

ASSIGNMENT

COURSE	Networking Fundamentals	ASSIGNMENT NO	9
MODULE	ACL	ASSIGNMENT DATE	2/09/2024
STUDENT NAME	Konganti Chaithanya kumar	SUBMISSION DATE	2/09/2024

Q1. What are types of ACL and their uses?

Ans: 1. Standard ACLs

- Uses:
 - Permit or deny traffic based on source IP address: Standard ACLs filter traffic by looking at the source IP address of packets.
 - Applied closest to the destination: Because they only filter by source IP, they are usually applied to the interface closest to the destination to prevent unwanted traffic from traversing the network.
- Limitations:
 - No granularity: Since standard ACLs only consider the source IP, they can't distinguish between different types of traffic from the same IP address.
- Example:
 - plaintext
 - access-list 10 permit 192.168.1.0 0.0.0.255
 - interface GigabitEthernet0/1
 - ip access-group 10 in

2. Extended ACLs

- Uses:

- Permit or deny traffic based on multiple criteria: Extended ACLs can filter traffic based on source and destination IP addresses, port numbers, protocols (TCP, UDP, ICMP, etc.), and even more specific conditions.
- Greater control and flexibility: Extended ACLs provide finer control over traffic by allowing you to specify exactly what types of traffic are allowed or denied.
- Applied closest to the source: Since extended ACLs are more specific, they are usually applied to the interface closest to the source of the traffic to prevent unwanted traffic from even entering the network.
- Example:
 - plaintext
 - access-list 100 permit tcp 192.168.1.0 0.0.0.255 172.16.0.0 0.0.0.255 eq 80
 - access-list 100 deny ip any any
 - interface GigabitEthernet0/1
 - ip access-group 100 in

Other Specialized ACL Types

- Named ACLs: Both standard and extended ACLs can be named, which makes them easier to manage and modify.
- Dynamic ACLs (Lock-and-Key ACLs): These ACLs require users to authenticate before allowing access. Once authenticated, temporary entries are created in the ACL to allow traffic.
- Reflexive ACLs: These are used for session filtering, where the ACL dynamically adjusts to allow return traffic based on sessions initiated from inside the network.
- Time-Based ACLs: These ACLs are configured to allow or deny traffic based on the time of day or day of the week.

Use Cases:

- Network Security: Blocking unauthorized access to sensitive network segments.

- Traffic Filtering: Controlling which types of traffic are allowed through a router.
- Network Performance: Preventing unnecessary traffic from consuming bandwidth by blocking it before it enters the network.

Q2. You are promoted as Security Engineer of your organisation and the CSO wants to take responsibility of configuring the ACL on your Router for both in/out bound traffic.



Configure the following ACL's

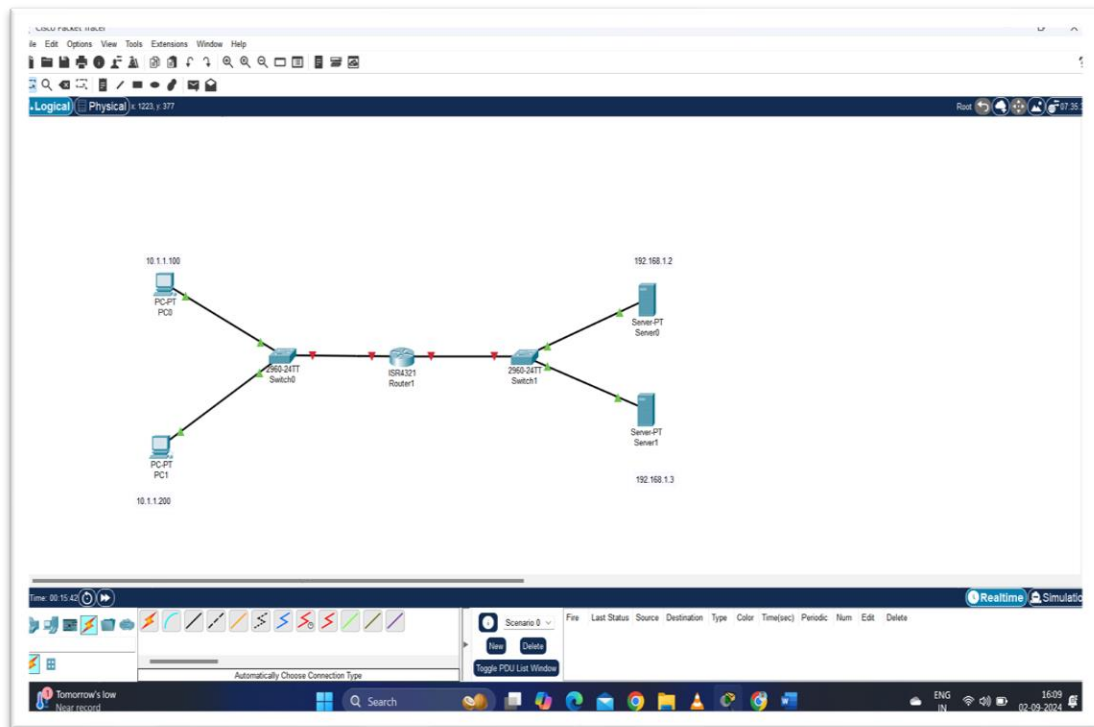
- (a) Permit traffic From PC A to server 1 but not to server 2
- (b) Permit PC B traffic to server 2 but only via http, do not permit PC B traffic to server 1

(c) Deny only ping from PC B to server 2

Solution:

1. Draw the Network and show the topology in Packet Tracer

“Attach the screenshot of Topology”



2. Check the connectivity and note down the observations

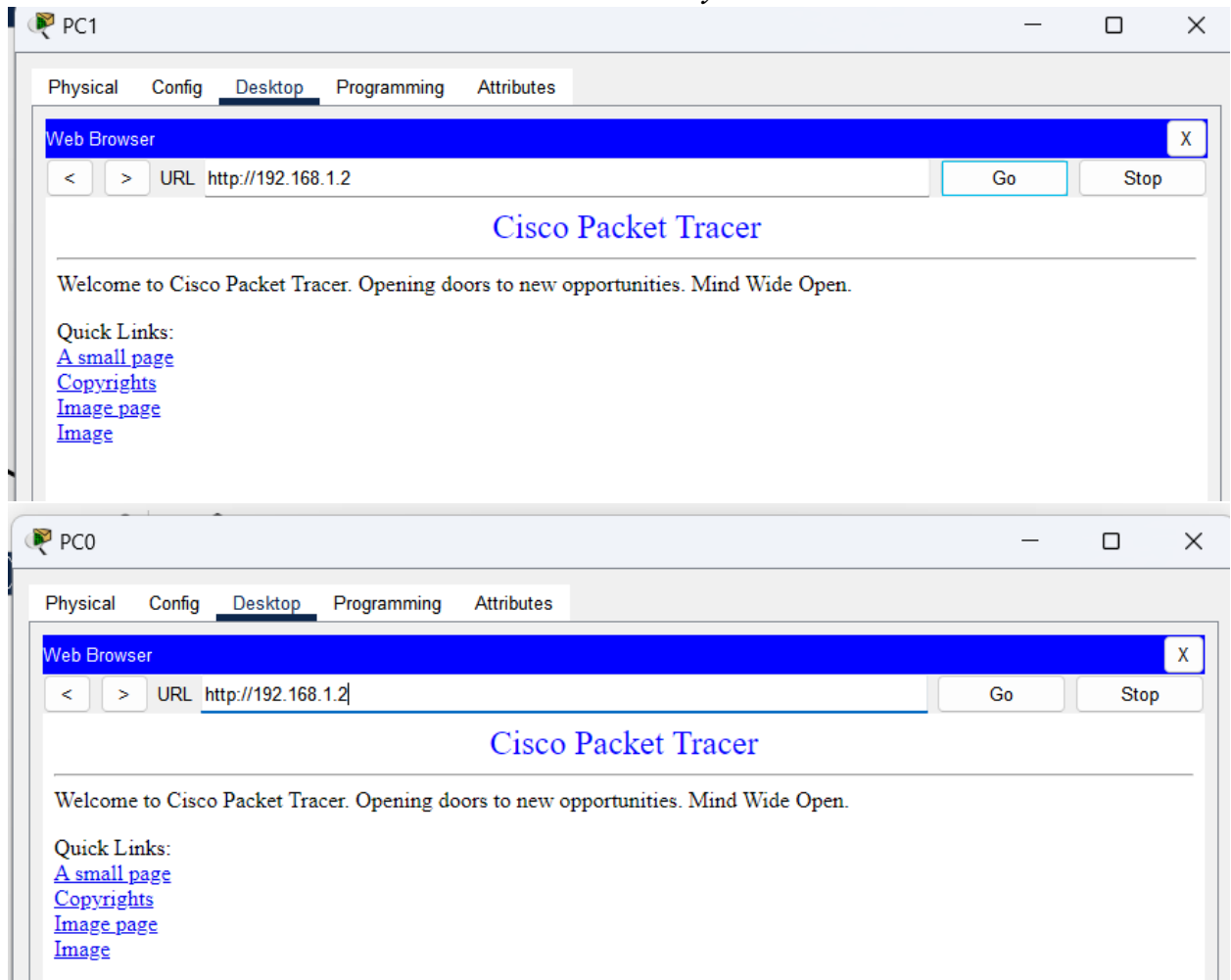
Test an connectivity between the devices before configuring the ACLs. Ping from PC A to Server 1, PC A to Server 2, PC B to Server 1, and PC B to Server 2.

Observations:

- **Before ACL Configuration:**
 - PC A should be able to ping Server 1 and Server 2.

- PC B should be able to ping Server 1 and Server 2.
- **After ACL Configuration:**
 - PC A should be able to ping Server 1 but not Server 2.
 - PC B should be able to access Server 2 via HTTP but not ping or access Server 1.
 - PC B should not be able to ping Server 2.

Attach the screenshot and note down your observations”



PC0

Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time=17ms TTL=127

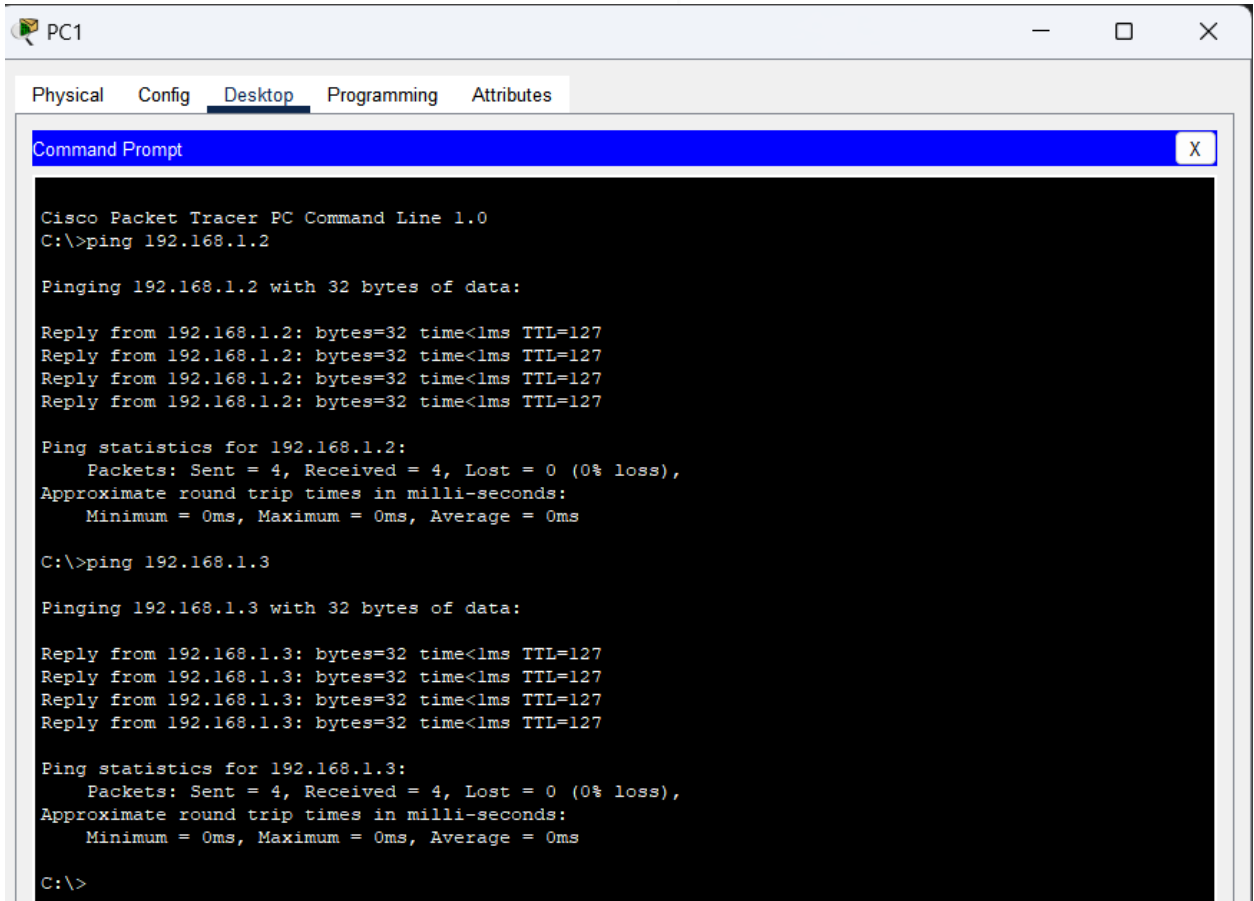
Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 17ms, Average = 4ms

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=127
Reply from 192.168.1.3: bytes=32 time<1ms TTL=127
Reply from 192.168.1.3: bytes=32 time<1ms TTL=127
Reply from 192.168.1.3: bytes=32 time=19ms TTL=127

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 19ms, Average = 4ms
```



The screenshot shows a Cisco Packet Tracer PC Command Line window for PC1. The window has tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, showing a Command Prompt window. The Command Prompt displays the output of two ping commands: one to 192.168.1.2 and another to 192.168.1.3. Both pings are successful, showing 4 packets sent and received with 0% loss. The ping statistics for both destinations show a minimum, maximum, and average round trip time of 0ms.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=127
Reply from 192.168.1.3: bytes=32 time<1ms TTL=127
Reply from 192.168.1.3: bytes=32 time<1ms TTL=127
Reply from 192.168.1.3: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

3. Go to Router and do the following configuration

Go to Router >>CLI Press ENTER

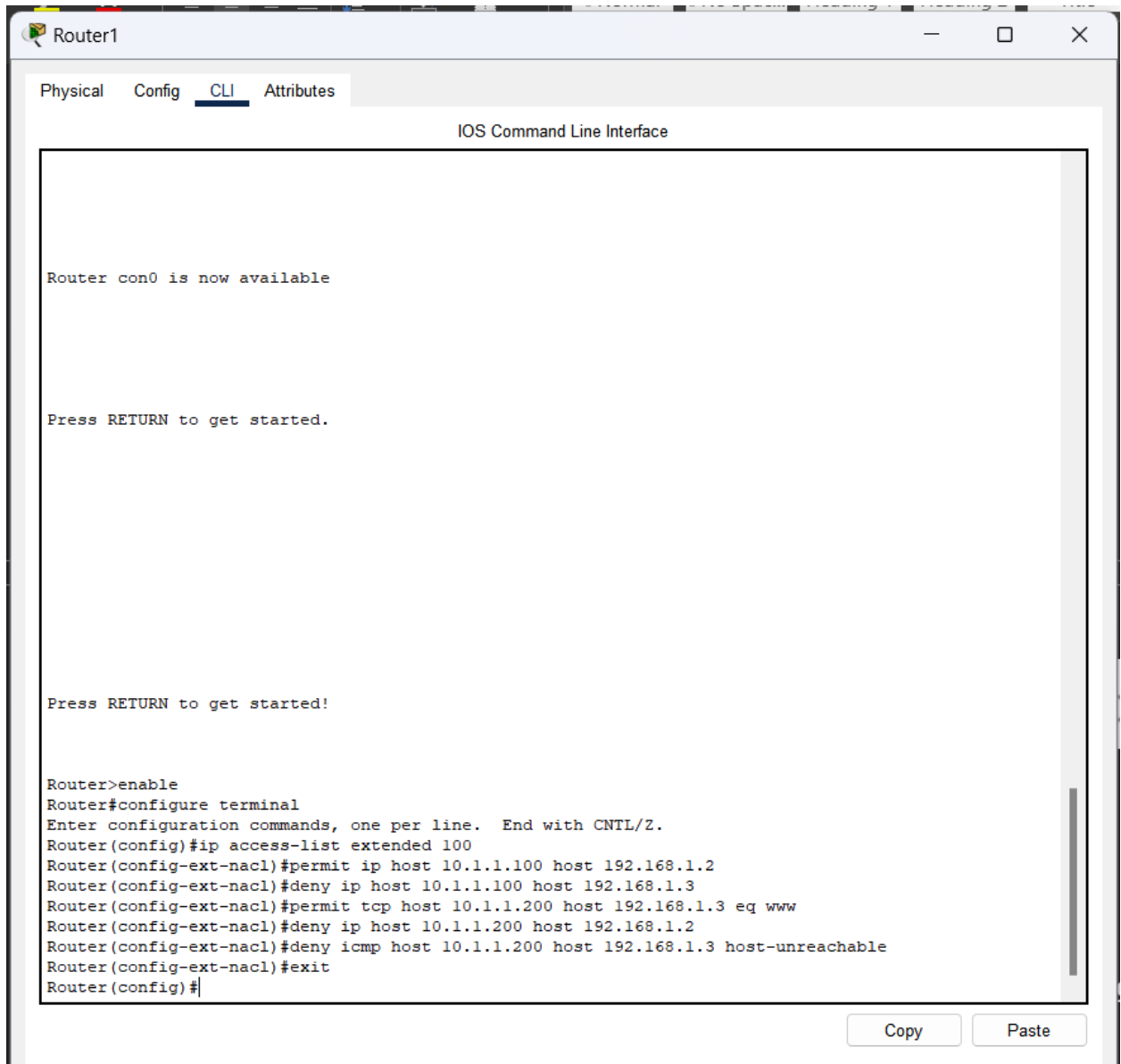
R1(config)# ip access-list extended 100

R1(config-ext-nacl)# permit ip host 10.1.1.100 host 192.168.1.2

R1(config-ext-nacl) # permit tcp host 10.1.1.200 host 192.168.1.3 eq www

R1(config-ext-nacl) # deny icmp host 10.1.1.200 host 192.168.1.3 host-unreachable

“Attach the screenshot of Router Configuration”



The screenshot shows a web-based interface for a router named 'Router1'. It has tabs for 'Physical', 'Config', 'CLI' (selected), and 'Attributes'. The main area is titled 'IOS Command Line Interface'. It displays the following text:

```
Router con0 is now available

Press RETURN to get started.

Press RETURN to get started!

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip access-list extended 100
Router(config-ext-nacl)#permit ip host 10.1.1.100 host 192.168.1.2
Router(config-ext-nacl)#deny ip host 10.1.1.100 host 192.168.1.3
Router(config-ext-nacl)#permit tcp host 10.1.1.200 host 192.168.1.3 eq www
Router(config-ext-nacl)#deny ip host 10.1.1.200 host 192.168.1.2
Router(config-ext-nacl)#deny icmp host 10.1.1.200 host 192.168.1.3 host-unreachable
Router(config-ext-nacl)#exit
Router(config)#
```

At the bottom right, there are 'Copy' and 'Paste' buttons.

Check the router configuration using following

R1# show access-list

```
Router#show access-list
Extended IP access list 100
 10 permit ip host 10.1.1.100 host 192.168.1.2
 20 deny ip host 10.1.1.100 host 192.168.1.3
 30 permit tcp host 10.1.1.200 host 192.168.1.3 eq www
 40 deny ip host 10.1.1.200 host 192.168.1.2
 50 deny icmp host 10.1.1.200 host 192.168.1.3 host-unreachable

Router#
```

“Attach the screenshot of Result”

4. **Establish the connectivity by sending ping packets from one Network to another and check the access-list functionality**

“Attach the screenshot of your findings”

