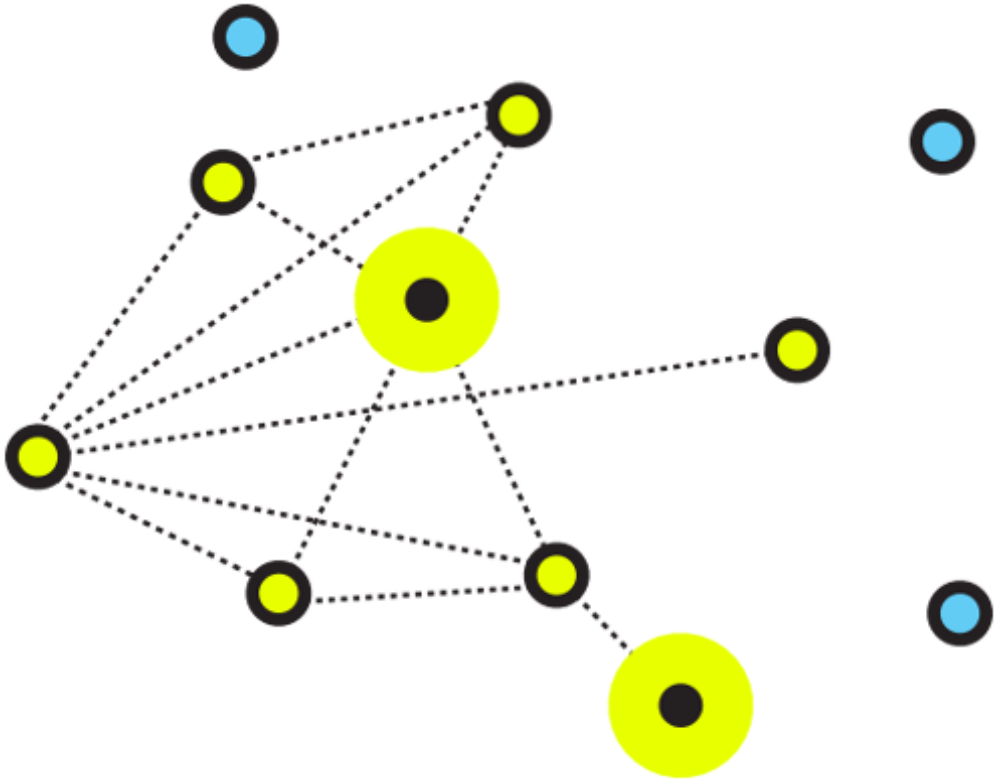
Learn Networking Basics



Introduction

This document covers the basics of how networking works, and how to use different devices to build networks. Computer networking has existed for many years, and as time has passed the technologies have become faster and less expensive. Networks are made up of various devices—computers, switches, routers—connected together by cables or wireless signals. Understanding the basics of how networks are put together is an important step in building a wireless network in a community or neighborhood.

This module covers the concepts of:

1. Clients and servers—how services such as e-mail and web pages connect using networks.
2. IP addresses—how devices on a network can be found.
3. Network hubs, switches and cables—the hardware building blocks of any network.
4. Routers and firewalls—how to organize and control the flow of traffic on a network.

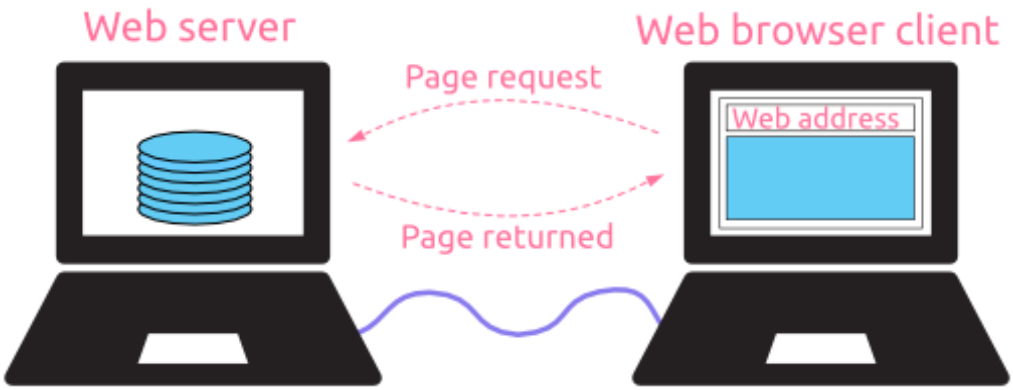
Reading through this material should take between half an hour to an hour. Exploring the activities and details of the subject with a group will take longer.

Clients and Servers

An important relationship on networks is that of the **server** and the **client**. A server is a computer that holds content and services such as a website, a media file, or a chat application. A good example of a server is the computer that holds the website for Google's search page: **http://www.google.com (http://www.google.com)**. The server holds that page, and sends it out when requested.

A client is a different computer, such as your laptop or cell phone, that requests to view, download, or use the content. The client can connect over a network to exchange information. For instance, when you request Google's search page with your web browser, your computer is the client.

In the example below, two computers are connected together with an Ethernet cable. These computers are able to see each other and communicate over the cable. The client computer asks for a website from the server computer. The website is delivered from the server, and displayed on the client's web browser.



Most requests and content delivery on networks are similar to, or are based on, a client to server relationship. On a network, the server can be located almost anywhere, and if the client has the address, it can access the content on the server.

Activity: What is one real world example of a client and server relationship:

```
Client: _________________

Server:_________________
```

Example:
client: radio receiver in your car
server: radio station

IP Addresses

In order to send and direct data across a network, computers need to be able to identify destinations and origins. This identification is an IP—Internet Protocol—address. An **IP address** is just a set of four numbers between 1 and 254, separated by dots. An example of an IP address is **173.194.43.7**.

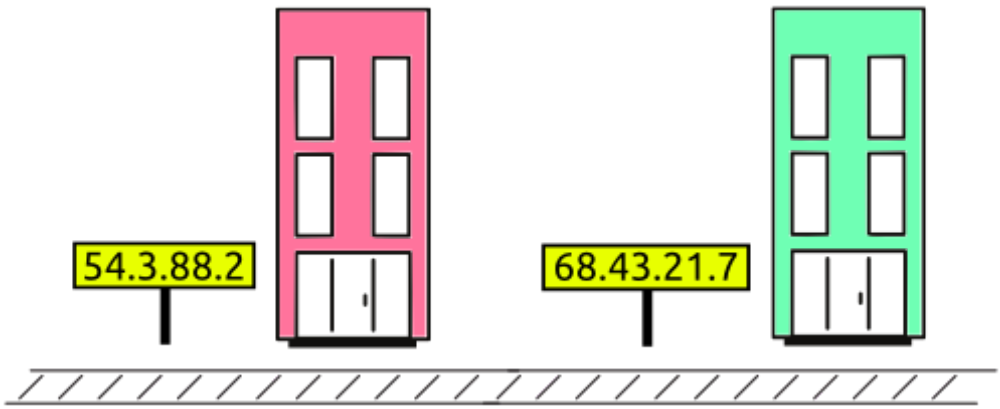
An IP address is similar to a street address. Parts of the address describe where in the world the building is located, another part narrows it down to a state or city, then the area within that state or city, then the location on the street.

Below we can see **192.168.1 Street**. On it are three houses:

The complete addresses for each of these houses is: 192.168.1.**20**, 192.168.1.**21**, and 192.168.1.**22**.

There are different classifications, or types of IP addresses. A network can be public, or it can be private. Public IP addresses are accessible anywhere on the Internet. Private IP addresses are not, and most are typically hidden behind a device with a public IP address.

Here we can see an example—a street with two buildings with **public IP addresses**—representing computers with addresses that are visible to the entire Internet. These buildings might be anywhere in the world, but their addresses are complete, so we know exactly where they are and can send messages to them.



To see an example of how public and private IP addresses are commonly used, let's take another look at **192.168.1 Street**. We have a new building on the street. That building has a public IP address, and a private IP address. There is also a fence that blocks the rest of the Internet from seeing and passing messages to addresses on the street.

The postal building controls messages that travel between the Internet and the street, keeping track of messages that leave the street, and directs return messages to the right house. On the street, it has the address **192.168.1.1**, and on the Internet it has the address **74.10.10.50**.

Activity: Find the IP addresses assigned to your computer, and your network.

```
What is the IP address for your computer? _____________________

Browse to http://ip.mayfirst.org/ (http://ip.mayfirst.org)
and write down the IP address it reports: _____________________
```

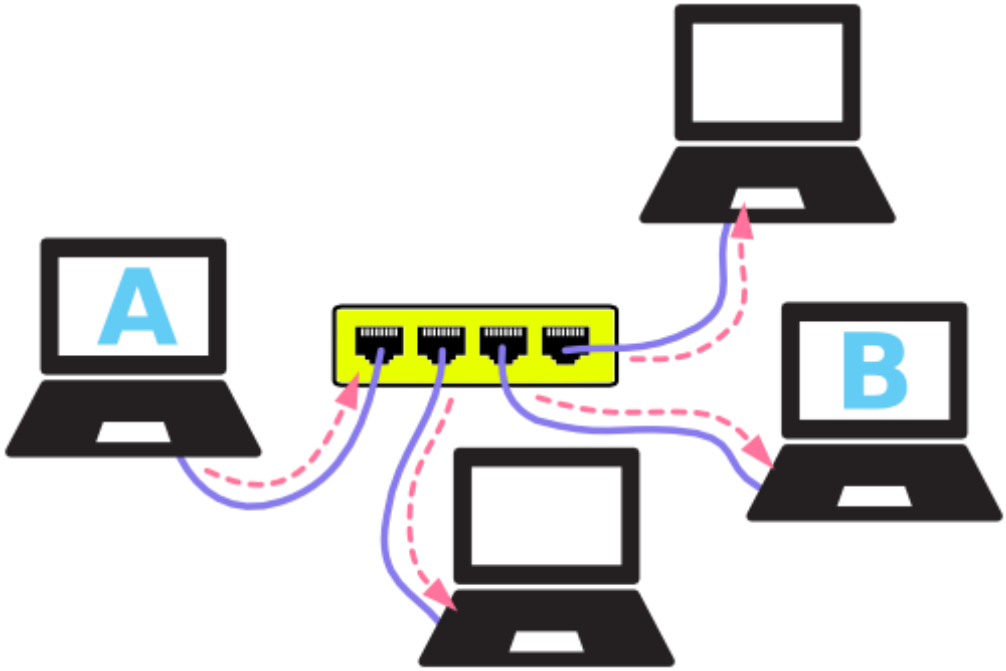
Are these numbers the same, or different? Why?

Network Hubs and Switches

Traditionally, computers are connected to each other using cables—creating a network. The cable used most often is Ethernet, which consists of four pairs of wires inside of a plastic jacket. It is physically similar to phone cables, but can transport much more data.

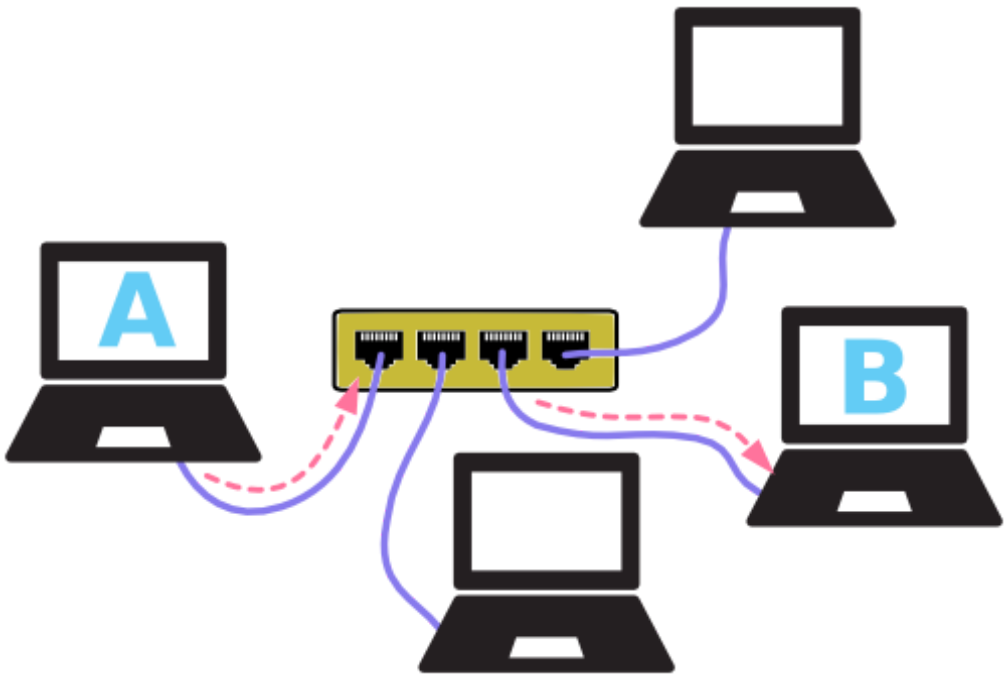
But cables and computers alone do not make a good network, so one early solution was to use a network **hub**. The Ethernet cables from the computer connect to the device similar to the hub of a bike wheel—where all of the spokes come together in the center.

An example of how a hub works is shown below. Computer **A** wants to send a message to computer **B**. It sends the message through the Ethernet cable to the hub, then the hub repeats the message to all of the connected computers.



A network using a hub can slow down if many computers are sending messages, since they may try and send messages at the same time and confuse the hub. To help with this problem, networks began to use another device called a **switch**. Instead of repeating all messages that come in, a switch only sends the message to the intended destination. This eliminates the unnecessary repetition of the hub.

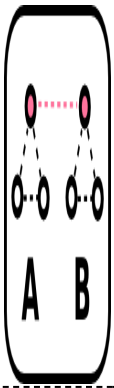
Using a switch, computer **A** sends a message to computer **B**—the other computers do not see the message. Those computers can send other messages at the same time without interfering.



Switches do have a limitation though—they only know about the addresses of equipment that is plugged directly into them. So, you can only send messages to a small number of devices—however many ports the switch has! If you need to send a message to a computer on another network, it will need to be sent through a router, which we discuss next.

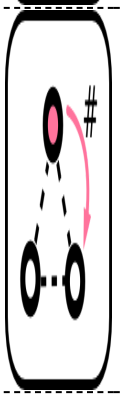
Routers and Firewalls

Routers do the majority of the hard work on a network - they make the decisions about all the messages that travel on the network, and whether to pass messages to and from outside networks. There are three main functions:



Separate and Bridge

Routers separate networks into sections, or bridge different networks together, as we see in the example above—the private network of 192.168.1 Street is bridged to the Internet with a public IP address.



Assign IPs

They can assign IP addresses. In the example of 192.168.1 Street, if a new house is built on the street, it would get whatever the next highest house number available. In the case of routers, they assign IP addresses using DHCP—Dynamic Host Configuration Protocol.

Firewall and Protect

They can filter messages or keep users out of private networks. Most routers have a Firewall built in. This is a software function that keeps unwanted messages from reaching the computers on the inside, or private part, of the network.

Let us take another look at 192.168.1 Street, and the postal service building we included when it had a public address for the entire street. As it turns out, that postal service building is acting as a **Router**.

In this case, the postal service building is routing messages between the rest of the Internet using its public address and the street with private addresses.

Definitions

DHCP—Dynamic Host Configuration Protocol
It assigns IP addresses to client devices, such as desktop computers, laptops, and phones, when they are plugged into Ethernet or connect to Wireless networks.

Ethernet
A type of networking protocol—it defines the types of cables and connections that are used to wire computers, switches, and routers together. Most often Ethernet cabling is Category 5 or 6, made up of twisted pair wiring similar to phone cables.

Hub
A network device that repeats the traffic it receives to all connected devices.

Switch
A network device that sends traffic it receives to a specific connected device, such as a single desktop computer or laptop.

Router
A network device that can bridge between different networks, determine what traffic can pass between them, and perform other functions on a network, such as assigning IP addresses.

Firewall
A function typically performed by routers, this filters traffic between networks and can protect them from interference or attacks.

Related Information

This module is intended to provide some helpful background on networking. We recommend reading the upcoming (but not finished!) Learn about Wireless after this guide.