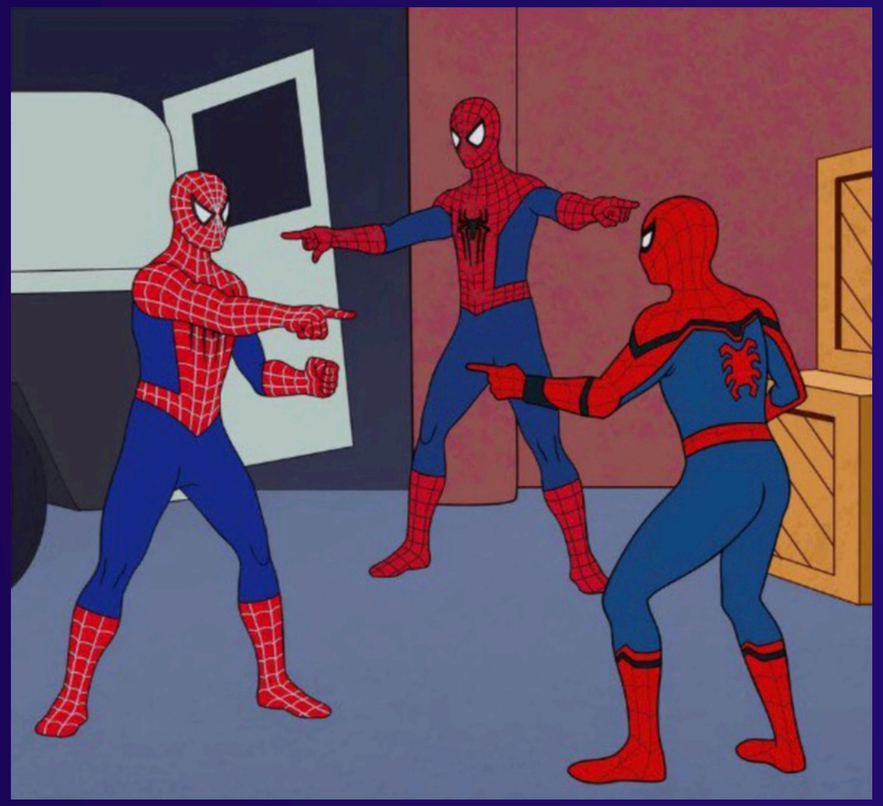
Peer to Peer (P2P) Networks

CS212-Computer Networks

2203115 - Shashank Kadam
2203126 - Hamza Sabugar
2204205 - Amit Shinde
2203139 - Yash Bhadauria

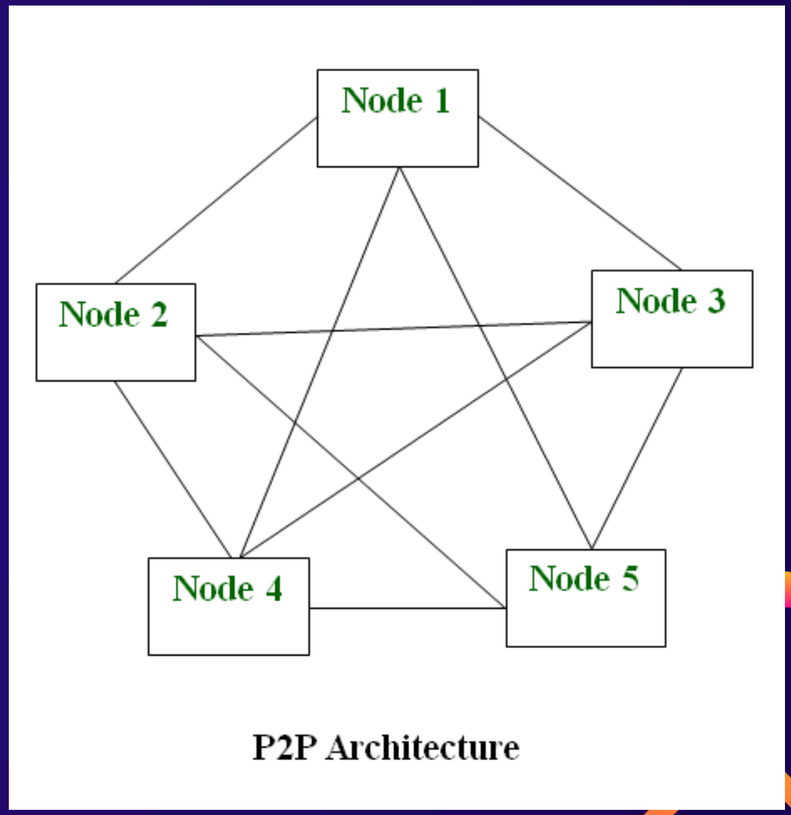
Table of contents



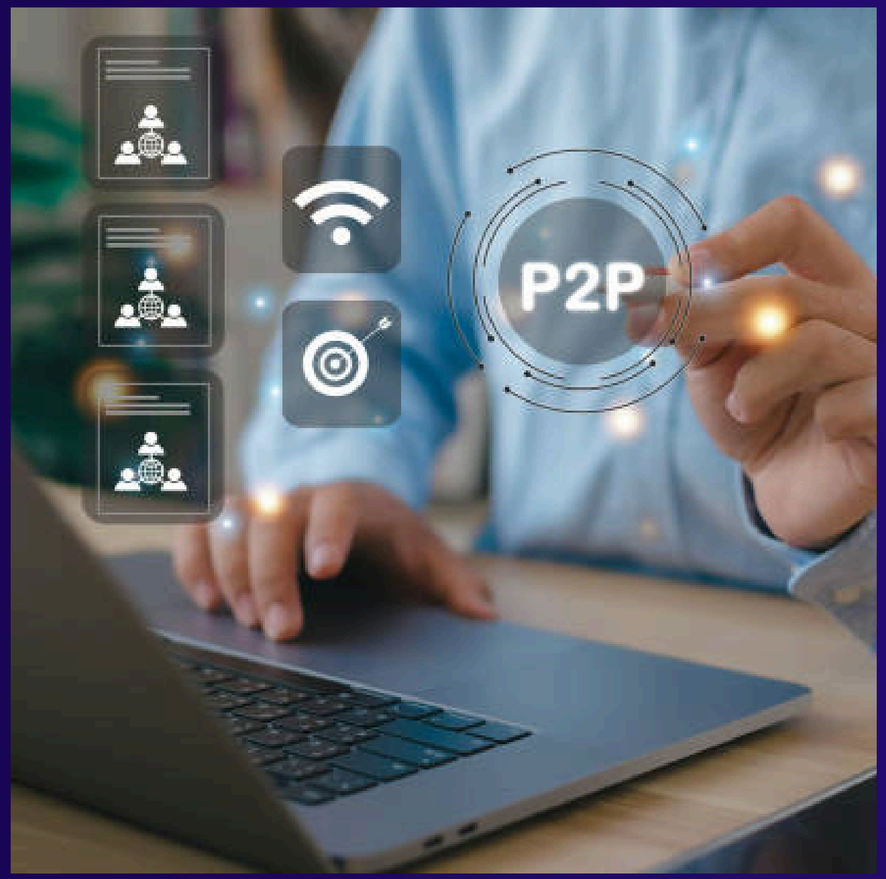
01 Introduction

What is Peer to Peer (P2P) Architecture?

- A peer-to-peer network is a simple network of computers
- Here each computer acts as a node for file sharing within the formed network. Here each node acts as a server and thus there is no central server in the network
- This allows the sharing of a huge amount of data
- The tasks are equally divided amongst the nodes.
- Each node connected in the network shares an equal workload
- For the network to stop working, all the nodes need to individually stop working
- Each node works independently



P2P Architecture



02 Types of P2P Networks

Types of P2P networks

Unstructured P2P networks

Devices Connected randomly in the network

Structured P2P networks

Network has a software built specific structure

Hybrid P2P networks

Combines features of both P2P and client-server architecture

Levels of P2P networks

1

Level 1

basic level which uses a USB to create a P2P network between two systems

2

level 2

intermediate level which involves the usage of copper wires in order to connect more than two systems

3

Level 3

Advanced level which uses software to establish protocols in order to manage numerous devices across the internet.

Unstructured P2P networks

- Each Device makes equal contribution
- Easy to build as devices can be connected randomly in the network
- Difficult to find content in this network
- These networks are particularly suitable for applications with high activity levels, such as social platforms, where users frequently enter or exit the network
- Napstar, Gnutella

Structured P2P networks

- These networks enable users to locate and utilize files more efficiently, eliminating random searches and Hash functions often facilitate database lookups in structured P2P networks
- Exhibit some degree of centralization due to their organized setup resulting in higher maintenance and setup costs compared to unstructured P2P networks
- Provide greater stability than their unstructured counterparts.
- P-Grid, Kademlia,

Hybrid P2P networks

- Combine P2P architecture with the client-server model. This hybridization introduces a central server with P2P capabilities, proving advantageous for specific network scenarios.
- Offer numerous advantages over structured and unstructured networks, including strategic approaches, enhanced performance, and other benefits
- Hybrid P2P networks present a compelling choice for networks that seek to leverage both P2P and client-server architectures.

Advantages of P2P networks

Scalability

Easily scaled by adding more peers to the network
As more nodes join, the network's capacity and resources grow organically.

Resource Sharing

Facilitate sharing of resources
Enables collaborative efforts and reduces the need for redundant storage

Cost Efficiency

Can operate with lower infrastructure costs compared to client-server models
Burden of maintaining and managing a central server is reduced.

Self-Healing

P2P networks can recover from failures more gracefully due to decentralised nature.
If a node goes offline, other nodes can compensate by taking over its tasks.

Disadvantages of P2P networks

S

Security Concerns

The open nature of P2P networks can expose them to security risks, including unauthorized access, data breaches, and malware distribution.

Q

Quality and Reliability

The quality and reliability of resources shared on P2P networks can vary significantly, making it important to verify the legitimacy and integrity of files.

M

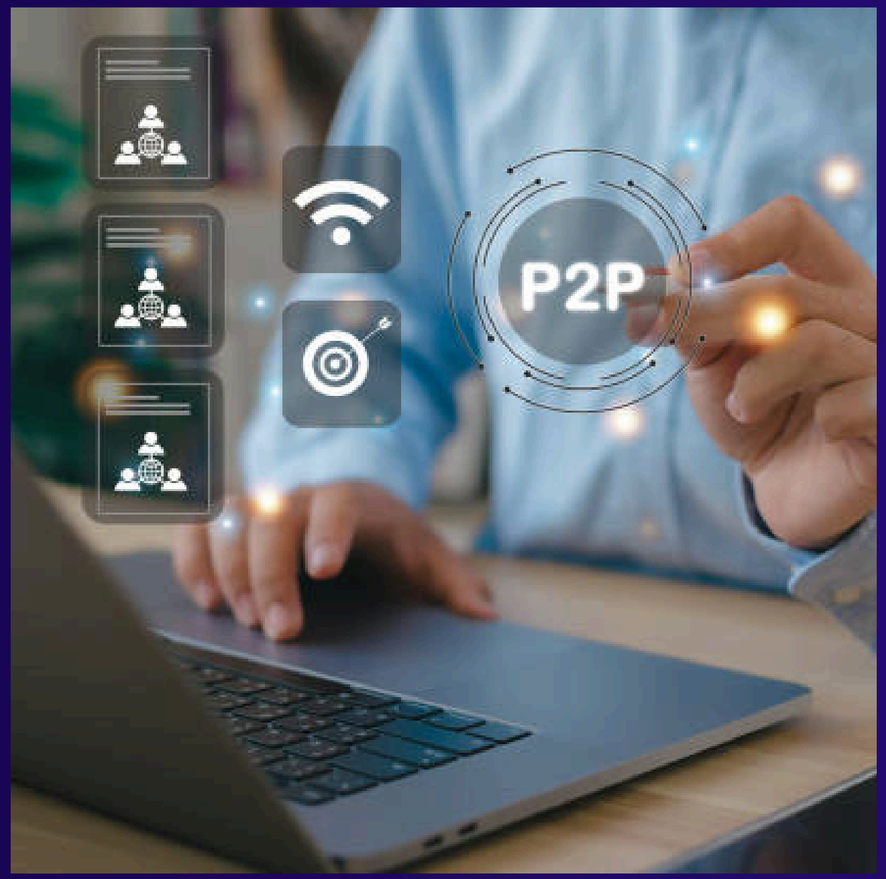
Management Complexity

Maintaining a P2P network can be more complex than a traditional network, requiring specialized protocols and mechanisms to ensure proper coordination.

L

Legal and Copyright Issues

P2P networks have been associated with copyright infringement due to the ease of sharing copyrighted material. This has led to legal challenges for both users and network operators.



03 History

History of P2P applications ...

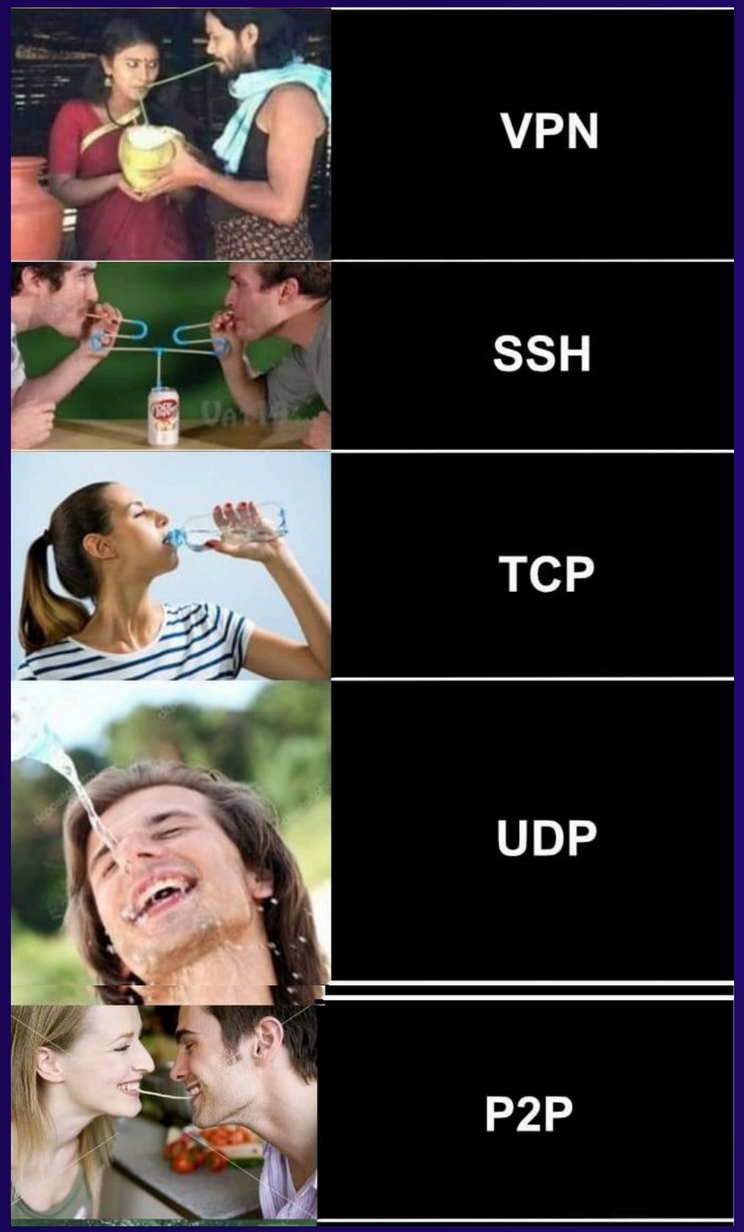
- Peer-to-peer (P2P) networks first appeared in the 1980s after the introduction of personal computers. The first P2P protocols were FidoNet and Usenet.
- The first P2P network, the Internet Relay Chat, was developed in 1988 to share text and chat.
- In 1999, Shawn Fanning created Napster, the first P2P application for file sharing and music, which allowed users to share audio and other files.
- The concept of P2P application popularised by file sharing applications such as Napster. But later, Napster was shutdown due to illegal file sharing or piracy

History of P2P applications ...

- Following Napster's demise, several decentralized file-sharing protocols emerged, including Gnutella and BitTorrent.
- BitTorrent, developed by Bram Cohen in 2001, introduced a more efficient method for distributing large files by dividing them into smaller pieces shared among multiple users. Kazaa, another popular file-sharing platform, also gained prominence during this time.
- The mid-2000s saw increased scrutiny and legal challenges against P2P networks due to copyright infringement concerns. Many file-sharing services faced legal action, leading to the shutdown of some platforms and changes in others to comply with copyright laws.

History of P2P applications ...

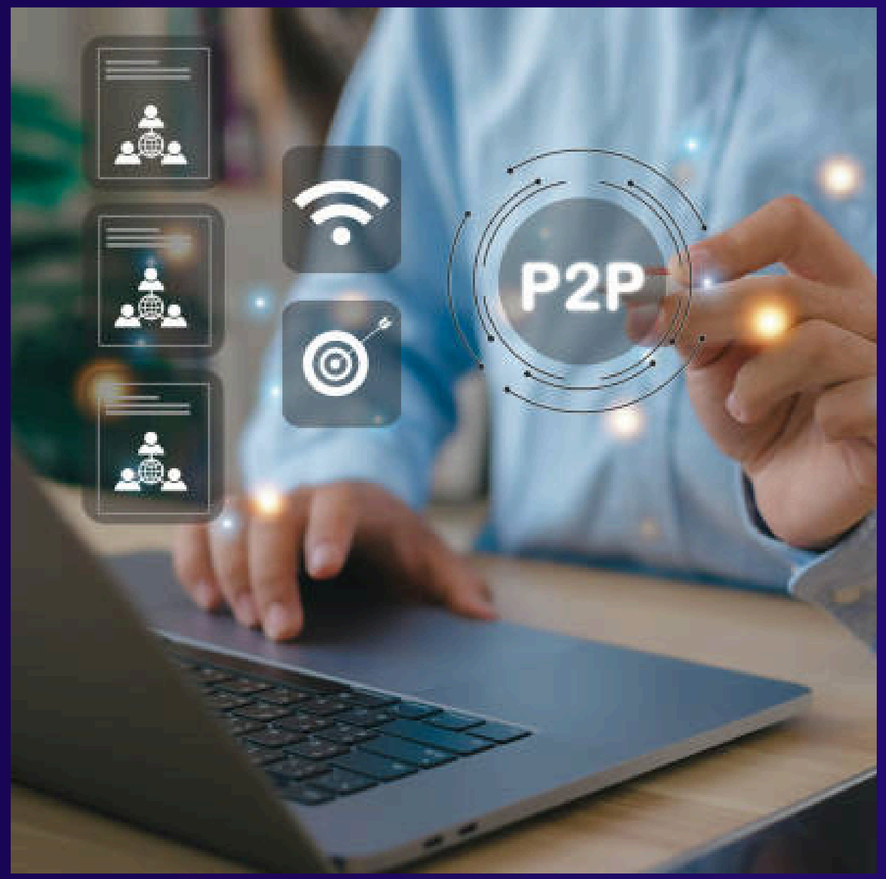
- In 2008, the publication of the Bitcoin by an anonymous person or group known as Satoshi Nakamoto introduced the concept of blockchain and decentralized cryptocurrencies. Bitcoin operates on a P2P network, allowing users to transact directly with each other without the need for intermediaries.
- The 2010s witnessed the proliferation of blockchain technology beyond cryptocurrencies. Projects like Ethereum introduced smart contracts, enabling developers to create decentralized applications (DApps) on top of blockchain networks. Additionally, decentralized storage platforms like IPFS (InterPlanetary File System) emerged, providing a distributed alternative to traditional cloud storage services



P2P VS Client-Server

Comparison of P2P and client-server architecture

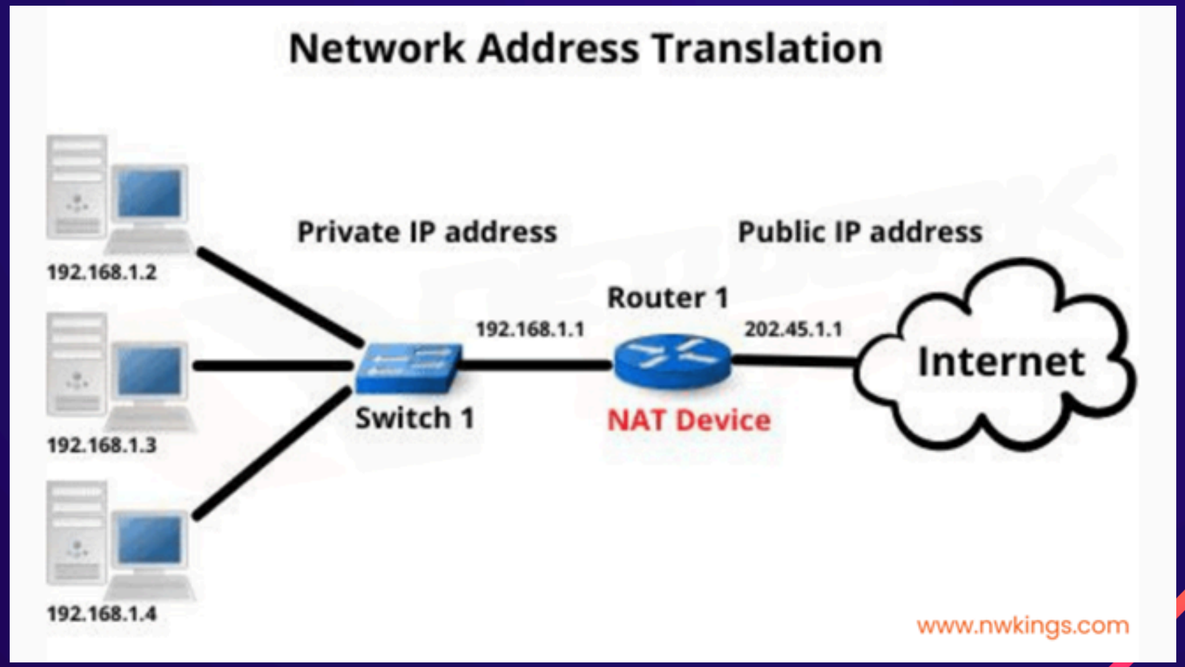
- In the terms of cost efficiency, P2P architecture is better due to reduced infrastructure costs but, client-server architecture is more stable.
- In terms of performance and security, client-server architecture is better than P2P architecture.
- The main focus of client server architecture is sending or sharing the information , but the purpose of P2P architecture is connectivity between 2 or multiple devices.
- In client-server architecture, the main server processes and responds to the requests , but in P2P architecture, each and every node can request and process the request.



05 Network Address Translation (NAT)

What is the need of NAT

- The idea of NAT is to allow multiple devices to access the Internet through a single public address. To achieve this, the translation of a private IP address to a public IP address is required. Network Address Translation (NAT)



Problem before the NAT

- Availability of IP ADDRESS - Each device would need a unique public IP address to directly communicate on the Internet, which would quickly exhaust available IP addresses.

- Security - Security would be compromised as internal devices would be directly exposed to the Internet without the NAT firewall acting as a barrier.

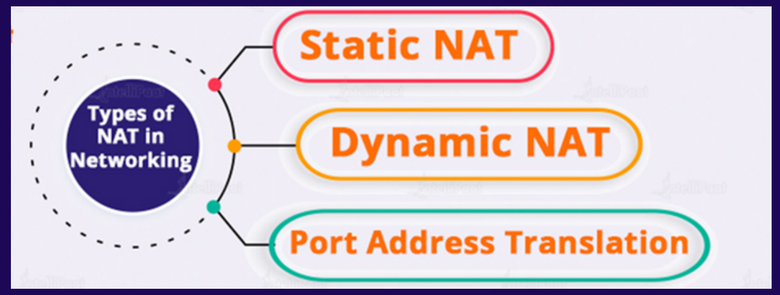
Goal of NAT

- **Private IP Addressing** – NAT allows organizations to use private IP addresses internally, which are not routable on the public Internet. This conserves public IP address space.

- **Address Translation** NAT translates private IP addresses to public IP addresses when data packets leave the local network and need to traverse the Internet. This translation is typically done by a router or firewall.

- **Conservation of Public IP Addresses:** NAT allows multiple devices within an organization to share a single public IP address. This is important because public IP addresses are limited and expensive.

- **Internet Access and security** Without NAT, devices with private IP addresses wouldn't be able to directly access the Internet because routers on the Internet would not recognize or route packets to these private addresses.



Types of NAT

S

Static NAT

One private ip address map with the one public ip address

In the port address translation(static) All the private ipaddress map with the singlepublic ip address

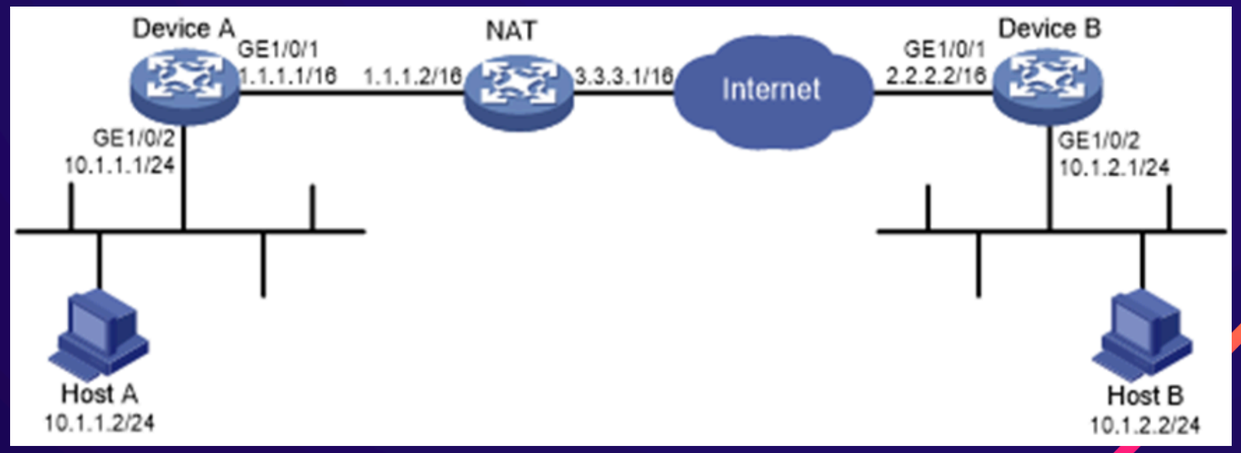
D

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 addresses.
If the IP address of the pool is not free, then the packet will be dropped as only a fixed number of private IP addresses can be translated to public addresses. Suppose, if there is a pool of 2 public IP addresses then only 2 private IP addresses can be translated at a given time

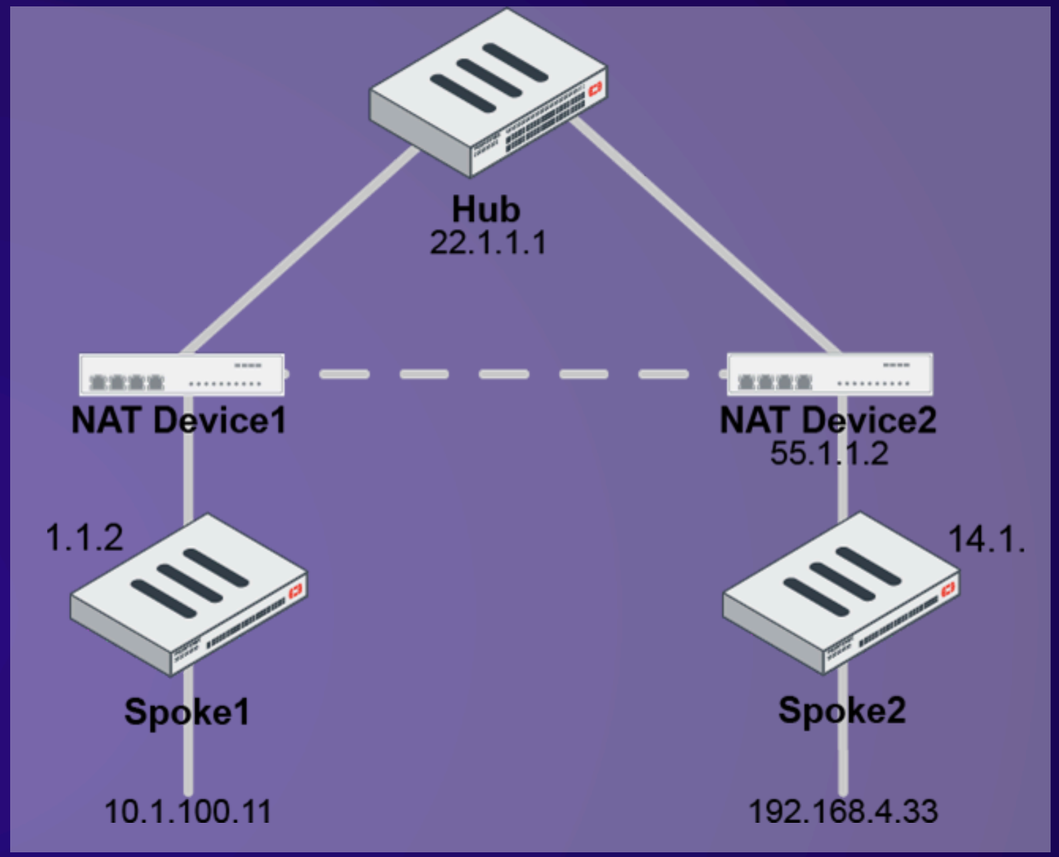
NAT Traversal

- NAT Traversal stands for Network Address Translation Traversal. This type of traversal method is used in web technologies to manage and process all the IP addresses while the data is being transferred through the IPSec tunnel for the translation-related issues that it faced in the data transmission
- NAT Traversal uses UDP encapsulation. This involves adding a new UDP header to the data packet, which hides the original header and allows the NAT device to treat the packet as a normal UDP packet



UDP HOLE PUNCHING

- Since most computers in the world are behind some kind of NAT this method is widely used in P2P (Peer to Peer) architectures. The establishment of a P2P network requires direct connection between any two nodes. Hole Punching is the most important concept one has to learn when creating a P2P network. Network firewalls can be bypassed using this concept. Hole Punching is very safe as Connection must be initiated from both ends, hence consent of both users is required.

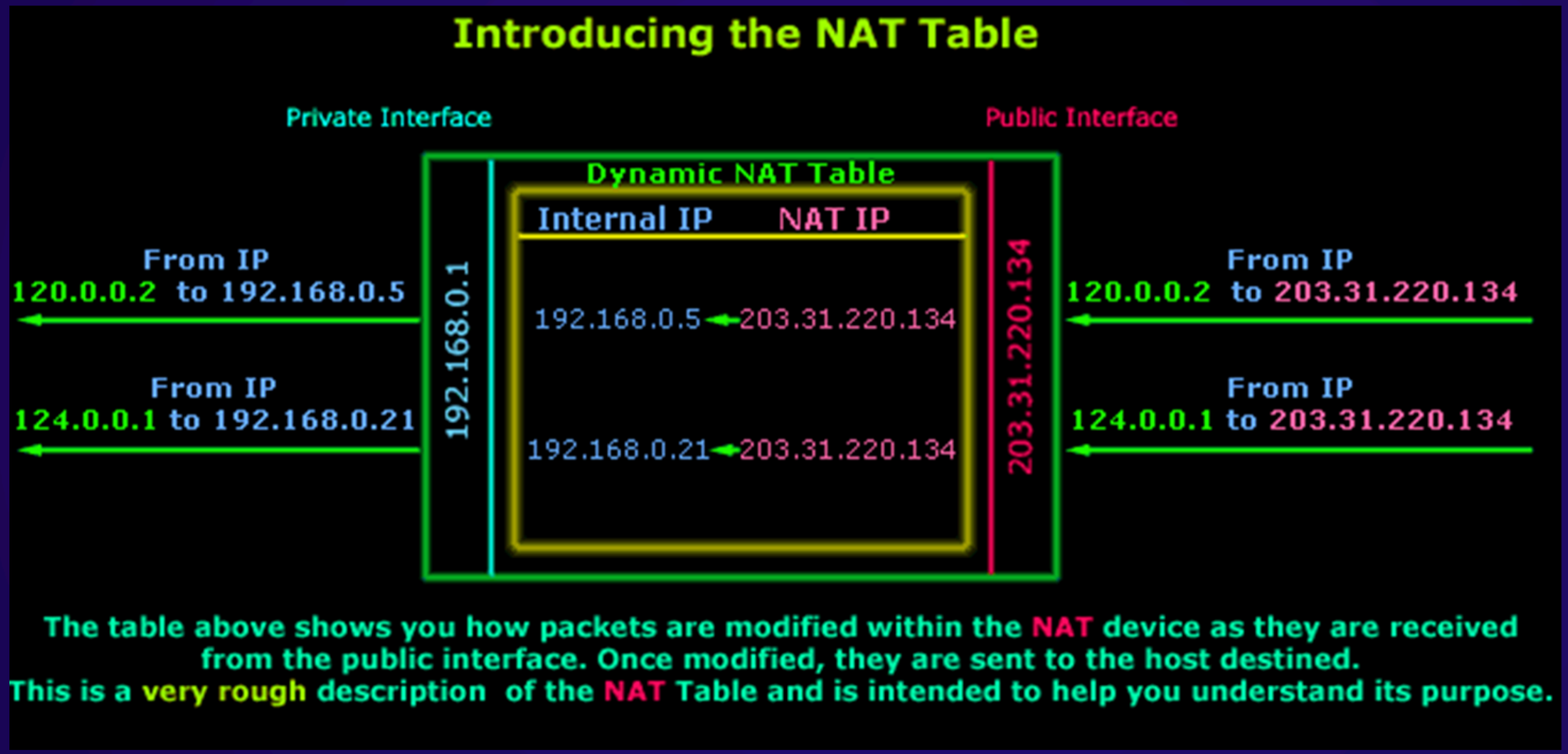


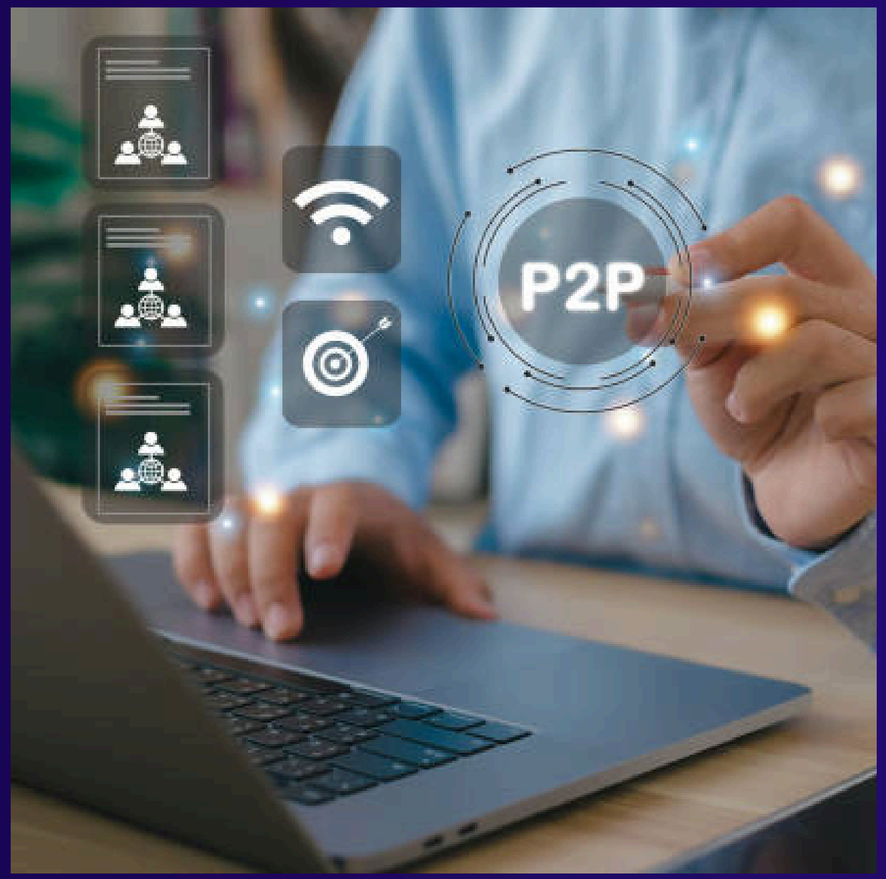
Steps:
1) A send S a requests connection to B.S sends A's address to B and B's address to A.
2) A sends garbage message to B and B sends garbage message to A. (Both Get discarded by their respective NATs) this is generaly use to know port number and ip
3) Step 3 is repeated.(conformation)
4) Connection Established.

Disadvantages of NAT

- Translation results in switching path delays. Certain applications will not function while NAT is enabled.
- NAT requires translation of IP addresses and ports of packets. This translation process consumes resources, which can lead to a decrease in network performance, especially under heavy network load..
- Also, the router being a network layer device, should not tamper with port numbers(transport layer) but it has to do so because of NAT.

NAT Table


Introducing the NAT Table
Private Interface
Public Interface
Dynamic NAT Table
Internal IP
NAT IP
From IP
120.0.0.2 to 192.168.0.5
From IP
124.0.0.1 to 192.168.0.21
192.168.0.1
192.168.0.5 ← 203.31.220.134
192.168.0.21 ← 203.31.220.134
203.31.220.134
From IP
120.0.0.2 to 203.31.220.134
From IP
124.0.0.1 to 203.31.220.134
The table above shows you how packets are modified within the NAT device as they are received from the public interface. Once modified, they are sent to the host destined.
This is a very rough description of the NAT Table and is intended to help you understand its purpose.



05 Applications

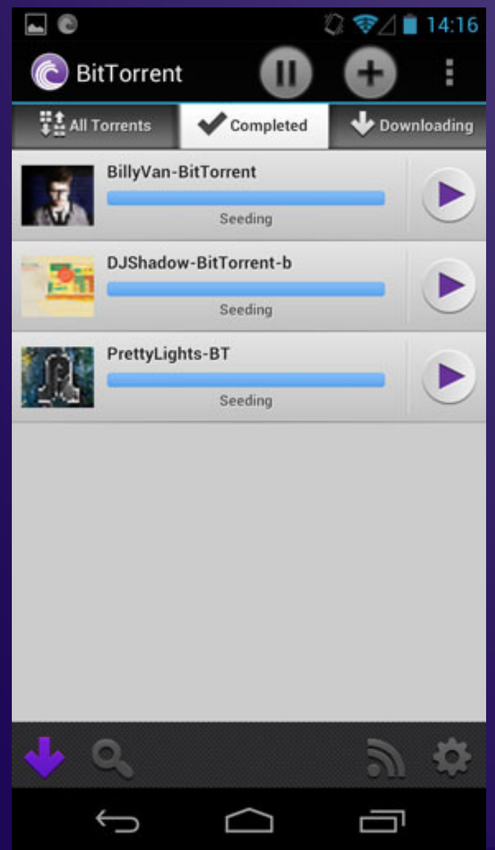
Applications using P2P model

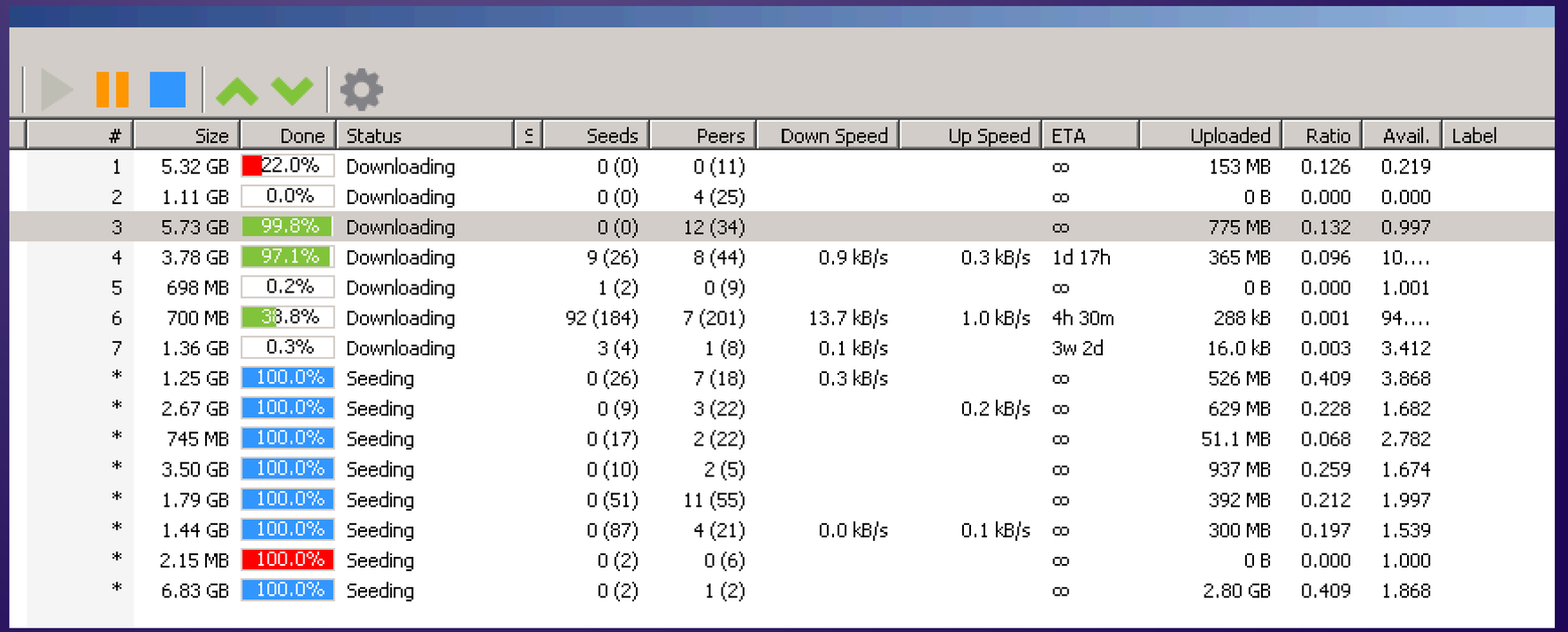
BitTorrent

History and Uses

- Programmer Bram Cohen designed the protocol in April 2001 and released a first implementation of the BitTorrent client on 2 July 2001.It is now maintained by Cohen's company.(source : Wikipedia)
- The BitTorrent client enables a user to search for and download torrent files using a built-in search box ("Search for torrents") in the main window, which opens the BitTorrent torrent search engine page with the search results in the user's default.
- Latest version of BitTorrent is 7.4.3 released on May 19, 2020.
- It allows decentralised peer to peer file sharing through centralised coordination mechanism.
- Many open-source projects use BitTorrent to distribute their software releases. As it can save bandwidth cost and help user to download fast.
- It also provide backup service for flies between devices. Example : BitTorrent Sync
- Researchers, scientists, and academic institutions often use BitTorrent to distribute large datasets, such as scientific data, research papers, or datasets for machine learning projects. BitTorrent's decentralized nature can help distribute these datasets efficiently to a large number of users.

History and Uses



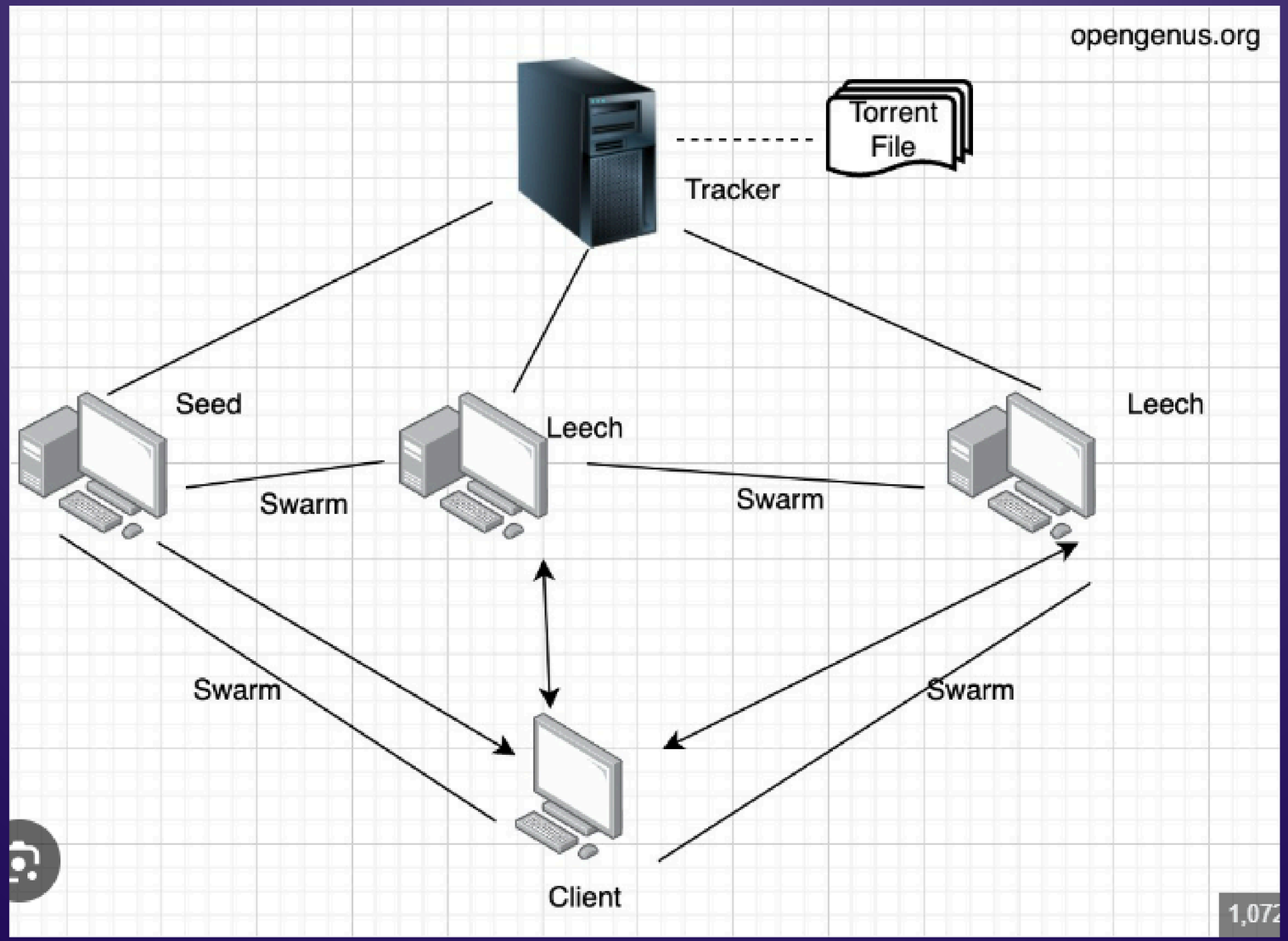


#	Size	Done	Status	S	Seeds	Peers	Down Speed	Up Speed	ETA	Uploaded	Ratio	Avail.	Label
1	5.32 GB	22.0%	Downloading		0 (0)	0 (11)			∞	153 MB	0.126	0.219	
2	1.11 GB	0.0%	Downloading		0 (0)	4 (25)			∞	0 B	0.000	0.000	
3	5.73 GB	99.8%	Downloading		0 (0)	12 (34)			∞	775 MB	0.132	0.997	
4	3.78 GB	97.1%	Downloading		9 (26)	8 (44)	0.9 kB/s	0.3 kB/s	1d 17h	365 MB	0.096	10....	
5	698 MB	0.2%	Downloading		1 (2)	0 (9)			∞	0 B	0.000	1.001	
6	700 MB	38.8%	Downloading		92 (184)	7 (201)	13.7 kB/s	1.0 kB/s	4h 30m	288 kB	0.001	94....	
7	1.36 GB	0.3%	Downloading		3 (4)	1 (8)	0.1 kB/s		3w 2d	16.0 kB	0.003	3.412	
*	1.25 GB	100.0%	Seeding		0 (26)	7 (18)	0.3 kB/s		∞	526 MB	0.409	3.868	
*	2.67 GB	100.0%	Seeding		0 (9)	3 (22)		0.2 kB/s	∞	629 MB	0.228	1.682	
*	745 MB	100.0%	Seeding		0 (17)	2 (22)			∞	51.1 MB	0.068	2.782	
*	3.50 GB	100.0%	Seeding		0 (10)	2 (5)			∞	937 MB	0.259	1.674	
*	1.79 GB	100.0%	Seeding		0 (51)	11 (55)			∞	392 MB	0.212	1.997	
*	1.44 GB	100.0%	Seeding		0 (87)	4 (21)	0.0 kB/s	0.1 kB/s	∞	300 MB	0.197	1.539	
*	2.15 MB	100.0%	Seeding		0 (2)	0 (6)			∞	0 B	0.000	1.000	
*	6.83 GB	100.0%	Seeding		0 (2)	1 (2)			∞	2.80 GB	0.409	1.868	

Components of BitTorrent Architecture

- **Tracker**: This is a server that helps peers find each other. When a user wants to download a file, their BitTorrent client connects to the tracker to get a list of other users who are also downloading or sharing the same file.
- **Seeder**: A seeder is a user who has a complete copy of the file and is sharing it with others.
- **Leecher**: A leecher is a user who is in the process of downloading the file. Once downloaded leecher can become seeder.
- **BitTorrent Client**: This is the software that users install on their devices to participate in the BitTorrent network.

BitTorrent Architecture



Protocols used in BitTorrent

- **Transmission Control Protocol)/ User Datagram Protocol** : It operates over both TCP and UDP. TCP is used for reliable data transfer, ensuring that all file pieces are successfully delivered to peers. UDP is used for faster communication and is often employed for tracking and communication with the BitTorrent tracker.

- **Tracker Protocol**: The tracker protocol is used for communication between BitTorrent clients and the centralized tracker server. It involves HTTP-based GET and POST requests, where clients announce their presence to the tracker, request a list of peers sharing the same file, and report their download progress.

- **Distributed Hash Table (DHT)**: DHT is a decentralized peer discovery protocol used in BitTorrent to enable peer-to-peer communication without relying on a central tracker. It operates over UDP and involves storing and querying peer information in a distributed hash table structure, allowing peers to discover other peers participating in the same torrent swarm.

- **Magnet Link Protocol**: These are type of URI (Uniform Resource Identifier) used to identify files available for download via BitTorrent. The Magnet link protocol specifies the format for Magnet links and how they are parsed by BitTorrent clients.

- **Peer Wire Protocol (PWP)**: The Peer Wire Protocol is a messaging protocol used between BitTorrent peers to exchange control messages and transfer file pieces. It operates over TCP and involves messages for handshaking, requesting and sending file pieces, choking and unchoking peers, and exchanging metadata such as peer and file information.

Applications using BitTorrent Protocol

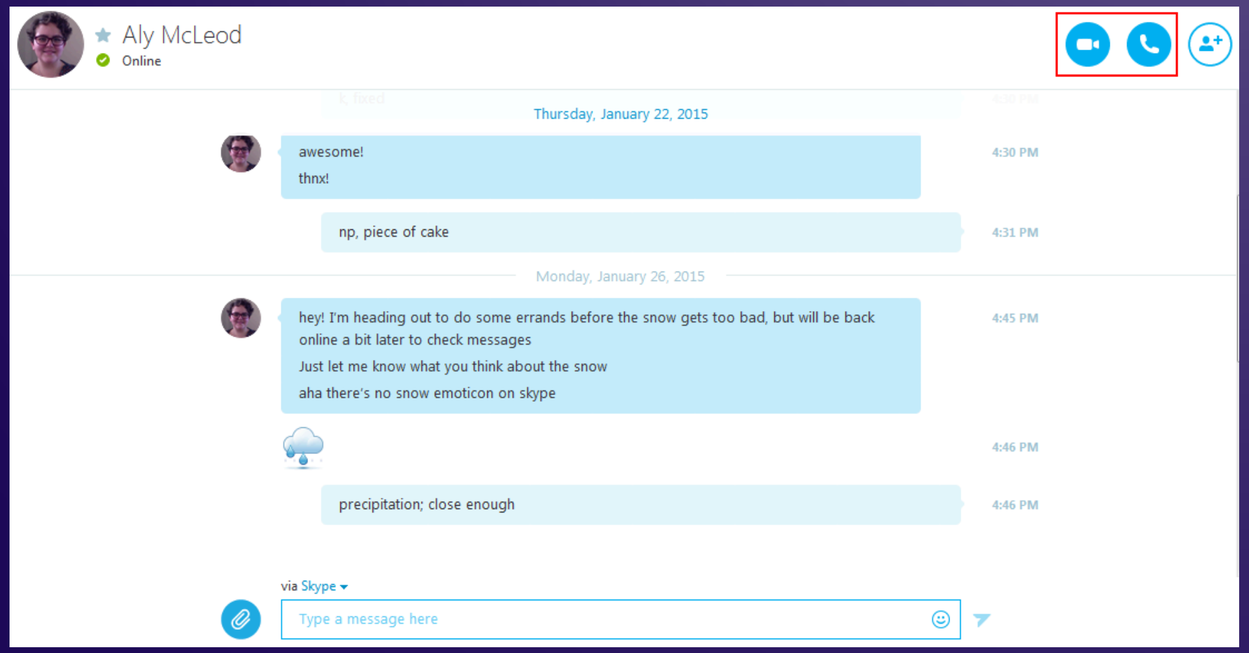
- µTorrent 
- BitTorrent 
- Libtorrent 

Skype

History and Uses

- Skype is a telecommunications application that provides video chat, voice call, and instant messaging services over the internet.
- It was created by Estonian developers Ahti Heinla, Priit Kasesalu, and Jaan Tallinn, and was released in August 2003.
- It was acquired by Microsoft in 2011. Since then it has been integrated with various Microsoft services, including Outlook, Office 365, and Xbox Live.
- Users can make free **voice calls** to other Skype users anywhere in the world. Calls between Skype users are typically free
- Users can make one on one or group **video calls** with other Skype users over internet.
- It is also used for instant messaging to other Skype users.
- Users can share files directly through Skype, sending documents, photos, videos, and other files to their contacts during conversations.
- Skype includes screen sharing features, allowing users to share their computer screens with others during calls. This is useful for collaboration, presentations, troubleshooting, and remote assistance.

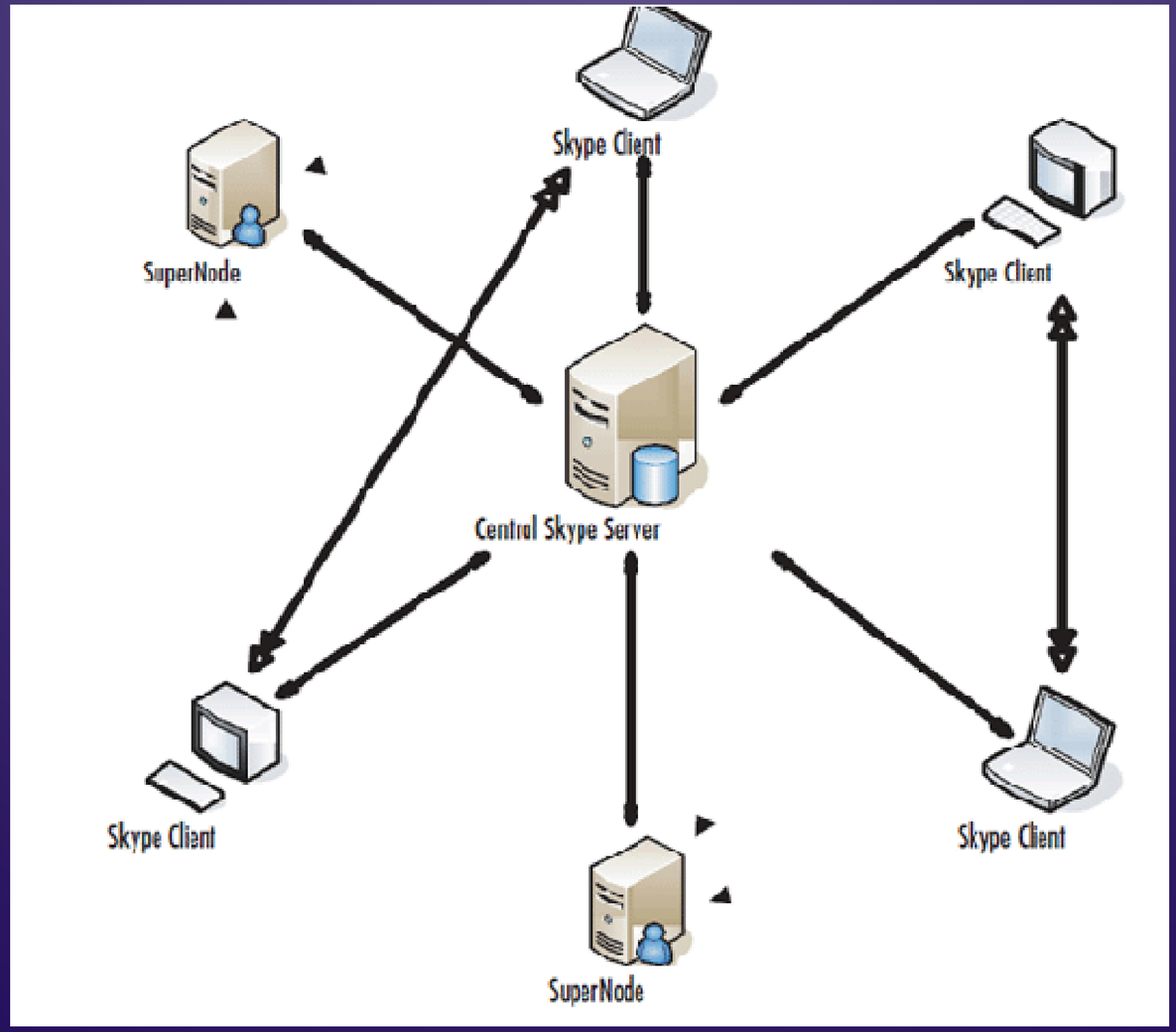
History and Uses



Skype Architecture

- **Client-Server Model**: Skype operates on a client-server architecture, where clients (Skype applications) communicate with centralized servers. This architecture enables users to connect with each other regardless of their network configurations, such as NAT (Network Address Translation) or firewall settings.
- **Peer-to-Peer (P2P) Overlay Network**: Skype used a peer-to-peer (P2P) overlay network for establishing direct connections between users. Each Skype client acted as both a client and a peer, facilitating communication and relaying data between users. But after acquisition by Microsoft P2P architecture was phased out for more centralized architecture.
- **Signaling Servers**: Microsoft operates signaling servers that handle user authentication, presence information (online status), contact lists, and routing of calls and messages. When a user logs into Skype, the client application communicates with these signaling servers to establish a connection and retrieve necessary information.
- **Media Relay Servers**: These servers relay media streams between clients, acting as intermediaries when direct peer-to-peer communication is not feasible/possible (due to NAT traversal etc.).
- **Login Servers:** These servers authenticate users and provide initial connection information to direct them to the P2P network.
- **Data Centers**: Microsoft operates a network of data centers worldwide to host Skype's backend infrastructure, including servers, databases, and other components. These data centers ensure high availability, reliability, and scalability of Skype's services.

Skype Architecture



Protocols used in Skype

- **Real-Time Transport Protocol (RTP)**: It is used for transmitting audio and video data. It is responsible for packetizing and transmitting media streams between clients during voice and video calls.
- **Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)**: Skype use TCP and UDP for various purposes, including signalling, media transmission, and file transfer. TCP is used for reliable data transmission, while UDP is often used for real-time communication to minimize latency.
- **Secure Real-Time Transport Protocol (SRTP)**: SRTP is an extension of RTP that provides encryption, message authentication, and integrity protection for voice and video data transmitted over the internet.
- **Skype Protocol (Skype's Proprietary Protocol)**: This protocol was developed by the original creators of Skype. Skype used it to handle various aspects of voice, video, and text communication between clients.

WhatsApp

History and Uses

- **WhatsApp** (officially **WhatsApp Messenger**) is an instant messaging (IM) and voice-over-IP (VoIP) application, founded in February 2009 by Brian Acton and Jan Koum.
- Meta (then Facebook) acquired WhatsApp in 2014.
- It is used for sending text messages, sharing images, videos and other files to other users.
- We can also create group chats to chat and share information with multiple users at one time.
- It allow users to make voice calls with other users. It also provide facility of making group voice calls with multiple users joining single voice call.
- It allow users to make video calls with other users, thus helping in face to face communication in real time. It also provide facility of making group video calls with multiple users joining single video call and interacting face to face with each other. This feature was added to WhatsApp in 2016
- It also provide peer-to-peer money transfer service. This feature is called WhatsApp Pay. In India, Brazil and Singapore this service is only available for business purpose.
- On November 10, 2016, WhatsApp launched a beta version of two-factor authentication for Android users, which allowed them to use their email addresses for further protection.

History and Uses

WhatsApp Architecture

- **Client Applications**: These are installed by users in there systems. These client applications allow users to send messages, make calls, and access other features of the platform.

- **WhatsApp Servers**: These are network of servers that handle various functions such as message routing, user authentication, presence management, and encryption. These servers are responsible for processing and delivering messages between users in real-time.

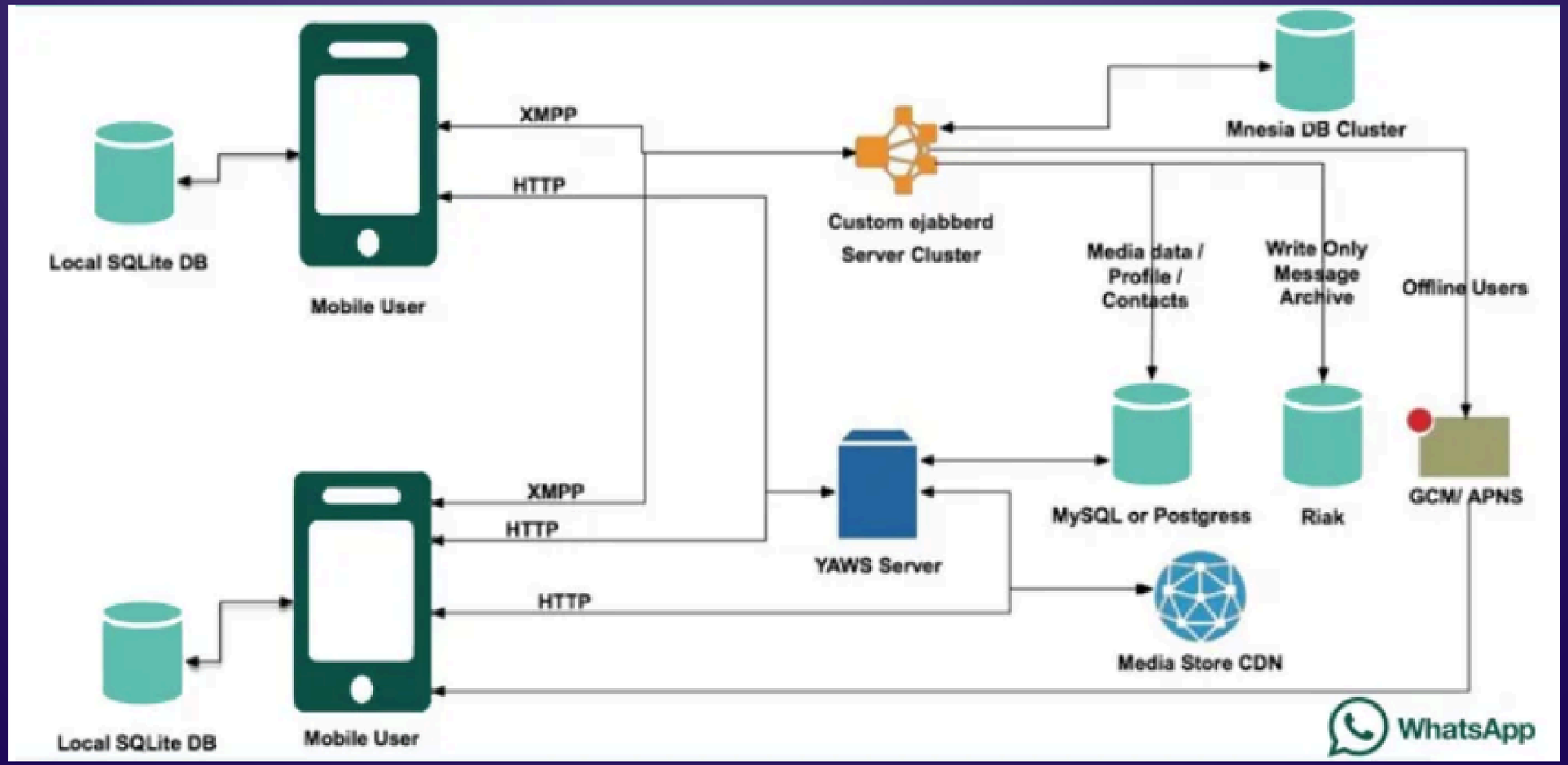
- **Voice and Video Calling Infrastructure**: It includes signaling servers, relay servers, and peer-to-peer (P2P) communication channels. These components facilitate the establishment of audio/video connections between users and ensure smooth communication during calls.

- **Messaging Infrastructure**: It includes components for message queuing, delivery, and synchronization across devices. It ensures that messages are reliably delivered to recipients, even in challenging network conditions.

- **Encryption Layer**: It implements end-to-end encryption for all messages and calls. This layer ensures that only the sender and receiver can access the content of the messages, providing privacy and security for users.

- **Backup and Synchronization Services**: These services involve securely storing encrypted backups in the cloud and synchronizing data between devices. These are used as backups and used to restore chat history.

WhatsApp Architecture

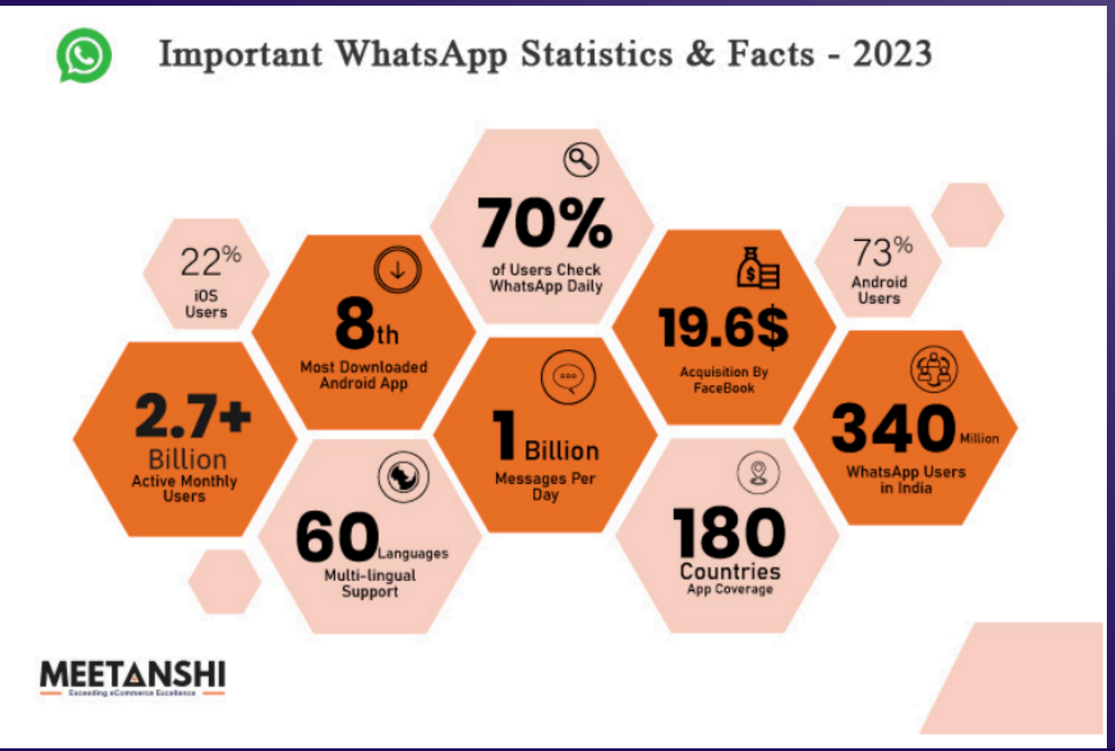


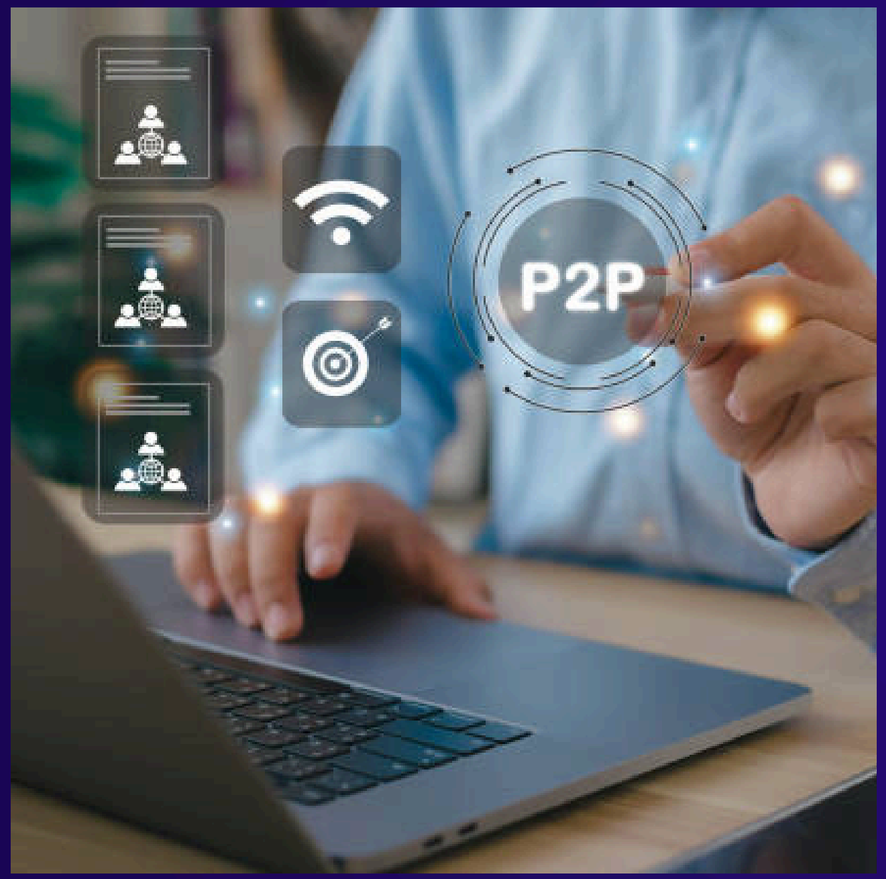
Protocols Used by Whatsapp

- **Client-Server Model**: WhatsApp follows a client-server architecture, where the client applications (installed on users' devices) communicate with WhatsApp servers over the internet.
- **Messaging Protocol**: It is a proprietary messaging protocol for communication between clients and servers. This protocol is optimized for real-time messaging and supports features like text messages, voice messages, images, videos, documents, and more.
- **Secure Real-Time Transport Protocol (SRTP)**: It is used to secure the transmission of audio and video data in voice and video calls. It provides encryption, authentication, and integrity protection for real-time multimedia communication.
- **Voice and Video Calling Infrastructure**: For voice and video calls, WhatsApp utilizes a combination of peer-to-peer (P2P) communication and relay servers to establish connections between users and facilitate audio/video streaming.
- **Content Delivery Network (CDN)**: It is used to efficiently deliver media content such as images, videos, and documents.

STATISTCS

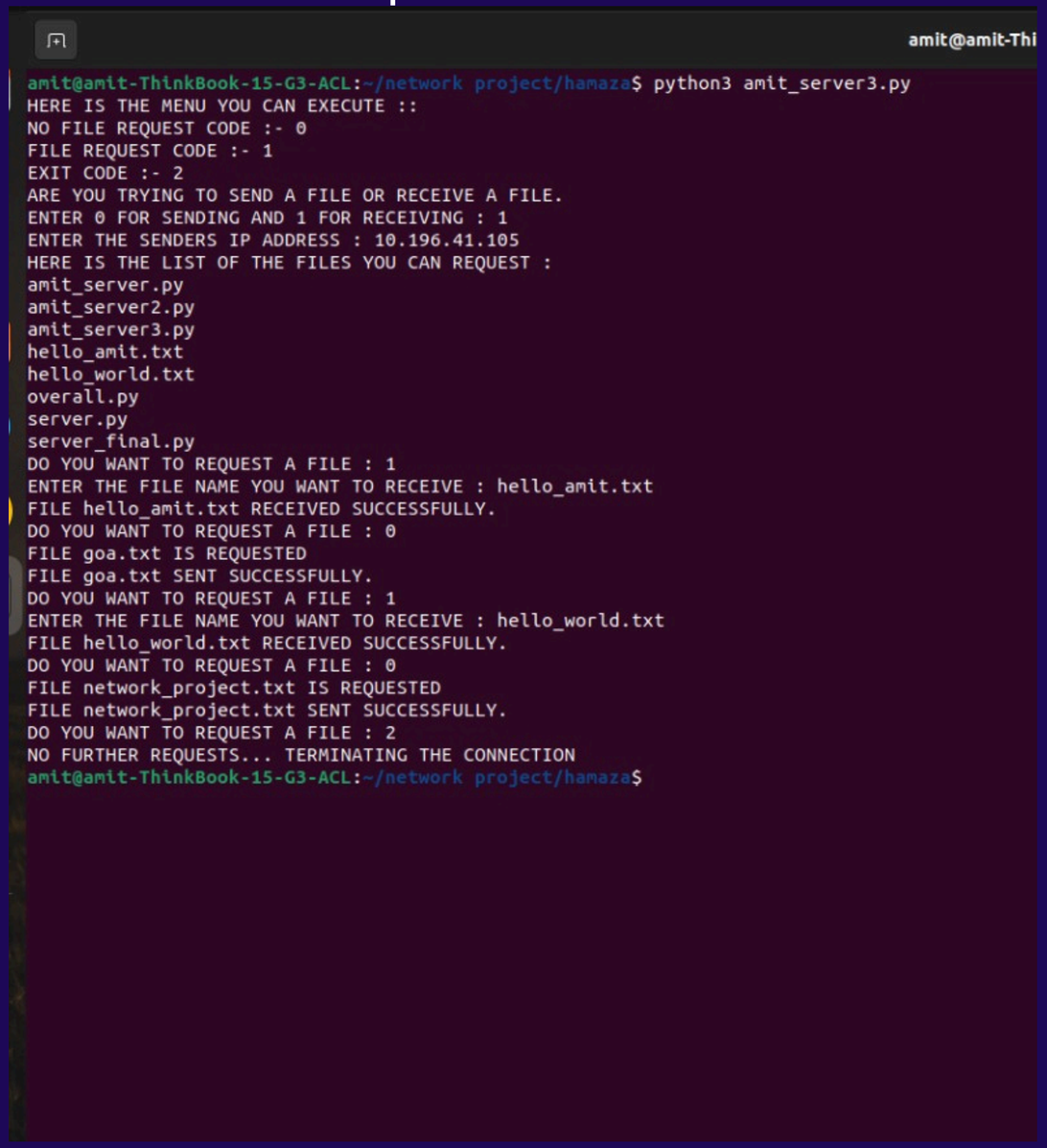
- It has more than 2 billion monthly active users by 2020.
- By 2020 number of messages sent per day crossed 100 billion.
- It is second most popular messaging app after Facebook .



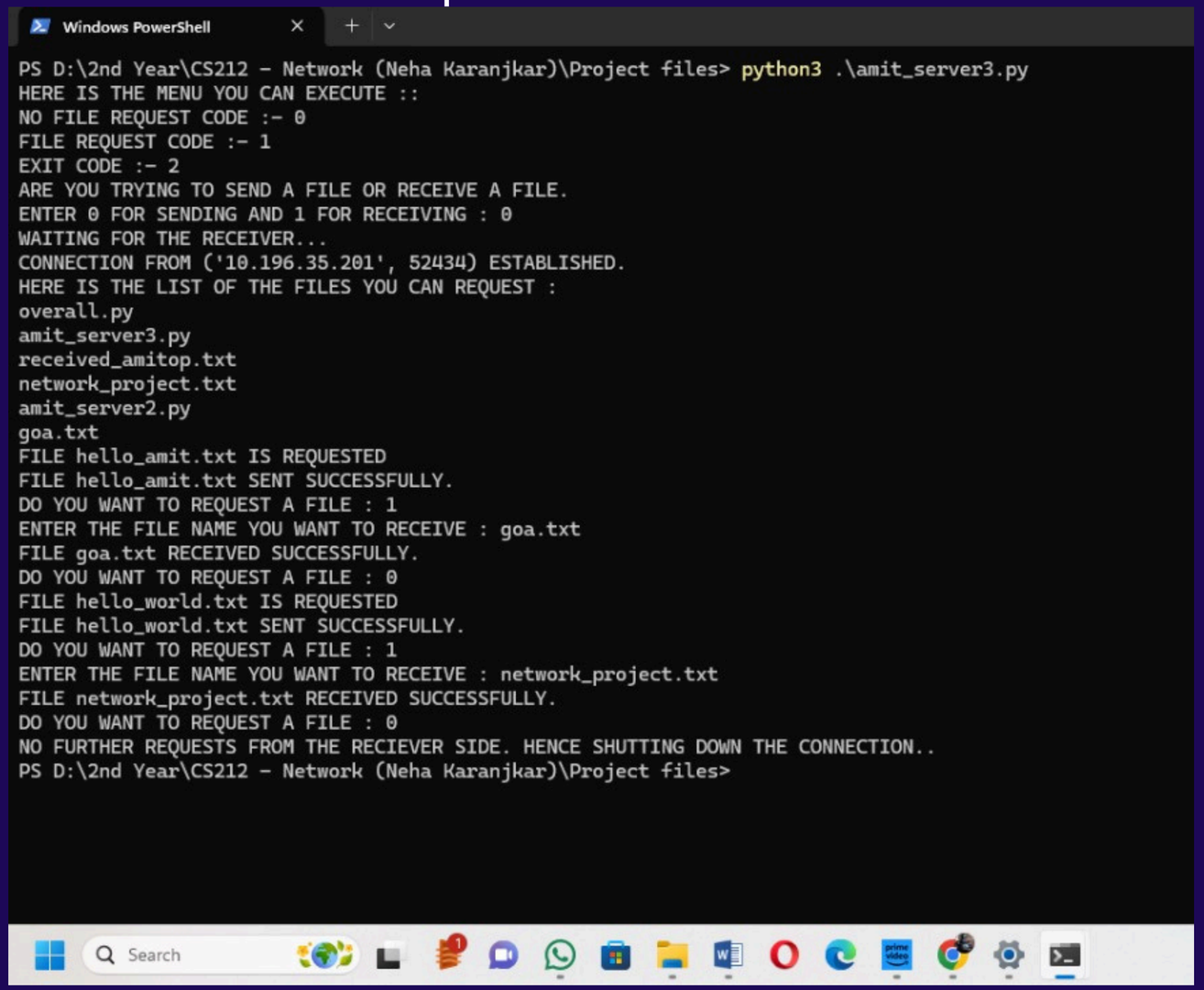


06
Demo

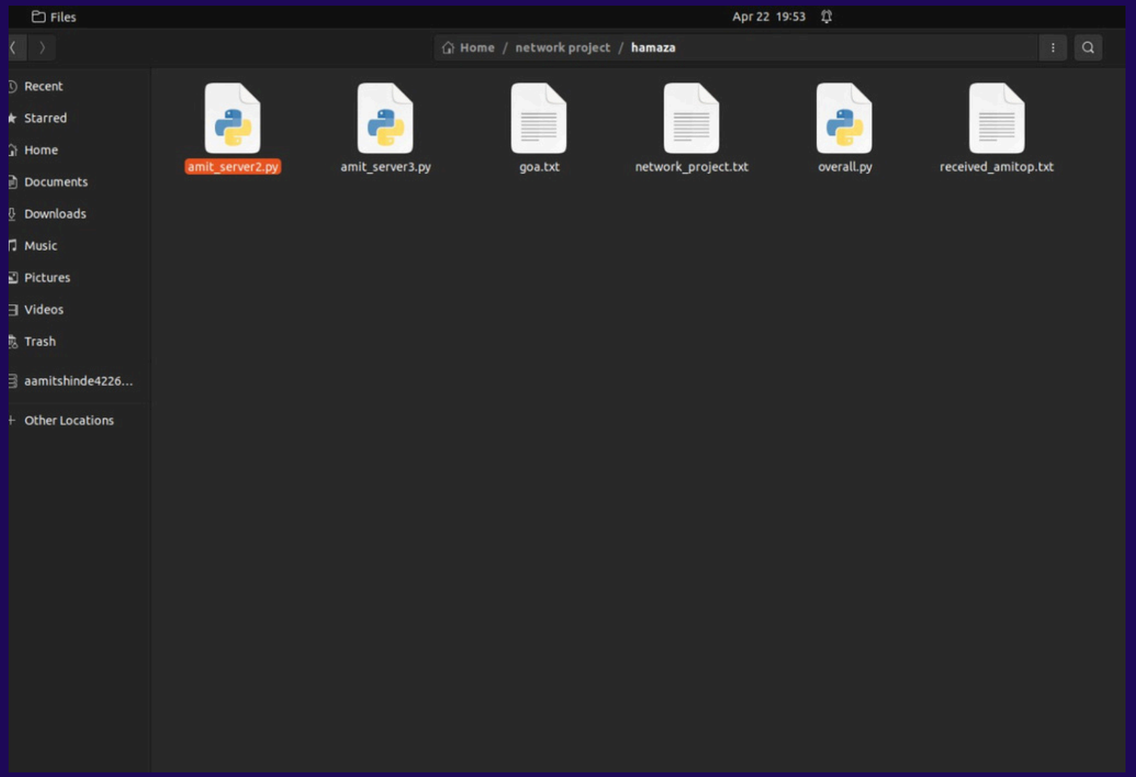
computer 1



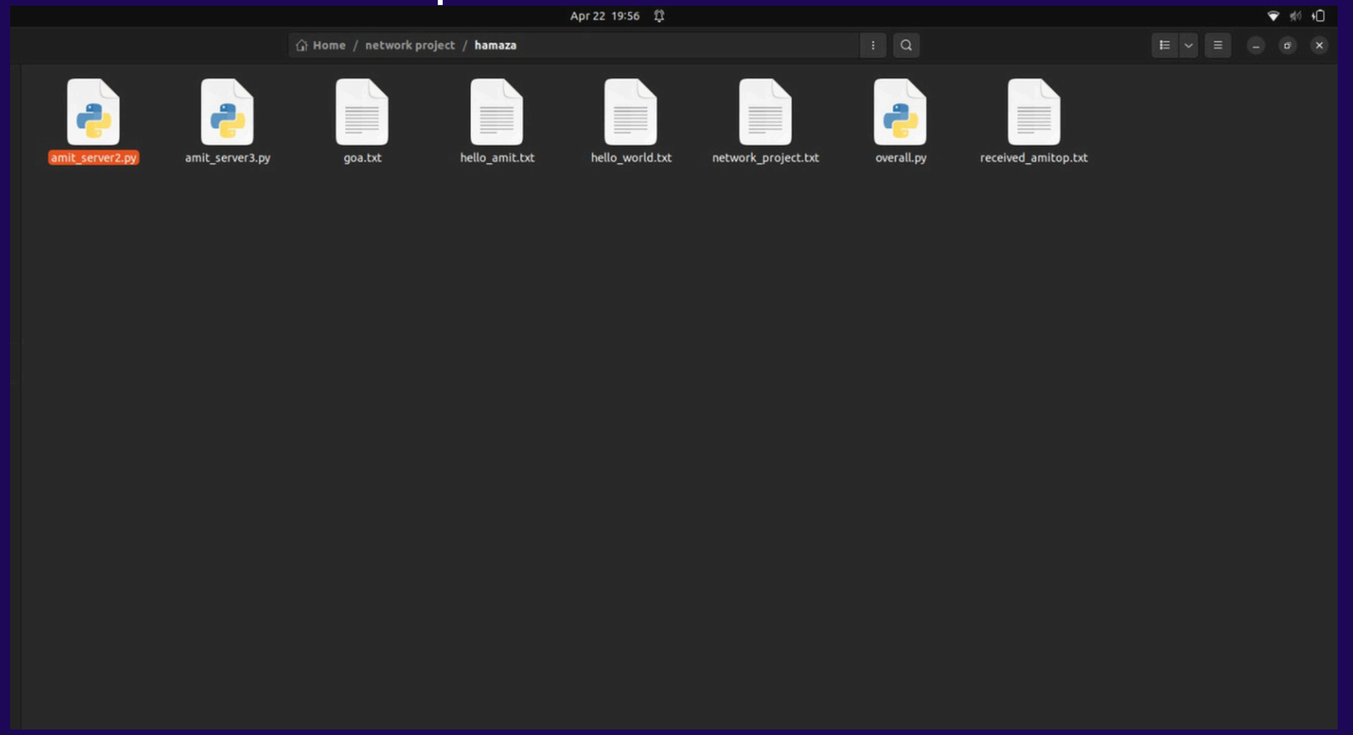
computer 2



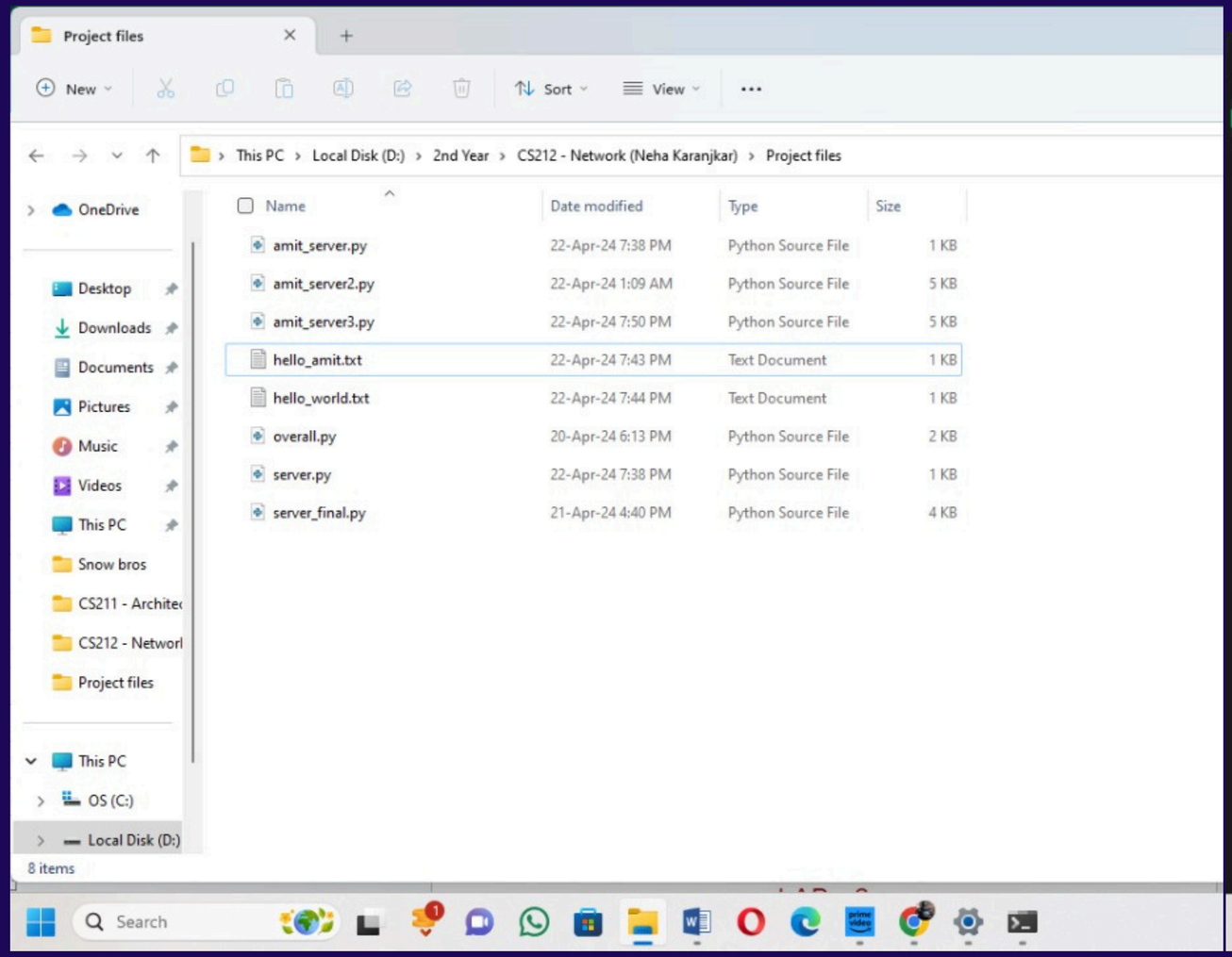
computer 1 before



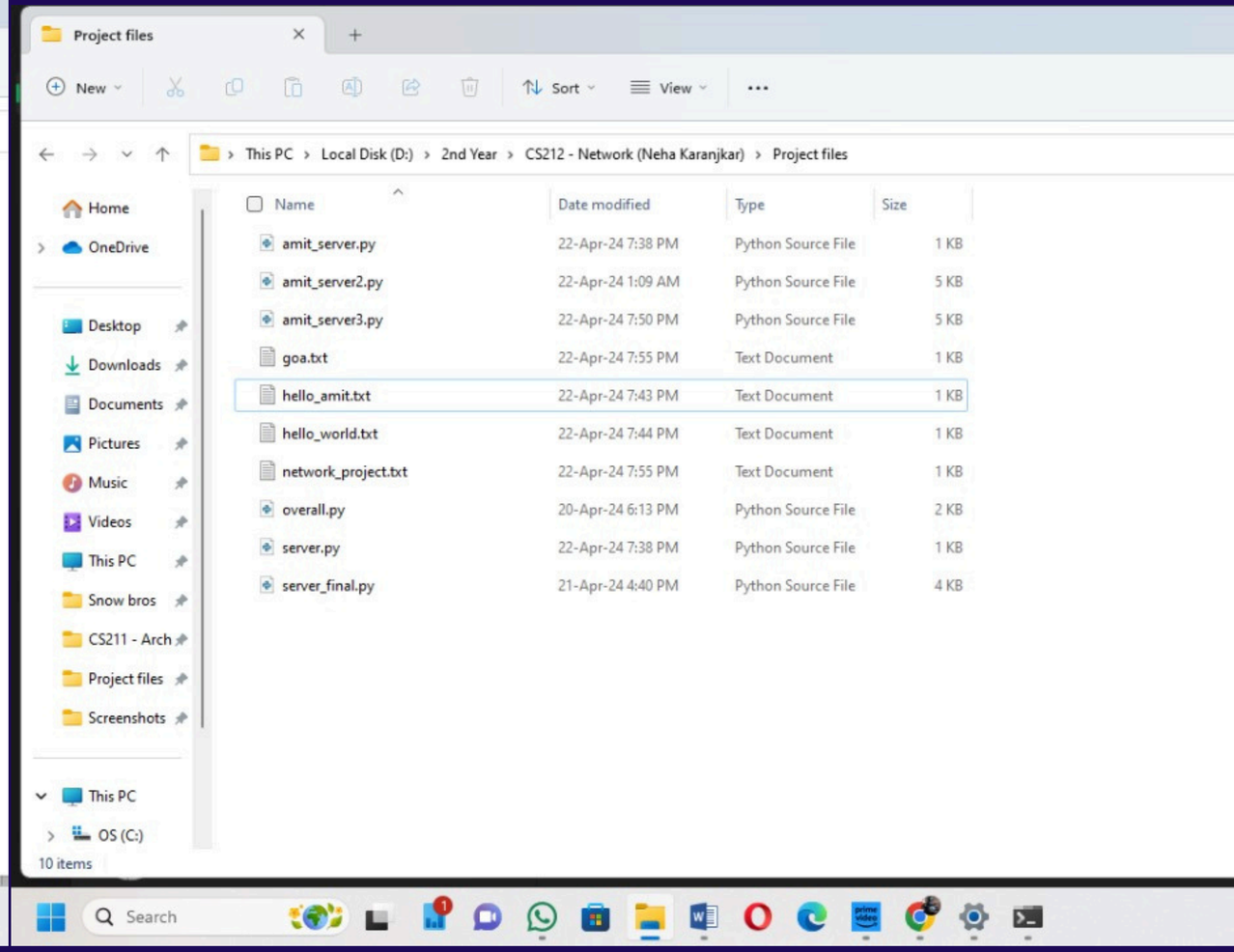
computer 1 after



computer 2 before



computer 2 after



Refrences

- https://en.wikipedia.org/wiki/WhatsApp
- https://backlinko.com/whatsapp-users
- https://en.wikipedia.org/wiki/Skype
- https://learn.microsoft.com/en-us/skypeforbusiness/plan-your-deployment/network-requirements/ports-and-protocols
- https://www.geeksforgeeks.org/network-address-translation-nat/