A

Practical Training Report

On

"Design Computer Network"

Submitted

in partial fulfilment

for the award of the Degree of

Bachelor of Technology

In

Computer Engineering

Submitted To:

Mr Madhav Sharma

Computer Science Department

Submitted By:

Midhula K Martin

B. Tech VI Year

16EJGCS200

JAGANNATH GUPTA INSTITUTE OF ENGINEERING AND TECHNOLOGY, JAIPUR

[2015-19]

Candidate's Declaration

I hereby declare that the work, which is being presented in the report entitled **"Design Computer Network"** in partial fulfillment for the award of Certificate of "IT & NETWORKING" in Computer Engineering, and submitted to the **Department of Computer Science ,** BSDU is a record of my own work carried out under the Guidance of Mr. Madhav Sharma.

(Signature of Candidate)
Midhula K Martin

ABSTRACT

Project for the B. Tech Students

Design a computer network for an organization having 2000 nodes including around 800 Wireless nodes

Following are the requirements of the organization:
a) Dynamic IP Address allotment to each node.
b) Central management of data for each member with space restriction.
c) Common Desktop background to each computer connected across network. All local drives
should be hidden except network drive.
d) Implementation of the Web Sen/er with website locally.
e) Deployment of the Operating system from Server to several client machines simultaneously.
f) Implementation of FTP Server with authentication.
g) Centralized management of the antivirus with monitoring on client machines.
h) Data security with RAID configuration.
i) Deployment of printer to 5 departments across the Network.
j) Sharing of internet connection with Authentication as per company policies.

1. Which topology will be preferred in the design? Explain.
2. Estimate the requirements of Network devices like Network Switches, Access Points, Patch
Panel, Cables, Routers, etc.
3. Estimates the cost of peripherals.

Problem Statement: In an Organisation of 5 storey building, we have design the Network for 1000 host such that 400 are wireless and remaining are wired.

Key Assumption:

1.) 5 Storey building such that at each floor have 10 rooms(5 rooms are left of corridor and right of corridor).
2.) Each room are having 20 nodes.
3.) Each floor are having independent node.
4.) Network ls scaleable.
5.) The wireless nodes which receive wifi signal. S0, at each floor wifi signal should be available with proper WPA/WPA 2.
6.)The wifi signal should have same SSID on all the floor for proper intregration of the client.
7.)The server room is located on the Ground floor.
8.)Speed of LAN = 1000 MBPS

Based on the above assumption empirical calculation can be easily done.

System Requirement:

Length of Cable Require:
Number of L-2 Switch:
Number of L-3 Switch:
Number of Patch Panel :
Number of Rack:
Number of Router:
Number of Firewall:
Number of Server:
Number of l/O require 1

Topology:

In the Organisation we have 1000 nodes including 400 wireless nodes.

Now we arrange the nodes in the organisation such that 200 nodes will be available on the ground floor next 200 nodes on the first floor and soon.

We connect wired nodes as each 60 nodes pair to one 12U rack on each floor and wireless 20 nodes to each access point such that four access points are available on each floor.

Now in order to connect each host in the network we use star topology such that each node is connect to its local switch and it is futher connect to main L-2 switch to which firewall is connect.

A star topology typically uses a network hub or switch and is common in home networks. Every device has its own connection to the L-2 switch. The performance of a star network depends on the L-2 switch. If the L-2 switch fails, the network is down for all connected devices. The performance of the attached devices is usually high because there are usually fewer devices connected in star topology that in other types of networks.

A star network is easy to set up and easy to troubleshoot. The cost of setup is higher than for bus and ring network topology.

Advantages of Star Topology

1) As compared to Bus topology it gives far much better performance, signals don‘t necessarily get transmitted to all the workstations. A sent signal reaches the intended destination after passing through no more than 3-4 devices and 2-3 links. Performance of the network is dependent on the capacity of central

2) Easy to connect new nodes or devices. ln star topology new nodes can be added easily without affecting rest of the network. Similarly components can also be removed easily.

3) Centralized management. lt helps in monitoring the network.

4) Failure of one node or link doesn‘t affect the rest of network. At the same time its easy to detect the failure and troubleshoot it.

Patch Panel:

According to the requirement of L-2 switch we will consider the same number of patch panel.

Therefore, Total number of patch panel require =10 (48 ports)

Total number of patch panel require =10 (24 ports)

L-3 switch:

Total Number of L-3 switch = 1

Router:

Number of Router = 1
Firewall (Hardware) 1
Number of firewall =1

Server:

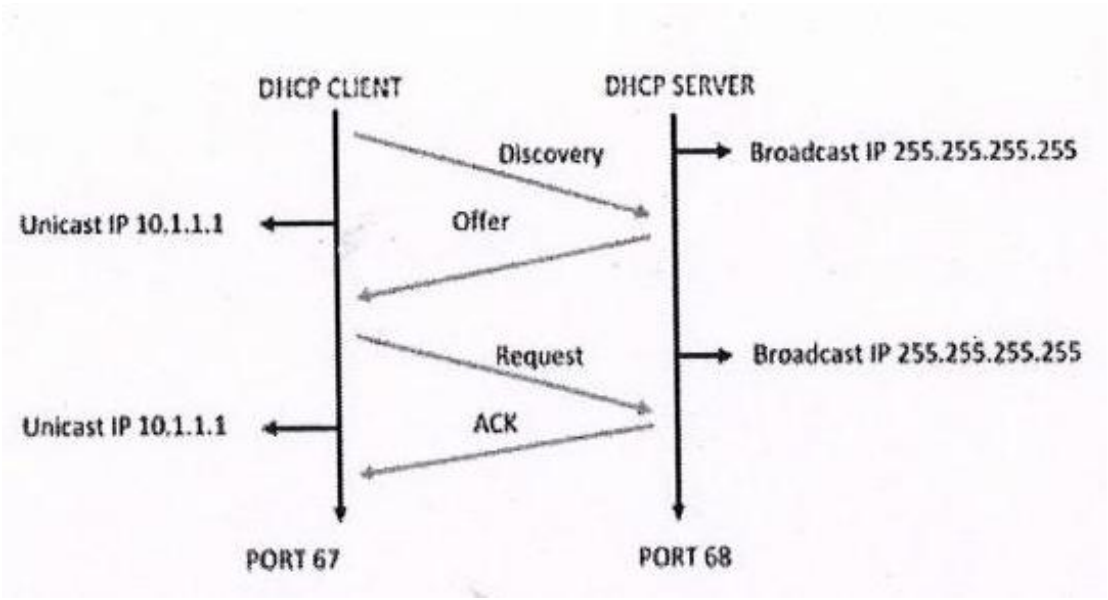
Number of server require = 2

CHAPTER 1:

DHCP (Dynamics host configuration protocol):

While configuring this services in the server we can assign the ip address to the system dynamically from the server pool. With DHCP it provides the lease duration of the ip address, subnet mask Gateway and Dns. Actually Dhcp works on the two principles. The principle are as follow:

a) DORA :

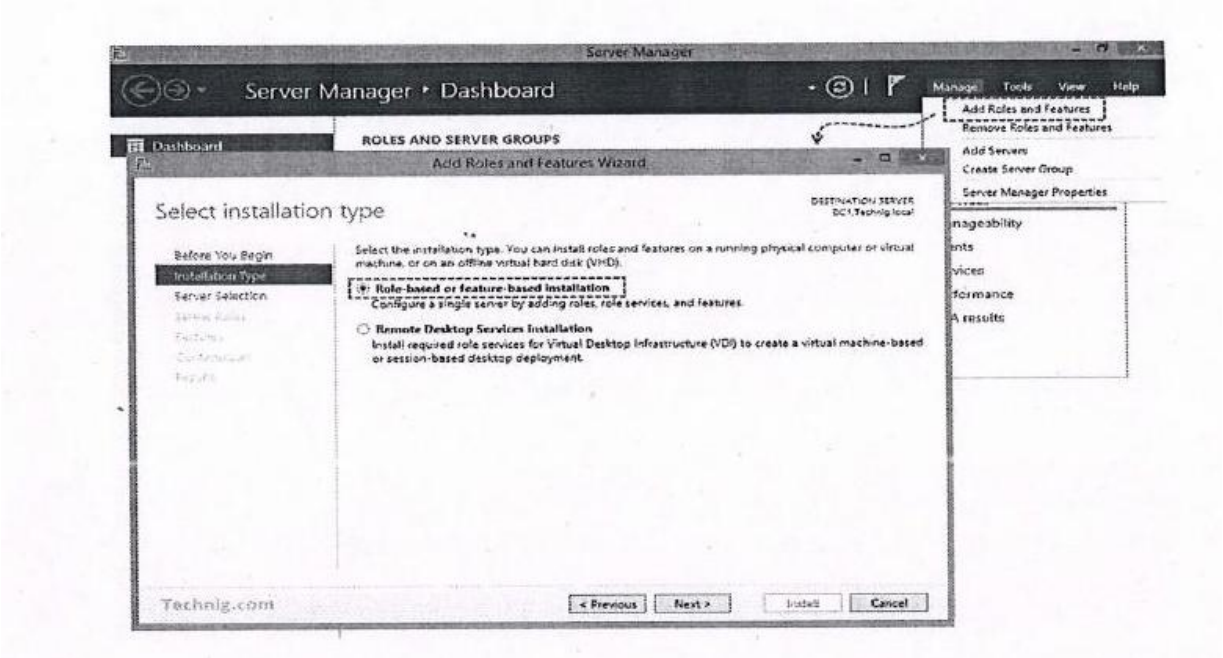


b) ROSA:

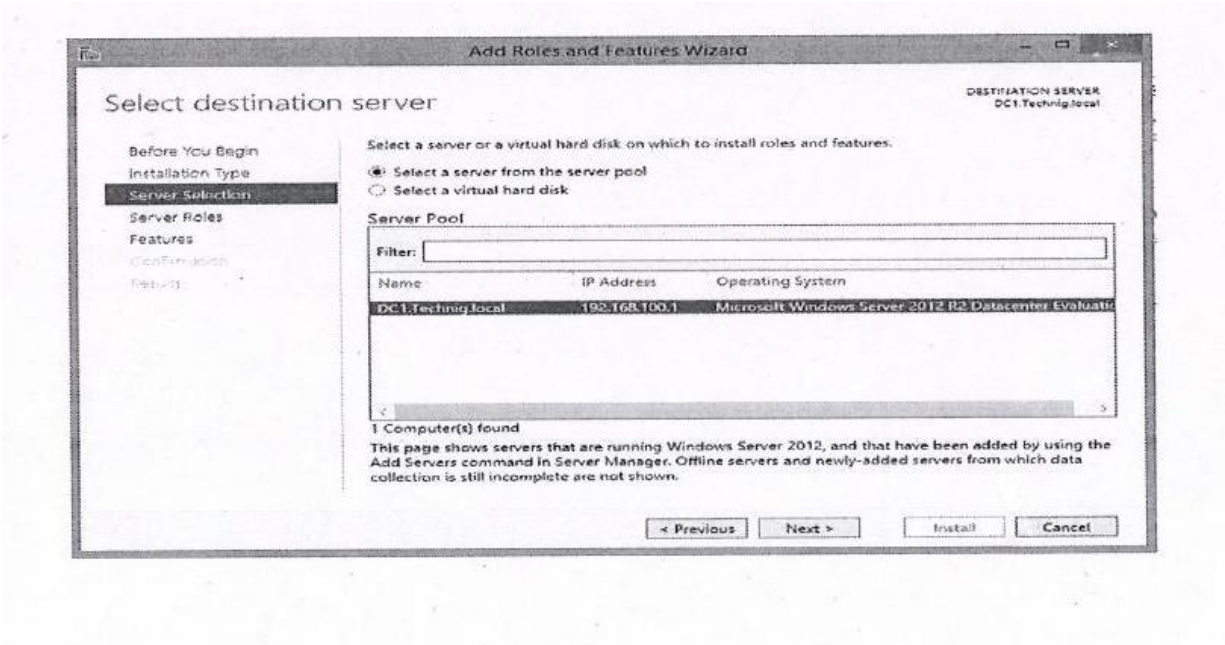
It is similar to Dosa but here the process start with client side as request and same procedure take place as follow:

Request ....>offer ....>send ....>acknowledgment.

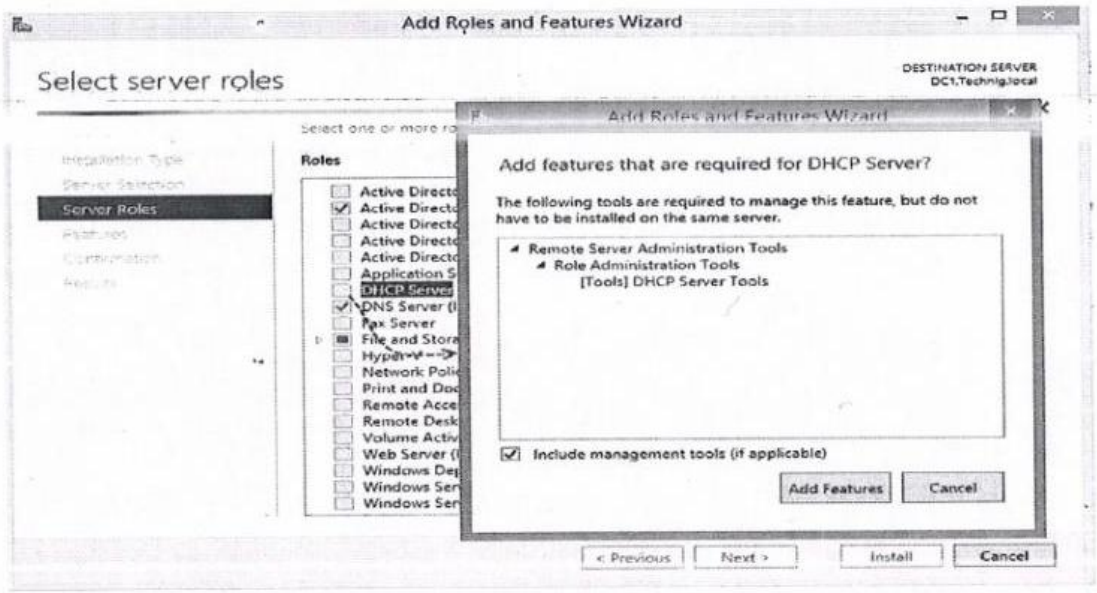
Step 1 : Adding Role of Features:



Step 2: Selection of the server:

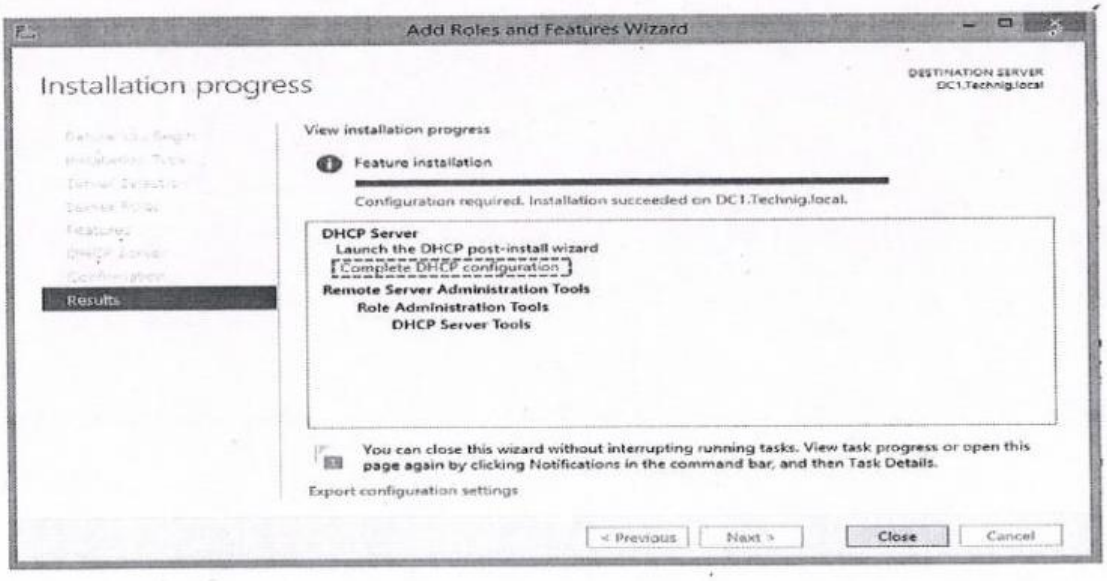


Step 3: Role and feature wizard:

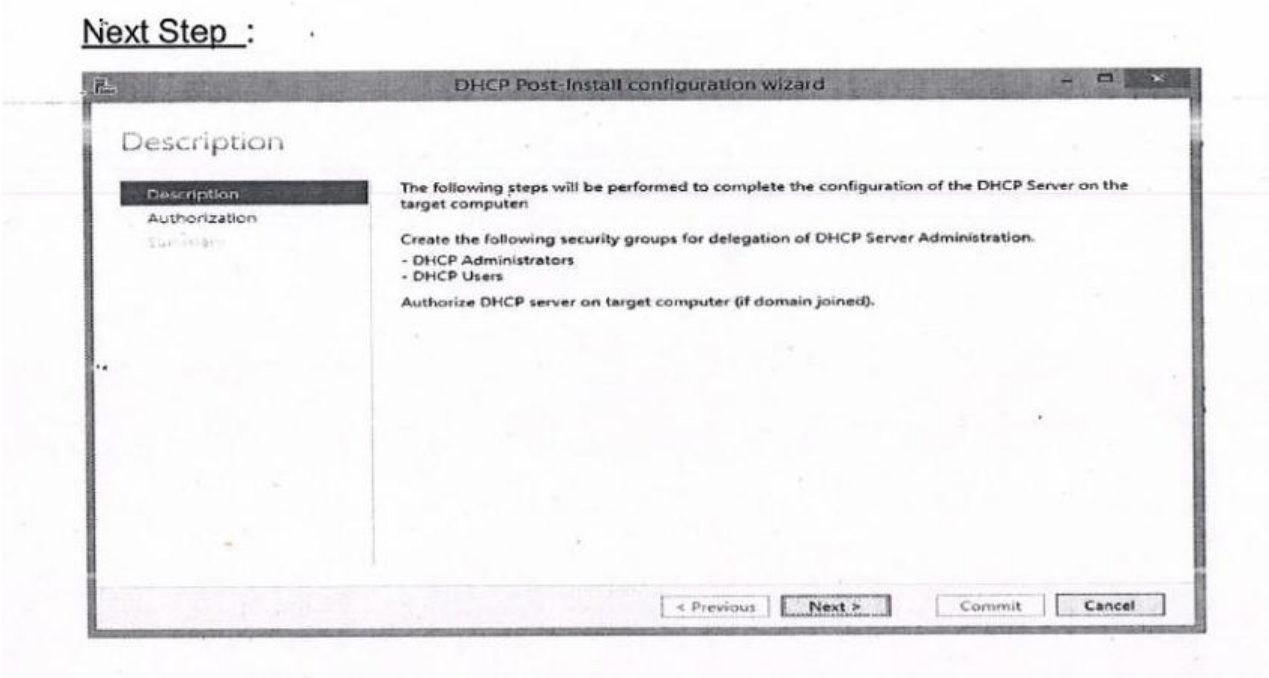


This wizard help to select the Dhcp server from the server pool. Finally on adding the services to services we will proceed for install the services.

Step 4: Feature installation:

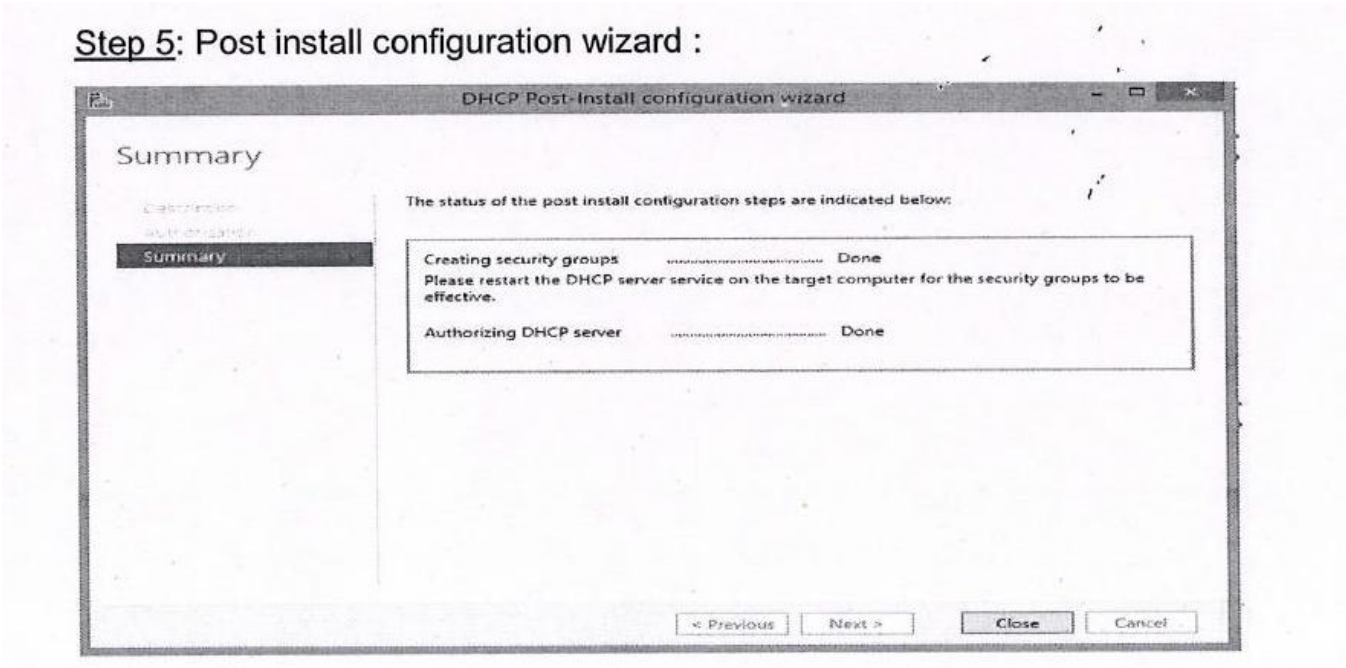


Next Step :

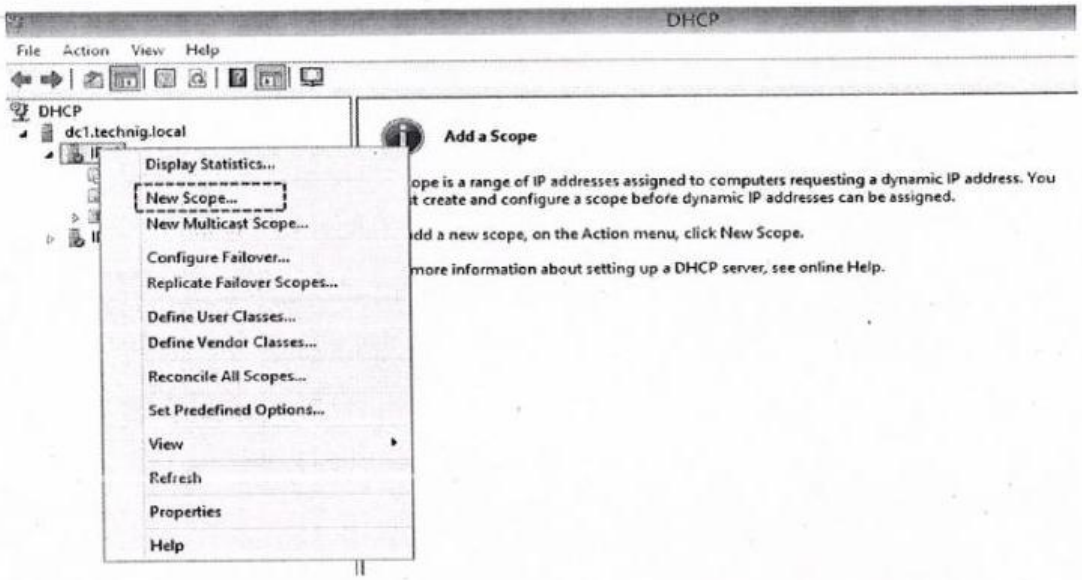


Finally here we install the dhcp services to the window 12 server. Now we are going to create the authorization for this service.

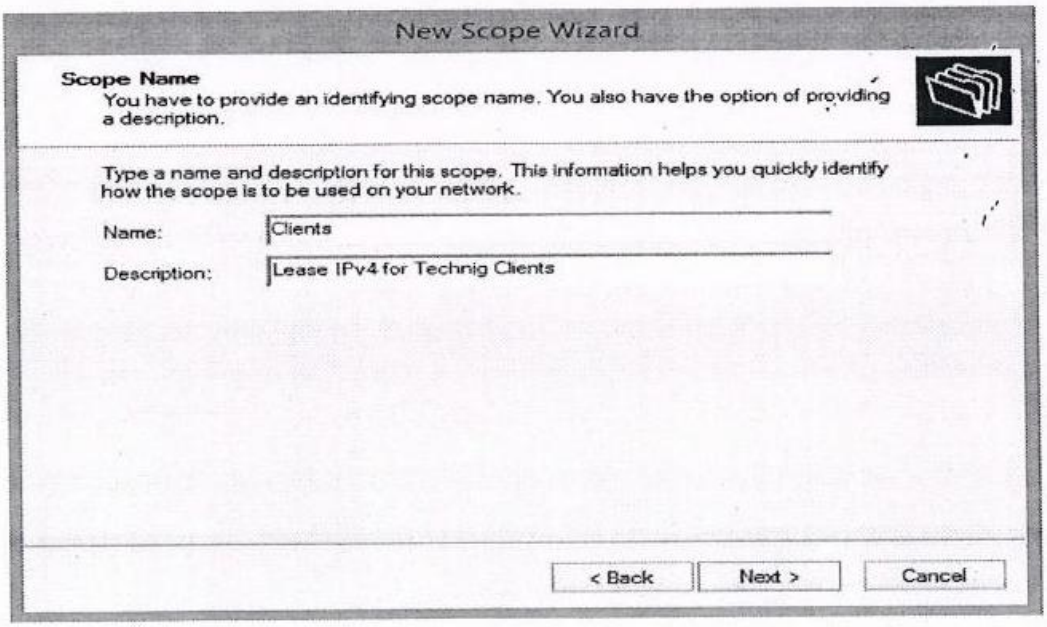
Step 5: Post install configuration wizard :



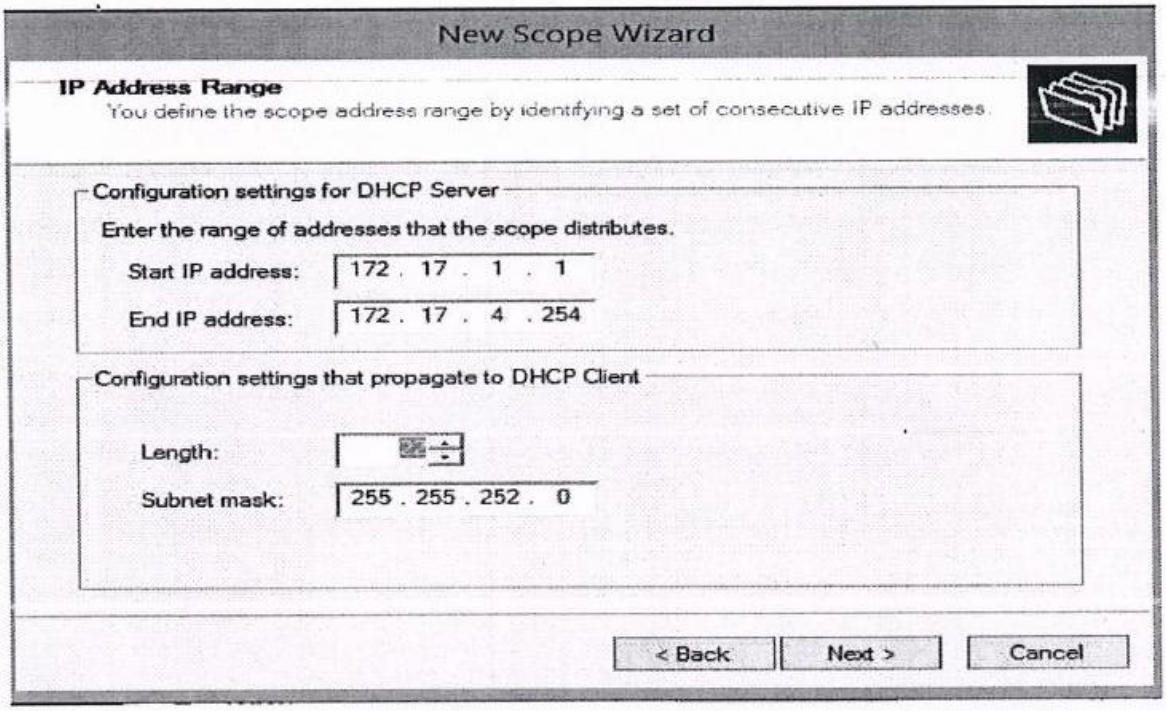
Step 6: Create new scope in the dhcp



Step 7: New Scope Wizard



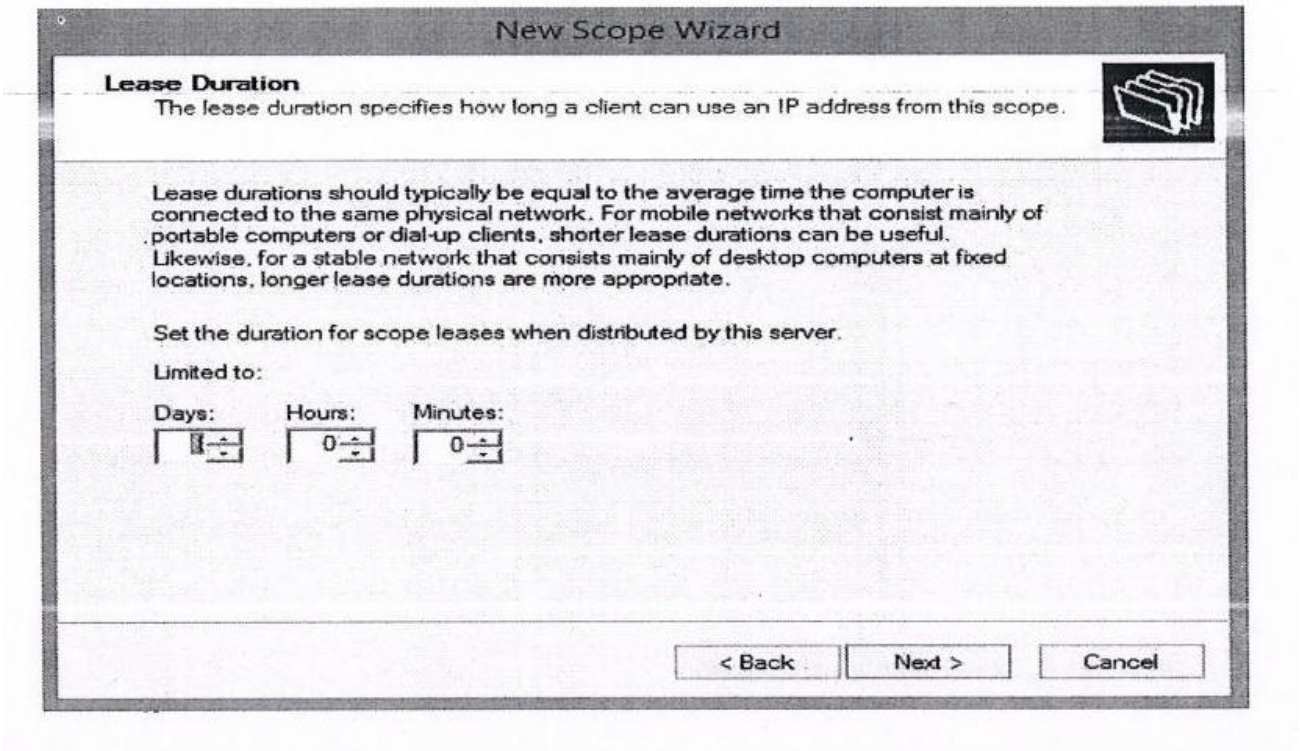
Step 8:Define the Scope



Range :

Assign the start IP address range and the end IP address range. l has set from 172.17.1.1 to 172.17.4.254 which is a class B IP. address . Leave the length 22 by default and click Next.

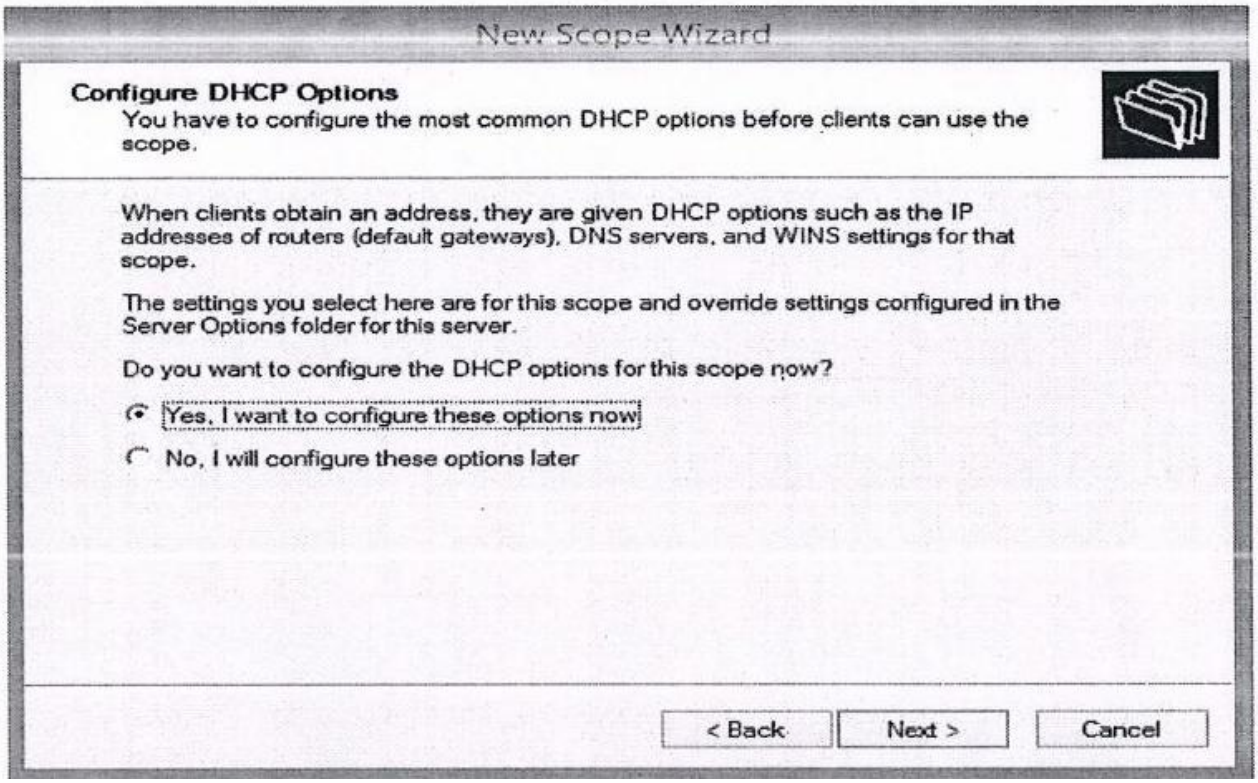
Step 9: Lease time for define Scope



DHCP Lease Duration

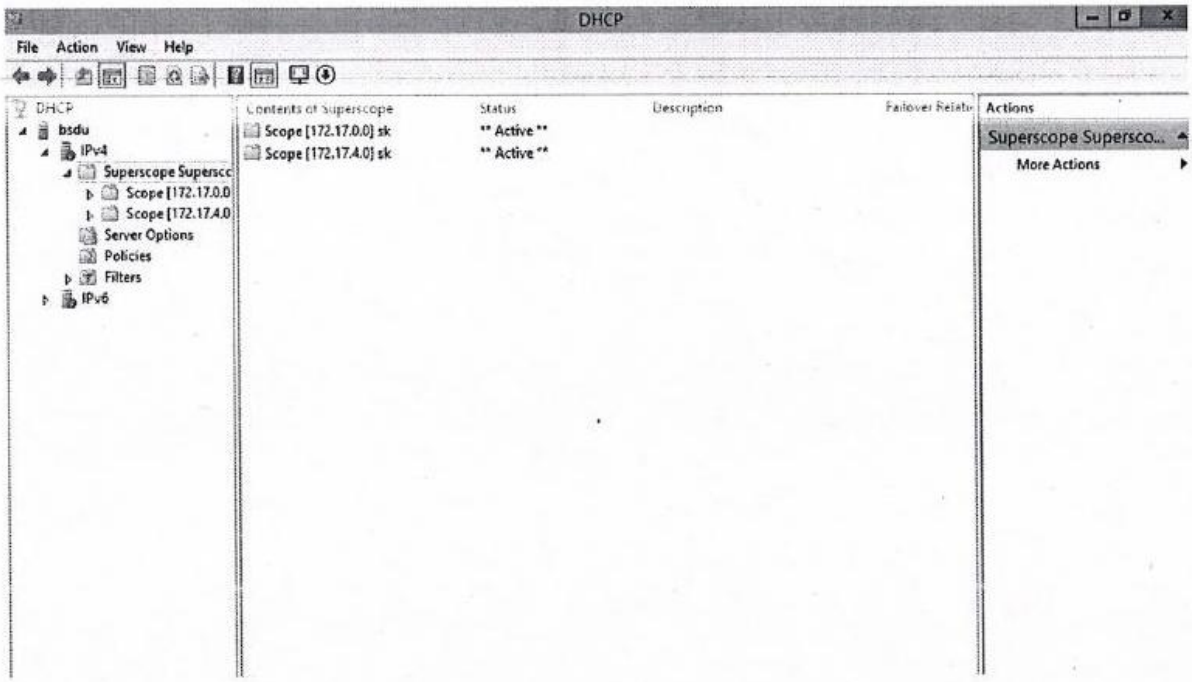
Let the **Lease Duration** by default and click **Next**

Step 10 : Validate the Configuration:



Step 11: Completion of new step wizard:

Step 12: Finally Dhcp is configure for 1000 hosts machine

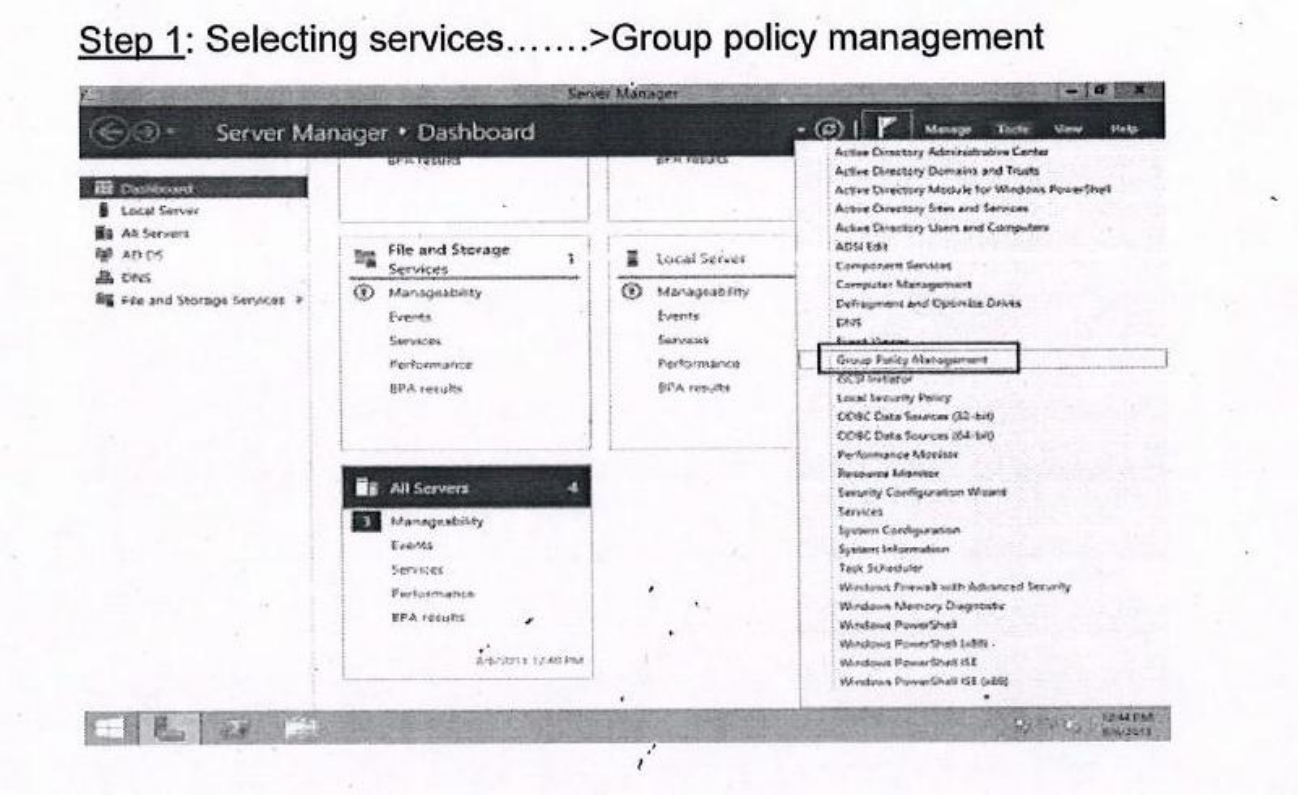


CHAPTER 2:

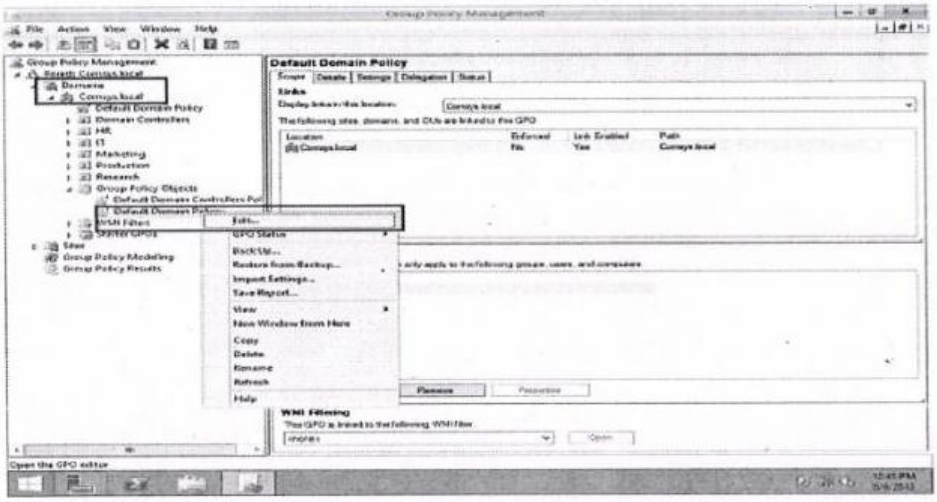
Group policy:

While configuring the group policy we can implement the single feature to number of host with common services. Here right now, we going to implement the common desktop to the system in the network.
Apart from implementing the common desktop we are also going to implement the antivirus with monitoring on all client machine to the network.

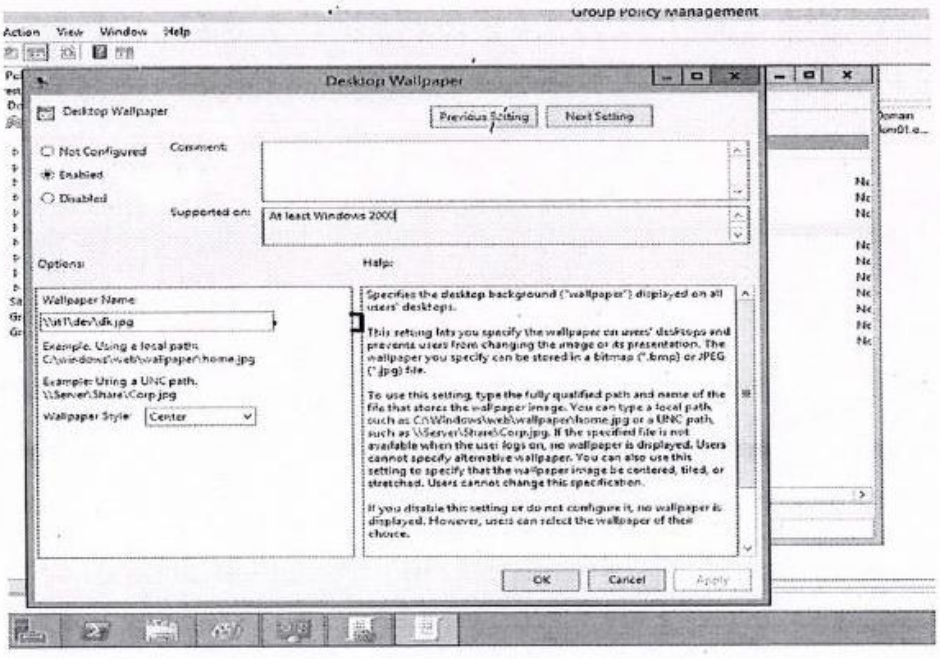
Step 1: Selecting sen/ices ....>Group policy management



Step 2: selecting the server and particular organization unit



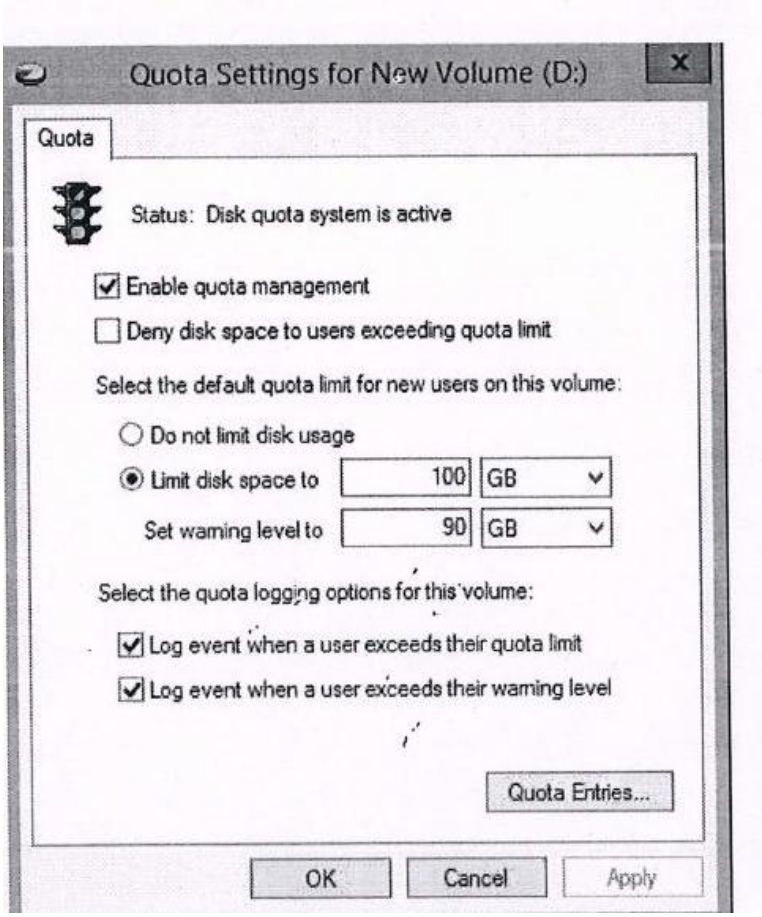
Step 3: Selecting the particular wallpaper for all the clients



Chapter: 3

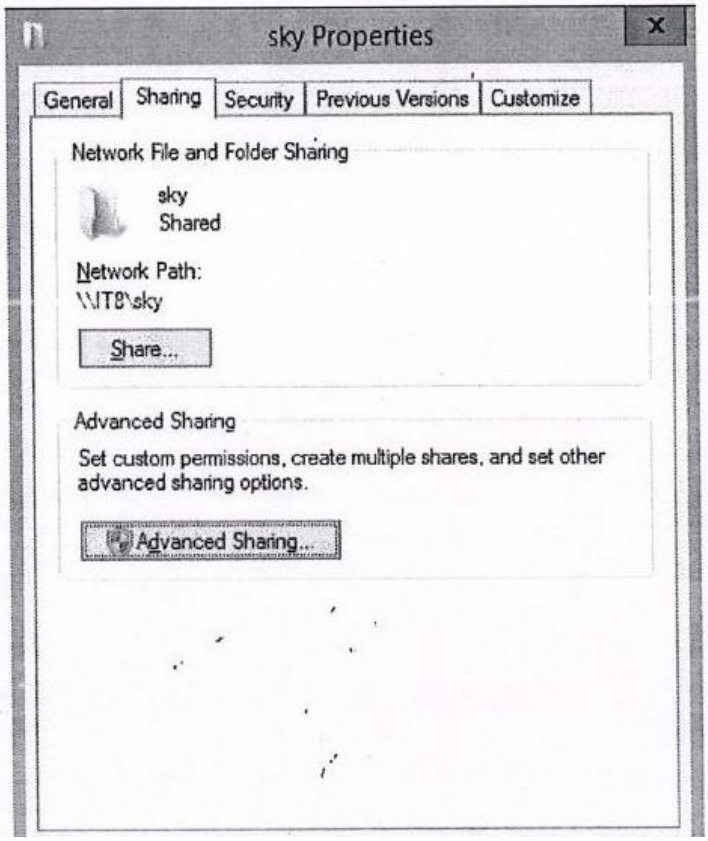
Disk Quota:

With disk quota we can set the disk size for particular user in the network
Even we share the common disk in the network and every user can use it
Step 1: Right click on drive .... ..> Properties... >quota

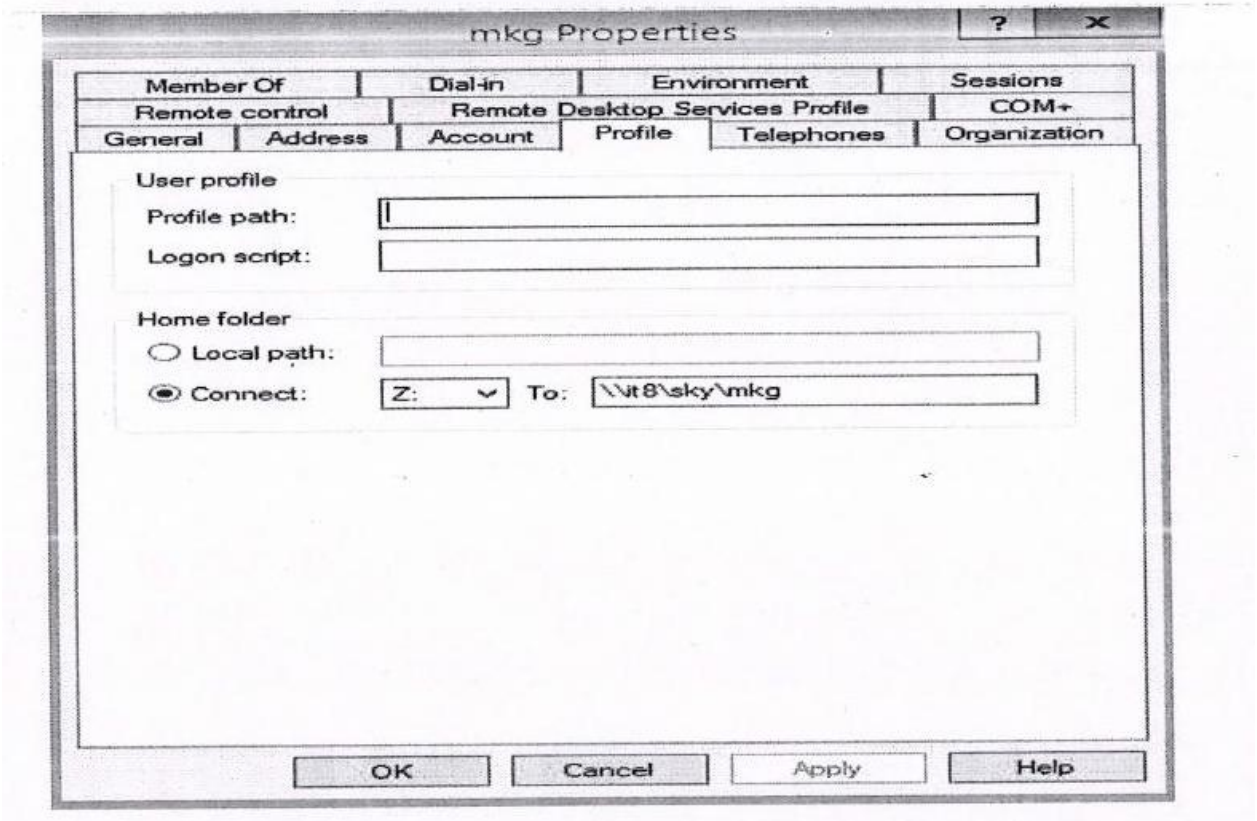


`

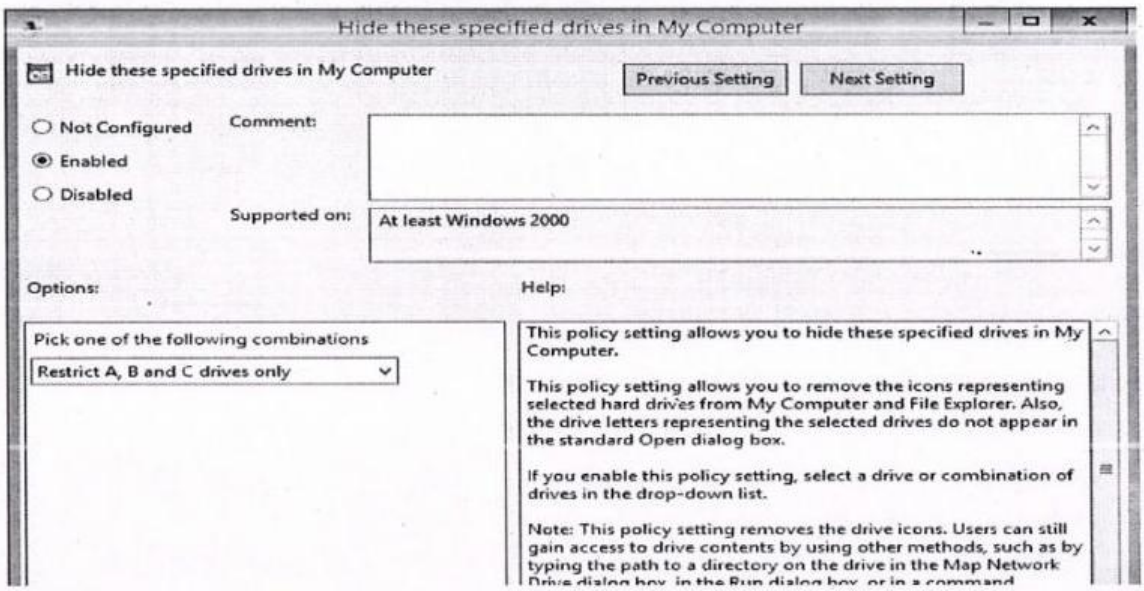
Step 2: Creating sky folder in D drive and advance sharing



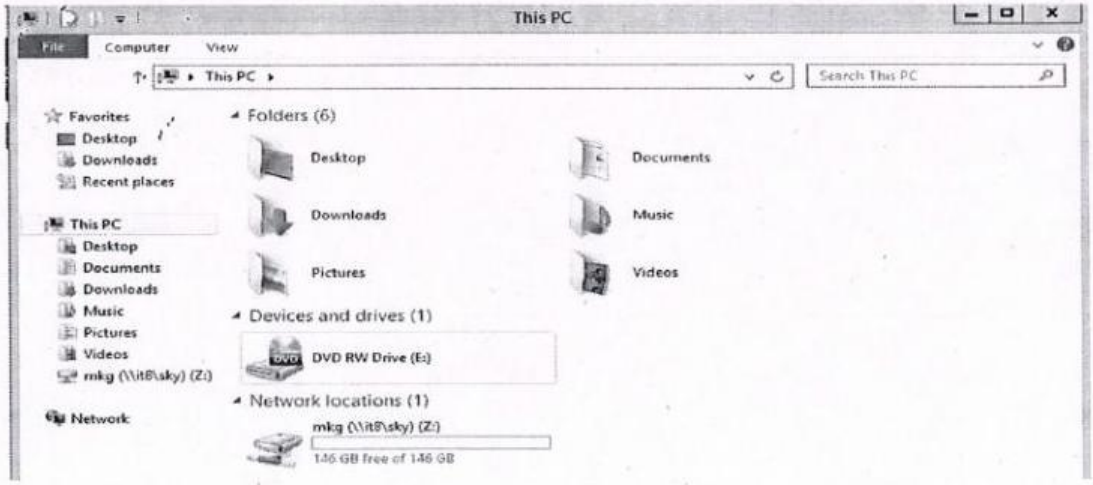
Step 3: Giving the UNC path and assigning the drive letter to the share drive.



Step 4: With group policy hide all the drive except share drive in the network



Step 5: Showing only the shared drive in the network and all the other drives are hidden.



CHAPTER 4:

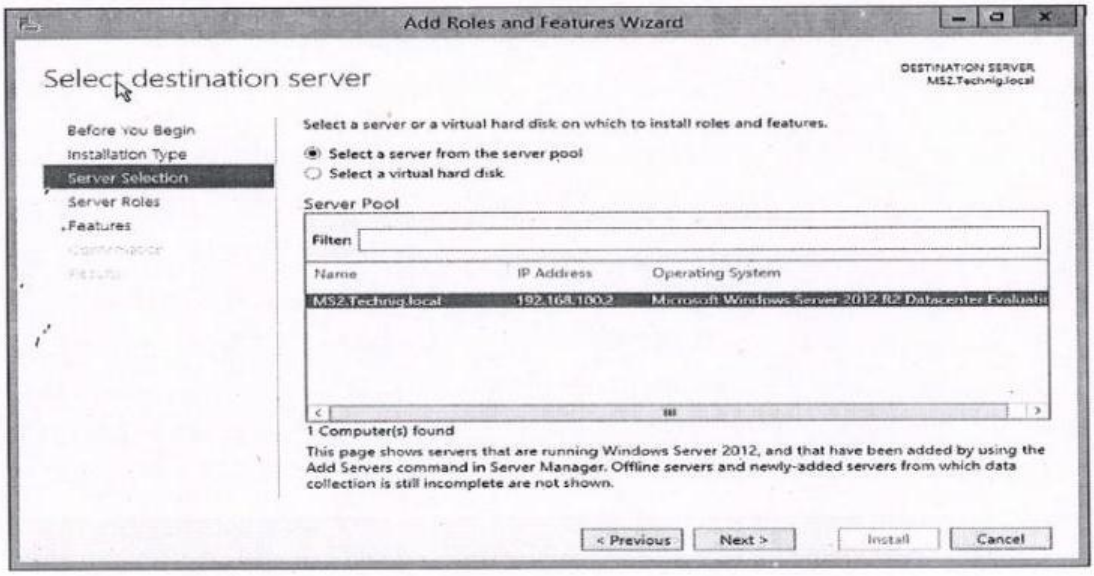
WDS (Window deployment service)

WDS Prerequisites

- The Windows Deployment Services server must be a member of an Active Directory Domain Services (AD DS) domain or a domain controller. '-
- The Domain Name System (DNS) server on the network before you can run Windows Deployment Services. DNS will install with Active directory domain services. , .
- For deploying lP address you must have a Dynamic Host Configuration Protocol (DHCP) server with an active scope on the network because Windows Deployment Services uses PXE, which relies on DHCP for IP addressing the clients that want to install OS remotely. ‘ for DHCP Server.
- You must have the appropriate credential to install role. It means you must be the member of local admin or domain admin. The hard disk volume must be NTFS.

In Windows Server, sign in to the server as a domain admin and open the Server Manager if it's not will start automatically.

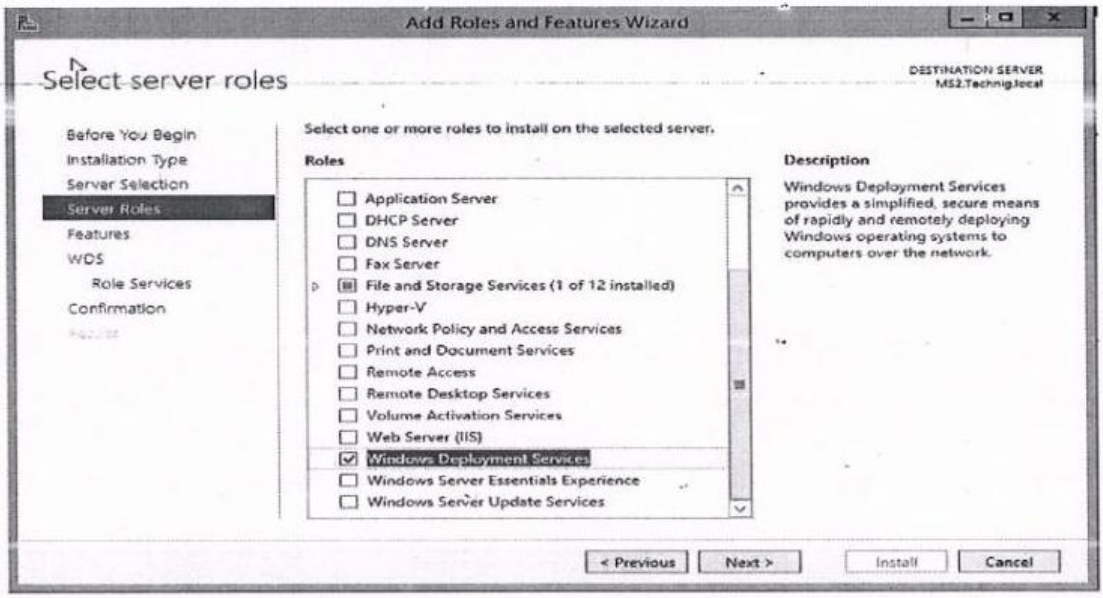
Step 2: Selection of the server



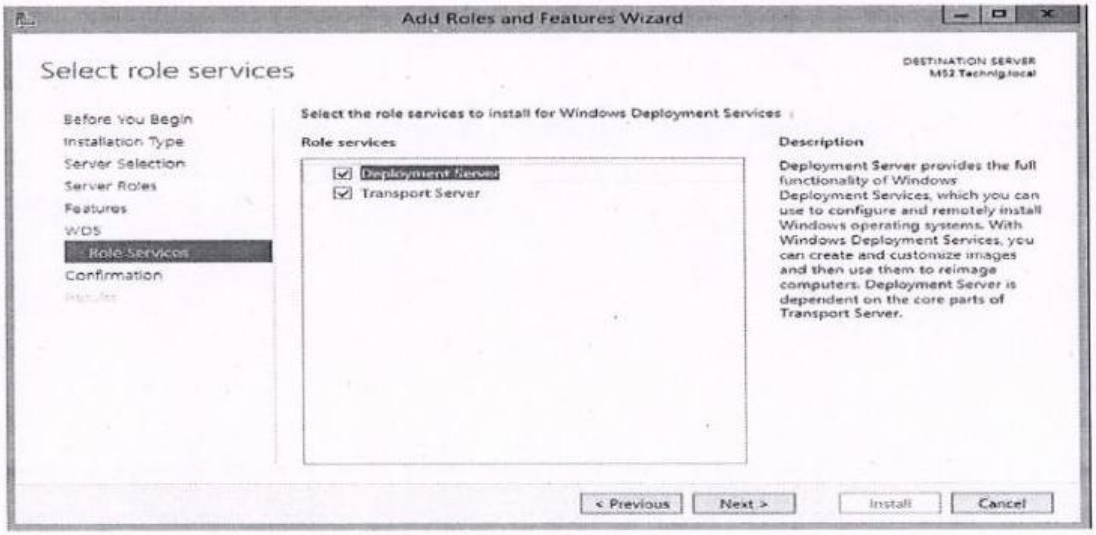
Step 3: Adding features to window deployment services

On the Select server roles page, scroll down and then select Windows Deployment Servicescheck box. in the Add feature that are required for Windows Deployment Services

Step 4: Selection of window deployment service

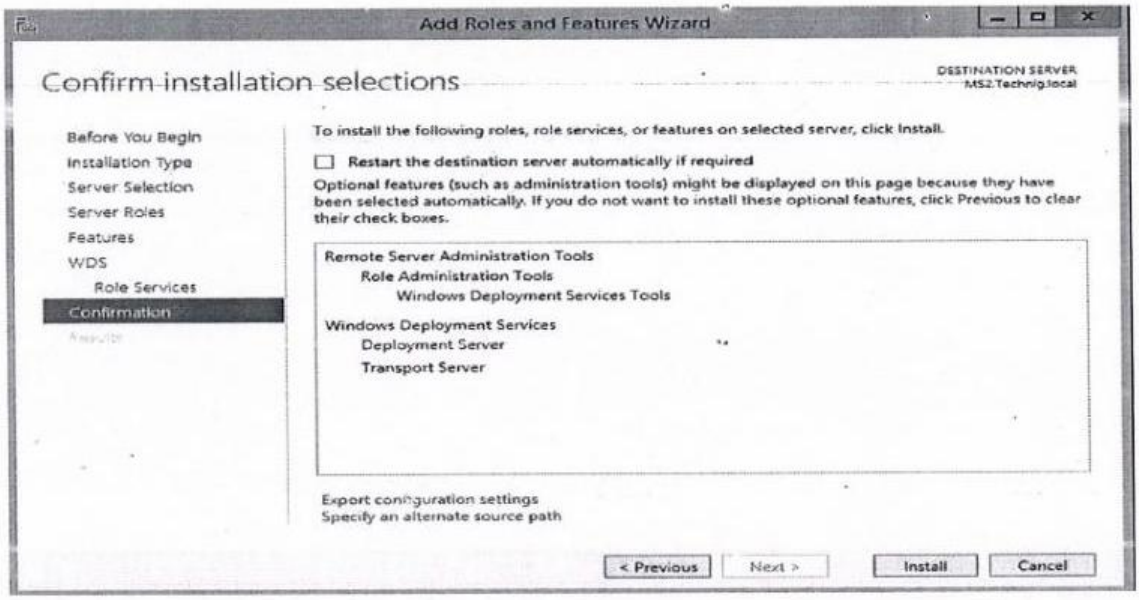


Step 5: Select the deployment server and transport server

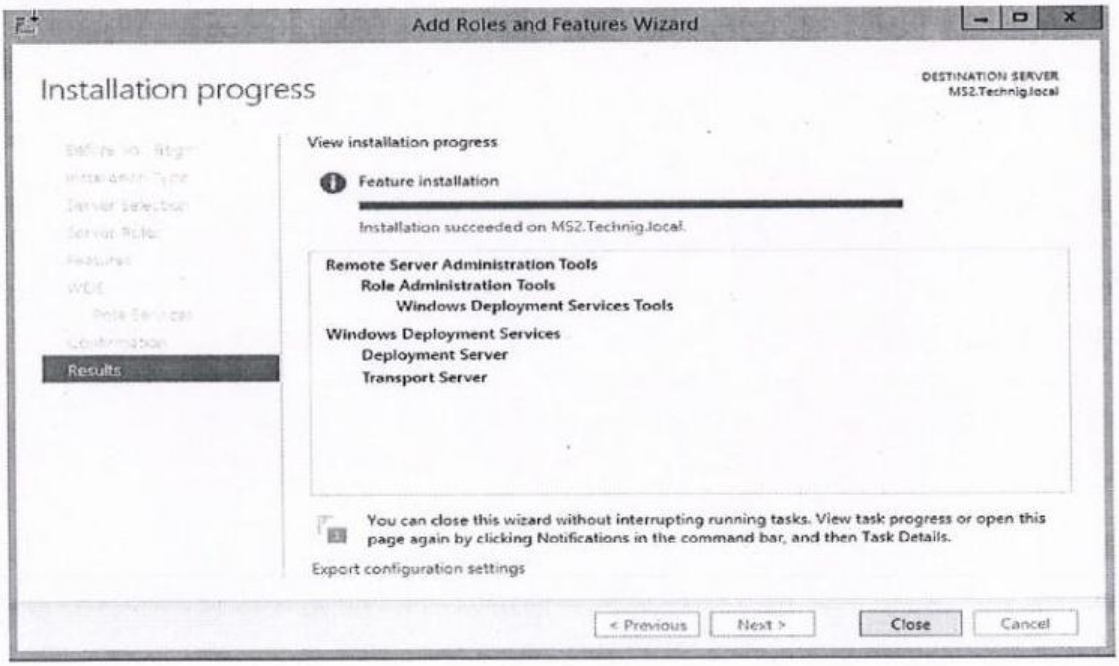


Deployment Server and Transport Server

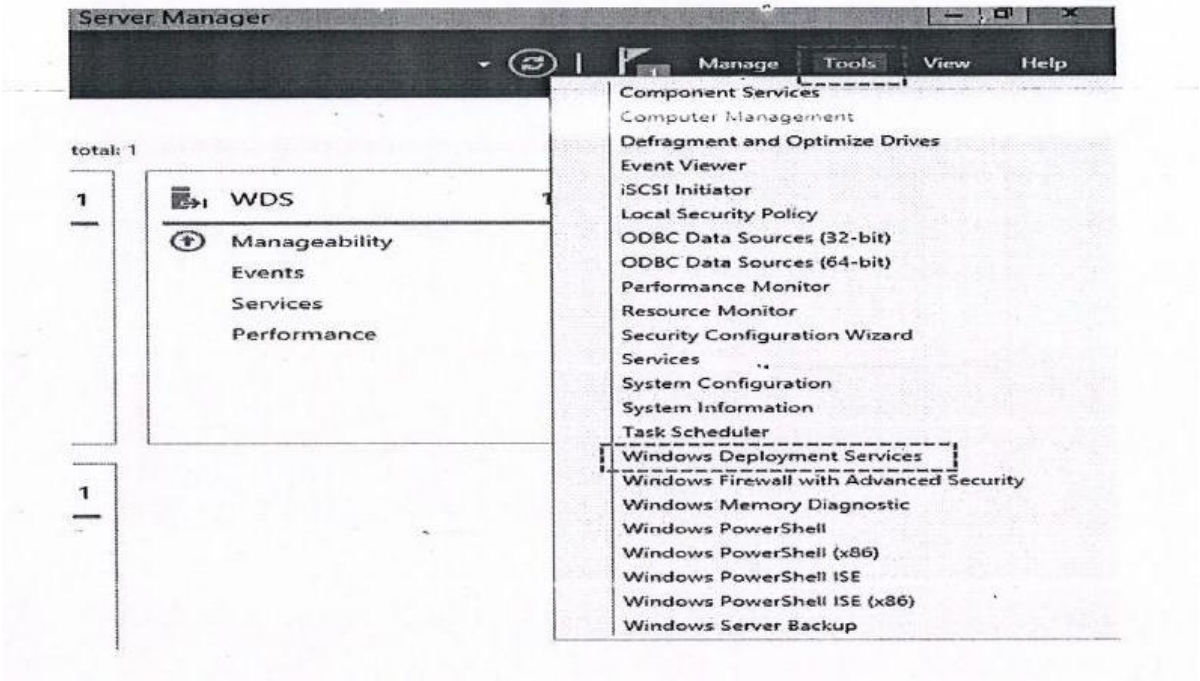
Step 6: Validating the services and going for restart



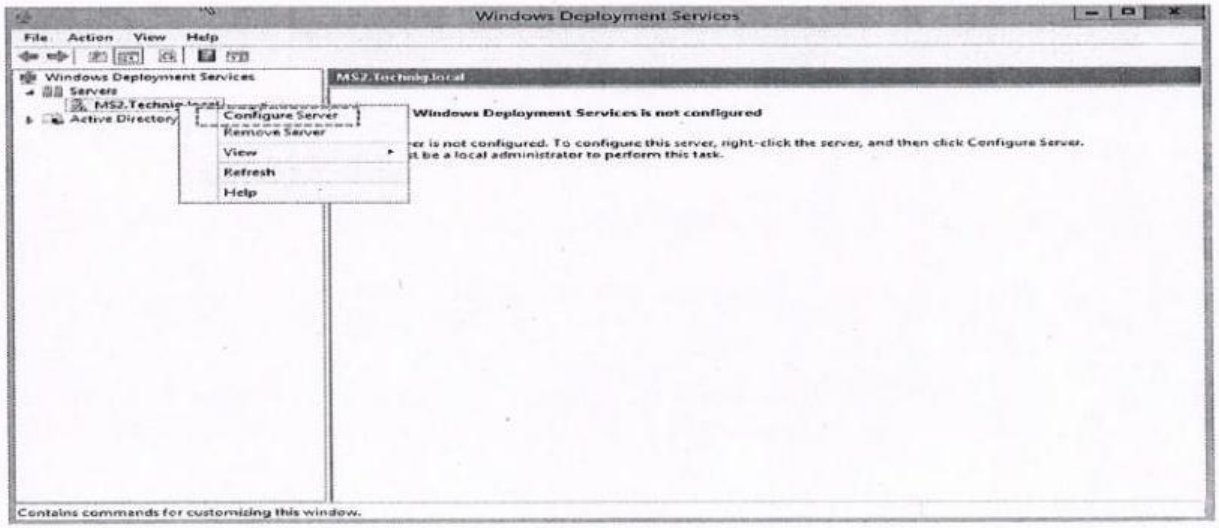
Step 7: Completion of the feature installation



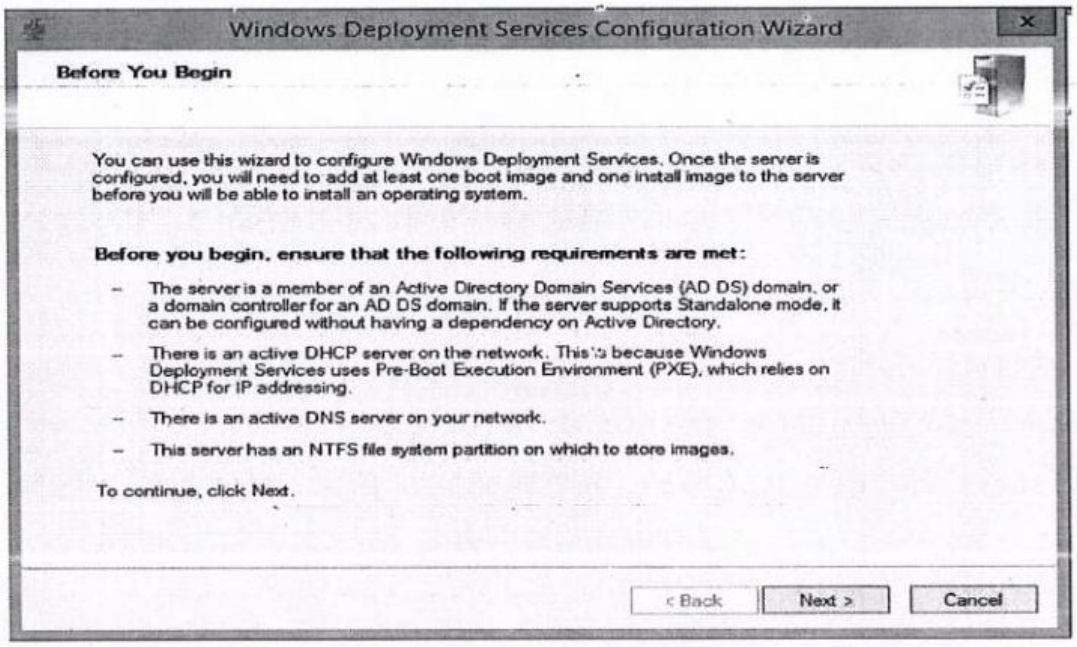
Step 8: Tools……..>select Window deployment service



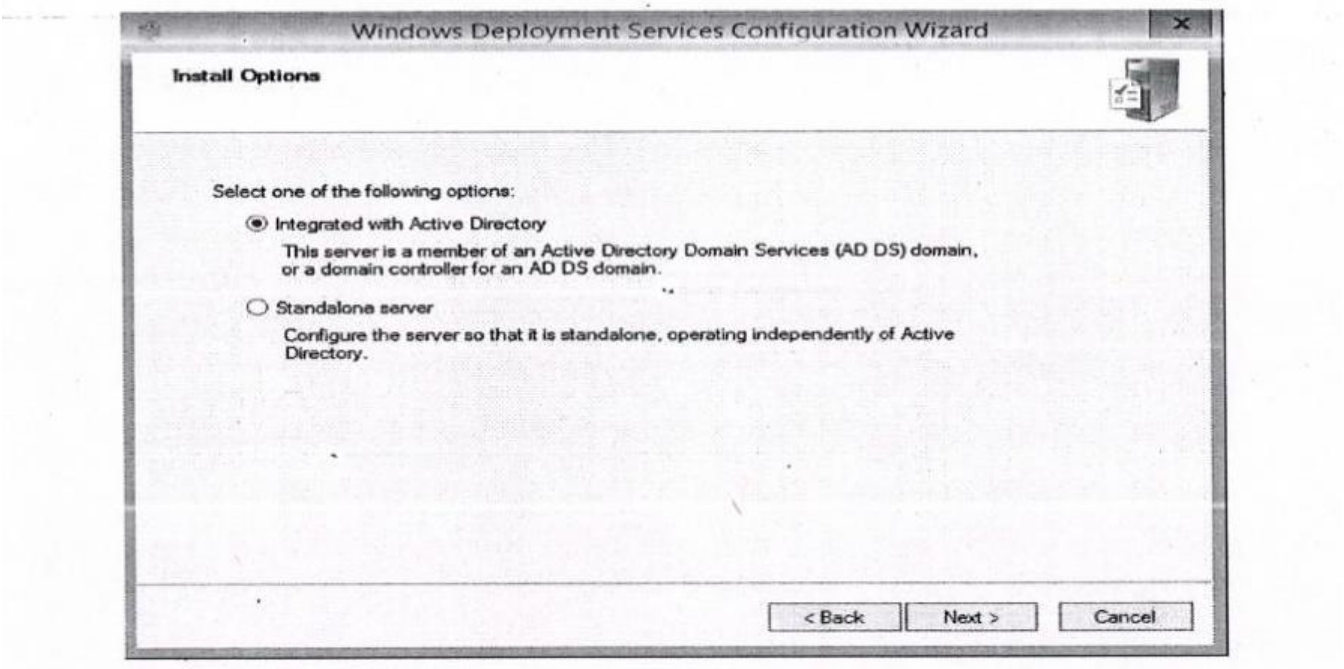
Step 9: Configure the server



Step 10: Windows Deployment Services Configuration Wizard



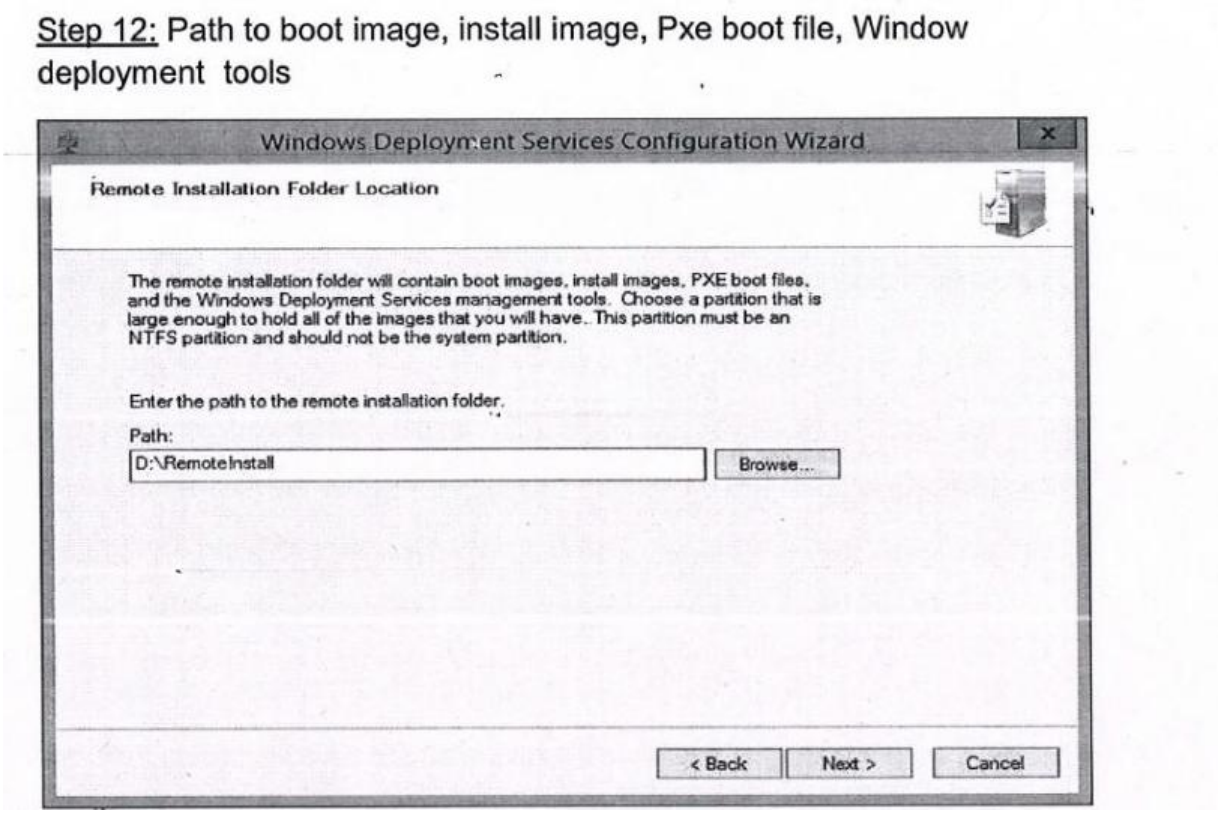
Step 11:.Window Deployment services configuration wizard



WDS Install Options

On the Remote Installation Folder Location, select the location where you want to '**keep all Windows images and configuration files and then click Next.**

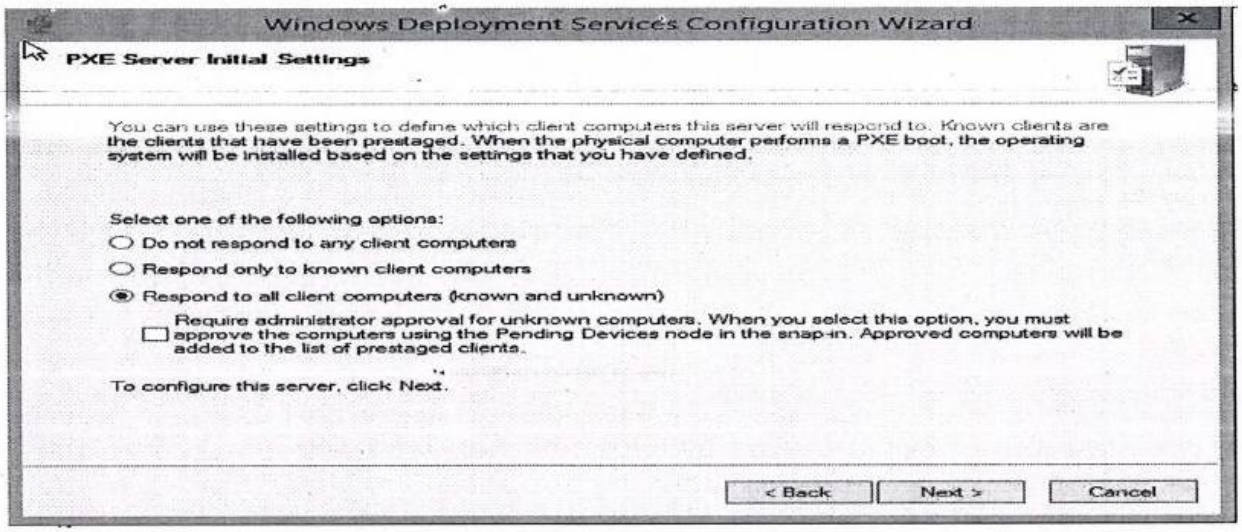
Step 12: Path to boot image, install image, Pxe boot file, Window deployment tools



Remote Installation Folder Location — Install and Configure WDS

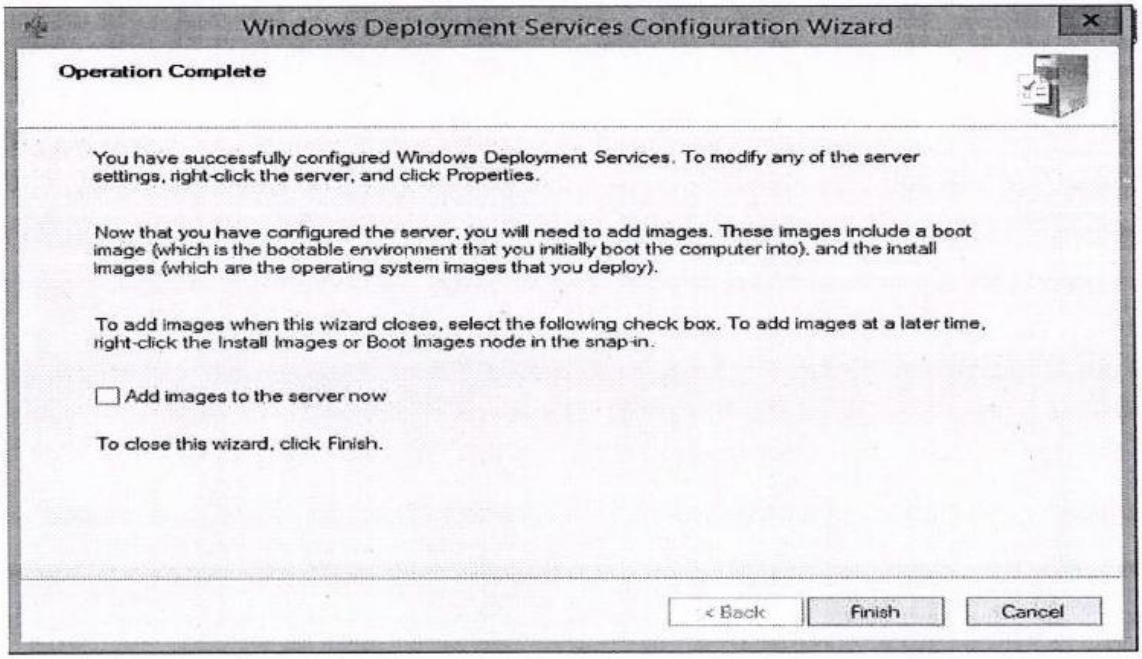
On the PXE Server Initial Settings page select Respond to all client computers (Known and unknown) and click Next. Remember, we are in the test area so in the real network environment select whatever you want

Step 13:.Pxe server and its setting

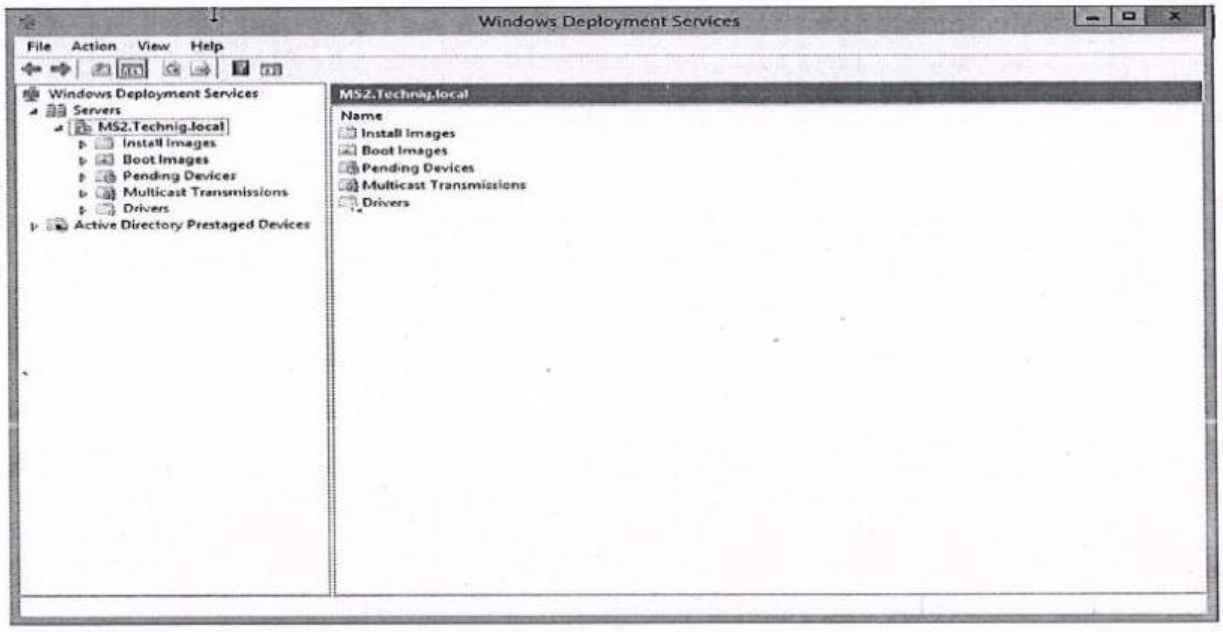


The sever will start and complete the configuration. On the **Operation Complete** page unchecked the **Add image to server now** and then click **Finish**

Step 14: Deployment of wds

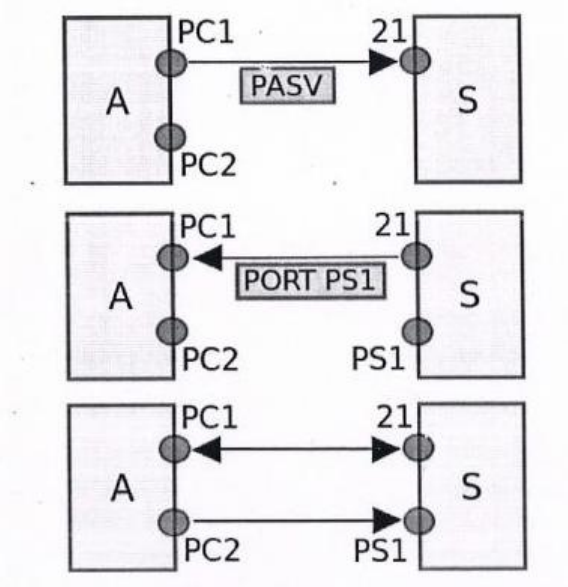


Step 15: Window Deployment services wizard



CHAPTHER 5:

FTP : (file transfer protocol) :



FTP may run in active or passive mode, which determines how the data connection is established. In both cases, the client creates a TCP control connection from a random, usually an unprivileged, port N to the FTP server command port 21.

ln active mode, the client starts listening for incoming data connections from the server on port M. It sends the FTP command PORT M to inform

For text files, different format control and record structure options are provided. These features were designed to facilitate files containing Telnet or ASA.

Data transfer can be done in any of three modes:

- Stream mode: Data is sent as a continuous stream, relieving FTP from doing any processing. Rather, all processing is left up to TCP. No End- of-file indicator is needed, unless the data is divided into records.
- Block mode: FTP breaks the data into several blocks (block header, byte count, and data field) and then passes it on to TCP.
- Compressed mode: Data is compressed using a simple algorithm (usually run-length encoding). _

Some FTP software also implements a DEFLATE-based compressed mode, sometimes called "Mode Z" after the command that enables it. This mode was described in an Internet Draft, but not standardized.

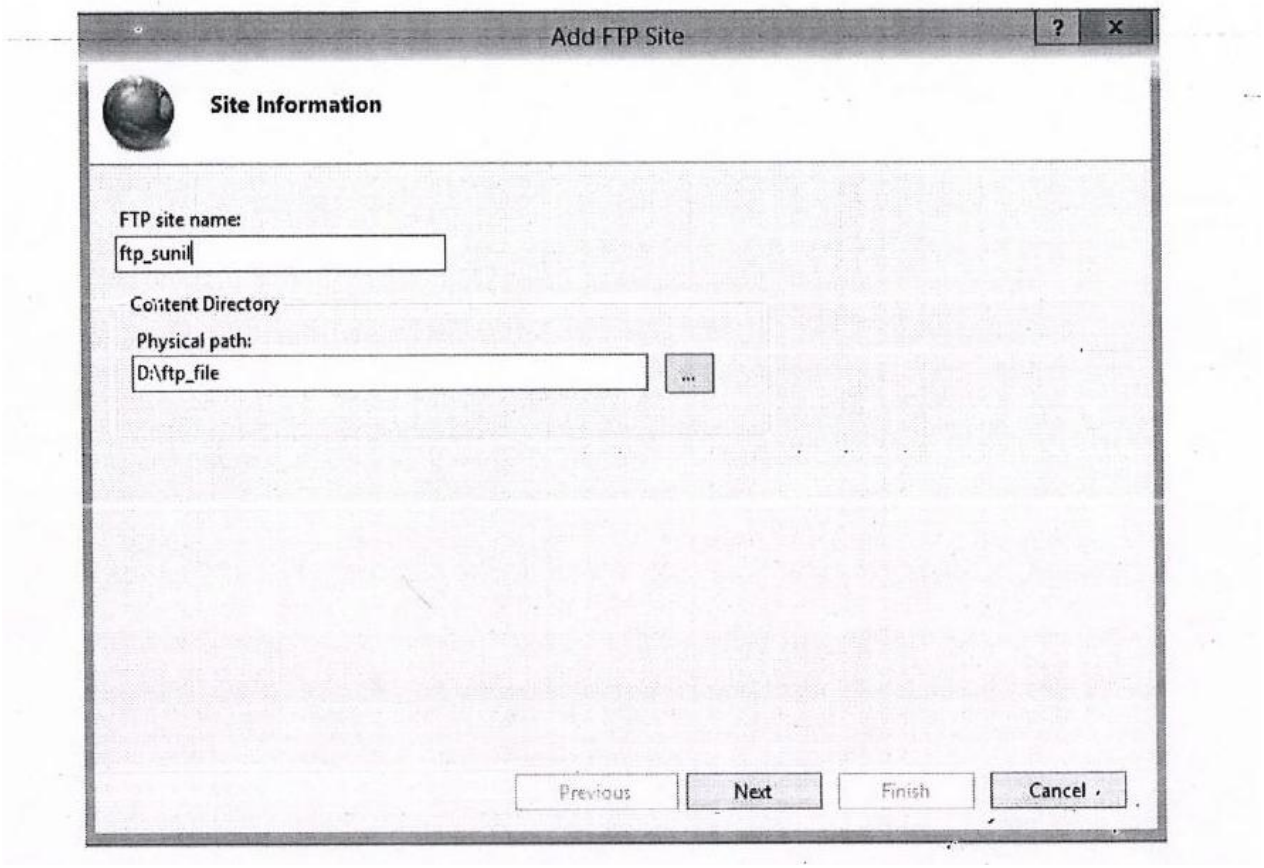
Login:

FTP login uses normal username and password scheme for granting access. The username is sent to the server using the USER command, and the password is sent using the PASS command. This sequence is unencrypted "on the wire“, so may be vulnerable to a network sniffing attack. lf the information provided by the client is accepted by the server, the server will send a greeting to the client and the session will commence. lf the server supports it, users may log in without providing login credentials, but the same server may authorize only limited access for such sessions.

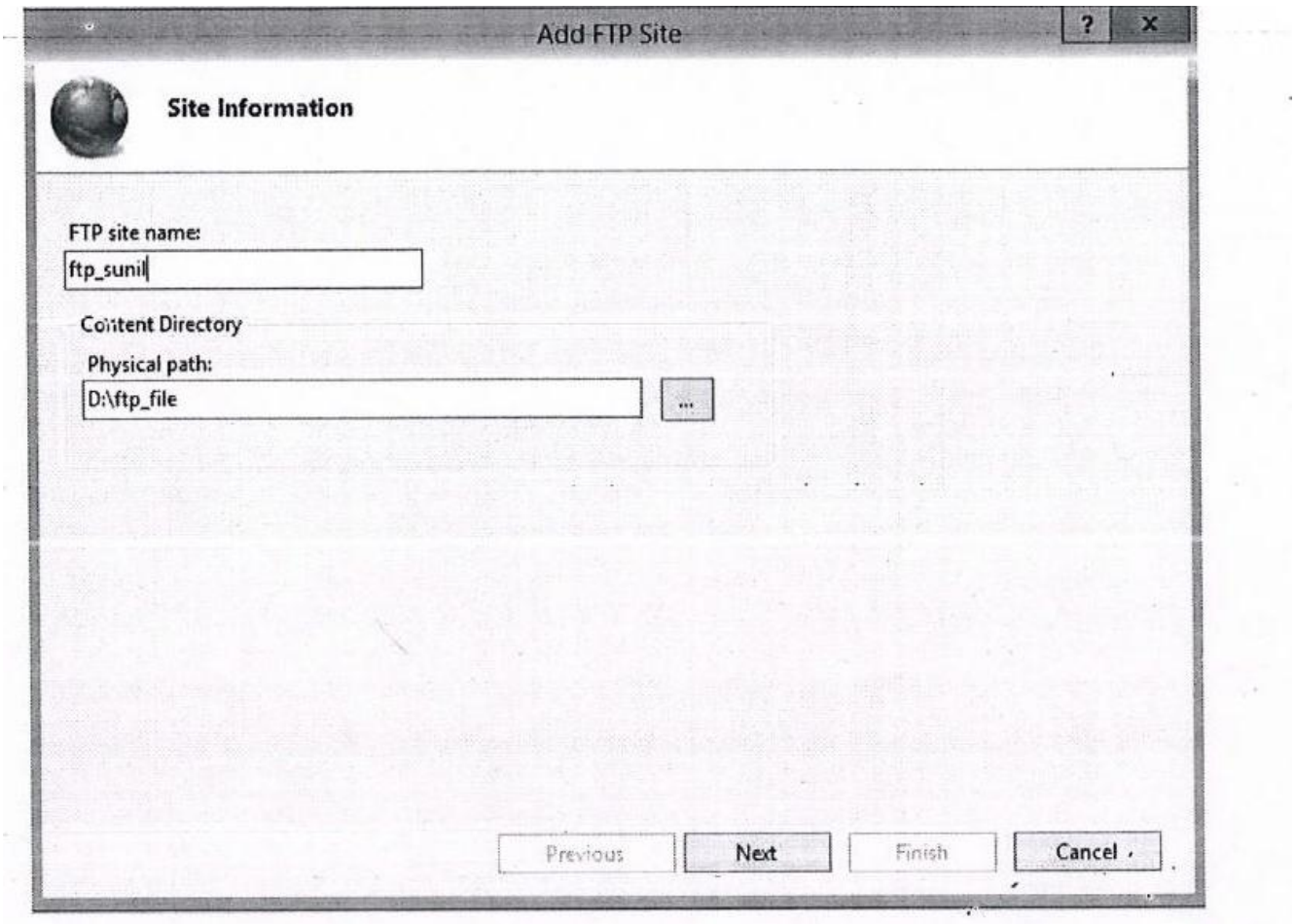
Anonymous FTP

A host that provides an FTP service may provide anonymous_FTP ' access. Users typically log into the service with an 'anonymous ‘(lower-case and case-sensitive in some FTP servers) account when prompted for username. Although users are commonly asked to send their data packet

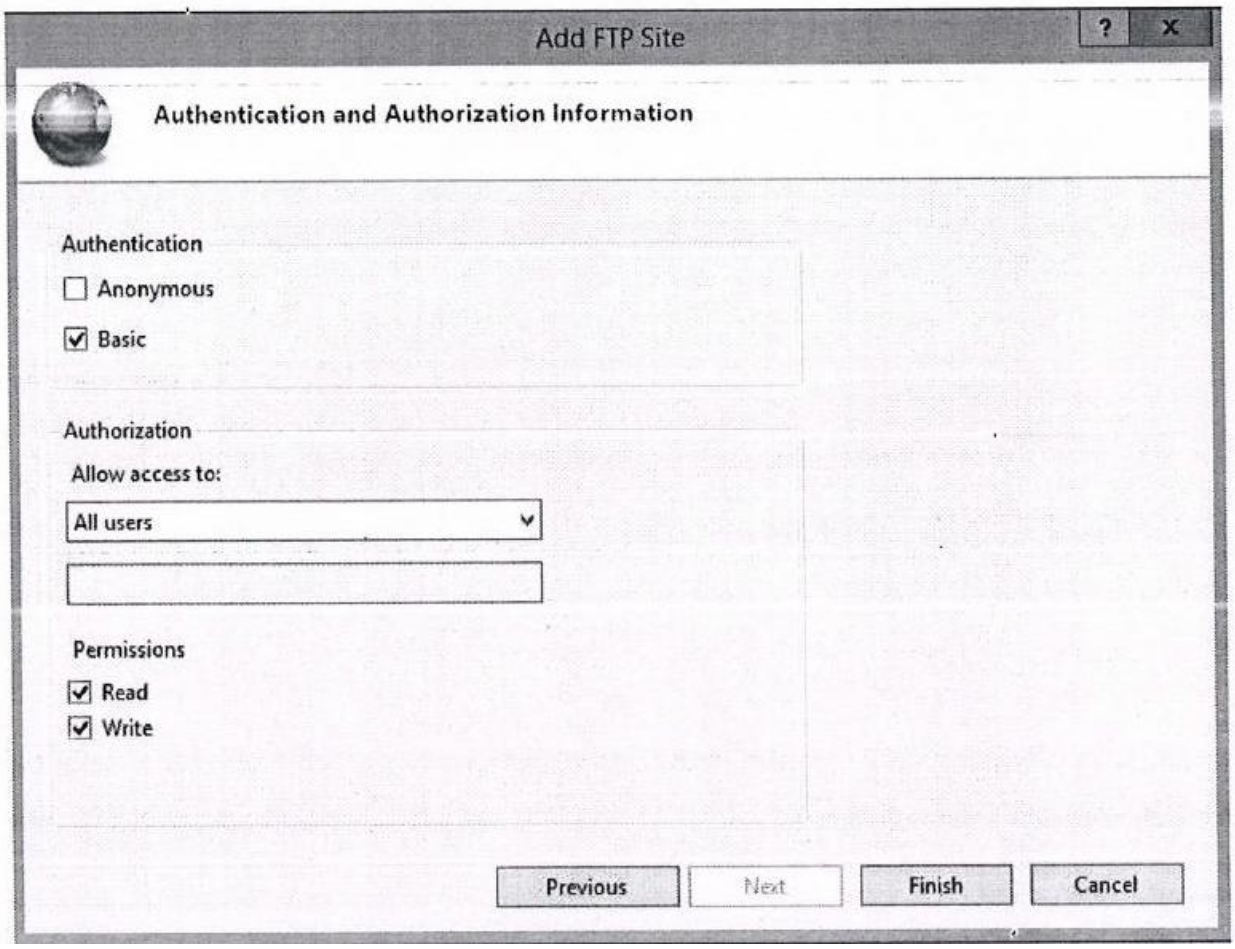
Steg 1: After the installation of the Ftp service from the server manager



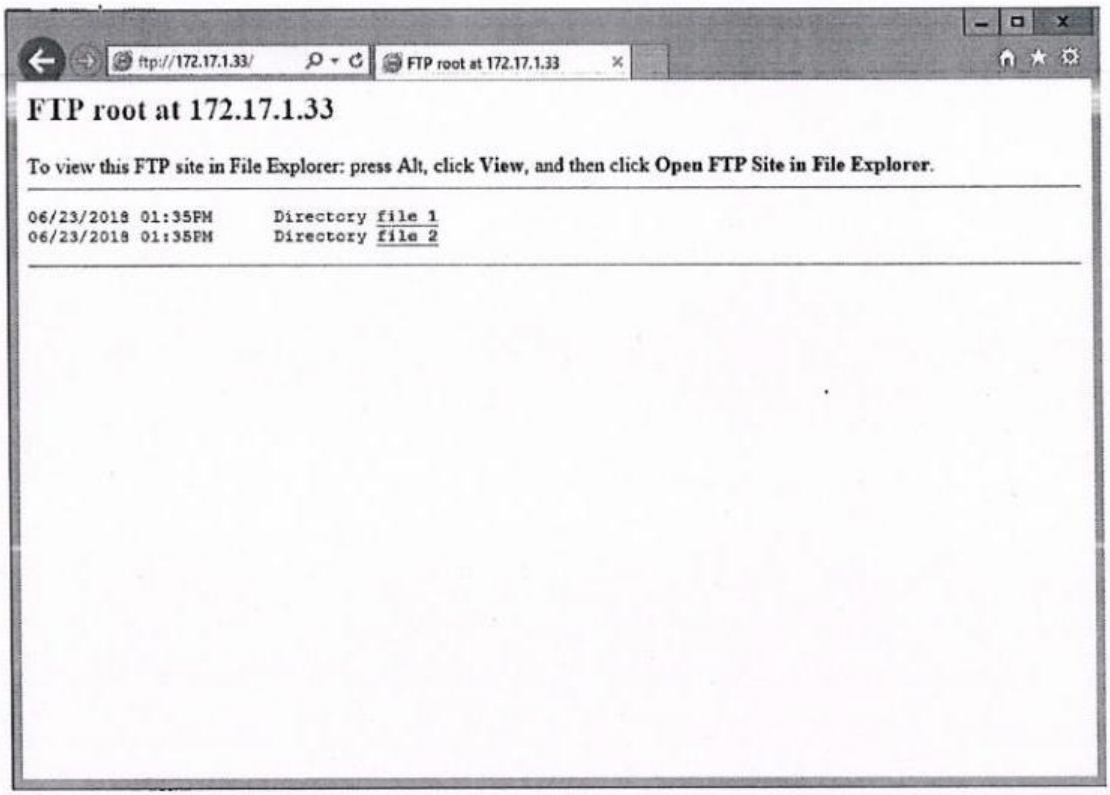
Step 2: Adding of the IP Address.



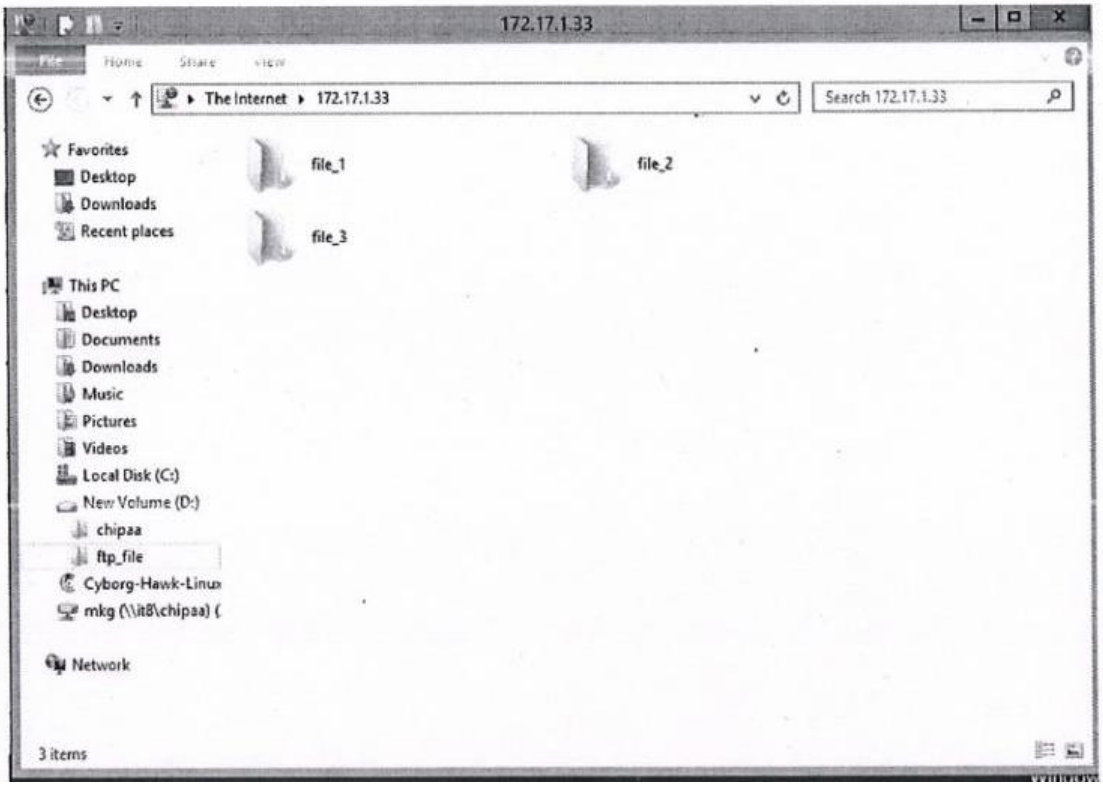
Step 3: Authentication for the particular users



Downloading: Download data using ftp on client machine



Uploading:`When the user is interested in uploading data to site using ftp on server machine



CHAPTER 6:

HTTP (Hypertext transfer protocol) :

HTTP is a Stateless Protocol
HTTP is called a stateless protocol because each command is executed independently, without any knowledge of the commands that came before it. This is the main reason that it is difficult to implement Web sites that react intelligently to user input. This shortcoming of HTTP is being addressed in a number of new technologies,
including ActiveX, Java, JavaScript and cookies.

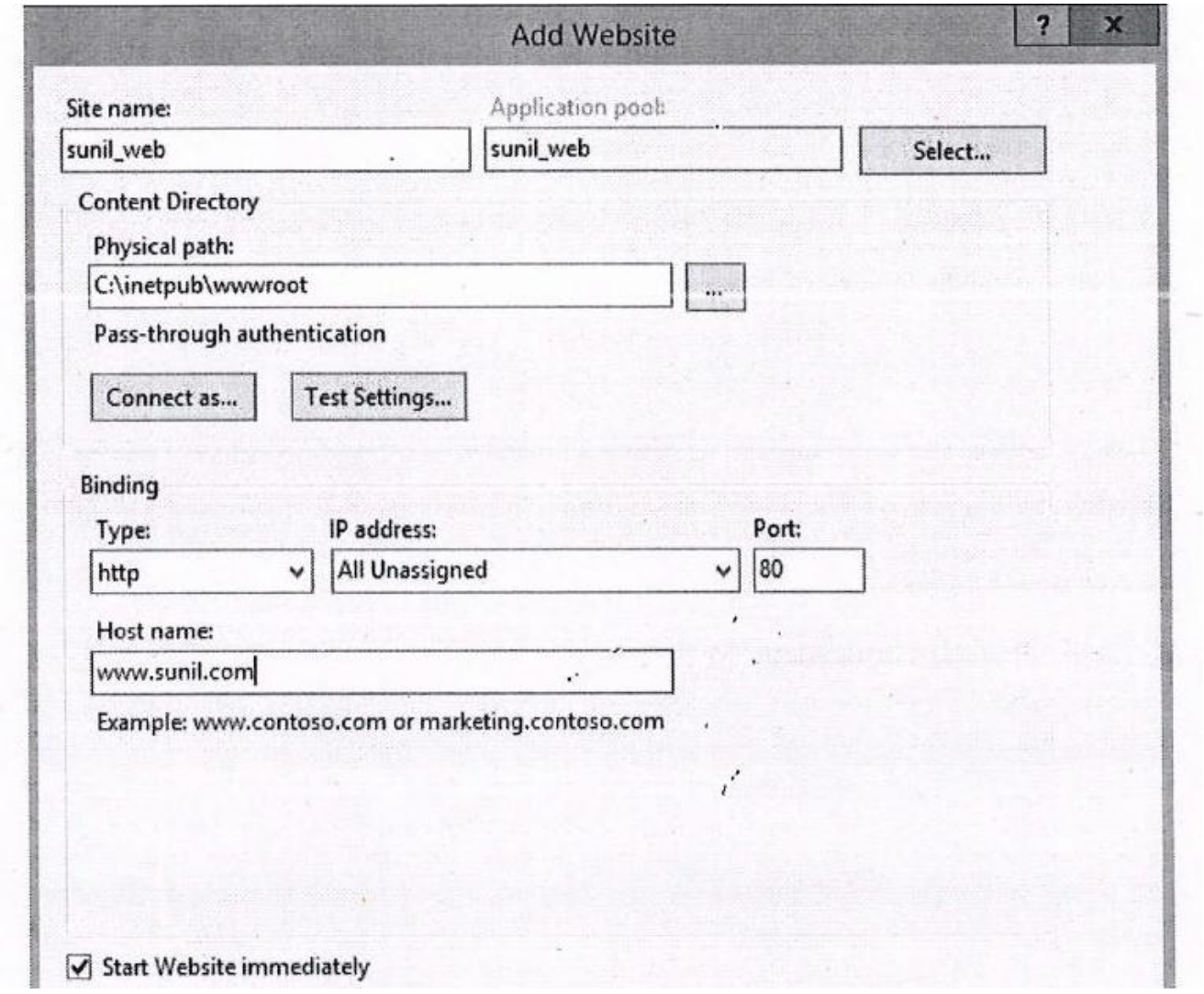
Difference between ftp and http:

HTTP essentially fixes the bugs in FTP that made it inconvenient to use for many small ephemeral transfers as are typical in web pages. FTP has a stately control connection which maintains a current working directory and other flags, and each transfer requires a secondary connection through which the data are transferred. In "passive" mode this secondary connection is from client to server, whereas in the default "active" mode this connection is from server to client. This apparent role reversal when in active mode, and random port numbers for all transfers, is why firewalls and NAT gateways have such a hard time with FTP. HTTP is stateless and multiplexes control and data over 5| single connection from client to server on well-known port numbers, which trivially passes through
NAT gateways and is simple for firewalls to manage.

Setting up an FTP control connection is quite slow due to the round-trip delays of sending all of the required commands and awaiting responses, so it is customary to bring up a control connection and hold it open for multiple file transfers rather than drop and re-establish the session afresh each time. In contrast, HTTP originally dropped the connection after each transfer because doing so was so cheap. While HTTP has subsequently gained the ability to reuse the TCP connection for multiple transfers, the conceptual model is still of independent requests rather than a session.

When FTP is transferring over the data connection, the control connection is idle. If the transfer takes too long, the firewall or NAT may decide that the control connection is dead and stop tracking it, effectively breaking the connection and confusing the download. The single HTTP connection is only idle between requests and it is normal and expected for such connections to be dropped after a time-out.

Way to host website with http using port no. 80



CHAPTER 7:

RAID

RAID is a technology that is used to increase the performance and/or reliability of data storage. The abbreviation stands for Redundant, Array of Inexpensive Disks. A RAID system consists of two or more drives working in parallel. These disks can be hard discs, but there is a trend to also use the technology for SSD (solid state drives). There are different RAID levels, each optimized for a specific situation. These are not standardized by anindustry group or standardization committee. This explains why companies sometimes come up with their own unique numbers and implementations. This article covers the following RAID levels:

RAID 0 — striping
RAID 1 — mirroring I
RAID 5 — striping with parity ' ’
RAID 6 — striping with double parity
RAID 10 — combining mirroring and striping

The software to perform the RAID-functionality and control the drives can either be located on a separate controller card (a hardware RAID controller) or it can simply be a driver. Some versions of Windows, such as Windows Server 2012 as well as Mac OS X, include software RAID functionality. Hardware RAID controllers cost more than pure software, but they also offer better performance, especially with RAID 5 and 6.
RAID-systems can be used with a number of interfaces, including SCSI, IDE, SATA or FC (fiber channel.) There are systems that use SATA disks internally, but that have a FireWire or SCSI-interface for the host system. Sometimes disks in a storage system are defined as JBOD, which stands for ‘Just a Bunch Of Disks’. This means that those disks do not use a pacific RAID level and acts as stand-alone disks. This is often done for drives that contain swap files or spooking data.

Below is an overview of the most popular RAID levels:

RAID level O — Striping -

In a RAID 0 system data are split up into blocks that get written across all the drives in the array. By using multiple disks (at least 2) at the same time, this offers superior I/O performance. This performance can be enhanced further by using multiple controllers, ideally one controller per disk.

Advantages:

- There is no overhead caused by parity controls.
- All storage capacity is used, there is no overhead.
- The technology is easy to implement.

Disadvantages:

- RAID O is not fault-tolerant. If one drive fails, all data in the RAID 0 array are lost. It should not be used for mission-critical systems.

Ideal use

RAID 0 is ideal for non-critical storage of data that have to be read/written at a high speed, such as on an image retouching or video editing station. If you want to use RAID 0 purely to combine the storage capacity of twee drives in a single volume, consider mounting one drive in the folder path of the other drive. This is supported in Linux, OS X as well as Windows and has the advantage that a single drive failure has no impact on the data of the second disk or SSD drive.

RAID level 1 — Mirroring
Data are stored twice by writing them to both the data drive (or set of data drives) and a mirror drive (or set of drives). If a drive fails, the controller uses either the data drive or the mirror drive for data recovery and continues operation. You need at least 2 drives for a RAID 1 array.

Advantages

- RAID 1 offers excellent read speed and a write-speed that is comparable to that of a single drive.
- In case a drive fails, data do not have to be rebuild, they just have to be copied to the replacement drive.
- RAID 1 is a very simple technology.

Disadvantages:

- The main disadvantage is that the effective storage capacity is only half of the total drive capacity because all data get written twice,
- Software RAID 1 solutions do not always allow a hot swap of a failed drive. That means the failed drive can only be replaced after powering down the computer it is attached to. For servers that are used simultaneously by many people, this may not be acceptable. Such systems typically use hardware controllers that do support hot swapping.

Ideal use:

RAID-1 is ideal for mission critical storage, for instance for accounting systems. It is also suitable for small servers in which only two data drives will be used. 1- '

RAID level 5:

RAID 5 is the most common secure RAID level. It requires at least 3 drives but can work with up to 16. Data blocks are striped across the drives and on one drive a parity checksum of all the block data is written. The parity data are not written to a fixed drive, they are spread across all drives, as the drawing below shows. Using the parity data, the computer can recalculate the data of one of the other data blocks, should those data no's longer be available. That means a RAID 5 array can withstand a single drive failure without losing data or access to data. Although RAID 5 can be achieved in software, a hardware controller is recommended. Often extra cache memory is used on these controllers to improve the write performance.

Advantages:

- somewhat slower (due to the parity that has to be calculated). If a drive fails, you still have access to all data, even while the failed drive is being replaced and the storage controller rebuilds the data on the new drive.
- Read data transactions are very fast while write data transactions are

Disadvantages:

- Drive failures have a.n effect on throughput, although this is still acceptable.
- This is complex technology. If one of the disks in an array using 4TB disks fails and is replaced, restoring the data (the rebuild time) may take a day or longer, depending on the load on the array and the speed of the controller. If another disk goes bad during that time, data are lost forever.

Ideal use:

RAID 5 is a good all-round system that combines efficient storage with excellent security and decent performance. It is ideal for file and application servers that have a limited number of data drives.

RAID level 6 — Striping with double parity:

RAID 6 is like RAID 5, but the parity data are written to two drives. That means it requires at Ieastl4 drives and can withstand 2 drives dying simultaneously. The chances that two drives break down at exactly the same moment are of course very small. However, if a drive in a RAID 5 systems dies and is replaced by a new drive, it takes hours or even more than a day to rebuild the swapped drive. If another drive dies during that time, you still lose all of your data. With RAID 6, the RAID array will even survive that second failure.

Advantages

- Like with RAID 5, read data transactions are very fast.

- If two drives fail, you still have access to all data, even while the failed drives are being replaced. So RAID 6 is more secure than RAID 5.

Disadvantages:

- Write data transactions are slower than RAID 5 due to the additional parity data that have to be calculated. In one report I read the write performance was 20% lower.
- Drive failures have an effect on throughput, although this is still acceptable.
- This is complex technology. Rebuilding an array in which one drive failed can take a long time.

Ideal use:

RAID 6 is a good all-round system that combines efficient storage with excellent security and decent performance. It is preferable over RAID 5 in file and application servers that use many large drives for data storage.

RAID level 10 — combining RAID 1 & RAID O

It is possible to combine the advantages (and disadvantages) of RAID 0 and RAID 1 in one single system. This is a nested or hybrid RAID configuration. It provides security by mirroring all data on secondary drives while using striping across each set of drives to speed up data transfers.

Advantages:

- If something goes wrong with one of the disks in a RAID 10 configuration, the rebuild time is very fast since all that is needed is copying all the data from the surviving mirror to a new drive. This can take as little as 30 minutes for drives of 1 TB.

Disadvantages:

- Half of the storage capacity goes to mirroring, so compared to large RAID 5 or RAID 6 arrays, this is an expensive way to have redundancy. RAID is no substitute for back-up!

All RAID levels except RAID 0 offer protection from a single drive failure. A RAID 6 system even survives 2 disks dying simultaneously. For complete security, you do still need to back-up the data from a RAID system.

- That back-up will come in handy if all drives fail simultaneously because of a power spike.
- It is a safeguard when the storage system gets stolen.
- Back-ups can be kept off-site at a different location. This can come in handy if a natural disaster or fire destroys your workplace.

Managed and Unmanaged Switches:

Basic network switches like those used in consumer routers require no special configuration beyond plugging in cables and power.

Compared to these unmanaged switches, high-end devices used on enterprise networks support a range of advanced features designed to be controlled by a professional administrator. Popular features of managed switches include SNMPmonitoring, link aggregation, and Q08 support.

Traditionally managed switches are built to be controlled from Unix-style command line interfaces. A newer category of managed switches called smart switches, targeted at entry-level and midrange enterprise networks, support web-based interfaces similar to a home router.

Layer 3 Switches

Traditional network switches operate at Layer 2 Data Link Layer of the OSI model. Layer 3 switches that blend the internal hardware logic of switches and routers into a hybrid device also have been deployed on some enterprise networks.

Compared to traditional switches, Layer 3 switches provide better support
for virtual LAN (VLAN) configurations.

Router:

in technical terms, a-router is a Layer 3 network gateway device, meaning that it connects two or more networks and that the router operates at the network layer of the QSI model.

A Routers contain a processor (CPU), several kinds of digital memory, and input-output (I/O) interfaces. They function as special-purpose computers, one that does not require a keyboard or display.

The router's memory stores an embedded operating system (O/S). Compared to general-purpose OS products like Microsoft Windows or Apple Mac OS, router operating systems limit what kind of applications can be run on them and also need much smaller amounts of storage space. Examples of popular router operating systems include Cisco Internetwork Operating System (IOS) and DD-WRT. These operating systems are manufactured into a binary firmware image and are commonly called router firmware.

By maintaining configuration information in a part of memory called the routing table, routers also can filter both incoming or outgoing traffic based on the addresses of senders and receivers.

Access point: Access points are used to spread the data in wireless medium. It is a Layer-2 device. Here we can provide the network connection to all the wireless devices. -r '

A single Access point can serve maximum 30-40 devices and provide best service. V

Patch panel:

within LANs connect network computers to each other and to outside lines, enabling the LANs to connect to the Internet or other wide area networks (WANs). Patch panels permit circuits to be arranged and rearranged by plugging and unplugging respective patch cords.

The advantage of using a patch panel is that it allows manual monitoring, testing, switching, routing, and other maintenance to be handled quickly because the cables in the front that connect to the more permanent cables in the back are configured and made so Patch panels that changes can be made quickly and easily when needed.

Categories cat 6 cable:

Category 6 cable, commonly referred to as Cat 6, is a standardized twisted pair cable for Ethernet and other network physical layers that is backward compatible with the Category 5/5e and Category 3 cable standards.

Compared with Cat 5 and Cat 5e, Cat 6 features more stringent specifications for crosstalk and system noise. The cable standard also specifies performance of up to 250 MHz compared to 100 MHz for Cat 5 and Cat 5e.ll1

Whereas Category 6 cable has a reduced maximum length of 55 meters when used for 1OGBASE-T, Category 6A cable (or Augmented Category 6') is characterized to 500 MHz and has improved alii crosstalk characteristics, allowing 10GBASE-T to be run for the same 100-meter maximum distance as previous Ethernet variants.

Conclusion

At last l want to conclude that after making this project l have learn the basic of Networking skill such as structure cabling, Server management (by deploying different services). In this Network designing project we mainly deploy the services on the Windows version 2016 edition Standard.

Firstly, we will convert the client machine from workgroup network to domain network while enabling the Active Directory Domain service in the server machine.

Secondly we have deploy the service of the dhcp, according to the host available in the Network, while choosing the proper subnets.

we will use group policy services on each client machine in order to deploy the common desktop wallpaper and We will share the common network drives to each client machine hide the other local drive of the client machine.

We have also deploy the service of FTP(File transfer protocol) and HTTP (hypertext transfer protocol services) in the Network in order share any files and host any websites.

We have also deploy the services related to WDS which the help of which we can configure any windows os on the client machine. We have also deploy the printer in given Network Organisation and sharing the printer in the given Network so that it is available to all client machine.

Therefore, while deploying these services in the Network we have learn and get the good experience about configuration of the services in the Network and designing of the Network.

At last, I want to thanks to Mr. Madhav Sharma who has given us such a nice project and also help us to accomplish this project successfully.