26-12-24

DAY 03

1. Site-to-Site VPN:

- A Site-to-site VPN establishes a link between two or more distinct networks such as companies main network and its satellites office networks.
- Many organizations adopt Site-to-Site VPN to utilize internet pathways for confidential data rather than private MPLS channels.
- Organizations with multiple branches spread across diverse regions often use site-to-site VPNs.
- Through this setup, businesses can safely integrate their central network with distant offices, enabling seamless communication and resource sharing as though they were one unified network.

ps-si-as

- A Site-to-Site solution can be deployed as an extranet-based VPN when a company connects its network to the networks of its partners, suppliers or customers.

2. Remote Access VPN

- Remote Access VPNs allow off-site users to securely connect to and utilize applications and information in the company's main data center, encrypting all user data transmitted and received.
- The remote access VPN ensures security regardless of the user's public location by forming a virtually private connection using a tunnel between the enterprise's network and a distant user.
- This is achieved by encrypting the data, rendering it indecipherable to potential interceptors.
- Users can interact with their company's network as if they were on-site, ensuring safe data transfer without the concern of external interface or data bridges.

3. Cloud VPN

- Cloud VPN, sometimes referred to as hosted VPN or VPN as a Service (VPNaaS), is a VPN approach tailored for cloud environments.
- This VPN allows user to securely access a business's resources, data, and applications in the cloud through a web interface or a dedicated app on desktop or mobile.

- Unlike conventional VPNs that necessitate specific infrastructure at the user's location, cloud VPNs integrate seamlessly into a company's cloud distribution framework.
- One significant benefit of cloud VPNs is rapid worldwide configuration and deployment.
- Using a cloud VPN enhances security. Compared to traditional VPNs and contributes to a more adaptable, nimble, and scalable cloud setup for businesses.

4. SSL VPN

- An SSL VPN, or Secure Sockets Layer virtual private network, allows remote users to connect to private networks in a secure manner.
- It employs the SSL security protocol, or its successor, the Transport Layer Security (TLS) security protocol, to ensure the encrypted transmission of data between the user's device and the VPN gateway.
- This encryption safeguards the integrity and confidentiality of data, ensuring that unauthorized entities cannot intercept or alter it.
- Unlike some VPN solutions, an SSL VPN does not require specialized VPN client software on user's devices.
- Instead, it uses standard web browsers making it more accessible and reducing the deployment complexity.
- All communications between the user's web browser and the VPN device are encrypted, making it safe for data transfer across potentially insecure networks.

5. ~~Remo~~ SSL Portal VPN

- In this model, users access a single webpage, or portal, which provides links to other private network resources.
- By visiting a specific website and entering credentials, users can initiate a secure SSL connection.
- This portal then grants access to designated applications or network services, as predefined by the organization.

6. SSL Tunnel VPN

- This variant is more comprehensive, enabling users to securely access multiple network services, not just those that are web-based.
- It establishes an encrypted tunnel under SSL, allowing for the secure access of various resources.
- To function optimally, SSL Tunnel VPN might require browsers equipped with additional applications, such as Javascript or flash.

7. Double VPN

- A double VPN is more of a configuration versus a type of VPN technology.
- This setup involves channeling user traffic through two sequential VPN servers, providing two layers of encryption.
- In standard use of VPN, data flows from the user's device to a single VPN server and then to the destination online.
- Using a double VPN configuration, the user's data is first encrypted and sent to an initial VPN server.
- Then it's encrypted again and directed to a second VPN server before reaching

its final online destination.

- While the double VPN method heightens security by adding an extra layer of encryption, it can also lead to slower connection speeds.
- This slowdown is a result of the data passing through two seperate servers and undergoing dual encryption processes.
- while beneficial for those seeking augmented security, it may not be ideal for all due to potential performance impacts.

* VPN and VPN Tunnel

- A VPN refers to the overall secure connection system, a VPN Tunnel specifically denotes the encrypted data passage within that system.

* Diff b/w VPN and VPN Protocol

- A VPN is the overall system or service, while the VPN Tunnel Protocol is the set of instructions that dictate how the VPN should secure the data being transmitted.

- Choosing a VPN depends on
  i. Security features
  ii. scalability
  iii. ease of use
  iv. support
  v. cost

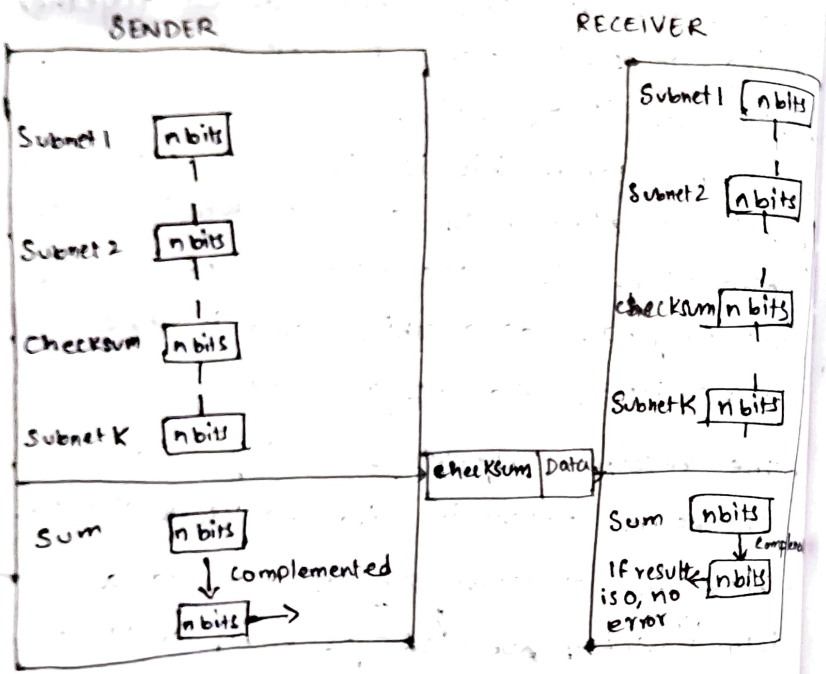
* Checksum

- Checksum is the error detection method used by upper-layer protocols and is considered to be more reliable than Longitudinal Redundancy check (LRC), Vertical Redundancy Check (VRC), and Cyclic Redundancy Check (CRC).

- This method uses a Checksum Generator on the Sender side and a Checksum checker on the receiver side.
- It is a unique number generated from data to verify its integrity.
- When data is created, a checksum is calculated and sent or saved with it.
- Later, when accessing the data, the checksum is recalculated. If the two checksums match, the data is likely error free.

* How Checksum Works

- On the Sender side, the data is divided into equal subunits of n bit of length by the Cheksum Generator.
- This bit is generally of 16-bit length.
- These subunits are then added together using one's complement method.
- This sum is of n bits.
- The resultant bit is then complemented.
- This complemented sum which is called checksum is appended to the end of the original data unit and is then transmitted to the receiver.
- The receiver after receiving data + checksum passes it to checksum checker.
- Checksum checker divides the data unit into various subunits of equal length and adds all these subunits.
- These subunits also contain checksum as one of the subunits.
- The resultant bit is then complemented.
- If the complemented result is zero, it means the data is error-free.
- If the result is non-zero it means the data contains an error and receiver rejects it.



Advantage

1. Error Detection
2. Simple and fast
3. Less Resources

Disadvantage

1. Limited Detection
2. No Error Correction
3. Not Secure

1. Example - If the data unit to be transmitted is 10101001 00111001, the following procedure is used at Sender site and Receiver site.

Sender site :

10101001	Subunit 1
00111001	Subunit 2
11100010	Sum (using 1's complement)
00011101	Checksum (complement of sum)

Data transmitted to Receiver is

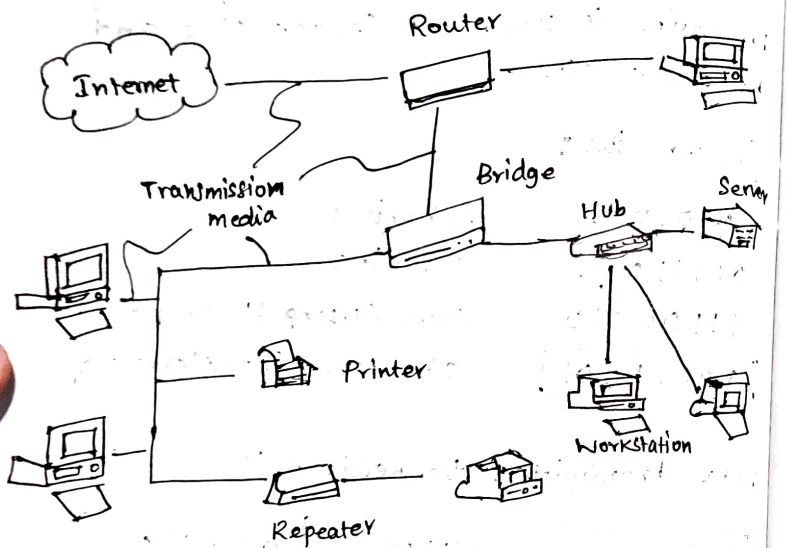
10101001	00111001	00011101
Data		Checksum

Receiver Site :

10101001	Subunit 1
00111001	Subunit 2
00011101	Checksum
11111111	Sum
00000000	Sum's complement

Result is zero, it means no error.

★ Computer Network Components



> Server

> Clients

> Peers - Peers are computers that provide as well as receive services from other peers in a workgroup network.

> Transmission Media - Transmission media are the channels through which data is transferred from one device to another in a network.

- Transmission media may be guided media like coaxial cable, fibre optic cables etc; or maybe unguided media like microwaves, infra-red waves etc.

- Connecting Devices - Connecting devices act as middleware between networks or computers, by binding the network media together.

- Some of the common connectivity devices are:
Routers, bridges, Hubs, Repeaters, Gateways and Switches.

★ Switch characteristics

- A Switch operates in the layer 2, i.e. data link layer of the OSI model.
- It is used in MAC addresses (addresses of medium access control sublayer) to send data packets to selected destination ports.
- It uses packet switching technique to receive and forward data packets from the source to the destination device.
- It supports unicast (one-to-one), multicast (one-to-many), and broadcast (one-to-all) communications.
- Transmission mode is full duplex, i.e. communication in the channel occurs in both the directions at the same time. Due to this, collisions do not occur.
- Switches are active devices, equipped with network software and network management capabilities.
- Switches can perform some error checking before forwarding data to the destined port.
- The number of ports is higher - 24/48.

★ Types of Switches

i. unmanaged Switch (ex: TP-Link TL-SF1005D): It is a basic plug-and-play network switch that requires no configuration or management. It operates out of the box, automatically forwarding data b/w devices within a network without any user intervention.

ii. Managed Switch

- A Managed Switch offers advanced features and allow full control over the network, include: ability to config, monitor and troubleshoot the switch. Ideal of large network & business to optimize performance.

iii. LAN Switch (Netgear GS108)

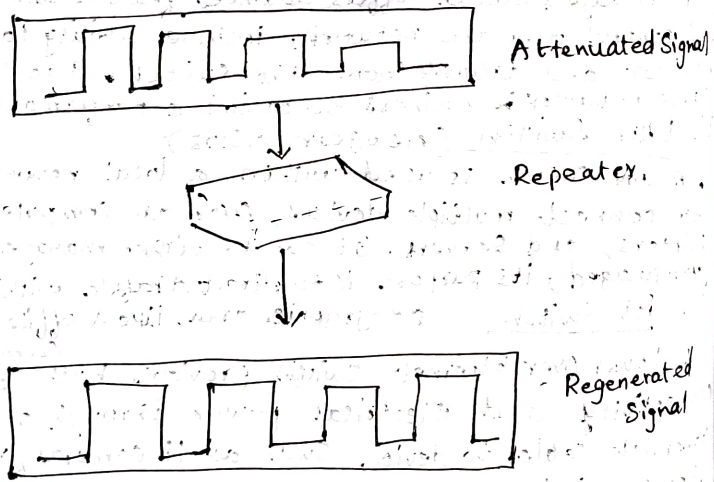
- A LAN Switch is used within a local network to connect multiple devices, such as computers, Printers, and Servers. It can be either managed or unmanaged, its purpose is to direct traffic within a geographic area, like a office or campus.

iv. PoE Switch

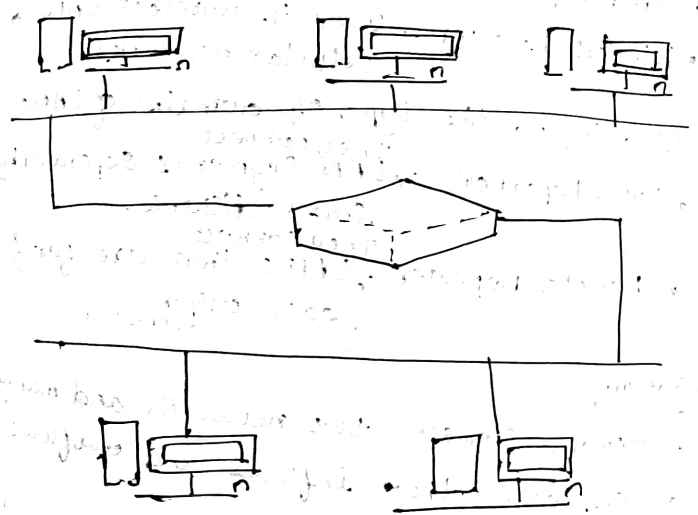
A Power Over Ethernet Switch provides both data connectivity and electrical power through a single Ethernet cable. to devices such as IP cameras, VoIP Phones, wireless access points, and other low-power devices. It eliminates the need for seperate power cables.

★ Repeaters

- Repeaters are network devices operating at the physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it.
- They are incorporated in networks to expand its coverage area.
- They are also known as Signal boosters.



- Repeaters amplifies the attenuated signal and then retransmits it.
- Digital repeaters can even reconstruct signals distorted by transmission loss.
- So, repeaters are popularly incorporated to connect b/w two LANs forming a large signal LAN. This is shown below.

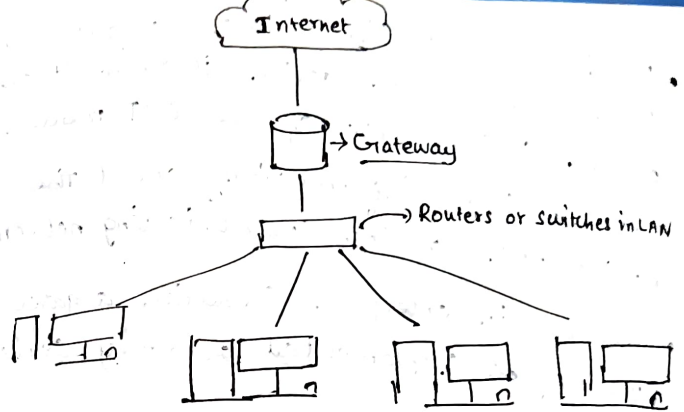


★ Types of Repeaters

- According to the type of Signals
  - Analog Repeater – Amplify analog signal
  - Digital Repeater – reconstruct a distorted signal
- According to the type of networks
  - Wired Repeater – used in wired LANs
  - Wireless Repeater – used in wireless LANs & cellular networks
- According to the type of domain of LANs
  - Local Repeater – They connect LAN segments seperated by small distance.
  - Remote Repeater – They connect LANs that are far from each other

★ Gateways

- Gateways connect two networks and manages all the data that inflows and outflows from that network.



Gateway b/w LAN and Internet

eg) Modem

★ features of Gateways

- Gateway is located at the boundary of a network and manages all data that inflows or outflows from the network.
- It forms a passage between two different networks operating with different transmission protocols.
- A gateway operates as a protocol converter, providing compatibility b/w the different protocols used in the two different networks.

- The feature that differentiates a gateway from other network devices is that it can operate at any layer of the OSI model.
- It also stores information about the routing paths of the communicating networks.
- When used in enterprise scenario, a gateway node may be supplemented as proxy server or firewall.
- A gateway is generally implemented as a node with multiple NICs (network interface cards) connected to different networks. However, it can also be configured using software.
- It uses packet switching technique to transmit data across the networks.

*Types of Gateways

- Unidirectional
- Bidirectional

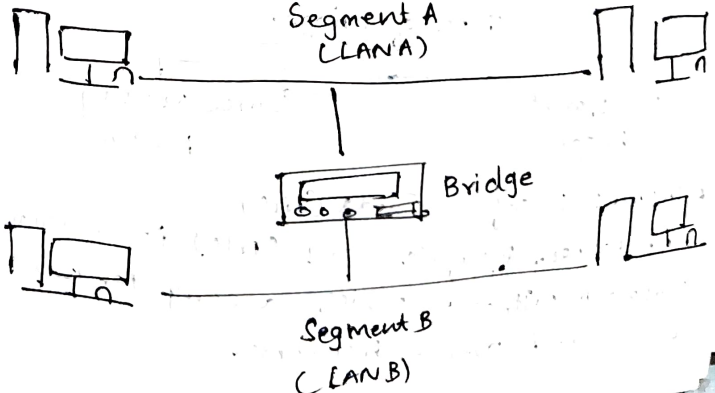
→ archiving tools
→ direction of data flow basis
→ synchronization tools.

- Network Gateway
- Cloud Storage Gateway
- Internet to IoT Gateway
- IoT gateway
- VoIP Trunk Gateway

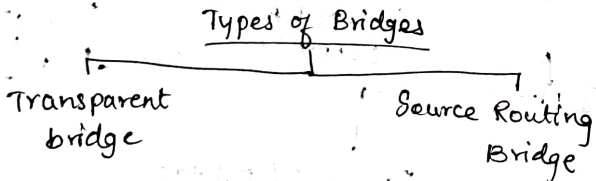
} Basis of functionalities

*Bridges

- It is used to connect two subnetworks that use interchangeable protocols.
- It combines two LANs to form an extended LAN. The main diff b/w a bridge and repeater is that the bridge has a penetrating efficiency.



- Bridges are used to divide large busy networks into multiple smaller and interconnected networks to improve performance.
- A bridge accepts all the packets and amplifies all of them to the other side.
- The bridges are intelligent devices that allow the passing of only selective packets from them.
- A bridge only passes those packets addressed from a node in one network to another node in the other network.



★ Network Interface Cards (NIC)

- A network interface card (NIC) is a hardware component without which a computer cannot be connected over a network.
- It is a circuit board installed in a computer that provides a dedicated network connection to the computer.
- It is also called Network Interface Controller (NIC), network adoptor, or LAN adapter.

Types of NIC.

- Internal Network card
- External Network card

i. Internal Network card:

- The motherboard has a slot for the network card where it can be inserted.
- It requires network cables to provide network access.
- Internal network cards are of two types
- The first type uses peripheral Component Interconnect (PCI) connection, while the second type uses Industry Standard Architecture (ISA).

ii. External Network Card

- In desktops and laptops that do not have an internal NIC, external NICs are used.
- External network cards of two types
  i. Wireless and ii. USB based
  i. Wireless network card needs to be inserted into the motherboard, however no network cable is required to connect to the network.
- They are useful while travelling or accessing a wireless signal.

* Purpose of Using Network Interface Card

- NIC allows both wired and wireless communication
- NIC allow communications b/w computers connected via local area network (LAN) as well as communications over large-scale network through Internet Protocol (IP).
- NIC is both a physical layer and a data link layer device, i.e., it provides the necessary hardware circuitry so that the physical layer processes and some data link layer processes can run on it.

* Types of Servers in Computing

i. Web Server
ii. Database Server
iii. Email Server
iv. Web Proxy Server
v. DNS Server
vi. FTP Server
vii. File Server
viii. DHCP Server
ix. Cloud Server
x. Application Server
xi. Print Server
xii. NTP Server
xiii. Radius Server
xiv. Syslog Server
xv. Physical Server

* Advantages of NIC

1. Faster network Speed
2. Reliability
3. Security
4. Compability
5. lower CPU usage

* Disadvantages of NIC

1. Limited transfer speed
2. Limited compatibility
3. Driver issues
4. Cost
5. Power consumption
6. Maintenance
7. Security risks.

* Web Server

- A Server that is in charge of publishing a website on the internet is known as Web server.
- A server that provides hosting, also called "hosting", over the internet protocol is called Web server.

* Types of Web Server

1. Apache HTTP Server
2. Internet Information Services
3. Light tpd
4. Nginx
5. Sun Java System Web Server

* Database Server

- A database server manages a database and provides database services to clients.
- The server manages data access and retrieval as well as the completion of client requests.
- A database server is a computer that runs database software and is dedicated to providing database services.

* Types of Database Servers

1. oracle
2. IBM DB2
3. Microsoft SQL Server
4. MySQL
5. SAP HANA
6. MS Access

* Mail Server

- A mail server, also known as an email server, is a computer system that sends and receives emails.
- When you send an email, it passes through several servers before arriving at its destination.

Mail servers — i. outgoing mail server.
ii. Incoming " "

i. Outgoing mail server

SMTP : Simple Mail Transfer Protocol, which handles all incoming mail and sends emails.

ii. Incoming mail server

IMAP / POP3 : Post Office Protocol version 3 (POP) Server are well-known for getting computer's inbox contents.

- IMAP servers, which stands for Internet Message ~~Access~~ Access Protocol, are used for one-way mailbox Synchronization.

* Web Proxy Server

- A proxy server is a web server that serves as a conduit between a client program, such as a browser, and the actual server.
- It sends queries to the accurate server on the client's behalf and sometimes fulfills the claim itself.
- Web proxy servers offer two key functions: They filter Requests and increase Performance

* Benefits of using Web Proxy Server

1. More Privacy
2. Access to restricted websites
3. Improved performance & bandwidth savings
4. Enhanced Security

* Most popular and greatest web proxy server

1. Smart Proxy
2. Bright Data
3. HMA
4. Whoer
5. Hide.me

★ DNS Server

- The Domain Name System (DNS) is the Internet's telephone directory.
- DNS is responsible for finding the correct IP address for websites when users enter their domain names, such as 'google.com' or 'nytimes.com' into web browsers.
- The addresses are then used by browsers to communicate with origin servers or CDN edge servers to access website information.
- All this is possible by DNS Servers, which are specialized machines for answering DNS queries.
- To resolve names, the DNS system has resolving systems.
- Name resolvers are used to find IP addresses associated with domain names.

- DNS clients are the people who use resolvers.
- A DNS system can have many name resolvers.
- As a result, if one of them become incapacitated the others take over and ensure that communication is not disrupted.