Microsoft Certified IT Professional (MCITP)

Prepared By: Muhammad Zubair

Teacher: Mr. Tahir Qazi (tahir2k22@hotmail.com)

Location: Corvit Lahore (14-C-III, Gulberg III)

Starting Date: 20th September, 2010

MCITP course consists of 5 Exams:

Exam-1 Windows Seven Deployment Exam Code: (70-680)

Exam-2 Windows Server 2008 Network Infrastructure, Configuring
Exam Code: (70-642)

Exam-3 Windows Server 2008 Active Directory, Configuring
Exam Code: (70-640)

Exam-4 Windows Server 2008 Application Infrastructure, Configuring
Exam Code: (70-643)

Exam-5 Windows Server 2008, Enterprise Administrator
Exam Code: (70-647)

Book source: www.4shared.com/dir/kGiCbH-p/MCITP.html
Password: pakistan

Lecturer no-1

First module is related to Windows 7. In this course there are mainly two operating systems one is Windows 7 and second one is Windows 2008 Server R2. Windows 2008 Server R2 is the most recent release of Microsoft in the market at this time. On client side first Windows Vista were used but there were some issues in Windows Vista that is why Windows 7 is released in October 2009. It is a fact that new products in a market fulfill the requirements of industries better than old ones.

First lecture is about Windows 7 deployment but before going to this we will discuss another module called operating system fundamentals. Precisely you can say Windows 7 fundamentals.

Being a system administrator what the industry will expect from you or what is the work of a system administrator and which tools in the operating system you can use to run it properly in any environments?

The job of the system administrator is to ensure business continuity. Because of any company important thing is business. At the end of the day the important thing for a company is money making. For all these things the proper work of the information technology department is necessary. It means that a company needs the work of a system administrator or network administrator.

Some companies business is not IT oriented but their business process needs the work of IT department. For example Banks does not give IT services but for their processes to run properly they need IT department, because their data bases will run on a computer their account system is stored in a computer their billing system is on computer so if the computer will not work then their business will not continue.

Now it is the responsibility of a system administrator to find out those computers which are asset for a business means if those computers will not work or down time comes then business will not continue.

Down time means when the business is out of service. For example if computer stop working for an hour on which billing system or credit cards are available then billing system or credit card process will not work. Sometimes we see that ATM machine is out of service means it's the down time of that computer then you cannot make any transaction. Down time suffer the customers and the company will lose trust of customers. All these issue will handle a person called system administrator which is responsible for business continuity.

There are two approaches with a system administrator:

1. **Reactive Approach:** In Reactive Approach if problem occurs then they will take actions otherwise no preparation for that problem in advance. For example if light is gone then they will check the generators if fuel is not available then they bring fuel from the bazaar and then start it.
2. **Proactive Approach:** In proactive approach you must be mentally prepared for all problems and you must take appropriate solutions for those problems. For example in Corvit a person is already prepared to start the generators if the light is gone, means the admin officer has given this responsibility to a person if this problem occur then you will provide this solution, it is called Proactive Approach.

   In Proactive Approach the system administrator first identify the systems and then he makes a replica (means copy). One system will offer services while the other will be in standby mode. If a problem occurs in the running system then the standby computer will take over and will provide services. In this case the down time will be very less. In some businesses down time is less affordable and in some businesses down time is not affordable. A business in which down time is not affordable then system administrators make clusters or real time replica. Cost will increase by decreasing down time.

   Operating systems tools are mainly divided into two categories:

   1. **Diagnostic:** Diagnostic means problem indicator. It will not give solutions but will give an apparent way to solve this problem. For example thermometer only checks the temperature it does not give any medicine. The system administrator knowledge is checked when all the diagnostic steps gives no result.
   2. **Trouble Shooting**

      Trouble shooting is done through diagnostic tool. Device manager (devmgmt.msc) is a tool or control panel is a tool. Therefore diagnostic is that tool which indicates the problem and will not give any solution.

      Operating system mainly consists of two things. First one is **device drivers** and second one is **services**. If your device drivers is ok and also your services is running then it means that your operating system is working properly.

      But if the operating system is not working properly then you will check these two device drivers and services.

      First diagnostic tool is **msinfo32**. It gives information about system.

      Steps:

      - Type **msinfo32** in Windows 7 run window and press ok
      - Click on components

- Click on **problem devices** (if you check the message so it will be written that the devices are disabled. It does not know that how these devices will be enabled? if you right click here nothing will happen).
- Now click on **software environment**
- Click on **services** (it will give information about services which one is start and which is stop but you cannot start or stop any service from here)

It is a very good tool you can say it is a laboratory of a computer where all kinds of tests can be done. You can also check system summary by click on the system summary option. You can also check basic information of hardware by clicking on the hardware resources option. This tool tells you a big picture about the devices and also about the services.

Eventvwr is another tool which gives more detail about a problem. It also gives information about new problems like if new viruses are come. Events Viewer means events can show and events are simply messages. For example if you boot your system sometimes message display that certain services are failed to start. These messages are saved in a place called windows log files.

Steps:

- Type **eventvwr** in run window and press ok
- After executing this command you will see different log files like Application, security, system etc. but we are mainly concern with system. These logs are dependent on machine operating system. Security log can only be viewed by system administrator. If you open the logs you will see events. There are many categories of events but three are very important i.e. error, information and warning because they are related with trouble shooting. Information events only give simple information or reporting. It is stored in a log because sometimes informational events solve your problem. You have to remember event ids, especially of system logs. For example **7036** id tells that **service status change**. It will give information which one service is stop and which one is start, means when the status change of which service. Another event id **6008** which tells about **un expected shutdown**.
- If you want to start or stop the services then you will run another tool called **services.msc**

Another diagnostic tool is **perfmon.** It is used to monitor or test hardware's and software's.

Steps:

- Type **perfmon** in run window and press ok
- Click on the performance monitor (it will show cpu, memory utilization in graphs, reports etc. it can also show you that how much load a processor gain when you are working in some applications like word or notepad)

Lecture no-2

Windows 7 deployment

Installation pre-requisites or minimum hardware requirements of windows 7:

- Processor : 1 Giga hertz
- RAM: 1 GB
- Hard Disk (Free Space): 15 GB

As a professional you should not keep your system on these minimum requirements. Because you will install other applications also. 15 GB of free space on a hard disk is minimum requirement and 20 GB is recommended. This space is required on that partition on which you are installing windows 7.

Installation Types

There are two types of installation.

1. **Manual Installation:** In Manual Installation we will attend the installation process.
2. **Automatic Installation:** In Automatic Installation you will not attend the installation process fully.

The industry in which you will work as a system administrator can be of two types. On is vendor company and the other is customer company.

Vendor Company is that company which provides computers and their services to the customers, for example Dell.

Customer Company is that company which uses that compute for their business, for example banks.

Requirements of Customer Company does not change rapidly but the requirements of the Vendor Company changes very rapidly.

For example if there are 200 brand new machines are you are asked to install windows 7 on all. Then automatic installation is the best method to use because it is time saving you can install windows 7 only in one day.

But the question is how brand new systems will boot because there is no operating system on it, their hard disk in blank.

Second question when you normally install OS then you provide source of operating system that is inserting operating system CD in the CD ROM. Now for 200 machines will you need 200 operating system CD's? Of course no. let us assume that your installation process will perform from one location and it only requires one operating system CD and this location is called Distribution Server which distribute windows 7 to client computers.

You will perform Installation on distribution server by yourself; it is not automatic while installation on client computers will be performed by distribution server.

Pre-requisites of distribution server

On distribution server we require a service through which we install operating system on client computers and this service is called **windows deployment service** or WDS. This service were introduced in window server 2003 with the name RIS (Remote Installation Services).

Requirements of WDS

We need three services which are required or you can say that these are the pre-requisites of WDS.

1. ADS (Active Directory Services)
2. DNS (Domain Name System)
3. DHCP (Dynamic Host Configuration Protocol)
4. NTFS Partition on WDS Server.

Remember that every Microsoft operating system is running in one of the two environments i.e. **Workgroup** (decentralize management of resources) and **Domain** (centralize management of resources).

If you want to use Windows Deployment Services (WDS) then environment must be domain. You can make domain environment by installing Active Directory.

Technically you can use WDS for a single system also but Microsoft recommend that if you have 50 or more machines then use WDS otherwise do manual installation.

Client Machines Pre-requisites

- Bootable NIC (Inside bootable NIC there is chip called Boot Rom or PXE boot Rom. It means Pre Boot Execution Environment; if this chip is available then it is bootable NIC).

Now a day all desktop computers come with this support. If there is no PXE ROM on client computer then you cannot use WDS. When you boot client computer press F12 for boot menu and then select boot from network adapter.

Note: Bootable CD is one for which you don't need operating system to run while for non bootable CD to run you need an operating system.

Preparation of Distribution Server

First of all you will install Windows 2008 Server R2 on your computer. Then you will install network services (ADS, DNS, DHCP etc) from Server Manager in administrative tools. In windows 2008 server DNS, DHCP etc are called Roles.

- Click on Server Manager
- Click on Roles
- Click on Add Roles
- Click on Server Roles
- Select Active Directory Services, DHCP and DNS
- Click on confirmation
- Click on install

If you are using Windows 2008 Server R1 then the confirmation option will not be visible at that time when you don't disable DHCP IPv6 stateless mode.

Now we have to install WDS. It is not necessary that WDS, DHCP, ADS, DNS must be installed on the same systems. You can install WDS on one system and ADS, DHCP, DNS on other system but the domain must be the same. But you require NTFS partition on that machine on which WDS is install. The main advantage of using WDS is time saving.

Steps for installing WDS

- Click on Server Manager

- Click on Roles then Add Roles
- Select Windows Deployment Service (there are two components of WDS one is Transport Server and other is Deployment Sever. Transport Server is one which push operating system and Deployment Server stores the information therefore select both components)
- Click on install

Microsoft has developed a new file format which is .WIM (Windows Imaging Format) available in Windows 7 CD. The sole purpose of making this format is remote installation. There are two files with this format within the sources folder of windows 7 CD. One is boot.wim and other is install.wim. In this case boot.wim is that file which starts the machine and the actual windows is installing by install.wim.

Configuration of WDS

- Click on start then windows deployment services
- It will show a warning sign that server is not yet configured
- Right click on it and select configure server click next
- You will see c:\remote install (NTFS partition is required for this file. In case of RIS this folder is not allowed to store on C drive but now it will give only a warning but you can store it on C drive).
- Select drive for this folder and click next
- Now there are two options
    - **Do not listen on port 67** (note: we have installed two DHCP. one DHCP is installed when we select add Role and other DHCP is within the WDS which is installed with WDS. The DHCP within WDS is not complete; it gives partial support and work similar with normal DHCP. Every application has a port number on the internet. FTP has 21, HTTP has 80, DNS has 53 and DHCP has 67. Now there are two DHCP so which one will work. By selecting this option you are stopping WDS DHCP.
    - **Configure DHCP option 60 to PXEClient** (when you select this option it tells the client that after getting IP address also take an image from this computer. When DHCP and WDS are installed on one computer then make it a rule of thumb to select these two options)
- After clicking next there are three options
    - **Do not respond to any client computer** (It means that don't start WDS services right now. For example if you planned to start deployment on Monday but everything is ready on Friday then select this option not to start services yet for security reasons

because if you don't check this option and somebody plug in his LAPTOP then installation will start)

- **Respond only to known client computers** (it tells the server to respond or give image to only those computer which you know; now how the computer will be known to the server; one through his name which is not available at this time second IP address which is also not available at this time so there must be a mechanism through which server know computers before installation. There are UUID or GUID of each computer which will provide you by manufacturer or vendor and these IDs are written on the casing or you can see it in BIOS. UUID means Universally Unique Identifier and GUID stands for Globally Unique Identifier. It consists of 32 characters. This process in which you give UUID or GUID of client computers to the distribution server to become known to it is called pre staging.
- **Respond to all (known and unknown) client computers** (it means that respond to every one or give image to every that connect to the network)
  - **For unknown clients notify administrator and respond after approval** (it means that if you select this checkbox then distribution server will not reject installation on unknown computers but it will install OS when administrator allow it for installation. The unknown devices installation will be pending in a folder called pending devices in a hierarchy. In this folder when administrator right click on its GUID and select Approve then installation will start)

- Click next
- Now in the hierarchy there will be two folders one is boot image and another one is install image.
- Right click on boot image and select add boot image then browse for windows 7 CD and click on boot.wim file.
- Right click on install image folder then select add install image browse for windows 7 CD and click on install.wim file.
- After creating these two images now in DHCP you will give IP addresses that can be assigned to client computers during installation.
- Now boot your client computer and press F12 to go to boot menu and from this menu select boot from network adapter installation will start.

Note: if you want to create an image of the running environment in which along with operating system application software's (word, VB, Flash etc) will also be installed. Then for this you will use a tool IMAGEX. IMAGEX is a WIM creator and modifier (C:\IMAGEX/capture) you will get

IMAGEX in WAIK (Windows Automated Installation Kit) which can be downloaded from microsof.com but unfortunately genuine window check will be done.

All port numbers can be viewed in a file C:\windows\system32\drivers\etc\services

For Active Directory installation an active network connection is required. If you are working on a single computer without network then install a loop back adapter as:

- Go to device manager by writing the command in run (devmgmt.msc)
- X

How to Assign UUID or GUID to Distribution Server

- Click on Active Directory users and computers
- Right click on computer
- Select new computer
- Give any name to computer
- Click next then enter UUID or GUID in the text field

How to configure DHCP

- Click on DHCP in Administrative tools
- Right click on IPv4
- Select new scope
- Right Click on scope
- Select activate and give IP address range

How to start WDS Services

- Open WDS
- Right click and select All Tasks
- Click on new
- Click on start services

If you want to modify some options of WDS then open WDS right click on it and select properties.

Lecture no-3

Disk Management

There are two types of disks with reference to operating system.

1. Basic Disk
2. Dynamic Disk

In **Basic Disks** we made partitions while in **Dynamic disks** we made volumes.

There are two types of partitions on Basic Disk i.e. **primary partition** and **extended partition**.

We make primary partition because it starts our machine. Boot files are stored on primary partition. You can only mark primary partition as active by right clicking on that partition and you cannot make an extended partition as active.

There are total number of partitions are four. It means that maximum numbers of partitions are 4. You cannot make more than four partitions because of architectural limitations. If you want to make only primary partitions then only four drive letters will be display in the computer. But if you want to dedicate separate drives for marketing, finance, HR, IT, support, security, means for seven departments. Then you can make extended partition. Extended partition gives you the ability to make more than four drives (not partition)

Partition information is stored in a table called partition table. The size of partition table is 64 bytes. One partition description consumes 16 bytes. That is why 16 X 4 = 64. Therefore you can only make four partitions.

It is not necessary that only operating system can reside on a primary partition which is active. On active partition only boot sector on which boot configuration data is stored. You can install operating system on other logical drives also. BASIC Disk cannot give some advance or enterprise features. That features are **improved performance** and **fault tolerance** (ability of a system to continue work of one of the system component failure).

Dynamic disk were introduced in windows 2000. **Dynamic Disk** provides these two features one is improved performance and second one is fault tolerance. In dynamic disk volume information is stored in 1 MB data base. It is for larger than 64 bytes.

Open disk management by using diskmgmt.msc command from run window.

For hard disk or storage administration there are two tools. One is **Disk Management** and the other is **Diskpart command.**

Disk management is a graphical tool while diskpart is a command line tool for disk administration. Disk part gives advance administration of storage devices it is introduced in windows 2003.

Types of volumes in Dynamic Disk

1. Simple volume (require 1 dynamic disk)
2. Spanned volume (require 2 ~ 32 dynamic disks)
3. Striped volume (require 2 ~ 32 dynamic disks)
4. Mirror volume (require only 2 dynamic disks)
5. RAID-5 volume (require 3 ~ 32 dynamic disks)

You can convert BASIC Disk to DYNAMIC Disk without loss of data but all data will be lost when you convert Dynamic disk into Basic disk. Because you can accommodate 64 bytes in 1 MB. But you cannot store 1 MB data into 64 bytes.

By graphical tool you can make three primary partition and one extended partition in Basic Disk. If you want to deviate from this structure then you will use Diskpart tool.

Steps for making partition in Basic Disk

- Right click on disk
- Create new
- Give size of partition
- Assign drive letter
- Format drive and click finish
- In this case you can make three primary partition and one extended partition.

In order to run the OS or to make the hard disk usable you must make primary partition. It means that primary partition is necessary while extended is not necessary.

Steps for making volumes in Dynamic Disk

1. **Simple volume** is just like partition. Right click on the allocated space and select make new simple volume follow the steps and click finish.
2. **Spanned volume** requires at least two dynamic disks. Right click on the disk and select spanned volume. Add disks for spanned volume then select space first from one disk then select space from another disk for spanned volume. It will show this combined space with one drive letter. Spanned volume is the only volume that combines unequal spaces. It will neither give improved performance nor fault tolerance. It gives only the ability to use scattered space on different disks. If you remove one hard disk then the whole drive become un accessible.

3. **Stripe volume** gives improved performance in read and writes operation. Strip volume takes equal space from each disk. For example if you want to copy a file of 5 MB on stripe volume of two disks then first 64 KB will store on disk 1 and next 64 KB will be stored on disk 2 and so on until the whole file is copied. It means that 2.5 MB is stored on disk 1 and 2.5 MB is stored on disk 2. Both hard disks are independent of each other both hard disks head is used in reading and writing in a file that is why it will give fast read and write response.
4. **Mirror volume** gives fault tolerance feature and improved performance only in read operations. Mirror volume requires only two dynamic disks. One file will be copied in both hard disks that is why if one hard disk is failed the file is still available on other hard disk that is why it is called fault tolerance.

   Mirror volume uses 50% size for fault tolerance. When you right click on the dynamic disk and select new mirror volume. Then select both disk and give space for example 500 MB from one and 500 MB from other but it will show only 500 MB in the total volume because it use another 500 MB for fault tolerance. Both disks will have same drive letter for mirror volume.

   Mirror volume can be made by two ways. One method is to create mirror by simply click on one dynamic disk and select create mirror volume. Second method is right click on already created volume with data and select add to mirror. Either both disks will have unallocated space (for creating mirror) or one disk has unallocated space (add to mirror) for mirror volume.

   There is a difference between backup and fault tolerance. Fault tolerance is the failure of a component (hard disk) while backup is disaster recovery (flood, fire, earth quake).
5. **RAID-5 volume** is not possible in client version of operating system. Fault tolerance is a server side feature. You can only make RAID-5 volume in server version of operating system. It requires minimum 3 hard disks. For example we have 3 disks and we want to make RAID-5 volume. Let's take a space 600 MB from these 3 hard disks. It will internally divide each hard disk in three slices. In two slices it will keep data and on one slice it will store stripping information. Stripping information is used for data recovery. So on 3 hard disks total space is for RAID-5 volume is 1800 MB in which 1200 MB for data and 600 MB for stripping information. If one disk is failed its data can be recovered on the basis of stripping information but if two hard disks are failed then you cannot recover data. In RAID-5 wastage of space is very minimum as compared to others.

Diskpart Commands

Diskpart command is used for advance management of disks. In GPT (GUI based Partition Table) you can make 128 partitions.

Steps

- Type **cmd** in Run window
- Now type **Diskpart** in command line interface and press enter
- Diskpart> **list disk** (press enter. It will show all the available disks in the system)
- Diskpart> **list volume** (press enter. It will display all volumes on all disks)
- Diskpart> **select disk 2** (press enter. It will select hard disk 2 and now all operations will be performed on disk 2 in this case)
- Diskpart> **create volume simple size 500** (press enter. This command will create a simple volume on disk 2)
- Diskpart> **create volume stripe size 300 disk 0, 1** (press enter. This command will create a stripe volume from two disks 0 and 1 because minimum requirement for stripe volume is 2 and will take equal size of 300 from both disks.)
- Diskpart> **create volume mirror size 250 disk 0, 2** (press enter. It will create a mirror volume on two disks 0 and 2 because mirror volumes require only two disks for making volumes. It will take equal size from both disks)
- Diskpart> **sel vol 1** (press enter. It will select volume 1)
- Diskpart> **add disk 2** (press enter. It will perform add mirror method of creating mirror volume in which one is existing volume 1 and it will take un allocated space from disk 2)
- Diskpart> **create volume raid size 200 disk 0, 1, 2** (press enter. Raid-5 requires at least 3 hard disks. It will take 200 MB space from each drive for making raid volume but this command only works on server not on client)
- Diskpart> **select disk 1** (press ok. Desk 1 will be selected because for spanned volume first we take simple volume and then extend it to spanned volume. You cannot make spanned volume directly.)
- Diskpart> **detail disk** (press ok. It will display detail information about disk 1 because in first command we have selected disk 1)
- Diskpart> **select volume 2** (press ok. In this command we have selected volume 2 on disk 1 because it is a simple volume)
- Diskpart> **extend size 500 disk 0** (press ok. This command will create spanned volume from disk 1 and disk 0. Disk 1 is already selected and we extend it on disk 0.)
- Diskpart> **assign letter J** (press enter. It will assign drive letter J to the selected volume.)

- Diskpart> **detail volume** (press enter. This command will show information about select volume)
- Diskpart> **create partition primary size 500** (press enter. It will create primary partition of 500 MB on BASIC disk)
- Diskpart> **create partition extended size 400** (press enter. It will create extended partition on basic disk of size 400 MB.)
- Diskpart> **create partition logical size 200** (press enter. It will create a logical partition within extended space of size 200 MB)

Note: if drive letters is finished then instead of assigning letter you will use mount point as (Diskpart>assign mount c:\ folder name (enter)

Lectuer-4

Scripting: - Diskpart is basically used for scripting. Script is a file in which commands are written together and saved as a batch file with .bat extension.

Steps:

- Open a note pad file
- Write the following commands
- Select disk 1
- Create partition primary size 200
- Create partition extended size 300
- Create partition logical size 100
- Save this file test.bat in C drive
- Now first select C drive then write the following command
- C:\> Diskpart /s test.bat (press enter. It will create the above partitions on disk 1)

You can expand a partition by assigning more space from other drives unallocated space by using shrinking without loss of data.

Network setting:

To set properties of a network is called network setting. In windows 2008 there is a mandatory support of IPV6. Some of the utilities in windows 2008 use IPV6 like direct access and windows

meeting space. Default protocol of windows 2008 is IPV6. For example if you type c:\ping loopback (enter)

IPV4 is a 32 bit address and IPV6 is 128 bit address. IPV4 structure is represented in doted decimal format while IPV6 structure is represented in hexadecimal format. In IPV4 each octate is separated by dot (.) while in IPV6 each 16 bits block is separated by colon (:)

IPV4 address: 192.168.1.1

IPV6 address: 4:5: f: 5: c: 2:1:0

If in IPV6 contiguous 0's are present then it is represented by colon only. For example

F: 0:0:0:0:0:0:0:5 then you can write it as F::5

IPV6 is also called next generation address.

Network properties -> select IPV6 if you are using windows meeting space.

If multiple network connections are available then you can set priority. For this press ALT key on the keyboard menu will be displayed then click on advance option then click on advance setting and use arrow keys to move up the connection in the priority list.

You can view basic information about a network by selecting network properties you will see the following things.

IP Address: It is an IPV4 address of the computer.

Subnet Mask: It is used to find out network. In subnet mask all the network bits are 1 and host bits are 0.

Default gateway: it is the address of a router.

DNS Server: DNS convert name into IP address

Device Management: There are two categories of devices. One is called Plug and Play devices and the other is called Non Plug and Play devices. Type devmgmt.msc (Microsoft console) in run window to enter into device manager.

Plug and Play devices has the quality that there drivers are already installed in the operating system. If you run devmgmt.msc then a list of plug and play devices will be displayed. Right click on

each drive and select properties, then you can perform some operations like update driver, rollback or disable driver etc.

Non Plug and Play devices need drivers to be installed for working. These are not already installed you have to install them when you plug it. To view non plug and play devices click on the view option in the menu and then select show hidden devices. After this non plug and play devices will be displayed in the device manager. Click on any non plug and play device select properties then click on drivers and then click stop if you want to stop the device.

Remote Management

If you want to perform management of a system which is available in other country or at some remote location then you will use remote management. It is introduced in windows 2003.

RDP (Remote Desktop Protocol) is always running between systems after establishing a remote desktop session. This protocol uses a port number 3389/TCP.

First of all you will check connectivity of two systems by using ping command. Disable fire wall on target computer. For remote logging you will need to know IP address or name of the target computer. You will enable the option of allowing remote access option on the target computer. You can go to the remote setting by pressing windows key+ Pause break key then click on remote settings then check either second option or third option for allowing access.

Now type **mstsc (Microsoft terminal services client)** in the computer from where you want to establish remote session. After this you will give IP address or name of the target computer. Then click on **options** then click on **experienced tab** then select LAN (10 mega bits per second) then click on **advance tab** and select connect and don't warn me for fast logging then click on **connect** button. When you enter to the target computer it will be log off. If you want to remotely log on to server machine and the other user is also logged in then you will do this by clicking by **administrative tools** then select **remote desktop services** then click on **remote desktop session host configuration** then click **restrict each user to a single session** and select it **No**.

You can copy and paste files from remote computer to your computer because in windows 2008 clipboard is shared.

Lecture no-5

BranchCache: It is a new feature of Windows 2008 Server R2 that speeds up branch office access to files hosted on remote networks by using a local cache. This feature is not available in previous version of Windows 2008 Server R1 and in other operating systems like windows server 2003.

For example if a company have a central office in Karachi and branch office in Peshawar. Branch office users wants to access some data from central office, then a request is sent by one of the branch office computers to the central office server. The data is delivered to the branch office computer by central office. Now if another computer wants the same data from central office then he will not sent a request to the central office server instead the client checks the cache on the branch office LAN to determine whether the requested data is already cached.

If the data is cached already, a check is made to see if the data is up to date and whether the client has permission to access it.

If the data is not already cached, the data is retrieved from the server and placed in the cache on the branch office LAN. This technique is called BrachCache. But in BranchCache only internet data is stored.

BranchCache reduces traffic on WAN link and speeds up the response time. **BrachCache for network file** is another feature of BranchCache that stores non web related data i.e. only stores internal network files and folders.

BranchCache cover web data in branch office. In order to cache (store) central side data two **Cache Modes** are used in branch office:

1. **Distributed Cache Mode:** In distributed Cache Mode the central office data is stored only on client computers running windows 7 on the branch office network. When a client running Windows 7 retrieves content over the WAN, it places that content into its own cache. If another BranchCache client running Windows 7 attempts to access the same content, it is able to access that content directly from the first client rather than having to retrieve it over the WAN link. When it accesses the file from its peer, it also copies that file into its own cache. The **advantage of distributed cache mode i**s that you can deploy it without having to deploy a server running Windows Server 2008 R2 locally in each branch office.
2. **Hosted Cache Mode:** In hosted Cache Mode the central office data is only stored in the hard disk of a dedicated server in branch office. Hosted Cache mode uses a centralized local cache that hosted on a branch office server running Windows Server 2008 R2.When clients needs that data they will only request to the dedicated server instead of sending requests to the central office. The **advantage of Hosted Cache mode** over Distributed Cache mode is that the cache is centralized and always available. Hosted Cache mode requires a computer running Windows Server 2008 R2 be present and configured properly in each branch office. You must

configure each BranchCache client with the address of the BranchCache host server running Windows Server 2008 R2.

Depending on which BranchCache mode is used, that cache is either hosted on a server running Windows Server 2008 R2 or in a distributed manner among clients running Windows 7 on the branch office network.

The BranchCache feature is available only on computers running Windows 7 Enterprise and Ultimate editions. BranchCache can cache only data hosted on Windows Server 2008 R2 file and Web servers. You cannot use BranchCache to speed up access to data hosted on servers running Windows Server 2008 R1, Windows Server 2003, or Windows Server 2003 R2.

Steps for Branch Cache in Hosted Cache Mode at Branch office

- Go to Server Manager
- Click on Role then click on add Role (for installing file services and BranchCache for network files)
- Check File Services in the list and click next
- Select BranchCache for network files
- Click finish
- Now for installing BranchCache click on Features
- Click on Add Feature
- Select BranchCache and click on Install

Steps for enabling clients for BranchCache at branch office

In order to install BrachCache on client computers at branch office you have to modify group policy. In the domain environment there is default group policy. Therefore modify this policy and it will be automatically applied on client computers.

- Type **gpmc.msc** (this is a utility which is used to modify group policy) in run window and press enter
- After applying this command group policy management snap in will be displayed expand it.
- Click on domain then click on group policy objects
- Now right click on default domain policy and choose edit
- Click on computer configurations
- Click on Policies
- Click on Administrative Templates

- Click on network
- Click on BranchCache
- Now at the right hand side window five options will be displayed
- Right Click on **Turn on BranchCache** and choose edit
- Select the enable radio button to enable it
- Now right click on **set BranchCache distributed cache mode** and choose edit
- Select enable radio button to enable it
- Now right click on **set BranchCache hosted cache mode** and choose edit
- Select enable radio button to enable it
- For hosted mode you will enter FQDN (Fully Qualified Domain Name. To check FQDN right click on computer select properties and check the pc name then check domain name and combine both which is called FQDN)
- Right click **on Configure BranchCache for network files** and choose edit
- Click on the enable radio button. BranchCache becomes active when the round-trip latency to a compatible server exceeds 80 milliseconds.
- Right click on **Set Percentage Of Disk Space Used For Client Computer Cache** and choose edit
- Click on enable radio button the cache size defaults to 5% of the total disk space of the client computer

Firewall

For security of the system we normally use three tools. One is Anti Virus, second one is windows defender and third one is firewall.

Anti Virus is used to protect the system from viruses while **windows defender** protects the system from spyware (unwanted software) and **firewall** control access to your computer from outside.

Click on windows firewall in control panel and you can make it off or on in the settings.

Windows Firewall with Advanced Security

Create a rule in Advance settings:

You can create two types of rules in firewall. One is called Inbound Rule and the other is called Outbound Rule. The process for configuring inbound rules and outbound rules is essentially the same.

- Select Inbound rule and then click New Rule. This opens the New Inbound Rule Wizard.

- Now select the type of rule you want create. You can select between a program, port, predefined, or custom rule.
- You would create a custom rule if you wanted a rule that applied to a particular service rather than a program or port. You can also use a custom rule if you want to create a rule that involves both a specific program and a set of ports. For example, if you wanted to allow communication to a specific program on a certain port but not other ports, you would create a custom rule.
- If you decide to create a program rule, you then need to specify a program for which the rule applies. If you choose a port rule, you must choose whether the rule applies to the TCP or the UDP protocol. You must also specify port numbers.
- In the next step, you specify what action to take when the firewall encounters traffic that meets the rule conditions.
- **Allow the connection** allows the connection if the traffic meets the rule conditions.
- **Block the connection** blocks the connection if the traffic meets the rule conditions.
- Next set to All IP addresses and finish it

Lecture no-6

BitLocker:

BitLocker is a security feature that provides encryption of full volume (drive) data which is confidential to the company. Encryption prevents data from reading until decryption.

Before BitLocker EFS (Encryption File System) were used, this is a part of the NTFS. But EFS only provides file level encryption while BitLocker provides drive or volume level encryption.

Reasons of using BitLocker:

If a computer is stolen from the company which have confidential data related to the business of the company. It is very crucial if this data is reached into the hands of a competing organization.

Universal serial bus (USB) flash devices present a similar problem. People often use them to transfer important data from home to the workplace. Because these devices are small, they are easy to misplace. When one of these devices is lost, there is a chance that some sensitive data may find its way into the hands of a competing organization.

BitLocker handles these problems if you lost a computer your data will be un accessible to other persons if they want to retrieve it. It prevents an attacker from recovering data from a stolen computer.

Without the BitLocker encryption key, the data stored on the volume is inaccessible. BitLocker stores the encryption key for the volume in a separate safe location.

Steps:

- Click on BitLocker Drive Encryption in Control Panel
- Click Turn On BitLocker wizard will be started
- Now it will ask a method how to unlock the drive that is by using a password or Use Smart card or Automatically unlock the drive on this computer.
- Select any one of the above options and click next
- Now it will ask how do you want to store your recovery key. The following options will be available.
    - Save the recovery key to a USB Flash drive
    - Save the recovery key to a file
    - Print the recovery key
- Select any one of the above and click on save
- Click next
- Start encrypting

DirectAccess

DirectAccess is an automatic connectivity solution that allows clients running Windows 7 to connect seamlessly to the corporate intranet the moment they establish a connection to the global Internet. It is the feature of windows server 2008 R2 on server side and windows 7 on client side.

DirectAccess is an always-on, IPv6, IPsec VPN connection. If a properly configured computer is able to connect to the Internet, DirectAccess automatically connects that computer to a properly configured corporate network.

Difference between DirectAccess and Traditional VPN

- The connection process is automatic and does not require user intervention or logon. Traditionally, users must initiate VPN connections to the corporate intranet manually.

- DirectAccess is bidirectional; with servers on the intranet (Company) being able to interact with the client running Windows 7 in the same way that they would if the client was connected to the local area network (LAN). In many traditional VPN solutions, the client can access the intranet but servers on the intranet cannot initiate communication with the client.
- DirectAccess provides administrators with greater flexibility in controlling which intranet (Company Network) resources are available to remote users and computers.

The following four steps must be keep in mind while using DirectAccess

1. Identify client computers
2. Configure network interfaces
3. Identity infrastructure servers (DC, DNS)
4. Identify Application Servers

How to install DirectAccess

- Go to Server Manager and click on Features
- Click on Add Features
- Select DirectAccess Management Console in the list and click next
- After installation press close button

How to install CA (Certificate Authority)

- Go to Server Manager and click on Roles
- Click on Add Roles
- Select Active Directory Certificate Services from the list and click next
- Simply click next, next and then click on Install

How to Issue Certificate

- Type mmc command in the run window
- Click on File menu and select Add/Remove Snap-in
- Select certificate and click add button
- Select computer account and click next
- Click on Finish and then click oK
- Now open the console click on personal
- Click on certificate and at the right side right click and select All tasks
- Now click on Request new Certificate and click next
- Click next and select Domain Controller

- Finally click on Enroll

Now if you want to check whether the certificate is assigned or not. To check click on start button then select Certificate Authority and then click on certificate issued, now at the right side you will see the computer name.

Provide two consecutive Live Public IP's and multiple network Connection

- For DirectAccess company need to purchase two live public IP's from any ISP.
- Now install two network adapters because DirectAccess will not work on single network adapter. (for practice you can install loop back adapter. To install loopback adapter go to device manager by typing devmgmt.msc command in the run window. Now right click and select legacy hardware and click on network adapter click on next then select Microsoft and then select loopback adapter and install it)
- Now right click on one connection and assign one live public IP and then click on the advance button and give another live public IP. This connection will be used for internet.
- Now right click on the other connection and give static IP. This connection will be used for company own network.

Turn On Firewall

For DirectAccess you need to turn on the firewall in the computer. Click on control panel then select firewall and turn it on if not enabled.

How to Make Clients and Group

- Click on start button and select Active Directory Users and Computers
- Click on computer and at the right side right click and select new
- Give name to the compute and click next then finish
- Similarly add required number of computer
- Now right click and select new group
- Give name to the group and click ok
- Now right click on the group and select properties
- Click on members
- Click on Find Now and select the members from the list and add them

How to Configure DirectAccess

- Click on start button and select DirectAccess Management Console

- Click on setup
- In step 1 click on configure button
- Click on Advance button
- Click on Find Now button
- Select your group and click on Add
- Then in step 2 click on configure but you cannot go forward if you haven't two public IP's

Mobility Options (Offline File)

Offline Files is a feature relevant to portable computers that allows content that is stored on shared folders to be cached temporarily on mobile computers so that it can still be accessed and worked on when the mobile computer is no longer connected to the office environment. When the computer reconnects to the environment that hosts the shared folder, the offline content is synced, updating the content on servers and clients as necessary.

You can use the Offline Files feature to ensure access when a client computer is out of the office or when a temporary disruption, such as a wide area network (WAN) link failing between a branch office and a head office, blocks access to specially configured shared folders.

When a user makes a file available for offline access, Windows 7 stores a copy of that file within a local cache. When the file server that hosts the file is no longer available, such as when a user disconnects from the network, the user can continue to work with the file stored within the local cache. When the file server that hosts the file becomes available, Windows 7 synchronizes the copy of the file in the cache with the copy of the file hosted on the shared folder.

Steps:

- Open file properties
- Click on Advance button
- Click on Share file
- Click on Caching
- Select Offline settings
- There will be option for manual caching, automatic caching and no caching and also a check box for optimization performance.
- Select your appropriate option and click finish

Managing Windows Update Process

The Windows Update control panel is the primary tool you use to manage software updates on clients running Windows 7. Through this control panel, a user with Administrator privileges is able to check for updates, change update settings, review installed updates, and review hidden updates.

Steps:

- Click on windows updates in control panel
- Click on turn on windows updates which is recommended
- Now click on change settings the following options will be displayed
- **Install Updates Automatically (Recommended)** Windows Update installs updates automatically at the time specified. This is the default setting for Windows Update.
- **Download Updates But Let Me Choose Whether To Install** Them Updates are downloaded to the computer, and the user is notified that the updates are available for installation.
- **Check For Updates But Let Me Choose Whether To Download And Install Them** The user is notified that updates are available for download and install.

Lecture no-7

Monitoring and Optimization

It is a proactive approach to monitor the performance of your system and prepare a baseline to convince manager of your company for up gradation or replacing of components.

There are some terminologies associated with performance monitoring. They are:

Object: Major components of a system is called object. For example RAM, Hard Disk, Processor is objects. Objects can be hardware or software.

Counter: To check different aspects of the same object is called counter.

Instance: Multiple of the same object is called Instance.

Bottleneck: When the component is overloaded then it is called bottleneck.

Baseline: Average performance is called baseline. It convey average load.

There are two types of monitoring which are

1. **Real Time Monitoring: -** Real time monitoring means to monitor the system objects at the present moment. It is similar when you are watching a live match. Type **Perfmon** in the run window then click on + sign to open counters in the performance monitor. Click on processor and select % processor time click on add and then ok.
2. **Log Monitoring: -** Log Monitoring means to record or save the monitoring information. Type **perfmon** in the run window then click on the **Data collector sets** then click on **user defined** then **right click** and select **new** then select **Data Collector Se**t then **give name** then **create manually** click on **next** then click on **create data logs** select **performance counter** then click **next** then **add counter** click **ok** then **next** click **sample interval** then **next** and select **root**

directory and click **finish**. But the Log monitor will be stop until you start it by right clicking and select start.

Command line Monitoring

Second method to monitor the performance of a system is by using commands. First type cmd in the run window to enter in the command line interface.

C:\ **typeperf "\processor (_Total)\%processor time"** (press enter)

In the above command processor is an object, _total is an instance and %processor time is a counter.

C:**typeperf "\memory (_total)\pages/sec"** (press enter)

But when you enter this command it will give an error message because in case of memory there is no instance therefore doesn't use _total in memory object.

Now again run memory object with processor object in the following command

C:**typeperf "processor (_Total)\%processor time" \memory\page/sec"** (press enter)

You can also enter instance number of processor if there are multiple processor in your system instead of total. For example

C:**typeperf "processor (3)\%processor time"** (press enter)

Tip: you can convert results of a command to a file as **C:\IPConfig>test.log (enter)**

Commands for Log monitoring

C:\ **logman create counter test –c "\processor(1)\%processor time** (press enter)

The log file is by default in stop mode you will start it in command prompt as

C:**logman start test** (press enter)

C:**logman stop test** (press enter. If you want to stop it)

These log files will be stored in the root directory of logs files.

Backup and Restore

A System Image is a copy of all the files and folders on the system disk (and other specified hard disks) on a computer. You can use a System Image backup to restore the computer to exactly what its configuration was when the System Image backup was created.

Do not store your backups on a separate partition on a single hard drive on your computer. If you lose the hard drive due to hardware failure or after a virus attack, you also lose your backup.

In windows server 2003 **ntbackup** command were used to start a backup process but it has been discontinued now.

In windows server 2008 **wbadmin.msc** command is used to start a backup process. On server 2008 windows backup in not installed by default while in windows 2003 it is by default installed.

How to Install Backup in Server 2008

- Go to server manager and click on features
- Click on add feature
- Select windows server backup
- Click install

How to take Backup in Windows 7

Backup source and destination can't be same. You can select the following as backup destination.

- A second internal hard drive
- An external hard drive
- DVD-ROM
- USB flash drives
- Network location

Run the Backup wizard

- Open Control Panel, click backup and restore, and click setup backup
- Click next
- Select a destination volume, for example a second internal hard disk drive or a USB external hard disk drive.
- Click Next. On the Set Up Backup page, select Let Me Choose. Click Next.
- Click start backup

Lecture no-1

Exam-2 Windows Server 2008 Network Infrastructure, Configuring Exam Code: (70-642)

DHCP (Dynamic Host Configuration Protocol)

We can assign IP addresses to the computer by two ways. They are:

1. **Manual IP Configuration (Static IP)**
2. **Automatic IP Configuration (Dynamic IP)**

DHCP gives flexibility or ease of administration to the system administrator. In Manual IP configuration we will click on the properties of the network adapter and give IP address manually which is called Static IP address. If you have 5-10 computers then it is easy to manually assign IP addresses to them.

But if you have a large environment having 1000 of computers then it is quite difficult to assign IP addresses manually. There must be an easy way to perform this task and the easy way is to use DHCP server. In DHCP or Automatic IP Configuration the IP addresses are automatically assigned to the client computers which are called Dynamic IP address.

For the first time when a computer needs IP address from DHCP that has no IP address of DHCP nor does it have its own IP address then it broadcast DHCP Discover packet on the network.
These DHCP discover packet is reached to all the devices on the network. if the DHCP server lies in the broadcast domain of the client then it will accept the client request and assign IPv4 IP address to the client.
Communication between client and DHCP sever occurs in four steps which is also called **DORA** (Discovery, Offer, Request, Acknowledgment)

1. **Client Broadcast DHCP Discover Packet**
   In the first step the client computer send a message on the network to find out the DHCP server. This message is called DHCP Discover Message which is broadcasted by client computer. Client broadcast because when a client does not know IP address of DHCP server then the only way with the client to communicate and find out the DHCP server is to broadcast.

2. **DHCP Server Unicast DHCP Offer Packet to the client**
   In the second step when DHCP server receives the client DHCP Discover message then the DHCP server give reply and sends a message with terms and conditions and available IP address to the client which is called DHCP Offer.

3. **DHCP Client send a DHCP request message to the DHCP server**
   In the third step when the client computer receives Offer from DHCP server it accept the offer and send a request to the DHCP server to give me the IP address contained in the DHCP Offer message.

4. **DHCP Server sends a DHCP Ack message to the DHCP client**
   In step number four when DHCP server receives client request message. Then it checks the availability of the requested IP address in pool if it is still available then DHCP server sends an Ack (Acknowledgment) message to the client that you can use this IP address.

Note: Now a question arises that how the DHCP server knows that this packet is for me? The answer is that when a client sends a request to the DHCP server it sends also port number 68 which is used for DHCP request. One server side port 68 is used. Both are well known port numbers.

IP Lease: - Lease means for a specific amount of time. The default time for leasing IP addresses is 8 days but you can increase or decrease the lease time. Lease time means that after this time client will release the current IP address and will request for new IP address from DHCP server. If the DHCP server is online then it will again assign IP address to the client but if the DHCP server is not available then again it will wait for half time then wait for 87.5 % less time expires. After this if client did not find the DHCP server then it starts searching of another DHCP server on the network.

Benefit of Lease Duration: Because of lease duration client configuration will be updated automatically to reflect changes in network infrastructure.

Installation of DHCP Server

Pre Requisites of DHCP:

There are two pre requisites for DHCP installation.

1. Static IP address must be assigned to the computer
2. Server based operating system must be installed on the computer

If your computer fulfills these two criteria then you can install DHCP server on your computer.

Steps of DHCP Installation

- Go to Server Manager and click on Roles
- Click on Add Roles
- Select DHCP Server from the list
- Click on confirmation button (if you are using R1 then disable stateless mode of DHCP. Because after that confirmation button will be visible)
- Click Install and then close

Steps of DHCP Configuration

- Click on start button go to administrative tools
- Click on DHCP services
- Right click on scope and select new scope
- Give name to the scope (you can give any name)
- Give range of IP addresses (you can define a pool of IP addresses here)
- Click on next
- Add exclusion and delay (if you want to exclude some IP addresses from the IP pool add them in the exclusion. Now DHCP will never assign these IP addresses to the clients. Subnet delay

in milliseconds means that DHCP server will assign IP addresses to client in random amount of time in order to avoid duplication of IPs)

- Click on next button
- Define time for the lease duration which is 8 days by default and client will send renew request after 50% time of the lease. Means in case of 8 days client will send renew request after 4 days.
- Click on next and then finish

Activate Scope

By default the scope is disable you have to activate it because without activation DHCP will be unable to assign IP addresses to the clients.

- Right click on the scope
- Select activate
- If you want to check whether DHCP server has assigned IP address or not click on the leases folder.

Reservations

If you want to assign the same IP address to the client every time when he requests for renewal then you will define reservations.

- Select client reservations
- Right click and select new reservation
- Give name
- Assign IP and MAC addresses.

If you want to release the IP address by force from the client then give the following command in command prompt:

Ipconfig /release

If you want to renew IP address of a client use the following command

Ipconfig /renew

To show all details of the computer on the network then use the command

Ipconfig /all

DHCP Options

DHCP options provide clients with additional configuration parameters. More than 60 DHCP standard options are available but most common are:

- 003 → default gateway → address of the router
- 006 → DNS address
- 015 → DNS suffix (Corvit.com)
- 044 → Wins address (for name resolution, NetBios name resolution)
- 046 → Node types

Steps of setting options

➔ Right click on scope
➔ Configure option
➔ 003 router
➔ 006 DNS Server
➔ Add addresses for both
➔ DNS Name → Corvit.com
➔ 044 wins server
➔ 0x8

DHCP Database

DHCP database is stored in windows → system32 → dhcp → dhcp.mdb

In every database log files is must stored with it. There are two advantages of log file. One it improve performance and the second one is the recovery. The log file is **j50.log.** DHCP stores information first in log files then transfer it to the database.

J50.chk: It is a check point file in which the DHCP checks the file that how many is transferred and how many remains from log file to the database.

.JRS: It is a reserved log file. If the log file is full then it uses the reserved file for saving information.

Backup and Restore of DHCP

It is very easy in 2008 server. You can only write the following command

C: netsh dhcp server backup dhcpbackup (press enter)

In system32 this back up is stored with the name of dhcpbackup file.

If something is happen to the dhcp then you can restore the backup file of dhcp. You can restore the dhcp backup by the following command

C: netsh dhcp server restore dhcpbackup (press enter)

After restoring the dhcp backup you have to stop the dhcp and again start the dhcp in order to function properly as:

C: net stop dhcpserver (press enter)

C: net start dhcpserver (press enter)

When a computer wants to communicate with dhcp then he broadcast. But if there is router inside the client and dhcp server. Then as we know that router does not allow broadcast then what should be done. There are two solutions for this one RFC-1542 Compliant Router but there is no router. The second method is to implement **Dhcp Relay Agent**. It converts the client broadcast into a unicast so that it can pass from router to reach to the dhcp server.

If you want to check which IP is assigned to which computer then you can check it from **audit log** which is placed in the dhcp folder in system32.

APIPA (Automatic Private IP Address): if there is a network in which 5 or 7 computers and you select obtains IP automatically. But there is no dhcp server then these computers assign APIPA addresses and broadcast to each other. The APIPA address is 169.254.x.y.
To check the IP address before assigning is called conflict detection.

MAC Filtering: It is the feature of server 2008 R2 in which you can filter the computers by MAC address. If that computer is comes in the allow list then dhcp will assign IP address otherwise dhcp will not assign any IP address to this computer. If you want to stop a compute from being assigning an IP address then add the MAC address in the deny list of filtering.
Steps:

- Click on Filtering. There are two options one is Allow and the other is Deny
- Right click on Allow and select new filter
- Give MAC address of the computer you want to allow and also give description
- Press ok
- Now right click on the Deny and select new filter
- Give MAC address of the computer you want to deny
- Click ok

Super Scope: - if your DHCP IP pool is finished then you can create another pool and combine them with the help of super scope.

Lecture no-2

Domain Name System:
Domain Name System is used for name translation into IP address or you can say that it is used for name resolution.
Active Directory cannot work without DNS. DNS convert name of the computer into IP address. DNS works in a hierarchy. DNS use FQDN (Fully Qualified Domain Name). DNS only tells the IP to others.
When we want to communicate with a computer we give name rather than IP address because it is difficult to remember IP address as compared to names. For example www.yahoo.com
This name is only for the benefit of the human. It is translated into an IP address to reach the destination. The translation process of a name is called Name Resolution.
Name resolution starts from right to left. There is another "." After com but it is hidden. This **dot** is called **root level domain**. When a request is sent to the root domain for translation it forwards this request to **com** domain which is called **top level domain**. Com passes the request to yahoo domain which is called **2nd level domain**. Yahoo then sends the request to **www** which is called **host name**.
Structure of the DNS is distributed over the internet. It means that the name resolution task is not assigned to only computer rather it is distributed over the internet.
DNS Queries
There are two types of queries in DNS:

1. **Recursive Query: -** It goes from DNS client to DNS server. Its answer is complete means processing is complete.
2. **Iterative Query:** - It goes from DNS server to DNS server. Its answer is not complete means its reply is referral. Iterative query is used to reach from one DNS to another DNS. It keeps the reply for 60 minutes in his cache

How to Install DNS

- Click on server manager
- Click on Roles
- Click on Add Role
- Select DNS Server from the list
- Click on Install

Zone

Database of DNS is called Zone. Or partition of Domain Name Space represented by Domain Name is called Zone.

When you click on Zone then you will see two zones one is Forward Lookup Zone and Reverse Lookup Zone.

Forward Lookup Zone sends name and get IP address of the computer.

While **Reverse Lookup Zone** sends IP address and get name of the computer. Now the question arises that if we know IP address of the computer then why we need name of the computer. The answer is that if firewall is installed on the computer then firewall stop or allow traffic on the basis of name that is why reverse lookup zone is used to convert IP address in the name.

Steps to create a zone:

- Select Forward Lookup Zone
- Right click on it and select new zone
- Give name to the zone
- Now right click on the newly created zone
- Create a new host
- Give name to the host
- Give IP address to the host

Resource Records

Resource records are the DNS database entries to answer DNS client queries.

Name, type and data. The client query is always shown under the name title; DNS server answer always shown under the data title, in type different types of records is shown. Common records in DNS are A (Name to IP), PTR (reverse of A), SRV, MX, MS, SOA etc.

Zone Types

There are four types of Zone they are:

1. **Primary DNS Zone:** It is a standard zone which is writeable.

Steps to create Primary Zone:

- Right click on the Forward Lookup zone

- Select to create a new zone
- Select Primary Zone from the list. Uncheck the checkbox below because then it will go to the active directory integrated DNS zone.

2. **Secondary DNS Zone:** It is also a standard zone which is read only. For secondary zone it is necessary that you allow zone transfer in primary zone. Right click on zone select zone transfer tab and check zone transfer check box. Because all the entries of the primary zone will be copied to the secondary zone and if the primary zone go down then secondary zone can be acted as primary zone.

Steps to create Secondary Zone:

- Create a zone
- Select its type secondary
- Now give IP address of the master DNS server
- Give IP address and click on next
- Configure notification automatically
- Give IP of primary DNS

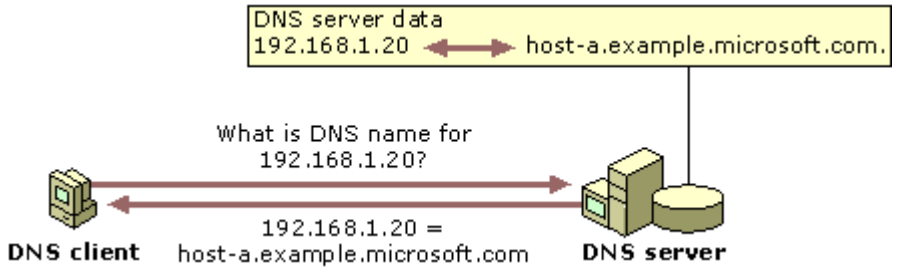
3. **Active Directory Integrated DNS Zone:** It is also a writeable zone. To make Active Directory Integrated zone the machine must be a Domain Controller. RODC (read only domain controller) feature is only available in server 2008 R2. The domain controller must be writeable not read only because it is more secure. There is a security tab in the AD integrated zone. It is a multi master structured. In case of AD integrated zone, DNS database will be replicated as a part of domain replication.
4. **Stub Zone:** It is by nature secondary. It has no database of its own. Its loads the database from master DNS. It only takes selective records not the complete database. Three records NS, SOA and Glue A will transfer into stub zone. Stub is read only.

DNS uses port 53 for communication and it uses both TCP and UDP protocols.
Dynamic DNS (DDNS) is used to automatically update IP addresses in DNS when changed by DHCP. You will enable DDNS option in the Zone properties to secure only.

Lecture no-3

Reverse Lookup Zone:

Domain Name System (DNS) servers can enable clients to determine the DNS name of a host based on the host's IP address by providing a special zone called a reverse lookup zone. A reverse lookup zone contains pointer (PTR) resource records that map IP addresses to the host name. Some applications, such as secure Web applications, rely on reverse lookups.
A reverse lookup takes the form of a question, such as "Can you tell me the DNS name of the computer that uses the IP address 192.168.1.20?"
A special domain, the in-addr.arpa domain, was defined in the DNS standards and reserved in the Internet DNS namespace to provide a practical and reliable way to perform reverse queries. In reverse lookup zone the IP address is written in reverse order.



Dynamic Updates in DNS:

With Windows Server 2008, a DHCP server can enable dynamic updates in the DNS namespace for any one of its clients that support these updates.

If the clients are belong to the pre-2000 family of computers then they are unaware of the dynamic updates therefore DHCP can do this work.

You have to enable this option in the DHCP properties. Then click on DNS tab in the DHCP properties and mark the checkbox of dynamic update DNS.

NSLOOKUP:

Displays information that you can use to diagnose Domain Name System (DNS) infrastructure. There are two mode of Nslookup they are

Interactive and noninteractive.

Noninteractive mode is useful when only a single piece of data needs to be returned. The syntax for noninteractive mode is:

C: nslookup pc1.corvit.com (press enter)

Interactive mode provides detail information about a DNS in order to diagnose, the syntax is:

C: nslookup (press enter)

>pc1.corvit.com (press enter)

>set type=ns (press enter)

>set type=soa (press enter)

>quit (press enter)

You can run Nslookup tool on DNS client.

Record Types: MX record type is responsible for resolving mail server name. In MX we give domain name as input and MX resolve that into mail server.

CNAME record type resolves name into name. This helps when running multiple services (like an FTP and a web server; each running on different ports) from a single IP address. Each service can then have its own entry in DNS (like ftp.example.com. and www.example.com.)

ftp.example.com. CNAME www.example.com.

www.example.com. A 192.0.2.23

When an A record lookup for ftp.example.com is done, the resolver will see a CNAME record and restart the checking at www.example.com and will then return 192.0.2.23.

WINS (Windows Internet Name Service)

It is used for Name resolution like DNS. But DNS is only concerned with FQDN (Fully Qualified Domain Name: pc1.corvit.com) while WINS concern with flat records such us pc1, mcitp or Corvit etc. it was used for NetBIOS for backward compatibility.

How to Install WINS:

- Click on server manager
- Click on features
- Click on add feature
- Select WINS Server from the list
- Click on next
- Click on install
- Click on close

NetBIOS Name: - NetBIOS is an acronym for Network Basic Input / Output System. It provides services related to the session layer of the OSI model allowing applications on separate computers to communicate over a local area network. It is a 16 characters name in which 15 characters are user defined and 16th character is service specific.

On the client computers right click on the adapter select properties then click on advance and select wins tab, now give IP address of wins server and press ok.

Now open wins server click active registration and then display registration.

Wins server is needed in two cases:

1. When clients belongs to pre-2000 family of operating system
2. When client running NetBIOS application.

Security

Security is the degree of protection against danger, damage, loss, and criminal activity. There are a number of security concerns which are

1. **Authentication:** It means to verify a person. There are three strategies used for authentication. i.e. who the person know (username and password), who the person has (ATM card etc), who the person is (Eye Scan or Thumb scan). Authentication guarantees that data was not altered during transmission. Example of authentication is Kerberos.
2. **Confidentiality:** confidentiality is the principle that an institution or individual should not reveal information to a third party. Example of confidentiality is BitLocker.
3. **Integrity:** Integrity means when you cannot change the contents. MD5 is the example of integrity.
4. **Anti Replay:** Anti-replay is the concept of not allowing an intercepted packet message to be sent to the recipient multiple times without the original sender knowing. IPSec uses sequential counters to guarantee that packets are received and processed in order.
5. **Non Repudiation:** Non-repudiation is the concept of ensuring that a party in a dispute cannot repudiate, or refute the validity of a statement or contract.

IPSec (IP Security)

Internet Protocol security (IPsec) is a framework of open standards for protecting communications over Internet Protocol (IP) networks through the use of cryptographic security services. IPsec supports network-level peer authentication, data origin authentication (uses Kerberos, shared key and CA), data integrity (MD5, SHA-1), data confidentiality (encryption: DES, 3DES), and replay protection.

It adds new headers with TCP/IP packet.

There are two sub protocols of IPSec. They are

1. **Authentication Header (AH)**
   Authentication Header (AH) provides authentication, integrity, and anti-replay for the entire packet (both the IP header and the data payload carried in the packet). It does not provide confidentiality, which means it does not encrypt the data. The data is readable, but protected from modification.
2. **Encapsulation Security Payload (ESP)**
   The main job of ESP is to provide the privacy we seek for IP datagrams by encrypting them. An encryption algorithm combines the data in the datagram with a key to transform it into an encrypted form. This is then repackaged using a special format, and transmitted to the destination, which decrypts it using the same algorithm.

Lecture no-4

ISAKMP (Internet Security Association Key Management Protocol)

It is a protocol for establishing security associations (SA) and encryption keys in an internet environment. Diffie Hellman is used to generate keys in IPSec. The encryption keys are always changing.

There are two phases of ISAKMP

Phase 1/Main Mode: Main Mode is also called Phase 1 in which a secure negotiation established called (SA) between two computers. The ISAKMP SA is used to protect security negotiations.

Phase 2/Quick Mode: Quick mode is also called Phase 2 establishes a secure channel between two computers to protect data.

Steps

- Type mmc in run window and press enter
- Click on file select Add Remove Snap-in
- Click on IPSec policy management and click on add button
- Click on IP Security Monitor and click add button
- Now make a policy (there are rules inside policy then there are filters or conditions inside a rules)
- Right click on IP Security Policy
- Click on create IP Security

- Click next then give any name to the policy
- Click next and then finish
- Now right click on the newly created policy and select properties
- Click on rules then click on Add
- Click on next then select All network connections
- Click on next
- Now click on Add button to create filter
- Give any name to the filter
- Click on add then click on next
- Select a specific IP address
- Select my IP address in destination
- Click on protocol any and click on next
- Click on finish and click ok
- Select the newly created filter and click on filter action
- Click on add and give any name to the filter action
- Click on next and select negotiate security
- Click on next and select don't allow unsecured communication
- Click on next and select integrity and encryption
- Click on next and then click on finish
- Now click on security rule wizard
- Click on use the…..
- Click finish then click on ok
- Now right click and select assign

If you click on the IP security monitor
→Active policy
→Main mode
  ➔ Security association
→Quick mode
  ➔ Security association

Note: In **Transport mode** the communication peers and IPSec peers are computers while in **Tunnel mode** the communication peers are computers and the IPSec peers are routers.

Remote Access

There are two ways through which we can communicate in a network. One is internet and the other is PSTN (Public Switch Telephone Network).
PSTN is secure as compared to internet but it is more costly.
Routing and remote access is a utility in windows for remote access.

Installation of Routing and Remote Access on Server

- Click on Roles and select Add Roles
- Click on network policy and access services

- Click on next and select routing and remote access
- Click on confirmation and then click on install
- Now open it and right click and select configure and enable routing and remote access
- Click on next and then click on remote access
- Click on dial up then select from a specified range
- Click on next and select new
- Give a range and click on ok
- Click on next then select no
- Click on next and then finish
- Now you will add a modem in server 2008
- Right click on ports and select properties
- Select modem then click on configure
- Click on remote access and select ok then click on apply

Allow users

- Go to the Active Directory Services
- Click on user properties and select Dial in
- Click on allow access and click on apply then ok

Create a new connection on network

- Click on create new connection
- Click on connect to the workplace
- Give telephone number
- Give user name and password
- Click connect

Call back

- Go to the Active Directory Services
- Click on user properties
- Select dial in
- Click on callback option
- Select set by caller
- Click on apply then ok

Callback security

- Go to the Active Directory Services
- Click on user properties
- Select dial in
- Select always call back to
- Give your telephone number
- Click on apply and then ok

Assigning IPs through DHCP

- Open routing and remote access

- Right click and select properties
- Click on IPv4 and select dynamic DHCP Relay agent
- Give IP address of DHCP server
- Now restart by right clicking and select all tasks
- Select restart

Lecture no-5

Virtual Private Network (VPN)

VPN is used for long distance connectivity. It is cheaper than Remote access because the medium is internet not PSTN.

Registered live public IP is needed for VPN server but there is no compulsion of live IP on client side. Static IP is the basic requirement of VPN.

You can connect multiple users on the same link in VPN which is not possible in remote access. In remote access you need a separate line for each user.

In VPN the connections are made on virtual ports. Multiple connections per physical medium is the advantage of VPN and it is possible due to the virtual ports of VPN. Less secure as compared to remote access because the medium is internet but you can say that VPN is secure because it uses IPSec for security. It is cleared that VPN is inherently insecure because medium is the internet.

VPN is the only way to connect private networks using internet.

Private IP ranges according to RFC 1918:

10.0.0.0/8

172.16.0.0/12

192.168.0.0/16

For example if there are two networks of Corvit one in Lahore and the other is in Islamabad. If these two networks have private addresses and want to communicate through internet. Then it is not possible without VPN because VPN make it possible that private networks can communicate using internet.

Installation of VPN

- Go to server manager
- Click on Roles then add roles
- Select Network policy and access services
- Click next
- Select routing and remote access server
- Click on next
- Click install
- Now give a live public IP to VPN server
- Give IP to client and assume that both are on internet
- Now open Routing and Remote Access from administrative tools
- Right click on it and select configure and enable

- Click on next and choose custom configuration
- Click on next select VPN access
- Select a connection and then select from a specified range option
- Give IPs range and click next
- Now select no, use routing and remote access option
- Click on ok and then finish

Allow users permissions

- Click on Active Directory users and computer in the administrative tools
- Right click on user and select properties
- Select dial-in and click on Allow access
- Click on apply and then ok

Now if you try to ping the system it will give no reply from the host. Therefore open the routing and remote access select IPv4 and click on general now right click on connection and press delete. The interface will be deleted

Connect through mstsc

- Make a connection on client computer as under
- Click on setup a new connection
- Click on connect to workplace and select next
- Click on use my internet connection and select I will setup internet connection later.
- Give IP address of VPN server
- Give username and password and click on next
- Click on create and then close

VPN protocols

1. IKEV2
2. SSTP
3. PPTP
4. L2TP

Connect on PPTP

- Go to the properties of the client adapter
- Click on security tab and select PPTP in type of VPN
- Click ok and then connect

Connect on L2TP

- Right click on network connection and select properties
- Select security tab
- Select L2TP
- Click on advance setting
- Give shared key MCITP2008
- Click on connect

Sharing

When you put a dollar sign ($) at the end, it is called hidden sharing.

Command:
C: hostname (press enter. It will display name of the computer)
C: net view pc1 (press enter. It will show shared files and folders)
C: mkdir test (press enter. It will create a folder named test)
C: net share test=c: \test (press enter. It will make test folder shared)
C: net view pc1 (press enter. It will show shared folders on pc1)
C: mkdir ishaq (press enter. It will create a folder named ishaq)
C: net share ishaq$=c \ishaq (press enter. It will make ishaq folder as hidden shared)
C: net view pc1 (press enter. It will show you shared folders but not hidden shared)
When you type \\pc1\ishaq in run window and press enter it will give an error message because this folder is hidden shared. If you want to open it place a dollar sign ($) after the folder name as: \\pc1\ishaq$ (press enter). It means that the person who knows the name of the hidden shared folder can open it otherwise computer will not show hidden shared folders.
Some folders are hidden shared by default which is called administrative hidden but administrator cannot give permissions to other users. It is just a facility for the administrator like C$, D$ etc. Administrator can give client only the permission of print$.
Note: if you want to shutdown the client computers remotely then the following command is used but you must be the administrator of those clients
shutdown –i (press enter) now add the computers like pc1, pc2 etc and press ok.
There are two types of permissions

1. **Share permissions:** It is used only for remotely access)
2. **NTFS permissions:** it is local permission. It is applied on both cases.

Everyone group is called special identity that represent all.

Exam 70-640: Active Directory Administration

Lecture no-1

Active Directory: Centralize repository that is store information about objects.
Normally when you check the system properties it will either be in a domain or in a workgroup.
In a **workgroup** systems are independent of each other. If there are 10 users in the workgroup then on each system you will create 10 users account. Workgroup performs decentralize management of resources. 10 computers are normally recommended for a workgroup.
Domain introduced first time in window NT of size 40 MB which provide centralize management of resources. In a domain one user one account and universal resource access. Now top level is forest inside forest there are trees and inside trees there are domains.
Forest is the collection of trees or domains .
Tree is the collection of domains has parent child relationship.

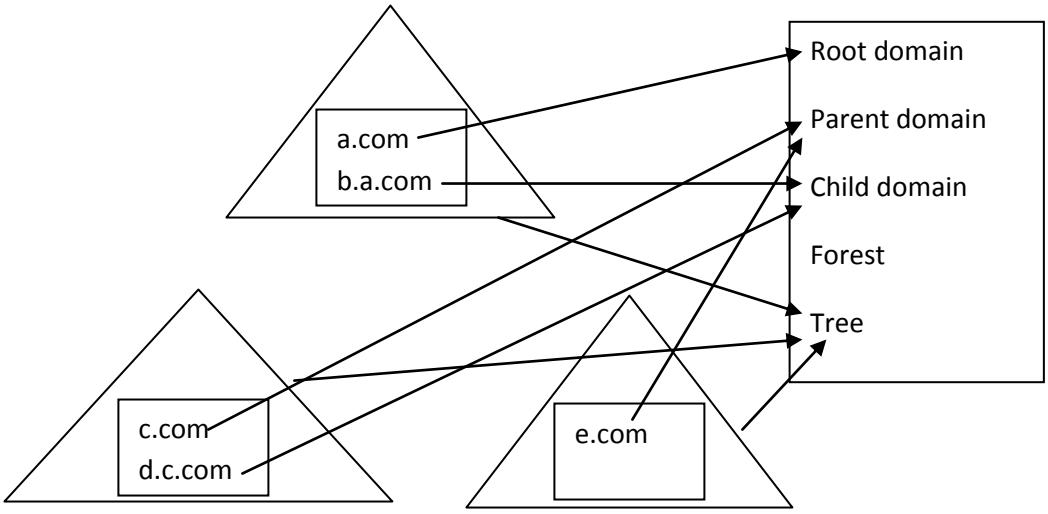
How to make system as Domain:

- Install server based operating system
- Install Active Directory
- Now your system will become a domain

Domain Types

There are three types of domain

1. **Root Domain:** first domain of a forest is called root domain. Only one root domain is possible in a forest. Installation of root domain creates a forest. Root domain is also a parent domain. When root domain crashed then the forest is also crashed but if other domain crashed then it will not affect forest.
2. **Parent Domain:** domain is installed either as a parent or a child. There can be multiple domains in a forest. Every parent domain is not a root domain but every root domain is a parent domain. First domain of a tree is called parent domain. Installation of parent domain creates a tree.
3. **Child Domain:**



No of forest= 1

Not of trees= 3

No of domains= 5

Types of Domain:

1. **Domain Controller (DC):** The machine on which active directory is installed is called Domain Controller. If it is the first domain installed then it is Domain Controller. In this case it is used a proper noun. Domain is the conceptual thing it

physically exists because of the Domain Controller. Only one domain can be installed on one computer.

2. **Additional Domain Controller (ADC**): When you install a second domain for load balancing then it is called Additional Domain Controller. It is also writable like Domain Controller. If the Domain Controller fails then Additional Domain Controller can be used.
3. **Read Only Domain Controller (RODC):** It is also used for load balancing but it not writeable it is only read only.

Logical Structure of AD:

- Forest
- Tree
- Domain
- OU

Physical Structure of AD:

- **Sites**
- **Subnets**
- **Domain Controllers**

Lecture no-2

Active Directory: - AD is the centralize repository that store information about objects.

Users and computers are the classes of objects. Objects properties in AD are called attributes. For example last name is the attribute of the user class. Classes, attributes, value set and their attribute types are stored in a place called schema.

All the trees in one forest have same schema. A collection of trees or domains have same configuration, schema and global catalog is called forest.

Note: when user logs in on the client system he enters username and password. The username is sent to the DC where it is checked with a password and encrypt with some

number and send it to the client to decrypt it. If the client decrypts that password then it is allowed for log on.

In Global Catalog values are stored while in Schema only attributes are stored.

Active Directory Partitions:

There are four partitions of Active Directory

1. Schema partition (forest specific)
2. Configuration partition (forest specific)
3. Domain Data Partition (domain specific)
4. Application Partition (configurable)

When you make changes in Schema partition or configuration partition then these changes are replicated in the whole forest.

States of Server base operating system:

There are three states of server base operating system

1. Stand alone server (workgroup)
2. Member server (no active directory)
3. Domain controller (active directory installed)

If you run dcpromo command then it will neither remain stand alone server nor member server.

Installation of Active Directory:

- Type dcpromo command in the run window
- Select advance check box
- Next page will show you operating system compatibility keep it unchanged and click on next
- Now there are four possibilities
    - Forest, tree, domain (root domain)→DC
    - Tree, Domain (parent domain) →DC

- Child Domain → DC
- ADC / RODC

- Now if you check Add a domain controller to an existing domain under the existing forest then it means that you are going to create **ADC /RODC**.
- If you check create a new domain in an existing forest under the existing forest option then it means that you are creating **child domain.**
- If you have marked create a new domain tree root instead of a new child domain check box under existing domain forest then it means that you are creating **parent domain**.
- If you check create a new domain in a forest option then it means that you are creating **root domain.**
- Select the last option create a new domain in a forest and click on next
- Give name to the domain (Corvit.com or test.com) and click next
- Now if you select windows server 2008 R2 in the domain functional level then you can use new features of Active Directory like recycle bin etc but your clients must be windows 7 or windows Vista.
- Therefore select windows server 2003 and click on next
- Select DNS server check box if you want to install DNS also and click next
- Click on yes and again click on yes
- Now it will show database folder, log files folder and SysVol folder (store group policy) and their locations.
- Now it will ask username and password. It is required if your Active Directory is crashed then all of user account will also be crashed then you can restore active directory by using this username and password.
- Click on next then next and select the Reboot on completion check box.
- When the installation complete then the system will be restarted.

Impact of Active Directory Installation

Before the installation of AD all the user accounts are stored in the computer management. You can go to computer management by using **compmgmt.msc** command. After installing AD all the user accounts are transferred to the Active

Directory by clicking Active Directory Services and the click on users to view the users account. Active Directory database file is ntds.dit (C:windows\ntds\ntds.dit) where dit stands for directory information tree and has 10MB size. Log file is edb, edb.chk is checkpoint file and res1, res2 are reserved files. Some services are also created like AD Domain services and AD web services after AD installation.

Regsvr32 schmmgmt.dll is the command to go to the schema where you see two things classes and attributes.

Active Directory Maintenance:

1. Backup → online (services start)
2. Restore
    a. Authoritative restore →DSRM (Directory Restore Mode)
    b. Non Authoritative restore → DSRM (Directory Restore Mode)
3. Move → offline (services stopped)
4. Defrag
    a. Manual → offline (services stopped)
    b. Automatic → online (services start)

In windows server 2008 R2 you don't need to reboot to offline ADS like windows server 2003.

Utility for taking Backup of AD

Wbadmin.msc is used to take a backup but this facility is not installed by default first you have to install backup services. Click on server manager then select Features then Add Features then select windows server backup then click on next and then install.

Now type wbadmin.msc command in the run window then select backup once click on next now select different options then select custom click on add item then select systemstate click on local drive and select the drive for backup click ok then click next and then click on backup.

Type **wbadmin get versions** command in the command line to show the name of the backup because the backup name is generated by the computer itself in date time format.

Lecture no-3

Active Directory Maintenance:

Active Directory is in the form of pages. A process which is called garbage collection process deletes unused files from Active Directory after every 12 hours. For maintenance you must stop the Active Directory services. There are two methods to stop AD services one is graphical that is click on administrative tools then click on services then right click on active directory domain services and click on stop.

Second method to stop AD services is from command line that is:

Commands for AD database and log files movement to another drive

- C:\net stop ntds (click enter) then click on yes (it will stop database services of AD)
- C: ntdsutil (press enter)
- Ntdsutil: activate instance ntds (press enter)
- Ntdsutil: files (press enter)
- File maintenance: move db to j: (press enter. This will move database to j drive)
- File maintenance: move logs to j: (press enter. It will move log files to j drive)
- File maintenance: quit (press enter)
- C: net start ntds (press enter. After movement again start AD database services)

Defrag or Compress AD database

- C: ntdsutil (press enter)
- Nudsutil: activate instance ntds (press enter. But before doing this stop AD database services by net stop ntds command otherwise it will give error)
- Ntdsutil: files (press ok)
- File maintenance: compact to e:\ (press enter. It will compress it to e drive)
- File maintenance: quit (press ok)

Restore of AD

There are two types of restore. One is called authoritative restore and the other is called non authoritative restore. When two DC's are working in the same domain then authoritative issue comes.

For example if two Dc's DC1 and DC2 are working in a domain. There are 95 user accounts on DC1 suddenly boss called you that I have fired 5 persons that is why delete the accounts of these persons therefore you have deleted but before that you have taken a backup yesterday. After 2 hours Boss again call you and told you that I have taken my decision back so again add these 5 persons accounts. You will restore the backup on DC1 but in this case the version Id's of DC1 are older and DC2 have latest version Id's. The DC who have latest version Id's are in full power. Now to give back the power to DC1 you will raise the version Id's of DC1 through a method called **Authoritative restore**.

For restoring the AD you will reboot your system then press F8 and select directory services restore mode then select other user.

Type wbadmin.msc in the run window and press ok then click on Restore then select this server press next then select system state then click on confirmation and then click on restore. This method is called **non authoritative restore**. In this case there is only one DC in the domain so there is no need of authority.

For authoritative restore

- First perform the wbadmin.msc process as mentioned above
- Then go to cmd and type c: ntdsutil (press enter)
- Ntdsutil: activate instance ntds (press enter)
- Ntdsutil: authoritative restore (press enter)
- Authoritative restore: restore object dc=Corvit, dc=com (press enter)
- Click on yes (it will raise version Id's of DC1 by one lakh in order to not override the previous one)
- Reboot the system

Operation Master

Some changes will only be performed on a specific DC not on all. That is why Active Directory is single master generally. Single master operation can be performed on a single DC. There are certain roles with that DC.

Roles:

1. Schema Master → one per forest
2. Domain Naming Master → one per forest
3. PDC (Primary Domain Controller) Emulator → one per domain
4. Infrastructure Master → one per domain
5. RID (Relative Identity) Master → one per domain

Root domain has the first two roles while on ADC there will 0 roles.

1. **Schema Master:** There are classes and their attributes in schema. Schema master is responsible for schema updates. Schema is available on all DC's but writeable schema is only available in schema master.
2. **Domain Naming Master:** It is responsible for the addition or removal of domains in a forest
3. **PDC Emulator:** It performs clock or time synchronization. It is responsible for group policy modification. It tells password reset information to all. It minimizes password change latency.
4. **Infrastructure Master:** It stores user to group references
5. **RID Master:** Permission to a user is given on the basis of SID (Security Identifier). It is a number which is generated when we create a user account. It is not changeable and not reusable it is unique.

   Object SID=Domain ID + RID

   RID Master gives a block of RID to other DC's. RID master is responsible for SID generation or it allocates blocks of RID to other domain controllers of the domain.

In order to view which computer has these roles go to command line and type fsmo (flexible single master operation) command.

c: netdom /query fsmo (press enter)

In graphical environment click on administrative tools then select active directory users and computers then right click on domain select operation master there you will see the domain name in the first field which is current role holder.

Now to check roles on forest (domain naming master)click on administrative tools select active directory users and computers then right click on root then select operation master.

Now to check schema master first run regsvr32 schmmgmt.dll in run window then run mmc click on add remove snap in from file menu then click on active directory schema and then click on add now right click on operation master.

Two things must be understand

1. **Transfer of role:** only possible if role holder is online. In this case no loss of information occurs.
2. **Seize of role:** only possible, if role holder is down (offline). In this case loss of information occurs.

These two operations can be performed on the successor means on which you want to transfer the roles.

How to connect with another DC

- Click on administrative tools
- Select active directory users and computers
- Right click on domain and select change domain controller
- Select the pc to connect
- Click ok

Transfer roles one by one

- Click on administrative tools
- Click on Active directory users and computers
- Right click on domain and select change domain controller
- Select ADC on which you transfer roles and press ok
- Now right click on AD and click on change operation

Transfer forest roles

- Click on administrative tools
- Click on Active directory Domain and trust
- Right click and select operation master
- Click on change

Transfer schema master role

- First connect with successor
- Now click on change domain controller
- Now right click and select change operation master.

Seize of roles

Seize means by force assign the role to other DC when one is crashed or down.

When you click on operation master and check the first field it will show an error there when DC1 is down.

Go to the cmd for seizing role

C: ntdsutil (press enter)

Ntdsutil: roles (press enter)

Fsmo maintenance: connections (press enter. Here you will connect to the pc to which you are making a role holder)

Server connections: connect to server pc1 (press enter)

Server connections: quit (press enter)

Fsmo maintenance: seize schema master (press enter)

Click on yes to continue

Fsmo maintenance: seize naming master (press ok and then yes to continue)

Fsmo maintenance: seize PDC master (press ok and then yes to continue)

Fsmo maintenance: seize infrastructure master (press ok and then yes to continue)

Fsmo maintenance: seize RID master (press ok and then yes to continue)

Lecture no-4

Managing user accounts:

Note: you can change the password policy by typing gpmc.msc command in the run window then click on domain then right click on default domain policy and select edit then click on policies → windows setting → security setting → account policies → password policies

You can create user accounts through bulk import process. There are three methods that can be used.

1. **CSVDE** (Comma Separated Value Data Exchange): It is used for only adding user accounts.

2. **LDIFDE** (Lightweight data interchange format data exchange): It is used to add, modify and delete user accounts.
3. **Windows Scripting Host**

Steps of CSVDE

- Open a notepad
- Write **dn,objectclass,samaccountname,useraccountcontrol** in the first line.
  Note: In the above line **dn** represent distinguish name for display; new naming convention called LDAP used by AD that uses distinguish name to make the name unique in the domain. **objectclass** represent the type of object you are creating. **Samaccountname** represent the logon name of the user. **Useraccountcontrol** represent to enable or disable the account 512 is used for enabled and 514 used for disable account.
- **"ou=mcitp,dc=khan,dc=com",organizational (this will create an organizational unit with the name mcitp in khan.com domain) after pressing enter key type the following in the next line**
  "cn=ishaq,ou=mcitp,dc=khan,dc=com",user,ishaq,512
  "cn=imran,ou=mcitp,dc=khan,dc=com",user,imran,512
  "cn=arshad,ou=mcitp,dc=khan,dc=com",user,arshad,514
  "cn=izzat,ou=mcitp,dc=khan,dc=com",user,izzat,514
  Note: the above four lines will create four users named ishaq, imran, arshad and izzat in the organizational unit mcitp on khan.com domain
- Save this file with **.csv** (test.csv) extension and select all files in D drive for example
- Go to cmd and import the file by typing **D: csvde –i –f test.csv** (press enter)
- You can also export file as **d: csvde –f file1.csv** (press enter). It will create a file with the name of file1 on D drive.

Steps for LDIFDE

- Open a notepad and type the following
- **Dn: cn=kashif,ou=mcitp,dc=khan,dc=com**
  changetype:add
  objectclass:user
  samaccountname:kashi
  useraccountcontrol:512
  Dn: cn=amir,ou=mcitp,dc=khan,dc=com
  changetype:add

objectclass:user
samaccountname:amir
useraccountcontrol:512 (the above lines will create two users named kashif and amir in the mcitp OU on the khan.com domain)

- Save the file with **.ldf** extension **(test1.ldf)** and select all files.
- Open cmd and import the file by using the command **d:ldifde –i –f test1.ldf** (press enter)

Steps for modification user account in LDIFDE

- Open note pad
- **Dn: cn=ishaq,ou=mcitp,dc=khan,dc=com**
  changetype:modify
  replace:description
  description: this is a test user account -

  Dn: cn=imran,ou=mcitp,dc,khan,dc=com
  changetype:modify
  replace:location location:
  kabul
- Save the file with **.ldf** extension **(test2.ldf)** and select all files.
- Open cmd and import the file by using the command **d:ldifde –i –f test2.ldf** (press enter)

Steps for deletion of user account in LDIFDE

- Open note pad
- **Dn: cn=ishaq,ou=mcitp,dc=khan,dc=com**
  changetype:delete
- Save the file with **.ldf** extension **(test3.ldf)** and select all files.
- Open cmd and import the file by using the command **d:ldifde –i –f test3.ldf** (press enter)

Lecture no-5

Steps for Windows Scripting Host

- Open note pad and type the following
- **Set objOU= getobject ("LDAP://ou=mcitp,dc=khan,dc=com")**
- **Set objUser = objOU.create("User", "cn=ishaq")**
- **objUser.put "samaccountname", "ishaq"**
- **objUser.SetInfo** (it show end of file)
- Now save the file with **.vbs** extension (test3.vbs) and select all files
- Now open the command line and import the file using the command
- C:**wscript test3.vbs** (press enter)

Managing Groups

Making groups provides flexibility. For example if you are applying some permissions on 1000 users on the same nature then you manually apply the permissions on each user means you have to modify 1000 users. Instead create a group and place the users of the same nature in this group and apply permissions on this group which will be applied to all 1000 users.

Group types: There are two types of groups

1. **Security group:** In Security group everything is possible means you can use it for permissions and also for email system.
2. **Distribution group:** It is only used for mailing system and cannot be used for permissions. That is why you right click on the folder and then click on permissions you will only see security groups not the distribution group.

Note: Create three groups as follow

- Go to active directory users and computers right click and select new then click on group.
- Give name to the group and select the type of this group security. Similarly create two more groups one of type security and the other is of type distribution type.
- Now in your computer right click on any folder select properties and then select sharing then click on add group and click on find button. You will only see the two groups having type security not the distribution group.

There are two types of permission one is share permission and the other is local permission. The share permission is applied when the object is accessing remotely. You can assign share permission on a folder by right clicking and select the properties and then click on sharing then click on advance sharing then give name to the shared folder then add the group and then assign permissions. Local permissions are applied on both type of access i.e. for remote access and for

local access but local permission override the remote permission. You can apply local permission on a folder by right clicking and then select properties then select NTFS tab and apply the permission.

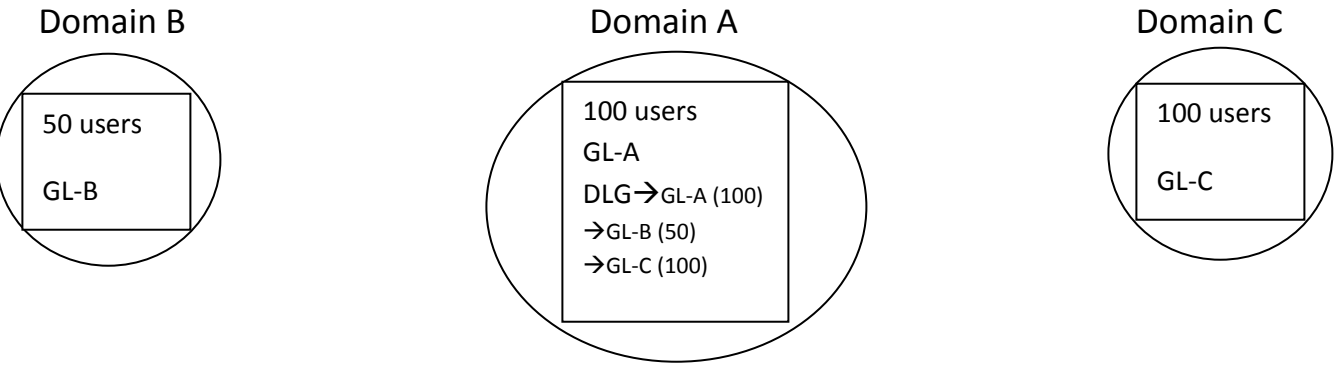
Group Scope: There are three scopes used

1. **Global group:** Two things are important in group scope one is membership and the other is visibility. The **membership** of the global group is only users from its own domain. The **visibility** of the global group is throughout the forest.
2. **Domain local:** Membership→ users from any domain in the forest while visibility →only in its own domain.
3. **Universal:** Global Group + Domain Local → Universal Group

You need all these things in a multi-domain environment. There is Microsoft rule A G D L P: A→ add users, G→ global group, DL→ domain local group, P→ permissions.

It means that add users to the global group then add the global group into the domain local group and then apply permissions.

Case Study:



If systems are attached to the Domain A then Domain A, B and C are called Accounts domain because the users are available on it while domain A is also called a resource domain. Account domain needs global group and Resource domain is called domain local group.

Consider another case study let a Folder named Folder A has the following permissions

	Share Permission	NTFS Permissions
Group-A	Read	Modify
Group-B	Change	Read

Ishaq (member of A, B) Full Control Read

Full Control (most) + Modify (most) → Modify (least)

Group Policy:

Group policy provide two things to the users

1. Facilities to the users
2. Restrictions on the users

There are two policies available on domain by default. One is called default domain policy and the other is called default domain controller policy. Type gpmc.msc command in the run window the group policy management console will be opened. Then click on domain then click on group policy object these two will be displayed.

Group policy is applied on a container. Inside the container there may be either users or computers. On users the policy is implemented when he logs on while on the computer it is applicable when the system reboots. Group policy enable containers are:

- Site (click on administrative tools and select AD sites)
- Domain (click on administrative tools and then AD users and computers)
- OU (right click on domain and select new Organization Unit)

By default only one OU called domain controller is installed when AD is installed.

GPO (Group Policy Object)

1. **GPC (Group Policy Container):** It is viewable through Active Directory users and computers (click on Active directory users and computers/right click and select view/advance features/system/policies/(you will see 2 default GPC policies) . It provides version information for synchronization.
2. **GPT (Group Policy Template):** It is viewable in SysVol (C:\ windows\Sysvol\domain\policies\(you will see 2 default GPT policies)

Now create another group policy in the policy management console by right click on the group policy object and select new then give name to the policy. Now check in both GPC and GPT the policies will be shown 3.

Overall Administration of Group Policy

1. Copy and paste
2. Backup and restore

Right click on one of the group policy object and select copy then select paste the policy object will be pasted then rename it and edit for further modifications.

There is a new feature in window 2008 server called Starter GPO. In which a company general template (rules) is made then whenever you create a new policy object. Select Starter GPO object then right click and select new then give name then click ok. Now if you want to create a new policy object right click on the group policy object right click and select new give name to the policy object and below in the drop down list select the starter GPO template and the click ok and then right click and select edit for further modifications and permissions.

Steps for backup and restore group policy

- Right click on group policy object
- Select backup
- Click browse and give name to the folder for backup
- Click on backup
- Now for restore, right click and select restore
- Browse for the location and select backup
- Click next and then ok

WMI Filter: - It is a tool which filters out the conditions during logon. For example if we want to install MS Office on the user account first of all we will check the free space. For this purpose you need to write a SQL query. A tool WMIMetic tool is also available on Microsoft website for download that makes a script for WMI filter.

Steps:

- Right click on WMI Filter and select new
- Give a name to the filter
- Click on Add now write the following in the query box
- Select *from win32logicaldisk where drivename=”c” and drivetype=2 and freespace >=1000000 (space is in bytes)
- Save it then go to the group policy object for example sales then select WMI filtering then click on MS Office then yes.

Software Deployment using Group Policy

Following files are used in software deployment

1. **.msi** (windows installer package) used for software deployment.
2. **.mst** (transform file) used for custom installation.
3. **.msp** (patch file) used for service packs / hot fixes
4. **.ZAP** (if software does not contain .msi file and only setup file is available then you create .ZAP file which for non-msi software)

There are two types of deployment

1. **Assign** (the assign deployed software is displayed in start menu)
2. **Publish** (published deployed software is available in control panel then programs and feature then in network)

First of all SDP (software distribution point) will be created on the hard disk that contains the software to be deployed. Generally assign deployment is used for computers which are fixed for the users. While publish deployment is used for users whose computer is not fixed.

Note: in domain environment when we create a user then click on the user properties and select member of tab and write "ba" and click on add and apply. Otherwise you cannot logon with this user.

Lecture no-6

Steps of Software Deployment

- First make a SDP (software Distribution Point) on your hard disk and right click on it go to properties then advance sharing and then give full control to every one group.
- Now open group policy management console (gpmc.msc) and click on domain and select group policy object
- Right click on the default domain policy and select edit
- There click on policies under computer and click on software settings
- Right Click on software installation and select new package
- Give the network path (\\pc10) and press enter the shared folders will be displayed.
- Select SDP and then click on .msi file and press ok then it will ask whether you want to assign or publish the application select your choice and click ok.
- If you want to install customize packages (like excel, word only) through software deployment then you need .mst file
- First of all install ORK(Office Resource Kit) from MS Office CD in order to make .mst file

- After installing ORK open it from programs then tools then resource kit
- Click on custom installation wizard
- Browse for Proclus.msi from SDP
- Create a new MST file give any name
- Next then next and select packages from the software
- Click on next and then click on exit
- At the end it will ask CD key as volume license.
- Now right click on group policy and edit default domain policy
- Select policies under computer configurations and then click on software settings
- Right click on software installation and select new package
- Give a network path select the SDP then office then Proclus
- Then select advance then select modification then click on Add
- Select MST then deployment then select assign
- Select install at logon and then click on ok
- Now update group policy by gpupdate command

Note: if there is no .msi file then you can create it by using a software called WININSTALL that is called msi maker.

How to create ZAP file

When only setup file is available of the software then you can create a ZAP file. It is published not assigned. There is no self repair in ZAP file.

- Open Notepad and write the following commands
- [application]
- Friendlyname= “acrobat reader”
- Setupcommand= acrobat.exe
- Version= 5.0.0.1
- Save this file with the .zap extension in the same location where the acrobat.exe is stored.
- Share this folder and assign permissions
- Now go to default domain policy right click and select edit
- Select policies under users and then select software settings
- Right click on software installation and select new package
- Select ZAP click on add then select publish and click on OK

Active Directory Certificate Authority (CA)

The purpose of Certificate Authority is authentication and confidentiality. CA provides certificate.

Symmetric encryption: In this method the decryption and encryption keys will be same. It means that you will need the same key for decryption that you have used for encryption.

Asymmetric encryption: In this method the encryption and decryption keys are different. It means that when you use one key for encryption then you can decrypt the information with a different key.

There are two important things

1. **Public key authentication:** In this case the senders encrypt information with its private key. It is asymmetric encryption now the receiver will use public key of the sender to decrypt this information
2. **Public key encryption:** In this case the senders encrypt the information with the receiver public key. It is also asymmetric encryption in which the receivers will use its private key to decrypt it.

Indirectly keys are issued by CA. CA issue first certificate to itself then he gets the ability to give certificates to others and CA always sends information in encrypted form. When a person request for the public key of the receiver. CA issues him his own certificate containing CA public key and then encrypt other person public key with its private key and send it to you. You will decrypt CA encrypted information by his public key and will take the public key of the other person.

CA Installation

There are some impacts of CA after its installation on the system. First impact you cannot change the system name after CA installation. Second you cannot remove or add system to domain after CA. Third you cannot remove Active Directory from the system after CA installation.

Steps

- Click on Server Manager and select Roles
- Click on Add Roles and click on next
- Select Active Directory Certificate Services from the list
- Click next then click next
- Select Certification Authority, CA web enrollment and online responder check boxes from the list
- Click next then select enterprise then click on next

- Select Root CA and click next
- Give any name to CA and click on next then give the validity period 5 years by default.
- Click on next then next then select on windows integrated authentication
- Click on next and then install
- After installation right click on CA and select properties click on advance you will see Issued to and Issued by information of certificate. You can also check the public key by clicking on the details button.

How to Issue a Certificate

There are two methods used to issue a certificate. One is using the mmc and the other is web enrollment.

Steps of mmc method

- Type mmc command in the run window
- Click on File menu and select Add/Remove Snap-in
- Select certificate from the list and then click on add button
- Select my user account
- Click on finish and then OK
- Now click on certificate then on personal the certificate that is already exist is un trusted.
- Now right click there and select new tasks then click on request a new certificate.
- Click on next then next
- Select user and click on enroll and then finish
- The certificate will be visible in the issued certificate folder.

Steps for web enrollment

- Open your web browser
- Type the URL pc1/certsrv
- Give user name and password
- Click on request a certificate link then select user certificate
- Click on submit button

Certificate Revocation List (CRL)

If you want to revoke a certificate from the user then use the following Steps

- Right click on the certificate

- Select all tasks then click revoke certificate
- Give reason code but remember that the certificate will be unrevoked only if you select certificate hold reason code.
- The certificate will be temporally disabled again right click on that certificate go to all tasks and select unrevoked

CA backup and Restore

Steps for CA Backup

- Right click on CA
- Select All Tasks and click on Backup CA
- Click on next and browse for the folder in which you want to store backup
- Give a password and then click on finish

Steps for CA Restore

- Right click on CA
- Select All Tasks
- Click on Restore and click ok
- Click on next and then browse for folder where backup is located
- Click on ok then click on next
- Give the password that you have assigned during backup
- Click finish then click on yes

Lecture no-7

Active Directory Replication

Replication is derived from a word replica which means copy. Replication means to make a copy. Actually ADC is the copy of the DC.

Sites: The collection of DC's connected with a high speed permanent and reliable connection is called a site.

In normal terms sites means locations. There are two types of replication.

1. **Inter-site Replication**

Inter-site replication means replication between sites. In this case there are multiple sites. The bandwidth of the link will be slow in case of inter-site replication because the link is WAN.

a. Compressed replication traffic is required when the bandwidth is low.
b. It performs Scheduled updates (by default 3 hours).
c. Automatic / Manual updates can be performed (by default 180 minutes interval).
d. Configuration is needed in case of inter-site replication

2. **Intra-site Replication**

Intera-site replication means replication within sites. Connection is high speed, reliable and permanent in case of intra-site replication.

a. Uncompressed replication traffic
b. Event triggered updates
c. Automatic / Manual and non scheduled
d. No configuration is needed.

Steps for Intra-site replication:

- First we need one DC and one ADC for replication.
- Click on Active Directory Users and computers from administrative tools
- Click on the Domain Controllers. You will see two DC's let say pc1, pc3.
- Now open DNS click on sites then on default sites. There will be six entries three for one DC and three for another DC.
- Now open Active Directory sites and trust.
- Right click on site and select new site.
- Give name to the site for example Lahore.
- The above site will be replicated on another DC. You can check it within the site of another DC.
- Now make a user on one DC. This user will be replicated automatically without any configuration on another DC because it is event triggered updates.

Multiple Sites: for example we have two sites A and B. There are two DC's in site A and three DC's on site B. Both sites are interconnected with each other through WAN link. It means that it is Inter-site replication. Now a question arises that is it logical that every DC of site B will send updates or changes to every DC in site or only one DC from site B sends or receive updates or changes from one DC of site A and then forward these updates or changes to the local DC's.

The DC on each side that sends or receives changes or updates from other site DC is called Bridge Head Server. Therefore we can define it as A domain controller that receives changes from remote site and then forward these changes to local DC.

If you want to display bridge head server then type the repadmin /bridgeheads command in the command line but you will see no bridge head server.

Now make two sites Lahore and Islamabad then move Lahore DC into Islamabad site then again run the above command.

Site links

Site links means when you are establishing links between sites then you must consider the following five things

1. Protocols
    a. IP
    b. SMTP (it runs on limited bandwidth)
2. Member site
3. Cost
4. Interval
5. Schedule

Steps:

- Click on Administrative tools then click on Active directory sites and trust
- Click on AD sites and services then click on sites
- click on inter site transport then select IP and right click on it and select new site link
- Give name to the site and press ok.
- Now right click on the created site and select properties
- Click on cost. When the value of cost is low then its priority is high. For example if you have two links A and B. The link will be preferred whose cost is low. But if both links have the same cost then defines a schedule by clicking on the schedule button.

Active Directory Partitions

There are four partitions of AD which is also called replication units

1. Schema Partition → Forest specific replication
2. Configuration Partition → Forest specific replication
3. Domain Data Partition → Domain specific replication
4. Application Partition → Configurable replication

Active Directory Replication Monitor

KCC stands for Knowledge Consistency Checker. It is a background service that makes the topology consistent. Type repadmin /kcc in the command line and press enter. Replication Monitor is an important tool which is used for the monitoring of Active Directory.

Steps:

- First install support tools from windows server 2003 CD. Click on support tools then inside the tools folder select support tools .msi and install it.
- Now type replmon in the command line and press ok
- Right click on the monitored server and select Add monitored servers
- Add the name of the server or click on search
- Click on expand

Exam 70-643: Windows Server 2008 Application Server Infrastructure, Configuring

Lecture no-1

Managing Server 2008 Storage

- Basic Disk
- Dynamic Disk
- Primary Partition
- Extended Partition
- Logical Partition
- Simple Volume
- Spanned Volume
- Stripped Volume
- Mirrored volume / disk duplexing
- Hardware implementation of RAID
- Software implementation of RAID

- RAID-0 (disk stripping / stripped volume)
- RAID-1 (disk mirroring / mirrored volume)
- RAID-5 (stripped volume with parity)
- San
- Nas
- Storage networking

Lecture no-2

IIS (Internet Information Service)

Microsoft implementation of web server is called IIS.

How to Install IIS

- Go to server manager click on Roles
- Click on add roles and click on next
- Select Web Server (IIS) and click on next
- Click on next then install and then click close

Steps for Making DNS Zone

- Open DNS from administrative tools
- Select forward lookup zone
- Right click on it and select new zone
- Select primary zone
- Give name to the zone (corvittraining.com)
- Inside this newly created zone create a host record by right clicking
- Give name www and assign IP address 192.168.0.1

Steps for making a website

- Open note pad and write some HTML code
- <html><body>
- This is a test website for web hosting
- </body></html>
- Make a folder with the name web in D drive and save this file with test.html

Steps for creating site

- Open IIS from administrative tools
- Right click on site and select add new site
- Give name to the website
- Give a physical path (browse for the website in D drive)
- Give hostname (www.corvittraining.com)
- Click ok
- Now click on the default documents and remove all documents
- Add your own document test.html to the default document
- Enable it and then click ok
- Stop the website then start the website
- Now go to Internet Explorer and type the URL www.corvittraining.com

Hosting multiple websites on same web server

There are three methods for hosting multiple websites on the same web server

1. Different IP's for each website
2. Different ports for each website
3. Different HTTP Headers (host names) for each website

Steps for hosting multiple websites on same web server using different IP's

- Firs assign another IP address to the network adapter
- Right click on the network adapter and select properties
- Click on advance setting and give another IP address (192.168.0.5)
- Then Open DNS from administrative tools
- Select forward lookup zone
- Right click on it and select new zone
- Select primary zone
- Give name to the zone (corvitsolution.com)
- Inside this newly created zone create a host record by right clicking
- Give name www and assign IP address 192.168.0.5
- Now Open IIS from administrative tools
- Right click on site and select add new site
- Give name to the website
- Give a physical path (browse for the website in D drive)
- Give hostname (www.corvitsolution.com)

- Click ok
- Now click on the default documents and remove all documents
- Add your own document test.html to the default document
- Enable it and then click ok
- Stop the website then start the website
- Now go to Internet Explorer and type the URL www.corvitsolution.com

In order to host multiple websites on the same web server by assigning different port numbers, you have to assign different port numbers in creating new websites and in the internet explorer write the port number along with URL as www.corvittech.com:8011 but it is impractical in real world.

URL Redirection

URL redirection means to redirect one website address to another address.

Steps:

- First of all install IIS redirection from server manager
- Click on roles then right click on add roles services
- select IIS redirection and click on install
- Then Open DNS from administrative tools
- Select forward lookup zone
- Right click on it and select new zone
- Select primary zone
- Give name to the zone (corvitlahore.com)
- Inside this newly created zone create a host record by right clicking
- Give name www and assign IP address 192.168.0.1
- Now Open IIS from administrative tools
- Right click on site and select add new site
- Give name to the website
- Give a physical path (browse for the website in D drive)
- Give hostname (www.corvitlahore.com)
- Click ok
- Now click on the default documents and remove all documents
- Add your own document test.html to the default document
- Enable it and then click ok
- Now click on HTTP redirect

- Write www.corvittraining.com in the redirect to
- Click on apply
- Stop the website then start the website
- Now open browser and type www.corvitlahore.com it will be redirected to www.corvittraining.com automatically.

IIS Backup

- Open command line by typing cmd in the run window
- C: cd windows (press enter)
- C:windows> cd system32 (press enter)
- C:windows>system32\cd inetsrv (press enter)
- C:windows\system32\inetsrv> appcmd add backup mybackup (press enter)

Now go to IIS and remove all sites in order to restore it again

IIS Restore

- Open command line by typing cmd in the run window
- C: cd windows (press enter)
- C:windows> cd system32 (press enter)
- C:windows>system32\cd inetsrv (press enter)
- C:windows\system32\inetsrv> appcmd restore backup mybackup (press enter)

Note: It will only restore site configuration not the web contents

Windows Share Point Services

Windows share point services are not available by default in the server 2008 CD. You have to download it from the Microsoft website. It is used to make portals, blogs etc. portal is a website which gives information as well as interaction to the users (for example facebook, orkit etc). Windows share point services change the website into portal. Perform the following three steps

1. Install share point services (select Basic installation in the wizard)
2. Run share point products and technology
3. Create a web application

- Open share point administration
- Click on application management
- Click on create or extend web application

- Click on create a new web application
- Give user name and password in configurable option
- Give name of the server in the search server option and click on ok
- Click on create site collection in the application management
- Give title doc then click on collaboration document workplace
- Give two user names and passwords and click ok
- Open it and add a new document
- In order to give quota open quota template
- Give name to the quota and assign size in MB and also size for warning
- Now click on create site collections
- Give title blog
- Give two user names and passwords.

Backup and restore operations of IIS

- Open share point administration
- Click on application management
- Click on perform a backup
- Store it in a shared folder
- Select all and click on continue to backup
- Select full backup and browse for the location to store
- In the restore operation click on restore from backup
- Browse for the location and click ok

Lecture no-3

Remote Desktop Services

There are two components of the remote desktop services. Remote Desktop Services is introduced in windows 2000 which is called terminal services in which both the components must be installed. In Windows 2003 both these components were separated. In windows 2008 R2 it is called remote desktop services.

1. Remote Administration

For remote administration you don't need to install remote desktop services only enable it from the properties of computer.

2. Application Sharing

If you want to perform application sharing then you must install remote desktop services from Roles.

Steps of installing remote desktop services:

- Click on server manager and click on roles
- Click on Add roles
- Select remote desktop services from the list and click on next
- Select remote desktop session, licensing, and web access from the list
- Click on next select don't required network
- Select per user then click on next and next
- Select domain and click on next then install
- Now type mstsc in the run window or click on the administrative tools and select remote desktop services then click on remote desktop
- Click on Remote Application Manager and then click on Add remote application.
- For example select power point application
- In IIS a virtual directory with a name RDweb for remote desktop is created.

Windows Media Services

It is the implementation of streaming media server is called Windows Media Services (WMS). When you want to online videos then you need WMS for that. There are two methods used for WMS:

1. Live stream by using http protocol
2. Live stream by using RSTP. It works on port 4554 and uses both UDP and TCP.

You need to create a publishing point when you on air live contents. There are two publishing points.

1. Broadcast publishing point: There is no control of the user on broadcast publishing point. You cannot pause the streaming video.
2. On demand publishing point: User can control, pause and start the video in on demand publishing point.

In order to use Windows Media Services you need to download Microsoft Standalone Package from the internet and install it. After that you will be able to see streaming window media server in the Add Role wizard. Then select it and click on install.

For windows Media Player

- Click on administrative tools
- Select features and click on Add feature
- Select Desktop experience from the list and click on install.
- Now go to Roles click on Add Role
- Select streaming media services and click on next
- Then select all options in this window
- Click on RSTP and click on next
- Click on next and then install.

Make a publishing point

- Open windows media services from the administrative tools
- Right click on publishing point and select new publishing point
- Give name to the publishing point
- Click on one file and then next
- Select broadcast publishing point and click on next
- Select unicast and then browse for the video clip
- Select file and click on next
- Then click on create an announcement file then next
- Click on finish

Note: after performing all these steps if still the video is not playing then only connect the computer to the internet it will be played. Similarly On Demand Publishing having the same steps.

Windows Server Update Services (WSUS)

- Click on server manager
- Click on Roles and then Add Roles
- Select windows server update services
- The update will be downloaded from the Microsoft website.
- After downloading configure it so that other clients will take updates from this server not from the internet.