ଓଡ଼ିଶା ରାଜ୍ୟ ମୁକ୍ତ ବିଶ୍ୱବିଦ୍ୟାଳୟ, ସମ୍ବଲପୁର, ଓଡ଼ିଶା
Odisha State Open University, Sambalpur, Odisha
Established by an Act of Government of Odisha.

DIPLOMA IN CYBER SECURITY

(DCS)

SESSION: 2016-2017

DCS02: DATA COMMUNICATION AND NETWORKING

LAB MANUAL

EXPERIMENT-1

AIM: To study about different physical equipments used for networking.

1.0 Learning Objective:

At the end of the session you will be able to become familiar with different types of equipment's and cables used in the networked lab.

1.1 What is a Computer Network?

Computer network means an interconnected collection of autonomous computers. Two computes said to be connected if they are able to exchange information. The connection needs to be done via some transmission media such as a coaxial cable, twisted pair cable; fiber optics, microwares and communication satellite can also be used. To interconnect the devices in the network requires some networking devices such as a hub, a switch or a router etc. To be autonomous means a device to be able to start or stop of its own.

Benefits of Computer network:

- Resource Sharing
- High Reliability
- Saving Money

1.2 Network Components

1.2.1 Server

Concept of a server is based on one or more personal computers to perform specific tasks for a number of other PCs. The most common function is disk, file and print servers.

A **Disk Server** provides low-level support and performs basic read/write operation to disk sectors.

A **File Sever** is a higher-level support mechanism, performing such function as lockout and dynamic allocation of space on disk. In a star topology the server is the principal connection point. All nodes, including the server, are connected to a hub. This enables the server to house and administer software, fie sharing, file

saving and to allocate printers or other peripherals. In a bus topology, the server acts like arbitrator, each node talks to the server when requesting information. The server then locates the information on one of the connected clients and sends it to the requesting client. Servers in any network can be an ordinary node but having more capabilities of handling the data and having more speed.

1.2.2 Workstation

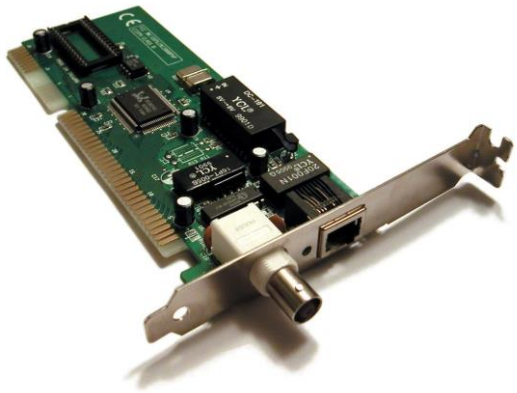
A node or stand-alone PC that is connected with network is called Workstation. A workstation is generally a Client.

NIC (Network Interface Card): The network Interface Card (NIC) is the interface between the PC and physical network connection. It is also called as Network Adapter Card. The NIC is responsible for the operation that tasks place in the physical layer of the OSI model. It is only concerned with sending and receiving) 0s and 1s, using the IEEE 802.3 Ethernet standard.

In windows, the NIC card is identified in the network property; to use protocol with NIC you must bind the protocol to the adapter card.

Function of NIC:

- Data Transfer
- Data Buffering
- Frame Construction
- Media Access Control
- Parallel/Serial Conversion
- Data Encoding/Decoding
- Data Transmission/Reception



1.2.3 Cables

To transmit the data the medium must exist, usually in the form of cables or wireless media. Here are some most commonly used cable types.

1.2.3.1 Thick Coaxial Cables (thick net) (RG-11)

Thick coaxial cables or thick wire is known as the Ethernet standard RG-11. This cable is mostly used as backbone cable, distributing Ethernet signal throughout a building, an office complex or other large installation. It is used in 10base5 Ethernet standard. The length may be up to 500 meters with a max of

five segments connected by repeaters. This gives a total distance of 2500 meters. This is called a network diameter. RG-11 cable is typically orange; with black rings around the cable every 2.5-meter to allow taps into the cable.

1.2.3.2 Thin coaxial cables (thin net) (RG-58)

RG-58 is typically used for wiring laboratories and offices, or another small group of computers. The maximum length of thin wire Ethernet segment is 185 meters, which is due to the nature of the CSMA/CD method of operation, the cable attenuation, and the speed at which signals propagate inside the coax.

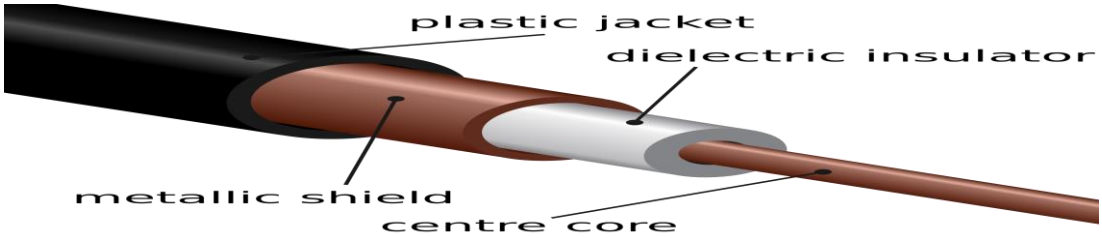


Fig: Thin coaxial cables (thin net) (RG-58)

The length is limited to guarantee that collision is detected when machines that are apart transmit at the same time. BNC connectors are used to terminate each end of the cable. When many machines are connected to the same Ethernet segment, a daisy chain approach is used. The BNC connectors allow the network interface card to the next machine. The machine each end of the cable must use a terminating resistor to eliminate collision-causing reflection in the cable.

1.2.3.3 Coaxial Cable Connectors

Coaxial connectors are needed to connect coaxial cable to devices. The most common type of connector used today is the Bayone-Neil-Concelman, in short, BNC connector.

Coaxial Cable Connector

The three popular types of connectors are: the BNC connector, the BNC T connector, and the BNC terminator. The BNC connector is used to connect the end of the cable to a device, such as a TV set. The BNC T connector is used in Ethernet networks to branch out to a connection to a computer or other device.

The BNC terminator is used at the end of the cable to prevent the reflection of the signal.

Applications

1. Coaxial cable was widely used in analog telephone networks, and later with digital telephone networks.
2. Cable TV networks use coaxial cables (RG-59) at the network boundaries. However, coaxial cable has largely been replaced today with fiber-optic cable due to its higher attenuation.
3. Traditional Ethernet LAN
   – 10Base-2, or thin Ethernet, uses RG-58 coax cable with BNC connectors.
   – 10Base-5, or thick Ethernet, uses RG-11 coax cable with specialized connectors.

1.2.3.4 Twisted pair cables

Twisted pair is probably the most widely used cabling system in Ethernet in networks. Two copper wires twist around each other to form the twisted pair cable. Depending on category several insulated wire strands can reside in the cable.

Twisted pair is available in two basic types

a) Unshielded Twisted Pair (UTP)

b) Shielded Twisted Pair (STP)

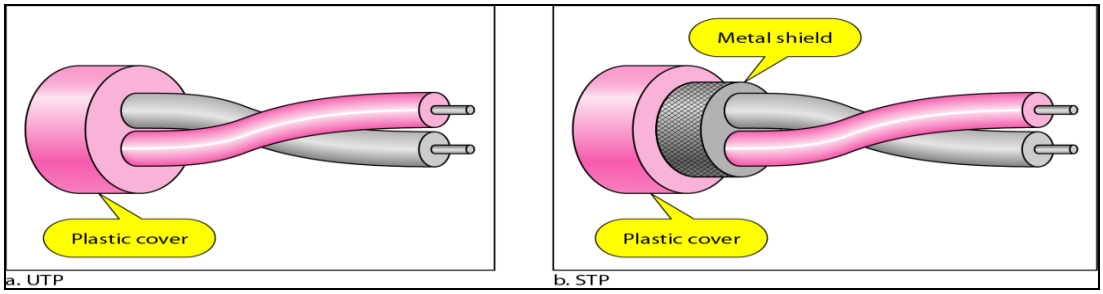


Fig: Twisted pair cables

Unshielded Twisted Pair

Mostly the UTP is used. A twisted pair segment can't exceed 100 meters. This limitation is the only drawback to twisted pair. Twisted pair is used for 10/100 based Ethernet networks. UTP cables are wired as straight through or crossover cables. Straight through cables typically connect the computer's networks interface can't to be a port on the hub. Crossover cables are used for NIC to

communication and for hub-to-hub connections when no crossover port is available.

Category	Descriptor
1	Used for voice for data.
2	Contains four twisted pair and a data transmission up to 4 Mbps. Used for some token ring network.
3	Contains four twisted pair and a data transmission up to 10 Mbps. Used for some token ring network.
4	Contains four twisted pair and a data transmission up to 16 Mbps. Used for some token ring network.
5	Contains four twisted pair and a data transmission up to 100 Mbps. Used for some token ring network.

Category-5 cables can be purchased or crimped as either straight through or crossed. A category-5 cable has 8 thin. Colours coded wires inside that run from one end of the cable to the other. Ethernet networks for communication use only wires 1, 2, 3 and to be connected in both jacks. Straight through cables are used for connecting to a hub. Crossed cables are used for connecting a hub to another hub (there is an exception: some hubs are a built in uplink port that is crossed internally, which allows you to uplink hubs with a straight cable instead.) In a straight through cable wires 1, 2, 3…. and 6 at the other end. In a crossed cable, one order of the wires change from one end to the other wire 1 becomes 3 and 2 becomes 6.

For PC 2 PC Communication without HUB (Cross Cable Connection)

Sl. No.	One Site	Second Site	Pin Configuration
01	Orange White	Green White	Transmit
02	Orange	Green	Transmit
03	Green White	Orange White	Receive
04	Blue	Blue	Not Use
05	Blue White	Blue White	Ground
06	Green	Green	Receive
07	Brown White	Brown White	DTR
08	Brown	Brown	DTS

For PC 2 PC Communication with HUB (Simple Cable Connection)

Sl. No.	One Site	Second Site	Pin Configuration
01	Orange White	Orange White	Transmit
02	Orange	Green	Transmit

03	Green White	Orange White	Receive
04	Blue	Blue	Not Use
05	Blue White	Blue White	Ground
06	Green	Green	Receive
07	Brown White	Brown White	DTR
08	Brown	Brown	DTS

For One Cable in Two PC Communication through HUB (Simple Cable Connection)

First Connection

Sl. No.	One Site	Second Site	Pin Configuration
01	Orange White	Green White	Transmit
02	Orange	Orange	Transmit
03	Green White	Green White	Receive
04	Green	Green	Receive

Second Connection:

Sl. No.	One Site	Second Site	Pin Configuration
01	Blue	Green White	Transmit
02	Blue White	Orange	Transmit
03	Brown White e	Green White	Receive
04	Brown	Green	Receive

Shielded Twisted Pair It is 150Ω cable containing additional shielding that protects signals against electromagnetic Interference (EMI) produced by electric motors power lines etc. It is primarily used in Token Ring Network & where UTP cable would provide insufficient protection against interface. Wires within cables are encased in a metallic sheath that is conductive as copper in wires. This sheath when properly grounded converts it ambient noise into current, like antenna. This current is carried to wires within where it creates an equal and opposite current flowing in twisted pair thus getting cancelled and no noise signal is resulted.

Unshielded Twisted-Pair Connector

The most common Unshielded Twisted-Pair connector is RJ45. RJ stands for registered jack.

Inside the Ethernet cable, there are 8 color coded wires, with all eight pins used as conductors. These wires are twisted into 4 pairs and each pair has a common

color theme. RJ45 specifies the physical male and female connectors as well as the pin assignments of the wires.

RJ45 uses 8P8C modular connector, which stands for 8 Position 8 Contact. It is a keyed connector which means that the connector can be inserted only in a single way. RJ45 is used almost exclusively to refer to Ethernet-type computer connectors.

Characteristics of twisted pair cable

1. Requires amplifiers every 5-6 km for analog signals
2. Requires repeaters every 2-3 km for digital signals
3. Attenuation is a strong function of frequency
4. Susceptible to interference and noise

Fig: Unshielded Twisted-Pair Connector

Applications

1. Used in telephone lines to provide voice and data channels.
2. The local loop –the line connecting the subscriber to the central telephone office- commonly consists of UTP cables.
3. DSL lines are also UTP cables.
4. LANs such as, 10Base-T and 100Base-T use UTP cables.

1.2.3.5 Fibre Optic.

Fibre Optic relies on pulsed as light to carry information. Two types of plastic or glass with different physical properties are used (the inner core and the outer cladding) to allow a beam of light to reflect off the boundary between the core and cladding. Some fibre optic cables allow many different paths other allow one single mode. They are called multimode and single mode fibres. A popular multimode fibre has core/cladding dimensions of 62.5/125 nanometres.

Fiber Optic cable connector

EXPERIMENT-2

Aim: To study different internetworking devices in a computer network.

1.0 Learning Objective: At the end of the session you will be able to be familiar with different types of internetworking devices and their functions.

1.1 REPEATER

A Repeater is a purely electrical device that extends maximum distance a LAN cable can span by Amplifying signals passing through it. A Repeater connects two segments and broadcasts packets between them. Since signal loss is a factor in the maximum length of a segment, a Repeater is used to amplify the signal and extend the usable length.

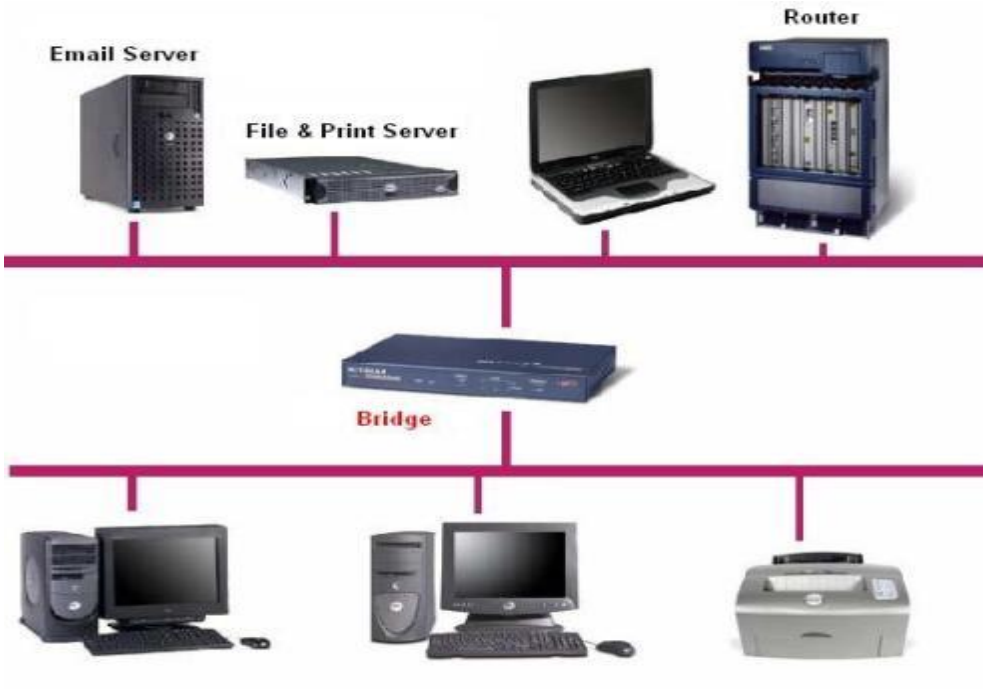
Repeaters

A common Ethernet rule is that no more than four repeaters may be used to join segments together. This is a physical limitation designed to keep collision detection working properly. Repeaters operate at layer 1 (Physical layer) of the OSI model.

1.2 BRIDGES

The networks bridge provides an inexpensive and easy way to connect network segments. A bridge provides Amplification function of a repeater plus, ability to select filter packets based on their addresses. When network grows in size, it is often necessary to partition it in to smaller group of nodes to help isolate traffic

and improve performance. One way to do this is to use bridge, the operation of it is to keep one segment traffic to that side and other side will cross the bridge. The bridge learns which packets should cross it as it is used.



Bridged network

1.3 ROUTERS

A router is a device that connects two LANs together to form an inter-network. A router is the basic building block of the Internet. Each router connects two or more networks together by providing an interface for an Ethernet network and ring network to which it is connected.

Routers

The router examines each packet of information to detection weather the packet must be translated form on one network to another network performing a function similar to a bridge. Unlike a ridge, a router can connect network that use

different technologies, addressing methods, media type, frame format and speeds. A router is a special purpose device designed to interconnect networks. Such that three networks can be connected using two routers. Routers maintain routing tables in their memories to store information about the physical connection on he network; the router examines each packet of data, checks the routing table and then forwards the packet if necessary. Every other router in the path (between any state destinations) performs a similar procedure. Note that a router does not maintain any state information about the packets; it simply moves them along the network. Routers are operated at layer 3(network) of OSI model.

1.4 GATEWAYS

A gateway is node in a network that serves as an entrance to another network. In enterprises, the gateway node often acts as a proxy server and a firewall. The gateway is also associated with both a switch, which provides the actual path for the packet in and out of the gateway. It is also known as a computer system located on earth that switches data signals and voice signals between satellites and terrestrial networks. A gateway can operate at any layer of the OSI or TCP/IP reference model. The hub of a gateway, also called a protocol converter, is much more complex than that of a router or switch. Typically a gateway must convert from one protocol stack to another. E.g. a gateway may connect a TCP/IP network to an IPX. /SPX network. A Circuit Level Gateway function provided by Application level gateway products enables trusted users on private network to access Internet services with all security of a proxy server. An Application Level Gateway provide much stricter form of security that packet filters, but they are designed to regulate access only for a particular application.

1.5 HUBS

Hubs are also called concentrators; expand one Ethernet connection into many. For example, a four-port hub connects up to four machines via UTP cables. The hub provides a star connection for the four ports. Many hubs contains a single BNC connectors as well to connect the hub to existing 10base2 network wiring, the hub can also be connected via one of its ports. One pot is desired to operate

in either straight through or crossover mode, selected by a switch on the hub. Hubs that can connect in this fashion are called stackable hubs. A hub is similar to a repeater, expect it broadcasts data received by any port to all other ports on the hub. Most hubs contain a small amount of intelligence as well. Examining received packets and checking them for integrity. If a bad packet arrives or the hub determines that a port is unreliable. It will shut down the line under the error condition is appears. The hub also acts like a repeater. Because of its slight delay when processing a packet, the numbers of hubs that may be connected in a series are limited.

There are three types of HUB passive hub, active hub and intelligent hub.

The Passive hubs do not process data signals with only purpose to combine the signal from several networks cables segments. All devices attached to the passive hub receive another packets that pass through the hub .Hub does not clear up or amplify the signals, on the contrary absorbs a small part of the signals that is why the distance between a hub and a computer should not be more than half of the permissible distance between two computers. Passive hubs have limited functionality so are inexpensive and easy to configure. It has four ports with four BNC (British Naval Connectors) female connectors to configure networks station or terminated with a 93 Ω BNC Terminator. The active hubs incorporate electronic components that amplify and cleanup the signals, that flaw between devices on the network. The process of cleaning up signal is called "signal regeneration". The benefits of signals regeneration are:

- A network is more robust i.e. less sensitive errors.
- Distance between devices can be increased.

Active hubs cost is considerable more than passive hub (active hub function impart as multi port repeaters). Intelligent hubs are enhanced active hubs the following functions add intelligence to a hub. Intelligent Hubs are units have form of integrated management capability.

Hub Management A hub supports networks network management protocols that enable the hub to send packets to central network console. Theses protocols enable network console to manage or control hub.

Switching hubs

Switching hubs include circuitry that quickly routes signals between ports on the hub. Insured of repeating a packet to all ports on the hub, it repeats a packet only to the port that connects to the destination computer for the packet.

1.6 SWITCHES

It is similar to a bridge, with some important enhancement. First, as witch may have multiple ports, thus directing packets to several different segments further partitioning and isolating network traffic in as way similar to router. For example, if 8-port n way switch is there it can route packets from any input to any output.

Some or all of incoming packet is called store and forward, which stores the received packet before examining it to for error before retransmitting. Bad packets are not forwarded. A switch typically has auto-sensing 10/100 mbps ports and will just the speed of each port accordingly; furthermore, a managed switch supports SNMP for further control over network traffic. Switches operated at layer 2 (Data Link) of OSI model.

EXPERIMENT-3

Aim: To study the working of Basic Networking Commands.

1.0 Learning objective:

At the end of the session you will be able to be familiar with working of different networking commands like: hostname, ifconfig, ping, host, telnet, ftp, net, arp, Winipcg, nslookup etc.

Networking Commands: The following commands are essentially used for network management.

1.1 **hostname**

This command is used for finding host/domain name and IP address.

Example:

hostname *with no options displays the machines host name*

hostname –d *displays the domain name the machine belongs to*

hostname –f *displays the fully qualified host and domain name*

hostname –i *displays the IP address for the current machine*

1.2 ifconfig

This command will display the assigned IP address of ETHERNET adapter.

Ubuntu : ifconfig | grep inet

Windows : ipconfig

1.3 ping

This command is used for checking the network connectivity.

Ping verifies IP-level connectivity to another TCP/IP device by sending Internet Control Message Protocol (ICMP) Echo Request messages. If received, the corresponding Echo Reply messages are displayed, along with round-trip times. Otherwise, a timed-out request or an ICMP unreachable message is displayed.

(i.e. You can "ping" an IP address to see if a machine is alive. If there is no response, you know something is wrong)

1.4 host

This command is used for mapping name to IP addresses?

Example: host www.google.com

www.google.com has address 74.125.200.147

www.google.com has address 74.125.200.106

www.google.com has address 74.125.200.103

www.google.com has address 74.125.200.104

www.google.com has address 74.125.200.105

www.google.com has address 74.125.200.99

www.google.com has IPv6 address 2404:6800:4003:c00:: 69

1.5 telnet

This command is used for connecting to a host on a particular port.

Example: telnet osou.ac.in 80

telnet command is also used to make a connection to a remote machine and execute programs as if one were physically present.

telnet (data are travelled without encryption; not secured)

1.6 ftp

This command allows you to send and receive files between two computers.

1.7 net

net command is used for checking/starting/stopping networking services, users, messaging, configuration and so on... ?

1.8 arp

This command is used for displaying or manipulating the ARP (Address Resolution Protocol) information on a network device or computer.

Explanation: The ARP protocol maps Layer 3 IP addresses to Layer 2 MAC addresses. If a packet must move across networks, the Layer 2 MAC address changes with each hop across a router, but the Layer 3 address never changes. ARP cache stores ARP address mappings. If the entry was learned dynamically, it will eventually be deleted from cache. If the entry was manually inserted in ARP cache, it is a static entry and will remain until the computer is turned off or the ARP cache is manually flushed.

On Windows, ***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.

1.9 Winipcg

This command is used to know the IP configuration of the PC in a graphical form. It shows the following in the windows command prompt.

- IP Address
- Subnet Mask
- Type of H/W used for communication & it’s address

1.10 nslookup

This command displays information from Domain Name System (DNS) name servers.

NOTE: If you write the command as above it shows as default your pc's server name firstly.

1.11 netstat

This command is used for finding connection to and from the host?

Example:

netstat nap| grep port *will display process id of application which is using that port*

netstat a or netstat –all *will display all connections including TCP and UDP*

netstat tcp or netstat –t *will display only TCP connection*

netstat udp or netstat –u *will display only UDP connection*

netstat g *will display all multicast network subscribed by this host.*

EXPERIMENT-4

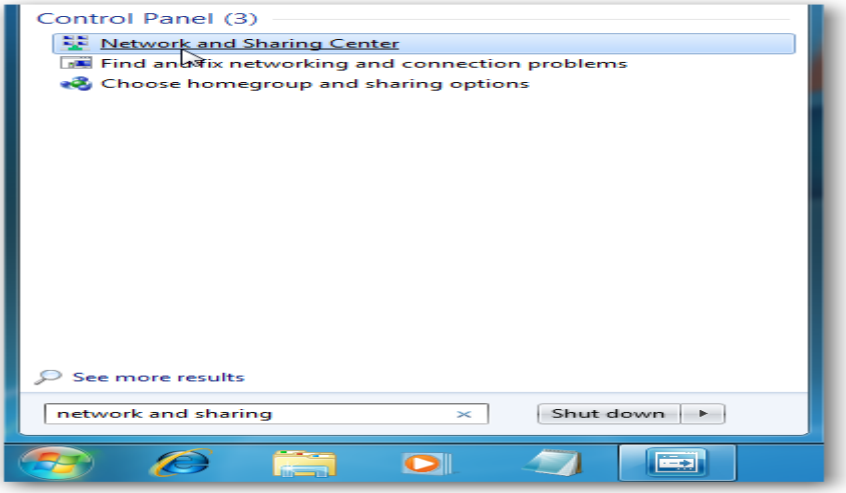
Aim: To assign IP address to the PC connected to the internet.

1.0 Learning Objective: At the end of the session you will be able to know how to assign IP address to a PC connected to the Internet.

1.1 Assigning IP address in Windows 7 or Windows 10

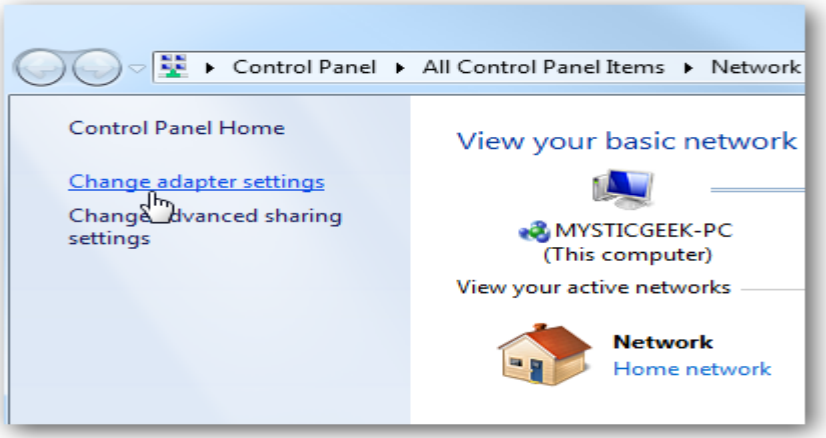
Step-1

To assign or change the computer's IP address in Windows, type *network and sharing* into the Search box in the Start Menu and select Network and Sharing Center when it comes up. If you're in Windows 7 or 10 it'll be in the start menu.



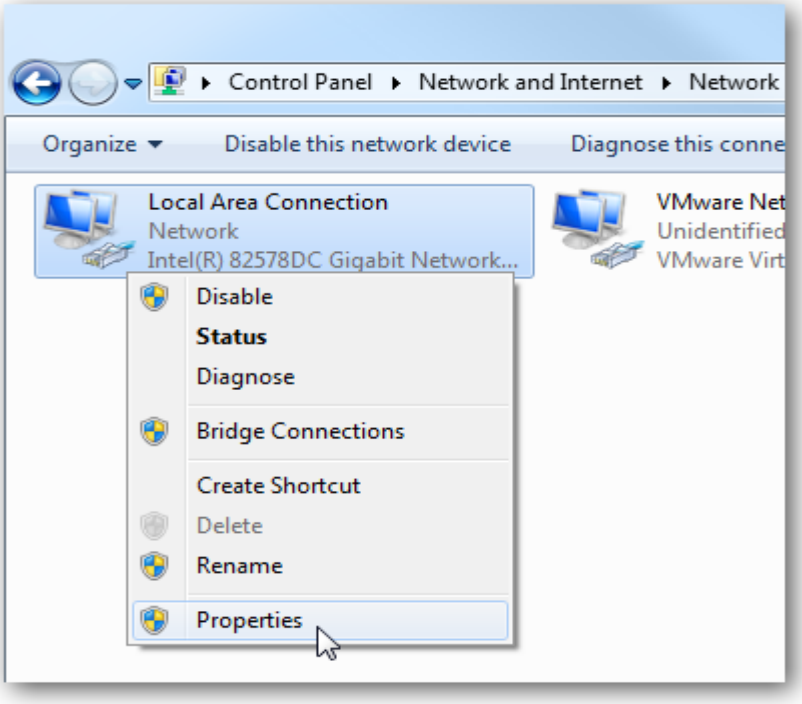
Step-2

Then when the Network and Sharing Center opens, click on *Change adapter settings*. This will be the same on Windows 7 or 10.



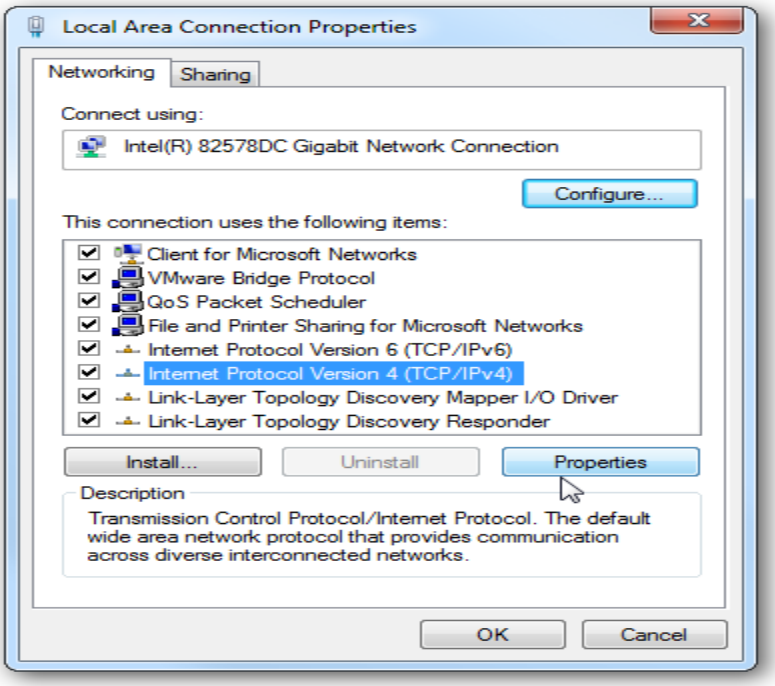
Step-3

Right-click on your local adapter and select Properties.



Step-4

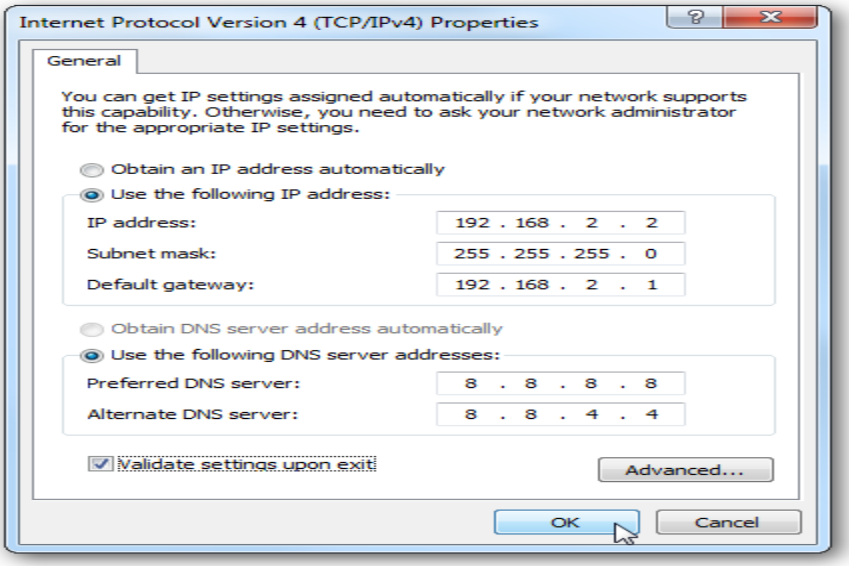
In the Local Area Connection Properties window highlight *Internet Protocol Version 4 (TCP/IPv4)* then click the Properties button.



Now select the radio button *Use the following IP address* and enter in the correct IP, Subnet mask, and Default gateway that corresponds with your network setup. Then enter your Preferred and Alternate DNS server addresses. Here we're on a home network and using a simple Class C network configuration and Google DNS.

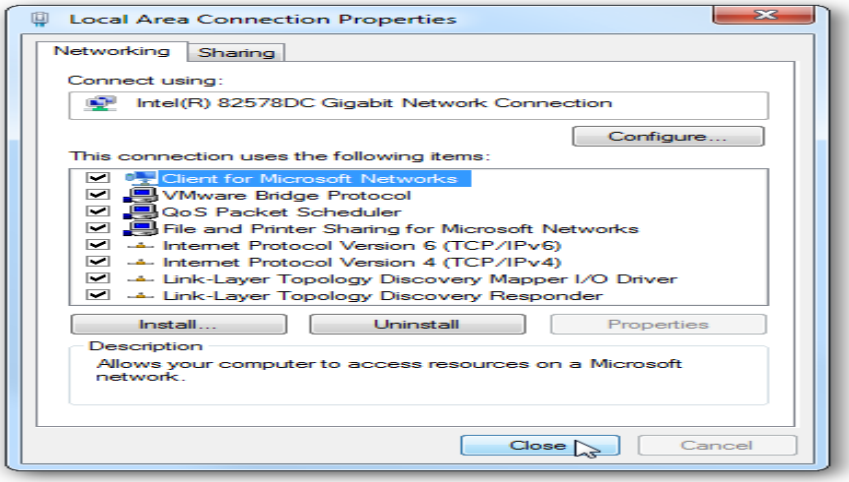
Step-5

Check *Validate settings upon exit* so Windows can find any problems with the addresses you entered. When you're finished click OK.

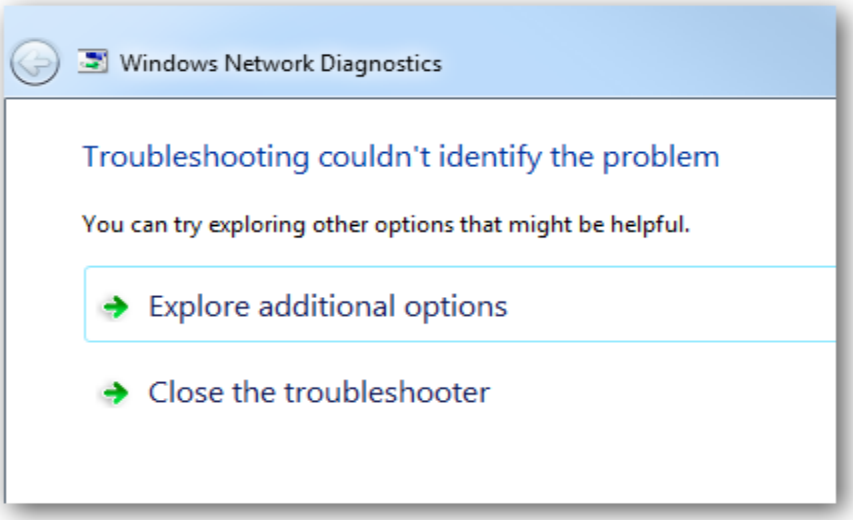


Step-6

Now close out of the Local Area Connections Properties window.

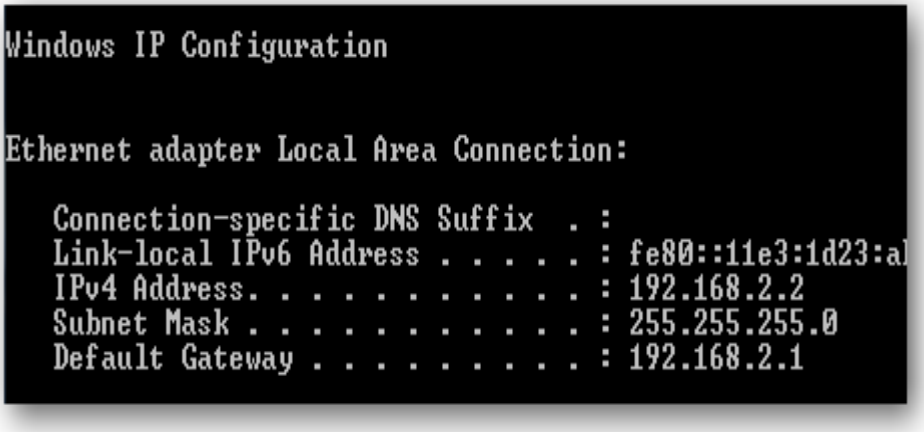


Windows will run network diagnostics and verify the connection is good. Here we had no problems with it, but if you did, you could run the network troubleshooting wizard.



Step-7

Now you can open the command prompt and do an *ipconfig* to see the network adapter settings have been successfully changed.



EXPERIMENT-5

AIM: To connect the computers in Local Area Network

1.0 Learning Objective: At the end of the session you should be able to learn how to connect your PC to a Local Area Network.

1.1 PROCEDURE ON THE HOST COMPUTER

On the host computer, follow these steps to share the Internet connection:

1. Log on to the host computer as Administrator or as Owner.
2. Click **Start**, and then click **Control Panel**.
3. Click **Network and Internet Connections**.
4. Click **Network Connections**.
5. Right-click the connection that you use to connect to the Internet. For example, if you

Connect to the Internet by using a modem, right-click the connection that you want under Dial-up / other network available.

6. Click **Properties**.
7. Click the **Advanced** tab.
8. Under **Internet Connection Sharing**, select the **Allow other network users to connect through this computer's Internet connection** check box.
9. If you are sharing a dial-up Internet connection, select the **Establish a dial-up connection whenever a computer on my network attempts to access the Internet** check box if you want to permit your computer to automatically connect to the Internet.
10. Click **OK**. You receive the following message:

When Internet Connection Sharing is enabled, your LAN adapter will be set to use IP address 192.168.0.1.

Your computer may lose connectivity with other computers on your network. If these other computers have static IP addresses, it is a good idea to set them to obtain their IP addresses automatically. Are you sure you want to enable Internet Connection Sharing?

11. Click **Yes**.

The connection to the Internet is shared to other computers on the local area network (LAN). The Network adapter that is connected to the LAN is configured with a static IP address of 192.168.0.1 and a subnet mask of 255.255.255.0

1.2 PROCEDURE ON THE CLIENT COMPUTER

To connect to the Internet by using the shared connection, you must confirm the LAN adapter IP configuration, and then configure the client computer.

To confirm the LAN adapter IP Configuration, follow these steps:

1. Log on to the client computer as Administrator or as Owner.
2. Click **Start**, and then click **Control Panel**.
3. Click **Network and Internet Connections**.
4. Click **Network Connections**.
5. Right-click **Local Area Connection** and then click **Properties**.
6. Click the **General** tab, click **Internet Protocol (TCP/IP)** in the **connection uses the Following items** list, and then click **Properties**.
7. In the **Internet Protocol (TCP/IP) Properties** dialog box, click **Obtain an IP address automatically** (if it is not already selected), and then click **OK**.

Note: You can also assign a unique static IP address in the range of 192.168.0.2 to 192.168.0.254.

For example, you can assign the following static IP address, subnet mask, and default gateway:

8. IP Address 192.168.31.202
9. Subnet mask 255.255.255.0
10. Default gateway 192.168.31.1
11. In the **Local Area Connection Properties** dialog box, click **OK**.
12. Quit Control Panel.

EXPERIMENT-6

Aim: Creating a Network topology using CISCO packet tracer software.

Learning Objective:

At the end of this session you should be able know how to create a network topology using CISCO packet tracer software.

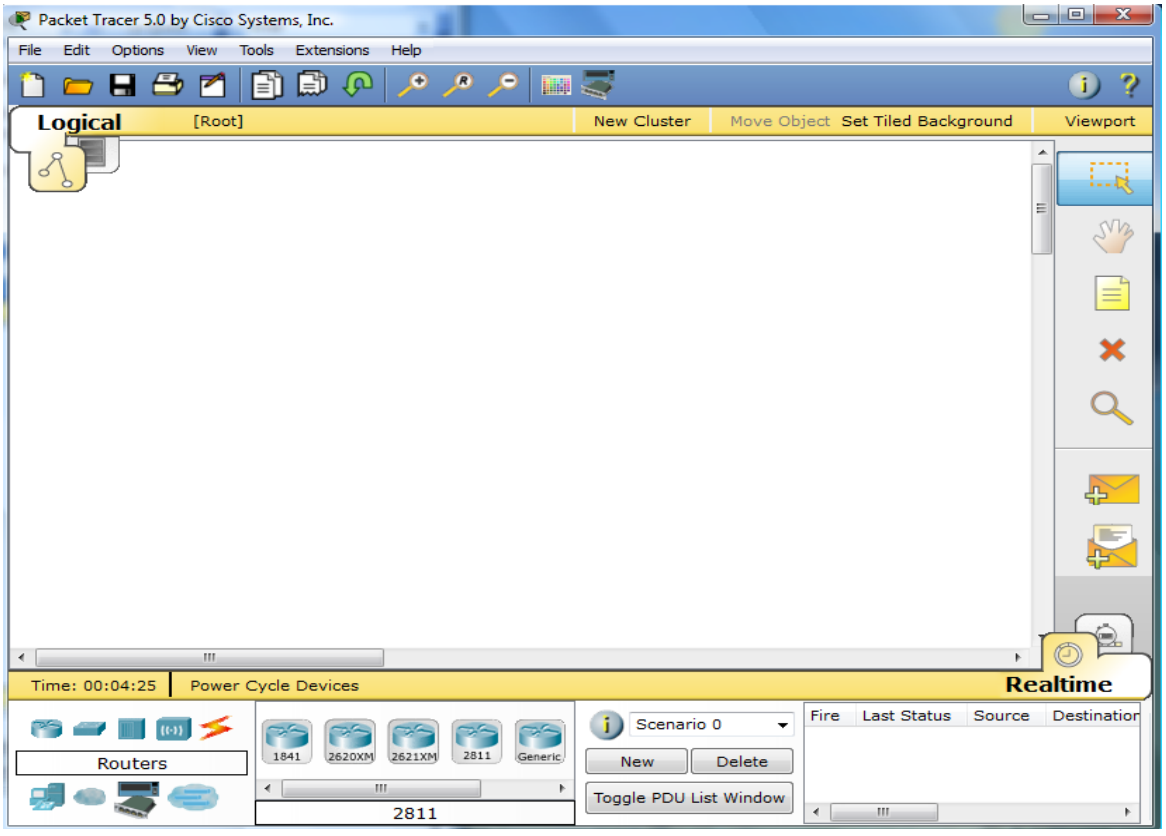
Apparatus ((Software): Packet tracer Software (Open Source)

Version: This lab is based on Packet Tracer 5.0.

Packet Tracer – Creating a New Topology

What is Packet Tracer? Packet Tracer is a protocol simulator developed by Dennis Frezzo and his team at Cisco Systems. Packet Tracer (PT) is a powerful and dynamic tool that displays the various protocols used in networking, in either Real Time or Simulation mode. This includes layer 2 protocols such as Ethernet and PPP, layer 3 protocols such as IP, ICMP, and ARP, and layer 4 protocols such as TCP and UDP. Routing protocols can also be traced.

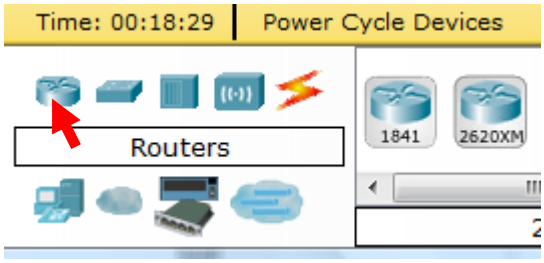
Step 1: Start Packet Tracer

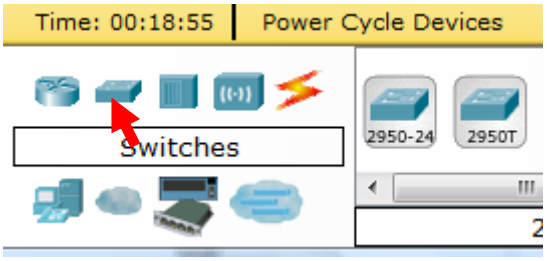


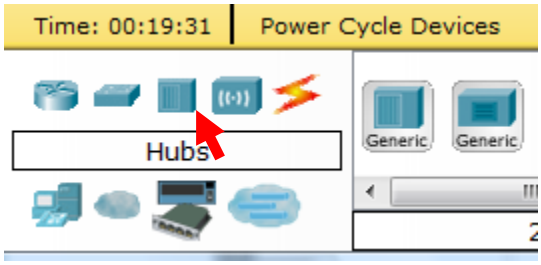
Step 2: Choosing Devices and Connections

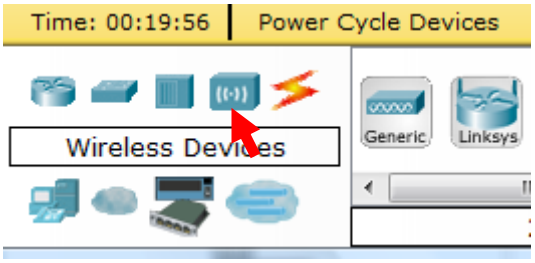
We will begin building our network topology by selecting devices and the media in which to connect them. Several types of devices and network connections can be used. For this lab we will keep it simple by using **End Devices**, **Switches**, **Hubs**, and **Connections**.

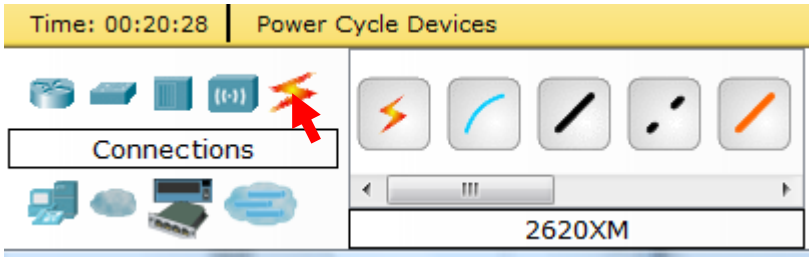
Single click on each group of devices and connections to display the various choices. The devices you see may differ slightly.

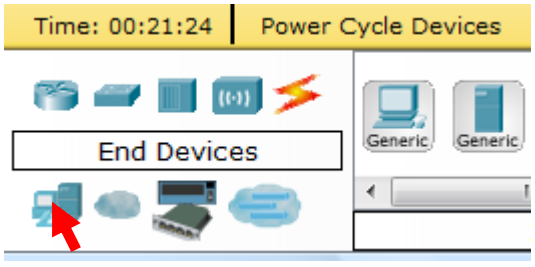


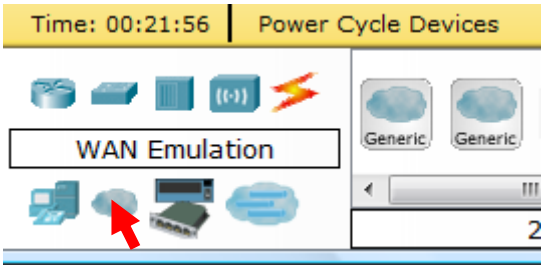


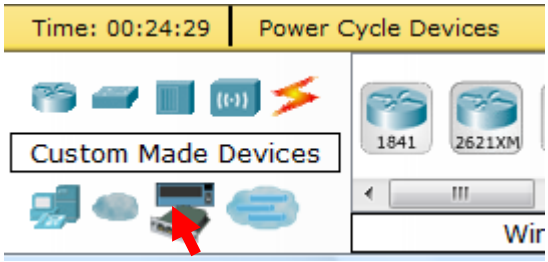


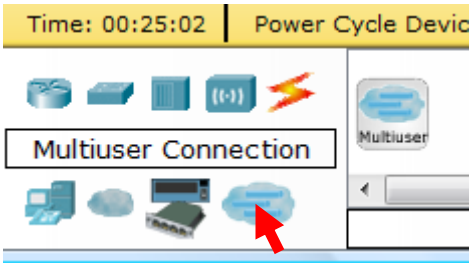






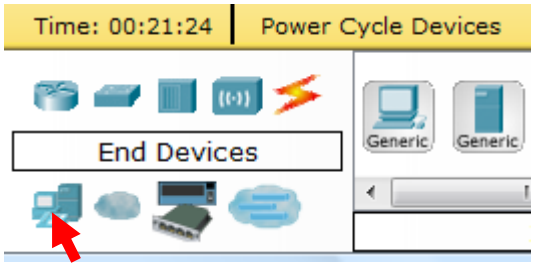




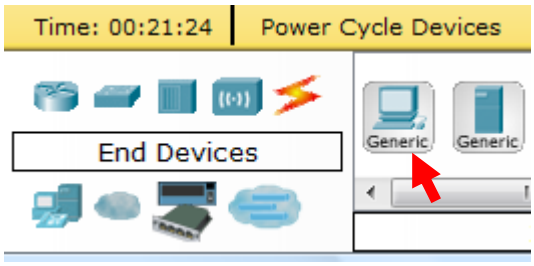


Step 3: Building the Topology – Adding Hosts

Single click on the **End Devices**.



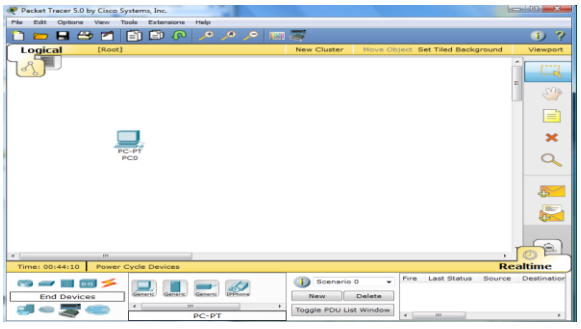
Single click on the **Generic** host.



Move the cursor into topology area. You will notice it turns into a plus "+" sign.

+

Single click in the topology area and it copies the device.

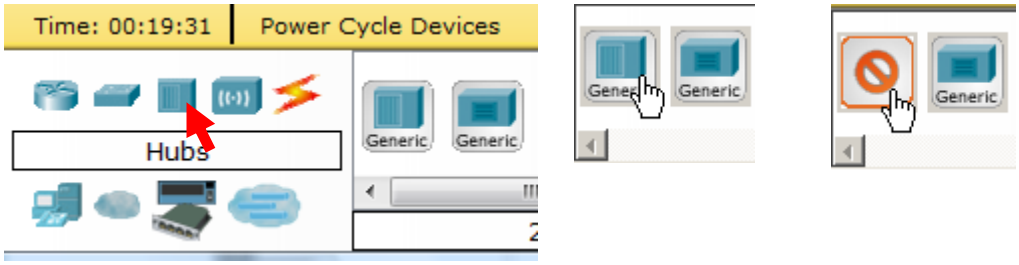


Add three more hosts.

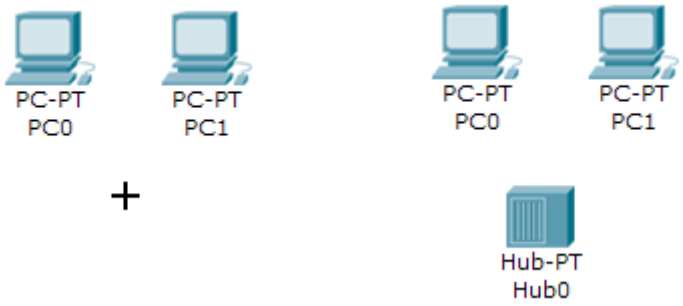
Step 4: Building the Topology – Connecting the Hosts to Hubs and Switches

Adding a Hub

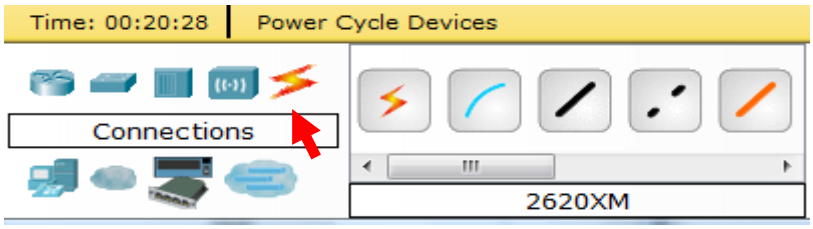
Select a hub, by clicking once on **Hubs** and once on a **Generic** hub.



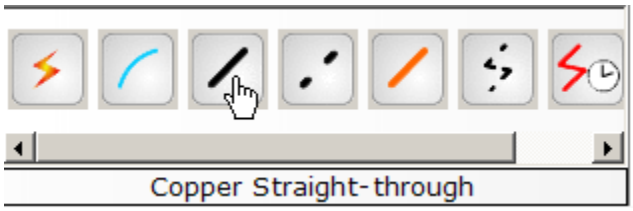
Add the hub by moving the plus sign "+" below PC0 and PC1 and click once.



Connect PC0 to Hub0 by first choosing **Connections.**



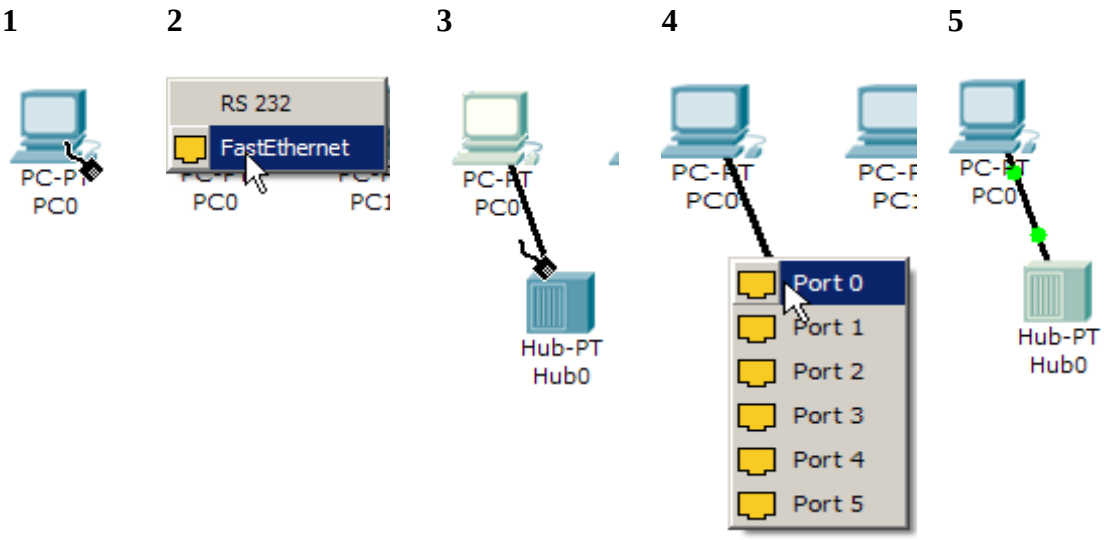
Click once on the **Copper Straight-through** cable.



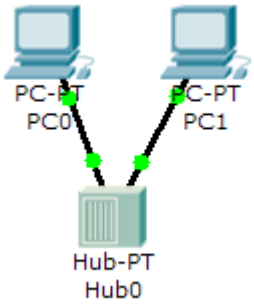
Perform the following steps to connect **PC0** to **Hub0**:

1. Click once on **PC0**
2. Choose **FastEthernet**
3. Drag the cursor to **Hub0**
4. Click once on **Hub0** and choose **Port 0**

5. Notice the green link lights on both the **PC0** Ethernet NIC and the **Hub0** Port 0 showing that the link is active.

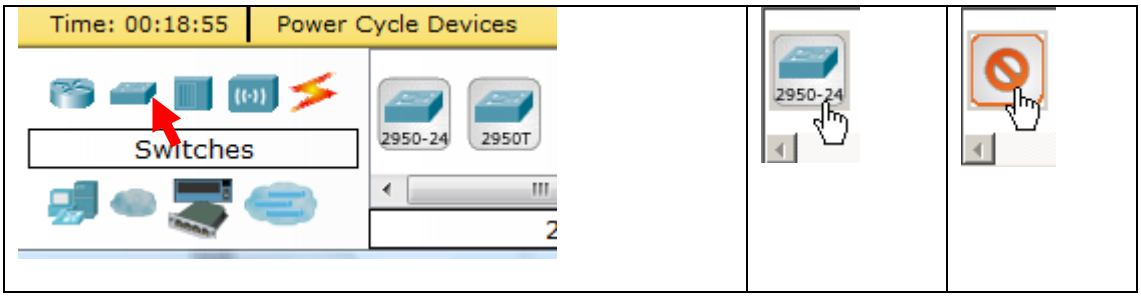


Repeat the steps above for **PC1** connecting it to **Port 1** on **Hub0**. (The actual hub port you choose does not matter.)

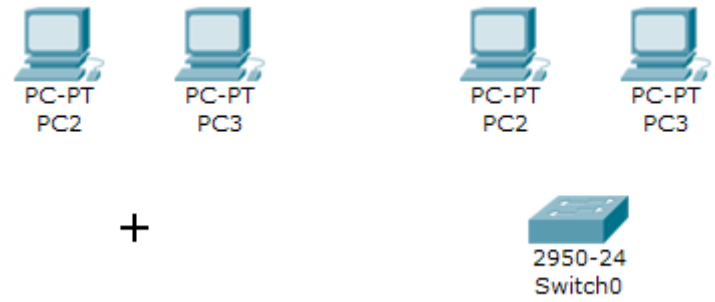


Adding a Switch

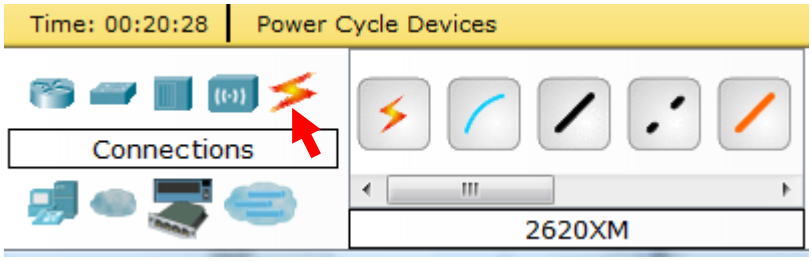
Select a switch, by clicking once on **Switches** and once on a **2950-24** switch.



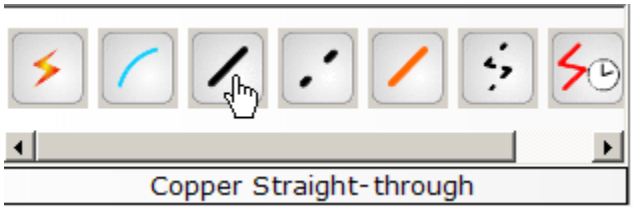
Add the switch by moving the plus sign "+" below PC2 and PC3 and click once.



Connect PC2 to Hub0 by first choosing **Connections.**



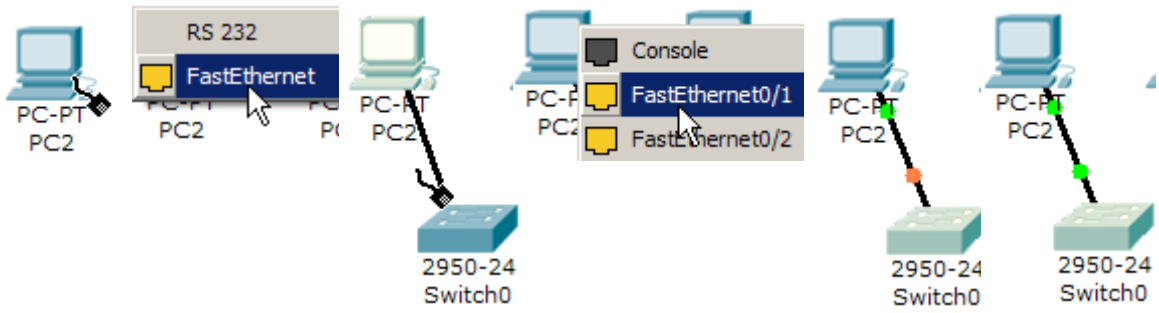
Click once on the **Copper Straight-through** cable.



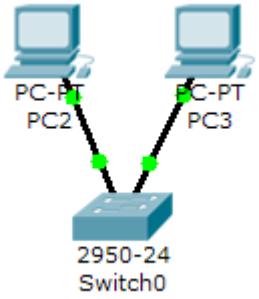
Perform the following steps to connect **PC2** to **Switch0**:

1. Click once on **PC2**
2. Choose **Fast Ethernet**
3. Drag the cursor to **Switch0**
4. Click once on **Switch0** and choose **FastEthernet0/1**
5. Notice the green link lights on **PC2** Ethernet NIC and amber light **Switch0 FastEthernet0/1 port**. The switch port is temporarily not forwarding frames, while it goes through the stages for the Spanning Tree Protocol (STP) process.
6. After a about 30 seconds the amber light will change to green indicating that the port has entered the forwarding stage. Frames can now forwarded out the switch port.

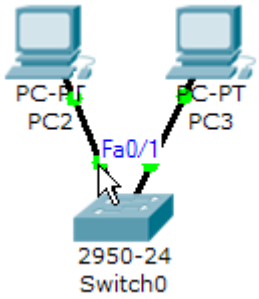
1 2 3 4 5 6



Repeat the steps above for **PC3** connecting it to **Port 3** on **Switch0** on port **FastEtherent0/2**. (The actual switch port you choose does not matter.)



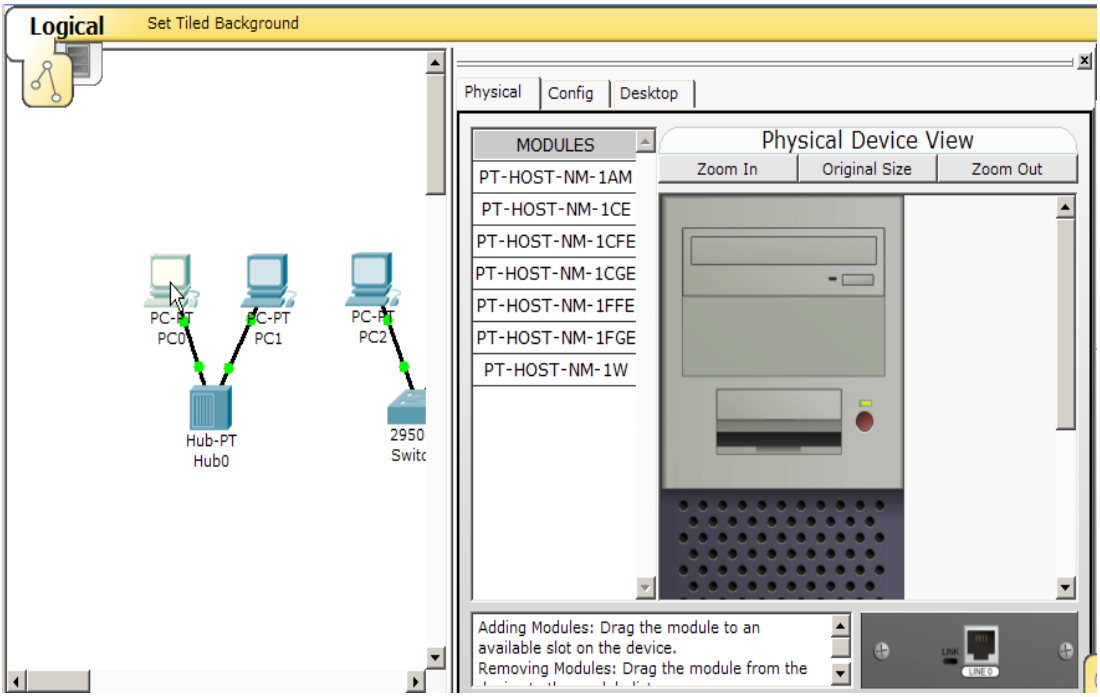
Move the cursor over the link light to view the port number. **Fa** means FastEthernet, 100 Mbps Ethernet.



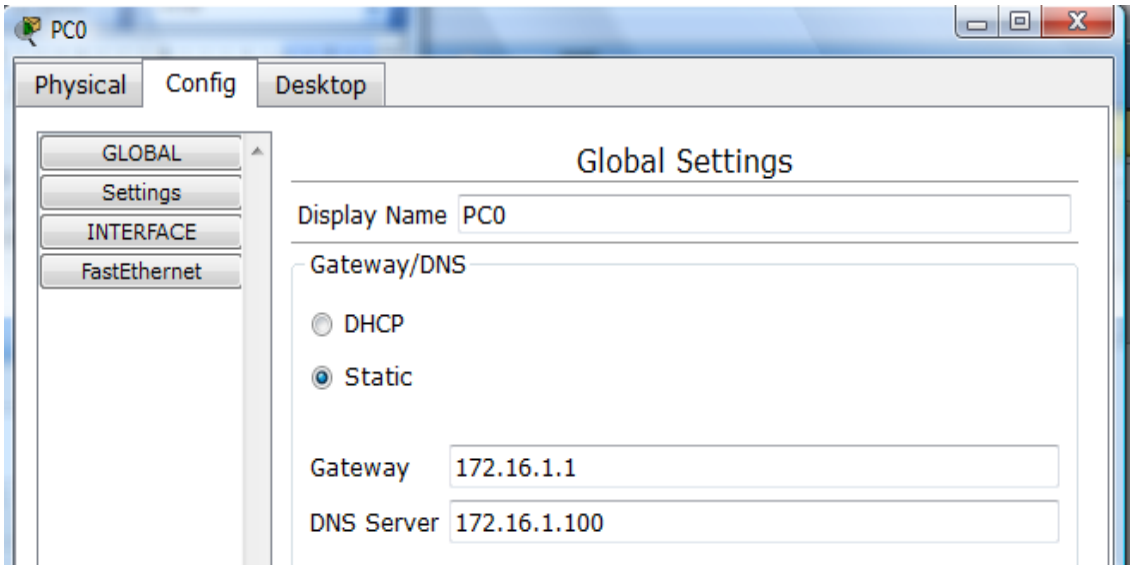
Step 5: Configuring IP Addresses and Subnet Masks on the Hosts

Before we can communicate between the hosts we need to configure IP Addresses and Subnet Masks on the devices.

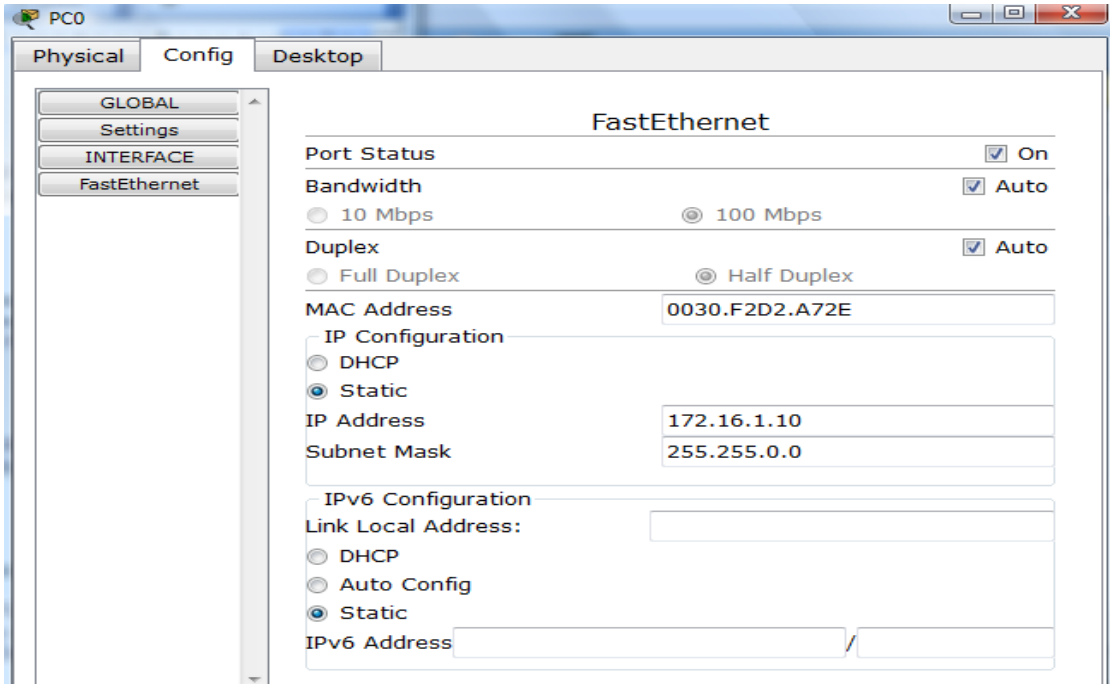
Click once on PC0.



Choose the **Config** tab and click on **Settings**. It is here that you can change the name of PC0. It is also here where you would enter a **Gateway** IP Address, also known as the default gateway and the **DNS Server** IP Address. We will discuss this later, but this would be the IP address of the local router. If you want, you can enter the Gateway IP Address 172.16.1.1 and DNS Server IP Address 172.16.1.100, although it will not be used in this lab.



Click on **Interface** and then **Fast Ethernet**. Although we have not yet discussed IP Addresses, add the IP Address to 172.16.1.10. Click once in the Subnet Mask field to enter the default Subnet Mask. You can leave this at 255.255.0.0. We will discuss this later.



Also, notice this is where you can change the Bandwidth (speed) and Duplex of the Ethernet NIC (Network Interface Card). The default is Auto (auto negotiation), which means the NIC will negotiate with the hub or switch. The bandwidth and/or duplex can be manually set by removing the check from the **Auto** box and choosing the specific option.

Bandwidth - Auto

If the host is connected to a hub or switch port which can do 100 Mbps, then the Ethernet NIC on the host will choose 100 Mbps (Fast Ethernet). Otherwise, if the hub or switch port can only do 10 Mbps, then the Ethernet NIC on the host will choose 10 Mbps (Ethernet).

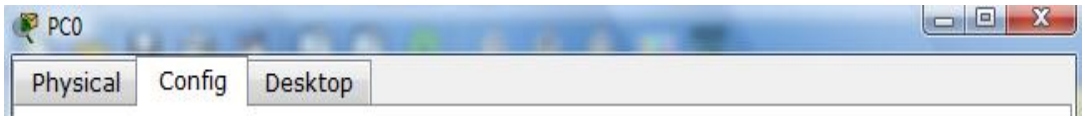
Duplex - Auto

Hub: If the host is connected to a hub, then the Ethernet NIC on the host will choose Half Duplex.

Switch: If the host is connected to a switch, and the switch port is configured as Full Duplex (or Auto negotiation), then the Ethernet NIC on the host will choose Full Duplex. If the switch port is configured as Half Duplex, then the Ethernet NIC on the host will choose Half Duplex. (Full Duplex is a much more efficient option.)

The information is automatically saved when entered.

To close this dialog box, click the "**X**" in the upper right.

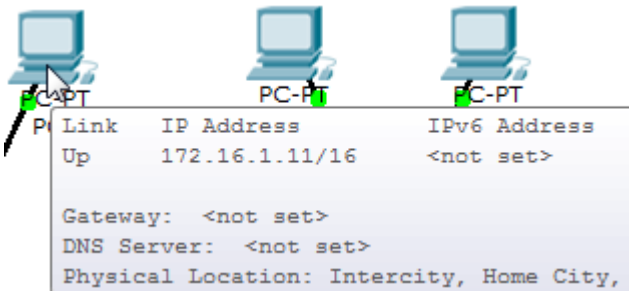


Repeat these steps for the other hosts. Use the information below for IP Addresses and Subnet Masks.

Host	IP Address	Subnet Mask
PC0	172.16.1.10	255.255.0.0
PC1	172.16.1.11	255.255.0.0
PC2	172.16.1.12	255.255.0.0
PC3	172.16.1.13	255.255.0.0

Verify the information

To verify the information that you entered, move the Select tool (arrow) over each host.

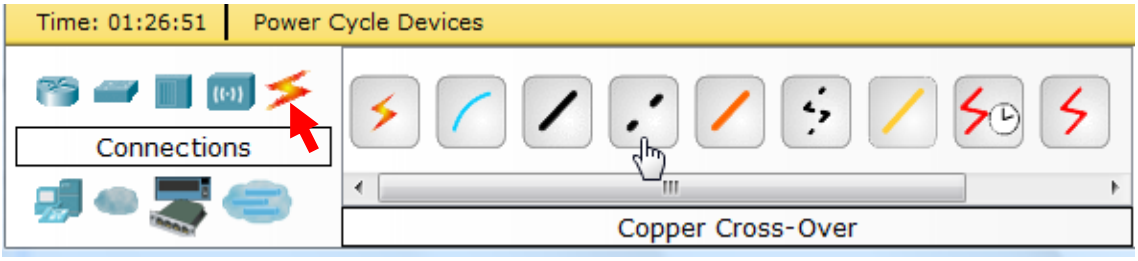


Deleting a Device or Link

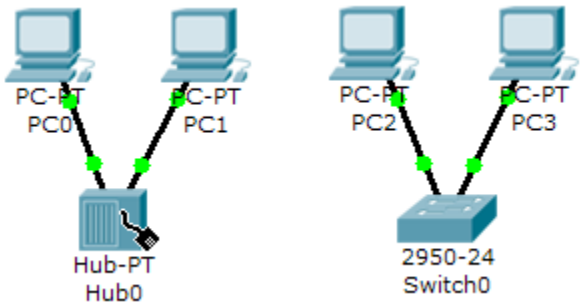
To delete a device or link, choose the **Delete** tool and click on the item you wish to delete.

Step 6: Connecting Hub0 to Switch0

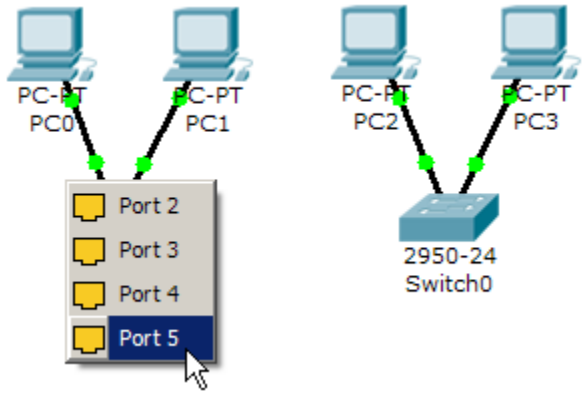
To connect like-devices, like a Hub and a Switch, we will use a Cross-over cable. Click once the **Cross-over** Cable from the **Connections** options.



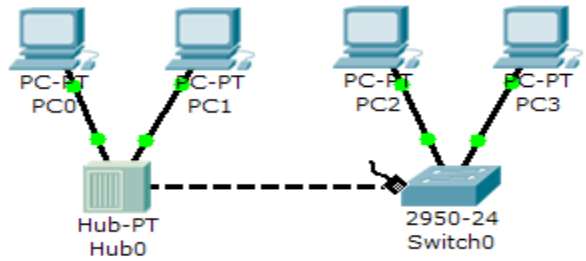
Move the Connections cursor over **Hub0** and click once.



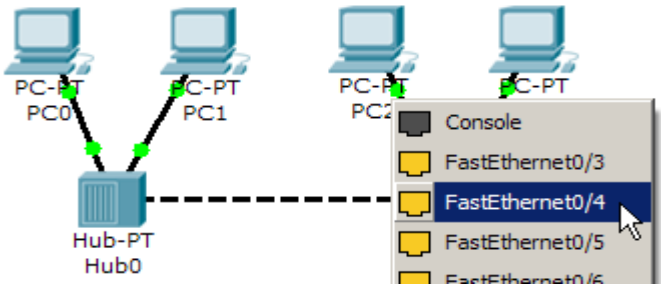
Select **Port 5** (actual port does not matter).



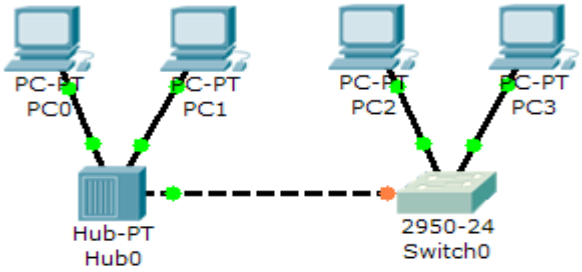
Move the Connections cursor to **Switch0**.

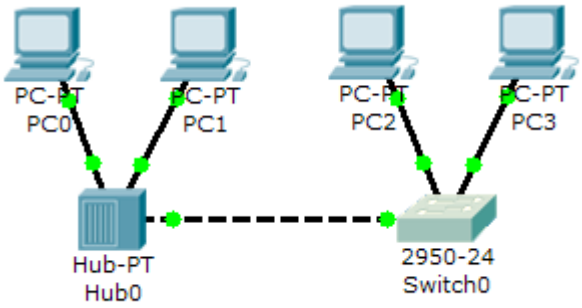


Click once on **Switch0** and choose **FastEthernet0/4** (actual port does not matter).



The link light for switch port **FastEthernet0/4** will begin as amber and eventually change to green as the Spanning Tree Protocol transitions the port to forwarding.



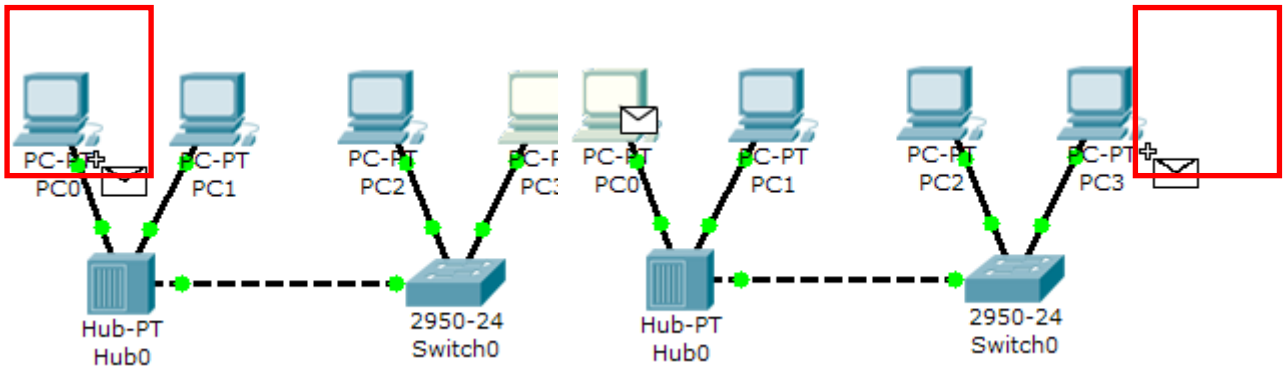


Step 7: Verifying Connectivity in Real-time Mode

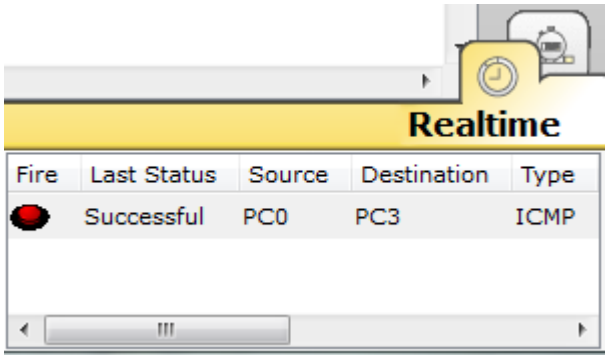
Be sure you are in **Real-time** mode.

Select the **Add Simple PDU** tool used to ping devices.

Click once on PC0, then once on PC3.



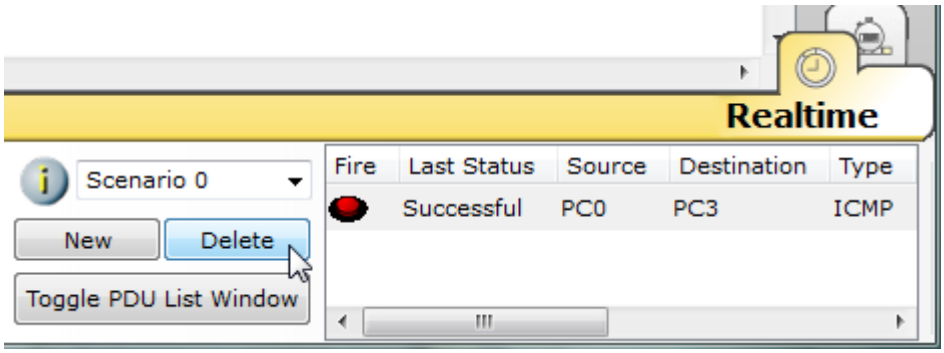
The PDU **Last Status** should show as **Successful**.



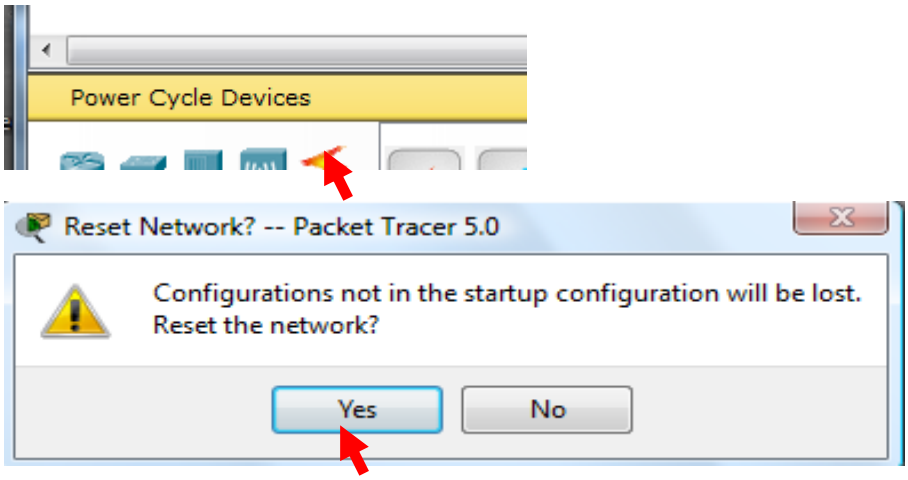
Retting the Network

At this point we will want to reset the network, whenever you want to reset the network and begin the simulation again, perform the following tasks:

Click **Delete** in the PDU area.

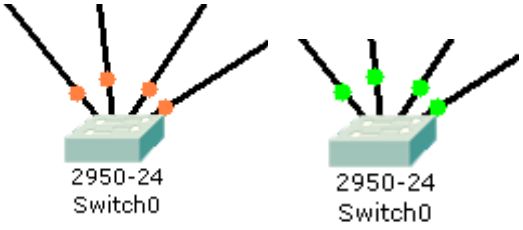


Now, Power Cycle Devices and confirm the action.



Waiting for Spanning Tree Protocol (STP)

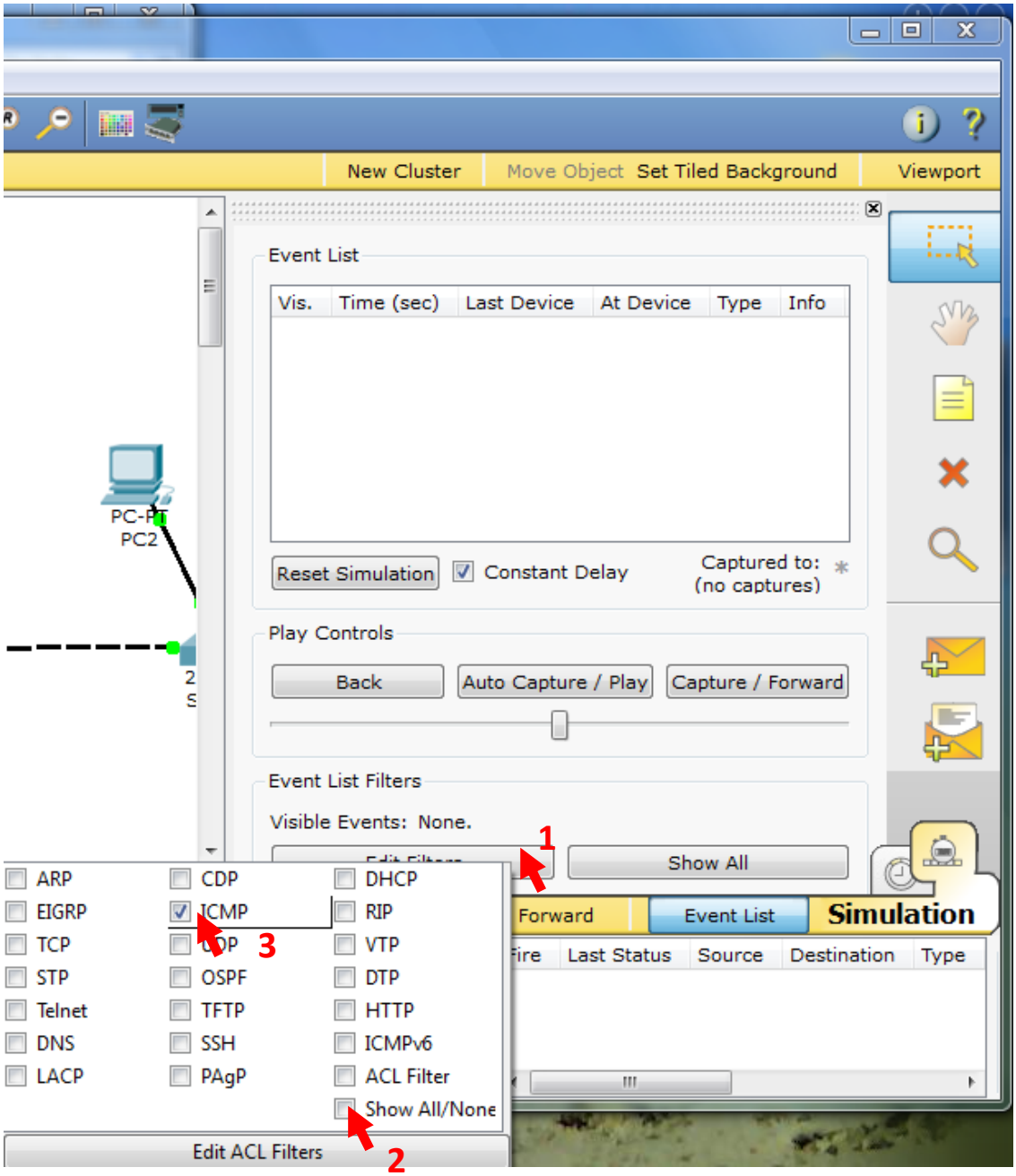
Note: Because Packet Tracer also simulates the Spanning Tree Protocol (later), at times the switch may show amber lights on its interfaces. You will need to wait for the lights to turn green on the switches before they will forward any Ethernet frames.



Step 8: Verifying Connectivity in Simulation Mode

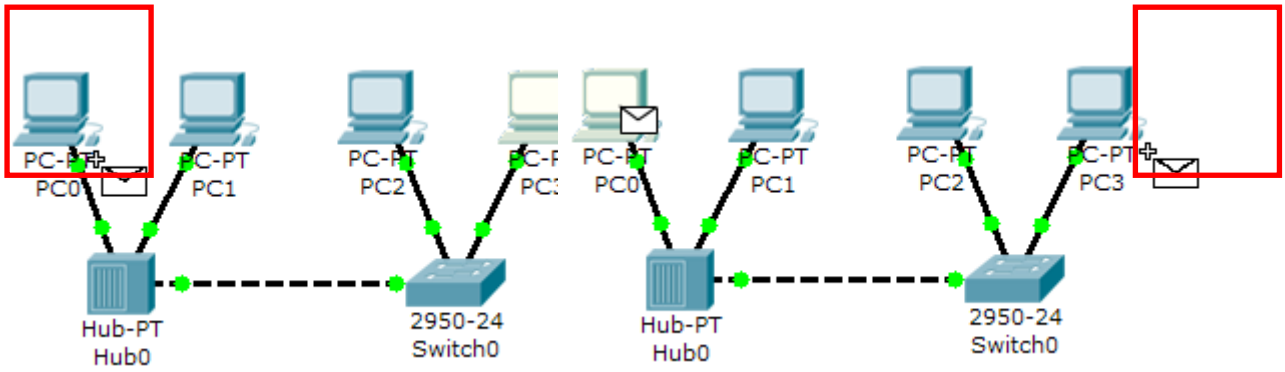
Be sure you are in **Simulation** mode.

Deselect all filters (All/None) and select only **ICMP**.

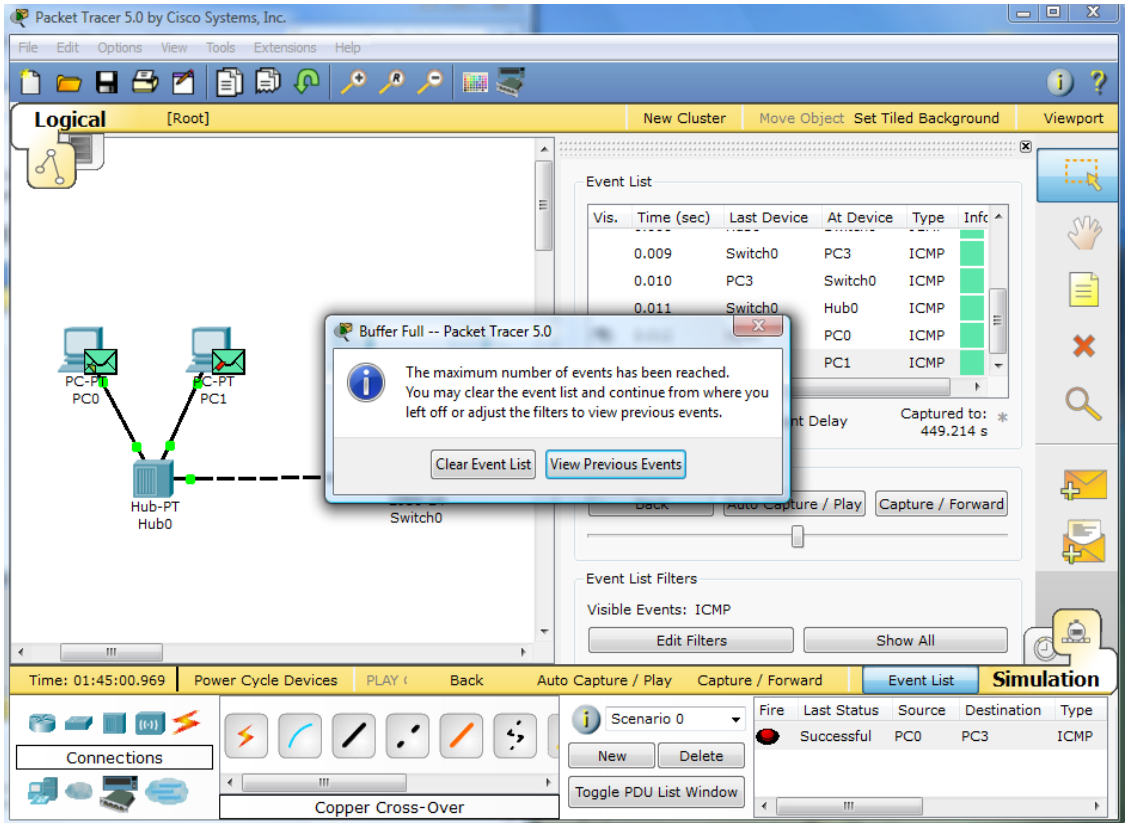

New Cluster
Move Object
Set Tiled Background
Viewport
Event List
Vis.
Time (sec)
Last Device
At Device
Type
Info
Reset Simulation
Constant Delay
Captured to:
(no captures)
Play Controls
Back
Auto Capture / Play
Capture / Forward
Event List Filters
Visible Events: None.
Show All
Forward
Event List
Simulation
Last Status
Source
Destination
Type
PC-PT
PC2
ARP
CDP
DHCP
EIGRP
ICMP
RIP
TCP
UDP
VTP
STP
OSPF
DTP
Telnet
TFTP
HTTP
DNS
SSH
ICMPv6
LACP
PAgP
ACL Filter
Show All/None
Edit ACL Filters
1
2
3

Select the **Add Simple PDU** tool used to ping devices..

Click once on PC0, then once on PC3.

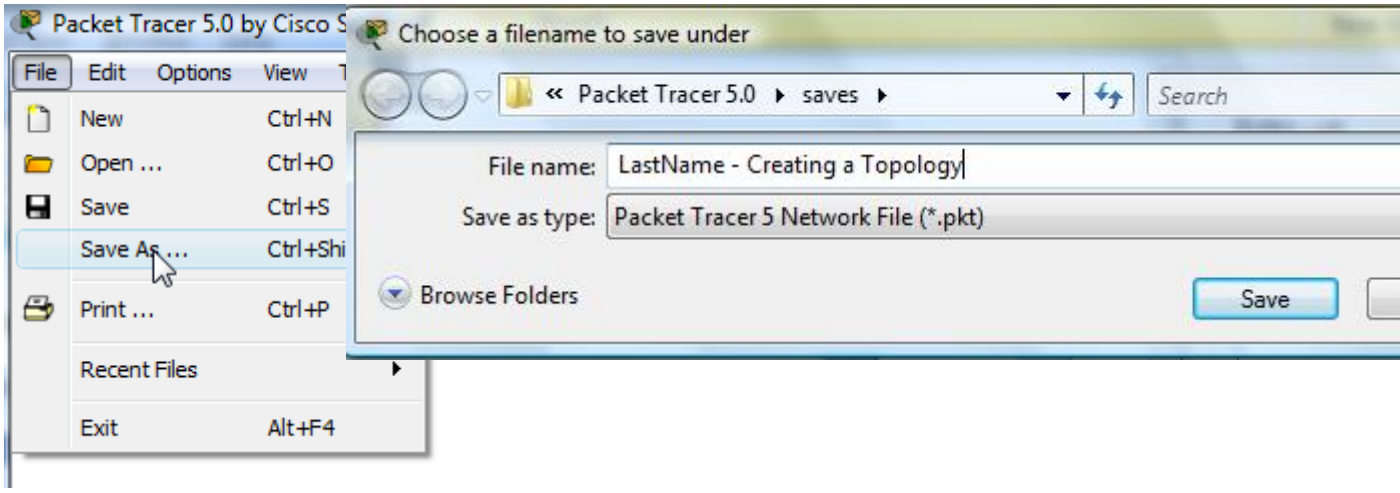


Continue clicking **Capture/Forward** button until the ICMP ping is completed. You should see the ICMP messages move between the hosts, hub and switch. The PDU **Last Status** should show as **Successful**. Click on **Clear Event List** if you do not want to look at the events or click **Preview Previous Events** if you do. For this exercise it does not matter.

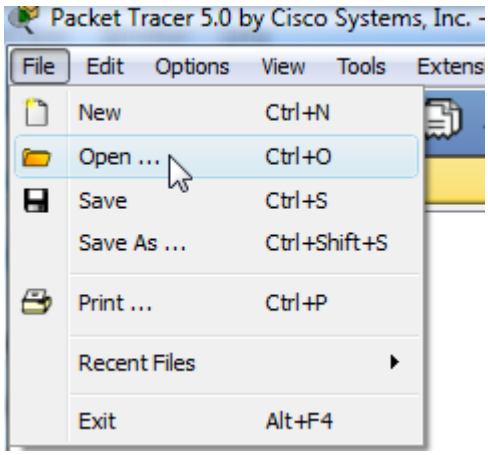


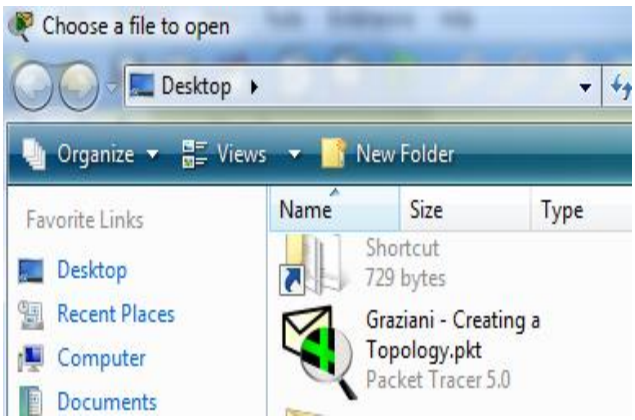
Step 9: Saving the Topology

Perform the following steps to save the topology (uses .pkt file extension).

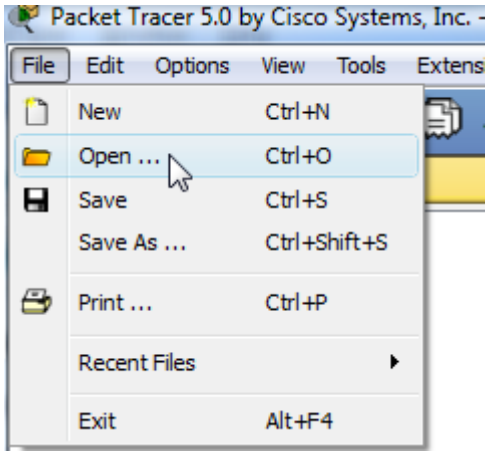


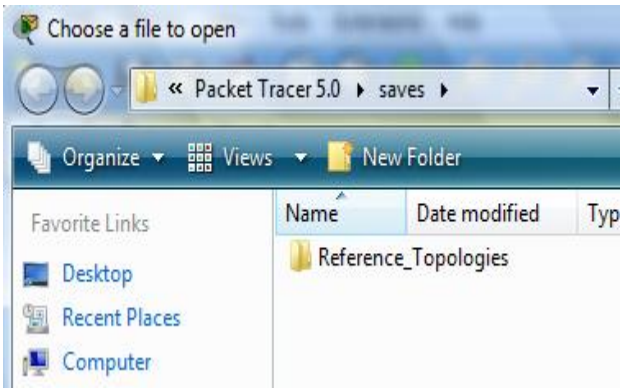
Opening Existing Topologies





Opening Existing PT Topologies





*****