

## 1.4: Network Basics

### IP Addresses

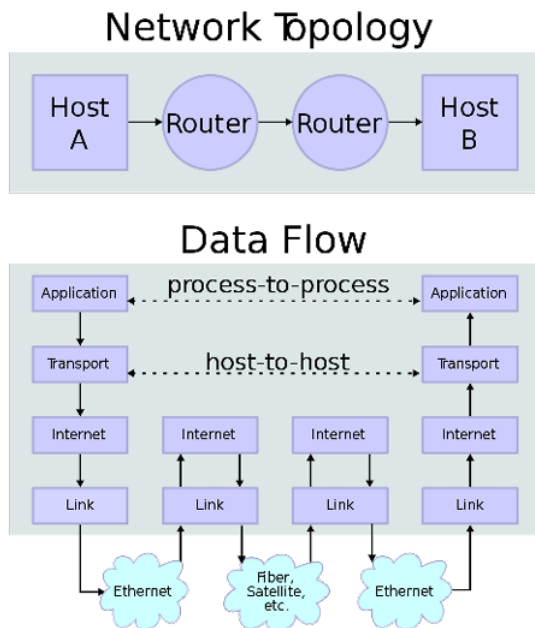


Figure 1.4.1: *Network Topology.* (By User:Kbrose [CC-BY-SA-3.0] via

[Wikimedia](#))

An IP (Internet Protocol) address is a unique code that identifies a piece of equipment connected to a network. These addresses are used in messages between network devices like the network or wireless card in your computer, the equipment from your ISP (internet service provider), and all pieces of equipment between your machine and the one your computer needs to talk to.

IP Addresses live in the network layer, which is one of seven layers in the protocol suite defined in the OSI Model. The OSI model stands for Open Systems Interconnection, and was created by the International Organization for Standardization, an international non-governmental group of professionals who strive to establish standards and best practices in a variety of fields. The OSI Model for networking breaks the system of transmitting data into the layers show below in an attempt to delineate where certain actions should take place.

### 7 Layers of the OSI Model

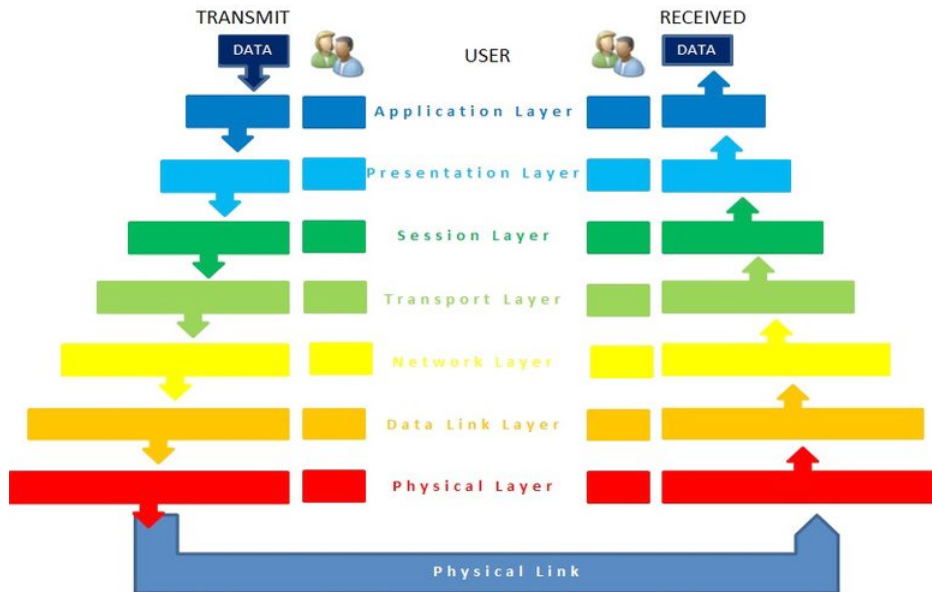


Figure 1.4.2 OSI 7 Layer Model. (By

MrsValdry [CC-BY-SA 3.0] via Wikimedia)

The seven layers depicted above make up the OSI body's recommended protocol suite. In the diagram, transmission of data crosses two routers and over the Internet to reach its destination. By following the data along the arrows, we see it pass through various layers of communication and processing as it crosses the internal network, through the first router, across the public network (internet connection), into the recipient's router, and then is reassembled into its original form.

Until recently, most network equipment has operated on IPv4, the fourth standard released for IP addresses, which has been in place for about thirty years. Addresses in this format are typically represented as a pattern of four blocks of up to three digits separated by periods, with no block of numbers exceeding 255 such as 127.0.0.1 or 24.38.1.251. This is referred to as dot-decimal representation, and although it is not the only way to express an IPv4 address it is the most recognized form. Segments of the addresses within the ranges of 192.168.xxx.xxx, 172.16.xxx.xxx to 172.31.xxx.xxx, and 10.0.xxx.xxx to 10.255.xxx.xxx are reserved for private networks, meaning they are used within a network in your house, at work, or anywhere else where a group of computers share a connection to the internet.

Each of these networks uses one or more of these blocks of numbers for devices on that network. Only the equipment connecting that local network to the Internet needs a unique address from the rest of the world. That equipment will track which computer inside the network to send data to and from by reading packets—the individual pieces of messages that are sent across networks. This means your computer might be 192.168.1.25 at home, and so might your computer at work, according to your home and work networks. The connection between your house and office though still have a different, unique number assigned to them.

This separation of networks was done to reduce the speed at which unique addresses were consumed. Although this scheme allows for almost 4.3 billion (accurately, 2<sup>32</sup>) addresses, the last one was officially assigned on February 4th, 2012. To sustain today's growing number of devices, IPv6 was created, which is depicted as eight blocks of four hexadecimal digits now separated by colons. These new addresses might look like 2001:0db8:85a3:0042:1000:8a2e:0370:7334, and can support roughly 4 billion unique addresses. Since the new range is so staggeringly large, additional protocols were created that specify when certain values or ranges are used in addresses. This allows additional information about the device to be conveyed just from the address.

The actual messages sent between machines are broken down into multiple pieces. These pieces, called packets, are sent piece by piece from sender to recipient. Each packet is sent the fastest way possible, which means some packets may take different routes—picture a short cut, or getting off a congested road to take a different one. This helps to ensure that the message gets from sender to receiver as fast as possible, but also means packets may arrive in a different order than they were sent.

### Additional Notes

Hexadecimal is a number scheme that allows 0 through 9 and A through F as unique values, which means we can count to 15 with one character.

To account for this, each piece of the message, or payload, is wrapped in a header—additional information that describes how many other pieces there are, what protocol is being used, where the packet came from and is headed to, along with some other related information.

## IP version 4 packet

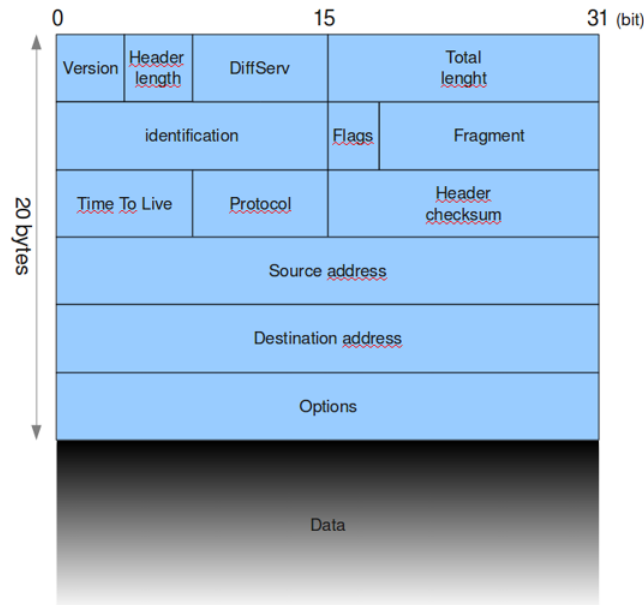


Figure 1.4.3 IP 4 Packet. (Nicolargo [ CC-BY-SA-3.0-2.5-

2.0-1.0] via Wikimedia Commons)

After the packets are reassembled, the receiving computer sends any necessary responses, and the process repeats. This all takes place in fractions of a second, beginning with the “hello,” or handshake packet to announce a communication request, to the last piece of the packet.

## URL

Seeing as most of us would have a hard time remembering what IP address is needed to get to, say, Facebook (173.252.100.16) or the Weather Channel (96.8.80.132) we instead use URLs, universal resource locators. This allows us to use [www.facebook.com](http://www.facebook.com) and [www.weather.com](http://www.weather.com) to get to where we want to go without referring to a long list of IP addresses. Specialized servers (called name servers) all around the world are responsible for responding to requests from computers for this information. When you type [facebook.com](http://facebook.com) into your address bar, if your router does not have a note of its own as to where that is, it will “ask” a name server, which will look it up in its records and reply.

There are three parts to a network address: the protocol, name, and resource id. The protocol represents how we want to send and receive messages, for example we can use <http://> for accessing websites and <ftp://> for moving files. The name is what we associate with the site, like [www.facebook.com](http://www.facebook.com), and the resource id, or URI, is everything after that, which points to the particular file we want to see.

## Ports

While an IP address and a URL will bring you to a particular web server, there may be more than one way you want to interact with it, or more than one thing you want it to do. Maybe you also want the server to provide email services, or you want to use FTP to update your files. These ports act as different doors into your server, so different applications can communicate without getting in each other’s way. Certain ports are typically used for certain activities, for example port 80 is the standard port for web traffic (your browser viewing a page), as opposed to ftp, which typically uses port 21. Using standard ports is not a rule, as applications can be configured to use any available port number, but it is recommended in most cases as firewalls and other security devices may

require additional configuring to keep them from blocking wanted traffic because it is arriving at an unusual, fire walled, or “locked” port.

## Hosting Facilities

If you are using a server that is not under your physical care, and is managed by an off-site third party, then you likely have an agreement with a hosting facility. Hosting facilities are typically for-profit companies that manage the physical equipment necessary to provide access to websites for a number of clients. Many offer web development and management services as well, but if you are still reading, then that tidbit is probably of little interest as you are here to build it yourself.

## Additional Notes

**Up Time** is the average amount of time that all services on a server are operational and accessible to end users. It is a typical measurement of a hosting company’s ability to provide the services they promise.

The benefit of using a hosting service falls under the same principles as other cloud computing services. You are paying to rent equipment and/or services in place of investing in equipment and managing the server and Internet connection yourself. Additionally, hosting facilities are equipped with backup power sources as well as redundant connections to the internet, and may even have multiple facilities that are physically dispersed, ensuring their clients have the best up time as possible. Ads like the one below are common to these services and often emphasize their best features. Price competition makes for relatively affordable hosting for those who are not looking for dedicated servers and are comfortable with sharing their (virtual) server resources with other customers.



## Domain Registrar

Domain registrars coordinate the name servers that turn URLs into the IP addresses that get us to our destinations. These companies are where you register available names in order to allow others to find your site. One of the most recognized registrars right now is GoDaddy—you may know them from their ads, which feature racecar driver Danica Patrick. Like many registrars, GoDaddy also offers other services like web and email hosting as well as web development in an effort to solve all of your website needs.

## Learn more

Keywords, search terms: Networking, network topology, OSI, network architecture

Cisco Networking Example: [http://docwiki.cisco.com/wiki/Internetworking\\_Basics](http://docwiki.cisco.com/wiki/Internetworking_Basics)

List and description of all top level domains: <http://www.icann.org/en/resources/registries/tlds>

Ongoing comparison of hosting providers: <http://www.findmyhosting.com/>

---

1.4: Network Basics is shared under a [not declared](#) license and was authored, remixed, and/or curated by LibreTexts.

- 1.4: Network Basics by Michael Mendez has no license indicated.