📘 Chapter-1: Introduction to Networking (Detailed Edition)

1.1 What is a Computer Network?

A **computer network** is a collection of computers and electronic devices that are connected to each other for the purpose of communication and resource sharing.

These devices exchange information using **wired** (LAN cable) or **wireless** (Wi-Fi) media.

Key objectives:

- Communication
- Resource Sharing
- Centralized management
- Internet access
- Security and control

1.2 Why Do We Need Networks?

Earlier computers worked like independent machines (standalone).
Networking allows:

Need	Example
File sharing	Google Drive, shared folders
Hardware sharing	Network printers
Internet access	Router + ISP
Communication	Email, VoIP, Zoom
Centralized services	DHCP, DNS, Active Directory

1.3 Characteristics of a Network

A network should provide:

- **Reliability**
- **Performance**
- **Security**

- **Scalability**
- **Manageability**

Example: A bank network must be secure + always available.

1.4 Basic Terminology

Node

Any device connected to the network
(example: PC, laptop, router, server)

Host

Any device that has an IP address.

Every host is a node, but not every node is a host.

Transmission Medium

The physical or wireless path where data travels.

- Copper cable
- Fiber optics
- Wi-Fi signals

Bandwidth

Maximum data a medium can carry (per second).

Latency

Time taken for data to travel.

1.5 Types of Networks

LAN (Local Area Network)

- Limited area (building/floor)
- Example: College campus, home network

MAN (Metropolitan Area Network)

- Connects multiple LANs inside a city

WAN (Wide Area Network)

- Covers large geographical areas
- Example: Internet

WLAN (Wireless LAN)

- Wireless version of LAN
- Wi-Fi

1.6 Client–Server vs Peer-to-Peer

Client–Server

Clients request → Server responds
Used in companies

Example:

- DNS
- DHCP
- Web Server
- Mail Server

Peer-to-Peer

No dedicated server, devices communicate directly
Used at homes or small networks

Example:

- Bluetooth sharing
- File sharing among laptops

1.7 Network Devices

Category	Devices
Passive (no intelligence)	Cables, connectors, patch panel
Active (intelligent devices)	Router, switch, firewall
Wireless devices	Access point, wireless controller

Category	Devices
Security devices	IDS, IPS, Firewall, Proxy

What active devices actually do?

- Make routing decisions
- Forward traffic
- Filter packets
- Apply security rules

1.8 OSI Reference Model

OSI = Open Systems Interconnection

A conceptual model by ISO that explains **how communication happens** between two devices in a network.

It has **7 layers**, each providing a specific role.

Layer	Example
Application	HTTP, DNS
Presentation	Encryption
Session	Session establishment
Transport	TCP, UDP
Network	IP
Data-Link	MAC
Physical	cable, signals

👍 we will study each layer in depth in OSI chapter.

1.9 What is a Protocol?

A protocol is a **rule-set** that defines how two devices will communicate.

Example protocols:

- DNS (Domain Name)

- DHCP (IP assignment)
- HTTP (web browsing)
- SSH (secure login)
- TCP/UDP (transport)
- IP (addressing)

Example:
HTTP defines how webpages are requested and delivered.

1.10 How Data Travels

When you open a website:

1. Browser requests information
2. DNS converts name into IP
3. Router forwards request to internet
4. Server sends webpage data
5. Browser displays it

1.11 Real Life Example

PC → Switch → Router → Firewall → Internet

Every step has a protocol working in the background.

1.12 Revision Points

✓ Network = connection between computers
✓ LAN = inside building
✓ WAN = long distance (Internet)
✓ Protocol = communication rules
✓ OSI = communication model

1.13 Interview Points

- A computer network allows devices to communicate and share resources.

- LAN operates in a limited area like home or office.
- WAN covers large geographical distance using ISP.
- Protocols define communication rules.
- OSI is a reference model with 7 layers.

🌐 Chapter 2 — Network Models (OSI & TCP/IP)

Networks follow structured models so devices from different vendors can communicate smoothly.
The two most widely used models are:

- **OSI Model (Open Systems Interconnection Model)**
- **TCP/IP Model (Transmission Control Protocol / Internet Protocol Model)**

⭐ OSI Model (7 Layers)

OSI model divides networking functions into **7 layers**, each having specific roles.

Layer No.	Layer Name	Function (Short)
7	Application	Services used by users (HTTP, SMTP, FTP)
6	Presentation	Encryption, compression, formatting
5	Session	Session creation & control
4	Transport	Reliable delivery, segmentation
3	Network	IP addressing, routing
2	Data Link	MAC addressing, switching
1	Physical	Bits, cables, signals

📌 Layer-wise explanation (easy detailed)

Layer 7 - Application Layer

- Provides network services to the **end user**
- Example protocols

    - HTTP (Hyper Text Transfer Protocol)
    - HTTPS (Secure HTTP)
    - SMTP (Simple Mail Transfer Protocol)
    - FTP (File Transfer Protocol)

Layer 6 - Presentation Layer

Handles:

- Data encoding
- Data encryption
- Data compression

Eg:

- JPEG
- GIF
- SSL/TLS (Secure Socket Layer / Transport Layer Security)

Layer 5 - Session Layer

Responsible for:

- Establish session
- Manage session
- Terminate session

Example:

- Session between browser & server

Layer 4 - Transport Layer

Main jobs:

- Segmentation
- Flow control
- Error control

Protocols:

- **TCP** (Transmission Control Protocol)
- **UDP** (User Datagram Protocol)

Layer 3 - Network Layer

Functions:

- Logical addressing (**IP addresses**)
- Routing the packets

Devices:

- Router
- Layer-3 Switch

Protocol examples:

- **IPv4**
- **IPv6**
- ICMP (Internet Control Message Protocol)

Layer 2 - Data Link Layer

Handles:

- MAC addressing
- Frame creation

Sub-layers:

- LLC
- MAC

Device examples:

- Switch
- Bridge

Addressing:

- MAC (Media Access Control)

Layer 1 - Physical Layer

Deals with:

- Bits (0 and 1)
- Cables
- Signals
- Connectors

Examples:

- Ethernet cable
- Fiber optic cable

🔶 **TCP/IP Model (4 Layers)**

Internet uses TCP/IP model in real world.

TCP/IP Layer	OSI Equivalent	Function
Application	7,6,5	Email, Web, FTP
Transport	4	TCP/UDP
Internet	3	IP routing
Network Access	2,1	LAN communication

✨ **Why TCP/IP is used?**

- Practical implementation
- Real-world communication
- Foundation of Internet
- Supported by everything!

🔥 **Key Differences (OSI vs TCP/IP)**

OSI	TCP/IP
7 Layers	4 Layers
Theoretical	Practical
Developed by ISO	Developed by DoD
Protocol independent	Protocol + implementation

💡 **Example IP Packet Travel (Simple flow)**

Browser → Application layer
↓
Transport Layer (TCP)
↓
Internet Layer (IP)
↓
Network Access (Ethernet frame)
↓
Physical (Actual signal on cable)

🌐 **Chapter 3 — IP Addressing (IPv4 & IPv6 Basics)**

3.1 What is an IP Address?

An **IP Address (Internet Protocol Address)** is a unique logical address assigned to every device in a network so that communication can happen.

Example IPv4:

192.168.10.5

Example IPv6:

2001:0db8:85a3::8a2e:0370:7334

3.2 Why we need IP

Without an IP address:

- devices cannot identify each other,

- packets cannot reach destination,
- routing is impossible,
- internet access cannot happen.

3.3 Types of Addresses

Type	Meaning	Example
IPv4	32-bit	192.168.1.10
IPv6	128-bit	fe80::1

🔹 **IPv4 (Internet Protocol v4)**

- 32-bit address
- written in decimal
- divided in 4 octets:

192 . 168 . 10 . 25

Each octet = 8 bits
4×8 = 32 bits total

3.4 Classes of IPv4

IPv4 addresses are grouped into classes based on range.

Class	Range	Usage
A	1–126	Large networks
B	128–191	Medium
C	192–223	Small
D	224–239	Multicast
E	240–255	Research

Example:

Class C → 192.168.1.10

3.5 Private vs Public IP

Private IP

Used inside LAN

10.x.x.x

172.16.x.x – 172.31.x.x

192.168.x.x

Public IP

Used on Internet, unique globally.

Public IP is provided by ISP.

3.6 Subnet Mask

Subnet mask decides which part of IP is:

- Network part
- Host part

Example:

255.255.255.0

means first 3 octets = network
last octet = host

3.7 CIDR (Classless Inter-Domain Routing)

CIDR represents subnet mask in short form

Example:

192.168.10.1/24

/24 → means 24 bits are network bits
subnet mask = 255.255.255.0

3.8 Default Gateway

A default gateway is the router through which packets exit the LAN and reach external networks.

Example:

PC IP: 192.168.1.20

Gateway: 192.168.1.1

3.9 DNS (Domain Name System)

DNS converts domain names into IP addresses.

Example:

google.com → 142.250.182.14

Without DNS, we would type IPs instead of names.

3.10 DHCP (Dynamic Host Configuration Protocol)

DHCP automatically assigns:

- IP address
- subnet mask
- gateway
- DNS

Without DHCP we would assign manually.

3.11 How IPv4 Address Works in LAN

➞ PC uses IP address
➞ switch uses MAC address
➞ router uses IP + routing
➞ gateway forwards traffic
➞ DNS resolves names
➞ DHCP assigns details

This creates end-to-end communication.

⭐ Quick Summary

- IPv4 = 32 bit
- private IP ranges = 10.x, 172.16–31, 192.168.x
- gateway connects LAN to Internet
- DNS resolves names
- DHCP assigns IP automatically

🌐 Chapter-4 — Subnetting (Easy & Detailed)

⭐ 4.1 What is Subnetting?

Subnetting means dividing a large network into smaller logical networks called **subnets**.

Example:

192.168.1.0/24 → split into small networks:

192.168.1.0/26

192.168.1.64/26

192.168.1.128/26 etc.

Why?

- better management
- security
- performance
- isolation
- avoid broadcast flooding

⭐ 4.2 Need of Subnetting

Without subnetting:

- too many hosts in one network
- broadcast storms

- performance drops
- no security segmentation
- routing becomes complex

⭐ 4.3 IP Address Structure

IPv4 = **32 bits**
Example:

192.168.50.10

Binary form:

11000000.10101000.00110010.00001010

Each part = 8 bits = **octet**

⭐ 4.4 Subnet Mask

Subnet mask tells how many bits are **Network** vs **Host**

Example:

255.255.255.0

Binary:

11111111.11111111.11111111.00000000

Number of 1's = network bits
Number of 0's = host bits

⭐ 4.5 CIDR Notation

CIDR = Classless Inter-Domain Routing

Written as "/" value:

/24

means 24 network bits.

/24 = 255.255.255.0
/25 = 255.255.255.128
/26 = 255.255.255.192

⭐ 4.6 Block Size Formula

Block size = **256 minus subnet mask value**
(example fourth octet mask)

Example:

/26 = 255.255.255.192

Block size = 256 – 192 = 64

So networks increase as:

0, 64, 128, 192

⭐ 4.7 Finding Network ID

Find the block your IP falls into.

Example:

192.168.10.50/26

Block = 64
Range:

0-63

64-127

128-191

192-255

50 belongs to **0-63**
So Network ID:

192.168.10.0

⭐ 4.8 Finding Broadcast ID

Just pick last number of that block:

192.168.10.63

⭐ 4.9 Usable Host Range

Remove first & last address:

192.168.10.1 to 192.168.10.62

⭐ 4.10 Example-2

10.10.10.73/29

/29 = 255.255.255.248
Block = 256 – 248 = 8

Blocks:

0,8,16,24,...,72,80

73 belongs to:

72-79

Network ID:

10.10.10.72

Broadcast ID:

10.10.10.79

Usable:

73–78

⭐ 4.11 Example-3

172.16.200.130/25

/25 = 255.255.255.128
Block = 128

Block ranges:

0–127

128–255

130 belongs in:

128–255

Network:

172.16.200.128

Broadcast:

172.16.200.255

Usable:

129–254

⭐ 4.12 Classful vs Classless

Classful → uses class A/B/C rule
Classless → uses /value (CIDR)

Modern networks use Classless only.

⭐ 4.13 Practice Rules

Always follow these steps:

1. Convert CIDR to Mask
2. Find block size
3. Divide into ranges
4. Find where IP lies
5. First = Network
6. Last = Broadcast
7. Remove first/last to get usable range

⭐ 4.14 Quick Table (must memorize)

CIDR	Mask
/24	255.255.255.0
/25	255.255.255.128
/26	255.255.255.192
/27	255.255.255.224

CIDR	Mask
/28	255.255.255.240
/29	255.255.255.248
/30	255.255.255.252

⭐ 4.15 Where is /30 used?

Used between routers (point to point links)
Because only 2 IPs are needed
(one for each router)

⭐ 4.16 Quick Revision

✓ Subnetting = divide network
✓ CIDR = /value
✓ Network ID = first
✓ Broadcast = last
✓ usable = between

🌐 Chapter-5 — Routing Basics (Very Clear & Beginner-Friendly)

Routing is one of the MOST important parts of networking.

⭐ 5.1 What is Routing?

Routing is the process of sending a packet from **one network** to **another network** using routers.

Example:

PC (192.168.1.10) → Router → Internet (8.8.8.8)

Routing decides:

- best path
- according to routing table
- based on routing protocols

⭐ 5.2 Why do we need routing?

Inside same network, communication happens via **switch + MAC**
Between different networks → routing required

Example:

VLAN 10 → VLAN 20

Needs routing.

⭐ 5.3 Static Routing

Routes are entered manually

Example Cisco:

ip route 192.168.10.0 255.255.255.0 10.0.0.2

Pros:

- simple
- secure
- predictable

Cons:

- manual
- not scalable

Used in:

- small networks
- labs
- branch connectivity

⭐ 5.4 Dynamic Routing

Routers learn routes automatically using protocols:

- RIP
- EIGRP

- OSPF
- BGP

Advantages:

- automatic
- scalable
- auto failover

⭐ 5.5 Types of Routing Protocols

Category	Protocols
Distance Vector	RIP, EIGRP (partly)
Link State	OSPF
Path Vector	BGP

⭐ 5.6 Distance Vector Routing

Uses **distance** (hop count) + **vector (direction)**

Example: RIP

Characteristics:

- slower
- periodic updates
- no complete topology knowledge

Routers do NOT know the entire network map.
Only know next-hop.

⭐ 5.7 Link State Routing

Routers exchange **LSA (Link State Advertisements)** and build **full network topology map** called **LSDB (Link State Database)**

Example: OSPF

Features:

- fast convergence
- smarter path selection
- scalable
- used in enterprise

⭐ 5.8 Path Vector Routing

Used between different organizations/ISPs via Internet

Example: BGP

Used in:

- ISP networks
- Internet backbone
- Data centers

⭐ 5.9 Convergence

Convergence means all routers agree on best paths.

Fast convergence = fast route changes
Slow convergence = outage during failure

⭐ 5.10 Administrative Distance (AD)

AD = trust level of routing protocol
Lower = more preferred

Protocol	AD
Connected	0
Static	1
EIGRP	90
OSPF	110
RIP	120

Higher AD = less preferred.

⭐ 5.11 Routing Table (show ip route)

Example:

C 192.168.1.0/24 is directly connected

S 10.10.10.0/24 via 10.0.0.2

O 172.16.0.0/16 via 10.0.0.5

C = Connected
S = Static
O = OSPF

⭐ 5.12 Router Packet Flow

1. Packet arrives
2. Router checks destination IP
3. Looks in routing table
4. Selects best route
5. Forwards to next-hop router
6. Packet finally reaches destination

⭐ Quick Revision

- Routing = between networks
- Static = manual
- Dynamic = automatic
- DV = simple but slow (RIP)
- LS = smart & fast (OSPF)
- AD = protocol priority
- Routing table decides everything

🌐 Chapter-6 — Switching Basics (Mumbai-Tapri level easy 😄)

Switching is all about **local communication** inside LAN using **MAC addresses**.

⭐ 6.1 What is Switching?

Switching is forwarding frames inside the **same network**, based on **MAC address**, using a **Switch**.

Example:

PC1 → Switch → PC2 (same network)

No router required.

⭐ 6.2 How Switch learns MAC addresses (CAM Table)

A switch stores MAC addresses in a table called **CAM (Content Addressable Memory)** table.

When switch receives a frame:

- it reads the **Source MAC**
- stores it along with the port number

Example:

MAC 00:A1:B2 → Fa0/1

So now switch knows which device is on which port.

⭐ 6.3 Frame Forwarding (VERY important)

When sending a frame, switch checks Destination MAC in the CAM table:

If MAC exists → Forward to correct port

If MAC unknown → Flood to all ports except incoming

⭐ 6.4 CAM Table Entries

CAM entry contains:

- MAC address

- Port number
- VLAN
- Age timer

Example:

Switch# show mac address-table

⭐ 6.5 Switching vs Routing

Switching	Routing
Uses MAC	Uses IP
Layer 2	Layer 3
Switch	Router
Local network	Between networks
Faster	Slightly slower

⭐ 6.6 Types of Switches

Layer-2 Switch

- basic switching
- supports VLAN
- used inside network

Layer-3 Switch

- can do routing also
- used in big networks
- Inter-VLAN routing
- supports OSPF, EIGRP

⭐ 6.7 Switch Port Types

Access Port

Used for end devices
Belongs to **one VLAN**

Example:

PC

Laptop

Printer

Command:

switchport mode access

Trunk Port

Carries multiple VLANs between switches

Command:

switchport mode trunk

Protocols:

- IEEE 802.1Q (standard)
- ISL (Cisco old)

⭐ 6.8 When do we need a Router?

Only when:

- networks are different
- VLANs need communication
- Internet access

Example:

VLAN10 → VLAN20 (needs routing)

⭐ 6.9 Broadcast Domain

Broadcast packets stay inside **same VLAN** only

Meaning:

- VLAN10 broadcast won't reach VLAN20

That is why VLAN increases security.

⭐ 6.10 Collision Domain

Every switch port = separate collision domain
(no collisions like hubs)

⭐ 6.11 STP (short intro)

When switches have multiple links → loop occurs
STP avoids loops by blocking extra links

(STP full chapter later)

⭐ 6.12 Switch Performance Advantages

✓ fast forwarding
✓ low latency
✓ isolation via VLANs
✓ full-duplex support
✓ loop protection

⭐ Quick Revision

- switching uses MAC
- router uses IP
- access ports for end devices
- trunk ports for switch-to-switch
- CAM table stores MAC
- unknown destination = Flood
- VLAN = isolation

🌐 Chapter-7 — VLAN (Virtual LAN) – explained slowly & clearly

---

⭐ 7.1 What is VLAN?

VLAN = **Virtual Local Area Network**

It logically divides **one physical LAN** into **multiple logical LANs**.

Example:

One switch → Multiple departments

Departments:

- HR
- Finance
- IT
- Accounts

Each can be a separate VLAN even though physically they are on the **same switch**.

⭐ 7.2 Why VLAN?

Because without VLAN, everything in one network causes:

- broadcast storms
- no isolation
- no security
- heavy traffic
- unnecessary communication

VLAN solves all of those.

⭐ 7.3 VLAN Benefits

Benefit	Explanation
Security	Separate departments

Benefit	Explanation
Performance	Reduced broadcast
Easy management	Move devices without rewiring
Scalability	Large networks
Flexible	Logical not physical

⭐ 7.4 VLAN = Separate Broadcast Domain

Broadcast of VLAN10 won't reach VLAN20
This is very important.

⭐ 7.5 VLAN ID Range

Type	Range
Normal	1-1001
Extended	1006-4094
Reserved	1002-1005

⭐ 7.6 Types of VLANs

Type	Based on	Example
Static	Port	Fa0/5 → VLAN10
Dynamic	MAC	MAC→VLAN mapping

static = most used
dynamic = rare (VMPS)

⭐ 7.7 Access Port

Belongs to **one VLAN**
Used for:

- PC

- Laptop
- Printer
- server

Command:

switchport mode access

switchport access vlan 10

⭐ 7.8 Trunk Port

Allows multiple VLANs through **one uplink**

Example:

Switch ↔ Switch

Switch ↔ Router

Command:

switchport mode trunk

Protocol:

- 802.1Q (industry standard)

⭐ 7.9 Native VLAN

Traffic which is **untagged** uses the native VLAN.
Default = VLAN1
Security best practice = change it.

⭐ 7.10 Inter-VLAN Routing

Devices in different VLANs cannot talk directly,
Example:

HR (VLAN10) ≠ Finance (VLAN20)

So we need:

- Router
- OR Layer-3 Switch

⭐ 7.11 VLAN Example (simple)

Switch Ports:

1-6 → VLAN10

7-12 → VLAN20

13-20 → VLAN30

Even though on same switch:

- VLAN10 is isolated from VLAN20
- VLAN20 isolated from VLAN30

⭐ 7.12 Real-life Example

College:

- Students VLAN
- Staff VLAN
- Admin VLAN
- Server VLAN

Companies:

- HR VLAN
- Accounts VLAN
- CCTV VLAN
- Server VLAN

⭐ 7.13 How VLAN improves security?

If someone plugs laptop in HR port,
he is inside HR VLAN but cannot access Finance VLAN.

This reduces insider abuse.

⭐ 7.14 Concept Diagram

[Switch]

┌──VLAN10──┐

└──VLAN20──┘

⭐ 7.15 VLAN tagging

Trunk link adds a **small header (tag)** which mentions VLAN ID.

So switch knows which packet belongs to which VLAN.

802.1Q tag is inserted into Ethernet frame.

⭐ 7.16 VLAN Table (important)

Field	Meaning
VLAN ID	10
Name	HR
Assigned Ports	Fa0/1-6

⭐ Quick Revision

- VLAN logically separates LAN
- Access ports = one VLAN
- Trunk = multiple VLAN
- VLAN reduces broadcast
- VLAN = security + flexibility
- Native VLAN = untagged traffic

🔐 Chapter-8 — LAN Security Basics (Port Security, DHCP Snooping, DAI)

⭐ 8.1 Why LAN Security?

Even inside an organization, users might:

- plug personal laptop
- start rogue server
- run hacking tools
- steal data
- sniff packets
- do man-in-the-middle attacks

LAN Security prevents this.

⭐ 8.2 Port Security (Layer-2 Security)

Port Security prevents unauthorized devices from connecting to switch ports.

How?
By controlling **MAC addresses** allowed on a port.

Command:

switchport port-security

Rules:

- if unknown MAC connects → block
- if attackers connect laptop → port shut down

8.2.1 Allowed MAC

You can set:

- exact MAC
- maximum number of MAC
- sticky MAC (auto-learn)

Example:

switchport port-security mac-address sticky

8.2.2 Violation options

Mode	Meaning
Protect	Drop silently
Restrict	Drop + log
Shutdown	Port down

Most common → shutdown.

8.2.3 Used on:

- access ports
- HR VLAN
- Finance VLAN
- critical departments

⭐ 8.3 DHCP Snooping

Prevents **fake DHCP servers** (attacker laptops) from giving wrong gateway/DNS.

Idea:

- mark trusted ports only
- block all DHCP replies from untrusted

Trusted port = connected to real DHCP server
Untrusted port = users

DHCP snooping builds **binding table**:

- MAC
- IP
- VLAN
- Port

⭐ 8.4 Dynamic ARP Inspection (DAI)

DAI stops **ARP Spoofing / ARP Poisoning**.

Meaning:

- attacker cannot fake gateway MAC
- cannot perform man-in-the-middle attack

DAI checks ARP packets against DHCP binding table.

⭐ 8.5 IP Source Guard

Blocks IP spoofing by validating:

- IP address
- MAC address
- Port

If device sends traffic claiming different IP → blocked.

⭐ 8.6 Putting it Together

LAN security workflow:

Port security → blocks unknown devices

DHCP snooping → blocks fake DHCP servers

DAI → blocks ARP poisoning

IP Source Guard → blocks IP spoofing

⭐ 8.7 Real attacks Prevented

- ARP poisoning
- MITM
- Rogue DHCP
- IP spoofing
- VLAN hopping (partially)

⭐ 8.8 Security is at Layer-2 (IMPORTANT)

LAN security is done at **switch**, not router.

Switch handles:

- MAC address
- DHCP frames
- ARP packets

Router handles IP layer only.

⭐ **Quick Revision**

- Port Security = limit MAC
- DHCP Snooping = block fake DHCP
- DAI = protect ARP
- Source Guard = stop IP spoofing

🌐 **Chapter-9 — Switching Protocols (STP, RSTP, PVST, EtherChannel)**

⭐ **9.1 Why switching protocols exist?**

In networks with multiple switches, we normally create **redundant links** for backup.

Example:

SW1——SW2

| |

└——————┘

These extra links create **layer-2 loops**.

Effects of loop:

- broadcast storm
- MAC table instability
- duplicate frames
- network collapse

Switches cannot detect loops automatically → STP handles it.

🔵 9.2 STP — Spanning Tree Protocol

Developed by IEEE **802.1D**

Main job:
✓ Detect loops
✓ Block extra links
✓ Allow only one active path

So **only one path is forwarding**, others are in blocking state.

🔵 9.3 STP Ports

Each switch port gets a state:

- Blocking
- Listening
- Learning
- Forwarding

Blocking = no traffic
Forwarding = active path

🔵 9.4 Root Bridge

STP creates a **Root Bridge**
(one main switch)

Rules:

- lowest Bridge ID becomes Root
- Admin can force a root

All paths are calculated relative to Root Bridge.

🔵 9.5 Root Port

On every NON-root switch:

- the port with least cost towards root becomes **Root Port**

🟣 9.6 STP Cost

Cost = inversely proportional to bandwidth

Speed	Cost
10Mbps	100
100Mbps	19
1Gbps	4
10Gbps	2

Shortest cost wins.

🟣 9.7 STP Problems

STP is slow:
Convergence time = **30–50 seconds**

Too slow for modern networks.

🟢 9.8 RSTP — Rapid Spanning Tree Protocol

RSTP = Rapid version of STP

Fast convergence:

- few seconds only

IEEE 802.1w

Use this instead of old STP.

🟢 9.9 PVST and PVST+ (Cisco)

PVST = Per-VLAN Spanning Tree
Every VLAN runs **its own STP instance**

Cisco feature.

More control, more load.

PVST+ new version.

🟦 9.10 MST (Multiple Spanning Tree)

MST groups multiple VLANs into a single STP instance.

Used in large networks.
Reduces overhead.

🔵 9.11 EtherChannel (important!)

EtherChannel is NOT STP.

But works WITH STP.

EtherChannel bundles multiple physical links into **one logical link**.

Example:

interface range fa0/1 - fa0/4

channel-group 1 mode on

Benefits:

- more bandwidth
- redundancy
- STP sees it as a single link (less chance of loops)

Protocols:

- LACP (IEEE 802.3ad)
- PAgP (Cisco)

⭐ Quick Revision

Protocol	Full Form	Speed
STP	Spanning Tree Protocol	slow
RSTP	Rapid STP	fast
PVST	Per VLAN STP	every VLAN
EtherChannel	link aggregation	bandwidth

After Switching, next:

Routing Protocols (OSPF + EIGRP) in detail

- LSAs
- metrics
- neighbor table
- topology table
- routing table
- packet types
- states
- area design

🌐 Chapter-10 — Routing Protocols

(OSPF + EIGRP explained like a story 😌)

⭐ 10.1 What are Routing Protocols?

Routing protocols allow routers to **automatically learn networks**, calculate **best paths**, and **update each other** when changes happen.

Examples:

- RIP
- OSPF
- EIGRP
- BGP

⭐ 10.2 Why dynamic routing?

Without dynamic routing:

- every route must be manually added
- impossible in large networks
- no auto failover

- no scalability

Dynamic routing automatically handles:
✓ multiple paths
✓ failures
✓ topology change
✓ network expansion

⭐ 10.3 Two main types

Type	Examples
Distance Vector	RIP, EIGRP (partial)
Link State	OSPF

⭐ 10.4 Distance Vector

- routers send full routing table periodically
- slow convergence
- used in small networks
- “vector = direction”
- “distance = hop count”

Example: RIP

⭐ 10.5 Link State

Routers exchange **link state information**
(not full routing tables)

They build a **complete map** of the entire network called **LSDB (Link State Database)**.

Main Link State protocol = **OSPF**

🌟 EIGRP (Enhanced Interior Gateway Routing Protocol)

Cisco’s hybrid routing protocol
(distance vector + link state features)

Benefits:

- Fast
- Efficient
- Supports multiple metrics:
  ✓ bandwidth
  ✓ delay
  ✓ load
  ✓ reliability

EIGRP tables:

- Neighbor table
- Topology table
- Routing table

🍀 10.6 OSPF (Open Shortest Path First)

Industry standard,
supported by all devices

OSPF uses:

- LSAs (Link State Advertisements)
- Areas
- SPF algorithm (Shortest Path First = Dijkstra algorithm)
- metric based on cost

⭐ OSPF works like this:

1️⃣ Routers form **neighbors**
2️⃣ Exchange **LSAs**
3️⃣ Build **LSDB (database)**
4️⃣ SPF calculation
5️⃣ Best path selected
6️⃣ populated into routing table

🍀 Terminology list (very important)

Name	Full Form	Meaning
SPF	Shortest Path First	routing calculation
LSA	Link State Advertisement	link details
LSDB	Link State Database	full topology
DR	Designated Router	central in broadcast network
BDR	Backup Designated Router	backup of DR

🌼 OSPF Area

OSPF divides networks into areas
(for stability)

Default area = area 0 (backbone)

Big networks = multiple areas for scalability.

⭐ OSPF Packet Types

1 Hello
2 DB Description
3 Link State Request
4 Link State Update
5 Link State Ack

⭐ Neighbor States

OSPF goes through 7 states when forming adjacency:

- Down
- Init
- 2-way
- ExStart
- Exchange

- Loading
- Full

⭐ **DR/BDR election**

In LAN:

- one router becomes DR
- second becomes BDR
- others are DROTHERS

This reduces traffic

⭐ **OSPF Cost**

Based on bandwidth

Cost = 10^8 / bandwidth

Higher bandwidth → lower cost = better path

⭐ **Quick Revision**

- RIP = distance vector
- OSPF = link state
- EIGRP = hybrid
- LSAs build LSDB
- SPF selects best path
- DR/BDR reduce traffic
- OSPF uses areas
- cost = bandwidth metric

🔥 **Chapter-11 — NAT, PAT, ACL & Firewall Basics**

This is where LAN meets Internet and firewall meets router.

🌐 11.1 NAT (Network Address Translation)

NAT converts **private IPs** into **public IP** so local devices can access the Internet.

Example:
PC:

192.168.1.10

Router NATs it to:

106.22.5.90 (public)

🌐 11.2 Why NAT exists?

Because IPv4 addresses are LIMITED.
Private IPs are reused everywhere.

NAT saves IPv4 by using **one public IP** for many internal devices.

🌐 11.3 Types of NAT

Type	Meaning
Static NAT	One Private ↔ One Public
Dynamic NAT	Pool of IPs
PAT	Many Private ↔ One Public

📦 Static NAT

1 Private ↔ 1 Public
Used for servers that must be accessible from outside.

Example:

Web server behind firewall → static NAT

📦 Dynamic NAT

Pool of Public IPs available
(local clients pick dynamically)

Used by big organizations.

🧨 PAT (Port Address Translation) – MOST IMPORTANT

PAT = Many internal clients share **one public IP**, router uses **unique port numbers**.

Also called **NAT Overload**.

Example:

3 PCs use same public IP → router uses different port mapping

This is how **home WiFi routers** work.

🌐 11.4 Private vs Public IP

Private IP ranges
✓ 10.0.0.0 – 10.255.255.255
✓ 172.16.0.0 – 172.31.255.255
✓ 192.168.0.0 – 192.168.255.255

Public IP = provided by ISP

🔥 11.5 ACL (Access Control Lists)

ACL filters network traffic based on:

- IP
- port number
- protocol

ACL used in:

- security
- routing
- firewall

Example:
Block traffic from:

192.168.1.30

🔐 ACL types

ACL	Meaning
Standard	Filters by IP only
Extended	IP + Port + Protocol

Extended ACL = more secure.

🔐 ACL Placement

Standard ACL → near destination
Extended ACL → near source

Rule (Cisco famous rule):

Place the filter where it has most impact

🔥 11.6 Firewall

Firewall controls:

- what enters the network
- what leaves the network

Firewall performs:

- Filtering
- NAT
- VPN
- IDS/IPS
- Threat protection

Examples:

- Cisco ASA
- Palo Alto
- Fortigate
- CheckPoint

🧠 **Firewall decision based on:**

- Source IP
- Destination IP
- Port number
- Application
- Protocol
- User identity

🔥 **Security Example**

Blocked:

- Internet FTP inbound
- Telnet inbound
- HTTP inbound

Allowed:

- HTTPS outgoing
- DNS outgoing
- SSH internal

⭐ **Quick Revision**

- NAT = convert private to public
- PAT = many to one
- ACL = filtering
- Firewall = main network security
- private ranges = 10, 172, 192

📡 **Chapter-12 — Wireless Networking & Wireless Security**

⭐ 12.1 What is WLAN?

WLAN = **Wireless Local Area Network**

Networking using:

- Radio signals instead of cables.

Example:

Wi-Fi at home

Wi-Fi in college

Wi-Fi hotspot

⭐ 12.2 Wireless Access Point (AP)

Access Point creates wireless coverage so devices can connect to the network wirelessly.

AP = wireless switch

⭐ 12.3 SSID (Service Set Identifier)

SSID = Wi-Fi network name.

Example:

HomeWiFi

Shravani-5G

College_Lab

Hidden SSID = AP broadcasting name is disabled.

⭐ 12.4 Wireless Channels

Wireless uses channels instead of cable frequency.

2.4 GHz band channels:
1,6,11 (non-overlapping)

5 GHz = higher speed, less range.

⭐ 12.5 AP Modes

Mode	Meaning
Autonomous AP	Works independently
Lightweight AP	Controlled by WLC
Repeater AP	Extends range
Workgroup Bridge	Converts wired device to wireless

Enterprise uses **WLC (Wireless LAN Controller)**.

⭐ 12.6 BSSID

Each SSID has a BSSID (MAC address) of AP radio.

🔒 Wireless Security

⭐ 12.7 WEP (Wired Equivalent Privacy)

- First wireless encryption
- Weak
- easily crackable
- NEVER use

⭐ 12.8 WPA (Wi-Fi Protected Access)

- Better than WEP
- Still weak for modern attacks
- Can be cracked using brute force

⭐ 12.9 WPA2

- Uses AES encryption
- Standard for many years

- Strong but vulnerable to KRACK attacks

⭐ 12.10 WPA3 (Latest)

- Strongest today
- Protects against brute force
- Better encryption
- Mandatory in new devices

🧠 Enterprise Wireless Authentication

Type	Meaning
WPA2-Personal	Password based (home use)
WPA2-Enterprise	Authentication via Server

Enterprise uses:

- RADIUS (Remote Authentication Dial-In User Service)
- 802.1X authentication

🔥 Wireless Attacks (important for cyber)

- Deauthentication attack
- Fake AP attack
- Evil Twin attack
- Captive portal phishing
- WPA handshake capture
- WPA2 cracking
- MITM over Wi-Fi
- WPS brute force

Tools:

- aircrack-ng

- Wireshark
- bettercap
- Kismet

⭐ 12.11 2.4GHz vs 5GHz Comparison

Feature	2.4GHz	5GHz
Speed	Slow	Fast
Range	High	Medium
Interference	More	Less
Channels	Few	Many

⭐ Quick Revision

- AP creates Wi-Fi
- SSID is Wi-Fi name
- WPA3 is recommended
- WEP is useless
- 5 GHz = faster
- Wireless requires security
- Most attacks target Wi-Fi

🌐 Chapter-13 — IPv6 (Internet Protocol version 6)

⭐ 13.1 What is IPv6?

IPv6 is the **new version of Internet Protocol** created to replace IPv4 because IPv4 addresses are almost finished.

IPv6 has **128-bit addresses**, compared to IPv4's **32-bit**.

⭐ 13.2 IPv6 Address Example

2001:0db8:85a3:0000:0000:8a2e:0370:7334

Shortened:

2001:db8:85a3::8a2e:370:7334

⭐ 13.3 IPv6 Notation

IPv6 uses:

- Hexadecimal digits
- Colons (:)
- Groups of 4 hex numbers
- 8 groups total

Each group = 16 bits
8 groups × 16 = **128 bits**

⭐ 13.4 Why IPv6?

IPv4 addresses are almost exhausted.

IPv6 provides:

- huge addressing space
- 340 undecillion addresses 😄

⭐ 13.5 IPv6 Advantages

✓ No NAT required
✓ Auto-configuration possible
✓ Simplified header
✓ Built-in security (IPsec)
✓ Practically unlimited addresses

⭐ 13.6 Types of IPv6 Addresses

🔹 **Unicast**

One-to-one communication
(Like IPv4 normal address)

🔹 **Multicast**

One-to-many communication

🔹 **Anycast**

One-to-nearest server
Used heavily in cloud + DNS services

Example:
Google DNS anycast IPv6:

2001:4860:4860::8888

⭐ **13.7 IPv6 Address Types (very important)**

Type	Prefix
Global Unicast	2000::/3
Link Local	FE80::/10
Unique Local	FC00::/7

🔹 **Link-Local Address**

Automatically assigned
Used inside LAN only
Starts with:

fe80::

Equivalent to APIPA in IPv4

🔹 **Global Unicast**

Globally routable
Equivalent to public IPv4

Example:

2001:db8::/32

🔹 **Unique Local**

Used inside private networks
Equivalent to private IPv4

Starts with:

fc00::

⭐ **13.8 IPv6 Security**

IPv6 was designed with **IPsec (IP Security)** as built-in support.

IPv4 added security later, IPv6 has it in design.

⭐ **Quick Revision**

✓ IPv6 = 128-bit
✓ Uses hexadecimal
✓ No NAT needed
✓ Types = unicast, multicast, anycast
✓ Link local starts with FE80
✓ Global unicast = internet routable

🌐 **Chapter-14 — Network Protocols (DNS, DHCP, ARP, ICMP)****

⭐ **14.1 DNS (Domain Name System)****

DNS converts domain names into IP addresses.

Example:

google.com → 142.250.182.14

Without DNS, we would type IPs instead of URLs.

🔹 **DNS Process (simple)**

1. User enters **google.com**
2. Browser sends query to DNS resolver
3. Resolver asks root server
4. Then TLD (.com)
5. Then authoritative server
6. IP returned to browser

🔹 **DNS Ports**

- UDP 53
- TCP 53

🔹 **DNS Record Types**

Type	Meaning
A	Domain → IPv4
AAAA	Domain → IPv6
MX	Mail server
CNAME	Alias
PTR	Reverse lookup

🔹 **DNS Security issues**

- DNS spoofing
- DNS poisoning
- MITM DNS attack
- Rogue DNS server

⭐ 14.2 DHCP (Dynamic Host Configuration Protocol)

DHCP automatically assigns:

- IP
- subnet mask
- gateway
- DNS

🔹 DHCP Process (DORA)

Discover

Offer

Request

Acknowledge

Example:

PC asks for IP

DHCP server offers

PC accepts

Server confirms

🔹 DHCP Ports

- UDP 67 (server)
- UDP 68 (client)

🔹 DHCP Security

Attackers run fake DHCP to give:

- fake gateway
- fake DNS
- internet redirection

Solution = **DHCP Snooping** (already explained)

⭐ 14.3 ARP (Address Resolution Protocol)

ARP converts IP address to MAC address.

Example:

IP: 192.168.1.5 → which MAC address?

ARP asks:

“Who has 192.168.1.5? Tell me your MAC”

Device replies:

“I am 192.168.1.5, MAC = AA:BB:CC:DD”

Switch stores mapping in CAM table.

🔹 ARP Attacks (important!)

- ARP Spoofing
- ARP Poisoning
- MITM

Attacker pretends to be gateway.

Solution:

- DAI (Dynamic ARP Inspection)
- DHCP Snooping
- IP Source Guard

⭐ 14.4 ICMP (Internet Control Message Protocol)

ICMP checks network connectivity.

Example:

ping google.com

Usage:

- Ping
- Traceroute
- network reachability tests

🔹 ICMP Not TCP/UDP

ICMP is NOT an application protocol.
It is a messaging protocol.

🔹 ICMP Attacks

- Ping Flood
- Smurf attack
- ICMP tunnel
- Firewall bypass

🔹 ICMP Solution

- Firewall block external ICMP
- Rate limiting

⭐ Quick Revision

- DNS = name → IP
- DHCP = automatic IP
- ARP = IP to MAC
- ICMP = reachability
- DORA = Discover, Offer, Request, ACK
- DNS uses port 53
- DHCP uses ports 67/68

🧠 Chapter-15 — Packet Sniffing, Wireshark & Packet Capture Basics

---

⭐ 15.1 What is Packet Sniffing?

Packet sniffing means capturing the network traffic flowing on the network and analyzing it.

Example:

- sniff packets going from PC to Router
- analyze HTTP, DNS, ARP, DHCP etc.

Tools:

- Wireshark
- tcpdump
- Tshark

⭐ 15.2 Wireshark

Wireshark is the most popular **packet analyzer** tool used to:

- capture packets
- analyze protocols
- detect malicious activity
- troubleshoot networks

⭐ 15.3 What can you see in Wireshark?

You can view:

- MAC address
- IP address
- Ports (TCP/UDP)
- Payloads
- HTTP GET requests

- ARP messages
- DNS queries (domain names)
- DHCP packets (offer, ack)

⭐ 15.4 What packets can we capture?

EVERYTHING

- ARP
- DNS
- DHCP
- TCP
- UDP
- HTTP
- ICMP
- SSL/TLS
- SSH (encrypted)
- HTTPS (encrypted)

⭐ 15.5 Promiscuous Mode

Normal network card only sees packets meant for itself.
Promiscuous mode makes NIC receive all packets.

Example: Wireshark puts NIC into promiscuous mode.

⭐ 15.6 Monitor Mode (Wireless)

Wireless sniffing needs monitor mode.
Captures Wi-Fi frames (needed for Wi-Fi hacking)

Tools:

- Wireshark
- Kismet

- Aircrack-ng

⭐ 15.7 Packet Structure (for analysis)

Basic headers inside a packet:

- Ethernet header (MAC)
- IP header
- Transport header (TCP/UDP)
- Application header (HTTP, DNS etc.)

Wireshark shows all layers.

⭐ 15.8 Example analysis in Wireshark

Selecting one packet shows:

Ethernet II → MAC address

Internet Protocol → IP address

Transmission Control Protocol → TCP info

Hypertext Transfer Protocol → URL requested

⭐ 15.9 Common Wireshark filters

Filter:

ip.addr == 192.168.1.10

Filter:

tcp.port == 443

Filter:

http

Filter:

dns

Filter:

arp

⭐ 15.10 Detecting attacks in Wireshark

You can identify:

- ARP spoofing
- Fake DHCP responses
- DNS poisoning
- Malicious HTTP redirects
- Data exfiltration
- Malware communication
- Port scanning

⭐ 15.11 Exam / Interview Points

- Wireshark is packet analyser tool
- Can analyze Layer 2–7
- Uses filters
- Shows packet headers
- Used in cyber forensics

⭐ Quick Revision

- Sniff = capture packets
- Promiscuous = capture all packets
- Monitor = capture wireless
- Wireshark analyzes everything
- Good for cyber attacks

🔥 Chapter-16 — Switching Security + Wireless Security Attacks

---

🌐 16.1 Layer-2 (Switch) Security Attacks

Layer-2 is a very weak security area because by default switches trust everyone 😅

Most common attacks 👇

⭐ (1) MAC Flooding Attack

Attacker sends thousands of fake MAC addresses to switch.

Switch CAM table becomes full.

Switch goes into "fail open" mode → **behaves like hub** 😱

Result:

- attacker sees traffic
- security gone
- sniffing possible

Defense:

- **Port Security**
- Limit MAC per port

⭐ (2) ARP Spoofing / ARP Poisoning

Attacker pretends to be the gateway by sending fake ARP replies.

Effect:

- MITM (Man in the middle)
- sniff passwords
- capture traffic
- session hijacking

Defense:

- **DAI (Dynamic ARP Inspection)**
- DHCP snooping

⭐ (3) DHCP Starvation Attack

Attacker requests thousands of DHCP IP addresses.

Result:

- DHCP pool exhausted
- no IP for real users
- attacker becomes fake DHCP

Defense:

- DHCP Snooping
- rate limiting

⭐ (4) VLAN Hopping Attack

Attacker tries to jump from one VLAN to another.

Methods:

- double tagging attack
- switch spoofing

Defense:

- never use VLAN1
- disable unused switch ports
- manually set access/trunk
- change native VLAN

🌐 16.2 Wireless Security Attacks

Wireless is easier to attack because no cable and air is shared.

⭐ (1) Deauthentication Attack

Attacker forces clients to disconnect from Wi-Fi.

Used in:

- WPA handshake capture
- Evil Twin attacks

⭐ **(2) Evil Twin Attack**

Attacker creates fake Wi-Fi with same name.

User connects accidentally → attacker captures:

- credentials
- traffic

⭐ **(3) fake AP / rogue AP**

Attacker creates unauthorized AP to capture traffic.

Defense:

- Wireless Intrusion Detection
- MAC authentication
- WPA enterprise

⭐ **(4) WPS Pin Brute Force**

Home routers have WPS (push button feature)

Very weak, easily brute-forcible.

Defense: disable WPS.

⭐ **(5) WPA Handshake Capture**

Steps:

1. Force client disconnect
2. Client reconnects
3. Capture WPA handshake
4. Crack password offline (dictionary attack)

Tools:

- aircrack-ng
- bettercap
- kismet

🌐 16.3 IoT Wireless Attacks

Smart devices are weak:

- CCTV
- Smart Bulbs
- Alexa
- Smart TVs

Common issues:

- weak password
- open ports
- outdated firmware
- default passwords

🌐 16.4 Wireless Best Security Practices

✓ Always use **WPA3**
✓ change default password
✓ disable WPS
✓ hide SSID (optional)
✓ use firewall
✓ MAC filtering
✓ segment IoT devices (IoT VLAN)

🌐 16.5 Forensics / Investigation in Wireshark

Using Wireshark you can detect:

- ARP poisoning

- DNS spoofing
- malicious beacon frames
- rogue DHCP
- deauth waves
- high ICMP floods
- suspicious TCP scans

⭐ **Quick Revision**

- MAC flooding → port security
- ARP spoofing → DAI
- DHCP attacks → DHCP snooping
- VLAN hopping → no VLAN 1
- Wireless deauth → WPA3
- Evil Twin → enterprise auth
- WPS weak → disable it

🌐 **Chapter-17 — IP Services (NTP, Syslog, SNMP, NetFlow, RADIUS, TACACS+)**

⭐ **17.1 NTP (Network Time Protocol)**

NTP synchronizes **time** across network devices.

Why important?

- logs accurate time stamps
- security authentication
- certificates validity
- correlation in SIEM
- digital forensics

Example:

Router time = consistent with Server time

If time mismatch happens:

- SSL fails
- Kerberos fails
- logs mismatch

⭐ 17.2 Syslog (System Logging Protocol)

Syslog collects logs from devices:

- routers
- switches
- firewalls
- servers
- IDS / IPS

Sent to:

- SIEM
- Syslog server

Levels:
0—emergency
1—alert
2—critical
3—error
4—warning
5—notice
6—info
7—debug

Useful in SOC and Incident Response.

⭐ 17.3 SNMP (Simple Network Management Protocol)

Used to monitor network devices.
Collects:

- interface status
- CPU

- temperature
- link up/down events

Versions:

- SNMPv1 (weak)
- SNMPv2 (better)
- SNMPv3 (secure)

Use SNMPv3 always – includes encryption.

⭐ 17.4 NetFlow

Cisco technology used to analyze traffic.

Tracks:

- who is talking to whom
- protocol usage
- bandwidth usage
- suspicious traffic
- volumetric attacks

Used in:

- SOC
- NOC
- forensics
- network analysis

⭐ 17.5 AAA (Authentication, Authorization, Accounting)

AAA manages:

- who can access (AuthN)
- what they can do (AuthZ)
- logging activity (Accounting)

Systems:

- RADIUS
- TACACS+

⭐ 17.6 RADIUS

Remote Authentication Dial-In User Service

Used for:

- Wi-Fi enterprise authentication
- VPN authentication
- central user management

Supports authentication + authorization

⭐ 17.7 TACACS+

Cisco proprietary
More secure than RADIUS
Encrypts full traffic (not just password)

Used for:

- Network device access control (routers/switches/firewalls)

⭐ 17.8 Why these services matter to Cybersecurity?

These services enable:
✓ monitoring
✓ auditing
✓ log analysis
✓ user authentication
✓ security visibility

Used in:

- SOC
- Blue Team
- security operations
- forensic investigation

⭐ Quick Revision

- NTP = time sync
- Syslog = logs
- SNMP = monitoring
- NetFlow = traffic analysis
- RADIUS = Wi-Fi authentication
- TACACS+ = device authentication

🌐 Chapter-18 — NAT, PAT, DMZ, VPN & Firewall Architecture

⭐ 18.1 NAT & PAT (Quick Recap)

Already studied but here again linked with firewall:

NAT

converts Private ⇄ Public

PAT

multiple devices share one Public IP
(Home Wi-Fi)

⭐ 18.2 What is DMZ?

DMZ = De-Militarized Zone

It is a **separate network zone** where public-facing services are hosted.

Example:

- Web server
- Mail server
- DNS server

DMZ keeps them isolated from internal LAN.

⭐ DMZ Architecture

Internet ↔ Firewall ↔ DMZ ↔ Internal LAN

So if someone hacks the web server, internal LAN is still safe.

⭐ 18.3 Why DMZ?

- protect internal LAN
- secure public services
- add extra firewall rules
- prevent LAN intrusion

⭐ 18.4 VPN (Virtual Private Network)

VPN creates secure **encrypted tunnel** between remote user and company network.

Used in:

- work from home
- branch office connection
- secure remote access

VPN Types

- Site-to-Site VPN
- Remote Access VPN (anywhere access)

VPN technology

- IPSec (IP Security)
- SSL/TLS VPN

⭐ 18.5 Firewall Architecture

Modern enterprise networks use multiple firewalls:

- Perimeter Firewall

- Internal Firewall
- DMZ Firewall
- Cloud Firewall

⭐ **Types of Firewall**

Type	Works On
Packet Filtering	Layer 3
Stateful Firewall	Layer 4
NGFW	Layer 7 (Application)

NGFW = Next Generation Firewall
(advanced, includes IDS/IPS)

⭐ **18.6 IDS / IPS**

- IDS (Intrusion Detection System) detects attacks
- IPS (Intrusion Prevention System) stops attacks

Used with firewalls.

⭐ **18.7 IPSec**

IPSec = IP Security

Used for:

- encrypted communication
- secure VPN tunnels
- remote access

Provides:

- Confidentiality
- Integrity
- Authentication

⭐ 18.8 Zero Trust Model

Zero Trust = “Trust None, Verify All”

No device/user is trusted by default,
everything must be authenticated constantly.

⭐ Quick Revision

- DMZ = public zone
- VPN = encrypted remote access
- IPSec = security for VPN
- Firewall filters traffic
- IDS/IPS detect attacks

🌐 Chapter-19 — Network Monitoring, Log Analysis & Troubleshooting

---

⭐ 19.1 Why Network Monitoring is important?

Networks constantly face:

- failures
- attacks
- performance issues
- link down events
- high latency
- packet drops

Monitoring detects these early.

⭐ 19.2 Tools for Monitoring

Tool	Use
SNMP	Network device statistics
Syslog	Logs collection
NetFlow	Traffic analysis
Ping	Connectivity
Traceroute	Path check
Wireshark	Packet capture
SolarWinds	Enterprise monitoring
Nagios	Server monitoring
Zabbix	Network & server monitoring

⭐ 19.3 Types of Network Issues

- No connectivity
- Slow network
- DNS failure
- Gateway problem
- IP conflict
- DHCP failure
- NAT not working
- Firewall blocking
- ISP outage

⭐ 19.4 Troubleshooting Commands

Command	Use
ping	test connectivity
tracert / traceroute	check path

Command	Use
ipconfig / ifconfig	check IP
arp -a	check ARP
nslookup	DNS test

⭐ 19.5 Troubleshooting Method

Always follow OSI approach:

Layer-1 Cable?

Layer-2 VLAN?

Layer-3 IP?

Layer-4 TCP?

Layer-7 application?

⭐ 19.6 Common Problem Scenarios

Case 1: No internet but LAN works

Reason:

- DHCP incorrect gateway
- DNS failure
- NAT failure
- ISP down

Case 2: DNS not working

Symptoms:

- cannot open websites
- IPs work fine

Case 3: DHCP not giving IP

Symptoms:

- 169.254.x.x APIPA address

Fix:

- DHCP service
- DHCP snooping
- rogue DHCP detection

Case 4: Wi-Fi connected but no internet

Cause:

- default gateway unreachable
- blocked DNS
- NAT failure

⭐ 19.7 Log Analysis (very important)

Logs show:

- who logged in
- what was accessed
- attack attempts
- blocked traffic
- suspicious scans

Collected via:

- Syslog
- SIEM (Security Information and Event Management)

⭐ 19.8 SIEM Tools

Used to correlate security logs:

- Splunk
- QRadar
- ELK Stack

- Microsoft Sentinel
- Wazuh

SIEM helps detect cyber attacks early.

⭐ **19.9 Incident handling steps**

- identify
- analyze traffic
- collect logs
- isolate endpoint
- block attacker
- apply firewall rules
- document incident

⭐ **Quick Revision**

- Monitoring detects failures
- Logs = forensic evidence
- SIEM alerts cybersecurity team
- troubleshooting starts from Layer-1

🌐 **Chapter-20 — Cisco Device Basics (Router/Switch, Modes, CLI, Putty, Packet Tracer)**

⭐ **20.1 Cisco Router**

Router connects **different networks** and forwards packets based on IP addresses.

Functions:

- routing
- NAT/PAT
- ACL filtering

- VPN
- DHCP (optional)
- Security features

⭐ 20.2 Cisco Switch

Switch operates at **Layer-2**

- forwards frames
- uses MAC address
- VLAN segmentation
- trunking
- STP (loop prevention)

⭐ 20.3 Router vs Switch

Feature	Router	Switch
Layer	Layer-3	Layer-2
Addressing	IP	MAC
Function	routing	switching
Example	Internet gateway	LAN network

⭐ 20.4 CLI Modes in Cisco

Cisco devices have different command modes:

Mode	Prompt	Use
User EXEC	>	basic commands
Privileged EXEC	#	advanced commands
Global Config	(config)#	configuration
Interface Config	(config-if)#	interface settings

Example:

Router> enable

Router# configure terminal

Router(config)# interface g0/1

Router(config-if)#

⭐ 20.5 Save and Apply Config

Commands:

write memory

copy run start

⭐ 20.6 Show Commands

show ip interface brief

show running-config

show version

show arp

show mac address-table

show vlan

show ip route

⭐ 20.7 Cisco Packet Tracer

Packet Tracer is **Cisco simulation software** where you:

- build networks
- configure devices
- test scenarios
- learn routing/switching

Used for CCNA training.

⭐ 20.8 PuTTY

PuTTY is a **terminal program** used to access Cisco devices using:

- SSH
- Telnet (not recommended!)
- Serial console

Why use PuTTY?

- remote access to router
- configure switches
- secure SSH access

⭐ 20.9 Basic Cisco Commands

Enable:

enable

Configure:

conf t

Interface:

int g0/0

Shutdown:

shutdown

No shutdown:

no shut

⭐ 20.10 Basic Security

Disable telnet:

line vty 0 4

transport input ssh

Enable SSH:

hostname R1

ip domain-name cisco.com

crypto key generate rsa

username admin privilege 15 secret cisco

line vty 0 4

transport input ssh

⭐ **Quick Revision**

- Router routes IP
- Switch handles MAC
- CLI modes exist
- Packet Tracer = simulation
- PuTTY = remote access
- SSH = secure
- Telnet = insecure

🌐 **Chapter-21 — VLAN Configuration & Trunking (Cisco Commands)**

⭐ **21.1 Create VLAN**

Switch(config)# vlan 10

Switch(config-vlan)# name HR

⭐ **21.2 Assign Port to VLAN**

Switch(config)# interface fa0/5

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 10

⭐ **21.3 Verify VLAN**

show vlan

show vlan brief

⭐ 21.4 Configure Trunk Port

Switch(config)# interface fa0/1

Switch(config-if)# switchport mode trunk

802.1Q is default trunking protocol.

⭐ 21.5 Allow only specific VLANs on trunk

switchport trunk allowed vlan 10,20

⭐ 21.6 Change Native VLAN

switchport trunk native vlan 99

⭐ 21.7 View trunk details

show interfaces trunk

⭐ 21.8 Access vs Trunk

Port	Type	Use
Access		connects to end device
Trunk		connects switches/routers

⭐ 21.9 VLAN Range Reminder

- Normal: 1-1001
- Extended: 1006-4094

(Cisco reserves 1002-1005 for old STP technologies)

⭐ 21.10 Inter-VLAN Routing (Router on a Stick)

interface g0/0.10

encapsulation dot1Q 10

ip address 192.168.10.1 255.255.255.0

⭐ 21.11 Inter-VLAN Routing (Layer 3 Switch)

ip routing

then:

interface vlan 10

ip address 192.168.10.1 255.255.255.0

⭐ 21.12 VLAN Troubleshooting

Check:

- VLAN exists?
- Port in VLAN?
- Trunk configured?
- Allowed VLANs correct?
- Native VLAN mismatch?

Commands:

show vlan

show interface trunk

show mac address-table

⭐ Quick Revision

✓ create vlan
✓ access port
✓ trunk port
✓ native vlan

✓ allowed vlan
✓ inter-vlan routing

🌐 Chapter-22 — STP, RSTP & EtherChannel (Cisco Configuration)

⭐ 22.1 Enable Rapid STP (default in new IOS)

Switch(config)# spanning-tree mode rapid-pvst

⭐ 22.2 Display STP Status

show spanning-tree

⭐ 22.3 Set Switch as Root Bridge

spanning-tree vlan 10 root primary

Backup:

spanning-tree vlan 10 root secondary

⭐ 22.4 Forcing STP Priority

spanning-tree vlan 10 priority 4096

Lower priority = more chance of becoming root.

⭐ 22.5 Disable STP on Port (rare, risky!)

spanning-tree portfast

Used for:

- PC
- Printers
- Laptops

Never use on trunk ports.

⭐ 22.6 Enable BPDU Guard

spanning-tree portfast bpduguard default

Prevents rogue switches.

🌟 EtherChannel (LACP & PAgP)

⭐ 22.7 Manual EtherChannel

interface range fa0/1 - 4

channel-group 1 mode on

⭐ 22.8 LACP (IEEE standard)

interface range fa0/1 - 4

channel-group 1 mode active

⭐ 22.9 PAgP (Cisco Proprietary)

interface range fa0/1 - 4

channel-group 1 mode desirable

⭐ 22.10 View EtherChannel

show etherchannel summary

⭐ Quick Revision

Feature	Notes
STP	loop protection
RSTP	fast version
PVST	per VLAN

Feature	Notes
Portfast	for PCs
EtherChannel	link aggregation
LACP	standard
PAgP	Cisco

🌐 Chapter-23 — DHCP, NAT, PAT & ACL Configuration (Cisco)

⭐ 23.1 DHCP Configuration on Router

ip dhcp pool VLAN10

network 192.168.10.0 255.255.255.0

default-router 192.168.10.1

dns-server 8.8.8.8

Exclude IPs:

ip dhcp excluded-address 192.168.10.1 192.168.10.10

⭐ 23.2 Verify DHCP

show ip dhcp binding

⭐ 23.3 NAT Configuration (Static NAT)

ip nat inside source static 192.168.1.10 172.16.5.10

Inside interface:

int g0/0

ip nat inside

Outside interface:

int g0/1

ip nat outside

⭐ **23.4 Dynamic NAT**

ip nat pool NATPOOL 172.16.5.10 172.16.5.20 netmask 255.255.255.0

ip nat inside source list 1 pool NATPOOL

Access list:

access-list 1 permit 192.168.1.0 0.0.0.255

⭐ **23.5 PAT (NAT Overload)**

ip nat inside source list 1 interface g0/1 overload

This is what your home router uses.

⭐ **23.6 Access Control List (Standard ACL)**

access-list 10 deny 192.168.5.10

access-list 10 permit any

Apply:

int g0/1

ip access-group 10 in

⭐ **23.7 Extended ACL**

access-list 100 deny tcp any any eq 23

access-list 100 permit ip any any

Apply:

int g0/1

ip access-group 100 in

⭐ **ACL Direction**

Direction	Means
in	packets entering the interface
out	packets leaving the interface

⭐ Verify ACL

show access-list

⭐ Where to apply ACL

- Standard ACL → near destination
- Extended ACL → near source

(very common viva question)

⭐ Quick Revision

✓ DHCP = auto IP
✓ NAT = private→public
✓ PAT = many→one
✓ ACL = allow/deny traffic

🌐 Chapter-24 — Static Route, Default Route, OSPF & EIGRP Configuration

---

⭐ 24.1 Static Route Syntax

ip route <destination network> <mask> <next-hop>

Example:

ip route 192.168.10.0 255.255.255.0 10.0.0.2

⭐ 24.2 Default Route (Gateway of Last Resort)

ip route 0.0.0.0 0.0.0.0 192.168.1.1

Meaning:
If route not found → send here.

⭐ 24.3 Verify routing table

show ip route

Output symbols:

- C (connected)
- S (static)
- O (OSPF)
- D (EIGRP)
- R (RIP)

🌟 OSPF Configuration (Single Area)

Router-ID auto assigns highest IP of active interface OR manually set:

router ospf 1

router-id 1.1.1.1

network 192.168.1.0 0.0.0.255 area 0

Wildcard mask = reverse subnet mask
255.255.255.0 → reverse → 0.0.0.255

⭐ OSPF Multiple Networks

network 10.0.0.0 0.0.0.255 area 0

network 20.0.0.0 0.0.0.255 area 0

⭐ Verify OSPF

show ip ospf neighbor

show ip ospf database

show ip route ospf

🌟 EIGRP Configuration

router eigrp 100

network 192.168.1.0 0.0.0.255

Autonomous System Number = 100

⭐ Verify EIGRP

show ip eigrp neighbors

show ip route eigrp

⭐ Passive Interface

Stops sending routing updates on user-facing interfaces

passive-interface g0/0

⭐ No Auto Summary (important)

no auto-summary

(IPv4 only)

⭐ Change administrative distance

distance 80

to prefer a protocol.

⭐ Quick Revision

- Static = manual
- Default = catch-all
- OSPF uses area 0
- EIGRP uses AS number

- Passive interface for security
- Wildcard = inverse mask
- show ip route

🌐 Chapter-25 — WAN & ISP Concepts (PPP, MPLS, Metro Ethernet, Broadband, Leased Line)

⭐ 25.1 What is WAN?

WAN = **Wide Area Network**
Connects remote locations over long distances.

Examples:

- ISP networks
- company branch connectivity
- internet backbone

⭐ 25.2 Leased Line

A leased line is a **dedicated** connection rented from ISP.

Features:

- always ON
- secure
- reliable
- fixed bandwidth
- expensive

Used by:

- banks
- hospitals
- data centers
- corporate

Examples:

- MPLS leased line
- Point-to-point fiber

⭐ 25.3 MPLS (Multiprotocol Label Switching)

MPLS is a WAN technology used by ISPs to route packets using **labels** instead of IP lookup.

Benefits:
✓ fast
✓ secure
✓ QoS support
✓ traffic engineering
✓ VPN supported

Used by:

- Banks
- Cloud
- Enterprise WAN

⭐ 25.4 PPP (Point-to-Point Protocol)

PPP is a WAN encapsulation protocol used over serial links.

Features:

- authentication
- compression
- error detection

Used with:

- leased lines
- DSL links
- older WAN circuits

⭐ 25.5 Metro Ethernet

High-speed Ethernet provided by ISP inside a city (Metro)

Example:
Mumbai Metro Ethernet connects offices within Mumbai city.

⭐ 25.6 Broadband Internet

Examples:

- Fiber broadband
- Cable modem
- DSL
- Home internet
- Airtel, JioFiber, ACT etc.

Not dedicated (shared bandwidth)

⭐ 25.7 ISP Architecture (Simple)

Home/Office → Router → ISP → Internet Backbone

⭐ 25.8 Undersea Fiber

The internet backbone consists of **submarine fiber cables** running under oceans.

⭐ 25.9 Public vs Private WAN

WAN	Example
Public	Internet
Private	MPLS, leased line

Private WAN = secure
Public WAN = cheap

⭐ 25.10 Redundancy

WAN connections often have backup links:

- VPN failover
- another ISP
- MPLS + Internet mix

⭐ **Quick Revision**

- WAN = long distance
- MPLS = ISP WAN tech
- PPP = point-to-point protocol
- Metro Ethernet = city level fiber
- Leased line = dedicated
- Broadband = shared

🌐 **Chapter-26 — VPN, IPSec, SSL VPN, Remote Access Architecture**

⭐ **26.1 What is a VPN?**

VPN = **Virtual Private Network**

VPN makes a private encrypted tunnel **over public internet**, so remote users can securely connect to company network.

⭐ **26.2 Why VPN?**

- Secure remote access
- Encrypt traffic
- Protect corporate data
- Remote work (WFH)
- Branch site connectivity

⭐ **26.3 Types of VPN**

Type	Meaning
Site-to-Site	Branch ↔ HQ
Remote Access	User ↔ HQ

⭐ 26.4 Site-to-Site VPN

Connects two branch offices securely:

Office A ↔ Office B

⭐ 26.5 Remote Access VPN

User connects from anywhere.
Example:
Employees working from home.

VPN client installs on laptop/mobile.

⭐ 26.6 IPSec VPN

Uses IPSec (IP Security)
Provides:

- Confidentiality
- Integrity
- Authentication

IPSec works in 2 modes:

- Transport mode
- Tunnel mode

⭐ 26.7 SSL VPN

Uses HTTPS encryption
(no need special VPN client)

Works inside browser:

- remote access portal
- cloud applications
- web applications

⭐ 26.8 Tunneling

VPN encapsulates IP packets inside encrypted packets.

Layers:

- original IP packet
- VPN header
- encrypted data

⭐ 26.9 VPN Encryption Protocols

- IPSec
- SSL/TLS
- L2TP
- OpenVPN
- IKEv2

⭐ 26.10 Authentication Methods

- Username/Password
- Certificates
- Tokens
- Multifactor Authentication (MFA)
- RADIUS / TACACS+

⭐ 26.11 VPN Devices

- Firewall
- Router

- VPN Gateway
- Cloud VPN

Examples:

- Cisco ASA
- Fortigate
- Palo Alto
- AWS VPN

⭐ 26.12 VPN Security Issues

- weak passwords
- split tunneling abuse
- unpatched VPN servers
- credential leak

⭐ 26.13 VPN Forensics

Investigate:

- authentication logs
- connection logs
- IP addresses
- suspicious access locations

⭐ Quick Revision

- VPN = secure tunnel
- Site-to-site = office to office
- IPSec = strong encryption
- SSL VPN = browser based
- remote access via client
- MFA for security

🌐 Chapter-27 — Cloud Basics, Cloud Networking & Cloud Security Intro

---

⭐ 27.1 What is Cloud?

Cloud = renting computing resources from data centers instead of owning servers.

Cloud provides:

- servers
- storage
- networking
- applications

Example providers:

- AWS
- Microsoft Azure
- Google Cloud Platform (GCP)

⭐ 27.2 Cloud Service Models

Model	Meaning	Example
IaaS	Infrastructure as a Service	AWS EC2
PaaS	Platform as a Service	Azure App Service
SaaS	Software as a Service	Gmail

⭐ IaaS (Infrastructure as a Service)

You get:

- VM
- network
- storage

You manage OS + apps.

⭐ PaaS

Cloud manages OS, you deploy code.

⭐ SaaS

Fully managed application
Example:

- Gmail
- Microsoft 365
- Dropbox

🌐 27.3 Cloud Networking

Cloud has:

- VPC (Virtual Private Cloud)
- Subnets
- Route tables
- Internet Gateway
- NAT Gateway
- Security groups
- VPN site-to-site

⭐ 27.4 VPC (Virtual Private Cloud)

VPC is a private isolated network inside cloud.

⭐ 27.5 Cloud Firewall

Cloud uses:

- Security Groups
- NACL (Network ACL)

These control inbound/outbound traffic.

⭐ 27.6 Cloud NAT

Same concept as NAT on router:

- private instances → access internet
- no inbound allowed

⭐ 27.7 VPN to Cloud

Companies connect office → cloud using:

- IPSec
- AWS VPN
- Azure VPN

⭐ 27.8 Cloud Advantages

- elastic
- scalable
- pay only what you use
- high availability
- global

⭐ 27.9 Cloud Security Responsibilities (VERY IMPORTANT)

Shared Responsibility Model:

- Cloud secures infra
- You secure configuration

Example 🔥
Cloud secure datacenter but YOU secure firewall rules.

⭐ 27.10 Cloud Risks

- misconfiguration
- open ports
- public S3 bucket
- weak IAM permissions

⭐ 27.11 Cloud Security Solutions

- IAM policies
- MFA
- Cloud firewall rules
- Encryption
- Logs (CloudTrail in AWS)
- SIEM integration

⭐ Quick Revision

- Cloud = rented hardware
- VPC = cloud network
- IaaS/PaaS/SaaS
- Cloud firewall = SG + NACL
- NAT gateway
- shared responsibility

🌐 Chapter-28 — Cybersecurity & Networking Relationship

⭐ 28.1 Why Networking is required in Cyber Security?

Because almost EVERY cyber attack uses networks:

- data theft
- network malware
- remote hacking

- command-and-control (C2)
- port scanning
- sniffing
- VPN misuse

So if you don't know networking,
you can't understand:

- attack paths
- packet behavior
- traffic visibility
- logs
- routing
- firewall rules

⭐ 28.2 Networking Knowledge Required for Ethical Hacking

You should know:

- IP addressing
- Subnetting
- Ports & protocols
- ARP, DNS, DHCP
- TCP handshake
- Wireshark basics
- VLANs
- Routing basics
- Firewall basics

⭐ 28.3 Required for Digital Forensics

You analyze:

- logs

- traffic capture
- suspicious IPs
- DNS queries
- VPN abuse

Tools:

- SIEM
- Wireshark
- ELK stack
- Splunk
- Security Onion

⭐ 28.4 Required for Penetration Testing

During pentesting you:

- scan network
- enumerate services
- exploit open ports
- spoof ARP
- send packets
- bypass firewall
- evade IDS

⭐ 28.5 Networking Helps in Incidents

Example:
Ransomware attack detected →
investigator checks:

- firewall logs
- suspicious outbound traffic
- DNS logs

- C2 IP addresses

⭐ 28.6 Zero Trust + Network Segmentation

Network knowledge required to:

- design secure networks
- enforce segmentation
- reduce attack spread
- protect internal network

Example:

- IoT in separate VLAN
- DMZ separate
- servers separate

⭐ 28.7 Networking Helps in Cloud Security

Cloud = networking + security

- VPC
- ACL
- routing
- firewall
- VPN
- NAT

Most cloud cyber issues = networking misconfigurations 😄

⭐ Quick Revision

Networking required to:

- detect attacks
- defend networks
- analyze packets

- secure cloud
- understand infrastructure

🌐 Chapter-29 — Interview Questions, Commands & Cheat Sheet

⭐ 29.1 Basic Networking interview questions

✓ What is IP address?
✓ What is subnet mask?
✓ Difference between public and private IP
✓ Explain static and dynamic routing
✓ What happens when you type google.com
✓ What is default gateway?
✓ What is NAT and PAT?
✓ What is VLAN?
✓ How does ARP work?
✓ What is DNS?

⭐ 29.2 Routing questions

✓ Difference OSPF vs EIGRP
✓ What is LSDB?
✓ Explain SPF algorithm
✓ Explain DR/BDR
✓ What is cost in OSPF?
✓ What is LSA?

⭐ 29.3 Switching questions

✓ How STP prevents loops?
✓ What is root bridge?
✓ What is VLAN hopping?
✓ What is port security?
✓ What is EtherChannel?

⭐ 29.4 Security questions

✓ Difference IDS vs IPS
✓ What is firewall?
✓ Explain DMZ
✓ Why NAT exists?
✓ What is VPN?
✓ What is Zero Trust?

⭐ 29.5 Cloud questions

✓ IaaS vs PaaS vs SaaS
✓ What is VPC?
✓ What is security group?
✓ Shared responsibility model
✓ Cloud firewall

⭐ Cisco CLI Cheat Sheet

Show commands

show ip interface brief

show running-config

show version

show vlan

show ip route

show arp

show mac address-table

show spanning-tree

Configuration

enable

configure terminal

interface g0/0

no shutdown

ip address 192.168.1.1 255.255.255.0

Save

write memory

copy run start

VLAN

vlan 10

interface f0/3

switchport mode access

switchport access vlan 10

Trunk

switchport mode trunk

switchport trunk allowed vlan 10,20

Static route

ip route 0.0.0.0 0.0.0.0 192.168.10.1

OSPF

router ospf 1

network 192.168.1.0 0.0.0.255 area 0

EIGRP

router eigrp 100

network 192.168.1.0 0.0.0.255

NAT / PAT

ip nat inside source list 1 interface g0/1 overload

⭐ **Final Revision Notes (Ultra Short)**

Network = communication between devices

Switch uses MAC

Router uses IP

NAT converts private to public

DHCP gives IP automatically

DNS converts domain → IP

ARP finds MAC

VLAN separate LAN

OSPF = link state

EIGRP = hybrid

STP = loop prevention

Firewall = security

VPN encrypts connection

Cloud = VPC + firewall