UNIT-4

NETWORK ADMINISTRATION PROTOCOLS AND SERVICES

4.1 DIRECTORY SERVICE

4.1.1 Directory

In computer networks, a directory store and organize no of users, their passwords and information about network resources that users can access. Network resources may be printers, computers, scanners etc.

4.1.2 Directory Services

- A Directory Service is nothing but a software system that responds to requests for information about entities, e.g. people in an organization.
- A directory service is a software system that stores, organizes and provides access to information in a computer operating system's directory.
- For ex: A user account is data then metadata specifies what information is included in every user account object.
- X.500 and Network Information Service (NIS) are examples of directory services.
- Organizations have a need to store information in a centralized data store so that it can be added to, deleted, modified, and queried by users and applications.
- The information stored could be user accounts, e-mail addresses, digital certificates, component object names, network names, printers, groups, etc.
- There is a need to access this information both from within the enterprise and from the Internet.
- The amount of information stored varies greatly with the customer. This data store has come to be known as a Directory Service.
- For our own use, we all maintain personal address directory where we store addresses, telephone nos. and other information in a format that is most suitable for us.
- But when we talk about maintaining a global directory service on Internet or in any organization,

The Directory Service must be:

- Flexible enough to store a range of information types
- Secure when accessing from both the Internet and intranet
- Scalable from a small business to the largest enterprise
- Extensible as business needs change
- Accessible via an open, standards-based protocol.

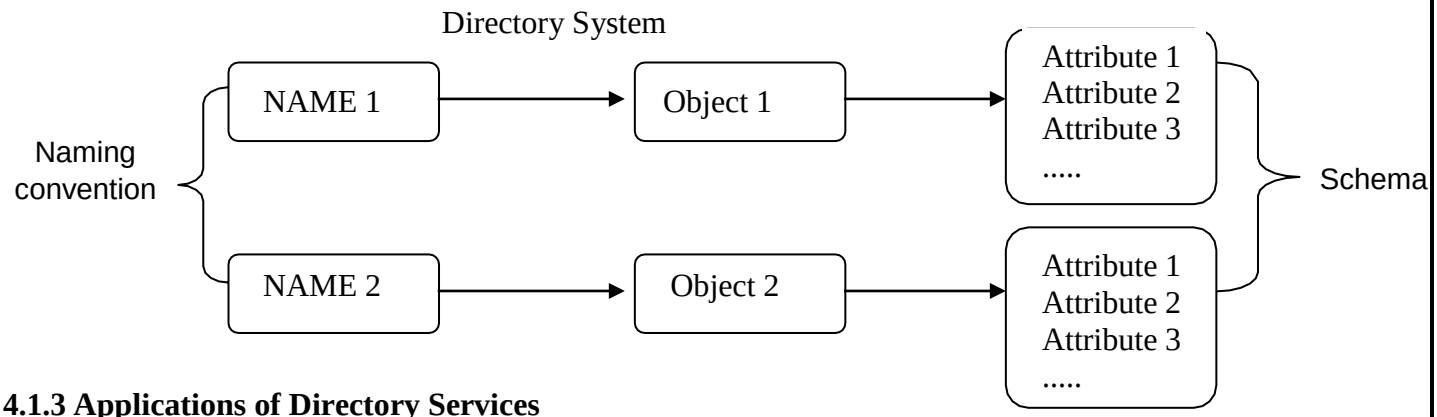
Directory service are important because they provide proper way to name, describe, locate access, manage and secure information about these resources.

A directory services uses standard protocols and API's to access the information contained in the directory.

Objects / Resources:

Emails, computers, peripheral devices (printer, scanner.....) etc. A directory object contains attributes that describe the object.

Directory service = Naming service + Object containing attributes



4.1.3 Applications of Directory Services

- Resource planning
- Security and firewalls
- Resource provisioning – for supplying or providing recourses.
- Deployment of e-business and extra-net applications.
- Value chain management - it focus on minimizing resources and accessing at each chain level, resulting in optimal process integration, decreased inventories, better products and enhanced customer satisfaction.

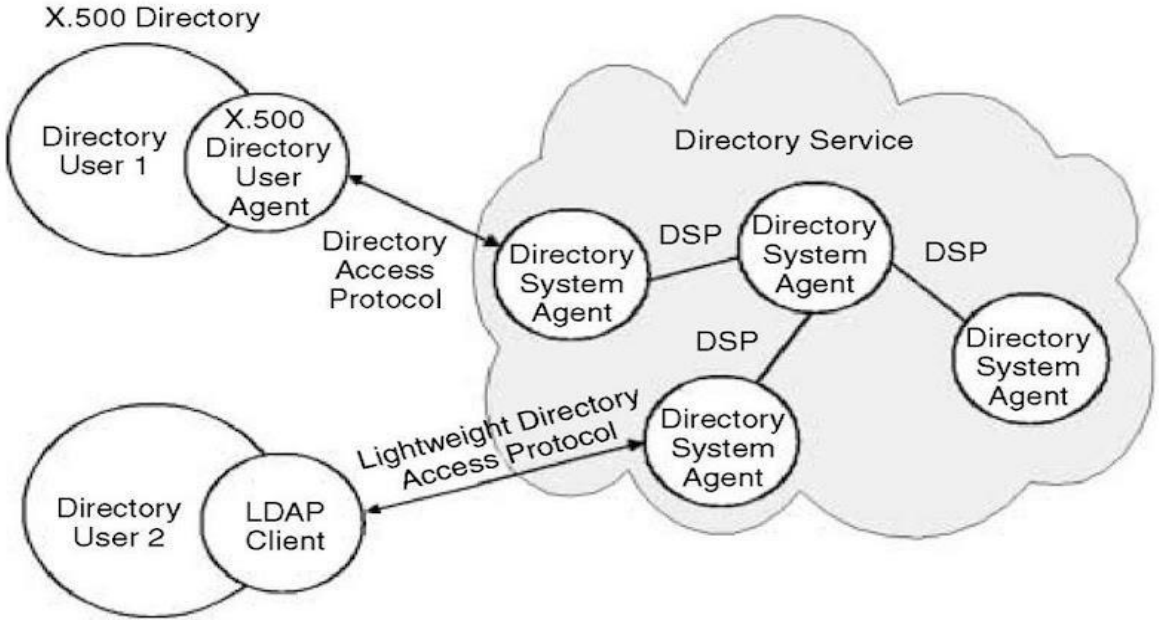
4.2 DIRECTORIES ACCESS PROTOCOLS

4.2.1 Novel Directory

- Novell directory service (NDS) is a popular software product for managing access to computer resources and keeping track of the users of a network.
- Using NDS, a network administrator can set-up a database of users and manage them using a directory with an easy-to-use graphical user interface.
- Users of computer at remote location can be added, updated and managed centrally.
- Application can be distributed electronically and maintained centrally.
- NDS can be installed to run under Windows NT, Sun-Microsystems's Solaris and UNIX and as well as under Novelle's own Netware.
- So, it can be used to control a multi-platform network.
- It also called Netware Directory Services.
- NDS automatically maintains directory information about network Internet protocol (IP) domain name and DHCP information.

4.2.2 X.500 Directory Service

- The X.500 protocol was first approved in 1988 and then enhanced in 1993 under the auspices of the International Telecommunications Union (ITU).
- Its purpose was to provide an international standard for directory systems.
- The X.500 protocol architecture consists of a Client-Server communicating via the Open Systems Interconnection (OSI) networking model. The Client is called the Directory Service Agent (DUA) and the Server is called the Directory System Agent (DSA).
- X.500 is a directory service used in the same way as a conventional name service, but it is primarily used to satisfy descriptive queries and is designed to discover the names and attributes of other users or system resources.
- Users may have a variety of requirements for searching and browsing in a directory of network users, organizations and system resources to obtain information about the entities that the directory contains.
- The uses for such a service are likely to be quite diverse.
- They range from enquiries that are directly analogous to the use of telephone directories, such as a simple „white pages" access to obtain a user's electronic mail address or a „yellow pages" query aimed, for example, at obtaining the names and telephone numbers of garages specializing in the repair of a particular make of car, to the use of the directory to access
- Personal details such as job roles, dietary habits or even photographic images of the individuals.



- The above figure shows model for X.500.
- In the X.500 directory architecture, the client queries and receives responses from one or more servers in the server's Directory Service with the Directory Access Protocol (DAP) controlling the communication between the client and the server.

- The Directory client, called the Directory User Agent (DUA), supports users in searching or browsing through one or more directory databases, and in retrieving the requested directory information.
- The DUA can be implemented in all kinds of user interfaces through dedicated DUA clients, Web-server gateways, e-mail applications, or middleware. DUAs are currently available for virtually all types of workstations.
- Directory information is stored in a Directory System Agent (DSA), a hierarchical database designed to provide fast and efficient search and retrieval. The Directory System Protocol (DSP) controls the interaction between two or more DSAs. This is done in a way that allows users to access information in the Directory without knowing its exact location.
- The Directory Access Protocol (DAP) is used for controlling communication between a DUA and DSA.

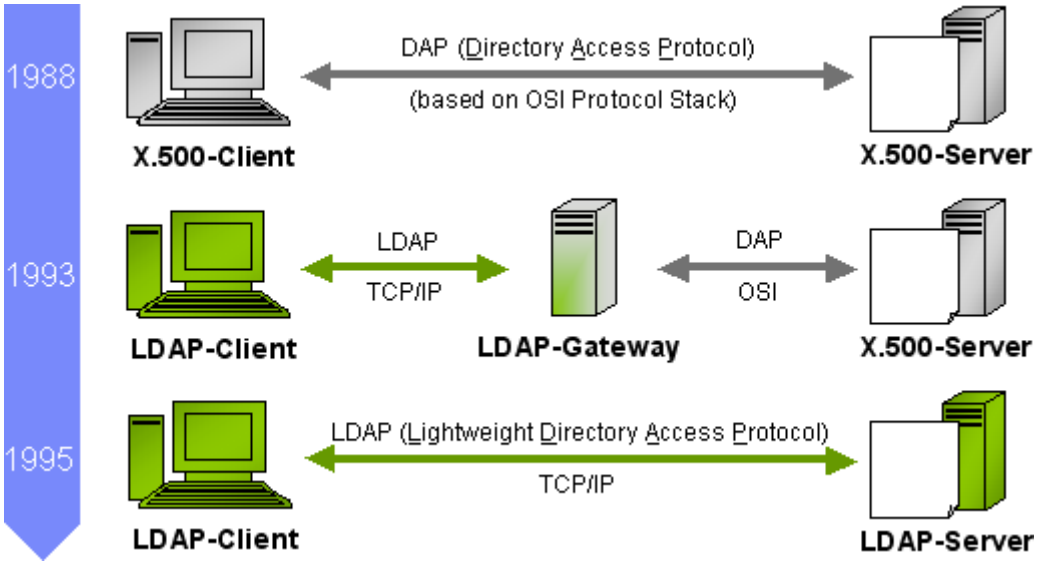
4.2.3 LDAP

- LDAP is a standard protocol designed to maintain and access "directory services" within a network. Think of a directory service as a phonebook for different network resources like files, printers, users, devices, and servers, etc.
- For example, an organization may store information for all their printers in a directory. LDAP can enable users to search for a specific printer, locate it on the network, and securely connect to it.
- LDAP is widely used to build central authentication servers. These servers contain usernames and passwords for all the users within a network. Any-and-all applications and services can connect to the LDAP server to authenticate and authorize users.
- LDAP directories typically contain data that is regularly accessed, but rarely changed. LDAP is designed to deliver exceptionally fast READ performance, even for larger datasets. However, the WRITE performance is significantly lower.
- Stands for Lightweight Directory Access Protocol.
- LDAP is a scaled-down implementation of the X.500 standard.
- Active Directory is based on LDAP.
- LDAP Is light weight
- Sufficient straight forward
- Easy To implement as against X.500 dap
- It uses string to represent data
- It is an application protocol used over an IP network to manage and access the distributed directory information service.

LDAP Security Model:

- It defines how information can be protected from unauthorized access.
- There are several LDAP API (Application Programming Interface) oldest ones written in C
- Now a days LDAP API's are available in other programming languages like Perl and Java

- LDAP Directory Service is based on client server model
- LDAP is a message oriented protocol
- Client constructs an LDAP message containing a request and sends it to the server and server reply to according to client's request.
- A client needs to connect to the server known as a Directory system Agent which is set by default to use TCP port 389.
- Directory data is represented as attribute-value pair.
- Any specific piece of information is associated with a descriptive attribute
- LDAP provides directory access, a centralized database of information about people, groups and other entities.
- It is defined as a set of protocol operations against servers.
- Assumes one (or more) servers which jointly provide access to the DIT (Directory Information Tree)
- An LDAP directory is organized in a simple "tree" hierarchy consisting of the following levels:
- The root directory (the starting place or the source of the tree), which branches out to Countries, each of which branches out to Organizations, which branch out to Organizational units (divisions, departments, and so forth), which branches out to (includes an entry for) Individuals (which includes people, files, and shared resources such as printers).



Advantages of LDAP:

- Data present in LDAP is available to many clients and libraries.
- LDAP support many types of application.
- LDAP is very general and has basic security.

Disadvantages in LDAP:

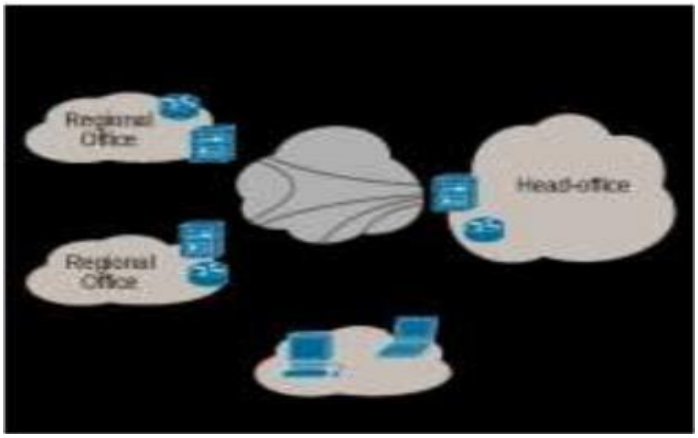
- It does not handle well relational database

4.3 MS ACTIVE DIRECTORY

- The computers in a Windows domain share a database called the Active Directory.
- The database is centralized, organized, and accessible to the resources of the domain.
- The domain controller stores the resource information and the security settings of an organization in the Active Directory.
- The Active Directory is a directory service that performs the following functions.
- As a directory, it stores information about users and resources
- As a service or services, it provides access to manipulate the resources
- The Active Directory manages all elements of the network, including computers, groups, users, domains, security policies, and other type of user-defined objects.
- An Active Directory can also be considered as a distributed database that can have enterprise scope if configured.
- An Active Directory provides distributed security, user, group, and computer management dynamic name services.
- Active Directory allows administrators to organize objects of a network (such as users, computers, and devices) into a hierarchical collection of containers known as the logical structure.
- The following are the logical components of an Active Directory.
  - **Forests**
  - **Trees**
  - **Organizational Units (OUs)**
  - **Site**
  - **Objects**

4.4 Virtual Private Network [VPN]

- A Virtual Private Network (VPN) is a network technology that creates a secure network connection over a public network such as the Internet or a private network owned by a service provider. Large corporations, educational institutions, and government agencies use VPN technology to enable remote users to securely connect to a private network.
- A VPN can connect multiple sites over a large distance just like a Wide Area Network (WAN). VPNs are often used to extend intranets worldwide to disseminate information and news to a wide user base.
- Educational institutions use VPNs to connect campuses that can be distributed across the country or around the world.
- In order to gain access to the private network, a user must be authenticated using a unique identification and a password.



4.4.1 Types of VPN

1. Remote Access VPN -

- It is also called as Virtual Private dial-up network (VPDN) is mainly used in scenarios where remote access to a network becomes essential.
- Remote access VPN allows data to be accessed between a company's private network and remote users through a third party service provider; Enterprise service provider.
- Remote Access VPN permits a user to connect to a private network and access all its services and resources remotely.
- The connection between the user and the private network occurs through the Internet and the connection is secure and private.
- Remote Access VPN is useful for home users and business users both. An employee of a company, while he/she is out of station, uses a VPN to connect to his/her company's private network and remotely access files and resources on the private network.
- Private users or home users of VPN, primarily use VPN services to bypass regional restrictions on the Internet and access blocked websites.
- Users aware of Internet security also use VPN services to enhance their Internet security and privacy.

2. Site to Site VPN

- A Site-to-Site VPN is also called as Router-to-Router VPN and is commonly used in the large companies. Companies or organizations, with branch offices in different locations, use Site-to-site VPN to connect the network of one office location to the network at another office location.
- Two types of site to site VPN
  - **Intranet based VPN**

    This type of VPN can be used when multiple Remote locations are present and can be made to join to a single network. Machines present on these remote locations work as if they are working on a single network.

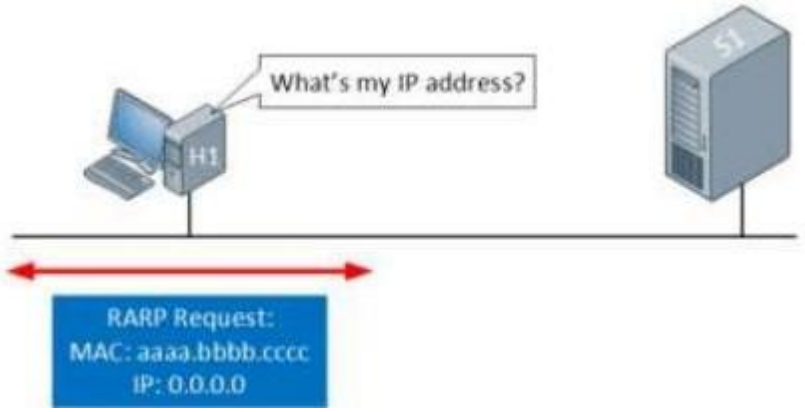
➢ **Extranet based VPN**

This type of VPN can be used when several different companies need to work in a shared environment. When companies use Site-to-site VPN type to connect to the office of another company, it is called as Extranet based VPN. E.g. Distributors and service companies. This network is more manageable and reliable.

4.5 DHCP ARCHITECTURE, RARP AND BOOTP

4.5.1 RARP (Reverse Address Resolution Protocol)

- (RARP) finds the logical address for a machine that knows only its physical address. Each host or router is assigned one or more logical (IP) addresses, which are unique and independent of the physical (hardware) address of the machine.
- To create an IP datagram, a host or a router needs to know its own IP address or addresses. The IP address of a machine is usually read from its configuration file stored on a disk file.
- However, a diskless machine is usually booted from ROM, which has minimum booting information. The ROM is installed by the manufacturer. It cannot include the IP address because the IP addresses on a network are assigned by the network administrator.



- The machine can get its physical address (by reading its NIC, for example), which is unique locally. It can then use the physical address to get the logical address by using the RARP protocol. A RARP request is created and broadcast on the local network. Another machine on the local network that knows all the IP addresses will respond with a RARP reply.
- The requesting machine must be running a RARP client program; the responding machine must be running a RARP server program.
- There is a serious problem with RARP: Broadcasting is done at the data link layer. The physical broadcast address, associates in the case of Ethernet, does not pass the boundaries of a network.
- This means that if an administrator has several networks or several subnets, it needs to assign a RARP server for each network or subnet.

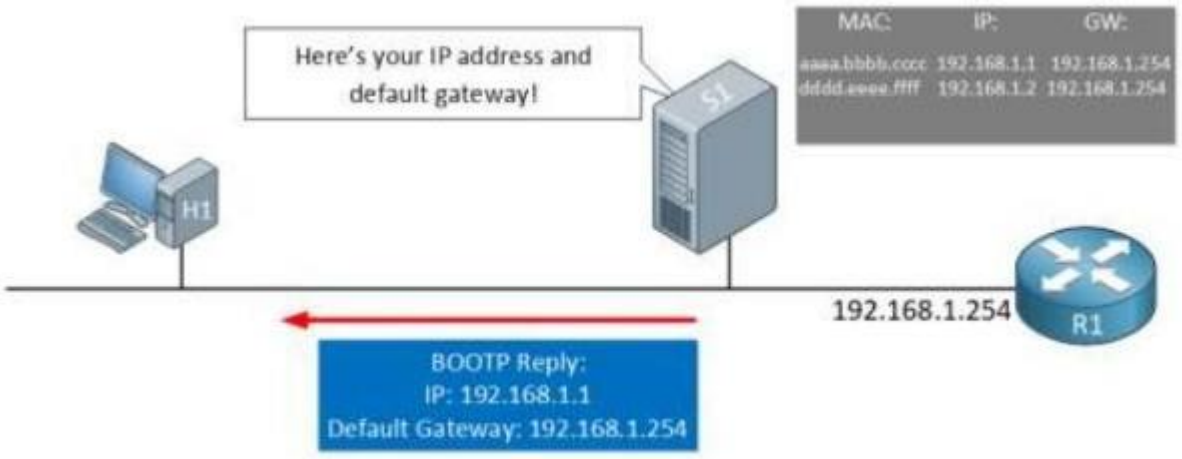
Disadvantages of RARP

The Reverse Address Resolution Protocol had few disadvantages which eventually led to its replacement by BOOTP and DHCP. Some of the disadvantages are listed below:

- The RARP server must be located within the same physical network.
- The computer sends the RARP request on very cheap layer of the network. Thus, it's unattainable for a router to forward the packet because the computer sends the RARP request on very cheap layer of the network.
- The RARP cannot handle the subnetting process because no subnet masks are sent. If the network is split into multiple subnets, a RARP server must be available with each of them.
- It isn"t possible to configure the PC in a very modern network.
- It doesn't fully utilize the potential of a network like Ethernet.

4.5.2 BOOTP (Bootstrap Protocol)

- The Bootstrap Protocol (BOOTP) is a client/server protocol designed to provide physical address to logical address mapping. BOOTP is an application layer protocol.
- The administrator may put the client and the server on the same network or on different networks. BOOTP messages are encapsulated in a UDP packet, and the UDP packet itself is encapsulated in an IP packet.
- One of the advantages of BOOTP over RARP is that the client and server are application-layer processes.
- As in other application-layer processes, a client can be in one network and the server in another, separated by several other networks. However, there is one problem that must be solved.
- The BOOTP request is broadcast because the client does not know the IP address of the server.
- A broadcast IP datagram cannot pass through any router.
- To solve the problem, there is a need for an intermediary. One of the hosts (or a router that can be configured to operate at the application layer) can be used as a relay.
- The host in this case is called a relay agent.
- The relay agent knows the unicast address of a BOOTP server. When it receives this type of packet, it encapsulates the message in a unicast datagram and sends the request to the BOOTP server. The packet, carrying a unicast destination address, is routed by any router and reaches the BOOTP server.
- The BOOTP server knows the message comes from a relay agent because one of the fields in the request message defines the IP address of the relay agent.



- The relay agent, after receiving the reply, sends it to the BOOTP client.

4.5.3 Dynamic Host Configuration Protocol (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
- DHCP is based on a client-server model and based on discovery, offer, request, and ACK.
- DHCP port number for server is 67 and for the client is 68.
- It is a Client server protocol which uses UDP services. 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 DORA process, but there are 8 DHCP messages in the process.
- 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.

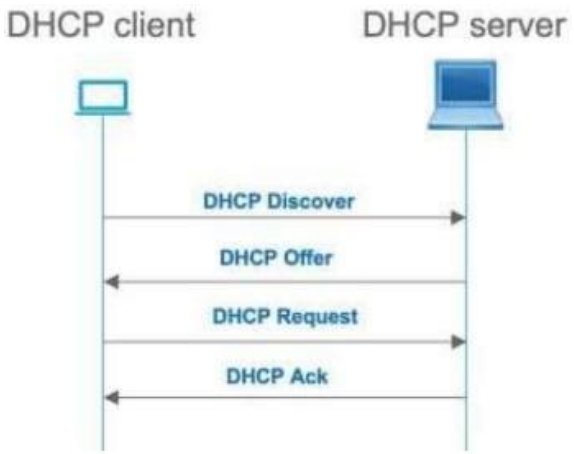
Components of DHCP

- DHCP server: It automatically provides network information (IP address, subnet mask, gateway address) on lease. Once the duration is expired, that network information can be assigned to another machine. It also maintains the data storage which stores the available IP addresses.
- DHCP client: Any node which requests an IP address allocation to a network is considered a DHCP client.
- DHCP Relay Agent: In case, we have only one DHCP server for multiple LAN‟s then this Agent which presents in every network forwards the DHCP request to the DHCP server. So, using DHCP Relay Agent we can configure multiple LANs with a single server

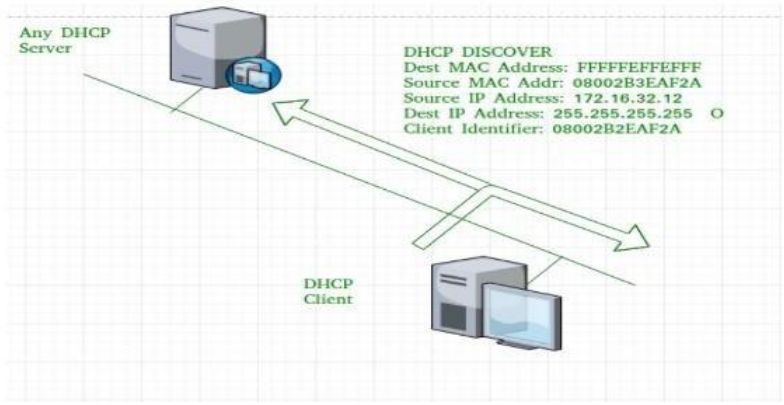
DHCP operation

- Manual Allocation: The administrator manually assigns a pre-allocated IP address to the client and DHCP only communicates the IP address to the device.
- Automatic Allocation: DHCP automatically assigns a static IP address permanently to a device, selecting it from a pool of available addresses. There is no lease and the address is permanently assigned to a device.
- Dynamic Allocation: DHCP automatically dynamically assigns, or leases, an IP address from a pool of addresses for a limited period of time chosen by the server, or the address will be withdrawn when the client tells the DHCP server that it no longer needs the address.

DHCP basically work on DORA process:



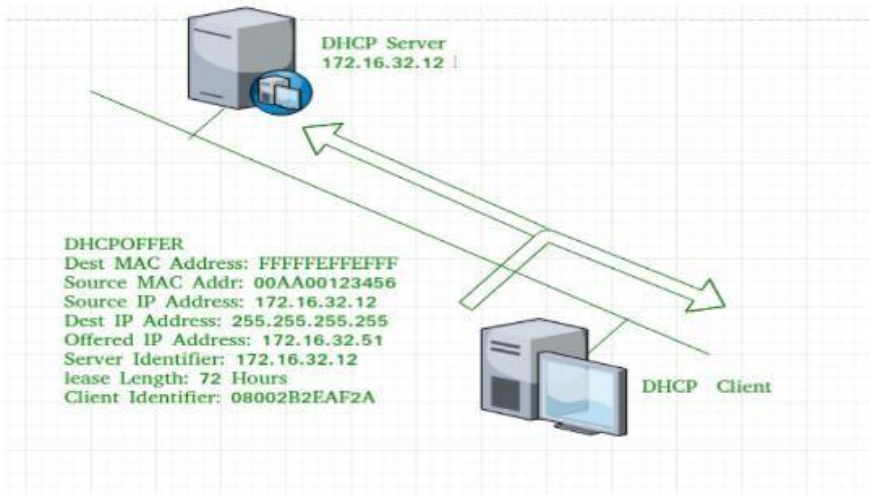
1. DHCP discover message:
   - This is the first message generated in the communication process between the server and the client.
   - This message is generated by the Client host in order to discover if there is any DHCP server/servers are present in a network or not.
   - This message is broadcasted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



- 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:

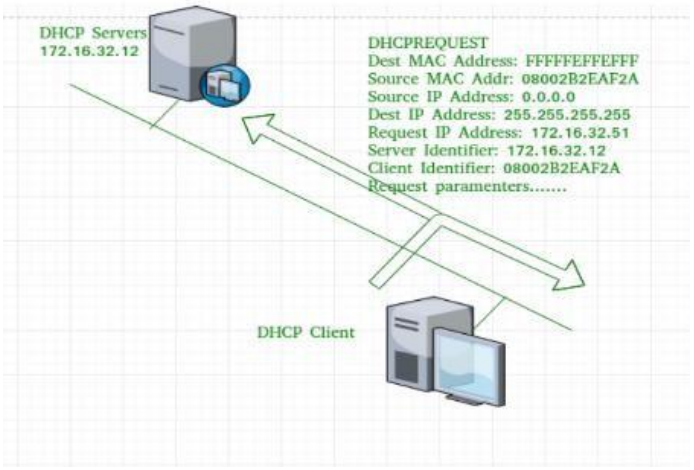
- The server will respond to the host in this message specifying the unleased IP address and other TCP configuration information.
- This message is broadcasted by the server and size of the message is 342 bytes.
- If there is more than one DHCP server present in the network then the client host will 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 FFFFFFFFFFFF.
- Here, the offer message is broadcast by the DHCP server therefore destination IP address is the broadcast IP address and destination MAC address is FFFFFFFFFFFF and the source IP address is the server IP address and the MAC address is the server MAC address.

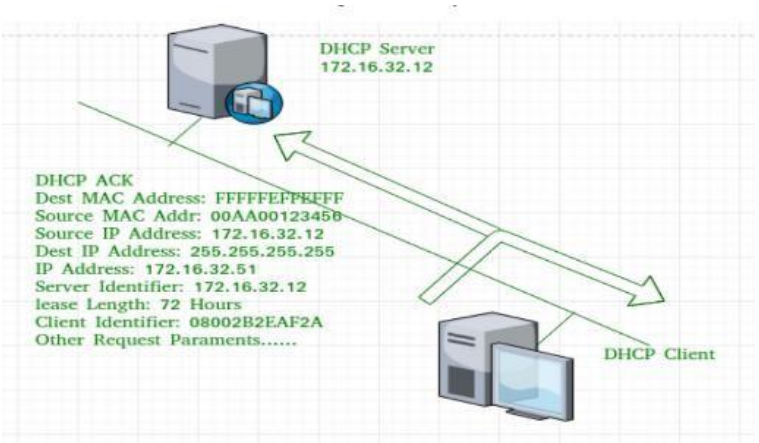
- Also, the server has provided the offered IP address 192.16.32.51 and a lease time of 72 hours (after this time the entry of the host will be erased from the server automatically). Also, the client identifier is the PC MAC address (08002B2EAF2A) for all the messages.

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.

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 FFFFFFFFFFFF 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 Nek 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:

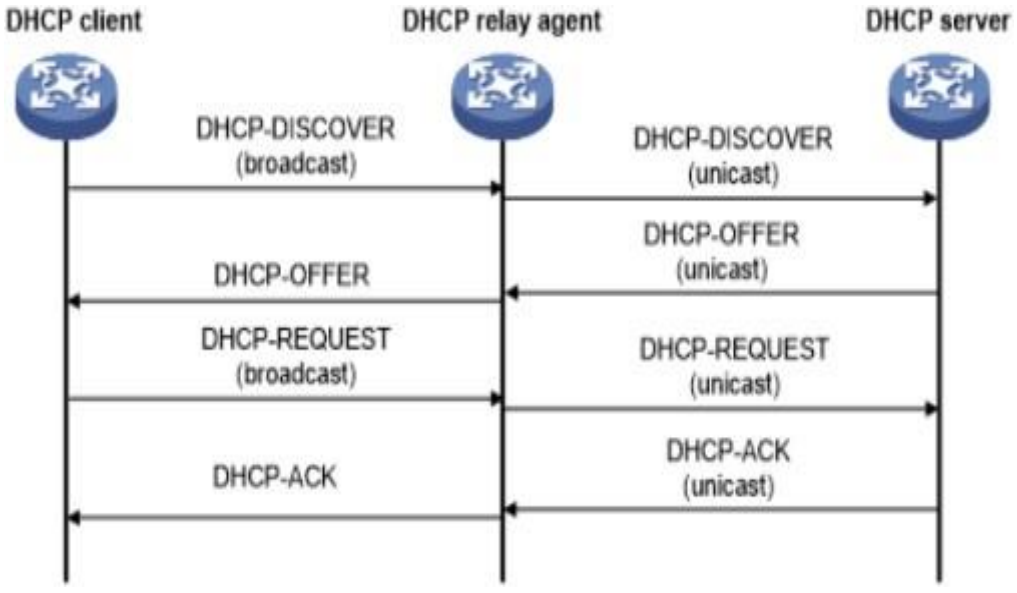
   If the DHCP client determines the offered configuration parameters are different or invalid, it sends a DHCP decline message to the server. When there is a reply to the gratuitous ARP by any host to the client, the client sends a DHCP decline message to the server showing the offered IP address is already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

- The DHCP relay agent is any TCP/IP host which is used to forward requests and replies between the DHCP server and client when the server is present on a different network.
- Relay agents receive DHCP messages and then generate a new DHCP message to send out on another INTERFACE. Also, the DHCP relay agent adds a giaddr (gateway address of the packet) field and also the Relay agent information option 82 if enabled. The options field is removed when the server reply is forwarded to the host.



Advantages of DHCP

The advantages of using DHCP include:

- 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 addresses 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.