“Module 6: Assignment 2 - Ethernet and TCP/IP Networking”

Harsh Siddhapura

“Dr. Dinesh Sthapit”

“October 17, 2023”

1. A framework that describes how two endpoints or hosts interact with one another is known as a communication model. Its goal is to offer a dependable and effective way to deliver communications. In this architecture, applications or services exchange messages or groups of messages between sender and receiver nodes.

   The communication model is implemented layer by layer. Throughout the connection process, each layer of the transmitting group sends data to the receiving node. Layers are used in systematic systems, with each layer being responsible for certain tasks and interacting with the layers above and below it. This keeps tasks distinct and ensures that each layer has sole control over how those in layers above and below interact.

   TCP/IP standards were independently developed to satisfy the requirements of Internet standards and improve their usability. It is consistently changed to meet evolving needs. The use of several systems that cooperate to provide network connectivity is required for the application of this standard. As long as the intersection of each layer is established, the functions of each layer may be separated and used independently.

   Each set of data reports contains data that the connection procedure's receiver can utilize. "This approach enables independent actions by guaranteeing that each layer solely controls the interfaces above and below it."As long as the connection is good, the functioning of one layer will be transparent to the other layers." The theoretical underpinning of the process or the communication between two endpoints is explained by the communication model. “Its goal is to offer a dependable and effective way to deliver communications. In this architecture, applications or services exchange messages or groups of messages between sender and receiver nodes” (Wiley, 2020, p. 430).

2. Advantages of implementing different protocols for different aspects of communication:
   - Flexibility and modularity: Since various types of communication employ various systems, communication design must be flexible and adaptable. Each process can be designed to

control a certain activity or function in a way that makes changes simple or that doesn't interfere with other communications.

- Efficiency and effectiveness: Different methods could be better suited for particular tasks, leading to quicker and more effective communication. Data transport, for instance, may be enabled by systems created for error detection and correction, whilst path analysis systems may enhance packing efficiency.
- Knowledge and Customization: Communications can be changed to meet certain requirements. For instance, the system may be set up to handle a variety of data kinds, including text, audio, and video, and it functions well in all formats.
- Keeping track of different systems can help ensure interoperability and compatibility across different systems and pieces of equipment. The conventional method ensures that various products may interact well, regardless of how specifically they were made or for what purpose.
- Extensibility and extensibility: By using distinct rules for various forms of communication, the system's scalability may be guaranteed. "New policies can be added or existing systems modified to adapt to changing needs or technological advances without disrupting all communications" (Wiley, 2020, p. 399).

3. The TCP/IP protocol suite consists of five layers: the application layer, transport layer, network layer, data link layer, and physical layer. Each layer has its own specific function in the communication process.
    - Delivering network services to user applications is the responsibility of the application layer. It is capable of online browsing, file transfers, email, and troubleshooting. It also supports the HTTP, FTP, SMTP, and DNS protocols.
    - The means of communication between hosts is known as transmission. Utilizing protocols like TCP (Transmission Control Protocol) and UDP (User Data Packet Protocol), it creates connections, controls data fragmentation, and offers error and recovery.

- The placement and distribution of data packets are handled by the network layer, sometimes referred to as the IP layer or the network layer. IP (Internet Protocol) is used to transmit data packets from one media source to another.
- The reliability of data via physical links is at the control of the data link layer. It includes tools for recognising Ethernet networks and network devices, like MAC (Media Access Control) addresses, as well as techniques for finding and fixing errors.
- Object layer: The original data is transported over the network by the entity layer. Examples of physical output include copper wire or fiber optic output. The term stands for "electrical, technological, and physical connection" (Wiley, 2020, p. 430).

4. The layer of the communication model that comprises communication is called the physical layer. It is in charge of controlling how information is sent from one place to another. The organizational system, which consists of the media, the signaling process, the specific signals, synchronization and timing problems, and the computer-to-media communication process, determines the access method to the space.

   The only components in physical systems are the network connections. Network interface controllers produce the voltages, light pulses, radio waves, clock and synchronization signals, and other physical signals needed for communications. It is in charge of using the medium to send and receive small streams. Each method has its own protocol, including twisted pair, cable service, Wi-Fi, and fiber optics. "The physical process defines the frequency of the carrier signal, data modulation and demodulation technology, bandwidth, transmission signal strength in different conditions, etc" (Wiley, 2020, p. 434).

5. The responsibility for assuring the trustworthy transmission and delivery of packets via a communication link between two nodes falls on the Data Link Layer. It is divided into two sublayers:

the software logical link control (LLC) sublayer and the hardware medium-access control (MAC) sublayer.

The LLC sublayer manages IP packet/frame conversions, retransmission, and packet reconstruction as well as traffic flow control, error correction, and these functions as needed. It counts and reorders frames to recover the original message if required and "provides appropriate error detection for each frame and allows for the request and retransmission of a frame that has not been successfully received" (Wiley, 2020, p. 435).

The task of assuring ordered access to the physical media falls to the MAC sublayer. It describes how to use the channel and spot problems. It encrypts data in the appropriate physical layer format, routes data to its intended location, finds errors, and avoids collisions. Multiple protocols and frame headers are defined for different physical media and signaling systems.

6. There are various parts that make up an Ethernet frame. Let's first go over what involves time synchronization between the sender and the receiver. Following that is the start frame delimiter, which marks the start of the frame's content. The frame contains both the address and the field designated as the MAC address. The data in the frame, the data fields themselves, and an error check known as cyclic redundancy check (CRC) are all detailed in a large file. The data field can be padded to a minimum size of 46 bytes and a maximum value of 1500 bytes.

   All nodes in hub-based Ethernet networks are connected to a single hub, utilizing a bus architecture. Any node in this configuration can utilize the bus to send messages to other nodes while it is not in use. Collisions might happen when several nodes try to communicate data at once, lowering performance.

   On the other hand, switched Ethernet uses a star topology, where each link is connected to a central switch. This switch creates a direct connection between nodes, removing conflicts and enabling

several pairs of nodes to communicate simultaneously. Full-duplex mode, which permits each pair of connections to operate at the network's maximum data rate, is another feature of switched Ethernet.

Switched Ethernet is the best option for faster, longer connections since it provides better performance and doesn't require a network connection. the hub-based Ethernet networks' use of the CSMA/CD protocol. "Hub-based Ethernet is more efficient and suitable for connecting light traffic, but as traffic increases and there are more conflicts, it will not be more valuable" (Wiley, 2020, p. 436).

7. Wi-Fi operates in infrastructure mode as shared content. All wireless stations depend on access points for communication. Since this area resembles a hub, collisions are inevitable. Two collisions, one mandatory and one optional, are shown in the model. Contrarily, locating conflicts in wireless networks is more difficult and effective than locating conflicts in wired networks. Some stations are ignorant of the conflict due to hidden networks and outside occurrences. Furthermore, the frame will be transmitted all the way through even if a collision occurs as the sender starts transmitting it. This occurs as a result of the supplied signal's greater strength than the receiver's, which causes continual listening. Therefore, collision delays in wireless networks are greater than in wired hubs.

   Based on a partial mesh network architecture, ad-hoc WiFi anticipates direct connections between Wi-Fi stations. However, because “self-provisioning Wi-Fi is reliant on the network of accessible locations, it is rarely used. Each Wi-Fi node can connect to the others in this mode without a base station” (Wiley, 2020, p. 437).

8. From their point of origin to their point of destination, packets must be routed and sent by the network layer. By employing logical IP addresses, it recognises and locates network services. The network layer employs data connections and other techniques to move data between nodes.

An essential network layer function is routing. It comprises determining the best route for a packet to take in order to reach each destination. The network layer deletes the current address and builds the next address at each intermediate step by using tables and other methods. The packet travels through this procedure again and again until it reaches its destination.

The Internet protocol uses logical IP addresses to find and identify network services. A device connected to the Internet is assigned a specific number called an IP address. "By assigning a unique address to each device, they ensure that data packets are sent to the correct destination." To send data and text from one device to another, IP and physical addresses are utilised.From their point of origin to their point of destination, packets must be routed and sent by the network layer. By “employing logical IP addresses, it recognises and locates network services. The network layer employs data connections and other techniques to move data between nodes” (Wiley, 2020, p. 439).

9. In a local area network, messages are sent from one site to another by the network layer. The network method throws away the previous node's physical address and uses tables and algorithms to create the address for the subsequent node. To establish a connection between nodes, the new address is added to the packet before it is sent to the data link layer. There is no need for routing because every node in the local network is directly linked, allowing packets to be addressed.

   The network layer is in charge of transporting messages from source to receiver via routers when they are transported over a network that is larger than the local one (such as the Internet). At each intermediate node, the network layer deletes the current physical address and creates an address for the following node. "Numerous tables and algorithms are used to provide routing. Before the packet is sent to the data link layer, additional addresses are added to it to ensure the connection between the nodes. Until the data packet reaches its destination, this process is repeated” (Wiley, 2020, p. 439).

10. The IP protocol manages networks and routing. It recognises network services and uses IP addresses to route packets from one location to another. Before sending a packet, IP must use Address Resolution Protocol (ARP) to ascertain the destination address. ARP is used by the network layer to translate an IP address into a physical address.

    The IP address is the foundation of the IP protocol's routing. ARP is used by IP to find the related address after detecting the IP address of the address. Every node on the local network receives an advertisement packet from ARP that contains an IP address. The appropriate node responds with its address, which in the case of Ethernet is its MAC address. Up till the ultimate point is achieved, this process is repeated.

    ARP is used in the IP protocol to resolve addresses. ARP is used by IP in order to ascertain a given address's physical address. ARP maintains a cache of frequently used IP address-address pairs to make this process simpler. The relevant node responds with its address, which is sent to the data link layer in a frame, when ARP meets an unknown IP address by sending a message containing the IP address to all nodes on the local network" (Wiley, 2020, p. 442).

11. The Internet Control Message Protocol (ICMP) is essential for producing error messages in the case of a network breakdown. When a network service breaks down or malfunctions, ICMP sends error messages that are contained in new IP records. The IP address receives this message back. Numerous types of failures are described by ICMP error messages, including "Unknown destination host" and "[IP data packet] lifetime exceeded." "ICMP is also used to query and is used by network tools such as ping and Traceroute to provide information about network connectivity and communications." (Wiley, 2020, p. 440).

12. The task of providing end-to-end communication services falls under the purview of the transportation system. It carries out a number of tasks and offers a range of services to make sure that information is transmitted across communication channels.

    Connecting the site base and the site region is one of the transportation system's main duties. The technique known as connection-oriented servicing is used to achieve this. Before sending data packets, TCP and other transport protocols establish connections by exchanging unique control packets. Data may now move more quickly and securely thanks to this link.

    Flow control is yet another important service provided by the transport layer. It ensures that information is transmitted in the safest way possible while also prohibiting the recipient from keeping the information private. The loading process controls the data flow by employing strategies including buffering, congestion management, and windows. This process maintains equilibrium between the transmitter and receiver and permits efficient data transmission.

    Data transmission is ensured by the transfer method. offers a system for recovering from errors so that gearbox problems may be found and fixed. "TCP uses acknowledgment messages to identify that each packet has been received and accepted," as an instance. In order to ensure effective delivery, TCP retransmits a packet if it is rejected" (Wiley, 2020, p. 443).

13. A port number, sometimes referred to as a port number, serves to identify the installation process. The first 1024 of these 16-bit numbers are said to represent well-known ports. These well-known ports are the default addresses for the majority of software. For example, Web services commonly utilize port 80.

    To create connections and send messages over the network, transport activities employ ports. When an application requests service over TCP, UDP, or SCTP, an IP address and port must be specified. In order to determine which application sent the message and which application would want to receive it, the transport mechanism then makes use of these ports.

The application has the ability to change the port number, and it may do so by using the user's port number. In order to identify certain network programmes or to assign different ports to distinct applications, such as hiding a web server by using a port number other than the standard port 80, a user-defined port number can be used. "Sockets connect the application and transport layers, allowing applications to establish connections and send messages across the network. The port number and IP address, the port number and IP address, and the port number and IP address are the four pieces of information that make up a socket" (Wiley, 2020, p. 444).

14. The addressing scheme used in IPv4 consists of network addresses, subnets, and hosts:
    - Network addresses: IPv4 addresses come in three categories. The network to which the device belongs is indicated by the network address at the top level. Traffic is routed via it.
    - Subnet: An IPv4 address's remaining space is divided up into subnetworks or subnetworks. There may be a number of hosts or nodes in each subnet. Masks are used to identify certain objects and distinguish between different locations.
    - A network-connected device is referred to as a host. They are all assigned unique IP addresses within the network.

    The addressing scheme allows for "efficient allocation of IP addresses and helps in routing and communication within the network" (Wiley, 2020, p. 448).

15. A better way to allocate IP addresses is using NAT. It makes it possible for small enterprises without internet access to set up their network behind a router and use IP addresses. Although these private IP numbers cannot be used online, they can assist you in hiding computers from the web and lowering the overall number of IP addresses in your company. Routers that support NAT use the router's IP address rather than a private address to redirect messages from other networks to the Internet.

Using DHCP is another way to assign a good IP address. In a short amount of time, it allows for the dynamic allocation of IP addresses. The DHCP client sends out a request to find the DHCP server when a computer joins a network. A lease that includes an IP address and other information is returned by the DHCP server. Large organizations and DSL/cable service providers frequently utilize DHCP to assign IP addresses to connected PCs. This technique helps to maximize the use of available IP addresses.

Therefore, "NAT and DHCP provide an efficient way to assign IP addresses, ensuring that anyone who needs access can obtain an address while maintaining good address quality" (Wiley, 2020, p. 450).

16. IPv6 was created to address the problem of running out of available IP addresses in IPv4. It offers several features and advantages over IPv4, including:
    - A 128-bit IPv6 address can include up to 256 trillion different IP addresses. Future expansion has plenty of room thanks to this.
    - A comma separates each eight-digit hexadecimal string that makes up an IPv6 address. The use of this notation, sometimes referred to as colon hexadecimal notation, simplifies the addressing method.
    - Two groups of colons can represent groups of colons that are entirely zero thanks to IPv6's capability for truncating zeros in colons. bowel. These abbreviations make it easier to comprehend IPv6 addresses.
    - IPv6 validates the idea of different levels, enabling issues to be handled as circumstances change and advance.

    IPv6 offers several advantages over IPv4, including:

    - More address space: IPv6 address space is increased to ensure that there is enough address space for all devices, even as the number of devices increases.

- IPv6 makes routing easier by reducing the need for packet segmentation and fragmentation. There should be less complexity in IP data packets. Thus, network performance is improved and accelerated.
- Support for new features: “IPv6 includes clauses that recognise the value of multimedia streams while also adding new features that enhance TCP/IP capabilities in the current context“ (Wiley, 2020, p. 451).

17. An exclusive identification for online transactions is a domain name. They provide yet another way to memorize the IP address. Using DNS, it is possible to convert TCP/IP network names into IP addresses. It uses a decentralized data structure based on the server directory system to obtain the necessary information. "Each database entry has a domain name and an IP address. “Because it offers a translation between domain names and IP addresses, DNS is essential for enabling network connections” (Wiley, 2020, p. 451).

18. QoS refers to a network's ability to provide different services to diverse traffic or application types. It is designed to ensure that crucial or time-sensitive data (such streaming media or instant messaging) is delivered with the least amount of lag, errors, and packet loss.

    Because it guarantees a defined level of performance and reliability for an application or service, QoS is crucial in networking. By prioritizing and managing network connections, QoS ensures timely and reliable data transmission even when networks are overcrowded or resources are few.

    The two most critical QoS criteria are throughput and latency. In contrast to latency, which is the time it takes for a data packet to move from one location to another, throughput is the amount of data that can be carried across a network in a given amount of time. By maximizing these attributes, QoS may improve the user experience for apps that need fast, low-latency, error-free data delivery.

In actuality, service quality, processing priorities, traffic generation, and so on. It is used in several concepts, including and resource reserve. "This technology allows network administrators to allocate network resources according to the specific needs of different applications or services, ensuring that critical data has the necessary bandwidth and priority" (Wiley, 2020, p. 456).

19. Categories of Network Security are as follows:

- Anti-Corruption: This category concentrates on strengthening the network and services of the system. It provides defenses against unauthorized access, tampering with system files, infiltration, and other dangerous behaviors. Firewalls, password encryption, and physical and circuit protection are all essential preventative measures.
- Privacy is characterized as the confidentiality of information and communication. Internet data privacy is protected via encryption. Data encryption guarantees that unauthorized people cannot access or understand the data.
- Authentication: Authentication is the process of verifying the identity of the person receiving the information. It guarantees that the data comes from a reliable source. Special cryptographic qualities akin to electronic signatures are employed for authentication.
- Information accuracy and non-repudiation: This category seeks to preserve the accuracy of communication data and pinpoint the message's origin. Special encryption qualities are necessary to maintain data integrity and non-repudiation, which implies that the data cannot be altered and the message's history may be determined.
- Limiting authorized users' access to network resources and turning on network resources are both topics covered under the issue of access management and network availability. "Use measures such as physical and logical access restrictions, firewalls, and encryption to control access and maintain network availability" (Wiley, 2020, p. 458).

These categories of network security measures are essential for designing a secure network infrastructure and protecting against various threats and vulnerabilities.

20. Network Security measures are as follows:

- Only those with the proper authorization can access the network cable and other devices. As a result, there is less physical eavesdropping on the local area network. Accessibility is constrained by smart electronics that block user access when it is not necessary and by powerful application networks that attack or reject incoming packets. Private networks are used to make it more difficult for hackers to determine the computer behind the firewall or router.
- An example of an access restriction is a firewall, which limits access to networks and systems. Intelligent design includes characteristics like blocking or disguising IP addresses of local and computer networks on the Internet, examining all packets for authentication, and prohibiting or blocking unnecessary port numbers.
- The act of reading the data contained in a packet as it moves through the network is known as packet sniffing. Software programmes called packet sniffers gather and examine network communication. They can be used maliciously to compromise important data, even if they may be used lawfully for things like network troubleshooting. Attacks on packet sniffing can be thwarted with the use of encryption and security protocols.
- In addition to additional security measures, encryption is utilized. It helps with the avoidance of unauthorized access, the maintenance of data integrity and non-repudiation, the protection of privacy, and the identification of users. "Mixed key encryption and public private key encryption are two types of encryption algorithms" (Wiley, 2020, p. 458).

21. The OSI (Open Systems Interconnection) model and the TCP/IP model are two different approaches to network protocol standards. While they share some similarities, there are also notable differences in their layer structures.

    OSI Model:

- The seven tiers of the OSI model are the transport layer, presentation layer, layer layer, layer layer, and layer layer.
- Each layer has particular responsibilities and performs certain tasks.
- The standard, which was developed by the International Standards Organisation (ISO), is intended to be a process protocol.
- For assessing the circumstances related to various types of communication and contrasting the performance of various systems, the OSI model is a crucial idea.

TCP/IP Model:

- Particularly in the context of the Internet, TCP/IP is the most popular and commonly used standard.
- Network interface, Internet, transportation, and application make up its four levels.
- TCP/IP is an independently created standard that is frequently updated to meet the requirements of the Internet standard.
- refers to the TCP/IP protocol suite and Ethernet-based communications as a choice for numerous configurations.

Differences:

- The TCP/IP design only comprises four layers, compared to the seven in the OSI paradigm.
- The OSI model includes functions like communication and representation that are absent from the TCP/IP paradigm. These layers are in charge of tasks including creating and managing distributed applications, moving data, and translating.
- Functions from the protocol and presentation layers are included into the application layer via the TCP/IP standard.
- The relationship between the physical layer and the data link layer of the OSI model is represented by the network interface layer/IP model of TCP.
- The network layer of the OSI model is equivalent to the Internet layer.

- The application layer is made up of "all communication layers, presentation layers, and application layers of the OSI model" (Wiley, 2020, p. 460).

22. It is the responsibility of the OSI protocol layer to establish, manage, and end communications between various nodes' applications or processes. It controls communication among different software to provide effective access and data flow. To ensure proper access to the remote printer and data flow control, it will be utilized, for instance, for network printing and remote access activities.

    Different systems can communicate with one another thanks to the data translation and transfer services provided by the OSI presentation layer. The main objective of this layer is to display data on the site with equivalent meaning and location. It comprises data compression, encryption, data conversion, and ASCII-Unicode conversion" (Wiley, 2020, p. 430).

23. SCSI over IP is an application that converts SCSI bus protocol messages into messages that may be delivered over a TCP/IP network via a computer interface. Hard discs and other SCSI devices can now be used from any location on the network that is reachable from the default location. The message is converted back to SCSI format via a connection on the SCSI device.

    Smartphones, car dashboard systems, and tablets all employ cellular technology to connect to the Internet and offer information and services. "Mobile phones use a variety of standards, including CDMA, HSPA+, GSM, and LTE (also known as 4G)." Now, 4G LTE is giving way to 5G technology, which offers faster speeds, lower latency, and improved data transfer rates" (Wiley, 2020, p. 461).

24. A network protocol called MPLS (Multiprotocol Label Switching) adds labels and enables routers to transport them more efficiently. In order to streamline routing and boost performance, it works at the

network and data link layers. MPLS, also known as the Layer 2.5 protocol, is mostly used for virtual passageways.

Two protocols, SONET and SDH, collaborate to offer high-speed, long-distance communication via optical fiber. By employing multiplexing and synced world clocks, they maximize packet speed. Other protocols can use SONET/SDH as a physical protocol, usually across great distances.

Frame Relay, a slower WAN protocol, is nevertheless extensively used for the Internet and low-cost on-ramp WANs. “It uses its own switches to send frames over virtual circuits over data links and layers. The usage of permanent virtual devices on the same channel for ground and ground packets is made easier by frame relay” (Wiley, 2020, p. 462).

References

Irv Englander. (2020). *ARCHITECTURE OF COMPUTER HARDWARE, SYSTEMS SOFTWARE, AND NETWORKING : an information... technology approach.* John Wiley.