My First Packet Tracer Lab

Introduction

Welcome to Packet Tracer. Research has shown that users who master a few basic tasks when first starting to use Packet Tracer get much more out of the software. This lab is designed to familiarize a user with Packet Tracer's features.

Lab Objectives

Important Terminology

1. ICMP ping: command consisting of an echo request message from one device to another, and the returning echo reply.
2. IP address: 32-bit address assigned to devices as identification in the network.
3. Ethernet: one of the most common LAN standards for hardware, communication and cabling.
4. Fast Ethernet Interface: 100 Mbps Ethernet port. In Packet Tracer, a GUI may be used to configure such interfaces.
5. OSI model: 7-layer framework for looking at network protocols and devices, consisting of the application, presentation, session, transport, network, data link, and physical layers.
6. PDU: protocol data unit, a grouping of data appropriate to a given layer in the OSI model.
7. Packets: OSI Layer 3 protocol data units. Represented by envelopes in Packet Tracer Simulation Mode.
8. Device Tables: includes ARP, switching, and routing tables. They contain information regarding the devices and protocols in the network.
9. ARP Table: Address Resolution Protocol (ARP) table, stores pairings of IP Addresses and Ethernet MAC addresses.
10. Scenario: one topology with a set of PDUs placed in the network to be sent at specific times. Using different scenarios, experiment with different combinations of packets using the same base topology.

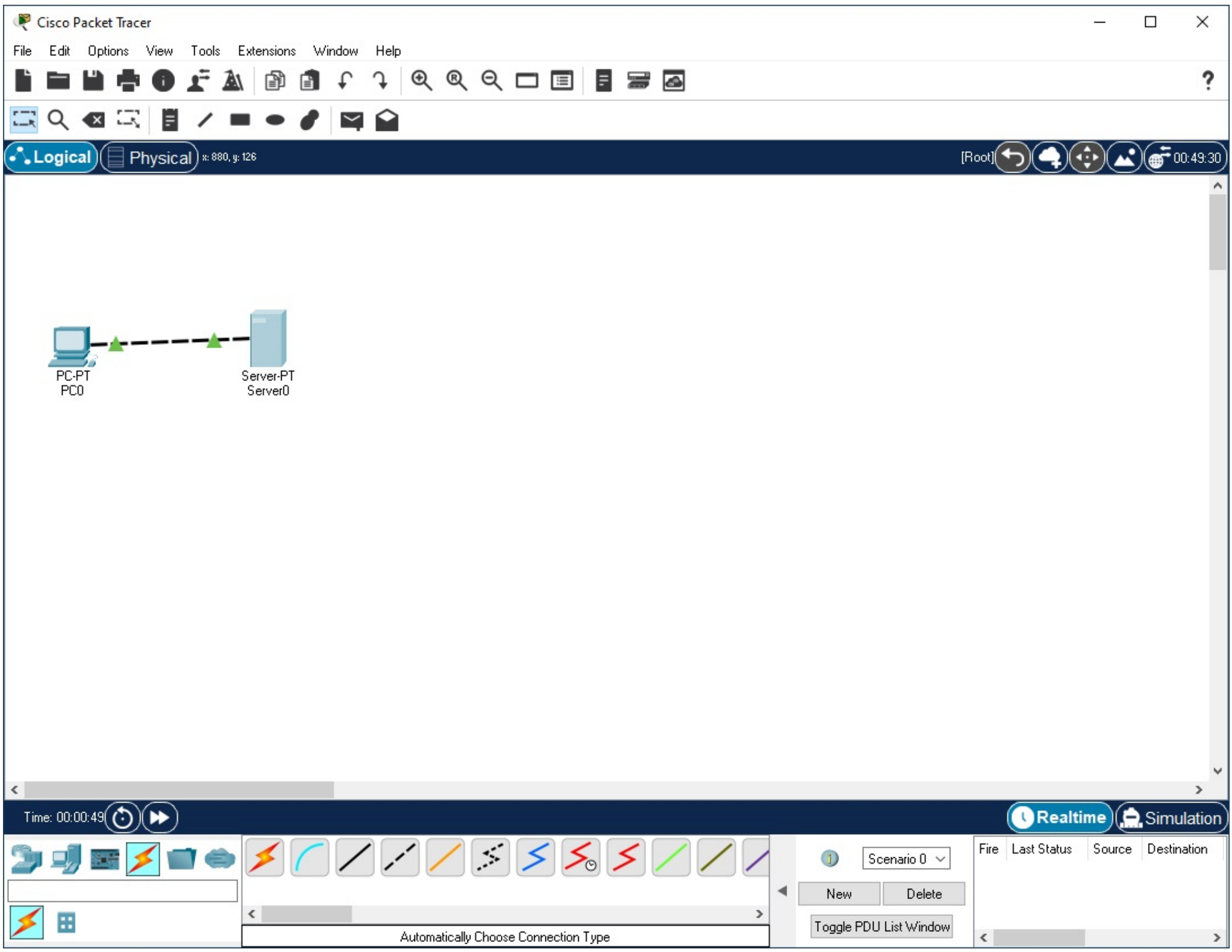
I. Viewing Help and Tutorials

1. Launch Packet Tracer.
2. Open the help content by clicking Help > Contents on the Menu bar. You can also click the question mark on the Main toolbar.
3. The menu will always be visible on the left side of the window while browsing through the help files. Skim through the help sections to get an idea of the functionality of Cisco Packet Tracer.
4. The What's New section under Introduction provides an overview of features that have been added to this version of Packet Tracer
5. Pay close attention to the Interface Overview section under Getting Started to familiarize yourself quickly to the Packet Tracer interface.
6. Browse the Tutorials to be shown how various components in Packet Tracer work.
7. Open the Interface Overview tutorial to learn the basics of the Packet Tracer graphical user interface. **Note:** The tutorials require Internet access and also some browsers may prevent the tutorial from playing. Configure your browser to allow active content to enable the viewing of the tutorial.
8. Click the Forward button to start the tutorial. Then click Pause.
9. Continue viewing the tutorial by pressing the Play button. Parts of the tutorial can also be skipped by dragging the slider to the right. If needed, click the Rewind button to restart the tutorial.
10. Click Exit (X) to close the tutorial window. Close the help content as well.

Congratulations on learning more about resources that will help you get the most out of Packet Tracer.

II. Creating a First Network

1. Start creating a network by first selecting the End Devices. Add a Generic PC and a Generic Server to the workspace.
2. Under Connections, select the Copper Straight-through cable (solid black line) and connect the devices with it. The red lights on the link indicate that the connection is not working. Now, use the Delete tool to remove the Copper Straight-through cable, and use a Copper Cross-over cable (dashed line) instead. The lights should turn green at this point. If the mouse pointer is held over either devices, the link status will be shown as "Up." The network should look similar to this:

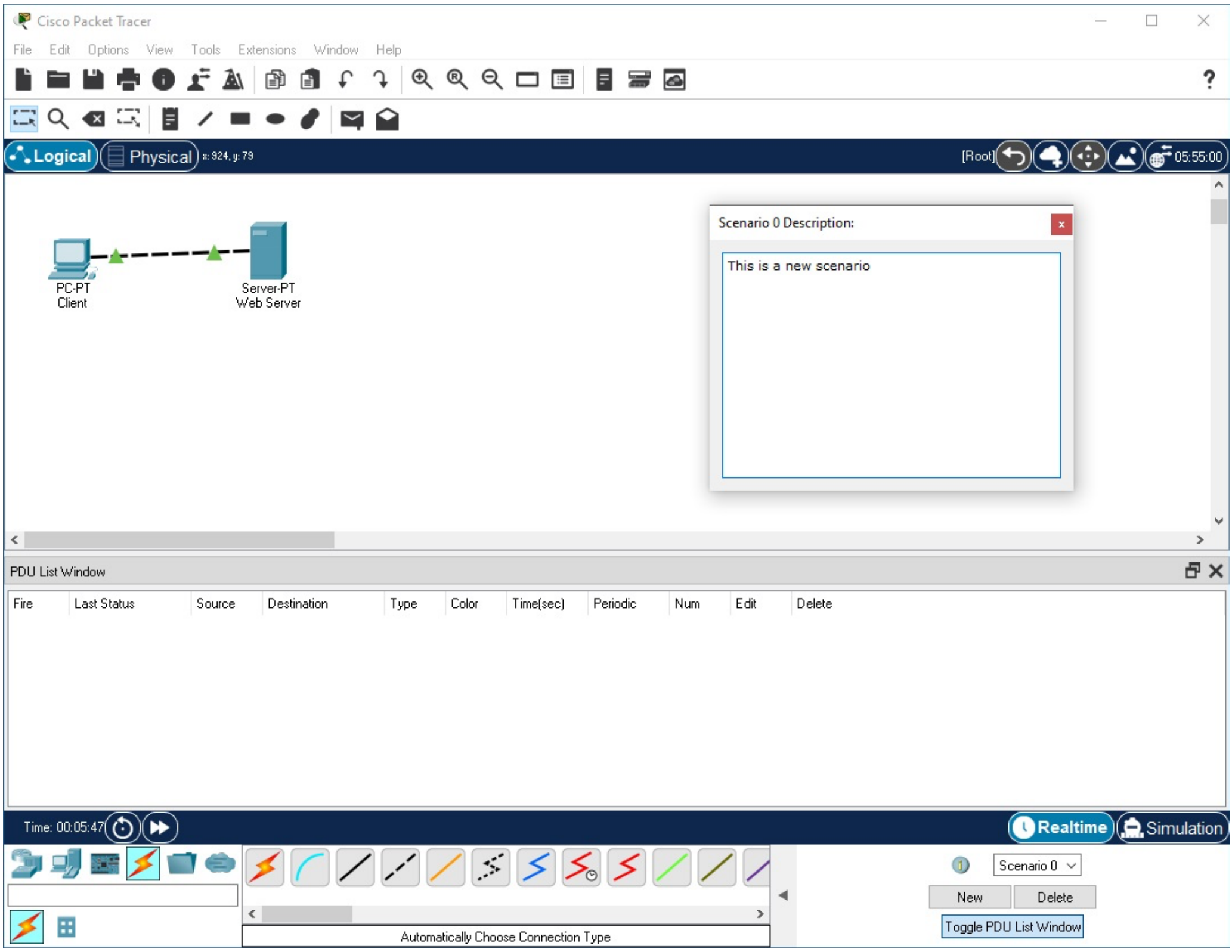


- Click on the PC. While paying attention to the link lights, turn the power off (as shown in the graphic below), and on again. Follow the same steps for the server. The link lights turn red when the device is off. This means that the link is down or is not working. The link lights turn green when the device is turned back on.
- Try all three ways to learn about the devices. First, mouse over the devices to see basic configuration information about them. Second, click on each device with the Select tool to show the device configuration window, which provides several ways to configure the device. Third, use the Inspect tool to view the tables the network device will build as it learns about the network around it. In this example, open the ARP table. Since the devices have not been configured yet, the ARP tables are empty. Always remember to close the windows after viewing them or they will clutter the workspace.
- Open the PC configuration window and change the settings using the Config tab. Change the display name to Client and set the DNS server to 192.168.0.105. Under Interface, click FastEthernet0 and set the IP address as 192.168.0.110. Packet Tracer automatically calculates other parameters. Make sure that the Port Status box is checked. For future reference, note that other Ethernet interface settings, such as bandwidth, duplex, MAC address, and subnet mask can be modified using this window.
- Go to the Desktop Tab and click on IP Configuration. Notice that the IP address, subnet mask and DNS server can be changed here as well.
- Open the Server configuration window and go to the Config tab. Change the display name to Web Server. Click FastEthernet0 and set the IP address as 192.168.0.105. Make sure that the Port Status is also on. Click on the Services Tab, then on the DNS selection and set the domain name as www.firstlab.com. Set the IP address as 192.168.0.105 and click Add. Finally, check to make sure that the service for DNS is on.
- Reposition the network devices by dragging them to a new location. Add a network description by using the “i” button on the upper right corner. Then add some text labels within the Logical Workspace by using the Place Note tool.
- Save your work using the File > Save As option and create a meaningful filename.

Congratulations on creating your first network.

III. Sending Simple Test Messages in Realtime Mode

1. Start by opening the file saved in the last section.
2. Notice that the file opens in Realtime Mode. Use the Add Simple PDU tool to send a simple one-time ping message, called an echo request, to the server. The server responds with an echo reply because all devices have properly configured IP address settings.
3. Open the User Created Packet Window by clicking on the left facing arrow in the lower right corner of the Packet Tracer program to see the different capabilities of this ping message, including an indication that the ping was successful.
4. Toggle the PDU List Window to see a larger display of this message. One or more of these messages can be saved as a scenario. Scenario 0 is displayed when starting. Label this first scenario with an “i” note. Different scenarios allow the use of the same topology for experiments with different groupings of user created packets.
5. Click New to create a new scenario. New scenarios will initially be blank.
6. Add two packets using the Simple PDU tool, a PDU from the PC to the Server and a different PDU from the Server to the PC. Then add an “i” note describing the scenario, to complete Scenario 1. An example is shown below:



7. Several scenarios can be saved with a single network. Alternate between Scenario 0 and 1.
8. Now, remove Scenario 0 using the Delete button.
9. Scenario 1 is now visible. Go to the last column in the User Created Packet Window and double-click (delete) to remove a PDU.
10. Delete the whole scenario. Notice that the list went back to the default Scenario 0.

Congratulations on being able to send and organize simple test messages in Realtime Mode.

IV. Establishing a Web Server Connection Using the PC's Web Browser

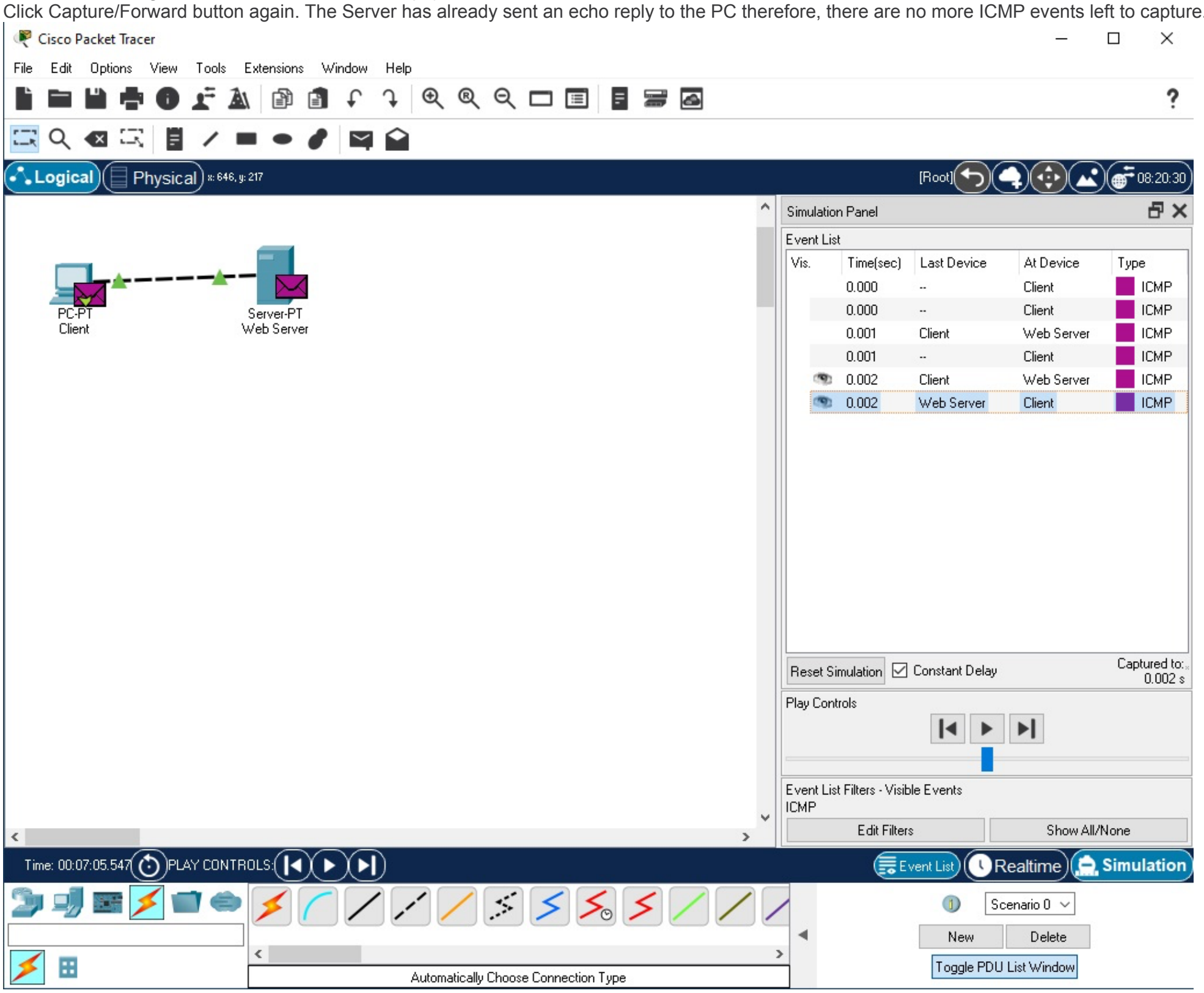
1. Open the file saved from the previous section.
2. Click on the PC to view the configuration window.
3. Select the Desktop tab, and then click Web Browser. Type in www.firstlab.com as the URL and click the Go button. The Packet Tracer welcome page, shown below, appears, indicating that the web connection has been successfully established.
4. Clear the URL, type www and click Go. Since the address entered is not complete, a "Host Name Unresolved" message appears.
5. Type 192.168.0.105 as the URL entry and click on Go. Notice that the Packet Tracer welcome page appears again. This is because the Server IP address can also be used to establish a web connection.
6. Close the window and try the same steps, detailed below, in Simulation Mode. In this mode, the user controls time, so the network can be viewed running at a slower pace, allowing observation of the paths packets take and inspection of packets in detail (packet tracing!).
7. Enter into Simulation mode by clicking on the stopwatch tab lin the lower right corner of the workspace. Select the PC again and go to the Web Browser in the Desktop tab. Type www.firstlab.com as the URL again and click Go. The welcome page should not appear yet.
8. Switch to the main interface of Packet Tracer without closing the PC configuration window. Notice that a DNS packet is added to the event list.
9. Click Auto Capture/Play or repeatedly click the Capture/Forward button until the HTTP packet appears on the PC. Go back to the PC configuration window. The Packet Tracer welcome page is now shown.
10. Close the PC configuration window.

Congratulations on successfully establishing a web server connection.

V. Capturing Events and Viewing Animations in Simulation Mode

1. Open the previously saved file.
2. In Realtime Mode, send a simple PDU from the PC to the Server.
3. Delete the PDU by using the method learned in the previous section.
4. Switch to Simulation Mode.
5. Click All/None to uncheck all fields and click Edit Filters. Then click ICMP to only view ICMP packets in the animation.
6. Add a simple PDU from the PC to the Server. Notice that the newly created PDU is added to the User Created PDU List. This packet has been captured as the first event in the event list and a new packet icon (envelope) appears in the workspace. The eye icon to the left of the event list indicates that this packet is currently displayed.
7. Click the Capture/Forward button once. This simulates a network sniffing program, capturing the next event that occurs on the network. Note that after clicking Capture/Forward, the packet in the workspace moves from one device to another (this is the ICMP echo request message from the PC to the Server). Another event is added in the event list – this reflects the change in the workspace.

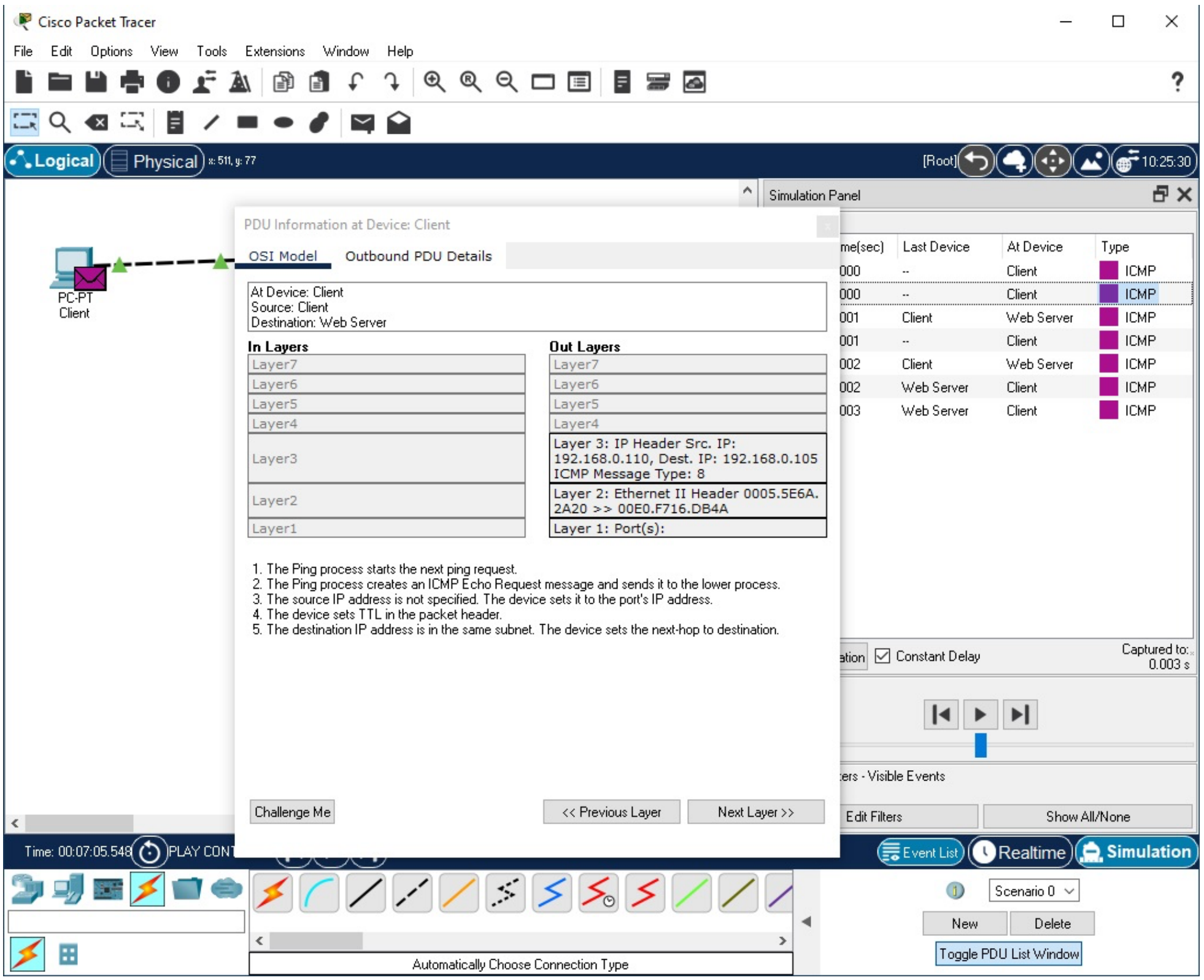
8. Adjust the speed of the animation by dragging the Play Speed slider to the right making it go faster. Dragging the speed slider in the opposite direction (to the left) will slow down the animation.
9. Click the Capture/Forward button a second time. This captures the next network event (this is the echo reply from the Server to the PC, shown as successful with a green check mark on the envelope).
10. Click Capture/Forward button again. The Server has already sent an echo reply to the PC therefore, there are no more ICMP events left to capture.



Congratulations on successfully capturing events and viewing animations in Simulation Mode.

VI. Looking Inside Packets in Simulation Mode

1. Continuing from the last activity, click Reset Simulation. This clears the entries in the event list except for the original packet.
2. Select the packet envelope on the workspace to show the PDU Information window like the one shown in the screenshot below. This window contains the OSI Model tab, which shows how the packet is processed at each layer of the OSI model by the current device. Close this window, noting that this packet is indicated in the event list by the eye icon. The whole row in the event list is also highlighted. Clicking on the color square in the Info column is equivalent to clicking directly on the packet envelope (try it!).

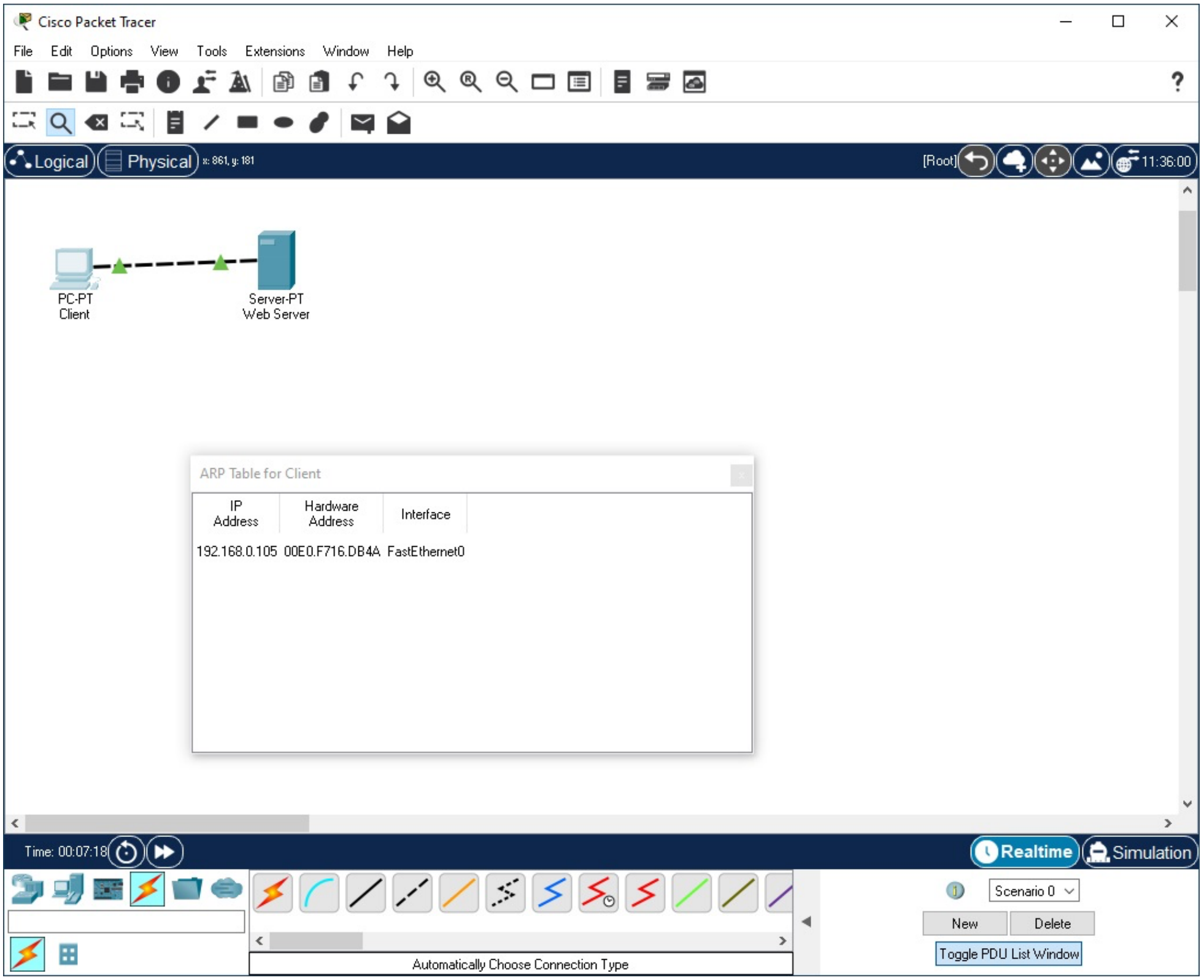


3. Use the Next Layer and Previous Layer buttons to see details of the packet processing at the relevant OSI layers. Note that only the Out Layers can be viewed in the case of this original echo request message.
4. Click on the Outbound PDU Details tab. This tab shows exactly what makes up the PDU headers. It is organized into header type and the individual fields in each header.
5. Close the PDU Information window. Click on Capture/Forward button once.
6. Click on the packet in the workspace again to open the PDU Information window. Notice that this time, information regarding both the In Layers and Out Layers can be viewed.
7. Click on the Inbound PDU Details tab. This shows the details of the inbound echo request packet from the PC to the Server. The Outbound PDU Details tab, shows similar information, but for the echo reply packet from the Server to the PC.
8. Click on Reset Simulation again. Now click on Auto Capture/Play. The echo request and echo reply are automatically captured. Click on the Back Button to rewind the animation one step at a time. Now click on the Capture/Forward button to forward the packet through the animation. Note the change in the event list and the workspace. Remember that at any time, a PDU Information Window can be opened by clicking directly on the envelope on the workspace, or by clicking the Info column in the Event List.
9. Click on the Back Button twice to rewind the animation. Now click Auto Capture/Play and the packet animation will automatically occur.

Congratulations on being able to manipulate the Play Controls and PDU Information Window to understand more about packet processing details.

VII. Viewing Device Tables and Resetting the Network

1. Open the file saved from the previous section.
2. Open the ARP Tables for both devices by clicking them with the Inspect tool. The ARP tables always appear on the same spot. Reposition them to make them both visible. You can also resize the tables for better viewing.
3. In Realtime Mode, send a simple PDU from the PC to the Server. Notice that the ARP tables are filled in automatically, as shown here:



4. Delete the PDU using the method covered in the previous sections. Notice that the entries in the ARP tables are NOT cleared. ARP entries for both devices have already been learned. Deleting the user created PDUs does not reset events what has already occurred in the network.
5. Click Power Cycle Devices. ARP tables are cleared because the Power Cycle Devices button turns the devices off and back on again therefore, losing temporary information like the ARP table entries.
6. Go to Simulation Mode. In the event list filters, make sure that ICMP and ARP are checked so that you can view ICMP and ARP packets in the animation.
7. Create a new simple PDU from the Server to the PC.
8. Notice that since the devices were power cycled earlier, the ARP tables are empty. ARP request packets need to be issued before the ICMP ping packets, so that the devices in the network can learn about each other. Click on Auto Capture/Play to watch the animation.
9. Click Reset Simulation. Notice that even though the event list is cleared (except for the user created PDU), the ARP tables remain full. Click Auto Capture/Play. This time, since the ARP tables are full, there are no new ARP packets issued.
10. Click Power Cycle Devices. Doing so will empty the tables. Notice that new ARP request packets appear automatically in the event list.

Congratulations! You can now view device tables, reset a simulation, and reset the network.

VIII. Reviewing Your New Skills

- Single-clicking on the Delete button removes the entire scenario including all the PDUs associated with it.
- Double-clicking on (delete) in the far right column in the PDU List window deletes individual PDUs.
- The Reset Simulation button clears all entries in the Event List, except for User Created PDUs, and allows the animation to restart. This, however, does not reset the device tables.
- The Power Cycle Devices button turns all of the devices in the network off and on so the tables that the devices built are lost along with configurations and other information not saved.
- Saving work periodically prevents lost configurations and state changes in the network.

Congratulations on being ready to build and analyze many different networks in Packet Tracer!