Day-2 :- [Networking Fundamentals & Security].

No.
Date

1.) Network, Networking, Internet & their fundamentals.

(a) Network :- Collection of interconnected devices that can communicate and share resources.

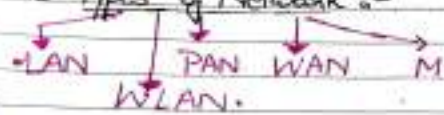
(b) Networking :- Process of connecting devices to enable communication.
(Network Access Types).

(c) Internet :- Global network of interconnected networks using TCP/IP protocols.
→ Access : public, used by anyone with internet access., protocols : TCP/IP., low security

(d) Intranet :- Private network used within an organization.
→ Restricted to internal users, used by employees internal staff., protocols :-> TCP/IP.
→ Secured by -> Firewalls.

(e) Extranet :- Controlled private network allowing external partners limited access to internal resources.
→ Restricted: (External + Internal users).
→ Protocols : (TCP/IP with VPN).
→ High security.

⊙ Types of Network :-



1.) LAN :- (Local-Area-Network)

→ Covers small area like an office or home
• offers high speed and is used for internal communication & sharing

2.) WAN :- (Wide-Area-Network)
Spans large geographical area.
Used to connect cities or countries, like the internet. Slower speed

3.) MAN :- (Metropolitan Area Network)
Covers a city or large campus.
Bridges LANs within a limited metro range.

4.) PAN :- Very small range (upto 10 mts).
Used to connect personal devices.
[Personal-Area-Network]

5.) WLAN :- (Wireless LAN).
Lan using wireless signals
Common in home, cafes & offices.

▸ Network Topologies :-

① Star-Topology :- All nodes connect to a central hub. Easy to manage, isolate faults quickly. Failure of central hubs disrupts the network. Common in LANs.

② Bus Topology :- All devices share a single backbone cable. Simple setup and minimal cabling. Backbone failure crashes entire network. Small, temporary networks

③ Ring Topology :- Devices form a closed loop, data travels in 1 direction.
Efficient for predictable traffic.
Single node failure disrupts network
Use: FDDI, SONET.

④ Mesh Topology :- Every device connects to every other. Highly reliable, redundant paths. Expensive and complex to implement. Used in Military, missiles -critical systems

⑤ Hybrid Topology :- Combination of two or more topologies. Complex config
Flexible & scalable. Used by large enterprise network.

Network Components :-

•) Network components are hardware and media used to established, maintain, and secure communication between systems in a network. They include connecting devices, data transfer medium and interfaces critical to cybersecurity.

•) Network Devices (Active Components)

ⓐ Router :- Connects different network (e.g. LAN to Internet)
- Routes packets based on IP address
- Operates at OSI Layer 3 (Network Layer)

ⓑ Switch :- Connects multiple devices within the same LAN. Forwards data based on MAC addresses. Operates @ OSI Layer 2 (Data Link Layer).

ⓒ Hub :- Broadcasts incoming data to all devices. No intelligence, no security filtering. Operates @ OSI layer 1 (Physical layer)

d. Modem :- Modulates digital signals to analog and demodulates back.
- Connects local devices to ISP over phone / cable lines.

e.) Access Point (AP) :- Provides wireless LAN access. Connects wireless devices to wired network.

f.) Firewall :- Filters traffic based on security rules (IP, port, protocol). Can be hardware, software, or cloud-based.

g.) Server :- Provides services to client (eg → file, web, mail). Centralized processing and data access.

h.) Client :- Devices that request services from servers. Includes PCs, laptops, mobile devices. Entry point for social engineering, malware.

•) Transmission Media :- Transmission media are physical or wireless channels used to transfer data between devices in a network.

CLASSIFICATION

No.

Date

Wired	Wireless.
Twisted Pair, Coaxial, fiber optic	Radio waves, infrared, & micro wave.

- Twisted Pair :→ Common Ethernet Cable (CAT 5/6)
- Coaxial Cable :→ Used in older LANs & Cable TV.
- Fiber Optic :- High speed, long-distance, secure.
- Wireless Media :-

① Radio Waves → Used in Wi-Fi

② Micro Waves → Point-to-Point links

③ Infrared → for short range line of sight communication.

- NIC (Network Interface Card)

→ Hardware installed in devices for network connectivity.
→ Each NIC has unique MAC address.

No.

Date

• Purpose of Each Layer :-

① **Physical** :- Transmits raw bits over physical medium.

② **Data Link** :- Provides MAC addressing & error detection

③ **Network** :- Handles logical addressing and routing (IP). and Path determination

④ **Transport** :- Ensures reliable data delivery, also do error control.

⑤ **Session** :- Manages session and control dialog.

⑥ **Presentation** :- Formats and encrypts/decrypts data. [Ec^2] Compression conversion

⑦ **Application** :- Interface for users interacts with network services.

Msg ⑦ :-

- MAC Address : Unique identifier of NIC
- Switches & Bridges :- Manage local traffic using MAC
- Frame :- Data encapsulated with MAC headers.
- Protocols :- Ethernet, ARP, PPP.
- VLANs (802.1Q) :- Isolate traffic logically

• Vulnerabilities :-
- MAC flooding
- ARP spoofing / poisoning
- VLAN hopping security measures :-
  - Port security on switches
  - Dynamic ARP Inspection (DAI)
  - MAC address filtering.

3. Network Layer :- Routing packets across different networks

• Components :-
- IP addressing : IPv4 (32-bit), IPv6 (128 bit)
- Routing Types : Static, Dynamic (RIP, OSPF, BGP).
- Devices : Routers
- Protocols : IP, ICMP (Ping), IGMP
- NAT : Translate private to public IP.
- Vulnerabilities :
  - IP spoofing
  - ICMP tunneling
  - Ping flood / ICMP DoS
- Security Measures :-
  - Firewalls (Layer 3 filtering)
  - Access control lists (ACLs).
  - IPSec for IP communication

4.) Transport Layer :- End to End connection and error control

• Components :-
- Protocols : TCP (connection-oriented)
- UDP (connectionless) ~~:- Ping~~
- Ports :-

WellKnown : 0 - 1023 (HTTP 80, HTTPS 443, FTP 21, SSH 22)
- Registered :- 1024 - 49151
- Dynamic / Private :- 49152 - 65535.

- TCP Mechanisms :- Three-way handshake

• Flow control, error recovery Vulnerabilities :-
- Port scanning
- TCP SYN flood
- Session hijacking

• Security Measures :-
- Stateful firewalls
- Intrusion detection/prevention system (IDS/IPS)
- Use secure protocols → (HTTPS, SSH).

5) Session Layer (Layer 5) :-
Manage sessions between applications.

• Components : - Session creation/termination
- Authentication & authorized protocols
- APIs, Net BIOS, RPC

• Vulnerabilities :- - Session hijacking
- Session fixation
- MITM

• Security Measures :-
- Secure session tokens
- TLS for encrypted session handling.
- MFA for session authentication.

6. Presentation Layer :- Data translation, encryption & formating

Components :-
- Data formats : ASCII, JPEG, MP3, MP4, HTML, XML, JSON
- Encryption / Decryption :- SSL/TSL
- Compression :- GZIP, MPEG

• Vulnerabilities :-
- SSL downgrade attack
- Padding oracle attack
- Malformed data injection

- Security Measures:
  - Use strong encryption protocols (TLS 1.3)
  - Certificate validation
  - Avoid weak ciphers.

7.) Application Layer :

Closest to the user, handles application-level protocols.

Protocols :

- Web : HTTP, HTTPS
- Email : SMTP, POP3, IMAP
- File transfer : FTP, SFTP
- Remote Access : SSH, Telnet
- Others : DNS, DHCP, SNMP

Vulnerabilities :

- SQL injection
- Cross-Site Scripting (XSS)
- DNS Spoofing
- Email spoofing/phishing

Security Measures:

- Web Application Firewall (WAF)
- Input validation
- Secure coding practices
- Use DNSSEC for DNS

- Summary - Table :-

Layer	Devices/Protocols	Attacks	Controls
L1	Hub, Cables	Wiretap	Locks, CCTV
L2	Switch, ARP	ARP Spoof	Port Secur
L3	Router, IP	IP Spoof	Firewalls
L4	TCP/UDP, Ports	SYN Flood	IDS/IPS
L5	API, RPC	Hijacking	Token Auth
L6	SSL, TLS	Downgrade	TLS 1.3
L7	HTTP, DNS, SMTP	XSS, SQLi	WAF

(end)

• IP Addressing :-

An IP (Internet Protocol) address is a unique numerical identifier assigned to each device on a network. It enables communication between devices by specifying source and destination addresses in a data packets.

• Types of IP - Addressing :-

1.) IPv4.

• Internet Protocol v4
• Size :- 32-bit (4 octet)
• Common, supports ~4.3B devices
→ eg) 192.168.1.1

→ Address Format
⇒ Dotted decimal

→ Address Space : 2^{32} (4.3 bn)

2.) IPv6.

• Internet Protocol v6
• 128-bit.
• Next gen, supports ~340 undecillion
eg) fe80::1

→ Hexadecimal, Seperated by colons

→ 2^{128} (340 undec)

A.) IPv4 :-

• Classes :- A (1.0.0.0), B (128.0.0.0), C (192.0.0.0), D (Multicast), E (Reserved) — Public.

• Private Ranges :-

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

• Security Issues :- IP spoofing, Dos attack, easy scanning.

B.) IPv6 :-

→ Simplification Rules :-

① Leading zeros can be omitted
② Double colons (::) for consecutive 0 blocks

→ eg) 2001 : 0db8 : 85a3 : 0000 : 0000 : 8a2e : 0370 : 7334

- Security Benefits :-

→ Built-in IPsec support
→ No NAT (end-to-end traceability)
→ Larger space = harder scanning

- Still vulnerable to : MITM, DDoS, DNS poisoning if misconfigured.

- IPv4 v/s IPv6 - Comparison Table :-

Feature	IPv4	IPv6
Bit Size	32 bit	128
Format	Decimal	Hexadecimal
Address Space	4.3 bn	340 undeci
Header Size	20 bytes	40 bytes
Security	Optional IPsec	Mandatory IPsec
NAT Usage	Required for Security	No needed
Configuration	Manual / DHCP	Auto config
Broadcast	Supported	Not supported

IP Address Type (in both IPv4 & IPv6)

- Public IP - Globally routable
- Private IP - Internal use within LAN
- Static IP - Fixed address
- Dynamic IP - Changes, assigned by DHCP
- Loopback - IPv4 : 127.0.0.1 | IPv6 : ::1
- Link local - IPv6 : fe80::/10 (used for communication within the same link)
- → APIPA → auto assigned when DHCP fails
- → Multicast IP - Delivers packets to multiple hosts
- → Broadcast IP - Sends packet to all devices in network segment

(1) Public type :- Routable on internet
assigned by ISP
eg) 8.8.8.8
Relevance → Identifies devices on internet
in cyber sect.

(2) Private IP → Used in internal network, not routable on internet
eg) 192.168.1.1.
Cyber → Common in LAN, NAT required for internet

(3) Static IP → Manually assigned, doesn't change. Assigned by admin
cyber → Servers, DNS Hosting, router tracking

(4) Dynamic IP → Assigned via DHCP, changes over time
example :- Varies
Cyber → Harder to track, used by ISPs for clients

(5) Loopback IP :- Refers to self
eg) 127.0.0.1
used in testing, internal communication

(6) APIPA :- Auto-assigned when DHCP fails (Windows)
eg) 169.254.x.x . Cyber → Indicates ↓ issues

(7) Link local (IPv6) :- Used for communication within a local segment.
ex) fe80::/10 . Cyber :- Auto-configured, no need for DHCP

(8) Multicast IP → Delivers packets to multiple hosts
eg) 224.0.0.0 - 239.255.255.255
Cyber → Used in routing protocols, security monitoring

(9) Broadcast IP →
Sends packet to all devices in network segment
eg) 255.255.255.255.
Cyber → Can be abused in DoS

• IPv4 Address Classes (A to E):

Class	Address Range	Default Subnet Mask
A	1.0.0.0 - 126.255.255.255	255.0.0.0
B	128.0.0.0 - 191.255.255.255	255.255.0.0
C	192.0.0.0 - 223.255.255.255	255.255.255.0
D	224.0.0.0 - 239.255.255.255	N/A
E	240.0.0.0 - 255.255.255.255	N/A

Class	1st Octet Range	Hosts/Net
A	1 - 126	~16 mn
B	128 - 191	~65K
C	192 - 223	~254
D	224 - 239	N/A

Class	1st Octet	Most Networks
E	240 - 255	N/A

Class	Use Case
A	Very large network (Govt)
B	Medium network (University)
C	Small network (Offices)
D	Multicasting (one to many communication)
E	Experimental, research, reserved.

- 127.x.x.x is reserved for loopback testing, not used for networking
- Classes D & E are not for host addressing.

No.

Date

⊙ Public v/s Private IP Address

→ ① Public :- Routable on internet, globally unique. Assigned by ISPs

② Private :- Not routable on the internet, used within private network

∴ Private IP Ranges (RFC 1918) :-

Class	Range	CIDR
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

★	Subnet Mask
B	255.240.0.0
C	255.255.0.0
A	255.0.0.0

Public IP :- Used in webservers, email servers

Private IP :- Home networks, internal enterprise LANs.

No.

Date

⊙ Security Comparison

Type	Exposure to Int	Attack surface
Public IP	Fully	High
Private	Isolated	low

eg: Public ip ⇒ 103.52.96.24

Private IP = 192.168.1.101

Key differences :-

Feature	Public IP	Private IP
Scope	Global	local
Uniqueness	Globally unique	not globally unique
Routable over Internet	Yes	No
assigned by	ISP	DHCP
Cost	May be Chargeable	Free
NAT Required	No	Yes
Conflict Possibility	NO	Yes
Common Ranges	Varies	10.x.x.x, 172.16.x.x, 192.168.x.x

① Reason for Private IP Ranges :-
- (a) Avoid IP exhaustion
- (b) Allows internal communication without Internet exposure
- (c) Required NAT to access internet

② CIDR Notation Eg:-
- Class A (10.0.0.0/8)
- Class B (172.16.0.0/12)
- Class C (192.168.0.0/16)

③ Static v/s Dynamic IPs(basic):-
- Static ⇒ manually assigned, fixed
- Dynamic = assigned via DHCP, Change over time.

↳ Static → used for servers, routers, VPNs or resources needing Consistent accessibility
Easier for DNS mapping, firewalls rules, remote access.

↳ Dynamic → Changes periodically used for home users, end user devices

Key diff	Static	Dynamic
Assignment	Manual	Automatic
IP Address change	Never	Can change anytime
Use-Case	Servers, hosting	Home users
Cost	High	Lower or free
Security Risk	Higher (easy to target)	Lower (changes often)

↳ Dynamic IPs reduce persistent attack surface but hinders consistent monitoring

↳ Firewalls and VPN configurations often rely on static IPs.

End

• CIDR :- (Classless Inter-Domain Routing) and ~~Slash Notation~~

→ CIDR is a method for allocating IP addresses and IP routing that replaces old class based system. Introduced to improve address efficiency and routing scalability.

2. Format : IP_address/Prefix_Length
Eg) 192.168.1.0/24

3) Prefix length (/x):
Indicates how many bits are for the network portion.

• /24 = 255.255.255.0 (24 bits for network, 8 bits for host)

4) Subnet Mask Mapping

CIDR	Subnet Mask	Hosts Per Subnet
/8	255.0.0.0	16,777,214
/16	255.255.0.0	65,534
/24	255.255.255.0	254
/30	255.255.255.252	2

5. Purpose :-

• More efficient IP address use
• Enables subnetting without strict class rules
• Reduces routing table size

6. Example Comparison :

• Classful : Class C → 192.168.0.0 to 192.168.255.255 (Fixed/2
• CIDR : 192.168.0.0/22 → Combines multiple Class C network.

→ CIDR eliminated wasteful address allocation of classful system and supports VLSM.

x x x

(End)

(Net masking to CIDR (7.5/10) for notes.

Subnetting and it's Basics :-

Subnetting :- Dividing a larger network (IP block) into smaller, manageable subnetworks. Help in efficient IP allocation, Traffic isolation, and security.

• Why it is used in CyberSecurity :-

- Limits broadcast domains
- Enhances network segmentation and isolation
- Aids in access control and containment
- Reduces attack surface.
- Optimize routing and monitoring.

• Key Terminologies :-

→ IP address : Identifies a device on network
→ Subnet Mask : Determines which part of IP is network v/s host.
→ Network Address : First Address in subnet (identifies Subnet)
→ Broadcast Address : Last Address (used to send all hosts)
→ Host Address Range :- Usable IPs between network and broadcast.

• Subnet Mask Format :-

- Written in two ways :

→ Dotted Decimal : 255.255.255.0
→ CIDR Notation : /24 → means 24 bits for network.

• Subnetting Formulae :-

→ No. of Subnet = 2^n (n = borrowed bits)
→ No. of Hosts per Subnet = $2^h - 2$ (h = host bits, subtract 2 for network and broadcast addresses)

• Subnetting Example :-

Given : IP : 192.168.10.0/24
Need : 4 Subnets
- Borrow 2 bits → /26
- Subnet mask : 255.255.255.192
- Each subnet has 64 addresses → 62 usable hosts.

Subnets :

- 192.168.10.0/26 → Hosts .1 to .62
- 192.168.10.64/26 → Hosts .65 to .126
- 192.168.10.128/26 → Hosts .129 to .190
- 192.168.10.192/26 → Hosts .193 to .254

Common Use Cases in Security :-

- Isolating DMZ from internal networks
- Segmenting departments (e.g. → HR, IT, Finance)
- Containing malware outbreaks
- Enforcing policy-based access through firewall rules.

Tools to practice :- Subnet-calculator.com

(Cont)

- NAT (Network Address Translation) -

1. Definition :- It is a method that maps multiple private IP addresses to a single public IP to enable internet access. It hides internal IPs from external networks.

Purpose :- ① Masks internal network structure
② Adds layer of security
③ Conserves IPv4 addresses
④ Prevents direct access to internal hosts from the net.

2. TYPES of NAT :-

1. Static NAT :- One to one mapping between private and public IP
eg: 192.168.1.10 → 203.0.113.5

2. Dynamic NAT :- Maps private IPs to available public IPs from a pool
eg: 192.168.1.10 → Pool: 203.0.113.5-7

3. PAT (Port Address Translation)/Overloading :-

Many private IPs share one Public IP using different Ports.
eg: 192.168.1.10 :1024 → 202.0.113.5 : 3001

- Use → Enterprises connecting multiple devices to the internet using a single public IP
- Hiding internal server IPs
- Creating DMZs (Demilitarized Zones).

- Advantages :- ① IP Conservation
② Adds anonymity
③ Security.

- Limitations :- ① Complicated end-to end encryption.
  ② May break protocols that embed IP address
  ③ Requires port forwarding for hosting services.

3.) NAT v/s PAT :-

NAT	PAT
• Maps IP to IP	• Maps IP + Port to IP + Port
• Needs many public IPs	• Needs only 1.
• Less efficient	• More scalable.

- Use in Cyber security
  → Common in firewalls & routers
  → Essential in perimeter security
  → Obstructs external attackers from scanning internal IPs directly
- ALG : Helps NAT work with Protocols that embed IP info in Payload.

- IP-related attack Vectors :-

→ Attacks that exploit the internet Protocol (IP) layer to manipulate, spoof, intercept or disrupt communication between networked devices. These attacks commonly target weaknesses in packet structure, addressing, or trust mechanisms.

1. IP Spoofing :- Forging the source IP address in packet headers to impersonate another system.
   Goal → Bypass security filters, launch DDoS, or initiate MITM.
   Example : Attacker pretends to be a trusted IP to send malicious traffic.
   - Mitigation :- Ingress/egress filtering, reverse path forwarding, packet inspection.

2. DHCP Starvation Attack :-
   Flooding DHCP server with requests using spoofed MACs to exhaust IP addresses.
   Prevent legitimate users from obtaining IPs.

Example :- Attacker sends hundreds of fake DHCP requests.

Mitigation :- DHCP snooping, port security, rate limiting.

3.) Rogue DHCP Server Attack :-

Unauthorized DHCP server distributed false IP configurations.

Redirect users to malicious gateway for MITM or DoS

eg:- Attacker assigns himself as the gateway.

Mitigation :- DHCP snooping, trusted switch ports.

4.) MITM via IP spoofing :-

Attacker intercepts traffic by spoofing a trusted IP, becoming an invisible relay.

Goal ⇒ Eavesdrop, steal or modify data.

Example :- Spoof gateway IP to route all victim traffic through attacker

Mitigation :- Encryption, static ARP entries, mutual authentication.

5. Smurf Attack :-

Sending ICMP echo requests to broadcast addresses with victim's spoofed IP.

Amplify traffic to flood the victim.

Example :- Single ping triggers multiple replies directed at victim.

Mitigation :- Disable IP-directed broadcast, block spoofed packets.

6. Ping of Death :-

Sending oversized or fragmented ICMP packets to crash target system.

Goal → Cause buffer overflow and system instability.

Example : >65,535 byte packet crashes unpatched OS.

Mitigation :- Patch OS, inspect ICMP traffic.

7. IP Fragmentation Attack :-

Sending fragmented packets to evade firewall or IDS.

Goal → Hide payload or execute DoS.

eg → Payload is split across multiple fragments to bypass inspection

Mitigation : Deep packet inspection, fragment reassembly

8. Source Routing Attack :-

Exploiting IP option to control packet route through attacker-controlled nodes.

Goal → to bypass security controls, spoof identity.

Example :- Force packet to route through attacker's system before reaching target.

Mitigation :- Disable source routing on routers/firewalls.

- Defense Summary - IP related attacks.

1.) Ingress/Egress Filtering → Routers/firewalls drop ip packets. to block fake ips.

2.) DHCP Snooping :- Switch detects and blocks unauthorized DHCP servers

3.) Port Security :- Only specific MAC/IP combinations are allowed on switch ports.

4.) IDS/IPS Systems :- Detect and block suspicious IP behaviours like spoofing and fragmentation.

5.) Disable Source Routing :- Disabling source routing on routers prevents attackers from setting custom packet paths.

6.) Disable IP-Directed Broadcast :-
Blocks amplification source for Smurf attacks

7.) Packet Fragment Reassembly Inspection
Firewalls inspect reassembled fragmented packet to detect malicious payloads.

8.) System & Router Patching :-
Security patches protect against known IP-related exploits

9.) Traffic Encryption (SSL/TLS, VPN)-
Secures data from IP-level sniffing and MITM attacks.
(end)

• MAC Address :-

MAC (Media Access Control) address is a unique 48 bit hardware identifier assigned to the NIC of a device, used for communication at Layer 2 of OSI Model.

Format : 6 pairs of hexa-decimal digits.
(eg. 00:1A:2B:3C:4D:5E)

Divided into :-

- OUI (Organizationally Unique Identifier) :
  → First 24 bits - Manufacturer
- NIC Specific : Last 24 bits - unique device ID.

→ Characteristics :- • Burned into the hardware (ROM) of the NIC.
→ Unique globally
→ Doesn't change unless manually spoofed.
→ Works within local network (non-routable across internet)

→ Types	Description
• Unicast	Assigned to a single device
• Multicast	» » group of » »
• Broadcast	FF:FF:FF:FF:FF:FF → sends to all devices on LAN

Use Cases:-

→ Device Identification on LAN
→ ARP resolution (MAC ↔ IP mapping)
→ Network filtering (eg→ MAC filtering on Wi-Fi).
→ Switch forwarding decisions (via MAC table).

MAC Address Table:-

→ Switch maintains a table: MAC & Port
→ Helps in forwarding frames only to intended recipient's port.

MAC Address v/s IP Address

	Layer 2	Layer 3
Scope:-	Local Network	Global
Format	Hexadecimal	Decimal
Changeable	Static	Dynamic
Example	00:1A:2B:3C:4D:5E	192.168.0.1

MAC Spoofing :-

→ Attacker changes their MAC to impersonate another device.

→ Used in → ① Bypassing MAC filters
② MITM attacks
③ Session Hijacking.

Detection & Prevention :-

Method	Description
Port Security	Limits MAC addresses per port
802.1X Authentication	Uses credentials, not just MAC
Static ARP entries	Prevents ARP Spoofing using fixed MAC-IP
Intrusion Detection System.	Detect unusual MAC behaviour.

▸ Tools to View/Change MAC address :

OS	Command/Tool
Window	ipconfig/all, getmac, netsh
Linux	ifconfig, ip link, macchanger
MacOS	ifconfig

→ MAC is essential for Layer 2 Communication

→ Fixed per NIC unless spoofed
→ Switches use MAC for frame delivery

→ Security :- MAC spoofing must be detected and blocked via port security, 802.1x, or IDS

(end)

• DNS - (Domain Name System)

→ DNS is a hierarchical and decentralized system that translates human-readable domain names (eg → google.com) → machine readable IP addresses (eg 142.250.195.78)

→ Uses → → IPs are hard to remember, domain names are easier
→ enables communication between browsers and web servers

→ DNS v/s IP

Factor	DNS	v/s	IP
Human-readable →	Yes		NO
Memory-friendly →	Yes		NO
Static/Dynamic →	Dynamic mapping allowed		both

eg) When u type www.facebook.com
→ DNS converts to IP 157.240.18.35
→ Your browser connects to that IP and loads the page

⊙ DNS uses UDP for most of queries. TCP is used when

Key Components :-

① Domain Name : HUMAN-readable name
② IP address : Machine address
③ DNS Resolver : Queries DNS servers on behalf of users
④ Root server : Knows where TLD servers are
⑤ TLD Server : Handles .com, .org, .net etc
⑥ Authoritative Name Server : Has final DNS records for domain.

Works :-

① User types → www.example.com
② Request sent to DNS Resolver (ISP)
③ Resolver checks local cache
④ If not found :
Asks root server → TLD server → Authoritative server
⑤ Authoritative Server returns IP.
⑥ Resolver caches and sends IP to user's browser
⑦ Browser connects to IP and loads website.

DNS Record Types :-

Record Type	Description
A	Maps domain to IPv4 address
AAAA	Maps domain to IPv6
CNAME	Canonical name (alias for another domain)
MX	Mail exchange (email server info)
NS	Nameserver for domain
TXT	Arbitrary text, often for SPF
SOA	Start of Authority (contains domain admin info)
PTR	→ Reverse DNS (IP → Domain)

DNS Caching :-

- Local resolver or browser stores DNS info temporarily
- Reduces lookup time
- TTL (Time to Live) controls how long cache is valid.

TYPES of DNS Servers :-

→ Recursive Resolver : Does all lookup steps on behalf of Client

→ Root DNS server : Top-level server, directs to TLD

→ TLD Server :- For .com, .in etc.

→ Authoritative Name Server : Final answer source

DNS Query Types :-

- Recursive :- Resolver must return final answer or error.
- Iterative :- Resolver may return referral to other DNS server.

DNS Vulnerabilities :-

Attack Type	Description
DNS Spoofing	Fake DNS reply redirects to malicious IP
DNS Cache Poisoning	Alters cached DNS records
DDoS via DNS	DNS amplification attacks
DNS Tunneling	Uses DNS queries to exfiltrate data

DNS Security Measures :-

→ DNSSEC :- (Domain Name System Security Extension) it adds digital signature to prevent tampering

- Split DNS : Internal v/s Public DNS views

→ Firewall Rules :- Block unauthorized DNS traffic

→ Monitoring :- Detect anomalies or tunneling behaviour

- Common Tools → • nslookup, • dig, • host

→ DNS Ports → UDP 53 → Standard DNS queries

TCP 53 → Zone transfers, large responses.

→ Public DNS v/s Private DNS

→ Public : offered by providers like google, cloudflare

→ Private : Internal DNS for corporate or local networks

DNS attack Vectors Part-2

1) DNS Amplification attack :→ Reflection based DDos using spoofed DNS queries

(2) Domain Hijacking :- Unauthorized access or control of domain registration

(3) NX DOMAIN Attack :- Flooding resolver with non-existent domain to exhaust resources

(4) Phantom Domain Attack :- Resolver waits on slow/non-responsive domains, causing delays

(5) Subdomain Attack :- Abuse of wildcard DNS or excessive sub-domain requests.

(6) Random Subdomain Attack :- Generating random sub-domains by bypass cache

(7) Typosquatting :- Registering mistyped domain variants to decieve users.

→ Authoritative v/s Non-authoritative DNS

→ Stores original source data for domain. Provides final answer	→ Caches answers from other servers. Delivers response from cache.
→ Trusted source	Fast response via cache

DAT-0

DNS Zone, Zone Transfer:

→ **DNS Zone:-** Portion of DNS namespace managed by one authority.
eg: example.com and it's subdomains

- **Zone file:-** Contains mapping of names to IPs.

- **Zone Transfer:** (AXFR) Mechanism to replicate DNS zone data from master to slave DNS servers.

- **Risk:-** If unsecured, can leak internal domain structure to attackers.

Reverse DNS lookup (rDNS)

→ Maps IP → Domain Name (opposite of regular DNS)

→ Uses PTR Record

→ Use → Email spam filtering, CTI correlation.

eg: 8.8.8.8 → dns.google.

DNS Logging and Monitoring

→ logs: Store DNS queries/responses for analysis

→ Detects: Data exfiltration, tunneling, C2 communication

→ Tools → dnstop, Bro/Zeek, Splunk

→ Monitored fields: Source IP, Query Type, Query domain, Response Code

---

DNS vs HTTP.

Feature	DNS	HTTP
Protocol Layer →	Application	→
Port	53	80/443
Response	IP address	Web Page/content
Purpose	Resolves domain to IP	Web communication

→ DNS vs DHCP

Feature	DNS	DHCP
Role	Resolves domain to IP	Assigns IP to device
Port	53	67/68
Server Type	Recursive/Authoritative	DHCP Server
Triggered by	Client DNS query	Device joining network.

3 Aug/25

- Real World DNS logs use in CTI
- Detect malicious domains, DGA patterns, fast flux techniques
- Use historical DNS data to track malware infrastructure.

→ CTI platforms ingest passive DNS data (eg→ Virus Total, Passive Total)

→ Helps identify C2 domains, botnets.

- DNSSEC (Domain Name System Security Extensions)

→ Purpose:→ Prevent DNS spoofing by verifying DNS data integrity

→ How it works→

Uses digital signatures with public key cryptography.

Each zone signs its DNS records using Zone Signing Key (ZSK).

→ Parent zone stores Delegation Signer record pointing to child's public key.

→ Record used:→

- RRSIG (Signature)
- DNSKEY (public key)
- DS (delegation Signer)
- NSEC / NSEC3 (proof of non-existence)

→ Limitations→ Doesn't encrypt data, only verifies authenticity.

(end)

NETWORK (4th Aug).

▶ PORTS :-

Logical endpoints in the Transport Layer (OSI Layer 4) that identify specific application or services on a device during network communication.

▶ Purpose :- • Allow multiple applications to use a single IP address by assigning unique port numbers.

⊙ Facilitate communication between client and server (e.g., browser on port 50000 connects to a web server on port 80).

• Range : 0 - 65535 (16-bit numbers)

• **Role:-** Ports are entry points for network traffic, making them prime target for attackers if misconfigured or exposed.

▸ **Type of Ports :-**

① Well-Known ports : 0-1023 (reserved by IANA, used by core services)

eg:- HTTP (80) :- Unencrypted web traffic.
HTTPS (443) :- Secure web traffic (TLS)
SSH (22) :- Secure remote access.
FTP (20/21) :- File transfer (data/control)
SMTP (25) :- Email sending
DNS (53) :- Domain name resolution
Telnet (23) :- Insecure remote access (avoid)
SNMP (161/162) :- Network management.

② Registered Ports (1024 - 49151) :-
→ Used by specific applications or vendor services.

eg:- 1443 :- Microsoft SQL Server
3306 :- My SQL database.
8080 :- Alternative HTTP (proxies, web apps).
5060 :- SIP (VoIP).

Risk:- Misconfigured services are vulnerable to brute force or exploits.

③ Dynamic/Private Ports (49152 - 65535) :-

Temporary ports for client-side connections (eg → browsers or app initiating a session)

eg:- A client use port 49153 to connect to a server's port 443.

Risk:- Rarely targeted directly but used in NAT traversal or backdoor communication.

▸ **Common Port Numbers & Protocols :-**

Port	Protocol	TCP/UDP	Use Case
20	FTP	TCP	File Transfer (Data)
21	FTP	↓	↓ (Control)
22	SSH	↓	Secure Shell
23	Telnet	↓	Remote login (insecure)
25	SMTP		Sending emails
53	DNS	both	Domain name resolution
67	DHCP	UDP	DHCP server
68	DHCP	UDP	DHCP client
69	TFTP	UDP	(UDP) Trivial File Transfer
80	HTTP	TCP	~~Email~~ Web traffic
110	POP3	↓	Email retrieval
123	NTP	UDP	Time synchronization
137-139	NetBIOS	UDP, UDP, TCP	Windows file/printer sharing
143	IMAP	(TCP) → Email retrieval.	

Post → TCP → 30 Post covered

Port	TCP/UDP	Protocol	Use case
161	UDP	SNMP	Network device monitoring
443	TCP	HTTPS	→ Secure web traffic
445	TCP	SMB	Windows file sharing
514	UDP	Syslog	Log forwarding
993	TCP	IMAPS	Secure IMAP
995	TCP	POP3S	Secure POP3

▶ How Port Work in Networking :-

1) Mechanics :-
- Ports are tied to TCP (reliable connection-oriented) or UDP (fast, connectionless).
- A connection is defined by : Source IP + Source Port + Destination IP + destination Port.
- Example :→ Client (192.168.1.10 : 50000) connects to Server (93.184.216.34 : 80)

- TCP v/s UDP :

→ TCP :- Ensures reliable delivery via three way handshake (SYN, SYN-ACK, ACK). Used for HTTP, HTTPS, FTP.

⊙ UDP : Faster, no handshake, used for DNS, DHCP, streaming.

→ Concern : Attackers exploit TCP's handshake (eg→ SYN flood) or UDP's lack of verification (eg→ Amplification attacks)

- TCP v/s UDP Ports :-

Aspect	TCP	UDP
Type →	Connection-oriented	Connectionless
Reliability	Reliable	Unreliable
Use case	Web, email, file transfer	DNS, VoIP, Streaming.

▶ Common Port Vulnerabilities :-

① Port Scanning :-
- Tools → Nmap, Nessus.
- Purpose → Identify open ports and services for exploitation.

eg→ Scanning port 3389 (RDP) to find weak credentials.

PTO....

② SYN Flood (TCP) :-

→ Floods port with SYN packets, exhausting server resources.
→ Eg) Targeting port 80 to disrupt a web server.

③ Amplification Attacks (UDP) :-
Exploits UDP services (eg, DNS on 53) to amplify traffic in DDoS attacks

④ Misconfigured / Open Ports :-
Unnecessary open ports (eg, 23 for Telnet) expose services.
Example → Port 445 (SMB) led to WannaCry ransomware spread.

⑤ Backdoors :-
Malware opens high numbered ports (eg 4444 for metasploit) for C2 (Command & Control)

⑥ Port Spoofing :- Attackers fake source ports to bypass firewall rules.

⑦ Session Hijacking :→ Stealing active TCP session on open port (eg) HTTP on 80).

• Cyber-Security Defense Strategies :-

1→ Minimize Attack Surface :

→ Close unused ports (eg) disable Telnet on 23, use SSH on 22).
→ Use netstat -tuln or ss -tuln to audit open ports

2→ Firewall Configuration :

→ Allow only necessary ports (eg) 80, 443 for web servers).
→ Tools :- iptables, ufw, pfSense, Windows Firewall.
→ Example rule :- iptables -A INPUT -p tcp --d port 22 -j ACCEPT

3→ Intrusion Detection / Prevention :-

Deploy IDS/IPS (eg → Snort, Suricata) to detect port scans or unusual traffic.
→ Monitor for spikes on critical ports (eg 53 for DNS).

4. Network Segmentation :-
→ Place sensitive services (eg MySQL on 3306) in a DMZ or VLAN.
→ Restrict access to internal ports (eg→ 1433 for MSSQL).

5. Port Knocking :-
Hide services by requiring a specific port sequence to open access.

6. Secure Protocols :-
· Use HTTPS (443) over HTTP (80) over, SFTP (22) over FTP (21).
→ Enforce TLS 1.2/1.3 for HTTPS, avoid deprecated SSL/TLS version.

7. Rate Limiting :-
Mitigate SYN floods or DDoS with tools like nginx or cloudflare

8. Monitoring and Logging :-
· Use SIEM (eg→ Splunk, ELK) to analyze port-related logs.
· Monitor high-numbered ports for backdoors (eg→ 12345, 4444).

9. Patch Management :-
Regularly update services (eg Apache on 80, MySQL on 3306) to fix vulnerabilities

10. Authentication :-
Secure ports like 22 (SSH) with strong passwords or key based authentication.

⊙ Real-World Examples :-

① Case : Wanna Cry Ransomware
→ Exploited port 445 (SMB) due to unpatched system.
Defense :- Block 445 externally, apply (MS17-010) MSFT Patches.

- Xmas Scan (-sX): Sends FIN, PSH, URG flags; detects closed ports via RST.

- ACK Scan :- Maps firewall rules; checks for filtered/unfiltered status.

- Port Enumeration Tools

1. Nmap :- Industry std. for scanning ports
2. Netcat : Port scanner and listener
3. Masscan : Very fast, scans entire internet ranges
4. Hping3 : Craft custom TCP/IP packets, used for adv. scanning and firewall testing.

→ Firewalls v/s IDS

→ Firewalls block or allow traffic based on port, IP, protocol rules

- IDS (Intrusion Detection System): Monitors traffic, alert on suspicious patterns.

→ Network Protocols :-

① Definition :- A standardized set of rules that governs how data is formatted, transmitted and processed across network, ensuring devices communicate effectively.

Protocols define how data moves, but vulnerabilities in their design or implementation (e.g., plaintext transmission) can be exploited.

→ Purpose in Networking :-

Enable reliable, standardized communication between devices.

Defines data formats, addressing, error handling and session management.

Facilitate specific functions (eg→ file transfer, email, web browsing)

→ Purpose :→

- Secure protocols (eg→ HTTPS, SSH) protect data confidentiality and Integrity.

- Misconfigured or insecure protocols expose system to attack

2 Case :- DNS Amplification Attack :-

- Attackers used open DNS servers (port 53) to amplify DDoS ~~attac~~ traffic.

Defense :- Restrict DNS to trusted Clients use rate limiting.

3 Case :- Web Server Attack :-

- Port 80 targeted with SQL injection
- Defense : Deploy WAF, sanitize inputs, use HTTPS (443).

4 Case :- Backdoor Malware :-

- Malware opened port 4444 for C2 communication.
- Defense :- Monitor high ports, use IDS to detect anomalies.

- Key Takeaways

→ Ports are critical for network communication but are common attack vectors,

→ secure ports by closing unnecessary one, using firewalls.

→ Understand Port - Protocol mapping and vulnerabilities for effective defense.

→ Regular auditing and layered security are essential.

--- (optional)

- Port states

→ Open :- Application is accepting connection

→ Closed :- Port reachable, but no application listening

→ Filtered :- Firewall or network device blocking probe, no response

- Nmap Scan Types :-

- SYN Scan (-sS) : Stealth scan, half-open handshake
- UDP Scan (-sU) : Scans UDP ports, slower requires response analysis

like spoofing or interception.

▸ Common Protocols : Details

① HTTP :- (HyperText Transfer Protocols) transfers web content between Clients and servers.
Port no → 80, TCP. Used in browsing website.

② HTTPS :- Encrypts web traffic using TLS/SSL for secure communication
Port no → 443, TCP. Used in secure online banking or shopping.

③ FTP :- File Transfer Protocol, it transfers file between System.
Port ⇒ 20(Data), 21(control), TCP.
Used for uploading files to web server.

④ SFTP :- Secure FTP, Encrypts file transfer using SSH. Port no:- 22, TCP
Used in securely transferring sensitive files to server.

⑤ SSH :- Secure Shell : Provides encrypted remote access and command execution
Port no. → 22, TCP, Remotely managing a Linux server securely.

⑥ Telnet :- Telecommunication Network, Provides remote access. Port no → 23, TCP
→ Used rarely for legacy remote access to network ~~se~~ devices.

⑦ SMTP :- Simple Mail Transfer Protocol
Port no → 25, TCP. Used for Sending email via Gmail

⑧ POP3 :- Post Office Protocol v3 :-
Retrieves emails from server
Port no- 110, TCP. Downloading emails to an outlook Client.
↳ use.

⑨ IMAP :- Internet Message Access Protocol
Syncs and retrieves emails keeping copies on server.
Port ⇒ 143, TCP, used for accessing email on multiple devices via a mail app.

- DNS :- Spoofing or amplification attacks
- SMTP :- Email spoofing, phishing
- ARP :- Spoofing to intercept LAN traffic
- ICMP :- Ping floods or tunneling for DoS.
- SNMP :- (V1/V2) ⇒ weak authentication, data exposure.

⊙ Defenses :-

Use encrypted protocols

Implement firewalls to restrict protocol ports

Deploy DNSSEC, SPF/DKIM for DNS and email security

Use ARP inspection, DHCP snooping to prevent spoofing

→ Monitor traffic with IDS/IPS (eg → Snort) for protocol abuse

→ Patch services to fix protocol vulnerabilities (eg → OpenSSL for TLS).

(end)

⊙ Common Network Attacks :-

Definition :- Malicious actions targeting network infrastructure, protocols, or services to compromise confidentiality, integrity, or availability (CIA Triad).

→ Understanding common attacks helps identify vulnerabilities, configure defenses and respond to incidents across TCP/IP layers.

(10) DNS :- Domain Name System Port→53
UDP(queries), TCP(Zone transfer)
(resolves domain names to IP addresses)

(11) DHCP :- Dynamic Host Configuration Protocol. Assigns IP addresses dynamically
Port no→ 67 (server), 68 (client), UDP
used for assigning IP to a device joining a WiFi network.

(12) SNMP :- Simple Network Management Protocol. Monitors and manages network devices.
Port no:→ 161 (agent), 162 (traps), UDP
used for monitoring router performance in network.

(13) ICMP :- Internet Control Message Protocol : Handles diagnostic and error messages.
N/A (no specific port), IP (layer 3)
~~used in Ping~~
Used in Pinging a server to check connectivity
(eg→ Ping 8.8.8.8).

(14) ARP :→ Address Resolution Protocol
→ Maps IP addresses to MAC addresses
N/A (Layer 2).

Used for resolving a local IP to a MAC address in a LAN.

- TCP v/s UDP Comparison

Feature	TCP	UDP
Connection	Connection-oriented (Three-way handshake :SYN, SYN-ACK, ACK).	Connectionless
Reliability	Ensures delivery with error checking, retransmission	No guaranteed delivery, no retransmission
Speed :-	Slow due to overhead	Faster
Use Cases :-	Web (HTTP/HTTPS), email, file transfer	DNS queries, VoIP, DHCP.
(Example) :-	HTTPS, SSH	DNS, DHCP

Secure v/s Insecure Protocols :-

• Secure Protocols :-

- HTTPS : Encrypts web traffic with TLS
- SFTP : Encrypts file transfers via SSH
- SSH : Encrypts remote access
- IMAPS (993), POP3S (995) : Encrypted email retrieval
- SNMPv3 :- Adds encryption and authentication

→ Cyber Security ~~Risk~~ Advantage → Protect against eavesdropping, MitM attacks.

Insecure Protocols :-

⊙ HTTP :- Plaintext web traffic (port 80), vulnerable to interception.

⊙ FTP :- Plain text file transfer (port 20/21) exposes credentials.

⊙ Telnet :- Plaintext remote access (port 23) easily intercepted.

⊙ SMTP (unencrypted) : Plaintext email sending (port 25), prone to spoofing.

⊙ SNMPv1/v2 :- Lacks strong encryption, vulnerable to sniffing.

• Cyber Risk → Data interception, credential theft, spoofing.

[Always use Secure protocols with enforce encryption]. (SNMP v3) → is apt choice

• Real-World Use :-

• HTTP/HTTPS :-
Use → Browsing a website (HTTP) or secure online shopping (HTTPS).
Cyber → HTTPS prevents MitM attacks, HTTP risks data exposure.

• FTP/SFTP :
Use → uploading website files (FTP) or securely transferring sensitive documents (SFTP).
Cyber → SFTP prevents credential theft; FTP is vulnerable.

• SSH/Telnet :-
Use → Sending email (SMTP) or accessing email on client (IMAP)

⊙ SSH/Telnet → Managing remote servers (SSH) or legacy router access (Telnet).

Cyber → Use SSH secure access; Telnet exposes commands.

⊙ SMTP/POP3/IMAP :-
Use → Sending emails (SMTP) or accessing emails on client (IMAP)

Cyber → Use SMTPS(465), POP3S(995), IMAPS(993) to prevent spoofing/sniffing.

⊙ DNS :-
use → Resolving domain names for browsing or email
Cyber → DNS spoofing can redirect users, use DNSSEC for protection.

⊙ DHCP :- Use → Assigning IPs in a corporate Wi-Fi network
Cyber → Rogue DHCP servers can assign malicious IPs, use DHCP snooping.

⊙ SNMP :-
Use → Monitoring network devices like routers

Cyber security :- SNMP v3 prevents unauthorized access; v1/v2 risks data leakage.

⊙ ICMP :-
Use → Troubleshooting network issues with ping or traceroute.

Cyber security :- Block excessive ICMP to prevent ping floods or tunneling

⊙ ARP :-
Use → Resolving IPs to MACs in a LAN for device communication.

Cyber security :- ARP spoofing enables MitM use ARP inspection.

▶ Protocols Vulnerabilities and Defense :-

• Vulnerabilities :->

⊙ HTTP, FTP, Telnet :- Plaintext transmission risks interception (eg → Wireshark sniffing).

Common Network Attacks.

① IP spoofing :→ Faking the source IP address in packet headers to impersonate a trusted system
eg> Attackers send packet with fake IP to bypass firewall rules
effect → Bypasses access controls, enables MitM or DoS attacks
TCP/IP layer → Internet layer
Mitigation → Use anti spoofing filters.

② ARP Spoofing :- Sending fake ARP messages to associate attacker's MAC address with a legitimate IP.
eg> Attacker links their MAC to a server IP in a LAN, intercepting traffic.
TCP/IP → Network Access
Effect → Enables MitM, data theft, or Session hijacking.
Mitigation :- Enable ARP inspection.

③ SYN flood :- Overwhelming a server with TCP SYN packets without completing handshakes.
TCP/IP layer → Transport layer.
eg> Flooding a web server's port 80 with SYN Packets.
Effect → Exhausts server resources, causing DoS
Mitigate :- Use SYN cookies, rate limiting.

④ DNS Spoofing :- Corrupting DNS response to redirect users to malicious sites. (TCP/IP layer → Application).
eg> Redirecting google.com to a phishing site via fake DNS replies.
effect :→ steals credentials, delivers malware.
Mitigate → Implement DNSSEC, use trusted DNS servers.

⑤ DDoS (Distributed Denial of Service) →
→ Flooding a target with traffic from multiple sources to disrupt service
eg> Botnet floods a website with HTTP requests
effect → Overloads server, disrupts availability.
TCP/IP layer → Application/Transport
Mitigate → Deploy WAF, rate limiting.

• TCP/IP Model :-

→ Definition :- The TCP/IP Model (Transmission Control Protocol/Internet Protocol) is a four-layer framework that standardizes network communication, describing how data is packaged, transmitted, and received across network.

Cyber Relevance ⇒ Understanding the TCP/IP model is critical for identifying vulnerabilities, configuring firewalls, and analysing network traffic for threats.

Purpose ⇒ ① Provides a practical, simplified model for network communication compared to the OSI model.

② Enables interoperability across diverse devices and network.

③ Supports scalable, reliable, and secure data transfer.

④ Cyber Purpose ⇒ Guides the implementation of secure protocols and defense against layer specific attacks.

⑥ MITM => Intercepting and altering communication between two parties.
example → Attackers intercepts HTTPS traffic via ARP spoofing.
effect → Steals sensitive data, modifies messages
TCP/IP → multiple Layers
Mitigate → Use HTTPS, IPsec.

⑦ Port scanning :- Probing a system to identify open ports and services.
example :=> Using Nmap to scan for open port (RDP) 3389.
effect → Reveals vulnerabilities for further exploits.
TCP/IP → Transport Layer.
Mitigate → Block scans with IDS/IPS (eg → Snort), close unused ports.

⑧ Email Spoofing :- Forging email headers to impersonate a trusted sender.
TCP/IP → Application layer.
example :- Fake email from "bank@kgit.com" via SMTP (port 25).
effect → Delivers phishing Links for malware.
Mitigate → Use SPF, DKIM, DMARC for email authentication.

⑨ DNS Amplification :- Exploiting UDP-based DNS queries to amplify traffic in a DDoS Attack
(TCP/IP layer → Application layer).
→ Eg → Sending small DNS queries to open resolvers, amplifying response to flood a Target
→ Effect → Overwhelms Target, causing DoS.
Mitigate → Restrict open DNS resolvers, use rate limiting, source validation.

⑩ Session Hijacking :- Stealing an active session
TCP/IP → Application or Transport.
eg) Capturing HTTP session cookies to access a user's account.
effect → Unauthorized access to system or data.

Mitigate :→ Use HTTPS, secure cookies, session timeouts.

(11) ICMP flood → Overloading a system with ICMP echo requests.

eg) Sending excessive pings to a server

effect → consumed bandwidth, causes DoS

TCP/IP → Internet layer.

Mitigate → Block unnecessary ICMP traffic, rate limit ICMP requests.

Special Addon

→

① Malware delivery → using network protocols to deliver malicious payloads

Mitigate → Email gateways, antivirus.

Eg) Malware sent via email attachment

effect) Infect systems

② Network sniffing

Capturing network traffic to extract sensitive data.

Eg) Using Wireshark to capture plaintext HTTP traffic

effect → Expose credentials, sensitive data.

→ Mitigate → Use encrypted protocols.

• Layers of TCP/IP Model :-

The TCP/IP model has 4 layers :=>
① Application, ② Transport
③ Internet ④ Network.

① Application Layer :=> Function :=>
Provides network services to end-user applications, handling data formatting, user interaction, and high-level protocols.

• Cyber Role => Entry point of Attack like SQL injection, XSS, or phishing via protocols like HTTP or SMTP.

② Transport Layer :=> Function :=>
Manages end-to-end communication, ensuring reliable data transfer, flow control, and error correction.

• Cyber Role => Protect against port based attacks and ensures secure data transmission

BTO.

③ Internet Layer :=> Function :=>
Handles logical addressing, routing, and packet forwarding across networks.

Cyber Sec Role :- Mitigates IP spoofing, DoS attacks, and ensures secure routing (eg-> IPsec).

④ Network Access Layer :=> Function :-
Manages physical data transmission, including hardware addressing and framing.

• Cyber Security Role :=> Prevents MAC spoofing, ARP poisoning, and physical tampering.

⑤ Protocols at Each Layer :-

Layer	Protocols
Transport	TCP/UDP
Internet	IP (IPv4, IPv6), ICMP, IGMP

• Elements in TCP/IP model •

→ Vulnerabilities in layers :-

① Network Access :- MAC spoofing, ARP poisoning

② Internet : IP spoofing, ICMP tunneling.

③ Transport : Port scanning, SYN floods.

④ Application : XSS, SQL injection, Phishing.

→ Mitigation Strategies :-

⊙ Use VLANs to segment traffic

⊙ Deploy IPsec for secure routing

⊙ Enable TLS for encryption

⊙ Use WAF (Application) to block web attacks.

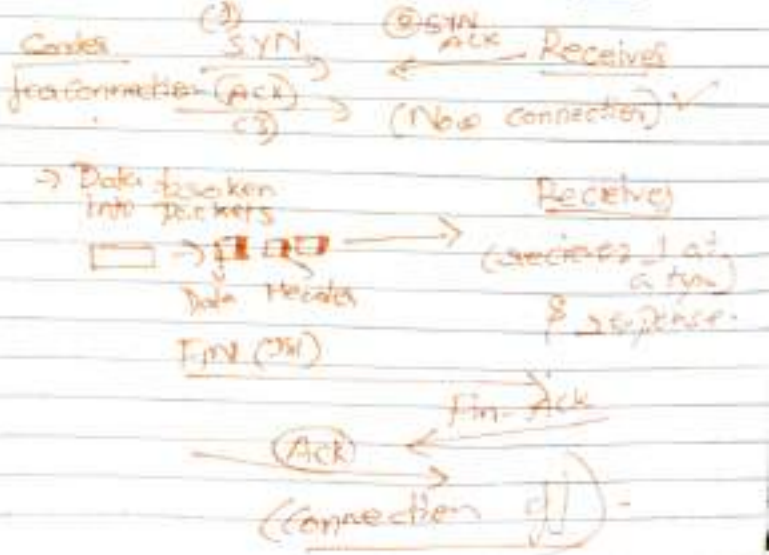
• Key Takeaways :-

→ The TCP/IP model is the backbone of Internet communication, critical for cyber security.

→ Each layer has specific protocols, functions & vulnerabilities.

→ Secure protocols and tools are essential for defense.

Imp: Cycle (TCP model) End.



OSI Model : Comparison

Aspect	OSI Model	TCP/IP Model
Layers	7	4
Development	Theoretical framework	Practical, Internet based
Complexity	More granular, complex	Simpler, Practical
Usage	Reference model for teaching design	Basis for Internet, real-world networks
Protocols	Broader, includes theoretical protocols	Specific : TCP, IP HTTP, DNS
Layer Mapping	Physical → Network Access Data Link → Network Access Network → Internet Transport → Transport Session, Presentation, Application → Application	Combines Session, Presentation, Application into one layer.

Cyber Security Relevance :-	OSI : Physical : Wire tapping - Data Link : ARP spoofing Network : IP spoofing : Transport : SYN floods. Session : Session hijacking, Presentation : TLS downgrade	TCP/IP :- Network Access = MAC/ARP spoofing Internet : IP spoofing, ICMP attacks - Transport : SYN floods. Port scanning. Application : XSS, phishing

- TCP/IP's simplicity makes it practical for securing real-world networks, but OSI's granularity helps analyze layer specific threats.

Layer	Protocols
Network Access	Ethernet, ARP, PPP, Wi-Fi, MAC.
Application	HTTP(80), HTTPS(443), FTP(20,21), SFTP(22), SSH(22), Telnet, POP3, IMAP, DNS, DHCP, SNMP.

① Application Layer :- Use HTTPS over HTTP, SFTP over FTP to prevent data interception.

② Transport Layer :- TCP for reliability, UDP for speed ; secure with TLS

③ Internet Layer :- IPsec for secure IP communication ; ICMP vulnerable to Ping floods.

④ Network Access layer :- ARP inspection to prevent spoofing

P10

• Data - Flow Process :-

→ Process :-

ⓐ Application layer → Application generates data

ⓑ Transport Layer → Data is segmented, assigned a port (eg TCP port 80), and headers added (TCP/UDP).

ⓒ Internet Layer :- Segments are encapsulated into packets with source / destination IP addresses (eg IPv4).

ⓓ Network Access Layer :- Packets are framed with MAC addresses and transmitted over physical media (eg Ethernet).

ⓔ Reverse Process : Receiving device processes frame (Network Access), packets (Internet), segment (Transport), and delivers data to the application.

Sending msg → Application → Transport → Internet → Network

Receiving → Network → Internet → Transport → Application