

User Manual

BEC MX-1000

Advanced In-Vehicle 4G/LTE Wireless M2M Router



TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION	1
INTRODUCTION TO YOUR ROUTER	1
FEATURES & SPECIFICATIONS	3
HARDWARE SPECIFICATIONS	6
APPLICATION DIAGRAMS	7
CHAPTER 2: PRODUCT OVERVIEW	8
IMPORTANT NOTE FOR USING THIS ROUTER	8
DEVICE DESCRIPTION	9
SYSTEM RECOVERY PROCEDURES	12
CABLING	12
CHAPTER 3: BASIC INSTALLATION	13
NETWORK CONFIGURATION – IPv4	14
Configuring PC in Windows 7/8 (IPv4)	14
Configuring PC in Windows Vista (IPv4)	16
Configuring PC in Windows XP (IPv4)	18
NETWORK CONFIGURATION – IPv6	20
Configuring PC in Windows 7/8 (IPv6)	20
Configuring PC in Windows Vista (IPv6)	22
Configuring PC in Windows XP (IPv6)	24
DEFAULT SETTINGS	25
CHAPTER 4: DEVICE CONFIGURATION	26
LOGIN TO YOUR DEVICE	26
STATUS	28
Device Info	29
System Log	31
3G/4G-LTE Status	32

GPS Status	34
Hardware Monitor	34
Statistics	35
DHCP Table.....	39
Disk Status.....	39
QUICK START	40
CONFIGURATION.....	43
Interface Setup.....	43
<i>Internet</i>	44
<i>LAN</i>	51
<i>Wireless</i>	55
<i>Wireless MAC Filter</i>	66
Advanced Setup	67
<i>Firewall</i>	67
<i>Routing</i>	68
<i>NAT</i>	69
<i>Static DNS</i>	74
<i>Time Schedule</i>	75
<i>Mail Alert</i>	76
<i>Remote System Log</i>	77
Access Management	78
<i>Device Management</i>	78
<i>SNMP</i>	79
<i>Universal Plug & Play</i>	80
<i>Dynamic DNS (DDNS)</i>	81
<i>Access Control</i>	83
<i>Packet Filter</i>	85
<i>CWMP (TR-069)</i>	89
<i>Parental Control</i>	91
<i>SAMBA & FTP Server</i>	92
Maintenance	95
<i>User Management</i>	95
<i>Time Zone</i>	99
<i>Firmware & Configuration</i>	100
<i>System Restart</i>	101
<i>Auto Reboot</i>	102
<i>Diagnostics Tool</i>	103
CHAPTER 5: TROUBLESHOOTING	104

Problems with the Router	104
Problem with LAN Interface	104
Recovery Procedures.....	105

APPENDIX: PRODUCT SUPPORT & CONTACT

..... **106**

CHAPTER 1: INTRODUCTION

Introduction to your Router

The MX-1000 Advanced Industrial 4G/LTE Wireless VPN Router is a high-performance all-in-one wireless communications platform with advanced software enabling high availability, reliable and secure connectivity for mission critical applications. The MX-1000 is specifically designed to provide outstanding network efficiency and internet security for a wide range of applications and vertical machine-to-machine (M2M) market segments. It features a rugged, compact design with integrated dual 4G/LTE WAN ports, 4-port Gigabit Ethernet switch, 802.11n Wi-Fi access point with multiple SSID supports, and two multi-function USB 2.0 host interfaces for Storage/NAS. Quality of Service (QoS), SPI firewall, and advanced VPN integration provide security needed to enhance the operations of Public Safety, Energy Wellhead and Gas Industry, Industrial M2M Segment, PoS/Kiosks/ATM, Fleet Management, and Smart Transportation/Bus.

Vehicle Tracking System

MX-1000 is embedded with a GNSS receiver for GPS or GLONASS. To co-work with On-Board Diagnostics(OBD) system, it eases the central control of geographically-dispersed fleets by presenting individual vehicles' detailed information, including remaining fuel levels, rapid accelerations, and locations.

4G/LTE Mobility

To offer an advanced network solution that meets the growing demands of M2M services, MX-1000 exclusively features dual WAN - load balance or auto-failover/failback to provide extraordinary, always-on internet connectivity. In addition to the deployment of Dual 4G LTE modules and Dual SIMs, MX-1000 broadens wireless coverage to rough terrains and rural areas and persists seamless connectivity without interruptions

Robust Design to Withstand in the Harshest Environments

The industrial-grade enclosure is designed to resist heat, dust, moisture and provides long-term operation in the toughest of environments. MX-1000 supports an extended temperatures range from -40 to 140° F (-40 to 60° C) for extremely challenging conditions such as industrial automation, mining plants, wellhead & gas drilling, manufacturing factories, and virtually anywhere that requires a robust wireless connection.

Wireless Mobility and Security

With an integrated 802.11n Wireless Access Point, this router delivers up to 3 times the wireless coverage of a 802.11b/g network device, so that wireless access is available everywhere in the house or office. If your network requires wider coverage, the built-in Wireless Distribution System (WDS) allows you to expand your wireless network without additional wires or cables. MX-1000 also supports the Wi-Fi Protected Setup (WPS) standard and allows users to establish a secure wireless network

just by pressing a button. Multiple SSIDs allow users to access different networks through a single access point. Network managers can assign different policies and functions for each SSID, increasing the flexibility and efficiency of the network infrastructure.

Secure VPN Connections (Optional)

The MX-1000 supports comprehensive and robust IPsec VPN (Virtual Private Network) protocols for business users to establish private encrypted tunnels over the public Internet to secure data transmission between headquarters and branch offices. It also supports VPN dial in from smart phones for secure remote Internet connection via your home broadband. With a built-in DES/3DES VPN accelerator, the router enhances IPsec VPN performance significantly.

IPv6 Supported

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

Quick Start Wizard

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

Firmware Upgradeable

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

Features & Specifications

- Dual 4G LTE broadband connectivity (3G Fallback optional)
- Dual-WAN 4G LTE interface for network expandability and reliable connectivity
- High performance antenna for increased coverage, signal reception and efficiency
- Embedded GNSS engine for real-time asset tracking and location data-based applications
- Enterprise level routing functionality
- Gigabit Ethernet WAN (GbE WAN) for Cable/Fiber/xDSL high WAN throughput
- Gigabit Ethernet LAN
- IPv6 ready (IPv4/IPv6 dual stack)
- Multiple wireless SSIDs with wireless guest access and client isolation
- IEEE 802.11 b/g/n compliant Wireless Access Point with Wi-Fi Protected Setup (WPS)
- Wi-Fi Protected Access (WPA-PSK/ WPA2-PSK) and Wired Equivalent Privacy (WEP)
- 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
- USB port for NAS (FTP/ SAMBA server)
- Global Navigation Satellite System (GNSS)
- Small form factor with multiple mounting options, easily installed by a single person
- Power ignition control option when mounted within vehicles
- Hardened enclosure with Industrial-graded components
- Designed to withstand hypothermia, heat and protect from shock, vibration, etc.

High-speed Mobile Wireless Communication

- Embedded Dual 4G/LTE module
- High performance external antennas

Global Navigation Satellite System (GNSS)

- Embedded GNSS receiver for GPS or GLONASS
- Active external antenna

Network Protocols and Features

- IPv4, IPv6 or IPv4 / IPv6 Dual Stack
- NAT, static (v4/v6) routing and RIP-1 / 2
- DHCPv4 / v6
- Universal Plug and Play (UPnP) Compliant
- Dynamic Domain Name System (DDNS)
- Virtual Server and DMZ
- SNTP, DNS proxy
- IGMP snooping and IGMP proxy
- MLD snooping and MLD proxy

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)

Wireless LAN

- Compliant with IEEE 802.11 b/ g/ n standards
- 2.4 GHz - 2.484GHz radio band for wireless
- Up to 300 Mbps wireless operation rate
- 64 / 128 bits WEP supported for encryption
- WPS (Wi-Fi Protected Setup) for easy setup
- Wireless Security with WPA-PSK / WPA2-PSK support
- Multiple wireless SSIDs with wireless guest access
- Wireless client isolation
- WDS repeater function support

USB Application Server

- Storage/NAS: SAMBA Server, FTP Server

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 v1, v2, v3, MIB-I and MIB-II
- TR-069 supports remote management
- Supports SNMP
- Embedded 4G LTE module debugging and firmware upgrade

Hardware Specifications

Physical interface

- 2 Embedded 4G/LTE modules
- 1 Embedded GNSS
- 4G LTE antenna: 4 detachable antennas (2 antennas for each 4G/LTE module)
- GPS antenna: 1 detachable GPS antenna
- Wi-Fi antenna: 2 detachable wireless antennas
- 2 mini-SIM (2FF) card slots (SIM card from Telco / ISP) for mobile broadband connectivity
- 2 USB 2.0 Type A Host port for storage service
- 2 Mini US connectors (For LTE module debug)
- 4-port 10 / 100 / 1000Mbps auto-crossover (MDI / MDI-X) Ethernet Switch
- EWAN: Port#4 is a WAN / LAN configurable port for Broadband connectivity.
- Factory default reset button
- Wireless on/off and WPS push button
- 4-pin power connector

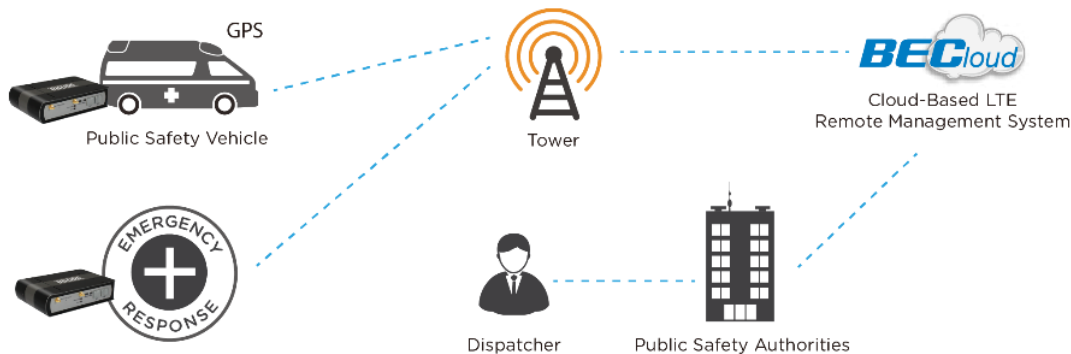
Physical Specifications

- Dimensions (W*H*D): 7.25" x 1.91" x 5.31" (184.25mm x 48.5mm x 135mm)
- Weight: 1.07kgs (2.36lbs)

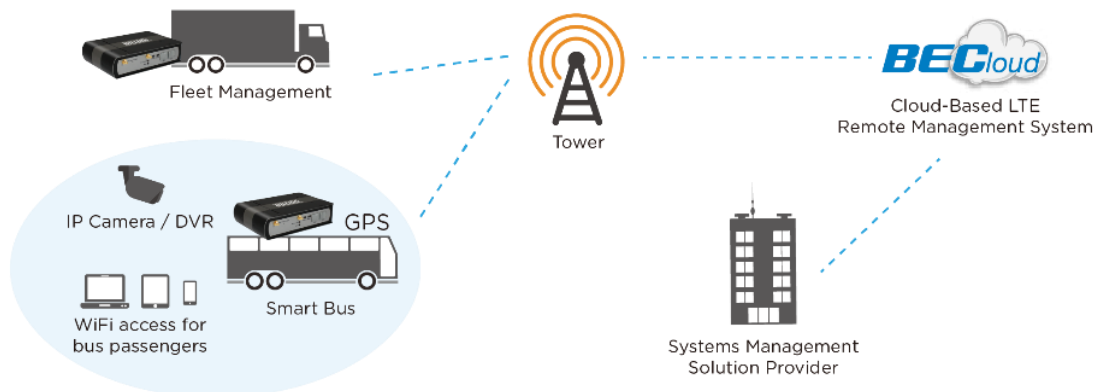
Application Diagrams

The MX-1000 Advanced Industrial 4G/LTE Wireless VPN Router is a high-performance all-in-one wireless communications platform with advanced software enabling high availability, reliable and secure connectivity for mission critical applications. The MX-1000 is specifically designed to provide outstanding network efficiency and internet security for a wide range of applications and vertical machine-to-machine (M2M) market segments.

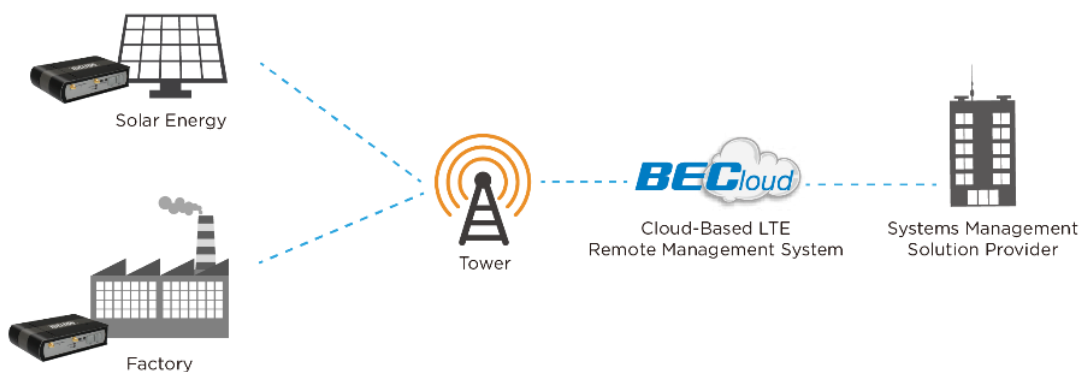
Public Safety:



Fleet Management / Smart Bus:



Power / Energy Industry:



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-1000 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.

Device Description



PORT & LED		MEANING
1	WIFI Antenna Connectors	Screw the supplied LTE antennas onto the antenna connectors on both sides.
2	WIFI & WPS LED	Bicolor LED behaves as follows
		Green Wireless connection established
		Green blinking Data being transmitted / received
		Orange WPS configuration is in progress
3	WIFI ON/OFF & WPS Button	By controlling the pressing time, users can achieve two different effects: (1) WPS* : Press &hold the button for less than 6 seconds to trigger WPS function. (2) Wireless ON/OFF button : Press & hold the button for more than 6 seconds to On/Off the wireless. <i>*For WPS configuration, please refer to the WPS section in the User Manual.</i>
4	RESET	After the device is powered on, press it 6 seconds or above : to restore to factory default settings (this is used when you cannot login to the router, e.g. forgot your password)
5	MINI USB Ports	(Use for debugging purposes) Connect to the ports to control / manage the LTE modules. MINI USB 1 controls 4G/LTE Module #1 MINI USB 2 controls 4G/LTE Module #2
6	SIM Card Slots	Insert the mini SIM card (2FF) with the gold contact facing down. Push the mini SIM card (2FF) inwards to eject it <i>* Power off the MX-1000 before inserting or removing the SIM card(s)</i>



PORTS		MEANING
1	WAN1 (CON1) 4G/LTE Antenna Connectors	Screw the supplied 4G/LTE antennas onto the antenna connectors for 4G LTE module 1.
2	WAN1 (CON2) 4G/LTE Antenna Connectors	Screw the supplied 4G/LTE antennas onto the antenna connectors for 4G LTE module 2.
3	GPS Antenna Connector	Screw the supplied GPS antenna to this connector
4	Power Jack	Connect the supplied Power cable to this jack port
5	USB Ports	The USB can support setup for storage/file sharing. Connect an external USB dongle / hard drive for storage.
6	Gigabit Ethernet (LAN 1 ~ 4)	Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to one of the four LAN ports when connecting to a PC or an office/home network of 10Mbps/ 100Mbps/ 1000Mbps



LEDS		MEANING	
1	Power	Green	System is up and ready
		Red	Boot failure
2	Internet	Green	IP connected and traffic is passing through the device
		Red	IP request failed
		Off	Either in bridged mode or WAN connection is not present
3 & 4	USB 1 / USB 2	Green	Connecting to a USB dongle or a hard drive
5	GPS LED	Green	GPS active
6 & 7	WAN 1 / WAN 2 (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 4G LTE module is in service
		Off	No LTE module or LTE module fails
8	Gigabit Ethernet (LAN 1 ~ 4)	Green	Transmission speed is at Gigabit speed (1000Mbps)
		Orange	Transmission speed is at 10/100Mbps
		Blinking	Data being transmitted/received

System Recovery Procedures

The purpose is to allow users to restore the MX-1000 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-1000 Device

- 2.1 Power off your MX-1000
- 2.2 Power on the MX-1000 while pushing the RESET button with a small pointed object (such as paper clip, needle, toothpick, and etc.).
- 2.3 When the POWER LED turns RED, keep holding and pushing the RESET button until the INTERNET LED flashes in GREEN

Step 3 – Restore your MX-1000 Device

With INTERNET light flashes green, MX-1000 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-1000 will not respond to any PING or other requests.
- 3.2 Browse to the new Firmware image file then click Upload to start the upgrade process.
- 3.3 INTERNET LED turns red means the Firmware upgrade is in process.
DO NOT power off or reboot the device, it would permanently damage your MX-1000.
- 3.4 INTERNET LED turns green after the Firmware upgrade completed
- 3.5 Power cycle on & off to regain access to the MX-1000.

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 XP / Vista / 7 / 8, Linux, Mac OS, etc. The product provides an easy and user-friendly interface for configuration.

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

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



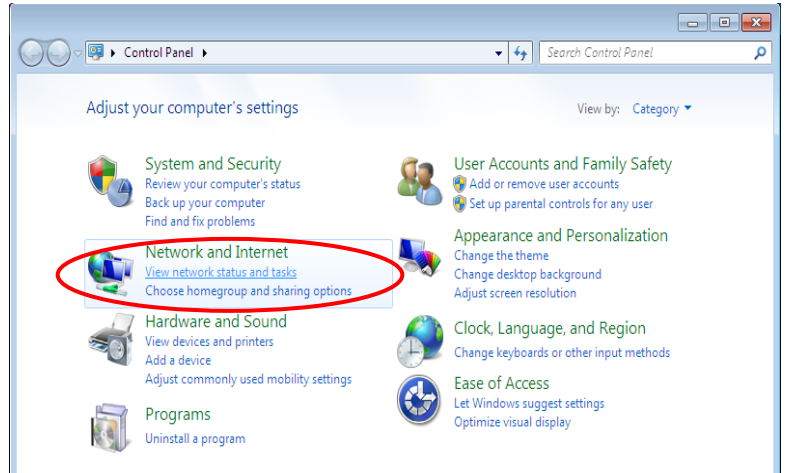
Attention

Any TCP/IP capable workstation can be used to communicate with or through the MX-1000. To configure other types of workstations, please consult the manufacturer's documentation.

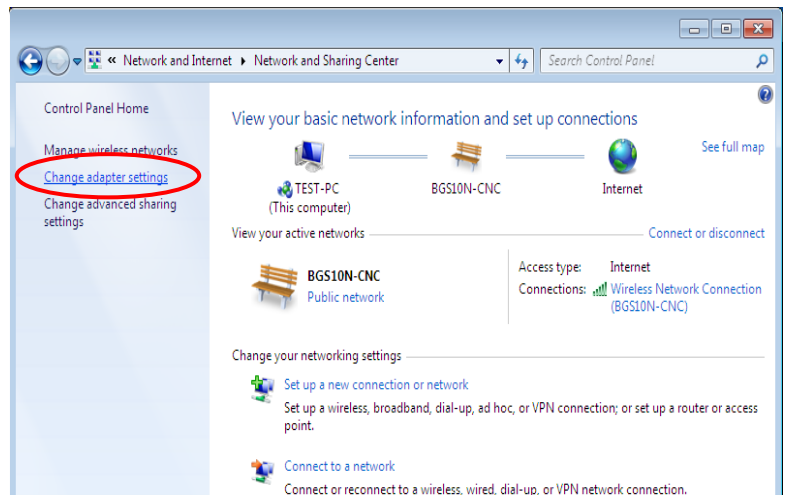
Network Configuration – IPv4

Configuring PC in Windows 7/8 (IPv4)

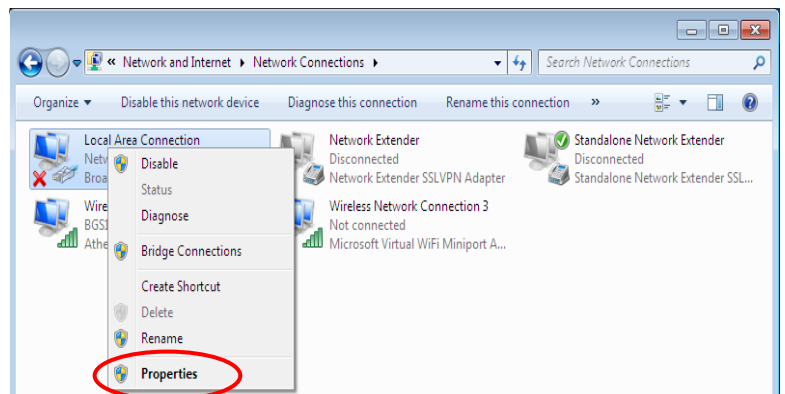
1. Go to **Start**. Click on **Control Panel**.
2. Then click on **Network and Internet**.



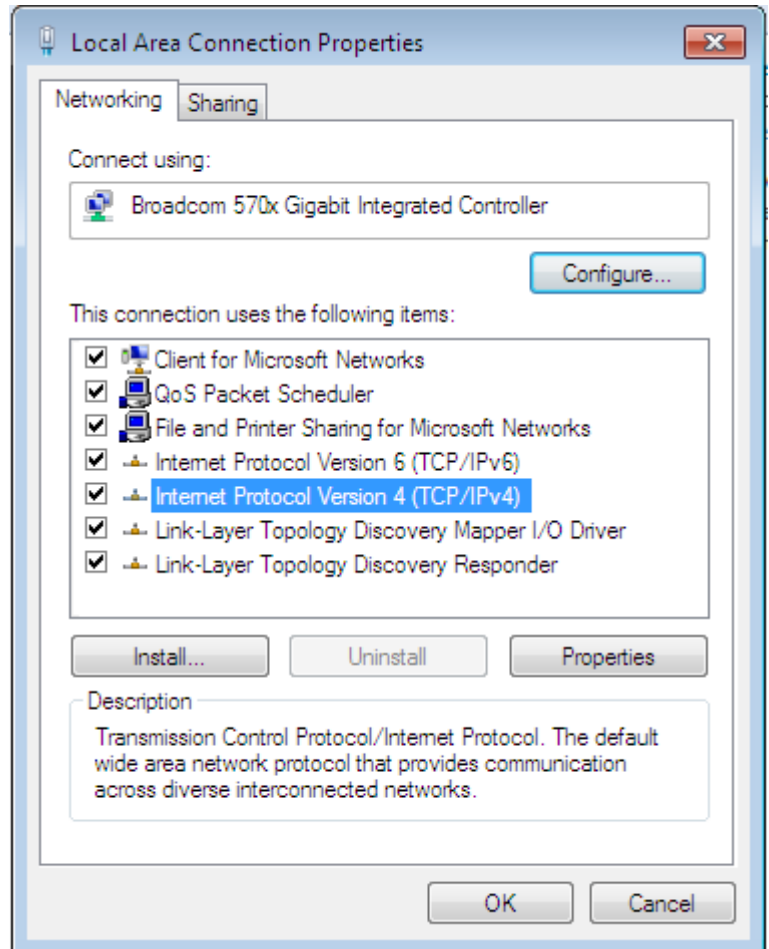
3. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



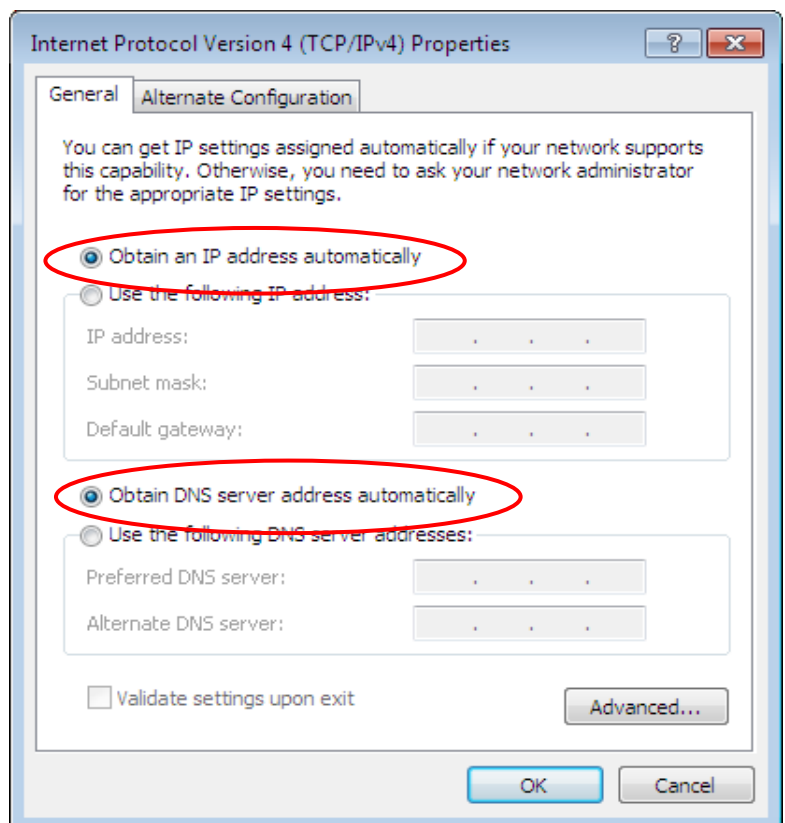
4. Select the **Local Area Connection**, and right click the icon to select **Properties**.



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

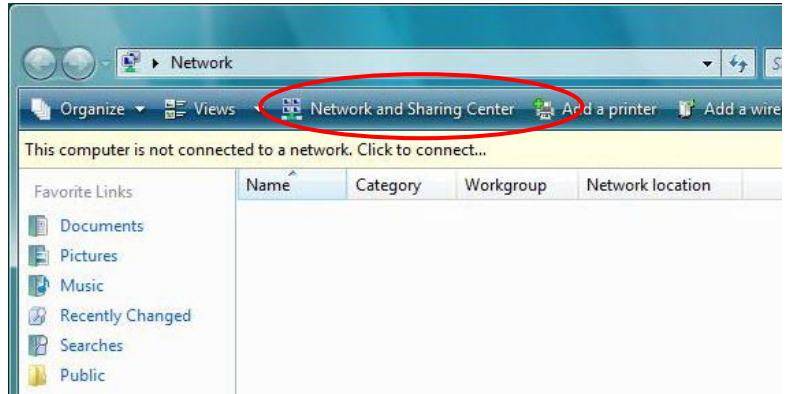


6. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



Configuring PC in Windows Vista (IPv4)

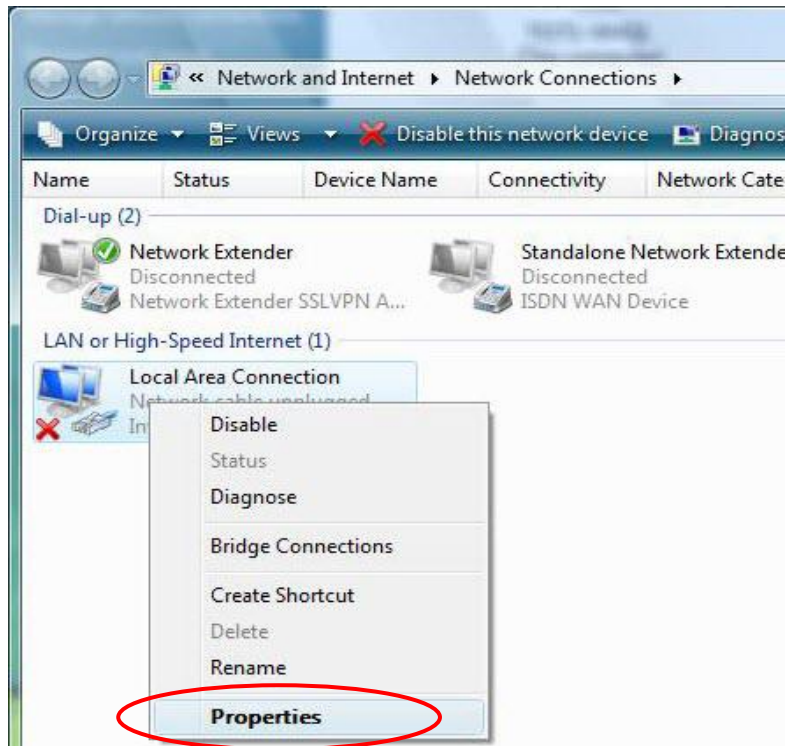
1. Go to **Start**. Click on **Network**.
2. Then click on **Network and Sharing Center** at the top bar.



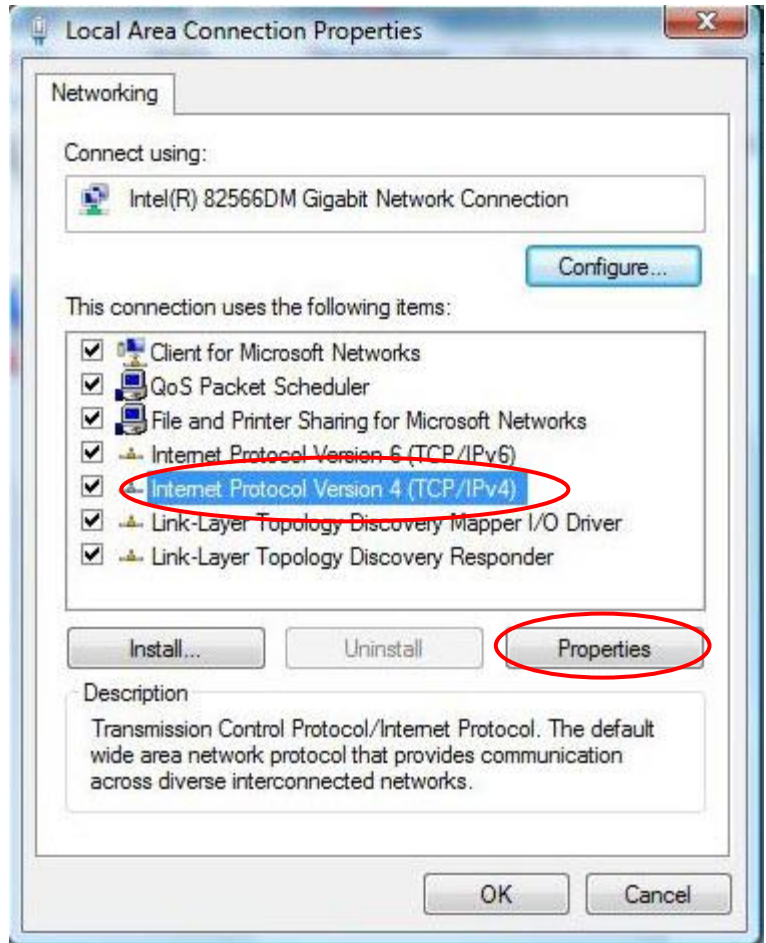
3. When the **Network and Sharing Center** window pops up, select and click on **Manage network connections** on the left window pane.



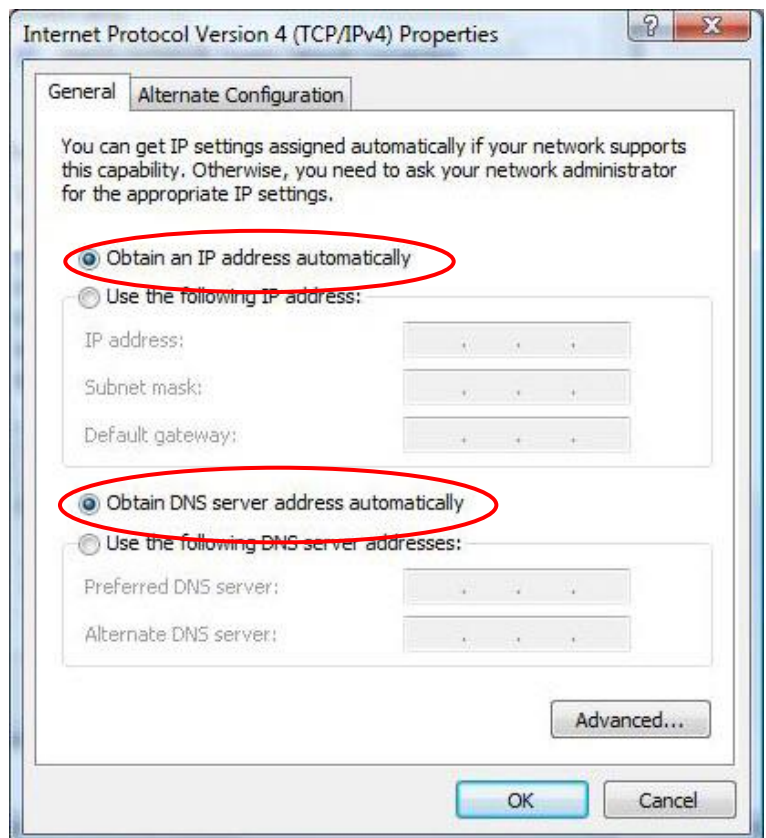
4. Select the **Local Area Connection**, and right click the icon to select **Properties**.



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

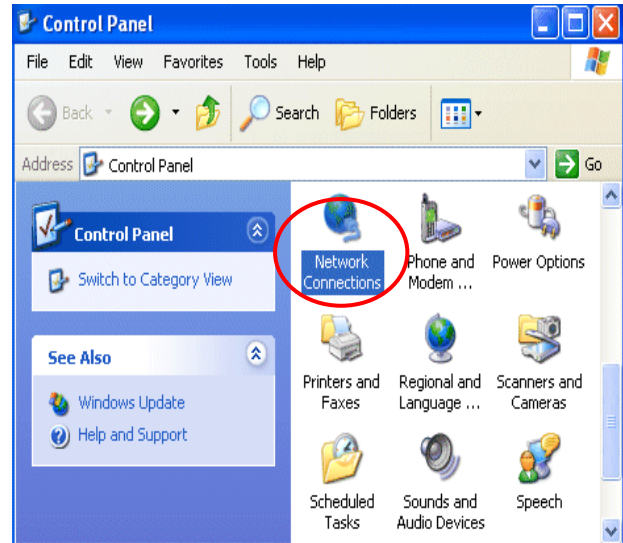


6. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.

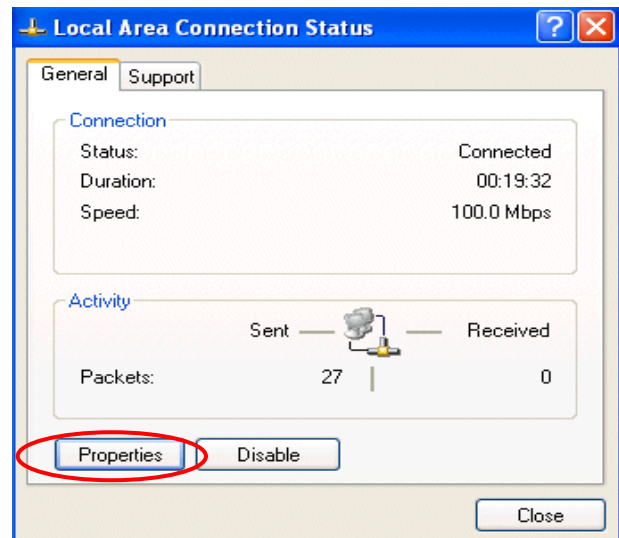


Configuring PC in Windows XP (IPv4)

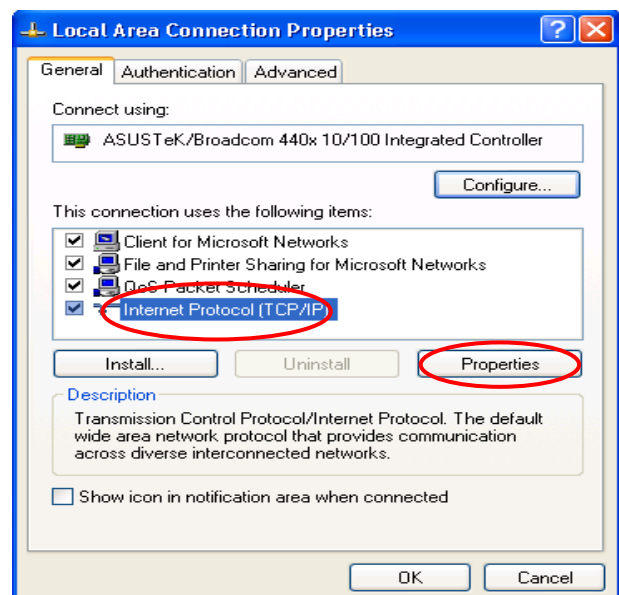
1. Go to **Start**. Click on **Control Panel**.
2. Then click on **Network and Internet**.



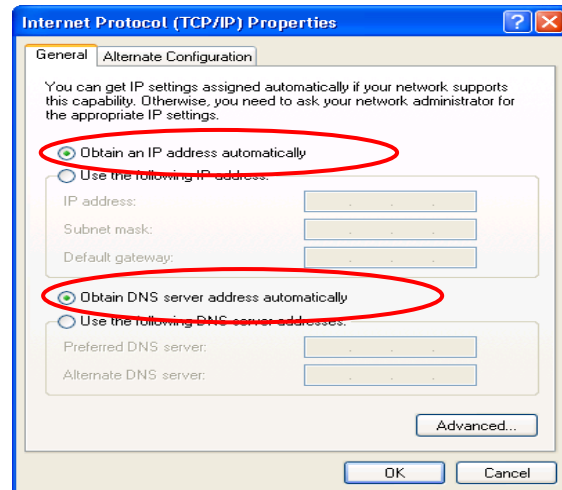
3. In the **Local Area Connection Status** window, click **Properties**.



4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



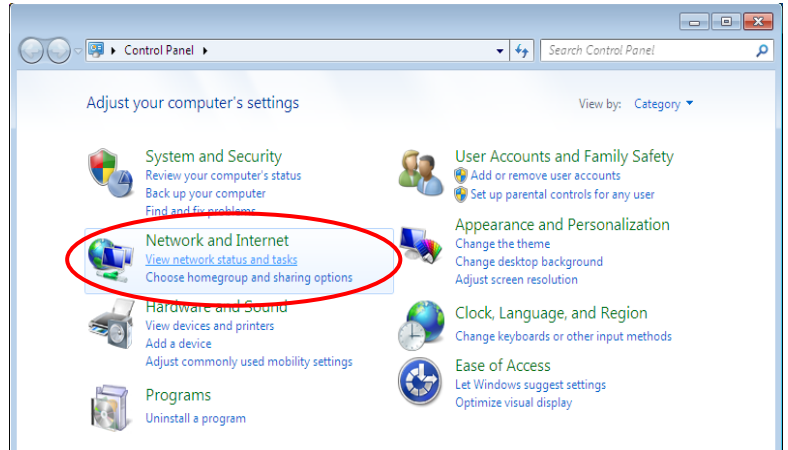
5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.
6. Click **OK** to finish the configuration.



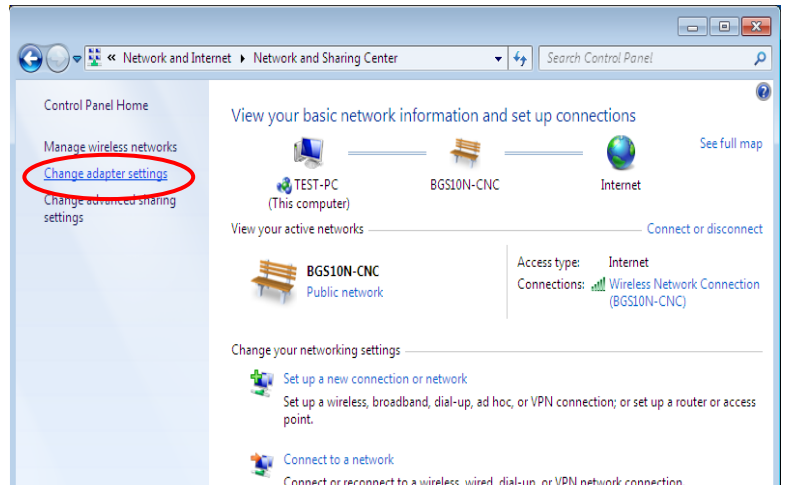
Network Configuration – IPv6

Configuring PC in Windows 7/8 (IPv6)

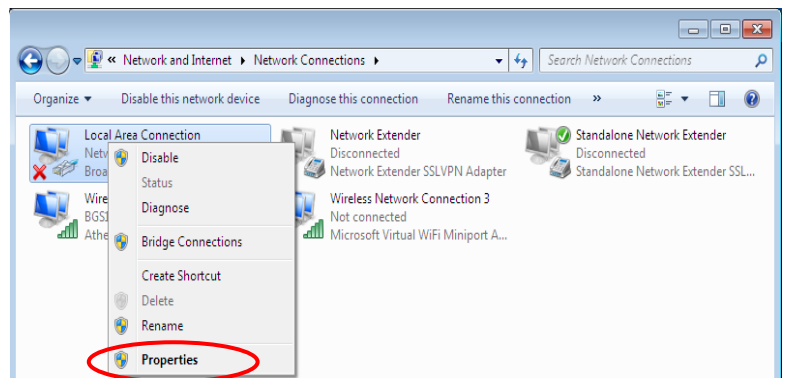
1. Go to **Start**. Click on **Control Panel**.
2. Then click on **Network and Internet**.



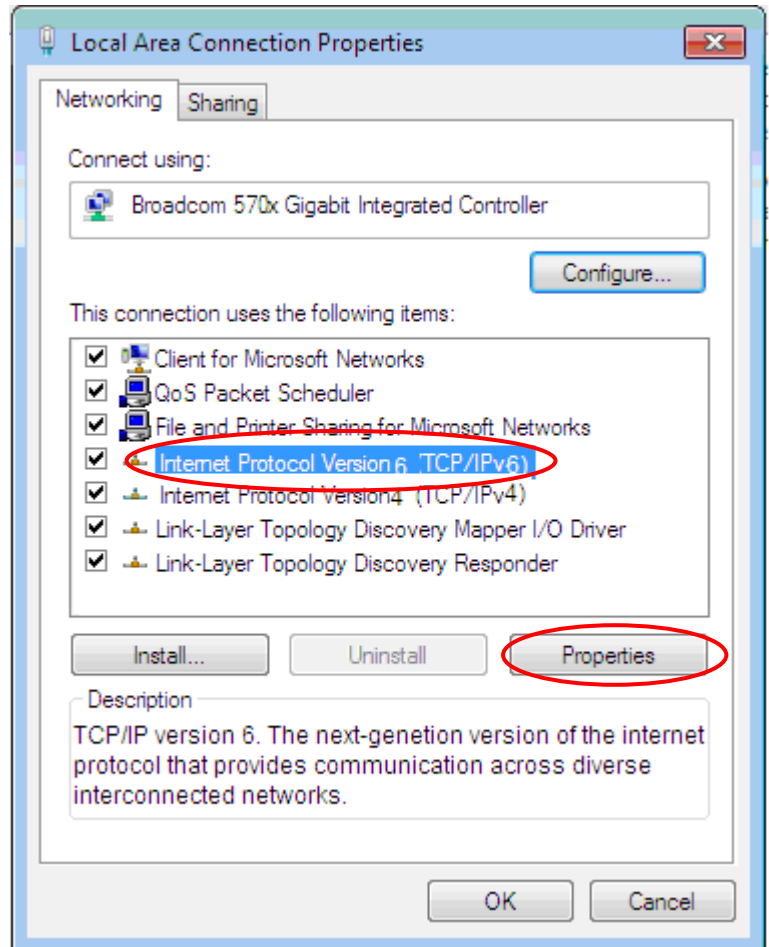
3. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



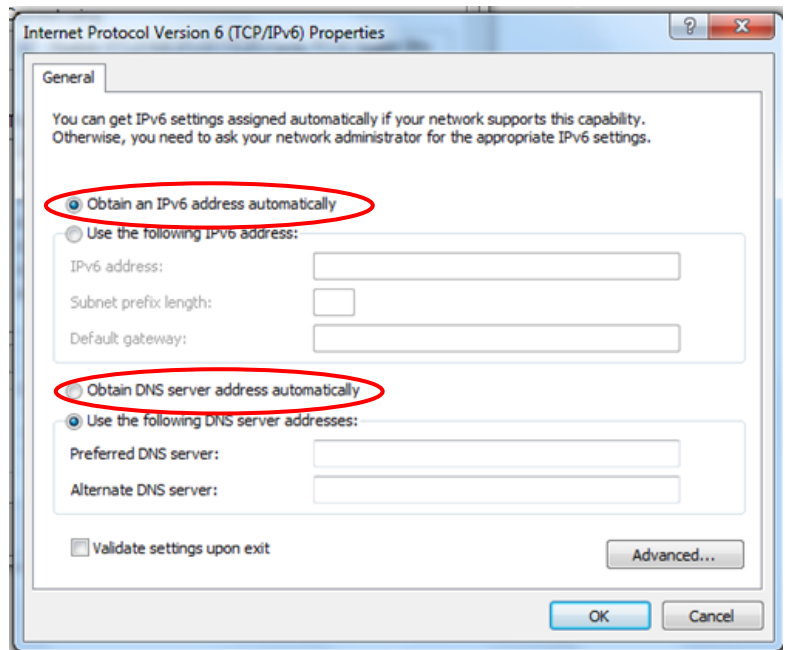
4. Select the **Local Area Connection**, and right click the icon to select **Properties**.



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

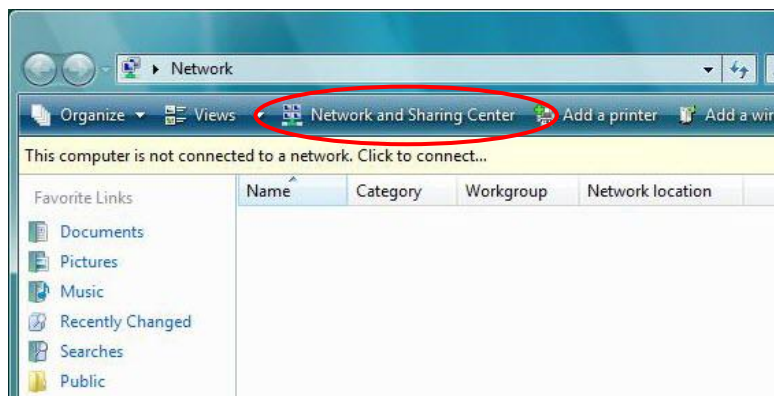


6. In the **TCP/IPv6 properties** window, select the **Obtain an IPv6 address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



Configuring PC in Windows Vista (IPv6)

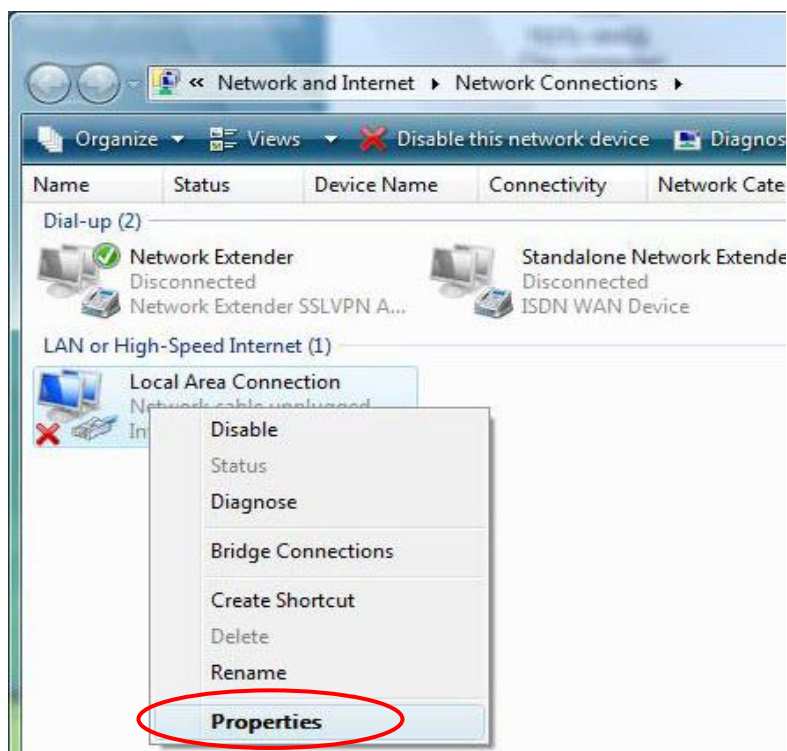
1. Go to **Start**. Click on **Network**.
2. Then click on **Network and Sharing Center** at the top bar.



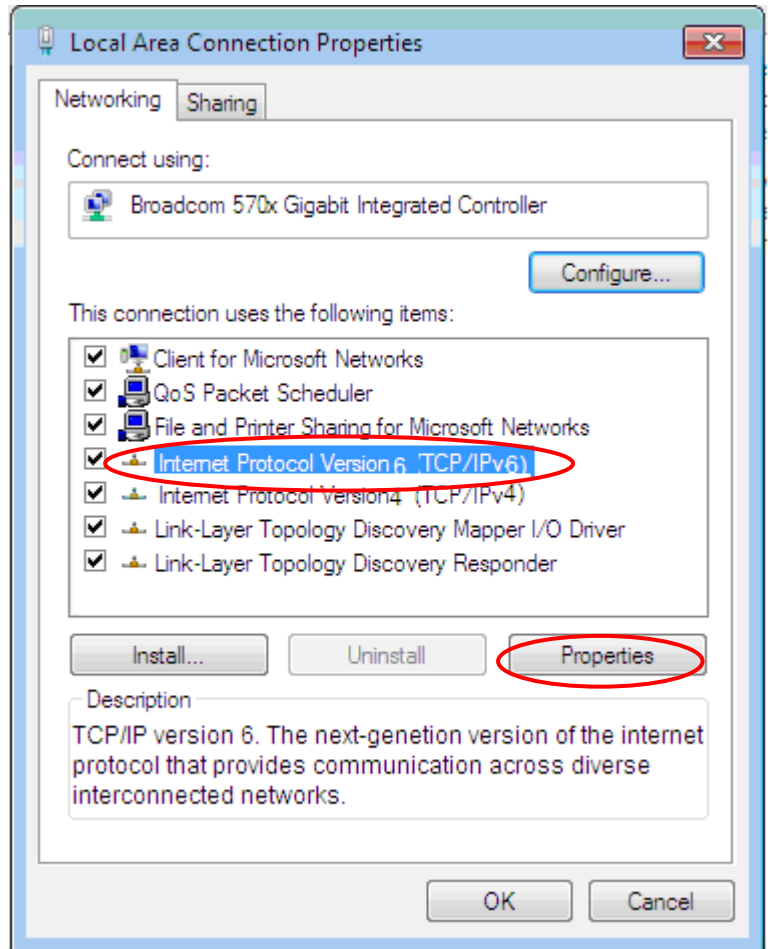
3. When the **Network and Sharing Center** window pops up, select and click on **Manage network connections** on the left window pane.



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

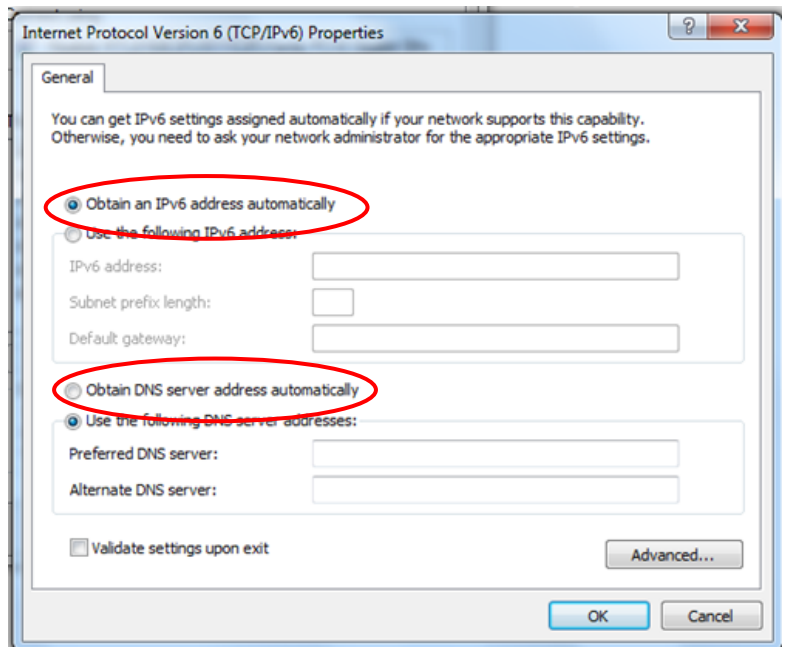


5. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**.



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.

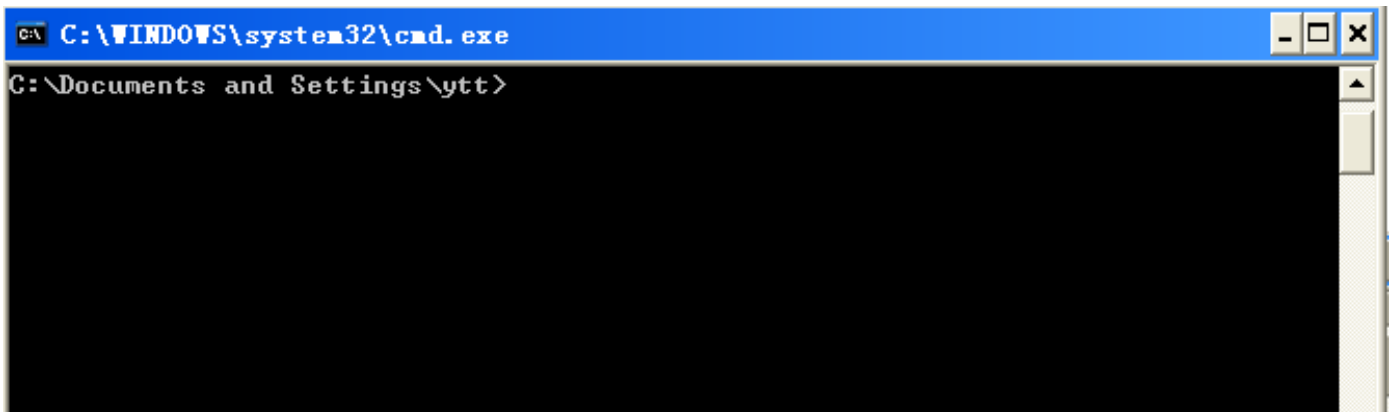


Configuring PC in Windows XP (IPv6)

IPv6 is supported by Windows XP, but you need to install it first.

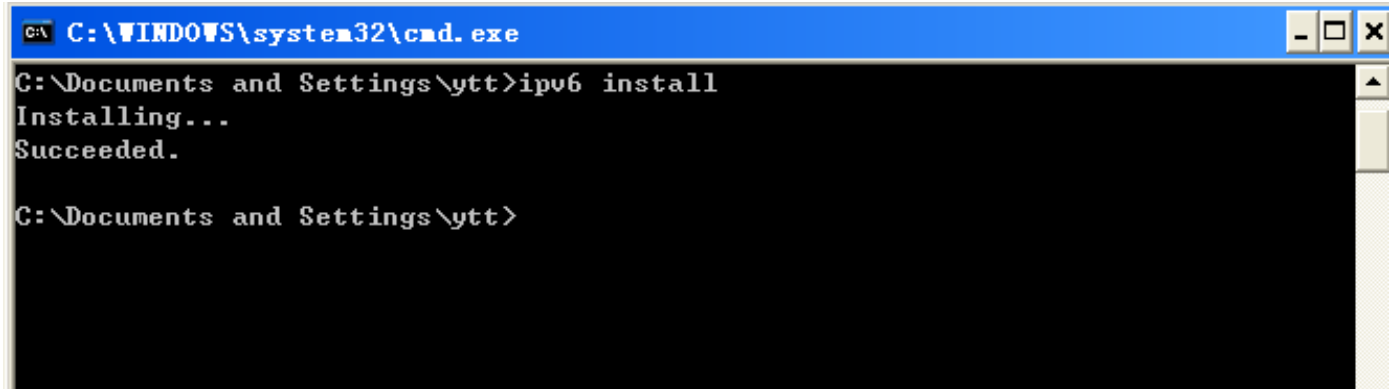
Please follow the steps to install IPv6:

1. On the Desktop, Click **Start > Run**, type **cmd**, then press **Enter** key in the keyboard, the following screen appears.



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\ytt>
```

2. Key in command **ipv6 install**



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\ytt>ipv6 install
Installing...
Succeeded.
C:\Documents and Settings\ytt>
```

Installation of IPv6 is now completed. Please test it to see if it works or not. .

Default Settings

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

Web Interface: (Username and Password)

Administrator

- ✓ Username: admin
- ✓ Password: admin

User

- ✓ Username: user
- ✓ Password: user



If you ever forget the username/password to login to the router, you may press the RESET button up to 6 seconds then release it to restore the factory default settings.

Caution: After pressing the RESET button for more than 6 seconds then

Device LAN IP Settings

- ✓ IP Address: 192.168.1.254
- ✓ Subnet Mask: 255.255.255.0

DHCP Server:

- ✓ DHCP server is enabled.
- ✓ Start IP Address: 192.168.1.100
- ✓ IP pool counts: 100


CHAPTER 4: DEVICE CONFIGURATION

Login to your Device

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

The default username and password is “**admin**” and “**admin**” respectively for the **Administrator**. For the **User** account, default username and password is “**user**” and “**user**”.

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



A Windows Security dialog box titled "Windows Security" with a close button (X) in the top right corner. The text inside reads: "The server 192.168.1.254 at MX-1000 requires a username and password." followed by a warning: "Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection)." Below this is a login form with a small icon of a flower on the left. The form has two input fields: "User name" and "Password". Below the "Password" field is a checkbox labeled "Remember my credentials". At the bottom right of the dialog are "OK" and "Cancel" buttons.

Congratulations! You have successfully logged on to your MX-1000



The screenshot shows the web interface of a BEC Technologies 4G LTE M2M Router. The top header is blue with the BEC Technologies logo on the left and "4G LTE M2M Router" in the center. On the left side, there is a navigation menu with "Status", "Quick Start", and "Configuration". The main content area is titled "Status" and contains several sections:

- Device Information:** Model Name: MX-1000, Firmware Version: (link), MAC Address: 00:04:ed:01:23:45, Date-Time: Wed May 20 21:42:00 UTC 2015, System Up Time: 18 mins.
- Physical Port Status:** 4G LTE -1 (green check), 4G LTE -2 (green check), EWAN (red X), Ethernet (green check), Wireless (green check).
- WAN:** A table showing interface 4G LTE -1 with Dynamic IP, connected for 0d: 0h:16m:41s, IP Address 100.79.1.235/255.255.255.248, and Default Gateway 100.79.1.233.
- LAN:** A table showing IP Address 192.168.1.254, Subnet Mask/Prefix Length 255.255.255.0, and DHCP Server settings (Enable / 192.168.1.100~192.168.1.199 and Enable / Stateless).
- Wireless:** A table showing Mode 802.11b+g+n, SSID BEC345, Channel 6, and Security Mixed WPA2/WPA-PSK.

At the bottom right, there are "Restart" and "Logout" buttons. The footer contains the copyright notice: "Copyright © BEC Technologies Inc. All rights reserved."


Once you have logged on to your MX-1000 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	Language
Sub-Items	Device Info		Interface Setup <ul style="list-style-type: none">- Internet- LAN- Wireless- Wireless MAC Filter	English
	System Log			
	4G/LTE Status		Advanced Setup <ul style="list-style-type: none">- Firewall- Routing- NAT- Static DNS- Time Schedule- Mail Alert- Remote System Log	
	GPS Status		Access Management <ul style="list-style-type: none">- Device Management- SNMP- Universal Plug & Play- Dynamic DNS- Access Control- Packet Filter- CWMP (TR-069)- Parental Control- SAMBA & FTP Server	
	Hardware Monitor		Maintenance <ul style="list-style-type: none">- User Management- Time Zone- Firmware & Configuration- System Restart- Auto Reboot- Diagnostic Tool	
	Statistics			
	DHCP Table			
	Disk Status			

Please see the relevant sections of this manual for detailed instructions on how to configure your **MX-1000** device.

Status

In this section, you can check the router working status, including **Device Info**, **System Log**, **4G LTE Status**, **GPS Status**, **Hardware Monitor**, **Statistics**, **DHCP Table**, and **Disk Status**

**4G LTE M2M Router**

▼Status

• Device Info

• System Log

• 4G LTE Status

• GPS Status

• Hardware Monitor

• Statistics

• DHCP Table

• Disk Status

• IPSec Status

• PPTP Status

• L2TP Status

• GRE Status

• Quick Start

►Configuration

Status

▼Device Information

Model Name	MX-1000
Firmware Version	
MAC Address	00:04:ed:01:23:45
Date-Time	Wed May 20 21:42:32 UTC 2015
System Up Time	19 mins

▼Physical Port Status

4G LTE -1	✓
4G LTE -2	✓
EWAN	✗
Ethernet	✓
Wireless	✓

▼WAN

Interface	Protocol	Connection	IP Address	Default Gateway
4G LTE -1	Dynamic IP	0d: 0h:17m:13s Connected	100.79.1.235/255.255.255.248	100.79.1.233

▼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

Restart

Logout

Copyright © BEC Technologies Inc. All rights reserved.

Device Info

It provides brief status summary of the device.

▼ Device Information		▼ Physical Port Status	
Model Name	MX-1000	4G LTE -1	✓
Firmware Version		4G LTE -2	✓
MAC Address	00:04:ed:01:23:45	EWAN	✗
Date-Time	Wed May 20 21:42:32 UTC 2015	Ethernet	✓
System Up Time	19 mins	Wireless	✓

▼ WAN				
Interface	Protocol	Connection	IP Address	Default Gateway
4G LTE -1 ▼	Dynamic IP	0d: 0h:17m:13s Connected	100.79.1.235/255.255.255.248	100.79.1.233

▼ 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	BEC345	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-1000** with your PC. Check on [Time Zone](#) section for more configuration information.

System Uptime: Display how long the **MX-1000** has been powered on.

Physical Port Status

Physical Port Status : Display available connection interfaces, WAN (3G/4G-LTE, EWAN), LAN (Ethernet) and Wireless, that are supported in the MX-1000.

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.

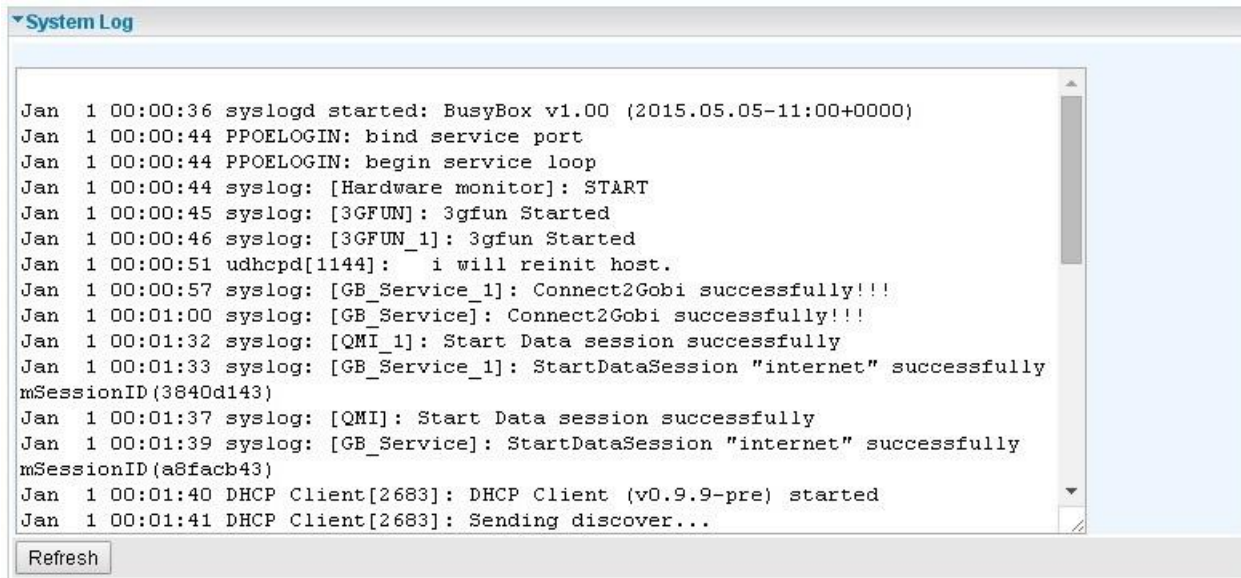
SSID: Display the name of the Wireless AP(s) to use

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

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

System Log

In system log, you can check the operations status and any glitches to the router.



The screenshot shows a web-based interface for the System Log. At the top, there is a tab labeled "System Log". Below it is a scrollable text area containing the following log entries:

```
Jan 1 00:00:36 syslogd started: BusyBox v1.00 (2015.05.05-11:00+0000)
Jan 1 00:00:44 PPOELOGIN: bind service port
Jan 1 00:00:44 PPOELOGIN: begin service loop
Jan 1 00:00:44 syslog: [Hardware monitor]: START
Jan 1 00:00:45 syslog: [3GFUN]: 3gfun Started
Jan 1 00:00:46 syslog: [3GFUN_1]: 3gfun Started
Jan 1 00:00:51 udhcpd[1144]: i will reinit host.
Jan 1 00:00:57 syslog: [GB_Service_1]: Connect2Gobi successfully!!!
Jan 1 00:01:00 syslog: [GB_Service]: Connect2Gobi successfully!!!
Jan 1 00:01:32 syslog: [QMI_1]: Start Data session successfully
Jan 1 00:01:33 syslog: [GB_Service_1]: StartDataSession "internet" successfully
mSessionID(3840d143)
Jan 1 00:01:37 syslog: [QMI]: Start Data session successfully
Jan 1 00:01:39 syslog: [GB_Service]: StartDataSession "internet" successfully
mSessionID(a8facb43)
Jan 1 00:01:40 DHCP Client[2683]: DHCP Client (v0.9.9-pre) started
Jan 1 00:01:41 DHCP Client[2683]: Sending discover...
```

At the bottom of the log area, there is a "Refresh" button.

Refresh: Press this button to refresh the statistics.

3G/4G-LTE Status

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

4G LTE Status	
WAN	4G LTE -1 ▾
Status	Up
Signal Strength	<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div> -64.00dbm
Signal Information	RSRP:-90 , RSRQ:-13 , SINR:3.6
Network Name	"Chunghwa Telecom"
Cell ID	04D4520D(81023501)
Card IMEI
Card IMSI
Network Mode	LTE
Network Band	B3
Refresh	

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

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

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

- ▶ RSRP (Reference Signal Receiving Power): is the average power of all resource elements which carry cell-specified reference signals over the entire bandwidth.
- ▶ RSRQ (Reference Signal Receiving Quality): measures the signal strength and is calculated based on both RSRP and RSSI.
- ▶ RSSI (Received Signal Strength Indicator): parameter which provides information about total received wide-band power (measure in all symbols) including all interference and thermal noise. Please refer to the [Device Description](#) for details.
- ▶ SINR (Signal to Interference plus Noise Ratio): is also a measure of signal quality as well. It is widely used by the operators as it provides a clear relationship between RF conditions and throughput.

NOTE: Some LTE modules do not provide this information.

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

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

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

To enable this feature, please go to **Configuration >> Interface Setup >> Internet** >> click **“Usage Allowance”** >> enable **“Save the statistics to ROM”**

[illegible]

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 this page.

GPS Status

In GPS status, you can check the UTC time, position of the router.

▼GPS Status

GPS 6 Satellites
UTC Time (hh:mm:ss): 03:31:22
Latitude: N2447.899658
Longitude: E12100.429688
Speed: 0 MPH, 0 km/h

Refresh

Hardware Monitor

In hardware monitor, you can check the voltage, current and temperature of system.

▼Hardware Monitor

Voltage:14.32V Current:0.35A
Temperature:41.75C / 107.15F

Refresh

Statistics

❖ 3G/4G-LTE

Take 3G/4G-LTE as an example to describe the following connection transmission information.

Statistics	
Traffic Statistics	
Interface	<input checked="" type="radio"/> 4G LTE -1 <input type="radio"/> 4G LTE -2 <input type="radio"/> EWMAN <input type="radio"/> Ethernet <input type="radio"/> Wireless
Transmit Statistics	
Transmit Frames of Current Connection	71
Transmit Bytes of Current Connection	9873
Transmit Total Frames	71
Transmit Total Bytes	9873
Receive Statistics	
Receive Frames of Current Connection	13
Receive Bytes of Current Connection	1642
Receive Total Frames	13
Receive Total Bytes	1642
Refresh	

Traffic Statistics

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

Transmit Statistics

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

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

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

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

Receive Statistics

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

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

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

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

Refresh: Click to refresh this page.

❖ EWAN

Statistics	
Traffic Statistics	
Interface	<input type="radio"/> 4G LTE -1 <input type="radio"/> 4G LTE -2 <input checked="" type="radio"/> EWAN <input type="radio"/> Ethernet <input type="radio"/> Wireless
Transmit Statistics	
Transmit Frames	0
Transmit Multicast Frames	0
Transmit Total Bytes	0
Transmit Collision	0
Transmit Error Frames	0
Receive Statistics	
Receive Frames	0
Receive Multicast Frame	0
Receive Total Bytes	0
Receive CRC Errors	0
Receive Under-size Frames	0
Refresh	

Traffic Statistics

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

Transmit Statistics

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

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

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

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

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

Receive Statistics

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

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

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

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

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

Refresh: Click to refresh this page.

❖ Ethernet

Status

Statistics

Traffic Statistics

Interface

☐ 3G/4G-LTE
 ☒ Ethernet

Transmit Statistics

Transmit Frames

886

Transmit Multicast Frames

232

Transmit Total Bytes

486510

Transmit Collision

0

Transmit Error Frames

0

Receive Statistics

Receive Frames

623

Receive Multicast Frame

140

Receive Total Bytes

117004

Receive CRC Errors

0

Receive Under-size Frames

0

Refresh

Traffic Statistics

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

Transmit Statistics

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

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

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

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

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

Receive Statistics

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

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

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

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

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

Refresh: Click to refresh this page.

❖ Wireless

Statistics	
Traffic Statistics	
Interface	<input type="radio"/> 4G LTE -1 <input type="radio"/> 4G LTE -2 <input type="radio"/> EWMAN <input type="radio"/> Ethernet <input checked="" type="radio"/> Wireless
Transmit Statistics	
Transmit Frames	18679
Transmit Error Frames	294
Transmit Drop Frames	294
Receive Statistics	
Receive Frames	27946
Receive Error Frames	837
Receive Drop Frames	837
Refresh	

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.

Refresh: Click to refresh this page.

DHCP Table

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

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

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

Host Name: Show 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.

Disk Status

▼Disk Status		
Partition	Disk Space(KB)	Free Space(KB)
usb1_1	15718272	14033064
usb2_1	15734652	11170204

Partition: Display the USB storage partition.

Disk Space (KB): Display the total storage space of the NAS in Kbytes unit.

Free Space (KB): Display the available space in Kbytes unit.

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, wireless, and WAN settings of your device. The Quick Start Wizard is a helpful guide for the first-time users to the device.

Quick Start

The 'Quick Start' wizard will guide you to configure the device to connect to your ISP(Internet Service Provider).
Please follow the 'Quick Start' wizard step by step to configure the device. It will allow you to have Internet access within minutes.

Run Wizard

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

Quick Start

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

Step 1. Set your new password

Step 2. Choose your time zone

Step 3. Set your wireless connection

Step 4. Set your internet connection

Step 5. Confirm the configuration and save it

Next

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

Step 1 – Password

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

Quick Start - Password

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

New Password

Confirm Password

Back Next

Step 2 – Time Zone

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

Quick Start - Time Zone

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

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

Back Next

Step 3 – Wireless

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

Quick Start - Wireless

Configure your wireless network, authentication type and click NEXT to continue.

Access Point	<input checked="" type="radio"/> Activated <input type="radio"/> Deactivated
SSID	<input type="text" value="BEC345"/>
Broadcast SSID	<input checked="" type="radio"/> Yes <input type="radio"/> No
Channel	UNITED STATES <input type="text" value="06"/>
Security Type	Mixed WPA2/WPA-PSK
WPA Algorithms	TKIP+AES
Pre-Shared Key	<input type="text" value="842CFFDE"/> (8~63 characters or 64 Hex string)
Key Renewal Interval	<input type="text" value="600"/> seconds (10 ~ 4194303)

Step 4 – ISP Connection Type

Set up your 3G/4G-LTE Internet connection.

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

Quick Start - ISP Connection Type

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

WAN Interface	4G LTE -1
---------------	-----------

4.2(1) If selected **4G LTE-1** or **4G LTE-2**

Input all relevant 3G/4G-LTE parameters from your ISP.

Click **Next** to continue.

Quick Start - 3G/4G-LTE

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

TEL No.	<input type="text" value="*99***1#"/>
APN	<input type="text" value="internet"/>
Username	<input type="text"/>
Password	<input type="text"/>
PIN	<input type="text"/>

4.2(2) If selected **EWAN / PPPoE**, please enter PPPoE account information provided by your ISP.

Click **NEXT** to continue.

Quick Start - PPPoE

Provide the PPPoE information. Click NEXT to continue.

Username

Password

Back

Next

Step 5 – Quick Start Completed

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

Quick Start - Quick Start Completed

Quick Start Completed !!

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

Back

Next

Quick Start - Quick Start Completed !!

Quick Start Completed !!

Saved Changes.

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

Configuration

Click to access and configure the available features in the following: **Interface Setup**, **Advanced Setup**, **Access Management**, and **Maintenance**.

These functions are described in the following sections.

Interface Setup

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

4G LTE M2M Router

Status

Quick Start

Configuration

Interface Setup

Internet

LAN

Wireless

Wireless MAC Filter

Dual WAN

Advanced Setup

VPN

Access Management

Maintenance

Configuration

Internet

WAN Interface

4G LTE -1

Status

☒ Activated
 ☐ Deactivated

Usage Allowance

☐ Enable

LTE Antenna Diversity

Enabled

Network Mode

Automatic

TEL No.

*99***1#

Dual APN

Single APN

APN

internet

Username

Password

PIN

Connection

☒ Always On (Recommended)
 ☐ Yes
 ☐ No

Keep Alive

☐ Yes
 ☒ No

Default Route

☒ Yes
 ☐ No

NAT

Enable

Save

Restart

Logout

Copyright © BEC Technologies Inc. All rights reserved.

Internet

❖ 3G/4G-LTE

Internet	
WAN Interface	4G LTE -1 ▼
Status	<input checked="" type="radio"/> Activated <input type="radio"/> Deactivated
Usage Allowance ▶	<input type="checkbox"/> Enable
LTE Antenna Diversity ▶	Enabled
Network Mode	Automatic ▼
TEL No.	*99***1#
Dual APN	Single APN ▼
APN	internet
Username	
Password	
PIN	
Connection	<input checked="" type="radio"/> Always On (Recommended)
Keep Alive	<input type="radio"/> Yes <input checked="" type="radio"/> No
Default Route	<input checked="" type="radio"/> Yes <input type="radio"/> No
NAT	Enable ▼
Save	

WAN Interface: List all available WAN interfaces. (In this section, you have selected to use 3G/4G-LTE)

Status: Choose Activated to enable the 3G/4G-LTE connection.

Usage Allowance: Enable and click “Usage Allowance” for further setting configuration of your 3G/4G-LTE data usage.

Usage Allowance

Usage Allowance	
Parameters	
Mode	<input type="radio"/> Volume-based
	Only Download ▼ <input type="text" value=""/> MB data volume per month included
	<input checked="" type="radio"/> Time-based
	720 <input type="text" value=""/> hours per month included
The billing period always begins on day 1 <input type="text" value=""/> of a month.	
Over usage allowance action	None ▼
Save the statistics to ROM	Disable ▼
Save Back	

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

- ▶ **Volume-based** include “only Download”, “only Upload”, and “Download and Upload” to limit the flow.
- ▶ **Time-based** control the flow by providing specific hours per month.

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

Over usage allowance action: Here are actions to perform when mobile data usage, defined in

Mode, reached to its maximum.

- ▶ **None:** No action taken
- ▶ **Disconnect:** Disconnect mobile connection
- ▶ **Email Alert:** Send an e-mail alert and keep the mobile connection alive.
- ▶ **Email Alert and Disconnect:** Disconnect mobile connection after an alert e-mail is being sent.

Save the statistics to ROM:

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

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

Usage Allowance	
Amount used	0Hours of 720Hours
Billing period	Day:15
<input type="button" value="Clean"/> <input type="button" value="Save"/>	

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. **NOTE:** Feature available when module supports multiple LTE bands. .

LTE Band

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

LTE Mode	
Parameters	
LTE Band	B12 ▼
***Please save config and restart to activate the setting. Please make sure device had get WAN IP, then config this feature.	
<input type="button" value="Apply"/> <input type="button" value="Save Config & Restart"/>	

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.

LTE Mode	
Parameters	
LTE Antenna Diversity	▼
***Please save config and restart to activate the setting. Please make sure device had get WAN IP, then config this feature.	
<input type="button" value="Apply"/> <input type="button" value="Save Config & Restart"/>	

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

TEL No.: The dial string to make a GPRS / 3G/4G-LTE user internetworking call. It may provide by your mobile service provider.

Dual APN: Can support up to two (2) APNs. Select Single or Dual.

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

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.

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.

Click Save to apply the settings.

❖ EWAN

Internet	
WAN Interface	EWAN ▼
Status	<input checked="" type="radio"/> Activated <input type="radio"/> Deactivated
IPv4/IPv6	
IP Version	<input type="radio"/> IPv4 <input checked="" type="radio"/> IPv4/IPv6 <input type="radio"/> IPv6
ISP Connection Type	
ISP	<input type="radio"/> Dynamic IP Address <input type="radio"/> Static IP Address <input checked="" type="radio"/> PPPoE <input type="radio"/> Bridge Mode
802.1q Options	
802.1q	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
VLAN ID	0 (range: 0~4095)
PPPoE	
Username	<input type="text"/>
Password	<input type="text"/>
Bridge Interface for PPPoE	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
Connection Setting	
Connection	<input checked="" type="radio"/> Always On (Recommended) <input type="radio"/> Connect Manually
TCP MSS Option	TCP MSS 0 bytes(0 means use default)
IP Options	
IP Common Options	
Default Route	<input checked="" type="radio"/> Yes <input type="radio"/> No
TCP MTU Option	TCP MTU 0 bytes(0 means use default:1492)
IPv4 Options	
Get IP Address	<input type="radio"/> Static <input checked="" type="radio"/> 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	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
IPv6 Options	
IPv6 Address	<input type="text"/> / <input type="text"/>
Obtain IPv6 DNS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
MLD Proxy	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<input type="button" value="Save"/>	

Status: Select to enable or disable the service.

IPv4/IPv6

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

ISP Connection Type:

ISP: Select the encapsulation type your ISP uses.

- ▶ **Dynamic IP:** Select this option if your ISP provides you an IP address automatically.
- ▶ **Static IP:** Select this option to set static IP information. You will need to enter in the Connection type, IP address, subnet mask, and gateway address, provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form. IP address from by four IP octets separated by a dot (xx.xx.xx.xx). The Router will not accept the IP address if it is not in this format.
- ▶ **PPPoE:** Select this option if your ISP requires you to use a PPPoE connection.
- ▶ **Bridge:** Select this mode if you want to use this device as an OSI Layer 2 device like a switch.

802.1q Options

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

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

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

Username: Enter the user name provided by your ISP.

Password: Enter the password provided by your ISP.

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

Connection Setting

Connection:

- ▶ **Always On:** Click on **Always On** to establish a PPPoE session during start up and to automatically re-establish the PPPoE session when disconnected by the ISP.
- ▶ **Connect Manually:** Select Connect Manually when you don't want the connection up all the time.

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

IP Options

IP Options	
IP Common Options	
Default Route	<input checked="" type="radio"/> Yes <input type="radio"/> No
TCP MTU Option	TCP MTU <input type="text" value="0"/> bytes(0 means use default:1492)
IPv4 Options	
Get IP Address	<input type="radio"/> Static <input checked="" type="radio"/> Dynamic
Static IP Address	<input type="text" value="0.0.0.0"/>
IP Subnet Mask	<input type="text" value="0.0.0.0"/>
Gateway	<input type="text" value="0.0.0.0"/>
NAT	<input type="button" value="Enable"/>
Dynamic Route	<input type="button" value="RIP1"/> Direction <input type="button" value="None"/>
IGMP Proxy	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
IPv6 Options	
IPv6 Address	<input type="text" value=""/> / <input type="text" value=""/>
Obtain IPv6 DNS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Primary DNS	<input type="text" value=""/>
Secondary DNS	<input type="text" value=""/>
MLD Proxy	<input type="radio"/> Enable <input checked="" type="radio"/> 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-1000 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 the 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
 ☒ LAN3
 ☒ LAN4
 ☒ WLAN1

DNS Relay

☒ Automatically
 ☐ Manually

Primary DNS

Secondary DNS

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 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.

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	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled <input type="radio"/> Relay
Start IP	<input type="text" value="192.168.1.100"/>
IP Pool Count	<input type="text" value="100"/>
Lease Time	<input type="text" value="86400"/> seconds (0 sets to default value of 259200)
DNS Relay	<input checked="" type="radio"/> Automatically <input type="radio"/> Manually
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>

DHCPv4 Server: If set to **Enabled**, your MX-1000 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-1000 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.

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.

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	<input type="text"/>
MAC Address	<input type="text"/>

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.

IPv6 Parameters	
Interface Address/Prefix Length	<input type="text"/> / <input type="text"/>
MLD Snooping	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
DHCPv6 Server	
DHCPv6 Server	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
DHCPv6 Server Type	<input checked="" type="radio"/> Stateless <input type="radio"/> Stateful
Start Interface ID	<input type="text"/>
End Interface ID	<input type="text"/>
Lease Time	<input type="text"/> seconds(0 sets to default value of 4800)
Router Advertisements	<input type="radio"/> Disable <input checked="" type="radio"/> Enable

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

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 the settings.

Wireless

This section introduces the wireless LAN and some basic configurations. Wireless LANs can be as complex as a number of computers with wireless LAN cards communicating through access points which bridge network traffic to the wired LAN.

▼Wireless	
Access Point Settings	
Access Point	<input checked="" type="radio"/> Activated <input type="radio"/> 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	<input checked="" type="radio"/> Yes <input type="radio"/> No
11n Settings	
Channel Bandwidth	20 MHz ▼
Guard Interval	Auto ▼
MCS	Auto ▼
SSID Settings	
Available SSID	1 ▼
SSID Index	<input checked="" type="radio"/> SSID1
SSID	BEC345
Broadcast SSID	<input checked="" type="radio"/> Yes <input type="radio"/> No
SSID Activated	Always ▼
WPS Settings	
Use WPS	<input checked="" type="radio"/> Yes <input type="radio"/> No
WPS State	Configured
WPS Mode	<input type="radio"/> PIN code <input checked="" type="radio"/> PBC
Security Settings	
Security Type	Mixed WPA2/WPA-PSK ▼
WPA Algorithms	TKIP+AES ▼
Pre-Shared Key	842CFFDE (8~63 characters or 64 Hex string)
Key Renewal Interval	600 seconds (10 ~ 4194303)
WDS Settings	
AP MAC Address	00:04:ED:01:23:45
WDS Mode	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
WDS Peer MAC #1	00:00:00:00:00:00
WDS Peer MAC #2	00:00:00:00:00:00
WDS Peer MAC #3	00:00:00:00:00:00
WDS Peer MAC #4	00:00:00:00:00:00
Save	

Access Point Settings

Access Point Settings	
Access Point	<input checked="" type="radio"/> Activated <input type="radio"/> 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	<input checked="" type="radio"/> Yes <input type="radio"/> No

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	
Channel Bandwidth	20 MHz ▼
Guard Interval	Auto ▼
MCS	Auto ▼
SSID Settings	
Available SSID	1 ▼
SSID Index	<input checked="" type="radio"/> SSID1
SSID	BEC345
Broadcast SSID	<input checked="" type="radio"/> Yes <input type="radio"/> No
SSID Activated	Always ▼

11n Settings

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

Guard Interval: Select either **400nsec** or **800nsec** 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

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.

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, in order 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.

SSID Activated: Select the time period during which the SSID is active. Default is always which means the SSID will be active all the time without time control. See [Time Schedule](#) to set the timeslot to flexibly control when the SSID functions.

WPS Settings

WPS (Wi-Fi Protected Setup) feature is a standard protocol created by Wi-Fi Alliance. This feature greatly simplifies the steps needed to create a Wi-Fi network for a residential or an office setting. WPS supports 2 types of configuration methods which are commonly known among consumers: [PIN Method](#) (Personal Information Number) & [PBC Method](#) (Push Button Configuration).

WPS Settings	
Use WPS	<input checked="" type="radio"/> Yes <input type="radio"/> No
WPS State	Configured
WPS Mode	<input type="radio"/> PIN code <input checked="" type="radio"/> PBC

Use WPS: Enable this feature by choosing "YES" radio button.

WPS State: Display whether the WPS is **configured** or **unconfigured**.

WPS Mode: Select the mode which to start WPS, choose between **PIN Code** and **PBC** (Push Button). Selecting **Pin Code** mode will require you to know the enrollee PIN code.

To future understand the two modes of configuration; please refer to the example of the **Wi-Fi Protected Setup**.

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.
<input checked="" type="radio"/> Key#1	<input type="text"/>
<input type="radio"/> Key#2	<input type="text"/>
<input type="radio"/> Key#3	<input type="text"/>
<input type="radio"/> Key#4	<input type="text"/>

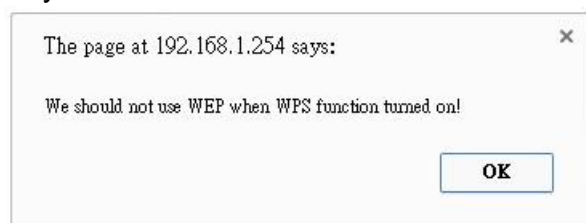
WEP Authentication Method: WEP authentication method, there are two methods of authentication used, Open System authentication (OPENWEB) and Share Key authentication (SHAREDWEB). We suggest you select OPENWEB.

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: When you enable WPS function, this WEP function will be invalid. And if you select one of WEP-64Bits/ WEP-128Bits, the following prompt box will appear to notice you.

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

Security Settings	
Security Type	Mixed WPA2/WPA-PSK ▼
WPA Algorithms	TKIP+AES ▼
Pre-Shared Key	<input type="text"/> (8~63 characters or 64 Hex string)
Key Renewal Interval	600 seconds (10 ~ 4194303)

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 ASCII 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.

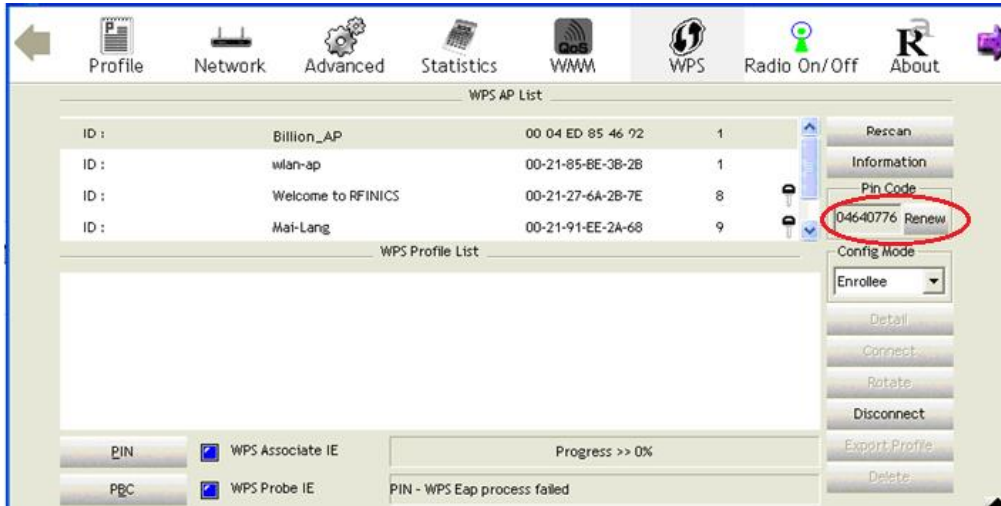
WDS Settings	
AP MAC Address	60:03:47:6C:48:00
WDS Mode	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
WDS Peer MAC #1	<input type="text"/>
WDS Peer MAC #2	<input type="text"/>
WDS Peer MAC #3	<input type="text"/>
WDS Peer MAC #4	<input type="text"/>

Click **Save** to apply the settings.

Example: WPS using PIN Method (Personal Information Number)

PIN Method – Configure MX-1000 as a Registrar

1. Jot down the client's Pin (e.g. 04640776) from the WPS utility (e.g. Ralink Utility)

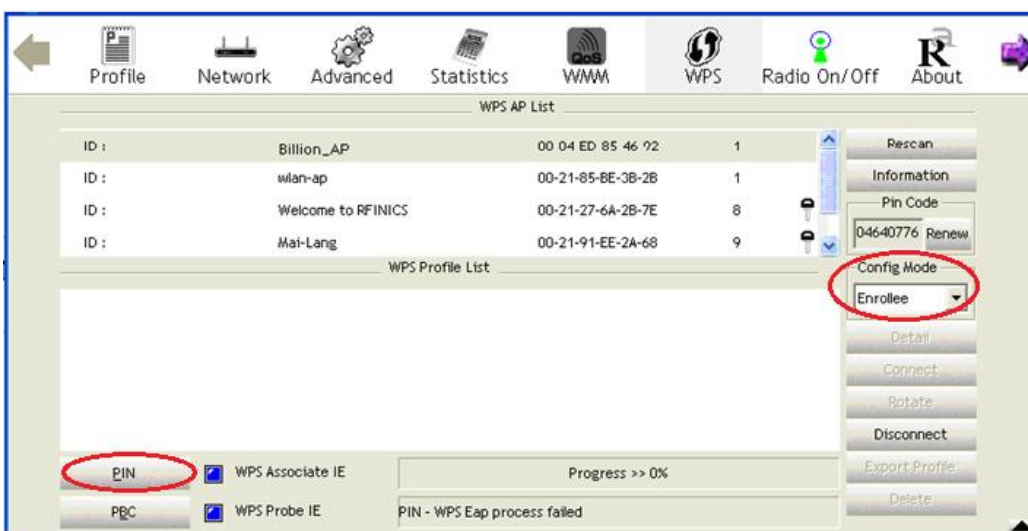


2. Enter the Enrollee (Client) PIN code and then press **Start WPS**.

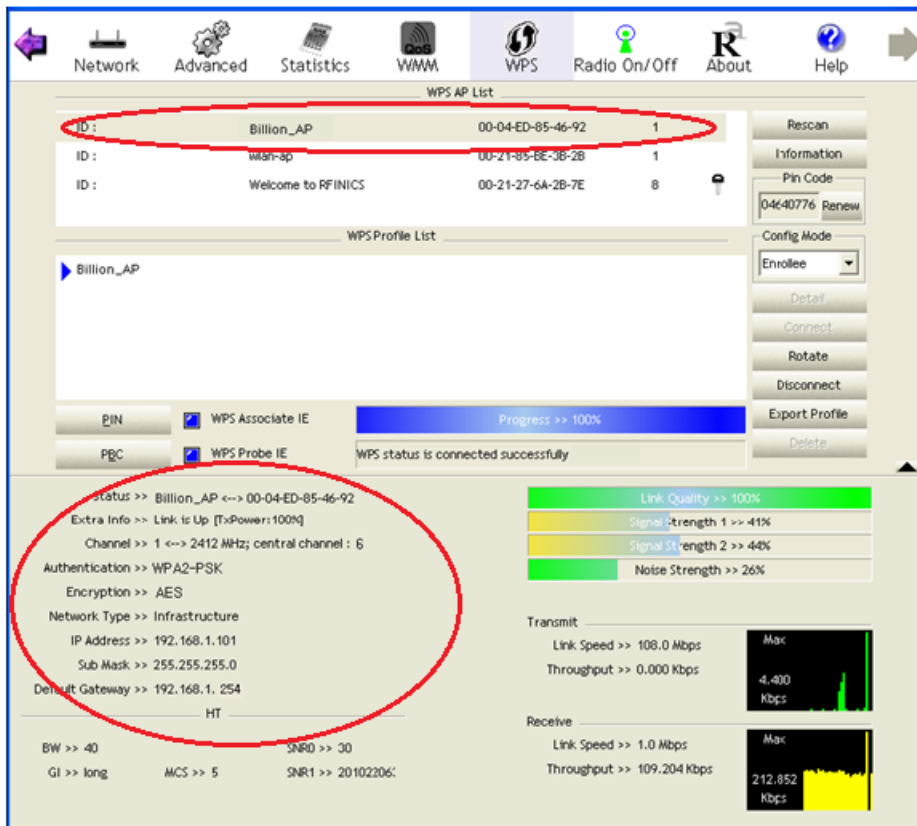


3. Go back to the wireless client's WPS utility (e.g. Ralink Utility).

Set the Config Mode as **Enrollee**, press the WPS button on the top bar, select the AP (e.g. Billion_AP) from the WPS AP List column. Then press the PIN button located on the middle left of the page to run the scan.



4. The client's SSID and security setting will now be configured to match the SSID and security setting of the registrar, the MX-1000 router.



SSID Settings

Available SSID: 1

SSID Index: SSID1

SSID: Billion-AP

Broadcast SSID: Yes

Clients Isolation: No

SSID Activated: Always

WPS Settings

Use WPS: Yes

WPS State: Configured

WPS Mode: PIN code

AP PIN Code: 70963205

Enrollee PIN Code: 04640776

WPS Progress: Idle

Security Settings

Security Type: WPA2-PSK

WPA Algorithms: AES

Pre-Shared Key: billion00486c (8~63 characters or 64 Hex string)

Key Renewal Interval: 600 seconds (10 ~ 4194303)

PIN Method – Configure MX-1000 as an Enrollee

1. Jot down the AP PIN Code (e.g. 03454435) from the BEC 6300VNL. Press **Start WPS**.

WPS Settings	
Use WPS	<input checked="" type="radio"/> Yes <input type="radio"/> No
WPS State	Configured
WPS Mode	<input checked="" type="radio"/> PIN code <input type="radio"/> PBC
AP PIN Code	03454435 <input type="button" value="Generate"/>
Enrollee PIN Code	<input type="text"/>
WPS Progress	In progress <input type="button" value="Stop WPS"/>

2. Launch the wireless client's WPS utility (e.g. Ralink Utility). Set the Config Mode as Registrar. Enter the PIN number in the PIN Code (e.g. 03454435) column then choose the correct AP (e.g. Billion_AP) from the WPS AP List before pressing the PIN button to run the scan.

The screenshot shows the Ralink WPS utility interface. At the top, there is a navigation bar with icons for Network, Advanced, Statistics, WPS, Radio On/Off, About, and Help. The main window is titled 'WPS AP List' and contains a table with the following data:

ID	SSID	BSSID	Signal	Key
ID : 0x0000	Billion_AP	00-04-ED-85-46-92	1	
ID :	Welcome to RFINICS	00-21-27-6A-2B-7E	8	
ID :	Mai-Lang	00-21-91-EE-2A-68	9	

Below the table is the 'WPS Profile List' section, which shows 'Billion_AP' selected. To the right of the table, there are buttons for 'Rescan', 'Information', 'Pin Code', 'Config Mode', 'Detail', 'Connect', 'Rotate', 'Disconnect', and 'Export Profile'. The 'Pin Code' field is set to '03454435' and the 'Config Mode' is set to 'Registrar'. At the bottom, there is a 'PIN' button and a 'PBC' button. The 'WPS status is connected successfully' message is displayed.

Below the WPS status, there is a 'Status' section showing the following information:

- Status >> Billion_AP <--> 00-04-ED-85-46-92
- Extra Info >> Link is Up [TxPower:100%]
- Channel >> 1 <--> 2412 MHz; central channel : 6
- Authentication >> WPA2-PSK
- Encryption >> AES
- Network Type >> Infrastructure
- IP Address >> 192.168.1.101
- Sub Mask >> 255.255.255.0
- Default Gateway >> 192.168.1.254

On the right side, there is a 'Link Quality' section showing the following values:

- Link Quality >> 100%
- Signal Strength 1 >> 24%
- Signal Strength 2 >> 35%
- Noise Strength >> 26%

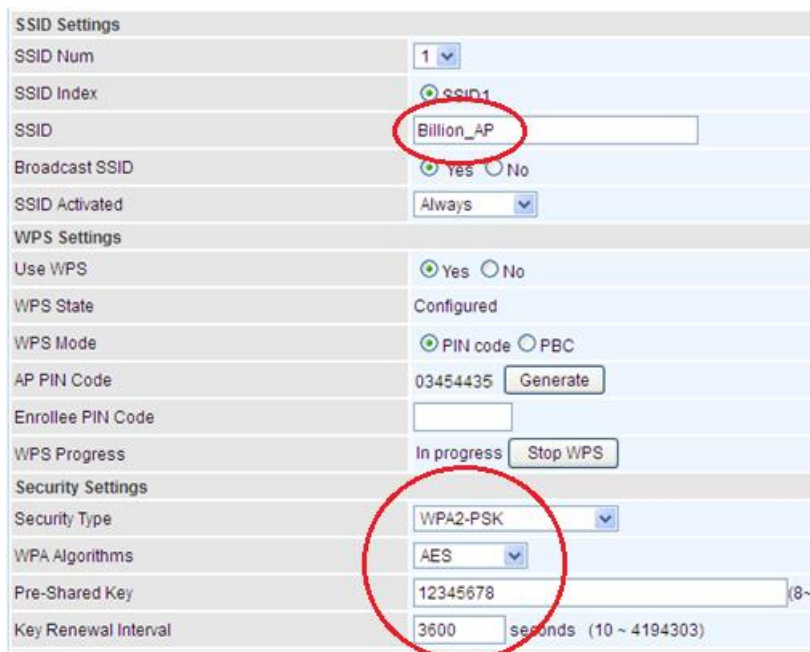
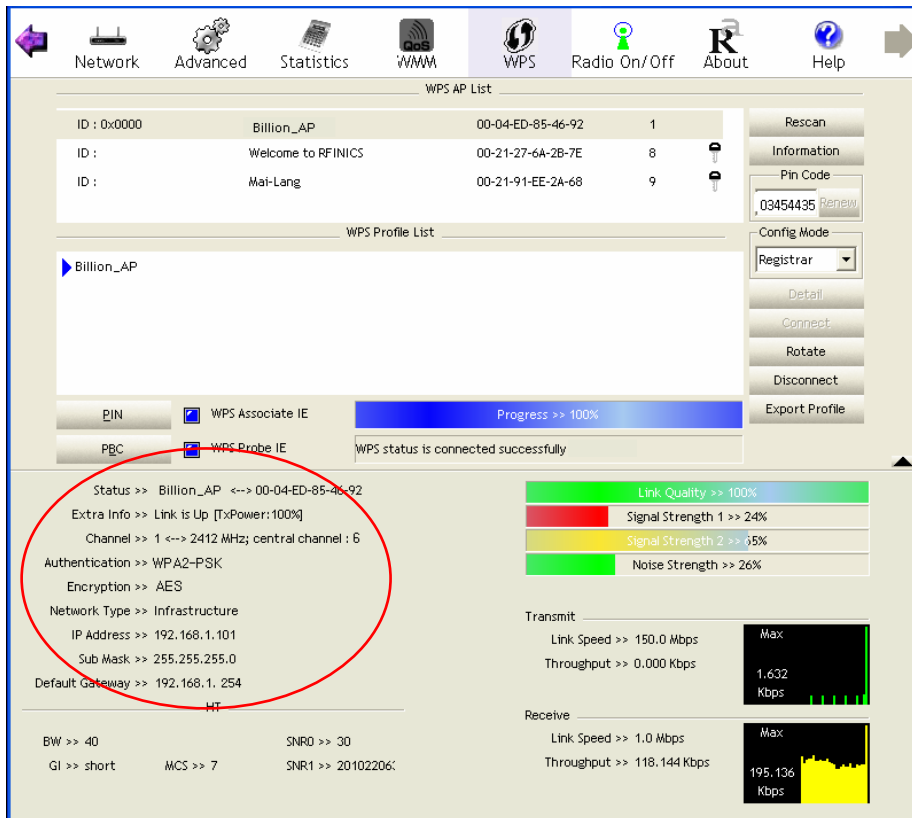
At the bottom, there is a 'Transmit' section showing the following values:

- Link Speed >> 150.0 Mbps
- Throughput >> 0.000 Kbps

And a 'Receive' section showing the following values:

- Link Speed >> 1.0 Mbps
- Throughput >> 118.144 Kbps

3. The router's (AP's) SSID and security setting will now be configured to match the SSID and security setting of the registrar (client).



Example: WPS using PBC Method (Push Button Configuration)

1. Click the **PBC** radio button and click **Save** to apply the settings

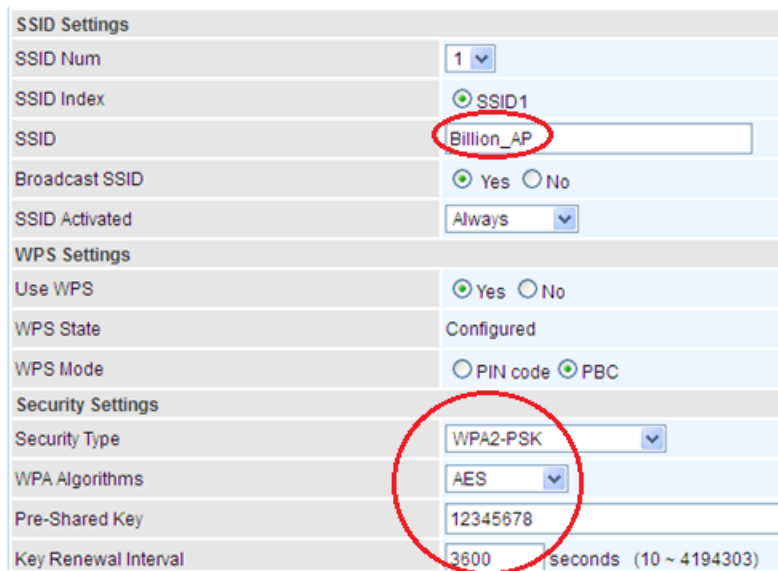
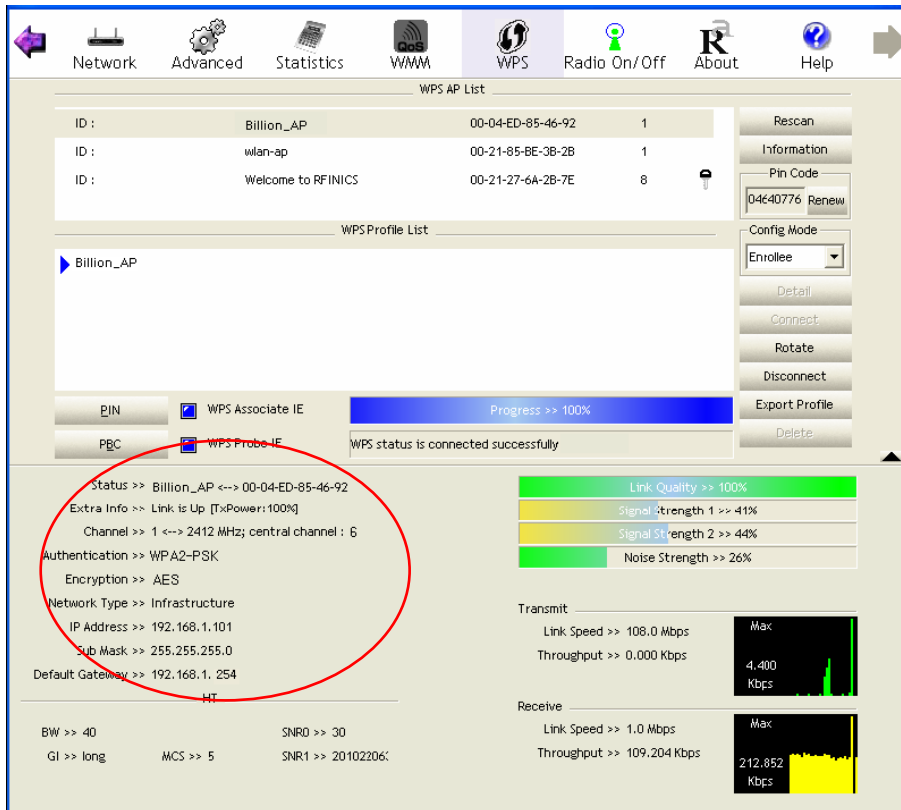
SSID Settings	
SSID Num	1
SSID Index	SSID1
SSID	Billion_AP
Broadcast SSID	Yes No
SSID Activated	Always
WPS Settings	
Use WPS	Yes No
WPS State	Configured
WPS Mode	PIN code PBC
Security Settings	

2. Launch the wireless client's WPS Utility (e.g. Ralink Utility). Set the Config Mode as **Enrollee**. Then press the **WPS button** and choose the correct AP (e.g. **Billion_AP**) from the WPS AP List section before pressing the **PBC** button to run the scan.

Profile	Network	Advanced	Statistics	WMM	WPS	Radio On/Off	About
WPS AP List							
ID :	Billion_AP	00 04 ED 85 46 92	1				
ID :	wlan-ap	00-21-85-BE-3B-2B	1				
ID :	Welcome to RFINICS	00-21-27-6A-2B-7E	8				
ID :	Mai-Lang	00-21-91-EE-2A-68	9				
WPS Profile List							
<div> <div> PIN WPS Associate IE WPS Probe IE </div> <div> Progress >> 0% PIN - WPS Eap process failed </div> </div>							
<div> Rescan Information Pin Code 04640776 Renew Config Mode Enrollee Detail Connect Rotate Disconnect Export Profile Delete </div>							

Interface Setup – Wireless (Example on WPS using PBC)

3. When the PBC button is pushed, a wireless communication will be established between your router and the PC. The client's SSID and security setting will now be configured to match the SSID and security setting of the router.



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.

Wireless MAC Address Filter

SSID Index

☒ SSID1

Active

☐ Activated
☒ Deactivated

Action

Allow the follow Wireless LAN station(s) association.

MAC Address

Save

Wireless MAC Address Filter Listing			
Index	MAC Address	Edit	Delete

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.

Advanced Setup

Advanced Setup provides advanced features including **Firewall**, **Routing**, **NAT**, **Static DNS**, **Time Schedule**, **Mail Alert** and **Remote System Log** for advanced users.

Firewall

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

Firewall	
Firewall	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
SPI	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
(WARNING: If You enabled SPI, all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.)	
<input type="button" value="Save"/>	

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

- ▶ **Enabled:** Activate your firewall function.
- ▶ **Disabled:** Deactivate the firewall function.

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

- ▶ **Enabled:** Activate your SPI function.
- ▶ **Disabled:** Deactivate the SPI function.

Click **Save** to apply the settings

Routing

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

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

Add Route

Index #: The numeric route indicator.

Destination IP Address: IP address of the destination network

Subnet Mask: The subnet mask of destination network.

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

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

Interface: Media/channel selected to append the route.

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

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

Add Route

▼Static Route	
Destination IP Address	<input type="text" value="0.0.0.0"/>
Destination Subnet Mask	<input type="text" value="0.0.0.0"/>
Gateway IP Address / Interface	<input type="radio"/> <input type="text" value="0.0.0.0"/> <input checked="" type="radio"/> <input type="text" value="4G LTE -1"/>
Metric	<input type="text" value="1"/>
<input type="button" value="Save"/> <input type="button" value="Back"/>	

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

Destination Subnet Mask: The subnet mask of destination network.

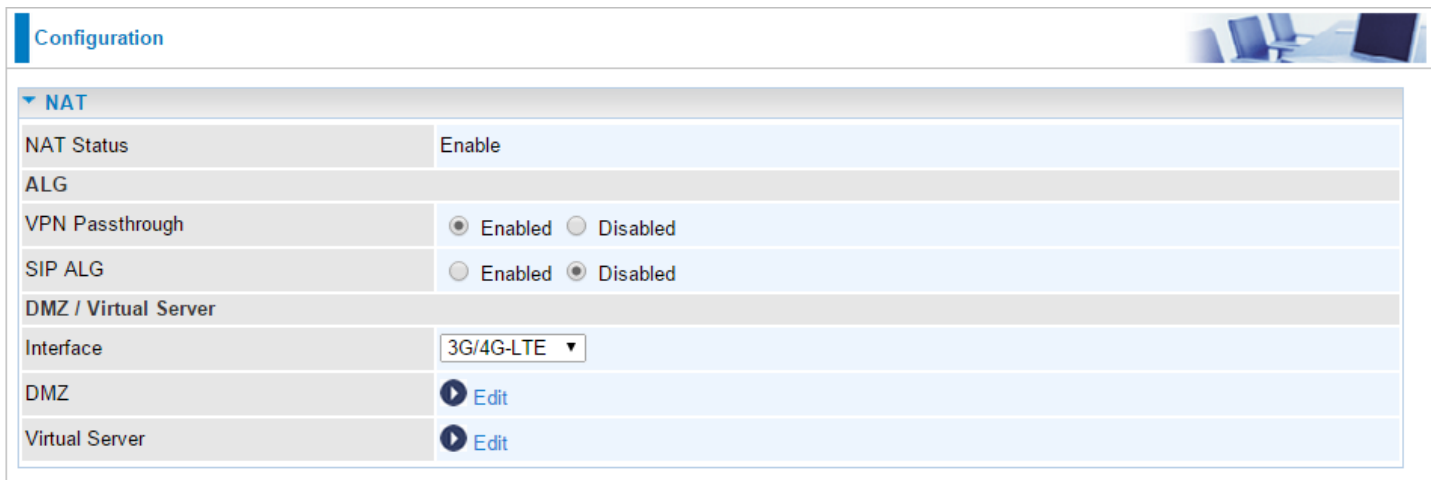
Gateway IP Address or Interface: This is the gateway IP address or existing interface to which packets are to be forwarded.

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

Click **Save** to add this route

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.



Configuration	
NAT	
NAT Status	Enable
ALG	
VPN Passthrough	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
SIP ALG	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
DMZ / Virtual Server	
Interface	3G/4G-LTE ▼
DMZ	Edit
Virtual Server	Edit

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

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.

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 exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets will be checked by the Firewall and NAT algorithms then passed to the DMZ host, when a packet received does not use a port number used by any other Virtual Server entries.

DMZ	
DMZ for	4G LTE -1
DMZ	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
DMZ Host IP Address	0.0.0.0
<input type="button" value="Save"/> <input type="button" value="Back"/>	

DMZ for (via a WAN Interface): Allows outside network to connect in and communicate with internal LAN devices via this 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 the settings

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-1000 to direct all incoming traffic to the servers on the LAN.

Configure a virtual rule in MX-1000 for remote users accessing services such as Web or FTP services via the public (WAN) IP address that can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network.

Virtual Server

Virtual Server for

4G LTE -1

Protocol

TCP

Start Port Number

End Port Number

Local IP Address

Start Port Number (Local)

End Port Number(Local)

Save

Back

Virtual Server Listing

Index	Protocol	Start Port	End port	Local IP Address	Start Port Local	End Port Local	Edit	Delete
0	N/A	N/A	N/A	N/A	N/A	N/A		
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		

Virtual Server for: Indicate the related WAN interface to allow outside network to connect in and communicate with internal LAN devices.

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 your server IP address in this field.

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-1000 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-1000 will forward port 21 request from WAN to the specific LAN PC (Example: 192.168.1.102) in the network.

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

Virtual Server

Virtual Server for

4G LTE -1

Protocol

TCP

Start Port Number

21

End Port Number

21

Local IP Address

192.168.1.110

Start Port Number (Local)

21

End Port Number(Local)

21

Save

Back

Virtual Server Listing

Index	Protocol	Start Port	End port	Local IP Address	Start Port Local	End Port Local	Edit	Delete
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		

Static DNS

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

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

Static DNS

IP Address

Domain Name

Save

Static DNS Listing

Index	IP Address	Domain Name	Edit	Delete
-------	------------	-------------	------	--------

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

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

Click **Save** to apply your settings.

Time Schedule

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

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

Time Schedule							
Rule Index	0 ▼						
Rule Name	TimeSlot1						
	Mon.	Tues.	Wed.	Thur.	Fri.	Sat.	Sun.
Day of Week	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Start Time	00:00	00:00	00:00	00:00	00:00	00:00	00:00
End Time	00:00	00:00	00:00	00:00	00:00	00:00	00:00
Save							

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

Name: User-defined identification for each time period.

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

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

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

Click **Save** to apply your settings.

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

Time Schedule							
Rule Index	0 ▼						
Rule Name	TimeSlot1						
	Mon.	Tues.	Wed.	Thur.	Fri.	Sat.	Sun.
Day of Week	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Start Time	09:00	00:00	00:00	00:00	00:00	00:00	00:00
End Time	24:00	18:00	00:00	00:00	00:00	00:00	00:00
Save							

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

Time Schedule							
Rule Index	1 ▼						
Rule Name	TimeSlot2						
	Mon.	Tues.	Wed.	Thur.	Fri.	Sat.	Sun.
Day of Week	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Start Time	00:00	00:00	09:00	00:00	00:00	00:00	00:00
End Time	00:00	00:00	18:00	00:00	00:00	00:00	00:00
Save							

Mail Alert

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

Mail Alert	
Server Information	
SMTP Server	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password"/>
Sender's E-mail	<input type="text"/> (Must be XXX@yyy.zzz)
SSL/TLS	<input type="checkbox"/> Enable
Port	<input type="text" value="25"/> (1~65535)
<input type="button" value="Account Test"/>	
WAN IP Change Alert	
Recipient's E-mail	<input type="text"/> (Must be XXX@yyy.zzz)
3G/LTE Usage Allowance	
Recipient's E-mail	<input type="text"/> (Must be XXX@yyy.zzz)
<input type="button" value="Apply"/>	

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.

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

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

Click **Apply** button to save your settings

Remote System Log

▼ Remote System Log

Remote System Log	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
Server IP Address	<input type="text" value="0.0.0.0"/>
Server UDP Port	<input type="text" value="514"/>
<input type="button" value="Save"/>	

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

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

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

Click **Save** to apply the settings

Access Management

Features including **Device Management**, **SNMP**, **Universal Plug & Play**, **Dynamic DNS**, **Access Control**, **Packet Filter**, **CWMP (TR-069)**, and **Parental Control**.

Device Management

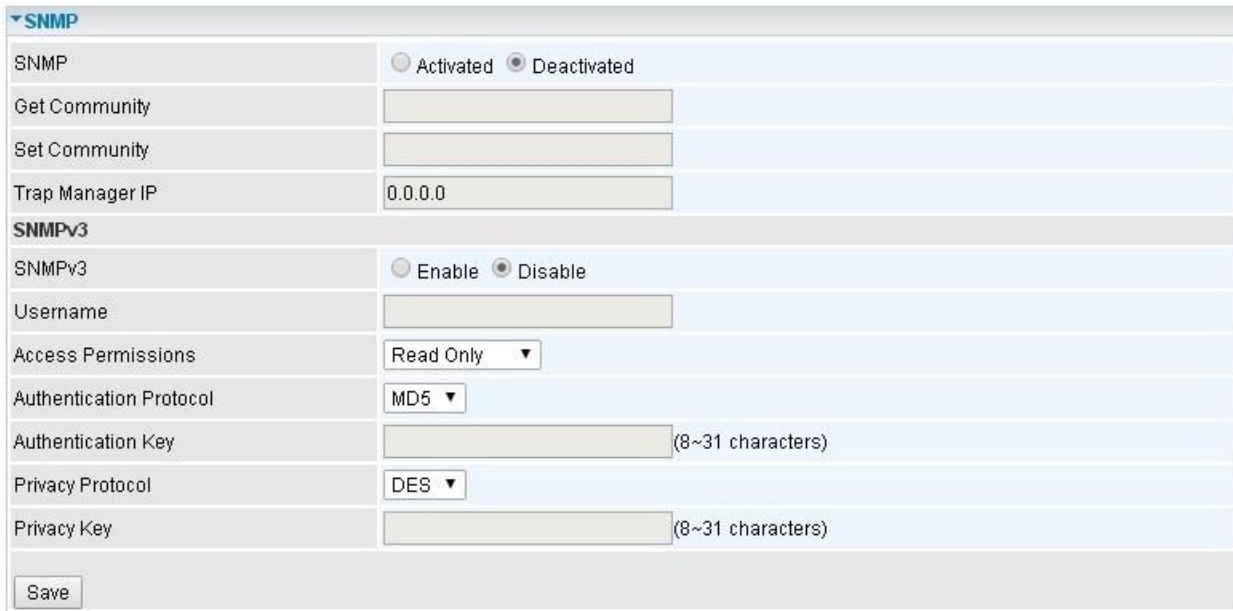
Device management offers users a way to change the embedded web server accessing port, default 80. User can change the http port to 8080 or something else here.

▼ Device Management	
Device Host Name	
Host Name	<input type="text" value="home_gateway"/>
<input type="button" value="Save"/>	
Embedded Web Server	
HTTP Port	<input type="text" value="80"/> (The default HTTP port number is 80.)
<input type="button" value="Save"/>	

Click **Save** to apply the settings.

SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. The MX-1000 serves as a SNMP agent that allows a manager station to manage and monitor the router through the network.



The screenshot shows a web-based configuration interface for SNMP. It is divided into two main sections: 'SNMP' and 'SNMPv3'. The 'SNMP' section includes radio buttons for 'Activated' and 'Deactivated' (selected), text input fields for 'Get Community' and 'Set Community', and a text input field for 'Trap Manager IP' with the value '0.0.0.0'. The 'SNMPv3' section includes radio buttons for 'Enable' and 'Disable' (selected), text input fields for 'Username', 'Authentication Key' (with a note '(8~31 characters)'), and 'Privacy Key' (with a note '(8~31 characters)'), a dropdown menu for 'Access Permissions' set to 'Read Only', and dropdown menus for 'Authentication Protocol' set to 'MD5' and 'Privacy Protocol' set to 'DES'. A 'Save' button is located at the bottom left of the form.

SNMP: Select to enable SNMP feature.

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.

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.

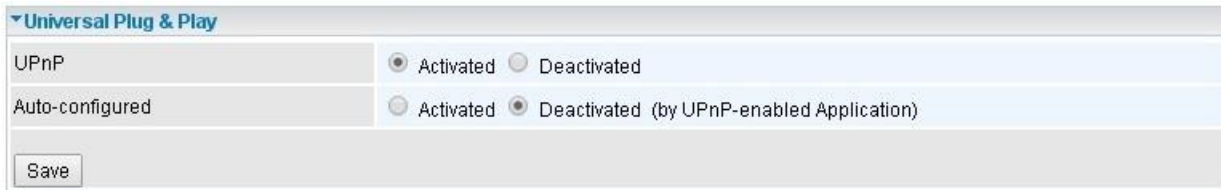
Privacy Key: Set the privacy key, 8-31 characters.

Click **Save** to apply the settings.

Universal Plug & Play

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

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



Universal Plug & Play	
UPnP	<input checked="" type="radio"/> Activated <input type="radio"/> Deactivated
Auto-configured	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated (by UPnP-enabled Application)
Save	

UPnP: Select this checkbox to activate UPnP. Be aware that anyone could use an UPnP application to open the web configuration's login screen without entering the MX-1000's IP address

Auto-configured: Select this check box to allow UPnP-enabled applications to automatically configure the MX-1000 so that they can communicate through the MX-1000, 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 the settings.

Dynamic DNS (DDNS)

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

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

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

Dynamic DNS	
Dynamic DNS	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
Service Provider	www.dyndns.org (dynamic) ▼
My Host Name	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password"/>
Wildcard support	<input type="radio"/> Yes <input checked="" type="radio"/> No
Period	25 Day(s) ▼
<input type="button" value="Save"/>	

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

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

My Host Name: Type the domain name assigned to your MX-1000 by your Dynamic DNS provider.

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

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

Period: Set the time period on how often the MX-1000 will update the DDNS server with your current external IP address.

Click **Save** to apply the 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

Dynamic DNS	
Dynamic DNS	<input checked="" type="radio"/> Activated <input type="radio"/> Deactivated
Service Provider	<input type="text" value="www.dyndns.org (dynamic)"/>
My Host Name	<input type="text" value="myhome.dyndns.org"/>
Username	<input type="text" value="myhome-123"/>
Password	<input type="password" value="*****"/>
Wildcard support	<input type="radio"/> Yes <input checked="" type="radio"/> No
Period	<input type="text" value="25"/> <input type="text" value="Day(s)"/>
<input type="button" value="Save"/>	

Access Control

Access Control Listing allows you to determine which services/protocols can access the MX-1000 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

☒ Activated
 ☐ Deactivated

Access Control Editing

Rule Index

1 ▼

Active

☒ Yes
 ☐ No

Secure IP Address

~
(0.0.0.0 ~ 0.0.0.0 means all IPs)

Application

ALL ▼

Interface

LAN ▼

Save

Delete

Access Control Listing

Index	Active	Secure IP Address	Application	Interface
1	Yes	0.0.0.0-0.0.0.0	ALL	LAN
2	Yes	0.0.0.0-0.0.0.0	Ping	WAN

Access Control: Select whether to make Access Control function available.

Rule Index: The numeric rule indicator.

Active: **Yes** to activate the rule.

Secure IP Address: The default 0.0.0.0 allows any client to use this service to manage the MX-1000. Type an IP address range to restrict access to the client(s) without a matching IP address.

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

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

Click **Save** to apply the 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.

Access Control

☒ Activated
 ☐ Deactivated

Access Control Editing

Rule Index

1 ▼

Active

☒ Yes
 ☐ No

Secure IP Address

0.0.0.0 ~ 0.0.0.0 (0.0.0.0 ~ 0.0.0.0 means all IPs)

Application

ALL ▼

Interface

LAN ▼

Save

Delete

Access Control Listing

Index	Active	Secure IP Address	Application	Interface
1	Yes	0.0.0.0-0.0.0.0	ALL	LAN
2	Yes	0.0.0.0-0.0.0.0	Ping	WAN

Default Rule 2: (Index 2), an ACL rule to open Ping to WAN side.

Access Control

☒ Activated
 ☐ Deactivated

Access Control Editing

Rule Index

2 ▼

Active

☒ Yes
 ☐ No

Secure IP Address

0.0.0.0 ~ 0.0.0.0 (0.0.0.0 ~ 0.0.0.0 means all IPs)

Application

Ping ▼

Interface

WAN ▼

Save

Delete

Access Control Listing

Index	Active	Secure IP Address	Application	Interface
1	Yes	0.0.0.0-0.0.0.0	ALL	LAN
2	Yes	0.0.0.0-0.0.0.0	Ping	WAN

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.

IP/MAC Filter Listing

Index #: The numeric rule indicator.

Active: Whether the connection is currently active.

Interface: show the interface the rule applied to.

Direction: show the direction the rule applied to.

Source IP (IPv6) Address/Mask (Prefix): The source IP address or range of packets to be monitored.

Destination IP (IPv6) Address/Mask (Prefix): This is the destination subnet IP address.

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

Source Port: The source port number of packets to be monitored.

Destination Port: 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**

Click **Save** to apply the settings.

❖ Filter Type - Application Filter

Packet Filter

Packet Filter

Filter Type

Application Filter ▼

Application Filter Editing

Application Filter	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
ICQ	<input checked="" type="radio"/> Allow <input type="radio"/> Deny
MSN	<input checked="" type="radio"/> Allow <input type="radio"/> Deny
YMSG	<input checked="" type="radio"/> Allow <input type="radio"/> Deny
Real Audio/Video(RTSP)	<input checked="" type="radio"/> Allow <input type="radio"/> Deny

Save

Application Filter: Select this option to Activated/Deactivated the Application filter.

ICQ: Select this option to Allow/Deny ICQ.

MSN: Select this option to Allow/Deny MSN.

YMSG: Select this option to Allow/Deny Yahoo messenger.

Real Audio/Video (RTSP): Select this option to Allow/Deny Real Audio/Video (RTSP).

Click **Save** to apply the settings.

❖ Filter Type- URL Filter

▼Packet Filter

Packet Filter

Filter Type

URL Filter ▼

URL Filter Editing

URL Filter

☐ Activated
☒ Deactivated

URL Filter Rule Index

1 ▼

Individual Active

☐ Yes
☒ No

URL (Host)

Save

Delete

URL Filter Listing

Index	Active	URL
-------	--------	-----

URL Filter: Select **Activated** to enable URL Filter.

URL Filter Rule Index: The numeric rule indicator.

Individual Active: To give control to the specific URL access individually, for example, you want to prohibit access to www.yahoo.com, please first press Activated in “URL Filter” field, and also Yes in “Individual Active” field; if some time you want to allow access to this URL, you simply select No in individual active field. In a word, the command serves as a switch to the access of some specific URL with the filter on.

URL (Host): Specified URL which is prohibited from accessing.

Click **Save** to apply the settings.

CWMP (TR-069)

CWMP, short for CPE WAN Management Protocol, also called TR069 is a Broadband Forum technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices. It defines an application layer protocol for remote management of end-user devices.

As a bidirectional SOAP/HTTP based protocol it can provides the communication between customer premises equipment (CPE) and Auto Configuration Server (ACS). It includes both a safe configuration and the control of other CPE management functions within an integrated framework. In the course of the booming broadband market, the number of different internet access possibilities grew as well (e.g. modems, routers, gateways, set-top box, VoIP-phones).At the same time the configuration of this equipment became more complicated –too complicated for end-users. For this reason, TR-069 was developed. It provides the possibility of auto configuration of the access types. Using TR-069 the terminals can get in contact with the Auto Configuration Servers (ACS) and establish the configuration automatically and let ACS configure CPE automatically.

CWMP (TR-069)	
CWMP	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
ACS Login Information	
URL	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Connection Request Information	
Path	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Periodic Inform Config	
Periodic Inform	<input checked="" type="radio"/> Activated <input type="radio"/> Deactivated
Interval	<input type="text" value="5000"/>
NATT Config	
NATT Server	<input type="text"/>
NATT Period	<input type="text"/>
<input type="button" value="Save"/>	

CWMP: Select activated to enable CWMP.

ACS Login Information

URL: Enter the ACS server login URL.

User Name: Specify the ACS User Name for ACS authentication to the connection from CPE.

Password: Enter the ACS server login password.

Connection Request Information

Path: Local path in HTTP URL for an ACS to make a Connection Request notification to the CPE.

Username: Username used to authenticate an ACS making a Connection Request to the CPE.

Password: Password used to authenticate an ACS making a Connection Request to the CPE.

Periodic Inform Config

Periodic Inform: Select Activated to authorize the router to send an Inform message to the ACS automatically.

Interval(s): Specify the inform interval time (sec) which CPE used to periodically send inform message to automatically connect to ACS. When the inform interval time arrives, the CPE will send inform message to automatically connect to ACS.

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 the 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.

Parental Control Provider

Parental Control Provider provides Web content filtering while surfing the web safer and more reliable. Please get an account and configure at the selected Provider in advance.

Provider	www.opendns.com
Parental Control	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
Host Name	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password"/>

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 **Activated**

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

Username / Password: Put down your OpenDNS account username and password

Click **Save** to apply the settings.

SAMBA & FTP Server

Samba and FTP are served as network sharing.

▼ SAMBA & FTP Server	
SAMBA	
SAMBA Server	<input checked="" type="radio"/> Activated <input type="radio"/> Deactivated
Work Group	<input type="text" value="MyGroup"/>
Net BIOS Name	<input type="text" value="SambaSvr"/>
FTP	
FTP Server	<input checked="" type="radio"/> Activated <input type="radio"/> Deactivated
FTP Server Port	<input type="text" value="21"/>
<input type="button" value="Save"/>	

SAMBA

SAMBA Server: Activated to enable SAMBA sharing.

Work Group: The same mechanism like in Microsoft work group, please set the Work Group name.

NetBIOS Name: The sharing NetBIOS name.

FTP

FTP Server: Activated to enable FTP sharing.

FTP Server Port: Set the working port. Well-known one is 21. User can change it.

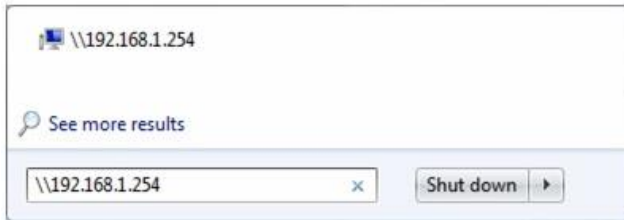
- ▶ **Default user:** admin/admin, it is the administrative user and a super user, it has the full authority of SAMBA /FTP access and operation permission of objects in SAMBA and FTP server.
- ▶ **New user:** users can create new user(s) to grant it (them) access and permission to the SAMBA & FTP server.

Please see [User Management](#).

Click **Save** to apply the settings.

Example: How to setup Samba

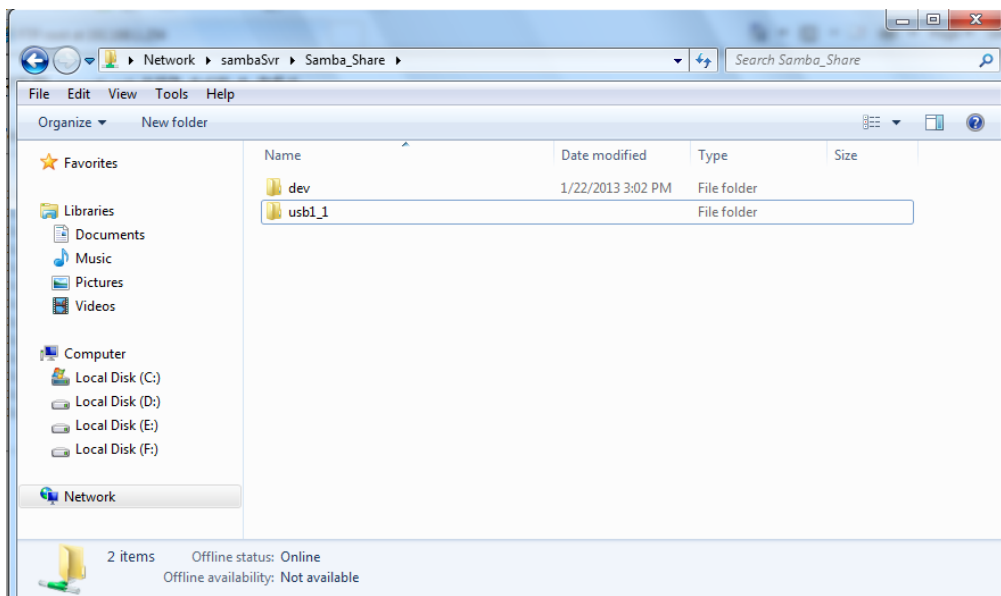
1. Go directly to Start > Run (enter [\\192.168.1.254](#) (from LAN side), [\\SambaSvr](#) , but if you enter [\\SambaSvr](#), please be sure your working PC is in the same workgroup as set in the samba server set above.)



2. Enter the Username and password.



3. Users can browse and access USB storage.

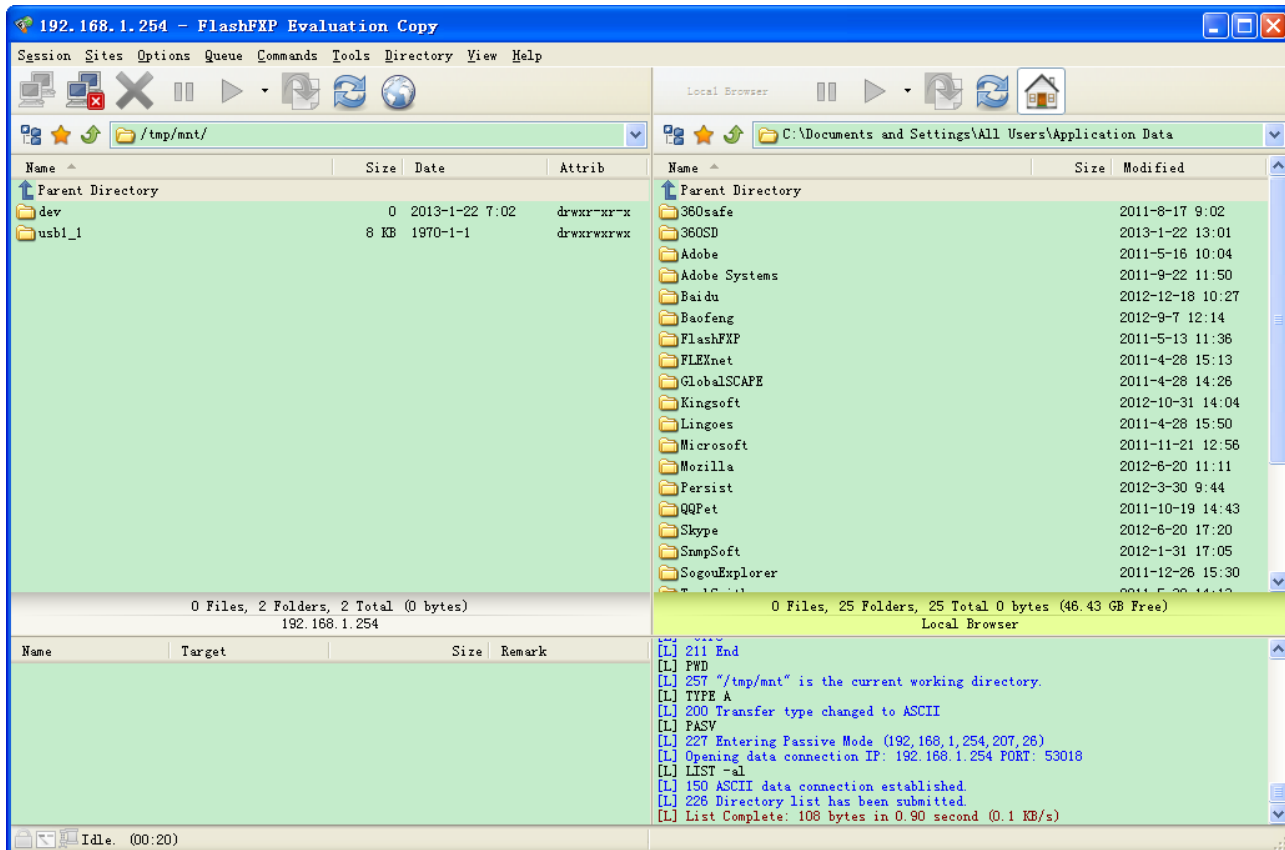


Example: How to setup FTP :

1. Access via FTP tools

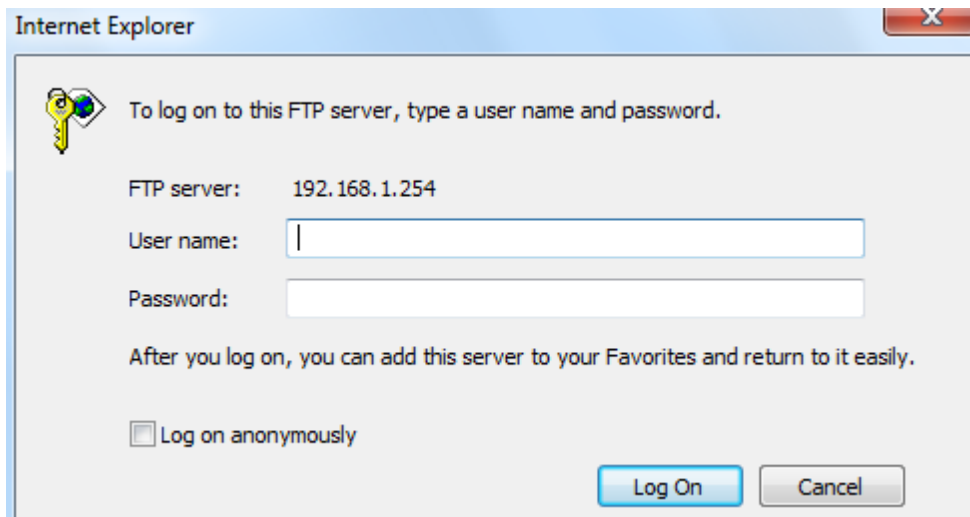
Take popular FTP tool of FlashFXP for example:

- 1) Open FlashFXP
- 2) Create ftp sites (LAN IP / WAN IP, 192.168.1.254, and set the account, port).
- 3) Connect to the ftp site.



2. Web FTP access

- 1) Enter <ftp://192.168.1.254> at the address bar of the web page.
- 2) Enter the account's username and password.



FTP Authority Setup

FTP Access: Enable to grant the user access to the FTP server.

Permission: Set the operation permission for the user, Read/Write or Read.

SAMBA Authority

SAMBA Access: Enable to grant the user access to the SAMBA server.

Permission: Set the operation permission for the user, Read/Write or Read.

Web GUI Permission

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 Account

user/user is the default user account username and password

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

▼ User Management

User Account

Index

2 ▼

Username

user

New Password

Confirm Password

FTP Authority Setup

FTP Access

☐ Enable
 ☒ Disable

Permission

☐ Read/Write
 ☒ Read

SAMBA Authority Setup

SAMBA Access

☐ Enable
 ☒ Disable

Permission

☐ Read/Write
 ☒ Read

Web GUI Permission

Guest Account

☐ Enable
 ☒ Disable

Interface Setup

☒ Enable
 ☐ Disable

Advanced Setup

☒ Enable
 ☐ Disable

Access Management

☒ Enable
 ☐ Disable

Maintenance

☒ Enable
 ☐ Disable

Please restart the Storage server after config changed

Save

Delete

User Account Listing

Index	User Name	FTP Access	FTP Permission	SAMBA Access	SAMBA Permission
1	admin	Enable	Read/Write	Enable	Read/Write
2	user	Disable	Read	Disable	Read

User Account Setup

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

User Name: Users can create account(s) to give it (them) access to SAMBA and FTP.

New Password: Password for the user account.

Confirm Password: Re-enter the password.

FTP Authority Setup

FTP Access: Enable to grant the user access to the FTP server.

Permission: Set the operation permission for the user, Read/Write or Read.

SAMA Authority Setup

SAMBA Access: Enable to grant the user access to the SAMBA server.

Permission: Set the operation permission for the user, Read/Write or Read.

Web GUI Permission

Guest Account: Enable to create this new guest account.

Interface Setup / Advanced Setup / Access Management Setup / Maintenances: Enable to grant this user access to these features.

When someone accesses to the MX-1000 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 the settings.

Time Zone

With default, MX-1000 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-1000. If you plan to use **Time Schedule** feature, it is extremely important you set up the Time Zone correctly.

Time Zone	
Current Date/Time	N/A (Can't find NTP server)
Time Synchronization	
Synchronize time with	<input checked="" type="radio"/> NTP Server <input type="radio"/> PC's Clock <input type="radio"/> Manually
Time Zone	(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London ▼
Daylight Saving	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
NTP Server Address	0.0.0.0 (0.0.0.0: Default Value)
<input type="button" value="Save"/>	

Synchronize time with: Select the methods to synchronize the time.

- ▶ **NTP Server automatically:** To synchronize time with the SNTP servers to get the current time from an SNTP server outside your network then choose your local time zone. After a successful connection to the Internet, MX-1000 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.

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.

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-1000 provides an easy way to update the code to take advantage of the changes. .

To upgrade the firmware of the MX-1000, 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-1000 will automatically restart and run the new firmware.

Firmware & Configuraiton	
Upgrade	<input checked="" type="radio"/> Firmware <input type="radio"/> Configuration
System Restart with	<input checked="" type="radio"/> Current Settings <input type="radio"/> Factory Default Settings
File	<input type="button" value="Choose File"/> No file chosen
Backup Configuration	<input type="button" value="Backup"/>
Status	
It might take several minutes, don't power off it during upgrading. Device will restart after the upgrade.	
<input type="button" value="Upgrade"/>	

Upgrade: Choose Firmware or Configuration you want to update.

System Restart with:

- ▶ **Current Settings:** Restart the device with the current settings automatically when finishing upgrading.
- ▶ **Factory Default Settings:** Restart the device with factory default settings automatically when finishing upgrading.

File: Type in the location of the file you want to upload in this field or click **Browse** to find it.

Choose File: Click “**Choose File**” to find the configuration file or firmware file you want to upload. Remember that you must extract / decompress / unzip the .zip files before you can upload them.

Backup Configuration: Click **Backup** button to back up the current running configuration file and save it to your computer in the event that you need this configuration file to be restored back to your MX-1000 device when making false configurations and want to restore to the original settings.

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

Firmware Upgrade	
File upload succeeded, starting flash erasing and programming!!	
Progress	<div><div></div></div>
Percent	15 %



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

Improper operation could damage your MX-1000.

System Restart

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



▼ System Restart

System Restart with

☒ Current Settings

☐ Factory Default Settings

Restart

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-1000 to ensure proper operation and best performance. This reboot will only reboot with current configuration settings and not overwrite any existing settings.

Auto Reboot											
Schedule	1.	<input type="checkbox"/> Enable	<input type="checkbox"/> Mon.	<input type="checkbox"/> Tues.	<input type="checkbox"/> Wed.	<input type="checkbox"/> Thur.	<input type="checkbox"/> Fri.	<input type="checkbox"/> Sat.	<input type="checkbox"/> Sun.	Time	00 : 00
	2.	<input type="checkbox"/> Enable	<input type="checkbox"/> Mon.	<input type="checkbox"/> Tues.	<input type="checkbox"/> Wed.	<input type="checkbox"/> Thur.	<input type="checkbox"/> Fri.	<input type="checkbox"/> Sat.	<input type="checkbox"/> Sun.	Time	00 : 00
<input type="button" value="Save"/>											

Click **Save** to apply the settings

Example: Schedule MX-1000 to reboot at 10:00pm (22:00) every weekday (Monday thru Friday) and reboot at 9:00am on Saturday and Sunday.

Auto Reboot											
Schedule	1.	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Mon.	<input checked="" type="checkbox"/> Tues.	<input checked="" type="checkbox"/> Wed.	<input checked="" type="checkbox"/> Thur.	<input checked="" type="checkbox"/> Fri.	<input type="checkbox"/> Sat.	<input type="checkbox"/> Sun.	Time	22 : 00
	2.	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Mon.	<input type="checkbox"/> Tues.	<input type="checkbox"/> Wed.	<input type="checkbox"/> Thur.	<input type="checkbox"/> Fri.	<input checked="" type="checkbox"/> Sat.	<input checked="" type="checkbox"/> Sun.	Time	09 : 00
<input type="button" value="Save"/>											

Diagnostics Tool

The Diagnostic Test page shows the test results for the connectivity of the physical layer and protocol layer for both LAN and WAN sides.

3G/4G-LTE

Diagnostic Tool	
WAN Interface	4G LTE -1 ▼
Testing Ethernet LAN Connection	N/A
Ping Primary DNS (N/A)	N/A
Ping www.google.com	N/A
Ping other IP Address <input type="radio"/> Yes <input checked="" type="radio"/> No	N/A
Start	

Click START to begin to diagnose the connection.

Diagnostic Tool	
WAN Interface	4G LTE -1 ▼
Testing Ethernet LAN Connection	PASS
Ping Primary DNS (168.95.1.1)	PASS
Ping www.google.com	PASS
Ping other IP Address <input checked="" type="radio"/> Yes <input type="radio"/> No	PASS
IP Address	8.8.8.8
Start	

EWAN

Diagnostic Tool	
WAN Interface	EWAN ▼
Testing Ethernet LAN Connection	N/A
Ping Primary DNS (139.175.1.1)	N/A
Ping www.google.com	N/A
Ping other IP Address <input type="radio"/> Yes <input checked="" type="radio"/> No	N/A
Start	

Click START to begin to diagnose the connection.

Diagnostic Tool	
WAN Interface	EWAN ▼
Testing Ethernet LAN Connection	PASS
Ping Primary DNS (139.175.1.1)	PASS
Ping www.google.com	PASS
Ping other IP Address <input type="radio"/> Yes <input checked="" type="radio"/> No	Skipped
Start	

Chapter 5: Troubleshooting

If your MX-1000 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
<ul style="list-style-type: none">- The front LEDs display incorrectly- Still cannot access to the router management interface after pressing the RESET button.- Software / Firmware upgrade failure	<p>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.</p> <ol style="list-style-type: none">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-1000

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 7/98, Windows NT, Windows 2000, Windows ME, Windows XP, and Windows Vista 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.