ACCESS CONTROL LIST PROJECT PRESENTATION (PROJECT 6)

For DEPI

AGENDA

1. OUR TEAM
2. INRODUCTION
3. NETWORK TOPOLOGY OVERVIEW
4. ACL CONFIGURATION OVERVIEW
5. DETAILED ACL CONFIGURATIONS (HQ ROUTER)
6. DETAILED ACL CONFIGURATIONS (BRANCH ROUTER)
7. CONNECTIVITY TESTS
8. CONCLUSION

OUR TEAM

1. MAHMOUD SAAD
2. AHMED MOHAMED
3. ESRAA KHALIFA
4. OMAR ABDALLA
5. AHMED MAGED
6. ARWA SARAYA

INRODUCTION

PROJECT OVERVIEW:

- This project utilized Cisco Packet Tracer to design and configure Access Control Lists (ACLs) in a virtual network environment.

PURPOSE:

- To manage and control the flow of network traffic between different segments of a simulated organization’s network**.**

KEY OBJECTIVE:

- Enhance the security of the network by preventing unauthorized access while allowing legitimate communication between network devices.

WHY ACLS?:

- ACLs help define rules for what traffic can enter or leave network interfaces.
- They are essential for implementing security policies within an organization’s network.

NETWORK TOPOLOGY OVERVIEW

NETWORK DESIGN:

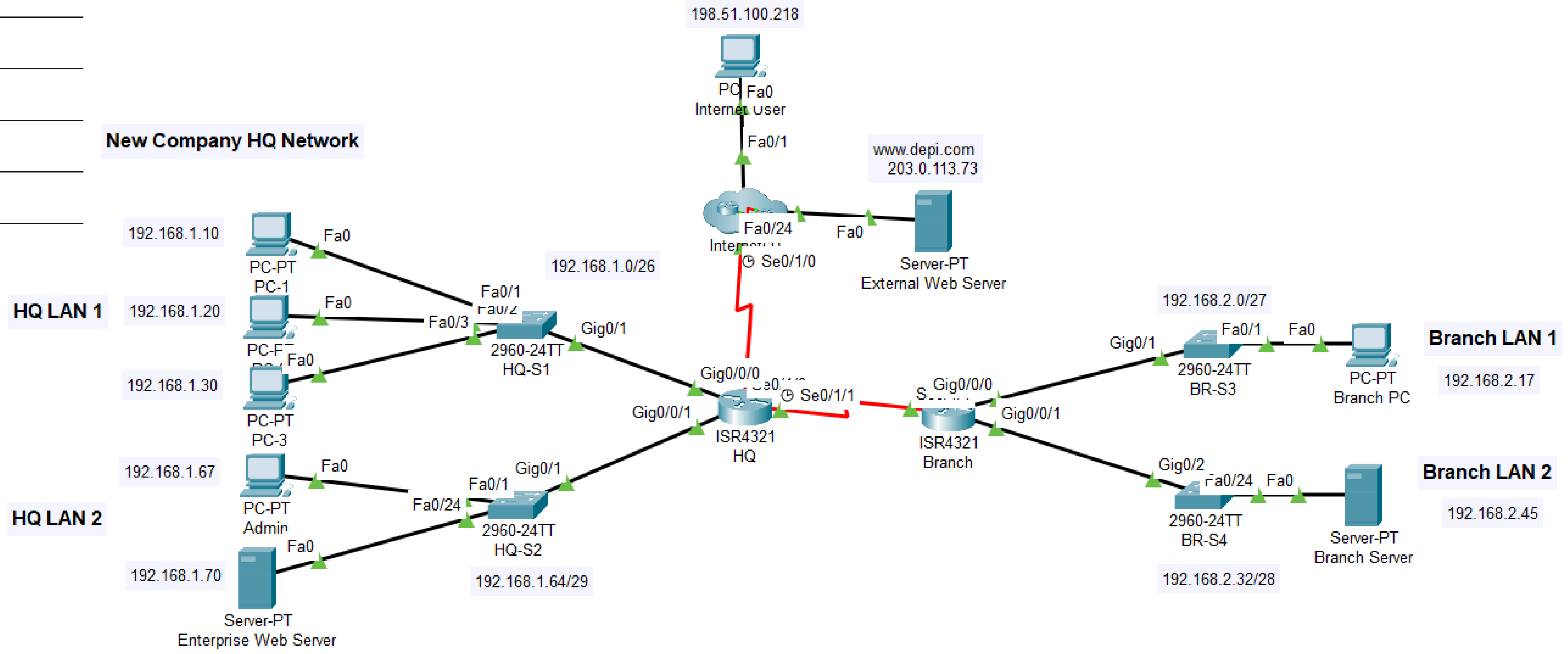
- The network includes two primary routers:
  - **HQ Router:** Manages communication within the headquarters network and connects to the internet.
  - **Branch Router:** Controls traffic at a branch office location.

- Each router connects to multiple LAN segments, handling traffic between the HQ, branch office, internet, and internal devices like servers and PCs.-

COMPONENTS:

- HQ Network: Two LAN segments with PCs and servers.
- Branch Network: Includes PCs, a server, and internet connectivity..

Device	Interface	IP Address
HQ	G0/0/0	192.168.1.1/26
	G0/0/1	192.168.1.65/29
	S0/1/0	192.0.2.1/30
	S0/1/1	192.168.3.1/30
Branch	G0/0/0	192.168.2.1/27
	G0/0/1	192.168.2.33/28
	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 OVERVIEW

- **PURPOSE OF CONFIGURING ACLS:**
  - TO FILTER INCOMING AND OUTGOING TRAFFIC ON SPECIFIC NETWORK INTERFACES.
  - TO RESTRICT OR ALLOW ACCESS BASED ON SECURITY POLICIES FOR DIFFERENT NETWORK SEGMENTS.
  - TO ENSURE COMPLIANCE WITH SECURITY REQUIREMENTS FOR INTERNAL AND EXTERNAL COMMUNICATION.
- **TYPES OF ACLS CONFIGURED:**
  - STANDARD NAMED ACLS: USED FOR BASIC FILTERING BASED ON SOURCE IP ADDRESSES.
  - EXTENDED ACLS: PROVIDE FINE-GRAINED CONTROL OVER TRAFFIC BY FILTERING BASED ON PROTOCOLS, SOURCE, AND DESTINATION IP ADDRESSES AND PORT NUMBERS.
- **APPLICATION OF ACLS:**
  - ACLS WERE APPLIED TO SPECIFIC INTERFACES ON EACH ROUTER TO CONTROL THE FLOW OF TRAFFIC AS IT ENTERS OR EXITS THE NETWORK.

DETAILED ACL CONFIGURATIONS (HQ ROUTER)

ROUTER HQ CONFIGURATIONS:

- ACL 101:
  - Blocks FTP access to the Enterprise Web Server from external users on the internet.
  - Blocks FTP access from Internet User to the Branch Server.
  - Denies ICMP traffic from the internet to the entire HQ LAN to prevent ping attacks.
  - Permits all other types of traffic, ensuring legitimate communication is unaffected.
  - Configuration Example:

```
access-list 101 deny tcp any host 192.168.1.70 eq ftp
access-list 101 deny icmp any 192.168.1.0 0.0.0.63
access-list 101 permit ip any any
```

ACL Application:

- Applied on the Serial0/1/1 interface to control outgoing traffic from the branch to HQ.

```
interface Serial0/1/0
ip access-group 101 in
```

DETAILED ACL CONFIGURATIONS (HQ ROUTER)

ROUTER HQ CONFIGURATIONS:

- ACL 111:
  - Blocks access from HQ LAN 1 to the Branch Server.
  - Allows all other traffic.

  - Configuration:

```
access-list 111 deny ip any host 192.168.2.45
access-list 111 permit ip any any
```

- ACL Application:

-Applied on the GigabitEthernet0/0/0 to control incoming traffic from the HQ LAN 1.

```
interface GigabitEthernet0/0/0
ip access-group 111 in
```

DETAILED ACL CONFIGURATIONS (HQ ROUTER)

- STANDARD NAMED ACL (VTY_BLOCK):

- Restricts VTY (Telnet/SSH) access to the HQ router, limiting it to HQ LAN 2.

- CONFIGURATION:

```
ip access-list standard vty_block
permit 192.168.1.64 0.0.0.7
```

- ACL APPLICATION:

- Applied on the VTY lines to control incoming traffic from the HQ LAN 2.

```
line vty 0 4
access-class vty_block in
```

DETAILED ACL CONFIGURATIONS (BRANCH ROUTER)

ROUTER BRANCH CONFIGURATIONS:

- EXTENDED NAMED ACL: (BRANCH_TO_HQ):

- Blocks any access attempts from Branch LAN 1 and Branch LAN 2 to HQ LAN1.

- CONFIGURATION:

```
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
```

- ACL APPLICATION:

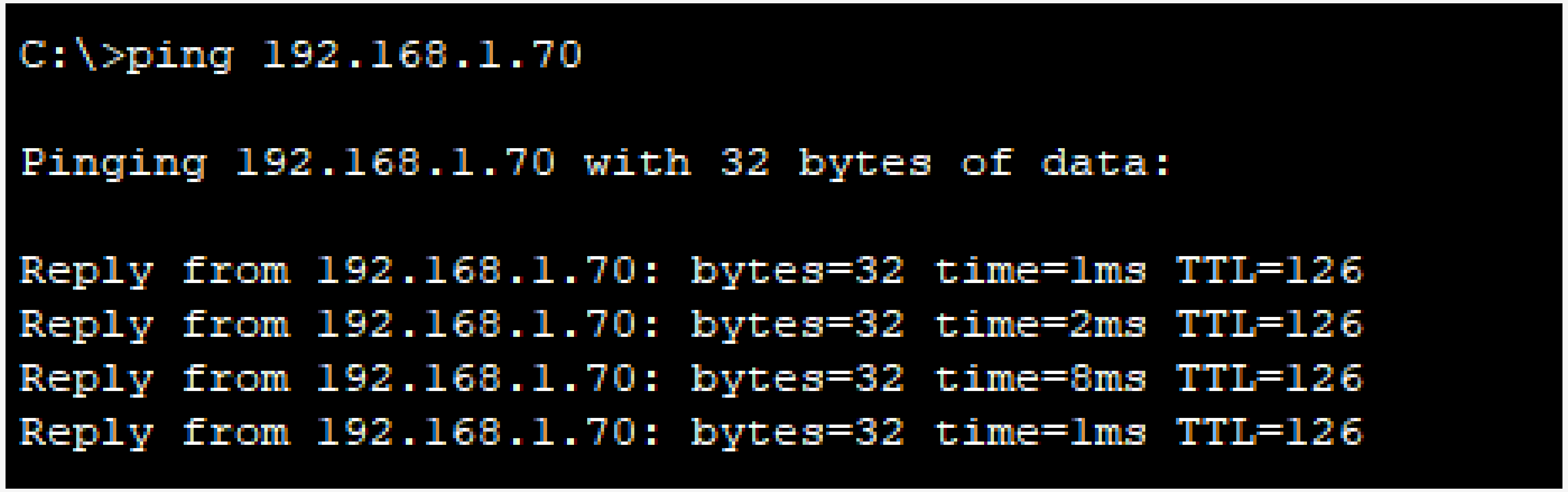
- Applied on the Serial0/1/1 interface to control outgoing traffic from the branch to HQ.

```
interface Serial0/1/1
ip access-group branch_to_hq out
```

CONNECTIVITY TESTS

- **PURPOSE OF TESTS:** TO VERIFY THAT THE ACLS WORK AS INTENDED AND RESTRICT OR ALLOW TRAFFIC ACCORDING TO THE CONFIGURED RULES.

- **TEST SCENARIOS:**
  - **TEST 1:** PING FROM BRANCH PC TO THE ENTERPRISE WEB SERVER.
  - **RESULT:** SUCCESSFUL PING, AS ACL 101 ONLY BLOCKS FTP TRAFFIC, NOT ICMP OR HTTP.
  - **OUTCOME:** CONFIRMS THAT REGULAR TRAFFIC BETWEEN THE BRANCH AND WEB SERVER IS ALLOWED.



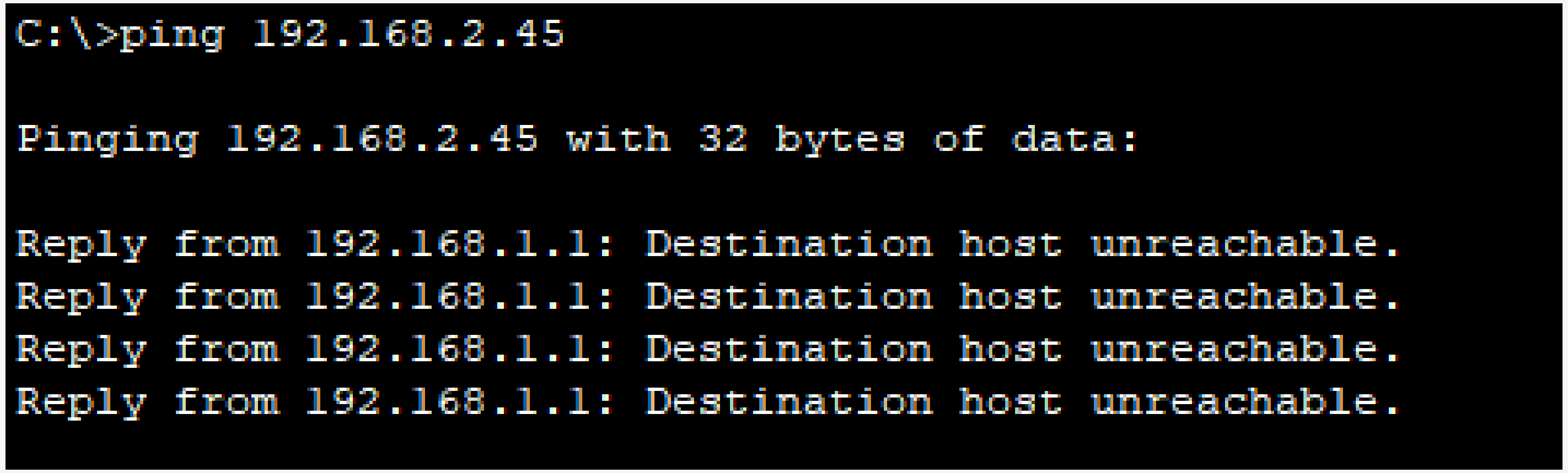
```
C:\>ping 192.168.1.70

Pinging 192.168.1.70 with 32 bytes of data:

Reply from 192.168.1.70: bytes=32 time=1ms TTL=126
Reply from 192.168.1.70: bytes=32 time=2ms TTL=126
Reply from 192.168.1.70: bytes=32 time=8ms TTL=126
Reply from 192.168.1.70: bytes=32 time=1ms TTL=126
```

CONNECTIVITY TESTS

- **Test 2:** Ping from HQ PC-1 to Branch Server.
- **RESULT:** UNSUCCESSFUL PING, AS ACL 111 BLOCKS TRAFFIC TO THE BRANCH SERVER.
- **OUTCOME:** VALIDATES THAT HQ LAN 1 CANNOT ACCESS RESTRICTED BRANCH RESOURCES.



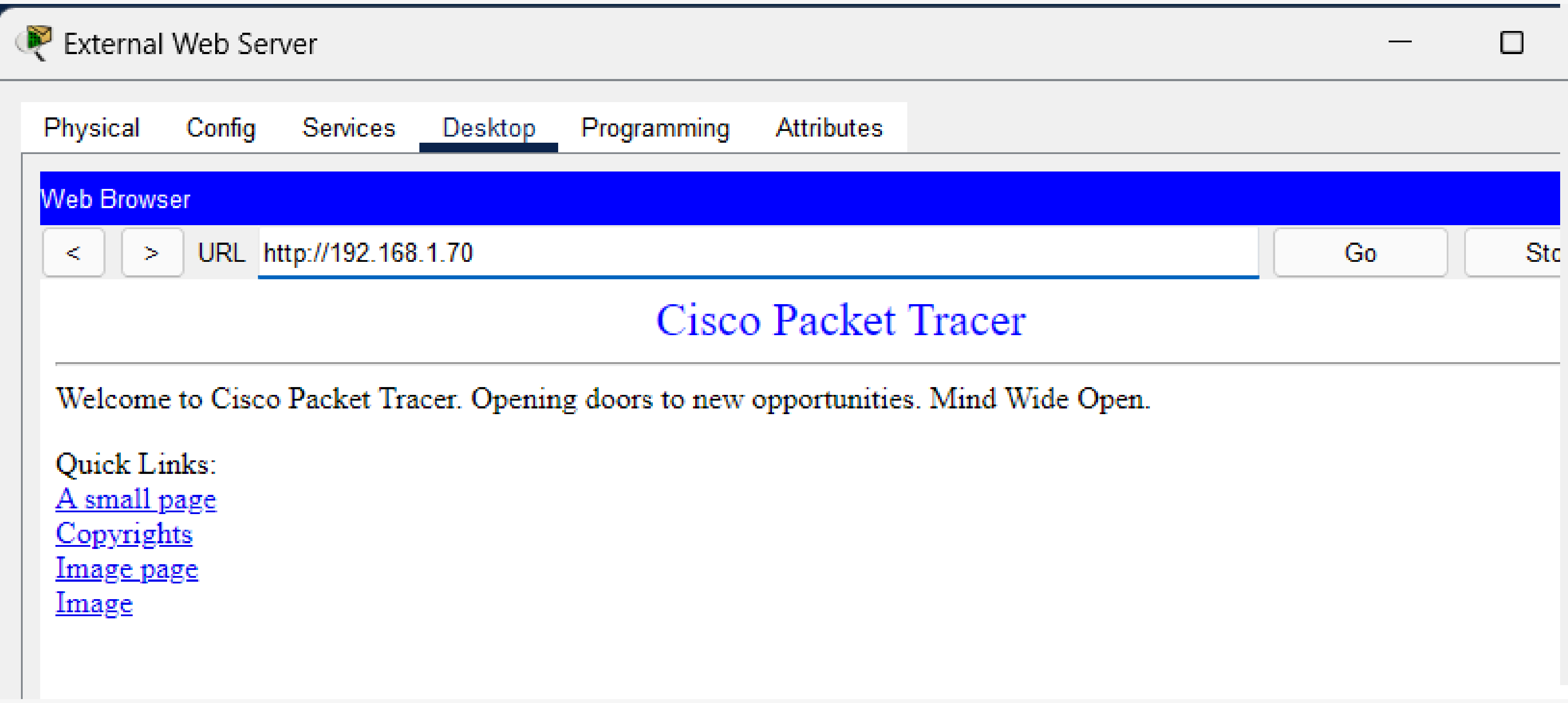
```
C:\>ping 192.168.2.45

Pinging 192.168.2.45 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
```

CONNECTIVITY TESTS

- **TEST 3:** HTTP ACCESS FROM EXTERNAL WEB SERVER TO THE ENTERPRISE WEB SERVER.
- **RESULT:** ACCESS WAS SUCCESSFUL, SHOWING THAT ACL 101 PERMITS HTTP TRAFFIC WHILE BLOCKING FTP.
- **OUTCOME:** CONFIRMS SECURE ACCESS FROM EXTERNAL SOURCES TO INTERNAL SERVERS.

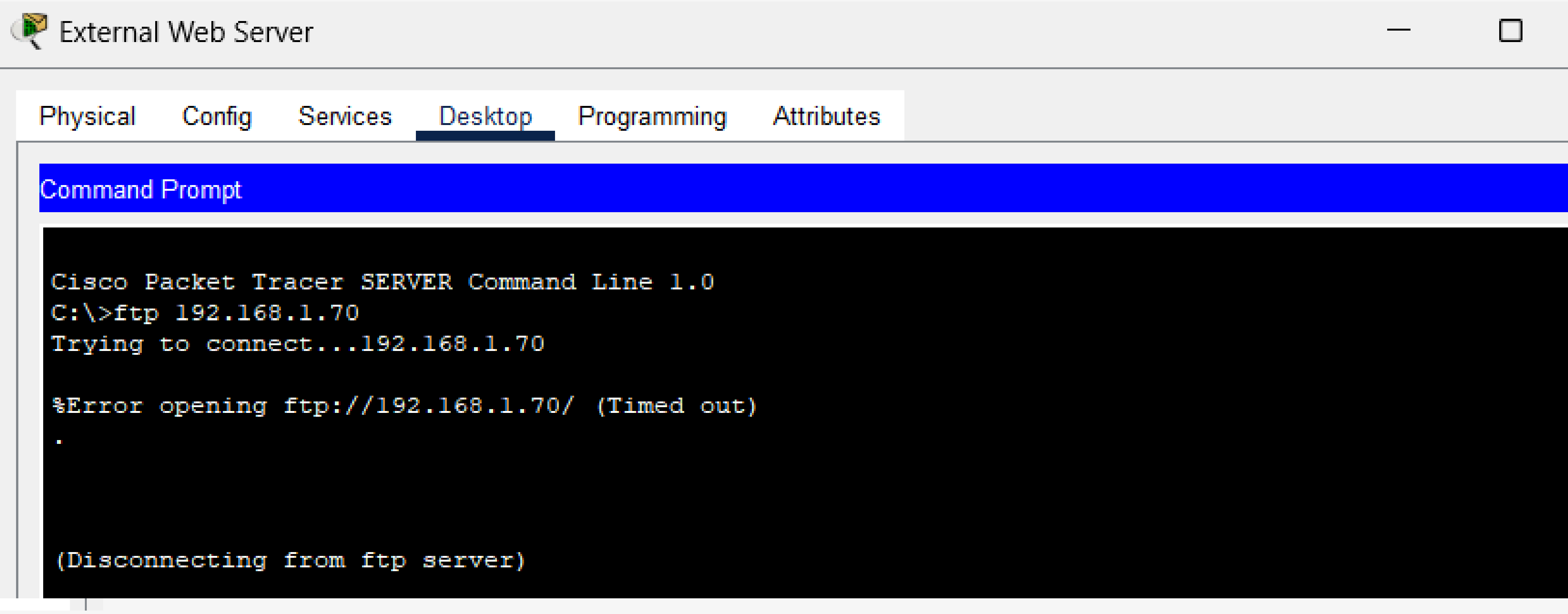


URL http://192.168.1.70

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image



```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ftp 192.168.1.70
Trying to connect...192.168.1.70

%Error opening ftp://192.168.1.70/ (Timed out)
.



(Disconnecting from ftp server)
```

CONCLUSION

- **Key Takeaways**:
  - Successfully configured ACLs provide a **layered security approach** in managing access between different network segments.
  - ACLs ensured that **specific traffic types** (e.g., FTP and ICMP) were blocked based on security requirements while allowing other legitimate communications.
  - **Validation** through connectivity tests confirmed that the ACL rules were applied correctly, securing the network.
- **Future Considerations**:
  - **Additional Adjustments**: Further improvements could involve blocking **unused ports** and **additional protocols** to enhance security.
  - Regular **review and updates** to ACL rules are essential to adapt to evolving security threats.

THANK YOU