

School of Engineering
Electrical and Computer Engineering Department
Computer Networks Lab
Lab. 1 Network Devices & Packet Tracer

Objectives

1. To become familiar with the switches and routers used in the lab.
2. To become familiar with the network simulator Packet Tracer.
3. To use the packet tracer to simulate a simple network.

Pre-lab Preparation:

1. Read thoroughly and prepare the experiment sheet.
2. Review the sections in Lab1 regarding the types of cables used.
3. You should try using Packet Tracer at home before the lab session.
4. You must bring a printed copy of this experiment with you to the lab.

Procedure:

Part 1: Router & Switch

Routers are computers and include many of the same hardware and software components found in a typical PC, such as CPU, RAM, ROM, and an operating system.

The main purpose of a router is to connect multiple networks and forward packets from one network to the next. This means that a router typically has multiple interfaces. Each interface is a member or host on a different IP network.

The router has a routing table, which is a list of networks known by the router. The routing table includes network addresses for its own interfaces, which are the directly connected networks, as well as network addresses for remote networks. A remote network is a network that can only be reached by forwarding the packet to another router.

Remote networks are added to the routing table in two ways: either by the network administrator manually configuring static routes or by implementing a dynamic routing protocol. Static routes do not have as much overhead as dynamic routing protocols; however, static routes can require more maintenance if the topology is constantly changing or is unstable.

Dynamic routing protocols automatically adjust to changes without any intervention from the network administrator. Dynamic routing protocols require more CPU processing and also use a certain amount of link capacity for routing updates and messages. In many cases, a routing table will contain both static and dynamic routes.

Routers make their primary forwarding decision at Layer 3, the Network layer. However, router interfaces participate in Layers 1, 2, and 3. Layer 3 IP packets are encapsulated into a Layer 2 data link frame and encoded into bits at Layer 1. Router interfaces participate in Layer 2 processes associated with their encapsulation. For example, an Ethernet interface on a router participates in the ARP process like other hosts on that LAN.

Router Components and their Functions

Like a PC, a router also includes:

- Central Processing Unit (CPU)
- Random-Access Memory (RAM)
- Read-Only Memory (ROM)

CPU

The CPU executes operating system instructions, such as system initialization, routing functions, and switching functions.

RAM

RAM stores the instructions and data needed to be executed by the CPU. RAM is used to store these components:

- Operating System: The Cisco IOS (Internetwork Operating System) is copied into RAM during bootup.
- Running Configuration File: This is the configuration file that stores the configuration commands that the router IOS is currently using. With few exceptions, all commands configured on the router are stored in the running configuration file, known as runningconfig.
- IP Routing Table: This file stores information about directly connected and remote networks. It is used to determine the best path to forward the packet.
- ARP Cache: This cache contains the IPv4 address to MAC address mappings, similar to the ARP cache on a PC. The ARP cache is used on routers that have LAN interfaces such as Ethernet interfaces.
- Packet Buffer: Packets are temporarily stored in a buffer when received on an interface or before they exit an interface.

RAM is volatile memory and loses its content when the router is powered down or restarted. However, the router also contains permanent storage areas, such as ROM, flash and NVRAM.

ROM

ROM is a form of permanent storage. Cisco devices use ROM to store:

- The bootstrap instructions
- Basic diagnostic software
- Scaled-down version of IOS

ROM uses firmware, which is software that is embedded inside the integrated circuit. Firmware includes the software that does not normally need to be modified or upgraded, such as the bootup instructions. Many of these features, including ROM monitor software, will be discussed in a later course. ROM does not lose its contents when the router loses power or is restarted.

Flash Memory

Flash memory is nonvolatile computer memory that can be electrically stored and erased. Flash is used as permanent storage for the operating system, Cisco IOS. In most models of Cisco routers, the IOS is permanently stored in flash memory and copied into RAM during the bootup process, where it is then executed by the CPU. Some older models of Cisco routers run the IOS directly from flash. Flash consists of SIMMs or PCMCIA cards, which can be upgraded to increase the amount of flash memory.

Flash memory does not lose its contents when the router loses power or is restarted.

NVRAM

NVRAM (Nonvolatile RAM) does not lose its information when power is turned off. This is in contrast to the most common forms of RAM, such as DRAM, that requires continual power to maintain its information. NVRAM is used by the Cisco IOS as permanent storage for the startup configuration file (startup-config). All configuration changes are stored in the running-config file in RAM, and with few exceptions, are implemented immediately by the IOS. To save those changes in case the router is restarted or loses power, the running-config must be copied to NVRAM, where it is stored as the startup-config file. NVRAM retains its contents even when the router reloads or is powered off.

ROM, RAM, NVRAM, and flash are discussed in the following section which introduces the IOS and the bootup process. They are also discussed in more detail in a later course relative to managing the IOS.

It is more important for a networking professional to understand the function of the main internal components of a router than the exact location of those components inside a specific router. The internal physical architecture will differ from model to model.

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.

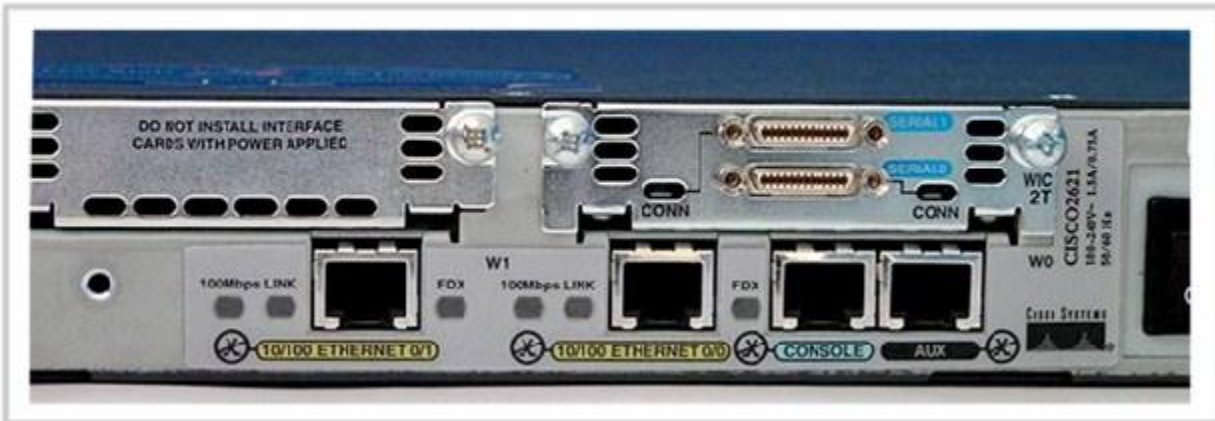
Network Interfaces

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 means 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



The network switch plays an integral part in most Ethernet LANs. Mid-to-large sized LANs contain a number of linked managed switches. A switch operates at the data-link layer of the OSI model to create a different collision domain per switch port.

Similar components available on switches as described above for routers, a switch has a console port for management and a set of Ethernet interfaces for LANs connections.



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.

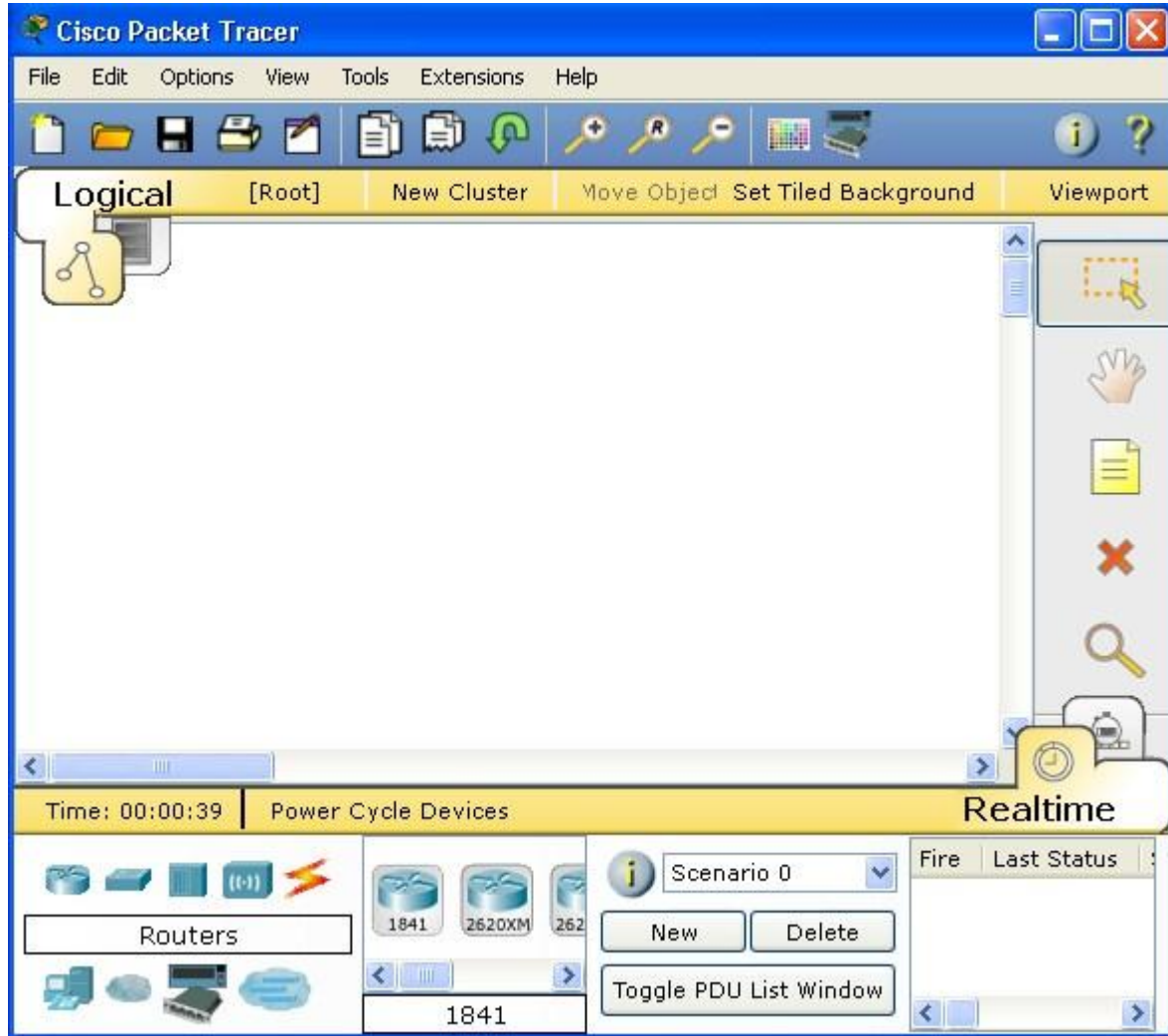
Before starting to follow the procedures below you should:

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.

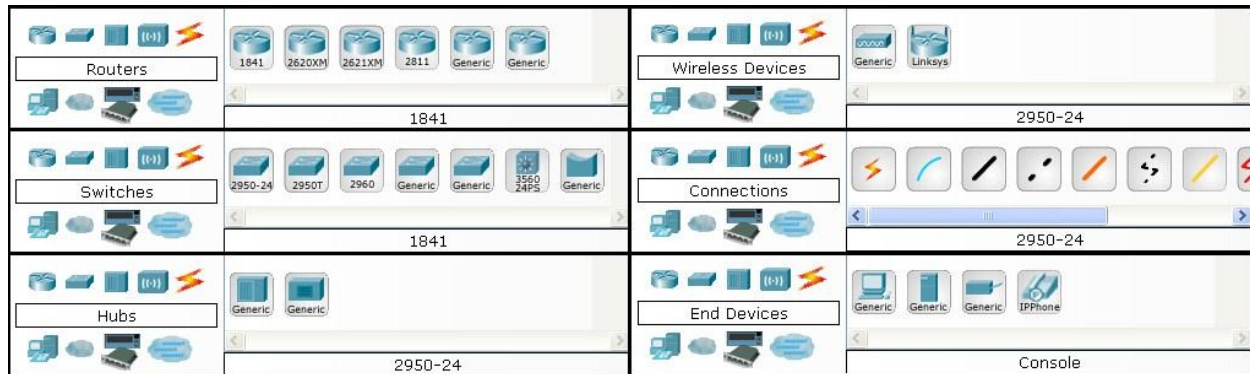
Introduction to the Packet Tracer Interface using a Hub Topology Step

1: Start Packet Tracer and Enter 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.



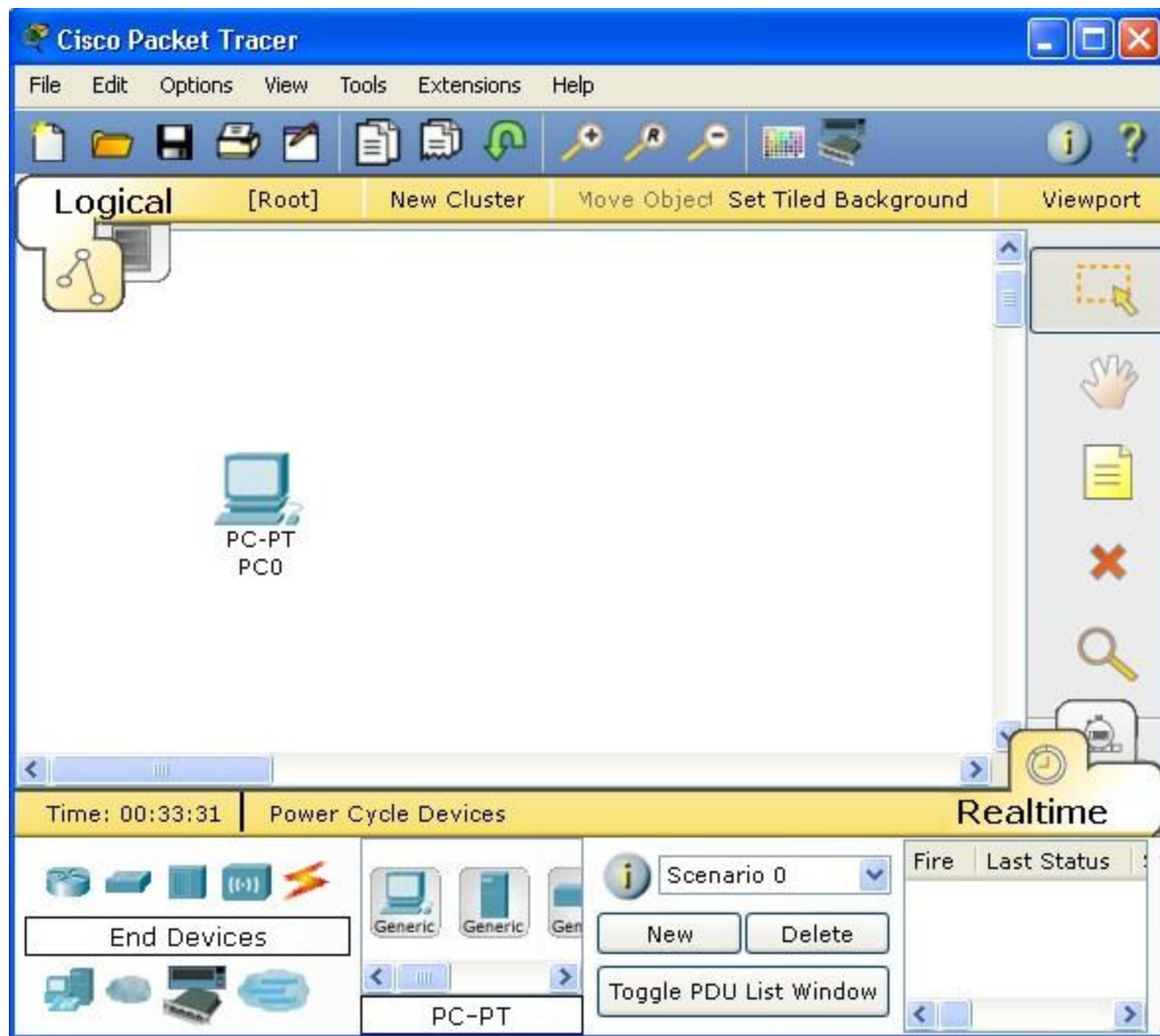
Step 3: Building the Topology – Adding Hosts •
Single click on the End Devices.



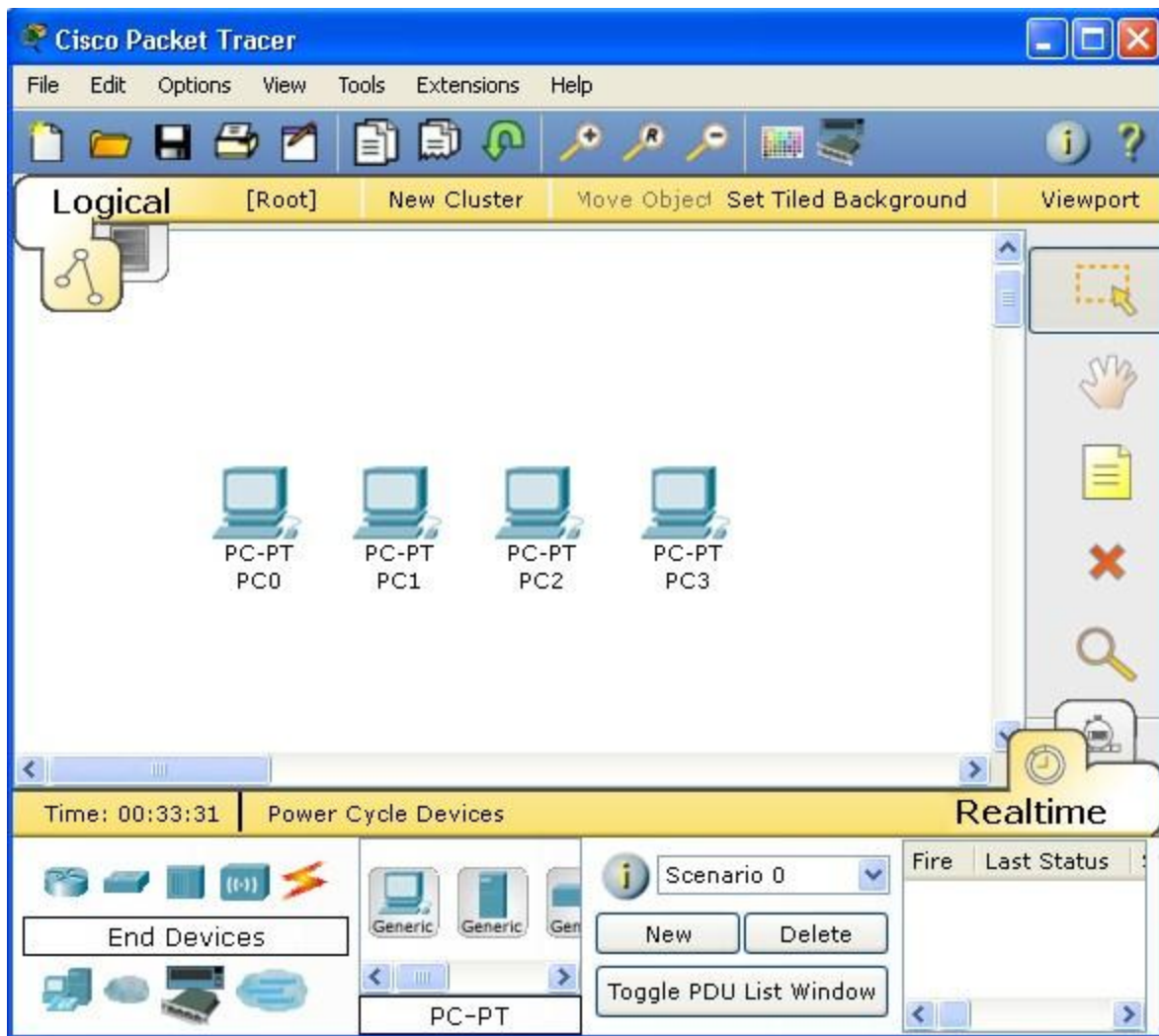
- Single click on the Generic host.



- 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.

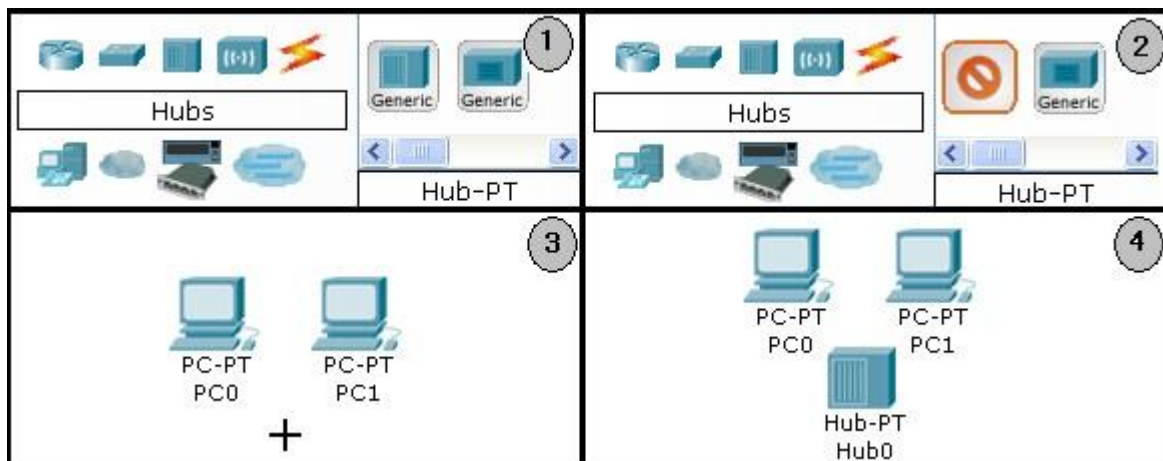


- Add three more hosts.

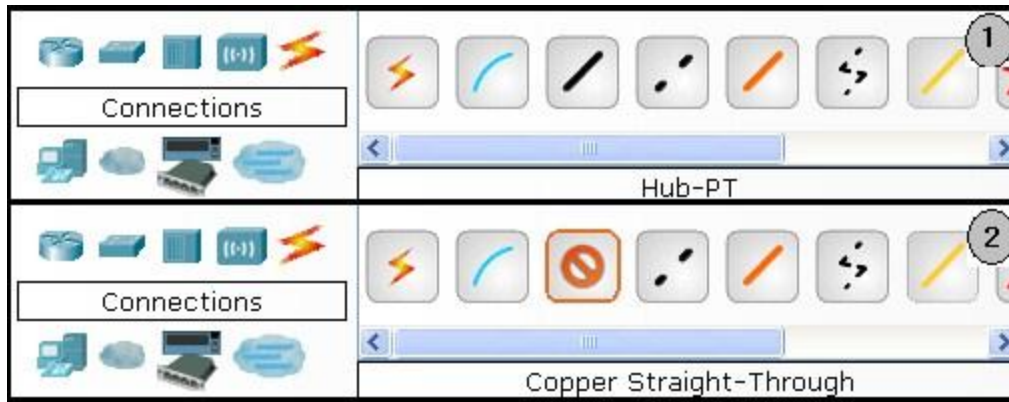


Step 4: Building the Topology – Connecting the Hosts to Hubs and Switches

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

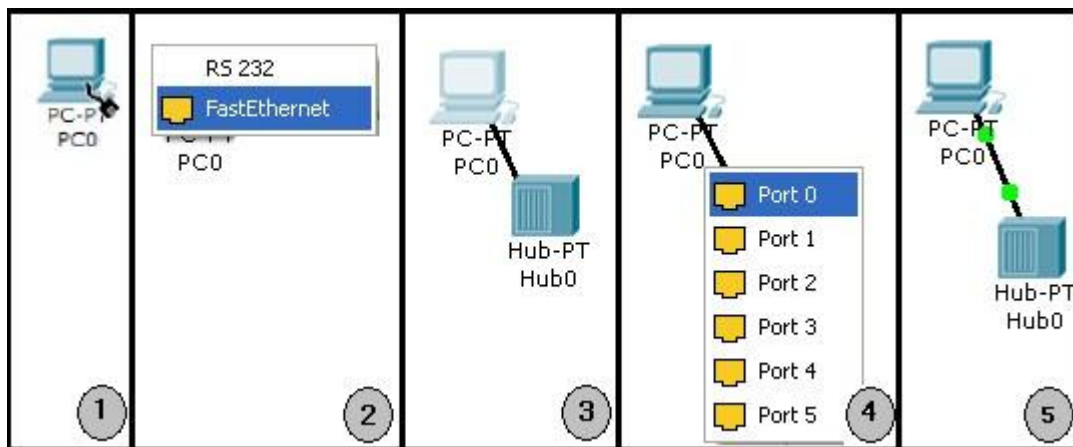


- Connect PC0 to Hub0 by first choosing Connections.
- Click once on the Copper Straight-through cable.

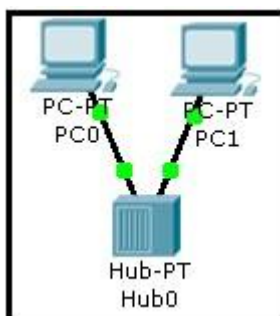


Perform the following steps to connect PC0 to Hub0:

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.



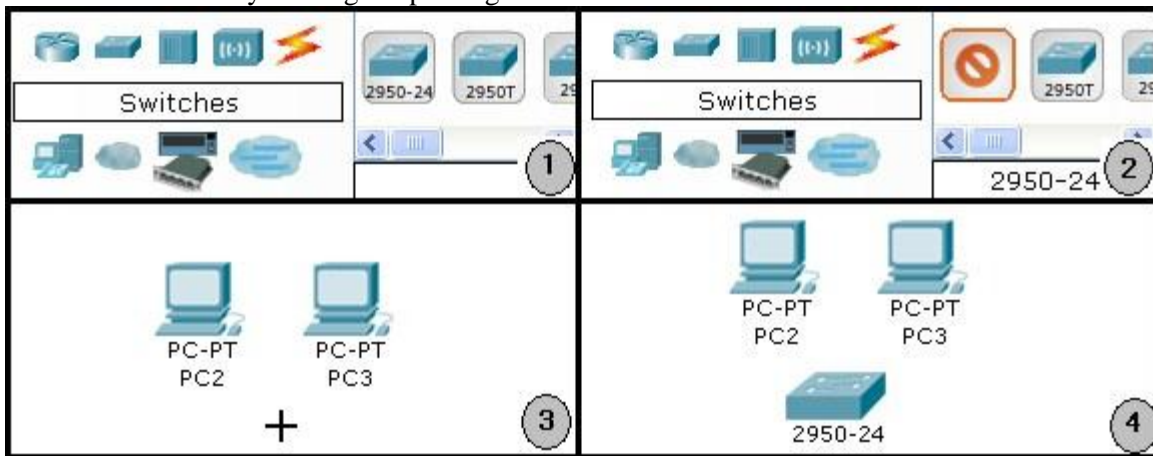
Repeat the steps above for PC1 connecting it to Port1 on Hub0. (The actual hub port you choose does not matter.)



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.

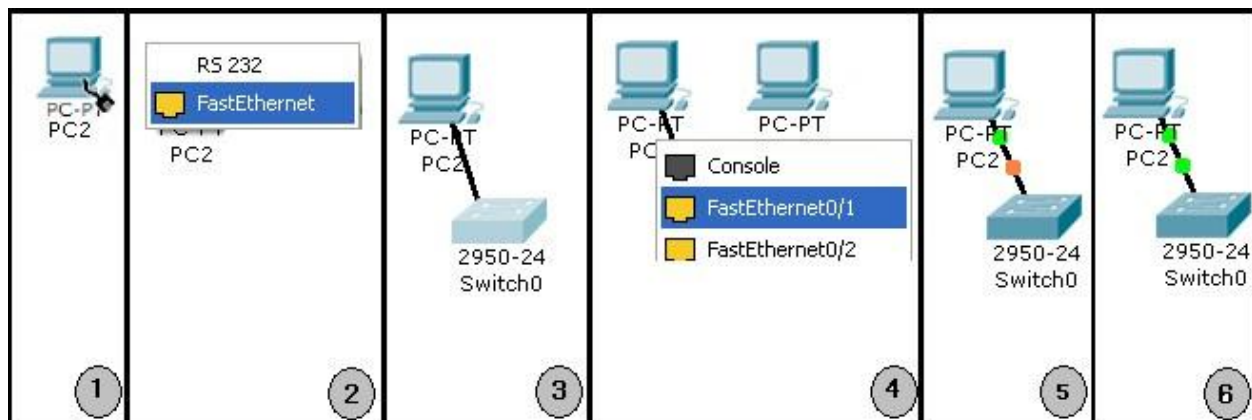


- Connect PC2 to Switch0 by first choosing Connections.
- Click once on the Copper Straight-through cable.
- Perform the following steps to connect PC2 to Switch0:

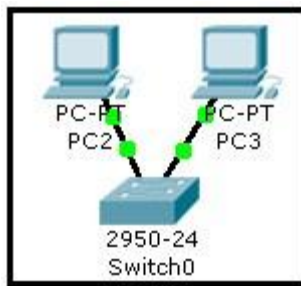
1. Click once on PC2
2. Choose FastEthernet
3. Drag the cursor to Switch0
4. Click once on Switch0 and choose FastEthernet0/1
5. Notice the green link lights on PC2 Ethernet NIC and amber light Switch0

FastEthernet0/1 port. The switch port is temporarily not forwarding frames, while it goes through the stages for the Spanning Tree Protocol (STP) process.

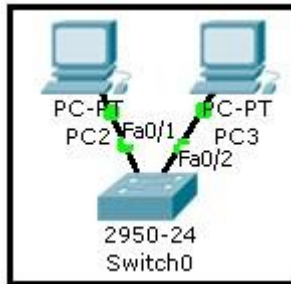
6. After a about 30 seconds the amber light will change to green indicating that the port has entered the forwarding stage. Frames can now be forwarded out the switch port.



- 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.)



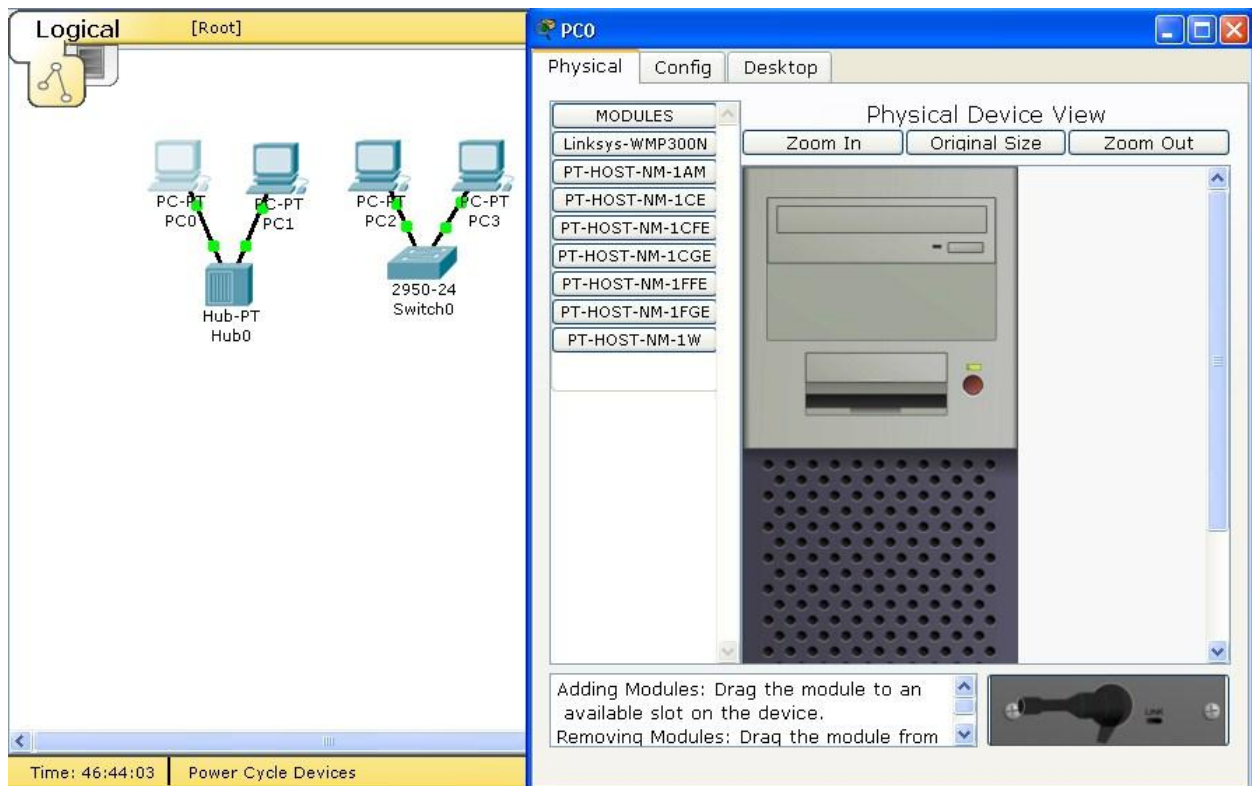
- Move the cursor over the link light to view the port. Fa means FastEthernet, 100 Mbps Ethernet.



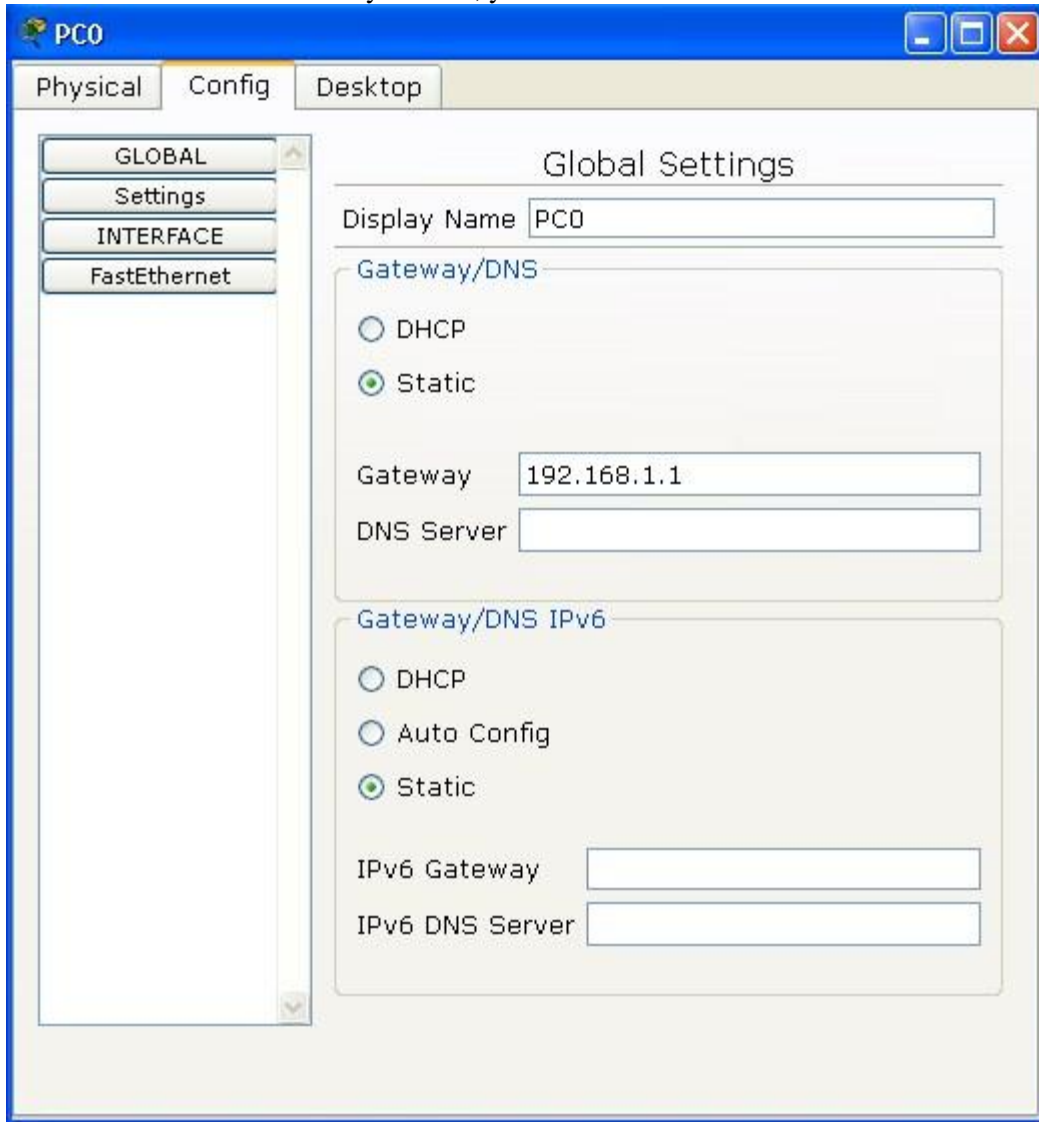
Step 5: Configuring IP Addresses and Subnet Masks on the Hosts

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

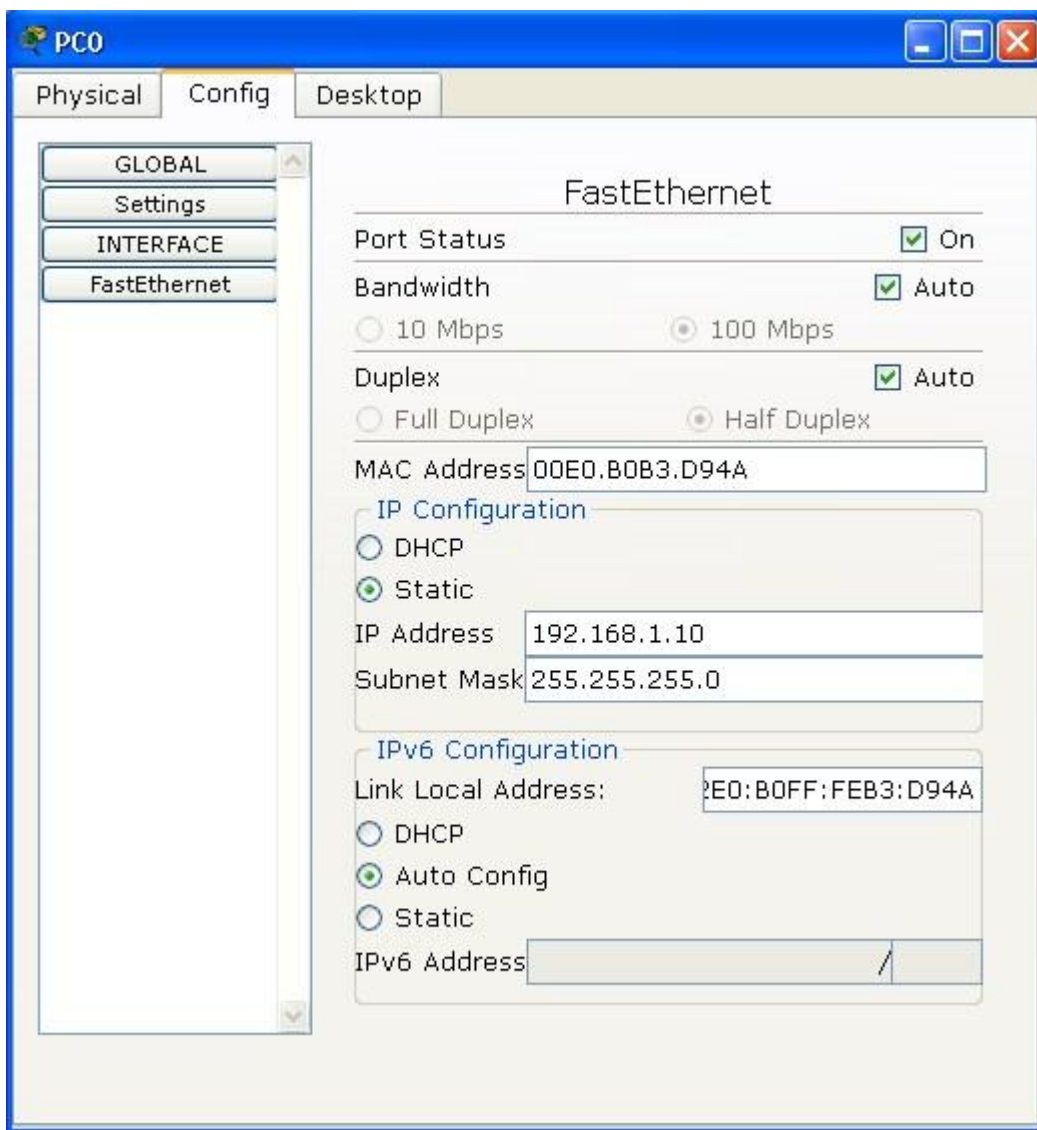
- Click once on PC0.



- 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.



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

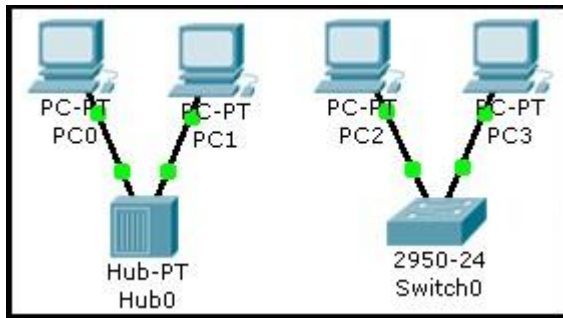


Step 6: Connecting Hub0 to Switch0

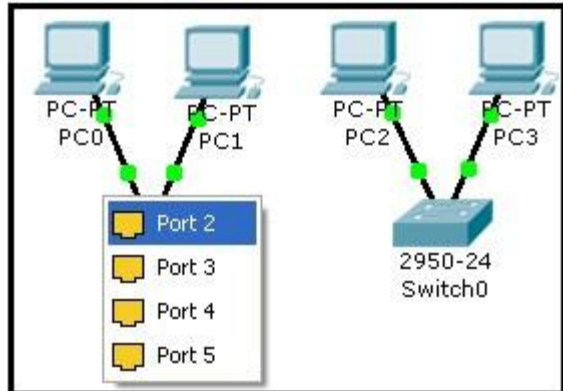
- To connect like-devices, like a Hub and a Switch, we will use a Cross-over cable. Click once the Cross-over Cable from the Connections options.



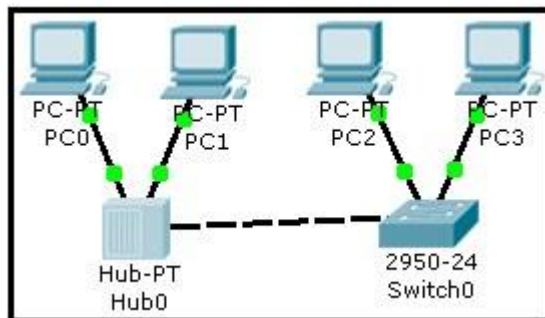
- Move the Connections cursor over Hub0 and click once.



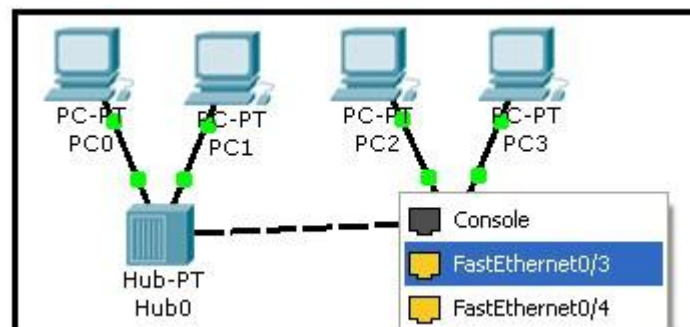
- Select Port2 (actual port does not matter).



- 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.

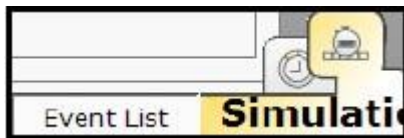
Task 1

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

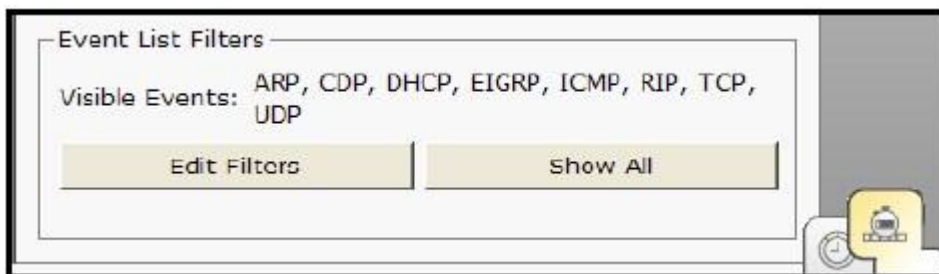
- a. Switch to Simulation Mode by selecting the tab that is partially hidden behind the Real Time tab in the bottom right-hand corner. The tab has the icon of a stopwatch on it.



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.



- b. 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.

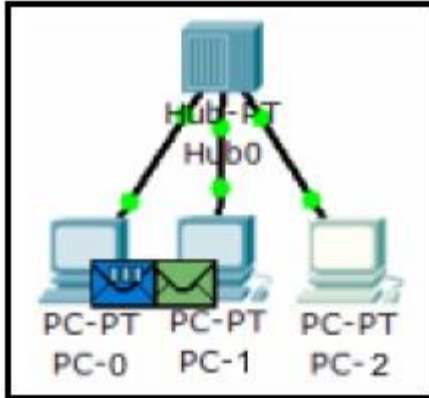


- c. Select a Simple PDU by clicking the closed envelope in the Common Tools Bar on the right.

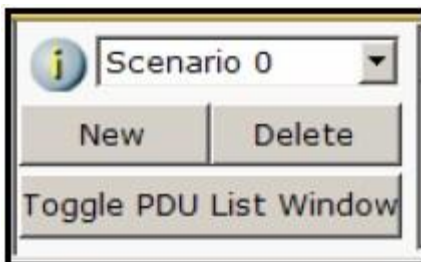


Move to PC0 and click to establish the source. Move to PC1 and click to establish the destination. Notice that two envelopes are now positioned beside PC0. This is referred to as a data traffic scenario. One envelope is an ICMP packet, while the other is an ARP packet. The Event List in the

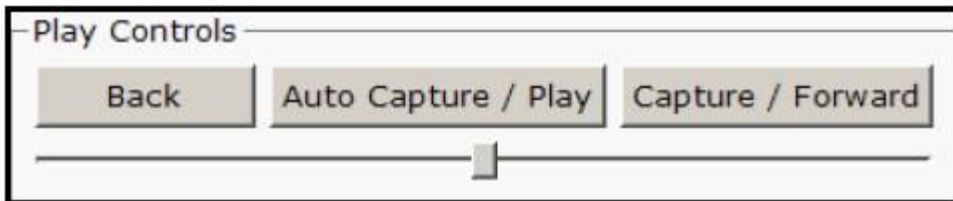
Simulation Panel will identify exactly which envelope represents ICMP and which represents an ARP.



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.



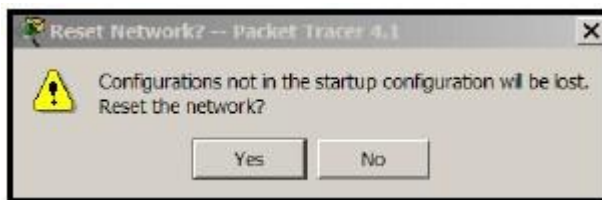
Notice that the ICMP envelope moved forward one device and stopped. The Capture / Forward



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.

- Choose the Auto Capture / Play button and allow the simulation to run completely.
- Click on PC-0 and select the Desktop tab.

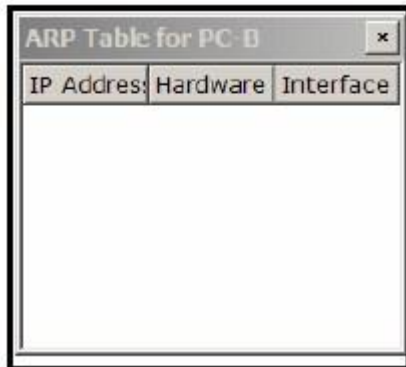


- Select the Command Prompt and type the command `arp -a`.

- 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.



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

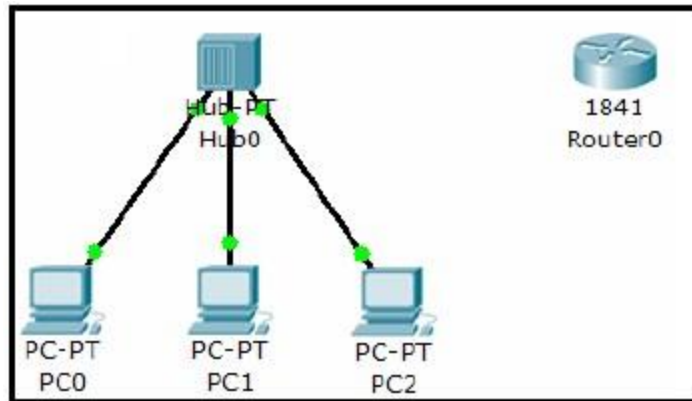
- a) In the Network Component Box, click on the router.



- 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:



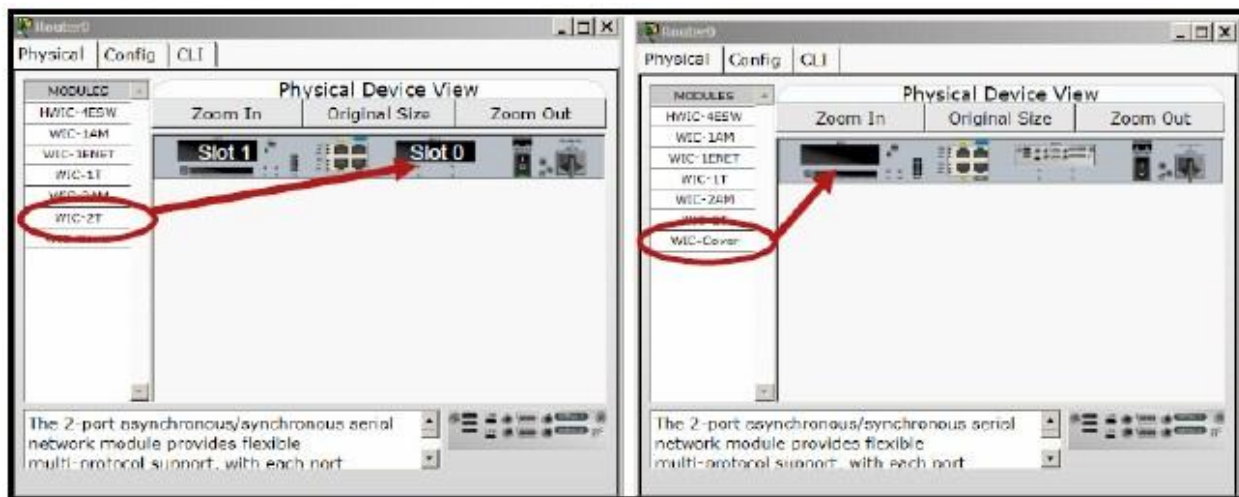
Physical, Config, and CLI (Physical is the default mode).

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.

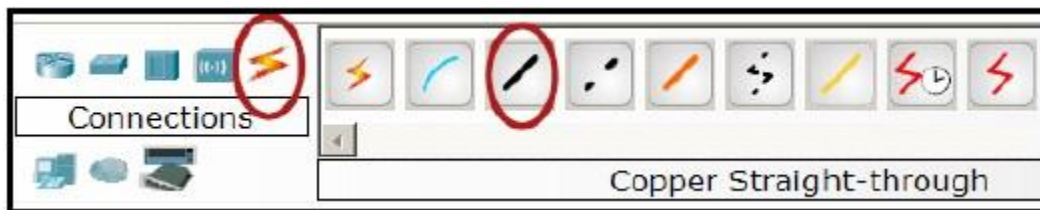
e) In the Physical mode, click on the router power switch to turn the device off.



f) Select the WIC-2T module and drag it to Slot 0 on the router. Then drag a WIC Cover to Slot1.



- g) Power the device back on.
- h) Click on the Network Component Box and select Connections. Then select a Copper Straightthrough 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

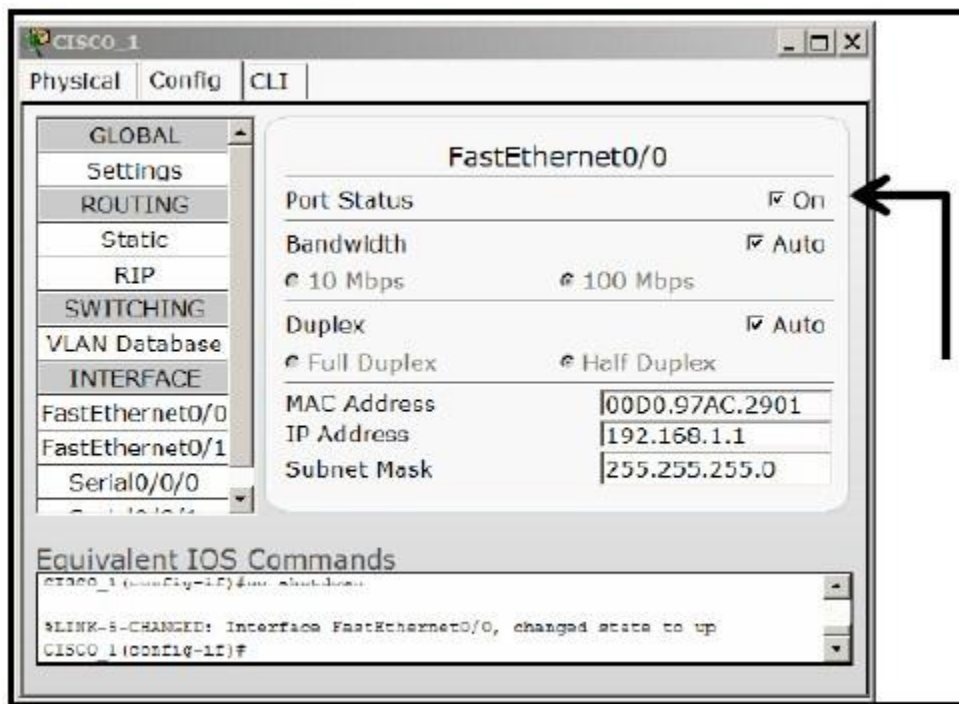
Basic router configuration

- 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, 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.



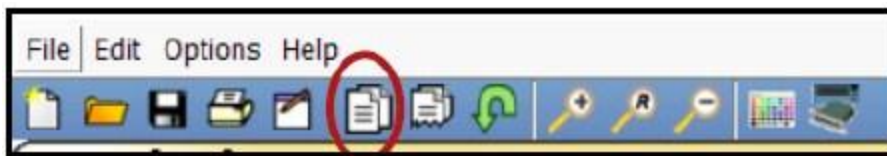
e) Click the Port Status to On to enable the port (no shutdown).

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).

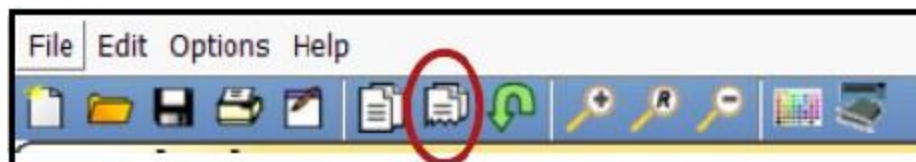
b) In the Main Tool Bar click on the Copy tool.



c) Click on the Paste tool and the copied

device will appear in the

work area.



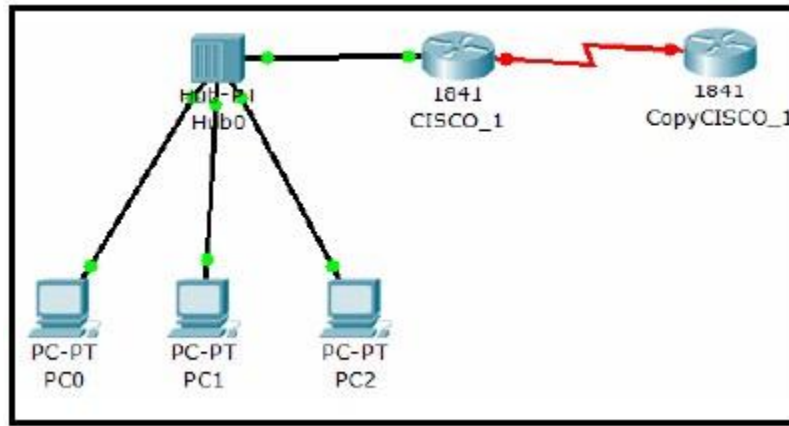
d) Drag the new device to the desired location.

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

- 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.
- Click on the CISCO_2 router and select the Config tab. Then click on RIP and add the network address 192.168.2.0.
- Go to each PC and set the Default Gateway to 192.168.1.1

Task 8

Set the default gateway on the PCs


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

Task 10 Save the Packet Tracer file

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

*** *Solve associated parts in the problem sheet* ***
