|  |
| --- |
| **LAPORAN PRAKTIKUM JARINGAN KOMPUTER**  **WEEK 5**  **13.3.1, 14.8.1, 13.2.7** |
|  |
| **Agus Pranata Marpaung \_ 13323033**  **Romaito Silaen \_ 13323042**  **Jeyshen Siallagan \_ 13323012**  **DIII TEKNOLOGI KOMPUTER** |
| **INSTITUT TEKNOLOGI DEL**  **FAKULTAS VOKASI** |

**Judul Praktikum**

|  |  |  |
| --- | --- | --- |
| **Minggu/Sesi** | : | V/3 |
| **Kode Mata Kuliah** | : | 4332101 |
| **Nama Mata Kuliah** | : | JARINGAN KOMPUTER |
| **Setoran** | : | Jawaban dalam bentuk *softcopy* |
| **Batas Waktu Setoran** | : | *Sesi Praktikum Selanjutnya* |
| **Tujuan** | : | 1. Mahasiswa dapat melakukan percobaan untuk memastikan keterhubangan perangkat jaringan dan menganalisis header pada protokol TCP dan UDP pada layer transport. |

**Petunjuk**



**Packet Tracer - Use ICMP to Test and Correct Network Connectivity**

**Addressing Table**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interface** | **Address** | **Mask/Prefix** | **Default Gateway** |
| RTR-1  *RTR-1*  *RTR-1*  *RTR-1*  *RTR-1*  *RTR-1* | G/0/0/0  *G/0/0/0* | 192.168.1.1 | 255.255.255.0 | N/A |
| 2001:db8:4::1 | /64 | N/A |
| S0/1/0  *S0/1/0* | 10.10.2.2 | 255.255.255.252 | N/A |
| 2001:db8:2::2 | /126 | N/A |
| S0/1/1  *S0/1/1* | 10.10.3.1 | 255.255.255.252 | N/A |
| 2001:db8:3::1 | /126 | N/A |
| RTR-2  *RTR-2*  *RTR-2*  *RTR-2* | G/0/0/0 | 10.10.1.1 | 255.255.255.0 | N/A |
| G0/0/1 | 2001:db8:1::1 | /64 | N/A |
| S0/1/0 | 10.10.2.1 | 255.255.255.252 | N/A |
| 2001:db8:2::1 | /126 | N/A |
| RTR-3  *RTR-3*  *RTR-3*  *RTR-3* | G0/0/0 | 10.10.5.1 | 255.255.255.0 | N/A |
| G0/0/1 | 2001:db8:5::1 | /64 | N/A |
| S0/1/0  *S0/1/0* | 10.10.3.2 | 255.255.255.252 | N/A |
| 2001:db8:3::2 | /126 | N/A |
| PC-1 | NIC | 10.10.1.10 | 255.255.255.0 | 10.10.1.1 |
| Laptop A | NIC | 10.10.1.20 | 255.255.255.0 | 10.10.1.1 |
| PC-2 | NIC | 2001:db8:1::10 | /64 | fe80::1 |
| PC-3 | NIC | 2001:db8:1::20 | /64 | fe80::1 |
| PC-4 | NIC | 10.10.5.10 | 255.255.255.0 | 10.10.5.1 |
| Server 1 | NIC | 10.10.5.20 | 255.255.255.0 | 10.10.5.1 |
| Laptop B | NIC | 2001:db8:5::10 | /64 | fe80::1 |
| Laptop C | NIC | 2001:db8:5::20 | /64 | fe80::1 |
| Corporate Server  *Corporate Server* | NIC  *NIC* | 203.0.113.100 | 255.255.255.0 | 203.0.113.1 |
| 2001:db8:acad::100 | /64 | fe80::1 |

**Objectives**

In this lab you will use ICMP to test network connectivity and locate network problems. You will also correct simple configuration issues and restore connectivity to the network.

* Use ICMP to locate connectivity issues.
* Configure network devices to correct connectivity issues.

**Background**

Customers have been complaining that they can’t reach some network resources. You have been asked to test connectivity in the network. You use ICMP to find out which resources are unreachable and the locations from which they can’t be reached. Then, you use trace to locate the point at which network connectivity is broken. Finally, you fix the errors that you find to restore connectivity to the network.

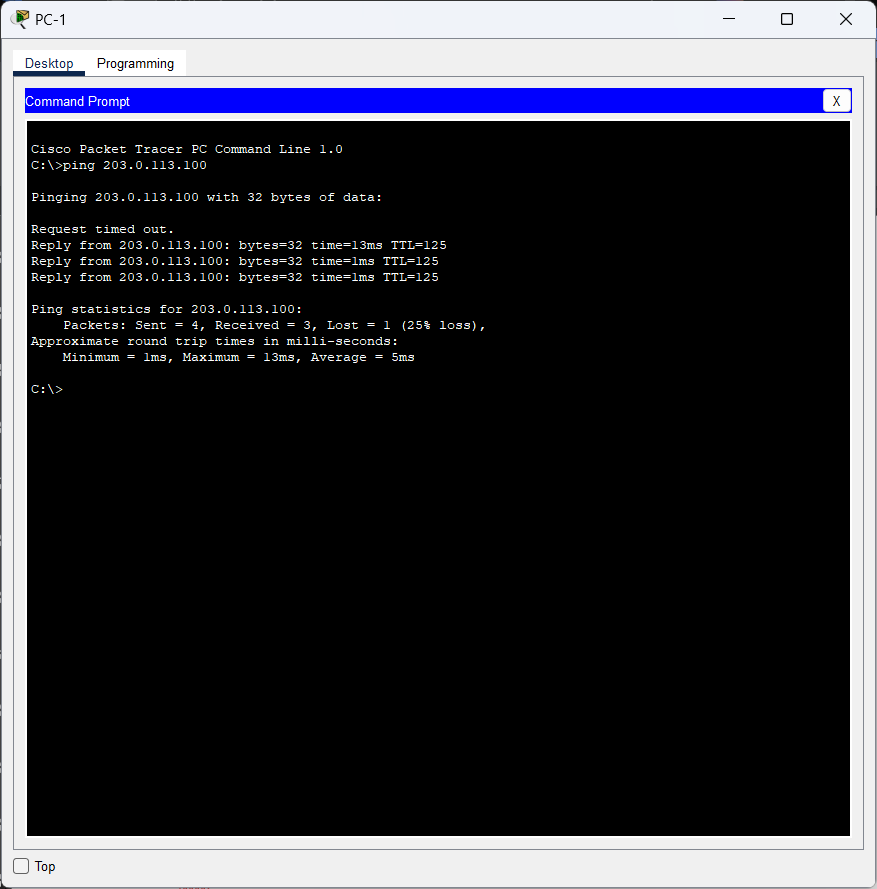
**Instructions**

All hosts should have connectivity to all other hosts and the Corporate Server.

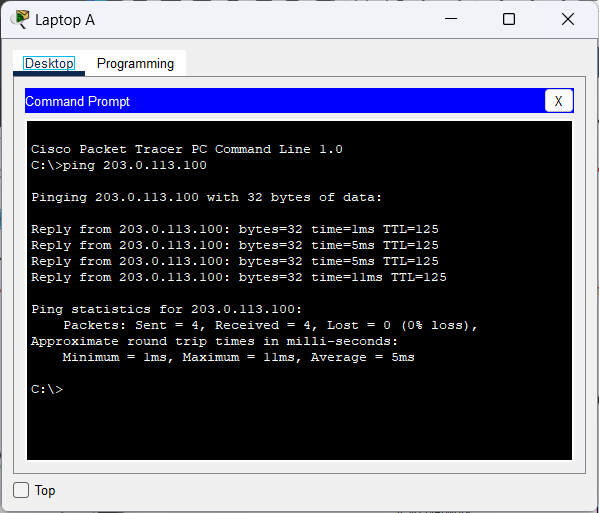
* Wait until all link lights are green.
* Select a host and use ICMP ping to determine which hosts are reachable from that host.
* If a host is found to be unreachable, use ICMP trace to locate the general location of the network errors.
* Locate the specific errors and correct them.

**Jawaban:**

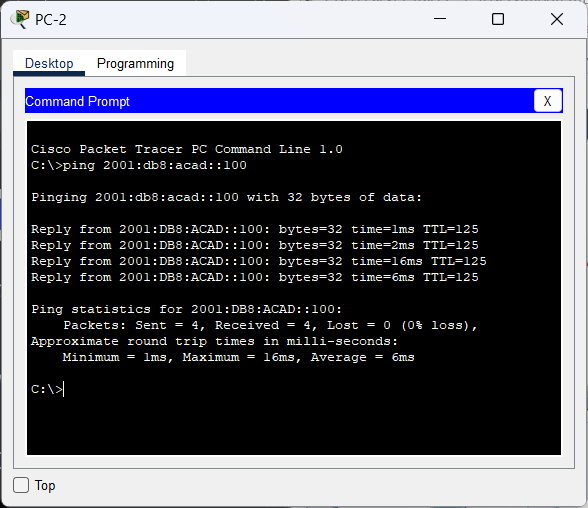
1. PC-1 ke Corporate Server dengan address 203.0.113.100

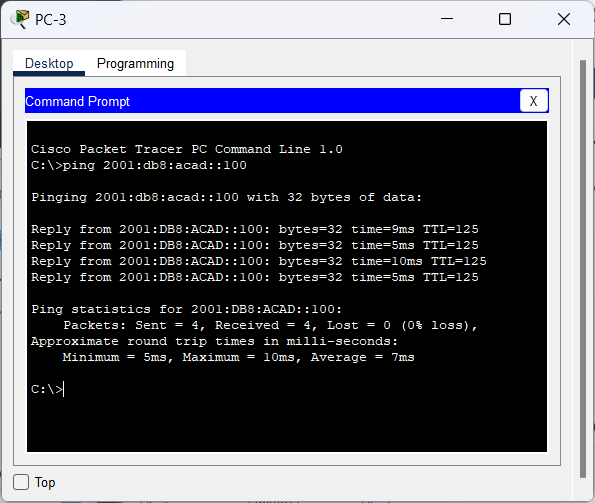


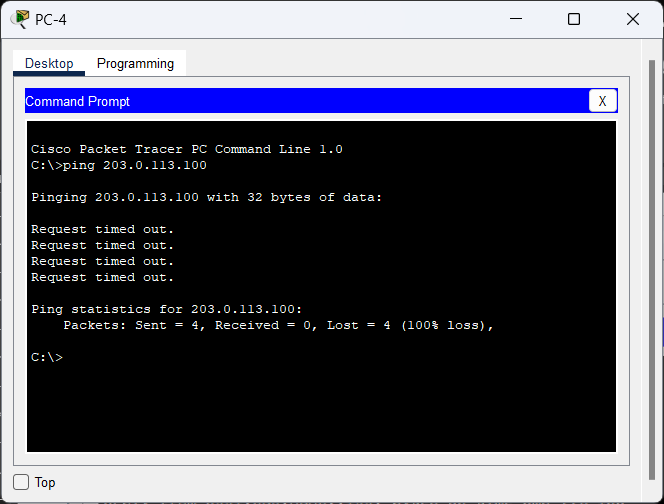
1. Laptop A ke Corporate Server dengan address 203.0.113.100

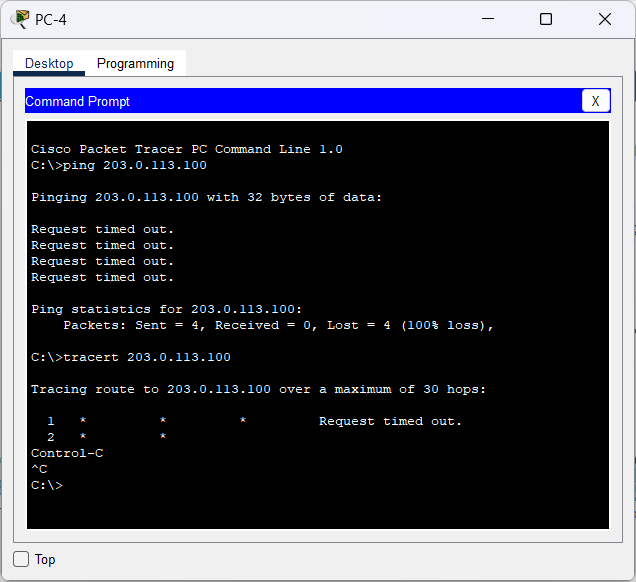


1. PC-2 ke Corporate Server dengan address 2001:db8:acad::100

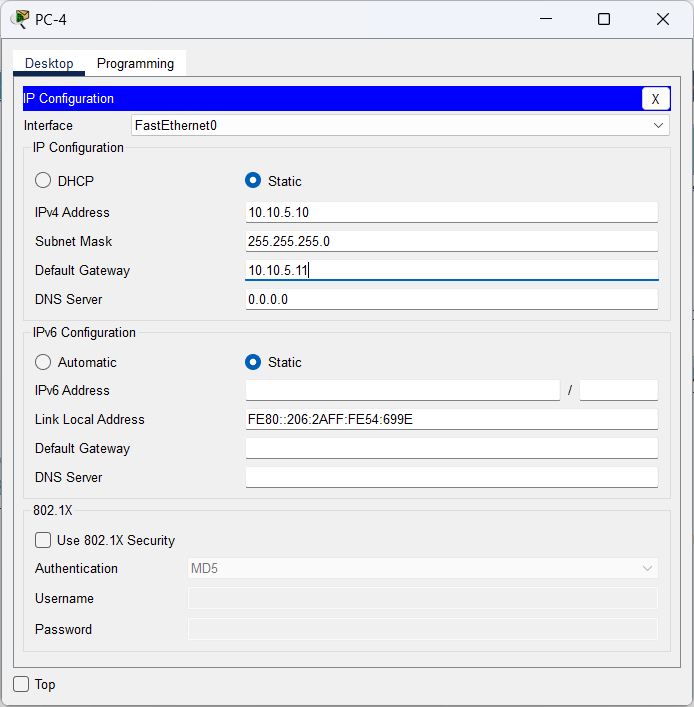
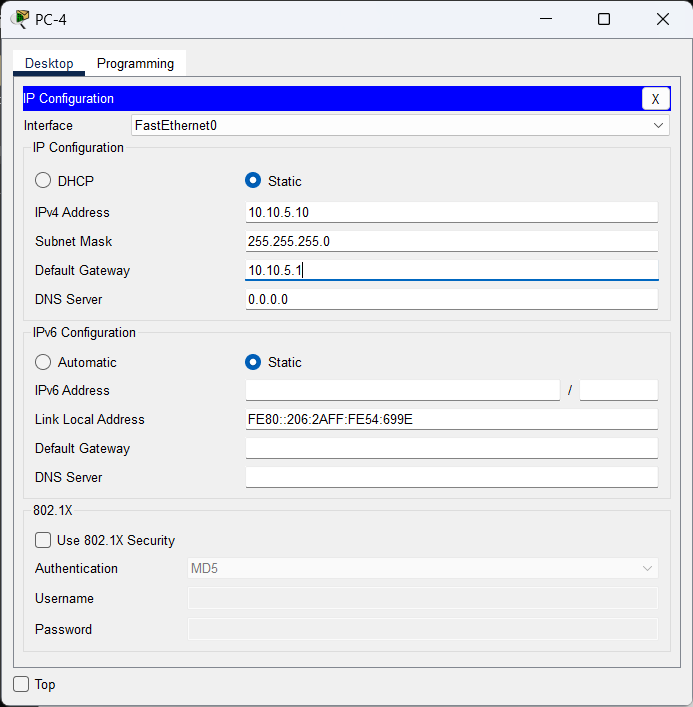


1. PC-3 ke Corporate Server dengan address 2001:db8:acad::100
2. PC-4 ke Corporate Server dengan address 203.0.113.100

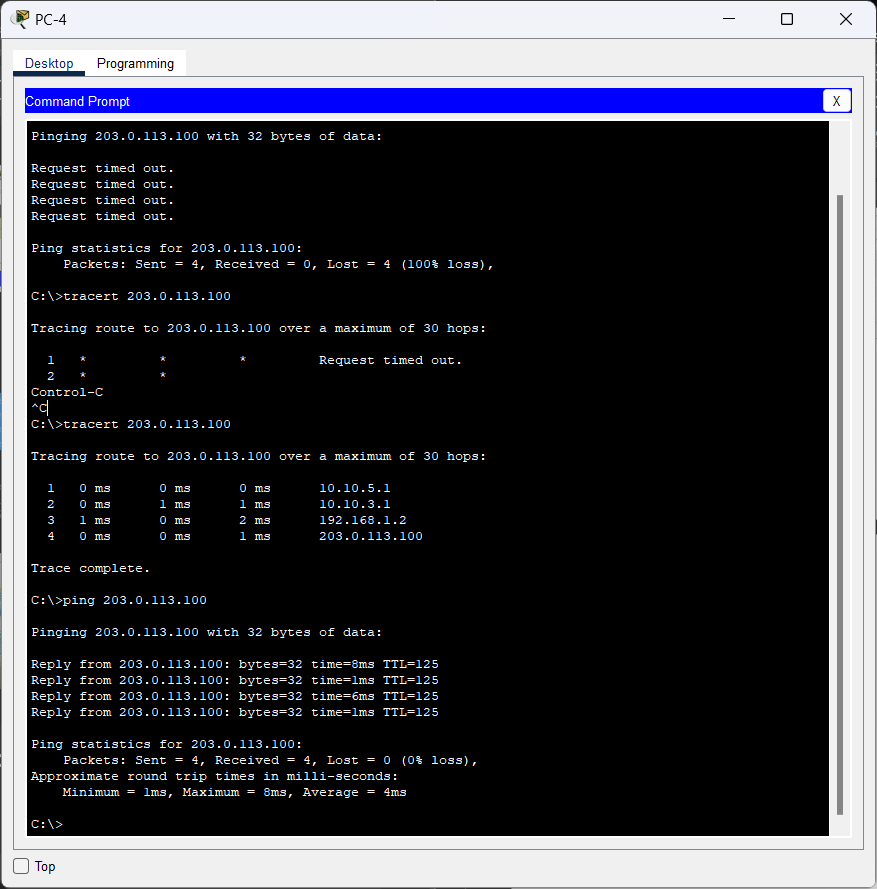




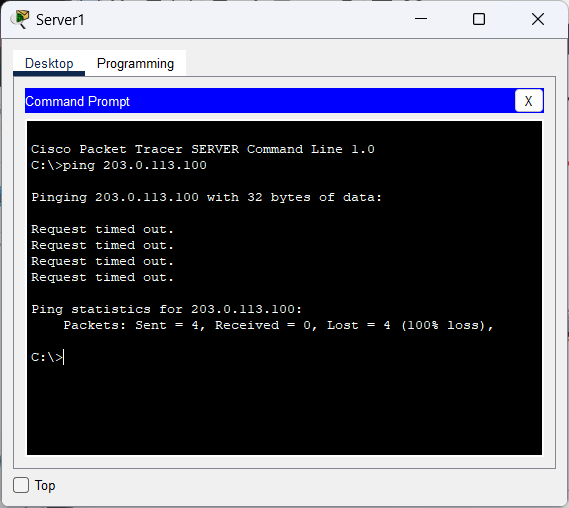
Karena waktu permintaannya telah habis, kita akan melakukan pengecekan pada IP Configuration. Ketika dicek dibagian **Default Gateway,** addressnya bermasalah sehingga diperbaiki jadi 10.10.5.1



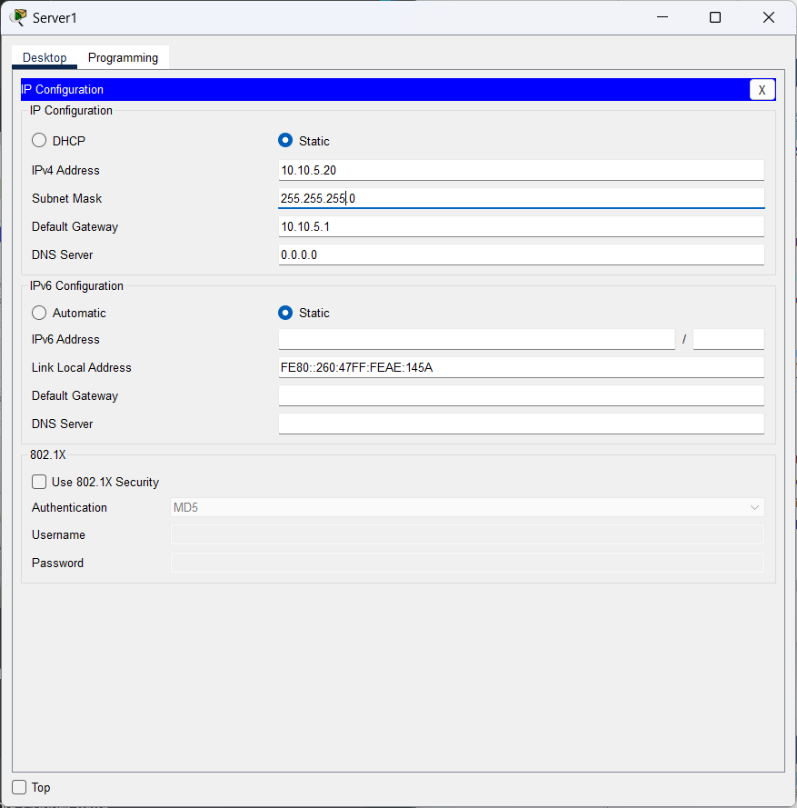
Setelah diperbaiki, kita akan lakukan ping dan tracer ke Corporate Server.



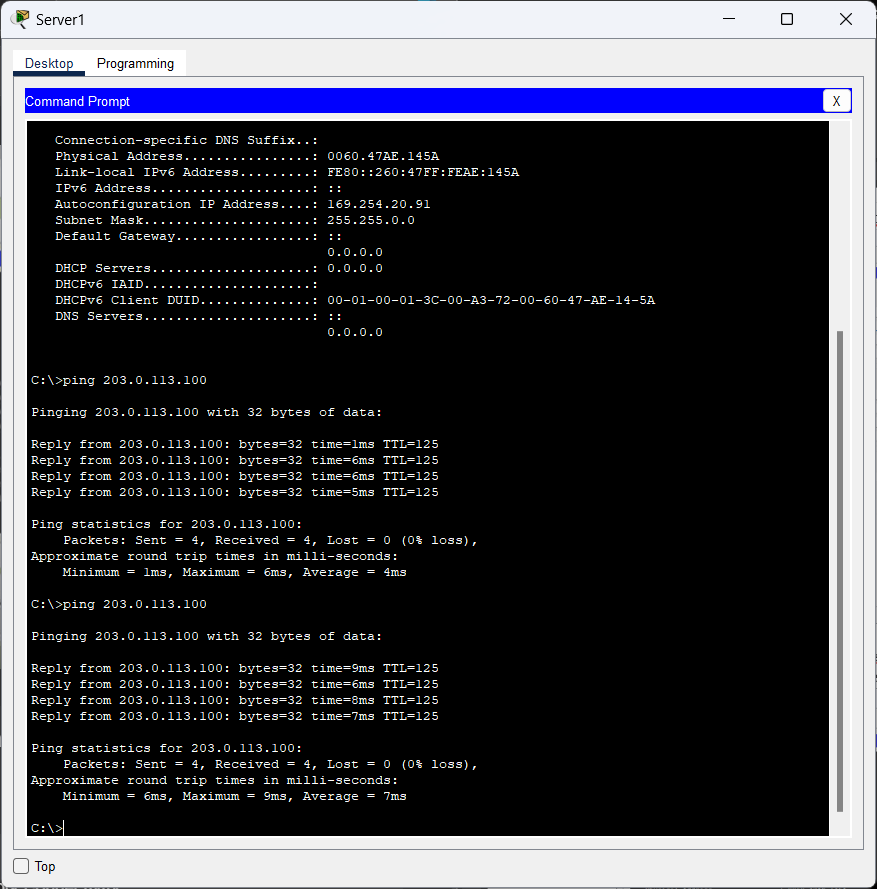
1. Server1 ke Corporate Server



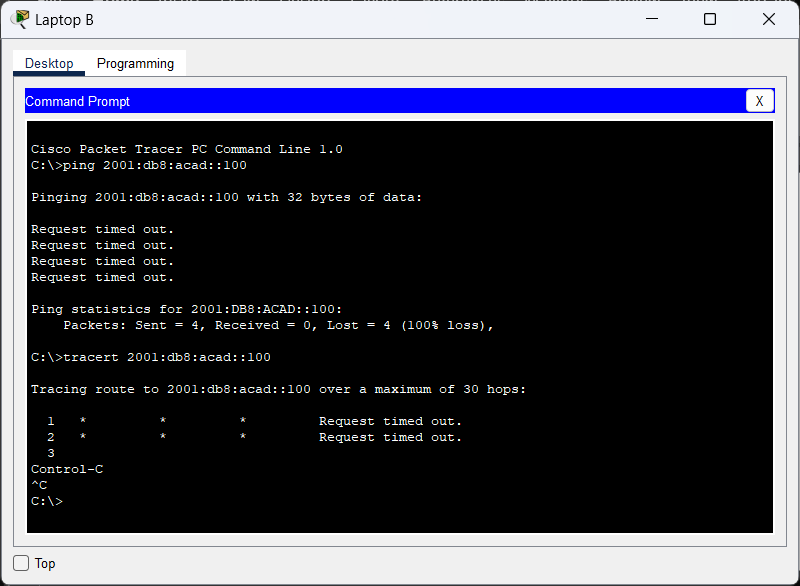
Karna disini ping nya tidak berhasil, kita akan lakukan perubahan pada konfigurasinya sesuai dengan **Addressing table** dan kita ubah jadi **Static**.



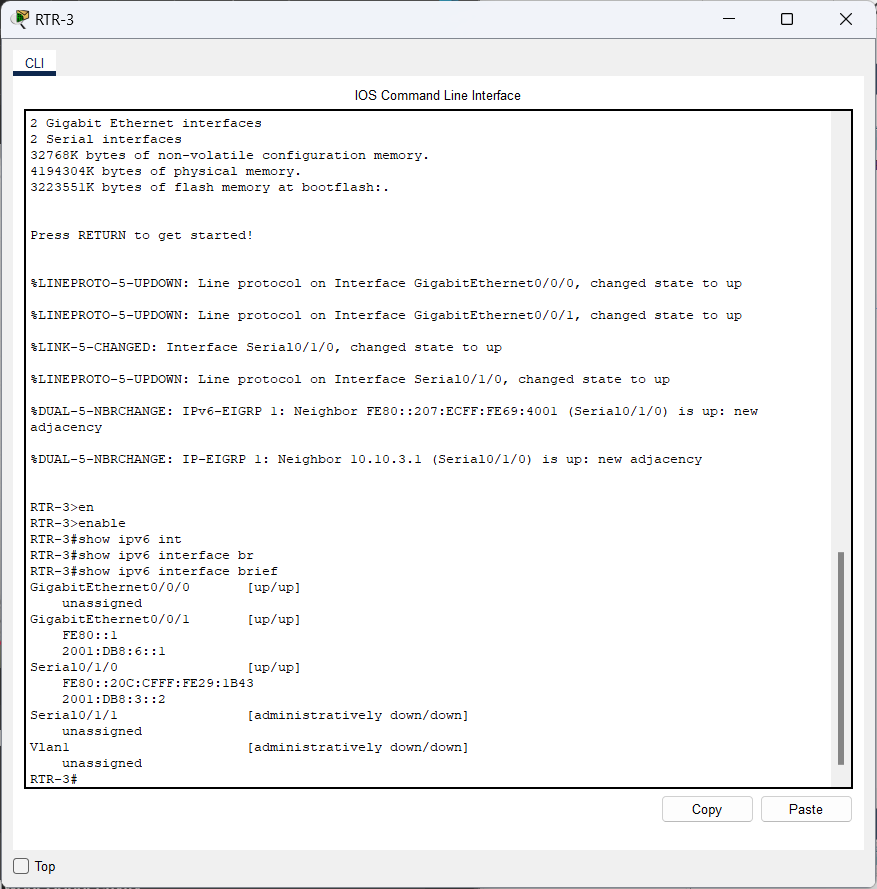
Setelah dilakukan perubahan konfigurasi, kita lakukan ping ke **Corporation Server.** Dan hasilnya bisa dilakukan ping ke **Corporation Server**.

****

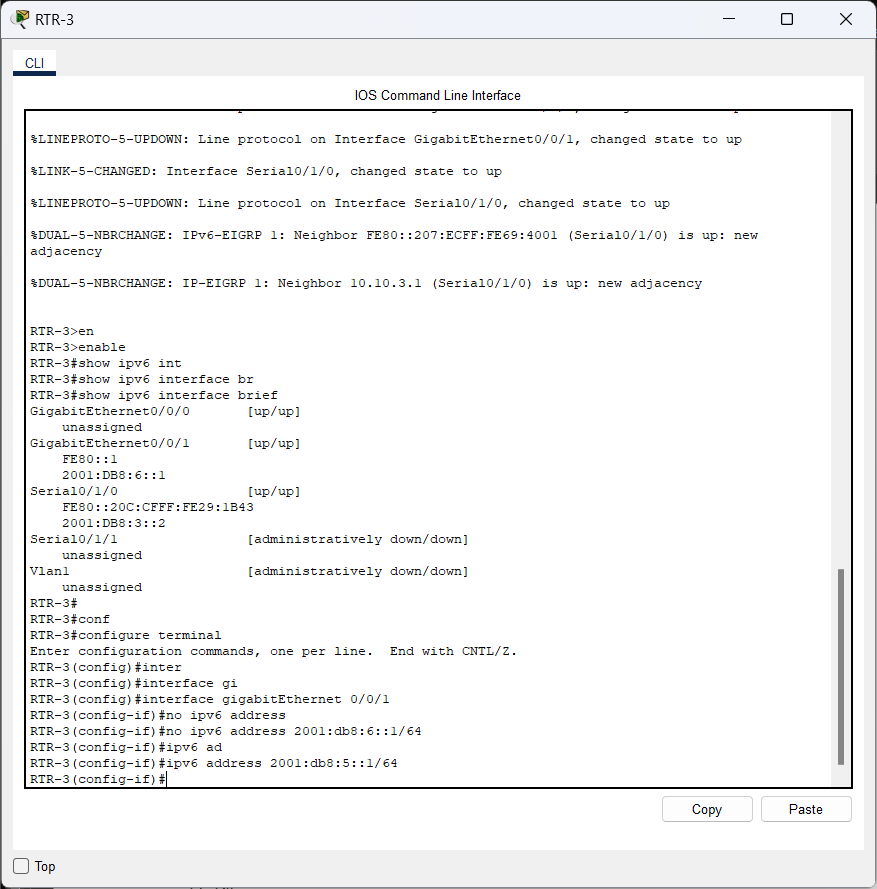
1. Laptop B ke Corporate Server



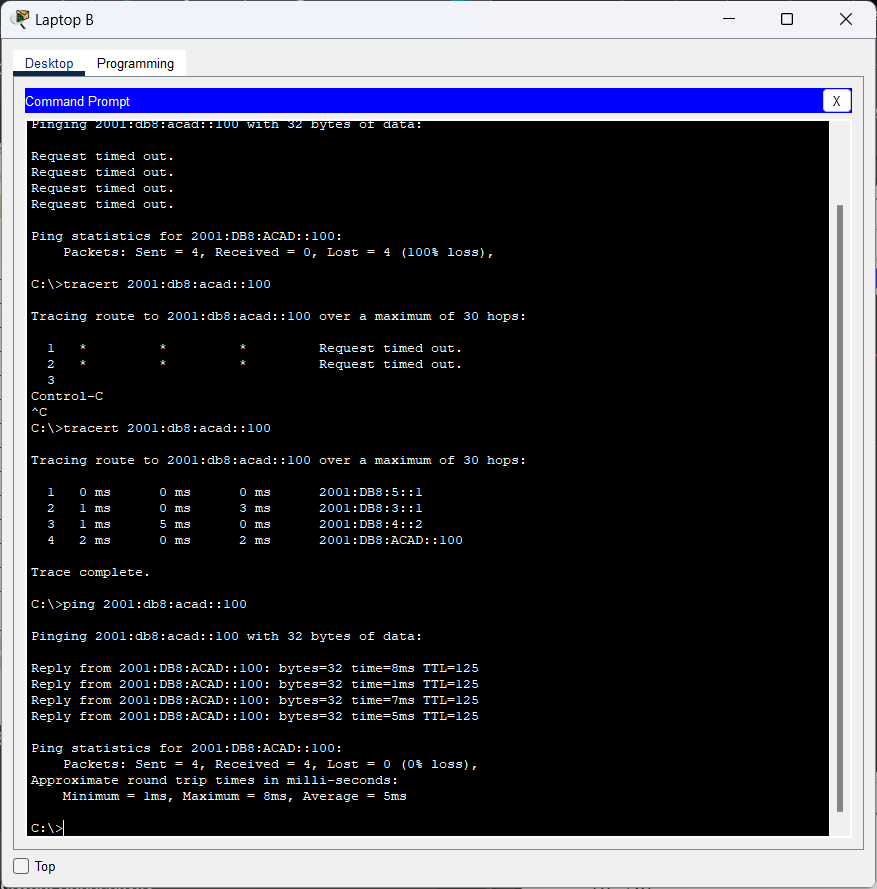
Kita akan lakukan pengecekan pada RTR-3 untuk menampilakn **ipv6**



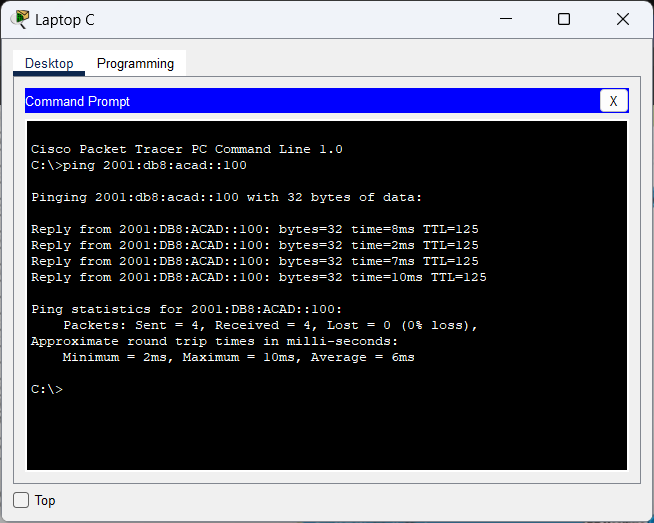
Kemudian, kita akan menghapus dan menambahkan **ipv6 address** pada RTR-3



Setelah itu, kita klik Laptop B dan lakukan tracert dan ping ke **Corporate Server** dengan address 2001:db8:acad::100.

****

1. Laptop C ke Corporate Server





**Packet Tracer - TCP and UDP Communications**

**Objectives**

**Part 1: Generate Network Traffic in Simulation Mode**

**Part 2: Examine the Functionality of the TCP and UDP Protocols**

**Background**

This simulation activity is intended to provide a foundation for understanding TCP and UDP in detail. Packet Tracer simulation mode provides you the ability to view the state of different PDUs as they travel through the network.

Packet Tracer Simulation mode enables you to view each of the protocols and the associated PDUs. The steps outlined below lead you through the process of requesting network services using various applications that are available on a client PC. You will explore the functionality of the TCP and UDP protocols, multiplexing, and the function of port numbers in determining which local application requested the data or is sending the data. Packet Tracer will not score this activity.

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

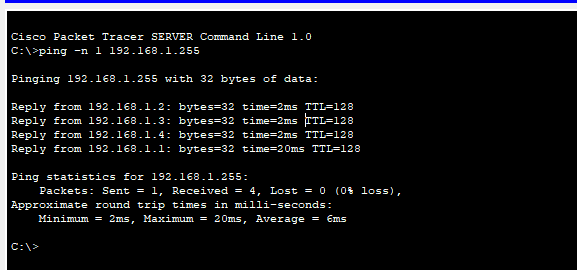
**Step 1: Generate traffic to populate Address Resolution Protocol (ARP) tables.**

Perform the following task to reduce the amount of network traffic viewed in the simulation. a. Click **MultiServer** and click the **Desktop** tab > **Command Prompt**.

A computer screen shot of a server

Description automatically generated

b. Enter the **ping -n 1 192.168.1.255** command. You are pinging the broadcast address for the client LAN. The command option will send only one ping request rather than the usual four. This will take a few seconds as every device on the network responds to the ping request from MultiServer. c. Close the **MultiServer** window.



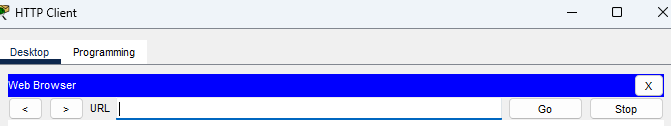
**Step 2: Generate web (HTTP) traffic.**

1. Switch to Simulation mode.

A blue and white keyboard with white text

Description automatically generated

1. Click **HTTP Client** and open the **Web Browser** from the desktop.



1. In the URL field, enter **192.168.1.254** and click **Go**. Envelopes (PDUs) will appear in the topology window.

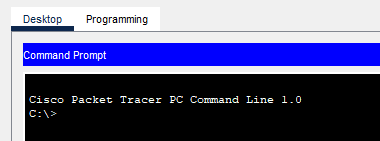
A blue and white stripes

Description automatically generated

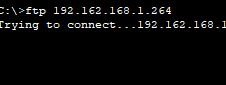
1. Minimize, but do not close, the **HTTP Client** configuration window.

**Step 3: Generate FTP traffic.**

1. Click **FTP Client** and open the **Command Prompt** from the desktop



1. Enter the **ftp 192.168.1.254** command. PDUs will appear in the simulation window.



1. Minimize, but do not close, the **FTP Client** configuration window.

**Step 4: Generate DNS traffic.**

1. Click DNS Client and open the **Command Prompt**.
2. Enter the **nslookup multiserver.pt.ptu** command. A PDU will appear in the simulation window.

A screenshot of a computer

Description automatically generated

1. Minimize, but do not close, the **DNS Client** configuration window.

Cisco and/or its affiliates. All rights reserved. Cisco

**Step 5: Generate Email traffic.**

1. Click **E-Mail Client** and open the **E Mail** tool from the Desktop.
2. Click **Compose** and enter the following information:
   1. **To:** user@multiserver.pt.ptu
   2. **Subject:** personalize the subject line
   3. **E-Mail Body:** personalize the Email

A screenshot of a computer

Description automatically generated

1. Click **Send**.
2. Minimize, but do not close, the **E-Mail Client** configuration window.

A computer screen shot of a computer

Description automatically generated

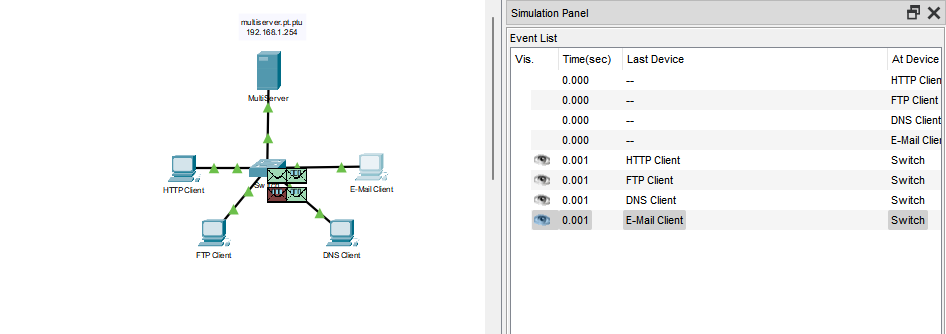
**Step 6: Verify that the traffic is generated and ready for simulation.**

There should now be PDU entries in the simulation panel for each of the client computers.

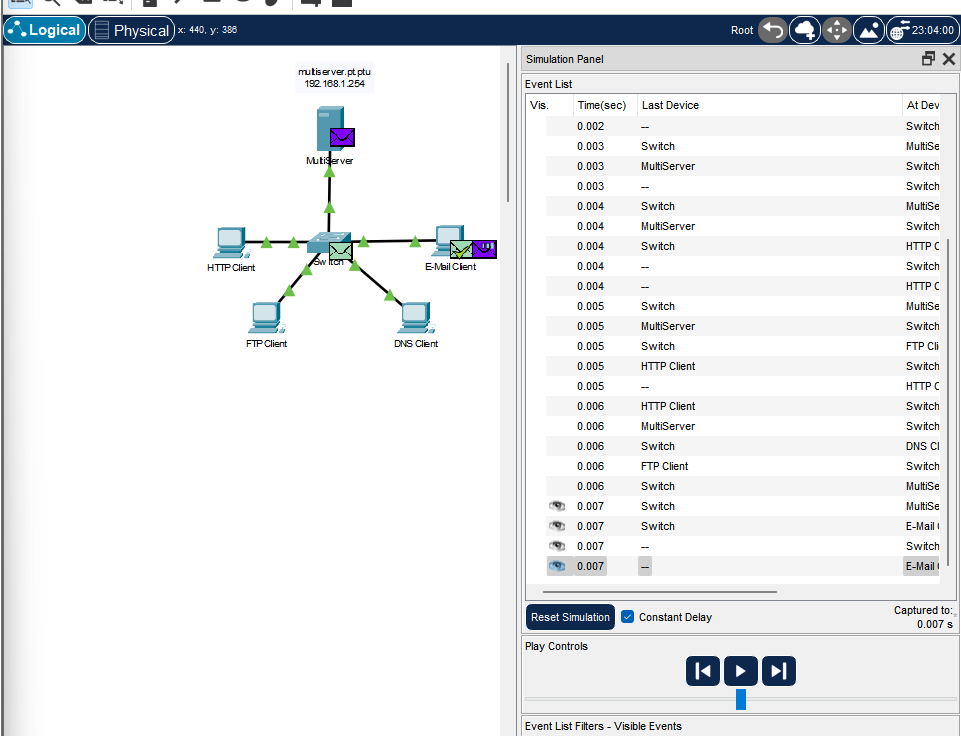
**Step 7: Examine multiplexing as the traffic crosses the network.**

You will now use the **Capture/Forward button** in the Simulation Panel to observe the different protocols travelling on the network.

**Note**: The **Capture/Forward** button ‘ **>|** ‘ is a small arrow pointing to the right with a vertical bar next to it. a. a. Click **Capture/Forward** once. All of the PDUs travel to the switch.

****

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.



Questions:

What is this called?

**Jawaban : Ini disebut komunikasi half-duplex, di mana data bisa berjalan dua arah tapi hanya satu arah pada satu waktu.**

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

**Jawaban :**

Warna-warna yang berbeda pada PDUs dalam Simulation Panel biasanya menunjukkan tipe protokol atau lapisan jaringan yang berbeda yang sedang dilacak. Berikut adalah beberapa contoh umum:

**Warna hijau:** Biasanya untuk protokol lapisan aplikasi, seperti HTTP atau DNS.

**Warna biru:** Menunjukkan protokol lapisan transport, seperti TCP atau UDP.

**Warna merah:** Digunakan untuk protokol lapisan jaringan, seperti IP.

**Warna oranye:** Menunjukkan lapisan data link, seperti Ethernet atau frame relay.

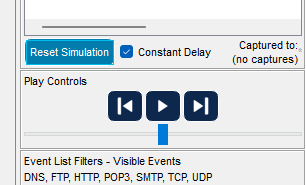
**Warna kuning:** Bisa digunakan untuk ICMP (protokol kendali).

Setiap warna membantu membedakan jenis PDU yang sedang diproses pada setiap lapisan dalam model OSI atau TCP/IP.

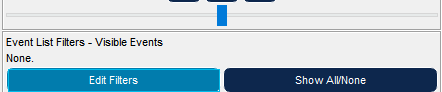
**Part 2: Examine Functionality of the TCP and UDP Protocols**

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

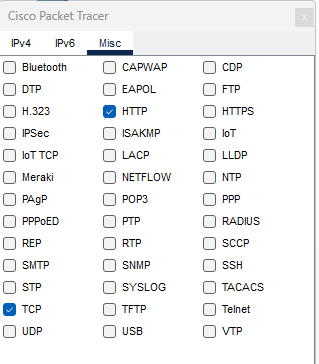
1. Click **Reset Simulation**.



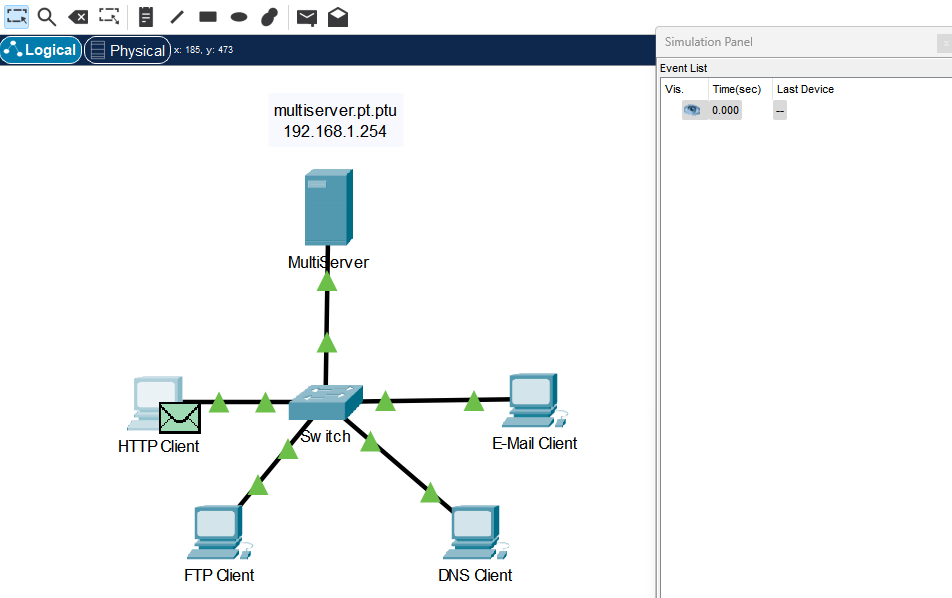
1. Filter the traffic that is currently displayed to only **HTTP** and **TCP** PDUs. To filter the traffic that is currently displayed:
   1. Click **Edit Filters** and toggle the **Show All/None** button.



* 1. Select **HTTP** and **TCP**. Click the red “x” in the upper right-hand corner of the Edit Filters box to close it. Visible Events should now display only **HTTP** and **TCP** PDUs.



1. Open the browser on HTTP Client and enter **192.168.1.254** in the URL field. Click **Go** to connect to the server over HTTP. Minimize the HTTP Client window.



1. 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?

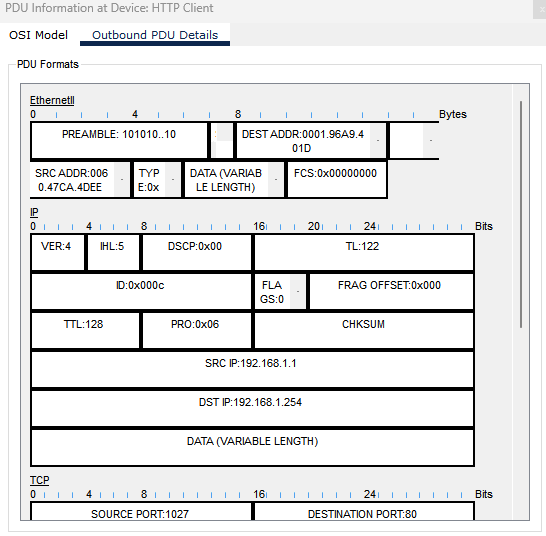
A screenshot of a computer

Description automatically generated

**Jawaban :**

**Karena tcp house membuka dahulu dengan multi server sehingga koneksi melakukan pertukaran data.**

1. 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.



Questions:

What is the section labeled?

**Jawaban : Pada Outbound PDU Details, bagian kedua dari terakhir biasanya diberi label "OSI Model" atau "Layer 2" (tergantung pada implementasi atau protokol yang digunakan). Bagian ini menggambarkan bagaimana PDU tersebut sesuai dengan model OSI atau TCP/IP dan menunjukkan detail header serta trailer yang melekat pada paket data sesuai dengan lapisan jaringan yang relevan.**

Are these communications considered to be reliable?

**Jawaban : Keandalan komunikasi bergantung pada protokol. TCP dianggap reliable, sementara UDP dianggap unreliable.**

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

**Jawaban :**

**SRC PORT : 1027**

**DEST PORT : 80**

**SEQUENCE NUM : 1**

**ACK NUM : 1**

1. 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.

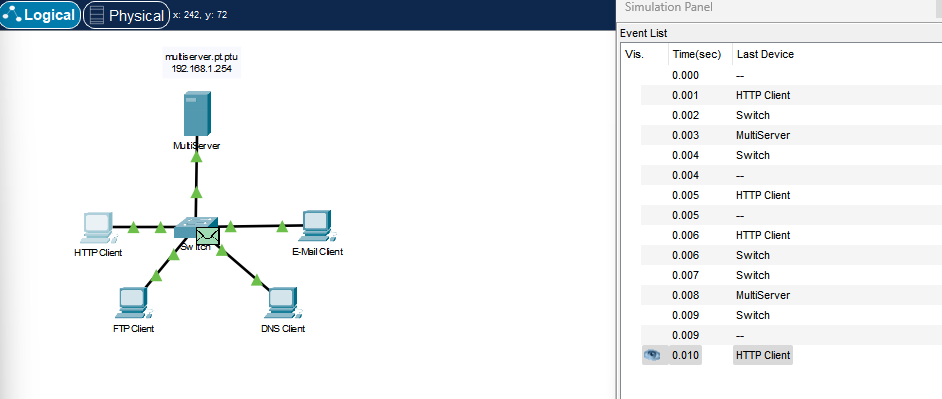
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Flag Place | **6** | **5** | **4** | **3** | **2** | **1** |
| Value | URG | ACK | PSH | RST | SYN | FIN |

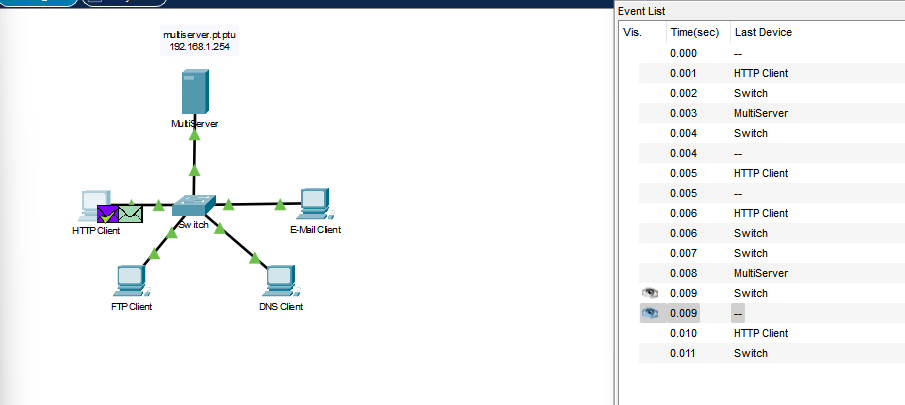
Question:

Which TCP flags are set in this PDU?

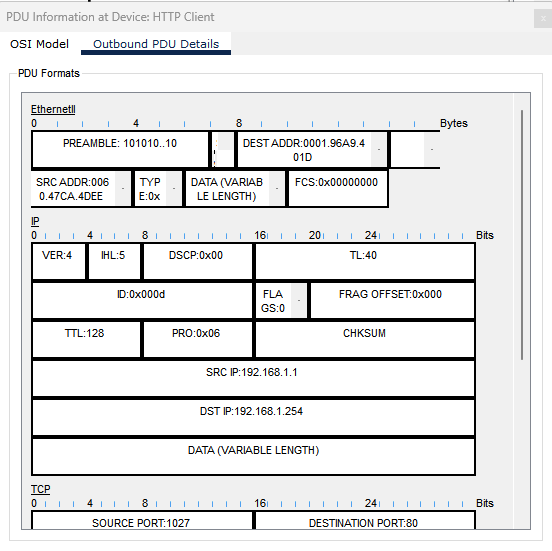
**Jawaban : PSH**

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





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



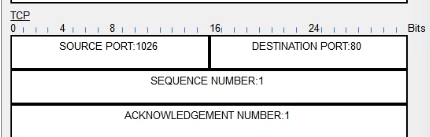
Question:

How are the port and sequence numbers different than before?

**Jawaban :**

****

1. 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**.



Question:

What information is now listed in the TCP section? How are the port and sequence numbers different from the previous two PDUs?

**Jawaban : SEQ NUM nya berubah menjadi 1**

1. Reset the simulation.

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

1. Open the command prompt on the FTP Client desktop. Initiate an FTP connection by entering **ftp 192.168.1.254**.

A computer screen shot of a black and blue screen

Description automatically generated

1. In the Simulation Panel, change **Edit Filters** to display only **FTP** and **TCP**.

A close up of a screen

Description automatically generated

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

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

Question:

Are these communications considered to be reliable?

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

A white rectangular box with black text

Description automatically generated

Question:

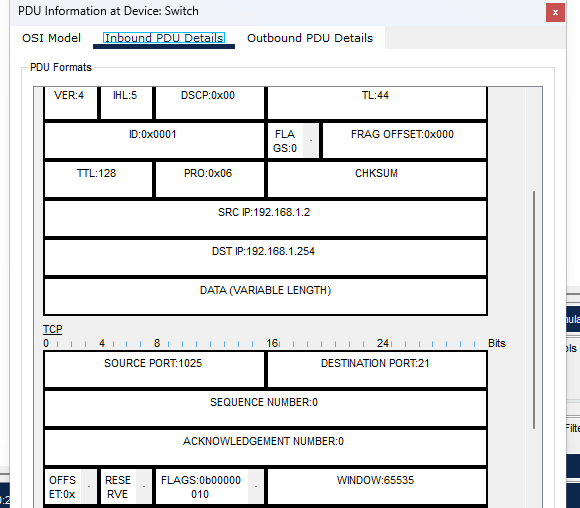
What is the value in the flagfield?



1. Close the PDU and click **Capture/Forward** until a PDU returns to the **FTP Client** with a checkmark.
2. Click the PDU envelope and select **Inbound PDU Details**.

Question:

How are the port and sequence numbers different than before?



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

A screenshot of a computer

Description automatically generated

Question:

How are the port and sequence numbers different from the previous results?

**Answer:** 1025, 21, 1, 1. The source and destination ports are reversed, and both the sequence number and acknowledgement are 1.

1. Close the PDU and click **Capture/Forward** until a second PDU returns to the **FTP Client**. The PDU is a different color.
2. Open the PDU and select **Inbound PDU Details**. Scroll down past the TCP section.

Question:

What is the message from the server?

**Answer**: Welcome to PUT Ftp server

1. Click Reset Simulation.

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

1. Repeat the steps in Part 1 to create DNS traffic.
2. In the Simulation Panel, change **Edit Filters** to display only **DNS** and **UDP**.
3. Click the PDU envelope to open it.
4. Look at the OSI Model details for the outbound PDU.

Question:

What is the Layer 4 protocol?

**Answer :** UDP

Are these communications considered to be reliable?

**Answer**: no, it is not always absolutely reliable, but the DNS protocol has a fallback mechanism that can ensure the client eventually gets the required response in case of failure.

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

Question:

Why are there no sequence and acknowledgement numbers?

**Answer**: 1025 (value may vary) and 53. Because UDP does not need to establish a reliable connection.Type

1. Close the **PDU** and click **Capture/Forward** until a PDU with a check mark returns to the **DNS Client**.
2. Click the PDU envelope and select **Inbound PDU Details**.

Question:

How are the port and sequence numbers different than before?

**Answer**: 53, 1025. 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**?

**Answer:** 53, 1025. The source and destination ports are reversed.swers here

1. Click Reset Simulation.

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

a. Ulangi langkah-langkah di Bagian 1 untuk mengirim email ke user@multiserver.pt.ptu.

b. Di Panel Simulasi, ubah Edit Filter untuk hanya menampilkan POP3, SMTP, dan TCP.

c. Klik amplop PDU pertama untuk membukanya.

d. Klik tab Detail PDU Keluar dan gulir ke bawah ke bagian terakhir.

**Pertanyaan:**

Protokol lapisan transport apa yang digunakan lalu lintas email?

**Jawaban:** TCP

Apakah komunikasi ini dianggap andal?

**Jawaban:** Ya, TCP dianggap komunikasi yang andal karena menggunakan koneksi yang terjamin, pengiriman ulang paket yang hilang, urutan pengiriman yang benar, dan kontrol aliran dan kemacetan.

e. Catat nilai SRC PORT, DEST PORT, SEQUENCE NUM, dan ACK NUM. Berapa nilai bidang bendera?

**Jawaban:** 1025 (nilai dapat bervariasi), 25, 0, 0. SYN.

f. Tutup PDU dan klik Capture/Forward hingga PDU kembali ke Klien Email dengan tanda centang. g. Klik amplop TCP PDU dan pilih Inbound PDU Details.

**Pertanyaan:**

Apa perbedaan nomor port dan urutan dengan sebelumnya?

**Jawaban:** 25, 1025, 0, 1. SYN+ACK. Port sumber dan tujuan dibalik, dan nomor pengakuan adalah 1.Ketik

h. Klik tab Outbound PDU Details

**Pertanyaan:**

Apa perbedaan nomor port dan urutan dari dua hasil sebelumnya

**Jawaban:**

Nomor port sumber dan tujuan dibalik antara hasil sebelumnya dan saat ini, dengan port sumber menjadi 25 dan port tujuan menjadi 1025, sementara nomor urutan tetap 0 dan nomor pengakuan berubah menjadi 1.

i. Ada PDU kedua dengan warna berbeda yang telah disiapkan oleh Klien Email untuk dikirim ke MultiServer. Ini adalah awal komunikasi email. Klik amplop PDU kedua ini dan pilih Outbound PDU Details.

**Pertanyaan:**Apa perbedaan nomor port dan urutan dari dua PDU sebelumnya?

**Jawaban:** Nomor port pada PDU kedua kemungkinan menunjukkan port sumber dan tujuan yang sesuai dengan protokol email (misalnya, 25 untuk SMTP), sementara nomor urutan mencerminkan posisi dalam komunikasi yang baru dimulai dan mungkin berbeda dari dua PDU sebelumnya.Jenis

**Pertanyaan** : Protokol email apa yang dikaitkan dengan port TCP 25? Protokol apa yang terkait dengan port TCP 110?

**Jawaban:** Protokol email yang terkait dengan port TCP 25 adalah SMTP (Simple Mail Transfer Protocol), sedangkan protokol yang terkait dengan port TCP 110 adalah POP3 (Post Office Protocol versi 3).



**Packet Tracer - Use Ping and Traceroute to Test Network Connectivity**

**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 |  |  |  |
| PC2 | NIC |  | |  |
| PC3 | NIC |  |  |  |
| PC4 | NIC |  | |  |

**Objectives**

**Part 1: Test and Restore IPv4 Connectivity Part 2: Test and Restore IPv6 Connectivity**

**Scenario**

There are connectivity issues in this activity. In addition to gathering and documenting information about the network, you will locate the problems and implement acceptable solutions to restore connectivity.

**Note:** The user EXEC password is **cisco**. The privileged EXEC password is **class**.

**Instructions**

**Part 1: Test and Restore IPv4 Connectivity**

**Step 1: Use ipconfig and ping to verify connectivity.**

1. Click **PC1** and open the **Command Prompt**.
2. Enter the **ipconfig /all** command to collect the IPv4 information. Complete the **Addressing Table** with the IPv4 address, subnet mask, and default gateway.
3. Click **PC3** and open the **Command Prompt**.
4. Enter the **ipconfig /all** command to collect the IPv4 information. Complete the **Addressing Table** with the IPv4 address, subnet mask, and default gateway.
5. Use the **ping** command to test connectivity between **PC1** and **PC3**. The ping should fail.

**Step 2: Locate the source of connectivity failure.**

1. From **PC1**, enter the necessary command to trace the route to **PC3**. What is the last successful IPv4 address that was reached?
2. The trace will eventually end after 30 attempts. Enter **Ctrl**+**C** to stop the trace before 30 attempts.
3. From **PC3**, enter the necessary command to trace the route to **PC1**. What is the last successful IPv4 address that was reached?
4. Enter **Ctrl**+**C** to stop the trace.
5. Click **R1**. Press **ENTER** and log in to the router.
6. 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?

1. 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?

Type your answers here.

1. Repeat steps 2e through 2g with **R3** and record your answers.
2. Click **R2**. Press **ENTER** and log into the router.
3. Enter the **show ip interface brief** command and record your addresses.
4. 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?

What solution would you propose to correct the problem? Type your answers here.

**Step 4: Implement the plan.**

Implement the solution you proposed in Step 3b.

**Step 5: Verify that connectivity is restored.**

1. From **PC1** test connectivity to **PC3**.
2. From **PC3** test connectivity to **PC1**. Is the problem resolved?

**Step 6: Document the solution.**

**Part 2: Test and Restore IPv6 Connectivity**

**Step 1: Use ipv6config and ping to verify connectivity.**

1. Click **PC2** and open the **Command Prompt**.
2. Enter the **ipv6config /all** command to collect the IPv6 information. Complete the **Addressing Table** with the IPv6 address, subnet prefix, and default gateway.
3. Click **PC4** and open the **Command Prompt**.
4. Enter the **ipv6config /all** command to collect the IPv6 information. Complete the **Addressing Table** with the IPv6 address, subnet prefix, and default gateway.
5. Test connectivity between **PC2** and **PC4**. The ping should fail.

**Step 2: Locate the source of connectivity failure.**

1. From **PC2**, enter the necessary command to trace the route to **PC4**. What is the last successful IPv6 address that was reached?
2. The trace will eventually end after 30 attempts. Enter **Ctrl**+**C** to stop the trace before 30 attempts.
3. From **PC4**, enter the necessary command to trace the route to **PC2**. What is the last successful IPv6 address that was reached?
4. Enter **Ctrl**+**C** to stop the trace.
5. Click **R3**. Press **ENTER** and log in to the router.
6. 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?

1. 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?

What solution would you propose to correct the problem?

**Step 4: Implement the plan.**

Implement the solution you proposed in Step 3b.

**Step 5: Verify that connectivity is restored.**

1. From **PC2** test connectivity to **PC4**.
2. From **PC4** test connectivity to **PC2**. Is the problem resolved?

**Step 6: Document the solution.**