User Guide

RT-N14UHP

Wireless-N High Power Router

IN SEARCH OF INCREDIBLE

E8824
First Edition
November 2013

Table of contents

Table of contents

Table of contents

1 Overview

Package contents

- ☑ RT-N14UHP wireless router
- ☑ Network cable (RJ-45)
- ☑ Power adapter
- ☑ Quick Start Guide
- ☑ Warranty card

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

Hardware features

Front

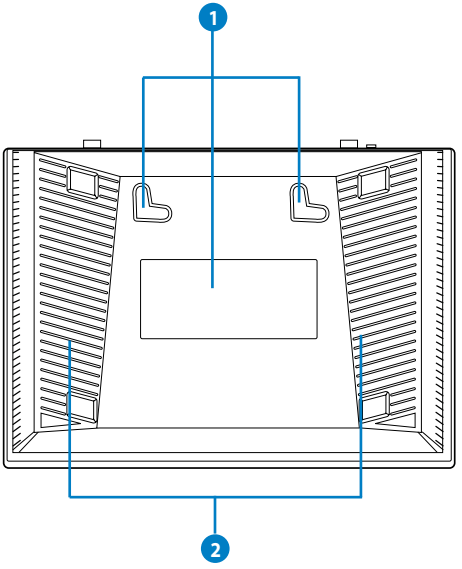
Status indicators

LED	Status	Indication
Power	Off	No power or wireless signal is disabled
	On	System ready
	Flashing slowly	Rescue mode
	Flashing quickly	WPS in progress
Wireless	Off	No power
	On	Wireless system ready
	Flashing	Transmitting or receiving data (wireless)
WAN Wide Area Network	Off	No power or no physical connection
	On	Has physical connection to an Ethernet network
	Flashing	Transmitting or receiving data (through Ethernet cable)
LAN 1-4 Local Area Network	Off	No power or no physical connection
	On	Has physical connection to an Ethernet network
	Flashing	Transmitting or receiving data (through Ethernet cable)

Rear

Label	Description
Reset	Press this button for more than five seconds to restore the system to its factory default settings.
Power	Press this button to power on/off the wireless router.
DCIN	Insert the AC adapter into this port to connect your router to a power source.
USB 2.0	USB 2.0 ports Insert USB 2.0 devices such as USB hard disks or USB flash drives into these ports. Insert your iPad's USB cable into one of these ports to charge your iPad.
WPS	Press this button for more than four seconds to establish a secure wireless connection with a WPS-supported wireless device.
WAN	Connect an RJ-45 Ethernet cable to this port to establish WAN connection.
LAN1-LAN4	Connect RJ-45 Ethernet cables to these ports to establish LAN connection.

Bottom panel



Item	Description
1	**Mounting hooks** Use the mounting hooks to mount your router on concrete or wooden surfaces using two round head screws.
2	**Air vents** These vents provide ventilation to your router.

Mounting the wireless router to a wall is not recommended as it reduces wireless performance.

2 Setting up your wireless network

Positioning your router

To get the best wireless network performance from your wireless router, follow the recommendations below:

- Place the wireless router at the center of your network for maximum wireless coverage.
- Keep the device away from metal obstructions and away from direct sunlight.
- 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.
- For the best front-to-rear wireless coverage, place the wireless router in an upright position.
- For the best upward and downward wireless coverage, place the wireless router in an inclined position.
- Always update to the latest firmware. Visit the ASUS website at http://support.asus.com to get the latest firmware updates.

What you need

To set up your network, you need one or two computers that meet the following system requirements:

- Ethernet RJ-45 (LAN) port (10Base-T/100Base-TX)
- IEEE 802.11b/g/n wireless capability
- An installed TCP/IP service
- Web browser such as Microsoft Internet Explorer, Mozilla Firefox, Apple Safari, or Google Chrome

- If your computer does not have built-in wireless capabilities, install an IEEE 802.11b/g/n WLAN adapter to your computer to connect to the network.
- The Ethernet RJ-45 cables used to connect the network devices should not exceed 100 meters.

Setting up your wireless router

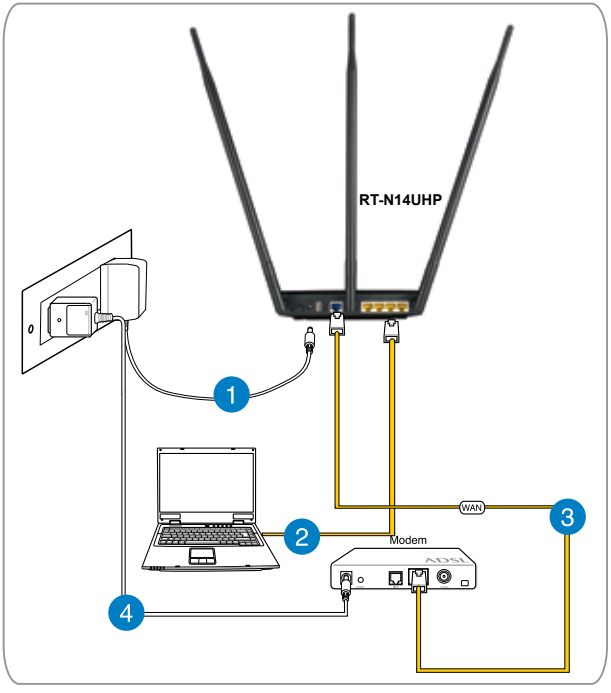
- Use a wired connection when setting up your wireless router to avoid possible wireless setup issues.
- Before setting up your ASUS wireless router, do the following:
  - If you are replacing an existing router, disconnect it from your network.
  - Disconnect the cables/wires from your existing modem. If your modem has a backup battery, remove it as well.
  - Reboot your computer (recommended).

Wired connection

Your wireless router supports both a straight-through or crossover cable when setting up a wired connection.

To set up a network using a wired connection:

1. Insert your wireless router's AC adapter to the DC-In port and plug it to a power outlet.
2. Using the bundled network cable, connect your computer to your wireless router's LAN port.



Ensure that the LAN LED is blinking.

3 Using another network cable, connect your modem to your wireless router's WAN port.

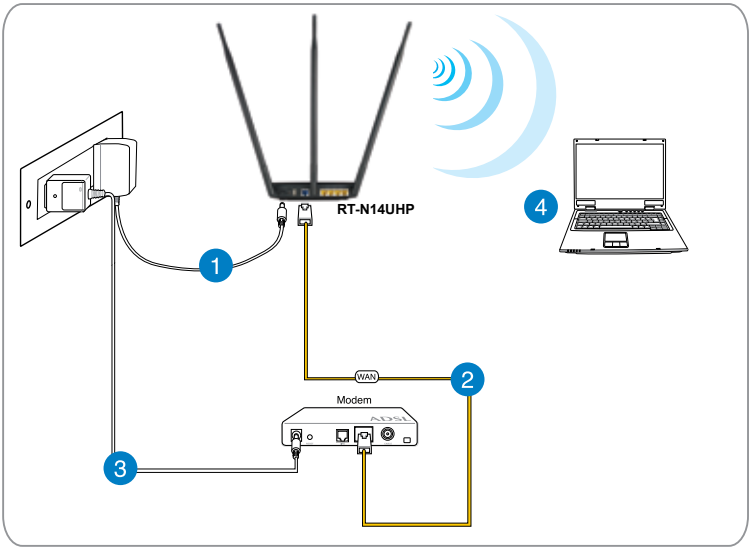
4. Insert your modem's AC adapter to the DC-In port and plug it to a power outlet.

Wireless connection

To set up your wireless network:

1. Insert your wireless router's AC adapter to the DC-In port and plug it to a power outlet.
2 Using the bundled network cable, connect your modem to your wireless router's WAN port.
3. Insert your modem's AC adapter to the DC-In port and plug it to a power outlet.
4. Install an IEEE 802.11b/g/n WLAN adapter on your computer.

- For details on connecting to a wireless network, refer to the WLAN adapter's user manual.
- To set up the security settings for your network, refer to the section **Setting up wireless security.**



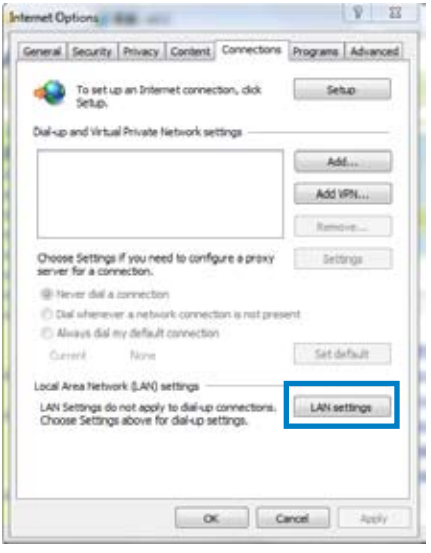
Before you proceed

Before configuring your wireless router, apply the steps described in this section to each computer on the network to avoid problems connecting to the wireless network.

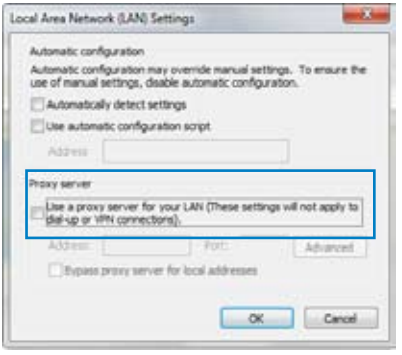
A. Disable any configured proxy servers.

Windows® 7

1. Click **Start > Internet Explorer**.
2. Click **Tools > Internet options > Connections tab > LAN settings.**



3. From the Local Area Network (LAN) Settings window, uncheck **Use a proxy server for your LAN**.
4. Click **OK** then **Apply**.



MAC OSX

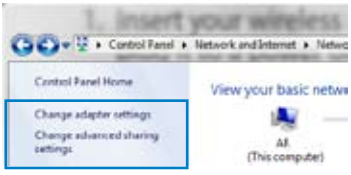
1. From your **Apple Safari** browser, click **Safari** > **Preferences** > **Advanced**. On the **Proxies** item, click **Change Settings**...

2. From the **Network** screen, uncheck **FTP Proxy** and **Web Proxy (HTTP)**.
3. Click **OK** then **Apply**.

B. Configure TCP/IP settings to automatically obtain an IP address.

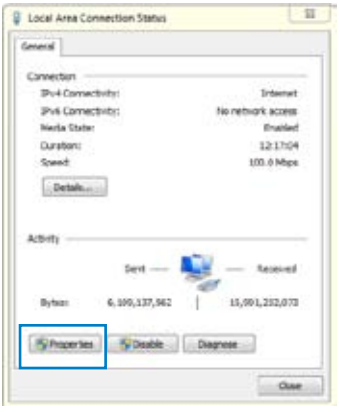
Windows® 7

1. Click **Start > Control Panel > Network and Internet > Network and Sharing Center > Change adapter settings**.

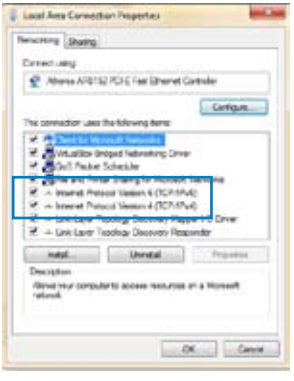


2. On the Network Connections window, click on **Local Area Connection**.

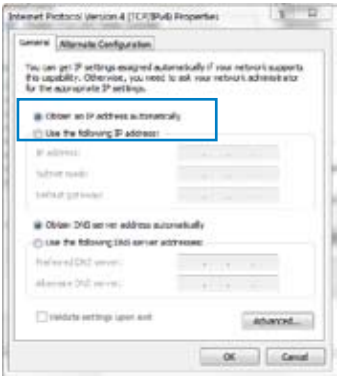
3. On the Local Area Connection Network Status window, click **Properties**.



4. Select Internet Protocol Version 4 (TCP/IPv4) or Internet Protocol Version 6 (TCP/IPv6), then click **Properties**.



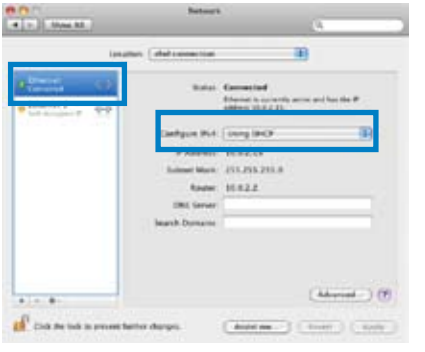
6. Tick **Obtain an IP address automatically.**
7. Click **OK**.



MAC OSX

1. Click **Apple Menu >System Preferences > Network**

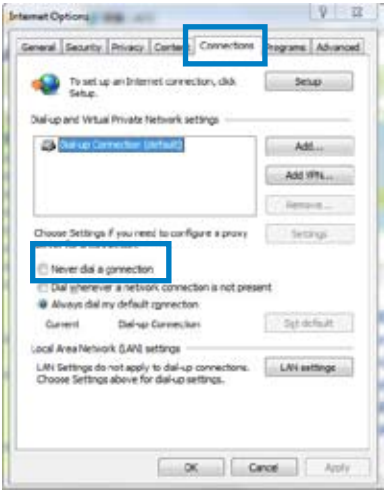
2. Click **Ethernet** on the left panel.
3. On the Configure IPv4, item select **Using DHCP**.
4. Cllick **Apply**.



C. Disable dial-up networking

Windows® 7

1. Click **Start > Internet Explorer**.
2. Click **Tools > Internet Options > Connections** tab.
3. Tick **Never dial a connection**.
4. Click **Apply** then **OK**.



3 Network configuration using the web GUI

Logging in to the web GUI

Your ASUS Wireless Router uses a web-based user interface that allows you to configure the router using any web browser such as Internet Explorer, Mozilla Firefox, Apple Safari, or Google Chrome.

To log in to the web GUI:

1. Launch your web browser and manually key in the wireless router's default IP address: **192.168.1.1** or default domain name: **http://router.asus.com**.
2. On the login page, key in the default user name (**admin**) and password (**admin**).

3. The wireless router GUI provides access to various configuration settings.

Setting up the Internet connection

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

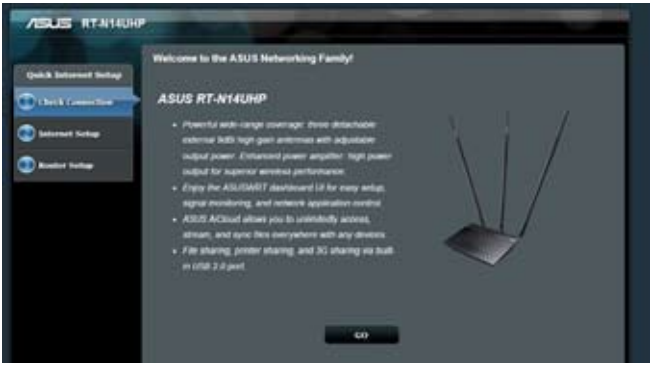
Quick Internet Setup (QIS) with auto-detection

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

To use QIS with auto-detection:

1. Launch a web browser such as Internet Explorer, Mozilla Firefox, Apple Safari, or Google Chrome.

2. Quick Internet Setup will launch automatically. Click **Next**.

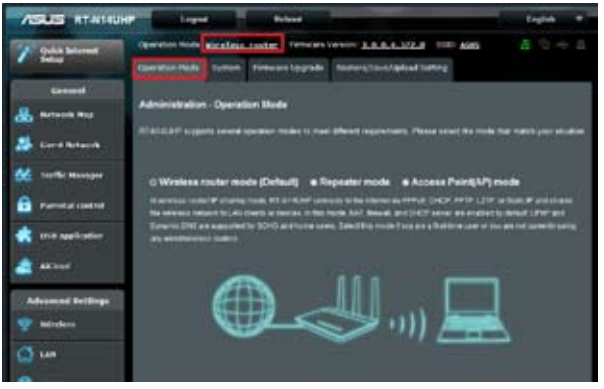


- If QIS failed to launch automatically, manually launch your wireless router's web GUI to access the QIS page. To do this, follow these steps:
  1. On your web browser, key in **http://192.168.1.1** or **http://router.asus.com**.
  2. On the login page, key in the default username **admin** and password **admin**.
  3. Click **Quick Internet Setup** on the navigation panel.

3. Key in a new administrator password to prevent unauthorized access to the router. Click **Next.**

4. Select Wireless router mode, Repeater mode, or Access Point (AP) mode. Click **Next.**

To set up a wireless network with Internet access, use **Wireless router mode.**



5. The wireless router will attempt to identify your connection type. If needed, select the necessary connection type and key in any necessary information required, such as your ISP user name and password.

Obtain the necessary information about your Internet connection type and additional login information from your Internet Service Provider.

- Auto-detection of your ISP connection type takes place when you configure the wireless router for the first time or when your wireless router is reset to its default settings.
- If QIS failed to detect your Internet connection type, click **Skip to manual setting** and manually configure your connection settings.

6. In the Wireless setting screen, key in a **network name (SSID)** and assign a security key for your wireless connection. Click **Apply**.

7. A summary of your network settings will be displayed. Click **Next** to continue.

Setting up wireless security

To protect your wireless network from unauthorized access, you need to configure your router's security settings.

To set up the wireless security settings:

1. Key in **192.168.1.1** or **http://router.asus.com** on your web browser.
2. On the login screen, key in the default user name (**admin**) and password (**admin**), then click **OK**. The wireless router's web GUI launches.
3. On the Network Map screen, the **System Status** area displays the SSID (Service Set Identifier), Authentication Method, and security key settings of your wireless network.

4. On the **Wireless name (SSID)** field, key in a unique name for your wireless network.
5. From the **Authentication Method** dropdown list, select the encryption method for your wireless network.

The IEEE 802.11n standard prohibits using High Throughput with WEP or WPA-TKIP as the unicast cipher. If you use these encryption methods, your data rate will drop to IEEE 802.11g 54Mbps connection.

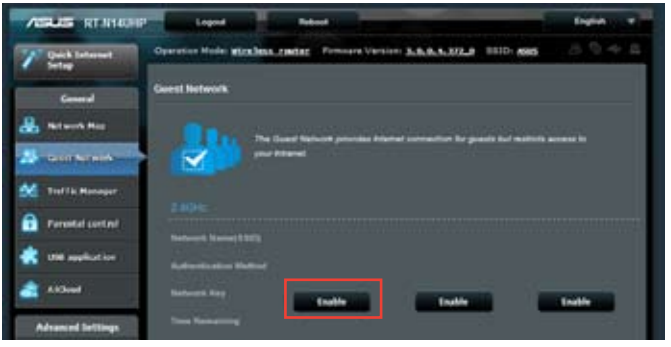
6. Key in your security passkey.
7. Click **Apply**.

Creating your Guest Network

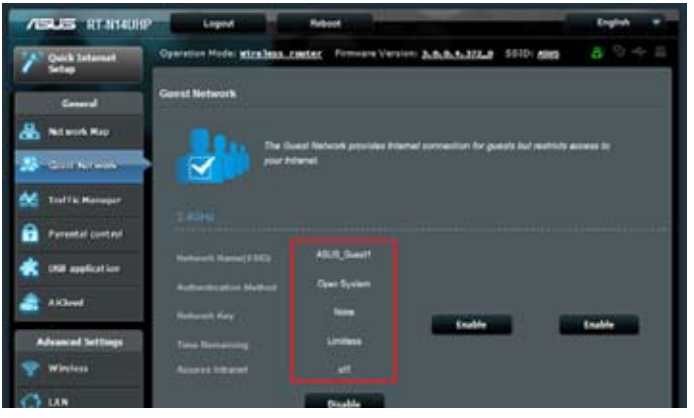
Setting up a Guest Network provides wireless Internet connectivity for temporary visitors while restricting access to your private network.

To create your guest network:

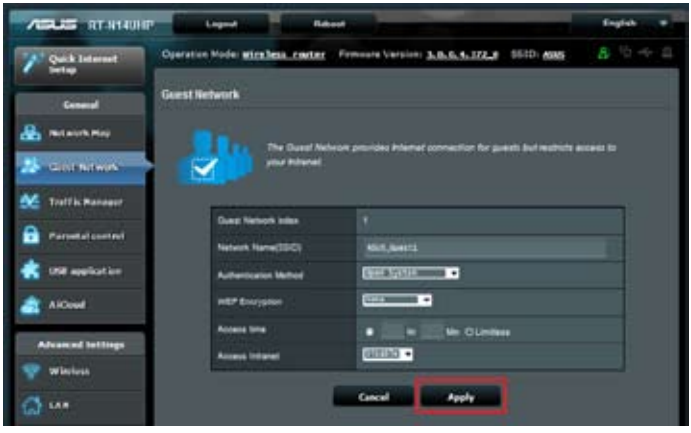
1. Click **Guest Network** on the navigation panel.
2. Click **Enable**.



3. To configure additional options, click any of the items listed.



4. Assign a wireless name for your temporary network on the **Network Name (SSID)** field.
5. Select an **Authentication Method**.
6. Select a **WEP Encryption** method.
7. Specify the **Access time** or click **Limitless**.
8. Select Disable or Enable on the **Access Intranet** item.
9. Click **Apply**.



Using the Traffic Manager

Managing QoS (Quality of Service) Bandwidth

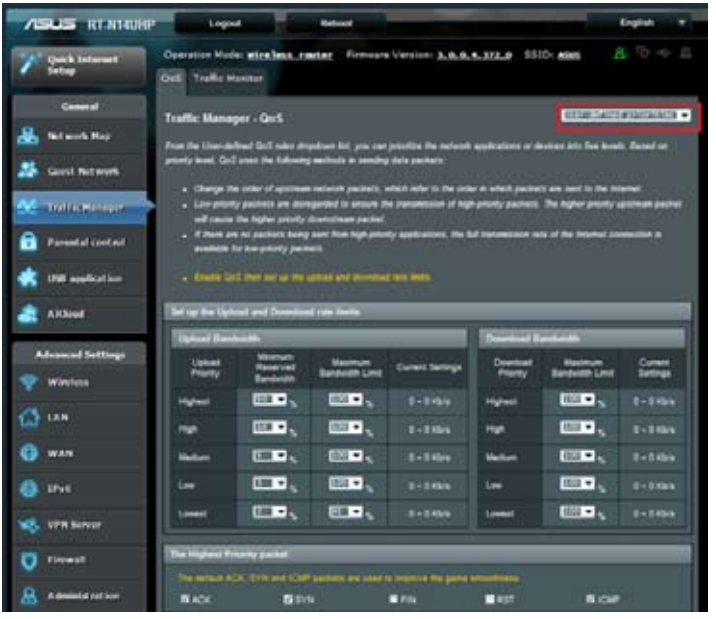
The **Quality of Service** feature allows you to set the bandwidth priority and manage network traffic.

To set up QoS:

1. Click **Traffic Manager** on the navigation panel and click the **QoS** tab.
2. Click **ON** to enable QoS.
3. Click **Save**.

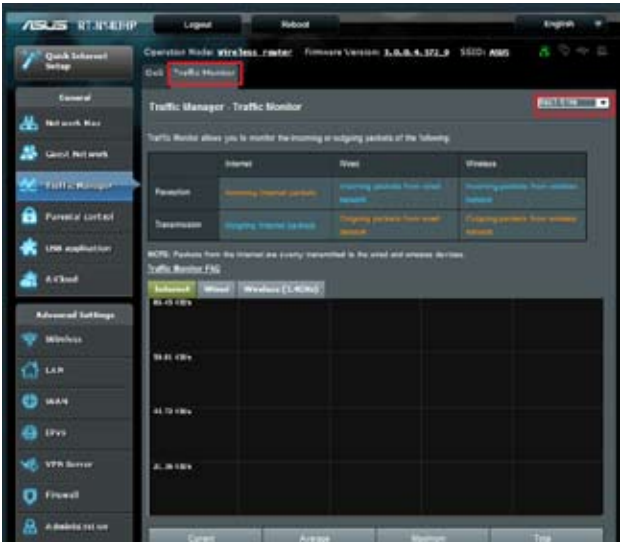
Your bandwidth information is available from your ISP.

3. If you want to prioritize specific network applications and network services, click **User-defined Priority** on the upper-right hand corner.
4. Adjust the values as needed. Click **Apply**.



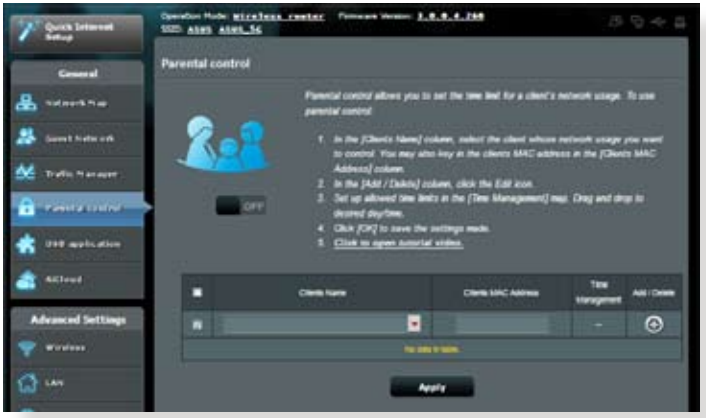
Monitoring Traffic

Click the **Traffic Monitor** tab to view real-time or historical bandwidth information of your Internet, Wired, and Wireless connections.



Setting up Parental Control

Parental Control allows you to control the Internet access time. Users can set the time limit for a client's network usage.



To use the parental control function:

1. From the navigation panel, go to **General** > **Parental control**.
2. Click **ON** to enable Parental Control.
3. Select the client whose network usage you want to control. You may also key in the client's MAC address in the **Client MAC Address** column.

Ensure that the client name does not contain special characters or spaces as this may cause the router to function abnormally.

4. Click ⊕ or ⊖ to add or delete the client's profile.
5. Set up the allowed time limit in **Time Management** map. Drag and drop a desired time zone to allow client's network usage.
6. Click **OK**.
7. Click **Apply** to save the settings.

Using the USB Application

The USB Applications function provides AiDisk, Servers Center, Network Printer Server and Download Master submenus.

To use the server functions, you need to insert a USB storage device, such as a USB hard disk or USB flash drive, in the USB 2.0 port on the rear panel of your wireless router. Ensure that the USB storage device is formatted and partitioned properly. Refer to the ASUS website at http://event.asus.com/2009/networks/disksupport/ for the file system support table.

Using AiDisk

AiDisk allows you to share files stored on a connected USB device through the Internet. AiDisk also assists you with setting up ASUS DDNS and an FTP server.

To use AiDisk:

1. From the navigation panel, go to **General** > **USB application**, then click the **AiDisk** icon.
2. From the Welcome to AiDisk wizard screen, click **Go**.

3. Select the access rights that you want to assign to the clients accessing your shared data.

4. Create your domain name via the ASUS DDNS services, read the Terms of Service and then select **I will use the service and accept the Terms of service** and key in your domain name. When done, click **Next**.

You can also select **Skip ASUS DDNS settings** then click **Next** to skip the DDNS setting.

5. Click **Finish** to complete the setting.
6. To access the FTP site that you created, launch a web browser or a third-party FTP client utility and key in the ftp link (**ftp://<domain name>.asuscomm.com**) you have previously created.

Using Servers Center

Servers Center allows you to share the media files from the USB disk via a Media Server directory, Samba share service, or FTP share service. You can also configure other settings for the USB disk in the Servers Center.

Using Media Server

Your wireless router allows DLNA-supported devices to access multimedia files from the USB disk connected to your wireless router.

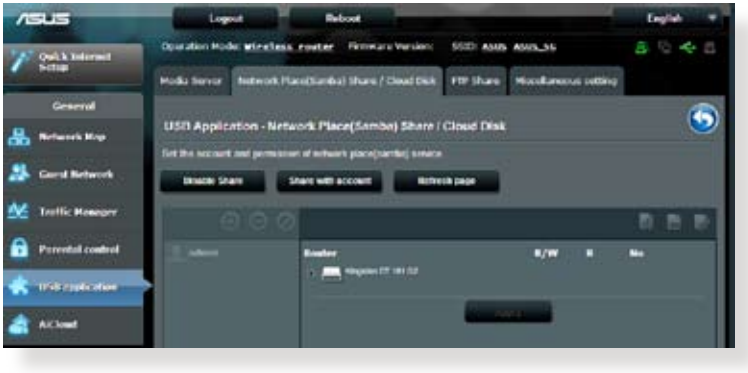
Before using the DLNA Media Server function, connect your device to the RT-N14UHP's network.

To launch the Media Server setting page, go to **General** > **USB application** > **Servers Center** > **Media Servers** tab. Refer to the following for the descriptions of the fields:

- **Enable DLNA Media Server**: Select ON/OFF to enable/disable the DLNA Media Server.
- **Enable iTunes Server?**: Select ON/OFF to enable/disable the iTunes Server.
- **Media server directory**: Select your media server directory and click **Apply** to share files from the USB disk to media devices in the network.
- **Media Server Status**: Displays the status of the media server.

Using Network Place (Samba) Share service

Network Place (Samba) Share allows you to set up the accounts and permissions for the Samba service.



To use Samba share:

1. From the navigation panel, go to **General** > **USB application** > **Servers Center**.

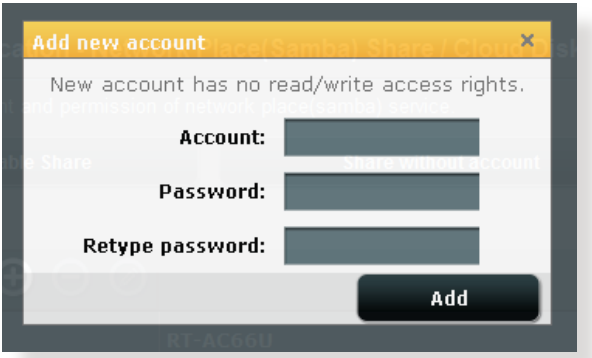
Network Place (Samba) Share is enabled by default.

2. Follow the steps below to add, delete, or modify an account.

To create a new account:

a) Click ⊕ to add new account.

b) In the **Account** and **Password** fields, key in the name and password of your network client. Retype the password to confirm. Click **Add** to add the account to the list.



To delete an existing account:

a) Select the account that you want to delete.

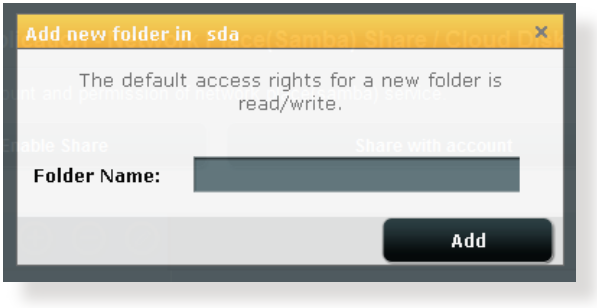
b) Click ⊖.

c) When prompted, click **Delete** to confirm the account deletion.

To add a folder:

a) Click .

b) Enter the folder name, and click **Add**. The folder that you created will be added to the folder list.

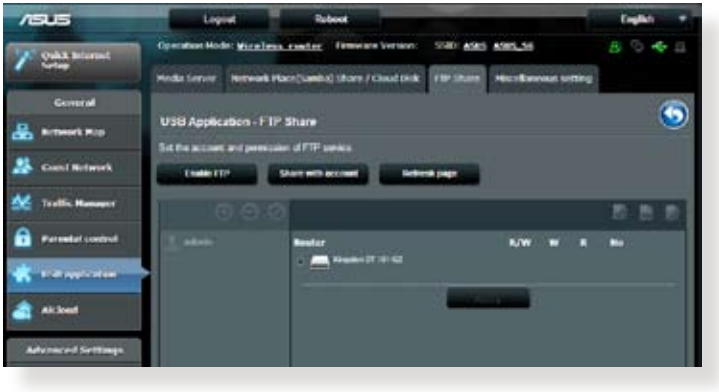


3. From the list of folders, select the type of access permission that you want to assign for specific folders:
   - **R/W:** Select this option to assign read/write access.
   - **R:** Select this option to assign read-only access.
   - **No**: Select this option if you do not want to share a specific file folder.
4. Click **Apply** to apply the changes.

Using the FTP Share service

FTP share enables an FTP server to share files from USB disk to other devices via your local area network or via the Internet.

Ensure that you safely remove the USB disk. Incorrect removal of the USB disk may cause data corruption.



To use FTP Share service:

Ensure that you have set up your FTP server through AiDisk. For more details, refer to the section **Using AiDisk**.

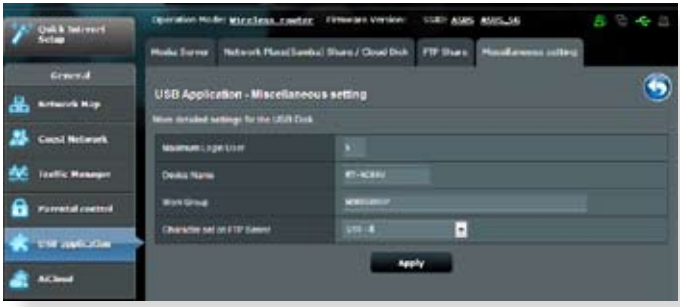
1. From the navigation panel, click **General** > **USB application** > **Servers Center** > **FTP Share** tab.
2. From the list of folders, select the type of access rights that you want to assign for specific folders:
   - **R/W**: Select to assign read/write access for a specific folder.
   - **W**: Select to assign write only access for a specific folder.
   - **R**: Select to assign read only access for a specific folder.
   - **No**: Select this option if you do not want to share a specific folder.
3. Click **Apply** to confirm the changes.
4. To access the FTP server, key in the ftp link **ftp://<hostname>.asuscomm.com** and your user name and password on a web browser or a third-party FTP utility.

Miscellaneous setting

Miscellaneous setting allows you to configure other settings for the USB disk, including the maximum number of user logins, the device name, work group, and character set used on the FTP server.

To configure Miscellaneous settings:

1. From the navigation panel, click **General** > **USB application** > **Servers Center** > **Miscellaneous setting** tab.



2. Configure the following settings:

   - **Maximum Login User**

     Set the maximum number of concurrent connections of the Network Neighborhood or FTP Server.

     Some FTP clients may establish more than one connection. Setting this number too low will lead to login failures.

   - **Device Name**

     Assigns the name of the device as shown on the network. For example, for a device with the name ABC, enter //ABC on the Internet Explorer address bar to access the Network Place service.

- **Work Group**

  Assigns the name of the local RT-N14UHP network as seen in Network Neighborhood.

  NOTE: For **Device Name** and **Work Group,** the standard input characters include letters (a-z, A-Z), digits (0-9), space, underscores(_), and hyphens(-). The first and last character should not contain any spaces. An invalid workgroup name makes it harder for other devices to find your device in the network.

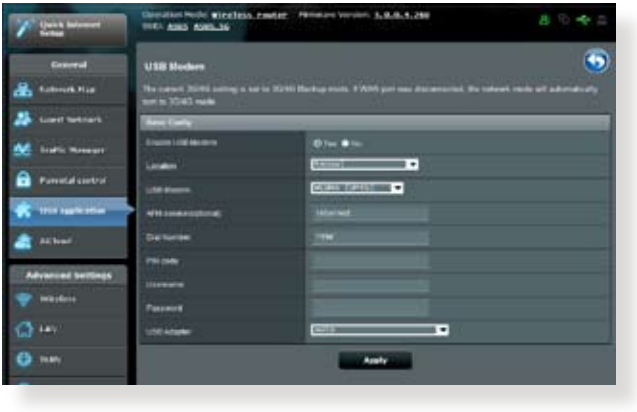
- **Character set on FTP Server**

  Select the appropriate encoding used during data exchange on the FTP server.

3G/4G

3G/4G USB modems can be connected to RT-N14UHP to allow Internet access.

For a list of verified USB modems, please visit:
http://event.asus.com/2009/networks/3gsupport/



To set up 3G/4G internet access:

1. From the navigation panel, click **General** > **USB application** > **3G/4G**.
2. In the **Enable USB Modem** field, select **Yes**.
3. Set up the following:
   - **Location:** Select your 3G/4G service provider's location from the dropdown list.
   - **ISP**: Select your Internet Service Provider (ISP) from the dropdown list.
   - **APN (Access Point Name) service (optional)**: Contact your 3G/4G service provider for detailed information.
   - **Dial Number and PIN code**: The 3G/4G provider's access number and PIN code for connection.

PIN code may vary from different providers.

   - **Username / Password:** The username and password will be provided by the 3G/4G network carrier.
   - **USB Adapter**: Choose your USB 3G / 4G adapter from the dropdown list. If you are not sure of your USB adapter's model or the model is not listed in the options, select **Auto**.
4. Click **Apply**.

The router will reboot for the settings to take effect.

Using AiCloud

AiCloud is a cloud service application that allows you to save, sync, share, and access your files.

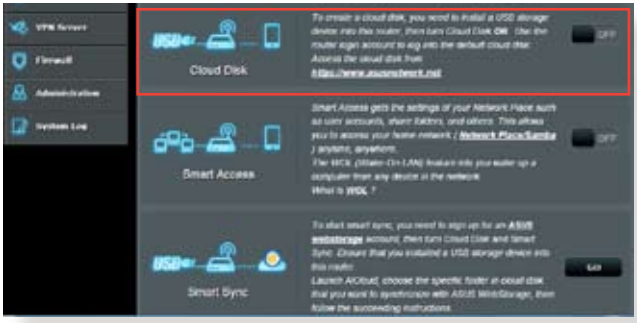
To use AiCloud:

1. From Google Play Store or Apple Store, download and install the ASUS AiCloud app to your smart device.
2. Connect your smart device to your network. Follow the instructions to complete the AiCloud setup process.

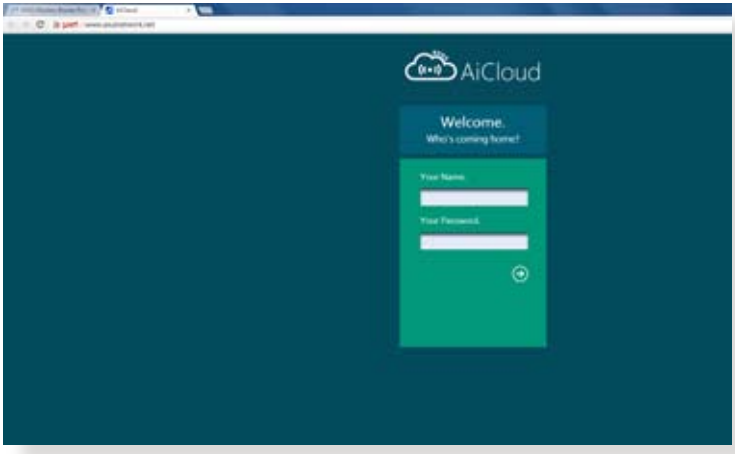
Cloud Disk

To create a cloud disk:

1. Insert a USB storage device into the wireless router.
2. Turn on **Cloud Disk**.

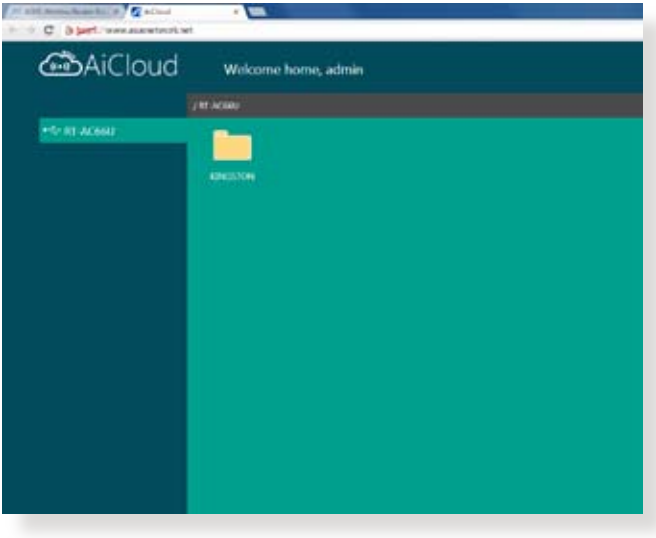


3. Go to https://www.asusnetwork.net and enter the router login account and password. For better user experience, we recommend that you use **Google Chrome** or **Firefox**.



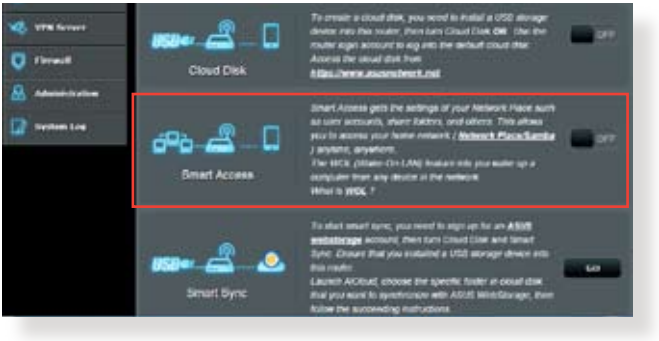
4. You can now start accessing Cloud Disk files on devices connected to the network.

When accessing the devices that are connected to the network, you need to enter the device's user name and password manually, which will not be saved by AiCloud for security reason.



Smart Access

The Smart Access function allows you to easily access your home network via your router's domain name.



NOTES:

- You can create a domain name for your router with ASUS DDNS. For more details, refer to section **DDNS**.
- By default, AiCloud provides a secure HTTPS connection. Key in https://[yourASUSDDNSname].asuscomm.com for a very secure Cloud Disk and Smart Access usage.

Smart Sync

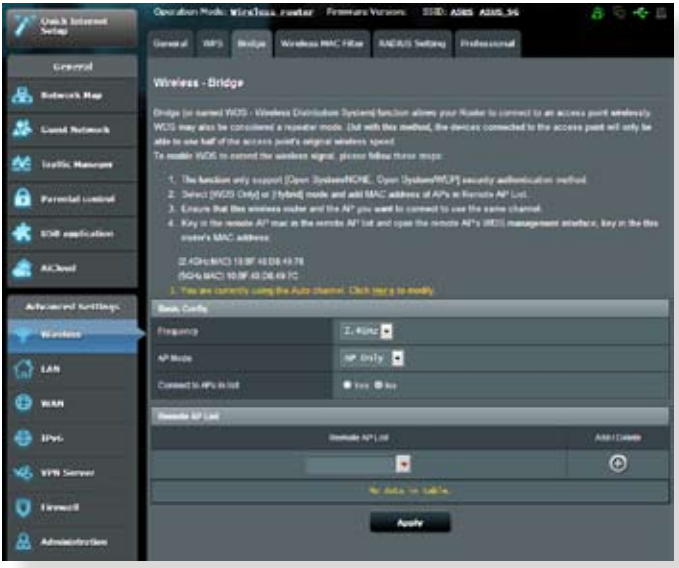
To use Smart Sync:

1. Launch AiCloud, click **Smart Sync** > **Go**.
2. Select **ON** to enable Smart Sync.
3. Click **Add new account**.
4. Enter your ASUS WebStorage account password and select the directory that you want to sync with WebStorage.
5. Click **Apply**.

4. Configuring Advanced settings

Bridge

Bridge or WDS (Wireless Distribution System) allows your ASUS wireless router to connect to another wireless access point exclusively, preventing other wireless devices or stations to access your ASUS wireless router. It can also be considered as a wireless repeater where your ASUS wireless router communicates with another access point and other wireless devices.



To set up the wireless bridge:

1. From the navigation panel, go to **Advanced Settings** > **Wireless** > **Bridge** tab.
2. Select the frequency band for the wireless bridge.
3. In the **AP Mode** field, select any of these options:
   - **AP Only**: Disables the Wireless Bridge function.
   - **WDS Only**: Enables the Wireless Bridge feature but prevents other wireless devices/stations from connecting to the router.

- **HYBRID**: Enables the Wireless Bridge feature and allows other wireless devices/stations to connect to the router.

In Hybrid mode, wireless devices connected to the ASUS wireless router will only receive half the connection speed of the Access Point.

4. In the **Connect to APs in list** field, click **Yes** if you want to connect to an Access Point listed in the Remote AP List.
5. In the **Control Channel** field, select the operating channel for the wireless bridge. Select **Auto** to allow the router to automatically select the channel with the least amount of interference.

Channel availability varies per country or region.

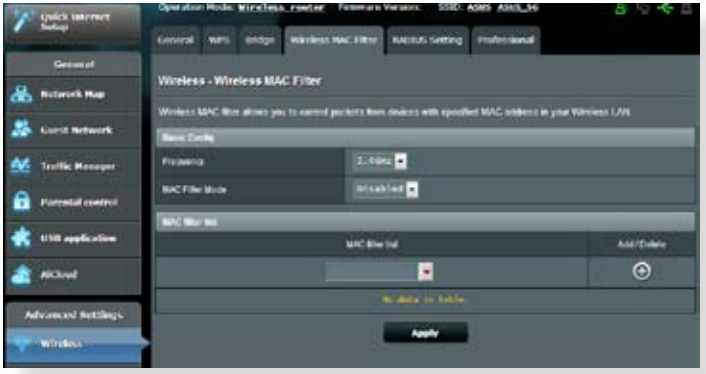
6. On the Remote AP List, key in a MAC address and click the **Add** button  to enter the MAC address of other available Access Points.

Any Access Point added to the list should be on the same Control Channel as the ASUS wireless router.

7. Click **Apply**.

Wireless MAC Filter

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

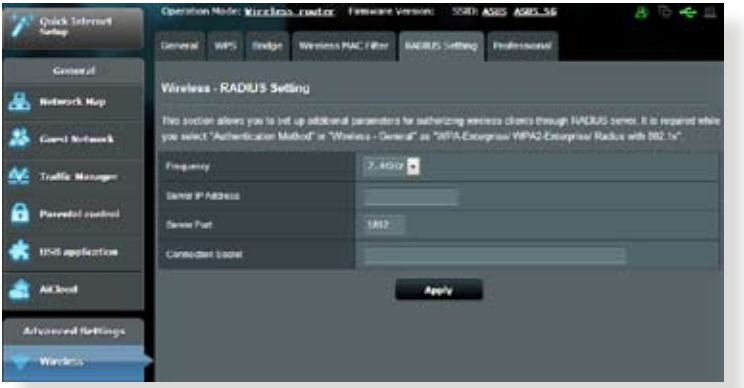


To set up the Wireless MAC filter:

1. From the navigation panel, go to **Advanced Settings** > **Wireless** > **Wireless MAC Filter** tab.
2. In the **Frequency** field, select the frequency band that you want to use for the 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 to the wireless network.
   - Select **Reject** to prevent devices in the MAC filter list to access to the wireless network.
4. On the MAC filter list, click the **Add** button and key in the MAC address of the wireless device.
5. Click **Apply**.

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.



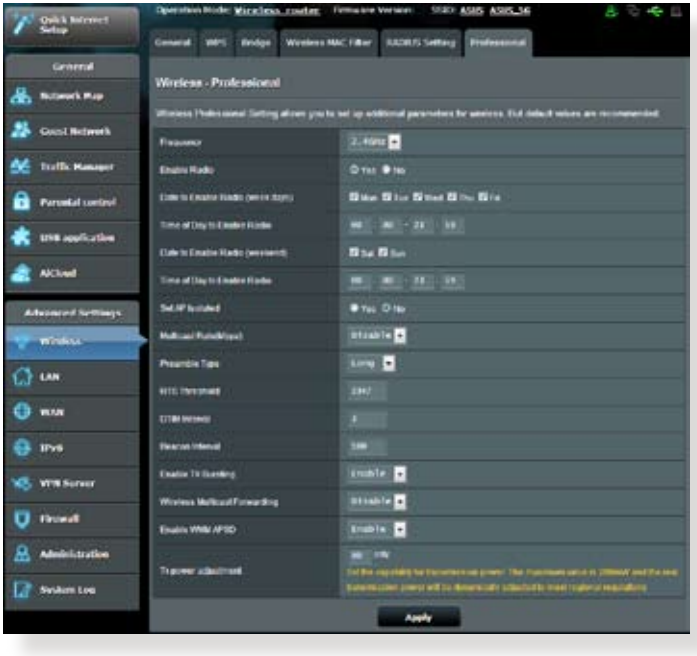
To set up wireless RADIUS settings:

1. Ensure that the wireless router's authentication mode is set to WPA-Enterprise, WPA2-Enterprise, or Radius with 802.1x.
2. From the navigation panel, go to **Advanced Settings** > **Wireless** > **RADIUS Setting**.
3. Select the frequency band.
4. In the **Server IP Address** field, key in your RADIUS server's IP Address.
5. In the **Connection Secret** field, assign the password to access your RADIUS server.
6. Click **Apply**.

Professional

The Professional screen provides advanced configuration options.

We recommend that you use the default values on this page.



In the **Professional Settings** screen, you can configure the following:

- **Frequency**: Select the frequency band that the professional settings will be applied to.
- **Enable Radio**: Select **Yes** to enable wireless networking. Select **No** to disable wireless networking.
- **Date to Enable Radio (weekdays)**: You can specify which days of the week wireless networking is enabled.
- **Time of Day to Enable Radio**: You can specify a time range when wireless networking is enabled during the week.

- **Date to Enable Radio (weekend)**: You can specify which days of the weekend wireless networking is enabled.
- **Time of Day to Enable Radio**: You can specify a time range when wireless networking is enabled during the weekend.
- **Set AP isolated**: The Set AP isolated item prevents wireless devices on your network from communicating with each other. This feature is useful if many guests frequently join or leave your network. Select **Yes** to enable this feature or select **No** to disable.
- **Multicast rate (Mbps)**: Select the multicast transmission rate or click **Disable** to switch off simultaneous single transmission.
- **Preamble Type**: Preamble Type defines the length of time that the router spent for CRC (Cyclic Redundancy Check). CRC is a method of detecting errors during data transmission. Select **Short** for a busy wireless network with high network traffic. Select **Long** if your wireless network is composed of older or legacy wireless devices.
- **RTS Threshold**: Select a lower value for RTS (Request to Send) Threshold to improve wireless communication in a busy or noisy wireless network with high network traffic and numerous wireless devices.
- **DTIM Interval**: DTIM (Delivery Traffic Indication Message) Interval or Data Beacon Rate is the time interval before a signal is sent to a wireless device in sleep mode indicating that a data packet is awaiting delivery. The default value is three milliseconds.
- **Beacon Interval**: Beacon Interval is the time between one DTIM and the next. The default value is 100 milliseconds. Lower the Beacon Interval value for an unstable wireless connection or for roaming devices.
- **Enable TX Bursting**: Enable TX Bursting improves transmission speed between the wireless router and 802.11g devices.

- **Wireless multicast forwarding**: Select **Enable** to allow the wireless router to forward multicast traffic to other wireless devices that support multicast. Select **Disable** to prevent the router from forwarding multicast transmissions.
- **Enable WMM APSD**: Enable WMM APSD (Wi-Fi Multimedia Automatic Power Save Delivery) to improve power management between wireless devices. Select **Disable** to switch off WMM APSD.
- **TX Power adjustment**: TX Power adjustment refers to the milliWatts (mW) needed to power the radio signal output of the wireless router. Enter a value between 0 to 100.

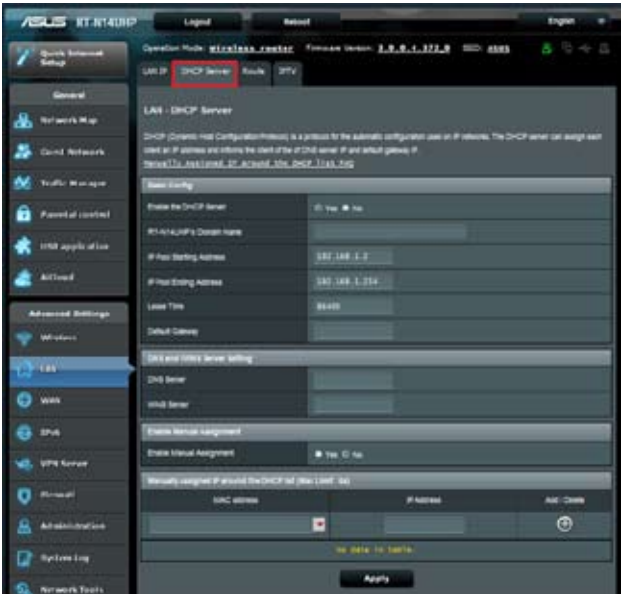
Increasing the TX Power adjustment values may affect the stability of the wireless network.

Setting up the DHCP Server

Your wireless router uses DHCP to assign IP addresses automatically on your network. You can specify the IP address range and lease time for the clients on your network.

To configure the DHCP server:

1. Click **LAN** on the navigation panel.
2. Click the **DHCP Server** tab.



3. In the **Enable the DHCP Server** field, tick **Yes**.
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.
6. In the **Lease Time** field, specify in seconds when an assigned IP address will expire. Once it reaches this time limit, the DHCP server will then assign a new IP address.

- ASUS recommeds 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 Address should not be greater than the IP Pool Ending Address.

Route

If your network makes use of more than one wireless router, you can configure a routing table to share the same Internet service.

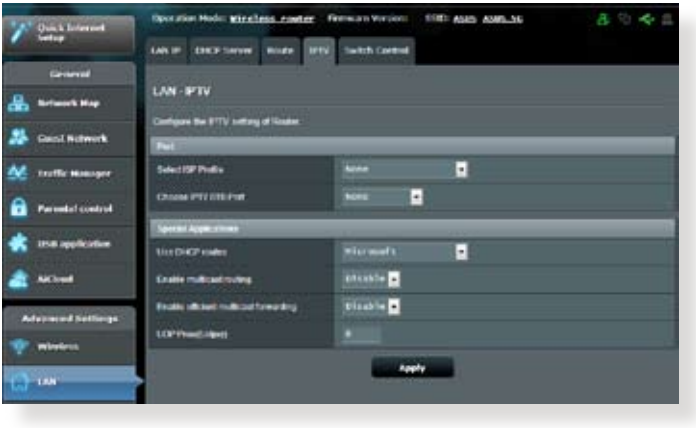
We recommend that you do not change the default route settings unless you have advanced knowledge of routing tables.

To configure the LAN Routing table:

1. From the navigation panel, go to **Advanced Settings** > **LAN** > **Route** tab.
2. On the **Enable static routes** field, choose **Yes**.
3. On the **Static Route List**, enter the network information of other access points or nodes. Click the **Add** or **Delete** button to add or remove a device on the list.
4. Click **Apply**.

IPTV

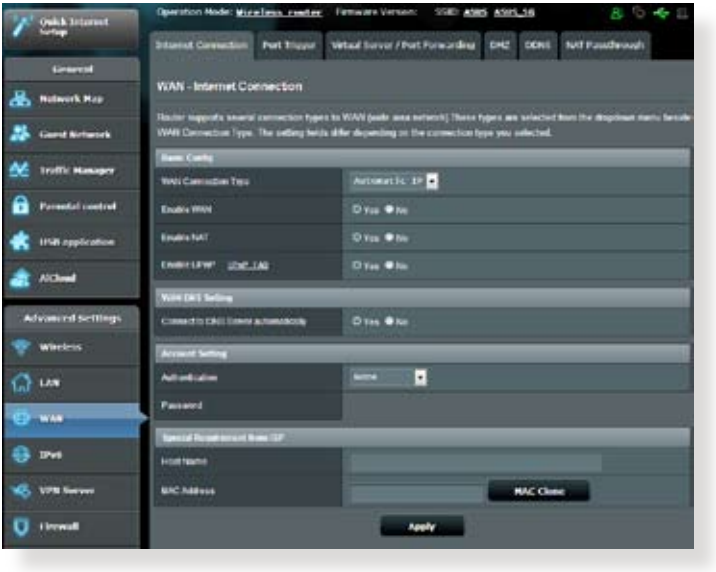
The wireless router supports connection to IPTV services through an ISP or a LAN. The IPTV tab provides the configuration settings needed to set up IPTV, VoIP, multicasting, and UDP for your service. Contact your ISP for specific information regarding your service.



WAN

Internet Connection

The Internet Connection screen allows you to configure the settings of various WAN connection types.



To configure the WAN connection settings:

1. From the navigation panel, go to **Advanced Settings** > **WAN** > **Internet Connection** tab.
2. Configure the following settings below. When done, click **Apply**.
   - **WAN Connection Type**: Choose your Internet Service Provider type. The choices are **Automatic IP**, **PPPoE**, **PPTP**, **L2TP** 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.

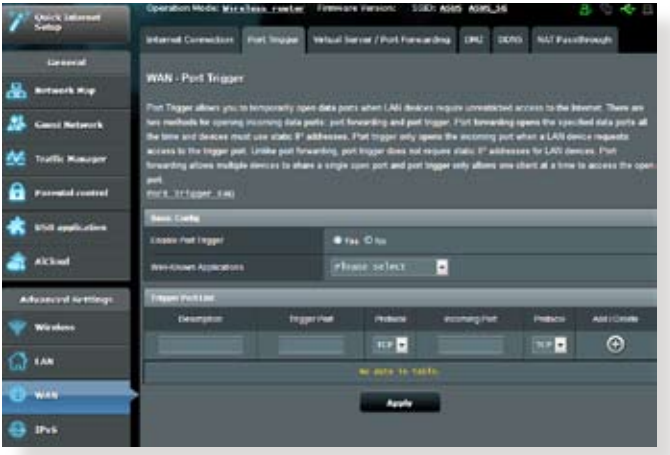
- E**nable NAT**: NAT (Network Address Translation) is a system where one public IP (WAN IP) is used to provide Internet access to network clients with a private IP address in a LAN. The private IP address of each network client is saved in a NAT table and is used to route incoming data packets.
- **Enable UPnP**: UPnP (Universal Plug and Play) allows several devices (such as routers, televisions, stereo systems, game consoles, and cellular phone), 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.
- **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.

Port Trigger

Port range triggering opens a predetermined incoming port for a limited period of time whenever a client on the local area network makes an outgoing connection to a specified port. Port triggering is used in the following scenarios:

- More than one local client needs port forwarding for the same application at a different time.
- An application requires specific incoming ports that are different from the outgoing ports.



To set up Port Trigger:

1. From the navigation panel, go to **Advanced Settings** > **WAN** > **Port Trigger** tab.
2. Configure the following settings below. When done, click **Apply**.

- **Enable Port Trigger**: Choose **Yes** to enable Port Trigger.
- **Well-Known Applications**: Select popular games and web services to add to the Port Trigger List.
- **Description**: Enter a short name or description for the service.

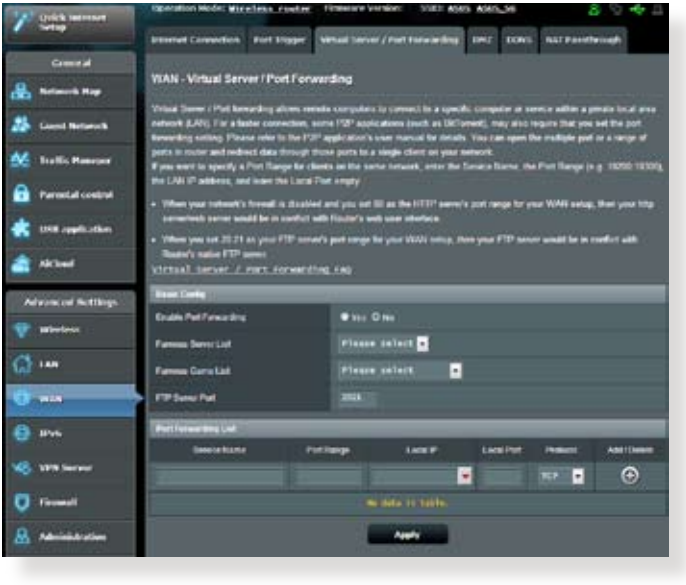
- **Trigger Port**: Specify a trigger port to open the incoming port.
- **Protocol**: Select the protocol, TCP, or UDP.
- **Incoming Port**: Specify an incoming port to receive inbound data from the Internet.
- **Protocol**: Select the protocol, TCP, or UDP.

- When connecting to an IRC server, a client PC makes an outgoing connection using the trigger port range 66660-7000. The IRC server responds by verifying the username and creating a new connection to the client PC using an incoming port.
- If Port Trigger is disabled, the router drops the connection because it is unable to determine which PC is requesting for IRC access. When Port Trigger is enabled, the router assigns an incoming port to receive the inbound data. This incoming port closes once a specific time period has elapsed because the router is unsure when the application has been terminated.
- Port triggering only allows one client in the network to use a particular service and a specific incoming port at the same time.
- You cannot use the same application to trigger a port in more than one PC at the same time. The router will only forward the port back to the last computer to send the router a request/ trigger.

Virtual Server/Port Forwarding

Port forwarding 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. Setting up Port Forwarding on your router allows PCs outside the network to access specific services provided by a PC in your network.

When port forwarding is enabled, the ASUS router blocks unsolicited inbound traffic from the Internet and only allows replies from outbound requests from the LAN. The network client does not have access to the Internet directly, and vice versa.



To set up Port Forwarding:

1. From the navigation panel, go to **Advanced Settings** > **WAN** > **Virtual Server / Port Forwarding** tab.

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

- **Enable Port Forwarding**: Choose **Yes** to enable Port Forwarding.
- **Famous Server List**: Determine which type of service you want to access.
- **Famous Game List**: This item lists ports required for popular online games to work correctly.
- **FTP Server Port**: Avoid assigning the port range 20:21 for your FTP server as this would conflict with the router's native FTP server assignment.
- **Service Name**: Enter a service name.
- **Port Range**: If you want to specify a Port Range for clients on the same network, enter the Service Name, the Port Range (e.g. 10200:10300), the LAN IP address, and leave the Local Port empty. Port range accepts various formats such as Port Range (300:350), individual ports (566,789) or Mix (1015:1024,3021).

- When your network's firewall is disabled and you set 80 as the HTTP server's port range for your WAN setup, then your http server/web server would be in conflict with the router's web user interface.
- A network makes use of ports in order to exchange data, with each port assigned a port number and a specific task. For example, port 80 is used for HTTP. A specific port can only be used by one application or service at a time. Hence, two PCs attempting to access data through the same port at the same time would fail. For example, you cannot set up Port Forwarding for port 100 for two PCs at the same time.

- **Local IP**: Key in the client's LAN IP address.

Use a static IP address for the local client to make port forwarding work properly. Refer to section **LAN** for information.

- **Local Port**: Enter a specific port to receive forwarded packets. Leave this field blank if you want the incoming packets to be redirected to the specified port range.
- **Protocol**: Select the protocol. If you are unsure, select **BOTH**.

To check if Port Forwarding has been configured successfully:

- Ensure that your server or application is set up and running.
- You will need a client outside your LAN but has Internet access (referred to as "Internet client"). This client should not be connected to the ASUS router.
- On the Internet client, use the router's WAN IP to access the server. If port forwarding has been successful, you should be able to access the files or applications.

Differences between port trigger and port forwarding:

- Port triggering will work even without setting up a specific LAN IP address. Unlike port forwarding, which requires a static LAN IP address, port triggering allows dynamic port forwarding using the router. Predetermined port ranges are configured to accept incoming connections for a limited period of time. Port triggering allows multiple computers to run applications that would normally require manually forwarding the same ports to each PC on the network.
- Port triggering is more secure than port forwarding since the incoming ports are not open all the time. They are opened only when an application is making an outgoing connection through the trigger port.

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.

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**.

- **IP address of Exposed Station:** Key in 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.

To remove DMZ:

1. Delete the client's LAN IP address from the **IP Address of Exposed Station** text box.
2. When done, click **Apply**.

DDNS

Setting up DDNS (Dynamic DNS) allows you to access the router from outside your network through the provided ASUS DDNS Service or another DDNS service.

To set up DDNS:

1. From the navigation panel, go to **Advanced Settings** > **WAN** > **DDNS** tab.
2. Configure the following settings below. When done, click **Apply**.
   - **Enable the DDNS Client**: Enable DDNS to access the ASUS router via the DNS name rather than WAN IP address.
   - **Server and Host Name**: Choose ASUS DDNS or other DDNS. If you want to use ASUS DDNS, fill in the Host Name in the format of xxx.asuscomm.com (xxx is your host name).
   - If you want to use a different DDNS service, click FREE TRIAL and register online first. Fill in the User Name or E-mail Address and Password or DDNS Key fields.

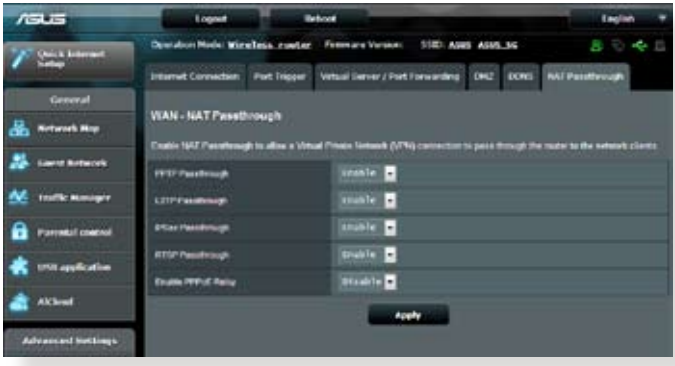
- **Enable wildcard**: Enable wildcard if your DDNS service requires one.

- DDNS service will not work under these conditions:
- When the wireless router is using a private WAN IP address (192.168.x.x, 10.x.x.x, or 172.16.x.x), as indicated by a yellow text.
- The router may be on a network that uses multiple NAT tables.

NAT Passthrough

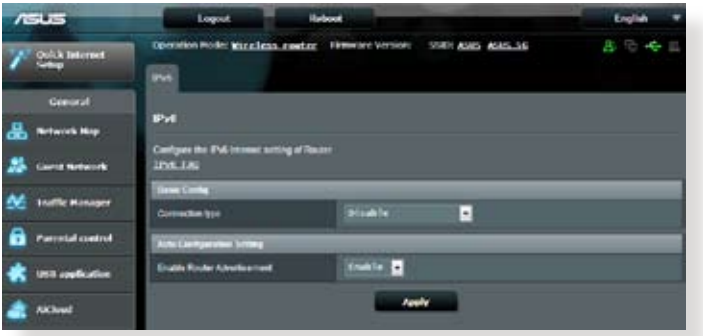
NAT Passthrough allows a Virtual Private Network (VPN) connection to pass through the router to the network clients. PPTP Passthrough, L2TP Passthrough, IPsec Passthrough and RTSP Passthrough are enabled by default.

To enable / disable the NAT Passthrough settings, go to the **Advanced Settings** > **WAN** > **NAT Passthrough** tab. When done, click **Apply**.



IPv6

This wireless router supports IPv6 addressing, a system that supports more IP addresses. This standard is not yet widely available. Contact your ISP if your Internet service supports IPv6.



To set up IPv6:

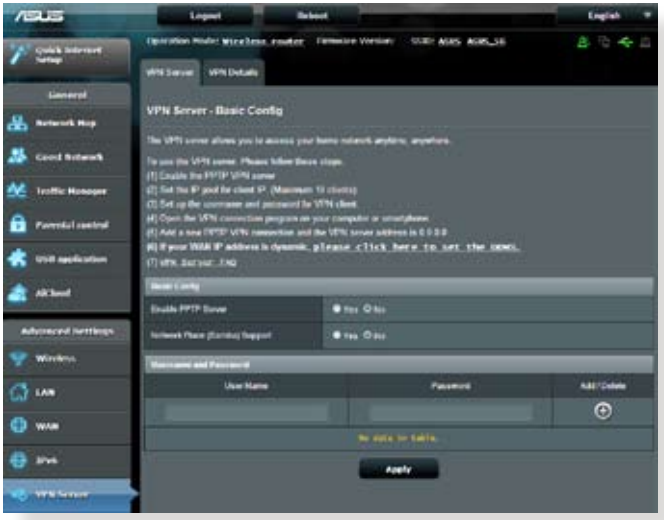
1. From the navigation panel, go to **Advanced Settings** > **IPv6**.
2. Select your **Connection Type**. The configuration options vary depending on your selected connection type.
3. Enter your IPv6 LAN and DNS settings.
4. Click **Apply**.

Please refer to your ISP regarding specific IPv6 information for your Internet service.

VPN Server

VPN (Virtual Private Network) provides a secure communication to a remote computer or remote network using a public network such as the Internet.

Before setting up a VPN connection, you would need the IP address or domain name of the VPN server you are trying to access.



To set up access to a VPN server:

1. From the navigation panel, go to **Advanced Settings** > **VPN Server**.
2. On the Enable PPTP Server field, select **Yes**.
3. On the Network Place (Samba) Support field, select **Yes**.
4. Enter the user name and password for accessing the VPN server. Click the button.
5. Click **Apply**.

For advanced VPN server settings, click the **VPN Server** tab to configure broadcast support, authentication, MPPE Encryption, and Client IP address range.

Firewall

The wireless router can serve as a hardware firewall for your network.

The Firewall feature is enabled by default.

General

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 **Yes.**
3. On the **Enable DoS** protection, select **Yes** to protect your network from DoS (Denial of Service) attacks though this may affect your router's performance.
4. You can also monitor packets exchanged between the LAN and WAN connection. On the Logged packets type, select **Dropped**, **Accepted**, or **Both**.
5. Click **Apply**.

URL Filter

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

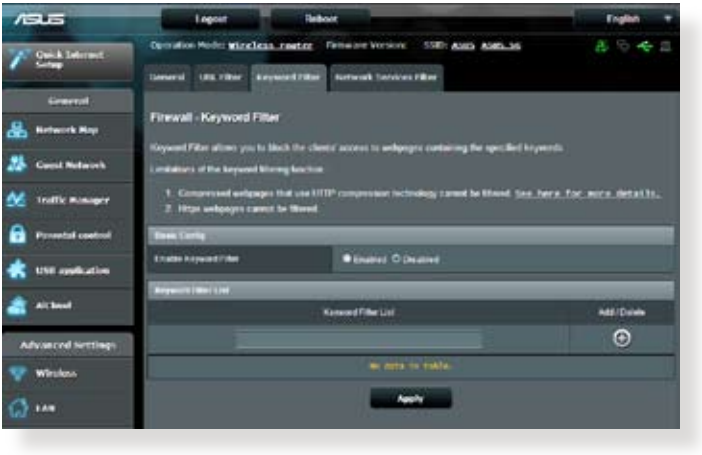
The URL Filter is based on a DNS query. If a network client has already accessed a website such as http://www.abcxxx.com, then the website will not be blocked (a DNS cache in the system stores previously visited websites). To resolve this issue, clear the DNS cache before setting up the URL Filter.

To set up a URL filter:

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

Keyword filter

Keyword filter blocks access to webpages containing specified keywords.



To set up a keyword filter:

1. From the navigation panel, go to **Advanced Settings** > **Firewall** > **Keyword Filter** tab.
2. On the Enable Keyword Filter field, select **Enabled**.

3. Enter a word or phrase and click the **Add** button.
4. Click **Apply**.

- The Keyword 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 Keyword Filter.
- Web pages compressed using HTTP compression cannot be filtered. HTTPS pages also cannot be blocked using a keyword filter.

Network Services Filter

The Network Services Filter blocks LAN to WAN packet exchanges and restricts network clients from accessing specific web services such as Telnet or FTP.

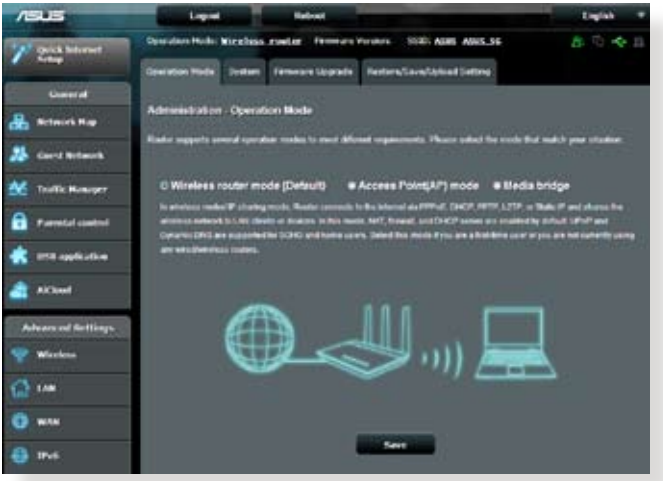
To set up a Network Service filter:

1. From the navigation panel, go to **Advanced Settings** > **Firewall** > **Network Service Filter** tab.
2. On the Enable Network Services Filter field, select **Yes**.
3. Select the Filter table type. **Black List** blocks the specified network services. **White List** limits access to only the specified network services.
4. Specify the day and time when the filters will be active.
5. To specify a Network Service to filter, enter the Source IP, Destination IP, Port Range, and Protocol. Click the  button.
6. Click **Apply**.

Administration

Operation Mode

The Operation Mode page allows you to select the appropriate mode for your network.



To set up the operating mode:

1. From the navigation panel, go to **Advanced Settings** > **Administration** > **Operation Mode** tab.
2. Select any of these operation modes:
   - **Wireless router mode (default)**: In wireless router mode, the wireless router connects to the Internet and provides Internet access to available devices on its own local network.
   - **Media Bridge**: This setup requires two wireless routers. The second router serves as a media bridge where multiple devices such as Smart TVs and gaming consoles can be connected via ethernet.
   - **Access Point mode**: In this mode, the router creates a new wireless network on an exising network.
3. Click **Apply**.

The router will reboot when you change the modes.

System

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

To set up the System settings:

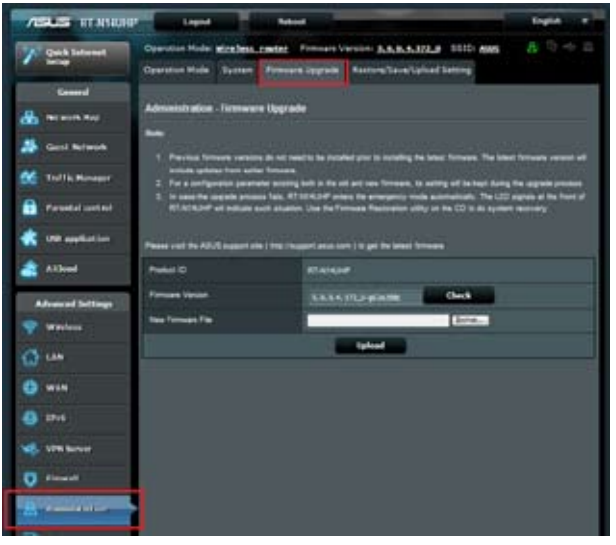
1. From the navigation panel, go to **Advanced Settings** > **Administration** > **System** tab.
2. You can configure the following settings:
   - **Change router login password**: You can change the password and login name for the wireless router by entering a new name and password.
   - **WPS button behavior**: The physical WPS button on the wireless router can be used to activate WPS or switch off wireless networking.
   - **Time Zone**: Select the time zone for your network.
   - **NTP Server**: The wireless router can access a NTP (Network time Protocol) server in order to synchronize the time.
   - **Enable Telnet**: Click **Yes** to enable Telnet services on the network. Click **No** to disable Telnet.
   - **Authentication Method**: You can select HTTP, HTTPS, or both protocols to secure router access.
   - **Enable Web Access from WAN**: Select **Yes** to allow devices outside the network to access the wireless router GUI settings. Select **No** to to prevent access.
   - **Only allow specific IP**: Click **Yes** if you want to specify the IP addresses of devices that are allowed access to the wireless router GUI settings from WAN.
   - **Client List**: Enter the WAN IP addresses of networking devices allowed to access the wireless router settings. This list will be used if you clicked **Yes** in the **Only allow specific IP** item.
3. Click **Apply**.

Upgrading the firmware

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

To upgrade the firmware:

1. Click **Administration** from the navigation panel.
2. Click the **Firmware Upgrade** tab.
3. In the **New Firmware File** item, click **Browse**. Navigate to the downloaded firmware file.
4. Click **Upload**.

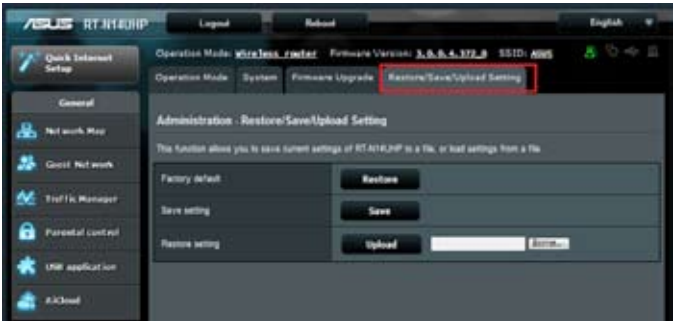


If the upgrade process fails, the wireless router automatically enters rescue mode and the power LED indicator on the front panel starts flashing slowly. To recover or restore the system, use the Firmware Restoration utility.

Restoring/Saving/Uploading settings

To restore/save/upload wireless router settings:

1. Click **Administration** on the navigation panel.
2. Click the **Restore/Save/Upload Setting** tab.



3. Select a task from the configuration options:
   - To restore to default factory settings, click **Restore**, and click **OK** once prompted.
   - 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**.

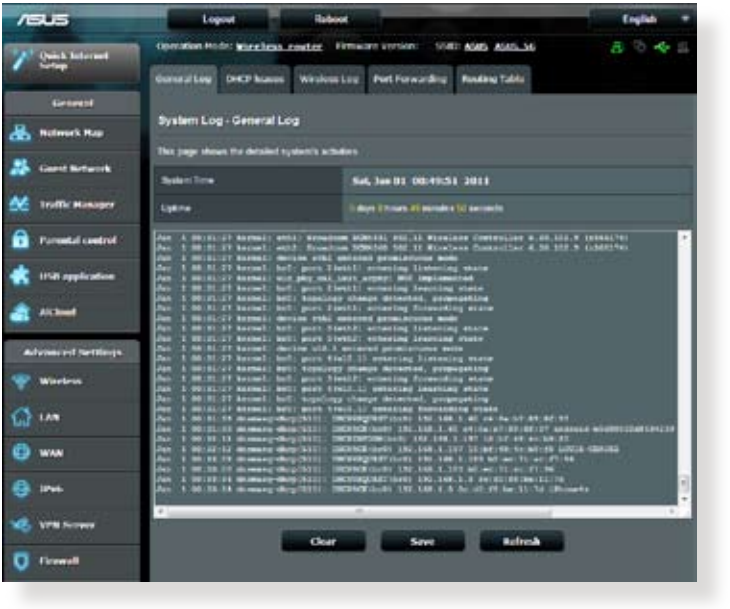
System Log

System Log contains your recorded network activities.

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 any of these tabs:
   - General Log
   - DHCP Leases
   - Wireless Log
   - Port Forwarding
   - Routing Table



Download Master

Download Master is a utility that helps you download files even while your laptops or other devices are switched off.

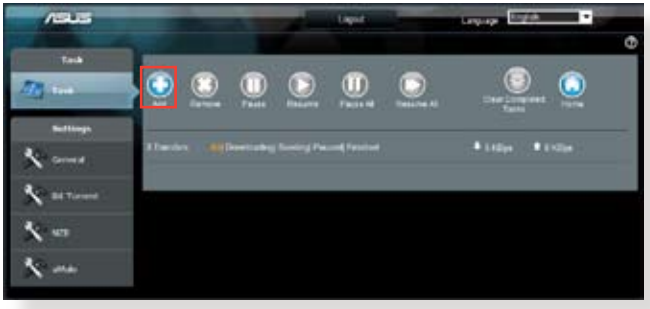
You need a USB device connected to the wireless router to use Download Master.

To use Download Master:

1. Click **General** > **USB application** > **Download Master** to download and install the utility automatically.

   If you have more than one USB drive, select the USB device you want to download the files to.

2. After the download process is finished, click the Download Master icon to start using the utility.
3. Click **Add** to add a download task.



4. Select a download type such as BitTorrent, HTTP, or FTP. Provide a torrent file or a URL to begin downloading.

   For details on Bit Torrent, refer to section **Configuring Bit Torrent download settings**.

5. Use the navigation panel to configure the advanced settings.

Configuring Bit Torrent download settings

To configure BitTorrent download settings:

1. From Download Master's navigation panel, click **Bit Torrent** to launch the **Bit Torrent Setting** page.
2. Select a specific port for your download task.
3. To prevent network congestion, you can limit the maximum upload and download speeds under **Speed Limits**.
4. You can limit the maximum number of allowed peers and enable or disable file encryption during downloads.

NZB settings

You can set up a USENET server to download NZB files. After entering USENET settings, **Apply**.

5. Troubleshooting

If you encounter problems that are not mentioned in this chapter, contact ASUS Technical Support.

Troubleshooting

I cannot access the router GUI for configuring the router.

- Delete the cookies and temporary files in your web browser. To do this in Internet Explorer 8:
  1. Launch your web browser, then click **Tools** > **Internet Options.**
  2. On the General tab, click **Delete** under Browsing history**.**
  3. Tick **Temporary Internet Files** and **Cookies**. Click **Delete**.

Instructions for deleting cookies and temporary Internet files vary with the web browser.

- Disable the proxy server settings, remove any dial-up connections, and set the TCP/IP settings to obtain IP addresses automatically. For more details, refer to the section **Before you proceed** in this user manual.

The client cannot establish a wireless connection with the router.

Out of Range:

- Place the router closer to the wireless client.
- Change the channel settings.

Authentication:

- Use a wired connection to connect to the router.
- Check the wireless security settings.
- Press the Reset button at the rear panel for more than five seconds.

Cannot find the router:

- Press the Reset button at the rear panel for more than five seconds.
- Check the settings in the wireless adapter such as SSID and encryption method.

Cannot access the Internet using a wireless LAN adapter.

- Place the router closer to the wireless client.
- Check whether the wireless adapter is connected to the correct wireless router.
- Check whether the wireless channel in use conforms to the channels available in your country/area.
- Check the encryption settings.
- Check if the ADSL or Cable connection is connected.
- Use a different Ethernet cable.

Internet is not accessible.

- Check the status indicators on the ADSL modem and the wireless router.
- Check if the WAN LED on the wireless router is on. If the LED is off, switch Ethernet cables and try again.

The ADSL Modem "Link" light is ON (steady and not blinking) and means Internet access is possible, but I still cannot browse the Internet.

- Restart your computer.
- Check if the WAN LED on the wireless router is on.
- Check the wireless encryption settings.
- Check if the computer can get an IP address (using both a wired or wireless connection).
- Check that your web browser is configured to use the local LAN and is not configured to use a proxy server.

If the ADSL "LINK" light blinks continuously or stays off, Internet access is not possible - the Router is unable to establish a connection with the ADSL network.

- Ensure that all your cables are properly connected .
- Disconnect the power cord from the ADSL or cable modem, wait a few minutes, then reconnect the cord.
- If the ADSL light continues to blink or stays OFF, contact your Internet service provider.

Network name or encryption keys are forgotten.

- Set up a wired connection and reconfigure the wireless security settings.
- Press the Reset button at the rear panel of the wireless router for more than five seconds.

How do you restore the system to its default settings?

- Press the Reset button at the rear panel of the wireless router for more than five seconds.
- Refer to the section **Restoring/Saving/Uploading settings** of this user manual.

The following are the factory default settings:

User name:	admin
Password:	admin
Enable DHCP:	Yes (if WAN cable is plugged in)
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:	ASUS

ASUS DDNS Service

RT-N14UHP routers support the ASUS DDNS service. If you have registered for the ASUS DDNS service but need to exchange devices at the service center, inform the service center that you want to keep the original domain name and retain the DDNS service. Visit your local service center for more information.

- If there is no activity in the domain - such as reconfiguring the router or accessing the registered domain name - within 90 days, the system automatically deletes the registered information.
- If you encounter any problem or difficulty in using your device, contact the service center.

Frequently Asked Questions (FAQs)

1. Will the registered information be lost or registered by others?

If you have not updated the registered information in 90 days, the system automatically deletes the registered information and the domain name may be registered by others.

2. I did not register the ASUS DDNS for the router I bought six months ago. Can I still register it?

Yes, you can still register the ASUS DDNS service for your router. The DDNS service is embedded in your router, so you can register the ASUS DDNS service anytime. Before registering, click **Query** to check if the hostname has been registered or not. If the hostname is available, the system registers the hostname automatically.

3. I have registered a domain name before and it has been working well until my friends told me that they could not access my domain name.

Check the following:

1. Internet connection is available.
2. The DNS server is working properly.
3. The last time you updated the domain name.

If there are still problems in accessing your domain name, contact the service center.

4. Can I register two domain names so I can access my HTTP and FTP servers separately?

No, you cannot. You can only register one domain name for one router. You can use port mapping to implement security in the network.

5. After restarting the router, why is it that I see a different WAN IP address in MS-DOS and in the router configuration page?

This is normal. The interval time between the ISP DNS server and ASUS DDNS results in different WAN IPs in MS-DOS and in the router configuration page. Different ISPs may have different interval times for updating IP addresses.

6. Is the ASUS DDNS service free, or is it just a trial version?

The ASUS DDNS service is a free and embedded service in some ASUS routers. Check your ASUS router if it supports the ASUS DDNS service.

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

Federal Communications Commission Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

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.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Prohibition of Co-location

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter

Safety Information

To maintain compliance with FCC's RF exposure guidelines, this equipment should be installed and operated with minimum distance 20cm between the radiator and your body. Use on the supplied antenna.

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- 2 has 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.

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 Wireless Device is below the Industry Canada (IC) radio frequency exposure limits. The 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。

Authorised distributors in Turkey

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

Tel: +90 212 3311000

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

CIZGI Elektronik San. Tic. Ltd. Sti.

Tel: +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: +90 216 5288888

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

AEEE Yönetmeliğine Uygundur.

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

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

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
	United Kindom	0044-870-1208340; 0035-31890719918	09:00-17:00 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

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

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 Australia (System/Notebook/Eee/LCD)	+43-820-240513
Support Fax	+49-2102-959911
Online support	support.asus.com