Question And Answer

10.2.1.8 Packet Tracer - Web and Email

Part 1: Configure and Verify Web Services

Step 2: Verify the web servers by accessing the web pages.

f. What protocol is translating the centralserver.pt.pka and branchserver.pt.pka names to IP addresses? **Ans: Domain Name Service (DNS)**

13.2.6 Packet Tracer - Verify IPv4 and IPv6 Addressing

Fill-in the **Addressing Table** with the IPv4 and IPv6 address, subnet mask, and default gateway.

Addressing Table

Device	Interface	IP Address / Prefix		Default Gateway
R1	G0/0	10.10.1.97	255.255.255.224	N/A
		2001:db8:1:1::1/64		
	S0/0/1	10.10.1.6	255.255.255.252	N/A
		2001:db8:1:2::2/64		
		fe80::1		
R2	S0/0/0	10.10.1.5	255.255.255.252	N/A
		2001:db8:1:2::1/64		
	S0/0/1	10.10.1.9	255.255.255.252	N/A
		2001:db8:1:3::1/64		
		fe80::2		
R3	G0/0	10.10.1.17	255.255.255.240	N/A
		2001:db8:1:4::1/64		
	S0/0/1	10.10.1.10	255.255.255.252	N/A
		2001:db8:1:3::2/64		
		fe80::3		
PC1	NIC	**10.10.1.100**	**255.255.255.224**	**10.10.1.97**
		2001:DB8:1:1::A/64		**FE80::1**
PC2	NIC	**10.10.1.20**	**255.255.255.240**	**10.10.1.17**
		2001:DB8:1:4::A/64		**FE80::3**

Part 2: Test Connectivity Using Ping

Step 1: Use ping to verify IPv4 connectivity.

a. From **PC1**, ping the IPv4 address for **PC2**.

Was the result successful? **Yes**

b. From **PC2**, ping the IPv4 address for **PC1**.

Was the result successful? **Yes**

Step 2: Use ping to verify IPv6 connectivity.

a. From **PC1**, ping the IPv6 address for **PC2**.

Was the result successful? **Yes**

From **PC2**, ping the IPv6 address of **PC1**.

Was the result successful? **Yes**

Part 3: Discover the Path by Tracing the Route

Step 1: Use tracert to discover the IPv4 path.

a. From **PC1**, trace the route to **PC2**.

```
PC> tracert 10.10.1.20
```

What addresses were encountered along the path? **10.10.1.97, 10.10.1.5, 10.10.1.10, 10.10.1.20**

With which interfaces are the four addresses associated? **G0/0 of R1, S0/0/0 on R2, S0/0/01 on R3, NIC of PC2**

b. From **PC2**, trace the route to **PC1**.

What addresses were encountered along the path? **10.10.1.17, 10.10.1.9, 10.10.1.6, 10.10.1.100**

With which interfaces are the four addresses associated? **G0/0 of R3, S0/0/1 of R2, S0/0/1 of R1, NIC of PC1**

Step 2: Use tracert to discover the IPv6 path.

a. From **PC1**, trace the route to the IPv6 address for **PC2**.

```
PC> tracert 2001:db8:1:4::a
```

What addresses were encountered along the path? **2001:db8:1:1::1, 2001:db8:1:2::1, 2001:db8:1:3::2, 2001:db8:1:4::a**

With which interfaces are the four addresses associated? **G0/0 of R1, S0/0/0 of r2, S0/0/1 of R3, NIC of PC2**

b. From **PC2**, trace the route to the IPv6 address for **PC1**.

What addresses were encountered along the path? **2001:db8:1:4::1, 2001:db8:1:3::1, 2001:db8:1:2::2, 2001:db8:1:1::a**

With which interfaces are the four addresses associated? **G0/0 of R3, S0/0/1 of R2, S0/0/1 of R1, NIC of PC1**

13.2.7 Packet Tracer - Use Ping and Traceroute to Test Network

Fill-in the **Addressing Table** with the IPv4 and IPv6 address, subnet mask, and default gateway.

Addressing Table

Device	Interface	IP Address / Prefix		Default Gateway
R1	G0/0	2001:db8:1:1::1/64		N/A
	G0/1	10.10.1.97	255.255.255.224	N/A
	S0/0/1	10.10.1.6	255.255.255.252	N/A
		2001:db8:1:2::2/64		
		fe80::1		
R2	S0/0/0	10.10.1.5	255.255.255.252	N/A
		2001:db8:1:2::1/64		
	S0/0/1	10.10.1.9	255.255.255.252	N/A
		2001:db8:1:3::1/64		
		fe80::2		
R3	G0/0	2001:db8:1:4::1/64		N/A
	G0/1	10.10.1.17	255.255.255.240	N/A
	S0/0/1	10.10.1.10	255.255.255.252	N/A
		2001:db8:1:3::2/64		
		fe80::3		
PC1	NIC	**10.10.1.98**	**255.255.255.224**	**10.10.1.97**
PC2	NIC	**2001:DB8:1:1::2**		**FE80::1**
PC3	NIC	**10.10.1.18**	**255.255.255.240**	**10.10.1.17**
PC4	NIC	**2001:DB8:1:4::2**		**FE80::2**

Part 1: Test and Restore IPv4 Connectivity

Step 2: Locate the source of connectivity failure.

a. From **PC1**, enter the necessary command to trace the route to **PC3**.

What is the last successful IPv4 address that was reached? **10.10.1.97**

b. The trace will eventually end after 30 attempts. Enter **Ctrl**+**C** to stop the trace before 30 attempts.

c. From **PC3**, enter the necessary command to trace the route to **PC1**.

What is the last successful IPv4 address that was reached? **10.10.1.17**

d. Enter **Ctrl**+**C** to stop the trace.

e. Click **R1**. Press **ENTER** and log in to the router.

f. Enter the **show ip interface brief** command to list the interfaces and their status. There are two IPv4 addresses on the router. One should have been recorded in Step 2a.

What is the other? **10.10.1.6**

g. Enter the **show ip route** command to list the networks to which the router is connected. Note that there are two networks connected to the **Serial0/0/1** interface.

What are they? **10.10.1.4/30 and 10.10.1.6/32**

h. Repeat steps 2e through 2g with **R3** and record your answers. **10.10.1.10 ipv4 address. 10.10.1.8/30 and 10.10.1.10/32 directly connected to Serial0/0/1**

i. Click **R2**. Press **ENTER** and log into the router.

j. Enter the **show ip interface brief** command and record your addresses. **10.10.1.2 and 10.10.1.9**

k. Run more tests if it helps visualize the problem. Simulation mode is available.

Step 3: Propose a solution to solve the problem.

Compare your answers in Step 2 to the documentation you have available for the network.

What is the error? **R2's Serial 0/0/0 has wrong IP address.**

What solution would you propose to correct the problem? **Change it to the correct IP address, 10.10.1.15.**

Step 5: Verify that connectivity is restored.

a. From **PC1** test connectivity to **PC3**.

b. From **PC3** test connectivity to **PC1**.

Is the problem resolved? **Yes**

Part 2: Test and Restore IPv6 Connectivity

Step 2: Locate the source of connectivity failure.

a. From **PC2**, enter the necessary command to trace the route to **PC4**.

What is the last successful IPv6 address that was reached? **2001:DB8:1:3::2**

b. The trace will eventually end after 30 attempts. Enter **Ctrl**+**C** to stop the trace before 30 attempts.

c. From **PC4**, enter the necessary command to trace the route to **PC2**.

What is the last successful IPv6 address that was reached? **No IPv6 address reached.**

d. Enter **Ctrl**+**C** to stop the trace.

e. Click **R3**. Press **ENTER** and log in to the router.

f. Enter the **show ipv6 interface brief** command to list the interfaces and their status. There are two IPv6 addresses on the router. One should match the gateway address recorded in Step 1d.

Is there a discrepancy? **Yes**

g. Run more tests if it helps visualize the problem. Simulation mode is available.

Step 3: Propose a solution to solve the problem.

Compare your answers in Step 2 to the documentation you have available for the network.

What is the error? **PC4 using the wrong default gateway.**

What solution would you propose to correct the problem? **Correct PC4 default gateway address, FE80::3.**

Step 5: Verify that connectivity is restored.

a. From **PC2** test connectivity to **PC4**.

b. From **PC4** test connectivity to **PC2**.

Is the problem resolved? **Yes**

14.8.1 Packet Tracer - TCP and UDP Communications

Part 1: Generate Network Traffic in Simulation Mode and View Multiplexing

Step 7: Examine multiplexing as the traffic crosses the network.

b. Click **Capture/Forward** six times and watch the PDUs from the different hosts as they travel on the network. Note that only one PDU can cross a wire in each direction at any given time.

What is this called? **Conversation multiplexing**

A variety of PDUs appears in the event list in the Simulation Panel. What is the meaning of the different colors? **Different colors represent protocols.**

Part 2: Examine Functionality of the TCP and UDP Protocols

Step 1: Examine HTTP traffic as the clients communicate with the server.

d. Click **Capture/Forward** until you see a PDU appear for HTTP. Note that the color of the envelope in the topology window matches the color code for the HTTP PDU in the Simulation Panel.

Why did it take so long for the HTTP PDU to appear? **TCP must establish first the connection before the HHTP PDU appear.**

e. Click the PDU envelope to show the PDU details. Click the **Outbound PDU Details** tab and scroll down to the second to the last section.

What is the section labeled? **TCP**

Are these communications considered to be reliable? **Yes**

Record the **SRC PORT**, **DEST PORT**, **SEQUENCE NUM**, and **ACK NUM** values. **1027, 80, 1, 1**

f. Look at the value in the Flags field, which is located next to the Window field. The values to the right of the "b" represent the TCP flags that are set for this stage of the data conversation. Each of the six places corresponds to a flag. The presence of a "1" in any place indicates that the flag is set. More than one flag can be set at a time. The values for the flags are shown below.

Flag Place	**6**	**5**	**4**	**3**	**2**	**1**
Value	URG	ACK	PSH	RST	SYN	FIN

Which TCP flags are set in this PDU? **ACK and PSH**

g. Close the PDU and click **Capture/Forward** until a PDU with a checkmark returns to the **HTTP Client**.

h. Click the PDU envelope and select **Inbound PDU Details**.

How are the port and sequence numbers different than before? **Source and destination ports are reversed. Sequence number is 1**

i. Click the HTTP PDU which **HTTP Client** has prepared to send to **MultiServer**. This is the beginning of the HTTP communication. Click this second PDU envelope and select **Outbound PDU Details**.

What information is now listed in the TCP section? How are the port and sequence numbers different from the previous two PDUs? **Source and destination ports are reversed. Both sequence number is 1, the acknowledgement number is 103. Flags are PSH and ACK.**

Step 2: Examine FTP traffic as the clients communicate with the server.

c. Click **Capture/Forward**. Click the second PDU envelope to open it.

Click the **Outbound PDU Details** tab and scroll down to the TCP section.

Are these communications considered to be reliable? **Yes**

d. Record the **SRC PORT**, **DEST PORT**, **SEQUENCE NUM**, and **ACK NUM** values. **1025, 21, 95, 144**

What is the value in the flag field? **FIN and ACK**

e. Close the PDU and click **Capture/Forward** until a PDU returns to the **FTP Client** with a checkmark.

f. Click the PDU envelope and select **Inbound PDU Details**.

How are the port and sequence numbers different than before? **21, 1025, 0, 1. SYN+ACK. Source and destination ports are reversed, and 1 is acknowledgement number.**

g. Click the **Outbound PDU Details** tab.

How are the port and sequence numbers different from the previous results? **The source and destination ports are reversed. Sequence is 144 and acknowledgement number is 95.**

h. Close the PDU and click **Capture/Forward** until a second PDU returns to the **FTP Client**. The PDU is a different color.

i. Open the PDU and select **Inbound PDU Details**. Scroll down past the TCP section.

What is the message from the server? **"Welcome to PT Ftp server"**

Step 3: Examine DNS traffic as the clients communicate with the server.

d. Look at the OSI Model details for the outbound PDU.

What is the Layer 4 protocol? **UDP**

Are these communications considered to be reliable? **No**

e. Open the Outbound PDU Details tab and find the UDP section of the PDU formats. Record the **SRC PORT** and **DEST PORT** values.

Why are there no sequence and acknowledgement numbers? **Because UDP does not need to establish a reliable connection.**

f. Close the **PDU** and click **Capture/Forward** until a PDU with a check mark returns to the **DNS Client**.

g. Click the PDU envelope and select **Inbound PDU Details**.

How are the port and sequence numbers different than before? **The source and destination ports are reversed.**

What is the last section of the **PDU** called? What is the IP address for the name **multiserver.pt.ptu**? **DNS ANSWER, 192.1681.254.**

h. Click Reset Simulation.

Step 4: Examine email traffic as the clients communicate with the server.

d. Click the **Outbound PDU Details** tab and scroll down to the last section.

What transport layer protocol does email traffic use? **TCP**

Are these communications considered to be reliable? **Yes**

e. Record the **SRC PORT**, **DEST PORT**, **SEQUENCE NUM**, and **ACK NUM** values. What is the flag field value? **1031, 80, 0, 0. SYN**

f. Close the **PDU** and click **Capture/Forward** until a PDU returns to the **E-Mail Client** with a checkmark.

g. Click the TCP PDU envelope and select **Inbound PDU Details**.

How are the port and sequence numbers different than before? **The source port is 25, destination port is 1026. Acknowledgement number is 1, and sequence number is 0. Flag field is SYN+ACK.**

h. Click the **Outbound PDU Details** tab.

How are the port and sequence numbers different from the previous two results? **The source and destination ports are reversed. Both sequence and acknowledgement numbers are 1. Flag field is ACK.**

i. There is a second **PDU** of a different color that **E-Mail Client** has prepared to send to **MultiServer**. This is the beginning of the email communication. Click this second PDU envelope and select **Outbound PDU Details**.

How are the port and sequence numbers different from the previous two **PDU**s? **The source port is 1026, destination ports is 25. Both sequence and acknowledgement numbers are 1, and flag field is PSH+ACK.**

What email protocol is associated with TCP port 25? **SMTP**

What protocol is associated with TCP port 110? **POP3**