LAB 2

Computer Netowrks

Objective

In today's lab we will explore the Packet tracer 4.11 to design a basic topology. Also we would see how we can build the topology using hub and switches. By the end of this lab, you should be familiar with Packet tracer interface and able to design a topology.

Submission Requirements

You are expected to complete the assigned tasks within the lab session and show them to the lab engineer/instructor. Some of these tasks are for practice purposes only while others (marked as '*Exercise'* or '*Question*') have to be answered in the form of a lab report that you need to prepare. Following guidelines will be helpful to you in carrying out the tasks and preparing the lab report.

Guidelines

- In the exercises, when you are asked to display an image, you have to put the image displayed in your project report. You may either save the image as 'jpeg' (File->Save As) or add it to the report or use the 'Print Screen' command on your keyboard to get a snapshot of the displayed image. This point will become clear to you once you actually carry out the assigned tasks**.**

- Name your reports using the following convention:
  - ***Lab#_Rank_YourFullName***

  - '#' replaces the lab number
  - '*Rank'* replaces Maj/Capt/TC/NC/PC
  - '*YourFullName*' replaces your complete name.
- You need to submit the report even if you have demonstrated the exercises to the lab engineer/instructor or shown them the lab report during the lab session.

Tasks for Today

Introduction to Packet Tracer

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

Purpose: The purpose of this lab is to become familiar with the Packet Tracer interface. Learn how to use existing topologies and build your own.

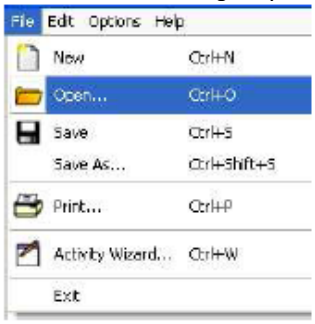
Requisite knowledge: This lab assumes some understanding of the Ethernet protocol. At this point we have not discussed other protocols, but will use Packet Tracer in later labs to discuss those as well.

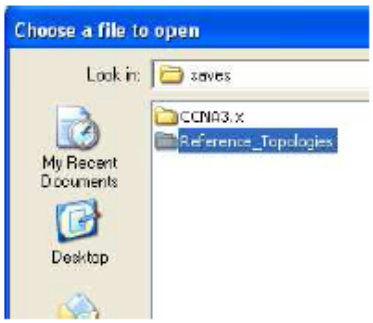
Version: This lab is based on Packet Tracer 4.11

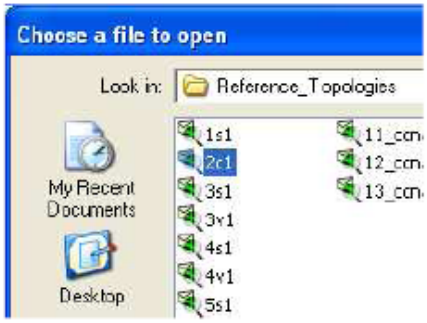
Introduction to the Packet Tracer Interface using a Hub Topology

Step 1: Start Packet Tracer and Entering Simulation Mode
Launch Packet Tracer program from the program list.

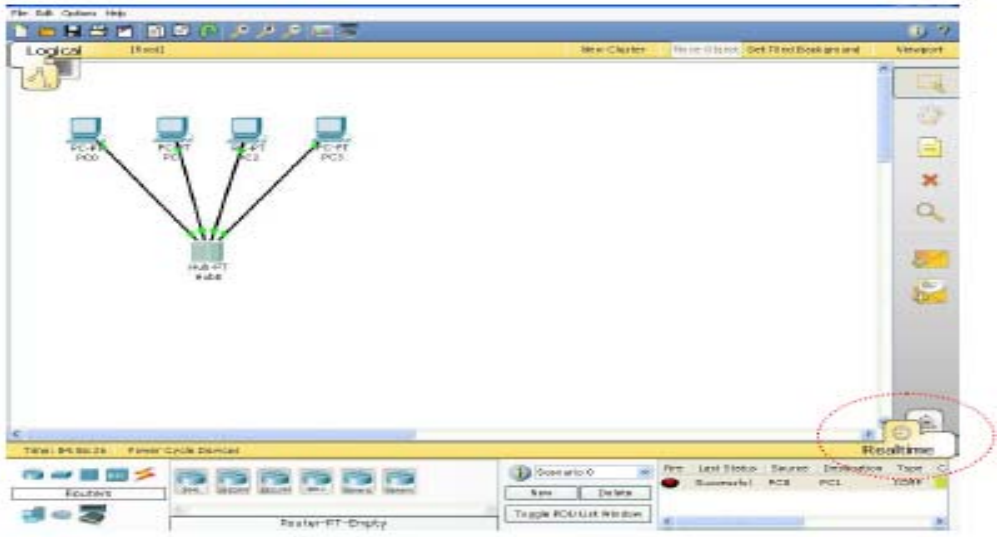
Step 2: Open an existing topology
Perform the following steps to open the **2c1** topology.







By default, the topology opens in **Realtime** mode.

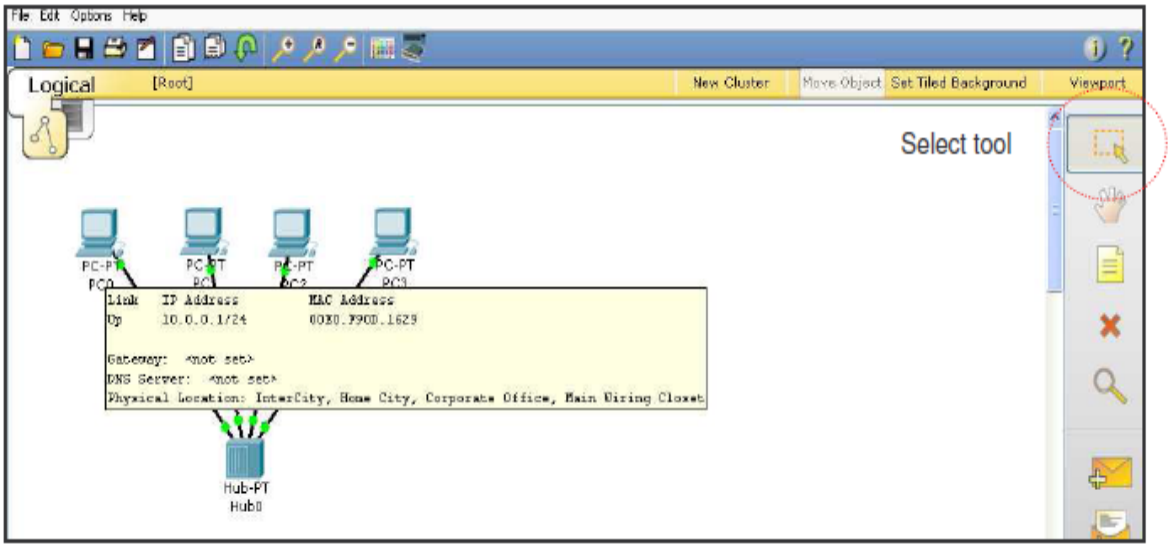


We will examine the difference between **Realtime** and **Simulation** modes in a moment.

Help can be obtained by using the Help menu. Both online help one each topic and tutorials are available. Please take advantage of these facilities.

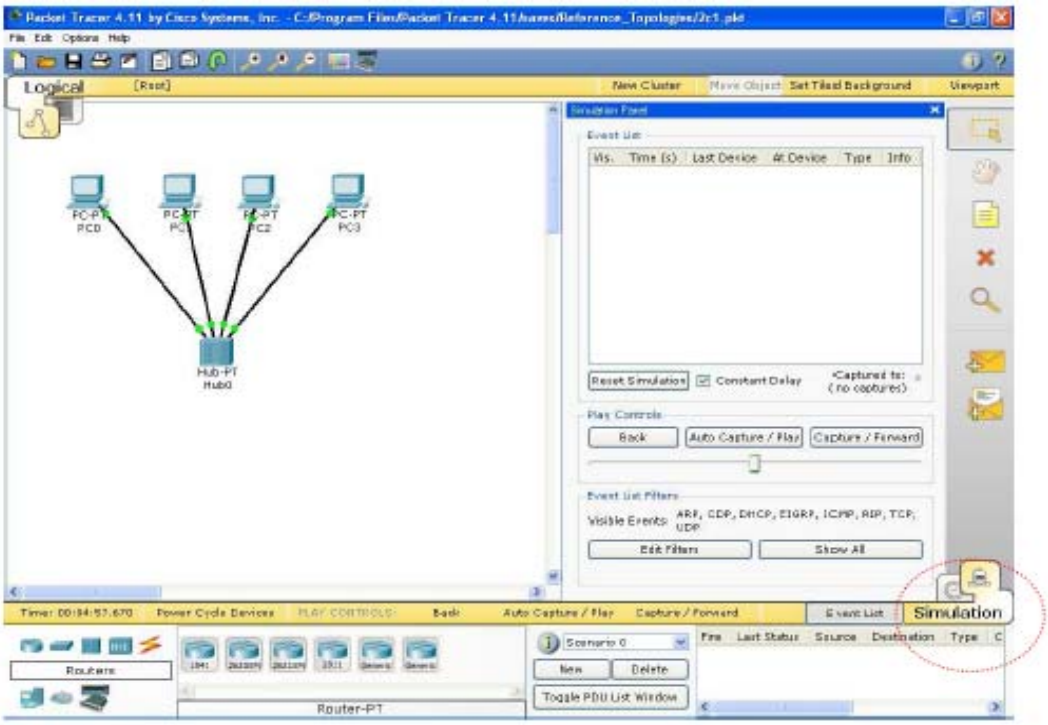
To view the IP address, subnet mask, default gateway, and MAC address of a host, move the cursor over that computer.

Be sure the **Select** box is checked at the top of the tool box.
Viewing PC0 information using the **Select** tool:



Once the file is opened, click the **Simulation** icon, to enter simulation mode. Simulation mode allows you to view the sequence of events associated with the communications between two or more devices.

Realtime mode performs the operation with all of the sequence of events happening at “real time”.



Step 3: PC0 pinging PC1

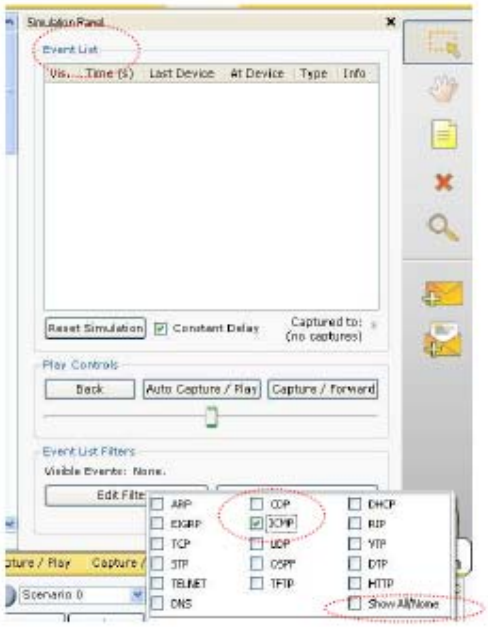
For those not familiar with ping: We will examine pings and the ICMP protocol in much more detail later. The ping program generates an IP packet with an encapsulated ICMP Echo Request message. It is a tool used to test basic layer 2 and layer 3 communications between two devices.

When the user issues the ping command, most operating systems send multiple (four or five) ICMP Echo messages. When the destination device receives the ping, Echo Request, it issues an Echo Reply.

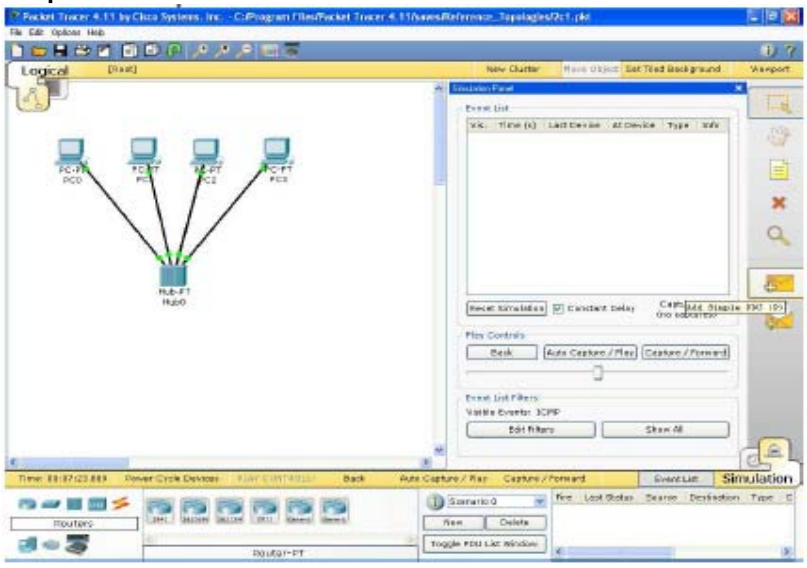
Command issued from PC0: ping 10.0.0.2

Packet Tracer allows us to either issue the command from the command prompt or to use the Add Simple PDU tool. We will look at both ways to do this.

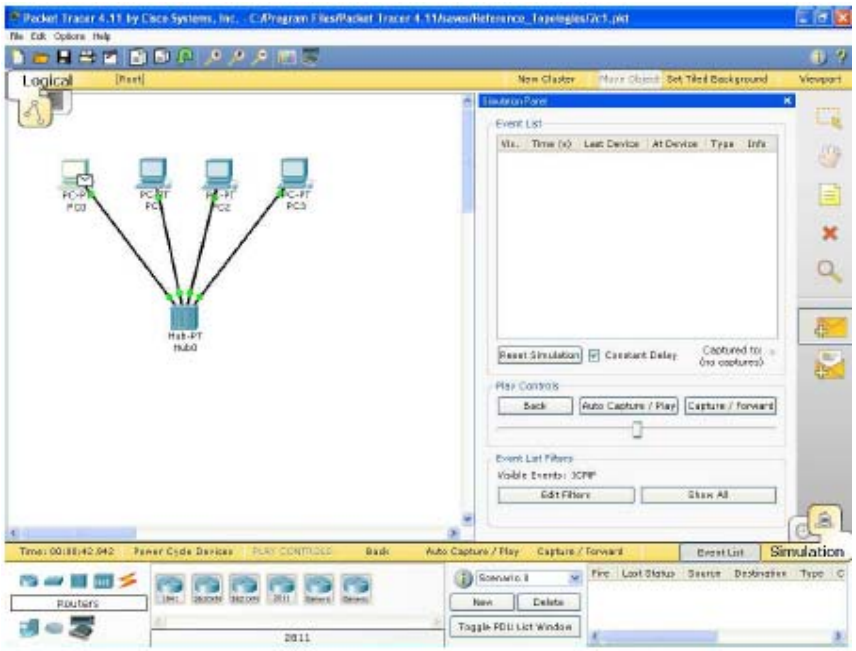
In order to view only the “pings”, in the **Event List Filter**, click on **SHOW ALL/NONE** to clear all protocols, and then click on **ICMP** to select only that protocol.



Using the Simple PDU Tool One method for pinging a device from another device is to use the **Simple PDU tool**. This tool performs the ping without having to issue the ping command. Choose the **Add Simple PDU** tool from the tool box:

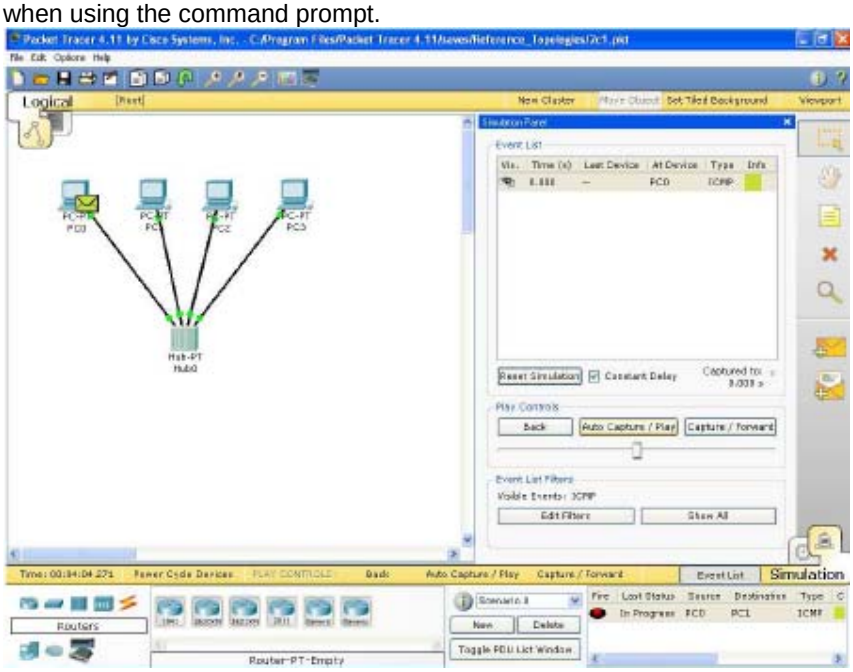


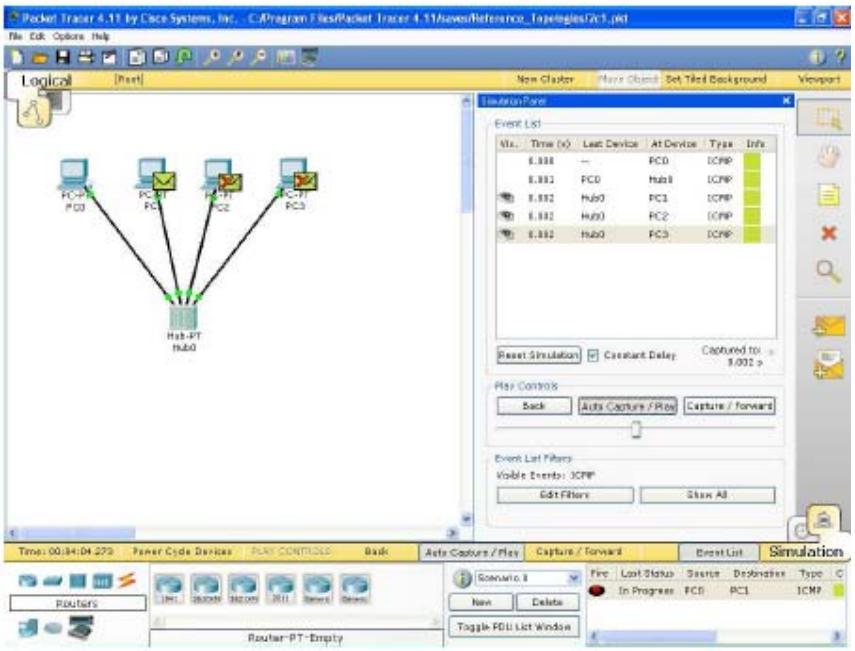
Click once on **PC0**, the device issuing the ping (ICMP Echo Request) and then click once on **PC1** (the destination of the ICMP Echo Request).

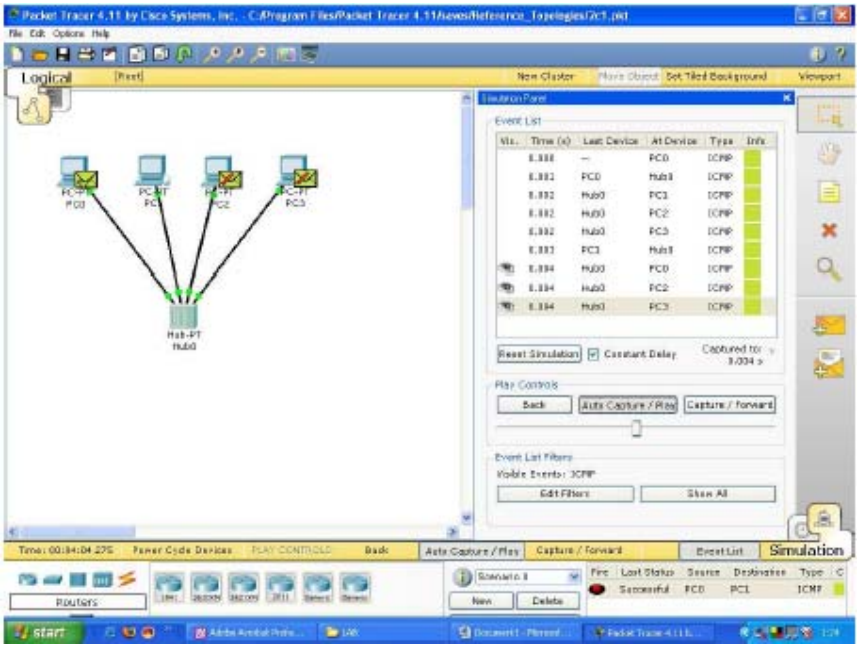


By clicking on the **Auto Capture/Play** button, this will capture all events in interval of 0.001 second. For example, the first event is the building of the ICMP packet and encapsulating it in an Ethernet frame. The next event will send this Ethernet frame from the Ethernet NIC in PC0 to the Hub.

Notice that the hub floods all of the frames out all ports except the port incoming port.
Normally, before the ICMP Echo Request, ping, is sent out by PC0, an ARP Request might first be sent. We will discuss this later, but we disabled the display of ARP in the Event List earlier.
Note: Using this tool, only a single ping, ICMP Echo Request is sent by PC0, instead of the four pings when using the command prompt.

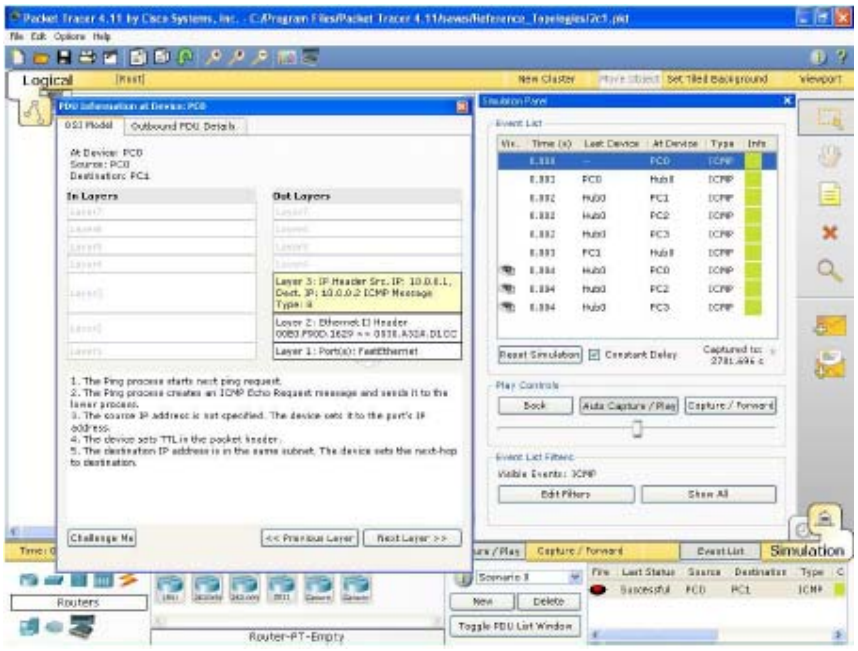




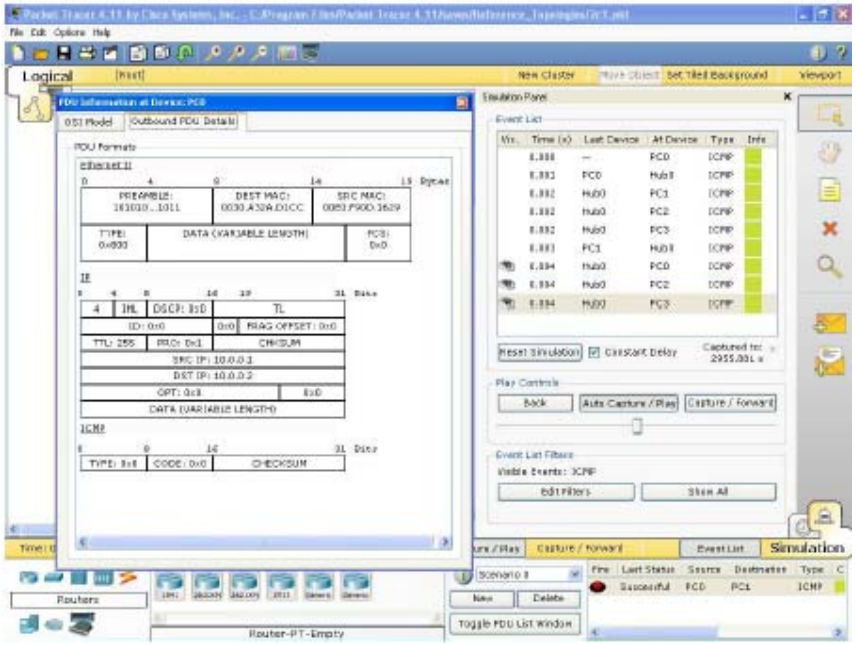


Step 4: Viewing the frame (Protocol Analyzer)
To examine the actual protocols being sent, click on the colored **Info** box in the **Event List**. The Event List shows where this Ethernet Frame is currently, "At Device", the previous devices, "Last Device", and the type of information encapsulated in the Ethernet Frame, "Info". Single click on the *second* event's Info box to view the Ethernet frame with the encapsulated IP Packet and the encapsulated ICMP message **"At Device" PC0**.

The PDU (Protocol Data Unit) is displayed in two different formats, **OSI Model** and **Outbound PDU Details**. View them both, paying particular attention to the Layer 2 Ethernet frame. We will discuss IP and ICMP later. If you only see the IP packet and the ICMP message, and do not see the **Ethernet II** frame, click on the next ICMP Info box. This happened because we are looking at the IP packet before it got encapsulated into an Ethernet frame.



The default is the **OSI Model** view with a brief description with what is occurring with this packet. Click on the **Outbound PDU Details** tab to see the protocol details including the layer 2 Ethernet frame, the layer 3 IP packet and ICMP message.



Exercise 1:

Build two topologies separately having four PC i.e. PC1, PC2, PC3 and PC4 connected to central location (switch and hub). Send 5, 10, 15, 20 and 25 packet from PC1 to PC4 using **ping** command in each topology.

OUTPUTS: Draw the graph showing the performance of both topologies between no packet and total time taken in each session.