

Lab 2: Network Devices & Packet Tracer

**Catalyst
switches**

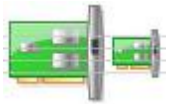


ASR 1000 routers



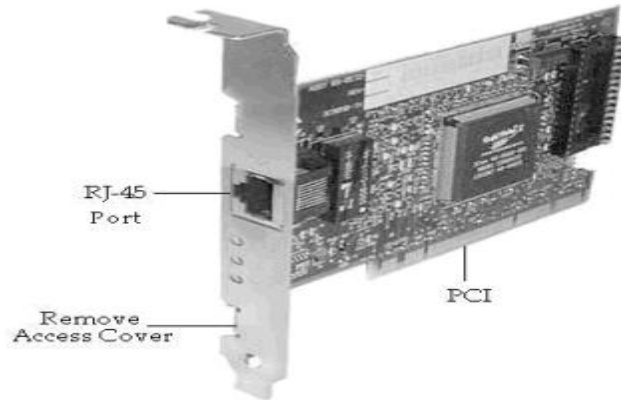
ISR G2 routers

University of Jordan
Faculty of Engineering & Technology
Computer Engineering Department
Computer Networks Laboratory
907528



NIC

The network interface card (NIC) is the expansion card you install in your computer to connect, your computer to the network. This device provides the physical, electrical, and electronic connections to the network media. A NIC is either an expansion card (the most popular implementation) or built in to the motherboard of the computer.

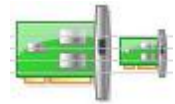


NIC cards generally all have one or two light emitting diodes (LEDs) that help in diagnosing problems with their functionality. If there are two separate LEDs, one of them may be the Link LED, which illuminates when proper connectivity to an active network is detected. The other most popular LED is the Activity LED. The Activity LED will tend to flicker, indicating the intermittent transmission or receipt of frames to or from the network.

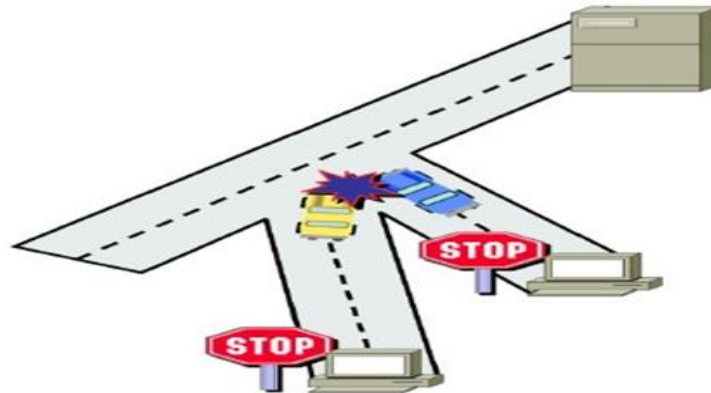
Hub

A hub is probably the most common Physical layer device found on networks. A hub serves as a central connection point for several network devices. It repeats what it receives on one port to all other ports, including the port on which the signal was received, so that the transmitting device may monitor and recover from collisions because every device in the network connects directly to the hub through a single cable.





Any transmission received on one port will be sent out all the other ports in the hub (broadcasting), including the receiving pair for the transmitting device, so that CSMA/CD on the transmitter can monitor for collisions.



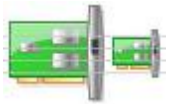
Bridge

A *bridge* is a network device, operating at the Data Link layer, that logically separates a single network into two segments, but it lets the two segments appear to be one network to higher layer protocols. The primary use for a bridge is to keep traffic meant for devices on one side of the bridge from passing to the other side.

Switch

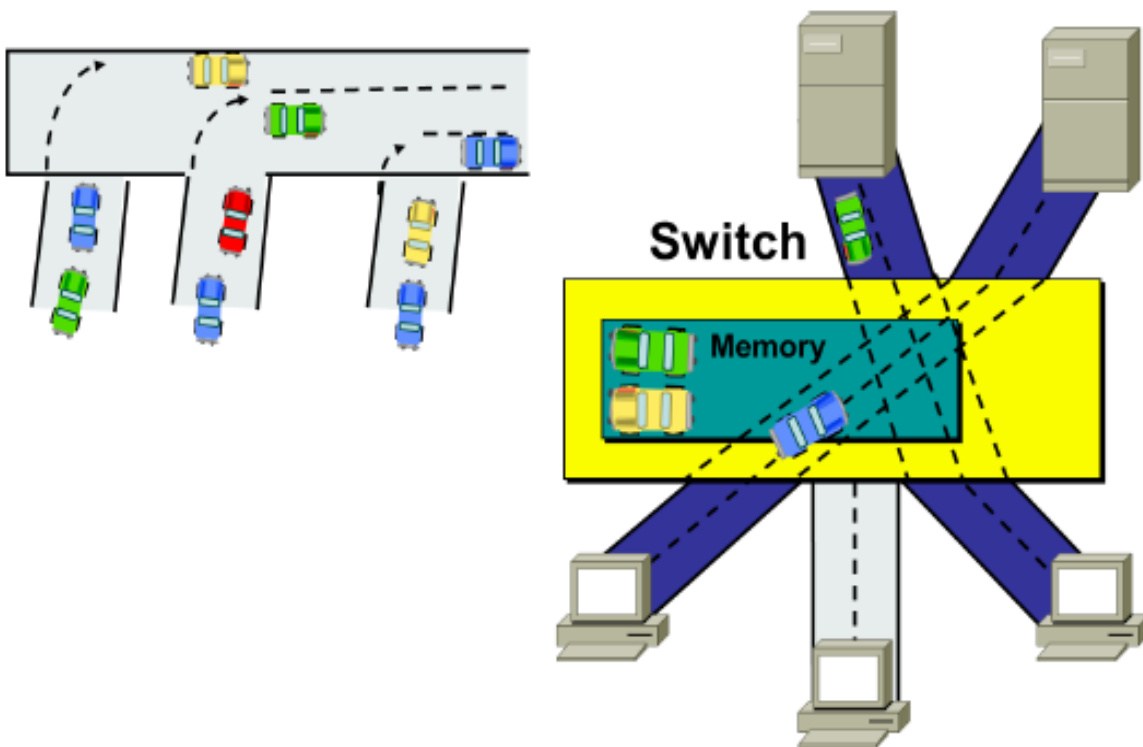
The *switch* is more intelligent than a hub in that it can actually understand the frames that pass through it. Switch builds a table of the MAC addresses of all the devices connected to it. When two devices attached to the switch want to communicate, the sending device sends its data on to its local segment. This data is heard by the switch (similar to the way a hub functions).

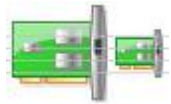
However, when the switch receives the data it examines the Data Link header for the MAC address of the destination device and forwards it to the correct port. This process triggers a function within the switch that opens a virtual pipe between ports that can use the full bandwidth of the topology.



Switches have risen to the high level of popularity because of their ability to prevent collisions from occurring between the devices attached directly to their ports, thus increasing overall network throughput and efficiency. This stems from the fact that every port on a switch is in a different collision domain.

A *collision domain* is that group of devices whose frames could potentially collide with one another.





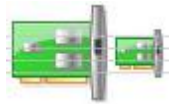
| | Hub | Switch |
|--------------------------------|--|--|
| Layer in the OSI model: | Physical layer(Layer 1 Device) | Data Link Layer (Layer 2 devices) |
| Transmission Type: | Only Broadcast | At Initial Level Broadcast then Uni-cast & Multicast |
| Table: | There is no MAC table in Hub, Hub can't learn MAC address. | Store MAC address in lookup table, Switch can Learn MAC address. |
| Usage : | LAN | LAN |
| Ports: | 4 ports | 24/48 ports |
| Collision: | In Hub collision occur. | In Full Duplex mode no Collision occurs. |
| Transmission Mode: | Half duplex | Full duplex |
| Collision Domain: | Hub has One collision domain. | In Switch, every port has its own collision domain. |
| Cost: | Cheaper than switches | 3-4 times costlier than Hub |
| Broadcast Domain: | Hub has one Broadcast Domain. | Switch has one broadcast domain |

The Wireless Access Point (WAP)

Layer 2 device that connect multiple wireless computers to an existing wired network. The WAP is essentially a wireless bridge (or switch, as multiple end devices can connect simultaneously). In addition, it can connect those wireless clients to a wired network. As with a bridge or switch, the WAP indiscriminately propagates all broadcasts to all wireless and wired devices while allowing filtering based on MAC addresses.

The WAP contains at least one radio antenna that it uses to communicate with its clients via radio frequency (RF) signals. The WAP can (depending on software settings) act as either an access point, which allows a wireless user transparent access to a wired network, or a wireless bridge, which will connect a wireless network to a wired network yet only pass traffic it knows belongs on the other side.

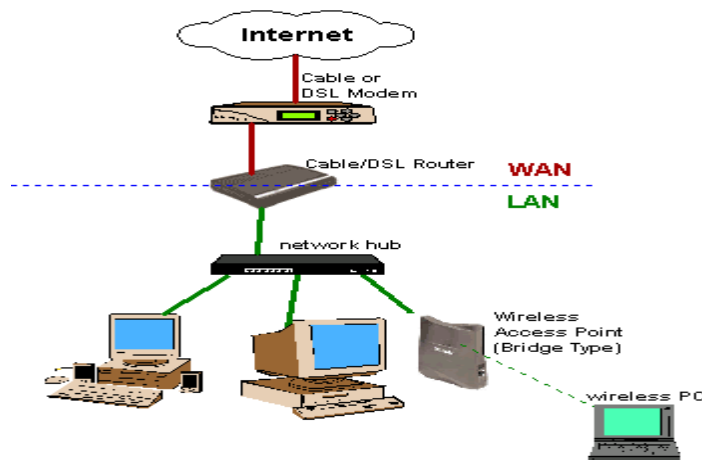




Router

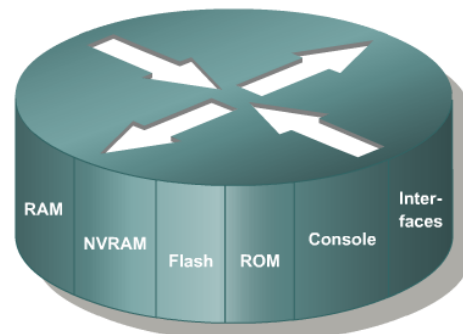
Routers are Network layer devices that connect multiple networks or segments to form a larger internetwork. They are also the devices that facilitate communication within this internetwork.

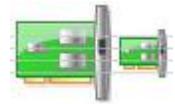
The main functions of routers as a gateway that connect LAN to WAN either it can make intelligent decisions about how best to get network data to its destination based on network performance data that it gathers from the network itself. Routers do not propagate broadcasts from one of their ports to another, meaning that each port on a router is in a different broadcast domain.



A *broadcast domain* is the collection of all devices that will receive each other's broadcast frames. Several companies manufacture routers, but probably three of the biggest names in the business are Nortel Networks, Juniper Networks, and Cisco Systems. A router is a special type of computer. It has the same basic components as a standard desktop PC. However, routers are designed to perform some very specific functions. Just as computers need operating systems to run software applications, routers need the Internetwork Operating System software (IOS) to run configuration files. These configuration files contain the instructions and parameters that control the flow of traffic in and out of the routers. The main parts of a router are:

- ROM
- Flash memory
- NVRAM
- RAM/DRAM
- Interfaces





Read-only memory (ROM)

Loads the bootstrap program that initializes the router's basic hardware components. It's not modified during normal operations, but it can be upgraded with special plug-in chips. The content of ROM is maintained even when the router is rebooted

Flash memory

A type of erasable, programmable, read-only memory (EPROM), not typically modified during normal operations. However, it can be upgraded or erased when necessary the content of flash memory is maintained even when the router is rebooted.

Flash memory contains the working copy of the current Cisco IOS. Is the component that initializes the IOS for normal router operations.

Nonvolatile random access memory (NVRAM)

A special type of RAM that is not cleared when the router is rebooted. The startup configuration file for the router is stored in NVRAM by default. This is the first file created by the person who sets up the router. The Cisco IOS uses the configuration file in NVRAM during the router boot process

Random access memory (RAM)

Also known as **dynamic random access memory (DRAM)** is a **volatile** hardware component, its information is not maintained in the event of a router reboot changes to the router's running configuration take place in RAM/DRAM.

Router Interfaces:

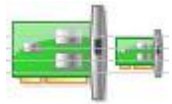
Management ports

Routers have physical connectors that are used to manage the router. These connectors are known as management ports. Unlike Ethernet and serial interfaces, management ports are not used for packet forwarding. The most common management port is the console port. The **console port** is used to connect a terminal, or most often a PC running terminal emulator software, to configure the router without the need for network access to that router. The console port must be used during initial configuration of the router.

Another management port is the **auxiliary port**. Not all routers have auxiliary ports. At times the auxiliary port can be used in ways similar to a console port. It can also be used to attach a modem.

Network Interfaces

The term interface refers to a physical connector on the router whose main purpose is to receive and forward packets. Routers have multiple interfaces that are used to connect to multiple networks. Typically, the interfaces connect to various types of networks, which mean that different types of media and connectors are required. Often a router will need to have different types of interfaces. For example, a router usually has FastEthernet interfaces for connections to different LANs and various types of WAN interfaces to connect a variety of serial links including T1, DSL and ISDN.



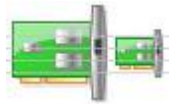
Like interfaces on a PC, the ports and interfaces on a router are located on the outside of the router. Their external location allows for convenient attachment to the appropriate network cables and connectors.

Like most networking devices, routers use LED indicators to provide status information. An interface LED indicates the activity of the corresponding interface. If an LED is off when the interface is active and the interface is correctly connected, this may be an indication of a problem with that interface. If an interface is extremely busy, its LED will always be on. Depending on the type of router, there may be other LEDs as well.

Router Interfaces - Physical Representation



| | Router | Switch |
|--------------------------------|--|--|
| Layer: | Network Layer (Layer 3 devices) | Data Link Layer (Layer 2 devices) |
| Transmission Type: | At Initial Level Broadcast then Uni-cast & Multicast | At Initial Level Broadcast then Uni-cast & Multicast |
| Table: | Store IP address in Routing table and maintain address at its own. | Store MAC address in lookup table and maintain address at its own, Switch can Learn MAC address. |
| Usage: | LAN & WAN | LAN |
| Collision: | No collisions. | In Full Duplex Switch no Collision occurs. |
| Ports: | 2/4/8 | 24/48 ports |
| Transmission Mode: | Full duplex | Full duplex |
| Data Transmission form: | Packet | Frame (L2 Switch) Frame & Packet (L3 switch) |
| Speed: | 1-10 Mbps(Wireless) 100 Mbps (Wired) | 10/100Mbps, 1Gbps |
| Broadcast Domain: | Every port has its own Broadcast domain. | Switch has one broadcast domain. |
| Routing Decision: | Take faster Routing Decision | Take more time for complicated routing Decision |



Layer 3 Switches

A Network layer device that has received much media attention of late is the Layer 3 Switch.

The Layer 3 part of the name corresponds to the Network layer of the OSI model. It performs the multiport, virtual LAN, data-pipelining functions of a standard Layer 2 Switch, but it can also perform basic routing functions between virtual LANs.

Gateways

A *gateway* is any hardware and software combination that connects dissimilar network environments. Gateways are the most complex of network devices because they perform translations at multiple layers of the OSI model. Router considered as a gateway because it combine LAN environment and WAN environment.

A router is assigned the gateway address for all the devices on the LAN. One purpose of a router is to serve as an entry point for packets coming into the network and exit point for packets leaving the network. Gateway addresses are very important to users. Cisco estimates that 80 percent of network traffic will be destined to devices on other networks, and only 20 percent of network traffic will go to local devices. If a gateway cannot be reached by the LAN devices, users will not be able to perform their job.

Other Devices

In addition to these network connectivity devices, there are several devices that, while maybe not directly connected to a network, participate in moving network data:

- Modems
- CSU/DSUs
- Firewalls

Modems

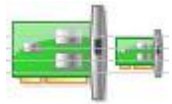
A *modem* is a device that modulates digital data onto an analog carrier for transmission over an analog medium and then demodulates from the analog carrier to a digital signal again at the receiving end. The term *modem* is actually an acronym that stands for Modulator/Demodulator.

When we hear the term *modem*, different types should come to mind:

- Traditional (POTS)
- DSL

Traditional (POTS)

Most modems you find in computers today fall into the category of traditional modems. These modems convert the signals from your computer into signals that travel over the plain old telephone service (POTS) lines. The majority of modems that exist today are POTS modems, mainly because PC manufacturers include one with a computer.



DSL

Digital subscriber line (DSL) is quickly replacing traditional modem access because it offers higher data rates for a reasonable cost. In addition, you can make regular phone calls while online. DSL uses higher frequencies (above 3200Hz) than regular voice phone calls use, which provides greater bandwidth (up to several megabits per second) than regular POTS modems provide while still allowing the standard voice frequency range to travel at its normal frequency to remain compatible with traditional POTS phones and devices. DSL “modems” are the devices that allow the network signals to pass over phone lines at these higher frequencies.

Most often, when you sign up for DSL service, the company you sign up with will send you a DSL modem for free or for a very low cost. This modem is usually an external modem, and it usually has both a phone line and an Ethernet connection. You must connect the phone line to a wall jack and the Ethernet connection to your computer (you must have an Ethernet NIC in your computer in order to connect to the DSL modem). Alternatively, a router, hub, or switch may be connected to the Ethernet port of the DSL modem, increasing the options available for the Ethernet network.

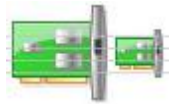
If you have DSL service on the same phone line you use to make voice calls, you must install DSL filters on all the phone jacks where you have a phone. Or, a DSL filter will be installed after the DSL modem for all the phones in a building. Otherwise, you will hear a very annoying hissing noise (the DSL signals) on your voice calls.

CSU/DSUs

The Channel Service Unit/Data Service Unit (CSU/DSU) is a common device found in equipment rooms when the network is connected via a T-series data connection or other digital serial technology such as T1 connection. It is essentially two devices in one that are used to connect a digital carrier to your network equipment. The *Channel Service Unit (CSU)* terminates the line at the customer’s premises. It also provides diagnostics and remote testing, if necessary. The *Data Service Unit (DSU)* does the actual transmission of the signal through the CSU. It can also provide buffering and data flow control.

Firewalls

A *firewall* is probably the most important device on a network if that network is connected to the Internet. Its job is to protect LAN resources from attackers on the Internet. Similarly, it can prevent computers on the network from accessing various services on the Internet. It can be used to filter packets based on rules that the network administrator sets. These rules state what kinds of information can flow into and out of a network’s connection to the Internet.



Part 2: Packet Tracer

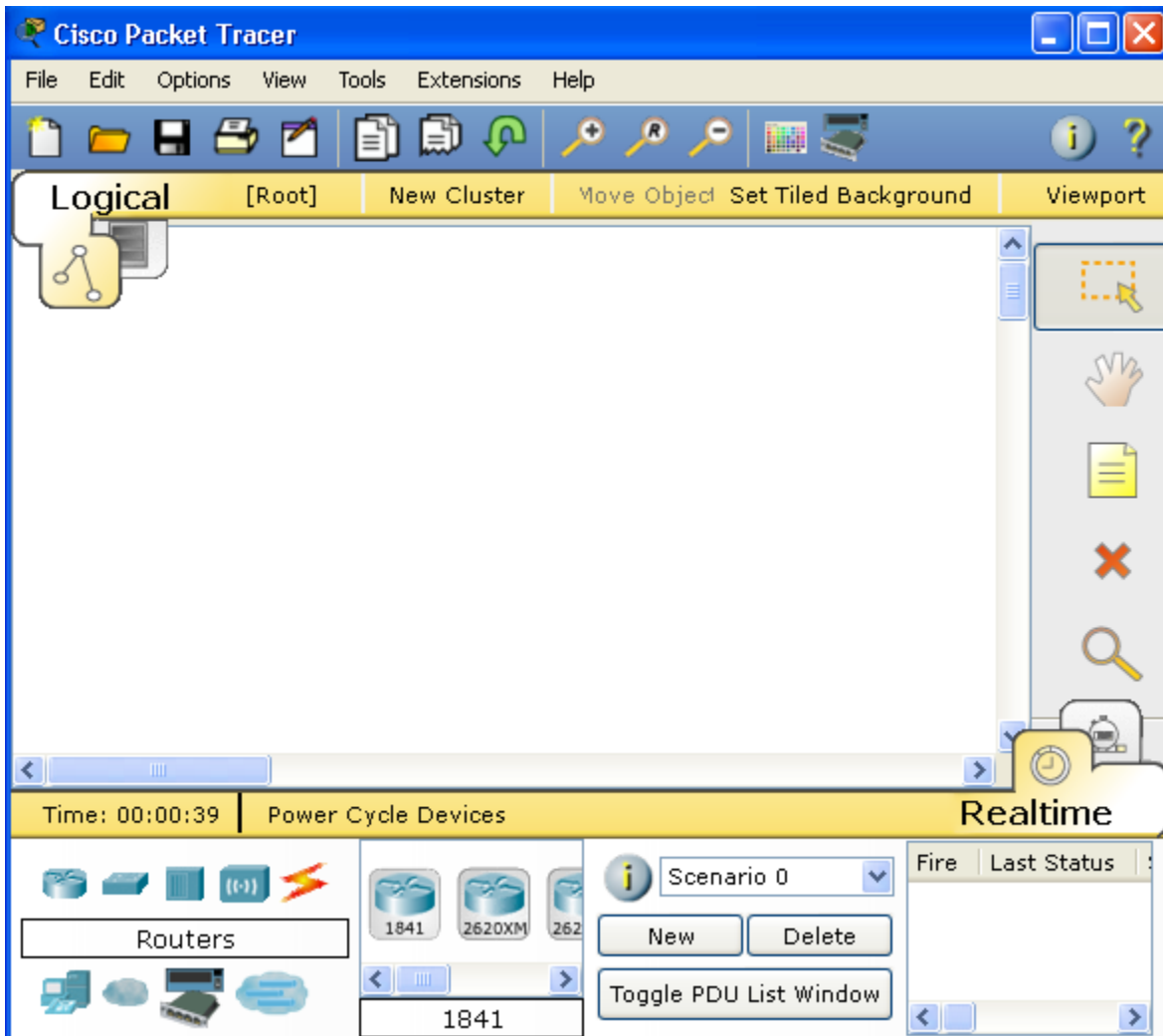
Packet Tracer is a protocol simulator developed by Dennis Frezzo and his team at Cisco Systems. Packet Tracer (PT) is a powerful and dynamic tool that displays the various protocols used in networking, in either Real Time or Simulation mode. This includes layer 2 protocols such as Ethernet and PPP, layer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

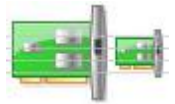
Before starting to follow the procedures below you should:

1. Download Packet Tracer Simulation Tool on your PC.
2. To get familiar with the Packet Tracer environment, watch this video named "Interface Overview" from the Help Tutorials.

Introduction to the Packet Tracer Interface using a Hub Topology

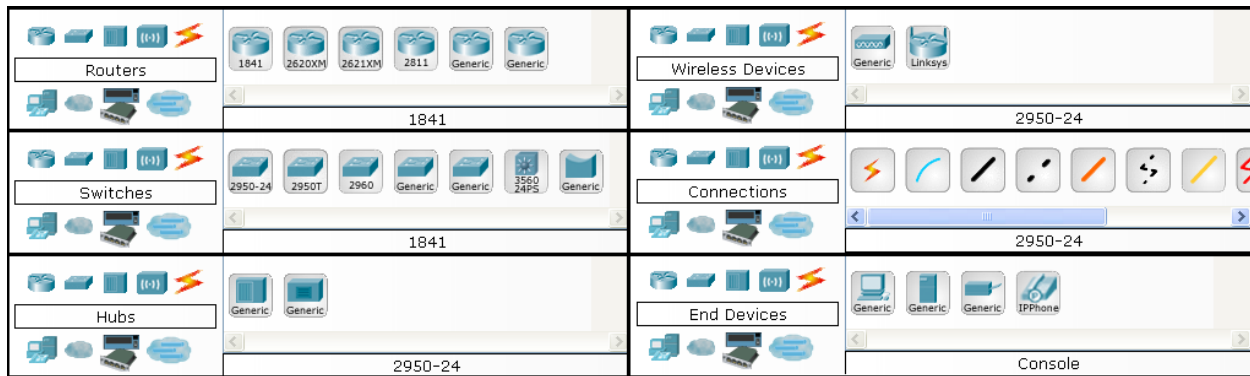
Step 1: Start Packet Tracer and Entering Simulation Mode





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.



Step 3: Building the Topology – Adding Hosts

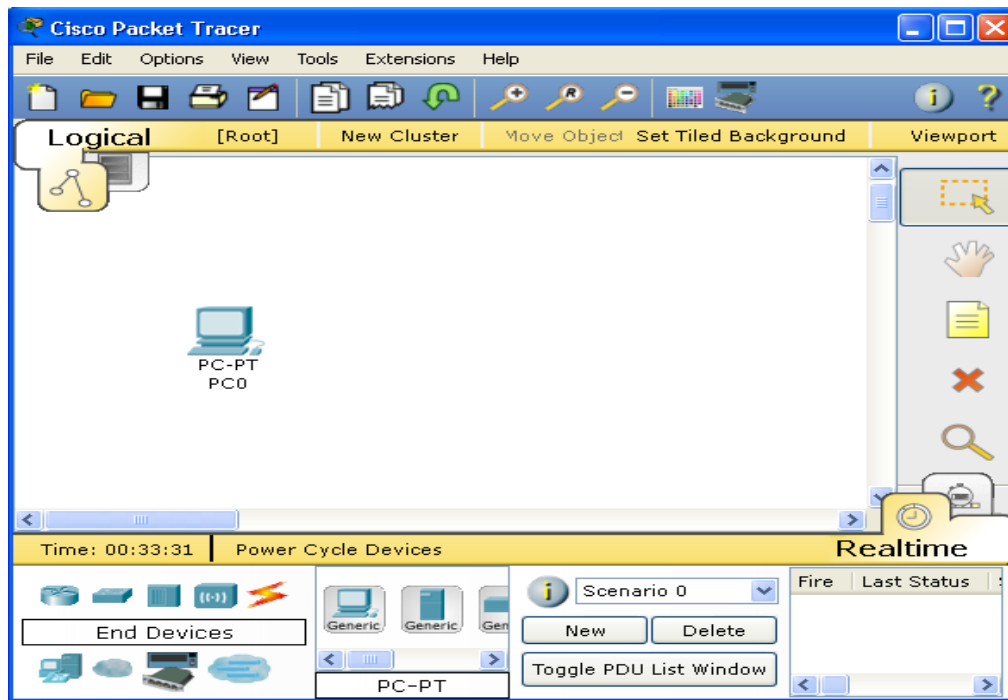
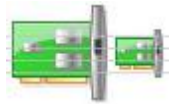
- Single click on the End Devices.



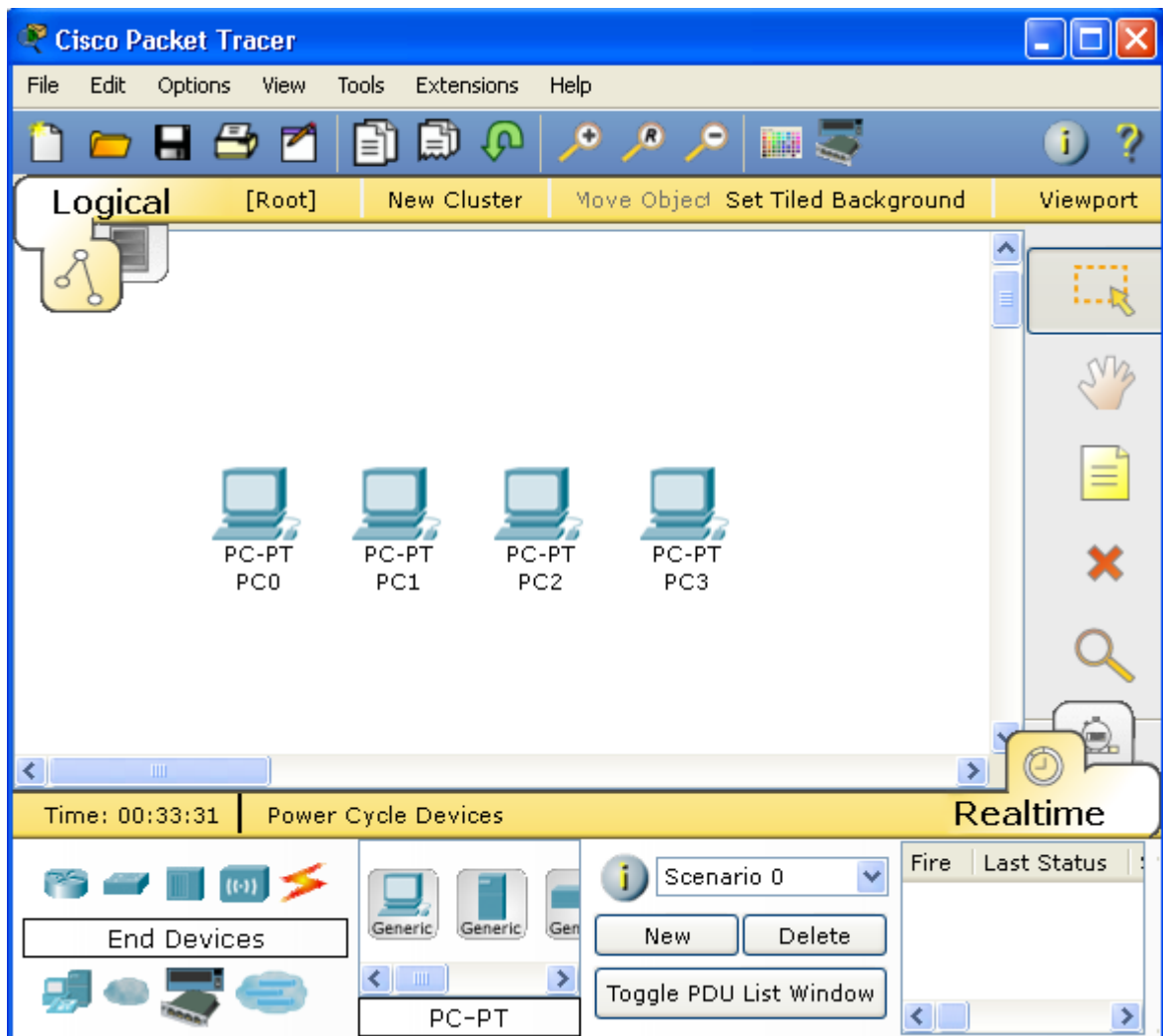
- Single click on the Generic host.

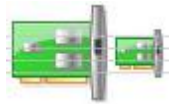


- Move the cursor into topology area. You will notice it turns into a plus “+” sign. Single click in the topology area and it copies the device.



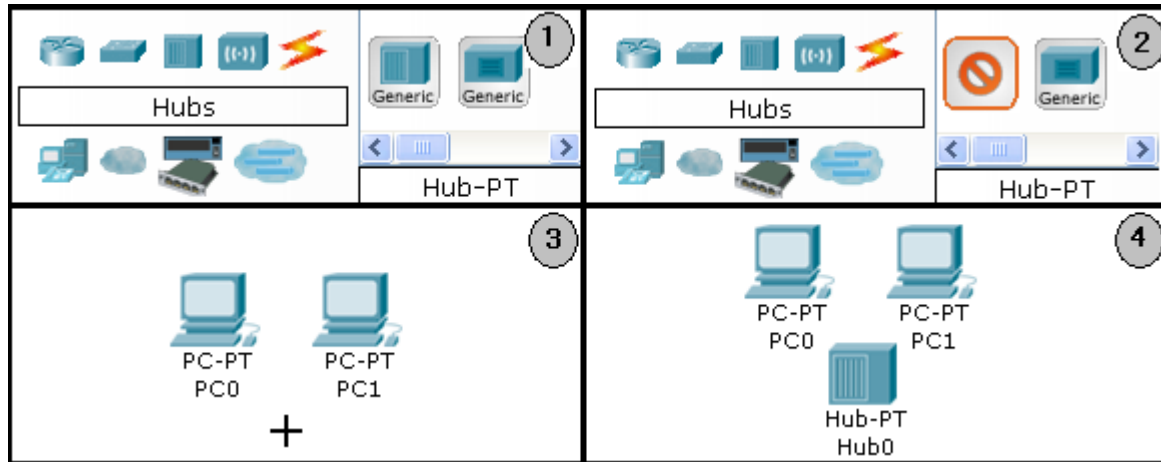
- Add three more hosts.



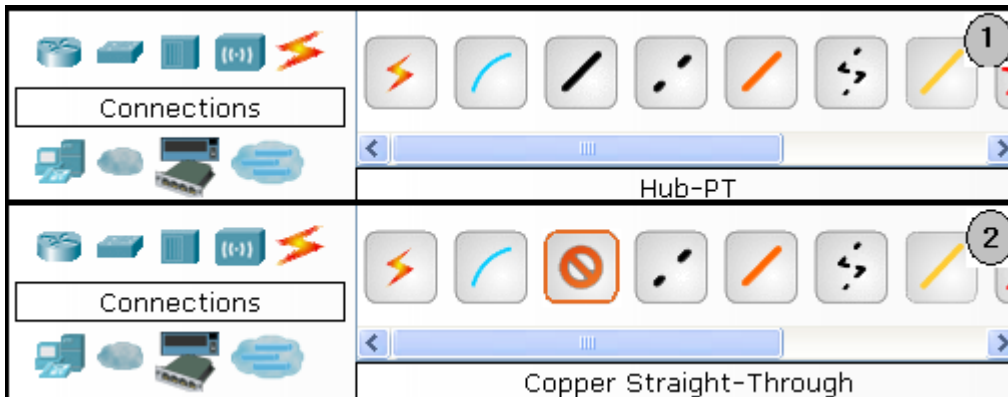


Step 4: Building the Topology – Connecting the Hosts to Hubs and Switches

- Adding a Hub: Select a hub, by clicking once on Hubs and once on a Generic hub.

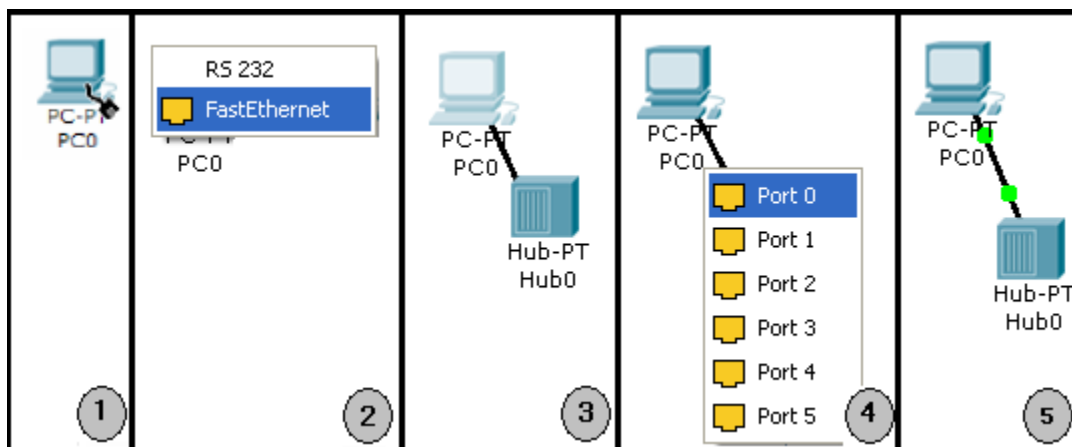
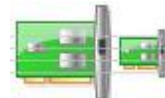


- Connect PC0 to Hub0 by first choosing Connections.
- Click once on the Copper Straight-through cable.

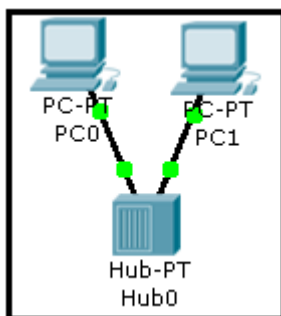


Perform the following steps to connect PC0 to Hub0:

1. Click once on PC0
2. Choose Fast Ethernet
3. Drag the cursor to Hub0
4. Click once on Hub0 and choose Port0
5. Notice the green link lights on both the PC0 Ethernet NIC and the Hub0 Port0 showing that the link is active.



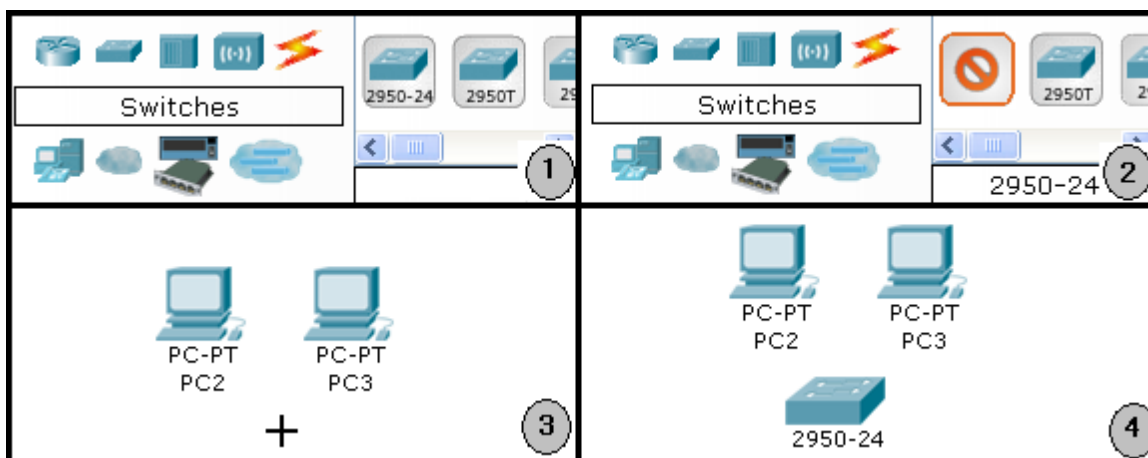
Repeat the steps above for PC1 connecting it to Port1 on Hub0. (The actual hub port you choose does not matter.)

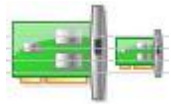


Adding a Switch

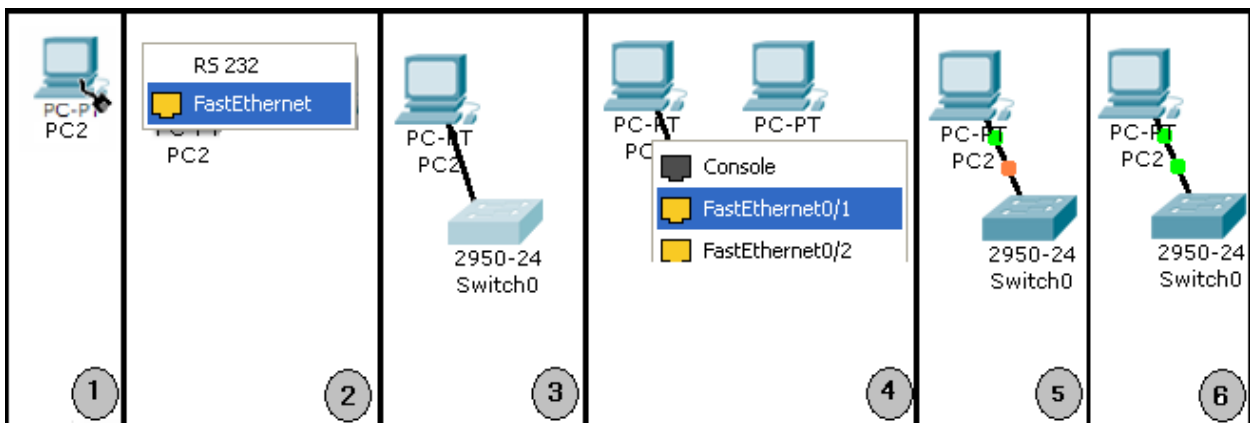
Select a switch, by clicking once on Switches and once on a 2950-24 switch.

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

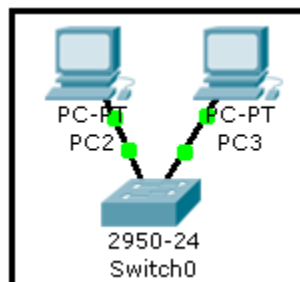


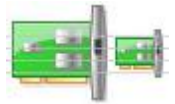


- Connect PC2 to Switch0 by first choosing Connections.
- Click once on the Copper Straight-through cable.
- Perform the following steps to connect PC2 to Switch0:
 1. Click once on PC2
 2. Choose FastEthernet
 3. Drag the cursor to Switch0
 4. Click once on Switch0 and choose FastEthernet0/1
 5. Notice 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 be forwarded out the switch port.

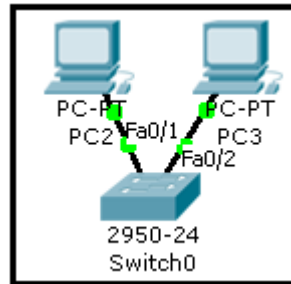


- Repeat the steps above for PC3 connecting it to Port3 on switch0 on port FastEthernet0/2. (The actual switch port you choose does not matter.)





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

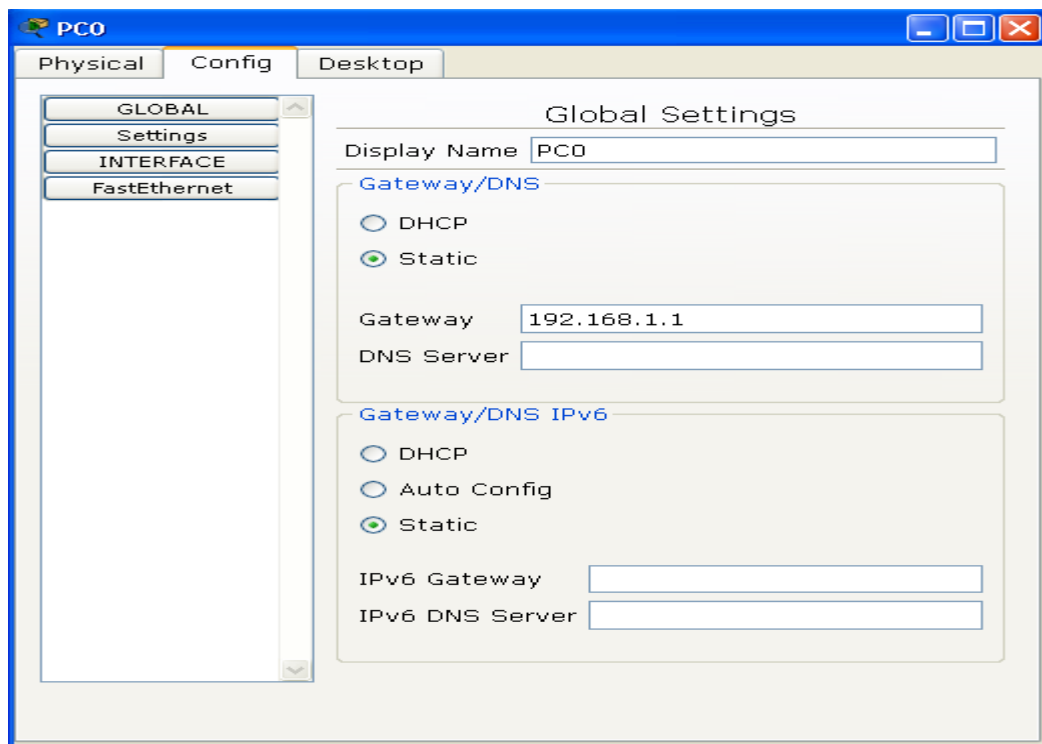
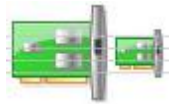


Step 5: Configuring IP Addresses and Subnet Masks on the Hosts

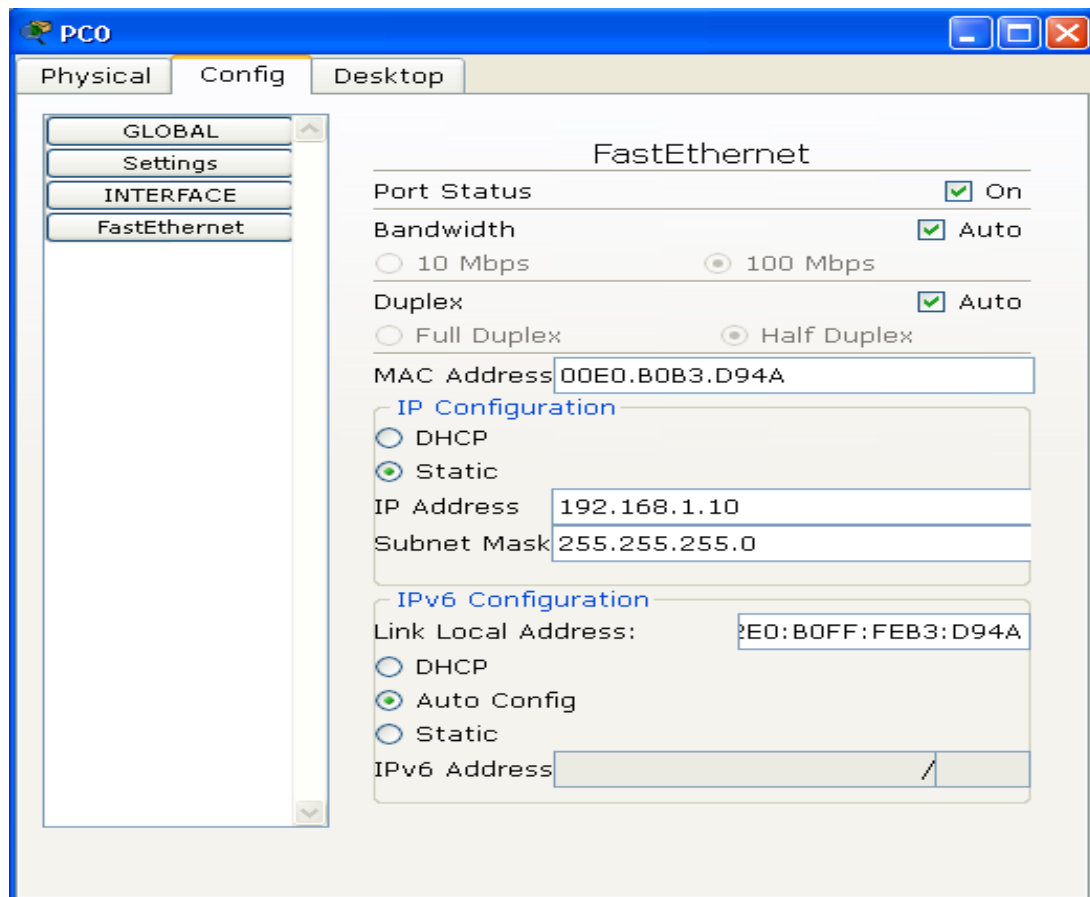
Before we can communicate between the hosts we need to configure IP Addresses and Subnet Masks on the devices.

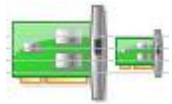
The screenshot shows the Packet Tracer interface. On the left, the 'Logical' view displays a network topology with a Hub-PT (Hub0) connected to PC0 and PC1, and a 2950-24 Switch0 connected to PC2 and PC3. On the right, the 'PC0' configuration window is open, showing the 'Config' tab. The 'Physical' tab shows a list of modules, including Linksys-WMP300N and various PT-HOST-NM modules. The 'Desktop' tab shows a physical device view of the PC. At the bottom, there is a status bar with the time '46:44:03' and the text 'Power Cycle Devices'.

- Click once on PC0.
- Choose the Config tab. 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. We will discuss this later, but this would be the IP address of the local router. If you want, you can enter the IP Address 192.168.1.1.



- Click on FastEthernet. Although we have not yet discussed IP Addresses, add the IP Address to 192.168.1.10. Click once in the Subnet Mask field to enter the default Subnet Mask. You can leave this at 255.255.255.0. 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 (autonegotiation), 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 Autonegotiation), 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.

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

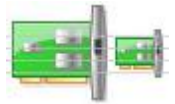
| Host | IP Address | Subnet Mask |
|------|-------------|---------------|
| PC0 | 192.68.1.10 | 255.255.255.0 |
| PC1 | 192.68.1.11 | 255.255.255.0 |
| PC2 | 192.68.1.12 | 255.255.255.0 |
| PC3 | 192.68.1.13 | 255.255.255.0 |

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

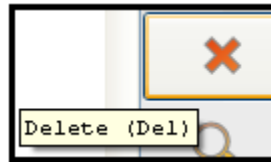
```

PC
PC
Link  IP Address  IPv6 Address  MAC Address
Up    192.168.1.10/24  <not set>    00E0.B0B3.D94A

Gateway: 192.168.1.1
DNS Server: <not set>
Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet
Hub0
  
```



- Deleting a Device or Link: To delete a device or link, choose the Delete tool and click on the item you wish to delete.

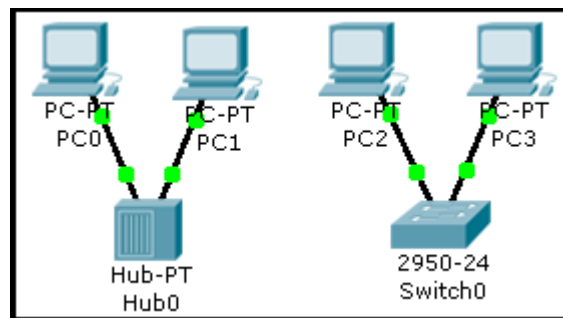


Step 6: Connecting Hub0 to Switch0

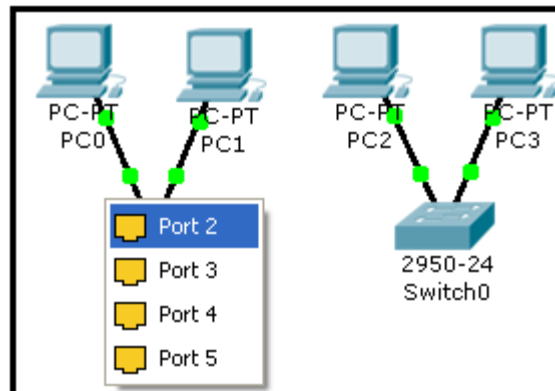
- To connect like-devices, like a Hub and a Switch, we will use a Cross-over cable. Click once the Cross-over Cable from the Connections options.

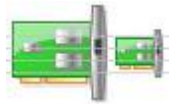


- Move the Connections cursor over Hub0 and click once.

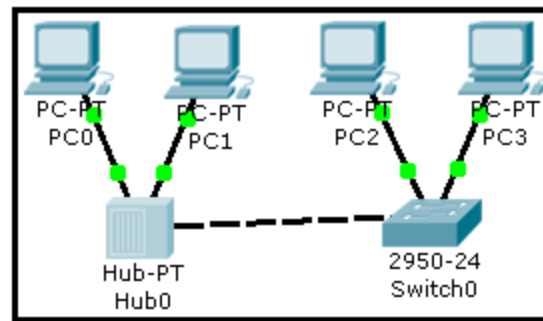


- Select Port2 (actual port does not matter).

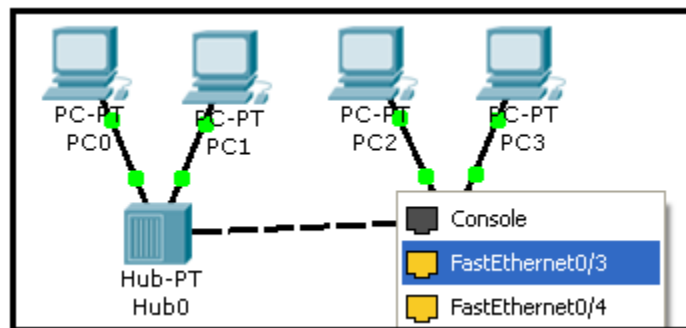




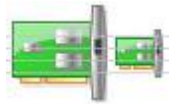
- Move the Connections cursor to Switch0.



- Click once on Switch0 and choose FastEthernet0/3 (actual port does not matter).



The link light for switch port FastEthernet0/3 will begin as amber and eventually change to green as the Spanning Tree Protocol transitions the port to forwarding.



Network Simulation

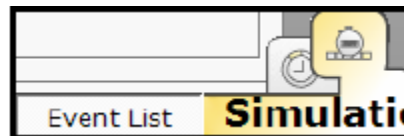
In this part, we are going to use the simulator to simulate traffic between hosts. For this scenario, delete the switch and host PC3, then connect host PC2 to the hub.

Task 1 Observe the flow of data from PC0 to PC1 by creating network traffic.

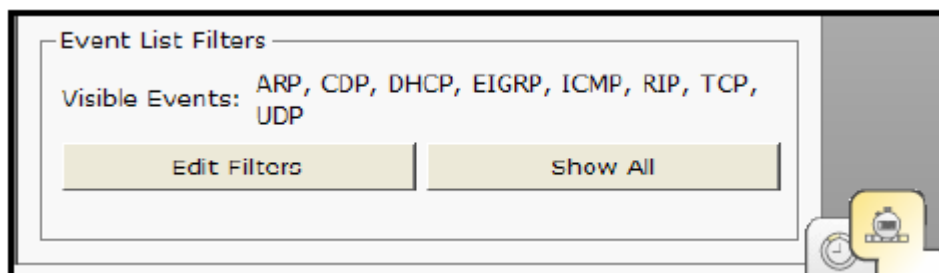
- Switch to Simulation Mode by selecting the tab that is partially hidden behind the Real Time tab in the bottom right-hand corner. The tab has the icon of a stopwatch on it.



NOTE: When Simulation Mode is chosen, a Simulation Panel will appear on the right side of the screen. This panel can be moved by moving the cursor at the top of the panel until it changes and then double-clicking on it. The panel can be restored to the original location by double-clicking on the Title bar. If the panel is closed, click on the Event List button.

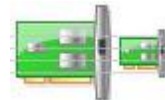


- Click on Edit Filters, and then select All/None to deselect every filter. Then choose ARP and ICMP and click in the workspace to close the Edit Filters window.

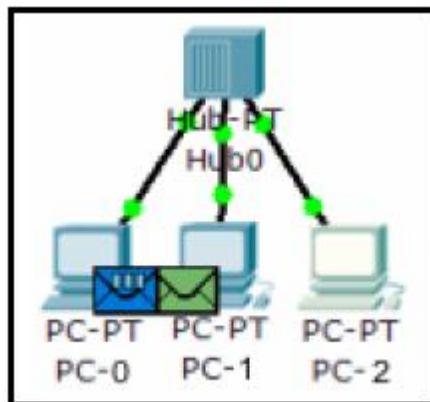


- Select a Simple PDU by clicking the closed envelope in the Common Tools Bar on the right.

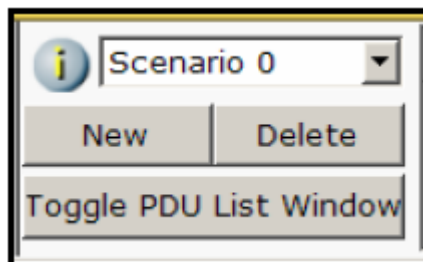




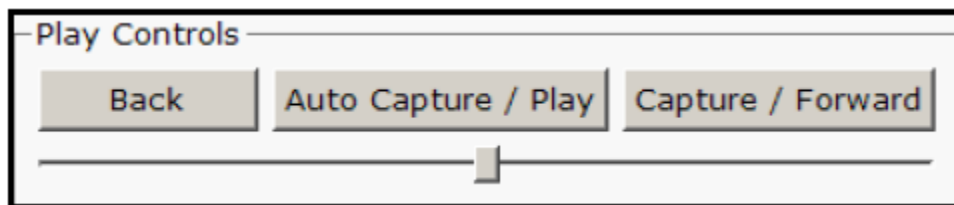
Move to PC0 and click to establish the source. Move to PC1 and click to establish the destination. Notice that two envelopes are now positioned beside PC0. This is referred to as a data traffic scenario. One envelope is an ICMP packet, while the other is an ARP packet. The Event List in the Simulation Panel will identify exactly which envelope represents ICMP and which represents an ARP.



A scenario may be deleted by clicking on the Delete button in the Scenario panel.

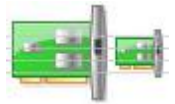


Multiple scenarios can be created by clicking on the New button in the Scenario panel. The scenarios can then be toggled between without deleting.



d. Select Auto Capture / Play from the Simulation Panel Play Controls.

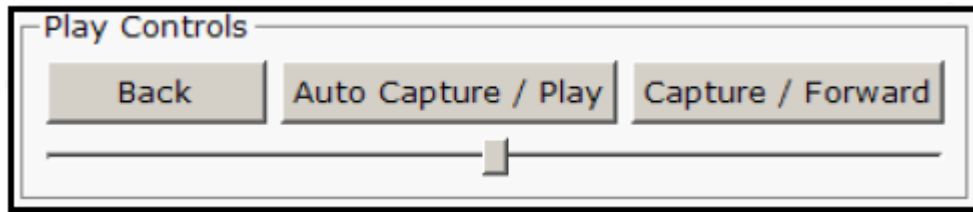
Below the Auto Capture / Play button is a horizontal bar, with a vertical button that controls the speed of the simulation. Dragging the button to the right will speed up the simulation, while dragging is to the left will slow down the simulation.



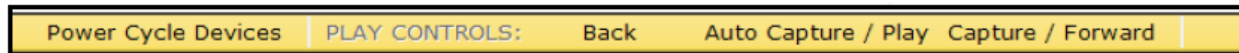
- e. Choose the Reset Simulation button in the Simulation window.



Notice that the ARP envelope is no longer present. This has reset the simulation but has not cleared any configuration changes or MAC / ARP table entries.

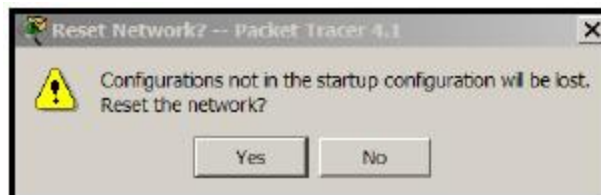


- f. Choose the Capture / Forward button.



Notice that the ICMP envelope moved forward one device and stopped. The Capture / Forward button will allow you to move the simulation one step at a time.

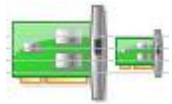
- g. Choose the Power Cycle Devices button on the bottom left, above the device icons.
- h. Choose Yes



Notice that both the ICMP and ARP envelopes are now present. The Power Cycle Devices will clear any configuration changes not saved and clear the MAC / ARP tables.

Task 2 View ARP Tables on each PC.

- a. Choose the Auto Capture / Play button and allow the simulation to run completely.



- b. Click on PC-0 and select the Desktop tab.



- c. Select the Command Prompt and type the command `arp -a`.
 d. Notice that the MAC address for PC2 is in the ARP table (to view the MAC address of PC2, click on PC2 and select the Config tab).
 e. To examine the ARP tables for PC1 and PC2 in another way, click on the Inspect Tool.



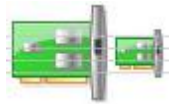
Then click on PC1 and the ARP table will appear in a new window.

| ARP Table for PC-B | | |
|--------------------|----------|-----------|
| IP Address | Hardware | Interface |
| | | |

Note that PC2 does not have an entry in the ARP table yet. Close the ARP Table window.

- f. Click on PC2 to view the ARP table. Then close the ARP Table window.

NOTE: To deactivate the Inspect Tool, click on the Select Tool



Task 3 Adding routers and



installing modules

a. In the Network

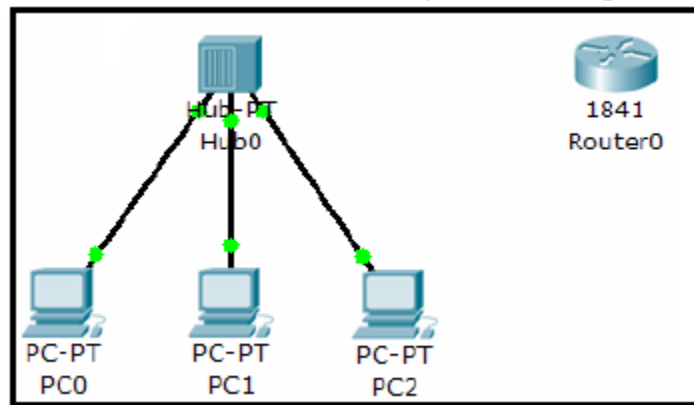
Component Box, click on the router.



b. Select an 1841 router.



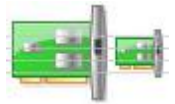
c. Move the cursor to the Logical Workspace and click on the desired location.



NOTE: If multiple instances of the same device are needed press and hold the **Ctrl** button, click on the desired device, and then release the **Ctrl** button. A copy of the device will be created and can now be move to the desired location.

d. Click on the router to bring up the Configuration Window. This window has three modes: Physical, Config, and CLI (Physical is the default mode).



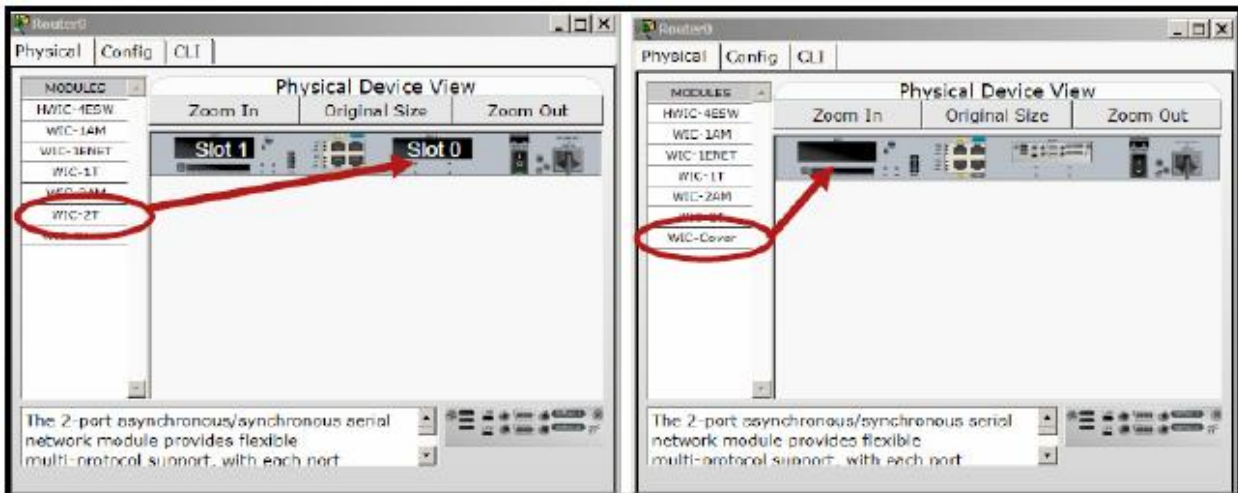


The Physical mode is used to add modules to a device, such as a WAN Interface Card (WIC). The Config mode is used for basic configuration. Commands are entered in a simple GUI format, with actual equivalent IOS commands shown in the lower part of the window. The CLI mode allows for advanced configuration of the device. This mode requires the user to enter the actual IOS commands just as they would on a live device.

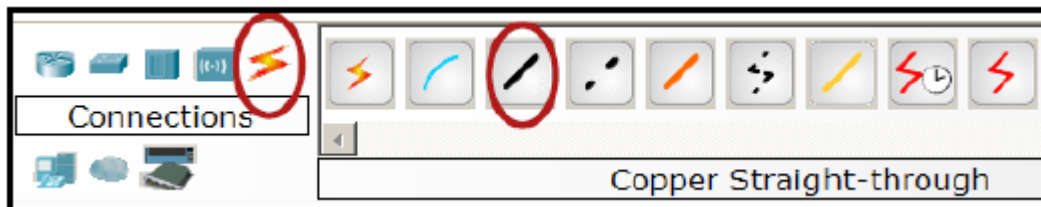
- e. In the Physical mode, click on the router power switch to turn the device off.




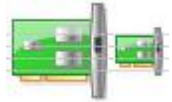
- f. Select the WIC-2T module and drag it to Slot 0 on the router. Then drag a WIC Cover to Slot 1.



- g. Power the device back on.
h. Click on the Network Component Box and select Connections. Then select a Copper Straight-through connection to connect the router to the hub.



NOTE: The Smart Connection  can be used to automatically select the appropriate cable type. However, the user will have no choice as to which interface the connection is assigned to; it will take the first available appropriate interface.



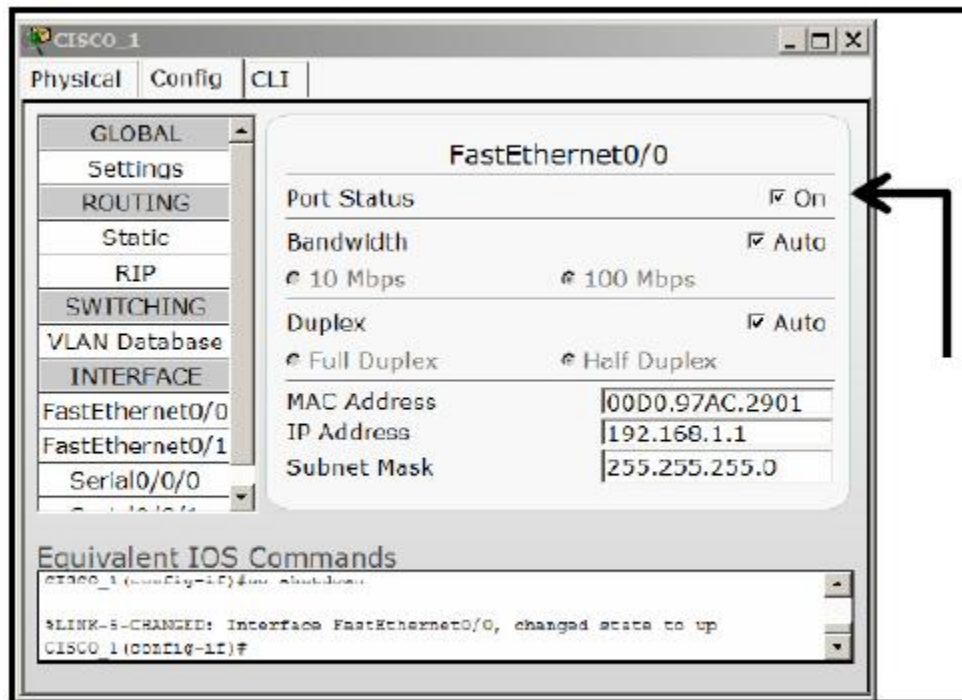
- i. Click on the hub and choose Port 3. Then click on the router and choose interface FastEthernet 0/0.

Task 4 Basic router configuration

- a. Click on the Config mode tab of Router0 to begin configuring the device.
- b. After the device has finished booting, change the display name of the router to CISCO_1. Changing the display name does not affect the configuration.

NOTE: If the device hangs up in the booting process, save the activity. Then close the application and reopen the file.

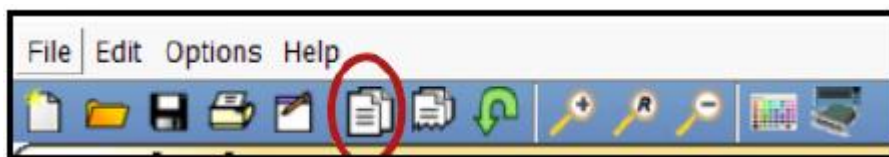
- c. Click in the Hostname field and type CISCO_1, and then press the TAB key. Note the equivalent IOS command is entered in the lower portion of the window.
- d. Click on interface FastEthernet 0/0 and assign the IP address 192.168.1.1, then press the TAB key. Enter the subnet mask 255.255.255.0.

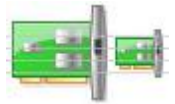


- e. Click the Port Status to On to enable the port (no shutdown).

Task 5 Create a copy of the existing router complete with WIC modules already in place

- a. Make sure that the existing router is selected (it will be grayed out).
- b. In the Main Tool Bar click on the Copy tool.





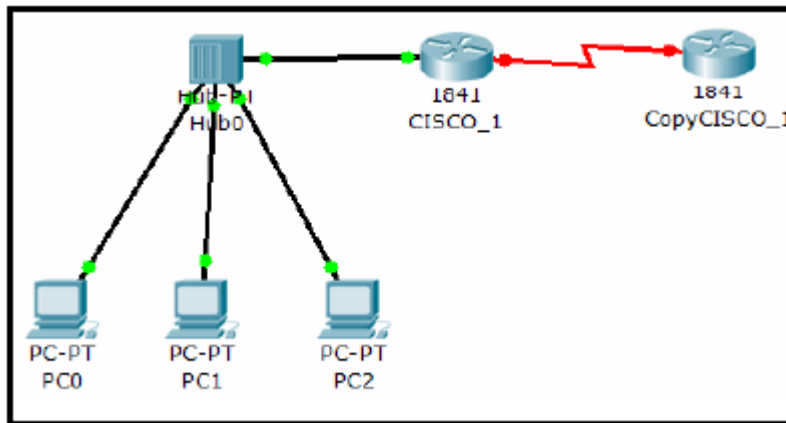
- c. Click on the Paste tool and the copied device will appear in the work area.



- d. Drag the new device to the desired location.
 e. Click on the Network Component Box and select Connections. Then select the Serial DCE connection.



- f. Click on the CISCO_1 router and connect to the Serial 0/0/0 interface.
 g. Click on the new router (copy CISCO_1) and connect to the Serial 0/0/0 interface.

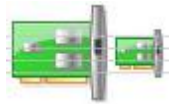


Task 6 Configuring the WAN link

- Click on the CISCO_1 router and select the Config mode
- Select interface Serial 0/0/0
- Configure the interface Serial 0/0/0 with the IP address 192.168.2.1, then press the TAB key and enter the subnet mask 255.255.255.0 on the interface.
- Set the clock rate to 56000
- Click the Port Status to On to enable the port (no shutdown).
- Click on the new router and select the Config mode.
- Change the Display Name and Hostname to CISCO_2.
- Configure the interface Serial 0/0/0 with the IP address 192.168.2.2, then press the TAB key and enter the subnet mask 255.255.255.0 on the interface.
- Click the Port Status to On to enable the port (no shutdown).

NOTE: The link lights on the serial link should change from red to green to indicate the link is active.

Task 7 Configure the routing protocol



- a. Click on the CISCO_1 router and select the Config tab. Then click on RIP and add the network address 192.168.1.0 and 192.168.2.0.
- b. Click on the CISCO_2 router and select the Config tab. Then click on RIP and add the network address 192.168.2.0.

NOTE: To configure RIP routing protocol, you add the directly connected networks ID IP addresses to each router.

- c. Go to each PC and set the Default Gateway to 192.168.1.1

NOTE: The default gateway is the fastethernet port which the PC is connected to.


Task 8 Set the default gateway on the PCs

- a. Click on PC0 and select the Config tab. Enter the default gateway address 192.168.1.1.
- b. Click on PC1 and select the Config tab. Enter the default gateway address 192.168.1.1.
- c. Click on PC2 and select the Config tab. Enter the default gateway address 192.168.1.1.

Task 9 Test the connectivity of the network

- a. Click on the Simulation mode.



- b. Select a Simple PDU  and click on PC-A as the source, then click on Cisco_2 as the destination. The ping should be successful.
- c. Test the ICMP packet sent from PC1 to CISCO_1 (first open the simulation mode and then open the info box that appears on the event list window to the right of the ICMP packet sent from PC1 to CISCO_1).

Task 10 Save the Packet Tracer file

- a. Save the Packet Tracer file as PT Basic.