Computer Networks
CL3001

LAB - 06
Telnet, SSH, ACL (Standard)

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

Computer Networks Lab 06

Course: Computer Networks (CL3001) **Semester:** Spring 2025
Instructor: Sameer Faisal **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 Telnet & configuration of Telnet in Cisco Packet Tracer.
- Introduction to SSH & configuration of SSH in Cisco Packet Tracer.
- Introduction to ACL & configuration of ACL in Cisco Packet Tracer.

SSH & Telnet

1. Introduction to Telnet

A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network. To start a Telnet session, you must log in to a server by entering a valid username and password. Telnet is a common way to remotely control Web servers.
To telnet means to establish a connection with the Telnet protocol, either with command line client or with a programmatic interface.

2. Configuration of Telnet

Below are the steps for Telnet Protocol. Follow the procedure for the configuration of Telnet Protocol.
Step 1: Build the following topology.

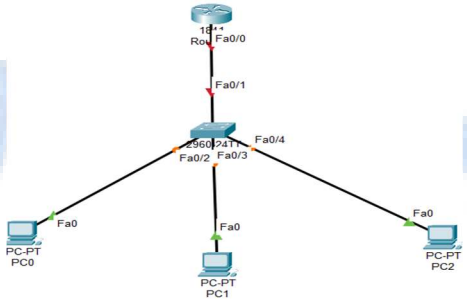

Figure 1

Step 2: Set IPs on the PCs. As, by default, all PCs are in vlan. We will create a virtual interface on switch with vlan 1 as follows:

```
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.1 255.255.255.0
Switch(config-if)#no shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
```

Figure 2

Assigning IP to PCs:

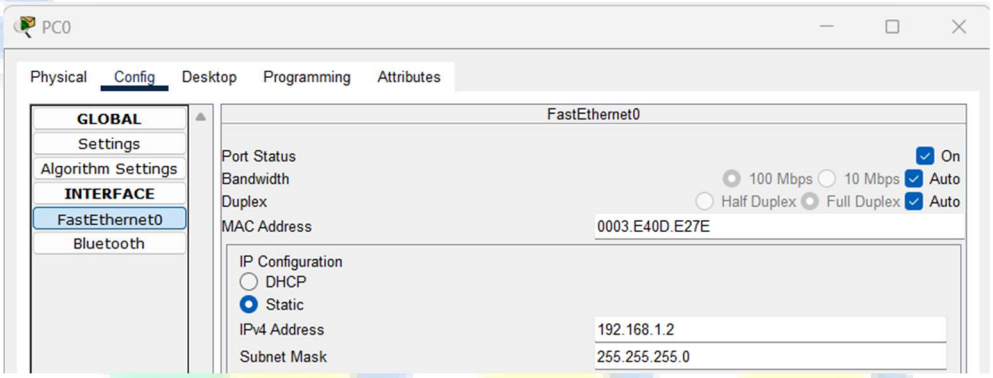

Figure 3

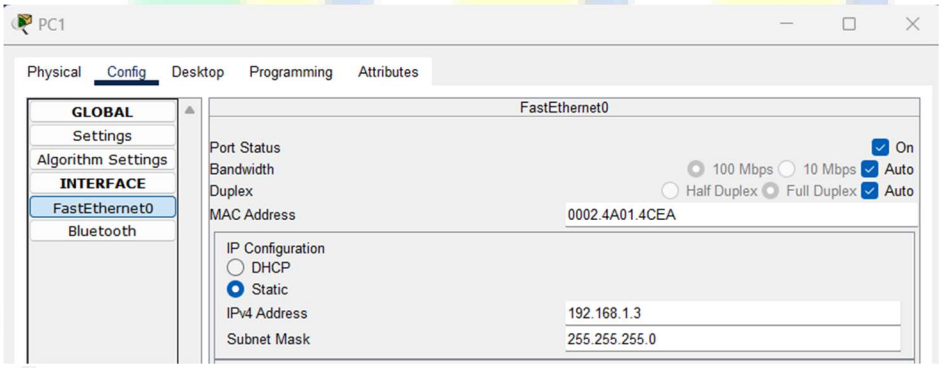

Figure 4

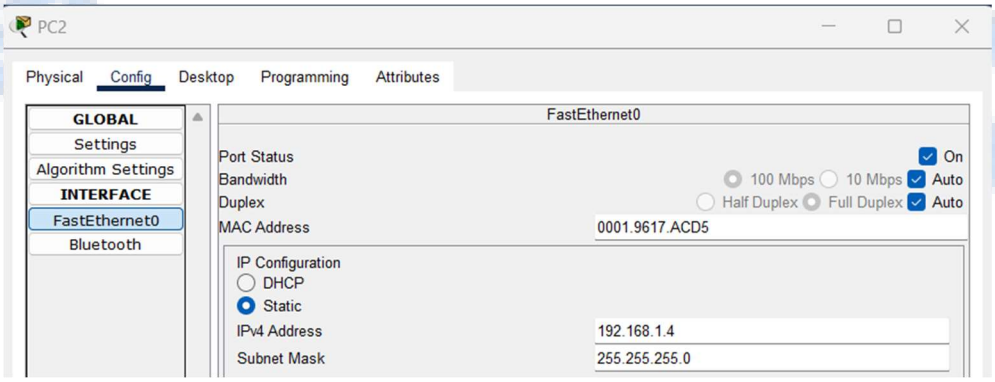

Figure 5

Step 3: Now, try to telnet the switch from our PC, it refuses because we have not applied authentication on the switch yet.

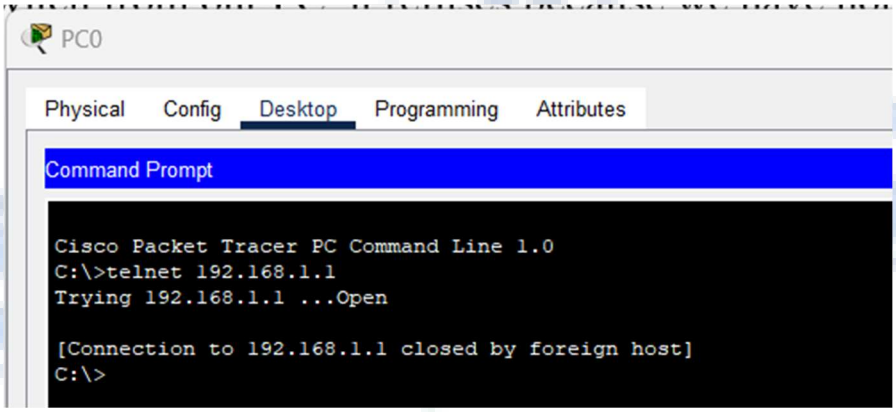

Figure 6

Secure Shell Server (SSH) and FTP services. Each Telnet, SSH, or FTP session requires one vty-line. You can add security to your system by configuring the software to validate login requests:

```
Switch(config-if)#exit
Switch(config)#line vty 0 15
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#
```

Figure 7

Now, we can easily telnet. But it does not let us go in the switch enabled mode because we have not set the password on the switch yet.

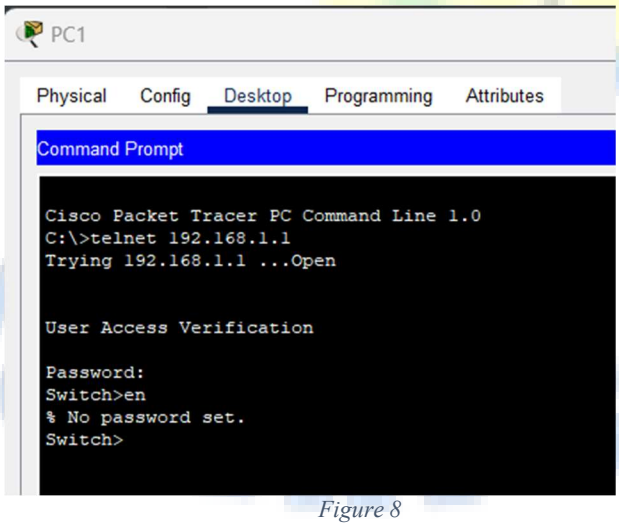

Figure 8

Let's apply password on the switch enabled mode.

```
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#enable password cs
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure 9

Now, we can go inside Switch configuration mode from our pc.

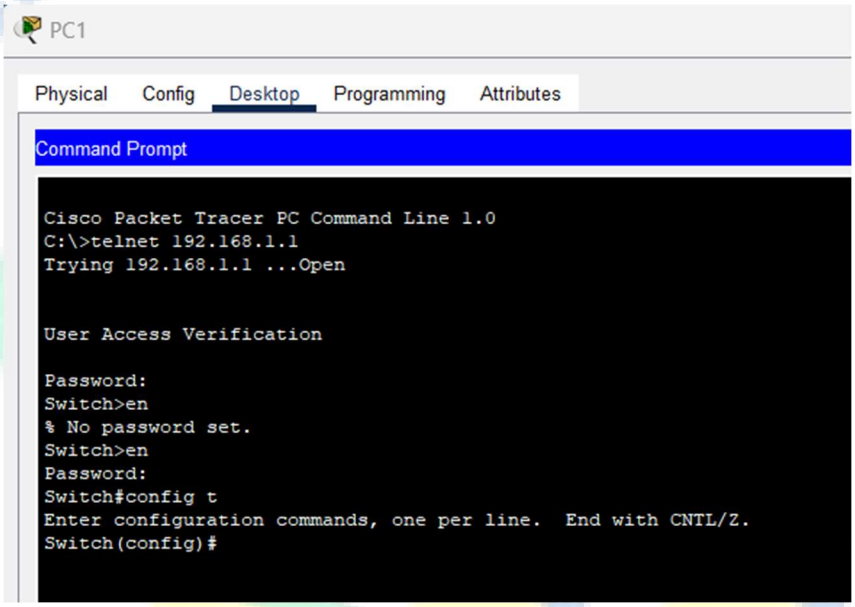

Figure 10

3. Introduction to SSH

Secure Shell or Secure Socket Shell is a network protocol. It is an application layer protocol that is in the 7th later of the Open Systems Interconnection (OSI) network model. It also refers to the suite of utilities that implements the SSH protocol.

Secure Shell also supports both password and key-based authentication. Password-based authentication let users provide username and password to authenticate to the remote server.

A key-based authentication allows users to authenticate through a key-pair. The key pairs are two cryptographically secure keys for authenticating a client to a Secure Shell server.

Furthermore, the Secure Shell protocol also encrypts data communication between two computers. It is extensively used to communicate with a remote computer over the Internet.

4. Configuration of SSH

Taking the same topology as mentioned in telnet.

Below are the steps for SSH Protocol. Follow the following procedure for the configuration of SSH Protocol.

```
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname sameer
sameer(config)#ip domain name ai-study
sameer(config)#crypto key generate rsa
The name for the keys will be: sameer.ai-study
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

sameer(config)#
```

Figure 11

```
sameer(config)#ip s
*Mar 1 0:29:49.71: %SSH-5-ENABLED: SSH 1.99 has been enabled
% Ambiguous command: "ip s"
sameer(config)#ip ssh version 2
sameer(config)#line vty 0 15
sameer(config-line)#transport input ssh
sameer(config-line)#
```

Figure 12

Protocol working on it. By default, username is admin. We can apply any sort of configuration on our switch from our PC.

```
C:\>ssh -l admin 192.168.1.1

Password:

Password:



sameer>en
Password:
sameer#config t
Enter configuration commands, one per line.  End with CNTL/Z.
sameer(config)#interface fa0/2
sameer(config-if)#no shutdown
sameer(config-if)#exit
sameer(config)#exit
sameer#
```

Figure 13

Now, if we want to change the username from admin to something else, we will do it as follows:

```
sameer(config)#username ds-study secret abc
sameer(config)#line vty 0 15
sameer(config-line)#login local
sameer(config-line)#
```

Figure 14

Now we will do the following on our PCs:

```
C:\>ssh -l ds-study 192.168.1.1

Password:
% Login invalid


Password:
% Login invalid


Password:



sameer>
```

Figure 15

5. Introduction to Access Control List (ACL)

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.

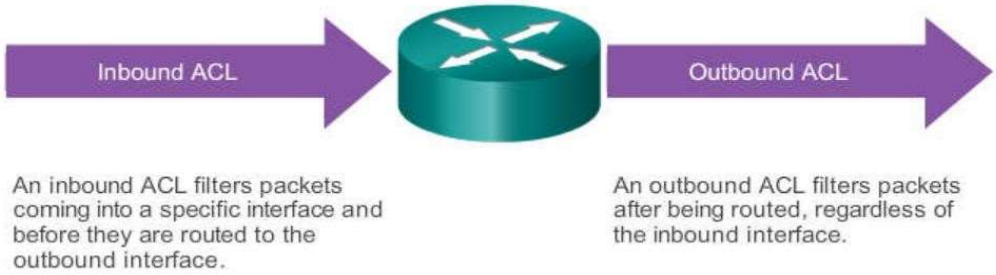

Figure 16

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.

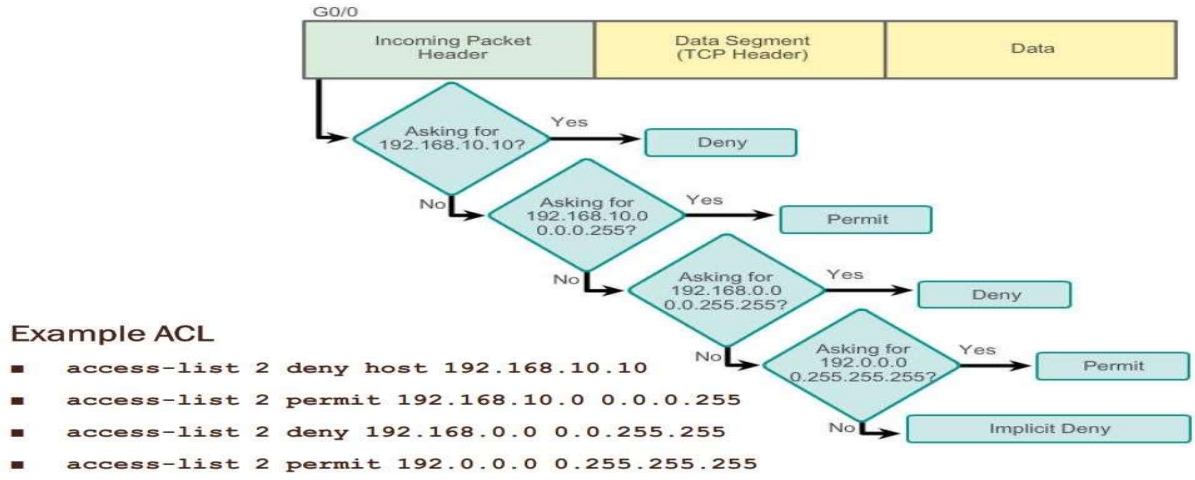

Figure 17

6. Implementation of Access Control List (ACL)

Consider the topology given below:

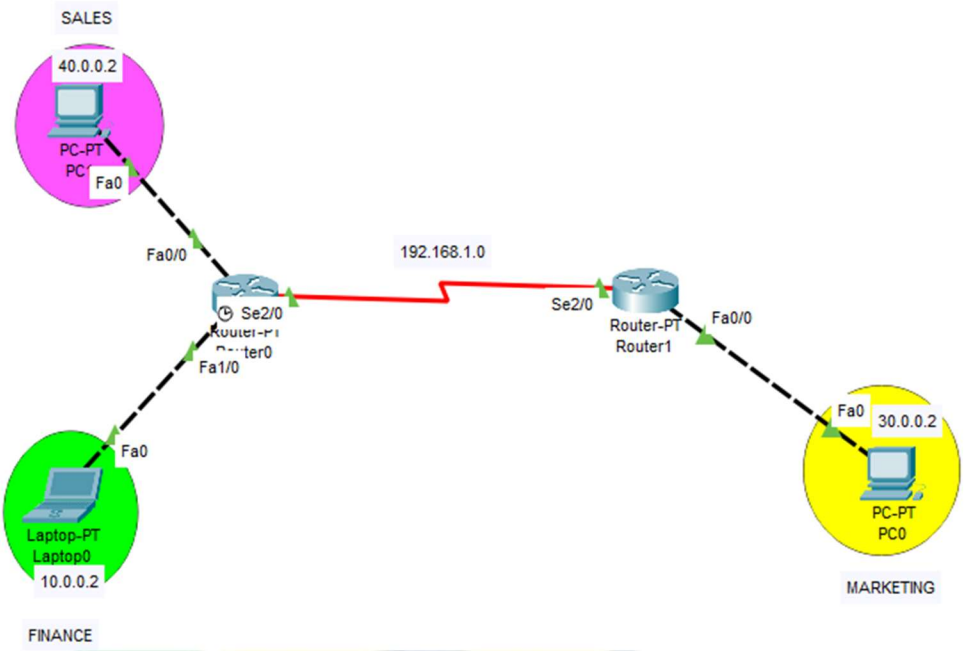

Figure 18

IP configuration on Router 0 (fa0/0):

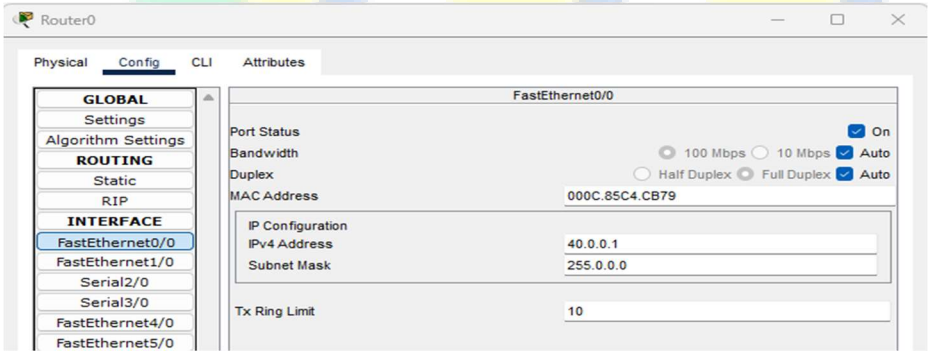

Figure 19

IP configuration on Router 0 (fa0/1):

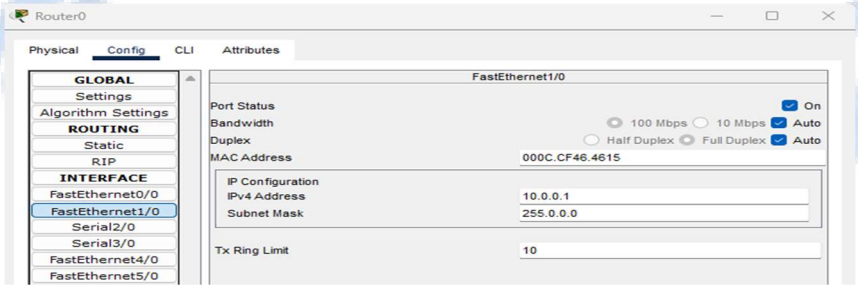

Figure 20

IP configuration on Router 0 (se2/0):

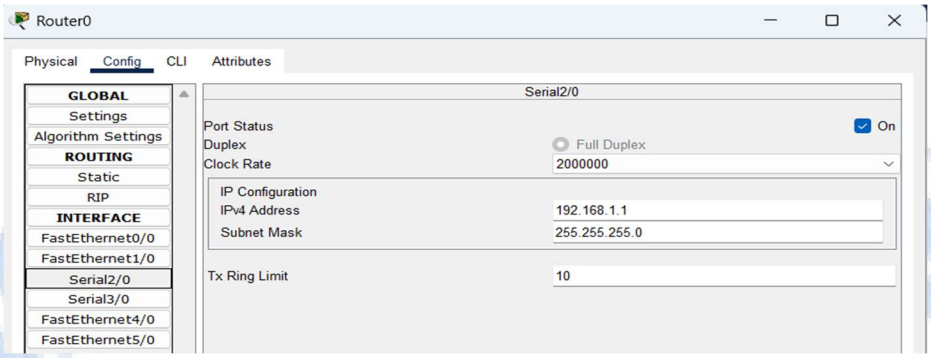

Figure 21

IP configuration on Router 1 (se2/0):

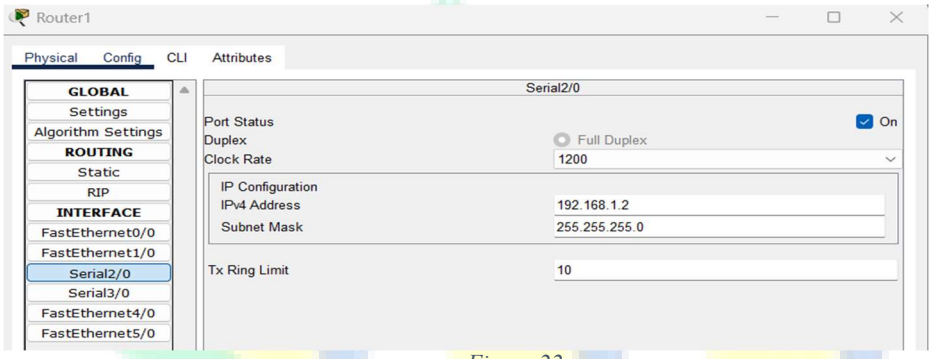

Figure 22

IP configuration on Router 1 (fa0/0):

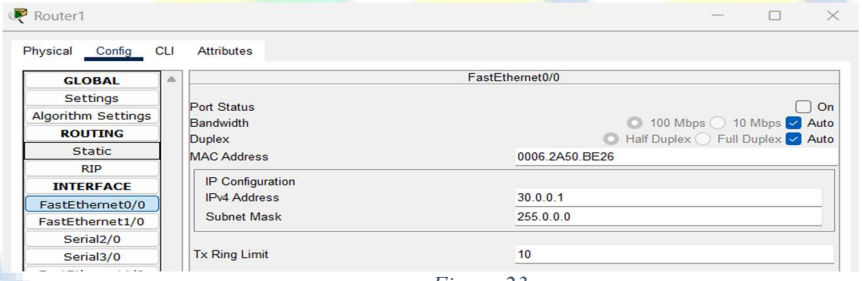

Figure 23

IP configuration on PC (SALES):

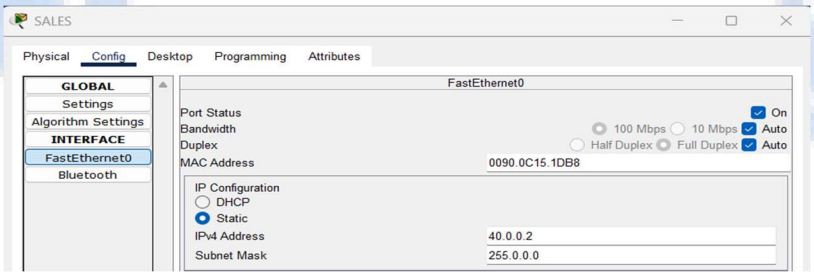

Figure 24

IP configuration on PC (FINANCE):

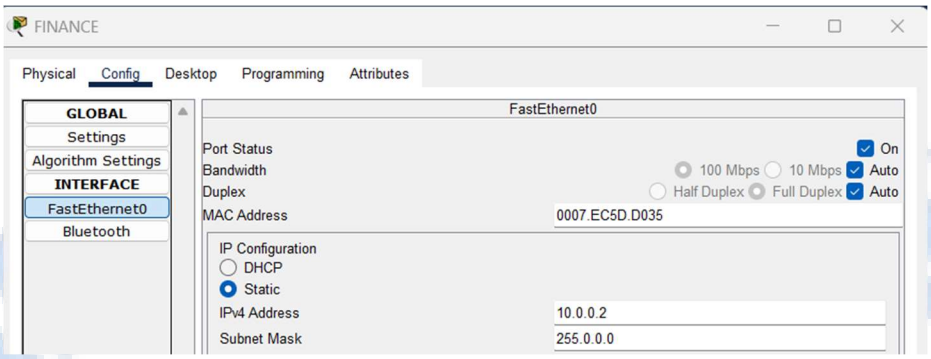

Figure 25

IP configuration on PC (MARKETING):

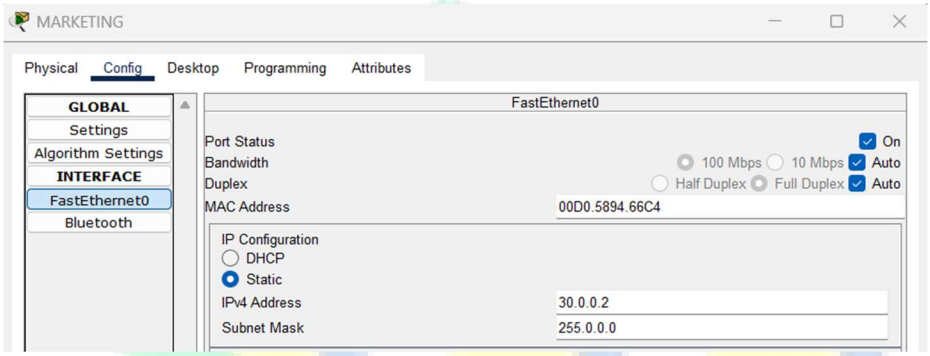

Figure 26

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

Router 0:

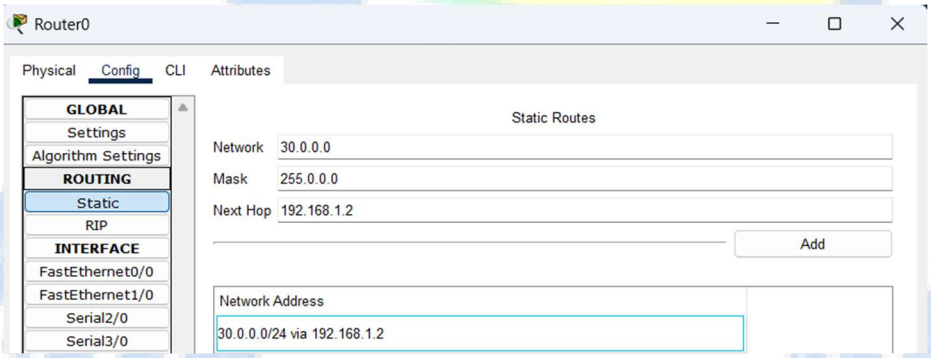

Figure 27

Router 1:

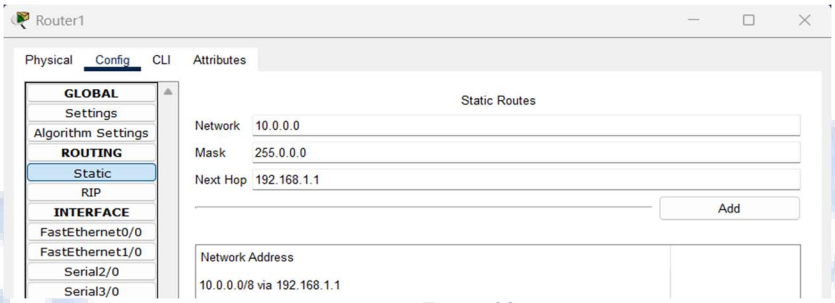

Figure 28

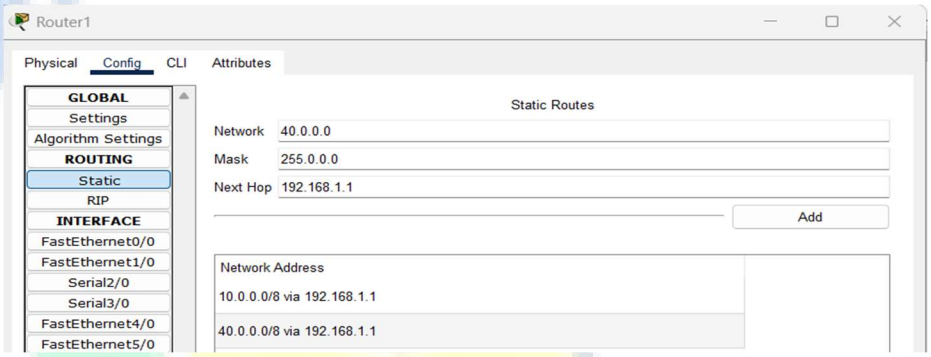

Figure 29

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 40.0.02 255.0.0.0 (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

Another way to create a standard ACL:
Configuring router 1 to block marketing from sending messages through se2/0 of router 1.

```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip access-list standard BlockMarketing
Router(config-std-nacl)#deny 30.0.0.2 0.0.0.0
Router(config-std-nacl)#exit
Router(config)#cint se2/0
Router(config-if)#ip access-group BlockMarketing out
```

Figure 32