JAIN DEEMED-TO-BE UNIVERSITY

FACULTY OF ENGINEERING AND TECHNOLOGY

Bachelor of Technology in Computer Science and Engineering

Lab Manual for Advance Computer Network Lab (22CSE529)

Faculty of Engineering & Technology
Global Campus
45th km NH – 209, Jakkasandra Post, Kanakapura Rd, Bangalore
www.set.jainuniversity.ac.in
Fax STD Code:- 080 Fax:- 2757 7199

CONTENTS

Faculty in-charge(s) **Head of the Department**

Institute Vision and Mission

Vision:

To be a leading technical institution that offers a transformative education to create leaders and innovators with ethical values to contribute for the sustainable development and economic growth of our nation.

Mission:

M1: To impart high standard of engineering education through innovative teaching and research to meet the changing needs of the modern society.

M2: To provide outcome-based education that transforms the students to understand and solve the societal, industrial problems through engineering and technology.

M3: To collaborate with other leading technical institutions and organization to develop globally competitive technocrats and entrepreneurs.

School Vision and Mission

Vision :

To be the Nation's Leading Research and Teaching School of Computer Science & Engineering.

Mission:

M1: To create, share and apply the knowledge in Computer Science, including interdisciplinary areas.

M2: To educate students to be successful, ethical, and effective problem-solvers and life-long learners.

M3: To make students ready to respond swiftly to the challenges of the 21st century.

Department Vision and Mission

Vision:

To emerge as a model Centre for education and research in the area of Computer Science and Engineering through Knowledge acquisition, dissemination and generation to meet societal demands.

Mission:

M1: To impart the quality education in cutting edge technologies, teaching & learning ambience in Computer Science and Engineering.

M2: To establish a center of excellence in collaboration with industries, research laboratories and other agencies to meet the changing needs of society.

M3: To provide an environment conducive to develop innovation, team-spirit and Entrepreneurship.

M4: To practice and promote high standards of professional ethics and transparency.

Program Educational Objectives (PEOs)

A few years after graduation, the Graduates of Computer Science and Engineering will be able

PEO1: To excel as professionals in the area of Computer Science and Engineering with an inclination towards continuous learning.

PEO2: To involve in interdisciplinary innovative and creative research work to solve societal needs and adopt themselves to rapidly evolving technologies.

PEO3: To develop entrepreneurial skills with leadership capabilities

PEO4: To exhibit professional ethics among the graduates to transform them as responsible citizens.

Program Specific Outcomes (PSO)

PSO 1: Design and develop network, web-based, cloud-based computational systems

PSO 2: Design efficient algorithms, understand software practices and implement code with optimization

Program Outcomes

Engineering Graduate's attributes

Sl.No.	Program Outcomes
1.	**Engineering knowledge**: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
2.	**Problem analysis**: Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
3.	**Design/development of solutions**: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
4.	**Conduct investigations of complex problems**: Use research-based knowledge and

	research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
5.	**Modern tool usage**: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modelling to complex engineering activities with an understanding of the limitations.
6.	**The engineer and society**: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.
7.	**Environment and sustainability**: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.
8.	**Ethics**: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
9.	**Individual and teamwork**: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
10.	**Communication**: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.
11.	**Project management and finance**: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
12.	**Life-long learning**: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

Course Outcome Statements and Course Articulation Matrix

Course Outcome Statements

After the completion of the course, the students are able to

CO-1	Explain the application layer of the OSI model and TCP/IP.
CO-2	Discuss the different Transport layer protocols
CO-3	Apply the networking layer concepts for IPV4 and subnetting.
CO-4	Implement the different dynamic routing protocols like RIP, EIGRP and OSPF.
CO-5	Discuss the basic protocols, VLANs, VTP , WAN, ATM in networks.
CO-6	Discuss the contemporary issues in Wifi and 802.11 networks.

CO – PO Mapping

CO/PO: Mapping												
(H/M/L indicates strength of correlation) 3-High, 2-Medium, 1-Low												
Course Outcome (COs)	**Programme Outcome (POs)**											
	PO-1	**PO-2**	**PO-3**	**PO-4**	**PO-5**	**PO-6**	**PO-7**	**PO-8**	**PO-9**	**PO-10**	**PO-11**	**PO-12**
CO-1	**2**	**2**	**1**	**1**	**1**						**1**	**1**
CO-2	**2**	**2**	**1**	**1**	**1**						**2**	**1**
CO-3	**3**	**1**	**2**	**1**	**1**						**2**	**2**
CO-4	**3**	**3**	**2**	**1**	**1**						**2**	**2**
CO-5	**3**	**3**	**2**	**1**	**1**						**2**	**2**
CO-6	**3**	**3**	**3**	**2**	**1**					**2**	**2**	**3**
Average	**3**	**3**	**2**	**1**	**1**					**2**	**2**	**2**

Rubrics for Evaluation (CA and Semester End Assessment)

Assessment and Evaluation

CA (Continuous Assessment) : Every experiment is evaluated for100 marks

Test1(Lab Internal-1) : Conducted for 100 marks (Open Ended Experiment) in the middle of the semester
Test1 (Lab Internal-1) : Conducted for 100 marks (Open Ended Experiment) towards end of the semester
Semester End Test : Conducted for 100 marks at the end of the semester

Rubrics for CA Marks :

Rubrics	Marks Allocated (100)	High	Medium	Low
Procedure	20	For given concept, algorithm and pseudo code is designed	For given concept, partial algorithm and pseudo code is designed	For given concept, low preparation before implementation but understood the concept
		20	10	5
Conduction	40	For given concept, implementation successfully done.	For given concept, implementation partially done.	For given concept, implementation still in process towards the goal.
		40	30	20
Calculation, Results, Graph	15	Desired output achieved and validation is processed.	Desired output partially achieved.	Desired output is yet to achieve.
		15	10	5
Viva/Oral	15	Student answered all the viva voce questions which include analytical skills	Student answered to all viva voce questions	Student answered to partial viva voce questions
		15	10	5
Record Writing	10	completed record was submitted on time	Record was submitted late Late submission	Record was submitted but incomplete
		10	8	5

Rubrics used for continuous evaluation lab internals

Rubrics	Marks Allocated (100)	High	Medium	Low
Write up	30	Student is able to analyze the problem statement, design the algorithm and pseudo code with expected logic and approach.	Student is able to analyze the problem statement, but partially design the algorithm and pseudo code with expected logic and approach.	Student is able to partially analyze the problem statement, but partially design the algorithm and pseudo code with expected logic and approach.
		30	20	10
Execution / Output	50	For given concept, implementation successfully done.	For given concept, implementation partially done.	For given concept, implementation still in process towards the goal.
		50	40	35
Viva Voce	20	Student answered all the viva voce questions which includes analytical skills	Student answered to all viva voce questions	Student answered to partial viva voce questions
		20	16	10

Rubrics for Semester End Assessment (Total 100 marks)

Experiment write Up : 35 marks

Results : 35 marks

Viva-Voce : 30 marks

List of Experiments

Experiment #	Title of Experiment	CO
1.	Switch Configuration - Basic Commands Switch Configuration - Switch Port Security Setting up of Passwords	CO1
2.	Router – Configuration - Basic Commands Router Configuration	CO1
3.	Configuration of IP Address for a Router & Default Route	CO2
4.	Configuration of Static Routing	CO3
5.	Configuration of Dynamic Routing	CO3
6.	Implementation of EIGRP	CO3
7.	Implementation of OSPF	CO3
8.	VLAN Configuration, Inter VLAN, VTP & Switch Troubleshooting	CO4
9.	Configuration of Access-lists - Standard	CO2
10.	Configuration of Access-lists - Extended ACLs	CO2
11.	Implementation of Network Address Resolution	CO5
12.	Implementation of HSRP	CO6

1.	Switch Configuration - Basic Commands Switch Configuration - Switch Port Security Setting up of Passwords	CO1

A switch is a layer 2 device used to forward packet from one device to another within the network. It forwards the packet through one of its ports on the basis of destination MAC address and the entry in the MAC table.

Following basic commands are used to configure a new switch :

1. Changing the hostname of a switch to CSE :

It is used to set the name of the device.

switch(config)#hostname CSE

CSE(config)#

2. To add a banner message :

It provides a short message to the user who wants to access the switch.

CSE(config)#banner motd &

Enter Text message. End with character '&'

$ This is GeeksforGeeks floor Switch &

3. To set IP address in Switch :

IP address is the address of device in network.

CSE(config)#interface vlan1

CSE(config-if)#ip address 172.16.10.1 255.255.255.0

CSE(config-if)#exit

CSE(config)#ip default-gateway 172.16.10.0

4. To set the current clock time :

This is set the current time stored in the switch.

CSE#clock set 3:03:14 June 25 2020

5. Apply password protection (enable password, secret password, console password and vty password) :

- **Enable password :**

  The enable password is used for securing privilege mode.

  CSE(config)#enable password CSEA

- **Enable secret password :**

  This is also used for securing privilege mode but the difference is that it will be displayed as ciphertext(***) on the configuration file.

  CSE(config)#enable secret CSEA

- **Line console password :**

  When a person will take access through console port then this password will be asked.

  CSE(config)#line console 0

  CSE(config-line)#password GFG

  CSE(config-line)#login

- **Line VTY password :**

  When a person want to access a router through VTY lines (telnet or ssh) then this password will be asked.

  CSE(config)#line VTY 0 2

  CSE(config-line)#password CSEA

  CSE(config-line)#exit

6. Copy to startup-configuration file from running-configuration file :

CSE#copy running-config startup-config

7. To watch startup-configuration file and running-configuration file :

CSE#show startup-config

CSE#show running-config

8. Clear mac address table :

Switch stores MAC addresses in MAC address table

CSE#clear mac address-table

2.	Router – Configuration - Basic Commands Router Configuration	CO1

In this network, a router and 2 PCs are used. Computers are connected with routers using a copper straight-through cable. After forming the network, to check network connectivity a simple PDU is transferred from PC0 to PC1. The network simulation status is successful. From this network, it can be observed that the router handles data transfers between multiple devices.

Procedure:

Step-1(Configuring Router1):

1. Select the router and Open CLI.
2. Press ENTER to start configuring Router1.
3. Type enable to activate the privileged mode.
4. Type config t(configure terminal) to access the configuration menu.
5. Configure interfaces of Router1:

   • *Type interface FastEthernet0/0 to access FastEthernet0/0 and Configure the Fast Ethernet0/0 interface with the IP address 192.168.10.1 and Subnet mask 255.255.255.0.*

   • *Type interface FastEthernet0/1 to access GigabitEthernet0/0 and Configure the FastEthernet0/1 interface with IP address 192.168.20.1 and Subnet mask 255.255.255.0.*

6. Type no shutdown to finish.

Router1 Command Line Interface:

Router>enable

Router#config t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#interface FastEthernet0/0

Router(config-if)#ip address 192.168.10.1 255.255.255.0

Router(config-if)#no shutdown

Router(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

Router(config-if)#interface FastEthernet0/1

Router(config-if)#ip address 192.168.20.1 255.255.255.0

Router(config-if)#no shutdown

Step-2(Configuring PCs):

1. Assign IP Addresses to every PC in the network.
2. Select the PC, Go to the desktop and select IP Configuration and assign an IP address, Default gateway, Subnet Mask
3. Assign the default gateway of PC0 as 192.168.10.1.
4. Assign the default gateway of PC1 as 192.168.20.1.

Step-3(Connecting PCs with Router):

1. Connect FastEthernet0 port of PC0 with FastEthernet0/0 port of Router1 using a copper straight-through cable.
2. Connect FastEthernet0 port of PC1 with FastEthernet0/1 port of Router1 using a copper straight-through cable.

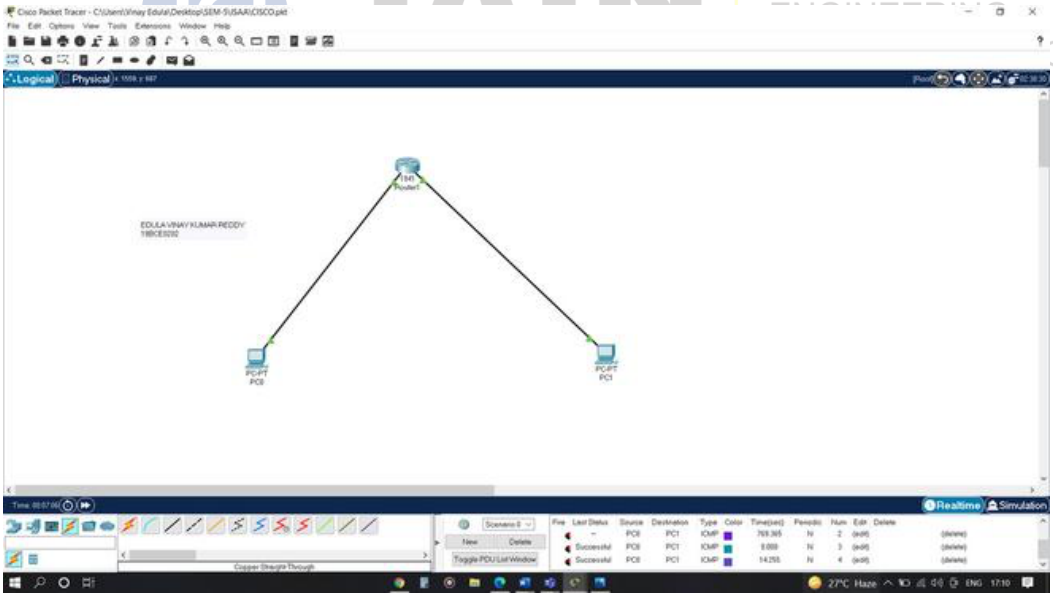
Router Configuration Table:

Device Name	IP address FastEthernet0/0	Subnet Mask	IP Address FastEthernet0/1	Subnet Mask
Router1	192.168.10.1	255.255.255.0	192.168.20.1	255.255.255.0

PC Configuration Table:

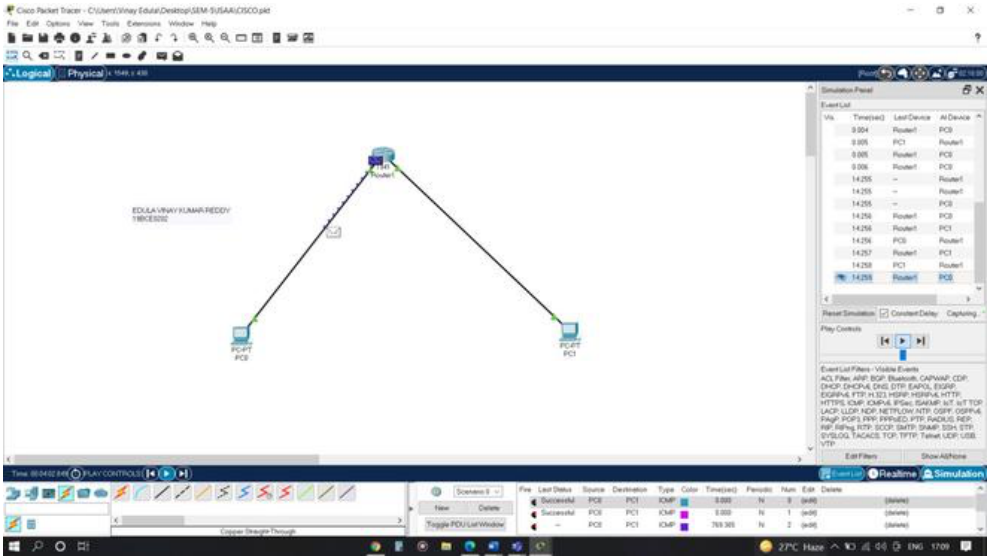
Device Name	IP address	Subnet Mask	Gateway
PC 0	192.168.10.2	255.255.255.0	192.168.10.1
PC 1	192.168.20.2	255.255.255.0	192.168.20.1

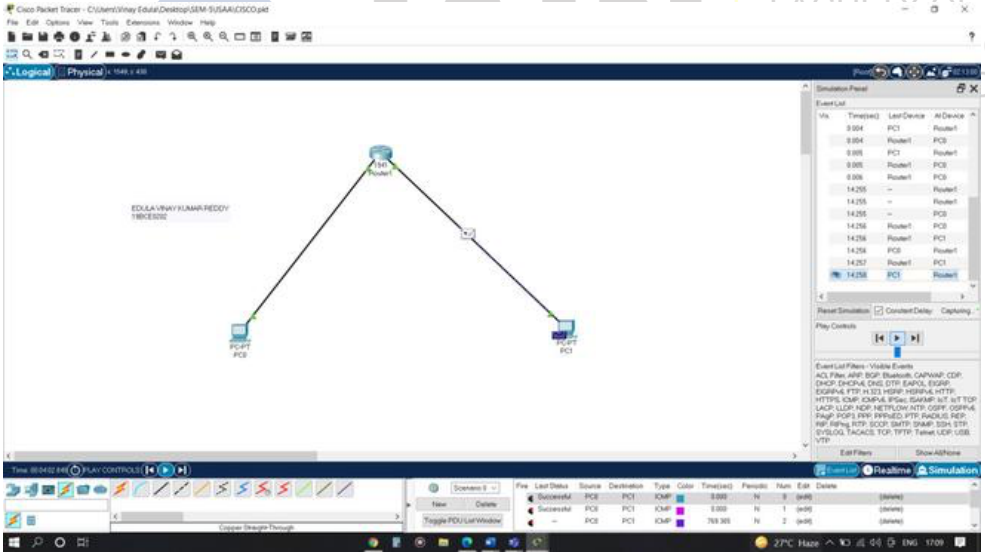
Designed Network topology:



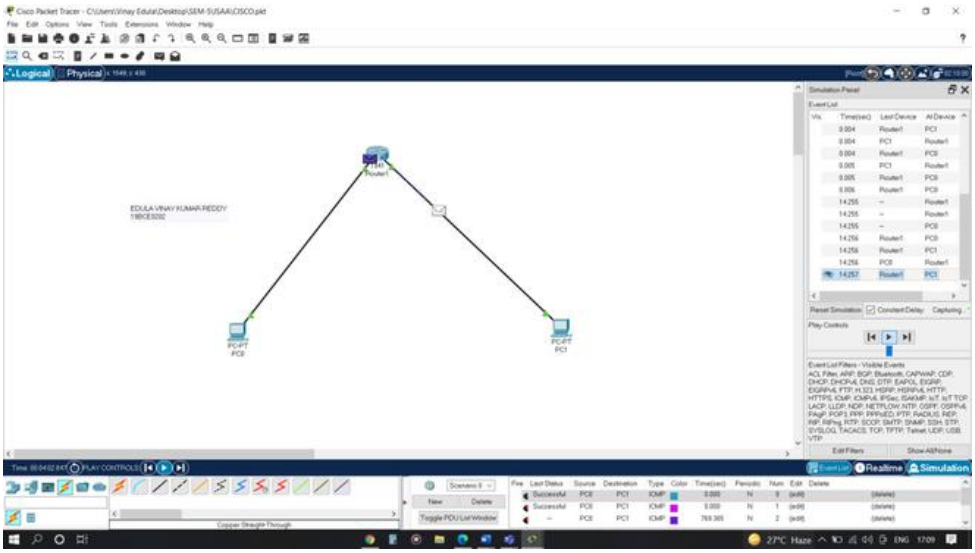
Simulation of Designed Network Topology:

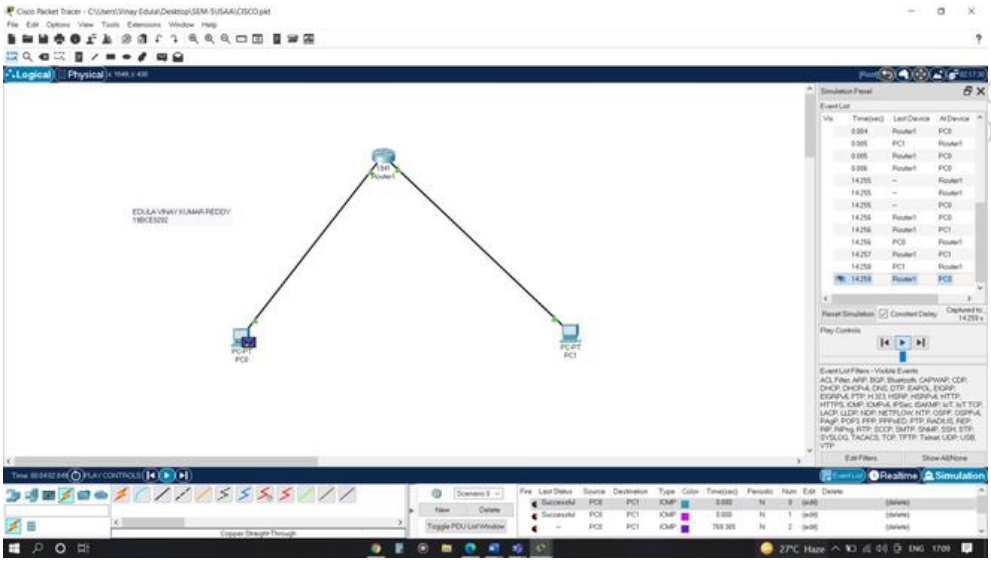
Sending a PDU From PC0 to PC1:





Acknowledgment From PC1 to PC0:





3.	Configuration of IP Address for a Router & Default Route	CO2

The default route is a route that a router uses to forward an incoming packet when no other route is available for that packet in the routing table. Routers use the routing table to make the forwarding decision. A routing table entry consists of two pieces: the remote network and the local interface that is connected to that network.

When a packet arrives on an interface of a router, the router reads the destination network address of the incoming packet and finds that network address in the routing table. If the routing table contains an entry for the destination network, the router forwards the incoming packet from the interface that is written next to the destination network in the entry.

If the routing table does not contain an entry for the destination address, the router drops the incoming packet. This is the point where the concept of default route fits. A default route gives a route to a router to forward all incoming packets whose destination network addresses are not available in the routing table.

Default route address

A default route contains all zero in the IP address. There are two versions of IP protocol, IPv4 and IPv6. In both versions, the address of the default route is the following.

IPv4 default route: - 0.0.0.0 0.0.0.0

IPv6 default route: - ::/0

All zero (0.0.0.0) in network portion and subnet mask represent all networks and all hosts in the specified network, respectively.

Command or syntax to configure a default route

To configure an IPv4 default route, use the following syntax from the global configuration mode.

Router(config)# ip route 0.0.0.0 0.0.0.0 {ip-address | exit-interface}

To configure an IPv6 default route, use the following syntax from the global configuration mode.

Router(config)# ipv6 route ::/0 {ipv6-address | exit-interface}

In both syntaxes: the *ip-address* is the IP address of the next-hop and the *exit-interface* is the local interface of the router.

If you use the IP address of the next-hop, the router will forward packets to the remote interface of the other router (next-hop) that is directly connected to the local router and has configured with the IP address that you assign in the default route.

If you use the exit-interface, the router forwards packets from the local interface that you configure in the default route.

You should configure the exit-interface instead of the next-hop IP address. The benefit of the exit-interface configuration over the next-hop IP address configuration is that the exit-interface configuration does not depend upon the IP address stability of the next-hop.

Let's take some examples of the default route configuration.

The following command configures an IPv4 default route that forwards all packets from the serial 0/0/0 interface.

Router(config)# ip route 0.0.0.0 0.0.0.0 serial 0/0/0

The following command configures an IPv4 default route that forwards all packets to the next-hop 192.168.1.1.

Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1

The following command configures an IPv6 default route that forwards all packets from the serial 1/1/1 interface.

Router(config)# ipv6 route ::/0 serial 0/0/0

The following command configures an IPv6 default route that forwards all packets to the next-hop 2001:DB8:1:F::1.

Router(config)# ipv6 route ::/0 2001:DB8:1:F::1

To view the default route configuration, use the **"show ip route"** command from the *privileged-exec* mode.

Router#show ip route

You can also use the **"show running-config"** command to view the command that was used to configure the default route.

Router#show running-config

The following image shows both commands with sample output.

```
Router>enable
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
Gateway of last resort is 0.0.0.0 to network 0.0.0.0

C    20.0.0.0/8 is directly connected, Serial0/0/0
C    30.0.0.0/8 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 is directly connected, Serial0/0/0

Router#show running-config
Building configuration...

Current configuration : 728 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
!
ip flow-export version 9
!
!
 --More--
```

Static default route v/s Dynamic default route

A default route configured by the "**ip route**" command is called the default static route. Some routing protocols such as RIP and EIGRP allow us to advertise the default static route. A default static route configured on other router and learned via a routing protocol is known as the dynamic default route.

AD (Administrative Distance) value of the default route

Administrative distance is a Cisco proprietary mechanism used to rank the IP routing protocols. Administrative distance assigns a value (from range 0 to 255) to each IP routing protocol.

Routers use AD value to select the best route from all available routes. If a router receives routing updates for a single network from multiple sources, the router uses AD value to choose a single best route from all available routes.

A smaller AD value is more believable by a router, with the best AD value being 0 and the worst, 255.

The AD value of the default route depends on the type of configuration. If the default route is statically configured by the **"ip route"** command, the router assigns it the AD value 1. **1** is the AD value of the static route.

Same way, if the default route is dynamically learned via a routing protocol, the router assigns it an AD value of the routing protocol. For example, if a router learns the default route from the RIP routing protocol, the router assigns the AD value 120. **120** is the AD value of the RIP routing protocol.

How a default route works in routing

A router forwards an incoming packet from the default route only if another route is not available for that packet in the routing table. In other words, if a route is available for an incoming packet in the routing table, the router does not use the default route for that packet.

Let's take an example. Suppose a packet arrives on an interface of a router. The router reads the destination network from the packet and searches that destination network in the routing table.

Now, there can be three situations. The following table describes each situation along with the action that the router will take in that situation.

Situation	Action
Neither an entry in the routing table for the destination network nor a default route is available.	Drop the packet

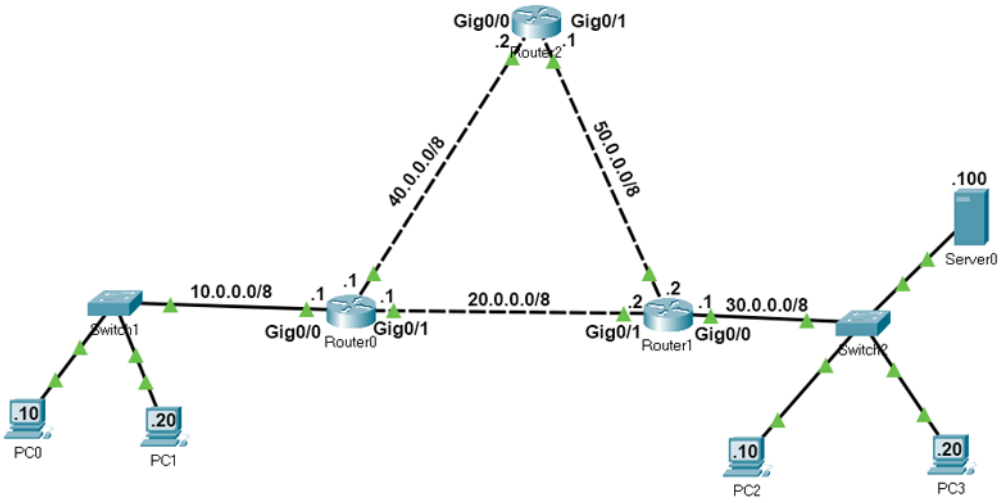
Both, an entry in the routing table for the destination network and a default route are available.	Use the entry to forward the packet
An entry for the destination network is not available in the routing table but the default route is available.	Use the default route to forward the packet

4.	Configuration of Static Routing	CO3

Static routes are the routes you manually add to the router's routing table. The process of adding static routes to the routing table is known as static routing. Let's take a packet tracer example to understand how to use static routing to create and add a static route to the routing table.

Setting up a practice lab

Create a packet tracer lab as shown in the following image or download the following pre-created lab and load it on Packet Tracer.



In this lab, each network has two routes to reach. We will configure one route as the main route and another route as the backup route. If the link bandwidth of all routes is the same, we use the route that has the least number of routers as the main route. If the link bandwidth and the number of routers are the same, we can use any route as the main route and another route as the backup route.

If we specify two routes for the same destination, the router automatically selects the best route for the destination and adds the route to the routing table. If you manually want to select a route that the router should add to the routing table, you have to set the AD value of the route lower

than other routes. For example, if you use the following commands to create two static routes for network 30.0.0/8, the route will place the first route to the routing table.

#ip route 30.0.0.0 255.0.0.0 20.0.0.2 10

#ip route 30.0.0.0 255.0.0.0 40.0.0.2 20

If the first route fails, the router automatically adds the second route to the routing table.

Creating, adding, verifying static routes

Routers automatically learn their connected networks. We only need to add routes for the networks that are not available on the router's interfaces. For example, network 10.0.0.0/8, 20.0.0.0/8 and 40.0.0.0/8 are directly connected to Router0. Thus, we don't need to configure routes for these networks. Network 30.0.0.0/8 and network 50.0.0.0/8 are not available on Router0. We have to create and add routes only for these networks.

The following table lists the connected networks of each router.

Router	Available networks on local interfaces	Networks available on other routers' interfaces
Router0	10.0.0.0/8, 20.0.0.0/8, 40.0.0.0/8	30.0.0.0/8, 50.0.0.0/8
Router1	20.0.0.0/8, 30.0.0.0/8, 50.0.0.0/8	10.0.0.0/8, 40.0.0.0/8
Router2	40.0.0.0/8, 50.0.0.0/8	10.0.0.0/8, 20.0.0.0/8, 30.0.0.0/8

Let's create static routes on each router for networks that are not available on the router.

Router0 requirements

- Create two routes for network 30.0.0.0/8 and configure the first route (via -Router1) as the main route and the second route (via-Router2) as a backup route.
- Create two routes for the host 30.0.0.100/8 and configure the first route (via -Router2) as the main route and the second route (via-Router1) as a backup route.
- Create two routes for network 50.0.0.0/8 and configure the first route (via -Router2) as the main route and the second route (via-Router1) as a backup route.
- Verify the router adds only main routes to the routing table.

Router0 configuration

Access the CLI prompt of Router0 and run the following commands.

Router>enable

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#ip route 30.0.0.0 255.0.0.0 20.0.0.2 10

Router(config)#ip route 30.0.0.0 255.0.0.0 40.0.0.2 20

Router(config)#ip route 30.0.0.100 255.255.255.255 40.0.0.2 10

Router(config)#ip route 30.0.0.100 255.255.255.255 20.0.0.2 20

Router(config)#ip route 50.0.0.0 255.0.0.0 40.0.0.2 10

Router(config)#ip route 50.0.0.0 255.0.0.0 20.0.0.2 20

Router(config)#exit

Router#show ip route static

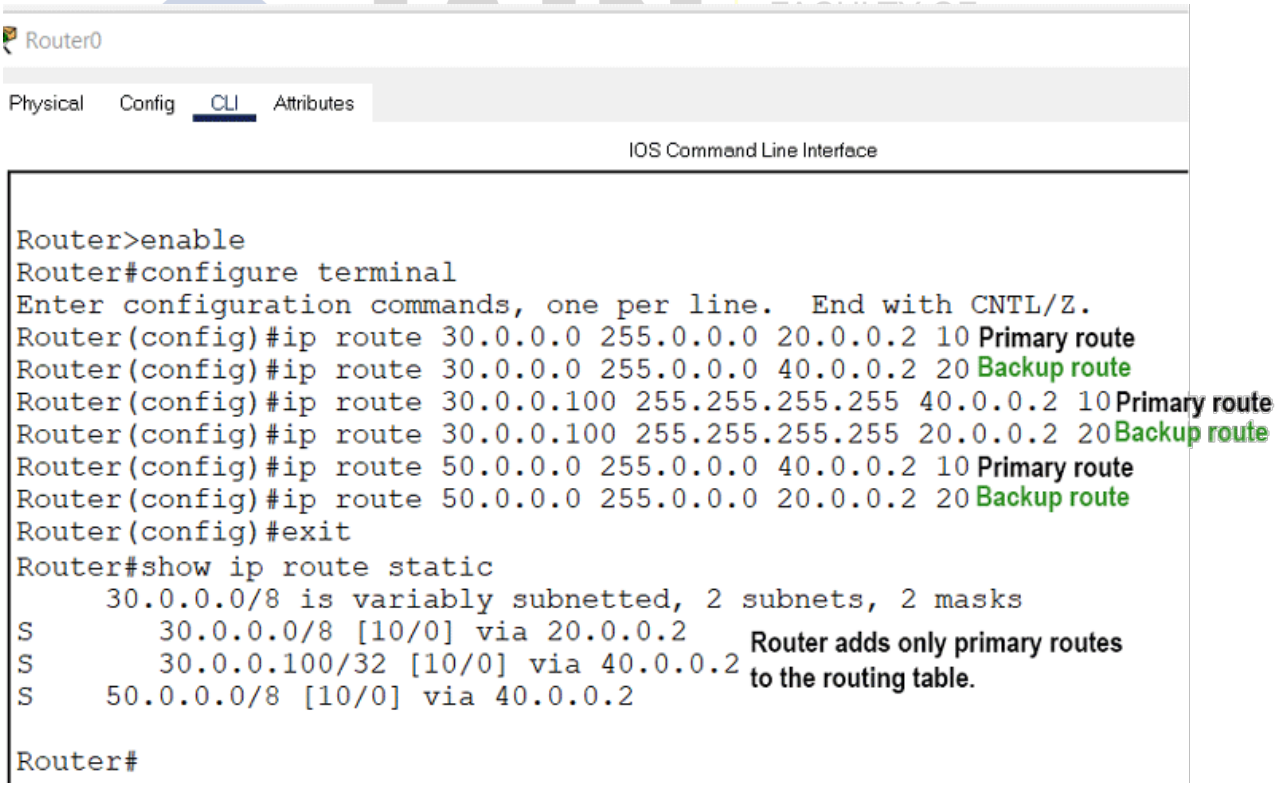
30.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

S 30.0.0.0/8 [10/0] via 20.0.0.2

S 30.0.0.100/32 [10/0] via 40.0.0.2

S 50.0.0.0/8 [10/0] via 40.0.0.2

Router#



Router1 requirements

- Create two routes for network 10.0.0.0/8 and configure the first route (via -Router0) as the main route and the second route (via-Router1) as a backup route.
- Create two routes for network 40.0.0.0/8 and configure the first route (via -Router0) as the main route and the second route (via-Router2) as a backup route.
- Verify the router adds only main routes to the routing table.

Router1 configuration

Router>enable

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#ip route 10.0.0.0 255.0.0.0 20.0.0.1 10

Router(config)#ip route 10.0.0.0 255.0.0.0 50.0.0.1 20

Router(config)#ip route 40.0.0.0 255.0.0.0 20.0.0.1 10

Router(config)#ip route 40.0.0.0 255.0.0.0 50.0.0.1 20

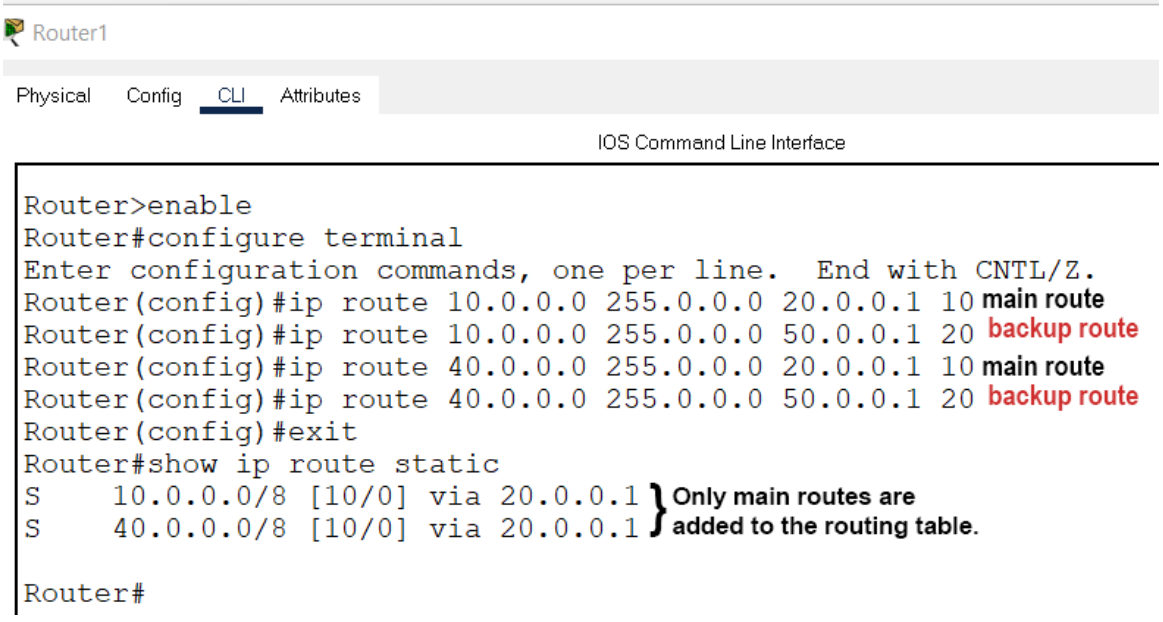
Router(config)#exit

Router#show ip route static

S 10.0.0.0/8 [10/0] via 20.0.0.1

S 40.0.0.0/8 [10/0] via 20.0.0.1

Router#



Router2 requirements

Create static routes for network 10.0.0.0/8 and network 30.0.0.0/8 and verify the router adds both routes to the routing table.

Router2 configuration

Router>enable

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#ip route 10.0.0.0 255.0.0.0 40.0.0.1

Router(config)#ip route 30.0.0.0 255.0.0.0 50.0.0.2

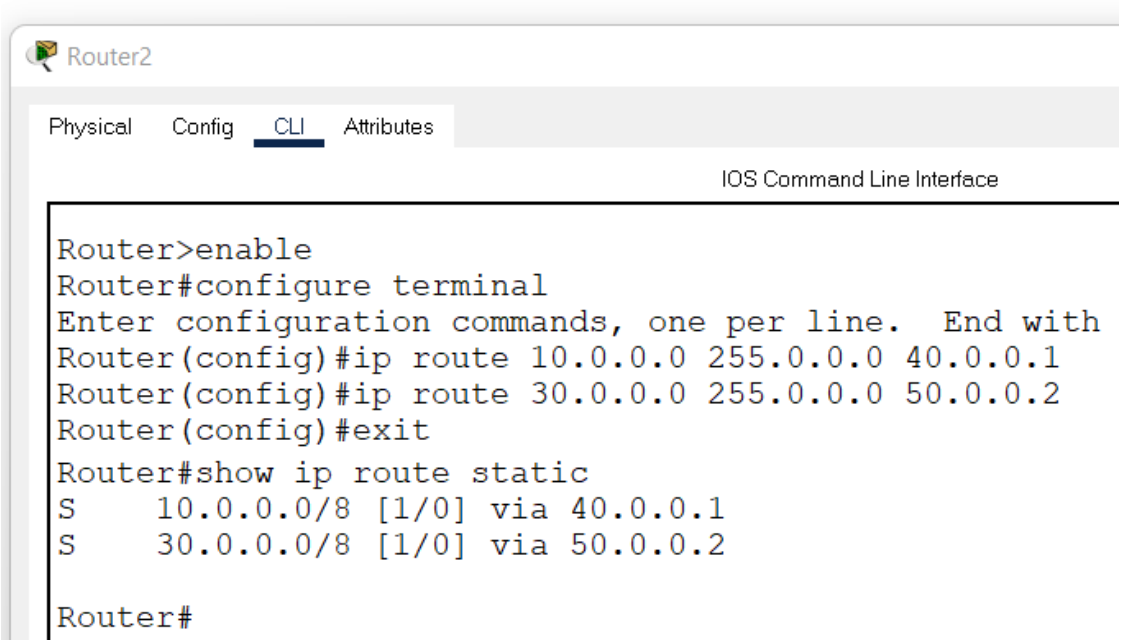
Router(config)#exit

Router#show ip route static

S 10.0.0.0/8 [1/0] via 40.0.0.1

S 30.0.0.0/8 [1/0] via 50.0.0.2

Router#



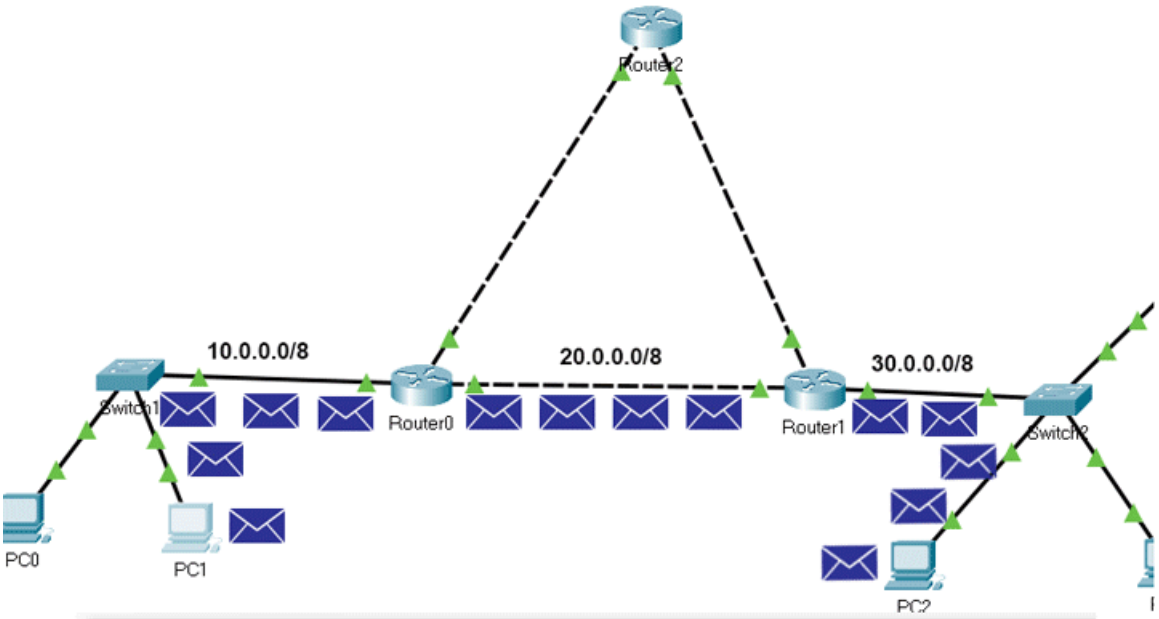
Verifying static routing

On Router0, we configured two routes for network 30.0.0.0/8. These routes are via Router1 and via Router2. We set the first route (via-Router1) as the main route and the second route as the backup route. We can verify this configuration in two ways.

By sending ping requests to a PC of network 30.0.0.0/8 and tracing the path they take to reach the network 30.0.0.0/8. For this, you can use **'tracert'** command on a PC of network 10.0.0.0/8. The **'tracert'** command sends ping requests to the destination host and tracks the path they take to reach the destination.

By listing the routing table entries on Router0. Since a router uses the routing table to forward data packets, you can check the routing table to figure out the route the router uses to forward data packets for each destination.

The following image shows the above testing.



Router0

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>enable
Router#show ip route static
     30.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
S       30.0.0.0/8 [10/0] via 20.0.0.2
S       30.0.0.100/32 [10/0] via 40.0.0.2
S    50.0.0.0/8 [10/0] via 40.0.0.2

Router#
```

PC1

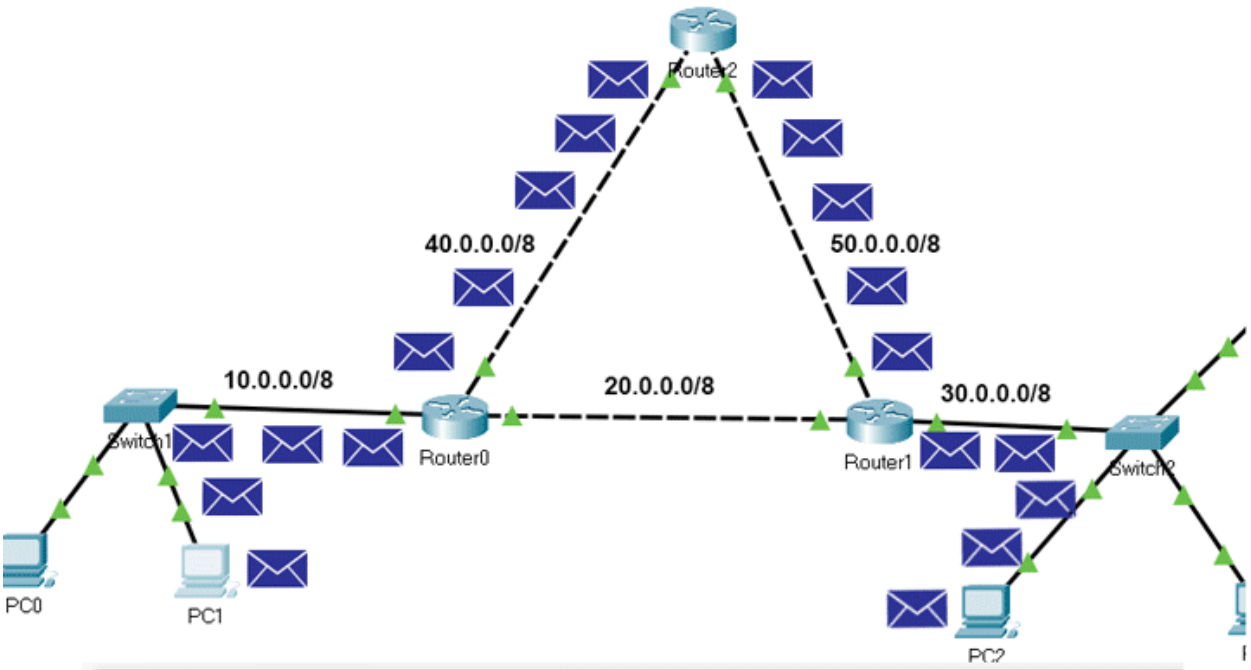
Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>tracert 30.0.0.20

Tracing route to 30.0.0.20 over a maximum of 30
hops:

  1    0 ms      0 ms      0 ms      10.0.0.1
  2    0 ms      0 ms      0 ms      20.0.0.2
  3    *         0 ms      0 ms      30.0.0.20

Trace complete.

C:\>
```

We also configured a separate static host route for the host 30.0.0.100/8. The router must use this route to forward data packets to the host 30.0.0.100/8. To verify this, you can do the same testing for the host 30.0.0.100/8.

The following image shows this testing.



Router0

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>enable
Router#show ip route static
     30.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
S       30.0.0.0/8 [10/0] via 20.0.0.2
S       30.0.0.100/32 [10/0] via 40.0.0.2
S    50.0.0.0/8 [10/0] via 40.0.0.2

Router#
```

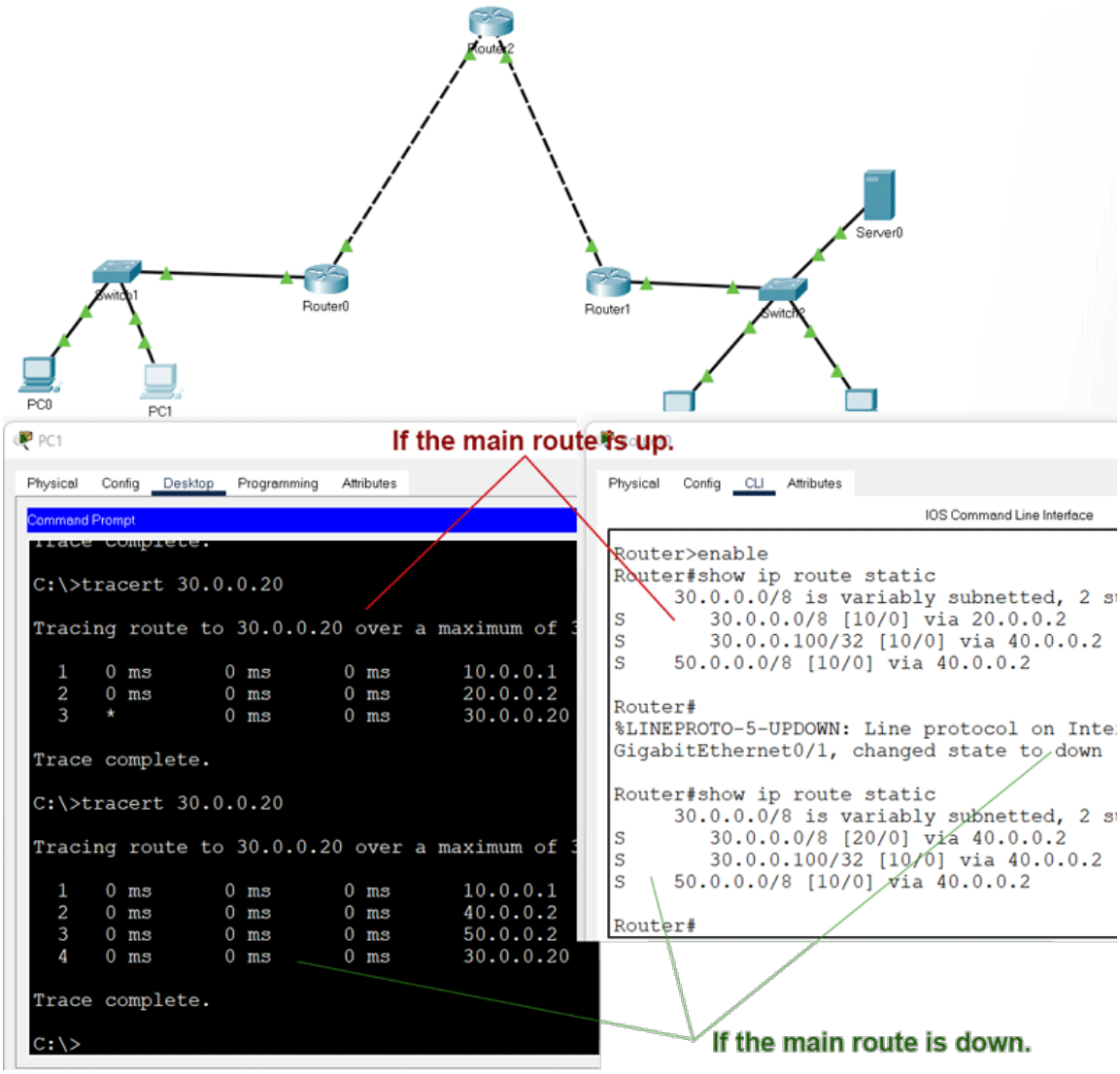
PC1

Physical Config Desktop Programming Attributes

```
Packet Tracer PC Command Line 1.0
C:\>tracert 30.0.0.100

Tracing route to 30.0.0.100 over a maximum of 30
hops:

  1    1 ms      0 ms      0 ms      10.0.0.1
  2    *         0 ms      0 ms      40.0.0.2
  3    *         *         0 ms      20.0.0.2
  4    *         0 ms      0 ms      30.0.0.100

Trace complete.

C:\>
```

We also configured a backup route for network 30.0.0.0/8. The router must put the backup route to the routing table and use it to forward data packets to network 30.0.0.0/8 when the main route fails. To verify this, we have to simulate the failure of the main route.

To simulate the failure of the main route, you can delete the link between Router0 and Router1. After deleting the link, do the same testing again for the network 30.0.0.0/8.



The following link provides the configured packet tracer lab of the above example.

Deleting a static route

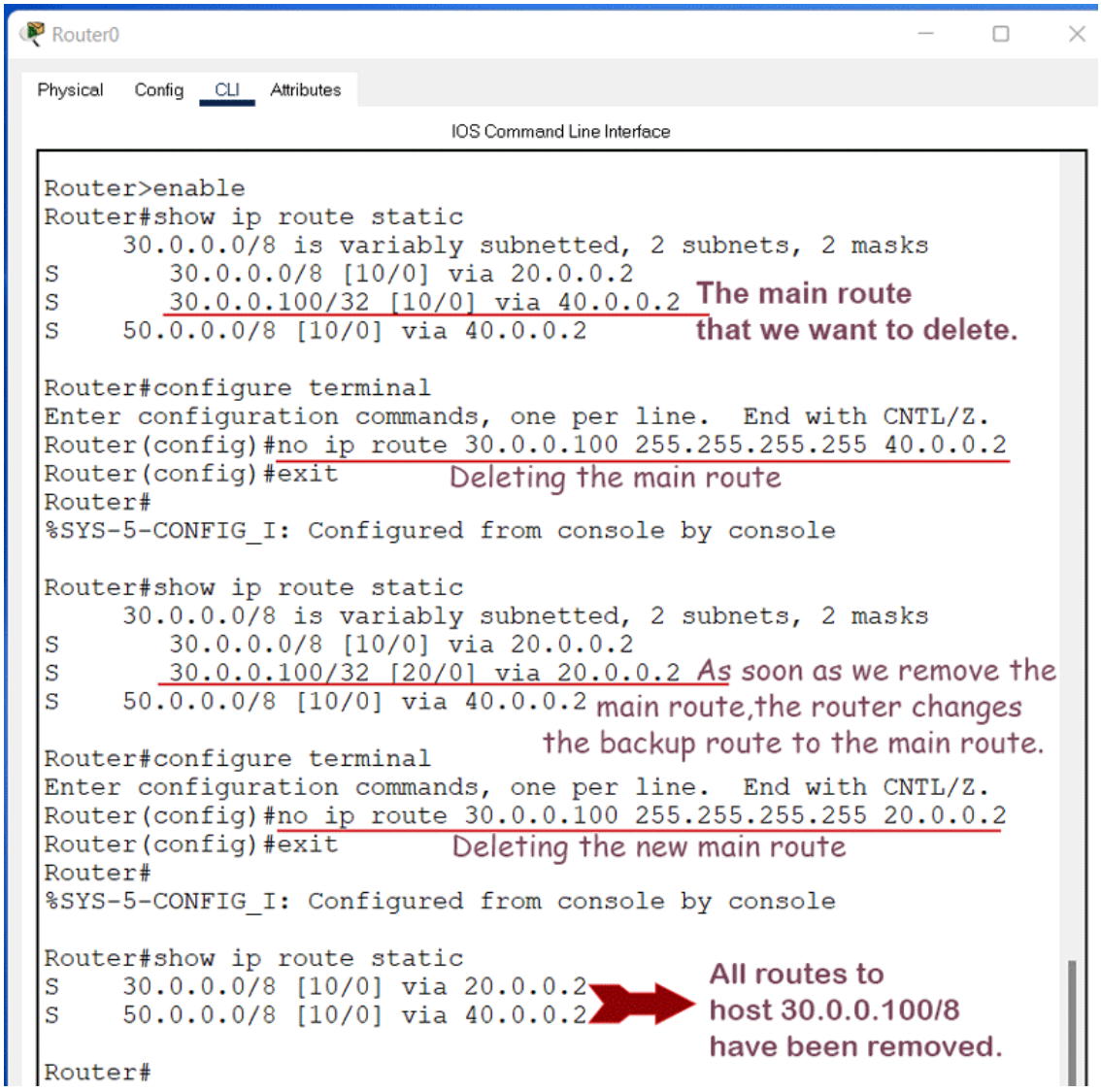
To delete a static route, use the following steps.

- Use the **'show ip route static'** command to print all static routes.

- Note down the route you want to delete.
- Use the **'no ip route'** command to delete the route.

If you have a backup route, the backup route becomes the main route when you delete the main route.

In our example, we have a backup route and a main route for the host 30.0.0.100/8. The following image shows how to delete both routes.



5.	Configuration of Dynamic Routing	CO3

Dynamic routing is all about configuring a network using dynamic routing protocols.

Dynamic Routing Protocol is divided in to two main parts.

1.Interior Gateway Protocol

2.Exterior Gateway Protocol

In this section will look at Interior Gateway Protocols.

-this is an autonomous system and handled by only one admin.

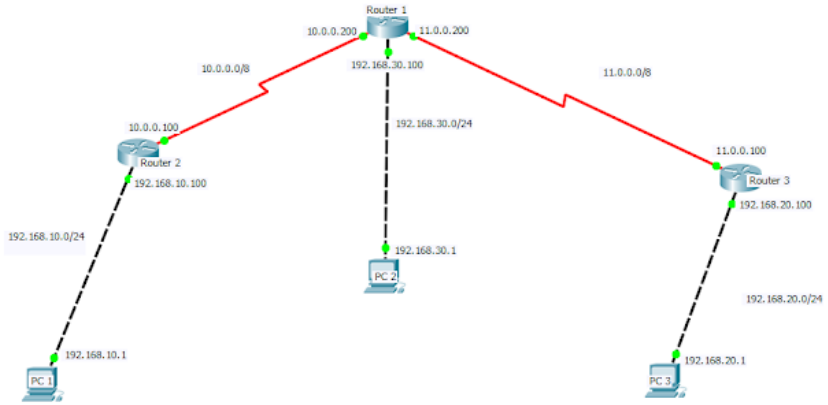
-this protocol is also divide into two parts,

1. Distant Vector Protocols(Bellman-Ford Algorithm) - distance is measured by `hop count` and use for simple networks

2. Link State Protocol(Dijkstra Algorithm) - this uses some other information like neighbour router info and this is best for complex network designs

In this Scenario we are using Routing Information Protocol(RIP) as the dynamic routing protocol.

So below mentioned diagram is the network plan for a small network.



In this Network diagram,

192.168.10.0 , 192.168.30.0 , 192.168.20.0 , 10.0.0.0 , 11.0.0.0 are 5 different networks.

Router 1, Router 2, Router 3 are routers in this network.

PC 1, PC 2, PC 3 are computers(end devices) in this network.

Black dashed lines are Copper Cross-Over cables which uses to connect different type devices.

Red colour lines are Serial DCE cables which are building the connection between two routers.

PC 1 - IP Address: 192.168.10.1(Fast Ethernet 0/0)

Default Gateway : 192.168.10.100(Fast Ethernet 0/0)

PC 2 - IP Address: 192.168.30.1(Fast Ethernet 0/0)

Default Gateway : 192.168.30.100(Fast Ethernet 0/0)

PC 3 - IP Address: 192.168.20.1(Fast Ethernet 0/0)

Default Gateway : 192.168.20.100(Fast Ethernet 0/0)

Router 1 - IP Address(SERIAL 0/2/0) : 10.0.0.200

IP Address(SERIAL 0/2/1) : 11.0.0.200

Router 2 - IP Address(SERIAL 0/0/0) : 10.0.0.100

IP Address(Fast Ethernet 0/0) : 192.168.10.100

Router 3 - IP Address(SERIAL 0/0/0) : 11.0.0.100

IP Address(Fast Ethernet 0/0) : 192.168.20.100

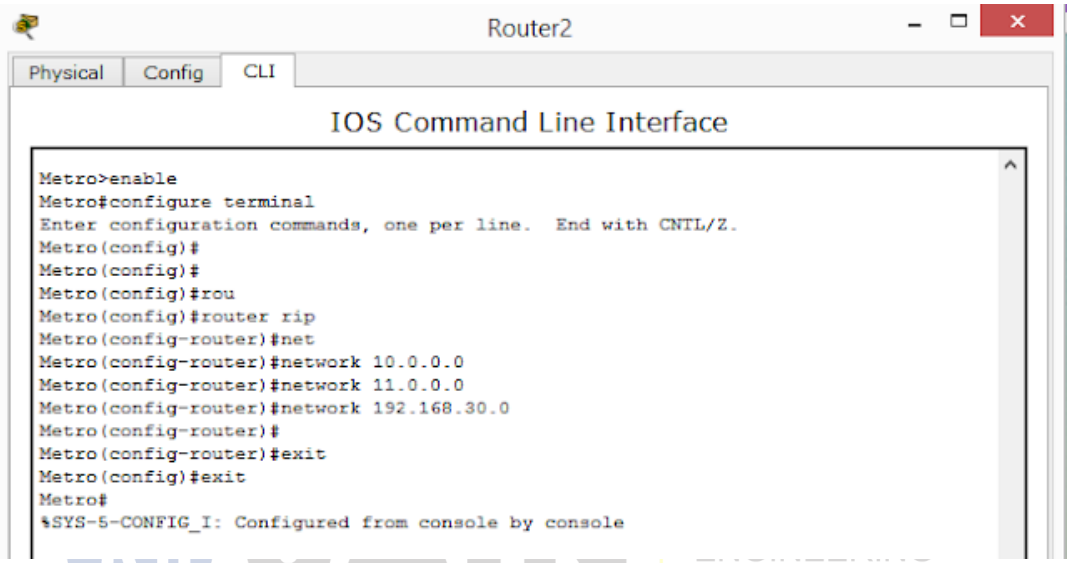
After configuring these IP addresses to the corresponding devices only, we should configure dynamic routing to the network.

When doing dynamic routing using RIP protocol first we should identify the networks which

are connected to each router and for those routers we have to connect those networks through RIP.

So below mentioned procedure will guide you to do the RIP dynamic routing.

1. Router 1 configuration steps.



The below figure shows us the routing table which is updating periodically.

C- directly connected networks are marked as C.

R- networks which connected using the RIP dyanamic routing

```
Metro#show ip ro
Metro#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, Serial0/2/0
C    11.0.0.0/8 is directly connected, Serial0/2/1
R    192.168.10.0/24 [120/1] via 10.0.0.100, 00:00:04, Serial0/2/0
R    192.168.20.0/24 [120/1] via 11.0.0.100, 00:00:16, Serial0/2/1
C    192.168.30.0/24 is directly connected, FastEthernet0/0
Metro#
```

Below two figures are showing us the **current running configurations** of the router 1.

```
Metro#show running-config
Building configuration...

Current configuration : 790 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Metro
!
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
```

```
interface FastEthernet0/0
 ip address 192.168.30.100 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/2/0
 ip address 10.0.0.200 255.0.0.0
 clock rate 64000
!
interface Serial0/2/1
 ip address 11.0.0.200 255.0.0.0
 clock rate 64000
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 network 10.0.0.0
 network 11.0.0.0
 network 192.168.30.0
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
line con 0
!
line aux 0
```

2. Router 2 configuration steps.

```
Malambe>enable
Malambe#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Malambe(config)#router rip
Malambe(config-router)#network 10.0.0.0
Malambe(config-router)#network 192.168.10.0
Malambe(config-router)#
Malambe(config-router)#exit
Malambe(config)#exit
Malambe#
%SYS-5-CONFIG_I: Configured from console by console

Malambe#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, Serial0/0/0
R    11.0.0.0/8 [120/1] via 10.0.0.200, 00:00:22, Serial0/0/0
C    192.168.10.0/24 is directly connected, FastEthernet0/0
R    192.168.20.0/24 [120/2] via 10.0.0.200, 00:00:22, Serial0/0/0
R    192.168.30.0/24 [120/1] via 10.0.0.200, 00:00:22, Serial0/0/0
Malambe#
```


3. Router 3 configuration steps.

```
Mathara>enable
Mathara#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Mathara(config)#router rip
Mathara(config-router)#network 11.0.0.0
Mathara(config-router)#network 192.168.20.0
Mathara(config-router)#
Mathara(config-router)#exit
Mathara(config)#exit
Mathara#
%SYS-5-CONFIG_I: Configured from console by console

Mathara#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R    10.0.0.0/8 [120/1] via 11.0.0.200, 00:00:13, Serial0/0/0
C    11.0.0.0/8 is directly connected, Serial0/0/0
R    192.168.10.0/24 [120/2] via 11.0.0.200, 00:00:13, Serial0/0/0
C    192.168.20.0/24 is directly connected, FastEthernet0/0
R    192.168.30.0/24 [120/1] via 11.0.0.200, 00:00:13, Serial0/0/0
Mathara#
```

After Configuring three routers as above mentioned, we can now send packets through one end to another. To check whether it is working we can check by ping command.

PING command can check the connection between two end devices and have to execute in terminal of the source device.

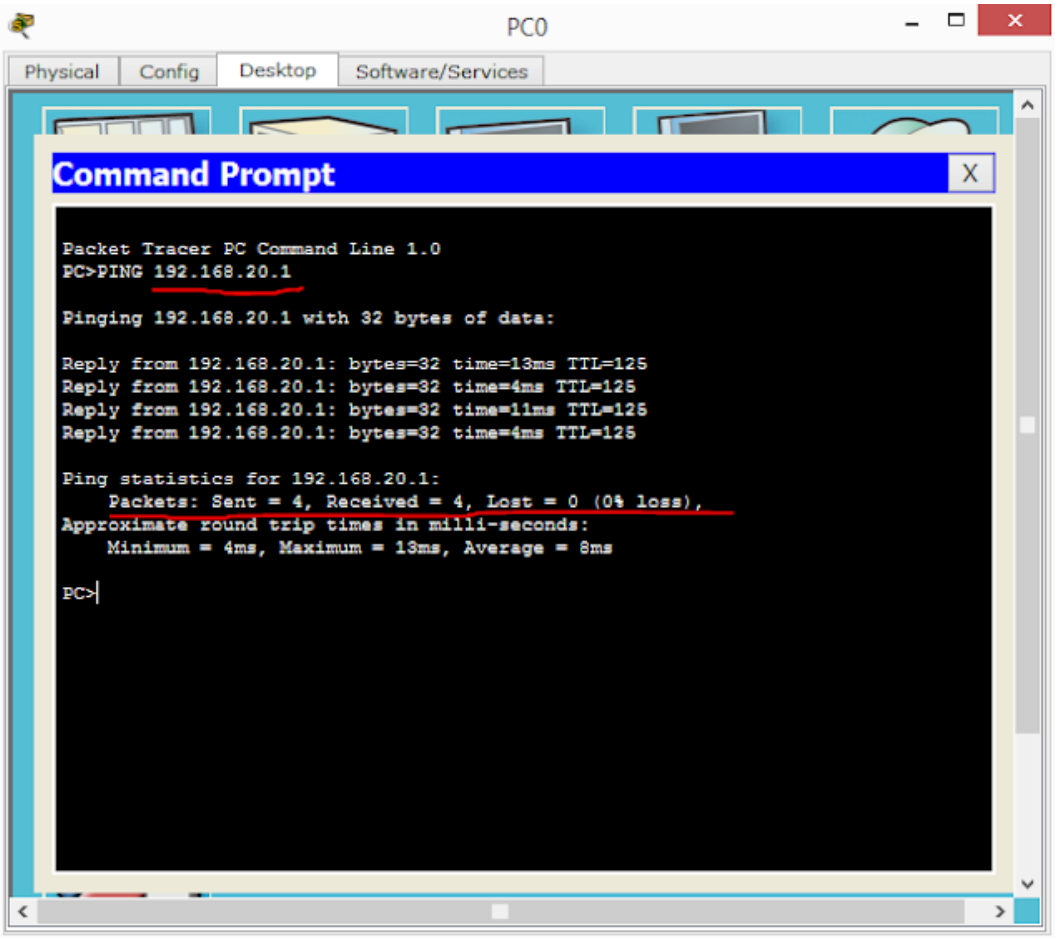
PING <IP address of the destination>

Now we will just get an example to demonstrate this scenario.So for that will take **PC 1** as the SOURCE DEVICE and **PC 3** as the DESTINATION DEVICE.

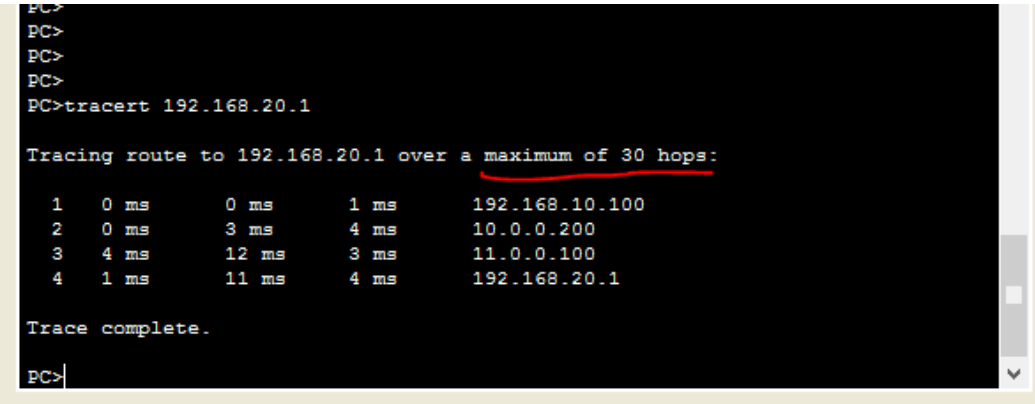
PC 1 IP- 192.168.10.1

PC 3 IP- 192.168.20.1

In Below figure we can see that the data packets transfer and the data packets which have lost their path.



In this figure it shows the path to the destination device(PC 3) from source device(PC 1). for this we are using **TRACERT <DESTINATION IP ADDRESS>**(TRACEROUTE) and it will show us the complete path and the time consumed to transfer data.



6.	Implementation of EIGRP	CO3

Enhanced Interior Gateway Routing Protocol (EIGRP) is an hybrid routing protocol possessing characteristics of both distance-vector and and link-state routing protocols. It was a proprietary Cisco routing protocol but Cisco decided to convert it to an open standard in 2013.

Let's see some **key features** that makes EIGRP helpful especially for large and complex networks.

- It supports both **IPv4** and **IPv6**
- Supports classless routing and **VLSM** (Variable Length Subnet Masking)
- Allows **route summarization** on any router in the network
- Supports **load balancing**
- Supports **MD5 authentication**

EIGRP uses a **multicast** address of 224.0.0.10 and uses Cisco's Reliable Transport Protocol (RTP) to send messages to the multicast address. It has a default **administrative distance** of 90, which is less than the default administrative distances of RIP and OSPF, implying that EIGRP routes will be preferred over RIP and OSPF routes.

For EIGRP, **routing metric** is calculated using bandwidth, delay, reliability and load.

EIGRP Neighborhood establishment

Before exchanging routing information, routers that run EIGRP must first become neighbors. EIGRP Routers send hello packets to the multicast address of 224.0.0.10 to dynamically discover neighbors on directly attached networks.

In order for routers in a network to become neighbors:

- They must be configured with the **same ASN** (Autonomous System Number). An autonomous system number is a group of EIGRP-enabled routers that should become EIGRP neighbors and exchange routes.
- The routers must also be using the **same parameters to calculate metric**.These parameters are called ***K* values** (components of metric). Just as we've seen, the K values are *bandwidth*,*delay*,*reliability* and *load*.

By default, the only parameters used to calculate EIGRP metric are **bandwith** and **delay**.The other two parameters are disabled by default ; so the network admin has to enable them on the router when desired for use.

EIGRP tables Explained

Each EIGRP router uses three tables to store routing information.

Neighborhood table -which stores information about EIGRP neighbors. Remember we said that routers need first to become neighbors before they can exchange routing information. A neighborhood table is thus used to keep neighborhood information such as the IP address of the neighbor, the local interface on which hellos were received , the hold down timer and others neighbor information.

Topology table– stores routing information learnt from neighbor routing tables. Every EIGRP route inside the autonomous system is stored here.The topology table also holds the metrics for each of the listed EIGRP routes, the feasible successor and the successor routes.

Routing table -Stores only the best routes to reach a remote network.

EIGRP configuration on a Router

Now we're ready to configure EIGRP. It is configured using these commands:

1. (config) router eigrp ASN – This command starts EIGRP on the router.In order to become EIGRP neighbors,routers must be configured with the same AS number.You can use any number between 1 and 65,535

2.(config-router) network SUBNET [WILCARD_MASK]. This command advertises a network directly connected to the router to other routers.

Let's configure this on Packet tracer

1.Build the network topology as shown below.

2. Do IP configurations on the PCs and the routers

Router1

R1(config)#

R1(config)#int fa0/0

R1(config-if)#ip add 10.0.0.1 255.0.0.0

R1(config-if)#no shut

R1(config-if)#int fa0/1

R1(config-if)#ip address 20.0.0.1 255.0.0.0

R1(config-if)#no shut

Router 2

R2(config)#

R2(config)#int fa0/0

R2(config-if)#ip add 30.0.0.1 255.0.0.0

R2(config-if)#no shutdown

R2(config-if)#int fa0/1

R2(config-if)#ip address 20.0.0.2 255.0.0.0

R2(config-if)#no shutdown

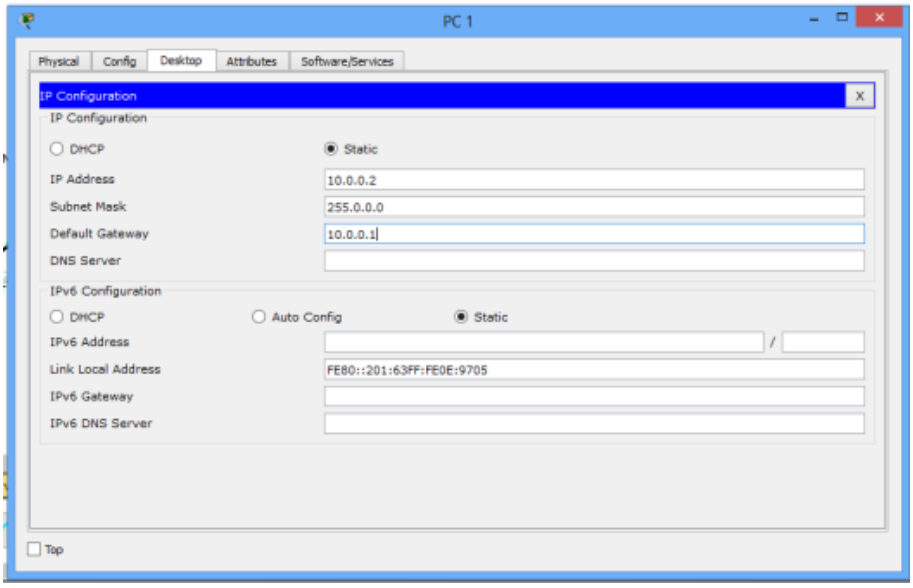
PC IP configuration

Click on **PC** ->**Desktop**->**IP configuration.** Here, fill in **static** IP addresses.

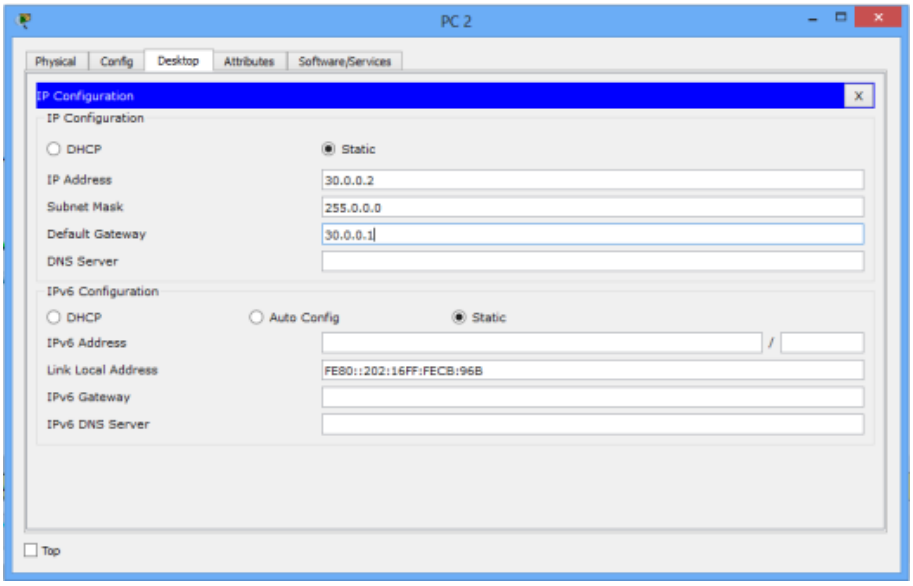
PC1 IP address: 10.0.0.2 **Subnet mask:** 255.0.0.0 **Default Gateway** 10.0.0.1

PC2 IP address: 30.0.0.2 **Subnet mask:** 255.0.0.0 **Default Gateway** 30.0.0.1

PC1



PC2



3. **Configure EIGRP on the routers**. Remember to use the **same ASN** number on both routers. Once configured, the routers become **EIGRP neighbors**.

Router 1:

R1(config)#

R1(config)#router eigrp 1

R1(config-router)#network 10.0.0.0

R1(config-router)#network 20.0.0.0

Router 2:

R2(config)#

R2(config)#router eigrp 1

R2(config-router)#network 20.0.0.0

R2(config-router)#network 30.0.0.0

You can see that we're simply enabling EIGRP on the routers, then advertising networks **directly connected to each router**. Simple!

4. Now **verify** EIGRP configuration.

First let's verify **EIGRP neighborhood** relationship of the routers.

Lets do this on **Router 1**

R1#

R1#show ip eigrp neighbors

Then observe the neighborhood:

```
R1#
R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address         Interface       Hold Uptime    SRTT   RTO   Q
Seq
                                    (sec)          (ms)       Cnt
Num
0   20.0.0.2        Fa0/1           12   00:05:27  40     1000  0
4

R1#
```

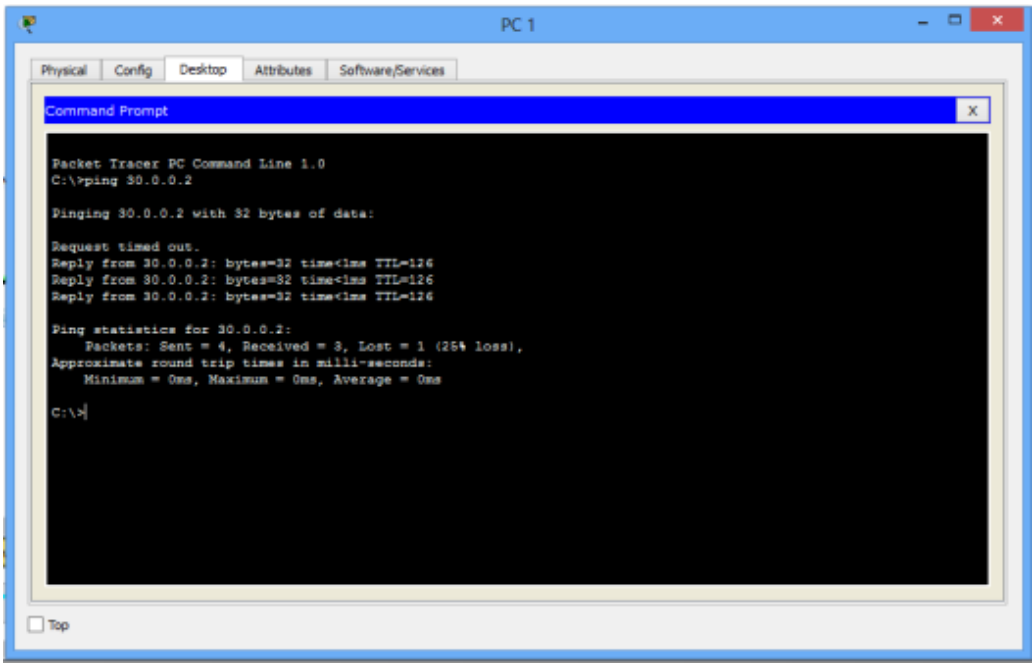
In the picture above,you can see that **R1** has a single neighbor with the IP address of 20.0.0.2

Secondly, we'll verify whether **R1** has received a route to reach the 30.0.0.0/8 network. We can use the *show ip route eigrp* command.

```
R1#show ip route eigrp
D    30.0.0.0/8 [90/30720] via 20.0.0.2, 01:33:56,
FastEthernet0/1
```


Lastly, let's ping **PC2** from **PC1**. Ping should succeed because. **R1** has learnt the route to 30.0.0.0/8 through EIGRP as denoted by letter **D**.

Try also to ping **PC1** from **PC2**. Ping should work.

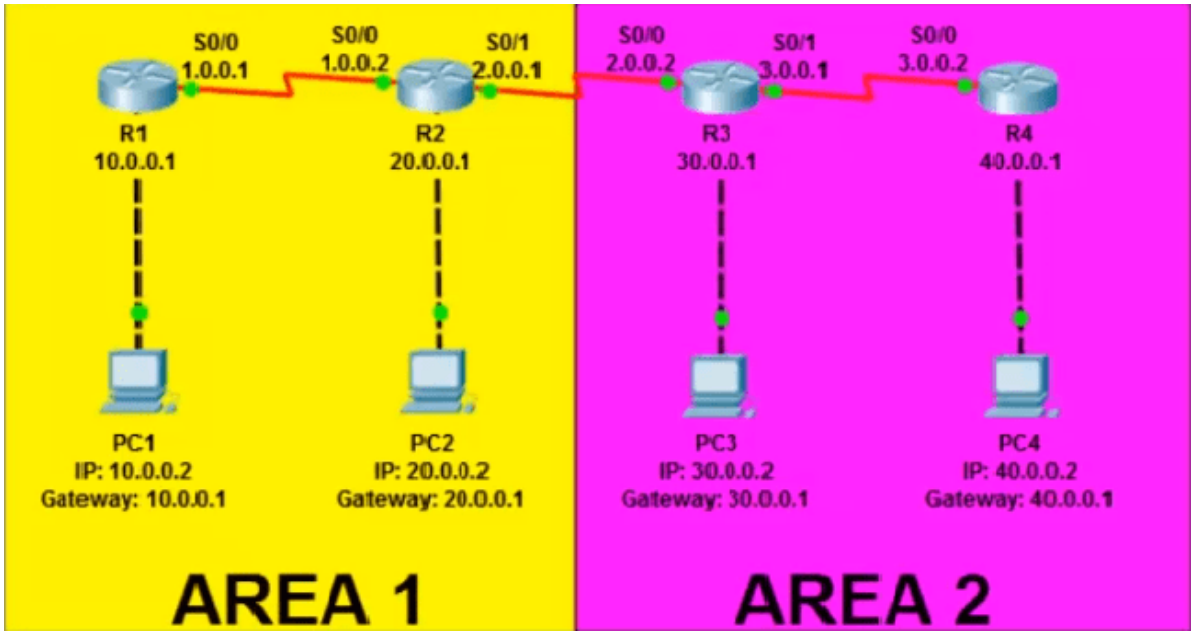


7.	Implementation of OSPF	CO3

OSPF stands for Open Shortest Path Fast. It is a link state routing protocol used to handle routing for IP traffic. Lets see

1. **How to configure OSPF in packet tracer**
2. **OSPF Configuration Commands Step by Step**
3. **OSPF Area Configuration**
4. **OSPF Troubleshooting Commands**
5. **Video Tutorial on how to configure OSPF in packet tracer.**

How to configure OSPF in Packet Tracer



So, in this example, we are going to take four Routers where one PC is connected to each. Router 1 and Router 2 belong to Area 1 and Router 3 and Router 4 belong to Area 2. OSPF Area Configuration we are going to do while configuring the route. Now, let's add IP Address on all the devices according to the picture given above.

Router 1 IP Configuration

Router>en

Router#conf t

Router(config)#int s0/0

Router(config-if)#ip add 1.0.0.1 255.0.0.0

Router(config-if)#clock rate 64000

Router(config-if)#no shut

Router(config-if)#int f0/0

Router(config-if)#ip add 10.0.0.1 255.0.0.0

Router(config-if)#no shut

Router 2 IP Configuration

Router>en

Router#conf t

Router(config)#int s0/0

Router(config-if)#ip add 1.0.0.2 255.0.0.0

Router(config-if)#no shut

Router>en

Router#conf t

Router(config)#int s0/1

Router(config-if)#ip add 2.0.0.1 255.0.0.0

Router(config-if)#clock rate 64000

Router(config-if)#no shut

Router(config-if)#int f0/0

Router(config-if)#ip add 20.0.0.1 255.0.0.0

Router(config-if)#no shut

Router 3 IP Configuration

Router>en

Router#conf t

Router(config)#int s0/0

Router(config-if)#ip add 2.0.0.2 255.0.0.0

Router(config-if)#no shut

Router>en

Router#conf t

Router(config)#int s0/1

Router(config-if)#ip add 3.0.0.1 255.0.0.0

Router(config-if)#clock rate 64000

Router(config-if)#no shut

Router(config-if)#int f0/0

Router(config-if)#ip add 30.0.0.1 255.0.0.0

Router(config-if)#no shut

Router 4 IP Configuration

Router>en

Router#conf t

Router(config)#int s0/0

Router(config-if)#ip add 3.0.0.2 255.0.0.0

Router(config-if)#no shut

Router(config-if)#int f0/0

Router(config-if)#ip add 40.0.0.1 255.0.0.0

Router(config-if)#no shut

So, this is how to add IP Address in Routers. Now add the IP Address and Gateway on PC according to the picture given above.

PC 1 IP Configuration

IP: 10.0.0.2

Subnet Mask: 255.0.0.0

Gateway: 10.0.0.1

PC 2 IP Configuration

IP: 20.0.0.2

Subnet Mask: 255.0.0.0

Gateway: 20.0.0.1

PC 3 IP Configuration

IP: 30.0.0.2

Subnet Mask: 255.0.0.0

Gateway: 30.0.0.1

PC 4 IP Configuration

IP: 40.0.0.2

Subnet Mask: 255.0.0.0

Gateway: 40.0.0.1

Now, its time to configure OSPF. Before that, let's understand the uses of the OSPF commands.

OSPF Routing Commands

Router ospf 10

This command allows you enable OSPF protocol on your router and number 10 is the process ID. You can give the process ID between 1 to 65,535.

Network 1.0.0.0 0.255.255.255 area 1

This command allows you to create a route in OSPF. Where **1.0.0.0** is the Network ID to which the router is connected to.

0.255.255.255 is a Wildcard Mask which is the complete inverse of **Subnet Mask**. The best way to find the wildcard mask is, just subtract the subnet mask from **255.255.255.255**. In this example, the default subnet mask for the class A IP address is 255.0.0.0. So we have subtracted it from 255.255.255.255 and got the wildcard mask as 0.255.255.255.

In the end, we have mentioned **area 1**. Here in OSPF, the area defines the complete different network. Two different Areas cannot communicate with each other directly. If you want

them to allow communication than you have to create an additional route that we are going to discuss in our next post.

OSPF Configuration Commands Step by Step

Configure OSPF in Router 1

Router#

Router#conf t

Router(config)#router ospf 10

Router(config-router)#network 1.0.0.0 0.255.255.255 area 1

Router(config-router)#network 10.0.0.0 0.255.255.255 area 1

Router(config-router)#^Z (Use **Ctrl + Z** to save settings)

Configure OSPF in Router 2

Router#

Router#conf t

Router(config)#router ospf 10

Router(config-router)#network 1.0.0.0 0.255.255.255 area 1

Router(config-router)#network 2.0.0.0 0.255.255.255 area 1

Router(config-router)#network 20.0.0.0 0.255.255.255 area 1

Router(config-router)#^Z

Configure OSPF in Router 3

Router#

Router#conf t

```
Router(config)#router ospf 10
Router(config-router)#network 2.0.0.0 0.255.255.255 area 2
Router(config-router)#network 3.0.0.0 0.255.255.255 area 2
Router(config-router)#network 30.0.0.0 0.255.255.255 area 2
Router(config-router)#^Z
```

Configure OSPF in Router 4

```
Router#
Router#conf t
Router(config)#router ospf 10
Router(config-router)#network 3.0.0.0 0.255.255.255 area 2
Router(config-router)#network 40.0.0.0 0.255.255.255 area 2
Router(config-router)#^Z
```


So guys, we have successfully configured the route on all the four Routers. Now, try to ping from PC 1 to all the PCs connected with different routers. You must be able to ping with PC 2 because it is in the same Area i.e. Area 1 as PC 1. and If you ping PC 3 and PC 4, you will get Destination Host Unreachable error because it is on different Area i.e. Area 2.

OSPF Troubleshooting Commands

1. **Show IP Protocol:** Tells you what protocol is configured in the **router**.
2. **Show IP Route:** Tells you all the available route via which the packet will reach the destination and also the network your router is directly connected to.
3. **Show IP Route OSPF:** Only display the best route according to OSPF.
4. **Show IP OSPF:** Display basic information about OSPF.
5. **Show IP OSPF Interface:** Display the current status of all the ports and their IP Address of a particular router.

6. **Show IP OSPF database:** Displays the link connected to the router and the router IDs of the neighboring routers.

8.	VLAN Configuration, Inter VLAN, VTP & Switch Troubleshooting	CO4

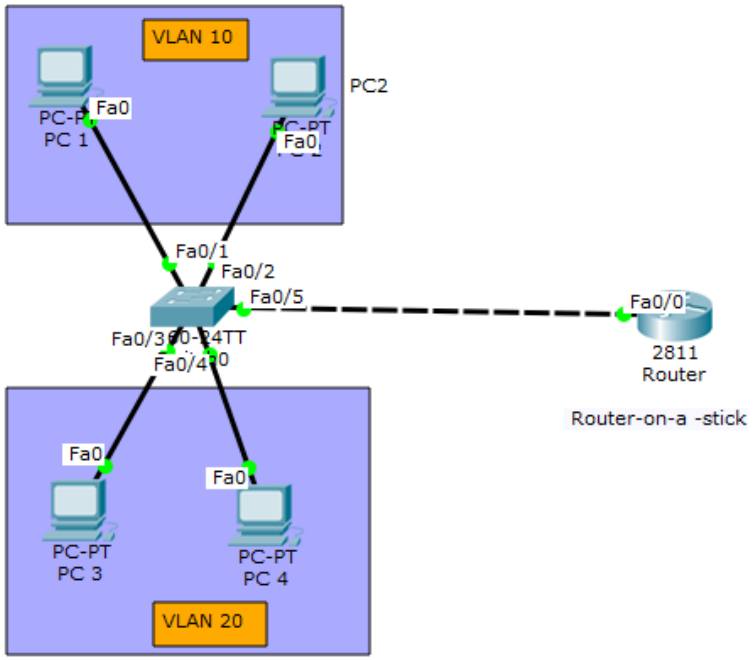
A Virtual LAN (**VLAN)** is simply a logical LAN, just as its name suggests. VLANs have similar characteristics with those of physical LANs, only that with VLANs, you can logically group hosts even if they are physically located on separate LAN segments.

We treat each VLAN as a separate subnet or broadcast domain. For this reason, to move packets from one VLAN to another, we have to use a router or a layer 3 switch.

VLANs are configured on switches by placing some interfaces into one broadcast domain and some interfaces into another. For this tutorial, we'll configure 2 VLANs on a switch. We'll then proceed and configure a router to enable communication between the two VLANs.

So then,

1. In Cisco Packet Tracer, **create the network topology** as shown below:



2. Create 2 VLANs on the switch: VLAN 10 and VLAN 20. You can give them custom names.

```
Switch#config terminal

Switch(config)#vlan 10

Switch(config-vlan)#name SALES

Switch(config-vlan)#vlan 20

Switch(config-vlan)#name IT
```

3. Assign switch ports to the VLANs. Remember each VLAN is viewed as separate broadcast domain.

And just before you configure, have in mind that switch ports could be either access or trunk.

- An *access port* is assigned to a single VLAN . These ports are configured for switch ports that connect to devices with a normal network card, for example a PC in a network.
- A *trunk port* on the other hand is a port that can be connected to another switch or router. This port can carry traffic of multiple VLANs.

So in our case, we'll configure switch interfaces fa 0/1 through fa 0/4 as access ports to connect to our PCs. Here, interfaces fa 0/1 and fa 0/2 are assigned to **VLAN 10** while interfaces fa 0/3 and fa 0/4 are assigned to **VLAN 20.**

Switch *Interface* fa0/5 will be configured as trunk port, as it will be used to carry traffic between the two VLANs via the router.

```
Switch>enable

Switch#config terminal
```

Switch(config)#int fa0/1

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 10

Switch(config-if)#int fa0/2

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 10

Switch(config-if)#int fa0/3

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 20

Switch(config-if)#int fa0/4

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 20

Worth noting: We could have configured all the above interfaces as access ports using *interface range* command as shown below:

Switch(config-if)#int range fa0/1-4

```
Switch(config-if-range)#switchport mode access
```

In the above commands, we have specified an interface range and then proceeded to configure all the ports specified as access ports.

Interface fa0/5 is configured as *trunk* and will be used to for inter-VLAN communication.

```
Switch(config)#int fa 0/5

Switch(config-if)#switchport mode trunk
```

The next thing is to:

4 . Assign static IP addresses to the four PCs which are located in the separate VLANs. PC1 and PC2 fall in VLAN 10 while PC3 and PC4 fall in VLAN 20.

PC1 IP address 192.168.1.10 **Subnet mask** 255.255.255.0 **Default gateway** 192.168.1.1

PC2: IP address 192.168.1.20 **Subnet mask** 255.255.255.0 **Default gateway** 192.168.1.1

PC3: IP address 192.168.2.10 **Subnet mask** 255.255.255.0 **Default gateway** 192.168.2.1

PC4: IP address 192.168.2.20 **Subnet mask** 255.255.255.0 **Default gateway** 192.168.2.1

And now it's very clear that we treat a VLAN just like a physical LAN when assigning IP addresses.

At this point let's try to test connectivity **within** VLANs and **between** VLANs

To test communication between hosts in the same VLAN:

Ping PC2 from PC1 both in VLAN 10. Ping test should be successful.

To test connectivity between hosts in different VLANs:

Ping PC3 in VLAN 20 from PC1 in VLAN 10. Ping here will definitely fail. Why? Because **inter-VLAN routing** is not yet enabled. Hope you can see how we've used VLANs to place the hosts into two logical networks which can be viewed as separate broadcast domains.

Now, in order to allow the hosts in the two VLANs to communicate, we need to do something extra. And you can guess what. We'll configure the router to permit inter-VLAN communication. Let's do that right away.

5. Configure inter-VLAN routing on the router

We'll configure the router so that it will enable communication between the two vlans via a single physical interface. How is this made possible? We'll divide the single physical interface on the router into logical interfaces (sub interfaces). Each sub-interface will then serve as a default gateway for each of the VLANs. This scenario is called **router on a stick** (R.O.A.S) and will allow the VLANs to communicate through the single physical interface.

Wort noting: We **can't** assign an IP address to the router's physical interface that we have subdivided into logical sub-interfaces. We'll instead assign IP addresses to the sub interfaces.

So let's do router configurations:

```
Router>enable

Router#config terminal
```

```
Router(config)#int fa0/0

Router(config-if)#no shutdown



Router(config-if)#int fa0/0.10

Router(config-subif)#encapsulation dot1q 10

Router(config-subif)#ip add 192.168.1.1 255.255.255.0

Router(config-subif)#



Router(config-subif)#int fa0/0.20

Router(config-subif)#encapsulation dot1q 20

Router(config-subif)#ip add 192.168.2.1 255.255.255.0
```


As you can notice from above, the routers physical interface fa0/0 was subdivided into two sub-interfaces(fa0/0.10 and fa0/0.20) , which are then configured as *trunk* interfaces and given IP addresses.

Finally,

6. Test **inter-VLAN** connectivity.

Here we'll test connectivity between computers in different VLANs . Don't forget that its the router that enables inter-VLAN routing.

Ping PC3 in **VLAN 20** from PC1 in **VLAN 10**. If everything is well configured, then ping should work perfectly

9.	Configuration of Access-lists - Standard	CO2

An Access Control List (or ACL or simply access list) is a security feature that allows you to filter the network traffic based on configured statements. An ACL can be used to filter either inbound or outbound traffic on an interface. Once you applied an access list on a router, the router examines every packet moving from one interface to another interface in the specified direction and takes the appropriate action. In this post, we will demonstrate the basics of ACL and how to **configure Standard ACL** on a Cisco router using Cisco Packet Tracer. The same steps can be used to configure Standard ACL in GNS3 or reach Cisco routers.

Types of ACL

An ACL can be either of the following two types.

1. **Standard access lists**

A Standard ACL can use only the source IP address in an IP packet to filter the network traffic. Standard access lists are typically used to permit or deny an entire host or network. They cannot be used to filter individual protocol or services such as FTP and Telnet. In the technical explanation, the standard ACL supports only source address.

2. **Extended access lists**

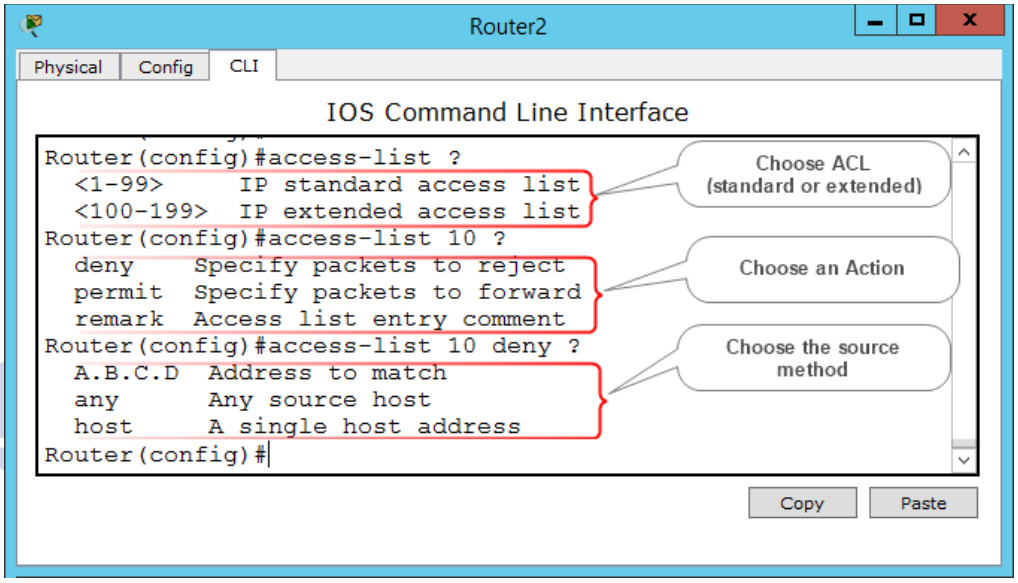
Extended access lists use the source as well as the destination addresses. An extended ACL can be used to filter a specific protocol or service. For example, you deny a host to access the Telnet program while permitting others services.

An ACL can be configured using either a number or a name. If you decide to use a name to configure an ACL, it is referred as Named ACL.

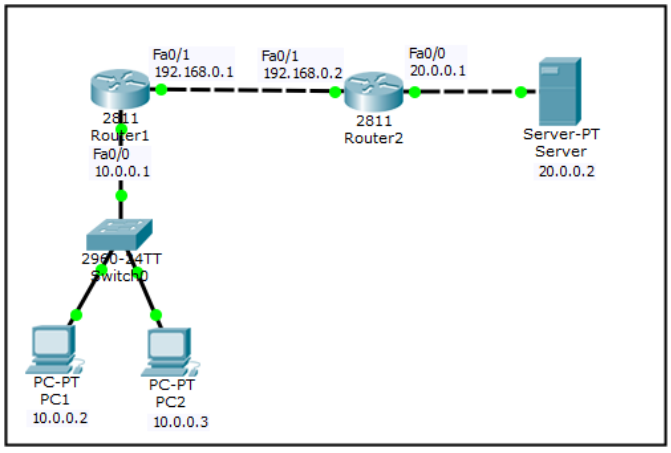
Configure Standard ACL

In this post, we will learn how to configure Standard ACL on Cisco routers. Before configuring an ACL, we would like to explain the command syntaxes used to configure it. As discussed earlier, you can either use the numbered ACL method or Named ACL method to configure an ACL.

The following figure shows the command syntax used to configure an ACL.



We will use the following topology to demonstrate how to configure ACL.



Once you have created the preceding topology, configure the appropriate IP addresses as mentioned in the topology. We assume that you are already familiar to configure IP addresses on Cisco devices. If you face any problem to configure IP addresses on the devices mentioned in the preceding topology, please visit the following link for step by step IP configuration.

Once you have configured appropriate IP addresses on the devices, use a routing method such as RIP. You can visit the following link to know how to configure RIP routing.

After configuring the IP addresses and RIP routing, open the Command Prompt on PC0, and type ping 20.0.0.2. You should be able to ping successfully.

Configure Standard ACL Step By Step

Let's see how to configure a Standard ACL. In this demonstration, we will restrict host 10.0.0.2 to access Router2. For this, we need to apply a standard ACL on the Fa0/1 interface to filter the incoming traffic.

1. First, execute the following command to deny host 10.0.0.2.

Router2(config)#access-list 10 deny host 10.0.0.2

2. When you deny a host on a router, the router will deny all the hosts until you explicitly define the list of permitted hosts. The following command will permit all the other hosts to access Router2.

Router2(config)#access-list 10 permit any

3. Next, switch to the interface on which you want to apply the ACL, in this case, Fa0/1, and define the direction (inbound or outbound) of traffic that you want to filter. In this case, we will filter the incoming packets on the Fa0/1 of Router2. To do so, execute the following commands.

Router2(config)#int fa0/1
Router2(config-if)#ip access-group 10 in

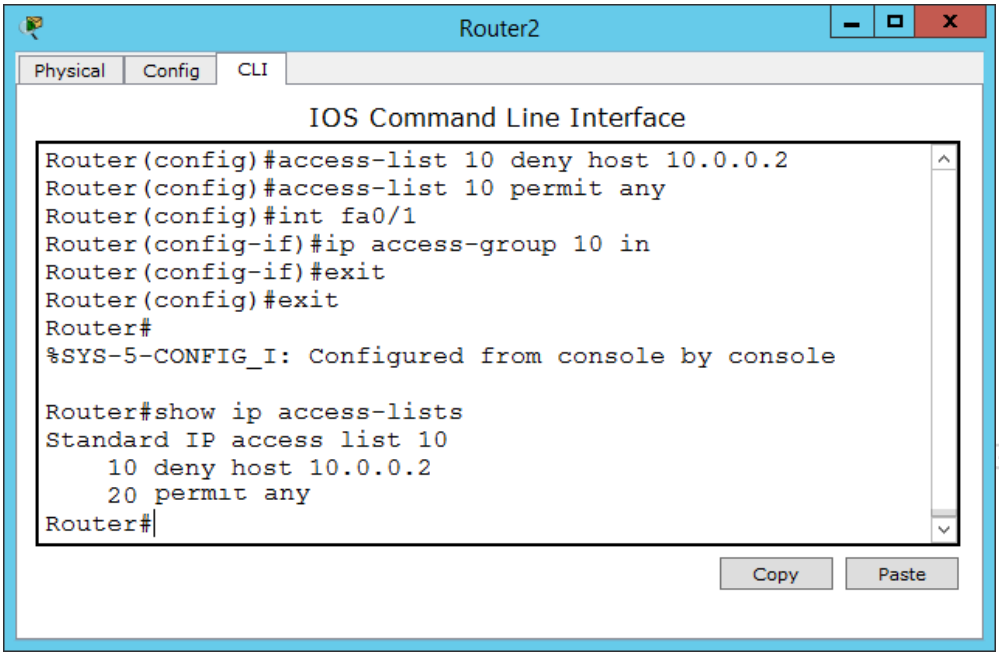
Router2(config-if)#exit

Router2(config)#exit

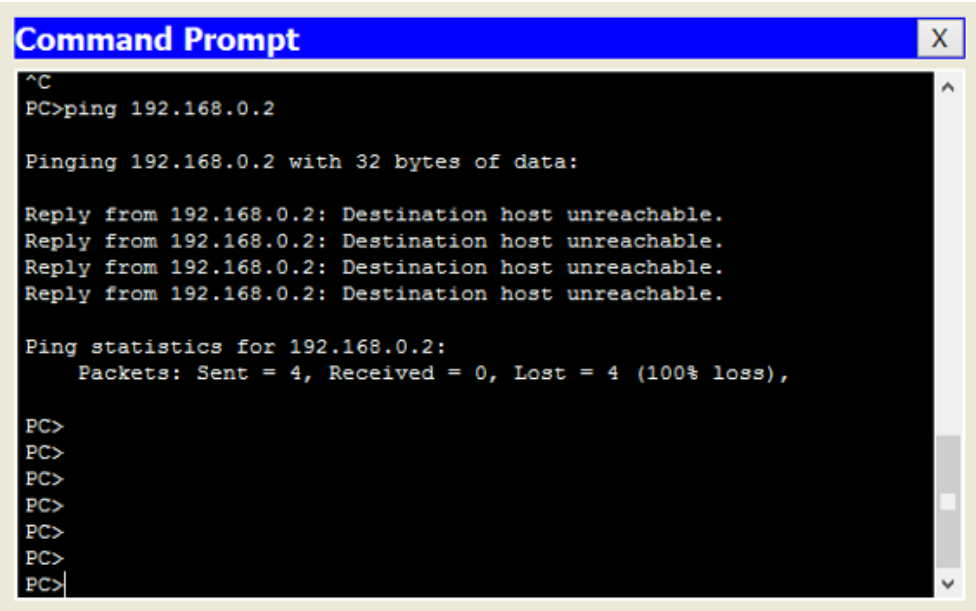
4. Once you applied an ACL on a router, execute the following command to view the applied ACLs.

Router2#show ip access-lists

The following figure shows the Standard ACL configuration of Router2.



5. Next, open the Command Prompt of PC0, try to ping 192.168.0.2. You should not be able to ping as shown in the following figure.



6. You can remove the configured ACLs if you want. To remove the ACL that we have configured, execute the following command on Router2.

Router2(config)#no access-list 10 deny host 10.0.0.2

7. Now, try to ping again from PC0 to Router2, this time, you should be able to ping successfully, because you have removed the applied ACL.

10.	Configuration of Access-lists - Extended ACLs	CO2

To be more precise when matching a certain network traffic, extended access lists are used. Extended access lists are more difficult to configure and require more processor time than the standard access lists, but they enable a much more granular level of control.

With extended access lists, you can evaluate additional packet information, such as:

- source and destination IP address
- type of TCP/IP protocol (TCP, UDP, IP…)
- source and destination port numbers

Two steps are required to configure an extended access list:

1. configure an extended access list using the following command:

(config) access list NUMBER permit|deny IP_PROTOCOL SOURCE_ADDRESS WILDCARD_MASK [PROTOCOL_INFORMATION] DESTINATION_ADDRESS WILDCARD_MASK PROTOCOL_INFORMATION

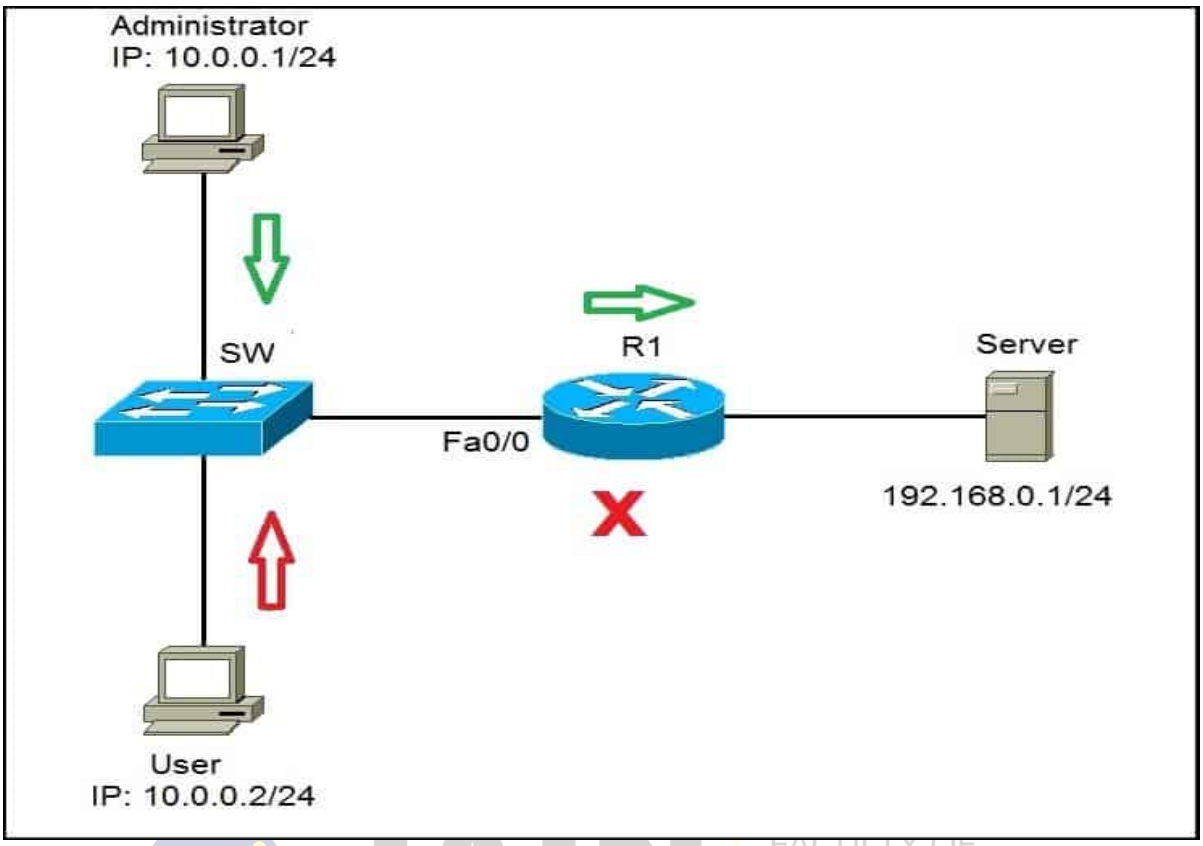
2. apply an access list to an interface using the following command:

(config) ip access-group ACL_NUMBER in | out

NOTE

Extended access lists numbers are in ranges from 100 to 199 and from 2000 to 2699. You should always place extended ACLs as close to the source of the packets that are being evaluated as possible.

To better understand the concept of extended access lists, consider the following example:



We want to enable the administrator's workstation (10.0.0.1/24) unrestricted access to Server (192.168.0.1/24). We will also deny any type of access to Server from the user's workstation (10.0.0.2/24).

First, we'll create a statement that will permit the administrator's workstation access to Server:

R1(config)#access-list 100 permit ip 10.0.0.1 0.0.0.0 192.168.0.1 0.0.0.0

Next, we need to create a statement that will deny the user's workstation access to Server:

R1(config)#access-list 100 deny ip 10.0.0.2 0.0.0.0 192.168.0.1 0.0.0.0

Lastly, we need to apply the access list to the **Fa0/0** interface on R1:

R1(config)#int f0/0

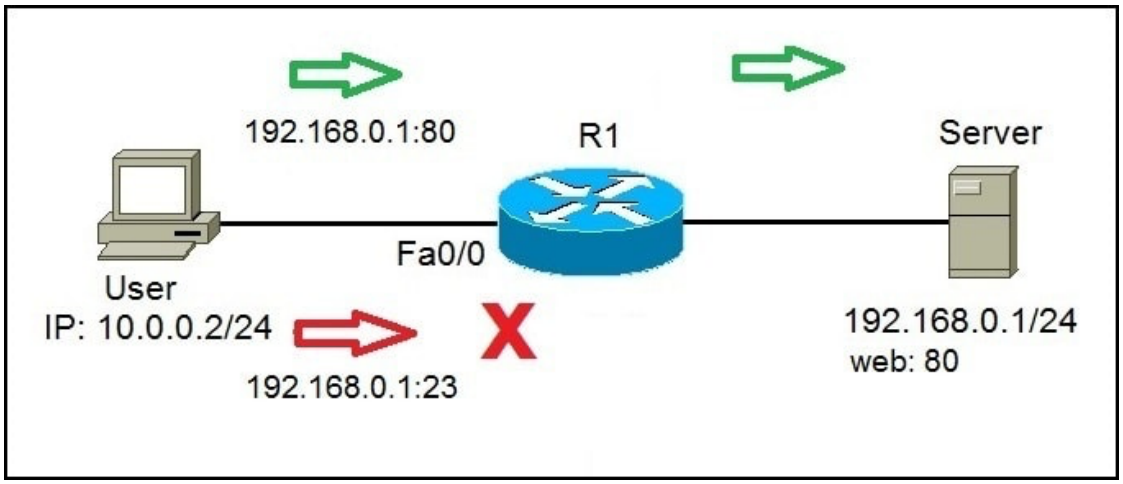
R1(config-if)#ip access-group 100 in

This will force the router to evaluate all packets entering Fa0/0. If the administrator tries to access Server, the traffic will be allowed, because of the first statement. However, if User tries to access Server, the traffic will be forbidden because of the second ACL statement.

NOTE

At the end of each access list there is an explicit **deny all** statement, so the second ACL statement wasn't really necessary. After applying an access list, every traffic not explicitly permited will be denied.

What if we need to allow traffic to Server only for certain services? For example, let's say that Server was a web server and users should be able to access the web pages stored on it. We can allow traffic to Server only to certain ports (in this case, port 80), and deny any other type of traffic. Consider the following example:



On the right side, we have a Server that serves as a web server, listening on port 80. We need to permit User to access web sites on S1 (port 80), but we also need to deny other type of access.

First, we need to allow traffic from User to the Server port of 80. We can do that using the following command:

R1(config)#access-list 100 permit tcp 10.0.0.2 0.0.0.0 192.168.0.1 0.0.0.0 eq 80

By using the *tcp* keyword, we can filter packets by the source and destination ports. In the example above, we have permitted traffic from 10.0.0.2 (User's workstation) to 192.168.0.1 (Server) on port 80. The last part of the statement, *eq 80*, specifies the destination port of 80.

Since at the end of each access list there is an implicit *deny all* statement, we don't need to define any more statement. After applying an access list, every traffic not originating from 10.0.0.2 and going to 192.168.0.1, port 80 will be denied.

We need to apply the access list to the interface:

R1(config)#int f0/0

R1(config-if)#ip access-group 100 in

We can verify whether our configuration was successful by trying to access Server from the User's workstation using different methods. For example, the ping will fail:

C:\>ping 192.168.0.1

Pinging 192.168.0.1 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 192.168.0.1:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)

Telnetting to the port 21 will fail:

C:\>telnet 192.168.0.1 21

Trying 192.168.0.1 ...

% Connection timed out; remote host not responding

However, we will be able to access Server on port 80 using our browser:

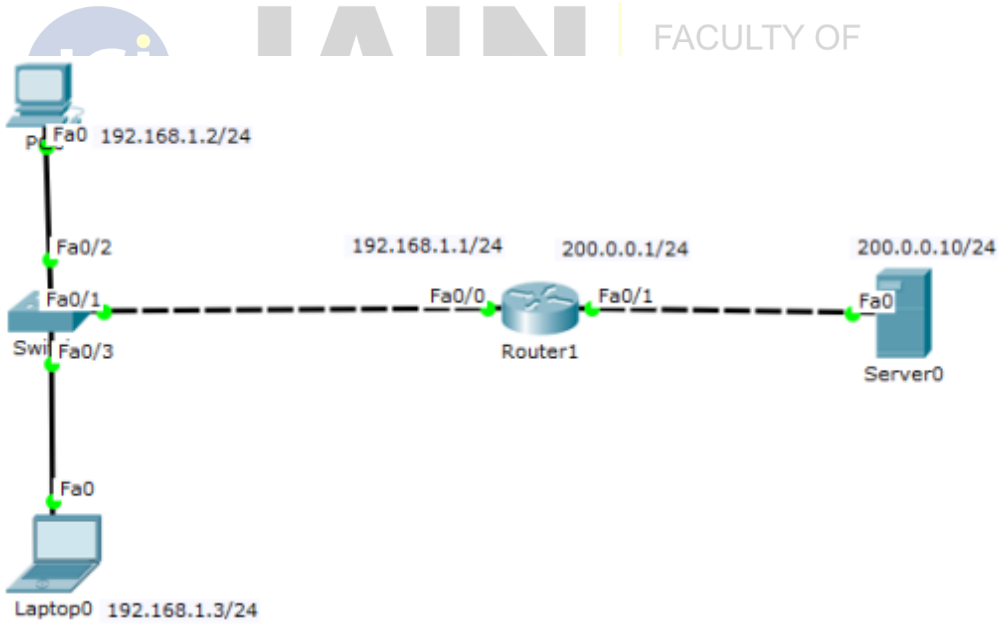
11.	Implementation of Network Address Resolution	CO5

Dynamic NAT maps a private IP address to a public IP address from a pool of public IP addresses. This is unlike static NAT in which one private IP address is translated into one public IP address.

In dynamic NAT, the router will dynamically pick a public address from the pool. The dynamic mapping entry will stay in the NAT translations as long as the traffic is being exchanged. Otherwise, after a period of no traffic flow, the global IP address will be reused for new translations.

Now, let's configure Dynamic NAT in Packet Tracer.

First build the network topology:



Then configure basic IP addressing on the router, the PC, laptop and the Server.

Router

Router(config)#int fa0/0

Router(config-if)#ip add 192.168.1.1 255.255.255.0

Router(config-if)#no shut

Router(config-if)#

Router(config-if)#int fa0/1

Router(config-if)#ip add 200.0.0.1 255.255.255.0

Router(config-if)#no shut

PC Ip add 192.168.1.2/24 Default gateway 192.168.1.1(int fa0/0)

Laptop **I**p add 192.168.1.3/24 Default gateway 192.168.1.1(int fa0/0)

Server IP add 200.0.0.10/24 Default gateway 200.0.0.1 (int fa0/1)

Now, to configure Dynamic NAT on the router we'll need to:

1.Configure the router's **inside address** using *ip nat inside* command.

2.Configure the router's **outside address** using *ip nat outside* command.

3.Create an **access list** of inside source source addresses to be translated.

4. Configure the pool of global IP addresses using the command *ip nat pool POOL_NAME FIRST_IP LAST _IP netmask SUBNET_MASK*

5. Enable dynamic NAT on the router using *ip nat inside source list ACL_NUMBER pool POOL_NAME*

Here are the dynamic NAT configurations:

Router(config)#int fa0/0

Router(config-if)#ip nat inside

Router(config-if)#

Router(config-if)#int fa0/1

Router(config-if)#ip nat outside

Router(config-if)#exit

Router(config-if)#access list 1 permit 192.168.1.0 0.0.5

Router(config)#ip nat pool mypool 155.21.21.10 155.21.21.15

netmask 255.255.0.0

Router(config)#ip nat inside source list 1 pool mypool

That's all for configurations. We now proceed to test whether the address translations are actually taking place. So then:

Ping the server from the PC to 'trigger' off dynamic NAT translations.

When the PC sends the server a request via the router, the router will first map the private IP address of the PC into a public IP address from the pool. The router will then forward the request to the server, with the public IP address of the PC as the source address.

When the server responds with a packet destined for the PC,the router will look into its dynamic NAT table and translate the public IP of the PC to the private one, then forward the packet to the PC via the *ip NAT inside* interface (int fa0/0).

Now let's verify dynamic NAT translations in the router using *show ip nat translations* command:

```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local
Outside global
icmp 155.21.21.10:10   192.168.1.2:10     200.0.0.10:10
200.0.0.10:10
icmp 155.21.21.10:11   192.168.1.2:11     200.0.0.10:11
200.0.0.10:11
icmp 155.21.21.10:12   192.168.1.2:12     200.0.0.10:12
200.0.0.10:12
icmp 155.21.21.10:9    192.168.1.2:9      200.0.0.10:9
200.0.0.10:9
```

From the command output in the picture above, you can see that the private IP address of the PC (**inside local**) has been translated to the first public address from the pool(**outside local**).

NAT is an important **security** technique of hiding your private site from access to outside networks. From the topology above, we can take the PC and laptop to be in our private LAN. Since we're using private addresses in the LAN, and given that private IP addresses are not unique to any organization, then this makes it difficult for a user outside the LAN to access the PC without knowing the private IP addresses being used in the this private site.

12.	Implementation of HSRP	CO6

HSRP (Hot Standby Router Protocol) is a redundancy protocol for setting up a fault-tolerant default gateway in a LAN environment. This is a Cisco proprietary protocol. The standard protocol is VRRP (Virtual Router Redundancy Protocol)

The primary router with the highest configured priority operates as a virtual router with a virtual gateway IP address. It responds to the ARP request from PC or servers connected to the LAN with the MAC address 0000.0c07.acXX where XX is the HSRP group ID (converted to an hexadecimal value). If the primary router should fail, the Cisco router with the next-highest priority available in the LAN segment would take over the gateway IP address and answer ARP requests with the same mac address, thus achieving transparent default gateway fail-over.

Update : HSRP version 2 is now supported in Cisco Packet Tracer 7.2.1

Key differences between HSRP v1 &v2

HSRP v1 & v2 share a lot of similarities, like the core functions of HSRP, but HSRP v2 brings some protocol improvements you need to be aware as a network engeneer :

- **Millisecond timer values**, which were not advertised by HSRP v1. In HSRP v2,the value is adverdised to make sure that the timer configuration is consistent accross the members of a standby group.
- **Group numbers range**, which has been increaed to 4096 groups (0 to 4095) in HSRP v2.
- Multicast address : HSRP v1 uses 224.0.0.2 whereas HSRP v2 now uses 224.0.0.102. The multicast address has been changed because of a conflict with CGMP (Cisco Group Management Protocol) which helps to direct multicast traffic but also uses 224.0.0.2 multicast address

HSRP in Packet Tracer 7.2.1

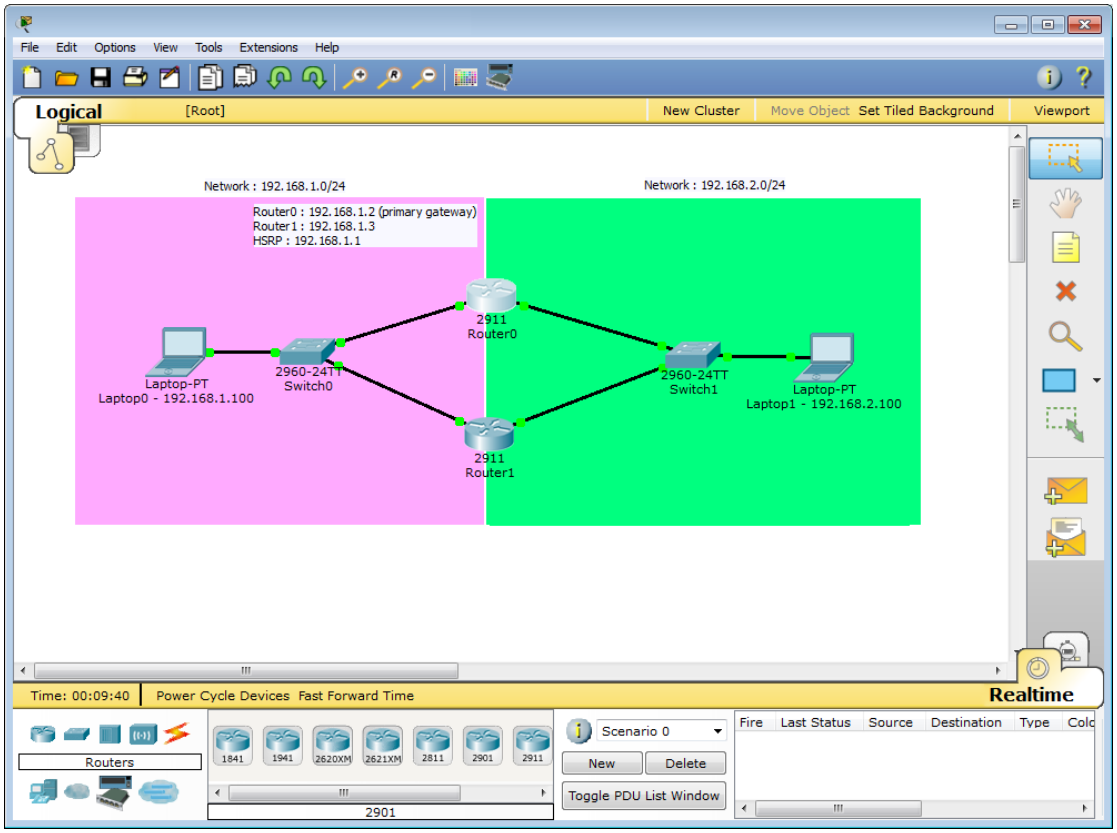
HSRP feature has been introduced in Packet Tracer 6.0. This protocol can be configured on every Cisco router available in Packet Tracer as well as on Cisco Catalyst 3560 layer 3 switch. HSRP preemption and interface tracking are supported in Packet Tracer 7.2.1

The following IOS commands are available :

- standby <0-4095> ip Enable HSRP and set the virtual IP address
- standby <0-4095> preempt Overthrow lower priority Active routers

- standby <0-4095> priority Priority level
- standby <0-4095> timers Hello and hold timers
- standby <0-4095> track Priority Tracking
- standby version <1-2> HSRP version

HSRP configuration using Cisco 2911 ISR routers



Two network are configured for this tutorial :

- Network 192.168.1.0/24
  - Router0 : 192.168.1.2 (GigabitEthernet 0/0)
  - Router1 : 192.168.1.3 (GigabitEthernet 0/0)

- Network 192.168.2.0/24
  - Router0 : 192.168.2.2 (GigabitEthernet 0/1)
  - Router1 : 192.168.2.3 (GigabitEthernet 0/1)

Two HSRP groups are configured on the ISR routers :

- HSRP Group 1 :
  - IP address : 192.168.1.1
  - Router0 with priority 120 (preemption enabled)
  - Router1 with HSRP default priority (100)

- HSRP Group 2 :
  - IP address : 192.168.2.1
  - Router0 with priority 120 (preemption enabled)
  - Router1 with HSRP default priority (100)

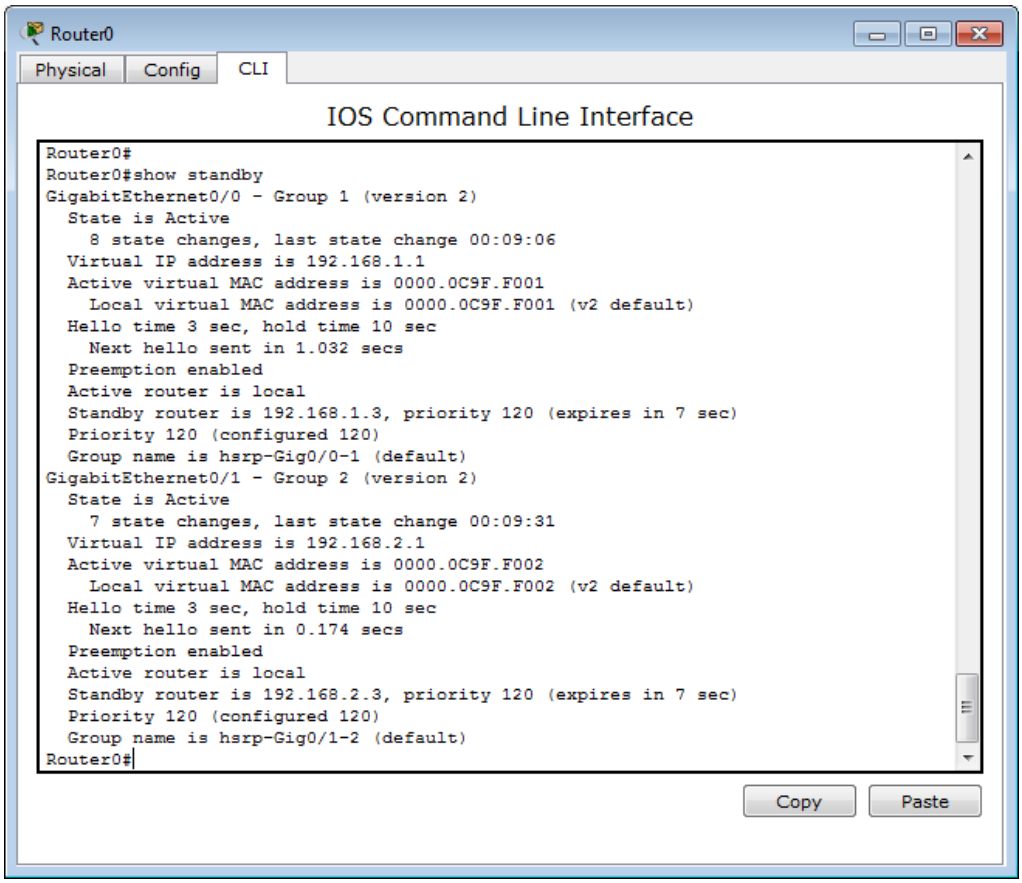
Cisco ISR routers configuration

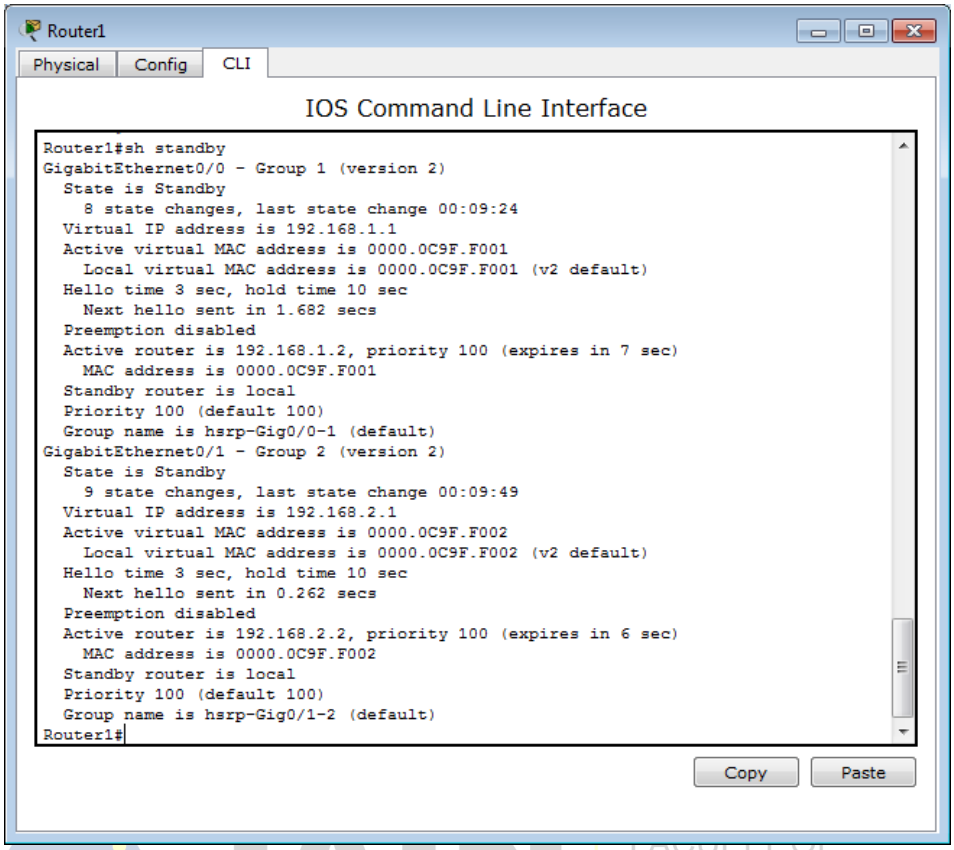
Router0 configuration	**Router1 configuration**
interface GigabitEthernet0/0 ip address 192.168.1.2 255.255.255.0 duplex auto speed auto standby version 2 standby 1 ip 192.168.1.1 standby 1 priority 120 standby 1 preempt ! interface GigabitEthernet0/1 ip address 192.168.2.2 255.255.255.0 duplex auto speed auto standby version 2 standby 2 ip 192.168.2.1 standby 2 priority 120 standby 2 preempt	interface GigabitEthernet0/0 ip address 192.168.1.3 255.255.255.0 duplex auto speed auto standby version 2 standby 1 ip 192.168.1.1 ! interface GigabitEthernet0/1 ip address 192.168.2.3 255.255.255.0 duplex auto speed auto standby version 2 standby 2 ip 192.168.2.1

Preemption is configured on Router0 using the **standby X preempt** commands. This router will always assume HSRP active state when it's online and if it has the highest HSRP priority in the network. The same

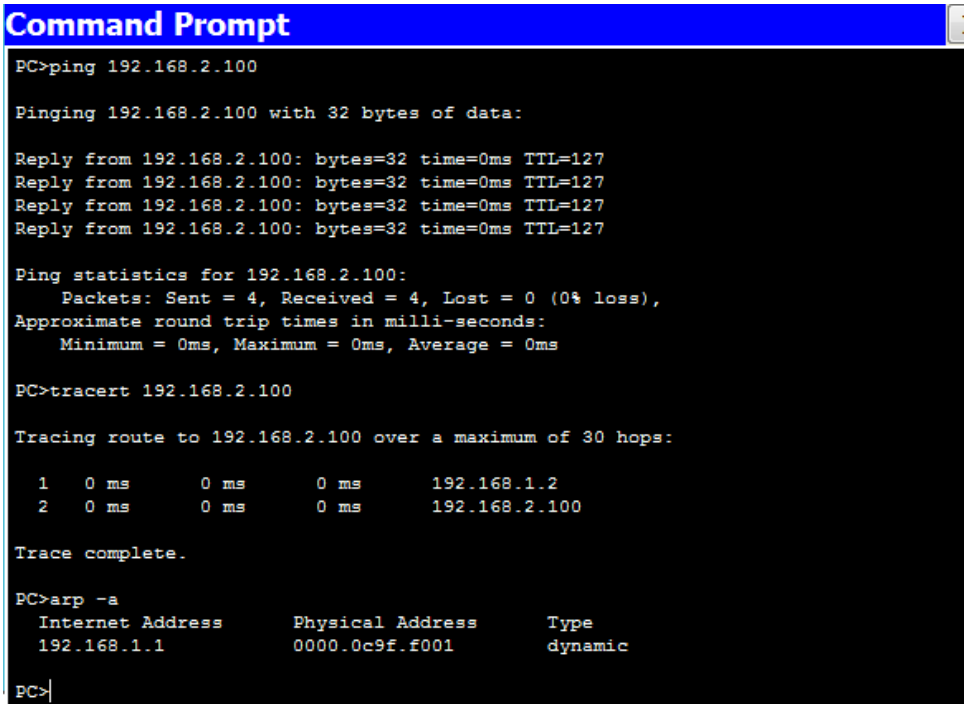
configuration without the **standby x priority 120** configuration on Router0 does not work and Router1 assumes the active state because it has a higher IP address configured.

Testing the configuration





Router0 is active for both HSRP groups. Both routers detected each other correctly but the priority seems to be wrong (**Standby router is 192.168.1.3, priority 120** should be **Standby router is 192.168.1.3, priority 100** on Router0**)**



Ping, traceroute and arp commands issued on Laptop0 confirms that the configuration is working. The IP packets are transiting through Router0 (192.168.1.2)

HSRP configuration using Cisco catalyst 3560 and 3650 switches

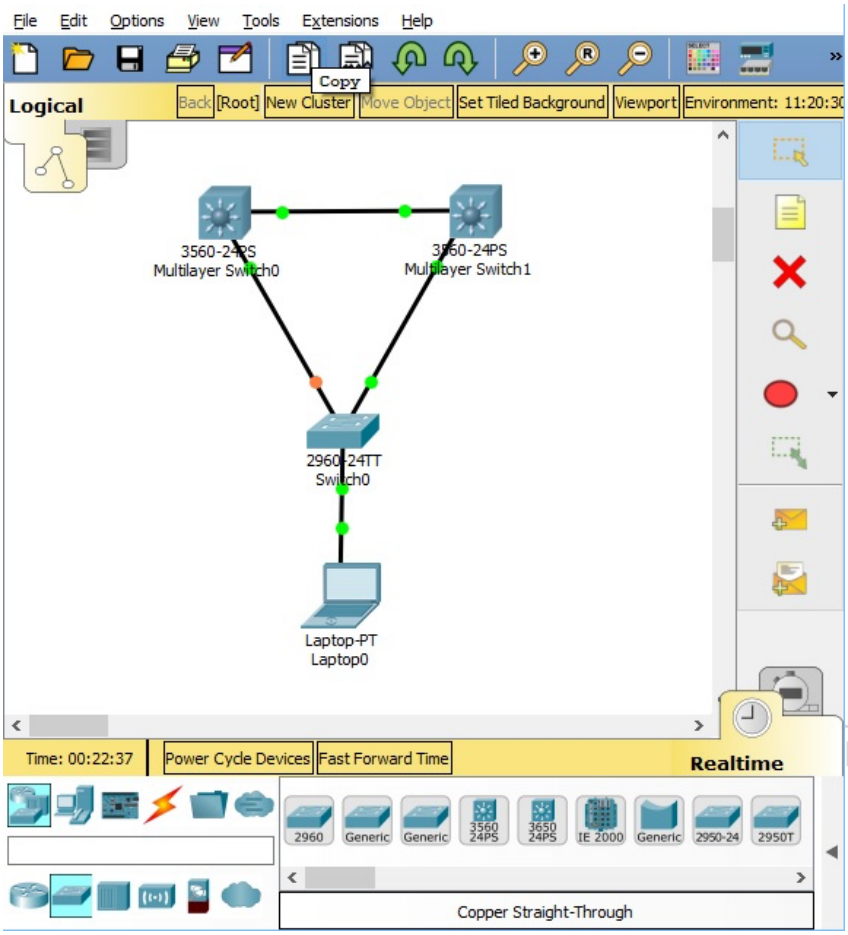
HSRP can be configured in the same way in Cisco catalyst 3560 and 3650 multilayer switch vlan interfaces using Cisco Packet Tracer.

The **standby version** command is now emulated in Catalyst layer 3 switches in Cisco Packet Tracer 7.2.1

```
interface Vlan100
 ip address 192.168.1.2 255.255.255.0
 standby 1 ip 192.168.1.1
 standby 1 preempt
 standby version 2
!
interface Vlan200
 ip address 192.168.2.2 255.255.255.0
 standby 2 ip 192.168.2.1
```

standby 2 preempt

standby version 2



Packet Tracer 7.1.1 HSRP configuration with catalyst 3560 switch