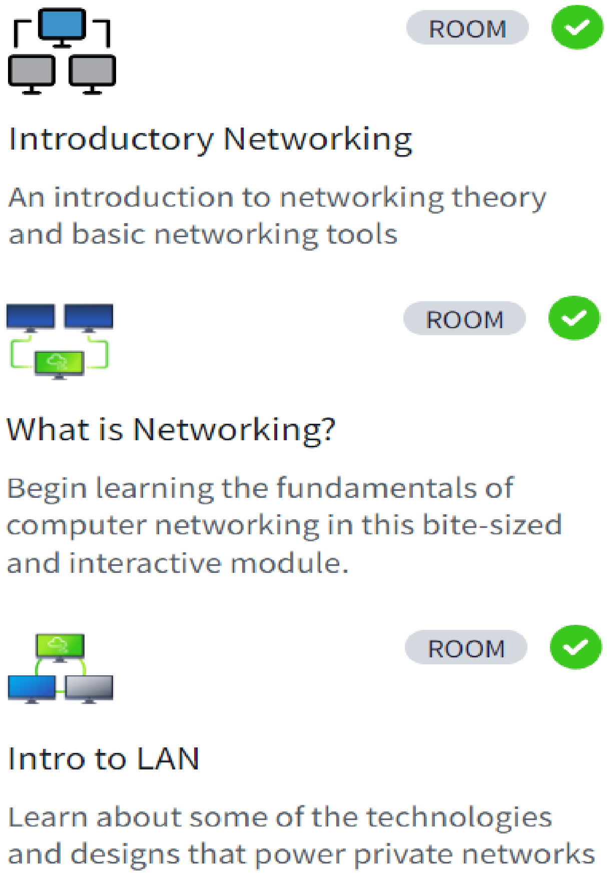
Task 3 :



ROOM ✓

Introductory Networking

An introduction to networking theory and basic networking tools

ROOM ✓

What is Networking?

Begin learning the fundamentals of computer networking in this bite-sized and interactive module.

ROOM ✓

Intro to LAN

Learn about some of the technologies and designs that power private networks

The OSI model : an Overview

The Open Systems Interconnection (OSI) Model is a conceptual framework used to understand and standardize the functions of a telecommunication or computing system. It divides network communication into seven distinct layers, each with specific responsibilities.

Layers of the OSI Model

1. Physical Layer (Layer 1) :
   - Function : Manages the physical connection between devices, including the transmission and reception of raw bit streams over a physical medium.
   - Examples : Cables, switches, and network interface cards (NICs).

2. Data Link Layer (Layer 2) :
    - Function : Provides node-to-node data transfer and handles error detection and correction from the physical layer. It ensures data is correctly framed and delivered to the correct device on a LAN.
    - Examples : Ethernet, Wi-Fi, MAC addresses.
3. Network Layer (Layer 3) :
    - Function : Manages data routing, packet forwarding, and logical addressing. It determines the best path for data to travel across networks.
    - Examples: IP (Internet Protocol), routers.
4. Transport Layer (Layer 4) :
    - Function : Ensures reliable data transfer between end systems, providing error checking, data flow control, and retransmission of lost data.
    - Examples : TCP (Transmission Control Protocol), UDP (User Datagram Protocol).
5. Session Layer (Layer 5) :
    - Function : Manages and controls the connections (sessions) between computers, including establishing, maintaining, and terminating sessions.
    - Examples : NetBIOS, RPC (Remote Procedure Call).
6. Presentation Layer (Layer 6) :
    - Function : Translates data between the application layer and the network format. It handles data encryption, compression, and translation.
    - Examples : SSL/TLS (Secure Sockets Layer / Transport Layer Security), data format conversion (e.g., JPEG, MPEG).

7. Application Layer (Layer 7) :
    - Function : Provides network services directly to end-user applications, enabling user interaction with the network.
    - Examples : HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), DNS (Domain Name System).

Encapsulation

Encapsulation is a key concept in networking where data is wrapped with the necessary protocol information at each layer of the OSI model before it is transmitted over the network. This process ensures that data is properly formatted for transmission and can be correctly interpreted by the receiving system. Here's a step-by-step explanation of the encapsulation process as data travels from the application layer to the physical layer :

Application Layer (Layer 7) :

- Data : User data is generated by an application (e.g., web browser, email client).
- Process : The data is prepared for transmission. Protocols like HTTP, FTP, or SMTP add application-specific headers to the data.
- Output : Application data with headers.

Presentation Layer (Layer 6) :

- Data : The application data is converted into a format suitable for transmission (e.g., encryption, compression).
- Process : The layer may apply transformations like encryption (e.g., SSL/TLS) or data compression.
- Output : Formatted data with presentation headers.

Session Layer (Layer 5) :

- Data : The formatted data is prepared for session management.
- Process : Establishes, maintains, and terminates sessions. Adds session-specific information like session IDs.
- Output : Data with session headers.

Transport Layer (Layer 4) :

- Data : The session data is segmented for transmission.
- Process : Adds transport layer headers (e.g., TCP or UDP headers) that include source and destination port numbers, sequence numbers, and error-checking information.
- Output : Segments (for TCP) or datagrams (for UDP).

Network Layer (Layer 3) :

- Data : The transport layer segments are prepared for routing.
- Process : Adds network layer headers (e.g., IP headers) containing source and destination IP addresses.
- Output : Packets.

Data Link Layer (Layer 2) :

- Data : The network layer packets are framed for physical network transmission.
- Process : Adds data link layer headers and trailers (e.g., MAC addresses, frame check sequences). This layer handles physical addressing and error detection.
- Output : Frames.

Physical Layer (Layer 1) :

- Data : The frames are converted to signals for transmission over the physical medium.
- Process : Encodes the frames into bits and transmits them as electrical, optical, or radio signals through the network medium (e.g., cables, wireless).
- Output : Bits transmitted as signals over the physical medium.

TCP/IP Model Overview

The TCP/IP Model (Transmission Control Protocol/Internet Protocol) is a conceptual framework used to understand and implement standard protocols for network communication. It is simpler than the OSI model, consisting of four layers that correspond to specific functionalities in data transmission.

Layers of the TCP/IP Model

1) Link Layer :
    - Function: Handles the physical and logical link control, managing the hardware addresses and the physical transmission of data.
    - Protocols : Ethernet, Wi-Fi (IEEE 802.11), ARP (Address Resolution Protocol).
    - Corresponding OSI Layers : Physical Layer and Data Link Layer.
2) Internet Layer :
    - Function : Manages logical addressing, routing, and the packaging of data into packets. It determines the best path for data to travel across networks.

    - Protocols : IP (Internet Protocol), ICMP (Internet Control Message Protocol), IGMP (Internet Group Management Protocol).
    - Corresponding OSI Layer : Network Layer.

3) Transport Layer :
    - Function : Ensures reliable data transfer between end systems, providing end-to-end communication, error checking, data flow control, and retransmission of lost data.
    - Protocols : TCP (Transmission Control Protocol), UDP (User Datagram Protocol).
    - Corresponding OSI Layer : Transport Layer.
4) Application Layer :
    - Function : Provides network services directly to user applications, enabling user interaction with the network.
    - Protocols : HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), DNS (Domain Name System), POP3, IMAP.
    - Corresponding OSI Layers : Session Layer, Presentation Layer, and Application Layer.

Comparison with OSI Model

- Simplicity : The TCP/IP model has four layers compared to the OSI model's seven, making it less complex and more widely implemented.
- Real-World Application : The TCP/IP model is the foundation of the internet and most modern networking.

Ping

Ping is a network utility used to test the reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer. It is one of the most basic tools for diagnosing connectivity issues.

Syntax : ping <IP address>

Eg : ping www.google.com

Traceroute

Traceroute is a network diagnostic tool used to track the path that an IP packet follows from the source to a specified destination. It provides valuable insights into the routing of data across networks, helping identify where delays or packet loss may occur.

Windows : tracert <IP address>

Eg : tracert google.com

Linux/Unix : traceroute <IP address>

Eg : traceroute google.com

WHOIS

WHOIS is a protocol and system used to query databases that store information about registered domain names and IP address allocations. It provides details about the registrant, registrar, and other pertinent information associated with domain names and IP addresses.

Web Interface : Many websites and tools offer web-based WHOIS lookup services where users input domain names or IP addresses.

Command-Line Tool : On Unix/Linux systems, WHOIS can be accessed using the whois command followed by the domain name or IP address.

Eg : whois google.com

DIG

Dig (Domain Information Groper) is a command-line tool used for querying DNS (Domain Name System) servers to retrieve DNS records for a specified domain name. It is widely used in network diagnostics and troubleshooting to gather information about DNS configurations and resolve domain-related issues.

Syntax : dig <domain name> [<type>]

Eg : dig google.com

Query types : Specifying query types like A, AAAA, MX, TXT, etc., retrieves specific types of DNS records.

Networking

Networking refers to the practice of connecting computers, devices, and other entities to share resources and information. It enables communication and data exchange between different systems and users, whether they are located in the same physical location or across the globe. The primary goal of networking is to facilitate efficient and effective communication, resource sharing, and collaboration among interconnected devices.

Internet

The Internet is a global network of interconnected computers and devices that use standardized communication protocols to exchange information and data. It is a vast network infrastructure that connects millions of private, public, academic, business, and government networks worldwide.

Identify devices on a network

IP Address (Internet Protocol Address) :

- Function : IP addresses are numerical identifiers assigned to devices (computers, smartphones, printers, etc.) connected to a network using the Internet Protocol (IP).
- Uniqueness : Each device on a network has a unique IP address, which serves as its identifier for communication.
- Types :
  - IPv4 : 32-bit address (e.g., 192.168.1.1).
  - IPv6 : 128-bit address

    (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
- Eg : Used for network communication, domain name resolution (DNS), and network management.

MAC Address (Media Access Control Address) :

- Function : MAC addresses are unique hardware addresses assigned to network interfaces (NICs) by manufacturers.
- Uniqueness : Each network interface (e.g., Ethernet or Wi-Fi adapter) has a globally unique MAC address.
- Format : MAC addresses are typically represented as six groups of two hexadecimal digits separated by colons or hyphens (e.g., 00:1A:2B:3C:4D:5E).
- Eg: Used for low-level device communication, such as Ethernet frame addressing and network device identification.

Network Topology

Network Topology refers to the layout or structure of a computer network, defining how devices and nodes are interconnected and how data flows within the network. It describes both the physical and logical arrangement of network components.

Types of Network Topologies :

Bus Topology :

- All devices are connected to a single central cable (the bus).
- Nodes communicate directly with each other through the bus.
- Simple and inexpensive to set up but prone to network disruptions if the main cable fails.

Star Topology :

- All devices are connected to a central hub or switch.
- Devices communicate through the hub/switch, which manages data flow.
- Robust and scalable, easy to troubleshoot, but relies heavily on the central hub/switch.

Ring Topology :

- Devices are connected in a closed-loop configuration.
- Data travels in one direction around the ring.
- Each device acts as a repeater to maintain signal strength but can be problematic if one device fails, disrupting the entire network.

Mesh Topology :

- Every device is connected to every other device in a point-to-point manner.
- Provides redundancy and fault tolerance as data can follow multiple paths.

- Complex and costly to implement due to the number of connections required but highly reliable.

Tree (Hierarchical) Topology :

- Combines characteristics of star and bus topologies.
- Devices are grouped into multiple star topologies connected to a central bus.
- Suitable for large networks, offering scalability and ease of management.

Hybrid Topology :

- Combines two or more different topologies (e.g., star-ring, star-bus).
- Offers flexibility in design to meet specific network requirements.
- Provides advantages of multiple topologies while mitigating their individual limitations.

Subnetting

Subnetting is the process of dividing a larger network (often called a "parent network") into smaller, more manageable sub-networks (subnets). This technique improves the efficiency and security of network management.

How Subnetting Works

i. IP Address Structure : IP addresses consist of two main parts: the network portion and the host portion. The subnet mask determines how these parts are divided.

   - Network Portion : Identifies the specific network or subnet.
   - Host Portion : Identifies the specific device within the subnet.

ii. Subnet Mask : A subnet mask is a 32-bit number used to divide an IP address into network and host portions. It uses '1's to denote the network portion and '0's for the host portion. For example :

- Subnet mask 255.255.255.0 (or /24 in CIDR notation) means the first 24 bits are for the network portion, and the remaining 8 bits are for host addresses.

iii. Subnetting Process : To subnet a network, you borrow bits from the host portion of the IP address and use them to create additional network identifiers (subnets). This effectively increases the number of available subnets while reducing the number of host addresses per subnet.

ARP (Address Resolution Protocol)

The Address Resolution Protocol (ARP) is a network protocol used to map an IP address to a physical machine address (MAC address) within a local network. This is essential for enabling communication within an Ethernet network where devices identify each other using MAC addresses.

How ARP Works

1. ARP Request : When a device wants to communicate with another device on the same local network, it first checks its ARP cache to see if it already has the corresponding MAC address. If not, it broadcasts an ARP request packet to all devices on the local network. This request contains the IP address of the destination device.
2. ARP Reply : The device with the matching IP address responds with an ARP reply, providing its MAC address. This reply is sent directly to the requesting device, not as a broadcast.
3. Updating ARP Cache : The requesting device stores this IP-to-MAC mapping in its ARP cache for future use, which reduces the need for repeated ARP requests.

DHCP (Dynamic Host Configuration Protocol)

The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to automate the process of configuring devices on IP networks. DHCP enables devices to automatically obtain IP addresses and other necessary network configuration information from a DHCP server.

How DHCP Works

1. DHCP Discovery : When a device (DHCP client) connects to a network and needs configuration, it sends out a DHCP DISCOVER broadcast message to find availableDHCP servers.
2. DHCP Offer : A DHCP server that receives the DHCP DISCOVER message responds with a DHCP OFFER message, which includes an available IP address and other configuration information.
3. DHCP Request : The client receives one or more DHCP OFFER messages and responds with a DHCP REQUEST message, indicating its acceptance of the offered IP address and configuration from one of the servers.
4. DHCP Acknowledgment : The chosen DHCP server sends a DHCP ACK message to the client, confirming the lease and finalizing the IP address allocation. The client can now use the assigned IP address.