



**FACULTY OF ENGINEERING AND
TECHNOLOGY SRM INSTITUTE OF SCIENCE
AND TECHNOLOGY**

Kattankulathur, Chengalpattu District

NOVEMBER 2022

In partial fulfilment for the Course

of

18CSC381T- CRYPTOGRAPHY

MINI PROJECT REPORT

On

“Access Control List”

Submitted by

Gokul MK(RA2011030010023)

Adhin Jibil (RA2011030010031)

Shanthosh Sivan S (RA2011030010044)

Under the Guidance of

DR.J.Prabakaran

INDEX

S. No.	Topic	Page no.
1.1	Introduction-ACL	3
1.2	Network Design	4
1.3	ACL Commands	5
1.4	Result	8
1.5	Conclusion	9

INTRODUCTION

Access Control Lists (ACL) are very powerful security feature of Cisco IOS. By using Access Control Lists (ACL), we can deny unwanted access to the network while allowing internal users appropriate access to necessary services. Access Control Lists (ACL) are a set of commands, grouped together (by a number or name), that are used to filter traffic entering or leaving an interface. Access Control Lists (ACL) commands define which traffic is permitted and which is denied.

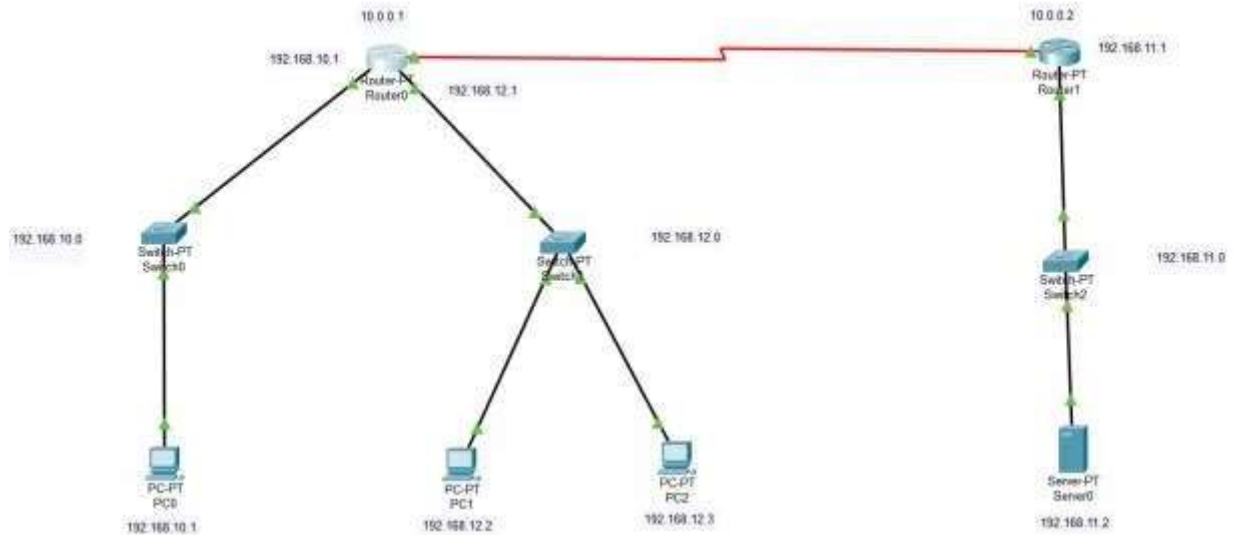
We have already discussed that an Access Control Lists (ACL) is a group of statements that define whether packets are accepted or rejected coming into an interface or leaving an interface. Access Control Lists (ACL) statements operate in sequential, logical order. If a condition match is true, the packet is permitted or denied and the rest of the Access Control Lists (ACL) statements are not checked. If all the Access Control Lists (ACL) statements are unmatched, an implicit "deny any" statement is placed at the end of the list by default. Access list statements operate in sequential, logical order and they evaluate packets from the top down. Once there is an access list statement match, the packet skips the rest of the statements. If a condition match is true, the packet is permitted or denied. You should remember that there is an implicit "deny any" at the end of every Access Control Lists (ACL).

We can classify Access Control Lists (ACL) as

- Numbered and Named Access Control Lists (ACL): A Numbered ACL is assigned a unique number among all Access Control Lists (ACL), but a Named Access Control Lists (ACL) is identified by a unique name.
- Standard and Extended Access Control Lists (ACL): Standard IP Access Control Lists (ACL) can be used filter traffic only based on the source IP address of the IP datagram packet. An extended Access Control Lists (ACL) can be used to filter traffic based on Source IP address, Destination IP address, Protocol (TCP, UDP etc), Port Numbers etc.

NETWORK DESIGN

The following is the network design.



It consists of 4 networks:

First network : 192.168.10.0

Second Network: 10.0.0.0

Third Network: 192.168.11.0

Fourth Network: 192.168.12.0

Device	Interface	Ip Address
PC0	Fa0/0	192.168.10.2
PC1	Fa0/0	192.168.11.2
PC2	Fa0/0	192.168.11.3
Server0	Fa0/0	192.168.12.2
Router 3	FastEthernet 0/0	192.168.10.1
Router 3	Serial0/0/0	10.0.0.1

Router 3	FastEthernet	192.168.11.1
Router 2	FastEthernet 0/0	192.168.12.1
Router 2	Serial0/0/0	10.0.0.2

4

ACL Commands

Physical
Config
CLI
Attributes

IOS Command Line Interface

```

Router(config-if)#ip access-group 10 out
Router(config-if)#exit
Router(config)#
Router(config)#
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet1/0
Router(config-if)#ip address 192.168.12.1 255.255.255.0
Router(config-if)#ip address 192.168.12.1 255.255.255.0
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 10 deny 192.168.12.0 0.0.0.255
Router(config)#access-list 10 permit any
Router(config)#interface se2/0
Router(config-if)#ip access-group 10 out
Router(config-if)#exit
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#

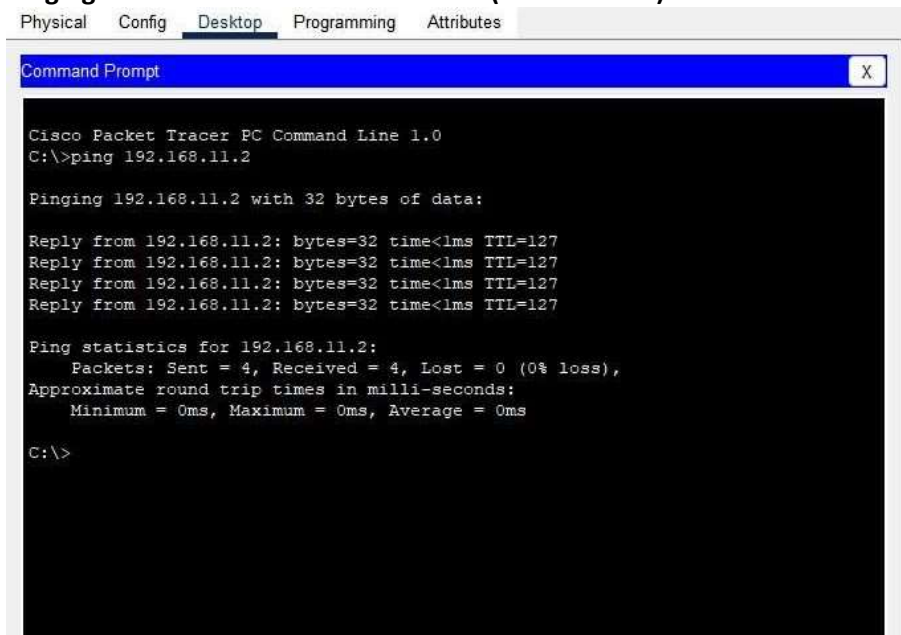
```

Ctrl+F6 to exit CLI focus
Copy
Paste

☐ Top

OUTPUT:

Pinging server from Permitted Network (192.168.10.0):



The screenshot shows a Cisco Packet Tracer PC Command Line window with tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active. The command prompt shows the following output:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.11.2

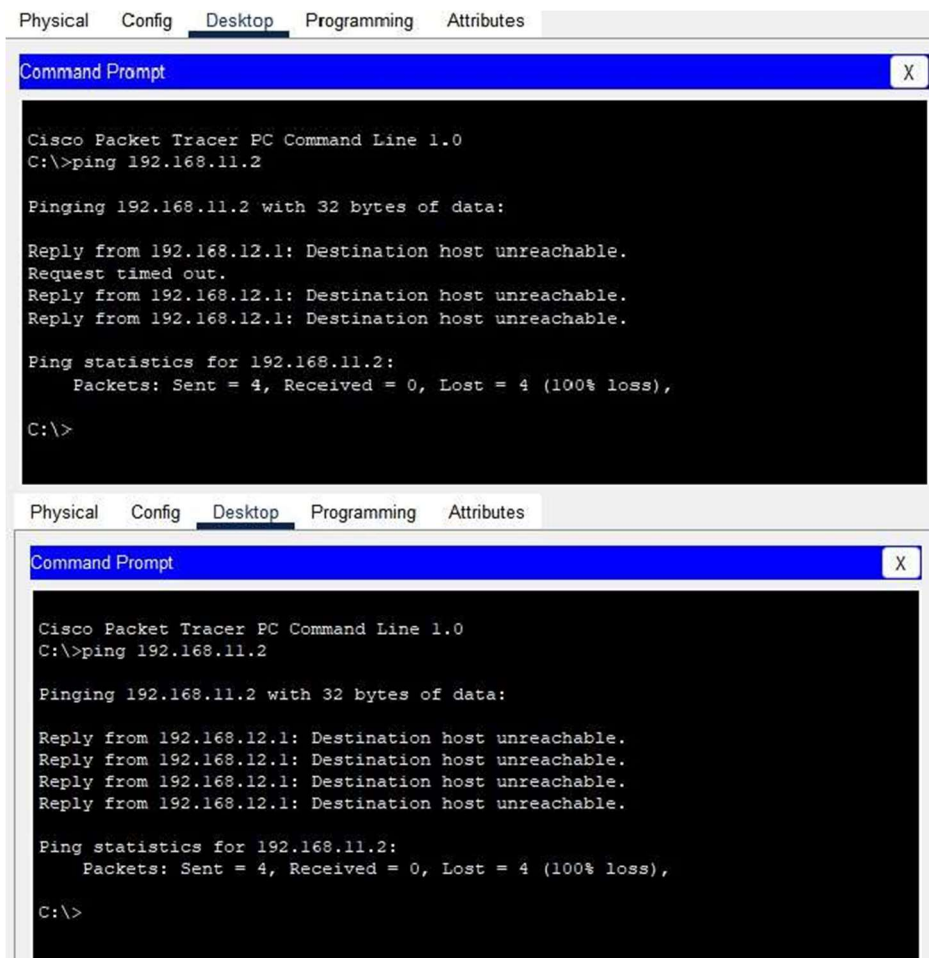
Pinging 192.168.11.2 with 32 bytes of data:

Reply from 192.168.11.2: bytes=32 time<1ms TTL=127
Reply from 192.168.11.2: bytes=32 time<1ms TTL=127
Reply from 192.168.11.2: bytes=32 time<1ms TTL=127
Reply from 192.168.11.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.11.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Pinging server from Denied Network (192.168.12.0):



The first screenshot shows a Cisco Packet Tracer PC Command Line window with tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active. The command prompt shows the following output:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.11.2

Pinging 192.168.11.2 with 32 bytes of data:

Reply from 192.168.12.1: Destination host unreachable.
Request timed out.
Reply from 192.168.12.1: Destination host unreachable.
Reply from 192.168.12.1: Destination host unreachable.

Ping statistics for 192.168.11.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

The second screenshot shows the same Cisco Packet Tracer PC Command Line window with the same output as the first screenshot.

Result: Numbered Access Control List has been implemented on PC0.

CONCLUSION

Access control lists are used for controlling permissions to a computer system or computer network. They are used to filter traffic in and out of a specific device. Those devices can be network devices that act as network gateways or endpoint devices that users access directly.

After implementing Access control on Router for PC0 we can see that PC0 is not being able to connect to the server. The permission is being denied by the gateway router which is not passing any packets that are sent by PC0. On the other hand, all the other PCs are able to communicate with server because they have been allowed on the network.

Access Control List is a great way to filter out traffic in and out of a device or a network. This method provides security by filtering out unwanted traffic and devices from the network.