Project 6

Configuring and Verifying ACLs

Team Members
Fady Monier Zaghloul
Omar Gamil Ahmed
Bola Joseph Rateb
Mohamed Sayed Mohamed

Under supervision:

Eng. Mohamed Abdelkader

Table of Contents

Introduction:

Project Overview

This project focuses on configuring a router with standard named ACLs, extended named ACLs, and numbered extended ACLs to meet specific security and communication requirements within a simulated enterprise network. The aim is to restrict and permit access between different network zones and devices.

Objectives

- Configure a router with standard named ACLs.
- Configure a router with extended named ACLs.
- Configure a router with extended ACLs to meet specific communication requirements.
- Configure ACLs to control access to terminal lines.
- Apply ACLs on appropriate router interfaces and directions.
- Verify ACL operation and behavior.

Tools and Technologies Used

- Cisco Packet Tracer / Networking Simulator
- Routers and Switches (Simulated)
- Basic Command Line Interface (CLI)

Network Design:

Network Topology

The topology consists of two routers (HQ and Branch), multiple LANs, an internet user, and web servers.

IP Addressing Scheme

Device	Interface	IP Address
HQ	G0/0/0	192.168.1.1/26
HQ	G0/0/1	192.168.1.65/29
HQ	S0/1/0	192.0.2.1/30
HQ	S0/1/1	192.168.3.1/30
Branch	G0/0/0	192.168.2.1/27
Branch	G0/0/1	192.168.2.33/28
Branch	S0/1/1	192.168.3.2/30
PC-1	NIC	192.168.1.10/26
PC-2	NIC	192.168.1.20/26
PC-3	NIC	192.168.1.30/26
Admin	NIC	192.168.1.67/29
Enterprise Web Server	NIC	192.168.1.70/29
Branch PC	NIC	192.168.2.17/27
Branch Server	NIC	192.168.2.45/28
Internet User	NIC	198.51.100.218/24
External Web Server	NIC	203.0.113.73/24

ACL Configuration:

ACL 101 (Extended)

- Block FTP access from Internet to Enterprise Web Server
- Block ICMP from Internet to HQ LAN
- Permit all other traffic

ACL 111 (Extended)

- Deny all access from HQ LAN 1 to Branch Server
- Permit all other traffic

Named Standard ACL (vty_block)

- Allow only HQ LAN 2 devices to access HQ router VTY lines

Named Extended ACL (branch_to_hq)

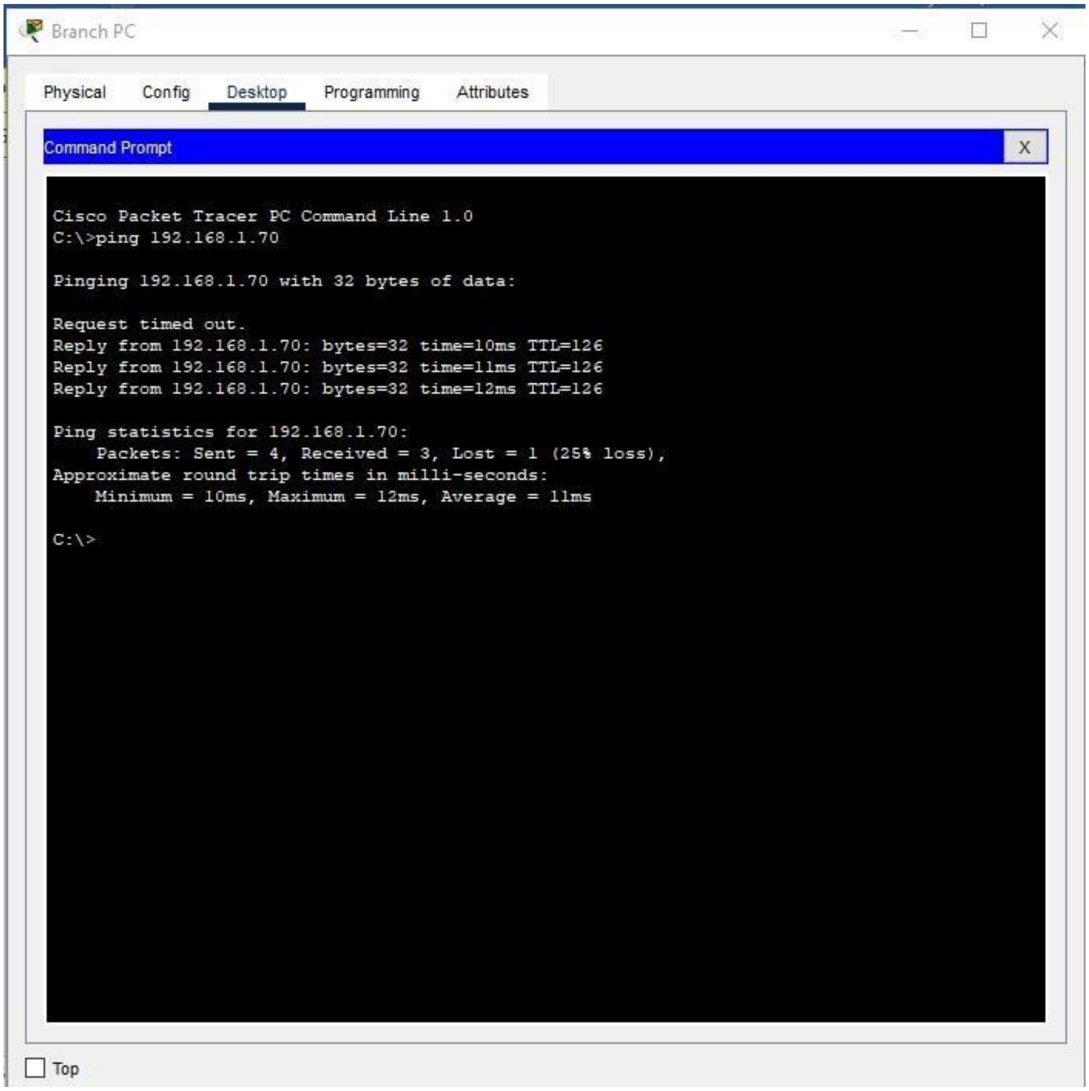
- Deny all access from Branch LANs to HQ LAN 1
- Permit all other traffic

ACL Application:

- ACL 101 applied on HQ's incoming external interface.
- ACL 111 applied on HQ’s interface facing HQ LAN 1.
- vty_block applied to line vty 0 4.
- branch_to_hq applied on Branch’s LAN-facing interfaces.

Testing and Troubleshooting:

Ping from Branch PC to Enterprise Web Server



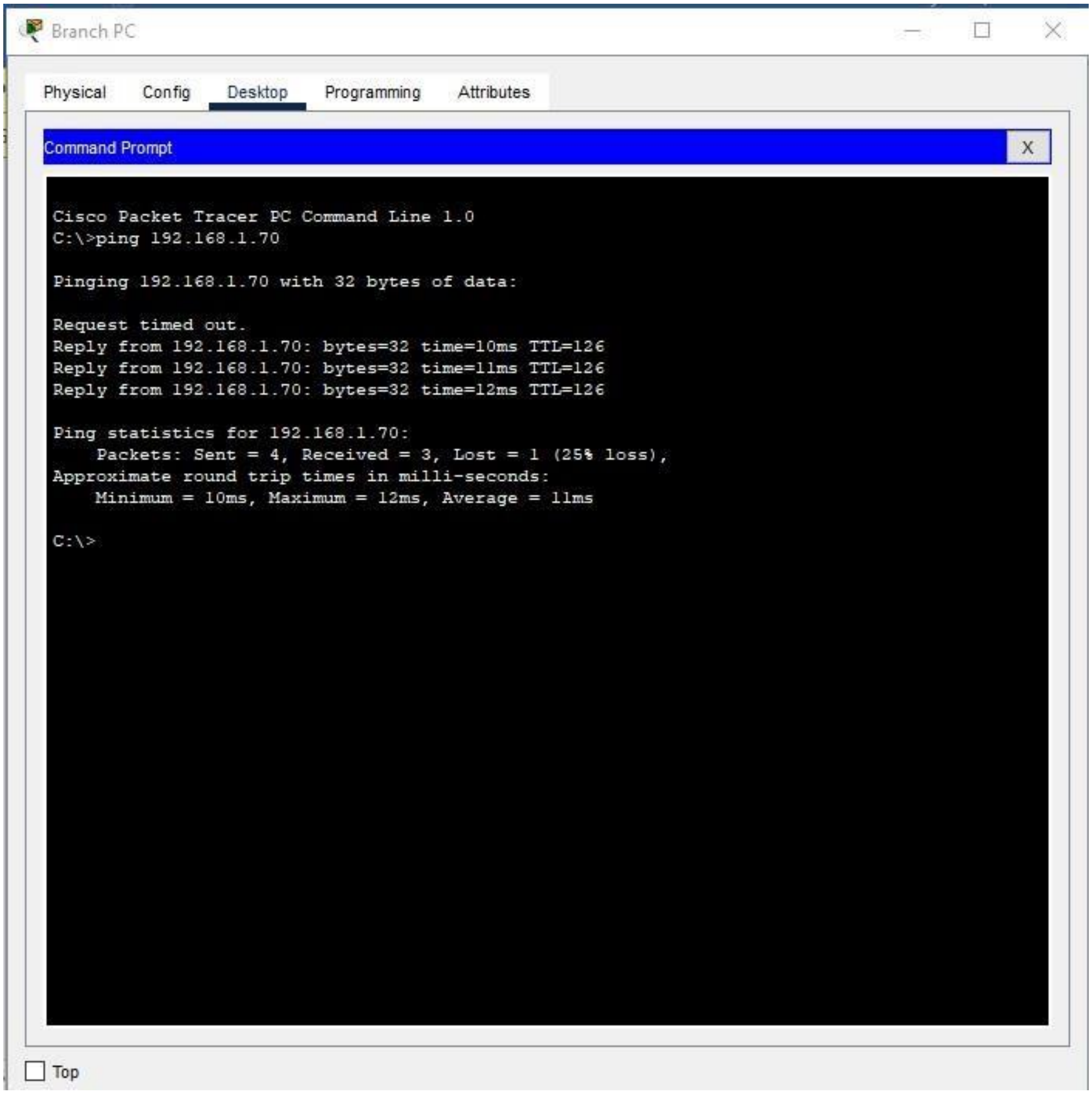
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.70

Pinging 192.168.1.70 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.70: bytes=32 time=10ms TTL=126
Reply from 192.168.1.70: bytes=32 time=11ms TTL=126
Reply from 192.168.1.70: bytes=32 time=12ms TTL=126

Ping statistics for 192.168.1.70:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 12ms, Average = 11ms

C:\>
```

Figure 1

Comment:

As shown in the figure, the ping was successful because it was permitted by the final 'permit ip any any' rule in the 'branch_to_hq' access list.

Ping from PC-1 to Branch Server



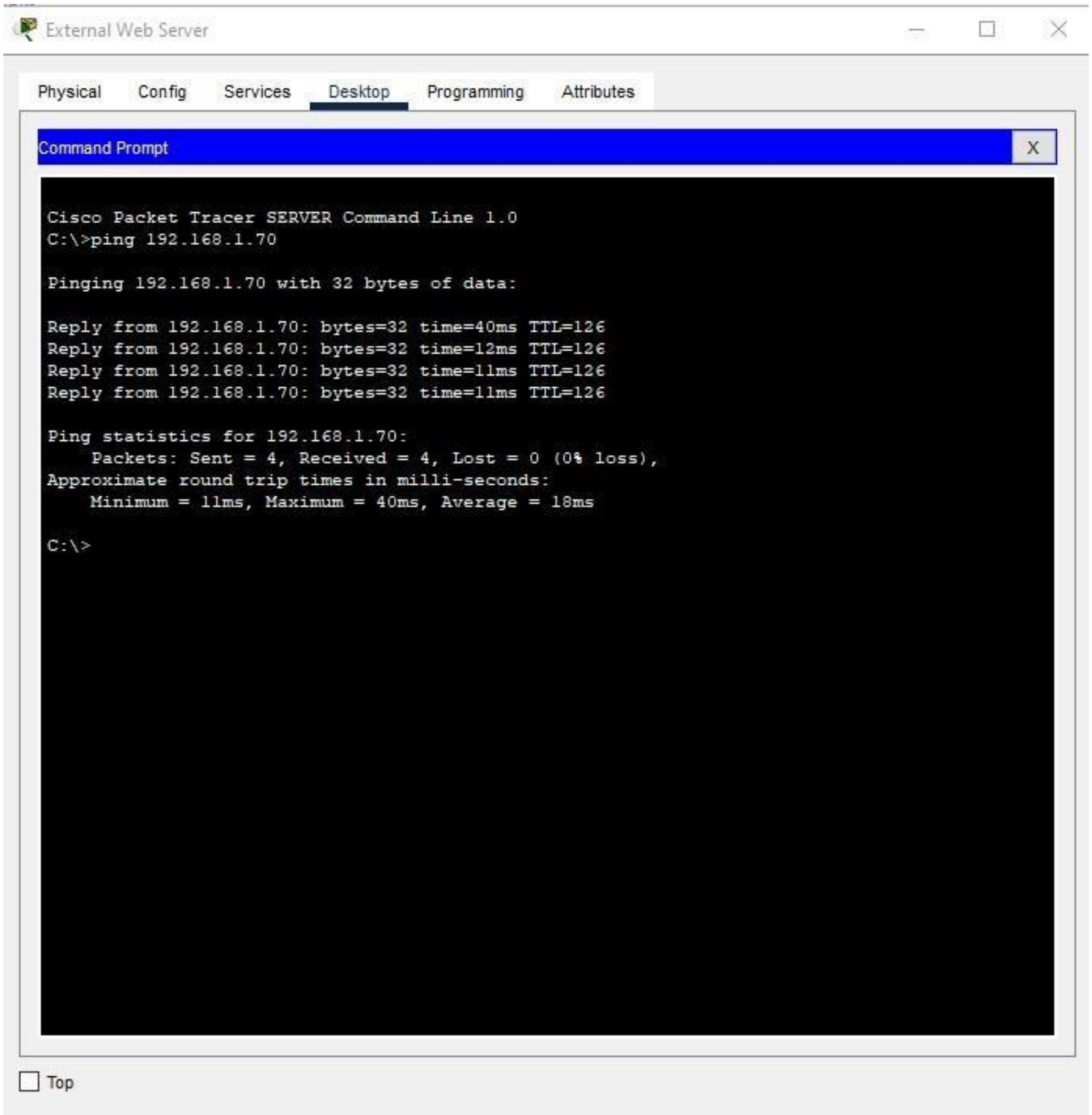
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.70

Pinging 192.168.1.70 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.70: bytes=32 time=10ms TTL=126
Reply from 192.168.1.70: bytes=32 time=11ms TTL=126
Reply from 192.168.1.70: bytes=32 time=12ms TTL=126

Ping statistics for 192.168.1.70:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 12ms, Average = 11ms

C:\>
```

Figure 2

Comment:

As shown in the figure, the request was blocked because it was denied by statement 10 in ACL 111 on HQ.

HTTP from External Server to Enterprise Web Server



```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.1.70

Pinging 192.168.1.70 with 32 bytes of data:

Reply from 192.168.1.70: bytes=32 time=40ms TTL=126
Reply from 192.168.1.70: bytes=32 time=12ms TTL=126
Reply from 192.168.1.70: bytes=32 time=11ms TTL=126
Reply from 192.168.1.70: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.1.70:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 40ms, Average = 18ms

C:\>
```

Figure 3

Comment:

As shown in the figure, the connection was successful because ACL 101 permits HTTP traffic.

FTP from Internet to Branch Server

Yes, the FTP connection from the internet User PC to the Branch Server is successful.

Which access list should be modified to prevent users from the Internet to make FTP connections to the Branch Server? our answers here.

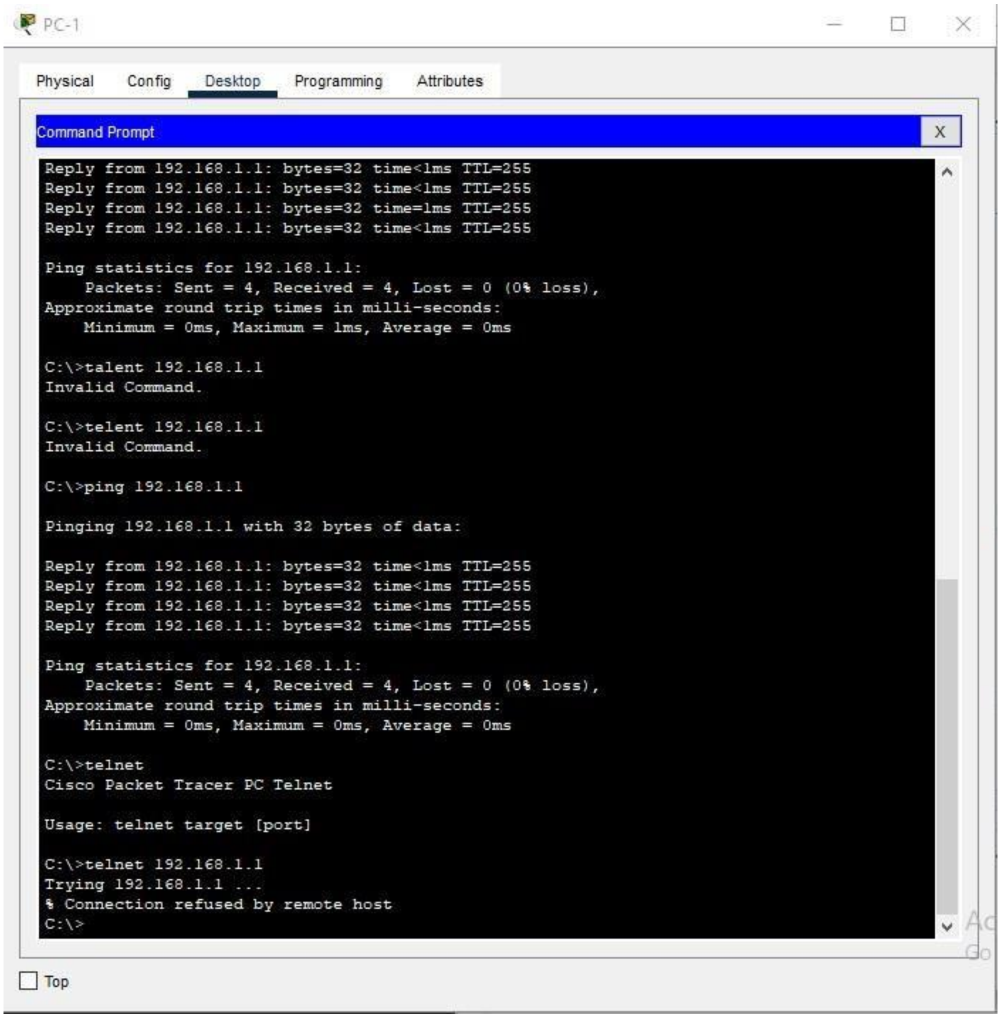
The access list 101 on the HQ router needs to be modified to deny this traffic.

Which statement(s) should be added to the access list to deny this traffic? Type your answers here.

The statement “deny tcp any host 192.168.2.45 eq 21” or “deny tcp any host 192.168.2.45 range 20 21” needs to be added to the access list 101.

Telnet to HQ Router

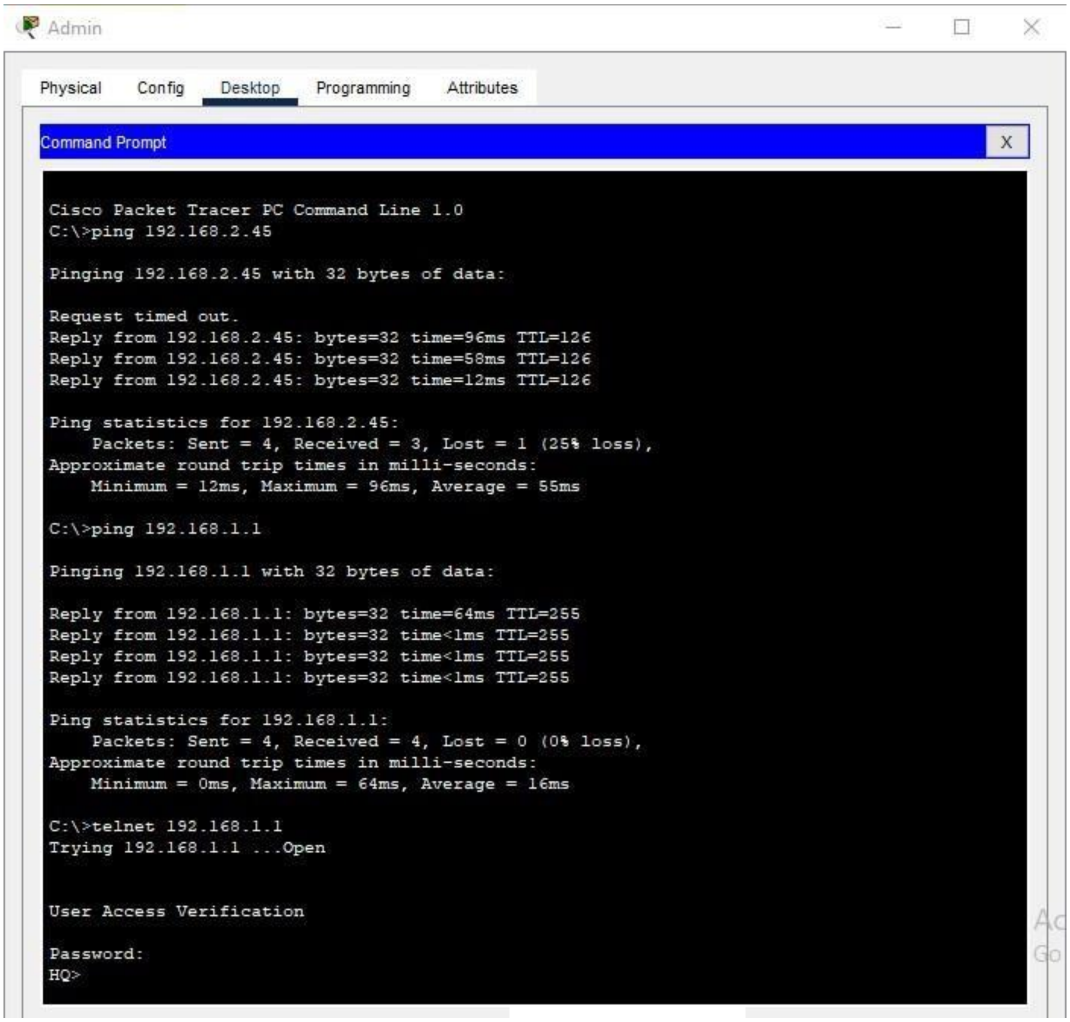
From PC0 (192.168.1.10)



```
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>talent 192.168.1.1
Invalid Command.

C:\>telent 192.168.1.1
Invalid Command.

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>telnet
Cisco Packet Tracer PC Telnet

Usage: telnet target [port]

C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...
% Connection refused by remote host
C:\>
```

Figure 4

From Admin (192.168.1.67)



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.45

Pinging 192.168.2.45 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.45: bytes=32 time=96ms TTL=126
Reply from 192.168.2.45: bytes=32 time=58ms TTL=126
Reply from 192.168.2.45: bytes=32 time=12ms TTL=126

Ping statistics for 192.168.2.45:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 96ms, Average = 55ms

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=64ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 64ms, Average = 16ms

C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open


User Access Verification

Password:
HQ>
```

Figure 5

Comment:

As shown in the figures, access was restricted because the 'vty_block' access list permits only the 192.168.1.64/29 subnet.

Results and Analysis:

- ACLs effectively managed traffic as per requirements
- Some adjustments were needed for FTP filtering
- Standard and named ACLs were correctly applied

Challenges and Solutions:

- Telnet blocked for unauthorized hosts: Solved with named standard ACL on vty lines
- FTP filtering not effective initially: Resolved with additional deny statements
- Complexity in ACL direction: Addressed via careful interface selection

Conclusion:

This project successfully configured and verified standard and extended ACLs to meet the specified requirements. The network topology was built, IP addresses assigned, routing established, and ACLs applied efficiently to control traffic and VTY access. All tests confirmed the ACLs function as intended.

Appendices:

Sample ACL Configuration

```
access-list 101 deny tcp any host 192.168.1.70 eq 21

access-list 101 deny icmp any 192.168.1.0 0.0.0.63

access-list 101 permit ip any any


access-list 111 deny ip 192.168.1.0 0.0.0.63 host 192.168.2.45

access-list 111 permit ip any any


ip access-list standard vty_block

 permit 192.168.1.64 0.0.0.7
```

```
ip access-list extended branch_to_hq
 deny ip 192.168.2.0 0.0.0.31 192.168.1.0 0.0.0.63
 deny ip 192.168.2.32 0.0.0.15 192.168.1.0 0.0.0.63
 permit ip any any
```

Network Topology Diagram

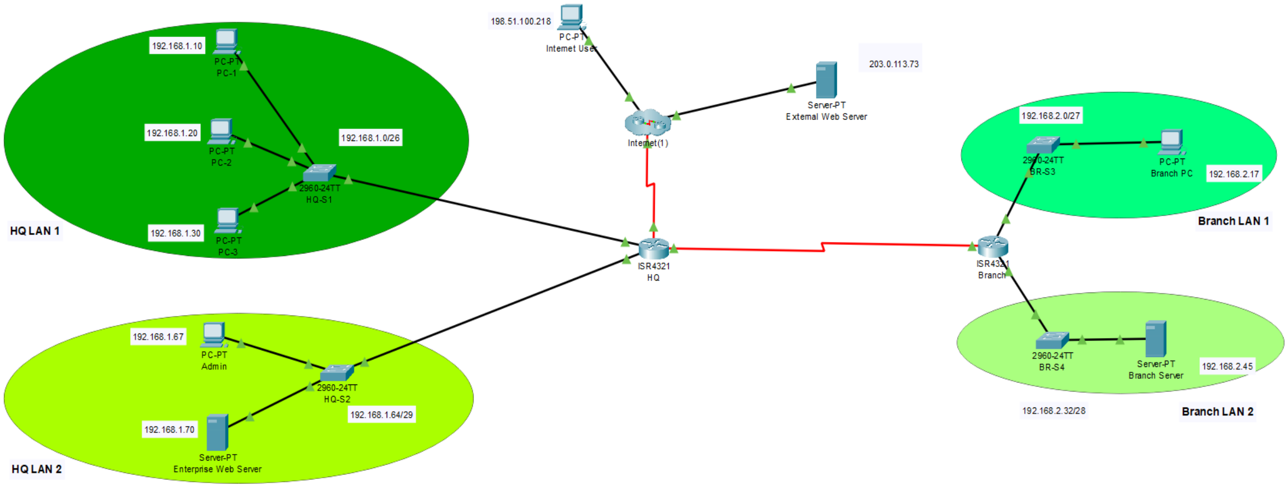


Figure 6