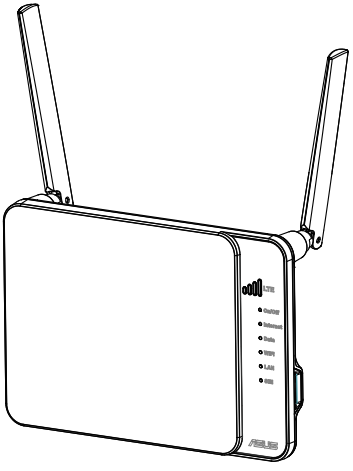
User Guide

4G-N12

Wireless-N300 LTE Modem Router



IN SEARCH OF INCREDIBLE

E9553
First Edition
November 2014

Contents

Contents

1 Getting to know your wireless router

1.1 Welcome!

Thank you for buying an ASUS 4G-N12 Wireless LTE Router!

ASUS 4G-N12 Wireless LTE Router features a 4G network module, letting you insert a SIM/USIM card to access and share your 4G LTE or 3G network connection via a secure wireless network or any of the four Ethernet ports. It offers a download speed of 100 Mbps and upload speed of 50 Mbps for fast Internet access, seamless media streaming, or easy data transfer.

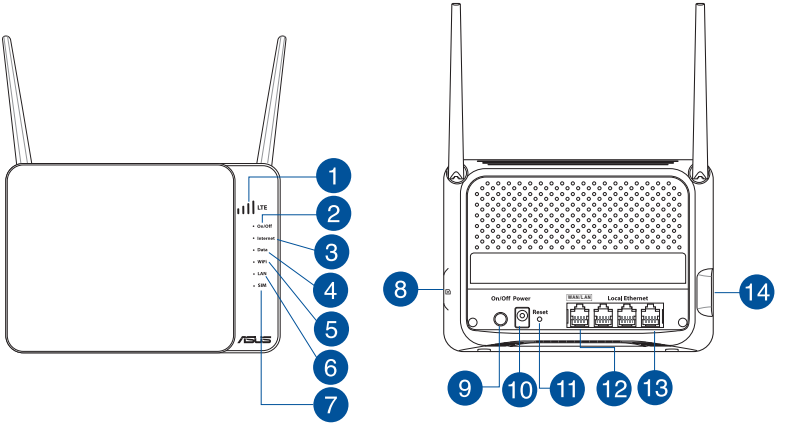
1.2 Package contents

- ☑ 4G-N12 Wireless Router
- ☑ Power adapter
- ☑ Network cable (RJ-45)
- ☑ Quick Start Guide

NOTES:

- If any of the items are damaged or missing, contact ASUS for technical inquiries and support, Refer to the ASUS Support Hotline list at the back of this user guide.
- Keep the original packaging material in case you would need future warranty services such as repair or replacement.

1.3 Your wireless router



1	**LTE signal strength LED 1~4** 1 lit LED: Very weak signal; 2 lit LEDs: Weak signal; 3 lit LEDs: Normal signal; 4 lit LEDs: Strong signal.
2	**Power LED** **Off**: No power. **On**: Device is ready.
3	**Internet LED** **Off**: No LTE connection. **Flashing**: Establishing a LTE/Ethernet WAN connection. **On**: Has a proper LTE/Ethernet WAN connection.
4	**Data LED (LTE/Ethernet WAN Traffic)** **Off**: No data activity. **On**: Data connection is ready.
5	**Wi-Fi LED** **Off**: No 2.4GHz signal. **On**: Wireless system is ready.
6	**LAN LED** **Off**: No power or no physical connection. **On**: Ethernet connection is established.

7	**USIM Card LED** **Off**: No USIM card is installed. **On**: A USIM card is installed properly.
8	**USIM card slot** Install a USIM card into this slot to establish a WAN LTE connection.
9	**Power button** Press this button to power on or off the stystem. 
10	**Power (DC-IN) port** Insert the bundled AC adapter into this port and connect your router to a power source.
11	**Reset button** Press this button for 5 seconds or longer to reset or restore the system to its factory default settings.
12	**WAN/LAN port** Using an Ethernet cable, connect your modem to the WAN/LAN port of your wireless router.
13	**LAN ports** Connect network cables into these ports to establish LAN connection.
14	**WPS button** This button launches the WPS Wizard.

NOTES:

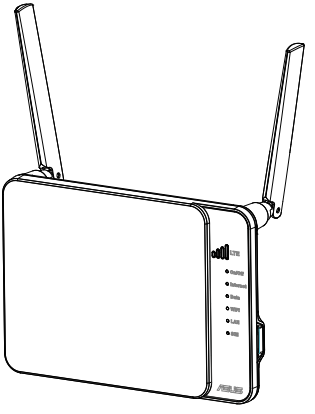
- Use only the adapter that came with your package. Using other adapters may damage the device.
- Ensure to insert the SIM card into the card slot before powering on the router.
- **Specifications:**

DC Power adapter	DC Output: +12V with max 1A current;		
Operating Temperature	0~40°C	Storage	0~70°C
Operating Humidity	50~90%	Storage	20~90%

1.4 Positioning your router

For the best wireless signal transmission between the wireless router and the devices connected to it, ensure that you:

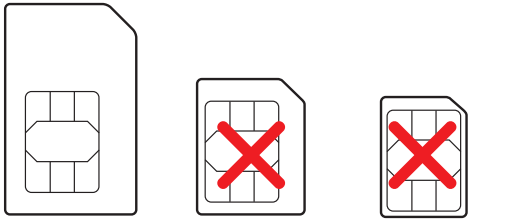
- Place the Wireless LTE Router near a window to receive the best LTE signal quality for maximum upstream performance with an LTE base station.
- Keep the device away from metal obstructions and away from direct sunlight.
- Do not place the Wireless LTE Router in a dusty or wet environment.
- Keep the device away from 802.11g or 20MHz-only Wi-Fi devices, 2.4GHz computer peripherals, Bluetooth devices, cordless phones, transformers, heavy-duty motors, fluorescent lights, microwave ovens, refrigerators, and other industrial equipment to prevent signal interference or loss.
- Always update to the latest firmware. Visit the ASUS website at **http://www.asus.com** to get the latest firmware updates.
- To ensure the best wireless signal, orient the two antennas as shown in the drawing below.



1.5 Setup requirements

To set up your wireless network, you need to meet the following requirements:

- A mini SIM/USIM card with WCDMA and LTE subscription



Mini SIM card **Micro SIM card** **Nano SIM card**

NOTE: A standard SIM/USIM card is a standard mini SIM card.

IMPORTANT! Ensure that your SIM/USIM card is subscribed to WCDMA and LTE services. Contact your mobile service provider about these services.

CAUTION! Use only a standard SIM/USIM card on your router. Using a different form of SIM card, such a micro or nano SIM card, may damage your router.

- An ADSL/cable modem with Internet subscription
- A computer with Ethernet RJ-45 (LAN) port (10Base-T/100Base-TX) or a Wi-Fi-enabled device with a 2.4 GHz 802.11 b/g/n wireless interface
- Web browser such as Internet Explorer, Firefox, Safari, or Google Chrome

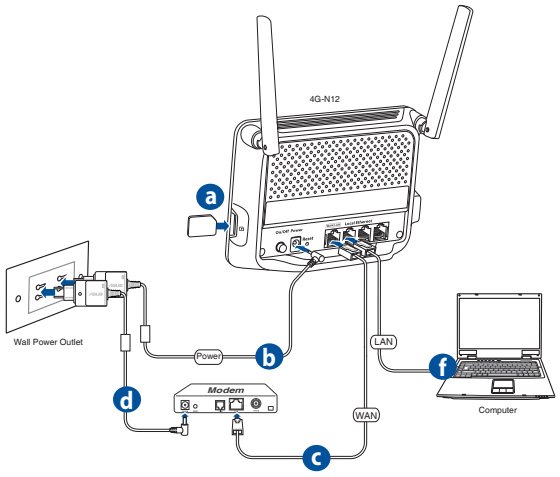
NOTES:

- If your computer does not have built-in wireless capabilities, you may install an IEEE 802.11 b/g/n WLAN adapter to your computer to connect to the network.
- Do not plug a phone jack into an RJ-45 port. This may damage the Wireless LTE Router.
- The Ethernet RJ-45 cables that will be used to connect the network devices should not exceed 100 meters.

1.6 Router Setup

WARNING!

- Avoid installing your Wireless LTE Router during an electrical storm. There may be a remote risk of electrical shock caused by lightning.
- Do not try to disassemble or reassemble this device. Tampering with your Wireless LTE Router might void its warranty.
- When mounting or cleaning the device, ensure to unplug the power cord from your Wireless LTE Router.
- Keep your hands dry when handling your Wireless LTE Router to avoid any possible electrical shock.



a. Insert the SIM/USIM card into the USIM card slot.

b. Insert the AC adapter of your router to the DC-IN port and plug it to a power outlet.

c. Using a network cable, connect your modem to the WAN/LAN port of your wireless router.

d. Insert the AC adapter of your modem to the DC-IN port and plug it to a power outlet.

e. Turn on your router.

f. Using the bundled network cable, connect your computer to the LAN port of your router.

g. To manually connect to a wireless network:

1. Enable the Wi-Fi function on your wireless client for it to automatically scan for wireless networks.
2. Select the wireless network named "ASUS", which is the default wireless network name (SSID) of ASUS wireless routers.
3. When prompted, key in the default password of the router, which can be found on the sticker at the back.

2 Getting started

2.1 Logging into the Web GUI

Your ASUS Wireless Router comes with an intuitive web graphical user interface (GUI) that allows you to easily configure its various features through a web browser such as Internet Explorer, Firefox, Safari, or Google Chrome.

NOTE: The features may vary with different firmware versions.

To log into the web GUI:

1. On your web browser, manually key in the wireless router's default IP address: **192.168.1.1** or enter http://router.asus.com.
2. On the login page, key in the default user name (**admin**) and password (**admin**).
3. You can now use the Web GUI to configure various settings of your ASUS Wireless Router.

NOTES:

- The default login password is **admin**. You can manually set up a new password that contains 3 to 16 case-sensitive alphanumeric characters.
- If the WAN connection is not ready, you will be directed to the Quick Internet Setup (QIS) page automatically.

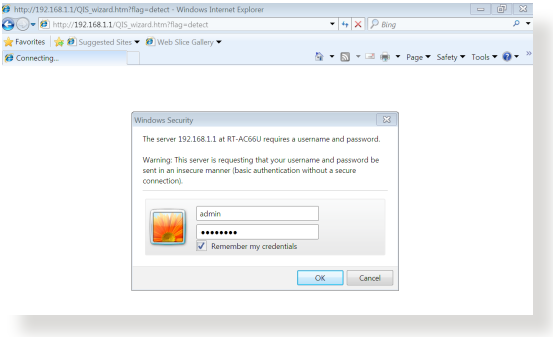
2.2 Quick Internet Setup (QIS) with Auto-detection

The Quick Internet Setup (QIS) function guides you in quickly setting up your Internet connection.

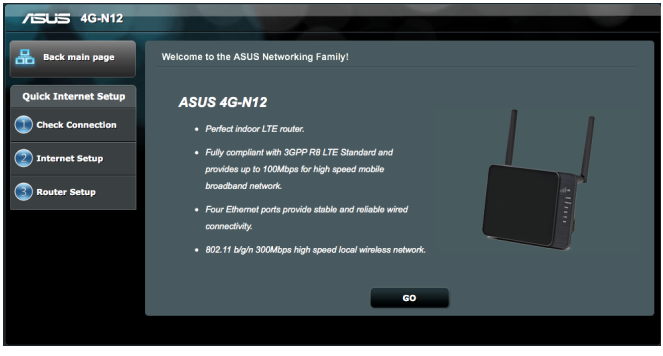
NOTE: When setting the Internet connection for the first time, press the Reset button on your wireless router to reset it to its factory default settings.

To use QIS with auto-detection:

1. Log into the Web GUI. The QIS page launches automatically.

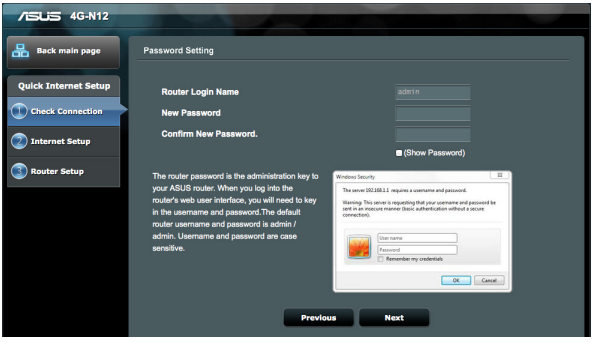


2. On the welcome page, click **Go** to continue.

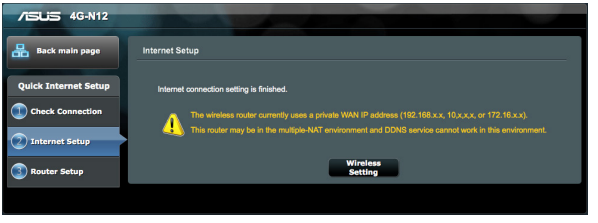


3. Change the password for the wireless router. When done, click **Next**.

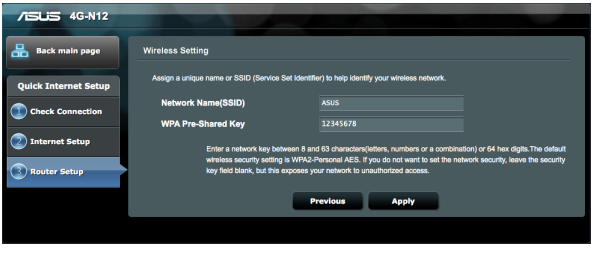
NOTE: We recommend that you assign a unique administrator password to protect your network from malicious attacks.



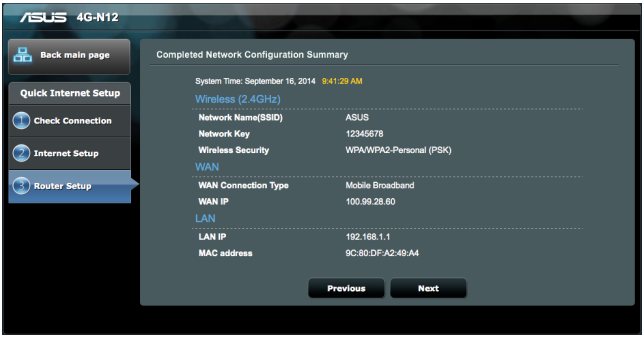
4. The wireless router automatically detects and applies the APN settings. When done, click **WLAN Setting** to configure the wireless LAN settings.



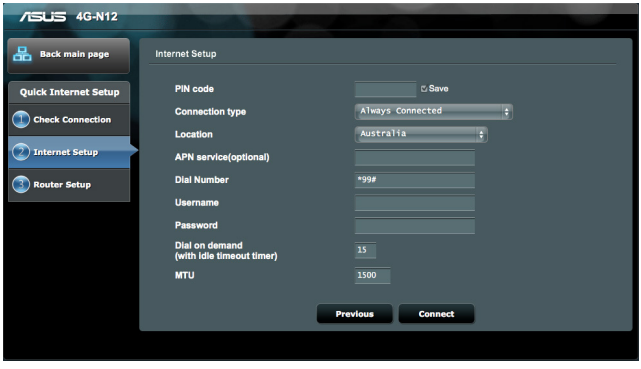
5. Assign a unique network name (SSID) and a network security key. When done, click **Apply**.



6. Your Internet and wireless settings are displayed. Click **Next** to continue.



7. If the wizard failed to apply the APN settings or the PIN code of the SIM card is required, you need to manually complete the mobile broadband connection. Key in the necessary APN settings and the PIN code of your SIM card. When done, click **Connect**.



NOTE: The auto-detection of your ISP connection takes place when you configure the wireless router for the first time or when your wireless router is reset to its default settings.

3 Configuring the General settings

3.1 Using the Network Map

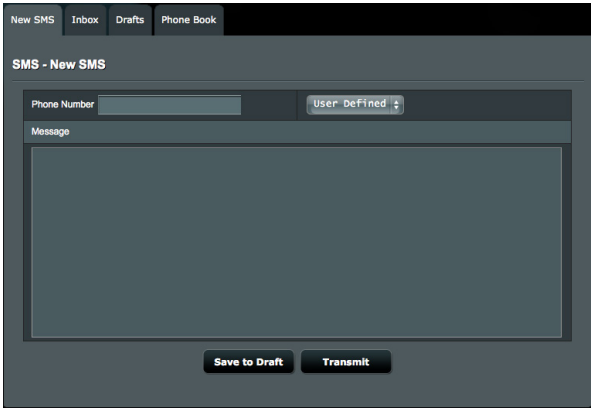
Network Map allows you to check the internet connection status, configure your network's security settings, and manage your network clients.

3.2 SMS

Short Message Service (SMS) is a text messaging service that allows you to send or receive messages from or on your wireless router.

3.2.1 New SMS

This function allows you to send short messages from your wireless router.



To send a new SMS message:

1. Enter the recipient's phone number.
2. Compose your message.
3. Click **Transmit** to send the message.

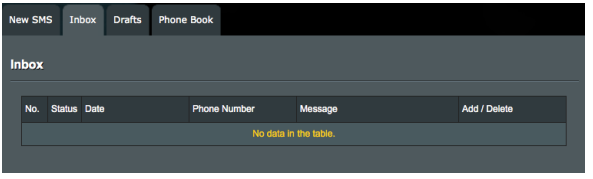
To save a SMS draft:

1. Enter the recipient's phone number.
2. Compose your message.
3. Click **Save to Draft** to save the message draft.

3.2.2 Inbox

Inbox allows you to view the received short messages saved in your device.

Click **Read** to read a message, or click **Delete** to delete a message.



3.2.3 Drafts

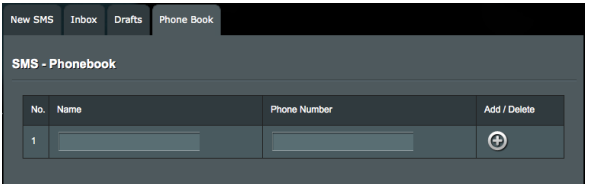
All the message drafts are saved in the Wireless LTE Router and displayed here.

Click **Transmit** to send a message, or click **Delete** to delete a message.

3.2.4 Phone Book

Phone Book allows you to save your frequent contacts' phone numbers.

To add a phone number, enter the name and phone number, and click  .



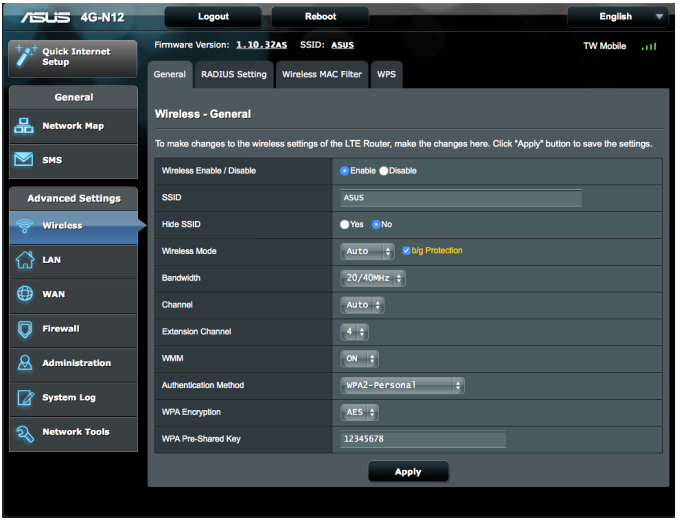
4 Configuring the Advanced Settings

4.1 Wireless

The Wireless LTE Router operates as a wireless access point, allowing wireless device to connect to the Internet. The GUI allows you to configure the radio channel, Service Set Identifier (SSID), security and WPS settings.

4.1.1 General

The General tab allows you to configure the basic wireless settings.



To configure the basic wireless settings:

1. From the navigation panel, go to **Advanced Settings** > **Wireless** > **General** tab.
2. **Wireless Enable / Disable**: Select **Enable** to use your router as a wireless access point.

3. Assign a unique name containing up to 32 characters for your SSID (Service Set Identifier) or network name to identify your wireless network. Wi-Fi devices can identify and connect to the wireless network via your assigned SSID. The SSIDs on the information banner are updated once new SSIDs are saved to the settings.
4. In the **Hide SSID** field, select **Yes** to prevent wireless devices from detecting your SSID. When this function is enabled, you would need to enter the SSID manually on the wireless device to access the wireless network.
5. Select any of these wireless mode options to determine the types of wireless devices that can connect to your wireless router:
   - **Auto**: Select **Auto** to allow 802.11ac, 802.11n, 802.11g, and 802.11b devices to connect to the wireless router.
   - **Legacy**: Select **Legacy** to allow 802.11b/g/n devices to connect to the wireless router. Hardware that supports 802.11n natively, however, will only run at a maximum speed of 54Mbps.
   - **N only**: Select **N only** to maximize wireless N performance. This setting prevents 802.11g and 802.11b devices from connecting to the wireless router.
   - **b/g Protection**: In most situations, the best performance is achieved with the wireless protected mode turned off. If you are using the router in an environment with heavy 802.11b, 802.11g traffic or serious interference, enable this function to ensure the best performance of your 802.11n throughput.
6. Select any of these channel bandwidth to accommodate higher transmission speeds:

   20/40MHz: Select this bandwidth to maximize the wireless throughput.

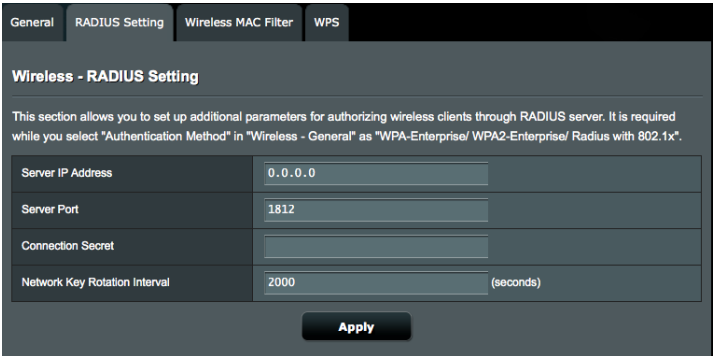
   20MHz (default): Select this bandwidth if you encounter some issues with your wireless connection.

7. Select the operating channel for your wireless router. Select **Auto** to allow the wireless router to automatically select the channel that has the minimum interference.
8. **Extension Channel**: The extension channel that you can assign is based on the following:
   - When Bandwidth is set to 20MHz, the extension channel is disabled.
   - When Wireless Channel (main channel) is set to 1, select channel 5 as the extension channel.
   - When the Wireless Channel is set to channel 9, select channel 5 or 13 as the extension channel.
9. **WMM**: Enables or disables the use of QoS. The QoS (Quality of Service) function allows you to differentiate WMM (Wi-Fi Multimedia) traffic and provide it with high-priority forwarding service.
10. Select any of these authentication methods:
    - **Open System**: This option provides no security.
    - **WPA/WPA2 Personal/WPA Auto-Personal**: This option provides strong security. You can use either WPA (with TKIP) or WPA2 (with AES). If you select this option, you must use TKIP + AES encryption and enter the WPA passphrase (network key).
    - **WPA/WPA2 Enterprise/WPA Auto-Enterprise**: This option provides very strong security. It is with integrated EAP server or an external RADIUS back-end authentication server.
11. When done, click **Apply**.

NOTE: Your wireless router supports the maximum transmission rate of 54Mbps when the Wireless Mode is set to Auto and the encryption method is WEP or TKIP.

4.1.2 RADIUS Setting

RADIUS (Remote Authentication Dial In User Service) Setting provides an extra layer of security when you choose WPA-Enterprise, WPA2-Enterprise, or RADIUS with 802.1x as your Authentication Mode.

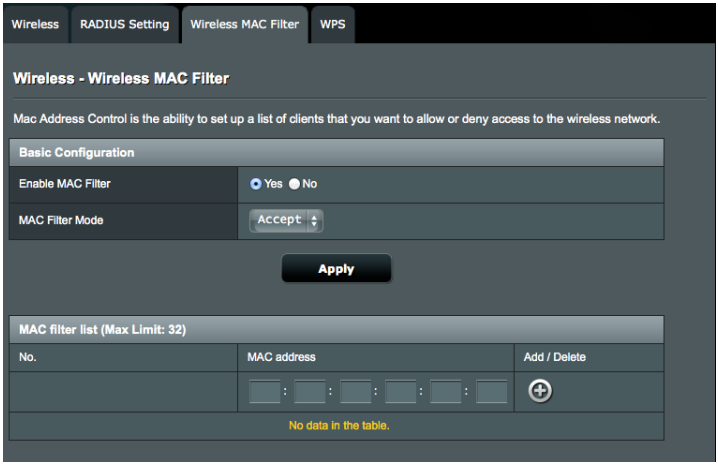


To configure the wireless RADIUS settings:

1. From the navigation panel, go to **Advanced Settings** > **Wireless** > **RADIUS Setting** tab.
2. **Server IP Address**: Enter the RADIUS server's IP Address in this field.
3. **Server Port**: Enter the RADIUS server's port number in this field.
4. **Connection Secret**: Enter the password to access your RADIUS server.
5. **Network Key Rotation Interval**: Define the renewal period that the RADIUS server sends a new encryption keys out to all clients.
6. When done, click **Apply**.

4.1.3 Wireless MAC Filter

Wireless MAC filter provides control over packets transmitted to a specified MAC (Media Access Control) address on your wireless network.

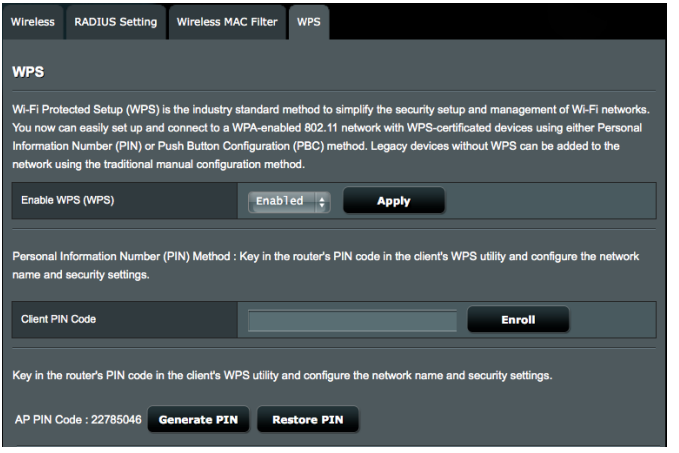


To set up the Wireless MAC filter:

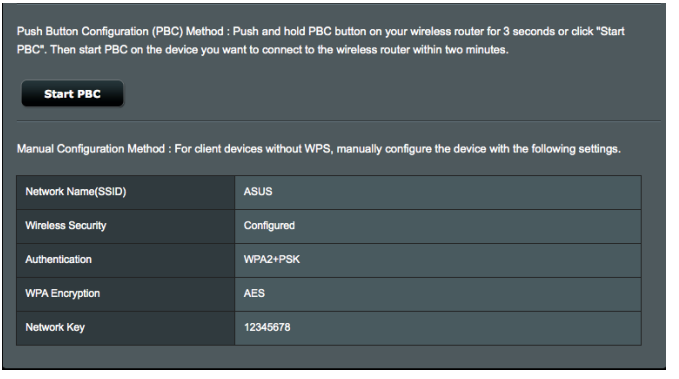
1. From the navigation panel, go to **Advanced Settings** > **Wireless** > **Wireless MAC Filter** tab.
2. In the **Enable MAC Filter** field, select **Yes** to enable Wireless MAC filter.
3. In the **MAC Filter Mode** dropdown list, select either **Accept** or **Reject**.
   - Select **Accept** to allow devices in the MAC filter list to access the wireless network.
   - Select **Reject** to prevent devices in the MAC filter list to access the wireless network.
4. On **the MAC filter list**, click ⊕ and key in the MAC address of the wireless device.
5. Click **Apply**.

4.1.4 WPS (Wi-Fi Protected Setup)

WPS (Wi-Fi Protected Setup) allows you easy create a secure wireless network via the PIN code or Push Button Control (PBC) feature.



Scroll down to display other items:



To create a secure network using WPS:

1. From the navigation panel, go to **Advanced Settings** > **Wireless** > **WPS** tab.
2. In the **Enable WPS** field, select **Enabled**, then click **Apply**.
3. Set up WPS via the PIN code or PBC (Push Button Control) method. Refer to the succeeding steps for more details.

To set up WPS via the PIN code method:

1. Power on your client device that supports WPS PIN (Personal Information Number) code method.
2. Enter the PIN code of the client device and click **Enroll**.

NOTE: The PIN code can be found either at the bottom of the packaging case or on the user interface of the client device.

3. Start the WPS PIN process on the client device.

NOTE: For details, refer to the user manual of the client device.

4. If you want to change the wireless router PIN code, click **Generate PIN** or **Restore PIN** to create or restore the PIN.

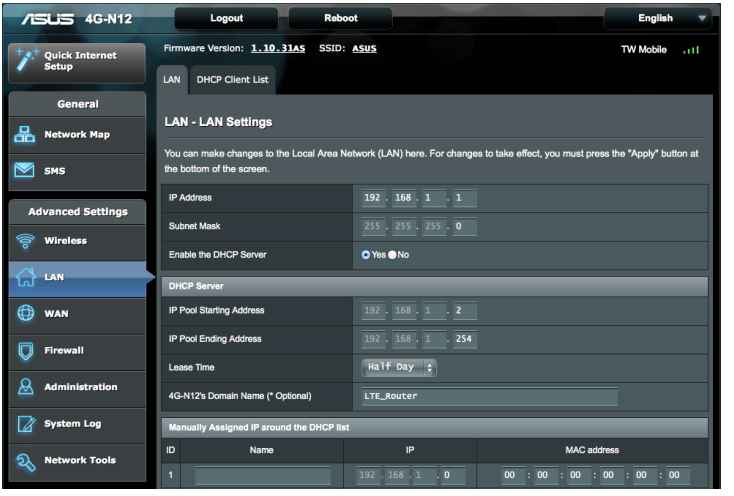
To set up WPS via the PBC method:

1. Power on your client device that supports WPS.
2. On your wireless router WPS screen, click **Start PBC**. You can also press the WPS button on the left side of your wireless router.
3. Press the WPS button on the client device.

4.2 LAN

4.2.1 LAN Settings

The LAN settings screen allows you to configure the local network IP address of the LTE Router and modify the DHCP server settings.



To modify the LAN settings:

1. From the navigation panel, go to **Advanced Settings** > **LAN** > **LAN** tab.
2. Enter the IP address and subnet mask of the wireless router.
3. In the **Enable the DHCP Server** field, select **Yes** or **No**. By default, the DHCP Server function is enabled.
4. In the **IP Pool Starting Address** field, key in the starting IP address.
5. In the **IP Pool Ending Address** field, key in the ending IP address.

NOTES:

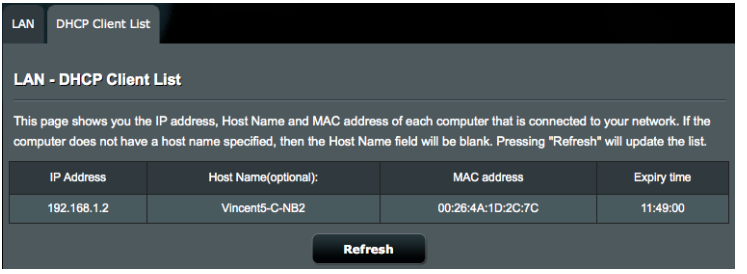
- We recommend that you use an IP address format of 192.168.1.xxx (where xxx can be any number between 2 and 254) when specifying an IP address range.
- An IP Pool Starting Addressn should not be greater than the IP Pool Ending Address.

6. In the **Lease Time** dropdown list, select the schedule when an IP address will expire. Once it reaches this specified schedule, the DHCP server will then assign a new IP address.

Static DHCP is a useful function, which allows you to bind specific client device with static IP address on your LAN. The IP address on DHCP server will be reserved for unique MAC address of a DHCP client device based on the settings below.

4.2.2 DHCP Client List

The DHCP Client List screen displays the DHCP client information. Click **Refresh** to update the connected client list.



4.3 WAN

The LTE Router is implemented with an LTE (Long Term Evolution) module. LTE network offers wide channel bandwidth from 5MHz to 20 MHz, and fast mobile data rates of up to 50 Mbps uplink and 100 Mbps downlink.

The supported bands show as below:

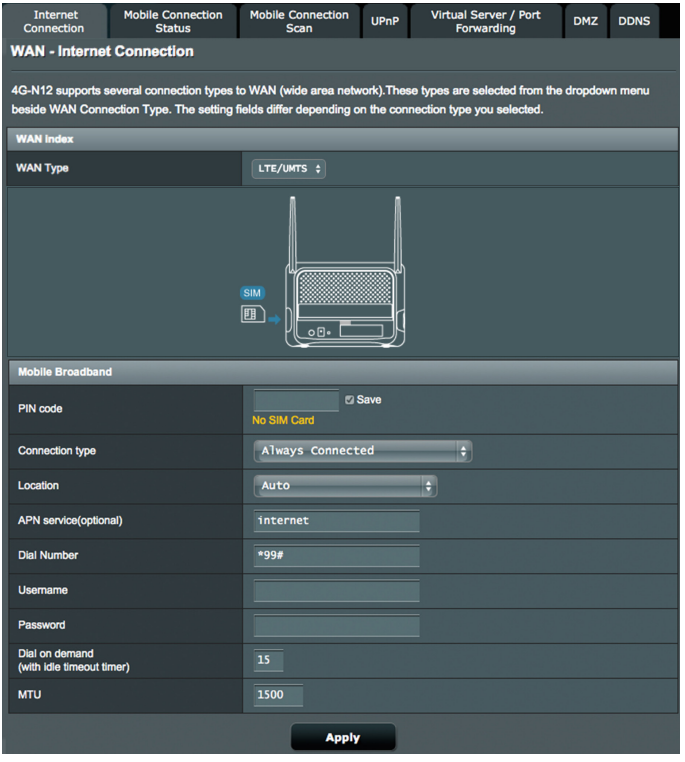
- LTE Band: FDD B3/7/20
  - LTE Cat. 3: DL: 100Mbps, UL: 50Mbps
- UMTS: B1/8
  - HSPA +: DL: 42Mbps, UL: 5.76Mbps

4.3.1 Internet Connection

To configure the Internet Connection settings:

1. From the navigation panel, go to **Advanced Settings** > **WAN** > **Internet Connection** tab.
2. In the **WAN Type** field, select **LTE/UMTS** or **WAN**.

- **WAN Type - LTE/UMTS**



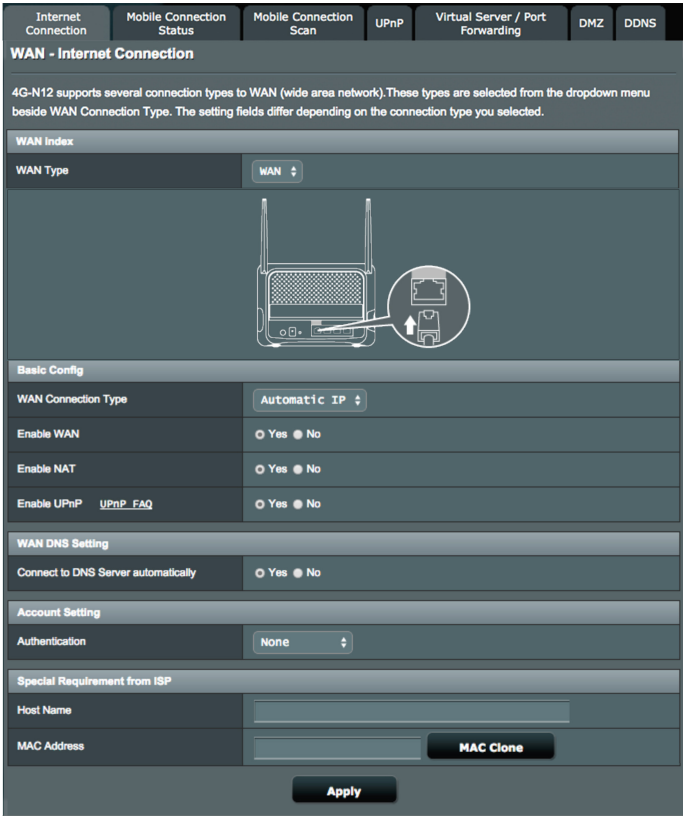
a. Set up the following:
   - **PIN Code**: Enter the 3G/4G provider's PIN code.
   - **Connection Type**: This field allows you to define your connection policies. We recommend you select **Auto-Triggered by traffic** if you are not using all-you-can-eat data service.
   - **Location**: Select your 3G/4G service provider's location from the dropdown list.
   - **APN services (optional)**: Enter the APN (Access Point Name) service information here. Contact your 3G/4G service provider for the detailed information.
   - **Dial Number**: Enter the 3G/4G provider's access number for connection.

- **Username / Password**: Enter the username and password provided by the 3G/4G network carrier.
- **Dial on demand (with idle timeout timer)**: Enter the time (in minutes) when the router goes into the sleep mode when there is no activity in the network.
- **MTU**: Sets the MTU (Maximum Transmission Unit).

b. Click **Apply** to connect to the 3G/4G network. The connection status will be displayed on **Mobile Connection Status** screen.

NOTE: The PIN code may vary with different providers.

- **WAN Type - WAN**



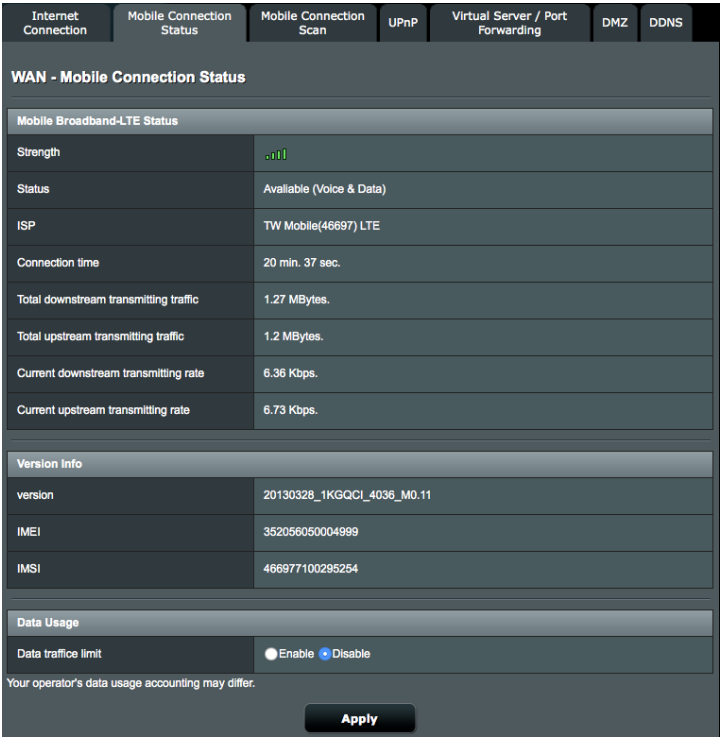
a. Configure the following settings below. When done, click **Apply**.

- **WAN Connection Type**: Choose your Internet Service Provider type. The choices are **Automatic IP**, **PPPoE** or **fixed IP**. Consult your ISP if the router is unable to obtain a valid IP address or if you are unsure the WAN connection type.
- **Enable WAN**: Select **Yes** to allow the router Internet access. Select **No** to disable Internet access.
- **Enable NAT**: NAT (Network Address Translation) is a system where one public IP (WAN IP) is used to provide Internet access to network clients with a private IP address in a LAN. The private IP address of each network client is saved in a NAT table and is used to route incoming data packets.
- **Connect to DNS Server**: Allows this router to get the DNS IP address from the ISP automatically. A DNS is a host on the Internet that translates Internet names to numeric IP addresses.
- **Authentication**: This item may be specified by some ISPs. Check with your ISP and fill them in if required.
- **Host Name**: This field allows you to provide a host name for your router. It is usually a special requirement from your ISP. If your ISP assigned a host name to your computer, enter the host name here.
- **MAC Address**: MAC (Media Access Control) address is a unique identifier for your networking device. Some ISPs monitor the MAC address of networking devices that connect to their service and reject any unrecognized device that attempt to connect. To avoid connection issues due to an unregistered MAC address, you can:
  - Contact your ISP and update the MAC address associated with your ISP service.

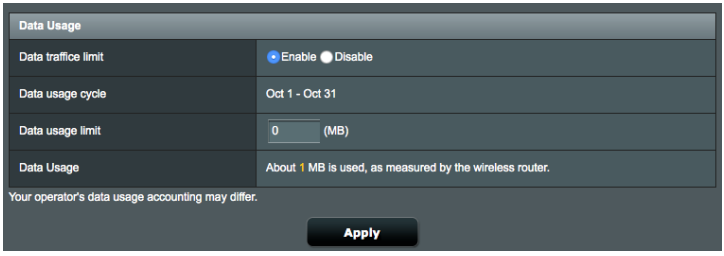
- Clone or change the MAC address of the ASUS wireless router to match the MAC address of the previous networking device recognized by the ISP.

4.3.2 Mobile Connection Status

The Mobile Connection Status screen displays the detailed Mobile Broadband connection status.



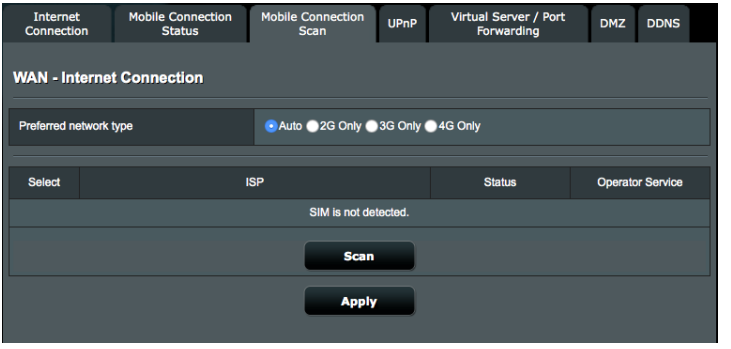
Scroll down to display other items:



To configure the Data Usage settings:

1. From the navigation panel, go to **Advanced Settings** > **WAN** > **Mobile Connection Status** tab.
2. **Data traffic limit**: Select **Enable** to allow setting a limit for your Internet traffic usage.
3. **Data usage limit**: Set a monthly upper limit for the Internet usage. When your data usage reaches the limit, the Internet access will be blocked
4. Click **Apply**.

4.3.3 Mobile Connection Scan



To select your preferred mobile broadband connection:

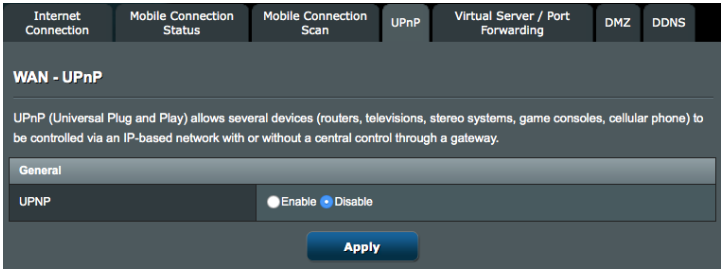
1. On the **Preferred network type** field, select a UMTS frequency band.
2. Click **Scan** to show all the available mobile networks.
3. Select a mobile network and click **Apply** to connect to it.

NOTES:

- The LTE Router can detect your ISP based on the IMSI information of your SIM card. If the mobile network from your ISP is not found, connect to a roaming network of other ISPs.
- Using a roaming service will incur additional charges. Inquire from your mobile service provider before using the roaming service.

4.3.4 UPnP

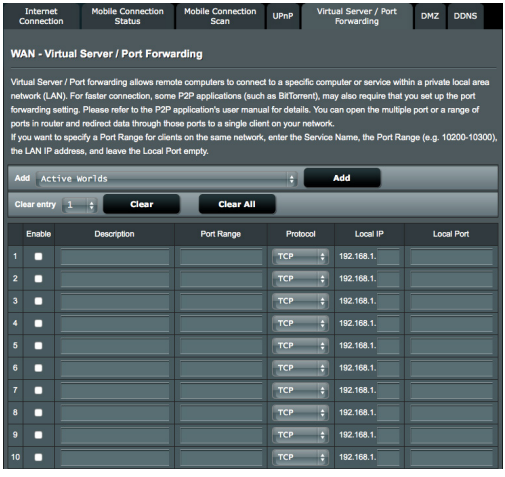
UPnP (Universal Plug and Play) allows several devices (such as routers, televisions, stereo systems, game consoles, and cellular phones), to be controlled via an IP-based network with or without a central control through a gateway. UPnP connects PCs of all form factors, providing a seamless network for remote configuration and data transfer. Using UPnP, a new network device is discovered automatically. Once connected to the network, devices can be remotely configured to support P2P applications, interactive gaming, video conferencing, and web or proxy servers. Unlike Port forwarding, which involves manually configuring port settings, UPnP automatically configures the router to accept incoming connections and direct requests to a specific PC on the local network.



4.3.5 Virtual Server / Port Forwarding

Virtual Server is a method to direct network traffic from the Internet to a specific port or a specific range of ports to a device or number of devices on your local network.

If you configure the LTE Router as a virtual server, remote users accessing services such as web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP addresses. In other words, depending on the requested service (TCP/UDP port number), the LTE Router redirects the external service request to the appropriate server (located at another internal IP address).



For example, if you set Type/Public Port to TCP/80 (Http or web) and the Private IP/Port to 192.168.2.2:80, then all HTTP requests from outside users will be transferred to 192.168.2.2 on port 80. Therefore, by just entering the IP address provided by the ISP, Internet users can access the service they need at the local address to which you redirect them.

NOTE: The more common TCP service ports include: HTTP: 80, FTP: 21, Telnet: 23, and POP3: 110. A list of ports is maintained at http://www.iana.org/assignments/port-numbers.

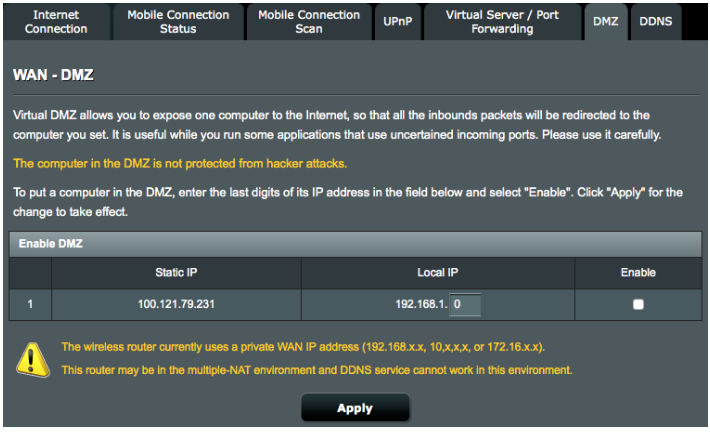
4.3.6 DMZ

Virtual DMZ exposes one client to the Internet, allowing this client to receive all inbound packets directed to your Local Area Network.

Inbound traffic from the Internet is usually discarded and routed to a specific client only if port forwarding or a port trigger has been configured on the network. In a DMZ configuration, one network client receives all inbound packets.

Setting up DMZ on a network is useful when you need incoming ports open or you want to host a domain, web, or e-mail server.

CAUTION: Opening all the ports on a client to the Internet makes the network vulnerable to outside attacks. Please be aware of the security risks involved in using DMZ.



To set up DMZ:

1. From the navigation panel, go to **Advanced Settings** > **WAN** > **DMZ** tab.
2. Configure the setting below. When done, click **Apply**.

- **Enable DMZ:** Key in the last digit of the client's LAN IP address that will provide the DMZ service and be exposed on the Internet. Ensure that the server client has a static IP address. Tick **Enable**.

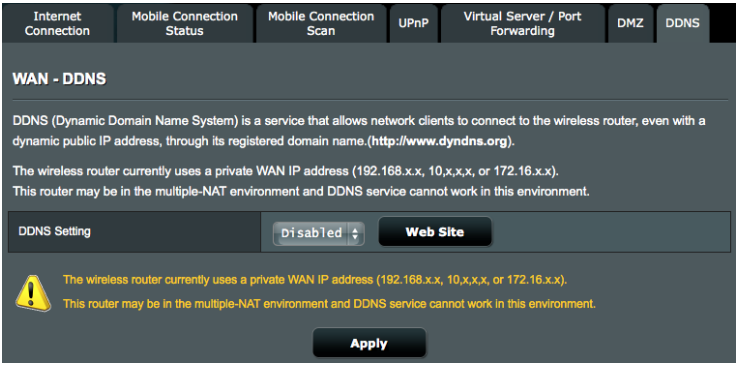
To remove DMZ:

1. Untick **Enable**, and click **Apply**.

4.3.7 DDNS

Setting up DDNS (Dynamic Domain Name System) allows you to access the router outside your network through the provided DDNS service. The DDNS service, which maps a domain name to a static or dynamic IP address, is powered by DynDNS.org.

With a DDNS connection, you can host a website, an email server, an FTP site, and other Internet apps in your local area network even when using dynamic IP addresses for the domain names.



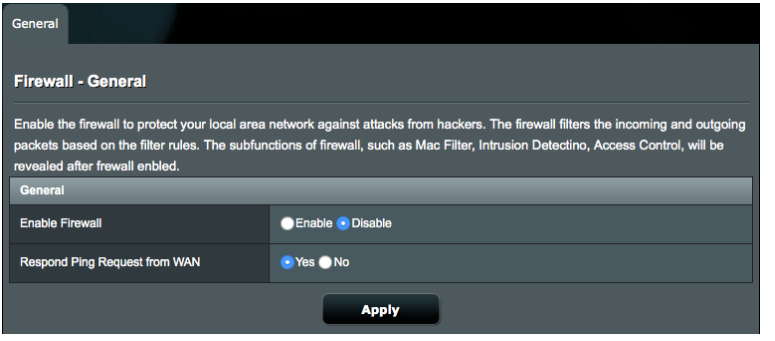
To set up DDNS:

1. Select **DDNS Setting** from the dropdown list and click **Web Site** to go to the DynDNS.org web site.
2. Complete the registration on the DDNS web site.
3. Enter the username, password and domain name of your DDNS settings.
4. Click **Update Dynamic DNS** to update your IP address configuration.
5. When done, click **Apply**.

4.4 Firewall

4.4.1 General

The wireless router can serve as a hardware firewall for your network. Set up the firewall to protect your network from malicious attacks such as Denial of Service (DoS) attacks. DoS attacks disable a device or network to deny users access to network resources.

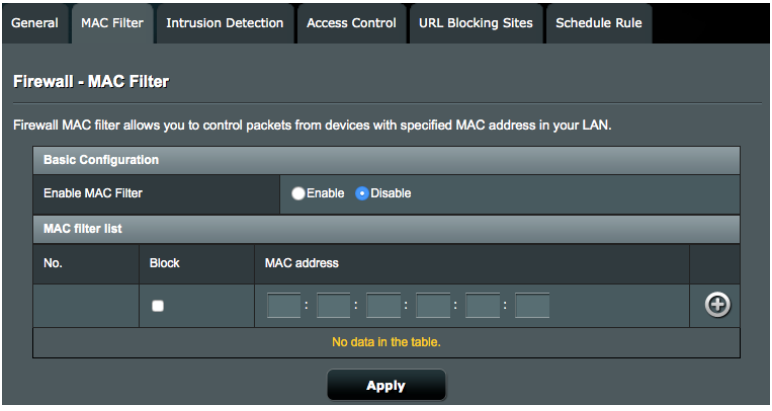


To set up basic Firewall settings:

1. From the navigation panel, go to **Advanced Settings** > **Firewall** > **General** tab.
2. On the **Enable Firewall** field, select **Enable**.
3. On the **Respond Ping Request from WAN** field, select **Yes** to block hackers from pinging devices in your network from the Internet.
4. Click **Apply**.

4.4.2 MAC Filter

When MAC Filter is enabled, only those MAC addresses in the list are allowed or denied access to your network.

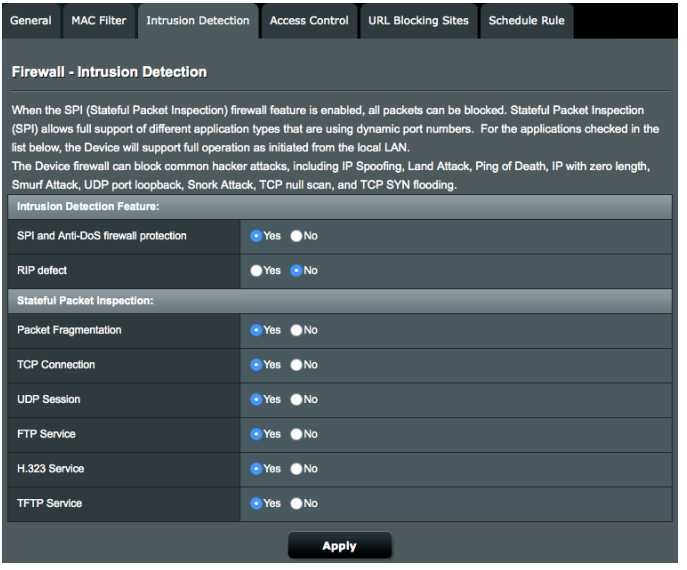


To set up a MAC filter:

1. From the navigation panel, go to **Advanced Settings** > **Firewall** > **MAC Filter** tab.
2. On the **Enable MAC Filter** field, select **Enable**.
3. Enter an MAC address and click the button.
4. Click **Apply**.

4.4.3 Intrusion Detection

Intrusion Detection blocks and prevents malicious attacks or intrusions from harming your network and the devices connected to it. Your wireless router prevents Dos attachs such as IP Spoofing, Ping of Death, IP with Zero Length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN floodng.



Intrusion Detection Feature

SPI and Anti-DoS firewall protection: When this item is enabled, all the incoming packets from the WAN services are blocked except for those types selected in the Stateful Packet Inspection (SPI) section.

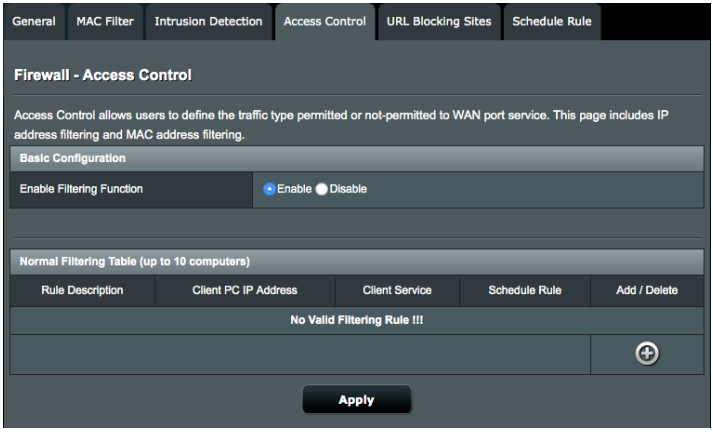
RIP defect: When this item is enabled, the router will not block RIP request packets from the WAN services, preventing the overflow of input queues due to packet accumulation.

Stateful Packet Inspection

Select **Yes** to allow the specific type of traffic to pass through the firewall or **No** to block the type of traffic.

4.4.4 Access Control

Access Control allows you to specify the clients or services that are allowed or blocked to the WAN port service. The access control rules are executed with the specified schedules.



To set up a network service filter:

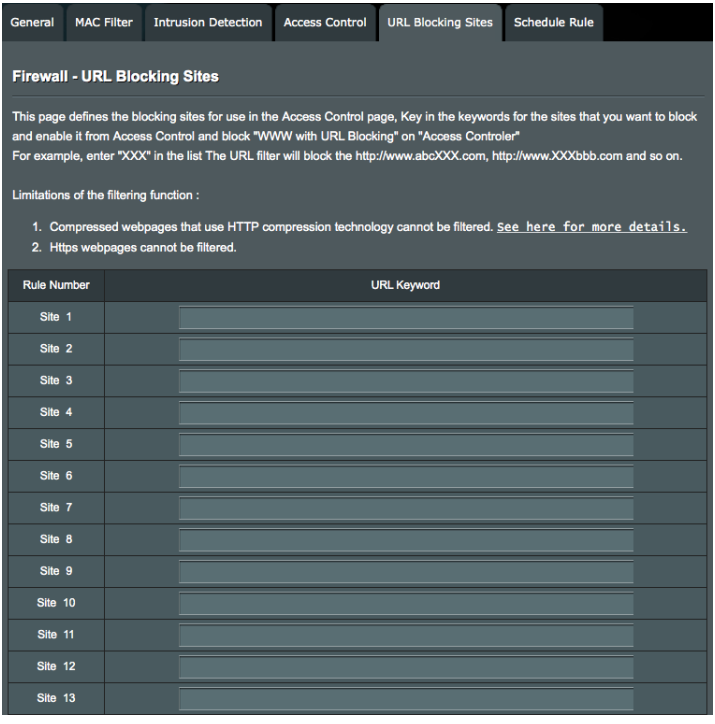
1. From the navigation panel, go to **Advanced Settings** > **Firewall** > **Access Control** tab.
2. On the **Enable Filtering Function** field, select **Enable**.
3. Click the button to launch the Add New Rule screen.

4. Enter a description of the clients.
5. Enter the clients' IP range to block the specified clients.
6. Define a scheduling rule. You can select Always Blocking or specify the day and time when the filters will be active.
7. To specify a network service to filter, select a network service and check **Blocking** on **Client PC Service** to block the pre-defined network service.
8. On the **User-defined services** field, select a protocol type and enter the clients' IP ranges to manually define the clients that will be blocked.
9. Click **Apply**.

4.4.5 URL Filter

You can specify keywords or web addresses to prevent access to specific URLs.

NOTE: The URL Filter is based on a DNS query. If a network client has already accessed a website such as http://www.abcxxx.com, then the website will not be blocked (a DNS cache in the system stores previously visited websites). To resolve this issue, clear the DNS cache before setting up the URL Filter.



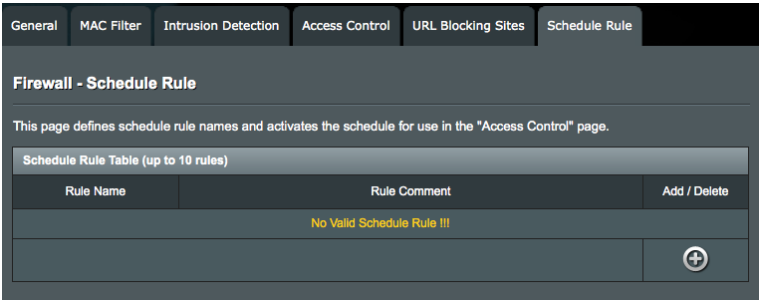
To set up a URL filter:

1. From the navigation panel, go to **Advanced Settings** > **Firewall** > **URL Filter** tab.
2. Enter a URL keyword.
3. Click **Apply**.

4.4.6 Schedule Rule

Each access control rule can be activated at a pre-defined scheduled time.

You can define the schedule rule in the **Schedule Rule** page, and apply the rule in the **Access Control** page.



4.5 Administration

4.5.1 System

The **System** page allows you to configure your wireless router settings.

To set up the System settings:

1. From the navigation panel, go to **Advanced Settings** > **Administration** > **System** tab.
2. You can configure the following settings:
   - **Administrator Password**: You can change the password and login name for the wireless router by entering a new name and password.
     - **Login Timeout**: Most Web administrators set this property to 10 minutes. It should not be set higher than 20 minutes (except in special cases) because every open session is holding onto memory.
   - **Time and Time Zone**: Select the time and time zone for your network.
     - **Time Zone**: Adjust time zone according to the location of the router.
     - **Daylight Saving Time (DST)**: If your region adopts daylight saving time (DST), enable this option.
     - **NTP Server**: The wireless router can access a NTP (Network time Protocol) server in order to synchronize the time.
   - **Web Access from WAN:**
     - **Enable Web Access from**: Select **Enable** to allow devices outside the network to access the wireless router GUI settings. Select **Disable** to prevent access.
     - **Permitted IP Address**:
       - **Any IP address can remotely manage the wireless router.**
       - **Only allow specific IP**: Enter the WAN IP addresses of networking devices allowed to access the wireless router settings from WAN.

- **Port of Web Access from WAN**: Specify the port number of the web server allowed to access the wireless router settings.

3. Click **Apply**.

4.5.2 Firmware Upgrade

NOTE: Download the latest firmware from the ASUS website at **http://www.asus.com**

To upgrade the firmware:

1. From the navigation panel, go to **Advanced Settings** > **Administration** > **Firmware Upgrade** tab.
2. In the **New Firmware File** field, click **Browse** to locate the downloaded file.
3. Click **Upload**.

NOTE: When the upgrade process is complete, wait for some time for the system to reboot.

4.5.3 Restore/Save/Upload Setting

To restore/save/upload wireless router settings:

1. From the navigation panel, go to **Advanced Settings** > **Administration** > **Restore/Save/Upload Setting** tab.
2. Select the tasks that you want to do:
   - To restore to the default factory settings, click **Restore**, and click **OK** in the confirmation message.
   - To save the current system settings, click **Save**, navigate to the folder where you intend to save the file and click **Save**.
   - To restore from a saved system settings file, click **Browse** to locate your file, then click **Upload**.

If issues occur, upload the latest firmware version and configure new settings. Do not restore the router to its default settings.

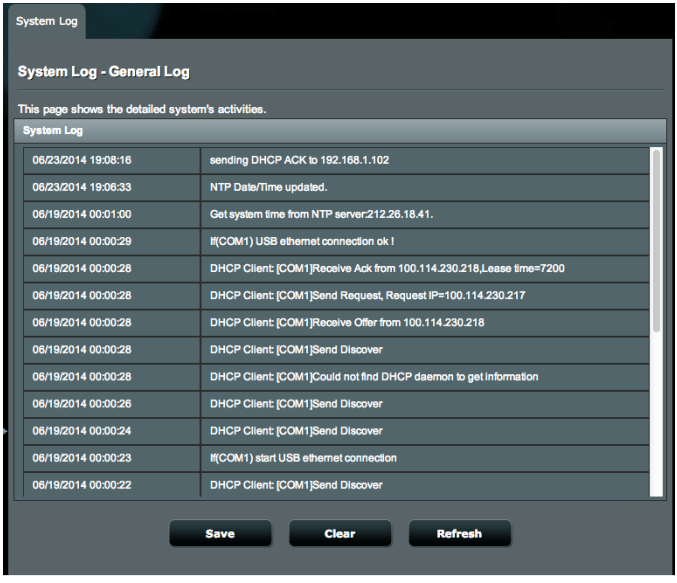
4.6 System Log

System Log contains your recorded network activities.

NOTE: System log resets when the router is rebooted or powered off.

To view your system log:

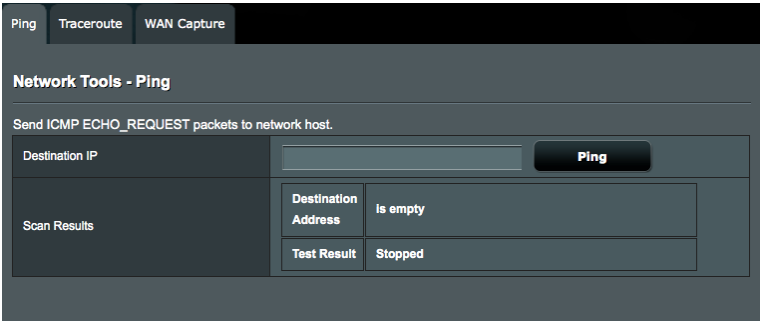
1. From the navigation panel, go to **Advanced Settings** > **System Log**.
2. You can view your network activities in this page:
3. (Optional) Click **Save** to export the system logs.



4.7 Network Tools

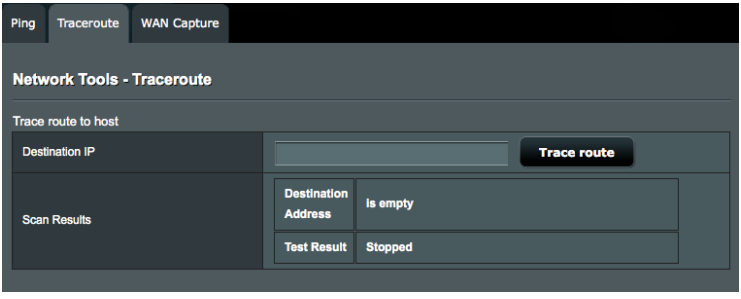
4.7.1 Ping

A ping test determines the latency (communication delay) between ASUS router and another server (such as www.google.com) on a network by sending multiple ICMP packets and listening for the replies. Enter a host name or IP address to perform a Ping. The test results display the shortest, the average and the maximum round-trip times and packet loss rate between hosts.



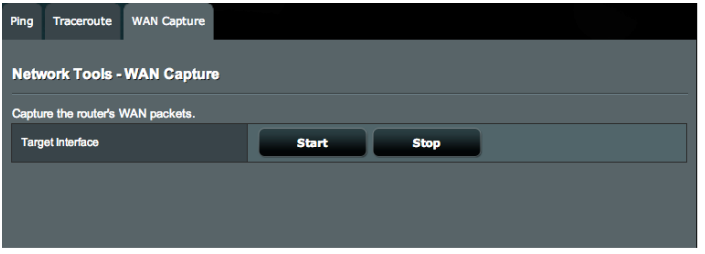
4.7.2 Traceroute

The Traceroute test (also known as trace route or tracert) will trace the route that test packets take from one server destination to another. The test results provide a list of hosts or IP addresses showing the route taken by the test packets starting from the selected monitoring location to the destination Domain or IP (such as www.google.com) . Common uses of the Traceroute test are network troubleshooting and to help identify routing problems or firewalls that may be blocking access to a web site.



4.7.3 WAN Capture

The WAN Capture allows you to capture all packets that pass through the Mobile Broadband Network.



To capture your router's WAN packets:

1. To start capturing the packets, click **Start**. The browser starts to download the pktDump.cap file to your computer.
2. To stop capturing the packets, click **Stop**. The browser terminates capturing the packets and completes downloading the pktDump.cap file.

NOTE: An external application like Wireshark is required to view the captured packets in the file.

5 Frequently Asked Questions (FAQs)

Cannot access the router GUI using a web browser.

- **Hardware Configuration:**
  - If your computer is wired, check the Ethernet cable connection and LED status.
- **Failed to log in:**
  - Ensure that you are using the correct login information. The default factory login name and password is "admin/admin". Ensure that the Caps Lock key is disabled when you enter the login information.
- **DNS Cache result to wrong DNS:**
  - Delete the cookies and files in your web browser.
- **Previous connection settings:**
  - Disable the proxy server, if enabled.
  - Set the TCP/IP settings to automatically obtain an IP address.
  - Disable the dial-up connection from browser, if enabled.

NOTES:

- The commands for deleting cookies and files vary with web browsers.
- Disable proxy server settings, cancel the dial-up connection, and set the TCP/IP settings to obtain IP addresses automatically. For more details, refer to Chapter 1 of this user manual.

The client cannot establish a wireless connection with the router.

- **Out of Range:**
  - Move the router closer to the wireless client.
  - Try to adjust antennas of the router to the best direction as described in section 1.4 Positioning your router.

- **DHCP server has been disabled:**
  - Launch the web GUI. Go to **General** > **Network Map** > **Clients** and search for the device that you want to connect to the router.
  - If you cannot find the device in the Network Map, go to **Advanced Settings** > **LAN**, select **Yes** on the Enable the DHCP Server.

- **Cannot find the SSID:**
  - If you are using a wireless LAN adapter, check if the wireless channel in use conforms to the channels available in your country/area. You can adjust the channel, channel bandwidth, and wireless mode available in your country/area.
- If you still cannot connect to the router wirelessly, you can reset your router to factory default settings. In the router GUI, click **Administration** > **Restore/Save/Upload Setting** and click **Restore**.

Internet is not accessible.

- Check if your router can connect to your ISP's WAN IP address. To do this, launch the web GUI and go to **General**> **Network Map**, and check the **Internet Status**.
- If there is still no Internet access, try to reboot your computer and verify the network's IP address and gateway address.

- Check the status indicators on the wireless router. If the Internet LED on the wireless router is not ON, check if all cables are plugged properly.

Forgot the SSID (network name) or network password:

- Set up a new SSID and encryption key via a wired connection (Ethernet cable). Launch the web GUI, go to **Network Map**, click the router icon, enter a new SSID and encryption key, and click **Apply**.
- Reset your router to the default settings. Launch the web GUI, go to **Administration** > **Restore/Save/Upload Setting**, and click **Restore**. The default login account and password are both "admin".

How to restore the system to its default settings?

- Go to **Administration** > **Restore/Save/Upload Setting**, and click **Restore**.

  The following are the factory default settings:

User Name:	admin
Password:	admin
Enable DHCP:	Yes
IP address:	192.168.1.1
Domain Name:	(Blank)
Subnet Mask:	255.255.255.0
DNS Server 1:	192.168.1.1
DNS Server 2:	(Blank)
SSID (2.4GHz):	ASUS

Appendices

Notices

ASUS Recycling/Takeback Services

ASUS recycling and takeback programs come from our commitment to the highest standards for protecting our environment. We believe in providing solutions for you to be able to responsibly recycle our products, batteries, other components, as well as the packaging materials. Please go to http://csr.asus.com/english/Takeback.htm for the detailed recycling information in different regions.

REACH

Complying with the REACH (Registration, Evaluation, Authorisation, and Restriction of Chemicals) regulatory framework, we published the chemical substances in our products at ASUS REACH website at

http://csr.asus.com/english/index.aspx

Declaration of Conformity for R&TTE directive 1999/5/EC

Essential requirements – Article 3

Protection requirements for health and safety – Article 3.1a

Testing for electric safety according to EN 60950-1 has been conducted. These are considered relevant and sufficient.

Protection requirements for electromagnetic compatibility – Article 3.1b

Testing for electromagnetic compatibility according to EN 301 489-1 and EN 301 489-17 has been conducted. These are considered relevant and sufficient.

Effective use of the radio spectrum – Article 3.2

Testing for radio test suites according to EN 300 328 & EN 301 893 have been conducted. These are considered relevant and sufficient.

CE Mark Warning

This is a Class B product, in a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

This equipment may be operated in AT, BE, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IE, IT, LU, MT, NL, PL, PT, SK, SL, ES, SE, GB, IS, LI, NO, CH, BG, RO, RT.

Canada, Industry Canada (IC) Notices

This Class B digital apparatus complies with Canadian ICES-003 and RSS-210.

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Radio Frequency (RF) Exposure Information

The radiated output power of the ASUS Wireless Device is below the Industry Canada (IC) radio frequency exposure limits. The ASUS Wireless Device should be used in such a manner such that the potential for human contact during normal operation is minimized.

This device has been evaluated for and shown compliant with the IC Specific Absorption Rate ("SAR") limits when installed in specific host products operated in portable exposure conditions (antennas are less than 20 centimeters of a person's body).

This device has been certified for use in Canada. Status of the listing in the Industry Canada's REL (Radio Equipment List) can be found at the following web address: http://www.ic.gc.ca/app/sitt/reltel/srch/nwRdSrch.do?lang=eng

Additional Canadian information on RF exposure also can be found at the following web: http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf08792.html

Canada, avis d'Industry Canada (IC)

Cet appareil numérique de classe B est conforme aux normes canadiennes ICES-003 et RSS-210.

Son fonctionnement est soumis aux deux conditions suivantes: (1) cet appareil ne doit pas causer d'interférence et (2) cet appareil doit accepter toute interférence, notamment les interférences qui peuvent a ecter son fonctionnement.

NCC 警語

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

GNU General Public License

Licensing information

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License. Please see The GNU General Public License for the exact terms and conditions of this license. We include a copy of the GPL with every CD shipped with our product. All future firmware updates will also be accompanied with their respective source code. Please visit our web site for updated information. Note that we do not offer direct support for the distribution.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

Terms & conditions for copying, distribution, & modification

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act

of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute

the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your

cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License.

Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance

on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission.

    For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11 BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12 IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

For Turkey only

Authorised distributors in Turkey:

BOGAZICI BIL GISAYAR SAN. VE TIC. A.S.

Tel. No.: +90 212 3311000

Address: AYAZAGA MAH. KEMERBURGAZ CAD. NO.10 AYAZAGA/ISTANBUL

CIZGI Elektronik San. Tic. Ltd. Sti.

Tel. No.: +90 212 3567070

Address: CEMAL SURURI CD. HALIM MERIC IS MERKEZI No: 15/C D:5-6 34394 MECIDIYEKOY/ ISTANBUL

KOYUNCU ELEKTRONiK BiLGi iSLEM SiST. SAN. VE DIS TIC. A.S.

Tel. No.: +90 216 5288888

Address: EMEK MAH.ORDU CAD. NO:18, SARIGAZi, SANCAKTEPE ISTANBUL

AEEE Yönetmeliğine Uygundur.

ASUS Contact information

ASUSTeK COMPUTER INC. (Asia Pacific)

Address	15 Li-Te Road, Peitou, Taipei, Taiwan 11259
Website	www.asus.com.tw

Technical Support

Telephone	+886228943447
Support Fax	+886228907698
Online support	support.asus.com

ASUS COMPUTER INTERNATIONAL (America)

Address	800 Corporate Way, Fremont, CA 94539, USA
Telephone	+15107393777
Fax	+15106084555
Website	usa.asus.com
Online support	support.asus.com

ASUS COMPUTER GmbH (Germany and Austria)

Address	Harkort Str. 21-23, D-40880 Ratingen, Germany
Support Fax	+49-2102-959931
Website	asus.com/de
Online contact	eu-rma.asus.com/sales

Technical Support

Telephone (Component)	+49-2102-5789555
Telephone Germany (System/Notebook/Eee/LCD)	+49-2102-5789557
Telephone Austria (System/Notebook/Eee/LCD)	+43-820-240513
Support Fax	+49-2102-959911
Online support	support.asus.com

Networks Global Hotline Information

Region	Country	Hotline Number	Service Hours
Europe	Cyprus	800-92491	09:00-13:00 ; 14:00-18:00 Mon-Fri
	France	0033-170949400	09:00-18:00 Mon-Fri
	Germany	0049-1805010920 0049-1805010923 (component support) 0049-2102959911 (Fax)	09:00-18:00 Mon-Fri 10:00-17:00 Mon-Fri
	Hungary	0036-15054561	09:00-17:30 Mon-Fri
	Italy	199-400089	09:00-13:00 ; 14:00-18:00 Mon-Fri
	Greece	00800-44142044	09:00-13:00 ; 14:00-18:00 Mon-Fri
	Austria	0043-820240513	09:00-18:00 Mon-Fri
	Netherlands/ Luxembourg	0031-591570290	09:00-17:00 Mon-Fri
	Belgium	0032-78150231	09:00-17:00 Mon-Fri
	Norway	0047-2316-2682	09:00-18:00 Mon-Fri
	Sweden	0046-858769407	09:00-18:00 Mon-Fri
	Finland	00358-969379690	10:00-19:00 Mon-Fri
	Denmark	0045-38322943	09:00-18:00 Mon-Fri
	Poland	0048-225718040	08:30-17:30 Mon-Fri
	Spain	0034-902889688	09:00-18:00 Mon-Fri
	Portugal	00351-707500310	09:00-18:00 Mon-Fri
	Slovak Republic	00421-232162621	08:00-17:00 Mon-Fri
	Czech Republic	00420-596766888	08:00-17:00 Mon-Fri
	Switzerland-German	0041-848111010	09:00-18:00 Mon-Fri
	Switzerland-French	0041-848111014	09:00-18:00 Mon-Fri
	Switzerland-Italian	0041-848111012	09:00-18:00 Mon-Fri
	United Kingdom	0044-8448008340	09:00-17:00 Mon-Fri
	Ireland	0035-31890719918	09:00-17:00 Mon-Fri
	Russia and CIS	008-800-100-ASUS	09:00-18:00 Mon-Fri
	Ukraine	0038-0445457727	09:00-18:00 Mon-Fri

Networks Global Hotline Information

Region	Country	Hotline Numbers	Service Hours
Asia-Pacific	Australia	1300-278788	09:00-18:00 Mon-Fri
	New Zealand	0800-278788	09:00-18:00 Mon-Fri
	Japan	0800-1232787	09:00-18:00 Mon-Fri 09:00-17:00 Sat-Sun
		0081-473905630 (Non-Toll Free)	09:00-18:00 Mon-Fri 09:00-17:00 Sat-Sun
	Korea	0082-215666868	09:30-17:00 Mon-Fri
	Thailand	0066-24011717 1800-8525201	09:00-18:00 Mon-Fri
	Singapore	0065-64157917 0065-67203835 (Repair Status Only)	11:00-19:00 Mon-Fri 11:00-19:00 Mon-Fri 11:00-13:00 Sat
	Malaysia	0060-320535077	10:00-19:00 Mon-Fri
	Philippine	1800-18550163	09:00-18:00 Mon-Fri
	India India(WL/NW)	1800-2090365	09:00-18:00 Mon-Sat 09:00-21:00 Mon-Sun
	Indonesia	0062-2129495000 500128 (Local Only)	09:30-17:00 Mon-Fri 9:30 – 12:00 Sat
	Vietnam	1900-555581	08:00-12:00 13:30-17:30 Mon-Sat
	Hong Kong	00852-35824770	10:00-19:00 Mon-Sat
Americas	USA Canada	1-812-282-2787	8:30-12:00 EST Mon-Fri 9:00-18:00 EST Sat-Sun
	Mexico	001-8008367847	08:00-20:00 CST Mon-Fri 08:00-15:00 CST Sat

Networks Global Hotline Information

Region	Country	Hotline Numbers	Service Hours
Middle East + Africa	Egypt	800-2787349	09:00-18:00 Sun-Thu
	Saudi Arabia	800-1212787	09:00-18:00 Sat-Wed
	UAE	00971-42958941	09:00-18:00 Sun-Thu
	Turkey	0090-2165243000	09:00-18:00 Mon-Fri
	South Africa	0861-278772	08:00-17:00 Mon-Fri
	Israel	*6557/00972-39142800	08:00-17:00 Sun-Thu
		*9770/00972-35598555	08:30-17:30 Sun-Thu
Balkan Countries	Romania	0040-213301786	09:00-18:30 Mon-Fri
	Bosnia Herzegovina	00387-33773163	09:00-17:00 Mon-Fri
	Bulgaria	00359-70014411	09:30-18:30 Mon-Fri
		00359-29889170	09:30-18:00 Mon-Fri
	Croatia	00385-16401111	09:00-17:00 Mon-Fri
	Montenegro	00382-20608251	09:00-17:00 Mon-Fri
	Serbia	00381-112070677	09:00-17:00 Mon-Fri
	Slovenia	00368-59045400	08:00-16:00 Mon-Fri
		00368-59045401	
	Estonia	00372-6671796	09:00-18:00 Mon-Fri
	Latvia	00371-67408838	09:00-18:00 Mon-Fri
	Lithuania-Kaunas	00370-37329000	09:00-18:00 Mon-Fri
	Lithuania-Vilnius	00370-522101160	09:00-18:00 Mon-Fri

NOTE: For more information, visit the ASUS support site at:
http://support.asus.com

Manufacturer:	**ASUSTeK Computer Inc.**	
	Tel:	+886-2-2894-3447
	Address:	4F, No. 150, LI-TE RD., PEITOU, TAIPEI 112, TAIWAN
Authorised representative in Europe:	**ASUS Computer GmbH**	
	Address:	HARKORT STR. 21-23, 40880 RATINGEN, GERMANY

McGrp.Ru

Сайт техники и электроники

Наш сайт McGrp.Ru при этом не является просто хранилищем инструкций по эксплуатации, это живое сообщество людей. Они общаются на форуме, задают вопросы о способах и особенностях использования техники. На все вопросы очень быстро находятся ответы от таких же посетителей сайта, экспертов или администраторов. Вопрос можно задать как на форуме, так и в специальной форме на странице, где описывается интересующая вас техника.