Unit:- 4

Page No. :
Date : / /20

Q. 1 Basic of network System. (LAN, WAN, MAN, CAN, PAN, SAN) ← DCN ques may read

→ A network operating system (NOS) provides services to client over a network. Both the client/server and peer-to-peer networking models use network operating system, and as such, NOS is must be able to handle typical network duties such as the following

- Providing access to remote Printers, managing which users are using which printers when, managing how (services) Print jobs are queued and recognizing when devices aren't available to the network.
- Enabling (access permission) and managing access to files on remote systems, and determining who can access what and who can't
- Granting (permission) access to remote applications and resources, such as the Internet and making those resources seem like local resources to the user.
- Providing routing services, including support for major network protocols, so that the operating system knows what data to send where.

- Providing basic network administration utilities (such as SNMP or simple Network Management Protocol) enabling an administrator to perform tasks involving managing network resources and users.

Q.2 Basics of TCP/IP Networking.
or
Introduction to TCP/IP Networks.

- TCP/IP is made up of two acronyms (full form of) TCP for Transmission Control Protocol and IP for Internet Protocol TCP handles packet flow between system and IP handles the routing of packets.

- TCP/IP based networks play an increasingly important role in computer networks. Perhaps (may be) one reason for their appeal is that they are based on an open specification that is not controlled by any vendor server

* TCP/IP Networking :-

TCP/IP is an abbreviation (Short name) for Transmission Control Protocal/Internet Protocal. It is a set of Protocals that define how two or more computers can communicate with each other.

- The Protocol is effectively a set of rules that describe how the data is passed between the computers.
- It is an open standard so can be implemented on any computer with the appropriate physical attributes.
- within the TCP/IP networking Protocol there are lots more Protocols. These provide different functionality important to the exchange of data over the networks.
- These can be integral to ~~that~~ the operation of the networking, such as the Domain Name System or could be an application that uses the network such as E-mail. (both of these are discussed ~~in further~~ detail later)
- Another related Protocol is UDP (User Datagram Protocol) which also runs on top of the IP (Internet Protocol).
- The difference between TCP and UDP is that TCP is connection based Protocol whereas UDP is connectionless.
- In other words when TCP is being used there is a session setup between the hosts

and the transfer is guaranteed.

- For UDP each data packet is sent but there is no checking that it has been received or any way of resending within the network layer.

- An application can run on top of UDP and implement it's own checking that each packet is received. [~~but that is not the same as leaving it to the networking stack to implement~~]

- A common way of comparing these is to liken TCP to the telephone system and UDP to the postal service with the telephone when you establish a connection with the other person, you know for certain that the user receives the message. If you were disconnected during the telephone conversation then you would know about it and be able to phone the other person again.

- with the postal system after you post the letter then you do not know for certain whether or not the mail will be received.

- After you have posted the letter it could be lost or destroyed on its way to its

destination or if the person has moved house they may never receive the letter.

* OSI Model :-

- Networking Protocols are often described relating to the OSI model. This is a model to describe the different networking functionality by the open standards Institute. The OSI model splits the different functions of networking into different layers.

→ There are seven types of layer are as under. / follow.

⇒ OSI 7 - layer Model

7. Application layer.
6. Presentation layer
5. Session layer
4. Transport layer
3. Network layer
2. Data link layer
1. Physical layer

Figure :- OSI - 7 layer Model.

Date : / / 20

[1] Physical layer :-

Describe the medical over which the data travels. For instance this describes the voltage of a 1 or 0 signal across a copper wire.

[2] Data - Link layer :-

Describes the means by which the bits are carried across the Physical layer. For Ex :- this can describe the start and end of a data stream is indicated.

[3] Network layer :-

This layer handles the routing of data through a network. As an example this describes how routing can happen based upon the address of the computers.

[4] transport layer and session layer :-

The transport and session layers provide ~~end~~ end-to-end session connection integrity. This includes keep alives to ensure the connection is maintained.

[5] Presentation layer and Application layer :-

- These Provide the interface to the application

Page No. :
Date : / /20

E.g. this may include the use of the nslookup command to convert a hostname into an IP address.

OSI model	TCP/IP stack
7. Application layer	Application
6. Presentation layer	
5. Session layer	
4. Transport layer	TCP or UDP
3. Network layer	IP
2. Data-link layer	Network interface
1. Physical layer	Physical

(PDNT-SPA)

- TCP-IP stack along side the OSI 7 layer Model.

Q.3 Explain IP address with its clause and mask.

⇒ The IP Address :-

- An important part of all networking protocols is the addressing scheme. Without being able to locate individual machines then it would not be possible for any communication between the hosts.
- There will be more than one addressing scheme in use but the most important of

these is the internet protocal, this is significant as it provides the addressing for each end of the connection.

- The other addressing schemes are effectively hidden from the user at layers two or below and are automatically handled by the networking hardware. The current version of IP is called IP version 4 but will be replaced by IPV6 in future.

- The addresses used in the internet protocal consist of four octets and is 32 bits long. The address is stored in a format known as dotted decimal.
  Ex xxx.xxx.xxx.xxx
  where xxx is a number between 0 and 255
  So an example IP address may be 192.168.3.27

- The IP addressing scheme provides 232 possible addresses, which could potentially have over 4.2 thousand million individual addresses.

- The problem with this however is that trying to locate each one of those addresses individual over the Internet would be an enormous task.

- So instead the address is split into a network and a host portion. The idea being that different organisations can be assigned a network which can have between 256 and 16.7 million addresses

SIP system investment plant

Page No.:
Date: / /20

available for assigned a network which can have between 256 and 16.7 million hosts on 2.1 million networks.

⇒ IP Address clause :-

- To ~~etc~~ accomodate for different sized organizations which require a different number of host addresses, the addresses are split into different network classes. There are 5 different classes however only 3 are commonly used.

Class A :- These are for large organisations. The network portion is 8 bits long and begins with binary 0. There are 126 possible networks each with up to 16.7 million hosts.

Class B :- These are for medium sized organisations. The network portion is 16 bits long and starts with binary 10. There are 16 thousand networks each with up to 65 thousand hosts.

Class C :- These are for smaller organisations. The network portion is 24 bits long and begins with binary 110. There are 200 thousand

possible networks each with up to 254 hosts.

Class D :- These are allocated for multicast although are rarely used. The addresses begin with binary 1110

Class E :- These are experimental. The addresses begin with binary 1111.

⇒ Ip Address class ranges :-

class	Range	Starting Binary
class-A	0.hhh.hhh.hhh to 127.hhh.hhh.	0
class-B	128.nn.hh.hh to 191.nn.hh.hh.	10
class-C	192.nn.nn.hh to 223.nn.nn.hh	110
class-D	224.xx.xx.xx to 239.xxxx.xx	1110
class-E	240.xxxx.xx. to 255.xx.xx.xx	1111

- Where as the nnn present the network portion of the address and the hhh represent the hosts portion of the address.

⇒ Reserved Ip Addresses :-

127.0.0.1 - Regers to localhosts
All host bits binary 0s - Regeres to the network
All host bits binary 1s - Broadcast address - send to all addresses.

⟹ Private IP Address Ranges :-

Class	Range
Class-A	10.0.0.0 to 10.255.255.255.
Class-B	172.16.0.0 to 172.31.255.255
Class-C	192.168.0.0 to 192.168.255.255

⟹ IP Adress subnet Masks :-

- The biggest Problem with the IP addressing scheme is that it is rapidly running out of free addresses.
- The long term solution is to move from IP version 4 to IP version 6 which will provide 340, 282, 366, 920, 938, 463, 463, 374, 631, 768, 456 seperate addresses.
- This should provide for all the Internet will ever need, even if every electronic device is given its own IP address. In the meantime a method was needed to make better use of the addresses available under The IP version 4 scheme.
- One of the problems with the current addressing is that the addresses are given away in large chunks.

- Subnetting allocas these large chunks of addresses to be further split into a further network and host component. This new network component is called the subnet.

- The following shows how a class B network address could effectively split into 254 separate virtual class C networks.

- Where as nnn = network portion of the address
  sss = Subnet Portion of the address
  hhh - host Portion of the address

- The network portion has been fixed so still stands as the first two octets. The next octet which would normally be part of the host address is then made to signify the subnet and effectively becomes part of the network address. The final octet is left as the host portion of the address.

- If the change which part of the address represents the network and host then we need to tell the computer and any routing devices of that. The technique used is known as creating a subnet mask.

- To create a subnet mask we need to use a binary one for every bit of the address that represents the network portion and a binary

Page No.:
Date: / /20

zero for any bit of the address that represents the host Portion.

- This gives us
  11111 1111 1111 00000
- We convert this to decimal to make it easier to read and it gives us a subnet mask of
  255 255 255 0

Q.4 What is a port number.

- In computer networking a port number is part of the addressing information used to identify the senders and receivers of message. Port number are most commonly used with TCP/IP connections.

- A Port number is a specific IP address in computers that identifies your computer and everytime data is transmitted.

- The IP address and Port number which the Programmed is responsible for must be disclosed any time the computer

- The Port number is a 16 bit binary number in the TCP. Therefore the Port number is in the range of 0 to 65535. The Port number are divided into three ranges.

(i) Well known ports.
(ii) Registered ports
(iii) Dynamic Ports.

(i) Well known Ports :-

The Port number ranging from 0-1023. They are assigned to standard server Processes such as FTP. Telnet The numbers are assigned by IANA (Internet Assigned numbers Authority)

- The well known Port numbers specifies the Port used by the server Process as its contact Port.

Port	Protocol	Description.
7	Echo	Echoes a received datagram back to the sender.
9	Discard	Discard any datagram that is received
11	Users	active user.
13	Daytime	returns the data and the time.
17	Quote	Returns the quote of the day.
19	chargen	Returns a string of characters
20	FTP, Data	file transfer Protocol (Data connection)
21	FTP, control	" " " (Control connection)
23	TELNET	Terminal Network.
25	SMTO	simple mail Transfer Protocol.
53	DNS	Domain Name Server
67	BOOTP	Bootstrap Protocol
79	Finger	Finger
80	HTTP	Hyper Text Transfer Protocol.
111	RPC	Remote Procedure Call

(ii) Register Port :-

The Port ranging from 1024-49151 are to be registered with IANA to Prevent duplicating. They can be used for Proprietary server processors or any client process.

- The registered Port numbers are the Port numbers that companies and other users registered with the Internet Corporation for assigned names and Numbers (ICANN) for used by the applications that communicate using the Internet's Transmission Control Protocol or the user Program protocol.

(iii) Dynamic Port :-

Port numbers from 49152 to 65535 are private Ports, also called "dynamic Ports". It can be frequently used. Normally they are used by client process temporarily.

- The dynamic Port number are the Port numbers that are available for used by any application to used in communicatly with any other application using the Internet's Transmission Control protocols (TCP) or the user Datagram protocol (UDP).

Page No.:
Date: / /20

Q.5 Domain Name System.

- The domain name server plays an important role in making Internet traffic possible.
- The DNS translates Internet domain and host names to IP address.
- DNS automatically converts the name we type in our web browser addressbar to the IP addresses of web servers hosting those sites.
- A domain name consists of two parts, the hostname and the domain. The host name is the computers specific name and the domain identifies the network of which the computer is a part.
- The domains used for the U.S. usually have extensions that identify the type of host. For eg: .edu is used for educational institutions and .com is used for business.
- DNS implements a distributed database to store this name and address information for all public hosts on the Internet.
- DNS assists in assigning an IP address to one or more names and assigning a name

to an IP address. In Linux this conversion is usually carried out by a special type of software known as bind.

- DNS can do more than just resolve host names. The name server also knows which host is receiving emails for an entire domain.

- Each domain name corresponds to numeric IP address. An IP address takes the form of 4 numbers each one between 0 to 255.

- No two organization can have the same domain name. The domains specify whether the names belong to a particular company, country and so on It is possible to create subgroups ~~shift~~ within a domain that are called sub domain.

- There are two kinds of TLD (Top Level Domain)
  (i) Generic Top Level Domain (gTLD)
  (ii) Country Code Top Level Domain (CCTLD)
  well known gTLDs are .edu, .com, .org, and .mil which are used mostly in the USA.
  And CCTLD are .in, .UK, .ch and .au

Page No.:
Date: / /20

Q.6 Describe NFS Server Configuration.

Ans NFS allows you to share file across networks. There are three ways to configure an NFS Server under Red Hat enterprise Linux.

(i) The NFS Server Configuration Tool.
(ii) The /etc/exports configuration File
(iii) The exports command.

(1) The NFS Server Configuration Tool :-

To use the NFS Server Configuration Tool, you must be running X Windows, have root privileges and have the system-config-nfs RPM Package installed. To start the application, click on System ⇒ Administration ⇒ Server Settings ⇒ NFS you can also type the command system-config-nfs in a terminal.

(2) The /etc/exports Configuration File :-

The /etc/exports file control which file systems are exported to remote hosts and specifies options.

Blank lines are ignored, comments can be made by starting a line with the hash mark (#) and long line can be wrapped with a backslash (\).

Each exported file system should be on its own individual line, and any lists of authorized hosts placed after an exported file system must be separated by space characters.

- options for each of the hosts must be placed in ~~part~~ parenthese directly after the host identifier, without any space separating the host and the first parenthesis valid host types are gss/krb5 gss/krb5i and gss/krb5p.

(3) The exportfs Command :-

- Every file system being exported to remote users via NFS, as well as the access level for those file systems, are listed in the /etc/exports file. When the nfs service starts, the /usr/sbin/exportfs command launches and reads this file, passes control to rpc.mountd (if NFSv2 or NFSv3) for the actual mounting process, then available to remote users.

⇒ Follow this divide to configure nfs server

(1) Scenario :-

In this scenario we are going to export the file system from the linux Config.

.org (IP address 10.1.1.200) host and mount it on linux config. local (IP address 10.1.1.10

(2) Prerequisites :-

At this point, we assume that the NFS service daemon is already installed on your system, including portmap deemon on which NFS setupt depends. Moreover your system needs to support the NFS file system.

(3) Server export file :-

3.1 Edit export file :- open up your favourite text editor, for example vim and edit /etc/exports file and add line /home/nfs/ *(ro, sync) to export /home/nfs directory for any host with read only permissions.

- Be sure that the directory you export by NFS exists you can also create a file inside the /home/nfs directory which will help you troubleshot once you mount this file system remotely

#touch /home/nfs/test-file

3.2 Restart NFS daemon :-

once you edit /etc/export file you need to restart NFS daemon to apply changes in the /etc/exports file. Depending on your Linux distribution, the restarting of NFS may differ.

Debian users:
#/etc/init.d nfs-kernel-server restart.

Redhat users:
#/etc/init.d/nfs restart

If you later decide to add more NFS exports to the /etc/exports file, you will need to either restart NFS daemon or run command exportfs:
#exportfs -ra

(4) Mount remote file system on client:-

- First we need to create a mount point:
#mkdir /home/nfs-local

If you are sure that the NFS client and mount point are ready, you can run the mount command to mount exported NFS remote file system.
#mount 10.1.1.200:/home/nfs/home

- Now you should be able to see that the file system is mounted. Notice that the mount command reports that the files stem is mounted as "read and write", although you can see that it provides a "read only" permission.

(5) Configure auto mount :- To make this completely transparent to end users, you can auto mount the NFS file system every time a user boots a PC, or you can also use PAM modules to mount once a user logs in with a proper username and password

- In this situation just edit /etc/fstab to mount system automatically during a system boot you can use your favourite editor and create new line.

Q 7 What is Samba?

- Samba is a suite of Unix Applications that speak the Server Message Block (SMB) Protocol.

- Microsoft Windows operating systems and the OS/2 operating System use SMB to perform client-server networking for file and printer sharing and associated operations.

- By supporting this Protocol, Samba enables computers running Unix to get in on the action, communicating with the same

networking Protocols as Microsoft Windows and appearing as another Windows system on the network from the perspective of same OS a windows client.

- A Samba server offers the following services:
  - Shares one or more directory trees
  - Shares one or more distributed filesystem (DFS) trees.
  - Shares printers installed on the server among Windows clients on the network
  - Assist clients with network browsing.
  - Authenticate clients logging onto a windows domain
  - Provide or assist with windows Internet Name Service (WINS) name server resolution

- The Samba suite ~~as~~ also includes client tools that allow users on a unix system to access folders and printers that windows systems and Samba servers offer on the network.

⇒ How to installing Samba?

- Installing a SAMBA server on the Mandrake Linux Server will allow file sharing and printers on a network that consists of a mix of Linux and Windows PCs.

- The SAMBA has a client-server based architecture and consists of tools that can be used for developing services or test configuration.

- Before installing a SAMBA server, certain packages are required to be installed on the Mandrake Linux system.

- After the installing, configuring a SAMBA server can be done easily by making changes in the smb.conf configuration file.

- SAMBA Server Commands can be used to start, stop, restart or perform other functions with the SAMBA Server. Use the following step for installing SAMBA Server

1. Use "yum" to install the Samba package!

```
yum -y install samba
```
(-y option)

⟹ Creating Samba Test Directory and files

for this part of the procedure, you'll use the su- Command to work as root. Although it's not best practise to do this regularly, there are times where it is much more practical to work directly as root instead of trying to use sudo to do everything. This is one of these time.

2 While logged on as root, create the new directory /smbdemo with the following command

mkdir /smbdemo

3 Change the permission on the new directory to 770 with the following command:

chmod 770 /smbdemo

4 Navigate to the new directory with the following command

cd /smbdemo

5 Add three empty files to the directory with the following command.

touch file1 file2 file3

Adding the Samba User

You must add users to the samba database in order for them to have access to their home directory and other samba shares.

6 Use the following command to add a new Samba user.

Smbpasswd -a <username>

for example to add the user don, use the command Smbpassad -a don

Page No.:
Date: / /20

⟹ Creating the Samba Group

+ Perform the following steps to create a smbusers group, change ownership of the /smbdemo directory, and add a user to the smbusers group:

```
groupadd smbusers
chown:smbusers /smbdemo
usermod -G smbusers don
```

⟹ Configuring Samba

- The default configuration file allows users to view their home directories as a Samba share.

- It also share all printers configured for the system as samba shared printers. In other words, you can attach a printer to the system and print to it from the windows machines on your network.

⟹ Samba's Configuration file is typically here!

- /etc/samba/smb.conf
- SMB passwords are stored in a distinct password file.
  /etc/samba/smbpassad
  /etc/samba/smbusers
- ~~Starting & stopping samber.~~

(1) Graphical Configuration :

- The Samba Server Configuration Tool is a graphical interface for managing samba shares, users, and basic server settings. It modifies the configuration files in the /etc/samba/ directory. Any changes to these files not made using the application are preserved.

(2) Configuring Server Setting :

- The first step in configuration ~~for~~ a samba server is to configure the basic settings for the server and a few security options. After starting the application, select Preference ⇒ Server settings from the pull down menu.

(3) Command Line Configuration :-

- Samba uses /etc/samba/smb.conf as its configuration file. If you change this configuration file, the changes do not take effect until you restart the samba daemon with the command service smb restart.

- All of samba is configured in one single file, the smb.conf file. This file, located at /etc/samba/smb.conf, allows you to specify

which resources on the linux machine you wish to share and who they can be accessed by.

(5) Encrypted Passwords:-

- Encrypted Passwords are enabled by default because it is more secure. If encrypted Passwords are not used, plain text passwords are used, which can be intercepted by someone using a network packet sniffer. It is recommended that encrypted passwords be used.

(6) To configure samba to use encrypted passwords follow these steps:-

- Create a separate password file for samba. To create one based on your existing /etc/passwd file, at a shell prompt, type the following command.

→ /cat /etc/passwd /mksmbpasswd.sh > /etc/samba/smbpasswd.

- Change the permission of the samba password file so that only root has read and write permission.

❖ FTP Server

- *File* **T***ransfer* **P***rotocol* **(FTP)** is the commonly used protocol for exchanging files over the Internet. FTP uses the Internet's TCP/IP protocols to enable data transfer. FTP uses a client-server architecture, often secured with SSL/TLS. FTP promotes sharing of files via remote computers with reliable and efficient data transfer.

How FTP Works

- FTP works in the same way as HTTP for transferring Web pages from a server to a user's browser and SMTP for transferring electronic mail across the Internet in that, like these technologies.

- FTP uses a client-server architecture. Users provide authentication using a sign-in protocol, usually a username and password, however some FTP servers may be configured to accept anonymous FTP logins where you don't need to identify yourself before accessing files. Most often, FTP is secured with SSL/TLS.

How to FTP

- Files can be transferred between two computers using FTP software. The user's computer is called the local host machine and is connected to the Internet. The second machine, called the remote host, is also running FTP software and connected to the Internet.

1. The local host machine connects to the remote host's IP address.
2. The user would enter a username/password (or use anonymous).
3. FTP software may have a GUI, allowing users to drag and drop files between the remote and local host. If not, a series of FTP commands are used to log in to the remote host and transfer files between the machines.