Chapter 1

Chapter 1

1 Introduction

Networking is about how we can get information from point A to B, and how we manage all the intricacies involved in making it work.

> OSI: Open Systems Interconnection

OSI was used to standardise all the necessary protocols so that any network could communicate with any other network. It's original intention was to serve as a general model of a network but also to specify the detailed protocols that could be used on each layer.

In the end it seems that ISO OSI was deprecated by the TCP/IP suite which was quite practical.

2 The Layers of ISO OSI

Each layer provides services for the one above, these services are isolated from one another as far as responsibility is concerned.

We must know:

- What functions each provides.
- What needn't be implemented at each layer (that can be delegated below.)

Starting from the to down ...

2.1 Application Layer (7)

- **Application Layer Overview:**
  - Layer 7 of the OSI model is the application layer.
  - Represents the functionality for network usage, such as sending emails, browsing web pages, etc.
  - Application software (e.g., web browser) interacts with the network's application layer.
  - New software applications often require new application layer protocols.
- **Examples of Application Layer Protocols:**
  - HTTP (Hypertext Transfer Protocol) for retrieving web pages.
  - SMTP (Simple Mail Transfer Protocol) for sending emails.
  - POP3 (Post Office Protocol version 3) for retrieving emails from a server.
- **HTTP Example:**
  - HTTP request example for retrieving a file from a server.
  - Response example includes server information and status codes.
- **Implementation of Application Layer Protocols:**
  - Software implementing application layer protocols reflects high-level tasks.
  - Components may be written as functions or may be more complex, especially for multiplayer games.
- **Role of Application Layer:**
  - Determines what should and shouldn't be achieved.
  - Should not be concerned with physical medium or routing details.
- **Abstract Services Provided by Lower Layers:**
  - Physical medium and routing should not impact the application layer.
  - The network should appear as a 'pipe' between application layer components.
  - Data should flow between client and server processes without consideration of low-level details.
- **Contentious Issues:**

- Data representation and message sequence are important considerations for the application layer protocol.

2.2 Presentation Layer (6)

- **Data Representation:**
  - Computers use binary numbers to represent data.
  - Different computers may use various encoding schemes like ASCII, EBCDIC, Unicode, UTF-8, UTF-16, and UTF-32.
  - ASCII and EBCDIC assign different numbers to the same characters, leading to encoding conflicts.
- **Character Encoding Translation:**
  - Computers with different encoding schemes cannot directly communicate.
  - Networks can translate requests into a common representation scheme.
  - Presentation layer translates characters between encoding schemes.
- **Issues with Character Encoding:**
  - Historical encoding schemes like Fieldata are rarely used today.
  - Modern application layer protocols like HTTP/1.1 handle character encoding directly.
  - Example: HTTP header may specify accepted character encodings, simplifying communication.
- **Date Representation:**
  - Different regions have varied interpretations of date formats.
  - Presentation layer could translate dates to a universal format for communication.
  - Example: Date formats may vary based on cultural and regional norms.
- **General Presentation Layer Functions:**
  - Presentation layer handles data representation and transformation.

- Standards like XML, HTML, MIME, and RFC 822 facilitate data presentation.
- Presentation layer functions may be integrated into application layer protocols or external utilities.
- **Integration with Protocol Stack:**
  - Presentation layer conceptually fits into layer 6 of the OSI model.
  - In practice, presentation layer functions may be included in the application layer or external tools.

2.3 Session Layer (5)

- **Session Layer Overview:**
  - Provides session-oriented services for applications.
  - Establishes, maintains, and terminates sessions.
  - Enforces dialogue control, determining message transmission between connected nodes.
- **Example: Reservation System:**
  - Illustrates session layer usage between a travel agency and airlines.
  - Agency interacts with a local system, unaware of communication with airlines.
  - Local system acts as a client to reservation services.
- **Session Management Challenges:**
  - Permanent connections to all airlines may be impractical due to various reasons.
  - Embedding session management in the application protocol is messy.
- **Role of Session Layer:**
  - Receives requests from the application layer and transmits them to the destination session layer.
  - Monitors session status, handling connection establishment, and termination transparently to the application layer.
- **Fault Tolerance and Transaction Handling:**

    - Session layer provides fault tolerance and transaction handling.
    - Re-establishes interrupted sessions, aborts actions, and replays requests in case of network failure.
    - Reports failure to the application layer if necessary.
- **Comparison with Current Protocols:**
    - Many current protocols lack fault tolerance at the session layer.
    - Web browsers typically report failure without attempting to re-establish sessions.
    - Fault tolerance is often part of the application layer protocol.
- **Ideal Layered Approach:**
    - Move technical details to lower layers whenever possible.
    - Work with abstract functionality on higher layers.
- **Modern Interpretation of Session Layer:**
    - In modern networks, the concept of a session layer often refers to the sequence of events in an application protocol.
    - Examples like POP3 demonstrate dialogue control within the application protocol sequence.
- **Potential Revival of True Session Layer:**
    - Web services and Service-oriented Architectures may revive interest in a true session layer, as envisioned by the ISO OSI model.

2.4 Transport Layer (4)

- **Layers 5, 6, and 7 Functionality:**
    - Layer 7 (Application Layer): Sends application requests.
    - Layer 6 (Presentation Layer): Adds semantic metadata.
    - Layer 5 (Session Layer): Handles session management.
- **Role of Layer 4 (Transport Layer):**

  - Enables process-to-process communication via the network.
  - Provides the pipe/channel/path for communication between processes.
- **Transport Layer Features:**
  - **End-to-End Connection:**
    - Ensures processes communicate without worrying about lower-level details.
  - **Reliability:**
    - Provides reliable end-to-end connections, including retransmission of lost parts of messages.
    - Indicates when something goes wrong to higher layers.
  - **Unreliable Pipes:**
    - Provides best-effort service for certain types of traffic.
    - May not attempt retransmission if a message cannot be delivered.
    - Preferred for certain types of traffic like voice, where interruptions are less significant.
    - In some cases, the underlying network infrastructure is reliable enough to not warrant additional reliability features.
    - Some application layer protocols do not require or cannot assume a reliable service.
- **Reasons for Unreliable Pipes:**
  - Some traffic types, like voice, benefit from continuous flow rather than stopping for retransmissions.
  - Overly reliable transport may slow down communication or be unnecessary due to robust network infrastructure.
  - Certain application layer protocols may not require reliability or cannot assume it during certain phases, like boot time.

2.5 Network Layer (3)

- **Functionality:**
  - Provides routing services to establish paths between processes across networks.
  - Handles the forwarding of messages from the source to the destination.
- **Routing Process:**
  - Involves navigating through networks to establish a route for message transmission.
  - Typically utilizes routing tables to determine the next hop for forwarding messages.
  - Routing tables contain address ranges and corresponding interfaces or next hops.
- **Example Scenario:**
  - Illustrates routing from a home network to a university's Computer Science Web server.
  - Involves multiple networks, ISPs, and routers interconnected to establish a path for communication.
  - Messages are forwarded based on routing tables, with each router determining the next hop towards the destination.
- **Realistic Considerations:**
  - Routing tables may use router addresses instead of interfaces for next hops.
  - Address ranges may need to be dynamically managed to accommodate network growth and reuse.
  - Various routing strategies exist, including source routing where the message itself includes the entire route to traverse.
  - Routing tables may be manually configured or automatically compiled through routing protocols like RIP (Routing Information Protocol).
- **Automated Routing:**
  - Routers exchange routing information with neighboring routers to update their routing tables.

- This automation process helps routers learn the network topology and determine routes effectively.
- **Routing Protocols:**
  - Application layer protocols, like RIP, handle route determination and utilize lower layers for message forwarding.
  - Detailed discussion on routing protocols will be covered in Chapter 3 and Chapter 7.
- **Distinction Between Routing and Route Determination:**
  - Routing involves forwarding messages based on established routes.
  - Route determination is an application layer function that utilizes lower layers for routing decisions.

2.6 Data Link Layer (2)

- **Functions:**
  - Solves data delineation problem: Marks the beginning and end of a message to distinguish between message frames.
  - Manages access to shared media to avoid collisions in broadcast scenarios.
  - Detects transmission errors to ensure data integrity.
- **Data Delineation Problem:**
  - Node needs to identify when a message starts and ends, even if the stream of bits contains sequences that might resemble message boundaries.
  - Data link layer protocols mark message boundaries to facilitate proper message reception and processing.
- **Broadcast Scenarios:**
  - Broadcast networks may have multiple nodes sharing the same medium.
  - Collision avoidance strategies, like master-slave protocols, are used to manage access to the medium.
  - Interference occurs if multiple nodes transmit simultaneously, leading to message loss.

- Transmission Error Detection:
  - Errors in message transmission need to be detected and corrected.
  - Error checking codes, such as checksums, are added to messages for verification at the receiving end.
- Layer Interaction:
  - Message received from higher layers is handed down to the data link layer.
  - Data link layer adds error checking codes and message markers before transmitting the message to the physical layer for transmission.
  - At the receiving end, the data link layer identifies message boundaries, verifies data integrity, and passes the message up to the network layer.
- Role in Protocol Stack:
  - Data link layer acts as an intermediary between the network and physical layers.
  - Prepares messages for physical transmission and ensures data integrity during transmission.
  - Examples of data link layer protocols include Ethernet, token ring, and HDLC.
- Future Considerations:
  - Chapter 8 will delve into specific data link layer protocols and their implementations, such as Ethernet, token ring, and HDLC.

2.7 Physical Layer (1)

- Physical Layer Functions:
  - Manages the physical connection between nodes.
  - Determines the transmission media (copper cable, optical fiber, radio waves, etc.).
  - Defines how bits are represented on the medium.
  - Considers physical network topology and connectivity.
- Additional Considerations:

        - Addresses signal attenuation and environmental interference (e.g., clouds, lightning).
        - Determines maximum transmission speeds.
        - Handles multiplexing of multiple logical channels onto a single physical medium.
        - Deals with interference from household equipment and other sources.
    - **Relevance to Computer Science Students:**
        - Many of these details have limited impact on typical Computer Science studies.
        - Chapter 9 will touch on physical layer topics, providing basic understanding without diving into extensive technical details.
    - **Example Topics:**
        - Transmission media types and characteristics (e.g., copper, fiber optics).
        - Encoding schemes for representing bits.
        - Physical network topologies (e.g., bus, star, mesh).
        - Signal propagation and attenuation.
        - Multiplexing techniques for efficient data transmission.
        - Interference mitigation strategies.

3 Messages, Packets, Frames, and Other Units of Data

- **Units of Data Transmission:**
    - **Message:** A general term for data to be transmitted but used infrequently in networking.
    - **Packet:** A unit of data transmission with a header and payload, used as a generic term across layers.
    - **Frame:** Specifically used in the data link layer, containing data link layer headers and payload.
    - **Datagram:** Used in the network layer, denoting packets in packet-switched networks like IP.
    - **Segment:** Used in the transport layer, representing segments of data with transport layer headers.

- **Characteristics of Data Units:**
  - Consist of a header and payload.
  - Header contains layer-specific information, while payload contains data from higher layers or to be delivered to higher layers.
  - Terminology may vary across layers and protocols but often follows similar patterns.
- **Example Scenario:**
  - A Web browser sends a request (e.g., HTTP GET) to a Web server.
  - Transport layer adds header with port numbers (source and destination).
  - Network layer adds header with source and destination addresses.
  - Data link layer adds header, checksum, and framing bits.
  - Frame is transmitted via physical layer.
  - At the destination, the process is reversed, with each layer handling its respective header and passing payload up the stack.
- **Key Concepts Illustrated:**
  1. Each layer communicates logically with its peer layer at the destination, adding and interpreting headers.
  2. Each layer communicates physically with the layers above and below, providing and utilizing services for transmission.

4 Standards

This section will eventually contain information about bodies that issue standards that are relevant for computer networking.

This will include:

- ISO, including the various national standards bodies
- IEEE

- IETF
- IANA (compare ZADNA, etc)
- ICANN
- W3C
- ITU-T / CCITT
- NIST (compare SANAS)

Summary

1. **Application Layer (Layer 7):**
   Provides interface for user applications, such as web browsers and email clients.
2. **Presentation Layer (Layer 6):**
   Handles data translation and encryption, ensuring data is in a readable format.
3. **Session Layer (Layer 5):**
   Manages sessions and dialogues between applications, establishing, maintaining, and terminating connections.
4. **Transport Layer (Layer 4):**
   Responsible for end-to-end communication between hosts, ensuring data delivery and reliability.
5. **Network Layer (Layer 3):**
   Handles routing and addressing, forwarding packets between different networks.
6. **Data Link Layer (Layer 2):**
   Controls data flow between adjacent network nodes, providing error detection and framing.
7. **Physical Layer (Layer 1):**
   Deals with physical transmission of data over the network medium, such as copper wires or fiber optics.
   Mnemonic:
   *A*ll
   *P*eople
   *S*eem
   *T*o
   *N*eed

*D*ata
*P*rocessing