

UNIT 1

Introduction to Computer Networking

(6 Hours) — Computer Networking (CACS303)

A computer network is a collection of interconnected computing devices — computers, servers, mobile devices, and other hardware — that are linked together using communication links so that they can exchange data and share resources such as files, printers, and internet connections. Networking forms the technological backbone of virtually every modern digital service, from email and web browsing to cloud computing and video conferencing.

1.1 Network as an Infrastructure for Data Communication

Data communication refers to the exchange of data between two devices through some form of transmission medium such as a copper wire, optical fibre, or radio wave. For communication to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs). A computer network provides the infrastructure — the physical and logical components — that enables this data communication to happen reliably and efficiently across distances ranging from a single room to across the globe.

Basic Components of Data Communication

- Message — the information (text, number, image, audio, video) to be communicated.
- Sender — the device that sends the message (e.g., a computer, workstation, telephone handset).
- Receiver — the device that receives the message at the other end of the medium.
- Transmission Medium — the physical path (twisted pair, coaxial cable, fibre optic, radio waves) through which the message travels.
- Protocol — a set of rules that governs data communication, ensuring both sender and receiver understand each other.

Data flows as electrical, optical, or radio signals over the medium



Effectiveness of a Data Communication System

The effectiveness of a data communication system depends on four fundamental characteristics:

- **Delivery** — data must be delivered to the correct destination and to no other device.
- **Accuracy** — data must be delivered accurately, without being altered during transmission.
- **Timeliness** — data must be delivered in a timely manner; delayed data, especially in real-time applications like audio/video, is of little or no use.
- **Jitter** — refers to the variation in packet arrival time; uneven jitter affects the quality of audio and video streams.

Note: A network is essentially the physical and logical infrastructure — cabling, switches, routers, protocols, and addressing schemes — that makes reliable data communication possible between many devices simultaneously, not just between a single pair.

1.2 Applications of Computer Network

Computer networks have become deeply embedded in business, education, government, and personal life. Some of the major application areas are described below.

Business Applications

- **Resource Sharing** — sharing of hardware (printers, scanners), software, and data among multiple users, reducing cost and duplication.
- **Communication** — email, instant messaging, video conferencing (e.g., Zoom, MS Teams) enable fast internal and external communication.
- **E-Commerce** — online buying/selling, electronic banking, and digital payment systems all rely on networked infrastructure.
- **Client-Server Computing** — centralized database servers allow many client applications to access and update shared business data.

Home and Personal Applications

- **Access to Remote Information** — web browsing, online news, digital libraries, and government e-services.
- **Person-to-Person Communication** — social media, VoIP calls, messaging apps.
- **Interactive Entertainment** — online gaming, video-on-demand (Netflix, YouTube), streaming music.

- Electronic Commerce — online shopping, auctions, and mobile payment apps such as eSewa or Khalti.

Mobile & Emerging Applications

- Mobile Networking — smartphones and tablets connect via cellular and Wi-Fi networks for always-on access.
- Internet of Things (IoT) — smart homes, wearables, and industrial sensors communicate over networks with minimal human intervention.
- Cloud Computing — storage, computation, and software delivered as services over the network (e.g., Google Drive, AWS).

Why Networks Matter

- ✓ Enable resource and information sharing across users and organizations
- ✓ Support real-time global communication and collaboration
- ✓ Form the backbone of e-commerce, cloud computing, and IoT
- ✓ Reduce cost by allowing shared use of expensive hardware and software

1.3 Network Architecture

Network architecture refers to the overall design of a computer network, including the physical layout (topology), the logical flow of data, communication protocols, and infrastructure arrangement. The two dominant architectural models for organizing how computers interact are the Client-Server model and the Peer-to-Peer (P2P) model.

Client-Server Architecture

In this model, one or more powerful computers called servers provide services (such as file storage, email, or web pages), while other computers called clients request and use those services. Servers are typically centralized, always available, and manage shared resources; clients initiate communication whenever they need a service.

Example 1.1 — Client-Server in Action

When a student opens a browser and types a college website's address, the browser (client) sends a request to the college's web server. The server processes the request and sends back the requested web page, which the browser then displays.

Peer-to-Peer (P2P) Architecture

In a peer-to-peer network, all connected devices ('peers') have equal status — each can act as both client and server, sharing resources directly with one another without relying on a centralized server. P2P networks are simple and inexpensive to set up but become difficult to manage and secure as the number of peers grows.

Aspect	Client-Server	Peer-to-Peer
Control	Centralized on server	Decentralized among peers
Scalability	High — servers can be upgraded independently	Limited — performance degrades with more peers
Cost	Higher (dedicated server hardware)	Lower (no dedicated server needed)
Security	Easier to manage centrally	Harder — each peer must secure itself
Example Use	Websites, email servers, databases	File-sharing networks, small office LANs

Note: Most large-scale real-world networks, including the Internet, use a combination of both architectures at different levels — client-server for core services and peer-to-peer for specific applications like content distribution.

1.4 Types of Computer Networks

Computer networks are commonly classified according to their geographical scale — the physical area they cover. The four principal categories are PAN, LAN, MAN, and WAN.

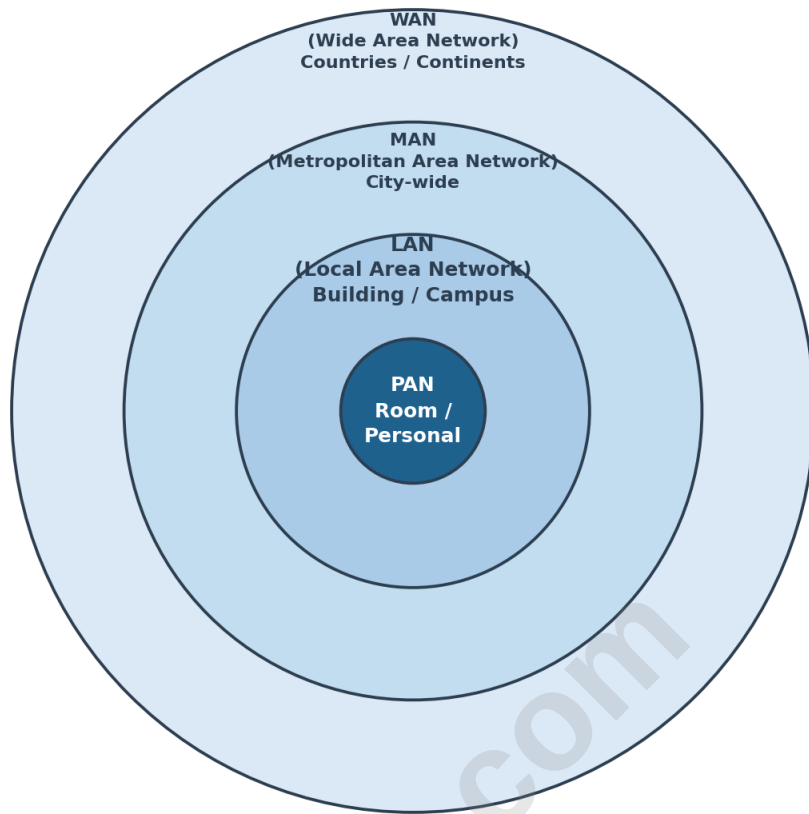


Figure 1.2: Classification of networks by geographical scale, from smallest (PAN) to largest (WAN)

Personal Area Network (PAN)

A PAN connects personal devices within the range of an individual, typically within a single room, such as a smartphone, laptop, wireless earbuds, and smartwatch connected via Bluetooth or infrared. Range is usually within a few metres.

Local Area Network (LAN)

A LAN connects computers and devices within a limited area such as a single building, office, or campus. LANs are typically owned and managed by a single organization and offer very high data transfer rates (100 Mbps to several Gbps) at low cost.

Metropolitan Area Network (MAN)

A MAN spans a larger geographical area than a LAN, typically covering a city or a large campus network spread across a town. MANs often interconnect multiple LANs and are commonly used by cable TV companies and municipal networks.

Wide Area Network (WAN)

A WAN spans a large geographical area — a country, continent, or the entire globe. The Internet itself is the largest and best-known example of a WAN. WANs typically use leased telecommunication lines, satellite links, or undersea fibre-optic cables, and generally have lower data rates and higher latency than LANs due to the greater distances involved.

Type	Typical Coverage	Ownership	Example
PAN	Few metres (a room)	Individual	Bluetooth headset with phone
LAN	Building / Campus	Single organization	Office or college network
MAN	City / Town	One or more organizations / ISP	Cable TV network, city Wi-Fi
WAN	Country / Global	Multiple organizations / ISPs	The Internet

1.5 Protocols and Standards

Protocols

A protocol is a formal set of rules and conventions that govern how data is formatted, transmitted, and received across a network, so that devices — even those made by different manufacturers — can communicate correctly. A protocol defines three key elements:

- Syntax — the structure or format of the data, i.e., the order in which data is presented.
- Semantics — the meaning of each section of bits; how a particular pattern is to be interpreted and what action is to be taken.
- Timing — when data should be sent and how fast it can be sent (synchronization of sender and receiver speeds).

Standards

Standards provide guidelines to manufacturers, vendors, and service providers to ensure interoperability among networking products from different sources. Standards are broadly classified into two categories:

- De facto standards — standards that have not been formally planned but have emerged and become widely accepted through common usage (e.g., early Ethernet).
- De jure standards — standards that have been legislated or formally adopted by an authorized, recognized body (e.g., standards from ISO, IEEE, ITU-T).

Organization	Full Form	Role
ISO	International Organization for Standardization	Developed the OSI Reference Model
IEEE	Institute of Electrical and Electronics Engineers	Defines LAN standards (e.g., IEEE 802.3 Ethernet, 802.11 Wi-Fi)
ITU-T	International Telecommunication Union	Standardizes telecommunication systems
IETF	Internet Engineering Task Force	Develops Internet standards (RFCs), TCP/IP protocols
ANSI	American National Standards Institute	Coordinates U.S. voluntary standards

1.6 The OSI Reference Model

The Open Systems Interconnection (OSI) model was developed by the International Organization for Standardization (ISO) in 1984 as a conceptual framework that standardizes the functions of a communication system into seven distinct, hierarchical layers. Each layer performs a specific set of functions and communicates only with the layer directly above and below it.

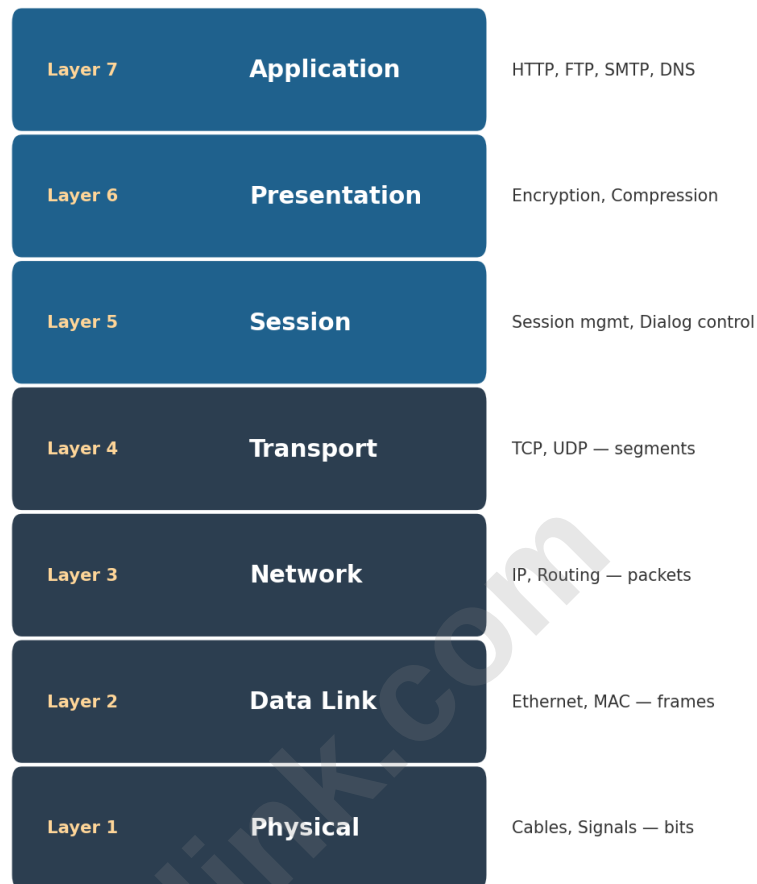


Figure 1.3: The seven layers of the OSI Reference Model, from Physical (Layer 1) to Application (Layer 7)

Functions of Each Layer

- Layer 1 — Physical: Transmits raw bits over a physical medium; deals with voltage levels, cabling, connectors, and data rates.
- Layer 2 — Data Link: Organizes bits into frames, handles physical addressing (MAC), error detection, and flow control between directly connected nodes.
- Layer 3 — Network: Responsible for logical addressing (IP) and routing of packets across multiple networks to reach the destination.
- Layer 4 — Transport: Provides end-to-end delivery of data (segments), including error recovery, flow control, and multiplexing (e.g., via TCP/UDP port numbers).
- Layer 5 — Session: Establishes, manages, and terminates sessions (dialogs) between two communicating applications.
- Layer 6 — Presentation: Handles translation, encryption/decryption, and compression of data so it is presented in a usable format to the Application layer.

- Layer 7 — Application: Provides network services directly to end-user applications, such as email, file transfer, and web browsing.

Note: A common mnemonic to remember the OSI layers from Layer 1 to Layer 7 is: 'Please Do Not Throw Sausage Pizza Away' (Physical, Data Link, Network, Transport, Session, Presentation, Application).

1.7 The TCP/IP Protocol Suite

The TCP/IP protocol suite (Transmission Control Protocol / Internet Protocol) was developed by the U.S. Department of Defense (DARPA) prior to the OSI model, and is the actual protocol suite that powers the modern Internet. Unlike OSI, which is largely a theoretical reference model, TCP/IP is an implemented and widely deployed protocol stack organized into four layers.

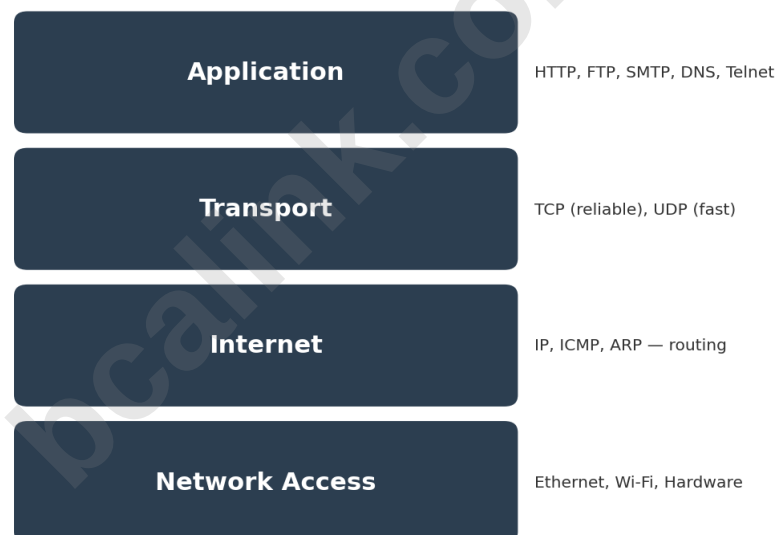


Figure 1.4: The four layers of the TCP/IP protocol suite

Layers of the TCP/IP Suite

- Application Layer: Combines the functions of OSI's Application, Presentation, and Session layers; includes protocols such as HTTP, FTP, SMTP, DNS, and Telnet.
- Transport Layer: Provides end-to-end communication using TCP (connection-oriented, reliable) or UDP (connectionless, fast, used for streaming/gaming).
- Internet Layer: Handles logical addressing and routing using the Internet Protocol (IP), along with supporting protocols like ICMP and ARP.

- Network Access Layer (also called Link Layer): Combines the functions of OSI's Data Link and Physical layers; deals with the physical transmission of data over hardware such as Ethernet or Wi-Fi.

Example 1.2 — Sending an Email over TCP/IP

When you send an email, the Application layer protocol SMTP hands the message to TCP at the Transport layer, which breaks it into segments and ensures reliable delivery. The Internet layer (IP) routes these segments across networks using IP addresses, and the Network Access layer transmits them as electrical or radio signals over the physical link.

1.8 Comparison between OSI and TCP/IP Reference Model

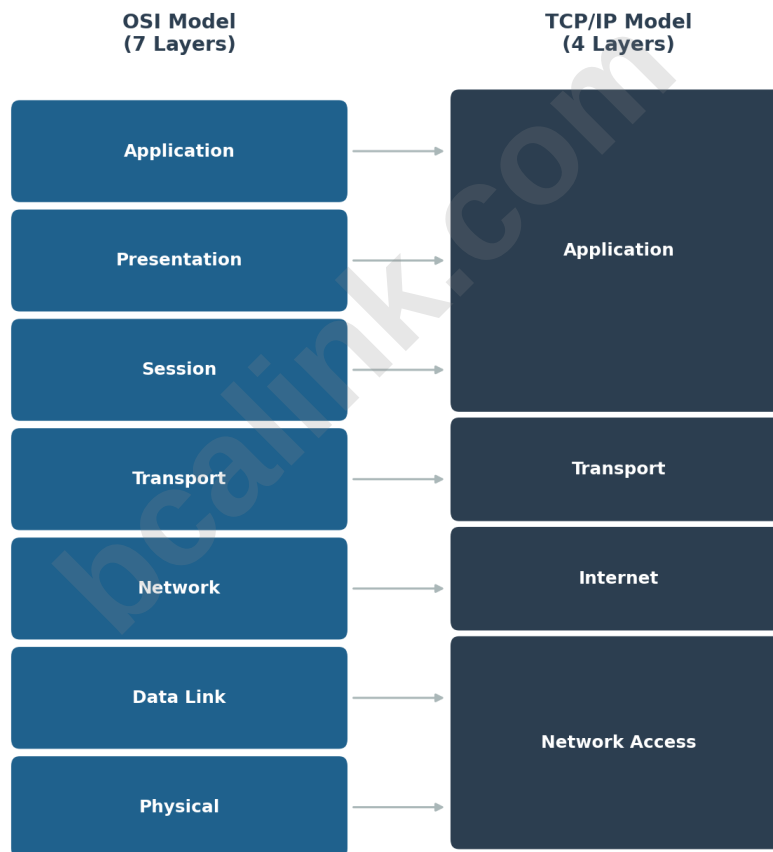


Figure 1.5: Mapping of the seven OSI layers onto the four layers of the TCP/IP model

Basis	OSI Model	TCP/IP Model
Full Form	Open Systems Interconnection	Transmission Control Protocol / Internet Protocol
Developed By	ISO (1984)	DARPA / U.S. Department of Defense (1970s)

Basis	OSI Model	TCP/IP Model
Number of Layers	7 layers	4 layers
Approach	Theoretical / reference model	Practical, implementation-based model
Layer Boundaries	Clearly defined and independent	Layers sometimes merged; less rigid boundaries
Protocol Dependency	Model is protocol-independent (generic)	Protocols came first; model describes existing protocols
Reliability Location	Reliability enforced mainly at Transport and Network layers	Reliability enforced only at Transport layer (TCP)
Usage Today	Used mainly as a conceptual/teaching reference	Actually implemented and used on the Internet

1.9 Critiques of OSI and TCP/IP Reference Model

Criticism of the OSI Model

- **Bad timing:** The OSI standard was published after TCP/IP protocols were already widely implemented, so vendors were reluctant to switch.
- **Bad technology:** Some layers (e.g., Session and Presentation) are nearly empty in practice, while functions like error handling appear redundantly in multiple layers.
- **Bad implementation:** Early OSI implementations were large, slow, and considered inferior in performance compared to TCP/IP-based systems.
- **Bad politics:** OSI was closely associated with European governments and bureaucratic standardization committees, which some in the technical community found slow and overly political.

Criticism of the TCP/IP Model

- **Not a generic model:** TCP/IP does not clearly distinguish between the concepts of service, interface, and protocol, unlike OSI, making it less suitable as a generic teaching reference.
- **Not general enough to describe other stacks:** The model does not describe protocol stacks other than TCP/IP itself (e.g., it struggles to describe Bluetooth stacks properly).
- **Network Access layer is not truly a layer:** It is more of an interface between the Internet layer and the physical network technology, rather than a genuine layer with its own well-defined function.
- **No clear separation between Physical and Data Link functions:** These are very different functions that OSI separates but TCP/IP does not.

Note: In practice, most networking professionals use a hybrid approach: OSI's seven-layer model is used for teaching, troubleshooting, and conceptual understanding, while TCP/IP remains the protocol suite that is actually implemented and running on real-world networks, including the Internet.

Key Takeaways — Unit 1

- ✓ A computer network is an infrastructure of interconnected devices enabling data communication, governed by protocols ensuring delivery, accuracy, timeliness, and low jitter
- ✓ Networks support diverse applications: business communication, e-commerce, entertainment, IoT, and cloud computing
- ✓ Network architecture is broadly Client-Server (centralized) or Peer-to-Peer (decentralized)
- ✓ Networks are classified by scale as PAN, LAN, MAN, and WAN
- ✓ Protocols define syntax, semantics, and timing; standards (de facto / de jure) ensure interoperability
- ✓ The OSI model has 7 layers and is a theoretical reference; TCP/IP has 4 layers and is the practically implemented suite powering the Internet
- ✓ Both models have well-documented criticisms — OSI for timing/complexity, TCP/IP for lack of generality

— *End of Unit 1* —