Final Assessment | Fall - 2023

Md. Shafayet Hossain

CSE - 21st Batch | **Course Code:** CSE - 435

Course Title: Data Communication | **ID:** 2121210071

Answer to the Question no- 1

(a)

Protocols and standards play a crucial role in data communication by providing a set of rules and guidelines that enable different devices and systems to communicate effectively. They ensure that data is transmitted, received, and interpreted consistently across diverse networks and technologies. Here's a discussion on protocols and standards in data communication:

Protocols

Definition: A protocol is a set of rules governing how data is transmitted and received over a network. It defines the format, timing, sequencing, and error control of data during communication.

Types of Protocols:

- **Communication Protocols:** Specify how devices identify and establish communication with each other (e.g., TCP/IP, HTTP).
- **Network Protocols:** Define how data is routed between devices in a network (e.g., Routing Information Protocol - RIP, Open Shortest Path First - OSPF).
- **Transport Protocols:** Control the flow of data between devices (e.g., Transmission Control Protocol - TCP, User Datagram Protocol - UDP).
- **Application Protocols:** Facilitate specific applications' communication (e.g., Hypertext Transfer Protocol - HTTP, File Transfer Protocol - FTP).

Key Features-

- **Addressing:** Protocols determine how devices are identified and addressed on a network.
- **Error Handling:** Specifies how errors in data transmission are detected and corrected.
- **Flow Control:** Manages the pace of data transmission to prevent overload.
- **Data Compression:** Some protocols include mechanisms to compress data for efficient transmission.

Examples:

- **TCP/IP:** Widely used for internet communication.
- **HTTP/HTTPS (Hypertext Transfer Protocol/Secure):** Used for web browsing.
- **SMTP (Simple Mail Transfer Protocol):** Manages email transmission.
- **DNS (Domain Name System):** Resolves domain names to IP addresses.

Standards

Definition: Standards define a common set of rules and specifications to ensure compatibility and interoperability between different systems and devices.

Types of Standards:

- **De facto Standards:** Evolve organically through widespread use and acceptance (e.g., USB).
- **De jure Standards:** Established by formal bodies, such as international or national organizations (e.g., IEEE, ISO).

Importance:

- **Interoperability:** Standards enable devices from different manufacturers to work together seamlessly.
- **Scalability:** Facilitates the growth and expansion of networks without compatibility issues.
- **Reliability:** Ensures consistent and reliable performance across various devices and systems.

Examples:

- **ISO/OSI Model:** A conceptual framework that standardizes the functions of a communication system.
- **IEEE 802.11 (Wi-Fi):** Standard for wireless local area networking.
- **USB (Universal Serial Bus):** Standard for connecting and transferring data between devices.
- **TCP/IP Suite:** Standard for internet communication.

1(b)

Applications of coaxial cable

Coaxial cables, commonly known as coax cables, are widely used in various applications due to their unique construction and electrical properties. Here are some common applications of coaxial cables:

1. Cable Television (CATV)
2. Internet and Broadband Services
3. Telecommunications
4. Closed-Circuit Television (CCTV)
5. RF (Radio Frequency) Transmission
6. Satellite Communication
7. Medical Imaging
8. Automotive Industry
9. Aerospace and Defense
10. Test and Measurement Equipment

Disadvantages of Fiber Optic Cable

Fiber optic cables offer incredible speed and bandwidth, but they also come with some drawbacks to consider:

1. High cost
2. More fragile than copper wires
3. Complex Installation challenges
4. Signal attenuation
5. Limited power delivery
6. Equipment compatibility
7. Security concerns
8. Environmental factors

Remember, the disadvantages of fiber optic cables need to be weighed against their significant advantages, like high speeds, low interference, and long-distance capabilities. The best choice will depend on specific needs and budget.

1(c)

Here's a comparison of guided and unguided media across various aspects:

Feature	Guided Media	Unguided Media
Transmission method	Physical cables (e.g., copper, fiber optic)	Wireless signals (e.g., radio waves, microwaves)
Mobility	Limited, requires fixed cable connections	High, allows movement freely within coverage area
Cost	Generally cheaper	Generally more expensive, especially setup and infrastructure
Security	More secure, signals confined within cables	Less secure, susceptible to signal interception and interference
Speed	Can be very high, especially fiber optic	Generally slower than guided media, varies with distance and interference
Reliability	More reliable, less prone to interference	Less reliable, can be affected by weather, obstacles, and interference
Scalability	Can be easily scaled by adding more cables	Limited scalability, spectrum congestion can be an issue

Examples	Ethernet cables, coaxial cables, fiber optic cables	Wi-Fi, Bluetooth, radio, satellite
Suitable for	Fixed installations, high-speed data transfer, secure communication	Mobile devices, wide-area coverage, broadcasting

Additional points to consider:

- **Installation:** Guided media is generally easier to install, while unguided media requires setting up infrastructure like towers and antennas.
- **Maintenance:** Guided media requires less maintenance, while unguided media might need regular maintenance of infrastructure.
- **Environmental impact:** Both have some environmental impact, but guided media can be recycled, while unguided media depends on energy-intensive infrastructure.

Answer to the Question no- 2

(a)

Internetwork

An internetwork, also known as an internet, is a system of interconnected computer networks. These networks can be of different sizes and types, such as local area networks (LANs), wide area networks (WANs), and metropolitan area networks (MANs). They are connected by devices called routers, which direct data packets between the different networks.

The most famous example of an internetwork is the Internet, which is a global network of networks that connects billions of computers and devices around the world. The Internet uses a standardized set of communication protocols called the Internet Protocol Suite (TCP/IP) to ensure that all devices can communicate with each other.

2(b)

Both wireless WAN and wireless LAN are technologies for connecting devices, but they differ in terms of scale, purpose, and technology:

Wireless LAN (WLAN):

- **What it is:** A network that connects devices within a limited area, such as a home, office, or school.
- **Range:** Typically covers tens to hundreds of meters.
- **Technology:** Uses radio waves (like Wi-Fi) to transmit data between devices and access point.
- **Purpose:** Allows devices to share resources like files, printers, and internet access.
- **Examples:** Your home Wi-Fi network, the Wi-Fi at a coffee shop.

Wireless WAN (WWAN):

- **What it is:** A network that connects devices across a wider geographic area, such as a city, country, or even the globe.
- **Range:** Can span long distances, depending on the technology used.
- **Technology:** Uses cellular networks (like 4G or 5G) or satellite connections to transmit data.
- **Purpose:** Provides internet access to mobile devices like smart phones and laptops when they're outside the range of a WLAN.
- **Examples:** The cellular network your phone uses to connect to the internet, satellite internet.

Answer to the Question no- 3

(a)

Implicit Congestion Signaling Explained

In network communication, congestion occurs when there's more data trying to flow through a network element than it can handle. Implicit congestion signaling is a method where senders (like your computer) infer the presence of congestion by observing how the network responds to their data packets, without receiving any explicit messages from network equipment. It's like playing detective, gathering clues to understand the traffic conditions.

Here are some common ways senders detect congestion implicitly:

- Increased delay: If it takes longer than usual for acknowledgments to arrive, it could indicate slowdowns due to congestion.
- Packet loss: When packets go missing, it might be because routers are discarding them to manage overload.
- Duplicated acknowledgments: This can happen if packets are reordered in the network due to congestion, causing confusion on the receiving end.
- Changes in sending rate: If a sender experiences frequent timeouts or slow response times, it might adjust its sending rate to avoid further problems, implying potential congestion.

Benefits of implicit signaling:

- Simpler network implementation: No need for additional messages or mechanisms in network devices.
- Adaptable to various network conditions: Senders can react dynamically to changing traffic patterns.
- Robust to partial failures: Even if some parts of the network are not functioning, senders can still adapt.

Examples of protocols using implicit signaling:

- TCP (Transmission Control Protocol): The most widely used transport protocol relies on timeouts, duplicate acknowledgments, and congestion windows to adjust its sending rate based on network feedback.
- HTTP (Hypertext Transfer Protocol): This protocol uses keep-alive connections and timeouts to manage congestion while fetching web content.

3(b)

The OSI Model: A Layered Approach to Network Communication

The Open Systems Interconnection (OSI) model is a conceptual framework that describes the seven layers involved in network communication. It serves as a universal language for understanding how data travels from one device to another, even if those devices use different hardware and software.

Here's a breakdown of each layer, starting from the bottom:

1. Physical Layer:

- Deals with the physical transmission of data bits over a network medium like cables or fiber optics.
- Handles tasks like sending and receiving electrical or optical signals, defining cable types, and managing connectors.
- Protocols: Ethernet, Token Ring, Wi-Fi.

2. Data Link Layer:

- Focuses on reliable data transmission between two directly connected devices.
- Ensures error-free delivery by adding error detection and correction codes.
- Manages Media Access Control (MAC) addresses for device identification.
- Protocols: Ethernet II, PPP, HDLC.

3. Network Layer:

- Responsible for routing data packets across networks, finding the best path to the destination.
- Uses logical addresses (IP addresses) to identify devices on different networks.
- Performs functions like packet forwarding, congestion control, and network address translation (NAT).
- Protocols: IP, ICMP, BGP.

4. Transport Layer:

- Provides reliable data transfer between applications on different devices.
- Breaks down messages into smaller packets, ensures in-order delivery, and manages flow control.
- Offers two main services: connection-oriented (TCP) and connectionless (UDP).
- Protocols: TCP, UDP.

5. Session Layer:

- Establishes, manages, and terminates sessions between applications.
- Handles tasks like authentication, authorization, synchronization, and error recovery.
- Less commonly used in modern networks, often combined with Presentation layer.
- Protocols: RPC, NetBIOS.

6. Presentation Layer:

- Deals with data format and representation, ensuring compatibility between different systems.
- Performs tasks like encryption, decryption, compression, and character set conversion.
- Often combined with Session layer in practice.
- Protocols: MIME, SSL/TLS, ASCII, EBCDIC.

7. Application Layer:

- Provides network services to user applications like web browsing, email, file transfer, and multimedia streaming.
- Directly interacts with users and applications.
- Examples: HTTP, FTP, SMTP, DNS.

Key Points:

- Each layer performs specific functions and communicates with its peer layer on the other device using protocols.
- The model is hierarchical, with each layer relying on the services provided by the layer below.
- While the OSI model provides a theoretical framework, the actual protocols used in real-world networks often combine functions from multiple layers (e.g., TCP/IP model has 4 layers).

3(c)

Analog vs. Digital Signals: A Detailed Comparison

The world around us is full of signals, carrying information in various ways. Two fundamental types are analog and digital signals, which differ in their representation and behavior. Here's a breakdown of their key characteristics:

Representation:

- **Analog:** Continuous variations in a physical quantity (e.g., voltage, pressure, sound wave) directly represent the information. Imagine a smooth, flowing curve.
- **Digital:** Discrete steps or levels represent information using a limited set of values, typically binary (0s and 1s). Think of a square wave with sharp transitions.

Data Values:

- **Analog:** Uses a continuous range of values to represent information, offering high precision and accuracy.
- **Digital:** Limited to discrete values (0 or 1), potentially losing some information during conversion from analog to digital (quantization).

Susceptibility to Noise:

- **Analog:** More susceptible to noise and interference, as even small changes in the signal can alter the information it carries.
- **Digital:** Less susceptible to noise, as changes smaller than a certain threshold won't affect the interpreted value (0 or 1).

Transmission and Storage:

- **Analog:** Transmission can be affected by distance and noise, potentially degrading the signal. Storage requires precise analog-to-digital conversion for accurate representation.
- **Digital:** Transmission is less prone to degradation due to noise immunity. Storage is efficient and reliable due to discrete values.

Examples:

- **Analog:** Temperature readings, sound waves, radio signals (AM/FM), vinyl records
- **Digital:** Computer data, CDs/DVDs, MP3 files, digital images, internet data

Additional Points:

- Digital signals can be easily manipulated and processed by computers.
- Analog signals often require specialized analog-to-digital converters (ADCs) for processing with digital devices.

The choice between analog and digital depends on specific requirements like accuracy, noise sensitivity, and processing needs.