Experiment No. (1)

Introduction to Network Lab

Object:

1. Give an indication about network importance in daily life and network engineering role in Institutions.
2. Reviewing type of network (LAN, WAN, MAN).
3. Explain (by hand) in detail computer hardware component.

Theory:

In this experiment PC and its peripheral (LAN card, etc.) will be used.

Procedure:

1. Turn off the computer and unplug all wires connected to the tower and if there is a power switch on the back switch it off.
2. Take out the screws on the back of the tower, take out the panel, and then wear an anti-static wrist strap to protect components by earthing your static electricity, and then take out the motherboard tray.
3. Take the motherboard and screw it on to the motherboard tray then slide it back into the case.
4. Firmly insert RAM (Random Access Memory) sticks into the long and narrow slots usually located at the top right of the motherboard
5. Carefully place the CPU into the socket that is square shaped on the motherboard then place the CPU fan on top.
6. For video cards, look for a slot about the length of your middle finger and has very small lever. Take out the small case panel about the size of your finger on the back and firmly insert the card into the slot, make sure the back of the card comes outside.

For sound/network cards look for a slot similar to the video card slot, but slightly shorter and without the lever.

7. Slowly slide the hard drive into the hard drive bay usually located at the front of the tower then connected the cables from the back of the hard drive to the motherboard.

8. CD (compact Disk)/DVD (Digital Video Disc) ROM (Read Only Memory) drives are similar to hard drives, just slide it into the bay at the top (right or left depending on the panel that was open) and connect the wires.

9. For audio devices match the colors and USB is pretty much self-explanatory.

10. If you have a video card the back of it should be sticking outside which is where you connect the monitor cable to, unless there is no video card then you connect to the motherboard.

Discussion:

1. What is the advantage of increasing processor speed?
2. Complete the following table for your personal PC?

device	measure
Hard Disk	Giga bytes
Processor	
RAM	
Video card	

3. What is the difference between server and clients?
4. What is the main difference between Linux and Microsoft Windows?

Experiment No. (2)

Network Connection

Object:

Student should be distinguish between different type of network connections (cables, 802.11x and WiMax), pros and cons of each one of them and understand network terms. Reviewing type of network (LAN, WAN, MAN).

Theory:

In this experiment different types of Internet connections will be introduced with their technical features, and compared according to their pros and cons related to the criteria of speed, costs, availability, etc.

Network Terms:

Term	Description
Analog signals	Continuously changing natural signal like human voice.
Digital signals	the signals for the performance of computer by turning on and off a series of electronic switches represented by the numerical digits of 0 (the code for off) and 1(the code for on)
Bandwidth	amount of data that can be transmitted across a network or cable; usually measured in bits per second (bps)
Broadband	Refers to telecommunication in which a wide band of frequencies is available to transmit information.

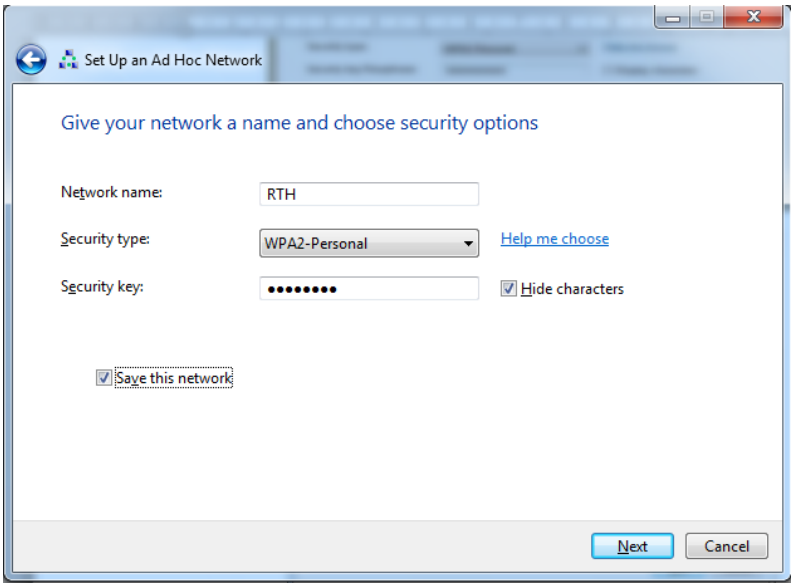
Baseband	Telecommunication system in which information is carried in digital form on a single un-multiplexed signal channel on the transmission medium.
Internet service provider (ISP)	A company that provides access to the Internet. For a monthly fee, the service provider gives a software package, username, password
ISDN (Integrated Services Digital Network)	Uses fully digital signals over copper phone wire, a standard telephone line. This means there is no conversion from digital to analog and back again in the manner that an analog modem works. Most ISDN lines offered by telephone companies give users two lines at once, called B channels. The users can use one line for voice and the other for data, or they can use both lines for data to give them data rates of 128 Kbps. Another version, called B-ISDN, is able to support transmission rates of 1.5 Mbps. B-ISDN requires fiber optic cables and is not widely available.
DSL (Digital Subscriber Lines)	Also known as xDSL (a generic name), is another broadband service that many telephone companies and other providers offer to consumers.

Procedure:

1. Set up a wireless network and file sharing (Win 7)
2. Open network and sharing center.
2. Setup new connection or network
3. Setup wireless ad hoc (computer to computer network)

4. Click next

5. Give name and security to the network



6. Open firewall

7. Choose windows firewall properties and turn off it from

- Domain profile
- Private profile
- Public profile

8. Open (change advance sharing setting)

9. Choose turn off password protected sharing

Discussion:

1. Complete the following table

IEEE 802.11 protocol	Data rate (Mbit)	Frequency GHz	Range (m)		Modulation
			In	out	
a					OFDM
b		2.4			
g					
n		2.4/5			

2. What is the advantage and disadvantage of using wireless connection
3. What is the difference between WiMax and Wifi?

Experiment No. (3)

Cables

Object:

Study of different types of network cables and implement a cross wired cables and straight through cables using crimping tool.

Component:

1. Small section of Cat-5 Ethernet wire
2. RJ-45 Male Plugs
3. Cable stripper or knife
4. RJ-45 Crimping tool
5. Electrical Network Cable tester

Theory:

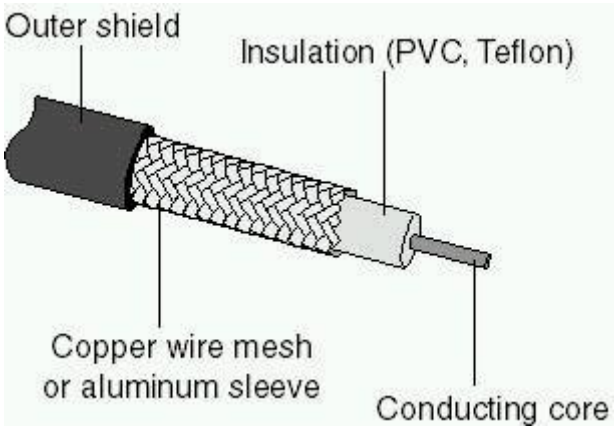
The following terms should be very well known by network engineer

Terms:

Term	Description
BNC	British Naval Connector is the connector used with coaxial cables.
Fiber Optic Cable	Fiber optic cable uses light to transmit information across a network. The core of the cable is made of glass, which is protected by a layer of gel or plastic. A plastic cover surrounds the entire cable.
EMI	(Electro-Magnetic Interference) The interference of electrical signals across a cable by outside electrical or magnetic devices. It is a factor that is used to evaluate cable.
RJ-11	A registered jack 11 is a telephone connector used

	on modern telephone lines.
RJ-45	A registered jack 45 is an eight-wire connector used to connect computers to category 5 unshielded twisted pair (UTP) cables in a network.
UTP	Unshielded Twisted-Pair Cable is network cable that consists of up to 4 pairs of wires. Each pair is twisted around each other at a different rate and the entire cable is encased in a protective plastic covering. The twisting of the wires in cables is to help prevent EMI (Electro- Magnetic Interference).
Thin Coaxial Cable	Thin coaxial cable is often referred to as *ThinNet*. It consists of a copper wire surrounded first by a layer of plastic, then a layer of metal mesh and a final layer of protective plastic. It is used for peer-to-peer networking

Thin Coaxial Cable



Decision Factor	Thin Coaxial Cable
Maximum Bandwidth	10 megabits per second.
EMI	Significant problems with neighboring electrical equipment.
Signal Attenuation	Maximum distance is 185 meters.
Expansion Issues	Expansion into multiple rooms is difficult since each computer must be connected directly on to the cable in a chain fashion, often referred to as a *bus topology*. The cable is thicker and less flexible than UTP cable. This cable is best used for peer-to-peer networking in a small workgroup LAN.
Relative Cost	Low.

Unshielded Twisted-Pair Cable

Unshielded twisted-pair cable is separated into five categories

- Category 1 is telephone cable.
- Category 2 was used for token ring networks, Data up to 4 Mbps.
- Categories 3 and 4 can be used with Ethernet networks, but suffer more from EMI than category 5.

  Category 3 cables (Data up to 10 Mbps) typically have two twists per foot.

  Category 4 (20Mbps) cables have more twists per foot;
- Category 5 (100Mbps) cable is primarily used in LANs. This cable has a very high twist rate per foot.

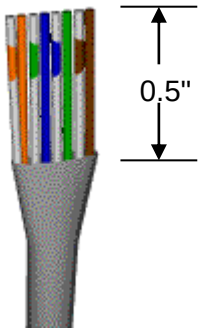
  Category 5e (1000Mbps)

- Category 6 (Data to 2500Mbps)

Decision Factor	Unshielded Twisted-Pair Cable: Category 5
Signal Attenuation	Maximum distance is 100 meters.
Expansion Issues	The cable is thin and flexible, which makes installation easy. Expansion is easy, but specialized network equipment is needed to boost the signal. This equipment increases the cost of expansion. This cable is used as a standard today in all Ethernet LANs.
Relative Cost	Least expensive.

Procedure:

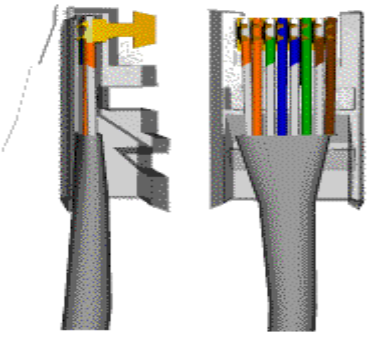
1. Strip about 1½ inches (40mm) of the outside PVC jacket, then trim any excess cord that accompanies the cable pairs.



2. Untwist the pairs to the edge of the stripped PVC jacket. As you go, mold each wire into a parallel, flat shape, like the tines of a fork, ordering the wire colors as necessary to match the pictures to the right. Now the wires must be gathered together and trimmed so that they can be inserted into the RJ-45 plug. Using the cutter in the crimp tool, trim the untwisted wires into a flat straight end about ½ inch (13mm) long. The wires gathered and trimmed are illustrated in the picture to the right.

3. While holding the cable firmly, insert the wires into the plug, taking great care that the wires remain properly ordered. The cable jacket should

pass into the plug, giving the entire assembly some stress relief once it's crimped.



4. Double-check the wire ordering. Look at the plug end of the cable assembly. The copper core of each wire should be visible and pressed tightly against the interior end of the plug. You should see a glint of copper from each wire clearly.

5. Insert the cable assembly into your crimp tool. Keeps consistent pressure on the assembly, forcing the cable into the plug, insuring the wires remain in their intended location, firmly squeeze the crimp tool, if you are using a less-expensive, non-ratcheted tool, squeeze twice.

6. Repeat at the opposite end of your cable.

7. Use a cable tester to ensure cables are correct. Re-crimp if necessary, and test again.

Discussion:

1- Complete the following table for fiber optical:

Decision Factor	**Fiber Optic Cable**
Maximum Bandwidth	
EMI	
Signal Attenuation	
Expansion Issues	
Relative Cost	

2- What is the relationship between twists to EMI in UTP cables?

3- What is thick net cable?

4- What is STP? And list the difference with UTP.

Experiment No. (4)

Network Device

Object:

Understanding how networking devices operate and identifying the functions they perform are essential skills for any network administrator.

Theory:

Following devices should understand in detail very well.

1. Hub
2. Switch
3. Router
4. Repeater

Procedure:

Following should understand in detail very well.

1- Repeater: is a device (work on physical layer) that receives a digital signal on an electromagnetic or optical transmission medium and regenerates the signal along the next leg of the medium. In electromagnetic media, repeaters overcome the attenuation caused by free-space electromagnetic-field divergence or cable loss. A series of repeaters make possible the extension of a signal over a distance. Repeaters remove the unwanted noise in an incoming signal. Unlike an analog signal, the original digital signal, even if weak or distorted, can be clearly perceived and restored. With analog transmission, signals are re-

strengthened with *amplifiers* which unfortunately also amplify noise as well as information.

2- Hubs: are used in networks (layer 1) that use twisted-pair cabling to connect devices. Hubs can also be joined together to create larger networks. *Hubs* are simple devices that direct data packets to all devices connected to the hub, regardless of whether the data package is destined for the device. This makes them inefficient devices and can create a performance bottleneck on busy networks.

3- Switches: (layer 2) are the connectivity points of an Ethernet network. Devices connect to switches via twisted-pair cabling, one cable for each device. The difference between hubs and switches is in how the devices deal with the data that they receive. Whereas a hub forwards the data it receives to all of the ports on the device, a switch forwards it only to the port that connects to the destination device. It does this by *learning* the MAC address of the devices attached to it, and then by matching the destination MAC address in the data it receives.

4- Bridges: (layer 2) are used to divide larger networks into smaller sections. They do this by sitting between two physical network segments and managing the flow of data between the two. By looking at the MAC address of the devices connected to each segment, bridges can elect to forward the data (if they believe that the destination address is on another interface), or block it from crossing (if they can verify that it is on the interface from which it came).

5- Routers: are devices that join multiple networks together. Technically, a router is work on Layer 3, meaning that it connects

two or more networks. A router derives its name from the fact that it can route data it receives from one network onto another. When a router receives a packet of data, it reads the header of the packet to determine the destination address. Once it has determined the address, it looks in its routing table to determine whether it knows how to reach the destination and, if it does, it forwards the packet to the next hop on the route.

6- Gateway: (layer 7) Any device that translates one data format to another is called a gateway. Some examples of gateways include a router that translates data from one network protocol to another, a bridge that converts between two networking systems, and a software application that converts between two dissimilar formats. The key point about a gateway is that only the data format is translated, not the data itself. In many cases, the gateway functionality is incorporated into another device.

Discussion:

1. What is the difference between active hub, passive hub and repeater hub?
2. Why repeater is not very useful for analog signal, whereas its work very well in digital signal?
3. study the following table and discuss it:

	Hub	Switch	Router	Workstation
Hub	Crossover	Crossover	Straight	Straight
Switch	Crossover	Crossover	Straight	Straight
Router	Straight	Straight	Crossover	Crossover
Workstation	Straight	Straight	Crossover	Crossover

4. What is the difference between bridge and switch?
5. What is the difference between router and switch?

Experiment No. (5)

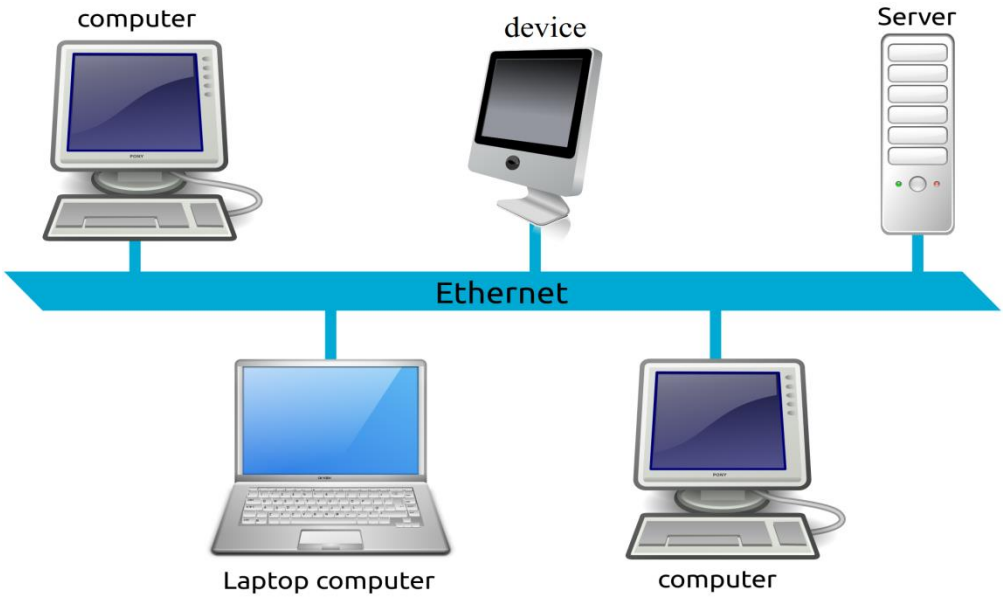
Building LAN Network using Hub

Object:

Build a LAN network using Ethernet cable

Theory:

LAN is a computer network that connects a relatively small area (a single building or group of buildings). Most LANs connect workstations and computers to each other. Each computer (also known as a "node"), has its own processing unit and executes its own programs; however, it can also access data and devices anywhere on the LAN.



Component:

1. Two or more computers/Laptops. (Example: 5 Computers).

2. Two or more NIC (Network Interface Card). In this case 5 NICs for 5 computers.
3. LAN cable (UTP cables with the desired length with RJ 45).
4. Eight port Hub.

Procedure:

1. Install the NIC into the PCMCIA slot of the PC's mother board. NIC is a hardware that interfaces between the computer and the network. The NIC has RJ 45 type port.
2. Take the desired length of 5 LAN cables and terminate both the ends with a RJ 45 type connector.
3. Now, connect one end of each of 5 cables to the computer and the other end to the Hub.
4. Now, The physical network is ready
5. Assign IP address, Subnet Mask to every PC.
6. To verify the IP address and Subnet Mask assignment in each computer, go to command prompt and type **CD:\>ip config /all**
7. To check the connectivity between PCs, go to command prompt and type CD:\>**ping <destination ip address>**
8. In return to the ping, the computer receives a reply back as an acknowledgement, thus the LAN connectivity is UP.

Discussion:

1. What is the difference between a physical design and a logical design?
2. What is the difference between Fast Ethernet and regular Ethernet?
3. List the advantages and disadvantages of local area networks.
4. What are the primary differences between baseband technology and broadband technology?

Experiment No. (6)

Network Tools 1

Object:

Get acquainted with the basic network control, diagnostics and management tools.

Theory:

In this experiment, students will learn two commands which are IPconfig and Nbtstat

Procedure:

1- **IPconfig:** Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, ipconfig displays the IP address, subnet mask, and default gateway for all adapters.

- **The general form is**

ipconfig [/? | /all | /release [adapter] | /renew [adapter] | /flushdns | /registerdns | /displaydns | /showclassid adapter | /setclassid adapter [Adapter [ClassID]]]

- **Try to apply all the following parameters**

Note1: To specify an adapter name, type the adapter name that appears when you use ipconfig without parameters.

Parameter	Description
/all	Displays the full TCP/IP configuration for all adapters.. Adapters can represent physical interfaces, such as installed network adapters, or logical interfaces.
/renew [Adapter]	Renews DHCP configuration for all adapters (if an adapter is not specified) or for a specific adapter if the Adapter parameter is included.
/release [Adapter]	Sends a DHCPRELEASE message to the DHCP server to release the current DHCP configuration and discard the IP address configuration for either all adapters (if an adapter is not specified) or for a specific adapter if the Adapter parameter is included.
/flushdns	Flushes and resets the contents of the DNS client resolver cache. During DNS troubleshooting, you can use this procedure to discard negative cache entries from the cache.
/displaydns	Displays the contents of the DNS client resolver cache, which includes both entries preloaded from the local Hosts file and any recently obtained resource records for name queries resolved by the computer.
/registerdns	Initiates manual dynamic registration for the DNS names and IP addresses that are configured at a computer. You can use this parameter to troubleshoot a failed DNS name registration or resolve a dynamic update problem between

	a client and the DNS server without rebooting the client computer.
/?	Displays help at the command prompt.

2- **Nbtstat:** Displays NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS name tables for both the local computer and remote computers, and the NetBIOS name cache. Nbtstat allows a refresh of the NetBIOS name cache and the names registered with Windows Internet Name Service (WINS). Used without parameters, nbtstat displays help.

- **The general form is**

nbtstat [-a RemoteName] [-A IPAddress] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [Interval]

- **Try to apply all the following parameters**

Parameter	Description
-a RemoteName	Displays the NetBIOS name table of a remote computer, where RemoteName is the NetBIOS computer name of the remote computer. The NetBIOS name table is the list of NetBIOS names that corresponds to NetBIOS applications running on that computer.
-A IPAddress	Displays the NetBIOS name table of a remote computer, specified by the IP address (in dotted decimal notation) of

	the remote computer.
-c	Displays the contents of the NetBIOS name cache, the table of NetBIOS names and their resolved IP addresses.
-n	Displays the NetBIOS name table of the local computer.
-r	Displays NetBIOS name resolution statistics.
-RR	Releases and then refreshes NetBIOS names for the local computer that is registered with WINS servers.
/?	Displays help at the command prompt.

Discussion:

1- What is the benefit of IP config?

2- What is the difference between ipconfig and ipconfig/all?

3- Define NetBIOS

Experiment No. (7)

Network Tools 2

Object:

Get acquainted with the basic network control, diagnostics and management tools.

Theory:

In this experiment, students will learn two commands which are ping and Tracert

Procedure:

1- **Ping:** verifies IP-level connectivity to another TCP/IP computer by sending Internet Control Message Protocol (ICMP) Echo Request messages. The receipt of corresponding Echo Reply messages are displayed, along with round-trip times. Ping is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution. Used without parameters, ping displays help

- **The general form is**

Ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS] [-r count] [-s count] [[-j host_list] | [-k host_list]] [-w timeout] target_name

- **Try to apply all the following parameters**

Parameter	Description
-t	Specifies that ping continue sending Echo Request messages to the destination until interrupted. To interrupt and display statistics, press CTRL-BREAK. To interrupt and quit ping, press CTRL-C.
-a	Specifies that reverse name resolution is performed on the destination IP address. If this is successful, ping displays the corresponding host name.
-n Count	Specifies the number of Echo Request messages sent. The default is 4.
-l Size	Specifies the length, in bytes, of the Data field in the Echo Request messages sent. The default is 32. The maximum size is 65,527.
-f	Specifies that Echo Request messages are sent with the Don't Fragment flag in the IP header set to 1.
-i TTL	Specifies the value of the TTL field in the IP header for Echo Request messages sent. The default is the default TTL value for the host. For Windows XP hosts, this is typically 128. The maximum TTL is 255.
-v TOS	Specifies the value of the Type of Service (TOS) field in the IP header for Echo Request messages sent. The default is 0. TOS is specified as a decimal value from 0 to 255.
-r Count	Specifies that the Record Route option in the IP header is used to

	record the path taken by the Echo Request message and corresponding Echo Reply message. Each hop in the path uses an entry in the Record Route option. If possible, specify a Count that is equal to or greater than the number of hops between the source and destination. The Count must be a minimum of 1 and a maximum of 9.
-w Timeout	Specifies the amount of time, in milliseconds, to wait for the Echo Reply message that corresponds to a given Echo Request message to be received. If the Echo Reply message is not received within the time-out, the "Request timed out" error message is displayed. The default time-out is 4000 (4 seconds).
Target Name	Specifies the destination, which is identified either by IP address or host name.
/?	Displays help at the command prompt.

2- **Tracert:** Determines the path taken to a destination by sending Internet Control Message Protocol (ICMP) Echo Request messages to the destination with incrementally increasing Time to Live (TTL) field values. The path displayed is the list of near-side router interfaces of the routers in the path between a source host and a destination. The near-side interface is the interface of the router that is closest to the sending host in the path. Used without parameters, tracert displays help.

- **The general form is**

tracert [-d] [-h max_hop] [-j host_list] [-w timeout] target

- **Try to apply all the following parameters**

Parameter	Description
d	Prevents tracert from attempting to resolve the IP addresses of intermediate routers to their names. This can speed up the display of tracert results.
-h max_hop	Specifies the maximum number of hops in the path to search for the target (destination). The default is 30 hops.
-w timeout	Specifies the amount of time in milliseconds to wait for the ICMP Time Exceeded or Echo Reply message corresponding to a given Echo Request message to be received. If not received within the time-out, an asterisk (*) is displayed. The default time-out is 4000 (4 seconds).
target	Specifies the destination, identified either by IP address or host name.
-?	Displays help at the command prompt.

Discussion:

1- What is the difference between Ping and tracert?

2- How ICMP is used in ping/ tracert?

3- Write a report about ICMP and its segment structure?

Experiment No. (8)

Network Tools 3

Object:

Get acquainted with the basic network control, diagnostics and management tools.

Theory:

In this experiment, students will learn the three commands which are Route, ARP and Nslookup

Procedure:

1- **Route:** Displays IP routing table and enables adding and deleting IP routes

- **The general form is**

route [-f] [-p] [command [target] [MASK subnet_mask] [gateway] [METRIC metric] [IF interface].

- **Try to apply all the following parameters**

Parameter	Description
-f	Clears the routing tables of all gateway records. If used with another command, cleaning is performed before the command.
-p	If used with ADD command, the route remains persistent during consecutive system restarts. Default routes are not preserved during system restart. This switch is ignored for other commands

	having effect on persistent routes.
command	one of the following: PRINT Prints the route ADD Adds the route DELETE Deletes the route CHANGE Modifies existing route
target	Denotes target host name.
MASK	Implies, that the next parameter stands for subnet mask (if not specified, default value 255.255.255.255 is taken).
gateway	Denotes gateway.
interface	Interface number for a particular route
METRIC	Specifies the metric, i.e. the cost of reaching the target.

2- **ARP:** Displays and modifies entries in the Address Resolution Protocol (ARP) cache, which contains one or more tables that are used to store IP addresses and their resolved Ethernet or Token Ring physical addresses. There is a separate table for each Ethernet or Token Ring network adapter installed on your computer. Used without parameters, ARP displays help.

- **The general form is**

ARP [-a [InetAddr] [-N IfaceAddr]] [-g [InetAddr] [-N IfaceAddr]] [-d InetAddr [IfaceAddr]] [-s InetAddr EtherAddr [IfaceAddr]].

- **Try to apply all the following parameters**

Parameter	Description
-a [InetAddr] [-N IfaceAddr]	Displays current ARP cache tables for all interfaces. To display the ARP cache entry for a specific IP address, use arp -a with the InetAddr parameter, where InetAddr is an IP address. To display the ARP cache table for a specific interface, use the -N IfaceAddr parameter where IfaceAddr is the IP address assigned to the interface. The -N parameter is case-sensitive.
-g [InetAddr] [-N IfaceAddr]	Identical to -a.
-d InetAddr [IfaceAddr]	Deletes an entry with a specific IP address, where InetAddr is the IP address. To delete an entry in a table for a specific interface, use the IfaceAddr parameter where IfaceAddr is the IP address assigned to the interface. To delete all entries, use the asterisk (*) wildcard character in place of InetAddr.
-s InetAddr EtherAddr [IfaceAddr]	Adds a static entry to the ARP cache that resolves the IP address InetAddr to the physical address EtherAddr. To add a static ARP cache entry to the table for a specific interface, use the IfaceAddr parameter where IfaceAddr is an IP address assigned to the interface.

/?	Displays help at the command prompt.

3- **Nslookup:** Lookup IP addresses on a NameServer.

- **The general form is**

nslookup [-SubCommand ...] [{ComputerToFind| [-Server]}]

- **Try to apply all the following parameters**

Parameter	Description
ComputerToFind	Looks up information for ComputerToFind using the current default DNS name server, if no other server is specified. To look up a computer not in the current DNS domain, append a period to the name.
-Server	Specifies to use this server as the DNS name server. If you omit -Server, the default DNS name server is used.
{help|?}	Displays a short summary of nslookup subcommands.

Discussion:

1- What is the benefit of ARP?

2- What is the benefit of Nslookup?

3- List and describe nslookup subcommand?

4- Explain with detail Netstat?

Experiment No. (9)

Internet Protocol (IP)

Object:

Study the structure of IP and its classes**.**

Theory:

IP addresses are used to uniquely identify individual TCP/IP networks and hosts (computers and printers) on networks in order for devices to communicate. Workstations and servers on a TCP/IP network are called "HOSTS" and each will have a unique IP address which is referred to as its "HOST" address. TCP/IP is the most widely used protocol in the world. In order for a host to access the Internet, it must have an IP address.

IP address format

In its basic form, the IP address has two parts; a Network Address and a Host Address. The network portion of the IP address is assigned to a company or organization. Routers use the IP address to move data packets between networks. IP Addresses are 32 bits long (with current version IPv4) and are divided into 4 octets of 8 bits each.

They operate at the network layer, Layer 3 of the OSI model, (the Internetwork Layer of the TCP/IP model) and are assigned statically (manually) by a network administrator or dynamically (automatically) by a Dynamic Host Configuration Protocol (DHCP) Server.

The IP address of a workstation (host) is a "logical address" meaning it can be changed. The MAC address of the workstation is a 48-bit "physical address" which is burned into the NIC and cannot change unless the NIC is replaced. The combination of the logical IP address and the physical MAC address help route packets to their proper destination.

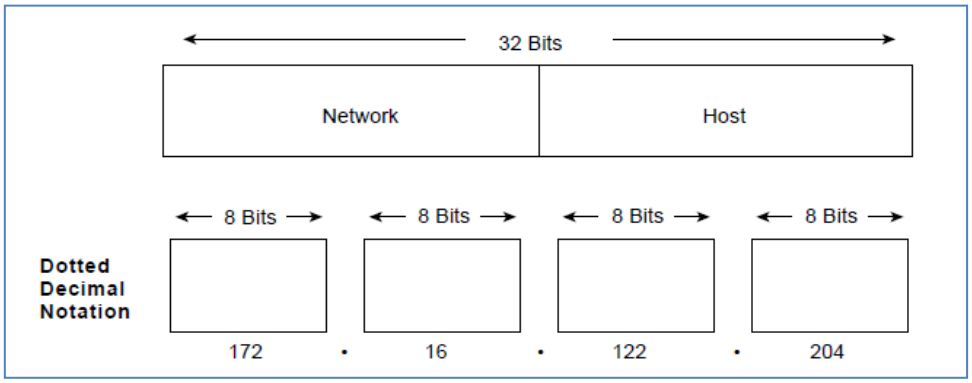


Figure 1: An IP address consists of 32 bits, grouped into four octets.

IP Address Classes

IP addressing supports five different address classes: A, B, C, D, and E. only classes A, B, and C are available for commercial use.

The left-most (high-order) bits indicate the network class. Table 1 provides reference information about the five IP address classes.

Table 1. IP Classes ranges

Class	1st Octet Decimal Range	1st Octet High Order Bits	Network/Host ID (N=Network, H=Host)	Default Subnet Mask	Number of Networks	Hosts per Network (Usable Addresses)
A	1 – 126	0	N.H.H.H	255.0.0.0	126 ($2^7 - 2$)	16,777,214 ($2^{24} - 2$)
B	128 – 191	10	N.N.H.H	255.255.0.0	16,382 ($2^{14} - 2$)	65,534 ($2^{16} - 2$)
C	192 – 223	110	N.N.N.H	255.255.255.0	2,097,150 ($2^{21} - 2$)	254 ($2^8 - 2$)
D	224 – 239	1110	Reserved for Multicasting			
E	240 – 254	1111	Experimental; used for research			

Private IP address

Some blocks of addresses had been reserved for special purposes, one of these purposes was for private networking and it is these private addresses that help to relieve the pressure on the remaining address space and make possible many of the cable and DSL routers that people have at home today to share their Internet connection amongst many PCs. In another words, using a private IP address on a residential or business computer can improve network security and conserve public addressing space. Table 2 show private IP address ranges.

Table 2. Private IP address

Class	Private Networks	Subnet Mask	Address Range
A	10.0.0.0	255.0.0.0	10.0.0.0 - 10.255.255.255
B	172.16.0.0- 172.31.0.0	255.240.0.0	172.16.0.0 - 172.31.255.255
C	192.168.0.0	255.255.0.0	192.168.0.0- 192.168.255.255

Procedure:

Try to write down all the ranges of all classes in decimal and convert it to binary to see how the bits are detailed in the IP classes

Discussion:

1- Why class A is ended to address 126? What 127.0.0.0 to 127.255.255.255 used for?

2- What is the role of subnet Mask?

3- What is the purpose of private IP?

4- What is the difference between IPv4 and IPv6?

5- What is NAT/ PAT?

Remark

Examine the following (binary and decimal)

128	64	32	16	8	4	2	1		
1	0	0	0	0	0	0	0	=	128
1	1	0	0	0	0	0	0	=	192
1	1	1	0	0	0	0	0	=	224
1	1	1	1	0	0	0	0	=	240
1	1	1	1	1	0	0	0	=	248
1	1	1	1	1	1	0	0	=	252
1	1	1	1	1	1	1	0	=	254
1	1	1	1	1	1	1	1	=	255

Experiment No. (10)

Introduction to Packet Tracer

Object:

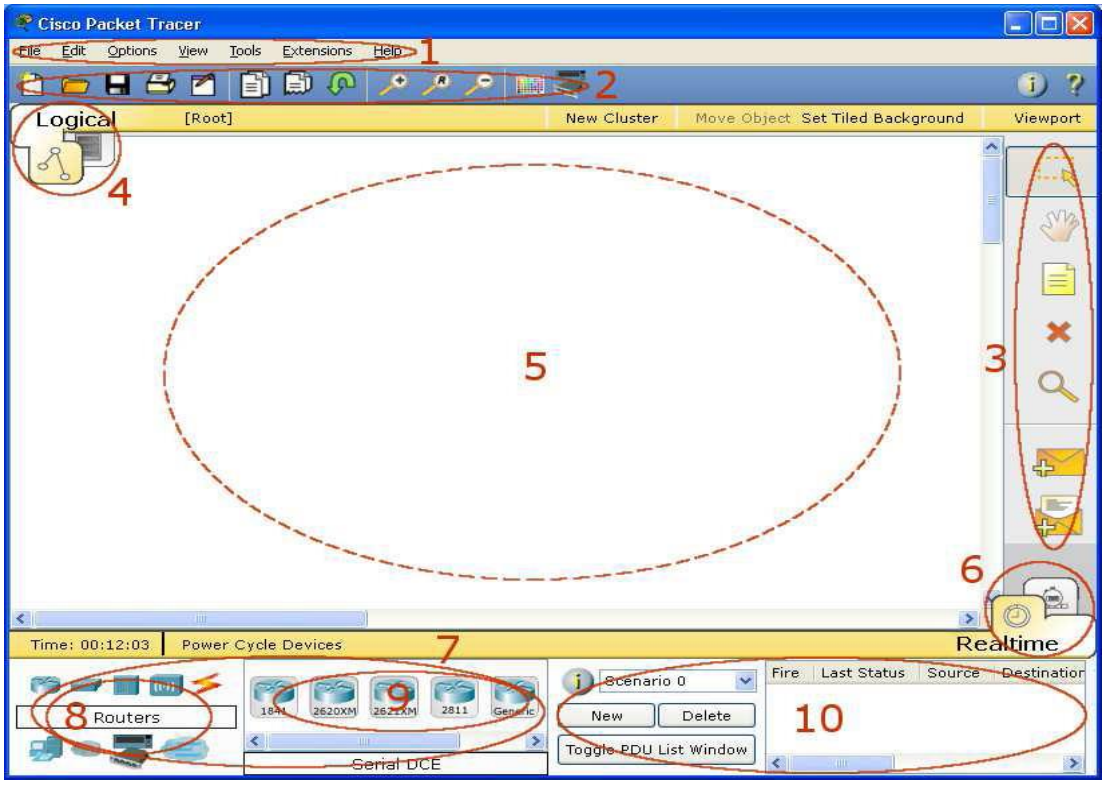
To give general introduction of packet tracer network simulator.

Theory:

Packet Tracer is a standalone, medium-fidelity, simulation-based learning environment for networking novices to design, configure, and troubleshoot computer networks at a CCNA-level of complexity. Packet Tracer supports student and instructor creation of simulations, visualizations, and animations of networking phenomena. Like any simulation, Packet Tracer relies on a simplified model of networking devices and protocols. However, real computer networks remain the benchmark for understanding network behavior. Packet Tracer was created to help address the "digital divide" in networking education, where many students and teachers lack access to equipment, bandwidth, and interactive modes of learning networking.

Procedure

1. Open Packet Tracer by Double-Click; the following screen represents the home screen for the simulator.



See the following important components:

1	**Menu Bar**	This bar provides the **File**, **Edit**, **Options**, **View**, **Tools**, **Extensions**, and **Help** menus. You will find basic commands such as **Open**, **Save**, **Print**, and **Preferences** in these menus. You will also be able to access the **Activity Wizard** from the **Extensions** menu.
2	**Main Tool Bar**	This bar provides shortcut icons to the **File** and **Edit** menu commands. This bar also provides buttons for **Zoom**, the drawing **Palette**, and the **Device Template Manager**. On the right, you will also find the **Network Information** button, which you can use to enter a description for the current network (or any text you wish to include).
3	**Common Tools Bar**	This bar provides access to these commonly used workspace tools: **Select**, **Move Layout**, **Place Note**, **Delete**, **Inspect**, **Add Simple PDU**, and **Add Complex PDU**. See "Workspace Basics" for more information.

4	**Logical/Physical Workspace and Navigation Bar**	You can toggle between the Physical Workspace and the Logical Workspace with the tabs on this bar. In Logical Workspace, this bar also allows you to navigate through levels of a cluster, create a new **New Cluster**, **Move Object**, **Set Tiled Background**, and **Viewport**. In Physical Workspace, this bar allows you to navigate through physical locations, create a **New City**, create a **New Building**, create a **New Closet**, **Move Object**, apply **Grid** to the background, **Set Background**, and go to the **Working Closet**.
5	**Workspace**	This area is where you will create your network, watch simulations, and view many kinds of information and statistics.
6	**Real-time /Simulation Bar**	You can toggle between Real-time Mode and Simulation Mode with the tabs on this bar. This bar also provides buttons to **Power Cycle Devices** as well as the **Play Control** buttons and the **Event List** toggle button in Simulation Mode. Also, it contains a clock that displays the relative **Time** in Real-time Mode and Simulation Mode.
7	**Network Component Box**	This box is where you choose devices and connections to put into the workspace. It contains the **Device-Type Selection** Box and the **Device-Specific Selection** Box.
8	**Device-Type Selection Box**	This box contains the type of devices and connections available in Packet Tracer 5.1. The **Device-Specific Selection** Box will change depending on which type of device you choose.
9	**Device-Specific Selection Box**	This box is where you choose specifically which devices you want to put in your network and which connections to make.
10	**User Created Packet Window***	This window manages the packets you put in the network during simulation scenarios. See the "Simulation Mode" section for more details.

2. Devices and connection supported

a. Choose a device type from the **Device- Type Selection** box

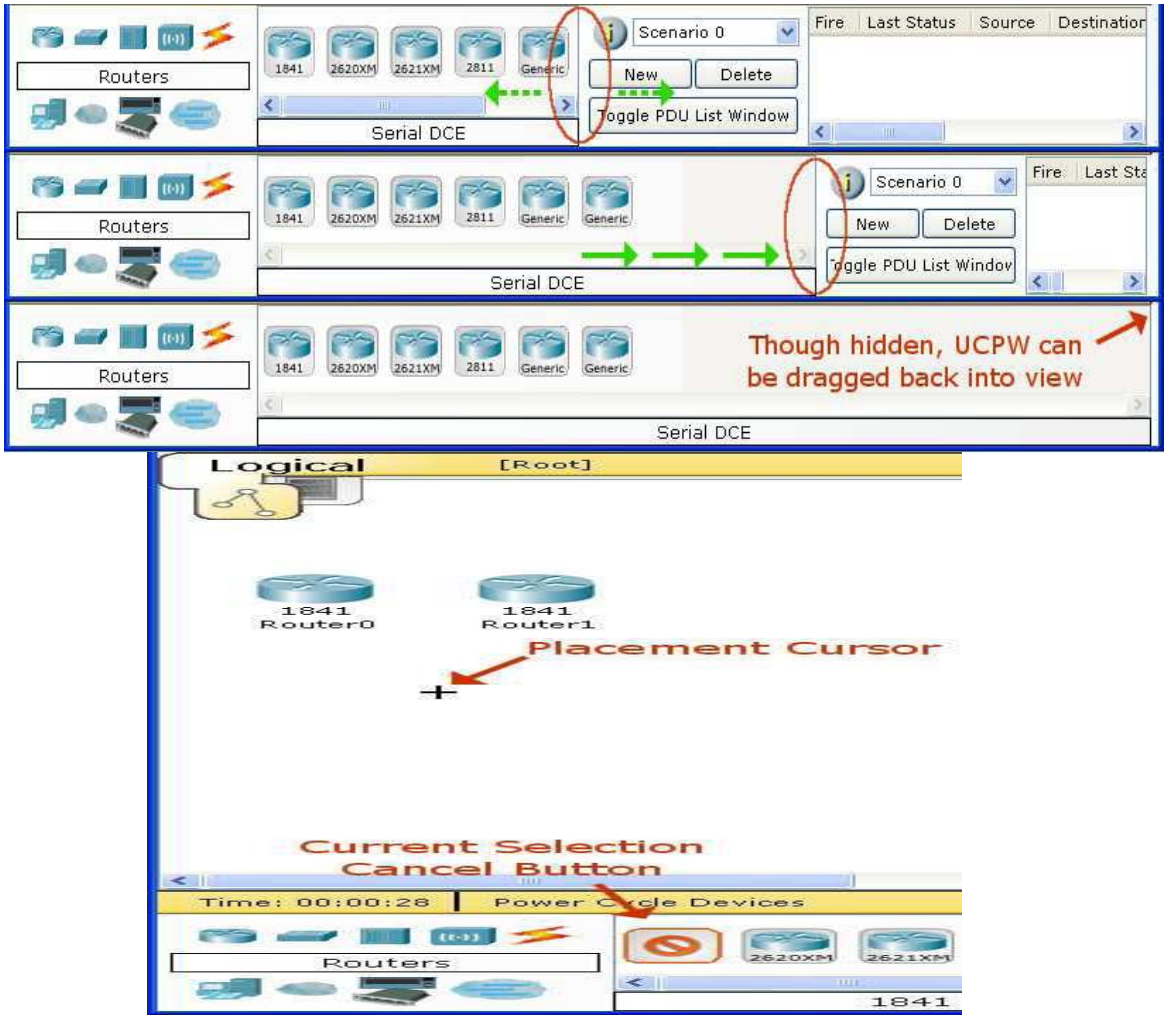
b. Click on the desired device model from the **Device-Specific Selection** box

c. Click on a location in the workspace to put your device in that location

d. If you want to cancel your selection, press the **Cancel** icon for that device

e. Alternatively, you can click and drag a device from the **Device Specific Selection** box onto the workspace

f. You can also click and drag a device directly from the **Device-Type Selection** box and a default device model will be Chosen.



3. Adding Modules

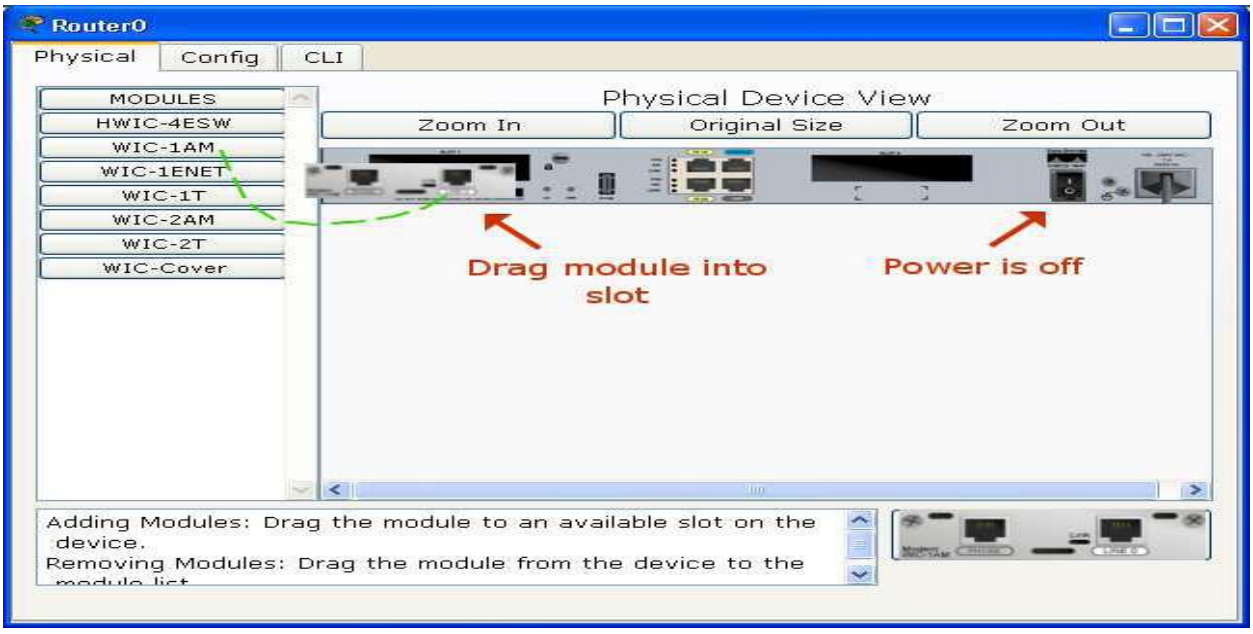
a. Click on a device to bring up its configuration window.

b. By default, you will be in the **Physical Device View** subpanel of the device.

c. You can browse (by clicking) through the list of modules and read their description in the information box at the bottom.

d. When you have found the module you want to add, simply drag it from the list into a compatible bay on the device picture.

e. You can remove a module by dragging it from the device back into the list.



4. Making Connections

a. To make a connection between two devices, first click the **Connections** icon from the **Device-Type Selection** box to bring up the list of available connections.

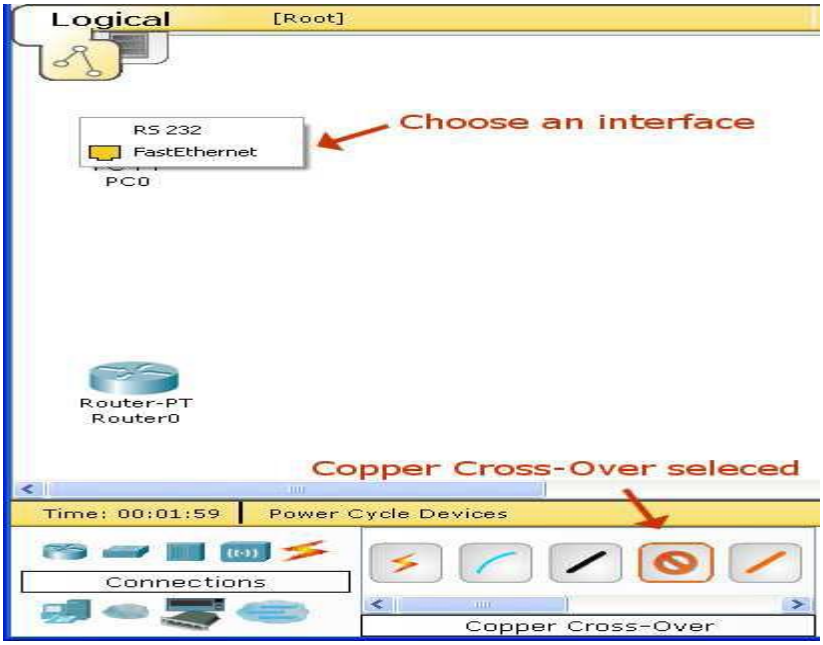
b. Then click the appropriate cable type.

c. The mouse pointer will change into a "connection" cursor.

d. Click on the first device and choose an appropriate interface to which to connect.

e. Then click on the second device and do the same.

f. A connection cable will appear between the two devices, along with link lights showing the link status on each end (for interfaces that have link lights).

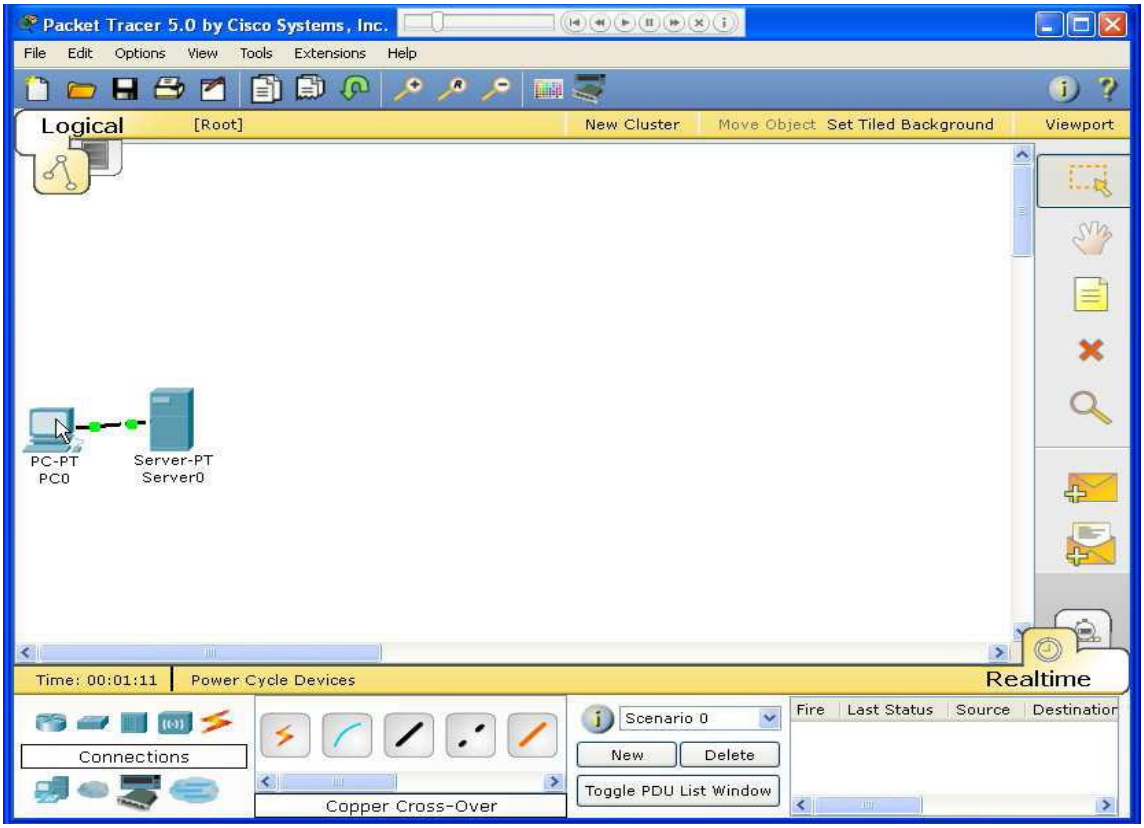


5. Connect PC to Server

1. Start creating a network by first selecting the End Devices. Add a Generic PC and a Generic Server to the workspace.
2. Under Connections, select the Copper Straight-through cable (solid black line) and connect the devices with it. The red lights on the link indicate that the connection is not working. Now, use the Delete tool to remove the Copper Straight-through cable, and use a Copper Cross-over cable (dashed line) instead. The lights should turn green at this point, and if the mouse pointer is held over either

the PC or the Server, the link status will be shown as “Up.” The network should look similar to the picture below.

3. Click on the PC. While paying attention to the link lights, turn the power on, off, and on again. Follow the same steps for the server. The link lights turn red when the device is off. This means that the link is down or is not working. The link lights turn green when the device is turned back on.
4. Try all three ways to learn about the devices. First, mouse over the devices to see basic configuration information about them. Second, click on each device with the Select tool to show the device configuration window, which provides several ways to configure the device. Third, use the Inspect tool to view tables the network device will build as it learns about the network around it. In this example, only the ARP tables will appear. Since the devices have not been configured yet, the ARP tables are empty. Always remember to close windows after viewing them or they will clutter the workspace.
5. Open the PC configuration window and change the settings using the Config tab. Change the display name to Client and set the DNS server to 192.168.0.105. Under Interface, click FastEthernet and set the IP address as 192.168.0.110. Packet Tracer automatically calculates other parameters. Make sure that the Port Status box is checked. For future reference, note that other Ethernet interface settings, such as bandwidth, duplex, MAC address, and subnet mask can be modified using this window.



6. Go to the Desktop Tab and click on IP Configuration. Notice that the IP address, subnet mask and DNS server can be changed here as well.
7. Open the Server configuration window and go to the Config tab. Change the display name to Web Server. Click FastEthernet and set the IP address as 192.168.0.105. Make sure that the Port Status is also on. Click DNS and set the domain name as www.firstlab.com. Set the IP address as 192.168.0.105 and click ***Add***. Finally, check to make sure that the service for DNS is on.
8. Reposition the network devices by dragging them to a new location. Add a network description by using the "i" button on the

upper right corner. Then add some text labels within the Logical Workspace by using the Place Note tool.

9. Load a background grid using the Set Tiled Background button.
10. Save your work using the File > Save As option and create a meaningful filename.

Discussion

1- Use network tools to check the network
2- Change the network information to your name and your location on Lab.
3- Change the IP addresses to suitable one for both client and server.
4- Change the name of Web server and open it from the desktop.
5- Check the button in 3, 7, 8, 10.