21BDS0340

Abhinav Dinesh Srivatsa

Information Security Management

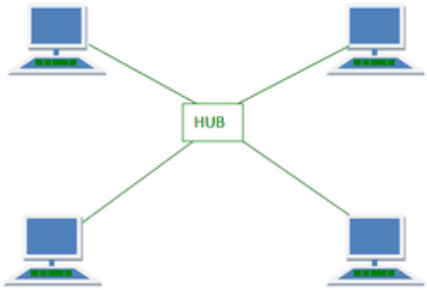
Assignment – I

Question 1

Hub

A hub is a network device that works on the physical layer in the OSI model. This network device connects multiple devices to a single network. Any packets transmitted to a hub are relayed to all nodes connected, regardless or addresses. A hub will never keep track of the receivers, unlike a switch.

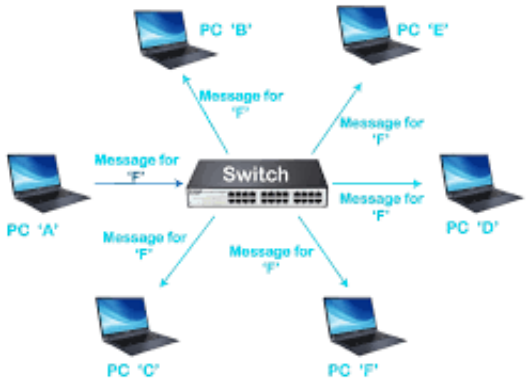
Before a hub is connected, a group of nodes must be talked to separately. After a hub is connected, messages can be sent to the hub, which will broadcast to all nodes connected to it.



Switch

A switch is a smarter hub that works on the data link layer in the OSI model. This network device connects multiple devices that are on a single network. Any packets transmitted to a switch are initially broadcast, but the switch keeps a table that tells who the actual receiver of the packet is, to narrow its sending for following packets.

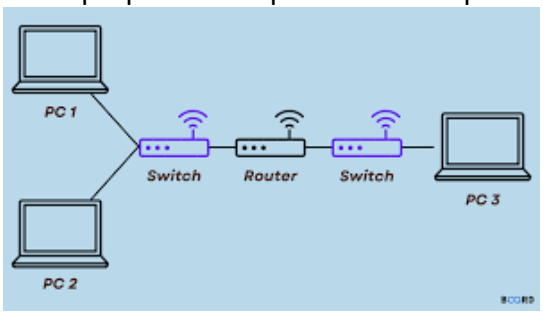
Before a switch is connected, a group of nodes must be talked to separately. After a switch is connected, messages can be sent the switch, which will more effectively reroute it to the correct node only.



Router

A router is a device that works on the network layer in the OSI model. This network device can connect multiple LANs or networks. The router uses routing tables to route packets through its network. Routers assign unique addresses to device on the network and use TCP/IP for effective communication.

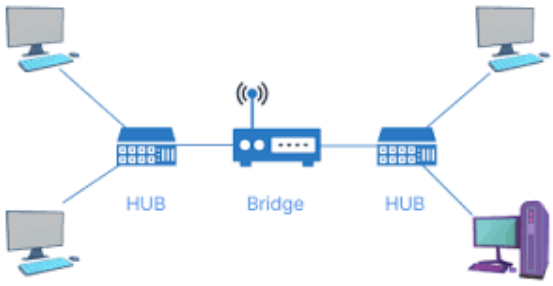
Before a router is connected, a network can only talk within itself. A router allows to connect multiple networks, allowing the internet to be what it is. Routers are instrumental in making private devices like laptops and cell phones access public internet.



Bridge

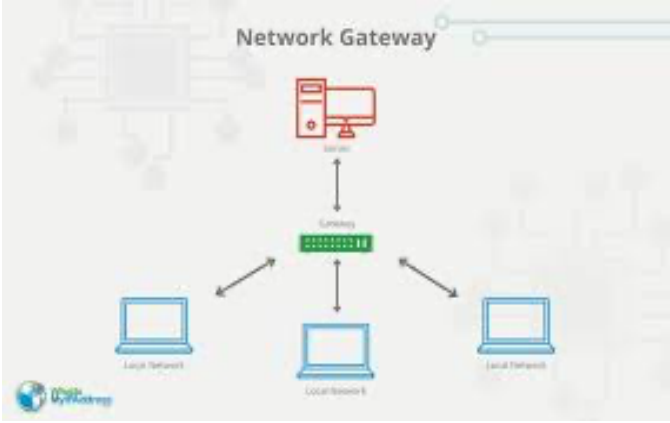
A bridge is a device that works in the data link layer in the OSI model. Bridges can help connect multiple end devices together to for a larger device pool. The bridges functionality is largely replaced by the switch nowadays.

Before a bridge is connected, separate devices can be isolated and will be accessed individually. After a bridge is connected, we can access the devices from one common area.



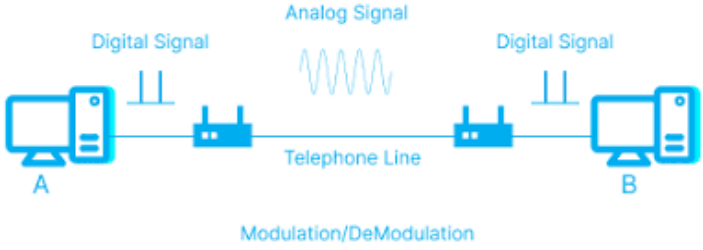
Gateway
A gateway is a network device that connects two networks that employ different transmission protocols. A network gateway is responsible for translation of one protocol to another for effective communication. Nowadays, the gateways functionality is being merged with the router. A gateway is utilised on the network layer of the OSI model.

Before a gateway is connected, different devices that use different communication standards may not be compatible. Examples can include Ethernet and Wi-Fi connections. After a centrallised gateway, these can be translated.



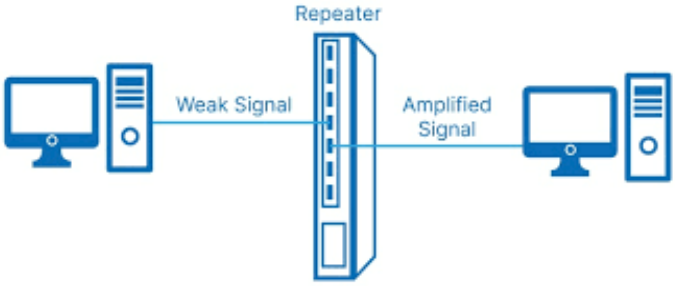
Modem
Short for modulator-demodulator, the modem is used to connect devices in a network to the internet. The modulation and demodulation are for converting digital signals to analog signals and vice versa.

Before a modem is used, the conversion of digital to analog and vice versa isn't easily available. This is extremely useful in wireless communication and standards.



Repeater
Repeaters are a device dedicated to extending the range of a network by amplifying or regenerating signals, particularly in wired or wireless communication setups. It serves as a crucial solution to combat signal degradation over lengthy distances. In situations where signals weaken due to factors such as cable attenuation or atmospheric interference, repeaters play a vital role in upholding effective communication. Repeaters operate within the network layer of the OSI model

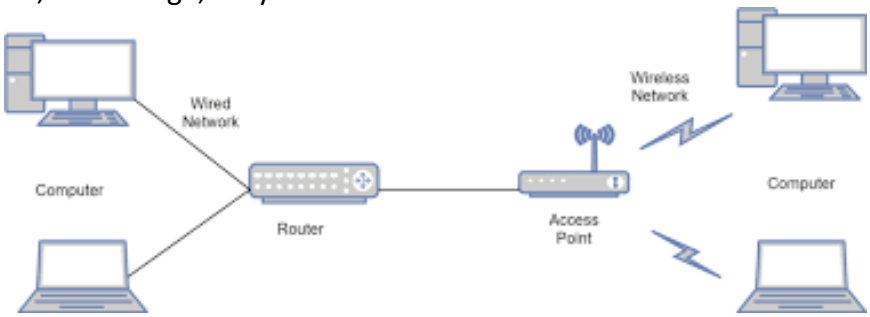
Before repeaters are used, signal loss can happen over long distance, which is not the case after utilizing them.



Access Point

An access point serves as a network device aimed at facilitating wireless connectivity by providing a link between wired and wireless networks. It functions as a gateway for wireless devices to connect to a broader network. Access points operate within the network layer of the OSI model.

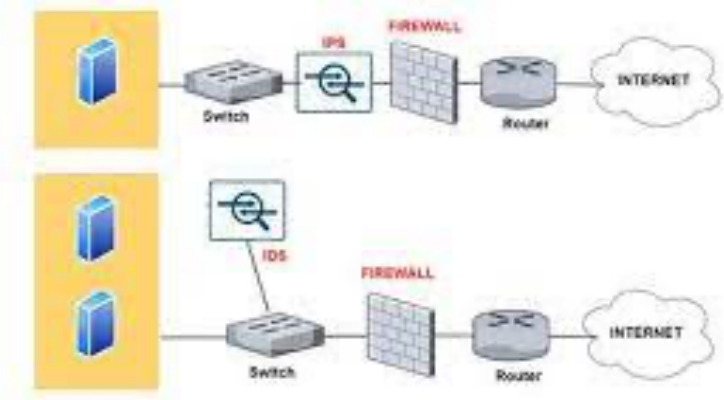
Before an access point is used, wired and wireless connections are not centrallised for communication, after usage, they are.



IDS/IPS

An Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) are sophisticated network security devices designed to monitor and safeguard against unauthorized access and potential threats. They operate within the network layer of the OSI model.

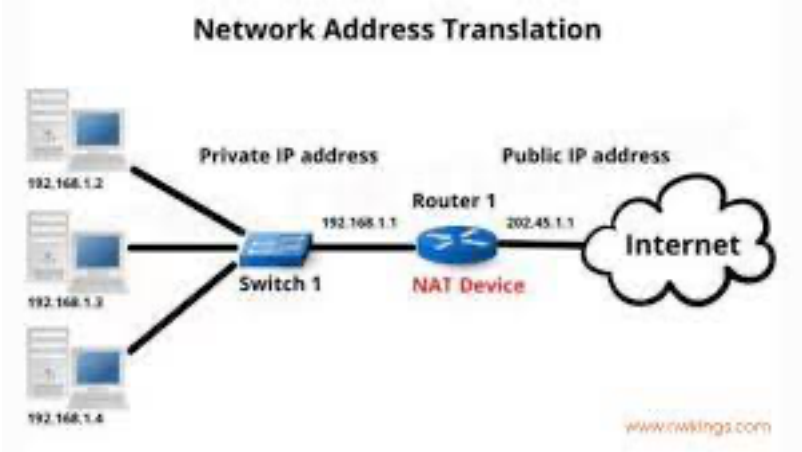
Before these systems are implemented, the network is vulnerable, and we cannot see unauthorized access. After these systems are put in place, the system is more secure.



NAT

Network Address Translation (NAT) is a pivotal networking technique employed to manage the distribution of IP addresses within a private network and connect it to external networks, such as the Internet. NATs use the network layer of the OSI model, NAT serves as a fundamental mechanism for conserving public IP addresses and enhancing network security.

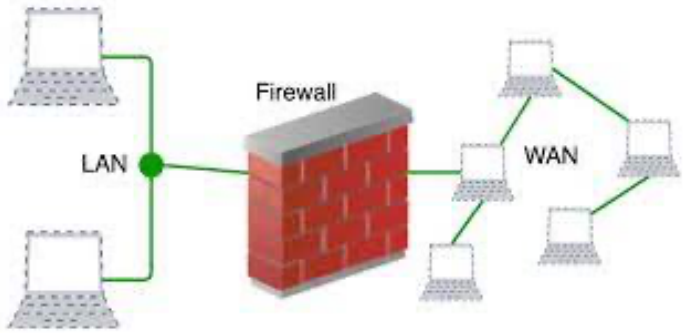
Before NATs are used, translation from addresses and machine addresses are not easy to route. After NAT usage, this becomes readily available.



Firewall

A firewall is a critical network security device designed to monitor, filter, and control incoming and outgoing network traffic based on predetermined security rules. Firewalls operate at the network layer of the OSI model, firewalls act as a barrier between a trusted internal network and untrusted external networks, such as the Internet.

Before firewalls, any access is allowed to a machine, after firewalls, inbound and outbound rules can be set to filter permissions.



VPN

A Virtual Private Network (VPN) is a technology that enables secure and private communication over a public network, typically the Internet. VPNs operate at the network layer of the OSI model, VPNs create a secure and encrypted tunnel for data transmission, ensuring the confidentiality and integrity of information exchanged between connected devices.

Before VPNs a client and server talk directly. After a VPN is setup, the client is proxied, and the communication is encrypted to talk to the server. The VPN acts as a middleman in the client-server communication.