## Lab 1: 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 7.0

### Organization of Packet Tracer

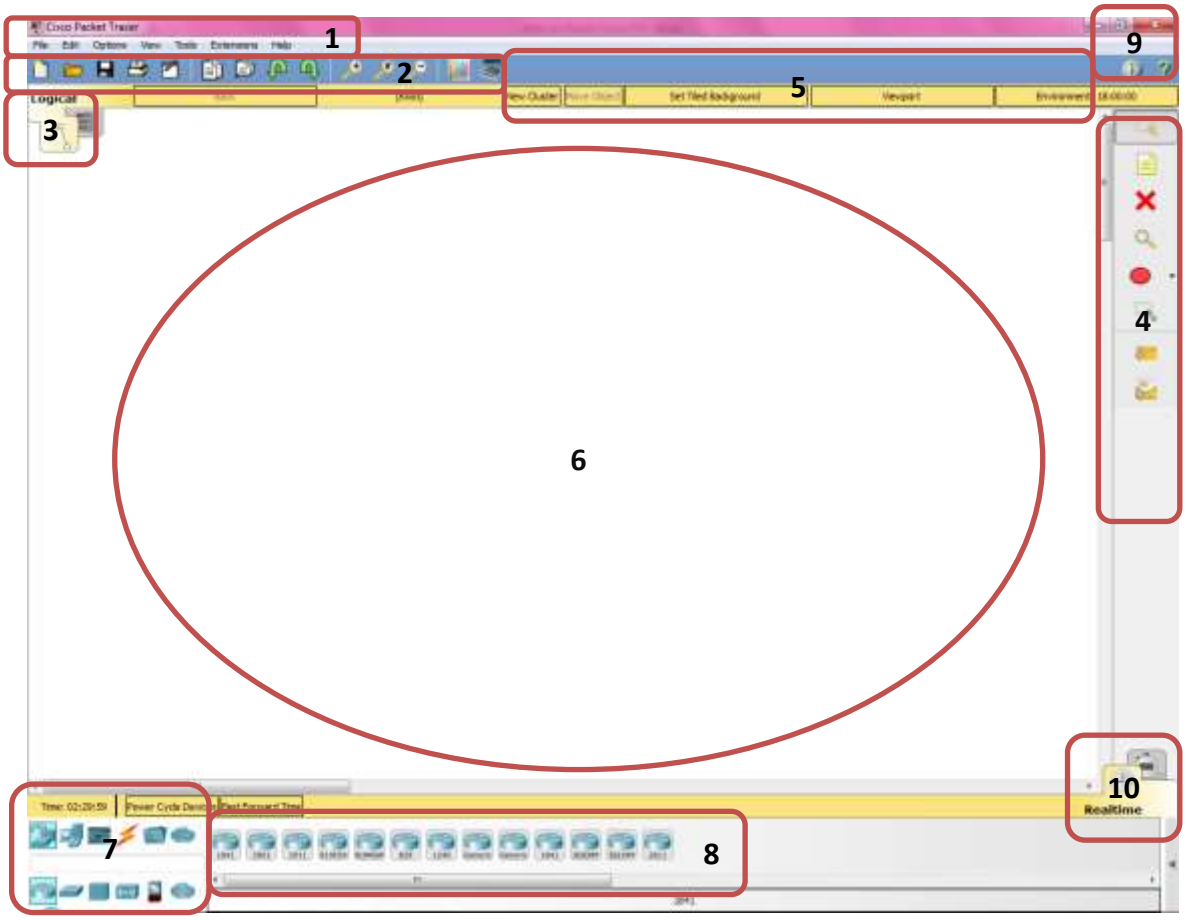
Packet Tracer has two different views

1. Logical Workspace
2. Physical Workspace

Packet Tracer also has two modes of operation

1. Real-time Mode
2. Simulation Mode

- At startup, you are in the Logical Workspace in **Real-time Mode**
- You can build your network and see it run in real-time in this configuration
- You can switch to **Simulation Mode** to run controlled networking scenarios
- You can also switch to the **Physical Workspace** to arrange the physical aspects, such as location of your devices
- You cannot run your network while you are in the Physical Workspace
- You should return to the **Logical Workspace** after you are done in the Physical Workspace




1. Menu Bar
   - This bar provides the File, Options, and Help menus
   - You will find basic commands such as Open, Save, Print, and Preferences in these menus
   - You will also be able to access the Activity Wizard from the File menu

2. Main Tool Bar
   - This bar provides shortcut icons to the File menu commands, including the Activity Wizard
   - On the right, you will also find the Network Information button, which you can use to enter a description for the current network or any text you wish to include

3. Workspace Type Bar
   - You can toggle between the Physical Workspace and the Logical Workspace with the tabs on this bar

4. Common Tool Bar
   - This bar provides access to these commonly used workspace tools:
     a. Select
     b. Move Layout

c. Place Note
d. Delete
e. Inspect
f. Encirclement Test
g. Add Simple PDU
h. Add Complex PDU

5. Created Packet Window
   - This window manages the packets you put in the network during simulation scenarios.

6. Workspace
   - This area is where you will create your network, watch simulations, and view many kinds of information and statistics

7. Network Component Box
   - This box is where you choose devices and connections to put onto the workspace
   - It contains the Device-Type Selection Box and the Device-Specific Selection Box

8. Device Type Selection Box
   - This box contains the type of devices and connections available in Packet Tracer 7.0
   - The Device-Specific Selection Box will change depending on which type of devices you clicked

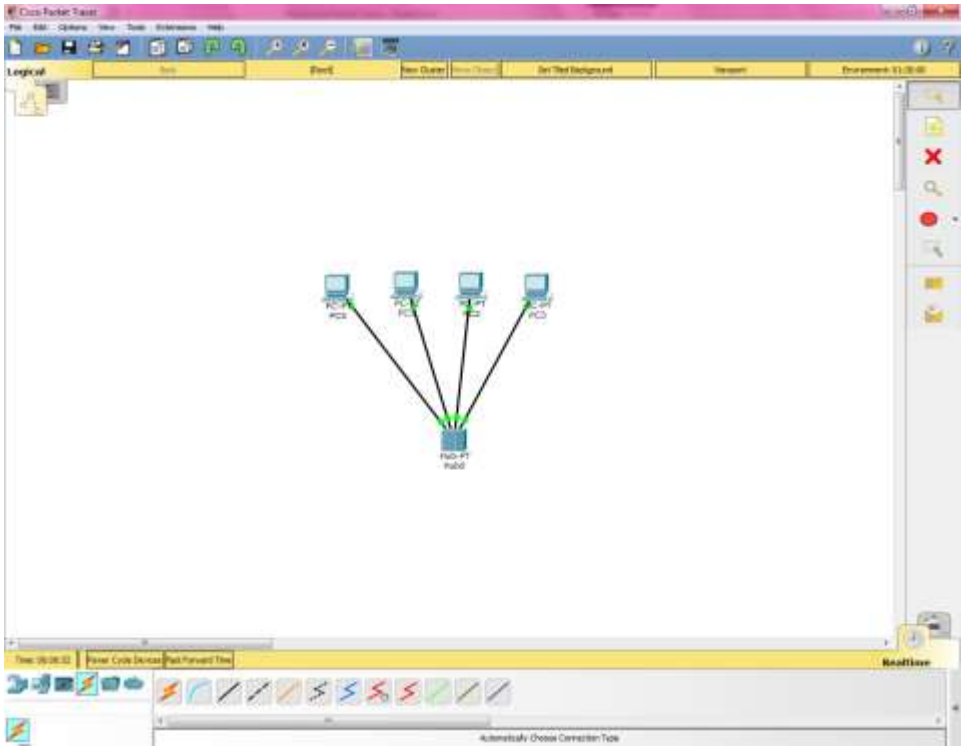
9. Help
   - This is a *how-to page* where you can get help on Packet Tracer 7.0.

10. Real-time or Simulation Mode
    - You can toggle between Real-time Mode and Simulation Mode with the tabs on this bar

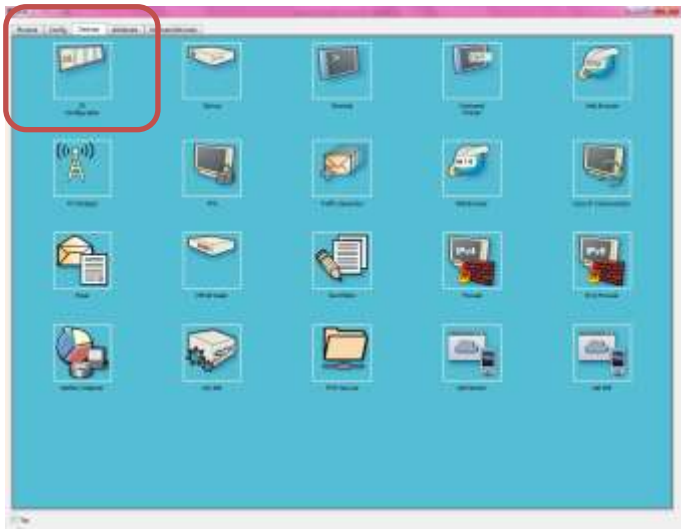
## Sample Network Simulation

Step 1: Start Packet Tracer and Entering Simulation Mode

- Let's create a sample network to see how Packet Tracer simulates a network
- Design a simple network as shown on next figure (connect 4 PCs to a hub).
- Just drag and drop the required devices from the Device Type Selection Box (label 7 & 8).



Step 2: Double click on the PC to assign an IP address to get the following window.



Step 3: Choose IP Configuration and assign the IP address

- The assignment as follows:
    a. PC0:192.168.1.1
    b. PC1:192.168.1.2
    c. PC2:192.168.1.3
    d. PC3:192.168.1.4

Step 4: Click on Simulation Mode

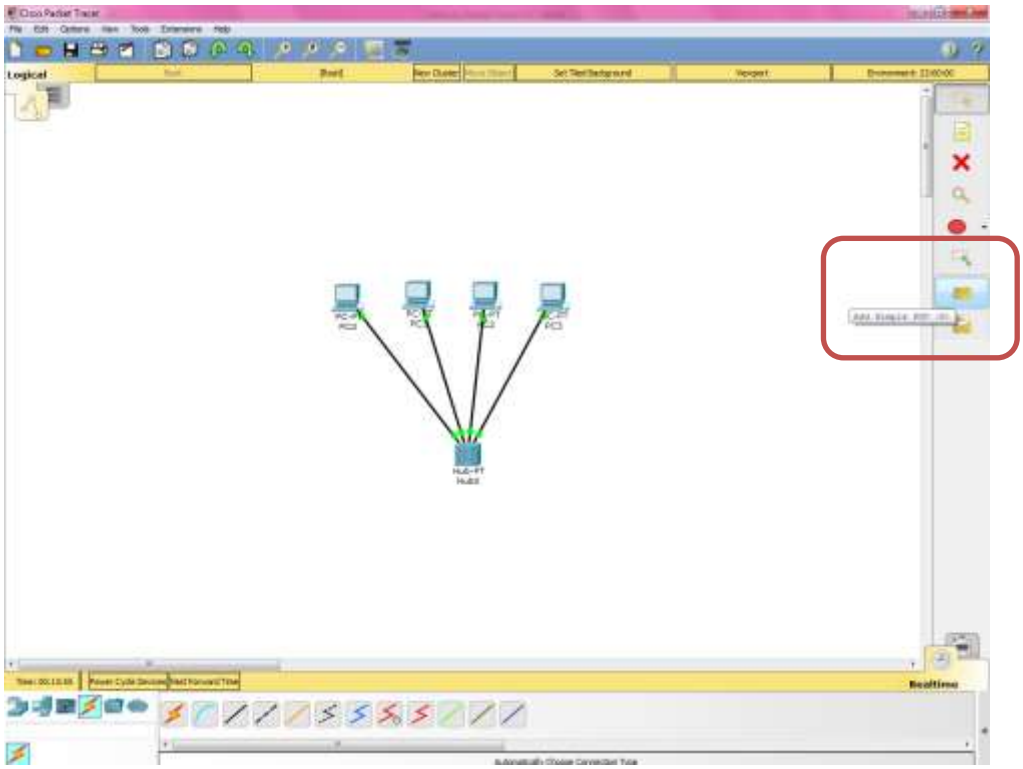
- You will get an event list window

Step 5: Click on Show All/None and Edit Filters to edit the event of the simulation

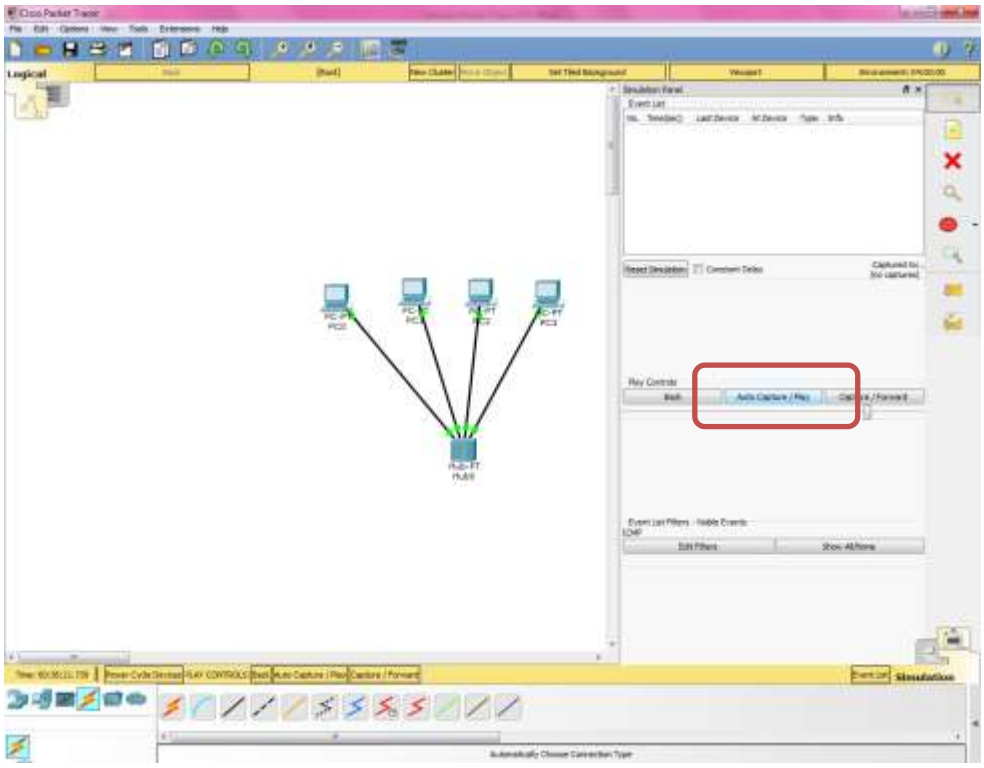
- Make sure you only choose "ICMP" on IPv4 tab as your event.

Step 6: Now switch to Real Time

- Use the Add Simple PDU tool to send a simple 1-time ping message called an echo request, to the other PC, which responds with an echo reply because you have properly configured their IP address settings

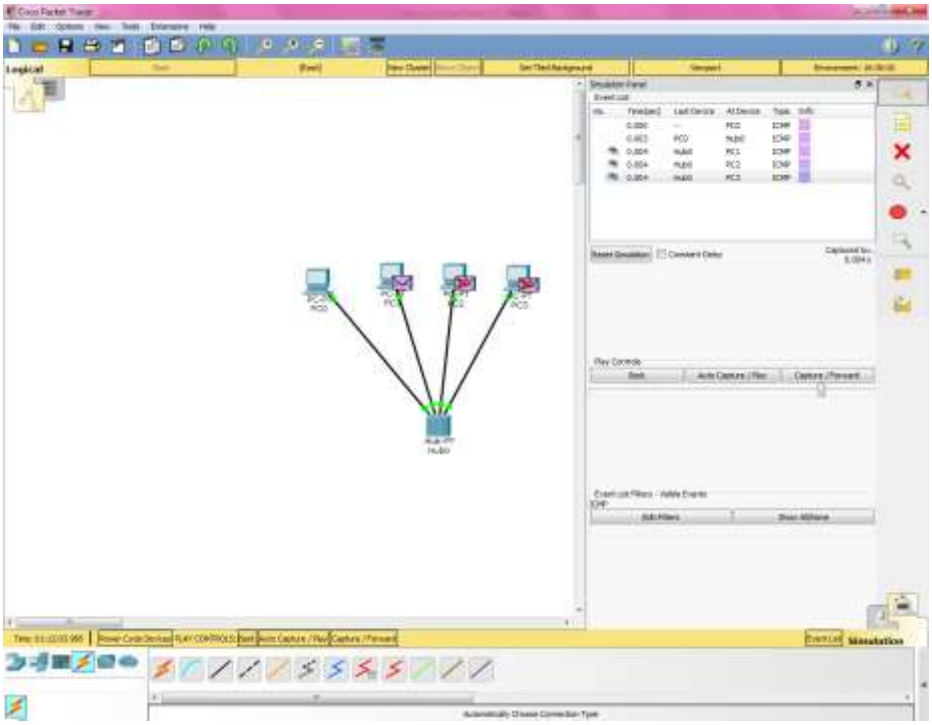


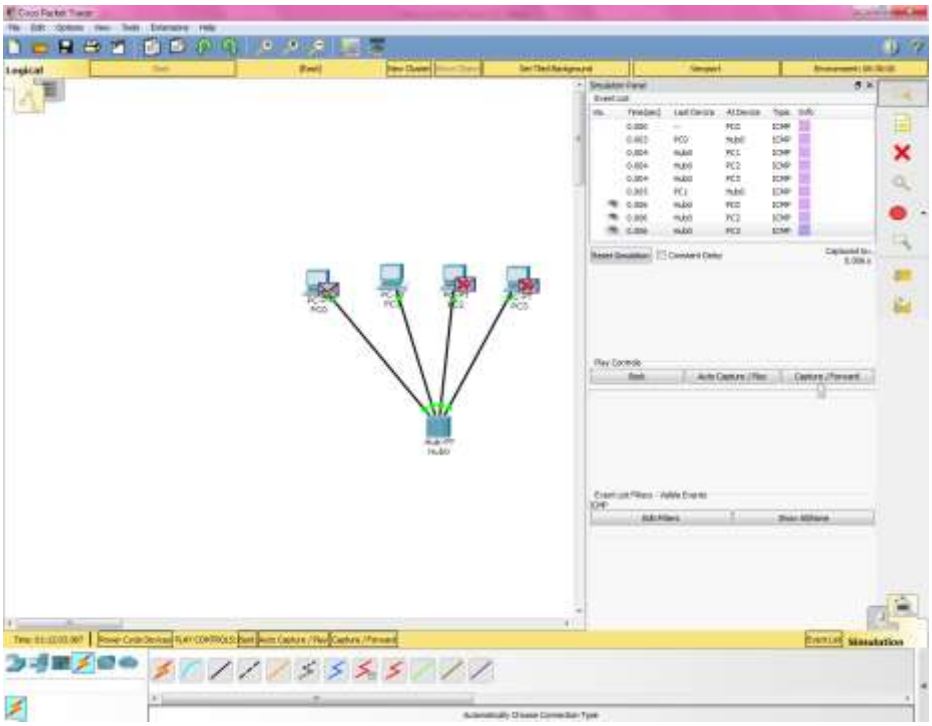
- Click once on PC0, the device issuing the ping (ICMP Echo Request) and then click once on PC1 (the destination of the ICMP Echo Request).



- 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 FastEthernet frame. The next event will send this FastEthernet frame from the FastEthernet 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.

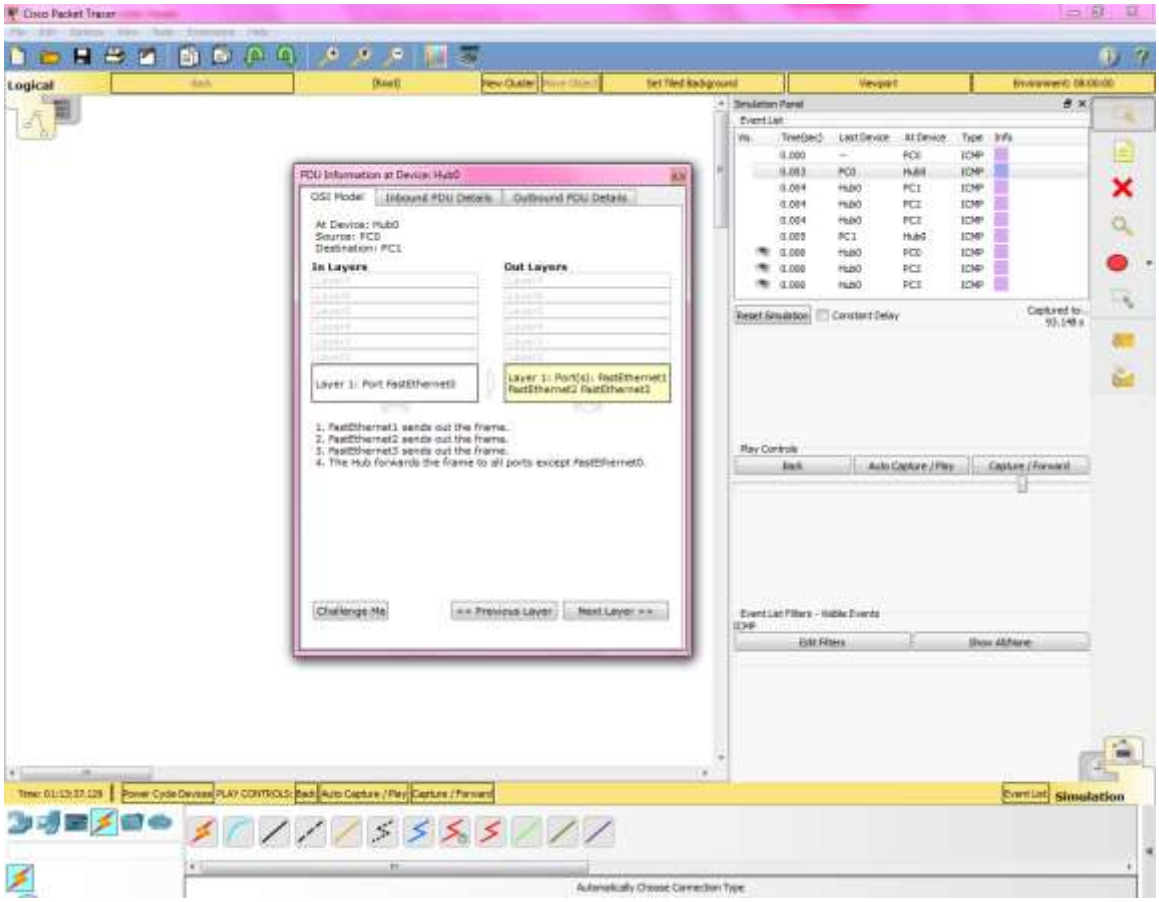




- Note: Using this tool, only a single ping, ICMP Echo Request is sent by PC0, instead of the four pings when using the command prompt.

Step 7: 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 FastEthernet Frame is currently, "At Device", the previous devices, "Last Device", and the type of information encapsulated in the FastEthernet Frame, "Info".
- Single click on the second event's Info box to view the FastEthernet frame with the encapsulated IP Packet and the encapsulated ICMP message "At Device" PC0. Click the *Hint* button.




- The PDU (Protocol Data Unit) is displayed in three different formats, OSI Model, Inbound and Outbound. The default is the OSI Model view with a brief description with what is occurring with this packet.
- You can click on the Inbound PDU Details or the Outbound PDU Details tab to see the protocol details.