Storage & DHCP Server

I. Storage Servers

Storage servers are dedicated computers designed to store, manage, and retrieve digital data. They are crucial for businesses and organizations that handle large volumes of information.

A. Types of Storage Servers:

- **File Servers:**
  - Centralized storage for files accessible by multiple users over a network.
  - Protocols: SMB/CIFS (Windows), NFS (Linux/Unix), AFP (macOS).
  - Use cases: Shared documents, user home directories, media libraries.
- **Database Servers:**
  - Optimized for storing and managing structured data.
  - Examples: MySQL, PostgreSQL, Oracle, Microsoft SQL Server.
  - Use cases: Applications, websites, data analysis.
- **Web Servers:**
  - Store and deliver web pages and related content.
  - Examples: Apache HTTP Server, Nginx, Microsoft IIS.
  - Use cases: Websites, web applications.
- **Object Storage Servers:**
  - Store data as objects with metadata, ideal for unstructured data.
  - Examples: Amazon S3, OpenStack Swift, MinIO.
  - Use cases: Cloud storage, backups, media storage.
- **Block Storage Servers (SAN - Storage Area Network):**
  - Provide block-level access to storage, like a local hard drive.
  - Protocols: Fibre Channel, iSCSI.
  - Use cases: Databases, virtualization, high-performance applications.

- **Network Attached Storage (NAS):**
  - A specialized file server that connects directly to the network, providing file-based storage to multiple devices.
  - Typically easier to configure and manage than a full server.
  - Protocols: SMB/CIFS, NFS, AFP.

B. Key Storage Concepts:

- **RAID (Redundant Array of Independent Disks):**
  - Combines multiple physical drives into a single logical unit for redundancy and/or performance.
  - Common RAID levels: RAID 0 (striping), RAID 1 (mirroring), RAID 5 (striping with parity), RAID 10 (mirroring and striping).
- **Storage Protocols:**
  - Define how data is transmitted between storage devices and clients.
  - Examples: iSCSI, Fibre Channel, NFS, SMB/CIFS.
- **Storage Virtualization:**
  - Abstracts physical storage resources into logical units, simplifying management and improving utilization.
- **Data Deduplication:**
  - Eliminates redundant data copies, saving storage space.
- **Storage Tiering:**
  - Automatically moves data between different storage tiers based on access frequency, optimizing performance and cost.
- **Snapshots and Backups:**
  - Snapshots: point-in-time copies of data.
  - Backups: copies of data stored separately for disaster recovery.

C. Considerations:

- **Capacity:** Determine the required storage capacity based on current and future needs.
- **Performance:** Select storage devices and configurations that meet performance requirements (IOPS, throughput).
- **Redundancy:** Implement RAID and other redundancy measures to protect against data loss.
- **Scalability:** Choose a storage solution that can scale as data grows.

- **Security:** Implement access controls, encryption, and other security measures to protect data.
- **Backup and Recovery:** Develop a comprehensive backup and recovery strategy.
- **Cost:** Balance performance, capacity, and redundancy with budget constraints.

II. DHCP Servers

A DHCP (Dynamic Host Configuration Protocol) server automatically assigns IP addresses and other network configuration parameters to devices on a network.

A. DHCP Server Functionality:

- **IP Address Assignment:**
    - Dynamically allocates IP addresses from a pool of available addresses.
    - Reduces the need for manual IP address configuration.
- **Subnet Mask Assignment:**
    - Provides the subnet mask, which defines the network portion of the IP address.
- **Default Gateway Assignment:**
    - Specifies the IP address of the router that connects the local network to other networks.
- **DNS Server Assignment:**
    - Provides the IP addresses of DNS servers, which translate domain names to IP addresses.
- **Lease Management:**
    - Assigns IP addresses for a specific period (lease time).
    - Reclaims IP addresses when leases expire.

B. DHCP Operation:

1. **DHCP Discover:** A client broadcasts a DHCP Discover message to find a DHCP server.
2. **DHCP Offer:** DHCP servers respond with a DHCP Offer message, proposing an IP address and other configuration parameters.

3. **DHCP Request:** The client selects an offer and sends a DHCP Request message to the chosen DHCP server.
4. **DHCP ACK (Acknowledgment):** The DHCP server acknowledges the request and sends a DHCP ACK message, confirming the IP address assignment.

C. DHCP Server Configuration:

- **IP Address Pool:** Define the range of IP addresses to be assigned.
- **Subnet Mask:** Specify the subnet mask for the network.
- **Default Gateway:** Configure the IP address of the default gateway.
- **DNS Servers:** Enter the IP addresses of DNS servers.
- **Lease Time:** Set the duration for which IP addresses are assigned.
- **Reservations:** Reserve specific IP addresses for particular devices (e.g., servers, printers).
- **Scopes:** allows for different sets of DHCP options to be given out on the same physical network.
- **DHCP Relay:** For networks with multiple subnets, a DHCP relay agent forwards DHCP requests to a DHCP server on a different subnet.

D. Considerations:

- **Reliability:** Ensure the DHCP server is reliable and available.
- **Security:** Implement DHCP snooping and other security measures to prevent rogue DHCP servers.
- **Scalability:** Choose a DHCP server that can handle the number of devices on the network.
- **IP Address Management:** Plan the IP address space to avoid conflicts and ensure efficient utilization.
- **Redundancy:** Implement redundant DHCP servers to provide failover.
- **Documentation:** Document the DHCP server configuration and IP address assignments.

iSCSI (Internet Small Computer System Interface)

ISCSI (Internet Small Computer System Interface) is a transport layer protocol that describes how Small Computer System Interface (SCSI) packets should be transported over a TCP/IP network.

ISCSI works on top of TCP and allows the SCSI command to be sent end-to-end over local area networks (LANs), wide area networks (WANs) or the internet.

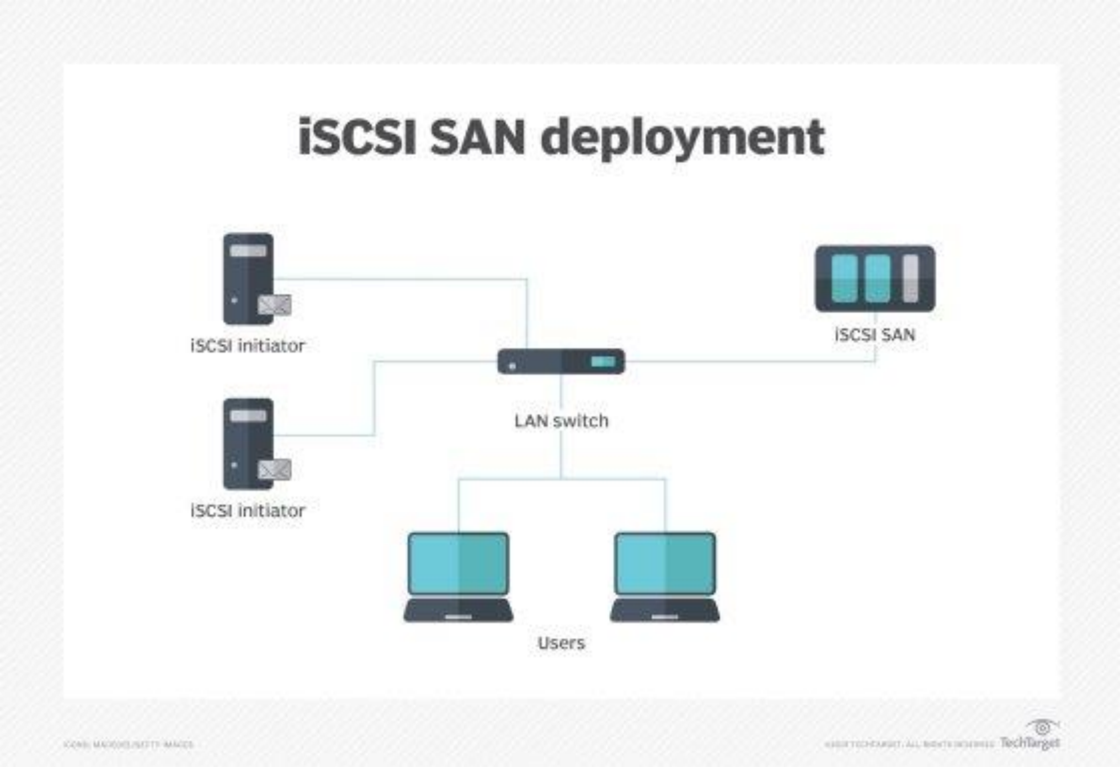
IBM developed iSCSI as a proof of concept in 1998 and presented the first draft of the iSCSI standard to the Internet Engineering Task Force in 2000. The protocol was ratified in 2003.

ISCSI makes it possible to set up a shared-storage network where multiple servers and clients can access central storage resources as if the storage was a locally connected device.

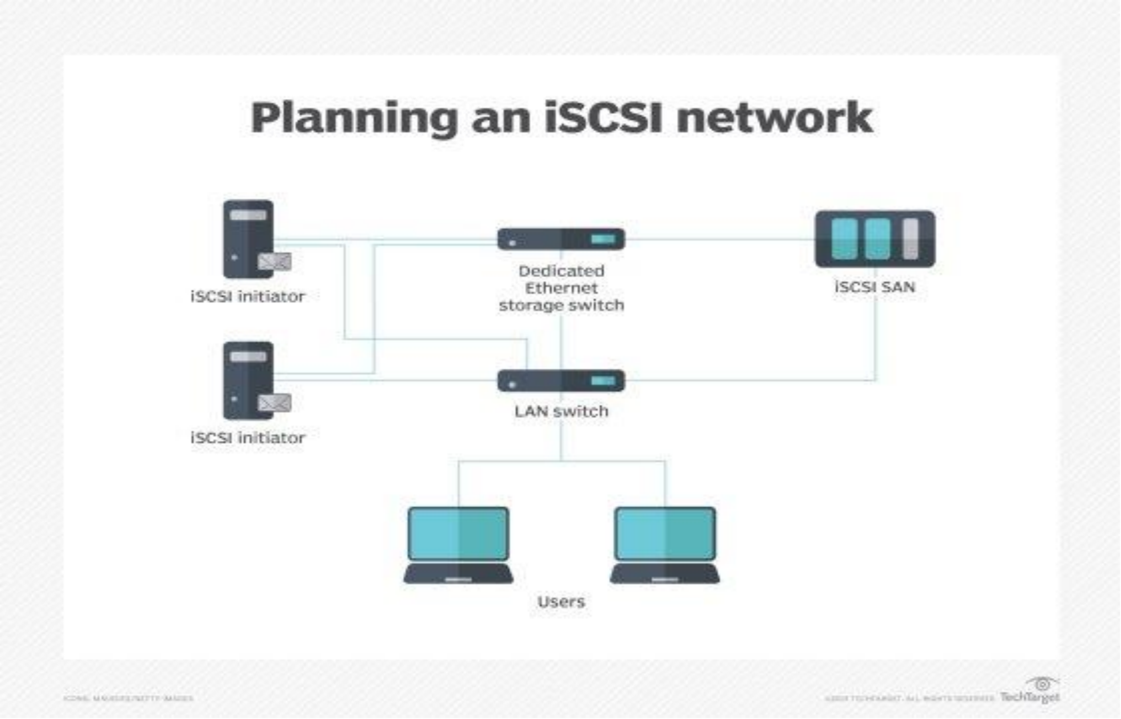
SCSI -- without the "i" prefix -- is a data access protocol that's been around since the early 1980s. It was developed by then-hard disk manufacturer Shugart Associates.

How iSCSI works

ISCSI transports block-level data between an iSCSI initiator on a server and an iSCSI target on a storage device. The iSCSI protocol encapsulates SCSI commands and assembles the data in packets for the TCP/IP layer. Packets are sent over the network using a point-to-point connection. Upon arrival, the iSCSI protocol disassembles the packets, separating the SCSI commands so the operating system will see the storage as if it was a locally connected SCSI device that can be formatted as usual.



Today, some of iSCSI's popularity in small and medium-sized businesses has to do with the way server virtualization makes use of storage pools. In a virtualized environment, the storage pool is accessible to all the hosts within the cluster. The cluster nodes communicate with the storage pool over the network through the use of the iSCSI protocol. There are a number of iSCSI devices that enable this type of communication between client servers and storage systems.



Components of iSCSI

Components of iSCSI include the following.

ISCSI initiator

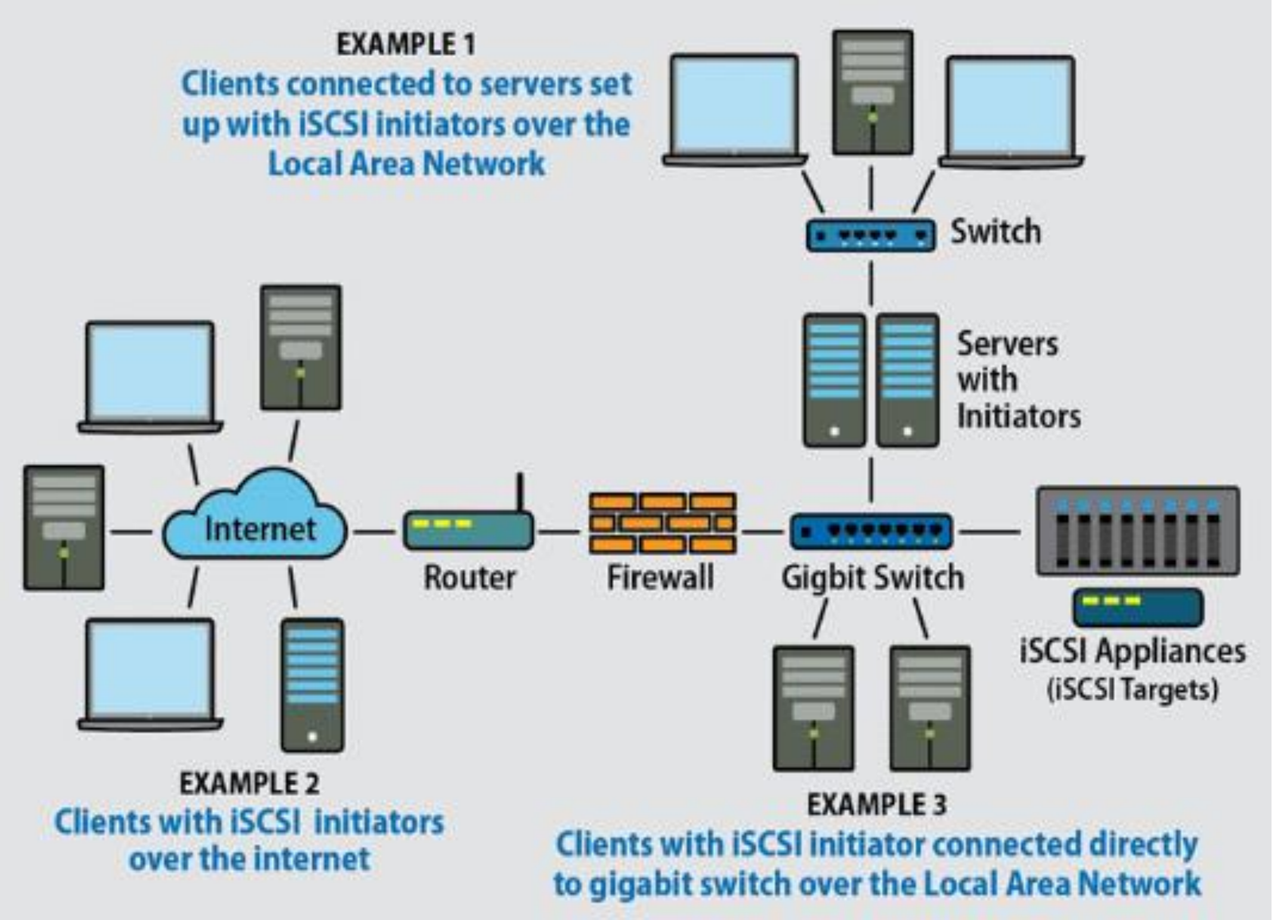
An iSCSI initiator is a piece of software or hardware that is installed in a server to send data to and from an iSCSI-based storage array or iSCSI target.

When a software initiator is used, standard Ethernet components such as network interface cards (NICs) can be used to create the storage network. But using a software initiator along with NICs leaves virtually all the processing burden on the servers' CPUs, which will likely have an impact on the servers' performance handling other tasks.

An iSCSI host bus adapter is similar to a Fibre Channel (FC) HBA. It offloads much of the processing from the host system's processor, improving performance of the server and the storage network. The improved performance, however, comes at a price as iSCSI HBAs typically cost three or four times as much as a standard Ethernet NIC. A similar, but somewhat less expensive, alternative is an iSCSI offload engine (iSOE), which, as its name suggests, offloads some of the process from the host.

ISCSI target

In the iSCSI configuration, the storage system is the "target." The target is essentially a server that hosts the storage resources and allows access to the storage through one or more NICs, HBAs or iSOEs.


EXAMPLE 1
Clients connected to servers set up with iSCSI initiators over the Local Area Network
Switch
Servers with Initiators
Internet
Router
Firewall
Gigbit Switch
iSCSI Appliances
(iSCSI Targets)
EXAMPLE 2
Clients with iSCSI initiators over the internet
EXAMPLE 3
Clients with iSCSI initiator connected directly to gigabit switch over the Local Area Network

iSCSI Initiator (Client)

Definition:
The **iSCSI Initiator** is a software or hardware component on a computer that connects to an iSCSI Target to access remote storage as if it were a local disk.

Types of iSCSI Initiators:

1. **Software Initiator** – A software driver (built into most modern OSs like Windows, Linux, VMware).
2. **Hardware Initiator** – A dedicated iSCSI HBA (Host Bus Adapter) for offloading processing from the CPU.

Function:

- Sends SCSI commands over an IP network to the target.
- Receives and processes responses from the target.
- Mounts remote storage like a locally attached disk.

Examples:

- Windows iSCSI Initiator (built into Windows Server).
- Linux open-iscsi package.
- VMware ESXi iSCSI adapter.

iSCSI Target (Server)

Definition:
The **iSCSI Target** is the storage device (SAN, disk array, or server) that provides storage resources to initiators.

Function:

- Listens for connections from iSCSI Initiators.
- Grants access to designated storage volumes (LUNs - Logical Unit Numbers).
- Manages multiple initiators (if configured in a shared storage setup).

Examples:

- **Windows iSCSI Target Server** (built into Windows Server).
- **Linux-based Targets** (e.g., targetcli, LIO).
- **Enterprise SAN Solutions** (Dell EMC, NetApp, HPE 3PAR, etc.).

iSCSI Initiator vs. iSCSI Target (Simple Explanation)

- **iSCSI Initiator (Client)** → The computer or server that **wants to use storage** from a remote device.
- **iSCSI Target (Server)** → The storage device that **provides the storage** to the initiator.

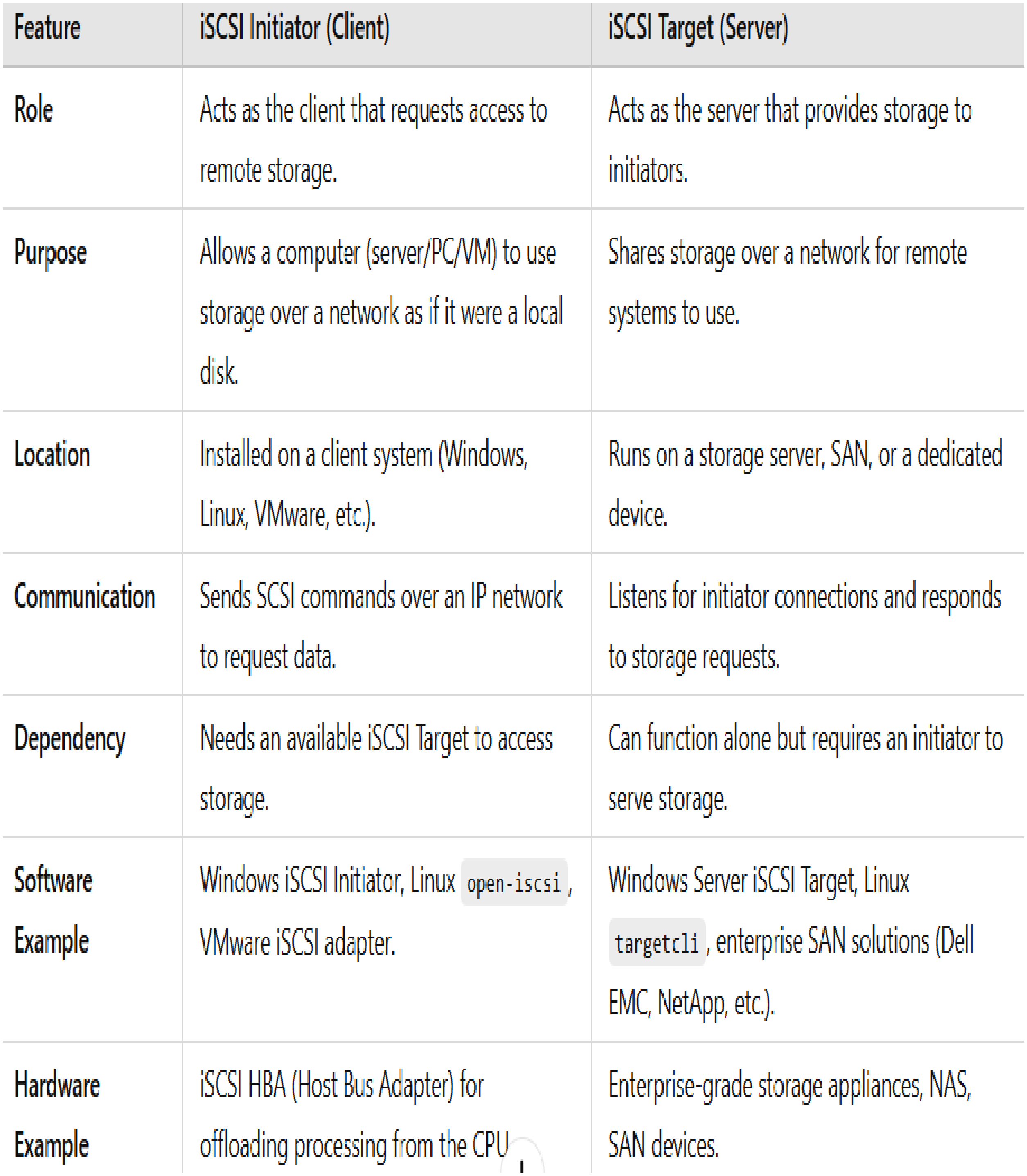
Example:

Think of it like **Netflix streaming**:

- Your **TV (Initiator)** requests a movie.
- **Netflix (Target)** provides the movie.
- The internet (Network) connects both.

In iSCSI:

- The **Initiator (client/server)** connects to the **Target (storage device/SAN)** over a network, making the remote storage act like a local disk.



Feature	iSCSI Initiator (Client)	iSCSI Target (Server)
Role	Acts as the client that requests access to remote storage.	Acts as the server that provides storage to initiators.
Purpose	Allows a computer (server/PC/VM) to use storage over a network as if it were a local disk.	Shares storage over a network for remote systems to use.
Location	Installed on a client system (Windows, Linux, VMware, etc.).	Runs on a storage server, SAN, or a dedicated device.
Communication	Sends SCSI commands over an IP network to request data.	Listens for initiator connections and responds to storage requests.
Dependency	Needs an available iSCSI Target to access storage.	Can function alone but requires an initiator to serve storage.
Software Example	Windows iSCSI Initiator, Linux `open-iscsi`, VMware iSCSI adapter.	Windows Server iSCSI Target, Linux `targetcli`, enterprise SAN solutions (Dell EMC, NetApp, etc.).
Hardware Example	iSCSI HBA (Host Bus Adapter) for offloading processing from the CPU	Enterprise-grade storage appliances, NAS, SAN devices.

Managing Roles in a Server

In a server environment, **roles** define the **primary functions** a server performs, such as file sharing, web hosting, or authentication. Proper role management ensures efficient performance, security, and scalability.

What Are Server Roles?

A **server role** is a specific function assigned to a server, such as:

- **Domain Controller** – Manages user authentication in a network (Active Directory).
- **File Server** – Stores and shares files over a network.
- **Web Server** – Hosts websites (IIS, Apache, Nginx).
- **Database Server** – Manages databases (SQL Server, MySQL, PostgreSQL).
- **Print Server** – Manages and shares printers.
- **DHCP Server** – Assigns IP addresses to devices.
- **DNS Server** – Translates domain names to IP addresses.

How to Manage Server Roles?

Windows Server (Using Server Manager)

1. Open Server Manager → Click "Manage" → "Add Roles and Features"
2. Select Installation Type → Choose Role-based or Feature-based**.**
3. Select the Server → Choose the server to configure.
4. Choose Server Roles → Select the role (e.g., File Server, DNS, DHCP**).**
5. Install & Configure → Follow prompts and configure settings.

To remove a role, go to **"Remove Roles and Features"** in Server Manager.

🔹 Linux Server (Using Command Line)

- Install a role using package managers:
  - **Web Server (Apache)**: sudo apt install apache2 (Ubuntu)
  - **File Server (Samba)**: sudo apt install samba
  - **DNS Server (Bind9)**: `sudo apt

Introduction to DHCP Server

A DHCP (Dynamic Host Configuration Protocol) Server automatically assigns IP addresses and other network settings (like DNS, subnet mask, and gateway) to devices on a network. This eliminates the need for manual IP configuration and ensures efficient network management.DHCP is a network system that automatically gives IP addresses and other settings (like gateway and DNS) to devices like computers and phones when they connect to a network. This removes the need to set up each device manually and helps keep the network organized and running smoothly.

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.

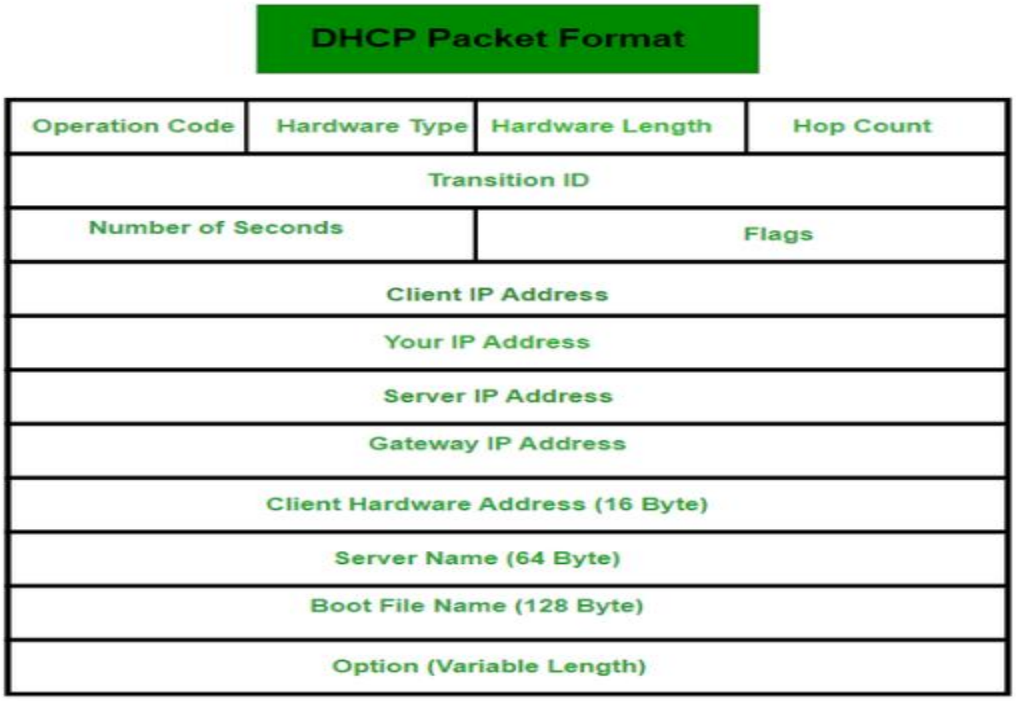
Renewal: DHCP clients can request to renew their lease before it expires to ensure that they continue to have a valid IP address and configuration information.

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

Operation Code	Hardware Type	Hardware Length	Hop Count
Transition ID			
Number of Seconds		Flags	
Client IP Address			
Your IP Address			
Server IP Address			
Gateway IP Address			
Client Hardware Address (16 Byte)			
Server Name (64 Byte)			
Boot File Name (128 Byte)			
Option (Variable Length)			

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 transaction 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 explicitly by the client in the request message.

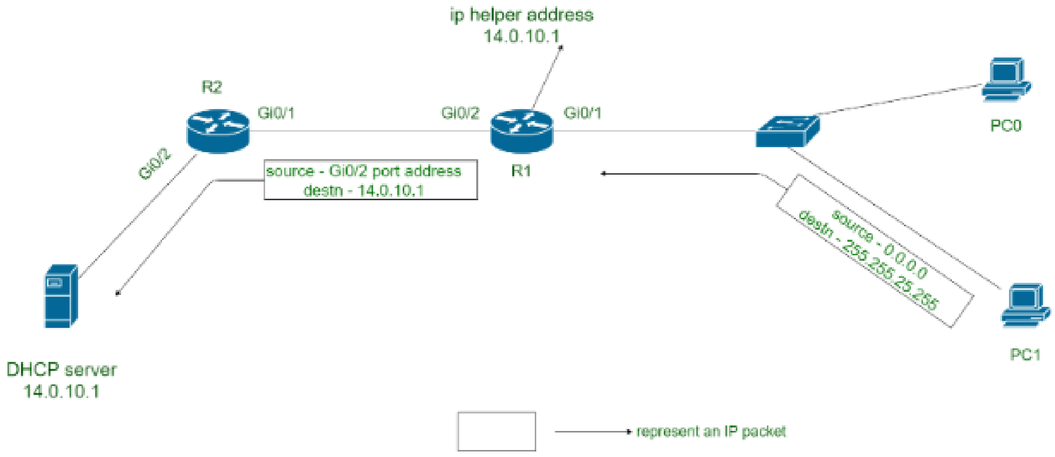
Server Name: This is a 64-byte field that is optionally filled by the server in a reply packet. It contains a null-terminated string consisting of the domain name of the server. If the server does not want to fill this filed with data, the server must fill it with all 0s.

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.



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.

Step-by-Step Process

1. **Discovery** – A new device (client) connects to the network and sends a DHCP request (broadcast).
2. **Offer** – The DHCP server responds with an available IP address and configuration details.
3. **Request** – The client requests the offered IP address.
4. **Acknowledgment** – The DHCP server confirms the lease, and the client starts using the assigned IP.

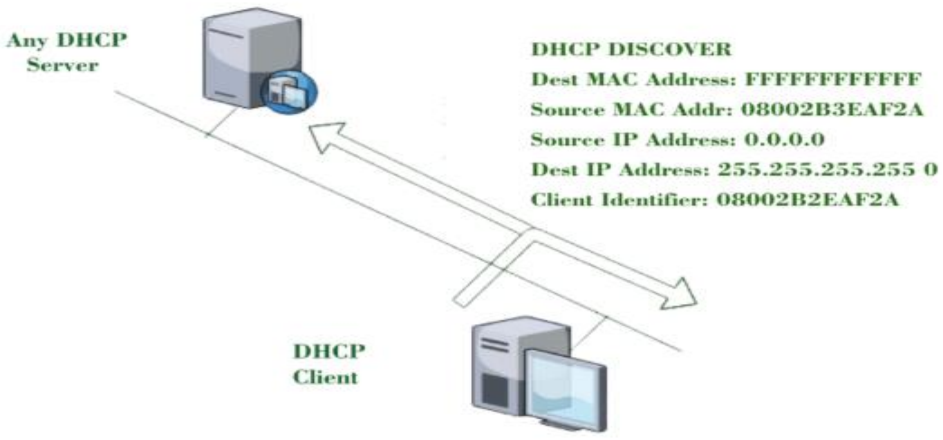
This process is known as **DORA** (Discover, Offer, Request and Acknowledge).

Working of DHCP

The 8 DHCP Messages

1. DHCP Discover Message: The **DHCP Discover message** is the first step in getting an IP address from a DHCP server.

- When a device (like a computer) connects to a network, it doesn’t have an IP address yet.
- It sends a DHCP Discover message to find a DHCP server that can assign an IP.
- This message is broadcasted to all devices in the network using:
  - **MAC Address:** Sent to FFFFFFFFFFFF (broadcast MAC, meaning all devices will receive it).
  - **IP Address:** Sent to 255.255.255.255 (broadcast IP, meaning it reaches every device).
  - **Source IP:** 0.0.0.0 (since the device doesn’t have an IP yet).
- If a DHCP server is available, it will respond and offer an IP address to the device



DHCP DISCOVER
Dest MAC Address: FFFFFFFFFFFF
Source MAC Addr: 08002B3EAF2A
Source IP Address: 0.0.0.0
Dest IP Address: 255.255.255.255 0
Client Identifier: 08002B2EAF2A

DHCP Discover Message

2. DHCP Offers A Message:

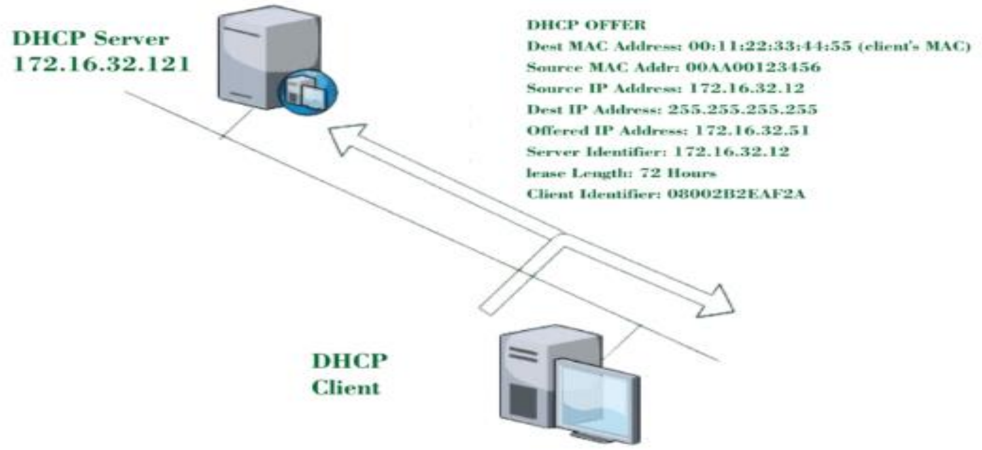
- After receiving the DHCP Discover message, the DHCP server responds with a DHCP Offer message.
- This message contains:
  - An available IP address (e.g., 192.16.32.51) for the client.
  - Other network settings like subnet mask, gateway, and lease time (e.g., 72 hours).

- A server ID to identify the DHCP server.

How It Works:

1. The server sends the offer message as a broadcast (255.255.255.255), so all devices can receive it.
2. The client's MAC address (e.g., 00:11:22:33:44:55) is included to ensure the right device gets the offer.
3. The first offer received is accepted by the client if multiple servers respond.
4. The lease time (e.g., 72 hours**)** means the client can use the IP for that period before needing renewal.

This step helps the client get an IP address and start communicating on the network.


DHCP Server
172.16.32.121
DHCP OFFER
Dest MAC Address: 00:11:22:33:44:55 (client's MAC)
Source MAC Addr: 00AA00123456
Source IP Address: 172.16.32.12
Dest IP Address: 255.255.255.255
Offered IP Address: 172.16.32.51
Server Identifier: 172.16.32.12
lease Length: 72 Hours
Client Identifier: 08002B2EAF2A
DHCP
Client

3. DHCP Request Message:

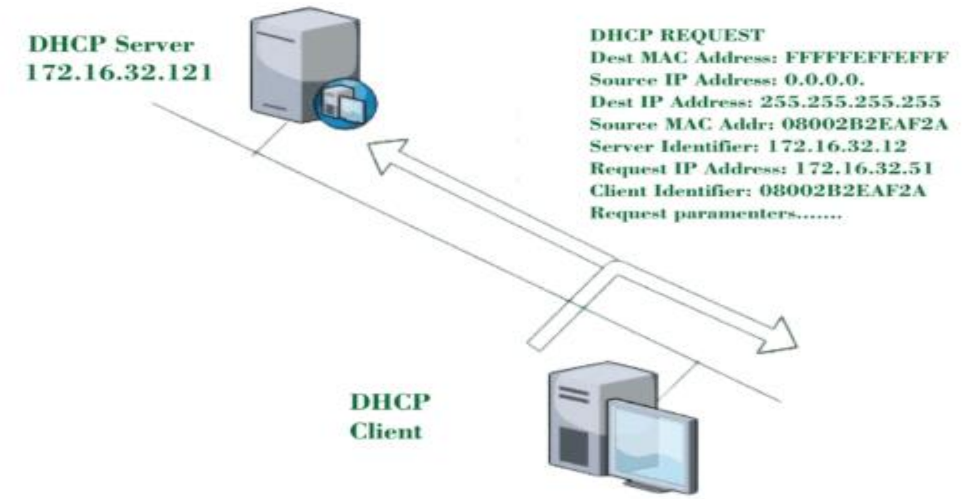
1. **Client Accepts the Offer:**
   - After receiving the DHCP Offer from the server, the client sends a DHCP Request message to confirm that it wants to use the offered IP address.
2. **Checking for IP Conflicts (Gratuitous ARP):**
   - Before accepting the IP, the client sends an ARP request to check if any other device is already using that IP.
   - If no device responds, it means the IP is available.
3. **Broadcasting the Request:**
   - The client broadcasts the DHCP Request message to the server.
   - Since it still doesn't have an IP, the source IP remains **0.0.0.0**.

  - The destination IP is **255.255.255.255** (broadcast to all).
  - The source MAC address is the client's MAC (08002B2EAF2A), and the destination MAC is FFFFFFFFFFFF (broadcast).

4. **Purpose of This Step:**
   - It tells the DHCP server that the client agrees to use the offered IP and network settings**.**
   - It also notifies other DHCP servers that their offers were not accepted (if multiple servers responded).

Summary:

- The client first checks if the IP is already in use using ARP.
- If no conflicts, it sends a request to the DHCP server to confirm the IP allocation.
- The request is broadcasted to all, ensuring only the right server finalizes the process.


DHCP Server
172.16.32.121
DHCP REQUEST
Dest MAC Address: FFFFFEFFFEFFF
Source IP Address: 0.0.0.0.
Dest IP Address: 255.255.255.255
Source MAC Addr: 08002B2EAF2A
Server Identifier: 172.16.32.12
Request IP Address: 172.16.32.51
Client Identifier: 08002B2EAF2A
Request paramenters.......
DHCP
Client

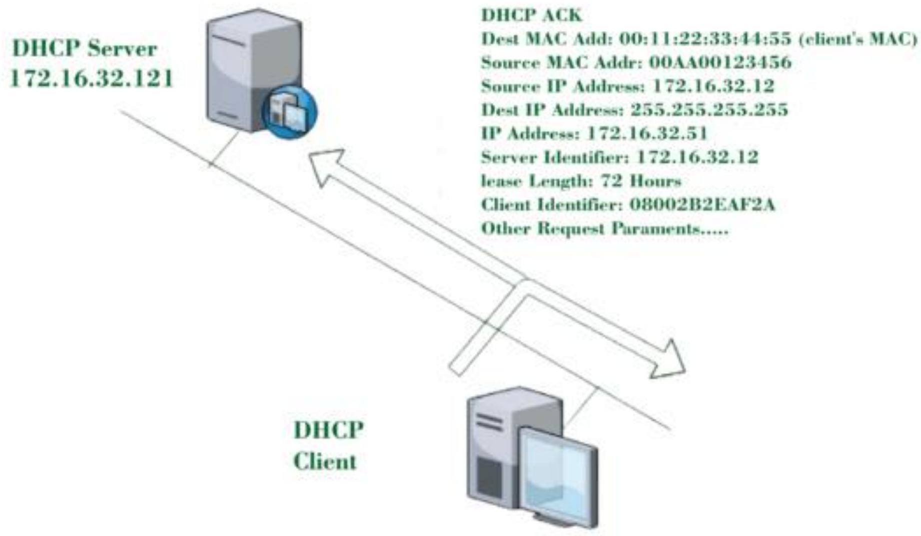
4. DHCP Acknowledgment Message:

1. **Server Confirms the IP Assignment:**
   - After receiving the DHCP Request from the client, the DHCP server finalizes the process by sending a DHCP Acknowledgment (ACK) message.
   - This confirms that the client can now officially use the assigned IP address.
2. **Server Reserves the IP for the Client:**
   - The server makes an entry in its database, linking the client's MAC address to the assigned IP address**.**
   - This means no other device will receive this IP until the lease time expires.

3. **Message Details:**
   - The server sends the ACK message as a broadcast (255.255.255.255) so the client gets it.
   - **Source IP:** 172.16.32.12 (DHCP server’s IP).
   - **Destination IP:** 255.255.255.255 (broadcast).
   - **Source MAC:** 00AA00123456 (server’s MAC).
   - **Destination MAC:** 00:11:22:33:44:55 (client’s MAC).
4. **Client Can Now Use the IP Address:**
   - Once the client receives the ACK message**,** it officially starts using the IP assigned by the DHCP server.

Summary:

- The **server locks the IP** for the client and ensures no other device gets the same IP.
- The **client receives confirmation** and can now communicate on the network.
- The **lease time starts**, meaning the client can use this IP for a set period before renewing.


DHCP Server
172.16.32.121
DHCP ACK
Dest MAC Add: 00:11:22:33:44:55 (client's MAC)
Source MAC Addr: 00AA00123456
Source IP Address: 172.16.32.12
Dest IP Address: 255.255.255.255
IP Address: 172.16.32.51
Server Identifier: 172.16.32.12
lease Length: 72 Hours
Client Identifier: 08002B2EAF2A
Other Request Paraments.....
DHCP
Client

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.

Advantages

- Centralized management of IP addresses.
- Centralized and automated TCP/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.

Introduction to IP Address

An **IP Address (Internet Protocol Address)** is a unique number assigned to each device connected to a network. It works like a home address for devices, allowing them to send and receive data over the internet or a local network.

Types of IP Addresses

1. **Public IP Address** – Used to connect to the internet (assigned by ISPs).
2. **Private IP Address** – Used within a local network (e.g., home or office).
3. **Static IP Address** – Fixed and does not change over time.
4. **Dynamic IP Address** – Changes periodically, assigned by a DHCP server.

Why is an IP Address Important?

An IP address is crucial for communication, security, and identification in networks. Here's why it matters:

1. Enables Device Communication

Every device (computer, phone, and server) needs an IP address to communicate over a network.

Just like a home address helps mail reach the right house, an IP ensures data reaches the correct device. Example:

When you visit a website, your device sends a request to the website's IP address, and the website responds to your IP with the requested content.

2. Identifies Devices on a Network

Each device in a network (home, office, or internet) has a unique IP address. It Helps in troubleshooting network issues and monitoring connected devices.

Example:

If an IT admin wants to find out which computer is using the most bandwidth, they can track the IP address.

3. Enables Internet Browsing

When you type a website name (e.g., google.com), your device first finds the IP address of the website using DNS (Domain Name System).

Without IP addresses, the internet wouldn’t work, as devices wouldn’t know where to send data.

Example: google.com is actually linked to an IP like 142.250.190.78.

4. Supports Network Security & Access Control

Helps firewalls and security systems block or allow traffic based on IP addresses.

Can be used for geo-blocking, VPNs, and security monitoring.

Example: Banks use IP tracking to detect suspicious logins from unknown locations.

5. Enables Remote Access & Hosting

IPs allow users to connect to devices remotely using Remote Desktop, VPNs, and cloud services.

Websites, servers, and online services need IP addresses to be accessible worldwide.

Example: A company may use a Static IP to host a website or allow remote employees to securely access company resources.

6. Necessary for IoT & Smart Devices

Smart home devices (like Alexa, CCTV cameras, and smart thermostats) use IP addresses to communicate and function properly.

Example: A smart doorbell connects to your phone over Wi-Fi using its unique IP address.

How to Look Up IP Addresses?

In Windows

- Open the Command Prompt.
- Type ipconfig and press Enter.
- Look for your IP under your network connection.

On Mac

- Open System Preferences > Network.
- Select your active connection.
- You’ll see your IP address in the connection details.

On iPhone

- Go to Settings > Wi-Fi.
- Tap the (i) icon next to your network.
- Find your IP under “IP Address.”

IPv4 (Internet Protocol Version 4)

IPv4 (Internet Protocol Version 4) is the older and most commonly used type of IP address. It uses a 32-bit address format, meaning it can create about 4.3 billion unique addresses. However, because of the growing number of internet-connected devices, we are running out of IPv4 addresses.

Characteristics of IPv4

32-bit address length: Allows for approximately 4.3 billion unique addresses.

Dot-decimal notation: IP addresses are written in a format of four decimal numbers separated by dots, such as 192.168.1.1.

Packet structure: Includes a header and payload; the header contains information essential for routing and delivery.

Checksum fields: Uses checksums in the header for error-checking the header integrity.

Fragmentation: Allows packets to be fragmented at routers along the route if the packet size exceeds the maximum transmission unit (MTU).

Address Resolution Protocol (ARP): Used for mapping IP network addresses to the hardware addresses used by a data link protocol.

Manual and DHCP configuration: Supports both manual configuration of IP addresses and dynamic configuration through DHCP (Dynamic Host Configuration Protocol).

Limited address space: The main limitation which has led to the development of IPv6 to cater to more devices.

Network Address Translation (NAT): Used to allow multiple devices on a private network to share a single public IP address.

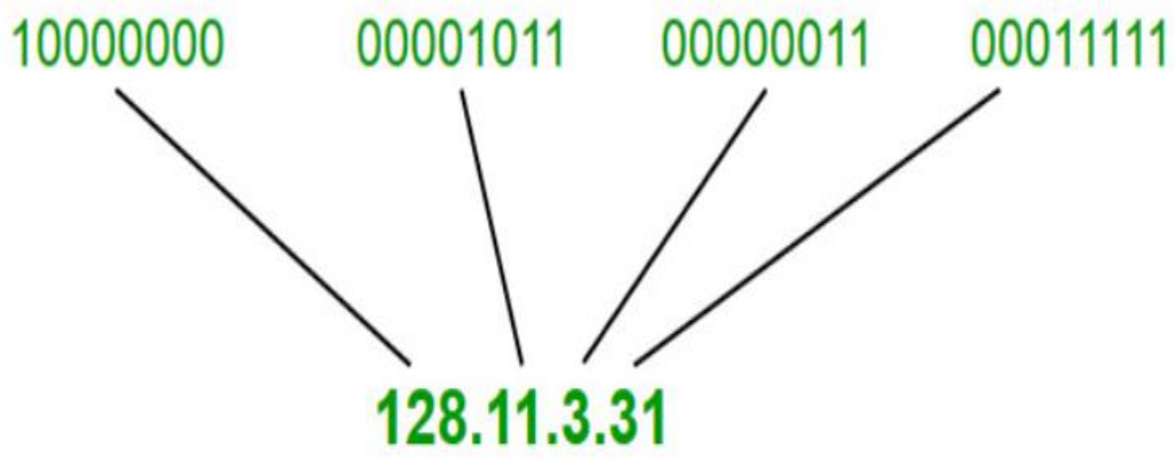
Security: Lacks inherent security features, requiring additional protocols such as IPSec for secure communications.

Example of an IPv4 Address:

➞ 192.168.1.1 (This is similar to your home Wi-Fi router's IP address)

Problem with IPv4:

- Limited number of addresses
- Requires NAT (Network Address Translation) to allow multiple devices to share one public IP.



IPv6 (Internet Protocol Version 4)

IPv6 (Internet Protocol Version 4) is the newer version designed to solve the IPv4 address shortage. It uses a 128-bit address format, which means it can support trillions of unique addresses. This ensures that every device (phones, laptops, smart gadgets) can have its own unique IP address without needing NAT.

To switch from IPv4 to IPv6, there are several strategies:

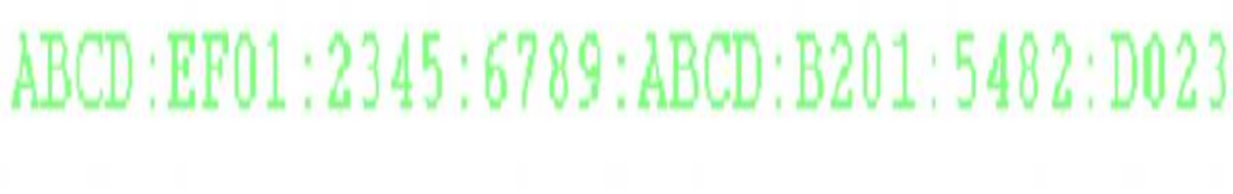
Dual Stacking: Devices can use both IPv4 and IPv6 at the same time. This way, they can talk to networks and devices using either version.

Tunneling: This method allows IPv6 users to send data through an IPv4 network to reach other IPv6 users. Think of it as creating a "tunnel" for IPv6 traffic through the older IPv4 system.

Network Address Translation (NAT): NAT helps devices using different versions of IP addresses (IPv4 and IPv6) to communicate with each other by translating the addresses so they understand each other.

Example of an IPv6 Address:

➞ 2001:db8::ff00:42:8329 (Looks longer and more complex than IPv4)



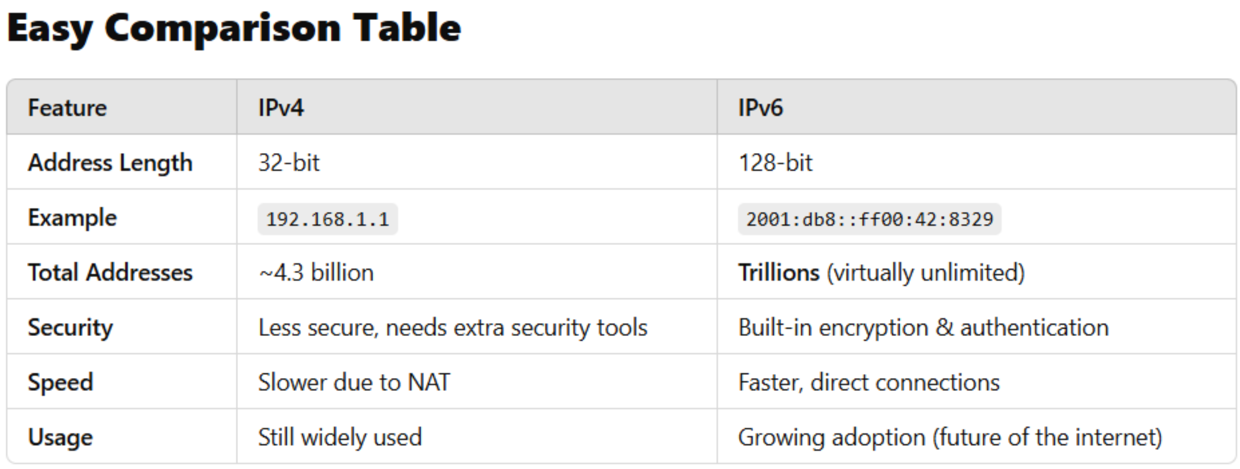
ABCD:EF01:2345:6789:ABCD:B201:5482:D023

Why IPv6 is better?

- More addresses (no risk of running out)
- Faster communication (removes NAT, allowing direct connections)
- Better security (built-in encryption and authentication)
- Supports modern devices and networks

Why Are We Still Using IPv4?

- Most networks & devices still support IPv4
- Switching to IPv6 takes time and investment
- Some old systems do not support IPv6.



Easy Comparison Table

Feature	IPv4	IPv6
Address Length	32-bit	128-bit
Example	`192.168.1.1`	`2001:db8::ff00:42:8329`
Total Addresses	~4.3 billion	**Trillions** (virtually unlimited)
Security	Less secure, needs extra security tools	Built-in encryption & authentication
Speed	Slower due to NAT	Faster, direct connections
Usage	Still widely used	Growing adoption (future of the internet)