TCP/IP Model: What are Layers & Protocol? TCP/IP Stack

Why Was the TCP/IP Model Needed in the First Place?

Solving Real-World Communication Problems

In the 1970s, different computer systems couldn’t easily talk to each other. Each vendor (IBM, DEC, etc.) had their own proprietary networking protocols.

> TCP/IP was developed by the U.S. Department of Defense (DoD) to create a universal, robust, and interoperable network—what became the Internet.

The goals:

- Enable different systems to communicate
- Make communication fault-tolerant, even in war conditions (original ARPANET vision)
- Use standardized, layered protocols that can work across any hardware

TCP/IP Model Came First (1974–1983)

- Developed practically by Vint Cerf and Bob Kahn.
- It wasn't just a model—it came with real working protocols (TCP, IP, etc.).
- It was used to build the actual Internet.
- In 1983, TCP/IP became the standard protocol suite for ARPANET.

So, TCP/IP was driven by implementation, not theory. That’s why it's so widely adopted—it works.

Then Came the OSI Model (1984)

The OSI model (Open Systems Interconnection) was developed by the ISO (International Organization for Standardization) after TCP/IP.

Why was it created if TCP/IP already existed?

- OSI was designed to be a universal reference model.
- It is more detailed and theoretical—with 7 layers instead of 4.
- Its goal was to:
    - Promote vendor interoperability

- Provide a standard framework for designing network protocols
- Educate and help in understanding networking systems

In short, OSI was a guidebook. TCP/IP was the actual vehicle already on the road.

So Why Do We Still Study the OSI Model?

Even though TCP/IP won the race in practice:

- OSI is more descriptive and educational.
- It helps clearly separate network functions across 7 layers.
- It provides universal language for network engineers to explain concepts.

When you troubleshoot a network, you often "think in OSI layers" even if you're using TCP/IP protocols.

TCP/IP Model

The TCP/IP model (Transmission Control Protocol/Internet Protocol) is a conceptual framework used to understand and design the internet and similar computer networks. It defines how data should be packetized, addressed, transmitted, routed, and received at the destination. It is the foundation of the modern internet.

The TCP/IP model has four abstraction layers, each with specific responsibilities. It is sometimes compared to the OSI model, which has seven layers, but TCP/IP is more practical and widely used in real-world networking.

The TCP/IP model is a four-layer conceptual model used for designing and understanding network communication protocols on the Internet.

TCP/IP Layer	OSI Equivalent	Key Role
Application Layer	Application, Presentation, Session	User-level network services
Transport Layer	Transport	End-to-end communication
Internet Layer	Network	Logical addressing and routing
Network Access Layer	Data Link + Physical	Physical data transmission

Application Layer

- **Purpose:**

Interface between software applications and the network.

- **Functions:**
  - Enables services like email, file transfer, remote login, web browsing
  - Identifies communication partners and synchronizes communication
  - Determines resource availability
  - Supports distributed databases and access to global information
- **Common Protocols:**

Protocol	Purpose
HTTP/HTTPS	Web browsing
FTP/SFTP	File transfers
SMTP/POP3/ IMAP	Email delivery and retrieval
DNS	Domain name to IP resolution
Telnet/SSH	Remote login to host systems

Transport Layer

- **Purpose:**

Ensures reliable or fast communication between devices.

- **Functions:**
  - Segments and reassembles data from the application layer
  - Ensures ordered and error-free delivery
  - Manages flow control and retransmission
  - Delivers data to the correct process using port numbers
- **Common Protocols:**

Protocol	Characteristics	Use Cases
TCP	Connection-oriented, reliable	Web, email, file transfer
UDP	Connectionless, fast, no guarantee	Streaming, DNS, VoIP

Internet Layer

🔹 **Purpose:**

Routes packets from source to destination across multiple networks.

🔹 **Functions:**

- Handles logical addressing using IP addresses
- Manages routing and packet forwarding
- Ensures each packet reaches the correct destination network

🔹 **Key Characteristics:**

- Delivery is not guaranteed (unreliable layer)
- Focused on best-effort delivery

🔹 **Common Protocols:**

Protocol	Function
IPv4/IPv6	Logical addressing & routing
ICMP	Network diagnostics (e.g., ping)
ARP	Resolves IP to MAC address
IGMP	Multicast group management

Network Access Layer (aka Link Layer / Network Interface Layer)

🔹 **Purpose:**

Manages physical transmission of data over network media.

🔹 **Functions:**

- Encapsulates IP packets into frames
- Adds MAC (hardware) addressing
- Defines how electrical, optical, or wireless signals are used

🔹 **Responsibilities:**

- Transmission between two devices on the same network
- Converts packets into bits and transmits them physically

🔹 **Common Protocols and Technologies:**

Technology	Description
Ethernet	Wired LAN communication
Wi-Fi	Wireless LAN communication
PPP	Point-to-point connections
MAC	Media Access Control addressing

📌 Key Points to Remember

- TCP/IP is a practical model, created before the OSI model.
- It forms the foundation of the modern Internet.
- Each layer is independent, allowing protocol changes at one layer without affecting others.
- The model is protocol-specific, unlike OSI which is protocol-agnostic.

OSI Model	TCP/IP model
It is developed by ISO (International Standard Organization)	It is developed by ARPANET (Advanced Research Project Agency Network).
OSI model provides a clear distinction between interfaces, services, and protocols.	TCP/IP doesn't have any clear distinguishing points between services, interfaces, and protocols.
OSI refers to Open Systems Interconnection.	TCP refers to Transmission Control Protocol.
OSI uses the network layer to define routing standards and protocols.	TCP/IP uses only the Internet layer.
OSI follows a vertical approach.	TCP/IP follows a horizontal approach.
OSI model use two separate layers physical and data link to define the functionality of the bottom layers.	TCP/IP uses only one layer (link).
OSI layers have seven layers.	TCP/IP has four layers.
OSI model, the transport layer is only connection-oriented.	A layer of the TCP/IP model is both connection-oriented and connectionless.
In the OSI model, the data link layer and physical are separate layers.	In TCP, physical and data link are both combined as a single host-to-network layer.

OSI Model	TCP/IP model
Session and presentation layers are not a part of the TCP model.	There is no session and presentation layer in TCP model.
It is defined after the advent of the Internet.	It is defined before the advent of the internet.
The minimum size of the OSI header is 5 bytes.	Minimum header size is 20 bytes.

TCP/IP Protocol Suite – Most Common Protocols

Most Common TCP/IP Protocols

1. TCP (Transmission Control Protocol)

- **Function**: Breaks data into segments at the sender's side and reassembles it at the receiver's side.
- **Type**: **Connection-oriented**, reliable
- **Use Cases**: Web browsing (HTTP), file transfer (FTP), email (SMTP)

2. IP (Internet Protocol)

- **Function**: Provides logical addressing (IP address) and routes packets across networks.
- **Types**: IPv4, IPv6
- **Key Role**: Enables internetworking; essential for data delivery across the Internet
- **Pairing**: Commonly used with TCP (TCP/IP)

3. HTTP (Hypertext Transfer Protocol)

- **Function**: Transfers web pages and other resources from web servers to clients (browsers).
- **Type**: Application layer protocol
- **Use Case**: Loading websites (used in Chrome, Firefox, etc.)

4. SMTP (Simple Mail Transfer Protocol)

- **Function**: Used to send emails between mail servers.
- **Limitation**: Cannot retrieve emails (used with POP3 or IMAP)

- **Type**: Application layer protocol

5. SNMP (Simple Network Management Protocol)

- **Function**: Manages and monitors network devices (routers, switches, printers).
- **Type**: Application layer protocol
- **Use Case**: Network performance monitoring

6. DNS (Domain Name System)

- **Function**: Converts domain names (like www.google.com) into IP addresses.
- **Use Case**: Human-friendly internet navigation
- **Type**: Application layer protocol

7. TELNET (Terminal Network)

- **Function**: Allows remote login and access to other computers via command line.
- **Type**: Application layer protocol
- **Limitation**: Not secure (sends data in plaintext)

8. FTP (File Transfer Protocol)

- **Function**: Transfers files from one computer to another over a network.
- **Features**: Supports authentication, directories, upload/download
- **Use Case**: Uploading files to web servers

✅ **Advantages of the TCP/IP Model**

Advantage	Explanation
✅ Platform Independent	Works across different operating systems and hardware
✅ Scalable	Supports both small and large networks
✅ Supports Routing	Works with multiple routing protocols
✅ Client-Server Architecture	Efficient for modern distributed systems
✅ Interoperability	Allows communication between different devices and networks
✅ Flexibility	Can be used to set up private or public networks
✅ Open Standard	Not controlled by a single vendor; widely adopted

❌ Disadvantages of the TCP/IP Model

Disadvantage	Explanation
❌ Complex to Configure	Requires detailed knowledge to set up and manage properly
❌ Overhead	Higher overhead than simpler protocols like IPX
❌ No Strict Layer Separation	Some functions are mixed across layers
❌ Difficult to Replace Protocols	Inflexible when swapping protocol components
❌ Transport Layer Limitation	Does not guarantee delivery in all cases (especially with UDP)

Common TCP/IP-Based Attacks

Network Access Layer (Link Layer) Attacks

ARP Spoofing / ARP Poisoning

- **What it is**: Attacker sends fake ARP messages to associate their MAC address with another host's IP.
- **Impact**: Man-in-the-middle (MITM), session hijacking, sniffing
- **Tool Example**: arpspoof, ettercap

MAC Flooding

- **What it is**: Attacker floods the switch with random MAC addresses.
- **Impact**: Switch turns into a hub (broadcasts traffic), allowing sniffing

Internet Layer (IP Layer) Attacks

IP Spoofing

- **What it is**: Attacker sends packets with a forged source IP.
- **Impact**: Bypasses IP-based ACLs; used in DDoS and MITM

ICMP Flood / Ping of Death

- **What it is**: Sends a large volume of ICMP Echo Requests (pings) or malformed packets.
- **Impact**: System crash or network exhaustion

Smurf Attack

- **What it is**: Spoofs victim’s IP and sends ICMP requests to broadcast addresses.
- **Impact**: Victim is overwhelmed by replies

Transport Layer Attacks (TCP/UDP)

SYN Flood

- **What it is**: Attacker sends many SYN requests but doesn’t complete the handshake.
- **Impact**: Exhausts server’s TCP backlog (DoS)

TCP Reset Attack (RST Injection)

- **What it is**: Sends forged TCP RST packets to tear down active connections.
- **Impact**: Disrupts sessions (used in censorship and MITM)

UDP Flood

- **What it is**: Attacker floods random ports on a target with UDP packets.
- **Impact**: Exhausts resources due to ICMP "port unreachable" replies

Application Layer Attacks (Often Over TCP)

HTTP Flood / Slowloris

- **What it is**: Sends incomplete HTTP requests very slowly or floods with HTTP GET/POST.
- **Impact**: Denies service by consuming web server resources

DNS Spoofing / DNS Cache Poisoning

- **What it is**: Injects fake DNS records into a resolver’s cache.
- **Impact**: Redirects users to malicious sites

SMTP Spoofing / Open Relay Abuse

- **What it is**: Sends fake emails with forged headers or uses an open relay to send spam.
- **Impact**: Phishing, spam, blacklisting

FTP Bounce Attack

- **What it is**: Abuses FTP’s PORT command to scan other hosts from the server.

- **Impact**: Port scanning, evading firewalls

🛡️ How SOC L1 Should Respond

Attack Type	Detection Source	L1 Actions
SYN Flood	Firewall/IDS alert, traffic spike	Validate with packet count, escalate if DoS suspected
ARP Spoofing	ARP logs, detection tool alerts	Identify rogue MAC-IP mappings, inform network team
DNS Spoofing	DNS logs, mismatched IP responses	Check DNS cache, monitor redirection
HTTP Flood	WAF logs, web server access logs	Identify offending IPs, check request rates
ICMP Flood	Network monitoring tool alerts	Compare normal baseline, block at firewall
TCP Reset	Unusual session terminations	Correlate with source IP, check packet captures