Presenter Demonstration Notes: PT Intermediate

This presentation is designed to build on basic skills that instructors have using Packet Tracer. The focus of this presentation is on using Simulation Mode, creating Scenarios, examining PDU information and using the Challenge Mode. It is important that instructors have basic skills in order to fully understand the tasks in this presentation.

There are speaker notes for each slide that can be helpful when discussing the concepts on that slide. Please note that this presentation will use both PowerPoint and Packet Tracer. You might practice switching between these applications using Alt+Tab.

Slides 14 – 25 (Simulation Mode)

Slides 15 & 16 give some overview information about Simulation Mode and how it can be used for instruction in the classroom. Use the speaker notes and your own experience to convey to instructors how Simulation Mode enhances their students' experiences.

Slides 17-26 go over the Simulation Mode interface and controls. A simple PING is generated between 2 hosts and screen shots are used to show how the routers learn the MAC addresses of the hosts and then ultimately process the ICMP packets.

After slide 26, open the .pkt file (Intermediate_1.pkt) to demonstrate each of the tasks described in the screen shots:

1. After "spanning tree" completes and all links turn green, switch to Simulation Mode.
2. Create a Simple PDU from HostB to HostA.
3. Point out that PT generated an ARP PDU in the Event List.
4. Open the ARP tables for HostA, HostB, BHM and GAD and arrange them so that you can see the topology and the Event List window. Point out that the only entries in the ARP tables for the routers are for the directly connected interfaces. The ARP tables of the hosts should be empty. (Note: If other addresses are in the ARP tables, use the Power Cycle Devices button to clear them out. Remember to switch to Realtime Mode to allow spanning tree to recalculate before returning to Simulation Mode.)
5. Click the Capture/Forward button. Point out that the ARP PDU goes first and the MAC address for HostB is added to the BHM router.
6. Continue to click the Capture/Forward button and watch as the ICMP PDU goes from HostB to GAD. Note that the ICMP will fail at GAD.
7. Continue to click Capture/Forward and watch as GAD sends an ARP request to HostA. When the ARP is returned, the ARP table on GAD is populated with the MAC address of HostA.
8. Point out that the Event List indicator in the bottom right of the screen lists the ICMP PDU as "failed". This is because the first PDU does fail due to the lack of MAC address in the ARP tables.
9. Now that the ARP tables are populated, Reset the Simulation and try the PING again. This time the ICMP PDU travels successfully from HostB to HostA. Point out that the Event List indicator now reads "Successful" for this packet.
10. Demonstrate hiding and unhiding the Event List window.

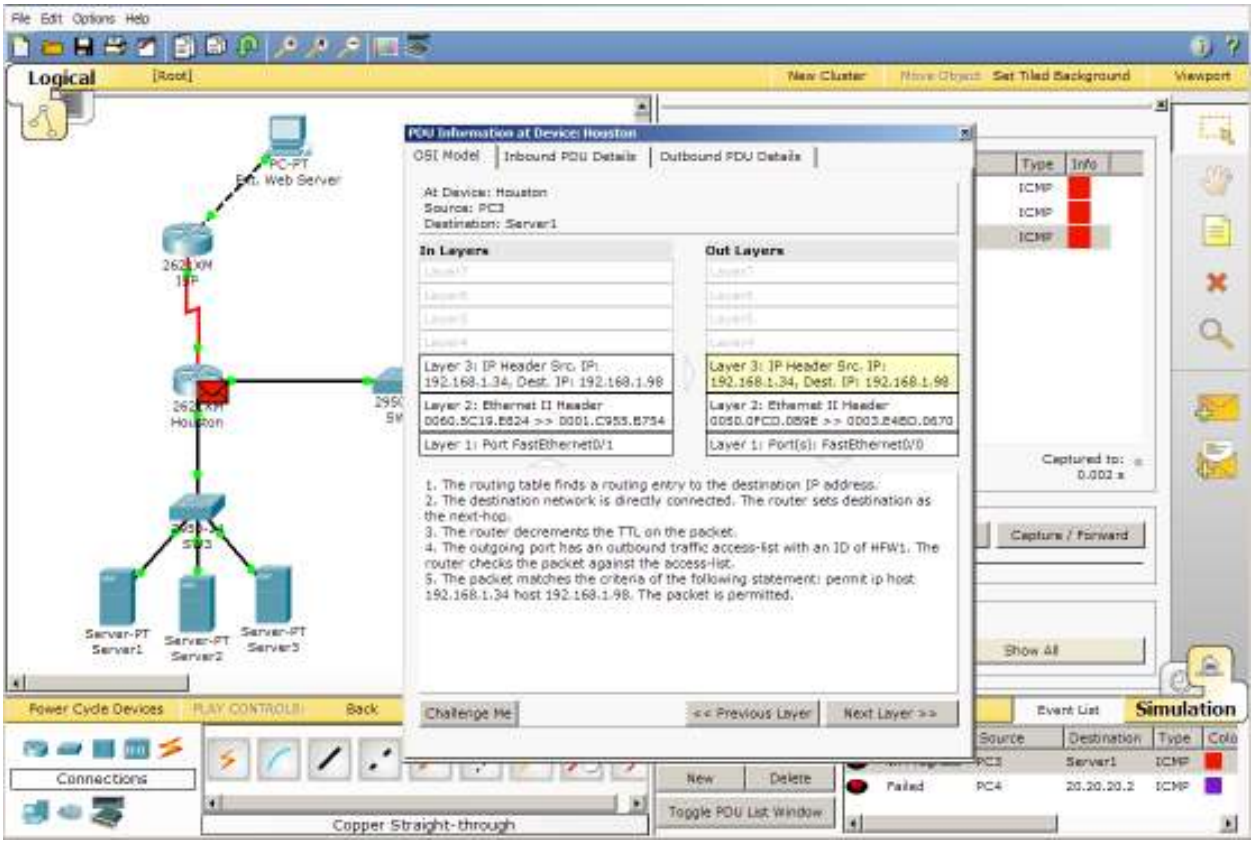
Slides 28 – 39 (PDU Information)

Slides 28-39 describe and demonstrate how the PDU information window can be used to show students what's "inside" the packet and how devices are processing the packets based on their contents.

The screen shots show how to open the PDU Information window and navigate the various tabs: OSI Model, Inbound and Outbound. Several examples of PDU information in the OSI Model are shown and what learning opportunities each presents. Please note that some of these screen shots apply to the topology used in this presentation, and some of them are from another .pkt file.

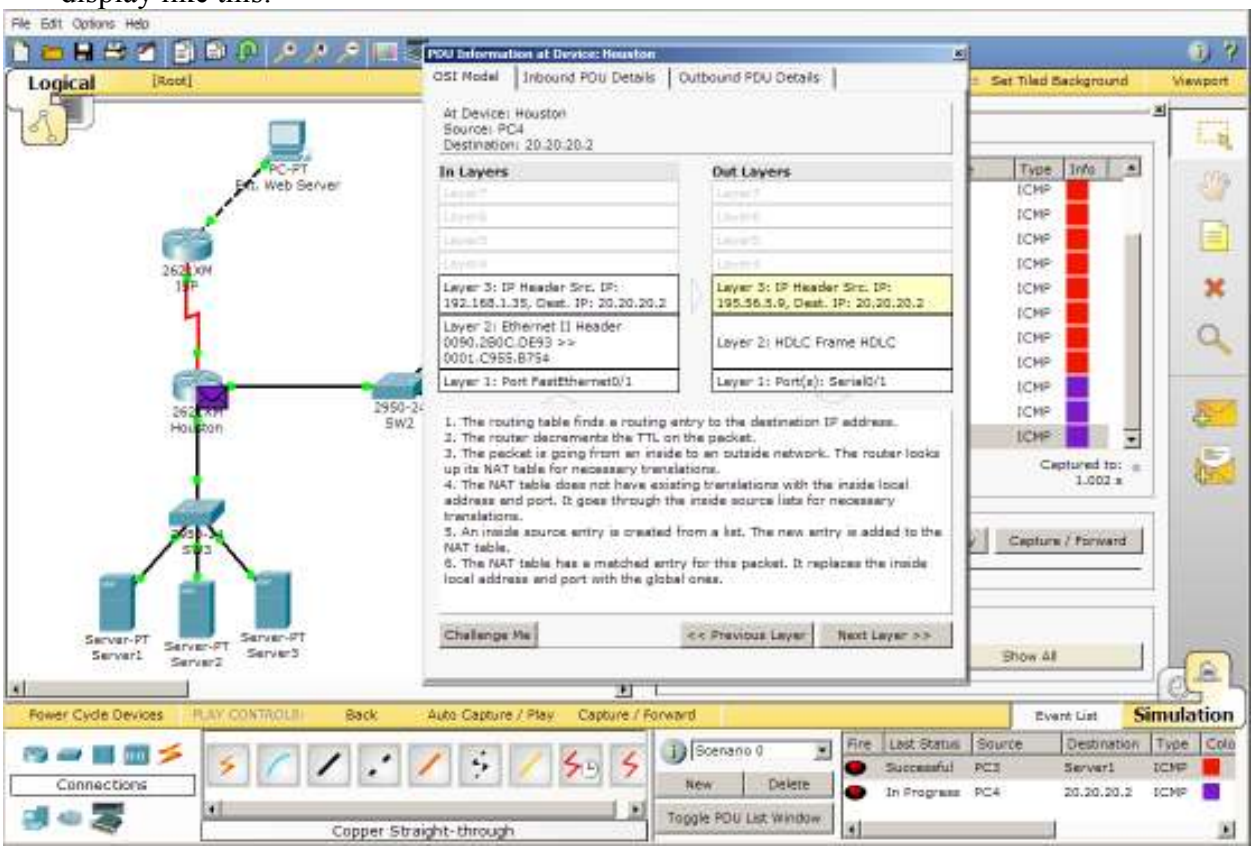
After Slide 39, switch to Packet Tracer and use the .pkt file (Intermediate_2.pkt) to demonstrate the following:

1. Open the file and wait for spanning tree to complete and all links to turn green.
2. Switch to **Simulation Mode**.
3. Click the **Auto Capture/Play** button to run through the simulation. Remember that this first ping will fail since the ARP tables are not populated.
4. Click the **Reset Simulation** button. Click the **Capture/Forward** button until the packet from PC3 arrives at the router Houston.
5. Click on the packet icon in the topology to open the PDU Information window. You should see this:

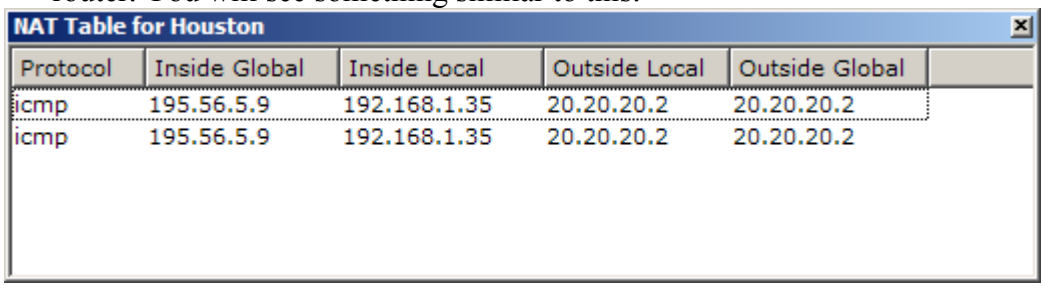


6. Click on Layer 3 in the Out Layers to show the information above. Point out that we can see from the information provided that the router checked the packet against an access-list. The packet matched a "permit" statement and the packet was sent to Layer 2 for processing.
7. Show other layers, if desired.

8. Close the PDU Information window and continue to click the **Capture/Forward** button until the ping from PC3 completes. You will see a green check mark on PC3 when the ping reply arrives at PC3.
9. Click the **Capture/Forward** button to begin the ping from PC4 to the External Web Server. You will know that the new packet is beginning because a different color will show up in the Event List. Stop clicking the button when the packet arrives at the Houston router.
10. Click the packet icon in the topology to open the PDU Information window. You will see a display like this:



11. Click on Layer 3 in the Out Layers. Point out that the information provided allows us to see that the router replaced the address of the packet in accordance with the NAT configuration.
12. As a special treat, show instructors the NAT table of the Houston router. Do this by closing the PDU Information window and then using the Inspect tool to open the NAT table of the Houston router. You will see something similar to this:



NAT Table for Houston

Protocol	Inside Global	Inside Local	Outside Local	Outside Global
icmp	195.56.5.9	192.168.1.35	20.20.20.2	20.20.20.2
icmp	195.56.5.9	192.168.1.35	20.20.20.2	20.20.20.2

Slides 41 – 46 (Complex PDUs)

Slides 41-46 describe and demonstrate how to create and use Complex PDUs. Point out to instructors that Complex does not mean complicated, rather it refers to the ability to control more

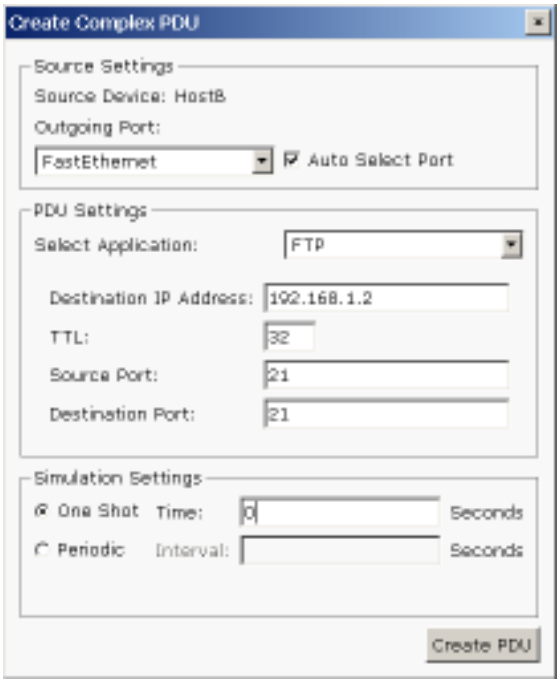
parameters of the packet. Remind them that a Simple PDU is a ping and that sometimes they will need to create a packet other than ping to test ACLs, NAT, connectivity, etc.

Show the slides and screenshots of the program. These will walk instructors through creating and editing PDUs as well as offer some good ideas about workspace management.

Slide 46 shows instructors that they can continue to use the Command Prompt even in Simulation Mode. This can be helpful when bridging the gap between "real" equipment and a simulation. The Command Prompt is familiar and trusted.

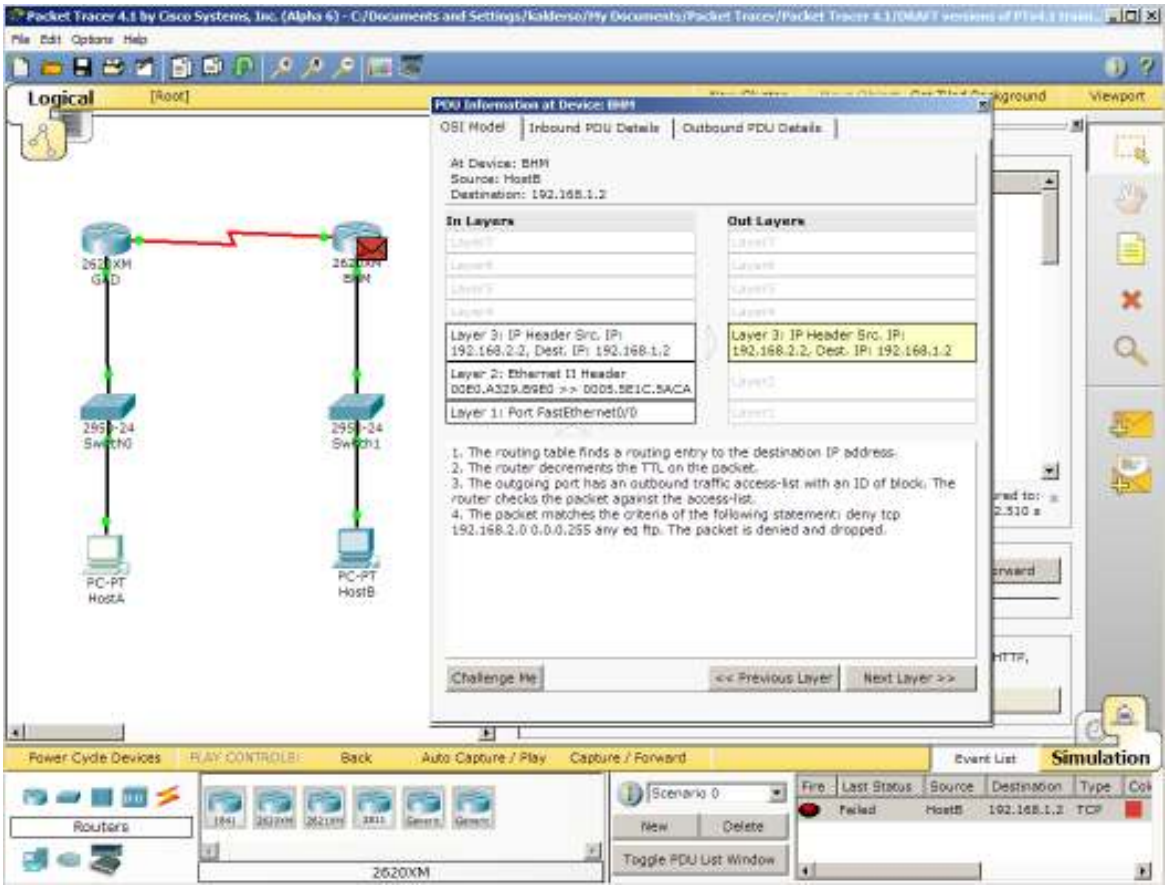
Complete these steps to demonstrate creating and editing Complex PDUs:

1. Open the .pkt file (Intermediate_3.pkt) and allow spanning tree to run in Realtime Mode before switching to Simulation Mode.
2. From Simulation Mode, click on the BHM router and look at its configuration. You should see that an access list has been configured and applied that blocks FTP (port 21) from hosts on the FastEthernet LAN.
3. To test functionality of this ACL, we will first create a Simple PDU and see that it is not blocked (remember that a Simple PDU is a ping and we haven't blocked ping).
4. Create a Simple PDU from HostB to HostA. Remember that this first run through will not work because the ARP table is not populated yet. Run the first one and then Reset the Simulation and then run it again. The ping should be successful.
5. In order to test the ACL we need to create a Complex PDU. First delete the existing Ping packet from the PDU List.
6. Next click the Complex PDU button and click HostB to begin defining the parameters of the PDU.
7. Complete the fields of the PDU as illustrated below:

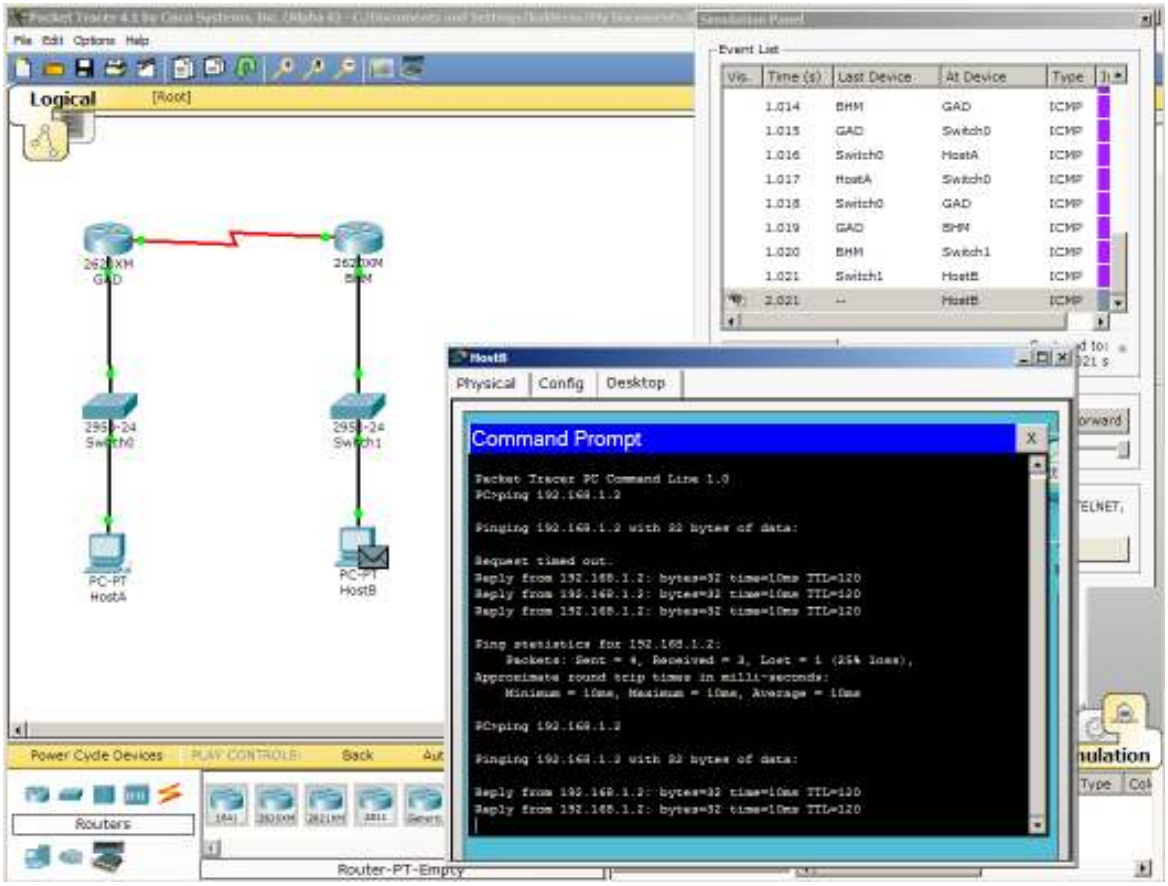


8. Click the Create PDU button and play the simulation. The packet should stop at the BHM router and be marked with a red X.

9. Click the packet with the red X. Click Layer 3 in the outbound column and you should see details similar to this:



10. Point out how we needed to use a Complex PDU in order to test the ACL, since the ping packet went through successfully, and only the FTP packet was blocked.
11. To illustrate how the Command Prompt window can be used in conjunction with the Simulation panel, undock the Simulation panel and move it to the right side of the screen.
12. Open the Command Prompt of HostB, and issue the command: ping 192.168.1.2. This will place a ping packet in the simulation window, but will not begin the ping until you use the play buttons.
13. Use the Auto Capture/Play button to process the pings. Notice that you can see the replies in the Command Prompt window as they return to HostB.



Presenter Demonstration Notes: PT Intermediate

Topic, Audience, Goal/Purpose of this PowerPoint presentation:
This presentation is designed to build on basic skills that instructors have using Packet Tracer. The focus of this presentation is on using Simulation Mode, creating Scenarios, examining PDU information and using the Challenge Mode. It is important that instructors have basic skills in order to fully understand the tasks in this presentation.

There are speaker notes for each slide that can be helpful when discussing the concepts on that slide. Please note that this presentation will use both PowerPoint and Packet Tracer. You might practice switching between these applications using Alt+Tab.

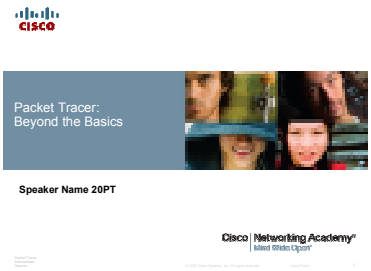
1. Who is the intended audience?
   Academy instructors; primarily related to CCNA content
   Academy instructors who already have basic skills using Packet Tracer.
   Basic skills include:
   - Create & arrange devices
   - Create connections
   - Configure devices
   - Add notes
   - Use PC desktop applications
   - Create a simple simulation

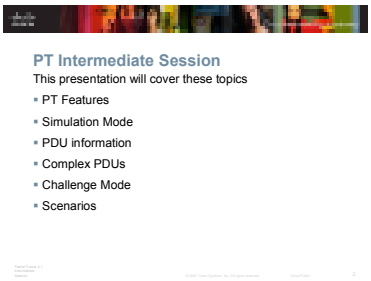
   If you don't already know how to do these things, you should start with the Novice session, as this session will not cover these basic skills.

2. What is the intended learning environment for using these presentation materials?
   Remote; 60 minute session using WebEx and the WebEx Internet Phone feature. You may use another web conferencing tool along with a conference call or a phone bridge. Also, these materials may be easily modified for use in an in-person environment.

3. What is the goal/purpose of these materials?
   For academy instructors and those interested in learning intermediate-level skills of Packet Tracer:
   - Simulation Mode
   - PDU information
   - Complex PDUs
   - Challenge Mode
   - Scenarios

   The purpose of this demonstration is to provide instructors with specific examples of how to teach using these features of Packet Tracer. By using specific examples, instructors will be able to see how they can add Packet Tracer to their classroom toolkit.

	4. Prior to the web conference session Send the handout to participants in advance of the training session. Have participants print out handout in advance. Demonstrate PT over WebEx while participants follow along with handout. Participants may then make notes on the handout during the session - or - If the participant has the available computers, they could have one logged into the WebEx session and the other they could use to practice using PT. **NOTE:** This PPT and Speaker Notes were created by updating the "PT Intermediate" PPT and Presenter Notes. The updates are based on PT5.2 and higher (RC1) on July 20, 2009. **Slides 1 – 2 (Session Overview)** All blue text in this document is intended to provide a guide to the session presenter of topics in this presentation and directions for demonstration. Set the stage for the presentation. Go through slides 1-2, setting the stage and adding information from the notes as desired.
 Title Slide	**Cisco Networking Academy Program** **Packet Tracer: Intermediate Session** Welcome. This 60-minute session will not allow much opportunity for you to speak so during the session please feel free to type questions in the WebEx chat window. Thank you for participating in this session of Packet Tracer. To get an idea of the experience-level of this group, I would like to ask you a few questions and ask you to use the yes and no indicators to respond. If you look in the right-hand side of the WebEx window, you should see the yes and no buttons. Click on the yes button to demonstrate that you have found it. Thank you. • Have you seen or tried any version of PT before? • Have you used any version of PT before in your teaching? • Did you participate in the Packet Tracer Novice session? The focus of this presentation is on using Simulation Mode, creating Scenarios, examining PDU information and using the Challenge Mode. It is important that instructors have basic skills in order to fully understand the tasks in this presentation.



Slide 2

Slide 2 – PT Intermediate Session

This session is designed for users who already have basic skills using Packet Tracer. Basic skills include:

- Create & arrange devices
- Create connections
- Configure devices
- Add notes
- Use PC desktop applications
- Create a simple simulation

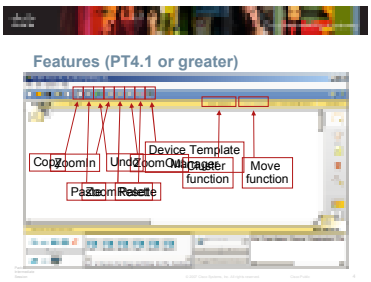
If you don't already know how to do these things, you should start with the Novice session, as this session will not cover these basic skills.

This presentation will cover these topics:

- PT Features
- Simulation Mode
- PDU information
- Complex PDUs
- Challenge Mode
- Scenarios

Slide 3

Slide 3 – PT Features



Slide 4

Slide 4 –Features

If you have used a previous version of Packet Tracer, then you will be very interested in learning about some of the features included in PT4.1 or greater.

Zoom viewing tools have been added.

- ZoomIn (Ctrl+I) to zoom into the workspace.
- ZoomOut (Ctrl+U) to zoom out of the workspace.
- ZoomReset (Ctrl+T) to reset the zoom of the workspace.

Editing tools

- Copy (Ctrl+C) to copy the selected item.
- Paste (Ctrl+V) to paste the selected item.
- Undo (Ctrl+Z) to undo the previous action.

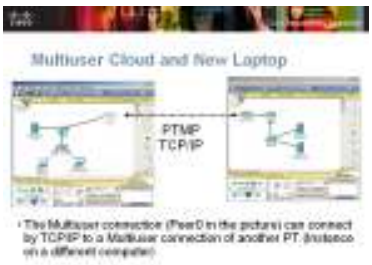
The drawing **Palette tool** (Ctrl+D) and **Device Template Manager**

A Cluster function

- Cluster function will group devices into a cloud.

A Move function

- Move will take a device and move it into or out of a cloud.

 Slide 5	Slide 5 – Create Bend Point
 Slide 6	Slide 6– Devices in PT 5.x
 Slide 7	Slide 7 – New Devices in PT5.x The new device: laptop-PT
 Slide 8	Slide 8 – Multiuser Cloud and New Laptop The Multiuser connection (Peer0 in the picture) can connect by TCP/IP to a Multiuser connection of another PT (Instance on a different computer)

Slide 9

Slide 9 – Device Template Manager

The Device Template Manager was added in response to a number of requests from instructors to be able to create pre-configured devices. The Device Template Manager allows you to save devices as templates and create devices from the saved templates.

1. To create a custom device template, first place a device on the workspace. Then add modules, if desired, and/or configure, if desired.
2. Click on the **Custom Devices Dialog** button.
3. Click on the **Select** button.
4. The Device Template Manager window will close. Now click on the device to make into a template.
5. The Device Template Manager window will reappear. Edit the name and add a description. Click the **Add** button.
6. PT4.1 or greater will prompt you to save your device template.

- To add a custom device on the Logical Workspace, click on the **Custom Made Devices** icon in the **Device-Type Selection Box** to display the custom devices in the **Device-Specific Selection Box**. Here you will find all of the device templates that have been created. You can then add the custom devices to the Logical Workspace as you would with other devices.
- To remove a custom device on the Logical Workspace, click on the **Custom Devices Dialog** on the **Main Tool Bar** to open the **Device Template Manager**. Under the Edit section, select the device template that you want to remove in the drop down menu and then click on the Remove button. The device template file that was saved in the 'templates' directory will be removed as well.

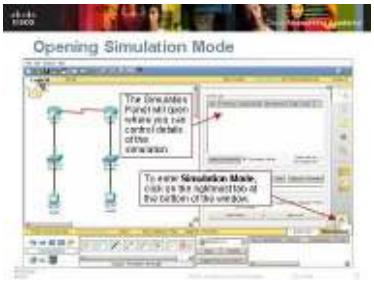
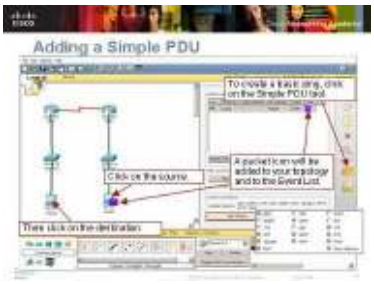
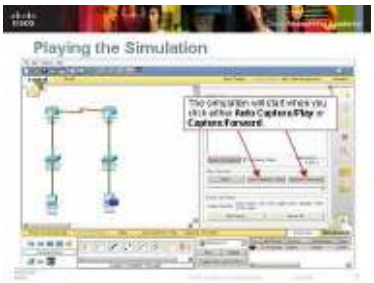
Slide 10

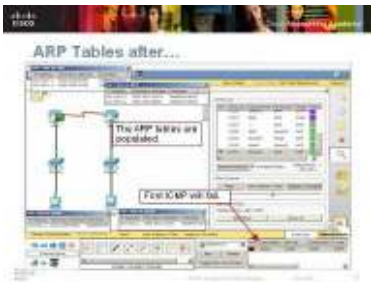
Slide 10 – Port Label Options and Other Options

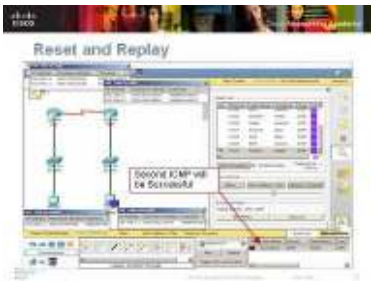
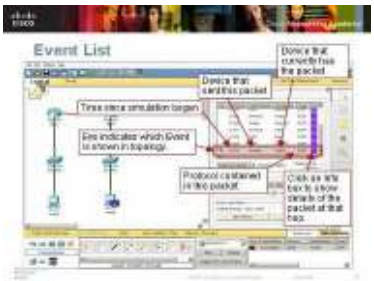
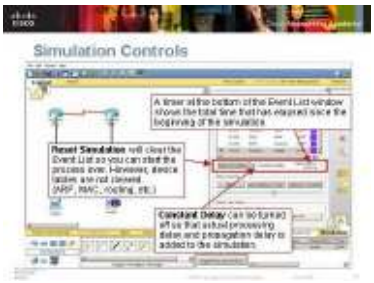
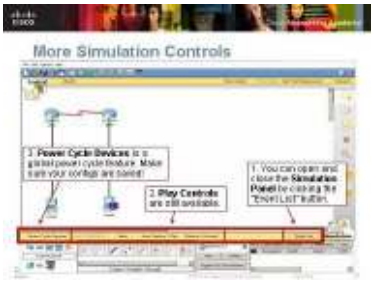
- Alternately, you can choose to have **Port Labels Always Shown** from the **Options** menu.
- Features in PT4.1 or greater are the **Show Link Lights** option and the **Hide Device Label** option. Use these options to show or hide the device link lights and the device labels.

 Slide 11	Slide 11 – Clustering Devices • PT4.1 or greater includes the feature of clustering devices to simplify the appearance of the Logical Workspace. Clustering reduces a group of devices and connections into a single image. • By default, devices are created in the Root level, which is indicated on the Logical/Physical Workspace Bar. In this slide, you see a small network of 4 PCs and a switch and this network is located at the Root level in the Logical Workspace. • To cluster this small network, select the devices on the workspace and then click on the New Cluster button. • To drill down into the cluster, simply click on the cluster. Notice in the navigational bar Cluster0 is listed. • To move back to the Root level, click on Root in the navigational bar. • To rename the cluster, click on its label to enable the label textbox. • To uncluster a group of devices, highlight the cluster and then delete it with the Delete tool.
 Slide 12	Slide 12 – Connect to a Device Within a Cluster • You can make a connection from a device outside of a cluster to a device within a cluster. In this example, the router is connected to the switch within the cluster using a copper straight-through cable. • Select the connection type of a copper straight-through cable. Click on the router and select one of the FastEthernet interfaces. • Then click on the cluster. From the menu, select Switch0 and then select one of the FastEthernet interfaces on the switch. • Let's say you have decided that the router should have been created within the cluster instead of outside of the cluster. You can move the router into the cluster using the Move Object button. • Click on the Move Object button • Also, when you can create a cluster, you can move objects and devices within the cluster hierarchy with the Move Object button. To do so, click on the Move Object button and then select an object or device. This opens a menu showing the cluster hierarchy. You can then select the location to which the object should be moved.

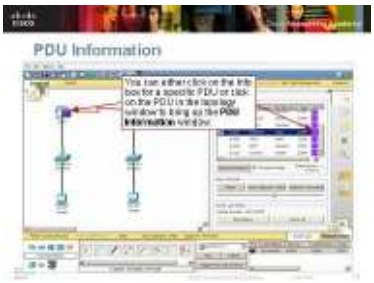
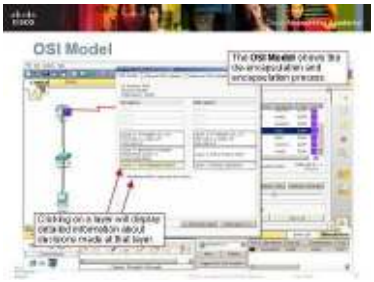
 Slide 13	Slide 13 – Multiple Device Windows • PT4.1 or greater supports multiple device windows open simultaneously. Notice in this slide there are two device windows open and visible simultaneously and they are independent of the main PT frame. Pop-up windows are now treated as independent windows so you can place them anywhere on the desktop. You can maximize and minimize windows by clicking the buttons in the Task Bar or by using the <**Alt**><**Tab**> key combination. You can have as many windows open as you need.
 Slide 14	Slide 14 – Where is the Activity Instructions Window? • Due to the feature of independent windows in PT, you may lose track of various windows. Remember you can maximize and minimize windows by clicking the buttons in the Task Bar or by using the <**Alt**><**Tab**> key combination. • In this slide, you see a screenshot of a Packet Tracer Activity launched from CCNA 1 Exploration 4.0. In a PT4.1 or greater Activity (a .pka file), it is not possible to close the Activity Instructions window. When you click on the Close button of the Activity Instructions window, the window is minimized in the Task Bar. • To maximize the window again, click on the **PT Activity** button in the Task Bar.
 Slide 15	Slide 15 – Simulation Mode Basics **Slides 15 – 27 (Simulation Mode)** Slides 15 & 16 give some overview information about Simulation Mode and how it can be used for instruction in the classroom. Use the speaker notes and your own experience to convey to instructors how Simulation Mode enhances their students' experiences. Slides 17-26 go over the Simulation Mode interface and controls. A simple PING is generated between 2 hosts and screen shots are used to show how the routers learn the MAC addresses of the hosts and then ultimately process the ICMP packets.
 Slide 16	Slide 16 – What is Simulation Mode? • Simulation Mode is the real power behind Packet Tracer. CCNA level students really benefit from the visual representations afforded by Packet Tracer. • The term "packet tracing" describes an animated movie mode where the learner can step through simulated networking events, one at a time, to investigate the complex networking events normally occurring at rates in the thousands and millions of events per second.

 Slide 17	Slide 17– Simulation Mode in Classroom Instruction • The packets are displayed graphically. The student can step the packet through the network, examining the processing decisions made by networking devices as they switch and route the packet to its destination. The networks, packet scenarios, and resulting animations can be annotated, saved, and shared.
 Slide 18	Slide 18 – Opening Simulation Mode • Note that when the file is opened the current mode is Realtime Mode. Packet Tracer defaults to Realtime Mode. • When using PT, you will be in Realtime or Simulation Mode. You can switch between them, by selecting the tabs in the lower right hand corner of the screen. • In Simulation mode, the Simulation Panel will open. Here you can control the precise details of a simulation when you create Simple or Complex PDUs.
 Slide 19	Slide 19 – Adding a Simple PDU 1. Click on the Add Simple PDU button to ping between two devices. **NOTE:** The Simple PDU button will create a single ICMP request from the source to the destination. If reachable, the destination will respond with a single ICMP reply. 2. Click on the source (HostB) for the ping packet 3. And then click on the destination (HostA) for the ping packet. 4. A packet icon will be added to the topology and to the Event List. 5. Use the "Event List Filters" to turn on and off specific packet types. When you filter for specific packet types, the "Event List" window will only display those packets.
 Slide 20	Slide 20 – Playing the Simulation • Once the Simple PDU (a ping) is created, you can use the "Capture/Forward" button to manually forward the packets one hop or event at a time. • You can also use the "Auto Capture/Play" button to have the animation play automatically. • The slider bar below the Play Control button allows you to control the speed of the animation.

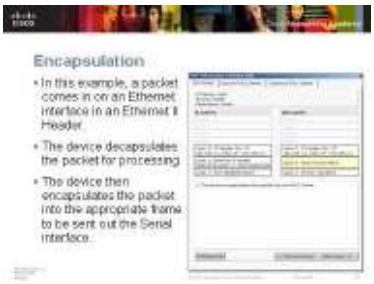
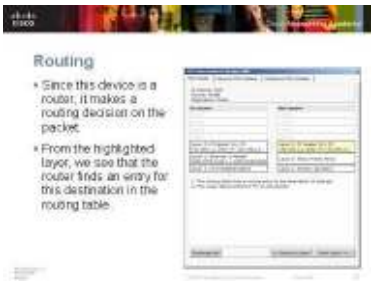
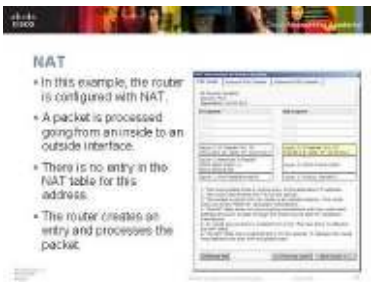
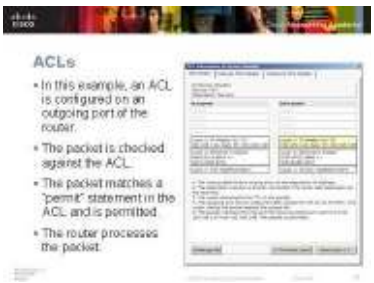
 Slide 21	Slide 21 – ARP Before PING! • If the destination MAC address is not in the ARP table, an ARP request will be generated. • The ARP request is not user generated. Packet Tracer will generate the ARP and put the packet in the Event List.
 Slide 22	Slide 22 – ARP Tables Before… • In the classroom, demonstrate why the ARP request must be generated. • Using the Inspect Tool (the magnifying glass), click on each host to view the ARP tables. • Show students the contents of HostB's and HostA's ARP tables before the ARP request is sent. The ARP tables are empty, since the hosts do not know the MAC addresses of any other devices. • The PING will not be successful until the ARP tables contain the necessary MAC addresses. • Play the simulation using Auto Capture/Play (control speed with slider) or Capture/Forward to go hop by hop.
 Slide 23	Slide 23 – ARP Tables After… • You can keep the ARP table windows open as the ARP requests traverse the network to see entries as they are added to the tables. • For the PING from HostB to HostA to be successful, all devices must populate their ARP tables with the needed entries. • One important thing to note here… Even after the ARP tables are populated, you will see an indication that the ICMP PDU has "Failed". This is because Packet Tracer only generates ONE packet when creating a Simple PDU. When the ARP tables are empty, the first packet will fail. Just like in a real network when the ARP table does not contain the needed MAC addresses, the first PING will timeout and subsequent PINGs will be successful. • So, in order to get a successful ICMP here, you will need to "Reset Simulation" and play again. This is equivalent to the 2nd PING packet going across the network.

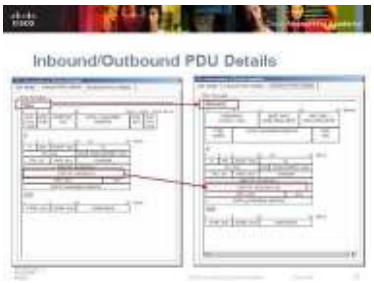
 Slide 24	Slide 24 – Reset and Replay • After the ARP tables are populated, Reset the Simulation and play it again. • You will see the ICMP PDUs traverse the network and return to HostB. The Event List window will show the Last Status as Successful.
 Slide 25	Slide 25– Event List Each hop or event will be listed in the “Event List” window. • The eye in the far left column of the “Event List” indicates which event is being shown in the topology. • “Time” indicates how long this simulation has been running. • “Last Device” indicates which device sent this packet. • “At Device” indicates which device currently has the packet in memory. • “Type” is the protocol of the packet. This column will list one of the PDU types supported by Packet Tracer. • Each colored square under “Info” is clickable. Clicking on an Info box for a particular event will display details about the PDU at that point in its progress from source to destination. (More on this later…)
 Slide 26	Slide 26 – Simulation Controls • A timer at the bottom of the Event List window shows the total time that has elapsed since the beginning of the simulation. • “Constant Delay” can be turned off so that actual processing delay and propagation delay is added to the simulation. • The “Reset Simulation” button can be clicked to start the simulation over. However, this will not clear tables that are currently in a device’s memory.
 Slide 27	Slide 27 – More Simulation Controls • You can hide the Simulation Panel completely by clicking on the Event List button. • Play Controls are still available even though the Simulation Panel is closed. • The “Power Cycle Devices” button will power cycle all devices in your topology. (the global power cycle button) Use this button to clear tables from device memory. If you have not saved configurations to NVRAM, then the devices will start up without a configuration. So this button is also a good way to reload all devices if you wish to start over with no configurations. Just make sure NVRAM is empty first. • “Power Cycle Devices” button will clear any tables from memory because all devices are reloaded.

	After slide 27, open the .pkt file (Intermediate_1.pkt) to demonstrate each of the tasks described in the screen shots: 1. After "spanning tree" completes and all links turn green, switch to Simulation Mode. 2. Create a Simple PDU from HostB to HostA. 3. Point out that PT generated an ARP PDU in the Event List. 4. Open the ARP tables for HostA, HostB, BHM and GAD and arrange them so that you can see the topology and the Event List window. Point out that the only entries in the ARP tables for the routers are for the directly connected interfaces. The ARP tables of the hosts should be empty. (Note: If other addresses are in the ARP tables, use the Power Cycle Devices button to clear them out. Remember to switch to Realtime Mode to allow spanning tree to recalculate before returning to Simulation Mode.) 5. Click the Capture/Forward button. Point out that the ARP PDU goes first and the MAC address for HostB is added to the BHM router. 6. Continue to click the Capture/Forward button and watch as the ICMP PDU goes from HostB to GAD. Note that the ICMP will fail at GAD. 7. Continue to click Capture/Forward and watch as GAD sends an ARP request to HostA. When the ARP is returned, the ARP table on GAD is populated with the MAC address of HostA. 8. Point out that the Event List indicator in the bottom right of the screen lists the ICMP PDU as "failed". This is because the first PDU does fail due to the lack of MAC address in the ARP tables. 9. Now that the ARP tables are populated, Reset the Simulation and try the PING again. This time the ICMP PDU travels successfully from HostB to HostA. Point out that the Event List indicator now reads "Successful" for this packet. 10. Demonstrate hiding and unhiding the Event List window.
 Slide 28	Slide 28 – PDU Information **<u>Slides 29 – 40 (PDU Information)</u>** Slides 29-40 describe and demonstrate how the PDU information window can be used to show students what's "inside" the packet and how devices are processing the packets based on their contents. The screen shots show how to open the PDU Information window and navigate the various tabs: OSI Model, Inbound and Outbound. Several examples of PDU information in the OSI Model are shown and what learning opportunities each presents. Please note that some of these screen shots apply to the topology used in this presentation, and some of them are from another .pkt file.

 Slide 29	Slide 29 – What is PDU Information? • The PDU Information window allows you to "open" a packet and look inside to see how it is being processed at each layer of the OSI Model. • It's like a very simple sniffer, presenting CCNA level information. • Students may be overwhelmed by the PDU Information window at first glance. Remember that you can direct them to look at specific fields in the window. This will help them to use the information provided without feeling "lost" in the fields they don't understand.
 Slide 30	Slide 30 – PDU Information • In the Event List window, if you click on the box under Info for a specific step you will open the "PDU Information" window for the PDU at that particular device. • You can also click on the PDU packet envelope in the topology window to open the "PDU Information" window.
 Slide 31	Slide 31 – OSI Model • The "PDU Information" window has three tabs: OSI Model, Inbound PDU Details, and Outbound PDU Details. • The **OSI Model** tab shows how the packet is processed at each layer of the OSI model by the current device. The process is further separated by the direction in which the packets are traveling—incoming versus outgoing. The incoming layers (**In Layer**) show how the device processes an incoming or a buffered packet, and the outgoing layers (**Out Layer**) show the process a device goes through when it sends a packet to one or multiple ports. • Layers are grayed out if the packet was not processed by that layer. In this example the ICMP packet is processed up through Layer 3 by the router. • The **In Layer** is meant to be read starting from bottom to top (from Layer 1 to Layer 7), while the **Out Layer** is read from top to bottom (from Layer 7 to Layer 1). This is because the physical layer is the first layer that incoming PDUs encounter, and it is the last layer that outgoing PDUs pass through when they exit the device. • Clicking on each layer will show detailed information about the processing at that layer of the OSI model. When a layer is selected, it will be highlighted in yellow. Text in the bottom of the window will give details about the processing.

 Slide 32	Slide 32 – How can I use the OSI Model Tab? • Demonstrate how switches process only to layer 2 (no layer 3 switches in PT) and routers process to layer 3. • Show what happens to a packet with no ARP table entry. • Show encapsulation and decapsulation to accommodate different interfaces. An Ethernet frame is changed to an HDLC frame when going from an Ethernet interface to a Serial interface. • Show routing decisions. When a packet is at a router, the router will make a routing decision about the packet…either forwarding it or dropping it based on routing table entries. • Show operation of an ACL. • Show operation of NAT. • Many other ways!
 Slide 33	Slide 33 – Packet at Layer 2 Device • When students first begin to look at PDU Information, remember to keep their tasks simple. • Here the packet is at a layer 2 switch. Notice that the packet is only processed up through Layer 2 of the OSI Model. • In this example, you might ask students to see how many layers “up” a device will process a packet. They could compare switches and routers, for example, to see that switches process up to layer 2, while routers process up to layer 3. • You can also point out which addresses each device is using. Again reinforcing their understanding of layer 2 and layer 3 devices and addresses.
 Slide 34	Slide 34 – No ARP Table Entry • Many students do not understand the relationship between layer 2 and layer 3 addresses and how they are used. One of the concepts that is very difficult for students to “see” in a real network is how ARP is used by various devices. In this example we can use the PDU Information window to see why the ARP request was generated in our Simulation scenario. • In this example, the router does not have an ARP Table entry for the next hop. An ARP is generated. The packet is dropped.

 Slide 35	Slide 35 – Encapsulation • A very simple way to use the PDU Information window is to show students that different interface types use different encapsulation. • In this example, a packet comes in on an Ethernet interface in an Ethernet II Header. • The device decapsulates the packet for processing. • The device then encapsulates the packet into the appropriate frame to be sent out the Serial interface.
 Slide 36	Slide 36 – Routing • The routing decisions made by routers in your PT topology provide opportunities for students to understand the routing process and how and if a packet will be routed. • Since this device is a router, it makes a routing decision on the packet. • From the highlighted layer, we see that the router finds an entry for this destination in the routing table.
 Slide 37	Slide 37 – NAT • A more advanced use of PDU information is to allow students to see processing of more complex configurations. • In this example, the router is configured with NAT. A packet is processed going from an inside to an outside interface. There is no entry in the NAT table for this address. The router creates an entry and processes the packet.
 Slide 38	Slide 38 – ACLs • Packet Tracer is an excellent way for students to learn to configure, test and troubleshoot ACLs. They can create very complex network topologies and easily test ACL configuration on various devices. The PDU Information window shows them exactly if, where, and when their ACL is applied. • In this example, an ACL is configured on an outgoing port of the router. The packet is checked against the ACL. The packet matches a “permit” statement in the ACL and is permitted. The router processes the packet.

 Slide 39	Slide 39 – Inbound/Outbound PDU Window • Both the “Inbound PDU Details” and “Outbound PDU Details” tab will display the details of PDU headers starting with Layer 2 at the top.
 Slide 40	Slide 40 – Inbound/Outbound PDU Details • This example shows the contents of the IP fields for a packet that had a NAT entry in the router NAT table. This packet comes into the router on a Serial interface and will leave the router on an Ethernet interface. • Notice that when the packet comes into the router the destination IP is 195.56.5.9. The router looks up this entry and finds it in the NAT table and replaces it with the local address of 192.168.1.35. • Notice that the encapsulation changes from HDLC to Ethernet II.

	After Slide 40, switch to Packet Tracer and use the .pkt file (Intermediate_2.pkt) to demonstrate the following: 1. Open the file and wait for spanning tree to complete and all links to turn green. 2. Switch to **Simulation Mode**. 3. Click the **Auto Capture/Play** button to run through the simulation. Remember that this first ping will fail since the ARP tables are not populated. 4. Click the **Reset Simulation** button. Click the **Capture/Forward** button until the packet from PC3 arrives at the router Houston. 5. Click on the packet icon in the topology to open the PDU Information window. 6. Click on Layer 3 in the Out Layers to show the details. Point out that we can see from the information provided that the router checked the packet against an access-list. The packet matched a "permit" statement and the packet was sent to Layer 2 for processing. 7. Show other layers, if desired. 8. Close the PDU Information window and continue to click the **Capture/Forward** button until the ping from PC3 completes. You will see a green check mark on PC3 when the ping reply arrives at PC3. 9. Click the **Capture/Forward** button to begin the ping from PC4 to the External Web Server. You will know that the new packet is beginning because a different color will show up in the Event List. Stop clicking the button when the packet arrives at the Houston router. 10. Click the packet icon in the topology to open the PDU Information window. 11. Click on Layer 3 in the Out Layers. Point out that the information provided allows us to see that the router replaced the address of the packet in accordance with the NAT configuration. 12. As a special treat, show instructors the NAT table of the Houston router. Do this by closing the PDU Information window and then using the Inspect tool to open the NAT table of the Houston router.
 Slide 41	Slide 41 – Complex PDUs **Slides 41 – 47 (Complex PDUs)** Slides 41-47 describe and demonstrate how to create and use Complex PDUs. Point out to instructors that Complex does not mean complicated, rather it refers to the ability to control more parameters of the packet. Remind them that a Simple PDU is a ping and that sometimes they will need to create a packet other than ping to test ACLs, NAT, connectivity, etc. Show the slides and screenshots of the program. These will walk instructors through creating and editing PDUs as well as offer some good ideas about workspace management.

<table>
<tr>
<td>

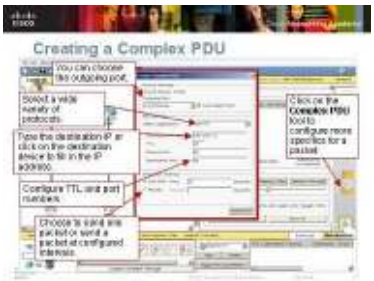

Slide 42
</td>
<td>
Slide 42 – Why would I want a Complex PDU?

When you create a Simple PDU, you are creating an ICMP packet. The default parameters of a Simple PDU may not be appropriate for your testing purposes.
For instance, you may need to generate a packet that comes FROM a specific IP address and goes TO a specific IP address.
You may need to create a packet to test an ACL. If the ACL is designed to permit or deny specific protocols, you will need to create a Complex PDU to test whether or not the ACL is working properly.
Creating a Complex PDU allows you to control parameters of the packet such as:

Protocol
Source and Destination IP
Port
TTL
Sequence number

This granular control allows you to test packets against ACLs. This also allows you to test connectivity to specific interfaces on a device.

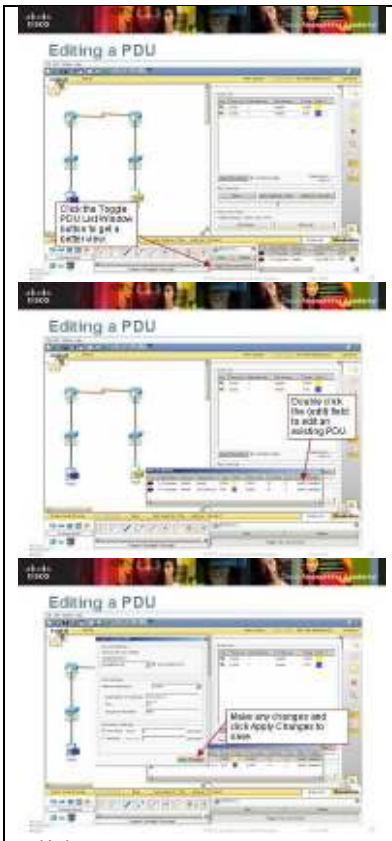
</td>
</tr>
</table>



Slide 43

Slide 43 – Creating a Complex PDU

- Click on the Complex PDU button then click on the source device to create a packet other than an ICMP ping packet or to specify more options in a ping packet.
- After you click on the source device (HostB) for the Complex PDU, the “Create Complex PDU” window opens as shown.
- Select the **Outgoing Port**. You can specify the outbound interface or let it be chosen automatically. In this example, the PC only has one possible choice for outbound interface, but a router will have multiple choices.
- Select the **Application**. You can change the TCP application to test ACL configurations on routers. In PT4.1 or greater, you can setup a web server and with an ACL you can permit or deny HTTP traffic to that server. **NOTE:** Based on the choice of application, the available and required fields will change.
- Configure the **Destination IP Address**. Clicking on the destination device (HostA) will choose the IP address of the closest interface to the source. To test connectivity to another IP address on the destination, you can type it in.
- Configure **TTL**. TTL defaults to 32. You can change this to another value. This can be useful when exploring routing loops or routing protocols.
- Configure **Source** and **Destination Ports**. For an HTTP and other packets – The source port is required. This is also a place where changing the port can be useful when testing configuration of an ACL.
- Configure **Sequence Number** (not shown) if required. For a PING - The sequence number is used by devices to track individual pings. Therefore, you must provide a sequence number. Any random number between 1 and 65536 will do.
- Configure **Simulation Settings**. You can specify that this Complex PDU be a one shot packet or have it repeat periodically. Either way, you must specify the seconds. A setting of 0 begins this PDU immediately when the simulation is played.



Slide 44

Slide 44 – Editing a PDU

After a PDU is created, it can easily be edited.

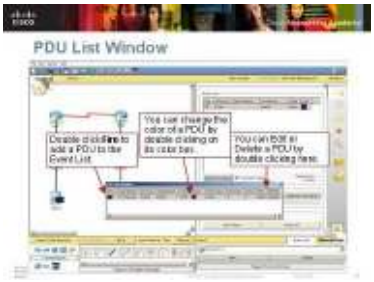
- To get a better view of the PDUs in your simulation, use the Toggle PDU List Window button to “float” the PDU List window. This window can be moved and resized as needed.
- From the list of PDUs in the window, select the one you wish to edit and double click the (edit) field for that PDU. **NOTE:** PDUs can be deleted from the list by double clicking the (delete) field from this window.
- A window will open showing the details of the PDU and will allow you to make changes.
- Click the Apply Changes button to save and close the window.

Slide 45

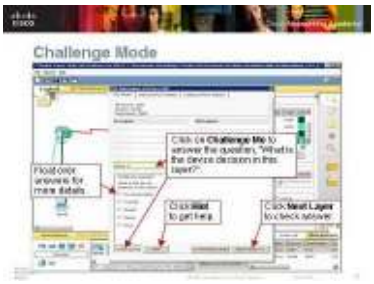
Slide 45 – Managing Your Workspace

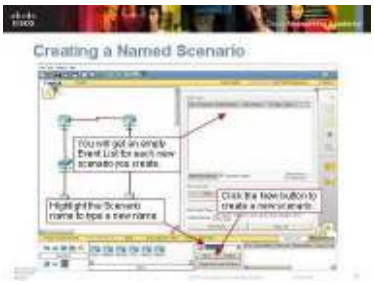
- Double-click on the Simulation Panel title bar to undock it so you can move it to a more convenient place. Note that you can actually drag the subwindow outside of the Packet Tracer window if you have a large monitor.

 Slide 46	Slide 46 – Using Command Prompt in Simulation Instructors can continue to use the Command Prompt even in Simulation Mode. This can be helpful when bridging the gap between “real” equipment and a simulation. The Command Prompt is familiar and trusted. • Once you have undocked the Simulation Panel, you can move the panel. This will allow you to access other windows, such as the Command Prompt window of a PC. • In Simulation Mode, you can still access the command line of devices. For example, you can access the command line of a PC and enter the **ping** command. Entering the command in the Command Prompt window of the PC will cause a packet to be added to the Event List window. • Then, you can watch the pings as they cross the network by using the Simulation Panel to start the animation. • Click on “Auto Capture/Play” to start the pings. • **NOTE:** Using the Command Prompt to generate pings will not add a PDU to the PDU List Window.


Slide 47
	Slide 47 – PDU List Window
	• The PDU List Window displays properties for each PDU created. Double-clicking on the red “Fire” button will add the PDU to the Event List. For instance, if you want 4 pings, you can create the first one and then double click the Fire button 3 times to add 3 more.
	• Most of the fields in the “PDU List Window” are self-explanatory. To change a field’s position in the table, click and drag it to the desired location.
	  • You can click on the color of the PDU to change its color.
	  • Time refers to the timing in the Event List.
	  • Periodic indicates whether this is a one shot PDU (“N”) or a PDU that repeats (“Y”).
	  • “Num” refers to the order that this PDU was created.
	  • Double-clicking on “Edit” allows you to change the specifics of this PDU.
	  • Double-clicking on “Delete” will delete this PDU.

	After Slide 47, switch to Packet Tracer and use the .pkt file (Intermediate_3.pkt) to demonstrate creating and editing Complex PDUs: 1. Open the .pkt file (Intermediate_3.pkt) and allow spanning tree to run in Realtime Mode before switching to Simulation Mode. 2. From Simulation Mode, click on the BHM router and look at its configuration. You should see that an access list has been configured and applied that blocks FTP (port 21) from hosts on the FastEthernet LAN. 3. To test functionality of this ACL, we will first create a Simple PDU and see that it is not blocked (remember that a Simple PDU is a ping and we haven't blocked ping). 4. Create a Simple PDU from HostB to HostA. Remember that this first run through will not work because the ARP table is not populated yet. Run the first one and then Reset the Simulation and then run it again. The ping should be successful. 5. In order to test the ACL we need to create a Complex PDU. First delete the existing Ping packet from the PDU List. 6. Next click the Complex PDU button and click HostB to begin defining the parameters of the PDU. 7. Complete the fields of the PDU as illustrated below: Outgoing Port: FastEthernet Check the "Auto Select Port" Select Application: FTP Destination IP Address: 192.168.1.2 TTL: 32 Source Port: 21 Destination Port: 21 Simulation Settings : One Shot Time : 0 8. Click the Create PDU button and play the simulation. The packet should stop at the BHM router and be marked with a red X. 9. Click the packet with the red X. Click Layer 3 in the outbound column. 10. Point out how we needed to use a Complex PDU in order to test the ACL, since the ping packet went through successfully, and only the FTP packet was blocked. 11. To illustrate how the Command Prompt window can be used in conjunction with the Simulation panel, undock the Simulation panel and move it to the right side of the screen. 12. Open the Command Prompt of HostB, and issue the command: ping 192.168.1.2. This will place a ping packet in the simulation window, but will not begin the ping until you use the play buttons. 13. Use the Auto Capture/Play button to process the pings. Notice that you can see the replies in the Command Prompt window as they return to HostB.

 Slide 48	Slide 48 – Challenge Mode
 Slide 49	Slide 49 – Challenge Mode • Students can quiz themselves on the encapsulation process by entering Challenge Mode. • The **Challenge Me** button from the OSI Model tab of the PDU Info window starts Challenge Mode. • The layer details are hidden, and the information window is replaced by a question window that asks what the device does to a PDU on a given layer. • Students select from a multiple-choice list. If they answer correctly, the details for that layer are shown and the question window advances to the next layer. • The **Hint** button provides hints.
 Slide 50	Slide 50 – Challenge Mode • Clicking on “Challenge Me” will allow you to answer the question, “What is the device decision at this layer?” for each layer of processing. • Floating over the possible answers will provide more information about that process. • You can also click on “Hint” for more information. • Click on Next Layer button to check your answer. • Packet Tracer will remain in Challenge Mode until the Challenge Me button is clicked again.
 Slide 51	Slide 51 – Scenario


Slide 52
	Slide 52 – Creating a Named Scenario
	• You can create named scenarios that are useful when testing specific connections. These scenarios can be especially helpful when you are working with a complex network that contains ACLs, NAT translations or complex subnetting schemes.
	• To create a new scenario, click on the “New” button in the Scenario window.
	  • This will give you a fresh Simulation Panel with an empty Event List without erasing the previous events.
	  • Change the Scenario name by highlighting it and then typing the new name. Use a descriptive name that will help you to remember what this scenario is designed to test.

 Slide 53	Slide 53 – Adding a Scenario Description • You can add information about the scenario by clicking the Info button and then typing in your description.
 Slide 54	Slide 54 – Interested in More Help? • Packet Tracer has extensive built in Help. • Access this help by clicking the “?” in the upper right hand corner of the program. (You may need to turn your pop-up blocker off to use all of the features of the Help file.) • The help files are designed to familiarize users with the Packet Tracer interface, functions, and features. Although they can be used as a reference guide, the pages are meant to be read in order (especially the sections presented at the beginning of the guide).
 Slide 55	Slide 55 – Reference Topologies PT comes with a number of built-in Activities which can be found in the “saves” folder. Notice the directory path in this slide. . Currently, the Exploration and Discovery directories shown in this slide will not be there. They will be available from the same locations as the rest of the auxiliary materials. Although the program includes some activities, we strongly encourage you to share activities that you create with others in the CCNA teaching and learning community.

 Slide 56	Slide 56 – Q and A
 Slide 57	