**Hardware**

**Router**

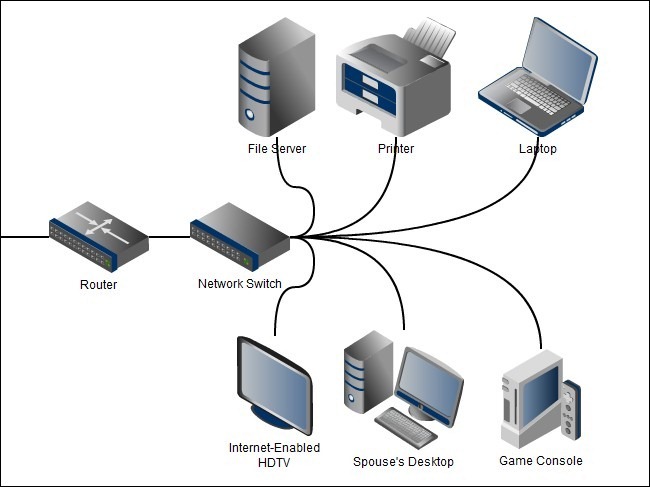
A router is a device that directs network traffic to other networks. Just as a letter has a label with a mailing address and destination address, network packet has a source and destination address, referred to as an IP address. When a post office receives a package, the postmaster read the address, checks their database, and sends it to either: the destination (if they’re in their neighborhood) or the next hop towards it (the next nearest postal code).

Errors may occur when sending network traffic. The destination may be unreachable, not exist, or it’s incorrect. If this happens, the network traffic is discarded. But as long as there are no errors, and the destination is reachable, the network traffic is forwarded until it reaches it’s destination.

**Network Switch**

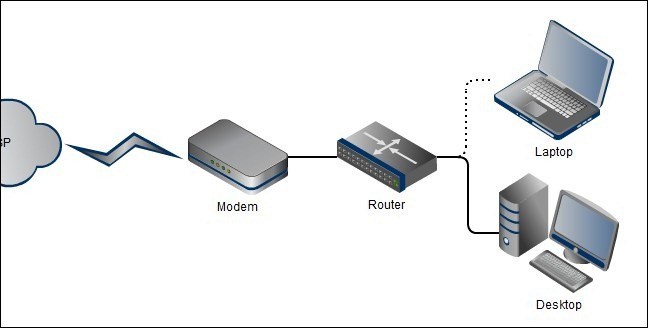
A network switch is like a router, and continuing with our letter analogy, instead of a post master sending letters across the world, a switch is the landlord at the location giving them to the right tenant within a building. Once the postmaster delivers a letter to a building, it’s then the landlord’s responsibility to make sure it reaches the right tenant. Unlike a how a post master (router) uses the address (IP address) the landlord (switch) uses the apartment number (Media Access Control i.e. MAC address) to find out where the letter needs to go.

Though they sound the same in theory, they operate at different levels. While routers are meant to be ‘edge devices’ that can communicate on the world wide web, switches are ‘internal devices’ and meant to operate within networks. In the same way a landlord doesn’t know about every apartment building in the world, so they ask their postmaster to send it for them, and vice versa. Check out the example below for a visual representation of the previous statement.



**Modem**

Modem means modulator-demodulator. Computers communicate using digital ones and zeros. But internet service providers use pre existing infrastructure like phone and cable lines, which are meant to send analog signals. Modems are used to translate from one to another. Relating to our letter analogy, it’s a person that knows read the addresses and says them to a the postmaster. It’s not that the postmaster doesn’t know what to do, it just needs to be told what the address is since it can’t read it, but can listen very well.

Though some modems may be built into some devices, they can be their own discrete component. Below is a diagram explaining this.

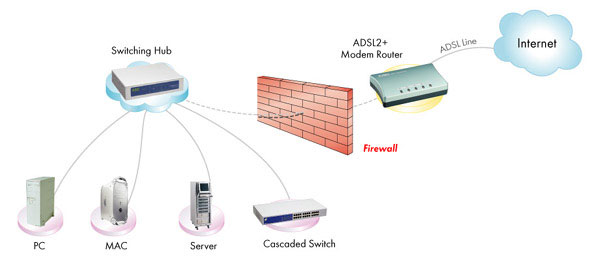
**Firewall**

The same way a security guard prevents unwanted people from entering a building, a firewall prevent unwanted network traffic from reaching a destination. Though it’s not required to be able to use the internet, it provides an extra layer of security to give you peace of mind when browsing the web. There are two common types of firewalls, client based and network based.

A client based firewall would be a passcode door lock, only those you give the code to are able to access your room. An everyday example is Windows Firewall application, and you have to give access to specific programs before they can access your computer or the internet.

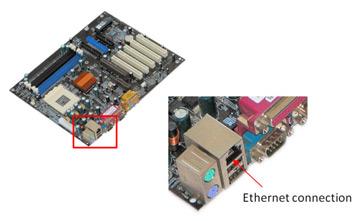
A network based firewall would be a security guard at the entrance to the building. Instead of letting attackers wander around the building and relying on everyone to have good locks, we want to stop them from entering the building at all.

Each have their pros and cons, but having both is best. Because a firewall communicates digitally, it’s placed after a modem, but before a router. Below is a diagram explaining what was stated before

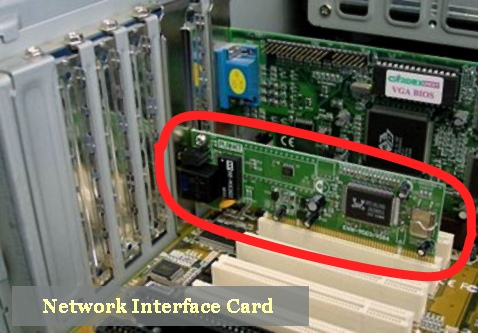


**Network Interface**

A network interface is a piece of hardware that allows a device the ability to communicate across a network in the same way you need a mail or post box to send letter. Most modern computers have one integrated into the motherboard.



It can be an aftermarket component installed as an expansion card

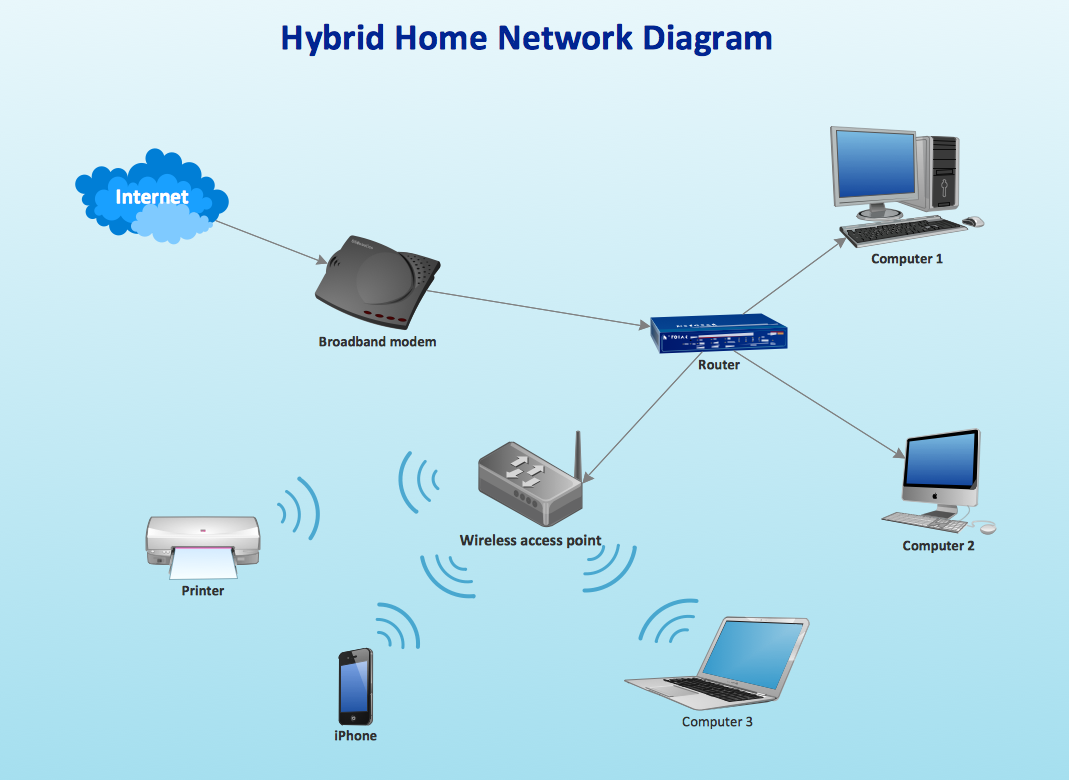
Or it can be directly attached to a circuit board, like in phones and laptops



**Wireless Access Point**

A wireless access point (WAP) is a device that allows devices to connect to a network wirelessly via radio waves. Keeping with our letter theme, this would be the same as throwing a letter to your landlord instead of handing it to them. It’s only wirelss between you two, and they still have to hand it off, i.e. use cables, to send the message.

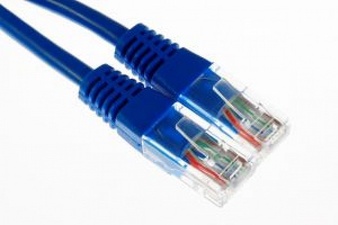
Below is a diagram explaining how this would look



**Ethernet Cable**

A standard Ethernet cable is slightly thicker than a phone cable and has an RJ45 connector on each end. Ethernet ports look similar to telephone jacks, but are slightly wider. Common types are Cat5, Cat5e, Cat6, and Cat7. The biggest difference in categories is their speed and cost. The higher the speed, the higher the cost.

In regards to our analogy, while wireless may be throwing a letter, it can be inconsistent and difficult, a wired connected would be walking and handing it off. Though not as convenient, it’s faster and more reliable.

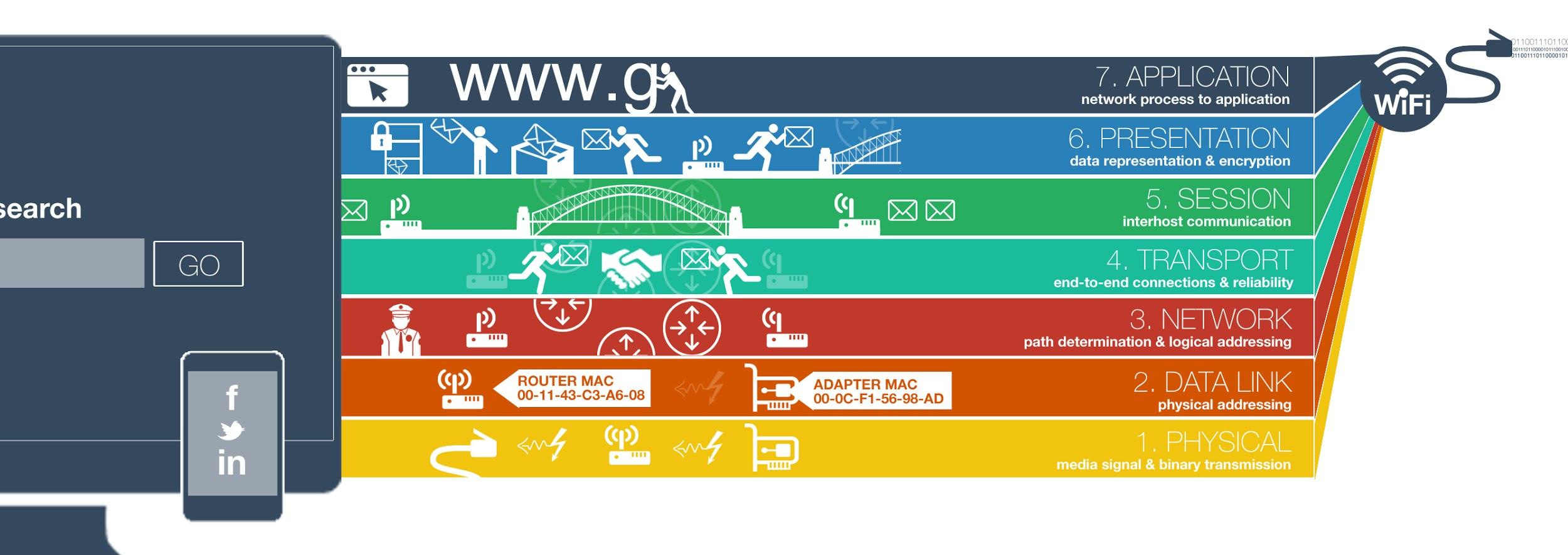


**OSI layer model**

The Open Systems Interconnection model is a conceptual model that standardizes the communication of computing system. Data is transmitted down the stack, from the application, to the operating system, then the network interface, sent on the wire which is received by another network interface, which gives it to the operating system, who give it to the applications.

Back to our analogy, your message is the application data. When you give it to your landlord, he doesn’t see the message, only the street address. When he give it to the postmaster, he doesn’t care about the street address and only reads the zip code. The process is then done in reverse at the destination. Once the recipient is give the letter from their landlord, they can unwrap it and read the message.

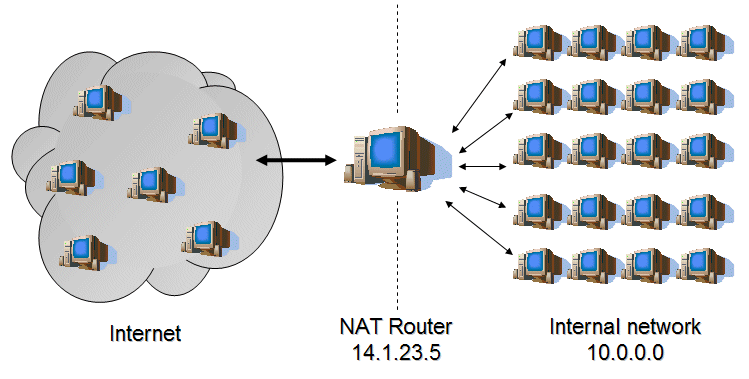
Below is an image explaining the layers in detail, but is out of scope for this discussion.



**Network Address Translation**

Network address translation (NAT) is the ability of having one external address to represent a bunch of internal addresses. Just how not every person in your house doesn’t have their own street address, instead once you get a letter it’s then given to the right person based on who it’s addressed to. This makes it more space efficient to send and receive network traffic to one address instead of worrying about addressing every single person in a household. Just how you can run out of spaces for mail boxes, NAT slowed down the exhaustion of IPv4 addresses. But this is less relevant with IPv6 being it’s replacement.

Below is an image explaining the concept visually.



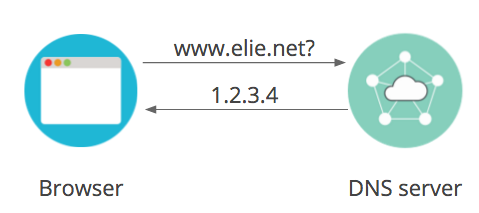
**Internet**

**Domain Name System**

Domain Name System (DNS) is the method that computers use to translate ‘www.google.com’ what humans understand to the right IP address eg. 142.43.85.195 which computers understand. With our analogy, this would be you using your address book to find your friends address information from their name. Remembering addresses is hard, but names are easy.

DNS covers a lot of technologies, but the biggest components are domain name servers, which provide the service, and the specific protocol that they use, which will be explained in detail later.

DNS is recursive in that the same way you’d ask someone else if you didn’t have an address, DNS is the same way in that if one server doesn’t know the address, it’ll ask another till it’s found or reaches the end and isn’t.



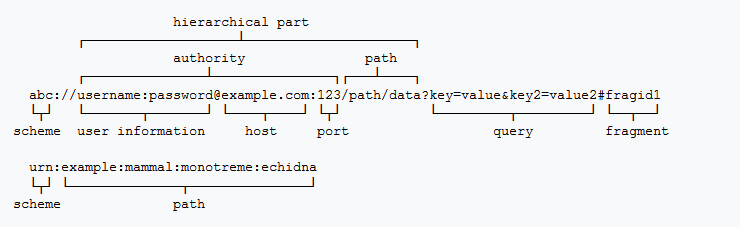
Below is an image showing a basic query and reply.

Top level domains (TLD) like .com, .net, or .gov are maintained by their respective owners and can’t be used by the average person and has to be verified by an authorizing body. But if you wanted to make your own domain call .myhighschoolisawesome, you can and you’d be the authorizing body about who could, and how it’d be used. If you were to make a subdomain, it would still have to be a part of .myhighschoolisawesome, but since it’s a sub set, you’d have to add on with it. An example would be mysubdomain.myhighschoolisawesome. This can be seen with other websites. A major governing body manages .com, and they allow subdomains for google, facebook, and imgur. Then those subdomains are managed by their respective owners.

**URI - Scheme, host port, query, fragment**

Uniform resource indicators (URI) are a string of characters used to identify something else. This allows the use of text to represent other web site locations. The most common type of URI is the uniform resource locator (URL) that almost all websites use. This simplifies web browsing by allowing one site to link to others instead of having to remember every website. When you click on a URL, a lot a things happen behind the scene. They use a specific scheme for how URL should be written that’s standardized to ensure compatibility across the web. There are many parts to what a URL looks like. Since URL are just text, they need to specify a few things to ensure that they’re able to communicate. Instead of trying to explain everything in detail, it’s easier to show with a picture.

Below is a picture showing the URL scheme.

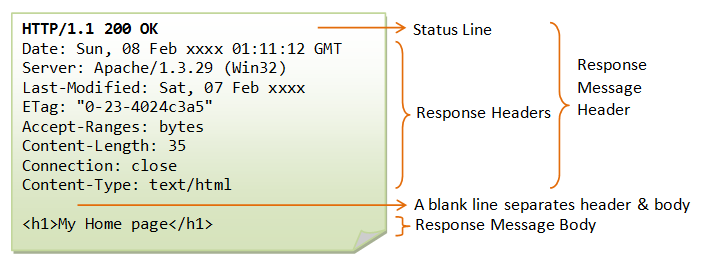
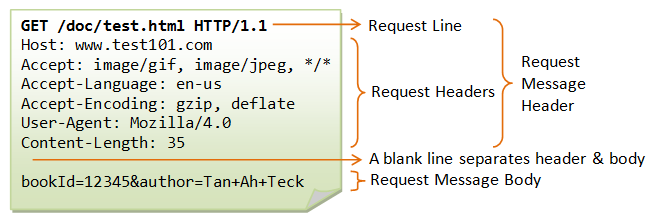
Looking at the picture, it can be seen that there is a lot that goes into simple URL. On the far left, it specifies the scheme (or protocol), then any user information if needed, the host i.e. domain. Then the port number to use, path to the data it’s referencing, and any data that the file will need. Like a database that’s expecting a query, or username and password for a login screen. Finally, there’s a fragment id incase the file asked for is too big to get at once, or if a network is too slow and we need to take out time sending information.

**Website - Server, HTML**

A web server is a computer system that processes requests for information. Servers can be something specific like a game server, or something simple like a web page server. For something to qualify as a website, it has to be hosted via a web server, and accessible using the internet. Websites are coded using the hyper-text markup language (HTML). All web servers basically do is ‘server’ data to ‘clients’. But since raw HTML text isn’t very useful, your web browser renders the text and shows you the intended website instead.

**Browser - HTTP request/response, methods, header, cookies, referer, user-agent**

A web browser is a software application for retrieving, presenting and traversing information resources on the World Wide Web. An information resource is identified by a Uniform Resource Identifier that may be a web page, image, video or other piece of content. Hyperlinks present in resources enable users easily to navigate their browsers to related resources. Clients use web browsers use the HyperText Transfer Protocol (HTTP) to make requests to HTTP servers, and these servers use HTTP to send responses back to the client. It utilizes human readable text called HTTP headers as labels for the information sent and received. There are a large amount of headers, and they unique to either a request or response. There are three request headers that must be noted: cookie, referer, and user-agent. Cookies are key-value pairs stored in the browser, specified by the server using the set-cookie header, and are used to save stateful information on the client such like a session key. Browsers include the cookie header in requests to relay cookies back to the server. There are several types or methods of requests, of which GET and POST are most common. The main difference being that POST includes information sent to the server as a header, and not in the URL, which makes POST requests more secure to use (eg, sending login information using a GET will put the username and password in the URL).



Referring back to the post service example, HTTP could be compared with a book subscription, where the headers are information about the subscription.

Cookies could be equated to a receipt which you can use to verify that you are the subscriber, which persists in the event that you change addresses. The user-agent could be loosely compared to the person sending the subscription request, who must add their name and phone number to subscribe.

**TCP/IP**

**\*IP address - v4, 32-bit, dotted decimal**

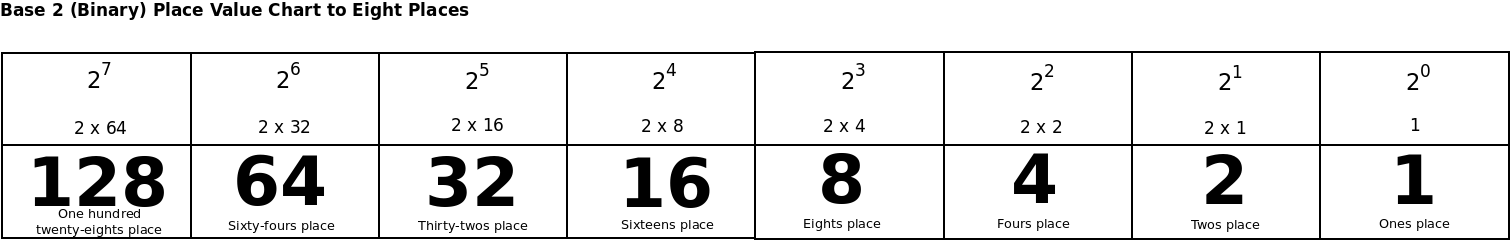
Internet Protocol version 4 (IPv4) is the fourth version of what’s know entirely as the Internet Protocol. A network protocol is a standardized definition on the structure of a packets that are sent over a network, in the same way there’s a standard way to write addresses on mail.

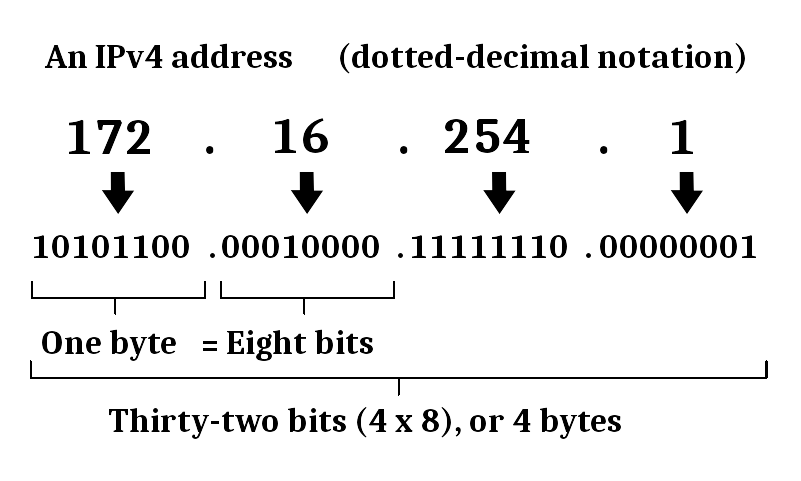
IPv4 is one of the core networking protocols of standards-based internetworking methods in the Internet. IPv4 is connectionless, designed for use on packet-switched networks. It operates on a best effort delivery model, in that it does not guarantee delivery.

In layman’s terms, an IP address is a unique identifier for a specific machine on the network. Just as your house has its own unique mailing address, your home router has its own unique IP address assigned to you by your Internet Service Provider.

IPv4 addresses are represented in whats called ‘dotted-decimal’ notation. Since computers only understand 1s and 0s, we translate the raw binary into something that we can understand. Remember that a single 1 or 0 is a single bit and 8 bits make a byte. Also understand that a 1 represents a certain ‘place’ in a binary number sequence. So ‘101’ in binary would be 5 to us since the ones are in the one and fourths slot.

Below is an image explaining binary and IPv4 addresses

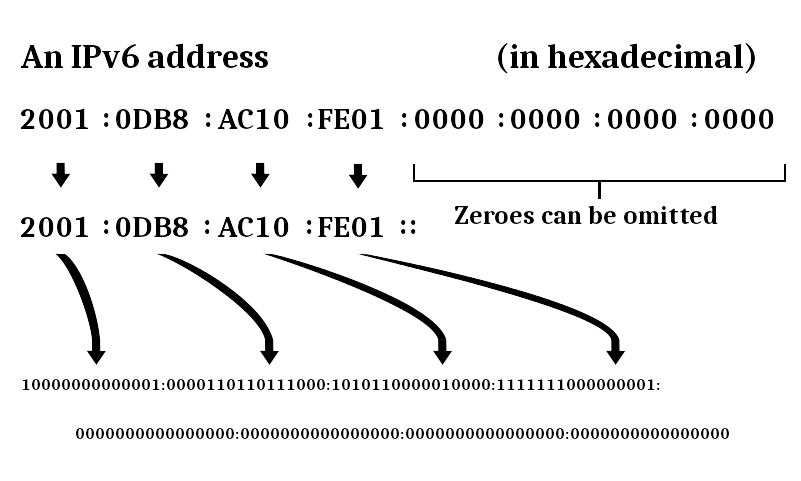


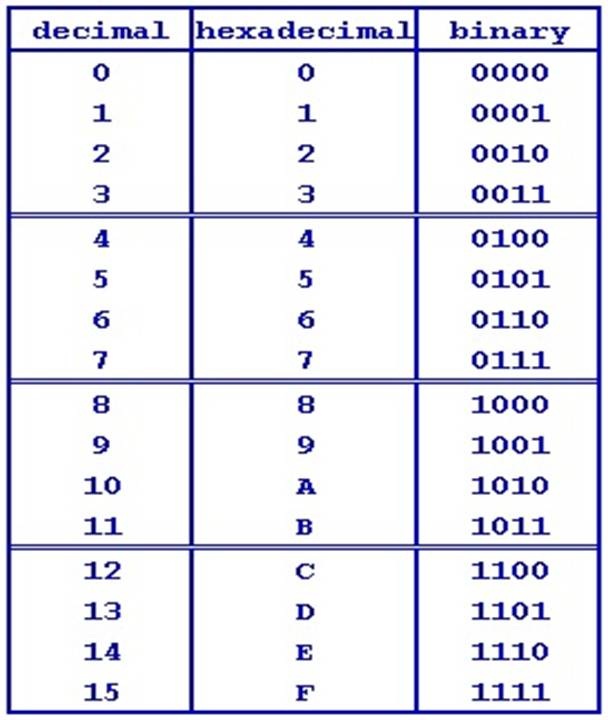


**Address space exhaustion - v6, 128-bit, hex**

Internet Protocol version 6 is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks. It was made to deal with the long-anticipated problem of IPv4 address exhaustion.

Every device on the Internet is assigned a unique IP address for identification and location definition. With the rapid growth of the Internet after commercialization in the 1990s, it became evident that far more addresses would be needed to connect devices than the IPv4 address space had available. Since they need to cram more data into IPv6, they use what’s called hexadecimal to represent the addresses instead of decimal number. But the underlying value is still binary.

In short, IPv6 allows for more addresses for more devices. Below is an image showing a hexadecimal chart, and how an IPv6 address are represented using them.



**Private Networks - 10, 172.16 - 172.31, 192.168**

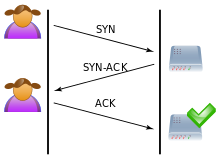
In the Internet addressing architecture, a private network is a network that uses private IP address space. These addresses are commonly used for home, office, and enterprise local area networks. Private IP address spaces were used to in an effort to try to slow down and delay the IPv4 address exhaustion, but they are also a feature of IPv6 where exhaustion is not an issue.

Addresses in the private space are not allocated to any specific organization, however, IP packets addressed from them cannot be transmitted through the public Internet, and so it must do so via a network address translator (NAT) gateway.

**Three way handshake - syn, ack, nak, fin**

A three-way handshake is the basis for all TCP communications and is used to establish a connection between two networked hosts as follows:

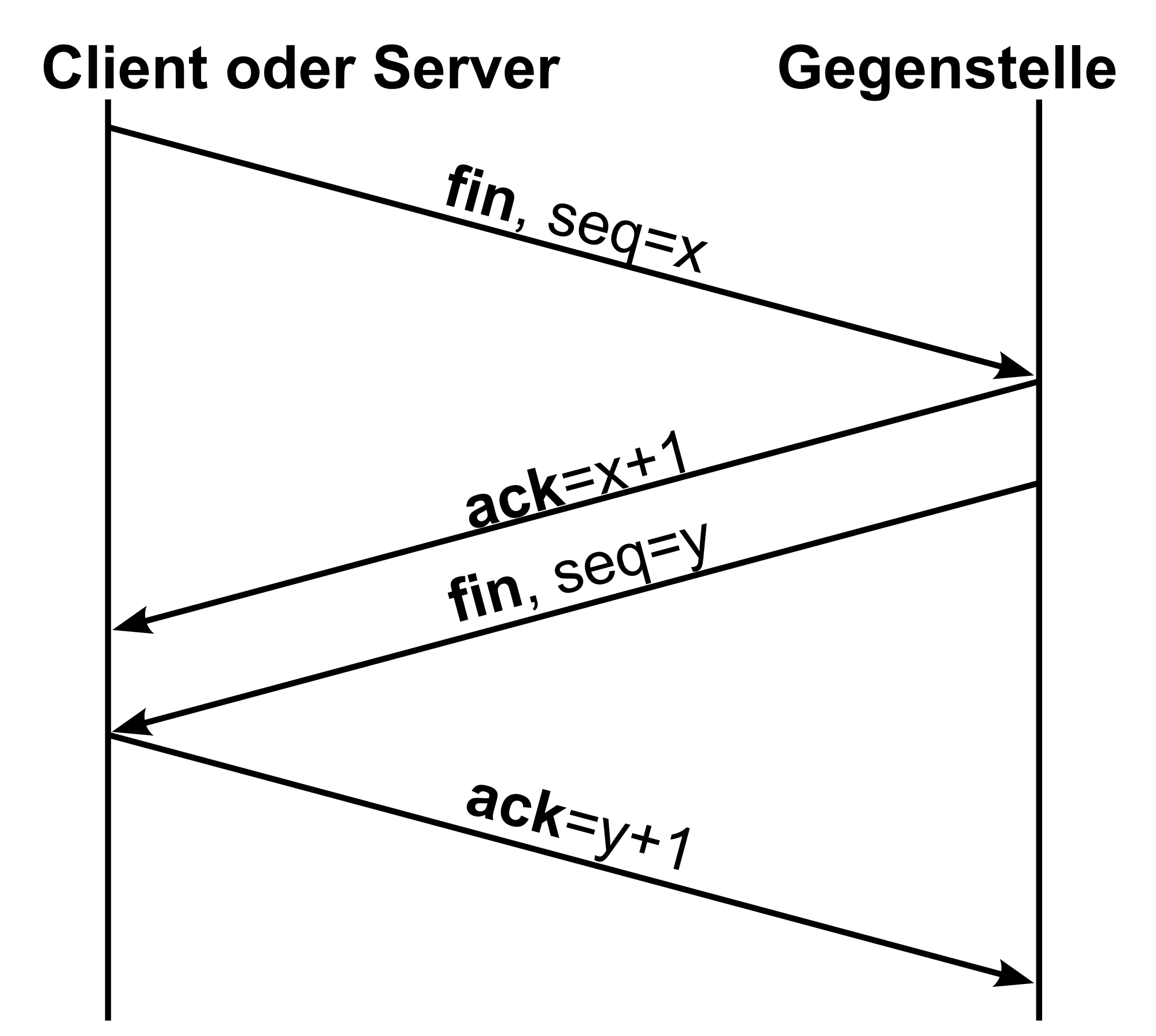
1. Client sends a TCP packet to the server with the SYN flag set.
2. Server responds to the client request with the SYN and ACK flags set.
3. Client completes the connection by sending a packet with the ACK flag set.

Below is a picture showing this visually

In order for the connection to exist, each side of the connection must send a SYN (Synchronize) flag and receive an ACK (Acknowledge) flag. This is required by TCP since it wants to make sure that any data it sends is received properly and in contact.

Just as there’s association steps, TCP also has tear down steps. It’s the same as the handshake, but in reverse and instead of SYN, FIN is used.

Below is a picture showing this visually



**Protocols - Ports (add port numbers)**

**Ports**

A port is an endpoint of communication in an operating system. In software it is a logical construct that identifies a specific process or a type of network service. A port is always associated with an IP address of a host and the protocol type of the communication, and thus completes the destination or origination network address of a communication session.

For example, an address may be "protocol: TCP, IP address: 1.2.3.4, port number: 80", which may be written 1.2.3.4:80 when the protocol is known from context.

Ports can be visualized as a computer version of a mailbox. To send a letter, you must put your letter in the mailbox. When expecting a letter, you frequently check your mailbox. Similarly, a computer uses ports to send and receive packets. Every port on a computer is numbered as 0-65535 allowing a maximum number of ports to be 65536.

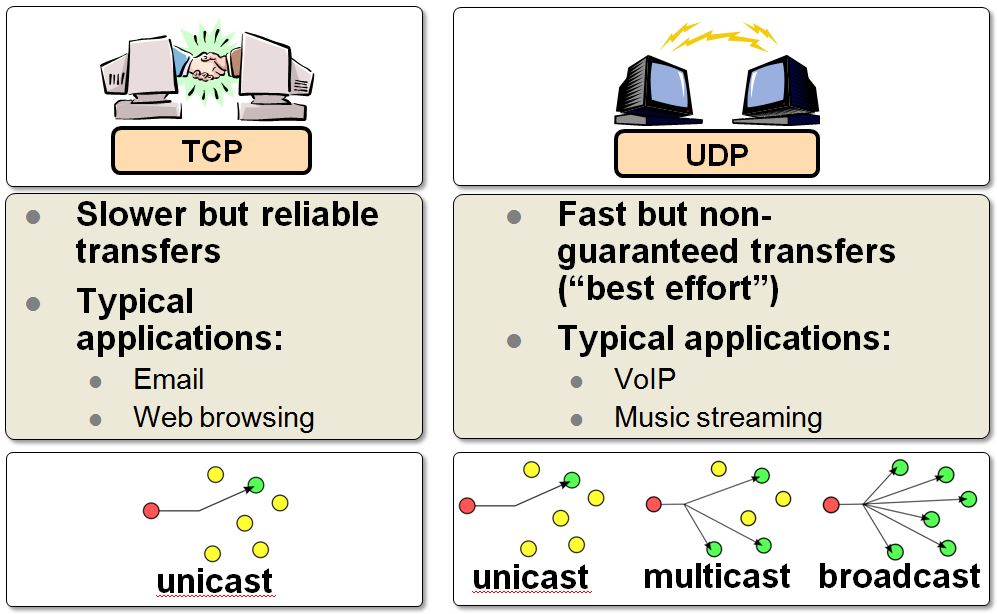
**TCP**

Transmission Control Protocol is one of the main protocols of the Internet protocol suite. Part of the initial network implementation of Internet Protocol (IP), the entire suite is commonly referred to as TCP/IP. TCP provides reliable, ordered, and error-checked delivery of packets between applications running on hosts communicating by an IP network.

**UDP**

User Datagram Protocol is one of the core members of the Internet protocol suite. Prior communication is not required to set up transmission channels or data paths like TCP. It uses a simple connectionless transmission model with a minimum data integrity checking. Time-sensitive applications often use UDP because dropping packets is preferable to waiting for delayed packets, like video games or streaming media.

A simplification of the differences between TCP and UDP can be seen in the picture below



**FTP - 21**

The File Transfer Protocol is a network protocol used to transfer computer files between a client and server on a computer network. It uses a client-server model, and users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it.

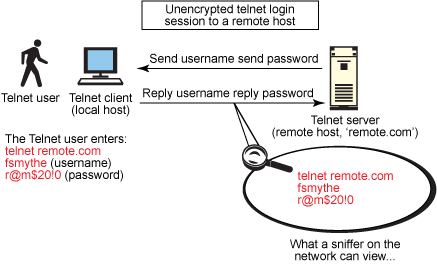
**SSH - 22**

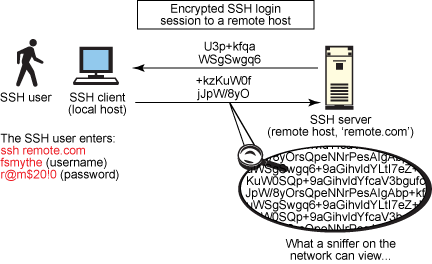
Secure Shell is a cryptographic network protocol for connecting to remote computers securely. It provides a secure channel in a client-server architecture, connecting a client application with a server. Common applications include remote command-line login and remote command execution, but any network service can be secured with SSH.

**Telnet - 23**

Telnet is protocol used on the Internet or local area networks to provide the ability to remotely manage a computer system. The name stands for "teletype network". Historically, Telnet provided access to a command-line interface on a remote host. However, because of serious security concerns when using Telnet over an open network such as the Internet, its use for this purpose has waned significantly in favor of SSH.

The difference between telnet and SSH can be show with the pictures below



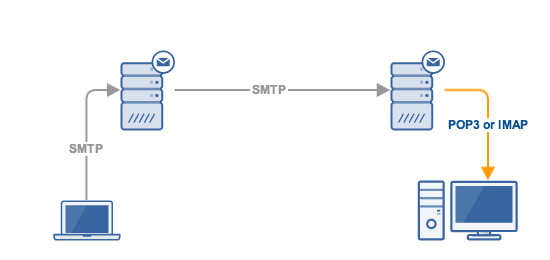


**SMTP - 25**

Simple Mail Transfer Protocol is an Internet standard for electronic mail transmission. Although electronic mail servers and other mail transfer agents use SMTP to send and receive mail messages, user-level client mail applications typically use SMTP only for sending messages to a mail server for relaying. For retrieving messages, client applications usually use either IMAP or POP3. SMTP connections secured by SSL, known as SMTPS.

**POP - 110**

Post Office Protocol is an application-layer Internet standard protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection. POP has been developed through several versions, with version 3 (POP3) being the last standard in common use before largely being made obsolete by the more advanced IMAP as well as webmail.

The difference between POP and SMTP can be explained with the picture below

**HTTP - 80**

The Hypertext Transfer Protocol is an application-layer protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web. Hypertext is structured text that uses logical links between nodes containing text. HTTP is the protocol to exchange or transfer hypertext. HTML (Hypertext Markup Language) is a collection of codes or tags used to create hypertext documents displayed on the World Wide Web, where they can be interpreted by Web browsers.