Router Setup Instructions

Version 1.0

Oregon Computer Solutions
https://steveshank.com
503 244 7517

These instructions are to help you use the form I made to setup and understand your router. To understand the basics, read my Wireless Networking basics article.

Controlling your router

What is its address? ☐

What is the username? ☐

What is the password? ☐

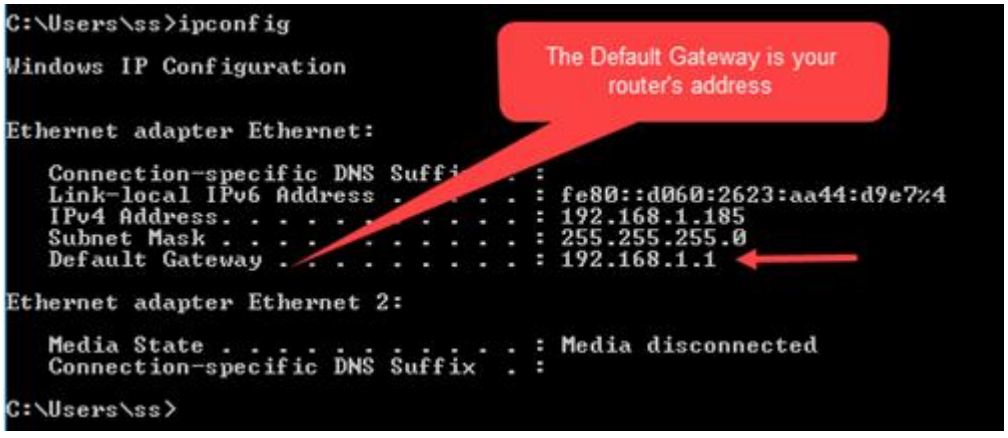
Have you updated the firmware? ☐

Stopping others from controlling your router!

Turned off Unpn? ☐ Turned off WPS? ☐ Turned off Remote Admin? ☐

Controlling your router:

The address is the IP address you'll stick in your browser's address bar to access the router's menu. It is often 192.168.1.1 or something similar. This should be in the quick start setup guide for your router. If your router is already running you can get a command prompt in Windows and type `ipconfig` and then press enter. You'll get something like this.



If you don't know how to get to a command prompt, have someone else setup your router for you.

When you enter this address in the browser's address bar, you'll be asked for a username and password. This will protect your router from hackers trying to change

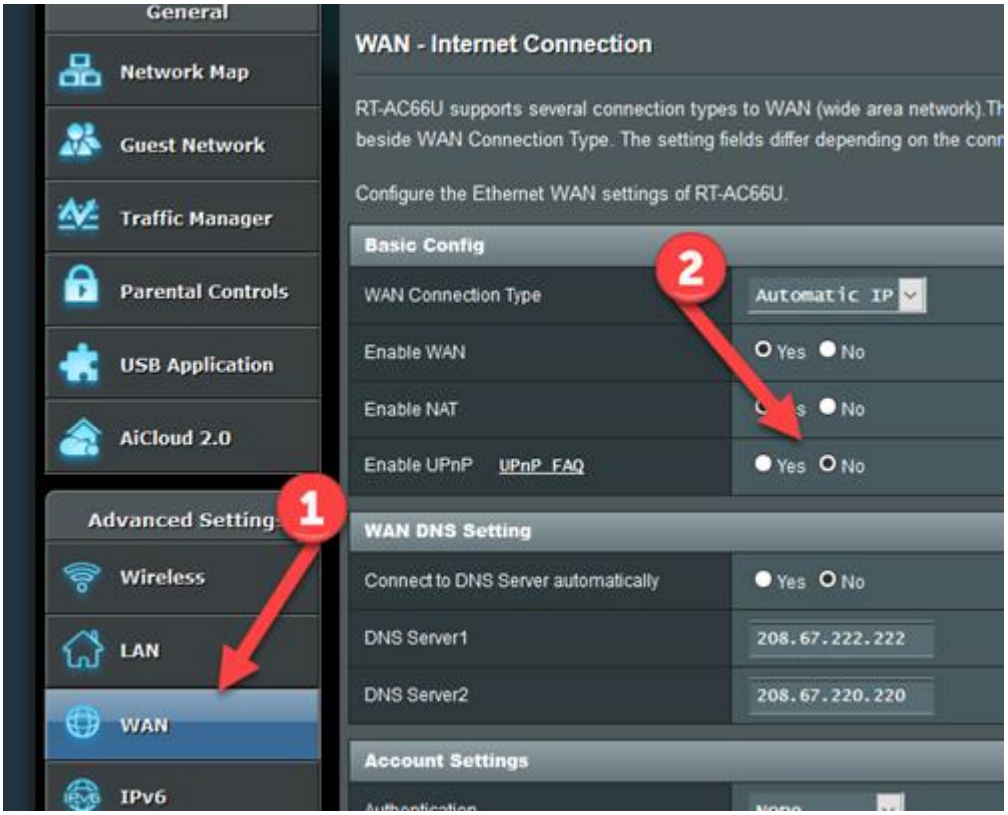
your router's settings. This is not the WiFi password. This is the router password that will enable you to setup a WiFi password. There will be a default username and password and you will need to change at least the password. Do not keep the default. You may be asked to change it right away, but if not you'll have to hunt down where in the menu structure of the router that option exists. Possibly under the Administration tab.

Routers have security flaws and other problems and the good ones get updated. Check your router to determine if there have been patches you should apply. The router will probably check for you, otherwise, check the Administration area to update if needed.

Stopping others from controlling your router!

You might think that the password is sufficient, but it is not. Other things have been done to make things easy at the expense of security. These "features" need to be turned off. However, there is no standard menu or place to put these "features" so you'll have to hunt around to find them, often in sub-menus of sub-menus.

Universal plug and play (UPnP) is a terrible idea from Microsoft where they thought it would be cool to allow printers and other devices to automatically install themselves on your equipment without even telling you about it. Before the specs were fully completed, there were viruses claiming to be legitimate devices trying to install on our machines. Unless you have a specific and necessary need for this, turn it off. But it might be hard to find. Here's where it is on my Asus router:

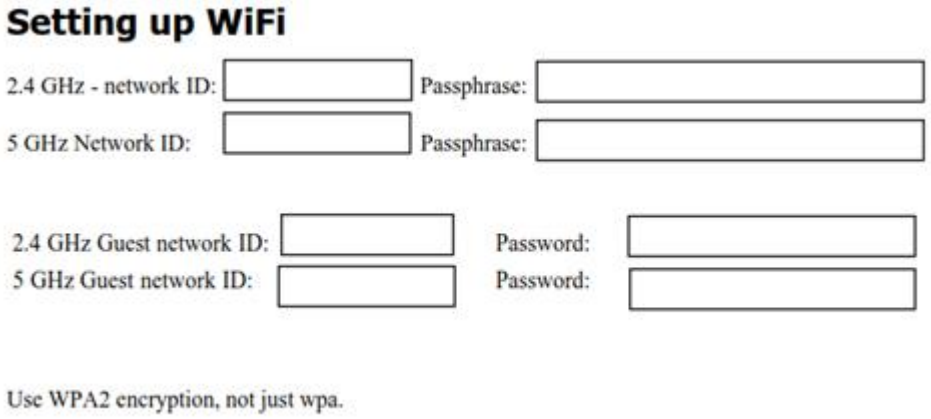


WAN is the Wide Area Network or the World. LAN is your home or office. So, under WAN you'll find the option to turn off UPnP. Other routers stick it under Security or Administration.

WPS stands for Wireless Protected Security. It is a blown attempt to make accessing WiFi connections easier, but still secure. They have a pairing scheme like Bluetooth, but they blew the security so it is easy to hack. Turn it off. Make people use the password. You'll normally find it under Wireless, perhaps in the security section and sometimes under administration.

Remote Admin is sometimes called Web Access from WAN. On Asus routers it is under administration/System. Turn it off unless you are sure you need it. It allows you to login to your router from anywhere (WAN) and change the configuration, instead of only allowing access from the inside (LAN).

WiFi Setup



Normally, you should setup 4 WiFi networks! This surprises most people, who only setup one network. Why you should have 4 networks is explained in the Wireless Networking - 1 article. <link>

Guest Network

You should always setup a Guest network in addition to your regular network. The Guest network can have a simpler password to make it easy for guests to sign in. In addition, at home, you can use it for media players like Roku, or Amazon Fire TV, Apple TV or Google Chromecast. It is also the network you should use for anything you have that connects but isn't your real network. Your router provides a barrier between the guest network and your real network with your computer(s) on it.

Your WiFi network id (SSID) is what devices will see to identify your wireless network. For homes, I suggest that it should convey NO information. Use something like "pumpkin" or "218". For businesses, it should identify your office's network because you probably want guests at least to see the name of your company. I see no reason to

ever identify the name of your router manufacturer. There is no reason to make the job of hackers easier for them. I usually do a -5 after the name to indicate the 5 GHz network.

So a typical home network could be:

- Asparagus
- Asparagus -5
- Asparagus guest
- Asparagus guest -5

A business would substitute their business name or initials for Asparagus.

Your 2.4 GHz and 5 GHz networks should have strong passwords that can still be typed even on a phone. I use the same password for both.

The 2.4 GHz and 5 GHz guest networks should have easier passwords for guests.

You should select WPA2 encryption.