Network Foundations

Introduction to Networks

Network Foundations mein aapka swagat hai! Is introductory module mein hum computer networking ke peeche ki technology ke baare mein jaanenge. Computer networking ko “networking” ya “networks” bhi kaha jaata hai, aur hum samjhenge ki yeh hamari zindagi ke liye kyun zaroori hai. Hum mainly do tarah ke networks par focus karenge: `Local Area Networks (LANs)` aur `Wide Area Networks (WANs)`.

Yeh samajhna ki devices ek-doosre ke saath kaise communicate karti hain, chahe woh hamare ghar ke andar hon ya poori duniya mein, un logon ke liye basic aur zaroori knowledge hai jo Cyber Security ke field mein aana chahte hain. Aaj ki duniya mein lagbhag har device ek-doosre se connected hai. Isi wajah se security professionals ki demand lagataar badh rahi hai.

What is a Network?

`Network` interconnected devices ka ek collection hota hai, jo ek-doosre ke saath communicate kar sakte hain. Yaani data send aur receive kar sakte hain, aur ek-doosre ke saath resources bhi share kar sakte hain.

In individual devices ko, jo network ke endpoints hote hain, aksar `nodes` kaha jaata hai. Inmein computers, smartphones, printers aur servers shaamil hain.

Lekin, sirf `nodes` se poora network nahi banta. Neeche di gayi table mein networking ke kuch important concepts diye gaye hain.

Concepts	Description
Nodes	Network se connected individual devices.

Links	Woh communication pathways jo nodes ko connect karte hain, chahe wired hon ya wireless.
Data Sharing	Network ka main purpose data ko ek-doosre ke saath exchange karna hai.

Chalo, upar di gayi baat ko ek real-world example se samajhte hain.

Socho, kuch dost ek room mein baithkar aapas mein baatein kar rahe hain. Har person ek device (`node`) ko represent karta hai, aur unka ek-doosre se baat kar paana aur sun paana `communication links` ko represent karta hai.

Unke beech jo conversation ho rahi hai, woh share kiya jaane wala `data` hai

---

Why Are Networks Important?

Networks ne, khaaskar Internet ke aane ke baad, hamare samaj ko poori tarah badal diya hai. Inhone bahut saari aisi possibilities ko possible banaya hai, jo aaj hamari zindagi ka zaroori hissa ban chuki hain.

Neeche is amazing technology ke kuch fayde diye gaye hain.

Function	Description
Resource Sharing	Ek se zyada devices hardware (jaise printers) aur software resources ko share kar sakti hain.
Communication	Instant messaging, emails aur video calls networks ki madad se kaam karte hain.
Data Access	Kisi bhi connected device se files aur databases ko access kar sakte hain.

Collaboration	Door-door rehkar bhi log real-time mein ek saath kaam kar sakte hain.

Types of Networks

Networks ka size aur coverage alag-alag hota hai. Do main types ke networks hote hain: `Local Area Network (LAN)` aur `Wide Area Network (WAN)`.

Local Area Network (LAN)

`Local Area Network (LAN)` devices ko ek chhoti distance ke andar connect karta hai, jaise ghar, school ya kisi chhote office building ke andar.

Iski kuch important characteristics neeche di gayi hain:

Characteristic	Description
Geographical Scope	Ek chhote area ko cover karta hai.
Ownership	Aam taur par ek hi person ya organization iska owner hota hai aur ise manage karta hai.
Speed	Ismein data transfer ki speed zyada hoti hai.
Media	Wired connection (Ethernet cables) ya wireless connection (Wi-Fi) ka use karta hai.

LAN aur WAN

Aspect	LAN	WAN
Size	Chhota area cover karta hai.	Bada area cover karta hai.
Ownership	Ek person ya organization ka hota hai.	Kai organizations ya service providers ka hota hai.
Speed	Zyada hoti hai.	LAN ke comparison mein kam hoti hai.
Maintenance	Manage karna aasaan aur kam kharchila hota hai.	Manage karna complex aur mehenga hota hai.
Example	Ghar ya office ka network.	Internet.

How Do LANs and WANs Work Together?

Local Area Networks (LANs), Wide Area Networks (WANs) se connect ho sakte hain, taaki apne chhote area se bahar ke bade networks ko access kar sakein. Is connectivity se communication aur resources sharing bahut bade level par possible ho jaati hai.

Example ke liye, jab hum Internet access karte hain, toh hamare ghar ka LAN, `Internet Service Provider (ISP)` ke WAN se connect hota hai. Isse ghar ke network mein connected sabhi devices ko Internet access milta hai. ISP ek aisi company hoti hai jo individuals aur organizations ko Internet access provide karti hai.

Is setup mein `modem (modulator-demodulator)` naam ka device important role play karta hai. Modem aapke home network aur ISP ke infrastructure ke beech bridge ka kaam karta hai. Yeh aapke router se aane wale digital signals ko aise format mein convert karta hai, jise telephone lines, cable systems aur fiber optics jaise alag-alag mediums ke through transmit kiya ja sake.

Yeh connection ek simple local network ko online available resources tak pahunchne ka raasta bana deta hai.

Business ke environment mein, companies apne multiple offices ke LANs ko WAN ke through connect karti hain, taaki alag-alag geographical locations par communication aur collaboration ek saath ho sake.

In LANs ko WAN ke through connect karne se, alag-alag offices ke employees information share kar sakte hain, centralized databases access kar sakte hain aur real-time mein ek saath kaam kar sakte hain. Isse organization ki productivity badhti hai.

Chalo, ek example se samajhte hain ki LAN aur WAN ek saath kaise kaam karte hain.

Ghar par hamare devices, jaise laptops, smartphones aur tablets, home router se connect hote hain. Isse ek LAN banta hai.

Yeh router sirf local network ke traffic ko manage nahi karta, balki hamare ISP ke WAN se bhi communicate karta hai.

WAN se connect hone ke baad, hamara home network duniya bhar mein hosted websites aur online services ko access kar sakta hai.

LAN aur WAN ka yeh smooth connection humein duniya bhar ka online content access karne aur apne local network se bahar ki services ke saath interact karne ki suvidha deta hai.

Answer questions in English to ensure an accurate response.

Q. What is the term for a collection of interconnected devices that can communicate and share resources with each other?

Ans. Network

Q. What is the term for a collection of interconnected devices that can communicate and share resources with each other?

Ans. Nodes

Q. What is the largest Wide Area Network (WAN) that connects millions of Local Area Networks (LANs) globally?

Ans. Internet

What is the acronym for a network that connects devices over a short distance, such as within a home, school, or small office building?

Ans. Lan

In networking, what term describes the communication pathways (wired or wireless) that connect nodes?

Ans. links

Network Concepts

Networking ke peeche ki basic technology ko samajhna bina kisi shak ke important hai. Lekin, bahut se logon ko pata nahi hai ki networking aaj hamari zindagi mein kitni zyada common ho gayi hai. Aaj hum jo complex technology use karte hain — jaise consumer electronics, multimedia devices, hardware, software aur firmware — yeh sab `TCP/IP` stack ke saath milkar ya uske upar build ki gayi hain.

Iske alawa, is section mein hum kuch important concepts cover karenge, jo samajhne mein madad karenge ki networking, technology ki poori duniya mein kaise fit hoti hai.

Hum `OSI` aur `TCP/IP` models, data exchange ke liye standards ke roop mein use hone wale kuch common network protocols, aur alag-alag `transmission methods` ke baare mein padhenge.

Yeh transmission methods information ko network ke through efficiently aur securely ek jagah se doosri jagah pahunchane mein madad karte hain.

OSI Model

Open Systems Interconnection (OSI) Model ek conceptual framework hai, jo telecommunication ya computer system ke functions ko 7 alag-alag layers mein divide karta hai. Is model ki madad se different companies ke developers aise network devices aur software bana sakte hain, jo ek-doosre ke saath kaam kar sakein.

Neeche OSI Model ki 7 layers di gayi hain.

Physical Layer (Layer 1)

`Physical Layer` OSI Model ki sabse pehli aur sabse neeche wali layer hai. Iska kaam raw bits (0 aur 1) ko physical medium ke through transmit karna hai.

Yeh devices ke beech physical connection ko handle karti hai. Ismein Ethernet cables, hubs aur repeaters jaise hardware components shaamil hain.

Data Link Layer (Layer 2)

`Data Link Layer` do directly connected nodes ke beech data transfer karti hai. Yeh ensure karti hai ki data frames sahi synchronization ke saath transmit hon aur errors ko detect aur correct kiya ja sake.

Switches aur bridges jaise devices is layer par kaam karte hain. Yeh network devices ko identify karne ke liye `MAC (Media Access Control) addresses` ka use karte hain.

Network Layer (Layer 3)

`Network Layer` data packets ko forward karne ka kaam karti hai. Ismein packets ko alag-alag routers ke through destination network tak pahunchane ke liye routing ki jaati hai.

Yeh logical addressing aur data ke liye sahi path decide karti hai, taaki data multiple networks se hote hue sahi destination tak pahunche.

Routers is layer par kaam karte hain. Yeh devices ko identify karne aur data bhejne ke liye suitable path decide karne mein `IP (Internet Protocol) addresses` ka use karte hain.

Transport Layer (Layer 4)

`Transport Layer` applications ke beech end-to-end communication provide karti hai.

Iske kaamon mein data ko reliable ya unreliable tareeke se deliver karna, data ko chhote parts mein divide karna (segmentation), dobara jodna (reassembly), flow control aur error checking shaamil hain.

Is layer par `TCP (Transmission Control Protocol)` aur `UDP (User Datagram Protocol)` jaise protocols kaam karte hain.

TCP reliable aur connection-oriented data transmission provide karta hai, jisme errors ko recover karne ki facility hoti hai. Wahin UDP faster, connectionless communication provide karta hai, jisme data delivery ki guarantee nahi hoti.

Session Layer (Layer 5)

`Session Layer` applications ke beech sessions ko manage karti hai.

Yeh connections ko establish, maintain aur terminate karti hai, jisse devices ke beech communication jaari reh sakta hai. Is communication ko session kaha jaata hai.

Yeh session checkpointing aur recovery mein bhi important hai, taaki connection interrupt hone ke baad data transfer dobara continue kiya ja sake.

Is layer par kaam karne wale protocols aur `APIs (Application Programming Interfaces)` different systems aur applications ke beech communication coordinate karte hain.

Presentation Layer (Layer 6)

`Presentation Layer`, Application Layer aur network ke data format ke beech translator ki tarah kaam karti hai.

Yeh data ko aise format mein represent karti hai ki ek system ki application se bheji gayi information doosre system ki application samajh sake.

Iske kaamon mein data encryption aur decryption, data compression aur data formats ko convert karna shaamil hai.

Encryption protocols aur data compression techniques data transmission ko secure aur efficient banane mein madad karti hain.

Application Layer (Layer 7)

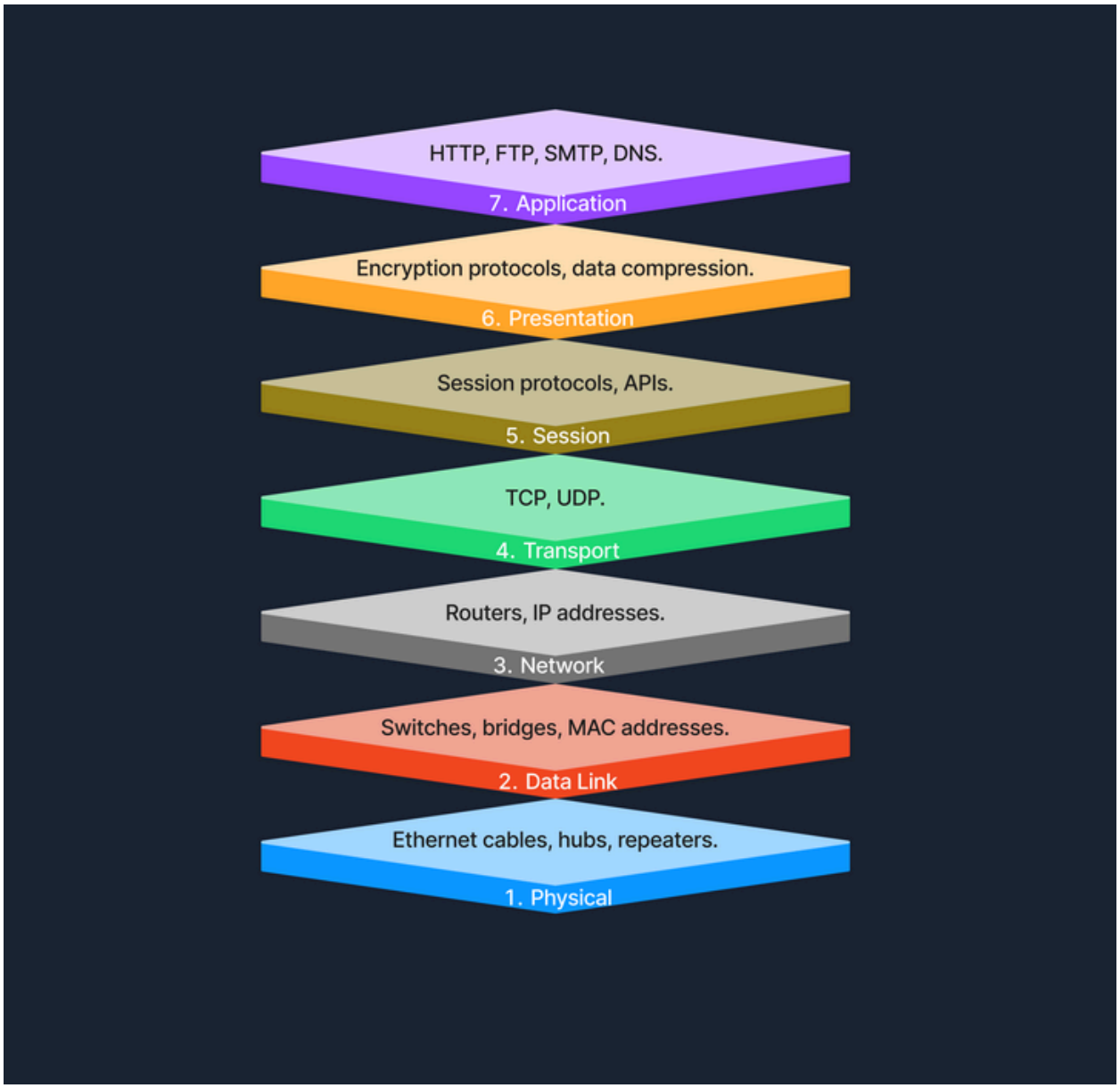
`Application Layer` OSI Model ki sabse upar wali layer hai. Yeh end-user applications ko directly network services provide karti hai.

Yeh resource sharing, remote files ko access karna aur doosri network services provide karti hai.

Is layer par use hone wale kuch common protocols hain:

- `HTTP (Hypertext Transfer Protocol)` — websites browse karne ke liye.
- `FTP (File Transfer Protocol)` — files transfer karne ke liye.
- `SMTP (Simple Mail Transfer Protocol)` — emails bhejne ke liye.
- `DNS (Domain Name System)` — domain names ko IP addresses mein resolve karne ke liye.

Yeh layer network aur application software ke beech interface ka kaam karti hai.



Example of sending a File across the Network layer

Jab hum network ke through koi file bhejte hain, toh network model ki alag-alag layers mein kai steps hote hain. Yeh process Application Layer se shuru hota hai, jo file transfer karne ki request start karti hai.

Iske baad, Presentation Layer file ko transmission ke dauran secure rakhne ke liye encrypt karti hai. Phir Session Layer, file bhejne wale device aur receive karne wale device ke beech communication session establish karti hai.

Transport Layer par file ko chhote-chhote segments mein divide kiya jata hai, taaki data ko sahi tarike se transfer kiya ja sake aur transmission mein hone wali errors ko handle kiya ja sake.

Phir Network Layer network ke through data transfer karne ke liye sabse achha route decide karti hai. Iske baad, Data Link Layer data ko frames mein pack karti hai, taaki use ek network node se doosre node tak bheja ja sake.

Aakhir mein, Physical Layer physical medium ke through bits ko transmit karti hai. Is tarah file bhejne ka process poora hota hai.

TCP/IP Model

`Transmission Control Protocol/Internet Protocol (TCP/IP) Model`, OSI Model ka ek simplified version hai, jise internet aur doosre networks par practically use karne ke liye banaya gaya hai. Neeche TCP/IP Model ki 4 layers di gayi hain.

1. Link Layer

Yeh layer network hardware aur media ke physical aspects ko handle karti hai. Ismein wired connections ke liye Ethernet aur wireless connections ke liye Wi-Fi jaisi technologies shamil hain.

Link Layer, OSI Model ki Physical Layer aur Data Link Layer ke barabar hoti hai. Yeh physical connection se lekar data ko frames mein pack karne tak ke kaam handle karti hai.

2. Internet Layer

Internet Layer devices ki logical addressing aur alag-alag networks ke beech packets ki routing ko manage karti hai.

IP (Internet Protocol) aur ICMP (Internet Control Message Protocol) jaise protocols is layer par kaam karte hain. Yeh ensure karte hain ki packets ke transmission ke liye logical paths decide karke data ko uski destination tak pahunchaya ja sake.

Yeh layer OSI Model ki Network Layer ke barabar hoti hai.

3. Transport Layer

TCP/IP Model ki Transport Layer internet par end-to-end communication services provide karti hai, jo internet ke kaam karne ke liye zaroori hain.

Ismein reliable communication ke liye TCP (Transmission Control Protocol) aur fast, connectionless communication ke liye UDP (User Datagram Protocol) ka use hota hai.

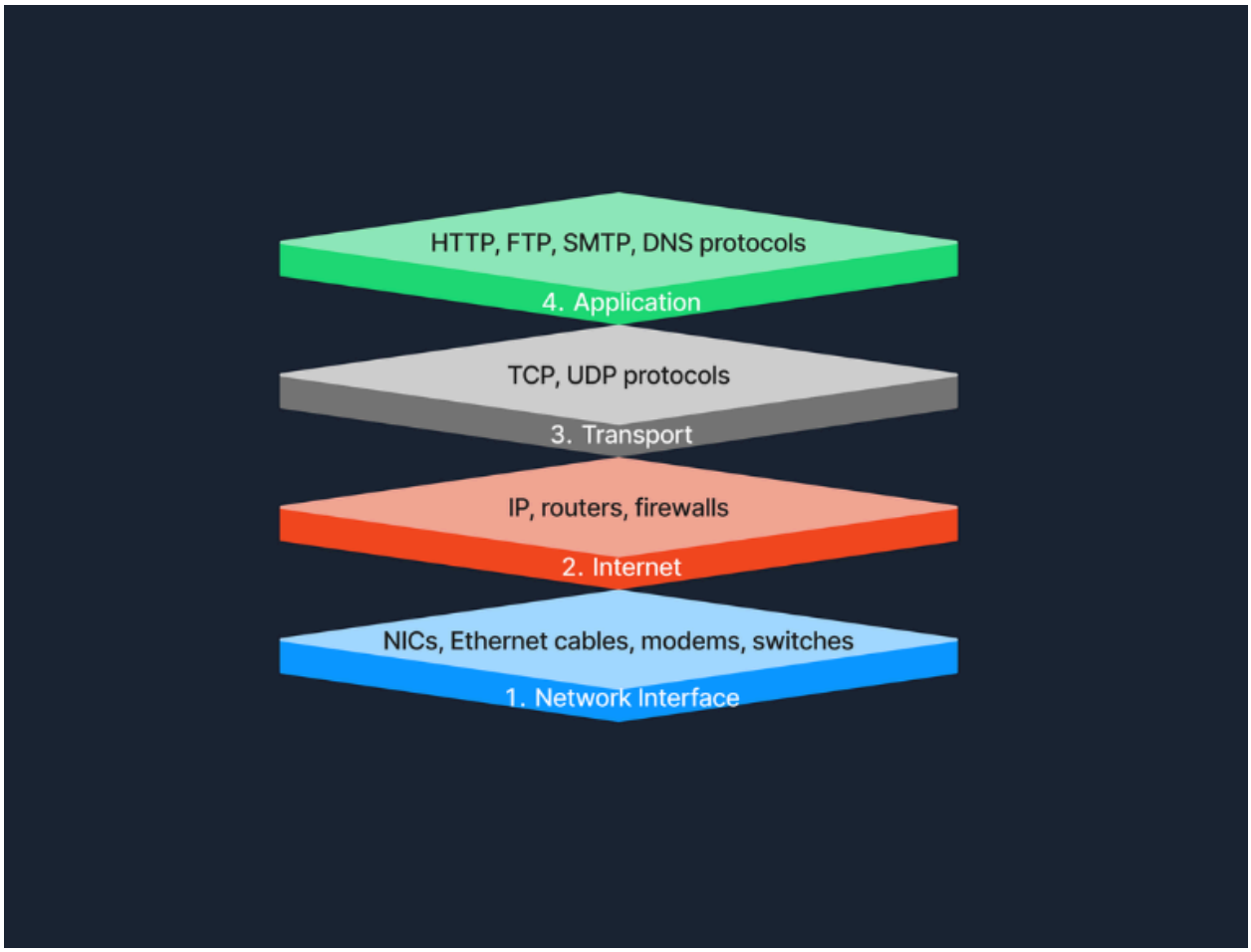
Yeh layer data packets ko sahi order mein deliver karne aur transmission errors ko handle karne mein madad karti hai. Yeh OSI Model ki Transport Layer ke barabar hoti hai.

4. Application Layer

TCP/IP Model ki Application Layer mein aise protocols hote hain jo applications ko specific data communication services provide karte hain.

HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol) aur SMTP (Simple Mail Transfer Protocol) jaise protocols web browsing, file transfer aur email services jaisi functionalities provide karte hain.

Yeh layer OSI Model ki upar ki teen layers — Session, Presentation aur Application — ke barabar hoti hai. Yeh systems ke beech data exchange karne ke liye zaroori interfaces aur protocols provide karti hai.

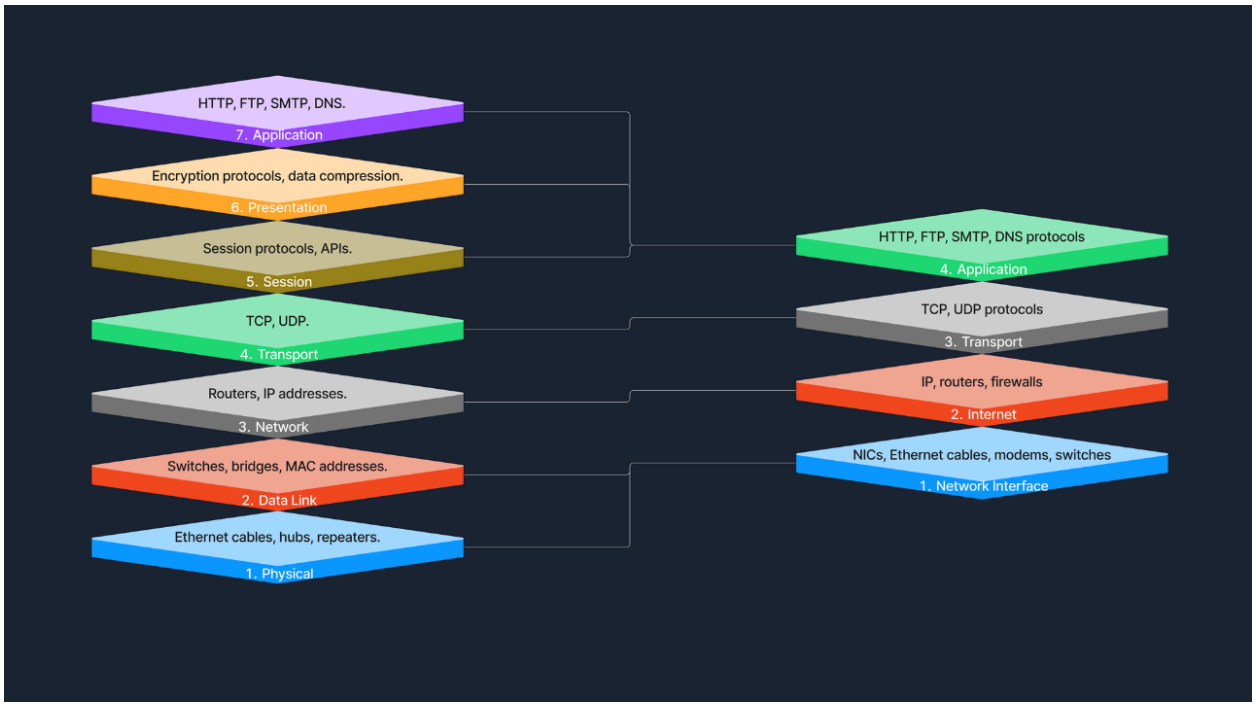


Comparison with OSI Model

TCP/IP Model, OSI Model ki complex structure ko simple banata hai. Iske liye kuch layers ko combine kiya gaya hai, taaki ise practically implement karna aasaan ho.

TCP/IP Model ko khaas taur par internet mein use hone wale protocols ko dhyan mein rakhkar banaya gaya hai. Yeh applications ki zarooraton par zyada focus karta hai aur real-world network communication ke liye design kiya gaya hai.

Is design ki wajah se TCP/IP Model internet ke through data exchange karne mein zyada effective hai aur modern technology ki zarooraton ko poora karta hai.



Example of Accessing a website

Jab hum kisi website ko access karte hain, toh TCP/IP Model ki kai layers milkar is process ko poora karti hain.

Application Layer par, hamara browser webpage ko request karne ke liye HTTP ka use karta hai.

Yeh request phir Transport Layer par jaati hai, jahan TCP data ko reliably transfer karna ensure karta hai.

Iske baad Internet Layer kaam karti hai, jahan IP hamare device se web server tak data packets ko route karne ka kaam karta hai.

Aakhir mein, Link Layer par data network ke through physically transmit hota hai. Is tarah connection establish hota hai aur hum website ko dekh paate hain.

Model ke Roles (Kaam)

Practical terms mein, TCP/IP Model network ke through data transmission ki backbone hai. Iska use alag-alag networking environments mein kiya jata hai.

Doosri taraf, OSI Model ko directly implement karne ke bajaye, ek detailed theoretical framework ke roop mein use kiya jata hai. Yeh network operations ki complexity ko samajhne mein madad karta hai aur ek clear, structured tareeka deta hai, jisse hum samajh sakte hain ki networks kaise kaam karte hain.

Dono models milkar networking ko poori tarah samajhne mein madad karte hain. TCP/IP Model practical application ko samjhata hai, jabki OSI Model networking ke concepts ko theoretically samajhne mein help karta hai.

Protocols

`Protocols` standard rules hote hain, jo decide karte hain ki network mein devices ke beech communication karne ke liye data ka format kaisa hoga aur usko process kaise kiya jayega.

Ye protocols network models ki alag-alag layers par kaam karte hain. Har protocol ko data aur communication ki specific zarooraton ko handle karne ke liye banaya gaya hai.

Neeche kuch common network protocols aur data exchange mein unke kaam diye gaye hain.

Common Network Protocols (आम नेटवर्क प्रोटोकॉल)

Network protocols yeh define karne ke liye zaroori hote hain ki networks ke beech data ka exchange kaise hoga. Har protocol OSI Model ki ek specific layer par kaam karta hai, jisse data ko sahi tarike se aur efficiently handle kiya ja sake.

Protocol	Description (Kaam)
HTTP (Hypertext Transfer Protocol)	Mainly web pages transfer karne ke liye use hota hai. Yeh Application Layer par kaam karta hai aur browser aur server ko web content deliver karne ke liye communicate karne deta hai.

FTP (File Transfer Protocol)	Alag-alag systems ke beech files transfer karne mein help karta hai. Yeh bhi Application Layer par kaam karta hai. Iski help se users server par files upload ya server se download kar sakte hain.
SMTP (Simple Mail Transfer Protocol)	Email bhejne ke liye use hota hai. Yeh Application Layer par kaam karta hai aur ek server se doosre server tak email messages bhejne ki zimmedari sambhalta hai, taaki messages intended recipients tak pahunch sakein.
TCP (Transmission Control Protocol)	Error checking aur recovery ki help se data ko reliably transfer karta hai. Yeh Transport Layer par kaam karta hai. Sender aur receiver ke beech connection establish karta hai, taaki data sahi order mein deliver ho.
UDP (User Datagram Protocol)	Fast, connectionless communication provide karta hai. Ismein TCP ki tarah built-in error recovery nahi hoti. Isliye yeh un applications ke liye useful hai jinmein speed zyada important hoti hai, jaise streaming services. UDP Transport Layer par kaam karta hai.
IP (Internet Protocol)	Alag-alag networks ke beech data packets ko route karne ke liye important hai. Yeh Internet Layer par kaam karta hai aur packets ki addressing aur routing handle karta hai, taaki data source se destination tak pahunch sake.

Transmission (डेटा ट्रांसमिशन)

Networking mein `Transmission` ka matlab hai data signals ko ek device se doosre device tak kisi medium ke through bhejna.

Is concept ko achhe se samajhne ke liye, hum transmission ke alag-alag types, data bhejne ke modes aur signals ko carry karne wale media ko samjhenge.

Transmission Types (ट्रांसमिशन के प्रकार**)**

Networking mein transmission ko do main types mein divide kiya ja sakta hai: Analog aur Digital.

Analog Transmission: Ismein information ko represent karne ke liye continuous signals ka use hota hai. Iska common example traditional radio broadcasting hai.

Digital Transmission: Ismein data ko represent karne ke liye alag-alag discrete signals, yaani bits (0 aur 1), ka use hota hai. Iska use modern communication technologies mein hota hai, jaise computer networks aur digital telephony.

Transmission Modes (डेटा भेजने के तरीके)

Transmission modes define karte hain ki do devices ke beech data kis tarah bheja jata hai.

- Simplex Mode: Ismein communication sirf ek direction mein hota hai. Jaise keyboard se computer tak signals jana.
- Half-duplex Mode: Ismein dono directions mein communication ho sakta hai, lekin ek hi samay par nahi. Jaise walkie-talkie, jahan users ko baari-baari se bolna padta hai.
- Full-duplex Mode: Ismein dono directions mein ek hi samay par communication ho sakta hai. Jaise telephone call, jahan dono log ek saath bol bhi sakte hain aur sun bhi sakte hain.

Transmission Media (डेटा भेजने के माध्यम)

Network mein jis physical medium ke through data transmit hota hai, use `Transmission Media` kehte hain. Yeh do types ka hota hai: Wired aur Wireless.

Wired Media: Ismein data bhejne ke liye cables ka use hota hai.

- Twisted Pair Cable: Iska use Ethernet networks aur Local Area Network (LAN) connections mein commonly hota hai.
- Coaxial Cable: Iska use cable TV aur purane Ethernet networks mein hota tha.
- Fiber Optic Cable: Ismein data ko light pulses ke form mein transmit kiya jata hai. Yeh high-speed internet ke main networks mein bahut important hai.

Wireless Media: Ismein bina physical cable ke signals ke through data transmit hota hai.

- Radio Waves: Wi-Fi aur cellular networks mein use hoti hain.
- Microwaves: Satellite communication mein use hoti hain.
- Infrared: Short-range communication mein use hoti hai, jaise TV remote control.

Har transmission medium ka apna use hota hai, jo network ki requirements aur environment par depend karta hai.

Q. What layer of OSI model is responsible for Physical connections like ethernet cables?(Format: two words)
Ans. Physical layer

Q. Name the OSI layer that deals with logical addressing and routing. (Format: two words)
Ans. Network layer

Q. Which protocol ensures reliable delivery of data and operates at the Transport Layer?
Ans. TCP

Q. At what layer do switches operate withinthe OSI model?(Format: three words)
Ans. Data link layer

Q.What layer of the TCP/IP model corresponds to the OSI model's Application, Presentation, and Session layers?(Format:two words)
Ans. Application layer

Q. Which layer of the OSI model manages data encryption and data format conversion?(Format: two word)
Ans. Presentation layer

Q. Name a protocol used for web browsing that operates at the Application Layer.
Ans. http

Q. Which OSI layer ensures the segments are transferred reliably and in sequence?(Format: two words)
Ans. Transport layer

Q. Which protocol fast, connectionless communication and operates at the Transport Layer?
Ans. Udp

Components of Networking

Jaise-jaise hum Information Security (InfoSec) seekh rahe hain, waise-waise network banane wale components ko samajhna bahut zaroori hai.

Hum jaante hain ki aajkal devices ek-doosre ke saath communicate kar sakte hain, resources share kar sakte hain aur internet access kar sakte hain. Ye sab kaise possible hota hai?

Iske peeche network ke kuch important components hote hain:

Component	Description (Matlab)
End Devices	Computers, Smartphones, Tablets aur IoT / Smart Devices.
Intermediary Devices	Switches, Routers, Modems aur Access Points.
Network Media and Software Components	Cables, Protocols, Management Software aur Firewall Software.
Servers	Web Servers, File Servers, Mail Servers aur Database Servers.

End Devices

Ek `End Device`, jise `Host` bhi kaha jaata hai, koi bhi aisa device hota hai jo network ke andar aakhir mein data bhejta ya receive karta hai.

Personal computers aur smart devices (jaise mobile phones aur smart TVs) common End Devices hain. Users inhe directly use karke web browsing karte hain, messages bhejte hain aur documents banate hain.

Zyada tar networks mein, ye devices data generate karne aur data receive karke use karne, dono mein important role play karte hain. Jaise jab users videos stream karte hain ya website par content padhte hain.

End Devices, World Wide Web ko access karne ke liye users ko main interface provide karte hain. Inki help se users network ke resources aur services ko aasani se access kar sakte hain. Ye connection wired (Ethernet cable) aur wireless (Wi-Fi), dono tarikon se ho sakta hai.

Iska ek aur common example hai: Ek student apne laptop ko school ke Wi-Fi network se connect karta hai. Isse woh online learning materials access kar sakta hai, assignments submit kar sakta hai aur apne teachers ke saath communicate kar sakta hai.

Intermediary Devices

Ek `Intermediary Device` ka khaas kaam `End Devices` ke beech data ke flow ko aasaan banana hota hai. Yeh data ek hi local area network ke andar ya alag-alag networks ke beech transfer ho sakta hai.

In devices mein routers, switches, modems aur access points shamil hain. Ye sab data ko tezi se aur surakshit tareeke se transfer karne mein important role nibhate hain.

Intermediary Devices ki zimmedari `Packet Forwarding` hoti hai. Iska matlab hai data packets ko unki destination tak pahunchana. Iske liye ye network address ki information ko read karte hain aur data bhejne ke liye sabse achha raasta decide karte hain.

Ye devices alag-alag networks ko connect karte hain aur network traffic ko control karte hain, jisse network ki performance aur reliability behtar hoti hai.

Protocols ki madad se data ke flow ko manage karke, ye devices data ka transfer smoothly karwate hain aur network mein congestion (zyada traffic ki wajah se bheed) hone se rokte hain.

Iske alawa, Intermediary Devices mein aksar `Firewalls` jaise security features bhi hote hain, jo networks ko bina permission ke access karne aur possible threats se bachate hain.

Ye devices OSI Model ki alag-alag layers par kaam karte hain. Jaise:

- Router: `Network Layer (Layer 3)` par kaam karta hai.
- Switch: `Data Link Layer (Layer 2)` par kaam karta hai.

Ye devices routing tables aur protocols ka use karke sahi faisla lete hain ki data ko kis taraf forward karna hai.

Iska ek aam example ghar ka network hai, jahan router aur switch jaise Intermediary Devices ghar ke sabhi devices, jaise laptops, smartphones aur smart TVs, ko internet se connect karte hain. Isse ye devices ek-doosre ke saath communicate kar sakte hain aur online resources ko access kar sakte hain.

Network Interface Cards (NICs)

`Network Interface Card (NIC)` ek hardware component hai, jo computer ya kisi doosre device mein install hota hai aur use network se connect hone ki suvidha deta hai.

Yeh device aur network media ke beech physical connection provide karta hai aur network ke through data bhejne aur receive karne ka kaam karta hai.

Har NIC ka ek unique `Media Access Control (MAC) Address` hota hai. Yeh address devices ko ek-doosre ki pehchaan karne aur `Data Link Layer` par communication karne mein madad karta hai.

NICs ko wired connection ke liye design kiya ja sakta hai, jaise Ethernet card, jo cable ke through connect hota hai. Ya wireless connection ke liye, jaise Wi-Fi adapter, jo radio waves ka use karta hai.

Example: Ek desktop computer local network se connect hone ke liye wired NIC aur Ethernet cable ka use kar sakta hai, jabki ek laptop Wi-Fi ke through connect hone ke liye wireless NIC ka use karta hai.

Routers

Ek `Router` ek intermediary device hai, jo bahut important kaam karta hai: alag-alag networks ke beech data packets ko forward karna aur internet traffic ko sahi direction mein bhejna.

OSI Model ki Network Layer (Layer 3) par kaam karte hue, routers data packets mein network address ki information ko read karte hain, taaki pata laga sakein ki data ko kahan pahunchana hai.

Routers `Open Shortest Path First (OSPF)` aur `Border Gateway Protocol (BGP)` jaise routing protocols aur routing tables ka use karte hain. Inki madad se routers data ko interconnected networks, jisme internet bhi shamil hai, ke through bhejne ke liye sabse efficient raasta dhoondhte hain.

Routers incoming data packets ko check karte hain aur unke IP addresses ke basis par packets ko unki destination ki taraf forward karte hain.

Multiple networks ko connect karke routers alag-alag networks ke devices ko ek-doosre ke saath communicate karne ki suvidha dete hain.

Routers data bhejne ke liye sabse achhe raaste select karke network traffic ko bhi manage karte hain. Isse network mein congestion (traffic ki bheed) ko rokne mein madad milti hai. Is process ko `Traffic Management` kaha jaata hai.

Iske alawa, routers firewalls aur access control lists jaise features ka use karke `Security` ko bhi behtar banate hain. Ye features network ko bina permission ke access aur possible threats se bachate hain.

Example

Ghar ke network mein, router ghar ke sabhi devices, jaise computers, smartphones aur smart TVs, ko Internet Service Provider (ISP) ke diye hue internet se connect karta hai.

Router internet se aane wale aur internet par jaane wale traffic ko efficiently sahi direction mein bhejta hai. Isse har device external networks ke saath aur zaroorat ke hisaab se ek-doosre ke saath bhi communicate kar sakta hai.

Switches

`Switch` network ka ek aur important component hai. Iska main kaam ek hi network ke andar multiple devices ko connect karna hota hai. Aam taur par yeh Local Area Network (LAN) mein use hota hai.

OSI Model ki Data Link Layer (Layer 2) par kaam karte hue, switches MAC addresses ka use karte hain, taaki data ko sirf usi device tak forward kiya ja sake jiske liye data bheja gaya hai.

Connected devices ke beech data traffic ko manage karke, switches network mein congestion (traffic ki bheed) ko kam karte hain aur network ki overall performance ko behtar banate hain.

Switches computers, printers aur servers jaise devices ko ek hi network ke andar seedhe ek-doosre ke saath communicate karne ki suvidha dete hain.

Example:

Ek corporate office mein switches employees ke computers ko connect karte hain. Isse employees jaldi se files share kar sakte hain aur printers aur servers jaise shared resources ko access kar sakte hain.

Hubs

`Hub` ek basic aur ab purana ho chuka networking device hai. Yeh ek network segment mein multiple devices ko connect karta hai aur aane wale data ko sabhi connected ports par bhej deta hai, chahe data kisi bhi device ke liye ho.

OSI Model ki Physical Layer (Layer 1) par kaam karne wale hubs, switches se zyada simple hote hain aur data traffic ko samajhdari se manage nahi karte.

Bina kisi farq ke data ko sabhi ports par bhejne ki wajah se network ki efficiency kam ho sakti hai aur data collisions ho sakte hain. Isi wajah se hubs modern networks ke liye kam suitable hote hain.

Example: Pehle ke samay mein, ek chhote home network mein hub kuch computers ko connect karne ke liye use ho sakta tha. Lekin aajkal switches ko prefer kiya jaata hai, kyunki unki performance aur efficiency behtar hoti hai.

Network Media and Software Components

`Network Media aur Software Components` aise zaroori elements hain jo network ke andar aasani se communication aur kaam karne mein madad karte hain.

`Network Media`, jaise cables aur wireless signals, physical raaste provide karte hain jo devices ko connect karte hain aur unke beech data transfer hone dete hain. Ismein Ethernet cables aur fiber-optic cables jaise wired media shamil hain, jo high-speed connections provide karte hain. Iske saath hi Wi-Fi aur Bluetooth jaise wireless media bhi hain, jo devices ko ek jagah se doosri jagah le jaane aur connection mein flexibility provide karte hain.

Doosri taraf, network protocols aur management software jaise `Software Components`, data transmission ke rules aur procedures tay karte hain. Ye ensure karte hain ki information ka format sahi ho, uska address sahi ho, data transmit aur route sahi tarah se ho, aur woh sahi jagah par receive ho.

`TCP/IP`, `HTTP` aur `FTP` jaise `Network Protocols` devices ko network ke through ek-doosre ke saath communicate karne mein madad karte hain. Wahin, `Network Management Software` administrators ko network ki performance monitor karne, devices configure karne aur software firewalls jaise tools ke through security behtar banane ki suvidha deta hai.

Cabling and Connectors

`Cabling aur Connectors` woh physical materials hain jinka use network ke andar devices ko connect karne ke liye kiya jaata hai. Ye woh raaste banate hain jinke through data transfer hota hai.

Ismein pehle bataye gaye alag-alag types ke cables ke saath RJ-45 plug jaise connectors bhi shamil hain, jinka use cables ko computers, switches aur routers jaise network devices ke saath connect karne ke liye kiya jaata hai.

Cabling aur connectors ki quality aur type network ki performance, reliability aur speed ko affect kar sakti hai.

Example ke liye, ek office mein RJ-45 connectors wali Ethernet cables desktop computers ko network switches se connect kar sakti hain, jisse Local Area Network ke andar high-speed data transfer possible hota hai.

Network Protocols

`Network Protocols` rules aur conventions ka ek set hain jo control karte hain ki network ke through data ko kaise format kiya jaata hai, transmit kiya jaata hai, receive kiya jaata hai aur interpret kiya jaata hai.

Ye ensure karte hain ki alag-alag manufacturers ke devices aur alag-alag configurations wale devices ek hi standard ko follow kar sakein aur effectively communicate kar sakein.

Protocols kai tarah ke aspects ko cover karte hain, jaise:

- `Data Segmentation`
- `Addressing`
- `Routing`
- `Error Checking`
- `Synchronization`

Common network protocols mein shamil hain:

- `TCP/IP`: Internet par hone wale sabhi communications mein iska use hota hai.
- `HTTP/HTTPS`: Web traffic ke liye standard.
- `FTP`: File transfers ke liye.
- `SMTP`: Email transmissions ke liye.

Example ke liye, jab hum kisi website ko browse karte hain, toh HTTP ya HTTPS protocol batata hai ki hamara browser web server ke saath web pages ko request karne aur receive karne ke liye kaise communicate karta hai. Ye ensure karta hai ki data ka format sahi ho aur data securely transmit kiya jaaye.

Network Management Software

`Network Management Software` mein aise tools aur applications shamil hote hain jinka use network ke components aur operations ko monitor, control aur maintain karne ke liye kiya jaata hai.

Ye software in kaamon ki suvidha provide karte hain:

- `Performance Monitoring`
- `Configuration Management`
- `Fault Analysis`
- `Security Management`

Ye network administrators ko ensure karne mein madad karte hain ki network efficiently kaam kare, secure rahe aur saamne aane wali kisi bhi problem ko jaldi solve kiya ja sake.

Example ke liye, ek corporate environment mein IT department company ke network se connected sabhi devices ko manage karne ke liye Network Management Software ka use kar sakta hai. Isse woh unusual activity ke liye network traffic monitor kar sakte hain, devices ki configurations ko remotely update kar sakte hain aur security policies ko lagu kar sakte hain, jisse network ki performance aur security behtar bani rahe.

Software Firewalls

Ek `Software Firewall` ek security application hai jo individual computers ya devices par install ki jaati hai. Yeh pehle se tay kiye gaye security rules ke basis par aane wale aur jaane wale network traffic ko monitor aur control karti hai.

Poore network ko protect karne wale hardware firewalls ke opposite, software firewalls (jinhe Host-based Firewalls bhi kaha jaata hai) har device ke level par protection provide karte hain. Yeh un threats se bachate hain jo network ki boundary par maujood security ko bypass kar sakte hain.

Ye bina permission ke access ko rokne mein madad karte hain, suspicious ya malicious data wale incoming packets ko reject karte hain aur inhe kuch specific applications ya services ka access restrict karne ke liye configure kiya ja sakta hai.

Example ke liye, zyada tar operating systems mein built-in software firewall hota hai, jise untrusted sources se aane wale connections ko block karne ke liye set up kiya ja sakta hai. Isse ensure hota hai ki sirf legitimate network traffic hi device tak pahunche.

Servers

Ek `Server` ek powerful computer hota hai, jise network ke through doosre computers, jinhe clients kaha jaata hai, ko services provide karne ke liye design kiya jaata hai.

Servers websites, emails, files aur applications ke peeche kaam karne wale main systems hote hain.

Computer networking mein servers bahut important role nibhate hain, kyunki ye aisi services host karte hain jinhe clients access karte hain, jaise web pages aur email services. Is process ko `Service Provision` kaha jaata hai.

Ye multiple users ko files aur printers jaise resources access karne ki permission dekar `Resource Sharing` ko possible banate hain.

Servers data ko ek central jagah par store aur manage karke `Data Management` bhi handle karte hain. Isse data ka backup lena aasaan hota hai aur security management behtar hota hai.

Iske alawa, servers network ke multiple components mein users ke access aur permissions ko control karke `Authentication` manage karte hain.

Servers aksar special operating systems chalate hain, jinhe ek hi samay mein multiple requests handle karne ke liye optimize kiya jaata hai.

Is process ko `Client-Server Model` kaha jaata hai. Ismein server clients ki requests ka intezaar karta hai aur request milne par uske according response deta hai.

Chahe tumhe pata ho ya nahi, pichhli baar jab tumne apne laptop se koi website access ki thi, tab bhi background mein yahi process ho raha tha.

Tumhara browser us web server ko request bhejta hai jahan website host hoti hai. Uske baad server request ko process karta hai aur apne response mein web page ka data wapas bhej deta hai.

Conclusion

Jaisa ki humne dekha, duniya bhar mein computer networking ke liye zaroori technology stack mein kai components ki zaroorat hoti hai.

End Devices, users ka network ke saath interact karne ka main zariya hote hain. Intermediary Devices, data traffic aur connectivity ko manage karte hain, aur Servers resources aur services provide karte hain.

Ye sabhi milkar information ke flow ko aasaan banate hain, jo aaj ke modern communication ko chalata hai.

Q. What type of network cable is used to transmit data over long distances with minimal signal loss?

Ans. Fibre optic

Q. Which protocol manages data routing and delivery across networks?
Ans. tcp/ip

Q. What software is used a oversee and administer network operations?(Format:3 words)
Ans. Network Management Software

Q. What software is used to protect individual devices from unauthorized network access?(Format: 1 word)
Ans. Firewall

Q.What type of cable is used to connect components within a local area network for high-speed data transfer?
Ans. ethernet

Q. Which device connects multiple networks and manages data traffic to optimize performance?
Ans. Router

Network Communication

Ek network ko sahi tarah se kaam karne aur communication karne ke liye teen zaroori components hote hain: `MAC Addresses`, `IP Addresses` aur `Ports`.

Ye teeno milkar ensure karte hain ki local aur global networks ke across devices ke beech data sahi tarah se send aur receive ho.

Ye components milkar smooth network communication ki buniyad banate hain.

MAC Address

`Media Access Control (MAC) Address` ek unique pehchaan hoti hai, jo kisi device ke `Network Interface Card (NIC)` ko di jaati hai. Isse local network par device ki pehchaan ki ja sakti hai.

OSI Model ki `Data Link Layer (Layer 2)` par kaam karne wala MAC Address, local network ke andar communication ke liye bahut zaroori hota hai. Yeh ensure karta hai ki data sahi physical device tak pahunche.

Har MAC Address 48 bits lamba hota hai aur aam taur par hexadecimal format mein likha jaata hai. Yeh hexadecimal digits ke 6 pairs ke roop mein hota hai, jo colon ya hyphen se alag kiye jaate hain.

Example: `00:1A:2B:3C:4D:5E`

MAC Address ki uniqueness uski structure se aati hai. Iske pehle 24 bits `Organizationally Unique Identifier (OUI)` ko represent karte hain, jo manufacturer ko assign kiya jaata hai. Baaki ke 24 bits kisi particular device ke liye hote hain.

Yeh design ensure karta hai ki duniya bhar mein har MAC Address unique ho, jisse devices address conflict ke bina ek-doosre ke saath communicate kar sakein.

How MAC Addresses are used in Network Communication

MAC addresses, Local Area Network (LAN) ke andar communication ke liye bahut zaroori hote hain, kyunki inka use data frames ko sahi physical device tak pahunchane ke liye kiya jaata hai.

Jab koi device data bhejta hai, toh woh information ko ek frame mein rakhta hai, jisme destination MAC address hota hai. Iske baad network switches is address ka use karke frame ko sahi port tak forward karte hain.

Iske alawa, `Address Resolution Protocol (ARP)` bhi important role nibhata hai. Yeh IP addresses ko MAC addresses ke saath map karta hai, jisse devices same network ke andar kisi known IP address se juda MAC address dhoondh sakte hain.

Yeh mapping LAN ke andar logical IP addressing aur physical hardware addressing ke beech ka gap door karti hai.

Maan lo do computers hain: Computer A (jiska IP address `192.168.1.2` hai, jiske baare mein hum thodi der mein discuss karenge) aur Computer B (`192.168.1.5`). Dono ek hi network switch se connected hain.

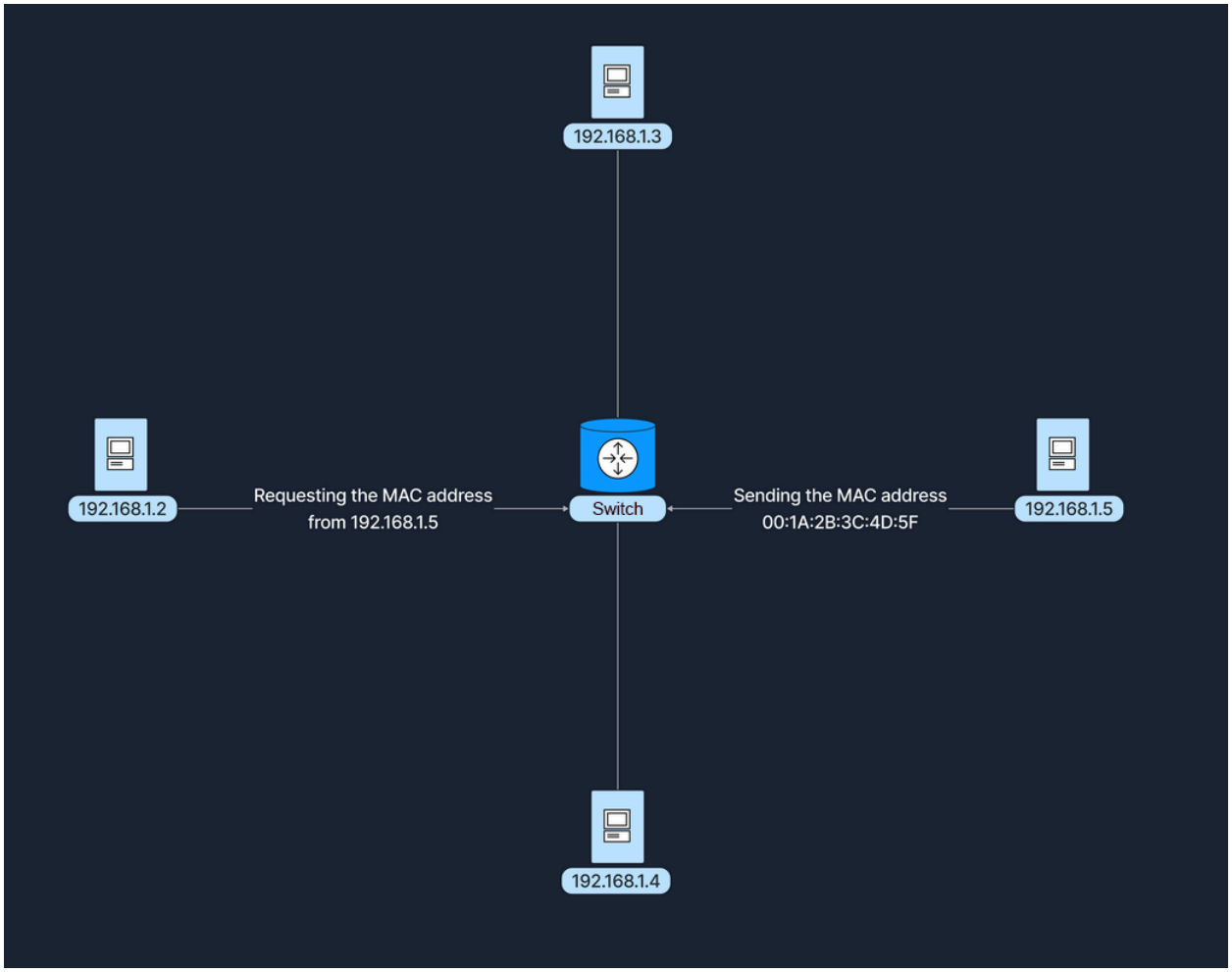
Computer A ka MAC address `00:1A:2B:3C:4D:5E` hai, jabki Computer B ka MAC address `00:1A:2B:3C:4D:5F` hai.

Jab Computer A, Computer B ko data bhejna chahta hai, toh woh sabse pehle Address Resolution Protocol (ARP) ka use karke Computer B ke IP address se juda MAC address dhoondhta hai.

Yeh information milne ke baad, Computer A ek data frame bhejta hai, jisme destination MAC address `00:1A:2B:3C:4D:5F` set hota hai.

Switch is frame ko receive karta hai aur use us specific port par forward karta hai, jahan Computer B connected hai. Isse ensure hota hai ki data sahi device tak pahunche.

Yeh process neeche diye gaye diagram mein dikhaya gaya hai.



IP Addresses

What is an IP Address?

`Internet Protocol (IP) Address` ek numerical label hota hai, jo network se connected har us device ko assign kiya jaata hai jo communication ke liye Internet Protocol ka use karta hai.

OSI Model ki `Network Layer (Layer 3)` par kaam karte hue, IP addresses devices ko alag-alag networks ke across ek-doosre ko locate karne aur communicate karne mein madad karte hain.

IP addresses ke do versions hote hain: `IPv4` aur `IPv6`.

IPv4 addresses mein 32-bit address space hota hai. Inhe aam taur par dots se alag kiye gaye chaar decimal numbers ke roop mein likha jaata hai, jaise `192.168.1.1`.

Iske opposite, IPv6 addresses ko IPv4 addresses ki kami ko door karne ke liye develop kiya gaya tha. Inmein 128-bit address space hota hai aur inhe hexadecimal digits ke aath groups mein likha jaata hai, jahan har group mein chaar hexadecimal digits hote hain.

Example: `2001:0db8:85a3:0000:0000:8a2e:0370:7334`

How IP Addresses are Used in Network Communication

Routers IP addresses ka use karke data ko uski destination tak pahunchane ke liye interconnected networks ke across sabse achha raasta decide karte hain.

MAC addresses ke opposite, jo device ke Network Interface Card se permanently jude hote hain, IP addresses zyada flexible hote hain. Ye badal sakte hain aur inhe network ki structure aur policies ke according assign kiya jaata hai.

Ek hi network par maujood do devices ke beech communication ka example bhi pehle MAC Address wale section mein dikhaye gaye example ki tarah samjha ja sakta hai.

Ports

Ek `Port` ek number hota hai, jo network par specific processes ya services ko assign kiya jaata hai, taaki computers network traffic ko sahi tarah se sort aur direct kar sakein.

Yeh OSI Model ki `Transport Layer (Layer 4)` par kaam karta hai aur TCP aur UDP jaise protocols ke saath kaam karta hai.

Ports ek hi IP address par multiple network services ko ek saath chalane mein madad karte hain. Yeh alag-alag applications ke liye bheje gaye traffic ko ek-doosre se alag karte hain.

Jab koi client application connection shuru karti hai, toh woh desired service se juda destination port number specify karti hai.

Client applications woh hoti hain jo data ya services ki request karti hain, jabki server applications un requests ka response deti hain aur data ya services provide karti hain.

Iske baad operating system, port number ke basis par incoming traffic ko sahi application tak pahunchata hai.

Ek simple example dekho, jahan koi user website access karta hai: user ka browser server ke IP address par port 80 se connection shuru karta hai, jo HTTP ke liye designated hai. Is port par listening karne wala server request ka response deta hai.

Agar user ko kisi secure website ko access karna hai, toh browser iske badle port 443 se connect karta hai, jo HTTPS ke liye standard port hai. Isse secure communication ensure hota hai.

Port numbers `0` se `65535` tak hote hain aur inhe teen main categories mein divide kiya gaya hai, jinmein se har category ek specific purpose ke liye kaam karti hai.

Using the netstat tools to view connections and listening ports.

```
netstat -ano -p tcp
```

Well-Known Ports (0–1023):

Well-known ports, jinke numbers 0 se 1023 tak hote hain, common aur universally recognized services aur protocols ke liye reserve kiye jaate hain. Inhe Internet Assigned Numbers Authority (IANA) standardize aur manage karti hai.

Example ke liye, HTTP, jo World Wide Web mein data communication ka base hai, port 80 ka use karta hai. Lekin users ka experience simple rakhne ke liye browsers aam taur par yeh port number display nahi karte.

Isi tarah, HTTPS networks par secure communication ke liye port 443 ka use karta hai. Yeh port bhi aam taur par browsers mein display nahi hota.

Ek aur example FTP hai, jo clients aur servers ke beech files transfer karne mein madad karta hai. FTP port 20 aur 21 ka use karta hai.

Registered Ports (1024–49151):

Registered ports, jinke numbers 1024 se 49151 tak hote hain, Well-known ports ki tarah itne strictly regulated nahi hote. Lekin inhe bhi Internet Assigned Numbers Authority (IANA) ke paas register kiya jaata hai aur specific services ko assign kiya jaata hai.

In ports ka use aam taur par un external services ke liye hota hai jinhe users apne device par install kar sakte hain.

Example ke liye, Microsoft SQL Server jaisi kai database services port 1433 ka use karti hain.

Software companies aksar apni applications ke liye ek port register karti hain, taaki unka software har system par consistently usi port ka use kare.

Yeh registration network traffic ko manage karne aur alag-alag applications ke beech port conflicts ko rokne mein madad karti hai.

Dynamic/Private Ports (49152–65535):

Dynamic ya Private ports, jinhe Ephemeral ports bhi kaha jaata hai, 49152 se 65535 tak hote hain.

Inka use aam taur par client applications servers se data bhejne aur receive karne ke liye karti hain, jaise jab koi web browser internet par kisi server se connect karta hai.

In ports ko Dynamic isliye kaha jaata hai kyunki ye fixed nahi hote. Zaroorat ke hisaab se client ka operating system har session ke liye inmein se koi port randomly select kar sakta hai.

Inka use aam taur par temporary communication sessions ke liye hota hai. Jab communication khatam ho jaata hai, toh ye ports band kar diye jaate hain.

Iske alawa, Dynamic ports ko custom server applications ko bhi assign kiya ja sakta hai, khaaskar un applications ko jo short-term connections handle karti hain.

Browsing the Internet Example

Neeche diye gaye example mein bataya gaya hai ki web request sahi destination tak kaise pahunchti hai aur humein jo information chahiye, woh wapas kaise aati hai.

1. DNS Lookup

Hamara computer domain name ko IP address mein convert karta hai (jaise `example.com` ke liye `93.184.216.34`).

2. Data Encapsulation

Step

Aapka browser HTTP request generate karta hai.

Request ko TCP ke saath encapsulate kiya jata hai, jisme destination port `80` ya `443` specify hota hai.

Packet mein destination IP address `93.184.216.34` hota hai.

Local network par, hamara computer default gateway (router) ka MAC address dhoondhne ke liye ARP ka use karta hai.

3. Data Transmission

Step

Data frame router ke MAC address par bheja jata hai.

Router packet ko destination IP address ki taraf forward karta hai.

Beech ke routers IP address ke basis par packet ko aage forward karte rehte hain.

4. Server Processing

Step

Server packet receive karta hai aur use port `80` ya `443` par listening karne wali application tak pahunchata hai.

Server HTTP request ko process karta hai aur same path se ulte direction mein response wapas bhejta hai.

5. Response Transmission

Step

Server response ko client ke temporary port par wapas bhejta hai. Yeh port client ke operating system ne session shuru hone par randomly select kiya tha.

Response network ke through ulte path se wapas aata hai. Router se router tak, source IP address aur port ki information ke basis par forward hota hai, jab tak client tak nahi pahunch jata.

Q. What protocol maps IP addresses to MAC addresses?
Ans. ARP

Q. Which IP version uses 128-bit addressing?
Ans. IPv6

Q. At which layer of OSI model do ports operate? (Format: two words)
Ans. Transport layer

Q. What is the designated port number for HTTP?
Ans. 80

Q. What is the first step in the process of a web browsing session? (Format: two words)
Ans. DNS lookup

Dynamic Host Configuration Protocol

Introduction to DHCP (DHCP ka parichay)

Computer network mein har device ko doosre devices ke saath communicate karne ke liye ek unique IP (Internet Protocol) address ki zaroorat hoti hai.

Har device ko manually IP address dena time-consuming ho sakta hai aur ismein galtiyan bhi ho sakti hain, khaaskar jab network mein bahut saare devices hon.

Is problem ko solve karne ke liye network mein DHCP (Dynamic Host Configuration Protocol) ka use kiya jaata hai.

DHCP ek network management protocol hai, jo IP network par devices ki settings ko automatically configure karne ke liye use hota hai.

Ye devices ko automatically IP address aur network ki doosri settings deta hai, jaise Subnet Mask, Default Gateway aur DNS Servers. Iske liye manually settings enter karne ki zaroorat nahi hoti.

DHCP network management ko kaise aasan banata hai?

DHCP automatically IP addresses assign karta hai, jisse network administrator ka kaam kaafi kam ho jaata hai.

Ye ensure karta hai ki network se connect hone wale har device ko ek unique IP address mile. Isse IP address conflict aur ek hi IP address ke duplicate use hone ki problem se bachne mein help milti hai.

Iske alawa, jab koi device network se disconnect ho jaata hai aur uska IP address dobara available ho jaata hai, toh DHCP us IP address ko kisi doosre device ko de sakta hai.

Isse available IP addresses ka achhe se use hota hai.

How DHCP Works (DHCP kaise kaam karta hai?)

DHCP process mein client aur server ke beech communication hota hai.

- DHCP Client: Woh device jo IP address maangta hai, jaise laptop ya mobile.
- DHCP Server: Woh service jo devices ko IP addresses assign karti hai.

DHCP ka ye process aam taur par DORA ke naam se jaana jaata hai.

DORA chaar steps ka short form hai:

1. D — Discover
2. O — Offer
3. R — Request
4. A — Acknowledge

Ye chaar steps milkar device ko IP address dene ka process complete karte hain.

DORA ke steps ko detail mein samajhne se pehle, DHCP server aur DHCP client ke roles ko samajhna zaroori hai.

DHCP Server aur DHCP Client ka role

DHCP Server: Ye available IP addresses mein se ek IP address device ko dene ka kaam karta hai.

DHCP Client: Ye woh device hota hai jo network se connect hote waqt IP address aur doosri network settings maangta hai.

Example: Jab tumhara laptop Wi-Fi se connect hota hai, toh laptop DHCP client hota hai aur tumhara router aam taur par DHCP server ka kaam karta hai.

Yaad rakho: DHCP ka main kaam devices ko automatically IP address aur doosri zaroori network settings dena hai.

DHCP Server aur DHCP Client

Role	Description
`DHCP Server`	Ek network device, jaise router ya dedicated server, jo IP addresses assign karne ka kaam manage karta hai. Ye available IP addresses ka ek pool aur network configuration ki settings maintain karta hai.
`DHCP Client`	Koi bhi device jo network se connect hota hai aur DHCP server se network configuration ki settings maangta hai.

DORA Process ke 4 Steps

Step	Description
1. Discover	Jab koi device network se connect hota hai, toh woh available DHCP servers ko dhoondhne ke liye ek DHCP Discover message broadcast karta hai.
2. Offer	Network par maujood DHCP servers Discover message receive karte hain aur DHCP Offer message ke saath reply karte hain. Is message mein client ko ek IP address lease par dene ka offer diya jaata hai.
3. Request	Client offer receive karne ke baad DHCP Request message bhejta hai, jismein woh batata hai ki woh offer kiya gaya IP address lena chahta hai.
4. Acknowledge	DHCP server DHCP Acknowledge (ACK) message bhejta hai aur confirm karta hai ki client ko IP address assign kar diya gaya hai. Ab client us IP address ka use karke network par communicate kar sakta hai.

Easy example

- Discover: Laptop poochta hai, “Kya network par koi DHCP server hai?”
- Offer: Server kehta hai, “Main tumhe ye IP address de sakta hoon.”
- Request: Laptop kehta hai, “Mujhe ye IP address chahiye.”
- Acknowledge: Server kehta hai, “Theek hai, ye IP address tumhe assign kar diya gaya hai.”

Yaad rakho: DORA = Discover → Offer → Request → Acknowledge.

A Linux host, connected to wireless network, initializes the DORA process

sudo dhclient wlan0

DHCP ke through IP address assign karna permanent nahi hota, balki IP address ek fixed time period ke liye diya jaata hai. Is fixed time period ko Lease Time kehte hain.

Example ke liye, DHCP server kisi smartphone ko 24 hours ke lease time ke saath IP address de sakta hai.

Is time period ke baad, smartphone ko wahi IP address use karte rehne ke liye lease renew karne ki request karni padti hai.

Lease Renewal Process: Lease expire hone se pehle, client ko apne IP address ki lease renew karne ki koshish karni hoti hai.

Iske liye client DHCP server ko ek renewal request bhejta hai.

Jab lease expire hone ka time nazdeek aata hai, toh client DHCP server se poochta hai ki kya woh assigned IP address ko aage bhi use kar sakta hai.

Agar DHCP server permission de deta hai, toh woh lease time ko badha deta hai, jisse client us IP address ko aur samay tak use kar sakta hai.

Example Scenario

Chalo, pehle discuss kiye gaye steps ke basis par ek simple example samajhte hain ki DHCP kisi device ko IP address kaise assign karta hai.

Alice apna naya laptop office laati hai aur use network se connect karti hai.

Kyuki laptop ke paas abhi IP address nahi hai, isliye woh DHCP server ko dhoondhne ke liye DHCP Discover message bhejta hai.

Office ka DHCP server is message ko receive karta hai aur DHCP Offer message ke through `192.168.1.10` IP address dene ka offer karta hai.

Alice ka laptop ye offer receive karta hai aur IP address accept karne ke liye DHCP Request message bhejta hai.

Aakhir mein, DHCP server is request ko acknowledge karta hai aur IP address assign hone ki confirmation deta hai.

Ab laptop ko `192.168.1.10` IP address mil gaya hai, jiska use karke woh network par communicate kar sakta hai.

Alice ke laptop ko diya gaya `192.168.1.10` IP address permanent nahi hai, balki ek fixed time period ke liye diya jaata hai. Is time period ko Lease Time kehte hain.

Jab lease expire hone ka time nazdeek aata hai, toh Alice ke laptop ko IP address use karte rehne ke liye lease renew karni padti hai.

Iske liye laptop DHCP server ko ek aur DHCP Request message bhejta hai aur lease time badhane ki request karta hai.

Agar server lease renew kar sakta hai, toh woh DHCP Acknowledge (ACK) message bhejta hai, jo confirm karta hai ki laptop abhi bhi us IP address ko use kar sakta hai.



Q. What protocol automates IP address configuration for devices on a network?

Ans. Dhcp

Q. What acronym describes the sequence of messages exchanged during the DHCP process?

Ans. DORA

Q. What type of message does a client send to accept an IP address from a DHCP server?

Ans. Request

Network Address Translation (NAT)

Internet data ko ek device se doosre device tak pahunchane ke liye numerical addresses ka use karta hai, jinhe IP Addresses kaha jata hai.

Original addressing system, IPv4, mein limited number of IP addresses available hain (lagbhag 4.3 billion ya 430 crore).

Halanki, ye number sunne mein bahut bada lag sakta hai, lekin Internet ke bahut tezi se badhne ki wajah se IP addresses ki kami ho gayi hai.

Is kami ki problem ka ek solution hai Network Address Translation (NAT).

NAT ka idea ye hai ki ek private network ke multiple devices ek hi Public IP Address ko share kar sakte hain.

Isse do fayde hote hain:

1. Public IP addresses ki bachat: Har device ke liye alag public IP address ki zaroorat nahi hoti.
2. Security: Ye internal network ko security ki ek extra layer provide karta hai.

Private vs. Public IP Addresses

Public IP Address

`Public IP` addresses globally unique identifiers hote hain, jo Internet Service Providers (ISPs) assign karte hain.

In IP addresses wale devices ko Internet par kahin se bhi access kiya ja sakta hai, jisse woh global network ke through ek-doosre se communicate kar sakte hain.

Example:

- `8.8.8.8` — Google ke DNS server ka IP address hai.
- `142.251.46.174` — Google ke web servers mein se ek ka IP address hai.

Ye addresses ensure karte hain ki Internet par devices ek-doosre ko uniquely identify kar sakein aur un tak data pahunch sake.

Private IP Address

`Private IP` addresses ka use local networks ke andar hota hai, jaise ghar, school aur office ke networks.

Ye addresses Global Internet par directly routable nahi hote, iska matlab hai ki Internet ke main routers in private IP addresses par bheje gaye packets ko aage forward nahi karte.

RFC 1918 ke according, common IPv4 private IP address ranges ye hain:

Private IP Range	Example
`10.0.0.0` – `10.255.255.255`	`10.0.0.5`
`172.16.0.0` – `172.31.255.255`	`172.16.0.10`
`192.168.0.0` – `192.168.255.255`	`192.168.1.10`

Is system se private networks Internet se alag apne internal network mein kaam kar sakte hain aur devices aapas mein communicate kar sakte hain.

Private IP Address ke Benefits

Private IP addresses public IP addresses ko bachane mein help karte hain.

NAT (Network Address Translation) ka use karke ek local network private IP addresses use kar sakta hai aur saath hi ek hi public IP address share kar sakta hai.

Isse har device ke liye alag public IP address ki zaroorat nahi padti.

Is setup se network ke devices Internet access kar sakte hain, bina multiple public IP addresses use kiye.

Iske alawa, private IP addresses internal devices ko Internet par direct exposure se alag rakhne mein help karte hain, jisse external threats se protection ki ek extra layer milti hai.

What is NAT? — Hinglish Translation

`Network Address Translation (NAT)` ek process hai, jo router ya uske jaise kisi device ke through kiya jata hai.

Jab IP packets router se hokar guzarte hain, toh router un packets ke header mein maujood Source IP Address ya Destination IP Address ko badal deta hai.

Is badlav ka use local network ke devices ke Private IP Addresses ko router ke ek Public IP Address mein convert karne ke liye kiya jata hai.

Easy example: Maan lo tumhare ghar mein laptop, mobile aur computer hain. In sabhi ke alag-alag Private IP addresses hain. NAT ki help se router in sabhi devices ko ek hi Public IP Address ke through Internet access karne deta hai.

How NAT Works :-

Ek ghar ke network mein kai devices ho sakte hain, jaise laptop, smartphone aur gaming console. Har device ko ek alag Private IP Address diya jata hai.

Laptop ka IP address `192.168.1.10`, smartphone ka `192.168.1.11` aur gaming console ka `192.168.1.12` hai.

Is network ko manage karne wale home router ke paas do important interfaces hote hain. LAN (Local Area Network) interface private network se connect hota hai, jiska IP address `192.168.1.1` hai. Jabki WAN (Wide Area Network) interface ISP (Internet Service Provider) ke network se connect hota hai, aur iska Public IP Address `203.0.113.50` hai.

NAT translation ki process tab shuru hoti hai jab koi device, maan lo laptop, `www.google.com` jaisi website open karne ke liye request bhejta hai.

Yeh request packet, jo laptop ke Private IP Address `192.168.1.10` se originate hota hai, router ko bheja jata hai.

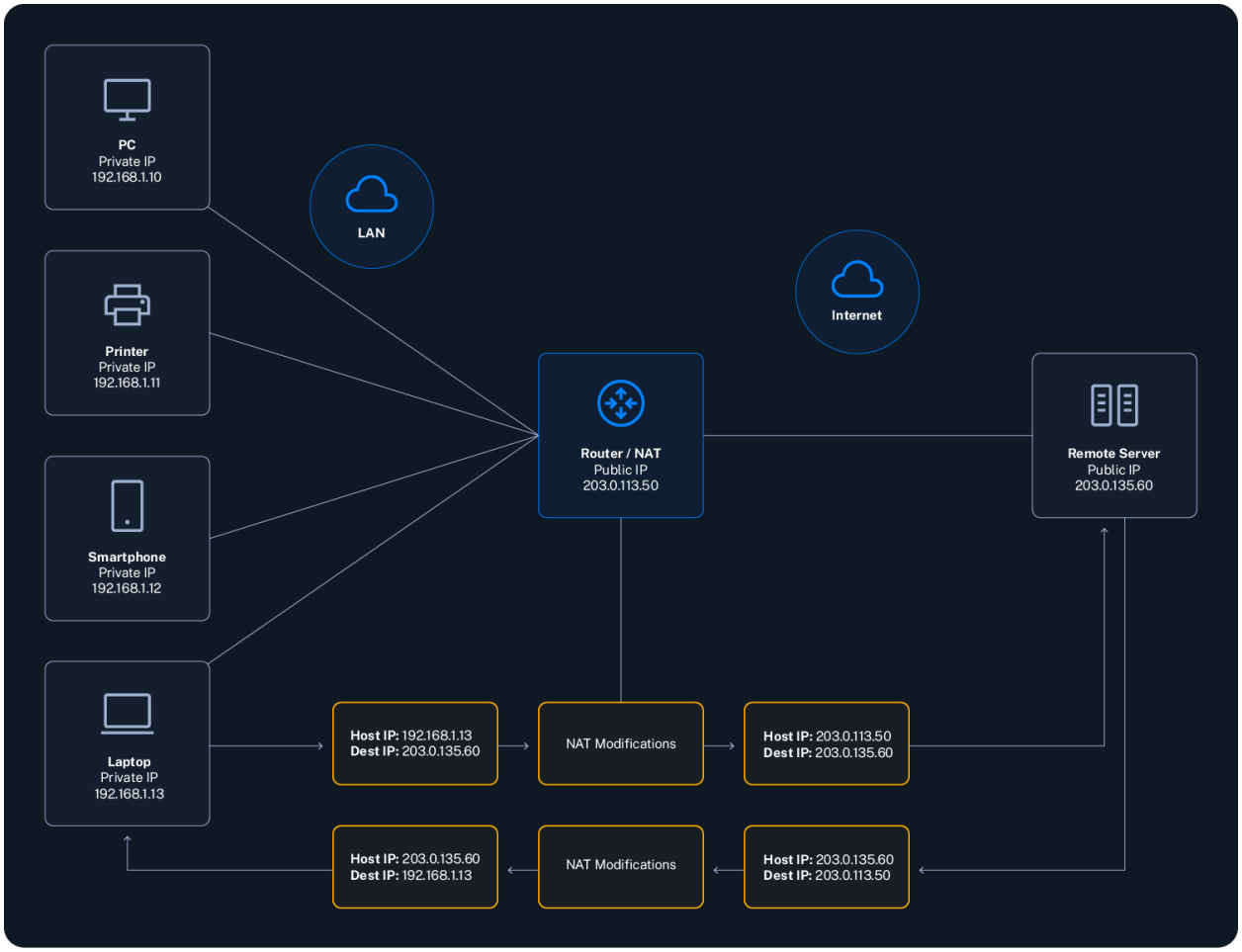
Yahan router ka NAT function packet header mein Source IP Address ko Private IP se badal kar router ke Public IP Address `203.0.113.50` mein change kar deta hai.

Iske baad yeh packet internet ke through travel karta hua apne destination web server tak pahunchta hai.

Jab web server ko packet mil jata hai, toh woh response router ke Public IP Address par wapas bhejta hai.

Jab response router ke paas aata hai, toh router ki NAT Table, jo IP addresses ki mapping ka record rakhti hai, identify karti hai ki `203.0.113.50:4444` laptop ke `192.168.1.10:5555` se related hai. Yahan port numbers `4444` aur `5555` dynamic hain, yani zaroorat ke hisaab se assign ho sakte hain.

Iske baad router Public IP ko laptop ke Private IP se map karta hai aur response laptop ko forward kar deta hai. Is tarah laptop aur website ke beech communication ka process complete ho jata hai.



Types of NAT

Yeh samajhna important hai ki Network Address Translation (NAT) ke kai types hote hain. Har type ko networking ki alag-alag zarooraton ke liye design kiya gaya hai. Neeche NAT ke different types diye gaye hain.

Static NAT

Ismein one-to-one mapping hoti hai, jahan har Private IP Address ko directly ek Public IP Address se connect kiya jata hai.

Dynamic NAT

Ismein available Public IP Addresses ke pool mein se zaroorat ke hisaab se ek Public IP, Private IP ko assign kiya jata hai. Yeh assignment network ki demand par depend karta hai.

Port Address Translation (PAT)

Ise NAT Overload bhi kaha jata hai. Yeh home networks mein sabse zyada use hone wala NAT ka type hai.

Ismein multiple Private IP Addresses ek hi Public IP Address share karte hain. Har connection ko alag pehchanne ke liye unique port numbers ka use kiya jata hai.

Yeh method ghar aur chhote offices ke networks mein widely use hota hai, jisse multiple devices ek hi Public IP Address ka use karke internet access kar sakte hain.

Benefits and Trade-Offs — Hinglish Translation

Network Address Translation (NAT) ke kai benefits (faayde) hain, lekin iske kuch trade-offs (nuksaan ya limitations) bhi hain.

Benefits (Faayde)

Conserves the limited IPv4 address space.

NAT limited IPv4 addresses ko bachane mein madad karta hai.

Provides a basic layer of security by not exposing internal network structure directly.

NAT security ki ek basic layer provide karta hai, kyunki yeh internal network ki structure ko directly internet par expose nahi karta.

Flexible for internal IP addressing schemes.

NAT internal network mein IP addresses ko manage aur assign karne mein flexibility deta hai.

Trade-Offs (Nuksaan / Limitations)

NAT ke peeche public server host karne jaisi complex services ke liye additional configuration ki zaroorat ho sakti hai, jaise Port Forwarding.

Kuch protocols ko devices ke beech direct end-to-end connection ki zaroorat hoti hai. NAT un protocols mein problem create kar sakta hai, agar unke liye special configuration na ki jaye.

NAT ki wajah se network connection ki problems ko identify karna aur solve karna thoda difficult ho sakta hai.

Q. What type of NAT allows multiple private ip addresses to share one public IP address using unique port numbers?
Ans. Port Address Translation

Q. What RFC specifies private IP ranges?
Ans. RFC 1918

Q. Which NAT type involves a one-to-one mapping of private IP addresses to public IP addresses?
Ans. static nat

Q. What type of NAT assigns a public IP from a pool as needed?
Ans. Dynamic NAT

Q. What device typically performs NAT in a home network?
Ans. router

Domain Name System (DNS)

Domain Name System (DNS) internet ki phonebook ki tarah kaam karta hai.
Yeh humein kisi website ke naam (Domain Name), jaise www.google.com, ka sahi IP address dhoondhne mein help karta hai.
DNS ke bina humein har website ko open karne ke liye uska lamba aur complicated IP address yaad rakhna padta.
DNS hamara kaam aasan bana deta hai, kyunki iski help se hum IP address yaad rakhne ke bajaye aasani se website ke naam ka use karke internet par websites access kar sakte hain.

Domain Names vs. IP Addresses

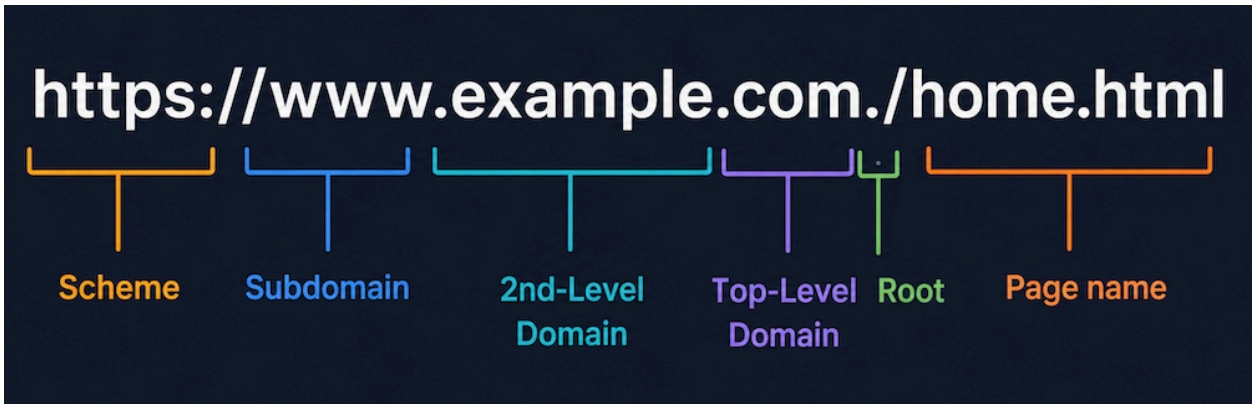
33

Address	Description
`Domain Name`	Ek aisa website address jise insaan aasani se padh aur yaad rakh sakte hain. Jaise `www.example.com`
`IP Address`	Numbers ka ek address hota hai. Jaise `93.184.216.34`

DNS in dono ke beech connection banata hai.

Iski wajah se humein website open karne ke liye uska IP address yaad rakhne ki zarurat nahi hoti.

Hum simply `www.google.com` type karte hain aur DNS us website ka IP address find karne mein help karta hai.



DNS Hierarchy

DNS ek tree (पेड़) ki tarah organized hota hai, jo Root se start hota hai aur alag-alag layers mein divide hota jata hai.

Layer	Description
`Root Servers`	DNS hierarchy ka sabse top level hota hai.
`Top-Level Domains (TLDs)`	Jaise `.com`, `.org`, `.net` ya country codes jaise `.uk`, `.de`.
`Second-Level Domains`	Jaise `example.com` mein `example` second-level domain hai.
`Subdomains or Hostname`	Jaise `www.example.com` mein `www` ya `accounts.google.com` mein `accounts`.

Easy Example:

`www.example.com` ko samjho:

- `.` (Root) = Sabse upar ka level
- `.com` = Top-Level Domain (TLD)
- `example` = Second-Level Domain
- `www` = Subdomain / Hostname

Yaad rakho: DNS hierarchy website ke naam ko alag-alag levels mein organize karti hai

DNS Resolution Process (Domain Translation)

Jab hum apne browser mein kisi website ka Domain Name enter karte hain, toh computer ko us website ka IP address find karna padta hai.

Is process ko DNS Resolution ya Domain Translation kehte hain.

Chalo step-by-step samajhte hain:

Step	Description
`Step 1`	Hum browser mein `www.example.com` type karte hain.
`Step 2`	Hamara computer sabse pehle apna Local DNS Cache check karta hai. Yeh ek chhoti storage hoti hai, jisme pehle se mile IP addresses save ho sakte hain.
`Step 3`	Agar IP address local cache mein nahi milta, toh computer `Recursive DNS Server` se poochta hai. Yeh server aksar hamare ISP (Internet Service Provider) ya Google DNS jaisi third-party service ka hota hai.
`Step 4`	Recursive DNS Server, `Root Server` se contact karta hai. Root Server use batata hai ki `.com` ke liye kis TLD Name Server ke paas jaana hai.
`Step 5`	TLD Name Server, `example.com` ke Authoritative Name Server ka address batata hai.
`Step 6`	Authoritative Name Server, `www.example.com` ka sahi IP address return karta hai.
`Step 7`	Recursive DNS Server woh IP address hamare computer ko bhej deta hai. Ab hamara computer directly website ke server se connect kar sakta hai.

Ek easy example se samjho

Maan lo tumhe Google ka ghar (server) dhoondhna hai, lekin tumhe uska address nahi pata.

1. Computer: Google ka address dhoondhta hai.
2. DNS Cache: Check karta hai ki address pehle se saved hai ya nahi.
3. Recursive DNS: Address dhoondhne ki responsibility leta hai.
4. Root Server: Batata hai `.com` ki information kahan milegi.
5. TLD Server: Batata hai Google ke official DNS server ka address.
6. Authoritative Server: Google ka actual IP address deta hai.
7. Computer: IP address milne ke baad Google ke server se connect ho jata hai.

Important terms yaad rakho:

- Root Server = Raasta batata hai.
- TLD Server = Domain ke DNS server ka raasta batata hai.
- Authoritative Server = Actual IP address deta hai.
- Recursive Server = IP address dhoondhkar tumhe deta hai.

Ek line mein: DNS Resolution ka kaam Domain Name ko IP Address mein convert karna hai.

Yeh poora process sirf ek second ke bahut chhote se hisse mein complete ho jata hai.

Neeche hum Domain Translation process ka ek simple example dekh sakte hain.

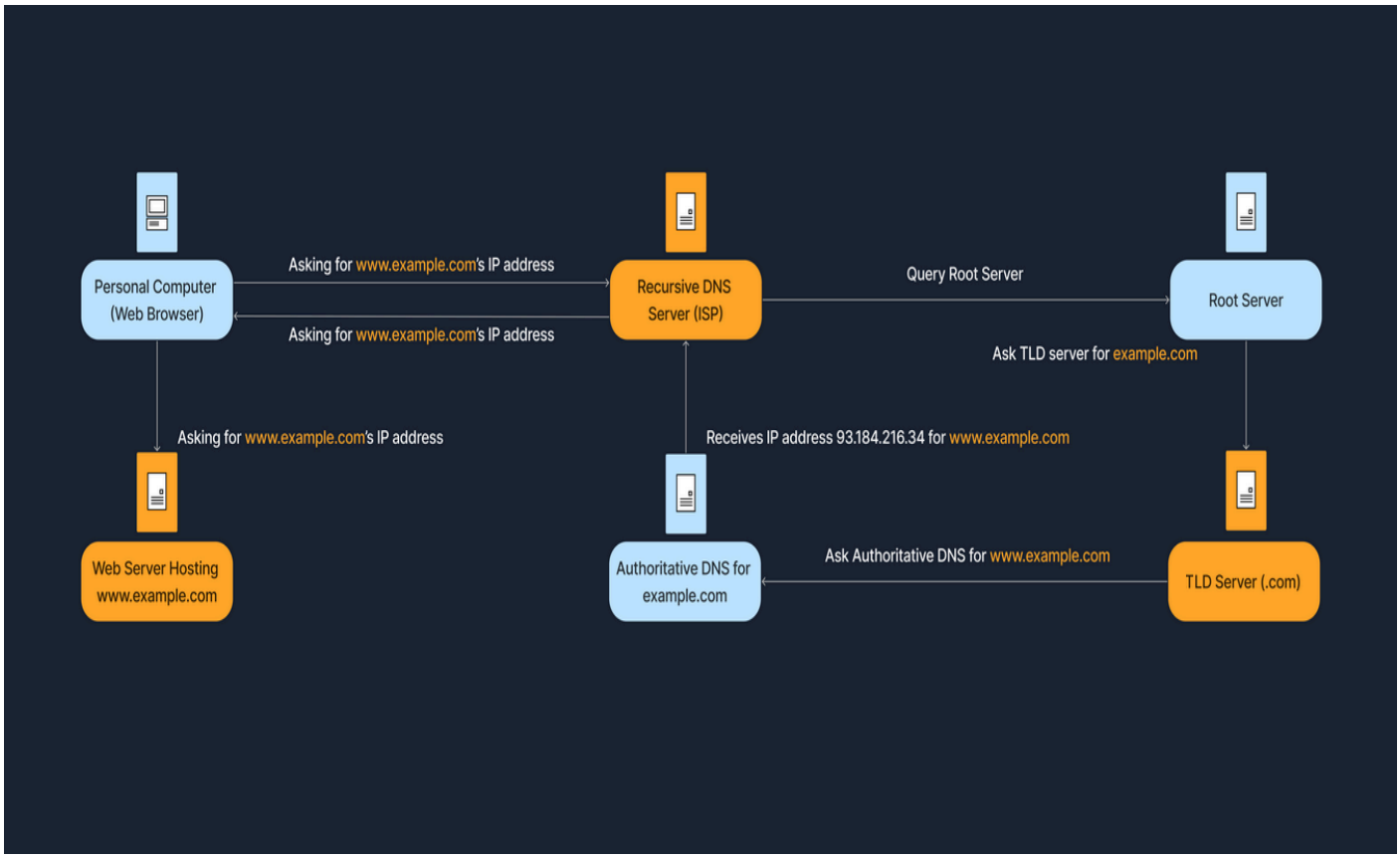
Maan lo tum `www.example.com` website visit karna chahte ho.

DNS (Domain Name System) ke bina, humein har baar us website ko access karne ke liye uska IP address pata hona chahiye aur type karna padega. Jaise `93.184.216.34`.

DNS ke hone se, hum simply apne browser mein `www.example.com` type kar sakte hain.

Background mein DNS automatically is Domain Name ko uske correct IP Address mein find aur translate kar deta hai, jisse website ke saath connection aasani se establish ho jata hai.

Neeche diya gaya diagram `DNS Query Process` ko dikhata hai.



Q. What type of domain is `.com` considered as? (Format: Three words, example: One-Two Three)

Ans. Top-Level-Domain

Q. In the domain `www.example.com`, what is `example` called?

Ans. Second-Level-Domain

Q. What is checked first in the DNS resolution process when you enter a domain name into a browser? (Format: Two words)

Ans. DNS cache

Q. What type of DNS server is typically provided by an Internet Service Provider?

Ans. recursive DNS server

Q. Which server directs the recursive DNS server to the appropriate TLD name server?

Ans. root server

Q. What numerical label uniquely identifies a device on a network?

Ans. ip address

Q. In the URL "accounts.google.com", what is `accounts` considered as?

Ans. subdomain

Internet Architecture

`Internet Architecture` batata hai ki networks ke andar data ko kaise organize, transmit (send) aur manage kiya jata hai.

Alag-alag architectural models, alag-alag zarooraton ko poora karte hain.

Kuch models simple `Client-Server` setup par kaam karte hain (jaise ek website), jabki kuch models `Distributed Approach` ka use karte hain (jaise file-sharing platforms).

In models ko samajhne se humein pata chalta hai ki networks ko kis tarah design aur operate kiya jata hai.

Alag-alag architectures, alag-alag problems ko solve karte hain.

Kai baar hum dekhte hain ki multiple architectures ko combine karke `Hybrid Models` banaye jate hain.

Har model ke apne kuch advantages aur disadvantages hote hain, jo in cheezon par depend karte hain:

- Scalability: Network ko kitna bada kiya ja sakta hai.
- Performance: Network kitni achhi speed aur performance deta hai.
- Security: Network kitna secure hai.
- Manageability: Network ko manage karna kitna aasan hai.

Aage ke paragraphs mein hum different architectures ko detail mein samjhenge.

Peer-to-Peer (P2P) Architecture

`Peer-to-Peer (P2P)` network mein har node, chahe woh computer ho ya koi doosra device, Client aur Server dono ki tarah kaam karta hai.

Yeh setup sabhi nodes ko ek-doosre ke saath directly communicate karne ki permission deta hai. Ismein nodes files, processing power ya bandwidth jaise resources ek-doosre ke saath share kar sakte hain, bina kisi central server ki zarurat ke.

P2P networks poori tarah `Decentralized` ho sakte hain, jismein koi central server nahi hota, ya partially centralized ho sakte hain, jahan ek central server kuch tasks ko coordinate kar sakta hai, lekin data ko host nahi karta.

Example

Maan lo kuch dost apni vacation (chhuttiyon) ki photos ek-doosre ke saath share karna chahte hain.

Saari photos ko ek hi website ya server par upload karne ke bajaye, har dost apne computer mein ek folder banata hai, jise doosre dost access kar sakte hain.

Iske liye woh ek file-sharing program ka use karte hain, jo unke computers ko directly connect karta hai.

P2P kaam kaise karta hai?

Sabse pehle, woh apne computers mein ek `Peer-to-Peer (P2P) File-Sharing Application` install karte hain.

Uske baad, woh apne computer mein us folder ko select karte hain jismein vacation ki photos hain, jinhe woh apne doosre doston ke saath share karna chahte hain.

Sabhi dost apne-apne computers mein yahi setup karte hain.

Jab sabhi log P2P application ke through connect ho jate hain, toh woh ek-doosre ke shared folders mein photos dekh sakte hain aur directly download kar sakte hain.

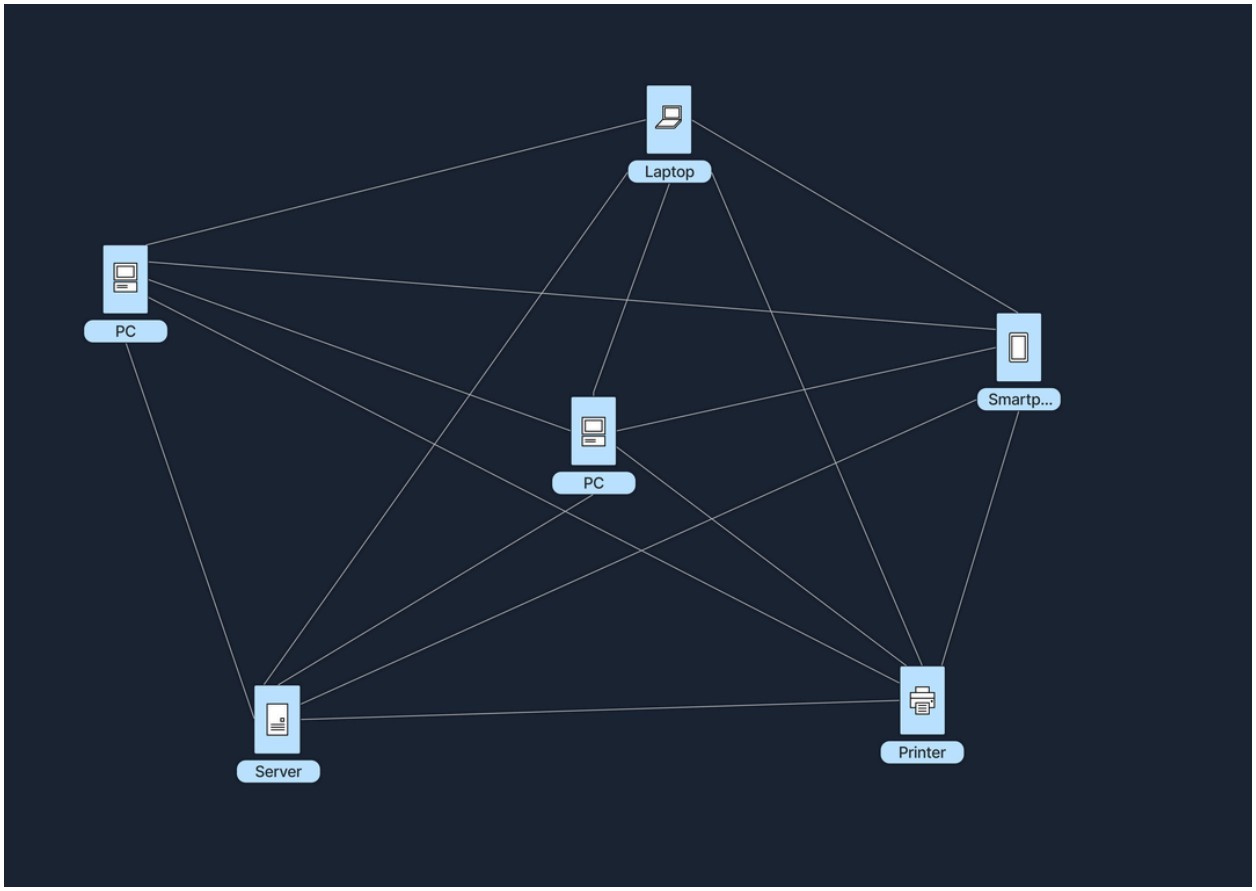
Is tarah bina kisi central server ki zarurat ke, sabhi log directly ek-doosre ke saath files exchange kar sakte hain.

Real-Life Example

`Peer-to-Peer (P2P) Architecture` ka ek popular example `Torrenting` hai, jaisa ki `BitTorrent` applications mein dekhne ko milta hai.

Is system mein jis person ke paas file hoti hai, use `Seeder` kaha jata hai.

Seeder us file ko upload kar sakta hai, jisse doosre log ek hi samay mein multiple sources se us file ko download kar sakte hain.



Peer-to-Peer Architecture ke advantages (faayde) aur disadvantages (nuksaan) hum neeche di gayi tables mein dekh sakte hain.

Advantages

Advantage	Description
`Scalability`	Network mein jitne zyada nodes add kiye jate hain, utne hi total resources (Storage, CPU etc.) badh sakte hain.
`Resilience`	Agar ek node offline ho jata hai, toh doosre nodes phir bhi kaam karte reh sakte hain.
`Cost Distribution`	Bandwidth aur Storage jaise resources ka load sabhi peers ke beech divide ho jata hai, jisse cost kam hoti hai.

Disadvantages (Nuksaan)

Disadvantage	Description
`Management Complexity`	Sabhi nodes par updates aur security policies ko control aur manage karna mushkil hota hai.
`Potential Reliability Issues`	Agar bahut saare peers network chhod dete hain, toh kuch resources available nahi ho sakte.
`Security Challenges`	Har node par security vulnerabilities (kamzoriyan) hone ka risk hota hai.

Client-Server Architecture

`Client-Server` model Internet par sabse zyada use hone wale architectures mein se ek hai.

Is setup mein `Clients` (jo users ke devices hote hain) requests bhejte hain, jaise koi web browser kisi webpage ko open karne ke liye request bhejta hai.

Aur `Servers` un requests ka response dete hain, jaise ek web server webpage ko host karta hai.

Is model mein aam taur par centralized servers hote hain, jahan data aur applications store hote hain. Multiple clients in servers se connect hokar services aur resources ko access karte hain.

Example

Maan lo hum kisi website par weather forecast (mausam ki jaankari) check karna chahte hain.

Sabse pehle hum apne phone ya computer mein web browser open karte hain aur website ka naam type karte hain, jaise `weatherexample.com`.

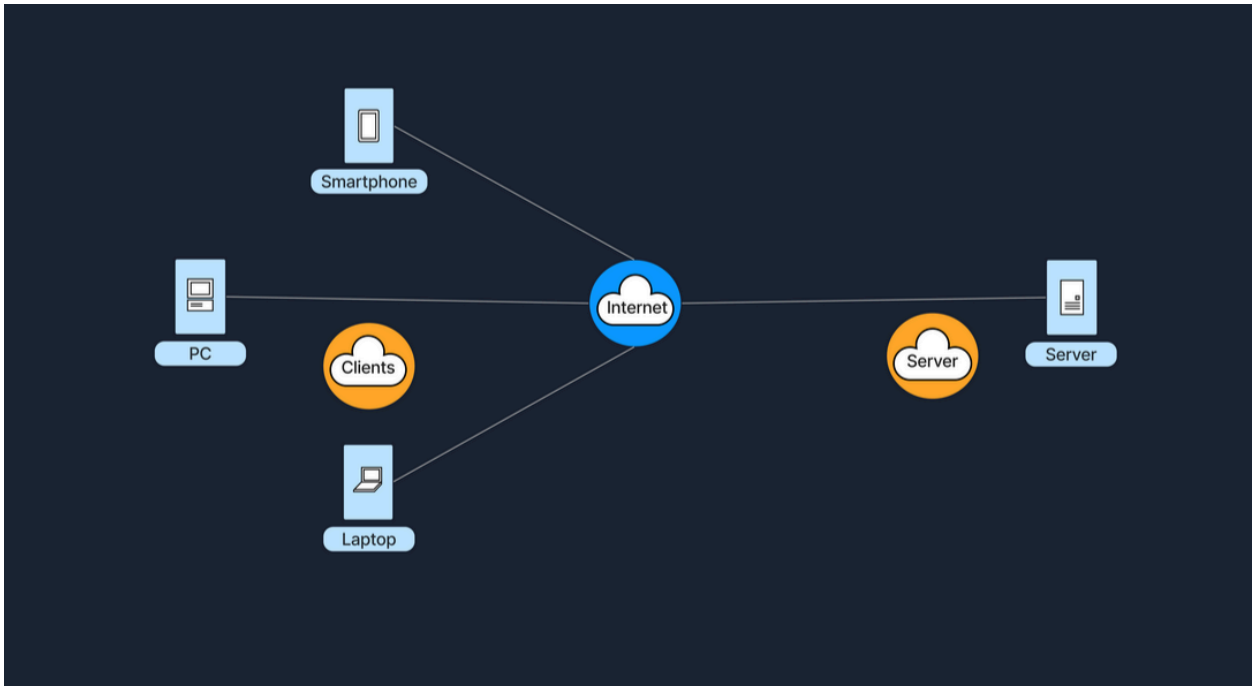
Jab hum Enter press karte hain, toh browser Internet ke through us server ko request bhejta hai, jahan `weatherexample.com` host ki gayi hai.

Yeh server ek powerful computer hota hai, jise specially website ka data store karne aur requests handle karne ke liye setup kiya jata hai.

Server hamari request receive karta hai aur use process karke requested webpage ko find karta hai.

Uske baad server weather se related data hamare browser ko wapas bhej deta hai, jiski humne request ki thi.

Hamara browser is information ko receive karta hai aur webpage par display karta hai, jisse hum mausam ke latest updates dekh sakte hain.



Is architecture ka ek important hissa **`Tier Model`** hai, jo server ke alag-alag kaamon (Roles) aur zimmedariyon (Responsibilities) ko alag-alag layers mein divide karta hai.

Isse network ko bada karna, manage karna, secure rakhna aur uski performance ko behtar banana aasan ho jata hai.

Single-Tier Architecture

`Single-Tier` architecture mein Client, Server aur Database teeno ek hi machine (computer) par hote hain.

Yeh setup simple hota hai, lekin Scalability aur Security mein kaafi limitations hone ki wajah se, iska use bade applications mein bahut kam kiya jata hai.

Two-Tier Architecture

`Two-Tier` architecture application ke environment ko Client aur Server mein divide karta hai.

Client, Presentation Layer ko handle karta hai aur Server, Data Layer ko manage karta hai.

Yeh model aam taur par Desktop Applications mein dekha jata hai, jahan User Interface user ki machine par hota hai aur Database ek Server par hota hai.

Communication aam taur par Client aur Server ke beech directly hota hai. Yeh Server ek Database Server ho sakta hai, jismein queries ko process karne ki capability hoti hai.

Note:-

Ek typical web application mein Client (Browser), directly Database Server ke saath interact nahi karta.

Iske bajaye, Browser ek `Web Server` se webpage ki request karta hai.

Web Server apna response (HTML, CSS, JavaScript) wapas Browser ko bhejta hai, taaki Browser us webpage ko render (display) kar sake.

Web Server apna response taiyar karne ke liye kisi `Application Server` ya Database ke saath interact kar sakta hai.

Lekin generally, jab koi person kisi website ko visit karta hai, toh is situation ko `Two-Tier Architecture` nahi kaha jata hai.

Three-Tier Architecture

`Three-Tier Architecture` mein Client aur Database Server ke beech ek additional layer add ki jati hai, jise `Application Server` kaha jata hai.

Is model mein Client, Presentation Layer ko manage karta hai, Application Server saare Business Logic aur Processing ko handle karta hai, aur third tier mein Database Server hota hai.

Yeh separation (alag-alag divide karna) zyada flexibility aur scalability provide karta hai, kyunki har layer ko independently develop (develop karna) aur maintain (manage karna) kiya ja sakta hai.

N-Tier Architecture

Zyada complex systems mein `N-Tier Architecture` ka use kiya jata hai, jahan `N` ka matlab three se zyada kisi bhi number of separate tiers (layers) se hota hai.

Is setup mein Application Servers ke multiple levels hote hain, jinmein se har server Business Logic, Processing ya Data Management ke alag-alag kaamon ki zimmedari sambhalta hai.

N-Tier Architectures bahut zyada Scalable hote hain aur Distributed Deployment ki permission dete hain. Is wajah se yeh Web Applications aur un services ke liye ideal hote hain, jinhe powerful aur flexible solutions ki zarurat hoti hai.

Client-Server Architectures mein alag-alag tiers use karne se kai improvements milte hain, lekin isse Deployment aur Maintenance mein complexity (mushkil) bhi badh jati hai.

Har tier ko sahi tarike se configure aur secure karna zaroori hota hai.

Saath hi, Performance Bottlenecks (performance slow hone ki problems) aur Security Vulnerabilities (security ki kamzoriyan) se bachne ke liye, sabhi tiers ke beech communication efficient aur secure hona chahiye.

Neeche di gayi table mein hum generally Client-Server Architecture ke advantages (faayde) aur disadvantages (nuksaan) dekh sakte hain.

Advantages

Advantage	Description
`Centralized Control`	Manage aur update karna aasan hota hai.
`Security`	Central security policies ko apply kiya ja sakta hai.
`Performance`	Dedicated servers ko unke specific kaam ke hisaab se optimize kiya ja sakta hai.

Disadvantages

Disadvantage	Description
`Single Point of Failure`	Agar central server band (down) ho jata hai, toh clients uski services access nahi kar sakte.
`High Cost and Maintenance`	Client-Server Architecture ko set up karna aur chalate rehna mehenga hota hai. Iske liye server ko continuously operate karna aur expert management ki zarurat hoti hai, jiski wajah se maintenance ka cost badh jata hai.
`Network Congestion`	Network par bahut zyada traffic hone se congestion (bheed) ho sakti hai. Jab ek hi samay mein bahut saare clients server ko access karte hain, toh connection slow ho sakta hai ya kaam karna band bhi kar sakta hai.

Hybrid Architecture

`Hybrid` model, `Client-Server` aur `Peer-to-Peer (P2P)` dono architectures ke elements ko combine karta hai.

Is setup mein central servers ka use coordination (talमेल bithane) aur authentication (identity verify karne) jaise tasks ke liye kiya jata hai, jabki actual data transfer directly peers ke beech hota hai.

Yeh combination dono architectures ki strengths (khoobiyon) ka use karke efficiency aur performance ko behtar banata hai.

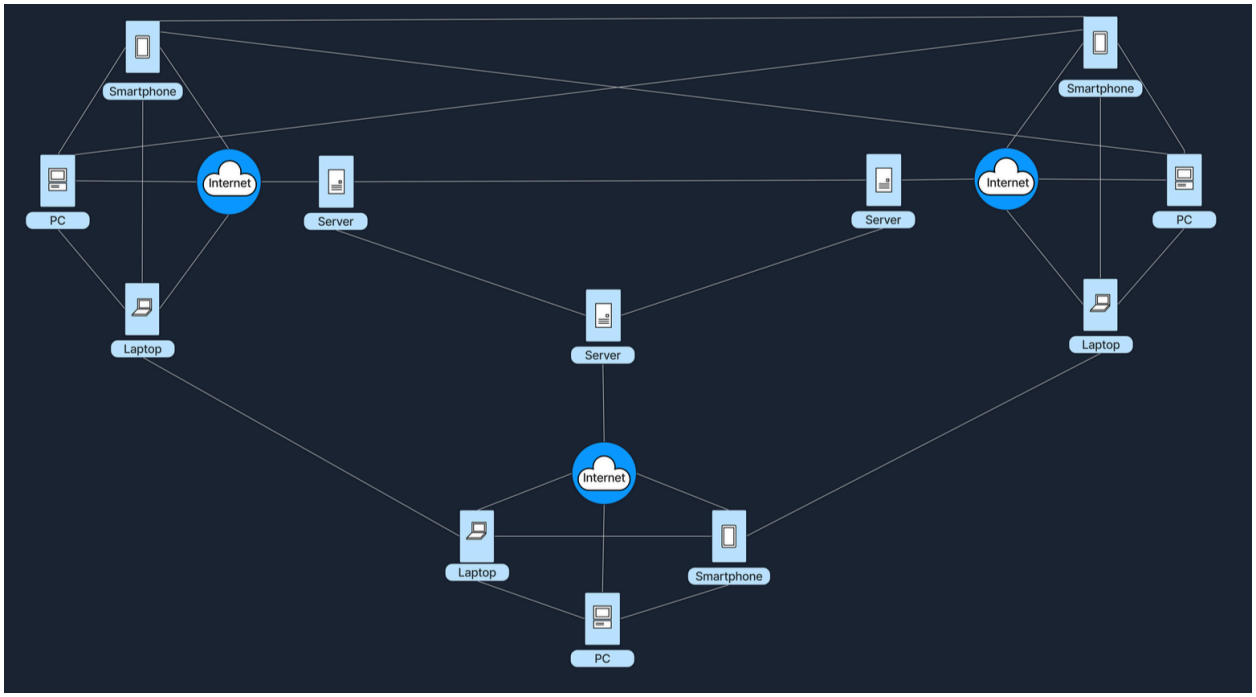
Neeche diya gaya example batata hai ki Hybrid Architecture kaise kaam karta hai.

Example

Jab hum kisi Video Conferencing App ko open karke login karte hain, toh hamare login credentials (Username aur Password) ko central servers verify karte hain.

Yehi servers meeting ko manage bhi karte hain, jaise meeting mein kaun-kaun shamil hai aur kisko access dena hai.

Jab hum login kar lete hain aur meeting shuru ho jati hai, toh actual Video aur Audio data hamare device aur doosre participants ke devices ke beech directly transfer hota hai.



Advantage (Faayda)	Description (Matlab)
`Efficiency (Kushalta)`	Servers ka workload kam ho jata hai, kyunki peers aapas mein data share kar sakte hain.
`Control (Control)`	Central server abhi bhi user authentication, directory services ya indexing ko manage kar sakta hai.

Disadvantage	Description
Complex Implementation (Mushkil Setup)	Centralized aur distributed dono components ko handle karne ke liye zyada advanced design ki zaroorat hoti hai.
Potential Single Point of Failure	Agar central coordinating server fail ho jata hai, toh peers ko discover karne ka process ruk sakta hai.

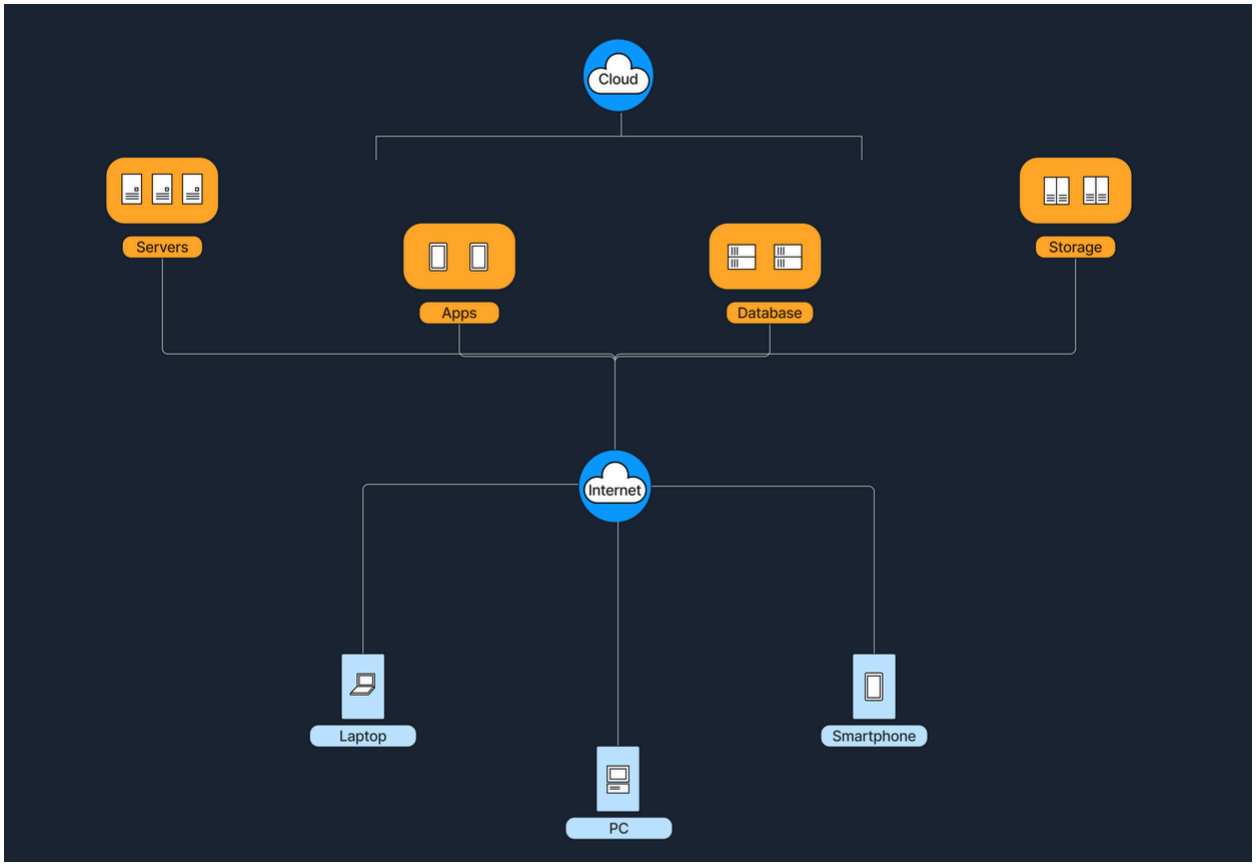
Cloud Architecture

Cloud Architecture ka matlab hai aisa computing infrastructure jo third-party providers, jaise AWS, Azure aur Google Cloud ke dwara host aur manage kiya jata hai.

Yeh architecture virtualized scale par Client-Server Model ko follow karta hai.

Yeh Internet ke through zaroorat ke hisaab se resources provide karta hai, jaise servers, storage aur applications.

Is model mein users in services ka use karte hain, lekin unke peeche jo actual hardware hota hai, usko control nahi karte.



Google Drive ya Dropbox jaisi services, Cloud Architecture ke examples hain. Yeh SaaS (Software as a Service) model ke under kaam karti hain.

Is model mein hum Internet ke through applications ko access karte hain, bina unke peeche ke hardware ko manage kiye.

Neeche 5 important characteristics di gayi hain, jo Cloud Architecture ko define karti hain.

Characteristic (Khaasiyat)	Description (Matlab)
1. On-demand self-service	Bina kisi insaan ki help ke services ko automatically setup aur manage karna.

`2. Broad network access`	Internet se connected kisi bhi device se services ko access karna.
`3. Resource pooling`	Multiple users ke beech service resources ko share karna aur zaroorat ke hisaab se allocate karna.
`4. Rapid elasticity`	Demand ke hisaab se services ko jaldi se badhana ya kam karna.
`5. Measured service`	Sirf unhi resources ke liye payment karna, jinhe aap use karte ho. Resources ka use accurately track kiya jata hai.

Neeche di gayi table mein Cloud Architecture ke kuch faayde aur nuksaan dikhaye gaye hain.

Advantage	Description
`Scalability`	**Zaroorat ke hisaab se computing resources ko aasani se badha ya hata sakte hain.**
`Reduced cost & maintenance`	**Hardware ko cloud provider manage karta hai, jisse cost aur maintenance kam ho jati hai.**
`Flexibility`	**Internet connection hone par kahin se bhi services ko access kar sakte hain.**

Disadvantage	Description
`Vendor lock-in`	**Ek cloud provider se doosre cloud provider par migrate karna mushkil ho sakta hai.**
`Security/Compliance`	**Data hosting ke liye third party par depend rehne se data privacy ko lekar concerns ho sakte hain.**
`Connectivity`	**Iske liye stable Internet connection ki zaroorat hoti hai.**

Software-Defined Architecture (SDN)

`Software-Defined Networking (SDN)` ek modern networking approach hai, jo Control Plane aur Data Plane ko alag karti hai.

- Control Plane: Yeh decide karta hai ki network traffic ko kahan bhejna hai.
- Data Plane: Yeh actual mein traffic ko aage forward karta hai.

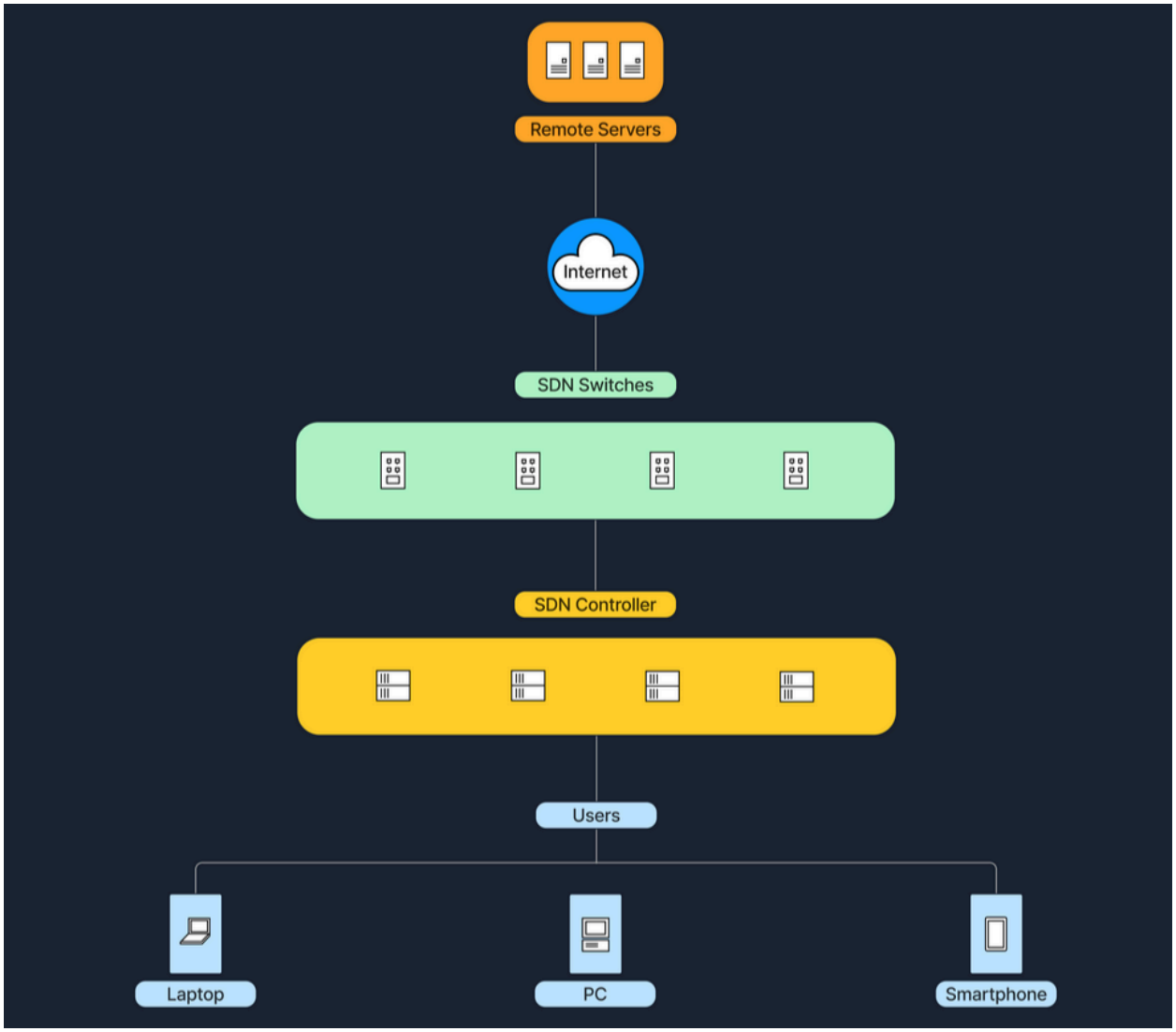
Traditional networking mein routers aur switches jaise devices ke andar dono planes (Control Plane aur Data Plane) hote the.

Lekin SDN mein, Control Plane ko ek software-based controller ke andar centralized rakha jata hai.

Is setup mein network devices sirf controller se milne wale instructions ko follow karte hain.

SDN ek programmable network management environment provide karta hai, jisse administrators zaroorat ke hisaab se network policies aur routing ko dynamically change kar sakte hain.

Yeh separation network ko zyada flexible banata hai aur network ko manage karna bhi aasan kar deta hai.



Badi companies (Large Enterprises) ya Cloud Providers, SDN ka use karke real-time demand ke hisaab se bandwidth allocate karte hain aur network traffic ke flow ko manage karte hain.

Neeche di gayi table mein Software-Defined Architecture ke faayde aur nuksaan bataye gaye hain.

Advantage	Description
`Centralized control`	Network ko manage karna aasan ho jata hai.

Programmability & Automation	Har device ko manually configure karne ke bajaye, software ke through network settings ko jaldi change kiya ja sakta hai.
Scalability & Efficiency	Network traffic ke flow ko dynamically optimize kar sakte hain, jisse resources ka behtar use hota hai.

Disadvantage	Description
Controller Vulnerability	Agar central controller kaam karna band kar de, toh network par bura asar pad sakta hai.
Complex Implementation	Iske liye naye skills aur specialized software/hardware ki zaroorat hoti hai.

Key Comparisons

Neeche di gayi table mein different Network Architectures ki important characteristics ka comparison diya gaya hai.

Architectue (Architecture ka type)	**Centralized** (Control kiske paas hai)	**Scalability** (Badhane ki kshamta)	**Ease of** Management (Manage karne mein aasani)	**Typical Use** Cases (Kahan use hota hai)
P2P	Decentralized ya partially centralized (Control kisi ek jagah nahi hota ya kuch had tak hota hai)	High (Peers badhne par bhi aasani se grow kar sakta hai)	Complex (Koi central control nahi hota)	File-sharing, Blockchain

Client-Server	Centralized (Control central server ke paas hota hai)	Moderate (Madhyam)	Easier (Server ki wajah se manage karna aasan hota hai)	Websites, Email services
Hybrid	Partially central (Kuch control central hota hai)	Client-Server se zyada	Management zyada complex hota hai	Messaging apps, Video conferencing
Cloud	Provider ke infrastructure mein centralized	High	Easier (Management cloud provider karta hai)	Cloud storage, SaaS, PaaS
SDN	Control Plane centralized hota hai	High (Policies ke hisaab se network ko badha sakte hain)	Moderate (Specialized tools ki zaroorat hoti hai)	Datacenters, Large enterprises

---

Conclusion

Har architecture ke apne alag-alag faayde aur challenges (mushkilein) hote hain.

Practical use mein, hum aksar in different models ko mix karke use karte hain, taaki performance, scalability aur cost ke beech balance banaya ja sake.

Jo bhi person network systems ko setup ya improve karna chahta hai, uske liye in differences ko samajhna bahut zaroori hai.

Q. What type of architecture allows nodes to act as both client and server?
Ans. Peer-to-Peer

Q. What architecture combines elements of both Client-Server and Peer-to-Peer models?
Ans. Hybrid

Q. Which cloud service model involves accessing applications over the internet without managing the underlying infrastructure?

Ans. saas

Q. In which architecture is the control plane separated from the data plane? (Format: two words, one of which is hyphenated)
Ans. Software-Defined Networking

Q. Which architecture is known for decentralized data sharing without a central server?
Ans. peer-to-peer

Q. What model is used by video conferencing apps to combine centralized coordination with peer-to-peer data transfer?
Ans. Hybrid

Wireless Networks

Ek **`Wireless Network`** ek aisa communication system hai jo computers, smartphones aur IoT devices jaise alag-alag devices ko connect karne ke liye radio waves ya doosre wireless signals ka use karta hai.

Iski help se ye devices bina kisi physical cable ke aapas mein communicate aur data exchange kar sakte hain.

Ye technology devices ko wireless tarike se internet se connect karne, files share karne aur services access karne ki suvidha deti hai.

Ye personal aur professional dono jagah par flexibility aur convenience provide karti hai.

Advantages

Advantages	Description
`Mobility`	Users coverage area ke andar freely move kar sakte hain.
`Ease of installation`	Isme zyada cables lagane ki zarurat nahi hoti.
`Scalability`	Wired network ke comparison mein naye devices add karna aasan hota hai.

Disadvantages

Disadvantages	Description
`Interference`	Wireless signals walls, doosre electronic devices ya atmospheric conditions ki wajah se disturb ho sakte hain.
`Security risks`	Agar proper security measures na hon, toh wireless signals ko intercept karna aasan ho sakta hai.
`Speed limitations`	Generally, same generation ke wired connections ke comparison mein wireless connections ki speed kam hoti hai.

Wireless Router

Ek `router` ek device hota hai jo alag-alag computer networks ke beech data packets ko forward karta hai.

Ghar ya chhote office mein ek `wireless router` do main functions ko combine karta hai:

Function	Description
`Routing`	Data ko uski sahi destination tak pahunchana (apne network ke andar ya internet par).
`Wireless Access Point`	Wi-Fi coverage provide karna.

Example: Ghar par hamare smartphones, laptops aur smart TVs sabhi wireless tarike se router se connect hote hain.

Router ek modem se connected hota hai, jo ISP (Internet Service Provider) se internet service lekar aata hai.

Neeche wireless router ke main components diye gaye hain:

Component	Description
`WAN (Wide Area Network) Port`	Internet source (jaise cable modem) se connect hota hai.
`LAN (Local Area Network) Ports`	Local devices (jaise desktop computer aur printer) ko wire ke through connect karne ke liye hote hain.

`Antennae`	Wireless signals ko transmit (bhejne) aur receive (receive karne) ka kaam karte hain. Kuch routers mein internal antennae bhi hote hain.
`Processor & Memory`	Routing aur network management se jude tasks ko handle karte hain.

Mobile Hotspot

Ek **`mobile hotspot`** smartphone (ya kisi doosre hotspot device) ki help se uske cellular data connection ko Wi-Fi ke through doosre devices ke saath share karne ki suvidha deta hai.

Doosre devices jaise laptops, tablets aadi is hotspot se bilkul normal Wi-Fi network ki tarah connect ho sakte hain.

Mobile hotspot cellular data ka use karta hai aur 4G ya 5G jaise cellular network ke through devices ko internet se connect karta hai.

Hotspot ki range aam taur par kuch meters tak hi limited hoti hai.

Hotspot chalane se smartphone ki battery bhi kaafi jaldi drain ho sakti hai.

Security ke liye hotspot ka access usually password se protected hota hai, bilkul home Wi-Fi network ki tarah.

Example: Socho hum kahin travel kar rahe hain aur humein public Wi-Fi nahi mil raha hai. Aise mein hum apne phone ka hotspot ON kar sakte hain aur apne laptop ko phone ke Wi-Fi signal se connect karke internet chala sakte hain.

Cell Tower

Ek `cell tower` (ya `cell site`) ek aisa structure hota hai jahan antennas aur electronic communication equipment lage hote hain, jo cellular network ka ek cell banate hain.

Cellular network mein `cell` ka matlab ek specific area hota hai, jahan ek cell tower network coverage provide karta hai.

Ek cell tower ko is tarah design kiya jata hai ki woh aas-paas ke doosre towers ke coverage areas ke saath smoothly connect rahe.

Har tower ek particular geographical area ko cover karta hai, jisse mobile phones aur doosre cellular devices signals send aur receive kar sakte hain.

Cell towers radio transmitters aur receivers ki help se kaam karte hain. Inmein antennas lage hote hain jo specific radio frequencies par communication karte hain.

Ye towers `Base Station Controller (BSC)` ke through manage kiye jaate hain. BSC multiple towers ke operations ko control karta hai.

Jab users ek cell se doosre cell mein move karte hain, toh BSC calls aur data sessions ko ek tower se doosre tower par transfer karne ka kaam karta hai.

Finally, ye towers `Backhaul Links` ke through core network se connected hote hain. Backhaul links usually fiber optic ya microwave links hote hain.

Cell towers ko unki coverage capacity ke basis par alag-alag categories mein divide kiya jata hai:

1. Macro Cells

Macro cells bade towers hote hain jo kai kilometers tak extensive coverage provide karte hain.

Ye rural areas (gaon) ke liye useful hote hain, jahan bade area mein network coverage dene ki zarurat hoti hai.

2. Micro/Small Cells

Micro aur small cells chhote installations hote hain, jo usually urban areas (shehron) mein lagaye jaate hain.

Ye towers densely populated areas (jahan bahut saare log rehte hain) mein lagaye jaate hain aur macro cells ke coverage gaps ko fill karte hain.

Example: Socho hum road trip par hain aur apne phone par music stream kar rahe hain. Jaise-jaise hum travel karte hain, hamara phone connection maintain rakhne ke liye ek cell tower se doosre cell tower par switch karta rehta hai.

Frequencies in Wireless Communications

Jaise ki humne pehle padha, wireless communication mein radio waves ka use kiya jata hai, jisse devices ek-doosre se connect aur communicate kar sakte hain.

Ye radio waves specific frequencies par emit hoti hain. In frequencies ko Oscillation Rates kaha jata hai, aur inhe Hertz (Hz) mein measure kiya jata hai.

Wireless networks mein commonly use hone wale frequency bands:

Frequency Bands

1. 2.4 GHz (Gigahertz) – Iska use purane Wi-Fi standards (802.11b/g/n) mein hota hai. Ye walls ko aasani se penetrate kar sakta hai, lekin ismein interference (jaise microwave aur Bluetooth) hone ki possibility zyada hoti hai.

2. 5 GHz – Iska use naye Wi-Fi standards (802.11a/n/ac/ax) mein hota hai. Ismein speed zyada hoti hai, lekin range kam hoti hai.

3. Cellular Bands – Inka use 4G (LTE) aur 5G mein hota hai. Inki frequencies lower frequencies (700 MHz) se lekar mid-range (2.6 GHz) aur kuch 5G services mein aur bhi higher frequencies (28 GHz aur usse zyada) tak hoti hain.

Alag-alag frequencies wireless communication mein important role play karti hain, kyunki har frequency ki apni characteristics hoti hain aur range aur speed ke beech trade-off hota hai.

Lower Frequencies: Ye zyada door tak travel kar sakti hain, lekin kam data carry kar sakti hain. Isliye inka use bade areas mein coverage provide karne ke liye hota hai, jahan data ki demand kam hoti hai.

Higher Frequencies: Ye zyada data carry kar sakti hain, lekin inki range bahut kam hoti hai.

Iske alawa, jab bahut saare devices same frequencies ka use karte hain, toh frequency bands congested (busy) ho sakte hain. Isse interference hota hai aur network ki performance kharab ho sakti hai.

In problems ko manage aur kam karne ke liye government agencies (jaise United States mein FCC) frequency allocation ko regulate karti hain. Isse radio waves ka proper use hota hai aur alag-alag users ke beech interference ko roka ja sakta hai.

Summarizing

Ek normal din mein hum wireless technology ke kai forms ka use kar sakte hain.

Ghar par, hamara wireless router 2.4 GHz aur 5 GHz dono frequencies par Wi-Fi ke through hamare phone aur laptop jaise devices ko internet access provide karta hai.

Jab hum ghar se bahar jaate hain, toh hamara phone automatically nearest cell tower se connect ho jata hai aur 4G ya 5G network ka use karke internet chalata hai.

Jab hum kisi doosre desh mein travel kar rahe hote hain, toh hum apne phone ka mobile hotspot ON karke apna cellular data kisi friend ke laptop ke saath share kar sakte hain.

In sabhi activities ke dauran hum 3 important wireless technologies ka use karte hain:

1. Wi-Fi: Local area mein wireless internet access provide karta hai.
2. Cellular Networks: Bade areas mein wireless network coverage provide karte hain.
3. Mobile Hotspot: Apne mobile data ko doosre devices ke saath share karne ki suvidha deta hai.

Q. What type of waves do wireless networks use to connect devices? (Format: two words)
Ans.

Q. What device combines the functions of routing and providing Wi-Fi coverage in a home network? (Format: two words)
Ans.

Q. What is used by a mobile hotspot to connect devices to the internet? (Format: two words)
Ans.

Q. What structure supports antennas and communications equipment to create cellular network coverage? (Format: two words)
Ans.

Q. What manages multiple cell towers in cellular networks? (Format: three words)
Ans.

Q. Which frequency band is known for better wall penetration but more prone to interference?
Ans.

Network Security

Networking mein `Security` ka matlab un measures (upayon) se hai, jo network ke andar data, applications, devices aur systems ko unauthorized access (bina permission ke access) ya damage se protect karne ke liye liye jaate hain.

Iska main goal `CIA Triad` ko maintain aur protect karna hota hai.

Principle	Description
`Confidentiality`	Sirf authorized users hi data ko dekh sakte hain.
`Integrity`	Data accurate (sahi) aur bina kisi badlav ke rehna chahiye.
`Availability`	Jab zarurat ho, tab network resources available hone chahiye.

Aage ke paragraphs mein hum Network Security ke do important components ke baare mein discuss karenge:

1. `Firewalls`
2. `Intrusion Detection/Prevention Systems (IDS/IPS)`

Firewalls

Ek Firewall ek network security device hota hai, jo hardware, software ya dono ke combination se bana ho sakta hai.

Ye incoming (aane wale) aur outgoing (bahar jaane wale) network traffic ko monitor karta hai.

Firewall kuch rules follow karta hai, jinhe Firewall Policies ya Access Control Lists (ACLs) kaha jata hai.

In rules ki help se firewall decide karta hai ki kisi specific network traffic ko Allow (permission dena) karna hai ya Block (rokna) hai.

Example: Hum firewall ko kisi building ke entrance par khade security guard ki tarah samajh sakte hain.

Security guard rules ki list check karta hai aur decide karta hai ki kise building ke andar aane ya bahar jaane ki permission deni hai.

Agar koi visitor rules ko follow nahi karta (jaise uska naam guest list mein nahi hai), toh use entry nahi di jaati.

The open source router/firewall pfSense. Its large number of plugins (known as "Packages") give it a range of capabilities.

Firewalls predefined rules aur policies ke according data packets ko analyze karke kaam karte hain. Ye mainly IP addresses, port numbers aur protocols jaise factors ko check karte hain.

Is process ko **`Traffic Filtering`** kaha jata hai.

System administrators specific conditions ke basis par rules define karte hain ki kis network traffic ko allow karna hai aur kis traffic ko deny karna hai.

Isse ensure hota hai ki sirf authorized connections ko hi network access mile.

Iske alawa, firewalls traffic se judi activities ka record (log) bhi rakh sakte hain aur kisi bhi suspicious activity ke baare mein alerts generate kar sakte hain.

Neeche firewalls ke kuch alag-alag types diye gaye hain.

---

1. Packet Filtering Firewall

Description

Ye OSI model ke Layer 3 (Network) aur Layer 4 (Transport) par kaam karta hai.

Ye source/destination IP address, source/destination port aur protocol type ko check karta hai.

`Example`: Ek simple router ACL jo sirf HTTP (port 80) aur HTTPS (port 443) ko allow karta hai aur baaki ports ko block kar deta hai.

2. Stateful Inspection Firewall

Description

Ye network connections ki state ko track karta hai.

Ye packet filtering firewall se zyada intelligent hota hai, kyunki ye poori communication ko samajhta hai.

`Example`: Ye sirf us incoming data ko allow karta hai jo pehle se ki gayi outgoing request se match karta hai.

3. Application Layer Firewall (Proxy Firewall)

Description

Ye OSI model ke Layer 7 (Application) tak kaam karta hai.

Ye network traffic ke actual content ko inspect kar sakta hai (jaise HTTP requests) aur malicious requests ko block kar sakta hai.

`Example`: Ek web proxy jo suspicious patterns wali malicious HTTP requests ko filter karke block karta hai.

4. Next-Generation Firewall (NGFW)

Description

Ye Stateful Inspection ko advanced features ke saath combine karta hai, jaise Deep Packet Inspection, Intrusion Detection/Prevention aur Application Control.

`Example`: Ek modern firewall jo known malicious IP addresses ko block kar sakta hai, encrypted traffic ko threats ke liye inspect kar sakta hai aur applications ke according security policies apply kar sakta hai.

Firewalls internet aur internal network ke beech mein kaam karte hain. Ye network traffic ko check karte hain aur uske baad hi use aage jaane ki permission dete hain.

Home Environment:

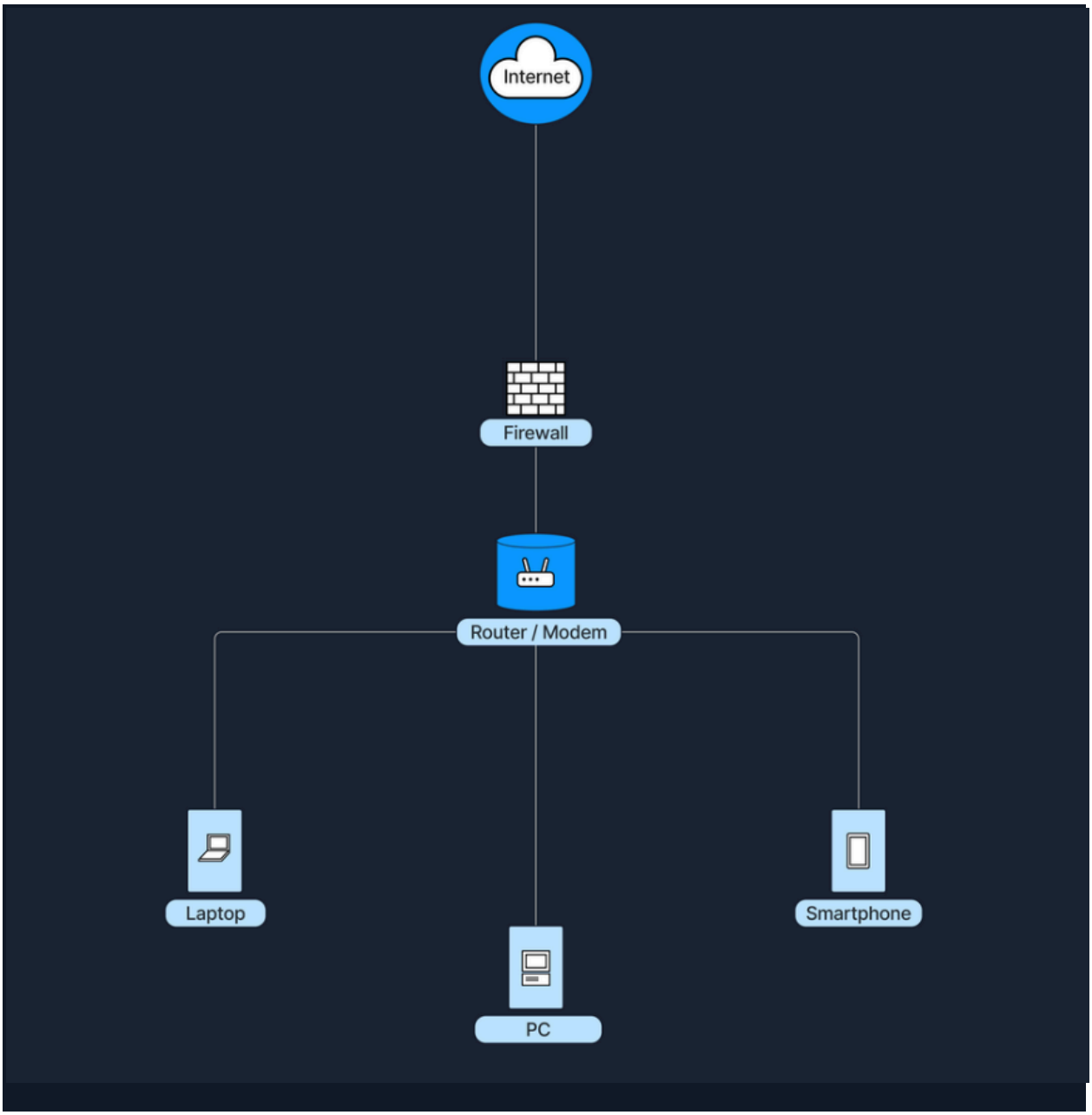
Ghar mein hamare router/modem ke andar aksar built-in firewall hota hai (jo software-based hota hai).

Is case mein sabhi functions ek hi device mein hote hain aur firewall ka function router ke `andar` hi hota hai.

Business Environment:

Bade networks (jaise business environments) mein firewall aksar ek separate device hota hai.

Ise modem/router ke baad aur internal network se pehle lagaya jata hai, taaki saara network traffic firewall se hokar hi guzre.



Intrusion Detection and Prevention Systems (IDS/IPS)

Intrusion Detection and Prevention Systems (IDS/IPS) aise security solutions hain, jinhe network ya system ki suspicious activities ko monitor karne aur unka response dene ke liye design kiya gaya hai.

Ek `Intrusion Detection System (IDS)` network traffic ya system events ko observe karta hai, taaki malicious behavior ya security policies ke violations ko identify kar sake. Ye alerts generate karta hai, lekin suspicious traffic ko block nahi karta.

Iske opposite, ek `Intrusion Prevention System (IPS)` bhi IDS ki tarah kaam karta hai, lekin ek extra step leta hai. Ye malicious traffic ko real time mein prevent ya reject karta hai.

In dono ke beech main difference inke actions mein hai:

- `IDS` = Detect karta hai aur alert deta hai.
- `IPS` = Detect karta hai aur prevent karta hai.
-

The widely used Suricata software can function as both an IDS and an IPS. Here, we see the user enable a detection rule, then begin inline monitoring.

Vim local.rules

Both IDS aur IPS solutions network packets ko analyze karte hain aur unhe known attack signatures ya normal traffic patterns ke saath compare karte hain.

Is process mein ye techniques use hoti hain:

Techniques	Description
`Signature-based detection`	Traffic ko known exploits ke database ke saath match karta hai.
`Anomaly-based detection`	Normal activity ke comparison mein kisi bhi unusual activity ko detect karta hai.

Jab koi suspicious ya malicious behavior identify hota hai, toh IDS further investigation ke liye ek alert generate karta hai.

Wahin IPS ek step aage jaakar malicious traffic ko real time mein block ya reject kar deta hai.

Suricata in IDS mode.
Cat /var/log/suricata/fast.log

Below IDS/IPS ke kuch alag-alag types diye gaye hain.

1. Network-Based IDS/IPS (NIDS/NIPS)

Description

Ye ek hardware device ya software solution hota hai, jise network ke important points par lagaya jata hai, taaki ye network se guzarne wale saare traffic ko inspect kar sake.

`Example`: Ek sensor jo core switch se connected hota hai aur data center ke andar hone wale network traffic ko monitor karta hai.

2. Host-Based IDS/IPS (HIDS/HIPS)

Description

Ye individual hosts ya devices par run hota hai aur us specific machine ke incoming/outgoing traffic aur system logs ko monitor karta hai, taaki suspicious behavior ko identify kar sake.

`Example`: Kisi server par installed antivirus ya endpoint security agent.

IDS/IPS ko network mein kai important locations par place kiya ja sakta hai.

1. Behind the Firewall:

Ek option hai IDS/IPS ko firewall ke peeche place karna. Ismein firewall obvious threats ko filter karta hai aur IDS/IPS bache hue traffic ko inspect karta hai.

2. DMZ (Demilitarized Zone):

IDS/IPS ko DMZ mein bhi place kiya ja sakta hai.

DMZ bade network ke andar ek separate network segment hota hai, jo directly internet ke contact mein hota hai.

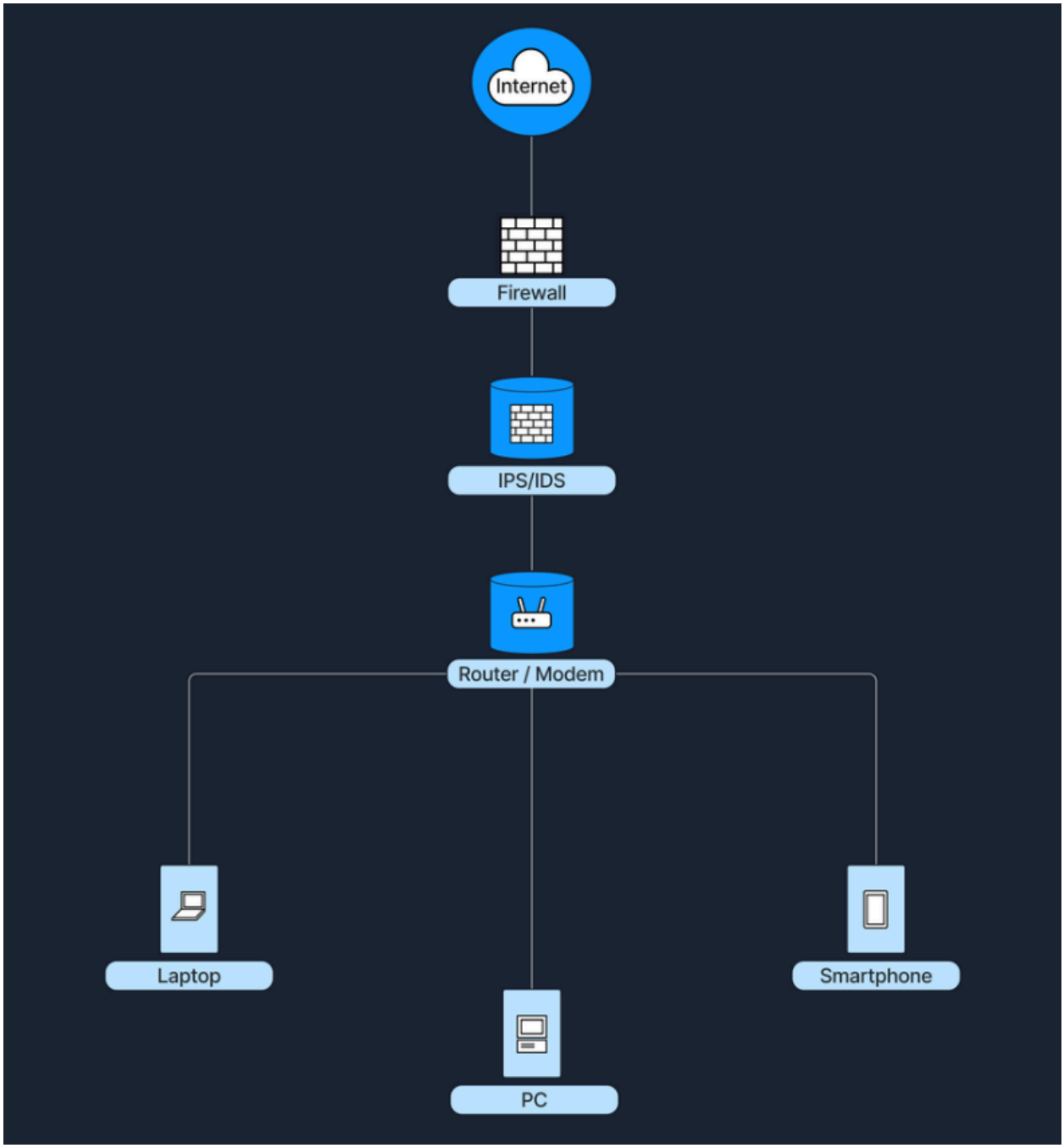
Yahan IDS/IPS publicly accessible servers ke andar aur bahar jaane wale traffic ko monitor karta hai.

3. Endpoint Devices:

Finally, IDS/IPS solutions ko directly endpoint devices, jaise servers ya workstations par bhi run kiya ja sakta hai.

Isse ye host level par suspicious activities ko detect kar sakte hain.

Neeche diye gaye diagram mein IDS/IPS ko firewall ke baad place kiya hua dikhaya gaya hai.



Best Practices

Network security ko improve karne ke liye kuch best practices neeche di gayi hain:

Practice	Description
`Define Clear Policies`	`Least Privilege` principle ke basis par consistent firewall rules define karein (sirf utni hi permission dein jitni zaroori ho).
`Regular Updates`	Latest threats se bachne ke liye firewall, IDS/IPS signatures aur operating systems ko regularly update rakhein.
`Monitor and Log Events`	Suspicious patterns ko jaldi identify karne ke liye firewall logs, IDS/IPS alerts aur system logs ko regularly check karein.
`Layered Security`	`Defense in Depth` strategy ka use karein. Ismein attack ko slow down karne ke liye multiple security layers ka use hota hai, jaise Firewalls, IDS/IPS, Antivirus aur Endpoint Protection, taaki alag-alag attack vectors se protection mil sake.
`Periodic Penetration Testing`	Real attacks ko simulate karke security policies aur devices ki effectiveness ko test karein.

Q. What device monitors network traffic and enforces rules to allow or block specific traffic?
Ans.

Q. Which type of firewall operates at the network and transport layers of the OSI model? (Format: two words)
Ans.

Q. What advanced feature does a Next-Generation Firewall include beyond stateful inspection? (Format: three words)
Ans.

Q. Which system generates alerts for suspicious network activity without blocking it? (Format: acronym)
Ans.

Q. Which system not only detects but also prevents suspicious network activity by blocking it? (Format: acronym)
Ans.

Q. What detection method involves comparing network traffic against a database of known exploits? (Format: three words)
Ans.

Data Flow Example

Pichhle sections mein humne jo knowledge gain ki hai, uske basis par neeche diye gaye paragraphs mein bataya jayega ki jab koi user apne laptop se kisi website ko access karne ki koshish karta hai, toh exactly kya hota hai.

Neeche in events ko `Client-Server Model` ke according step-by-step explain kiya gaya hai.

---

1. Accessing the Internet (Internet Access Karna)

Socho ek user apne laptop ko home Wireless LAN (WLAN) network ke through internet se connect kar raha hai. Jab laptop is network se connect hota hai, toh ye steps hote hain:

Steps

Laptop sabse pehle sahi wireless network/SSID ko identify karta hai.

Agar network WPA2/WPA3 security use karta hai, toh user ko authenticate hone ke liye sahi password ya credentials enter karne hote hain.

Finally, connection establish ho jata hai aur IP configuration ka kaam DHCP protocol sambhal leta hai.

2. Checking Local Network Configuration (DHCP)

Jab user website access karne ke liye web browser (jaise Chrome, Firefox ya Safari) open karta hai aur `www.example.com` type karta hai, toh browser webpage ke liye request bhejne ki taiyari karta hai.

Laptop se koi packet bahar jaane se pehle, operating system check karta hai ki laptop ke paas Local Area Network ke liye valid IP address hai ya nahi.

Steps	Description
`IP Address Assignment`	**Agar laptop ke paas pehle se IP address nahi hai, toh woh home router ke `DHCP` server se IP address request karta hai. Ye IP address sirf local network ke andar valid hota hai.**
`DHCP Acknowledgement`	**DHCP server laptop ko ek private IP address (jaise 192.168.1.10) assign karta hai. Iske saath subnet mask, default gateway aur DNS server jaisi configuration details bhi deta hai.**

3. DNS Resolution

Ab laptop ko `www.example.com` ka IP address find karna hota hai. Iske liye neeche diye gaye steps follow hote hain.

Steps	Description
`DNS Query`	**Laptop DNS server ko DNS query bhejta hai. Ye DNS server usually ISP dwara provide kiya gaya external DNS server ya Google DNS jaisi third-party service hoti hai.**

`DNS Response`	**DNS server `www.example.com` domain ko lookup karta hai aur uska IP address (jaise 93.184.216.34) return karta hai.**

4. Data Encapsulation and Local Network Transmission

Ab laptop ke paas destination IP address aa gaya hai. Isliye woh data transmission ke liye data prepare karna shuru karta hai.

`OSI/TCP-IP` model ke andar ye steps hote hain:

Steps	Description
`Application Layer`	**Browser webpage ke liye HTTP (ya HTTPS) request create karta hai.**
`Transport Layer`	**Request ko TCP segment (ya UDP, lekin web traffic ke liye usually TCP) mein wrap kiya jata hai. Is segment mein source aur destination ports hote hain (HTTP ka default port 80 aur HTTPS ka 443).**
`Internet Layer`	**TCP segment ko IP packet mein rakha jata hai. Source IP laptop ka private IP (jaise 192.168.1.10) hota hai aur destination IP remote server ka IP (93.184.216.34) hota hai.**
`Link Layer`	**IP packet ko Ethernet frame (agar Ethernet use ho raha hai) ya Wi-Fi frame mein rakha jata hai. Ismein MAC addresses include hote hain. Source MAC laptop ke network interface ka aur destination MAC router ke interface ka hota hai.**

Jab encapsulated frame ready ho jata hai, toh laptop apni ARP table check karta hai ya ARP request bhejta hai, taaki default gateway (router) ka MAC address find kar sake.

Uske baad frame ko router ke MAC address ko destination banakar `Link Layer` par router tak bhej diya jata hai.

5. Network Address Translation (NAT)

Jab router frame receive karta hai, toh woh IP packet ko process karta hai.

Is point par router packet header mein private IP (192.168.1.10) ko apne public IP address (jaise 203.0.113.45) se replace kar deta hai.

Is process ko `Network Address Translation (NAT)` kaha jata hai.

Iske baad router packet ko ISP ke network mein forward karta hai. Wahan se packet internet ke through destination IP (93.184.216.34) tak travel karta hai.

Is process ke dauran packet kai intermediate routers se hokar guzarta hai. Ye routers destination IP ko check karte hain aur decide karte hain ki destination network tak pahunchne ke liye kaunsa best path use karna hai.

6. Server Receives the Request and Responds

Jab packet destination network tak pahunchta hai, toh server ka firewall (agar available hai) check karta hai ki port 80 (HTTP) ya 443 (HTTPS) par aane wale traffic ko allow karna hai ya nahi.

Agar traffic firewall rules pass kar leta hai, toh woh `www.example.com` ko host karne wale server tak pahunch jata hai.

Iske baad web server software (jaise Apache, Nginx ya IIS) request receive aur process karta hai.

Phir ye webpage (HTML, CSS, images aadi) prepare karta hai aur response ke roop mein wapas bhej deta hai.

Server ka response process bhi similar hota hai, lekin reverse direction mein.

Ab server ka IP (93.184.216.34) source hota hai aur hamare home router ka public IP (203.0.113.45) destination hota hai.

Jab packet hamare home router (203.0.113.45) tak pahunchta hai, toh NAT use wapas laptop ke private IP (192.168.1.10) se map kar deta hai.

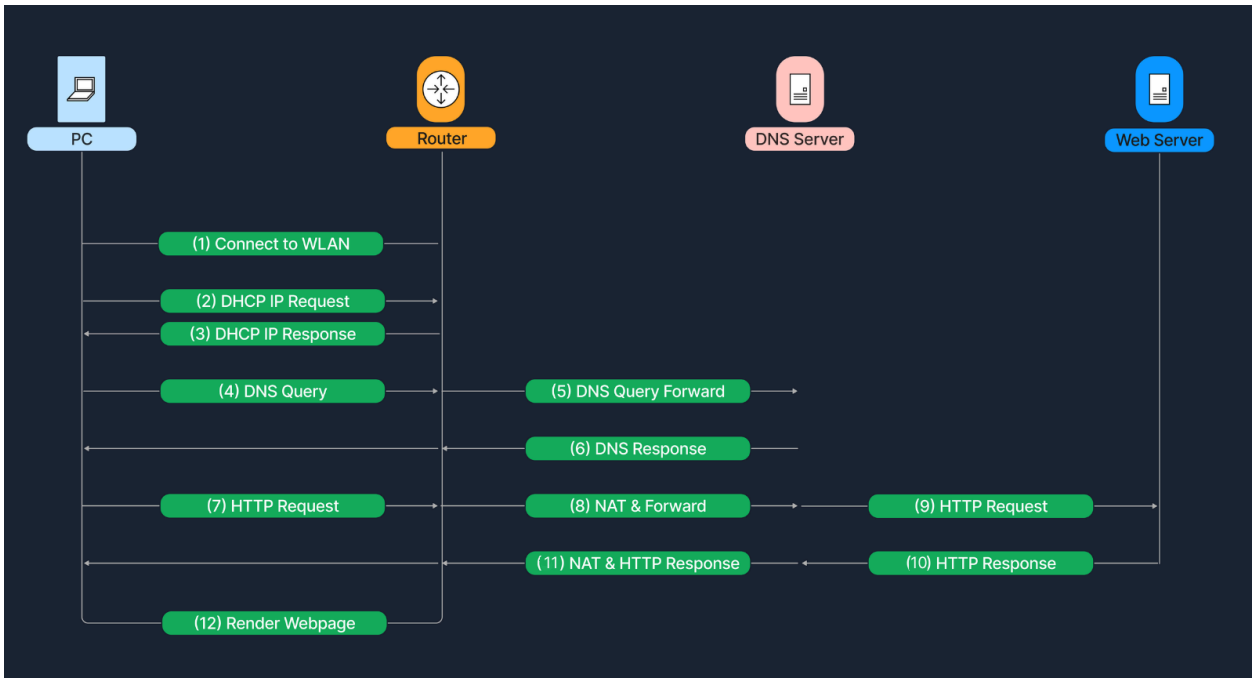
7. Decapsulation and Display

Finally, hamara laptop response receive karta hai aur Ethernet/Wi-Fi frame, IP header aur TCP header ko remove karta jata hai, jab tak application layer ka data extract nahi ho jata.

Laptop ka browser HTML/CSS/JavaScript ko read karta hai aur aakhir mein webpage ko screen par display kar deta hai.

Data Flow Diagram

Below is a flow chart showing the complete journey of a user accessing a website on the internet.



Skills Assessment

Ab jab hum computer networking ke basic concepts se familiar ho chuke hain, toh ab in concepts ko real-world scenario mein apply karne ka time hai.

Is guided assessment mein hum HTB Academy ke lab environments ke peeche kaam karne wali networking ko explore karenge.

Ye assessment 3 chapters mein divided hai, lekin challenge questions complete karne aur assessment finish karne ke liye sirf pehle 2 chapters complete karna zaroori hai.

Third chapter optional hai, un learners ke liye jo is topic ko aur detail mein explore karna chahte hain.

Keep me in the Loop

Is assessment ke first chapter mein hum HTB Academy ke `Pwnbox` ko dekhenge.

Pwnbox ek fully functional Linux machine hai, jo `Parrot OS` par run karti hai aur jise hum poori tarah web browser ke through access kar sakte hain.

Hum ise students ko provide karte hain, taaki woh hamare platform par available alag-alag exercises aur labs complete karte waqt ise apne workstation ke roop mein use kar saken.

Agar tumne pehle kabhi Linux use nahi kiya hai, toh ghabrane ki zarurat nahi hai. Har cheez ko step-by-step guide kiya jayega.

Jab tum start karne ke liye ready ho jao, toh neeche scroll karke apni Pwnbox location select karo aur `Launch Instance` par click karo.

Jab Pwnbox start ho jaye, toh zyada clearly dekhne ke liye `Full Screen` button par click kar sakte ho.

Uske baad, example mein dikhaye gaye tarike se apne mouse cursor ka use karke `Parrot Terminal` open karo.

`ifconfig` tool ka use network interfaces ko configure karne aur unki current status ko display karne ke liye kiya jata hai.

Ifconfig -a

By default, ye sirf active network interfaces ko show karta hai. Lekin agar hum `-a` flag ka use karte hain, toh ye sabhi interfaces ko display karta hai, including woh interfaces jo currently down hain.

Command run karne ke baad, humein 3 network interfaces dikhne chahiye:

- **`ens3`**
- **`lo`**
- **`tun0`**

Inke saath detailed output bhi dikhai dega.

Kuch samay nikaalkar inki information ko dhyan se dekho aur note karo ki in interfaces mein kya similarities aur differences hain.

Agar abhi kuch information samajh nahi aa rahi hai, toh chinta mat karo. Jaise-jaise hum aage badhenge, sab kuch aur clearly samajh aane lagega.

ifconfig -a

Ismein samajhne ke liye kaafi saari cheezein hain. Humein 3 alag-alag IPv4 addresses dikh rahe hain. Saath hi kuch IPv6 addresses bhi dikh rahe hain.

Lekin ek interface baaki sabse alag nazar aa raha hai. `lo` interface mein kuch alag lag raha hai.

Hum jo dekh rahe hain, use Loopback Address kaha jata hai. Yeh hamesha IPv4 address `127.0.0.1` se juda hota hai.

Yeh IP address tab use hota hai jab kisi device ko network data khud apne hi paas bhejna hota hai.

Aap soch rahe honge ki iska kya kaam hai? Iske kai kaam hain.

- Testing: Iska use aksar testing ke liye hota hai, taaki network par live karne se pehle check kiya ja sake ki application sahi tarah kaam kar rahi hai ya nahi.
- Security: Servers bhi iska use kuch services ko bahar ke users se hidden rakhne ke liye karte hain.

Ek e-commerce website ka example sochiye, jo apne clients ke saath authentication use karti hai (yaani registered accounts, jinmein username aur password hote hain).

Login credentials aur session cookies aam taur par ek database mein store hote hain.

Database ko public ke saamne expose karne ke bajaye, use sirf server ke liye accessible rakha ja sakta hai.

Jab koi user website par login karne ki koshish karta hai, toh website user aur database ke beech API ki tarah kaam karti hai.

Server, end user ki taraf se information retrieve karne ke liye apne hi database se query karta hai.

Ab dekhte hain ki Pwnbox mein Loopback Address use ho raha hai ya nahi.

Apne terminal mein neeche diya gaya command enter karein:

---

netstat -tulnp4

`netstat` utility network connections, routing tables aur interface statistics ko display karti hai.

Upar diye gaye options ke saath, yeh IPv4 ke sabhi open ya listening TCP aur UDP ports ko **`IP:PORT`** format mein dikhati hai.

Agar permissions allow karti hain, toh yeh har open port ke liye us program ka naam bhi dikha sakti hai jo us port ko chala raha hai.

Output ko dhyan se dekhein.

Kya aapko Loopback Address par koi services running dikh rahi hain?

Jab hum `-n` option hata dete hain, toh output `IP:PORT` ke bajaye `hostname:service` format mein dikhai deta hai.

Hum dekh sakte hain ki Loopback IP address ko `localhost` mein convert kar diya jata hai.

`ens3` IP address ko Pwnbox ke hostname mein convert kar diya jata hai.

Ek aur important baat dhyan dene layak hai: jo service `0.0.0.0` par listening kar rahi hoti hai, woh sabhi network interfaces par listening kar rahi hoti hai.

Is information se ab humein samajh aa raha hai ki hum Pwnbox ko kaise dekh pa rahe hain aur uske saath kaise interact kar pa rahe hain.

Module ke shuru mein humne seekha tha ki websites browse karne ke liye `HTTP` protocol use hota hai, jo well-known port 80 par kaam karta hai.

Jaisa ki hum dekh sakte hain, Pwnbox bhi port 80 par listening kar raha hai. Isse samajh aata hai ki hum web browser ke through connection kaise bana pa rahe hain.

Iske baad hum confidence ke saath keh sakte hain ki `ens3` interface se juda IP address Pwnbox ka Public IP address hai.

Yaad rakhein, Public IP addresses ko internet ke through access kiya ja sakta hai.

Hum Loopback Address par VNC service bhi running dekh rahe hain.

VNC (Virtual Network Computing) ek protocol hai, jiska use remote screen sharing aur remote access ke liye hota hai.

Kyunki students apne web browser ke through Pwnbox ka desktop environment access kar sakte hain, isliye sambhav hai ki wahan kisi tarah ka Port Forwarding laga hua hai.

Isse HTTP ke through bheje gaye traffic ko Loopback Address par running VNC service tak forward kiya ja sakta hai.

Port Forwarding ek technique hai, jo ek TCP/UDP port par bheje gaye traffic ko kisi doosre port par redirect karne ki permission deti hai. Yeh alag-alag machines ke beech bhi ho sakta hai.

Loopback Address ka use karne ka yeh bhi ek tareeka hai.

Example ke liye, neeche diye gaye scenario mein ek Windows host apne local port `8888` ke traffic ko Linux VM ke SSH port `22` par forward karta hai.

Linux machine ek Virtual Machine hai jisme NAT enabled hai.

Iska matlab hai ki Linux machine ke paas network par directly access kiya ja sakne wala IP address nahi hai.

Iske bajaye, Windows host ek intermediary ki tarah kaam karta hai aur traffic ko Linux machine tak forward karta hai.

Chapter 2. - Having Tuns of Fun

Chapter One ki shuruaat mein humne bataya tha ki Pwnbox ka use hamare lab environments mein target machines ke saath interact karne ke liye hota hai.

Chapter One ke end tak humne available 3 network interfaces mein se 2 ko successfully samajh liya tha:

- Loopback (lo): Pwnbox ko khud apne paas network traffic bhejne ki permission deta hai.
- Public IP (ens3): Pwnbox ko internet ke through humse communicate karne mein help karta hai.

Ab ek interface baaki hai: `tun0`.

Iske naam se hum andaza laga sakte hain ki yeh ek Tunnel Interface hai, jo aam taur par VPNs (Virtual Private Networks) se juda hota hai.

Kyunki lab targets ek alag private network par hote hain, isliye Pwnbox ko us environment se ek secure connection banana padta hai, jisse hum un tak pahunch sakein.

Chaliye, check karke confirm karte hain ki target ke saath communicate karne ke liye Pwnbox kaunsa route use karta hai.

Is section ke end tak scroll karein aur `Click here to spawn the target system!` par click karein.

Kuch seconds baad ek target machine start ho jayegi aur humein uska IP address diya jayega.

Uske baad Pwnbox par wapas aayein aur Parrot Terminal mein neeche diya gaya command enter karein:

```
None
ip route get <target ip>
```

Yeh command dikhayega ki Pwnbox se target tak bheja gaya traffic kaunsa route follow karta hai.

```
None
┌──[eu-academy-1]─[10.10.14.21]─[htb-ac-594497@htb-5mix2gkv1a]─[~]
└──╼ [★]$ ip route get 10.129.233.197

10.129.233.197 via 10.10.14.1 dev tun0 src 10.10.14.21 uid 1002
    cache
```

Hamari theory confirm ho gayi hai — target tak jaane wala saara traffic `tun0` ke through route hota hai.

`tun0` ek VPN tunnel hai, jo Pwnbox ko private lab network se connect karta hai.

Iski help se hum lab machines ke saath aise interact kar sakte hain, jaise woh hamare same local network par hon.

VPN configuration file aur `OpenVPN` jaise software ka use karke computers VPN server se connect hote hain, jo unhe network access provide karta hai.

HTB Academy ka VPN section ke end mein download ke liye available hai. Yeh un logon ke liye hai jo Pwnbox ke bajaye apna khud ka workstation use karna pasand karte hain.

Target machine ke saath pehla interaction

Chaliye, ab target machine ke saath apna pehla interaction shuru karte hain.

Hum aam taur par sabse pehle `ping` ka use karte hain.

`ping` ek networking utility hai, jiska use check karne ke liye hota hai ki network par koi host reachable hai ya nahi.

Yeh TCP ya UDP ports ka use nahi karta. Isi wajah se OSI model ke hisaab se yeh `Layer 3` protocol hai.

Apne terminal mein neeche diya gaya command type karein aur output dekhein:

```
None
ping -c 4 <target ip>
```

Yahan hum apne target ki taraf 4 ping requests bhej rahe hain.

Dhyan dein, Linux mein agar hum ping ki count specify nahi karte, toh yeh lagataar (`indefinitely`) ping bhejta rahega, jab tak hum terminal mein `Ctrl + C` press nahi karte.

```
None
┌─[eu-academy-1]─[10.10.14.21]─[htb-ac-594497@htb-5mix2gkv1a]─[~]
└──╼ [★]$ ping -c4 10.129.233.197

PING 10.129.233.197 (10.129.233.197) 56(84) bytes of data.
64 bytes from 10.129.233.197: icmp_seq=1 ttl=127 time=71.6 ms
64 bytes from 10.129.233.197: icmp_seq=2 ttl=127 time=71.3 ms
64 bytes from 10.129.233.197: icmp_seq=3 ttl=127 time=71.8 ms
64 bytes from 10.129.233.197: icmp_seq=4 ttl=127 time=71.2 ms

--- 10.129.233.197 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 71.205/71.470/71.776/0.223 ms
```

Ab humne confirm kar liya hai ki hamara attack host target machine tak pahunch sakta hai.

Kuch important cheezein hain jin par dhyan dena chahiye: `ttl` aur `time`.

- TTL (Time-To-Live): Yeh batata hai ki target tak pahunchne ke liye hamare packets kitne "hops" le sakte hain.
  Yeh aam taur par un devices ke liye zyada useful hota hai jo hamare same local network par nahi hote, balki internet par hote hain. Aise devices tak pahunchne ke liye packets ko kai routers se hokar guzarna padta hai.

- Time: Iske paas di gayi information humein network ki latency ke baare mein batati hai. Upar diye gaye example mein har ping ko lagbhag `71 milliseconds` lag rahe hain.

Abhi humne target machine ke IP address par `ping` karke confirm kar liya hai ki hamara attack host target ke saath communicate kar sakta hai.

Open ports ko scan karna

Ab hamara agla step machine par open TCP/UDP ports ko enumerate karna hai.

Jaise humne Pwnbox ke open ports dekhne ke liye `netstat` utility ka use kiya tha, waise hi ek aur tool hai jiska use remote machine ke open ports pata karne ke liye kar sakte hain.

Is tool ka naam `nmap` hai. Yeh kisi bhi current ya future Infosec professional ke liye ek bahut hi important tool hai.

Chaliye, apne target ke open TCP ports ko enumerate karna shuru karte hain.

Apne terminal mein neeche diya gaya command enter karein:

```
None
nmap <target IP>
```

Kuch seconds baad `nmap` humein target machine par available open TCP ports dikha dega.

```
None
┌─[eu-academy-1]─[10.10.14.21]─[htb-ac-594497@htb-5mix2gkv1a]─[~]
└──╼ [★]$ nmap 10.129.233.197

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-08 18:07 CST
Nmap scan report for 10.129.233.197
Host is up (0.073s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
```

```
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
```

Hum dekh sakte hain ki kai ports open hain.

- Port 135, 139 aur 445: Windows-based host par aam taur par ye ports open rehte hain.
- Port 3389: Is port ka use Remote Desktop Protocol ke liye hota hai, jise short mein RDP kehte hain. Yeh Windows machines par dekhi jaane wali ek common service hai.
- Port 5357: Iska use `Microsoft's Web Services for Devices API` ke liye hota hai. Yeh ek aur Windows protocol hai, jiska use network par devices ko discover karne ke liye hota hai.

Ab hum Pwnbox ke teeno network interfaces ko achhe se samajh chuke hain aur yeh bhi verify kar liya hai ki hum target machine ke saath interact kar sakte hain.

Isi ke saath Chapter Two khatam hota hai.

Ab aap challenge questions aur assessment complete karne ke liye ready hain.

Agar aap aage continue karna chahte hain, toh Chapter Three optional hai. Ismein aapko specific ports aur protocols ka use karke target machine ke saath interact karna sikhaya jayega.

Chapter 3. - Target Acquired (OPTIONAL)

Hamare final chapter mein, hum target machine ke port `21` aur port `80` par focus karenge, jinhe `FTP (File Transfer Protocol)` aur `HTTP (Hyper-Text Transport Protocol)` ke liye use kiya jata hai.

Chalo ek aur `nmap` scan karte hain. Is baar hum sirf upar bataye gaye dono ports par focus karenge.

nmap -p21,80 -sC -sV <target ip>

`Apne scan mein` **`-sC`** `aur` **`-sV`** `options add karne se nmap ko ye pata lagane mein madad milegi:`

- `-sV: Kisi port par kaunsa program chal raha hai aur uska version kya hai.`
- `-sC: Us service ke baare mein extra information, jaise service ki configuration kaise ki gayi hai.`

```
eu-academy-1]─[10.10.14.21]─[htb-ac-594497@htb-5mix2gkv1a]─[~]
└──╼ [★]$ nmap -p21,80 -sC -sV 10.129.233.197

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-08 19:17 CST
Nmap scan report for 10.129.233.197
Host is up (0.071s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
80/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.05 seconds
```

`Nmap` hume batata hai ki FTP service mein Anonymous FTP enabled hai. Iska matlab hai ki koi bhi FTP service se connect kar sakta hai (usually username `anonymous` dekar).

Lekin port 80 par HTTP service utni information nahi deti.

Generally, `nmap` webserver ke software ko identify kar sakta hai, jaise `Apache`, `Nginx` ya `IIS`.

Hamara initial `nmap` scan, OSI Model ki Layer 4 par kaam karta hai. Yaani ye check karta hai ki TCP/UDP level par port open hai ya closed.

`-sV` (version scan) aur `-sC` (default scripts) jaise scans ke liye `nmap`, protocol-specific Layer 7 packets ka use karta hai.

Hamare second scan ke baad bhi port 80 se koi extra information nahi mili. Isliye hum andaza laga sakte hain ki wahan kisi tarah ki Request Filtering lagi hui ho sakti hai. Iske baare mein hum thodi der mein aur jaanenge.

IMPORTANT: Kisi aise device par `nmap` (ya koi bhi port scanning tool) use karna, jo aapka nahi hai ya jise scan karne ki aapke paas clear permission nahi hai, illegal na bhi ho, lekin ise unethical (galat) maana jata hai.

Ab chalo port 21 par chal rahi FTP service ko check karte hain.

Connect karne ke liye hum netcat use karenge. Ye ek utility hai jo raw TCP/UDP connections banane ke kaam aati hai.

Jab hum `netcat` se connect ho jayenge, toh hum jo bhi characters type karenge, woh us port par send ho jayenge jisse hum connected hain.

Ek specific `FTP client` utility use karne ke bajaye, hum `netcat` use karenge, taaki humein samajh aaye ki FTP protocol kaise kaam karta hai.

Dusri taraf, HTTP service ke liye web browser ya command-line tools jaise `curl` aur `wget` apne aap protocol-specific data ko format karke send kar dete hain.

Jab aap ready ho, toh apne terminal mein neeche diya gaya command enter karo aur Enter press karo.

---

nc <target ip> 21

Yahan hum `netcat` ko keh rahe hain ki target machine ke port 21 se connect ho.

Connect hone ke baad, FTP service ki taraf se humein ek banner dikhai deta hai. Iska matlab hai ki hum successfully connect ho chuke hain.

```
┌─[eu-academy-1]─[10.10.14.21]─[htb-ac-594497@htb-5mix2gkv1a]─[~]
└──╼ [★]$ nc 10.129.233.197 21
```

220 Microsoft FTP Service

Next, hum neeche diye gaye commands ka use karke `anonymous user` ke roop mein login karenge. Uske baad hum specify karenge ki hum Passive Mode ka use karenge.

USER anonymous[Ctrl+V][Enter][Enter]
PASS anything[Ctrl+V][Enter][Enter]
PASV[Ctrl+V][Enter][Enter]

Humne `[Ctrl + V] [Enter] [Enter]` ka use isliye kiya, kyunki FTP ke commands ke liye `return character` aur `new-line character (\r\n)` dono zaroori hote hain.

Jab hum keyboard par sirf Enter press karte hain, toh Netcat keval `\n` send karta hai.

```
┌──[eu-academy-1]─[10.10.14.21]─[htb-ac-594497@htb-5mix2gkv1a]─[~]
└──╼ [★]$ nc 10.129.233.197 21
```

220 Microsoft FTP Service
USER anonymous^M
331 Anonymous access allowed, send identity (e-mail name) as password.
PASS anything^M
230 User logged in.
PASV^M
227 Entering Passive Mode (10,129,233,197,194,40).

FTP (File Transfer Protocol) apne operations ke liye 2 alag channels ka use karta hai:

Channel	Kaam (Purpose)	Port
Control Channel	FTP commands send karta hai (USER, PASS, LIST, RETR, etc.)	Port 21
Data Channel	Files aur directory listings transfer karta hai	Dynamic Port (Active ya Passive mode ke hisaab se change hota hai)

Yahan humne Passive Mode select kiya hai. Iske baad humein FTP server se kisi doosre port par dobara connect karna hoga.

Port number pata karne ke liye humein kuch calculations karni hongi.

Aisa mainly FTP protocol ki limitations ki wajah se hota hai. Isme poora port number ek saath display nahi ho sakta. Isliye port number ko 2 chhote numbers mein divide kar diya jata hai: `p1` aur `p2` (upar diye gaye output ke last 2 numbers).

Uske baad actual port number calculate karne ke liye ye formula use hota hai:

```
p1 * 256 + p2
```

Iske baare mein aur information ke liye ye documentation dekho.

Ab port number calculate karne ke liye hum last ke 2 numbers use karenge. Upar diye gaye example mein ye numbers `194` aur `40` hain.

- Pehle number ko `256` se multiply karenge.
- Phir usme doosra number add kar denge.

```
194 * 256 + 40 = 49704
```

Ab ek naya Parrot Terminal open karte hain.

Iske liye apne current Parrot Terminal ke top-left corner mein `File` par click karo. Phir `Open Terminal` → `Bash` select karo.

Ab naye Terminal mein hum `netcat` ka use karke Data Channel se connect karenge.

nc -v <target ip> <dynamic port>

┌──[eu-academy-1]─[10.10.14.21]─[htb-ac-594497@htb-5mix2gkv1a]─[~]
└──╼ [★]$ nc -v 10.129.233.197 49704

10.129.233.197: inverse host lookup failed: Unknown host
(UNKNOWN) [10.129.233.197] 49704 (?) open

Ab chalo apne pehle Terminal par wapas chalte hain aur Connection Channel ka use karke FTP share mein available files ki list dekhenge.

Iske liye neeche diya gaya command enter karo:

LIST[Ctrl+V][Enter][Enter]

Humein ek message dikhna chahiye, jo batayega ki Data Connection pehle se open hai, isliye ab file transfer start ho raha hai.

┌──[eu-academy-1]─[10.10.14.21]─[htb-ac-594497@htb-5mix2gkv1a]─[~]
└──╼ [★]$ nc 10.129.233.197 21

220 Microsoft FTP Service
USER anonymous^M
331 Anonymous access allowed, send identity (e-mail name) as password.
PASS anything^M
230 User logged in.
PASV^M
227 Entering Passive Mode (10,129,233,197,194,40).

LIST^M
125 Data connection already open; Transfer starting.
226 Transfer complete.

Jab hum Data Channel check karte hain, toh humein note ka content dikhai deta hai

```
┌─[eu-academy-1]─[10.10.14.21]─[htb-ac-594497@htb-5mix2gkv1a]─[~]
└──╼ [★]$ nc -v 10.129.233.197 49714
```

10.129.233.197: inverse host lookup failed: Unknown host
(UNKNOWN) [10.129.233.197] 49714 (?) open
Bertolis,

The website is still under construction. To stop users from poking their nose where it doesn't belong, I've configured IIS to only allow requests containing a specific user-agent header. If you'd like to test it out, please provide the following header to your HTTP request.

User-Agent: Server Administrator

The site should be finished within the next couple of weeks. I'll keep you posted.

Cheers,
Jarednexgent

IT team ke note mein kuch important information mili hai.
Pata chala hai ki Web Server ko is tarah configure kiya gaya hai ki woh sirf unhi requests ko allow karta hai, jinmein ek specific User-Agent Header diya gaya ho.
Humne dekha hai ki FTP protocol mein USER, PASS, PASV, LIST aur RETR jaise commands hote hain.
Lekin HTTP protocol mein Requests aur Responses ka system use hota hai, jismein HTTP Headers hote hain.
Agar hum ye header provide karte hain:
User-Agent: Server Administrator
Toh hum port 80 ke through serve ho rahi website ko dekh sakenge.
Ab chalo, neeche diye gaye command ka use karke netcat ke saath apna initial TCP Connection banate hain:

nc -v <target ip> 80

Humein ek message dikhai deta hai, jo batata hai ki port open hai.

┌──[eu-academy-1]─[10.10.14.21]─[htb-ac-594497@htb-5mix2gkv1a]─[~]
└──╼ [★]$ nc -v 10.129.233.197 80

10.129.233.197: inverse host lookup failed: Unknown host
(UNKNOWN) [10.129.233.197] 80 (http) open

Ab hum apni HTTP Request taiyar kar sakte hain. Apne netcat session mein neeche diya gaya text enter karo:

┌──[eu-academy-1]─[10.10.14.21]─[htb-ac-594497@htb-5mix2gkv1a]─[~]
└──╼ [★]$ nc -v 10.129.233.197 49714

10.129.233.197: inverse host lookup failed: Unknown host
(UNKNOWN) [10.129.233.197] 49714 (?) open
Bertolis,

The website is still under construction. To stop users from poking their nose where it doesn't belong, I've configured IIS to only allow requests containing a specific user-agent header. If you'd like to test it out, please provide the following header to your HTTP request.

User-Agent: Server Administrator

The site should be finished within the next couple of weeks. I'll keep you posted.

Cheers,
jarednexgent

IT team ke note mein kuch important information mili hai.
Pata chala hai ki Web Server ko is tarah configure kiya gaya hai ki woh sirf unhi requests ko allow karta hai, jinmein ek specific User-Agent Header diya gaya ho.
Humne dekha hai ki FTP protocol USER, PASS, PASV, LIST aur RETR jaise commands ko pehchanta hai.
Dusri taraf, HTTP protocol Requests aur Responses ke system ka use karta hai, jismein HTTP Headers hote hain.
Agar hum User-Agent: Server Administrator header provide karte hain, toh hum port 80 ke through serve ho rahi website ko dekh sakte hain.
Ab chalo, neeche diye gaye command ka use karke netcat ke saath apna initial TCP Connection banate hain:

nc -v <target ip> 80

Humein ek message dikhai deta hai, jo batata hai ki port open hai.

```
┌──[eu-academy-1]─[10.10.14.21]─[htb-ac-594497@htb-5mix2gkv1a]─[~]
└──╼ [★]$ nc -v 10.129.233.197 80

10.129.233.197: inverse host lookup failed: Unknown host
(UNKNOWN) [10.129.233.197] 80 (http) open
```

Ab hum apni HTTP Request taiyar kar sakte hain. Apne netcat session mein neeche diya gaya text enter karo:

```
GET / HTTP/1.1[enter]
Host: <target ip>[enter]
User-Agent: Server Administrator[enter][enter]
```

Web Server humein response deta hai!

Jab hum web browser use karte hain, toh browser automatically HTTP Request send karta hai aur HTML ko ek sundar aur aasani se padhne layak website mein convert karke dikhata hai.

Lekin jab hum `netcat` use karte hain, toh webpage ka content directly hamare Terminal mein print hota hai.

Hum HTML ke comments mein chhupa hua ek Flag bhi find kar sakte hain.

Agar hum web browser use karte, toh ye hidden flag humein dikhai nahi deta.

```
┌──[eu-academy-1]─[10.10.14.21]─[htb-ac-594497@htb-5mix2gkv1a]─[~]
└──╼ [★]$ nc -v 10.129.233.197 80

10.129.233.197: inverse host lookup failed: Unknown host
(UNKNOWN) [10.129.233.197] 80 (http) open
GET / HTTP/1.1
Host: 10.129.233.197
User-Agent: Server Administrator

HTTP/1.1 200 OK
```

```
Content-Type: text/html
Accept-Ranges: bytes
ETag: "5acd7854a179db1:0"
Server: Microsoft-IIS/10.0
Date: Tue, 5 Feb 2025 00:44:43 GMT
Content-Length: 746

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
   color:#000000;
   background-color:#0072C6;
   margin:0;
}

#container {
   margin-left:auto;
   margin-right:auto;
   text-align:center;
   }

a img {
   border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&amp;clcid=0x409"><img
src="iisstart.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
<!-- HTB{REDACTED} →
```

`GET /` ek HTTP Request hai, jo Web Server ko kehti hai: "Mujhe is website ka Homepage (Root Directory) do."

Agar humein kisi website ka Login Page access karna ho, toh hamari request kuch aisi ho sakti hai:

```
GET /login.php
```

`Host` Header server ko batata hai ki hum kis host ko request bhej rahe hain. Ek hi server par multiple alag-alag websites host ho sakti hain.

`User-Agent` Header batata hai ki Web Request kaun sa agent bhej raha hai.

Example: Agar browser request bhej raha hai, toh User-Agent mein usually browser ka naam aur version hota hai.

Server bhi apne Headers ke saath reply karta hai:

- `Content-Type` Header: Batata hai ki server kis type ka data reply mein bhej raha hai.
- `Accept` Header: Batata hai ki client kis type ka data receive kar sakta hai.
- `Server` Header: Batata hai ki server par kaunsa Web Server Software use ho raha hai. Yahan ye Microsoft IIS hai.

In Headers ke neeche us website ka HTML code hota hai, jise hum access karne ki koshish kar rahe hain.

Ab humne khud dekha ki FTP aur HTTP protocols kaise kaam karte hain.

Specific data packets send karke hum us `protocol` ko follow karte hain. Yaani us particular service ki specific "language" mein baat karte hain.

Humne dekha:

- FTP Data Channel aur Connection Channel dono ka use karta hai.
- FTP protocol mein commands ke saath New-line aur Return characters send karna zaroori hota hai.
- Dusri taraf, HTTP protocol syntax ke mamle mein zyada flexible hai.
- Lekin agar koi request administrator ke banaye rules ko follow nahi karti, toh HTTP use accept nahi karta.

Example: Agar request mein administrator ke according required `User-Agent` Header nahi hai, toh server request ko reject kar sakta hai. Ise User-Agent Header Request Filtering kehte hain.

Q. What IPv4 address is used when a host wants to send and receive network traffic to itself?

Ans.

Q. What is the the name of the Program listening on localhost:5901 of the Pwnbox?

Ans.

Q. Which network interface allows us to interact with target machines in the HTB lab environment?

Ans.

Q. What command-line tool is used to configure network interfaces and display their current status?

Ans.

Q. What command-line tool is used to display network connections, routing information, and interface statistics?

Ans.

Optional Exercise :- 1
Q. What is the FTP command used to retrieve a file? (Format: XXXX)
Ans.

Optional Exercise :- 2
Q. Bypass the request filtering found on the target machine's HTTP service, and submit the flag found in the response. The flag will be in the format: HTB{...}
Ans.