Computer Networks

Question & Answer Style Revision Notes

Nishant IITH

October 12, 2025

Contents

1 Network Fundamentals

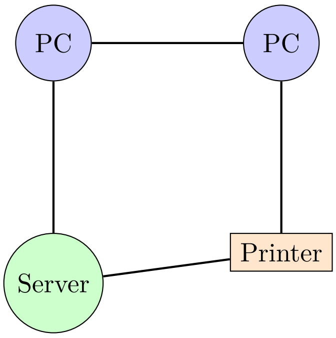
1.1 What is a Computer Network?

Definition

A **network** is a set of devices connected with physical media links. It is a collection of devices (nodes) connected to each other to allow sharing of data and resources.

Key Components:

- **Nodes:** Two or more devices (computers, servers, routers)
- **Links:** Physical connections (cables, fiber, wireless)
- **Purpose:** Data sharing, resource sharing, communication



Connected Devices
Network

1.2 What is Network Topology?

Definition

Network Topology is the arrangement of nodes and links in a network. It defines how devices are physically or logically connected.

Types:

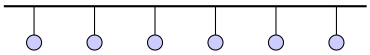
- **Physical Topology:** Actual physical layout of cables and devices
- **Logical Topology:** Data flow path between devices

Key Point

The topology of a network is key to determining its **performance**, **reliability**, and **scalability**.

1.2.1 Common Network Topologies

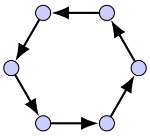
1. Bus Topology:



All devices connected to single cable
Failure in main cable stops entire network

Pros: Simple, cheap, easy to install
Cons: Single point of failure, performance degrades with more devices

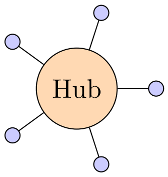
2. Ring Topology:



Data travels in circular path
Each device receives and forwards

Pros: Equal access, no collisions, predictable performance
Cons: Single break affects entire network, unidirectional

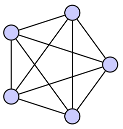
3. Star Topology:



All devices connect to central hub
Most common in modern networks

Pros: Easy to add/remove devices, fault isolation, centralized management
Cons: Hub failure stops network, requires more cable

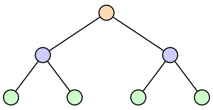
4. Mesh Topology:



Every device connected to every other
Maximum redundancy

Pros: High redundancy, fault tolerant, no single point of failure
Cons: Expensive, complex installation and maintenance

5. Tree Topology (Hierarchical):



Combines bus and star topology
Good for large organizations

Pros: Hierarchical, scalable, easy to manage and maintain
Cons: Root node failure critical, can be expensive

Quick Recap

Topology Selection:

- **Small office:** Star topology (most practical)
- **Large organization:** Tree/Hierarchical
- **Critical systems:** Mesh (redundancy needed)
- **Legacy systems:** Bus/Ring (rarely used today)

1.3 What is Bandwidth, Node, and Link?

Definition

Bandwidth: The data transfer capacity of a network measured in bits per second (bps). It represents the maximum amount of data that can be transmitted over a connection.

Common Units:

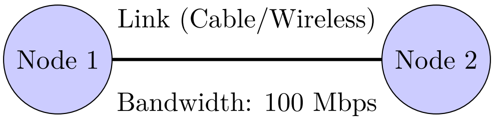
- Kbps (Kilobits per second) = 1,000 bps
- Mbps (Megabits per second) = 1,000,000 bps
- Gbps (Gigabits per second) = 1,000,000,000 bps

Definition

Node: A device or computer connected to a network that can send, receive, or forward data.

Definition

Link: The physical medium of connection between nodes (optical fiber, coaxial cable, wireless radio waves).



2 Network Models

2.1 What is the TCP/IP Model?

Key Point

TCP/IP is a compressed version of the OSI model with only **4 layers**. Developed by US Department of Defense (DoD) in the 1960s. Named after two core protocols: **TCP** (Transmission Control Protocol) and **IP** (Internet Protocol).

TCP/IP Layers (Bottom to Top):

4. Application Layer
High-level protocols, user interface
Examples: HTTP, SMTP, DNS, FTP, RTP

3. Transport Layer
Peer-to-peer communication, error recovery
Examples: TCP, UDP

2. Internet Layer
Delivers IP packets to destination (routing)
Examples: IP, ICMP, ARP

1. Network Access/Link Layer
Decides physical links (Ethernet, WiFi, serial lines)
Examples: Ethernet, SONET, 802.11 (WiFi)

Quick Recap

TCP/IP vs OSI:

- OSI = 7 layers (theoretical model)
- TCP/IP = 4 layers (practical implementation)
- Internet uses TCP/IP
- OSI layers 5, 6, 7 combined into TCP/IP Application layer
- OSI layers 1, 2 combined into TCP/IP Link layer

2.2 What are the Layers of OSI Model?

Key Point

The OSI (Open Systems Interconnection) model has **7 layers**. It's a conceptual framework for understanding network communication.

7. Application — HTTP, FTP, SMTP, DNS

6. Presentation — Encryption, compression, translation

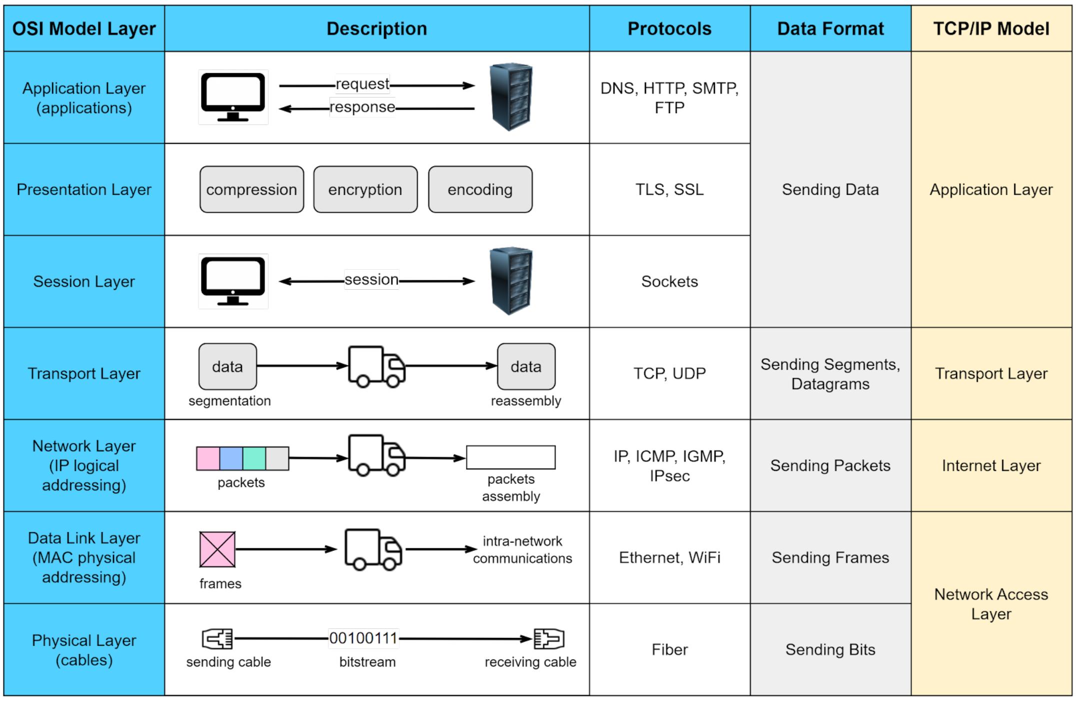
5. Session — Connection management

4. Transport — TCP, UDP (Segments)

3. Network — IP, routing (Packets)

2. Data Link — MAC, switches (Frames)

1. Physical — Cables, bits, signals



OSI Model Layer	Description	Protocols	Data Format	TCP/IP Model
Application Layer (applications)	request response	DNS, HTTP, SMTP, FTP	Sending Data	Application Layer
Presentation Layer	compression encryption encoding	TLS, SSL		
Session Layer	session	Sockets		
Transport Layer	data segmentation data reassembly	TCP, UDP	Sending Segments, Datagrams	Transport Layer
Network Layer (IP logical addressing)	packets packets assembly	IP, ICMP, IGMP, IPsec	Sending Packets	Internet Layer
Data Link Layer (MAC physical addressing)	frames intra-network communications	Ethernet, WiFi	Sending Frames	Network Access Layer
Physical Layer (cables)	sending cable 00100111 bitstream receiving cable	Fiber	Sending Bits	

Image Reference: Cloudflare Learning Center

Memory Aid: "All People Seem To Need Data Processing"

3 Data Link Layer

3.1 What is the Significance of Data Link Layer?

Key Point

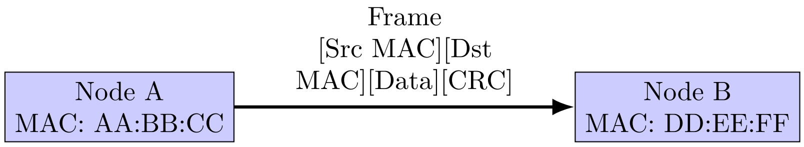
The Data Link Layer (Layer 2) is responsible for **node-to-node** data transfer within the same network.

Main Functions:

1. **Data Transfer:** Transfers data from one node to another
2. **Framing:** Receives data from Network layer, converts into frames
3. **Physical Addressing:** Attaches MAC addresses to frames
4. **Error-free Transfer:** Ensures reliable data delivery

Detailed Functions:

- **Frame Synchronization:** Ensures destination recognizes frame boundaries
- **Flow Control:** Controls data flow within network
- **Error Control:** Detects and corrects transmission errors
- **Addressing:** Uses MAC addresses for device identification
- **Link Management:** Manages initiation, maintenance, termination of links



Data Link Layer handles this

4 Network Devices

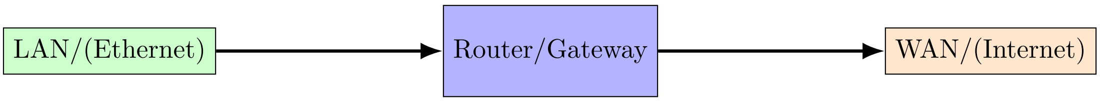
4.1 What is a Gateway? Difference between Gateway and Router?

Definition

Gateway: A node connected to two or more networks. It forwards messages from one network to another. Also known as a router in many contexts.

Key Difference:

Router	**Gateway**
Sends data between two **similar** networks	Sends data between two **dissimilar** networks
Operates at Network Layer (L3)	Can operate at multiple layers (up to L7)
Uses IP addresses for routing	Performs protocol conversion
Example: Home router connecting LAN to Internet	Example: Email gateway, VoIP gateway



Routes and regulates traffic

Quick Recap

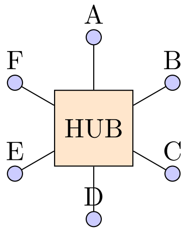
Both regulate traffic, but:

- **Router:** Connects similar networks (e.g., two Ethernet LANs)
- **Gateway:** Connects dissimilar networks (e.g., LAN to Internet, email to SMS)

4.2 Hub vs Switch

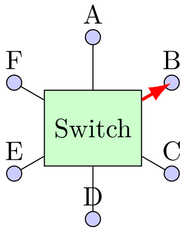
Feature	Hub	Switch
OSI Layer	Physical (Layer 1)	Data Link (Layer 2)
Operation	Broadcasts to all ports	Forwards to specific port
Intelligence	Dumb device	Intelligent device
Packet Filtering	Not available	Available (MAC table)
Transmission	Half-duplex	Full-duplex
Collision Domain	Single (all ports)	Separate per port
Speed	Slower	Faster
Usage	Obsolete	Modern LANs

Hub Operation:



Data from A is sent to **ALL** ports
Devices filter irrelevant data themselves

Switch Operation:



Data from A sent **ONLY** to B
Learns MAC addresses, maintains table

Key Point

Modern networks use switches exclusively. Hubs are obsolete due to:

- Poor performance (shared bandwidth)
- Security issues (all data visible to all devices)
- Collision problems

5 Network Protocols & Utilities

5.1 What does the Ping Command Do?

Definition

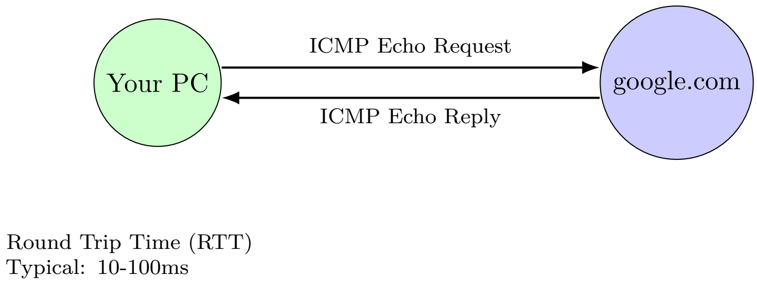
Ping is a utility program that checks connectivity between network devices. It measures the round-trip time (RTT) for packets to reach destination and return.

How Ping Works:

1. Sends ICMP Echo Request packets to target
2. Target responds with ICMP Echo Reply
3. Calculates time difference (RTT)
4. Reports packet loss and latency

Usage:

- `ping google.com` — Ping by domain name
- `ping 8.8.8.8` — Ping by IP address
- `ping -c 4 google.com` — Send 4 packets (Linux)
- `ping -n 4 google.com` — Send 4 packets (Windows)



Example

Ping Output:

```
PING google.com (142.250.77.206): 56 bytes
64 bytes from 142.250.77.206: icmp_seq=0 time=15.2 ms
64 bytes from 142.250.77.206: icmp_seq=1 time=14.8 ms
64 bytes from 142.250.77.206: icmp_seq=2 time=15.1 ms
```

Shows: IP address, packet size, sequence number, response time

5.2 What is DNS?

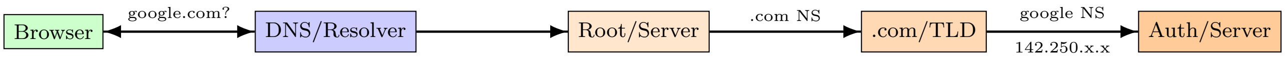
Definition

DNS (Domain Name System): A naming system that maps domain names to IP addresses. Introduced by Paul Mockapetris and Jon Postel in 1983.

Why DNS is Needed:

- Humans remember names easily (google.com)
- Computers need IP addresses (142.250.77.206)
- DNS translates names to IPs
- Without DNS, we'd need to memorize IP addresses

DNS Resolution Process:



Key Point

DNS is hierarchical:

1. Root servers (13 worldwide)
2. TLD servers (.com, .org, .net, etc.)
3. Authoritative servers (specific domain)

5.3 What is DNS Forwarder?

Definition

A **DNS Forwarder** is used when a DNS server receives queries it cannot resolve quickly. It forwards those requests to external DNS servers for resolution.

Behavior:

- Non-forwarder: Performs recursive resolution itself

- Forwarder: Sends query to external DNS server
- Improves efficiency and reduces load

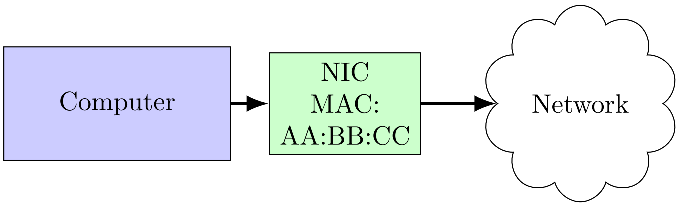
5.4 What is NIC?

Definition

NIC (Network Interface Card): A hardware component that connects a computer to a network. Each NIC has a unique MAC address.

Features:

- Provides wired (Ethernet) or wireless (WiFi) connection
- Has unique MAC address (48-bit)
- Converts data to electrical/radio signals
- Modern computers have integrated NICs



6 Network Addressing

6.1 What is MAC Address?

Definition

MAC (Media Access Control) Address: A unique identifier assigned to a Network Interface Controller (NIC). Used for network addressing within a network segment.

Characteristics:

- **Length:** 48 bits (6 bytes)
- **Format:** AA:BB:CC:DD:EE:FF (hexadecimal)
- **First 24 bits:** Manufacturer ID (OUI)
- **Last 24 bits:** Device serial number
- **Uniqueness:** Globally unique (burned into hardware)
- **Layer:** Data Link Layer (Layer 2)

Example

MAC Address: 00:1A:2B:3C:4D:5E

- 00:1A:2B = Manufacturer (e.g., Cisco)
- 3C:4D:5E = Device identifier

6.2 What is IP Address?

Definition

IP (Internet Protocol) Address: A unique address that identifies a device on the Internet or local network. It follows rules defined by the Internet Protocol.

Purpose:

- Identifies host/network interface
- Enables routing between networks

- Location addressing for devices

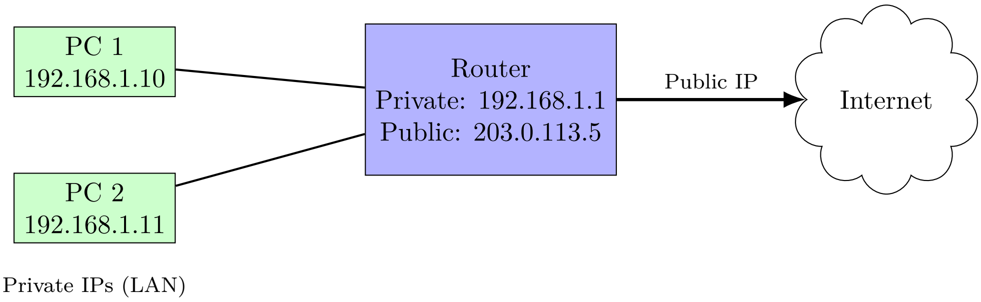
6.2.1 Private IP Address

Key Point

Private IP addresses are reserved ranges NOT valid for Internet use. Used within local networks only. To access Internet, must use NAT or proxy server.

Private IP Ranges:

- **Class A:** 10.0.0.0 to 10.255.255.255 (10.0.0.0/8)
- **Class B:** 172.16.0.0 to 172.31.255.255 (172.16.0.0/12)
- **Class C:** 192.168.0.0 to 192.168.255.255 (192.168.0.0/16)



6.2.2 Public IP Address

Definition

Public IP Address: An address assigned by Internet Service Provider (ISP) for communication on the Internet. Globally unique and routable.

Characteristics:

- Assigned by ISP
- Globally unique
- Directly accessible from Internet
- Can be static (permanent) or dynamic (changes)

6.2.3 APIPA (Automatic Private IP Addressing)

Definition

APIPA: A feature in operating systems (Windows, etc.) that enables computers to self-configure an IP address when DHCP server is unreachable.

Details:

- **Range:** 169.254.0.0 to 169.254.255.255
- **When used:** DHCP server not responding
- **Purpose:** Allow limited local communication
- **Limitation:** Cannot access Internet

Example

Your computer tries to get IP from DHCP:

1. DHCP request sent
2. No response from DHCP server
3. System auto-assigns: 169.254.x.x
4. Can communicate with other APIPA devices only

6.3 IPv4 vs IPv6

Feature	IPv4	IPv6
Address Length	32 bits	128 bits
Format	Decimal (192.168.1.1)	Hexadecimal (2001:0db8::1)
Address Space	∼4.3 billion	∼340 undecillion
Header Size	20-60 bytes (variable)	40 bytes (fixed)
Fragmentation	Routers and hosts	Only hosts
Checksum	Yes	No (handled by other layers)
NAT	Required (address shortage)	Not needed
Security	Optional (IPSec)	Mandatory (IPSec)
Configuration	Manual or DHCP	Auto-config or DHCPv6

Key Point

Why IPv6?

- IPv4 addresses exhausted
- IoT needs billions of addresses
- Simplified header for efficiency
- Built-in security features
- Better quality of service

6.4 What is a Subnet?

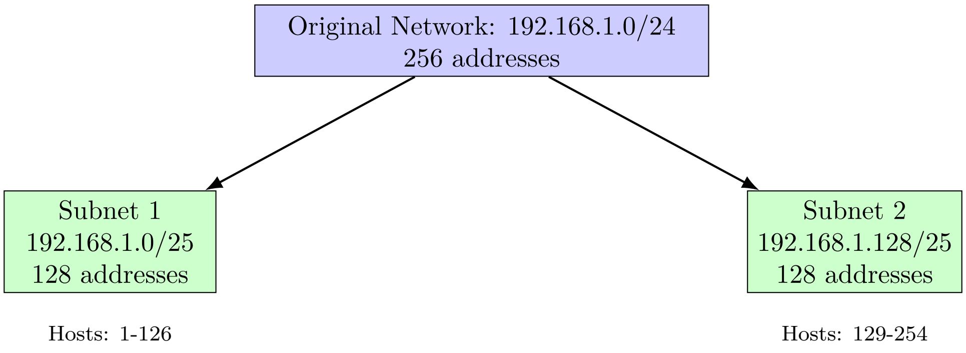
Definition

Subnet (Subnetwork): A logical subdivision of an IP network. Created through the process of **subnetting**.

Purpose:

- **Higher routing efficiency:** Reduces routing table size
- **Enhanced security:** Isolate network segments
- **Reduced congestion:** Limits broadcast domain size
- **Better organization:** Group devices logically

How Subnetting Works:



Example

Subnetting Example:

- Network: 192.168.1.0/24
- Subnet Mask: 255.255.255.0
- Network portion: 192.168.1
- Host portion: 0-255
- Usable hosts: 1-254 (0=network, 255=broadcast)

7 Network Security

7.1 What are Firewalls?

Definition

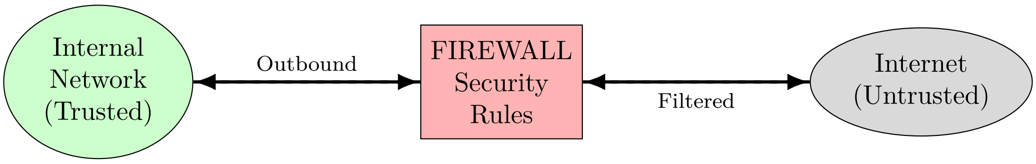
Firewall: A network security system that monitors and controls incoming and outgoing traffic based on security policies. Acts as a barrier between trusted internal network and untrusted external network (Internet).

Types:

- **Hardware Firewall:** Physical device (router with firewall)
- **Software Firewall:** Program running on computer
- **Combination:** Both hardware and software together

Functions:

- Monitor incoming/outgoing traffic
- Block/allow based on rules
- Protect against unauthorized access
- Log security events
- Prevent malware spread



Key Point

Firewall adds security layer by:

1. Filtering packets based on IP, port, protocol
2. Blocking suspicious traffic
3. Logging all activities
4. Implementing security policies
5. Preventing intrusions

7.2 What is RSA Algorithm?

Definition

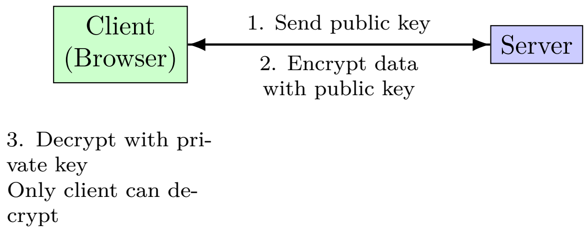
RSA: An asymmetric cryptography algorithm using two different keys—Public Key and Private Key. Named after inventors: Rivest, Shamir, Adleman.

How it Works:

- **Public Key:** Shared with everyone (encrypts data)

- **Private Key:** Kept secret (decrypts data)
- Data encrypted with public key can only be decrypted with private key

Example Process:



Example

Asymmetric Encryption in Action:

1. Client sends public key to server
2. Server encrypts data with client's public key
3. Server sends encrypted data
4. Client decrypts with private key
5. Even if attacker has public key, cannot decrypt (needs private key)

8 Network Performance

8.1 Different Types of Delays

Key Point

Network delays affect the time taken for packet processing and transmission. Total delay = sum of all delay types.

Types of Delays:

1. Transmission Delay:

- Time to push all packet bits onto link
- Formula: $D_{trans} = \frac{L}{R}$ where L=packet length, R=bandwidth
- Depends on: Packet size, link bandwidth

2. Propagation Delay:

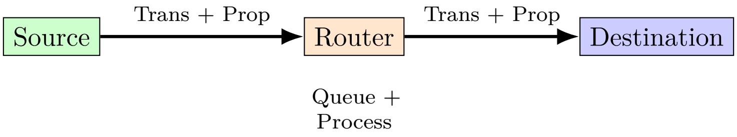
- Time for bit to travel from sender to receiver
- Formula: $D_{prop} = \frac{d}{s}$ where d=distance, s=propagation speed
- Depends on: Physical distance, medium (fiber vs copper)

3. Queueing Delay:

- Time packet waits in router queue
- Variable (depends on congestion)
- Can be zero if no queue

4. Processing Delay:

- Time router takes to process packet header
- Check errors, determine output link
- Usually negligible (microseconds)



Quick Recap

Total Delay = Transmission + Propagation + Queueing + Processing

- **Transmission:** Depends on bandwidth
- **Propagation:** Depends on distance
- **Queueing:** Depends on traffic
- **Processing:** Usually minimal

9 Connection Management

9.1 What is 3-Way Handshaking?

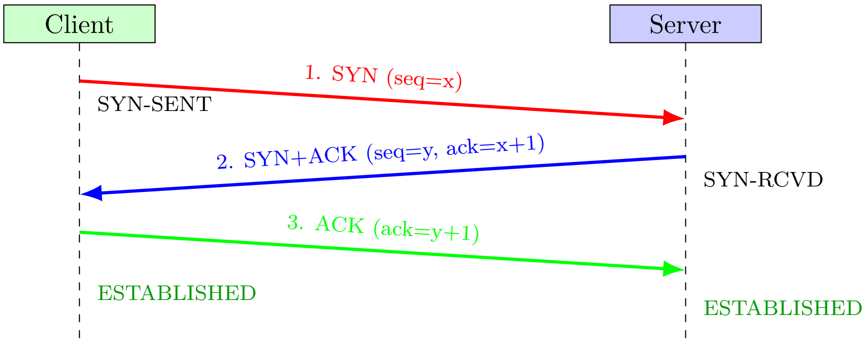
Definition

Three-Way Handshake: A process in TCP/IP to establish connection between client and server. Ensures both sides are ready for data transfer.

Purpose:

- Synchronize sequence numbers
- Establish connection parameters
- Confirm both sides are ready
- Enable reliable bidirectional communication

Three Steps:



Detailed Steps:

1. **Step 1 - SYN:**
   - Client sends SYN packet with random sequence number (x)
   - Indicates desire to establish connection
   - Client enters SYN-SENT state
2. **Step 2 - SYN+ACK:**
   - Server receives SYN
   - Sends back SYN+ACK with its sequence number (y)
   - Acknowledges client's sequence (ack=x+1)
   - Server enters SYN-RECEIVED state
3. **Step 3 - ACK:**
   - Client receives SYN+ACK
   - Sends ACK acknowledging server's sequence (ack=y+1)
   - Both enter ESTABLISHED state
   - Connection ready for data transfer

Key Point

Why 3-way?

- Prevents old duplicate connections
- Synchronizes sequence numbers on both sides
- Confirms both devices are ready
- Allows bidirectional communication setup

10 Application Layer Protocols

10.1 What is HTTP and HTTPS?

Definition

HTTP (HyperText Transfer Protocol): Defines rules for transmitting information on the World Wide Web. Foundation of data communication on web.

HTTP Characteristics:

- **Stateless:** Each request independent
- **Application Layer:** Layer 7 protocol
- **Transport:** Runs on TCP
- **Port:** 80 (default)
- **Client-Server:** Request-response model

Definition

HTTPS (HTTP Secure): Advanced and secured version of HTTP. Uses SSL/TLS for encryption.

HTTPS Characteristics:

- **Encrypted:** All data encrypted with TLS/SSL
- **Port:** 443 (default)
- **Secure:** Prevents eavesdropping, tampering
- **Certificate:** Verifies server identity
- **Trust:** Indicated by padlock in browser

Feature	**HTTP**	**HTTPS**
Security	No encryption	Encrypted (TLS/SSL)
Port	80	443
Speed	Slightly faster	Slightly slower (encryption overhead)
SEO	Lower ranking	Higher ranking (Google preference)
Certificate	Not required	SSL/TLS certificate required
URL	http://	https://
Use Case	Non-sensitive data	Sensitive data (login, payment)

Key Point

Always use HTTPS for:

- Login pages (passwords)
- Payment processing
- Personal information
- Any sensitive data

10.2 What is SMTP Protocol?

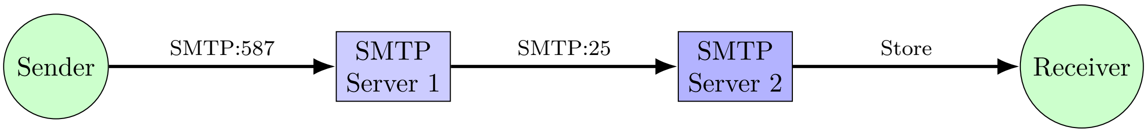
Definition

SMTP (Simple Mail Transfer Protocol): Sets rules for communication between mail servers. Used for **sending** emails.

SMTP Characteristics:

- **Purpose:** Send/relay emails
- **Port:** 25 (server-to-server), 587 (client submission)
- **Transport:** TCP
- **Mode:** Always-listening
- **Methods:** End-to-End and Store-and-Forward

How SMTP Works:



Quick Recap

Email Protocol Combo:

- **SMTP:** Sending emails (push)
- **POP3/IMAP:** Receiving emails (pull)
- SMTP only handles outgoing mail
- Receiving requires different protocol

10.3 TCP vs UDP Protocol

Feature	TCP	UDP
Full Form	Transmission Control Protocol	User Datagram Protocol
Connection	Connection-oriented (handshake)	Connectionless
Reliability	Guaranteed delivery	No guarantee (best-effort)
Ordering	In-order delivery	No ordering
Speed	Slower (overhead)	Faster (minimal overhead)
Header Size	20-60 bytes	8 bytes
Error Checking	Extensive (checksum + retransmit)	Basic (checksum only)
Flow Control	Yes (sliding window)	No
Congestion Control	Yes	No
Use Cases	Web, Email, File Transfer	Streaming, Gaming, DNS, VoIP

Key Point

When to use TCP:

- Data integrity is critical
- Order matters
- Can tolerate latency
- Examples: HTTP, FTP, SMTP, SSH

When to use UDP:

- Speed is priority
- Some data loss acceptable
- Real-time applications
- Examples: Video streaming, VoIP, DNS, online gaming

11 The Famous Question

11.1 What Happens When You Enter "google.com"?

Interview Question

This is one of the **most asked interview questions** in networking!

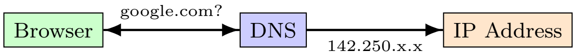
Complete Step-by-Step Process:

Step 1: Browser Cache Check

- Check if content is fresh and cached
- If yes, display from cache
- If no, proceed to next step

Step 2: DNS Lookup

- Browser checks if IP is in cache (browser + OS)
- If not found, OS performs DNS lookup
- Uses UDP to query DNS server
- DNS resolves google.com to IP (e.g., 142.250.77.206)



Step 3: TCP Connection (3-Way Handshake)

- Establish TCP connection with server
- Port 443 for HTTPS (or 80 for HTTP)
- SYN → SYN+ACK → ACK

Step 4: HTTP Request

- Browser sends HTTP GET request
- Includes headers (User-Agent, Accept, Cookies)
- Request travels through TCP connection

Step 5: Server Processing

- Web server receives HTTP request
- Processes request (database queries, logic)
- Generates HTTP response

Step 6: HTTP Response

- Server sends HTTP response (200 OK)
- Includes HTML, CSS, JavaScript
- May include headers (Cache-Control, Set-Cookie)

Step 7: Caching

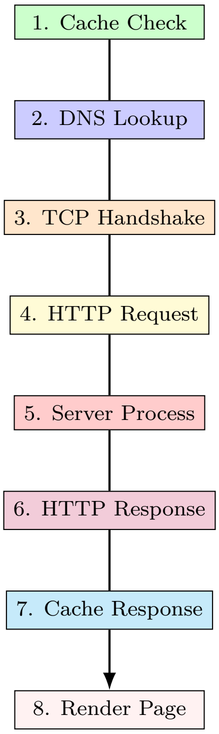
- If data is cacheable, browser caches it
- Future requests served from cache
- Reduces load time

Step 8: Rendering

- Browser decodes response
- Parses HTML → builds DOM
- Parses CSS → builds CSSOM
- Executes JavaScript
- Renders content on screen

Step 9: Connection Management

- Browser may close TCP connection
- Or reuse for future requests (keep-alive)



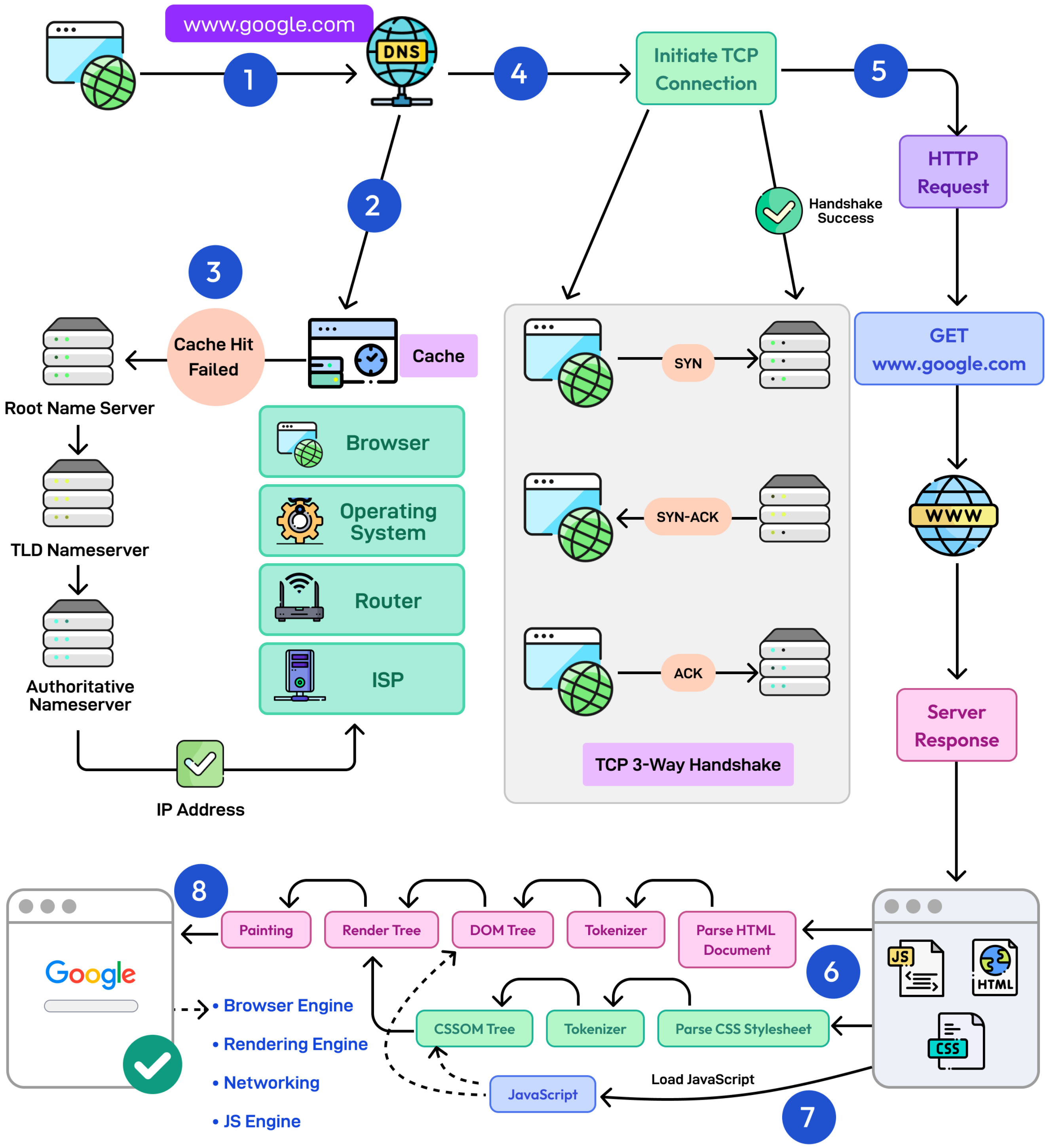
Key Point

Key Technologies Involved:

- **DNS:** Domain to IP resolution
- **TCP:** Reliable connection
- **HTTP/HTTPS:** Application protocol
- **TLS/SSL:** Encryption (HTTPS)
- **Caching:** Performance optimization

What Happens When You Type Google.com in Your Browser?

ByteByteGo



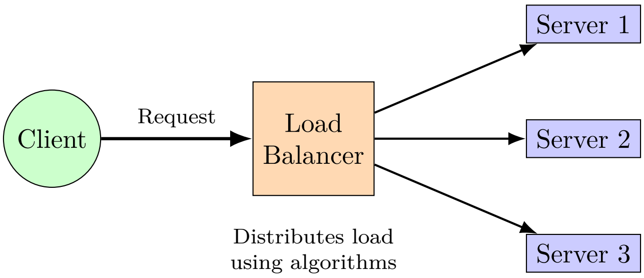
12 Advanced Topics

12.1 Server-Side Load Balancer

Definition

Load Balancer: A device or software that distributes network traffic across multiple backend servers to ensure high availability and reliability.

How it Works:



Load Balancing Algorithms:

- **Round Robin:** Distribute requests sequentially
- **Least Connections:** Send to server with fewest active connections
- **IP Hash:** Same client always goes to same server
- **Weighted:** Based on server capacity
- **Random:** Random server selection

Example: AWS ELB (Elastic Load Balancing)

- Registers multiple EC2 instances in auto-scaling group
- Client requests sent to load balancer
- Load balancer routes to one of the EC2 instances
- Monitors health of instances
- Removes unhealthy instances from rotation

Advantages of Server-Side Load Balancing:

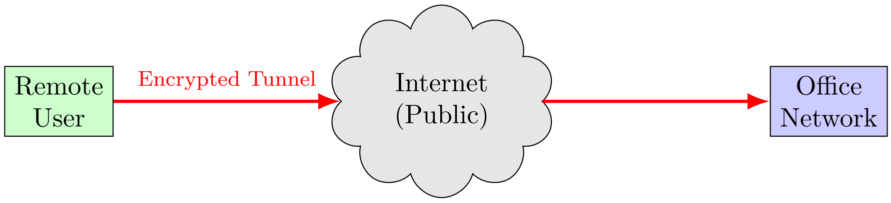
1. **Simple Client Configuration:**
    - Clients only need load balancer address
    - No need to know backend servers
2. **Clients Can Be Untrusted:**
    - All traffic goes through load balancer
    - Can inspect and filter traffic
    - Backend servers hidden from clients
3. **High Availability:**
    - If one server fails, traffic redirected
    - Automatic failover
4. **Scalability:**
    - Add/remove servers dynamically
    - Handle increased load
5. **Security:**
    - Single entry point
    - Can implement SSL termination
    - DDoS protection

12.2 What is VPN?

Definition

VPN (Virtual Private Network): A private WAN built on the Internet. Creates a secured tunnel between different networks using the public network.

How VPN Works:



VPN creates secure
encrypted connection

VPN Features:

- Creates encrypted tunnel over Internet
- Masks IP address and location
- Secure data transmission
- Access remote networks as if local

Advantages of VPN:

1. **Cost-Effective:**
   - Connect offices remotely via Internet
   - Cheaper than dedicated WAN connections
2. **Secure Transactions:**
   - Encrypted data transfer
   - Secure for confidential information
   - Works across geographical locations
3. **Information Security:**
   - Protection against threats and intrusions
   - Uses virtualization for security
4. **Privacy:**
   - Encrypts Internet traffic
   - Disguises online identity
   - Prevents tracking

Disadvantages of VPN:

1. **Not for Continuous Use:**
   - Can be unstable for 24/7 connections
   - May drop connections
2. **Complexity Prevents Scalability:**
   - Difficult to manage large deployments
   - Complex configuration
3. **Lack of Granular Security:**
   - All-or-nothing access model
   - Cannot easily restrict specific resources
4. **Unpredictable Performance:**
   - Depends on Internet connection quality
   - Encryption adds overhead
5. **Unreliable Availability:**
   - Dependent on public Internet

- No guaranteed uptime

Quick Recap

VPN Use Cases:

- Remote work (access corporate network from home)
- Secure browsing on public WiFi
- Bypass geographic restrictions
- Privacy protection
- Site-to-site connectivity (branch offices)

12.3 What is LAN?

Definition

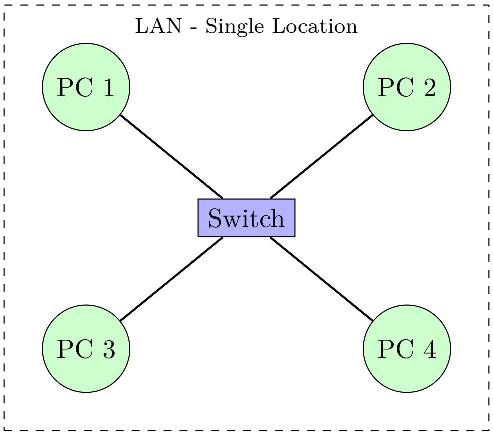
LAN (Local Area Network): A collection of devices connected together in one physical location, such as a building, office, or home.

LAN Characteristics:

- **Geographic Coverage:** Small area (building, campus)
- **Speed:** High (typically 100 Mbps to 10 Gbps)
- **Ownership:** Usually owned by one organization
- **Latency:** Very low
- **Technology:** Ethernet, WiFi (802.11)
- **Cost:** Low (compared to WAN)

LAN Size:

- Can be small: Home network with 2-10 devices
- Can be large: Enterprise network with thousands of devices



Common LAN Topologies:

- **Star:** Most common (all devices connect to central switch)
- **Bus:** Legacy (single cable backbone)
- **Ring:** Rare (token ring networks)

Example

Home LAN:

- WiFi router connects all devices
- Laptops, phones, smart TV, IoT devices
- Share Internet connection
- Share printers, file storage
- Private IP addresses (192.168.x.x)

13 Quick Reference & Summary

13.1 Port Numbers Reference

Port	Protocol	Description
20, 21	FTP	File Transfer Protocol
22	SSH	Secure Shell
23	Telnet	Remote Terminal (insecure)
25	SMTP	Email Sending
53	DNS	Domain Name System
67, 68	DHCP	Dynamic IP Assignment
80	HTTP	Web Traffic
110	POP3	Email Retrieval
143	IMAP	Email Sync
443	HTTPS	Secure Web Traffic
587	SMTP	Email Submission

13.2 Network Commands Cheat Sheet

Key Point

Essential Commands:

- `ping <host>` — Test connectivity, measure RTT
- `traceroute <host>` — Show path to destination
- `nslookup <domain>` — DNS lookup
- `ipconfig` (Win) / `ifconfig` (Linux) — Network config
- `netstat -an` — Active connections
- `arp -a` — ARP table
- `route print` — Routing table

13.3 OSI vs TCP/IP Quick Comparison

OSI Model (7 Layers)	TCP/IP Model (4 Layers)
7. Application 6. Presentation 5. Session	Application
4. Transport	Transport
3. Network	Internet
2. Data Link 1. Physical	Network Access/Link

13.4 Key Concepts Summary

Quick Recap

Network Fundamentals:

- Network = connected devices sharing data
- Topology = arrangement of nodes and links
- Bandwidth = data transfer capacity

OSI Model:

- 7 layers: Application to Physical
- Each layer has specific function
- Data encapsulated at each layer

TCP/IP Model:

- 4 layers: Application, Transport, Internet, Link
- Practical implementation used by Internet
- TCP = reliable, UDP = fast

Addressing:

- MAC address = Physical (Layer 2)
- IP address = Logical (Layer 3)
- Port number = Application (Layer 4)

Devices:

- Hub = Layer 1 (broadcast, obsolete)
- Switch = Layer 2 (MAC-based forwarding)
- Router = Layer 3 (IP-based routing)
- Gateway = Protocol converter

Protocols:

- HTTP/HTTPS = Web communication
- SMTP = Email sending
- POP3/IMAP = Email receiving
- DNS = Name to IP resolution
- DHCP = Automatic IP assignment

14 Interview Preparation Tips

14.1 Most Frequently Asked Questions

Interview Question

Top 10 Interview Questions:

1. What happens when you type google.com?
2. Explain OSI model layers
3. TCP vs UDP differences
4. What is 3-way handshake?
5. How does DNS work?
6. Difference between Hub, Switch, and Router
7. What is subnet and subnetting?
8. Explain HTTP vs HTTPS
9. What is a firewall and how does it work?
10. Different types of network delays

14.2 Key Topics to Master

Key Point

Must-Know Areas:

1. **OSI and TCP/IP Models:** All layers and their functions
2. **Protocols:** HTTP, HTTPS, TCP, UDP, DNS, DHCP, SMTP
3. **Addressing:** IP addressing, MAC addresses, subnetting
4. **Devices:** Hub, Switch, Router, Gateway differences
5. **Security:** Firewalls, VPN, encryption (RSA, TLS)
6. **Troubleshooting:** ping, traceroute, common issues
7. **Connection Management:** 3-way handshake, connection states
8. **Performance:** Delays, bandwidth, latency

14.3 Study Strategy

1. Understand Concepts:

- Don't just memorize—understand why
- Know the purpose of each protocol
- Understand layer interactions

2. Practice with Tools:

- Use ping, traceroute, nslookup
- Analyze with Wireshark
- Set up small test networks

3. Draw Diagrams:

- Network topologies
- Data flow through layers
- Protocol interactions

4. Compare and Contrast:

- TCP vs UDP
- HTTP vs HTTPS
- IPv4 vs IPv6
- Hub vs Switch vs Router

5. Real-World Scenarios:

- Trace complete data flow
- Troubleshoot connectivity issues
- Explain security implementations

15 Conclusion

Key Point

Remember the Fundamentals:
Networks enable communication between devices. Understanding how data flows through layers, how devices forward traffic, and how protocols work together is essential for any networking role.

Key Takeaways:

- OSI has 7 layers; TCP/IP has 4 layers (practical)
- Each layer adds headers (encapsulation)
- TCP is reliable; UDP is fast
- Routers connect networks; Switches connect devices
- DNS translates names to IPs
- DHCP assigns IPs automatically
- Security is multi-layered (firewalls, encryption, VPN)

Quick Recap

Study Tips for Success:

1. Focus on understanding, not memorization
2. Practice with real tools and commands
3. Draw diagrams to visualize concepts
4. Explain concepts to others (teaching solidifies learning)
5. Work through the "google.com" question multiple times
6. Understand both theory and practical applications

Best of Luck with Your Preparation!

"In networking, understanding the 'why' is more important than memorizing the 'what'."

Practice → Understand → Master

Quick Memory Aids:

OSI Layers:	"All People Seem To Need Data Processing"
TCP/IP:	Application, Transport, Internet, Link
3-Way Handshake:	SYN → SYN+ACK → ACK
Email:	SMTP sends, POP3/IMAP receives
Delays:	Transmission, Propagation, Queueing, Processing