

Lecture: Fundamentals of Computer Networks

1. Basics of Computer Networks

Definition

A computer network is a system of interconnected computing devices (computers, servers, routers, switches, etc.) that communicate and share resources (data, applications, printers, etc.) using wired or wireless transmission media.

Uses of Computer Networks

- Resource Sharing (files, printers, internet)
- Communication (email, video calls, messaging)
- Distributed Computing (cloud computing, parallel processing)
- Remote Access (VPN, SSH)
- E-commerce & Online Services (banking, streaming)

Types of Networks

(a) PAN (Personal Area Network)

- Range: Very small (up to 10 meters)
- Example: Bluetooth, USB tethering, smartwatches

(b) LAN (Local Area Network)

- Range: Small (home, office, campus)
- Characteristics: High speed, low latency, owned by a single organization
- Example: Ethernet, Wi-Fi in an office

(c) MAN (Metropolitan Area Network)

- Range: City-wide (10-50 km)
- Example: Cable TV networks, city-wide Wi-Fi

(d) WAN (Wide Area Network)

- Range: Global (countries, continents)
- Characteristics: Uses leased lines, satellites, or undersea cables
- Example: The Internet, corporate networks (bank branches worldwide)

(e) Other Types

- CAN (Campus Area Network) – University/Corporate campuses
 - SAN (Storage Area Network) – High-speed storage networks
 - VPN (Virtual Private Network) – Secure remote access
-

2. Network Topologies

(a) Star Topology

- Structure: All devices connect to a central hub/switch.
- Pros: Easy to manage, fault isolation.
- Cons: Hub failure disrupts the entire network.

(b) Bus Topology

- Structure: All devices share a single communication line (backbone).
- Pros: Simple, low cost.
- Cons: Collisions occur, difficult to troubleshoot.

(c) Ring Topology

- Structure: Devices form a closed loop; data travels in one direction (or bidirectional).
- Pros: No collisions, predictable performance.
- Cons: Failure of one node breaks the ring.

(d) Mesh Topology

- Structure: Every device connects to every other device.
 - Full Mesh: All nodes interconnected (expensive, highly reliable).

- Partial Mesh: Some nodes interconnected (cost-effective).
- Pros: Redundant, fault-tolerant.
- Cons: High cabling cost, complex setup.

(e) Hybrid Topology

- Structure: Combination of two or more topologies (e.g., Star-Bus, Star-Ring).
- Pros: Flexible, scalable.
- Cons: Complex design.

3. Circuit Switching vs. Packet Switching

Feature	Circuit Switching	Packet Switching
Connection	Dedicated path	No dedicated path
Usage	Traditional telephony	Internet (IP)
Efficiency	Low (idle time)	High (shared lines)
Delay	Fixed	Variable
Example	PSTN (Phone lines)	Internet (TCP/IP)

- Circuit Switching: Used in old telephone networks; resources reserved for the entire session.
- Packet Switching: Data split into packets, sent independently, and reassembled at the destination (more efficient).

4. Network Models

(a) OSI Model (7 Layers)

A theoretical framework defining how data travels across networks.

Layer	Name	Function	Example Protocols
7	Application	User interface (HTTP, FTP)	HTTP, SMTP, FTP
6	Presentation	Data formatting, encryption	SSL, JPEG, MPEG
5	Session	Manages connections	NetBIOS, RPC
4	Transport	End-to-end communication (reliability)	TCP, UDP
3	Network	Logical addressing & routing	IP, ICMP, BGP
2	Data Link	Framing, MAC addressing	Ethernet, PPP
1	Physical	Raw bit transmission	Fiber, Wi-Fi, USB

(b) TCP/IP Model (4 Layers)

A practical model used in the real-world Internet.

Layer	Name	OSI Equivalent	Example Protocols
4	Application	Application, Presentation, Session	HTTP, FTP, DNS
3	Transport	Transport	TCP, UDP
2	Internet	Network	IP, ICMP
1	Network Access	Data Link, Physical	Ethernet, Wi-Fi

(c) Comparison: OSI vs. TCP/IP

Feature	OSI Model	TCP/IP Model
Layers	7	4
Approach	Theoretical	Practical
Usage	Teaching, reference	Real-world Internet
Protocol Dependency	Protocol-independent	Built around TCP/IP

Summary

- Networks enable communication and resource sharing.
- Topologies define how devices are interconnected.
- Switching methods (Circuit vs. Packet) determine efficiency.
- OSI Model is a reference; TCP/IP is what the Internet uses.

Lecture: Physical Layer in Computer Networks

The Physical Layer (Layer 1) of the OSI model is responsible for transmitting raw bits over a communication channel. It deals with:

- Transmission media (wired/wireless)
 - Signal encoding & modulation
 - Multiplexing techniques
 - Physical devices that transmit data
-

1. Transmission Media

Transmission media are the pathways that carry data from sender to receiver. They are classified into:

A. Guided (Wired) Media

Data travels through a physical medium.

(1) Twisted Pair Cable

- Structure: Two insulated copper wires twisted together to reduce interference.
- Types:
 - Unshielded Twisted Pair (UTP): Common in Ethernet (Cat5, Cat6).
 - Pros: Cheap, flexible, easy to install.
 - Cons: Susceptible to EMI (Electromagnetic Interference).
 - Shielded Twisted Pair (STP): Extra shielding to reduce EMI.
 - Used in: Industrial environments.

- Applications: Telephone lines, Ethernet (LAN).

(2) Coaxial Cable

- Structure:
 - Inner conductor (copper core)
 - Insulation layer
 - Outer metallic shield (reduces EMI)
 - Plastic jacket
- Pros: Better noise immunity than UTP, higher bandwidth.
- Cons: Expensive, bulky.
- Applications: Cable TV, broadband internet (DOCSIS).

(3) Fiber Optic Cable

- Structure:
 - Core: Glass/plastic (carries light pulses).
 - Cladding: Reflects light back into the core.
 - Outer Jacket: Protects the fiber.
 - Types:
 - Single-mode Fiber (SMF): Thin core, long-distance (100+ km).
 - Multi-mode Fiber (MMF): Thicker core, shorter distances (2 km).
 - Pros:
 - Extremely high bandwidth (Tbps).
 - Immune to EMI, secure (no signal leakage).
 - Cons: Expensive, fragile, difficult to install.
 - Applications: Internet backbones, undersea cables, data centers.
-

B. Unguided (Wireless) Media

Data travels through the air (no physical medium).

(1) Radio Waves

- Frequency Range: 3 kHz – 300 GHz.
- Propagation: Omni-directional (travels in all directions).
- Pros: Long-range, penetrates walls.

- Cons: Susceptible to interference.
- Applications: AM/FM radio, Wi-Fi (2.4 GHz, 5 GHz), Bluetooth.

(2) Microwaves

- Frequency Range: 1 GHz – 300 GHz.
- Propagation: Line-of-sight (requires antennas).
- Types:
 - Terrestrial Microwave: Used between towers (e.g., cellular networks).
 - Satellite Microwave: Communication via satellites (e.g., GPS, satellite TV).
- Pros: High bandwidth, long-distance.
- Cons: Affected by weather, expensive infrastructure.

(3) Infrared (IR)

- Frequency Range: 300 GHz – 400 THz.
 - Propagation: Short-range, line-of-sight.
 - Pros: Secure (doesn't pass through walls).
 - Cons: Short range (~5m).
 - Applications: TV remotes, IR data transfer (old smartphones).
-

2. Modulation Techniques

Modulation modifies a carrier signal to encode data.

A. Analog Modulation

- Amplitude Modulation (AM): Varies signal strength.
- Frequency Modulation (FM): Varies frequency.
- Phase Modulation (PM): Varies phase.

B. Digital Modulation

- ASK (Amplitude Shift Keying): Binary 0/1 represented by different amplitudes.
- FSK (Frequency Shift Keying): Different frequencies for 0/1.
- PSK (Phase Shift Keying): Phase changes represent bits.

- QAM (Quadrature Amplitude Modulation): Combines ASK & PSK (used in Wi-Fi, cable modems).

3. Multiplexing

Combining multiple signals into one medium.

Technique	Description	Application
FDM (Frequency Division Multiplexing)	Divides bandwidth into frequency slots	FM radio, cable TV
TDM (Time Division Multiplexing)	Divides time into slots, each signal gets a turn	Traditional telephony
WDM (Wavelength Division Multiplexing)	Different wavelengths (colors) in fiber optics	Fiber-optic networks

4. Digital Transmission

A. Line Coding

Converts binary data into electrical signals.

- NRZ (Non-Return to Zero): 1 = High voltage, 0 = Low voltage.
- Manchester Encoding: Transition in middle of bit (used in Ethernet).

B. Block Coding

Adds redundancy for error detection (e.g., 4B/5B encoding in Fast Ethernet).

5. Physical Layer Devices

Device	Function	Layer
Hub	Broadcasts data to all ports (dumb device)	Physical
Repeater	Amplifies signals to extend range	Physical
Modem	Converts digital ↔ analog signals (for DSL/cable)	Physical

Summary

- Guided Media: Twisted pair (cheap), coaxial (better shielding), fiber (best speed).
- Wireless Media: Radio (long-range), microwave (line-of-sight), IR (short-range).
- Modulation: ASK, FSK, PSK, QAM for encoding data.
- Multiplexing: FDM (frequency), TDM (time), WDM (wavelength).
- Devices: Hubs (obsolete), repeaters (signal boosters), modems (signal conversion).

Lecture: Data Link Layer (Layer 2)

The Data Link Layer (DLL) is OSI Layer 2 and ensures reliable data transfer between directly connected nodes. It handles:

- Framing (packaging data into frames)
- Error detection & correction
- Flow control (managing data transmission speed)
- Media Access Control (MAC) (regulating shared medium access)
- LAN technologies (Ethernet, Wi-Fi, VLANs)

1. Framing & Error Detection

A. Framing

- Breaks data into frames for transmission.
- Methods:
 1. Character Count (header specifies frame size) → Rarely used (prone to errors).
 2. Flag Bytes with Byte Stuffing (Uses FLAG=01111110, escape byte ESC if data contains FLAG).
 3. Bit Stuffing (Adds extra 0 after five consecutive 1s to avoid 01111110 in data).

B. Error Detection Techniques

Method	How It Works	Use Case
Parity Check	Adds an extra bit (even/odd parity)	Single-bit error detection
Checksum	Sum of data bits sent as extra field	Simple error detection (UDP, IP)
CRC (Cyclic Redundancy Check)	Uses polynomial division for checksum	Ethernet, Wi-Fi, storage

CRC Example:

- Sender & receiver agree on a generator polynomial (e.g., $x^3 + x + 1 = 1011$).
 - Append (n-1) zeros to data, divide by polynomial, send remainder as CRC code.
-

2. Flow Control

Prevents sender from overwhelming receiver.

A. Stop-and-Wait

- Sender sends one frame, waits for ACK before next.
- Pros: Simple
- Cons: Inefficient (low throughput).

B. Sliding Window

- Allows multiple frames in transit.
- Types:
 - Go-Back-N (GBN): Resends all frames after lost one.
 - Selective Repeat (SR): Resends only lost/damaged frames.

Feature	Go-Back-N	Selective Repeat
Retransmission	All frames after error	Only corrupted frames
Efficiency	Low (wastes bandwidth)	High
Complexity	Simple	Complex (needs buffers)

3. Error Control (ARQ)

Automatic Repeat Request (ARQ) ensures reliable delivery.

ARQ Type	How It Works	Example
Stop-and-Wait ARQ	Sender waits for ACK before next frame	Basic protocols
Go-Back-N ARQ	Resends entire window on error	TCP (partially)
Selective Repeat ARQ	Only retransmits lost frames	Modern networks

4. MAC (Medium Access Control) Protocols

Controls how devices access a shared medium (Ethernet, Wi-Fi).

A. CSMA/CD (Ethernet)

- Carrier Sense Multiple Access / Collision Detection.
- Steps:
 1. Listen before sending.
 2. If collision detected, wait random time (exponential backoff).
- Used in: Wired Ethernet (IEEE 802.3) (obsolete in modern full-duplex switches).

B. CSMA/CA (Wi-Fi)

- Carrier Sense Multiple Access / Collision Avoidance.
- Steps:
 1. Wait for DIFS (Distributed Inter-Frame Space).
 2. Send RTS/CTS (Request-to-Send / Clear-to-Send) to reserve channel.
- Used in: Wireless (IEEE 802.11).

C. Polling

- Master-slave model (controller asks devices if they want to transmit).
- Used in: Bluetooth.

D. Token Passing

- Token circulates, only the holder can transmit.
 - Used in: Token Ring (IEEE 802.5), FDDI.
-

5. LAN Technologies

A. Ethernet (IEEE 802.3)

- Frame Format:
 - text
 - Copy
 - Download
 - | Preamble | Dest MAC | Src MAC | Type/Length | Data | CRC |
 - Speeds: 10 Mbps (Ethernet), 100 Mbps (Fast Ethernet), 1 Gbps (Gigabit Ethernet).
 - MAC Address: 48-bit (e.g., 00:1A:2B:3C:4D:5E).

B. Wi-Fi (IEEE 802.11)

- Standards:

Version	Speed	Frequency
802.11a	54 Mbps	5 GHz
802.11b	11 Mbps	2.4 GHz
802.11g	54 Mbps	2.4 GHz
802.11n	600 Mbps	2.4/5 GHz
802.11ac	1.3 Gbps	5 GHz

802.11ax	10 Gbps	2.4/5/6 GHz
----------	---------	-------------

- CSMA/CA used instead of CSMA/CD (no collision detection in wireless).

C. VLANs (Virtual LANs)

- Logically separates networks within a physical LAN.
 - Uses 802.1Q tagging (adds VLAN ID to Ethernet frame).
 - Benefits:
 - Improved security (isolates traffic).
 - Reduces broadcast domains.
-

6. Switching (Bridge vs. Switch)

Feature	Bridge	Switch
Ports	Few (2-16)	Many (24-48+)
Speed	Slow	Fast (Gigabit+)
Learning	Uses MAC table	Uses MAC table
Type	Software-based	Hardware-based (ASIC)

- Switches dominate modern networks (faster, more ports).
-

7. PPP (Point-to-Point Protocol)

- Used for direct two-node connections (e.g., dial-up, DSL).
 - Features:
 - Authentication (PAP, CHAP)
 - Supports multiple network protocols (IP, IPX).
 - Frame Format:
 - | Flag | Address | Control | Protocol | Data | CRC | Flag |
-

Summary

- Framing: Breaks data into frames (bit/byte stuffing).
- Error Detection: CRC (best), Checksum, Parity.
- Flow Control: Stop-and-Wait (slow), Sliding Window (efficient).
- MAC Protocols: CSMA/CD (Ethernet), CSMA/CA (Wi-Fi), Token Passing (old LANs).
- LAN Tech: Ethernet (wired), Wi-Fi (wireless), VLANs (logical separation).
- Switching: Bridges (legacy), Switches (modern).
- PPP: For point-to-point links (DSL, dial-up).

Lecture: Network Layer (Layer 3)

The Network Layer (OSI Layer 3) is responsible for logical addressing, routing, and forwarding packets across different networks. Key topics include:

1. IP Addressing

A. IPv4 (32-bit)

- Format: 192.168.1.1 (4 octets, dotted-decimal notation).
- Address Classes:

Class	Range	Purpose
A	1.0.0.0 – 126.255.255.255	Large networks
B	128.0.0.0 – 191.255.255.255	Medium networks
C	192.0.0.0 – 223.255.255.255	Small networks
D	224.0.0.0 – 239.255.255.255	Multicast
E	240.0.0.0 – 255.255.255.255	Reserved

- Private IP Ranges:
 - 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 (used in LANs).

B. IPv6 (128-bit)

- Format: 2001:0db8:85a3::8a2e:0370:7334 (hexadecimal, 8 groups of 16 bits).
- Advantages over IPv4:
 - Larger address space (3.4×10^{38} addresses).
 - Built-in security (IPSec).
 - Simplified header (faster routing).
 - No NAT needed (end-to-end connectivity).

2. Subnetting & Supernetting

A. Subnetting (Dividing a Network)

- Purpose: Efficient IP allocation, security, reducing broadcast domains.
- Example:
 - Given `192.168.1.0/24`, divide into 4 subnets:
 - Subnet Mask: `255.255.255.192 (/26)`
 - Subnets:
 - `192.168.1.0/26 (1-62)`
 - `192.168.1.64/26 (65-126)`
 - `192.168.1.128/26 (129-190)`
 - `192.168.1.192/26 (193-254)`

B. Supernetting (CIDR – Classless Inter-Domain Routing)

- Purpose: Combine multiple small networks into a larger one.
- Example:
 - Merge `192.168.1.0/24` and `192.168.2.0/24` → `192.168.0.0/22`.

C. VLSM (Variable Length Subnet Mask)

- Allows different subnet sizes in the same network.
- Use Case: Efficiently allocate IPs where some subnets need more hosts than others.

3. Routing Algorithms

A. Static vs. Dynamic Routing

Feature	Static Routing	Dynamic Routing
Configuration	Manual	Automatic
Scalability	Poor (small networks)	Good (large networks)

Overhead	Low	High (updates consume bandwidth)
Example	Home routers	OSPF, BGP

B. Distance Vector (RIP)

- How it works:
 - Routers share entire routing tables with neighbors.
 - Uses hop count as metric (max 15 hops).
- Disadvantages: Slow convergence, prone to loops.
- Example: RIP (Routing Information Protocol).

C. Link State (OSPF)

- How it works:
 - Routers share link-state advertisements (LSAs).
 - Builds a topology map using Dijkstra's algorithm.
- Advantages: Fast convergence, loop-free.
- Example: OSPF (Open Shortest Path First).

D. Path Vector (BGP)

- How it works:
 - Used in Internet backbone.
 - Routes based on AS (Autonomous System) paths.
- Example: BGP (Border Gateway Protocol).

4. Key Network Protocols

Protocol	Purpose	Layer
ARP	Maps IP → MAC (e.g., <code>arp -a</code>)	L2/L3

RARP	Maps MAC → IP (obsolete, replaced by DHCP)	L2/L3
ICMP	Error reporting (e.g., <code>ping</code> , <code>traceroute</code>)	L3
DHCP	Assigns IPs dynamically (e.g., <code>dhclient</code>)	L3

5. NAT (Network Address Translation)

- Purpose: Allows private IPs to access the Internet via a single public IP.
- Types:
 - Static NAT (1 private IP ↔ 1 public IP).
 - Dynamic NAT (pool of public IPs).
 - PAT (Port Address Translation) (Many private IPs → 1 public IP with ports).

6. Routing Devices

Device	Function	Key Feature
Router	Connects different networks	Uses IP routing tables
Layer 3 Switch	Switch with routing capabilities	Faster than routers (hardware-based)

7. IPv6 Features & Transition Mechanisms

A. IPv6 Key Features

- No Broadcasts (uses multicasting).
- Stateless Address Autoconfiguration (SLAAC).
- Simplified Header (fixed 40 bytes).

B. Transition Mechanisms

Method	How It Works	Use Case
Dual Stack	Runs IPv4 & IPv6 simultaneously	Most common
Tunneling	Encapsulates IPv6 in IPv4	Transition networks
NAT64	Translates IPv6 ↔ IPv4	Legacy IPv4 support

Summary

- IPv4 vs. IPv6: IPv6 solves address exhaustion.
- Subnetting: Efficient IP allocation.
- Routing:
 - Distance Vector (RIP) – Simple but slow.
 - Link State (OSPF) – Fast, scalable.
 - Path Vector (BGP) – Internet backbone.
- NAT: Allows private IPs to use a single public IP.
- IPv6 Transition: Dual-stack, tunneling, NAT64.

Lecture: Transport Layer (Layer 4)

The Transport Layer (OSI Layer 4) ensures end-to-end communication between applications. It provides:

- ✓ Reliable data transfer (TCP)
 - ✓ Unreliable but fast delivery (UDP)
 - ✓ Flow & congestion control
 - ✓ Error recovery
-

1. TCP (Transmission Control Protocol)

Key Features

- Connection-oriented (establishes a session before data transfer).
- Reliable (acknowledgments, retransmissions).
- Flow & congestion control.
- Full-duplex (simultaneous two-way communication).

A. TCP 3-Way Handshake

Establishes a connection before data transfer:

1. SYN (Client → Server): "Can we connect?"
2. SYN-ACK (Server → Client): "Yes, here's my initial sequence number."
3. ACK (Client → Server): "Got it, let's start!"

Why 3 steps?

- Ensures both sides are ready.
- Synchronizes sequence numbers (prevents old duplicate packets).

B. TCP Flow Control

- Prevents sender from overwhelming receiver.
- Uses sliding window mechanism:
 - Receiver advertises window size (free buffer space).
 - Sender adjusts transmission rate accordingly.

C. TCP Congestion Control

- Prevents network overload.
- Mechanisms:
 - Slow Start: Exponential growth until threshold.
 - Congestion Avoidance: Linear growth after threshold.
 - Fast Retransmit: Resends lost packet after 3 duplicate ACKs.
 - Fast Recovery: Avoids resetting window after packet loss.

D. TCP Error Recovery

- Sequence Numbers: Track sent/received bytes.
 - ACKs: Confirm received data.
 - Retransmission Timeout (RTO): Resends lost packets if no ACK.
-

2. UDP (User Datagram Protocol)



Key Features

- Connectionless (no handshake).
- Unreliable (no ACKs, retransmissions).
- Low overhead (faster than TCP).
- No congestion control.

Use Cases

- Real-time apps (VoIP, video streaming).
- DNS queries.
- Gaming (fast but loss-tolerant).

Feature	TCP	UDP
Reliability	✓ Guaranteed	✗ Best-effort
Ordering	✓ In-order delivery	✗ No ordering

Speed	 Slower (overhead)	 Faster
Use Case	Web, email, FTP	VoIP, gaming, DNS

3. Ports & Sockets

A. Ports

- 16-bit identifiers (0-65535).
- Well-known ports (0-1023):
 - 80 (HTTP), 443 (HTTPS), 22 (SSH).
- Dynamic ports (49152-65535): Temporary client ports.

B. Sockets

- Combination of IP + Port (e.g., 192.168.1.1:80).
 - Types:
 - Stream (TCP): Reliable, connection-based.
 - Datagram (UDP): Unreliable, connectionless.
-

4. Congestion Control Algorithms

A. TCP Tahoe

- Slow Start → Congestion Avoidance.
- On packet loss:
 - Reset window to 1 (too aggressive).

B. TCP Reno

- Improves Tahoe with Fast Recovery.
- On 3 duplicate ACKs:
 - Retransmits lost packet without full reset.

C. TCP CUBIC

- Modern default in Linux.
- Uses cubic function for window growth (scales better in high-speed networks).

Algorithm	Key Feature	Weakness
Tahoe	Basic slow start	Resets window too aggressively
Reno	Fast recovery	Performs poorly with multiple losses
CUBIC	High-speed optimized	Complex

5. QoS (Quality of Service)

Ensures priority handling for critical traffic.

Techniques

1. Traffic Shaping:
 - Limits bandwidth (e.g., 100 Mbps for VoIP).
2. Priority Queuing:
 - VoIP > Streaming > Web Browsing.
3. DiffServ (Differentiated Services):
 - Marks packets with DSCP (e.g., EF for VoIP).
4. RSVP (Resource Reservation Protocol):
 - Reserves bandwidth for specific flows.

Use Cases

- VoIP: Low latency, minimal jitter.
 - Video Streaming: High bandwidth.
 - Gaming: Low packet loss.
-

Summary

Concept	Key Takeaway
TCP	Reliable, connection-oriented, flow/congestion control.
UDP	Fast, connectionless, no guarantees.
Ports/Sockets	Identify apps (e.g., 80=HTTP).
Congestion Control	Tahoe (basic), Reno (fast recovery), CUBIC (modern).
QoS	Prioritizes critical traffic (VoIP, video).

Lecture: Application Layer (Layer 7)

The Application Layer (OSI Layer 7) enables user applications to access network services. It includes protocols for:

- ✓ Web browsing (HTTP/HTTPS)
- ✓ File transfers (FTP)

- ✓ Email (SMTP, POP3, IMAP)
 - ✓ Network management (SNMP, DHCP)
 - ✓ Modern web APIs (REST, WebSockets)
-

1. Web Protocols: HTTP & HTTPS

A. HTTP (Hypertext Transfer Protocol)

- Stateless, text-based protocol (port 80).
- Request Methods:
 - GET (fetch data)
 - POST (submit data)
 - PUT (update resource)
 - DELETE (remove resource)

HTTP Request Example:

http

Copy

Download

```
GET /index.html HTTP/1.1
```

```
Host: www.example.com
```

```
User-Agent: Mozilla/5.0
```

HTTP Response Example:

http

Copy

Download

```
HTTP/1.1 200 OK
```

```
Content-Type: text/html
```

```
Content-Length: 137
```

```
<html>...</html>
```

B. HTTPS (HTTP Secure)

- HTTP + SSL/TLS encryption (port 443).
 - Prevents eavesdropping, tampering, MITM attacks.
 - Uses certificates (PKI) for authentication.
-

2. File Transfer Protocol (FTP)

- Ports: 21 (control), 20 (data).
 - Modes:
 - Active FTP: Server initiates data connection.
 - Passive FTP: Client initiates data connection (better for firewalls).
 - Security Issues:
 - SFTP (SSH FTP) and FTPS (FTP + SSL) are secure alternatives.
-

3. Email Protocols

A. SMTP (Simple Mail Transfer Protocol)

- Sends emails (port 25 or 587 for TLS).
- Flow:
 - text
 - Copy
 - Download
- Sender → SMTP Server → Recipient's SMTP Server → POP3/IMAP

B. POP3 (Post Office Protocol v3)

- Downloads emails to local device (port 110 or 995 for SSL).
- Deletes from server by default (no synchronization).

C. IMAP (Internet Message Access Protocol)

- Syncs emails across devices (port 143 or 993 for SSL).
- Stores emails on server (better for multiple devices).

Feature	SMTP	POP3	IMAP
Purpose	Send mail	Download mail	Sync mail
Port	25/587	110/995	143/993
Storage	N/A	Local	Server

4. DNS (Domain Name System)

- Translates `example.com` → `93.184.216.34`.
- Hierarchical Structure:
 - text
 - Copy
 - Download
- Root (.) → TLD (.com) → Domain (example) → Subdomain (www)
- Record Types:
 - A (IPv4), AAAA (IPv6)
 - MX (Mail Server), CNAME (Alias)
 - TXT (SPF, DKIM for email security)

DNS Lookup Process:

1. Checks local cache.
2. Queries recursive resolver (ISP).
3. If not found, goes to root → TLD → authoritative DNS.

5. DHCP (Dynamic Host Configuration Protocol)

- Assigns IPs automatically (port `67/UDP` server, `68/UDP` client).
- 4-Step Process (DORA):

1. Discover (Client broadcasts "Need IP").
 2. Offer (Server responds with IP offer).
 3. Request (Client accepts the offer).
 4. Acknowledge (Server confirms lease).
- Lease Time: IPs are temporary (default: 24 hours).
-

6. SNMP (Simple Network Management Protocol)

- Monitors & manages network devices (routers, switches).
 - Components:
 - Manager (collects data).
 - Agent (runs on devices).
 - MIB (Management Information Base: database of device metrics).
 - Versions:
 - SNMPv1/v2c: No encryption (uses community strings).
 - SNMPv3: Supports encryption & authentication.
-

7. P2P Networks & CDNs

A. P2P (Peer-to-Peer)

- No central server (e.g., BitTorrent, Blockchain).
- Pros: Scalable, resilient.
- Cons: Security risks (malware, illegal content).

B. CDN (Content Delivery Network)

- Distributed servers for faster content delivery.
 - Examples: Cloudflare, Akamai.
 - How it works:
 - User accesses nearest CDN node instead of origin server.
-

8. Web APIs & Real-Time Communication

A. REST APIs (Representational State Transfer)

- Stateless, uses HTTP methods.
- JSON/XML data format.
- Example:

- http
- Copy
- Download

GET /api/users/1 HTTP/1.1

- Host: api.example.com

B. WebSockets

- Full-duplex real-time communication (e.g., chat apps).
- Upgrades HTTP connection (ws:// or wss://).

9. Email Security

- SPF (Sender Policy Framework): Prevents email spoofing.
- DKIM (DomainKeys Identified Mail): Signs emails with DNS.
- DMARC (Domain-based Message Authentication): Combines SPF + DKIM.

Summary

Protocol	Purpose	Port
HTTP/HTTPS	Web browsing	80/443
FTP/SFTP	File transfer	21/22
SMTP	Send email	25/587

POP3/IMAP	Receive email	110/995, 143/993
DNS	Domain → IP	53
DHCP	Auto IP assignment	67/68
SNMP	Network monitoring	161/162

Key Takeaways:

- HTTP/HTTPS power the web (TLS adds security).
- Email relies on SMTP (send) + POP3/IMAP (receive).
- DNS is the Internet's phonebook.
- DHCP automates IP assignment.
- CDNs & P2P improve performance.

Lecture: Network Security

1. Cryptography

A. Symmetric Encryption

- Single shared key for encryption & decryption.
- Algorithms:
 - AES (Advanced Encryption Standard) – Most secure (128/256-bit).
 - DES (Data Encryption Standard) – Obsolete (56-bit key).
 - 3DES – Triple DES (168-bit, slow).
- Pros: Fast, efficient for bulk data.
- Cons: Key distribution problem.

B. Asymmetric Encryption (Public-Key Cryptography)

- Two keys:
 - Public Key (encrypts data).
 - Private Key (decrypts data).
- Algorithms:
 - RSA (Rivest-Shamir-Adleman) – Used in SSL/TLS.
 - ECC (Elliptic Curve Cryptography) – Smaller keys, faster.
- Pros: Solves key exchange issue.
- Cons: Slower than symmetric encryption.

C. Hybrid Encryption (Best of Both Worlds)

- How it works:
 1. Asymmetric encryption to exchange a symmetric key.
 2. Symmetric encryption for actual data transfer.
 - Used in: SSL/TLS, VPNs.
-

2. Authentication Protocols

A. Kerberos

- Purpose: Secure authentication in Windows Active Directory.
- How it works:
 1. User requests Ticket Granting Ticket (TGT) from Authentication Server (AS).
 2. Uses TGT to get service ticket from Ticket Granting Server (TGS).
 3. Accesses service (e.g., file server) with the ticket.
- Pros: No password transmission, prevents replay attacks.

B. OAuth 2.0

- Purpose: Delegated authorization (e.g., "Login with Google").
- Flow:
 1. App redirects user to OAuth provider (e.g., Google).
 2. User logs in & grants permissions.
 3. Provider issues an access token to the app.

- Used in: Social logins, API access.

Protocol	Purpose	Use Case
Kerberos	Authentication	Enterprise networks
OAuth	Authorization	Web/mobile apps

3. Firewalls, IDS/IPS

A. Firewalls

- Filters traffic based on rules (IP, port, protocol).
- Types:
 - Packet Filtering (Stateless) – Checks headers only.
 - Stateful Inspection – Tracks connections (e.g., TCP handshake).
 - Next-Gen Firewalls (NGFW) – Deep packet inspection (DPI), blocks malware.

B. IDS (Intrusion Detection System)

- Monitors traffic for attacks (passive).
- Types:
 - Network-based (NIDS) – Analyzes network traffic.
 - Host-based (HIDS) – Monitors a single device.

C. IPS (Intrusion Prevention System)

- Blocks attacks in real-time (active).
- Example: Snort (open-source IDS/IPS).

System	Action	Placement
--------	--------	-----------

Firewall	Blocks based on rules	Network perimeter
IDS	Alerts on threats	Passive (monitoring)
IPS	Blocks threats	Inline (active)

4. VPNs (Virtual Private Networks)

- Creates secure tunnel over public internet.
 - Protocols:
 - IPsec (L3 security, used in corporate VPNs).
 - OpenVPN (SSL/TLS-based, open-source).
 - WireGuard (Lightweight, faster than IPsec).
 - Use Cases:
 - Remote work (access company network).
 - Bypass geo-restrictions (not recommended for illegal use).
-

5. SSL/TLS & HTTPS

A. SSL/TLS Handshake

1. Client Hello – Sends supported cipher suites.
2. Server Hello – Chooses cipher, sends certificate.
3. Key Exchange – Client verifies cert, generates session key.
4. Secure Data Transfer – Encrypted with symmetric key.

B. HTTPS (HTTP + TLS)

- Port 443, encrypts web traffic.
- Prevents:

- Eavesdropping (MITM attacks).
 - Data tampering.
-

6. Cyber Threats

A. DDoS (Distributed Denial of Service)

- Floods target with traffic (e.g., botnets).
- Types:
 - Volumetric (UDP floods).
 - Application-layer (HTTP floods).
- Defense: Cloudflare, rate limiting.

B. Phishing

- Tricks users into revealing data (fake login pages).
- Example: "Your account is locked, click here."
- Defense: Email filters, user training.

C. MITM (Man-in-the-Middle)

- Attacker intercepts & alters traffic.
 - Example: Fake Wi-Fi hotspots.
 - Defense: HTTPS, VPNs, certificate pinning.
-

Summary

Concept	Key Takeaway
Symmetric Encryption	Fast, uses one key (AES).

Asymmetric Encryption	Solves key exchange (RSA, ECC).
Kerberos	Enterprise authentication (tickets).
OAuth	Delegated authorization (social logins).
Firewall	Blocks unauthorized traffic.
IDS/IPS	Detects/blocks attacks.
VPN	Secure remote access (IPSec, OpenVPN).
HTTPS	Encrypts web traffic (TLS 1.3).
DDoS/Phishing/MITM	Common attacks; use filtering & encryption.

Lecture: Wireless & Mobile Networks

1. WiFi Standards (IEEE 802.11 Family)

WiFi enables wireless local area networking (WLAN) under the IEEE 802.11 standard.

Evolution of WiFi Standards

Standard	Release Year	Frequency Band	Max Speed	Key Features
802.11a	1999	5 GHz	54 Mbps	First 5GHz standard, less interference
802.11b	1999	2.4 GHz	11 Mbps	Popular but slow, prone to interference
802.11g	2003	2.4 GHz	54 Mbps	Backward compatible with 802.11b
802.11n (WiFi 4)	2009	2.4/5 GHz	600 Mbps	MIMO (Multiple Input Multiple Output)
802.11ac (WiFi 5)	2013	5 GHz	3.5 Gbps	Wider channels (80/160 MHz), Beamforming
802.11ax (WiFi 6)	2019	2.4/5/6 GHz	9.6 Gbps	OFDMA, BSS Coloring, Better efficiency
802.11be (WiFi 7)	2024 (Expected)	2.4/5/6 GHz	40 Gbps	320 MHz channels, Multi-Link Operation

Key WiFi Technologies

- MIMO (Multiple Input Multiple Output): Uses multiple antennas for better throughput.
- OFDMA (Orthogonal Frequency Division Multiple Access): Allows multiple devices to share a channel (WiFi 6).
- Beamforming: Directs signals towards devices instead of broadcasting.

- BSS Coloring (WiFi 6): Reduces interference in dense networks.
-

2. Cellular Networks (4G LTE & 5G)

A. 4G LTE (Long-Term Evolution)

- Speed: 100 Mbps – 1 Gbps
- Technologies:
 - OFDMA (Efficient spectrum usage)
 - MIMO & Carrier Aggregation (Combines multiple bands)
 - VoLTE (Voice over LTE, better call quality)
- Latency: ~50ms

B. 5G (Fifth Generation)

- Speed: 1 – 10 Gbps (theoretical)
- Latency: <1ms (Ultra-Reliable Low Latency Communication - URLLC)
- Three Bands:
 - Low-Band (Sub-1GHz) – Wide coverage (similar to 4G).
 - Mid-Band (1-6GHz) – Balance of speed & coverage (e.g., 3.5GHz).
 - High-Band (mmWave, 24-100GHz) – Ultra-fast but short-range (stadiums, cities).
- Key Features:
 - Network Slicing (Custom virtual networks for different uses)
 - Massive MIMO (Hundreds of antennas in base stations)
 - Edge Computing (Reduces latency by processing data closer to users)

Generation	Speed	Latency	Key Innovation
4G LTE	100 Mbps – 1 Gbps	~50ms	All-IP networks
5G	1 – 10 Gbps	<1ms	mmWave, Network Slicing

3. Short-Range Wireless Technologies

A. Bluetooth

- Range: ~10m (Class 2), up to 100m (Class 1)
- Versions:
 - Bluetooth 4.0 (BLE - Low Energy): IoT devices (wearables).
 - Bluetooth 5.0: 2x speed, 4x range over 4.2.
- Use Cases: Wireless headphones, smartwatches, keyboards.

B. Zigbee (IEEE 802.15.4)

- Range: 10-100m (mesh networking extends range).
- Low Power: Ideal for IoT (smart home sensors).
- Frequency: 2.4 GHz (global), 915 MHz (Americas), 868 MHz (Europe).

C. NFC (Near Field Communication)

- Range: <10 cm.
- Use Cases:
 - Contactless payments (Apple Pay, Google Wallet).
 - Smart cards (transit passes).

Technology	Range	Data Rate	Power Use	Use Case
Bluetooth	10-100m	1-3 Mbps	Medium	Audio, peripherals
Zigbee	10-100m	250 Kbps	Very Low	Smart home IoT
NFC	<10 cm	424 Kbps	Ultra-Low	Payments, tags

4. Mobile IP

- Allows devices to keep the same IP address while moving across networks.
 - How it works:
 1. Home Agent (HA) tracks the device's location.
 2. Foreign Agent (FA) provides a temporary IP when roaming.
 3. Tunneling forwards packets to the mobile device.
 - Used in: Cellular networks (4G/5G), VoIP.
-

5. Ad-hoc & Sensor Networks

A. Ad-hoc Networks

- Decentralized, self-configuring (no fixed infrastructure).
- Types:
 - MANET (Mobile Ad-hoc Network): Devices move (e.g., military, disaster recovery).
 - VANET (Vehicular Ad-hoc Network): Cars communicate (V2V - Vehicle-to-Vehicle).

B. Wireless Sensor Networks (WSN)

- Low-power sensors collect & transmit data (e.g., temperature, motion).
 - Use Cases:
 - Environmental monitoring (forest fires, pollution).
 - Industrial IoT (predictive maintenance).
 - Protocols: Zigbee, LoRaWAN, 6LoWPAN.
-

Summary

Topic	Key Takeaway
-------	--------------

WiFi	802.11 ax (WiFi 6) is fastest; OFDMA improves efficiency.
5G	mmWave offers ultra-speed but short range; network slicing enables custom use cases.
Bluetooth	Best for short-range audio & peripherals.
Zigbee	Low-power, mesh networking for smart homes.
NFC	Secure, ultra-short-range (payments, access control).
Mobile IP	Maintains connectivity while roaming.
Ad-hoc Networks	Self-forming, no infrastructure (MANET, VANET).
Sensor Networks	IoT devices collect & transmit data (Zigbee, LoRaWAN).

Lecture: Advanced Networking Topics

1. SDN (Software-Defined Networking)

A. What is SDN?

- Decouples control plane (brains) from data plane (forwarding).

- Centralized controller manages network behavior via software.

B. Key Components

1. Application Layer (Network apps, e.g., load balancing)
2. Control Layer (SDN Controller, e.g., OpenDaylight, ONOS)
3. Infrastructure Layer (Switches/routers with OpenFlow support)

C. How SDN Works

- OpenFlow Protocol: Allows controller to program switches.
- Flow Tables: Rules installed in switches for packet handling.
- Example:
 - A firewall rule can be pushed to all switches centrally.

D. Benefits

- ✓ Network Programmability (Automate configs via APIs)
- ✓ Dynamic Traffic Management (QoS, load balancing)
- ✓ Reduced Vendor Lock-in (Open standards like OpenFlow)

E. Use Cases

- Data Center Networking (Google B4 uses SDN)
 - 5G Network Slicing
 - IoT Traffic Optimization
-

2. Cloud Networking

A. Key Concepts

- Virtualization: VMs, containers share physical resources.
- Overlay Networks: Virtual networks on top of physical (VXLAN, GRE).
- Elasticity: Auto-scaling based on demand.

B. Cloud Service Models & Networking

Service Model	Networking Responsibility	Example
IaaS (AWS EC2)	User manages VMs, networks	Custom VPC setups
PaaS (Azure App Service)	Provider manages OS/network	Focus on app code
SaaS (Gmail)	Fully managed by provider	Zero networking config

C. Major Cloud Networking Services

1. AWS VPC (Virtual Private Cloud)
 - Subnets, Route Tables, Security Groups
2. Azure Virtual Network
 - Network Security Groups (NSGs), Peering
3. Google Cloud VPC
 - Global load balancing, Cloud CDN

D. Challenges

- Latency: Multi-region apps need optimization.
- Security: Shared responsibility model.
- Cost: Egress traffic charges add up.

3. IoT (Internet of Things) Networking

A. IoT Network Stack

Layer	Technologies
Physical	LPWAN (LoRa), Zigbee, BLE
Network	6LoWPAN (IPv6 over Low-Power)
Transport	MQTT, CoAP (UDP-based)
Application	AWS IoT, Azure IoT Hub

B. Key Protocols

1. MQTT (Message Queuing Telemetry Transport)
 - Publish-Subscribe model (lightweight for sensors).
2. CoAP (Constrained Application Protocol)
 - RESTful, runs over UDP (suitable for low-power devices).

C. Challenges

- Security: Weak authentication in many IoT devices.
- Scalability: Billions of devices need efficient protocols.
- Interoperability: Different vendors, standards.

4. Multimedia Networking (VoIP, Streaming)

A. VoIP (Voice over IP)

- Protocols:
 - SIP (Session Initiation Protocol): Sets up calls.
 - RTP (Real-Time Transport Protocol): Carries voice/video.
- QoS Requirements:
 - Latency <150ms, Jitter <30ms, Packet Loss <1%.

B. Video Streaming

1. Adaptive Bitrate Streaming (ABR)
 - Dynamically adjusts quality (e.g., HLS, DASH).
2. CDNs (Content Delivery Networks)
 - Edge servers reduce latency (Akamai, Cloudflare).

C. Technologies

- WebRTC: Browser-based real-time communication.
 - SVC (Scalable Video Coding): Encodes video in layers.
-

5. Blockchain & Networking

A. How Blockchain Uses Networking

- P2P Networks: Nodes propagate transactions (Bitcoin, Ethereum).
- Consensus Protocols:
 - PoW (Proof of Work): Miners compete (high energy use).
 - PoS (Proof of Stake): Validators chosen based on stake.

B. Blockchain for Networking

1. Decentralized Identity (No central CA for certificates).
2. Secure IoT Device Authentication.
3. Smart Contracts for Automated Network Policies.

C. Challenges

- Scalability: Bitcoin processes ~7 TPS vs. Visa's 24,000 TPS.
 - Latency: Block confirmation times (10 mins for Bitcoin).
-

Summary

Topic	Key Takeaway
SDN	Centralized control via OpenFlow; enables programmable networks.
Cloud Networking	VPCs, overlay networks; AWS/Azure/GCP offer scalable solutions.
IoT Networking	LPWAN, MQTT, CoAP for low-power devices; security is a major concern.
Multimedia Networking	VoIP uses SIP/RTP; streaming relies on ABR & CDNs.
Blockchain	P2P networks for decentralization; PoW/PoS consensus mechanisms.

Lecture: Network Troubleshooting & Tools

1. Basic Network Diagnostics Tools

A. Ping (Packet Internet Groper)

- Purpose: Tests reachability & measures round-trip time (RTT).
- How it works:
 - Sends ICMP Echo Request → Waits for Echo Reply.
- Key Flags:
 - `ping -t` (Continuous ping – Windows)
 - `ping -c 5` (Send 5 packets – Linux)

- Interpretation:
 - High latency/packet loss → Network congestion or routing issues.
 - Request timed out → Host down or blocking ICMP.

B. Traceroute (tracert on Windows)

- Purpose: Maps path packets take to reach a destination.
- How it works:
 - Sends packets with increasing TTL (Time-To-Live) values.
 - Each router decrements TTL; when TTL=0, sends ICMP "Time Exceeded".
- Key Flags:
 - `tracert -I` (Use ICMP instead of UDP – Linux)
 - `tracert -d` (Skip DNS resolution – Windows)
- Use Cases:
 - Identify where packets are dropped.
 - Detect routing loops (* * * in output).

C. Netstat (Network Statistics)

- Purpose: Displays active connections, listening ports, and routing tables.
- Key Commands:
 - `netstat -a` (All active connections)
 - `netstat -tuln` (Show listening TCP/UDP ports)
 - `netstat -r` (Routing table)
- Modern Alternatives:
 - `ss` (Linux, faster than netstat)
 - `Get-NetTCPConnection` (PowerShell)

2. Network Scanners

A. Nmap (Network Mapper)

- Purpose: Discovers hosts, services, and vulnerabilities.
- Common Scans:

Command	Description
---------	-------------

<code>nmap -sP 192.168.1.0/24</code>	Ping sweep (find live hosts)
<code>nmap -sS 192.168.1.1</code>	SYN stealth scan (fast, no full TCP handshake)
<code>nmap -sV 192.168.1.1</code>	Version detection (identify OS/services)
<code>nmap -O 192.168.1.1</code>	OS fingerprinting
<code>nmap -A</code>	Aggressive scan (OS, version, scripts)

- - Advanced Features:
 - NSE (Nmap Scripting Engine): Automate vuln checks (e.g., `--script vuln`).
 - Output Formats: `-oX` (XML), `-oN` (normal text).

B. Alternatives to Nmap

- Angry IP Scanner: GUI-based, fast host discovery.
- Masscan: Scans entire Internet in minutes (for research).

3. Bandwidth Monitoring Tools

A. CLI Tools

1. iftop (Linux)
 - Real-time bandwidth usage per connection.
 - Example: `iftop -i eth0` (Monitor eth0 interface).
2. nload (Linux)
 - Displays incoming/outgoing traffic graphs.
3. bmon (Linux/BSD)
 - Advanced interface statistics.

B. GUI Tools

1. Wireshark (Packet-level analysis)
2. PRTG Network Monitor (Enterprise-grade)
3. SolarWinds Bandwidth Analyzer (Historical trends)

C. SNMP-Based Monitoring

- Tools: Cacti, Zabbix.
 - Measures: Interface utilization, errors, discards.
-

4. Packet Analysis with Wireshark

A. Key Features

- Live Capture: Filter traffic on NICs.
- Deep Inspection: Decrypts protocols (if keys provided).
- Display Filters:
 - `http.request.method == "GET"` (Filter HTTP GETs)
 - `tcp.port == 443` (HTTPS traffic)
 - `ip.src == 192.168.1.1` (Packets from specific IP)

B. Common Use Cases

1. Troubleshooting Latency:
 - Check TCP retransmissions (`tcp.analysis.retransmission`).
2. Detecting Malware:
 - Unusual DNS queries or beaconing.
3. VoIP Analysis:
 - Filter RTP streams → Play audio.

C. Advanced Tips

- Color Rules: Highlight suspicious traffic (e.g., TCP SYN scans).
- IO Graphs: Visualize throughput over time.
- Follow TCP Stream: Reconstruct full conversations.

5. Real-World Troubleshooting Flow

Scenario: "Website is Slow"

1. Ping the Server:
 - High latency? → Check routing (`tracert`).
 2. Test Alternate Paths:
 - Use `mtr` (combines ping + `tracert`).
 3. Check Local Services:
 - `netstat -tuln` → Is the web server listening?
 4. Inspect Traffic:
 - Wireshark → Are requests reaching the server?
 5. Monitor Bandwidth:
 - `iftop` → Is the link saturated?
-

Summary Table: Tool Cheat Sheet

Tool	Purpose	Key Command
Ping	Basic connectivity	<code>ping example.com</code>
Traceroute	Path analysis	<code>tracert example.com</code>
Netstat	Connection/port listing	<code>netstat -tuln</code>
Nmap	Network discovery	<code>nmap -sV 192.168.1.1</code>
Wireshark	Packet-level analysis	<code>tshark -i eth0 -Y "http" (CLI)</code>

iftop

Real-time bandwidth

`iftop -i eth0`

Key Takeaways

- Ping/traceroute for basic connectivity.
- Nmap for discovery and vuln scanning.
- Wireshark when you need deep packet inspection.
- Bandwidth tools help identify congestion.