Computer Networks (DI03000051)

GTU Diploma Engineering

Table of Contents I

Table of Contents II

Table of Contents III

Table of Contents IV

Table of Contents V

Table of Contents VI

Table of Contents VII

Computer Networks (DI03000051)

GTU Diploma Engineering

Agenda

- What is a Computer Network?
- The Need and Advantages of Networking
- Key Network Applications
- Client-Server and P2P Architectures

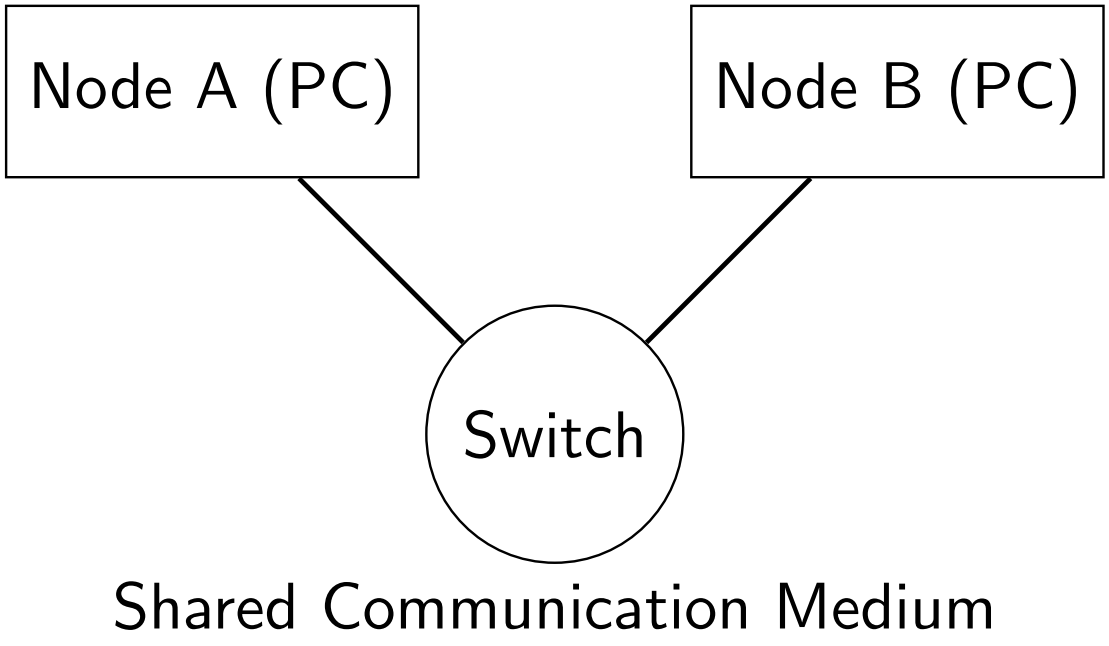
What is a Computer Network?

- A computer network is an interconnected collection of autonomous computers.
- Two computers are said to be interconnected if they are able to exchange information.
- The connection can be established via copper wire, fiber optics, microwaves, infrared, or communication satellites.
- Key concepts: Nodes (devices like PCs, routers, switches) and Links (communication channels).

The Need for Computer Networks

- Resource Sharing: Making all programs, equipment, and data available to anyone on the network without regard to the physical location.
- High Reliability: Having alternative sources of supply (e.g., multiple copies of files across different machines to prevent data loss).
- Cost Reduction: Personal computers have a much better price/performance ratio than mainframes. The client-server model leverages this.
- Scalability: System performance can be increased gradually by adding more processors (clients or servers) as workload increases.

Diagram: A Simple Computer Network



Computer Network Applications (Business)

- Resource sharing: Printers, scanners, and high-capacity storage drives shared among employees in an office.
- Information Management: Centralized databases accessible via VPNs and intranets (e.g., ERP systems, customer records).
- Communication: Email, instant messaging, VoIP (Voice over IP), and video conferencing which enable remote work.
- Electronic Commerce: B2B (Business-to-Business) and B2C (Business-to-Consumer) interactions like online supply chain management.

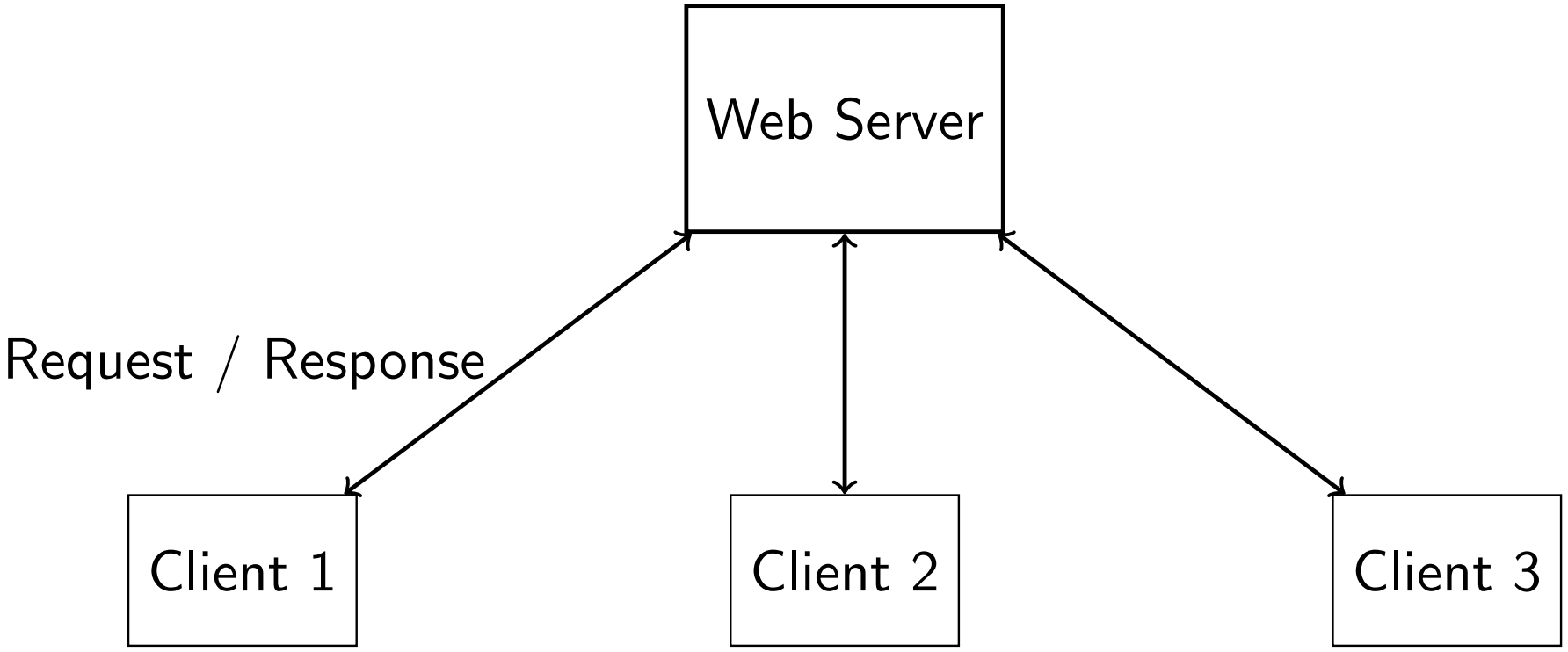
Computer Network Applications (Home & Mobile)

- Access to remote information: Web browsing, digital libraries, Wikipedia, and online news portals.
- Person-to-person communication: Social media platforms, instant messaging (WhatsApp, Telegram).
- Interactive entertainment: Video on demand (Netflix, YouTube), live streaming, and multiplayer online gaming.
- Mobile Apps: GPS navigation, m-commerce, and IoT (Internet of Things) device control (smart home appliances).

Architecture Application: Client-Server Model

- The Client-Server model is a distributed application structure that partitions tasks or workloads between the providers of a resource (servers) and service requesters (clients).
- Clients initiate communication sessions with servers which await incoming requests, processing them, and sending back responses.
- Examples: Web browsers (clients) requesting web pages from web servers (Apache, Nginx).
- Email clients (Outlook) communicating with mail servers (SMTP/IMAP to send and receive messages).

Diagram: Client-Server Architecture



Summary

- Networks are essential for modern computing, providing resource sharing, reliability, scalability, and cost savings.
- Applications range from enterprise business databases to home entertainment and mobile IoT systems.
- The Client-Server architecture remains a dominant model for structuring network applications and services.
- Next Lecture: Network Hardware components (routers, switches, hubs) and Network Topologies (star, ring, mesh).

Computer Networks (DI03000051)

GTU Diploma Engineering

Agenda

- Definition of Computer Networks
- Need for Networking
- Resource Sharing Architecture
- Key Network Applications
- Client-Server Model

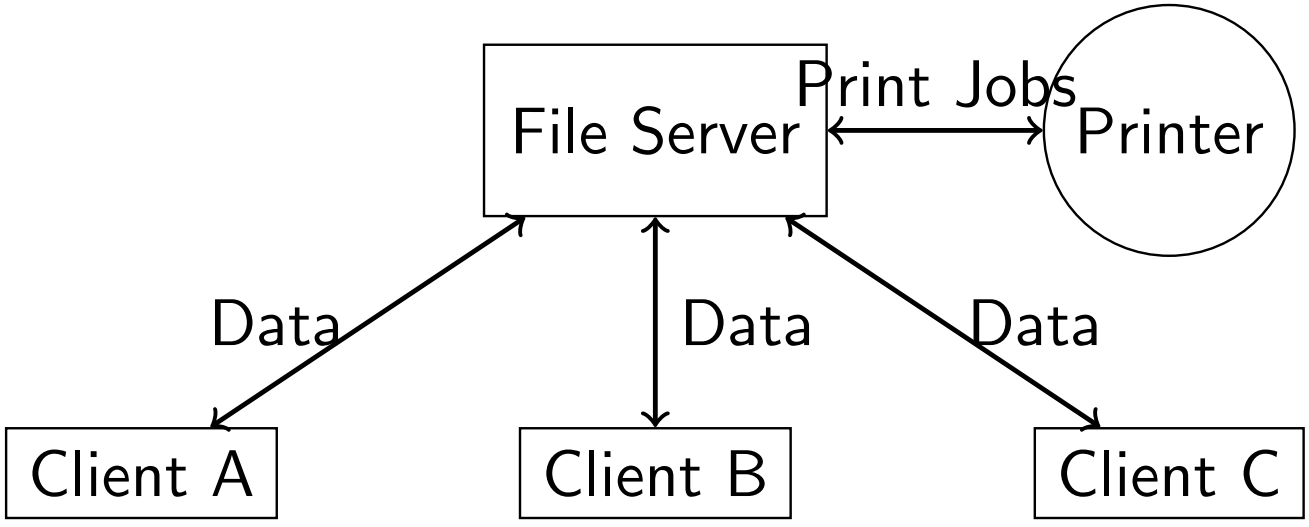
Definition of a Computer Network

- A computer network is a set of interconnected nodes or computing devices that exchange data and share resources.
- Nodes can be computers, printers, servers, or any device capable of sending and receiving data generated by other nodes on the network.
- Interconnections are established using physical media like copper cables, fiber optics, or wireless technologies like Wi-Fi and Bluetooth.
- The fundamental purpose is to enable seamless communication and data transfer across distinct geographic locations using standard protocols.

The Need for Computer Networks

- Resource Sharing: Enables multiple users to share expensive hardware devices (like high-volume printers or massive storage arrays) and software applications.
- High Reliability: Networks provide redundancy. If one system or path fails, alternative paths or replicated servers ensure continued availability (fault tolerance).
- Cost Reduction: Centralized software deployment and shared infrastructure drastically reduce IT operational costs compared to standalone systems.
- Communication Medium: Facilitates instantaneous communication mechanisms such as email, instant messaging, VoIP, and video conferencing across the globe.

Resource Sharing Architecture



Computer Network Applications: Business

- Database Access: Employees can securely access centralized corporate databases via intranet portals to retrieve customer data, inventory, and financials.
- Supply Chain Management: Automated B2B interactions allow companies to electronically order supplies, track shipments, and manage logistics using EDI (Electronic Data Interchange).
- Cloud Computing & SaaS: Businesses leverage remote servers to host enterprise applications, avoiding localized hardware limitations.
- Virtual Private Networks (VPNs): Enable secure, encrypted remote access to corporate internal networks for off-site employees over the public internet.

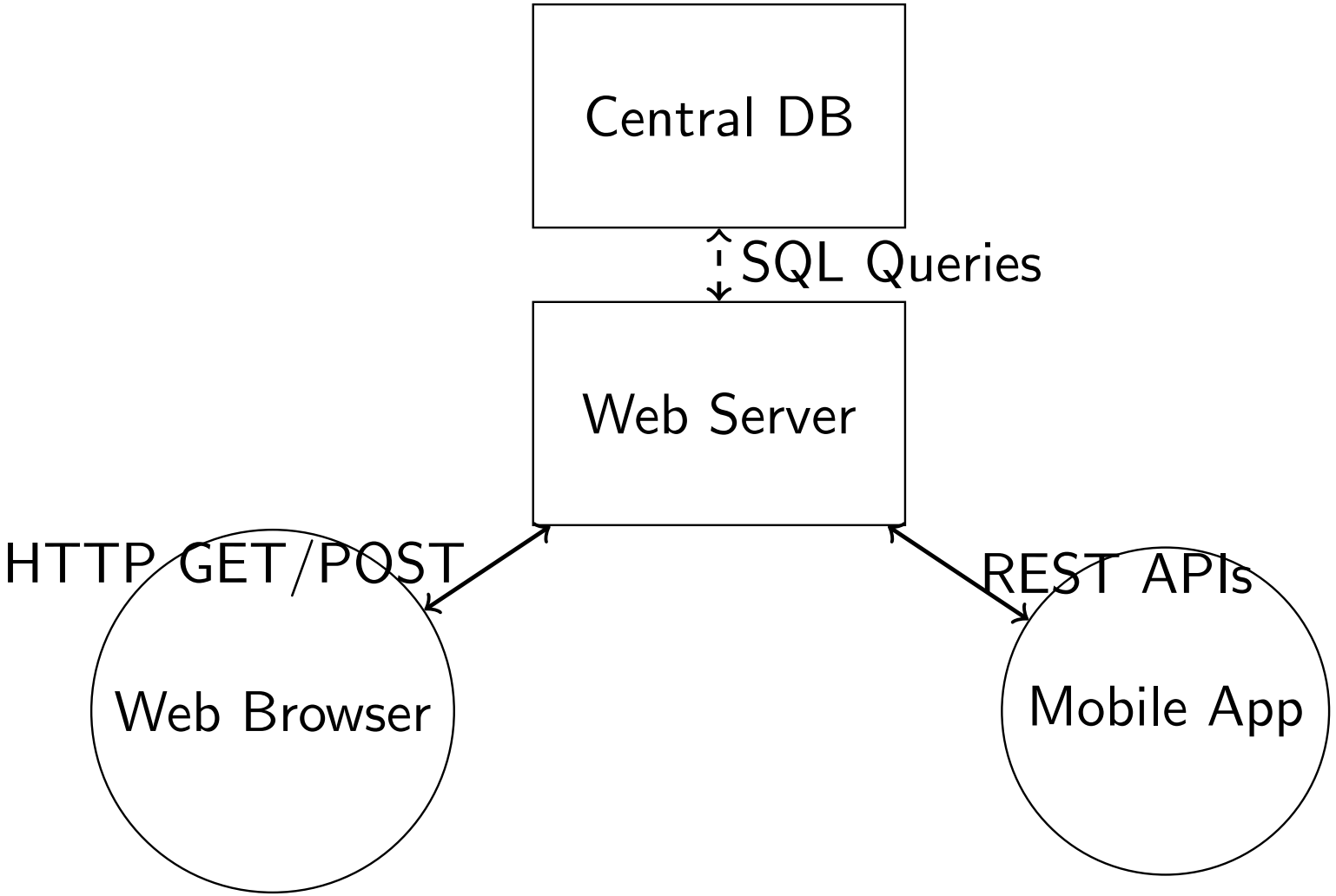
Computer Network Applications: Home

- Internet Access & Browsing: The most prevalent home application, enabling users to access web servers to consume news, research, and general information.
- Entertainment & Streaming: Networks provide the high bandwidth necessary for IPTV, VOD (Video on Demand), and interactive multiplayer gaming.
- IoT and Smart Homes: Interconnected home devices (thermostats, security cameras, smart appliances) communicate via local Wi-Fi and connect to external servers.
- Peer-to-Peer (P2P) Communication: Direct data exchange between user computers without central servers, heavily used for file sharing and decentralized communication.

Computer Network Applications: Mobile

- Location-Based Services: Mobile networks utilize GPS and cellular triangulation to provide navigation, local search, and proximity-based advertising.
- Mobile Banking & E-Commerce: Secure transactional protocols enable users to perform financial operations and purchases globally via smartphones.
- Ubiquitous Computing: Continuous connectivity via 4G/5G technologies ensures seamless application state transitions as users physically move across different geographic cells.
- Sensor Networks: Wide-area deployment of mobile devices contributing telemetry data for traffic analysis, environmental monitoring, and crowd-sourcing.

Client-Server Model Application



Summary

- Networks essentially bridge the gap between physically separated computing resources, promoting collaboration and efficiency.
- The need for networks fundamentally stems from economic and functional desires: sharing resources, improving reliability, and facilitating human communication.
- Business applications focus on B2B/B2C communications, central database access, and secure remote VPN connections.
- Home and mobile applications highlight entertainment, seamless connectivity, location awareness, and internet of things (IoT).

Computer Networks (DI03000051)

GTU Diploma Engineering

Agenda

- 1. Introduction to Network Connections
- 2. Point-to-Point (P2P) Connections
- 3. Characteristics and Applications of P2P
- 4. Multipoint (Multidrop) Connections
- 5. Medium Access in Multipoint
- 6. Comparative Summary

Introduction to Network Connections

- A network connection defines the physical and logical link between two or more devices (nodes) to establish a communication channel.
- Connections are fundamentally characterized by their topology, capacity (bandwidth), and the number of participating endpoints.
- In modern networking, data link layer (OSI Layer 2) protocols govern how nodes share the communication medium.
- The physical layer transmission medium can be guided (copper wires, fiber optics) or unguided (radio waves, microwaves).
- Regardless of the underlying medium, connections are broadly classified into two primary types: Point-to-Point and Multipoint.

Point-to-Point Connection (P2P)

- A Point-to-Point (P2P) connection provides a dedicated physical or logical link between exactly two devices.
- The entire bandwidth capacity of the channel is reserved exclusively for transmission between those two specific nodes.
- Most P2P connections use a dedicated cable, but microwave, laser, or satellite links are also utilized for long-distance P2P.
- Examples include a direct serial connection between a router and a modem, or a remote control interacting with a television.
- Enterprise WANs frequently utilize P2P topologies via dedicated leased lines (such as T1/E1 circuits) to connect remote branch offices securely.

Diagram: Point-to-Point Connection

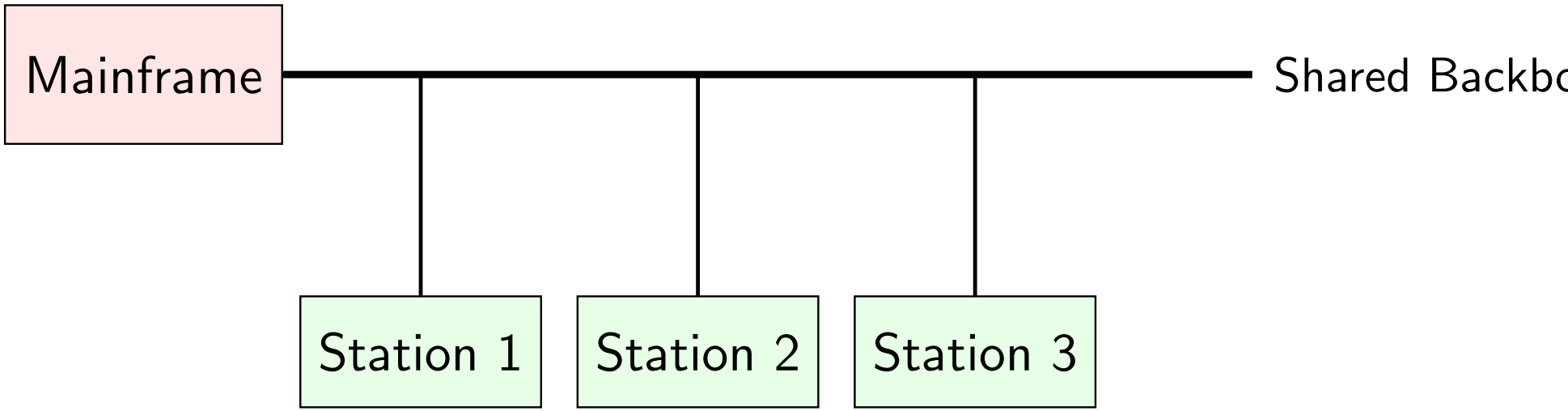
Characteristics & Protocols of P2P

- High Security and Privacy: Data travels exclusively between the two endpoints, preventing intermediate snooping by other local devices.
- Predictable Performance: Guaranteed bandwidth without any contention or medium access delays from other nodes.
- Simplicity: Routing and medium access control (MAC) mechanisms are highly simplified or unnecessary.
- Point-to-Point Protocol (PPP): A standard OSI Layer 2 protocol used to establish a direct connection over synchronous and asynchronous circuits.
- High-Level Data Link Control (HDLC): Another foundational bit-oriented synchronous data link layer protocol used over P2P leased lines.

Multipoint Connection (Multidrop)

- A Multipoint (or Multidrop) connection is an arrangement where more than two specific devices share a single communication link.
- The capacity of the channel is divided among the connected devices, requiring coordination to avoid signal collisions.
- Spatial Sharing: Devices can use the link simultaneously if bandwidth is divided via Frequency Division Multiplexing (FDM).
- Temporal Sharing: Devices take turns transmitting data using Time Division Multiplexing (TDM) or contention-based protocols.
- Multipoint is typical in legacy bus topologies (like 10Base5 Ethernet) and prevalent in modern shared environments like Wi-Fi networks.

Diagram: Multipoint Connection



Medium Access in Multipoint

- Because the physical link is shared, a Medium Access Control (MAC) protocol is strictly required to manage transmission rights.
- Contention-based access: Devices independently determine when to send, often resulting in collisions (e.g., CSMA/CD in Ethernet, CSMA/CA in Wi-Fi).
- Controlled access: Access is deterministic. Devices might pass a logical token (Token Ring) or a primary device might poll secondary devices.
- Cost-Efficiency: Drastically reduces the amount of physical cabling, infrastructure, and switch port density compared to a full-mesh P2P network.
- Vulnerability: A physical break in the shared backbone link can cause a widespread outage for all connected downstream devices.

Summary: P2P vs Multipoint

- Capacity: P2P guarantees dedicated bandwidth, whereas Multipoint dictates that bandwidth is shared and potentially congested.
- Cost & Infrastructure: Multipoint is more economical for connecting numerous localized devices; P2P cabling costs scale rapidly with node count.
- Security: P2P is inherently secure at the physical layer; Multipoint requires robust encryption to prevent neighboring nodes from intercepting frames.
- Fault Tolerance: P2P fault isolation is straightforward. Multipoint networks can suffer from single points of failure on the shared medium.
- Scalability: Adding devices to a Multipoint link degrades overall performance per user, whereas new P2P links require new, dedicated hardware interfaces.

Computer Networks (DI03000051)

GTU Diploma Engineering

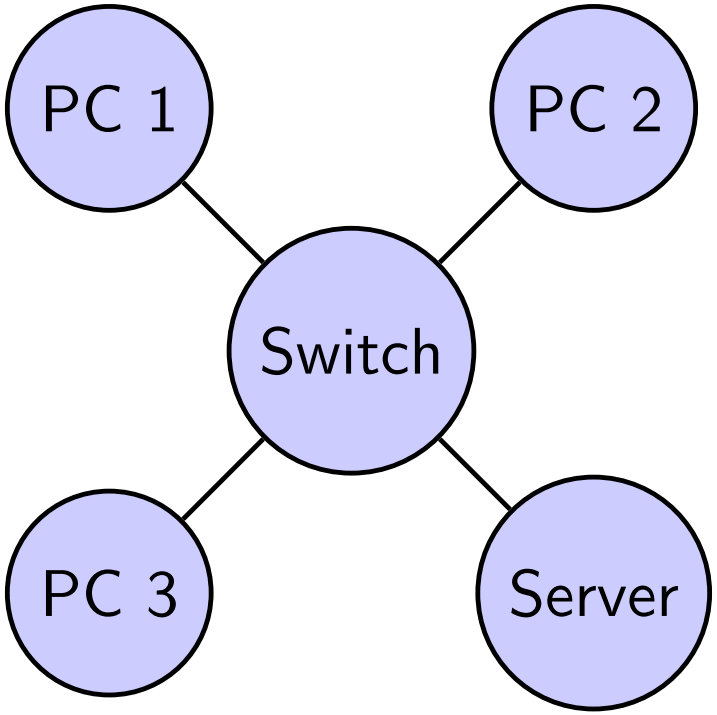
Agenda

- Introduction to Network Categories
- Local Area Network (LAN)
- Metropolitan Area Network (MAN)
- Wide Area Network (WAN)
- The Internet

Introduction to Network Types

- Networks are broadly classified based on their geographical span and ownership.
- The primary categories include Personal Area Network (PAN), Local Area Network (LAN), Metropolitan Area Network (MAN), and Wide Area Network (WAN).
- PANs cover very short distances (e.g., Bluetooth devices within 10 meters).
- The choice of network type dictates the underlying technologies, transmission media, and routing protocols used.
- As geographical span increases, network complexity, latency, and cost typically increase, while data transfer rates may decrease compared to tightly coupled local networks.

Local Area Network (LAN) Topology



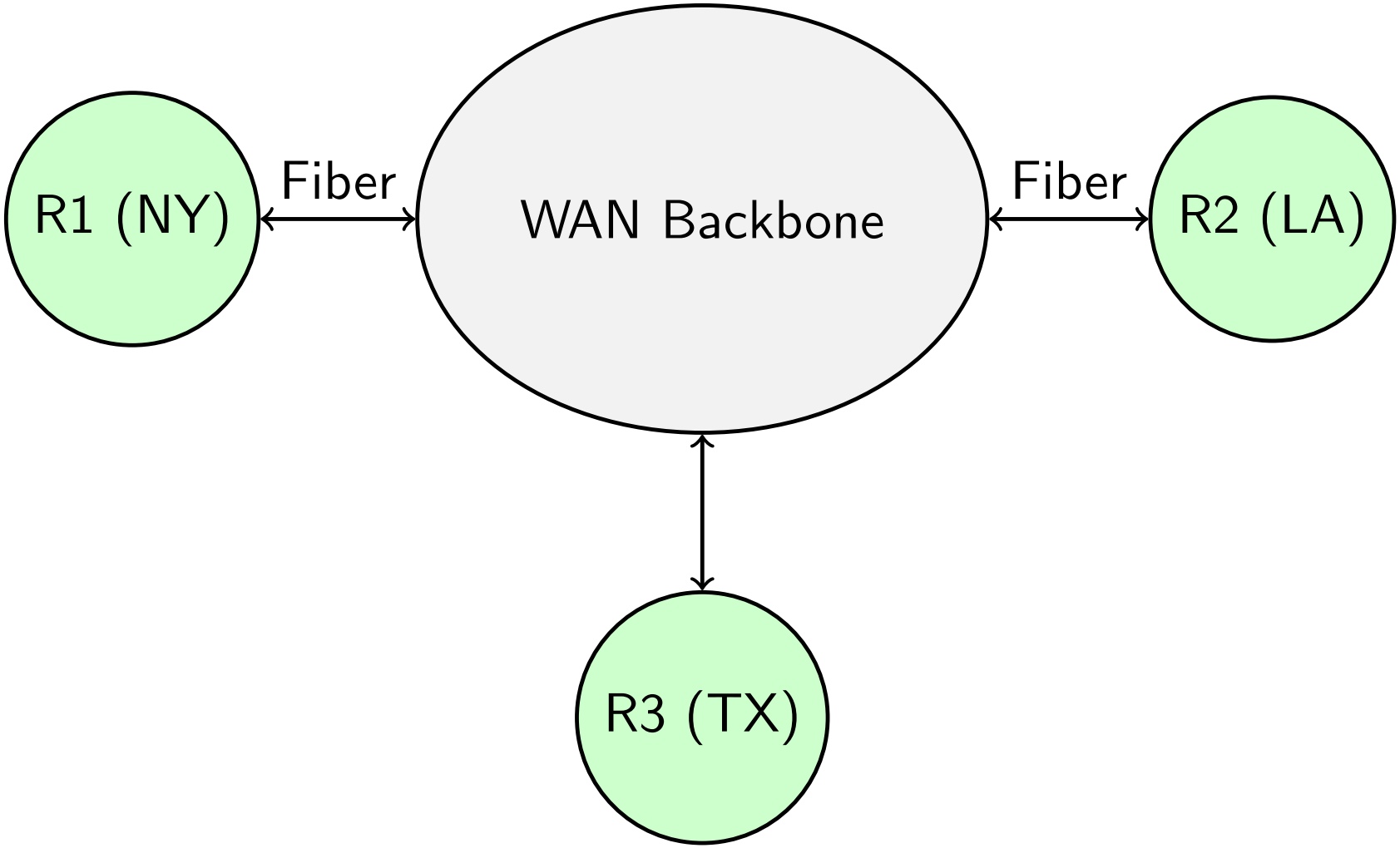
Local Area Network (LAN): Characteristics & Protocols

- Scope: Confined to a single building, office, or campus (typically ¡ 1-2 km).
- Ownership: Privately owned and managed by a single organization.
- Speeds: Extremely high data transfer rates, typically 1 Gbps, 10 Gbps, or even 40/100 Gbps in enterprise environments.
- Protocols: IEEE 802.3 (Ethernet) is the dominant wired standard; IEEE 802.11 (Wi-Fi) for wireless LANs (WLANs).
- Hardware: Utilizes Layer 2 Switches (MAC address based forwarding) and access points. Hubs are obsolete due to collision domain issues.
- Use Case: Resource sharing (printers, local file servers) and providing local clients with access to the enterprise core.

Metropolitan Area Network (MAN)

- Scope: Covers a city or a large university campus (typically 5 to 50 km).
- Ownership: Can be privately owned (e.g., a massive corporate campus) or a service provided by a public telecommunications company.
- Purpose: Serves as an interconnection between multiple LANs within a geographic area to form a larger cohesive network.
- Technologies: Often utilizes fiber-optic links. Historically used FDDI (Fiber Distributed Data Interface) or ATM. Modern MANs frequently deploy Metro Ethernet or Gigabit Passive Optical Networks (GPON).
- Use Case: Cable television networks, connecting various branch offices within the same metropolis, or providing high-speed city-wide municipal Wi-Fi.

Wide Area Network (WAN) Architecture



Wide Area Network (WAN): Deep Dive

- Scope: Spans large geographical areas, covering countries, continents, or the globe.
- Ownership: Infrastructure is generally owned by multiple Internet Service Providers (ISPs) and leased by enterprises.
- Technologies: Utilizes leased lines, Multiprotocol Label Switching (MPLS), Frame Relay, and increasingly Software-Defined WAN (SD-WAN).
- Routing: Heavily reliant on Layer 3 routers. Protocols like OSPF, IS-IS (for interior routing) and BGP (for exterior/inter-AS routing) are fundamental.
- Characteristics: Higher latency and error rates compared to LANs. Bandwidth is highly variable and often asymmetrical depending on the leased circuit SLA.

The Internet: The Global Network

- Definition: The 'Network of Networks'. A globally connected system of interconnected private, public, academic, business, and government networks.
- Architecture: Hierarchical structure of Tier 1, Tier 2, and Tier 3 ISPs. Autonomous Systems (AS) interconnect via Internet Exchange Points (IXPs).
- Protocol Suite: Exclusively relies on the TCP/IP protocol stack. IPv4 (32-bit addresses) and IPv6 (128-bit addresses) provide logical addressing.
- Governance: Decentralized, but standards are maintained by bodies like the Internet Engineering Task Force (IETF) and IP address allocation by IANA/ICANN.
- Use Case: World Wide Web (HTTP/HTTPS), email (SMTP/IMAP), file transfer (FTP), and practically all global digital communication.

Comparison Summary

- LAN: Smallest scope (rooms/buildings), lowest latency, highest bandwidth, private ownership, Layer 2 switching focus.
- MAN: Medium scope (cities), moderate latency, high bandwidth (often fiber-based), bridging LANs.
- WAN: Massive scope (national/global), higher latency, variable bandwidth, relies on ISP leased infrastructure and complex Layer 3 routing.
- Internet: The ultimate public WAN interconnecting everything, built strictly on TCP/IP and BGP routing.
- Security implementations vary vastly: LANs use simple port security/802.1x, while WANs/Internet require robust firewalls, IPsec VPNs, and BGP route filtering.

Computer Networks (DI03000051)

GTU Diploma Engineering

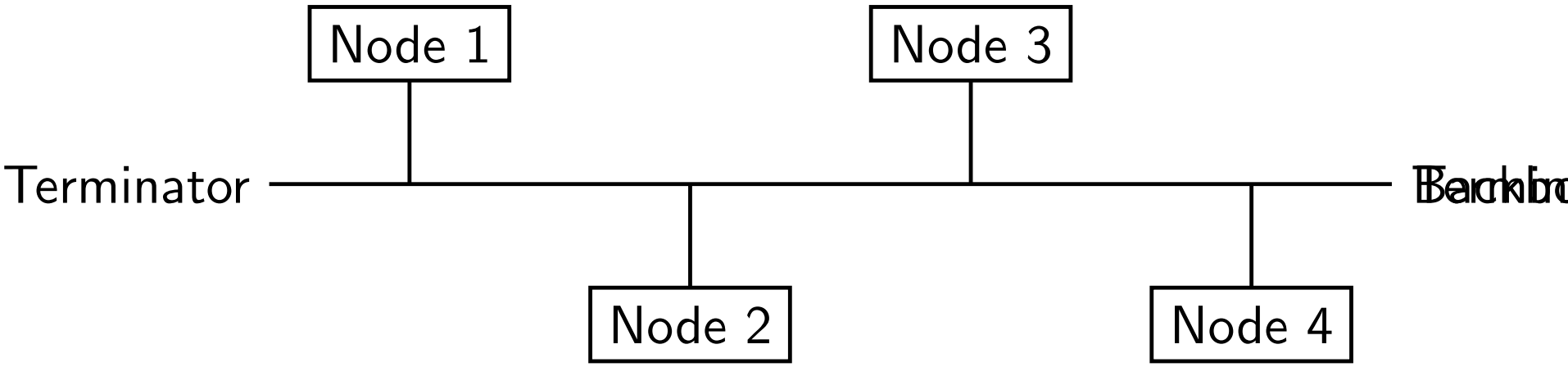
Agenda

- 1. Network Topology: Definition and Use
- 2. Bus Topology
- 3. Star Topology
- 4. Ring Topology
- 5. Mesh Topology
- 6. Tree and Hybrid Topologies

Network Topology: Definition and Use

- Definition: Network topology is the physical or logical arrangement of nodes, devices, and connections in a network.
- Physical Topology: The actual layout of the wire or media (e.g., cables).
- Logical Topology: How data actually flows through the network, regardless of the physical layout.
- Use: Topologies determine the network's performance, scalability, troubleshooting complexity, and cost.

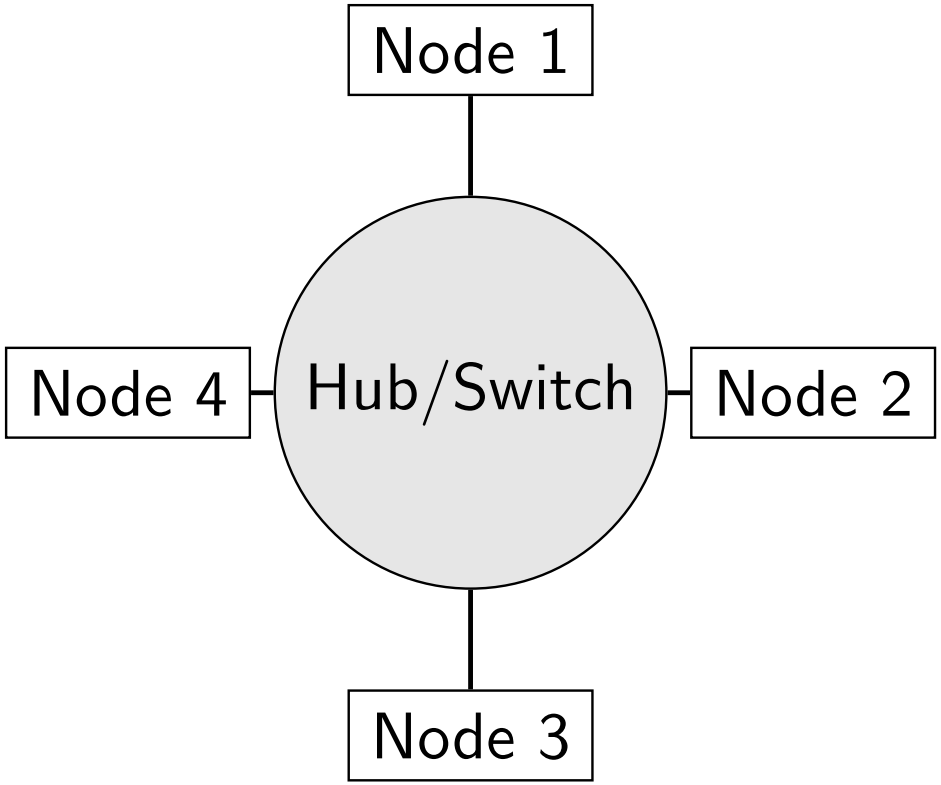
Bus Topology: Architecture



Bus Topology: Advantages and Disadvantages

- Advantages:
- - Easy to connect a computer or peripheral to a linear bus.
- - Requires less cable length than a star topology, making it cost-effective.
- - Works well for small networks.
- Disadvantages:
- - Entire network shuts down if there is a break in the main cable.
- - Terminators are required at both ends of the backbone cable.
- - Difficult to identify the problem if the entire network goes down.
- - Not meant to be used as a stand-alone solution in a large building.

Star Topology: Architecture



Star Topology: Advantages and Disadvantages

- Advantages:
- - Easy to install and wire.
- - No disruptions to the network when connecting or removing devices.
- - Easy to detect faults and to remove parts.
- Disadvantages:
- - Requires more cable length than a linear topology.
- - If the hub, switch, or concentrator fails, nodes attached are disabled.
- - More expensive than linear bus topologies because of the cost of the hubs/switches.

Ring Topology

- Definition: Devices are connected in a closed-loop configuration with adjacent nodes.
- Advantages:
- - Data is transferred quickly, as data only flows in one direction (unidirectional).
- - No need for a network server to control the connectivity between workstations.
- Disadvantages:
- - A single node failure can cause the entire network to fail.
- - Moving, adding, or changing devices can affect the network.
- - Bandwidth is shared on all links between devices.

Mesh Topology

- Definition: Every node is connected to every other node in the network (Full Mesh).
- Advantages:
- - Provides redundant paths; if one connection fails, data can be routed through another.
- - Can handle high amounts of traffic because multiple nodes can transmit data simultaneously.
- - Easy to isolate and diagnose faults.
- Disadvantages:
- - The most expensive topology to implement due to high cable requirements.
- - Setup and maintenance are very difficult.
- - Requires massive amounts of I/O ports on each device.

Tree and Hybrid Topologies

- Tree Topology:
- - Combines characteristics of linear bus and star topologies.
- - Consists of groups of star-configured workstations connected to a linear bus backbone cable.
- - Advantage: Easy expansion of existing networks.
- - Disadvantage: Entire network goes down if the backbone breaks.
- Hybrid Topology:
- - Uses a combination of any two or more topologies in such a way that the resulting network does not exhibit one of the standard topologies.
- - Advantage: Extremely flexible and reliable.
- - Disadvantage: Complex design and high cost of installation.

Computer Networks (DI03000051)

GTU Diploma Engineering

Agenda

- Definition and Concept of Network Topology
- Bus Topology
- Star Topology
- Ring Topology
- Mesh Topology
- Tree and Hybrid Topologies

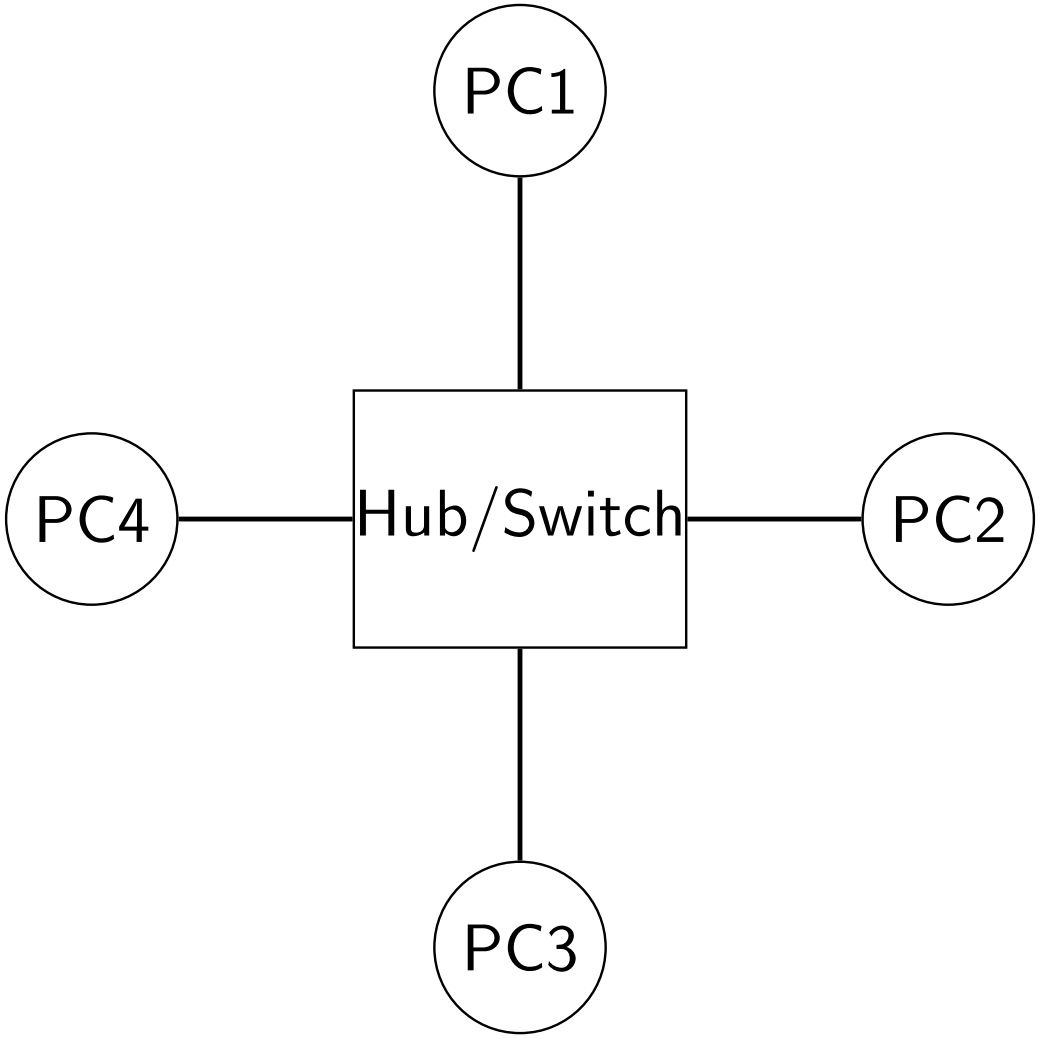
Network Topology: Definition and Use

- A network topology is the physical or logical arrangement of nodes, links, and devices in a network.
- Physical Topology maps the actual physical layout of the cables and devices (e.g., Ethernet cabling in a star shape).
- Logical Topology describes how data actually flows through the network regardless of physical design (e.g., Token Ring passes data logically in a ring even if physically wired as a star).
- Use: Dictates network scalability, fault tolerance, cost of implementation, and ease of troubleshooting.
- Crucial for network administrators during the design phase to align with organizational requirements (e.g., choosing mesh for high redundancy in core routers vs star for end-user LANs).

Bus Topology

- Definition: All devices share a single common communication cable (the backbone or bus) with terminators at both ends to absorb signals.
- Advantage: Very cost-effective and easy to install for small networks. Requires minimal cable length compared to other topologies.
- Advantage: Works well for temporary or small networks (legacy 10Base-2 Thinnet or 10Base-5 Thicknet).
- Disadvantage: Highly vulnerable to backbone failure; a single cable break brings down the entire network segment.
- Disadvantage: Performance degrades under heavy traffic due to collisions (uses CSMA/CD). Difficult to troubleshoot fault locations.

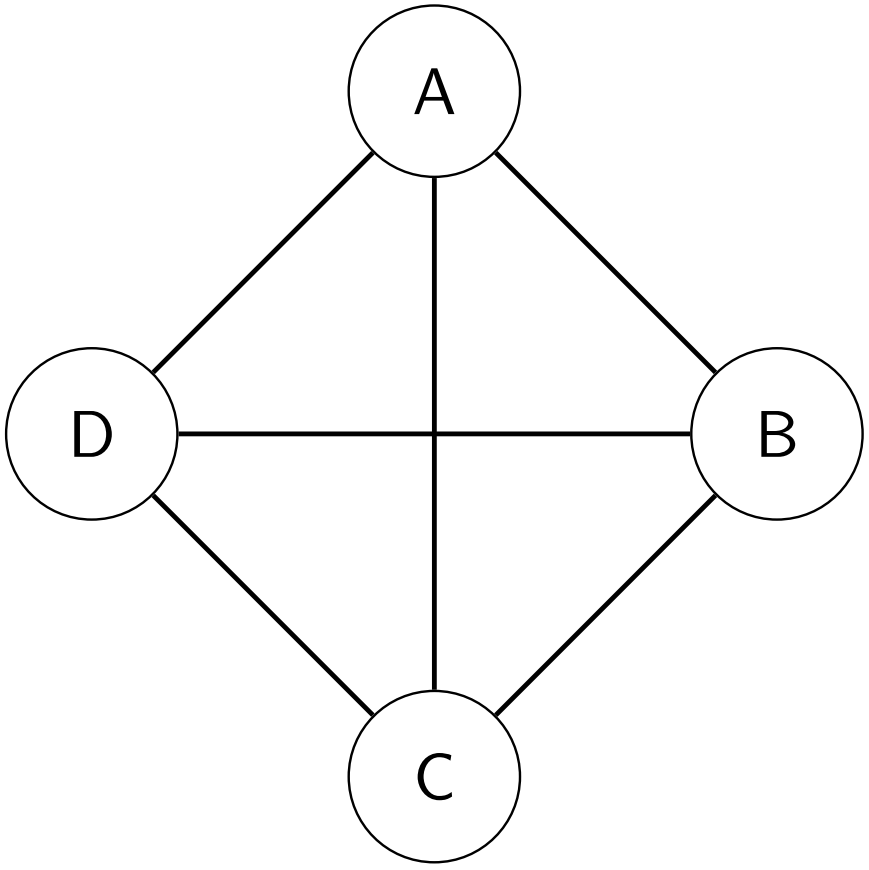
Star Topology Diagram



Ring Topology

- Definition: Each node connects to exactly two other nodes, forming a continuous circular pathway for data. Data travels in one direction (unidirectional) or both (bidirectional/dual-ring).
- Token Passing: Often uses a token-passing mechanism (like IEEE 802.5 Token Ring) to grant transmission rights, eliminating collisions.
- Advantage: Predictable performance and delay. Orderly network where every device has equal access to transmit.
- Disadvantage: In a standard unidirectional ring, one failed node or cable break disables the entire network.
- Disadvantage: Harder to reconfigure or add devices without disrupting current network operations.

Mesh Topology Diagram



Tree Topology

- Definition: A hierarchical topology that integrates multiple star topologies onto a bus or centralized root node.
- Structure: Features a root node (often a high-speed core switch) connected to distribution layer switches, which connect to access layer switches.
- Advantage: Highly scalable and flexible. Enables grouping of devices into subnets or branches, simplifying management and fault isolation.
- Advantage: Supported by most hardware and software providers. Standard for modern corporate LANs.
- Disadvantage: If the core/backbone segment fails, it can fragment the network into isolated segments. Cabling costs can be significant.

Hybrid Topology

- Definition: A combination of two or more different standard topologies (e.g., Star-Bus or Star-Ring) to form a complex, cohesive network.
- Use: Common in large organizations or wide area networks (WANs) that expand and inherit different legacy networks.
- Advantage: Extremely flexible. Can be designed to optimize specific segments according to their needs (e.g., mesh for core servers, star for endpoints).
- Advantage: Scalable and fault-tolerant, depending on the specific combination.
- Disadvantage: Complex administration and design. Troubleshooting can be difficult due to differing hardware and protocols in varying network segments.

Summary

- Network topologies define the physical and logical structure of computer networks.
- Bus is cheap but vulnerable; Star is robust and standard for LANs; Ring offers deterministic access.
- Mesh provides the highest fault tolerance at maximum cost.
- Tree and Hybrid topologies allow for massive scalability in enterprise environments.
- Selection depends on cost, desired reliability, scale, and maintenance capabilities.

Computer Networks (DI03000051)

GTU Diploma Engineering

Agenda

- Introduction to Network Standards
- IEEE (Institute of Electrical and Electronics Engineers)
- ISOC (Internet Society)
- IETF (Internet Engineering Task Force)
- IRTF (Internet Research Task Force)
- ISO (International Organization for Standardization)

The Need for Standards

- Interoperability: Ensures hardware and software from different vendors can communicate seamlessly.
- Market Growth: Promotes a competitive market by preventing vendor lock-in.
- Quality and Reliability: Establishes a baseline for network performance and safety.
- Two types of standards: De facto (by fact/convention) and De jure (by law/regulation).

Key Standard Organizations

- Standards committees coordinate the development of open standards.
- IEEE focuses primarily on physical and data link layer standards.
- ISOC, IETF, and IRTF work primarily on Internet protocols (TCP/IP suite).
- ISO develops comprehensive standards, most notably the OSI reference model.

IEEE: Institute of Electrical and Electronics Engineers

- World's largest technical professional organization dedicated to advancing technology.
- IEEE 802 LAN/MAN Standards Committee develops networking standards.
- IEEE 802.3: Defines the Ethernet standard (CSMA/CD, cabling, physical layers).
- IEEE 802.11: Defines Wireless LAN (WLAN) standards, commonly known as Wi-Fi.
- IEEE 802.15: Defines Wireless PAN standards (e.g., Bluetooth, Zigbee).

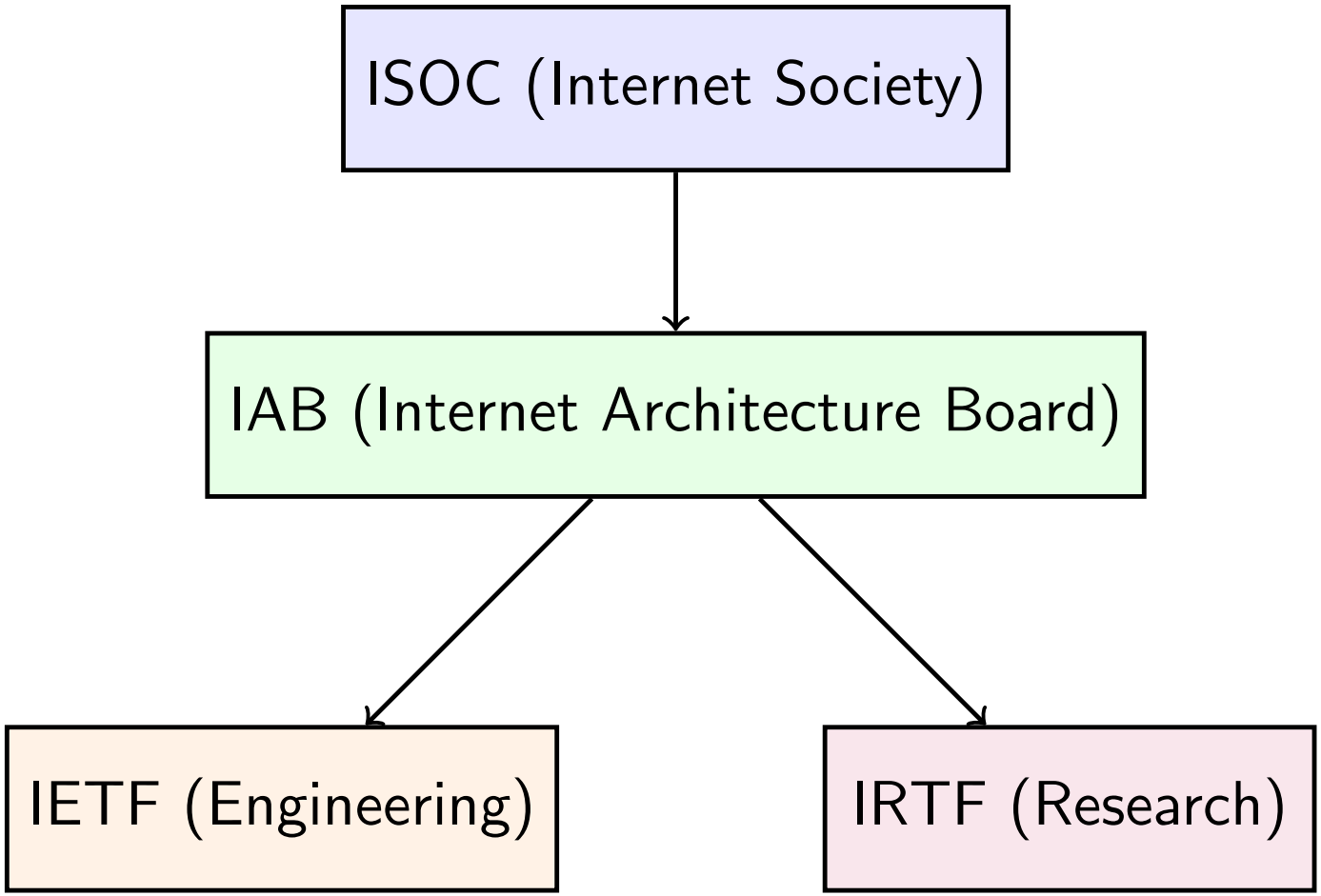
ISOC: Internet Society

- Founded in 1992, ISOC is a non-profit organization that provides leadership in Internet-related standards, education, and policy.
- Promotes the open development, evolution, and use of the Internet for the benefit of all people throughout the world.
- Acts as the organizational home for the Internet Engineering Task Force (IETF), the Internet Architecture Board (IAB), and the Internet Research Task Force (IRTF).

IETF: Internet Engineering Task Force

- The premier Internet standards body, developing open standards through open processes.
- Focuses on short- to medium-term engineering issues related to Internet architecture and protocols.
- Produces Request for Comments (RFC) documents (e.g., IPv4, IPv6, TCP, UDP, HTTP).
- Divided into Working Groups (WGs) categorized by areas such as Routing, Transport, and Security.

Relationship: ISOC, IAB, IETF, IRTF



ISO and the OSI Reference Model

7. Application Layer

6. Presentation Layer

5. Session Layer

4. Transport Layer

3. Network Layer

2. Data Link Layer

1. Physical Layer

Summary and Conclusion

- Standard organizations are crucial for global network interoperability.
- IEEE dominates LAN/WAN physical and link layer standards (802.3, 802.11).
- The Internet protocol suite (TCP/IP) is primarily governed by IETF via RFCs, under the ISOC umbrella.
- IRTF handles long-term research, while IETF handles immediate engineering tasks.
- ISO developed the OSI model, which remains the primary framework for conceptualizing network communications.

Computer Networks (DI03000051)

GTU Diploma Engineering

Agenda

- Introduction to Server Types
- File Server
- Print Server
- Mail Server & Architecture
- Web Server
- Proxy Server Concept & Features

Introduction to Server Types

- A server is a computer hardware or software (computer program) that provides functionality for other programs or devices, called 'clients'.
- This architecture is called the client-server model.
- Servers provide various functionalities, often called 'services', such as sharing data or resources among multiple clients, or performing computation for a client.
- A single server can serve multiple clients, and a single client can use multiple servers.
- Typical physical servers are often headless, meaning they operate without a monitor or input device, managed remotely via SSH or dedicated out-of-band management.

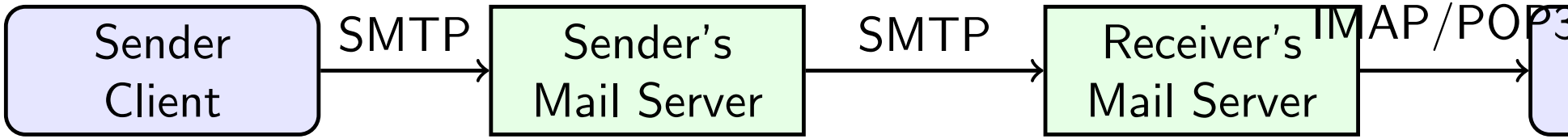
File Server

- A file server is a computer responsible for the central storage and management of data files so that other computers on the same network can access them.
- Key Protocols: Server Message Block (SMB) / Common Internet File System (CIFS) for Windows, Network File System (NFS) for UNIX/Linux, and Apple Filing Protocol (AFP).
- Features: Centralized backup, access control lists (ACLs) for security, quota management, and file locking mechanisms.
- Hardware: Typically features RAID arrays for fault tolerance, high-speed network interfaces (e.g., 10 Gigabit Ethernet), and hot-swappable drives.
- Unlike block-level storage like SAN (Storage Area Network), a file server provides file-level access over a network.

Print Server

- A print server is a software application, network device or computer that manages print requests and makes printer queue status information available to end users and network administrators.
- Features: Spooling print jobs, converting print data formats, enforcing print quotas, and routing print jobs to the appropriate physical printer.
- Protocols: Line Printer Daemon (LPD/LPR), Internet Printing Protocol (IPP) on TCP port 631, and JetDirect (Raw port 9100).
- Print servers abstract the physical printers from the clients, requiring clients only to install a single network driver.
- They also manage user authentication and can pause, cancel, or re-route jobs in the event of hardware failure.

Mail Server Architecture



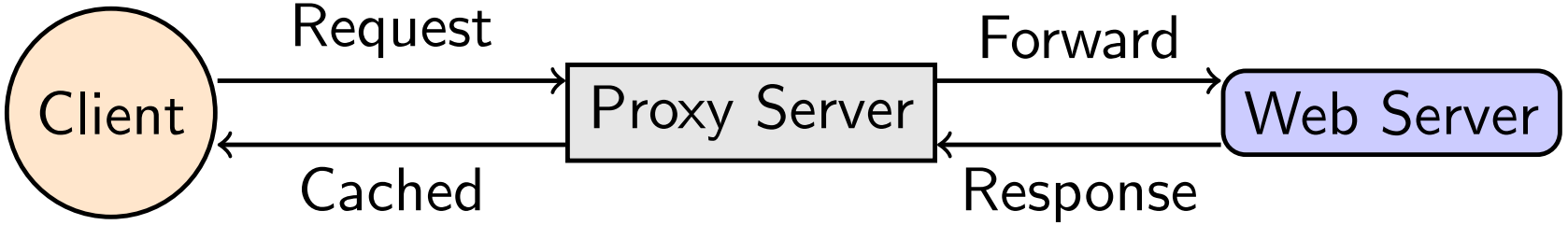
Mail Server Features

- Mail servers (Message Transfer Agents or MTAs) transfer electronic mail messages from one computer to another using client-server application architecture.
- Key Protocols: Simple Mail Transfer Protocol (SMTP) for sending, Post Office Protocol 3 (POP3) and Internet Message Access Protocol (IMAP) for retrieving.
- SMTP operates over TCP port 25 (unencrypted) or 587/465 (secure). POP3 uses 110/995, and IMAP uses 143/993.
- Features: Spam filtering, antivirus scanning, email archiving, and auto-responders.
- Mail servers use DNS MX (Mail Exchanger) records to determine the destination server for a given email domain.

Web Server

- A web server stores, processes, and delivers web pages to clients.
- Protocols: Hypertext Transfer Protocol (HTTP) on port 80 and HTTP Secure (HTTPS) on port 443.
- Common Software: Apache HTTP Server, Nginx, Microsoft Internet Information Services (IIS), and LiteSpeed.
- Features: Virtual hosting (serving multiple websites on one IP address), bandwidth throttling, URL rewriting, and server-side scripting support (CGI, FastCGI).
- Web servers process incoming network requests over HTTP and respond with static content (HTML, images) or dynamic content generated by an application server.

Proxy Server Concept



Proxy Server Features

- A proxy server acts as an intermediary for requests from clients seeking resources from other servers.
- Features: Caching to improve performance, content filtering (blocking access to certain websites), logging, and IP anonymization.
- Types: Forward Proxy (protects the client), Reverse Proxy (protects the server, used for load balancing and SSL termination), and Transparent Proxy.
- Reverse proxies are commonly used in front of web servers to distribute load (e.g., HAProxy, Nginx).
- They enhance security by hiding the internal network structure and filtering out malicious requests before they reach the backend application servers.

Computer Networks (DI03000051)

GTU Diploma Engineering

Agenda

- Introduction to OSI Model
- Upper Layers (Application, Presentation, Session)
- Transport Layer
- Lower Layers (Network, Data Link, Physical)
- Summary and Complete Stack Diagram

Introduction to OSI Reference Model

- OSI (Open Systems Interconnection) is a conceptual model created by ISO in 1984.
- It characterizes and standardizes the communication functions of a computing system without regard to its underlying internal structure.
- The model partitions a communication system into abstraction layers, specifically 7 layers.
- A layer serves the layer above it and is served by the layer below it.

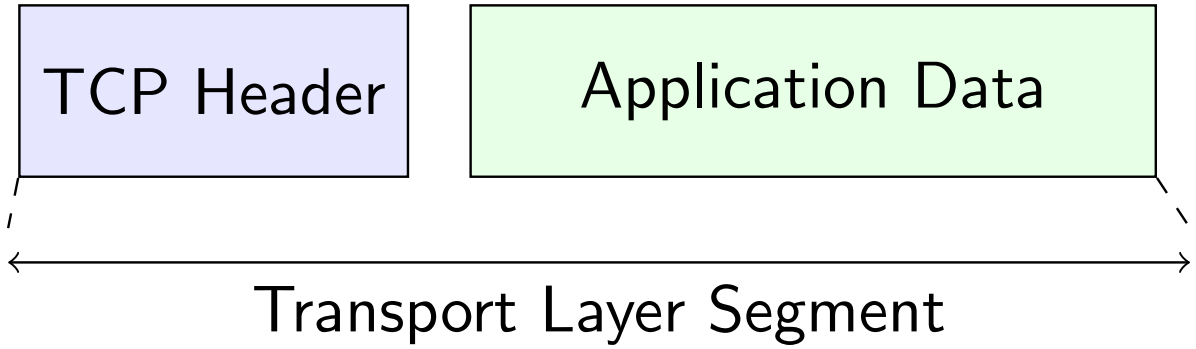
Layer 7: Application Layer

- The Application layer is the closest to the end user.
- Both the OSI application layer and the user interact directly with the software application.
- It provides network services to user applications (e.g., email, file transfer, terminal emulation).
- Common Protocols: HTTP, HTTPS, FTP, SMTP, POP3, DNS, Telnet.

Layers 6 & 5: Presentation and Session

- Presentation Layer (Layer 6): Translates data between the application layer and the network format. Responsible for data encryption/decryption, compression, and character encoding (e.g., ASCII to EBCDIC, SSL/TLS).
- Session Layer (Layer 5): Controls the dialogs (connections) between computers. It establishes, manages, and terminates the connections between the local and remote application.
- Protocols include NetBIOS, RPC, and PPTP.

Layer 4: Transport Layer Encapsulation



Layer 3: Network Layer

- Provides data routing paths for network communication.
- Transfers variable length data sequences (packets) from one node to another connected in different networks.
- Responsible for logical addressing (IP addressing) and determining the best path to the destination (routing).
- Key Protocols: IPv4, IPv6, ICMP, IPSec, OSPF, BGP.

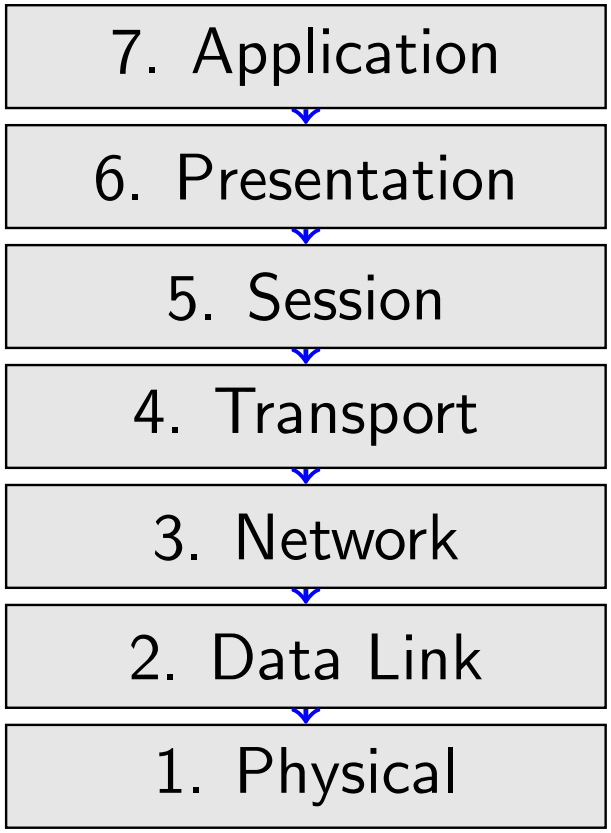
Layer 2: Data Link Layer

- Provides node-to-node data transfer—a link between two directly connected nodes.
- Detects and possibly corrects errors that may occur in the physical layer.
- Divided into two sublayers: MAC (Media Access Control) and LLC (Logical Link Control).
- Key Concepts: MAC Addresses, Frames, Switches.
- Key Protocols: Ethernet (IEEE 802.3), Wi-Fi (IEEE 802.11), PPP, ARP.

Layer 1: Physical Layer

- Defines the electrical and physical specifications of the data connection.
- It dictates the relationship between a device and a physical transmission medium (e.g., copper or optical cable).
- Transmits raw bit stream (0s and 1s) over the physical medium.
- Key Concepts: Hubs, Repeaters, Cables, Voltages, Radio Frequencies.

Complete OSI Model Diagram



Computer Networks (DI03000051)

GTU Diploma Engineering

Agenda

- Introduction to the OSI Reference Model
- Layer 1: Physical Layer
- Layer 2: Data Link Layer
- Layer 3: Network Layer
- Layer 4: Transport Layer
- Layers 5-7: Session, Presentation, Application Layers
- Data Encapsulation and Decapsulation

Introduction to the OSI Model

- The Open Systems Interconnection (OSI) model is a conceptual framework created by ISO in 1984.
- It characterizes and standardizes the communication functions of a telecommunication or computing system without regard to its underlying internal structure and technology.
- The model partitions a communication system into abstraction layers. The original version of the model defined seven layers.
- Benefits include standardizing network components to allow multiple-vendor development, troubleshooting by isolating network problems to specific layers, and preventing changes in one layer from affecting other layers.

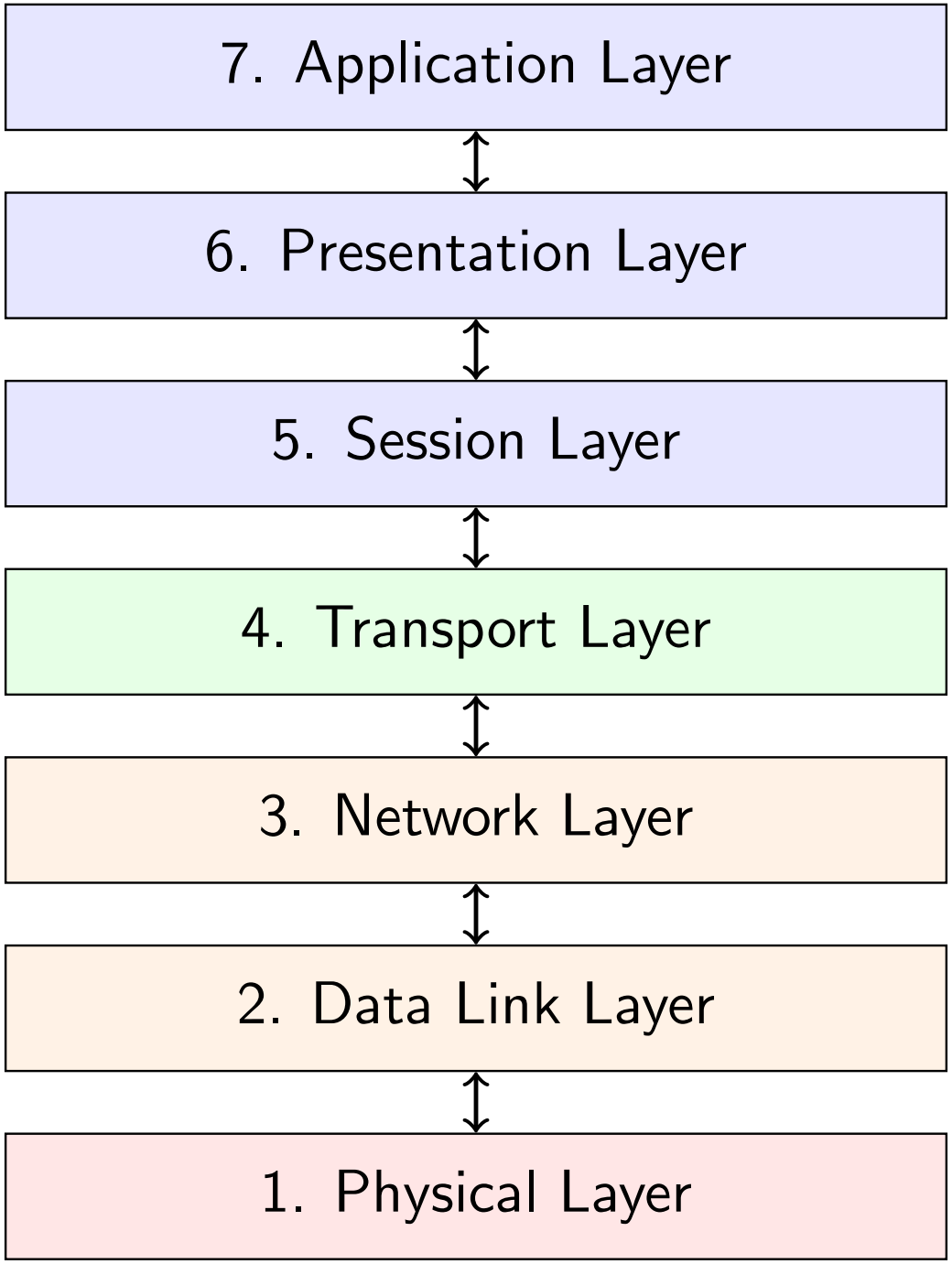
Layer 1: Physical Layer

- The Physical Layer is responsible for the transmission and reception of unstructured raw data between a device and a physical transmission medium.
- It converts the digital bits into electrical, radio, or optical signals.
- Key functions: Bit synchronization, bit rate control, physical topologies (bus, star, mesh), and transmission mode (simplex, half-duplex, full-duplex).
- Hardware components: Cables (Ethernet, fiber optic), Hubs, Repeaters, Network Interface Cards (NICs), Modems.

Layer 2: Data Link Layer

- The Data Link Layer provides node-to-node data transfer and handles error correction from the physical layer.
- It is divided into two sublayers: Logical Link Control (LLC) for multiplexing protocols and framing, and Media Access Control (MAC) for dealing with media access and physical addressing.
- Protocol Data Unit (PDU): Frame.
- Key functions: Framing, Physical addressing (MAC address), Flow control, Error control (CRC, checksum), and Access control (CSMA/CD).
- Hardware devices: Switches, Bridges.

Diagram: The 7 Layers of the OSI Model



Layer 3: Network Layer

- The Network Layer is responsible for packet forwarding including routing through intermediate routers.
- It manages multi-node network architectures, logical addressing (IP addresses), and translates logical addresses to MAC addresses (via ARP).
- Protocol Data Unit (PDU): Packet.
- Key functions: Routing (OSPF, BGP, RIP), Logical addressing (IPv4, IPv6), Subnetting, and Fragmentation of packets.
- Hardware devices: Routers, Layer 3 Switches.

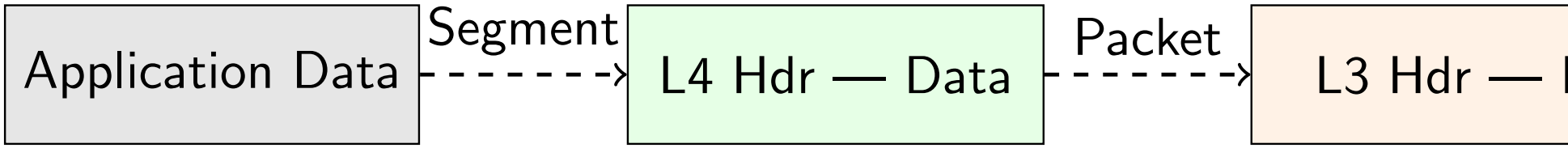
Layer 4: Transport Layer

- The Transport Layer provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers.
- It controls the reliability of a given link through flow control, segmentation/desegmentation, and error control.
- Protocol Data Unit (PDU): Segment (TCP) or Datagram (UDP).
- Key Protocols: TCP (Transmission Control Protocol) for connection-oriented reliable transmission, and UDP (User Datagram Protocol) for connectionless, fast, but unreliable transmission.
- Functions: Service-point addressing (Port numbers), Segmentation and reassembly, Connection control, Multiplexing.

Layers 5, 6, and 7: The Upper Layers

- Layer 5 (Session Layer): Controls the dialogues (connections) between computers. It establishes, manages, and terminates the connections between the local and remote application. Handles duplex/half-duplex operation and synchronization points.
- Layer 6 (Presentation Layer): Transforms data to provide a standard interface for the application layer. Responsible for Data Translation (EBCDIC to ASCII), Data Encryption/Decryption (SSL/TLS), and Data Compression.
- Layer 7 (Application Layer): Closest to the end user. Interfaces directly with software applications. Provides network services to the applications. Examples: HTTP, FTP, SMTP, DNS, SSH.

Diagram: Data Encapsulation Process



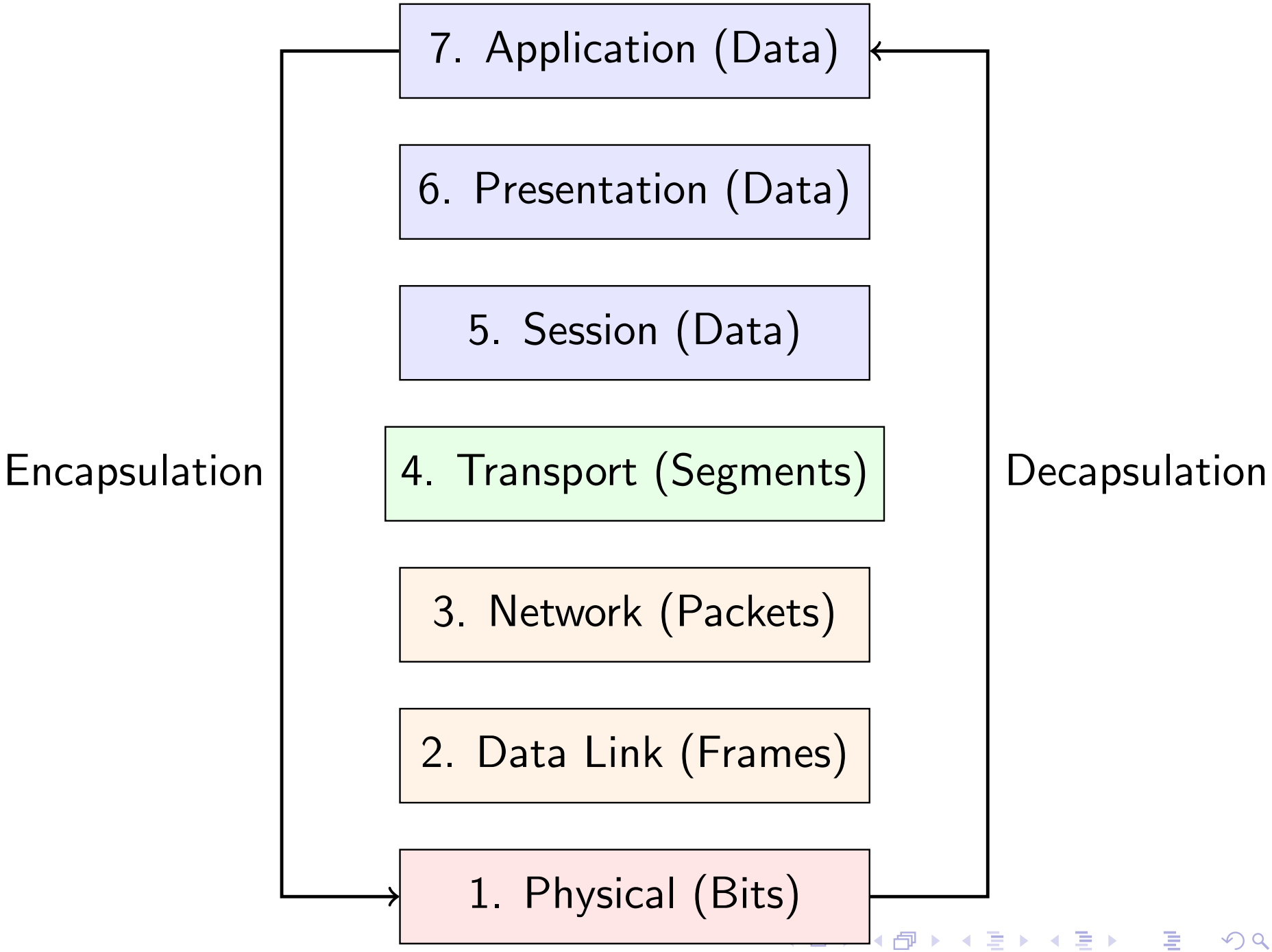
Computer Networks (DI03000051)

GTU Diploma Engineering

Agenda

- Introduction to the OSI Reference Model
- The 7 Layers of the OSI Model
- Functions of Layers 1 to 4 (Data Flow)
- Functions of Layers 5 to 7 (Application)
- Data Encapsulation and Decapsulation
- Visualizing the Stack (Diagrams)

The OSI Model Stack Diagram



Layer 1: Physical Layer

- Function: Transmits raw bit stream over a physical medium.
- Responsibilities: Defines physical topology, signal types (electrical, optical, radio), bit synchronization, and multiplexing.
- PDU (Protocol Data Unit): Bits.
- Devices: Hubs, Repeaters, Cables, NICs (transceiver portion).
- Protocols/Standards: IEEE 802.3 (Ethernet physical), USB, Bluetooth (PHY).

Layer 2: Data Link Layer

- Function: Provides node-to-node data transfer and handles error correction from the physical layer.
- Sublayers: Logical Link Control (LLC) for multiplexing, and Media Access Control (MAC) for addressing and channel access.
- Responsibilities: MAC addressing (physical addressing), framing, error detection (FCS/CRC).
- PDU: Frames.
- Devices: Switches, Bridges.
- Protocols: Ethernet (IEEE 802.3 MAC), PPP, Frame Relay, VLANs (802.1Q).

Layer 3: Network Layer

- Function: Routes data from one node to another on different networks.
- Responsibilities: Logical addressing (IP addresses), routing, subnetting, and fragmentation.
- PDU: Packets (or Datagrams).
- Devices: Routers, Layer 3 Switches.
- Protocols: IPv4, IPv6, ICMP (Ping), IPsec, OSPF, BGP.

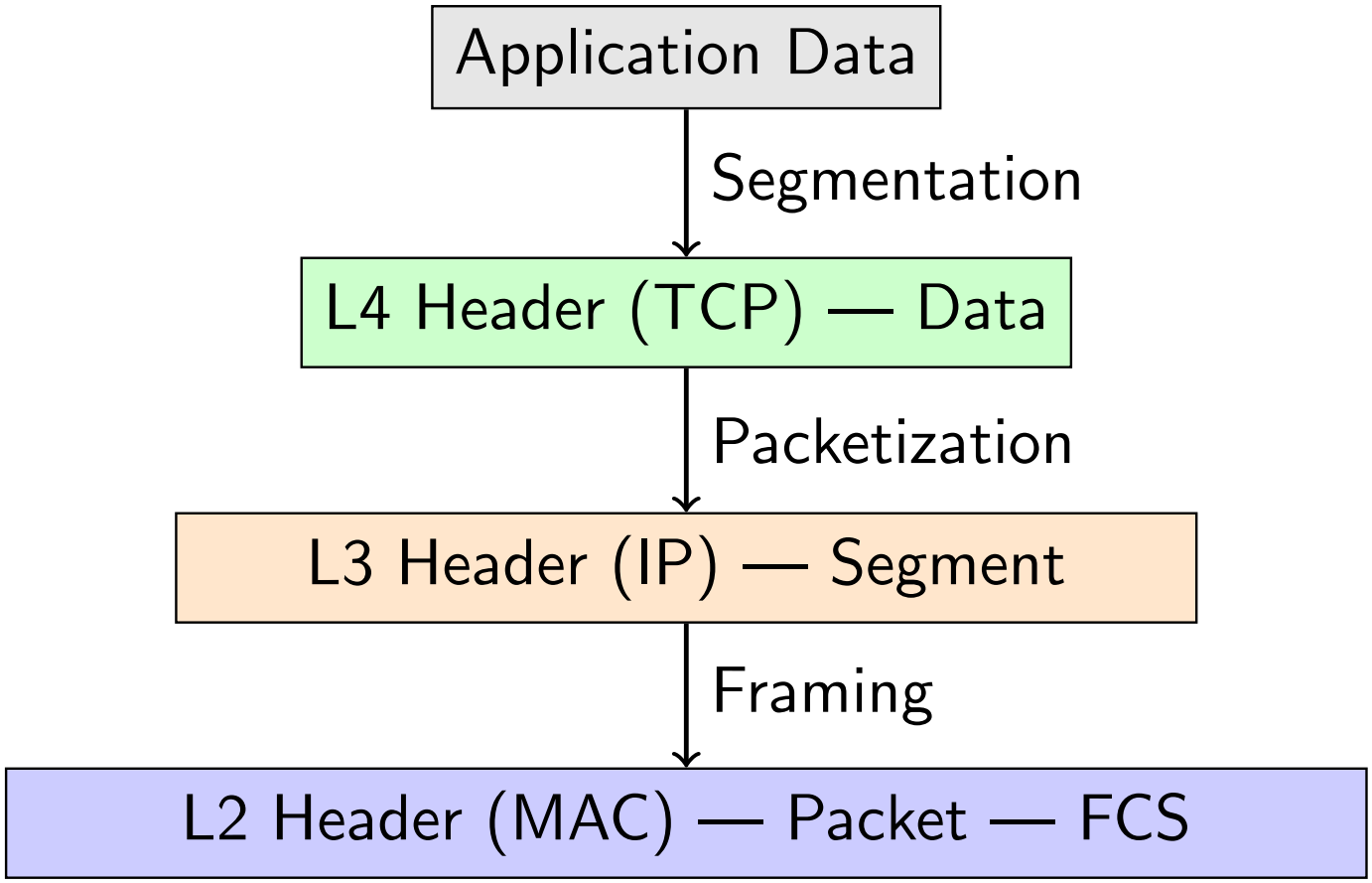
Layer 4: Transport Layer

- Function: Ensures complete data transfer and provides end-to-end communication control.
- Responsibilities: Segmentation and reassembly, connection multiplexing (using port numbers), reliability (TCP), and flow control (windowing).
- PDU: Segments (TCP) or Datagrams (UDP).
- Connection-oriented vs Connectionless: TCP provides reliable delivery (3-way handshake); UDP provides fast, best-effort delivery.
- Protocols: TCP, UDP, SCTP.

Upper Layers: Session, Presentation, Application

- Layer 5 (Session): Establishes, maintains, and terminates communication sessions. Controls half/full-duplex operations. Protocols: NetBIOS, RPC.
- Layer 6 (Presentation): Transforms data formats to provide a standard interface for the Application layer. Handles encryption, decryption, and compression. Protocols: TLS/SSL, JPEG, ASCII.
- Layer 7 (Application): Closest to the end user. Provides network services to user applications. Identifies communication partners and synchronizes communication.
- Layer 7 Protocols: HTTP/HTTPS, DNS, SMTP, FTP, SSH.

Data Encapsulation Flow Diagram



Summary & Conclusion

- The OSI model is a conceptual framework defining how network protocols interact and communicate.
- It consists of 7 distinct layers: Application, Presentation, Session, Transport, Network, Data Link, and Physical.
- Data flows down the stack during transmission (Encapsulation) and up the stack upon receipt (Decapsulation).
- Understanding OSI is crucial for network troubleshooting and isolating faults to specific hardware or software layers.

Computer Networks (DI03000051)

GTU Diploma Engineering

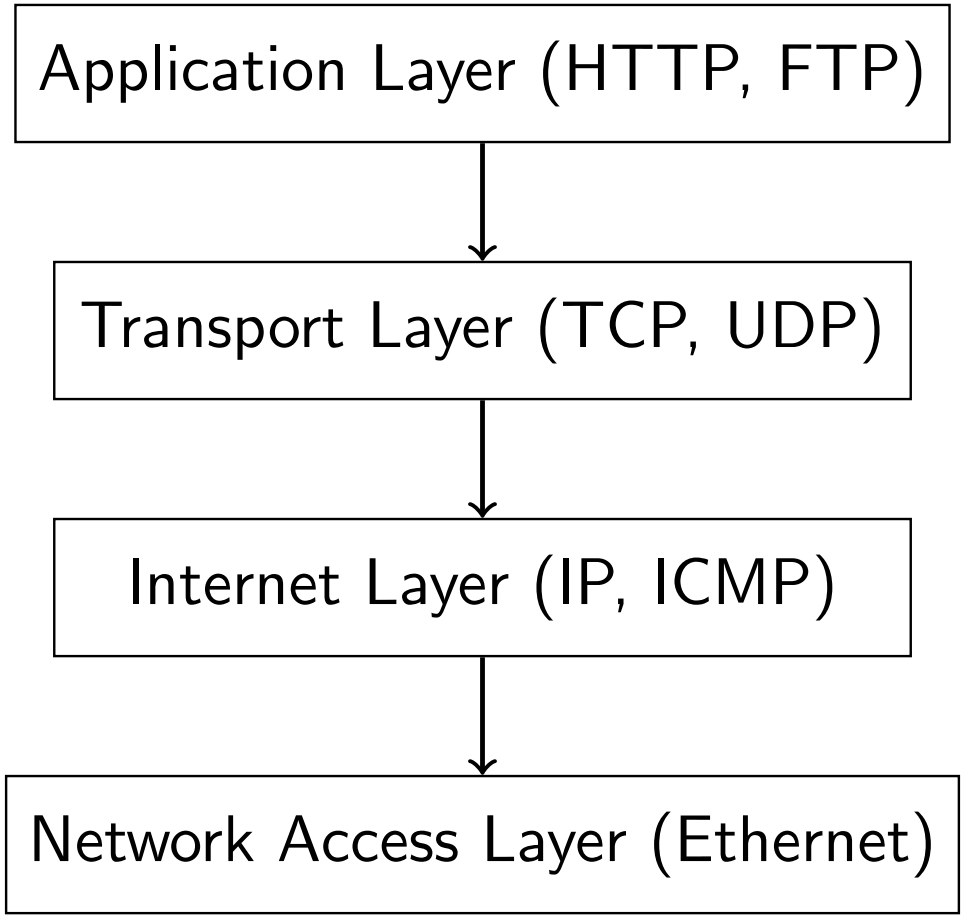
Agenda

- Introduction to the TCP/IP Model
- Layered Architecture and Functions
- Application and Transport Layers
- Internet and Network Access Layers
- Data Encapsulation Process

Introduction to TCP/IP Model

- Developed by the Department of Defense (DoD) in the 1970s for ARPANET.
- Provides end-to-end connectivity specifying how data should be packetized, addressed, transmitted, routed, and received.
- Unlike the theoretical OSI model, TCP/IP is a practical, protocol-oriented standard.
- Usually represented as a 4-layer model (DoD model), but often mapped to 5 layers for easier comparison with OSI.

TCP/IP Model Architecture



Application Layer

- The highest layer in the TCP/IP suite, combining OSI's Application, Presentation, and Session layers.
- Provides network services directly to user applications.
- Handles high-level protocols, issues of representation, encoding, and dialog control.
- Key Protocols: HTTP/HTTPS (Web), SMTP/POP3/IMAP (Email), FTP (File Transfer), DNS (Name Resolution), DHCP (IP Configuration).

Transport Layer

- Ensures logical communication between application processes running on different hosts.
- Provides multiplexing/demultiplexing using port numbers to distinguish multiple applications.
- Transmission Control Protocol (TCP): Connection-oriented, reliable delivery, error checking, flow control (sliding window), and congestion control.
- User Datagram Protocol (UDP): Connectionless, best-effort delivery, no reliability guarantees, low latency (ideal for streaming/gaming).

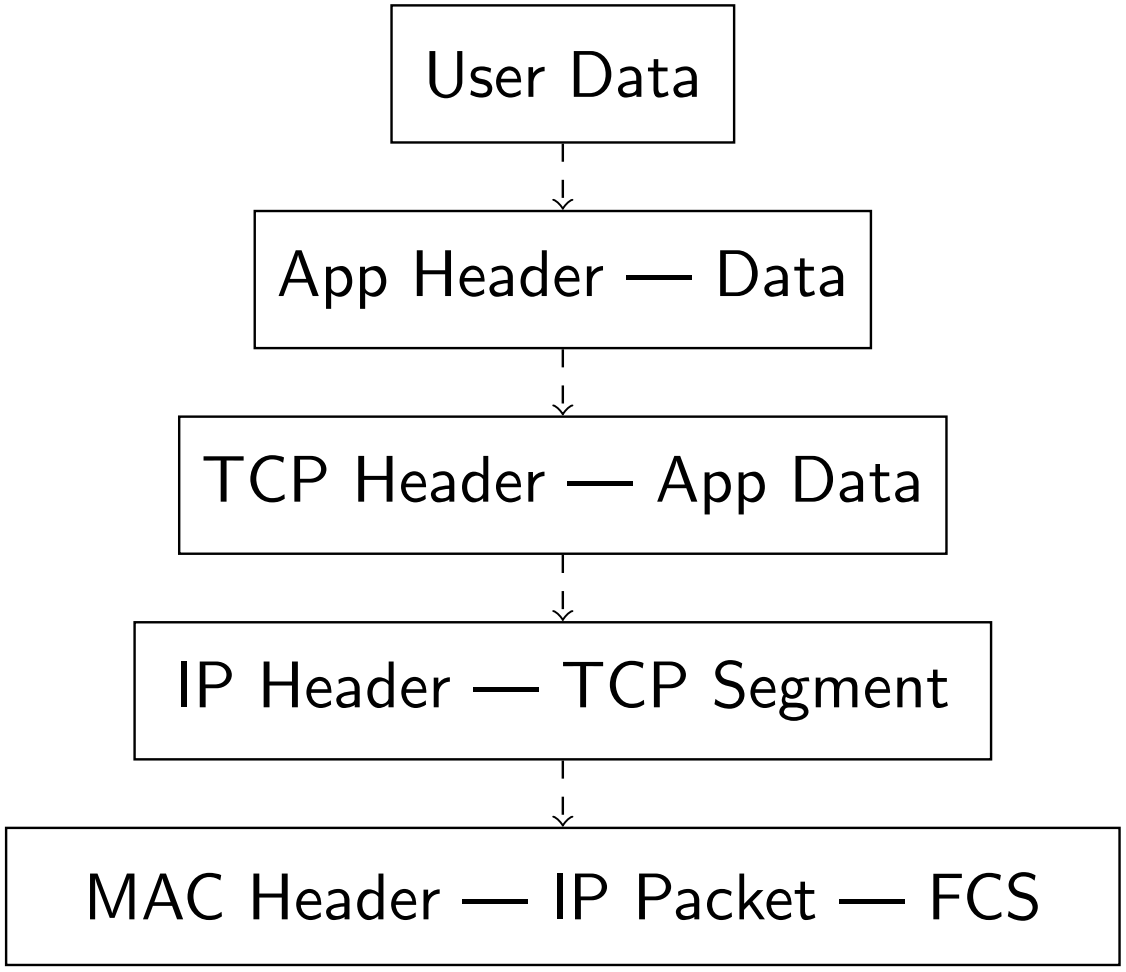
Internet Layer

- Equivalent to the OSI Network layer. Responsible for logical addressing and routing packets across multiple networks.
- Internet Protocol (IP): Defines IP addresses (IPv4/IPv6), encapsulates transport layer segments into IP datagrams, handles routing.
- Internet Control Message Protocol (ICMP): Used for network diagnostics and error reporting (e.g., ping, traceroute).
- Address Resolution Protocol (ARP): Maps logical IP addresses to physical MAC addresses on a local network.

Network Access Layer

- Corresponds to OSI Data Link and Physical layers. Defines how data is physically sent through the network.
- Responsible for node-to-node frame delivery on the same physical network.
- Handles MAC (Media Access Control) addressing, framing, and physical medium transmission.
- Common technologies: Ethernet (802.3), Wi-Fi (802.11), Point-to-Point Protocol (PPP), Frame Relay.

Data Encapsulation Process



Summary

- TCP/IP is a pragmatic, 4-layer architecture foundational to the modern Internet.
- Application Layer: User interface and high-level protocols.
- Transport Layer: End-to-end communication and reliability (TCP) or speed (UDP).
- Internet Layer: Logical addressing (IP) and best-path routing.
- Network Access Layer: Physical transmission and hardware addressing (MAC).

Computer Networks (DI03000051)

GTU Diploma Engineering

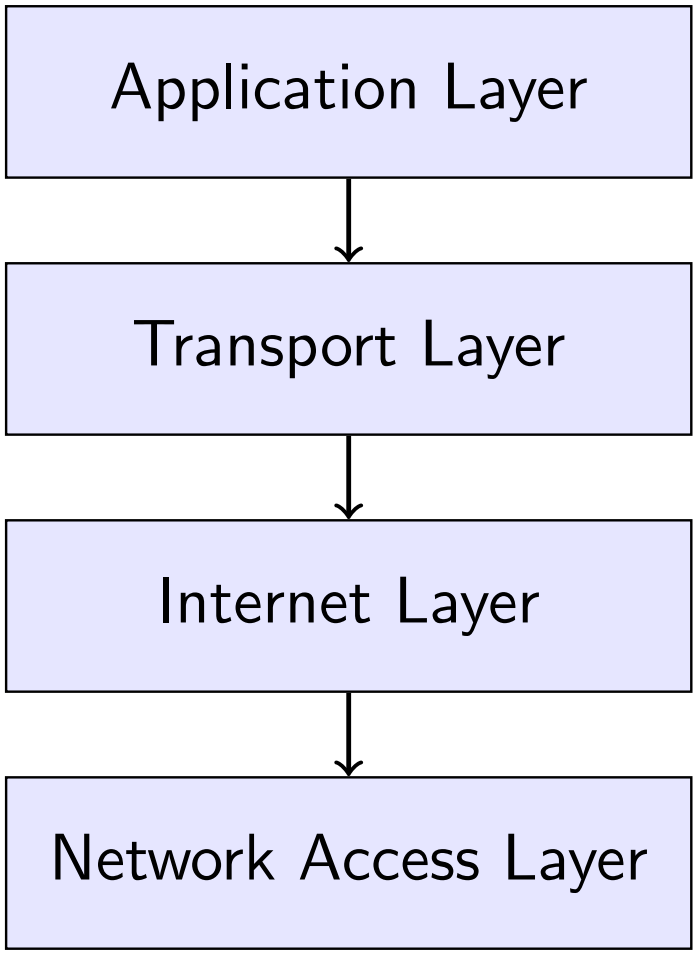
Agenda

- Introduction to the TCP/IP Model
- The Four Layers of TCP/IP
- Application Layer
- Transport Layer
- Internet Layer
- Network Access Layer
- Data Encapsulation Process
- Comparison with the OSI Model

Introduction to the TCP/IP Model

- Developed by the Department of Defense (DoD) in the 1970s for ARPANET.
- A concise, practical protocol suite that became the foundation of the modern Internet.
- Follows a 4-layer architecture, unlike the 7-layer theoretical OSI reference model.
- Provides end-to-end connectivity specifying how data should be packetized, addressed, transmitted, routed, and received.
- Highly robust, designed to dynamically route around network failures and differing physical networks.

The Four Layers of TCP/IP



Application Layer

- The highest layer in the TCP/IP model, interacting directly with software applications.
- Combines the functions of the OSI model's Application, Presentation, and Session layers.
- Responsible for node-to-node application communication, formatting, and providing user services.
- Common protocols include: HTTP/HTTPS (web), FTP (file transfer), SMTP/IMAP (email), DNS (name resolution), and SSH.
- Data produced here is passed down to the Transport layer in the form of messages or streams.

Transport Layer

- Provides end-to-end data delivery services and establishes logical connections between hosts.
- The primary protocols operating here are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).
- TCP is connection-oriented, providing reliable delivery, error checking, flow control (windowing), and sequencing.
- UDP is connectionless, providing faster but unreliable delivery with minimal overhead (often used for streaming, DNS, gaming).
- Uses logical port numbers (e.g., 80 for HTTP, 443 for HTTPS) to multiplex data to the correct application process.

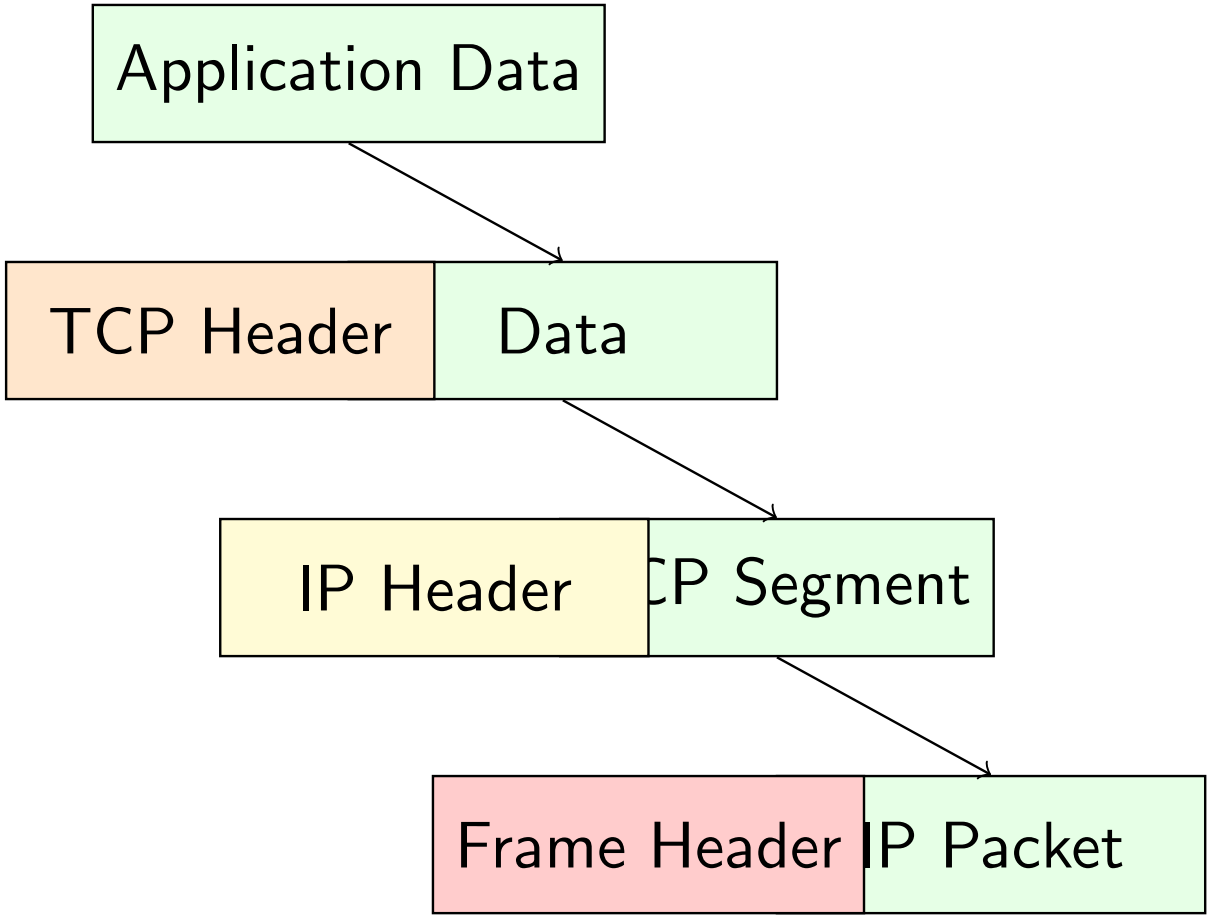
Internet Layer

- Also known as the Network layer; handles the routing of packets across independent networks.
- The core protocol is IP (Internet Protocol - IPv4 and IPv6), which provides logical addressing and routing.
- Other key protocols include ICMP (Internet Control Message Protocol) for diagnostics like ping and traceroute, and IGMP for multicasting.
- Data units at this layer are called IP datagrams or packets.
- IP provides best-effort, connectionless delivery; it does not guarantee delivery, sequence, or error recovery.

Network Access Layer

- Also referred to as the Link layer or Network Interface layer.
- Defines how data is physically sent through the network medium (copper cables, fiber optics, wireless).
- Combines the Data Link and Physical layers of the OSI model.
- Responsible for MAC (Media Access Control) addressing, hardware mapping (via ARP), and framing data for physical transmission.
- Examples of standards/protocols operating here: Ethernet (IEEE 802.3), Wi-Fi (IEEE 802.11), and PPP (Point-to-Point Protocol).

Data Encapsulation in TCP/IP



Comparison with the OSI Model

- TCP/IP has 4 layers, while the OSI model has 7 distinct layers.
- TCP/IP's Application layer maps to the OSI's Application, Presentation, and Session layers.
- TCP/IP's Network Access layer maps to the OSI's Data Link and Physical layers.
- TCP/IP is a practical, implementation-first model based on standard protocols used on the Internet, whereas OSI is a theoretical reference model.
- TCP/IP supports only connectionless communication in the network layer (IP), but supports both connectionless and connection-oriented in the transport layer.

Computer Networks (DI03000051)

GTU Diploma Engineering

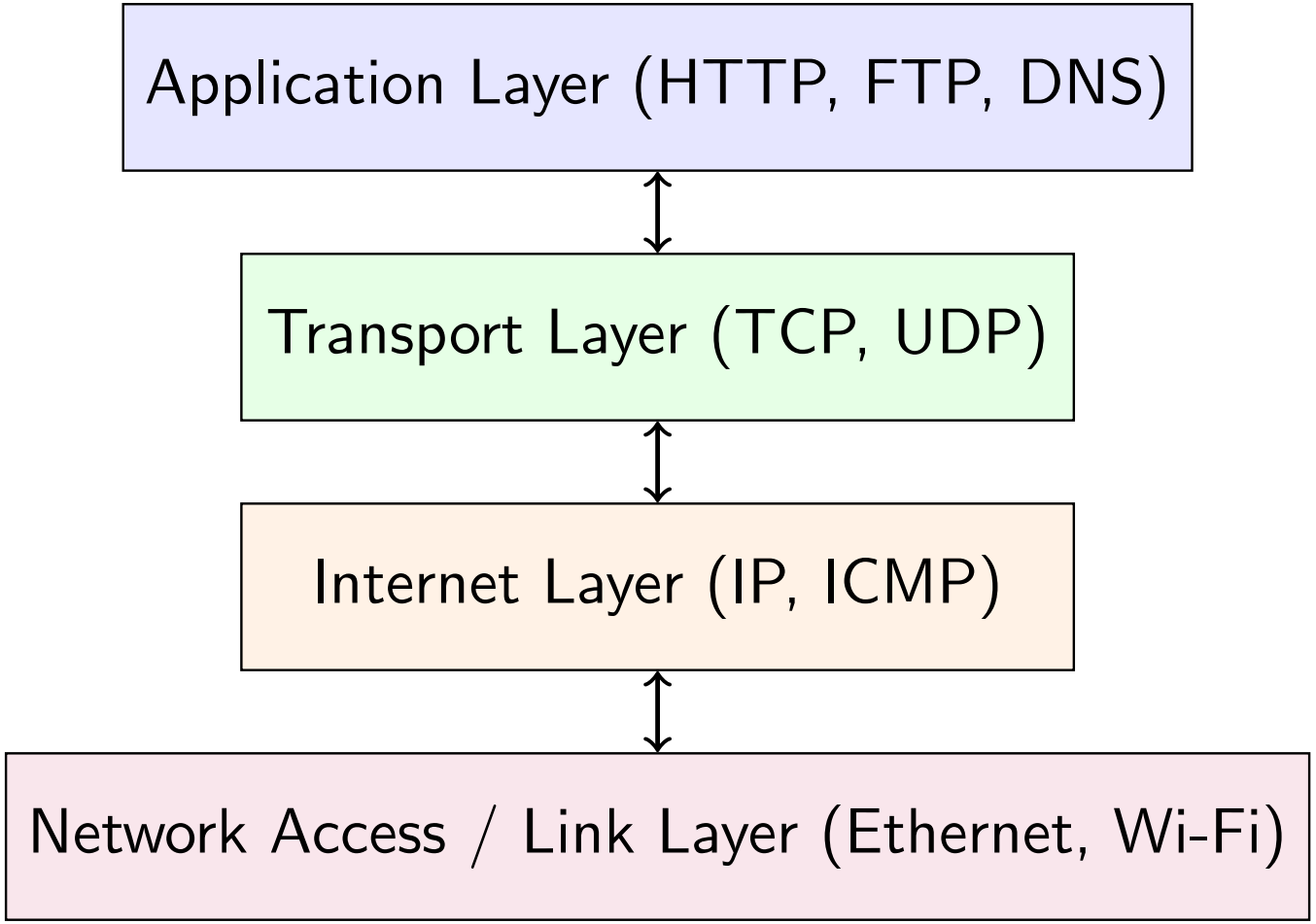
Agenda

- Introduction to the TCP/IP Model
- The 4-Layer Architecture (Diagram)
- Link/Network Access Layer
- Internet Layer
- Transport Layer
- Application Layer
- Data Encapsulation (Diagram)
- Comparison with the OSI Model

Introduction to the TCP/IP Model

- The Transmission Control Protocol/Internet Protocol (TCP/IP) model is a conceptual model and set of communications protocols used in the Internet and similar computer networks.
- Developed by the Department of Defense (DoD) in the 1970s via the ARPANET project, predating the OSI model.
- It focuses heavily on robustness, allowing communications to survive network failures.
- Unlike the 7-layer OSI model, the original TCP/IP model defines a 4-layer architecture.

TCP/IP 4-Layer Architecture



Network Access / Link Layer

- Lowest layer of the TCP/IP model, analogous to the OSI Physical and Data Link layers.
- Defines how data is physically sent through the network, including hardware addressing (MAC addresses) and frame formatting.
- Handles the translation of logical IP packets into physical frames suitable for the transmission medium (e.g., Ethernet, Wi-Fi).
- Protocols and standards include Ethernet (IEEE 802.3), Wi-Fi (IEEE 802.11), ARP (Address Resolution Protocol), and Point-to-Point Protocol (PPP).

Internet Layer

- Corresponds to the OSI Network layer. It is responsible for logical transmission of packets over the entire network.
- Handles addressing, packaging, and routing functions. Packets may traverse multiple routers from source to destination.
- Core protocol: Internet Protocol (IP). IP is a connectionless, best-effort delivery protocol.
- Other key protocols: ICMP (Internet Control Message Protocol) for diagnostics like ping, and IGMP (Internet Group Management Protocol) for multicasting.

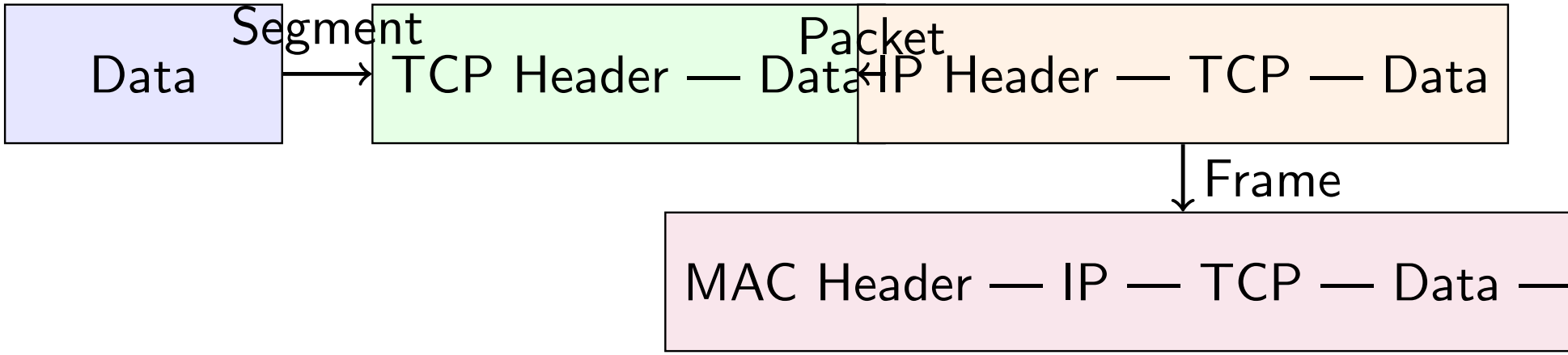
Transport Layer

- Provides end-to-end communication services for applications. Equivalent to the OSI Transport layer.
- Responsible for multiplexing via port numbers (e.g., Port 80 for HTTP, Port 443 for HTTPS), allowing multiple applications to communicate simultaneously.
- TCP (Transmission Control Protocol): Provides reliable, connection-oriented delivery with error checking, sequencing, and flow control. Uses a 3-way handshake.
- UDP (User Datagram Protocol): Provides unreliable, connectionless delivery. Faster, with less overhead, suitable for streaming or VoIP.

Application Layer

- Highest layer in the TCP/IP model, combining the functions of OSI Application, Presentation, and Session layers.
- Interacts directly with software applications, providing network services to the user.
- Handles data formatting, encryption, and dialogue control.
- Common protocols: HTTP/HTTPS (Web), SMTP/IMAP (Email), FTP (File Transfer), SSH (Secure Shell), and DNS (Domain Name System).

Data Encapsulation Process



TCP/IP vs. OSI Model

- Architecture: OSI is a 7-layer model; TCP/IP is a 4-layer model.
- Development: OSI was developed theoretically before protocols were invented; TCP/IP was developed empirically based on existing protocols.
- Strictness: OSI has strict boundaries between layers (services, interfaces, protocols are clearly distinguished); TCP/IP is more pragmatic and less strict.
- Network Layer Support: OSI supports both connectionless and connection-oriented communication in the network layer, but only connection-oriented in the transport layer. TCP/IP has only connectionless at the network layer, but supports both in the transport layer.

Computer Networks (DI03000051)

GTU Diploma Engineering

Agenda

- 1. Introduction to Reference Models
- 2. Overview of the OSI Model
- 3. Overview of the TCP/IP Model
- 4. Visual Comparison of the Models
- 5. Key Similarities
- 6. Key Differences
- 7. The Encapsulation Process
- 8. Summary and Conclusion

Introduction to Reference Models

- Reference models provide a conceptual framework for standardizing communication between heterogeneous network systems.
- They break down the complex process of networking into more manageable, standardized layers.
- The two most prominent models in computer networking are the Open Systems Interconnection (OSI) model and the Transmission Control Protocol/Internet Protocol (TCP/IP) model.
- While OSI is a generic, protocol-independent standard, TCP/IP is a practical, protocol-oriented architecture upon which the modern Internet is built.

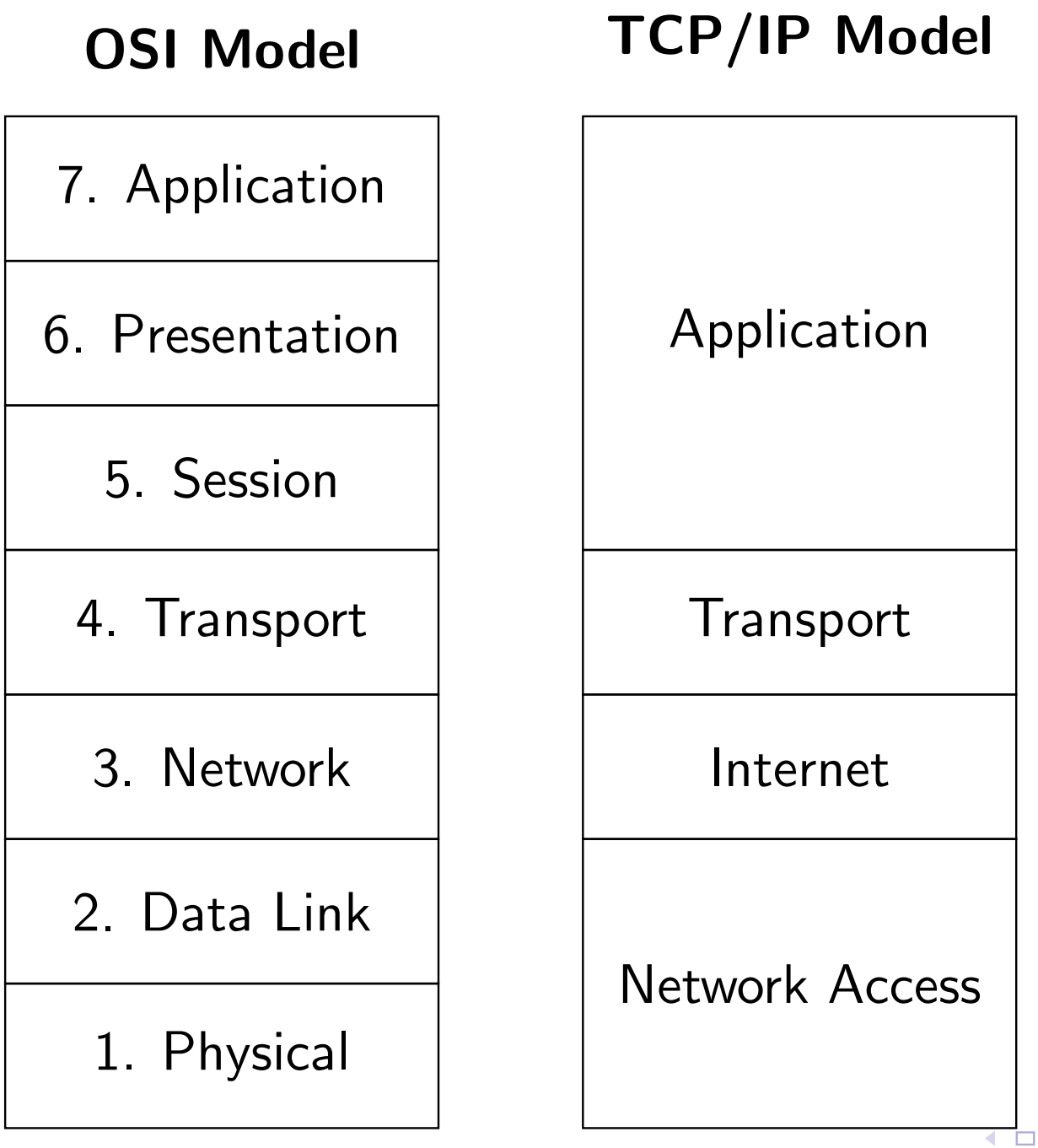
Overview of the OSI Model

- Developed by the International Organization for Standardization (ISO) in 1984.
- Consists of 7 distinct layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.
- Strictly separates the concepts of services, interfaces, and protocols, offering a highly modular approach.
- Operates as a theoretical model for teaching and understanding network functions, rather than a widely implemented protocol suite.

Overview of the TCP/IP Model

- Developed by the Department of Defense (DoD) in the 1970s for ARPANET.
- Consists of 4 layers: Network Access (or Link), Internet, Transport, and Application.
- Does not strictly distinguish between services, interfaces, and protocols, focusing instead on practical implementation and robustness.
- The de facto standard framework of the Internet, utilizing well-known protocols like IP, TCP, UDP, and HTTP.

Visual Comparison of the Models



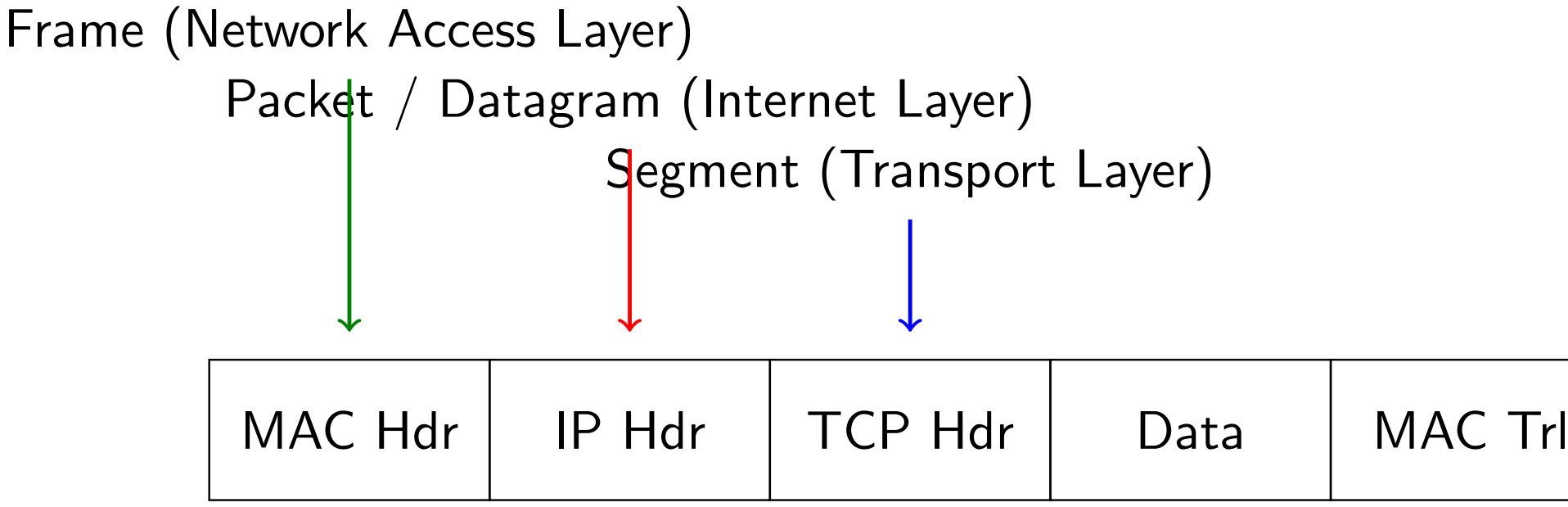
Key Similarities

- Both models use a layered architecture to simplify network design and troubleshooting.
- Both have roughly comparable Transport and Network (or Internet) layers.
- Both assume a packet-switched network architecture rather than circuit-switching.
- Both models rely on the concept of encapsulation and decapsulation as data moves up and down the stack.

Key Differences

- Layer Count: OSI has 7 layers, while TCP/IP has 4 layers. The OSI Session and Presentation layers are absorbed into the TCP/IP Application layer.
- Network Layer Support: The OSI Network layer supports both connectionless and connection-oriented communication, whereas the TCP/IP Internet layer is exclusively connectionless (IP).
- Transport Layer Support: The OSI Transport layer guarantees delivery (connection-oriented), whereas TCP/IP offers both connection-oriented (TCP) and connectionless (UDP) options.
- Standardization: OSI was standardized before protocols were developed, leading to complex implementations. TCP/IP protocols were developed first, making the model a description of existing protocols.

The Encapsulation Process in TCP/IP



Summary and Conclusion

- The OSI model provides an excellent theoretical framework for understanding network operations, but it proved too complex for widespread implementation.
- The TCP/IP model, while theoretically less rigorous, became the foundation of the Internet due to its practical, protocol-first approach and robustness.
- Understanding both models is essential for network engineers: TCP/IP for practical configuration and troubleshooting, and OSI for theoretical discussions and vendor-neutral terminology.

Computer Networks (DI03000051)

GTU Diploma Engineering

Agenda

- 1. Overview of the OSI Model
- 2. Overview of the TCP/IP Model
- 3. Architectural Comparison
- 4. Key Differences in Layering and Protocols
- 5. Encapsulation and Decapsulation
- 6. Advantages and Disadvantages of each model
- 7. Why TCP/IP became the de facto standard

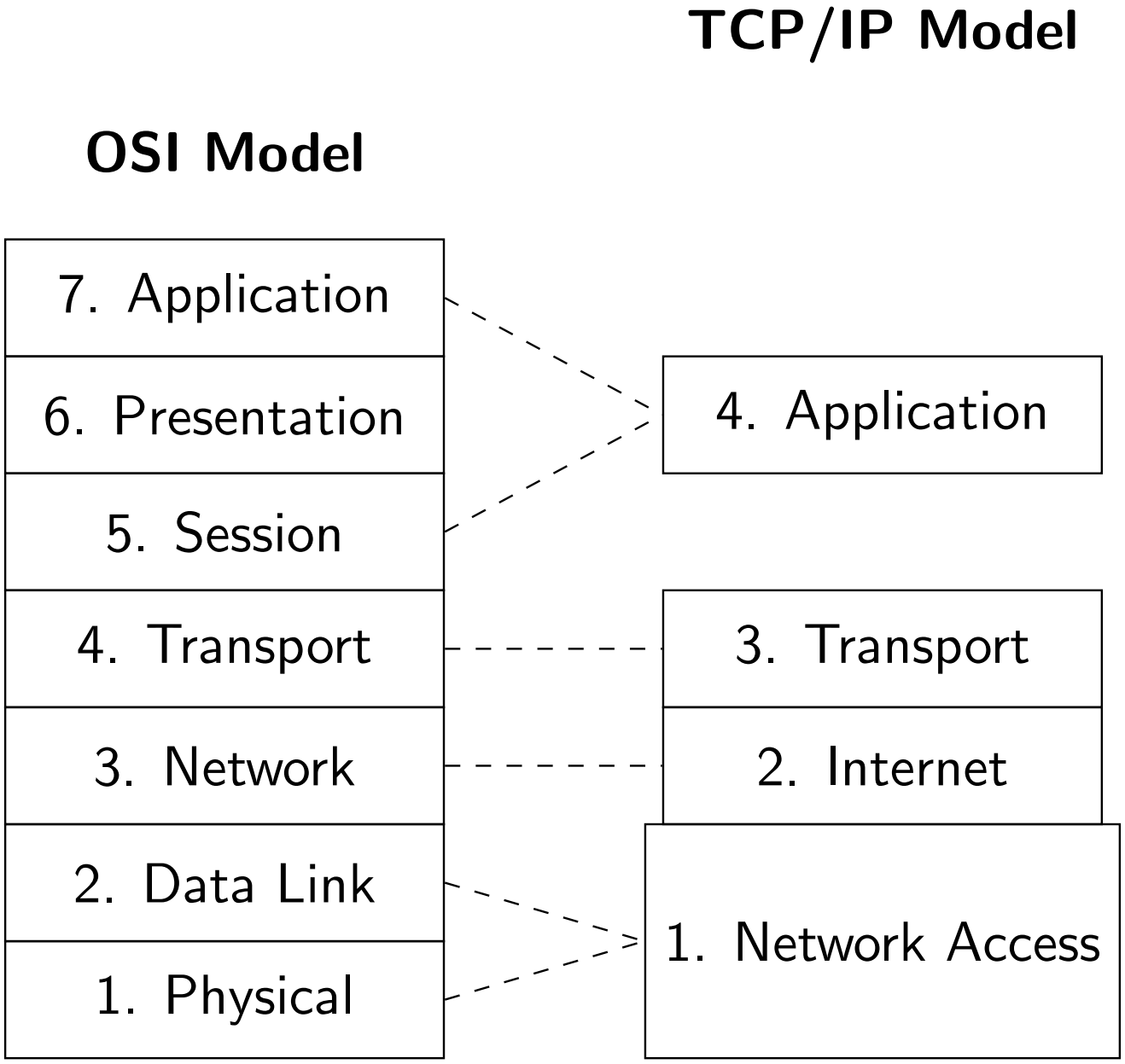
The OSI Reference Model Recap

- Conceptual model created by ISO in 1984 to standardize communication systems.
- Consists of 7 distinct layers: Physical, Data Link, Network, Transport, Session, Presentation, Application.
- Strict separation of services, interfaces, and protocols.
- Layer 7 (Application) interfaces with the user, while Layer 1 (Physical) deals with raw bit streams over a physical medium.
- Provides a clear distinction between connection-oriented and connectionless services at the Network layer, though it typically implements connection-oriented at the Transport layer.

The TCP/IP Reference Model Recap

- Developed by the Department of Defense (DoD) in the 1970s for ARPANET.
- A practical, protocol-oriented model consisting of 4 layers: Network Access (Link), Internet, Transport, and Application.
- Does not strictly distinguish between services, interfaces, and protocols, focusing more on the implementation.
- The Internet layer (IP) provides connectionless, best-effort packet delivery.
- The Transport layer provides both connection-oriented (TCP) and connectionless (UDP) communication.

Architectural Comparison of the Models



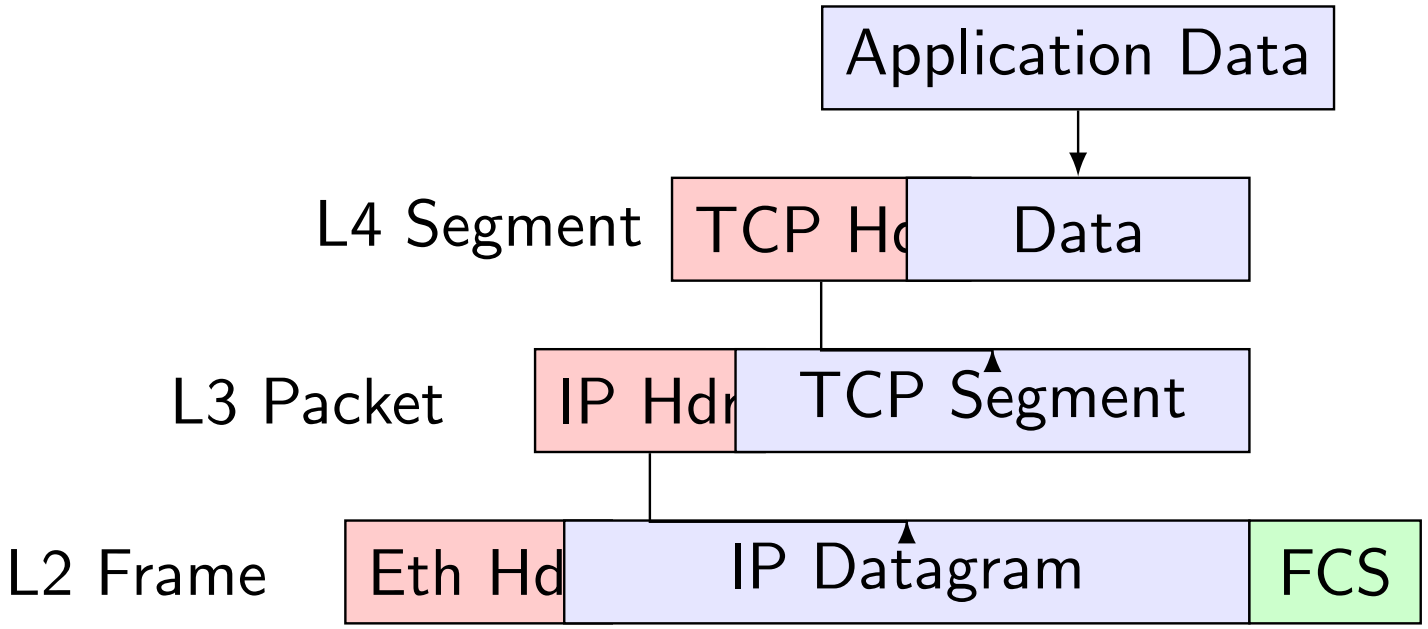
Key Differences: Layer Mapping

- Application Layer Mapping: The OSI model explicitly separates Application, Presentation (data formatting/encryption), and Session (dialogue control). TCP/IP combines all three into a single Application layer.
- Network Interface Mapping: OSI separates Data Link (MAC and LLC sublayers) from Physical (signaling/medium). TCP/IP combines them into the Network Access (or Link) layer.
- Connectionless vs. Connection-oriented: OSI Network layer supports both, while OSI Transport layer is typically connection-oriented. TCP/IP Internet layer is connectionless only (IP), and TCP/IP Transport supports both (TCP/UDP).

Core Philosophical Differences

- OSI was a theoretical, prescriptive model created before the corresponding protocols were fully developed. This led to a very general, but sometimes overly complex design.
- TCP/IP was a descriptive model created after the protocols were already in use. The model was designed around the protocols, making it highly practical and efficient.
- OSI has strict boundaries and clear distinction between Services, Interfaces, and Protocols. TCP/IP blurs these lines, focusing on delivering functionality.
- Complexity: OSI is complex, leading to slow adoption. TCP/IP is simpler, favoring rapid deployment and interoperability.

Encapsulation Process Comparison



Why TCP/IP Won the Protocol Wars

- Timing: TCP/IP protocols were operational and deployed widely (e.g., in UNIX) while OSI was still in the standardization phase.
- Simplicity: TCP/IP's pragmatic approach (4 layers) was easier to implement than OSI's rigid 7-layer architecture.
- Free and Open: The TCP/IP specification (RFCs) was publicly available and largely free, whereas OSI standards were expensive to obtain.
- Investment: Enormous funding from the US DoD accelerated TCP/IP deployment across universities and research institutions.
- The "Hourglass" Model: IP at the center allowed any application to run over any physical network, proving incredibly adaptable.

Summary and Conclusion

- The OSI model remains the premier theoretical framework for teaching networking concepts and understanding protocol behavior.
- The TCP/IP model is the practical foundation of the modern Internet.
- Understanding both models is crucial: use OSI to troubleshoot and understand the 'why', and TCP/IP to understand the 'how'.
- Key takeaway: OSI strictly separates Presentation and Session layers, while TCP/IP merges them; OSI separates Physical and Data Link, while TCP/IP merges them.
- Next Lecture: Deep dive into the Physical Layer and transmission media.

Computer Networks (DI03000051)

GTU Diploma Engineering

Agenda

- Definition of Guided Media
- Twisted Pair Cables (UTP & STP)
- Coaxial Cables
- Fiber Optic Cables
- Connectors, Applications, Advantages & Disadvantages

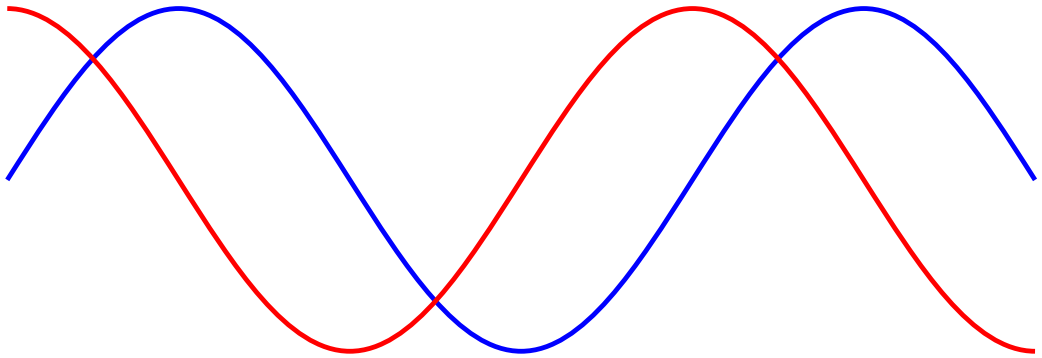
Guided Media: Definition

- Guided media provide a physical path along which signals are propagated.
- They direct and contain the electromagnetic waves within a solid medium.
- Signal transmission is typically point-to-point.
- Commonly used for local area networks (LANs) and long-distance telecommunications.
- Three main categories: Twisted Pair, Coaxial Cable, and Optical Fiber.

Twisted Pair (UTP & STP)

- Consists of two insulated copper wires twisted together.
- Twisting reduces electromagnetic interference (EMI) and crosstalk from adjacent pairs.
- Unshielded Twisted Pair (UTP): Most common, used in telephone lines and Ethernet (e.g., Cat 5e, Cat 6). Uses RJ-45 connectors.
- Shielded Twisted Pair (STP): Includes a metal foil or braided mesh covering the pairs to further reduce EMI. Costlier but better performance in noisy environments.
- Advantages: Inexpensive, easy to install, widely available.
- Disadvantages: High attenuation, susceptible to noise (UTP), limited distance without repeaters.

Twisted Pair Structure

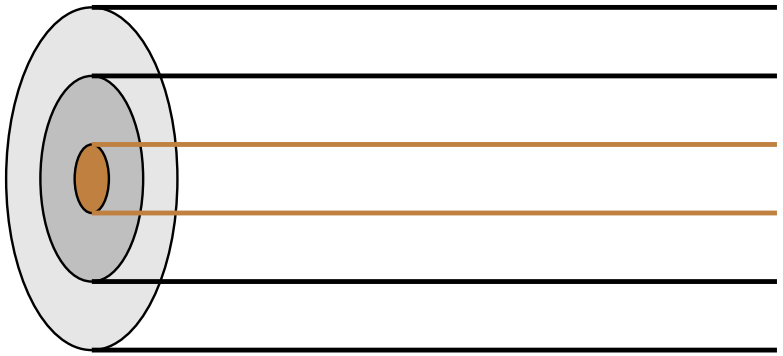


Insulated Copper Wires Twisted Together

Coaxial Cable

- Carries signals of higher frequency ranges than twisted pair.
- Structure: Central core (solid copper) enclosed in an insulating sheath, surrounded by a braided metal mesh (shield), enclosed in a plastic cover.
- Connectors: BNC (Bayonet Neill-Concelman) connectors are widely used (e.g., BNC T-connector, BNC terminator).
- Applications: Cable TV networks, traditional Ethernet LANs (10Base2, 10Base5).
- Advantages: Higher bandwidth than twisted pair, less susceptible to noise and crosstalk.
- Disadvantages: Bulkier, more difficult to install than twisted pair, more expensive.

Coaxial Cable Structure



Core (Copper) - Insulator - Braided Sh

Fiber Optic Cable

- Transmits signals in the form of light (photons) rather than electrical current.
- Structure: Very thin glass or plastic core surrounded by cladding with a lower refractive index (enables total internal reflection), covered by a protective jacket.
- Types: Multimode (step-index, graded-index) for shorter distances, Single-mode for long-haul networks.
- Connectors: SC, ST, LC, MT-RJ.
- Applications: Backbone networks, long-distance telecommunications, high-speed internet (FTTH).

Fiber Optics Characteristics

- Advantages: Exceptionally high bandwidth (Tbps range), extremely low attenuation over long distances.
- Advantages: Completely immune to electromagnetic interference (EMI) and radio frequency interference (RFI).
- Advantages: Lighter and thinner than copper cables, inherently secure (difficult to tap).
- Disadvantages: Installation and maintenance require highly specialized skills and equipment.
- Disadvantages: More expensive than copper cables, fragile and cannot be sharply bent.

Summary

- Guided media provide physical constraint for signals.
- Twisted Pair: Good for short distances, inexpensive, susceptible to noise.
- Coaxial Cable: Better bandwidth and noise immunity, used in TV and older LANs.
- Fiber Optics: Unmatched bandwidth and noise immunity, ideal for long distances, uses light for transmission.

Computer Networks (DI03000051)

GTU Diploma Engineering

Agenda

- Definition of Guided Media
- Twisted-Pair Cable (UTP and STP)
- Coaxial Cable and Connectors
- Fiber-Optic Cable and Applications
- Advantages and Disadvantages of Media Types
- Summary

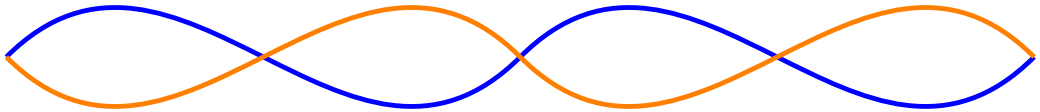
What is Guided Media?

- Guided media, also known as wired or bounded transmission media, provide a physical conduit from one device to another.
- Signals propagating along these media are directed and confined by the physical boundaries of the medium itself.
- They offer higher security and reliability compared to unguided (wireless) media.
- The three primary categories are: Twisted-Pair Cable, Coaxial Cable, and Fiber-Optic Cable.

Twisted-Pair Cable: UTP & STP

- Consists of two insulated copper wires twisted together to reduce electromagnetic interference (EMI) and crosstalk from adjacent pairs.
- Unshielded Twisted Pair (UTP): Most common in LANs (e.g., Cat 5e, Cat 6). Uses standard RJ-45 connectors. Highly flexible and cost-effective.
- Shielded Twisted Pair (STP): Includes a metal foil or braided mesh covering around each pair or the entire bundle to further block external EMI.
- Applications: Telephone networks, local area networks (Ethernet), DSL lines.

Twisted-Pair Visualization

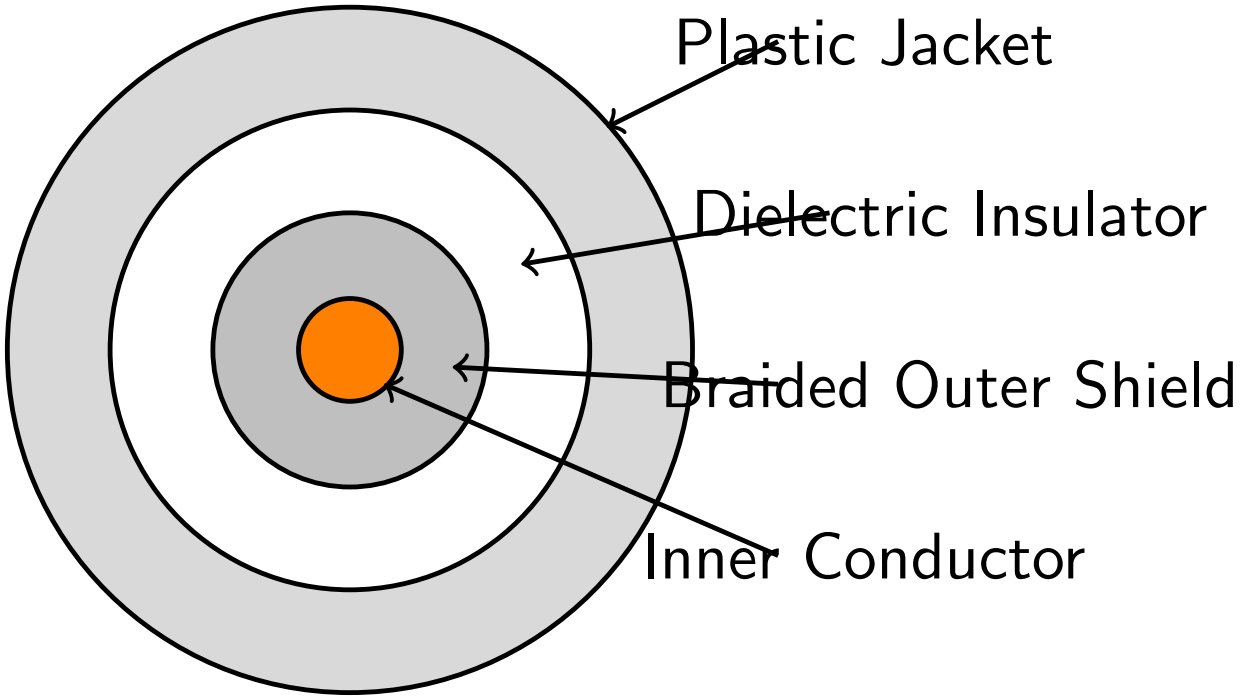


Twisted Pair Concept (Differential Signaling)

Coaxial Cable

- Carries signals of higher frequency ranges than twisted-pair cable due to its constructed shielding.
- Structure: A central copper conductor, an insulating dielectric material, a braided metallic outer shield (acts as a second conductor and EMI shield), and an outer plastic cover (jacket).
- Connectors: Typically utilizes BNC (Bayonet Neill-Concelman) connectors, BNC T-connectors, and terminators to prevent signal reflection.
- Applications: Cable TV networks, traditional Ethernet implementations (10Base5 Thicknet, 10Base2 Thinnet).

Coaxial Cable Cross-Section



Fiber-Optic Cable

- Transmits data as pulses of light through a glass or plastic core rather than electrical signals, providing immense bandwidth.
- Operates on the principle of Total Internal Reflection (TIR).
- Structure: Core (highest refractive index), Cladding (lower refractive index to reflect light back into the core), and a protective Kevlar/plastic Jacket.
- Connectors: SC (Subscriber Connector), ST (Straight-Tip), LC (Lucent Connector).
- Propagation Modes: Multimode (step-index or graded-index for short distances) and Single-mode (for long-haul transmission).

Advantages & Disadvantages

- Advantages of Fiber Optics: Extremely high bandwidth, complete immunity to EMI, very low signal attenuation, and lighter weight.
- Disadvantages of Fiber Optics: High installation and maintenance cost, fragile, cannot carry electrical power (unlike PoE), and requires specialized splicing skills.
- Advantages of Copper (Twisted Pair/Coax): Cost-effective, very easy to install and terminate, supports Power over Ethernet (PoE).
- Disadvantages of Copper: Highly susceptible to EMI/RFI, severe attenuation over long distances, limited bandwidth compared to fiber.

Summary

- Guided media are foundational for reliable, high-speed, localized, and backbone networking infrastructure.
- UTP remains the de facto standard for enterprise and residential LANs due to its excellent balance of cost and performance.
- Coaxial cable continues to be relevant for broadband internet delivery (DOCSIS) and specialized video distribution.
- Fiber-optic cables form the critical backbone of the modern internet, enabling long-distance, ultra-high-speed communication.

Computer Networks (DI03000051)

GTU Diploma Engineering

Agenda

- Guided Media: Definition & Characteristics
- Twisted Pair Cables (UTP & STP)
- Coaxial Cables: Connectors and Applications
- Fiber Optics: Structure, Propagation, and Applications

Guided Media: Definition

- Guided media, also known as wired or bounded transmission media, provide a physical conduit from one device to another.
- Signals transmitted over guided media are directed and confined by the physical limits of the medium.
- Capacity of guided media is defined in terms of bandwidth (Hz) or data rate (bps) over a specific distance.
- Key types: Twisted Pair (Copper), Coaxial Cable (Copper), and Fiber Optic Cable (Glass/Plastic).
- Guided media is characterized by attenuation, which dictates the need for repeaters over long distances.

Unshielded Twisted Pair (UTP)

- Consists of two insulated copper wires twisted together to reduce electromagnetic interference (EMI) and crosstalk from adjacent pairs.
- Categories defined by EIA/TIA 568: Cat 3 (10 Mbps), Cat 5e (1 Gbps), Cat 6 (10 Gbps up to 55m), Cat 6a (10 Gbps up to 100m).
- Connectors: Typically utilizes the 8P8C (commonly referred to as RJ45) modular connector.
- Applications: Widespread in LANs (Ethernet), telephone systems, and short-distance audio/video transmission.
- Advantages: Low cost, ease of installation, and highly flexible.
- Disadvantages: Susceptible to external EMI/RFI, higher attenuation at high frequencies compared to coaxial.

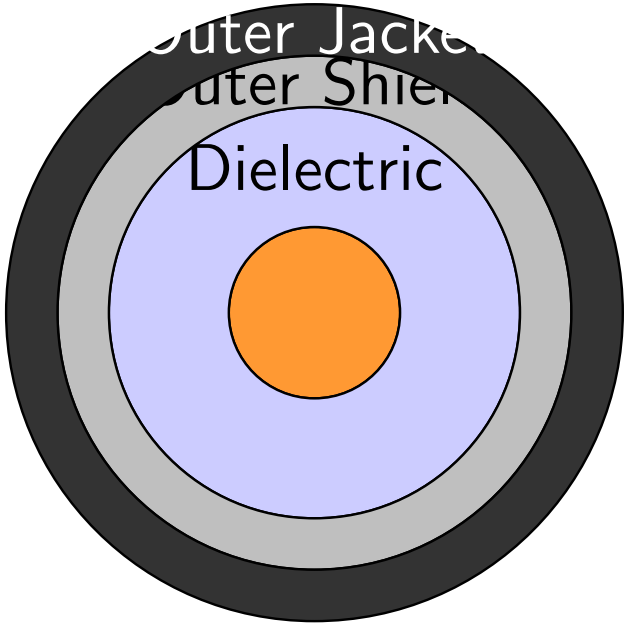
Shielded Twisted Pair (STP)

- Similar to UTP but includes a metal foil or braided mesh covering that encases each pair of insulated conductors.
- The metal casing improves the quality of cable by preventing the penetration of noise or crosstalk.
- Connectors: RJ45 connectors with metal shielding connected to the drain wire for grounding.
- Applications: Environments with high EMI, such as industrial settings or where high data rates must be maintained securely (e.g., Token Ring).
- Advantages: Significantly better noise immunity than UTP, allowing for higher theoretical data rates over longer distances.
- Disadvantages: More expensive, thicker, stiffer, and requires proper grounding to be effective.

Coaxial Cable

- Carries signals of higher frequency ranges than twisted pair cable.
- Structure consists of a central inner solid copper conductor, encased in a plastic insulator, which is then surrounded by a woven metallic foil or braid (outer conductor), enclosed in an outer insulating sheath.
- Connectors: BNC (Bayonet Neill-Concelman) connectors, including BNC T, BNC barrel, and BNC terminators.
- Applications: Cable TV networks (CATV), older LANs (10Base2, 10Base5 Ethernet), and broadband internet connections (DOCSIS).
- Advantages: Higher bandwidth (up to 500 MHz), better shielding against noise, can span longer distances than UTP before requiring repeaters.

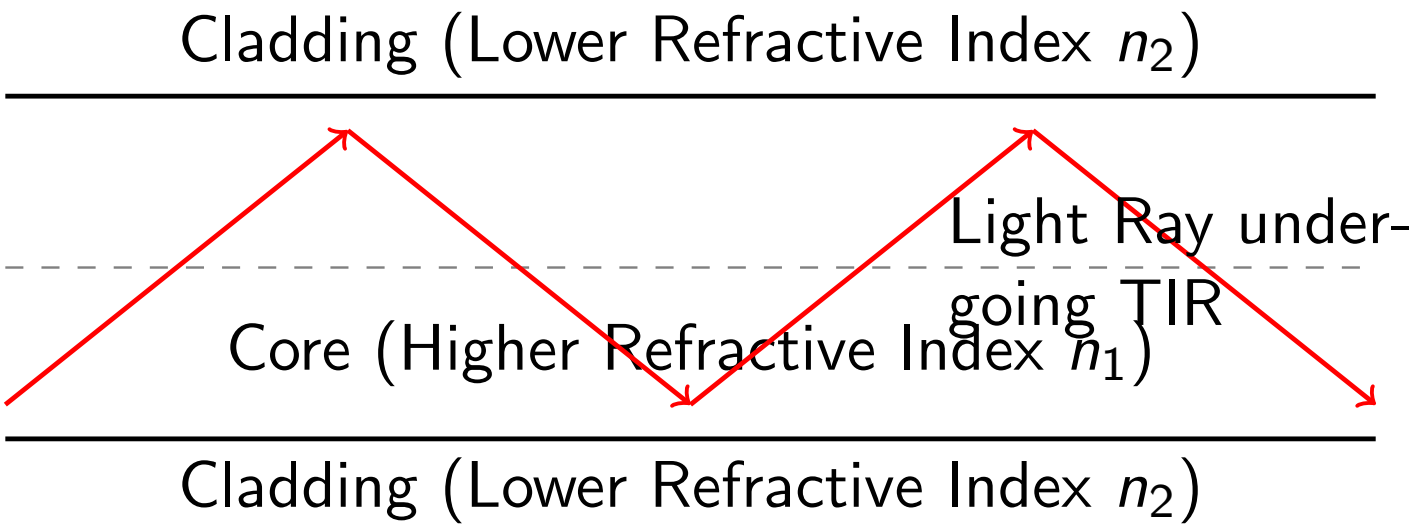
Coaxial Cable Cross-Section Diagram



Fiber Optics Cable

- Transmits data as pulses of light instead of electrical signals, eliminating EMI issues completely.
- Core and cladding are made of glass or plastic with differing refractive indices, enabling Total Internal Reflection (TIR).
- Connectors: SC (Subscriber Connector), ST (Straight Tip), LC (Lucent Connector), MT-RJ.
- Applications: Long-haul telecommunication links, internet backbones, high-speed LANs (e.g., 10GBASE-SR), undersea cable networks.
- Advantages: Enormous bandwidth (Tbps range), immune to electromagnetic interference, lightweight, virtually no signal attenuation over short to medium distances.
- Disadvantages: High cost of installation and termination, fragile, requires specialized skills to splice or repair.

Total Internal Reflection in Optical Fiber



Summary & Comparison

- Twisted Pair is best for low-cost, short-distance LANs and telephony.
- Coaxial Cable offers better bandwidth and shielding for medium-distance broadband applications (e.g., Cable TV).
- Fiber Optic is the ultimate choice for high-speed, long-distance, secure communication backbones.
- Copper media are constrained by resistance, capacitance, and radiation (crosstalk).
- Fiber media are constrained by dispersion (modal and chromatic) and attenuation (scattering and absorption).
- Selection of media depends on cost constraints, bandwidth requirements, distance limitations, and environmental factors.

Computer Networks (DI03000051)

GTU Diploma Engineering

Agenda

1. Definition of Guided Media
2. Twisted Pair Cable (UTP & STP)
3. Coaxial Cable
4. Fiber Optic Cable
5. Connectors & Applications
6. Advantages & Disadvantages

What is Guided Media?

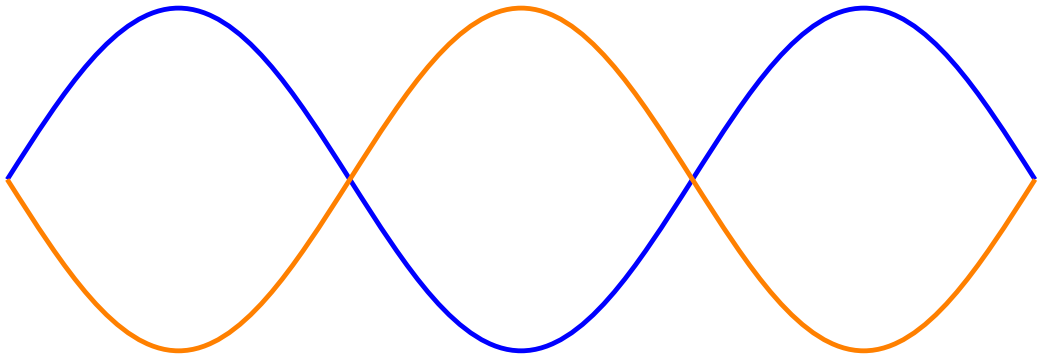
- Guided media, also known as wired or bounded transmission media, provides a physical conduit from one device to another.
- Signals are confined and directed within physical boundaries (e.g., a wire or cable).
- Important characteristics include bandwidth, transmission impairment (attenuation, distortion, noise), and interference.
- The three major categories are Twisted-Pair Cable, Coaxial Cable, and Fiber-Optic Cable.

Twisted Pair Cable (UTP & STP)

- Consists of two insulated copper wires twisted together to reduce crosstalk and electromagnetic interference (EMI).
- Unshielded Twisted Pair (UTP): Most common, inexpensive, flexible, but more susceptible to EMI (e.g., Cat 5e, Cat 6).
- Shielded Twisted Pair (STP): Includes a metal foil or braided mesh covering to block external interference, providing better performance in noisy environments.
- Connectors: RJ-45 (Registered Jack 45) is the standard connector.
- Applications: LANs (Ethernet), Telephone lines.
- Advantages: Cheap, easy to install. Disadvantages: High attenuation, lower bandwidth compared to fiber, sensitive to EMI (UTP).

Twisted Pair Architecture

Insulated Copper Wires Twisted Together



Coaxial Cable

- Carries signals of higher frequency ranges than twisted-pair cables, due to concentric construction.
- Structure: Inner solid copper conductor, encased in a plastic insulating layer, surrounded by a braided metal shielding, all enclosed in a plastic outer jacket.
- Connectors: BNC (Bayonet Neill-Concelman) connectors, including BNC T and BNC terminators.
- Applications: Cable TV networks, traditional Ethernet LANs (10Base-2, 10Base-5).
- Advantages: Higher bandwidth than UTP, less susceptible to EMI, spans longer distances. Disadvantages: Bulky, more expensive than UTP, hard to install.

Coaxial Cable Structure

Outer Jacket
Braided Shield
Insulator
Inner Conductor

Fiber Optic Cable

- Transmits signals in the form of light using the principle of total internal reflection.
- Structure: Core (glass/plastic), Cladding (different refractive index), and Jacket.
- Types: Multimode (Step-index, Graded-index) and Single-mode.
- Connectors: SC (Subscriber Channel), ST (Straight-Tip), LC (Lucent Connector).
- Applications: Backbone networks, long-haul telecommunication, undersea cables.

Fiber Optic - Advantages & Disadvantages

- Advantages: Extremely high bandwidth (Tbps), immunity to electromagnetic interference (EMI), low attenuation (supports very long distances), lightweight, and highly secure (hard to tap).
- Disadvantages: Very expensive installation and maintenance, fragile (glass core can break if bent too sharply), requires specialized skills for splicing and termination.
- Unidirectional: Light propagates in one direction, so bidirectional communication typically requires two fibers.

Summary & Conclusion

- Guided Media provides a physical path for data transmission.
- Twisted Pair is cost-effective and used primarily for local networking and telephony.
- Coaxial cable offers better shielding and higher bandwidth for applications like cable TV.
- Fiber optics represents the pinnacle of guided transmission, offering unmatched bandwidth and immunity to noise, albeit at a higher cost.

Computer Networks (DI03000051)

GTU Diploma Engineering

Agenda

- 1. Unguided Media: Definition
- 2. The Electromagnetic Spectrum
- 3. Propagation Methods: Ground, Sky, Line-of-Sight
- 4. Radio Transmission
- 5. Microwave Transmission
- 6. Infrared Transmission
- 7. Satellite Transmission

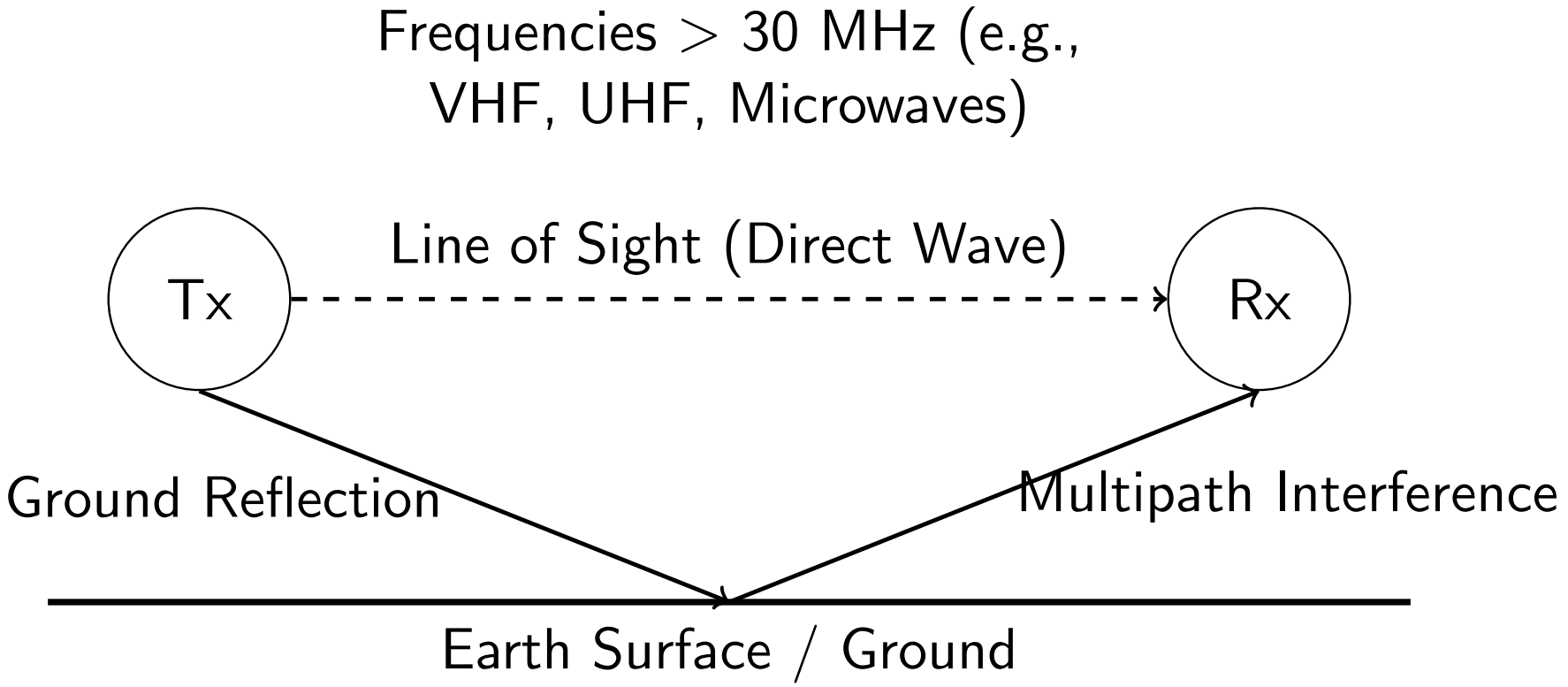
Unguided Media & Electromagnetic Spectrum

- Unguided media (wireless communication) transports electromagnetic waves without using a physical conductor.
- Signals are typically broadcasted through free space and are available to anyone who has a device capable of receiving them.
- The Electromagnetic Spectrum for wireless communication ranges from 3 kHz to 900 THz.
- Radio waves and microwaves (3 kHz to 300 GHz) are highly used for networking.
- Infrared waves (300 GHz to 400 THz) are utilized for short-range communication.
- Lightwave transmission (optical free space) operates at higher frequencies and requires strictly line-of-sight propagation.

Propagation Methods: Ground & Sky

- Ground Propagation (Below 2 MHz): Radio waves travel through the lowest portion of the atmosphere, hugging the Earth's contour.
- AM radio is a typical example of ground propagation. The waves propagate spherically over long distances due to their low frequency.
- Sky Propagation (2 MHz to 30 MHz): Higher-frequency radio waves radiate upward into the ionosphere.
- In the ionosphere, they are refracted (bent) back toward Earth, enabling intercontinental distances without satellite relays.
- Amateur radio and international broadcasts (like shortwave radio) heavily utilize sky wave propagation.
- The distance a sky wave can reach depends on the angle of transmission and the ionosphere's electron density (which varies with time of day).

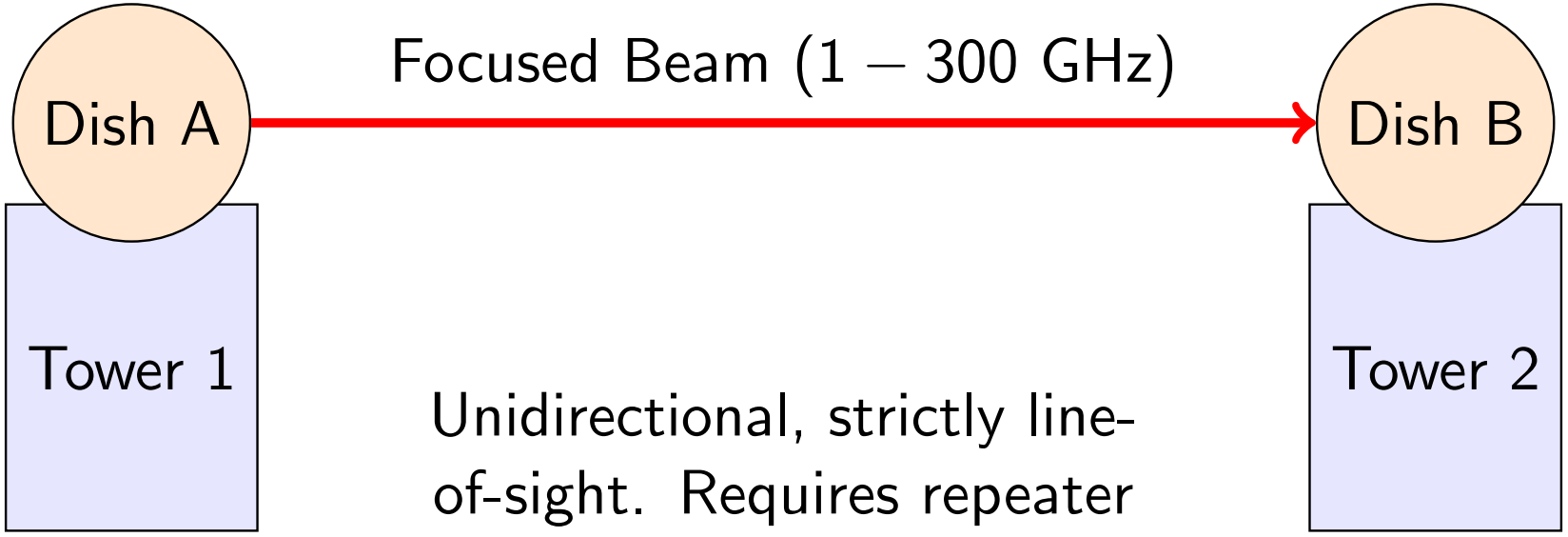
Propagation Methods: Line of Sight



Radio Transmission

- Radio waves operate at frequencies between 3 kHz and 1 GHz.
- They are omnidirectional, meaning they propagate in all directions from the transmitting antenna.
- Omnidirectional properties are advantageous for multicasting (one sender, many receivers), such as FM radio and television broadcasting.
- Low and medium frequencies can easily penetrate walls, which makes them ideal for indoor communication.
- A major drawback of omnidirectional propagation is interference; signals from one antenna can interfere with signals from another if they operate on the same frequency band.
- The regulatory environment (e.g., FCC in the US) strictly controls radio frequency allocation to prevent congestion and interference.

Microwave Transmission Architecture



Unidirectional, strictly line-of-sight. Requires repeater stations for long distances due to Earth's curvature.

Microwave & Infrared Transmission Details

- Microwave Transmission (1 GHz to 300 GHz): Operates unidirectionally. Antennas (like parabolic dishes) must be strictly aligned.
- Microwaves are heavily used for cellular networks, satellite communication, and wireless LANs (e.g., IEEE 802.11 b/g/n/ac in 2.4 GHz and 5 GHz bands).
- Microwaves suffer from attenuation due to environmental factors, notably 'rain fade' where water drops absorb microwave energy.
- Infrared Transmission (300 GHz to 400 THz): Operates at highly localized, short distances.
- Infrared signals are highly directional and cannot penetrate solid obstacles like walls.
- This inability to pass through walls prevents interference between adjacent rooms and provides inherent security (e.g., IrDA standard for remote controls and peripheral links).

Satellite Transmission

- Satellite communication acts as a giant microwave repeater in the sky, receiving signals on an uplink frequency, amplifying them, and broadcasting them on a downlink frequency.
- Geosynchronous Earth Orbit (GEO) satellites reside approximately 35,786 km above the equator. Their orbital period matches Earth's rotation, making them appear stationary.
- GEOs introduce a high propagation delay (approx 250-300 ms round trip) which affects latency-sensitive protocols like TCP.
- Medium Earth Orbit (MEO) satellites (e.g., GPS network) orbit between 2,000 and 35,000 km, balancing coverage area and latency.
- Low Earth Orbit (LEO) satellites (e.g., Starlink, Iridium) operate at 500 to 2,000 km. They provide low latency but require a constellation of many satellites for continuous global coverage.
- Frequency bands utilized include L-band (1-2 GHz), C-band

Applications & Conclusion

- Unguided media forms the backbone of modern mobility and ubiquitous connectivity.
- Personal Area Networks (PAN): Bluetooth (2.4 GHz ISM band) and Infrared for peripherals and wearable technology.
- Local Area Networks (WLAN): Wi-Fi (IEEE 802.11 suite) operating primarily in 2.4 GHz, 5 GHz, and recently 6 GHz (Wi-Fi 6E).
- Wide Area Networks (WWAN): Cellular networks ranging from 2G to 5G, utilizing a mix of low-band, mid-band, and high-band (mmWave) microwaves.
- Global Coverage: Satellite broadband provides internet access to remote and maritime regions where guided media (fiber/copper) is economically unfeasible.
- Conclusion: While unguided media provides unmatched flexibility, it requires robust protocol design to handle interference, security vulnerabilities, and varying propagation delays.

Computer Networks (DI03000051)

GTU Diploma Engineering

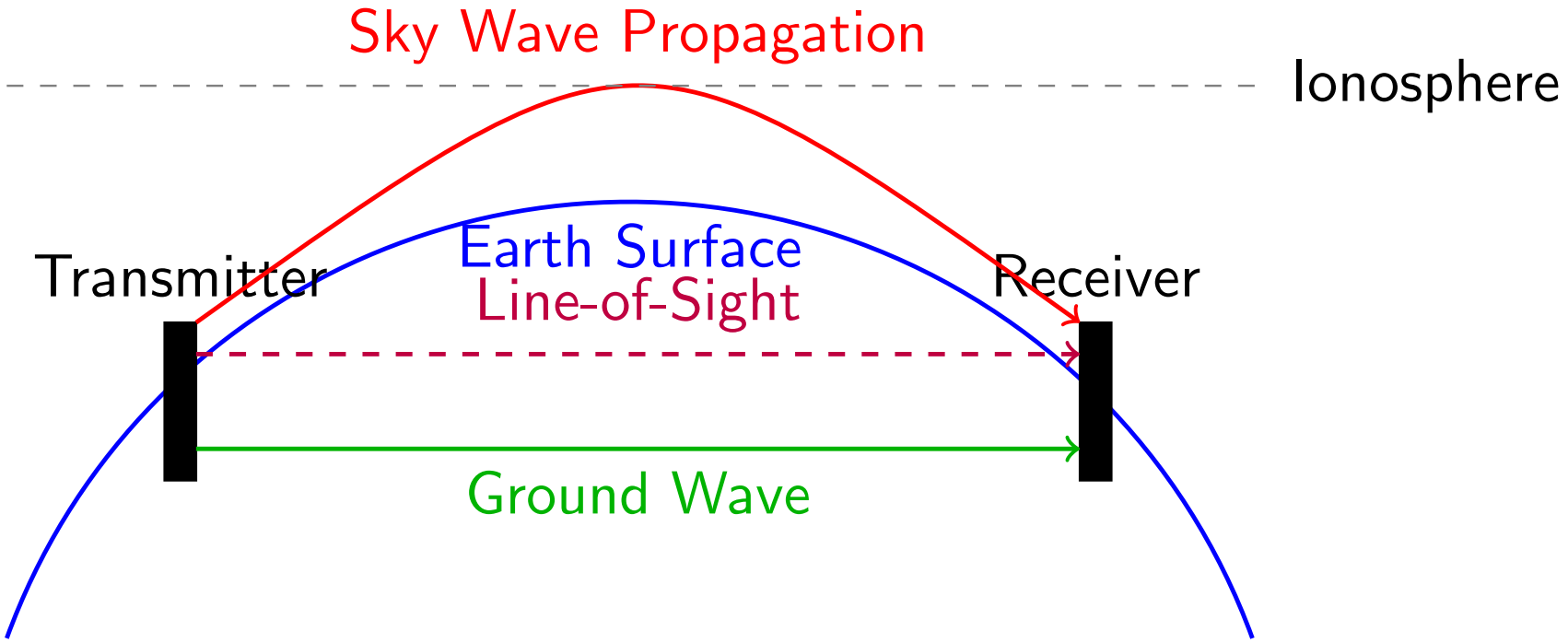
Agenda

- Definition and Electromagnetic Spectrum
- Propagation Methods (Ground, Sky, Line of Sight)
- Radio Transmission
- Microwave Transmission
- Infrared Transmission
- Satellite Transmission

Definition & Electromagnetic Spectrum

- Unguided media transport electromagnetic waves without using a physical conductor, often referred to as wireless communication.
- Signals are broadcast through the air or vacuum and are available to anyone possessing a device capable of receiving them.
- The electromagnetic spectrum ranges from 3 kHz to 900 THz.
- Radio wave frequencies range from 3 kHz to 1 GHz.
- Microwave frequencies range from 1 GHz to 300 GHz.
- Infrared frequencies range from 300 GHz to 400 THz.

Propagation Methods



Propagation Methods Explained

- Ground Propagation (Below 2 MHz): Radio waves travel through the lowest portion of the atmosphere, hugging the earth. They follow the curvature of the planet. Distance depends on the signal's power. Example: AM radio.
- Sky Propagation (2 - 30 MHz): Higher frequency radio waves radiate upward into the ionosphere where they are reflected back to earth. This allows for long-distance communication. Example: Amateur radio, international broadcasts.
- Line-of-Sight Propagation (Above 30 MHz): Very high-frequency signals are transmitted in straight lines directly from antenna to antenna. Antennas must be directional and face each other. Example: FM radio, microwave links.

Radio Transmission

- Radio waves are omnidirectional, meaning they travel in all directions from the source, so the transmitter and receiver do not have to be carefully aligned.
- Frequencies span from 3 kHz to 1 GHz.
- Advantages: Can penetrate walls, making them highly suitable for communication indoors and outdoors.
- Disadvantages: Highly susceptible to interference from other antennas transmitting at the same frequency or band.
- Applications: AM and FM radio, television broadcasts, maritime radio, cordless phones, and paging.
- Strictly regulated by government agencies (like the FCC) to allocate bandwidth and avoid interference.

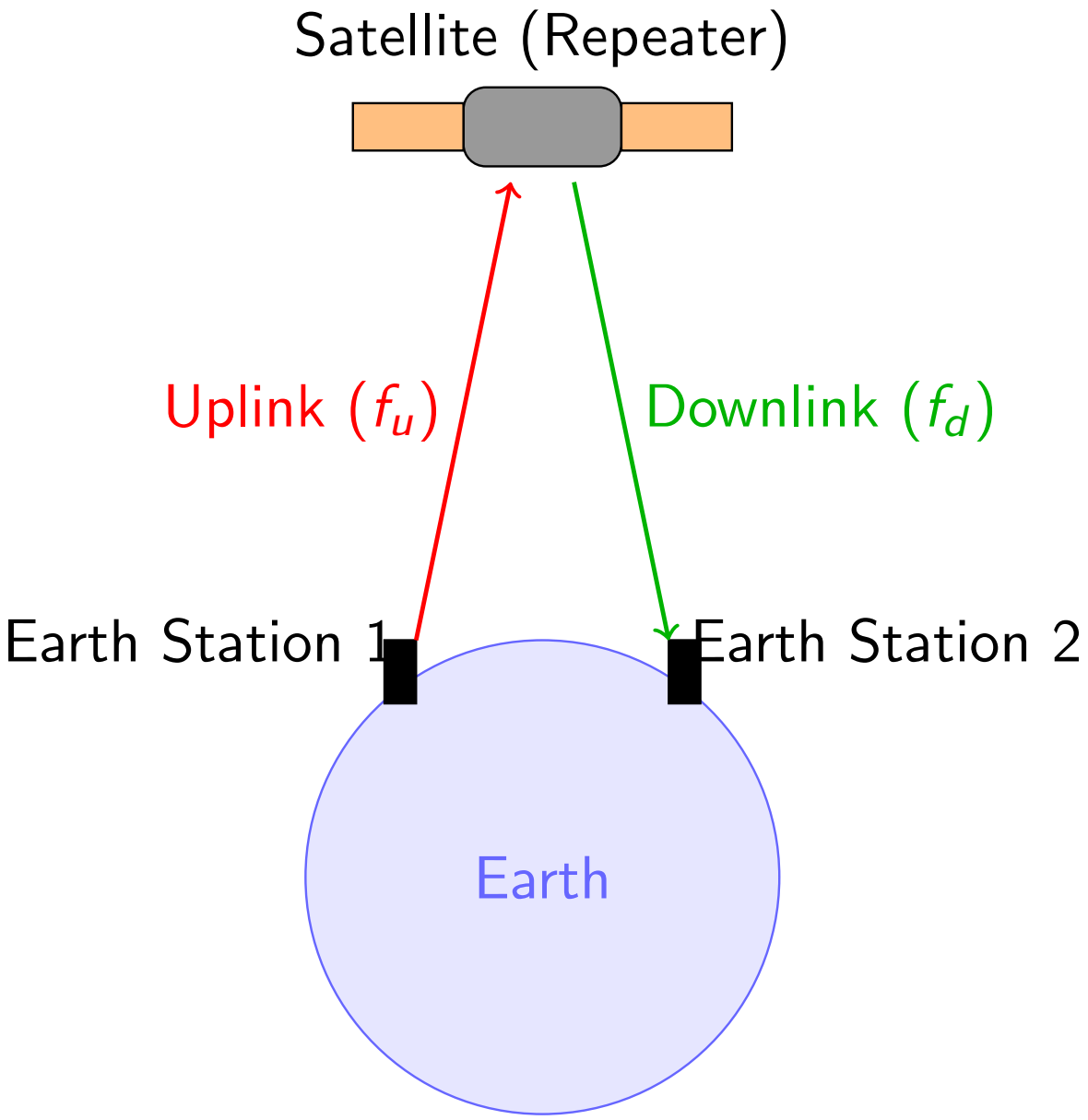
Microwave Transmission

- Microwaves are unidirectional: they travel in a straight line (line-of-sight propagation).
- Frequencies range from 1 GHz to 300 GHz.
- Sending and receiving antennas need to be perfectly aligned. For long-distance communication, tall towers are required to counteract the Earth's curvature.
- Unlike radio waves, high-frequency microwaves cannot easily penetrate solid obstacles like walls.
- Common antennas: Parabolic dish antennas and Horn antennas.
- Applications: Cellular networks, wireless LANs, and satellite communication.

Infrared Transmission

- Used for short-range communication in a closed area using line-of-sight propagation.
- Frequencies range from 300 GHz to 400 THz.
- The high frequencies prevent penetration through solid obstacles like walls, ensuring high security against eavesdropping from adjacent rooms.
- Cannot be used reliably outdoors because the sun's rays contain strong infrared waves, which heavily interfere with communication.
- Applications: TV remote controls, wireless keyboards, mice, and communication between PCs and peripheral devices (standardized by IrDA).

Satellite Transmission Diagram



Satellite Transmission

- A satellite acts as a microwave relay station in space, linking two or more earth-based microwave transmitter/receivers (earth stations).
- Uses different frequency bands for uplink and downlink to avoid signal interference.
- Uplink: Transmission from an earth station up to the satellite.
- Downlink: Transmission from the satellite down to an earth station.
- Orbits: Geostationary Earth Orbit (GEO), Medium Earth Orbit (MEO), and Low Earth Orbit (LEO).
- Footprint: The specific geographical area on Earth that can receive the satellite's signal.
- Applications: GPS navigation, Satellite Television, and global telecommunication backbones.

Computer Networks (DI03000051)

GTU Diploma Engineering

Agenda

- Unguided Media Overview
- Electromagnetic Spectrum
- Propagation Methods
- Radio Waves
- Microwaves
- Infrared
- Satellite Transmission

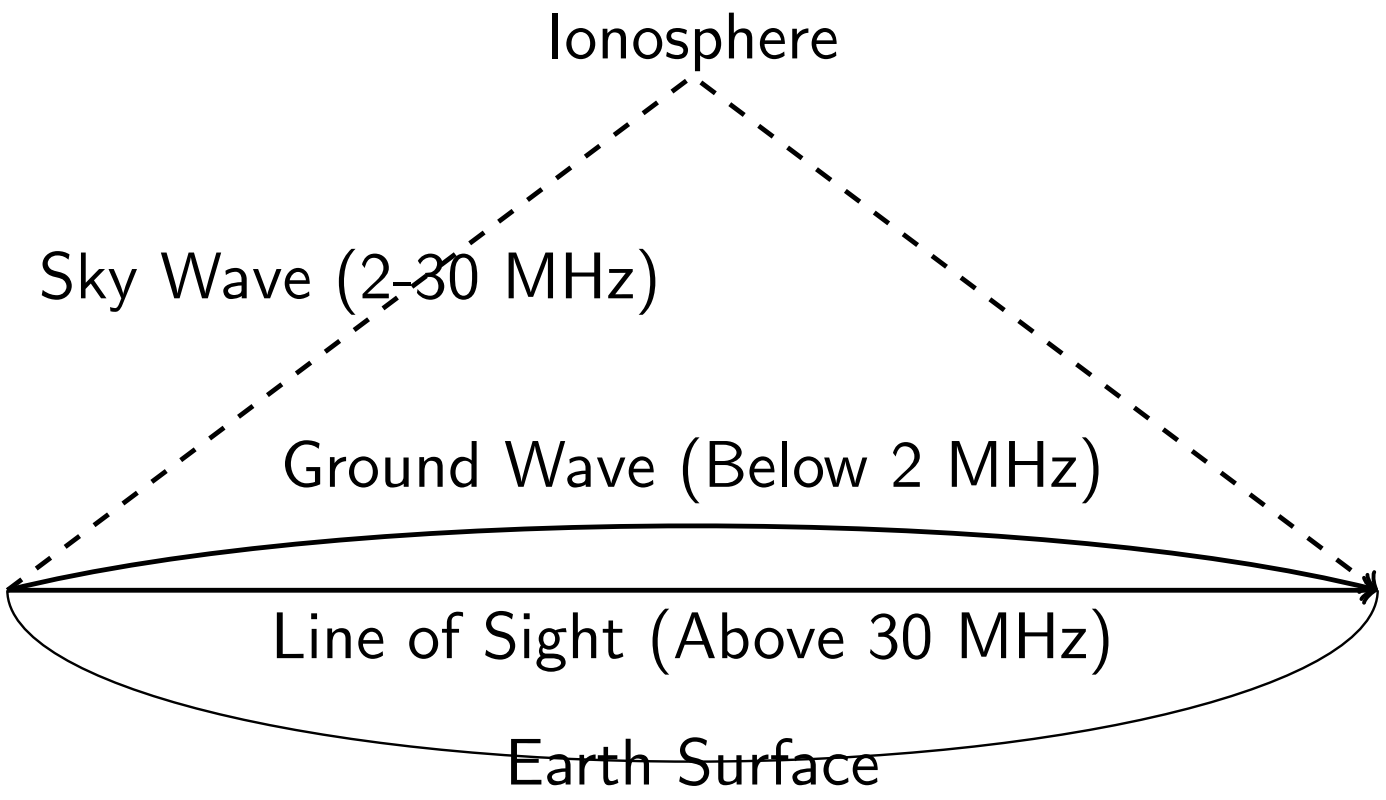
Unguided Media: Definition

- Unguided media transport electromagnetic waves without using a physical conductor.
- This type of communication is often referred to as wireless communication.
- Signals are broadcast through free space and thus are available to anyone who has a device capable of receiving them.
- Applications include cellular networks, satellite communications, wireless LANs, and Bluetooth.

Electromagnetic Spectrum

- The electromagnetic spectrum spans from low-frequency radio waves to high-frequency gamma rays.
- Wireless communication primarily uses a specific range of the spectrum: 3 kHz to 900 THz.
- Radio Waves: 3 kHz to 1 GHz (Omnidirectional, penetrate walls easily).
- Microwaves: 1 GHz to 300 GHz (Unidirectional, Line of sight required).
- Infrared: 300 GHz to 400 THz (Short range, cannot penetrate solid objects).

Propagation Methods



Radio Transmission

- Frequency Range: 3 kHz to 1 GHz.
- Omnidirectional: Antennas transmit radio waves in all directions, so sending and receiving antennas do not need alignment.
- Ground and Sky Propagation: Lower frequencies follow the earth's curvature; higher frequencies bounce off the ionosphere.
- Applications: AM and FM radio, television broadcasting, cordless phones, and paging systems.
- Characteristics: Easily penetrates walls (highly beneficial inside buildings), but prone to interference from other signals.

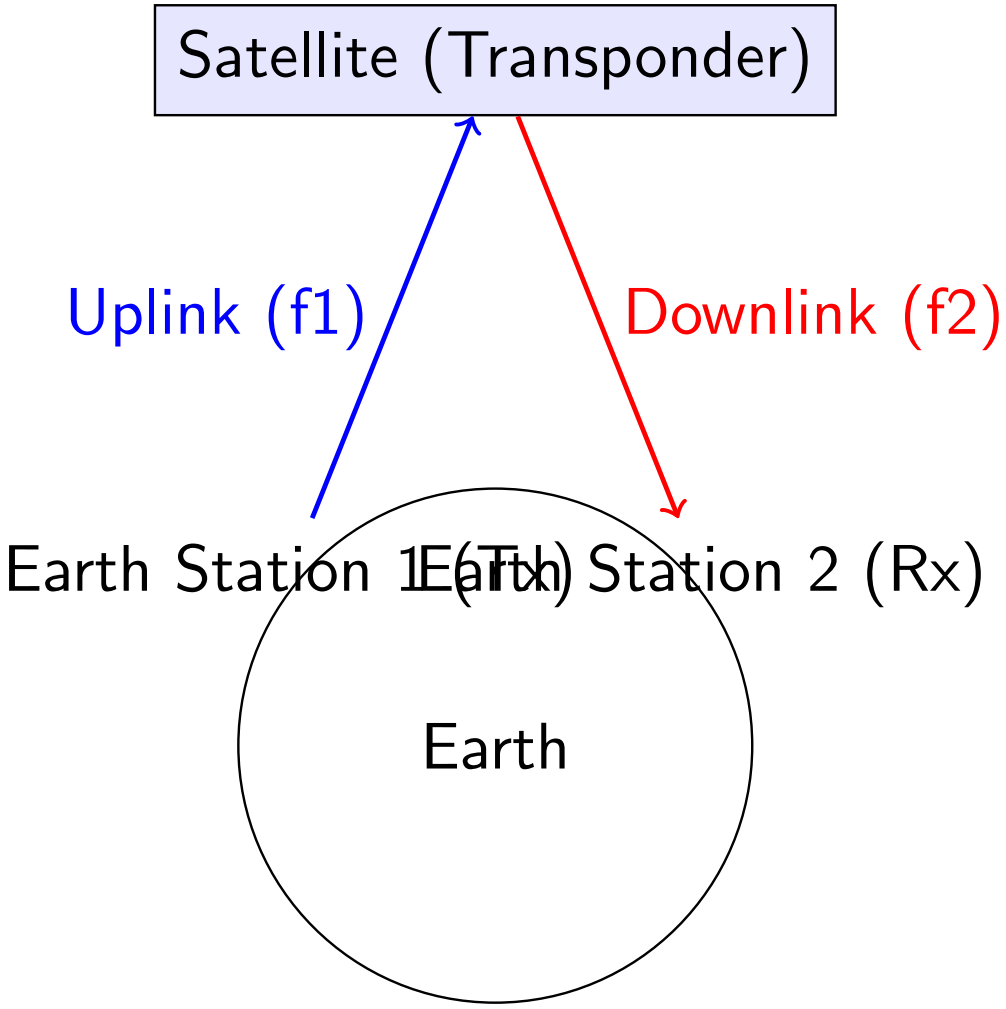
Microwave Transmission

- Frequency Range: 1 GHz to 300 GHz.
- Unidirectional: Antennas send out signals in a specific direction. Sending and receiving antennas must be perfectly aligned (Line of Sight).
- Cannot Penetrate Solid Objects: Requires a clear path between antennas, leading to the use of tall towers.
- Applications: Cellular networks (2G, 3G, 4G, 5G), satellite communications, and wireless LANs (Wi-Fi).
- Antenna Types: Parabolic dish antennas and Horn antennas are commonly used.

Infrared Transmission

- Frequency Range: 300 GHz to 400 THz.
- High Frequencies: Cannot penetrate walls, preventing interference between adjacent rooms.
- Security: Inherently secure due to its short range and inability to pass through physical barriers.
- Applications: TV remote controls, wireless keyboards, mice, and short-range communication between devices.
- Limitations: Useless for outdoor communication as the sun's rays contain infrared waves which cause severe interference.

Satellite Transmission



Summary

- Unguided media use free space to transmit electromagnetic signals without physical conductors.
- Ground propagation is for low frequencies, sky propagation for medium/high, and line-of-sight for very high frequencies.
- Radio waves are omnidirectional and can penetrate most solid objects.
- Microwaves are unidirectional, require line-of-sight, and are used for terrestrial point-to-point and satellite links.
- Infrared is restricted to short-range, line-of-sight communications and cannot penetrate solid walls.

Computer Networks (DI03000051)

GTU Diploma Engineering

Agenda

- Network Interface Cards (NICs)
- Repeaters and Hubs
- Bridges and Switches
- Layer 2 vs Layer 3 Switches
- Routers and Gateways
- Wireless Access Points

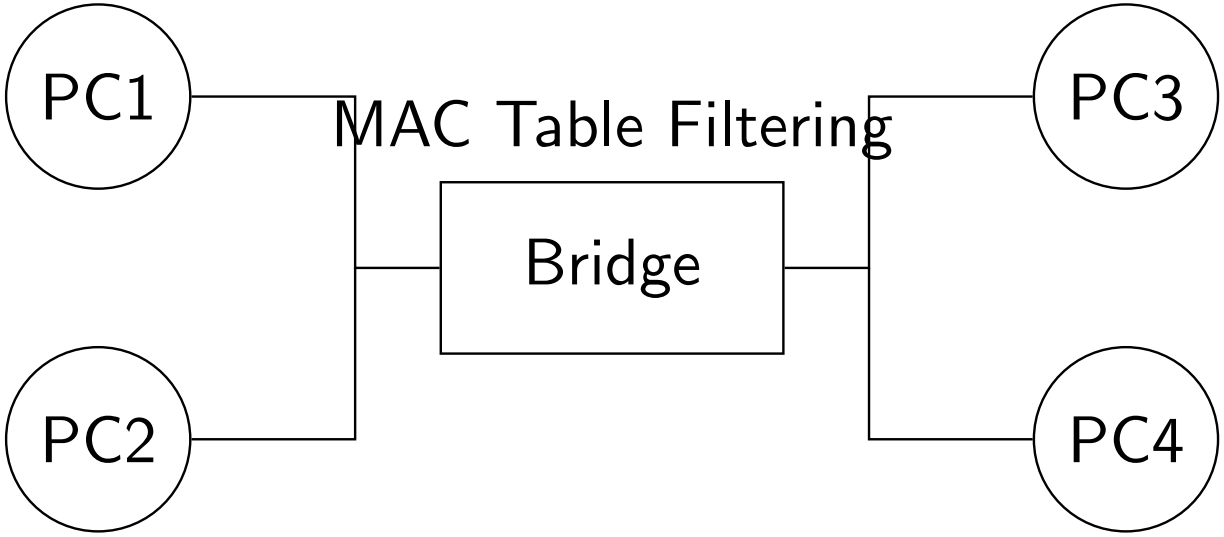
Network Interface Card (NIC)

- Definition: Hardware component that connects a computer to a computer network, operating at Layer 1 and 2.
- Types of NIC: Ethernet (wired, RJ-45) and Wi-Fi (wireless, antenna).
- Components of NIC: Memory (RAM), Microcontroller, Transceiver, MAC address PROM, and Bus interface.
- Advantages: Dedicated connection, high speed transmission.
- Disadvantages: Requires physical installation, hardware specific to the bus architecture.

Repeaters and Hubs

- Repeater: Layer 1 device used to regenerate or replicate a signal.
- Use: Extends the transmission distance of a signal over a network segment.
- Advantage (Repeater): Inexpensive, extends network range. Disadvantage: Cannot filter data.
- Hub: A multiport repeater. Broadcasts incoming data to all other ports.
- Advantage (Hub): Simple to set up, cheap. Disadvantage: High collision domain, wastes bandwidth.

Bridge Operations Diagram



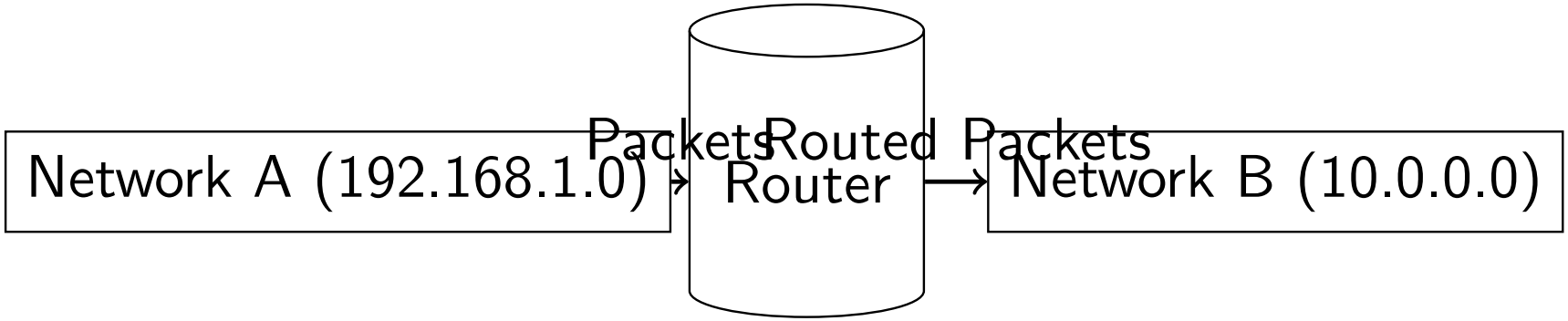
Bridges and Switches

- Bridge: Layer 2 device that connects two LAN segments and filters traffic based on MAC addresses.
- Advantage (Bridge): Reduces collision domains. Disadvantage: Slower than switches due to software-based processing.
- Switch: Multiport bridge, operates at Layer 2 (Data Link).
- Advantage (Switch): High performance, dedicated bandwidth per port, hardware-based switching using ASICs.
- Disadvantage (Switch): More expensive than hubs, can become a single point of failure for connected devices.

Layer 2 vs Layer 3 Switches

- Layer 2 Switch: Operates on MAC addresses, performs hardware-based frame forwarding within the same VLAN.
- Layer 3 Switch: Operates on IP addresses as well as MAC addresses. Incorporates routing functions.
- Difference 1: L2 forwards frames; L3 routes packets between different subnets/VLANs.
- Difference 2: L2 relies entirely on ARP; L3 maintains routing tables.
- Advantage (L3): Faster inter-VLAN routing than traditional routers.

Router Architecture Diagram



Routing Table Lookup

Routers and Gateways

- Router: Layer 3 device that connects multiple networks and forwards packets based on IP addresses.
- Advantage (Router): Broadcast domain isolation, intelligent path selection. Disadvantage: Higher latency, complex setup.
- Gateway: Operates across all OSI layers. Acts as an entrance to another network.
- Use: Connects networks with different protocols (e.g., OSI to TCP/IP).
- Advantage: Protocol translation. Disadvantage: Slowest network device due to high processing overhead.

Access Points

- Access Point (AP): A device that allows wireless devices to connect to a wired network (usually Wi-Fi).
- Use: Extends a wired LAN to wireless clients.
- Advantage: Mobility, easy deployment, supports multiple concurrent wireless users.
- Disadvantage: Security vulnerabilities (cracking), susceptible to physical radio interference.
- Conclusion: Network devices form the backbone of modern communication, each serving a highly specialized role.

Computer Networks (DI03000051)

GTU Diploma Engineering

Agenda

- Physical Layer: Repeaters and Hubs
- Data Link Layer: Bridges and Switches
- Network Layer: Routers
- Comparative Analysis: Layer 2 vs Layer 3 Switches
- Access Points and Gateways
- Network Interface Cards (NIC)

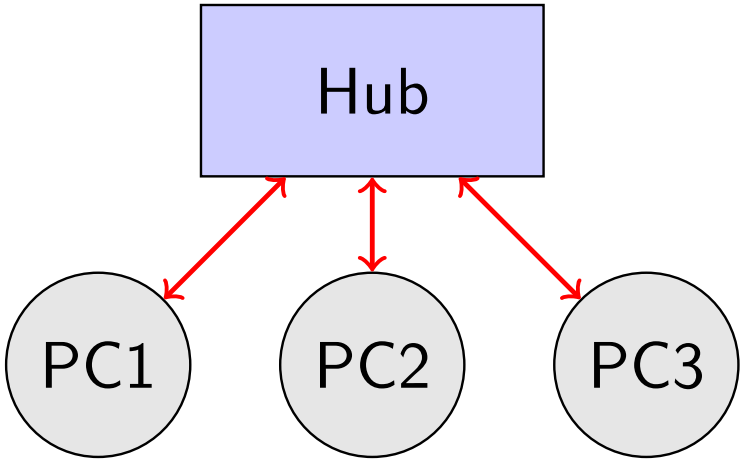
Physical Layer: Repeaters and Hubs

- Definition: Operate at OSI Layer 1, focusing on bit-level transmission and physical signal regeneration.
- Repeater: An electronic device that receives a signal and retransmits it at a higher power, extending network range by overcoming attenuation.
- Hub: A multi-port repeater used to connect multiple Ethernet devices, effectively making them a single network segment.
- Advantage (Repeater): Highly cost-effective method to extend cabling distances (e.g., beyond the 100m Ethernet limit).
- Disadvantage (Hub): Broadcasts all data to every port, creating a single massive collision domain. Highly inefficient bandwidth utilization and poses severe security sniffing risks.

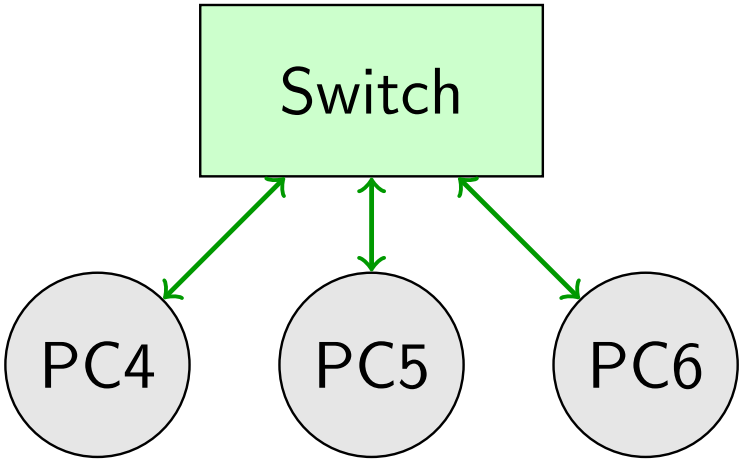
Data Link Layer: Bridges and Switches

- Definition: Operate at OSI Layer 2, using MAC addresses to make forwarding decisions for data frames.
- Bridge: Connects two LAN segments, actively learning MAC addresses and filtering traffic to reduce collisions between segments.
- Switch: A high-density, multi-port bridge that allocates dedicated bandwidth to each port via hardware ASICs, effectively eliminating collision domains on full-duplex links.
- Advantage (Switch): High performance, micro-segmentation of the network, and robust support for Virtual LANs (VLANs).
- Disadvantage (Bridge/Switch): Vulnerable to broadcast storms if Spanning Tree Protocol (STP) is not correctly implemented to prevent loops.

Visualizing Collision Domains: Hub vs Switch



Shared Collision Domain



Separate Collision Domains

Network Layer: Routers

- Definition: Operate at OSI Layer 3, utilizing logical IP addresses to route packets between disparate networks.
- Use: Interconnects distinct subnets, WANs, and LANs, executing complex algorithms to determine the optimal path for data packets.
- Advantage: Breaks up broadcast domains, provides robust security through Access Control Lists (ACLs), and supports dynamic routing protocols (e.g., OSPF, BGP).
- Disadvantage: Introduces higher processing latency due to software-based routing table lookups and is generally more expensive and complex to manage than edge switches.

Comparative Analysis: Layer 2 vs Layer 3 Switches

- Layer 2 Switch: Forwards frames strictly based on hardware MAC addresses within the same subnet or VLAN. Fast but relies on a router for inter-subnet communication.
- Layer 3 Switch: Combines the hardware-driven speed of L2 switching with the IP routing logic of L3 routing natively on specialized silicon.
- Key Difference 1: Routing Capability. L2 switches cannot route traffic between different IP networks; L3 switches can perform high-speed inter-VLAN routing.
- Key Difference 2: Protocol Support. L3 switches support dynamic IP routing protocols (RIP, EIGRP, OSPF), whereas L2 switches are limited to spanning-tree and VLAN protocols.

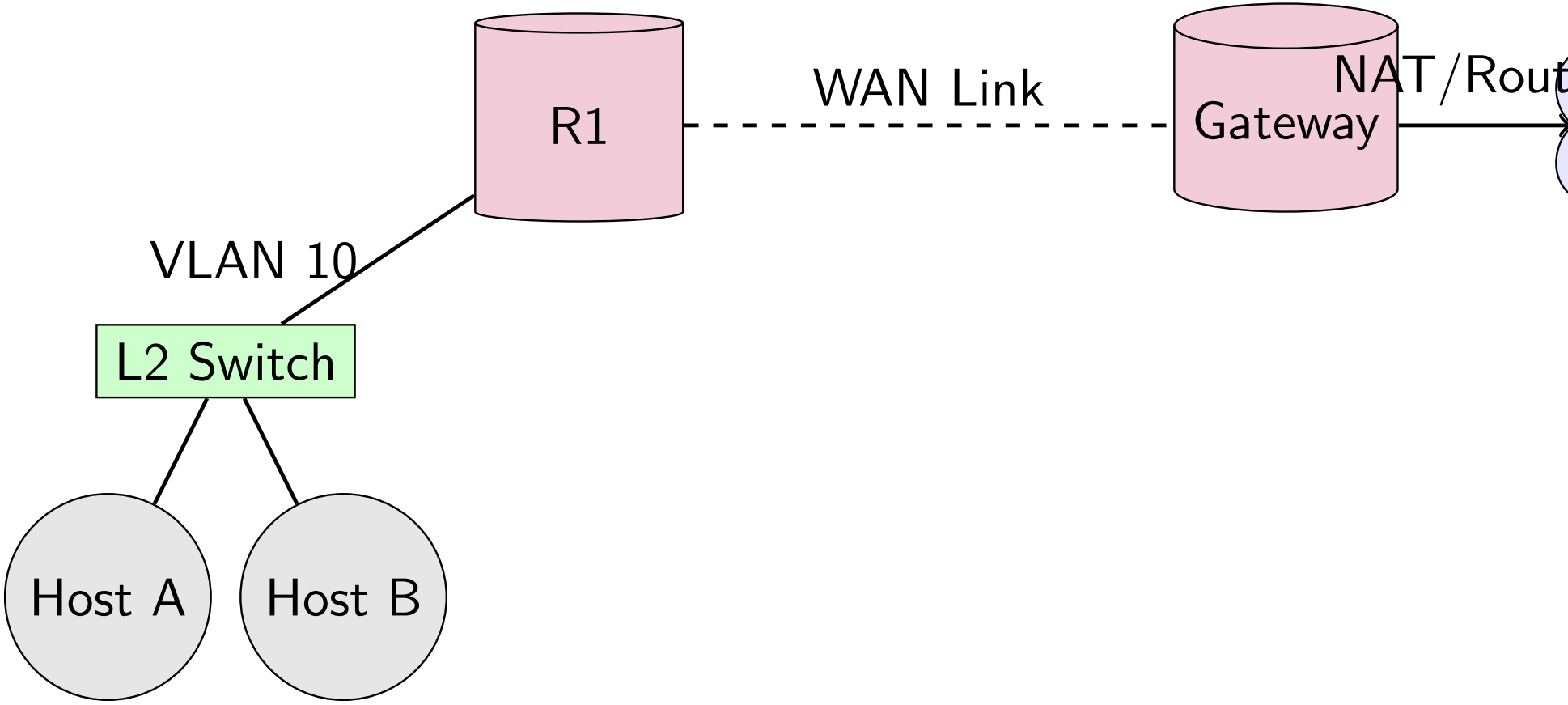
Access Points & Gateways

- Wireless Access Point (WAP): A device operating primarily at Layer 2 that allows wireless devices to connect to a wired network backbone via Wi-Fi standards (IEEE 802.11).
- Advantage/Disadvantage (WAP): Provides excellent endpoint mobility; however, wireless media is subject to RF interference, shared medium contention, and complex security requirements.
- Gateway: A comprehensive protocol converter acting as an entry/exit point to another network, potentially operating up to OSI Layer 7.
- Advantage (Gateway): Can translate between fundamentally different network architectures (e.g., translating TCP/IP to legacy IBM SNA).
- Disadvantage (Gateway): High computational overhead for deep protocol translation and often represents a single point of failure.

Network Interface Card (NIC)

- Definition: The physical hardware component (often integrated into motherboards) that provides a device with dedicated network connectivity and a burned-in MAC address.
- Types of NIC: Ethernet (Wired, IEEE 802.3, utilizing RJ45 connectors) and Wi-Fi (Wireless, IEEE 802.11, utilizing built-in antennas).
- Key Components of NIC: The transceiver (transmits/receives signals), MAC controller chip, boot ROM socket for PXE booting, LED link indicators, and PCIe bus interface.
- Advantage: Offloads extensive packet processing tasks from the host CPU and provides dedicated hardware for maximum throughput.
- Disadvantage: Hardwired to specific architecture speeds; upgrading from 1Gbps to 10Gbps requires a physical hardware swap.

Visualizing Inter-Network Routing and Gateways



Computer Networks (DI03000051)

GTU Diploma Engineering

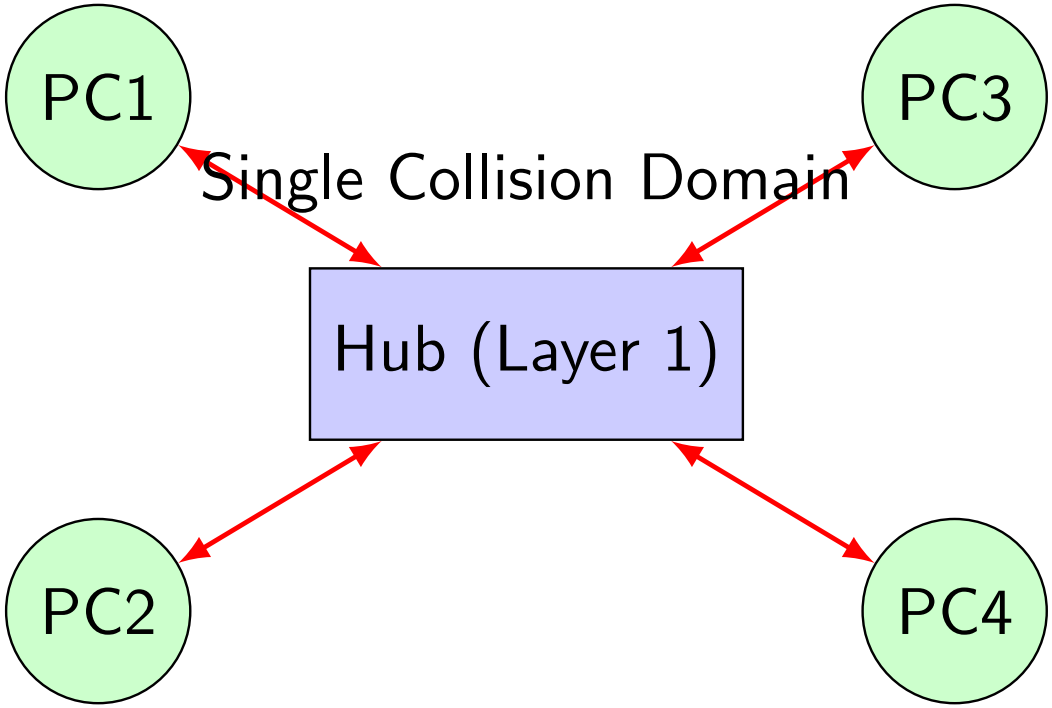
Agenda

- Network Devices: Definition and Uses
- Repeaters and Hubs (Physical Layer)
- Bridges and Switches (Data Link Layer)
- Layer 2 vs Layer 3 Switches
- Routers and Gateways (Network Layer & Above)
- Wireless Access Points
- Network Interface Cards (NIC)

Repeaters and Hubs

- Repeater: Operates at the Physical layer (OSI Layer 1). Regenerates or replicates signals weakened by attenuation. Use: Extending maximum cable lengths.
- Advantage: Inexpensive, straightforward to implement. Disadvantage: Cannot filter frames or isolate traffic; simply repeats everything blindly.
- Hub: Essentially a multiport repeater. It broadcasts all incoming data out to all other connected ports. Forms a single collision domain and broadcast domain.
- Use: Legacy networking for connecting multiple twisted-pair Ethernet devices.
- Advantage: Low cost, easy to monitor traffic (promiscuous mode).
- Disadvantage: High collision rates in half-duplex CSMA/CD, no dedicated bandwidth per port, poses a significant security risk.

Hub vs Switch Topology



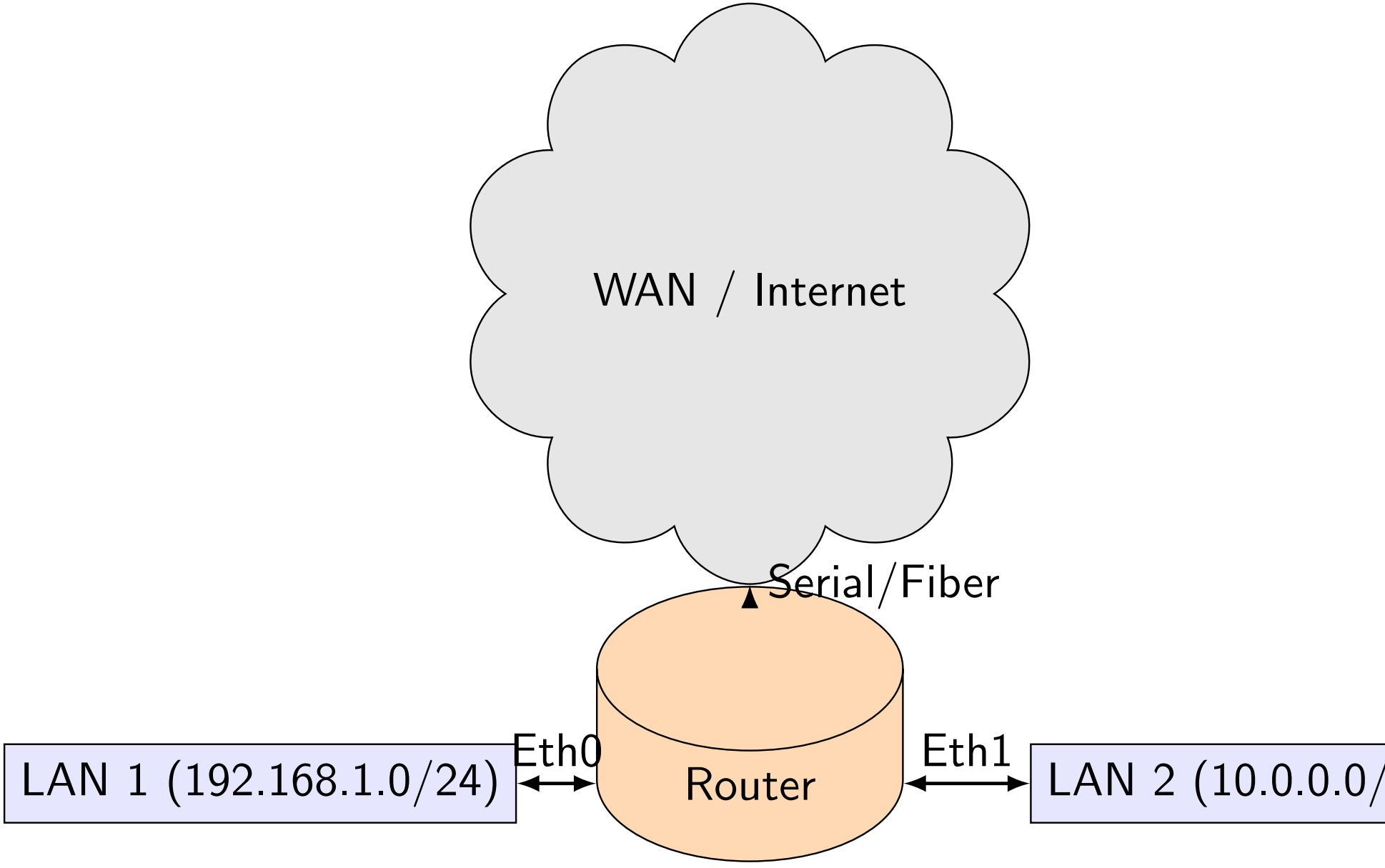
Bridges and Switches

- Bridge: A Layer 2 device that filters traffic by MAC address. Divides collision domains but maintains a single broadcast domain. Use: Connecting two LAN segments.
- Advantage: Reduces network traffic on segments by filtering. Disadvantage: Slower than switches (often software-based filtering), limited ports.
- Switch: A multiport bridge that uses Application-Specific Integrated Circuits (ASICs) for fast hardware-based MAC address learning and forwarding.
- Use: The primary distribution point for endpoint devices in modern LANs. Operates in full-duplex, eliminating collisions.
- Advantage: Microsegmentation (each port is its own collision domain), dedicated bandwidth per port, supports Virtual LANs (VLANs).
- Disadvantage: More expensive than hubs, can create broadcast storms if loops exist (requires STP - Spanning Tree Protocol).

Layer 2 vs Layer 3 Switches

- Layer 2 Switch: Operates strictly at the Data Link Layer. Forwarding decisions are based purely on hardware MAC addresses using CAM (Content Addressable Memory) tables.
- Layer 2 Characteristics: Fast, intra-VLAN routing only. Cannot route traffic between different IP subnets. Only reads Ethernet headers.
- Layer 3 Switch: Contains both switching and routing functionality. Operates at the Network Layer for high-speed inter-VLAN routing.
- Layer 3 Characteristics: Uses IP addresses for routing decisions, but does so at hardware speed (ASIC-based routing) using CEF (Cisco Express Forwarding) or a Forwarding Information Base (FIB).
- Core Difference: L2 switch relies on MACs for intra-LAN traffic; L3 switch performs inter-VLAN routing internally without sending traffic to a dedicated external router ('router on a stick').

Router Architecture



Routers and Gateways

- Router: Operates at the Network layer (OSI Layer 3). Connects multiple logical subnets and routes packets based on IP addresses using dynamic routing protocols (OSPF, BGP, EIGRP).
- Advantage: Breaks broadcast domains entirely, provides advanced security (ACLs), optimal path selection. Disadvantage: Higher latency due to packet inspection, complex configuration.
- Gateway: A protocol converter or default egress point. Often operates across Layers 4-7 (Application Gateway), or Layer 3 as a default gateway router.
- Use: Connecting networks of completely different architectures, protocols, or formats (e.g., VoIP gateway mapping SIP to traditional PSTN networks).
- Advantage: Enables true interoperability between heterogeneous systems. Disadvantage: Extremely resource intensive, potential performance bottleneck.

Access Points (APs)

- Access Point (AP): A Layer 2 device that acts as a bridge between a wired Ethernet network and a wireless LAN (WLAN).
- Use: Provides Wi-Fi access (IEEE 802.11 standard) to mobile devices, forming a Basic Service Set (BSS). APs translate 802.3 Ethernet frames to 802.11 wireless frames.
- Advantage: High mobility, rapid deployment in areas difficult to cable. Highly scalable when managed centrally via Wireless LAN Controllers (WLCs).
- Disadvantage: Wireless medium operates in half-duplex using CSMA/CA (Collision Avoidance), susceptible to RF interference (microwave, bluetooth), requires robust encryption (WPA2/WPA3) to prevent unauthorized access.

Network Interface Card (NIC)

- Network Interface Card (NIC): The essential hardware component that allows a computer to connect to a network medium (operates at Layer 1 and Layer 2).
- Types of NIC: Ethernet (wired RJ-45, 802.3, speeds up to 100Gbps+), Wi-Fi (wireless 802.11 with integrated or external antennas), Fiber Optic (SFP/SFP+ transceivers).
- Components: PCB (Printed Circuit Board), MAC address ROM (Burned-In Address / BIA), Controller/Processor (handles CSMA/CD or CSMA/CA logic), Transceiver (PHY component for electrical/optical conversion), Bus Interface (PCIe, USB), LED status indicators.
- Advantage: Offloads networking protocol processing from the computer's main CPU, provides a unique and dedicated hardware MAC address.
- Disadvantage: Hardwired to a specific transmission medium (e.g., cannot use an Ethernet NIC for Fiber connections without an adapter).

Computer Networks (DI03000051)

GTU Diploma Engineering

Agenda

- IPV4 Characteristics
- Advantages and Disadvantages
- Classful Addressing Scheme
- Classless Addressing Scheme
- Subnet & Masking
- Reserved Address

IPV4: Characteristics

- Internet Protocol version 4 is the fourth version of the Internet Protocol (IP).
- It is one of the core protocols of standards-based internetworking methods in the Internet.
- IPv4 is a connectionless protocol for use on packet-switched networks.
- It operates on a best-effort delivery model, meaning it does not guarantee delivery, assure proper sequencing, or avoid duplicate delivery.
- Data integrity and sequencing are addressed by upper-layer transport protocols, such as the Transmission Control Protocol (TCP).
- IPv4 uses 32-bit (4-byte) addresses, which limits the total address space to 4,294,967,296 (2^32)*addresses*.

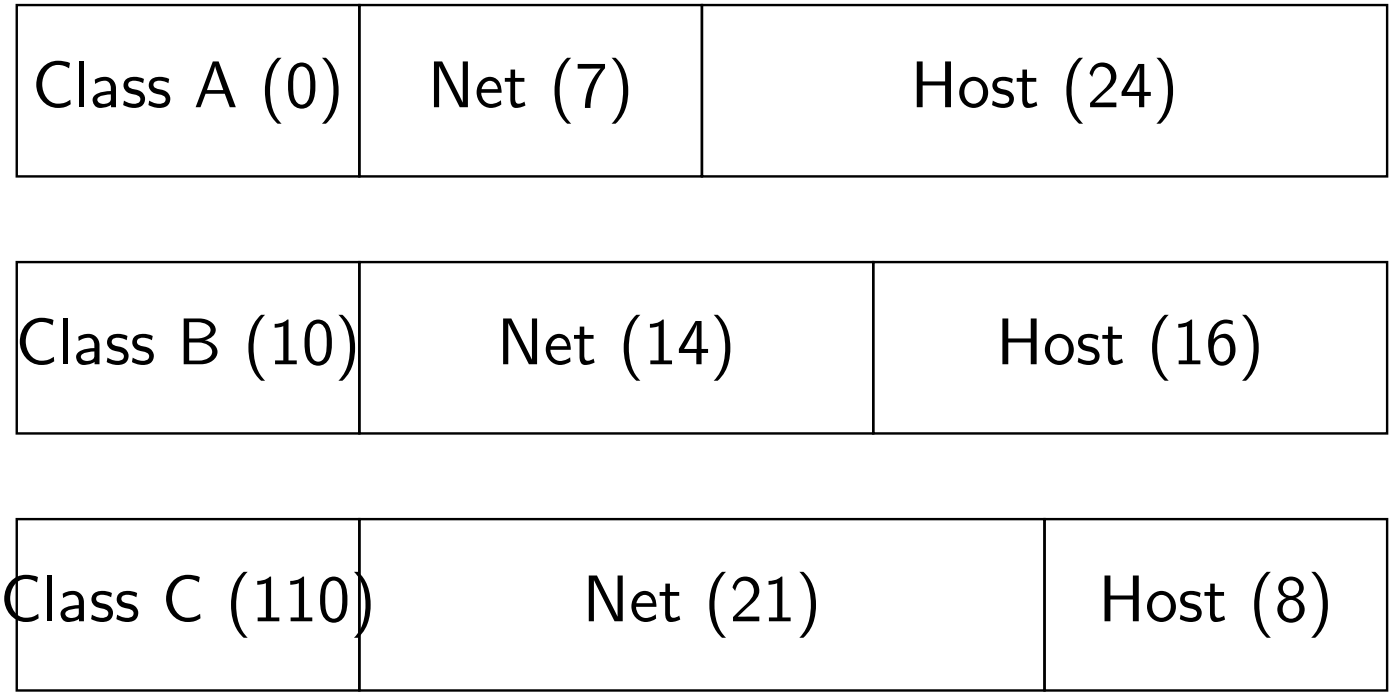
Advantages and Disadvantages

- Advantages: Universal deployment, widespread compatibility with legacy systems, simple to implement and manage on small networks, and supported by a vast array of tools and utilities.
- Disadvantages: Impending address exhaustion due to the 32-bit limit (only 4.3 billion addresses).
- Disadvantages: Lack of built-in security, as IPsec is optional and requires manual configuration.
- Disadvantages: Complex configuration for routing tables; NAT (Network Address Translation) is often required to conserve addresses, which breaks end-to-end connectivity.
- Disadvantages: No built-in Quality of Service (QoS) guarantees, relying instead on DiffServ or external mechanisms.

Classful Addressing Scheme

- The original architecture of the Internet divided the IP address space into five primary classes: A, B, C, D, and E.
- Class A: Leading bit 0. Network ID is 8 bits, Host ID is 24 bits. Range: 1.0.0.0 to 126.255.255.255. Used for very large networks.
- Class B: Leading bits 10. Network ID is 16 bits, Host ID is 16 bits. Range: 128.0.0.0 to 191.255.255.255. Used for medium-sized networks.
- Class C: Leading bits 110. Network ID is 24 bits, Host ID is 8 bits. Range: 192.0.0.0 to 223.255.255.255. Used for small networks.
- Class D: Leading bits 1110. Range: 224.0.0.0 to 239.255.255.255. Reserved exclusively for multicast groups.
- Class E: Leading bits 1111. Range: 240.0.0.0 to 255.255.255.255. Reserved for future use and experimental research.

Classful Address Format



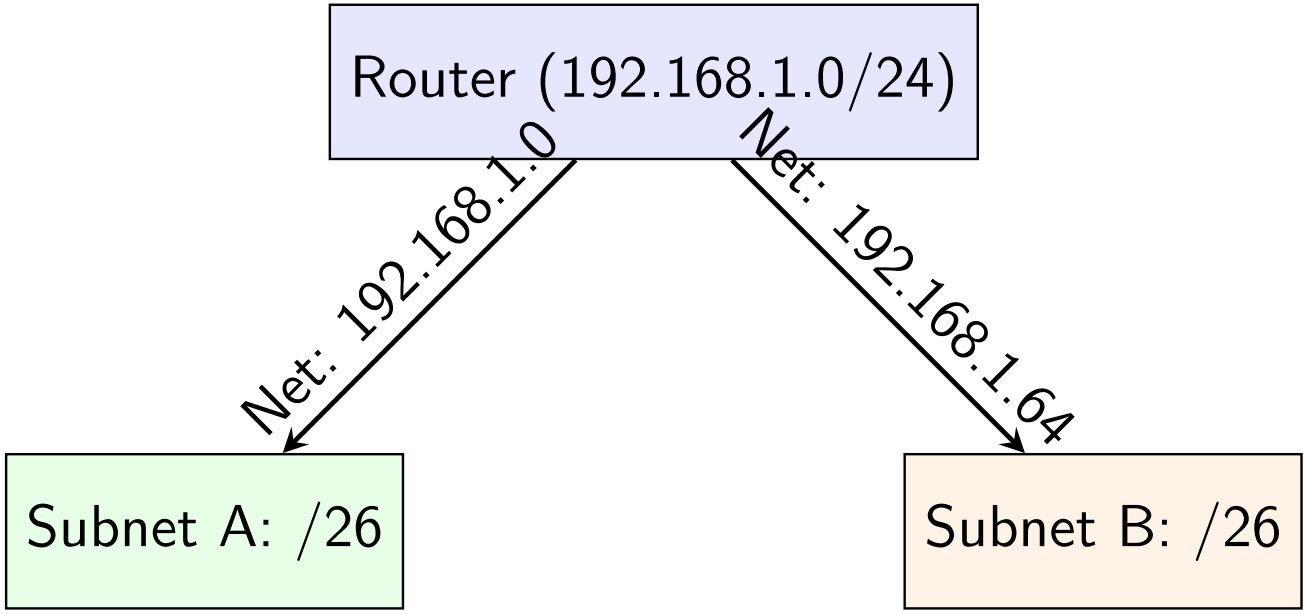
Classless Addressing Scheme (CIDR)

- Classless Inter-Domain Routing (CIDR) was introduced in 1993 to replace the inefficient classful network design.
- CIDR's primary goals were to slow the rapid exhaustion of IPv4 addresses and to limit the exponential growth of routing tables in core internet routers.
- It supports Variable-Length Subnet Masking (VLSM), meaning network prefixes can be of any length, not just restricted to 8, 16, or 24 bits.
- An IP address in CIDR is written with a slash suffix indicating the exact number of bits in the network prefix (e.g., 192.168.1.0/24).
- The suffix '/24' implies that the first 24 bits represent the network portion, leaving the remaining 8 bits for host addresses.

Subnet & Masking

- Subnetting is the logical division of a single, large IP network into multiple smaller, manageable broadcast domains called subnets.
- A subnet mask is a 32-bit number used to differentiate the network component of an IP address from the host component.
- Subnetting is calculated by performing a bitwise AND operation between the IP address and the configured subnet mask.
- For example, applying the subnet mask 255.255.255.0 to the IP 192.168.1.10 isolates the network address 192.168.1.0.
- By borrowing bits from the host portion of the address to create a subnet identifier, administrators can significantly improve network performance and security.

Subnetting Hierarchy



Reserved Address

- Certain IPv4 address blocks are strictly reserved by the IANA for specialized networking purposes and cannot be routed on the global internet.
- Loopback Address: 127.0.0.0/8 (usually configured as 127.0.0.1) allows a host interface to send packets back to itself for internal network stack testing.
- Private IP Addresses: Defined in RFC 1918 (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16) for use entirely within isolated LAN environments.
- Zero Address: 0.0.0.0/8 is typically used in routing tables to denote a default route (0.0.0.0/0) or an unknown source address during initial boot.
- Broadcast Address: 255.255.255.255 acts as a limited broadcast to reach every single host active on the immediate local network segment.
- Link-Local Addresses: The 169.254.0.0/16 block (APIPA) is utilized for automatic self-assignment when no DHCP server

Computer Networks (DI03000051)

GTU Diploma Engineering

Agenda

- 1. IPv4: Characteristics
- 2. Advantages and Disadvantages
- 3. Classful Addressing Scheme
- 4. Classless Addressing Scheme (CIDR)
- 5. Subnet & Masking
- 6. Reserved Addresses

IPv4: Characteristics

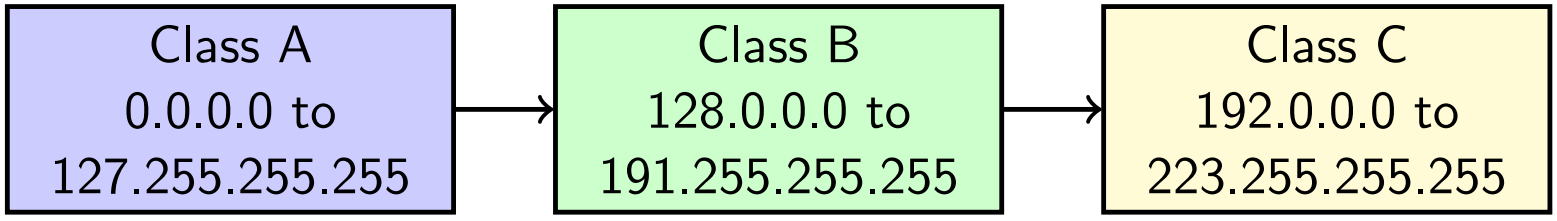
- Internet Protocol version 4 (IPv4) is the fourth version of the Internet Protocol and the core protocol of standards-based internetworking methods in the Internet.
- IPv4 uses a 32-bit address space, limiting it to 4,294,967,296 (2^32)*uniqueaddresses*.

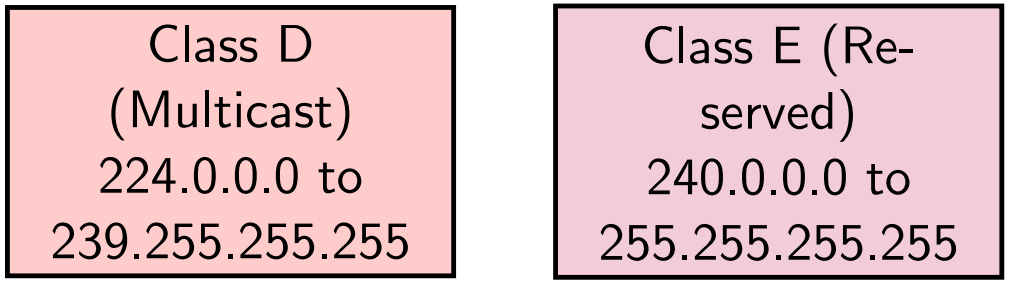
- It operates at the Network Layer (Layer 3) of the OSI model.
- IPv4 is a connectionless protocol, meaning data is sent without establishing a dedicated connection beforehand.
- It operates on a best-effort delivery model, meaning it does not guarantee delivery, proper sequencing, or avoidance of duplicate delivery. These aspects are handled by upper-layer protocols like TCP.
- The IPv4 header is variable in length (20 to 60 bytes) depending on the Options field, though it is most commonly 20 bytes.

Advantages and Disadvantages

- Advantages:
- - Widespread Adoption: IPv4 is universally supported and forms the foundation of most existing network infrastructure.
- - Simple Addressing: The 32-bit dotted-decimal notation (e.g., 192.168.1.1) is relatively easy for humans to read and remember compared to IPv6.
- - Proven Reliability: Decades of use have resulted in highly optimized routing algorithms and robust hardware support.
- Disadvantages:
- - Address Exhaustion: The theoretical limit of 4.3 billion addresses has been reached, necessitating workarounds like NAT (Network Address Translation).
- - Security: IPSec is optional in IPv4, unlike IPv6 where it is a mandatory standard, making native IPv4 communications potentially less secure.
- - Configuration: Often requires manual configuration (static IP) or reliance on DHCP, lacking the robust stateless

Classful Addressing Scheme





Classful Addressing: Details

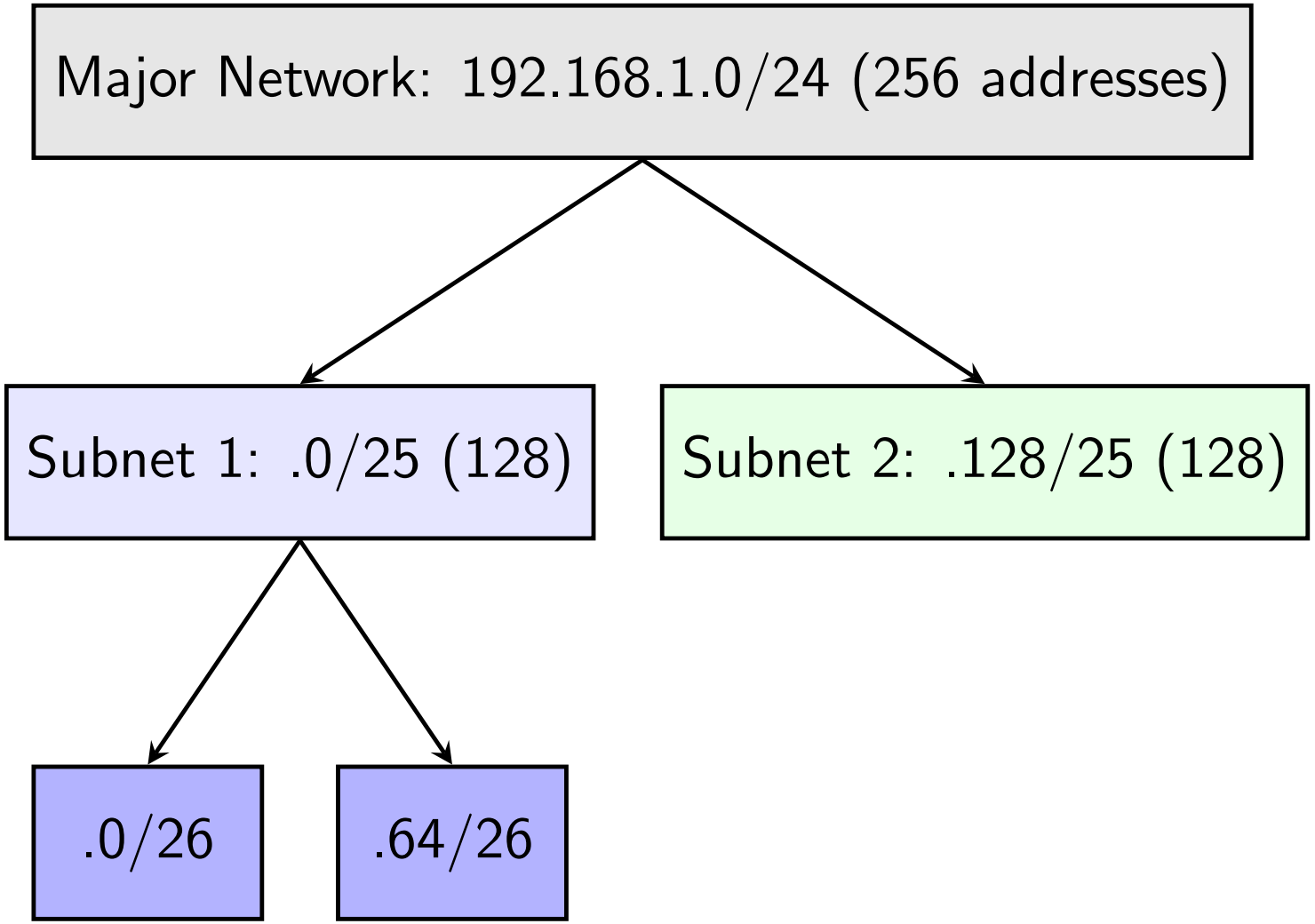
- In classful addressing, the IP address space is divided into five classes: A, B, C, D, and E.
- Class A: Designed for huge networks. The first octet is the network ID (leading bit '0'), leaving 24 bits for hosts. Subnet Mask: 255.0.0.0.
- Class B: Designed for medium-sized networks. The first two octets are the network ID (leading bits '10'), leaving 16 bits for hosts. Subnet Mask: 255.255.0.0.
- Class C: Designed for small networks. The first three octets are the network ID (leading bits '110'), leaving 8 bits for hosts. Subnet Mask: 255.255.255.0.
- Class D: Reserved for Multicasting (leading bits '1110'). No subnet mask applies.
- Class E: Reserved for experimental purposes and future use (leading bits '1111').

Classless Addressing Scheme (CIDR)

- Classless Inter-Domain Routing (CIDR) was introduced in 1993 to replace classful addressing and slow the exhaustion of IPv4 addresses.
- CIDR allows for variable-length subnet masking (VLSM), meaning network boundaries can occur at any bit position, not just on octet boundaries (/8, /16, /24).
- It uses CIDR notation, represented by the IP address followed by a slash ('/') and the number of network bits (e.g., 192.168.1.0/26).
- A /26 network provides 64 addresses ($2^{(32-26)}$), $reducingwastecomparedtoallocatingafullClassC/24networkwi$

- CIDR enables route aggregation (supernetting), allowing a single routing table entry to represent multiple contiguous networks, significantly reducing the size of global routing tables.

Subnet & Masking



Subnetting Concepts

- Subnetting is the practice of dividing a larger network into smaller, logical sub-networks (subnets).
- It improves network performance by reducing broadcast domains (broadcast traffic is confined to the subnet).
- It enhances security by allowing administrators to apply firewall policies and access controls between subnets.
- A Subnet Mask is a 32-bit number that masks an IP address and divides it into network address and host address.
- The mask operates by performing a bitwise AND operation between the IP address and the subnet mask to determine the network ID.
- Formula for hosts per subnet:
  $2^h - 2(wherehisthenumberofhostbits).The' - 2'accountsforthenetworkaddress(all0s)andbroadcastaddress(all1s)$

Reserved Addresses

- Specific IPv4 addresses and blocks are reserved by IANA for special purposes and cannot be routed on the public Internet.
- Private IP Ranges (RFC 1918): Used for local area networks behind NAT.
- - 10.0.0.0 to 10.255.255.255 (10.0.0.0/8)
- - 172.16.0.0 to 172.31.255.255 (172.16.0.0/12)
- - 192.168.0.0 to 192.168.255.255 (192.168.0.0/16)
- Loopback Address (127.0.0.0/8): Used to test the local network stack (typically 127.0.0.1).
- APIPA / Link-Local (169.254.0.0/16): Auto-assigned when a DHCP server is unavailable.
- Limited Broadcast (255.255.255.255): Used to send a message to every host on the local network segment.

Computer Networks (DI03000051)

GTU Diploma Engineering

Agenda

- IPv4 Characteristics
- Advantages and Disadvantages
- Classful Addressing Scheme
- Classless Addressing Scheme (CIDR)
- Subnetting & Masking
- Reserved Addresses

IPv4 Characteristics

- Connectionless protocol: No connection is established before data is sent.
- Best-effort delivery: Does not guarantee delivery, ordering, or error-free transmission.
- Media independent: Operates independently of the medium carrying the data.
- 32-bit addressing: Uses 32-bit logical addresses, providing approximately 4.3 billion unique IP addresses.
- Dotted-decimal notation: Addresses are represented as four octets separated by dots (e.g., 192.168.1.1).

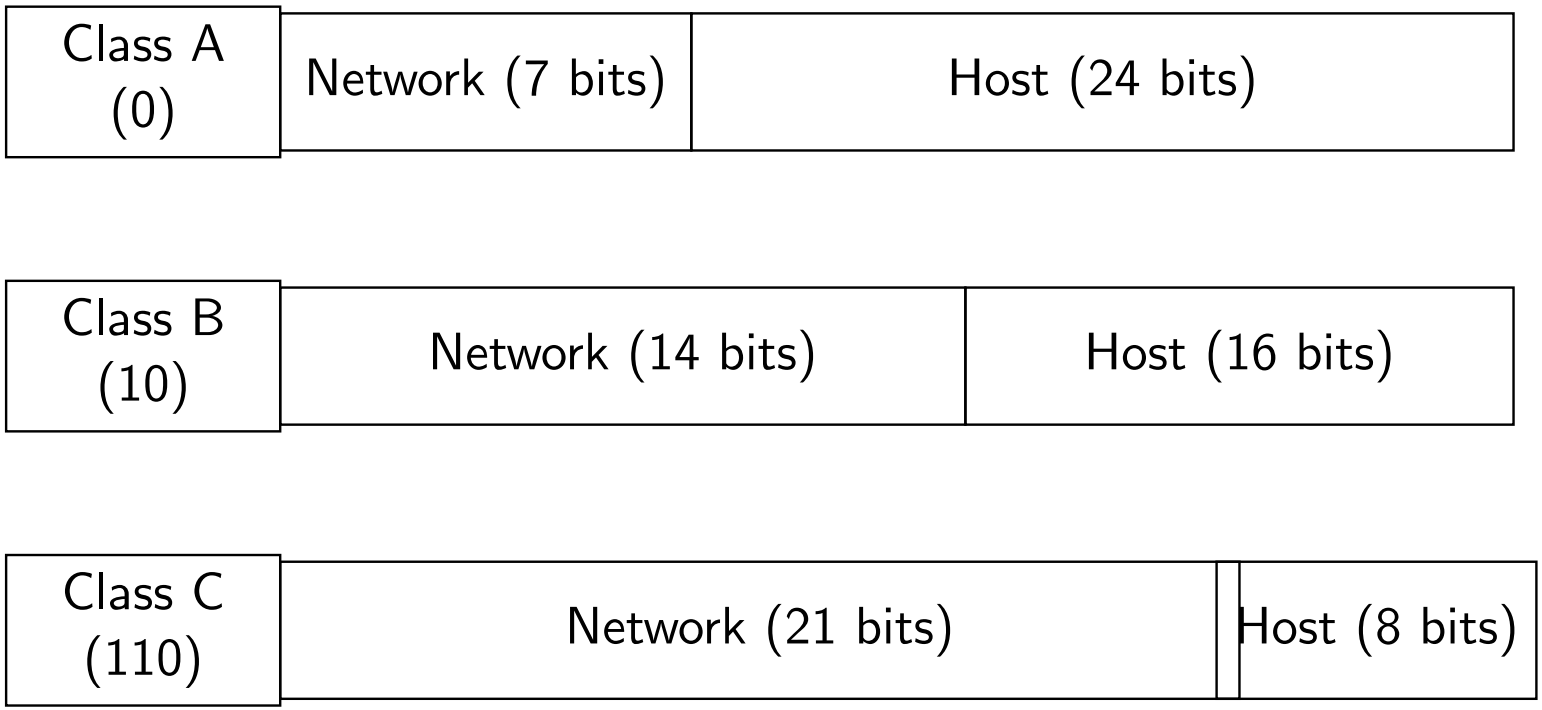
IPv4 Advantages & Disadvantages

- Advantages:
- Simplicity and widespread adoption: Supported by almost all network devices.
- Efficient routing: Simple header format allows for fast processing by routers.
- Disadvantages:
- Address exhaustion: The 32-bit address space is insufficient for the growing number of devices.
- Lack of built-in security: IPsec is optional, making it vulnerable to spoofing and interception.
- Inefficient address allocation: Classful addressing led to significant waste of IP addresses.

Classful Addressing Scheme

- Divided the IP address space into five classes: A, B, C, D, and E.
- Class A: 1st octet (1-126), Network prefix is 8 bits. Used for very large networks.
- Class B: 1st octet (128-191), Network prefix is 16 bits. Used for medium-sized networks.
- Class C: 1st octet (192-223), Network prefix is 24 bits. Used for small networks.
- Class D: 1st octet (224-239), reserved for Multicasting.
- Class E: 1st octet (240-255), reserved for Experimental use.

Classful Addressing Structure



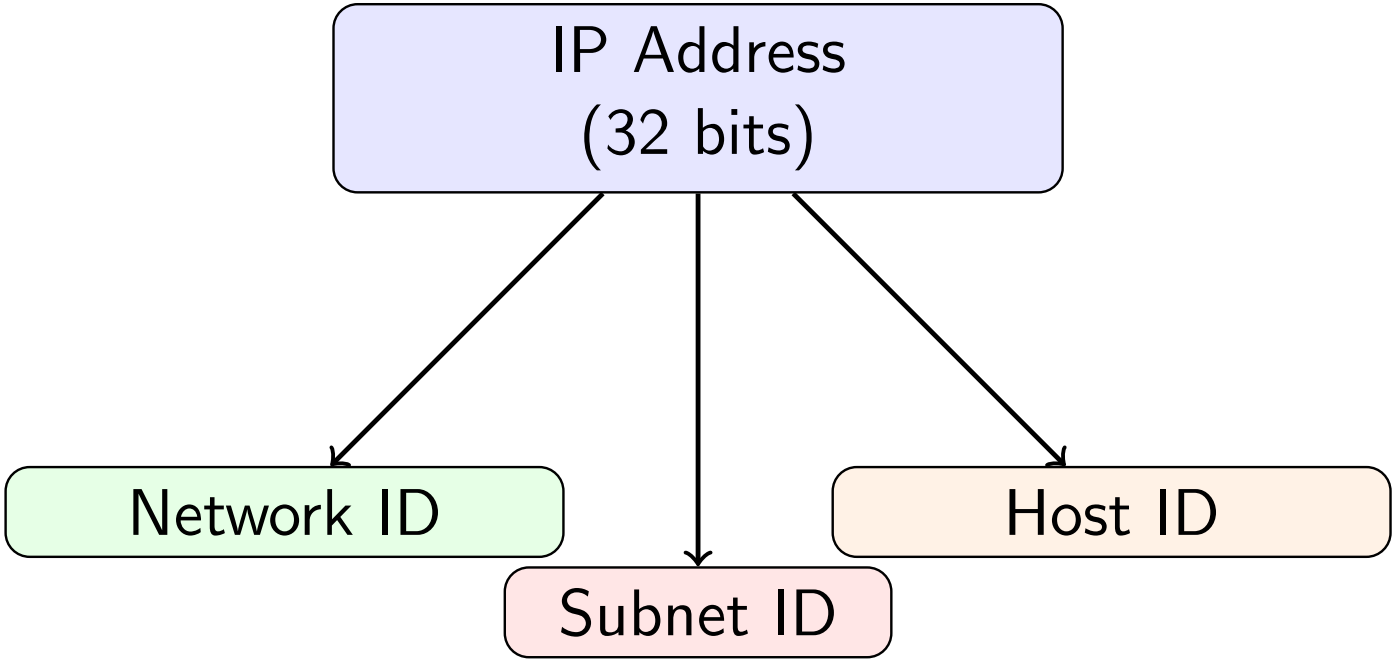
Classless Addressing Scheme (CIDR)

- CIDR (Classless Inter-Domain Routing) eliminates strict class boundaries.
- Allows for variable-length subnet masking (VLSM).
- Represented in slash notation (e.g., 192.168.1.0/24).
- The /24 indicates that the first 24 bits represent the network portion.
- Reduces routing table sizes through route summarization/aggregation.
- Significantly slows down IPv4 address exhaustion.

Subnetting & Masking

- Subnetting: The process of logically dividing a single large network into multiple smaller sub-networks (subnets).
- Improves network performance by reducing broadcast domain size and enhances security.
- Subnet Mask: A 32-bit number that masks an IP address and divides it into network address and host address.
- In a subnet mask, binary '1's represent the network portion, and binary '0's represent the host portion.
- Example: 255.255.255.0 (or /24) means the first 24 bits are network, the last 8 bits are for hosts.

Subnetting Concept Diagram



Subnet ID is borrowed from Host bits to create logical sub-networks

Reserved Addresses

- Private IP Addresses (RFC 1918): Not routable on the public internet.
- - 10.0.0.0 to 10.255.255.255 (10.0.0.0/8)
- - 172.16.0.0 to 172.31.255.255 (172.16.0.0/12)
- - 192.168.0.0 to 192.168.255.255 (192.168.0.0/16)
- Loopback Address (127.0.0.1): Used to test the local network interface.
- APIPA / Link-Local (169.254.0.0/16): Automatically assigned if DHCP fails.
- Broadcast Address (255.255.255.255): Targets all hosts on the local network.

Computer Networks (DI03000051)

GTU Diploma Engineering

Agenda

- IPv4 Characteristics
- Advantages and Disadvantages
- Classful Addressing Scheme
- Classless Addressing Scheme (CIDR)
- Subnetting & Masking
- Reserved Addresses

IPv4: Characteristics

- IPv4 uses 32-bit (4-byte) addresses, logically allowing for 4,294,967,296 (2^32)*uniquenumericaladdresses*.
- It is a connectionless protocol functioning at the Network Layer (Layer 3) of the OSI model, primarily responsible for logical routing.
- IPv4 operates on a best-effort delivery model, meaning it does not guarantee delivery, packet sequencing, or data integrity (these are handled by TCP at Layer 4).
- The standard IPv4 packet header is typically 20 bytes long (without options) and contains fields like Time to Live (TTL), Protocol, and Header Checksum.
- Addresses are conventionally represented in dot-decimal notation, dividing the 32 bits into four 8-bit octets (e.g., 192.168.1.1).

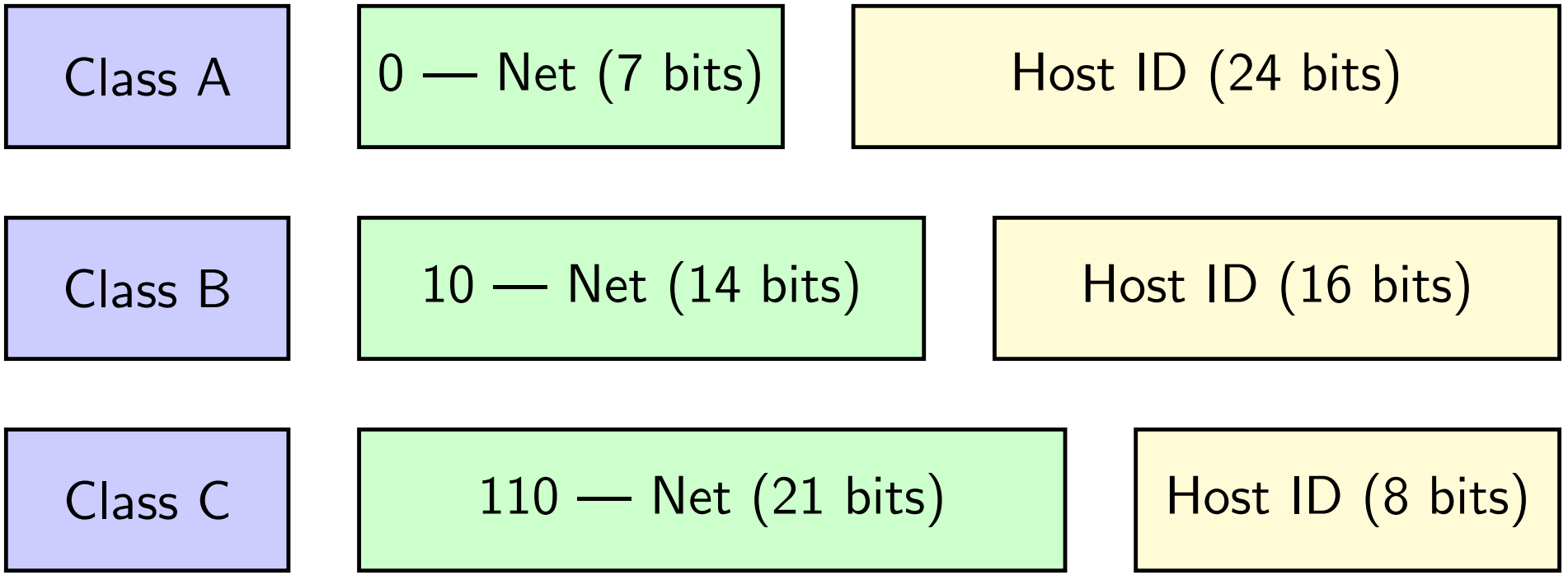
Advantages and Disadvantages

- Advantage: Extremely widely supported, mature, and robust protocol serving as the foundational layer of the legacy and current internet.
- Advantage: Operates seamlessly with highly optimized core routing protocols like OSPF and BGP.
- Disadvantage: Address exhaustion due to the limited 32-bit space, which necessitated the widespread adoption of NAT (Network Address Translation).
- Disadvantage: Lacks mandatory, built-in IPsec support natively, making traffic susceptible to interception without upper-layer encryption.
- Disadvantage: Heavy reliance on broadcast traffic (e.g., ARP, DHCP) which can cause network congestion in large flat topologies.

Classful Addressing Scheme

- Class A: Leading bit 0. 8-bit network ID, 24-bit host ID. Subnet mask 255.0.0.0. Supports 16.7 million hosts per network.
- Class B: Leading bits 10. 16-bit network ID, 16-bit host ID. Subnet mask 255.255.0.0. Supports 65,534 hosts per network.
- Class C: Leading bits 110. 24-bit network ID, 8-bit host ID. Subnet mask 255.255.255.0. Supports 254 hosts per network.
- Class D: Leading bits 1110 (224.0.0.0 to 239.255.255.255). Reserved strictly for Multicast groups.
- Class E: Leading bits 1111 (240.0.0.0 to 255.255.255.255). Reserved for experimental use and future R&D.

Classful Addressing Diagram



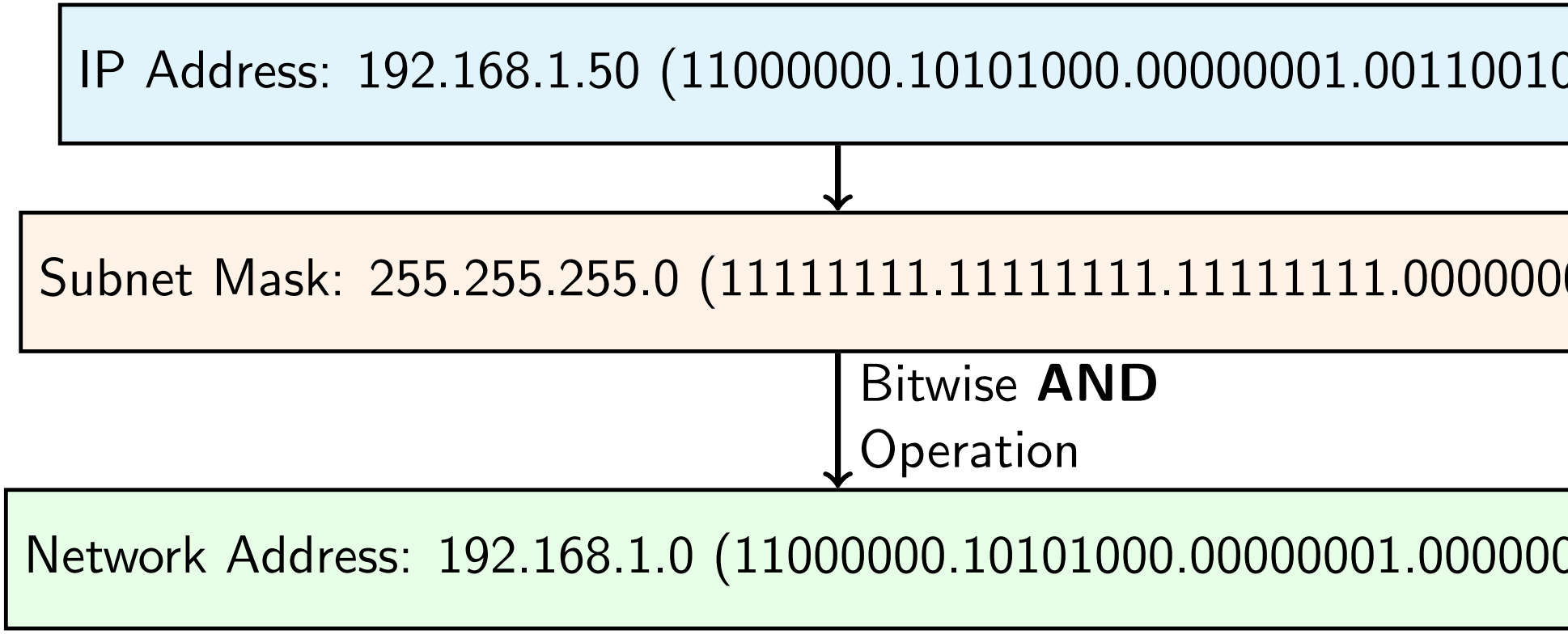
Classless Addressing Scheme (CIDR)

- CIDR (Classless Inter-Domain Routing) was introduced in 1993 (RFC 1519) to mitigate IP address exhaustion by eliminating rigid class boundaries.
- Allows Variable-Length Subnet Masking (VLSM), enabling network administrators to allocate IP space that precisely fits the required host count.
- Uses CIDR notation, appending a slash and the number of active network bits to the IP address (e.g., 192.168.1.0/26 means 26 network bits).
- Facilitates route aggregation (supernetting), allowing multiple contiguous subnets to be advertised as a single route, reducing core internet routing table sizes.
- For example, a /28 subnet provides 16 total IP addresses, yielding 14 usable host addresses after subtracting the network and broadcast addresses.

Subnetting & Masking

- Subnetting is the logical partitioning of a single massive network into multiple smaller, manageable, and more secure broadcast domains.
- A Subnet Mask is a 32-bit contiguous binary sequence used to distinguish the network prefix from the host identifier within an IP address.
- The specific Network Address is computationally determined by performing a bitwise AND operation between the device's IP address and the subnet mask.
- In binary representation, consecutive 1s represent the network/subnet portion, and consecutive 0s dictate the host portion.
- The formula for calculating usable hosts per subnet is $2^n - 2, where' n' represents the number of available host bits (0s in the mask)$.

Subnet Masking Diagram



Reserved Addresses

- 0.0.0.0/8: Represents the 'this' network. Often used in default routing or as a source address during DHCP Discover broadcasts.
- 127.0.0.0/8: Loopback addresses (e.g., 127.0.0.1) used for local host testing and internal inter-process communication without hardware transmission.
- Private IP Ranges (RFC 1918): 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. These address blocks are non-routable on the public internet.
- 169.254.0.0/16: Link-local block, typically known as APIPA (Automatic Private IP Addressing), assigned when a DHCP server is unreachable.
- 255.255.255.255: The limited broadcast address, effectively targeting every node strictly on the local physical network segment.

Computer Networks (DI03000051)

GTU Diploma Engineering

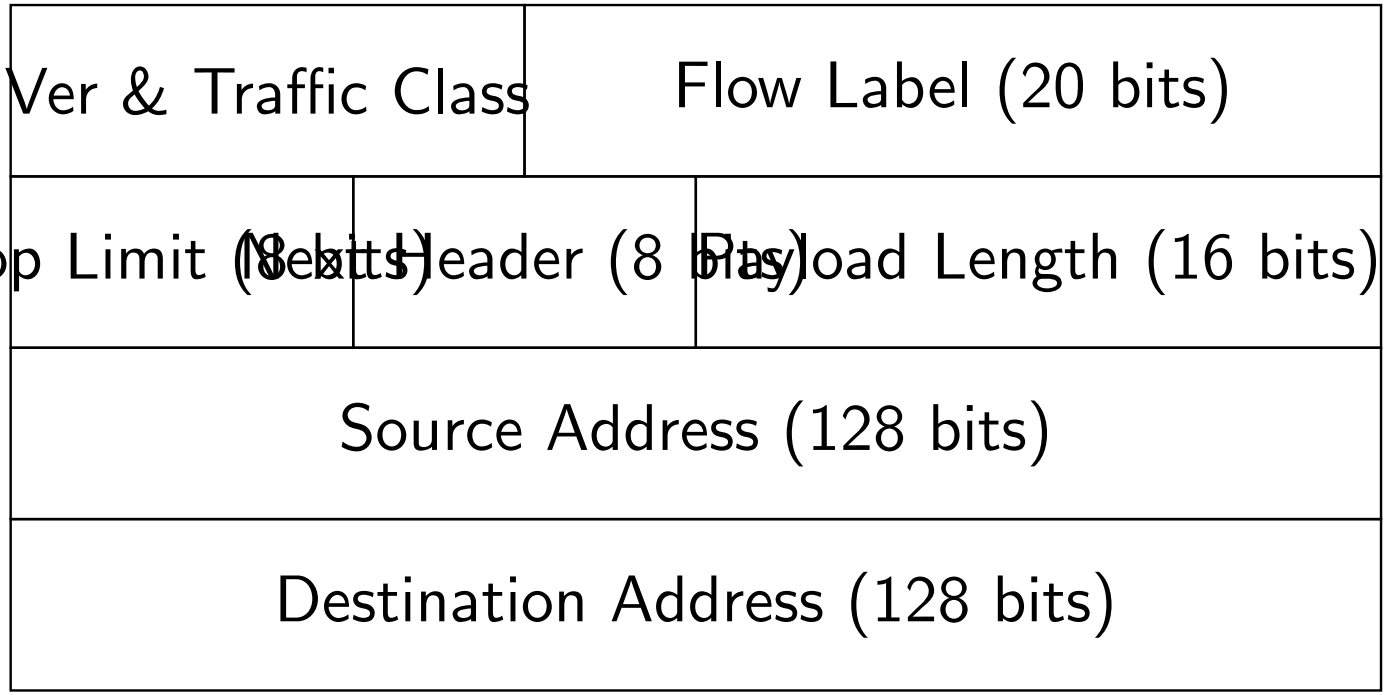
Agenda

- IPv6 Characteristics and Need
- IPv6 Addressing Modes
- IPv6 Address Types
- Special IPv6 Addresses

IPv6 Characteristics

- Expanded Addressing Capabilities: Increases address size from 32 bits to 128 bits, providing a virtually unlimited number of IP addresses (approx 3.4 x 10^38).
- Header Format Simplification: Fixed-length, 40-byte base header reduces processing overhead at routers.
- Improved Support for Extensions and Options: Options are placed in separate extension headers that are located between the IPv6 header and the transport-layer header.
- Flow Labeling Capability: Enables labeling of packets belonging to particular traffic flows for which the sender requests special handling, such as non-default quality of service or real-time service.
- Authentication and Privacy Capabilities: IPsec (AH and ESP) is deeply integrated into IPv6 architecture.

IPv6 Header Format Diagram



IPv6 Addressing Modes

- Unicast: An identifier for a single interface. A packet sent to a unicast address is delivered to the interface identified by that address.
- Multicast: An identifier for a set of interfaces (typically belonging to different nodes). A packet sent to a multicast address is delivered to all interfaces identified by that address.
- Anycast: An identifier for a set of interfaces (typically belonging to different nodes). A packet sent to an anycast address is delivered to one of the interfaces identified by that address (the 'nearest' one, according to the routing protocols' measure of distance).
- Note: IPv6 does not implement Broadcast addressing; its functions are superseded by Multicast.

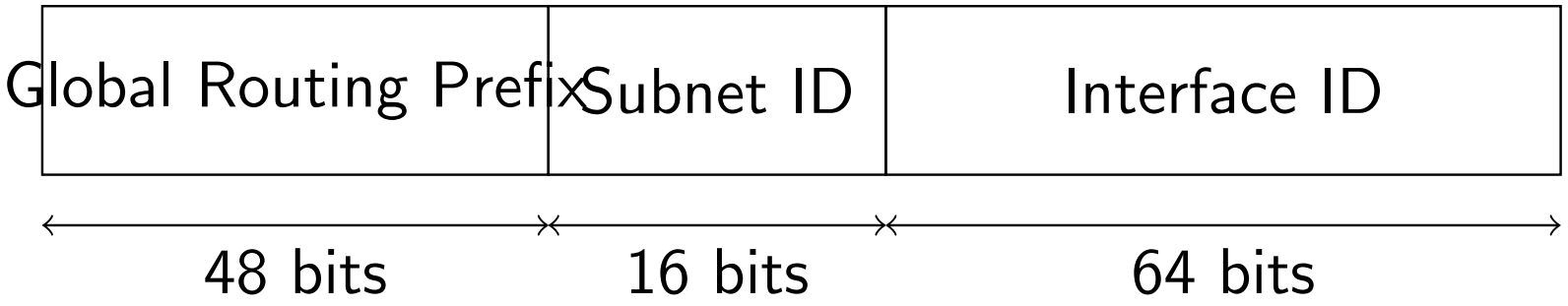
IPv6 Address Representation

- Format: 128 bits represented as eight groups of four hexadecimal digits, separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
- Zero Compression Rule 1: Leading zeros in a 16-bit group can be omitted. (e.g., :0000: becomes :0: and :0db8: becomes :db8:).
- Zero Compression Rule 2: One contiguous sequence of 16-bit blocks of zeros can be compressed into a double colon '::'. This can only be applied once per address to avoid ambiguity.
- Example: 2001:db8:0:0:0:0:2:1 compresses to 2001:db8::2:1.

IPv6 Address Types

- Global Unicast: Equivalent to IPv4 public addresses. Globally routable and reachable on the IPv6 Internet. Format generally uses a 48-bit global routing prefix, a 16-bit subnet ID, and a 64-bit interface ID.
- Link-Local Unicast: Used for communication among nodes on the same link. Automatically configured on all IPv6 interfaces. Prefix is FE80::/10.
- Unique Local Unicast (ULA): Analogous to IPv4 private addresses (RFC 1918). Intended for local communication within a site or between a limited number of sites. Prefix is FC00::/7.
- Multicast Addresses: Always begin with the prefix FF00::/8. Scope limits routing range (e.g., link-local multicast vs. site-local multicast).

Global Unicast Address Structure



Special IPv6 Addresses

- Unspecified Address: 0:0:0:0:0:0:0:0 or simply :: . Used by a host as its source address during initialization when it does not yet have a configured address (similar to 0.0.0.0 in IPv4).
- Loopback Address: 0:0:0:0:0:0:0:1 or ::1 . Identifies the loopback interface on a host, allowing a node to send packets to itself (equivalent to 127.0.0.1 in IPv4).
- IPv4-Mapped IPv6 Address: Used to represent IPv4 nodes as IPv6 addresses. Format is ::FFFF:d.d.d.d (where d.d.d.d is the IPv4 address).
- Documentation Prefix: 2001:db8::/32 is reserved for use in documentation and examples.

Summary

- IPv6 provides a massively expanded 128-bit address space, resolving IPv4 exhaustion.
- Simplified header structure (40 bytes fixed) improves router processing efficiency.
- Supports Unicast, Multicast, and Anycast addressing modes, formally eliminating Broadcast.
- Subnetting relies heavily on standardized 64-bit interface identifiers combined with varied network prefixes.
- Built-in security (IPsec) and QoS capabilities make IPv6 essential for modern, scalable networking.

Computer Networks (DI03000051)

GTU Diploma Engineering

Agenda

- IPv6 Characteristics
- IPv6 Addressing Modes
- IPv6 Address Types
- Special IPv6 Addresses

IPv6 Characteristics

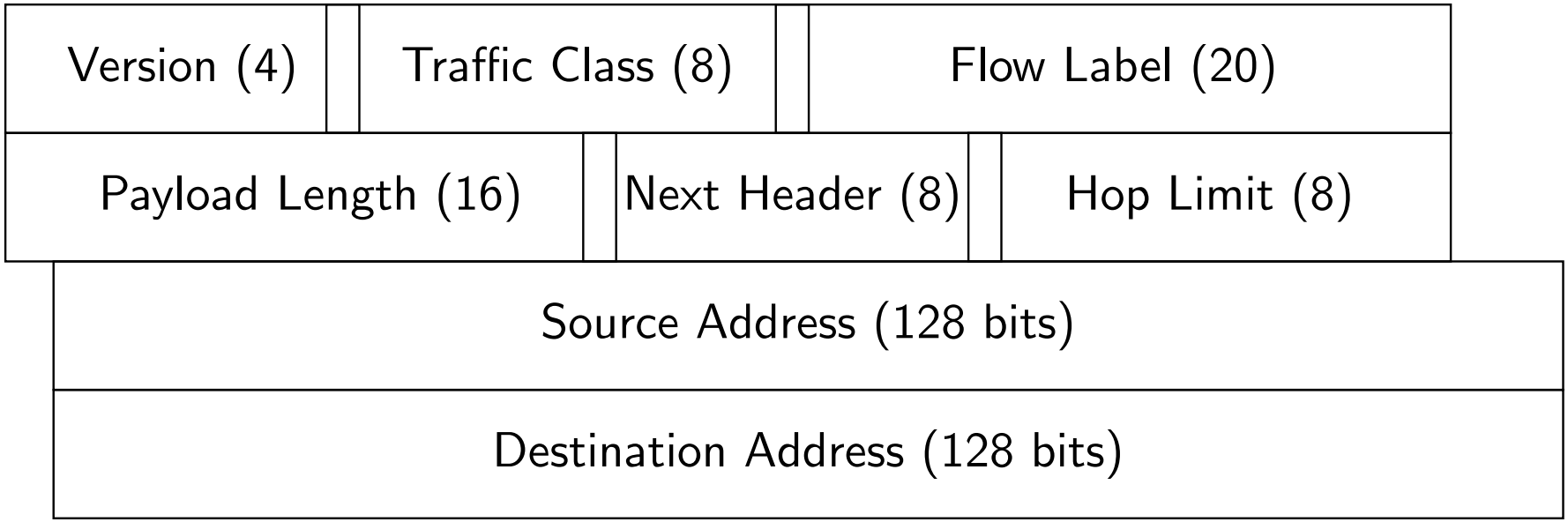
- 128-bit address space, allowing approximately 3.4 x 10^38*addresses*.

- Simplified header format: Only 8 fields compared to 14 in IPv4, enabling faster processing by routers.
- No checksum in the IPv6 header, relying on upper-layer protocols (TCP/UDP) for error detection.
- Built-in security (IPsec is mandated), providing authentication and encryption natively.
- Elimination of broadcast addressing; replaced entirely by multicast and anycast.
- Stateless Address Autoconfiguration (SLAAC) allows hosts to generate their own IP addresses without a DHCP server.

IPv6 Header Format

- Version (4 bits): Indicates IPv6 (value = 6).
- Traffic Class (8 bits): Similar to IPv4 ToS, used for QoS packet prioritization.
- Flow Label (20 bits): Identifies packets belonging to the same flow for non-default routing.
- Payload Length (16 bits): Length of the IPv6 payload (extension headers + upper-layer data).
- Next Header (8 bits): Identifies the type of header immediately following the IPv6 header.
- Hop Limit (8 bits): Decremented by 1 at each router (similar to IPv4 TTL).
- Source Address (128 bits): The original sender of the packet.
- Destination Address (128 bits): The intended recipient of the packet.

IPv6 Base Header Layout



Addressing Modes

- Unicast: Delivers a packet to a single specific interface. The most common addressing mode.
- Multicast: Delivers a packet to a set of interfaces (typically on different nodes). Replaces IPv4 broadcast.
- Anycast: Delivers a packet to a set of interfaces, but it is routed to the 'nearest' interface among them (based on routing distance).
- Note: IPv6 does NOT have broadcast addresses. Multicast handles all one-to-many communication needs, such as ARP replacement (NDP).

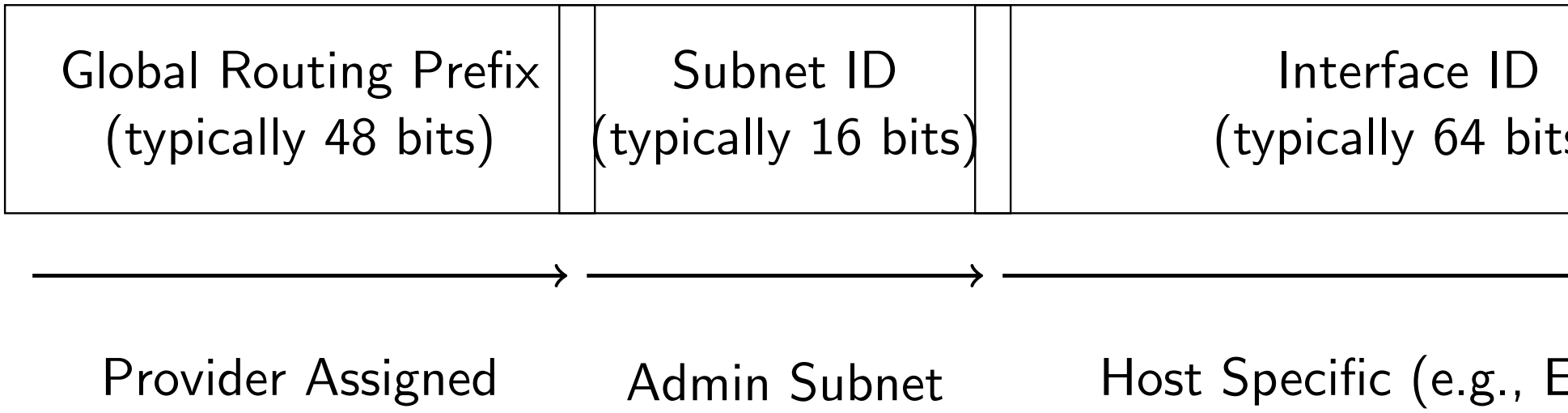
IPv6 Address Representation

- Represented as eight groups of four hexadecimal digits (16 bits each), separated by colons (:).
- Example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
- Rule 1 (Omit Leading Zeros): 0db8 becomes db8. 0000 becomes 0.
- Rule 2 (Double Colon): Contiguous sequences of zero blocks can be replaced by a double colon (::). This can only be applied ONCE per address.
- Compressed Example: 2001:db8:85a3::8a2e:370:7334

Address Types and Scopes

- Global Unicast (2000::/3): Routable on the public internet, analogous to IPv4 public addresses.
- Link-Local (fe80::/10): Used for communication on a single local network segment. Not routable. Used for Neighbor Discovery.
- Unique Local (fc00::/7): Routable within an organization's private network but not on the public internet. Analogous to IPv4 private addresses (RFC 1918).
- Multicast (ff00::/8): Used for one-to-many communication. Flags and Scope ID determine the behavior and range.

Global Unicast Address Structure



Special IPv6 Addresses

- Unspecified Address (::/128): All zeros. Used as a source address during initialization. Equivalent to 0.0.0.0 in IPv4.
- Loopback Address (::1/128): Used by a node to send an IPv6 packet to itself. Equivalent to 127.0.0.1 in IPv4.
- IPv4-Mapped IPv6 Address (::ffff:0:0/96): Used to represent an IPv4 address within the IPv6 address space, easing transition.
- Documentation Prefix (2001:db8::/32): Reserved specifically for use in examples and documentation to prevent conflict with live networks.

Computer Networks (DI03000051)

GTU Diploma Engineering

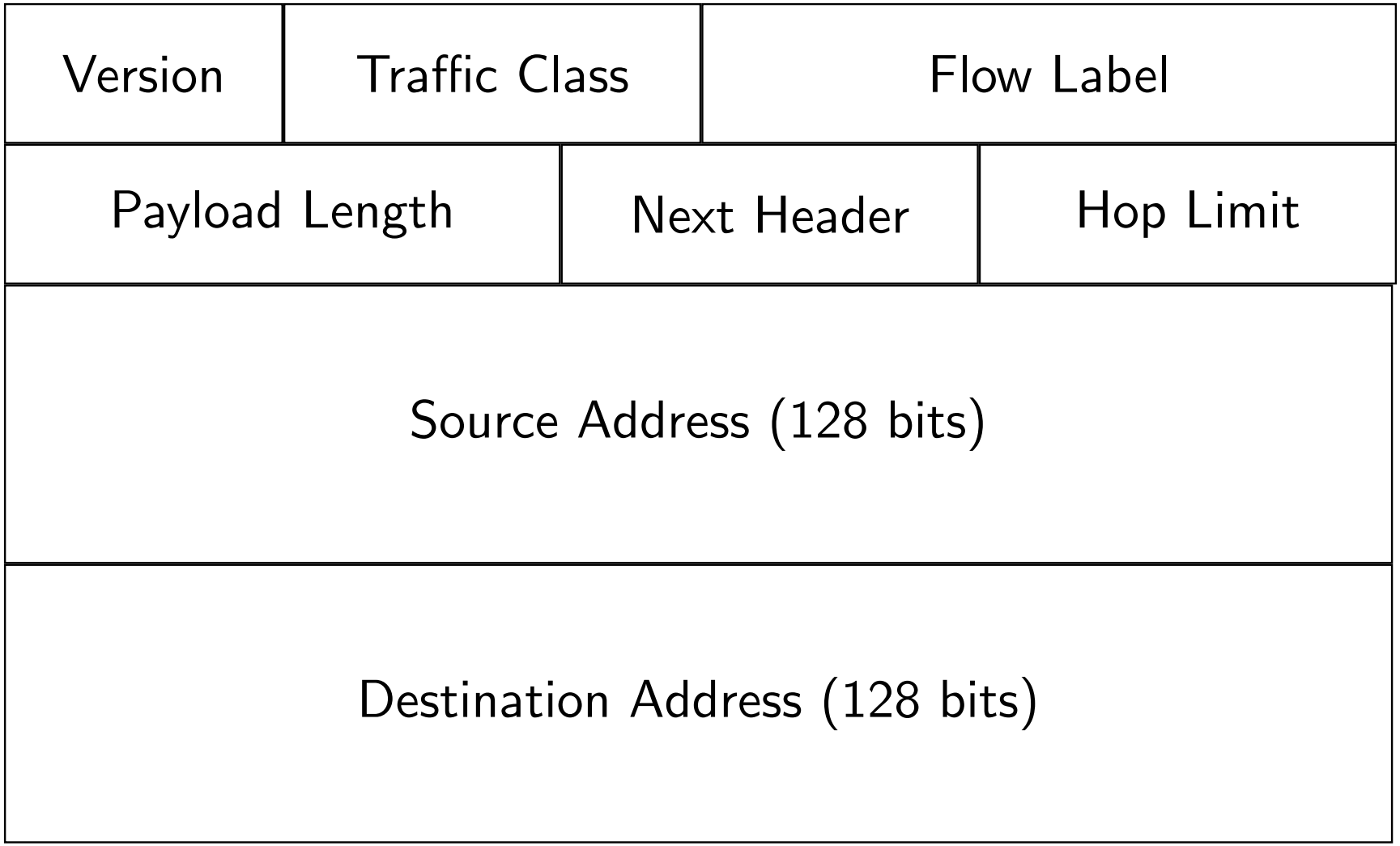
Agenda

- Characteristics of IPv6
- IPv6 Addressing Modes
- IPv6 Address Types
- Special Addresses in IPv6

Characteristics of IPv6

- 128-bit address space, allowing for 3.4×10^38 *uniqueaddresses*.
- Simplified Header Format: Reduced from 14 fields in IPv4 to 8 fields in IPv6 for faster processing.
- No Checksum in Header: Relies on upper-layer protocols (TCP/UDP) to ensure data integrity.
- Built-in Security: IPsec is mandatory in IPv6, providing authentication and encryption natively.
- Stateless Address Autoconfiguration (SLAAC): Devices can generate their own IP addresses without a DHCP server.
- Elimination of Broadcasts: Uses multicast and anycast instead of broadcast for network communications.

IPv6 Header Structure



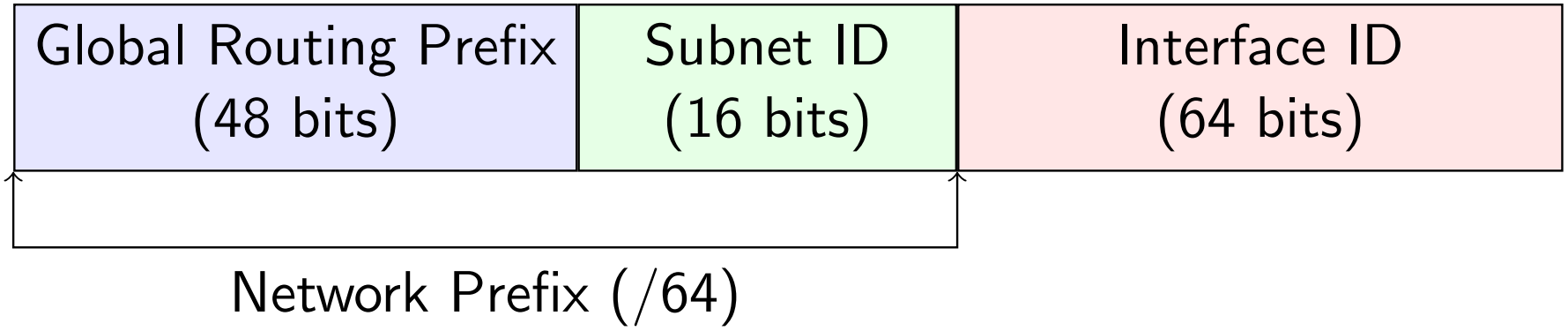
IPv6 Addressing Modes

- Unicast: Identifies a single interface. A packet sent to a unicast address is delivered to the interface identified by that address.
- Multicast: Identifies a group of interfaces, typically belonging to different nodes. A packet sent to a multicast address is delivered to all interfaces identified by that address.
- Anycast: Identifies a set of interfaces, but a packet sent to an anycast address is delivered to the 'closest' interface (according to routing protocols) among the set.
- Note: IPv6 does not implement Broadcast addressing. Multicast handles functionalities previously reliant on broadcast.

IPv6 Address Types

- Global Unicast Address (GUA): Globally routable and reachable on the IPv6 Internet. Equivalent to public IPv4 addresses. Starts with 2000::/3.
- Link-Local Address (LLA): Used for communication within a single local subnet. Not routable across routers. Always begins with fe80::/10.
- Unique Local Address (ULA): Intended for local communications within a site or multiple sites. Routable within private networks but not on the global Internet. Begins with fc00::/7.
- Multicast Addresses: Used for one-to-many communication. Begin with ff00::/8.

Global Unicast Address Structure



Special IPv6 Addresses

- Unspecified Address: ::/128 (all zeros). Used when a device does not yet have an assigned IPv6 address.
- Loopback Address: ::1/128. Used by a node to send an IPv6 packet to itself. Equivalent to 127.0.0.1 in IPv4.
- IPv4-Mapped IPv6 Address: ::ffff:0:0/96. Used to represent an IPv4 address within an IPv6 network, easing transition.
- Documentation Prefix: 2001:db8::/32. Reserved for use in documentation and examples to prevent conflicts with real addresses.

IPv6 Address Representation

- Represented as eight groups of four hexadecimal digits separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
- Rule 1: Leading Zeros can be omitted within any group. (e.g., 0db8 becomes db8, 0000 becomes 0).
- Rule 2: Double Colon (::). One contiguous sequence of multiple zero-value groups can be replaced with a double colon. This can only be used once per address.
- Example simplification: 2001:0db8:0000:0000:0000:ff00:0042:8329 can be written as 2001:db8::ff00:42:8329.

Summary

- IPv6 provides a vastly larger address space (128-bit) to solve IPv4 exhaustion.
- Features streamlined headers, mandatory IPsec, and SLAAC.
- Replaces broadcast with robust multicast and anycast capabilities.
- Special addresses handle loopback, unspecified states, and IPv4 transition.
- Addresses can be compressed using leading zero omission and double colon rules.

Computer Networks (DI03000051)

GTU Diploma Engineering

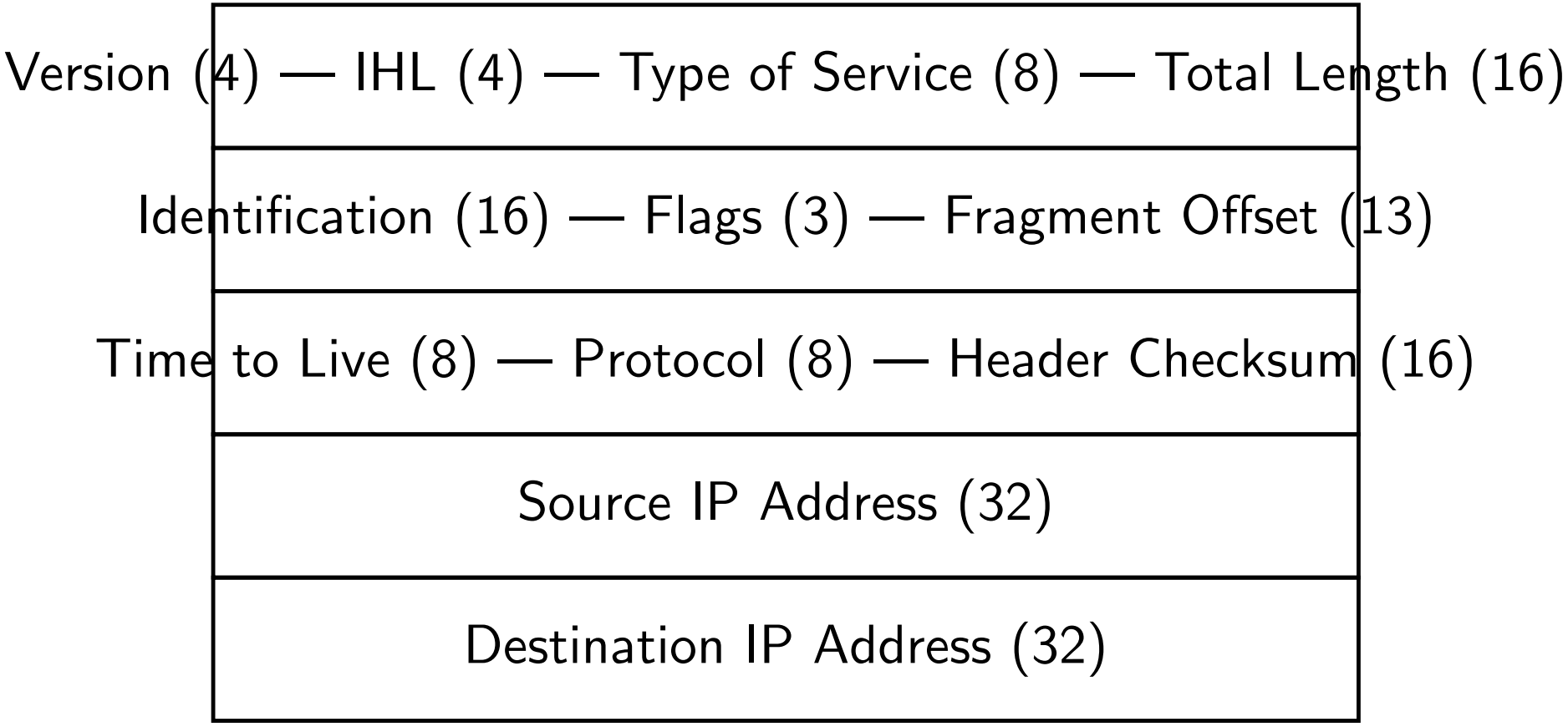
Agenda

1. Address Space and Format
2. IPv4 Header Structure
3. IPv6 Header Structure
4. Header Complexity and Checksums
5. Security (IPsec)
6. Fragmentation
7. Network Configuration
8. Summary of Differences

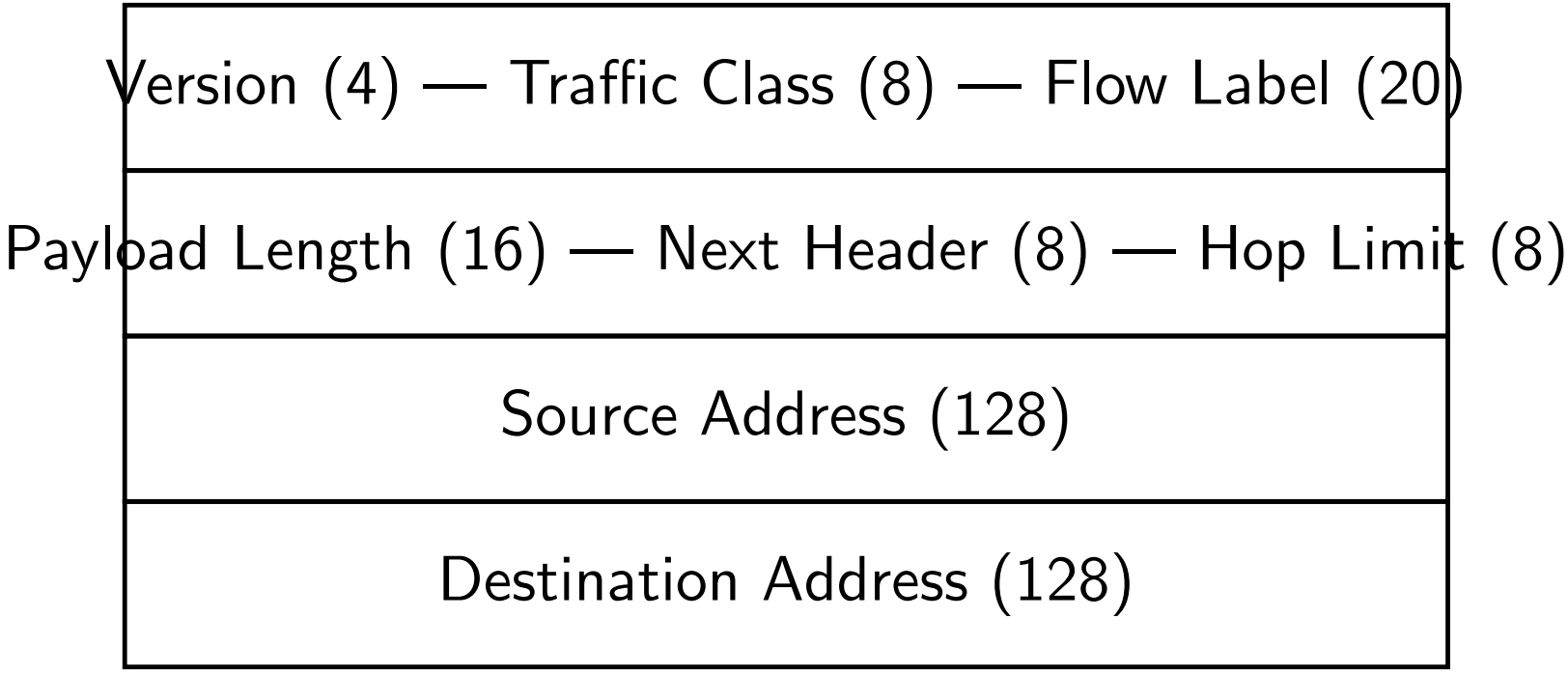
Address Space and Format

- IPv4 uses a 32-bit address space, allowing for approximately 4.3 billion unique IP addresses (2^32).
- IPv4 addresses are typically represented in dotted-decimal notation (e.g., 192.168.1.1).
- IPv6 uses a 128-bit address space, allowing for 340 undecillion addresses (2^128).
- IPv6 addresses are represented in hexadecimal format, separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

IPv4 Header Structure Diagram



IPv6 Header Structure Diagram



Header Complexity and Checksums

- IPv4 has a variable length header (20-60 bytes) due to the Options field. It also includes a Header Checksum that must be recalculated at every router.
- IPv6 has a fixed 40-byte header, greatly simplifying router processing.
- IPv6 eliminates the Header Checksum entirely, relying on upper-layer protocols (like TCP or UDP) and link-layer error detection to ensure data integrity.
- Extension headers in IPv6 handle options, linked as a chain after the main header.

Security (IPsec)

- In IPv4, IPsec (Internet Protocol Security) is optional and often requires manual configuration or add-on software.
- In IPv6, IPsec support is fundamentally built into the protocol.
- While not strictly mandatory for every single packet in modern standard revisions, the framework for end-to-end security, authentication, and payload encryption is natively integrated into IPv6 extension headers.

Fragmentation

- IPv4 allows routers to fragment packets if they exceed the Maximum Transmission Unit (MTU) of the next link.
- This router-level fragmentation causes processing overhead.
- IPv6 requires the sending host to perform Path MTU Discovery and fragment the packet before sending.
- Routers in an IPv6 network will simply drop packets that are too large and send an ICMPv6 'Packet Too Big' message back to the source.

Network Configuration

- IPv4 relies heavily on DHCP (Dynamic Host Configuration Protocol) for automatic IP address assignment, or manual static configuration.
- IPv6 introduces SLAAC (Stateless Address Autoconfiguration).
- With SLAAC, a host can autonomously generate its own IPv6 address using the network prefix advertised by a local router combined with a locally generated interface identifier.

Summary of Differences

- Address Space: IPv4 (32-bit) vs IPv6 (128-bit).
- Header: IPv4 (Variable length, complex) vs IPv6 (Fixed length, streamlined).
- Checksum: IPv4 (Header checksum included) vs IPv6 (No header checksum).
- Fragmentation: IPv4 (By routers and hosts) vs IPv6 (By sending host only).
- Configuration: IPv4 (DHCP/Manual) vs IPv6 (SLAAC/DHCPv6).

Computer Networks (DI03000051)

GTU Diploma Engineering

Agenda

- Overview of IPv4 and its limitations
- Introduction to IPv6
- Address Space Comparison
- Header Format Differences
- Security and IPsec
- Configuration and Fragmentation
- Summary of Differences

IPv4 Overview and Limitations

- Internet Protocol version 4 (IPv4) is the fourth version of the Internet Protocol (IP).
- It uses a 32-bit address space, providing approximately 4.3 billion unique addresses.
- Due to the rapid growth of the Internet, IPv4 address exhaustion became a critical issue.
- Techniques like Network Address Translation (NAT) and Classless Inter-Domain Routing (CIDR) were introduced to delay exhaustion.
- IPv4 relies heavily on ARP for address resolution and IGMP for multicast management.

Introduction to IPv6

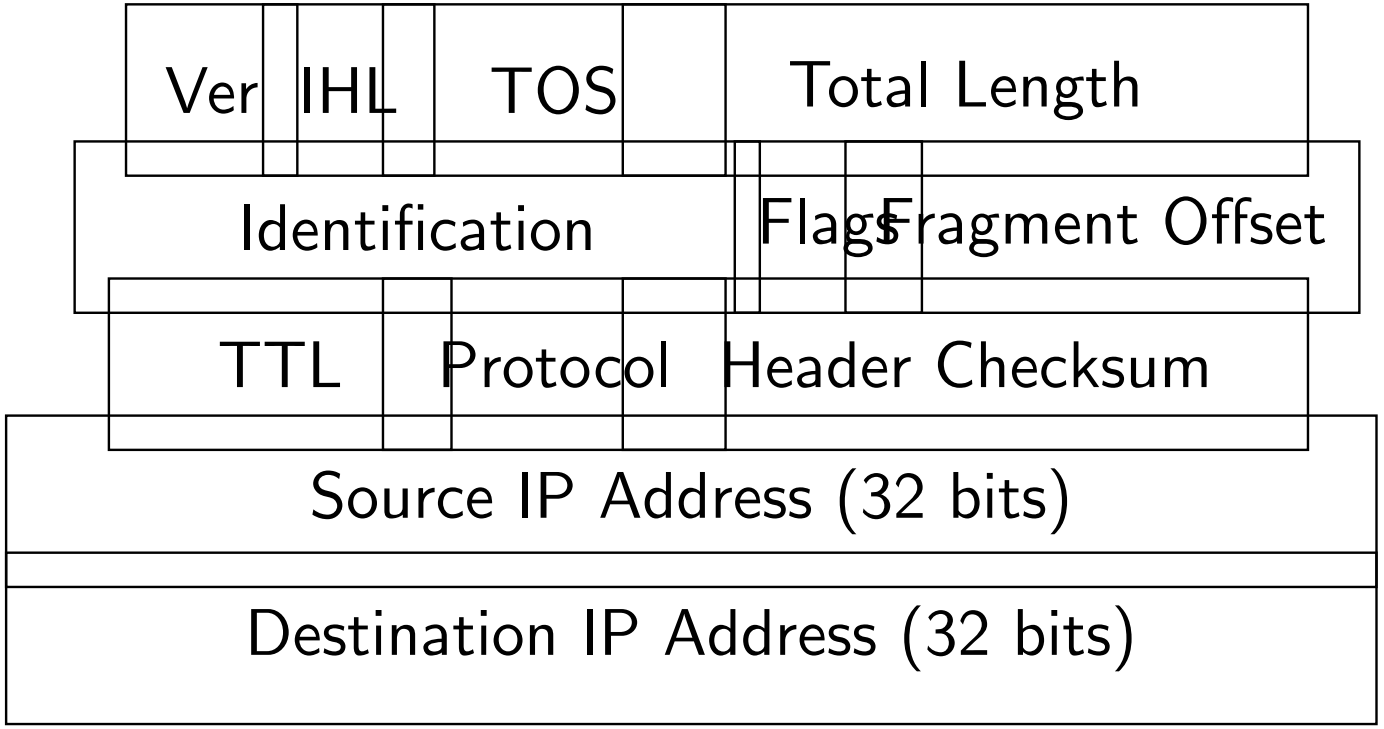
- Internet Protocol version 6 (IPv6) was designed by the IETF to replace IPv4 and solve the address exhaustion problem.
- It features a vastly expanded 128-bit address space, allowing for $3.4 \times 10^38 unique addresses$.

- IPv6 simplifies the header format to reduce processing overhead at routers.
- It inherently supports stateless address autoconfiguration (SLAAC) and eliminates the need for NAT.
- Neighbor Discovery Protocol (NDP) replaces ARP, improving efficiency and security.

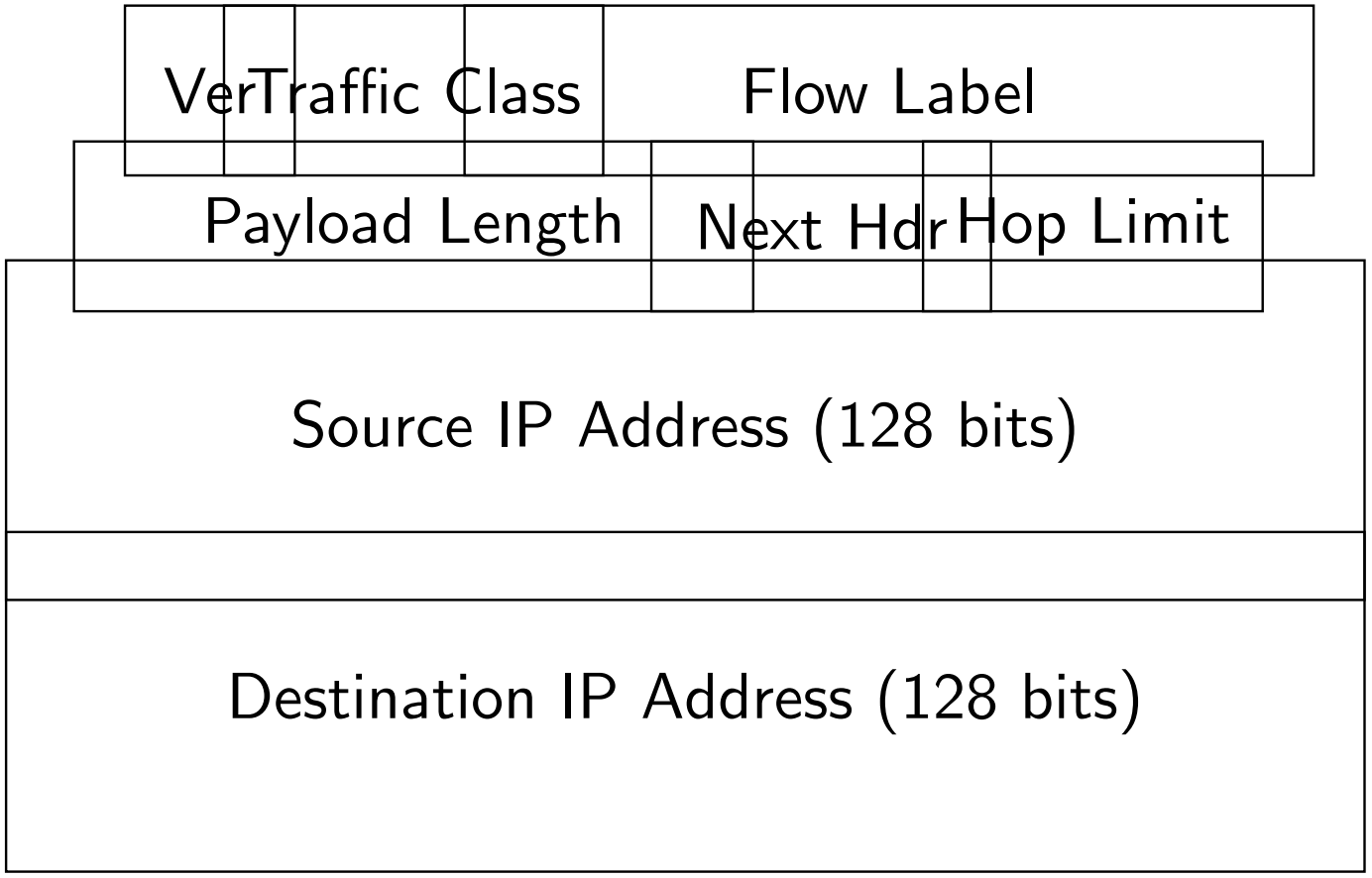
Address Space and Notation

- IPv4 addresses are 32 bits long, represented in dotted-decimal format (e.g., 192.168.1.1).
- IPv6 addresses are 128 bits long, represented in hexadecimal format, separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
- IPv6 allows for zero compression (e.g., 2001:db8::8a2e:370:7334) to simplify representation.
- The massive address space of IPv6 allows every device on the planet to have multiple public IP addresses.
- Subnetting in IPv6 usually uses a /64 prefix length for LANs, allocating 64 bits for the interface identifier.

IPv4 Header Structure



IPv6 Header Structure



Fragmentation and Checksum

- In IPv4, fragmentation is handled by routers and the sending host. This adds processing overhead at each hop.
- In IPv6, fragmentation is exclusively handled by the sending host. Routers will drop oversized packets and send an ICMPv6 Packet Too Big message.
- IPv4 headers include a checksum field to detect errors in the header.
- IPv6 eliminates the header checksum entirely, relying on upper-layer protocols (like TCP or UDP) and link-layer error detection.
- This removal of checksum processing at each hop significantly speeds up routing for IPv6.

Configuration and Security

- IPv4 requires manual configuration or a DHCP server for address assignment.
- IPv6 supports Stateless Address Autoconfiguration (SLAAC), allowing hosts to configure themselves automatically without a DHCPv6 server.
- IPsec support is optional in IPv4, often requiring complex implementations and NAT traversal techniques.
- IPsec was originally mandated in IPv6 (though later made optional for implementation), integrating network-layer security (authentication and encryption) natively.
- IPv6 eliminates broadcast addressing, using anycast and multicast instead, reducing network noise.

Summary Comparison

- Address Space: IPv4 (32-bit) vs IPv6 (128-bit).
- Header Size: IPv4 (20-60 bytes, variable) vs IPv6 (40 bytes, fixed).
- Address Configuration: IPv4 (DHCP/Manual) vs IPv6 (SLAAC/DHCPv6).
- Address Resolution: IPv4 (ARP broadcast) vs IPv6 (NDP multicast).
- Fragmentation: IPv4 (Routers/Hosts) vs IPv6 (Hosts only).
- IPsec: IPv4 (Optional/Add-on) vs IPv6 (Native/Integrated).
- Migration is ongoing, utilizing techniques like Dual-Stack, Tunneling, and Translation.

Computer Networks (DI03000051)

GTU Diploma Engineering

Agenda

1. Overview of IP Versions
2. Address Space and Format
3. IPv4 Header Structure
4. IPv6 Header Structure
5. Header Simplification & Extensions
6. Address Resolution (ARP vs NDP)
7. Security & QoS Enhancements
8. Summary

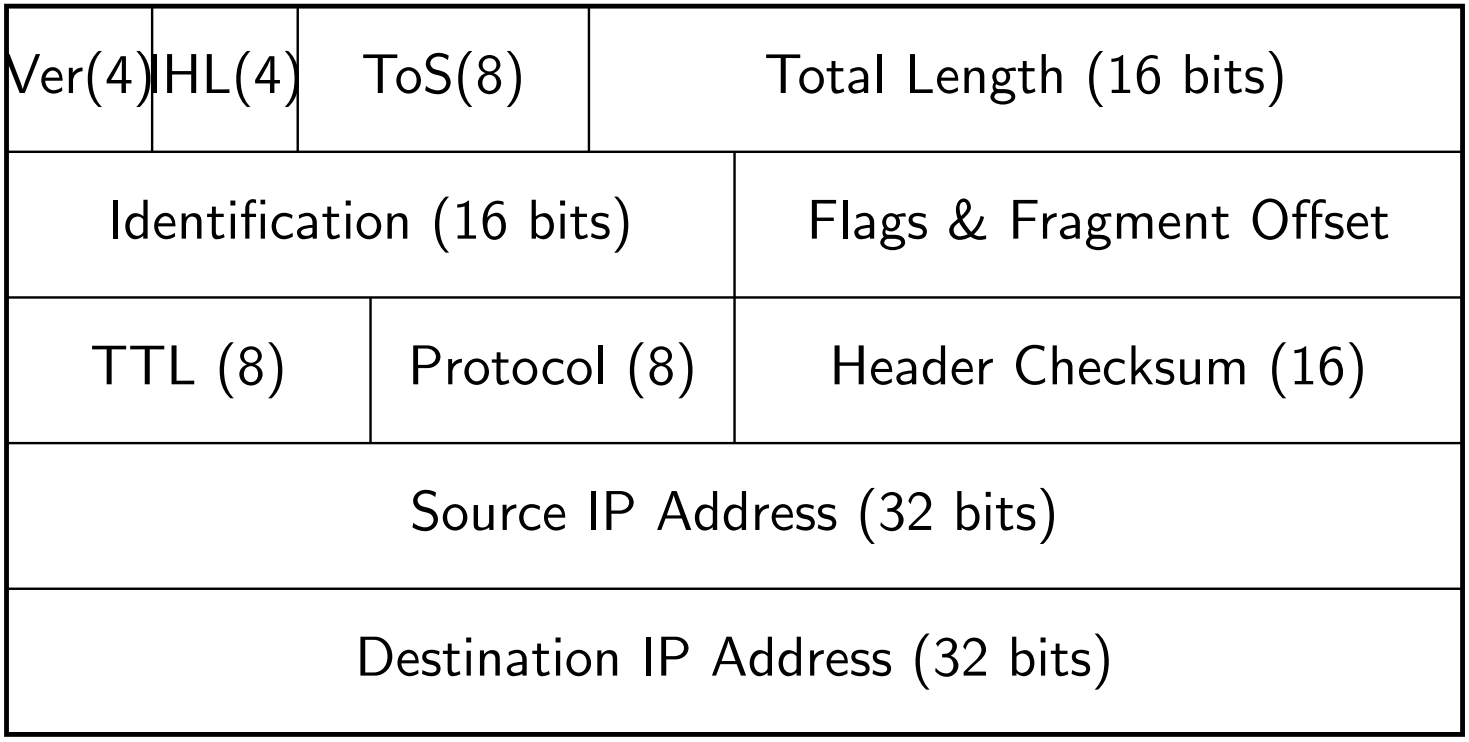
Overview of IP Versions

- Internet Protocol version 4 (IPv4) was deployed in 1983 and uses a 32-bit address space, allowing for approximately 4.3 billion unique addresses.
- Due to the rapid expansion of the Internet and IoT devices, IPv4 address exhaustion became a critical global issue.
- Internet Protocol version 6 (IPv6) was developed by the IETF (RFC 2460) to resolve this, utilizing a massive 128-bit address space.
- IPv6 provides roughly 3.4 x $10^38 addresses, ensuringvirtuallylimitlessIPavailabilityandeliminatin$

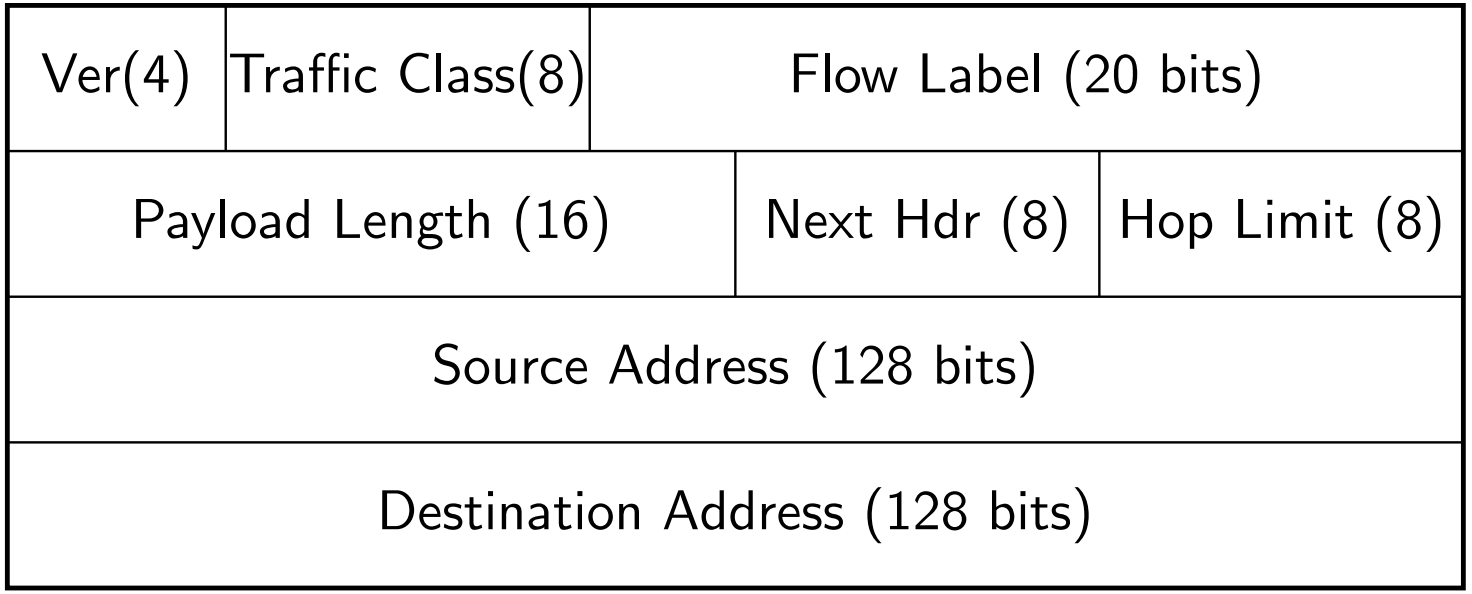
Address Space and Format

- IPv4 addresses are represented in dotted-decimal format (e.g., 192.168.1.1), divided into four 8-bit octets.
- IPv6 addresses are represented in hexadecimal format, divided into eight 16-bit blocks separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
- IPv6 allows for zero-compression, where contiguous blocks of zeros can be replaced with a double colon (::) once per address (e.g., 2001:db8::8a2e:370:7334).
- IPv4 supports Unicast, Multicast, and Broadcast addressing, whereas IPv6 completely replaces Broadcast with Anycast and enhanced Multicast groups.

IPv4 Header Structure



IPv6 Header Structure



Header Simplification & Extensions

- The IPv4 header has a variable length (20-60 bytes) due to optional fields, requiring the Internet Header Length (IHL) field to determine where the payload begins.
- The IPv6 header is fixed at exactly 40 bytes, streamlining router processing by keeping fields in predictable, fixed locations.
- IPv6 eliminates the header checksum entirely, reducing processing overhead since checksums are reliably handled by Layer 2 and Layer 4 protocols.
- Instead of embedding options directly, IPv6 introduces Extension Headers (e.g., Routing, Fragmentation, ESP) which are chained sequentially only when needed.

Address Resolution: ARP vs NDP

- IPv4 uses the Address Resolution Protocol (ARP) to map IP addresses to MAC addresses by broadcasting requests to all hosts on the local subnet.
- ARP relies on network-wide broadcasts, which consume processing cycles on every device and can degrade performance in large networks.
- IPv6 completely replaces ARP with the Neighbor Discovery Protocol (NDP), which utilizes ICMPv6 messaging and multicast routing.
- NDP relies on highly specific Solicited-Node Multicast Addresses, significantly reducing background noise and improving overall network efficiency.

Security and QoS Enhancements

- In IPv4, IPsec (Internet Protocol Security) is an optional add-on that often requires complex configuration and suffers from NAT traversal issues.
- In IPv6, IPsec architecture is deeply integrated and standard, providing robust end-to-end security via Authentication Header (AH) and Encapsulating Security Payload (ESP).
- IPv4 manages QoS (Quality of Service) using the 8-bit Type of Service (ToS) / Differentiated Services Code Point (DSCP) field.
- IPv6 introduces a dedicated 20-bit 'Flow Label' field, enabling routers to identify and maintain specific traffic flows (e.g., VoIP, streaming) without deep packet inspection.

Summary

- IPv6 represents a fundamental architectural redesign of the network layer, not just an increase in address bits.
- The shift from 32-bit to 128-bit addressing resolves address exhaustion and restores the end-to-end communication model by removing reliance on NAT.
- Fixed-size headers, the removal of checksums, and the transition from ARP to NDP make IPv6 routing significantly faster and more efficient.
- Transition mechanisms such as dual-stack configurations, tunneling (6to4, Teredo), and translation (NAT64) ensure seamless coexistence during migration.

Computer Networks (DI03000051)

GTU Diploma Engineering

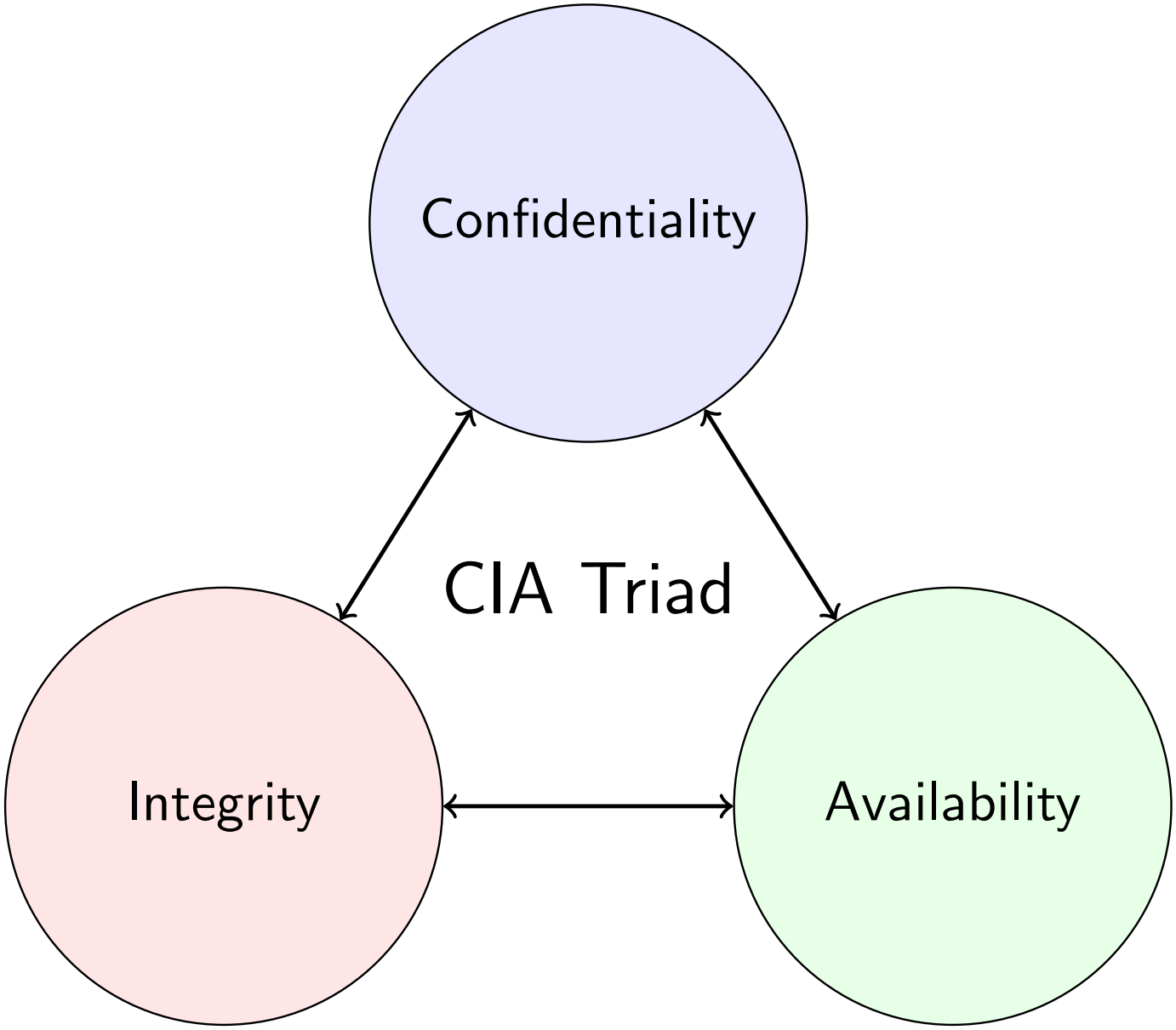
Agenda

- 1. Introduction to Network Security and The Cyber Threat Landscape
- 2. The CIA Triad: Core Principles of Information Security
- 3. Confidentiality: Encryption and Access Control
- 4. Integrity: Hashing and Digital Signatures
- 5. Availability: Redundancy and DDoS Mitigation
- 6. Threat Modeling and Vulnerability Assessment

Introduction to Network Security

- Network Security encompasses the policies, processes, and practices adopted to prevent, detect, and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.
- In modern TCP/IP networks, data traverses through multiple untrusted intermediate nodes (routers, switches), making it susceptible to various attacks at different layers of the OSI model.
- The fundamental goal of network security is to mitigate risk by establishing secure communication channels, authenticating entities, and enforcing access control policies.
- To systematically address security requirements, the industry relies on a foundational model known as the CIA Triad, which defines three core security objectives.

The CIA Triad Conceptual Model



Confidentiality: Protecting Data Privacy

- Confidentiality ensures that information is not disclosed or made available to unauthorized individuals, entities, or processes.
- In transit, confidentiality is typically achieved using cryptographic protocols such as TLS (Transport Layer Security) or IPsec (Internet Protocol Security), which employ symmetric encryption algorithms (e.g., AES-256) for bulk data encryption.
- At rest, confidentiality relies on full-disk encryption, file-level encryption, and strict Access Control Lists (ACLs) using models like RBAC (Role-Based Access Control) or MAC (Mandatory Access Control).
- Threats to confidentiality include packet sniffing (e.g., via Wireshark on a mirrored switch port), eavesdropping, man-in-the-middle attacks, and unauthorized data exfiltration.

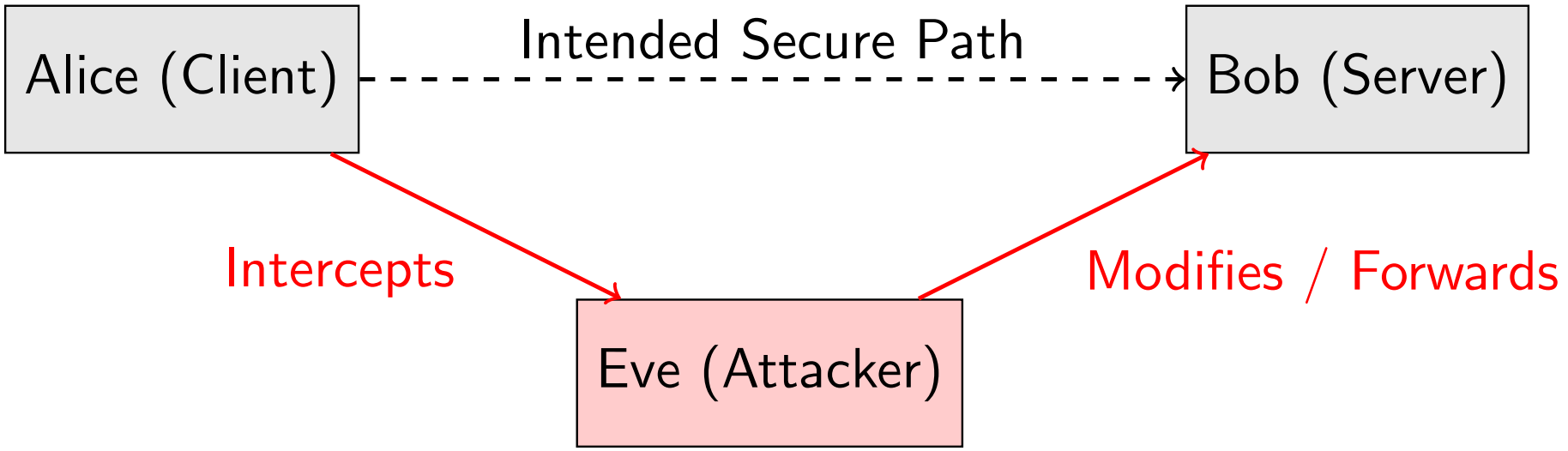
Integrity: Ensuring Data Accuracy and Trust

- Integrity guarantees that data has not been altered, deleted, or otherwise modified in an unauthorized or undetected manner during transit or storage.
- To verify integrity, systems utilize cryptographic hash functions (e.g., SHA-256, SHA-3). A hash function takes an input message and produces a fixed-size string of bytes. Any change in the input drastically changes the output (avalanche effect).
- Message Authentication Codes (MACs) and Digital Signatures (using asymmetric cryptography like RSA or ECDSA) combine hashing with authentication to prove both data integrity and the sender's identity (non-repudiation).
- Threats to integrity include unauthorized database modifications, malware infections, bit-flipping attacks, and protocol manipulation (e.g., ARP spoofing or DNS cache poisoning).

Availability: Maintaining Operational Readiness

- Availability ensures that systems, applications, and data are accessible and usable by authorized users when required, without unacceptable delays.
- High Availability (HA) architectures rely on hardware redundancy (e.g., RAID, multiple power supplies), network redundancy (e.g., BGP multi-homing, spanning tree protocol, load balancers), and geographic clustering.
- Threats to availability primarily take the form of Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks, such as SYN floods, UDP amplification attacks, and application-layer (HTTP POST) attacks.
- Mitigation strategies include implementing rate limiting, anycast routing, traffic scrubbing centers, robust disaster recovery plans, and continuous system monitoring.

Threat Vector: Man-in-the-Middle (MitM)



Balancing the CIA Triad

- Achieving perfect security is practically impossible; the CIA triad involves inherent trade-offs between Confidentiality, Integrity, and Availability.
- For example, enforcing highly stringent access controls and complex multi-factor authentication (MFA) to maximize Confidentiality can negatively impact Availability by slowing down authorized users or locking them out during system failures.
- Similarly, implementing pervasive data encryption and continuous integrity hashing consumes significant computational overhead (CPU/RAM), which can increase latency and degrade the Availability of high-throughput network services.
- Security architecture involves risk management: identifying the specific threat profile of a system and finding the optimal balance of CIA controls to meet business requirements without degrading operational efficiency.

Summary and Next Steps

- The CIA Triad (Confidentiality, Integrity, Availability) forms the cornerstone of all network security policies and architectural decisions.
- Confidentiality is maintained through encryption and strict access controls; Integrity is ensured via hashing and digital signatures; Availability is achieved through redundancy and DDoS mitigation.
- Security is not a singular product, but a continuous process of risk assessment, implementation, monitoring, and incident response.
- In the next lecture, we will dive deeper into Applied Cryptography, exploring the mathematical foundations of Symmetric (AES) and Asymmetric (RSA/ECC) encryption algorithms.

Computer Networks (DI03000051)

GTU Diploma Engineering

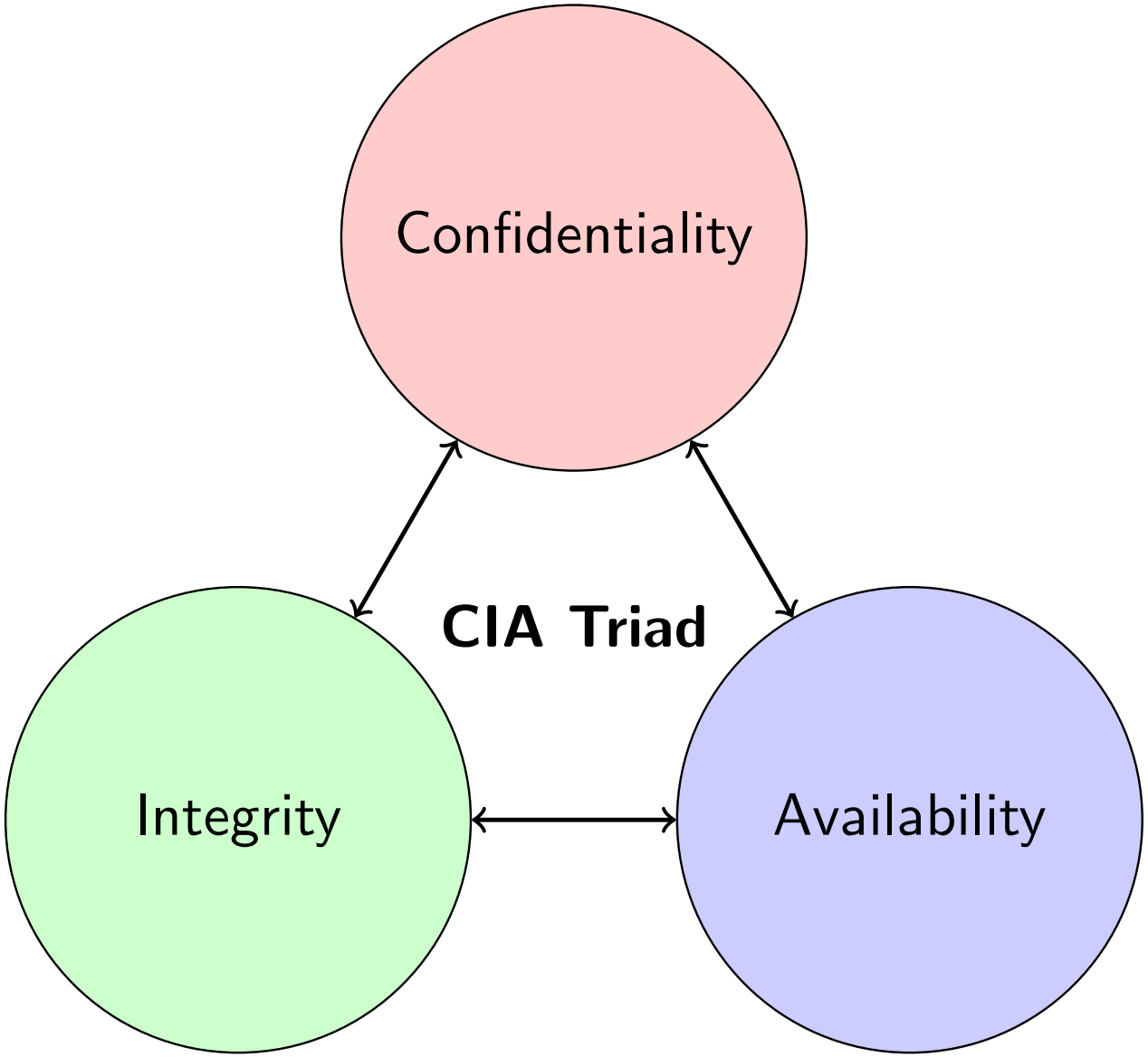
Agenda

- Introduction to Network Security
- The CIA Triad
- Confidentiality Deep Dive
- Integrity Mechanisms
- Availability Concepts
- Threats and Controls Overview

Introduction to Network Security

- Network security involves protecting the underlying networking infrastructure from unauthorized access, misuse, or theft.
- It requires creating a secure infrastructure for devices, applications, users, and applications to work in a secure manner.
- Fundamental goals are often summarized by foundational principles, the most prominent being the CIA triad.
- In the context of the OSI model, security mechanisms can be applied at various layers (e.g., IPsec at Network layer, TLS at Transport layer).

The CIA Triad Diagram



Confidentiality

- Confidentiality ensures that data is only accessible to authorized individuals or systems.
- It is the equivalent of privacy in a network context.
- Primary mechanism for ensuring confidentiality is encryption (symmetric like AES, and asymmetric like RSA).
- Access control lists (ACLs) and strict authentication protocols (like Kerberos or OAuth) also enforce confidentiality by restricting access.
- Threats to confidentiality include packet sniffing, wiretapping, and keylogging.

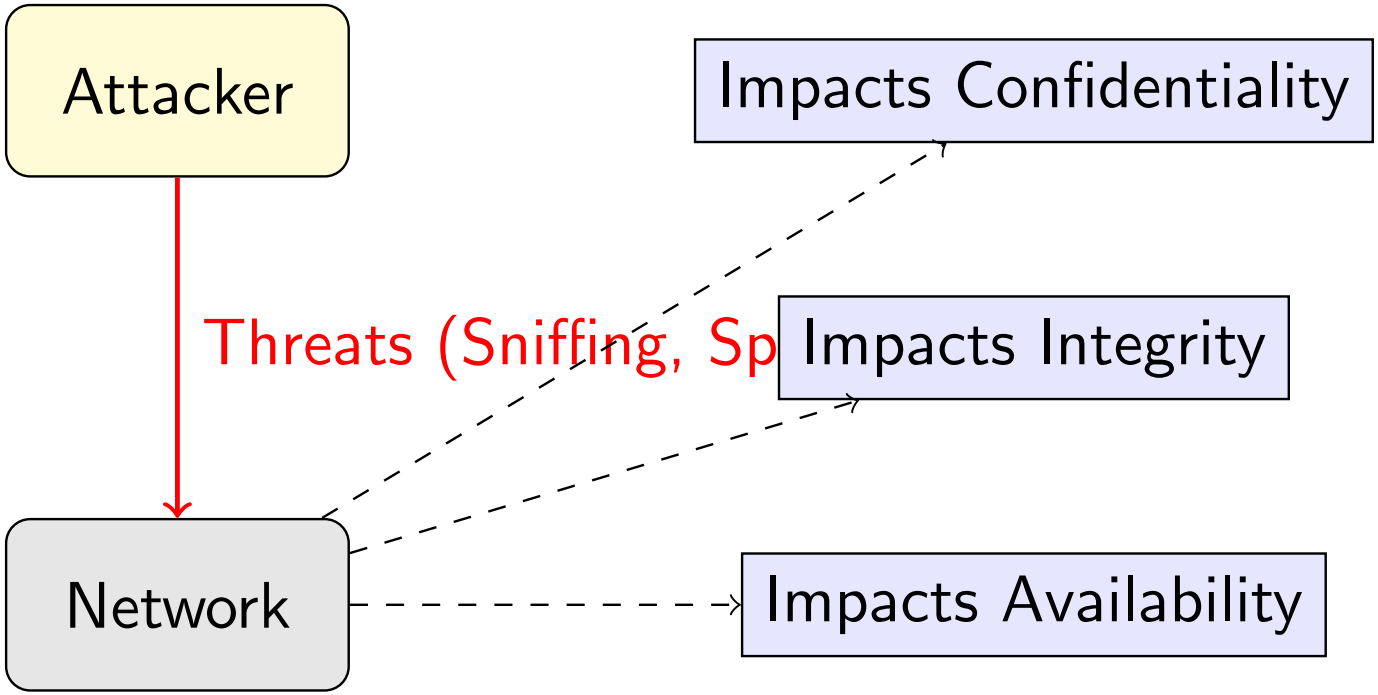
Integrity

- Integrity guarantees that data has not been altered, destroyed, or tampered with in an unauthorized manner during transmission or storage.
- Crucial for financial transactions, medical records, and system configurations.
- Mechanisms include cryptographic hash functions (e.g., SHA-256), Message Authentication Codes (MACs), and digital signatures.
- Digital signatures provide non-repudiation in addition to integrity, proving the origin of the message.
- Threats to integrity include Man-in-the-Middle (MitM) attacks and malicious code injection.

Availability

- Availability ensures that systems, networks, and data are accessible and functional when needed by authorized users.
- It requires maintaining hardware, performing software patching, and ensuring adequate bandwidth and network capacity.
- Mechanisms include redundancy (failover clusters, RAID), load balancing, and comprehensive disaster recovery plans.
- The primary threat to availability is the Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS) attack, which overwhelms resources.
- Other threats include hardware failures, natural disasters, and power outages.

Threats Mapping Diagram



Applying Security Controls

- Defense in Depth: Applying multiple layers of security controls throughout an IT system.
- Administrative Controls: Policies, procedures, and training (e.g., password policies, security awareness training).
- Logical/Technical Controls: Software and hardware mechanisms (e.g., Firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), Encryption).
- Physical Controls: Securing physical access to the network infrastructure (e.g., biometric locks on server room doors, security cameras).
- Balancing security with usability and cost is a continuous challenge in network engineering.

Summary

- The CIA Triad (Confidentiality, Integrity, Availability) forms the cornerstone of network security.
- Confidentiality is protected primarily through encryption and access controls.
- Integrity relies on hashing and digital signatures to detect tampering.
- Availability requires redundancy, load balancing, and DDoS mitigation strategies.
- A holistic approach using Defense in Depth is necessary to address the evolving threat landscape.

Computer Networks (DI03000051)

GTU Diploma Engineering

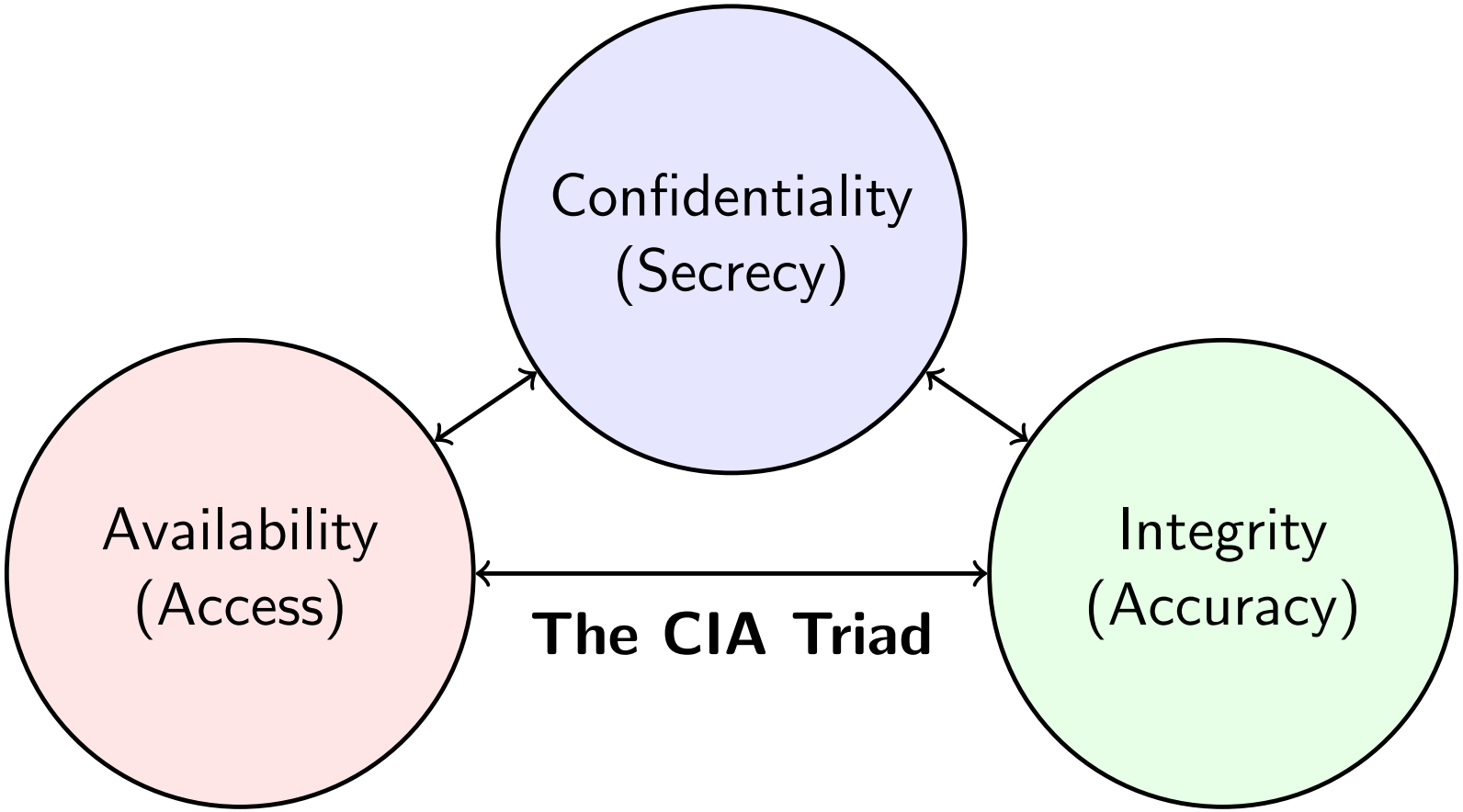
Agenda

- 1. Introduction to Network Security
- 2. The CIA Triad: Core Principles
- 3. Deep Dive: Confidentiality and Encryption
- 4. Deep Dive: Integrity and Hashing
- 5. Deep Dive: Availability and Redundancy
- 6. Common Threats to the CIA Triad

Introduction to Network Security

- Network security consists of the policies, processes, and practices adopted to prevent, detect, and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.
- The primary goal is to protect the underlying networking infrastructure from unauthorized access, malfunction, destruction, or improper disclosure.
- Security must be integrated at multiple layers of the OSI model (e.g., Physical security, IPSec at Network layer, TLS at Transport layer, Application layer firewalls).
- Fundamentally, information security is built upon three foundational principles known as the CIA Triad.

The CIA Triad Overview



Confidentiality

- Confidentiality ensures that sensitive information is accessed only by an authorized person and kept away from those not authorized to possess it.
- Also known as secrecy or privacy, it prevents passive attacks like eavesdropping or packet sniffing (e.g., using Wireshark on an open Wi-Fi network).
- Common mechanisms to ensure confidentiality include access control lists (ACLs), authentication protocols (like Kerberos or OAuth), and data encryption.
- Example: In networking, TLS (Transport Layer Security) encrypts HTTP traffic to form HTTPS, ensuring that intermediate routers cannot read the payload of the web traffic.

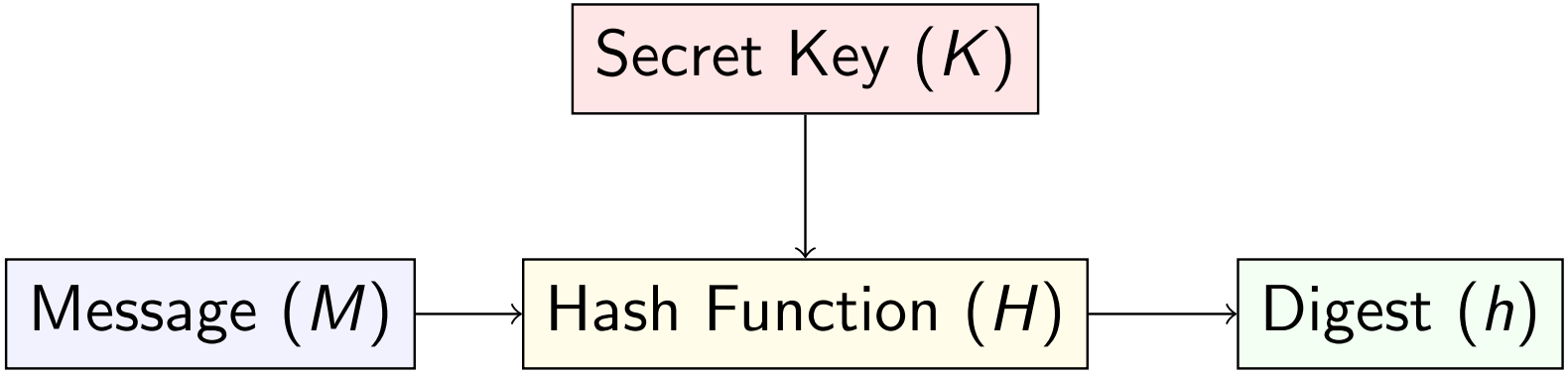
Ensuring Confidentiality: Encryption

- Encryption transforms plaintext into ciphertext using a cryptographic algorithm and a key.
- Symmetric Encryption: Uses the same key for encryption and decryption (e.g., AES - Advanced Encryption Standard, DES, ChaCha20). It is fast and suitable for bulk data transfer.
- Asymmetric Encryption: Uses a public key for encryption and a private key for decryption (e.g., RSA, Elliptic Curve Cryptography). Often used for secure key exchange and digital signatures.
- Modern protocols like TLS use asymmetric encryption for the initial handshake to securely exchange a session key, which is then used for symmetric encryption of the data stream.

Integrity

- Integrity guarantees that information is trustworthy and accurate. It ensures that data has not been altered in an unauthorized manner during storage or transit.
- It protects against active attacks where an adversary intercepts a message and modifies its contents before forwarding it to the destination (Man-in-the-Middle attack).
- Integrity mechanisms must detect any accidental corruption (like bit errors during transmission, handled by CRCs) or malicious tampering.
- Key mechanisms include Cryptographic Hash Functions, Message Authentication Codes (MACs), and Digital Signatures.

Ensuring Integrity: Hashing and MACs



HMAC Generation
(Hash-based Message Authentication Code)

Availability

- Availability ensures that systems, applications, and data are available and accessible to authorized users when they need them.
- A network must have the necessary capacity, reliability, and resilience to handle both normal traffic loads and unexpected surges or failures.
- Threats to availability include Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, hardware failures, software bugs, and environmental disasters.
- Mitigation strategies include hardware redundancy (e.g., RAID, clustered servers), network redundancy (multiple ISPs, BGP routing), load balancing, and using Content Delivery Networks (CDNs).

Threats to the CIA Triad

- Threats to Confidentiality: Packet sniffing, password cracking, phishing, malware (spyware), unencrypted data transmission.
- Threats to Integrity: Session hijacking, Man-in-the-Middle (MitM) attacks, malicious code injection (SQL injection, XSS), unauthorized database modifications.
- Threats to Availability: SYN Floods, UDP Floods, DNS Amplification attacks, ransomware, physical destruction of networking equipment.
- Effective security requires a defense-in-depth approach, implementing overlapping controls (firewalls, IDS/IPS, strong cryptography, access controls) to protect all three pillars simultaneously.

Computer Networks (DI03000051)

GTU Diploma Engineering

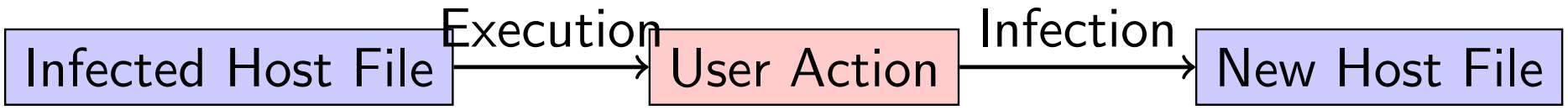
Agenda

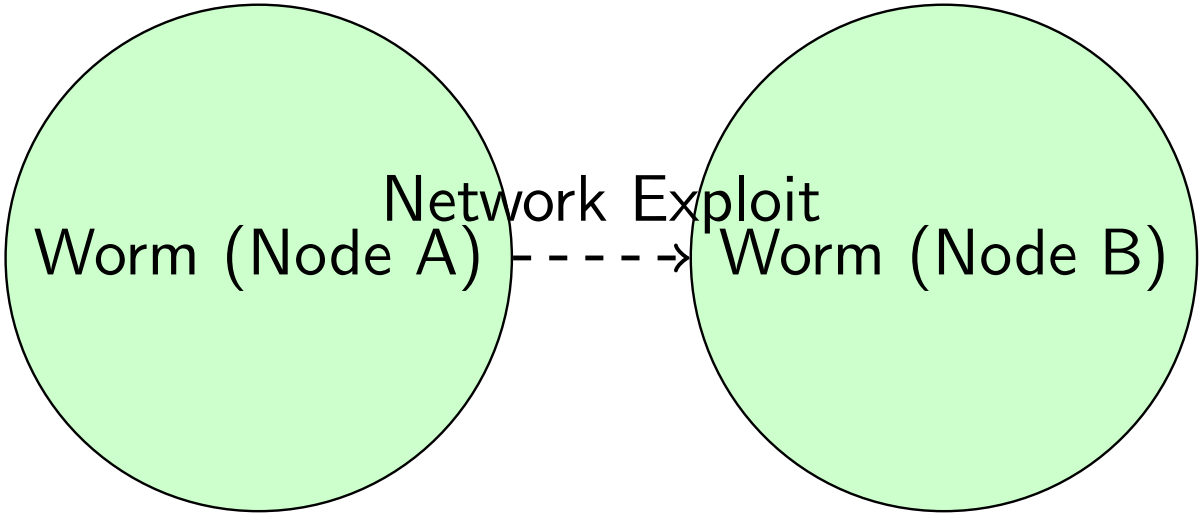
- Viruses and Worms
- Intruders (Hackers/Crackers)
- Insiders
- Criminal Organizations
- Terrorists
- Information Warfare

Malware: Viruses and Worms

- Malware (Malicious Software) is designed to cause damage to a computer, server, client, or computer network.
- Viruses: A computer program that replicates itself by modifying other computer programs and inserting its own code. Requires a host program and user interaction to spread.
- Worms: Standalone malware computer programs that replicate themselves in order to spread to other computers. They use a computer network to spread, relying on security failures on the target computer to access it.
- Key Difference: Worms do not need a host program or human help to propagate; they are self-replicating and self-contained.
- Impact: Can consume bandwidth, delete files, steal data, or create botnets.

Virus vs Worm Propagation Diagram





Intruders (Hackers and Crackers)

- Intruders attempt to breach security perimeters to gain unauthorized access to system resources.
- Classes of Intruders (RFC 4949):
- 1. Masquerader: An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account.
- 2. Misfeasor: A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses their privileges.
- 3. Clandestine user: An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection.
- Motivations range from curiosity and bragging rights (traditional 'hackers') to malicious intent and financial gain ('crackers').

The Insider Threat

- Insiders possess authorized access to the network, systems, and data, making them one of the most dangerous threat vectors.
- Types of Insiders:
- 1. Malicious Insiders: Employees or contractors who intentionally steal data, sabotage systems, or commit fraud. Motivated by financial gain, revenge, or ideology.
- 2. Negligent Insiders: Employees who inadvertently cause security breaches through carelessness, such as falling for phishing scams, misconfiguring servers, or mishandling sensitive data.
- 3. Compromised Insiders: Legitimate credentials stolen by external attackers.
- Mitigation: Principle of Least Privilege, Separation of Duties, User and Entity Behavior Analytics (UEBA).

Criminal Organizations

- Organized crime has heavily infiltrated cyberspace, moving from isolated hackers to highly structured cybercriminal syndicates.
- Characteristics:
- 1. Highly resourced and technically sophisticated.
- 2. Profit-driven: Primary goals are financial theft, extortion, and corporate espionage.
- Tactics used:
- 1. Ransomware-as-a-Service (RaaS): Developing ransomware and leasing it to affiliates.
- 2. Large-scale phishing and spear-phishing campaigns.
- 3. Carding forums and dark web marketplaces for selling stolen PII and financial data.
- 4. Botnet herding for DDoS extortion.

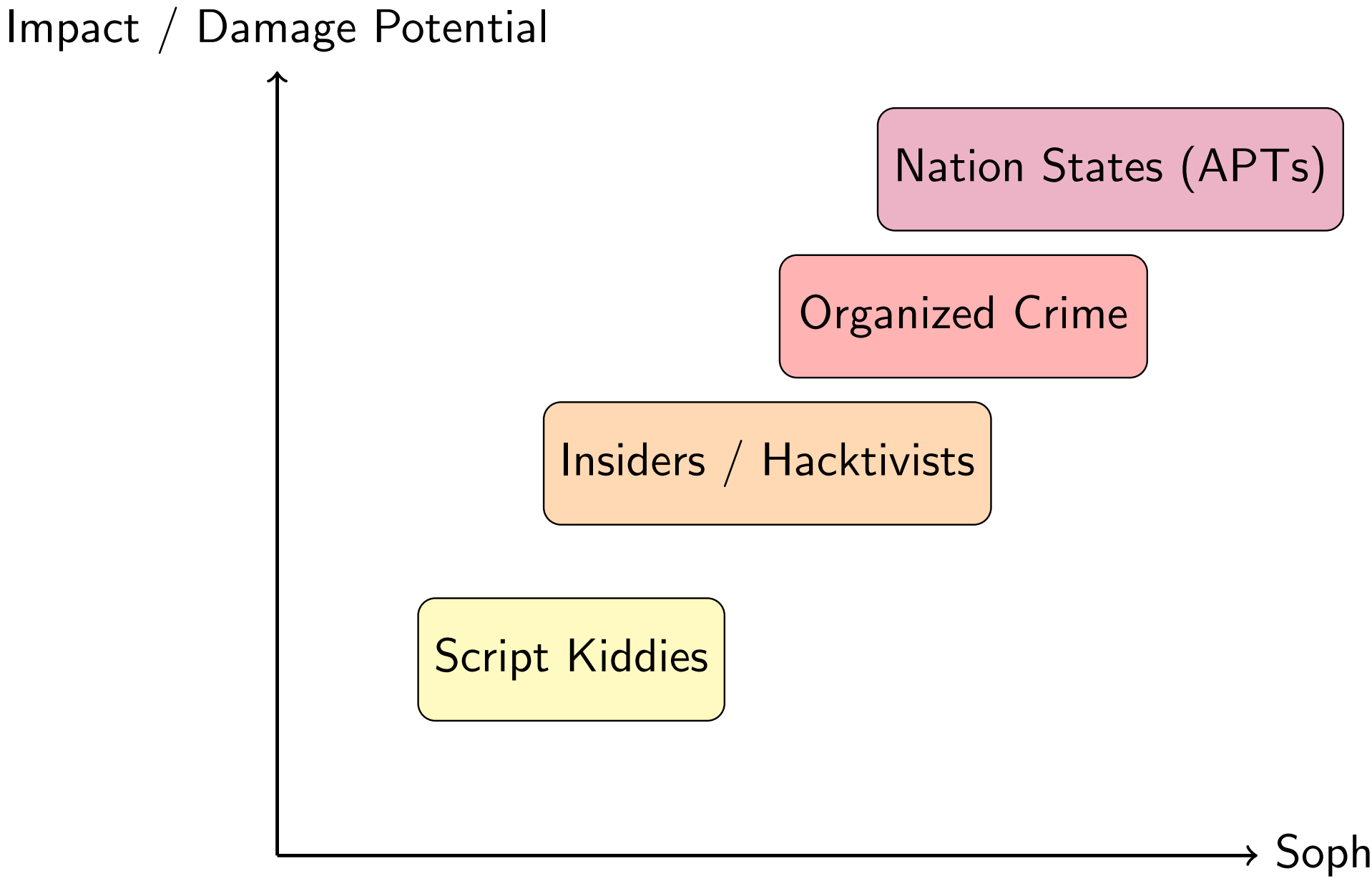
Terrorists and Cyberterrorism

- Cyberterrorism: The convergence of terrorism and cyberspace. It involves unlawful attacks and threats of attack against computers, networks, and the information stored therein.
- Objectives:
- 1. Intimidation or coercion of a government or its people in furtherance of political or social objectives.
- 2. Causing physical violence, severe economic disruption, or widespread panic.
- Targets: Critical Infrastructure (power grids, water treatment plants, transportation systems, financial networks).
- Methods: SCADA (Supervisory Control and Data Acquisition) system exploits, large-scale DDoS attacks on essential services, wiping critical databases.

Information Warfare

- Information Warfare (IW): The use of information and communication technology to gain a competitive advantage over an opponent.
- Often conducted by Nation-State actors (Advanced Persistent Threats - APTs).
- Key Components:
- 1. Cyber Espionage: Stealing state secrets, intellectual property, and military intelligence without detection.
- 2. Cyber Sabotage: Disrupting or destroying enemy critical infrastructure (e.g., Stuxnet attacking Iranian nuclear centrifuges).
- 3. Psychological Operations (PsyOps) / Disinformation: Manipulating public opinion, spreading propaganda, and interfering in democratic processes via social media.
- 4. Electronic Warfare: Jamming or spoofing enemy communications and radar.

Threat Actor Capabilities Diagram



Computer Networks (DI03000051)

GTU Diploma Engineering

Agenda

- Overview of Network Security Threats
- Viruses and Worms
- Intruders (External Threats)
- Insider Threats
- Criminal Organizations
- Terrorists and Information Warfare

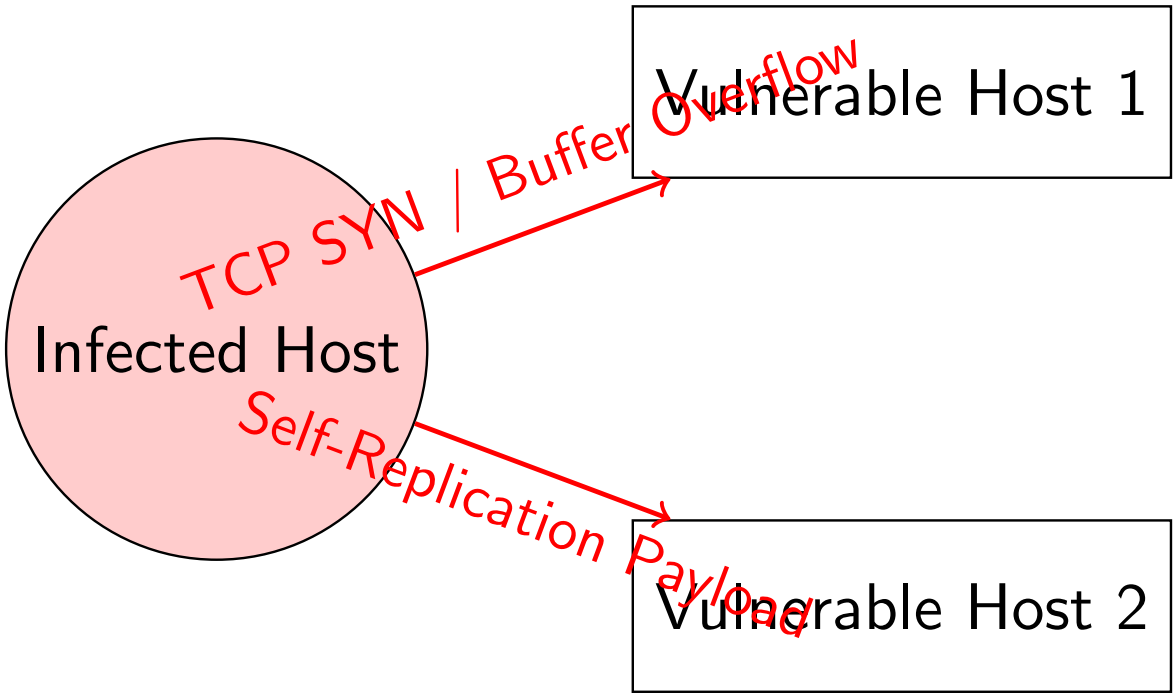
Overview of Network Security Threats

- Security threats exploit vulnerabilities in network protocols (e.g., TCP/IP routing, DNS spoofing) or operating system flaws.
- Threat actors range from script kiddies using pre-packaged exploits to state-sponsored Advanced Persistent Threats (APTs).
- Primary motivations include financial gain, corporate espionage, ideological goals, and service disruption.
- A robust defense strategy must protect the CIA triad: Confidentiality (encryption), Integrity (hashing, digital signatures), and Availability (redundancy, anti-DDoS).

Viruses and Worms

- Viruses: Malicious executable code that requires a host program and human interaction to spread, often infecting boot sectors or utilizing macro languages in documents.
- Worms: Self-replicating network malware that propagates autonomously without human intervention by exploiting software vulnerabilities (e.g., the Morris Worm exploiting fingerd, SQL Slammer exploiting MS SQL UDP port 1434).
- Propagation Methodology: Worms often utilize pseudo-random IP scanning algorithms to discover and compromise vulnerable hosts rapidly.
- Impact: Significant network congestion due to scanning traffic, execution of malicious payloads, and recruitment of hosts into botnets.

Worm Propagation Mechanism



Intruders

- Intruders, commonly referred to as hackers or crackers, typically fall into three categories: Masqueraders (unauthorized users), Misfeasors (authorized users abusing privileges), and Clandestine users (bypassing auditing).
- Attack Lifecycle: Reconnaissance (Nmap port scanning), Exploitation (Metasploit payloads), Privilege Escalation, and Maintaining Access (deploying rootkits).
- Common Techniques: Dictionary/Brute-force password cracking, Man-in-the-Middle (MitM) via ARP spoofing or DNS cache poisoning, and Social Engineering.
- Countermeasures: Deployment of Network Intrusion Detection/Prevention Systems (NIDS/NIPS), strict Access Control Lists (ACLs), and multi-factor authentication (MFA).

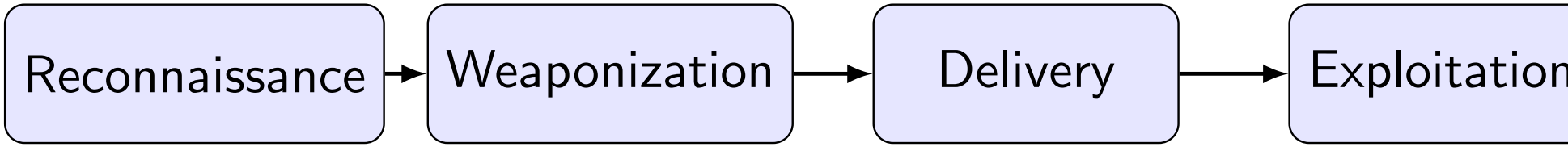
Insider Threats

- Definition: Current or former employees, contractors, or partners who possess legitimate access credentials to network systems and sensitive data.
- Risk Factor: Insiders bypass traditional perimeter defenses (firewalls, edge routers) because their access is already authorized.
- Types: Malicious insiders intentionally steal intellectual property, sabotage systems, or deploy logic bombs. Accidental insiders unintentionally compromise security via phishing or misconfiguration.
- Mitigation Strategies: Enforcing the Principle of Least Privilege (PoLP), Separation of Duties (SoD), deploying User and Entity Behavior Analytics (UEBA), and rigorous audit logging.

Criminal Organizations & Terrorists

- Criminal Organizations: Highly structured syndicates operating in the digital underground. They monetize exploits via Ransomware-as-a-Service (RaaS), coordinate vast IoT botnets for massive volumetric DDoS attacks, and trade stolen credentials.
- Cyber Terrorism: Groups aiming to cause widespread panic, fear, or physical disruption by targeting Critical Infrastructure (e.g., SCADA systems in power grids, financial networks).
- Tactics: Utilization of zero-day exploits, advanced encryption algorithms to hide C2 (Command and Control) traffic, and deployment of destructive malware rather than merely extractive tools.
- Impact: Blurs the line between logical attacks and kinetic damage, potentially causing physical equipment failure.

Targeted Attack Framework



Information Warfare

- Definition: The strategic use of information and communication technologies (ICT) to gain a competitive advantage over a geopolitical adversary.
- Scope: Encompasses state-sponsored cyber espionage, sabotage of critical national infrastructure, and psychological operations (e.g., coordinated disinformation campaigns).
- Techniques: Advanced Persistent Threats (APTs) maintaining long-term, stealthy network presence; supply chain compromises (e.g., SolarWinds attack).
- Defensive Posture: Implementing Zero Trust Architecture, enhancing cyber deterrence policies, fostering international intelligence sharing, and rigorous incident response planning.

Computer Networks (DI03000051)

GTU Diploma Engineering

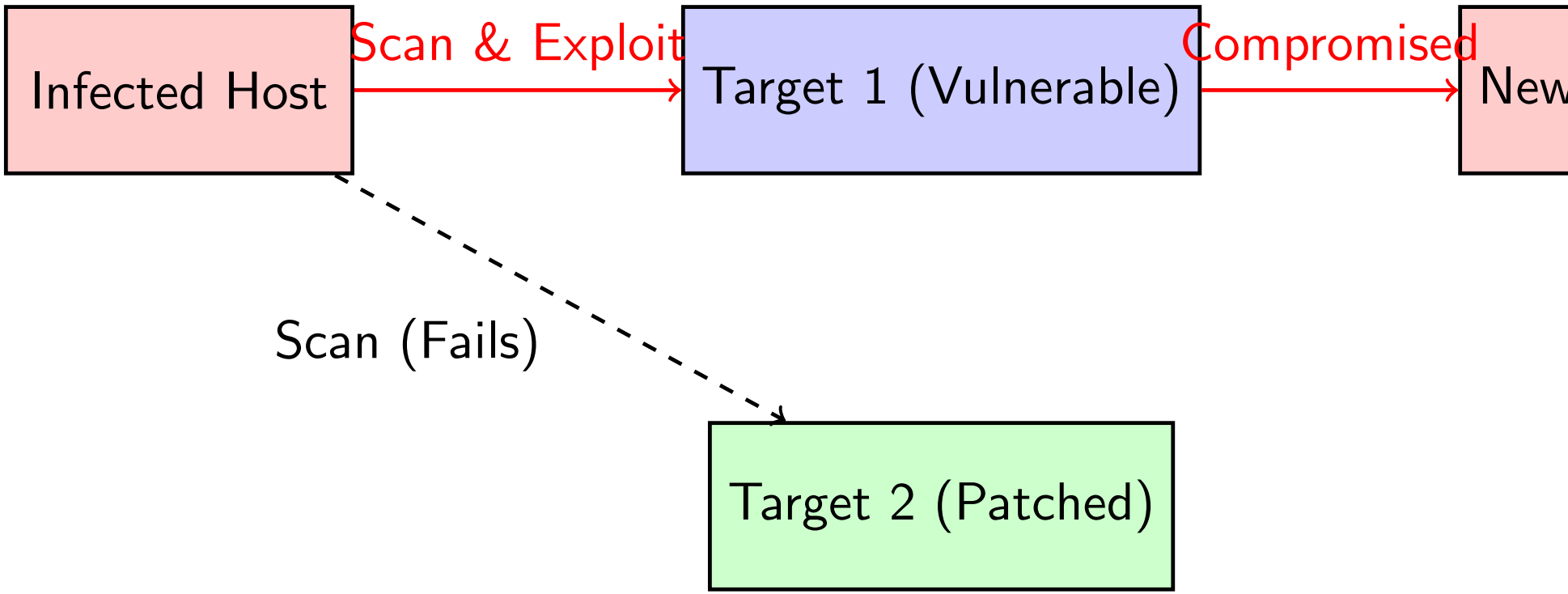
Agenda

- Viruses and Worms
- Intruders (Hackers and Crackers)
- Insiders
- Criminal organizations
- Terrorists
- Information warfare

Viruses and Worms

- A virus is a piece of code that inserts itself into a host program and propagates when the host is executed. It often requires user interaction, such as opening an infected email attachment.
- A worm is a standalone malicious program that actively transmits itself over a network to infect other computers. Worms exploit vulnerabilities in network protocols or operating systems.
- Worms like the Morris Worm or SQL Slammer caused massive denial of service by consuming network bandwidth through rapid self-propagation via UDP/TCP scanning.
- Defense mechanisms include Antivirus software (signature-based and heuristic detection), Intrusion Detection Systems (IDS), and timely patching of software vulnerabilities.

Worm Propagation Mechanism



Intruders

- Intruders, often categorized as hackers (explorers) or crackers (malicious intent), aim to gain unauthorized access to computer systems and networks.
- Classes of intruders include Masqueraders (outsiders assuming an authorized identity), Misfeasors (insiders misusing privileges), and Clandestine users (individuals bypassing supervisory controls).
- Intrusion techniques include password cracking (dictionary attacks, brute-force), exploiting buffer overflows in network daemons, and social engineering.
- Countermeasures involve robust authentication (Multi-Factor Authentication), Intrusion Prevention Systems (IPS), and implementing the principle of least privilege.

Insiders

- Insider threats originate from employees, contractors, or business partners who have legitimate access to the network and systems.
- They are often considered the most dangerous threat because they bypass perimeter defenses (like firewalls) and possess knowledge of internal security protocols.
- Motivations range from financial gain (selling corporate secrets) and revenge (disgruntled employees) to unintentional errors (falling for phishing attacks).
- Mitigation strategies include strict Access Control Lists (ACLs), comprehensive network auditing/logging (e.g., using Syslog/SIEM), and Data Loss Prevention (DLP) systems.

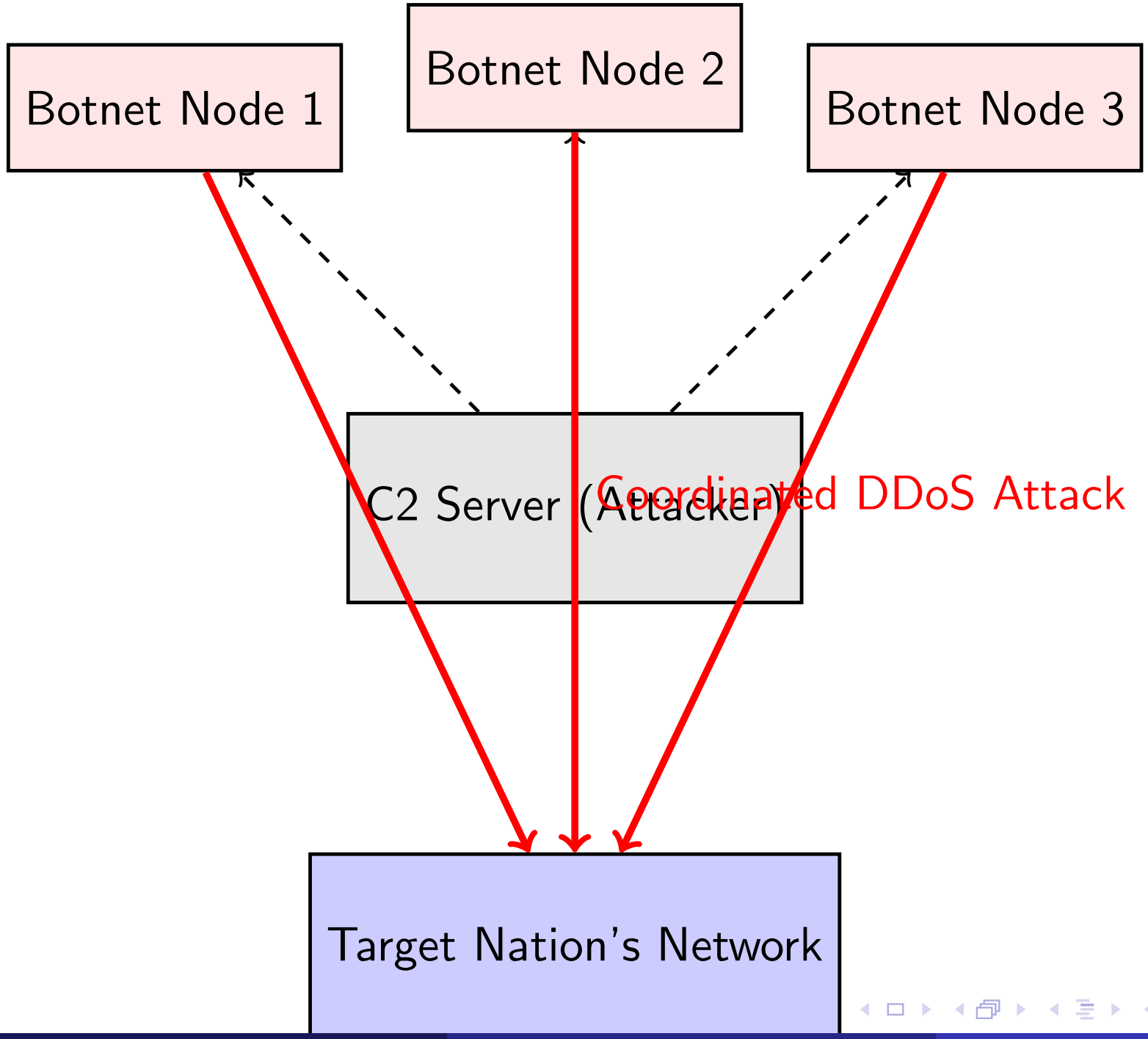
Criminal Organizations

- Organized crime syndicates utilize advanced networking attacks for financial gain, engaging in activities like ransomware, identity theft, and large-scale fraud.
- They often employ 'Crime-as-a-Service' models, renting out botnets for Distributed Denial of Service (DDoS) attacks or selling custom malware on the dark web.
- Advanced Persistent Threats (APTs) are frequently used, where attackers maintain long-term, stealthy access to a network to exfiltrate sensitive data over time without triggering alarms.
- Defenses require global threat intelligence sharing, advanced endpoint detection and response (EDR), and robust incident response plans.

Terrorists

- Cyberterrorism involves politically or ideologically motivated attacks against critical infrastructure networks (e.g., power grids, financial networks, transportation systems).
- The goal is to cause physical disruption, panic, or economic damage by compromising Supervisory Control and Data Acquisition (SCADA) systems and Industrial Control Systems (ICS).
- Attacks may utilize zero-day exploits and highly targeted malware, similar to the Stuxnet worm which targeted nuclear enrichment facilities.
- Protecting against cyberterrorism necessitates isolating critical networks (air-gapping), stringent physical security, and international cooperation in cyberspace.

Information Warfare Architecture



Information Warfare & Summary

- Information warfare involves nation-states conducting cyber espionage, sabotage, and propaganda campaigns against adversaries' digital infrastructure.
- It includes attacking command and control systems, disrupting enemy communications (e.g., BGP hijacking), and orchestrating psychological operations.
- Summary: Network security must address a wide spectrum of threats, from automated malware to sophisticated, state-sponsored attackers targeting core routing infrastructure.
- Effective defense requires a defense-in-depth strategy, combining technological solutions with rigorous policies, encryption protocols (IPsec/TLS), and human awareness.

Computer Networks (DI03000051)

GTU Diploma Engineering

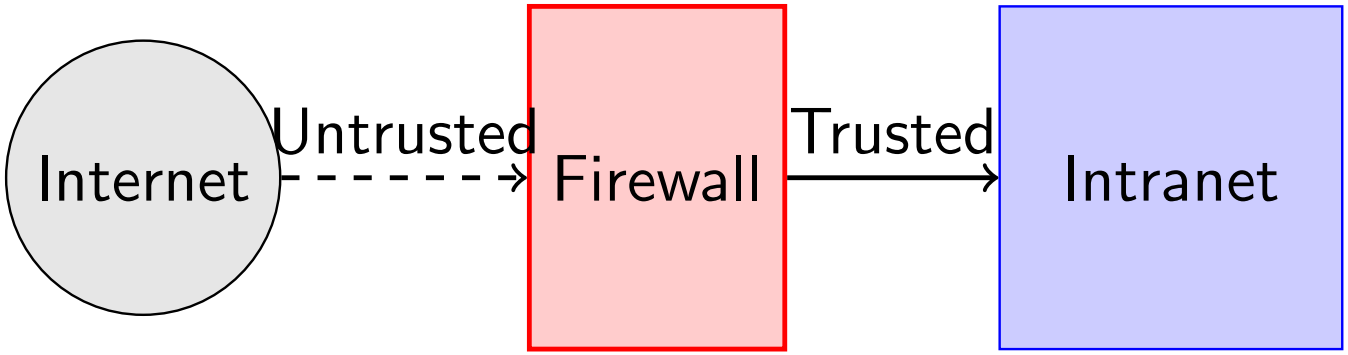
Agenda

- Firewalls: Working and Design Principle
- Packet Filter Firewall
- Proxy Firewall

Firewall Design Principles

- A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predefined security rules.
- Design Principle 1: All traffic from inside to outside, and vice versa, must pass through the firewall.
- Design Principle 2: Only authorized traffic, as defined by the local security policy, will be allowed to pass.
- Design Principle 3: The firewall itself is immune to penetration (implemented on a hardened system with a secured operating system).
- Firewalls establish a controlled link and act as a choke point for security auditing and access control.

Network Perimeter and Firewall Topology



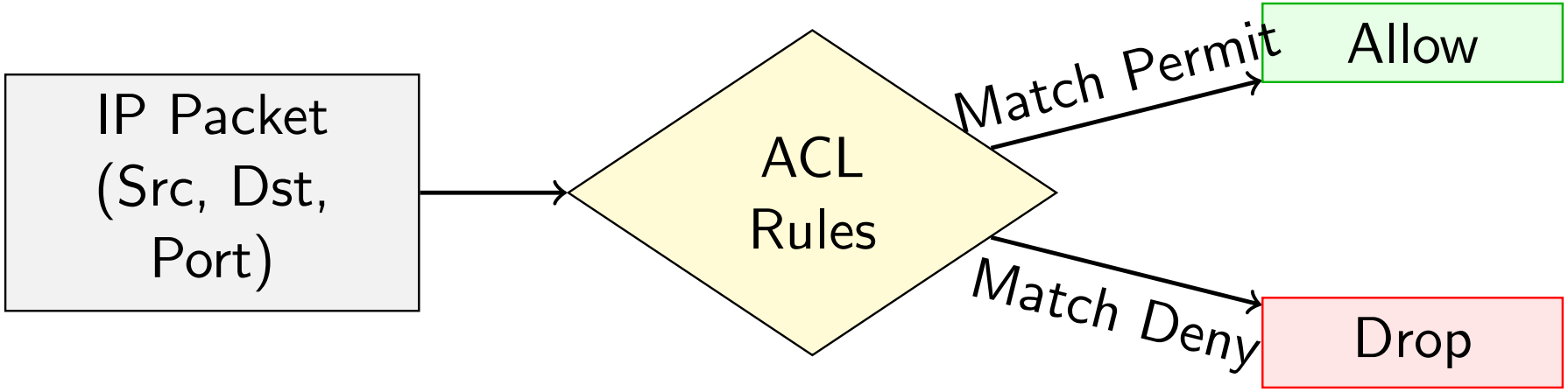
Firewall Working Mechanisms

- Firewalls use various techniques to filter traffic, primarily categorized into packet filtering, stateful inspection, and application-level proxying.
- Security policies are implemented using Access Control Lists (ACLs) that evaluate packet headers or application payloads.
- Default Policies define the baseline security posture:
- Default Discard: Prohibits everything that is not expressly permitted. This is highly secure but requires explicit rules for all legitimate traffic.
- Default Forward: Permits everything that is not expressly prohibited. This is easier to configure but exposes the network to unknown threats.

Packet Filter Firewall

- Operates at the Network and Transport layers (Layers 3 and 4 of the OSI model).
- Applies a set of rules to each incoming and outgoing IP packet independently.
- Filtering decisions are based on: Source/Destination IP address, Source/Destination Transport-level port (TCP/UDP), IP protocol field, and Network Interface.
- Advantages: Simplicity, high processing speed, and complete transparency to end users.
- Disadvantages: Vulnerable to IP spoofing attacks, lacks application context, and improper configuration can inadvertently expose services.

Packet Filtering Architecture



Stateful vs. Stateless Packet Filters

- Traditional (stateless) packet filters examine each packet in complete isolation, unaware of the connection's broader context.
- Stateful inspection firewalls dynamically track the state of active connections.
- They maintain a state table (directory) of outbound TCP/UDP connections.
- Incoming traffic to high-numbered ephemeral ports is only permitted if the packet fits the profile of an established connection in the state table.
- This prevents attackers from exploiting stateless rules by sending unsolicited packets with the ACK bit set or spoofed source ports.

Proxy Firewall (Application-Level Gateway)

- Operates at the Application layer (Layer 7 of the OSI model), offering deep packet inspection.
- Acts as a specialized intermediary or proxy for specific applications (e.g., HTTP, FTP, SMTP).
- The client contacts the proxy, the proxy authenticates the request, and then the proxy establishes a secondary connection to the actual destination.
- Provides robust security by validating application commands and payloads, blocking non-compliant traffic.
- Disadvantages: Higher processing overhead due to deep inspection and connection splicing, potentially causing performance bottlenecks.

Summary

- Firewalls are fundamental chokepoints that enforce access control policies between trusted intranets and untrusted internets.
- Packet filters provide high-speed, layer 3/4 enforcement but lack deep context.
- Stateful inspection enhances security by tracking the lifecycle of transport-layer connections.
- Proxy firewalls deliver maximum scrutiny by validating layer 7 application data.
- Modern enterprise security relies on Next-Generation Firewalls (NGFW) which combine all these techniques with intrusion prevention in a unified appliance.

Computer Networks (DI03000051)

GTU Diploma Engineering

Agenda

- Firewalls: Introduction and Working Principles
- Design Principles and Goals
- Packet Filter Firewalls
- Proxy (Application-Level) Firewalls
- Comparison and Best Practices

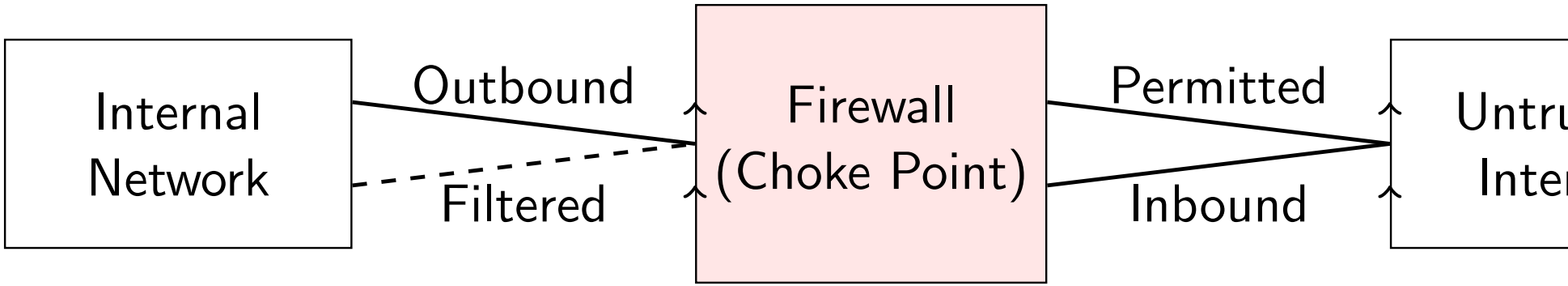
Firewalls: Introduction & Working Principles

- A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
- It establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet.
- Working Principle: Traffic enters or leaves the network strictly through the firewall. The firewall evaluates traffic against an Access Control List (ACL).
- Traffic that does not meet the specified security criteria is dropped, preventing unauthorized access while allowing legitimate communication.

Firewall Design Goals

- Choke Point Functionality: All traffic from inside to outside, and vice versa, must pass through the firewall, centralizing access control.
- Authorized Traffic Only: Only authorized traffic, as defined by the local security policy, is permitted to pass.
- Immunity to Penetration: The firewall system itself must be highly secured against penetration, typically running a hardened operating system.
- Default Deny Posture: The most secure approach where everything not explicitly permitted is forbidden.
- Default Allow Posture: Everything not explicitly forbidden is permitted (easier to manage, but significantly less secure).

Diagram: General Firewall Architecture



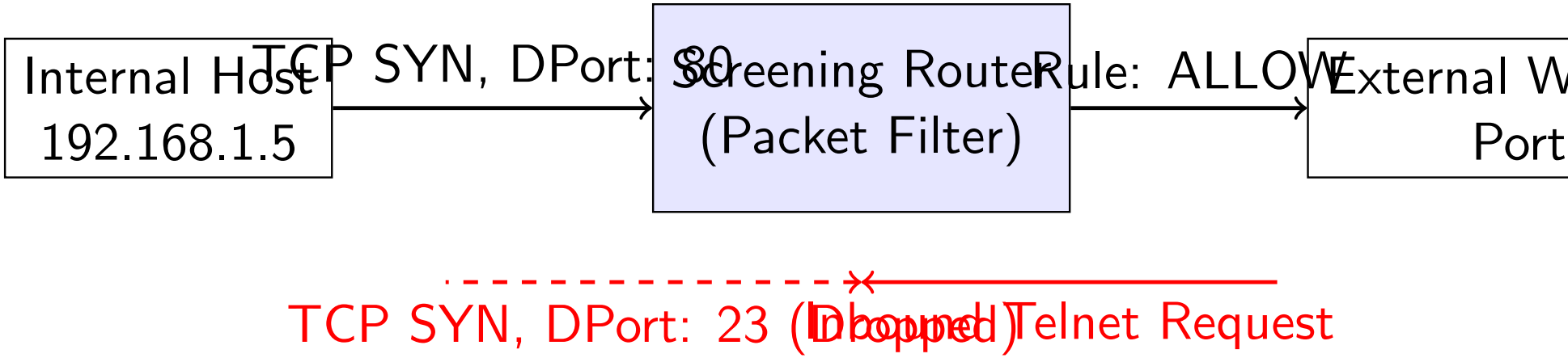
Packet Filter Firewalls

- A packet filtering firewall applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet.
- Operates primarily at the Network layer (Layer 3) and Transport layer (Layer 4) of the OSI model.
- Filtering rules are based on fields in headers: Source/Destination IP address, Source/Destination port, and Protocol type (TCP, UDP, ICMP).
- Advantages: Low cost, widely available in standard routers, high performance and low processing overhead.
- Disadvantages: Cannot prevent application-layer attacks (e.g., malicious payloads), susceptible to IP spoofing if not configured with anti-spoofing rules.

Packet Filtering Rules Example

- Rule 1 (Allow Web Browsing): Allow outbound TCP packets with Destination Port 80 (HTTP) or 443 (HTTPS).
- Rule 2 (Allow DNS): Allow outbound UDP packets to port 53 (DNS) for domain name resolution.
- Rule 3 (Block Telnet): Deny incoming TCP packets destined for port 23 to prevent insecure remote access.
- Rule 4 (Block IP Spoofing): Deny incoming packets arriving on an external interface but possessing a source IP address from the internal network range.
- Rule 5 (Default Drop): Deny all other traffic (implicit deny at the end of the Access Control List).

Diagram: Packet Filter Operation



Proxy Firewalls (Application-Level Gateways)

- A proxy firewall operates at the Application layer (Layer 7), acting as an intermediary for specific applications (e.g., HTTP, FTP).
- Instead of directly routing packets, the user contacts the proxy, which then establishes a separate connection to the actual destination on behalf of the user.
- Deep Packet Inspection: Proxy firewalls inspect the entire payload of the packet to detect malicious content (e.g., viruses, SQL injection).
- Advantages: Highly secure, prevents direct end-to-end connections, hides internal IP addresses, provides detailed application-level logging.
- Disadvantages: High processing overhead causing latency, breaks client-server model, requires a specific proxy for each supported protocol.

Proxy vs. Packet Filter Comparison

- OSI Layer: Packet Filters operate at L3/L4 (Network/Transport). Proxies operate at L7 (Application).
- Inspection Depth: Packet Filters only examine headers (IP, TCP/UDP). Proxies examine headers and the full data payload.
- Performance: Packet Filters offer high speed and low latency. Proxies introduce significant latency due to connection termination and deep inspection.
- Security Level: Proxies provide higher security against application-layer attacks. Packet filters are susceptible to spoofing and payload exploits.
- Typical Deployment: Packet filters are deployed at the network perimeter (edge routers). Proxies are often deployed in the DMZ or as part of a layered defense architecture.

Computer Networks (DI03000051)

GTU Diploma Engineering

Agenda

- Introduction to Firewalls
- Working and Design Principles
- General Firewall Architecture
- Packet Filter Firewalls
- Proxy Firewalls
- Summary and Conclusion

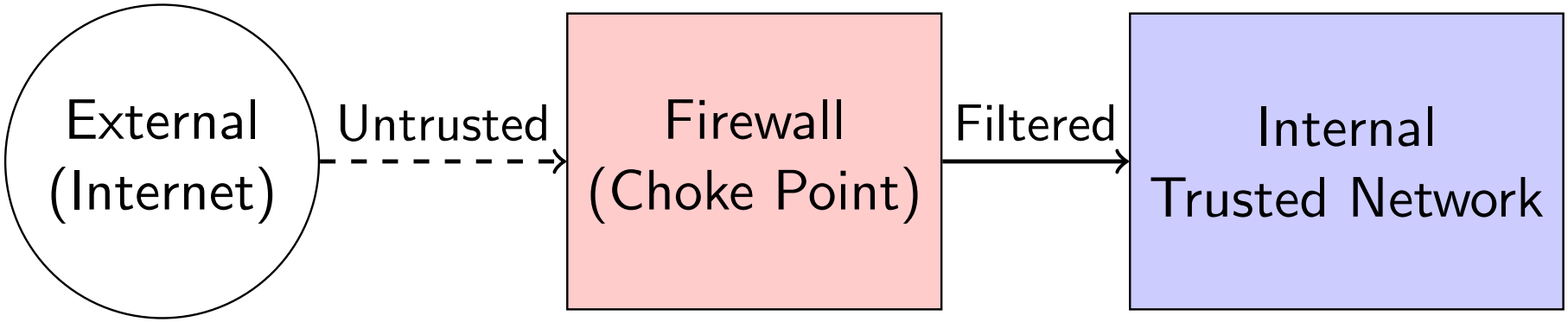
Firewalls: Introduction & Working Principle

- A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
- It establishes a barrier between a trusted internal network and untrusted external networks, such as the Internet.
- Working Principle: It acts as a choke point where all traffic must pass, allowing the system to inspect packets and drop those that violate security policies.
- Firewalls can be implemented in both hardware and software, or a combination of both.
- Commonly deployed at the network perimeter to defend against unauthorized access, malicious traffic, and denial-of-service attacks.

Design Principles of Firewalls

- Principle of Least Privilege: Deny everything by default, and only explicitly allow required services and traffic (Default Deny policy).
- Choke Point: A firewall must be the single point of entry and exit between the protected network and external environments, ensuring no bypassing is possible.
- Defense in Depth: Firewalls are only one layer of security and should be complemented with Intrusion Detection/Prevention Systems (IDS/IPS), antivirus, and strong authentication.
- Simplicity: Keep firewall rule sets as simple as possible. Complex rule sets increase the likelihood of misconfiguration and security holes.
- Logging and Auditing: All dropped packets and critical administrative actions must be logged for forensic analysis and intrusion detection.

Diagram: General Firewall Architecture



All traffic must pass through the firewall

Packet Filter Firewall: Overview

- Operates primarily at the Network layer (Layer 3) and Transport layer (Layer 4) of the OSI model.
- Inspects individual packets in isolation without understanding the context of a connection or application state (Stateless).
- Filtering rules are based on IP headers and TCP/UDP headers.
- Common match criteria include Source/Destination IP address, Protocol ID (e.g., TCP, UDP, ICMP), and Source/Destination port numbers.
- Example rule: ALLOW Inbound TCP packets to Destination IP 192.168.1.10 on Port 80 (HTTP).

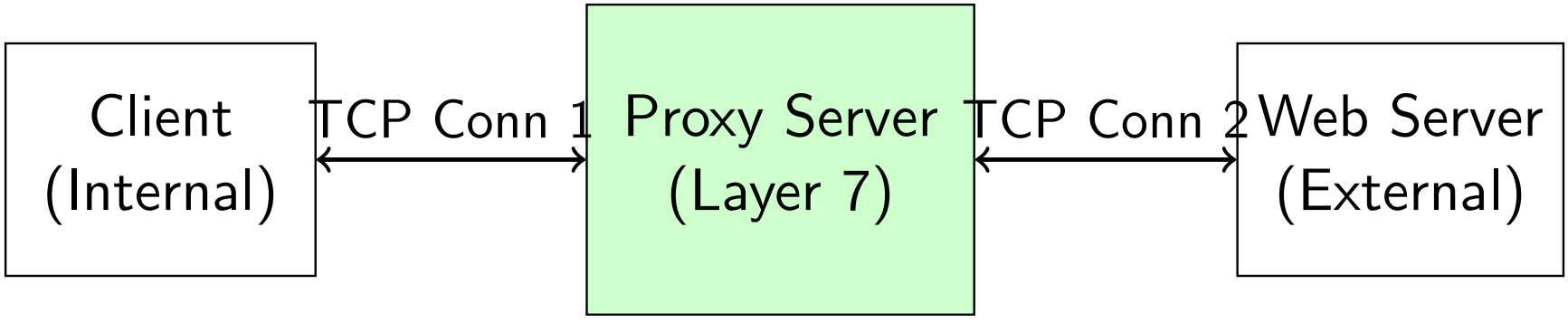
Packet Filter Firewall: Advantages & Limitations

- Advantages:
- - High Performance: Extremely fast because inspection requires minimal processing (just header evaluation).
- - Transparency: Users and applications are unaware of the firewall's presence.
- - Low Cost: Most basic routers provide packet filtering capabilities natively.
- Limitations:
- - No Application Awareness: Cannot detect application-layer attacks or malicious payloads.
- - Vulnerable to IP Spoofing: If filtering relies only on source IP, attackers can forge IP addresses.
- - Complex Rule Management: Maintaining large access control lists (ACLs) is error-prone.

Proxy Firewall: Overview

- Also known as Application-Level Gateway (ALG). Operates at the Application layer (Layer 7) of the OSI model.
- Breaks the direct client-server connection by acting as an intermediary. The client connects to the proxy, and the proxy connects to the destination server.
- Deep Packet Inspection: Understands application protocols (e.g., HTTP, FTP, SMTP) and can inspect the actual payload for malicious content or policy violations.
- Can perform content caching, URL filtering, and user authentication before allowing access.
- Provides the highest level of security among traditional firewalls but at the cost of performance due to heavy processing overhead.

Diagram: Proxy Firewall Architecture



No direct end-to-end network connection

Conclusion & Summary

- Firewalls enforce network perimeter security by controlling traffic flow based on policies.
- Design principles mandate a single choke point, default-deny policies, and simplicity in rules.
- Packet Filters offer high-speed, stateless filtering at layers 3/4 but lack deep payload inspection.
- Proxy Firewalls (Application Gateways) provide robust layer 7 security by breaking direct connections and inspecting payloads, though they introduce latency.
- Modern networks often use Next-Generation Firewalls (NGFW) which combine packet filtering, stateful inspection, and application-level proxies into a single appliance.