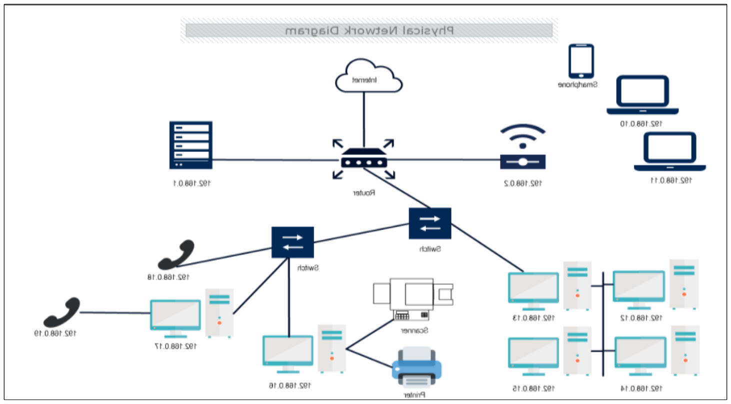
1 Concept-First Structure (Foundational Layer)

Networking fundamentals must be understood conceptually before working with commands or tools. This foundational layer focuses on **what networking concepts are and why they exist**, ensuring that practical usage is driven by reasoning rather than memorization.

1.1 What Is a Network and Why It Exists

A network is a collection of interconnected devices that communicate with each other to exchange data and share resources. Networks exist to enable efficient communication, centralized resource access, scalability, and collaboration between systems.

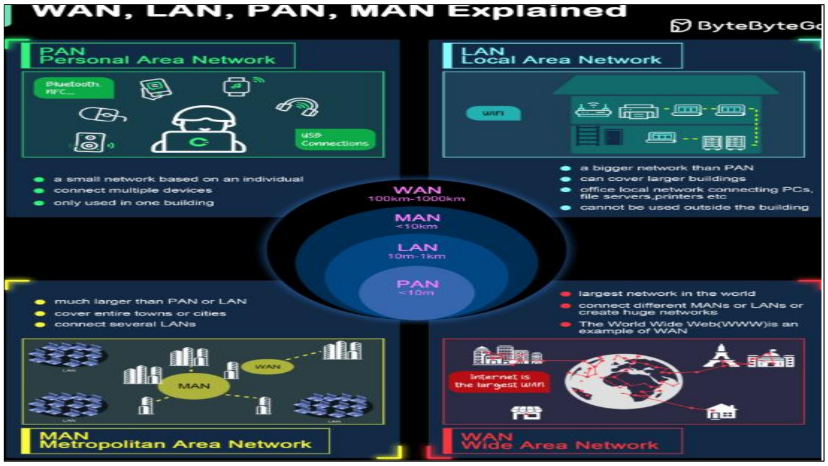


Key Points:

- Enables data communication between devices
- Supports sharing of resources such as files and printers
- Reduces duplication of hardware and services
- Forms the backbone of the internet and cloud services

1.2 Types of Networks: LAN, WAN, MAN, PAN

Networks are categorized based on their geographical coverage and scale. Each type serves a specific purpose depending on distance, ownership, and performance requirements.

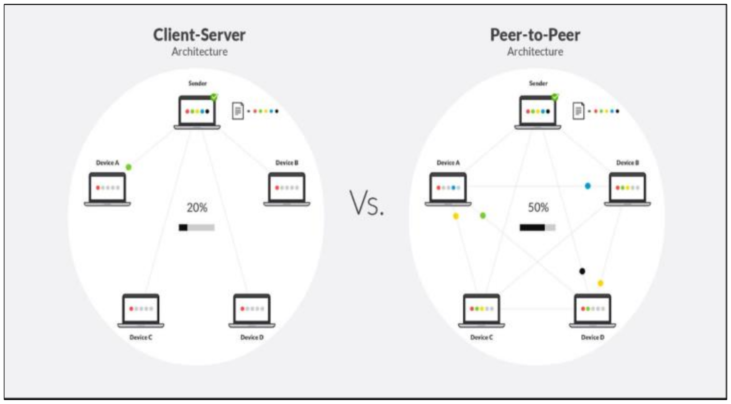

WAN, LAN, PAN, MAN Explained
ByteByteGo
PAN
Personal Area Network
Bluetooth, NFC...
USB Connections
a small network based on an individual
connect multiple devices
only used in one building
LAN
Local Area Network
WiFi
a bigger network than PAN
can cover larger buildings
office local network connecting PCs, file servers,printers etc
cannot be used outside the building
WAN
100km-1000km
MAN
<10km
LAN
10m-1km
PAN
<10m
much larger than PAN or LAN
cover entire towns or cities
connect several LANs
LAN
WAN
MAN
LAN
LAN
MAN
Metropolitan Area Network
largest network in the world
connect different MANs or LANs or create huge networks
The World Wide Web(WWW)is an example of WAN
Internet is the largest WAN
WAN
Wide Area Network

Key Points:

- LAN (Local Area Network): Covers a small area such as a home or office
- WAN (Wide Area Network): Spans large geographical areas, e.g., the internet
- MAN (Metropolitan Area Network): Covers a city or campus
- PAN (Personal Area Network): Connects personal devices over short distances

1.3 Client–Server vs Peer-to-Peer Model

Network communication models define how devices interact and share responsibilities. The client–server model centralizes control, while peer-to-peer distributes it among participants.



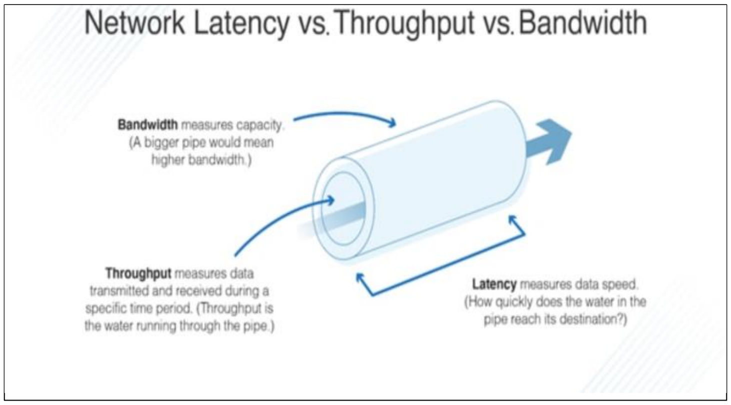
Key Points:

- Client–Server model uses centralized servers for services

- Peer-to-Peer model allows devices to act as both client and server
- Client–Server offers better control and security
- Peer-to-Peer is simpler but less scalable

1.4 Bandwidth vs Latency vs Throughput

These metrics describe network performance and are often misunderstood. Each represents a different aspect of how data moves across a network.


Network Latency vs. Throughput vs. Bandwidth
Bandwidth measures capacity. (A bigger pipe would mean higher bandwidth.)
Throughput measures data transmitted and received during a specific time period. (Throughput is the water running through the pipe.)
Latency measures data speed. (How quickly does the water in the pipe reach its destination?)

Key Points:

- Bandwidth: Maximum data capacity of a network link
- Latency: Time taken for data to travel from source to destination
- Throughput: Actual data successfully transferred over time
- High bandwidth does not guarantee low latency

1.5 Packet vs Frame (Logical vs Physical Delivery)

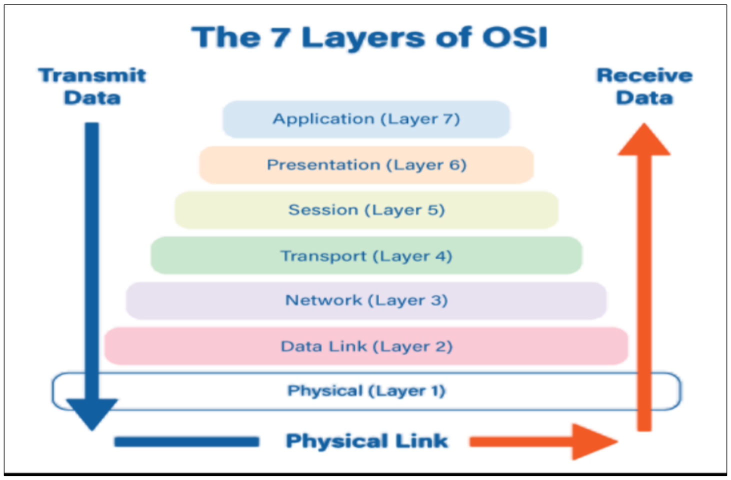
Data is broken into smaller units for transmission. These units differ based on the layer of communication and delivery method

Key Points:

- Packets operate at the network layer (logical delivery)
- Frames operate at the data link layer (physical delivery)
- Packets carry IP addressing information
- Frames carry MAC addressing information

2 OSI Model Layers and Functions

The OSI (Open Systems Interconnection) model is a conceptual framework that explains how data travels from one system to another across a network. It divides network communication into seven layers, each responsible for a specific function. This layered approach simplifies design, implementation, troubleshooting, and security analysis.



2.1 Layer 7: Application Layer

The Application layer provides network services directly to end-user applications. It is the layer closest to the user and enables interaction with network services such as web browsing and email.

Key Functions:

- Provides network access to applications
- Handles user authentication and authorization
- Supports services like HTTP, FTP, SMTP, DNS
- Interface between user software and the network

2.2 Layer 6: Presentation Layer

The Presentation layer ensures that data is in a usable format for the receiving system. It handles data translation, encryption, and compression.

Key Functions:

- Translates data formats between systems
- Encrypts and decrypts data

- Compresses and decompresses data
- Ensures data readability across platforms

2.3 Layer 5: Session Layer

The Session layer manages sessions between communicating systems. It controls the establishment, maintenance, and termination of connections.

Key Functions:

- Establishes and terminates communication sessions
- Manages session checkpoints and recovery
- Controls dialog (full-duplex or half-duplex)
- Maintains session synchronization

2.4 Layer 4: Transport Layer

The Transport layer ensures reliable or unreliable data delivery between hosts. It manages segmentation, flow control, and error handling.

Key Functions:

- Segments and reassembles data
- Provides end-to-end communication
- Implements flow and error control
- Supports protocols like TCP and UDP

2.5 Layer 3: Network Layer

The Network layer is responsible for logical addressing and routing of data packets between different networks.

Key Functions:

- Provides logical addressing (IP addresses)
- Determines best path for data delivery
- Handles packet forwarding and routing
- Enables inter-network communication

2.6 Layer 2: Data Link Layer

The Data Link layer ensures reliable data transfer between directly connected devices. It handles physical addressing and error detection.

Key Functions:

- Uses MAC addresses for physical identification
- Frames packets for transmission
- Detects and handles transmission errors
- Controls access to the physical medium

2.7 Layer 1: Physical Layer

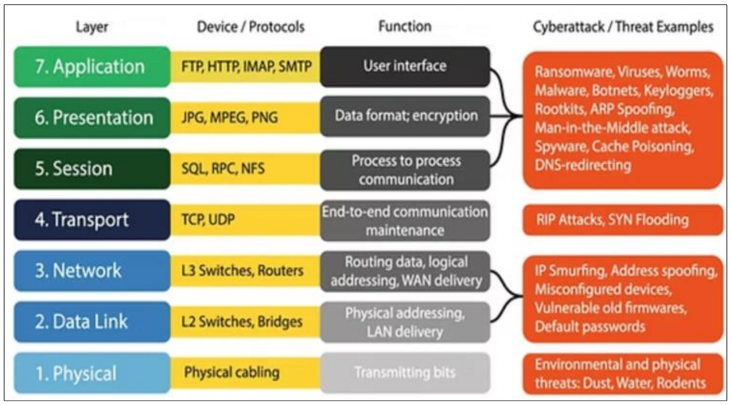
The Physical layer deals with the actual transmission of raw bits over a physical medium. It defines hardware specifications and signaling.

Key Functions:

- Transmits raw binary data
- Defines cables, connectors, and voltages
- Controls data rates and transmission modes
- Converts digital data to physical signals

2.8 Why the OSI Model Matters

The OSI model provides a structured way to understand network communication and troubleshoot problems by isolating issues to specific layers.



Layer	Device / Protocols	Function	Cyberattack / Threat Examples
7. Application	FTP, HTTP, IMAP, SMTP	User interface	Ransomware, Viruses, Worms, Malware, Botnets, Keyloggers, Rootkits, ARP Spoofing, Man-in-the-Middle attack, Spyware, Cache Poisoning, DNS-redirecting
6. Presentation	JPG, MPEG, PNG	Data format; encryption	
5. Session	SQL, RPC, NFS	Process to process communication	
4. Transport	TCP, UDP	End-to-end communication maintenance	RIP Attacks, SYN Flooding
3. Network	L3 Switches, Routers	Routing data, logical addressing, WAN delivery	IP Smurfing, Address spoofing, Misconfigured devices, Vulnerable old firmwares, Default passwords
2. Data Link	L2 Switches, Bridges	Physical addressing, LAN delivery	
1. Physical	Physical cabling	Transmitting bits	Environmental and physical threats: Dust, Water, Rodents

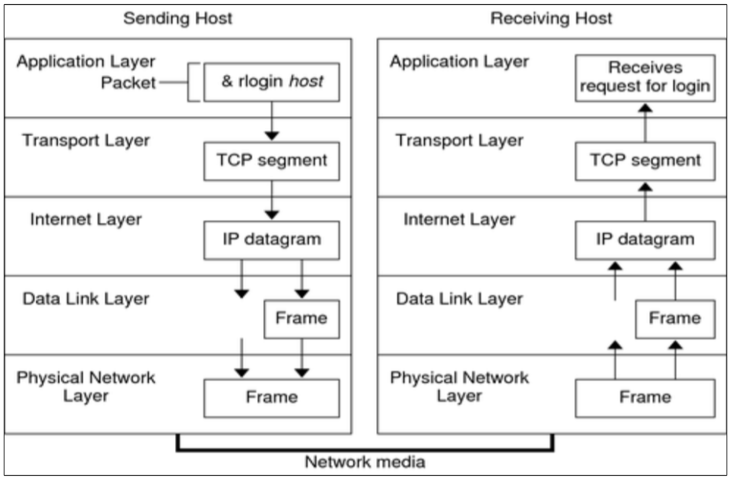
Key Points:

- Simplifies network design and learning

- Helps isolate and troubleshoot network issues
- Provides a common reference model
- Widely used in networking and cybersecurity

3 TCP/IP Protocol Suite

The TCP/IP Protocol Suite is the practical networking model used by the internet and most modern networks. Unlike the OSI model, which is conceptual, TCP/IP is an implementation-focused model that defines how data is packaged, addressed, transmitted, routed, and received across networks.



3.1 Overview of the TCP/IP Model

The TCP/IP model consists of four layers, each grouping related networking functions. These layers collectively enable end-to-end communication between devices across interconnected networks.

Key Points:

- Practical and implementation-driven model
- Used by the internet and real-world networks
- Fewer layers than the OSI model
- Focuses on interoperability and scalability

3.2 Application Layer

The Application layer in TCP/IP combines the responsibilities of the Application, Presentation, and Session layers of the OSI model. It provides network services directly to user applications.

Key Functions:

- Enables communication between applications over the network
- Handles data formatting and session management internally

- Provides user-level protocols and services

Common Protocols:

- HTTP / HTTPS
- FTP
- SMTP, POP3, IMAP
- DNS
- SSH

3.3 Transport Layer

The Transport layer provides end-to-end communication services for applications. It is responsible for reliability, flow control, and segmentation of data.

Key Functions:

- Ensures end-to-end data delivery
- Segments and reassembles data
- Performs error detection and flow control

Common Protocols:

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

3.4 Internet Layer

The Internet layer is responsible for logical addressing and routing of packets across multiple networks. It determines how data moves from the source to the destination.

Key Functions:

- Provides logical IP addressing
- Routes packets between networks
- Handles packet fragmentation and reassembly

Common Protocols:

- IP (IPv4, IPv6)
- ICMP
- ARP
- IPsec

3.5 Network Access Layer

The Network Access layer defines how data is physically transmitted over the network medium. It combines the Data Link and Physical layers of the OSI model.

Key Functions:

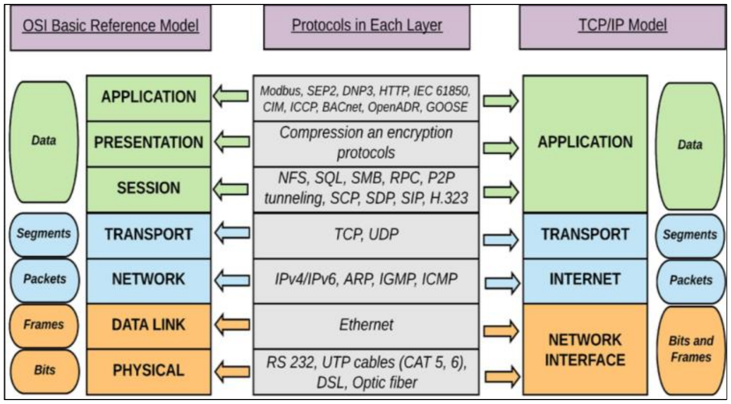
- Handles physical addressing (MAC addresses)
- Frames data for transmission
- Manages access to the physical medium

Common Technologies:

- Ethernet
- Wi-Fi
- ARP (address resolution)

3.6 TCP/IP vs OSI Model

While both models describe network communication, they serve different purposes. OSI is primarily educational, whereas TCP/IP is operational.


OSI Basic Reference Model
Protocols in Each Layer
TCP/IP Model
Data
APPLICATION
PRESENTATION
SESSION
Modbus, SEP2, DNP3, HTTP, IEC 61850, CIM, ICCP, BACnet, OpenADR, GOOSE
Compression an encryption protocols
NFS, SQL, SMB, RPC, P2P tunneling, SCP, SDP, SIP, H.323
APPLICATION
Data
Segments
TRANSPORT
TCP, UDP
TRANSPORT
Segments
Packets
NETWORK
IPv4/IPv6, ARP, IGMP, ICMP
INTERNET
Packets
Frames
DATA LINK
Ethernet
Bits
PHYSICAL
RS 232, UTP cables (CAT 5, 6), DSL, Optic fiber
NETWORK INTERFACE
Bits and Frames

Key Differences:

- TCP/IP has 4 layers; OSI has 7 layers
- TCP/IP is protocol-oriented; OSI is concept-oriented
- TCP/IP is used in real networks; OSI is a reference model
- OSI explains *how*; TCP/IP defines *how it is done*

3.7 Why the TCP/IP Protocol Suite Matters

The TCP/IP protocol suite enables global communication by providing standardized rules that allow heterogeneous systems to interoperate across diverse networks.

Key Points:

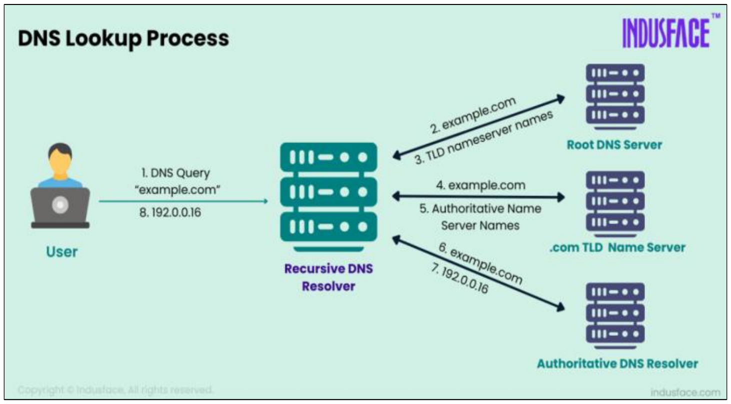
- Forms the foundation of the internet
- Enables scalable and reliable communication
- Supports diverse hardware and software platforms
- Essential knowledge for networking and cybersecurity

4 DNS and HTTP/HTTPS Deep Dive

Modern networking and web communication rely heavily on DNS and HTTP/HTTPS. DNS enables name resolution, while HTTP and HTTPS govern how web resources are requested, transferred, and secured. Understanding these mechanisms is critical before working with networking tools or security analysis.

4.1 Domain Name System (DNS)

DNS is a distributed naming system that translates human-readable domain names into IP addresses. This abstraction allows users to access services without memorizing numerical IP addresses.



How DNS Resolution Works:

- User enters a domain name in a browser
- Local DNS cache is checked
- Query is sent to a recursive resolver

- Resolver contacts root, TLD, and authoritative servers
- IP address is returned to the client

Key Points:

- DNS operates primarily over UDP port 53
- Uses TCP for large responses and zone transfers
- Highly distributed for scalability and reliability
- Critical dependency for almost all internet services

4.2 Common DNS Record Types

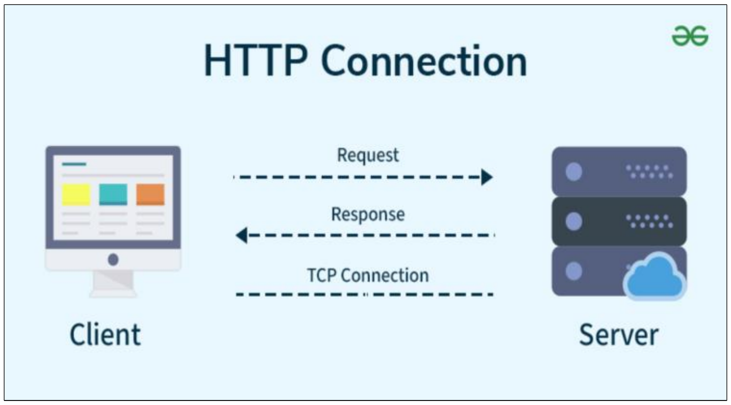
DNS records define how domain-related information is stored and retrieved.

Key Records:

- A: Maps a domain name to an IPv4 address
- AAAA: Maps a domain name to an IPv6 address
- CNAME: Creates an alias for another domain
- MX: Specifies mail servers for a domain
- NS: Identifies authoritative name servers

4.3 Hypertext Transfer Protocol (HTTP)

HTTP is an application-layer protocol used for transferring web resources between clients and servers. It follows a request–response communication model.



How HTTP Works:

- Client sends an HTTP request to a server

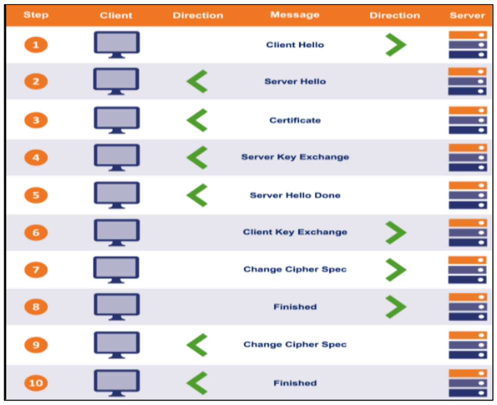
- Server processes the request
- Server returns an HTTP response
- Connection may be closed or reused

Key Characteristics:

- Stateless protocol
- Uses TCP port 80 by default
- Supports methods such as GET, POST, PUT, DELETE
- Does not provide encryption by default

4.4 Hypertext Transfer Protocol Secure (HTTPS)

HTTPS is the secure version of HTTP. It uses encryption to protect data in transit and ensure confidentiality, integrity, and authenticity.



Step	Client	Direction	Message	Direction	Server
1	🖥		Client Hello	>	🗄
2	🖥	<	Server Hello		🗄
3	🖥	<	Certificate		🗄
4	🖥	<	Server Key Exchange		🗄
5	🖥	<	Server Hello Done		🗄
6	🖥		Client Key Exchange	>	🗄
7	🖥		Change Cipher Spec	>	🗄
8	🖥		Finished	>	🗄
9	🖥	<	Change Cipher Spec		🗄
10	🖥	<	Finished		🗄

How HTTPS Secures Communication:

- Client initiates a secure connection
- Server presents a digital certificate
- TLS handshake establishes encryption keys
- Encrypted HTTP data is exchanged

Key Characteristics:

- Uses TCP port 443 by default
- Encrypts data using TLS
- Prevents eavesdropping and tampering
- Verifies server identity using certificates

4.5 HTTP vs HTTPS

HTTP and HTTPS differ primarily in security. HTTPS addresses the major weaknesses of HTTP by introducing encryption and authentication.

Key Differences:

- HTTP transmits data in plaintext; HTTPS encrypts data
- HTTP is vulnerable to interception; HTTPS resists MITM attacks
- HTTP uses port 80; HTTPS uses port 443
- HTTPS is mandatory for secure web applications

4.6 Security Perspective

DNS and HTTP/HTTPS are frequent targets for attacks due to their central role in internet communication.

Security Considerations:

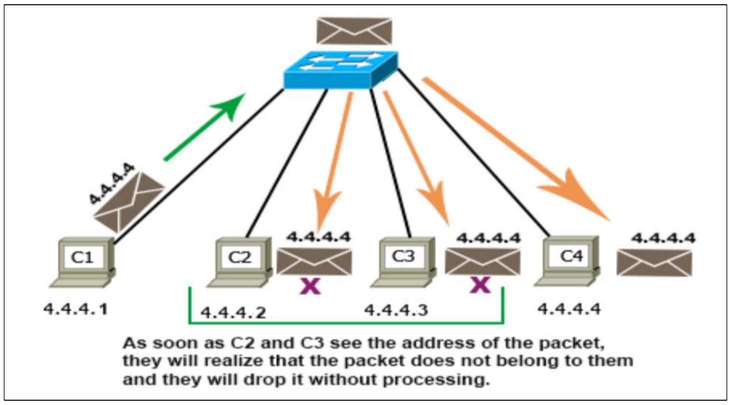
- DNS spoofing and cache poisoning
- Man-in-the-middle attacks on HTTP
- Certificate misconfiguration in HTTPS
- Importance of DNSSEC and TLS

5 IP Addressing, Subnetting, and NAT

IP addressing, subnetting, and Network Address Translation (NAT) form the core of how devices are identified, grouped, and connected across networks. These concepts are fundamental for understanding routing, scalability, and real-world network design.

5.1 IP Addressing

An IP address is a logical identifier assigned to a device on a network. It enables devices to locate each other and exchange data across interconnected networks.



As soon as C2 and C3 see the address of the packet, they will realize that the packet does not belong to them and they will drop it without processing.

Key Points:

- IP addresses uniquely identify devices on a network
- IPv4 uses 32-bit addresses; IPv6 uses 128-bit addresses
- Each IP address consists of a network part and a host part
- Logical addressing operates at the network layer

5.2 Types of IP Addresses

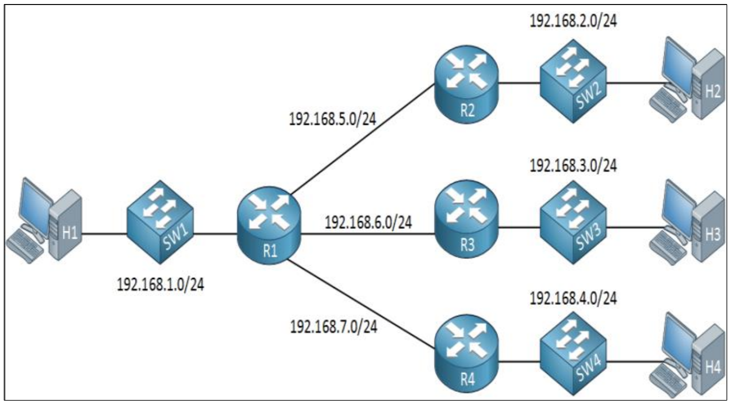
IP addresses are categorized based on scope, assignment method, and usage.

Key Types:

- Public IP: Globally routable on the internet
- Private IP: Used within internal networks
- Static IP: Manually assigned and fixed
- Dynamic IP: Assigned automatically using DHCP

5.3 Subnetting

Subnetting is the process of dividing a larger network into smaller, manageable subnetworks. It improves efficiency, performance, and security.



Why Subnetting Is Used:

- Reduces broadcast traffic
- Improves network performance
- Enhances security through isolation
- Enables efficient IP address utilization

5.4 Subnet Mask and CIDR

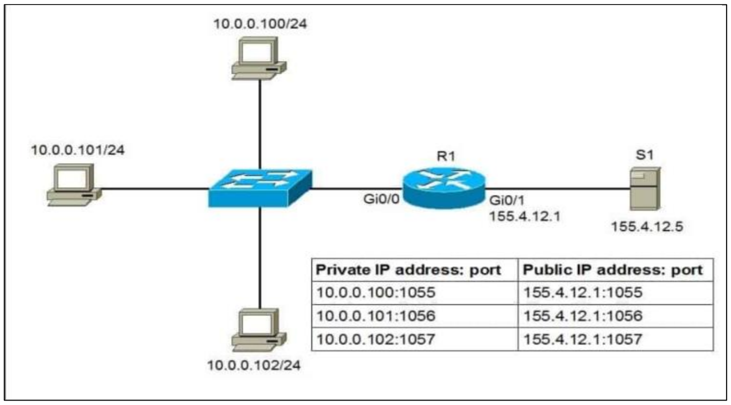
A subnet mask defines how many bits of an IP address belong to the network portion. CIDR notation provides a compact representation of this information.

Key Concepts:

- Subnet mask separates network and host portions
- CIDR notation uses a slash followed by the prefix length
- Example: /24 indicates 24 network bits
- Smaller subnets allow finer network control

5.5 Network Address Translation (NAT)

NAT allows multiple devices within a private network to share a single public IP address. It is widely used in home and enterprise networks.



Private IP address: port	Public IP address: port
10.0.0.100:1055	155.4.12.1:1055
10.0.0.101:1056	155.4.12.1:1056
10.0.0.102:1057	155.4.12.1:1057

Why NAT Exists:

- Conserves public IPv4 addresses
- Enables private networks to access the internet
- Adds a basic layer of obscurity
- Simplifies internal network design

5.6 Types of NAT

Different NAT implementations serve different networking requirements.

Common Types:

- Static NAT: One-to-one IP address mapping
- Dynamic NAT: Maps private IPs to a pool of public IPs
- PAT (Port Address Translation): Many-to-one mapping using ports

5.7 Security and Real-World Perspective

IP addressing, subnetting, and NAT directly impact network security, routing, and scalability. Misconfiguration can lead to exposure, inefficiency, or loss of connectivity.

Key Points:

- Proper subnetting limits attack surfaces
- NAT hides internal IP structure from external networks
- Incorrect IP configuration causes routing failures
- Essential knowledge for networking and cybersecurity roles