

How Does Wireless Networking Work?

Wireless networking has grown from only being a tool employed by academia and Fortune 500 companies to being deployed in locations such as McDonald's, Starbucks, and gas stations for free consumer use over the past decade.

Consumers can install a wireless network in the home for minimal cost today, and many home theater set-top boxes include the ability to connect to a WiFi network. With the penetration of WiFi capabilities to all modes of life, a common question is how does wireless networking work?

What is Wireless Networking?

Wireless networking, or WiFi, refers to the [Institute of Electrical and Electronic Engineers](#) (IEEE) 802.11 WiFi standard. The 802.11B version of the IEEE standard was the first to gain significant use throughout academic and consumer circles in the early 2000's. As the WiFi standard undergoes improvements, the number at the end of the standard designation is incremented, sometimes resulting letters being skipped. After 802.11B, 802.11G became the most prevalent featuring increased security, with 802.11N seeing significant market penetration at the time of this writing. No matter what wireless standard is employed, a WiFi network allows end users to connect to a network without using a USB, [Ethernet](#), or other "hardwired" connection.

What Makes a Wireless Network Work?

Commercial wireless networks operate in the 2.4 to 5 GHz radio frequency (RF) spectrum. Similar to a TV or mobile phone signal, computers that are WiFi capable leverage a wireless adapter to encode network data packets into a RF signal. The signal is transmitted via the associated wireless antenna connected to the computer. [WiFi antennas](#) are commonly built in to the screen of laptops or smart phones, but can also be installed using an external wireless card on desktop computers or non-wireless capable notebooks.

Once the network transmission is sent by the client device, the network router (WiFi capable) receives the transmission from the computer. The router translates

the RF transmission to network data packets and forwards to the appropriate destination on the local network or Internet. Wireless network routers can be



configured to allow any client computer to connect to the network without a password; however, most wireless routers are now sold with security turned on to avoid nefarious actors from using the wireless networks of others without permission.

What Does a Wireless Router Do?

In order to connect client computers to a local network or the Internet, a wireless router has to be connected to a LAN or valid Internet connection. The router functions as a “gateway” for authorized devices to the LAN or Internet services. In the home, a traditional Internet connection setup through a local ISP (either DSL or cable provider), can be turned into a WiFi network by connecting (and configuring) a wireless modem to the network. Once configured, the router will send and receive network traffic with client computers via RF signal by translating the network packets to / from RF signals and datagrams.

In addition to managing network traffic, modern wireless routers are capable of implementing various levels of network security. These options include local network security (encryption of data through the implementation of one of the available encryption standards accessed via password), network firewall settings, and MAC address filtering.

Wireless Networking Standards

The [IEEE 802.11 wireless networking standard](#) is the primary WiFi implementation sold in industry. Over the course of development of the standard over the previous two decades, there have been a number of improvements made to the standard.

802.11a

The [802.11a wireless standard](#) was released in September of 1999. Supporting

speeds that approach 54 Mbs in the 5 GHz spectrum, the standard achieves a throughput in the mid-20 Mbit/s range. This version of the standard suffers from interference issues and has a smaller overall effective range when compared to succeeding versions of the IEEE wireless standard.

802.11b

The 802.11b standard was also released in September of 1999. Supporting a raw data rate of 11 Mbit/s, this version of the standard was first sold on the market in early 2000. Operating in the 2.4 GHz range, 802.11b was the first WiFi standard to gain widespread acceptance in the marketplace due to significantly reduced cost of the equipment required to support the standard.

802.11g

The [802.11g standard](#) was released in June of 2003. Operating in the 2.4 GHz band, the "Golf" standard achieves a greater bit rate of 54 Mbit/s with a 22 Mbit/s average throughput. Designed to be backwards compatible with the 802.11b hardware, the standard also incorporates more advanced security features than found in previous iterations of the WiFi standard.

802.11n

The [802.11n standard](#) was released in October of 2009. This version supports operations in both the 2.4 GHz and 5 GHz with a maximum data rate ranging from 54 Mbits/s to 600 Mbits/s. The "N" standard also adds multiple-input multiple-output (MIMO) antenna support.

802.11ac

The 802.11ac standard is under draft development with a potential release scheduled for February 2014. 802.11ac work is targeting high throughput in the 5 GHz band and will allow multi-client or station WLAN throughput of 1 gigabit per second.

802.11ad

The [802.11ad standard](#) is referred to as "WiGig." Already published in December of 2012, the new standard is designed to use the 60 GHz standard and will be the first tri-band WiFi solution to be released on the marketplace. 802.11ad will be released on the market in early 2014 and will feature throughput speeds of 7 Gbit/s.

How Do Computers Connect to Wireless Networks?

A laptop, desktop computer, or smart phone require two items to connect to a wireless network: 1 – A wireless adapter, and 2 – A wireless antenna. Unlike the early 2000s when consumers had to purchase wireless cards to connect to a WiFi network, the majority of mobile devices sold today have a built-in antenna with the required wireless adapter pre-installed by the OEM. Once the adapter and antenna are activated by the end-user, the computer will detect all wireless networks in range of the device. On a Windows computer, the System Tray displays a “Network” icon that when expanded will show the [available networks](#) in range of the computer.

By selecting the desired wireless network from this menu (there is an equivalent menu on Mac OS X, [Linux](#), and iOS devices), the end-user is prompted to enter the network password for the network. If the password is successfully entered, the network router will assign a temporary IP address to the device based on the network configuration, and the device will be able to use the LAN or Internet services as if it was connected to the network via Ethernet or USB cable.

How Do Consumers Setup Wireless Routers?

Since the first widespread commercial availability of wireless networking hardware in the early 2000s, it has become significantly easier to setup wireless networking capability in the home or small business. Although many [Internet Service Providers](#) (ISPs) will offer the wireless setup for a fee, most wireless router manufacturers have incorporated “Setup Wizards” into the software configuration options of their hardware. Basic steps to setup a wireless router include:

Step 1 – Connecting the wireless router to the DSL or Cable modem via Ethernet or USB cable. The router should be located in a central location in the home or business to avoid “dead zones” where the network availability will not be optimal.

Step 2 – Turning on the wireless router.

Step 3 – Connecting a laptop to the router via USB or Ethernet cable.

Step 4 – Access the router configuration page by entering the required URL included with the router setup instructions.

Step 5 – Follow the instructions included on the setup wizard, or choosing manual configuration of the device. The setup will include providing a “name” for the network entered under the [SSID](#) (Service Set Identifier) heading, desired security settings (includes the required password to access the network), firewall settings, and if desired, MAC address filtering.

Step 6 – Once the router configuration settings are entered, most devices will require a “reset” before client devices can now use the wireless network.

How Do You Connect to a Wireless Router Configuration Panel?

Most wireless routers sold on the market provide a configuration panel to setup the router through the web browser on a connected client device. The client device must be connected via Ethernet or USB cable to the router to access this page. The default IP address to enter in the web browser’s address bar varies based on manufacturer; however, this address typically resides in the private IP address range of addresses. For example, the default [Netgear Router IP address](#) is [192.168.0.1](#). Once this address is entered in the browser’s address bar, the router configuration login screen will appear. The default password for the router will be included in the user’s guide for the wireless router, but can also be found on the manufacturer’s website if purchasing a router from a third party who may not have the user’s guide available to pass on to the new router’s owner. After the default login and password are entered on the login screen, the router’s configuration panel will be accessible to the end-user to change or setup the network’s configuration.

How Do You Change the Router’s Default Password?

Although many consumers do not change the default router password for home WiFi installations, a good security practice is to change the default password when installing a new wireless router. This task ensures that anyone who can gain

physical access to the router cannot easily change the network configuration without a full reset of the router.

Step 1 – Ensure the router is turned on. Once verified, connect a laptop to the router via Ethernet or USB cable depending on the model of router.

Step 2 – If there is a light that corresponds to the Ethernet port the laptop is connected to on the router, ensure it is illuminated (indicating a valid connection). Not all models of router will have lights that correspond to the Ethernet inputs.

Step 3 – Open the primary web browser on the computer by double-clicking the program icon located on the computer's desktop.

Step 4 – Input the required IP address in the browser's address bar and connect to the router's configuration panel.

Step 5 – Enter the default login and password for the specific router manufacturer and brand of device in the login and password text fields displayed on the login page. If these entries were changed on installation of the router, the newer values will need to be used to access the configuration page.

Step 6 – Select the "Administration" menu tab on the router's configuration menu. Depending on the variant of router, this menu option can be alternatively labeled "Administrator" or "Management."

Step 7 – Enter the desired user name in the "login" or "name" field on this page.

Step 8 – Enter the desired password in the "Password" field on the configuration page. The new password will require a validation entry to confirm correct entry.

Step 9 – Choose the "Save" or "Save Settings" menu button on the configuration panel to save the changes to the router access login and password.

How Do You Set the Wireless Network's SSID?

A wireless network has to be "named" or have a SSID ([Service Set Identifier](#)) setup in order for client devices to connect to the network. In order to allow a wireless network to be used "out of the box," wireless router manufacturers setup the devices to have a default [SSID](#) if the end-user does not change the setting on installation. Although some router manufacturer's now sell routers which have unique default SSIDs, older models will use the same network name that can result in conflicts in areas that see a large number of WiFi networks such as apartment

buildings. SSIDs are case sensitive and can consist of a text string of up to 32 characters.

What are the Popular WiFi Encryption Standards?

Depending on the brand and model of wireless router installed on the network, there will be a number of encryption standards available for use on the network. One of the original (and still fairly popular) encryption standards in use is Wired Equivalency Privacy (WEP). The [WEP](#) implementation is fairly user-friendly; however, can be susceptible to dedicated attempts to hack or crack the network password.

The WPA ([WiFi Protected Access](#)) protocol uses the temporarily key integrity protocol (TKIP) to encrypt network traffic and is increasingly becoming the preferred option in wireless network deployments. Focus on WiFi security and finding the balance between usability continues to be an area of ongoing research by the wireless networking working groups in existence today.

Source: <http://www.tech-faq.com/how-does-wireless-networking-work.html>