

Computer Networks Lab 06

Course: Computer Networks (CL3001)

Instructor: Sameer Faisal

Semester: Spring 2025

T.A: N/A

Note:

- Maintain discipline during the lab.
 - Listen and follow the instructions as they are given.
 - Just raise hand if you have any problem.
 - Completing all tasks of each lab is compulsory.
 - Get your lab checked at the end of the session.
-

Lab Objective

- Introduction to ACL & configuration of ACL in Cisco Packet Tracer.

1. Introduction to Access Control List (ACL)

Computer Networks

CL3001

LAB – 06(B)

ACL (Standard + Extended)

NATIONAL UNIVERSITY OF COMPUTER AND EMERGING SCIENCES,
KARACHI CAMPUS
FAST SCHOOL OF COMPUTING (AI & DS, CS, CY, SE)
SPRING 2025

Access-list (ACL) is a set of rules defined for controlling network traffic and reducing network attacks. ACLs are used to filter traffic based on the set of rules defined for the incoming or outgoing of the network. ACLs are mainly found in network devices with packet filtering capabilities including routers and switches.

Different ACLs have different working mechanisms based on what they do. For File system ACLs, they work by creating tables that inform the operating system of access privileges given for certain system subjects. Each object has a unique security property that acts as an identification factor in its access control list. Some privileges include read/write privileges, file execution, and several others.

Some popular operating systems utilizing this mechanism include Unix-based systems, Windows NT/2000, and Novell's Netware.

In the case of Networking ACLs, they are installed in networking devices (Routers and switches) with the sole purpose of filtering traffic. This is done by using pre-defined rules that decided which packets transferred. Source and destination IP addresses also play a major role in this decision.

Packet filtering improves network security by decreasing network traffic access, restricting device and user access to the involved network.

Access lists are sequential, and are made up of two major components; permit and deny statements. A name and a number are used to identify access lists.

Features of ACL

1. The set of rules defined are matched serial wise i.e. matching starts with the first line, then 2nd, then 3rd, and so on.
2. The packets are matched only until it matches the rule. Once a rule is matched then no further comparison takes place and that rule will be performed.
3. There is an implicit denial at the end of every ACL, i.e., if no condition or rule matches then the packet will be discarded.

Once the access-list is built, then it should be applied to inbound or outbound of the interface.

Inbound access lists

When an access list is applied on inbound packets of the interface then first the packets will be processed according to the access list and then routed to the outbound interface.

Outbound access lists

When an access list is applied on outbound packets of the interface then first the packet will be routed and then processed at the outbound interface.

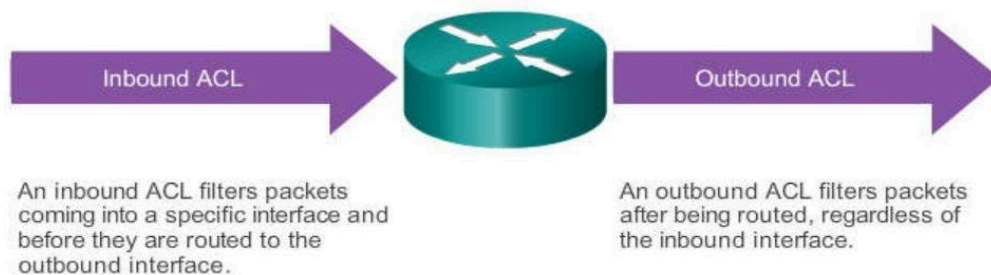


Figure 1

Types of ACL

1. **Standard ACL:** These are the Access-list that are made using the source IP address only. These ACLs permit or deny the entire protocol suite. They don't distinguish between the IP traffic such as TCP, UDP, HTTPS, etc. By using numbers 1-99 or 1300-1999, the router will understand it as a standard ACL and the specified address as the source IP address.
2. **Extended ACL:** These are the ACL that uses source IP, Destination IP, source port, and Destination port. These types of ACL, we can also mention which IP traffic should be allowed or denied. These use range 100-199 and 2000-2699.
3. **Reflexive ACL:** Also known as IP session ACLs, Reflective ACLs use upper-layer session details to filter traffic.
4. **Dynamic ACL:** As the term suggests, Dynamic ACLs are reliable on extended ACLs, Telnet, and authentication. They grant users access to a resource only if the user authenticates the device through telnet.

Also, there are two categories of access-list:

- **Numbered Access-List:** These are the access list that cannot be deleted specifically once created i.e., if we want to remove any rule from an Access-list then this is not permitted in the case of the numbered access list. If we try to delete a rule from the access list, then the whole access list will be deleted. The numbered access-list can be used with both standard and extended access lists.
- **Named Access-List:** In this type of access list, a name is assigned to identify an access list. It is allowed to delete a named access list, unlike numbered access list. Like numbered access lists, these can be used with both standards and extended access lists.

Advantages of ACL

- Improve network performance.
- Provides security as the administrator can configure the access list according to the needs and deny the unwanted packets from entering the network.
- Provides control over the traffic as it can permit or deny according to the need of the network.

Rules of ACL

1. The standard Access-list is generally applied close to the destination (but not always).
2. The extended Access-list is generally applied close to the source (but not always).
3. We can assign only one ACL per interface per protocol per direction, i.e., only one inbound and outbound ACL is permitted per interface.
4. We can't remove a rule from an Access-list if we are using numbered Access-list. If we try to remove a rule, then the whole ACL will be removed. If we are using named access lists, then we can delete a specific rule.
5. Every new rule which is added to the access list will be placed at the bottom of the access list therefore before implementing the access lists, analyses the whole scenario carefully.
6. As there is an implicit deny at the end of every access list, we should have at least a permit statement in our Access-list otherwise all traffic will be denied.
7. Standard access lists and extended access lists cannot have the same name.

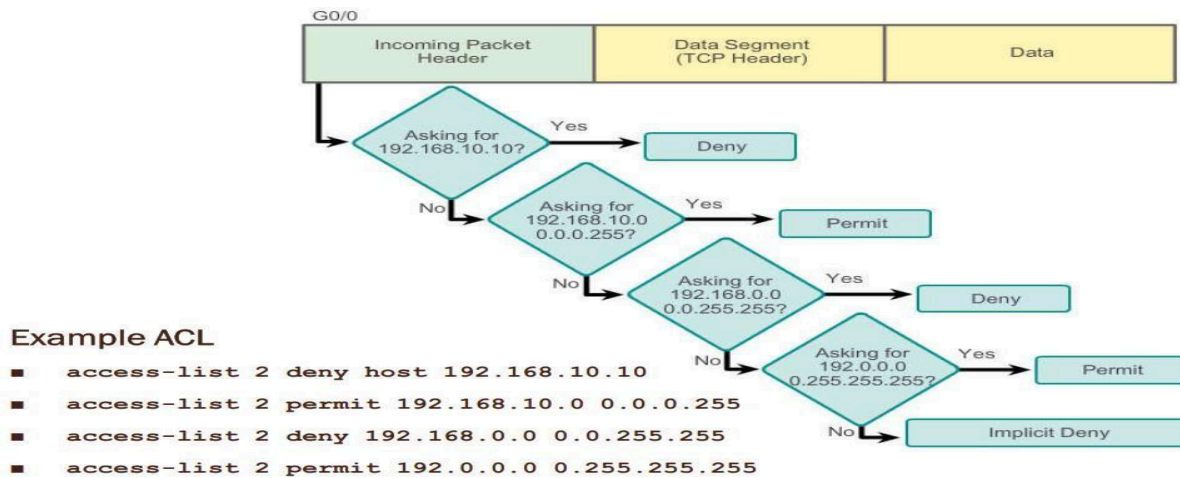


Figure 2

2. Implementation of Standard Access Control List (ACL)

Consider the topology given below:

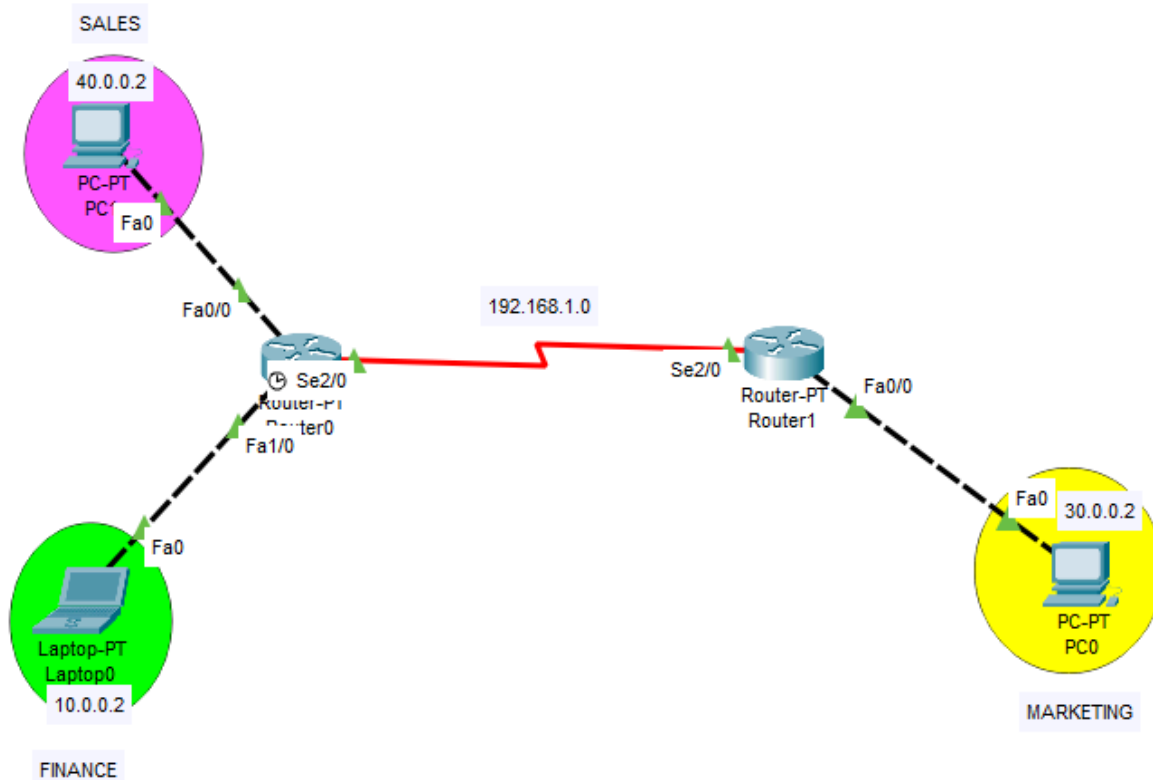


Figure 3

IP configuration on Router 0 (fa0/0):

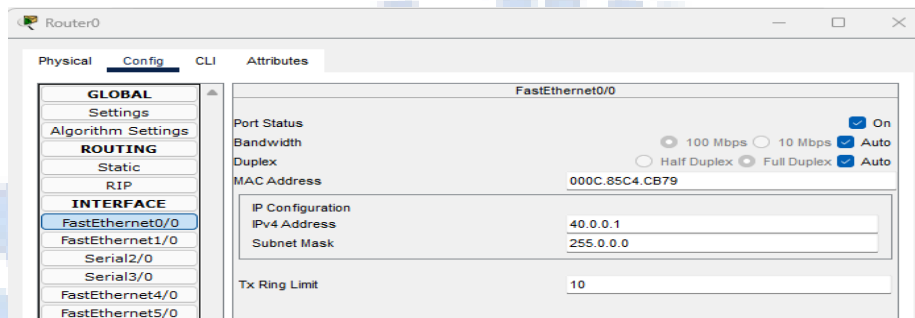


Figure 4

IP configuration on Router 0 (fa0/1):

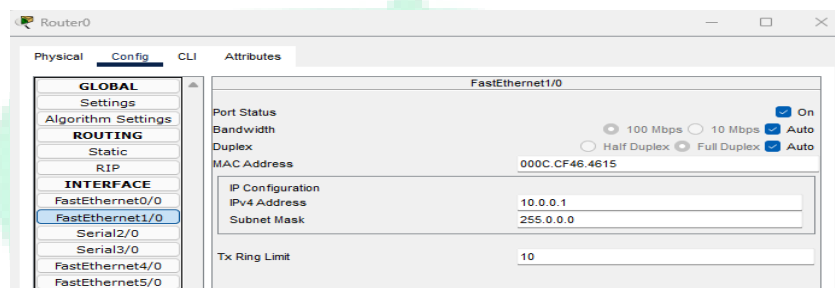


Figure 5

IP configuration on Router 0 (se2/0):

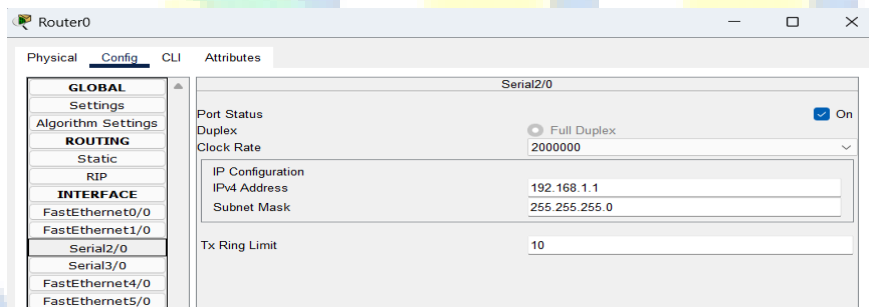


Figure 6

IP configuration on Router 1 (se2/0):

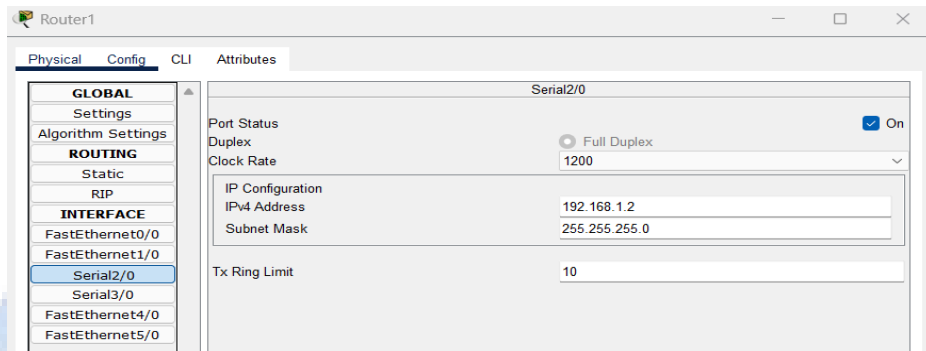


Figure 7

IP configuration on Router 1 (fa0/0):

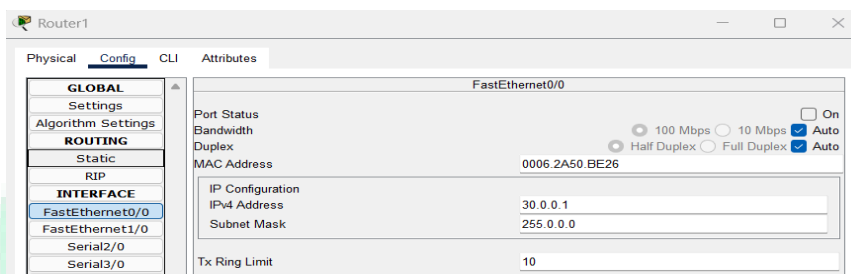


Figure 8

IP configuration on PC (SALES):

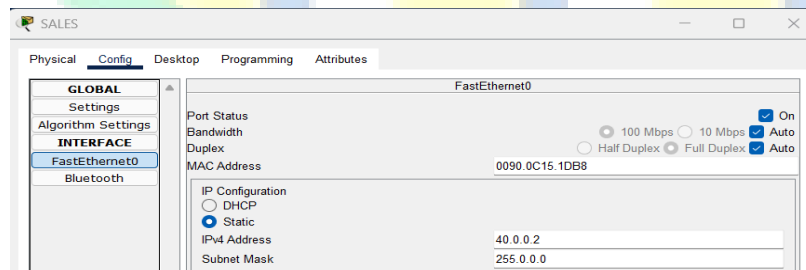


Figure 9

IP configuration on PC (FINANCE):

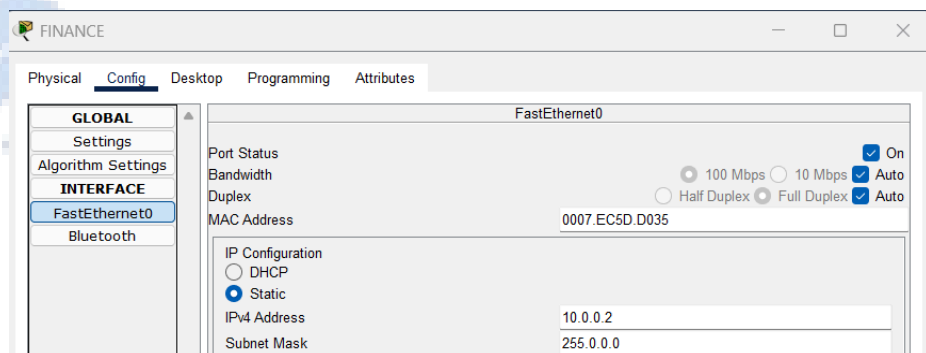


Figure 10

IP configuration on PC (MARKETING):

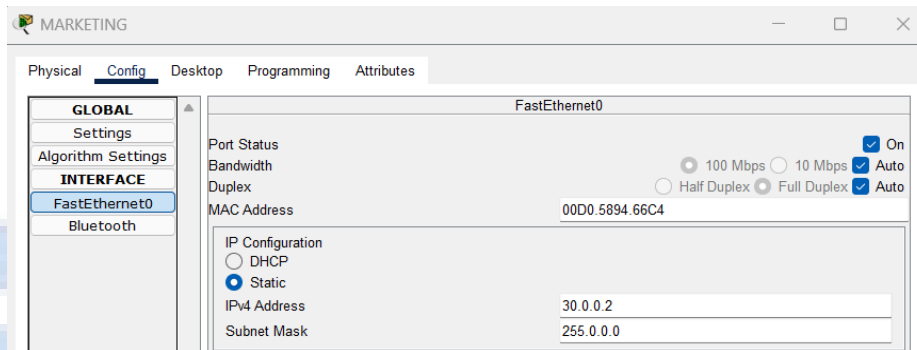


Figure 11

Configure static routing on both routers (specify serial port IPs in static routing):

Router 0:

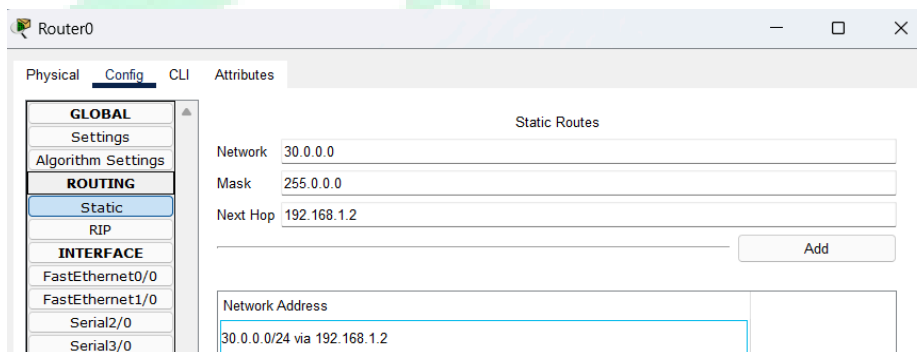


Figure 12

Router 1:

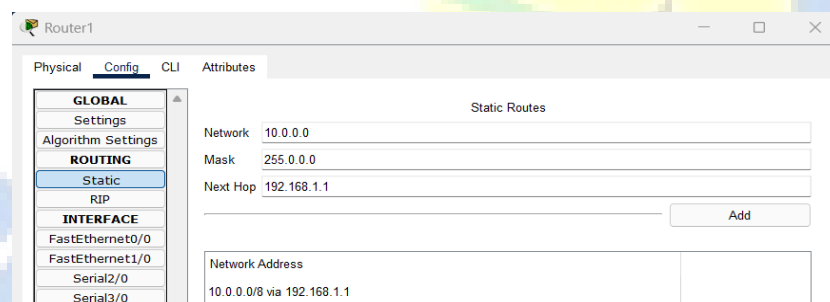


Figure 13

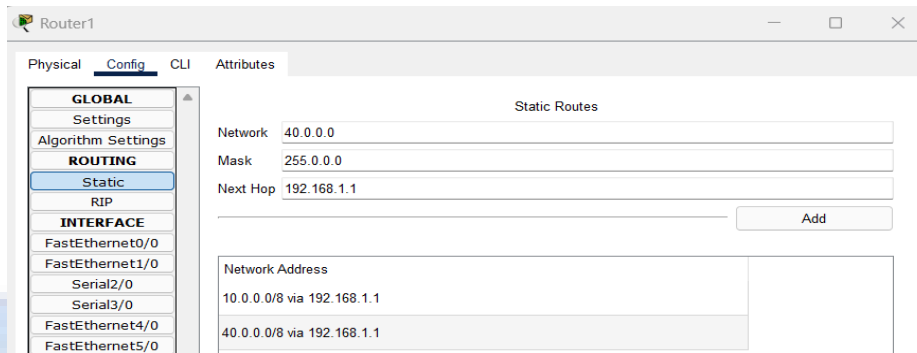


Figure 14

Now suppose we want to allow only one host address 10.0.0.2 255.0.0.0 (FINANCE) to send traffic out through serial2/0 port while blocking the other host 40.0.0.2 255.0.0.0 (SALES) to send from this port. To meet with this requirement, we need to create two ACL conditions (on router 0):

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 1 permit 10.0.0.2 0.0.0.0
Router(config)#access-list 1 deny 40.0.0.2 0.0.0.0

Router(config)#in se2/0
Router(config-if)#ip access-group 1 out
Router(config-if)#
```

Figure 30

Explanation:

- **access-list 1 permit 10.0.0.2 0.0.0.0:** This allows traffic only from the host 10.0.0.2.

You can also apply wildcard mask which specifies how much of the IP address should be matched.

- **10.0.0.2:** This is the IP address that we want to permit.
- **0.0.0.0:** This is the wildcard mask, meaning match exactly all bits of 10.0.0.2.

0.0.0.0 = Exact match (all bits must match).

255.255.255.255 = Ignore all bits (match anything).

In our above case, 0.0.0.0 means "all 32 bits must match exactly," so it allows traffic only from 10.0.0.2.

- **access-list 1 deny 40.0.0.2 0.0.0.0:** This blocks traffic only from the host 10.0.0.2.
- **ip access-group 1 out:** Applies the ACL in the outbound direction on Serial 2/0 of Router 0, filtering traffic leaving toward Router 1.

Standard ACL Syntax:

access-list <number 1-99> permit <source> <wildcard-mask>

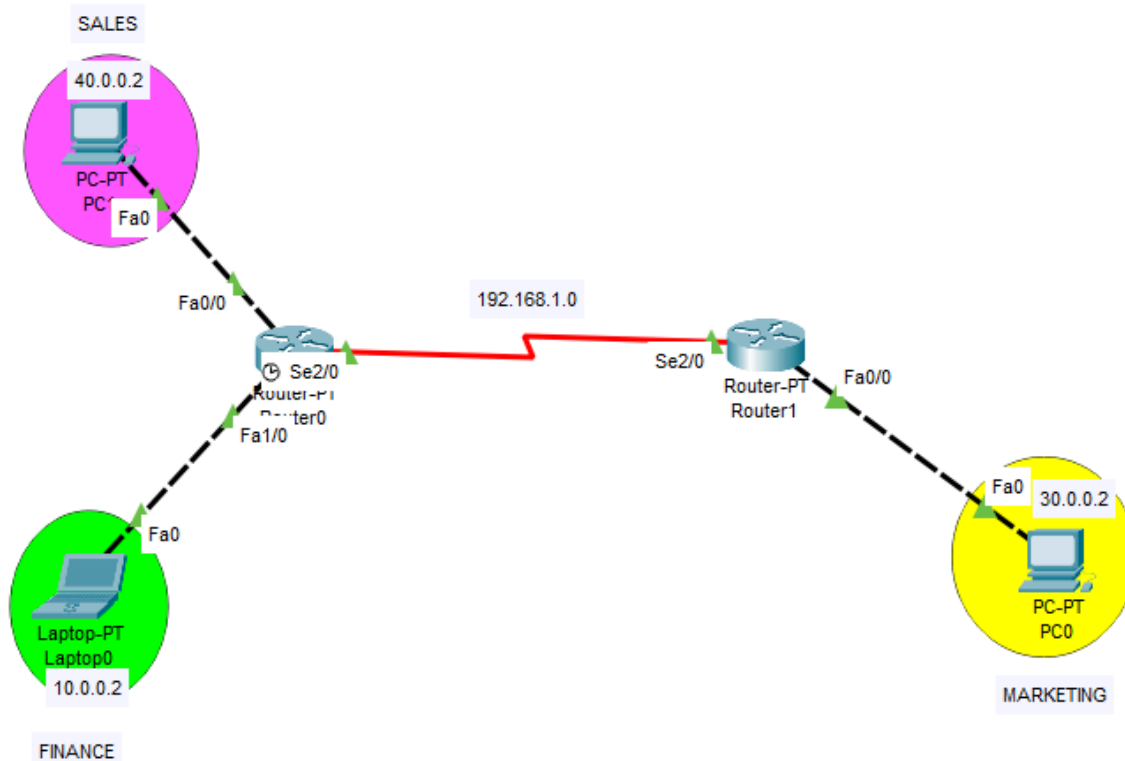
Verification of ACL Lists` Working:

```
Router#show access-lists
Standard IP access list 1
 10 permit host 10.0.0.2 (2 match(es))
 20 deny host 40.0.0.2 (2 match(es))
```

Figure 31

3. Implementation of Standard Access Control List (ACL)

Consider the topology given below:



All configurations for the above topology are provided in standard ACL.

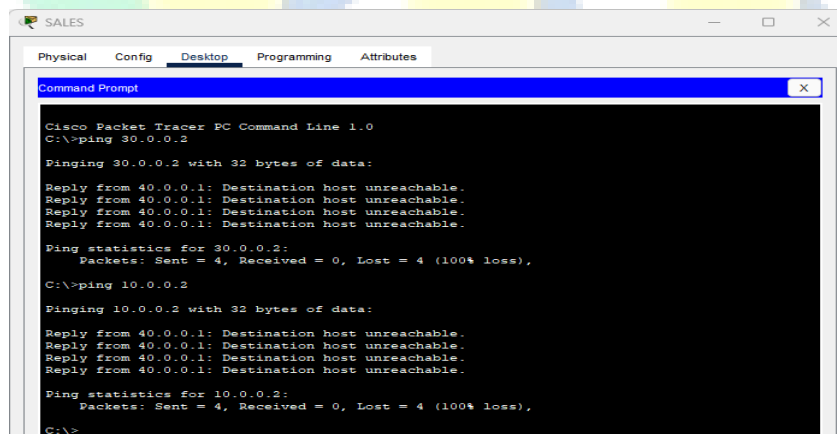
Extended ACL Syntax:

access-list <number 100-199> <permit | deny> <protocol> <source> <wildcard-mask>

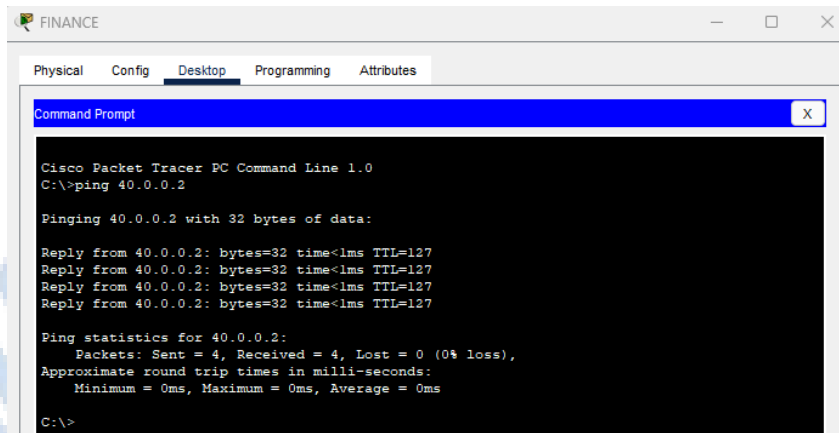
1. Block All ICMP (PING & Other Messages):

Suppose we want to block SALES to ping any other PCs (MARKETING & FINANCE). But, all other PCs must be allowed to ping SALES:

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 110 deny icmp host 40.0.0.2 any echo
Router(config)#access-list 110 permit icmp any host 40.0.0.2 echo-reply
Router(config)#access-list 110 permit ip any any
Router(config)#interface Se2/0
Router(config-if)#ip access-group 110 out
Router(config-if)#exit
Router(config)#interface Fa1/0
Router(config-if)#ip access-group 110 out
Router(config-if)#
```



As you can see, SALES is now unable to ping FINANCE & MARKETING. Now let's try pinging SALES from other hosts:



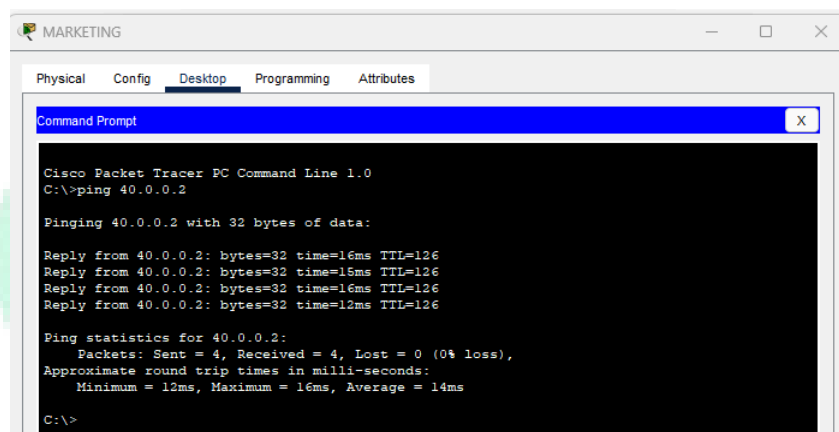
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 40.0.0.2

Pinging 40.0.0.2 with 32 bytes of data:

Reply from 40.0.0.2: bytes=32 time<1ms TTL=127
Reply from 40.0.0.2: bytes=32 time<1ms TTL=127
Reply from 40.0.0.2: bytes=32 time<1ms TTL=127
Reply from 40.0.0.2: bytes=32 time<1ms TTL=127

Ping statistics for 40.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 40.0.0.2

Pinging 40.0.0.2 with 32 bytes of data:

Reply from 40.0.0.2: bytes=32 time=16ms TTL=126
Reply from 40.0.0.2: bytes=32 time=16ms TTL=126
Reply from 40.0.0.2: bytes=32 time=16ms TTL=126
Reply from 40.0.0.2: bytes=32 time=12ms TTL=126

Ping statistics for 40.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 16ms, Average = 14ms

C:\>
```

All other hosts are now able to ping SALES.

2. Block a Whole Network:

Suppose we want to block the entire network of MARKETING (30.0.0.0/8) to be accessed from FINANCE:

```
Router>
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 120 deny ip 10.0.0.0 0.255.255.255 30.0.0.0 0.255.255.255
Router(config)#access-list 120 permit ip any any
Router(config)#int fa/0
Router(config-if)#ip access-group 120 out
Router(config-if)#
```

Ping from MARKETING to FINANCE Network (Successful):

```
C:\>ping 10.0.0.0

Pinging 10.0.0.0 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=3ms TTL=254
Reply from 192.168.1.1: bytes=32 time=1ms TTL=254
Reply from 192.168.1.1: bytes=32 time=2ms TTL=254
Reply from 192.168.1.1: bytes=32 time=1ms TTL=254

Ping statistics for 10.0.0.0:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 1ms

C:\>
```

Ping from FINANCE to MARKETING Network (Failed):

```
C:\>ping 30.0.0.0

Pinging 30.0.0.0 with 32 bytes of data:

Reply from 10.0.0.1: Destination host unreachable.
Reply from 10.0.0.1: Destination host unreachable.
Reply from 10.0.0.1: Destination host unreachable.
Reply from 10.0.0.1: Destination host unreachable.

Ping statistics for 30.0.0.0:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Lab Exercise – III

Implement the topology given below on cisco packet tracer:

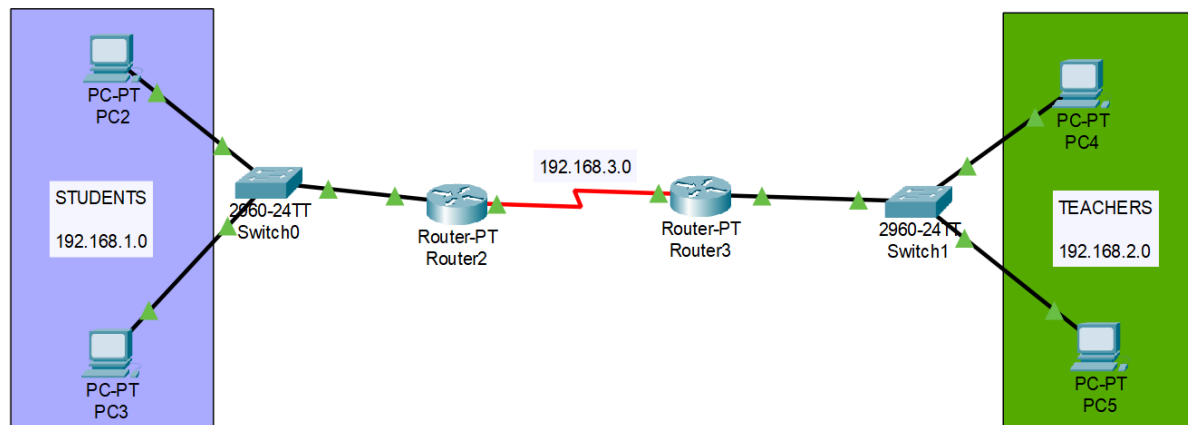


Figure 35

1. Prevent PCs in the STUDENTS network from communicating with any device in the TEACHERS network. But, TEACHERS should be able to communicate with the STUDENTS.
2. Only allow any one PC in the STUDENTS network (for example: as a CR communicates with teachers) to access and communicate with the TEACHERS network, blocking every other device in the STUDENTS network.