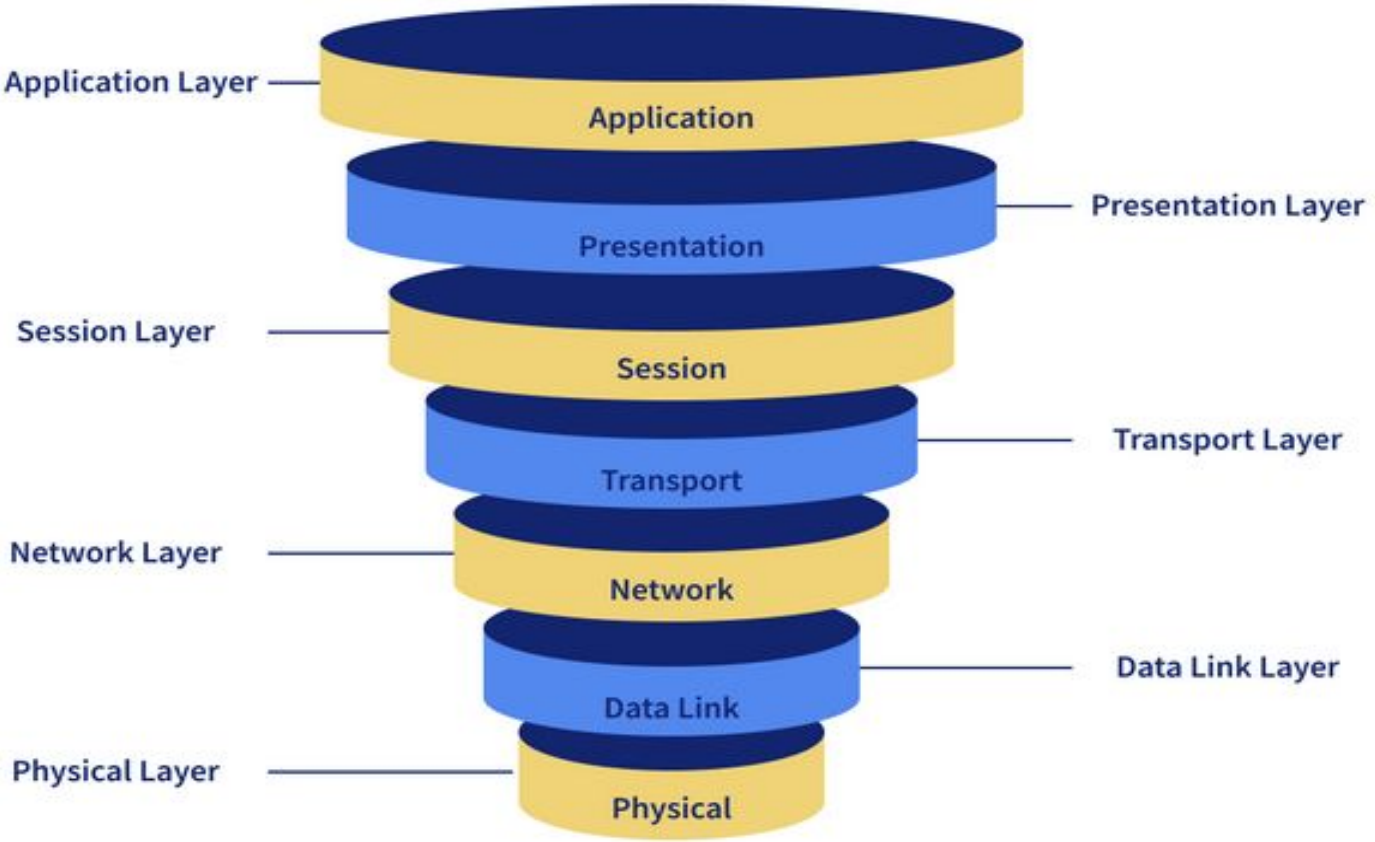
NETWORKING In CLOUD COMPUTING

By Vignesh

OSI Model


Application Layer
Application
Presentation Layer
Presentation
Session Layer
Session
Transport Layer
Transport
Network Layer
Network
Data Link Layer
Data Link
Physical Layer
Physical

Router

A router is a networking device that connects multiple networks together and directs network traffic between them.

It operates at the network layer (Layer 3) of the OSI model and uses IP addresses to forward packets between networks.

Routers play a crucial role in connecting devices within a network and facilitating communication between different networks, such as connecting a local network to the internet

Routers are responsible for determining the best path for data packets to reach their destination.

Firewall

A firewall is a security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between an internal network and external networks, filtering and blocking unwanted or unauthorized traffic. Firewalls play a crucial role in network security.

Traffic Filtering: Firewalls examine network traffic based on specific criteria, such as source and destination IP addresses, port numbers, protocols, and packet contents. They use this information to make decisions on whether to allow or block the traffic.

(Proxy Firewalls): Some advanced firewalls act as application-level gateways or proxy servers. They inspect network traffic at the application layer and provide more granular control over specific protocols or applications, offering enhanced security and filtering capabilities.

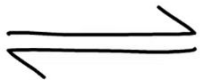
NAT (Network Address Translation)

NAT is a technique used to translate IP addresses between different networks. NAT plays a crucial role in conserving IP address space and providing a layer of security.

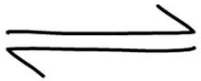
In a local network, devices are typically assigned private IP addresses

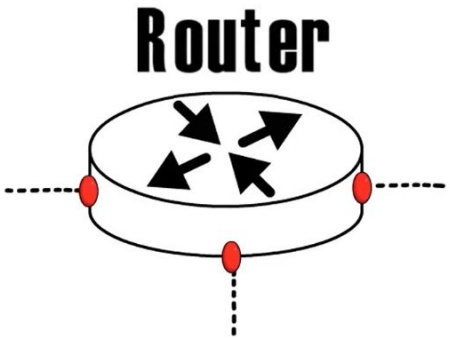
These private IP addresses are not routable on the internet. And connects to the internet through a router or gateway device that has a public IP address.

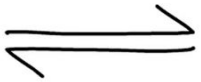
When a device on the local network wants to communicate with a device on the internet, NAT comes into play. The NAT device replaces the private IP address of the requesting device with its public IP address before forwarding the packet to the internet



IP Datagrams

IP addresses  Interface





IP Datagrams

INTERNET PROTOCOL ADDRESS

- An IP address is a unique numerical label that uses the Internet Protocol for communication.
- It serves two primary purposes: identifying the host or network interface and providing the location of the device in the network.
- IP addresses are typically represented in a format called IPv4 (e.g., 192.168.0.1).
- Each set can range from 0 to 255, providing a total of around 4.3 billion unique addresses.

BINARY NUMBERS

- Binary numbers are a numeral system that uses only two symbols: 0 and 1. It is commonly used in computing and digital systems because it directly corresponds to the on/off states of electronic switches
- Example: Convert the binary number 011110110 to decimal.
- 1 1 1 1 0 1 1 0
- 2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0
- 1x128 + 1x64 + 1x32 + 1x16 + 1x8 + 1x4 + 1x2 + 1x1
- Therefore, the binary number 11110110 is equivalent to the decimal number 246.
- Example: Convert the decimal number 37 to binary.
- We have to divide the number until the quotient becomes zero
- The remainders in reverse order are 100101, so the decimal number 37 is equivalent to the binary number 100101.

Binary Number System

'o' and 'ı'

oolooloı

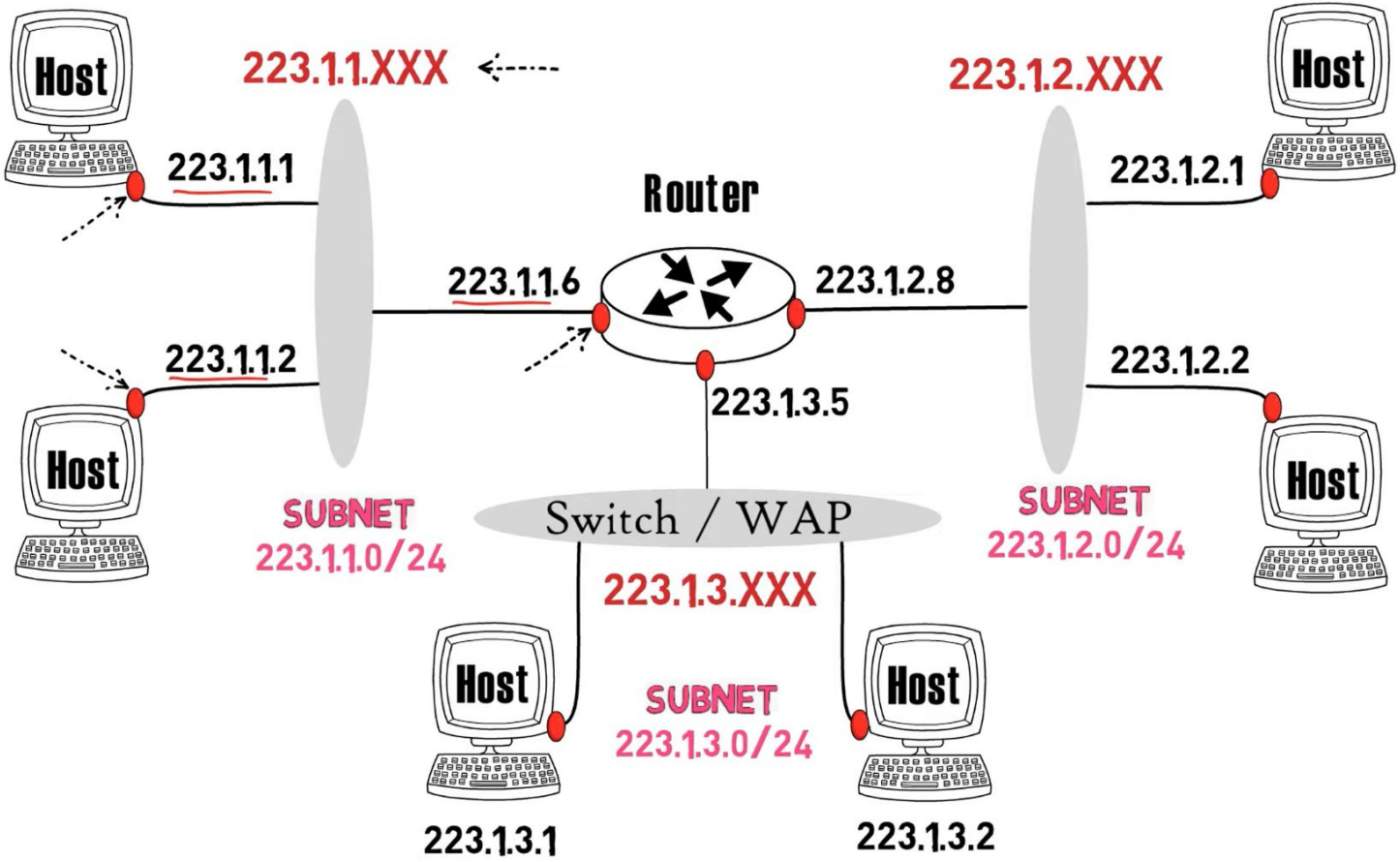
8-bit in length

IPv4

IIOOOOOI OOIOOOOO IIOIIOOO OOOOIOOI

SUBNETTING

- Subnet addressing, is a technique used to divide a larger network into smaller sub networks or subnets.
- It helps in better control of network traffic and security.
- A portion of the IP address is reserved for network identification, and the remaining portion is used to identify specific hosts within that network
- Subnet masks are used to determine the boundary between the network and host portions of an IP address. The subnet mask consists of a series of binary digits with 1s representing the network bits and 0s representing the host bits.


Host
223.1.1.XXX
223.1.2.XXX
Host
223.1.1.1
223.1.2.1
Router
223.1.1.6
223.1.2.8
223.1.1.2
223.1.2.2
223.1.3.5
Host
Host
SUBNET
223.1.1.0/24
Switch / WAP
SUBNET
223.1.2.0/24
223.1.3.XXX
Host
Host
SUBNET
223.1.3.0/24
223.1.3.1
223.1.3.2

Why?

1. **Efficient utilization of IP addresses**: conserve IP address space and prevents wastage.
2. **Network segmentation and organization:** segmentation improves network performance by reducing network congestion and isolating traffic within specific segments
3. **Enhanced network security**: By placing devices with similar security requirements or belonging to the same department in the same subnet, it becomes easier to implement security measures and control access between subnets
4. **Improved network performance:**In a network without subnetting, every device receives broadcast traffic sent by any device on the network, which can lead to increased network congestion and decreased performance.
5. **Scalability and flexibility**:Subnetting provides scalability and flexibility for network design and expansion.

Class A:

- Range: 1.0.0.0 to 126.0.0.0
- Default Subnet Mask: 255.0.0.0 (/8)
- Subnetting: Class A networks are generally used for large-scale networks. They have a default allocation of 16,777,214 host addresses. Subnetting a Class A network involves borrowing bits from the host portion to create multiple subnets with smaller ranges of IP addresses.

Class B:

- Range: 128.0.0.0 to 191.255.0.0
- Default Subnet Mask: 255.255.0.0 (/16)
- Subnetting: Class B networks are used for medium-sized networks. They provide a default allocation of 65,534 host addresses. Subnetting a Class B network involves dividing the network into smaller subnets by borrowing bits from the host portion.

Class C:

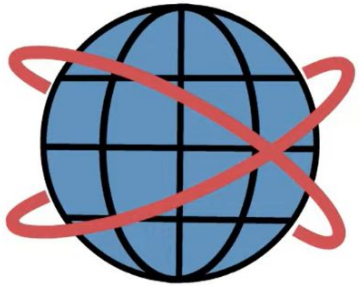
- Range: 192.0.0.0 to 223.255.255.0
- Default Subnet Mask: 255.255.255.0 (/24)
- Subnetting: Class C networks are used for small-scale networks. They offer a default allocation of 254 host addresses. Subnetting a Class C network involves dividing the network into multiple subnets by borrowing bits from the host portion.

CIDR

- CIDR stands for Classless Inter-Domain Routing. It is a method used to allocate and specify IP addresses and their associated routing information in computer networks.
- In CIDR notation,

  IP address is represented as a combination of the network address and the prefix length. The prefix length indicates the number of bits in the network portion of the address.

  For example, in the CIDR notation "192.168.0.0/24," the "/24" indicates that the first 24 bits of the IP address represent the network address.

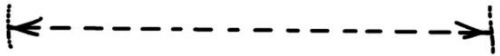


Classless Interdomain Routing

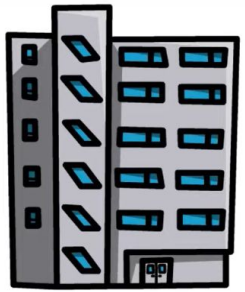
CIDR

Subnet Address : a.b.c.d/x

11001000 00010111 00010000 00000000



Network prefix



Organisation IP block

200.23.16.0/20

X = 20

Binary form

11001000 00010111 00010000 00000000

Subnet 0	200.23.16.0/23	11001000 00010111 00010000 00000000
Subnet 1	200.23.18.0/23	11001000 00010111 00010010 00000000
Subnet 2	200.23.20.0/23	11001000 00010111 00010100 00000000

PROBLEM:

IP address range 192.168.0.0/24 and we want to create subnets for four departments in an organization. Each department requires at least 30 host addresses.

Procedure

STEP1 : Determine number of bits?____ Since we need at least 30 host addresses per subnet, we need to find the closest power of 2 that is 32 (2^5)

STEP2 : Subtract bits from original bits____ the original network had 24 bits. Subtracting 5 bits for the host addresses leaves us with 19 bits for the network portion.

STEP3 : Calculate the subnet mask____ The subnet mask is determined by the number of network bits. In this case, the subnet mask is 255.255.255.224 (which corresponds to /27

STEP4 : Assign the Subnets

- Subnet 1: 192.168.0.0/27 (30 usable host addresses)
- Subnet 2: 192.168.0.32/27 (30 usable host addresses)
- Subnet 3: 192.168.0.64/27 (30 usable host addresses)
- Subnet 4: 192.168.0.96/27 (30 usable host addresses)

IMPORTANT PROTOCOLS

- **TCP:TCP (Transmission Control Protocol):** It ensures reliable, ordered, and error-checked delivery of data packets between devices over a network. TCP breaks data into packets, sends them to the destination device, and reassembles them in the correct order.
- **UDP (User Datagram Protocol):** It is an alternative to TCP that provides a connectionless protocol for sending datagrams across networks. Unlike TCP, UDP does not guarantee reliable delivery or ordered packets, but it is faster and more efficient for certain types of applications.
- **ICMP (Internet Control Message Protocol):** It handles diagnostic and error reporting messages, such as ping requests and error notifications, between network devices.
- **ARP (Address Resolution Protocol):** It maps an IP address to a physical MAC (Media Access Control) address on a local network.

- **HTTP (Hypertext Transfer Protocol):** HTTP is used for transmitting web pages, API requests, and other data over the internet. It is the foundation of communication between web browsers and web servers, making it crucial for cloud-based applications and services.
- **HTTPS (Hypertext Transfer Protocol Secure):** HTTPS is a secure version of HTTP that uses encryption (SSL/TLS) to protect data transmitted between clients and servers. It ensures secure communication for web-based applications and is especially important for cloud-based services handling sensitive data.
- **DNS (Domain Name System):** DNS translates domain names into IP addresses, allowing users to access cloud services using human-readable domain names instead of IP addresses. Understanding DNS is vital for configuring domain names, managing DNS records, and ensuring proper connectivity in cloud environments.

- **SSH (Secure Shell):** SSH is a cryptographic network protocol that provides secure remote access to devices over an unsecured network. It enables secure login, command execution, file transfer, and tunneling. SSH ensures confidentiality and integrity of data during communication.

- **RTP (Real-time Transport Protocol):** RTP is a protocol specifically designed for real-time transmission of multimedia data, such as audio and video. It provides mechanisms for timing, sequencing, and error recovery to ensure smooth playback of real-time media streams over IP networks.

- **FTP (File Transfer Protocol):** FTP is a protocol used for transferring files between systems over a network. It provides a set of commands for file operations, directory listing, and file transfer. FTP can operate in active or passive mode depending on the network configuration

CLOUD NETWORKING CONCEPTS

- **Load Balancing:** Load balancing refers to the distribution of network traffic across multiple servers or resources to optimize performance and ensure high availability. It helps evenly distribute incoming requests and prevent any single resource from becoming overwhelmed. Load balancers can be implemented at various levels, such as application-level load balancing or network-level load balancing.
- **Content Delivery Networks (CDNs)**: CDNs are geographically distributed networks of servers that deliver web content and other digital assets to users based on their geographic location. CDNs store cached copies of content in multiple locations, reducing latency and improving content delivery speed. When a user requests content, the CDN serves it from the closest server, minimizing the distance data needs to travel.

VIRTUAL PRIVATE CLOUD

A Virtual Private Cloud (VPC) is a virtual network infrastructure within a public cloud provider's environment. It provides users with the ability to create and manage their own isolated network environment in the cloud.

With Amazon VPC, users have complete control over their virtual networking environment:

Selection of IP address ranges

Creation of subnets,

Configuration of route tables,

Management of network gateways.

It allows users to create a virtual network topology that closely resembles a traditional on-premises network architecture, providing familiarity and flexibility in cloud network design.

FEATURES

Subnets: Users can divide their VPC into one or more subnets to segment and isolate resources. Each subnet can be associated with a specific availability zone, allowing users to distribute their resources across multiple data centers for high availability and fault tolerance.

Internet Gateway: Amazon VPC provides an Internet Gateway that serves as a connection point between the VPC and the internet. It enables resources within the VPC to communicate with the internet and vice versa.

Route Tables: Users can define custom route tables to control traffic between subnets and gateways within the VPC. Route tables determine the path that network traffic takes within the VPC.

Network Address Translation (NAT) Gateway: NAT Gateway allows private subnets within the VPC to access the internet while keeping the instances within those subnets hidden behind a public IP address.

FEATURES

Security: Amazon VPC integrates with AWS Identity and Access Management (IAM) to provide fine-grained access control and security. Users can define network security groups to control inbound and outbound traffic at the instance level, as well as network ACLs (Access Control Lists) to control traffic at the subnet level.

VPN Connectivity: Amazon VPC supports secure connectivity options, including Virtual Private Network (VPN) connections, which allow users to establish encrypted connections between their on-premises networks and their VPCs.

Amazon VPC provides a secure and scalable environment for deploying a wide range of AWS resources, such as Amazon EC2 instances, RDS databases, and Elastic Load Balancers, within a user-defined network infrastructure. It enables organizations to extend their on-premises networks seamlessly into the cloud while maintaining control over their network configuration and security settings.

THANK YOU !!