Lab # 03 (a): Introduction to IP Addressing (Classful addressing)

IP address:

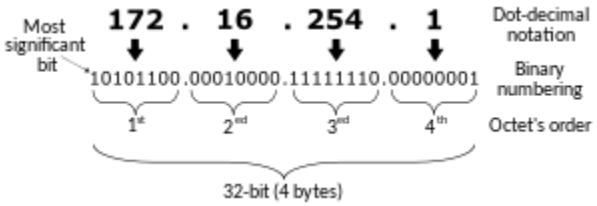
IP address is an address having information about how to reach a specific host, especially outside the LAN. It is a 32-bit address that identifies a connection to the Internet. The IP addresses are universally unique. The address space of IPv4 is 232 or 4,294,967,296.

IP address notation:

Generally, there are two notations in which IP address is written, dotted decimal notation and binary notation.

Typically, it is written in decimal digits, formatted as four 8-bit fields separated by periods. Each 8-bit field represents a byte of the IPv4 address, each ranging from 0 to 255. This form of representing the bytes of an IPv4 address is often referred to as the **dotted-decimal format.**

In **binary notation** each decimal number is represented by its 8-bit binary. The example of each notation is given below.



Classful addressing:

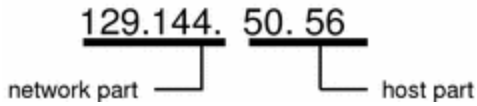
Classful addressing is a concept that divides the available address space of IPv4 into five classes namely A, B, C, D & E.

Each of these classes has a valid range of IP addresses. Classes D and E are reserved for multicast and experimental purposes respectively. The order of bits in the first octet determines the classes of IP address.

IPv4 address is divided into two parts:

Network ID: This part specifies the unique number assigned to your network. It also identifies the class of network assigned.

Host ID: This is the part of the IPv4 address that you assign to each host. It uniquely identifies this machine on your network. Note that for each host on your network, the network part of the address will be the same, but the host part must be different.



The class of IP address is used to determine the bits used for network ID and host ID and the number of total networks and hosts possible in that class.

Class A:

IP address belonging to class A are assigned to the networks that contain a large number of hosts.

The network ID is 8 bits long.

The host ID is 24 bits long.

The highest order bit of the first octet in class A is always set to 0. The remaining 7 bits in first octet are used to determine network ID. The 24 bits of host ID are used to determine the host in any network. The default subnet mask for class A is 255.0.0.0.

Class B:

IP address belonging to class B are assigned to the networks that ranges from medium-sized to large-sized networks.

The network ID is 16 bits long.

The host ID is 16 bits long.

The higher order bits of the first octet of IP addresses of class B are always set to 10. The remaining 14 bits are used to determine network ID. The 16 bits of host ID is used to determine the host in any network. The default sub-net mask for class B is 255.255.0.0.

Class C:

IP address belonging to class C are assigned to small-sized networks.

The network ID is 24 bits long.

The host ID is 8 bits long.

The higher order bits of the first octet of IP addresses of class C are always set to 110. The remaining 21 bits are used to determine network ID. The 8 bits of host ID is used to determine the host in any network. The default sub-net mask for class C is 255.255.255.0.

Class D:

IP address belonging to class D are reserved for multi-casting. The higher order bits of the first octet of IP addresses belonging to class D are always set to 1110. The remaining bits are for the address that interested hosts recognize. Class D does not possess any sub-net mask.

Class E:

IP addresses belonging to class E are reserved for experimental and research purposes. This class doesn't have any sub-net mask. The higher order bits of first octet of class E are always set to 1111.

Summary of classful addressing

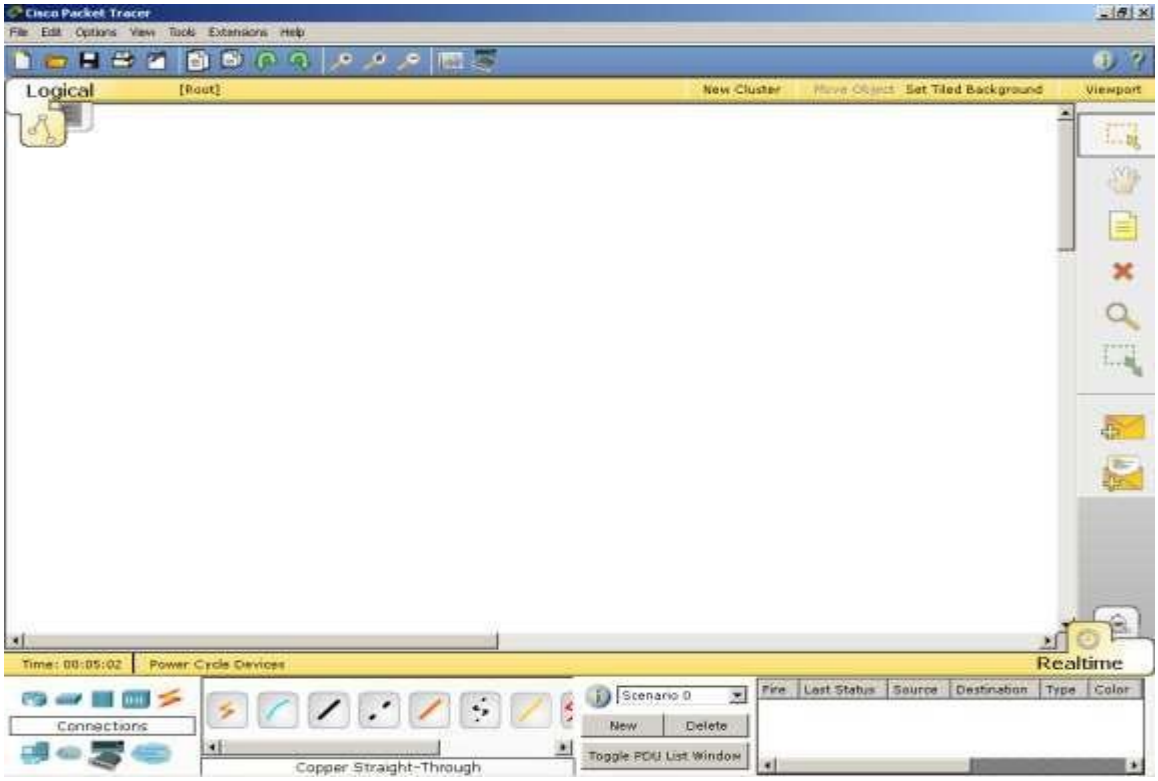
CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

Lab # 3 (b): Basic Network Configuration (connecting 2 nodes directly) using Packet Tracer

Introduction

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. The purpose of this lab is to become familiar with the Packet Tracer interface. Learn how to use existing topologies and build your own. This activity will provide an opportunity to explore the standard lab setup using Packet Tracer simulator. Packet Tracer has two file formats it can create: .pkt files (network simulation model files) and .pka files (activity files for practice). When you create your own networks in Packet Tracer or modify existing files from your instructor or your peers, you will often use the .pkt file format. When you launched this activity from the curriculum, these instructions appeared. They are the result of the .pka, Packet Tracer activity file format. At the bottom of these instructions are two buttons: Check Results (which gives you feedback on how much of the activity you have completed) and Reset Activity (which starts the activity over if you want to clear your work or gain more practice).

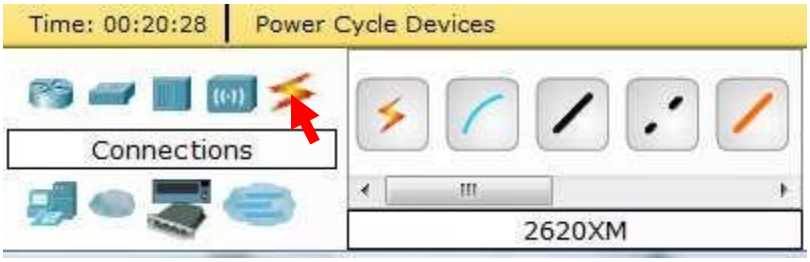
Step 1: Start Packet Tracer

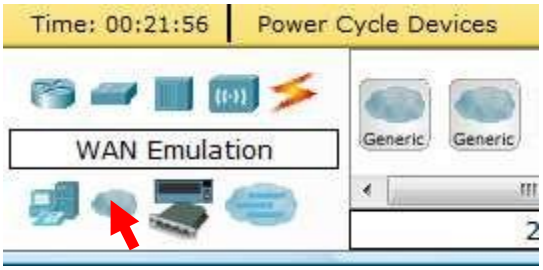


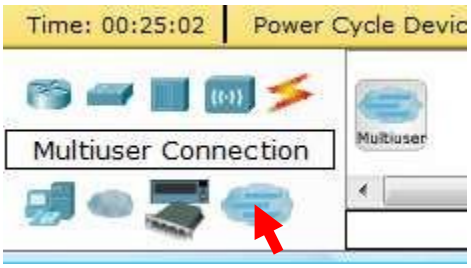
Step 2: Choosing Devices and Connections

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 and Connections.

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

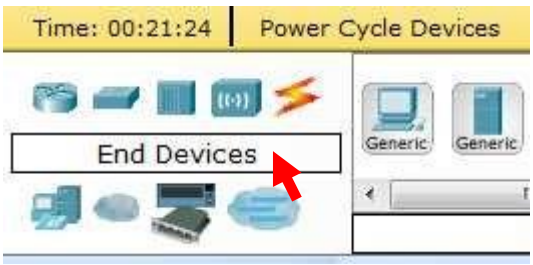






Step 3: Building the Topology – Adding Hosts

Single click on the End Devices.

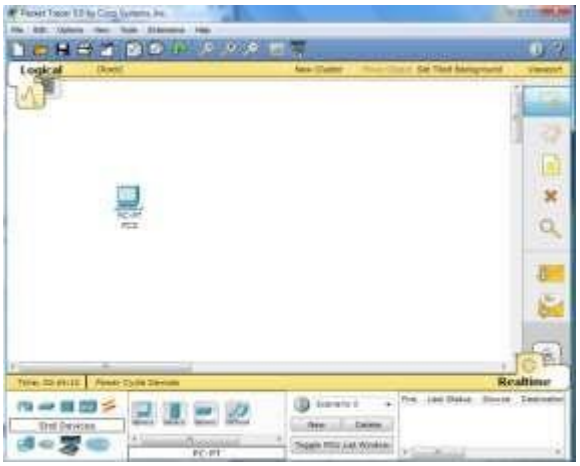


Single click on the Generic host.

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

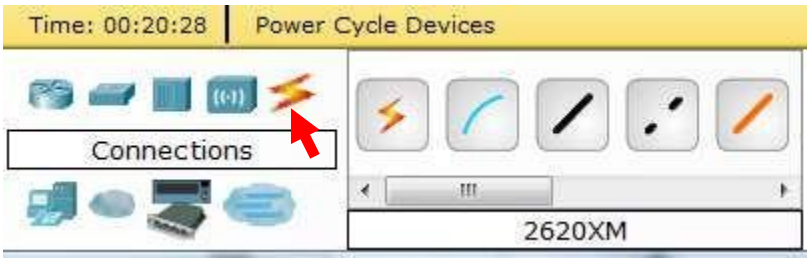
+

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



Add another node by following the same steps.

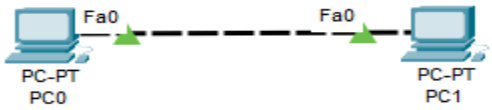
Connect PC0 to PC1:

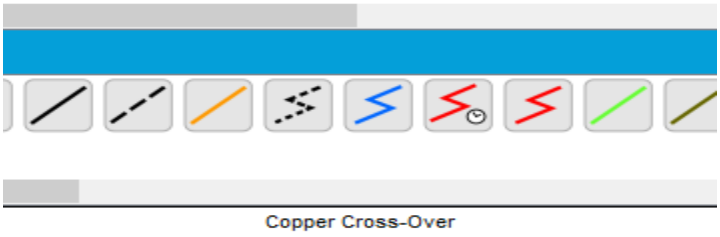


Click once on the copper cross over cable

Perform the following steps to connect PC0 to PC1:

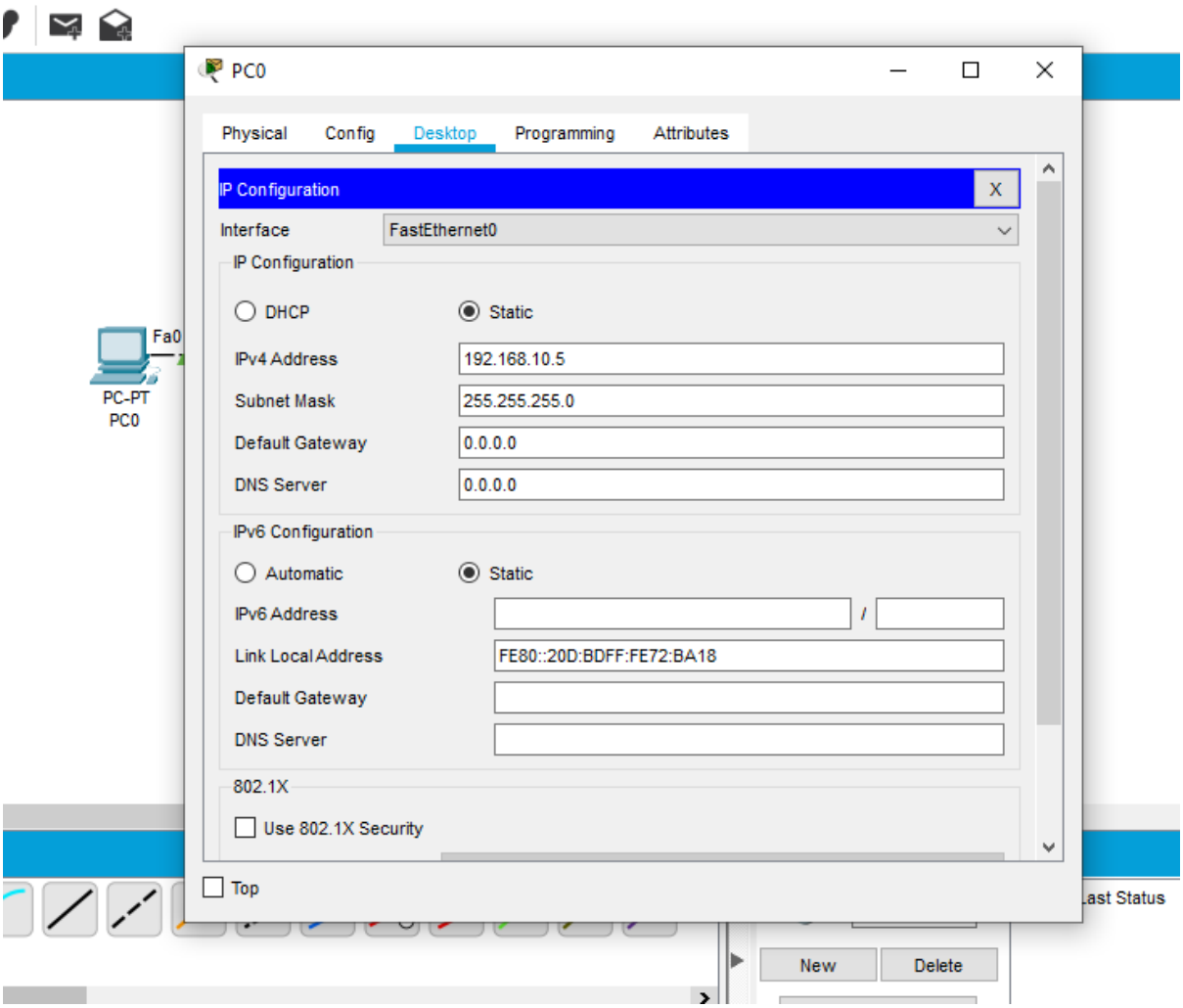
1. Click once on PC0
2. Choose FastEthernet
3. Drag the cursor to PC1
4. Click once on PC1
5. Choose FastEthernet





Step 4: Configuring IP Addresses and Subnet Masks on the Hosts

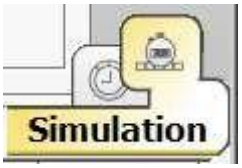
Before we can communicate between the hosts, we need to configure IP Addresses and Subnet Masks on the devices. Click once on PC0. Choose the desktop tab and click on IP configuration. It is also here where you would enter a Gateway IP Address, also known as the default gateway and the DNS Server IP Address. We will discuss this later.



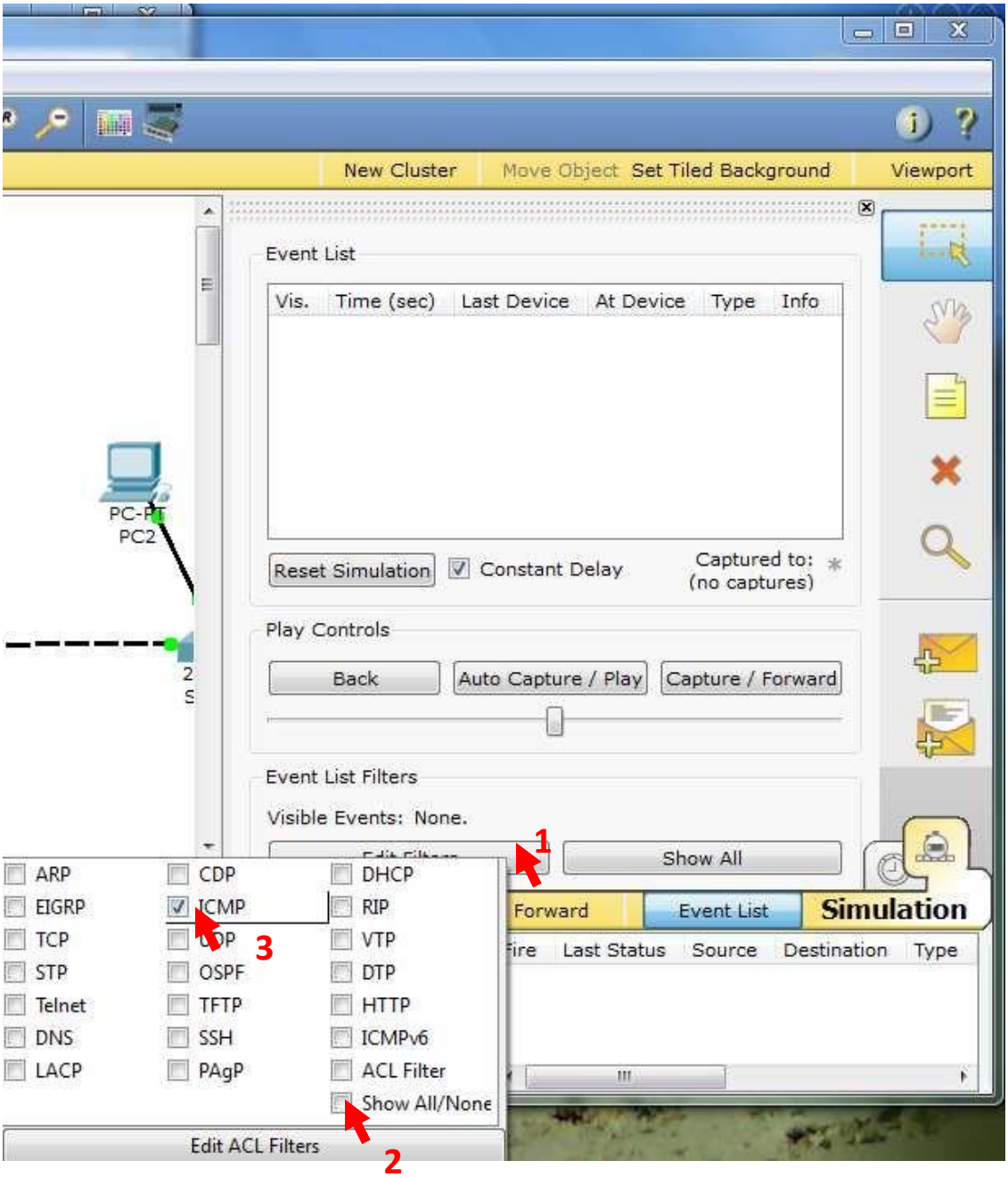
For now, we will add IP address and subnet mask. We will use class C IP address of network 192.168.10.0. Add the IP address as given in the above image and the subnet mask. Repeat the same for PC1 using different IP address from same network. Use 192.168.10.6 for practice.

Step 5: Verifying Connectivity in Simulation Mode

Be sure you are in Simulation mode.



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



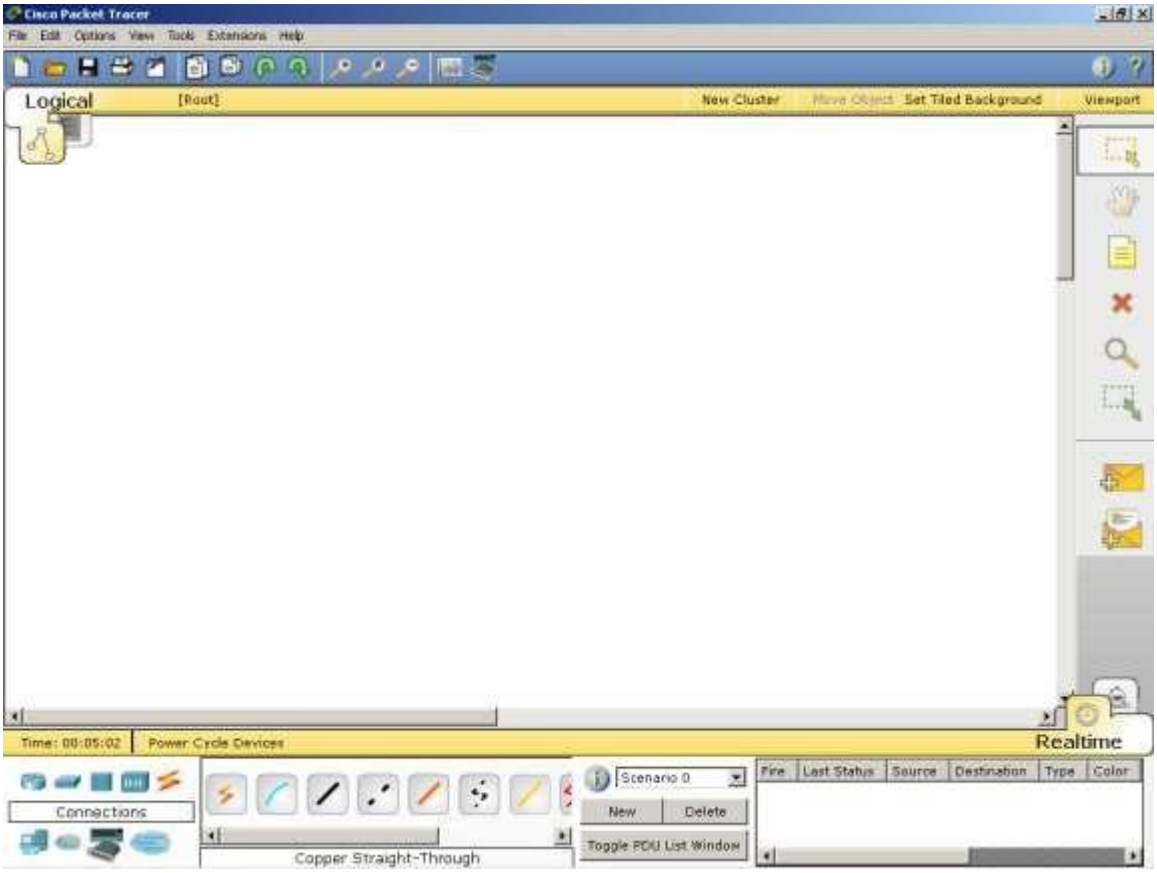
Select the Add Simple PDU tool used to ping devices.

Click once on PC0, then once on PC1. Continue clicking Capture/Forward button until the ICMP ping is completed. You should see the ICMP messages move. The PDU Last Status should show as Successful.

The configuration is complete.

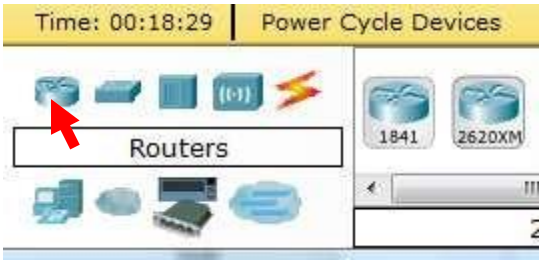
Lab # 3 (c): Basic Network Configuration (connecting multiple end devices through switch) using Packet Tracer

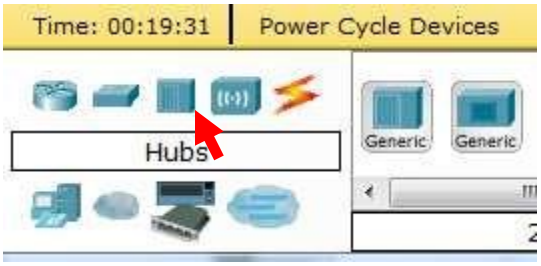
Topology Step 1: Start Packet Tracer

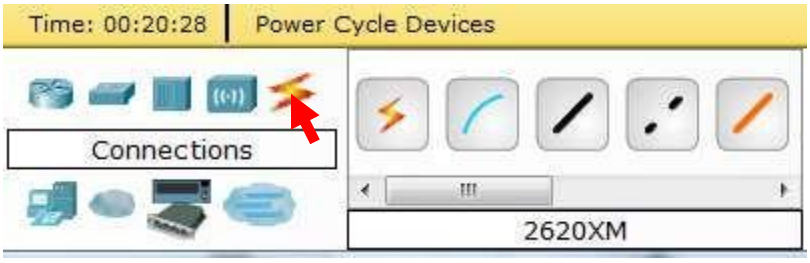


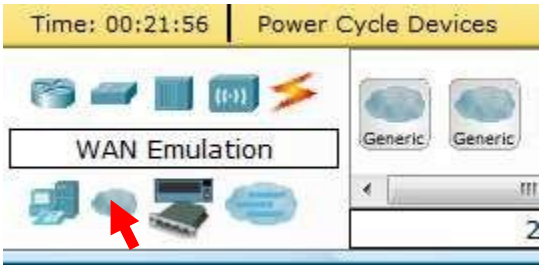
Step 2: Choosing Devices and Connections

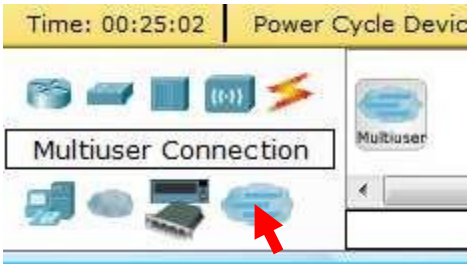
We will begin building our network topology by selecting devices and the media in which to connect them. Several types of devices and network connections can be used. For this lab we will keep it simple by using End Devices, Switches, and Connections. Single click on each group of devices and connections to display the various choices. The devices you see may differ slightly.











Step 3: Building the Topology – Adding Hosts

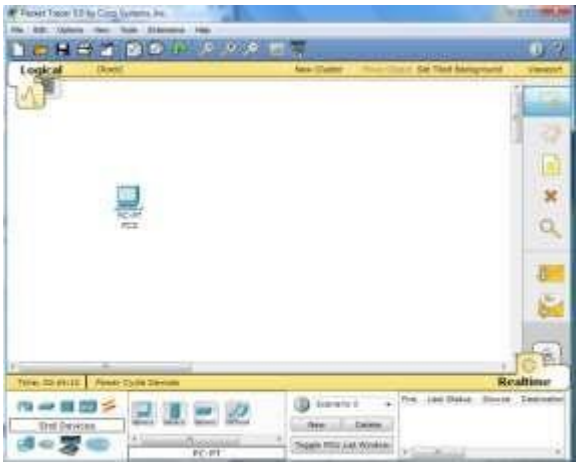
Single click on the End Devices.

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.



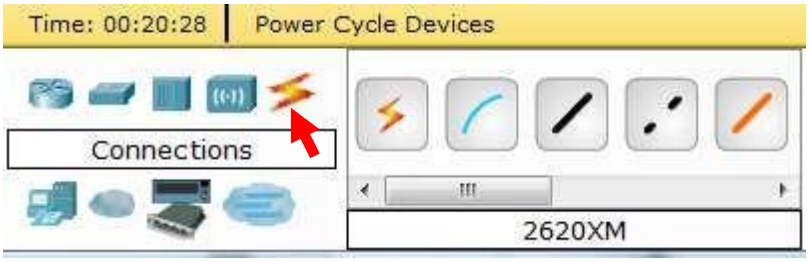
Add three more hosts.

Building the Topology – Connecting the Hosts to Switch.

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 switch by first choosing Connections.

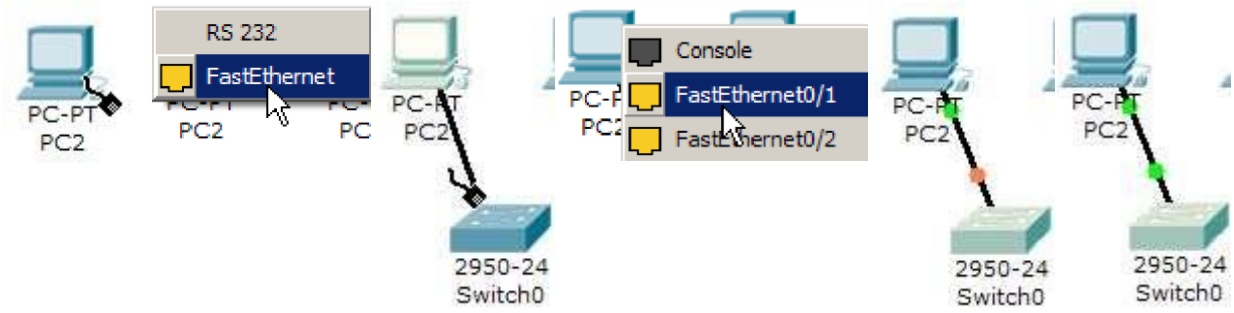


Click once on the Copper Straight-through cable.

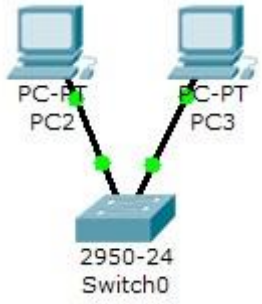
Perform the following steps to connect PC2 to Switch0:

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 forward out the switch port.

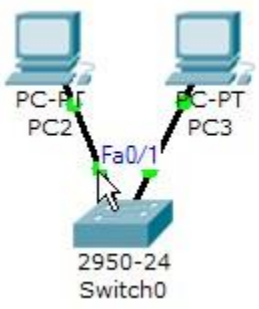
1 2 3 4 5 6



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.)



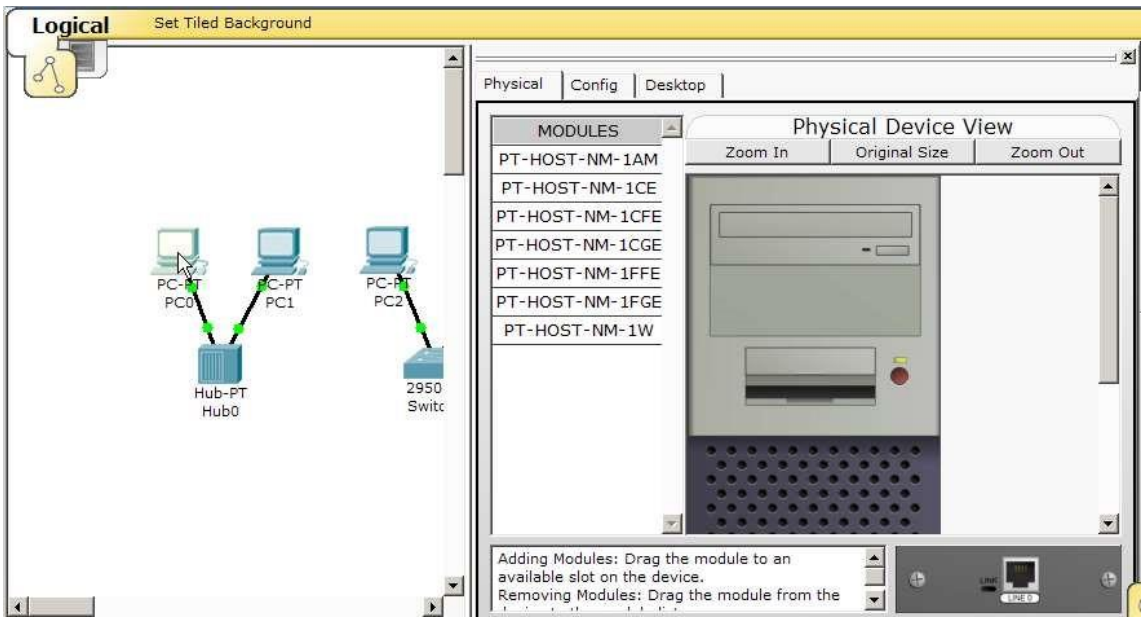
Move the cursor over the link light to view the port number. Fa means FastEthernet, 100 Mbps Ethernet.



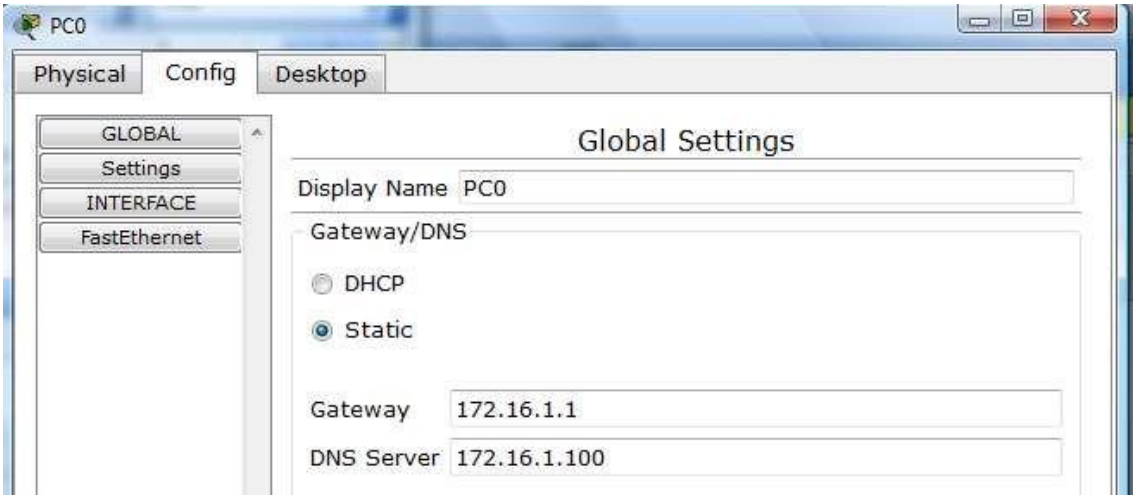
Repeat same steps to connect other PCs with switch.

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

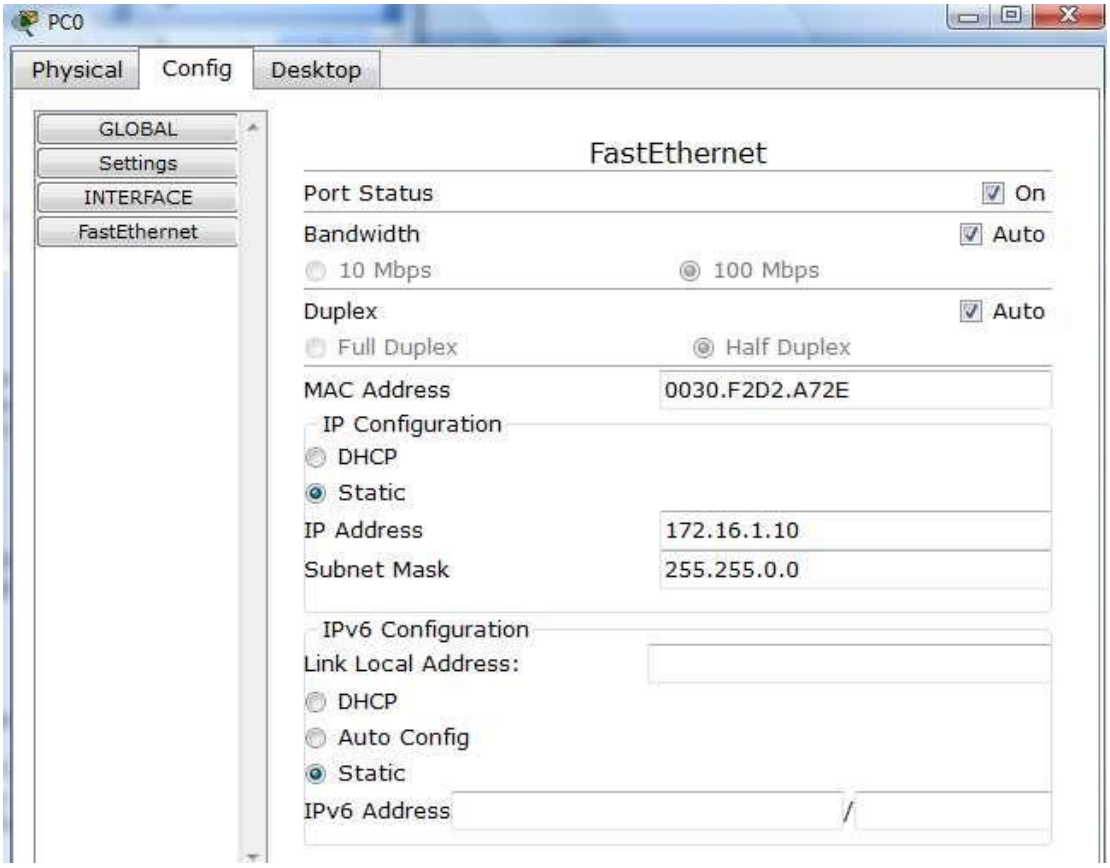
Before we can communicate between the hosts, we need to configure IP Addresses and Subnet Masks on the devices. Click once on PC0.



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 FastEthernet. 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.



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

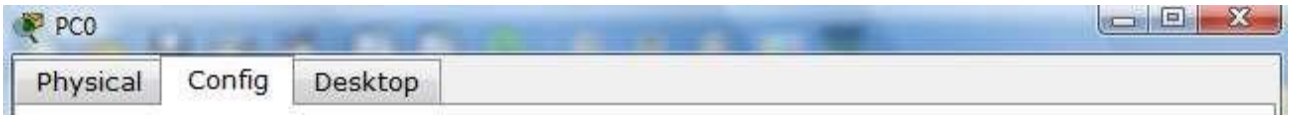
If the host is connected to a hub or switch port which can do 100 Mbps, then the Ethernet NIC on the host will choose 100 Mbps (Fast Ethernet). Otherwise, if the hub or switch port can only do 10 Mbps, then the Ethernet NIC on the host will choose 10 Mbps (Ethernet).

Duplex - Auto

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.

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

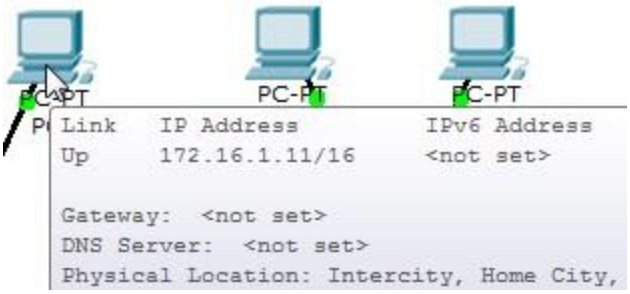


Repeat these steps for the other hosts. Use the information below for IP Addresses and Subnet Masks.

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

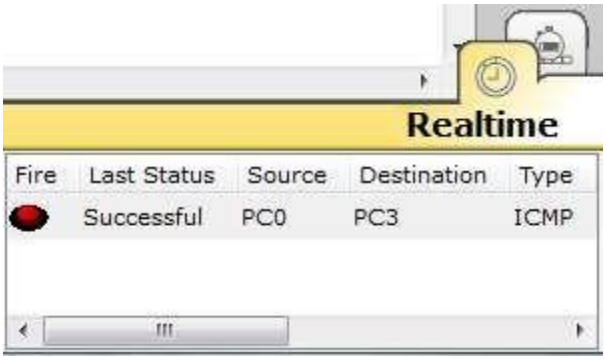
To delete a device or link, choose the Delete tool and click on the item you wish to delete.

Step 7: verify connectivity in Realtime mode

Be sure you are in Realtime mode.

Select the Add Simple PDU tool used to ping devices.

Click once on PC0, then once on PC3.



Change the IP address of PC3 to 172.16.2.13. Perform a ping from PC0 to PC3. What is the ping result?

_____

Return the IP address of PC3 to 172.16.1.13. Change the IP address of PC2 to 172.17.1.12. Perform a ping from PC0 to PC2. What is the ping result?

_____

Resetting the Network

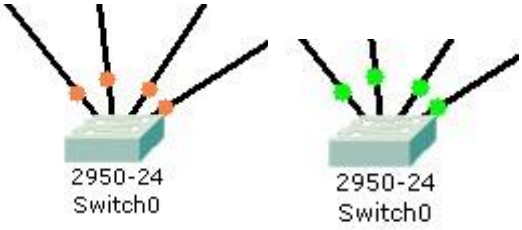
At this point we will want to reset the network, whenever you want to reset the network and begin the simulation again, perform the following tasks:

Click Delete in the PDU area.

Now, Power Cycle Devices and confirm the action.

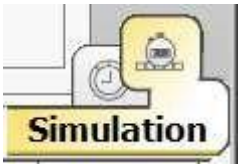
Waiting for Spanning Tree Protocol (STP)

Note: Because Packet Tracer also simulates the Spanning Tree Protocol, 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.

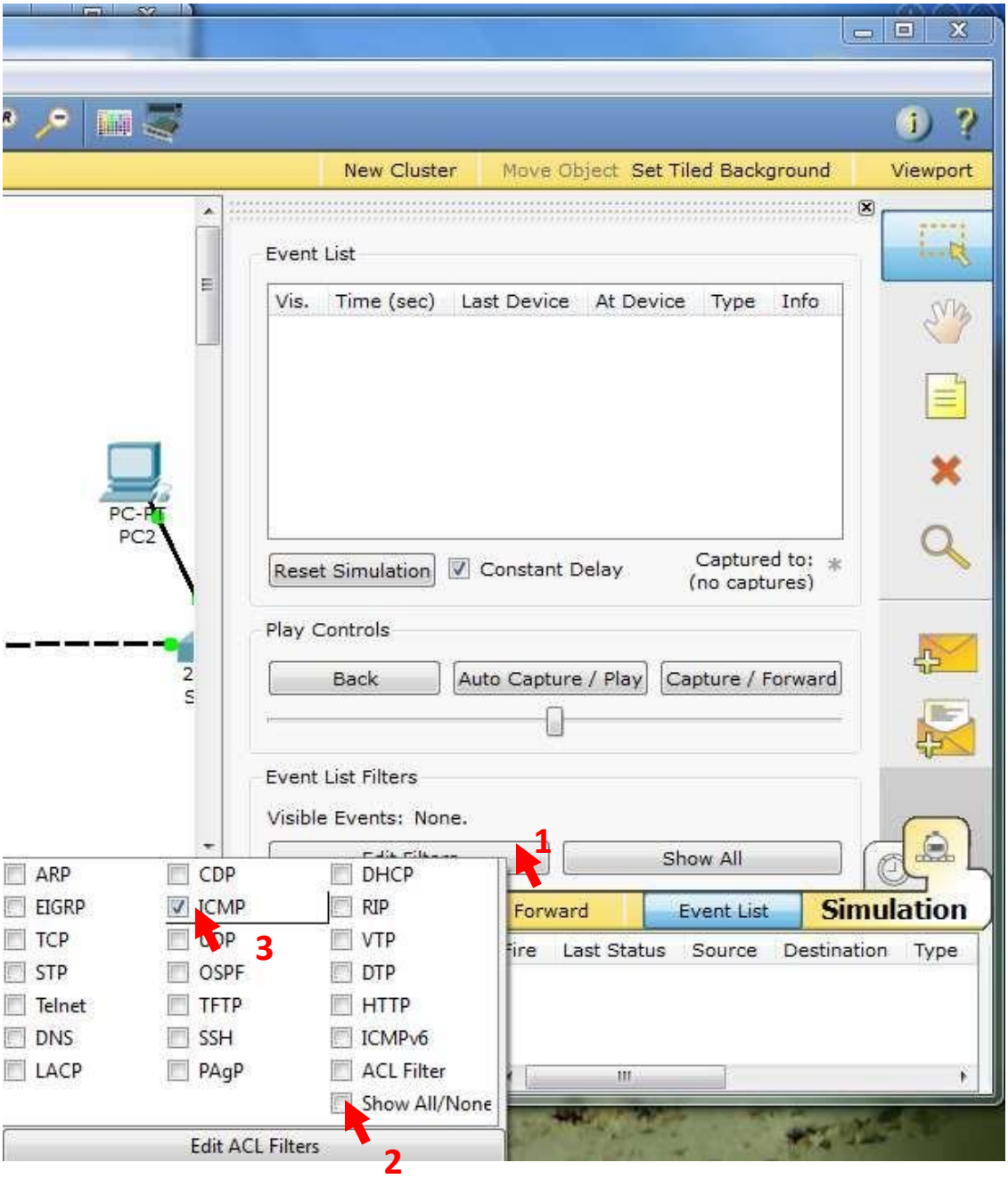


Step 8: Verifying Connectivity in Simulation Mode

Be sure you are in Simulation mode.



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



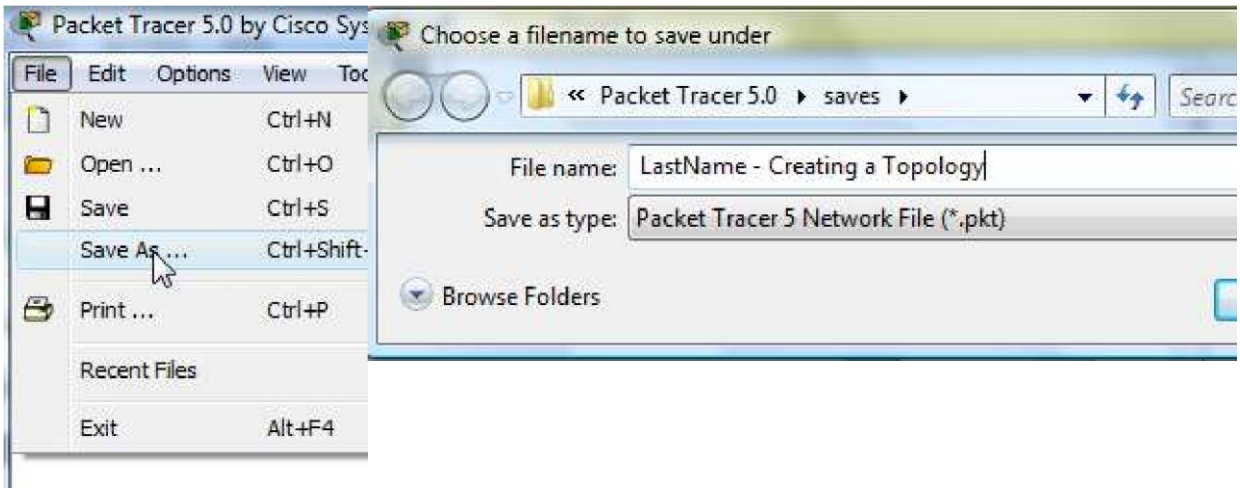
Select the Add Simple PDU tool used to ping devices.

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. 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