МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ   
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение

высшего образования

«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. В. И. ВЕРНАДСКОГО»

ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ

Кафедра компьютерной инженерии и моделирования

**ACLs**

Отчет по лабораторной работе № 6

по дисциплине «Компьютерные сети»

студента 2 курса группы ПИ-б-о-231(2)  
Аметов Кемран Ленверович

Направления подготовки 09.03.01«Информатика и вычислительная техника»

Симферополь, 2024

**Packet Tracer - Troubleshooting IPv4 ACLs**

**Addressing Table**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **Default Gateway** |
| R1 | G0/0 | 10.0.0.1 | 255.0.0.0 | N/A |
| G0/1 | 172.16.0.1 | 255.255.0.0 | N/A |
| G0/2 | 192.168.0.1 | 255.255.255.0 | N/A |
| Server1 | NIC | 172.16.255.254 | 255.255.0.0 | 172.16.0.1 |
| Server2 | NIC | 192.168.0.254 | 255.255.255.0 | 192.168.0.1 |
| Server3 | NIC | 10.255.255.254 | 255.0.0.0 | 10.0.0.1 |
| L1 | NIC | 172.16.0.2 | 255.255.0.0 | 172.16.0.1 |
| L2 | NIC | 192.168.0.2 | 255.255.255.0 | 192.168.0.1 |
| L3 | NIC | 10.0.0.2 | 255.0.0.0 | 10.0.0.1 |

**Objectives**

**Part 1: Troubleshoot ACL Issue 1**

**Part 2: Troubleshoot ACL Issue 2**

**Part 3: Troubleshoot ACL Issue 3**

**Scenario**

This network is meant to have the following three policies implemented:

·        Hosts from the 192.168.0.0/24 network are unable to access any TCP service of **Server3**.

·        Hosts from the 10.0.0.0/8 network are unable to access the HTTP service of **Server1**.

·        Hosts from the 172.16.0.0/16 network are unable to access the FTP service of **Server2**.

**Note**: All FTP usernames and passwords are “**cisco**”.

No other restrictions should be in place. Unfortunately, the rules that have been implemented are not working correctly. Your task is to find and fix the errors related to the access lists on **R1**.

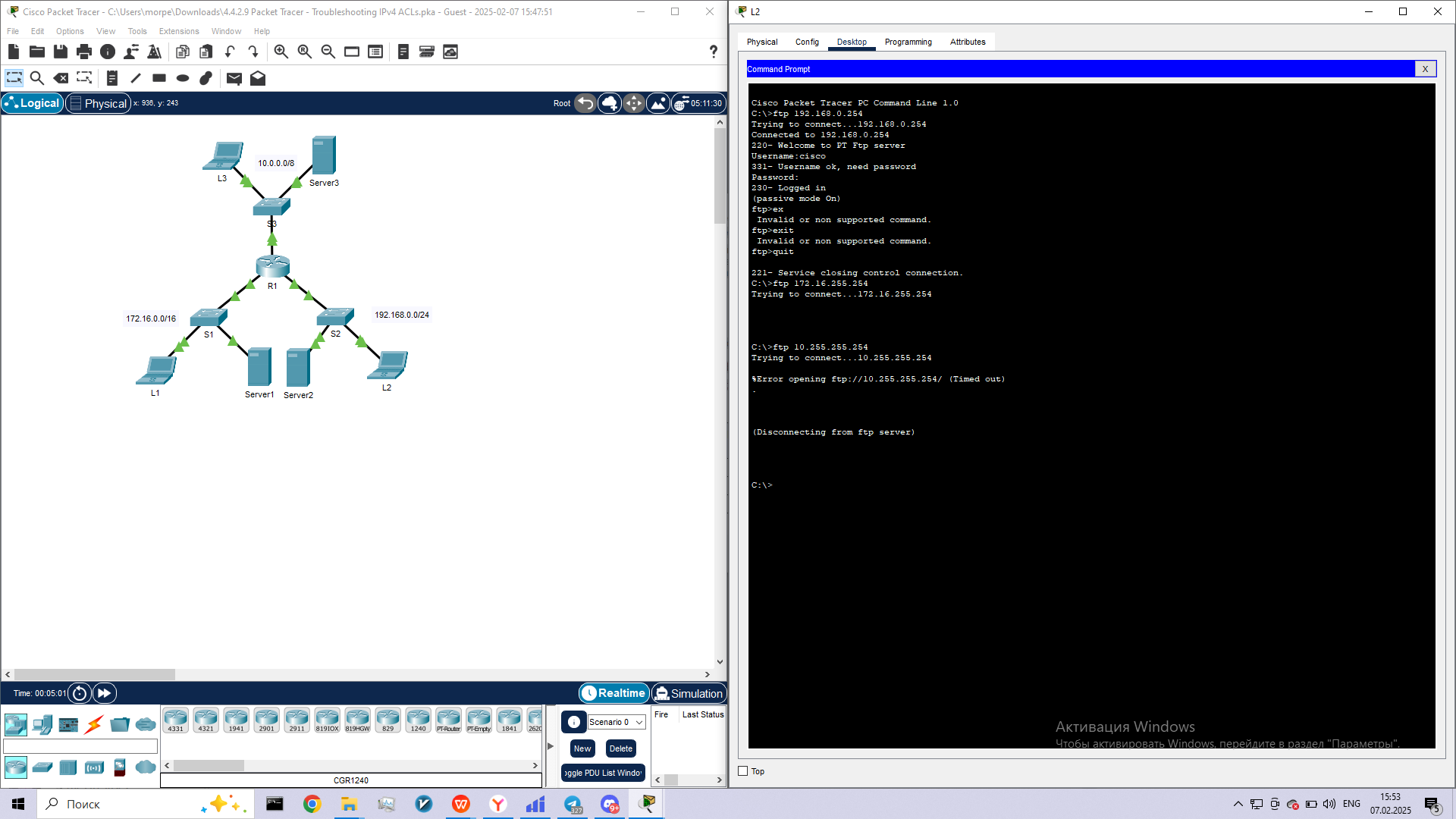
**Part 1:      Troubleshoot ACL Issue 1**

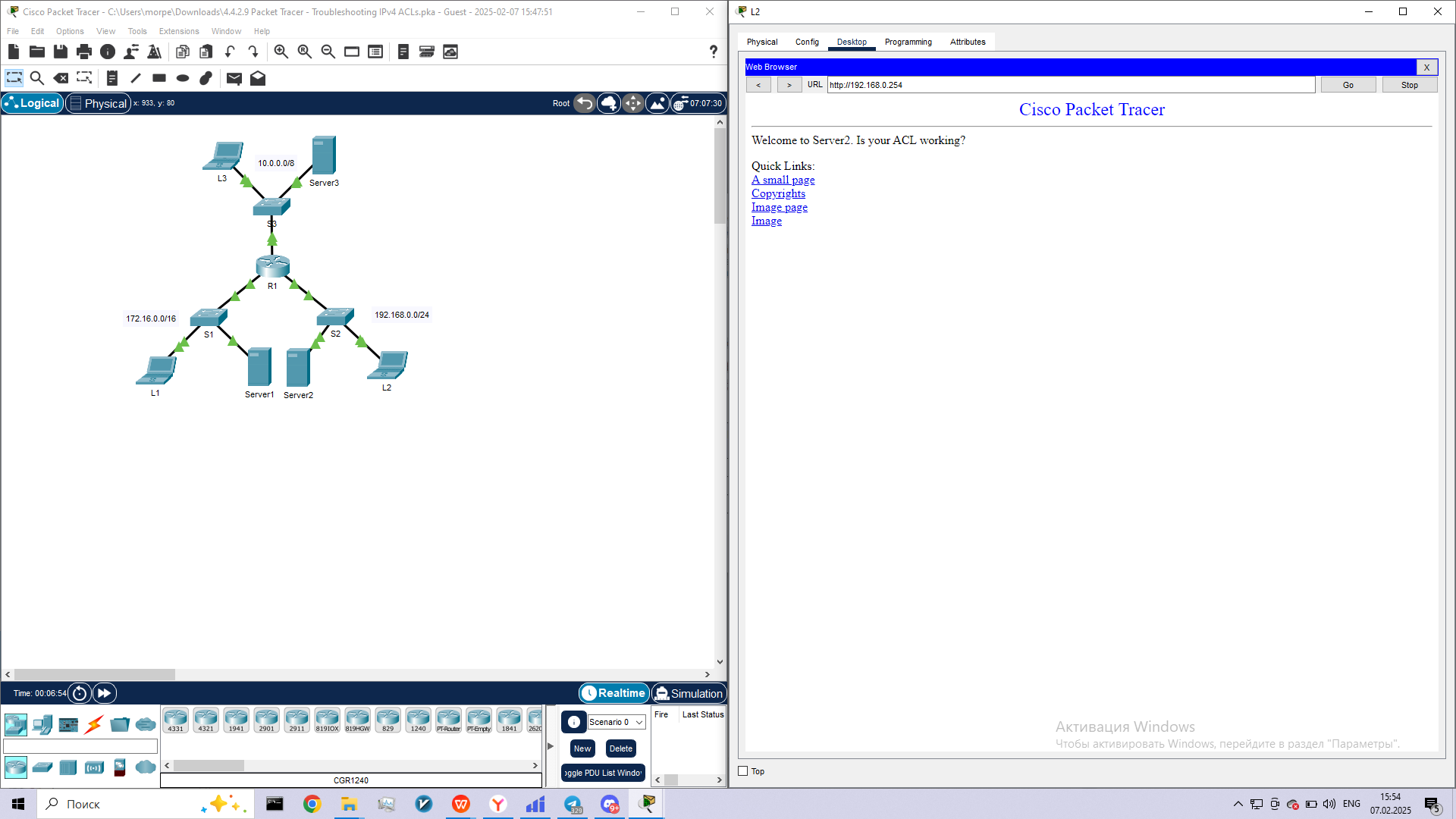
Hosts from the 192.168.0.0/24 network are intentionally unable to access any TCP service of **Server3**, but should not be otherwise restricted.

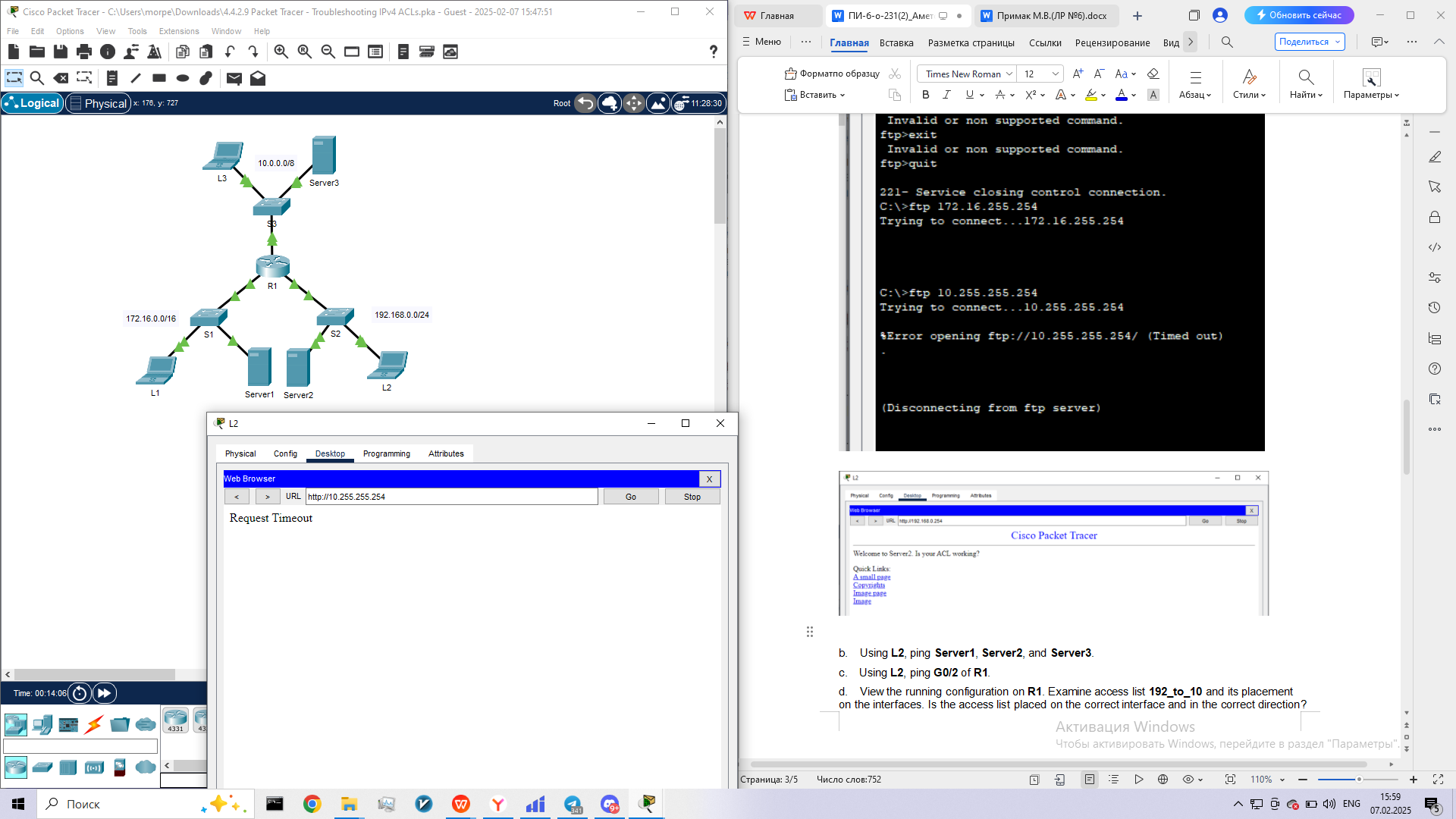
**Step 1:      Determine the ACL problem.**

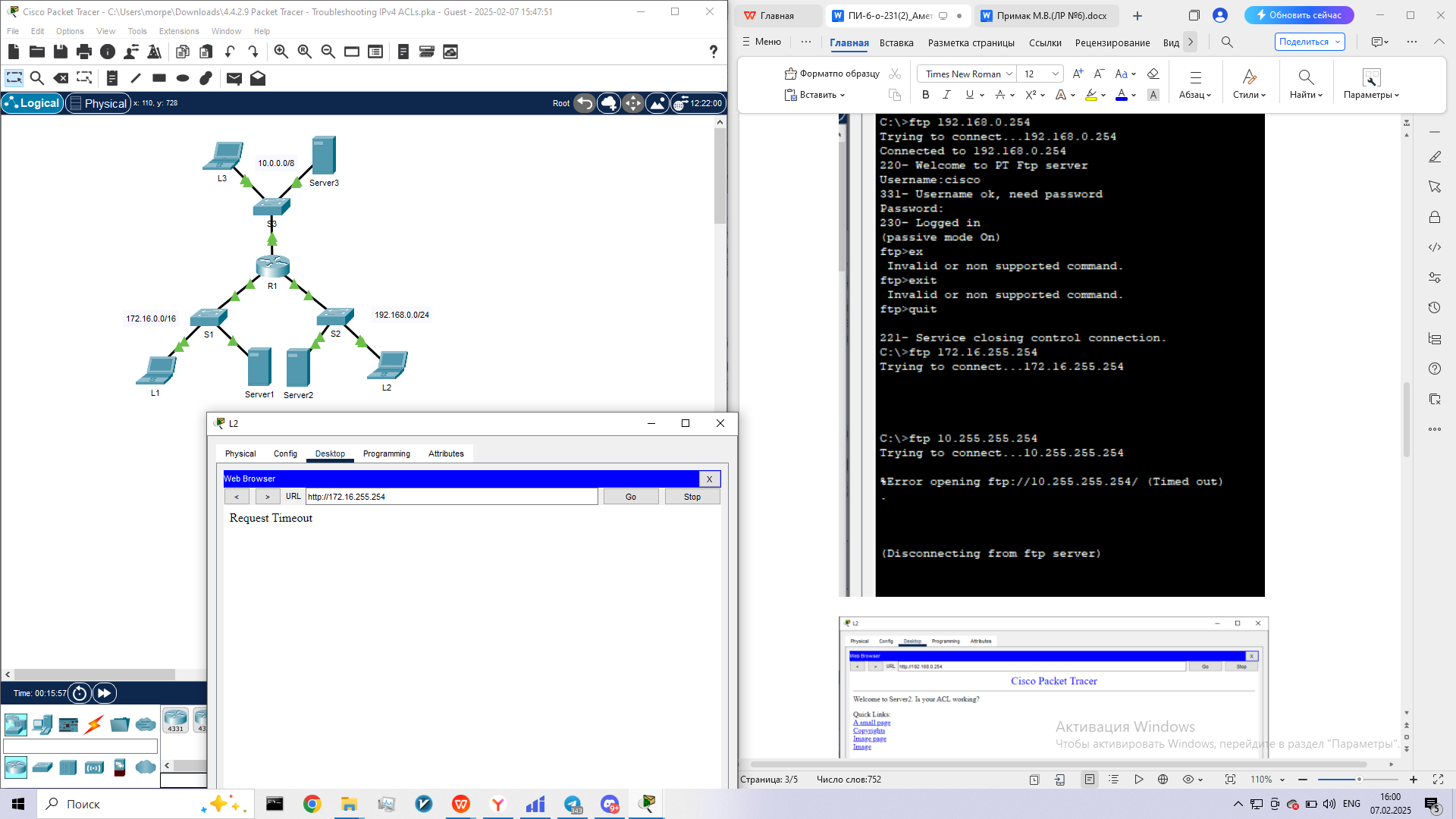
As you perform the following tasks, compare the results to what you would expect from the ACL.

1. Using **L2**, attempt to access FTP and HTTP services of **Server1**, **Server2**, and **Server3**.

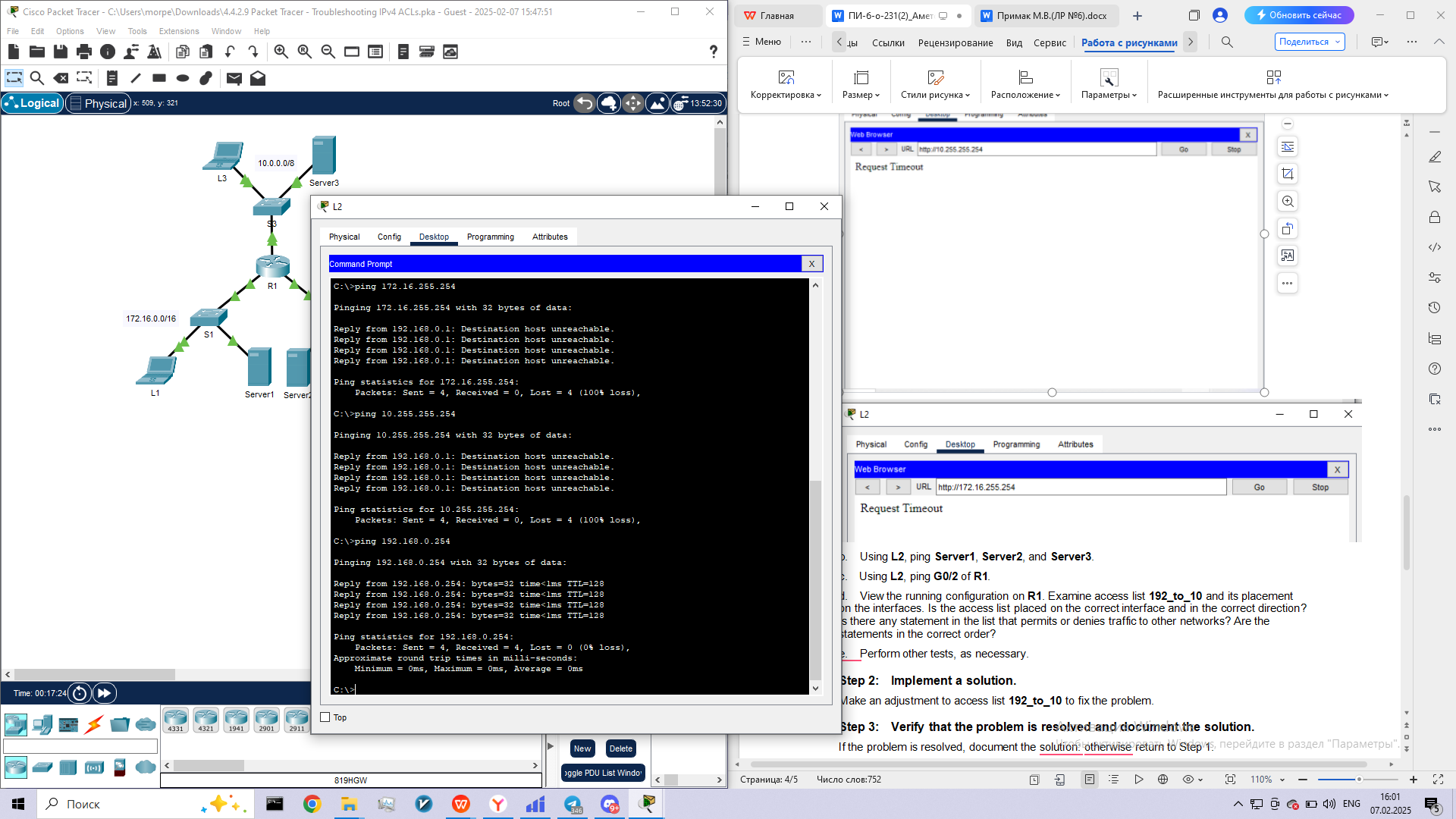




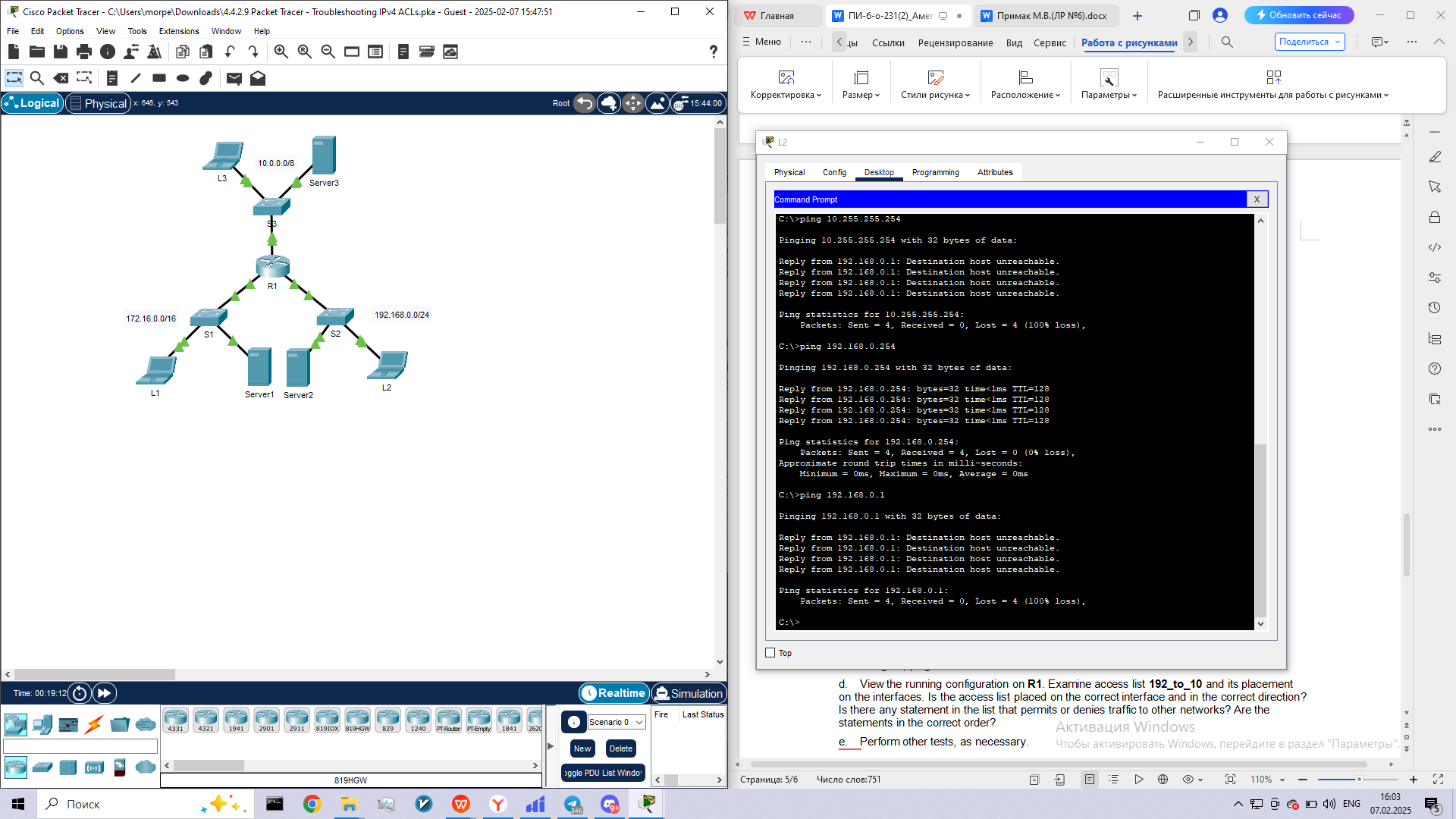




1. Using **L2**, ping **Server1**, **Server2**, and **Server3**.



1. Using **L2**, ping **G0/2** of **R1**.



1. View the running configuration on **R1**. Examine access list **192\_to\_10** and its placement on the interfaces. Is the access list placed on the correct interface and in the correct direction? Is there any statement in the list that permits or denies traffic to other networks? Are the statements in the correct order?

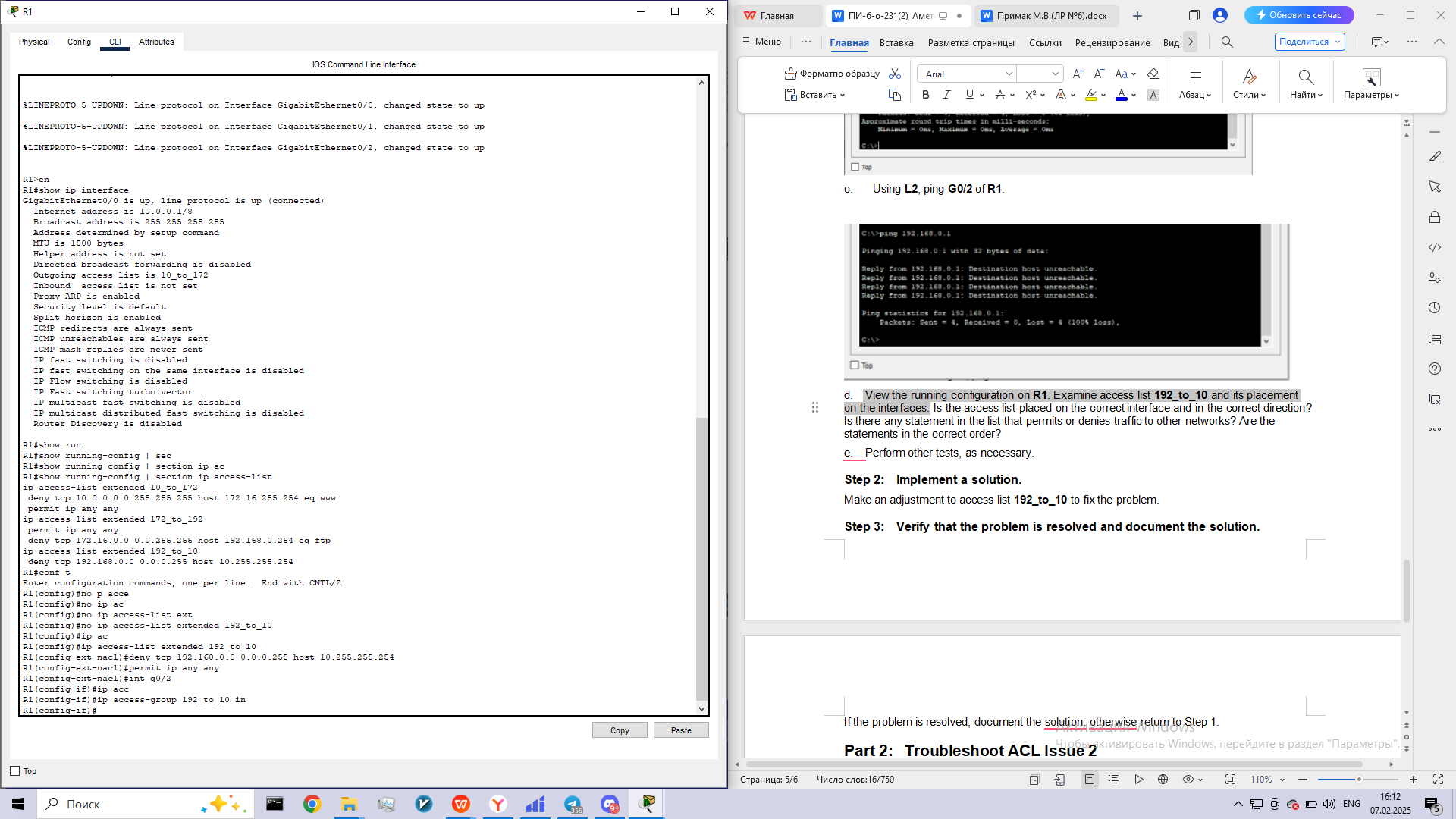
e.      Perform other tests, as necessary.

**Step 2:      Implement a solution.**

Make an adjustment to access list **192\_to\_10** to fix the problem.

**Step 3:      Verify that the problem is resolved and document the solution.**

If the problem is resolved, document the solution: otherwise return to Step 1.



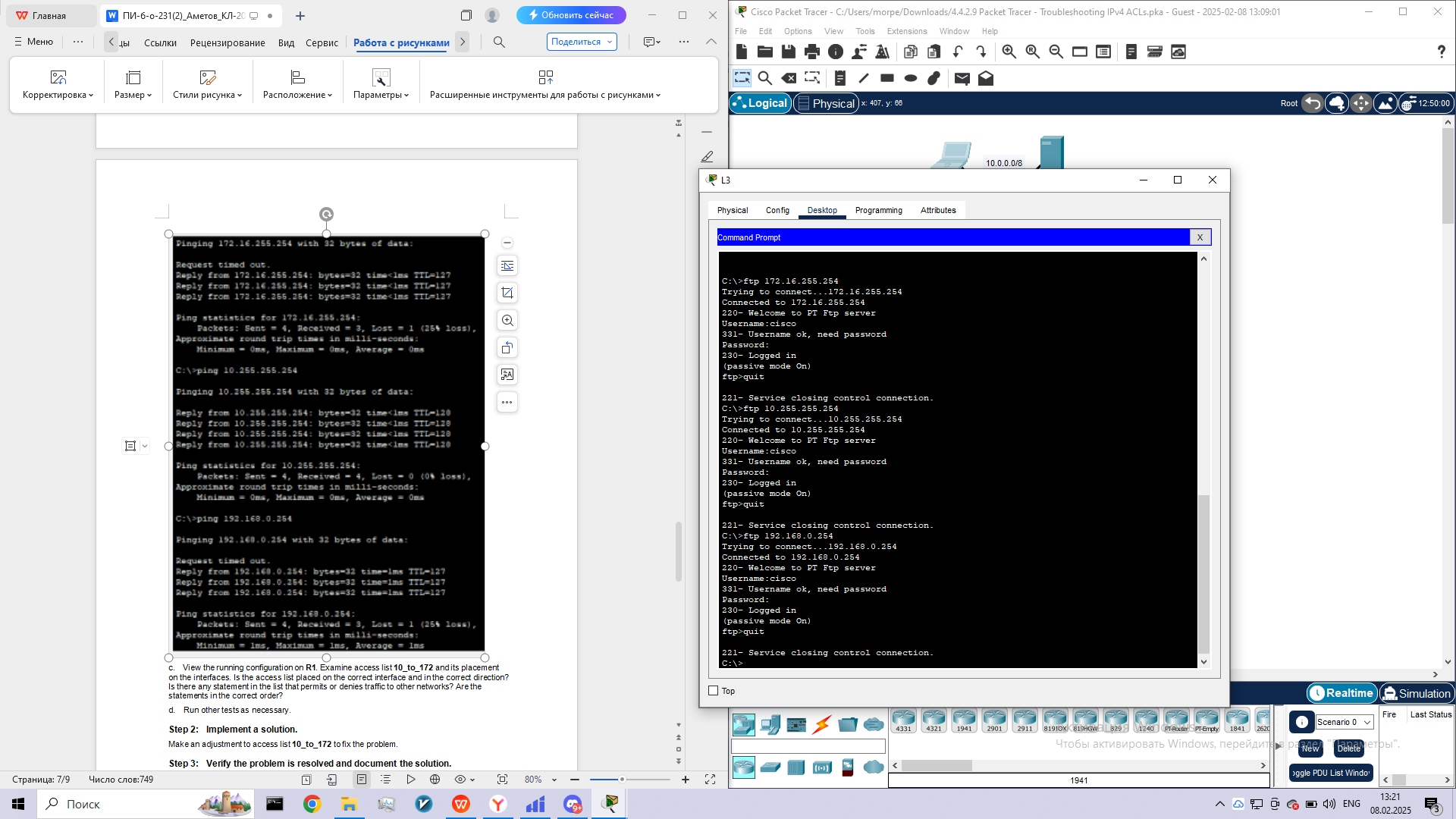
**Part 2:      Troubleshoot ACL Issue 2**

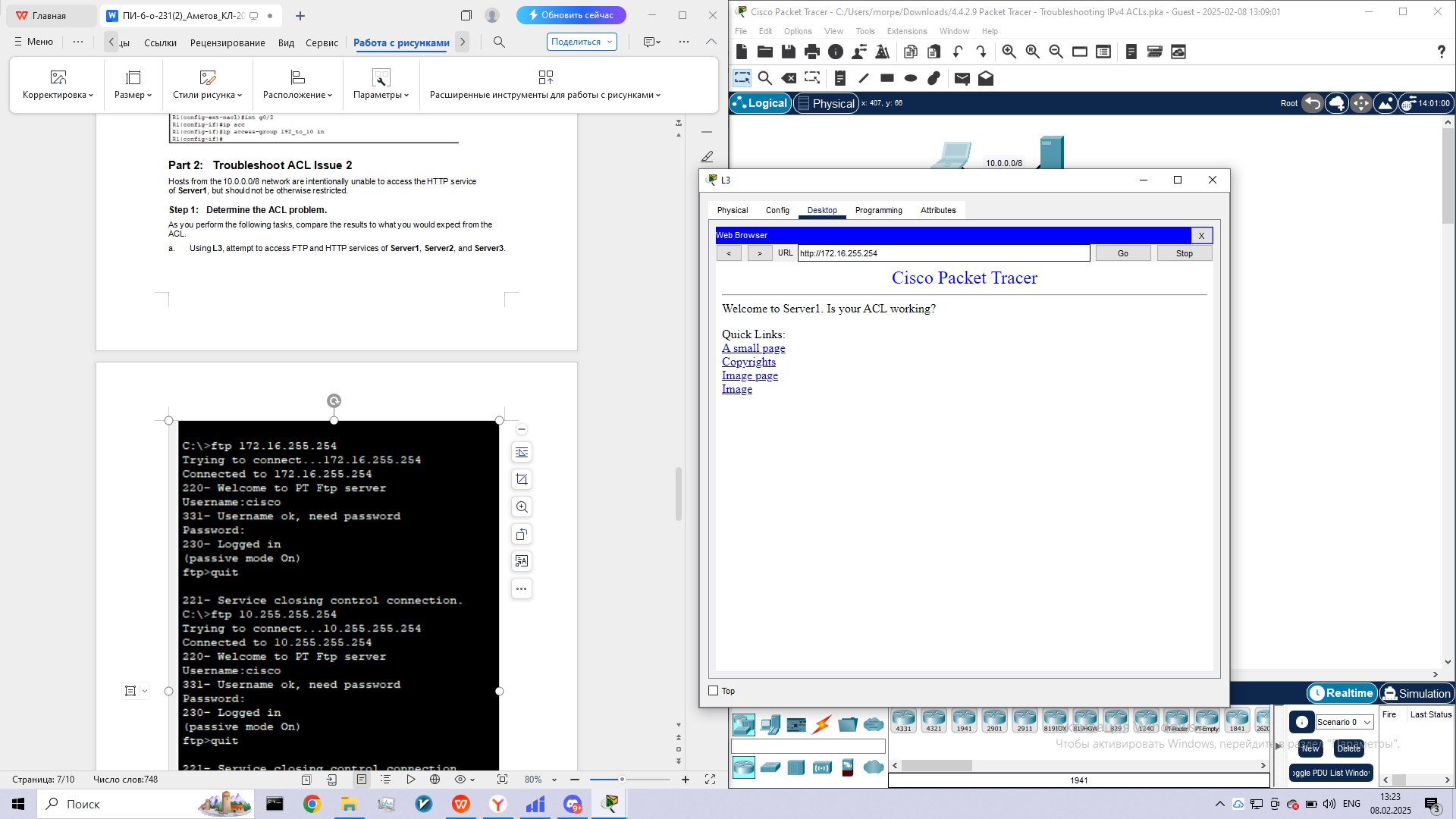
Hosts from the 10.0.0.0/8 network are intentionally unable to access the HTTP service of **Server1**, but should not be otherwise restricted.

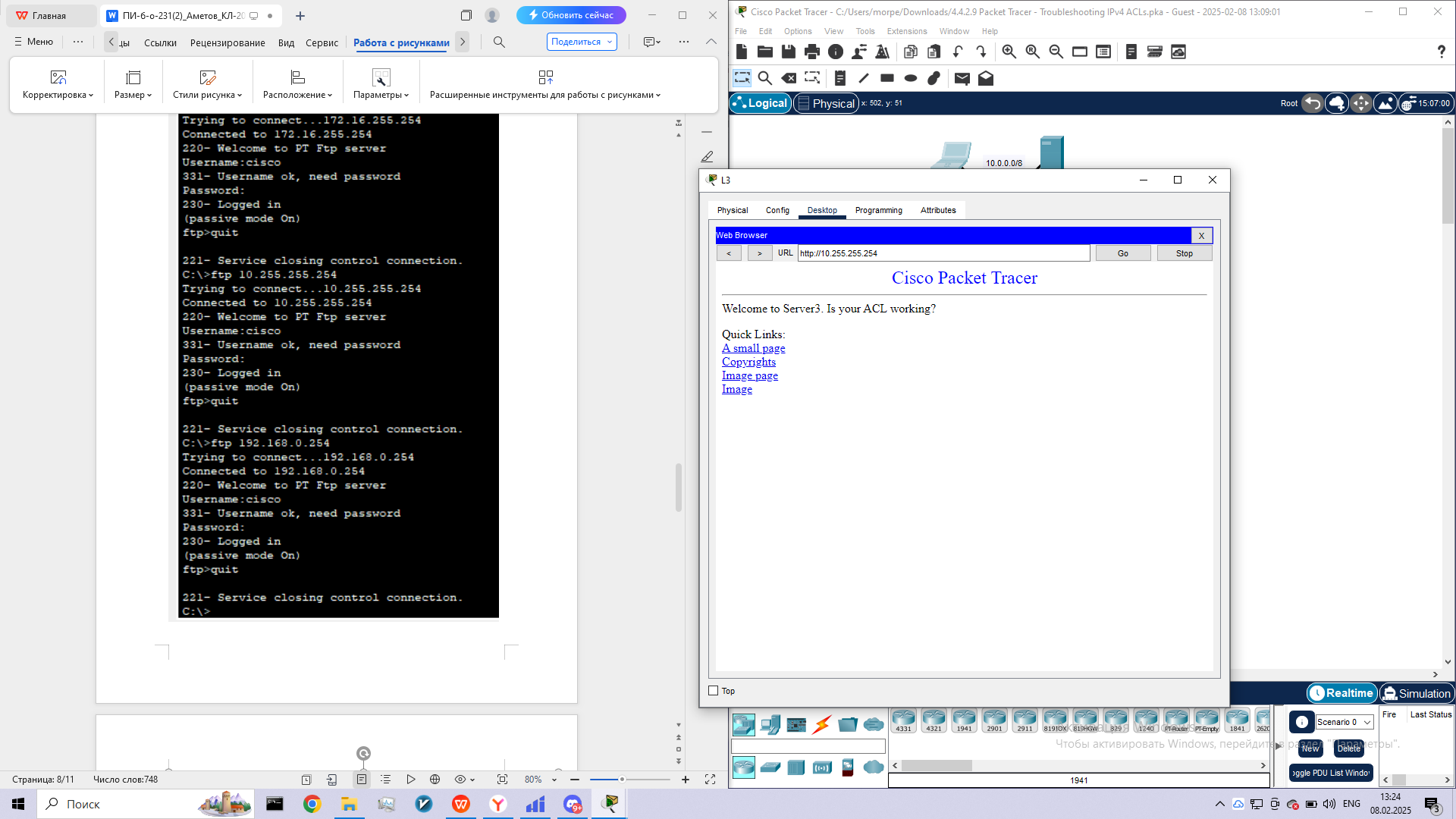
**Step 1:      Determine the ACL problem.**

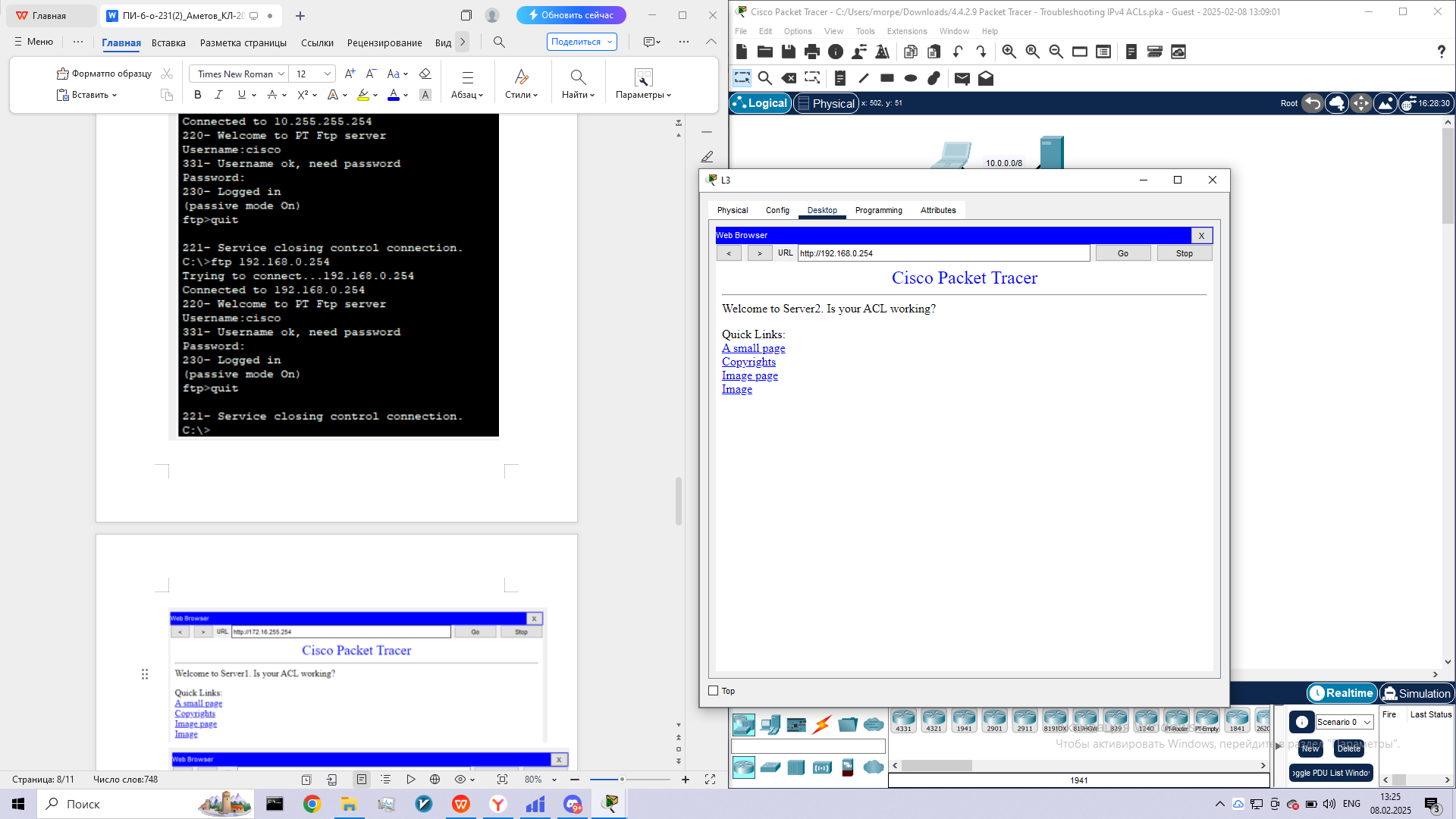
As you perform the following tasks, compare the results to what you would expect from the ACL.

1. Using **L3**, attempt to access FTP and HTTP services of **Server1**, **Server2**, and **Server3**.

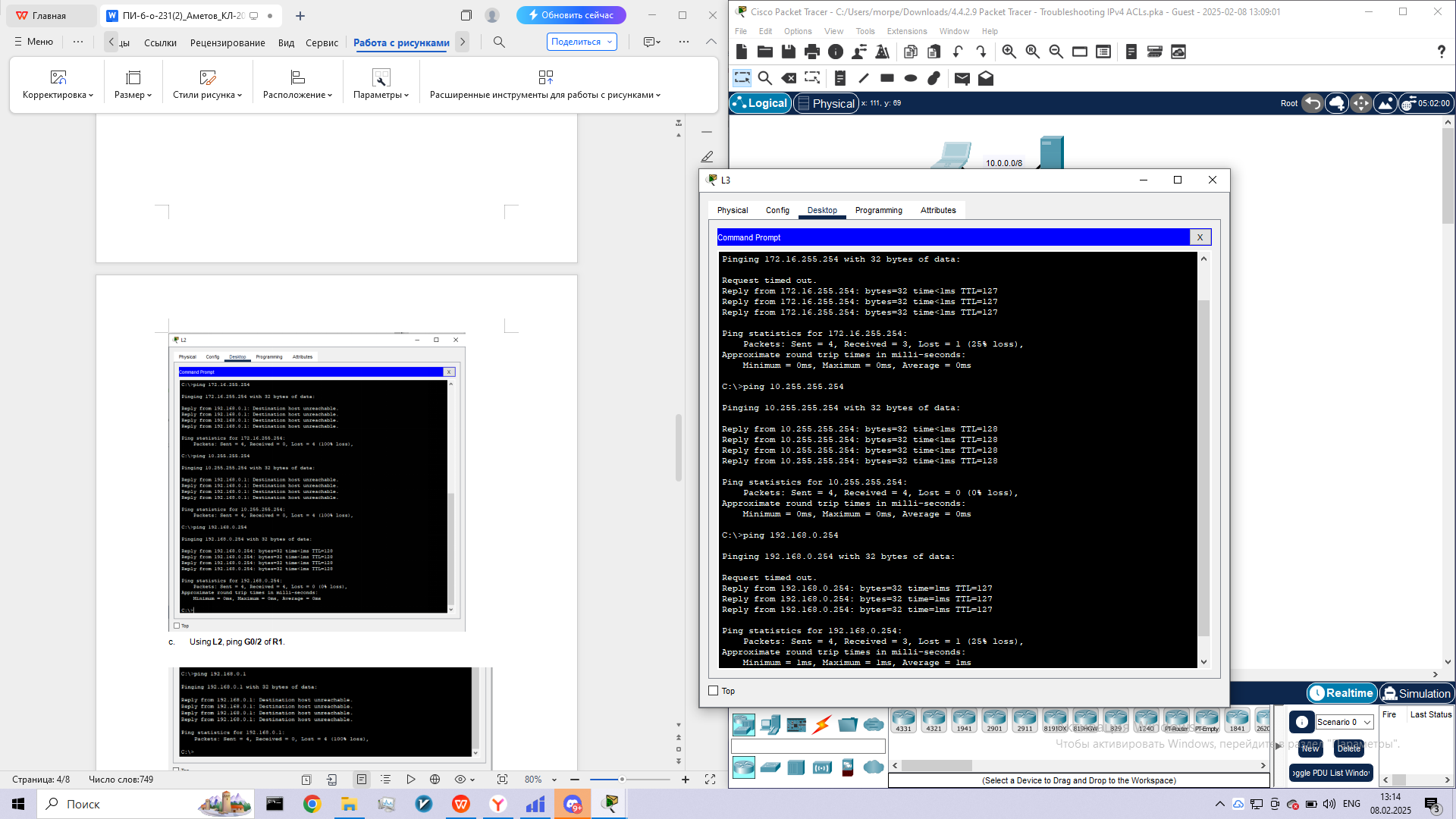




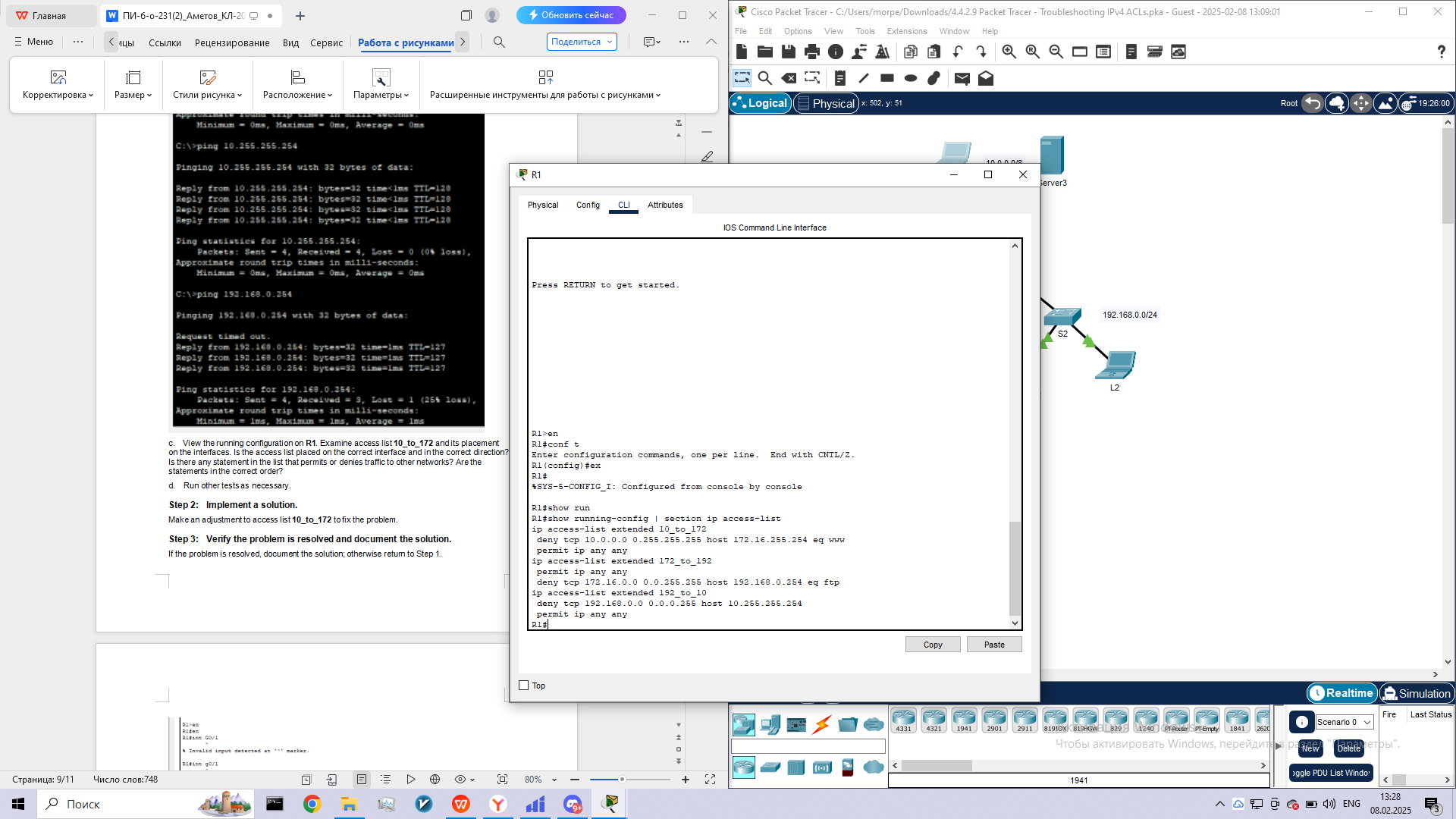




b.      Using **L3**, ping **Server1**, **Server2**, and **Server3**.



1. View the running configuration on **R1**. Examine access list **10\_to\_172** and its placement on the interfaces. Is the access list placed on the correct interface and in the correct direction? Is there any statement in the list that permits or denies traffic to other networks? Are the statements in the correct order?



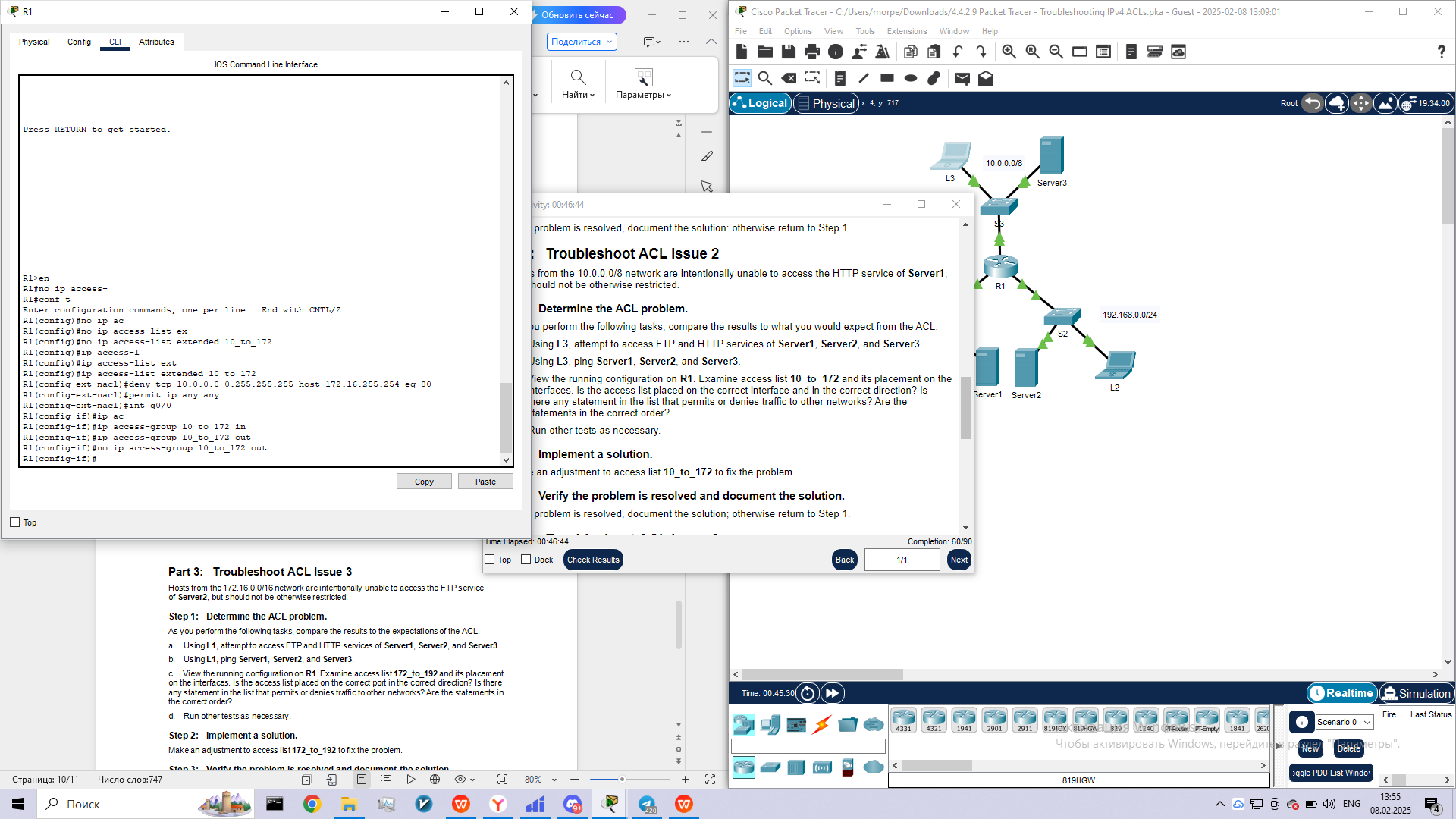
d.      Run other tests as necessary.

**Step 2:      Implement a solution.**

Make an adjustment to access list **10\_to\_172** to fix the problem.

**Step 3:      Verify the problem is resolved and document the solution.**

If the problem is resolved, document the solution; otherwise return to Step 1.



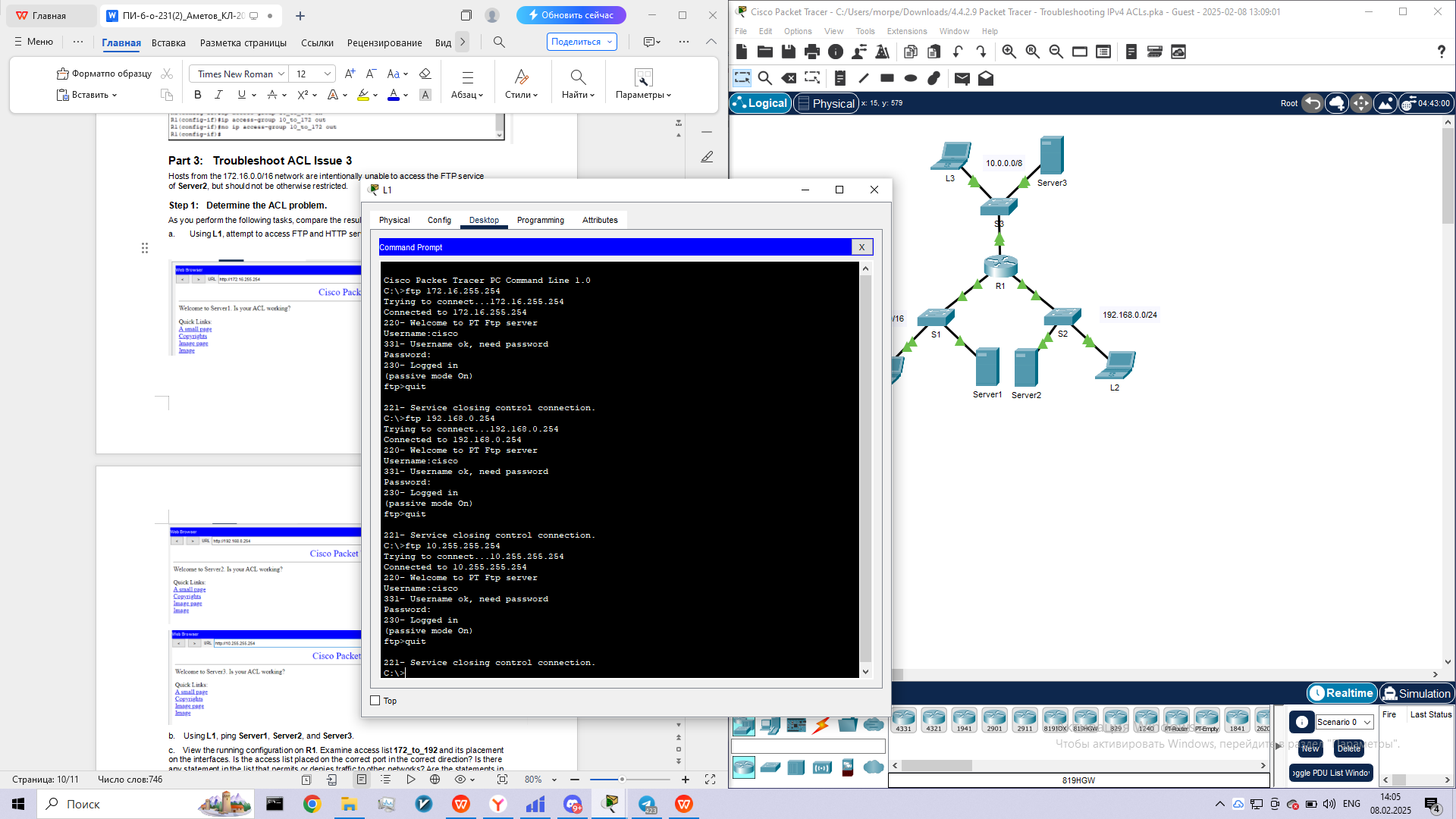
**Part 3:      Troubleshoot ACL Issue 3**

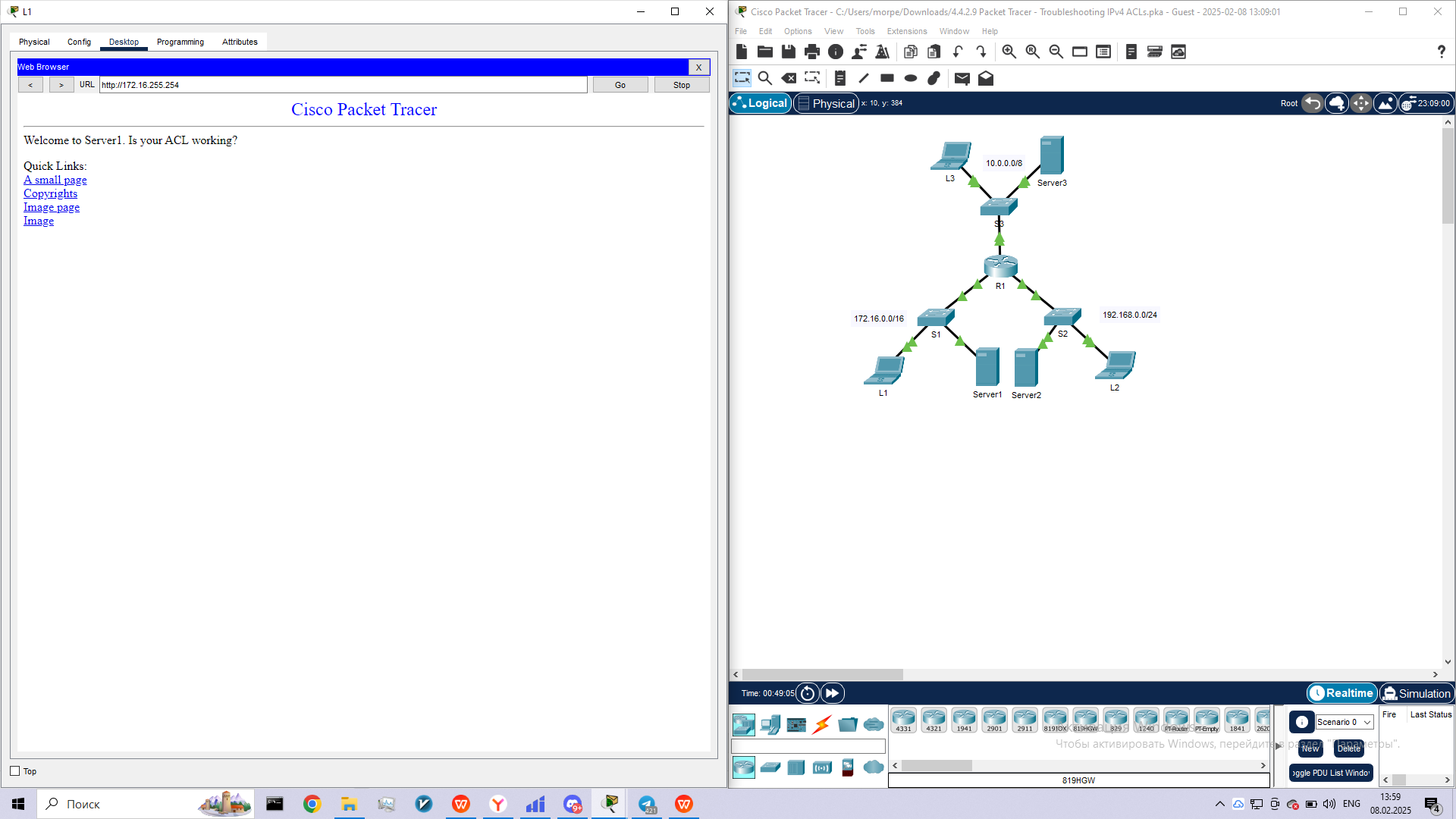
Hosts from the 172.16.0.0/16 network are intentionally unable to access the FTP service of **Server2**, but should not be otherwise restricted.

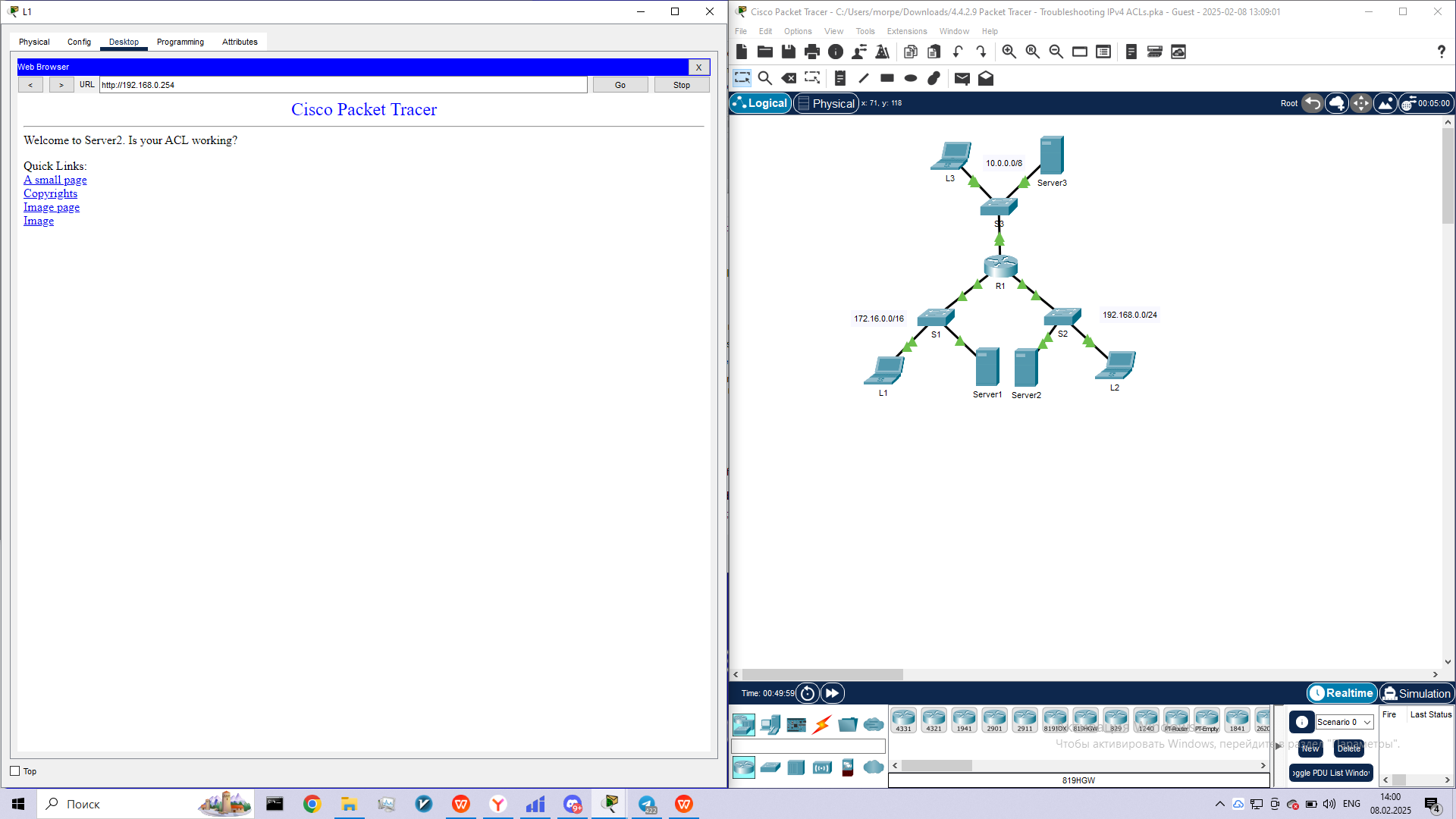
**Step 1:      Determine the ACL problem.**

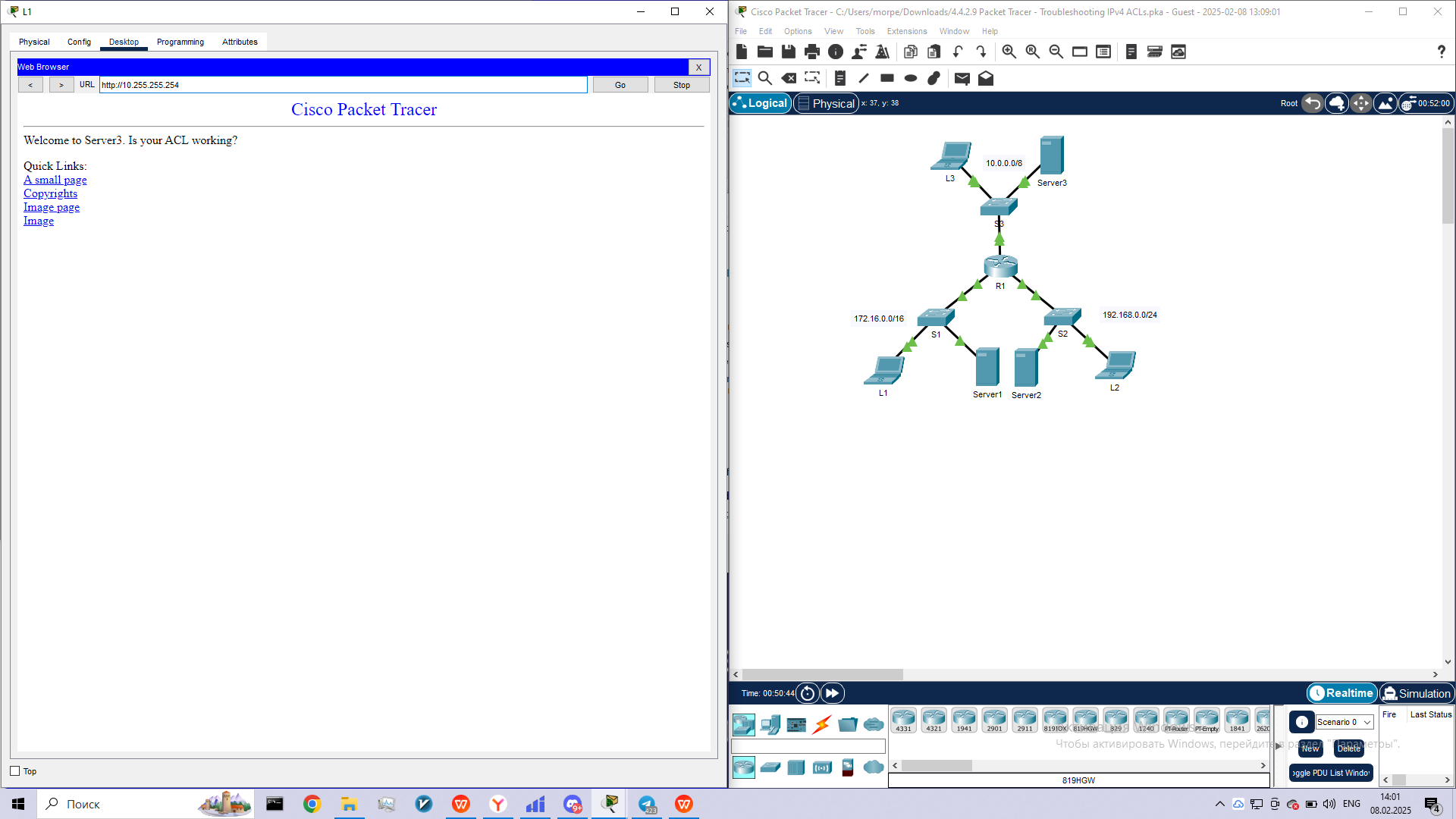
As you perform the following tasks, compare the results to the expectations of the ACL.

1. Using **L1**, attempt to access FTP and HTTP services of **Server1**, **Server2**, and **Server3**.

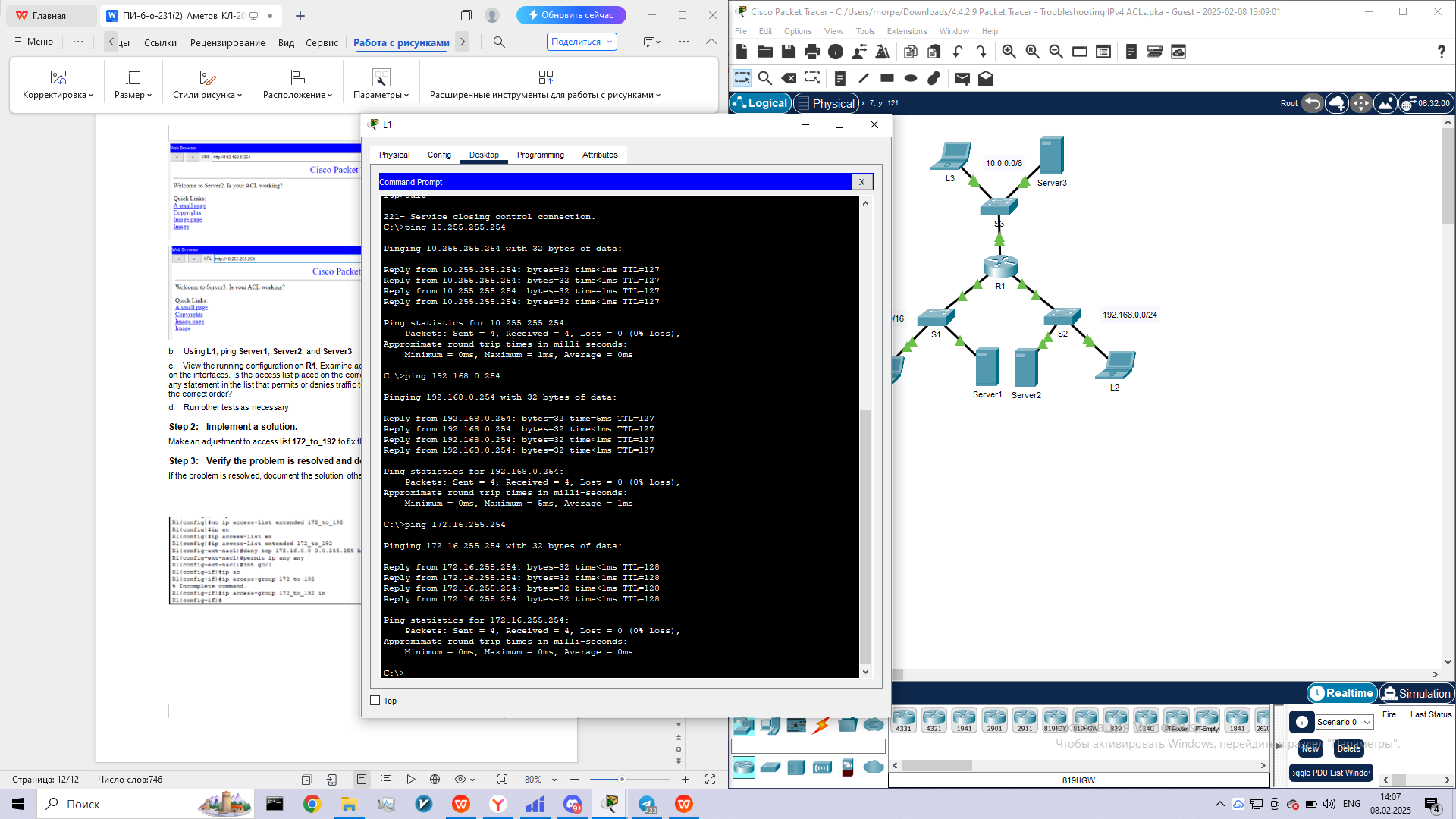




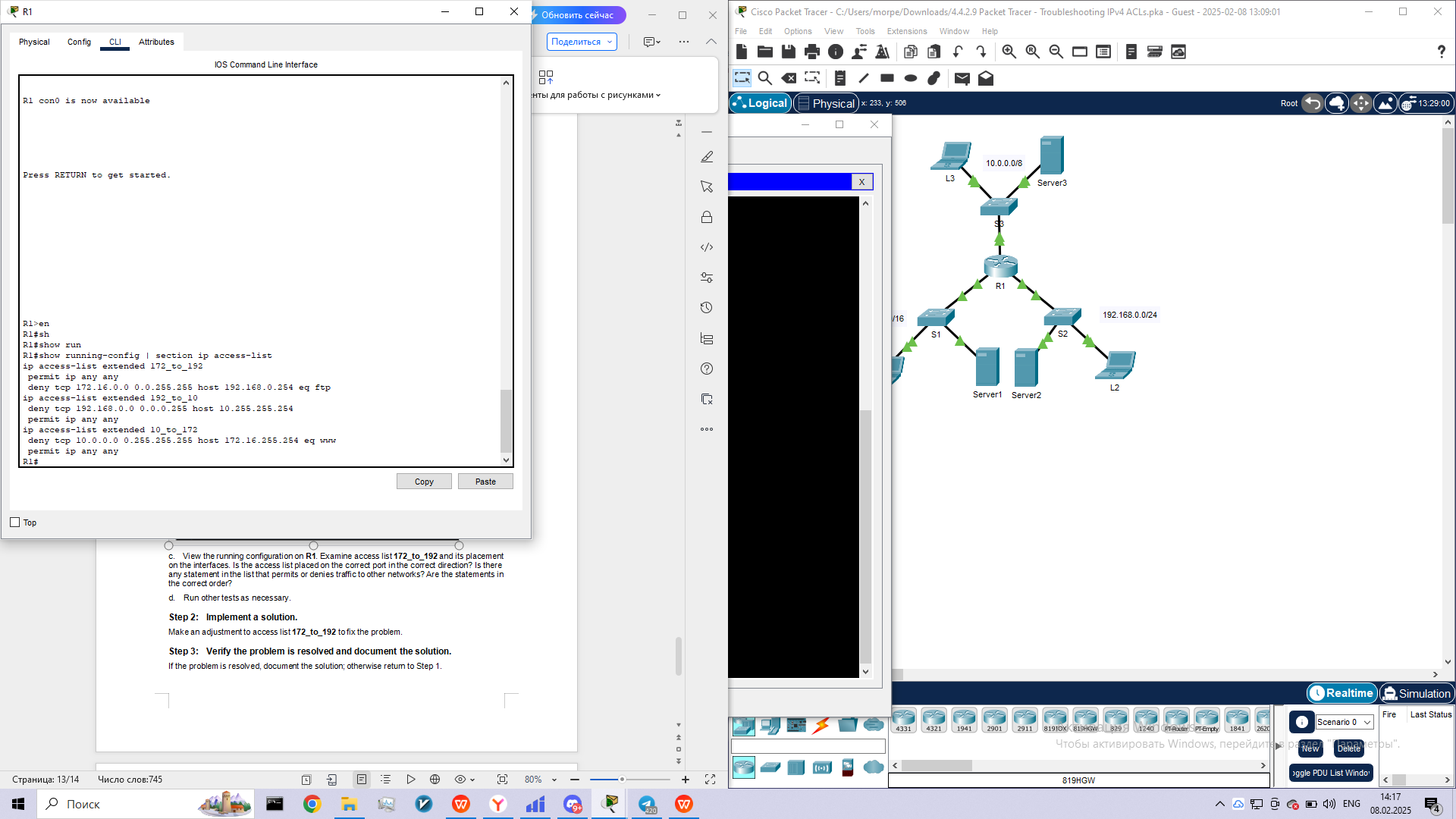




1. Using **L1**, ping **Server1**, **Server2**, and **Server3**.



1. View the running configuration on **R1**. Examine access list **172\_to\_192** and its placement on the interfaces. Is the access list placed on the correct port in the correct direction? Is there any statement in the list that permits or denies traffic to other networks? Are the statements in the correct order?



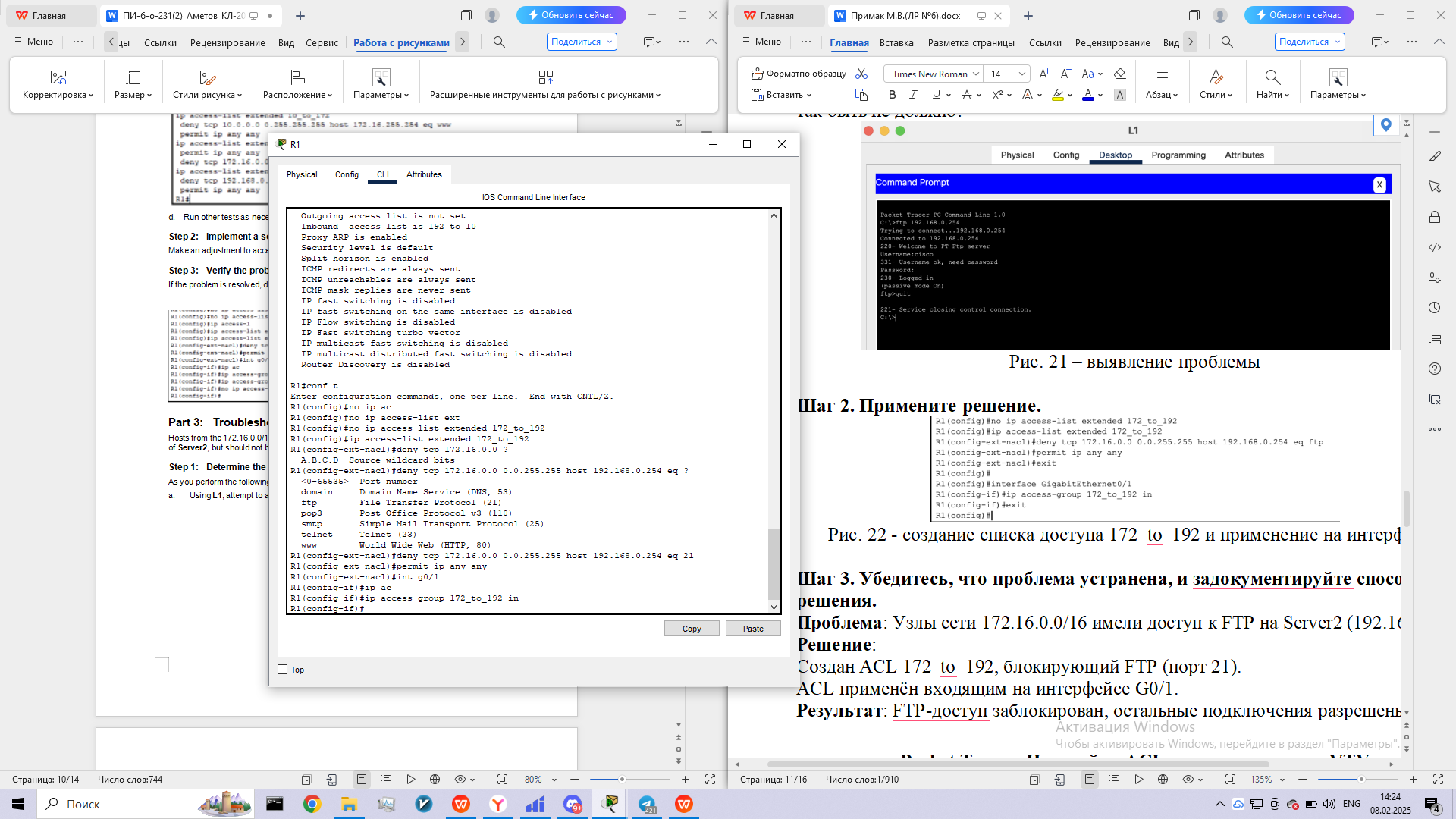
d.      Run other tests as necessary.

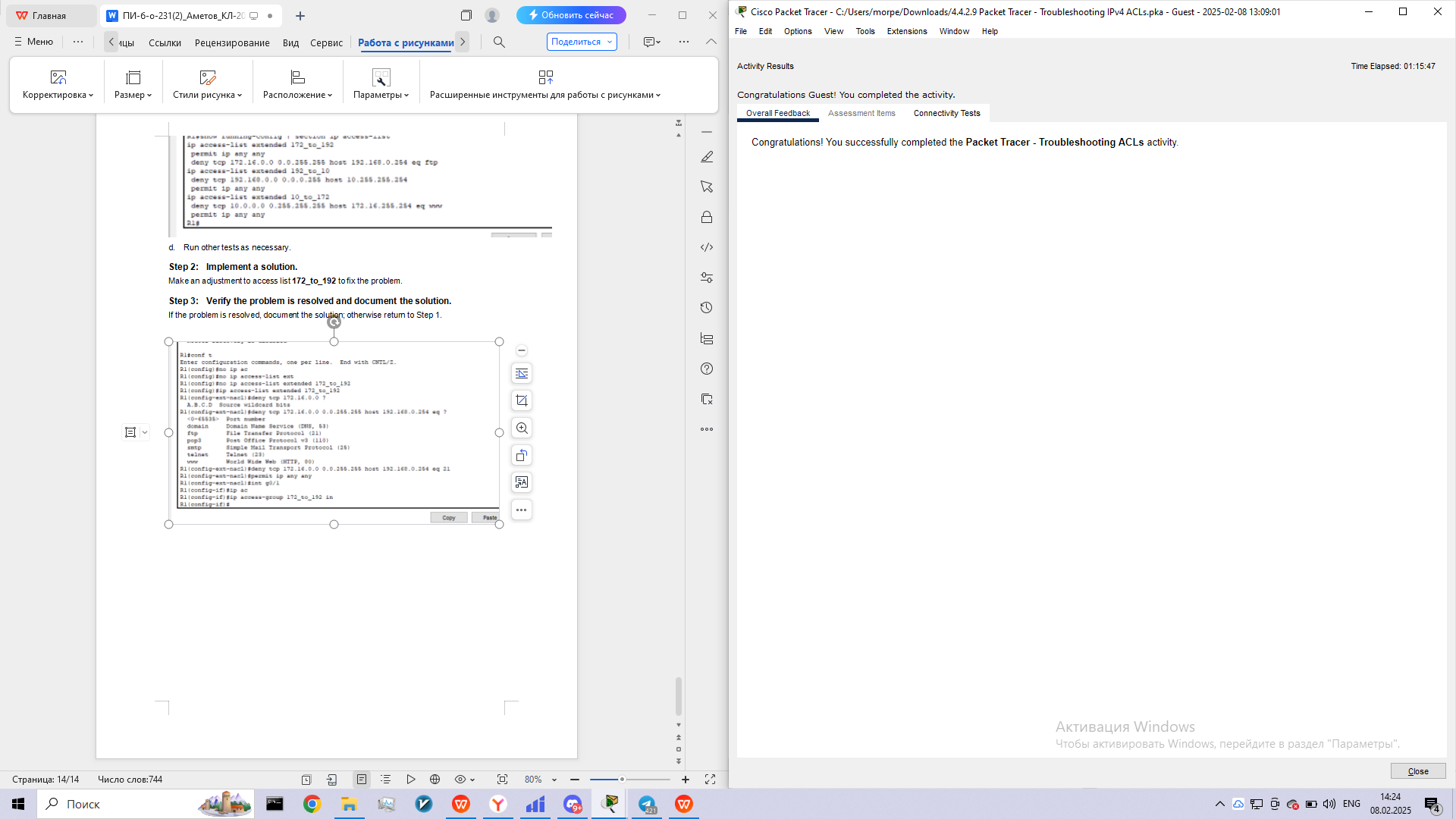
**Step 2:      Implement a solution.**

Make an adjustment to access list **172\_to\_192** to fix the problem.

**Step 3:      Verify the problem is resolved and document the solution.**

If the problem is resolved, document the solution; otherwise return to Step 1.





**Packet Tracer - Configuring an ACL on VTY Lines**

**Addressing Table**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **Default Gateway** |
| Router | F0/0 | 10.0.0.254 | 255.0.0.0 | N/A |
| PC | NIC | 10.0.0.1 | 255.0.0.0 | 10.0.0.254 |
| Laptop | NIC | 10.0.0.2 | 255.0.0.0 | 10.0.0.254 |

**Objectives**

**Part 1: Configure and Apply an ACL to VTY Lines**

**Part 2: Verify the ACL Implementation**

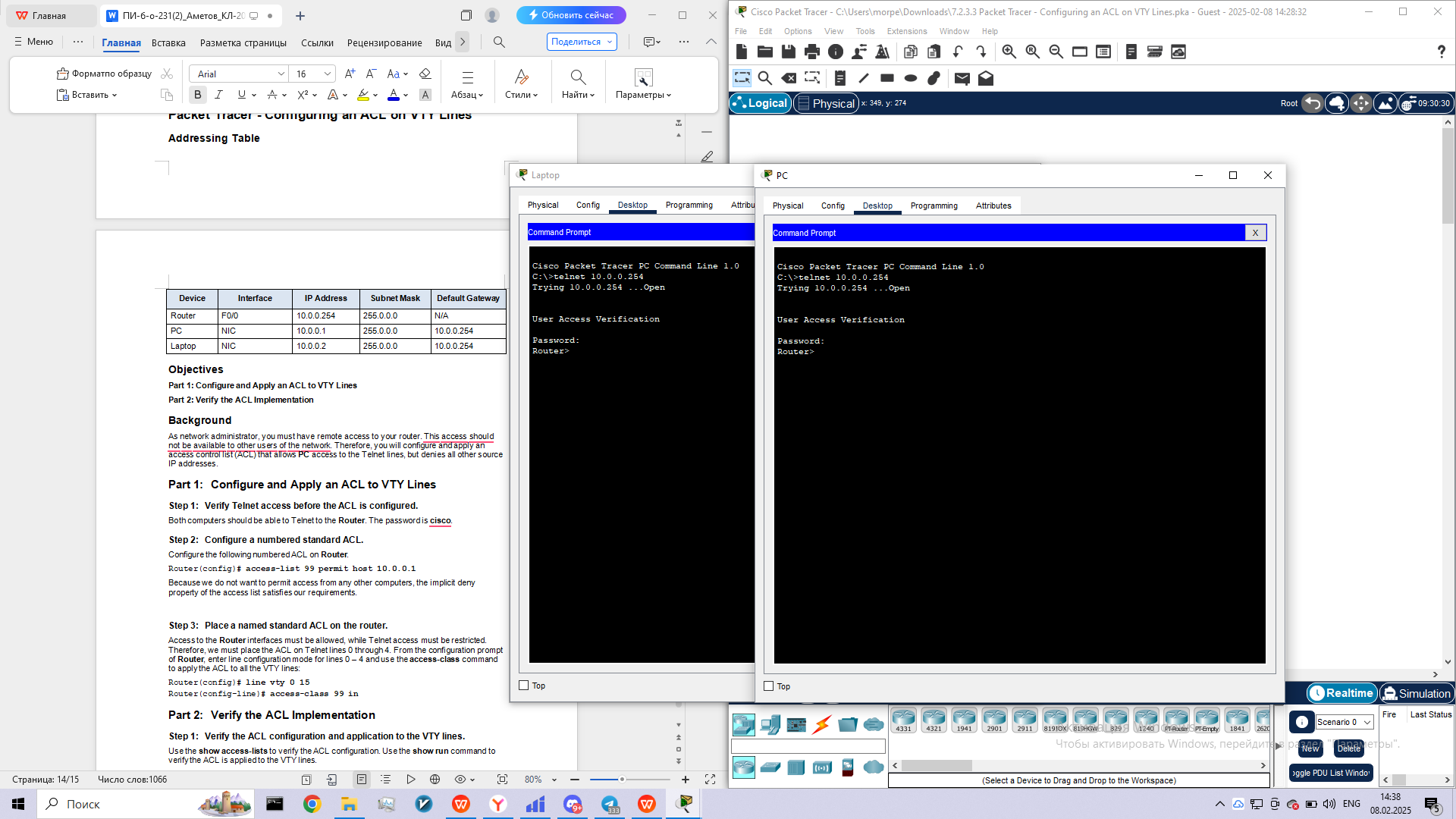
**Background**

As network administrator, you must have remote access to your router. This access should not be available to other users of the network. Therefore, you will configure and apply an access control list (ACL) that allows **PC**access to the Telnet lines, but denies all other source IP addresses.

**Part 1:     Configure and Apply an ACL to VTY Lines**

**Step 1:     Verify Telnet access before the ACL is configured.**

Both computers should be able to Telnet to the **Router**. The password is **cisco**.



**Step 2:     Configure a numbered standard ACL.**

Configure the following numbered ACL on **Router**.

Router(config)# **access-list 99 permit host 10.0.0.1**

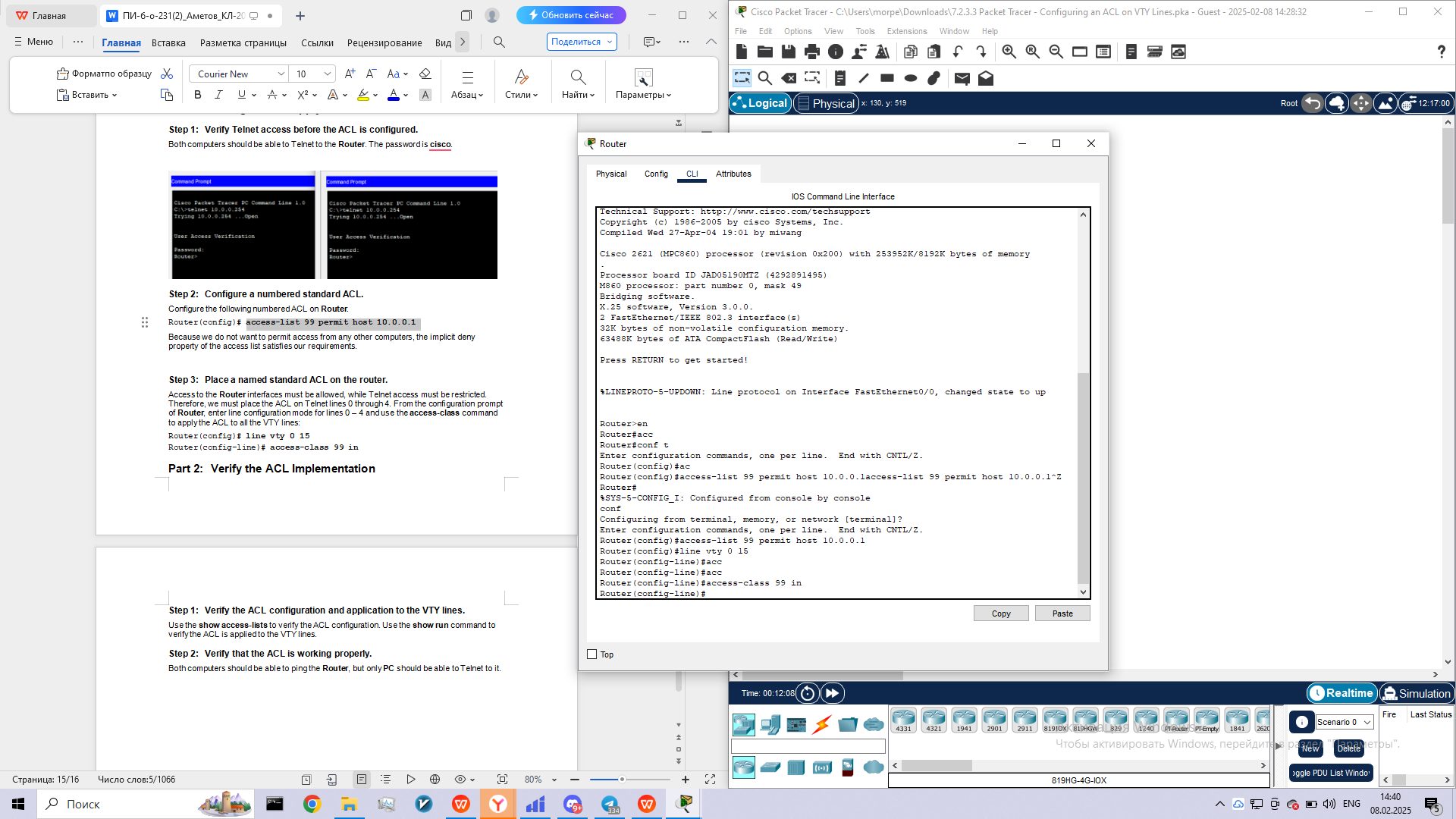
Because we do not want to permit access from any other computers, the implicit deny property of the access list satisfies our requirements.

**Step 3:     Place a named standard ACL on the router.**

Access to the **Router** interfaces must be allowed, while Telnet access must be restricted. Therefore, we must place the ACL on Telnet lines 0 through 4. From the configuration prompt of **Router**, enter line configuration mode for lines 0 – 4 and use the **access-class**command to apply the ACL to all the VTY lines:

Router(config)# **line vty 0 15**

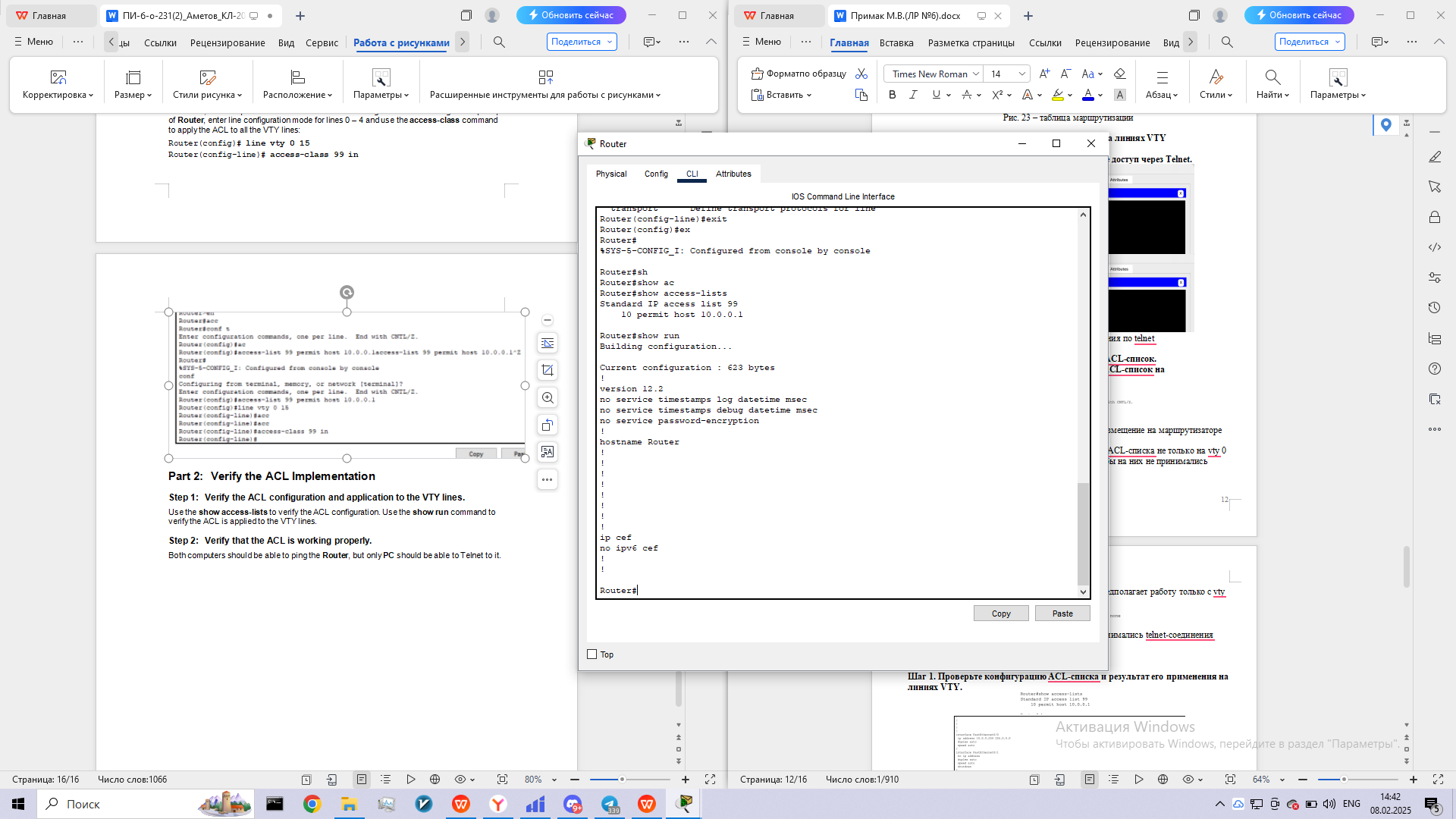
Router(config-line)# **access-class 99 in**



**Part 2:     Verify the ACL Implementation**

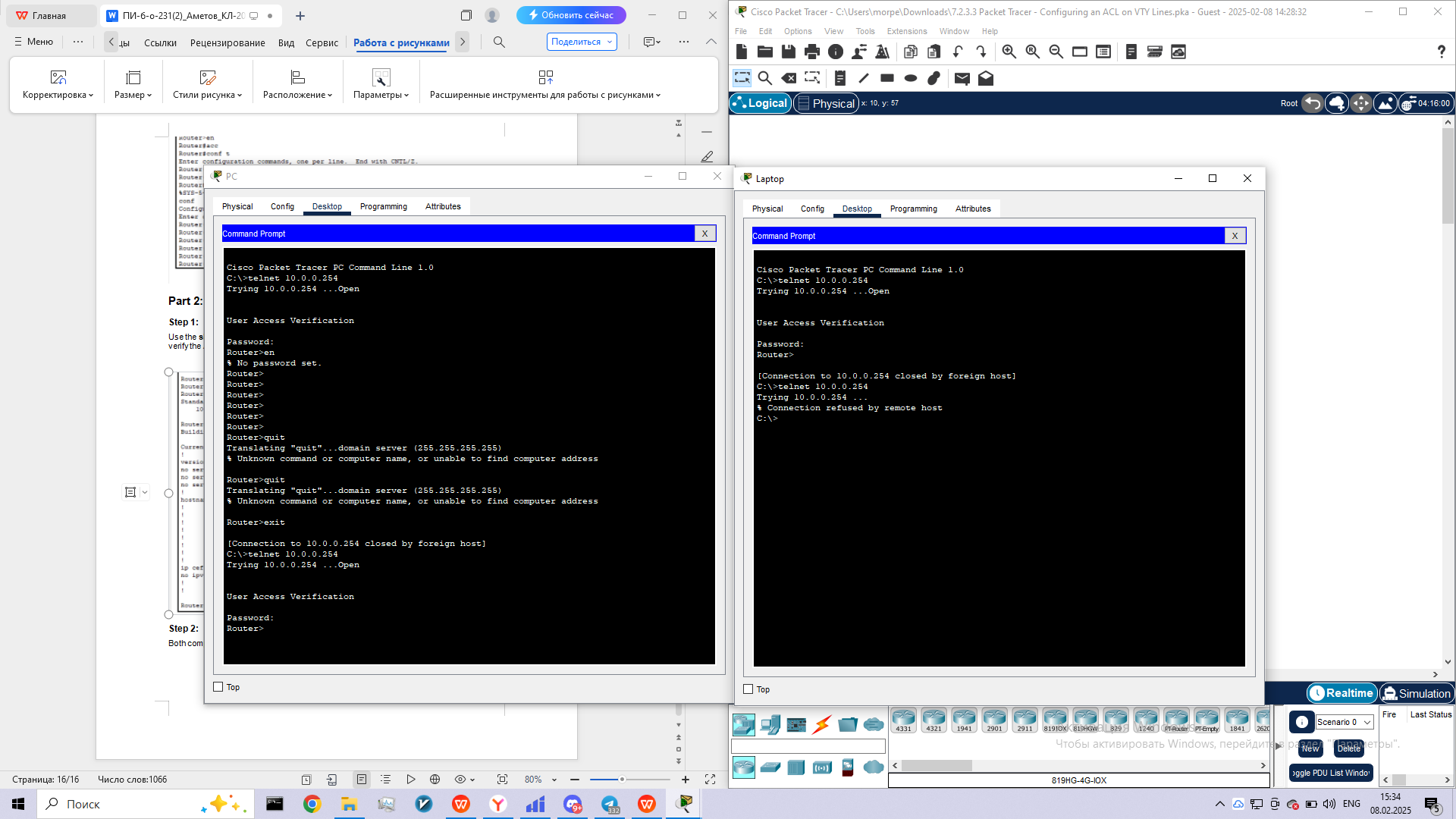
**Step 1:     Verify the ACL configuration and application to the VTY lines.**

Use the **show access-lists**to verify the ACL configuration. Use the **show run** command to verify the ACL is applied to the VTY lines.



**Step 2:     Verify that the ACL is working properly.**

Both computers should be able to ping the **Router**, but only **PC** should be able to Telnet to it.



**Packet Tracer - Configuring IPv6 ACLs**

**Addressing Table**

|  |  |  |  |
| --- | --- | --- | --- |
| **Device** | **Interface** | **IPv6 Address/Prefix** | **Default Gateway** |
| Server3 | NIC | 2001:DB8:1:30::30/64 | FE80::30 |

**Objectives**

**Part 1: Configure, Apply, and Verify an IPv6 ACL**

**Part 2: Configure, Apply, and Verify a Second IPv6 ACL**

**Part 1:     Configure, Apply, and Verify an IPv6 ACL**

Logs indicate that a computer on the 2001:DB8:1:11::0/64 network is repeatedly refreshing their web page causing a Denial-of-Service (DoS) attack against **Server3**. Until the client can be identified and cleaned, you must block HTTP and HTTPS access to that network with an access list.

**Step 1:     Configure an ACL that will block HTTP and HTTPS access.**

Configure an ACL named **BLOCK\_HTTP** on **R1** with the following statements.

a.     Block HTTP and HTTPS traffic from reaching **Server3**.

R1(config)# **deny tcp any host 2001:DB8:1:30::30 eq www**

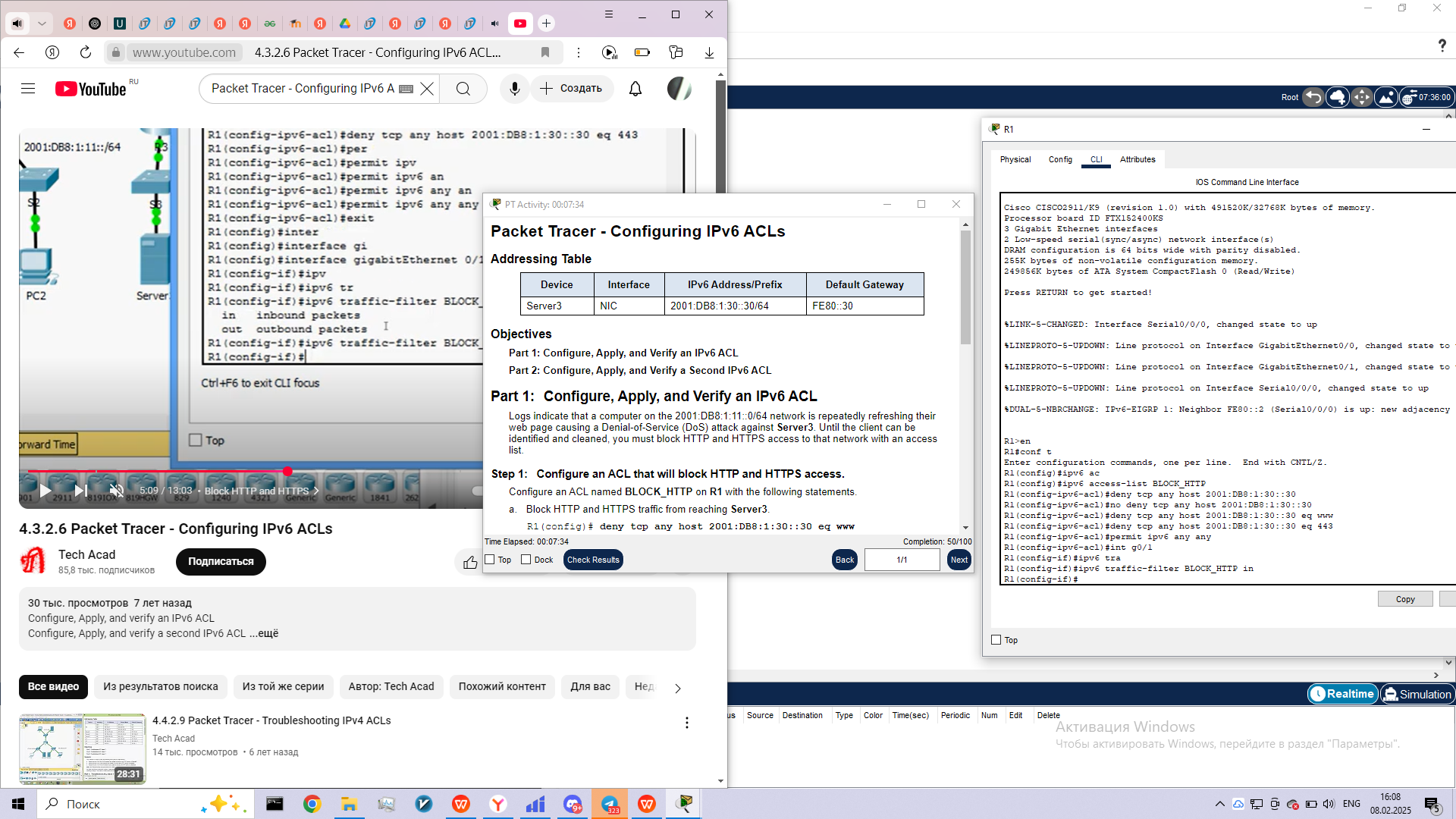
R1(config)# **deny tcp any host 2001:DB8:1:30::30 eq 443**

b.    Allow all other IPv6 traffic to pass.

**Step 2:     Apply the ACL to the correct interface.**

Apply the ACL on the interface closest the source of the traffic to be blocked.

R1(config-if)# **ipv6 traffic-filter BLOCK\_HTTP in**



**Step 3:     Verify the ACL implementation.**

Verify the ACL is operating as intended by conducting the following tests:

·         Open the **web browser** of **PC1** to http:// 2001:DB8:1:30::30 or https://2001:DB8:1:30::30. The website should appear.

·         Open the **web browser** of **PC2** to http:// 2001:DB8:1:30::30 or https://2001:DB8:1:30::30. The website should be blocked

·         Ping from **PC2** to 2001:DB8:1:30::30. The ping should be successful.

**Part 2:     Configure, Apply, and Verify a Second IPv6 ACL**

The logs now indicate that your server is receiving pings from many different IPv6 addresses in a Distributed Denial of Service (DDoS) attack. You must filter ICMP ping requests to your server.

**Step 1:     Create an access list to block ICMP.**

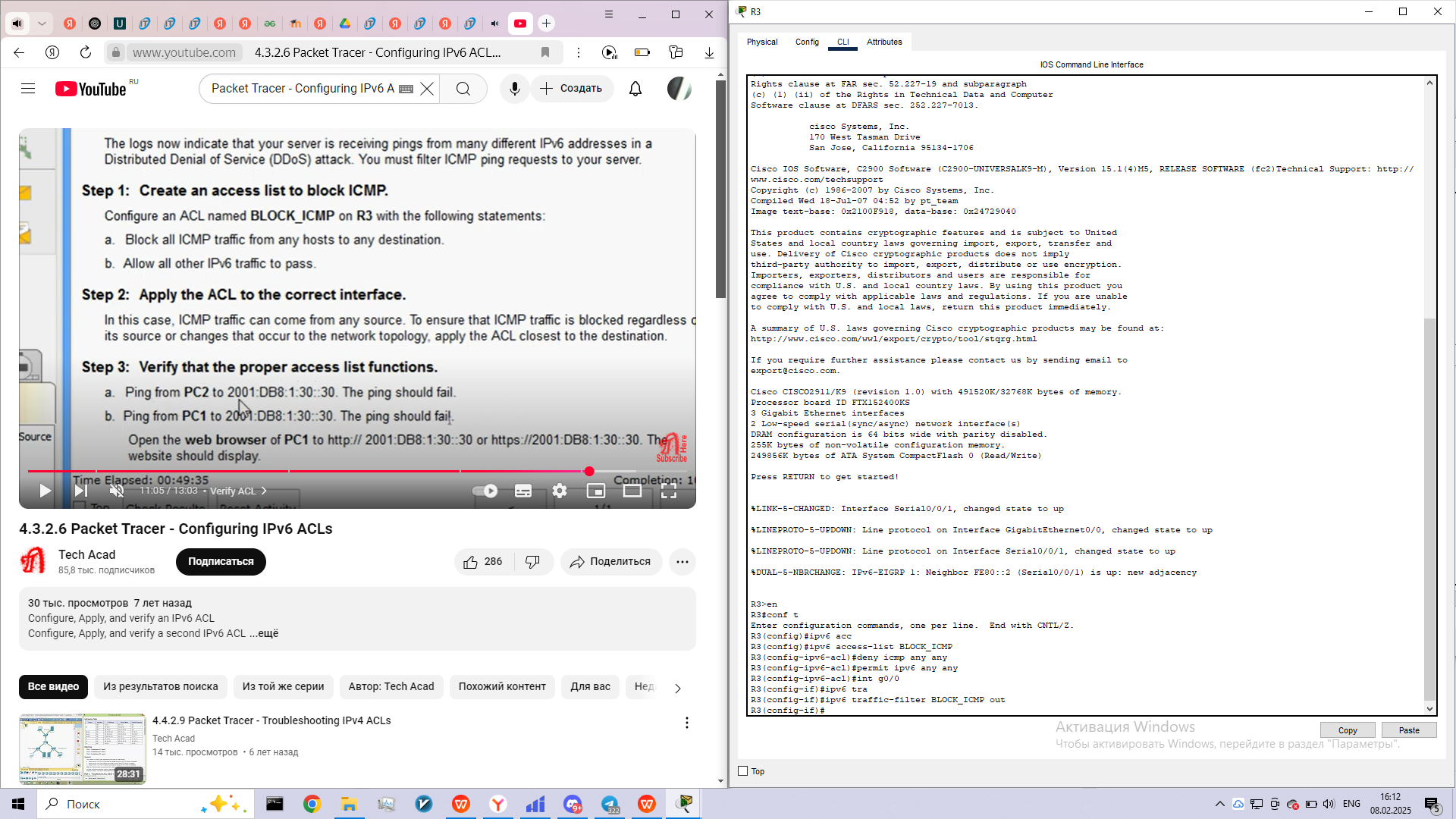
Configure an ACL named **BLOCK\_ICMP**on **R3**with the following statements:

a.     Block all ICMP traffic from any hosts to any destination.

b.    Allow all other IPv6 traffic to pass.

**Step 2:     Apply the ACL to the correct interface.**

In this case, ICMP traffic can come from any source. To ensure that ICMP traffic is blocked regardless of its source or changes that occur to the network topology, apply the ACL closest to the destination.



**Step 3:     Verify that the proper access list functions.**

a.     Ping from **PC2** to 2001:DB8:1:30::30. The ping should fail.

b.    Ping from **PC1** to 2001:DB8:1:30::30. The ping should fail.

Open the **web browser** of **PC1** to http:// 2001:DB8:1:30::30 or https://2001:DB8:1:30::30. The website should display.