Week 02:

NETWORK?

Set of technologies

Allows communication between users.

Collection of computers and devices connected.

MAIN TYPES OF NETWORKS?

Wide Area Network (WAN): Connect systems over a large geographic area.

Local Area Network (LAN): Provide network connectivity for computers located in the same geographic area.

OSI REFERENCE MODEL - a reference model and an effective means of teaching distributed communication.

A diagram of a computer

Description automatically generated with medium confidence

The bottom two layers are implemented in hardware, and the top five are implemented through software.

OSI LAYERS

Application Layer

- Responsible for interacting with end users applications.

- Application software accesses network services.

Presentation layer

- Responsible for the coding of data.

- Includes file formats and character representations.

- Encryption generally takes place at the Presentation Layer.

Session layer

- Responsible for maintaining communication sessions between computers.

- Creates, maintains, and disconnects communications that take place between processes over the network.

Transport layer.

- Responsible for breaking data into packets and properly transmitting it over the network.

- Flow control and error checking take place here.

- The transport layer is responsible for maintaining end-to-end communications between hosts across the network

Network layer.

- Responsible for the logical implementation of the network.

- In TCP/IP networking, this layer is crucial for handling logical addressing using IP addresses.

- Handles routing and forwarding of data packets across interconnected networks.

Data Link layer.

- Responsible for framing data received from the Network Layer.

- Prepares data for transmission over the Physical Layer.

- Manages physical addressing, including controlling access to the physical medium.

- Detects and corrects errors that may occur during transmission.

Physical layer

- Responsible for the physical operation of the network.

- Translates binary data (1s and 0s) of computer language into signals suitable for transmission over the physical medium.

- Handles transmission of raw data bits over the physical medium, such as copper wires, fibre-optic cables, or wireless frequencies.

A screen shot of a computer

Description automatically generated

Internet packet encapsulation refers to the process of wrapping data into successive layers of headers as it moves through the network stack.

A close-up of a box

Description automatically generated

1. Data: The original data, such as a web page or a file, is broken down into smaller units called packets.

2. Application Layer: The data from the application layer (e.g., HTTP, FTP) is encapsulated into a payload.

3. Transport Layer: The transport layer header is added, which typically includes information such as source and destination port numbers (e.g., TCP or UDP header).

4. Network Layer: The transport layer segment or datagram is further encapsulated into an IP packet. This involves adding an IP header containing source and destination IP addresses.

5. Link Layer: Finally, the IP packet is encapsulated into a frame at the link layer, which includes information such as MAC addresses and CRC for error checking. This process varies depending on the type of physical network (e.g., Ethernet, Wi-Fi).

Each layer adds its own header (and possibly a trailer) to the data, creating a nested structure of encapsulation. When the packet reaches its destination, each layer in the receiving system's network stack peels off the corresponding header until the original data is extracted.

Encapsulation ensures that data can traverse different types of networks and devices by providing a standardized format for communication. It also enables routers and switches to route and forward packets based on the information contained in the headers.

A PROTOCOL is a set of rules and formats that govern the communication between communicating peers. protocols ensure that communication between peers is standardized, reliable, and interpretable by both the sender and receiver, whether they are humans or computers. Classified as connectionless and connection oriented.

Connectionless protocol - Sends data out as soon as there is enough data to be transmitted.

E.g., user datagram protocol (UDP)

Connection-oriented protocol - Provides a reliable connection stream between two nodes. Consists of set up, transmission, and tear down phases. Creates virtual circuit-switched network.

E.g., transmission control protocol (TCP)

PACKET CONTENTS

Control Information (Header and Trailer):

- Headers: Added at the beginning of the packet, containing information about the packet,

such as origin and destination IP addresses, protocol type, sequence number, and acknowledgment.

- Footers (Trailer): Placed at the end of the packet, containing information

such as error-checking data (e.g., CRC) and timestamps.

* Data (Payload): The actual data being transmitted,

which may include text, images, audio, video, or any other type of information intended for delivery to the recipient.

* is not considered Control Information.

ENCAPSULATION IN NETWORKING:

**Inter-protocol Communication**: A Network protocol (N1) can utilize the services of another network protocol (N2).

**Packet Encapsulation**: A packet (p1) belonging to protocol N1 is encapsulated into a packet (p2) of protocol N2.

**Payload Relationship**: The payload of packet p2 is packet p1. In other words, the data carried by p1 becomes the payload of p2.

**Control Information**: The control information of packet p2 is derived from that of packet p1, ensuring that relevant information from p1 is preserved and adapted for use by protocol N2. A blue and orange rectangular box with white text

Description automatically generated

**THE DOMAIN NAME SYSTEM (DNS) -** an application-layer protocol for mapping domain names to IP addresses.

DNS provides a distributed database, that stores various **resource records**, including:

* Address (A) record: IP address associated with a host name.
* Mail exchange (MX) record: mail server of a domain.
* Name server (NS) record: authoritative server for a domain.

**DNS CACHING**

* There would be too much network traffic if a path in the DNS tree would be traversed for each query.
* Caching prevents the need to traverse the entire DNS tree for each query, avoiding overload of the root zone.
* Results are cached for a specified duration indicated by the Time-to-Live (TTL) field in the DNS response.
* Some operating systems maintain DNS caches: Windows, Linux.
* DNS queries are typically sent over UDP on port 53.
* Requests contain a 16-bit request identifier in the payload, which may pose privacy concerns.

What is the primary role of the Domain Name System (DNS) as an application-layer protocol in network communication? To map domain names to IP addresses

What is the primary function of the Dynamic Host Configuration Protocol (DHCP)? To dynamically distribute IP addressing and configuration information to clients

**USER DATAGRAM PROTOCOL (UDP):**

Lightweight and connectionless: UDP does not establish or maintain a connection before transmitting data.

Small packet sizes: UDP headers are smaller (8 bytes) compared to TCP (20 bytes), making UDP more efficient for certain applications.

No connection setup: There is no need to establish a connection before sending data.

More control over data transmission: Applications have more control over when and how data is sent.

No error recovery: UDP does not compensate for lost packets or retransmit them.

No packet ordering: UDP does not guarantee the delivery of packets in the order they were sent.

No congestion control: UDP does not check if the network is busy before sending data, which can lead to congestion issues.

**TRANSPORT LAYER: TRANSMISSION CONTROL PROTOCOL (TCP)**

- Reliable and connection-based: TCP ensures reliable data transmission through a connection-oriented approach.

- Sequence numbers, timeouts, and retransmissions: Protect against loss, reordering, and duplication of data.

[Sequence numbers are used to manage data sequence, timeouts for detecting lost packets, and retransmissions for re-sending lost packets]

- Header section with flags field: TCP packets contain a flags field in the header section, indicating various control information.

Four possible flags:

- SYN (Synchronize): Used to initiate a connection.

- ACK (Acknowledge): Confirms receipt of data.

- FIN (Finished): Signals the end of data transmission.

- RST (Reset): Indicates an abnormal termination of the connection.

\*\* Which protocol of the TCP/IP suite addresses reliable data transport? The Transmission Control Protocol (TCP) is the protocol within the TCP/IP suite that addresses reliable data transport.

**TCP PACKETS: THREE-WAY HANDSHAKE**

1. SYN (Synchronize) packet:

- The initiating system sends a SYN packet to the destination to request a connection establishment.

2. SYN/ACK (Synchronize/Acknowledge) packet:

- Upon receiving the SYN packet, the destination sends a combined SYN/ACK packet to acknowledge the receipt of the first packet and signal its readiness to establish the connection.

3. ACK (Acknowledge) packet:

- Finally, the initiating system sends an ACK packet to acknowledge the receipt of the SYN/ACK packet, completing the three-way handshake.

Once the three-way handshake is completed, data transfer can begin between the two systems. This process ensures reliable and orderly connection establishment in TCP communications.

**IPV4 ADDRESSES:** Four-byte (32-bit) addresses that uniquely identify every device on the network. Still the most common.

**IPV6 ADDRESSES:** 128 bits long. Provide more unique device addresses. More secure

**IPV4 ADDRESSING** 32 bits Binary address. Divided into 4 parts, separated by 8 binary each. Each 8 binary digits are converted to Decimal. Hence is called Dotted Decimal. Each IP represents the Network address and the host address.

For example, the IP address in this figure tell us the following:

192.168.10.0 is the Network Address

192.168.10.255 is the Broadcast address.

Hosts can have any IP between 192.168.10.1 to 192.168.10.254

This is called a Class C IP address. In class C-the network part is the three first dots. The host part is only the last decimal number of the IP.

**DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)** DHCP is used within a network to simplify the configuration of each user’s computer.

**MAC ADDRESS**

- Most network interfaces have a predefined MAC (Media Access Control) address.

- A MAC address is a 48-bit number typically represented in hexadecimal format.

- Example: 00-1A-92-D4-BF-86

- On Windows, you can obtain the MAC address using "getmac".

- On Linux, you can view the MAC address by typing "ip addr".

**ADDRESS RESOLUTION PROTOCOL (ARP)**

- ARP connects the network layer to the data link layer by converting IP addresses to MAC addresses.

- ARP works through broadcasting requests and caching responses for future use.

- The protocol starts with a computer broadcasting a message in the form:

"Who has <IP address1> tell <IP address2>"

- When the machine with IP address1 or an ARP server receives this message, it broadcasts the response:

"<IP address1> belongs to <MAC address>"

- The command "arp -a" displays the ARP table on both Linux and Windows systems.

**NETWORK INTERFACE**

- Network interfaces, although not protocols, are physical devices that determine which network interface card the system will use.

- Considered both Physical Layer and Data Link Layer interfaces as they provide the MAC address of the interface.

- Connects a computer to a network and can include devices such as Ethernet cards or WiFi adapters.

- Packets are transmitted between network interfaces, with most local area networks broadcasting frames.

- Each network interface receives the frames intended for it based on its MAC address.

- Hackers or penetration testers may conduct traffic sniffing by configuring the network interface to read all frames in promiscuous mode, also known as Monitor mode.