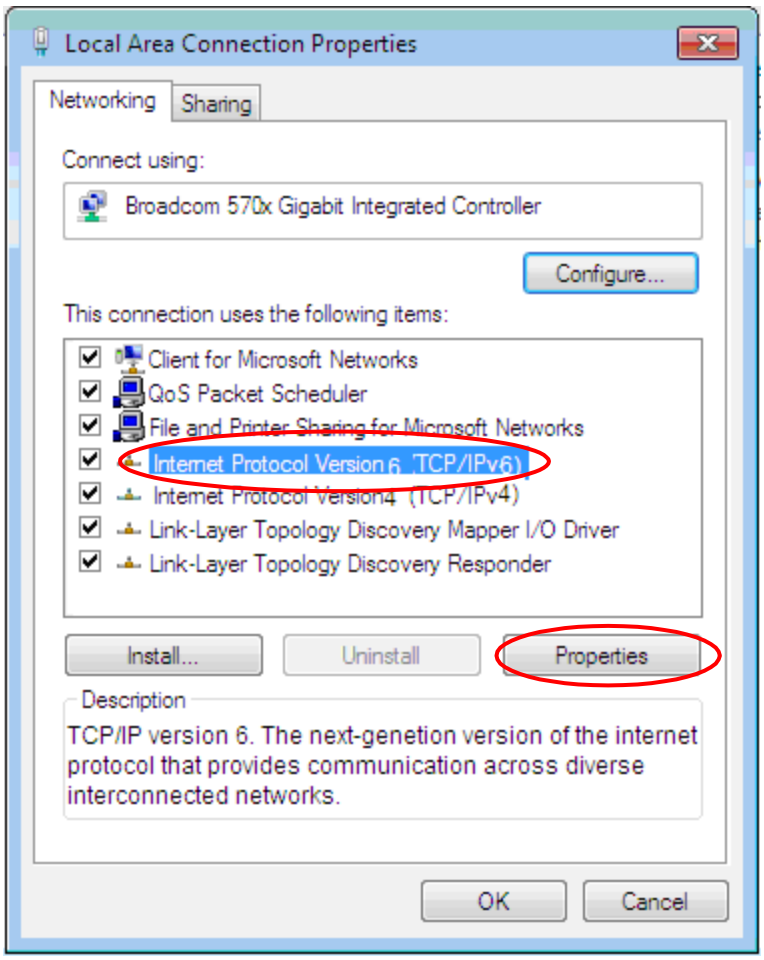
3. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



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

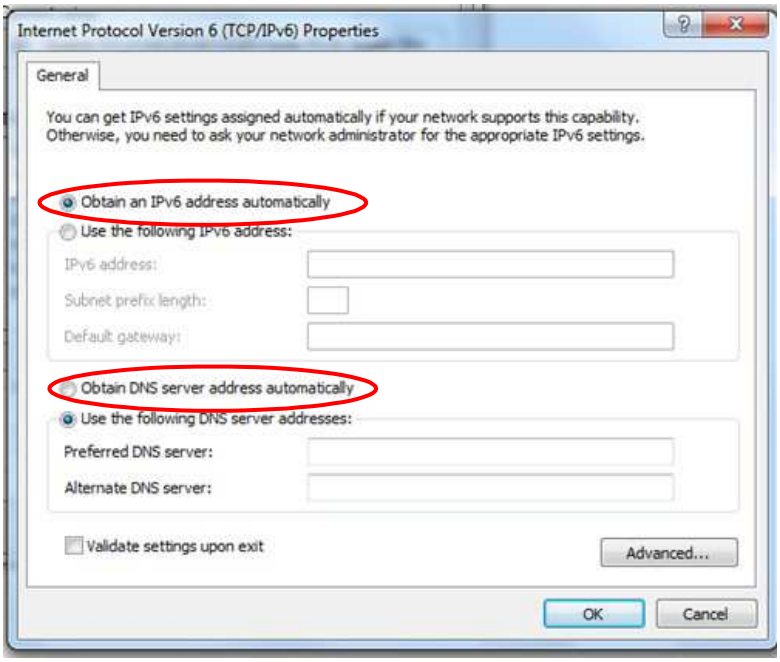


5. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**.



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.

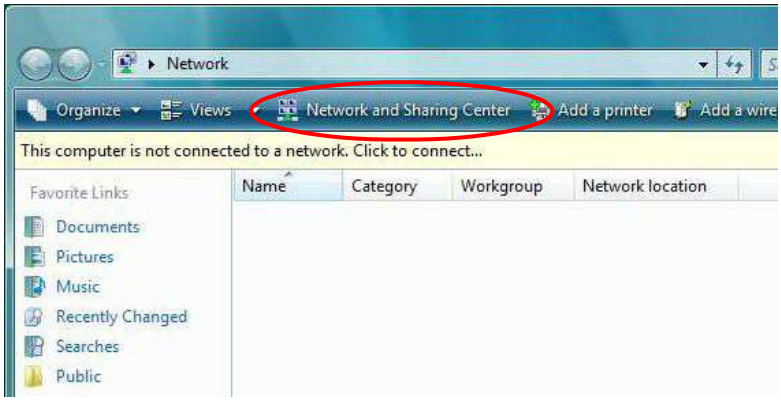
7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



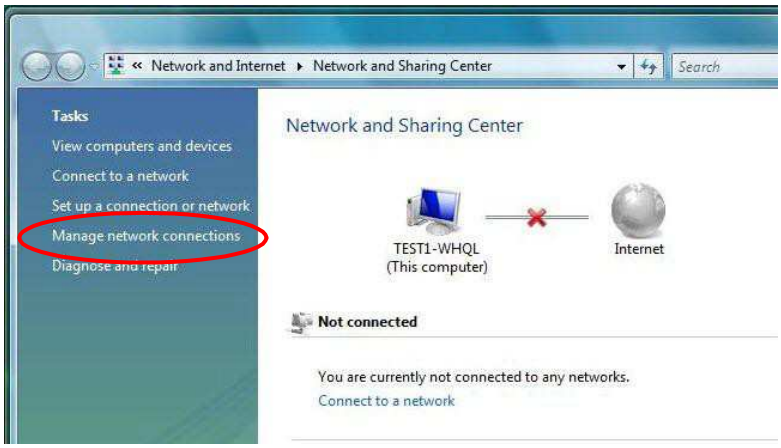
Configuring PC in Windows Vista (IPv6)

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

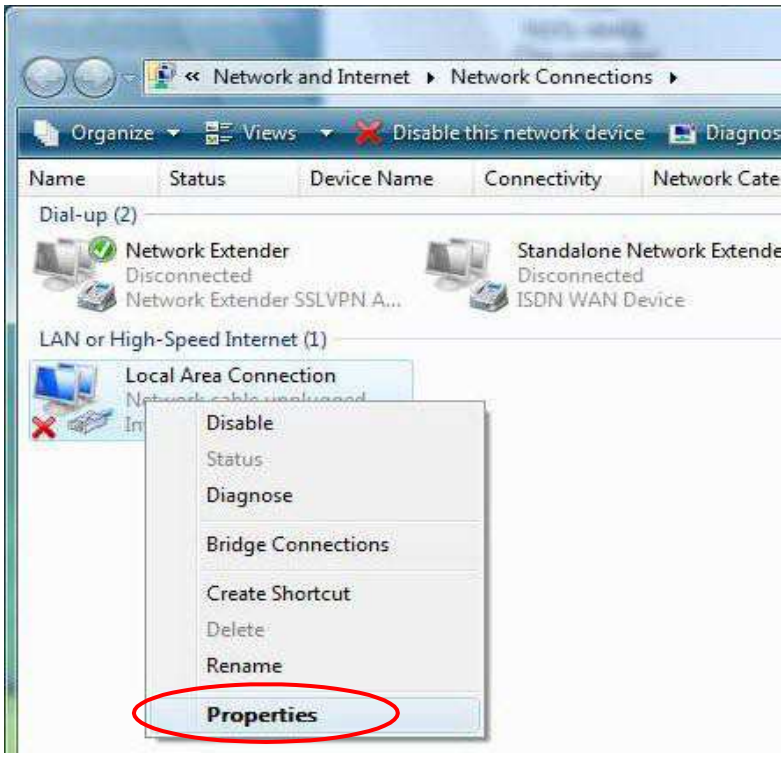
2. Then click on **Network and Sharing Center** at the top bar.



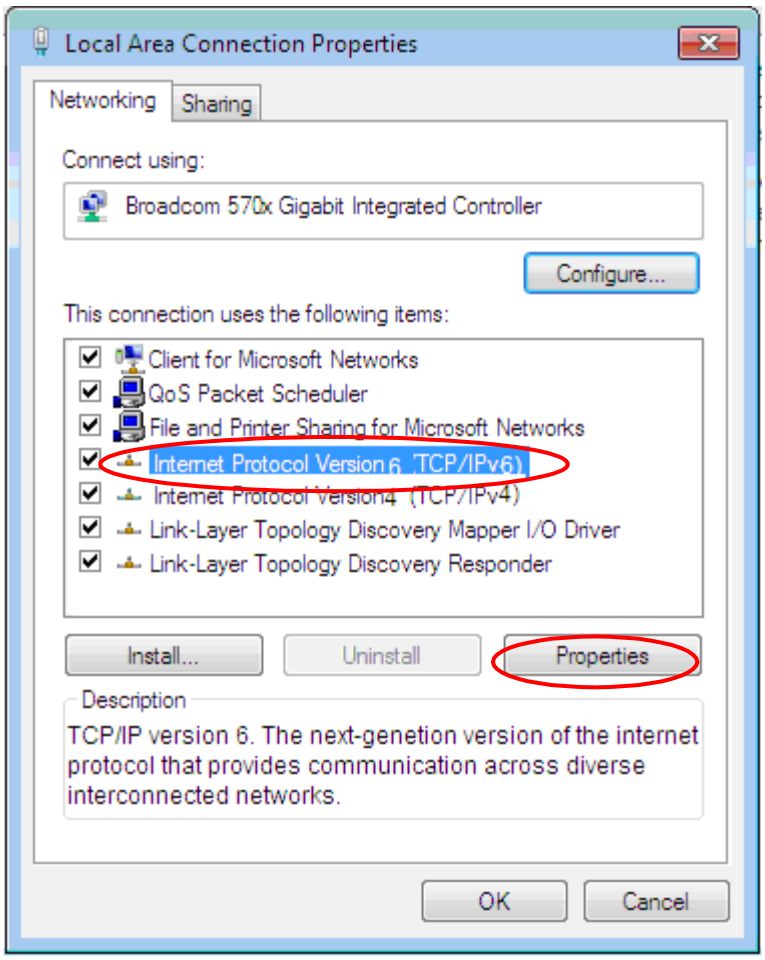
3. When the **Network and Sharing Center** window pops up, select and click on **Manage network connections** on the left window pane.



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

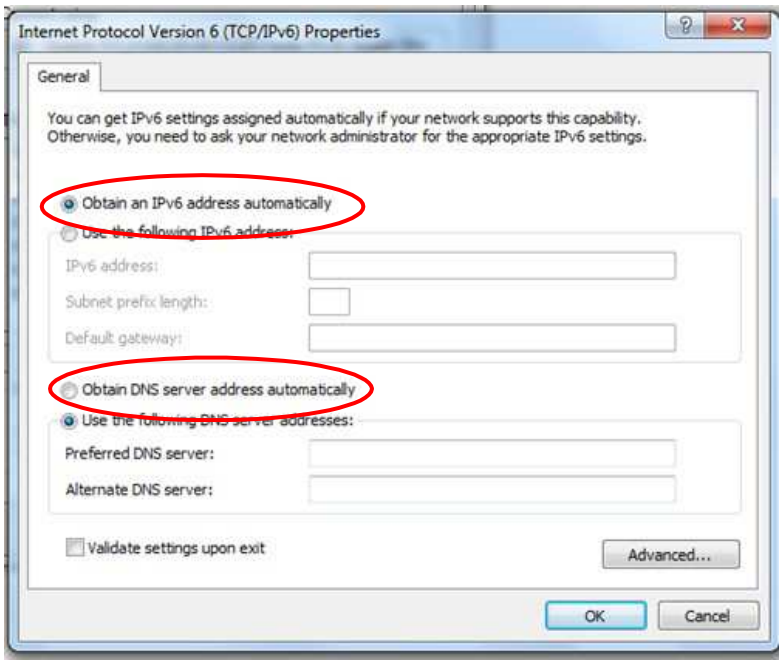


5. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**.



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: admin or a unique12-digit password can be found on the device label.

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

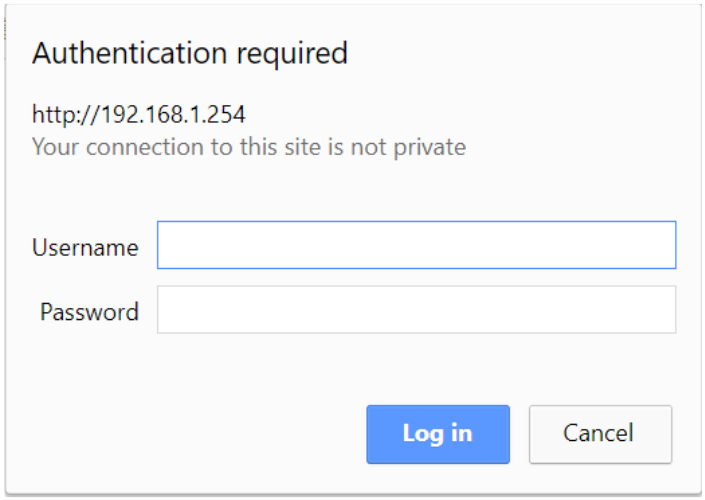
Login to your Device

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 are **"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.



Congratulations! You have successfully logged on to your MX-210NP-R17AF

Once you have logged on to your MX-210NP-R17AF 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 4G/LTE Status Wireless Status Statistics DHCP Table ARP Table VRRP Status		**Interface Setup** - Internet - LAN - Wireless - Wireless MAC Filter - Loopback **Dual WAN** - General Setting - Outbound Load Balance - Protocol Binding **Advanced Setup** - Firewall - Routing - Dynamic Routing - NAT - VRRP - Static DNS - QoS - Time Schedule - Mail Alert **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-210NP-R17AF** device.

Status

Device Info

It provides brief status summary of the device.

Device Information	
Model Name	
Firmware Version	1.04.1.235
MAC Address	00:04:ed:01:23:45
Date-Time	Mon Apr 10 05:55:35 2017
System Up Time	5 hours 56 mins

Physical Port Status	
4G/LTE	✓
EWAN(LAN2)	✗
Ethernet	✓
Wireless	✓

WAN

Interface	Protocol	Connection	IP Address	Default Gateway
4G/LTE	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

Wireless

Mode	SSID	Channel	Security
802.11b+g+n	cchu	6	Mixed WPA2/WPA-PSK

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-210NP-R17AF** with your PC. Check on **Time Zone** section for more configuration information.

System Uptime: Display how long the **MX-210NP-R17AF** 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-210NP-R17AF.

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

Wireless

Mode: Display selected Wireless mode.

SSID: Display the name of the Wireless AP(s) to use

Channel: Display radio frequency to be used for this wireless link

Security: Display security method to be used for this wireless link

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
```

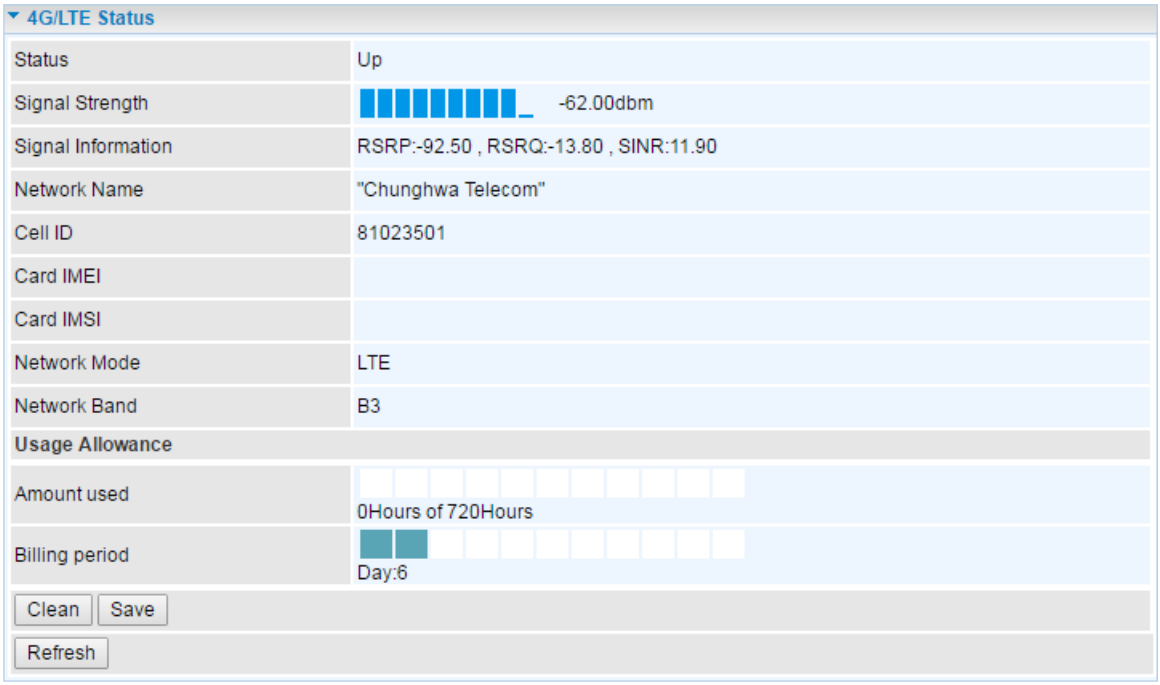
Refresh Backup

Refresh: Press this button to refresh the statistics.

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

4G/LTE Status

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



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.

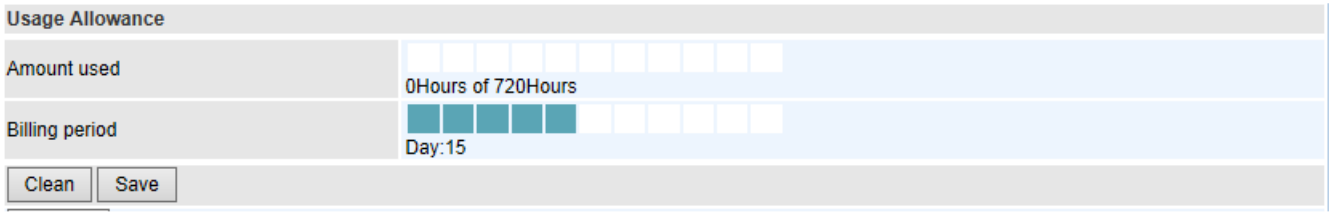
Card IMEI: The unique identification number that is used to identify the 3G/4G-LTE module.

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



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.

Wireless Status

Wireless Status

Wireless Status

MAC	SSID	RSSI	Connected Time	Host Name	IP Address	Expire Time
d4:6a:6a:64:e3:09	cchu	-69/-64	00:00:36	DESKTOP-PPUSERT	192.168.1.100	0 days 23:59:23

Refresh

MAC: The MAC of the connected wireless device.

SSID: Display the total bytes transmitted till the latest second for the current connection for the current connection.

RSSI: Display the signal strength between the wireless client and the AP (Access Point)

Connected Time: Display the total amount of time the wireless client has connected with the wireless AP

Host Name: Display the hostname of the Wi-Fi client.

IP Address: The LAN IP address assigned to the wireless device.

Expire Time: Display remaining time before connection expires or timeout.

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(LAN2) ○ Ethernet ○ Wireless		
Transmit Statistics		**Receive Statistics**	
Transmit Frames of Current Connection	0	Receive Frames of Current Connection	0
Transmit Bytes of Current Connection	0	Receive Bytes of Current Connection	0
Transmit Total Frames	0	Receive Total Frames	0
Transmit Total Bytes	0	Receive Total Bytes	0
Transmit Speed	0.00KBps	Receive Speed	0.00KBps
Refresh		Auto Refresh	None ▼

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.

Transmit Speed: Display the data rate can be transferred to the server, the mobile Internet.

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.

Receive Speed: Display the data rate receives from the mobile Internet.

Refresh: Click to manually refresh the data.

Auto Reresh: Select a time interval to refresh the data automatically or none to disable the feature.

❖ EWAN (LAN2)

Statistics			
Traffic Statistics			
Interface	○ 3G/4G-LTE Status ◉ EWAN(LAN2) ○ Ethernet ○ Wireless		
Transmit Statistics		**Receive Statistics**	
Transmit Frames	0	Receive Frames	0
Transmit Multicast Frames	0	Receive Multicast Frame	0
Transmit Total Bytes	0	Receive Total Bytes	0
Transmit Collision	0	Receive CRC Errors	0
Transmit Error Frames	0	Receive Under-size Frames	0
Traffic Speed			
Transmit Speed	0.00KBps	Receive Speed	0.00KBps
Refresh			Auto Refresh None ▼

Traffic Statistics

Interface: List all available network interfaces in the router. You are currently checking on the physical status of the **EWAN (Ethernet #2)** 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.

Traffic Speed

Transmit Speed: Display the data rate can be transferred to the server, the Broadband Internet Service Provider.

Receive Speed: Display the data rate receives from the Broadband Internet Service Provider.

Refresh: Click to manually refresh the data.

Auto Reresh: Select a time interval to refresh the data automatically or none to disable the feature.

❖ Ethernet

Statistics

Traffic Statistics			
Interface	3G/4G-LTE Status EWAN(LAN2) Ethernet Wireless		
Transmit Statistics		**Receive Statistics**	
Transmit Frames	6560	Receive Frames	2696
Transmit Multicast Frames	5044	Receive Multicast Frame	1308
Transmit Total Bytes	1039911	Receive Total Bytes	791906
Transmit Collision	0	Receive CRC Errors	0
Transmit Error Frames	0	Receive Under-size Frames	0
Traffic Speed			
Transmit Speed	0.00KBps	Receive Speed	0.00KBps
Refresh			Auto Refresh None ▼

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.

Traffic Speed

Transmit Speed: Display the data rate can be transferred to the server, the LAN network.

Receive Speed: Display the data rate receives from the LAN network.

Refresh: Click to manually refresh the data.

Auto Reresh: Select a time interval to refresh the data automatically or none to disable the feature.

❖ Wireless

Statistics			
Traffic Statistics			
Interface	○ 3G/4G-LTE Status ○ EWAN(LAN2) ○ Ethernet ◉ Wireless		
Transmit Statistics		**Receive Statistics**	
Transmit Frames	593	Receive Frames	2659
Transmit Error Frames	1394	Receive Error Frames	771
Transmit Drop Frames	1394	Receive Drop Frames	771
Traffic Speed			
Transmit Speed	0.00KBps	Receive Speed	0.00KBps
Refresh		Auto Refresh	None ▼

Traffic Statistics

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

Transmit Statistics

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

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

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

Receive Statistics

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

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

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

Traffic Speed

Transmit Speed: Display the data rate can be transferred to the server, the Wireless AP.

Receive Speed: Display the data rate receives from the Wireless AP.

Refresh: Click to manually refresh the data.

Auto Reresh: Select a time interval to refresh the data automatically or none to disable the feature.

DHCP Table

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

DHCP Table

Index	Host Name	IP	MAC Address	Expire Time
1	DESKTOP-PPUSERT	192.168.1.100	[redacted]09	0days 22:29:22

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.

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

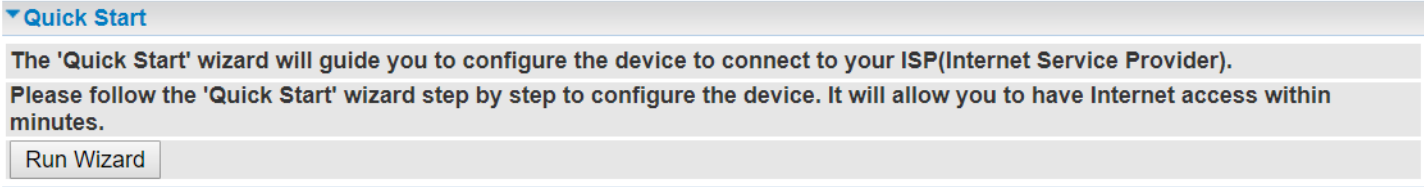
Current Status	N/A
Current Master	N/A

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

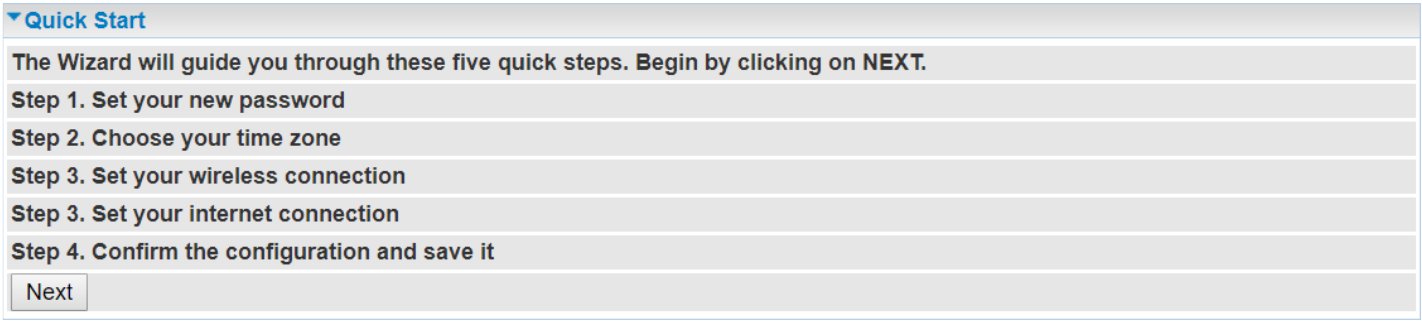
Current Master: Display the IP address of the Master

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.



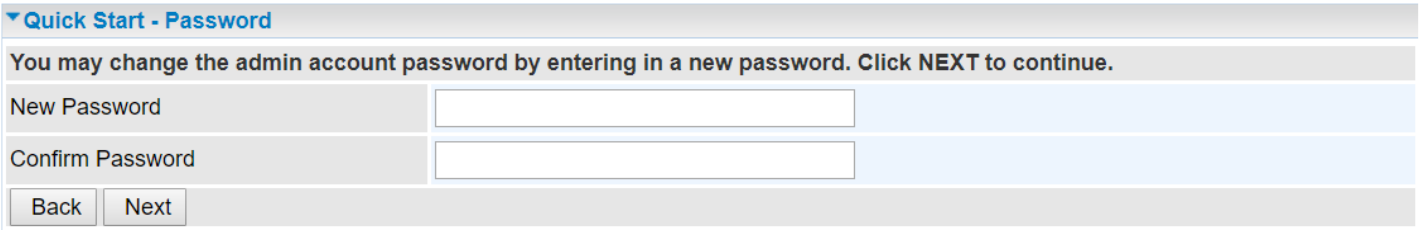
For detailed instructions on configuring WAN settings, see refer to the **Interface Setup** section.



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

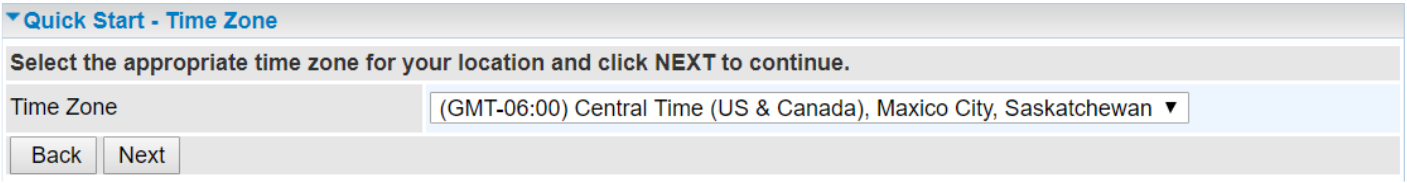
Step 1 – Password

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.



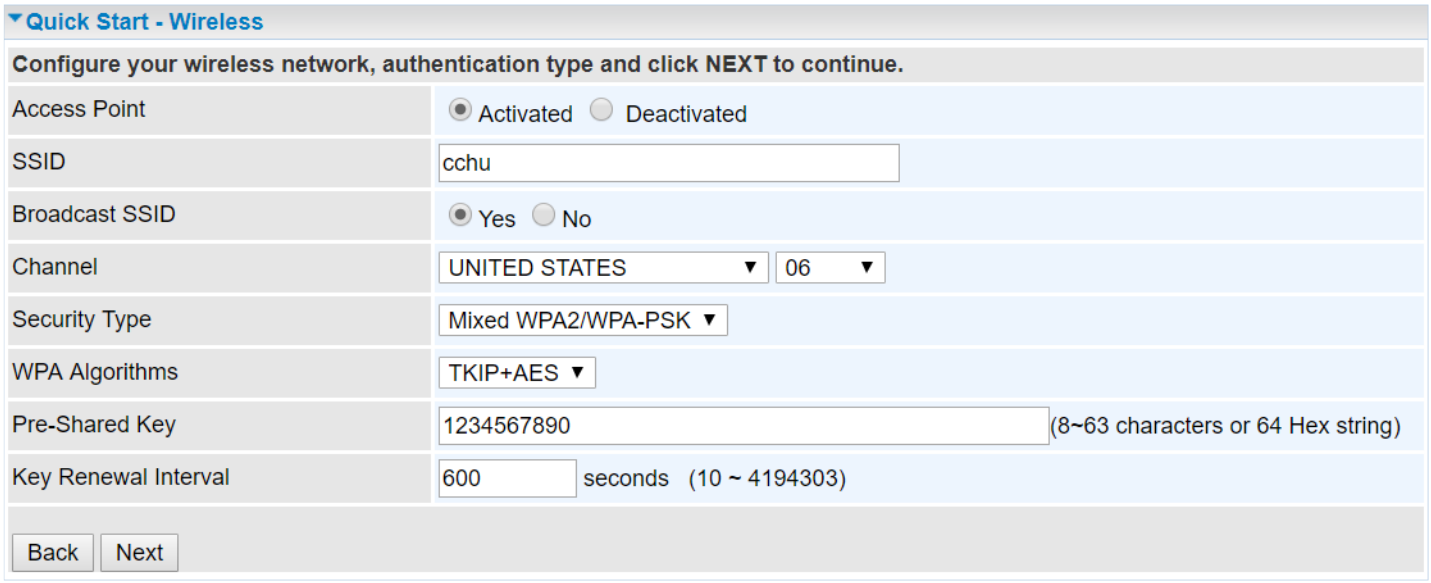
Step 2 – Time Zone

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



Step 3 – Wireless

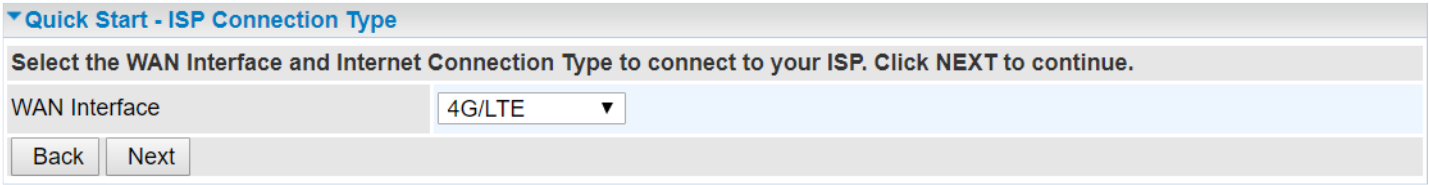
Set up your wireless connection if you want to connect to the Internet wirelessly on your PCs. Click **NEXT** to continue.



Step 4 – ISP Connection Type

Set up your Internet connection.

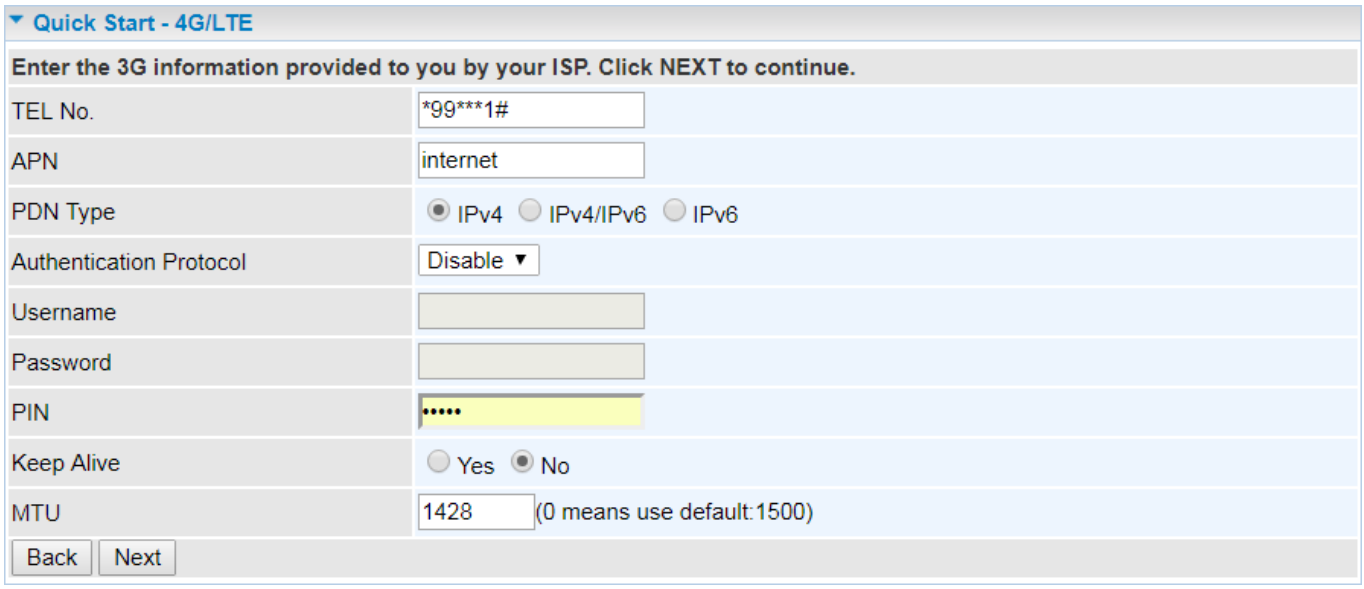
Select an appropriate WAN connection protocol then click **NEXT** to continue.



>> If selected **4G/LTE**

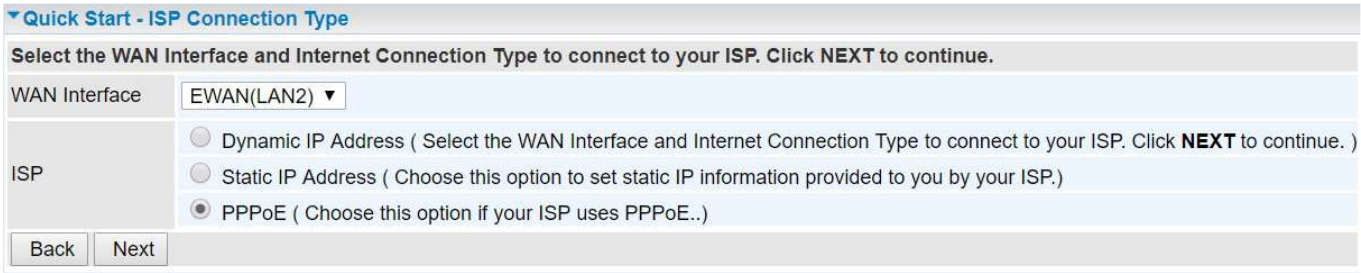
Input all relevant 4G/LTE parameters from your cellular provider.

Click **Next** to continue.



>> If selected **EWAN (LAN2) / Static IP or PPPoE**, enter the static IP address or PPPoE account information provided by your ISP.

Click **NEXT** to continue.



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.

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

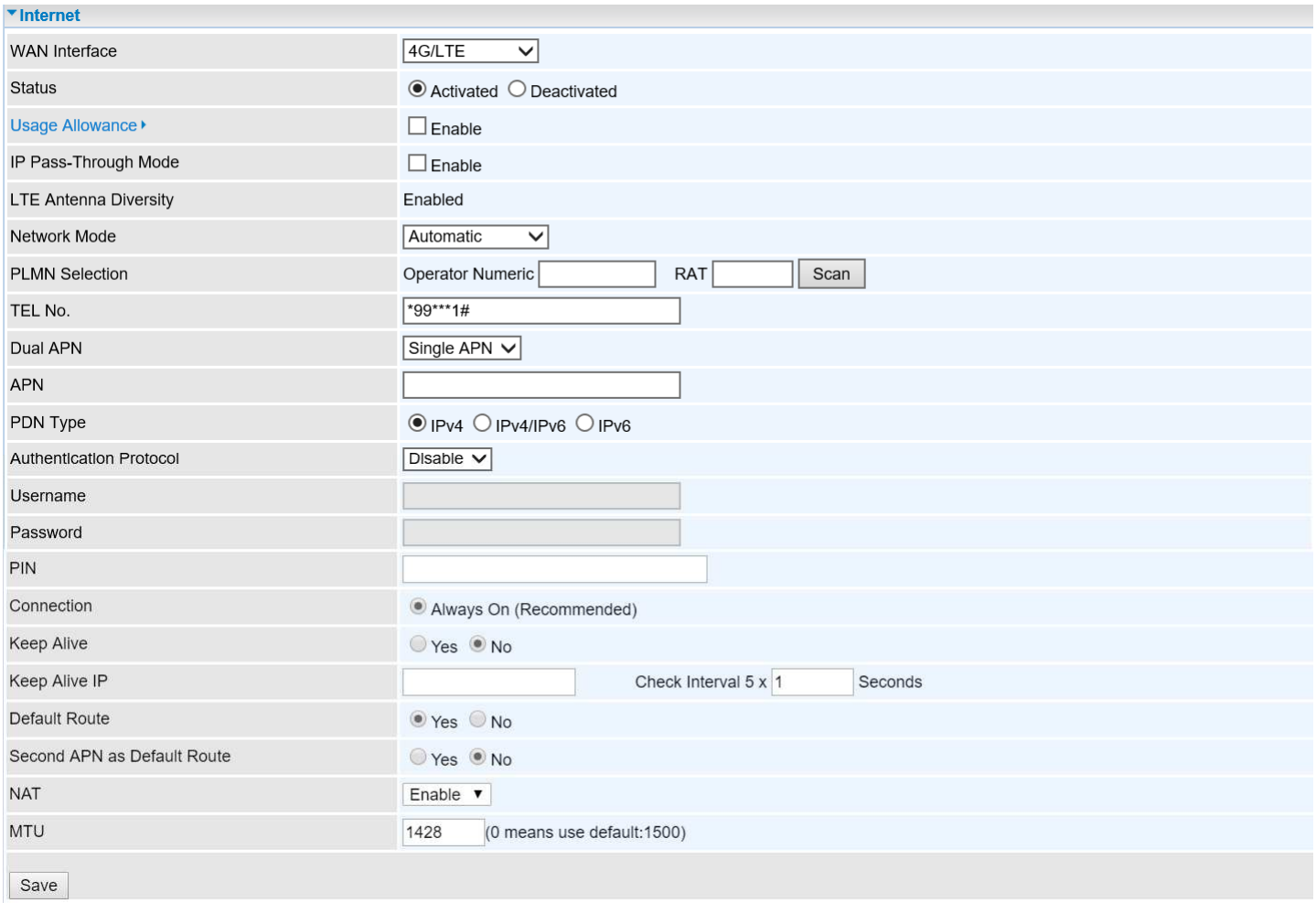
Device Configuration

Interface Setup

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

Internet

❖ 4G/LTE



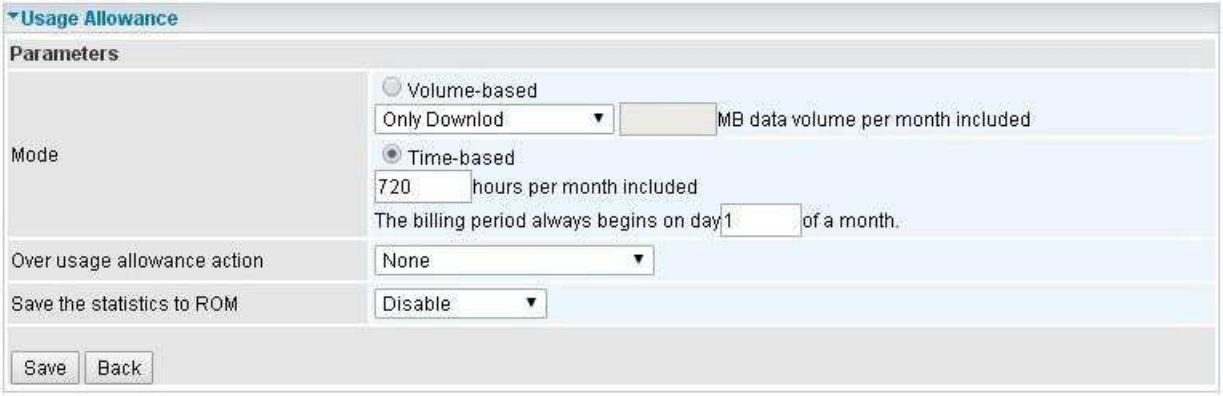
WAN Interface: List all available WAN interfaces. (In this section, you have selected to use 4G/LTE)

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

Usage Allowance (Cont.)



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

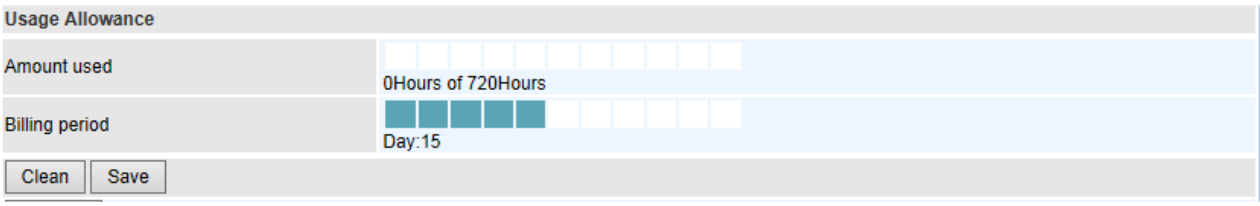
Email Alert: Send an e-mail alert and keep the mobile connection alive.

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

Save the statistics to ROM:

Every 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.



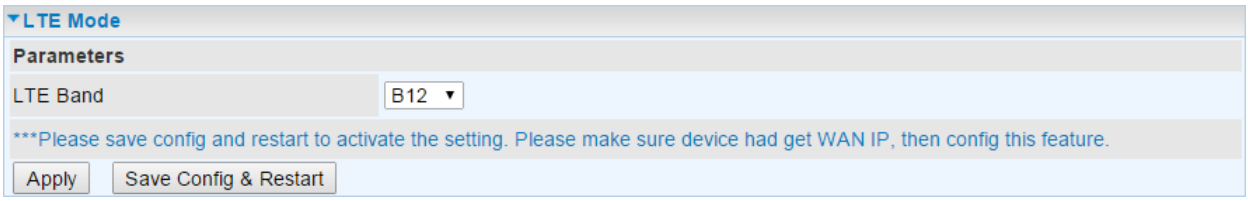
NOTE: This statistic information will get deleted after a factory reset.

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.

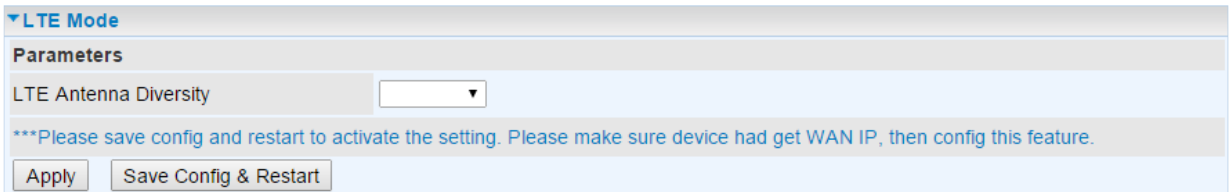


IP Pass-through Mode: When **enabled**, MX-210NP-R17AF is in bridge mode that it does not obtain a WAN IP address; features such as routing capabilities, NAT, firewall, etc., are being disabled. The client router that is behind the MX-210NP-R17AF now obtains a WAN IP address. When **disabled**, MX-210NP-R17AF is in router mode that it handles a WAN IP address and all features become available.

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**

Network Mode: There are numbers of services to select from. 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.

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 like a URL on the WWW, it is what the unit makes a GPRS / UMTS call. The service provider can 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: Select **Yes** to keep the 3G/4G-LTE connection always on

Keep Alive IP: Manually enter the Keep Alive IP Address to be used for ping operation to check if the connection is still on.

Check Interval 5 x____Seconds: Default is set to 1 (5 seconds). Setup a timer to ping the keep alive IP.

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 2)

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.

802.1q Options

802.1 q: 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-210NP-R17AF 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	
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 ☑ WLAN1
DNS Relay	◉ Automatically ○ Manually
Primary DNS	
Secondary DNS	
Option 66	
Option 160	

DHCPv4 Server: If set to **Enabled**, your MX-210NP-R17AF 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-210NP-R17AF 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.

Wireless

This section introduces the wireless LAN and some basic configurations.

NOTE: WLAN1 / 2 / 3 / 4 Interface refers to as SSID1 / 2 / 3 / 4 Wi-Fi networks.

Access Point Settings

Wireless | Site Survey

Access Point Settings

Access Point	◉ Activated ○ Deactivated
AP MAC Address	00:04:ED:01:23:45
Wireless Mode	802.11b+g+n ▼
Channel	UNITED STATES ▼ 06 ▼ Current Channel : 6
Beacon Interval	100 (range: 20~1000)
RTS/CTS Threshold	2347 (range: 1500~2347)
Fragmentation Threshold	2346 (range: 256~2346, even numbers only)
DTIM Interval	1 (range: 1~255)
TX Power	100 (range:1~100)
IGMP Snooping	◉ Yes ○ No

Site Servey: Click to view all other available Wireless-AP devices around the MX-210NP-R17AF.

Site Survey

CH	SSID	BSSID	Security	Signal (%)
1	Meriton Guest WiFi	1c:b9:c4:94:97:b8	NONE	42
11	Meriton Guest WiFi	1c:b9:c4:93:b5:28	NONE	0

Refresh | Back

CH (Channel): Channel ID used.

SSID: The name of the wireless AP.

BSSID: The MaC address of the wireless AP.

Security: The security mode in the wireless AP.

Singal (%): Singal strength of the wireless AP. Signal incrases means the wireless AP is closer to your MX-210NP-R17AF and may cause interferences.

Access Point: Default setting is set to **Activated**. If you want to close the wireless interface, select **Deactivated.**

AP MAC Address: The MAC address of wireless AP.

Wireless Mode: The default setting is **802.11b+g+n** (Mixed mode). If you do not know or have both 11g and 11b devices in your network, then keep the default in **mixed mode**. From the drop-down manual, you can select **802.11g** if you have only 11g card. If you have only 11b card, then select **802.11b** and if you only have 802.11n then select **802.11n**.

Channel: The range of radio frequencies used by IEEE 802.11b/g/n wireless devices is called a channel. There are Regulation Domains and Channel ID in this field. The Channel ID will be different based on Regulation Domains. Select a channel from the drop-down list box.

Beacon interval: The Beacon Interval value indicates the frequency interval of the beacon. Enter a value between 20 and 1000. A beacon is a packet broadcast by the Router to synchronize the wireless network.

RTS/CTS Threshold: The RTS (Request To Send) threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Enter a value between 1500 and 2347.

Fragmentation Threshold: The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between 256 and 2346, even number only.

DTIM Interval: This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM).

TX Power: The transmission power of the antennas, ranging from 1-100, the higher the more powerful of the transmission performance.

IGMP Snooping: Enable or disable the IGMP Snooping function for wireless. Without IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic - that is, it is forwarded to all ports. With IGMP snooping, multicast traffic of a group is only forwarded to ports that have members of that group."

11n Settings

11n Settings	
Channel Bandwidth	20/40 MHz ▼
Extension Channel	Auto ▼
Guard Interval	Auto ▼
MCS	Auto ▼

Channel Bandwidth: Select **20 MHz, 40 MHz,** or **20/40 MHz** for the channel bandwidth. The wider the Channel bandwidth the better the performance will be.

Extension Channel (20/40 MHz only): Select either **Auto** or **Above the control channel**.

Guard Interval: Select either **800nsec** or **Automatic** for the guard interval. The guard interval is here to ensure that data transmission do not interfere with each other. It also prevents propagation delays, echoing and reflections. The shorter the Guard Interval, the better the performance will be. We recommend users to select **Auto**.

MCS (Modulation and Coding Scheme): There are options **0~15** and **AUTO** to select from. **AUTO** is recommended.

SSID Settings

SSID Settings	
Available SSID	4 ▼
SSID Index	◉ SSID1 ○ SSID2 ○ SSID3 ○ SSID4
SSID	cchu
Broadcast SSID	◉ Yes ○ No
Clients Isolation	○ Yes ◉ No

Available SSID: User can determine how many virtual SSIDs to be used. Default is 1, maximum is 4.

SSID Index: Select the number of SSIDs you want to use; up to 4 SSIDs are available in the list.

SSID1 SSID known as **wlan-ap1** Interface

SSID2 known as **wlan-ap2**Interface

SSID3 known as **wlan-ap3** Interface

SSID4 known as **wlan-ap4** Interface

SSID: The SSID is the unique name of a wireless access point (AP) to be distinguished from another. For security propose, change the default **wlan-ap** to a unique ID name to the AP which is already built-in to the router's wireless interface. Make sure your wireless clients have exactly the SSID as the device to get connected to your network.

Broadcast SSID: Select **Yes** to make the SSID visible so a station can obtain the SSID through passive scanning. Select **No** to hide the SSID in so a station cannot obtain the SSID through passive scanning.

Client Isolation: Enable by clicking **Yes** to prevent wireless clients communicating with other wireless clients.

Security Settings

Security Type: You can disable or enable wireless security for protecting wireless network. The default type of wireless security is OPEN and to allow all wireless stations to communicate with the access points without any data encryption.

To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers secure data encryption, known as WEP and WPA.

There are five alternatives to select from: WEP 64-bit, WEP 128-bit, WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK. If you require high security for transmissions, please select WPA-PSK, WPA2-PSK or WPA/WPA2-PSK.

WEP

Security Settings	
Security Type	WEP 64-bit
WEP Authentication Method	Both
WEP 64-bit	For each key, please enter either (1) 5 characters, or (2) 10 characters ranging from 0~9, a, b, c, d, e, f.
Key#1	
Key#2	
Key#3	
Key#4	

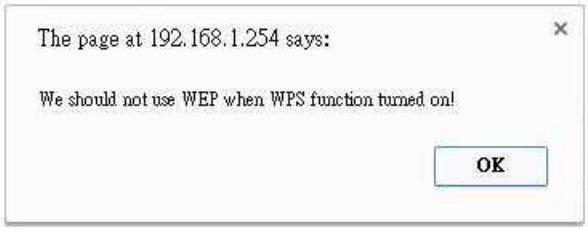
WEP Authentication Method: WEP authentication method, there are two methods of authentication used, Open System authentication (OPENWEB) and Share Key authentication (SHAREDWEB). We suggest you select OPENWEB.

Key 1 to Key 4: Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format is in HEX style, 5 and 13 HEX codes are required for 64-bitWEP and 128-bitWEP respectively.

If chose **WEP 64-bit**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").

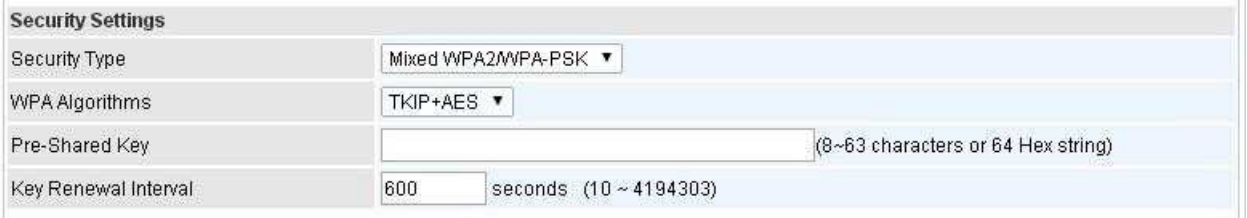
If chose **WEP 128-bit**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").

You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.



NOTE: WPS requires a higher level of security than WEP, 64bits or 128bits. Select WAP / WAP2 security when using WPS.

WPA-PSK / WPA2-PSK / Mixed WPA & WPA2



WPA Algorithms: TKIP (Temporal Key Integrity Protocol) or AES (Advanced Encryption System) utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers.

Pre-Shared key: The key for network authentication. The input format should be 8-63 ASKII characters or 64 hexadecimal characters

Key Renewal Interval: The time interval for changing the security key automatically between wireless client and AP.

WDS Settings

WDS (Wireless distributed system) is a wireless access point mode that enables wireless link and communication with other access point. It is easy to be installed, just define the peer's MAC of the connected AP.

WDS Mode: select Activated to enable WDS feature and Deactivated to disable this feature.

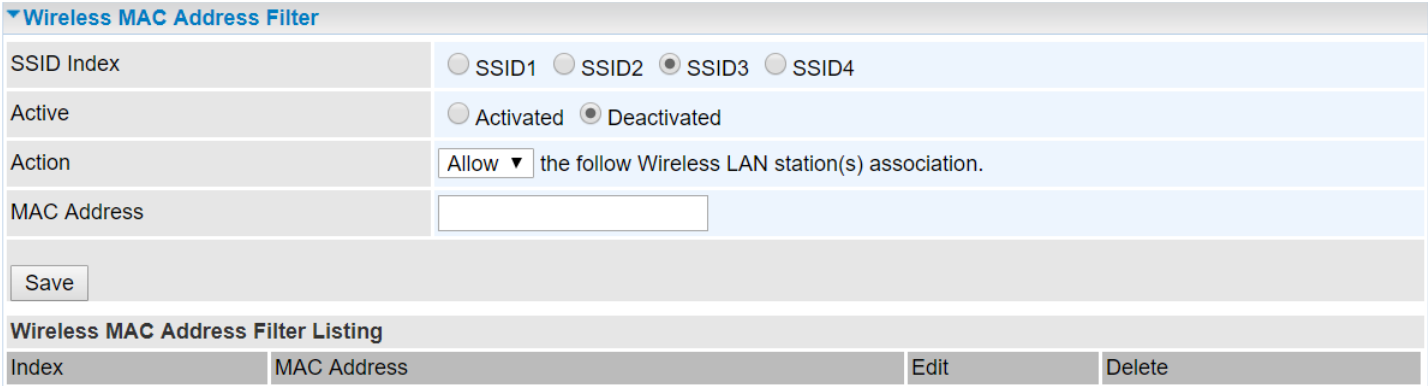
MAC Address: Enter the AP MAC addresses (in XX:XX:XX:XX:XX:XX format) of the peer connected AP.

Click **Save** to apply the settings.

Wireless MAC Filter

The MAC filter screen allows you to configure the router to give exclusive access to up to 8 devices (Allow Association) or exclude up to 8 devices from accessing the router (Deny Association). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:AA:BB:00:00:02.

You need to know the MAC address of the devices you wish to filter.



SSID Index: Select the targeted SSID you want the MAC filter rules to apply to.

Active: Select **Activated** to enable MAC address filtering.

Action: Define the filter action for the list of MAC addresses in the MAC address filter table.

Select **Deny** to block access to the AP, MAC addresses not listed will be allowed to access the router.

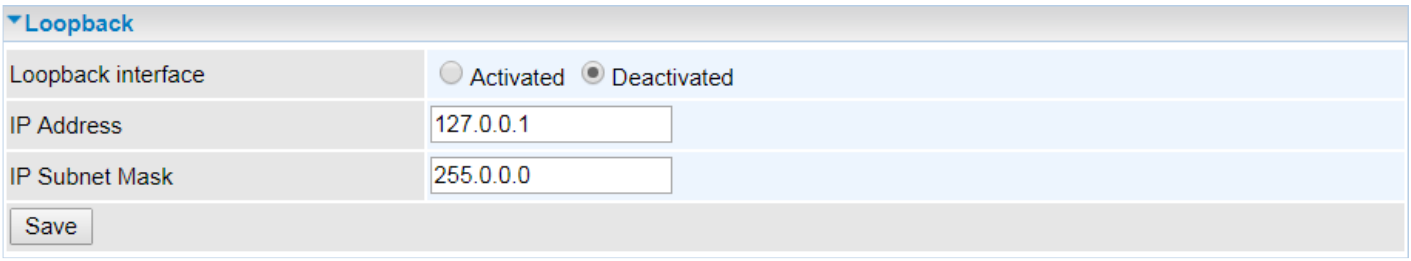
Select **Allow** to permit access to the router, MAC addresses not listed will be denied access to the router.

MAC Address: Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless station that are allowed or denied access to the specified in these address fields.

Click **Save** to apply the 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.



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 connections connected concurrently, offers a reliable Internet connectivity and maximize bandwidth utilization for critical applications delivery.

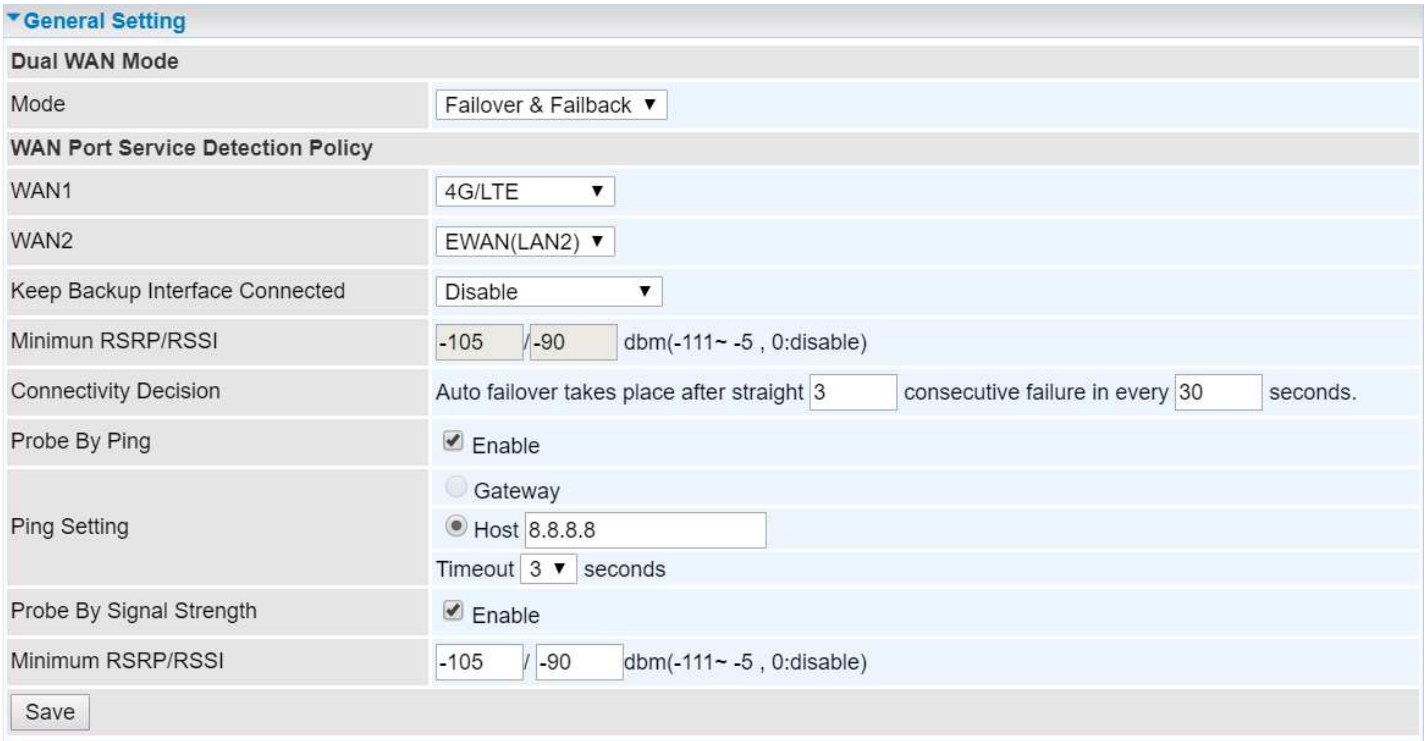
General Setting

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.



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 primaryWAN 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 -111 ~ -5. 0 means don't care/no need to check this value.

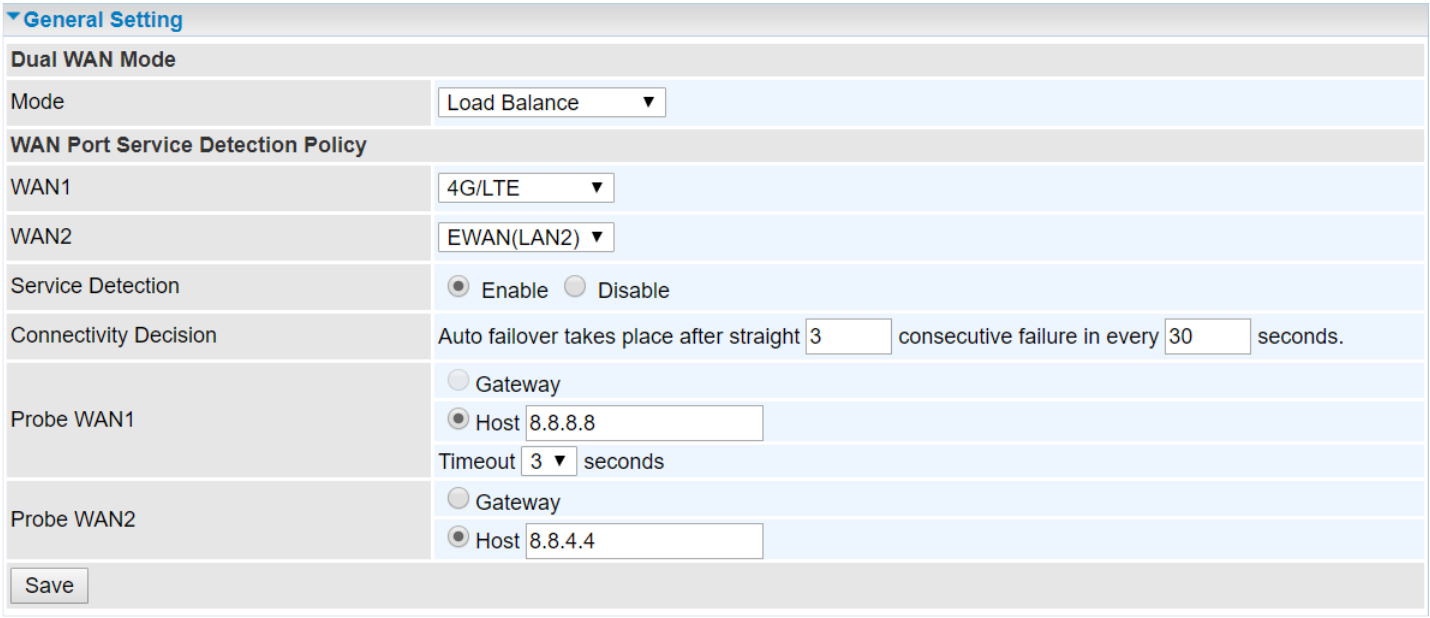
   NOTE: Both the RSRP and RSSI cannot be 0 at the same time.

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.



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: 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.

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

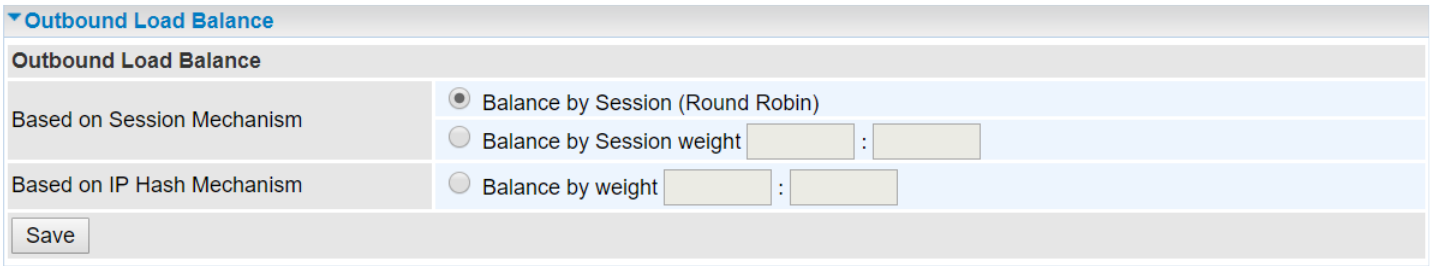
Gateway: Internal system will wait for responses to the pings from the gateway of the WAN.

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.

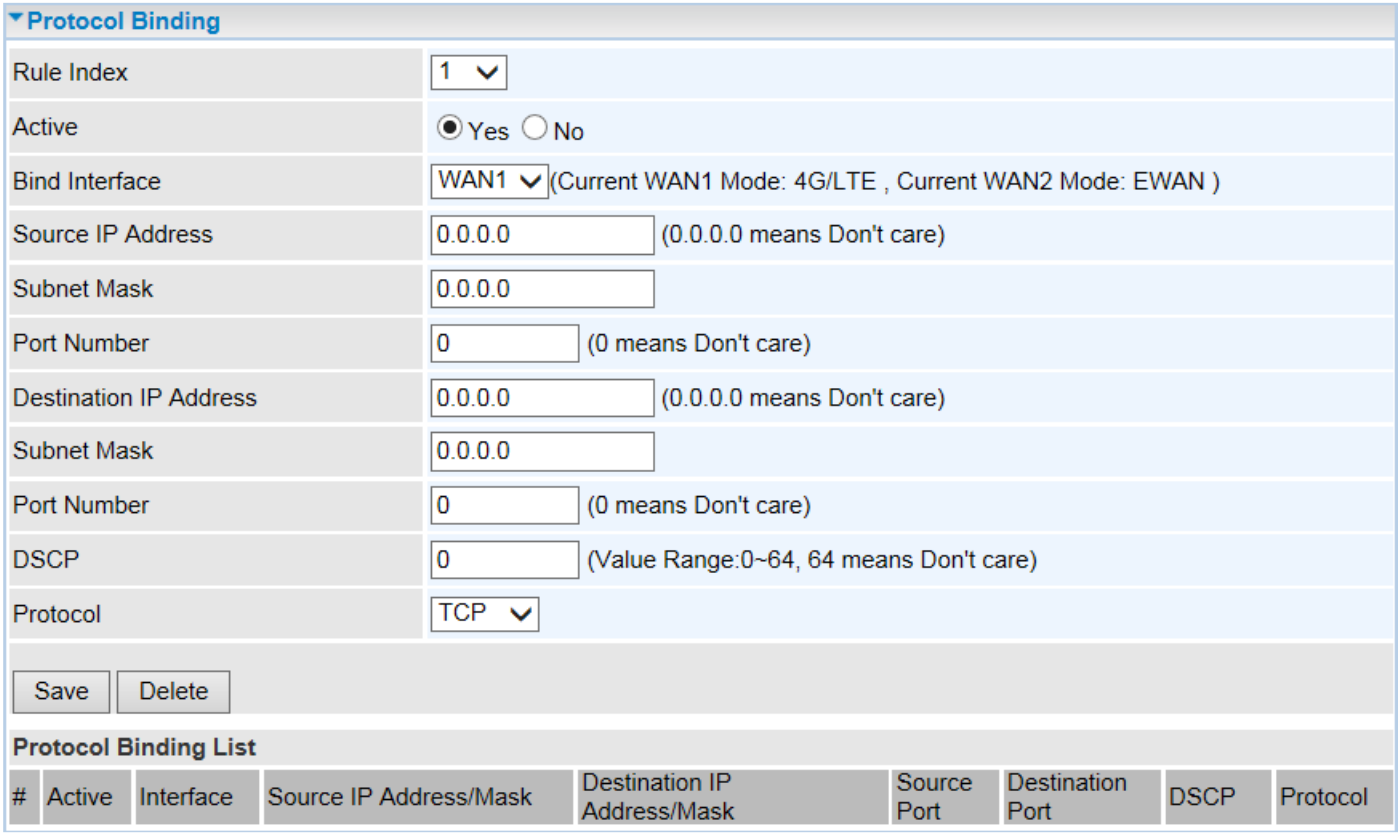
Base on IP Hash Mechanism:

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.



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

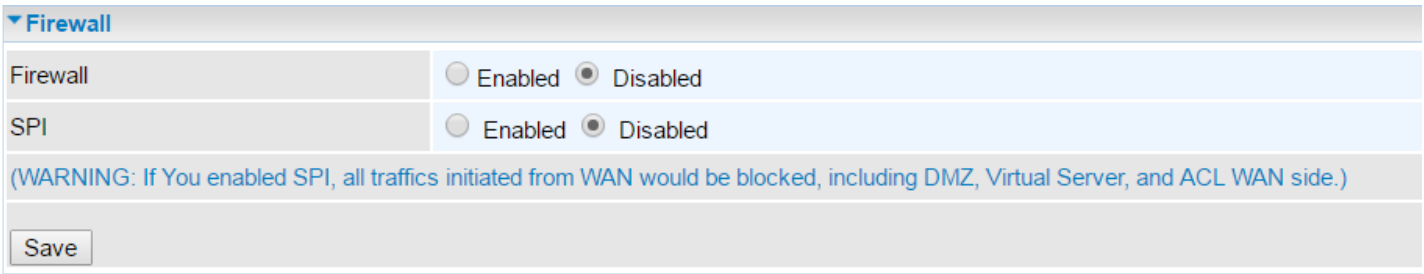
#	Active	Interface	Source IP Address/Mask	Destination IP Address/Mask	Source Port	Destination Port	DSCP	Protocol
1	Yes	WAN1	192.168.1.100/ 255.255.255.0	0.0.0.0/ 0.0.0.0	8080	0	0	TCP

Advanced Setup

Advanced configuration features provide advanced features, including Firewall, Routing, NAT, VRRP, Static DNS, QoS, Time Schedule and Mail Alert 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: 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
1	192.168.1.0	255.255.255.0	0.0.0.0	0	br0		
2	127.0.0.0	255.255.0.0	0.0.0.0	0	loopback		
3	239.0.0.0	255.0.0.0	0.0.0.0	0	br0		

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 <u>or</u> Interface: This is the gateway IP address <u>or</u> 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

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.

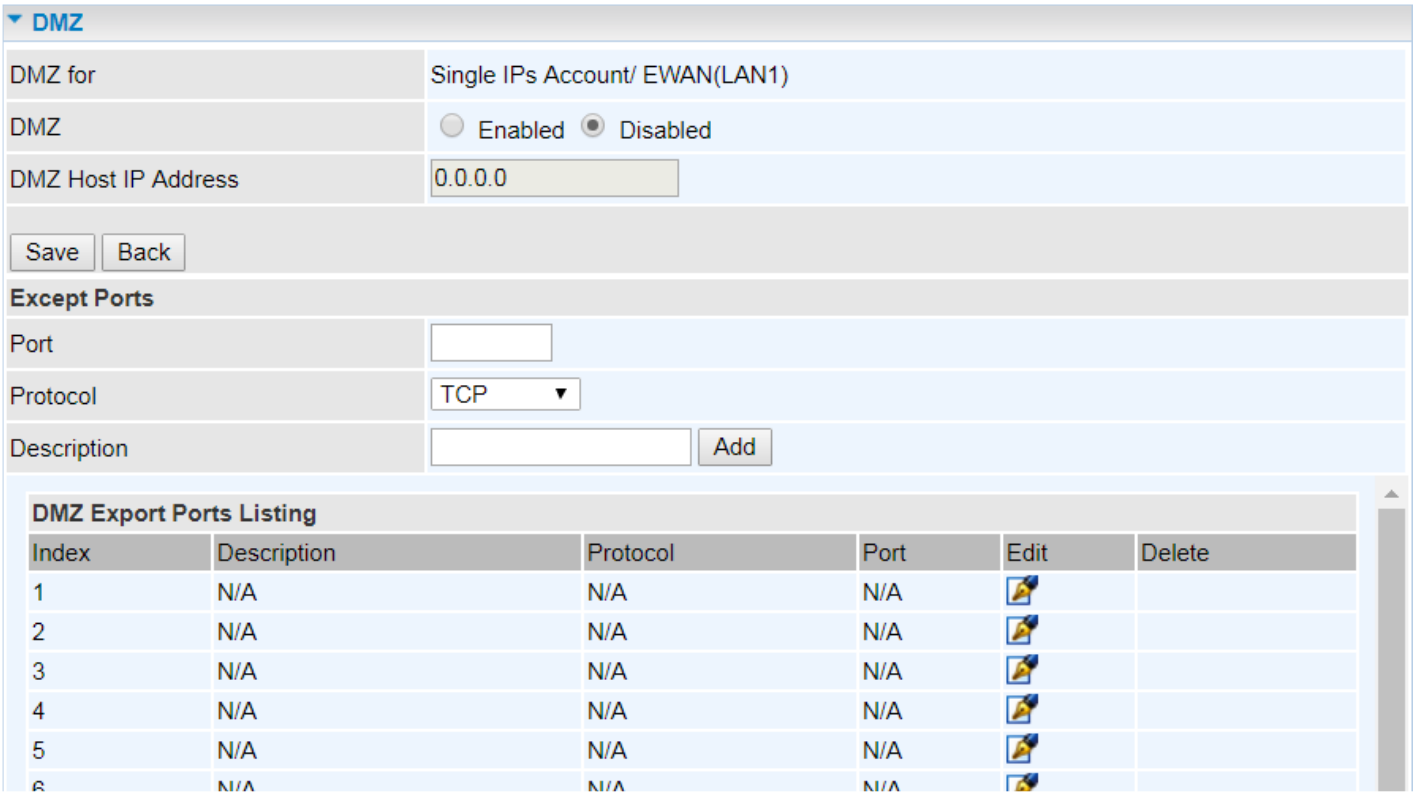
Service Index: Associated to EWAN interface marking each EWAN service (0-7), to select which EWAN service the DMZ and Virtual server are applied to.

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 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-210NP-R17AF instead of the DMZ host.

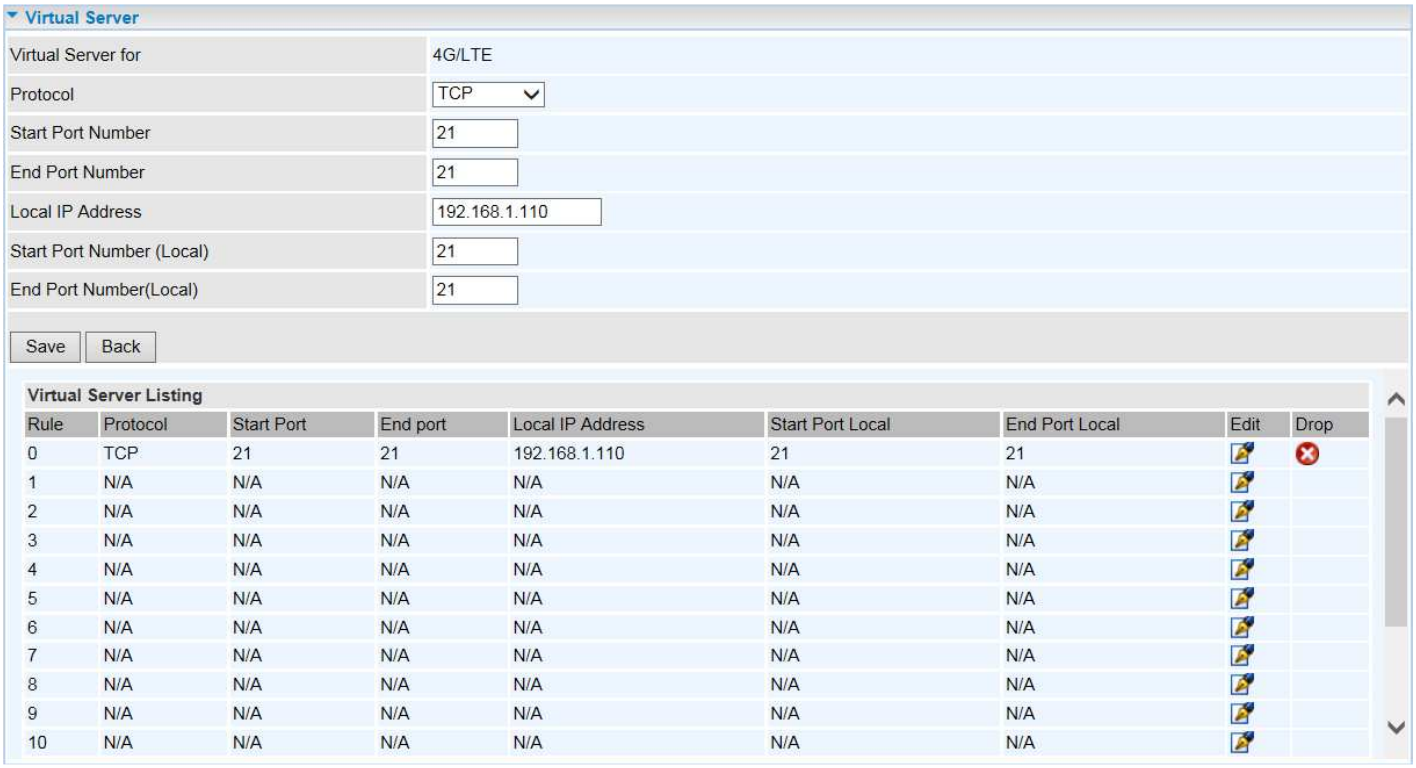
Click **Add** to add an entry to the Except Listing.

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-210NP-R17AF to direct incoming traffic to a specific device in the network.

Configure a virtual rule in MX-210NP-R17AF 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 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.

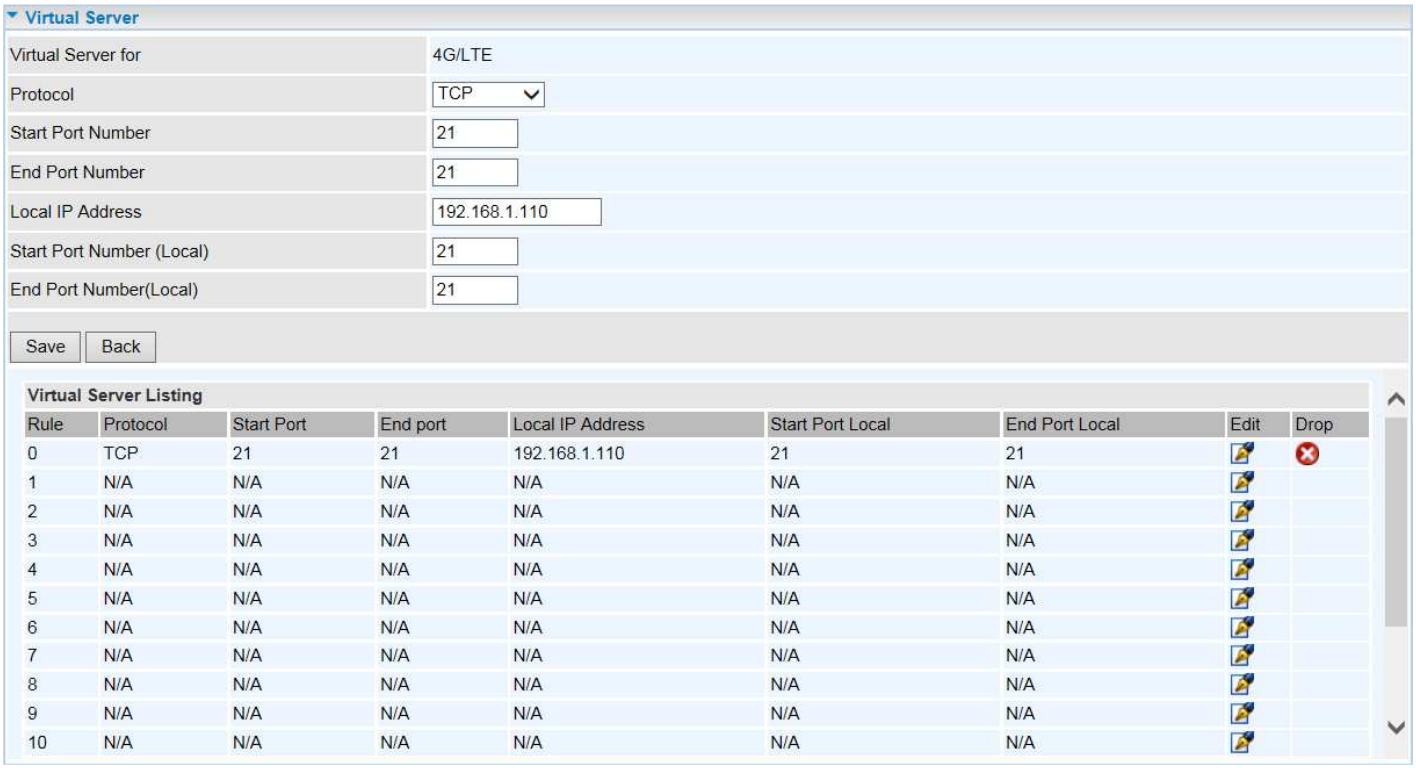
Step 2: Login to the Gateway and go to **Configuration / Advanced Setup / NAT / Virtual Server.**

FTP server uses TCP protocol with port 21.

Enter "21" to Start and End Port Number. The MX-210NP-R17AF 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-210NP-R17AF will forward port 21 request from WAN to the specific LAN PC (Example: 192.168.1.102) in the network.

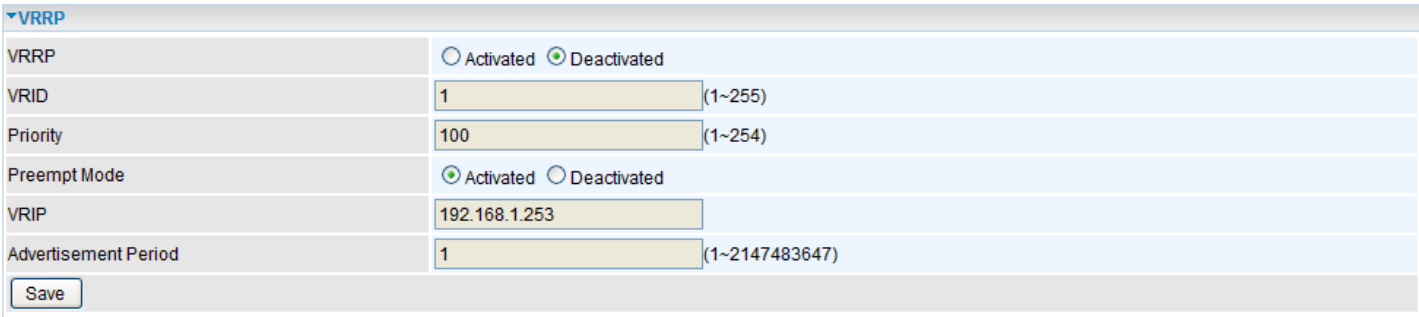
Step 3: Click **Save** to save settings.



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: 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.

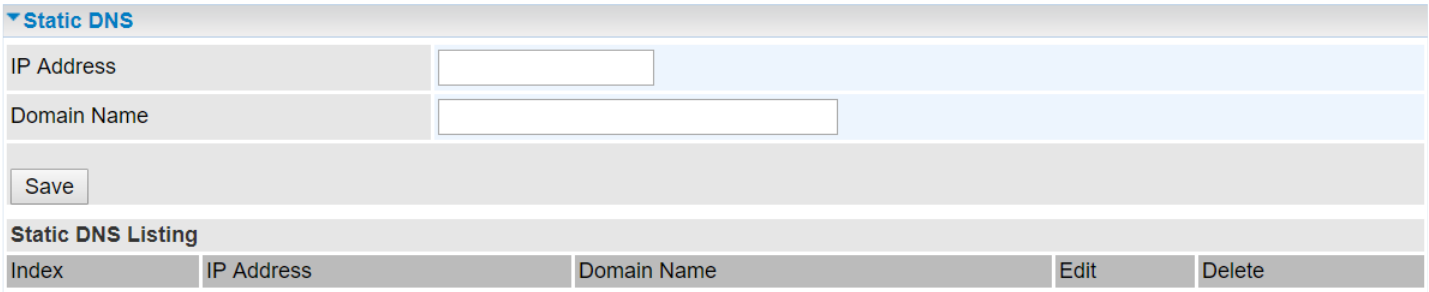
Advertisement period: Indicates the time interval in seconds between advertisements. Default in 1 second.

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 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).



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

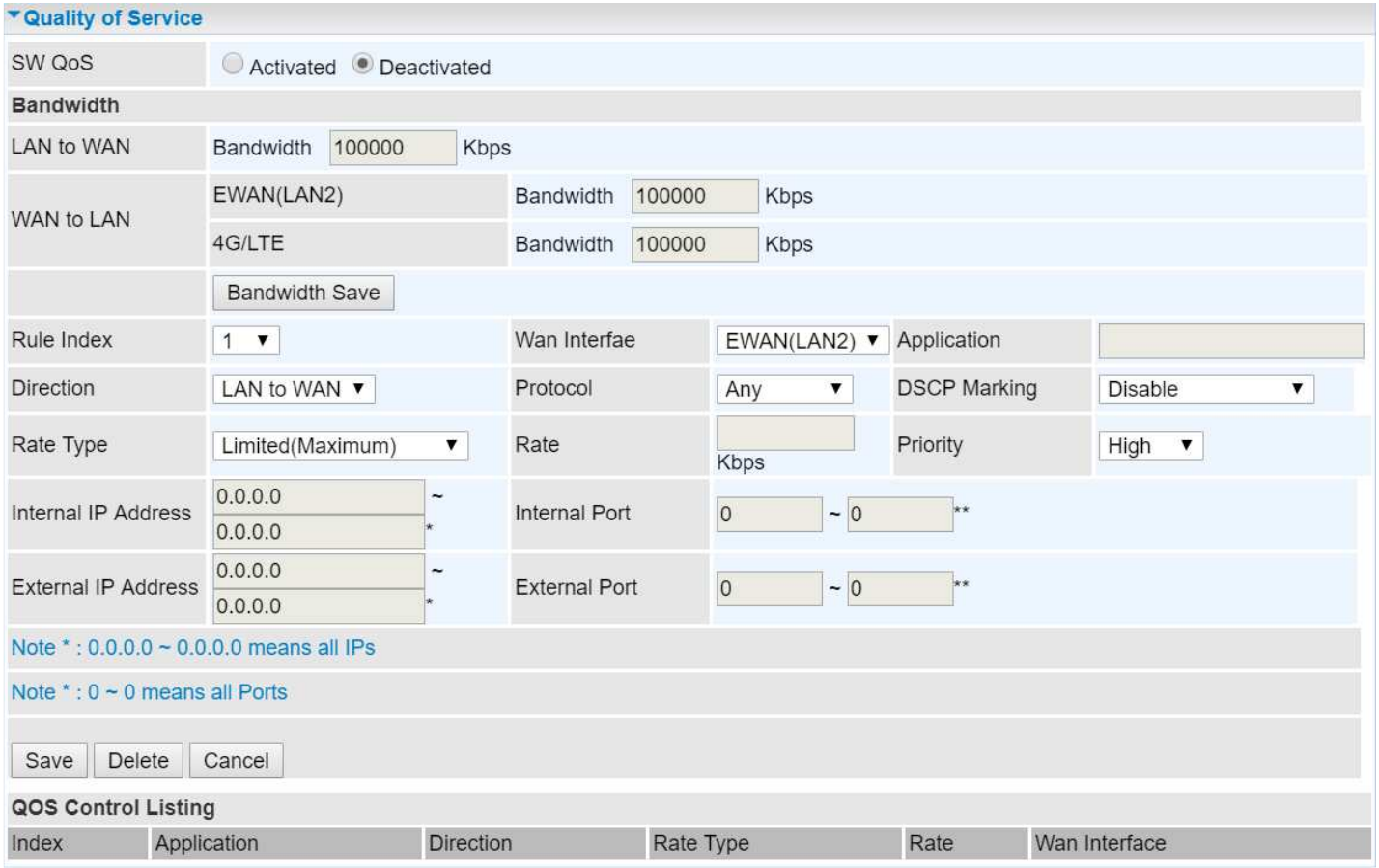
Domain Name: The friendly domain name for the IP address.

Click **Save** to apply settings.

QoS

QoS helps you control the upload traffic of each application from LAN (Ethernet and/or Wireless) to WAN (Internet).

It facilitates you the features to control the quality of throughput for each application. This is useful when there on certain types of data you want giver higher priority to, such as voice data packets given higher priority than web data packets.



SW QoS: Select **Activate** to enable the QoS

LAN to WAN (Bandwidth): You want to control the traffic from local network to the outside (Upstream). You can assign the priority for the application or you can limit the rate of the application.

Eg: you have a FTP server inside the local network, and you want to have a limited control by the QoS policy and so you need to add a policy with LAN to WAN direction setting.

WAN to LAN (Bandwidth): Control traffic from WAN to LAN (Downstream).

Click **Bandwidth Save** to save settings.

Rule Index: Index marking for each rule up to maximum of 16.

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

Application: Assign a name that identifies the new QoS application rule. Select from the list box for quick setup.

Direction: Shows the direction mode of the QoS application

Protocol: Select a protocol from the drop down list

DSCP Marking: Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to classify the traffic of the application to be executed according to the DSCP value.

Rate Type: Choose ***Limited*** (Maximum) or ***Guaranteed*** (Minimum) to specify the date rate is allowed for this policy.

Rate: Specify the date rate in Kbps.

Priority: Set the priority given to each policy/application. Specify the priority for the use of bandwidth. You can specify which application can have higher priority to acquire the bandwidth. Its default setting is set to High. You may adjust this setting to fit your policy / application.

Internal IP Address: The IP address values for Local LAN devices you want to give control.

Internal Port: The Port number on the LAN side, it is used to identify an application.

External IP Address: The IP address on remote / WAN side.

External Port: The Port number on the remote / WAN side.

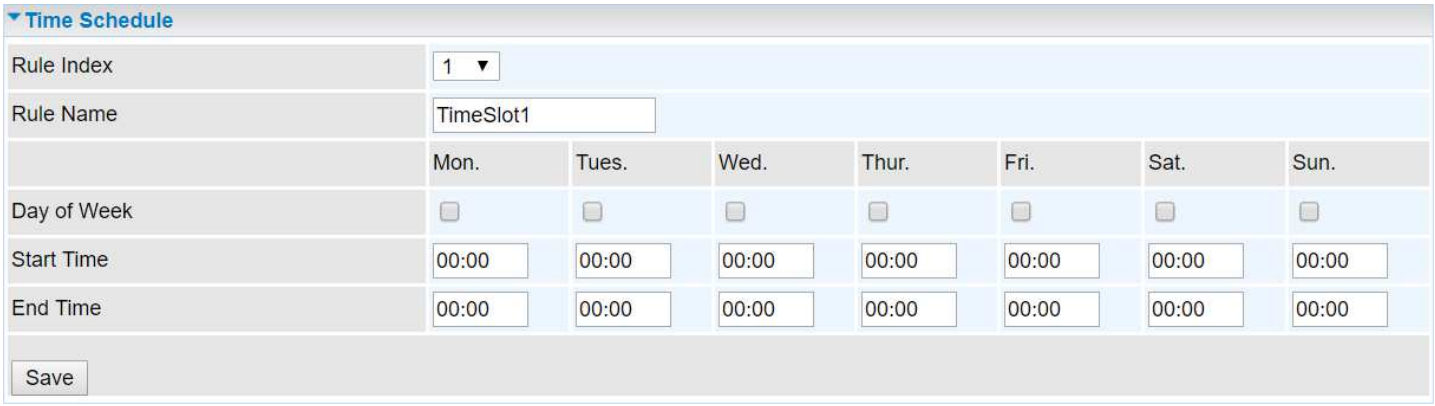
Click **Save** to apply settings.

To Remove a Policy: Simply select the Index then hit the **Delete** button to remove from the list.

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

Name: User-defined identification for each time period.

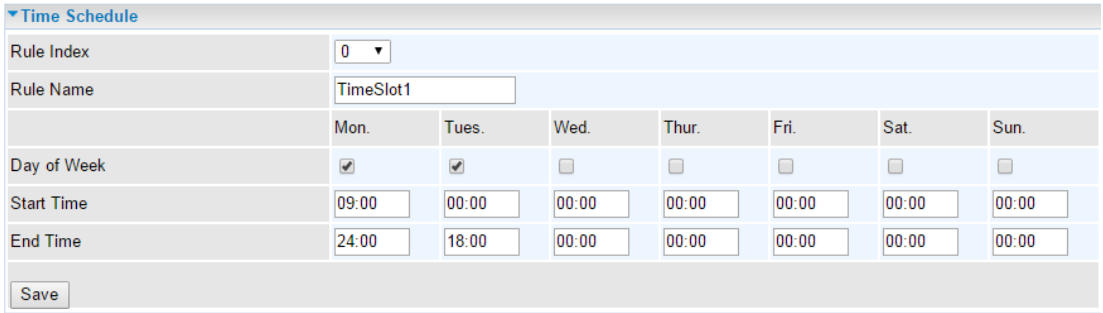
Day of Week: Mon. to Sun. Specify the time interval for each timeslot from "Day of Week".

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.

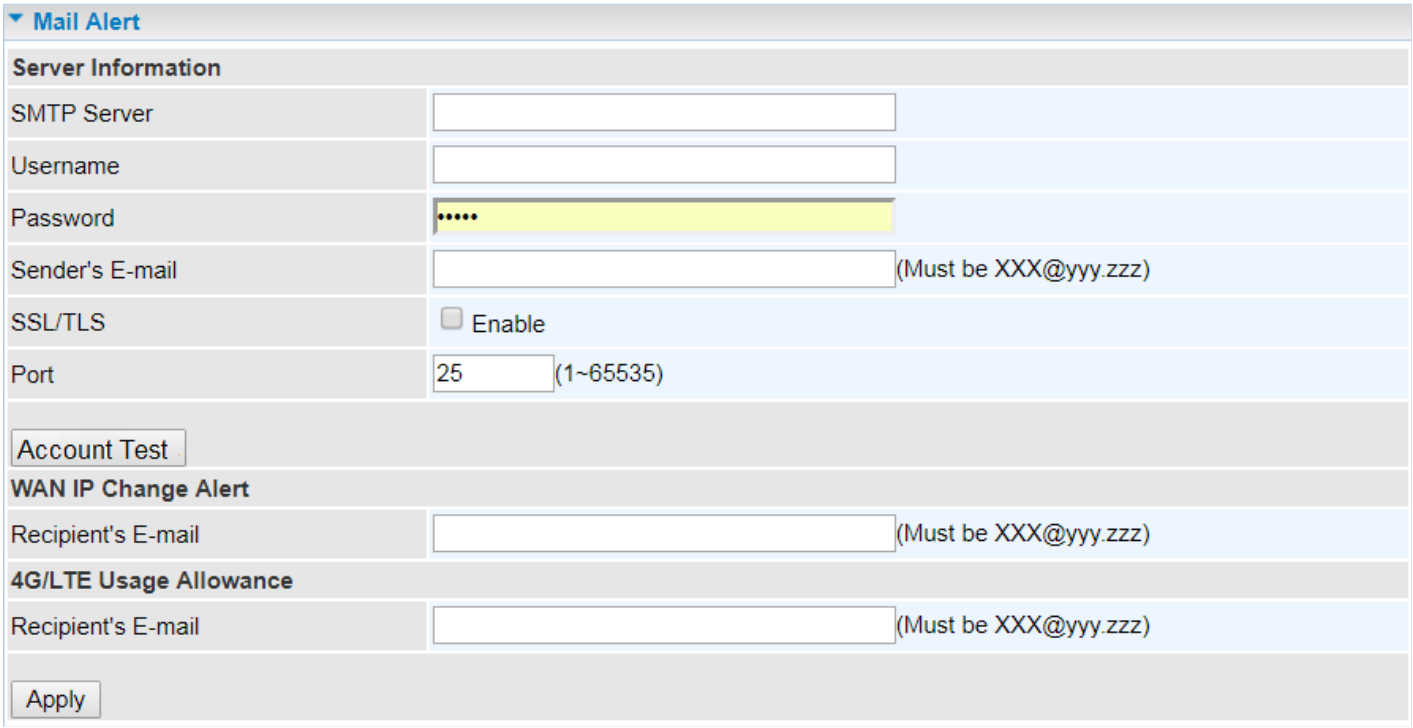
Example, you can add a timeslot named "TimeSlot1" which features a period from 9:00 of Monday to 18:00 of Tuesday.



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

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.



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

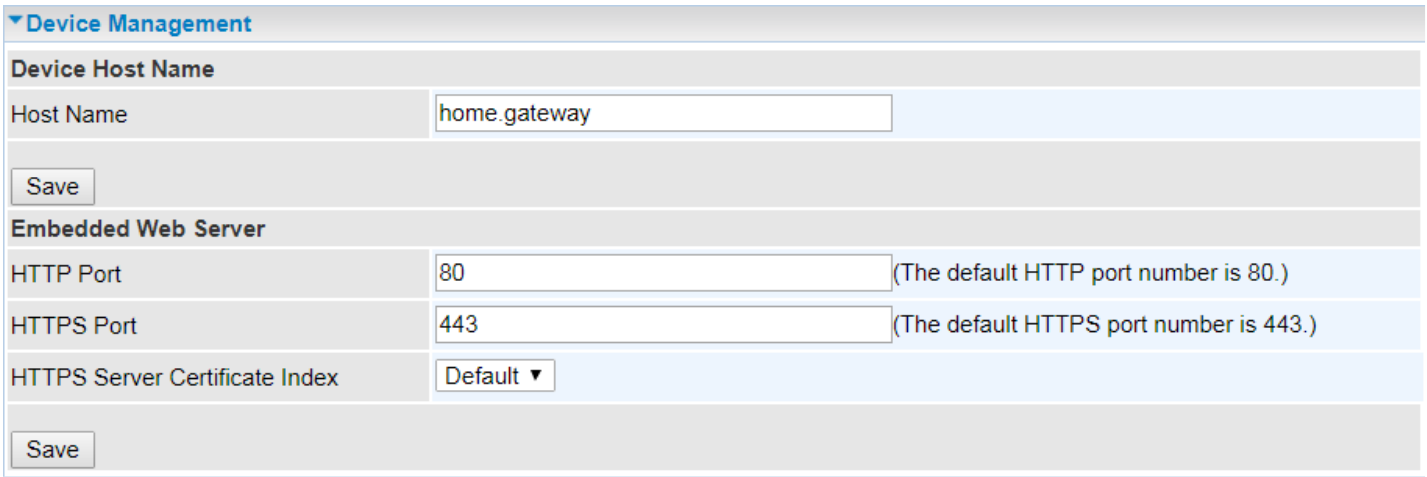
Recipient's Email (WAN IP Change Alert): Enter a valid e-mail address to receive an alert message when WAN IP change has been detected.

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

Click **Apply** button to save settings

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-210NP-R17AF 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	
Interface	ALL
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.

Interface: Select the access interface. Choices are **LAN** or **ALL** (Both LAN and WAN).

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.

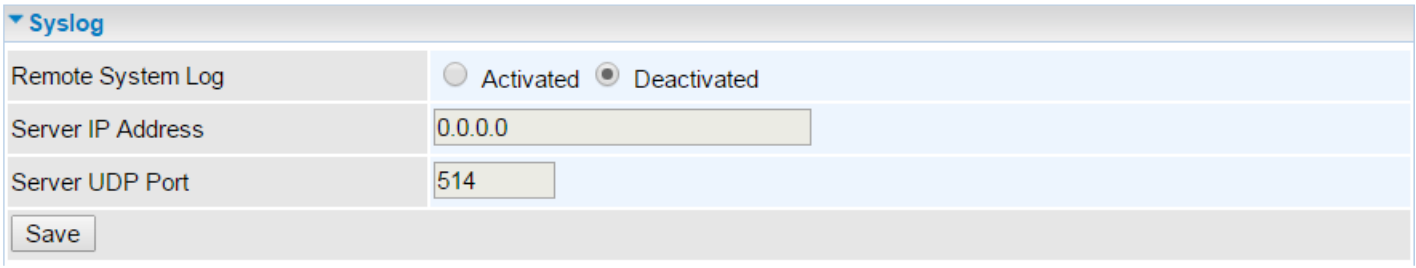
Privacy Protocol: Select the privacy mode, DES and AES.

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.



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

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

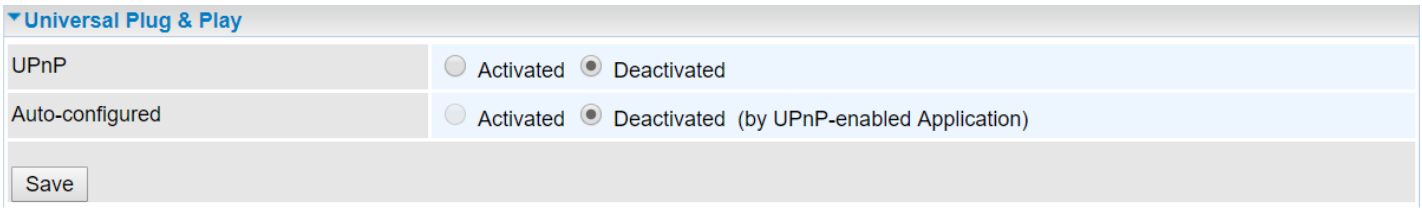
Server UDP Port: Assign the remote log server port, 514 is commonly used.

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.



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-210NP-R17AF's IP address

Auto-configured: Select this check box to allow UPnP-enabled applications to automatically configure the MX-210NP-R17AF so that they can communicate through the MX-210NP-R17AF, 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.

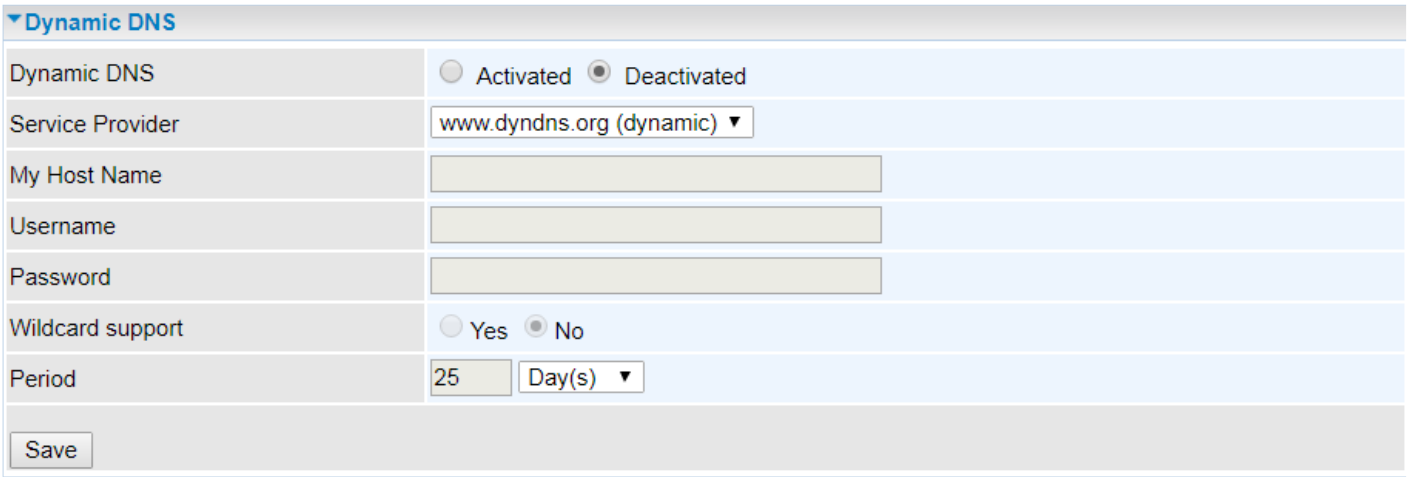
Click **Save** to apply settings.

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: 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-210NP-R17AF 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: Setup a time on how often the MX-210NP-R17AF 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.

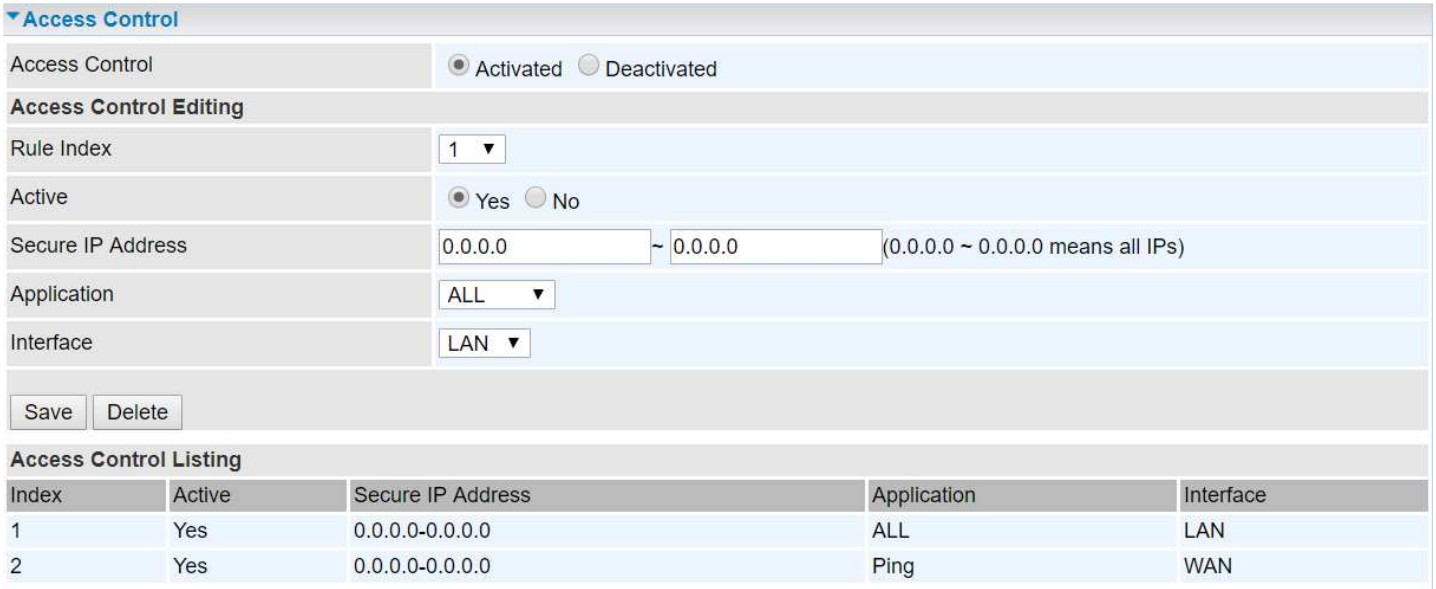
User ***test1*** register a Dynamic Domain Names in DDNS provider **http://www.dyndns.org/** .

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-210NP-R17AF 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: 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-210NP-R17AF. Type an IP address range to restrict access to the client(s) without a matching IP address.

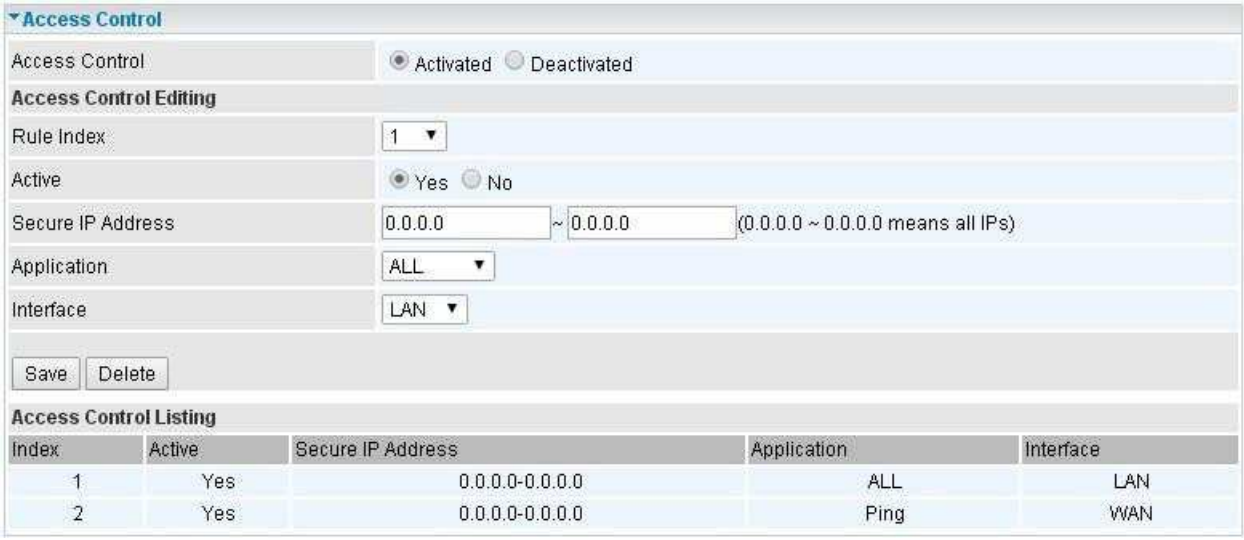
Application: Choose a service that you want to all access to all the secure IP clients. The drop-down menu lists all the common used applications.

Interface: Select the access interface. Choices are **LAN**, **WAN**, **GRE** and **ALL**.

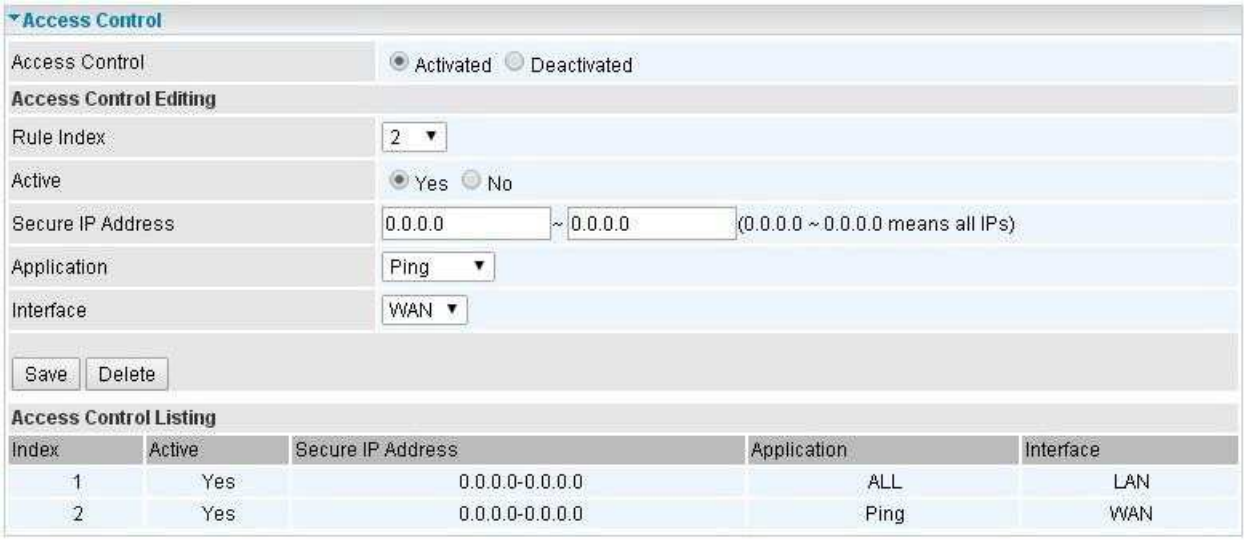
Click **Save** to apply settings.

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	
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

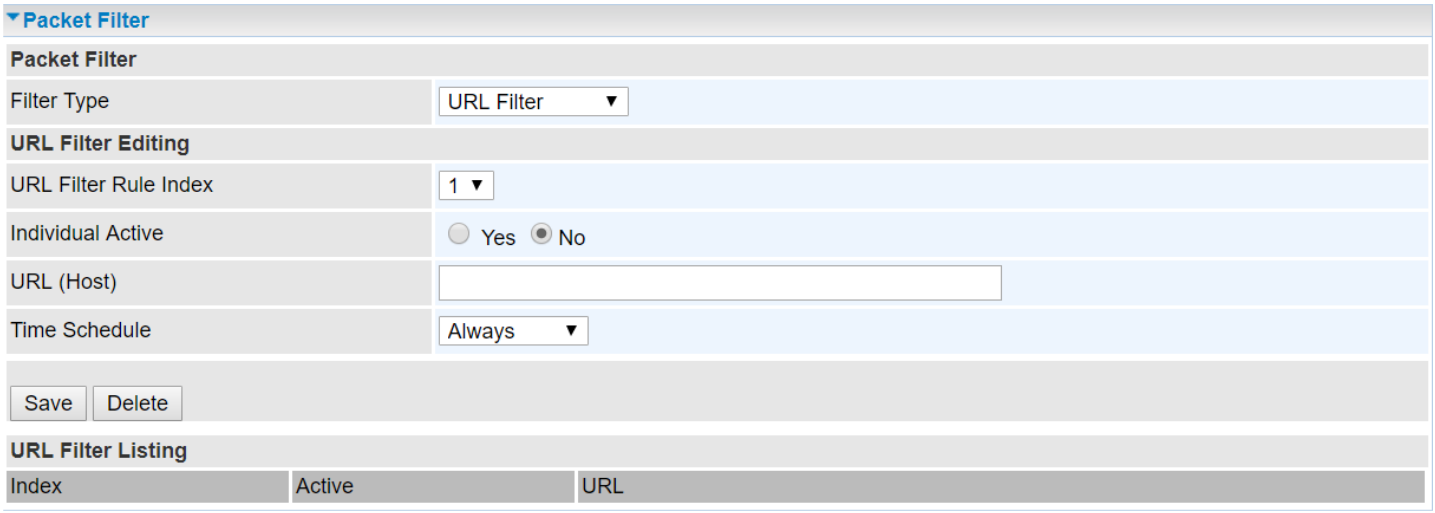
Type	MAC
Source MAC Address	

Source MAC Address: show the MAC address of the rule applied.

Time Schedule: Select a TimeSlot to activate the rule. Go to **Time Schedule** to configure a time control first.

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.

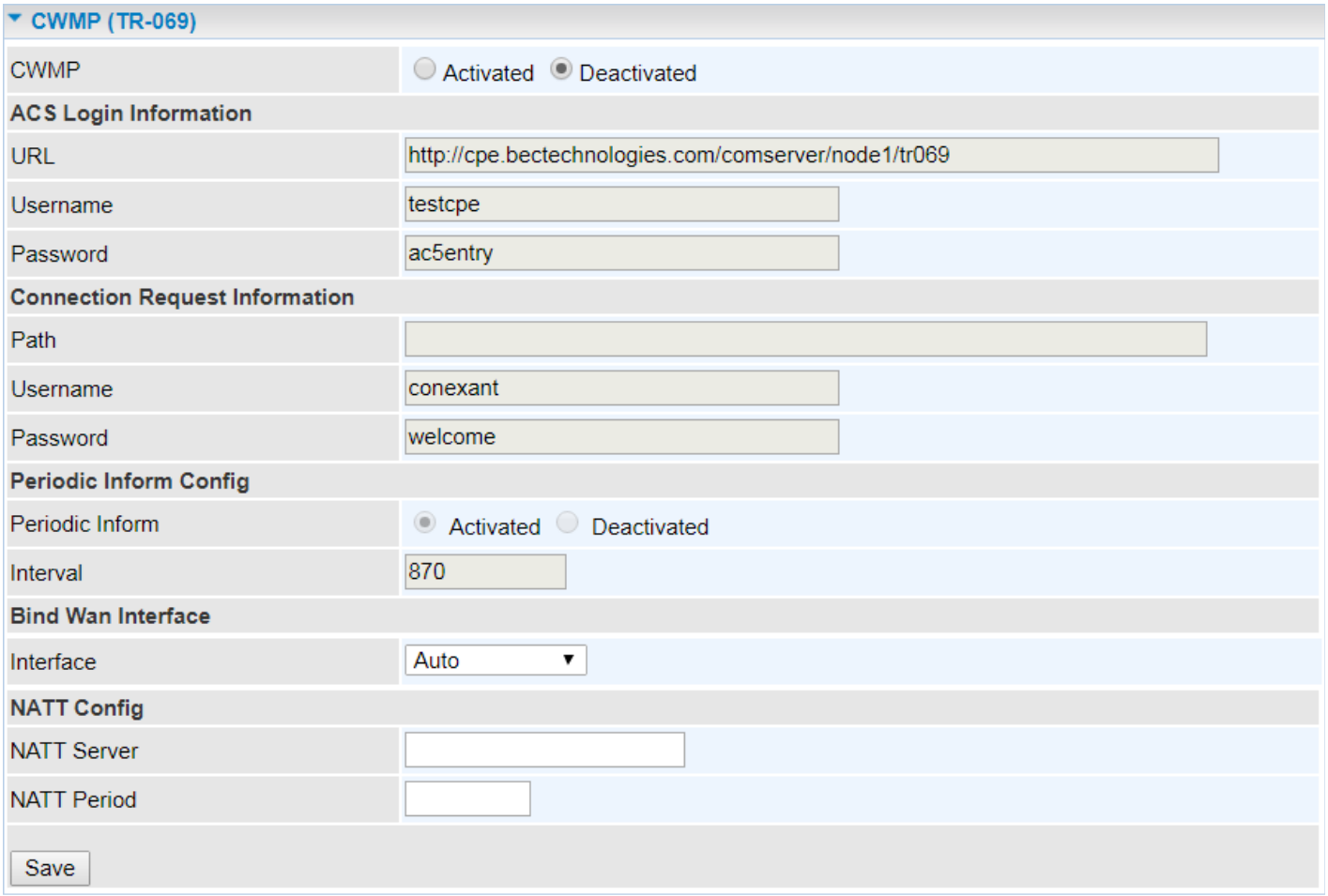
Time Schedule: Select a TimeSlot to activate the rule. Go to **Time Schedule** to configure a time control first.

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: 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

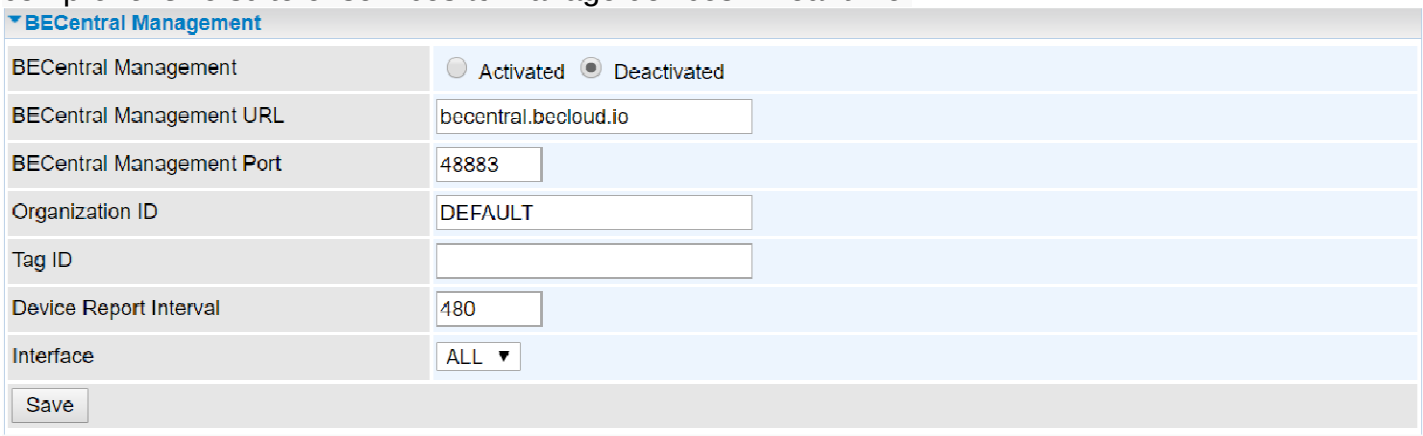
Host Name: It is the domain name of your OpenDNS. If you don't have one, please leave it blink.

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: 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 (By BE C administrator only)

Tag ID: By BEC administrator only.

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.

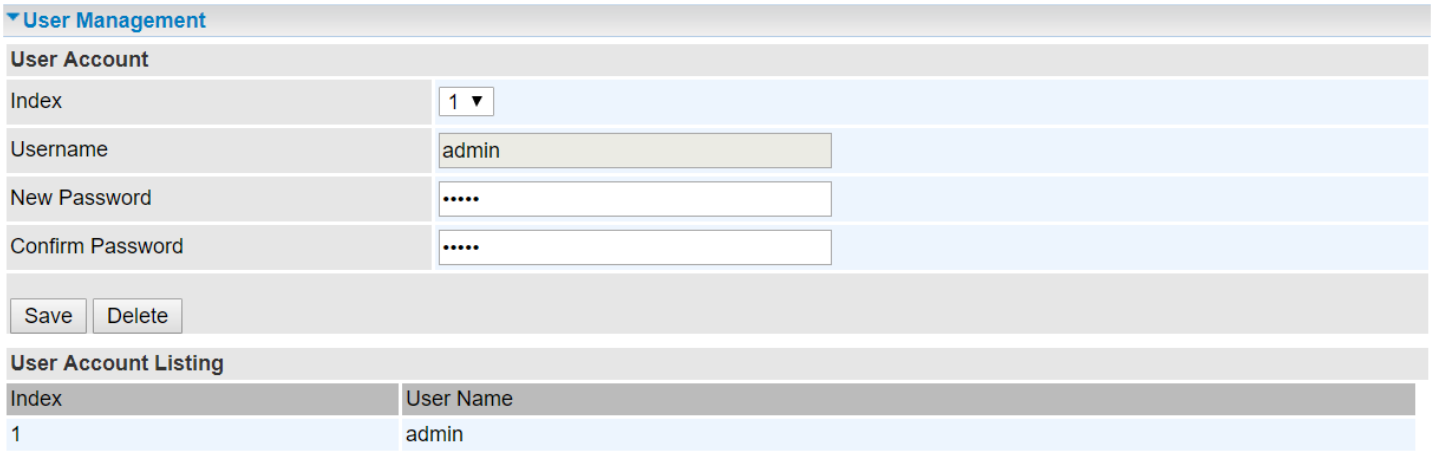
Total of **8** accounts can be created to grant access to manage the MX-210NP-R17AF via the web page.

❖ 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 Setup

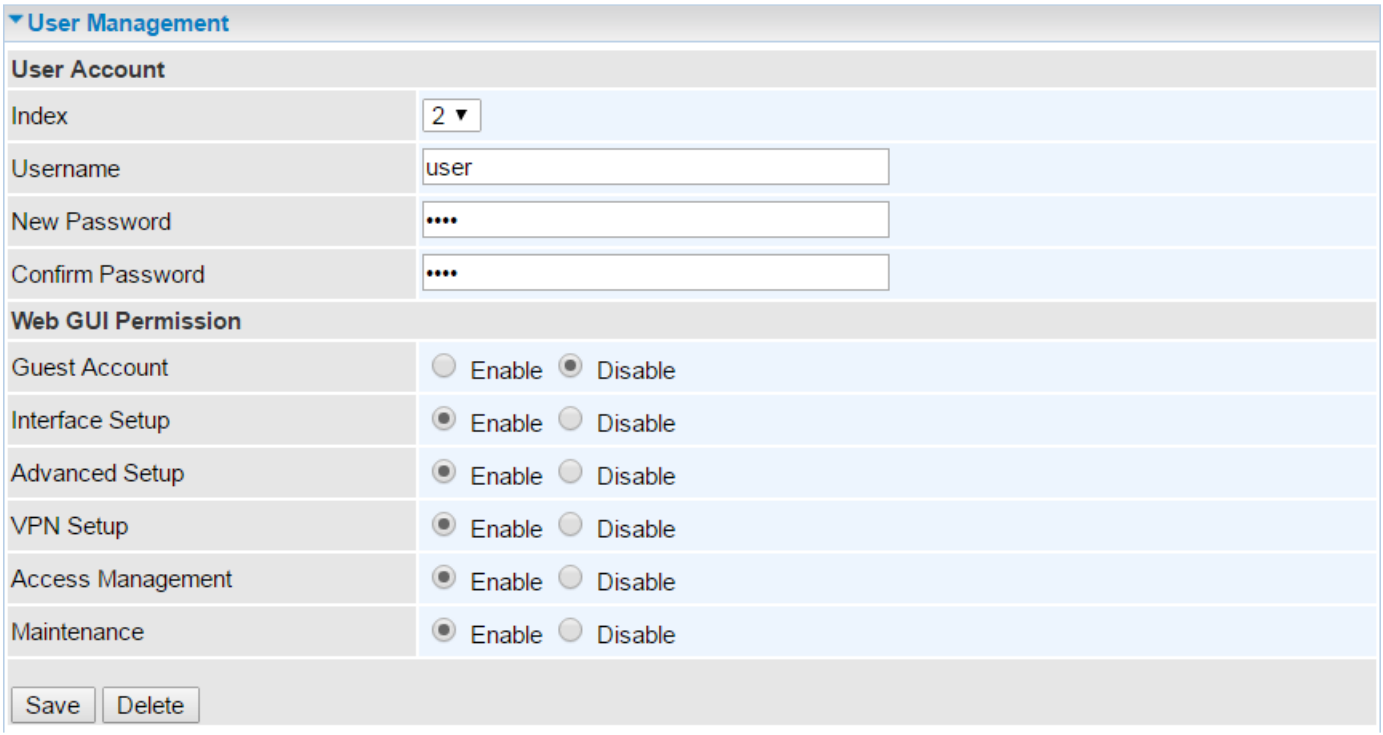
Index: The numeric account indicator. The maximum entry is up to 8 accounts.

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 exactly the same as in the previous field

❖ Other Account



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-210NP-R17AF 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.

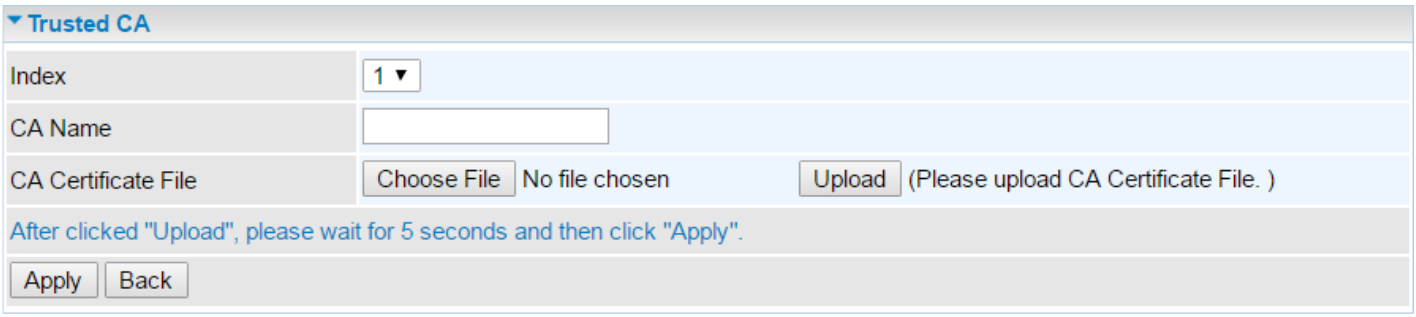
Certificate File: Browse to locate the target certificate file on PC before uploading it.

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



Index #: The numeric account indicator. The maximum entry is up to 2.

CA Name: Description of the CA.

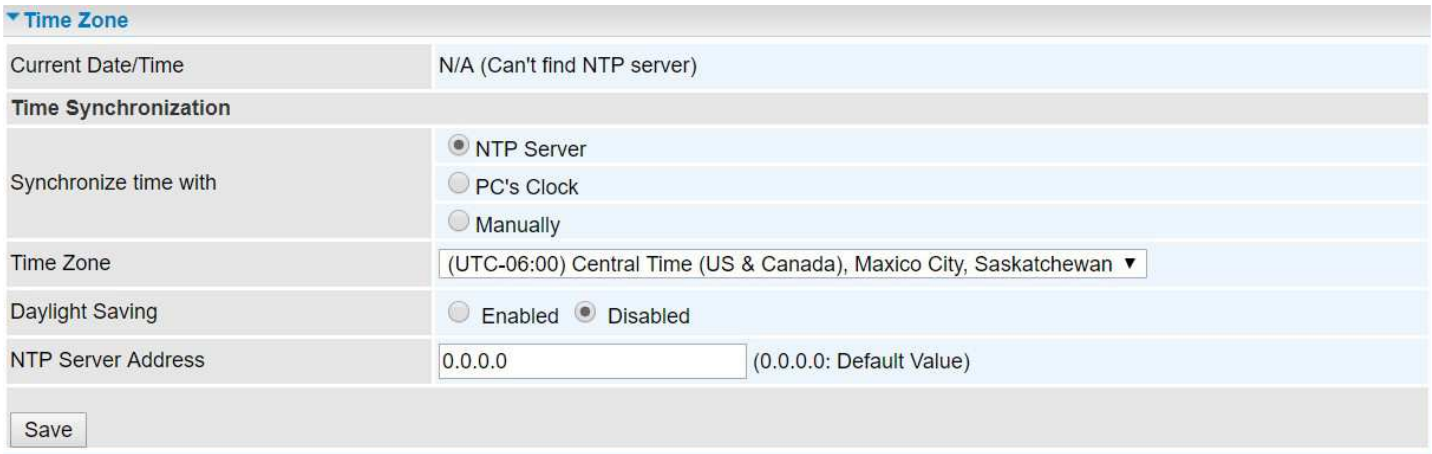
CA Certificate File: Browse to locate the target certificate file on PC before uploading it.

Click **Apply** to save settings.

Time Zone

With default, MX-210NP-R17AF 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-210NP-R17AF. If you plan to use **Time Schedule** feature, it is extremely important you set up the Time Zone



correctly.

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-210NP-R17AF 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.

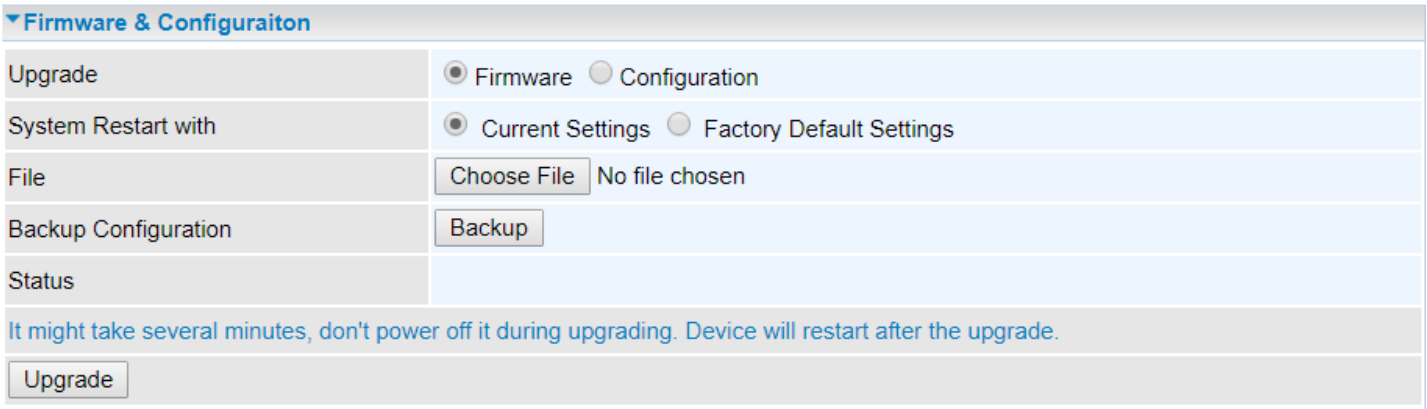
NTP Server Address: Enter the IP address of your time server. Check with your ISP/network administrator if you are unsure of this information.

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-210NP-R17AF provides an effortless way to update the code to take advantage of the changes.

To upgrade the firmware of the MX-210NP-R17AF, 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-210NP-R17AF will automatically restart and run the new firmware.



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 if you need this configuration file to be restored back to your MX-210NP-R17AF device when making false configurations and want to restore to the original settings.

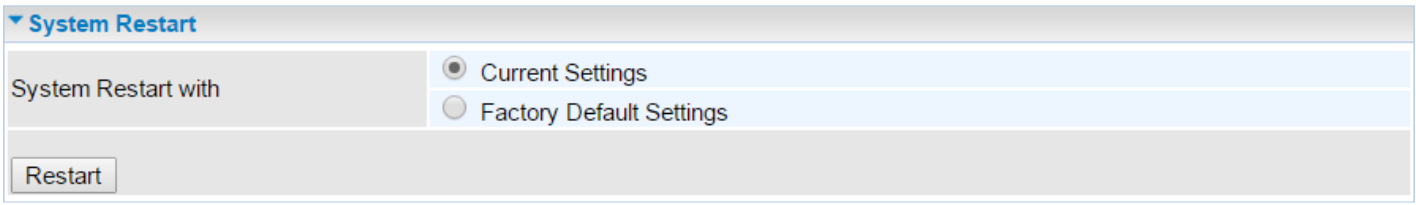
Upgrade: Click **"Upgrade"** to begin the upload process. This process may take up to two minutes.

DO NOT turn off or power cycle the device while firmware upgrading is still in process.

Improper operation could damage your MX-210NP-R17AF.

System Restart

Click **System Restart** with option **Current Settings** to reboot your router.

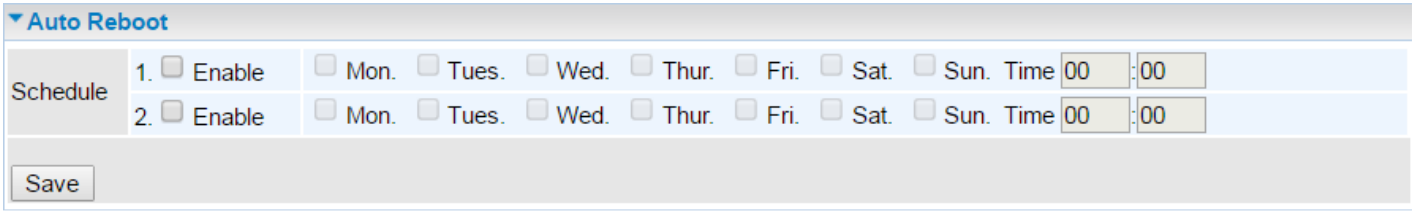


If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select **Factory Default Settings** to restore to factory default settings.

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

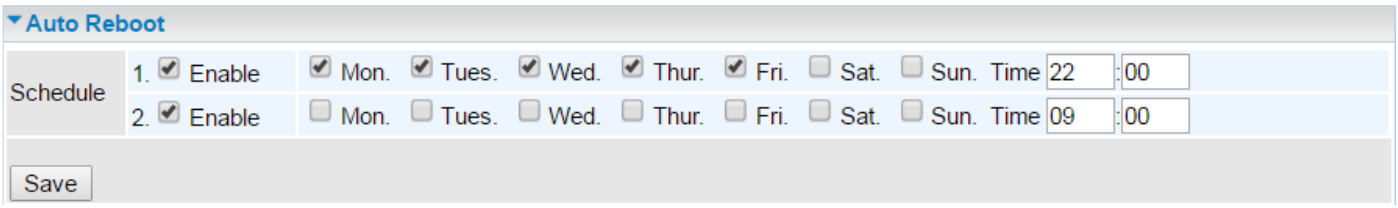
Schedule an automatic reboot for your MX-210NP-R17AF to ensure proper operation and best performance. This reboot will only reboot with current configuration settings and not overwrite any



existing settings.

Click **Save** to apply settings

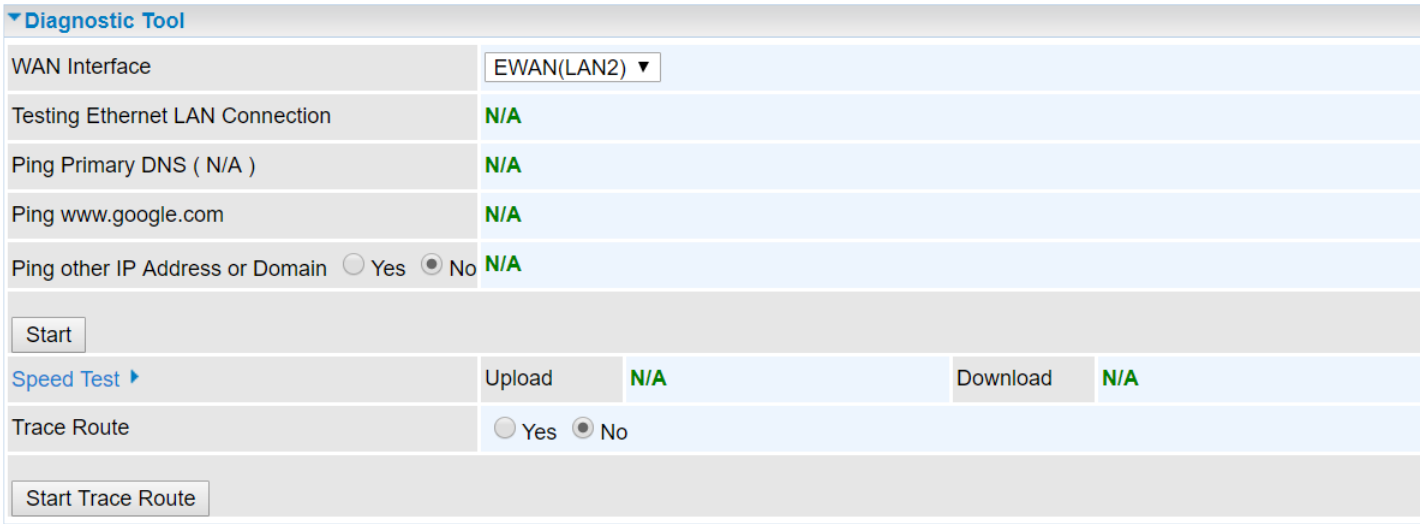
Example: Schedule MX-210NP-R17AF to reboot at 10:00pm (22:00) every weekday (Monday thru Friday) and reboot at 9:00am on Saturday and Sunday.



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.

4G-LTE / EWAN (LAN2)

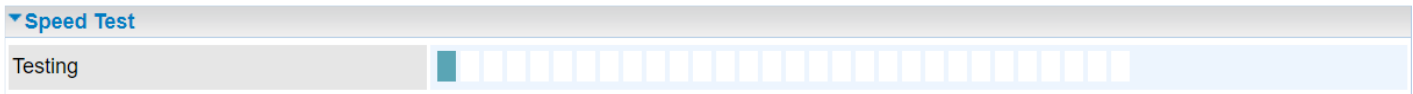


Ping other IP Address: Click **Yes** if you wish to ping other IP address rather than google.com

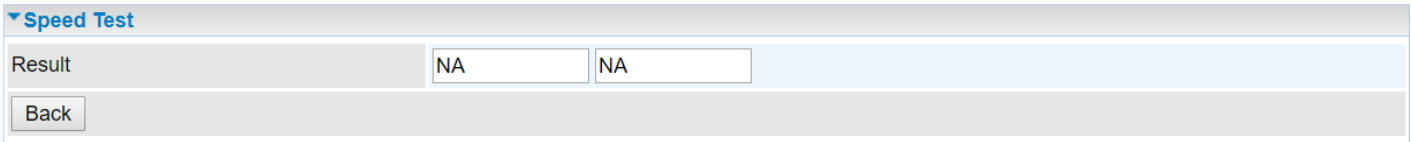
Click **START** to begin to diagnose the connection.

Speed Time: Measure the current uplink and downlink speed rate.

Take less than a minute to run the test.



Result in Uplink / Downlink



Click **Back** to go back to the Diagnostic Tool

Trace Route is to display how many hops (also view the exact hops) required to get to the destination.

Click **Yes**, enter the IP address or domain then **Start Trace Route**.

Trace Route ◉ Yes ○ No	
IP Address or Domain	
Max TTL Value	16 [2-30]
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	N/A			
Ping other IP Address or Domain ○ Yes ◉ No	N/A			
Start				
Speed Test ▸	Upload	NA	Download	NA

Ping other IP Address: Click **Yes** to ping any desired IP address or a domain.

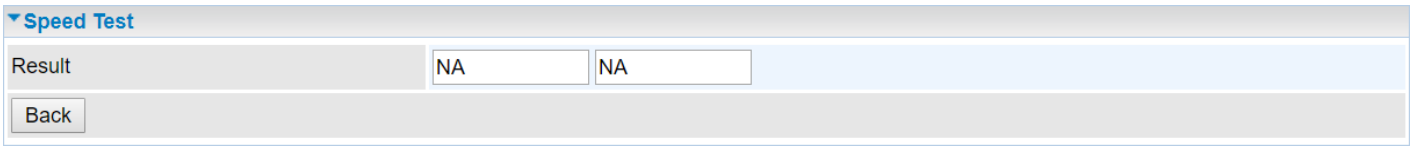
Speed Time: Measure the current uplink and downlink speed rate.

Take less than a minute to run the test.

Speed Test

Testing	

Result in Uplink / Downlink



Click **Back** to go back to the Diagnostic Tool

Click **START** to begin to diagnose the connection.

Chapter 5: Troubleshooting

If your MX-210NP-R17AF 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-210NP-R17AF

APPENDIX: PRODUCT SUPPORT & CONTACT

If you come across any problems please contact the dealer from where you have purchased the product.

Contact BEC @ http://www.bectechnologies.net

MAC OS is a registered Trademark of Apple Computer, Inc.

Windows 10/8/7 are registered Trademarks of Microsoft Corporation

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.

V1041235