FACULTY OF ELECTRONICS

COMPUTER ENGINEERING AND TELECOMMUNICATIONS DEPARTMENT

LABORATORY WORK #6

Internet and NAT Address Translation

Student: Mark Mikula

Teacher: Artūras Medeišis

Vilnius, 2025

Contents

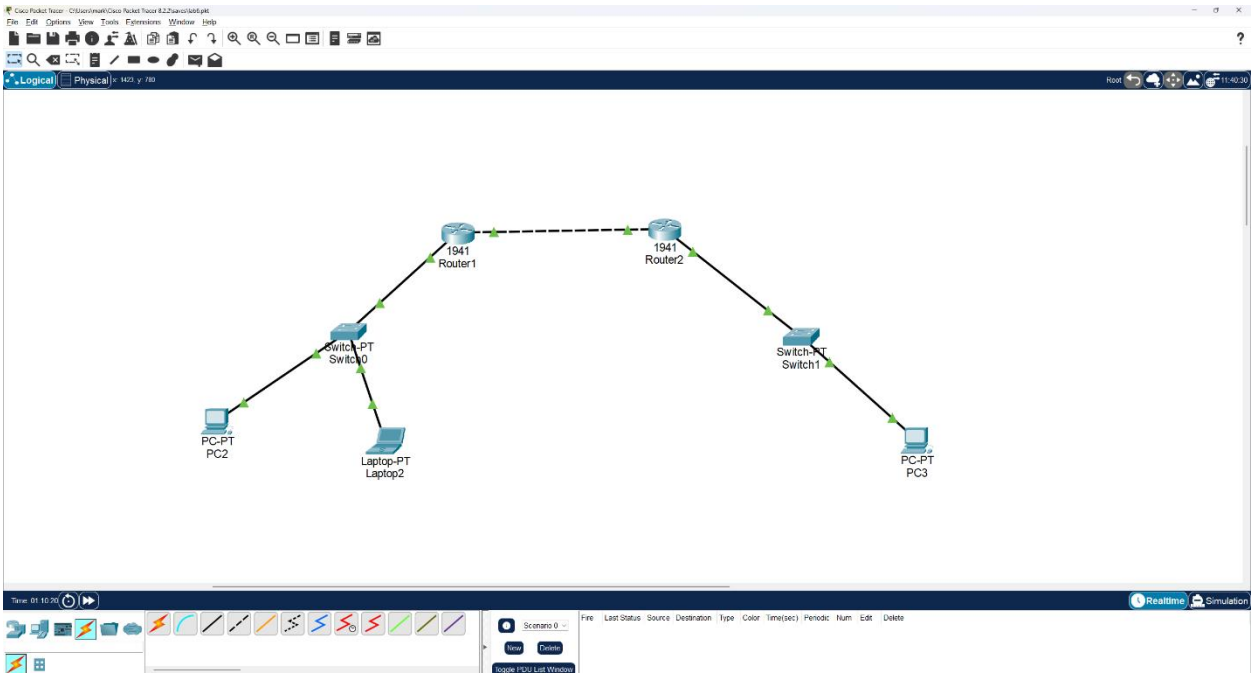
Objective

The primary objective of this lab work was to model the connection of two LANs over a public Internet network

This involved understanding the difference between private and public IP addresses and investigating the conversion of private-public IP addresses through the Network Address Translation (NAT) mechanism.

Topology Overview

The scenario featured two LANs linked over a public Internet network



The connection diagram (Figure 1) involved two Cisco 1941 routers and two switches. The routers were connected directly to each other using a crossover cable, modelling the

public Internet link. Each router was connected to a switch, which in turn connected to end devices (lab computers like PC1, Laptop on one side and PC2 on the other)

The LANs used IP addresses from reserved private IP address ranges

One LAN was configured with the network 172.16.1.0/24, and the other with 10.1.1.0/24. The interconnection between the two networks was realized through the public Internet, which was modelled by having the two gateway routers use public IP addresses on their externally facing ports. Specifically, the external interface of R1 (Gi0/0) was assigned 8.8.8.11/8, and the external interface of R2 (Gi0/0) was assigned 8.8.8.22/8. R1's internal interface (Gi0/1) used 172.16.1.1/24, serving the 172.16.1.0/24 network, and R2's internal interface (Gi0/1) used 10.1.1.1/24, serving the 10.1.1.0/24 network. DHCP pools were configured on each router to service their respective LAN subnets

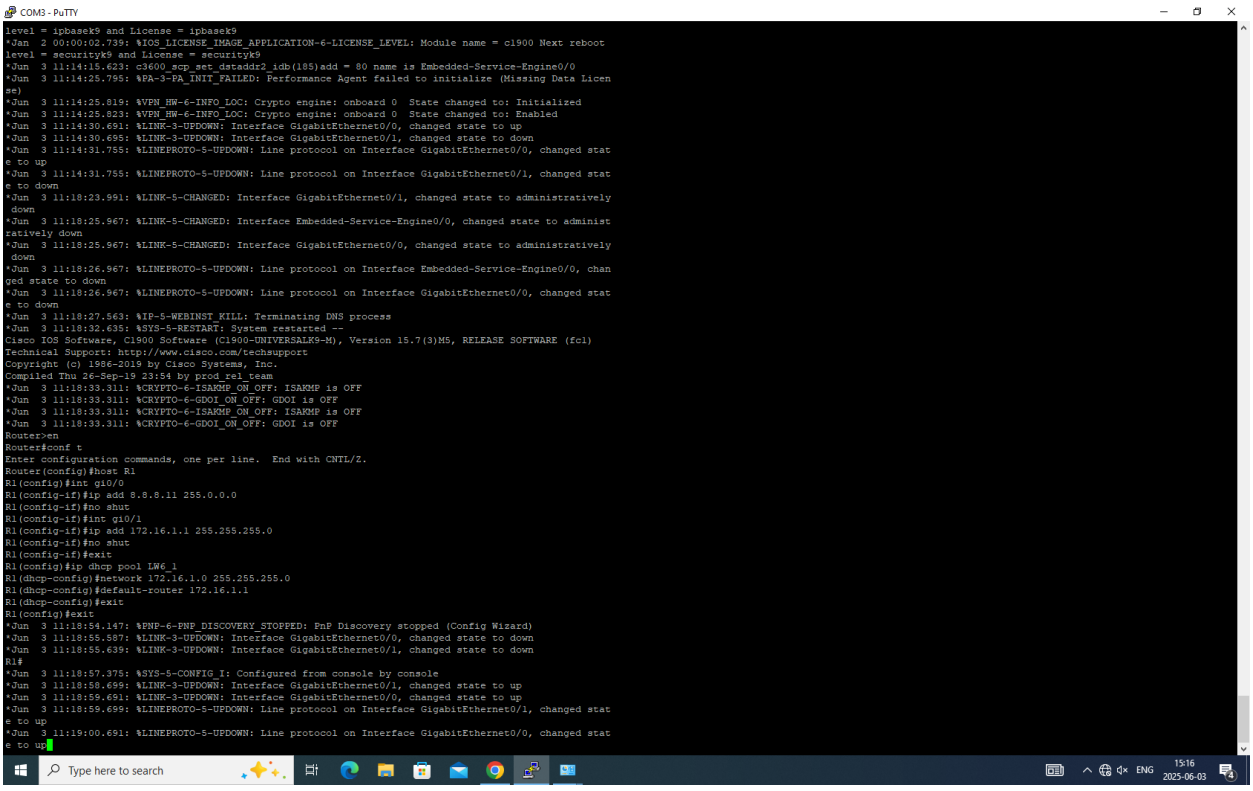
Lab Work Steps

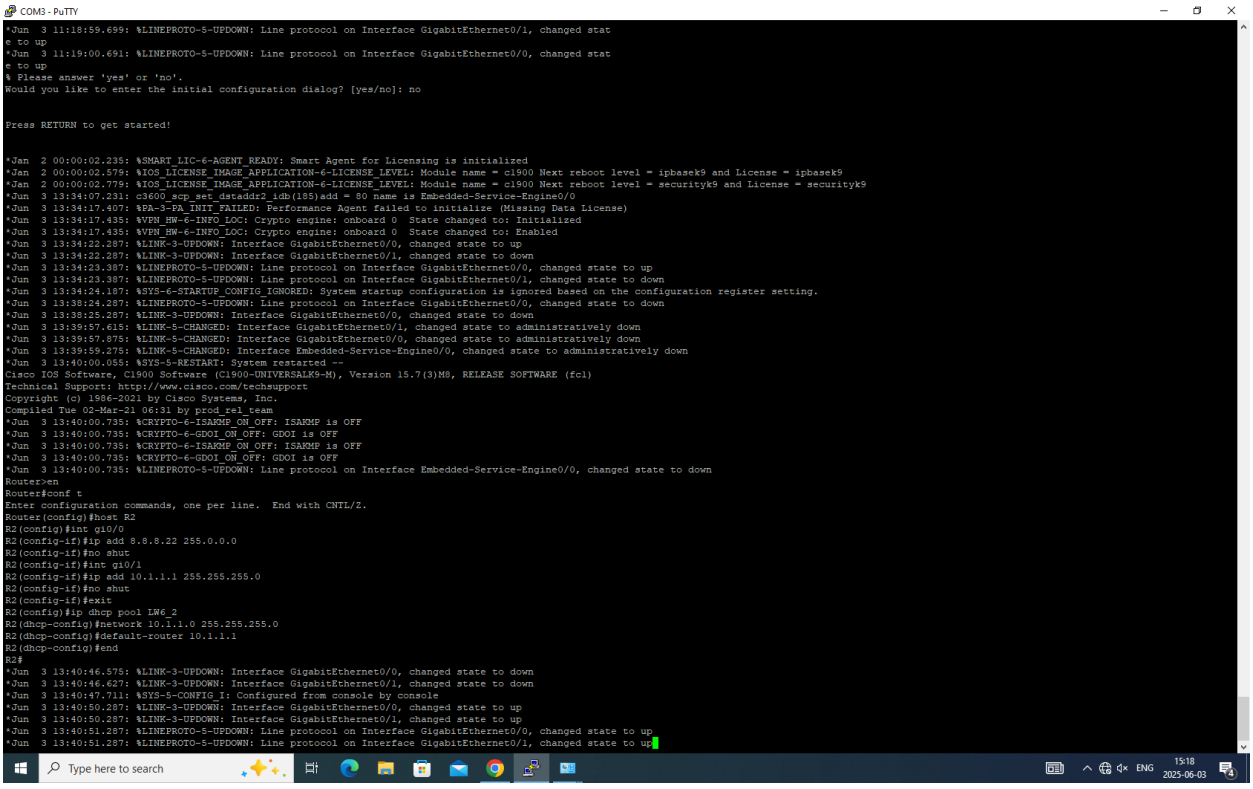
The lab work followed a series of steps

1.

Initial Configuration: Cisco 1941 routers (R1 and R2) and switches were connected

Console cables were used to configure each router according to the diagram and IP addressing scheme. End devices (PC1, Laptop, PC2) were connected to their corresponding switches. Initial IP configurations were obtained, for example: PC1: 172.16.1.3, Laptop: 172.16.1.4, PC2: 10.1.1.3

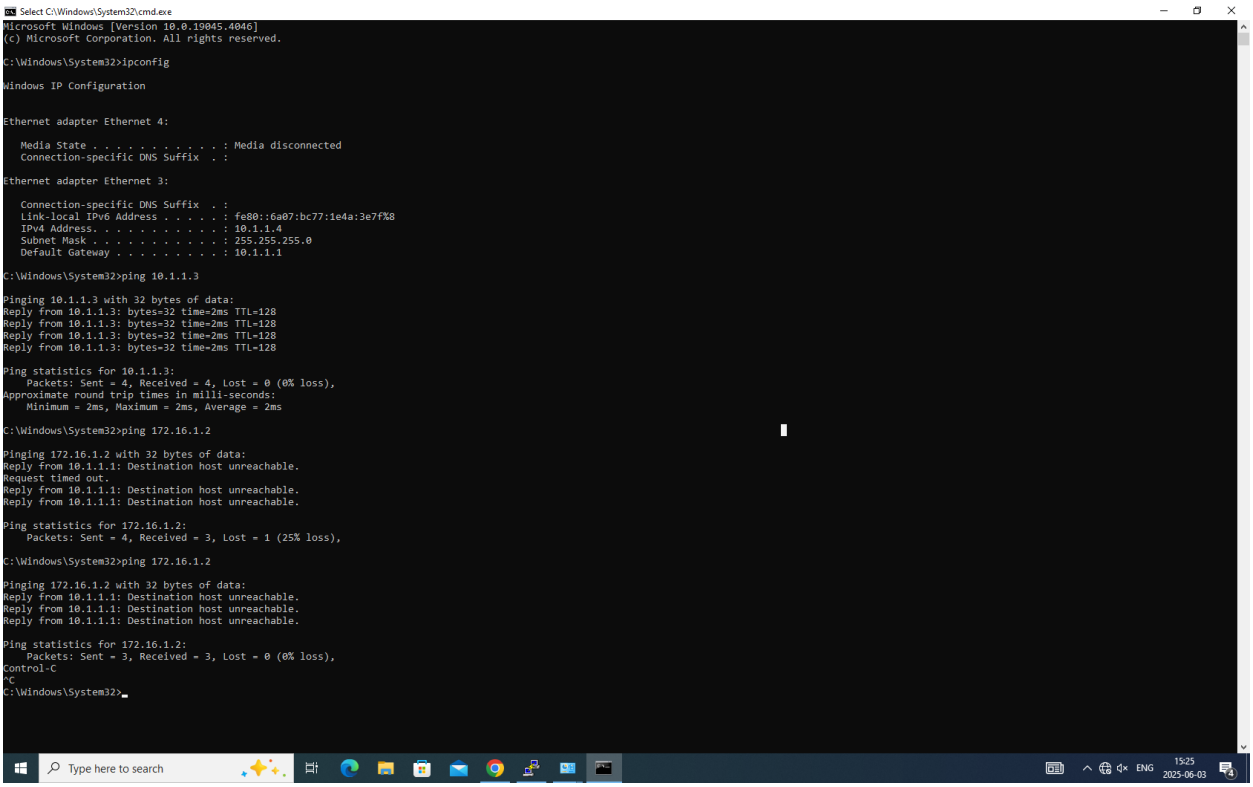

COM3 - PuTTY
level = ipbasek9 and License = ipbasek9
*Jan 2 00:00:02.739: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name = c1900 Next reboot level = securityk9 and License = securityk9
*Jun 3 11:14:15.623: c3600_scp_set_dstaddr2_idb(185)add = 80 name is Embedded-Service-Engine0/0
*Jun 3 11:14:25.795: %PA-3-PA_INIT_FAILED: Performance Agent failed to initialize (Missing Data License)
*Jun 3 11:14:25.819: %VPN_HW-6-INFO_LOC: Crypto engine: onboard 0 State changed to: Initialized
*Jun 3 11:14:25.823: %VPN_HW-6-INFO_LOC: Crypto engine: onboard 0 State changed to: Enabled
*Jun 3 11:14:30.691: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Jun 3 11:14:30.695: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to down
*Jun 3 11:14:31.755: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
*Jun 3 11:14:31.755: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down
*Jun 3 11:18:23.991: %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
*Jun 3 11:18:25.967: %LINK-5-CHANGED: Interface Embedded-Service-Engine0/0, changed state to administratively down
*Jun 3 11:18:25.967: %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to administratively down
*Jun 3 11:18:26.967: %LINEPROTO-5-UPDOWN: Line protocol on Interface Embedded-Service-Engine0/0, changed state to down
*Jun 3 11:18:26.967: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to down
*Jun 3 11:18:27.563: %IP-5-WEBINST_KILL: Terminating DNS process
*Jun 3 11:18:32.635: %SYS-5-RESTART: System restarted --
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.7(3)M5, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Thu 26-Sep-19 23:54 by prod_rel_team
*Jun 3 11:18:33.311: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
*Jun 3 11:18:33.311: %CRYPTO-6-GDOI_ON_OFF: GDOI is OFF
*Jun 3 11:18:33.311: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
*Jun 3 11:18:33.311: %CRYPTO-6-GDOI_ON_OFF: GDOI is OFF
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#host R1
R1(config)#int gi0/0
R1(config-if)#ip add 8.8.8.11 255.0.0.0
R1(config-if)#no shut
R1(config-if)#int gi0/1
R1(config-if)#ip add 172.16.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#ip dhcp pool LW6_1
R1(dhcp-config)#network 172.16.1.0 255.255.255.0
R1(dhcp-config)#default-router 172.16.1.1
R1(dhcp-config)#exit
R1(config)#exit
*Jun 3 11:18:54.147: %PNP-6-PNP_DISCOVERY_STOPPED: PnP Discovery stopped (Config Wizard)
*Jun 3 11:18:55.587: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to down
*Jun 3 11:18:55.639: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to down
R1#
*Jun 3 11:18:57.375: %SYS-5-CONFIG_I: Configured from console by console
*Jun 3 11:18:58.699: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
*Jun 3 11:18:59.691: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Jun 3 11:18:59.699: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
*Jun 3 11:19:00.691: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
Type here to search
ENG
15:16
2025-06-03


COM3 - PuTTY
*Jun 3 11:18:59.699: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
*Jun 3 11:19:00.691: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
% Please answer 'yes' or 'no'.
Would you like to enter the initial configuration dialog? [yes/no]: no
Press RETURN to get started!
*Jan 2 00:00:02.235: %SMART_LIC-6-AGENT_READY: Smart Agent for Licensing is initialized
*Jan 2 00:00:02.579: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name = c1900 Next reboot level = ipbasek9 and License = ipbasek9
*Jan 2 00:00:02.779: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name = c1900 Next reboot level = securityk9 and License = securityk9
*Jun 3 13:34:07.231: c3600_scp_set_dstaddr2_idb(185)add = 80 name is Embedded-Service-Engine0/0
*Jun 3 13:34:17.407: %PA-3-PA_INIT_FAILED: Performance Agent failed to initialize (Missing Data License)
*Jun 3 13:34:17.435: %VPN_HW-6-INFO_LOC: Crypto engine: onboard 0 State changed to: Initialized
*Jun 3 13:34:17.435: %VPN_HW-6-INFO_LOC: Crypto engine: onboard 0 State changed to: Enabled
*Jun 3 13:34:22.287: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Jun 3 13:34:22.287: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to down
*Jun 3 13:34:23.387: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
*Jun 3 13:34:23.387: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down
*Jun 3 13:34:24.187: %SYS-6-STARTUP_CONFIG_IGNORED: System startup configuration is ignored based on the configuration register setting.
*Jun 3 13:38:24.287: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to down
*Jun 3 13:38:25.287: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to down
*Jun 3 13:39:57.615: %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
*Jun 3 13:39:57.875: %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to administratively down
*Jun 3 13:39:59.275: %LINK-5-CHANGED: Interface Embedded-Service-Engine0/0, changed state to administratively down
*Jun 3 13:40:00.055: %SYS-5-RESTART: System restarted --
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.7(3)M8, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2021 by Cisco Systems, Inc.
Compiled Tue 02-Mar-21 06:31 by prod_rel_team
*Jun 3 13:40:00.735: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
*Jun 3 13:40:00.735: %CRYPTO-6-GDOI_ON_OFF: GDOI is OFF
*Jun 3 13:40:00.735: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
*Jun 3 13:40:00.735: %CRYPTO-6-GDOI_ON_OFF: GDOI is OFF
*Jun 3 13:40:00.735: %LINEPROTO-5-UPDOWN: Line protocol on Interface Embedded-Service-Engine0/0, changed state to down
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#host R2
R2(config)#int gi0/0
R2(config-if)#ip add 8.8.8.22 255.0.0.0
R2(config-if)#no shut
R2(config-if)#int gi0/1
R2(config-if)#ip add 10.1.1.1 255.255.255.0
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#ip dhcp pool LW6_2
R2(dhcp-config)#network 10.1.1.0 255.255.255.0
R2(dhcp-config)#default-router 10.1.1.1
R2(dhcp-config)#end
R2#
*Jun 3 13:40:46.575: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to down
*Jun 3 13:40:46.627: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to down
*Jun 3 13:40:47.711: %SYS-5-CONFIG_I: Configured from console by console
*Jun 3 13:40:50.287: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Jun 3 13:40:50.287: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
*Jun 3 13:40:51.287: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
*Jun 3 13:40:51.287: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
Type here to search
ENG
15:18
2025-06-03

2.

Initial Connectivity Testing (Before NAT): Connectivity between all terminals and router ports was tested using ping commands

The results were documented in a connectivity matrix.



3.

Initial Connectivity Matrix (Before R1 Routing and NAT):

Terminal	IP address	PC1	Laptop	R1 Gi0/1	R1 Gi0/0	R2 Gi0/0	R2 Gi0/1	PC2
PC1	172.16.1.3		YES	YES	YES	NO	NO	NO
Laptop	172.16.1.4	YES		YES	YES	NO	NO	NO
R1 Gi0/1	172.16.1.1	YES	YES		YES	YES	NO	NO
R1 Gi0/0	8.8.8.11	YES	YES	YES		YES	NO	NO
R2 Gi0/0	8.8.8.22	NO	NO	NO	YES		YES	YES
R2 Gi0/1	10.1.1.1	NO	NO	NO	YES	YES		YES
PC2	10.1.1.3	NO	NO	NO	NO	YES	YES	

4.

Based on the results

Successful pings occurred between devices on the same subnet and switch (e.g., PC1 to Laptop, PC1/Laptop to R1 Gi0/1)

Pings between R1's external interface (8.8.8.11) and R2's external interface (8.8.8.22) were also successful as they are on the same "public internet" segment

Failed pings occurred between devices on different LANs (e.g., PC1/Laptop to R2 interfaces or PC2) due to different subnets and the lack of routing to bridge these networks

PC2 could ping R2's interfaces (Gi0/0 and Gi0/1) and vice-versa as they are on the same network segment or directly connected

5.

Additional R1 Configuration (Static Route and NAT): As full connectivity between both LANs was not achieved initially

additional configuration was performed on R1

A static default route was added to R1, instructing it to send all packets with an unknown destination network (0.0.0.0/0) to R2's public IP address (8.8.8.22)

This ensures traffic destined for networks beyond R1's directly connected segments (like R2's internal network) is forwarded towards R2

An NAT address pool named LW6 was created, consisting of a single public IP address (8.8.8.11)

NAT was configured to translate packets from internal IP addresses defined in source list #1 to the public IP address in the LW6 pool, using the NAT overload method

An access-list 1 permit any was configured, setting any internally connected terminals to be part of internal access list #1

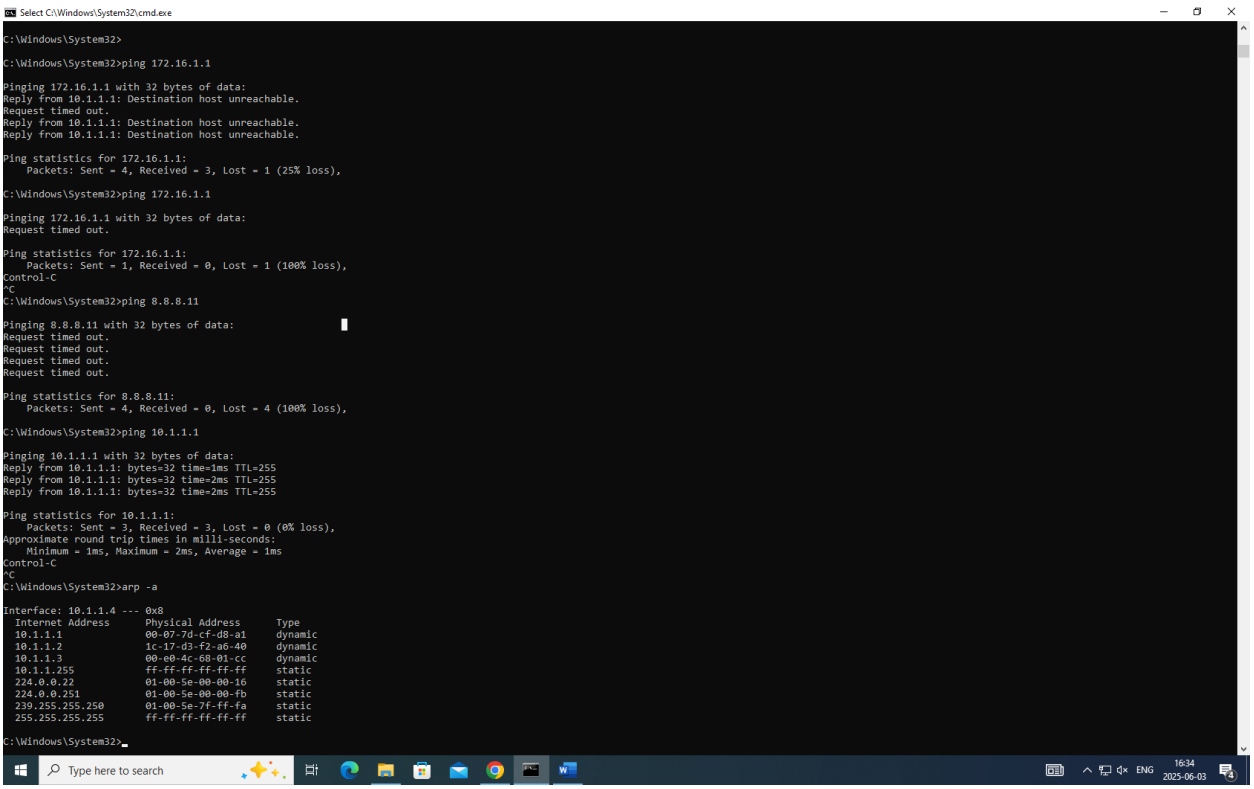
Interface Gi0/1 was configured as the internal side of the NAT conversion (ip nat inside)

Interface Gi0/0 was configured as the external side of the NAT conversion (ip nat outside)

6.

Retesting Connectivity (After NAT): Connectivity was re-tested from PC1 (and Laptop) to destinations that were previously unreachable

A second version of the connectivity matrix was prepared



7.

Second Connectivity Matrix (After R1 Routing and NAT):

Terminal	IP adress	PC1	Laptop	R1 Gi0/1	R1 Gi0/0	R2 Gi0/0	R2 Gi0/1	PC2
PC1			YES	YES	Yes	Yes	Yes	No
Laptop		YES		Yes	Yes	Yes	Yes	No
R1 Gi0/1	172.16.1.1	Yes	Yes		Yes	Yes	Yes	No
R1 Gi0/0	8.8.8.11	No	No	Yes		Yes	Yes	No
R2 Gi0/0	8.8.8.22	No	No	Yes	Yes		Yes	No
R2 Gi0/1	10.1.1.1	No	No	Yes	Yes	Yes		Yes
PC2		No	No	No	Yes	Yes	Yes	

8.

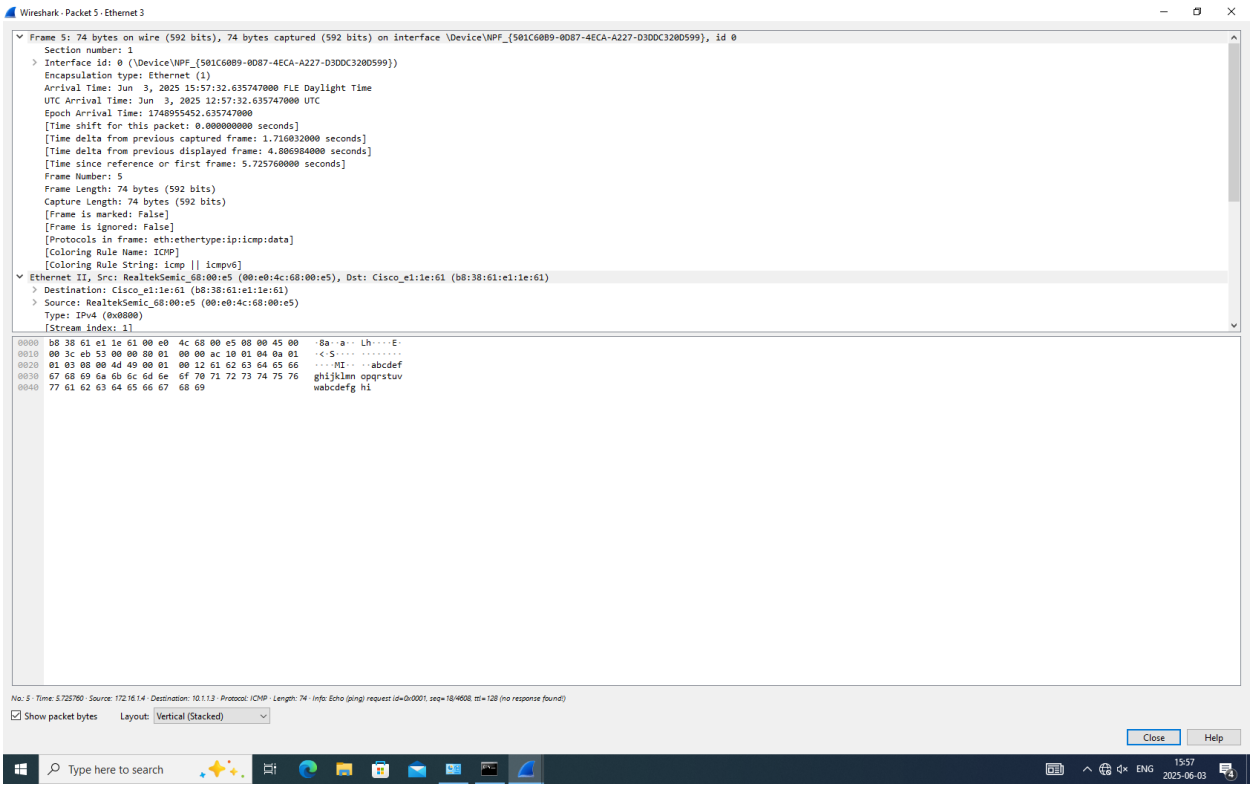
After configuring static routing and NAT on R1, full connectivity was achieved between most devices

The default route allowed R1 to forward packets to R2, and NAT enabled communication between different subnets by translating internal IPs.

9.

Packet Analysis (Wireshark): Wireshark was launched on PC1 and PC2 to log network traffic

A ping was sent from PC1 to PC2. The logs were analyzed to observe Layer 2 (MAC) and Layer 3 (IP) addressing changes due to NAT



10.

Outbound ping packet sent from PC1 to PC2				
	Destination MAC	Source MAC	Source IP	Destination IP
Addresses:	B8:38:61:e1:1e:61	00:e0:4c:68:00:e5	172.164.1.4	10.1.1.3
Terminal:	R1 Gi0/1	PC1	PC1	PC2

Inbound ping packet from PC1, as received at PC2				
	Destination MAC	Source MAC	Source IP	Destination IP
Addresses:	00:e0:4c:68:01:cc	00:07:79:cf:d8:a1	8.8.8.11	10.1.1.3
Terminal:	PC2	R2 Gi0/1	R1 Gi0/0	PC2

11.

When PC1 pings PC2, R1 performs NAT, replacing PC1's private source IP (172.16.1.3) with its public IP (8.8.8.11)

PC2 receives the ping with the source IP of 8.8.8.11. The MAC addresses change at each hop; the source MAC arriving at PC2 would be R2's internal interface MAC, and the destination MAC would be PC2's MAC

Answering Questions:

What is NAT and why did enabling it on the R1 router help with specific connectivity issues? Network Address Translation (NAT) allows multiple devices on a local (private) network to share a single public IP address for accessing external networks like the Internet

It translates private IP addresses of local devices to a public IP address when traffic leaves the private network and translates the public IP back to the correct private IP for incoming responses. Enabling NAT on R1 resolved connectivity issues by allowing devices on the private network behind R1 (PC1, Laptop) to communicate with devices on the private network behind R2 (PC2) by translating their private source IPs to R1's public IP. This makes the traffic appear to originate from R1's public address, which is routable across the "public internet" segment between R1 and R2

Why was the ‘NAT overload’ method chosen when programming the NAT functionality? NAT overload, also known as Port Address Translation (PAT), was chosen because it is an efficient method that allows numerous devices on a local network to share a single public IP address

It achieves this by using unique source port numbers to keep track of the different connections from each internal device. This method is highly effective for conserving limited public IP addresses, making it a cost-effective and scalable solution for providing Internet access to multiple devices behind a single router

Conclusion

This lab successfully demonstrated how to connect two LANs using reserved private IP addresses over a simulated public Internet network

The core concept of NAT was explored, highlighting the difference between private and public IP addresses. By implementing NAT on the gateway router (R1), devices on the private network were able to communicate with devices on the other private network across the public link. The lab provided practical experience with configuring static routing and NAT, including the use of the NAT overload method, and troubleshooting connectivity

issues. Analyzing packet headers with Wireshark confirmed the IP address translation performed by NAT. The use of connectivity matrices proved valuable in understanding the state of inter-subnet communication before and after the implementation of routing and NAT. This exercise enhanced practical skills in network configuration, particularly concerning IP addressing, routing, and address translation