CONTENTS

EXPERIMENT-1

AIM - To implement the star topology using cisco packet tracer

STAR TOPOLOGY -A star may be a topology for a Local Area Network (LAN) during which all nodes are individually connected to a central connection point, sort of a hub or a switch. A star takes more cable than e.g. a bus, but the benefit is that if a cable fails, just one node is going to be brought down. Each device within the network is connected to a central device called a hub. If one device wants to send data to another device, it's to first send the info to the hub then the hub transmits that data to the designated device.

OBJECTIVE - To reduce the impact of a transmission line failure by independently connecting each host to the hub.

ADVANTAGES -

- It is very reliable – if one cable or device fails then all the others will still work
- It is high-performing as no data collisions can occur
- Less expensive because each device only needs one I/O port and wishes to be connected with a hub with one link.
- Easier to put in
- Robust in nature
- Easy fault detection because the links are often easily identified.
- No disruptions to the network when connecting or removing devices.
- Each device requires just one port i.e. to attach to the hub.
- If N devices are connected to each other in star, then the amount of cables required to attach them is N. So, it's easy to line up.

DISADVANTAGES-

- Requires more cable than a linear bus .
- If the connecting network device (network switch) fails, nodes attached are disabled and can't participate in network communication.

- More expensive than linear bus topology due to the value of the connecting devices (network switches)
- If the hub goes down everything goes down, none of the devices can work without a hub.
- Hubs require more resources and regular maintenance because it's the central system of the star .
- Extra hardware is required (hubs or switches) which adds to cost
- Performance is predicated on the one concentrator i.e. hub.

LIMITATIONS-

- The cable length is limited. ...
- It is suitable for networks with low traffic. ...
- It is heavily dependent on the central bus. ...
- It is not easy to isolate faults in the network nodes.

DIAGRAM-

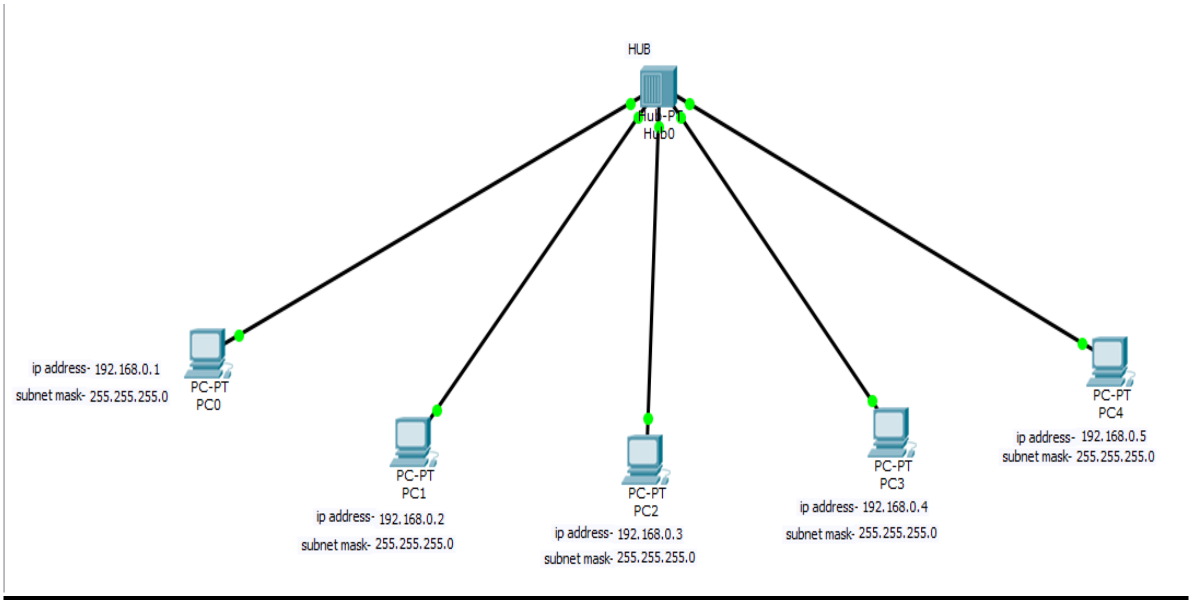
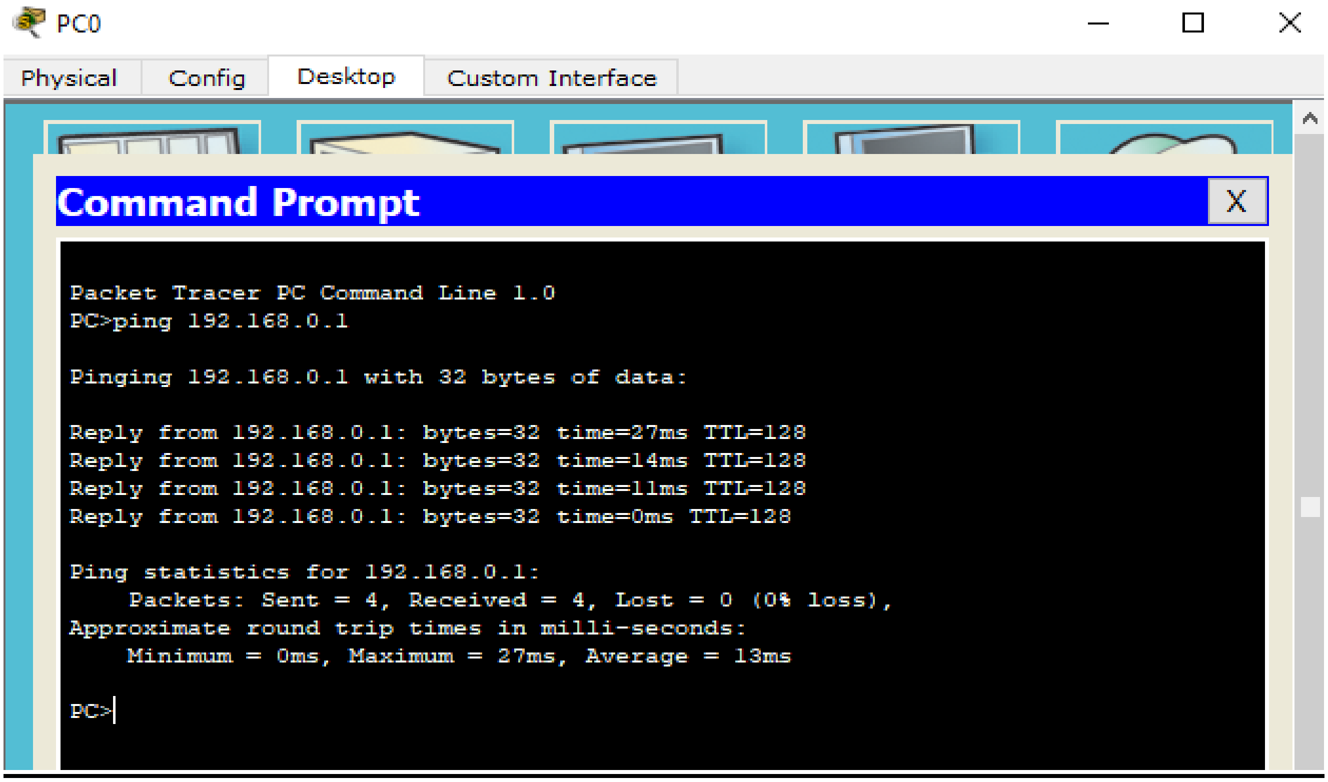


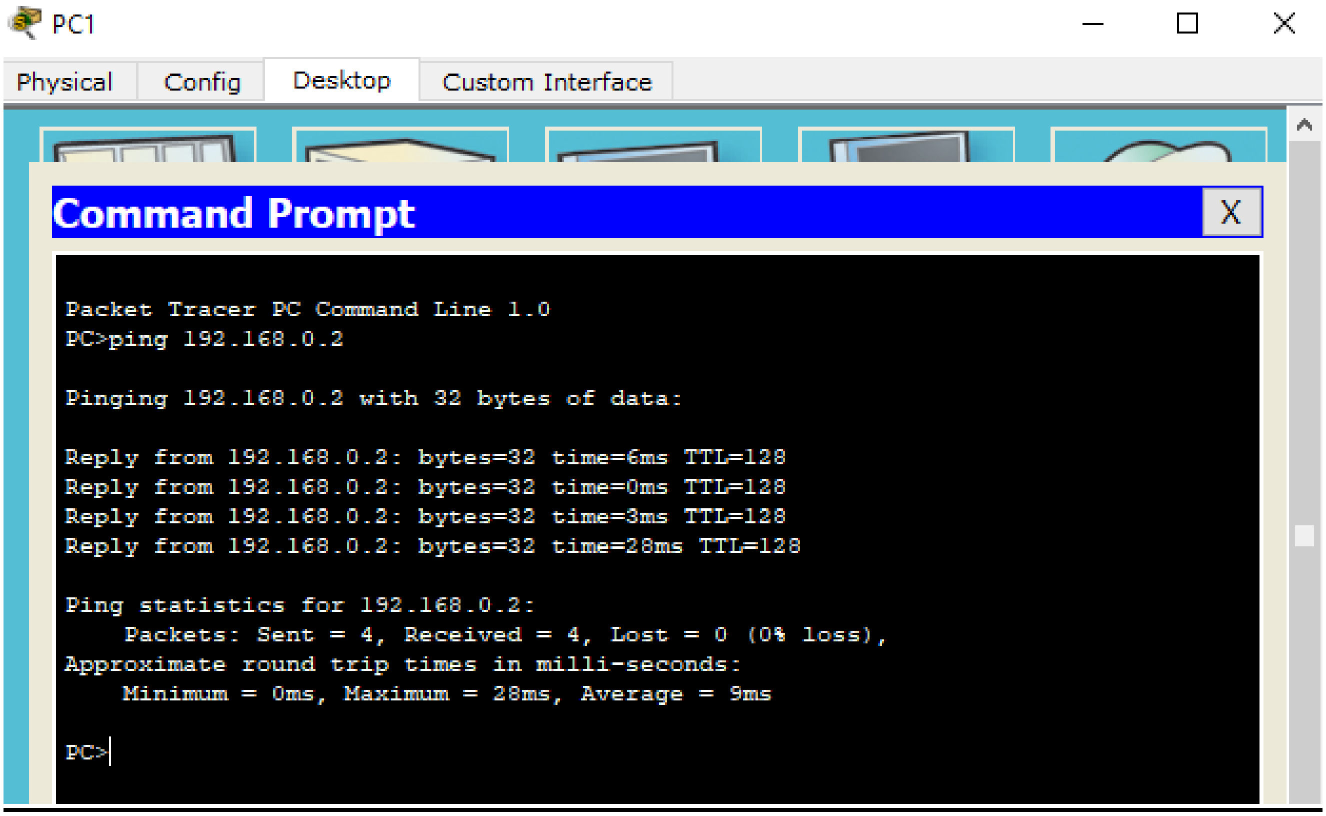
TABLE-

S.NO	PC NAME	IP ADDRESS	SUBNET MASK
1.	PC0	192.168.0.1	255.255.255.0
2.	PC1	192.168.0.2	255.255.255.0
3.	PC2	192.168.0.3	255.255.255.0
4.	PC3	192.168.0.4	255.255.255.0
5.	PC4	192.168.0.5	255.255.255.0

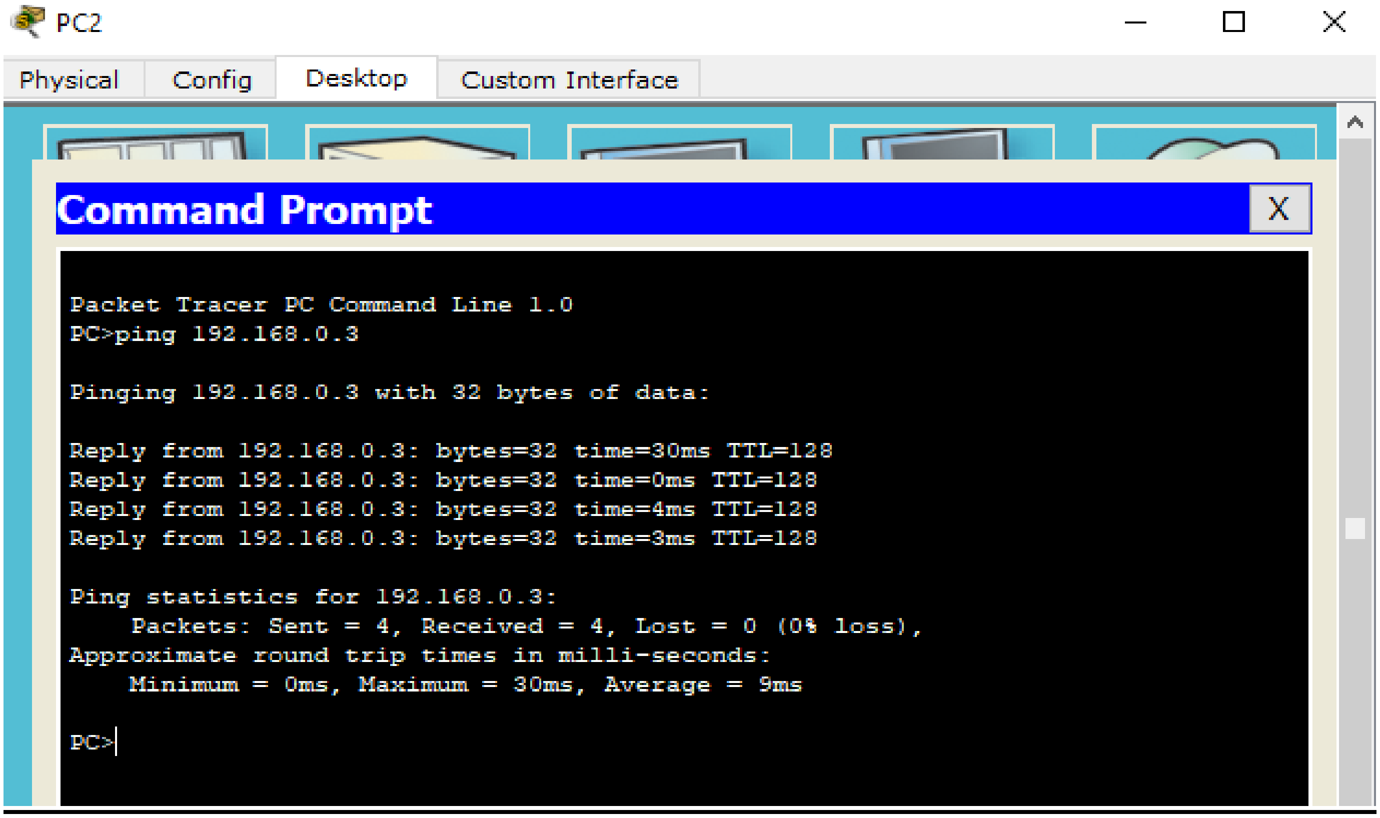
PING -



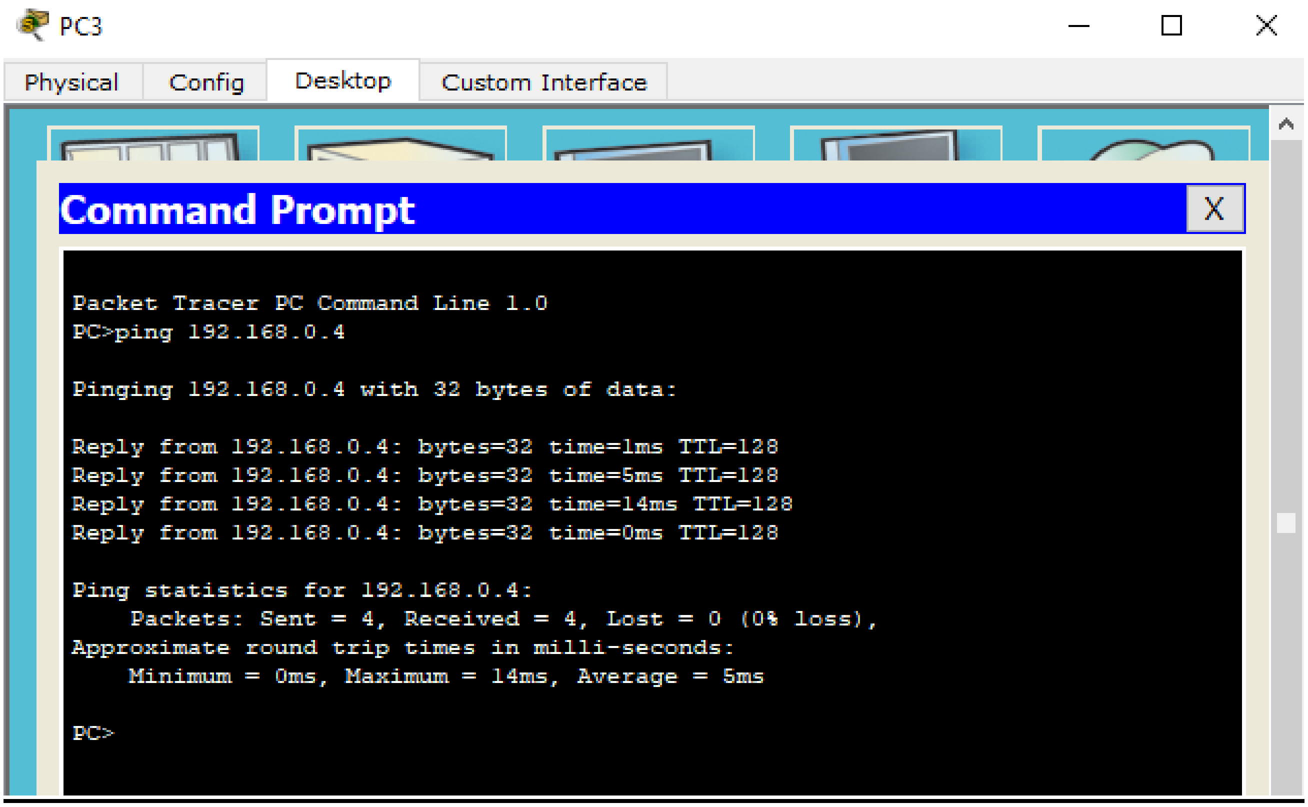
```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=27ms TTL=128
Reply from 192.168.0.1: bytes=32 time=14ms TTL=128
Reply from 192.168.0.1: bytes=32 time=11ms TTL=128
Reply from 192.168.0.1: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 27ms, Average = 13ms

PC>
```



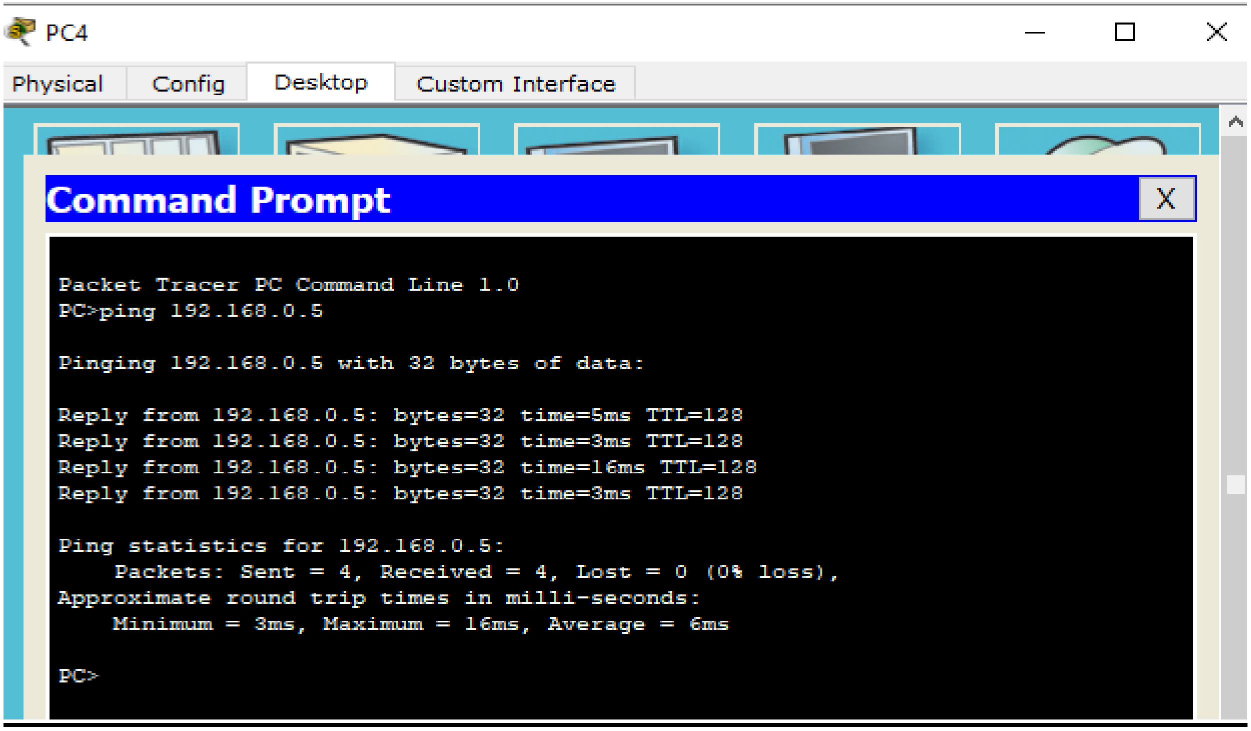
```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.0.2

Pinging 192.168.0.2 with 32 bytes of data:

Reply from 192.168.0.2: bytes=32 time=6ms TTL=128
Reply from 192.168.0.2: bytes=32 time=0ms TTL=128
Reply from 192.168.0.2: bytes=32 time=3ms TTL=128
Reply from 192.168.0.2: bytes=32 time=28ms TTL=128

Ping statistics for 192.168.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 28ms, Average = 9ms

PC>
```



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:

Reply from 192.168.0.3: bytes=32 time=30ms TTL=128
Reply from 192.168.0.3: bytes=32 time=0ms TTL=128
Reply from 192.168.0.3: bytes=32 time=4ms TTL=128
Reply from 192.168.0.3: bytes=32 time=3ms TTL=128

Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 30ms, Average = 9ms

PC>
```



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.0.4

Pinging 192.168.0.4 with 32 bytes of data:

Reply from 192.168.0.4: bytes=32 time=1ms TTL=128
Reply from 192.168.0.4: bytes=32 time=5ms TTL=128
Reply from 192.168.0.4: bytes=32 time=14ms TTL=128
Reply from 192.168.0.4: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 14ms, Average = 5ms

PC>
```



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.0.5

Pinging 192.168.0.5 with 32 bytes of data:

Reply from 192.168.0.5: bytes=32 time=5ms TTL=128
Reply from 192.168.0.5: bytes=32 time=3ms TTL=128
Reply from 192.168.0.5: bytes=32 time=16ms TTL=128
Reply from 192.168.0.5: bytes=32 time=3ms TTL=128

Ping statistics for 192.168.0.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 16ms, Average = 6ms

PC>
```

<u>RESULT</u> - Successful implementation of Star Topology

EXPERIMENT-2

AIM- Implementation of static routing using cisco packet tracer

ROUTING - Routing is the process of selecting a path for traffic in a network or between or across multiple networks. ... Packet forwarding is the transit of network packets from one network interface to another. Intermediate nodes are typically network hardware devices such as routers, gateways, firewalls, or switches. Routing is performed in two different ways :-

1. **Static routing**
2. **Dynamic routing**

STATIC ROUTING -

>> Static routing is a type of network routing technique. Static routing is not a routing protocol; instead, it is the manual configuration and selection of a network route, usually managed by the network administrator. It is employed in scenarios where the network parameters and environment are expected to remain constant.

>> Static routing is only optimal in a few situations. Network degradation, latency and congestion are inevitable consequences of the non-flexible nature of static routing because there is no adjustment when the primary route is unavailable.

OBJECTIVE - To help transfer routing information from one routing protocol to another (routing redistribution).

ADVANTAGES -

1. 1.Predictability-The path that static routing takes to the destination is very predictable. Even if there is a change in the network design and layout, there won't be any changes in the router. The users always know where the path is going to be.

2. Network Overheads

Unlike dynamic routing, static routing does not contain any overheads ; almost zero. Therefore, routers and network links don't get imposed overhead.

3. Configurations

Configuring networks that are small is relatively easy compared to a large network. The network administrator only has to apply changes to each router so that they can reach their respective network segments. These network segments are not directly attached to the router.

4. Resource Requirement

Static routing requires very less resources. Extra resources such as CPU and memory are not needed here.

5. Bandwidth

Static routing does not use any CPU cycles for the communication purposes. Hence, it imposes less load on the router CPU. This makes them consume less bandwidth compared to a dynamic routing protocol.

DISADVANTAGES -

1. Maintenance

Configuration of a network is only easier when the network is small, whenever the size increases the complexity grows as well. The static configuration contains a large number of routes which can take a tremendous amount of time to manage.

2. Updates

Not only maintenance, updating routes in a large network is known to be a complicated process. Routes needed to be updated individually as well as in the correct order. If the routes are updated in the wrong order, there would be problems in the internet access.

3. Redundancy

In the event of a failure, there is no automatic updating in static routing. Users have to adjust routes manually so that the data flows through an alternative path.

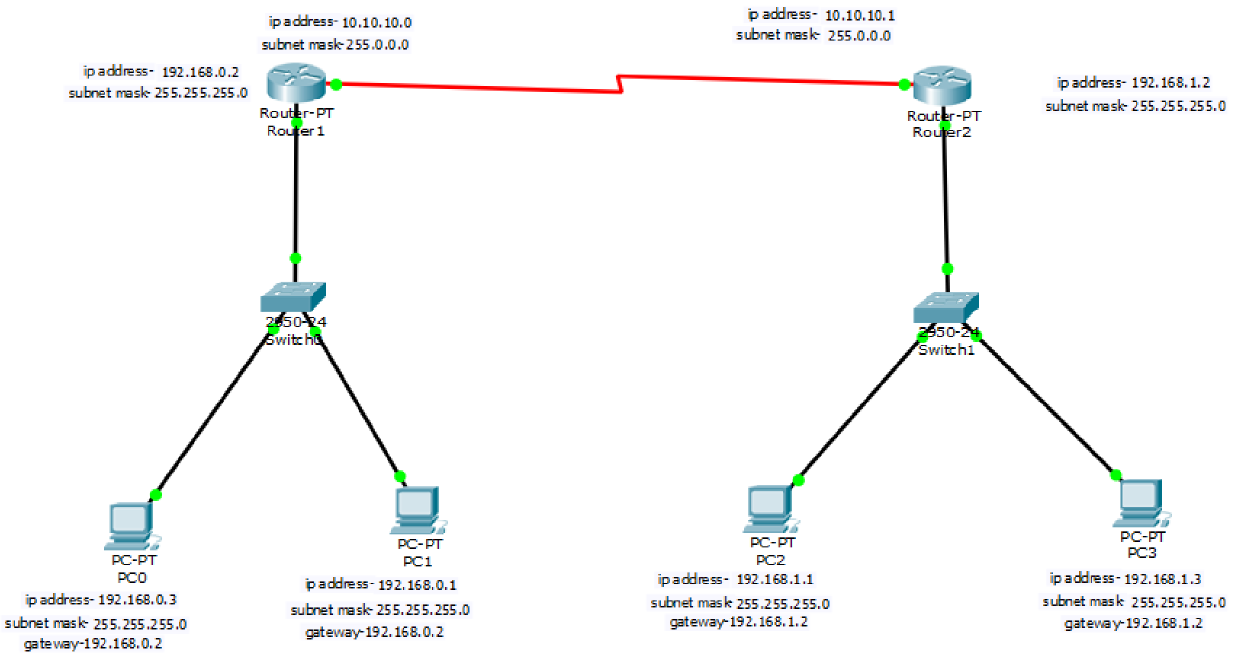
4. Input Errors

Static routing is vulnerable to input errors since they are configured manually. Errors can probably appear as a result of a mistake. Network administrators can make mistakes in configuring routing paths or network information.

5. Protocol Support

Routing protocols lack the freedom of independence when working with static routes. It always gives less preference with routes that are configured with dynamic routing protocol.

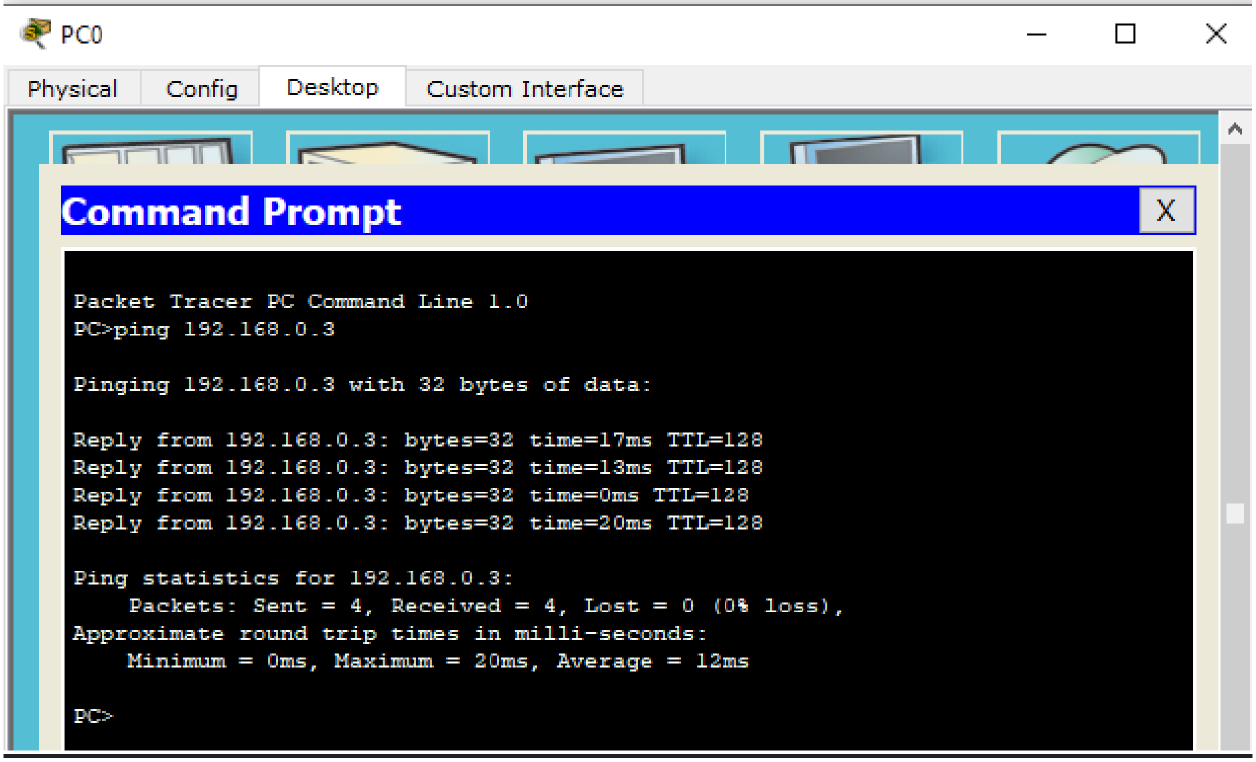
DIAGRAM-



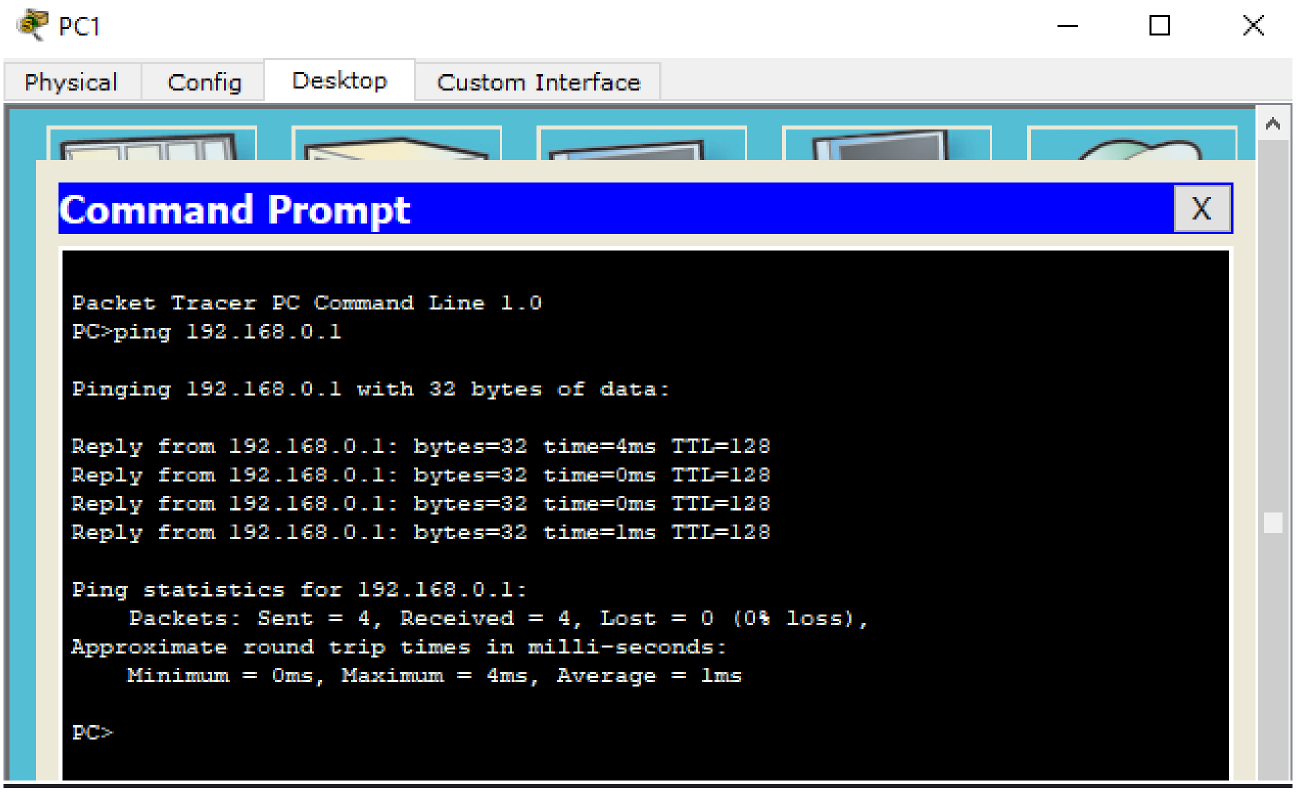
ADDRESSING TABLE:-

S.NO	**DEVICE NAME**	**IP ADDRESS**	**SUBNET MASK**
1	PC0	192.168.0.3	255.255.255.0
2	PC1	192.168.0.1	255.255.255.0
3	PC2	192.168.1.1	255.255.255.0
4	PC3	192.168.1.3	255.255.255.0

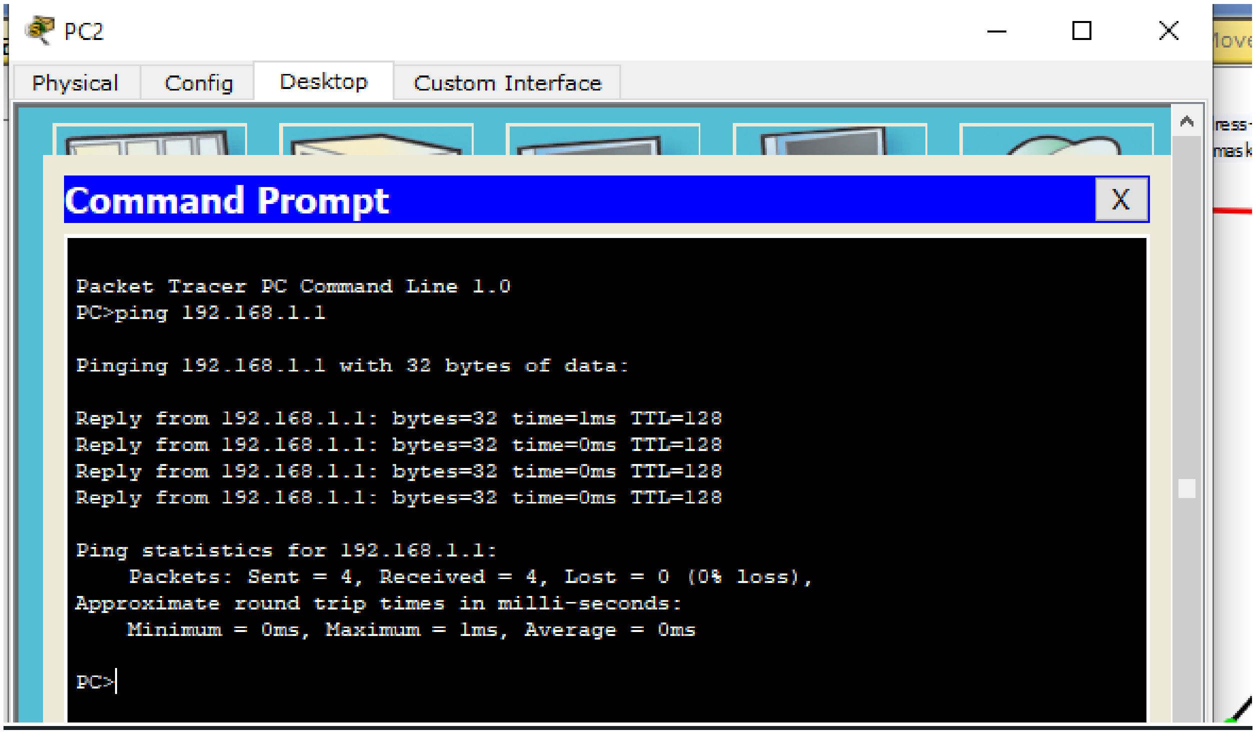
PING -



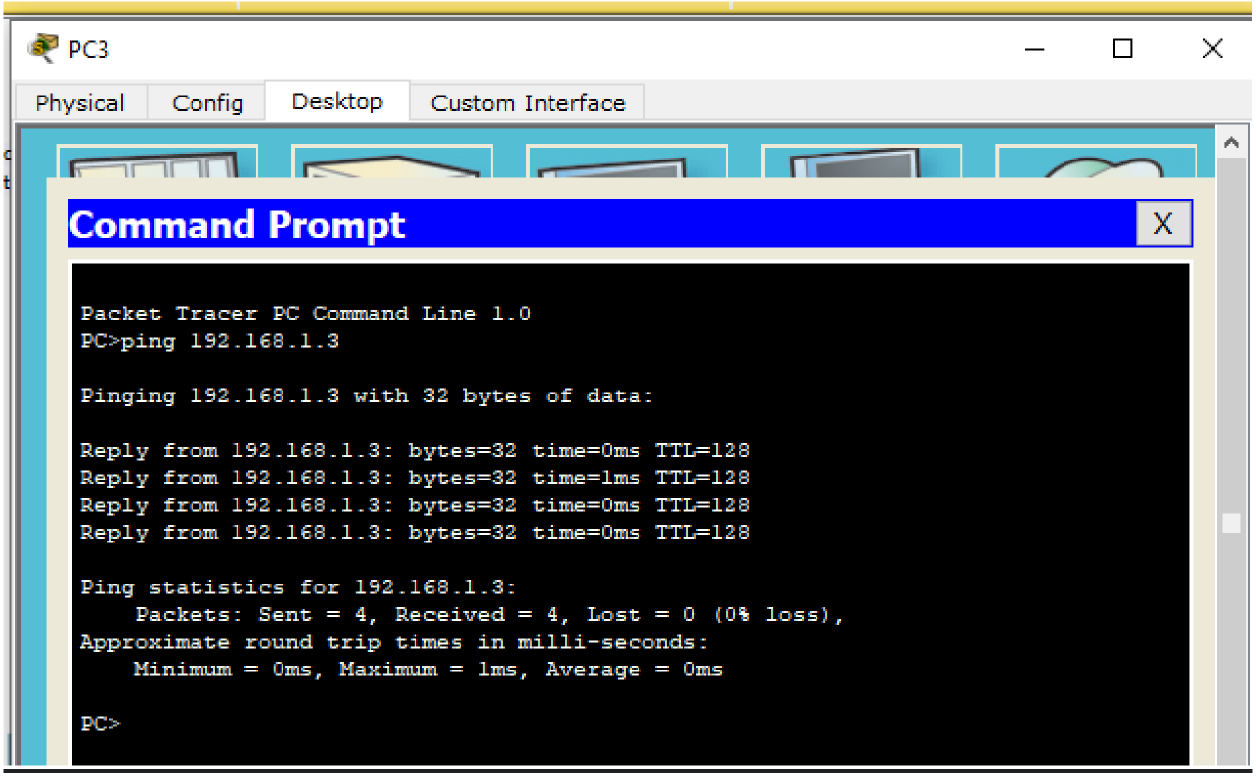
```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:

Reply from 192.168.0.3: bytes=32 time=17ms TTL=128
Reply from 192.168.0.3: bytes=32 time=13ms TTL=128
Reply from 192.168.0.3: bytes=32 time=0ms TTL=128
Reply from 192.168.0.3: bytes=32 time=20ms TTL=128

Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 20ms, Average = 12ms

PC>
```



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=4ms TTL=128
Reply from 192.168.0.1: bytes=32 time=0ms TTL=128
Reply from 192.168.0.1: bytes=32 time=0ms TTL=128
Reply from 192.168.0.1: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms

PC>
```



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=0ms TTL=128
Reply from 192.168.1.1: bytes=32 time=0ms TTL=128
Reply from 192.168.1.1: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```

RESULT - Successful implementation of static routing

Experiment :3

Aim: To implement default routing using Cisco Packet Tracer.

Default Routing: In computer networking, the default route is a configuration of the Internet Protocol (IP) that establishes a forwarding rule for packets when no specific address of a next-hop host is available from the routing table or other routing mechanisms.

The default route is generally the address of another router, which treats the packet the same way: if a route matches, the packet is forwarded accordingly, otherwise the packet is forwarded to the default route of that router. The route evaluation process in each router uses the longest prefix match method to obtain the most specific route. The network with the longest subnet mask or network prefix that matches the destination IP address is the next-hop network gateway. The process repeats until a packet is delivered to the destination host. Each router traversal counts as one hop in the distance calculation for the transmission path.

1. The default route in Internet Protocol Version 4 (IPv4) is designated as the zero address, 0.0.0.0/0 in CIDR notation.

2. Similarly, in IPv6, the default route is specified by ::/0. The subnet mask is specified as */0*, which effectively specifies all networks and is the shortest match possible. A route lookup that does not match any other rule falls back to this route.

Objective: Configure and analyse the performance of Default routing.

Advantages of Static routing:

1. Suitable in all topologies where multiple routers are required.

2. Generally independent of the network size.

3. Automatically adapts topology to reroute traffic if possible.

Disadvantages of Default routing:

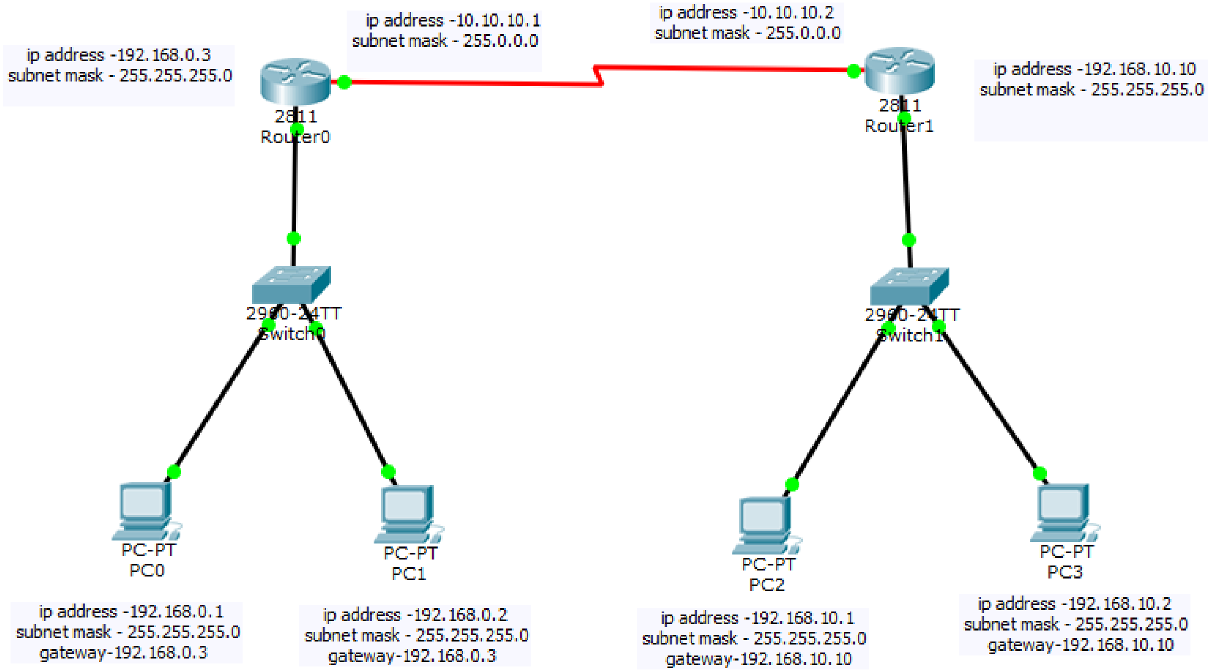
1. Can be more complex to initially implement.

2. Less secure due to the broadcast and multicast routing updates. Additional configuration settings such as passive interfaces and routing protocol authentication are required to increase security.

3. Route depends on the current topology.

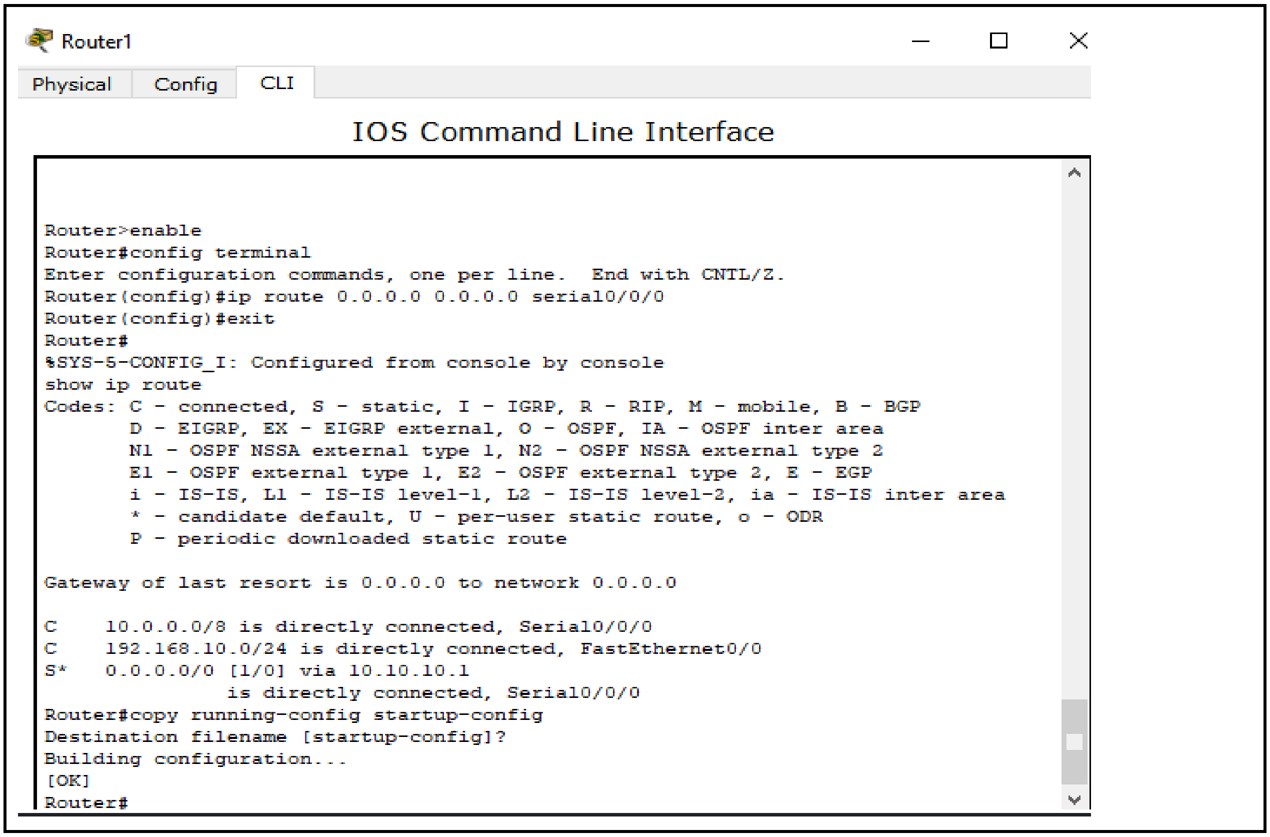
4. Requires additional resources such as CPU, memory, and link bandwidth.

DIAGRAM-

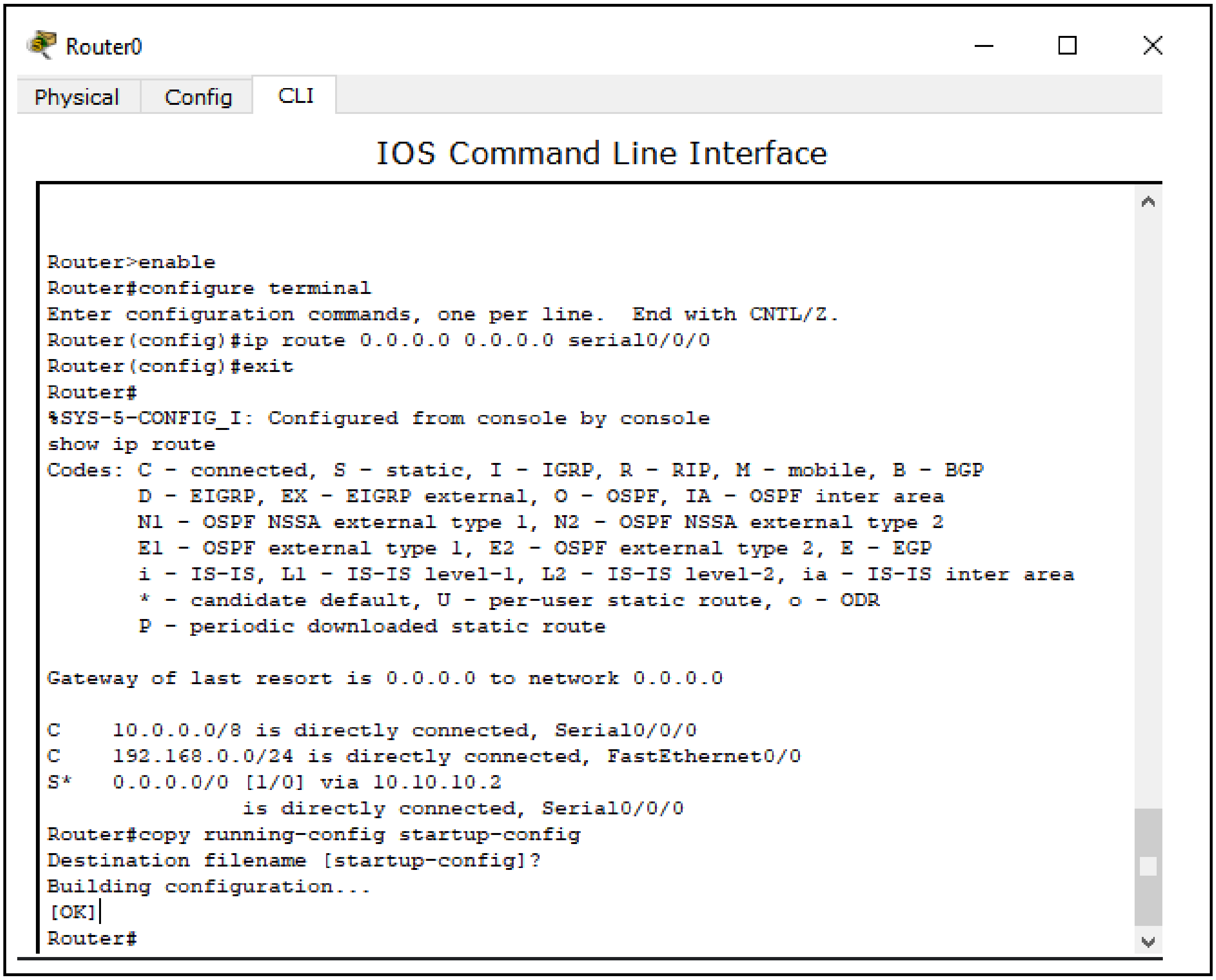


ADDRESSING TABLE -

S.NO	NAME OF DEVICE	IP ADDRESS	SUBNET MASK
1.	PC0	192.168.0.1	255.255.255.0
2.	PC1	192.168.0.2	255.255.255.0
3.	PC2	192.168.10.1	255.255.255.0
4.	PC3	192.168.10.2	255.255.255.0
5.	ROUTER0	192.168.0.3	255.255.255.0
6.	ROUTER1	192.168.10.10	255.255.255.0

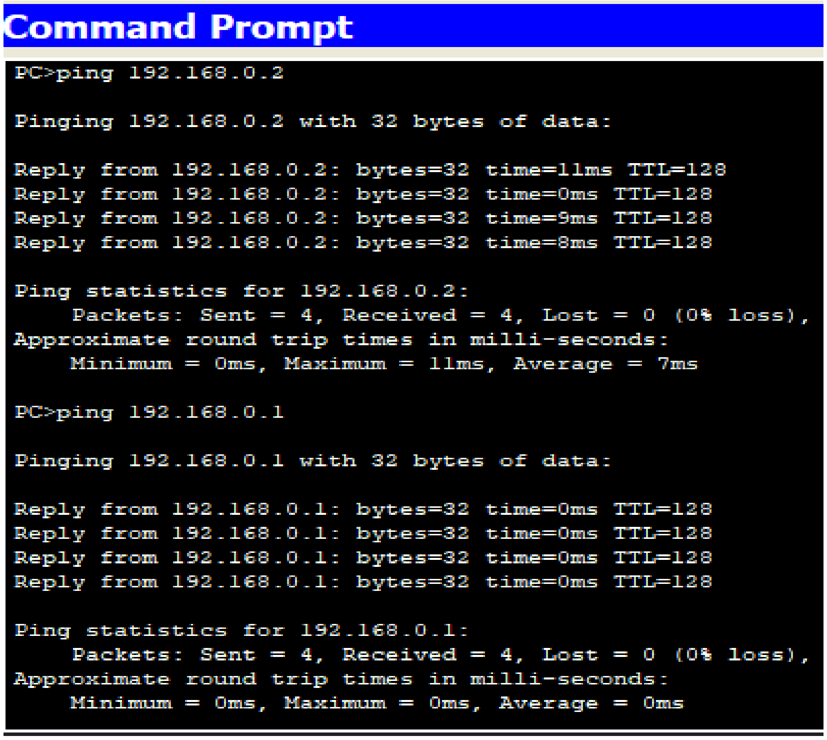


```
Router>enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip route 0.0.0.0 0.0.0.0 serial0/0/0
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, 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 0.0.0.0 to network 0.0.0.0

C    10.0.0.0/8 is directly connected, Serial0/0/0
C    192.168.10.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 10.10.10.1
               is directly connected, Serial0/0/0
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
```

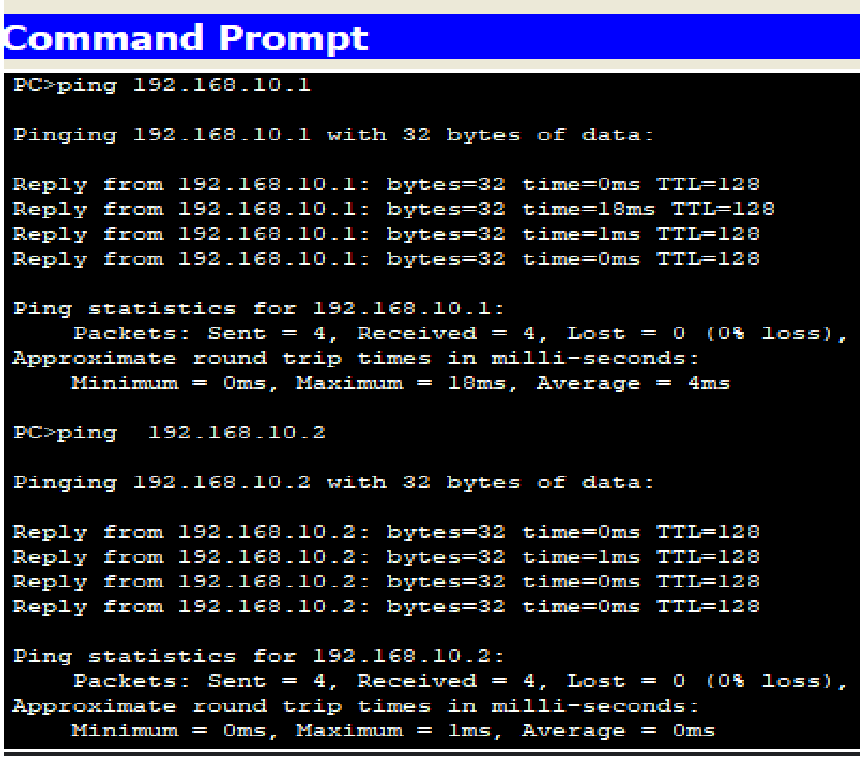


```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip route 0.0.0.0 0.0.0.0 serial0/0/0
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, 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 0.0.0.0 to network 0.0.0.0

C    10.0.0.0/8 is directly connected, Serial0/0/0
C    192.168.0.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 10.10.10.2
               is directly connected, Serial0/0/0
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
```

PING-



```
PC>ping 192.168.0.2

Pinging 192.168.0.2 with 32 bytes of data:

Reply from 192.168.0.2: bytes=32 time=11ms TTL=128
Reply from 192.168.0.2: bytes=32 time=0ms TTL=128
Reply from 192.168.0.2: bytes=32 time=9ms TTL=128
Reply from 192.168.0.2: bytes=32 time=8ms TTL=128

Ping statistics for 192.168.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 7ms

PC>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=0ms TTL=128
Reply from 192.168.0.1: bytes=32 time=0ms TTL=128
Reply from 192.168.0.1: bytes=32 time=0ms TTL=128
Reply from 192.168.0.1: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```



```
PC>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time=0ms TTL=128
Reply from 192.168.10.1: bytes=32 time=18ms TTL=128
Reply from 192.168.10.1: bytes=32 time=1ms TTL=128
Reply from 192.168.10.1: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 18ms, Average = 4ms

PC>ping  192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time=0ms TTL=128
Reply from 192.168.10.2: bytes=32 time=1ms TTL=128
Reply from 192.168.10.2: bytes=32 time=0ms TTL=128
Reply from 192.168.10.2: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

RESULT - Successful implementation of Default routing

Experiment :4

Aim: To implement Rip Version using Cisco Packet Tracer.

ROUTING INFORMATION PROTOCOL : The Routing Information Protocol (RIP) is a distance-vector, interior gateway (IGP) routing protocol used by routers to exchange routing information. RIP uses the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination.

OBJECTIVE : Configure and analyze the performance of the Routing Information Protocol.

Advantages of RIP :-

•It is easy to configure.

•that it does not require an update every time the topology of network changes.

•Guaranteed to support almost all routers

Disadvantages of RIP :-

•It is only based on hop count. So, if there is a better route available with better bandwidth then it will not select that route.

•Bandwidth utilization in RIP is very high as it broadcasts its updates every 30 seconds.

•RIP supports only 15 hop count so a maximum of 16 routers can be configured in RIP.

•Here the convergence rate is slow. It means that when any link goes down it takes a lot of time to choose alternate routes.

Limitations:

•Inability to support paths longer than 15 hops

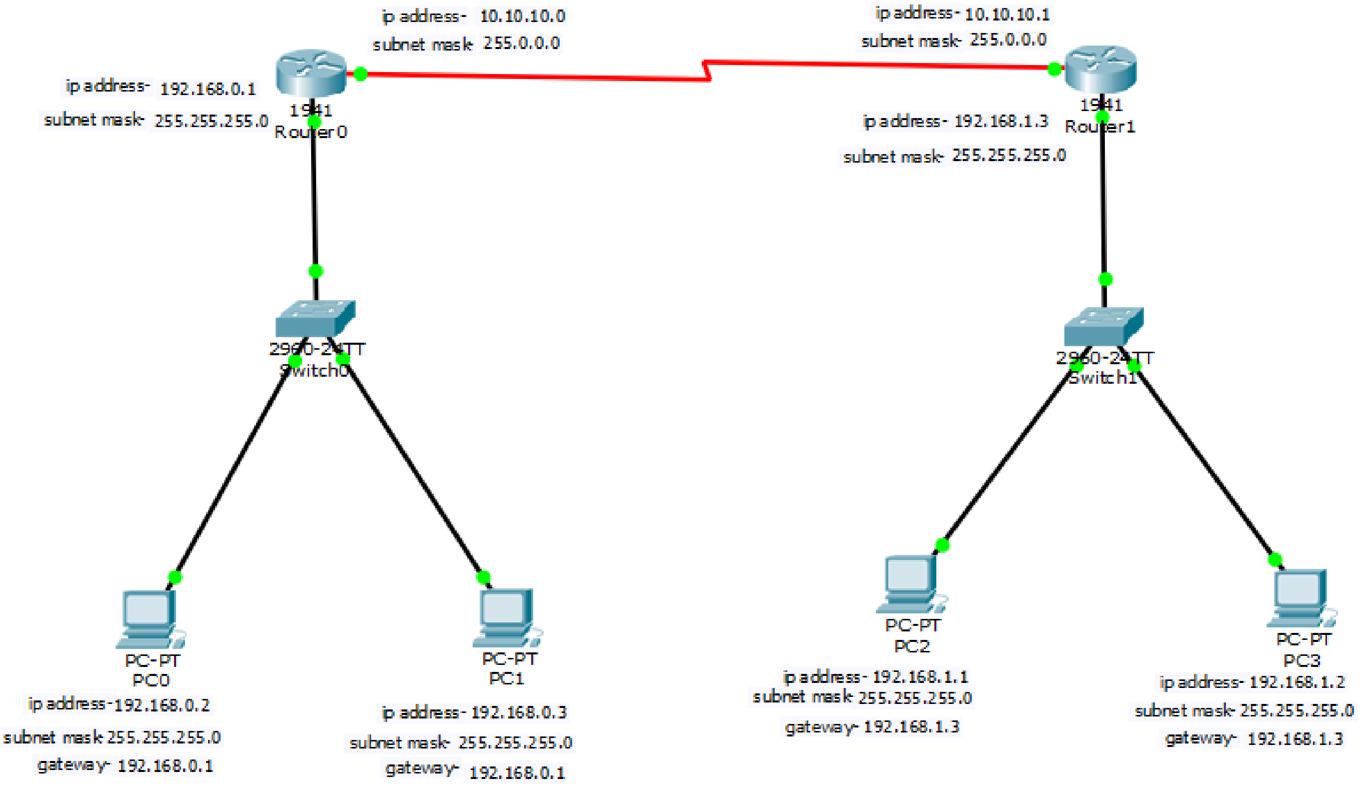
•Reliance on fixed metrics to calculate routes

•Network intensity of table updates

•Relatively slow convergence

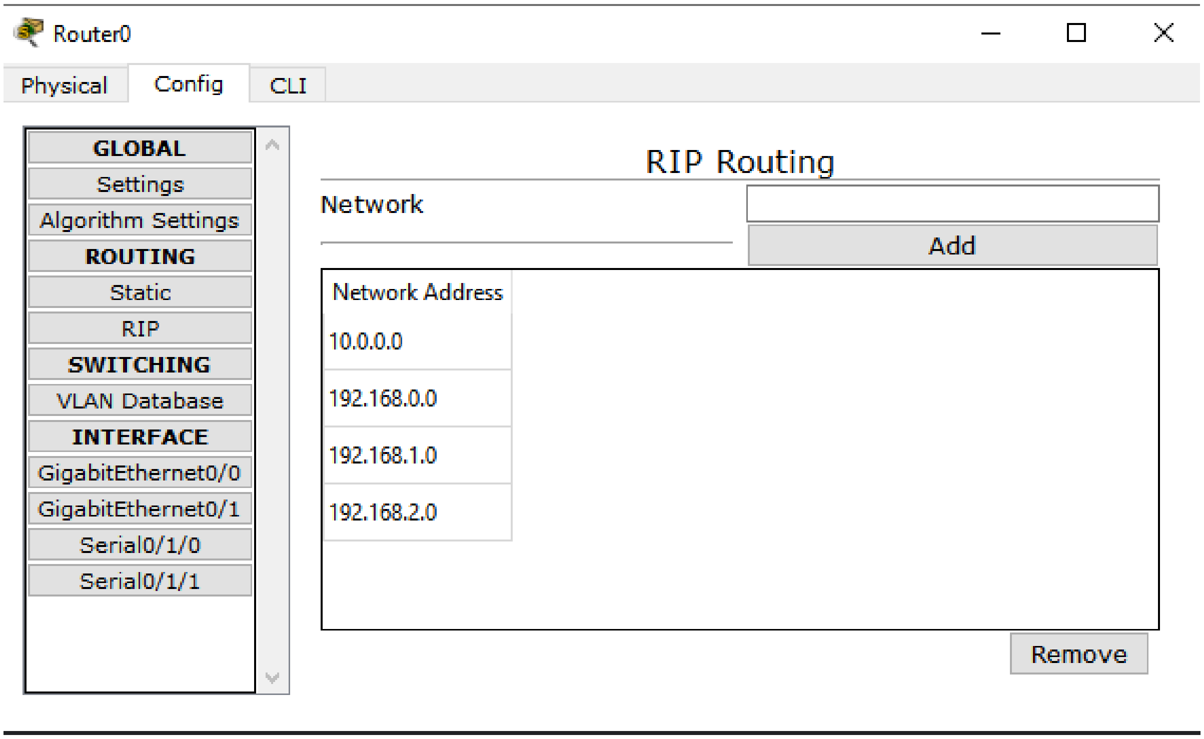
•Lack of support for dynamic load balancing

DIAGRAM-



ADDRESSING TABLE -

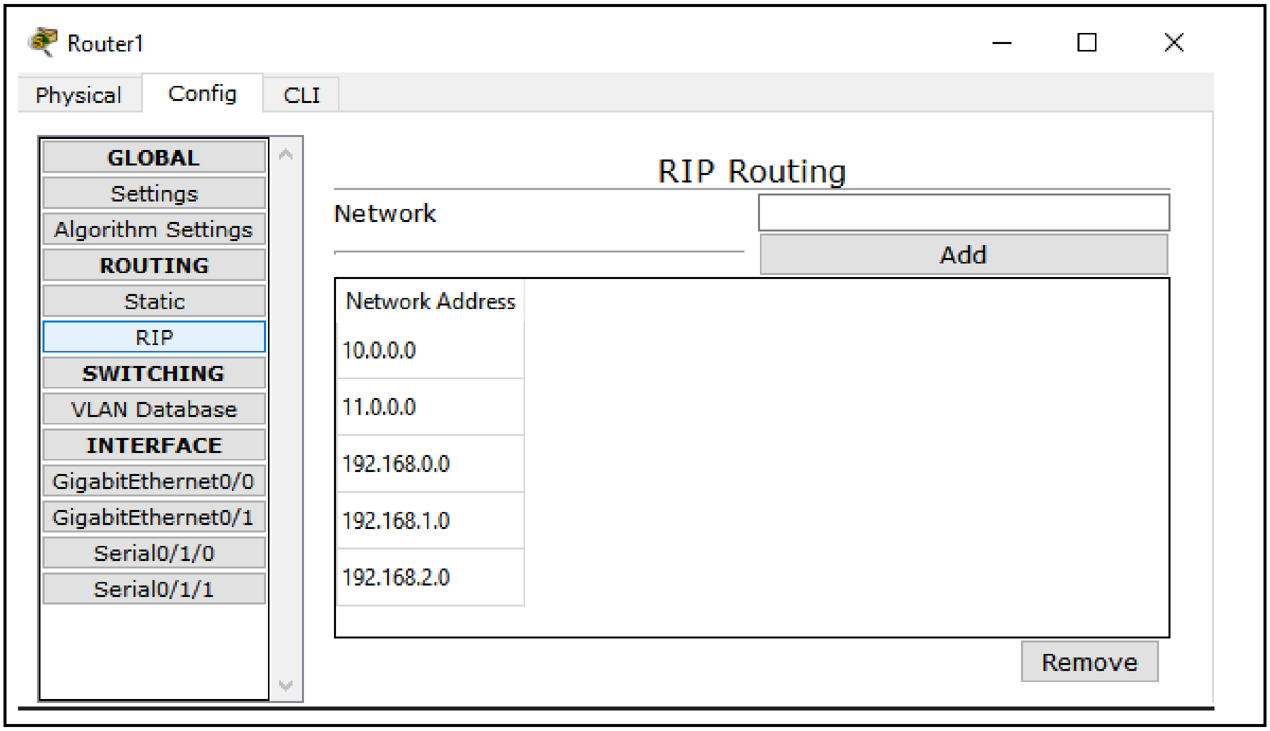
S.NO	NAME OF DEVICE	IP ADDRESS	SUBNET MASK
1.	PC0	192.168.0.2	255.255.255.0
2.	PC1	192.168.0.3	255.255.255.0
3.	PC2	192.168.1.1	255.255.255.0
4.	PC3	192.168.1.2	255.255.255.0
5.	ROUTER0	192.168.0.1	255.255.255.0
6.	ROUTER1	192.168.1.3	255.255.255.0



RIP Routing

Network

Network Address
10.0.0.0
192.168.0.0
192.168.1.0
192.168.2.0

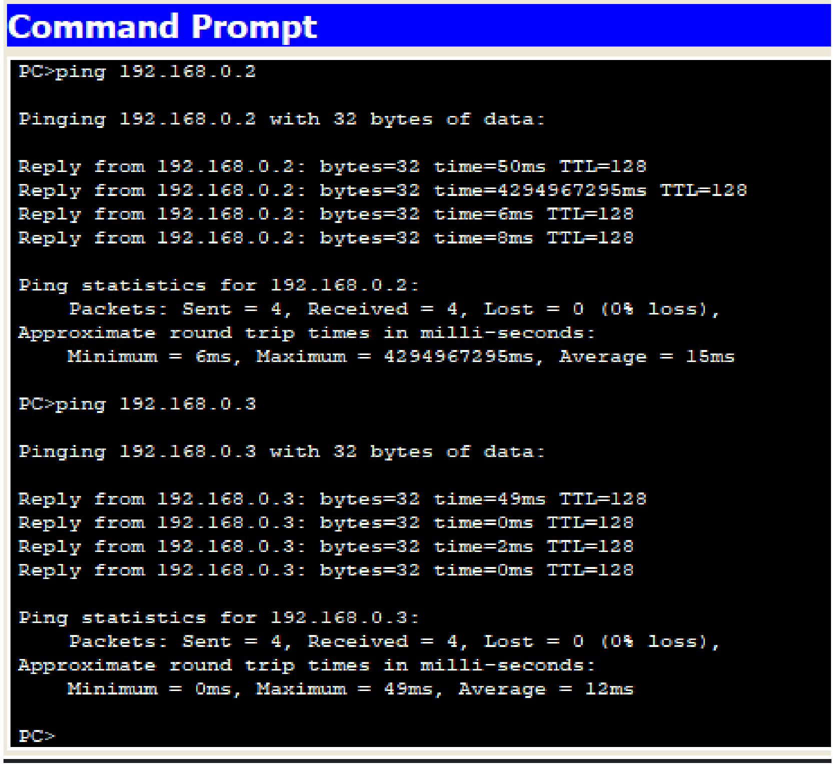


RIP Routing

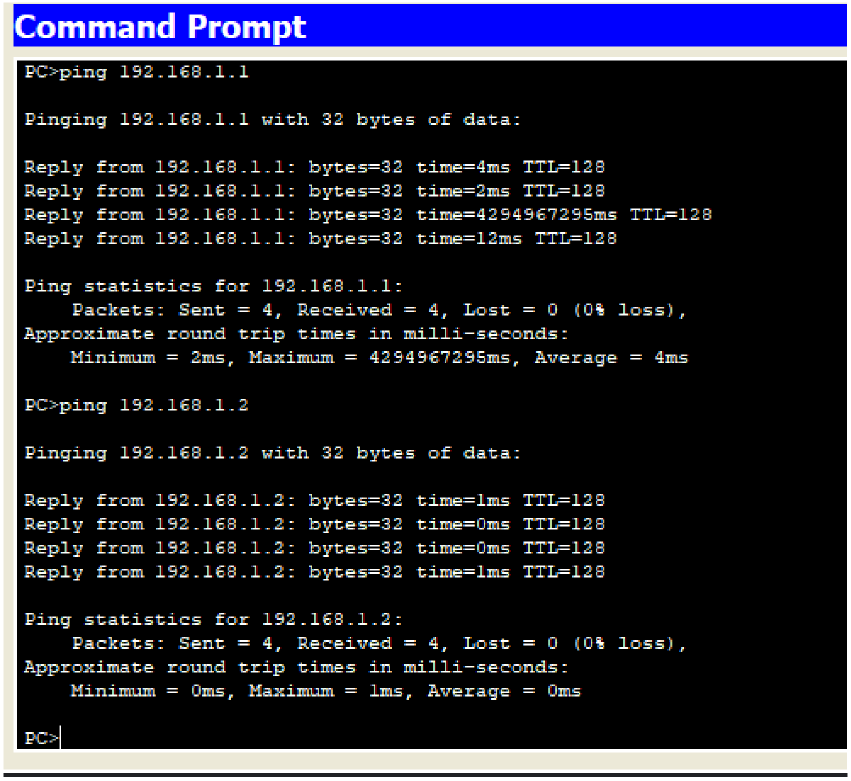
Network

Network Address
10.0.0.0
11.0.0.0
192.168.0.0
192.168.1.0
192.168.2.0

PING-



```
PC>ping 192.168.0.2

Pinging 192.168.0.2 with 32 bytes of data:

Reply from 192.168.0.2: bytes=32 time=50ms TTL=128
Reply from 192.168.0.2: bytes=32 time=4294967295ms TTL=128
Reply from 192.168.0.2: bytes=32 time=6ms TTL=128
Reply from 192.168.0.2: bytes=32 time=8ms TTL=128

Ping statistics for 192.168.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 4294967295ms, Average = 15ms

PC>ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:

Reply from 192.168.0.3: bytes=32 time=49ms TTL=128
Reply from 192.168.0.3: bytes=32 time=0ms TTL=128
Reply from 192.168.0.3: bytes=32 time=2ms TTL=128
Reply from 192.168.0.3: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 49ms, Average = 12ms

PC>
```



```
PC>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=4ms TTL=128
Reply from 192.168.1.1: bytes=32 time=2ms TTL=128
Reply from 192.168.1.1: bytes=32 time=4294967295ms TTL=128
Reply from 192.168.1.1: bytes=32 time=12ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 4294967295ms, Average = 4ms

PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=0ms TTL=128
Reply from 192.168.1.2: bytes=32 time=0ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```

RESULT - **Successful implementation of RIP**

Experiment - 5

Aim: To implement the Rip Version 2 using Cisco Packet Tracer.

Rip Version 2: Due to some deficiencies in the original RIP specification, RIP version 2 was developed in 1993. It supports classless Inter-Domain Routing (CIDR) and has ability to carry subnet information, its metric is also hop count and max hop count 15 is the same as rip version 1.

It supports authentication and does subnetting and multicasting. Auto summary can be done on every router. In RIPv2 Subnet masks are included in the routing update. RIPv2 multicasts the entire routing table to all adjacent routers at the address 224.0.0.9, as opposed to RIPv1 which uses broadcast (255.255.255.255).

Objective: Configure and analyze the performance of Rip Version 2.

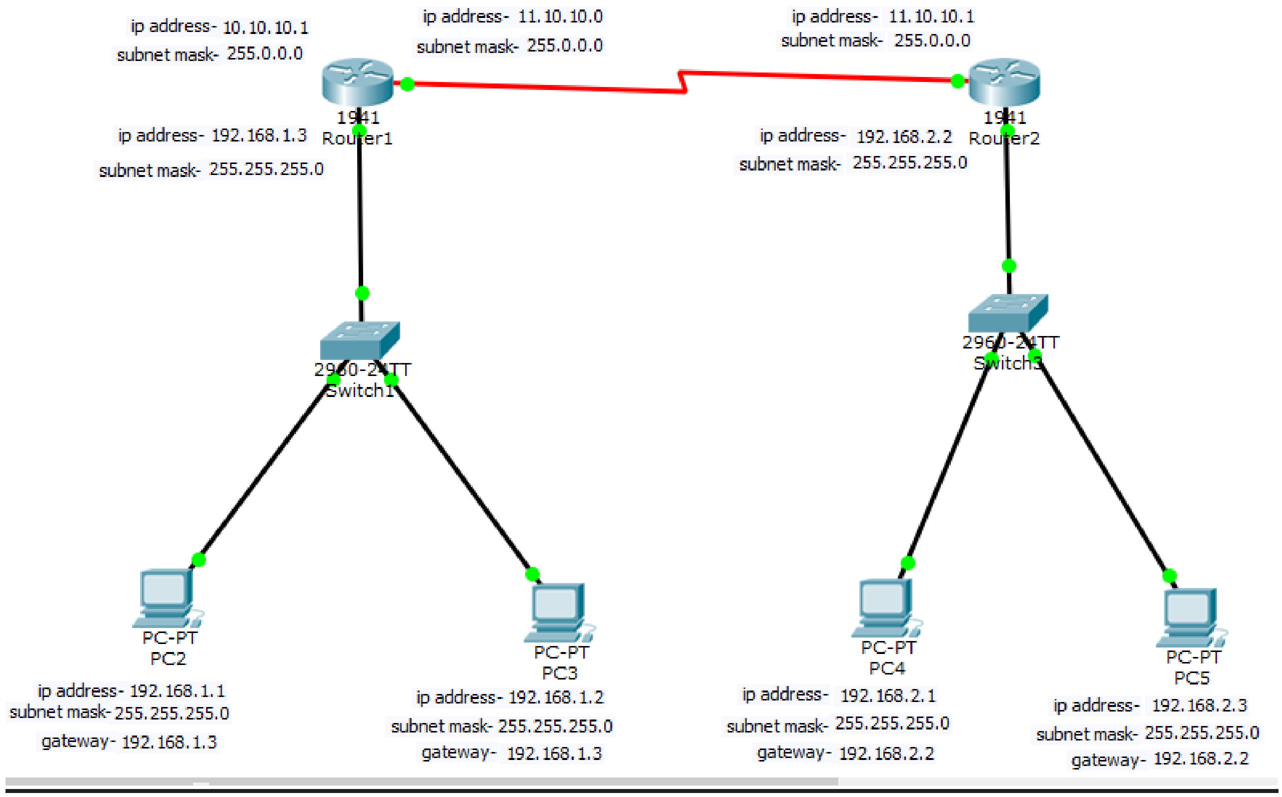
Advantages of Static routing:

1. It's a standardized protocol.
1. It sends triggered updates when the network changes.
2. Provides fast convergence.

Disadvantages of Default routing:

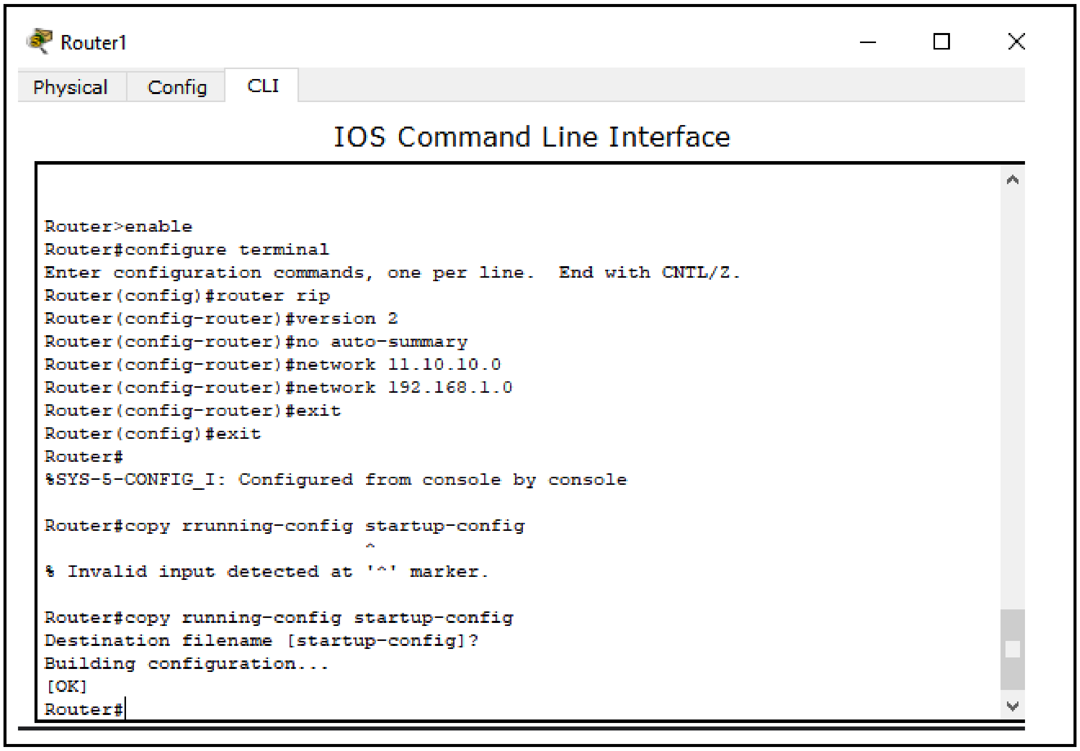
1. Max hop count of 15, due to the 'count-to-infinity' vulnerability.
1. No concept of neighbours.
2. Exchanges the entire table with all neighbours every 30 seconds (except in the case of a triggered update).

DIAGRAM-

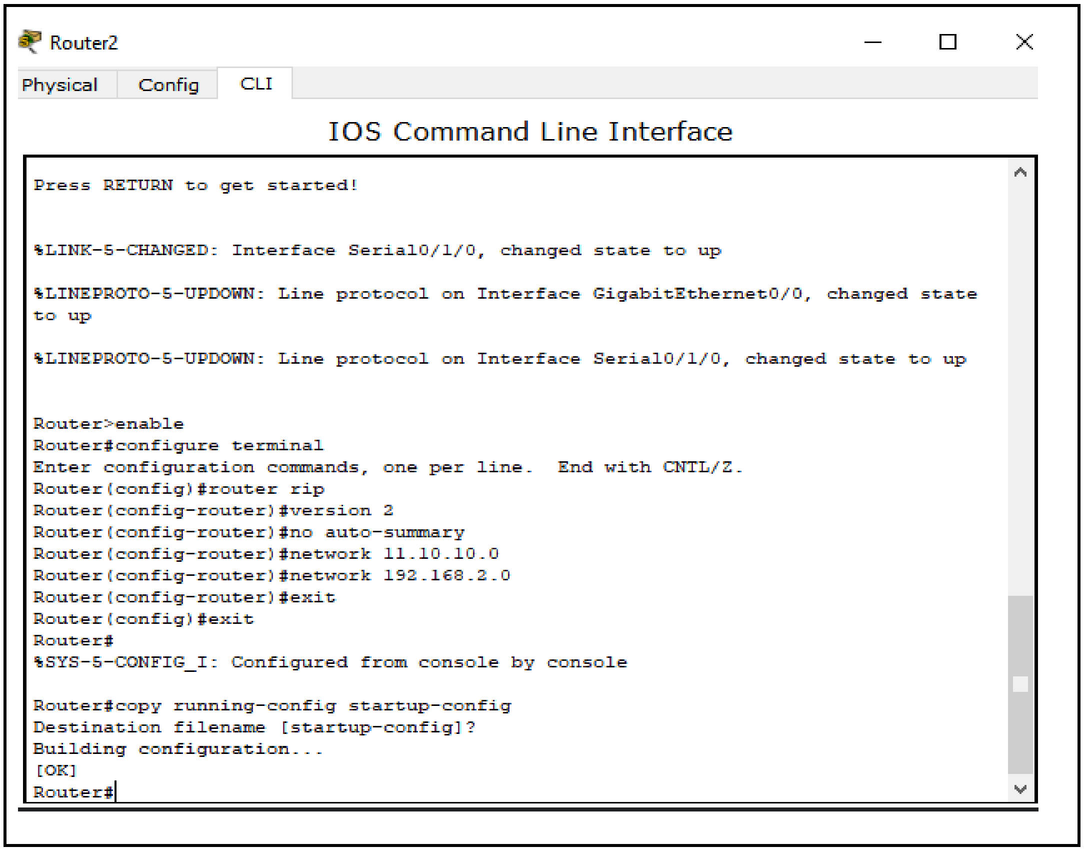


ADDRESSING TABLE -

S.NO	NAME OF DEVICE	IP ADDRESS	SUBNET MASK
1.	PC2	192.168.1.1	255.255.255.0
2.	PC3	192.168.1.2	255.255.255.0
3.	PC4	192.168.2.1	255.255.255.0
4.	PC5	192.168.2.3	255.255.255.0
5.	ROUTER1	192.168.1.3	255.255.255.0
6.	ROUTER2	192.168.2.2	255.255.255.0

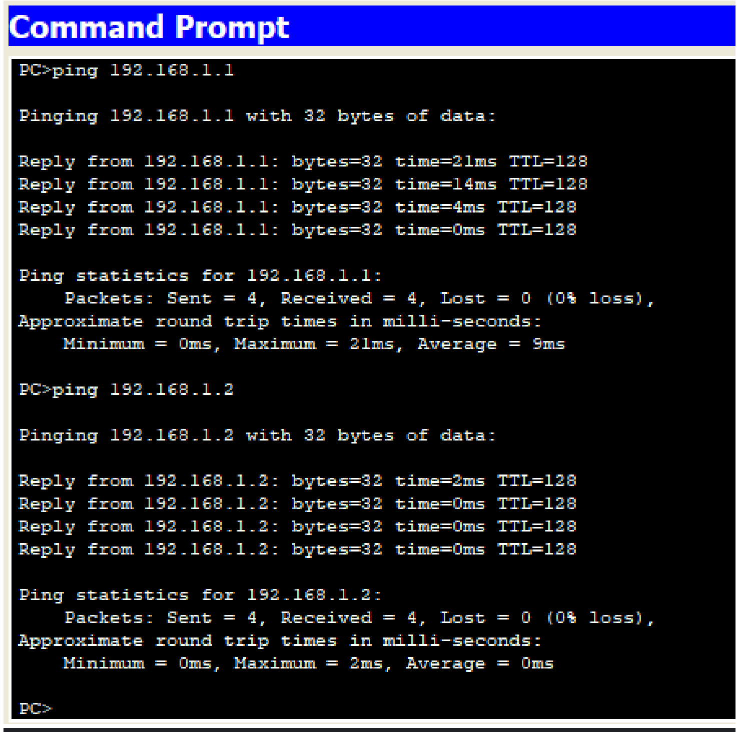


```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#no auto-summary
Router(config-router)#network 11.10.10.0
Router(config-router)#network 192.168.1.0
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#copy rrunning-config startup-config
                             ^
% Invalid input detected at '^' marker.

Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
```

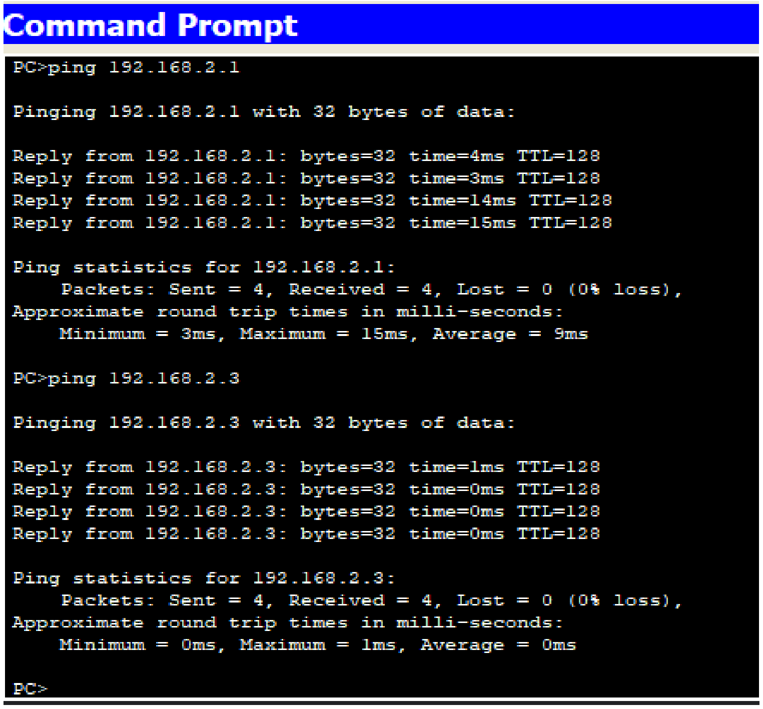


```
Press RETURN to get started!


%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state
to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up


Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#no auto-summary
Router(config-router)#network 11.10.10.0
Router(config-router)#network 192.168.2.0
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
```

PING-



```
PC>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=21ms TTL=128
Reply from 192.168.1.1: bytes=32 time=14ms TTL=128
Reply from 192.168.1.1: bytes=32 time=4ms TTL=128
Reply from 192.168.1.1: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 21ms, Average = 9ms

PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=2ms TTL=128
Reply from 192.168.1.2: bytes=32 time=0ms TTL=128
Reply from 192.168.1.2: bytes=32 time=0ms TTL=128
Reply from 192.168.1.2: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

PC>
```



```
PC>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=4ms TTL=128
Reply from 192.168.2.1: bytes=32 time=3ms TTL=128
Reply from 192.168.2.1: bytes=32 time=14ms TTL=128
Reply from 192.168.2.1: bytes=32 time=15ms TTL=128

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 15ms, Average = 9ms

PC>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=1ms TTL=128
Reply from 192.168.2.3: bytes=32 time=0ms TTL=128
Reply from 192.168.2.3: bytes=32 time=0ms TTL=128
Reply from 192.168.2.3: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```

RESULT - **Successful implementation of RIP2**

EXPERIMENT :- 6

Aim : To implement EIGRP (Enhanced Interior Gateway Routing Protocol) using Cisco packet Tracer.

Enhanced Interior Gateway Routing Protocol : The Enhanced Interior Gateway Routing Protocol is a network routing protocol which promotes an efficient information exchange between the routers.

This routing protocol is developed by Cisco and is compatible only with Cisco hardware (routers) and not with other vendors. EIGRP is an advanced distance vector protocol version of RIP

.**Advantages of EIGRP :-**

• EIGRP routing protocol is capable of routing several different Layer 3 protocols using protocol-dependant modules (PDM). Protocols include IPX, AppleTalk and IPv6.

• EIGRP is the only routing protocol, which is capable of unequal cost load balancing. Unequal cost paths are the different paths to a destination network with different metric values. Benefit if there is more than one link to the destination but the metric is different engineer can configure variance between those links.

• Sub second convergence in 200 milliseconds. EIGRP can converge after link failure in less than a second by using Feasible Successor. Critical applications require fast convergence.

• Manual route summarization is one of the best features of EIGRP routing protocol. EIGRP allows engineer to summarize at any point of the network and on every router. This improves stability and reduces size of the routing table.

• Ease of implementation. EIGRP was designed to be easy to configure. The basic configuration does not require advanced technical knowledge. To enable EIGRP the only commands necessary are EIGRP autonomous system number and network statement commands.

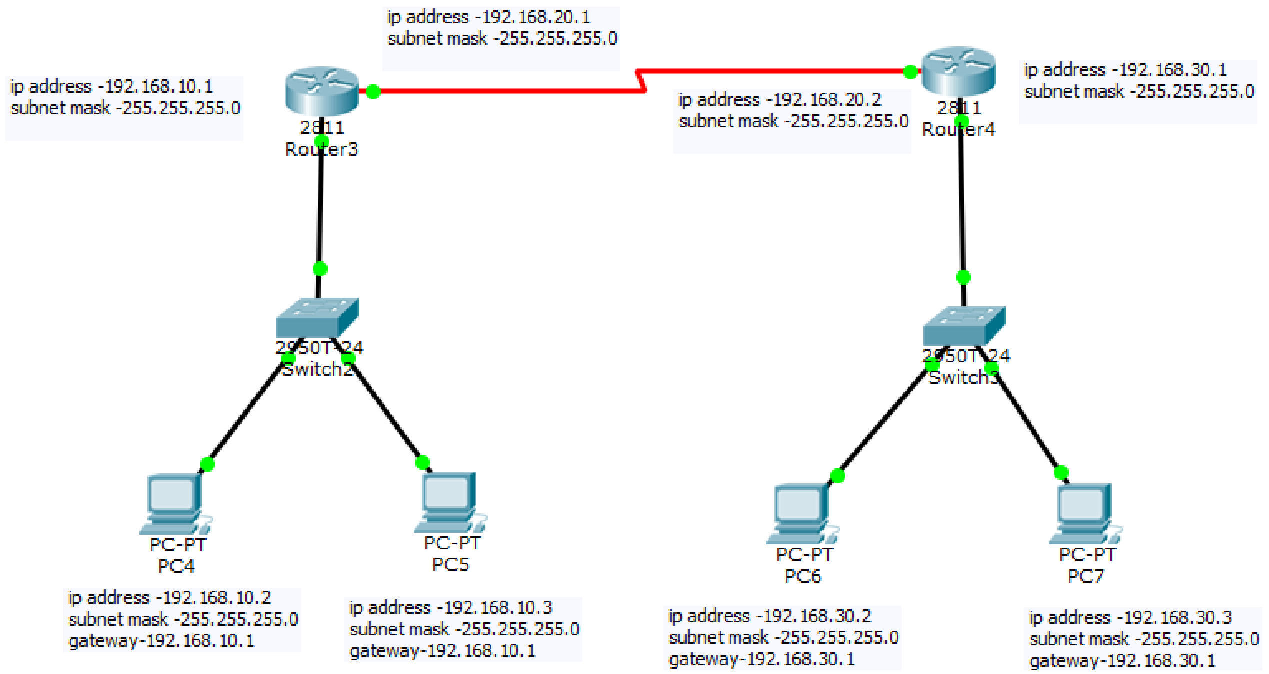
Disadvantages of EIGRP :-

• EIGRP routing protocol can be used only on Cisco network devices so if the company has multiple vendors networking equipment, it will not work. Cisco has opened EIGRP standard to other vendors in March 2013. Now all vendors can implement and use EIGRP on their networking equipment but advanced features are still maintained and controlled by Cisco.

• EIGRP is still distance vector routing protocol and only relies on routed provided by directly connected neighbour.

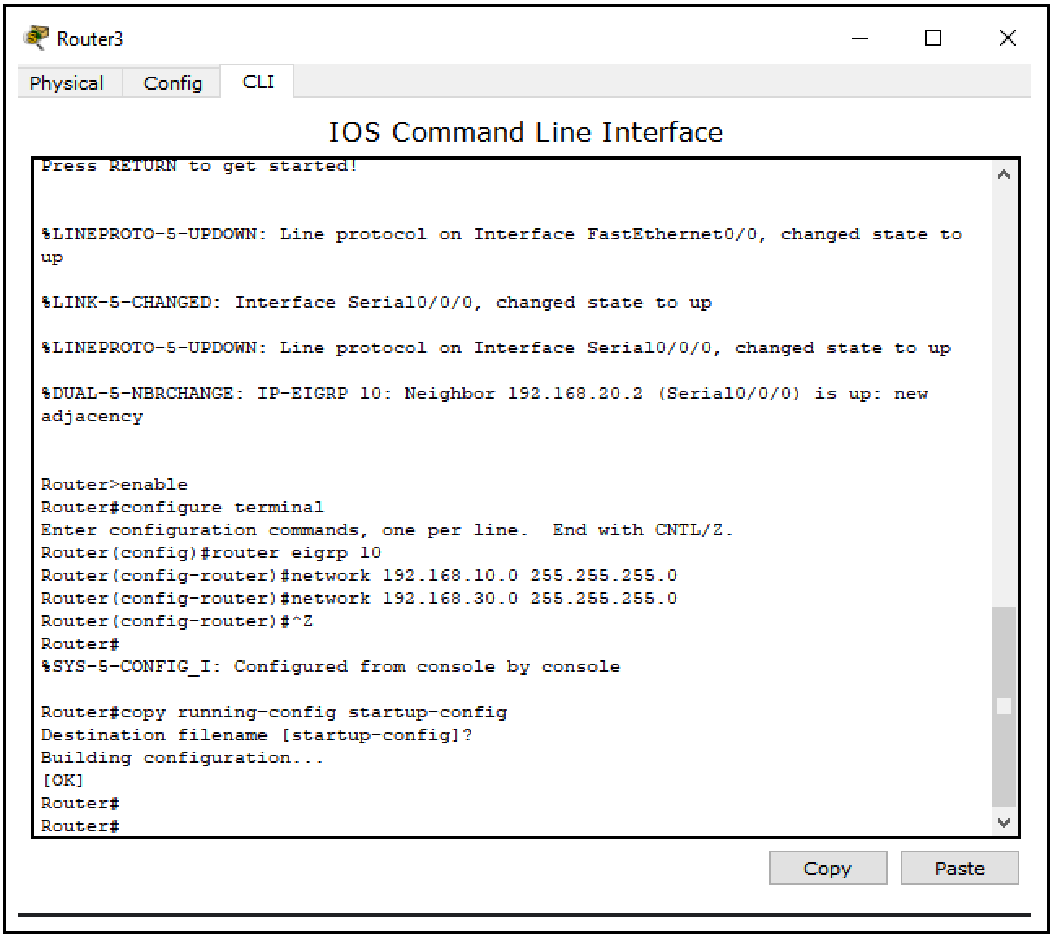
• EIGRP is not extensible and does not support future application through ‘’opaque’’ LSA, e.g. MPLS Traffic Engineering. Opaque LSAs provide a generalized mechanism to allow for the future extensibility of OSPF.

DIAGRAM-

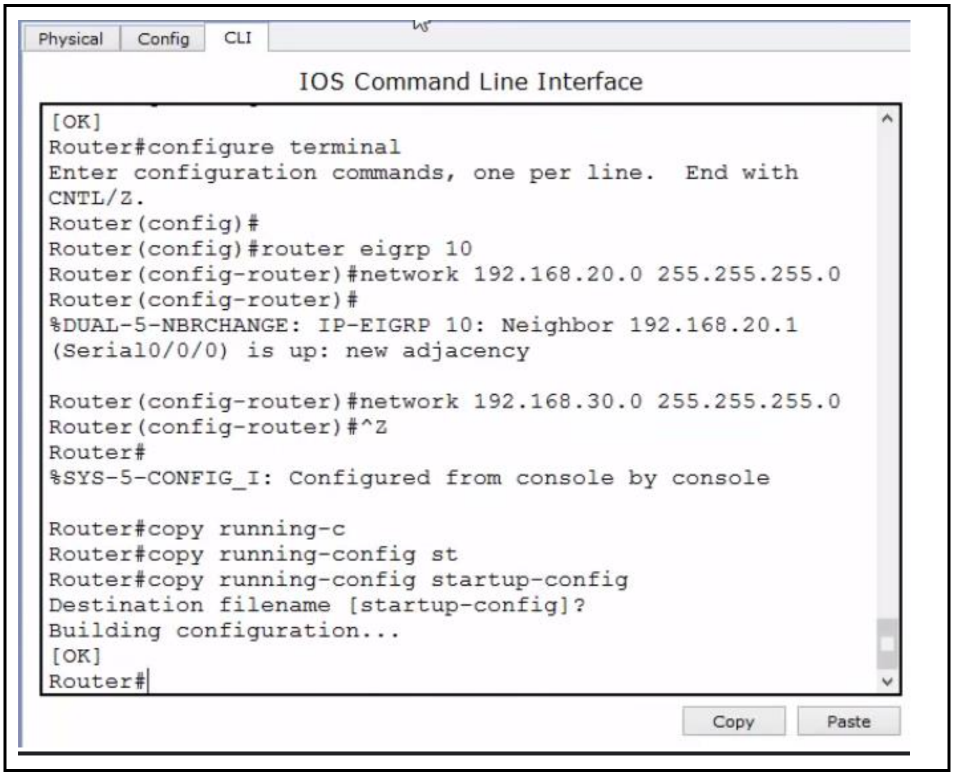


ADDRESSING TABLE -

S.NO	NAME OF DEVICE	IP ADDRESS	SUBNET MASK
1.	PC4	192.168.10.2	255.255.255.0
2.	PC5	192.168.10.3	255.255.255.0
3.	PC6	192.168.30.2	255.255.255.0
4.	PC7	192.168.30.3	255.255.255.0
5.	ROUTER3	192.168.10.1	255.255.255.0
6.	ROUTER4	192.168.30.1	255.255.255.0

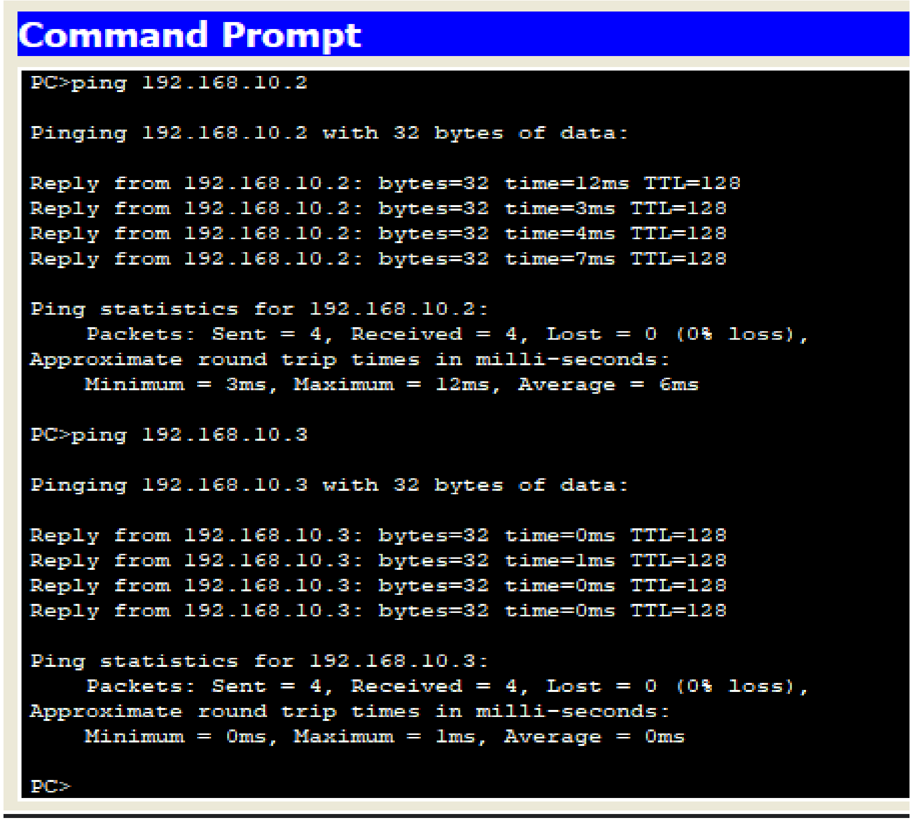


```
Press RETURN to get started!


%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to
up

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 192.168.20.2 (Serial0/0/0) is up: new
adjacency


Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router eigrp 10
Router(config-router)#network 192.168.10.0 255.255.255.0
Router(config-router)#network 192.168.30.0 255.255.255.0
Router(config-router)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
Router#
```

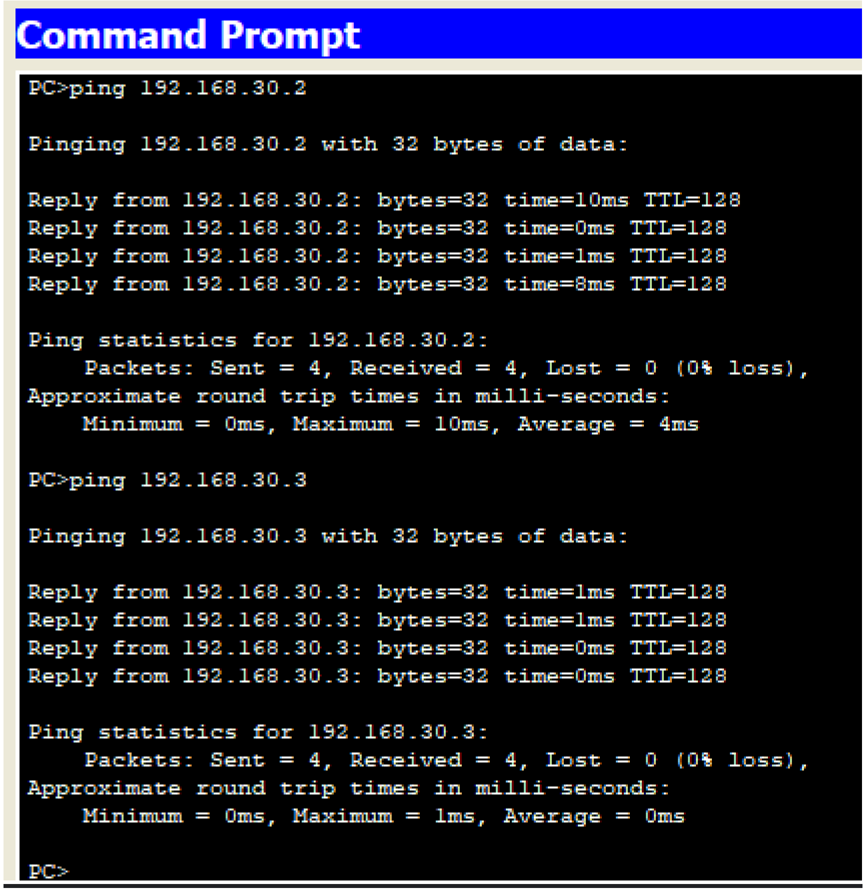


```
[OK]
Router#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
Router(config)#
Router(config)#router eigrp 10
Router(config-router)#network 192.168.20.0 255.255.255.0
Router(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 192.168.20.1
(Serial0/0/0) is up: new adjacency

Router(config-router)#network 192.168.30.0 255.255.255.0
Router(config-router)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#copy running-c
Router#copy running-config st
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
```

PING-



```
PC>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time=12ms TTL=128
Reply from 192.168.10.2: bytes=32 time=3ms TTL=128
Reply from 192.168.10.2: bytes=32 time=4ms TTL=128
Reply from 192.168.10.2: bytes=32 time=7ms TTL=128

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 12ms, Average = 6ms

PC>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Reply from 192.168.10.3: bytes=32 time=0ms TTL=128
Reply from 192.168.10.3: bytes=32 time=1ms TTL=128
Reply from 192.168.10.3: bytes=32 time=0ms TTL=128
Reply from 192.168.10.3: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```



```
PC>ping 192.168.30.2

Pinging 192.168.30.2 with 32 bytes of data:

Reply from 192.168.30.2: bytes=32 time=10ms TTL=128
Reply from 192.168.30.2: bytes=32 time=0ms TTL=128
Reply from 192.168.30.2: bytes=32 time=1ms TTL=128
Reply from 192.168.30.2: bytes=32 time=8ms TTL=128

Ping statistics for 192.168.30.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 4ms

PC>ping 192.168.30.3

Pinging 192.168.30.3 with 32 bytes of data:

Reply from 192.168.30.3: bytes=32 time=1ms TTL=128
Reply from 192.168.30.3: bytes=32 time=1ms TTL=128
Reply from 192.168.30.3: bytes=32 time=0ms TTL=128
Reply from 192.168.30.3: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```

RESULT - **Successful implementation of EIGRP**

Experiment :7

Aim: To implement OSPF (Open Shortest Path First) using Cisco Packet Tracer.

OSPF- The OSPF (Open Shortest Path First) protocol is one of a family of IP Routing protocols, and is an Interior Gateway Protocol (IGP) for the Internet, used to distribute IP routing information throughout a single Autonomous System (AS) in an IP network.

The OSPF protocol is a link-state routing protocol, which means that the routers exchange topology information with their nearest neighbours. The topology information is flooded throughout the AS, so that every router within the AS has a complete picture of the topology of the AS. This picture is then used to calculate end-to-end paths through the AS, normally using a variant of the Dijkstra algorithm. Therefore, in a link-state routing protocol, the next hop address to which data is forwarded is determined by choosing the best end-to-end path to the eventual destination.

Operation-

OSPF maintains link-state databases, which are really network topology maps, on every router on which it is implemented. The state of a given route in the network is the cost, and OSPF algorithm allows every router to calculate the cost of the routes to any given reachable destination. The link cost of a path connected to a router is determined by the bit rate (1 Gbit/s, 10 Gbit/s, etc.) of the interface. A router interface with OSPF will then advertise its link cost to neighboring routers through multicast, known as the Hello procedure.

An OSPF network can be divided into areas that are logical groupings of hosts and networks. An area includes its connecting router having interfaces connected to the network. Each area maintains a separate link-state database whose information may be summarized towards the rest of the network by the connecting router. Thus, the topology of an area is unknown outside the area. This reduces the routing traffic between parts of an autonomous system.

Features:

1. OSPF implements a two-layer hierarchy: the backbone (area 0) and areas off of the backbone (areas 1– 65,535)
2. To provide scalability OSPF supports two important concepts: autonomous systems and areas.
3. Synchronous serial links, no matter what the clock rate of the physical link is, the bandwidth always defaults to 1544 Kbps.
4. OSPF uses cost as a metric, which is the inverse of the bandwidth of a link.

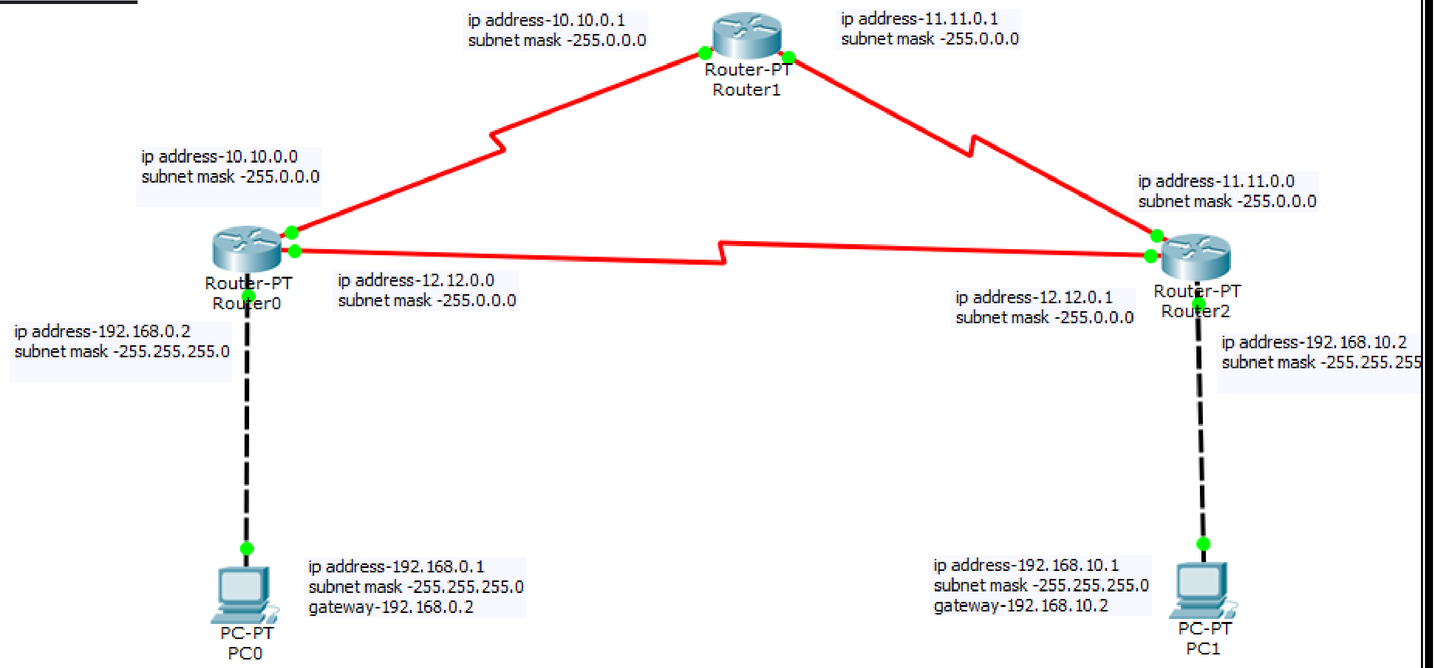
Advantages

1. It will run on most routers, since it is based on an open standard.
2. It uses the SPF algorithm, developed by Dijkstra, to provide a loop-free topology.
3. It provides fast convergence with triggered, incremental updates via Link State Advertisements (LSAs).
4. It is a classless protocol and allows for a hierarchical design with VLSM and route summarization.

Disadvantages

1. It requires more memory to hold the adjacency (list of OSPF neighbors), topology and routing tables.
2. It requires extra CPU processing to run the SPF algorithm
3. It is complex to configure and more difficult to troubleshoot.

DIAGRAM-

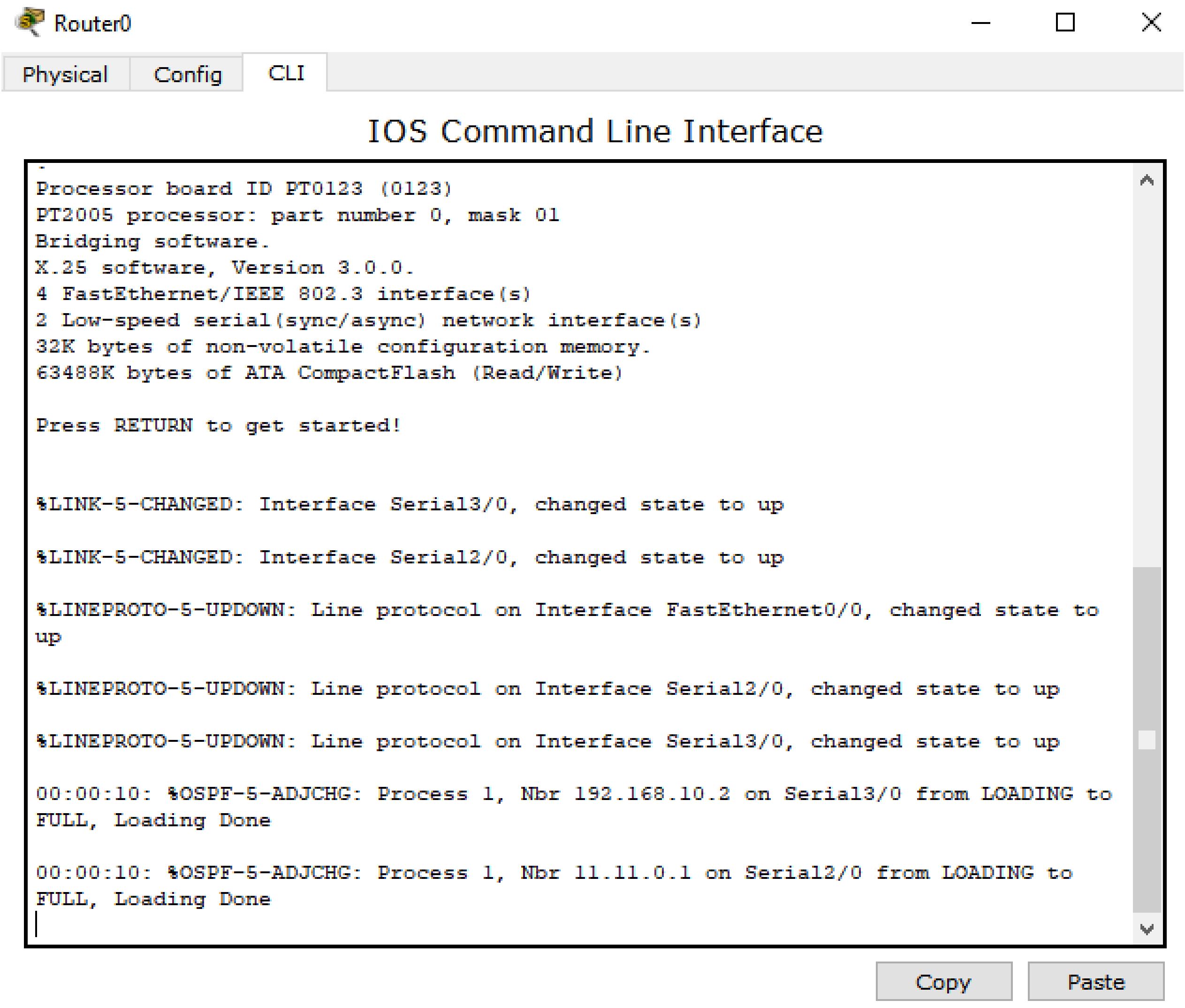


ADDRESSING TABLE -

S.NO	NAME OF DEVICE	IP ADDRESS	SUBNET MASK
1.	PC0	192.168.0.1	255.255.255.0
2.	PC1	192.168.10.1	255.255.255.0
3.	ROUTER0	192.168.0.2	255.255.255.0
4.	ROUTER2	192.168.10.2	255.255.255.0

ROUTER 0

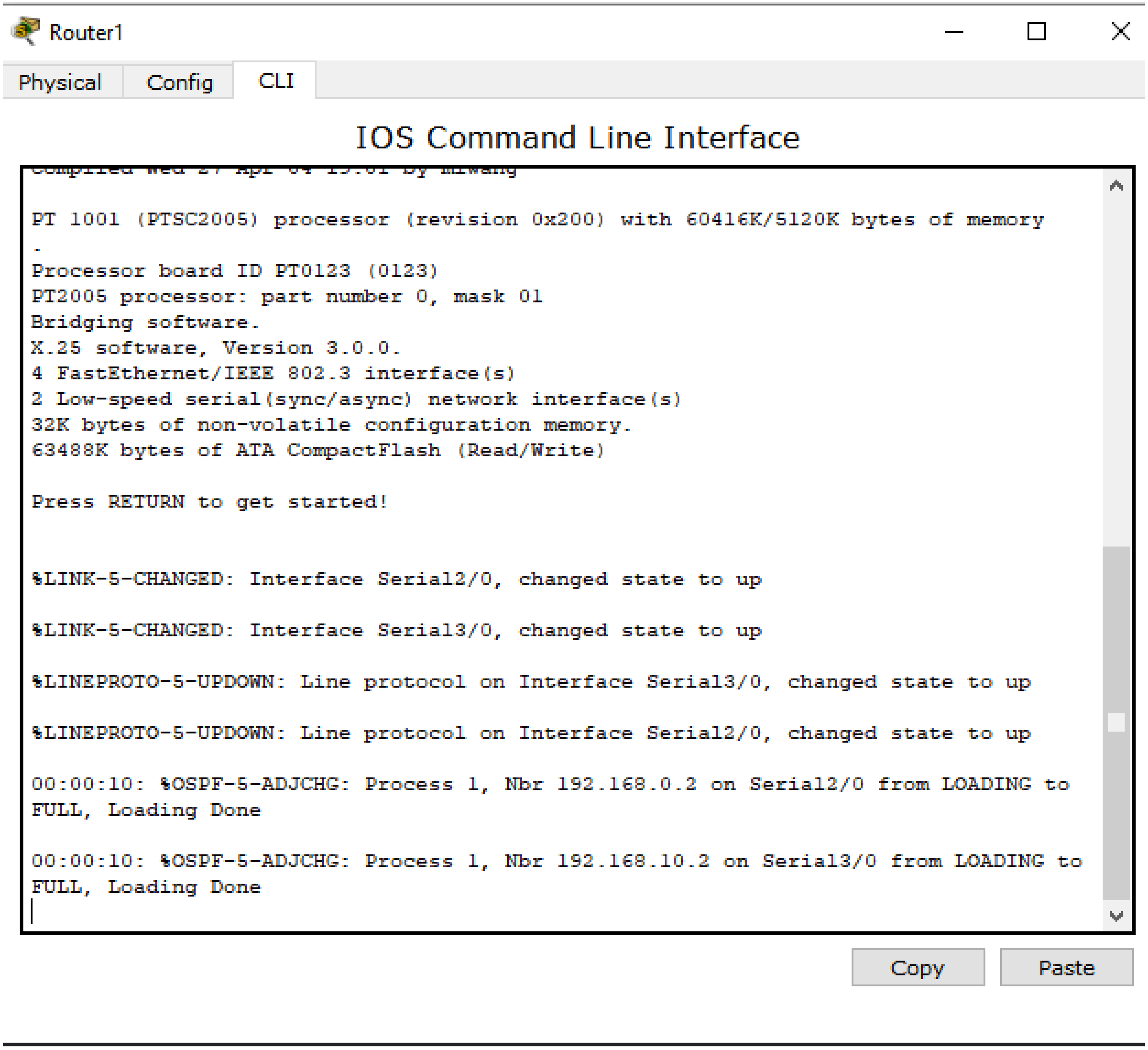
```
router >enable
router#configure terminal
router(config-if)#router ospf 1
router(config-router)#network 192.168.0.0 0.0.0.255 area 0
router(config-router)#network 10.10.0.0 255.0.0.0 area 0
router(config-router)#network 12.12.0.0 255.0.0.0 area 0
```



```
Processor board ID PT0123 (0123)
PT2005 processor: part number 0, mask 01
Bridging software.
X.25 software, Version 3.0.0.
4 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)

Press RETURN to get started!


%LINK-5-CHANGED: Interface Serial3/0, changed state to up

%LINK-5-CHANGED: Interface Serial2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0, changed state to up

00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.2 on Serial3/0 from LOADING to
FULL, Loading Done

00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.0.1 on Serial2/0 from LOADING to
FULL, Loading Done
```

ROUTER 1

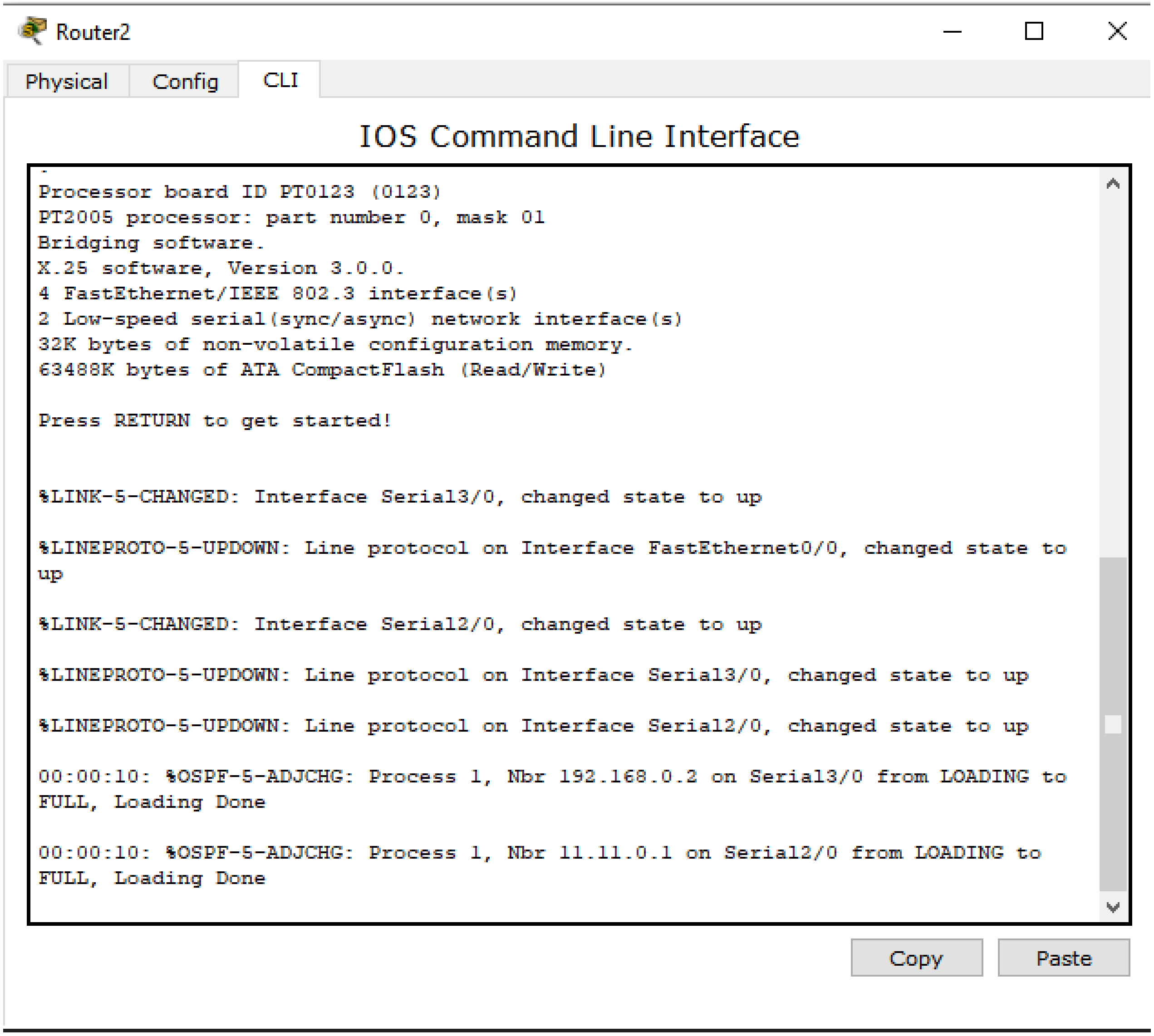
```
router >enable
router#configure terminal
router(config-if)#router ospf 1
router(config-router)#network 10.10.0.0 255.0.0.0 area 0
router(config-router)#network 11.11.0.0 255.0.0.0 area 0
```



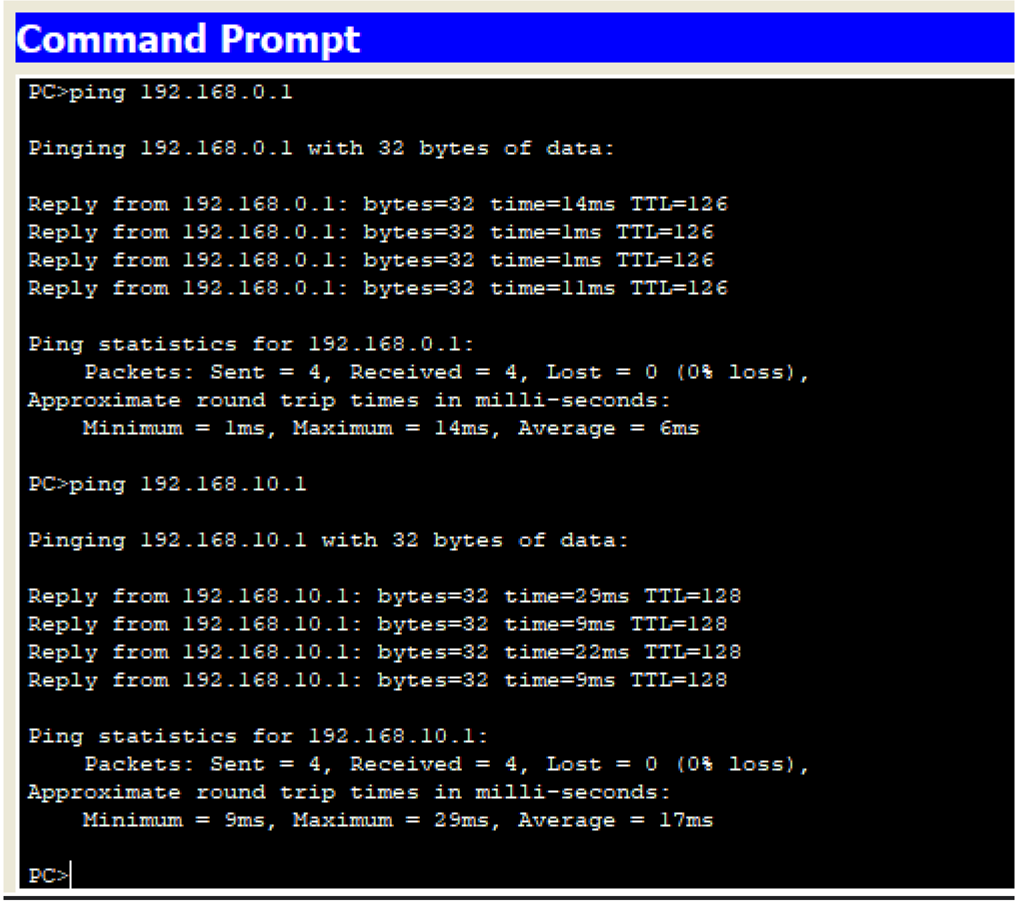
```
Compiled Wed 27 Apr 04 19:01 by miwang

PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory
.
Processor board ID PT0123 (0123)
PT2005 processor: part number 0, mask 01
Bridging software.
X.25 software, Version 3.0.0.
4 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)

Press RETURN to get started!


%LINK-5-CHANGED: Interface Serial2/0, changed state to up

%LINK-5-CHANGED: Interface Serial3/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up

00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.0.2 on Serial2/0 from LOADING to
FULL, Loading Done

00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.2 on Serial3/0 from LOADING to
FULL, Loading Done
```

ROUTER 0

```
router >enable
router#configure terminal
router(config-if)#router ospf 1
router(config-router)#network 11.11.0.0 255.0.0.0 area 0
router(config-router)#network 12.12.0.0 255.0.0.0 area 0
router(config-router)#network 192.168.10.0 0.0.0.255 area 0
```



```
Processor board ID PT0123 (0123)
PT2005 processor: part number 0, mask 01
Bridging software.
X.25 software, Version 3.0.0.
4 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)

Press RETURN to get started!


%LINK-5-CHANGED: Interface Serial3/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to
up

%LINK-5-CHANGED: Interface Serial2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up

00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.0.2 on Serial3/0 from LOADING to
FULL, Loading Done

00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.0.1 on Serial2/0 from LOADING to
FULL, Loading Done
```



```
PC>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=14ms TTL=126
Reply from 192.168.0.1: bytes=32 time=1ms TTL=126
Reply from 192.168.0.1: bytes=32 time=1ms TTL=126
Reply from 192.168.0.1: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 14ms, Average = 6ms

PC>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time=29ms TTL=128
Reply from 192.168.10.1: bytes=32 time=9ms TTL=128
Reply from 192.168.10.1: bytes=32 time=22ms TTL=128
Reply from 192.168.10.1: bytes=32 time=9ms TTL=128

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 29ms, Average = 17ms

PC>
```

RESULT - **Successful implementation of OSPF**

Experiment :8

Aim: To implement DHCP (Dynamic Host Configuration Protocol) using Cisco Packet Tracer.

DHCP: Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway. RFCs 2131 and 2132 define DHCP as an Internet Engineering Task Force (IETF) standard based on Bootstrap Protocol (BOOTP), a protocol with which DHCP shares many implementation details. DHCP allows hosts to obtain required TCP/IP configuration information from a DHCP server.

Windows Server 2016 includes DHCP Server, which is an optional networking server role that you can deploy on your network to lease IP addresses and other information to DHCP clients. All Windows-based client operating systems include the DHCP client as part of TCP/IP, and DHCP client is enabled by default.

Objective : Configure and analyze the performance of DHCP.

Advantages of DHCP:

1. Automatic management of IP addresses, including the prevention of duplicate IP address problems
2. Allows support for BOOTP clients, so you can easily transition your networks from BOOTP to DHCP
3. Allows the administrator to set lease times, even on manually allocated IP addresses.
4. Allows limiting which MAC addresses are served with dynamic IP addresses
5. Allows the administrator to configure additional DHCP option types, over and above what is possible with BOOTP
6. Allows the definition of the pool or pools of IP addresses that can be allocated dynamically. A user might have a server that forces the pool to be a whole subnet or network. The server should not force such a pool to consist of contiguous IP addresses.

Disadvantages of DHCP:

1.DHCP server can be single point of failure in networks having only one configured DHCP server.

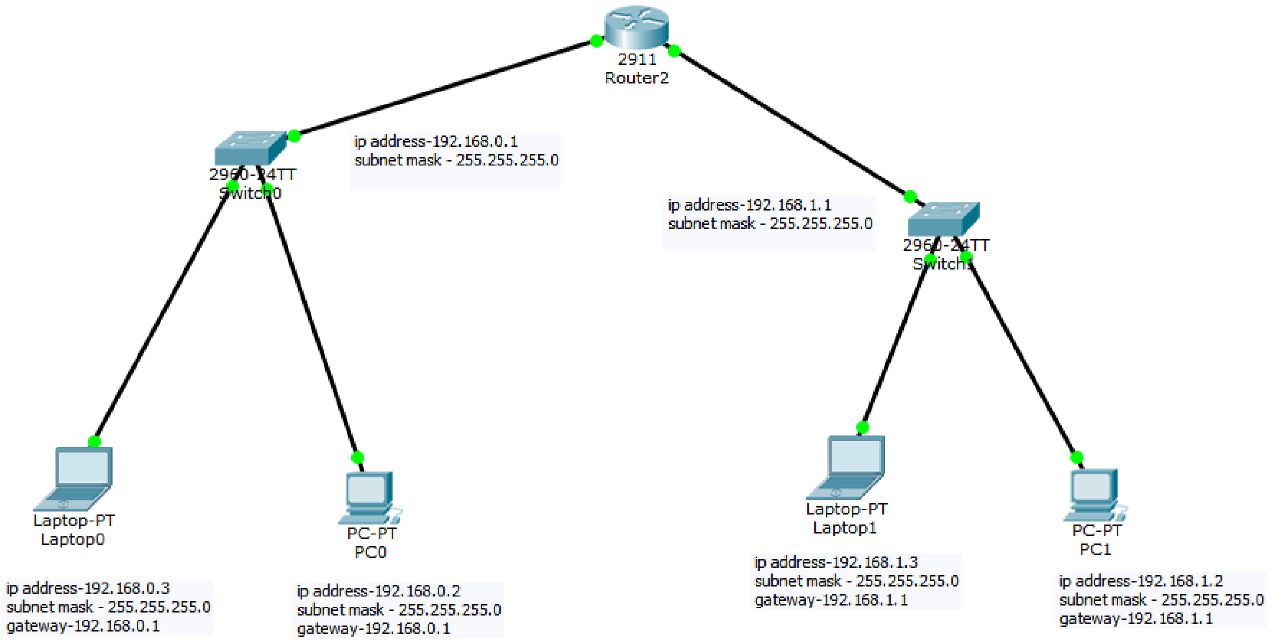
2. DHCP packets cannot travel across router, Hence relay agent is necessary to have DHCP server handle all leases on both network segments. Relay agents receive broadcast DHCP packets and forward them as unicast packets to DHCP server. Here relay agent must be configured with IP address of the DHCP server.

3. Security: As DHCP server has no secure mechanism for authentication of the client, it can gain unauthorized access to IP addresses by presenting credentials such as client identifiers which belong to other DHCP clients.

4. The machine name does not change when a new IP address is assigned.

5. Client is not able to access the network in the absence of the DHCP server.

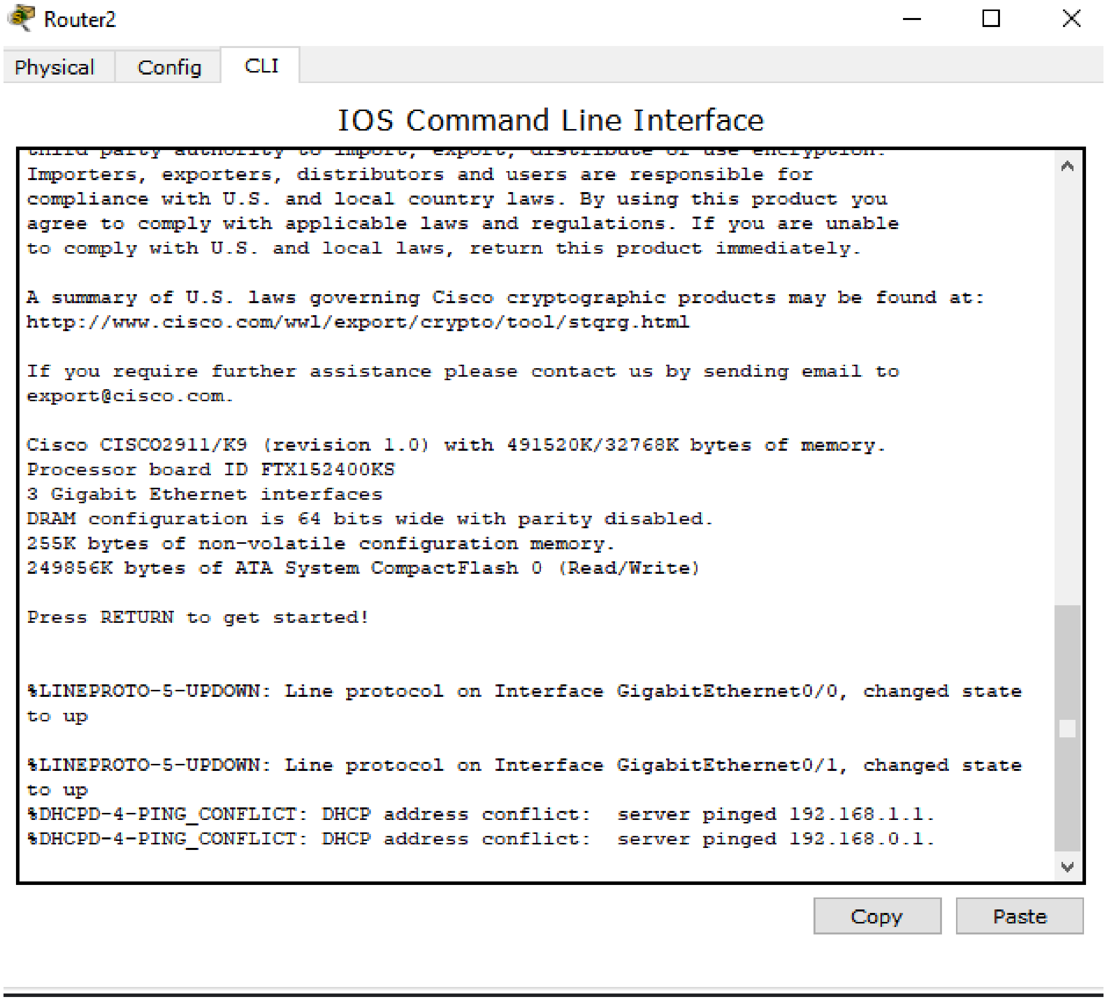
DIAGRAM-



ADDRESSING TABLE -

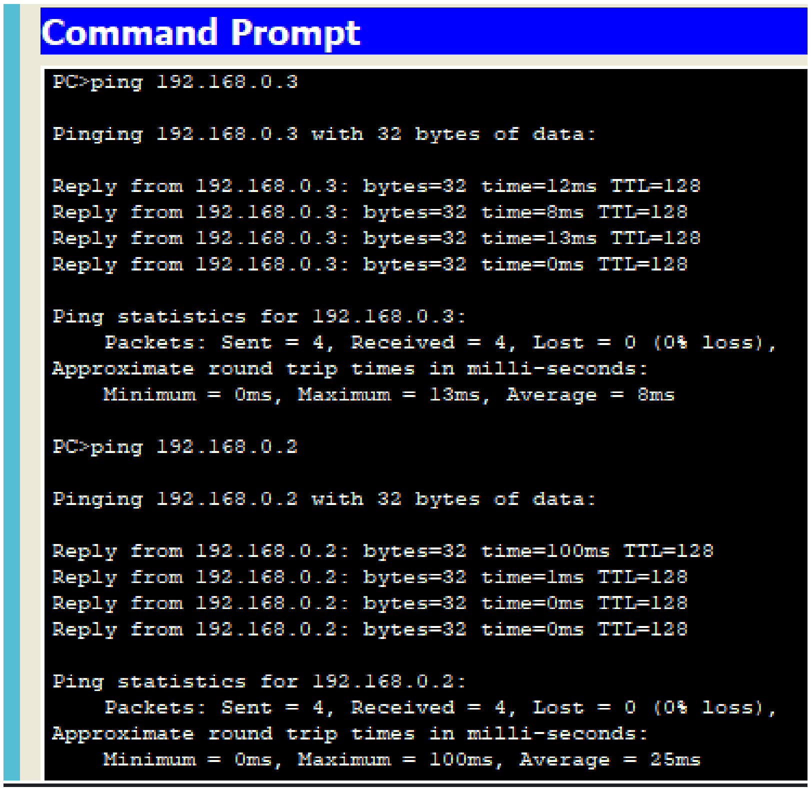
S.NO	NAME OF DEVICE	IP ADDRESS	SUBNET MASK
1.	PC0	192.168.0.2	255.255.255.0
2.	PC1	192.168.1.2	255.255.255.0
3.	laptop0	192.168.0.3	255.255.255.0
4.	laptop1	192.168.1.3	255.255.255.0

Router
Ip dhcp pool pool_name

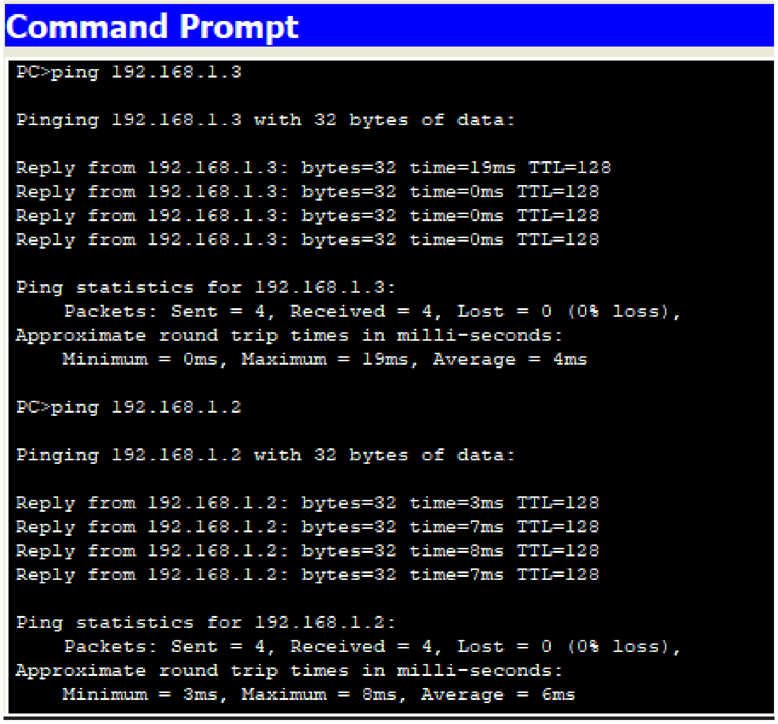


```
third party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco CISCO2911/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
3 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!


%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state
to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state
to up
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 192.168.1.1.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 192.168.0.1.
```

PING-



```
PC>ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:

Reply from 192.168.0.3: bytes=32 time=12ms TTL=128
Reply from 192.168.0.3: bytes=32 time=8ms TTL=128
Reply from 192.168.0.3: bytes=32 time=13ms TTL=128
Reply from 192.168.0.3: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 8ms

PC>ping 192.168.0.2

Pinging 192.168.0.2 with 32 bytes of data:

Reply from 192.168.0.2: bytes=32 time=100ms TTL=128
Reply from 192.168.0.2: bytes=32 time=1ms TTL=128
Reply from 192.168.0.2: bytes=32 time=0ms TTL=128
Reply from 192.168.0.2: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 100ms, Average = 25ms
```



```
PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=19ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128

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

PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=3ms TTL=128
Reply from 192.168.1.2: bytes=32 time=7ms TTL=128
Reply from 192.168.1.2: bytes=32 time=8ms TTL=128
Reply from 192.168.1.2: bytes=32 time=7ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 8ms, Average = 6ms
```

RESULT - **Successful implementation of DHCP**

Experiment - 9

Aim: To implement NAT (Network Address Translation) using Cisco Packet Tracer

NAT - Network address translation (NAT) is a method of mapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.

We can also say, It is a way to map multiple local private addresses to a public one before transferring the information.

Working - Let’s say that there is a laptop connected to a home router. Someone uses the laptop to search for directions to their favourite restaurant. The laptop sends this request in a packet to the router, which passes it along to the web. But first, the router changes the outgoing IP address from a private local address to a public address.

If the packet keeps a private address, the receiving server won’t know where to send the information back to — this is akin to sending physical mail and requesting return service but providing a return address of anonymous. By using NAT, the information will make it back to the laptop using the router’s public address, not the laptop’s private one

Types of NAT –

1. Static NAT - When the local address is converted to a public one, this NAT chooses the same one. This means there will be a consistent public IP address associated with that router or NAT device.

2. Dynamic NAT - Instead of choosing the same IP address every time, this NAT goes through a pool of public IP addresses. This results in the router or NAT device getting a different address each time the router translates the local address to a public address.

3. PAT - PAT stands for port address translation. It’s a type of dynamic NAT, but it bands several local IP addresses to a singular public one. Organizations that want all their employees’ activity to use a singular IP address use a PAT, often under the supervision of a network administrator.

Advantages -:

1. NAT helps in preserving the IPv4 address space when the user uses NAT overload

2. NAT enhances the reliability and flexibility of interconnections to the global network by deploying multiple source pools, load balancing pool, and backup pools.

3. NAT has a prominent network addressing method. If there is the usage of a global IP address, then address space should be properly assigned. Because when a network is developed, there might be a need for many IP address

4. NAT gives an added layer of security in the network because the host inbuilt in the NAT network are unreachable by other network devices as per user preference.

Disadvantages-:

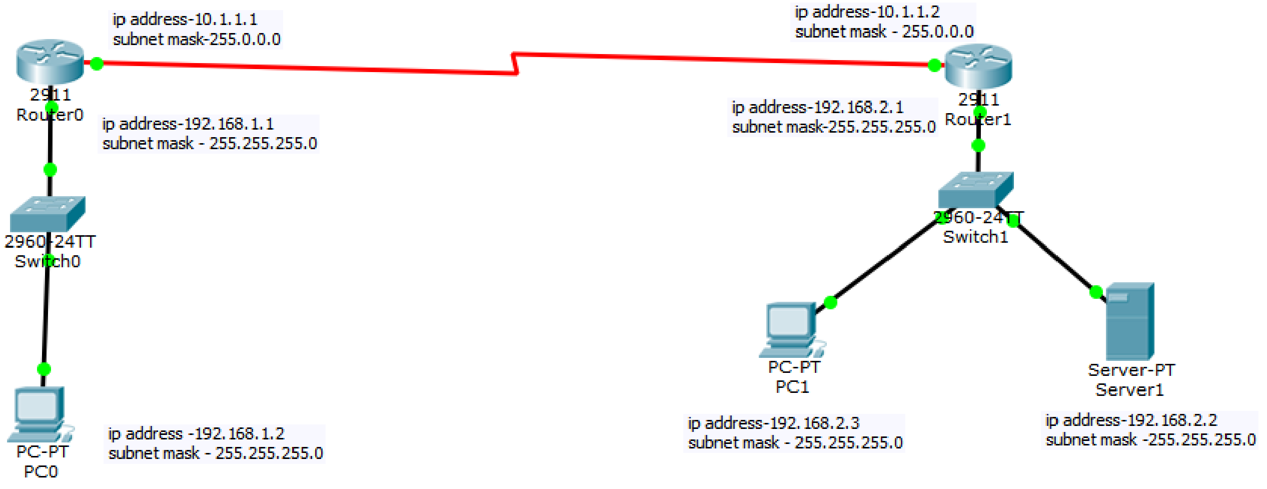
1. When a guest request for remote access, it will double-check whether connections are from the router belongs to NAT. But some guests established the connection from another host; if the particular user doesn't respond to the correct host, then it will get a request, another host. This criterion will lead to degrading in the performance of the network

2. If multiple applications and protocols rely on end-to-end functions, then the user's network cannot be accessible by other users. Because the host is inbuilt inside the NAT network, which is unreachable, as discussed above

3. If there is any need to troubleshoot the network from remote areas, troubleshooting will be tough and lead to loss of end traceability.

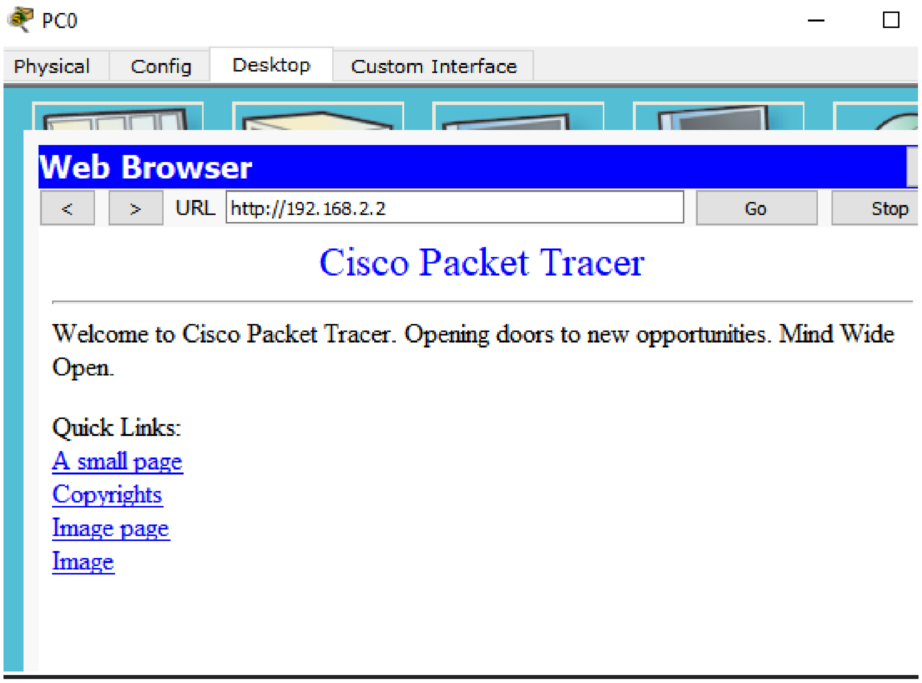
4. Services that need UDP or TCP installation connections from the global side can be impacted and maybe not reachable at times.

DIAGRAM-



ADDRESSING TABLE -

S.NO	NAME OF DEVICE	IP ADDRESS	SUBNET MASK
1.	PC0	192.168.1.2	255.255.255.0
2.	PC1	192.168.2..3	255.255.255.0
3.	ROUTER0	192.168.1.1	255.255.255.0
4.	ROUTER1	192.168.2.1	255.255.255.0
5.	SERVER1	192.168.2.2	255.255.255.0

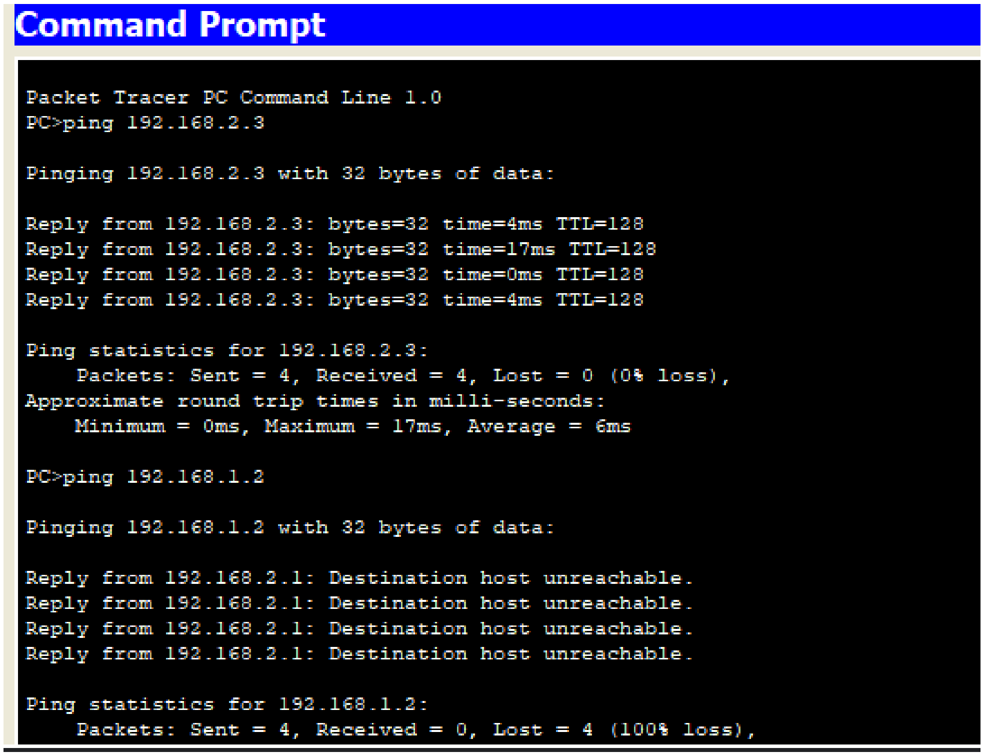


http://192.168.2.2

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=4ms TTL=128
Reply from 192.168.2.3: bytes=32 time=17ms TTL=128
Reply from 192.168.2.3: bytes=32 time=0ms TTL=128
Reply from 192.168.2.3: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 17ms, Average = 6ms

PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

RESULT - **Successful implementation of NAT**

EXPERIMENT :- 10

AIM : To implement VLAN using Cisco packet Tracer.

VLAN: A VLAN (virtual LAN) is a subnetwork which can group together collections of devices on separate physical local area networks (LANs). A LAN is a group of computers and devices that share a communications line or wireless link to a server within the same geographical area.

VLANs make it easy for network administrators to partition a single switched network to match the functional and security requirements of their systems without having to run new cables or make major changes in their current network infrastructure. VLANs are often set up by larger businesses to re-partition devices for better traffic management.

Advantages of VLAN :-

- VLANs provide a number of advantages, such as ease of administration, confinement of broadcast domains, reduced broadcast traffic, and enforcement of security policies.

- Higher performance and reduced latency.

- Users may work on sensitive information which should not be seen by other users.

- VLANs reduce the need to have routers deployed on a network to contain broadcast traffic.

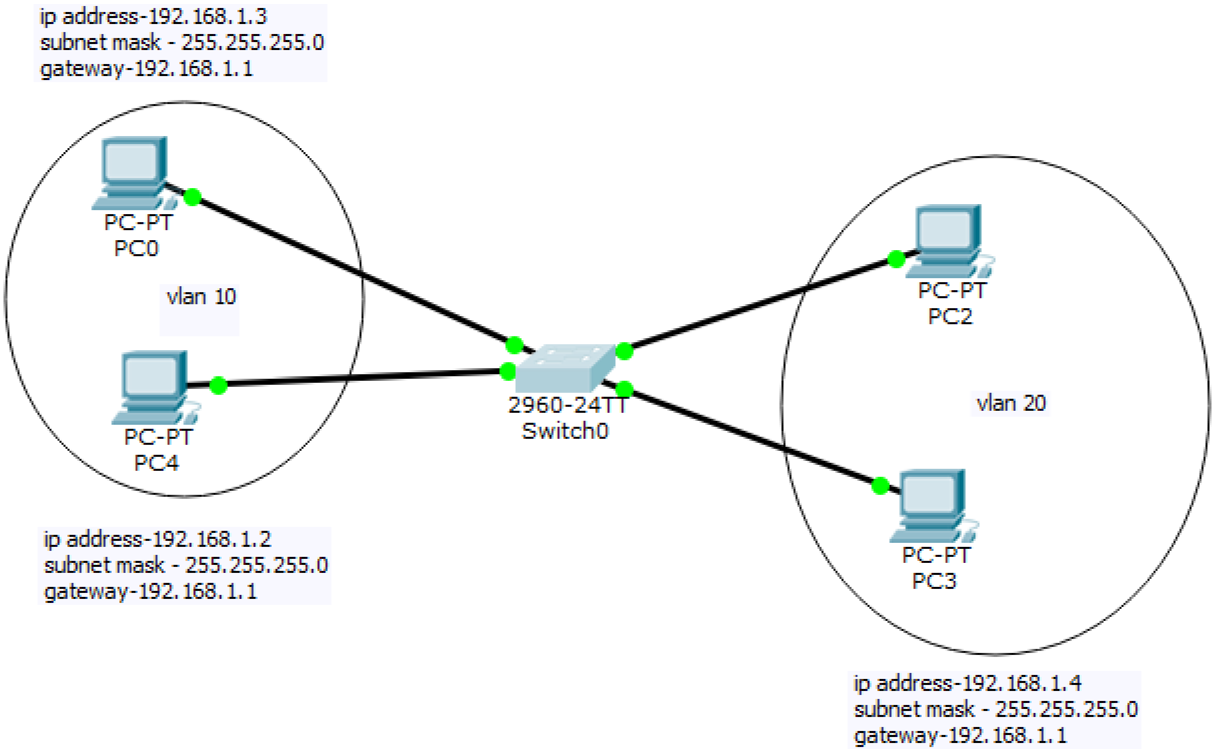
Disadvantages of VLAN :-

- Management is complex

- Possible problems in interoperability

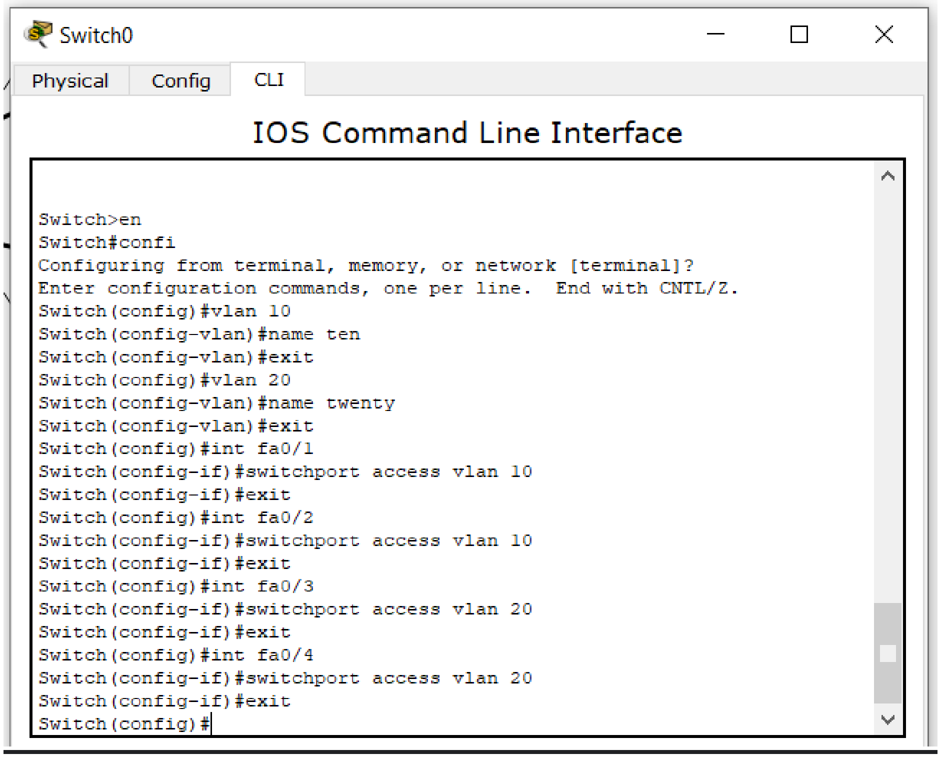
- A VLAN cannot forward traffic to another VLAN (need a router to communicate between VLANs)

DIAGRAM-

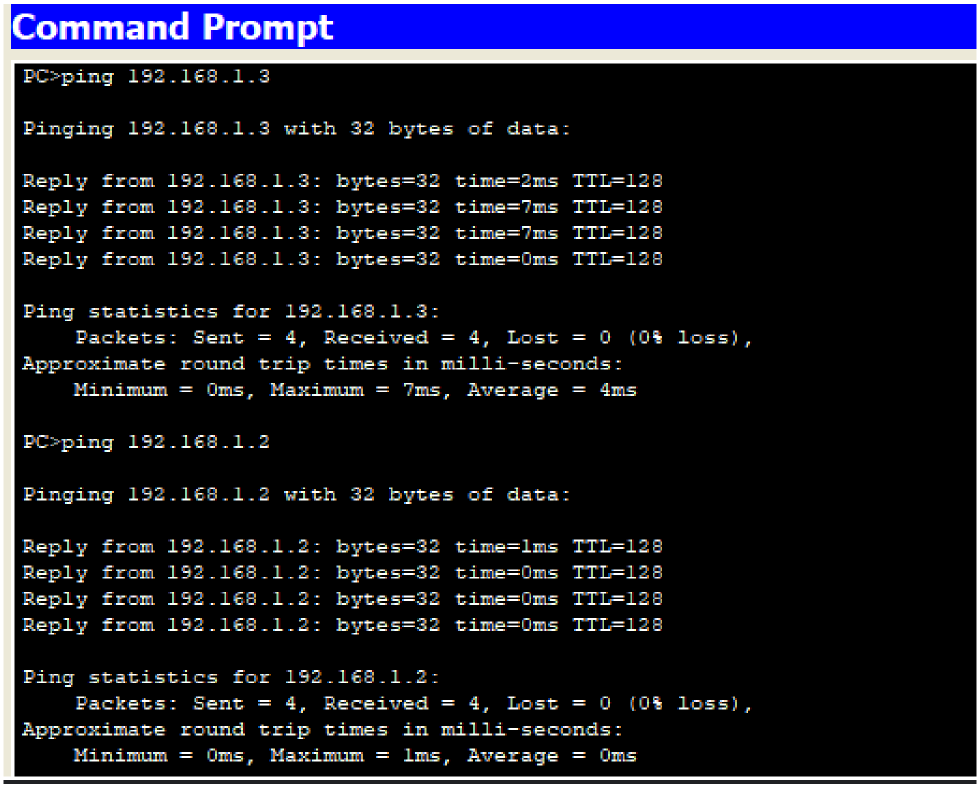


ADDRESSING TABLE -

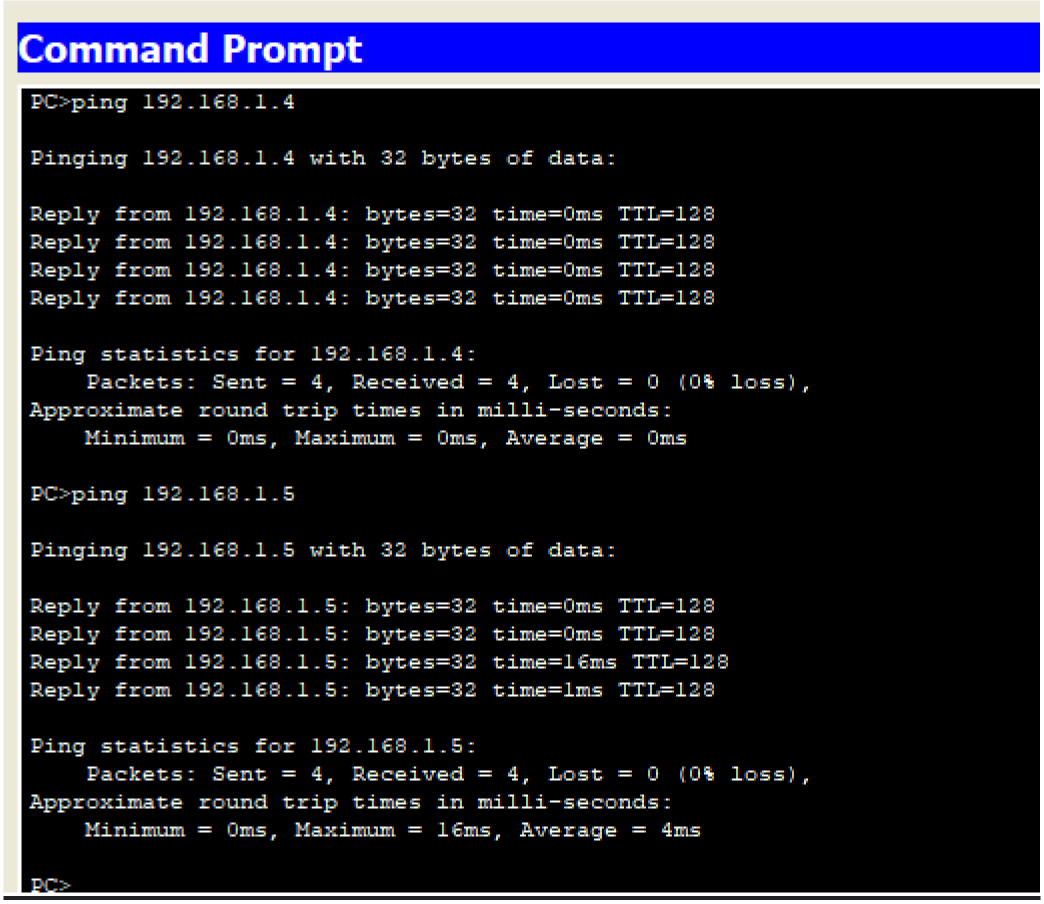
S.NO	NAME OF DEVICE	IP ADDRESS	SUBNET MASK
1.	PC0	192.168.1.3	255.255.255.0
2.	PC2	192.168.1.5	255.255.255.0
3.	PC3	192.168.1.4	255.255.255.0
4.	PC4	192.168.1.2	255.255.255.0



```
Switch>en
Switch#confi
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name ten
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name twenty
Switch(config-vlan)#exit
Switch(config)#int fa0/1
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#int fa0/2
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#int fa0/3
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#int fa0/4
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#
```



```
PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=2ms TTL=128
Reply from 192.168.1.3: bytes=32 time=7ms TTL=128
Reply from 192.168.1.3: bytes=32 time=7ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 7ms, Average = 4ms

PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=0ms TTL=128
Reply from 192.168.1.2: bytes=32 time=0ms TTL=128
Reply from 192.168.1.2: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```



```
PC>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time=0ms TTL=128
Reply from 192.168.1.4: bytes=32 time=0ms TTL=128
Reply from 192.168.1.4: bytes=32 time=0ms TTL=128
Reply from 192.168.1.4: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time=0ms TTL=128
Reply from 192.168.1.5: bytes=32 time=0ms TTL=128
Reply from 192.168.1.5: bytes=32 time=16ms TTL=128
Reply from 192.168.1.5: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 16ms, Average = 4ms

PC>
```

RESULT - **Successful implementation of VLAN**

EXPERIMENT :- 11

AIM : To trace packet in Wireshark.

Wireshark:

Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format. Wireshark includes filters, color coding, and other features that let you dig deep into network traffic and inspect individual packets.

This tutorial will get you up to speed with the basics of capturing packets, filtering them, and inspecting them. You can use Wireshark to inspect a suspicious program’s network traffic, analyze the traffic flow on your network, or troubleshoot network problems.

After starting Wireshark, do the following:

1. Select Capture | Interfaces

2. Select the interface on which packets need to be captured. This will usually be the interface where the Packet/s column is constantly changing, which would indicate the presence of live traffic). If you have multiple network interface cards (i.e. LAN card and Wi-Fi adapter) you may need to check with your IT administrator to determine the right interface.

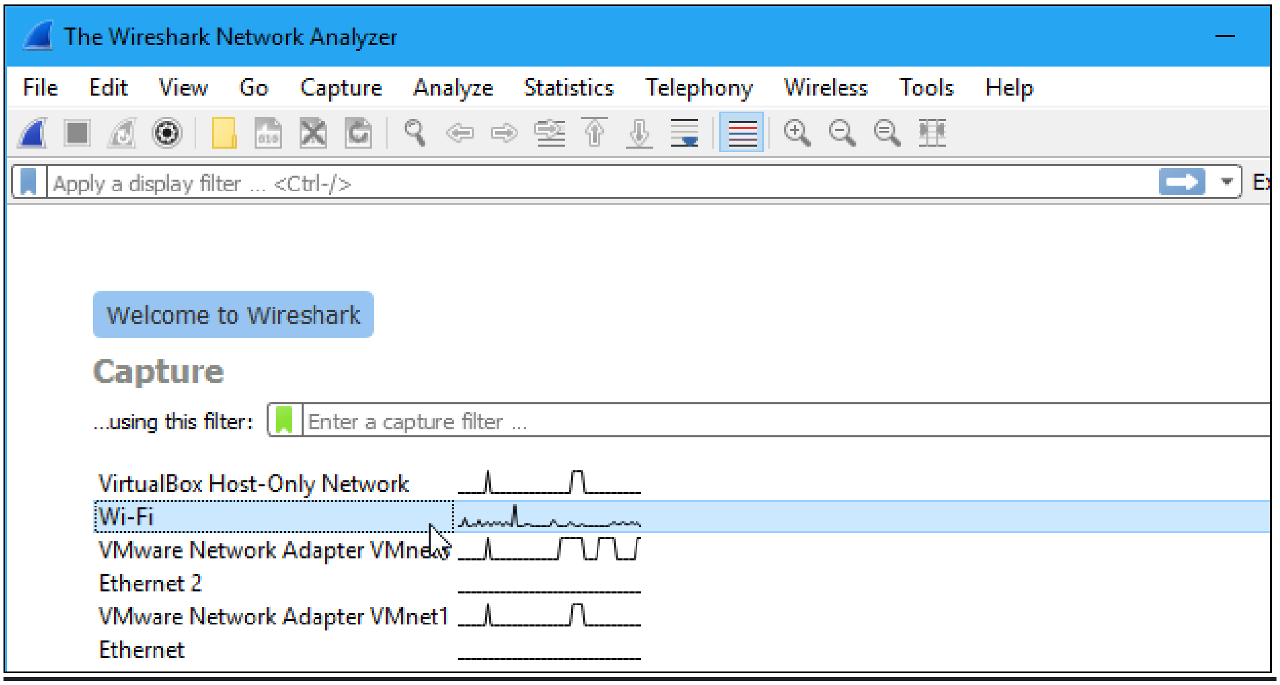
3. Click the Start button to start the capture.

4. Recreate the problem. The capture dialog should show the number of packets increasing. Try to avoid running any other internet applications while capturing, closing other browsers, Instant messengers etc.

5. Once the problem which is to be analyzed has been reproduced, click on Stop. It may take a few seconds for Wireshark to display the packets captured.

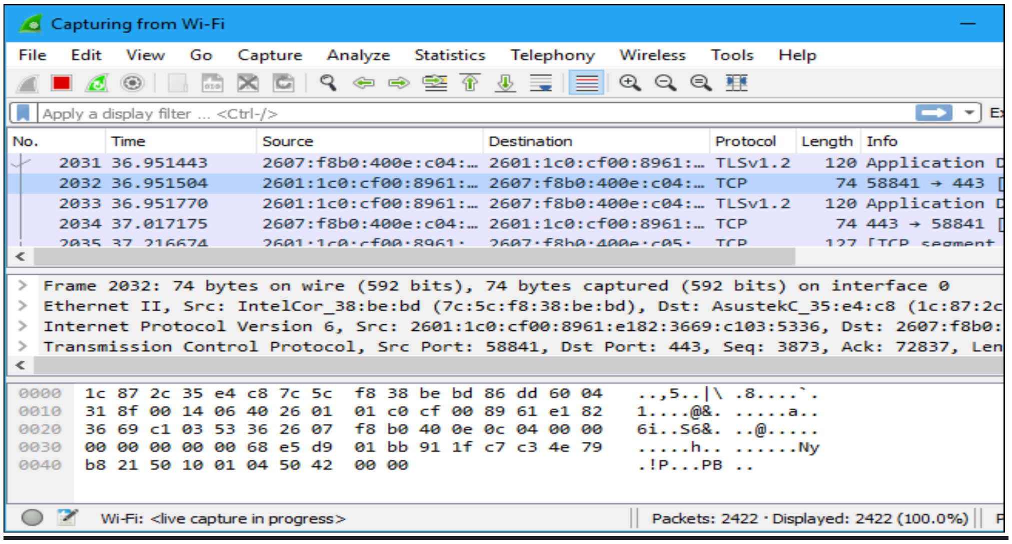
6. Save the packet trace in the default format. Click on the File menu option and select Save As. By default Wireshark will save the packet trace in libpcap format. This is a filename with a.pcap extension.

After downloading and installing Wireshark, you can launch it and double-click the name of a network interface under Capture to start capturing packets on that interface. For example, if you want to capture traffic on your wireless network, click your wireless interface. You can configure advanced features by clicking Capture > Options, but this isn't necessary for now.


The Wireshark Network Analyzer
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
Ex
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
VirtualBox Host-Only Network
Wi-Fi
VMware Network Adapter VMnet8
Ethernet 2
VMware Network Adapter VMnet1
Ethernet

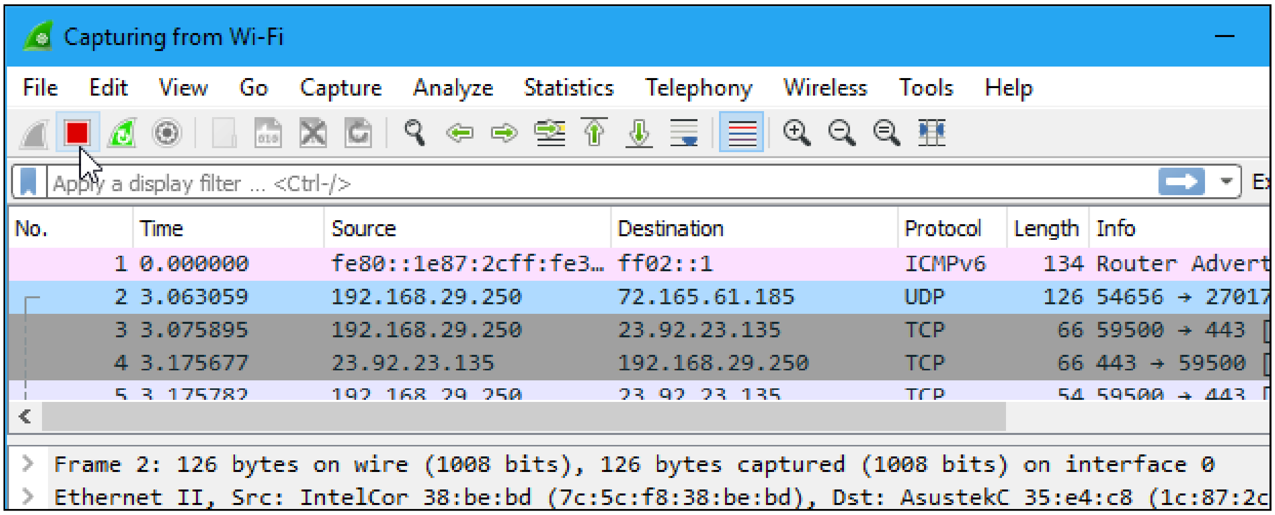
As soon as you click the interface's name, you'll see the packets start to appear in real time. Wireshark captures each packet sent to or from your system.

If you have promiscuous mode enabled—it's enabled by default—you'll also see all the other packets on the network instead of only packets addressed to your network adapter. To check if promiscuous mode is enabled, click Capture > Options and verify the "Enable promiscuous mode on all interfaces" checkbox is activated at the bottom of this window.


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.    Time       Source                   Destination              Protocol  Length Info
  2031 36.951443  2607:f8b0:400e:c04:…     2601:1c0:cf00:8961:…     TLSv1.2     120 Application D
  2032 36.951504  2601:1c0:cf00:8961:…     2607:f8b0:400e:c04:…     TCP          74 58841 → 443 [
  2033 36.951770  2601:1c0:cf00:8961:…     2607:f8b0:400e:c04:…     TLSv1.2     120 Application D
  2034 37.017175  2607:f8b0:400e:c04:…     2601:1c0:cf00:8961:…     TCP          74 443 → 58841 [
  2035 37.216674  2601:1c0:cf00:8961:      2607:f8b0:400e:c05:      TCP         127 [TCP segment

> Frame 2032: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: IntelCor_38:be:bd (7c:5c:f8:38:be:bd), Dst: AsustekC_35:e4:c8 (1c:87:2c
> Internet Protocol Version 6, Src: 2601:1c0:cf00:8961:e182:3669:c103:5336, Dst: 2607:f8b0:
> Transmission Control Protocol, Src Port: 58841, Dst Port: 443, Seq: 3873, Ack: 72837, Len

0000  1c 87 2c 35 e4 c8 7c 5c  f8 38 be bd 86 dd 60 04   ..,5..|\ .8....`.
0010  31 8f 00 14 06 40 26 01  01 c0 cf 00 89 61 e1 82   1....@&. .....a..
0020  36 69 c1 03 53 36 26 07  f8 b0 40 0e 0c 04 00 00   6i..S6&. ..@.....
0030  00 00 00 00 00 68 e5 d9  01 bb 91 1f c7 c3 4e 79   .....h.. ......Ny
0040  b8 21 50 10 01 04 50 42  00 00                     .!P...PB ..

Wi-Fi: <live capture in progress>        Packets: 2422 · Displayed: 2422 (100.0%)
```

Click the red “Stop” button near the top left corner of the window when you want to stop capturing traffic.


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.    Time       Source                   Destination              Protocol  Length Info
     1 0.000000   fe80::1e87:2cff:fe3…     ff02::1                  ICMPv6      134 Router Advert
     2 3.063059   192.168.29.250           72.165.61.185            UDP         126 54656 → 27017
     3 3.075895   192.168.29.250           23.92.23.135             TCP          66 59500 → 443 [
     4 3.175677   23.92.23.135             192.168.29.250           TCP          66 443 → 59500 [
     5 3.175782   192.168.29.250           23.92.23.135             TCP          54 59500 → 443 [

> Frame 2: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface 0
> Ethernet II, Src: IntelCor_38:be:bd (7c:5c:f8:38:be:bd), Dst: AsustekC_35:e4:c8 (1c:87:2c
```

Result:

Packet Traced in Wireshark Successfully.