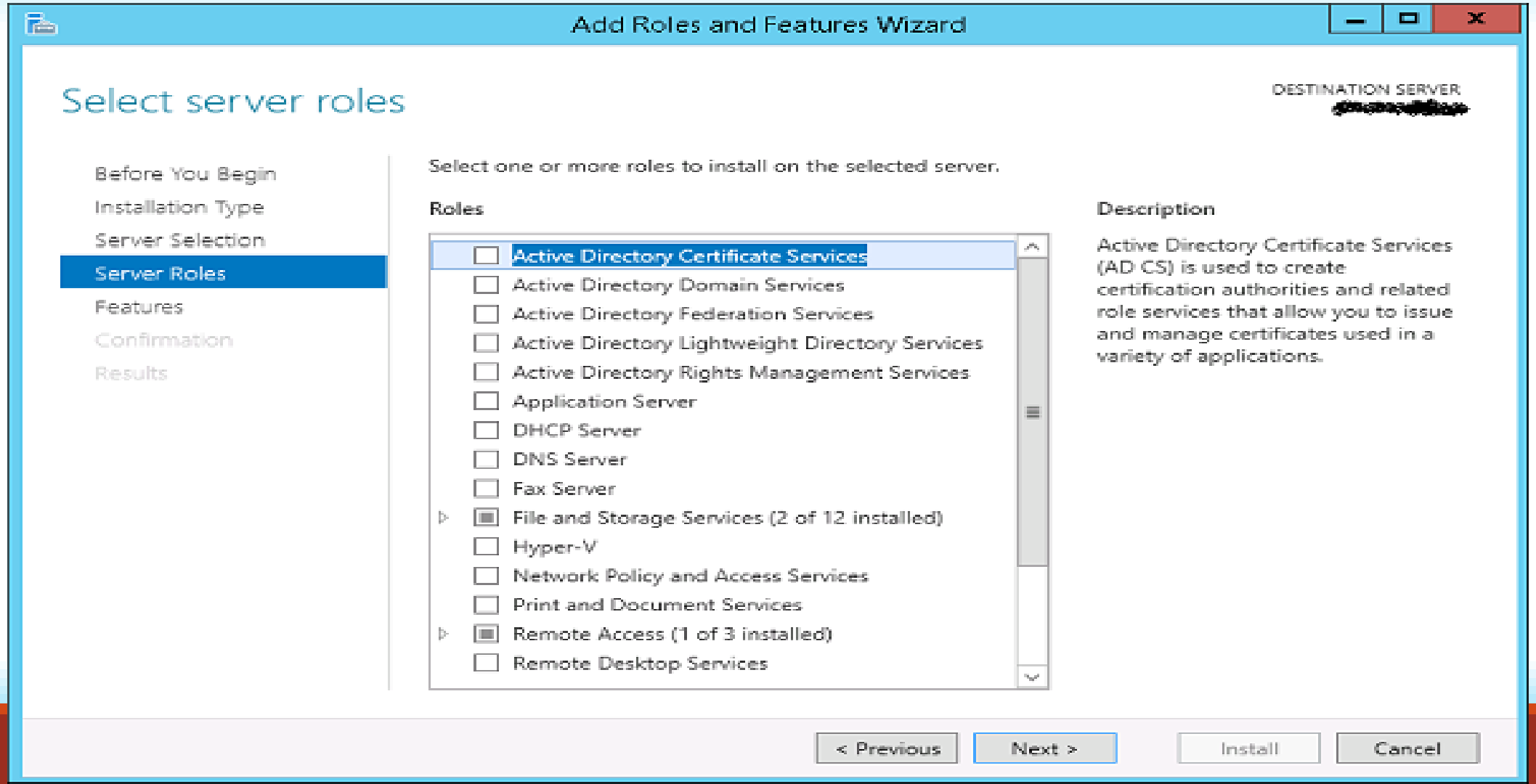
Server Roles and Features

CET 05202: SERVER ADMINISTRATION

Ms Jamila L.

Server Roles and Features



Server Roles and Features

Roles and Features are the tools that you need to install or activate in order to complete your IT Administration duties, without their installation you cannot do anything.

One of the role and feature to be configured and activated are **Active directory, DHCP, DNS and etc.**

The Active Directory

Active Directory (AD) : Introduction

Active Directory (AD) is a proprietary directory service developed by Microsoft to manage the authentication and authorization of users and machines on a Windows domain network.

- Active Directory was first released in 2000 and runs on Windows Server. Microsoft developed AD to provide secure access to corporate networks.
- Active Directory stores information related to user accounts, computer objects, groups, policies and other resources on the network.
- It also provides an efficient way for administrators to manage the security settings of their organization's IT infrastructure.

Active Directory (AD) : Introduction cont…

Active Directory (AD) is a Microsoft technology used to manage computers and other devices on a network.

- It is a primary feature of Windows Server, an operating system that runs both local and Internet-based servers.

Active Directory **stores information about objects on the network** and makes this information easy for administrators and users to find and use.

Active Directory **uses a structured data store as the basis for a logical, hierarchical organization of directory information**

Primary components of Active Directory

1. Active Directory Domain Services (AD DS):

Active Directory Domain Services (AD DS) provides directory services for managing Windows-based computers on a network.

AD DS stores information about objects such as users, groups, computers, and other resources, and provides authentication and authorization services.

Active Directory uses a structured data store, which organizes directory information and is optimized to enhance query performance, making it easy for network users to quickly find and utilize any information they need.

Primary components of Active Directory

2. Domain Controller:

A server that is running Active Directory Domain Services is called a **domain controller.** Domain controllers **host and replicate the directory service database inside the forest.**

A domain controller (DC) is a network server that responds to security authentication requests and authorizes host access to domain resources.

- This server enforces security policies, authenticates registered users, and stores important user account information.
- Domain controllers manage and secure domain networks by only allowing authorized users access to directory services while denying unauthorized access.

Primary components of Active Directory

3. Lightweight Directory Services (AD LDS):

AD LDS is a Lightweight Directory Access Protocol (LDAP) directory service that offers dedicated data storage and APIs for accessing stored information.

- It functions independently of Active Directory and can function as a standalone data store or can replicate data.

4. Federation Services (AD FS):

Active Directory Federation Services (AD FS) is a service that allows the secure sharing of identity information between trusted business partners.

- It is based on industry standards and facilitates federations across extranets, enabling trusted partners to share sensitive identity data.

Primary components of Active Directory

5. Rights Management Services (AD RMS):

AD RMS enables users and admins to control access permissions for sensitive documents, workbooks, and presentations.

- By utilizing IRM policies, unauthorized individuals are prevented from duplicating and disseminating the restricted information.

6. Certificate Services (AD CS):

- Active Directory Certificate Services (AD CS) is a Windows server designed to issue digital certificates.
- AD CS offers digital certificates that have a wide range of applications, including the encryption and digital signing of documents and messages, as well as authenticating computer, user, or device accounts on a network.
- Certificates granted by AD CS are valid for a specified period and can be renewed or revoked as needed, providing granular control over the certificates' lifespan.

Common Terminologies in Active Directory Concepts:

Schema – A set of rules, the schema, that defines the classes of objects and attributes contained in the directory, the constraints and limits on instances of these objects, and the format of their names.

Global catalog – A global catalog that contains information about every object in the directory. This allows users and administrators to find directory information regardless of which domain in the directory actually contains the data.

Forest Root Domain – The first domain that is installed in an Active Directory Forest is referred to as the root domain.

Common Terminologies in Active Directory Concepts:

Sites – Sites in AD DS represent the physical structure, or topology, of your network. AD DS uses network topology information, which is stored in the directory as site, subnet, and site link objects, to build the most efficient replication topology.

Organizational Unit – An organizational unit (OU) is a container object in Active Directory that can hold other objects, such as users, groups, and computers. OUs are used to help organize objects within a domain and can be used to apply group policies to specific sets of objects.

Group Policy – Group Policy is a feature in Active Directory that allows administrators to define and enforce policies on groups of computers or users. These policies can include security settings, software deployment, and other system configurations.

Common Terminologies in Active Directory Concepts:

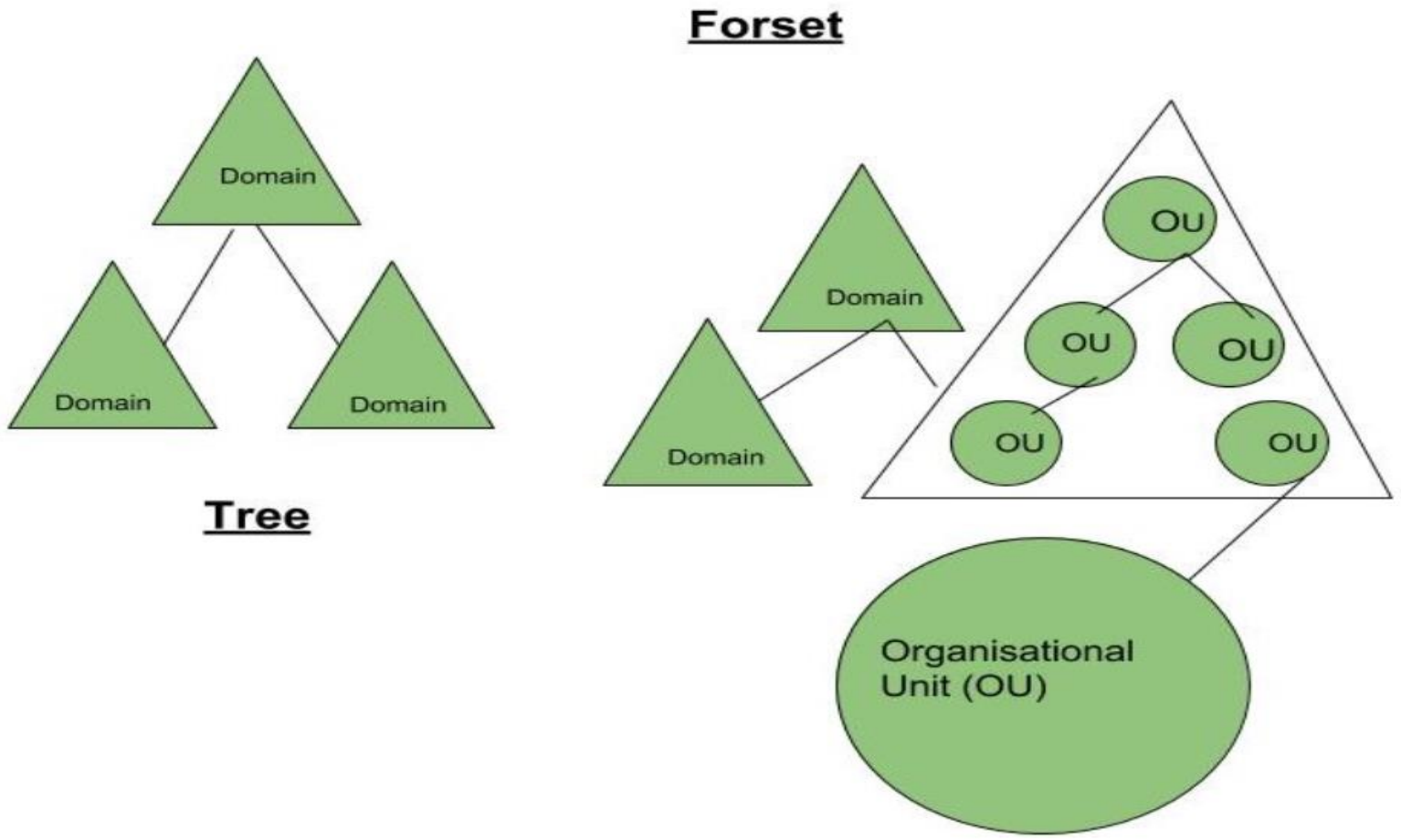
Trust Relationship – A trust relationship is an association between two domains that enables users in one domain to access resources in the other domain. Trust relationships can be one-way or two-way, and can be transitive or non-transitive.

Replication – Replication is the process by which changes made to the Active Directory database on one domain controller are synchronized with the database on other domain controllers. Replication ensures that all domain controllers have the same information and helps to maintain consistency across the directory.

Kerberos – Kerberos is a network authentication protocol used by Active Directory to provide secure authentication for users and computers. Kerberos uses encryption to prevent unauthorized access to network resources and is integrated with Active Directory to provide a seamless authentication experience for users.

Group – A group is a collection of user accounts or computer accounts that can be used to assign permissions or apply policies to multiple objects at once. Groups can be used to simplify administration and improve security by reducing the number of individual permissions or policies that need to be assigned to each object.

Common Terminologies in Active Directory Concepts:



Active Directory Objects:

Container Objects – These objects can contain other objects inside them, and we can make collection from them. For Example- Forest, Tree, Domains, Organizational Units.

Leaf Objects – These objects can not contain other objects inside them. For Example- users, computers, printers, etc.

How is data organized in Active Directory?

- Data is stored in Active Directory **as objects** and organized by name and attributes.
- A group of objects that share the same Active Directory database is called a **domain.**
- One or more domains with a common schema and configuration constitute what is known as **a tree**.
- The top tier of Active Directory's logical structure is **a forest (*Root domain*)**, which is made up of a group of *trees*.
- A forest constitutes Active Directory's **security boundary**.

Active Directory as a target for attackers

- For attackers, Active Directory is the keeper of the crown jewels.
- When threat actors compromise a network, they typically try to elevate their privileges so they can move to more critical systems, access sensitive data, and gain a broader foothold in the environment to maintain persistence.
- As a result, attacking Active Directory and obtaining administrator-level access is one of the attackers' chief goals.

What tools are used by Active Directory attackers?

- Attacks are usually commenced by using tools such as BloodHound, which is an open-source application used for analyzing the security of Active Directory domains and revealing the potential for escalating access entitlements.
- Once the cyber attackers have uncovered hidden or complex attack paths that can potentially compromise the security of the network, they then use tools likes Mimikatz to steal the necessary credentials.

Active Directory Domains

Boundary of Authentication



Boundary of Policies

Boundary of Replication

The Domain in AD

After installing AD DS, you need to create a domain.

The domain **is the logical grouping of resources on the network.**

When you create a domain, you also create a domain name, which is used to identify the domain on the network.

Active Directory: The Domain

Domains represent logical partitions within Active Directory for security and directory replication.

Domains are unique names, like the domain names we're all used to seeing on the Web. "Microsoft.com" is an example of a domain name, and so is "Contoso.com." There is a one-to-one correspondence between Active Directory domains and DNS domains.

[BUILD 1]

Domains function as containers for Active Directory objects. Active Directory objects include users, servers, workstations, and network devices, such as printers.

Each domain stores information only about the objects it contains, and theoretically an Active Directory domain can contain up to 10 million objects. One million objects in an Active Directory domain is the supported limit.

Active Directory :The Domain

[BUILD2]

Because all Active Directory users log on to a domain, domains are boundaries of authentication.

Domain controllers are responsible for authenticating user and group passwords, and Active Directory provides single log-on security throughout the domain.

Domain-wide authentication means fewer lost passwords and fewer problems with configuring permissions.

[BUILD3]

Domains are also policy boundaries. Security policies that are defined in one domain are not extended to other domains. This means that settings, such as administrative rights, do not cross from one domain to another.

Active Directory :The Domain

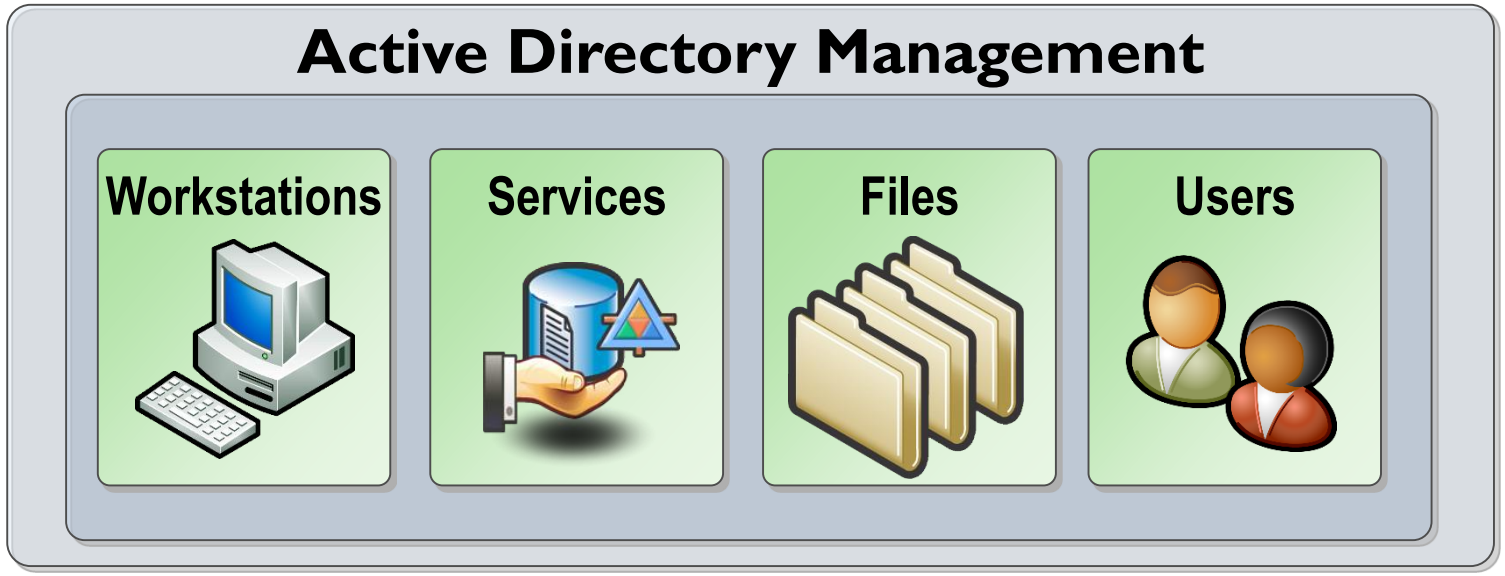
[BUILD4]

- Within a domain, information about objects is replicated between all domain controllers for additional security and redundancy.
- Important files within a domain may also be replicated to provide failover support without requiring expensive additional hardware. However, information is not replicated between domains.
- This means that domains are also boundaries for data replication.

In short, domains define the borders of an Active Directory system. Domains provide seamless network services for users within the domain, and offer good security against systems outside of the domain.

What Is a Directory Service?

A service that helps track and locate objects on a network



Directory Service

Active Directory provides several different services, which fall under the umbrella of "**Active Directory Domain Services**, " (AD DS). These services include:

Domain Services: Stores centralized data and manages communication between users and domains; includes login authentication and search functionality

Certificate Services: It generates, manages and shares certificates. A certificate uses encryption to enable a user to exchange information over the internet securely with a public key.

Directory Service

Lightweight Directory Services: Supports directory-enabled applications using the open (LDAP) protocol.

Directory Federation Services: Provides single-sign-on (SSO) to authenticate a user in multiple web applications in a single session.

Rights Management: It controls information rights and management. AD RMS encrypts content, such as email or Word documents, on a server to limit access.

Active Directory Installation

Demonstration for AD DS installation on Windows server 2016 as a VM in virtual box…

Domain Name System(DNS)

The DNS

The domain name system (DNS) is a naming database in which internet domain names are located and translated into Internet Protocol (IP) addresses. The domain name system maps the name people use to locate a website to the IP address that a computer uses to locate that website.

- DNS Role is one of the most important services in a network with Domain Controllers Environment.
- It helps us to resolve domain names internally and externally to IP and to have access to the requested service for the respective domain.

The DNS Server

Active Directory Domain Services (AD DS) uses Domain Name System (DNS) name resolution services to make it possible for clients to locate domain controllers and for the domain controllers that host the directory service to communicate with each other.

AD DS enables easy integration of the Active Directory namespace into an existing DNS namespace.

DNS ensures that servers, clients, and services can be found by their names.

*** Strictly speaking, DNS is not a component of Active Directory.

Dynamic Host Configuration Protocol (DHCP) Server

THE DHCP

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to dynamically assign an IP address to nay device, or node, on a network so they can communicate using IP (Internet Protocol).

- DHCP automates and centrally manages these configurations.
- There is no need to manually assign IP addresses to new devices.
- Therefore, there is no requirement for any user configuration to connect to a DHCP based network.
- DHCP can be implemented on local networks as well as large enterprise networks.
- DHCP is the default protocol used by the most routers and networking equipment.
- DHCP is also called RFC (Request for comments)

Function of DHCP

- DHCP manages the provision of all the nodes or devices added or dropped from the network.
- DHCP maintains the unique IP address of the host using a DHCP server.
- It sends a request to the DHCP server whenever a client/node/device, which is configured to work with DHCP, connects to a network. The server acknowledges by providing an IP address to the client/node/device.
- DHCP is also used to configure the proper subnet mask, default gateway and DNS server information on the node or device.

***There are many versions of DCHP are available for use in IPV4 (Internet Protocol Version 4) and IPV6 (Internet Protocol Version 6).

How DHCP works

DHCP runs at the application layer of the OSI model stack to dynamically assign IP addresses to DHCP clients/nodes and to allocate TCP/IP configuration information to the DHCP clients.

- Information includes subnet mask information, default gateway, IP addresses and domain name system addresses.

DHCP is based on client-server protocol in which servers manage a pool of unique IP addresses, as well as information about client configuration parameters, and assign addresses out of those address pools.

Components of DHCP

1. DHCP Server: The networked device running the DCHP service that holds IP addresses and related configuration information. This is typically a server or a router but could be anything that acts as a host.
2. DHCP client: DHCP client is the endpoint that receives configuration information from a DHCP server. This can be any device like computer, laptop, IoT endpoint or anything else that requires connectivity to the network.
3. IP address pool: IP address pool is the range of addresses that are available to DHCP clients.
4. Subnet: Subnet is the partitioned segments of the IP networks. Subnet is used to keep networks manageable.
5. Lease: Lease is the length of time for which a DHCP client holds the IP address information. When a lease expires, the client has to renew it.
6. DHCP relay: A host or router that listens for client messages being broadcast on that network and then forwards them to a configured server. The server then sends responses back to the relay agent that passes them along to the client.

Lease period in DHCP Server

The **lease time/period** is the amount of time before the DHCP **server** will reclaim an IP address , preventing IP address from permanent being retain by the host if the **lease** expires.

Lease period indicate how long a device is allowed to use that IP address.

How does Lease Period Work…

Now let's say you have set the lease time to 8 days (pretty long, but common in an enterprise network for wired devices).

After 4 days the network device will try to renew the lease. On day 5 it is able to contact the DHCP server and renew the current lease.

At that point, the DHCP Lease life cycle will start over, so the timers (T1 and T2) will reset and the lease is valid for another 8 days.

Assigning IP address in Client PC

Client Pc can be configured IP address statically or dynamically.

Static IP address:

- This is a fixed IP address that is manually assigned to a device and does not change over time.
- It is useful for devices that require a consistent address such as servers or Printers.

Dynamic IP address:

- It is an IP address that is automatically assigned to device by DHCP server.
- It can change over time , depending on the networking configuration. It can reduce security by frequently changing addresses,

Benefits and drawbacks of static IP address

Benefits:

- Provides consistency for devices that require a fixed ip ADDRESS.
- Can improve network performance and reduce traffic.
- Simplifies remote access to devices

Drawback:

- Can be more expensive to obtain and manage
- Can lead to security risk if address is not properly secured
- May not be necessary for devices that do not require a fixed ip address.

Benefits and drawbacks of Dynamic IP address

Benefits:

- Can reduce cost associated with obtaining and managing IP address
- Make it easier to connect to networks and internet
- Can improve network security by frequently by changing the IP address

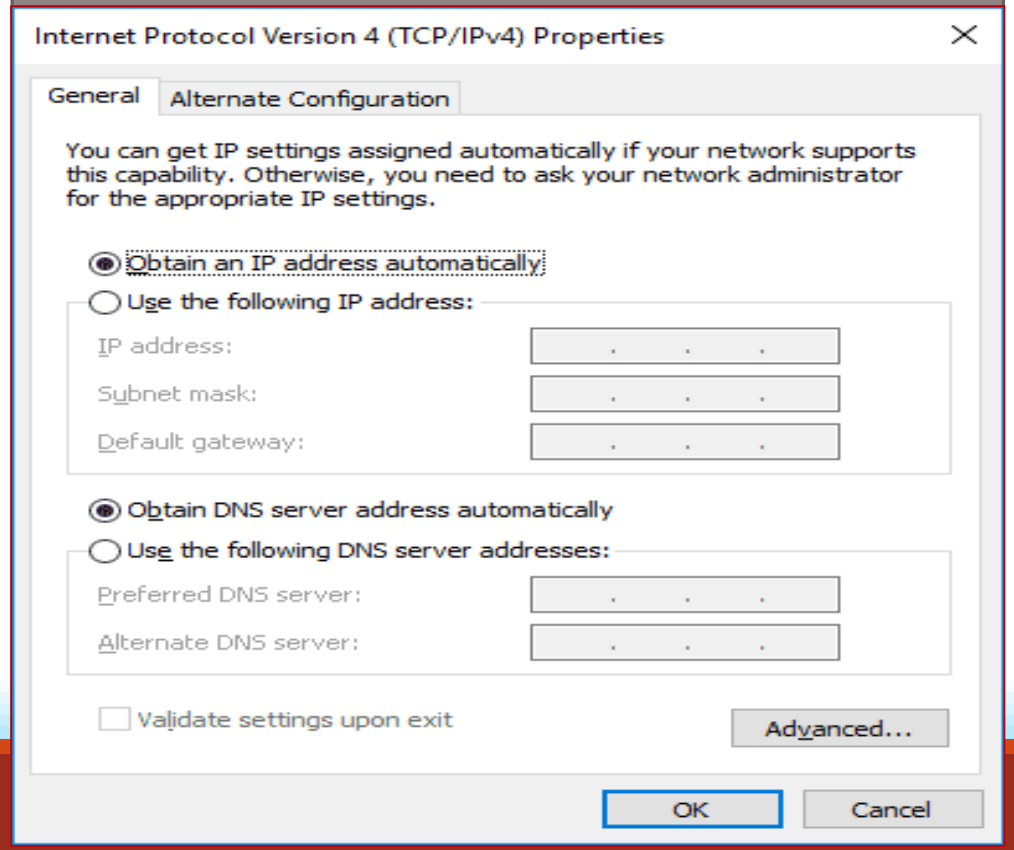
Drawback:

- Can cause issues on for devices that require a fixed address.
- Can lead to network congestion and slow performance
- Can make it more difficult to access devices remotely.

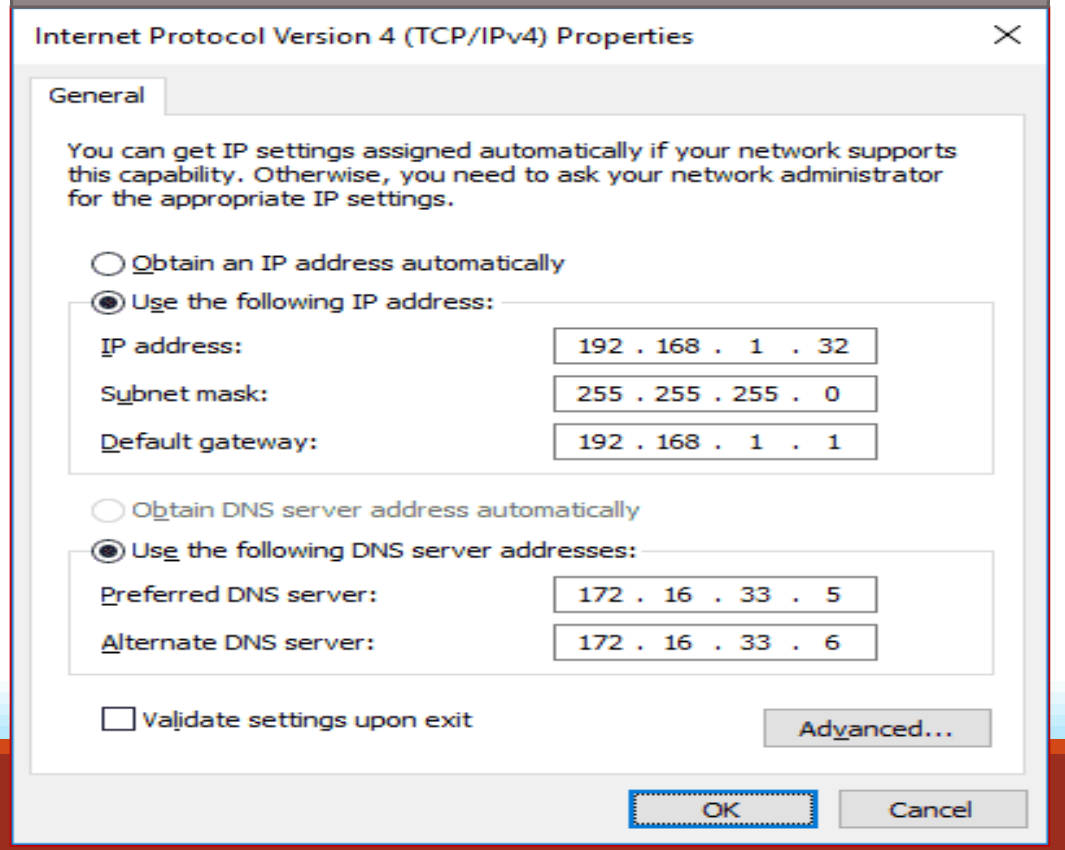
This is how IP address are assigned

In windows OS: Go to the network change adapter settings…

STATIC IP ADDRESS



DYNAMIC IP ADDRESS



Benefits of DHCP

- **Centralized administration of IP configuration:** DHCP IP configuration information can be stored in a single location and enables that administrator to centrally manage all IP address configuration information.
- **Dynamic host configuration:** DHCP automates the host configuration process and eliminates the need to manually configure individual host.
- **Seamless IP host configuration:** The use of DHCP ensures that DHCP clients get accurate and timely IP configuration IP configuration parameter such as IP address, subnet mask, default gateway and so on without user intervention.
- **Flexibility and scalability:** Using DHCP gives the administrator increased flexibility, allowing the administrator to move easily change IP configuration when the infrastructure changes.

Thank you!!

For listen