**LAN SETUP AND MONITORING**

1. **Objectives**
* Study the types of Ethernet cabling and when and how to use them.
* Installing a Peer-to-Peer local area network (Workgroup LAN) using crossover cable.
* Learn to create a simple LAN with two PCs using an Ethernet switch and two straight-through cables to connect the workstations
* Learn to configure and verify the network connectivity.
* Implementing some applications like file sharing between workstations
* Learn about various network related commands.
1. **Lab Setup:**
* 2 PCs with Network Interface Card (NIC) for each.
* One Ethernet hub and one Ethernet switch.
* Single crossover cable
* Two CAT5 straight-wired cables
* Cable tester.
1. **Pre Lab:**
* Answer questions number 1, 2, 3, 4 and 5.
* Build and simulate the network topology in fig. 1.5 using Packet Tracer Simulator.
1. **Background:**
	1. **Networks Cables:**

There are many types of network cables used in the real-world applications. Some of them are given below:

1. Unshielded twisted pair: As the name indicates, the wires are twisted with one another and there is no shield.
2. Shielded twisted pair: Shield with twisted pair.
3. Coaxial cable: Similar to our TV cables.
4. Fiber-optic cable.

**Question#1:**

1. What are the advantages, disadvantages, bandwidth, and applications of each type of the network cables?
2. Draw the layout of each type.
	1. **Network Devices:**

There are many types of network devices used in building network topology. Some of them are given below:

Figure 1.1 Most common network devices

**Question#2:**

Figure 1.1 shows the most common Network Devices; explain the function of each device and the difference between them? In which layer each device operates?

* 1. **Network Addressing:**

Each Network Interface Card (NIC or Network card) present in a PC is assigned one Network address called as IP address [or Network address]. This IP address is assigned by the administrator of the network. No two PCs can have the same IP address.

There is a burned-in address on the NIC called as Physical Address [or MAC address or Hardware address]. The MAC address of a network card indicates the vendor of that card and a unique serial number.

IP addresses are divided into different classes. These classes determine the maximum number of hosts per network ID. Only three classes are actually used for network connectivity.

**Question#3:**

1. Compare Mac address with IP address with respect to address format, functions, OSI layer that operate on, and who assign it?
2. Define the following terms: Subnet Mask and Default Gateway**.**
3. Fill the following table:

|  |  |  |  |
| --- | --- | --- | --- |
| **Address Class** | **IP Range** | **Bits for Subnet Mask** | **Subnet Mask** |
| **Class A** |  |  |  |
| **Class B** |  |  |  |
| **Class C** |  |  |  |

1. Which address class will allow you to have more than 1000 hosts per network?
2. Which address will allow only 254 hosts per network?
	1. **Cable Connection for Network Devices**

Since there’s a bunch of different types of devices specified at the different layers of the OSI model, it’s also very important to understand the many types of cables and connectors used for connecting all those devices to a network. We’ll go over cabling devices, discussing how to connect to a router or switch along with Ethernet LAN technologies. Ethernet cabling is an important discussion, especially if you are planning on build LAN.

*Students will be given a demonstration on various network devices like: Cables, RJ45, etc. Students will be provided a tutorial about various connectivity issues.*

**4.4.1 Straight Through Cable**

Here, the connections are same on both the ends the cable. This type of cable is used when we connect dissimilar devices [switch and router, router and hub, switch and PC, etc]. The wires and their respective pin numbers are shown below:



Figure 1.2. Straight through cable

Notice that only pins 1, 2, 3, and 6 are used. Just connect 1 to 1, 2 to 2, 3 to 3, and 6 to 6, and you’ll be up and networking in no time. However, remember that this would be an Ethernet- only cable and wouldn’t work with Voice, Token Ring, ISDN, etc

**4.4.2 Cross-Over Cable**

Here, the connections are different with a specific pattern. This type of cable is used when we connect similar devices [router and router, switch and switch, PC and PC, etc] and with some exceptions [switch and hub, Router and PC]. The wires and their respective pin numbers are shown below:



Figure 1.3 Cross-Over cable

The same four wires are used in this cable as in the straight-through cable, but we just connect different pins together. Notice that instead of connecting 1 to 1, etc. here we connect pins 1 to 3 and 2 to 6 on each side of the cable.

**4.4.3 Roll-over Cable**

Here, the connections are made in reverse order. This type of cable is used to connect the router/switch to the PC via console port for management purposes.



Figure 1.4 Roll-Over cable

**5. Setting up a Simple Network**

In this experiment, we will learn how to connect two PCs to create a simple Peer-to-Peer network. The instructions for this lab focus on the Windows XP operating system. You will share a folder on one workstation and connect to that folder from the other workstation.

The two PCs will be connected with a switch between them [see figure 1.5]. Using a switch allows for more than just two workstations to be connected depending on the number of ports on the switch.

Figure 1.5 Simple network topology

## 5.1 Check Local Area Network Connections

## 5.1.1 Verify that the Network Interface Card (NIC) is installed for the two PCs

1. From device manager verify that the NIC is installed. In each PC what is the type of your NIC?
2. Click on the Start button at the lower left of the computer screen and select "**Run..."**
3. In the field, type **cmd**, which will allow for a command prompt window to appear.
4. Type **ping 127.0.0.1** or **ping local host.** This is the diagnostic or loopback address, and if you get a successful ping, your IP stack is then considered to be initialized and your Network Interface Card (NIC) card is functioning. If it fails, then there is a problem with the NIC card. This doesn’t mean that a cable is plugged into the NIC, only that the IP protocol stack on the host can communicate to the NIC.

**5.1.2 Verify the Cables.**

Verify that the pins are wired straight through by holding the two RJ-45 connectors for each cable side by side with the clip down and inspect them. All pins should have the same color wire on the same pin at both ends of the cable. (Pin 1 should match pin 1 and pin 8 should match pin 8 etc.)

5.1.3 Plug in and Connect the Equipment

Plug the straight through cable from PC 1 into port 1 of the switch and the cable from PC 2 into port 2 of the switch. After the PCs have booted, check the green link light on the back of each NIC and the green lights on ports 1 and 2 of the switch to verify that they are communicating. This also verifies a good physical connection between the switch and the NICs in the PCs (OSI Layers 1 and 2). If the link light is not on it usually indicates a bad cable connection, an incorrectly wired cable or the NIC or switch may not be functioning correctly.

**5.1.4 Observe the Configuration of Each PC**

1. In the DOS windows type **ipconfig /all** and press enter.
2. There is a lot of information that is returned. Fill in the following table with values from the information returned.

|  |  |
| --- | --- |
| Physical Address |  |
| IP address |  |
| Gateway |  |
| Host name |  |
| Subnet Mask |  |

1. Right click on ***my computer*** in the desktop, select **computer name** then select change, write name of your computer then select **workgroup, write a** name of your workgroup "network\_lab"

**Question#4:**

What is the different between workgroup LAN and domain LAN.

**5.1.5 Configure an IP address and subnet mask for *each computer* manually**

1. At the desktop window, find the icon labeled My Network Places. Right click on this icon and select "Properties."
2. A window named “Local Area Connection”. Right click on this icon and again select "Properties."
3. Double click "Internet Protocol (TCP/IP)" Select **Use the following IP address***.*

*  *

Figure 1.6 Configuring IP address

1. Set the IP address to be 172.5.5.5 and the Subnet mask to be 255.255.0.0. Clear the Default Gateway and DNS Server fields and click on OK for both windows.(what is the class of this ip address Class A Or B or C).
2. Verify that the IP Address for the computer has indeed changed. To do this, execute the ipconfig/all command again.
3. Once each of you has set up the configuration correctly, it is time to verify that all computers are on the same network, and can indeed communicate with each other.
4. Repeat the steps 1-4 for the second PC but set the IP to 172.5.5.6

**5.1.6 Verify Connectivity in Your Network with Ping**

Use the Ping Command to check for basic TCP/IP connectivity. This will verify that you have a good OSI Layers 1 through 3 connections.

1. Click on Start then Command Prompt. Enter the Ping command followed by the IP address of the other workstation. Fill the following table with the values returned after each execution.



1. Ping an address that is not in your network for example 192.168.0.253. What is the result and how is it different from the result of the above step?
2. Change the IP address of the second PC to 172.6.5.6, check the connection again what do you notice? How to make the Two PCs connected again?

**5.2 File, Folders and Sharing Options**

* 1. Click “My network places”, Click on "Microsoft Windows Network" choice in the drop down box. You should see a list of workgroups/domains. What are they?
	2. Click on "network\_lab ". You should see a list of all the network\_lab machines. Click on each of the machines. What folder do you see on every machine?
	3. Click on the Start button at the lower left of the computer screen and select "**Run..."** type [**\\your**](file:///%5C%5Cyour) **Machine name**.What do you see?
	4. Put a file in this folder (any file will do), Create a folder called subshare in the Labshare Put a file in subshare, Right click on the Labshare folder and click on sharing and security You should see a window titled Labshare share properties Click on share this folder on the network Enter a share name of your choice Click on apply Click on ok, Look at the icon for the folder. How has it changed?
	5. Can you access the file placed in the Labshare on the other machine? Can you access the file placed in the subshare folder on the other machine? Did you have to "turn on" sharing for subshare to allow access? If not why was the folder accessible?
	6. Try to place a file in the Labshare on your neighbor's machine. Can you do it? If not what do you have to do to make it possible?
	7. Can you see (access) shares on other machines in the lab? What prevents you from reading shares on any machine that has simple file sharing enabled (what we are doing) and has created a network share?
	8. It is possible to associate a drive letter i.e. x: with a network shared folder, this is called a network drive. Thereafter the drive letter appears as a device with windows explorer. Create a network drive as X: for a share on your neighbor's machine. How did you do it?

**ToDo#1:**

How do you connect 2 computers for file sharing without using hub or switch? Test the network during the lab.

1. **Various Network Related Commands**

To know and learn about various network related commands [ping, tracert, netstat, at, net, route, arp] and few definitions cum settings.

**6.1 IPCONFIG Command**

This command is used to get IP configurations present in your PC.

**6.2 PING Command**

Ping is a basic Internet program that lets you verify that a particular IP address exists and can accept requests. The verb ping means the act of using the ping utility or command. Ping is used diagnostically to ensure that a host computer you are trying to reach is actually operating. Various options available in the ping command (see windows help).

1. Mention the difference between fragmenting and non-fragmenting packets.
2. Test the reach ability towards a Ritaj server with fragmenting option enabled and limit the number of echos to 5.

**6.3 TRACERT Command**

If someone would like to know how he goes from his house to his office he could just tell the list of the crossroads where he passes. The same way we can ask the data sent over from your computer to the web server which way does it go, through which devices? We ask it by using the utility called traceroute. In most computers today you can use this tool from the command line: In UNIX machines it is called traceroute, in MS Windows machines it is called tracert. Various options available in the ping command (see windows help).

1. Find the route from your PC to [ritaj.birzeit.edu].
2. Using the answers of the above, determine what is the first device your packet reaches to move from our network lab.

**6.4 Enhanced Ping**

TJPing tool is an excellent, widely acclaimed ping/lookup/traceroute utility for Win95/98/Me/NT/2000/XP. It's fully configurable, multithreaded, and is very fast. All configuration options, hosts, and interface settings are remembered from session to session. Users can log all results to the file of their choice.

1. Repeat the exercises provided to you in Ping and Tracert commands and store the result in a file for further reference.

**6.5 NETSTAT Command**

This command is used to get information about the open connections on your system (ports, protocols being used, etc.), incoming and outgoing data and also the ports of remote systems to which you are connected.

1. Open a browser connection to http server [www.birzeit.edu] and write down the outcome of the command 'netstat -an'.

**6.6 NetStat Live**

Have you ever wondered just how fast your network connection is? Not just how fast the modem is connected at, but how much data you can actually get? Does your internet connection sometimes seem slower than normal? NetStat Live is a small, easy to use TCP/IP protocol monitor which can be used to see your exact throughput on both incoming and outgoing data - whether you're using a modem, cable modem, DSL, or even local network! NSL doesn't just stop there, it lets you see how quickly your data goes from your computer to another computer on the internet; it even will tell you how many other computers your data must go through to get there! NSL also graphs your CPU usage of your system!

1. Generate traffic to any server using ping command [with various packet size options] or download a file and see how much of your outgoing interface is being used.

**Question#5:**

What are the functions of the following commands: AT Command, NET Command.

##