27-12-2024

DAY 04

★IP Addressing

- IPV4 & IPV6

→IPV4 - 32 Bit Address - 2^{32} - 4.29 billion
(or)
429 crore
IP addresses

World population - 8 billion Netizens
- 2 to 2.5 billion

- IPV6 - Trillion and Trillions of IP's

1. The IPV4 addressing mode has 32 bits

0.0.0.0 to 255.255.255.255

00000000.00000000.00000000.00000000 to 11111111.11111111.11111111.11111111

10.0.0.255 – 00001010.00000000.00000000.11111111

10.0.1.0 : 00001010.00000000.00000001.00000000

2. 5 Different classes.

Class A – 0.0.0.0 to 127.255.255.255 – 128.0.0.0 addresses

Class B – 128.0.0.0 to 191.255.255.255 – 64.0.0.0 addresses

Class C – 192.0.0.0 to 233.255.255.255 – 32.0.0.0 addresses

Class D – 224.0.0.0 to 239.255.255.255 – 16.0.0.0 addresses

Class E – 240.0.0.0 to 255.255.255.255 – 16.0.0.0 addresses

★ FTP Server

i. FTP is a network protocol that is used to transfer files between a client and a server on a computer network.

ii. FTP is a well-known protocol that was developed in the 1970s to allow two computers to transfer data over the internet.

iii. One computer servers as the server, storing information, while the others servers as the client, sending or requesting files from the server.

iv. The FTP protocol's primary mode of communication is normally port 21. On port 21, an FTP server will accept client connections.

v. FTP servers, as well as the more secure SFTP server Software, carry out two basic functions: "Put" and "Get".

vi. An FTP server is useful if you have remote employees who need to submit non-confidential material (such as timesheets) or if you wish to allow your clients to obtain white papers and documentation.

★ File Server

- A File Server is a central server in a computer network that serves File Systems or portions of file systems to clients connected to the network.
- As a result, file servers provide users with a central storage location for files on internal data media that is available to all authorized clients.
- The server administrator establishes rigorous guidelines for which users have which access rights; for Example: The configuration of file authorizations of the individual file system allow the admin to specify which files a certain user or user group may access and open, as well as whether data can only be seen or additionally added, altered, or deleted.

★ DHCP Server

1. A DHCP Server is a network server that gives and assigns IP addresses, default gateways, and other network information to client devices on an automatic basis.
2. To reply to client broadcast inquiries, it uses the standard Protocol known as Dynamic Host Configoration Protocol or DHCP.
3. A DHCP server automatically sends the network parameters required for clients to communicate successfully on the network.
4. Without it, the network administrator must manually configure each client that connects to the network, which can be time-consuming, especially in big networks.
5. DHCP Servers typically assign a unique dynamic IP address to each client, which changes when the client's lease for the IP address expires.

★ Cloud Server

- A cloud server is a pooled, centralized server resource that is hosted and distributed across a network - typically the internet - and may be accessed by multiple users on demand.
- Cloud servers provide all of the same services as traditional physical servers, including processing power, storage & applications.
- Cloud servers can be situated anywhere in the world & provide remote services via a cloud computing environment.
- Traditional dedicated server hardware, on the other hand, is often installed on premises for the sole use of one firm.
- Because any software issue is isolated from your environment, a cloud server is used.
- Other cloud servers will have no impact on yours, and vice versa.

★ Application Server

- An application server is software that runs on the server and is written by a server programmer to provide business logic for any application.
- This server might be part of a network or a dispersed network.
- Server programs are typically used to give services to client programs that are either on the same system or a network.
- Application servers reduce traffic while increasing security.
- It is not possible to achieve ideal web server agility by handling both HTTP requests from web clients & pasting or storing resources from numerous websites.
- Application servers fill this need with a powerful architecture designed to handle dynamic online content requests.
- Application servers provide programs with protection & redundancy.

* Advantages of Application Server.

1. Provides a framework for managing all components and operating services.
2. They make it simple to deliver patches and security upgrades.
3. It allows you to route requests to other servers based on their availability. Load balancing is used to accomplish this.
4. It ensures the security of applications. It allows for fault tolerance as well as recovery/failover recovery.
5. It saves us a lot of time.
6. The application server dramatically enhances application performance.

* Print Server

i. A print Server is a software program, network device, or a computer that manages print requests and provides end users and network administrators with printer queue status information.

ii. Print Servers are used in big business network as well as small or home office (SOHO) networks.

iii. A single dedicated computer operating as a print server, in a large firm manages hundreds of printers.

iv. A print server in a small office is generally a customized plug-in board or tiny network device the size of a hub that serves the same function as a dedicated print server while freeing up critical disk space on the workplace's limited number of PCs.

v. A print Server, like other Servers, works on the client-server arch, receiving and processing user requests.

* NTP Server

> Network Time Protocol (NTP) is an Internet protocol that is used to Synchronize with Computer clock time sources in a network.

> It belongs to and is one of the earliest components of the TCP / IP Suite.

> The word NTP refers to both the protocol and the Client-Server applications that operate on computers.

> It is intended to be extremely fault-tolerant and scalable, while also allowing temporal Synchronization.

The NTP time Synchronization procedure consist of 3 steps:

1. The NTP Client conducts a time-request exchange with the NTP Server.
2. The client may then determine the connection latency and its local offset, as well as change its local time to match the clock on the Server's computer.
3. Typically, six exchanges over a five to ten minute period are required to set the clock.

* Radius Server

- Radius (Remote Authentication Dial-In User Service) is a networking protocol that connects clients and servers.
- RADIUS is a computer network authentication, authorization, and accounting (AAA) management Protocol.
- RADIUS is a UDP-based protocol that authenticates users using a shared secret.
- The Radius protocol employs a Radius Server and Radius Clients.
- Radius Server: checks User's credentials against a database of usernames & passwords.

- It also grants network resources access.
- Radius client : A network - connected device that provides its credentials to the Radius Server.
- After that, the radius Server authenticates the client and returns authorization or access control information to it.
- To establish an authentication session, the radius Server, and client exchange messages.
- This Session is used for duties such as authorization, bookkeeping and others.

(*) RADIUS Authentication Methods

- The RADIUS Server offers a variety of authentication techniques.
- When supplied with the user's username and original password, it can support PAP, CHAP, MS-CHAP, EAP, EAP TLS, UNIX login, and other authentication protocols.
- PAP: Password Authentication Protocol Authentication
  - It configures authentication using PPP configuration files and the PAP database.
  - PAP works similarly to the UNIX login software, However, PAP does not allow the user shell access.
- CHAP: Challenge - Handshake Authentication Protocol Authentication employs challenge and response, which means that the authenticator challenges the caller (authenticates) to prove their identity.
- The challenge includes the authenticator's unique ID and a random number.

- The caller generates the answer (handshake) to send to the peer using the ID, random number, and CHAP security credentials.
- MS-CHAP: MS-CHAP is the Microsoft Challenge-Handshake Authentication Protocol
  - It is used as an authentication option in Microsoft's PPTP protocol implementation for VPNs.
- EAP: Extensible Authentication Protocol
  - It is a wireless network and point-to-point connection authentication mechanism.

★ Syslog Server

> The System Logging Protocol (Syslog) is a standard message format used by network devices to connect with a logging server.

> It was created primarily to make monitoring network devices simple.

> Devices can use a Syslog agent to send out notification messages under a variety of scenarios.

> These log messages comprise a timestamp, a severity rating, a device ID (including IP address), and event-specific information.

> Though it has flaws, the Syslog protocol is extensively used because it is simple to reconstruct and very open-ended, allowing for a variety of proprietary implementations and hence the ability to monitor practically any connected device.

The Syslog standard specifies three layers:

- Syslog Content Layer: This is the content in the event message.

> It includes several data items such as facility codes and severity ratings.

- Syslog Application Layer: The message is generated, interpreted, routed and stored in this layer.
- Syslog Transport Layer: This layer is responsible for sending messages across a network.

★ Physical Server

> Some Servers are solely utilized for specific functions.

> An Application Server, for ex, just hosts the webpage.

> Physical Servers are easy to use for a wide range of network tasks because of their software and hardware.

Some of those transactions are:

1. Operating System updates
2. Services for firewalls
3. Anti-Spam software
4. Antivirus Software
5. Defense against DDoS assaults
6. DNS hosting
7. Intrusion detection
8. SNMP management
9. Database administration
10. Backups and restoration
11. Security procedures

★ IP Address and Subnets

• Subnetting is the process of dividing a large network into smaller networks called as "Subnets". Subnets provide each group of devices their own space to communicate, that ultimately helps network to work easily.

• This also boosts security and makes it easier to manage the network, as each subnet can be monitored and controlled seperately.

⊙ Subnet

> A Subnet is like a smaller group within a large network.

> It is a way to split a large network into smaller networks so that devices present in one network can transmits data more easily.

> For eg) In a company, different departments can each have their own subnet, keeping their data traffic seperate from others.

> Subnet makes the network faster and easier to manage and also improves the

Security of the network.

★ Why Subnetting Necessary?

- Subnetting helps in organizing the network in an efficient way which helps in expanding the technology for large firms and companies.
- Subnetting is used for specific staffing structures to reduce traffic and maintain order and efficiency.
- Subnetting divides domains of the broadcast so that traffic is routed efficiently, which helps in improving network performance.
- Subnetting is used to increase network security.

★ what is Subnet Mask

- A Subnet mask is a 32-bit number used in IP addressing to seperate the network portion of an IP address from the host portion.
- It helps computers and devices determine which part of an IP address refer to the network they are present, and which part refers to their Specific location or address within the network.

. It helps computers and devices determine which part of an IPaddress refer to the network they are present, and which part refers to their Specific location or address within the network.

★ Advantages

1. It provides Security to one network from another network. eg) In an organization, the code of the Developer department must not be accessed by another department.

2. It may be possible that a particular Subnet might need higher network priority than others. For eg, a sales department needs to host webcasts or video conferences.

3. In the case of Small networks, maintenance is easy.

★ Disadvantage

1. In the case of a single network, only three steps are required to reach a Process i.e., Source Host to Destination Network, Destination Network to Destination Host, and then Destination Host to Process.

2. In the case of a Single Network, only two IP. addresses are wasted to represent network ID and broadcast address but in the case of subnetting two IP addresses are wasted for each subnet.

3. The cost of the overall Network also increases. Subnetting requires integral routers, Switches, Hubs, Bridges, etc. which are very costly.