LABORATORY MANUAL ON NETWORKING LAB(NW LAB) (PR-2)

(4TH SEM CSE/IT)

PREPARED BY

SMT REETANJALI PANDA

LECTURER,UCPES,

BERHAMPUR

COURSE CONTENT OF NETWORKING LAB AS PER SYLLABUS

LIST OF PRACTICALS:-

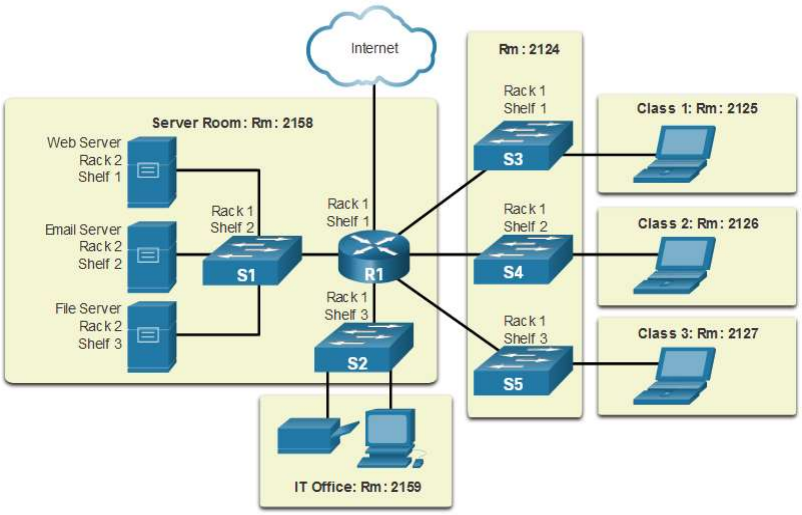
1. Recognize the physical topology and cabling (coaxial, OFC, UTP, STP) of a network.
2. Recognition and use of various types of connectors RJ-45, RJ-11,BNC and SCST
3. Making of cross cable and straight cable
4. Install and configure a network interface card in a workstation.
5. Identify the IP address of a workstation and the class of the address and configure the IP Address on a workstation
6. Managing user accounts in windows and LINUX
7. Sharing of Hardware resources in the network.
8. Use of Netstat and its options.
9. Connectivity troubleshooting using PING, IPCONFIG
10. Installation of Network Operating System(NOS)
11. Create a network of at least 6 computers.
12. Study of Layers of Network and Configuring Network Operating System
13. Study of Routing and Switching, configuring of Switch and Routers, troubleshooting of networks
14. Study of Scaling of Networks, Design verities of LAN and forward of Traffic
15. Study WAN concepts and Configure and forward Traffic in WAN
16. Configure IPv4 and IPv6 and learn Quality, security and other services
17. Learn Network programming
18. Troubles shoot Networks.

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

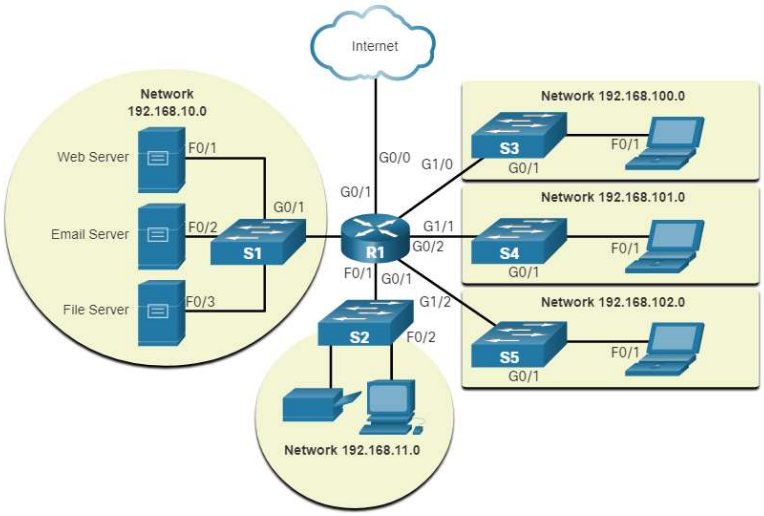
Network Representations and Topologies

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:

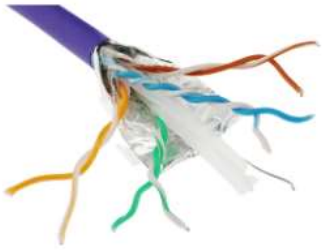
- Attenuation – the longer the electrical signals have to travel, the weaker they get.
- The electrical signal is susceptible to interference from two sources, which can distort and corrupt the data signals (Electromagnetic Interference (EMI) and Radio Frequency Interference (RFI) and Crosstalk).

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

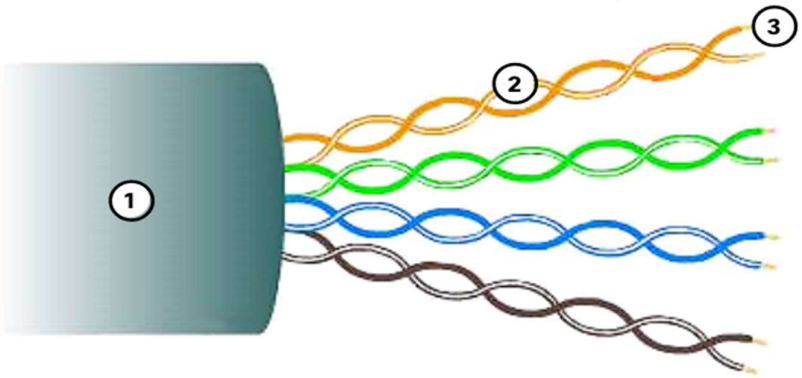
Unshielded Twisted-Pair (UTP) Cable



Shielded Twisted-Pair (STP) Cable

Coaxial Cable

Unshielded Twisted Pair (UTP)

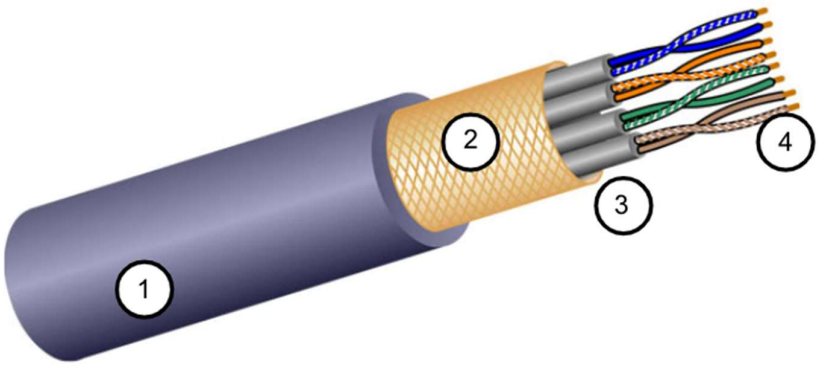


- UTP is the most common networking media.
- **Terminated with RJ-45 connectors**
- Interconnects hosts with intermediary network devices.

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)



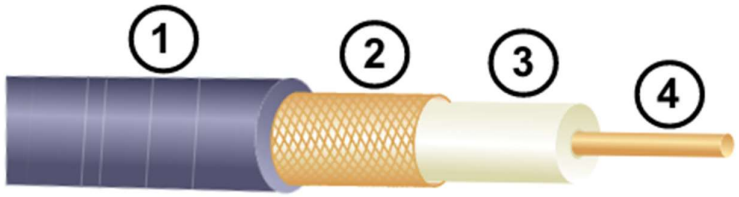
- Better noise protection than UTP
- More expensive than UTP
- Harder to install than UTP
- **Terminated with RJ-45 connectors**
- Interconnects hosts with intermediary network devices

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:

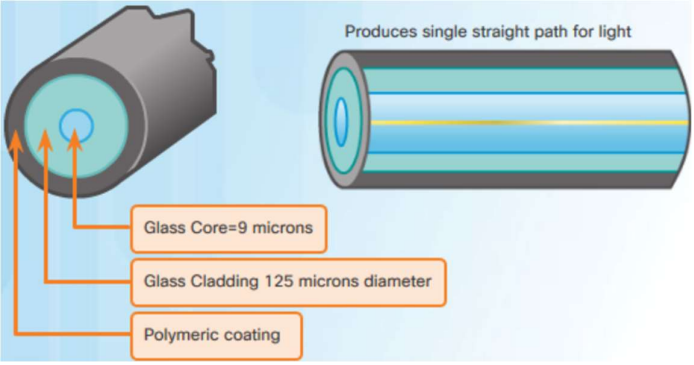
1. Outer cable jacket to prevent minor physical damage
2. A woven copper braid, or metallic foil, acts as the second wire in the circuit and as a shield for the inner conductor.
3. A layer of flexible plastic insulation
4. A copper conductor is used to transmit the electronic signals.
5. **BNC connectors**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

Fiber-Optic Cabling

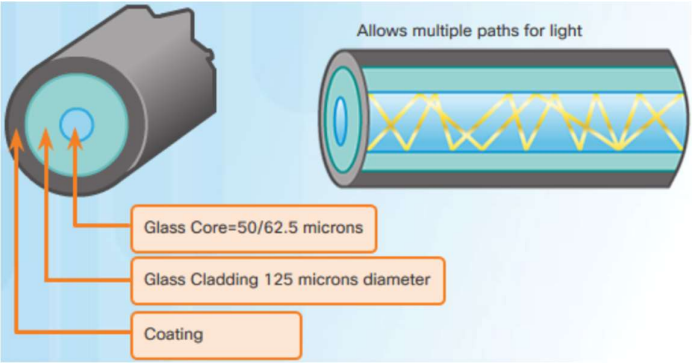
Properties of Fiber-Optic Cabling

- 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



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



- 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)

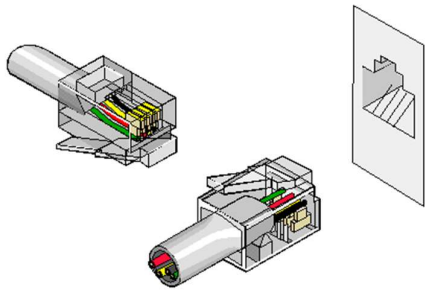
RJ-45 Connector

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

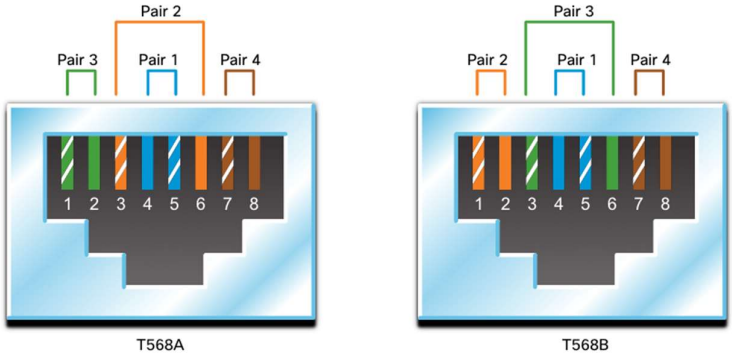
Subscriber Connector (SC) Connectors

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 (push-pull) 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

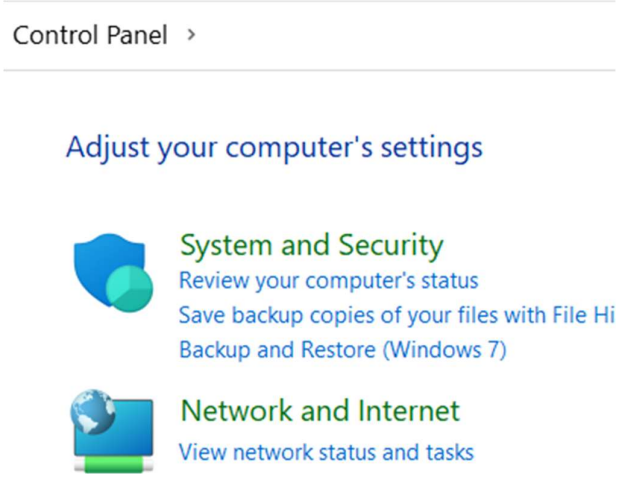
EXPERIMENT-4 Install and configure a network interface card in a workstation.

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.



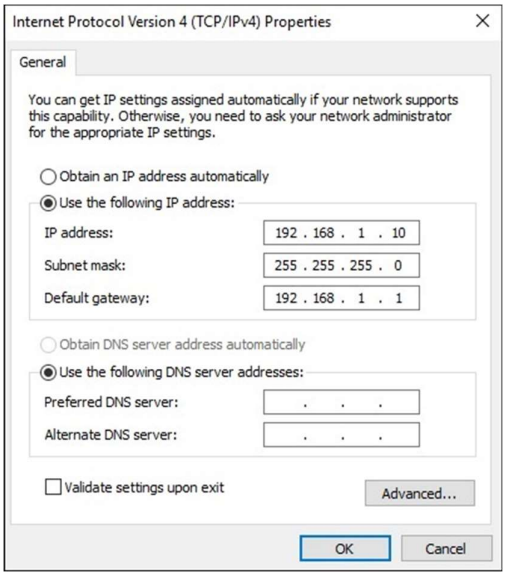
EXPERIMENT-5 Identify the IP address of a workstation and the class of the address and configure the IP Address on a workstation .

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

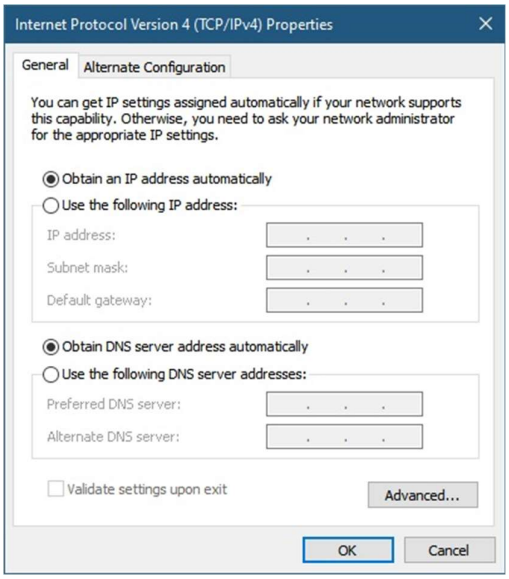
select Properties to display the Local Area Connection Properties.

- 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.



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.



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

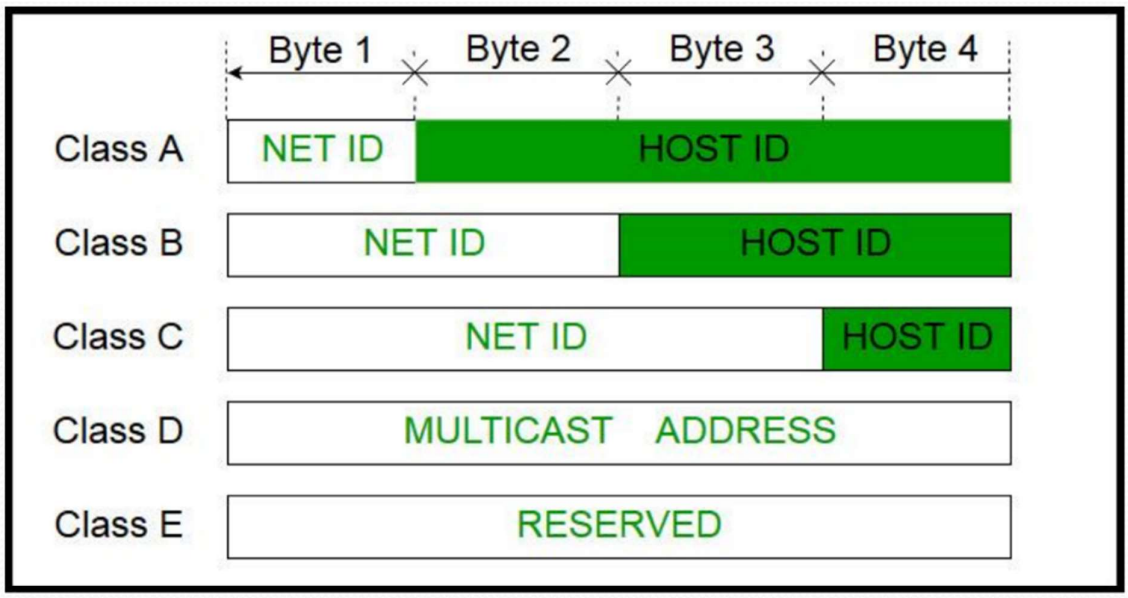
  Class A: It uses first octet for network addresses and last three octets for host addressing.

  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

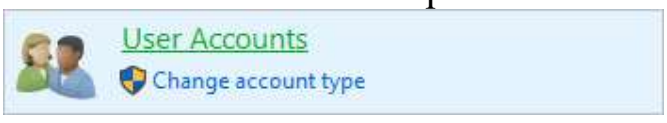
	First byte	Second byte	Third byte	Fourth byte
Class A	0–127			
Class B	128–191			
Class C	192–223			
Class D	224–239			
Class E	240–255			

b. Dotted-decimal notation

EXPERIMENT-6 Managing user accounts in windows and linux

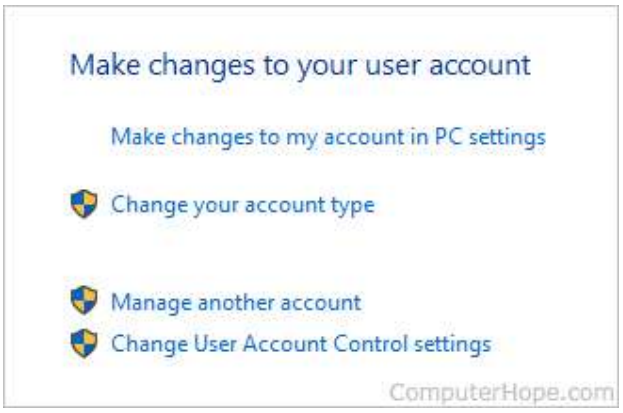
Windows 10 and 11

Press the Windows key, type Control Panel, and then press Enter.
Click the User Accounts option in the Control Panel.



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

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.



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.

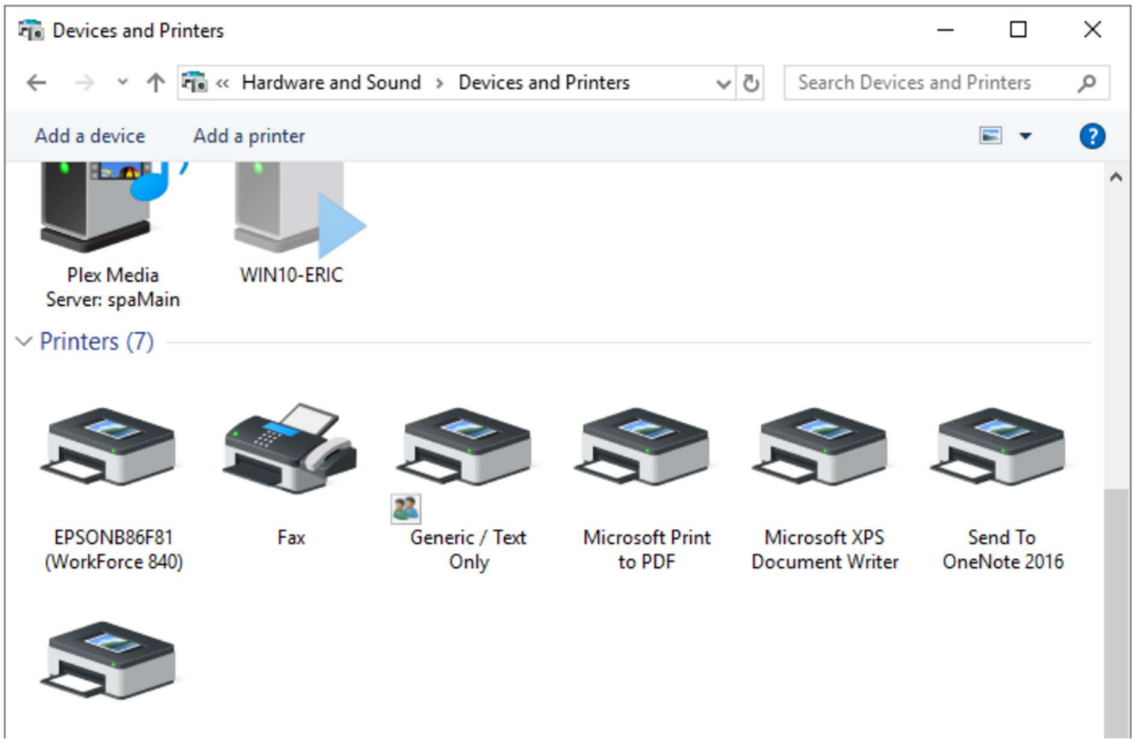
Linux

- 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.

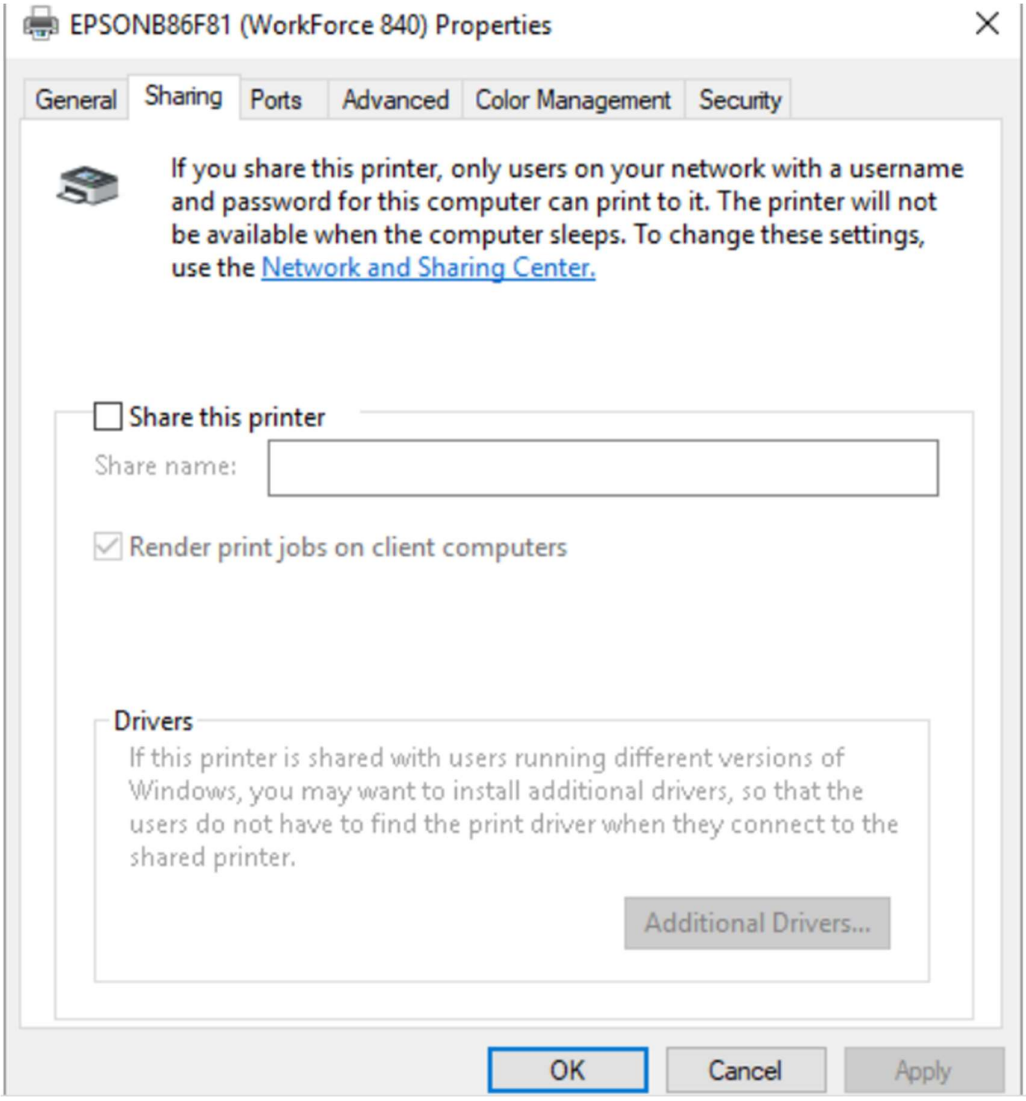
EXPERIMENT-7 Sharing of Hardware resources in the network.

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.



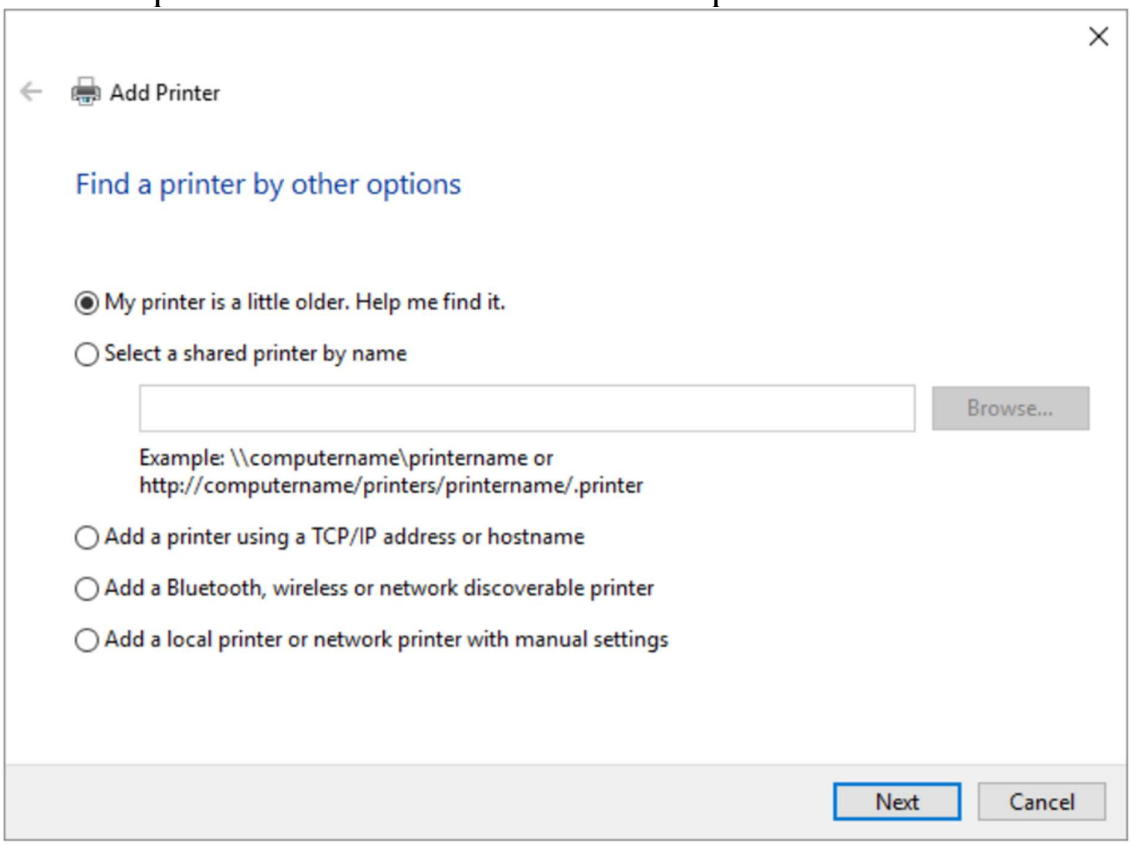
- Right-click the printer you want to share and select Printer Properties from the Context menu. Windows displays the Properties dialog box for the selected printer. The contents of the dialog box vary depending on the capabilities of your printer. Make sure the Sharing tab is displayed.



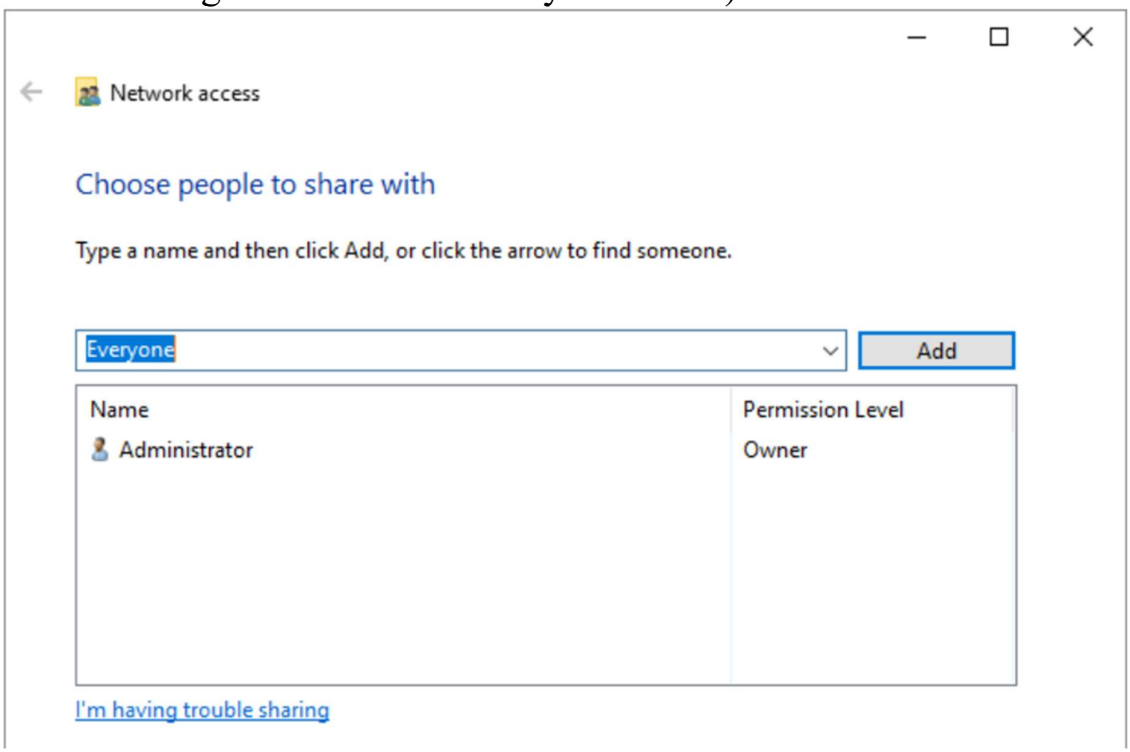
- Click the Share this Printer check box and optionally change the Share Name of the printer. Depending on the configurations of your particular systems you may either check or uncheck the Render Print Jobs on Client Computers check box. If checked, then all the processing required prior to queuing the 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.



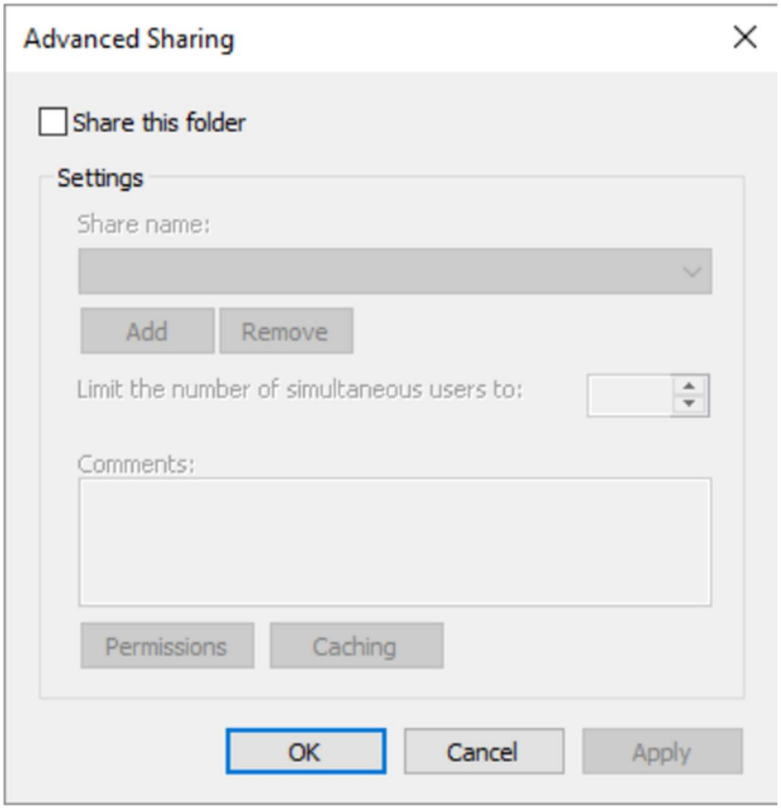
- **File Folders and Disk Drives**
- File folders and entire disks can also be shared among network-connected systems, and the procedure is similar to that of sharing a printer. Using Windows Explorer, right-click the folder you want to share with others on the network and select **Share With | Specific 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.)



- 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.



- 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
```

Copy

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
```
Copy

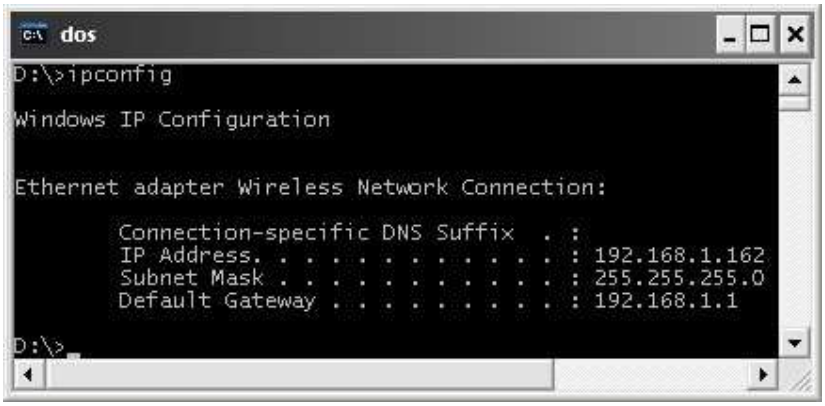
Interpret the output from tracert:

- 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:



- 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

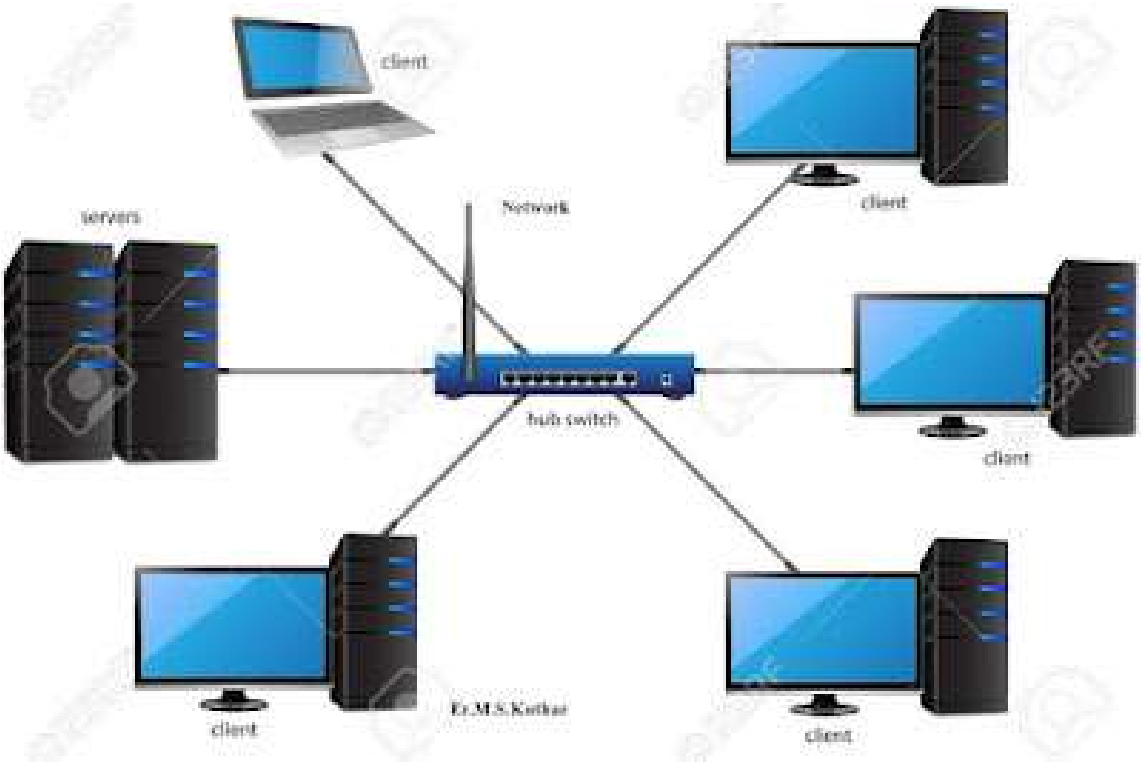
Step 5. LogonThe Logon screen begins the final step in the boot-up process. Although this is the final step, it is not considered a completed or successful boot until a user logs on.

- 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.

11. Create a network of at least 6 computers.

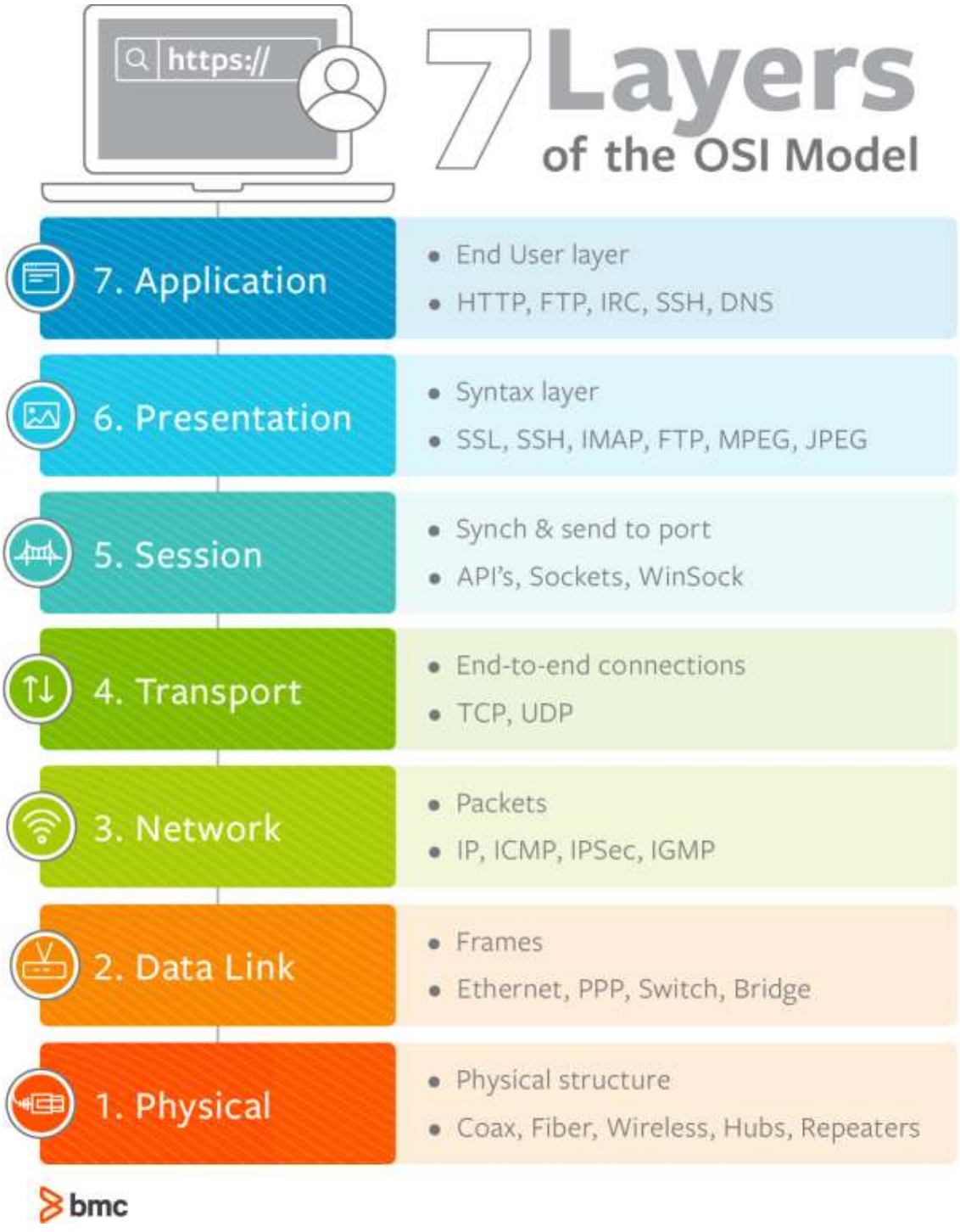


PROCEDURE:

- Take the computer for which you are making server, insert the second LAN in that computer.
- Connect your internet connection into the first LAN (inbuilt) on that computer.
- Enter the IP address which you got from your ISP and check whether you can able to use internet on that system.
- Now make sure that the second LAN is detected and is showing Unplugged.
- Open properties of the first LAN (inbuilt LAN) and then go to "Advanced" option which is available on the top, then check both the boxes and say ok. and close everything.
- Now take an Internet cable which is crimped on both the sides with same colors of wires.
- Connect one end to the second LAN and the other end to the switch.

- Now open your second LAN properties and go to the TCP/IP properties and there enter IP address as (192.168.0.1) or anything you wish Subnet Mask (255.255.255.0) and the gateway as (192.168.0.1).
- Now open click on the switch and you will get a notification on your server saying that "Local Area Connection 2" is connected.
- Now take an another Internet cable and one end of that cable should be in any one port of the Switch and the other should be in the second computer.
- Now you will get a notification that you are connected to internet, open the LAN properties and enter the IP address as (192.168.0.2) subnet mask and gateway should be same as server. say ok
- You will now be able to browse Internet on that particular system now.
- Do the same with the rest of the systems.
- And one more thing should be kept in mind that is you wont be able to browse internet Unless or Until your Server Pc is turned ON.
- NOTE :- THE GATEWAY SHOULD BE SAME AS THE IP ADDRESS ONLY FOR THE SERVER.
- NOTE :- THE IP ADDRESSES SHOULD NOT BE USED SAME FOR TWO SYSTEMS. SO BETTER GO WITH 192.168.0.1 (FOR SERVER) 192.168.0.2 (1ST CLIENT) 192.168.0.3(SECOND CLIENT) AND SO ON.....BUT THE SUBNET MASK AND GATEWAYS SHOULD BE SAME FOR ALL THE CLIENT AND SERVER SYSTEM.

12. Study of Layers of Network and Configuring Network Operating System



- **1. Physical Layer**
- The lowest layer of the OSI model is concerned with data communication in the form of electrical, optic, or electromagnetic signals physically transmitting information between networking devices and infrastructure. The physical layer is responsible for the communication of unstructured raw data streams over a physical medium. It defines a range of aspects, including:

- Electrical, mechanical, and physical systems and networking devices that include specifications such as cable size, signal frequency, voltages, etc.
- Topologies such as Bus, Star, Ring, and Mesh
- Communication modes such as Simplex, Half Duplex, and Full Duplex
- Data transmission performance, such as Bit Rate and Bit Synchronization
- Modulation, switching, and interfacing with the physical transmission medium
- Common protocols including Wi-Fi, Ethernet, and others
- Hardware including networking devices, antennas, cables, modem, and intermediate devices such as repeaters and hubs
- **2. Data Link Layer**
- The second layer of the OSI model concerns data transmission between the nodes within a network and manages the connections between physically connected devices such as switches. The raw data received from the physical layer is synchronized and packaged into data frames that contain the necessary protocols to route information between appropriate nodes. The data link layer is further divided into two sublayers:

- The Logical Link Control (LLC) sublayer is responsible for flow controls and error controls that ensure error-free and accurate data transmission between the network nodes.
- The Media Access Control (MAC) sublayer is responsible for managing access and permissions to transmit data between the

network nodes. The data is transmitted sequentially and the layer expects acknowledgement for the encapsulated raw data sent between the nodes.

- **3. Network Layer**
- The third layer of the OSI model organizes and transmits data between multiple networks.

- The network layer is responsible for routing the data via the best physical path based on a range of factors including network characteristics, best available path, traffic controls, congestion of data packets, and priority of service, among others. The network layer implements logical addressing for data packets to distinguish between the source and destination networks.

- Other functions include encapsulation and fragmentation, congestion controls, and error handling. The outgoing data is divided into packets and incoming data is reassembled into information that is consumable at a higher application level. Network layer hardware includes routes, bridge routers, 3-layer switches, and protocols such as Internet (IPv4) Protocol version 4 and Internet Protocol version 6 (IPv6).

- **4. Transport Layer**
- The fourth layer of the OSI model ensures complete and reliable delivery of data packets.

- The transport layer provides mechanisms such as error control, flow control, and congestion control to keep track of the data packets, check for errors and duplication, and resend the information that fails delivery. It involves the service-point addressing function to ensure that the packet is sent in response to a specific process (via a port address).
- Packet Segmentation and reassembly ensure that the data is divided and sequentially sent to the destination where it is rechecked for integrity and accuracy based on the receiving sequence.

- Common protocols include the Transmission Control Protocol (TCP) for connection-oriented data transmission and User Datagram Protocol (UDP) for connectionless data transmission.

- **5. Session Layer**
- As the first of three layers that deal with the software level, the session layer manages sessions between servers to coordinate communication. Session refers to any interactive data exchange between two entities within a network. Common examples include HTTPS sessions that allow Internet users to visit and browse websites for a specific time period. The Session Layer is responsible for a range of functions including opening, closing, and re-establishing session activities, authentication and authorization of communication between specific apps and servers, identifying full-duplex or half-duplex operations, and synchronizing data streams.

- Common Session Layer protocols include:
- Remote procedure call protocol (RPC)
- Point-to-Point Tunneling Protocol (PPTP)
- Session Control Protocol (SCP)
- Session Description Protocol (SDP), as described here
- **6. Presentation Layer**
- The sixth layer of the OSI model converts data formats between applications and the networks. Responsibilities of the presentation layer include:

- Data conversion
- Character code translation
- Data compression
- Encryption and decryption
- The presentation layer, also called the syntax layer, maps the semantics and syntax of the data such that the received information is consumable for every distinct network entity. For example, the data we transfer from our encryption-based

communication app is formatted and encrypted at this layer before it is sent across the network.

- At the receiving end, the data is decrypted and formatted into text or media information as originally intended. The presentation layer also serializes complex information into transportable formats. The data streams are then deserialized and reassembled into original object format at the destination.

- **7. Application Layer**
- The application layer concerns the networking processes at the application level. This layer interacts directly with end-users to provide support for email, network data sharing, file transfers, and directory services, among other distributed information services. The upper most layer of the OSI model identifies networking entities to facilitate networking requests by end-user requests, determines resource availability, synchronizes communication, and manages application-specific networking requirements. The application layer also identifies constraints at the application level such as those associated with authentication, privacy, quality of service, networking devices, and data syntax.

Configuring Network Operating System

Navigate the IOS
Primary Command Modes

- The user EXEC mode allows only a limited number of basic monitoring commands.
- Often referred to as “view-only” mode.
- By default, there is no authentication required to access the user EXEC mode but it should be secured.
- The privileged EXEC mode allows the execution of configuration and management commands.
- Often referred to as “enable mode” because it requires the enable user EXEC command.

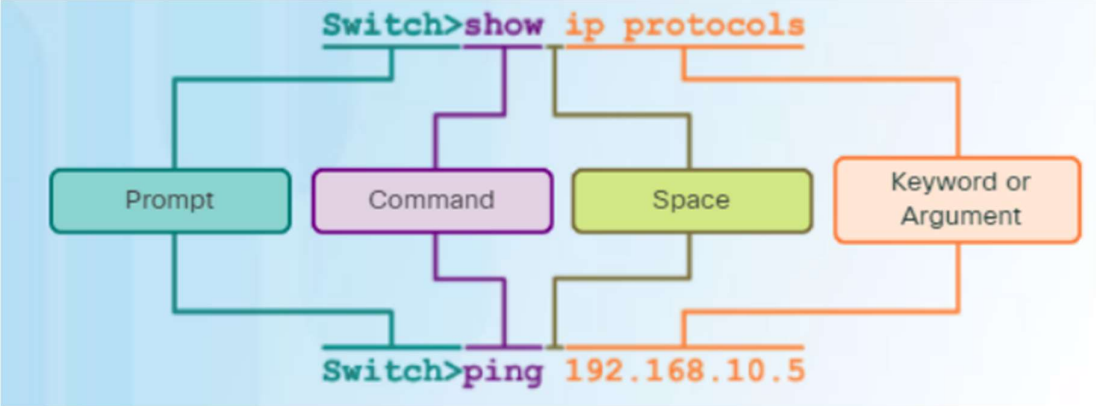
- By default, there is no authentication required to access the user EXEC mode but it should be secured.

Command Mode	Description	Default Device Prompt
User Exec Mode	• Mode allows access to only a limited number of basic monitoring commands. • It is often referred to as "view-only" mode.	`Switch>` `Router>`
Privileged EXEC Mode	• Mode allows access to all commands and features. • The user can use any monitoring commands and execute configuration and management commands.	`Switch#` `Router#`

The primary configuration mode is called global configuration or simply, global config.
• Use the configure terminal command to access.
• Changes made affect the operation of the device.
Various methods can be used to exit / quit configuration modes:
• exit - Used to move from a specific mode to the previous more general mode, such as from interface mode to global config.
• end - Can be used to exit out of global configuration mode regardless of which configuration mode you are in.
• ^z - Works the same as end.

Basic IOS Command Structure

The syntax for a command is the command followed by any appropriate keywords and
arguments.
• Keyword - a specific parameter defined in the operating system (in the figure, ip protocols)
• Argument - not predefined; a value or variable defined by the user (in the figure, 192.168.10.5)
After entering each complete command, including any keywords and arguments, press the Enter key to submit the command to the command interpreter.



13. Study of Routing and Switching, configuring of Switch and Routers.

When building networks, we typically divide routing into two components: host and router. Routers handle traffic flowing between networks but hosts make many decisions long before the packets hit the network. Most routing protocols used to find pathways to destinations are router based, however.Hosts are typically configured one of two ways: statically with an IP address, default gateway, and domain name server, or with values learned via the Dynamic Host Configuration Protocol (DHCP). Hosts send all traffic going off the local network to the default gateway, with the hope that the gateway can route the packets to the destination Before doing anything else, a host must process its routing table. Routers operate at the internetwork layer of the TCP/IP model and process IP addresses based on their routing table. A router's main function is to forward traffic to destination networks via the destination address in an IP packet. Routers also resolve MAC addresses (particularly their own) by using the Address Resolution Protocol (ARP). It is important to remember that Layer 2 (link layer) frames and MAC addresses do not live beyond the router. This means that an Ethernet frame is destroyed when it hits a router. When operating in a network, a router can act as the default gateway for hosts, as in most home networks. A router may be installed as an intermediate hop between other routers without any direct connectivity to hosts.

Switches operate at Layer 2 of the TCP/IP (and OSI) model.The operation of switches and bridges is defined in the IEEE 802.1D standard.

In addition to forwarding Ethernet frames based on Media Access Control (MAC) addresses and processing the Cyclical Redundancy Check (CRC), switches provide a couple of very important services:

- Filter out traffic that should not be forwarded, such as local unicast frames
- Prevent the forwarding of collisions
- Prevent the forwarding of frames with errors

There are many types of switching: packet, circuit, multilayer, virtual circuit, wide area network (WAN), local area network (LAN). Packet switching usually concerns a router or perhaps a WAN switch. Multilayer switching is a technique for improving the processing of IP packets.

Steps to configure selected global parameters for the switch:

	Command	**Purpose**
Step 1	configure terminal Example: switch> enable switch # configure terminal switch (config)#	Enters global configuration mode, when using the console port.
Step 2	hostname *name* Example: switch (config)# hostname switch switch (config)#	Specifies the name for the router.

Step 3	enable secret *password* Example: switch(config)# enable secret cr1ny5ho switch (config)#	Specifies an encrypted password to prevent unauthorized access to the router.

Steps to configure selected global parameters for the router:

	Command	**Purpose**
Step 1	configure terminal Example: Router> enable Router# configure terminal Router(config)#	Enters global configuration mode, when using the console port.
Step 2	hostname *name* Example: Router(config)# hostname Router Router(config)#	Specifies the name for the router.
Step 3	enable secret *password* Example: Router(config)# enable secret cr1ny5ho Router(config)#	Specifies an encrypted password to prevent unauthorized access to the router.

14. Study of Scaling of Networks, Design varieties of LAN and forward of Traffic.

The Need to Scale the Network :

As a business grows, so does its networking requirements. To keep pace with a business's expansion and new emerging technologies, a network must be designed to scale. A network that scales well is not only one that can handle growing traffic demands, but also one designed with the inevitable need to expand.

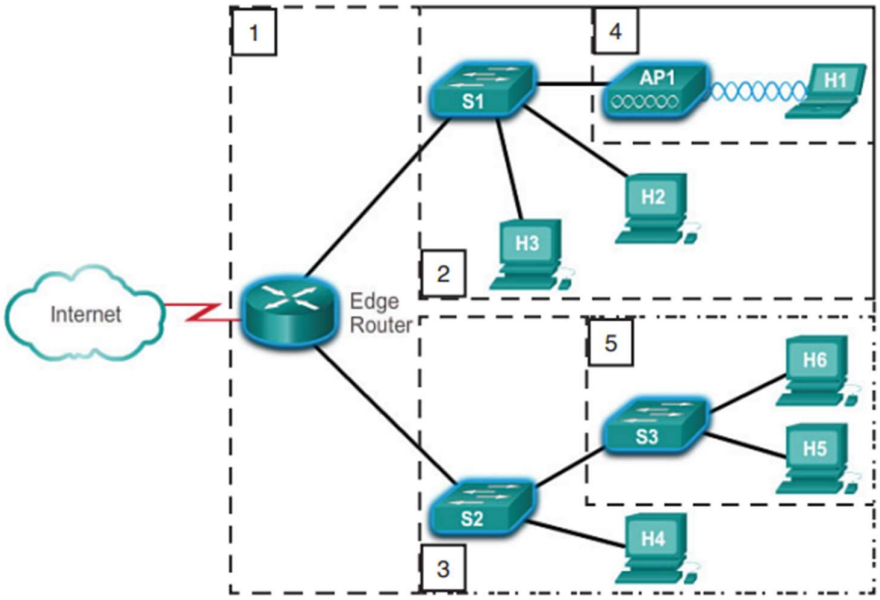
Failure Domains

A well-designed network not only controls traffic but also limits the size of failure domains. A failure domain is the area of a network that is impacted when a critical device or network service experiences problems.

The function of the device that initially fails determines the impact of a failure domain. For example, a malfunctioning switch on a network segment normally affects only the hosts on that segment. However, if the router that connects this segment to others fails, the impact is much greater.

The use of redundant links and reliable enterprise-class equipment minimizes the chance of disruption in a network. Smaller failure domains reduce the impact of a failure on company productivity. They also simplify the troubleshooting process, thereby shortening the downtime for all users.

Failure domains often include other, smaller failure domains. For example, the following failure domains:



(FAILURE DOMAIN EXAMPLE)

1. If the Edge Router fails, it will impact every device connected to it.
2. If S1 fails, it will impact H1, H2, H3, and AP1.
3. If S2 fails, it will impact S3, H4, H5, and H6.
4. If AP1 fails, it will impact H1.
5. If S3 fails, it will impact H5 and H6.

Limiting the Size of Failure Domains

Because a failure at the core layer of a network can have a potentially large impact,the network designer often concentrates on efforts to prevent failures. These effortscan greatly increase the cost of implementing the network. In the hierarchical designmodel, it is easiest and usually least expensive to control the size of a failure domain in the distribution layer. In the distribution layer, network errors can be contained to a smaller area, thus affecting fewer users. When using Layer 3 devices at the distribution layer, every router functions as a gateway for a limited number of access layer users.

Expanding the Network

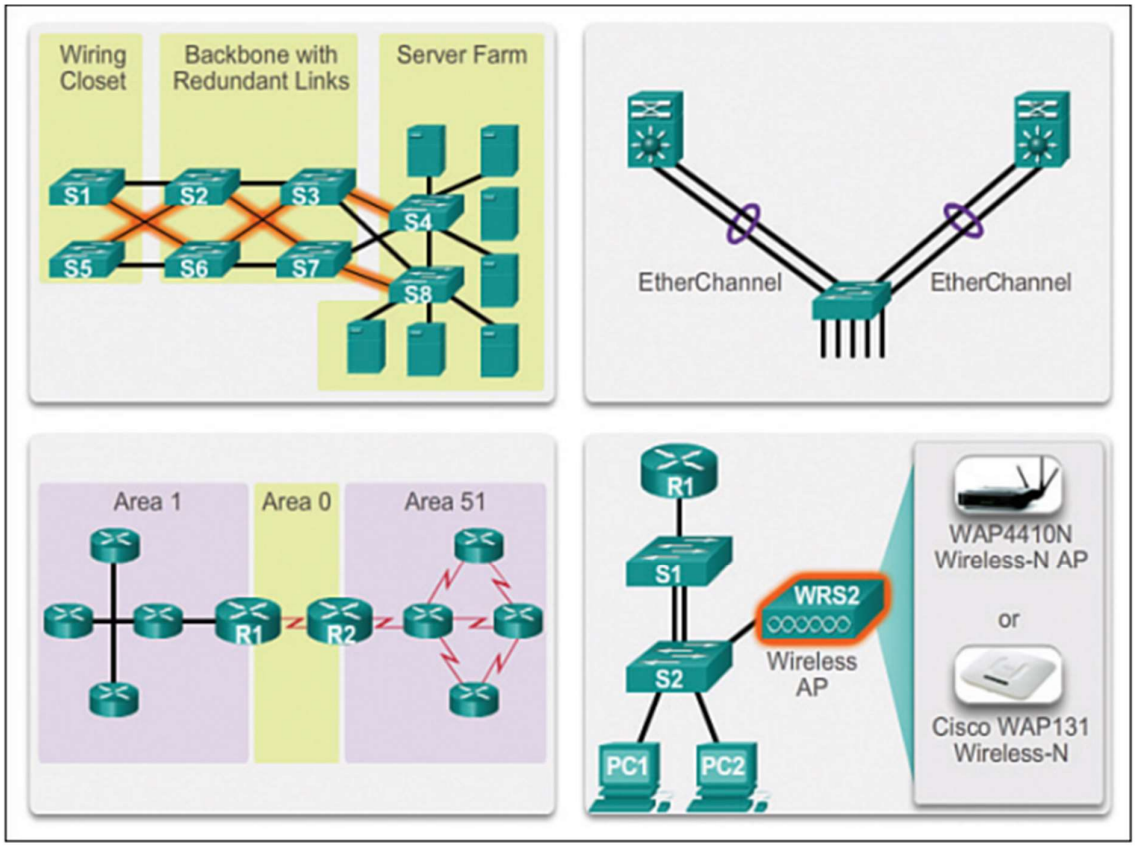
A solid network design is not all that is needed for network expansion. This section reviews the features necessary to ensure that the network scales well as the
company grows.

Design for Scalability

To support an enterprise network, the network designer must develop a strategy to enable the network to be available and to scale effectively and easily. Included in a basic network design strategy are the following recommendations:

- Use expandable, modular equipment or clustered devices that can be easily upgraded to increase capabilities. Device modules can be added to the existing equipment to support new features and devices without requiring major equipment upgrades. Some devices can be integrated in a cluster to act as one device to simplify management and configuration.
- Design a hierarchical network to include modules that can be added, upgraded,and modified, as necessary, without affecting the design of the other functional
- areas of the network. For example, you can create a separate access layer that can be expanded without affecting the distribution and core layers of the campus network.
- Create an IPv4 or IPv6 address strategy that is hierarchical. Careful address planning eliminates the need to re-address the network to support additional users and services.
- Choose routers or multilayer switches to limit broadcasts and filter other undesirable traffic from the network. Use Layer 3 devices to filter and reduce traffic to the network core.
- Implementing redundant links in the network between critical devices and between access layer and core layer devices.
- Implementing multiple links between equipment, with either link aggregation(EtherChannel) or equal-cost load balancing, to increase bandwidth.
- Combining multiple Ethernet links into a single, load-balanced EtherChannel configuration increases available bandwidth. EtherChannel implementations can be used when budget restrictions prohibit purchasing high-speed interfaces and fiber runs.
- Implementing wireless connectivity to allow for mobility and expansion.

- Using a scalable routing protocol and implementing features within that routing protocol to isolate routing updates and minimize the size of the routing table.



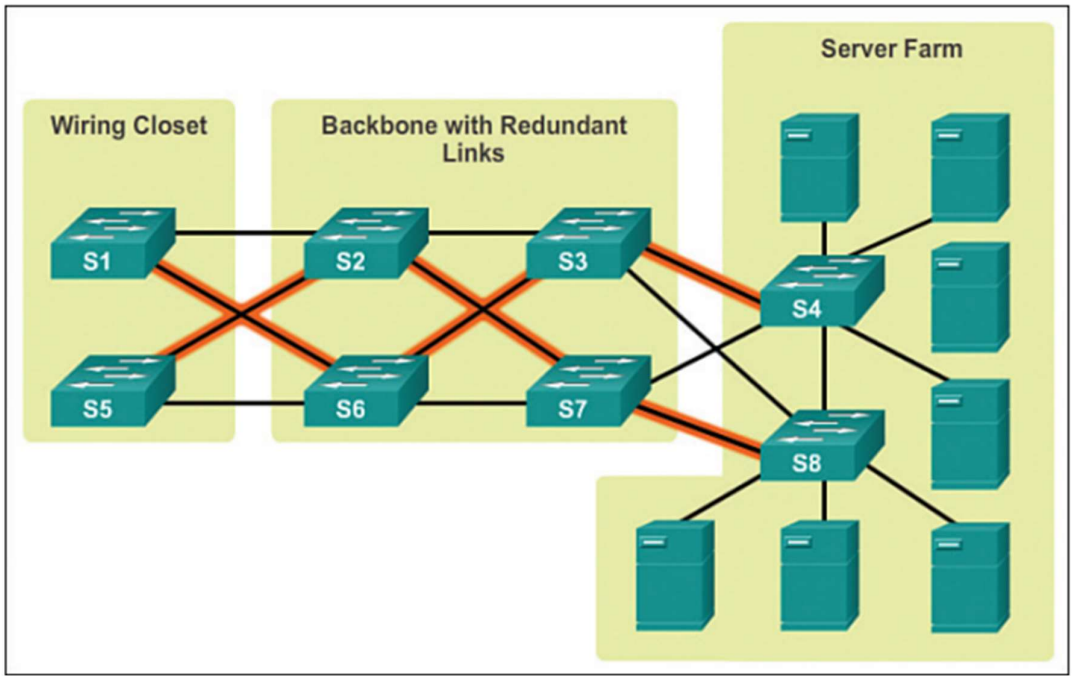
(DESIGN FOR SCALABILITY)

Implementing Redundancy

- For many organizations, the availability of the network is essential to supporting business needs. Redundancy is an important part of network design for preventing disruption of network services by minimizing the possibility of a single point of failure. One method of implementing redundancy is by installing duplicate equipment and providing failover services for critical devices.
- Another method of implementing redundancy is using redundant paths, as shown in the Figure .
- Redundant paths offer alternate physical paths for data to traverse the network.Redundant paths in a switched network support high availability. However, because of the operation of switches, redundant paths in a switched Ethernet network can cause logical Layer 2 loops. For this reason, Spanning Tree Protocol (STP) is

required.

- STP allows for the redundancy required for reliability but eliminates the switching loops. It does this by providing a mechanism for disabling redundant paths in a switched network until the path is necessary, such as when failures occur. STP is an open standard protocol, used in a switched environment to create a loop-free logical topology.



(LAN REDUNDANCY)

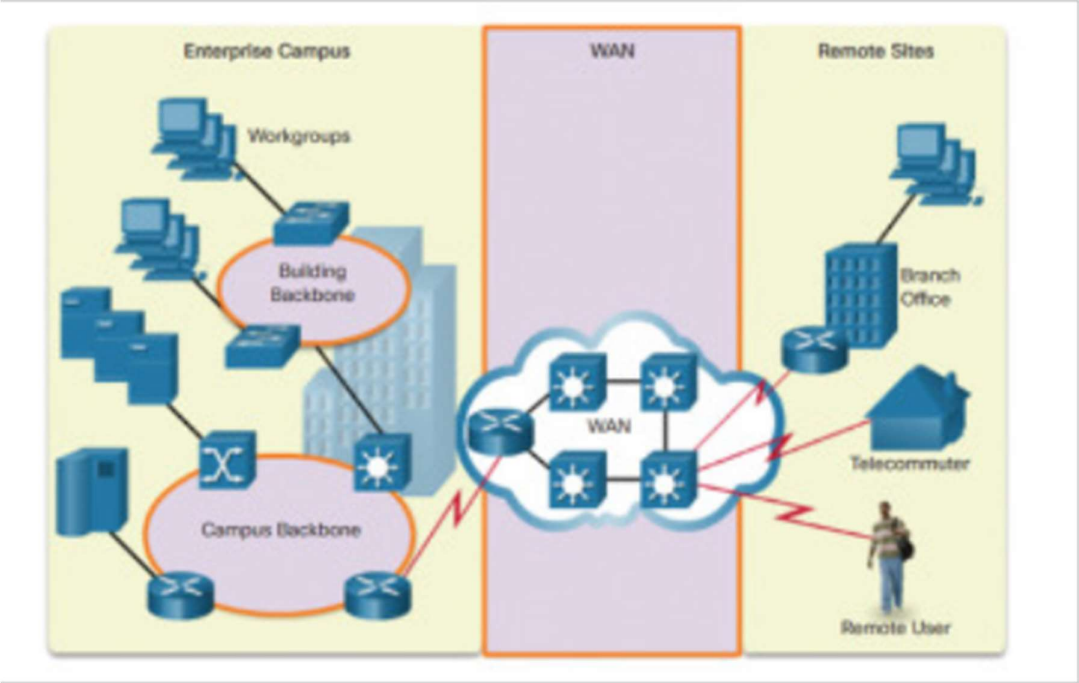
15. Study WAN concepts and Configure and forward Traffic in WAN

Purpose of WANs

- A WAN operates beyond the geographic scope of a LAN. WANs are used to interconnect the enterprise LAN to remote LANs in branch sites and telecommuter sites.
- A WAN is owned by a service provider. A user must pay a fee to use the provider's network services to connect remote sites. WAN service providers include carriers, such as a telephone network, cable company, or satellite service. Service providers provide

links to interconnect remote sites for the purpose of transporting data, voice, and video.

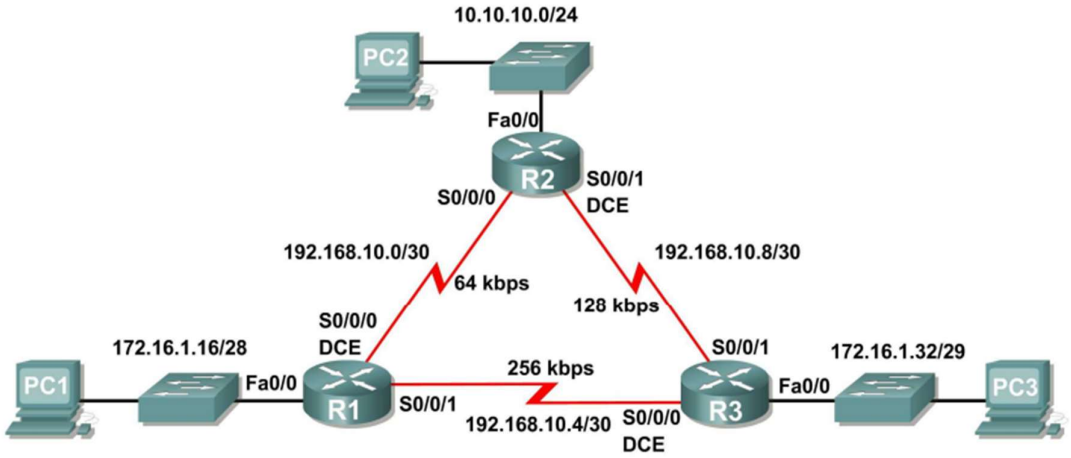
- In contrast, LANs are typically owned by an organization. They are used to connect local computers, peripherals, and other devices within a single building or other small geographic area. Without WANs, LANs would be a series of isolated networks.



(WANs interconnect users and LANs)

Configure OSPF:

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	172.16.1.17	255.255.255.240	N/A
	S0/0/0	192.168.10.1	255.255.255.252	N/A
	S0/0/1	192.168.10.5	255.255.255.252	N/A
R2	Fa0/0	10.10.10.1	255.255.255.0	N/A
	S0/0/0	192.168.10.2	255.255.255.252	N/A
	S0/0/1	192.168.10.9	255.255.255.252	N/A
R3	Fa0/0	172.16.1.33	255.255.255.248	N/A
	S0/0/0	192.168.10.6	255.255.255.252	N/A
	S0/0/1	192.168.10.10	255.255.255.252	N/A
PC1	NIC	172.16.1.20	255.255.255.240	172.16.1.17
PC2	NIC	10.10.10.10	255.255.255.0	10.10.10.1
PC3	NIC	172.16.1.35	255.255.255.248	172.16.1.33

- **Step 1: Configure the routers**
- On the routers, enter global configuration mode and configure the hostname as shown on the chart. Then configure the console, virtual terminal lines password (both “cisco”) and privileged EXEC password (“class”):

- **Step 2: Configure the interfaces on R1, R2, and R3**
- Configure the interfaces on the R1, R2, and R3 routers with the IP addresses from the table under the Topology Diagram.
- **Step 3: Verify IP addressing and interfaces**
- Use the show ip interface brief command to verify that the IP addressing is correct and that the interfaces are active.
- **Step 4: Configure Ethernet interfaces of PC1, PC2, and PC3**
- Configure the Ethernet interfaces of PC1, PC2, and PC3 with the IP addresses and default gateways from the table under the Topology Diagram.
- **Task: Configure OSPF on the R1 Router**
- **Step 1:** Use the router ospf command in global configuration mode to enable OSPF on the R1 router. Enter a process ID of 1 for the process-ID parameter.
- R1(config)#router ospf 1
- R1(config-router)#
- **Step 2:** Configure the network statement for the LAN network.
- Once you are in the Router OSPF configuration sub-mode, configure the LAN network 172.16.1.16/28 to be included in the OSPF updates that are sent out of R1.
- The OSPF network command uses a combination of network-address and wildcard-mask similar to that which can be used by EIGRP. Unlike EIGRP, the wildcard mask in OSPF is required.
- Use an area ID of 0 for the OSPF area-id parameter. 0 will be used for the OSPF area ID in all of the network statements in this topology.
- R1(config-router)#network 172.16.1.16 0.0.0.15 area 0
- R1(config-router)#
- **Step 3:** Configure the router to advertise the 192.168.10.0/30 network attached to the Serial0/0/0 interface.
- R1(config-router)# network 192.168.10.0 0.0.0.3 area 0
- R1(config-router)#
- **Step 4:** Configure the router to advertise the 192.168.10.4/30 network attached to the Serial0/0/1 interface.
- R1(config-router)# network 192.168.10.4 0.0.0.3 area 0
- R1(config-router)#

- **Step 5:** When you are finished with the OSPF configuration for R1, return to privileged EXEC mode.
- R1(config-router)#end
  Output: %SYS-5-CONFIG_I: Configured from console by console
- R1#
- **Task: Configure OSPF on the R2 and R3 Routers**
- **Step 1:** Enable OSPF routing on the R2 router using the router ospf command.
- Use a process ID of 1.
- R2(config)#router ospf 1
- R2(config-router)#
- **Step 2:** Configure the router to advertise the LAN network 10.10.10.0/24 in the OSPF updates.
- R2(config-router)#network 10.10.10.0 0.0.0.255 area 0
- R2(config-router)#
- **Step 3:** Configure the router to advertise the 192.168.10.0/30 network attached to the Serial0/0/0 interface.
- R2(config-router)#network 192.168.10.0 0.0.0.3 area 0
- R2(config-router)#
  Output: 00:07:27: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.5 on Serial0/0/0 from EXCHANGE to FULL, Exchange Done
- Notice that when the network for the serial link from R1 to R2 is added to the OSPF configuration, the router sends a notification message to the console stating that a neighbor relationship with another OSPF router has been established.
- **Step 4:** Configure the router to advertise the 192.168.10.8/30 network attached to the Serial0/0/1 interface.
- When you are finished, return to privileged EXEC mode.

- R2(config-router)#network 192.168.10.8 0.0.0.3 area 0
- R2(config-router)#end
  Output: %SYS-5-CONFIG_I: Configured from console by console
- R2#

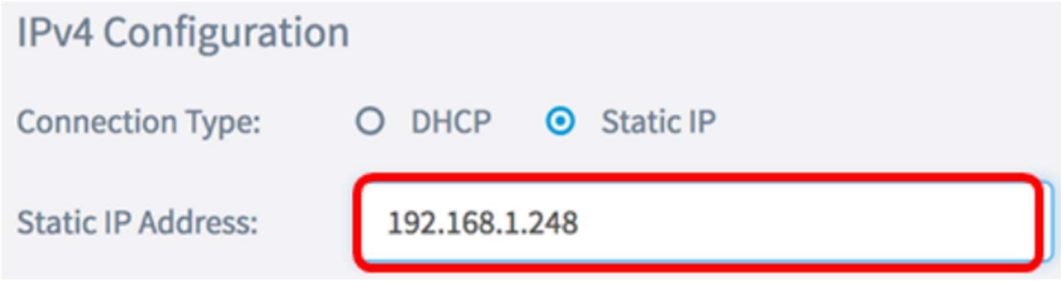
- **Step 5:** Configure OSPF on the R3 router using the router ospf and network commands.
- Use a process ID of 1. Configure the router to advertise the three directly connected networks.When you are finished, return to privileged EXEC mode.
- R3(config)#router ospf 1
- R3(config-router)#network 172.16.1.32 0.0.0.7 area 0
- R3(config-router)#network 192.168.10.4 0.0.0.3 area 0
- R3(config-router)#
  Output: 00:17:46: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.5 on Serial0/0/0 from LOADING to FULL, Loading Done
- R3(config-router)#network 192.168.10.8 0.0.0.3 area 0
- R3(config-router)#
  Output: 00:18:01: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.9 on Serial0/0/1 from EXCHANGE to FULL, Exchange Done
- R3(config-router)#end
  Output: %SYS-5-CONFIG_I: Configured from console by console
- R3#
- Notice that when the networks for the serial links from R3 to R1 and R3 to R2 are added to the OSPF configuration, the router sends a notification message to the console stating that a neighbor relationship with another OSPF router has been established.

- R3#show ip protocols
  Output: Routing Protocol is "ospf 1"
- R3#show ip ospf
  Output: Routing Process "ospf 1" with ID 192.168.10.10
- R3#show ip ospf interface
  Output: FastEthernet0/0 is up, line protocol is up
  Internet address is 172.16.1.33/29, Area 0,Process ID 1, Router ID 192.168.10.10, Network Type BROADCAST, Cost:1

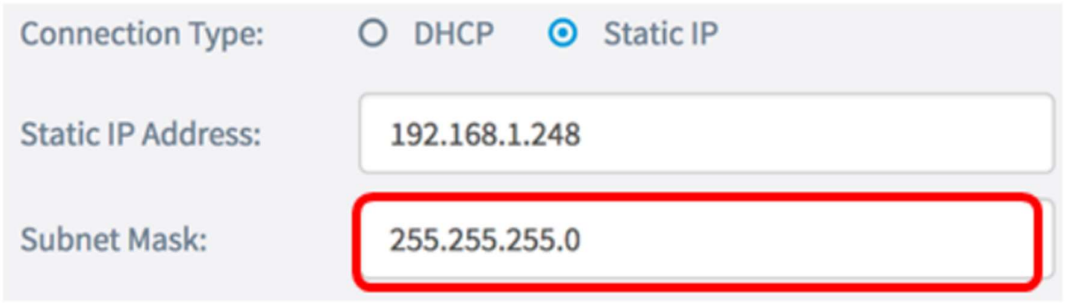
16. Configure IPv4 and IPv6 and learn Quality, security and other services

Configure IPv4 or IPv6 Settings
IPv4 Settings

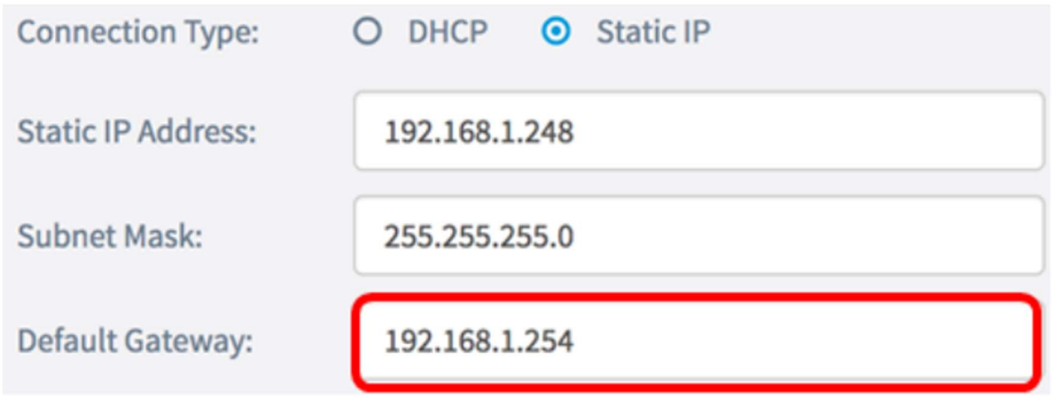
- **Step 1.** Log in to the access point web-based utility by entering your Username and Password in the fields provided and then click Login.
- **Step 2.** Choose System Configuration > LAN
- **Step 3.** Under IPv4 Configuration, click a radio button in the Connection Type to choose the
- type of connection you want the WAP to use in the network. The options are:
- DHCP — This option allows the WAP to get its IP settings from the DHCP server on the network. If you choose this option, skip to Step 6.
- Static IP — This option allows you to manually assign IP settings to the WAP. If you choose this option, the Domain Name Servers settings will be automatically set to Manual.
- **Step 4.** In the Static IP Address field, enter a permanent IP address for the WAP. This IP address should be unique and no other device in the network would be able to use it.



Step 5. In the Subnet Mask field, enter a subnet mask for the WAP.



Step 6. In the Default Gateway field, enter the IP address of the router or the DHCP server on the network.

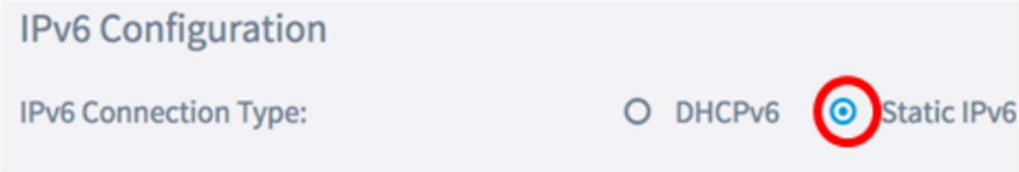


Step 7. If you have chosen DHCP in Step 2, choose a radio button to set how the WAP would acquire a DNS address in the Domain Name Servers area. The options are:
Dynamic — This option allows the WAP to acquire the DNS server addresses from a DHCP server on the LAN. If you choose this option, skip to Step 8.
Manual — This option allows you to manually configure DNS server addresses. You can enter up to two addresses in the fields provided.
Step 8. Enter a DNS Server address(es) in the field(s) provided.
Step 9. Click the SAVE button.

IPv6 Settings

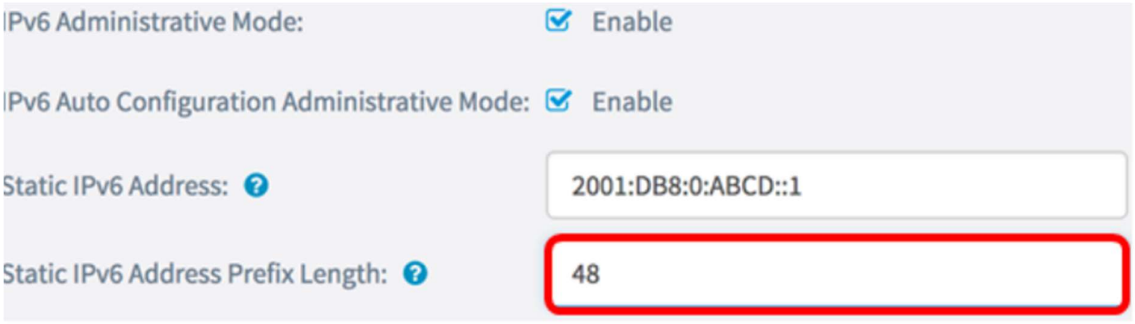
Step 1. Under IPv6 Configuration, click a radio button in the IPv6 Connection Type to choose
the type of connection you want the WAP to use in the network. The options are:
DHCPv6 — This option allows the WAP to get its IPv6 settings from the DHCP server on

the network. If you choose this option, skip to Step 7.
Static IPv6 — This option allows you to manually assign IPv6 settings to the WAP. If you choose this option, the IPv6 Domain Name Servers settings will be automatically set to Manual.



Step 2. (Optional) To permit IPv6 management access to the access point, check the Enable IPv6 Administrative Mode check box. This box is checked by default.
Step 3. (Optional) Check the Enable IPv6 Auto Configuration Administrative Mode checkbox. This would allow the WAP to learn its IPv6 settings through router advertisements received on the LAN port.
Step 4. In the Static IPv6 Address field, enter a permanent IP address for the WAP. This IP address should be unique and no other device in the network would be able to use it.

Step 5. Enter the prefix length of the static address in the Static IPv6 Address Prefix Length field. The prefix length specifies the network portion of the IPv6 IP address and in the range of 0 to 128.



Step 6. Enter the IPv6 address of the default gateway in the Default IPv6 Gateway field.

Step 7. If you have chosen DHCPv6 in Step 1, choose a radio button to set how the WAP would acquire an IPv6 DNS address in the IPv6 Domain Name Servers area. The options
are:
Dynamic — This option allows the WAP to acquire the DNS server addresses from a DHCP server on the LAN. If you choose this option, skip to Step 9.
Manual — This option allows you to manually configure DNS server addresses. You can enter up to two addresses in the fields provided.
Step 8. Enter an IPv6 DNS Server address(es) in the field(s) provided.

Step 9. Click the SAVE button.

17. Learn Network programming

Client/Server Communications

A server is any application that provides a service and allows clients to communicate with it.
A client is any application that requests a service from a server.
Using TCP the client and server must establish a connection in order to communicate. To do this, each program binds a socket to its end of the connection. A socket is one endpoint of a twoway communication link between 2 programs running on the network. A socket is bound to a port number so that the TCP layer can identify the application to which the data is to be sent. It is similar to the idea of plugging the two together with a cable. The port number is used as the server's location on the machine that the server application is running. So if a computer is running many different server applications on the same physical

machine, the port number uniquely identifies the particular server that the client wishes to communicate with:
The client and server may then each read and write to the socket bound to its end of the connection.

In JAVA, the server application uses a ServerSocket object to wait for client connection requests. When you create a ServerSocket, you must specify a port number (an int). It is possible that the server cannot set up a socket and so we have to expect a possible IOException.
Example:

```
public static int SERVER_PORT = 5000;
ServerSocket serverSocket;
try {
serverSocket = new ServerSocket(SERVER_PORT);
}
catch(IOException e) {
 System.out.println("Cannot open server connection");
}
```

The server can communicate with only one client at a time.
The server waits for an incoming client request through the use of the accept() message:

```
Socket aClientSocket;
try {
 aClientSocket = serverSocket.accept();
}
catch(IOException e) {
 System.out.println("Cannot connect to client");
}
```

When the accept() method is called, the server program actually waits (i.e., blocks) until a client becomes available (i.e., an incoming client request arrives). Then it creates and returns a Socket object through which communication takes place. Once the client and server have completed their interaction, the socket is then closed:

```
aClientSocket.close();
```

Only then may the next client open a socket connection to the server. So, remember ... if one client has a connection, everybody else has to wait until they are done:

So how does the client connect to the server ? Well, the client must know the address of the server as well as the port number. The server's address is stored as an InetAddress object which represents any IP address (i.e., an internet address, an ftp site, local machine etc,...).

If the server and client are on the same machine, the static method getLocatHost() in the InetAddress class may be used to get an address representing the local machine as follows:

```
public static int SERVER_PORT = 5000;
try {
 InetAddress address = InetAddress.getLocalHost();
 Socket socket = new Socket(address, SERVER_PORT);
}
catch(UnknownHostException e) {
 System.out.println("Host Unknown");
}
catch(IOException e) {
 System.out.println("Cannot connect to server");
}
```

Once again, a socket object is returned which can then be used for communication.

Here is an example of what a local host may look like:

```
cr850205-a/169.254.180.32
```

The getLocalHost() method may, however, generate an UnknownHostException.

You can also make an InetAddress object by specifying the network IP address directly or the machine name directly as follows:

```
 InetAddress.getByName("169.254.1.61");
 InetAddress.getByName("www.scs.carleton.ca");
```

So how do we actually do communication between the client and the server ? Well, each socket has an inputStream and an outputStream. So, once we have the sockets, we simply ask for these streams … and then reading and writing may occur.

```
try {
 InputStream in = socket.getInputStream();
```

```
 OutputStream out = socket.getOutputStream();
}
catch(IOException e) {
 System.out.println("Cannot open I/O Streams");
```

Normally, however, we actually wrap these input/output streams with text-based, datatypebased or object-based wrappers:

```
ObjectInputStream in = new
ObjectInputStream(socket.getInputStream());
ObjectOutputStream out = new
ObjectOutputStream(socket.getOutputStream());
BufferedReader in = new BufferedReader(new
InputStreamReader(socket.getInputStream()));
PrintWriter out = new PrintWriter(socket.getOutputStream());
DataInputStream in = new
DataInputStream(socket.getInputStream());
DataOutputStream out = new
DataOutputStream(socket.getOutputStream());
```

You may look back at the notes on file I/O to see how to write to the streams. However, one more point ... when data is sent through the output stream, the flush() method should be sent to the output stream so that the data is not buffered, but actually sent right away.

Also, you must be careful when using ObjectInputStreams and ObjectOutputStreams.

When you create an ObjectInputStream, it blocks while it tries to read a header from the underlying SocketInputStream. When you create the corresponding ObjectOutputStream at the far end, it writes the header that the ObjectInputStream is waiting for, and both are able to continue. If you try to create both ObjectInputStreams first, each end of the connection is waiting for the other to complete before proceeding which results in a deadlock situation (i.e.,the programs seems to hang/halt).

Let us now take a look at a real example. In this example, a client will attempt to:

1. connect to a server
2. ask the server for the current time

3. ask the server for the number of requests that the server has handled so far
4. ask the server for an invalid request (i.e., for a pizza)

Here is the server application. It runs forever, continually waiting for incoming client requests:

```
import java.net.*; // all socket stuff is in here
import java.io.*;
public class Server {
 public static int SERVER_PORT = 5000; // arbitrary, but above 1023
 private int counter = 0;
 // Helper method to get the ServerSocket started
 private ServerSocket goOnline() {
 ServerSocket serverSocket = null;
 try {
 serverSocket = new ServerSocket(SERVER_PORT);
 System.out.println("SERVER online");
 } catch (IOException e) {
 System.out.println("SERVER: Error creating network connection");
 }
 return serverSocket;
 }
 // Handle all requests
 private void handleRequests(ServerSocket serverSocket) {
 while(true) {
 Socket socket = null;
 BufferedReader in = null;
 PrintWriter out = null;
 try {
 // Wait for an incoming client request
socket = serverSocket.accept();
 // At this point, a client connection has been made
in = new BufferedReader(new InputStreamReader(
 socket.getInputStream()));
 out = new PrintWriter(socket.getOutputStream());
} catch(IOException e) {
 System.out.println("SERVER: Error connecting to client");
 System.exit(-1);
```

```
}
// Read in the client's request
try {
String request = in.readLine();
System.out.println("SERVER: Client Message Received: " + request);
if (request.equals("What Time is It ?")) {
out.println(new java.util.Date());
counter++;
}
else if (request.equals("How many requests have you handled ?"))
out.println(counter++);
else
System.out.println("SERVER: Unknown request: " + request);
out.flush(); // Now make sure that the response is sent
socket.close(); // We are done with the client's request
} catch(IOException e) {
System.out.println("SERVER: Error communicating with client");
}
}
}
public static void main (String[] args) {
Server s = new Server();
ServerSocket ss = s.goOnline();
if (ss != null)
s.handleRequests(ss);
}
}
```

Here is the client application:

```
import java.net.*;
import java.io.*;
public class ClientProgram {
 private Socket socket;
 private BufferedReader in;
 private PrintWriter out;
 // Make a connection to the server
 private void connectToServer() {
 try {
```

```
 socket = new Socket(InetAddress.getLocalHost(),
Server.SERVER_PORT);
 in = new BufferedReader(new InputStreamReader(
 socket.getInputStream()));
 out = new PrintWriter(socket.getOutputStream());
 } catch(IOException e) {
 System.out.println("CLIENT: Cannot connect to server");
 System.exit(-1);
 }
 }
// Disconnect from the server
 private void disconnectFromServer() {
 try {
 socket.close();
 } catch(IOException e) {
 System.out.println("CLIENT: Cannot disconnect from server");
 }
 }
 // Ask the server for the current time
 private void askForTime() {
 connectToServer();
 out.println("What Time is It ?");
 out.flush();
 try {
 String time = in.readLine();
 System.out.println("CLIENT: The time is " + time);
 } catch(IOException e) {
 System.out.println("CLIENT: Cannot receive time from server");
 }
 disconnectFromServer();
 }
 // Ask the server for the number of requests obtained
 private void askForNumberOfRequests() {
 connectToServer();
 out.println("How many requests have you handled ?");
 out.flush();
 int count = 0;
```

```
try {
count = Integer.parseInt(in.readLine());
} catch(IOException e) {
System.out.println("CLIENT: Cannot receive num requests from server");
}
System.out.println("CLIENT: The number of requests are " + count);
disconnectFromServer();
}
// Ask the server to order a pizza
private void askForAPizza() {
connectToServer();
out.println("Give me a pizza");
out.flush();
disconnectFromServer();
}
private static void Delay() {
try{Thread.sleep(3000);}catch(InterruptedException e){}
}
public static void main (String[] args) {
ClientProgram c = new ClientProgram();
Delay(); c.askForTime();
Delay(); c.askForNumberOfRequests();
Delay(); c.askForAPizza();
Delay(); c.askForTime();
Delay(); c.askForNumberOfRequests();
}
}
```

18. Troubleshoot Networks.

Tools for Troubleshooting IP Problems:

Ping: The ping tool uses the IP ICMP echo request and echo reply messages to test reachability to a remote system. In its simplest form, ping simply confirms that an IP packet is capable of getting to and getting back from a destination IP address (Figure 7-7). This tool generally returns two pieces of information:

whether the source can reach the destination (and, by inference, vice versa), and the round-trip time (RTT, typically in milliseconds).

CiscoRtr1>ping 10.3.1.6

Output: Type escape sequence to abort.

Sending 5, 100-byte ICMP Echoes to 10.3.1.6, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

traceroute : If ping fails or returns an unusual RTT, traceroute can be used to help narrow down the problem. It is also possible to vary the size of the ICMP echo payload to test problems related to maximum transmission unit (MTU).

CiscoRtr1>traceroute 10.3.1.6

Output:Type escape sequence to abort.

Tracing the route to 10.3.1.6

1 CiscoRtr2 (10.1.1.2) 0 msec

CiscoRtr3 (10.1.1.3) 0 msec

CiscoRtr4 (10.1.1.4) 4 msec

2 CiscoRtr5 (10.2.1.6) 4 msec 4 msec 0 msec

3 CiscoRtr6 (10.3.1.6) 4 msec 4 msec 4 msec

Troubleshooting Local Connectivity Problems

- **Configuration problem**
- **DHCP or BOOTP issue**
- **Physical layer issue**
- **Duplicate IP address**

Check for Configuration Problems

To begin troubleshooting, display and examine the IP configuration of the source device. The method to determine this information varies greatly from platform to platform. If you are unsure of how to display this information, consult the manual for the device or operating system.

• On a Cisco router, use show ip interface and show running-config.

• On Windows 95 or 98, use winipcfg.exe.

• On Windows 2000 or NT, use ipconfig.exe.
• On a UNIX platform, use ifconfig.

Examine the configuration, looking specifically for the IP address and subnet mask. On Windows 9x or Windows 2000 platforms, the default gateway address should also be displayed.

If no IP address is configured, verify that this node receives its IP address from BOOTP or DHCP.

Otherwise, an IP address should be statically configured for this interface. Configure an address if one is not present. If the source is configured to receive an IP address via DHCP or BOOTP and is not receiving one, make sure that the bootp (IP) helper address is configured on the router interface facing the source device.

If the incorrect IP address, subnet mask, or default gateway is configured, verify that this node receives its IP address from BOOTP or DHCP, and then contact the DHCP or BOOTP administrator. Ask the administrator to troubleshoot the DHCP or BOOTP server's configuration. If the address is statically configured, configure the correct address.

Check for Local Connectivity

If the destination is on the same subnet as the source, try pinging the destination by IP address. If the destination is on a different subnet, then try pinging the default gateway or appropriate next hop obtained from the routing table. If the ping fails, double-check the configuration of the next-hop router to see if the subnet and mask match the source's configuration. If the configuration is correct, check that the source or next-hop router is capable of pinging any other device on the local LAN segment. If you cannot ping the next-hop address, and if the next-hop address is an HSRP virtual address, try pinging one of the next-hop router's actual IP addresses. If the actual address works but the virtual address does not, you may be experiencing an HSRP issue. Failure to communicate with some or all devices on the LAN segment could indicate a physical connectivity problem, a switch or bridge misconfiguration, or a duplicate IP address.

Ruling Out Duplicate IP Addresses

To rule out a duplicate IP address, you can disconnect the suspect device from the LAN or shut down the suspect interface and then

try pinging the device from another device on that same LAN segment. If the ping is successful, then there is another device on that LAN segment using the IP address. You will be able to determine the MAC address of the conflicting device by looking at the ARP table on the device that issued the ping.

Troubleshooting Physical Connectivity Problems

Even though it may seem logical to first troubleshoot at the physical layer, problems can generally be found more quickly by first troubleshooting at Layer 3 and then working backward when a physical problem is found or suspected.

Possible problems include these:

- Configuration is incorrect.
- Cable is faulty or improperly connected.
- Wiring closet cross-connect is faulty or improperly connected.
- Hardware (interface or port) is faulty.
- Interface has too much traffic.