### 3323

**Activity 3.3.2:   
Network Representations**

**Addressing Table:**

This Lab does not include an Addressing Table.

**Learning Objectives:**

* Configure services and support
* Configure DNS on the Server
* Confirm HTTP on the Server
* Configure DNS support on the PC
* Verify Connectivity in Realtime Mode
* Ping the Server using the URL **www.example.com**
* Open web page on the Eagle Server using the URL
* View how DNS and HTTP work together using Simulation Mode

**Introduction:**

In this activity, you will configure a Server to provide DNS services and to host a web page, configure a PC to use DNS services, and view how DNS and HTTP work together.

**Task 1: Configure services and support**

**Step 1. Configure DNS on the Server.**

Click on the Server. The server configuration window opens, Click the **Config** tab. The **Global Settings** appear. Click the button on the left for **DNS**. Verify the service is **On**. Set the **Domain Name** to www.example.com and the **IP Address** to 192.168.1.254. Click the **Add** button. Additional domain names can be added in this fashion.

**Step 2. Configure HTTP on the Server.**

Click the button on the left for **HTTP**. Turn the service **On**. The **Default Page Content** window contains the page that is displayed when a web page is requested using the server's IP address. This page is in HTML format. This page can be changed if you would like to customize it. Close the server configuration window.

**Step 3. Configure DNS support on the PC labeled Client**

**//**

**5.6.1: Skills Integration Challenge-Routing IP Packets**

**Topology Diagram:**

Partial topology given; must be completed.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **Default Gateway** |
| **R1-ISP** | **Fa0/0** | 192.168.254.253 | 255.255.255.0 | N/A |
| **S0/0/0** | 10.10.10.6 | 255.255.255.252 |
| **R2-Central** | **Fa0/0** | 172.16.255.254 | 255.255.0.0 | N/A |
| **S0/0/0** | 10.10.10.5 | 255.255.255.252 |
| **S1-Central** | **VLAN 1** | 172.16.254.1 | 255.255.0.0 | 172.16.255.254 |
| **PC-PT 1A** | **NIC** | 172.16.1.1 | 255.255.0.0 | 172.16.255.254 |
| **PC-PT 1B** | **NIC** | 172.16.1.2 | 255.255.0.0 | 172.16.255.254 |
| **Eagle Server** | **NIC** | 192.168.254.254 | 255.255.255.0 | 192.168.254.253 |

**Learning Objectives:**

* Configure a router interface using a GUI
* Explore a routing table
* Configure a static route using a GUI
* Explore the routing of IP packets

**Background:**

Throughout the course, you will be using a standard lab setup created from actual PCs, servers, routers, and switches to learn networking concepts. At the end of each chapter, you will build increasingly larger parts of this topology in Packet Tracer, and analyze increasingly more complex protocol interactions. You have already studied a variety of application protocols, such as DNS, HTTP, TFTP, DHCP, and Telnet, and two transport layer protocols, TCP and UDP. You may have noticed that regardless of what application and transport protocols were involved, in **Inbound** and **Outbound PDU Details** view they were always encapsulated in IP Packets. In this activity, we will examine how the Internet Protocol, the dominant network layer protocol of the Internet, works in the context of a simple example of IP routing.

**Task 1: Configure a router interface**

There are problems on the local area network: PC-PT 1A cannot communicate with the Eagle Server (verify this in Realtime mode by pinging Eagle Servers IP address: 192.168.254.254). It appears there is a problem with the router. Mouse over the R2-Central router, and note the condition of the Fa0/0 interface (to which S1-Central is connected). This interface must have an IP address, subnet mask, and be turned on in order to act as the default gateway for the LAN. Click on router R2-Central, and go to the **Config** tab. At the end of the course, you will learn how to use the Cisco Internetwork Operating System (IOS) command line interface (CLI) to perform this task. For now, the **Config** tab is easier and will allow you to focus on the basic idea of IP routing. In the list shown, find **INTERFACE, FastEthernet0/0**. Add the IP address 172.16.255.254 with subnet mask of 255.255.0.0, and turn the port on. Close the router window. Verify that the router interface (port) is now working by using the mouse over. Try reaching Eagle Server. The request still fails. What are some possible reasons why? 

**Task 2: Examining routes**

Use the **Inspect** tool (magnifying glass) to examine the routing table of R2-Central. You will see the router's directly connected networks, but there is no way to reach the Eagle Server network. 

**Task 3: Configure a route using a GUI**

Click on router R2-Central and go to the **Config** tab. In the list shown, find **ROUTING, Static**. Configure a default static route, using the address 0.0.0.0, mask 0.0.0.0, and the next hop of 10.10.10.6 (the S0/0/0 interface on the R1-ISP router) and click the **Add** button. This route is configured so that wherever packets from the 172.16.0.0 /16 LAN are destined, they will go to the R1-ISP router. Under **GLOBAL, Settings**, click on the **Save** button to save the interface and route configuration you have just done to NVRAM in case the router is power cycled. Use the **Inspect Tool** (magnifying glass) to examine the routing table of R2-Central again. You should now see the route you configured in the routing table.   
  
Verify your work using feedback from the **Check Results** button and the **Assessment Items** tab. Test connectivity, in Realtime, by using ADD SIMPLE PDU to test connectivity between PC-PT 1A and the Eagle Server. The PDU, a one-shot ping, will appear in the User Created PDU List for future use as well. The first ping attempt will fail because the ARP tables are not populated; double click on **Fire** to send it again - this should be successful. 

**Task 4: Examine the routing of the IP packet**

Switch to Simulation mode. Using the PDU you created in Task 3, trace the packet's journey from PC-PT 1A to Eagle Server and back using the **Capture / Forward** button and examining the packet's contents by either clicking on the envelope or clicking on the colored square in the **Info** column of the **Event List**. 

**Reflection:**

What data can an IP Packet contain? What is meant by the phrase "the IP packet is routed"? What is a route? Where might things go wrong? 

Click on PC Client. The PC configuration window opens, Click the **Config** tab. The **Global Settings** appear. Set the **DNS Server** to **192.168.1.254**, the IP address on the Server. Close the PC configuration window.

**At the end of this task your completion rate should be 100%.**

**Task 2: Verify Connectivity in Realtime Mode**

**Step 1. Ping the server using the URL.**

Click the **Desktop** tab. Click the **Command Prompt**button. A Command Prompt window opens. Type **ping www.example.com** (the URL of the Server) and press Enter. After the ping succeeds, close the Command Prompt window.

**Step 2. From the PC, Open a Web Page.**

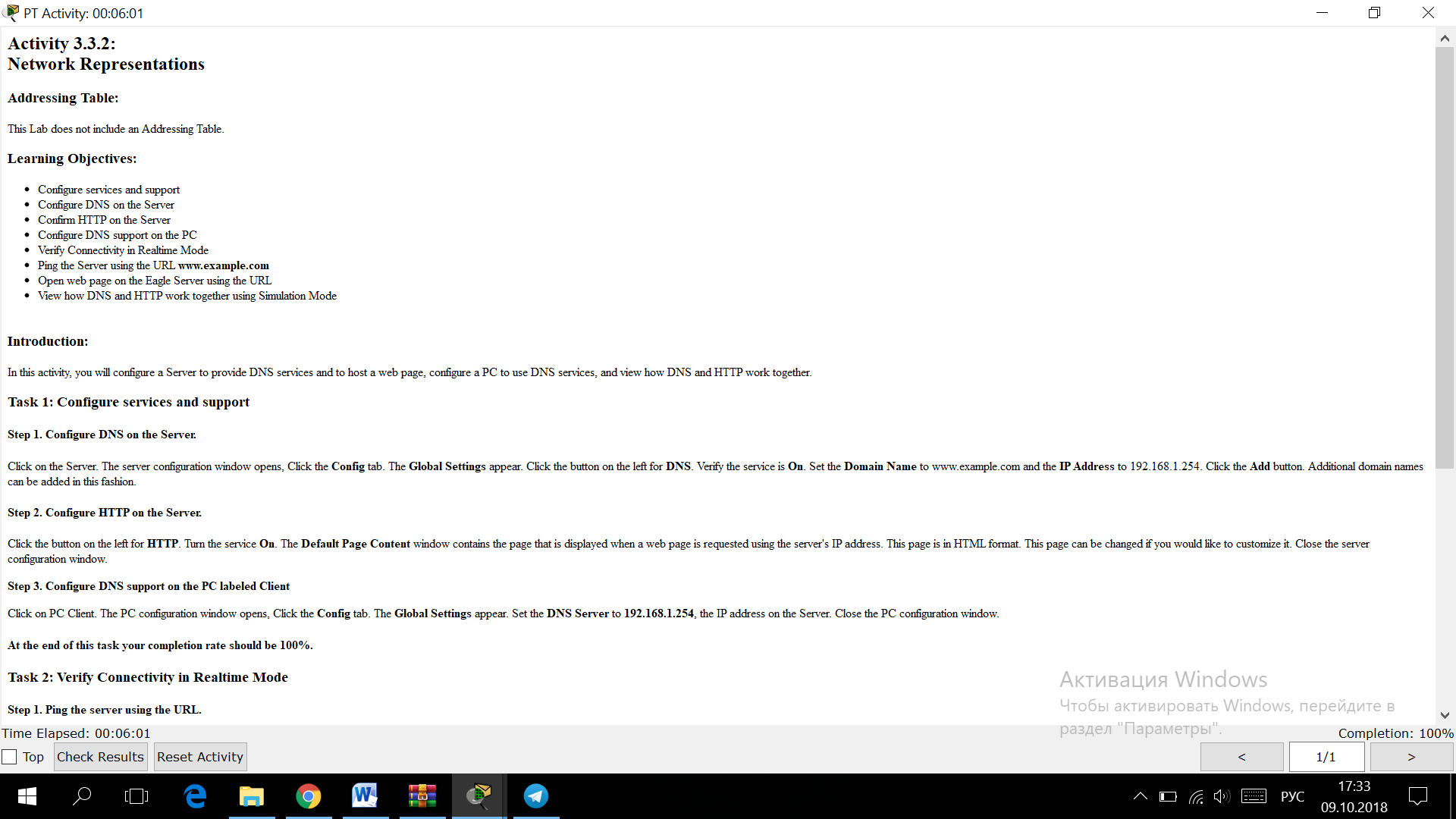
From the PC desktop, click the **Web Browser** button. A simulated web browser opens. Type www.example.com (the URL of the Server) into the **URL** box and click the **Go** button. A web page should appear. Close the PC configuration window.

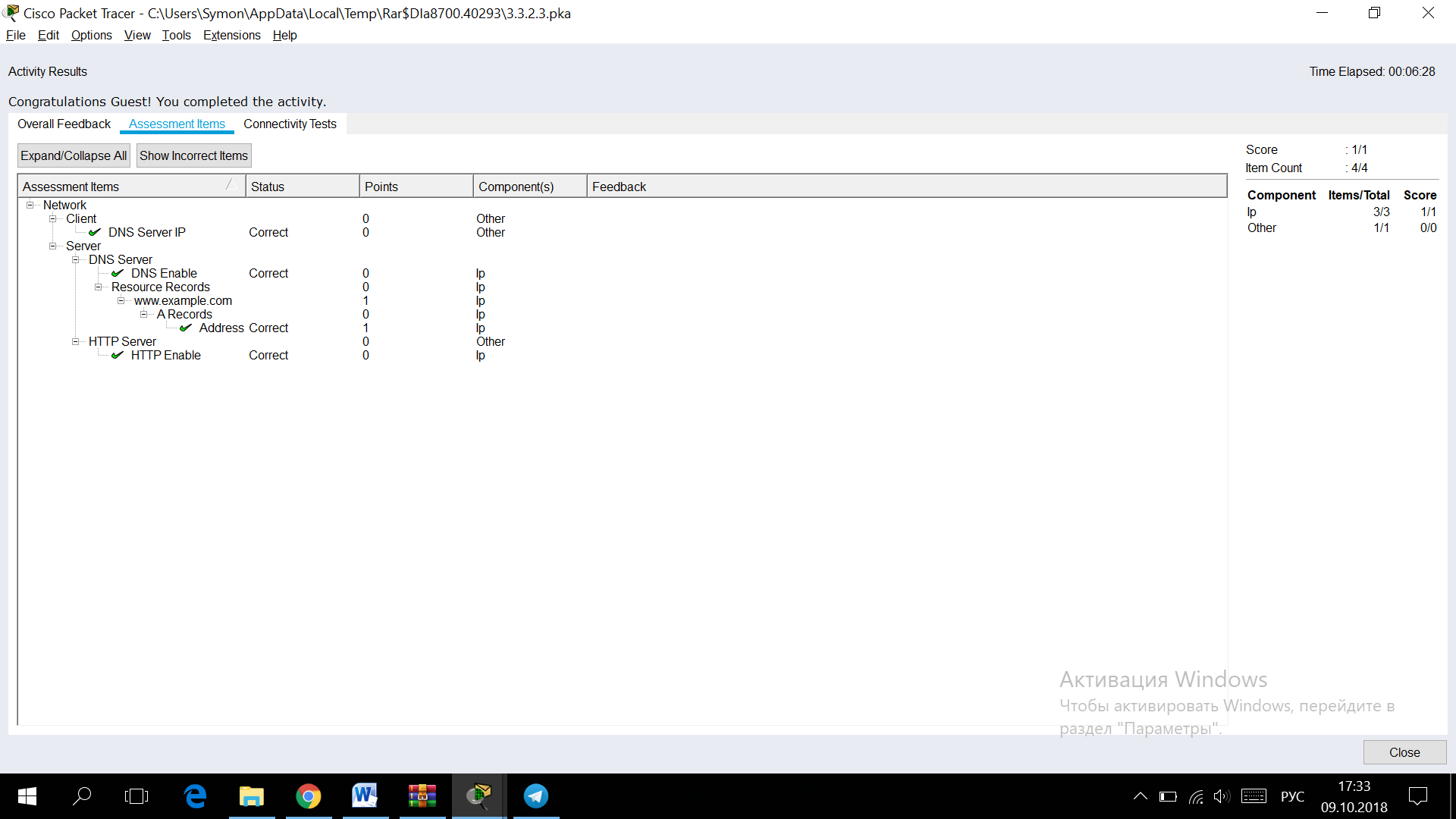
**Task 3: View how DNS and HTTP work Together using Simulation Mode**

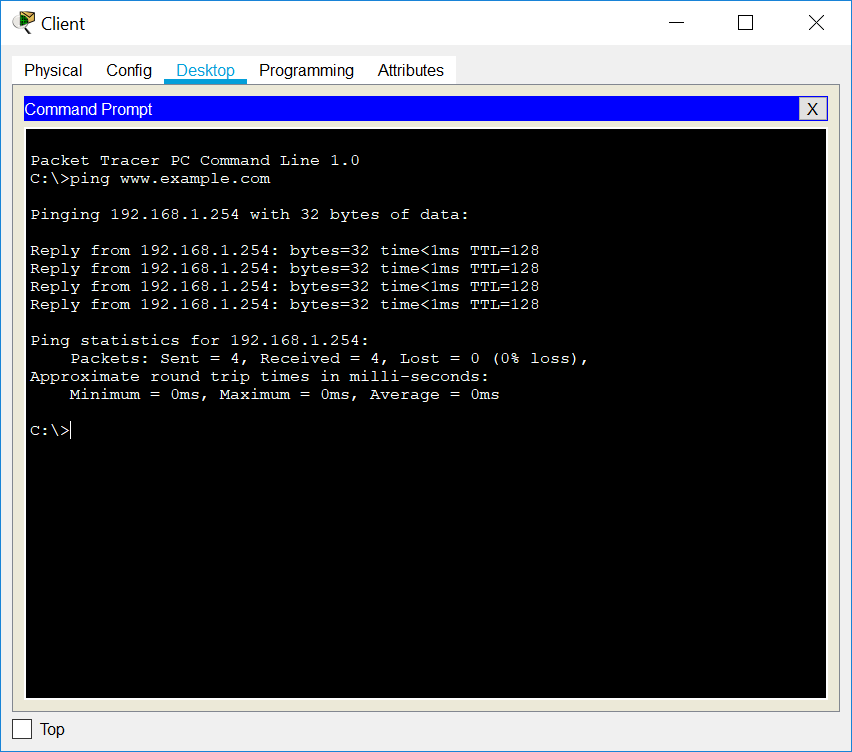
**Step 1. Ping the Server using the URL**  
Enter Simulation Mode. Click on PC Client. The PC configuration window opens. Click the **Desktop** tab. Click the **Command Prompt**button. A Command Prompt window opens. Type ping www.example.com (the URL of the Server) and press Enter. Minimize the simulated Command Prompt window.Use Capture/Forward to view the DNS and ICMP packets on the network. Each time you click the Capture/Forward the packet transfer process will proceed another packet or two. Anytime during this process you can click on the colored square in the Info column to open the PDU information and view encapsulation and device processing details. Close the command prompt window; click on the**Reset Simulation** button.

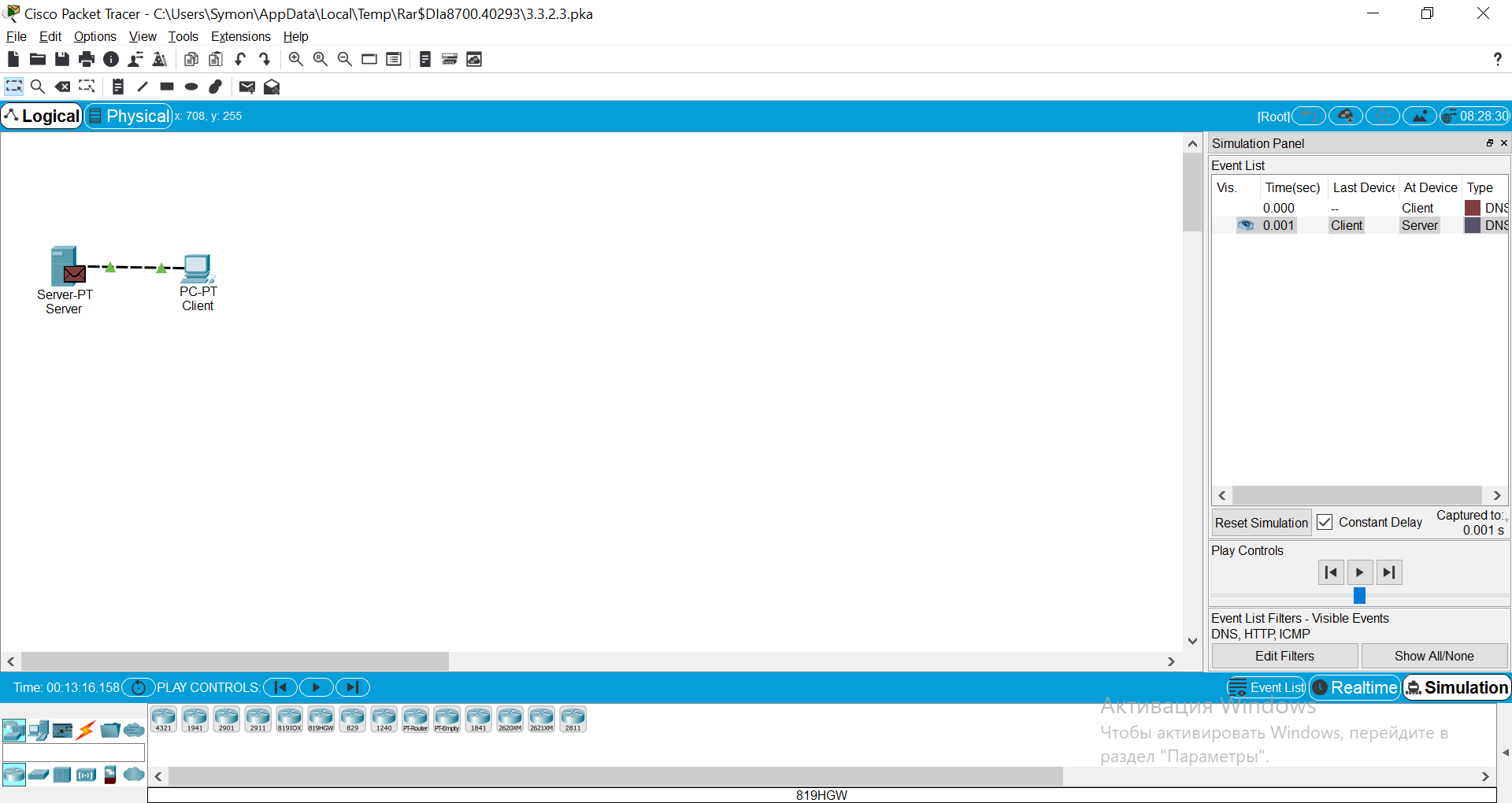
**Step 2. Open web page on the Server using the URL**

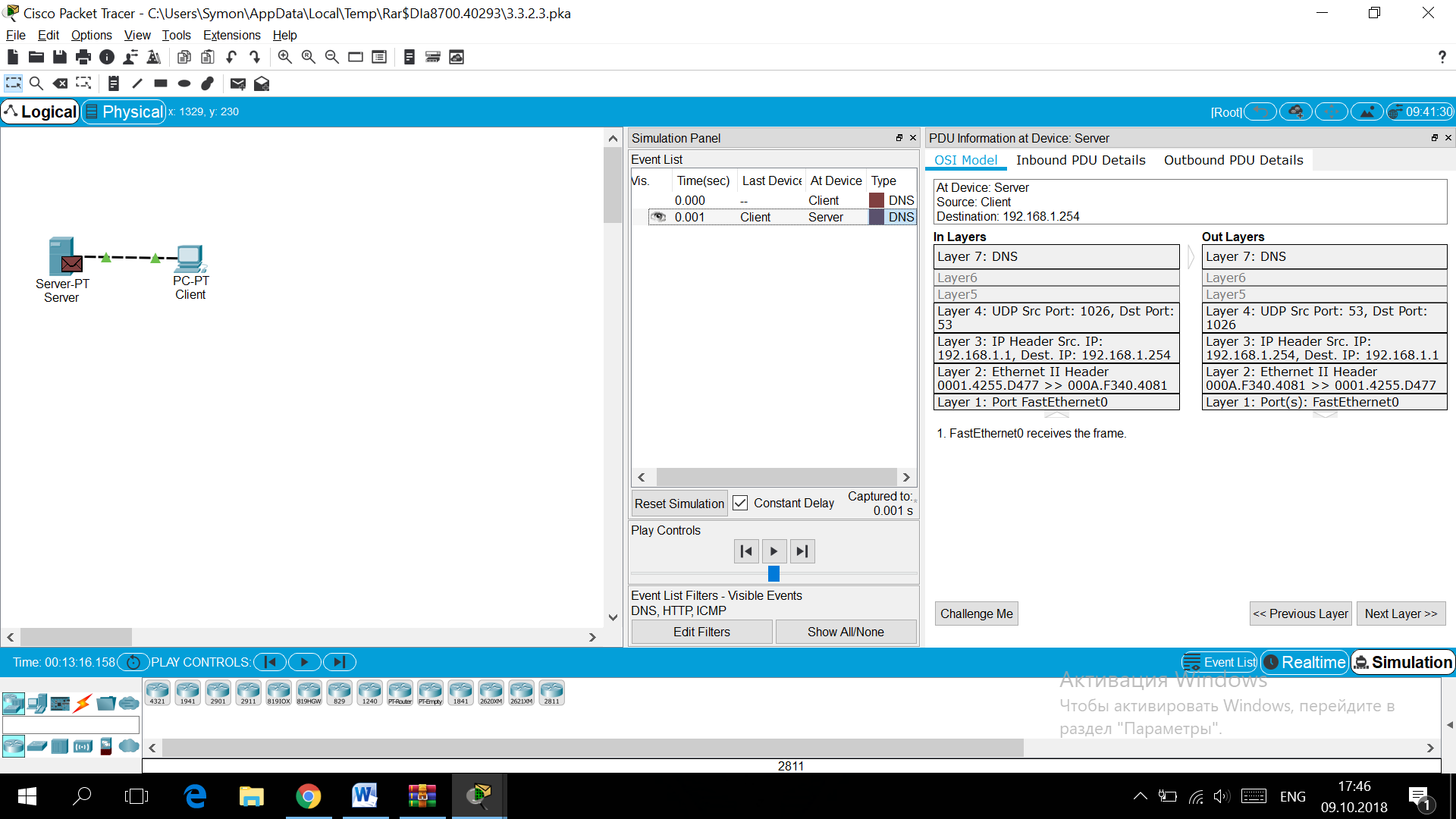
Click the **Web Browser** button. A simulated web browser opens. Type www.example.com (the URL of the Server) into the **URL** box and click the **Go** button. Minimize the simulated browser window. Use **Capture/Forward** to examine the DNS and HTTP packets. For each packet in the event list, click on the colored square in the **Info** column to open the PDU information and view encapsulation and device processing details.   
  
*All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.*

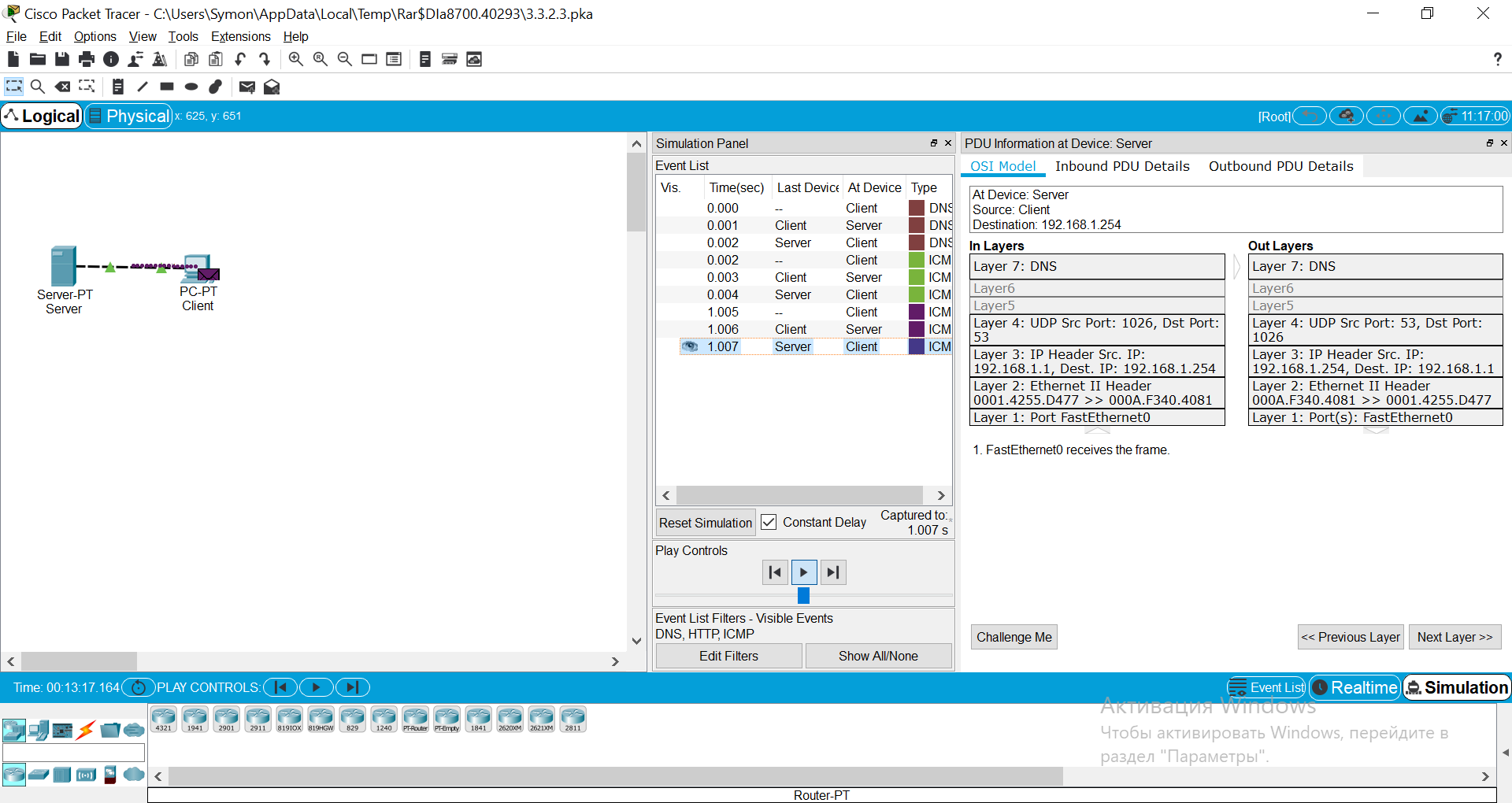












**3.5.1: Skills Integration Challenge-Configuring Hosts and Services**

**Topology Diagram:**

Partial topology given; must be completed.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **Default Gateway** |
| **R1-ISP** | **Fa0/0** | 192.168.254.253 | 255.255.255.0 | N/A |
| **S0/0/0** | 10.10.10.6 | 255.255.255.252 |
| **R2-Central** | **Fa0/0** | 172.16.255.254 | 255.255.0.0 | N/A |
| **S0/0/0** | 10.10.10.5 | 255.255.255.252 |
| **S1-Central** | **VLAN 1** | 172.16.254.1 | 255.255.0.0 | 172.16.255.254 |
| **PC 1A** | **NIC** | 172.16.1.1 | 255.255.0.0 | 172.16.255.254 |
| **PC 1B** | **NIC** | 172.16.1.2 | 255.255.0.0 | 172.16.255.254 |
| **Eagle Server** | **NIC** | 192.168.254.254 | 255.255.255.0 | 192.168.254.253 |

**Learning Objectives:**

* Configure Hosts and Services
* Add, configure, and connect hosts and servers
* Explore How DNS and HTTP Work Together
* Use simulation mode to view the details of packets generated by DNS and HTTP

**Background:**

Throughout the course, you will be using a standard lab setup created from actual PCs, servers, routers, and switches to learn networking concepts. At the end of each chapter, you will build increasingly larger parts of this topology in Packet Tracer.

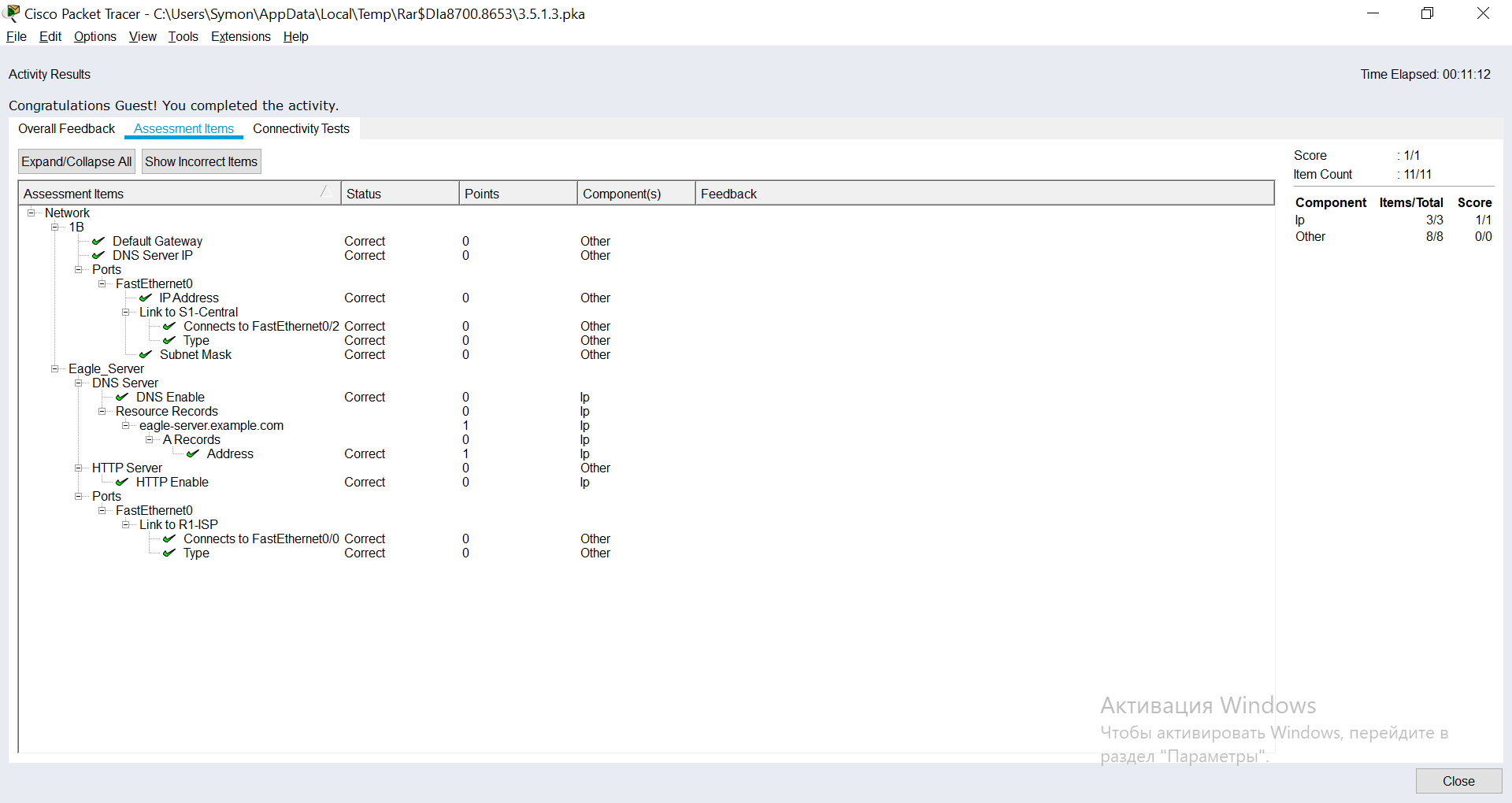
**Task 1: "Repair" and Test the Topology**

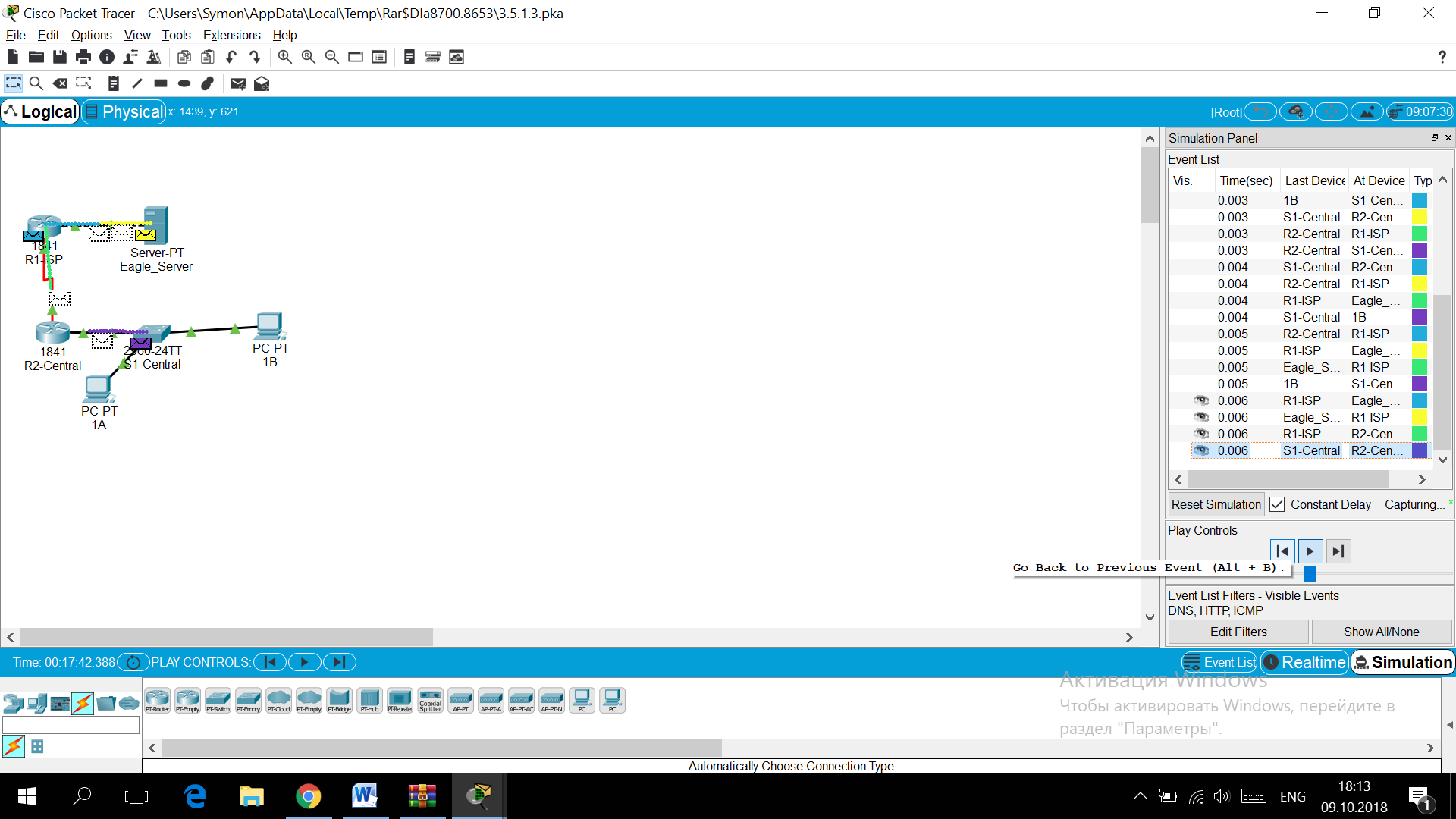
Add a PC with a display name of "1B" (without quotes) to the topology. Configure it with the following settings: IP Address 172.16.1.2, Subnet Mask 255.255.0.0, Default Gateway 172.16.255.254, and DNS Server 192.168.254.254. Connect PC 1B to the Fa0/2 port of the S1-Central switch.   
  
Connect the Eagle Server to the Fa0/0 port on the R1-ISP router. Turn on web services on the server by enabling HTTP. Enable DNS services and add a DNS entry that associates "eagle-server.example.com" (without quotes) with the IP address of the server. Verify your work using feedback from the **Check Results** button and the **Assessment Items** tab. Test connectivity, in realtime, by using ADD SIMPLE PDU to test connectivity between PC 1B and the Eagle Server.   
  
Note that when you add a simple PDU, it appears in the PDU List Window as part of "Scenario 0". The first time you issue this one-shot ping message, it will show as **Failed**--this is because of the ARP process which, will be explained later. Double clicking the "Fire" button in the PDU List Window, send this single test ping a second time. This time it will be successful. In Packet Tracer, the term "scenario" means a specific configuration of one or more test packets. You can create different test packet scenarios by using the **New** button--for example Scenario 0 might have one test packet from PC 1B to Eagle Server, Scenario 1 might test packets between PC 1A and the routers... You can remove all test packets in a particular scenario by using the **Delete** button. For example, if you use the **Delete** button for Scenario 0 the test packet you just created between PC 1B and Eagle Server will be removed--please do this prior to the next task.

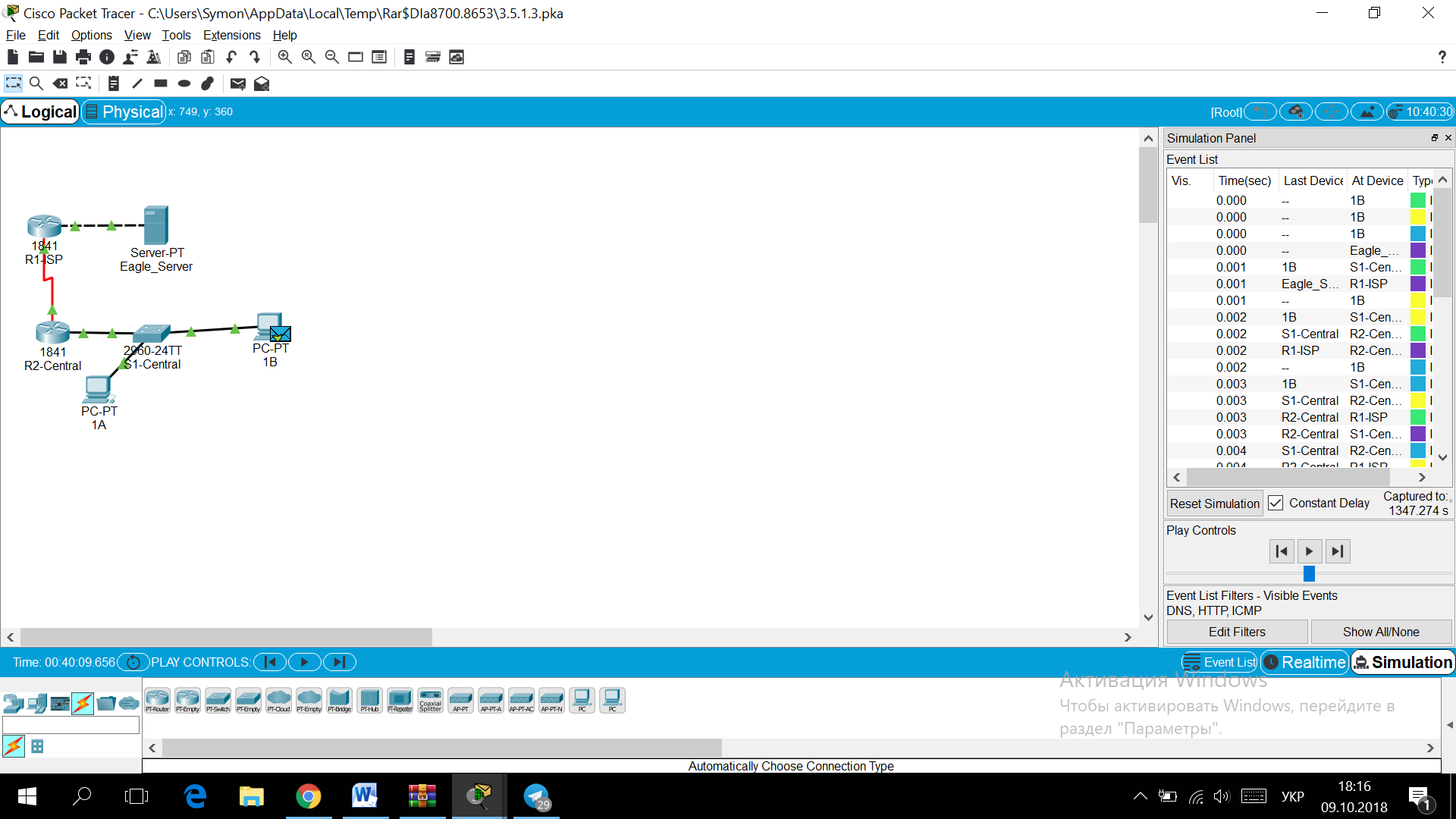
**Task 2: Explore How DNS and HTTP Work Together**

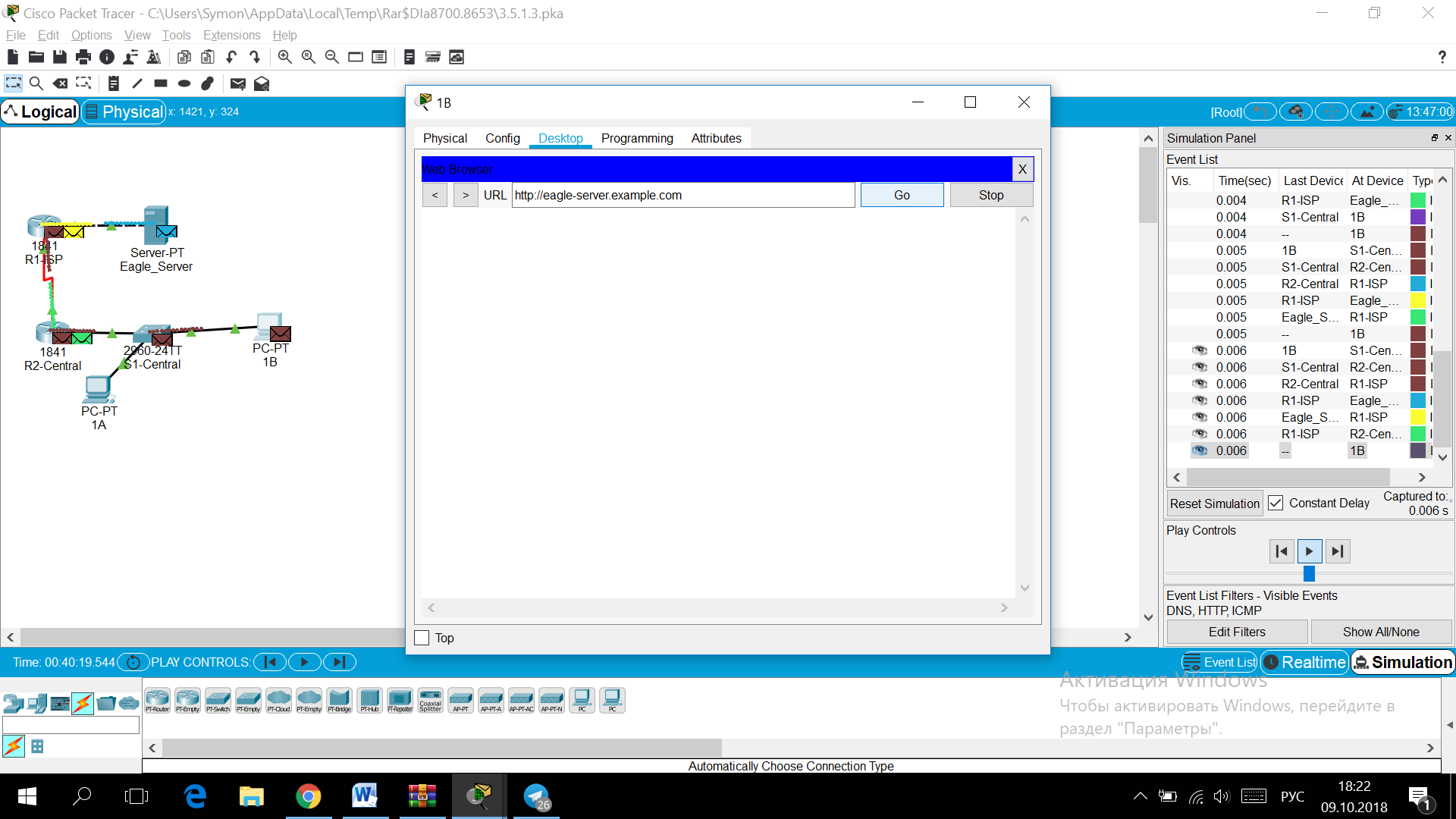
Switch from Realtime to Simulation mode. Open a web browser from the desktop of PC 1B. Type in "eagle-server.example.com" (without quotes) into the Address Bar, press Enter, and then use the **Capture / Forward** button in the **Event List** to capture the interaction of DNS and HTTP. Play this animation and examine the Packet contents (**PDU Information** Window, **Inbound PDU Details, Outbound PDU Details**) for each event in the event list, especially when the packets are at PC 1B or at the Eagle Server. If you receive a "Buffer Full" message, click the **View Previous Events** button. While the processing of the packets by the switch and the routers may not make sense to you yet, you should be able to see how DNS and HTTP work together.

**Reflection:**

Can you now explain the process that occurs when you type a URL into a browser and a web page returns? What types of client-server interactions are involved?   
If you have not already done so, you are encouraged to obtain Packet Tracer from your instructor and complete My First PT Lab (choose the HELP Pulldown Menu, choose CONTENTS).   








**4.6.1: Skills Integration Challenge-Analyzing the Application and Transport Layers**

**Topology Diagram:**

Partial topology given; must be completed.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **Default Gateway** |
| **R1-ISP** | **Fa0/0** | 192.168.254.253 | 255.255.255.0 | N/A |
| **S0/0/0** | 10.10.10.6 | 255.255.255.252 |
| **R2-Central** | **Fa0/0** | 172.16.255.254 | 255.255.0.0 | N/A |
| **S0/0/0** | 10.10.10.5 | 255.255.255.252 |
| **S1-Central** | **VLAN 1** | 172.16.254.1 | 255.255.0.0 | 172.16.255.254 |
| **PC 1A** | **NIC** | 172.16.1.1 | 255.255.0.0 | 172.16.255.254 |
| **PC 1B** | **NIC** | 172.16.1.2 | 255.255.0.0 | 172.16.255.254 |
| **Eagle Server** | **NIC** | 192.168.254.254 | 255.255.255.0 | 192.168.254.253 |

**Learning Objectives:**

* Configure Hosts and Services
* Connect and configure hosts and services on the model of the lab network
* Explore How DNS, UDP, HTTP, and UDP Work Together
* Use simulation mode to visualize the operation of DNS, UDP, HTTP, and TCP on the model of the lab network

**Background:**

Throughout the course, you will be using a standard lab setup created from actual PCs, servers, routers, and switches to learn networking concepts. At the end of each chapter, you will build increasingly larger parts of this topology in Packet Tracer, and analyze increasingly more complex protocol interactions.

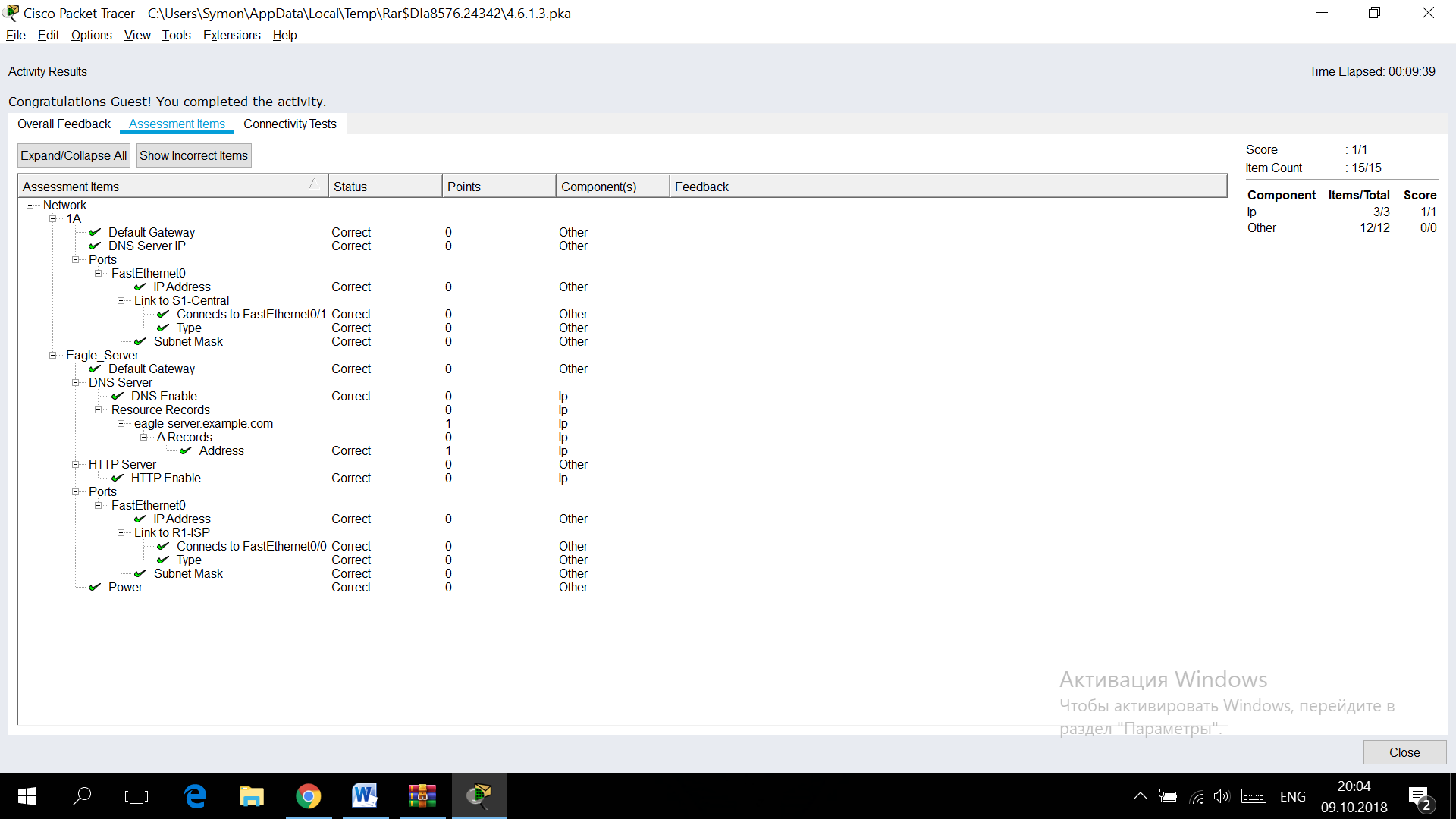
**Task 1: Repair and Test The Topology**

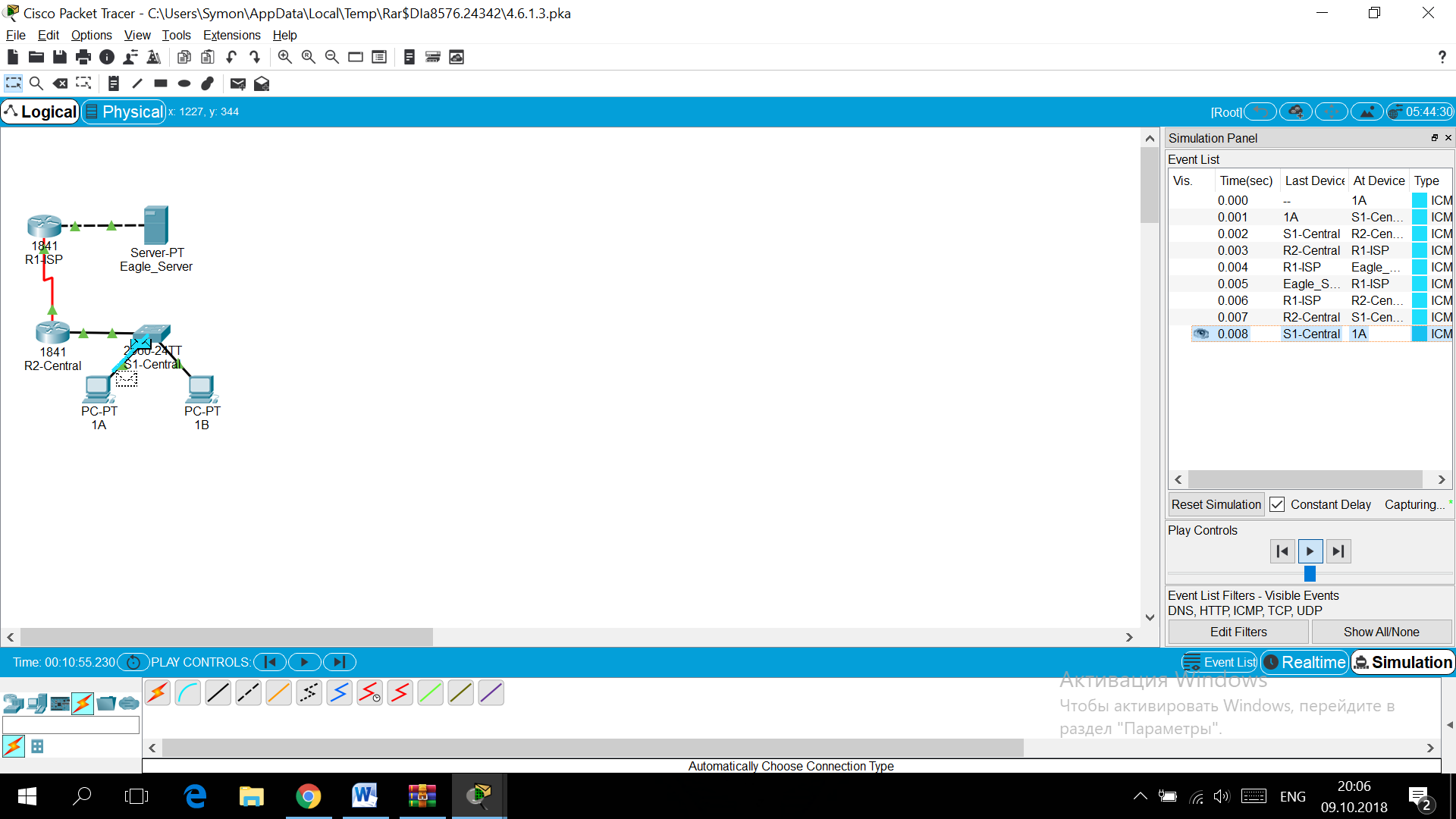
The server has been replaced. Configure it with the following settings: IP Address 192.168.254.254, Subnet Mask 255.255.255.0, Default Gateway 192.168.254.253, DNS enabled, with the association of "eagle-server.example.com" (without the quotes) with the server's IP address, HTTP enabled. Connect the Eagle Server to the Fa0/0 port on the R1-ISP router.  
  
PC 1A has lost its IP address information. Configure it with the following settings: IP Address 172.16.1.1, Subnet Mask 255.255.0.0, Default Gateway 172.16.255.254, and DNS Server 192.168.254.254. Connect PC 1A to the Fa0/1 port of the S1-Central switch.   
  
Verify your work using feedback from the **Check Results** button and the **Assessment Items** tab. Test connectivity, in realtime, by using ADD SIMPLE PDU to test connectivity between PC 1A and the Eagle Server.   
  
Note that when you add a simple PDU, it appears in the PDU List Window as part of "Scenario 0". The first time you issue this one-shot ping message, it will show as **Failed**--this is because of the ARP process which will be explained later. Double clicking the "Fire" button in the PDU List Window, send this single test ping a second time. This time it will be successful. In Packet Tracer, the term "scenario" means a specific configuration of one or more test packets. You can create different test packet scenarios by using the **New** button--for example Scenario 0 might have one test packet from PC 1A to Eagle Server; Scenario 1 might test packets between PC 1B and the routers... You can remove all test packets in a particular scenario by using the **Delete** button. For example, if you use the **Delete** button for Scenario 0 the test packet you just created between PC 1A and Eagle Server will be removed--please do this prior to the next task.

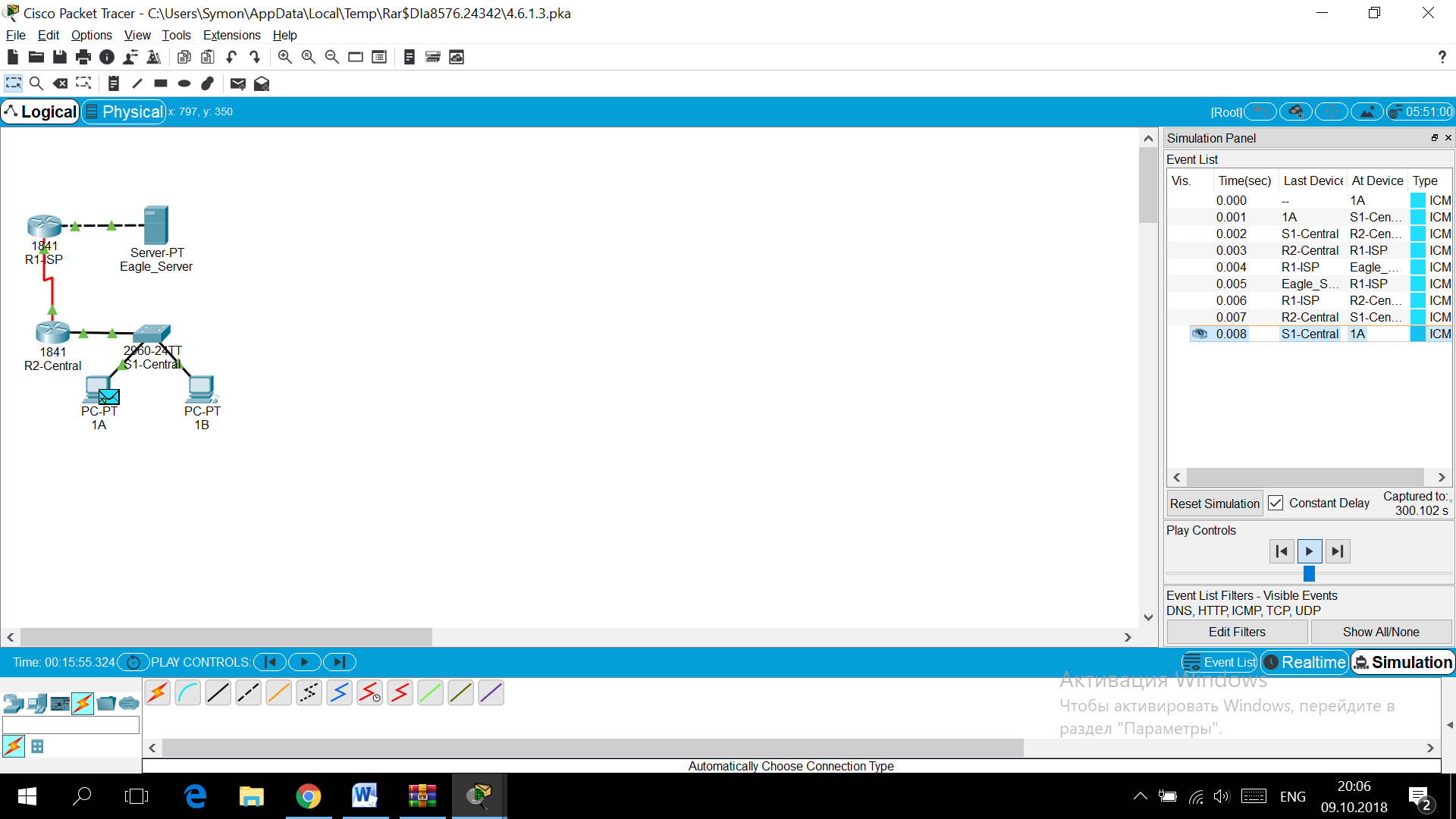
**Task 2: Explore How DNS, UDP, HTTP, and TCP Work Together**

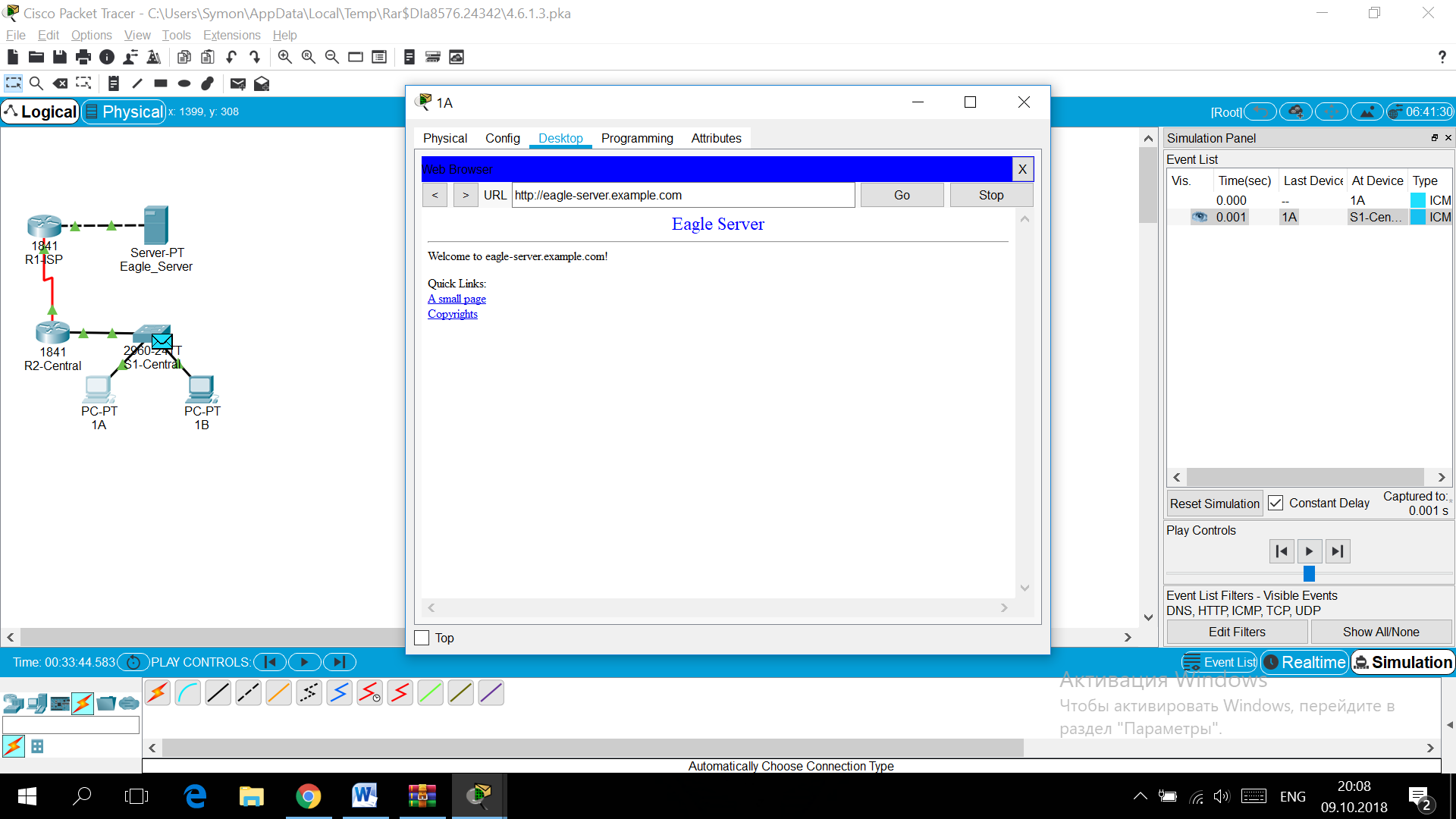
Switch from Realtime to Simulation Mode. Make sure Event Filter is set to display DNS, UDP, HTTP, TCP, and ICMP. Open a web browser from the desktop of 1A. Type in the URL eagle-server.example.com, press Enter, and then use the **Capture / Forward** button in the **Event List** to capture the interaction of DNS, UDP, HTTP and TCP.  
  
You can examine the packet in two ways: by clicking on the packet envelope as it is displayed in the animation, or by clicking on the **Info** column for that packet instance as it is listed in the **Event List**. Play this animation and examine the Packet contents (**PDU Information** Window, **Inbound PDU Details, Outbound PDU Details**) for each event in the event list, especially when the packets are at PC 1A or at the Eagle Server. If you receive a "Buffer Full" message, click the **View Previous Events** button. While the processing of the packets at the switch and the routers may not make sense to you yet, you should be able to see how DNS, UDP, HTTP, and TCP work together by tracing the packets and using the PDU Information window to look "inside" them.

**Reflection:**

Can you make a diagram of the sequence of protocol events involved in requesting a web page using a URL? Where might things go wrong? Compare and contrast DNS and HTTP, and UDP and TCP.   








**Activity 5.5.1:   
Examining a Device's Gateway**

**Addressing Table**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interference** | **IP Address** | **Subnet Mask** | **Default Gateway** |
| **R1-ISP** | S0/0/0 | 10.10.10.6 | 255.255.255.252 | N/A |
| Fa0/0 | 192.168.254.253 | 255.255.255.0 | N/A |
| **R2-Central** | S0/0/0 | 10.10.10.5 | 255.255.255.252 | N/A |
| Fa0/0 | 172.168.255.254 | 255.255.0.0 | N/A |
| **Eagle Server** | FastEthernet | 192.168.254.254 | 255.255.255.0 | 192.168..254.253 |
| **Host 1A** | FastEthernet | 172.16.1.1 | 255.255.0.0 | 172.16.255.254 |
| **Host 1B** | FastEthernet | 172.16.1.2 | 255.255.0.0 | 172.16.255.254 |
| **Host 11A** | FastEthernet | 172.16.11.1 | 255.255.0.0 | 172.16.255.254 |
| **Host 11B** | FastEthernet | 172.16.1.2 | 255.255.0.0 | 172.16.255.254 |
| **S1-Central** | N/A | 172.16.254.1 | 255.255.0.0 | 172.16.255.254 |

**Learning Objectives**

* Understand and explain the purpose of a gateway address
* Understand how network information is configured on a Windows computer
* Troubleshoot a hidden gateway address problem

**Introduction:**

An IP address is composed of a network portion and a host portion. A computer that communicates with another device must first know how to reach the device. For devices on the same local area network (LAN), the host portion of the IP address is used as the identifier. The network portion of the destination device is the same as the network portion of the host device.

However, devices on different networks have different source and destination network numbers. The network portion of the IP address is used to identify when a packet must be sent to a gateway address, which is assigned to a network device that forwards packets between distant networks.

A router is assigned the gateway address for all the devices on the LAN. One purpose of a router is to serve as an entry point for packets coming into the network and exit point for packets leaving the network.

Gateway addresses are very important to users. Cisco estimates that 80 percent of network traffic will be destined to devices on other networks, and only 20 percent of network traffic will go to local devices. This is called the 80/20 rule. Therefore, if a gateway cannot be reached by the LAN devices, users will not be able to perform their job.

*All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.*

### Task 1: Understand and Explain the Purpose of a Gateway Address.

#### Step 1. Open a command prompt window on a pod host computer.

Issue the **ipconfig** command.

What is the default gateway address?

#### Step 2. Use the ping command to verify connectivity with IP address 127.0.0.1.

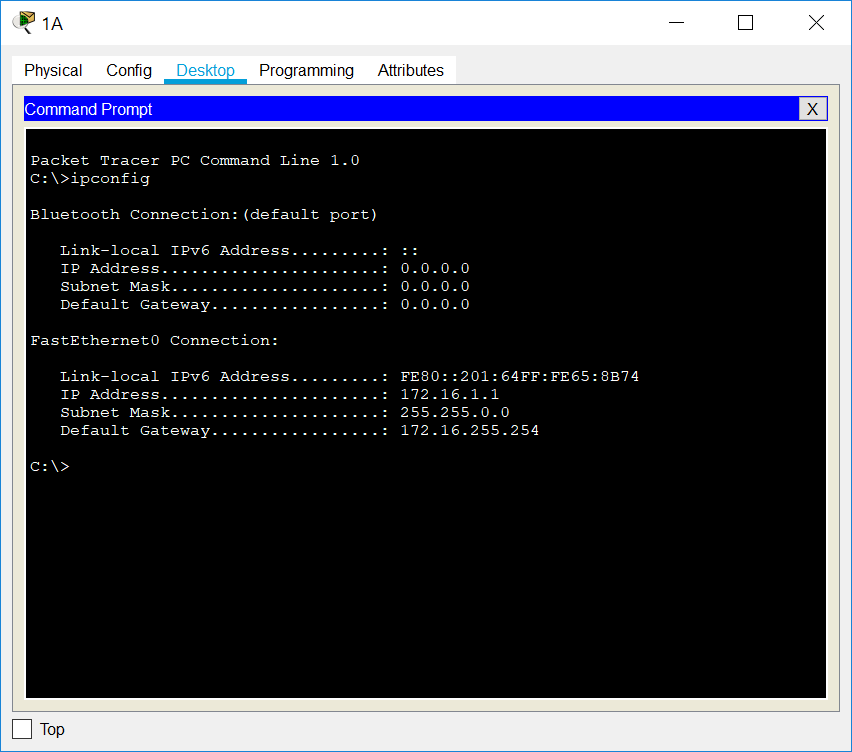
Was the ping successful?

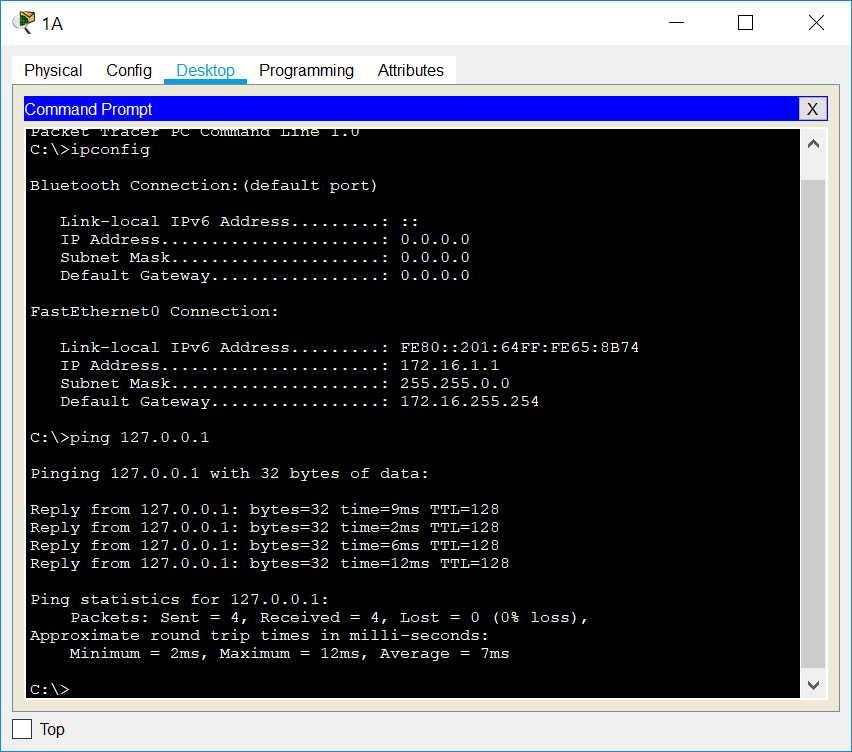
**Step 3.** **Use the ping command to ping different IP addresses on the 127.0.0.0 network, 127.10.1.1, and 127.255.255.255.**

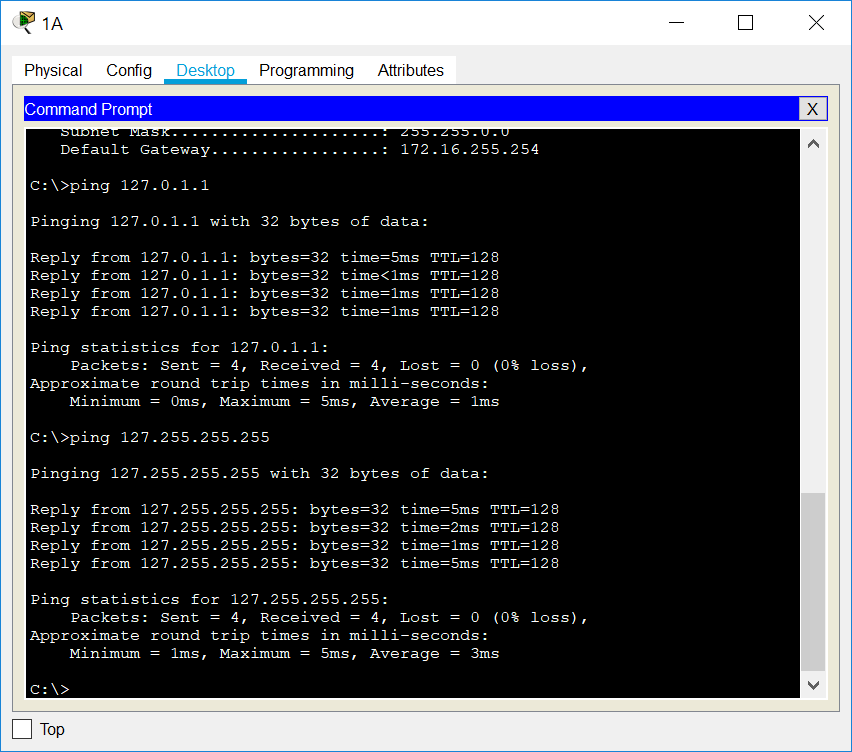
Were responses successful? If not, why?

#### At the end of this task your completion rate should be 0%.

*All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.*







**Task 2: Understand how Network Information is Configured.**

Many times connectivity issues are attributed to wrong network settings. In troubleshooting connectivity issues, several tools are available to quickly determine the network configuration.

**Step 1.** **Examine network IP address properties:**

* By Clicking on the **PC** > **Desktop** Tab> **IP Configuration**

**Step 2. To examine network properties using the ipconfig command:**

* Click on the **PC**>**Desktop**Tab > **Command Prompt**
* Then type **ipconfig** or **ipconfig /all**

**At the end of this task your completion rate should be 0%.**

//

### Task 3: Troubleshoot a Hidden Gateway Address Problem.

When troubleshooting network issues, a thorough understanding of the network can often assist in identifying the real problem.

As the 3rd shift help desk Cisco engineer, you are asked for assistance from the help desk technician. The technician received a trouble ticket from a user on computer host-1A, complaining that computer host-11B, **host-11B.example.com**, does not respond to pings. The technician verified the cables and network settings on both computers, but nothing unusual was found. You check with the corporate network engineer, who reports that R2-Central has been temporarily brought down for a hardware upgrade. Nodding your head in understanding, you ask the technician to ping the IP address for host-11B, 172.16.11.2 from host-1A. The pings are successful. Then, you ask the technician to ping the gateway IP address, 172.16.254.254, and the pings fail.

**Your task is to find and fix the problem that is occurring within this network.**

**HINT: In Order to Solve This Problem, Check R2-Central's Interfaces**

#### At the end of this task your completion rate should be 100%.

#### 

**5.6.1: Skills Integration Challenge-Routing IP Packets**

**Topology Diagram:**

Partial topology given; must be completed.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **Default Gateway** |
| **R1-ISP** | **Fa0/0** | 192.168.254.253 | 255.255.255.0 | N/A |
| **S0/0/0** | 10.10.10.6 | 255.255.255.252 |
| **R2-Central** | **Fa0/0** | 172.16.255.254 | 255.255.0.0 | N/A |
| **S0/0/0** | 10.10.10.5 | 255.255.255.252 |
| **S1-Central** | **VLAN 1** | 172.16.254.1 | 255.255.0.0 | 172.16.255.254 |
| **PC-PT 1A** | **NIC** | 172.16.1.1 | 255.255.0.0 | 172.16.255.254 |
| **PC-PT 1B** | **NIC** | 172.16.1.2 | 255.255.0.0 | 172.16.255.254 |
| **Eagle Server** | **NIC** | 192.168.254.254 | 255.255.255.0 | 192.168.254.253 |

**Learning Objectives:**

* Configure a router interface using a GUI
* Explore a routing table
* Configure a static route using a GUI
* Explore the routing of IP packets

**Background:**

Throughout the course, you will be using a standard lab setup created from actual PCs, servers, routers, and switches to learn networking concepts. At the end of each chapter, you will build increasingly larger parts of this topology in Packet Tracer, and analyze increasingly more complex protocol interactions. You have already studied a variety of application protocols, such as DNS, HTTP, TFTP, DHCP, and Telnet, and two transport layer protocols, TCP and UDP. You may have noticed that regardless of what application and transport protocols were involved, in **Inbound** and **Outbound PDU Details** view they were always encapsulated in IP Packets. In this activity, we will examine how the Internet Protocol, the dominant network layer protocol of the Internet, works in the context of a simple example of IP routing.

**Task 1: Configure a router interface**

There are problems on the local area network: PC-PT 1A cannot communicate with the Eagle Server (verify this in Realtime mode by pinging Eagle Servers IP address: 192.168.254.254). It appears there is a problem with the router. Mouse over the R2-Central router, and note the condition of the Fa0/0 interface (to which S1-Central is connected). This interface must have an IP address, subnet mask, and be turned on in order to act as the default gateway for the LAN. Click on router R2-Central, and go to the **Config** tab. At the end of the course, you will learn how to use the Cisco Internetwork Operating System (IOS) command line interface (CLI) to perform this task. For now, the **Config** tab is easier and will allow you to focus on the basic idea of IP routing. In the list shown, find **INTERFACE, FastEthernet0/0**. Add the IP address 172.16.255.254 with subnet mask of 255.255.0.0, and turn the port on. Close the router window. Verify that the router interface (port) is now working by using the mouse over. Try reaching Eagle Server. The request still fails. What are some possible reasons why? 

**Task 2: Examining routes**

Use the **Inspect** tool (magnifying glass) to examine the routing table of R2-Central. You will see the router's directly connected networks, but there is no way to reach the Eagle Server network. 

**Task 3: Configure a route using a GUI**

Click on router R2-Central and go to the **Config** tab. In the list shown, find **ROUTING, Static**. Configure a default static route, using the address 0.0.0.0, mask 0.0.0.0, and the next hop of 10.10.10.6 (the S0/0/0 interface on the R1-ISP router) and click the **Add** button. This route is configured so that wherever packets from the 172.16.0.0 /16 LAN are destined, they will go to the R1-ISP router. Under **GLOBAL, Settings**, click on the **Save** button to save the interface and route configuration you have just done to NVRAM in case the router is power cycled. Use the **Inspect Tool** (magnifying glass) to examine the routing table of R2-Central again. You should now see the route you configured in the routing table.   
  
Verify your work using feedback from the **Check Results** button and the **Assessment Items** tab. Test connectivity, in Realtime, by using ADD SIMPLE PDU to test connectivity between PC-PT 1A and the Eagle Server. The PDU, a one-shot ping, will appear in the User Created PDU List for future use as well. The first ping attempt will fail because the ARP tables are not populated; double click on **Fire** to send it again - this should be successful. 

**Task 4: Examine the routing of the IP packet**

Switch to Simulation mode. Using the PDU you created in Task 3, trace the packet's journey from PC-PT 1A to Eagle Server and back using the **Capture / Forward** button and examining the packet's contents by either clicking on the envelope or clicking on the colored square in the **Info** column of the **Event List**. 

**Reflection:**

What data can an IP Packet contain? What is meant by the phrase "the IP packet is routed"? What is a route? Where might things go wrong? 

