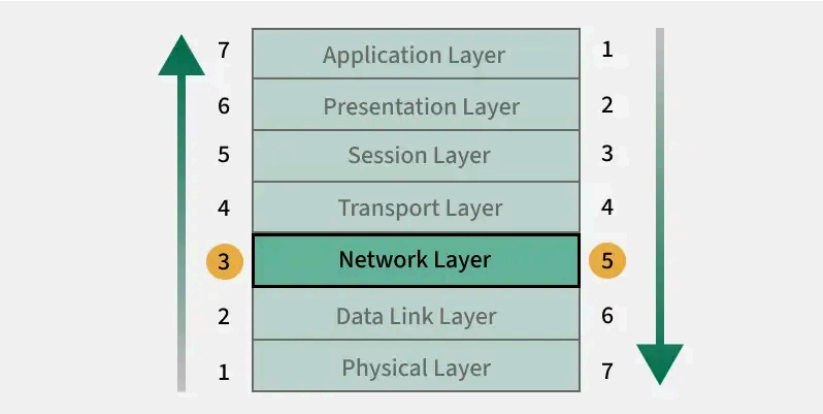
Network Layer in OSI Model

Last Updated : 27 Jan, 2025

The Network Layer is the 5th Layer from the top and the 3rd layer from the Bottom of the OSI Model. It is one of the most important layers which plays a key role in data transmission. The main job of this layer is to maintain the quality of the data and pass and transmit it from its source to its destination. It also handles routing, which means that it chooses the best path to transmit the data from the source to its destination, not just transmitting the packet. There are several important protocols that work in this layer.



Network Layer in OSI Model

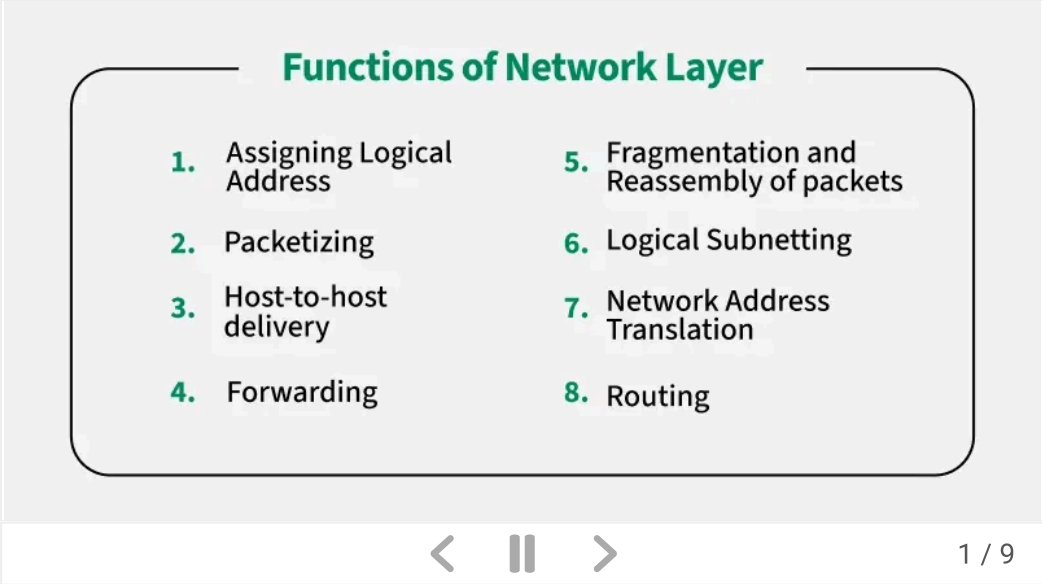
Data is transmitted in the form of packets via various logical network pathways between various devices. It offers routes for data packet transfers across the network. The network layer is also responsible for organizing and controlling the available paths for data transfer.

Functions of Network Layer

Some of the most important functions of the network layer are given below :

1. **Assigning Logical Address**: It provides unique IP addresses to devices for identification and communication across networks.

2. **Packetizing**: It encapsulates data into packets for efficient transmission.
3. **Host-to-Host Delivery**: It ensures data is delivered from the sender to the intended receiver across networks.
4. **Forwarding**: It is the process of moving packets from the input to the appropriate output interface in a router, based on the destination address
5. **Fragmentation and Reassembly**: It splits large packets into smaller fragments for transmission and reassembles them at the destination.
6. **Logical Subnetting**: It divides larger networks into smaller subnetworks for better management and routing efficiency.
7. **Network Address Translation (NAT)**: Maps private IP addresses to a public IP for internet access, conserving IPs and adding security.
8. **Routing**: It determines the best path for packets to travel to their destination across multiple networks.



Read more about Functions of Network Layer.

How Does the Network Layer Work?

- Every device gets a unique address (IP address) to identify it on the network.
- Data is packaged into small packets, with labels showing where it's coming from and where it's going.

- Routers figure out the best path to send the packets to their destination.
- Packets travel step by step through different routers until they reach the right device.
- If a packet is too big, it gets broken into smaller pieces to fit through the network.
- At the destination, the pieces are put back together into the original data.
- If something goes wrong, like the destination can't be reached, an error message is sent back.

Protocols Used at Network Layer

The **protocols used at the Network Layer** are:

1. **IP (Internet Protocol)**
2. **ICMP (Internet Control Message Protocol)**
3. **ARP (Address Resolution Protocol)**
4. **RARP (Reverse Address Resolution Protocol)**
5. **NAT (Network Address Translation)**
6. **Routing Protocols**:
   - **RIP (Routing Information Protocol)**
   - **OSPF (Open Shortest Path First)**
   - **BGP (Border Gateway Protocol)**
7. **IPSec (Internet Protocol Security)**
8. **MPLS (Multiprotocol Label Switching)**

Advantages of Network Layer

- Using the network layer in the OSI paradigm offers a multitude of advantages. Let's delve into some of these benefits:
- The network layer takes the data and breaks it down into packets, which makes transmitting the data over the network easier. This process also eliminates any weak points in the transmission, ensuring that the packet successfully reaches its intended destination.

- Router is the important component of the network layer . Its role is to reduce network congestion by facilitating collisions and broadcasting the domains within the network layer.
- Used to send data packets across the network nodes, the forwarding method is various.

Limitations of Network Layer

- There is no flow control mechanism provided by the network layer design.
- There may be times when there are too many datagrams in transit over the network, causing congestion. This could put further strain on the network routers. In some circumstances, the router may lose some data packets if there are too many datagrams. Important data may be lost in the process of transmission as a result of this.
- Indirect control cannot be implemented at the network layer since the data packets are broken up before being sent. Additionally, this layer lacks effective error control systems.

Difference Between Routing and Flooding

Routing	Flooding
A routing table is required.	No Routing table is required
May give the shortest path.	Always gives the shortest path.
Routing is less reliable	Flooding is more reliable
Traffic is less in Routing	Traffic is more in Flooding
Duplicate packets are not present	Duplicate packet are present

For practice, solve quiz on Network Layer

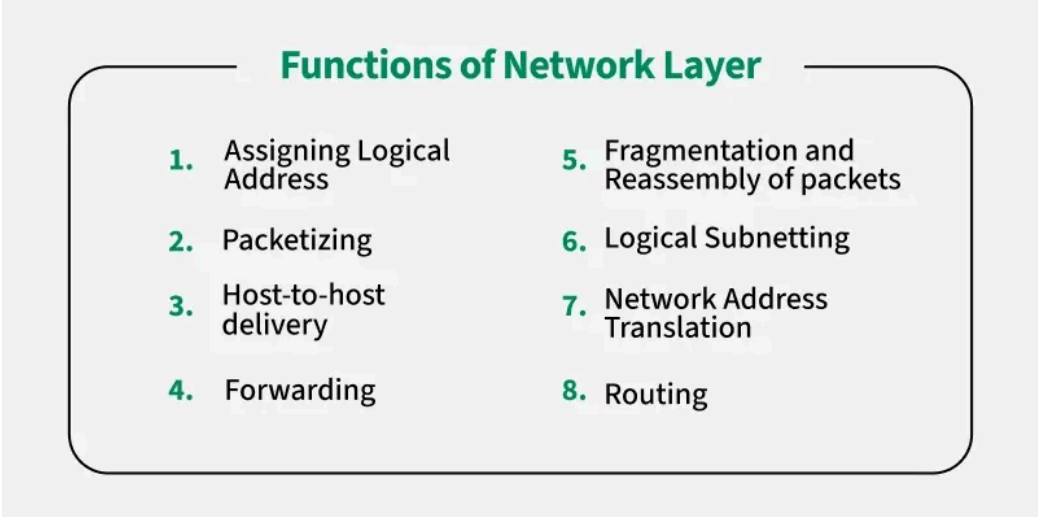
Network Layer Services

Last Updated : 27 Jan, 2025

The network layer is a part of the communication process in computer networks. Its main job is to move data packets between different networks. It helps route these packets from the sender to the receiver across multiple paths and networks. Network-to-network connections enable the Internet to function. These connections happen at the**network layer** which sends data packets between different networks. In the 7-layer OSI model, the network layer is layer 3. The Internet Protocol (IP) is a key protocol used at this layer, along with other protocols for routing, testing, and encryption.

Services Offered by Network Layer

The **services** which are offered by the network layer are as follows:



1. Assigning Logical Address

Logical addressing is the process of assigning unique IP addresses (IPv4 or IPv6) to devices within a n ork. Unlike physical addresses (MAC addresses), logical addr hange based on network

configurations. These addresses are hierarchical and help identify both the network and the device within that network. Logical addressing is important for:

- Enabling communication between devices on different networks.
- Facilitating routing by providing location-based information.

2. Packetizing

The process of encapsulating the data received from the upper layers of the network (also called payload) in a network layer packet at the source and decapsulating the payload from the network layer packet at the destination is known as packetizing.

The source host adds a header that contains the source and destination address and some other relevant information required by the network layer protocol to the payload received from the upper layer protocol and delivers the packet to the data link layer.

The destination host receives the network layer packet from its data link layer, decapsulates the packet, and delivers the payload to the corresponding upper layer protocol. The routers in the path are not allowed to change either the source or the destination address. The routers in the path are not allowed to decapsulate the packets they receive unless they need to be fragmented.

3. Host-to-Host Delivery

The network layer ensures data is transferred from the source device (host) to the destination device (host) across one or multiple networks. This involves:

- Determining the destination address.
- Ensuring that data is transmitted without duplication or corruption.

Host-to-host delivery is a foundational aspect of communication in large-scale, interconnected systems like the internet.

4. Forwarding

Forwarding is the process of transferring packets between network devices such as routers, which are responsible for directing the packets toward their destination. When a router receives a packet from one of its attached networks, it needs to forward the packet to another attached network (unicast routing) or to some attached networks (in the case of multicast routing).The router uses:

- **Routing tables**: These tables store information about possible paths to different networks.
- **Forwarding decisions**: Based on the destination IP address in the packet header. Forwarding ensures that packets move closer to their destination efficiently.

5. Fragmentation and Reassembly of Packets

Some networks have a **maximum transmission unit (MTU)** that defines the largest packet size they can handle. If a packet exceeds the MTU, the network layer:

- **Fragments** the packet into smaller pieces.
- Adds headers to each fragment for identification and sequencing. At the destination, the fragments are **reassembled** into the original packet. This ensures compatibility with networks of varying capabilities without data loss.

Read more about Fragmentation at Network Layer.

6. Logical Subnetting

Logical subnetting involves dividing a large IP network into smaller, more manageable sub-networks (subnets). Subnetting helps:

- Improve network performance by reducing congestion.
- Enhance security by isolating parts of a network.
- Simplify network management and troubleshooting. Subnetting uses subnet masks to define the range of addresses within each

subnet, enabling efficient address allocation and routing.

7. Network Address Translation (NAT)

NAT allows multiple devices in a private network to share a single public IP address for internet access. This is achieved by:

- Translating private IP addresses to a public IP address for outbound traffic.
- Reversing the process for inbound traffic. Benefits of NAT include:
- Conserving IPv4 addresses by reducing the need for unique public IPs for each device.
- Enhancing security by masking internal IP addresses from external networks.

8. Routing

Routing is the process of moving data from one device to another device. These are two other services offered by the network layer. In a network, there are a number of routes available from the source to the destination. The network layer specifies some strategies which find out the best possible route. This process is referred to as routing. There are a number of routing protocols that are used in this process and they should be run to help the routers coordinate with each other and help in establishing communication throughout the network.

Advantages of Network Layer Services

- Packetization service in the network layer provides ease of transportation of the data packets.
- Packetization also eliminates single points of failure in data communication systems.
- Routers present in the network layer reduce network traffic by creating collision and broadcast domains.
- With the help of Forwarding, data packets are transferred from one place to another in the network.

Disadvantages of Network Layer Services

- There is a lack of flow control in the design of the network layer.
- Congestion occurs sometimes due to the presence of too many datagrams in a network that is beyond the capacity of the network or the routers. Due to this, some routers may drop some of the datagrams, and some important pieces of information may be lost.
- Although indirect error control is present in the network layer, there is a lack of proper error control mechanisms as due to the presence of fragmented data packets, error control becomes difficult to implement.

Frequently Asked Questions on Network Layer Services – FAQs

How do routers decide the best path for data packets?

Routers use routing tables and protocols to decide the best path. They consider factors like distance, speed, and network congestion to choose the most efficient route.

What information is in a packet header?

A packet header contains information about the packet, such as the source and destination IP addresses, packet size, and routing information. This helps the network layer manage the packet's journey.

Why is packetizing important?

Packetizing allows data to be transmitted efficiently and reliably. Smaller packets can navigate network paths more easily and can be reassembled at the destination even if they take different routes.

What is an IP Address?

Last Updated : 17 Dec, 2024

Imagine every device on the internet as a house. For you to send a letter to a friend living in one of these houses, you need their home address. In the digital world, this home address is what we call an **IP (Internet Protocol) Address**. It's a unique string of numbers separated by periods (IPv4) or colons (IPv6) that identifies each device connected to the internet or a local network.

Here's the definition:

> ### *What is an IP Address?*
>
> *An IP address, or Internet Protocol address, is a unique string of numbers assigned to each device connected to a computer network that uses the Internet Protocol for communication. It serves as an identifier that allows devices to send and receive data over the network, ensuring that this data reaches the correct destination.*

Types of IP Address

IP addresses can be classified in several ways based on their structure, purpose, and the type of network they are used in. Here's a breakdown of the different classifications of IP addresses:

1. Based on Addressing Scheme (IPv4 vs. IPv6)

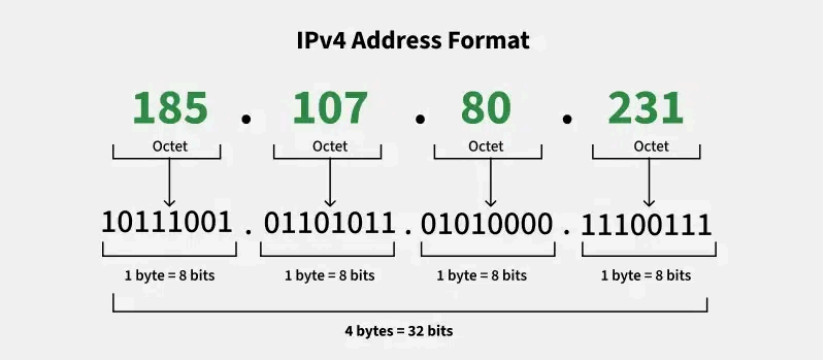
IPv4:

This is the most common form of IP Address. It consists of four sets of numbers separated by dots. For example, 192.158.1.38. Each set of

numbers can range from 0 to 255. This format can support over 4 billion unique addresses. Here's how the structure is broken down:

- **Four Octets**: Each octet represents eight bits, or a byte, and can take a value from 0 to 255. This range is derived from the possible combinations of eight bits (2^8 = 256 combinations).
- **Example of IPv4 Address**: 192.168.1.1
    - **192** is the first octet
    - **168** is the second octet
    - **1** is the third octet
    - **1** is the fourth octet

Each part of the IP address can indicate various aspects of the network configuration, from the network itself to the specific device within that network. In most cases, the network part of the address is represented by the first one to three octets, while the remaining section identifies the host (device).



IPv4 Address Format

IPv6:

IPv6 addresses were created to deal with the shortage of IPv4 addresses. They use 128 bits instead of 32, offering a vastly greater number of possible addresses. These addresses are expressed as eight groups of four hexadecimal digits, each group representing 16 bits. The groups are separated by colons.

- **Example of IPv6 Address**: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

- Each group (like **2001**, **0db8**, **85a3**, etc.) represents a 16-bit block of the address.

For detailed information, refer to this article – ***IPv4 vs. IPv6***

2. Based on Usage (Public vs. Private)

Public IP Addresses

A Public IP address is assigned to every device that directly accesses the internet. This address is unique across the entire internet. Here are the key characteristics and uses of public IP addresses:

- **Uniqueness:** Each public IP address is globally unique. No two devices on the internet can have the same public IP address at the same time.
- **Accessibility:** Devices with a public IP address can be accessed directly from anywhere on the internet, assuming no firewall or security settings block the access.
- **Assigned by ISPs:** Public IP addresses are assigned by Internet Service Providers (ISPs). When you connect to the internet through an ISP, your device or router receives a public IP address.
- **Types:** Public IP addresses can be static (permanently assigned to a

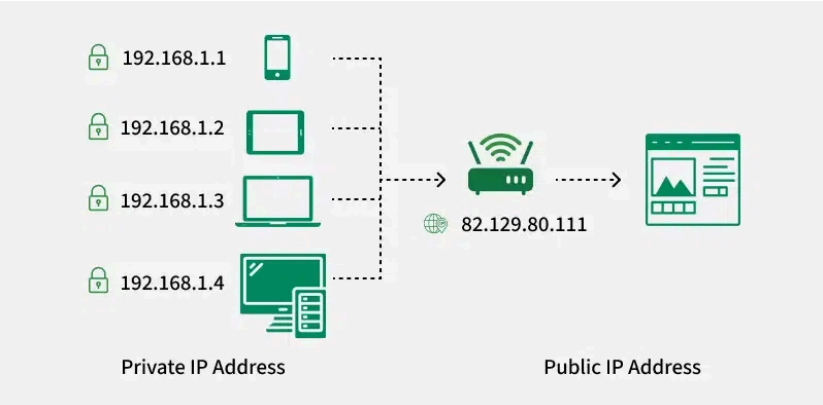
Example Use: *Public IP addresses are typically used for servers hosting websites, email servers, or any device that needs to be accessible from the internet. For instance, if you host a website on your own server at home, your ISP must assign a public IP address to your server so users around the world can access your site.*

Private IP Addresses

Private IP addresses are used within private networks (such as home networks, office networks, etc.) and are not routable on the internet. This means that devices with private IP addresses cannot directly communicate with devices on the internet without a translating mechanism like a router performing Network Address Translation (NAT). Key features include:

- **Not globally unique:** Private IP addresses are only required to be unique within their own network. Different private networks can use the same range of IP addresses without conflict.
- **Local communication:** These addresses are used for communication between devices within the same network. They cannot be used to communicate directly with devices on the internet.
- **Defined ranges:** The Internet Assigned Numbers Authority (IANA) has reserved specific IP address ranges for private use:
    - **IPv4:** 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, 192.168.0.0 to 192.168.255.255
    - **IPv6:** Addresses starting with FD or FC

> ***Example Use:*** *In a typical home network, the router assigns private IP addresses to each device (like smartphones, laptops, smart TVs) from the reserved ranges. These devices use their private IPs to communicate with each other and with the router. The router uses NAT to allow these devices to access the internet using its public IP address.*



3. Based on Assignment: Static vs. Dynamic

Static IP Addresses:

- These are permanently assigned to a device, typically important for servers or devices that need a constant address.
- Reliable for network services that require regular access such as websites, remote management.

Dynamic IP Addresses:

- Temporarily assigned from a pool of available addresses by the Dynamic Host Configuration Protocol (DHCP).
- Cost-effective and efficient for providers, perfect for consumer devices that do not require permanent addresses.

For detailed information, refer to this article – ***Static vs. Dynamic IP Address***

How Do IP Addresses Work?

Here's how IP addresses work:

1. Unique Identification

Every device connected to a network, such as computers, smartphones, and servers, is assigned an IP address. This address is used to identify the device on the network, similar to how a home address identifies a specific location.

2. Communication Protocol

The Internet Protocol (IP), part of the broader suite of internet protocols, uses these addresses to facilitate the routing of data packets between devices. Each piece of data sent over a network is broken into smaller units called packets. Each packet includes both the sender's and the recipient's IP addresses.

3. Data Routing

When a device sends information to another device over the internet:

- The data is divided into packets.
- Each packet contains the IP address of the device it is destined for.
- Routers within the network read the destination IP address on each packet and determine the best path for the packet to travel. Routers communicate with each other to update and maintain records of the fastest, most efficient routes for data.

4. Local Area Networks (LAN) and Wide Area Networks (WAN)

- **LAN:** On local networks, IP addresses can be assigned manually by an administrator (static IP) or automatically by a DHCP server. Devices within the same network communicate directly using their local IP addresses.
- **WAN:** For devices on different networks, the data must travel through multiple routers across the internet. Each router makes independent decisions about the best route for the packets based on the destination IP address.

5. Network Address Translation (NAT)

Most devices on a home or small business network share a single public IP address when accessing the internet, even though each device has its own private IP address within the local network. NAT is a process where multiple local IP addresses are mapped to a single public IP address. This conserves IP addresses and adds a layer of security by hiding internal IP addresses from the external network.

Real World Scenario: Sending an Email from New York to Tokyo

Let’s explore how IP addresses work through a real-world example that involves sending an email from one person to another across the globe:

Step 1: Assigning IP Addresses

- Alice in New York wants to send an email to Bob in Tokyo.
- Alice's laptop has a private IP address (e.g., 192.168.1.5) assigned by her router at home.
- Bob's computer in Tokyo has a private IP address (e.g., 192.168.2.4) assigned by his router at his office.

Step 2: Connection to the Internet

- Both Alice and Bob's routers have public IP addresses assigned by their Internet Service Providers (ISPs). These public IP addresses are what the devices use to send and receive data over the internet.

Step 3: Sending the Email

- Alice writes her email and hits send.
- Her email service (e.g., Gmail) packages the message and its attachments into data packets. Each packet includes the source IP (Alice's router's public IP) and the destination IP (Bob's email server's public IP).

Step 4: Routing the Packets

- The data packets leave Alice's laptop and travel to her home router. The router notes that the destination IP is outside the local network.
- The router sends the packets to Alice's ISP. The ISP uses routers that examine the destination IP address of the packets and determine the best route to send them toward their destination.
- The packets may pass through several routers around the world — in data centers in countries like Canada, Germany, and finally Japan. Each router along the way reads the destination IP and forwards the packets accordingly.

Step 5: Reaching Bob

- The packets arrive at Bob's email server's ISP in Tokyo and are then forwarded to the server.
- Bob's email server reassembles the packets into the original email message.

Step 6: Bob Accesses the Email

- Bob's computer requests the email from his server using his local network IP.
- The server sends the email to Bob's computer, allowing him to read the message Alice sent.

Additional Details

- **NAT (Network Address Translation)**: Both Alice and Bob's routers perform NAT, translating the private IP addresses to and from the public IP addresses when interfacing with the internet. This process is crucial for keeping the number of public IPs needed lower and adds a layer of security by masking internal network structures.
- **Dynamic IP Addressing**: If either Alice or Bob's public IP is dynamic, it might change if they restart their routers. This doesn't affect their ongoing activities much because the DNS (Domain Name System) helps update the mapping of domain names (like gmail.com) to the current IP addresses.

This example illustrates the fundamental role of IP addresses and the complex network of routers involved in even the simplest internet activities like sending an email. Each part of the process depends on the IP address to ensure that data finds its way correctly from sender to receiver, no matter where they are in the world.

—> Other Important Things to Know About IP Address

Classes of IPv4 Address

There are around 4.3 billion IPv4 addresses and managing all those addresses without any classification is next to impossible.

Let's understand it with a simple example. If you have to find a word from a language dictionary, how long will it take just think about it. Usually you will take less than 5 minutes to find that word. You are able to do this because words in the dictionary are organized in alphabetical order. If you have to find out the same word from a dictionary that doesn't use any sequence or order to organize the words, it will take an eternity to find the

word. If a dictionary with one billion words without order can be so disastrous, then you can imagine the pain behind finding an address from 4.3 billion addresses.

For easier management and assignment IP addresses are organized in numeric order and divided into the following 5 classes:

IP addresses are also classified into different classes based on their range and intended use:

- **Class A** (1.0.0.0 to 127.255.255.255):
    - Used for very large networks (like multinational companies).
    - Supports up to 16 million hosts per network.
    - **Example:** `10.0.0.1` (Private IP in this class).
- **Class B** (128.0.0.0 to 191.255.255.255):
    - Used for medium-sized networks, such as large organizations.
    - Supports up to 65,000 hosts per network.
    - **Example:** `172.16.0.1` (Private IP in this class).
- **Class C** (192.0.0.0 to 223.255.255.255):
    - Used for smaller networks, like small businesses or home networks.
    - Supports up to 254 hosts per network.
    - **Example:** `192.168.1.1` (Private IP in this class).
- **Class D** (224.0.0.0 to 239.255.255.255):
    - Reserved for multicast groups (used to send data to multiple devices at once).
    - Not used for traditional devices or networks.
- **Class E** (240.0.0.0 to 255.255.255.255):
    - Reserved for experimental purposes and future use.

IP Class	Address Range	Maximum number of networks
Class A	1-126	126 (2^7-2)

IP Class	Address Range	Maximum number of networks
Class B	128-191	16384
Class C	192-223	2097152
Class D	224-239	Reserve for multitasking
Class E	240-254	Reserved for Research and development

Special IP Addresses

There are also some special-purpose IP addresses that don't follow the usual structure:

- **Loopback Address**:
    - The loopback address `127.0.0.1` is used to test network connectivity within the same device (i.e., sending data to yourself).
    - Often called "localhost."
- **Broadcast Address**:
    - The broadcast address allows data to be sent to all devices in a network. For a typical network with the IP range `192.168.1.0/24`, the broadcast address would be `192.168.1.255`.
- **Multicast Address**:
    - Used to send data to a group of devices (multicast). For example, `233.0.0.1` is a multicast address.

How to Look Up IP Addresses?

In Windows

1. Open the Command Prompt.
2. Type `ipconfig` and press Enter.

3. Look for your IP under your network connection.

On Mac

1. Open System Preferences > Network.
2. Select your active connection.
3. You'll see your IP address in the connection details.

On iPhone

1. Go to Settings > Wi-Fi.
2. Tap the (i) icon next to your network.
3. Find your IP under "IP Address."

IP Address Security Threats

IP addresses are essential for connecting devices on the internet, but they also come with various security risks. Understanding these threats can help you protect your network and personal information more effectively. Here are some common IP address security threats:

- **IP Spoofing:** Hackers use this technique to bypass security measures, launch attacks, or gain unauthorized access to systems. By pretending to be a trusted IP address, attackers can trick networks into granting them access or allowing malicious activities.

- **Distributed Denial of Service (DDoS) Attacks:** This happens by overloading a website or service with too much traffic. Many hacked devices send lots of requests to a target all at once, making the website or service crash. This means real users can't access it which can cause crashing of site, businesses to lose money and many more.

- **Man-in-the-Middle (MitM) Attacks:** Eavesdropping or altering messages between two people without letting them know is MitM attack. Attackers intercept the communication between two parties

and can steal sensitive information like passwords or credit card details by targeting the IP addresses involved.

- **Port Scanning: It** is a technique used to identify open ports and services running on a device's IP address. Hackers use port scanners to find vulnerabilities in network services, which they can then exploit to gain unauthorized access or deploy malware. Regularly monitoring and securing open ports is essential to prevent such attacks.

How to Protect and Hide Your IP Address?

- **VPN** (**Virtual Private Network**): A VPN hides your IP by masking it with the VPN server's IP, giving you privacy. Your internet traffic passes through the VPN server, masking your real IP address with the server's IP. This makes it difficult for others to track your online activities or identify your location.
- **Proxy Server**: Routes your data through a different server, hiding your real IP. When you use a proxy, your requests go through the proxy server, which hides your real IP address by replacing it with its own.
- **Tor Browser**: Encrypts and bounces your data around multiple servers for anonymity. This multi-layered routing makes it extremely difficult to trace your IP address or monitor your online activities.
- **Enable Your Firewall:** A **firewall** is a security system that monitors and controls incoming and outgoing network traffic. It can block unauthorized access to your device, making it harder for attackers to target your IP address.

Conclusion

IP addresses are essential for connecting devices over the internet. While they help identify and communicate with other devices, it's important to protect your IP to keep your information safe and private. IP addresses also come with challenges such as privacy risks and vulnerability to cyberattacks. Understanding both the benefits and

Dynamic Host Configuration Protocol (DHCP)

Last Updated : 27 Dec, 2024

Dynamic Host Configuration Protocol is a network protocol used to automate the process of assigning IP addresses and other network configuration parameters to devices (such as computers, smartphones, and printers) on a network. Instead of manually configuring each device with an IP address, DHCP allows devices to connect to a network and receive all necessary network information, like IP address, subnet mask, default gateway, and DNS server addresses, automatically from a DHCP server.

This makes it easier to manage and maintain large networks, ensuring devices can communicate effectively without conflicts in their network settings. DHCP plays a crucial role in modern networks by simplifying the process of connecting devices and managing network resources efficiently.

What is DHCP?

DHCP stands for Dynamic Host Configuration Protocol. It is the critical feature on which the users of an enterprise network communicate. DHCP helps enterprises to smoothly manage the allocation of IP addresses to the end-user clients' devices such as desktops, laptops, cellphones, etc. is an application layer protocol that is used to provide:

```
Subnet Mask (Option 1 - e.g., 255.255.255.0)
Router Address (Option 3 - e.g., 192.168.1.1)
DNS Address (Option 6 - e.g., 8.8.8.8)
Vendor Class Identifier (Option 43 - e.g.,
'unifi' = 192.168.1.9 ##where unifi = controller)
```

DHCP is based on a client-server model and based on discovery, offer, request, and ACK.

Why Do We Use DHCP?

DHCP helps in managing the entire process automatically and centrally. DHCP helps in maintaining a unique IP Address for a host using the server. DHCP servers maintain information on TCP/IP configuration and provide configuration of address to DHCP-enabled clients in the form of a lease offer.

Components of DHCP

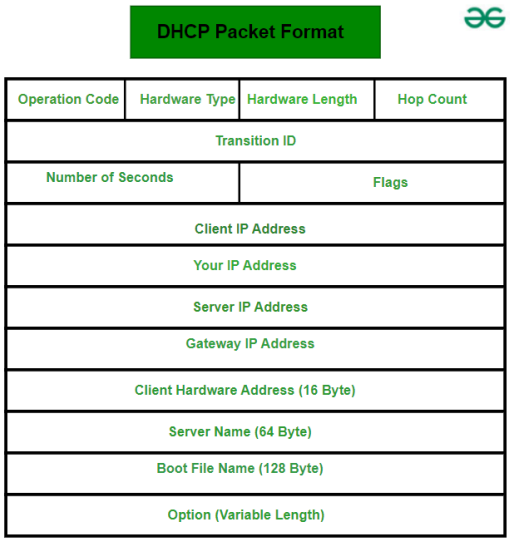
The main components of DHCP include:

- **DHCP Server:** DHCP Server is a server that holds IP Addresses and other information related to configuration.
- **DHCP Client:** It is a device that receives configuration information from the server. It can be a mobile, laptop, computer, or any other electronic device that requires a connection.
- **DHCP Relay:** DHCP relays basically work as a communication channel between DHCP Client and Server.
- **IP Address Pool:** It is the pool or container of IP Addresses possessed by the DHCP Server. It has a range of addresses that can be allocated to devices.
- **Subnets:** Subnets are smaller portions of the IP network partitioned to keep networks under control.
- **Lease:** It is simply the time that how long the information received from the server is valid, in case of expiration of the lease, the tenant must have to re-assign the lease.
- **DNS Servers:** DHCP servers can also provide DNS (Domain Name System) server information to DHCP clients, allowing them to resolve domain names to IP addresses.
- **Default Gateway:** DHCP servers can also provide information about the default gateway, which is the device that packets are sent to when the destination is outside the local network.
- **Options:** DHCP servers can provide additional configuration options to clients, such as the subnet mask, domain name, and time server information.
- **Renewal:** DHCP clients can request to renew their lease before it expires to ensure that they continue to have a valid IP address and

configuration information.

- **Failover:** DHCP servers can be configured for failover, where two servers work together to provide redundancy and ensure that clients can always obtain an IP address and configuration information, even if one server goes down.
- **Dynamic Updates:** DHCP servers can also be configured to dynamically update DNS records with the IP address of DHCP clients, allowing for easier management of network resources.
- **Audit Logging:** DHCP servers can keep audit logs of all DHCP transactions, providing administrators with visibility into which devices are using which IP addresses and when leases are being assigned or renewed.

DHCP Packet Format



DHCP Packet Format

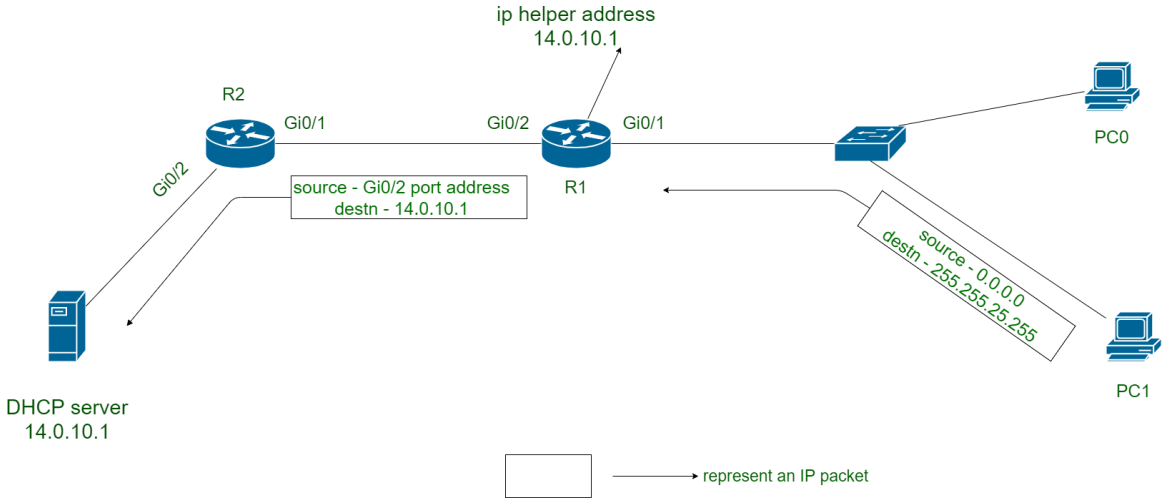
- **Hardware Length:** This is an 8-bit field defining the length of the physical address in bytes. e.g for Ethernet the value is 6.
- **Hop count:** This is an 8-bit field defining the maximum number of hops the packet can travel.
- **Transaction ID:** This is a 4-byte field carrying an integer. The transcation identification is set by the client and is used to match a reply with the request. The server returns the same value in its reply.

- **Number of Seconds:** This is a 16-bit field that indicates the number of seconds elapsed since the time the client started to boot.
- **Flag:** This is a 16-bit field in which only the leftmost bit is used and the rest of the bit should be set to os. A leftmost bit specifies a forced broadcast reply from the server. If the reply were to be unicast to the client, the destination. IP address of the IP packet is the address assigned to the client.
- **Client IP Address:** This is a 4-byte field that contains the client IP address . If the client does not have this information this field has a value of 0.
- **Your IP Address:** This is a 4-byte field that contains the client IP address. It is filled by the server at the request of the client.
- **Server IP Address:** This is a 4-byte field containing the server IP address. It is filled by the server in a reply message.
- **Gateway IP Address:** This is a 4-byte field containing the IP address of a routers. IT is filled by the server in a reply message.
- **Client Hardware Address:** This is the physical address of the client .Although the server can retrieve this address from the frame sent by the client it is more efficient if the address is supplied explicity by the client in the request message.
- **Server Name:** This is a 64-byte field that is optionally filled by the server in a reply packet. It contains a null-terminated string consisting of the domain name of the server. If the server does not want to fill this filed with data, the server must fill it with all 0s.
- **Boot Filename:** This is a 128-byte field that can be optionally filled by the server in a reply packet. It contains a null- terminated string consisting of the full pathname of the boot file. The client can use this path to retrieve other booting information. If the server does not want to fill this field with data, the server must fill it with all 0s.
- **Options:** This is a 64-byte field with a dual purpose. IT can carry either additional information or some specific vendor information. The field is used only in a reply message. The server uses a number, called a magic cookie, in the format of an IP address with the value of 99.130.83.99. When the client finishes reading the message, it looks for this magic cookie. If present, the next 60 bytes are options.

Working of DHCP

DHCP works on the Application layer of the **UDP Protocol**. The main task of DHCP is to dynamically assigns IP Addresses to the Clients and allocate information on TCP/IP configuration to Clients. For more, you can refer to the Article **Working of DHCP**.

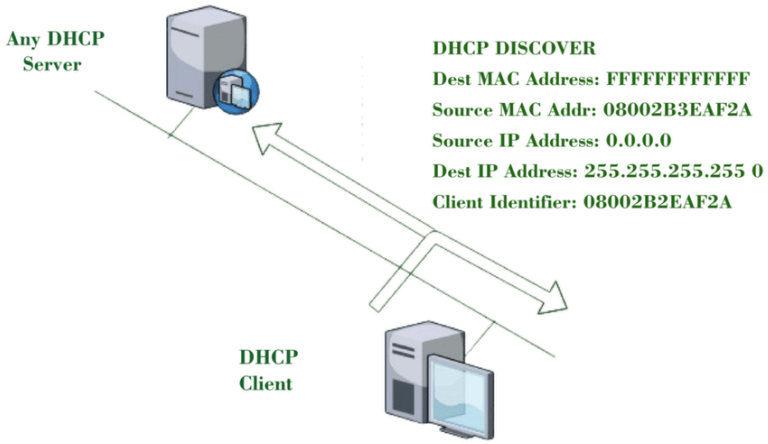
The DHCP **port number** for the server is 67 and for the client is 68. It is a client-server protocol that uses **UDP services**. An IP address is assigned from a pool of addresses. In DHCP, the client and the server exchange mainly 4 DHCP messages in order to make a connection, also called the **DORA** process, but there are 8 DHCP messages in the process.



Working of DHCP

The 8 DHCP Messages

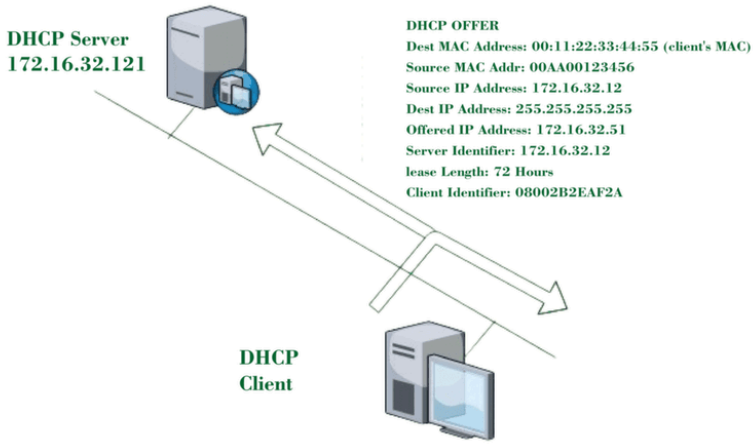
1. DHCP Discover Message: This is the first message generated in the communication process between the server and the client. This message is generated by the Client host in order to discover if there is any DHCP server/servers are present in a network or not. This message is broadcasted to all devices present in a network to find the DHCP server. This message is 342 or 576 bytes long.



DHCP Discover Message

As shown in the figure, the source MAC address (client PC) is 08002B2EAF2A, the destination MAC address(server) is FFFFFFFFFFFF, the source IP address is 0.0.0.0(because the PC has had no IP address till now) and the destination IP address is 255.255.255.255 (IP address used for broadcasting). As they discover message is broadcast to find out the DHCP server or servers in the network therefore broadcast IP address and MAC address is used.

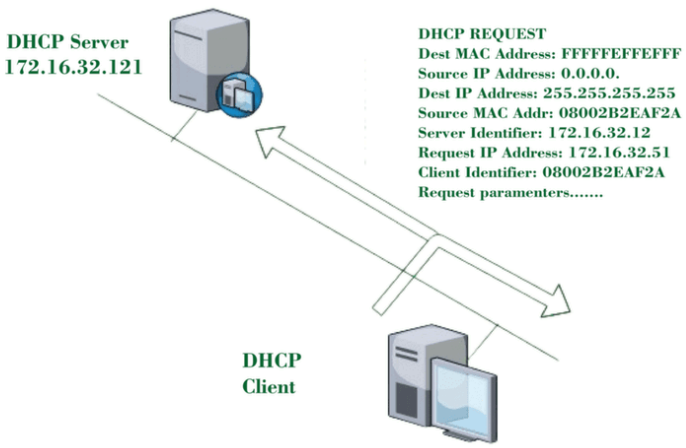
2. DHCP Offers A Message: The server will respond to the host in this message specifying the unleased IP address and other TCP configuration information. This message is broadcasted by the server. The size of the message is 342 bytes. If there is more than one DHCP server present in the network then the client host will accept the first DHCP OFFER message it receives. Also, a server ID is specified in the packet in order to identify the server.



Now, for the offer message, the source IP address is 172.16.32.12 (server's IP address in the example), the destination IP address is 255.255.255.255 (broadcast IP address), the source MAC address is 00AA00123456, the destination MAC address is 00:11:22:33:44:55 (client's MAC address). Here, the offer message is broadcast by the DHCP server therefore destination IP address is the broadcast IP address and destination MAC address is 00:11:22:33:44:55 (client's MAC address)and the source IP address is the server IP address and the MAC address is the server MAC address.

Also, the server has provided the offered IP address 192.16.32.51 and a lease time of 72 hours(after this time the entry of the host will be erased from the server automatically). Also, the client identifier is the PC MAC address (08002B2EAF2A) for all the messages.

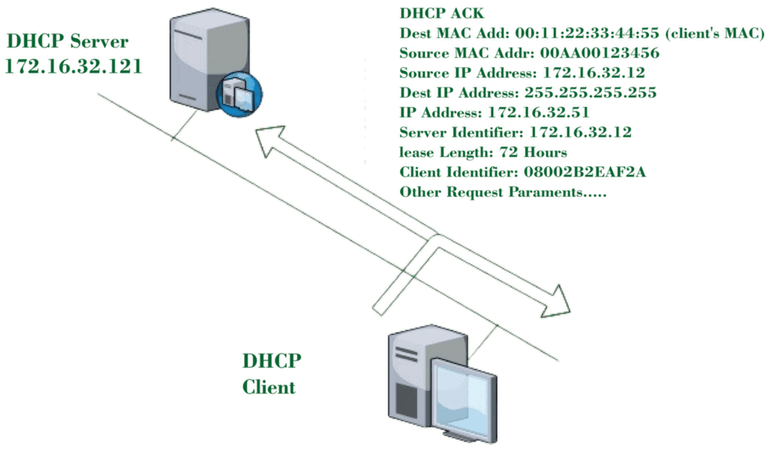
3. DHCP Request Message: When a client receives an offer message, it responds by broadcasting a DHCP request message. The client will produce a gratuitous ARP in order to find if there is any other host present in the network with the same IP address. If there is no reply from another host, then there is no host with the same TCP configuration in the network and the message is broadcasted to the server showing the acceptance of the IP address. A Client ID is also added to this message.



Now, the request message is broadcast by the client PC therefore source IP address is 0.0.0.0(as the client has no IP right now) and destination IP address is 255.255.255.255 (the broadcast IP address) and the source MAC address is 08002B2EAF2A (PC MAC address) and destination MAC address is FFFFFFFFFFFF.

Note – This message is broadcast after the ARP request broadcast by the PC to find out whether any other host is not using that offered IP. If there is no reply, then the client host broadcast the DHCP request message for the server showing the acceptance of the IP address and Other TCP/IP Configuration.

4. DHCP Acknowledgment Message: In response to the request message received, the server will make an entry with a specified client ID and bind the IP address offered with lease time. Now, the client will have the IP address provided by the server.



Now the server will make an entry of the client host with the offered IP address and lease time. This IP address will not be provided by the server to any other host. The destination MAC address is 00:11:22:33:44:55 (client's MAC address) and the destination IP address is 255.255.255.255 and the source IP address is 172.16.32.12 and the source MAC address is 00AA00123456 (server MAC address).

5. DHCP Negative Acknowledgment Message: Whenever a DHCP server receives a request for an IP address that is invalid according to the scopes that are configured, it sends a DHCP Nak message to the

client. Eg-when the server has no IP address unused or the pool is empty, then this message is sent by the server to the client.

6. DHCP Decline: If the DHCP client determines the offered configuration parameters are different or invalid, it sends a DHCP decline message to the server. When there is a reply to the gratuitous ARP by any host to the client, the client sends a DHCP decline message to the server showing the offered IP address is already in use.

7. DHCP Release: A DHCP client sends a DHCP release packet to the server to release the IP address and cancel any remaining lease time.

8. DHCP Inform: If a client address has obtained an IP address manually then the client uses DHCP information to obtain other local configuration parameters, such as domain name. In reply to the DHCP inform message, the DHCP server generates a DHCP ack message with a local configuration suitable for the client without allocating a new IP address. This DHCP ack message is unicast to the client.

Note – All the messages can be unicast also by the DHCP relay agent if the server is present in a different network.

Security Considerations for Using DHCP

To make sure your DHCP servers are safe, consider these DHCP security issues:

- **Limited IP Addresses** : A DHCP server can only offer a set number of IP addresses. This means attackers could flood the server with requests, causing essential devices to lose their connection.
- **Fake DHCP Servers** : Attackers might set up fake DHCP servers to give out fake IP addresses to devices on your network.
- **DNS Access** : When users get an IP address from DHCP, they also get DNS server details. This could potentially allow them to access more data than they should. It's important to restrict network access, use firewalls, and secure connections with VPNs to protect against this.

Protection Against DHCP Starvation Attack

A DHCP starvation attack happens when a hacker floods a DHCP server with requests for IP addresses. This overwhelms the server, making it unable to assign addresses to legitimate users. The hacker can then block access for authorized users and potentially set up a fake DHCP server to intercept and manipulate network traffic, which could lead to a man-in-the-middle attack.

Reasons Why Enterprises Must Automate DHCP?

Automating your DHCP system is crucial for businesses because it reduces the time and effort your IT team spends on manual tasks. For instance, DHCP-related issues like printers not connecting or subnets not working with the main network can be avoided automatically.

Automated DHCP also allows your operations to grow smoothly. Instead of hiring more staff to handle tasks that automation can manage, your team can focus on other important areas of business growth.

Advantages

- Centralized management of IP addresses.
- Centralized and automatedTCP/IP configuration .
- Ease of adding new clients to a network.
- Reuse of IP addresses reduces the total number of IP addresses that are required.
- The efficient handling of IP address changes for clients that must be updated frequently, such as those for portable devices that move to different locations on a wireless network.
- Simple reconfiguration of the IP address space on the DHCP server without needing to reconfigure each client.
- The DHCP protocol gives the network administrator a method to configure the network from a centralized area.
- With the help of DHCP, easy handling of new users and the reuse of IP addresses can be achieved.

Disadvantages

- IP conflict can occur.

- The problem with DHCP is that clients accept any server. Accordingly, when another server is in the vicinity, the client may connect with this server, and this server may possibly send invalid data to the client.
- The client is not able to access the network in absence of a DHCP Server.
- The name of the machine will not be changed in a case when a new IP Address is assigned.

Conclusion

In conclusion, DHCP is a technology that simplifies network setup by automatically assigning IP addresses and network configurations to devices. While DHCP offers convenience, it's important to manage its security carefully. Issues such as IP address exhaustion, and potential data access through DNS settings highlight the need for robust security measures like firewalls and VPNs to protect networks from unauthorized access and disruptions. DHCP remains essential for efficiently managing network connections while ensuring security against potential risks.

Next Article

DHCP Starvation Attack

Similar Reads

Working of Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used in networks to dynamically assign IP addresses & other...

15 min read

DHCP Relay Agent in Computer Network

Classes of Routing Protocols

Last Updated : 28 Dec, 2024

Routing protocols are essential for determining how data packets are transferred across networks. They help routers communicate with each other to find the most efficient paths for data to travel.

Routing protocols are typically divided into categories like **distance vector**, **link-state**, and **hybrid protocols**. Distance vector protocols, such as RIP, determine routes based on the number of hops. Link-state protocols, like OSPF, rely on a more detailed understanding of the entire network topology. Hybrid protocols, such as EIGRP, incorporate elements from both approaches to balance efficiency and accuracy.

1. Distance Vector Routing Protocol

These protocols select the best path based on hop counts to reach a destination network in a particular direction. Dynamic protocol like RIP is an example of a distance vector routing protocol. Hop count is each router that occurs between the source and the destination network. The path with the least hop count will be chosen as the best.

Features

- Updates of the network are exchanged periodically.
- Updates (routing information) are not broadcasted but shared to neighboring nodes only.
- Full routing tables are not sent in updates; only the distance vector is shared.
- Routers always trust routing information received from neighbor routers. This is also known as routing rumors.

Advantages

- **Simple to Use** : Easy setup and operation.
- **Low Resource Usage** : Requires minimal CPU and memory.
- **Automatic Updates** : Handles network changes automatically.
- **Good for Small Networks** : Works well in simple setups.

Disadvantages

- **Slow Convergence** : Takes time to update routes after a network change.
- **Limited Scalability** : Not efficient for large networks.
- **High Bandwidth Use** : Frequent updates may consume more network bandwidth.
- **Less Accurate** : Routes may not always be optimal.

2. Link State Routing Protocol

These protocols know more about Internetwork than any other distance vector routing protocol. These are also known as SPF (Shortest Path First) protocol. OSPF is an example of link-state routing protocol.

Features

- Hello, messages, also known as keep-alive messages are used for neighbor discovery and recovery.
- The concept of triggered updates is used i.e. updates are triggered only when there is a topology change.
- Only that many updates are exchanged which is requested by the neighbor router.

Tables Used in Link State Routing

Link state routing protocol maintains three tables namely:

- **Neighbor table:** the table which contains information about the neighbors of the router only, i.e, to which adjacency has been formed.

- **Topology table:** This table contains information about the whole topology i.e contains both best and backup routes to a particular advertised networks.
- **Routing table:** The Routing table contains all the best routes to the advertised network.

Advantages

- **Faster Updates** : Quickly adapts to network changes.
- **Accurate Routing** : Provides optimal routes with a complete network view.
- **Works for Large Networks** : Suitable for big, complex networks.
- **Prevents Routing Loops** : Avoids errors in route calculations.
- **More Reliable** : Less prone to mistakes in routing.

Disadvanatges

- **High Resource Usage** : Requires more memory and processing power.
- **Complex Setup** : More difficult to configure and maintain.
- **Increased Bandwidth** : Uses more bandwidth for network updates.
- **Not Ideal for Small Networks** : Overhead is unnecessary in small setups.

3. Hybrid Protocol

It is also known as hybrid routing protocol which uses the concept of both distance vector and link-state routing protocol. Enhanced Interior Gateway Routing Protocol (EIGRP) is an example of this class of routing protocol. EIGRP acts as a link-state routing protocol as it uses the concept of Hello protocol for neighbor discovery and forming an adjacency. Also, partial updates are triggered when a change occurs. EIGRP acts as a distance-vector routing protocol as it learned routes from directly connected neighbors.

Advanatages

- **Combines Strengths** : Mixes benefits of distance vector and link state routing.
- **Scalable** : Works well in both small and large networks.
- **Quick Updates** : Adapts fast to network changes.
- **Efficient Bandwidth** : Uses less bandwidth than pure link state.
- **Better for Larger Networks** : More suitable for bigger networks.

Disadvanatges

- **Complex Setup** : Harder to configure and manage.
- **Higher Resource Use** : Requires more memory and CPU .
- **Inconsistent Updates** : Can sometimes lead to slower updates.

Conclusion

Routing protocols help routers find the best paths for data to travel across a network. The three main types are **distance vector**, **link-state**, and **hybrid protocols**. Distance vector protocols choose paths based on the number of hops and are best for smaller networks. Link-state protocols build a network map to select the shortest paths, making them ideal for larger networks. Hybrid protocols combine both methods, providing efficiency for networks of any size. Using the right protocol ensures that data flows efficiently and improves network performance.

Next Article

Routing Protocol Code

Similar Reads

What is Routing?

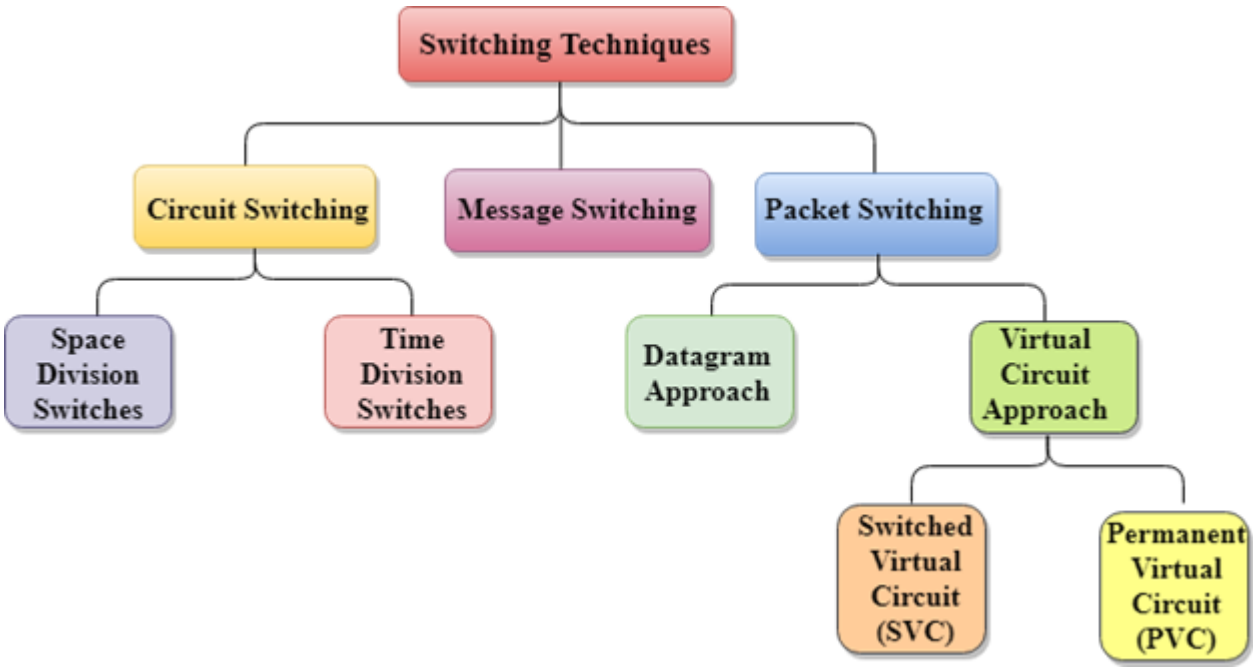
The process of choosing a path across one or more networks is known as Network Routing. Nowadays, [illegible] are more connected on the...

Switching techniques

In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.

Switching technique is used to connect the systems for making one-to-one communication.

Classification Of Switching Techniques



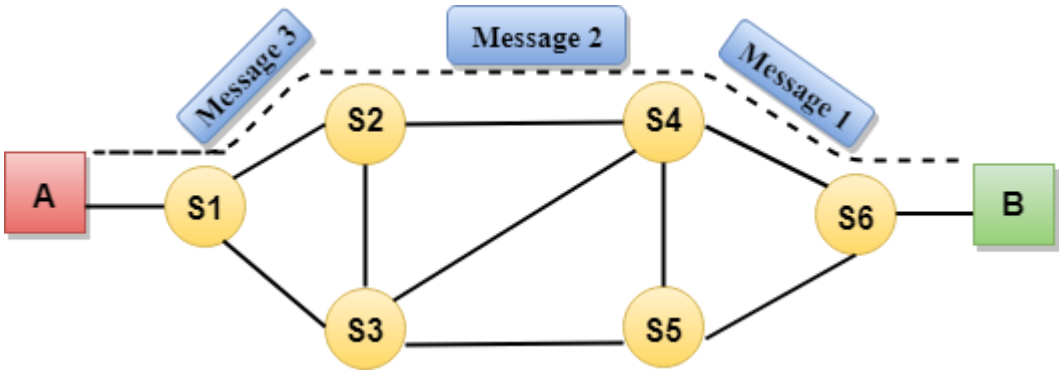
Circuit Switching

- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.
- A complete end-to-end path must exist before the communication takes place.

- In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
- Circuit switching is used in public telephone network. It is used for voice transmission.
- Fixed data can be transferred at a time in circuit switching technology.

Communication through circuit switching has 3 phases:

- Circuit establishment
- Data transfer
- Circuit Disconnect



Circuit Switching can use either of the two technologies:

Space Division Switches:

- Space Division Switching is a circuit switching technology in which a single transmission path is accomplished in a switch by using a physically separate set of crosspoints.
- Space Division Switching can be achieved by using crossbar switch. A crossbar switch is a metallic crosspoint or semiconductor gate that can be enabled or disabled by a control unit.
- The Crossbar switch is made by using the semiconductor. For example, Xilinx crossbar switch using FPGAs.
- Space Division Switching has high speed, high capacity, and nonblocking switches.

Space Division Switches can be categorized in two ways:

- **Crossbar Switch**
- **Multistage Switch**

Crossbar Switch

The Crossbar switch is a switch that has n input lines and n output lines. The crossbar switch has n^2 intersection points known as **crosspoints.**

Disadvantage of Crossbar switch:

The number of crosspoints increases as the number of stations is increased. Therefore, it becomes very expensive for a large switch. The solution to this is to use a multistage switch.

Multistage Switch

- Multistage Switch is made by splitting the crossbar switch into the smaller units and then interconnecting them.
- It reduces the number of crosspoints.
- If one path fails, then there will be an availability of another path.

Advantages Of Circuit Switching:

- In the case of Circuit Switching technique, the communication channel is dedicated.
- It has fixed bandwidth.

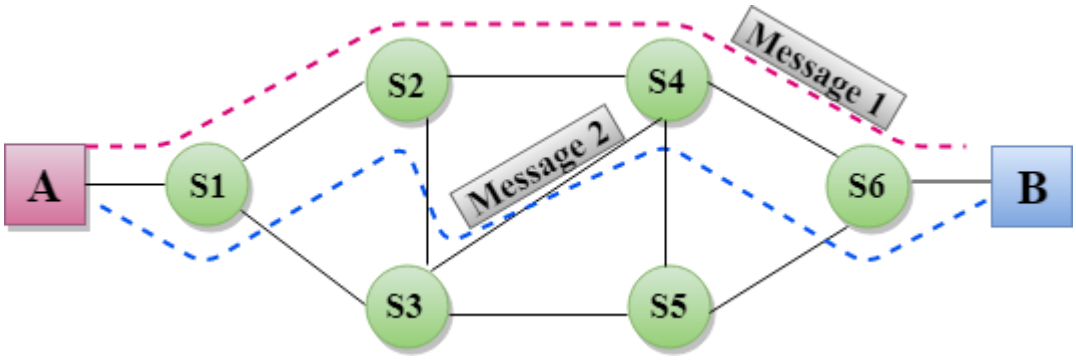
Disadvantages Of Circuit Switching:

- Once the dedicated path is established, the only delay occurs in the speed of data transmission.
- It takes a long time to establish a connection approx 10 seconds during which no data can be transmitted.
- It is more expensive than other switching techniques as a dedicated path is required for each connection.
- It is inefficient to use because once the path is established and no data is transferred, then the capacity of the path is wasted.

- In this case, the connection is dedicated therefore no other data can be transferred even if the channel is free.

Message Switching

- Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
- In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
- The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.
- Message switches are programmed in such a way so that they can provide the most efficient routes.
- Each and every node stores the entire message and then forward it to the next node. This type of network is known as **store and forward network.**
- Message switching treats each message as an independent entity.



Advantages Of Message Switching

- Data channels are shared among the communicating devices that improve the efficiency of using available bandwidth.
- Traffic congestion can be reduced because the message is temporarily stored in the nodes.
- Message priority can be used to manage the network.
- The size of the message which is sent over the network can be varied. Therefore, it

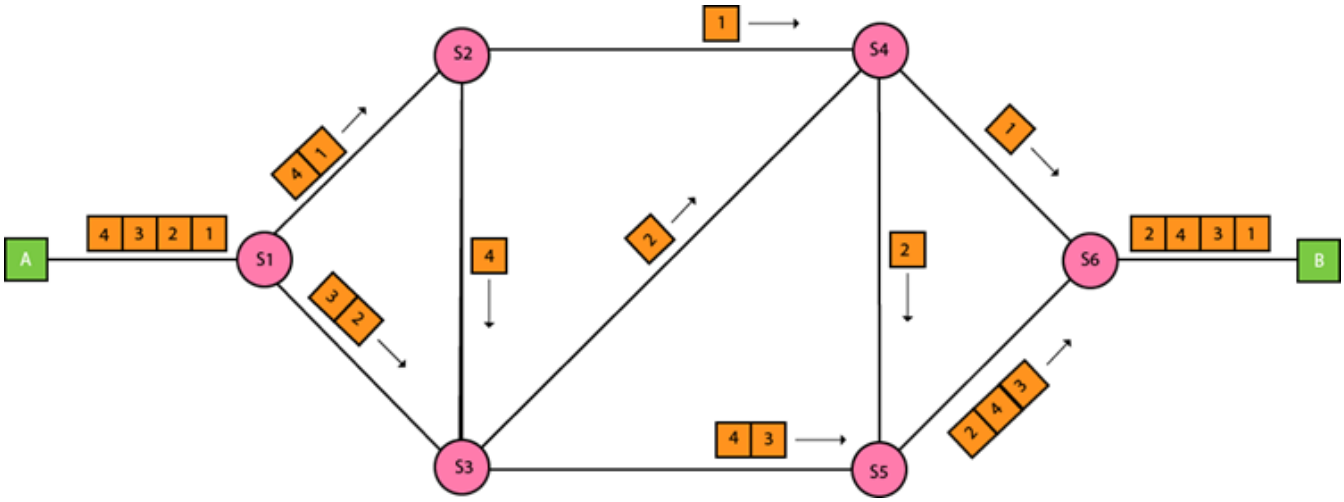
supports the data of unlimited size.

Disadvantages Of Message Switching

- The message switches must be equipped with sufficient storage to enable them to store the messages until the message is forwarded.
- The Long delay can occur due to the storing and forwarding facility provided by the message switching technique.

Packet Switching

- The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.
- The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, taking the shortest path as possible.
- All the packets are reassembled at the receiving end in correct order.
- If any packet is missing or corrupted, then the message will be sent to resend the message.
- If the correct order of the packets is reached, then the acknowledgment message will be sent.



Approaches Of Packet Switching:

There are two approaches to Packet Switching:

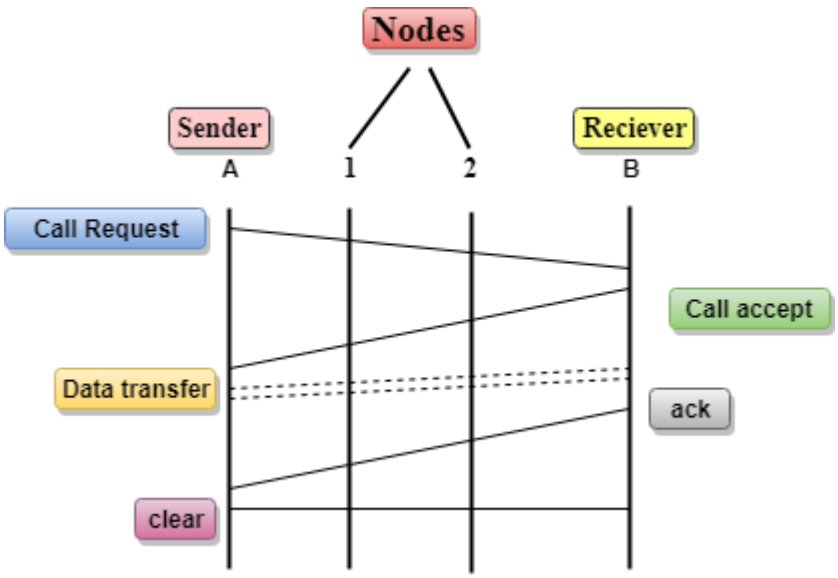
Datagram Packet switching:

- It is a packet switching technology in which packet is known as a datagram, is considered as an independent entity. Each packet contains the information about the destination and switch uses this information to forward the packet to the correct destination.
- The packets are reassembled at the receiving end in correct order.
- In Datagram Packet Switching technique, the path is not fixed.
- Intermediate nodes take the routing decisions to forward the packets.
- Datagram Packet Switching is also known as connectionless switching.

Virtual Circuit Switching

- Virtual Circuit Switching is also known as connection-oriented switching.
- In the case of Virtual circuit switching, a preplanned route is established before the messages are sent.
- Call request and call accept packets are used to establish the connection between sender and receiver.
- In this case, the path is fixed for the duration of a logical connection.

Let's understand the concept of virtual circuit switching through a diagram:



- In the above diagram, A and B are the sender and receiver respectively. 1 and 2 are the nodes.
- Call request and call accept packets are used to establish a connection between

the sender and receiver.

- When a route is established, data will be transferred.
- After transmission of data, an acknowledgment signal is sent by the receiver that the message has been received.
- If the user wants to terminate the connection, a clear signal is sent for the termination.

Differences b/w Datagram approach and Virtual Circuit approach

Datagram approach	Virtual Circuit approach
Node takes routing decisions to forward the packets.	Node does not take any routing decision.
Congestion cannot occur as all the packets travel in different directions.	Congestion can occur when the node is busy, and it does not allow other packets to pass through.
It is more flexible as all the packets are treated as an independent entity.	It is not very flexible.

Advantages Of Packet Switching:

- **Cost-effective:** In packet switching technique, switching devices do not require massive secondary storage to store the packets, so cost is minimized to some extent. Therefore, we can say that the packet switching technique is a cost-effective technique.
- **Reliable:** If any node is busy, then the packets can be rerouted. This ensures that the Packet Switching technique provides reliable communication.
- **Efficient:** Packet Switching is an efficient technique. It does not require any established path prior to the transmission, and many users can use the same communication channel simultaneously, hence makes use of available bandwidth very efficiently.

Disadvantages Of Packet Switching:

- Packet Switching technique cannot be implemented in those applications that

require low delay and high-quality services.

- The protocols used in a packet switching technique are very complex and requires high implementation cost.
- If the network is overloaded or corrupted, then it requires retransmission of lost packets. It can also lead to the loss of critical information if errors are nor recovered.

Most Asked MCQs on Switching Techniques

1. What is the primary function of switching in computer networks?

a. To connect different networks together
b. To transmit data in the form of packets or circuits
c. To provide security to the network
d. To manage network protocols

Show Answer Workspace

2. Which switching technique is most efficient for real-time voice and video transmission?

a. Packet switching
b. Circuit switching
c. Message switching
d. Frame switching

Show Answer Workspace

3. In packet switching, how is data transmitted across the network?

a. In a continuous stream
b. Through a dedicated path
c. In discrete units called packets
d. By broadcasting

Show Answer Workspace

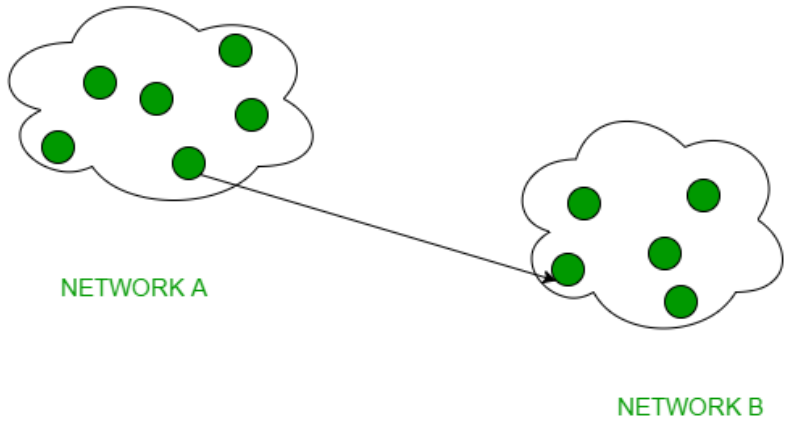
4. What is the one key advantage of message switching over circuit switching?

Unicast Routing – Link State Routing

Last Updated : 05 Feb, 2025

Unicast means the transmission from a single sender to a single receiver. It is a point-to-point communication between the sender and receiver. There are various unicast protocols such as TCP, HTTP, etc.

- TCP (Transmission Control Protocol) is the most commonly used unicast protocol. It is a connection-oriented protocol that relies on acknowledgment from the receiver side.
- HTTP stands for HyperText Transfer Protocol. It is an object-oriented protocol for communication.



UNICAST EXAMPLE

Unicast Routing

Major Protocols of Unicast Routing

1. **Distance Vector Routing:** Distance-Vector routers use a distributed algorithm to compute their routing tables.
2. **Link-State Routing:** Link-State routing uses link-state routers to exchange messages that allow each router to learn the entire network topology.

3. **Path-Vector Routing:** It is a routing protocol that maintains the path that is updated dynamically.

Link State Routing

Link state routing is the second family of routing protocols. While distance-vector routers use a distributed algorithm to compute their routing tables, link-state routing uses link-state routers to exchange messages that allow each router to learn the entire network topology. Based on this learned topology, each router is then able to compute its routing table by using the shortest path computation.

Link state routing is a technique in which each router shares the knowledge of its neighborhood with every other router i.e. the internet work. The three keys to understand the link state routing algorithm.

1. **Knowledge about the neighborhood** : Instead of sending its routing table, a router sends the information about its neighborhood only. A router broadcast its identities and cost of the directly attached links to other routers.
2. **Flooding:** Each router sends the information to every other router on the internetwork except its neighbors. This process is known as flooding. Every router that receives the packet sends the copies to all the neighbors. Finally each and every router receives a copy of the same information.
3. **Information Sharing** : A router send the information to every other router only when the change occurs in the information.

Link state routing has two phase:

1. **Reliable Flooding: Initial state** – Each node knows the cost of its neighbors. Final state- Each node knows the entire graph.
2. **Route Calculation** : Each node uses Dijkstra' s algorithm on the graph to calculate the optimal routes to all nodes. The link state routing algorithm is also known as Dijkstra's algorithm which is used to find the shortest path from one node to every other node in the network.

Features of Link State Routing Protocols

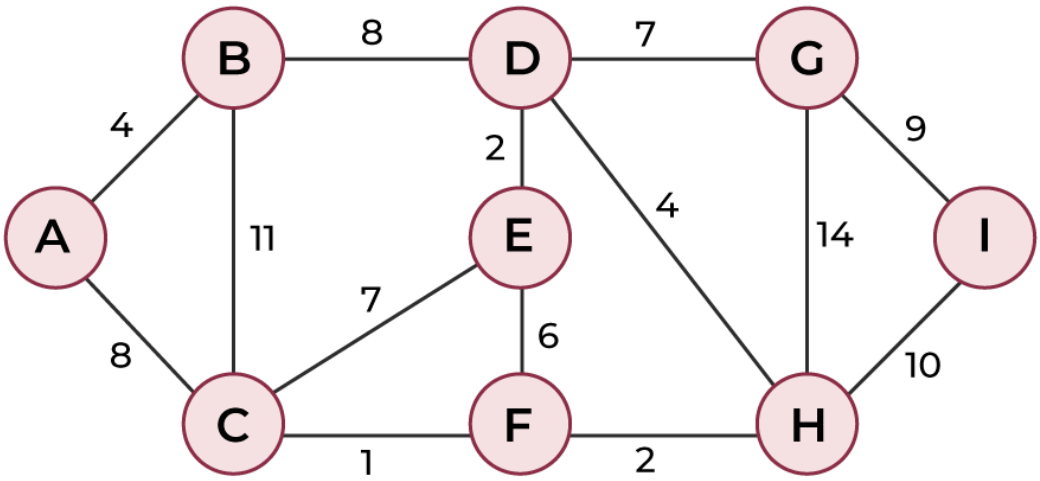
- **Link State Packet:** A small packet that contains routing information.
- **Link-State Database:** A collection of information gathered from the link-state packet.
- **Shortest Path First Algorithm (Dijkstra algorithm):** A calculation performed on the database results in the shortest path
- **Routing Table:** A list of known paths and interfaces.

Calculation of Shortest Path

To find the shortest path, each node needs to run the famous Dijkstra algorithm. Let us understand how can we find the shortest path using an example.

Note: We use a boolean array **sptSet[]** to represent the set of vertices included in SPT. If a value **sptSet[v]** is true, then vertex v is included in SPT, otherwise not. Array **dist[]** is used to store the shortest distance values of all vertices.

Consider the below graph and src = 0.

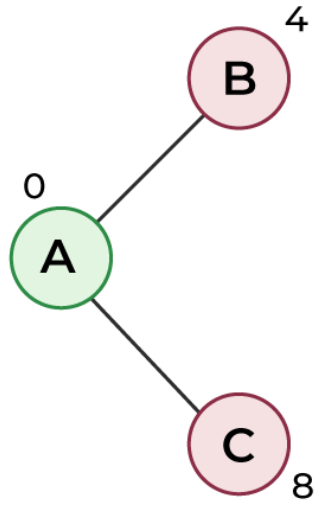


Shortest Path Calculation – Step 1

STEP 1: The set sptSet is initially empty and distances assigned to vertices are {0, INF, INF, INF, INF, INF, INF, INF} where INF indicates infinite. Now pick the vertex with a minimum distance value. The vertex 0 is picked and included in sptSet. So sptSet becomes {0}. After including 0 to sptSet, update the distance values of its adjacent

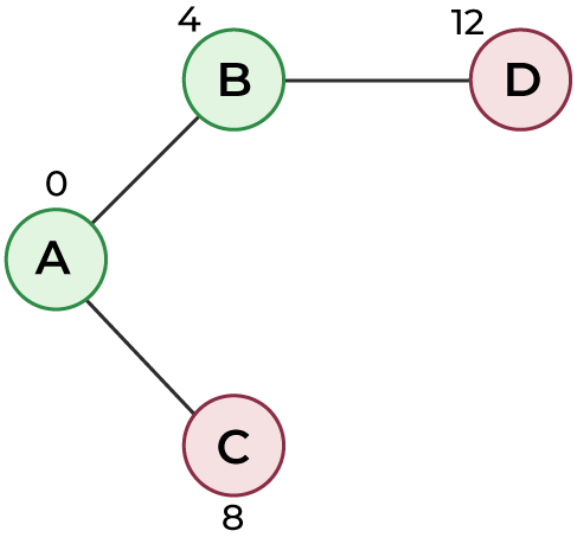
vertices. Adjacent vertices of 0 are 1 and 7. The distance values of 1 and 7 are updated as 4 and 8.

The following subgraph shows vertices and their distance values. Vertices included in SPT are included in GREEN color.



Shortest Path Calculation – Step 2

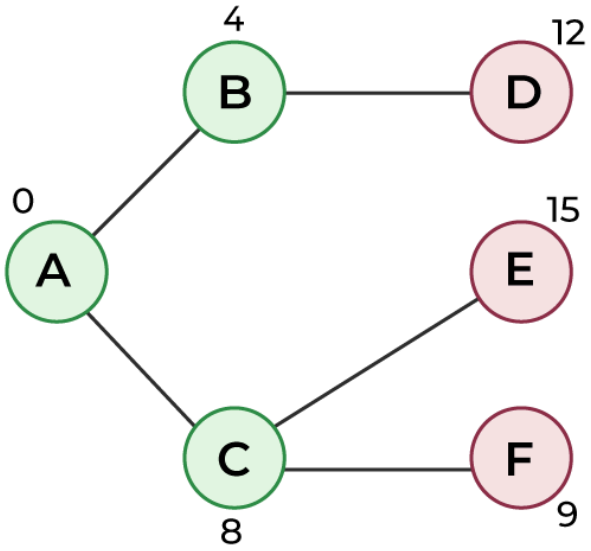
STEP 2: Pick the vertex with minimum distance value and not already included in SPT (not in sptSET). The vertex 1 is picked and added to sptSet. So sptSet now becomes {0, 1}. Update the distance values of adjacent vertices of 1. The distance value of vertex 2 becomes 12.



Shortest Path Calculation – Step 3

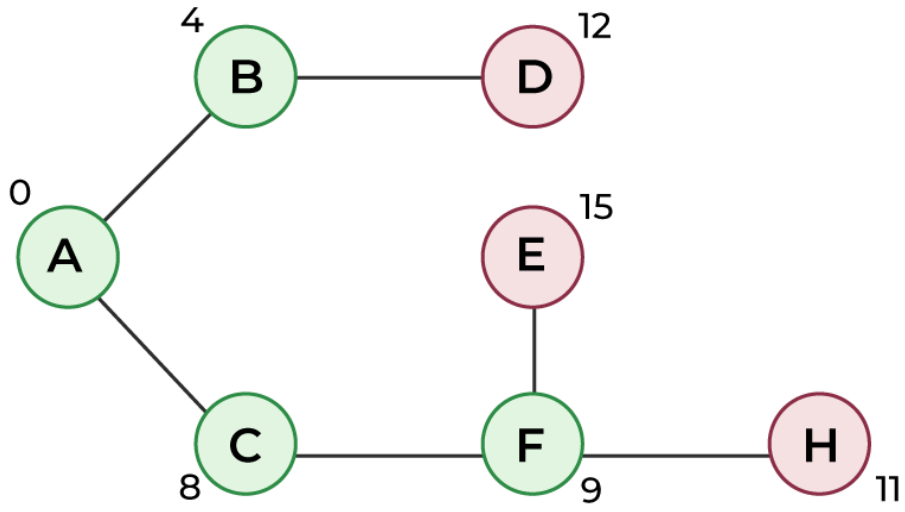
STEP 3: Pick the vertex with minimum distance value and not already included in SPT (not in sptSET). Vertex 7 is picked. So sptSet now becomes {0, 1, 7}. Update the distance values of adjacent vertices of 7.

The distance value of vertex 6 and 8 becomes finite (15 and 9 respectively).



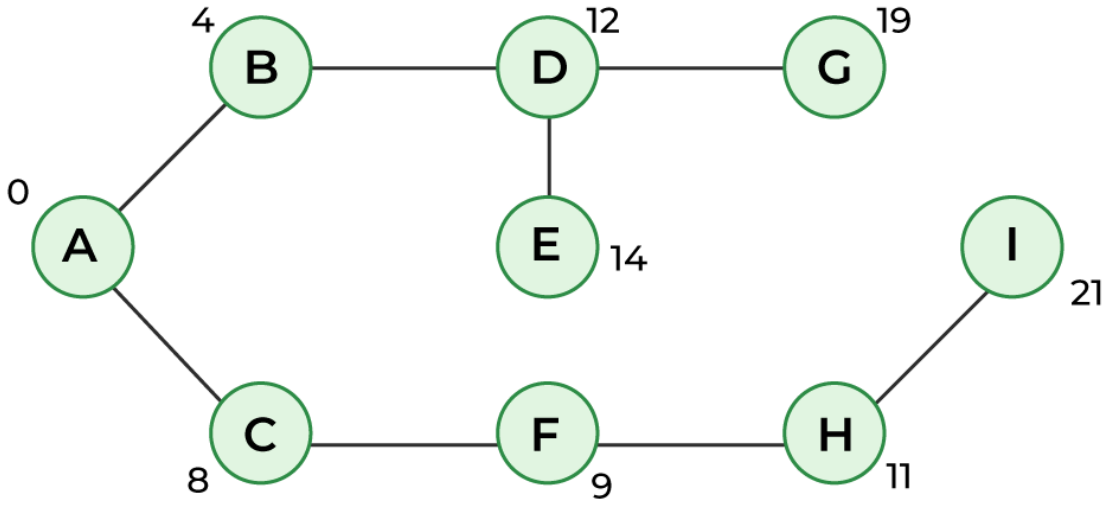
Shortest Path Calculation – Step 4

STEP 4: Pick the vertex with minimum distance value and not already included in SPT (not in sptSET). Vertex 6 is picked. So sptSet now becomes {0, 1, 7, 6}. Update the distance values of adjacent vertices of 6. The distance value of vertex 5 and 8 are updated.



Shortest Path Calculation – Step 5

We repeat the above steps until sptSet includes all vertices of the given graph. Finally, we get the following Shortest Path Tree (SPT).



Shortest Path Calculation – Step 6

Characteristics of Link State Protocol

- It requires a large amount of memory.
- Shortest path computations require many CPU circles.
- If a network uses little bandwidth; it quickly reacts to topology changes
- All items in the database must be sent to neighbors to form link-state packets.
- All neighbors must be trusted in the topology.
- Authentication mechanisms can be used to avoid undesired adjacency and problems.
- No split horizon techniques are possible in the link-state routing.
- OSPF Protocol

Protocols of Link State Routing

1. Open Shortest Path First (OSPF)
2. Intermediate System to Intermediate System (IS-IS)

Open Shortest Path First (OSPF): Open Shortest Path First (OSPF) is a unicast routing protocol developed by a working group of the Internet Engineering Task Force (IETF). It is an intradomain routing protocol. It is an open-source protocol. It is similar to Routing Information Protocol (RIP). OSPF is a classless routing protocol, which means that in its updates, it includes the subnet of each route it knows about, thus, enabling variable-length subnetting. With variable-length subnet

masks, an IP network can be broken into many subnets of various sizes. This provides network administrators with extra network configuration flexibility. These updates are multicasts at specific addresses (224.0.0.5 and 224.0.0.6). OSPF is implemented as a program in the network layer using the services provided by the Internet Protocol. IP datagram that carries the messages from OSPF sets the value of the protocol field to 89. OSPF is based on the SPF algorithm, which sometimes is referred to as the Dijkstra algorithm.

Intermediate System to Intermediate System (IS-IS): Intermediate System to Intermediate System is a standardized link-state protocol that was developed as the definitive routing protocol for the OSI Model. IS-IS uses System ID to identify a router on the network. IS-IS doesn't require IP connectivity between the routers as updates are sent via CLNS instead of IP.

For more about OSPF and IS-IS, you can refer to Difference between OSPF and IS-IS.

Next Article

Distance Vector Routing (DVR) Protocol

Similar Reads

Distance Vector Routing (DVR) Protocol

Distance Vector Routing (DVR) Protocol is a method used by routers to find the best path for data to travel across a network. Each router keeps ...

15+ min read

Hierarchical Routing

Hierarchical routing protocols consist of a hierarchical topology to organize the network and routing information. Multiple layers and levels...

ARP Protocol

Last Updated : 24 May, 2024

ARP (Address Resolution Protocol) is an important protocol that plays an important role in the networking world. When working with your network systems, this protocol helps to identify specified network devices and find their addresses. Its main purpose is to duly transport data packets over the network, allowing them to move between devices connected to your heritage network.

In this article, we will give you with information about the introductory principles of ARP protocol, how it works, and its significance. We'll also tell you why ARP is important and how it can be used in your networking systems. Through this article, you'll gain deep knowledge of ARP protocol and make your place in the world of networking.

What is the ARP Protocol?

ARP stands for “Address Resolution Protocol”. It is a network protocol used to determine the MAC address (hardware address) from any IP address.

In other words, ARP is used to mapping the IP Address into MAC Address. When one device wants to communicate with another device in a LAN (local area network) network, the ARP protocol is used.

This protocol is used when a device wants to communicate with another device over a local area network or ethernet.

ARP is a network layer protocol. This is a very important protocol in the TCP/IP protocol suite. Although it was developed in the early 80s, it was defined in RFC 826 in 1982. ARP is implemented with important technologies like IPv4, X.25, frame relay, and ATM.

ARP protocol finds the MAC address based on IP address. IP address is used to communicate with any device at the application layer. But to

communicate with a device at the data link layer or to send data to it, a MAC address is required.

When data is sent to a local host, the data travels between networks via IP address. But to reach that host in LAN, it needs the MAC address of that host. In this situation the address resolution protocol plays an important role.

Important ARP Terms

- **ARP Cache :-** After receiving the MAC address, ARP passes it to the sender where it is stored in a table for future reference. And this is called ARP Cache which is later used to obtain the MAC address.
- **ARP Cache Timeout :-** This is the time in which the MAC address can remain in the ARP Cache.
- **ARP request :-** Broadcasting a packet over the network to verify whether we have arrived at the destination MAC address.
- **ARP response/reply :-** It is a MAC address response that the sender receives from the receiver which helps in further communication of data.

Types of ARP

There are four types of ARP protocol they are as follows:-

1. Proxy ARP
2. Gratuitous ARP
3. Reverse ARP
4. Inverse ARP

1. Proxy ARP

This is a technique through which proxy ARP in a network can answer ARP queries of IP addresses that are not in that network. That is, if we understand it in simple language, the Proxy server can also respond to queries of IP-address of other networks.

Through this we can fool the other person because instead of the MAC address of the destination device, the MAC address of the proxy server

is used and the other person does not even know.

2. Gratuitous ARP

This is an arp request of a host, which we use to check duplicate ip-address. And we can also use it to update the arp table of other devices. That is, through this we can check whether the host is using its original IP-address, or is using a duplicate IP-address.

This is a very important ARP. Which proves to be very helpful in protecting us from the wrong person, and by using it we can check the ip-address.

3. Reverse ARP

This is also a networking protocol, which we can use through client computer. That is, it is used to obtain information about one's own network from the computer network. That is, if understood in simple language, it is a TCP/IP protocol which we use to obtain information about the IP address of the computer server.

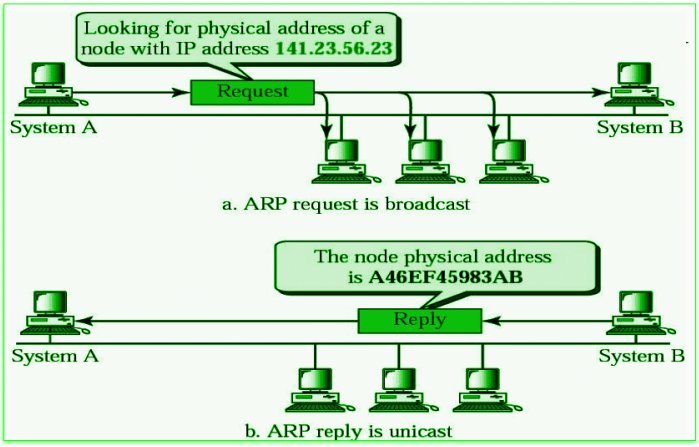
That is, to know the IP address of our computer server, we use Reverse ARP, which works under a networking protocol.

4. Inverse ARP (InARP)

Inverse ARP, it is the opposite of ARP, that is, we use it to know the IP address of our device through MAC Address, that is, it is such a networking technology, through this we convert MAC Address into IP address. Can translate. It is mainly used in ATM machines.

How ARP Protocol Works?

Below is a Working flow diagram of ARP Protocol



ARP Protocol

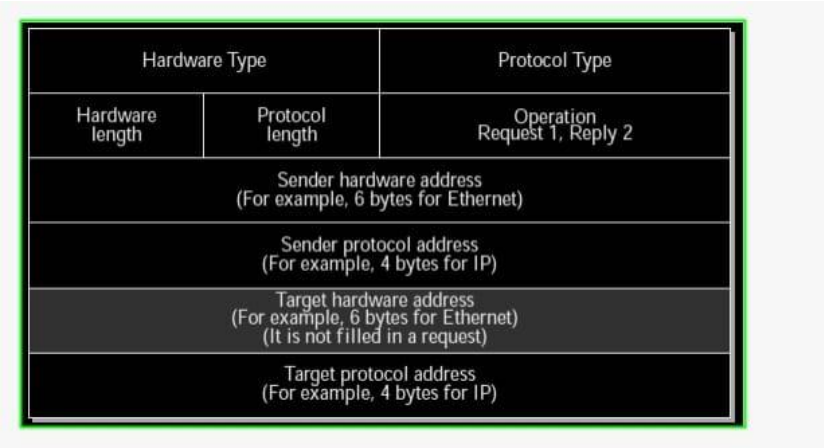
Below is the working of address resolution protocol is being explained in some steps :-

- When a sender wants to communicate with a receiver, the sender first checks its ARP cache. Sender checks whether the receiver's MAC address is already present in the ARP cache or not?
- If the receiver's MAC address is already present in the ARP cache, the sender will communicate with the receiver using that MAC address.
- If the MAC address of the receiver device is not already present in the ARP cache, then in such a situation an ARP request message is prepared by the sender device.This message contains the MAC address of the sender, IP address of the sender and IP address of the receiver. The field containing the MAC address of the receiver is left blank because it is being searched.
- Sender device broadcasts this ARP request message in the LAN. Because this is a broadcast message, every device connected to the LAN receives this message.
- All devices match the receiver IP address of this request message with their own IP address. Devices whose IP address does not match drop this request message.
- The device whose IP address matches the receiver IP address of this request message receives this message and prepares an ARP reply message. This is a unicast message which is sent only to the sender.

- In ARP reply message, the sender's IP address and MAC address are used to send the reply message. Besides, in this message the receiver also sends its IP address and MAC address.
- As soon as the sender device receives this ARP reply message, it updates its ARP cache with the new information (Receiver's MAC address). Now the MAC address of the receiver is present in the ARP cache of the sender. The sender can send and receive data without any problem.

Message Format of ARP Protocol

Messages are sent to find the MAC address through ARP(address resolution protocol). These messages are broadcast to all the devices in the LAN. The format of this message is being shown in the diagram below :



Message format of ARP

All the fields given in ARP message format are being explained in detail below:-

- **Hardware Type:** The size of this field is 2 bytes. This field defines what type of Hardware is used to transmit the message. The most common Hardware type is Ethernet. The value of Ethernet is 1.
- **Protocol Type:** This field tells which protocol has been used to transmit the message. substantially the value of this field is 2048 which indicates IPv4.
- **Hardware Address Length:** It shows the length of the tackle address in bytes. The size of Ethernet MAC address is 6 bytes.
- **Protocol Address Length:** It shows the size of the IP address in bytes. The size of IP addres

- **OP law:** This field tells the type of message. If the value of this field is 1 also it's a request message and if the value of this field is 2 also it's a reply message.
- **Sender Hardware Address:** This field contains the MAC address of the device transferring the message.
- **Sender Protocol Address:** This field contains the IP address of the device transferring the message.
- **Target Hardware Address:** This field is empty in the request message. This field contains the MAC address of the entering device.
- **Target Protocol Address:** This field contains the IP address of the entering device.

Advantages of ARP Protocol

There are many Advantages of ARP protocol but below we have told you about some important advantages.

- By using this protocol we can easily find out the MAC Address of the device.
- There is no need to configure the end nodes at all to extract the MAC address through this protocol.
- Through this protocol we can easily translate IP address into MAC Address.
- There are four main types of this protocol. Which we can use in different ways, and they prove to be very helpful.

Next Article
HRMA protocol

Similar Reads

Presentation Layer Services

Bootstrap Protocol (BOOTP)

Last Updated : 08 Dec, 2022

Overview :

In this article, we will discuss the bootstrapping protocol and how it plays its important role in maintaining the protocol between connected devices on a network. **Bootstrap Protocol (BOOTP)** is a networking protocol which is used by networking administration to give IP addresses to each member of that network for participating with other networking devices by the main server.

Important Features of Bootstrap Protocol :

Here, we will discuss the features of Bootstrap Protocol as follows.

- Bootstrap Protocol (BOOTP) is a basic protocol that automatically provides each participant in a network connection with a unique IP address for identification and authentication as soon as it connects to the network. This helps the server to speed up data transfers and connection requests.
- BOOTP uses a unique IP address algorithm to provide each system on the network with a completely different IP address in a fraction of a second.
- This shortens the connection time between the server and the client. It starts the process of downloading and updating the source code even with very little information.
- BOOTP uses a combination of **TFTP** (Trivial File Transfer Protocol) and **UDP** (User Datagram Protocol) to request and receive requests from various network-connected participants and to handle their responses.
- In a BOOTP connection, the server and client just need an IP address and a gateway address to establish a successful connection. Typically, in a BOOTP network, the server and client share the same

LAN, and the routers used in the network must support BOOTP bridging.

- A great example of a network with a TCP / IP configuration is the Bootstrap Protocol network. Whenever a computer on the network asks for a specific request to the server, BOOTP uses its unique IP address to quickly resolve them.

How Bootstrap Protocol differs from DHCP :

DHCP network servers have much broader use than a **BOOTP** network server. It may be used for the purpose when a user gives request to the server for a particular IP address and it gives the response of that particular IP address only, hence, time is not wasted for monitoring other addresses. BOOTP uses **UDP** (User Datagram Protocol) through an **IPv4 address** connection to identify and authenticate each network user. Also, a BOOTP connection has a stable static database of IP addresses which serves the client immediately with the required IP address.

Working of Bootstrap Protocol :

Here, we will discuss the Working steps of Bootstrap Protocol as follows.

- At the very beginning, each network participant does not have an IP address. The network administrator then provides each host on the network with a unique IP address using the IPv4 protocol.
- The client installs the BOOTP network protocol using TCP / IP Intervention on its computer system to ensure compatibility with all network protocols when connected to this network.
- The BOOTP network administrator then sends a message that contains a valid unicast address. This unicast address is then forwarded to the BOOTP client by the master server.

Uses of Bootstrap Protocol :

Here, we will discuss the uses of Bootstrap Protocol as follows.

1. Bootstrap (BOOTP) is primarily required to check the system on a network the first time you start your computer. Records the BIOS

cycle of each computer on the network to allow the computer's motherboard and network manager to efficiently organize the data transfer on the computer as soon as it boots up.
2. BOOTP is mainly used in a diskless environment and requires no media as all data is stored in the network cloud for efficient use.
3. BOOTP is the transfer of a data between a client and a server to send and receive requests and corresponding responses by the networking server.
4. BOOTP supports the use of motherboards and network managers, so no external storage outside of the cloud network is required.

Next Article

Difference between encapsulation and decapsulation

Similar Reads