Introduction to Computer Networks

Understanding Networks & The OSI Model

Your Name

Institution Name

February 19, 2025

What is a Computer Network? Understanding the Basics

- A **computer network** is a collection of interconnected devices that can communicate and share resources with each other.
- Networks enable the sharing of resources such as files, printers, and internet connections between connected devices.

Key Concept

Networks operate using standardized **protocols**, which are sets of rules that govern how devices communicate.

-
- Modern networks range from simple home setups connecting a few devices to complex enterprise systems connecting thousands of computers.

Networks in Our Daily Lives: From Home to Enterprise

Common Network Applications

- Home Networks:
  - Wi-Fi connections for smartphones, laptops, and smart devices
  - Shared printers and media servers
  - Smart home automation systems
- Enterprise Networks:
  - Shared database access and file storage
  - Email and communication systems
  - Customer management systems

Every time you browse the internet, stream videos, or send messages, you're utilizing multiple computer networks.

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

- A **Local Area Network (LAN)** connects devices within a limited area like a home, school, or office building.
- A **Wide Area Network (WAN)** spans a large geographic area, with the Internet being the largest example.
- A **Metropolitan Area Network (MAN)** covers a city or large campus, bridging the gap between LANs and WANs.
- A **Personal Area Network (PAN)** connects devices within a very short range, such as Bluetooth connections between your phone and headphones.

Network Type	Typical Range
PAN	1-10 meters
LAN	Up to 1 kilometer
MAN	Up to 50 kilometers
WAN	Worldwide

Network Topologies: Star, Bus, Ring, and Mesh

- A **network topology** defines the physical or logical arrangement of devices and connections in a network.
- The **star topology** connects all devices to a central hub or switch, making it easy to manage but vulnerable to central point failure.
- The **bus topology** connects all devices to a single central cable, creating a simple but outdated design that was common in early Ethernet networks.

Advanced Topologies

- The **mesh topology** connects devices with multiple paths, providing redundancy and fault tolerance.
- The **ring topology** connects each device to exactly two other devices, forming a circular path for data transmission.

Client-Server vs Peer-to-Peer Networks

Client-Server Network:

- Dedicated servers provide resources and services to client computers.
- Examples include email servers, web servers, and file servers.
- Offers centralized control and better security but requires more maintenance.

Peer-to-Peer Network:

- Each computer can act as both client and server, sharing resources directly.
- Examples include BitTorrent file sharing and early versions of Napster.
- Provides simpler setup but less security and harder to manage at scale.

Introduction to the OSI Model: Why It Matters

Definition

The **OSI (Open Systems Interconnection) Model** is a conceptual framework that standardizes the functions of a telecommunication or computing system into seven distinct layers.

- The OSI model helps network professionals understand, troubleshoot, and communicate about network operations.
- Each layer in the model performs specific functions and provides services to the layer above it.
- Understanding the OSI model is crucial for effective network design, maintenance, and troubleshooting.
- The model creates a common language for network professionals across different platforms and technologies.

The OSI Model: A Seven-Layer Journey

Layer Structure (Bottom to Top)

1. **Physical Layer:** Handles raw bit transmission
2. **Data Link Layer:** Provides node-to-node delivery
3. **Network Layer:** Manages addressing and routing
4. **Transport Layer:** Ensures end-to-end delivery
5. **Session Layer:** Manages connections between applications
6. **Presentation Layer:** Formats and encrypts data
7. **Application Layer:** Provides network services to applications

Key Concept

Data flows down the layers when sending and up the layers when receiving, with each layer adding or removing its own control information.

Layer 1 - Physical Layer: The Foundation

Physical Layer Responsibilities

- The **Physical Layer** is responsible for transmitting raw bits over a physical medium like copper wire, fiber optic cable, or radio waves.
- This layer defines physical characteristics such as voltage levels, timing of voltage changes, physical data rates, and maximum transmission distances.
- It specifies the shape and layout of pins in network interfaces, as well as the functions of each pin.
- The Physical Layer converts digital bits into signals that can be transmitted over the network media.

Physical Layer Components: Cables, Hubs, and Signals

Common Physical Media:

- **Twisted Pair Cable:** Used in Ethernet networks, comes in shielded (STP) and unshielded (UTP) varieties.
- **Fiber Optic Cable:** Uses light for transmission, offering high speeds and immunity to electromagnetic interference.
- **Wireless Media:** Uses radio frequencies to transmit data through the air.

Key Devices

- Hubs
- Repeaters
- Network adapters
- Cable connectors

Layer 2 - Data Link Layer: Bridging the Gap

- The **Data Link Layer** provides reliable point-to-point delivery of data frames between directly connected nodes.
- This layer detects and possibly corrects errors that may occur in the Physical Layer.

Primary Functions

- **Framing:** Organizes bits from Physical Layer into manageable data units called frames.
- **Physical Addressing:** Adds MAC addresses to identify source and destination devices.
- **Error Control:** Detects and retransmits corrupted or lost frames.
- **Flow Control:** Prevents overwhelming slower receiving devices.

MAC Addresses and Ethernet: Data Link Essentials

What is a MAC Address?

A **Media Access Control (MAC) address** is a unique 48-bit identifier assigned to network interfaces for communications at the Data Link Layer.

- MAC addresses are written as six pairs of hexadecimal digits (e.g., 00:1A:2B:3C:4D:5E).
- Every network interface card (NIC) has a unique MAC address burned into it during manufacturing.
- **Ethernet** is the most common Data Link Layer protocol, providing rules for:
  - Cable types and connections
  - Data packet format
  - Protocol for sharing cable capacity

Layer 3 - Network Layer: Finding the Path

Network Layer Purpose

The **Network Layer** is responsible for packet forwarding and routing between different networks, enabling data to travel across multiple networks to reach its final destination.

- This layer handles logical addressing (IP addresses) and determines the best path for data to travel.
- **Routers** operate at the Network Layer, making decisions about how to forward packets based on logical addresses.
- The Network Layer must handle congestion and ensure quality of service (QoS) for different types of data.
- It manages the connection of heterogeneous networks, allowing different types of networks to communicate.

IP Addressing and Routing: Network Layer Deep Dive

IPv4 Addressing:

- 32-bit addresses written in four octets (e.g., 192.168.1.1)
- Divided into network and host portions
- Supports about 4.3 billion unique addresses

IPv6 Addressing:

- 128-bit addresses written in hexadecimal
- Provides vastly more unique addresses
- Designed to replace IPv4 as addresses run out

Routing Concepts

- Routers maintain routing tables to determine the best path for packets
- Path selection can be static (manually configured) or dynamic (automatically updated)

Layer 4 - Transport Layer: End-to-End Communication

- The **Transport Layer** ensures complete data transfer by providing:
  - End-to-end error recovery
  - Flow control
  - Segmentation of data
- This layer can establish multiple connections for different applications on the same device.
- It provides either connection-oriented (**TCP**) or connectionless (**UDP**) communication.

Key Concept

The Transport Layer is the first layer to provide end-to-end communication between source and destination hosts.

TCP vs UDP: Understanding Transport Protocols

Transmission Control Protocol (TCP):

- Provides reliable, ordered delivery of data
- Establishes connections before sending data
- Includes error checking and recovery
- Used for email, web browsing, file transfer

User Datagram Protocol (UDP):

- Offers fast, connectionless delivery
- No guarantee of delivery or ordering
- Lower overhead than TCP
- Used for streaming, gaming, DNS queries

When to Use Each

Choose TCP when reliability is crucial, and UDP when speed is more important than guaranteed delivery.

Layer 5 - Session Layer: Managing Connections

Primary Role

The **Session Layer** establishes, manages, and terminates connections (sessions) between applications on different devices.

- This layer handles the organization of communication through features like dialog control and synchronization.
- It provides three different modes of communication:
  - **Simplex:** One-way communication
  - **Half-duplex:** Two-way communication, one direction at a time
  - **Full-duplex:** Simultaneous two-way communication
- The Session Layer can establish checkpoints for long data transfers, enabling recovery from failures without starting over.

Layer 6 - Presentation Layer: Data Translation

- The **Presentation Layer** ensures that data is readable by the receiving system through:
  - Character code translation (e.g., ASCII to EBCDIC)
  - Data compression to reduce size
  - Data encryption for security
  - Data formatting for different systems

Important Note

This layer acts as the "translator" of the network, converting data between different formats while maintaining its meaning.

- Common data formats handled include JPEG, MIDI, MPEG, and ASCII.
- The Presentation Layer enables different systems to communicate regardless of their internal data representations.

Encryption and Data Formats in the Presentation Layer

Data Security Functions

- **Encryption Protocols:**
  - SSL/TLS for secure web browsing
  - SSH for secure remote access
  - PGP for secure email communication

- The Presentation Layer handles data compression using various algorithms:
  - Lossless compression for critical data
  - Lossy compression for multimedia content
- Common data format conversions include:
  - Text encodings (ASCII, Unicode, UTF-8)
  - Image formats (JPEG, PNG, GIF)
  - Audio/Video formats (MP3, MP4, AVI)

Layer 7 - Application Layer: User Interface

Definition

The **Application Layer** is the topmost layer of the OSI model, providing network services directly to end-user applications.

- This layer enables users and applications to access network services through:
    - Network resource identification and synchronization
    - Partner identification and quality of service
    - User authentication and privacy considerations
- The Application Layer handles user interface and support for services like email, file transfer, and web browsing.
- It determines resource availability and synchronizes communication between applications.

Common Application Layer Protocols: HTTP, FTP, SMTP

Web and File Transfer:

- **HTTP/HTTPS:** Web browsing and secure transactions
- **FTP:** File Transfer Protocol for uploading and downloading files
- **DNS:** Domain Name System for translating domain names

Email and Communication:

- **SMTP:** Sending email messages
- **POP3/IMAP:** Receiving email messages
- **DHCP:** Automatic IP address assignment

Protocol Functions

Each protocol provides specific services:

- Data formatting and encoding
- Session management
- Error reporting

Data Flow Through the OSI Layers: The Big Picture

Data Encapsulation (Sending)

1. Application Layer creates user data
2. Presentation Layer formats and encrypts
3. Session Layer adds session control
4. Transport Layer segments data and adds port numbers
5. Network Layer adds IP addresses
6. Data Link Layer adds MAC addresses
7. Physical Layer converts to bits for transmission

Key Concept

Each layer adds its own header information to the data, a process called encapsulation. The receiving device reverses this process through de-encapsulation.

Encapsulation and De-encapsulation in OSI Model

- **Protocol Data Units (PDUs)** have different names at each layer:
    - Application Layer: Data
    - Transport Layer: Segments
    - Network Layer: Packets
    - Data Link Layer: Frames
    - Physical Layer: Bits
- Each layer adds control information:
    - Headers added at the beginning
    - Trailers added at the end (in some layers)
    - Original data remains unchanged

Important Note

The receiving device removes headers in reverse order, ensuring data integrity throughout the process.

Practical Example: Web Browsing Through OSI Layers

When you type www.example.com in your browser:

1. **Application Layer:** HTTP request is generated
2. **Presentation Layer:** Data is formatted and possibly encrypted (HTTPS)
3. **Session Layer:** TCP session is established
4. **Transport Layer:** Data is segmented, TCP ports assigned
5. **Network Layer:** IP addresses added after DNS lookup
6. **Data Link Layer:** Frame created with MAC addresses
7. **Physical Layer:** Converted to bits and transmitted

Think About

How would this process differ for streaming video vs. sending an email?

Troubleshooting Scenario: Network Problems

Symptom: Cannot access website

- **Physical Layer:** Check cables connected?
- **Data Link:** Network adapter working?
- **Network:** IP address valid?
- **Transport:** Ports blocked?

Common Tools:

- ping (Network Layer)
- ipconfig (Network Layer)
- tracert (Network Layer)
- nslookup (Application Layer)

Discussion

What layer would you check first if a specific application fails but others work?

Review: Key Concepts and Their Relationships

- **Data Flow Understanding:**
  - How does encapsulation protect data integrity?
  - Why do we need different PDUs at different layers?
  - How do upper layers depend on lower layers?
- **Protocol Relationships:**
  - How do TCP and IP work together?
  - Why do we need both MAC and IP addresses?
  - How do application protocols use transport protocols?

Critical Thinking

Consider how changes in one layer might affect the others. For example, what happens when upgrading from IPv4 to IPv6?

Discussion Questions and Activities

Group Discussion Topics

- Compare and contrast different network topologies for a small business network.
- Explain how video conferencing applications use different layers of the OSI model.
- Analyze the security implications of using different protocols at each layer.
- Design a basic network setup for a home office, considering all OSI layers.

Hands-On Activities

- Use Wireshark to capture and analyze network traffic through OSI layers.
- Configure a basic home network and identify components at each layer.
- [illegible]