**Networking - Basics**

**Network Types**

1. Personal area networks (PAN)
2. Local area networks (LAN)
3. Metropolitan area networks (MAN)
4. Wide area networks (WAN)

**Network Topologies**

1. Bus
2. Ring
3. Mesh
4. Star

**Network Standard**

Network standards are designed to ensure that hardware and software made by different vendors work seamlessly together.

**Media Access Control (MAC) Address**

* Unique identifier assigned to every network-enabled device at the time of manufacture.
* Referred to as the burned-in address, the Ethernet hardware address, or a physical address.
* Has a standard composition of six hexadecimal numbers separated by a colon or dash, for example, AA-6A-BA-2B-68-C1.
* The first three numbers of the MAC address define the manufacturer's organizationally unique identifier (OUI). The remaining three numbers uniquely identify the device.

**Network Devices**

* Repeaters
* Hubs
* Bridges
* Switches
* Routers

Nearly all of these devices depend on a media access control or an Internet Protocol (IP) address to deliver data on the network

**Repeater:**

* Regenerates Signal
* Doesn't modify or interpret data packets
* Doesn't amplify the signal. Instead, it regenerates the data packet at the original strength, bit by bit.

**Hub:**

* It does not filter data.
* When a data packet comes from one device, it broadcast to multiple devices connected on this hub.
* They allow multiple Ethernet-based network-enabled devices to communicate with each other.
* It does not read MAC address of network devices. So, it shares signal with all devices connected with hub which is security concern.

**Switches:**

* Able to read MAC address
* Filter data based on MAC address
* Data is being sent only to matching MAC address device.
* Reduces security concerns compare to Hub.

**Router:**

* Both Hub and Switch used to create LAN network, does not connect Internet. So, Router comes into picture.
* Used for routing data from one network to another based on IP.
* When data with IP comes to router which matches IP of data packet with intended network. If it matches, it sends data. Otherwise, it routes to another different network.

NOTE:

Hubs & Switches are used to create networks whereas Routers are used to connect to networks.

**Network Address**

1. Media Access Control (MAC) address that identifies the network interface on the hardware level.

2. Internet Protocol (IP) address that identifies the network interface on a software level.

**Routing**

Routing, in the context of networks, refers to the mechanism used to make sure that data packets follow the correct delivery path between the sending and receiving device on a network.

**Subnet**

A subnet defines one or more logical networks within the class A, B, or C network. Without subnets, you're restricted to a single network in each of the class A, B, or C networks. Subnets allow multiple subnetworks to exist within one network.

**Classless Interdomain Routing (CIDR) notation**

* Common way to define the subnet and the routing prefix is to use the Classless Interdomain Routing (CIDR) notation.
* CIDR applies to the IP address as the number of bits you want to allocate to your subnet.
* Using CIDR notation, at the end of the IP address, add a "/" and then the number of bits.
* For example, 198.51.100.0/24 is the same as using the dotted-decimal format subnet mask 255.255.255.0. It offers an address range of 198.51.100.0 to 198.51.100.255.
* Each segment in the IP is 8 bits. So, in a 32 bits IP address, you’ll have 8+8+8+8=32 bits.
* As a bit is 0 and 1, basically it’s 2. So 8 bits on one segment is 2^8 which is 255 (starting is 0 ).

**DNS**

The Domain Name System is a decentralized lookup service that translates a human-readable domain name or URL into the IP address of the server that's hosting the site or service.

**Network Client**

A network client is a lightweight computer or device that can't run programs on its own. This type of client is typically used to access and interact with a mainframe computer / Server. This server is located elsewhere and is accessed through a network.

**Firewall**

A network firewall is a security appliance that blocks or remedy unauthorized access into your network. Network firewalls also monitor and make logs of all traffic across your network.

**Authentication Vs Authorization**

Graphical user interface, text, application, email

Description automatically generated

**OSI & TCP/IP Model**

Graphical user interface, text, application, chat or text message

Description automatically generated

Diagram, table

Description automatically generated

Table

Description automatically generated