Self Study Material -1

What is an IP Address?

An IP address, or Internet Protocol address, is a series of numbers that identifies any device on a network. Computers use IP addresses to communicate with each other both over the internet as well as on other networks. Read on to learn how IP addresses work and why it's so important to protect yours with dedicated privacy software.

IP address stands for "Internet Protocol address." The Internet Protocol is a set of rules for communication over the internet, such as sending mail, streaming video, or connecting to a website. **An IP address identifies a network or device on the internet.**

The internet protocols manage the process of assigning each unique device its own IP address. (Internet protocols do other things as well, such as routing internet traffic.) This way, it's easy to see which devices on the internet are sending, requesting, and receiving what information.
IP addresses are like telephone numbers, and they serve the same purpose. When you contact someone, your phone number identifies who you are, and it assures the person who answers the phone that you are who you say you are. IP addresses do the exact same thing when you're online — that's why **every single device that is connected to the internet has an IP address**.

There are two types of IP addresses: IPv4 and IPv6. It's easy to recognize the difference if you count the numbers.

IPv4 addresses contain a series of four numbers, ranging from 0 (except the first one) to 255, each separated from the next by a period — such as 5.62.42.77.

IPv6 addresses are represented as eight groups of four hexadecimal digits, with the groups separated by colons. A typical IPv6 address might look like this: 2620:0aba2:0d01:2042:0100:8c4d:d370:72b4.

The parts of your IP address

An IP address has two parts: the **network ID**, comprising the first three numbers of the address, and a **host ID**, the fourth number in the address. So on your home network — 192.168.1.1, for example – 192.168.1 is the network ID, and the final number is the host ID.
The Network ID indicates which network the device is on. The Host ID refers to the specific device on that network. (Usually your router is .1, and each subsequent device gets assigned .2, .3, and so on.)

You may not always want the outside world to know exactly which device and network you're using. In this case, it's possible to mask your IP address from the outside world through a Virtual Private Network (VPN). When you use a VPN, it prevents your network from revealing your address.

Where do IP addresses come from?

IPv4 dates back to the early 1980s, when the internet was a private network for the military. IPv4 has a total pool of 4.3 billion addresses, which sounds like a lot. But with all the computers, smartphones, and tablets that connect to the internet, not to mention IoT devices, we have run out of IPv4 addresses. In fact, we began running out in the 1990s. Very clever technical networking tricks have kept things going.

The Internet Engineering Task Force (IETF), which designs the backbone technologies of the internet, came up with IPv6 about a decade ago. It has a potential pool of 340 undecillion addresses — that's the number 340 followed by 36 zeroes — meaning we can (in theory) never run out of addresses. It is slowly replacing IPv4, but for now, the two co-exist.

Public vs. local IP addresses

There are two types of IP addresses: external, or public IP addresses; and internal, also called local or private addresses. Your internet service provider (ISP) gives you your external address. When you surf the web, the site you're visiting needs to know who you are (for traffic-monitoring reasons). Your ISP uses your external IP address to introduce you to the website and establish the connection.

You have a different IP address for internal purposes, such as identifying your devices within a home network or inside a business office. The local or internal IP address is assigned to your computer by the router, which is the hardware that connects a local network to the internet. In most cases, that internal IP address is assigned automatically by the router (or cable modem).

Here's what matters: In most cases, you'll have a different IP address internally than you do on the public internet. Your local IP address represents your device on its network, and your public IP address is the face of your network to the greater internet.

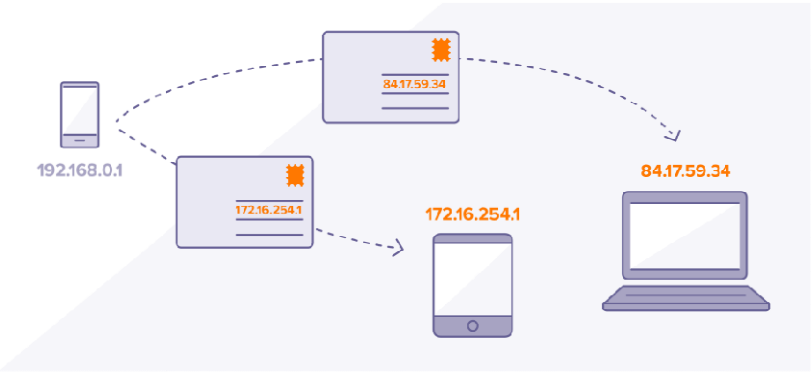
How do IP addresses work?

The post office uses your physical address as a marker for the real-world location of a person, residence, or business. It's how mail is routed. It's where you reside. It's how others know where to find you.

All of these descriptions apply to an IP address, in a digital way. An IP address is where a computer resides, in a virtual sense. IP addresses may identify your own computer, a favorite website, a network server, or even a device (such as a webcam).

IP addresses are especially important for sending and receiving information. They route internet traffic where it needs to go, and they direct emails to your inbox.

The important thing to remember is this: **Every active device on the internet has an IP address.**



First, TCP/IP...

IP addresses are only one part of the internet's architecture. After all, having a postal address for your house is meaningless unless there's a post office responsible for delivering the mail. In internet terms, IP is one part of TCP/IP.

The Transmission Control Protocol/Internet Protocol (TCP/IP) is a set of rules and procedures for connecting devices across the internet. TCP/IP specifies how data is exchanged: **Data is broken down into packets and passed along a chain of routers from origin to destination.** This is the basis for all internet communication.

TCP defines how applications communicate across the network. It manages how a message is broken down into a series of smaller packets, which are then transmitted over the internet and reassembled in the right order at the destination address.

The IP portion of the protocol directs each packet to the right destination. Each gateway computer on the network checks this IP address to determine where to forward the message.

How IP addresses are assigned: dynamic vs. static

IP addresses can be permanent (static) or temporary (dynamic). The difference between static and dynamic IP addresses is that while the former never change, the latter can and do.

Static addresses are mostly used by businesses, since their websites and web applications must be reliably accessible at all times. But your home IP address doesn't have to stay the same, since it's only needed when you're using the internet.

Your ISP will usually give you a dynamic IP address. While your IP address may not change often, it's possible to receive a new one from your ISP every time you reboot your computer. The same holds true with the local IP addresses your home wireless router assigns to your laptop, tablet, or smartphone. These devices might get a new address every time you restart your router.

The only real negative with dynamic addresses is that a given computer can't be reliably found. That makes it difficult to, say, run a web server in your home, as the address might change and no one would be able to find you. Many ISPs allow you to make arrangements for a business connection with a static address if you want to run a server.

A packet's journey

Every time you visit a website, your trip is routed through a complex and hidden series of hops through major traffic backbones. It's akin to an integrated highway system. A visit to a website might involve a dozen hops, all of which take place near-instantaneously and behind the scenes.

Whether you're sending an email, loading a webpage or watching a video, **all data sent over the internet is broken up into packets**. Think of it like a bucket brigade, where buckets of water are passed down a line of people.

Best of all, you usually don't need to know how it works. One of the coolest things about the internet's design is that it keeps this structure wholly invisible to ordinary users. This way, you're free to focus on what you need to do, without worrying about how it gets done.

Each packet has a maximum size of 1,500 bytes and includes a wrapper with a header and a footer. The information in the wrapper communicates the type of data in the packet, where it came from, where it's going, and how it fits together with other packets.

As packets travel, they move in a stream, but all the packets don't always take the exact same path. If there is congestion across the internet, various packets from the same message might travel across different network backbones. As the packets arrive, the receiving computer reassembles the packets into the original (and final) data.

That's one reason that IP addresses are so important. Because every packet includes the IP address for its origin and destination, the internet can make sure that all packets reach the right destination.

DNS servers

The Domain Name System (DNS) makes the modern internet possible. The DNS pairs website names you can easily remember with IP addresses that computers can use.

IPv4 addresses are every bit as valid as a website's alphabetical name. You can type **157.240.22.35** into your web browser, and it'll take you to Facebook. But who's going to remember that? Most of us barely remember our own phone numbers.

Familiar domain names are substitutes for real IP addresses. In the early days of the internet, you could connect to another site only by typing in the numbers of its IP address. But thanks to the DNS, we don't need to do this anymore.

The DNS freed us from the headache of remembering IP addresses by giving each site a name. DNS servers sit between your browser and the site you want to visit. When you type a URL into your browser, your browser looks up that domain name in the DNS server, retrieves the corresponding IP address, and sends you to the site you want. All without you, the user, needing to do a thing.

What is the purpose of an IP address?

The purpose of an IP address is to handle the connection between devices that send and receive information across a network. The IP address uniquely identifies every device on the internet; without one, there's no way to contact them. IP addresses allow computing devices (such as PCs and tablets) to communicate with destinations like websites and streaming services, and they let websites know who is connecting.

An IP address also acts like a return address on postal mail. When a letter you've mailed is delivered to the wrong address, you get the letter back if you include a return address on the envelope.

The same holds true for email. When you write to an invalid recipient (such as someone who left their job and no longer has a company email address) your IP address lets the company's mail server send you back a bounce message so that you know your email wasn't sent to the right place.

IP addresses and geolocation

In addition to making sure other computers on the internet can communicate with yours, IP addresses also mark the real-world location of your device. This comes in handy when a website wants to customize itself to suit your needs — such as by automatically changing its language, or showing you products that are available in your country. Streaming platforms can also use your IP address to show you the content that they're allowed to provide you based on where you live.

While your IP address won't give away your precise location, it *can* get pretty close. Your IP address can be used to identify your city, postal code, internet service provider (ISP), and latitude and longitude. **Since you may not want everyone in the world knowing roughly where you are, consider hiding your IP address with a VPN.**

Rather than broadcasting your real IP address to the world, a VPN, masks your IP address behind another one. This way, anyone else on the internet will only see your VPN's IP address, while yours remains protected.

Public vs. Private IP Addresses: What's the Difference?

Public and private IP addresses are two crucial parts of your device's identity that most people rarely think about. But with a huge increase in employees working from home, and cybercrime on the rise, it's more important than ever to understand how your device's IP address can reveal your identity on the internet.

What is a public IP address?

A *public* IP address is an IP address that can be accessed directly over the internet and is assigned to your network router by your internet service provider (ISP). Your personal device also has a *private* IP that remains hidden when you connect to the internet through your router's public IP.

Using a public IP address to connect to the internet is like using a P.O. box for your snail mail, rather than giving out your home address.

How does a public IP address differ from an external IP address?

The terms *public IP address* and *external IP address* are essentially interchangeable. No matter which phrasing you prefer, the function is the same: **a public (or external) IP address helps you connect to the internet from inside your network, to outside your network**.

Are public IP addresses traceable?

Yes. Public IP addresses can be traced back to your ISP, which can potentially reveal your general geographical location. When advertisers, governments, or hackers know where you're connecting from, it's easier for them to follow what you do online.

Websites also use IP tracking to analyze online behavior patterns, making it easier for them to determine if the same individual visits the site repeatedly. Websites can then use these patterns to predict your preferences.

To browse the internet more anonymously, you can hide your IP address by connecting through a security protocol: a proxy server, a VPN, or the Tor browser. You can also try your luck with private browsers, but most of them don't provide the kind of disguise your IP address needs. These days, the quickest way to ensure your IP address is safely hidden online is to connect with a VPN.

What is a private IP address?

A private IP address is the address your network router assigns to your device. **Each device within the same network is assigned a unique private IP address** (sometimes called a private network address) — this is how devices on the same internal network talk to each other.

Private IP addresses let devices connected to the same network communicate with one another without connecting to the entire internet. By making it more difficult for an external host or user to establish a connection, **private IPs help bolster security within a specific network**, like in your home or office. This is why you can print documents via wireless connection to your printer at home, but your neighbor can't send their files to your printer accidentally.

Local IP addresses are also how your router directs internet traffic internally — in other words, how your router returns search results to *your computer* rather than another device connected to your network (like your phone or your partner's phone).

Private vs. local vs. internal IP addresses

Similar to how *public IP address* and *external IP address* are interchangeable terms, *private IP address* and *internal IP address* are interchangeable terms as well. A private IP address is also often called a *local IP address* — it's up to you which term you use.

Are private IP addresses traceable?

Yes, private IP addresses are traceable, but only by other devices on your local network. Each device connected to your local network has a private IP address, and each device's private IP address can be seen only by other devices within that network. But unlike the public IP address that your router uses to connect your device to the internet, **your private IP address cannot be seen online**.

Key differences between public and private IP addresses

The main difference between public and private IP addresses is how far they reach, and what they're connected to. A **public IP address** identifies you to the wider internet so that all the information you're searching for can find you. A **private IP address** is used within a private network to connect securely to other devices within that same network.

Each device within the same network has a unique private IP address.

Public and private IP address ranges

Your private IP address exists within specific private IP address ranges reserved by the Internet Assigned Numbers Authority (IANA) and should never appear on the internet. There are millions of private networks across the globe, all of which include devices assigned private IP addresses within these ranges:

- Class A: 10.0.0.0 — 10.255.255.255
- Class B: 172.16.0.0 — 172.31.255.255
- Class C: 192.168.0.0 — 192.168.255.255

These might not seem like wide ranges, but they don't really need to be. Because these IP addresses are reserved for private network use only, they can be **reused on different private networks** all over the world — without consequence or confusion.

And don't be surprised if you have a device or two at home with a so-called 192 IP address, or a private IP address beginning with **192.168**. This is the most common default private IP address format assigned to network routers around the globe.

Unsurprisingly, the public IP address range encompasses every number *not* reserved for the private IP range. Since a public IP address is a unique identifier for each device connected to the internet, it needs to be just that: unique.

Summarizing the differences between private and public IP addresses

Public IP address	**Private IP address**
External (global) reach Scope is global.	Internal (local) reach Scope is local
Used for communicating outside your private network, over the internet It is used to communicate outside the network.	Used for communicating within your private network, with other devices in your home or office It is used to communicate within the network.
A unique numeric code never reused by other devices	A non-unique numeric code that may be reused by other devices in other private networks
Found by Googling: "What is my IP address?"	Found via your device's internal settings Private IP can be known by entering "ipconfig" on command prompt.

Assigned and controlled by your internet service provider	Assigned to your specific device within a private network
Not free	Free
Any number not included in the reserved private IP address range Example: 8.8.8.8.	10.0.0.0 — 10.255.255.255; 172.16.0.0 — 172.31.255.255; 192.168.0.0 — 192.168.255.255 Example: 10.11.12.13

How can I check which type of IP address I'm using?

When you connect to the internet, your private IP address is replaced with your ISP-assigned public IP address. This protects your private IP and other devices in your network, while also ensuring you can still connect online. Both types of IP addresses are important for your device's connection to the outside world — but how do you find them?

The easiest way to find your public IP address is to Google: "What is my IP address?" Depending on your ISP, you might see both an IPv4 and IPv6 address listed due to the increasing use of IPv6 addresses over IPv4. You can find your private IP address on Windows or macOS with a few quick clicks.

As you learn about private and public IP addresses, remember that they may change. If your ISP assigns you a dynamic IP address vs. a static IP address, for example, you might be subject to more network outages or connectivity issues in the long run.

And if you need to use a VPN to connect to the internet, your public IP address will change each time you connect — each new connection is encrypted to hide your IP address and keep prying eyes away.

Network address translation (NAT)

To access Internet, one public IP address is needed but as you use private IP address in our private network, translation of private IP address to a public IP address is required.

Network Address Translation (NAT) is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts. Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to destination. It then makes the corresponding entries of ip address and port number in the NAT table. NAT generally operates on router or firewall.

Network Address Translation (NAT) working –

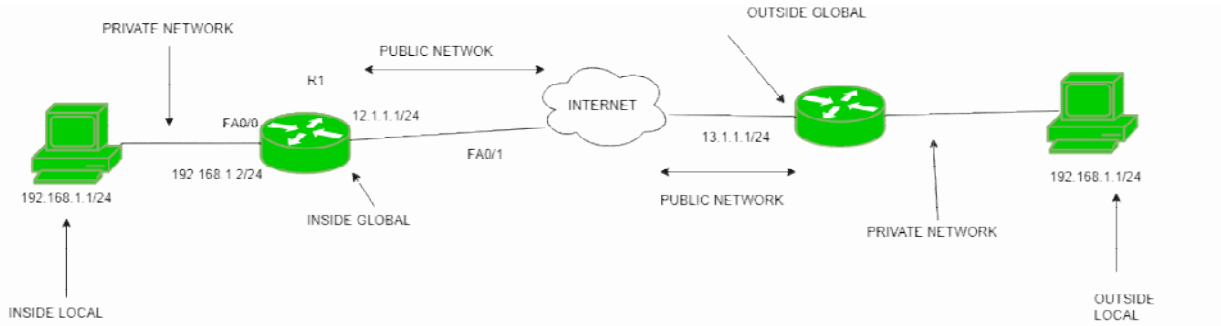
Generally, the border router is configured for NAT i.e the router which have one interface in local (inside) network and one interface in global (outside) network. When a packet traverse outside the local (inside) network, then NAT converts that local (private) IP address to a global (public) IP address. When a packet enters the local network, the global (public) IP address is converted to local (private) IP address.
If NAT run out of addresses, i.e., no address is left in the pool configured then the packets will be dropped and an Internet Control Message Protocol (ICMP) host unreachable packet to the destination is send.

Why mask port numbers?

Suppose, in a network, two hosts A and B are connected. Now, both of them request for the same destination, on the same port number, say 1000, on host side, at the same time. If NAT does only translation of ip addresses, then when their packets will arrive at the NAT, both of their IP addresses would be masked by the public IP address of the network and sent to the destination. Destination will send replies on the public ip address of the router. Thus, on receiving reply, it will be unclear to NAT as to which reply belongs to which host (because source port numbers for both A and B are same). Hence, to avoid such a problem, NAT masks the source port number as well and makes an entry in the NAT table.

NAT inside and outside addresses –

Inside refers to the addresses which must be translated. Outside refers to the addresses which are not in control of an organization. These are the network Addresses in which the translation of the addresses will be done.



- **Inside local address –** An IP address that is assigned to a host on the Inside (local) network. The address is probably not a IP address assigned by the service provider i.e., these are private IP address. This is the inside host seen from the inside network.
- **Inside global address –** IP address that represents one or more inside local IP addresses to the outside world. This is the inside host as seen from the outside network.
- **Outside local address –** This is the actual IP address of the destination host in the local network after translation.
- **Outside global address –** This is the outside host as seen form the outside network. It is the IP address of the outside destination host before translation.

Network Address Translation (NAT) Types –

There are 3 ways to configure NAT:

1. **Static NAT –** In this, a single unregistered (Private) IP address is mapped with a legally registered (Public) IP address i.e one-to-one mapping between local and global address. This is generally used for Web hosting. These are not used in organisations as there are many devices who will need Internet access and to provide Internet access, public IP address is needed.

   Suppose, if there are 3000 devices who needs access to Internet, the organisation have to buy 3000 public addresses that will be very costly.
2. **Dynamic NAT –** In this type of NAT, an unregistered IP address is translated into a registered (Public) IP address from a pool of public IP address. If the IP address of pool are not free, then the packet will be dropped as only fixed number of private IP address can be translated to public addresses.

   Suppose, if there is pool of 2 public IP addresses then only 2 private IP addresses can be translated at a given time. If 3rd private IP address wants to access Internet then the packet will be dropped therefore many private IP addresses are mapped to a pool of public IP addresses. NAT is used when the number of users who wants to access the Internet are fixed. This is also very costly as the organisation have to buy many global IP addresses to make a pool.
3. **Port Address Translation (PAT) –** This is also known as NAT overload. In this, many local (private) IP addresses can be translated to single registered IP address .Port numbers are used to distinguish the traffic i.e., which traffic belongs to which IP address. This is most frequently used

as it is cost effective as thousands of users can be connected to the Internet by using only one real global (public) IP address.

Advantages of NAT –

- NAT conserves legally registered IP addresses .
- It provides privacy as the device IP address, sending and receiving the traffic, will be hidden.
- Eliminates address renumbering when a network evolves.

Disadvantage of NAT –

- Translation results in switching path delays.
- Certain applications will not function while NAT is enabled.
- Complicates tunneling protocols such as IPsec.
- Also, router being a network layer device, should not tamper with port numbers(transport layer) but it has to do so because of NAT.

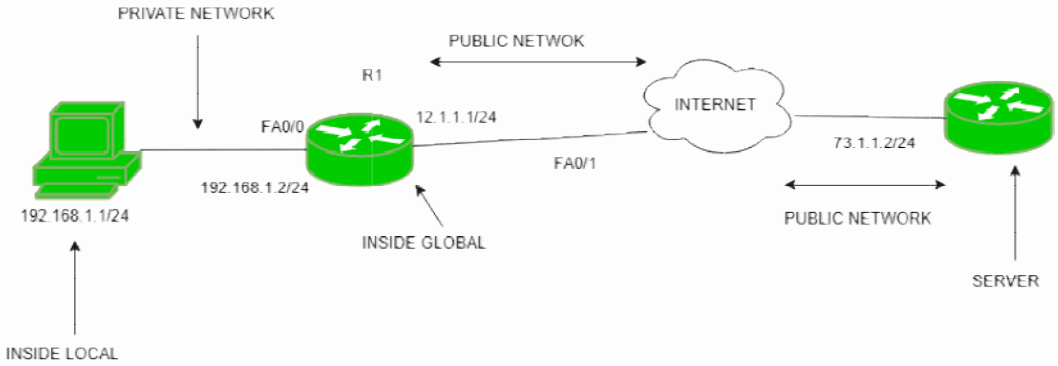
Network address translation (NAT) working –

Generally, the border router is configured for NAT i.e the router which have one interface in local (inside) network and one interface in global (outside) network. When a packet traverse outside the local (inside) network, then NAT converts that local (private) IP address to a global (public) IP address. When a packet enters the local network, the global (public) IP address is converted to local (private) IP address.
If NAT run out of addresses, i.e., no address is left in the pool configured then the packets will be dropped and an Internet Control Message Protocol (ICMP) host unreachable packet to the destination is send.

NAT types –
There are 3 types of NAT:

1. Static NAT –
In this, a single private IP address is mapped with single Public IP address, i.e., a private IP address is translated to a public IP address. It is used in Web hosting.

Configuration –



Here is a small topology in which there is PC having IP address 192.168.1.1/24, Router R1 having IP address 192.168.1.2/24 on interface fa0/0, 12.1.1.1/24 on fa0/1 and server having IP address 73.1.1.2/24.

Now, inside local and inside global are shown in the figure. Configuring the static NAT through command ip nat inside source static INSIDE_LOCAL_IP_ADDRESS INSIDE_GLOBAL_IP_ADDRESS.

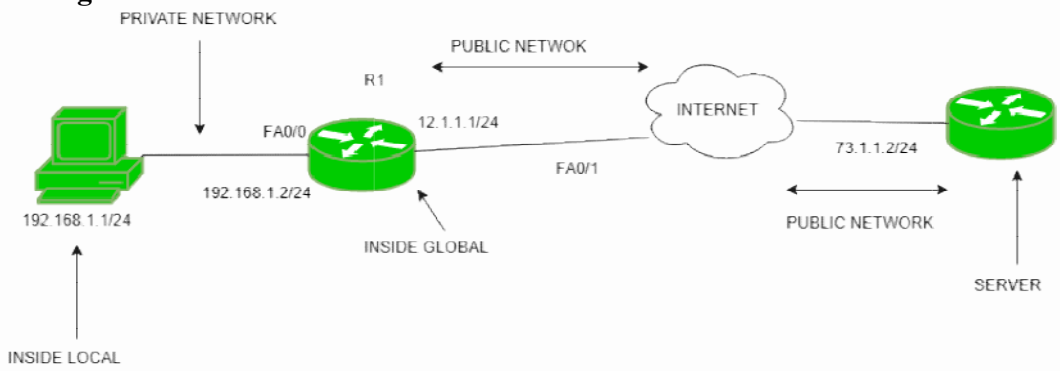
```
R1(config)# ip nat inside source static 192.168.1.1 12.1.1.1
```

Now, we have configure router's inside interface as IP NAT inside and outside interface as IP NAT outside.

```
R1(config)# int fa0/0
R1(config-if)# ip nat inside
R1(config)# int fa0/1
R1(config-if)# ip nat outside
```

2. Dynamic NAT –
In this type of NAT, multiple private IP address are mapped to a pool of public IP address . It is used when we know the number of fixed users wants to access the Internet at a given point of time.

Configuration –



There is PC having IP address 192.168.1.1/24, Router R1 having IP address 192.168.1.2/24 on interface fa0/0, 12.1.1.1/24 on fa0/1 and server having IP address 73.1.1.2/24. Now, first configuring the access-list:

```
R1(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

Configuring the nat pool from which a public IP will be selected.

```
R1(config)# ip nat pool pool1 12.1.1.1 12.1.1.3 netmask 255.255.255.0
```

Now, enabling Dynamic NAT:

```
R1(config)# ip nat inside source list 1 pool pool1
```

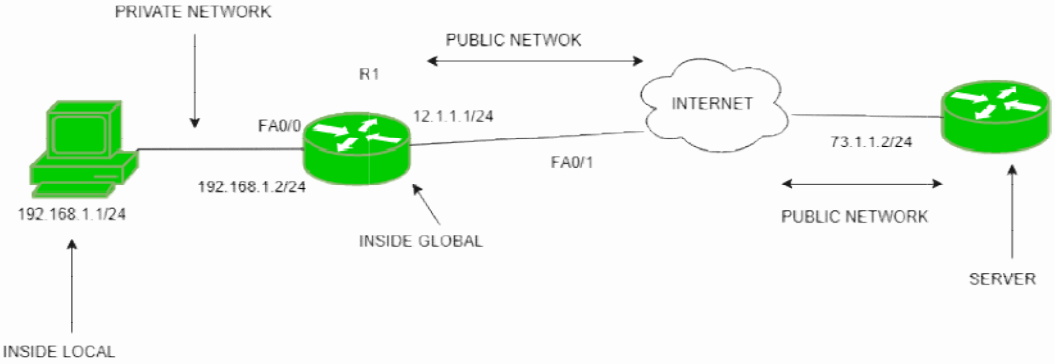
At last, we have to configure router interfaces as inside or outside.

```
R1(config)# int fa0/0
R1(config-if)# ip nat inside
R1(config)# int fa0/1
R1(config-if)# ip nat outside
```

3. Port Address Translation (PAT) –

This is also known as NAT overload. In this, many local (private) IP addresses can be translated to single public IP address. Port numbers are used to distinguish the traffic, i.e., which traffic belongs to which IP address. This is most frequently used as it is cost effective as thousands of users can be connected to the Internet by using only one real global (public) IP address.

Configuration –



Taking the same topology, There is PC1 having IP address 192.168.1.1/24, Router R1 having IP address 192.168.1.2/24 on interface fa0/0, 12.1.1.1/24 on fa0/1 and server having IP address 73.1.1.2/24.

Now, first configuring the access-list:

```
R1(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

Configuring the nat pool from which a public IP will be selected.

```
R1(config)# ip nat pool pool1 12.1.1.1 12.1.1.1 netmask 255.255.255.0
```

Here, note that the nat pool is shrunk to one ip address only and the IP address used is the outside interface ip address of the router. If you have additional IP then you can use that also. Now, enabling Dynamic NAT overload (PAT):

```
R1(config)# ip nat inside source list 1 pool pool1 overload
```

Or we can also use

```
R1(config)# ip nat inside source list 1 interface fastEthernet 0/1 overload
```

At last, we have to configure router interfaces as inside or outside.

```
R1(config)# int fa0/0
R1(config-if)# ip nat inside
R1(config)# int fa0/1
R1(config-if)# ip nat outside
```

Ipconfig

This batch command displays Windows IP Configuration. Shows configuration by connection and the name of that connection.

Syntax

ipconfig

Example

```
@echo off
ipconfig
```

Output

The above command will display the Windows IP configuration on the current machine. Following is an example of the output.

```
Windows IP Configuration

Wireless LAN adapter Local Area Connection* 11:
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix . :

Ethernet adapter Ethernet:
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix . :

Wireless LAN adapter Wi-Fi:
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix . :
```

Reference link

https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ipconfig

ping command

https://www.paessler.com/it-explained/ping

netstat command

https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/netstat

traceroute command

https://kb.intermedia.net/article/682

What is a protocol?

A Protocol is a set of rules that we use for specific purposes. In the current scenario, when we are talking about *protocols,* it is about communication- the way we talk to each other. For instance, a newsreader speaks in English and because you understand English, you are able to understand. English is the protocol.

The moment the newsreader starts speaking in a language that you don't understand, the protocol beats its purpose. Thus, we need both the parties to agree to a set of rules for the communication to take place. The protocol, in this case, is for communication.

Now, talking about the web, in particular, multiple protocols are used to communicate. Primarily for end users, the most important and visible protocols are HTTP and HTTPS. Though there are many other protocols as well, HTTP and HTTPS protocols cater to most of the population.

What is HTTP?

HTTP is Hypertext transfer protocol. Simply put - Rules to sending and receiving text-based messages. As we all know, computers work in a language of 1's and 0's i.e. Binary language. Therefore, potentially every set of 1's and 0's construct something, it could be a word.

Let's say I want to write 'a'. Now, if 0 stands for 'a', 1 stands for 'b', and 01 stands for 'c', I can infer that a combination of 0's and 1's can construct a word as well. In this case, the text is already constructed and is being sent on the wire. The computer works on many languages - pure binary, text and some other formats like byte codes. Here, what is being transferred is text. I am emphasizing on 'text' because this text is interpreted by the browser and the moment browser interprets it, it becomes hypertext, and the protocol that transfers the text is referred to as *hypertext transfer protocol - HTTP.*

Using HTTP, you can definitely transfer images and text and even sound, but not videos.

What is HTTPS?

Hyper Text Transfer Protocol Secure (HTTPS) is the secure version of HTTP, the protocol over which data is sent between your browser and the website that you are connected to. The 'S' at the end of HTTPS stands for 'Secure'. It means all communications between your browser and the website are encrypted. HTTPS is often used to protect highly confidential online transactions like online banking and online shopping order forms.

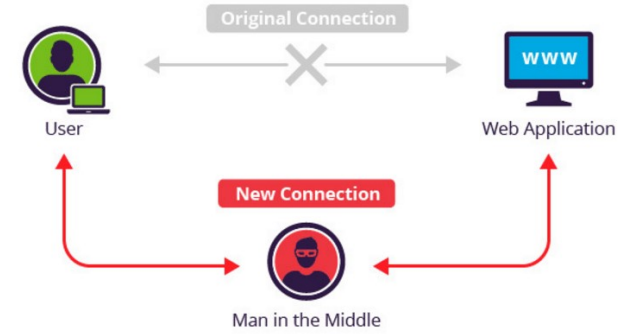
What is the importance of HTTPS?

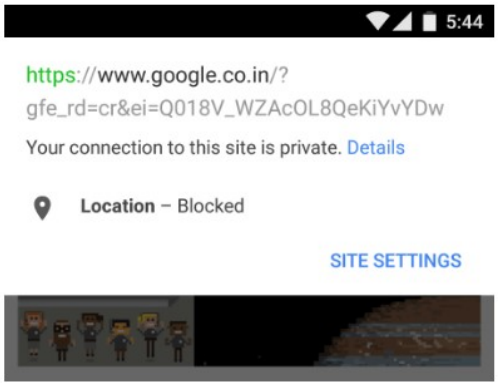
We agreed upon the fact that what is being transferred from one point to another is text. To understand why HTTPS protocol, we first should know how wi-fi routers function.Let's say you are at an airport and you are connecting to the wi-fi which is the property of a third party. Now, when you are communicating over HTTP, the text is being transferred by their router. And if I go to a low version of the router, I can comfortably check and read the text that is being transferred. There could be a password that I can use to login to your bank site and do a fraudulent

transaction!. Point being - this is fundamentally insecure. This is called the *man in the middle attack.*

And this why do we need https when HTTP seems to suffice.

Now, to save our data from such attacks, we need to encrypt that data.





This is what HTTPS site looks like.

Encryption and Encryption Levels

Encryption is simple terms is a hiding information. There are various ways to do so. You must have heard these terms - 128 bit encrypt HTTPS and 64 bit encrypt HTTPS. 128-bit Encrypt is a high encryption technique and it's very difficult to decrypt (decode). In the case of HTTPS when the data is being transferred on the wires, the man in the middle may still know what is being transferred, but can not make sense out of it as the data is encrypted. Only the browser will decrypt it and show it, and the server will decrypt it and use it for transactions.

For the curious one's - There also happens to be a movie on encryption, Imitation Games. The entire plot of the movie was based on decrypting the German codes, which were to reform the entire course of the war. Those codes were very difficult to decrypt, but how Alan Turing finally does it.

How does this happens when you request to open a site in a browser?

To understand this, let us imagine that there is one *Server that resides somewhere* serving all the request for one domain. Now, when I type xyz.com, it's a server that I am connecting to, taking data from and rendering it in the browser.

To simplify further, imagine a domain name google.com being broadcasted from one server. There resides one machine somewhere connected to the internet and the moment you say google.com in your browser, you connect to that machine, pick data from that machine and show it in the browser. If you have saved your picture, it gets uploaded to that machine. Now, if you want to see that picture, you go to google.com/show-me-my-picture, which transfers the picture from the machine to the browser to be shown to you.

This process cannot be completed if I am not able to reach that particular machine. For this to happen, every machine has an address (the way we have a mobile number), it is called the IP address and every domain has an IP map. The moment you enter this user-friendly URL - google.com, it converts this username into IP and connects to the router to reach out to that particular service line associated with this URL. Once it reaches to the server, it raises a request of what is needed. It is represented as 'google.com/s=', helping the user understand the request made by him. As a result, the server gives him the results according to your request, which gets rendered to the browser.

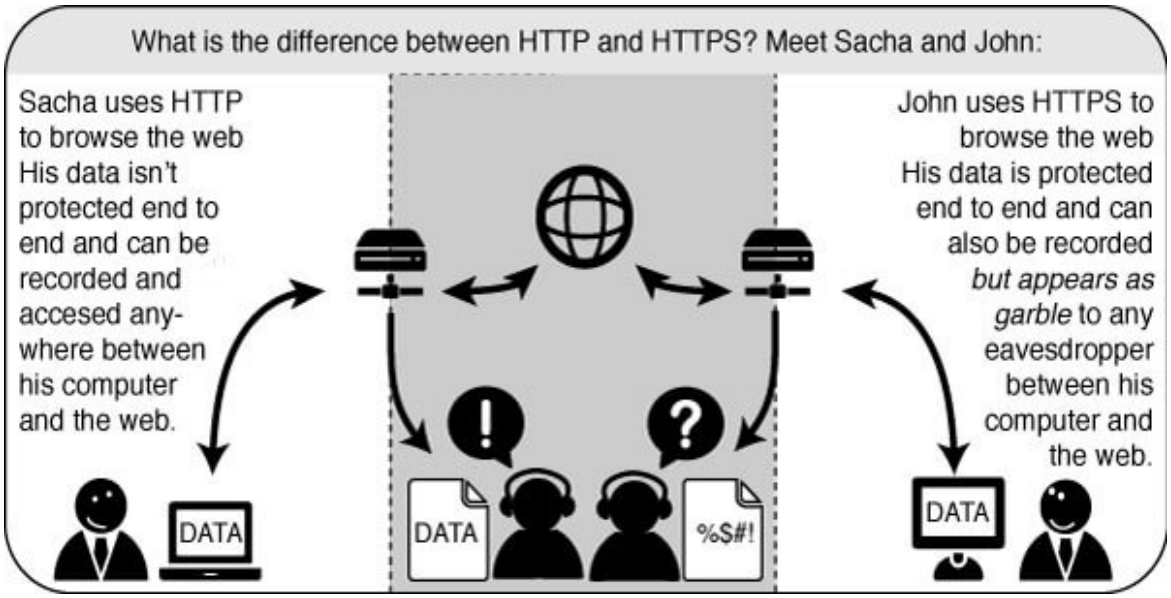
What happens when a request for a website URL is made which is on HTTP protocol?

As the first step, it is the job of HTTP to find out the server and once the communication route is established, the server sends a text to the browser. This text could either be in its pure form or encrypted form, which is then rendered by the browser or used for whatever purpose it has to it has to be used.

There also happens to be a movie on encryption- Imitation Games. The entire plot of the movie was based on decrypting the German codes by the protagonists, which were to reform the entire course of the war. Those codes were very difficult to decrypt, but Alan Turing finally does it.

As there should be a measurement of this difficulty quotient, we interpret that, higher the number of bits, more difficult it is to decrypt. However, it only increases the level of complexity making it very difficult to decrypt, but not impossible.

Deciding between HTTP and HTTPS



Source: http://en.flossmanuals.net/basic-internet-security/_all/

Anything and everything is personal. If you are searching for "How to install SSL Certificate", that search would be private to you, isn't it? Whether you are browsing or looking for a product, reading an article, you generally do not want others to know about it. As an end user, I would want to keep it as private. There are things I might not want to keep private and for those, I can use HTTP. However, for personal information, banks and transnational information, HTTPS has become a standard.

HTTPS sounds great. What else should you know about it?

There is no denying to the fact that privacy has a cost to it. There are a couple of *cons*-

1. HTTPS requests take more time to process.

2. Because it needs more time to process, it needs more hardware - the server that you are utilizing. This also means additional cost

Whereas, for HTTP you use lesser energy as compared to HTTPS as the communication happens faster (without encryption and decryption). However, I will not refer to it as a *limitation* for HTTPS. It is highly subjective and personal, I consider it a very low cost that we pay to ensure our privacy.

The idea of building a secure web has been around for a while. Building a Secure web as an agenda is being driven by likes of Google, Facebook, Akamai and so forth as I had mentioned this is primarily because of the following two reasons -

1. User Data and User Privacy: Using HTTPS ensures that you as a developer care value user data, user's privacy, and its security.

2. Protecting Your Data: As a developer, we would never want to give away our critical data to malicious participants

Here are some of the features which are now only available on HTTPS.

- GeoLocation: You can no longer seek user's location if you are on HTTP
- Web Push Notification: Push Notifications are only available on HTTPS.
- GetUserMedia: You can no longer trigger permissions of using user's camera/ microphone if you are on HTTP
- HTTP/2: All major browsers, support HTTP/2 for HTTPS now.

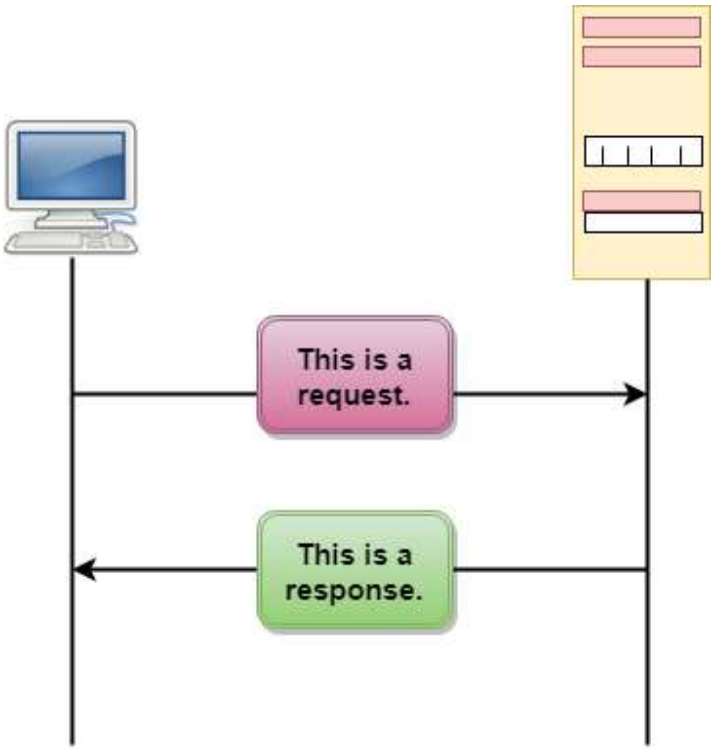
HTTP

- HTTP stands for **HyperText Transfer Protocol**.
- It is a protocol used to access the data on the World Wide Web (www).
- The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.
- This protocol is known as HyperText Transfer Protocol because of its efficiency that allows us to use in a hypertext environment where there are rapid jumps from one document to another document.
- HTTP is similar to the FTP as it also transfers the files from one host to another host. But, HTTP is simpler than FTP as HTTP uses only one connection, i.e., no control connection to transfer the files.
- HTTP is used to carry the data in the form of MIME-like format.
- HTTP is similar to SMTP as the data is transferred between client and server. The HTTP differs from the SMTP in the way the messages are sent from the client to the server and from server to the client. SMTP messages are stored and forwarded while HTTP messages are delivered immediately.

Features of HTTP:

- **Connectionless protocol:** HTTP is a connectionless protocol. HTTP client initiates a request and waits for a response from the server. When the server receives the request, the server processes the request and sends back the response to the HTTP client after which the client disconnects the connection. The connection between client and server exist only during the current request and response time only.
- **Media independent:** HTTP protocol is a media independent as data can be sent as long as both the client and server know how to handle the data content. It is required for both the client and server to specify the content type in MIME-type header.
- **Stateless:** HTTP is a stateless protocol as both the client and server know each other only during the current request. Due to this nature of the protocol, both the client and server do not retain the information between various requests of the web pages.

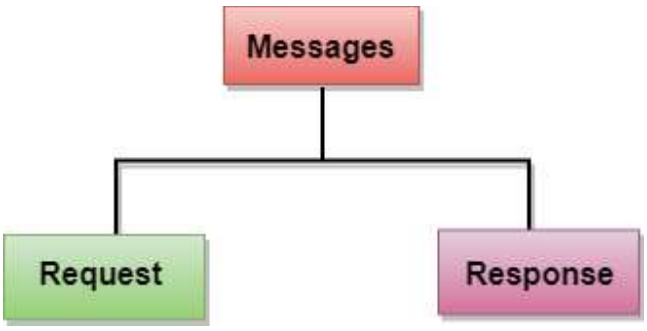
HTTP Transactions



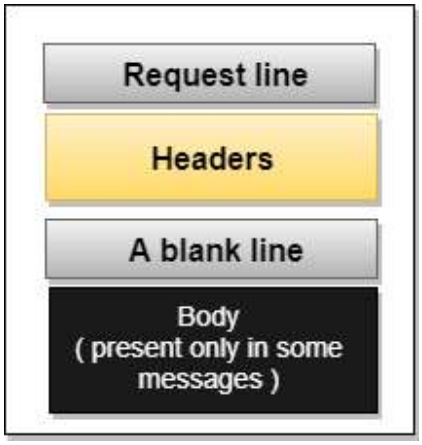
The above figure shows the HTTP transaction between client and server. The client initiates a transaction by sending a request message to the server. The server replies to the request message by sending a response message.

Messages

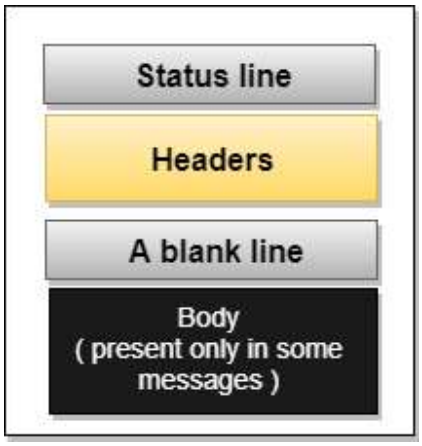
HTTP messages are of two types: request and response. Both the message types follow the same message format.



Request Message: The request message is sent by the client that consists of a request line, headers, and sometimes a body.



Response Message: The response message is sent by the server to the client that consists of a status line, headers, and sometimes a body.



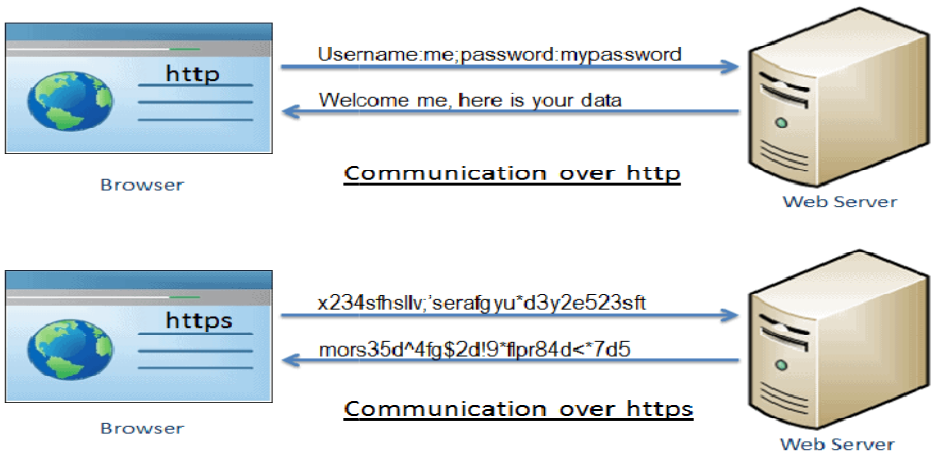
Uniform Resource Locator (URL)

- A client that wants to access the document in an internet needs an address and to facilitate the access of documents, the HTTP uses the concept of Uniform Resource Locator (URL).
- The Uniform Resource Locator (URL) is a standard way of specifying any kind of information on the internet.
- The URL defines four parts: method, host computer, port, and path.

- **Method:** The method is the protocol used to retrieve the document from a server. For example, HTTP.
- **Host:** The host is the computer where the information is stored, and the computer is given an alias name. Web pages are mainly stored in the computers and the computers are given an alias name that begins with the characters "www". This field is not mandatory.
- **Port:** The URL can also contain the port number of the server, but it's an optional field. If the port number is included, then it must come between the host and path and it should be separated from the host by a colon.
- **Path:** Path is the pathname of the file where the information is stored. The path itself contain slashes that separate the directories from the subdirectories and files.

HTTPS

HTTPS stands for Hyper Text Transfer Protocol Secure. It is a protocol for securing the communication between two systems e.g. the browser and the web server. The following figure illustrates the difference between communication over http and https:



Communication over https and http

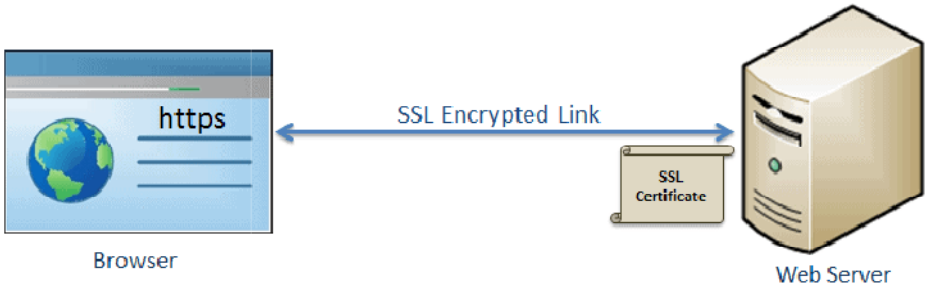
As you can see in the above figure, http transfers data between the browser and the web server in the hypertext format, whereas https transfers data in the encrypted format. Thus, https prevents hackers from reading and modifying the data during the transfer between the browser and the web server. Even if hackers manage to intercept the communication, they will not be able to use it because the message is encrypted.

HTTPS established an encrypted link between the browser and the web server using the Secure Socket Layer (SSL) or Transport Layer Security (TLS) protocols. TLS is the new version of SSL.

Secure Socket Layer (SSL)

SSL is the standard security technology for establishing an encrypted link between the two systems. These can be browser to server, server to server or client to server. Basically, SSL ensures that the data transfer between the two systems remains encrypted and private.

The https is essentially http over SSL. SSL establishes an encrypted link using an SSL certificate which is also known as a digital certificate.



SSL

http vs https

http	https
Transfers data in hypertext (structured text) format	Transfers data in encrypted format
Uses port 80 by default	Uses port 443 by default
Not secure	Secured using SSL technology
Starts with http://	Starts with https://

Advantage of https

- **Secure Communication:** https makes a secure connection by establishing an encrypted link between the browser and the server or any two systems.
- **Data Integrity:** https provides data integrity by encrypting the data and so, even if hackers manage to trap the data, they cannot read or modify it.

- **Privacy and Security:** https protects the privacy and security of website users by preventing hackers to passively listen to communication between the browser and the server.
- **Faster Performance:** https increases the speed of data transfer compared to http by encrypting and reducing the size of the data.
- **SEO:** Use of https increases SEO ranking. In Google Chrome, Google shows the **Not Secure** label in the browser if users' data is collected over http.
- **Future:** https represents the future of the web by making internet safe for users and website owners.

FTP

- FTP stands for File transfer protocol.
- FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.
- It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.
- It is also used for downloading the files to computer from other servers.

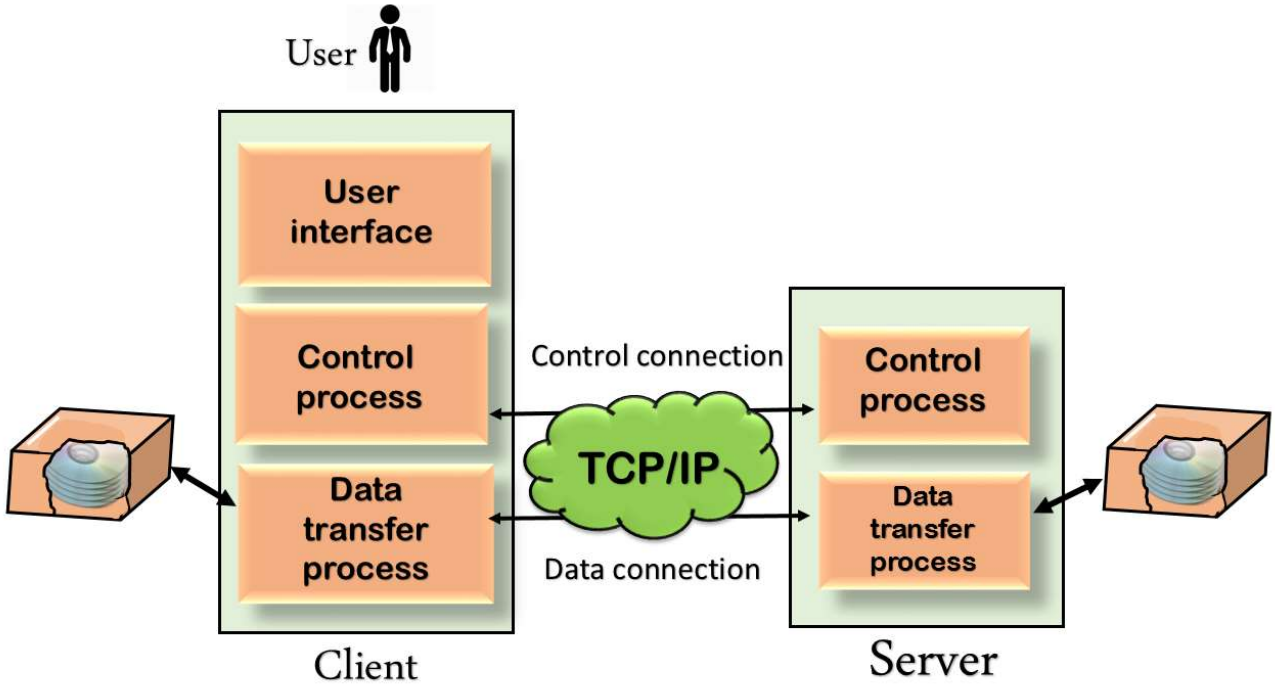
Objectives of FTP

- It provides the sharing of files.
- It is used to encourage the use of remote computers.
- It transfers the data more reliably and efficiently.

Why FTP?

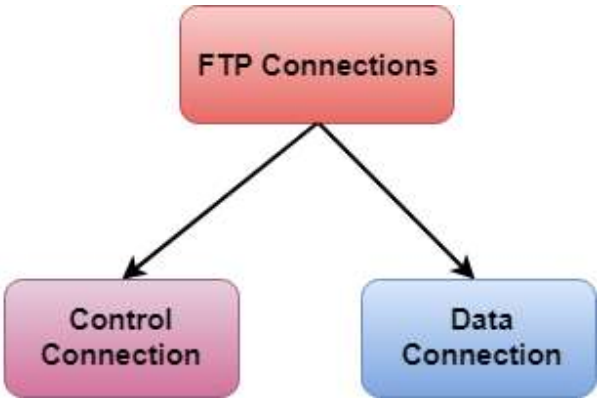
Although transferring files from one system to another is very simple and straightforward, but sometimes it can cause problems. For example, two systems may have different file conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures. FTP protocol overcomes these problems by establishing two connections between hosts. One connection is used for data transfer, and another connection is used for the control connection.

Mechanism of FTP



The above figure shows the basic model of the FTP. The FTP client has three components: the user interface, control process, and data transfer process. The server has two components: the server control process and the server data transfer process.

There are two types of connections in FTP:



- **Control Connection:** The control connection uses very simple rules for communication. Through control connection, we can transfer a line of command or line of response at a time. The control connection is made between the control processes. The control connection remains connected during the entire interactive FTP session.

- **Data Connection:** The Data Connection uses very complex rules as data types may vary. The data connection is made between data transfer processes. The data connection opens when a command comes for transferring the files and closes when the file is transferred.

FTP Clients

- FTP client is a program that implements a file transfer protocol which allows you to transfer files between two hosts on the internet.
- It allows a user to connect to a remote host and upload or download the files.
- It has a set of commands that we can use to connect to a host, transfer the files between you and your host and close the connection.
- The FTP program is also available as a built-in component in a Web browser. This GUI based FTP client makes the file transfer very easy and also does not require to remember the FTP commands.

Advantages of FTP:

- **Speed:** One of the biggest advantages of FTP is speed. The FTP is one of the fastest way to transfer the files from one computer to another computer.
- **Efficient:** It is more efficient as we do not need to complete all the operations to get the entire file.
- **Security:** To access the FTP server, we need to login with the username and password. Therefore, we can say that FTP is more secure.
- **Back & forth movement:** FTP allows us to transfer the files back and forth. Suppose you are a manager of the company, you send some information to all the employees, and they all send information back on the same server.

Disadvantages of FTP:

- The standard requirement of the industry is that all the FTP transmissions should be encrypted. However, not all the FTP providers are equal and not all the providers offer encryption. So, we will have to look out for the FTP providers that provides encryption.
- FTP serves two operations, i.e., to send and receive large files on a network. However, the size limit of the file is 2GB that can be sent. It also doesn't allow you to run simultaneous transfers to multiple receivers.
- Passwords and file contents are sent in clear text that allows unwanted eavesdropping. So, it is quite possible that attackers can carry out the brute force attack by trying to guess the FTP password.
- It is not compatible with every system.