Laboratory Manual

ON

NETWORKING LAB

(For 4th Semester CSE/IT)

Prepared by:

Smt Reetanjali Panda
Lecturer(CSE&IT)
UCP Engineering School
Berhampur.

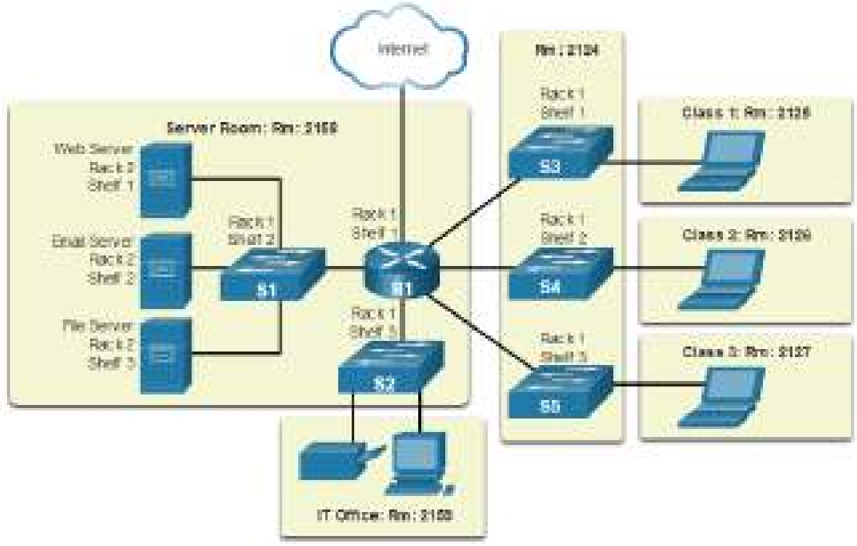
Miss Sasmita Panigrahi
PTGF(CSE&IT)
UCP Engineering School
Berhampur.

EXPERIMENT-1 Recognize the physical topology and cabling (coaxial, OFC, UTP, STP) of a network.

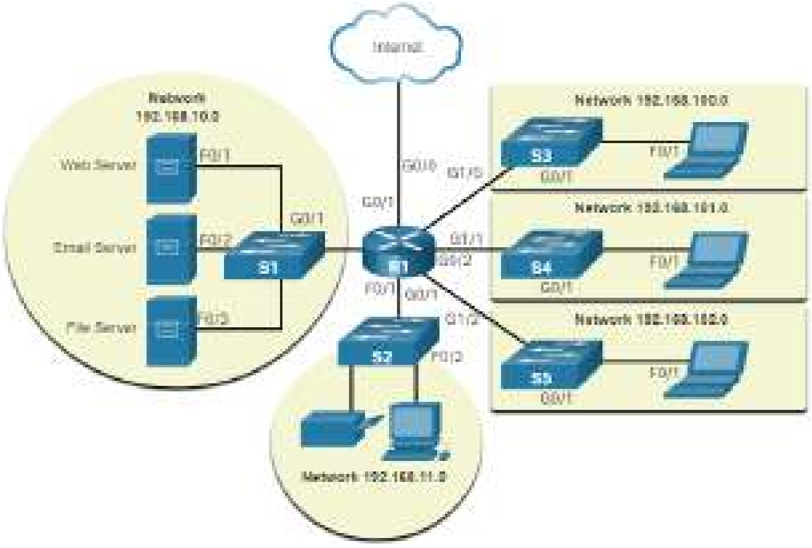
Network Representations and Topologies

Topology Diagrams

Physical topology diagrams illustrate the physical location of intermediary devices and cable installation.



Logical topology diagrams illustrate devices, ports, and the addressing scheme of the network.



Copper Cabling

Copper cabling is the most common type of cabling used in networks today. It is inexpensive, easy to install, and has low resistance to electrical current flow.

Limitations:

- Attenuation – the longer the electrical signals have to travel, the weaker they get.
- The electrical signal is susceptible to interference from two sources, which can distort and corrupt the data signals (Electromagnetic Interference (EMI) and Radio Frequency Interference (RFI) and Crosstalk).

Mitigation:

- Strict adherence to cable length limits will mitigate attenuation.
- Some kinds of copper cable mitigate EMI and RFI by using metallic shielding and grounding.
- Some kinds of copper cable mitigate crosstalk by twisting opposing circuit pair wires together.

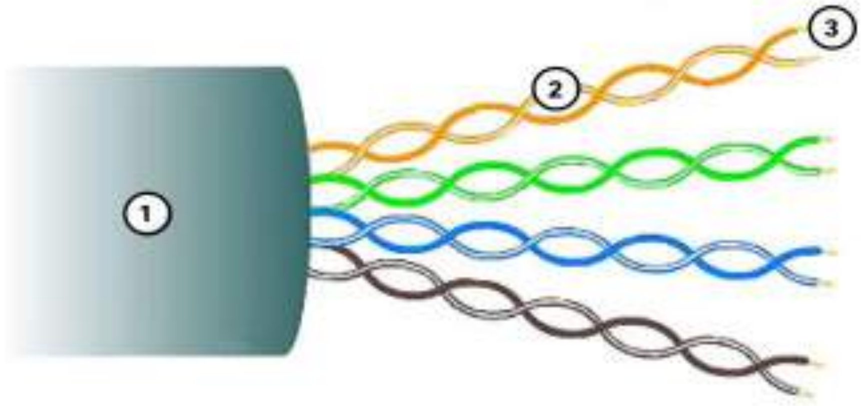
Types of Copper Cabling

Unshielded Twisted-Pair (UTP) Cable

Shielded Twisted-Pair (STP) Cable

Coaxial Cable

Unshielded Twisted Pair (UTP)

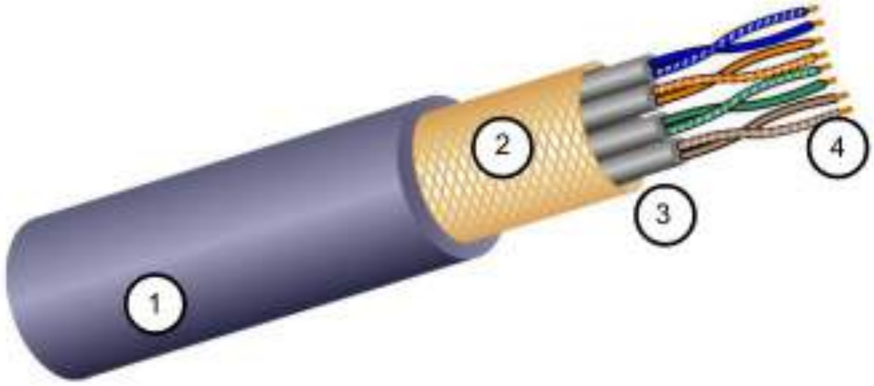


- UTP is the most common networking media.
- **Terminated with RJ-45 connectors**
- Interconnects hosts with intermediary network devices.

Key Characteristics of UTP

1. The outer jacket protects the copper wires from physical damage.
2. Twisted pairs protect the signal from interference.
3. Color-coded plastic insulation electrically isolates the wires from each other and identifies each pair.

Shielded Twisted Pair (STP)



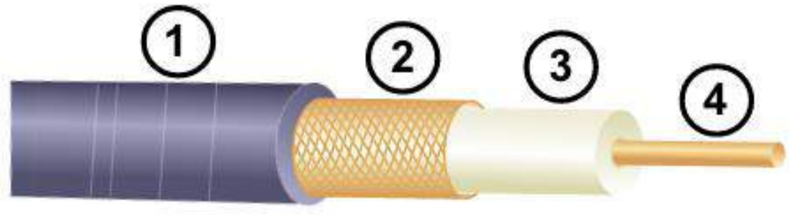
- Better noise protection than UTP
- More expensive than UTP
- Harder to install than UTP
- **Terminated with RJ-45 connectors**
- Interconnects hosts with intermediary network devices

Key Characteristics of STP

1. The outer jacket protects the copper wires from physical damage
2. Braided or foil shield provides EMI/RFI protection
3. Foil shield for each pair of wires provides EMI/RFI protection

4. Color-coded plastic insulation electrically isolates the wires from each other and identifies each pair

Coaxial Cable



Consists of the following:

1. Outer cable jacket to prevent minor physical damage
2. A woven copper braid, or metallic foil, acts as the second wire in the circuit and as a shield for the inner conductor.
3. A layer of flexible plastic insulation
4. A copper conductor is used to transmit the electronic signals.
5. **BNC connectors** are used with coax cable.

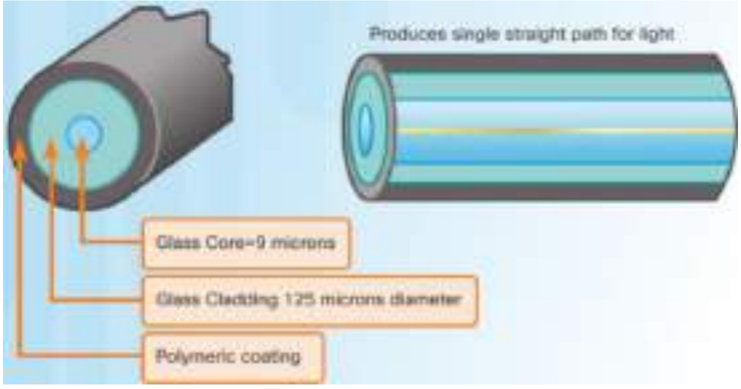
Fiber-Optic Cabling

Properties of Fiber-Optic Cabling

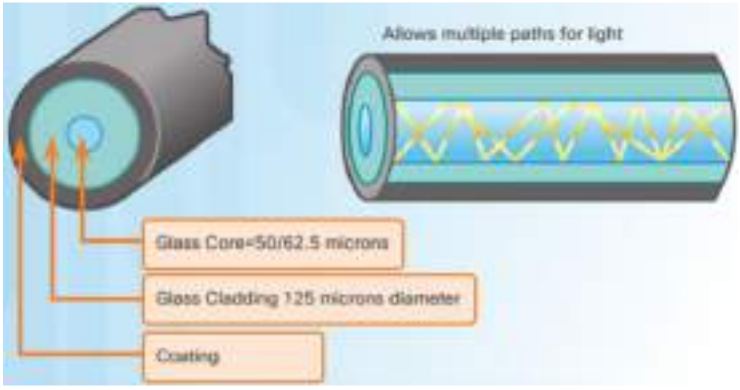
- Not as common as UTP because of the expense involved
- Ideal for some networking scenarios
- Transmits data over longer distances at higher bandwidth than any other networking media
- Less susceptible to attenuation, and completely immune to EMI/RFI
- Made of flexible, extremely thin strands of very pure glass
- Uses a laser or LED to encode bits as pulses of light
- The fiber-optic cable acts as a wave guide to transmit light between the two ends with minimal signal loss

Types of Fiber Media

Single-Mode Fiber


Produces single straight path for light
Glass Core=9 microns
Glass Cladding 125 microns diameter
Polymeric coating

- Very small core
- Uses expensive lasers
- Long-distance applications
- **Multimode Fiber**


Allows multiple paths for light
Glass Core=50/62.5 microns
Glass Cladding 125 microns diameter
Coating

- Larger core
- Uses less expensive LEDs
- LEDs transmit at different angles
- Up to 10 Gbps over 550 meters

EXPERIMENT-2 Recognition and use of various types of connectors RJ-45, RJ-11,BNC and SCST

Registered Jack-45(RJ-45 Connector)

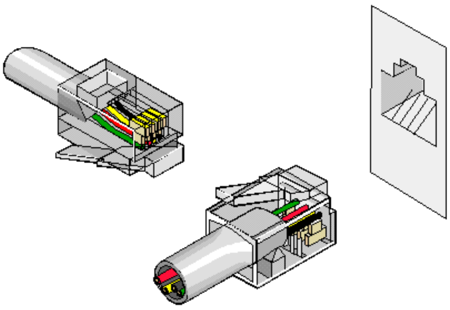
RJ-45 Connector

An 8-pin/8-position plug or jack is commonly used to connect computers onto Ethernet-based local area networks (LAN). Two wiring schemes–T568A and T568B–are used to terminate the twisted-pair cable onto the connector interface.

RJ-45 Socket

Registered Jack-11(RJ-11 Connector)

A telephone interface that uses a cable of twisted wire pairs and a modular jack with two, four or six contacts. RJ-11 is the common connector for plugging a telephone into the wall and the handset into the telephone.



BNC Connector:

A Bayonet Neill Concelman (BNC) connector is a miniature quick connect/disconnect radio frequency (RF) connector used with coaxial cables in a 10Base-2 Ethernet system and for video and radio frequency applications. These connectors are some of the most widely used RF connectors because they are simple to use and offer high performance.

Fiber-Optic Connectors:

Straight-Tip (ST) Connectors

It is the most popular connector for multimode fiber optic LAN applications . It has a long 2.5mm diameter ferrule made of ceramic (zirconia), stainless alloy or plastic. It mates with a interconnection adapter and is latched into place by twisting to engage a spring-loaded bayonet socket.

Straight-Tip (ST) Connectors

Subscriber Connector (SC) Connectors

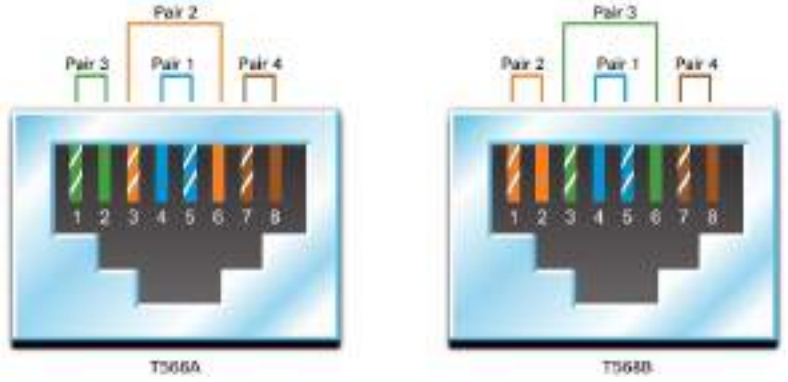
SC was developed by NTT of Japan. It is widely used in single mode applications for its excellent performance. SC connector is a non-optical disconnect connector with a 2.5mm pre-radiused zirconia or stainless alloy ferrule. It features a snap-in (pushpull) connection design for quick patching of cables into rack or wall mounts.

Subscriber Connector (SC) Connectors

EXPERIMENT-3 Making of cross cable and straight cable

UTP Cabling

Straight-through and Crossover UTP Cables



Cable Type	Standard	Application
Ethernet Straight-through	Both ends T568A or T568B	Host to Network Device
Ethernet Crossover *	One end T568A, other end T568B	Host-to-Host, Switch-to-Switch, Router-to-Router

EXPERIMENT-4 Install and configure a network interface card in a workstation.

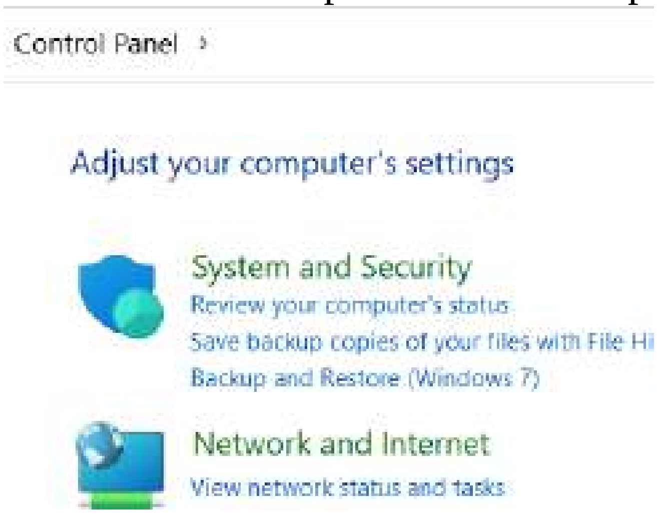
i. Open the PC case. The power should be off when you do this.
ii. Ensure that you have an antistatic wrist strap attached to your wrist and grounded to the PC when working with it.
iii. Remove the strap before you switch on the power.
iv. Now take the NIC card and install it into one of the PCI slots by aligning the guide notches with the PCI slot.

v. Press straight down with gentle pressure until the card snugly fits into the PCI slot.

vi. Secure the card with a single screw used to attach the card to the PC.

vii. Check the card whether it moves from its position. If it does, it could damage itself when the PC is turned on.
viii. Close the PC case and turn on the power.

ix. Check if the internet works or not. If not then check the connections and repeat the above steps.

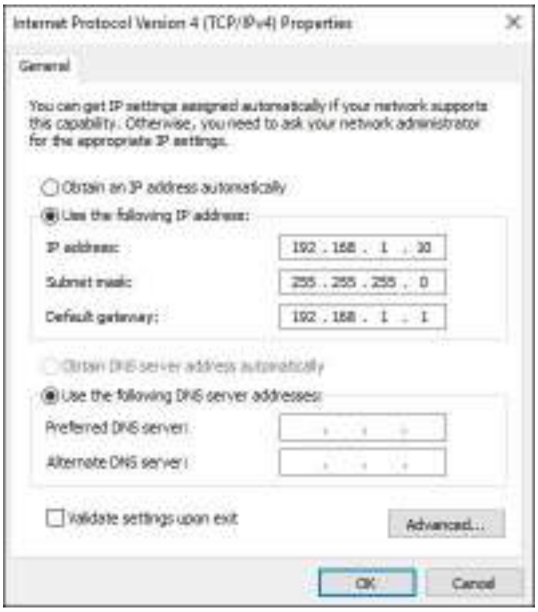

Control Panel ›
Adjust your computer's settings
System and Security
Review your computer's status
Save backup copies of your files with File Hi
Backup and Restore (Windows 7)
Network and Internet
View network status and tasks

EXPERIMENT-5 Identify the IP address of a workstation and the class of the address and configure the IP Address on a workstation .

Configure IP Addressing

Manual IP Address Configuration for End Devices

- End devices on the network need an IP address in order to communicate with other devices on the network.
- IPv4 address information can be entered into end devices manually, or automatically using Dynamic Host Configuration Protocol (DHCP).
- To manually configure an IPv4 address on a Windows PC, open the Control Panel > Network Sharing Center > Change adapter settings and choose the adapter. Next right-click and select Properties to display the Local Area Connection Properties.
- Next, click Properties to open the Internet Protocol Version 4 (TCP/IPv4) Properties window. Then configure the IPv4 address and subnet mask information, and default gateway.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

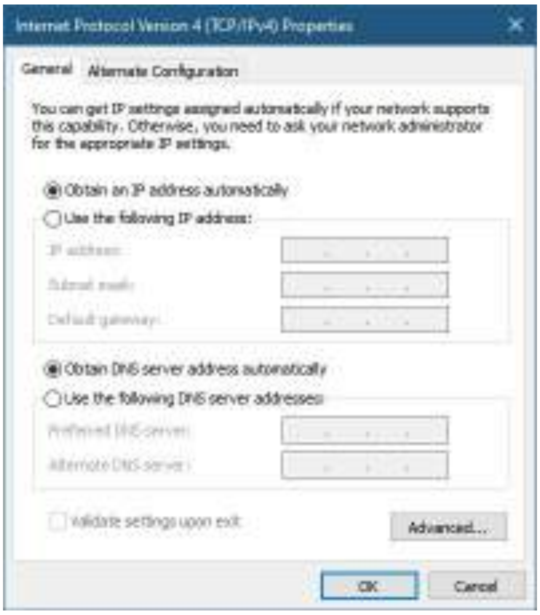
Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

Automatic IP Address Configuration for End Devices

- DHCP enables automatic IPv4 address configuration for every end device that is DHCP-enabled.
- End devices are typically by default using DHCP for automatic IPv4 address configuration.
- To configure DHCP on a Windows PC, open the Control Panel > Network Sharing Center > Change adapter settings and choose the adapter. Next right-click and select Properties to display the Local Area Connection Properties.
- Next, click Properties to open the Internet Protocol Version 4 (TCP/IPv4) Properties window, then select Obtain an IP address automatically and Obtain DNS server address automatically.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

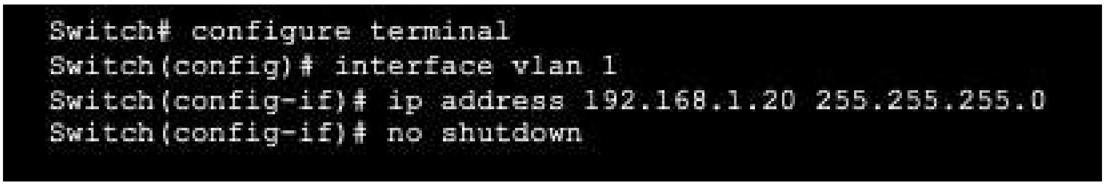
Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

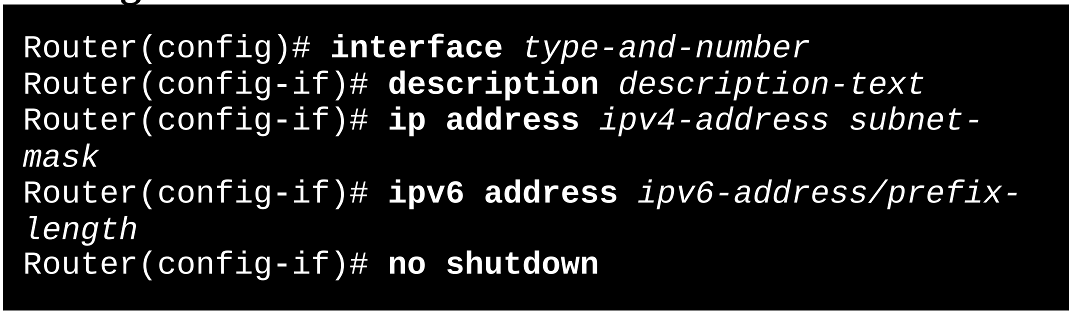
Switch Virtual Interface Configuration

- To access the switch remotely, an IP address and a subnet mask must be configured on the SVI.
- To configure an SVI on a switch:
- Enter the interface vlan 1 command in global configuration mode.
- Next assign an IPv4 address using the ip address ip-address subnet-mask command.
- Finally, enable the virtual interface using the no shutdown command.



```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.1.20 255.255.255.0
Switch(config-if)# no shutdown
```

Configure Router Interfaces



```
Router(config)# interface type-and-number
Router(config-if)# description description-text
Router(config-if)# ip address ipv4-address subnet-
mask
Router(config-if)# ipv6 address ipv6-address/prefix-
length
Router(config-if)# no shutdown
```

IPv4 Address Structure

- An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a device (for example, a computer or a router) to the Internet.
- The IPv4 addresses are unique and universal. The address space of IPV4 is 232 or 4,294,967,296. In IPv4 addressing, a block of addresses can be defined as x.y.z.t /n in which x.y.z.t defines one of the addresses and the /n defines the mask. The first address in the block can be found by setting the rightmost 32 − n bits to 0s , called as Network Address that identifies a particular network.

- The last address in the block can be found by setting the rightmost 32 – n bits to 1s , which is the broadcast address.

The 32 bit IP address is divided into five sub-classes. These are:

- Class A
- Class B
- Class C
- Class D
- Class E

Each of these classes has a valid range of IP addresses. Classes D and E are reserved for multicast and experimental purposes respectively. The order of bits in the first octet determine the classes of IP address.

IPv4 address is divided into two parts:

- Network ID
- Host ID

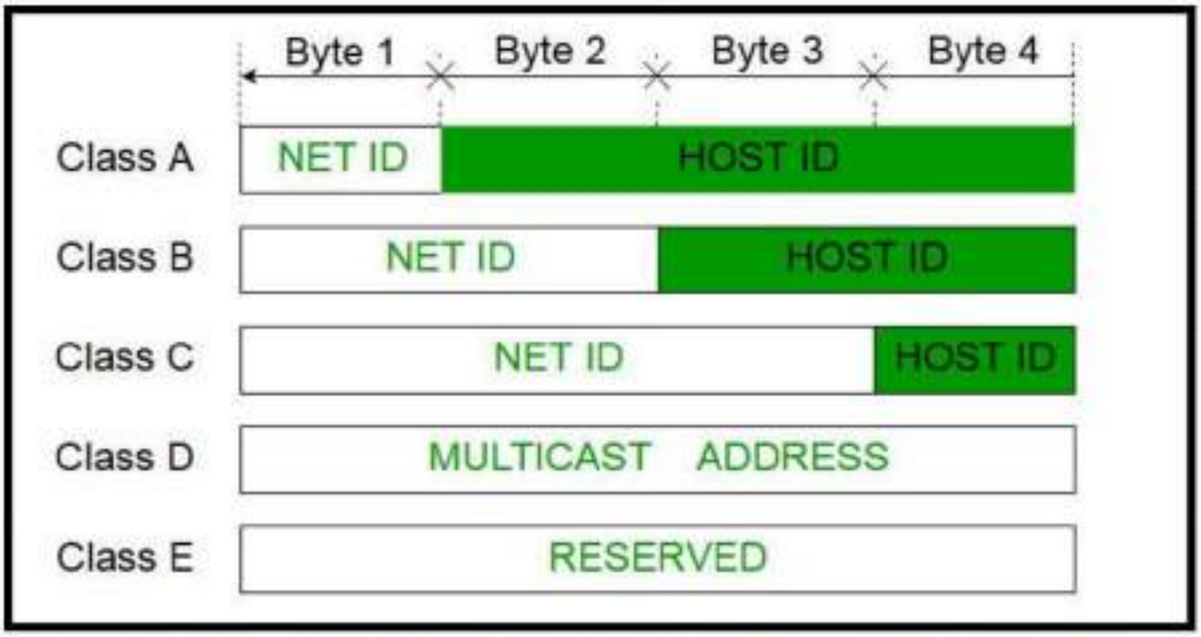
  Class A: It uses first octet for network addresses and last three octets for host addressing.

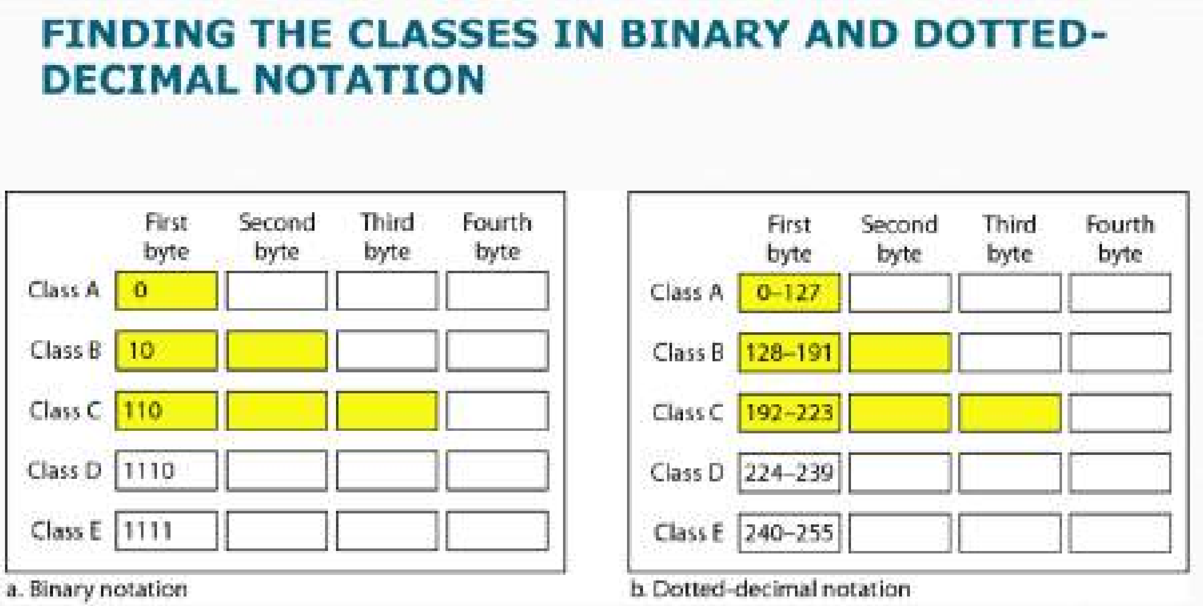
  Class B: It uses first two octets for network addresses and last two for host addressing.

  Class C: It uses first three octets for network addresses and last one for host addressing.

  Class D: It provides flat IP addressing scheme in contrast to hierarchical structure for above three.

  Class E: It is used as experimental.





FINDING THE CLASSES IN BINARY AND DOTTED-DECIMAL NOTATION

	First byte	Second byte	Third byte	Fourth byte
Class A	0			
Class B	10	🟨		
Class C	110	🟨	🟨	
Class D	1110			
Class E	1111			

a. Binary notation

	First byte	Second byte	Third byte	Fourth byte
Class A	0–127			
Class B	128–191	🟨		
Class C	192–223	🟨	🟨	
Class D	224–239			
Class E	240–255			

b. Dotted-decimal notation

EXPERIMENT-6 Managing user accounts in windows and linux

Windows 10 and 11

Press the Windows key, type Control Panel, and then press Enter.

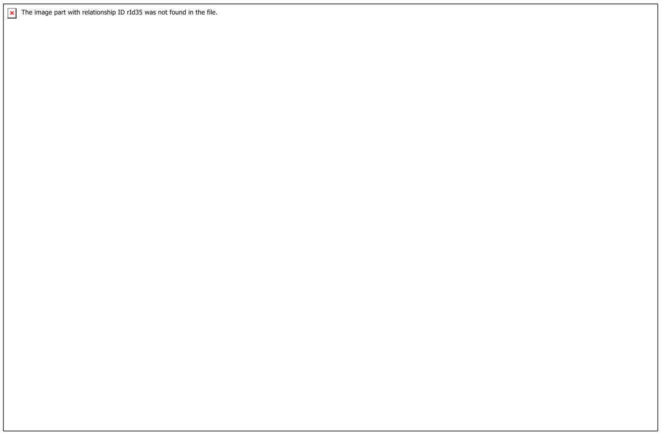
Click the User Accounts option in the Control Panel.

☒ The image part with relationship ID rId33 was not found in the file.

If using the View by Category option in the Control Panel, click the User Accounts link.

The image part with relationship ID rId34 was not found in the file.

In the User Accounts window, the middle section allows you to change various aspects of user accounts. Clicking the Manage another account link takes you to a menu where you can add, edit, or remove user accounts.


The image part with relationship ID rId35 was not found in the file.

Windows 8

- From the Windows desktop, open the Charms menu by pressing the Windows key+C key and select Settings.
- In the Settings window, select Control Panel.
- Click the User Accounts option.
- If using the View by Category option in the Control Panel, click the User Accounts link.
- You can add or remove user accounts or guest accounts in the User Accounts window. You can also select a user account and make necessary changes, including changing the user account name.

Windows Vista and 7

In both Windows Vista and Windows 7:

- Open the Control Panel.
- Click Add or remove user accounts.
- In the User Accounts window, you can add or remove user accounts. You can also select a user account and make necessary changes, including changing the user account name.

Windows 2000

- Changing settings for a user account in Windows 2000 requires you to be logged in with an administrator account.
- Open the Control Panel.
- Double-click the Users and Password icon.
- In the Users and Passwords window, you can add or remove user accounts. You can also select a user account and make any necessary changes, including changing the user account name.

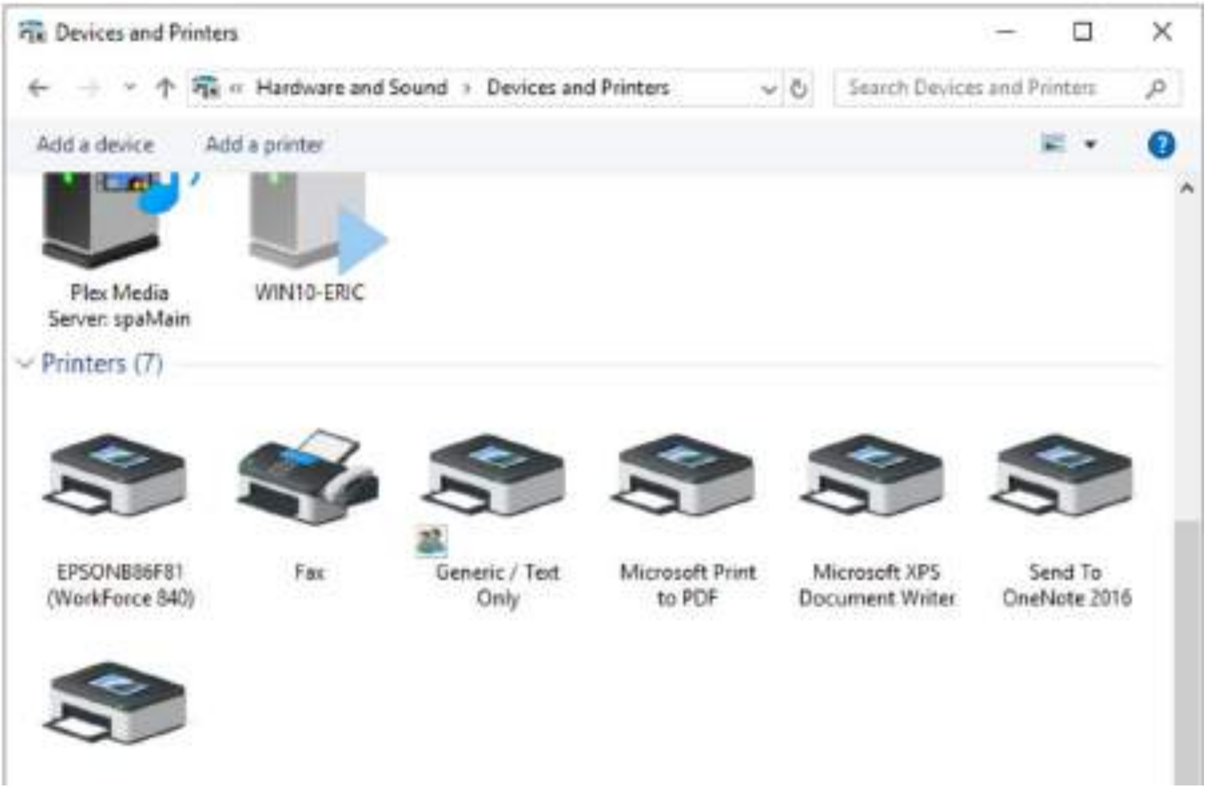
Linux

- To add a user account, use the adduser command. See the adduser command page for additional information about this command.
- To remove a user account, use the deluser command. See the deluser command page for additional information about this command.
- To change the user settings, such as group membership, default login shell, and home directory, use the usermod command. See the usermod command page for additional information about this command.

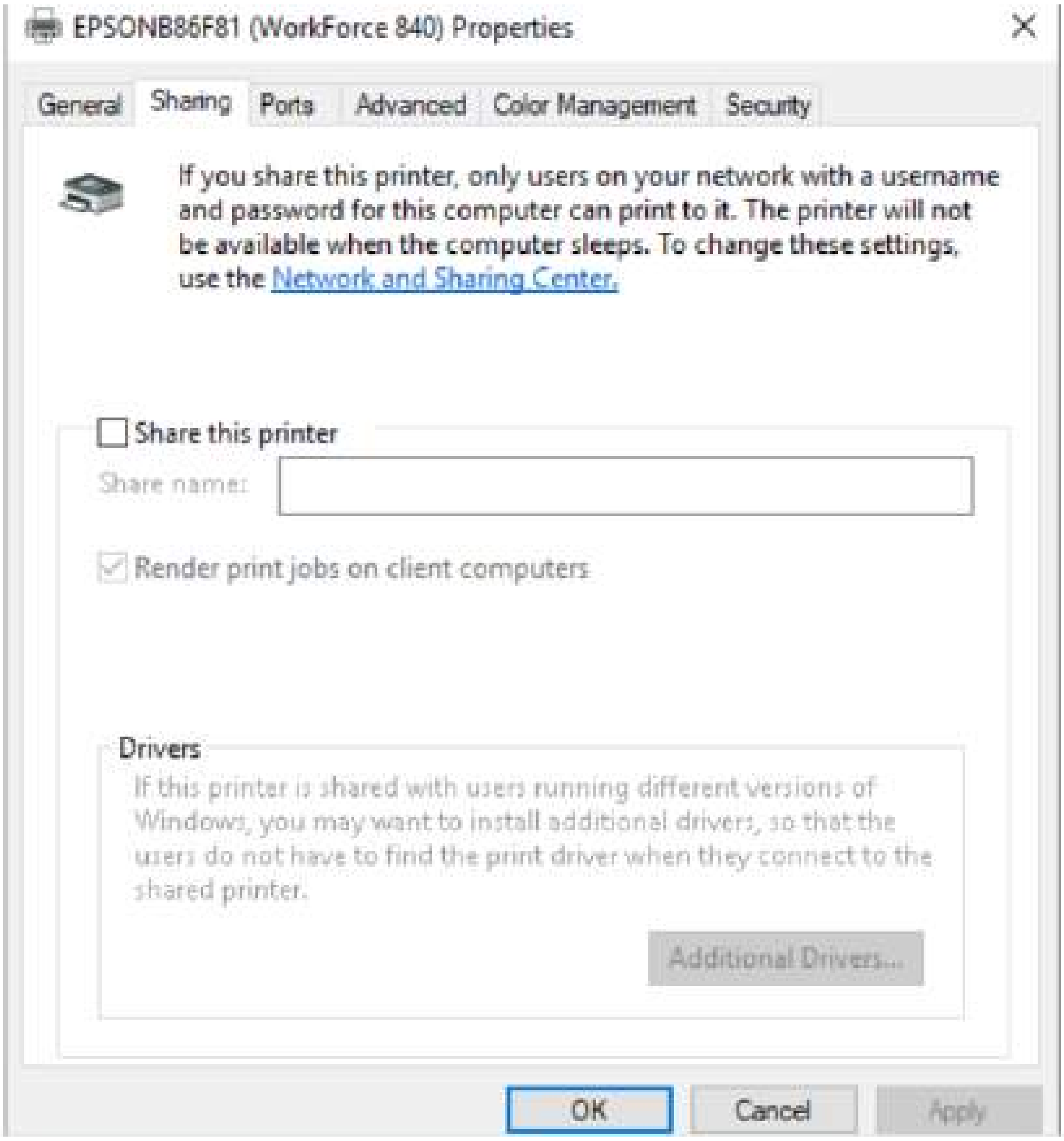
EXPERIMENT-7 Sharing of Hardware resources in the network.

Printers:

- Network printers can be configured as shared devices so that others on the network can use them. If you are using Windows 7 go to **Start | Devices and Printers**. If you are using Windows 8 or Windows 10, display control panel and click **View Devices and Printers** (under the Hardware and Sound heading). Windows displays the Devices and Printers dialog box.


Devices and Printers
Hardware and Sound › Devices and Printers
Search Devices and Printers
Add a device
Add a printer
Plex Media Server: spaMain
WIN10-ERIC
Printers (7)
EPSONB86F81 (WorkForce 840)
Fax
Generic / Text Only
Microsoft Print to PDF
Microsoft XPS Document Writer
Send To OneNote 2016

- Right-click the printer you want to share and select Printer Properties from the Context menu. Windows displays the Properties dialog box for the selected printer. The contents of the dialog box vary depending on the capabilities of your printer. Make sure the Sharing tab is displayed.



If you share this printer, only users on your network with a username and password for this computer can print to it. The printer will not be available when the computer sleeps. To change these settings, use the Network and Sharing Center.

□ Share this printer

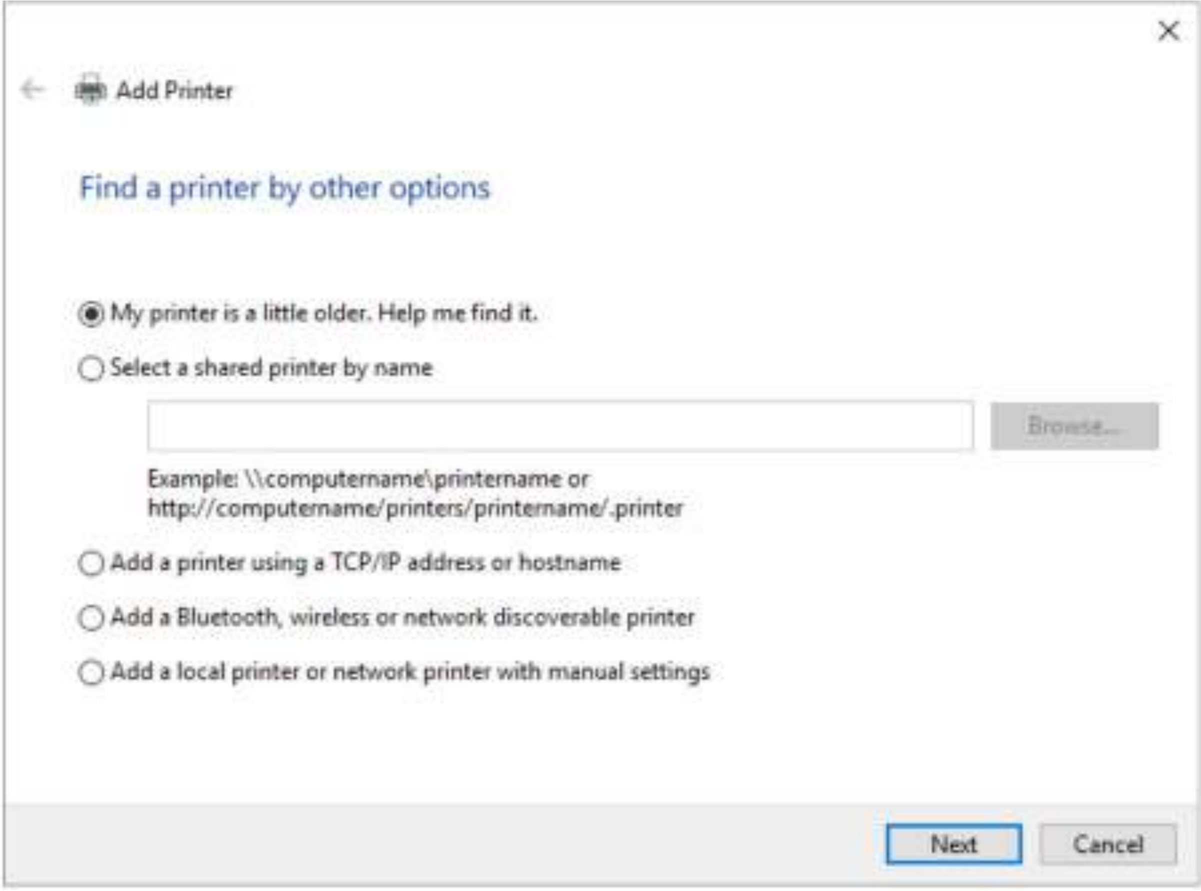
Share name:

☑ Render print jobs on client computers

If this printer is shared with users running different versions of Windows, you may want to install additional drivers, so that the users do not have to find the print driver when they connect to the shared printer.

- Click the Share this Printer check box and optionally change the Share Name of the printer. Depending on the configurations of your particular systems you may either check or uncheck the Render Print Jobs on Client Computers check box. If checked, then all the processing required prior to queuing the print job occurs on the client computer. If unchecked, the computer hosting (serving) the printer does the processing for all print jobs sent through it.

- When you are done sharing the printer, click OK to close the printer's Properties dialog box. The printer is immediately made available to others on your network. In order to access the shared printer from a different system, go to that system and, if the system is using Windows 7, choose **Start | Devices and Printers** and click on Add a Printer. If the system is using Windows 8 or Windows 10, display the Control Panel and click **View Devices and Printers** (under the Hardware and Sound heading) and then click the Add a Printer option, at the top of the dialog box. Windows starts the Add Printer wizard. The Windows 10 system will perform a search for a device or printer to this PC. Click on The Printer I want isn't Listed if our printer isn't found. Windows displays the Find a Printer by Other Options section of the Add Printer wizard. Click the second option (Add a Network, Wireless or Bluetooth Printer if you are using Windows 7 or Windows 8) or click the fourth option (Add a Bluetooth, Wireless or Network Discoverable Printer) if you are using Windows 10, and the system immediately starts scanning the network for available printers. After all of the printers have been found, select the printer name that you want to use and click **Next**. The network printer is added to the computer's list of available printers. Click **Finish** to finish the process.



Add Printer

Find a printer by other options

● My printer is a little older. Help me find it.

○ Select a shared printer by name

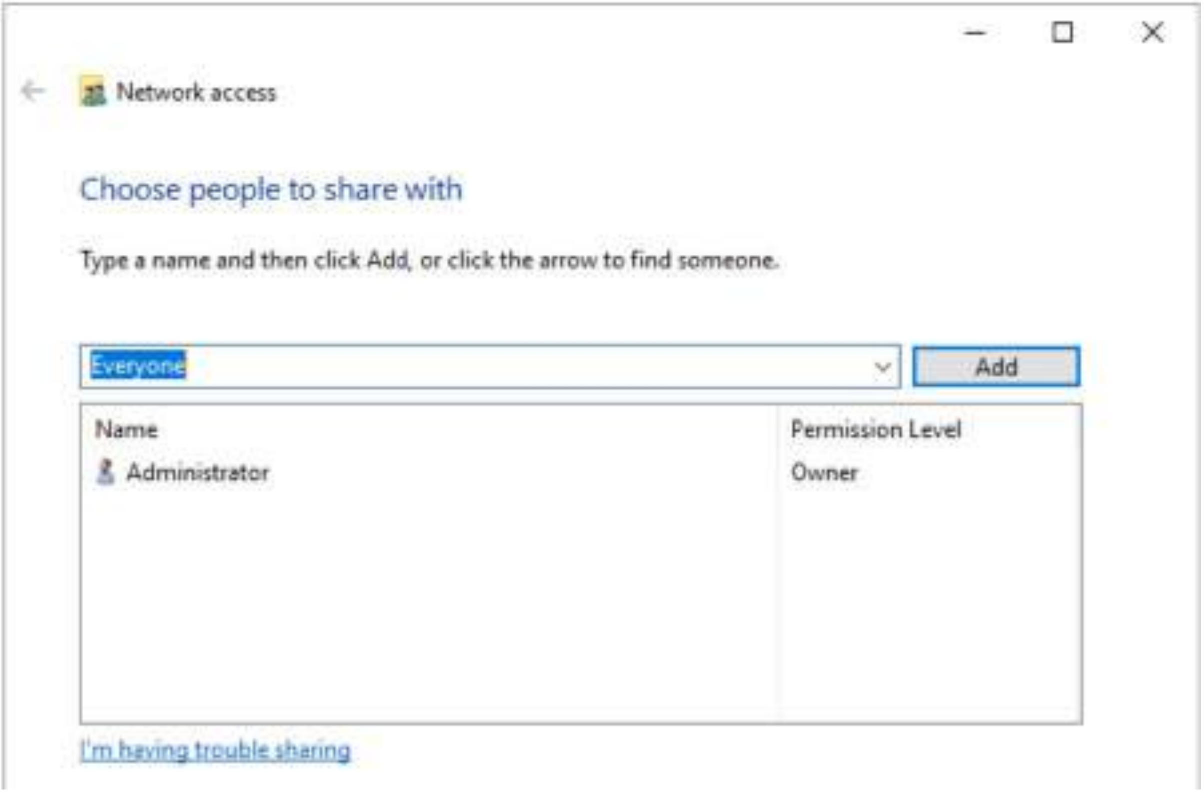
Example: \\computername\printername or
http://computername/printers/printername/.printer

○ Add a printer using a TCP/IP address or hostname

○ Add a Bluetooth, wireless or network discoverable printer

○ Add a local printer or network printer with manual settings

- **File Folders and Disk Drives**
- File folders and entire disks can also be shared among network-connected systems, and the procedure is similar to that of sharing a printer. Using Windows Explorer, right-click the folder you want to share with others on the network and select **Share With | Specific People** (Windows 7) or **Share | Specific People** (Windows 8). Windows then displays the File Sharing dialog box. If you are using Windows 10, display File Explorer and make sure the Share tab of the ribbon is displayed. Then right-click the folder you want to share with others on the network and select **Give Access to | Specific People**. Windows then displays the Network Access dialog box. (The File Sharing and Network Access dialog boxes are essentially the same.)



Network access

Choose people to share with

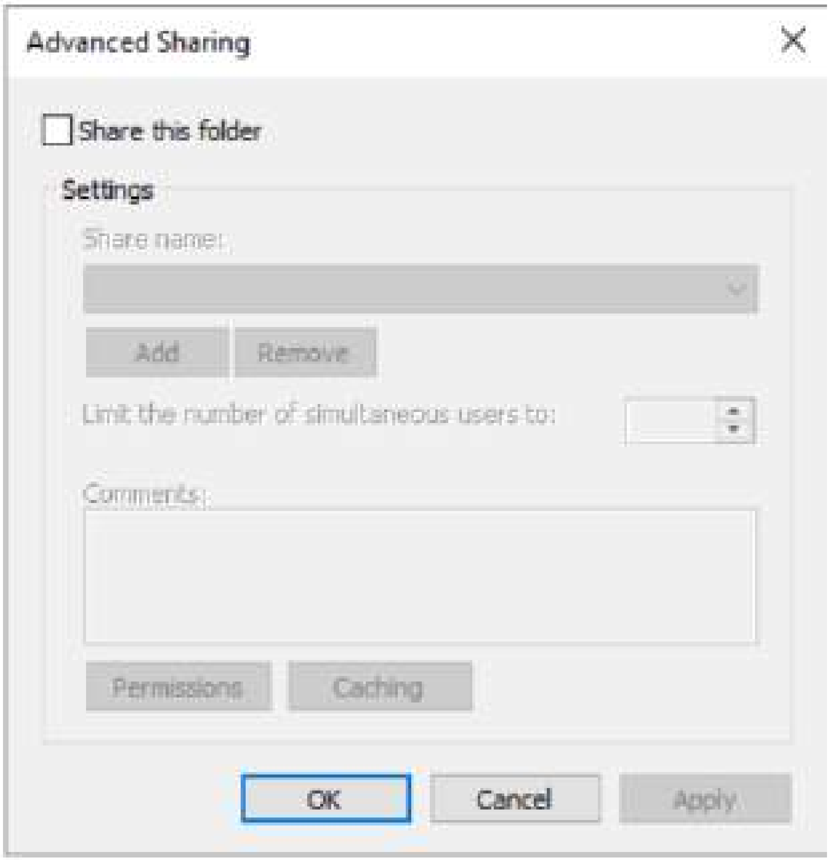
Type a name and then click Add, or click the arrow to find someone.

Everyone

Name	Permission Level
Administrator	Owner

- The dialog box looks like it does because I clicked the drop-down arrow to the left of the **Add** button and selected Everyone from the list. When I then clicked the **Add** button, the group "Everyone" was added to the list of those allowed to access my folder.

- When you add a person or a group to those permitted to access your folder, the permission level for your addition is set to "Read." If the group being added is "Everyone," then this allows everyone on the network to read from the shared folder. Clicking the down-arrow beside the Read setting (in the File Sharing dialog box) allows you to change the permission level to something else, such as to allow them to write to the folder. Once you've set the desired permission level, click the **Share** button to commit your changes.
- Sharing an entire disk drive is similar to sharing a folder, but the mechanics are a bit different. Under Windows Explorer, right-click the disk drive you want to share and choose **Share With | Advanced Sharing** or **Share | Advanced Sharing** (Windows 8). If you are using Windows 10, display File Explorer, right-click the disk drive you want to share and choose **Give Access to | Advanced Sharing**. Windows displays the Sharing tab of the disk drive's Properties dialog box, and you should click the **Advanced Sharing** button within the dialog box. Windows then displays the Advanced Sharing dialog box.



Advanced Sharing

□ Share this folder

- Click the Share this Folder check box (yes, I know it's not really a folder; it's a disk drive). You can then optionally change the Share Name. When ready to share, click **OK** to finish the process.

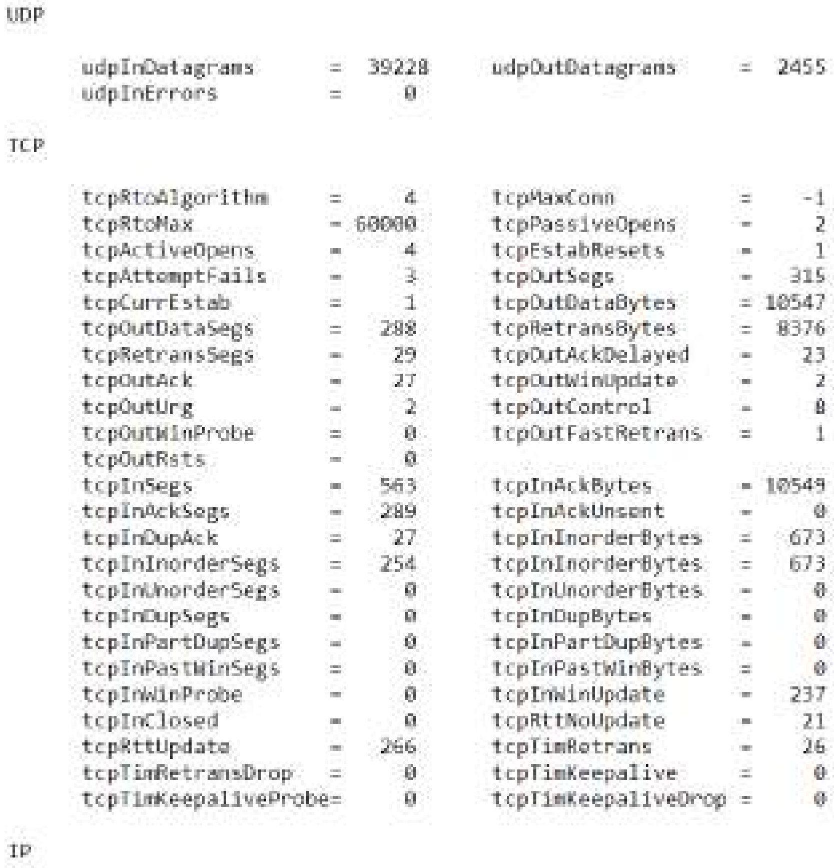
EXPERIMENT-8 Use of Netstat and its options.

netstat Command

- The netstat command generates displays that show network status and protocol statistics. You can display the status of TCP and UDP endpoints in table format, routing table information, and interface information.
- netstat displays various types of network data depending on the command line option selected. These displays are the most useful for system administration. The syntax for this form is:
- netstat [-m] [-n] [-s] [-i | -r] [-f address_family]
- The most frequently used options for determining network status are: s, r, and i.

Displaying Per Protocol Statistics

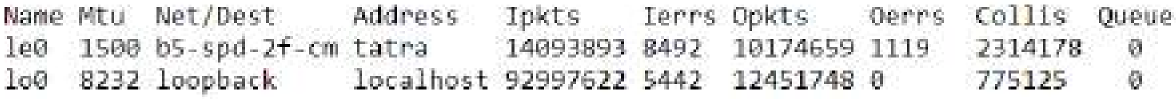
- The netstat -s option displays per protocol statistics for the UDP, TCP, ICMP, and IP protocols.



```
UDP

      udpInDatagrams      =  39228     udpOutDatagrams     =  2455
      udpInErrors         =      0

TCP

      tcpRtoAlgorithm     =      4     tcpMaxConn          =     -1
      tcpRtoMax           =  60000     tcpPassiveOpens     =      2
      tcpActiveOpens      =      4     tcpEstabResets      =      1
      tcpAttemptFails     =      3     tcpOutSegs          =    315
      tcpCurrEstab        =      1     tcpOutDataBytes     =  10547
      tcpOutDataSegs      =    288     tcpRetransBytes     =   8376
      tcpRetransSegs      =     29     tcpOutAckDelayed    =     23
      tcpOutAck           =     27     tcpOutWinUpdate     =      2
      tcpOutUrg           =      2     tcpOutControl       =      8
      tcpOutWinProbe      =      0     tcpOutFastRetrans   =      1
      tcpOutRsts          =      0
      tcpInSegs           =    563     tcpInAckBytes       =  10549
      tcpInAckSegs        =    289     tcpInAckUnsent      =      0
      tcpInDupAck         =     27     tcpInInorderBytes   =    673
      tcpInInorderSegs    =    254     tcpInInorderBytes   =    673
      tcpInUnorderSegs    =      0     tcpInUnorderBytes   =      0
      tcpInDupSegs        =      0     tcpInDupBytes       =      0
      tcpInPartDupSegs    =      0     tcpInPartDupBytes   =      0
      tcpInPastWinSegs    =      0     tcpInPastWinBytes   =      0
      tcpInWinProbe       =      0     tcpInWinUpdate      =    237
      tcpInClosed         =      0     tcpRttNoUpdate      =     21
      tcpRttUpdate        =    266     tcpTimRetrans       =     26
      tcpTimRetransDrop   =      0     tcpTimKeepalive     =      0
      tcpTimKeepaliveProbe=      0     tcpTimKeepaliveDrop =      0

IP
```

Displaying Network Interface Status

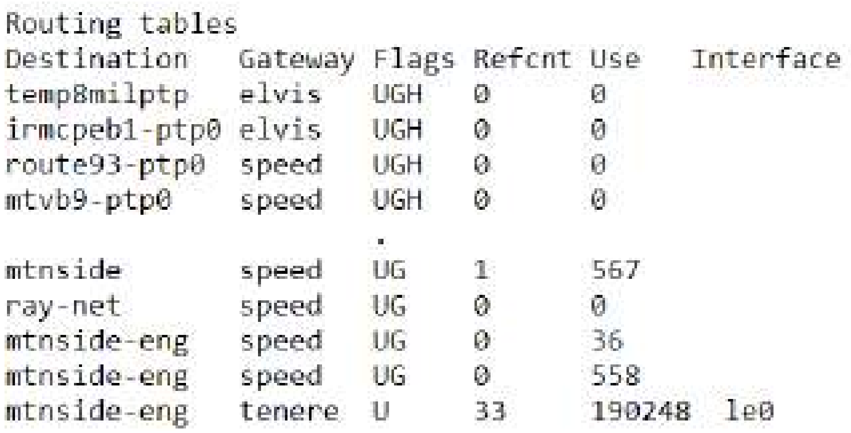
- The -i option of netstat shows the state of the network interfaces that are configured with the machine where you ran the command.



```
Name Mtu  Net/Dest     Address   Ipkts    Ierrs Opkts    Oerrs  Collis  Queue
le0  1500 b5-spd-2f-cm tatra     14093893 8492  10174659 1119   2314178   0
lo0  8232 loopback     localhost 92997622 5442  12451748 0      775125    0
```

Displaying Routing Table Status

- The -r option of netstat displays the IP routing table.



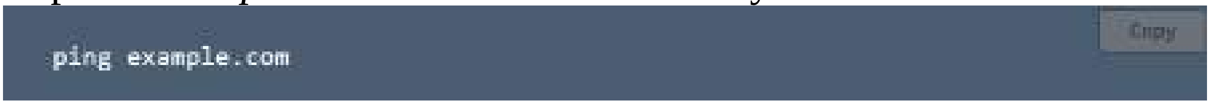
```
Routing tables
Destination    Gateway Flags Refcnt Use    Interface
temp8milptp    elvis   UGH   0      0
irmcpeb1-ptp0  elvis   UGH   0      0
route93-ptp0   speed   UGH   0      0
mtvb9-ptp0     speed   UGH   0      0
                       .
mtnside        speed   UG    1      567
ray-net        speed   UG    0      0
mtnside-eng    speed   UG    0      36
mtnside-eng    speed   UG    0      558
mtnside-eng    tenere  U     33     190248  le0
```

EXPERIMENT-9 Connectivity troubleshooting using PING, IPCONFIG

Testing network connectivity

Check host availability with ping test

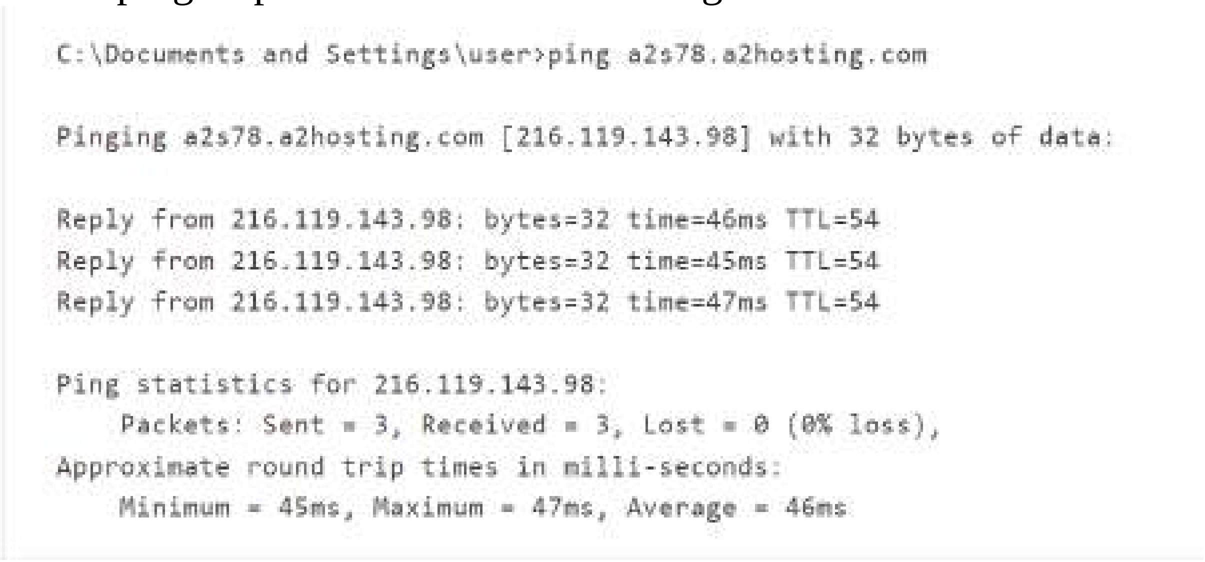
- To use the ping program on Microsoft Windows, follow these steps:
- Open a DOS command window. To do this, click Start, click Run, type cmd, and then press Enter.
- At the command prompt, type the following command. Replace *example.com* with the domain that you want to test:



```
ping example.com
```

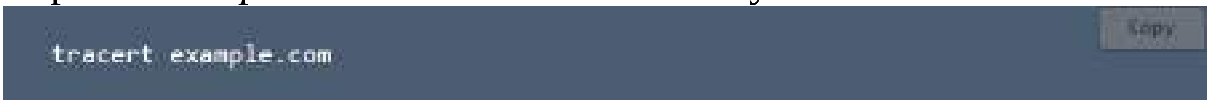
Interpret the output from ping:

- If the remote host is active and configured to respond to ping requests, responses appear. For example, the following output shows ping responses from an A2 Hosting server:



```
C:\Documents and Settings\user>ping a2s78.a2hosting.com

Pinging a2s78.a2hosting.com [216.119.143.98] with 32 bytes of data:

Reply from 216.119.143.98: bytes=32 time=46ms TTL=54
Reply from 216.119.143.98: bytes=32 time=45ms TTL=54
Reply from 216.119.143.98: bytes=32 time=47ms TTL=54

Ping statistics for 216.119.143.98:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 45ms, Maximum = 47ms, Average = 46ms
```

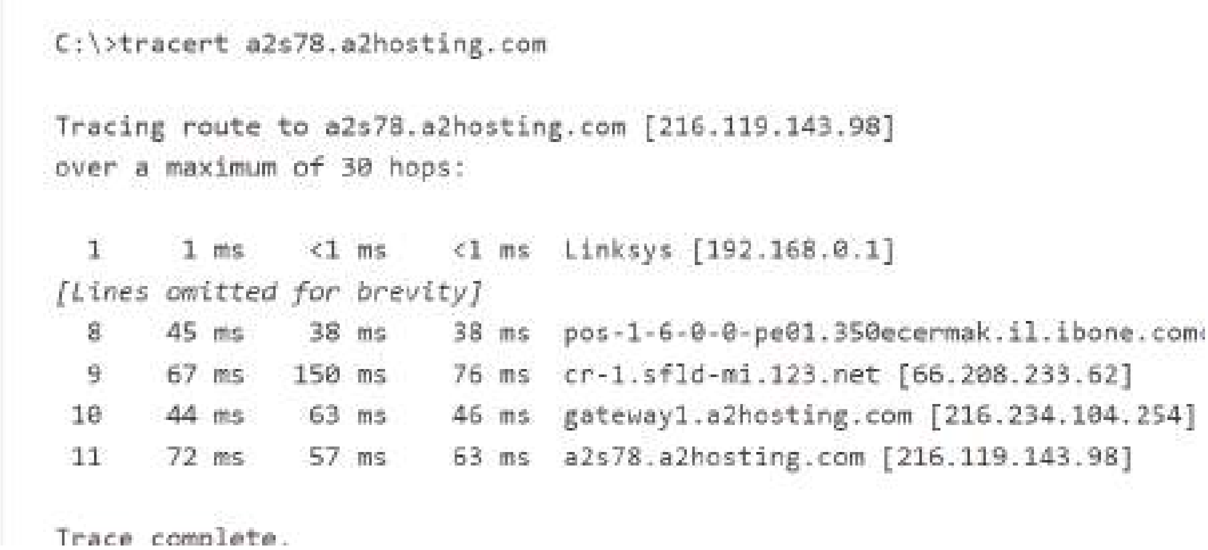
- Alternatively, if the remote host is down, or not configured to respond to ping requests, you do not see any responses.
- Testing the path to a remote host with traceroute
- The traceroute program provides much more detailed information about a connection to a remote host than ping. Traceroute (or *tracert* on Microsoft Windows systems) displays information about each "hop" a packet takes from your computer to the remote host. It is often a good way to pinpoint possible ISP connection issues or network bottlenecks.
- **Using tracert**
- On Windows-based systems, use the *tracert* program to test the path to a server. To do this, follow these steps:
- Open a DOS command window. To do this, click Start, click Run, type cmd, and then press Enter.
- At the command prompt, type the following command. Replace *example.com* with the domain that you want to test:



```
tracert example.com
```

Interpret the output from tracert:

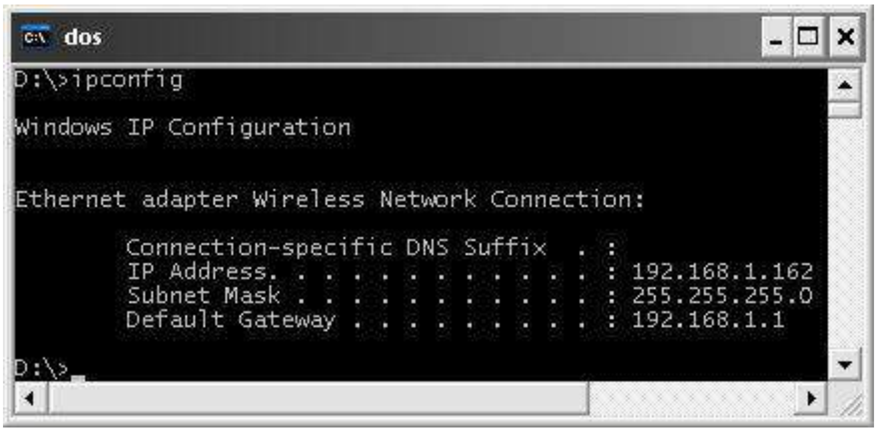
- tracert displays each hop, indicated by a number in the left column. It also displays the domain and IP address at each hop, as well as the time spent. For example, the following output shows the path to an A2 Hosting server:



```
C:\>tracert a2s78.a2hosting.com

Tracing route to a2s78.a2hosting.com [216.119.143.98]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  Linksys [192.168.0.1]
[Lines omitted for brevity]
  8    45 ms    38 ms    38 ms  pos-1-6-0-0-pe01.350ecermak.il.ibone.com
  9    67 ms   150 ms    76 ms  cr-1.sfld-mi.123.net [66.208.233.62]
 10    44 ms    63 ms    46 ms  gateway1.a2hosting.com [216.234.104.254]
 11    72 ms    57 ms    63 ms  a2s78.a2hosting.com [216.119.143.98]

Trace complete.
```

- You can examine the times between each hop to look for places where the connection “hangs”. In some cases, tracert may also time out, which is indicated by an asterisk (*****).

The ipconfig Command Basics:



```
D:\>ipconfig

Windows IP Configuration


Ethernet adapter Wireless Network Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.162
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

D:\>
```

- Used to find the local IP address assigned to your computer or the MAC address of your Ethernet Adapter

Here are some different options of this command:

- ipconfig /? : Displays all available options.
- ipconfig /all : This will display output as shown on the screenshot above but for ALL network connection adapters of the computer (Wired Ethernet, WiFi, Vmware adapters etc).
- ipconfig /release : This will release the current IPv4 addresses which were assigned dynamically from a DHCP server. If you specify also a connection name at the end, it will release only the IP of that connection adapter.
- **nslookup command:**
- “nslookup” stands for “Name System Lookup” and is very useful in obtaining Domain Name System (DNS) related information about a domain or about an IP address (reverse DNS lookup).
- nslookup [domain name]: The most popular usage of this command is to find quickly the IP address of a specific domain name (A-record) as shown below:
  Example:
  nslookup www.ucpesbam.in

- nslookup [IP Address]: This will perform a reverse-DNS lookup and will try to match the given IP address in the command with its corresponding domain name.
  Example:
  nslookup 8.8.8.8

EXPERIMENT-10 Installation of Network Operating System(NOS)

- A network operating system (NOS) is a computer operating system (OS) that is designed primarily to support workstations, personal computers and, in some instances, older terminals that are connected on a local area network (LAN).
- Network Operating System is a computer operating system that facilitates to connect and communicate various autonomous computers over a network.
- There are mainly two types of Network O.S., they are:
- **Peer-to-Peer**
- Peer-to-Peer Network Operating System is an operating system in which all the nodes are functionally and operationally equal to each other.
- **Client-Server**
- The Client-Server Networking Operating System operates with a single server and multiple client computers in the network. The Client O.S. runs on the client machine, while the Network Operating System is installed on the server machine.

Installing NOS Network operating system (NOS): Installation is the process of creating and copying NOS system files to a hard disk.By purchasing a PC or server with a preinstalled OS, a customer avoids the complex process of installation and configuration.The drawback is that a customer may not be able to control the exact features, packages, and configuration of the OS or NOS.NOS administrators usually prefer to have direct control of software versions, updates, and patches installed on the system.

- **Planning the System The NOS installation should be carefully prepared.**
  There is no NOS that works with all computer hardware, so determine whether the currently available hardware will work with the NOS.Determine if the NOS supports all application

software that will be loaded on the system.Become familiar with the NOS itself. As part of the installation process, important configuration decisions will have to be made.

- **Planning Hardware Installation**

  Verify that everything specified in the installation plan is ready and available before beginning the installation.Activities include:Verifying the Installation SiteVerifying the Power SourceVerifying the UPS SizeAdequate Temperature in a Server RoomVerifying the Network Connection

- **Server Hardware Components**

  Check the components that will be used to assemble the network server.Some vendors do not assemble all the hardware for a network server when they are ordered.Verify that the server chassis is the correct model that was ordered and the correct form factor.Most server chassis are either of a tower configuration, a wide- or “fat-” tower configuration, or a rack-mount configuration.

- **Server Hardware Components**

  A rack-mount server chassis must be mounted in an equipment rack designed for rack-mounted hardware.The racks generally come in several sizes (heights).The rack size is measured in rack units (U) and a standard rack unit is 1.75 inches.

- **Server Hardware Components**

  Verify that the following products are ordered:A monitor that supports VGA resolution of at least 1024 by 768 dots per inch (dpi)UPS is available for the network serverAn adequate backup systemThe correct cables have been delivered to connect the SCSI channel controller to the disk drivesThe correct number and type of processors are available with memory for them to adequately perform their functionThe correct SCSI adapter and RAID controllerThe correct Fibre Channel host bus adapter

(HBA)The network interface card (NIC)Other hardware that might be required for the network server

- **Hardware Requirements**

  The most current versions of popular NOSs, such as Windows XP and Red Hat 7, can only run on certain hardware configurations.When choosing an NOS version to install, verify that the key elements of the system hardware meet the minimum requirements of the NOS.CPU type (architecture)CPU speedAmount of RAMAmount of available hard disk space

- **Creating a Hardware Inventory**

  The hardware inventory should be created before any installation programs are run or before any attempt to prepare the hard disk for installation.The hardware inventory should include the following for each device:Device typeManufacturerModel numberDevice driver versionBIOS revision numberExpansion cards and peripheral devices attached to the system

- **Creating a Hardware Inventory**

  Some installations may require more details about the hardware, such as the slot where an expansion card is located, or even the jumper settings on a particular card.Most of this information can be obtained by using a utility such as Device Manager.

- **Identifying Hardware Using Device Manager**

  In Windows 2000 the device appears with a yellow question mark next to the device name in Device Manager.The easiest way to identify if the hardware driver has not been installed is to look at the device and if it has a question mark in a yellow circle next to it.This icon means Windows 2000 recognized the device but could not find a suitable driver for it.

- **Checking Hardware Compatibility Lists**

  Check with the NOS and hardware manufacturers to verify that the hardware is compatible with the NOS.While software and hardware manuals may contain compatibility information, the most up-to-date source of this information is the World Wide Web.The Red Hat website offers a hardware compatibility list.

- **Verifying the Network:** To test network connectivity when using the TCP/IP protocol, all network operating systems use the ping command.Here are successful ping commands using a TCP/IP address in Windows and LinuxHere are unsuccessful ping commands in Windows and Linux.
- **The Installation Process**
- Installation MediaTypically, a NOS is installed using a CD-ROM that contains the system files and an installation program.In some cases, a NOS is installed via floppy disks.If a high-speed Internet connection is available, it may be possible to install a version of Windows, UNIX, or Linux over a network.With a LAN connection, it is possible to install most NOSs using the local network.
- BIOS SettingsThe Basic Input/Output System (BIOS) typically resides in ROM on the motherboard and is the first program run when a system is powered on.It is responsible for testing hardware devices using a process called Power-On Self Test (POST).The BIOS also loads the operating system from various media, including hard disks, floppy disks, and usually CD-ROMs.
- **The Installation Program**

  An installation program controls and simplifies the installation process.Depending on the NOS, the installation program prompts the user for configuration information.Most installation programs allow partitioning and formatting of the hard disk before copying system files. Partitioning and formatting are discussed in the next few sections.
- **The Installation Program**

  In Windows, the installation program is called setup.exe.On a Red Hat Linux system, the installation program is currently called Anaconda.These programs guide the user through the NOS installation process.

- **The Installation Program**

  Installation programs also give the user the option to install a default set of components or choose each component manually.If installing a NOS for the first time, or installing a NOS on a non-production server, consider using one of these defaults. Using a default setting simplifies the installation process and ensures that a crippled or non-functioning system will not be created.
- **The Installation Program**

  If the server is going to be put into production, strongly consider a custom installation.Manually choosing the components and features will guarantee that the system is built for the specific tasks required in a specific environment.
- **Disk partitions**: In order to efficiently use the storage space on a hard disk, the disk is divided into sections called partitions or slices.Each partition, or slice, is a logical division of the hard disk. A disk can have one or more partitions.Typically, a network server is configured with multiple partitions before installing the NOS.
- A system with multiple disk partitions has the following advantages:Multiple operating systems can be installed on the same disk. Data can be physically separated from the system files to provide security, file management, and/or fault tolerance.A specific partition, called a "swap" partition, can be created in order supplement the system RAM and enhance performance.
- Partitioning a diskOn systems that use a DOS-type partition table, such as Windows and Linux, the first sector of the disk is called the Master Boot Record (MBR) or the Master Boot Sector.If the MBR or disk label is corrupted or otherwise lost, the system will no longer boot properly. For this reason, a copy of the MBR/disk label should be kept as a backup on a floppy disk.

- Partitioning ToolsMost NOS installation software includes a program called FDISK. FDISK stands for fixed disk. FDISK programs are designed to manipulate the partition table of a hard disk. A FDISK program can be used to create partitions, delete partitions, and set partitions as "active".Linux provides a version of FDisk as well, although the version that Linux uses is fdisk, with all lowercase letters. The Linux version of fdisk is test-based as well but provides a more flexible means of partitioning a hard disk than does Microsoft version.
- Partitioning ToolsLinux provides its own tools that can be used when installing a Linux-only system. These are GUI tools that are much more easier to use than fdisk. There are some third party tools that can be used to partition a Linux system. The best-known tool for doing this is PowerQuest PartitionMagicFIPS is a partitioning tool is included in the installation CD that come with most of the Linux distributions. First Nondestructive Interactive Partitioning Splitting (FIPS) is a large partitioning tool that can be used to split a FAT partition into two partitions. FIPS is most commonly used on Windows systems that need to make a separate partition to install Linux on. FIPS does this by first splitting the existing FAT partition. Then you can delete that partition and installing Linux on that new partition.
- Swap FilesA swap file is an area of the hard disk that is used for virtual memory. Virtual memory is hard disk space that is used to supplement RAM.
- Swap FilesAlthough Windows uses a swap file, it does not have to be configured. The swap file is created as a file in the NOS partition.UNIX systems typically dedicate an entire partition to swap space. This partition, or slice, is called the swap partition. The minimum size of the swap partition should be equal to twice the computer RAM, or 32 MB, whichever amount is larger, but no more than 128 MB on a Red Hat Linux system.
- Formatting the DiskWhen formatting a partition on a Windows NOS, choose between the following file systems:· NTFS (New Technology File System) – Recommended for network servers· FAT32· FAT When formatting a UNIX or Linux

partition, choose between the following file systems:· UFS (UNIX File System)· EXT3

- **Creating an Initial Administrative Account** The administrative account has unrestricted access to create and delete users and files.An administrative account is very powerful and requires a "strong" password. A password is considered strong when it contains eight characters or more and does not use recognizable names or words found in a dictionary. Strong passwords also use a combination of upper and lowercase letters, numbers, and other characters.For example: is a stronger password than buccaneer03!
- **Completing the Installation**

  After providing the installation program with the necessary information, the program will create the NOS system files on the hard disk.Other basic applications and components will also be copied to the hard disk, as determined by the installation program.Depending on the size of the NOS, the number of selected components, and the speed of server, it can take from a few minutes to over an hour to complete the copying process.
- **The Boot Process**
- **The Steps of the Boot Process**

  The Windows 2000 boot process occurs in five stages:Step 1. The pre-boot sequenceStep 2. The boot sequenceStep 3. The kernel loadStep 4. The kernel initializationStep 5. The logon process
- 34 Basic Files RequiredThe following is a list of major files that a Windows 2000 system needs in order to boot properlyNTLDRBoot.iniBootsect.dos (only if dual booting)Ntdetect.comNtbootdd.sysNtoskrnl.exeHal.dllSYSTEM registry keyDevice drivers
- **BIOS Interaction BIOS controls all aspects of the boot process.**
  The instructions and data in the ROM chip that control the boot process and the computer hardware are known as the Basic Input/Output System (BIOS).The Power On Self Test (POST):

During the POST, a computer will test its memory and verify that it has all the necessary hardware, such as a keyboard and a mouse. This information is used by the BIOS to control all aspects of the boot process.

Detailed Steps of the Boot Process

Step 1. Pre-boot SequenceThe first step of the boot process is the POST. This is actually something that every computer will do, regardless of its operating system.After the computer completes the POST, it will allow for other adapter cards to run their own POSTs, such as a SCSI card that is equipped with its own BIOS, for example.After the POST routine is complete, the computer will locate a boot device and load the Master Boot Record (MBR) into memory, which in turn locates the active partition and loads it into memory.

Step 2. Boot SequenceOnce the computer loads NTLDR, the boot sequence begins to gather information about hardware and drivers.NTLDR uses the Ntdetect.com, boot.ini, and bootsect.dos files. The bootsect.dos file will only be used in the event that the computer is set up to dual-boot.A major function provided by NTLDR is switching the processor into 32-bit flat memory mode.

Step 3. Kernel LoadThe kernel load phase begins with Ntoskrnl.exe loading along with the file. At this point NTLDR still plays a role in the boot process.NTLDR will also read the system registry key into memory, and select the hardware configuration that is stored in the registry. It will load the configuration needed for the computer to boot.

Step 4. Kernel InitializationThe initial kernel load phase is now complete and the kernel will begin to initialize.Four additional steps will now take place:The hardware key is createdThe clone control set is createdDevice drivers are loaded and initializedServices are started

Step 5. LogonThe Logon screen begins the final step in the boot-up process. Although this is the final step, it is not considered a completed or successful boot until a user logs on.

- Linux Boot ProcessThe boot process between Windows 2000 and Linux is very similar.One main difference is the file types that are used. The names of the files types that are used to boot the two systems may be different, but they essentially perform the same functions.In the end, both systems will come to a logon prompt that will ask for a username and password to authenticate into the system.
- **Troubleshooting NOS Installation**
- **Unable to Boot from Installation Media** There are several steps to take if the system will not boot from a CD-ROM:Consult the system Basic Input/Output System (BIOS) setup menu. A hotkey sequence is generally required to enter the BIOS monitor.Make sure that the BIOS is capable of supporting and booting from a CD-ROM, and that the correct boot sequence is configured in BIOS.Consult the documentation that came with the CD. Make sure the CD contains system files and is designed to be bootable.
- **Unable to Boot from Installation Media (cont.)** Check that the CD is recognized by the operating system and proper device drivers are available.Check to see if another system can boot from the CD or read the CD.Inspect the data side for scratches, fingerprints, or dust, if it is suspected that the problem is with the disc itself.Determine if the problem is with the CD-ROM drive.
- **Problems During the Installation Process** When something goes wrong during the installation process, use the "back" button or key so the configuration can be reversed. Here are some other common problems:Partitioning or formatting the hard disk fails. Check the BIOS settings and hard disk documentation to troubleshoot this problem.The system "hangs" during the installation process. A hang is defined, as a period of several minutes during which there is no discernable activity on the system.The installation media cannot be read at some point during the installation process. This problem occurs when installing with a CD that is dirty or scratched.
- **Post-installation Problems**

After installing the Network Operating System (NOS), the system may not load the NOS properly or will not allow a logon.If the system fails to load the NOS, consult the manufacturer website and documentation. First time load failures are difficult to troubleshoot.

- Very specific information about the system and the NOS will need to be gathered. If the system reports specific errors, write those down and search for information about those errors on the web or in the documentation. If necessary, call a technical support line and ask for help.If unable to logon, the problem is usually forgotten administrator account information that was configured during the installation process.