- ALMUSTAQBAL UNIVERSITY
- Department of Radiology Technologies

security and networking
Fourth lecture
by Hasan Faez

Network :

A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

Software modules in one system are used to communicate with one or more software modules in the distance System. Such interfaces across a distance are termed as “peer-to-peer” interfaces; and the local interfaces are termed as “service” interfaces. The modules on each end are organized as a sequence of functions called “layers

Networking

Classification of Networks :

1.Based on Transmission Mode :

Transmission mode defines the direction of signal flow between two linked devices. There are three types of transmission modes

Simplex : In simplex mode, the communication is unidirectional. Among the stations only one can transmit and the other can only receive.

Half-Duplex :

In half-Duplex mode, the communication is bidirectional. In this both station can sent and receive but not at the same time.

Full-Duplex : In Full-Duplex mode, both stations can transmit and receive simultaneously.

2. Based on Time in Transmission Type

Synchronous Transmission:

In synchronous Transmission both the sender and the receiver use the same time cycle forthe transmission. We send bits one after another without start/stop bits or gaps. It is the responsibility of the receiver to group the bits. Bit stream is delivered with a fixed delay and given error rate. Each bit reaches the destination with the same time delay after leaving the source.

Asynchronous Transmission :

In Asynchronous Transmission we send one start bit at the beginning and one stop bit at the end of each byte. There may be a gap between each byte. Bit stream is divided into packets. Packets are received with varying delays, so packets can arrive out of order. Some packets are not received correctly

3. Based on Authentication

Peer to Peer Connection: In peer-to-peer networks, there are no dedicated servers. All the computers are equal and, therefore, are termed as peers. Normally, each computer functions as both a client and a server. No one can control the other computers.

Server Based Connection: Most networks have a dedicated server. A dedicated server is a computer on a network which functions as a server, and cannot be used as a client or a workstation. A dedicated server is optimized to service requests from network clients. A server can control the clients for its services

4. Based on Geographical location

Local Area Networks (LAN): LAN is a small high speed network. In LAN few numbers of systems are interconnected with networking device to create network. As the distance increases between the nodes or system it speed decreases. So it is limed to few meters only. Networks which cover close geographical area. LAN used to link the devices in a single office, building or campus. It provides high speeds over short distance. Systems are connecting directly to Network. The LAN is owned by private people

Wide Area Network (WAN): WAN is collection of network (or LAN). This network speed is less than the LAN network speed . WAN network connect systems indirectly. WAN spread over the world may be spread over more than one city country or continent. Systems in this network are connected indirectly. Generally WAN network are slower speed than LAN's. The WAN network are owned or operated by network providers. If it is owned by a single owner then it is called Enterprise network. Often these types have combination of more than one topology.

MAN (Metropolitan Area Network) : Metropolitan area network is an extension of local area network to spread over the city. It may be a single network or a network in which more than one local area network can share their resources.

5. Based on Reliability:

Connection-oriented :

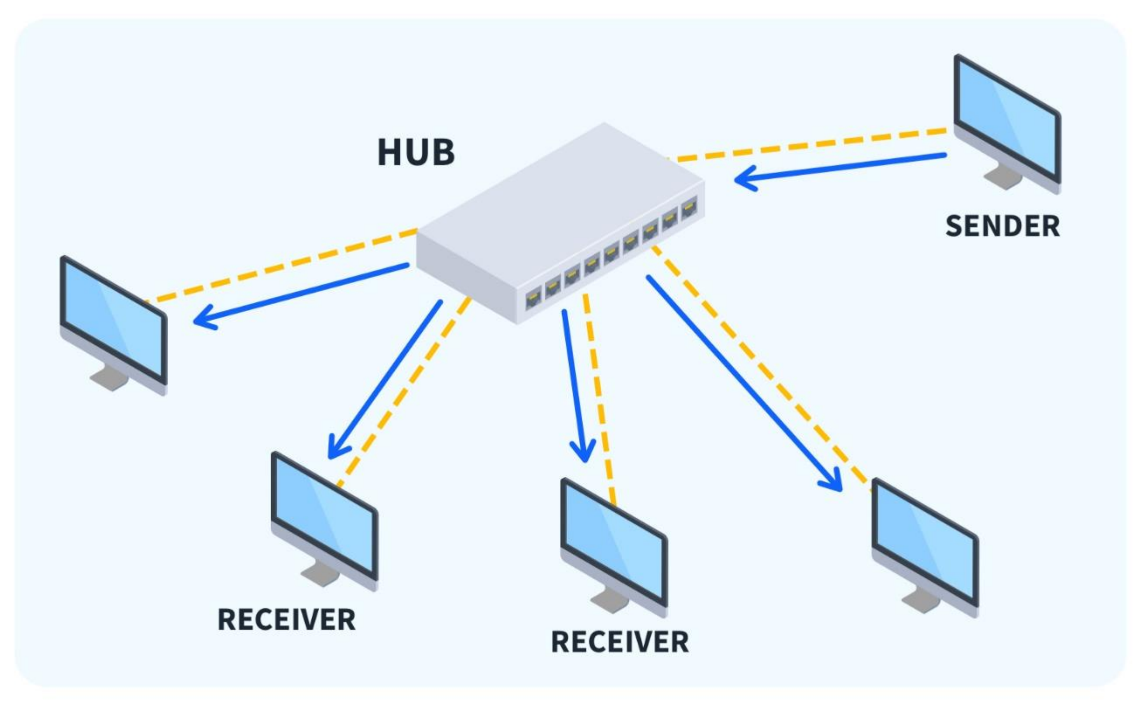
This type of communication establishes a session connection before data can be sent. This method is often called a "reliable" network service. It can
guarantee that data will arrive in the same order.

Connection less : This type of communication does not require a session connection between sender and receiver for data transfer. The sender simply starts sending packets to the destination. A connectionless network provides minimal services.

basic network components

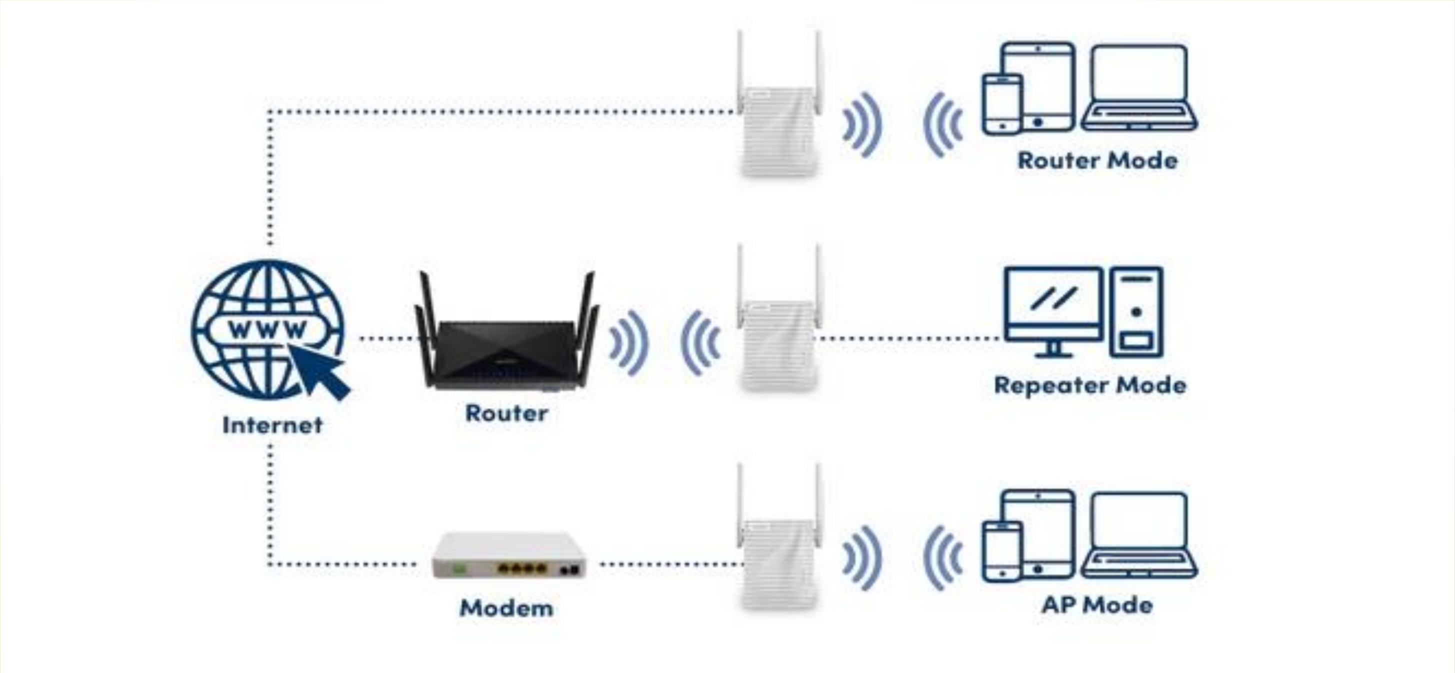
1. Hub:

- It is uses to connect systems or nodes or networks.
- It has direct connection to a node (point to point connection).
- It suffers from high collision of data, results to data loss.
- A hub takes data from input port and retransmits the input data on output port



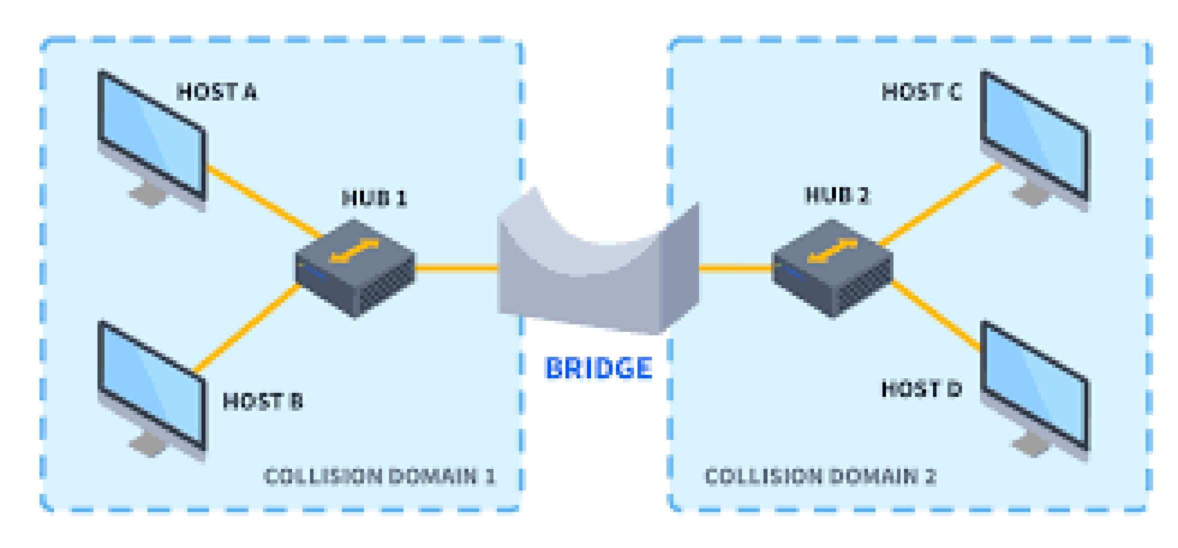
2. Repeater:

- A repeater is a device which regenerates or amplifies the data or signal so that it can be travel to the other segment of cable.
- It is use to connect two networks that uses same technology and protocol.
- It does not filter or translate any data.
- Work in physical layer.



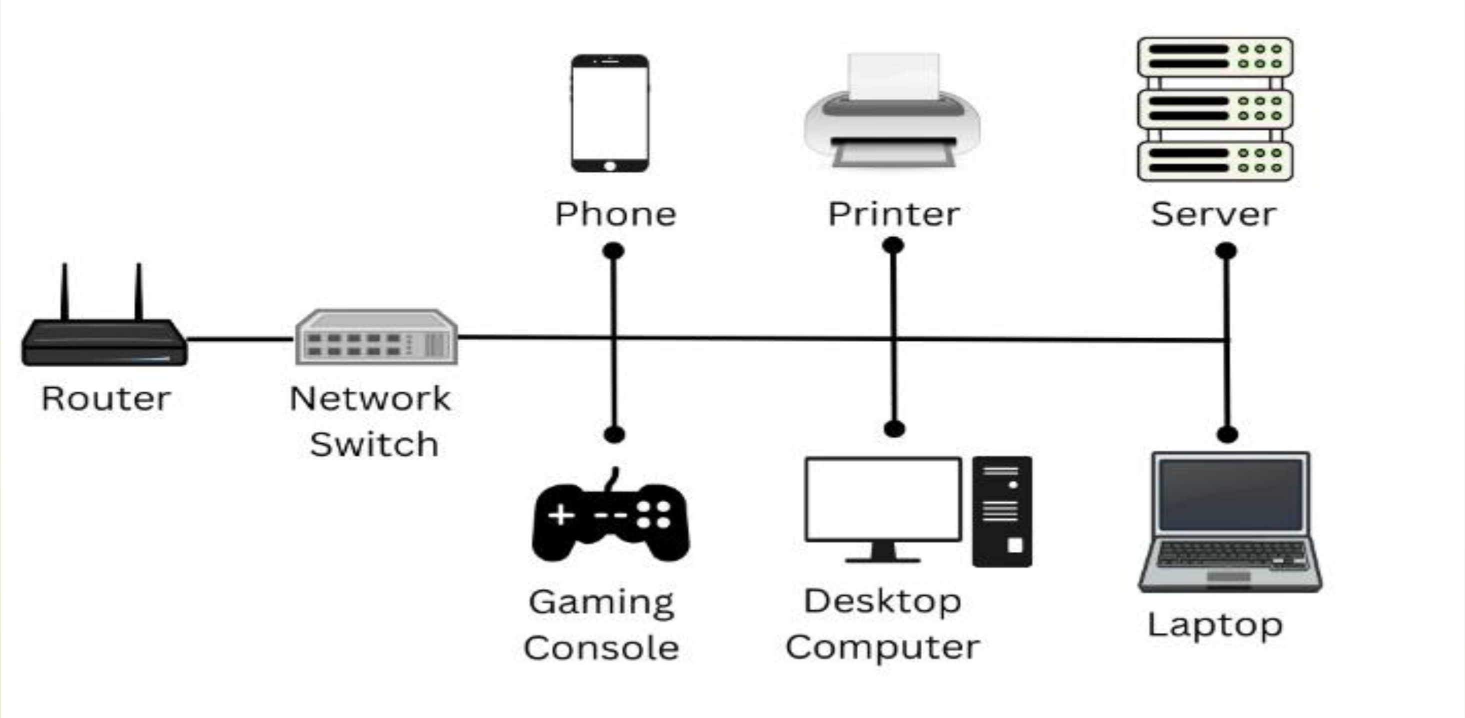
3- Bridge:

- It is used to connect two networks.
- It divides the collision domain based on number of ports or interface present in a bridge.
- It uses the packet switches that forward and filter the frames using LAN destination address.
- Bridge examines the destination address of frame and forwards it to the interface or port which leads to the destination.
- It uses the routing table for routing frame from one node to other using MAC address.
- It works in Data Link Layer.



4. Switch :

- It is similar to bridge. It has more number of interfaces as compared to bridge.
- It allows direct communication between the nodes
- It works in Data Link Layer.
- It uses MAC address for data transmission and communication

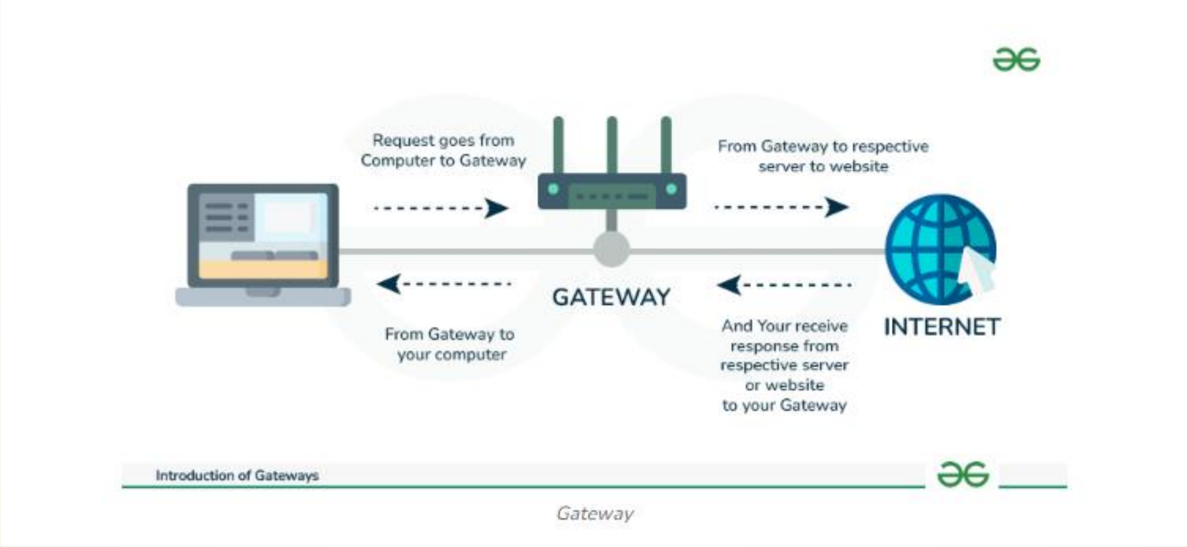


5. Router:

- It is used to connect different types of network (types- architecture/ Protocol).
- It work similar to bridge but it uses IP address for routing data.
- Router can't be used for connecting Systems.
- It works in Network Layer.

6. Gateways:

Gateways make communication possible between systems that use different communication protocols, data formatting structures, languages and architectures. Gateways repackage data going from one system to another. Gateways are usually dedicated servers on a network and are task-specific.



Request goes from Computer to Gateway
From Gateway to respective server to website
GATEWAY
INTERNET
From Gateway to your computer
And Your receive response from respective server or website to your Gateway
Introduction of Gateways

Gateway

Network Security Basics

Every week, networks seem to grow in size and complexity. New SaaS services come online, while innovative communication tools make remote working easier. Data storage methods shift, with new assets to secure. And new malware threats constantly emerge. In an ever-changing digital world, network security has never been more crucial.

What is network security and why is it important ?

Network security is the process of protecting networks against potential threats. It includes software and hardware designed to detect and block malicious agents. Securing networks also extends to access control, network organization, and security policies.

Networking security is closely related to cybersecurity and information security.

Cybersecurity guards against digital threats. InfoSec focuses on data protection.

Both feed into protecting a single computer connected to the network infrastructure against outside threats.

Network security matters because data and apps need protection. Businesses depend on reliable access to workloads and databases. However, they must secure confidential data from external observers via information security techniques. A well-thought-out security strategy balances access and protection while also meeting compliance goals.

The main types of network security

- Firewalls
- Access control
- Application security
- Data loss prevention
- Malware protection
- Web gateways
- Email security
- Behavior monitoring
- Virtual private networks VPNs
- Intrusion Prevention Systems IPS

understanding network threats

What is a network security threat ?

Network security vulnerabilities are weak points in physical devices or software which present an opportunity for cyber attackers. Weaknesses could range from poor server surveillance and physical protection to inadequate operating system and antivirus updates.

Types of threats :

Phishing
Phishing is a social engineering attack designed to induce the recipient of a message to take some action .

Ransomware
Ransomware has emerged as one of the top malware threats of recent years. Ransomware attacks have grown increasingly common, and ransom demands are commonly in the millions of dollars .

DDoS Attacks
Distributed Denial of Service (DDoS) attacks target the availability of an organization’s IT assets or online services .

Viruses
Viruses are malware that can spread themselves but require some form of human interaction .

Worms
Worms are malware that can spread themselves without the need for human interaction.

Trojans
Trojans are a type of malware that relies on deception. If malware masquerades as a legitimate file, users may download or execute it of their own volition.

network troubleshooting

Network troubleshooting is the systematic process of finding problems that prevent network operation. It entails isolating and fixing these issues. This procedure includes a variety of approaches and technologies. Network engineers employ troubleshooting techniques to identify connectivity issues. They also employ similar methods to detect and correct slowdowns, hardware failures, and software misconfigurations.

Importance of Network Troubleshooting

- Resolving issues rapidly reduces downtime
- A well-functioning network increases user productivity
- Proactive troubleshooting identifies possible security flaws before they are exploited.
- Efficient troubleshooting reduces the need for reactive maintenance and expensive fixes.

Thank you for listening