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

P.T.O

DNS Zone, Zone Transfer :-

→ DNS Zone :- Portion of DNS namespace managed by one authority.
eg: example.com and its 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 infra structure.
- → 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 Singer)
- 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.

① 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 → browser 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.

Port => IP => 3D Post Engined

No.
Date

Port	TCP/UDP	Protocol	Use case
161	UDP	SNMP	Network device monitoring
443	TCP	HTTPS	-> secure web traffic
445	TCP	SMB	Window 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 Host 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 Managment :-

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.

2 Case :- DNS Amplification Attack :-

- Attackers used open DNS servers (port 53) to amplify DDoS ~~attack~~ 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

- 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

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.

(10) DNS :- Domain Name System Port → 53
UDP (queries), TCP (transfer Zone)
(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 Managment 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 Pig~~
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 retransmis
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 best 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 → Assiging 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).

- 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.

Common Network Attacks-

① IP spoofing :→ Forging the source IP address in packet headers to impersonate a trusted system
eg> Attacker 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 Services) :→

→ Flooding a target with traffic from multiple sources to disrupt services.
eg> Botnet floods a website with HTTP requests
effect → Overloads server, disrupts availability.
TCP/IP layer → Application / Transport

Mitigate → Deploy WAF, rate limiting.

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@legit.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 -> Consumes 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.

No.

Date

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.

• 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

PTO.

③ Internet Layer :- Function →

Handles logical addressing, routing, and packet forwarding across networks.

Cyber Sect 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.

ⓘ Protocols at Each Layer :-

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

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

PTO

• 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

Recievery ⇒ Network → Internet → Transport → Application

OSI vs TCP/IP Model : Comparison

Aspect	OSI Model	TCP/IP Model
Layers	7	4
Development	Theoretical framework	Practical, Internet based
Complexity	More granular, complex	Simpler, Practical

Aspect	OSI Model	TCP/IP Model
Layer Development	7 Theoretical framework	4 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	Combines Session, Presentation,

OSI :- Transport - Session / Presentation / Application → Application

TCP/IP :- 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.

• Elements in TCP/IP Model •

→ Vulnerabilities in layers :-

- ⊙ Network Access :- MAC spoofing, ARP poisoning
- ⊙ Internet : IP spoofing, ICMP tunneling.
- ⊙ Transport : Port Scanning, SYN floods.
- ⊙ 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.