

Module II

IP addressing, Access Control and User Permission Settings

Syllabus

Domain and workgroup network architecture:-client server architecture -the Requirements of domain network-Domain controllers and Active directory.

Analyze IP addressing-IPV4 and IPV6:-Versions of IP addressing-Classes of IP address-Understanding subnet mask-Concept of DNS DHCP server -Working of DNS and DHCP-Installation requirements of DNS and DHCP.

Domain and workgroup users:-Managing user, group accounts-Adding group memberships-Physical and logical components of domain-Understanding child domain-additional domain controller-Trust relation.Securing files and folders:- setting share permission-setting security permission. RemoteManagement:- remote desktop connections-Remote Desktop Assistance. Operating system security overview:- windows firewall- Encryption techniques-IP security-system backup- active directory backup.

Domain and workgroup

Computers on a network can be part of a workgroup or a domain. The main difference between workgroups and domains is how resources on the network are managed.

In a workgroup:

- All computers are peers; no computer has control over another computer.
- Each computer has a set of user accounts. To use any computer in the workgroup, you must have an account on that computer.
- There are typically no more than ten to twenty computers.
- All computers must be on the same local network or subnet.

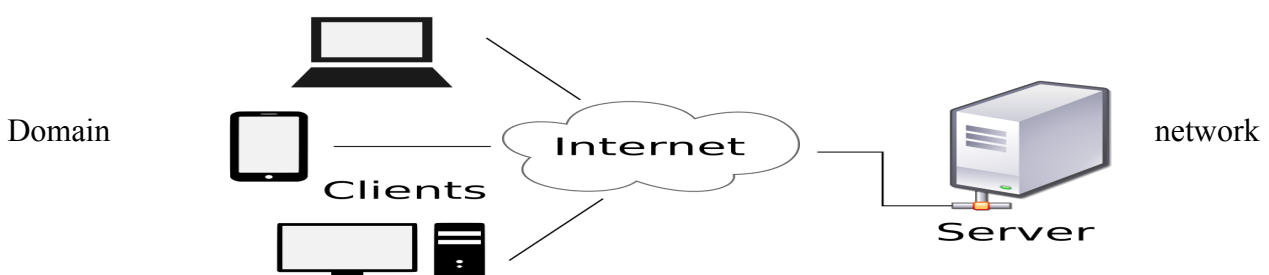
In a domain:

- One or more computers are servers. Network administrators use servers to control the security and permissions for all computers in the domain. This makes it easy to make changes because the changes are automatically made to all computers.
- If you have a user account on the domain, you can log on to any computer on the domain without needing an account on that computer.
- There can be hundreds or thousands of computers.
- The computers can be on different local networks.

Client server architecture

Client/server architecture is a producer/consumer computing architecture where the server acts as the producer and the client as a consumer. The server provides services such as application access, storage, file sharing or printer access. Client/server architecture works when the client computer sends a request to the server over the network connection, which is then processed and delivered to the client.

Example:- internet



Requirements of domain network

A domain network refers to any group of users, workstations, devices, printers, computers and database servers that share different types of data through network resources.

Requirements:-

- First, computer must belong to the domain
- To join the domain, the computer must have an account in the domain like a user account.
- Those credentials enable the computer to authenticate against the domain and to create a secure relationship that then enables users to log on to the system with domain accounts.

Domain Controller

A domain controller is a server that manages network security by providing user authentication and authorization.

Active Directory

Active Directory is the central database on a domain controller where the login credentials of all client computers, printers, and other shared resources in the network are stored. When someone tries to login, their login credentials must match those saved in Active Directory.

Internet Protocol

- An Internet Protocol address is also known as IP address.
- IP address acts as an identifier for a specific machine on a particular network.
- IPv4 was the first version of IP.
- The IPv4 uses a 32-bit address scheme allowing to store 2^{32} addresses.
- IPv6 is the most recent version of the Internet Protocol. It uses 128-bit address scheme.

| IPv4 | IPv6 |
|--|--|
| IPv4 addresses are 32 bit length. | IPv6 addresses are 128 bit length. |
| IPv4 addresses are binary numbers represented in decimals. | IPv6 addresses are binary numbers represented in hexadecimals. |
| IPSec support is only optional. | Inbuilt IPSec support. |
| Fragmentation is done by sender and forwarding routers. | Fragmentation is done only by sender. |
| No packet flow identification. | Packet flow identification is available within the IPv6 header using the Flow Label field. |
| Checksum field is available in IPv4 header | No checksum field in IPv6 header. |
| Options fields are available in IPv4 header. | No option fields, but IPv6 Extension headers are available. |
| Address Resolution Protocol (ARP) is available to map IPv4 addresses to MAC addresses. | Address Resolution Protocol (ARP) is replaced with a function of Neighbor Discovery Protocol (NDP). |
| Internet Group Management Protocol (IGMP) is used to manage multicast group membership. | IGMP is replaced with Multicast Listener Discovery (MLD) messages. |
| Broadcast messages are available. | Broadcast messages are not available. Instead a link-local scope "All nodes" multicast IPv6 address (FF02::1) is used for broadcast similar functionality. |
| Manual configuration (Static) of IPv4 addresses or DHCP (Dynamic configuration) is required to configure IPv4 addresses. | Auto-configuration of addresses is available. |

Classes of IP address

- IPv4 Addressing system is divided into five classes of IP Addresses.
- All the five classes are identified by the first octet of IP Address.
- The number of networks and the number of hosts per class can be derived by this formula –
number of networks = $2^{\text{network_bits}}$
number of hosts/network = $2^{\text{host_bits}} - 2$

Class A Address

The first bit of the first octet is always set to 0 (zero). Thus the first octet ranges from 1 – 127, i.e.

00000001 – 01111111
1 – 127

Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The IP range 127.x.x.x is reserved for loopback IP addresses.

The default subnet mask for Class A IP address is 255.0.0.0

Class B Address

An IP address which belongs to class B has the first two bits in the first octet set to 10, i.e.

10000000 – 10111111
128 – 191

Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x.

Class C Address

The first octet of Class C IP address has its first 3 bits set to 110, that is –

11000000 – 11011111
192 – 223

Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x.

Class D Address

Very first four bits of the first octet in Class D IP addresses are set to 1110, giving a range of –

11100000 – 11101111
224 – 239

Class D has IP addresses range from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting.

Class D does not have any subnet mask.

Class E Address

This IP Class is reserved for experimental purposes only for research and development or future use. IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254. Like Class D, this class is not equipped with any subnet mask.

Understanding subnet mask

Subnet mask is a mask used to determine what subnet an IP address belongs to. An IP address has two components, the network address and the host address. For example, consider the IP address 150.215.017.009. Assuming this is part of a Class B network, the first two numbers (150.215) represent the Class B network address, and the second two numbers (017.009) identify a particular host on this network.

Subnetting enables the network administrator to further divide the host part of the address into two or more subnets.

Example:-

The subnet mask is the network address plus the bits reserved for identifying the subnetwork -- by convention, the bits for the network address are all set to 1, though it would also work if the bits were set exactly as in the network address. In this case, therefore, the subnet mask would be 11111111.11111111.11110000.00000000. It's called a *mask* because it can be used to identify the subnet to which an IP address belongs by performing a bitwise AND operation on the mask and the IP address. The result is the subnetwork address:

| | | |
|----------------|-----------------|-------------------------------------|
| Subnet Mask | 255.255.240.000 | 11111111.11111111.11110000.00000000 |
| IP Address | 150.215.017.009 | 10010110.11010111.00010001.00001001 |
| Subnet Address | 150.215.016.000 | 10010110.11010111.00010000.00000000 |

The subnet address, therefore, is 150.215.016.000.

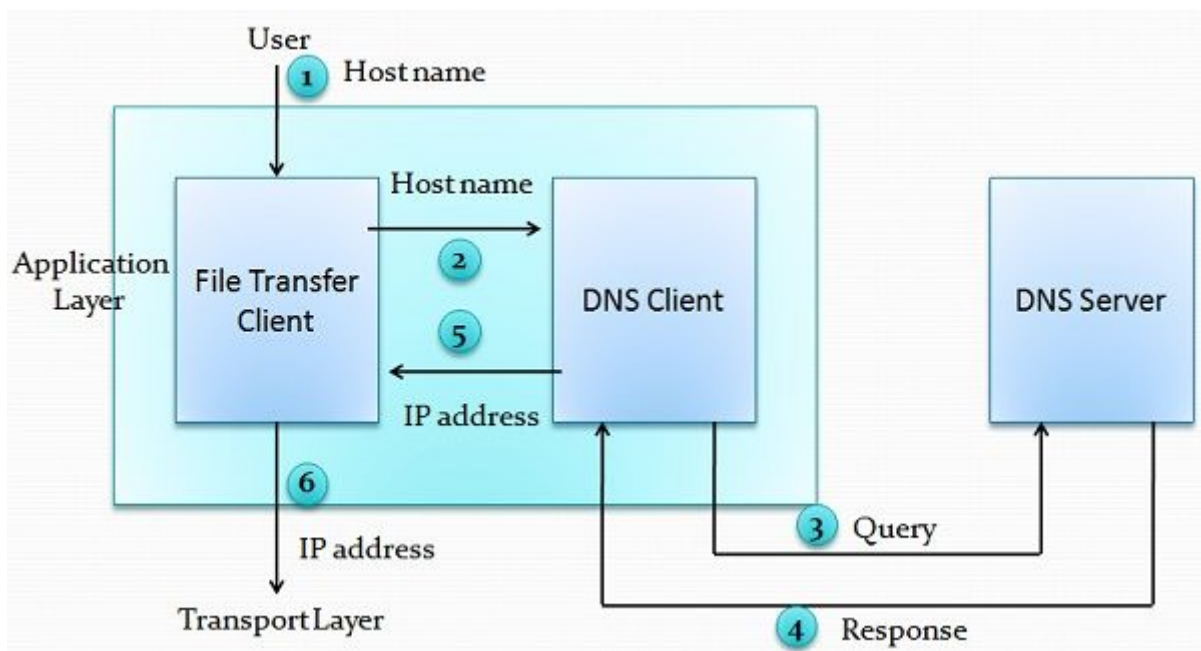
Concept of DNS Server

A DNS server is a computer server that contains a database of public IP addresses and their hostnames, and it translates to IP addresses as requested.

Example:- it translates human-friendly domain names, such as google.com into machine-readable IP addresses, such as 173.194.32.195

Working of DNS

When a user wants to use a file transfer client to access the file transfer server running on a remote host. To establish the connection the TCP/IP suite must need the IP address of the file transfer server. The given figure illustrates the working of the DNS step by step.



1. The hostname is passed to the file transfer client by the user.
2. The file transfer client transmits the hostname to the DNS client.
3. The DNS client sends the query to the DNS server which gives file transfer server name by utilizing known IP address of the DNS server.
4. DNS server sends the response with the IP address of the required file transfer server.
5. The DNS client passes the IP address to the file transfer server.
6. The received IP address is used by file transfer clients to access the file transfer server.

Concept of DHCP Server

- A DHCP Server is a network server that automatically provides and assigns IP addresses to client devices.
- It relies on the standard protocol known as Dynamic Host Configuration Protocol or DHCP.
- Without DHCP, the network administrator has to manually set up every client that joins the network.
- DHCP servers usually assign each client with a unique dynamic IP address.

DHCP supports three mechanisms for IP address allocation:

- Automatic allocation—DHCP assigns a permanent IP address to a client.
- Dynamic allocation—DHCP assigns an IP address to a client for a limited period of time, which is called a lease.
- Manual allocation—The network administrator assigns an IP address to a client.

Working of DHCP

- Following are the different messages that are used in DHCP process.

1. DHCPDISCOVER

- It is a DHCP message that marks the beginning of a DHCP interaction between client and server.
- This message is sent by a client which is connected to a local subnet.

2. DHCPOFFER

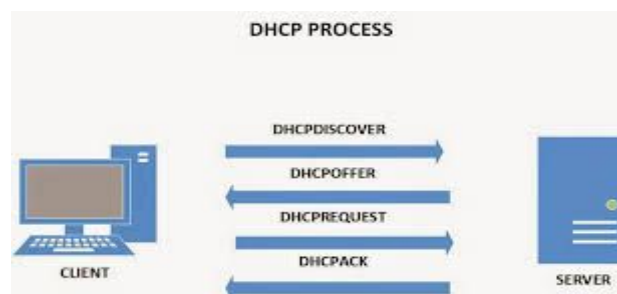
- It is a DHCP message that is sent in response to DHCPDISCOVER by a DHCP server to DHCP client.
- This message contains the network configuration settings for the client that sent the DHCPDISCOVER message.

3. DHCPREQUEST

- This DHCP message is sent in response to DHCPOFFER indicating that the client has accepted the network configuration sent in DHCPOFFER message from the server.

4. DHCPACK

- This message is sent by the DHCP server in response to DHCPREQUEST received from the client.
- This message marks the end of the process that started with DHCPDISCOVER.
- It is an acknowledgement by the DHCP server that authorizes the DHCP client to start using the network configuration.



Here are the steps :

- Step 1: When the client computer (or device) boots up or is connected to a network, a DHCPDISCOVER message is sent from the client to the server. As there is no network configuration information on the client so the message is sent with 0.0.0.0 as source address and 255.255.255.255 as destination address. The transport protocol used for this message is UDP and the port number used is 67. The client enters the initializing stage during this step.
- Step 2: When the DHCP server receives the DHCPDISCOVER request message then it replies with a DHCPOFFER message. As already explained, this message contains all the network configuration settings required by the client. For example, the address field of the message will contain the IP address to be assigned to the client. In this case also, UDP protocol is used at the transport layer with destination port as 68. The client enters selecting stage during this step.
- Step 3: The client forms a DHCPREQUEST message in reply to DHCPOFFER message and sends it to the server indicating it wants to accept the network configuration sent in the DHCPOFFER message. The DHCPREQUEST message will still contain the source address as 0.0.0.0 as the client is still not allowed to use the IP address passed to it through DHCPOFFER message. The client enters the requesting stage during this step.

- Step 4: Once the server receives DHCPREQUEST from the client, it sends the DHCPACK message indicating that now the client is allowed to use the IP address assigned to it. The client enters the bound state during this step.

Local users

In Windows, a local user is one whose username and encrypted password are stored on the computer itself. When you log in as a local user, the computer checks its own list of users and its own password file to see if you are allowed to log into the computer. The computer itself then applies all the permissions (e.g., "can use the CD-ROM", "can install programs") and restrictions (e.g., "cannot install programs") that are assigned to you for that computer.

Domain users

A domain user is one whose username and password are stored on a domain controller rather than the computer the user is logging into. When you log in as a domain user, the computer asks the domain controller what privileges are assigned to you. When the computer receives an appropriate response from the domain controller, it logs you in with the proper permissions and restrictions.

Active Directory

- Active Directory is a network structure that stores domain and network information about all computers and devices as well as user and device software settings.
- It resides on each domain controller in an organization and replicates itself between the domain controllers.
- Active Directory has both a logical and physical structure.
- The logical parts of Active Directory include forests, trees, domains, OUs and global catalogs.
- The physical elements of Active Directory are domain controllers and sites.

Each element of the **logical structure of Active Directory** is defined below:

Domain – It is a logical group of users and computers that share the characteristics of centralized security and administration. Domains in the same forest automatically have trust relationships configured.

Tree – Domain trees are collections of domains that are grouped together in hierarchical structures. When you add a domain to a tree, it becomes a child of the tree root domain. The domain to which a child domain is attached is called the parent domain.

Forest – A forest is the largest unit in Active Directory and is a collection of trees that share a common Schema, the definition of objects that can be created. In a forest all trees are connected by transitive two-way trust relationships, thus allowing users in any tree access to resources in another. By default the first domain created in a forest is referred to as the root domain.

Organizational Unit – An organizational unit (OU) is a container object that helps to organize objects for the purpose of administration or group policy application. An OU exists within a domain and can only contain objects from that domain. One popular use of OUs is to delegate administrative authority – this allows you to give a user a degree of administrative control over just the OU, and not the entire domain.

The **physical structure of Active Directory** helps to manage the communication between servers.

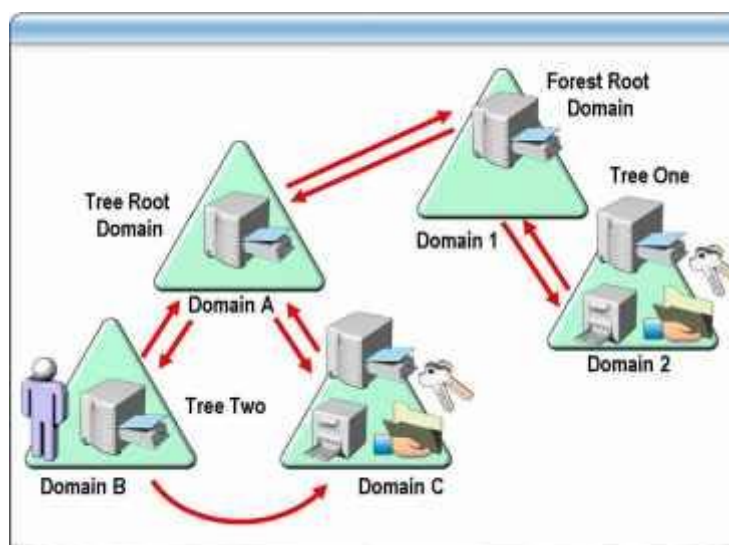
Each element of the **physical structure of Active Directory** is defined below:

Domain Controllers – Domain controllers are Windows 2000 Server-based systems that store the Active Directory database. Every Windows 2000 domain controller has a writable copy of the directory.

Site – In Active Directory, sites are groups of IP subnets that are connected at high speed. The purpose of defining sites in Active Directory is to control network traffic relating to directory synchronization, as well as to help ensure that users connect to local resources.

Trust Relationship

- A trust relationship is a logical link established between two domains.
- Between the two domains, one domain is called the trusting domain while the other is called the trusted domain.
- Trusts can be created automatically or manually.
- A trust relationship must be transitive and two-way trust.
- Transitive trust simply means that if Domain A trusts Domain B and Domain B trusts Domain C, then Domain A trusts Domain C.
- Two_way trust means if there is a trust relationship between domain A and domain B, then domain A trusts domain B and domain B trusts domain A.



Trusted Domain Object (TDO)

Each trust relationship in a domain is represented by an object known as the trusted domain object (TDO). The TDO stores information about the trust, such as the trust transitivity and trust type. Whenever you create a trust, a new TDO is created and stored in the System container in the trust's domain.

Trust Protocol

A domain controller authenticates users and applications using one of the two protocols:-

- **Kerberos V5 Protocol** - This protocol is the default protocol for computers in an active directory domain. Here, the client requests a ticket from a domain controller in its account

domain. The client uses this trusted ticket to the server in the trusting domain for authentication.

- **NTLM protocol** - NTLM is Windows new technology LAN manager. When a client tries to access resources on a server in another domain using NTLM authentication, the server that contains the resources must contact domain controller in the client account to verify the account credentials.

If any computer doesn't support the Kerberos V5 protocol, NTLM protocol is used.

Encryption Techniques

- Encryption is a security method in which information is encoded in such a way that only authorized users can read it.
 - ie, it is the process of converting plaintext to ciphertext.
 - Encryption requires the use of an encryption key: a set of mathematical values that both the sender and the recipient of an encrypted message know.
- (1) **AES** - The Advanced Encryption Standard, is a symmetric encryption algorithm and one of the most secure. This method uses a block cipher, which encrypts data one fixed-size block at a time, unlike other types of encryption, such as stream ciphers, which encrypt data bit by bit. AES is comprised of AES-128, AES-192 and AES-256.
 - (2) **Triple DES** - Triple Data Encryption Standard is a block cipher. It's similar to the older method of encryption, Data Encryption Standard, which uses 56-bit keys. However, 3DES is a symmetric-key encryption that uses three individual 56-bit keys. It encrypts data three times, meaning your 56-bit key becomes a 168-bit key.

Unfortunately, since it encrypts data three times, this method is much slower than others. Also, because 3DES uses shorter block lengths, it is easier to decrypt and leak data. However, many financial institutions and businesses in numerous other industries use this encryption method to keep information secure.

- (3) **Twofish** - It is a symmetric block cipher based on an earlier block cipher – Blowfish. Twofish has a block size of 128-bits to 256 bits, and it works well on smaller CPUs and hardware. Similar to AES, it implements rounds of encryption to turn plaintext into ciphertext. In addition, this method provides plenty of flexibility. You can choose for the key setup to be slow but the encryption process to be quick or vice versa.
- (4) **RSA** - This asymmetric algorithm is named after Rivest, Shamir and Adelman. It uses public-key cryptography to share data over an insecure network. According to Search Security, RSA is secure because it factors large integers that are the product of two large prime numbers. Additionally, the key size is large, which increases the security. Most RSA keys are 1024-bits and 2048-bits long.
- (5) **Honey Encryption** - It is a security tool that makes it difficult for an attacker who is carrying out a brute force attack to know if he has correctly guessed a password or encryption key. Typically, an attacker will know he's guessed wrong because the decrypted results will be unintelligible. If Honey Encryption has been used, however, the wrong guess will generate phony results that appear to be genuine. Because each incorrect guess generates a plausible result, it will be difficult for the attacker to know when he has guessed correctly.

Windows Firewall

Windows Firewall is a Microsoft Windows application that filters information coming to your system from the Internet and blocking potentially harmful programs. The software blocks most programs from communicating through the firewall. Users simply add a program to the list of allowed programs to allow it to communicate through the firewall. When using a public network, Windows Firewall can also secure the system by blocking all unsolicited attempts to connect to your computer. It was first included in Windows XP and Windows Server 2003.

Two types of firewall:-

- Software firewall - less expensive, used in home computers and laptops.
- Hardware firewall - provide higher level of security, used in servers.

The main **characteristics of the firewall** protection include the following:

- Different protection levels based on the location of the computer

When your PC connects to a network, the firewall applies a security level depending on the type of network. If you want to change the security level assigned initially, you can do this at any time through the firewall settings.

- Protection of wireless networks (Wi-Fi)

This blocks intrusion attempts launched through wireless networks (Wi-Fi). When an intruder attempts to access, a pop-up warning is displayed that allows you to immediately block the attack.

- Access to the network and the Internet

It specifies which programs installed on your computer can access the network or the Internet.

- Protection against intruders

It prevents hacker attacks that try to access your computer to carry out certain actions.

- Blocks

The firewall can block the access of the programs that you specify should not be able to access the local network or the Internet. It also blocks access from other computers that try to connect to programs installed on your computer.

Applications

- Reduces the risk of network security threats.
- Safeguards sensitive data and intellectual property
- Extends the value of existing investments.

Remote desktop connections



With Remote Desktop Connection, you can connect to a computer running Windows from another computer running Windows that's connected to the same network or to the Internet. For example, you can use all of your work computer's programs, files, and network resources from your home computer, and it's just like you're sitting in front of your computer at work.

To connect to a remote computer, that computer must be turned on, it must have a network connection, Remote Desktop must be enabled, you must have network access to the remote computer (this could be through the Internet), and you must have permission to connect. For

permission to connect, you must be on the list of users. Before you start a connection, it's a good idea to look up the name of the computer you're connecting to and to make sure Remote Desktop connections are allowed through its firewall.

If your user account doesn't require a password to sign in, you'll need to add a password before you're allowed to start a connection with a remote computer.

Steps to allow remote connections on the computer you want to connect to:-

1. Open System by clicking the Start button , right-clicking Computer, and then clicking Properties.
2. Click Remote settings.  If you're prompted for an administrator password or confirmation, type the password or provide confirmation. Under Remote Desktop, select one of the three options.
3. Click Select Users.

If you're an administrator on the computer, your current user account will automatically be added to the list of remote users and you can skip the next two steps.

4. In the Remote Desktop Users dialog box, click Add.
5. In the Select Users or Groups dialog box, do the following:
 1. To specify the search location, click Locations, and then select the location you want to search.
 2. In Enter the object names to select, type the name of the user that you want to add, and then click OK.
 3. The name will be displayed in the list of users in the Remote Desktop Users dialog box. Click OK, and then click OK again.



Remote Desktop Assistance

With Remote Desktop Connection, you can connect to a computer running Windows from another computer running Windows that's connected to the same network or to the Internet. For example, you can use all of your work computer's programs, files, and network resources from your home computer, and it's just like you're sitting in front of your computer at work.

To connect to a remote computer, that computer must be turned on, it must have a network connection, Remote Desktop must be enabled, you must have network access to the remote computer (this could be through the Internet), and you must have permission to connect. For permission to connect, you must be on the list of users. Before you start a connection, it's a good idea to look up the name of the computer you're connecting to and to make sure Remote Desktop connections are allowed through its firewall.

If your user account doesn't require a password to sign in, you'll need to add a password before you're allowed to start a connection with a remote computer.

Steps to allow remote connections on the computer you want to connect to:-

1. Open System by clicking the Start button , right-clicking Computer, and then clicking Properties.
2. Click Remote settings.  If you're prompted for an administrator password or confirmation, type the password or provide confirmation. Under Remote Desktop, select one of the three options.

3. Click Select Users.

If you're an administrator on the computer, your current user account will automatically be added to the list of remote users and you can skip the next two steps.

4. In the Remote Desktop Users dialog box, click Add.
5. In the Select Users or Groups dialog box, do the following:
 1. To specify the search location, click Locations, and then select the location you want to search.
 2. In Enter the object names to select, type the name of the user that you want to add, and then click OK.
 3. The name will be displayed in the list of users in the Remote Desktop Users dialog box. Click OK, and then click OK again.

System Backup

- A system backup is the process of backing up the operating system, files and system-specific data.
- Backup is a process in which the state, files and data of a computer system are duplicated to be used as a backup or data substitute when the primary system data is corrupted, deleted or lost.
- The system backup is performed through backup software and the end file (system backup) generated through this process is known as the system snapshot/image.

There are several ways to back up your PC. One of them is:-

1. Select the Start button, then select Control Panel > System and Maintenance > Backup and Restore.
2. Do one of the following:
 - If you've never used Windows Backup before, or recently upgraded your version of Windows, select Set up backup, and then follow the steps in the wizard.
 - If you've created a backup before, you can wait for your regularly scheduled backup to occur, or you can manually create a new backup by selecting Back up now.
 - If you've created a backup before, but want to make a new, full backup rather than updating the old one, select Create new, full backup, and then follow the steps in the wizard.

Active Directory Backup

Backing up Active Directory is important, since a crash of a domain controller causes all network information to be lost. Backup involves backing up the system state, which is all the system components that rely on each other. They have to be backed up and restored together for accurate results. There are different ways to backup Active Directory using Microsoft tools. The choice depends on the Windows operating system that is running on the domain controller.

1. Log on to the Domain Controller locally as an administrator or a backup operator.
2. Left-click on the start button. Navigate to Programs, Accessories, System Tools. Select "Backup." Click on the backup wizard button and choose "next."
3. Choose "backup selected files, drives, or network data."
4. Select "System State" on the screen that asks what items to back up.
5. Click the plus sign next to the drive letter that contains the system files to expand the selection. Select "system disk." Click "next."
6. Specify a folder or tape device to backup to in the "Where to Store the Backup" choice.
7. Name the file if using file backup, or select the tape to be used if using a tape in the "Backup Media or File Name" box.
8. Make sure the selection "Prompt to replace data" is included under the "How" category. If necessary, select the Advanced button and follow the prompts until reaching the Media Options screen. Choose "Replace the data on the media with this backup."
9. Follow the prompts to the "finish" screen. Choose "yes" to overwrite data.