Linnéuniversitetet
Kalmar Växjö

Report

Assignment 4

1DV701

Author: Katarina Simakina
Semester: Spring 2023
Email es225hi@student.lnu.se

Linnéuniversitetet
Kalmar Växjö

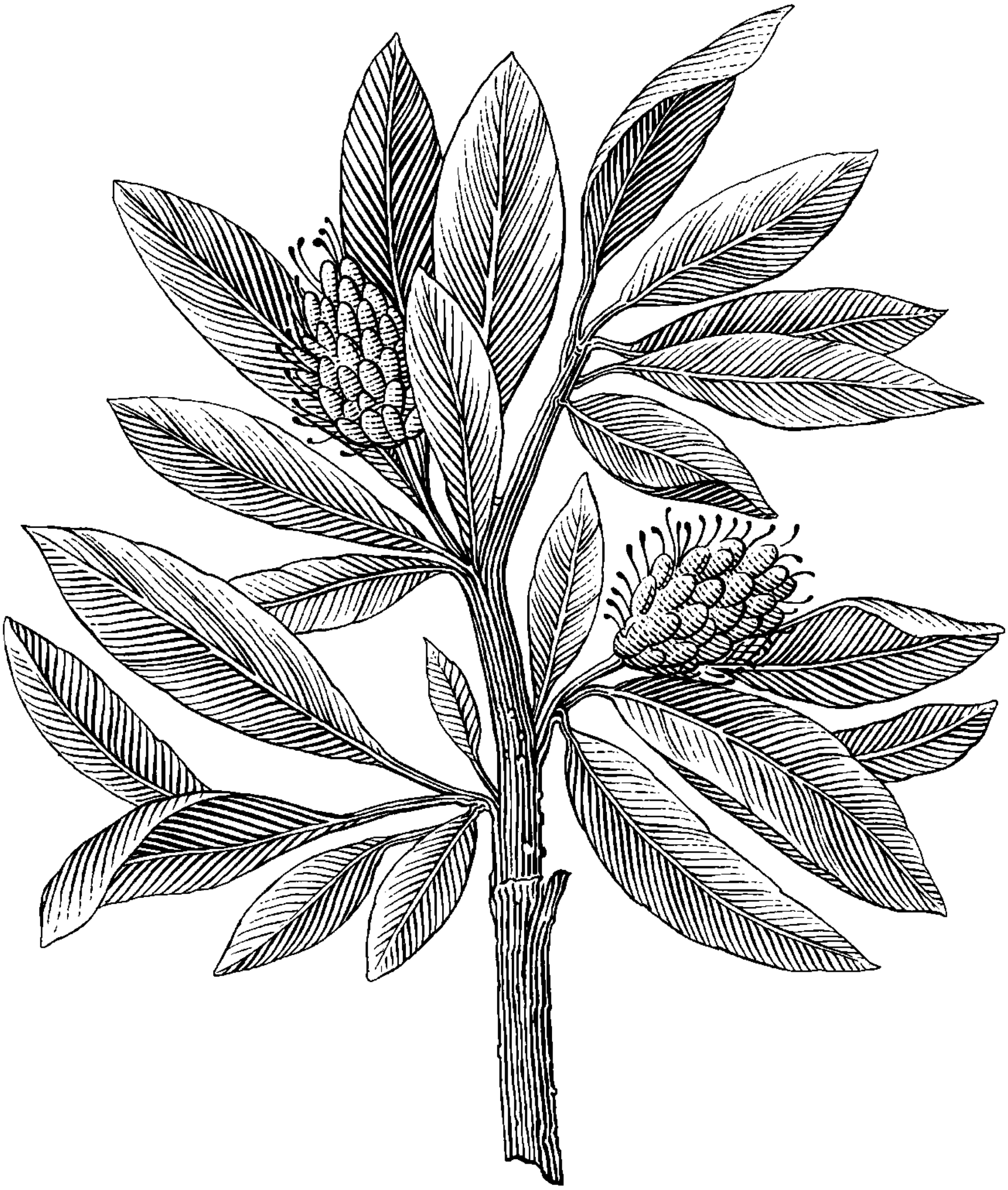
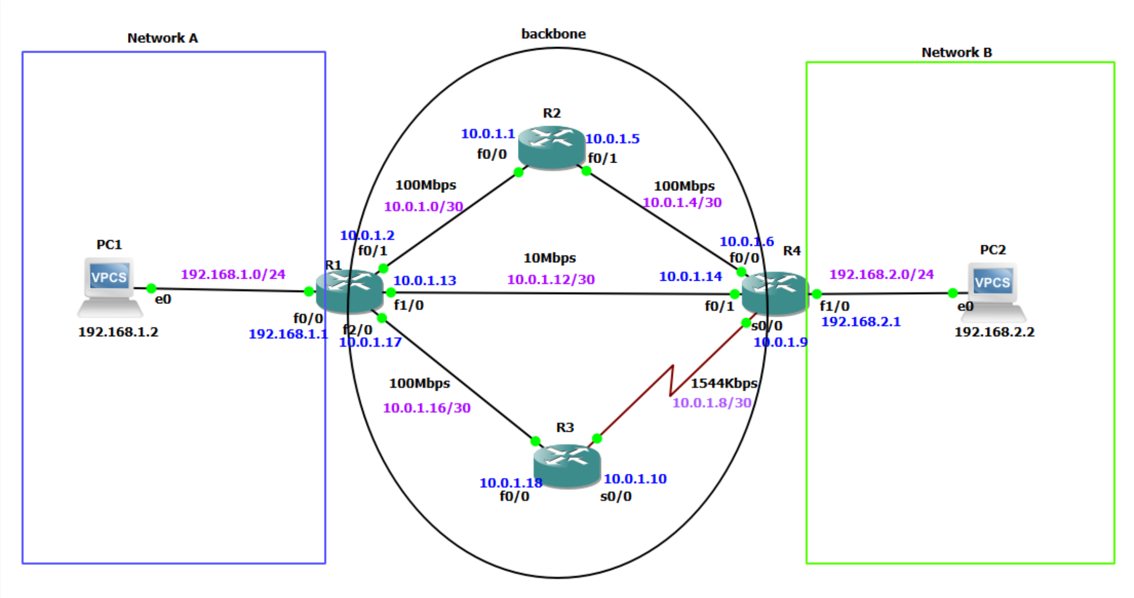


Table of Contents

Problem 1
1.a



1.b Screenshots of pings from R1 to PC-1.

Figure1. Screenshots of pings from R1 to PC-1.

Screenshots of pings from R1 to R4.

Figure 2. Screenshots of pings from R1 to R4.

Screenshots of pings from PC-1 to PC-2. It was information that it is Destination unreachable as PC1 can see only its neighbours.

Figure 3. Screenshots of pings from PC-1 to PC-2.

1.c <u>An explanation of NM-1FE-TX and WIC-1T abbreviations and why these modules are chosen among the available alternatives.</u>

NM-1FE-TX and WIC-1T are both interface modules used in Cisco networking equipment.

NM-1FE-TX stands for "Network Module with one Fast Ethernet port (100BASE-TX)". It is a network module that provides one Fast Ethernet (FE) port with a transmission rate of 100 Mbps over a twisted-pair copper cable. It uses the RJ-45 connector, which is a common connector used in Ethernet networks. <u>The NM-1FE-TX module is chosen when there is a need for additional Fast Ethernet ports on a network device</u>.

WIC-1T stands for "WAN Interface Card with one serial port (T1/E1)". It is a type of WAN interface card that provides one serial port for connecting to a WAN link. It supports both T1 and E1 transmission rates and uses a DB-60 connector. The WIC-1T module is chosen when there is a need to connect to a WAN link using a serial connection.

The properties of each type of interface are as follows:

Fast Ethernet (FE) is a high-speed Ethernet standard that supports a data transfer rate of 100 Mbps. It is commonly used in LAN networks to connect devices such as computers, printers, and switches. Serial connections are used to connect to WAN links such as leased lines, frame relay, or T1/E1 circuits. The serial port provides a dedicated point-to-point connection between two devices.

The NM-1FE-TX and WIC-1T interface modules are chosen based on the specific requirements of the network. The NM-1FE-TX is used when there is a need for additional Fast Ethernet ports, while the WIC-1T is used when there is a need to connect to a WAN link using a serial connection.

The NM-1FE-TX and WIC-1T interface modules are chosen for this network due to its specific bandwidth requirements. With three different bandwidths needed - 100Mbps, 10Mbps, and 1544Kbps - the network needs flexible interface modules to handle the varying demands.

The NM-1FE-TX module is an ideal choice for the uplink and middle lines because of its auto sensing and auto-negotiating capabilities. It can automatically adjust to the required bandwidths of 100Mbps and 10Mbps, which helps to ensure efficient network operation and reduces the need for manual configuration.

The WIC-1T module is chosen to establish a serial connection between R3 and R4 with a maximum speed of 2Mbps. The WIC-1T's capabilities match the requirements of this particular connection, making it a suitable fit for the network.

In conclusion, the decision to use the NM-1FE-TX and WIC-1T interface modules is based on the network's specific bandwidth requirements. These modules provide the flexibility and performance needed to support the network's operations effectively. The auto sensing and auto-negotiating capabilities of the NM-1FE-TX module and the suitable features of the WIC-1T module make them the optimal choice for this network configuration.

1.d Difference between a/24 and a/30 subnet.

a/24:
Subnet mask is 255.255.255.0
Number of the addresses is 256.
Number of the hosts is 254.

a/30:
Subnet mask is 255.255.255.252
Number of the addresses is 4.
Number of the hosts is 2.

The practical difference between a/24 and a/30 subnet is that a/24 subnet provides a larger range of IP addresses and is typically used for larger LANs (between network A and B it needs more IP addresses), while a /30 subnet provides a smaller range of IP addresses and is typically used for point-to-point connections. In the backbone, it is used a/30, communication mainly is going between routers not between end hosts so it can be useful for connecting the routers as it minimizes the wastage of IP addresses and ensures efficient use of address space.

Problem 2.

2.a Explain each of the parameters of the ip route command.

enable
conf t
ip route [ip] [mask] [router_interface] [metric]
end

ip route – the command to configure a static route on a Cisco IOS device.
[ip] - the IP address of the destination network.
[mask] - the subnet mask associated with the destination IP address.
[router_interface] - the interface through which the destination network or host can be reached. It is specified as the next-hop IP address of a router that can forward the packets to the destination.
[metric]- it is a value used by routing algorithms to determine the best path to a destination network. The metric indicates the distance or cost to reach the destination network, and the route with the lowest metric is usually chosen as the best path. The valid range for the metric is from 1 to 255. The default metric value is 1, but it can be adjusted according to specific requirements.

2.b I have choosen the routing part from R1 to R4 to create static routing as short distance. That is, we have on this path only two routers. If we compare and take other choice for example path will be R1-R2-R3: there are 3 routers, it is not so efficient. So, the choice from R1 to R4 is so effective as the route from PC1 to PC2 has less routers and less possible failures.

Figure 4. Screenshots of pings from PC-1 to PC-2.

Figure 5. Screenshots trace route.

The route has been used R1-R4 (look to the Figure 5). It has less routers than others routes.

2.c Shutdown interfaces:

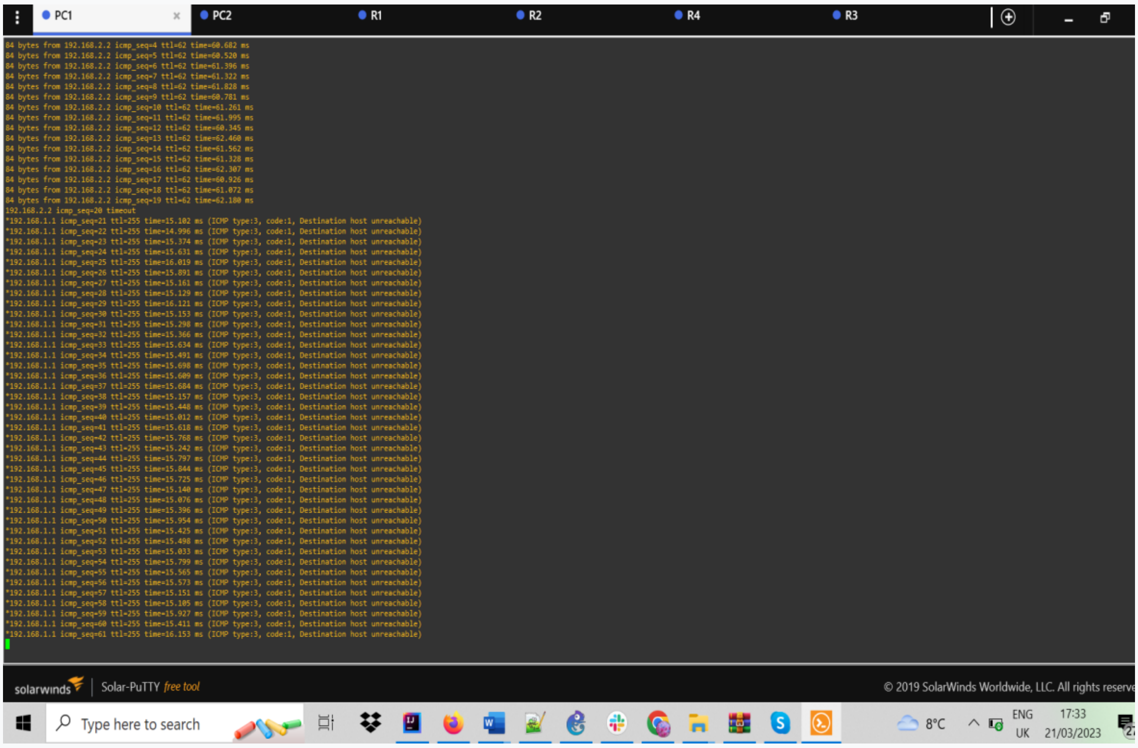


Figure 6. Screenshot ping failure after shutdown the interfaces

Please look on the Figure 6. I have started a continuous ping from PC-1 and PC-2 and then shut down both active router interfaces. My observation showed that the active interfaces on both sides of routers R1 and R4 were shut down after ping from PC1 to PC2. As a result, the ping responses indicated that the destination was unreachable.

2.d Configure the remaining two possible routing paths between PC-1 and PC-2:

The following remaining two possible routing paths between PC-1 and PC-2:
-the route starts from R1 and passing through R2 and R4, it has a metric of 2.
-the route starts from R1 and passing through R3 and R4, it has a metric of 3.

To observe how many packets are lost three routing paths have been configured:

1. R1-R4 with metric 1.
2. R1-R2-R4 with metric 2.
3. R1-R3-R4 with metric 3.

I have started a continuous ping from PC-1 to PC-2. The first route which have been used was R1 to R4. After it the following routers such as R1 and R4 have been shut down. The router R1 have been shut down and we got error message that “Destination host unreachable” . It has been sent by the router to indicate that the destination host is not reachable. After it, the router R4 have been shut down and we got error timeout. A "timeout" message indicates that the sender did not receive a response from the destination host within a certain time period. After it, the new route has been found and it starts working in normal way. It was lost 4 packets before the new route has been found. Please look the Figure 7.

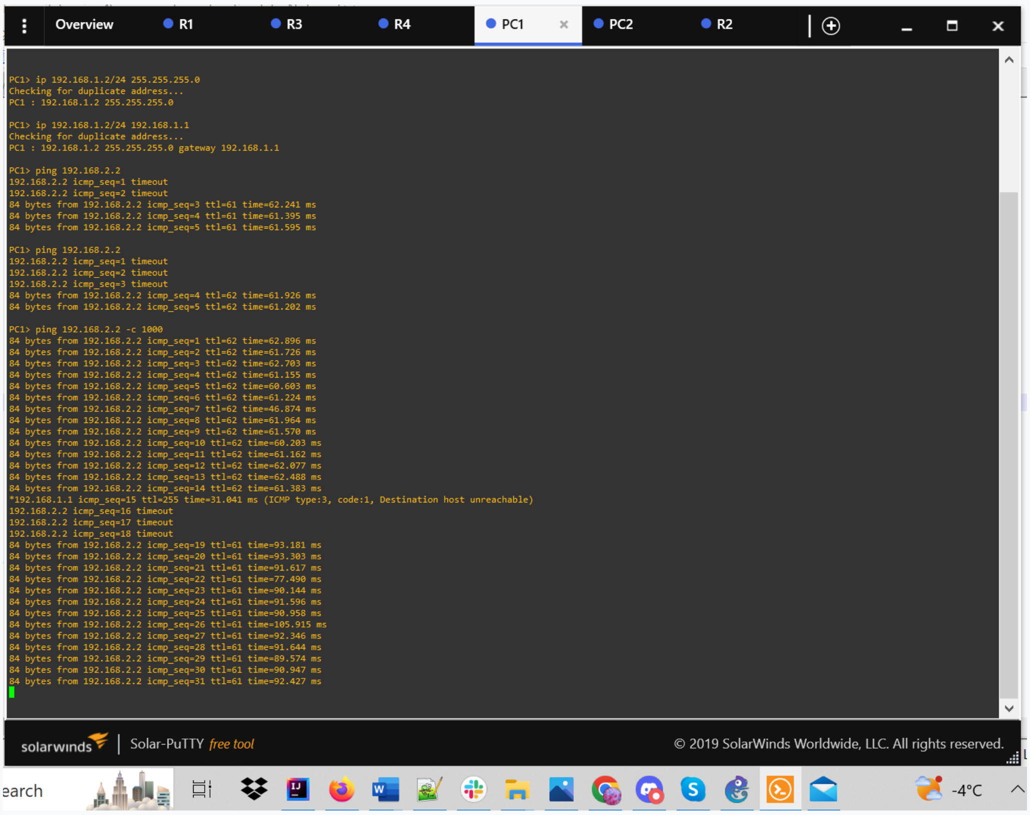


Figure 7. Interfaces have been shut down.

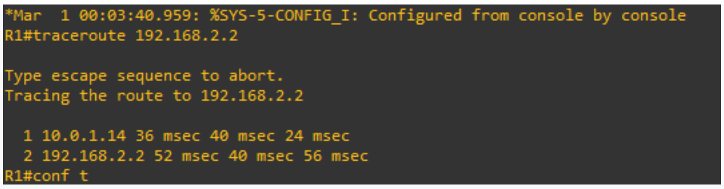


Figure 8. screenshot of the traceroute before shut down the route R1-R4.

After shut down the route R1-R4 the following route R1-R2-R4 have been taken to forward the remaining of the packets. It was mentioned above that the route R1-R4 has metric 1, the route R1-R2-R4 has metric 2, R1-R3-R4 with metric 3. The parameter metric gives the priority to choose the route. For this reason, the route R1-R2-R4 has been taken, as it has metric 2. In general, a higher metric value indicates a less preferred or more expensive route, while a lower metric value indicates a more preferred or less expensive route. Please look to the Figure 9.

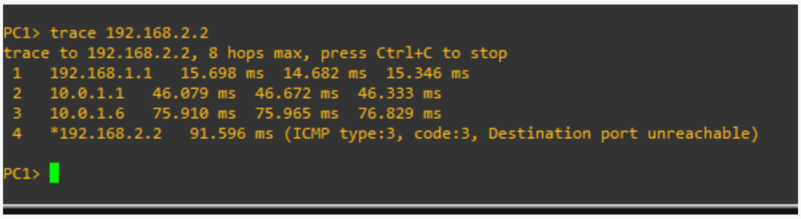


Figure 9. screenshot of the traceroute after shut down the route R1-R4.

Problem 3.

3.a Configuration RIPv2 of the routers and traceroute to see which routing path has been picked by RIPv2**.**

Figure 10. Traceroute and configuration RIPv2.

I have done configuration RIPv2 for the routers and used the a traceroute command to see which routing path has been picked by RIPv2. The route R1-R4 has been picked by RIPv2 as the best route. RIPv2 selects the optimal route based on the hop count, which represents the number of routers a packet must traverse to reach its destination. RIPv2 considers the route with the lowest hop count to be the most efficient. So the route R1-R4 has lowest hop count compering with the routes such as R1-R2-R4 and R1-R3-R4 for this reason the route R1-R4 has been picked up by RIPv2.

3.b Start a continuous ping between PC-1 and PC-2 and shut down one of the active router interfaces.

For this task it was start a continuous ping between PC-1 and PC-2. After it the active routers interfaces R1 and R4 have been shut down. So, 21 packets have been lost and after the new route have been found.

Figure 11. Screenshot of the lost packets and interfaces have been shut down.

```
84 bytes from 192.168.2.2 icmp_seq=40 ttl=61 time=63.133 ms
84 bytes from 192.168.2.2 icmp_seq=41 ttl=61 time=61.385 ms
84 bytes from 192.168.2.2 icmp_seq=42 ttl=61 time=62.364 ms
84 bytes from 192.168.2.2 icmp_seq=43 ttl=61 time=61.121 ms

PC1> trace 192.168.2.2
trace to 192.168.2.2, 8 hops max, press Ctrl+C to stop
 1   192.168.1.1   15.566 ms  15.229 ms  15.405 ms
 2   10.0.1.18   46.100 ms  46.432 ms  46.055 ms
 3   10.0.1.9   46.365 ms  47.102 ms  46.341 ms
 4   *192.168.2.2   60.739 ms (ICMP type:3, code:3, Destination port unreachable)

PC1>
```

Figure 12. Traceroute after shutdown R1-R4.

I have used the command to shut down interfaces of the active routers R1 and R4. After it, the new route has been found, R1-R3-R4. RIPv2 chose the path R1-R3-R4 because the metric (or cost) for this path was the lowest among all available paths to reach the destination network. Assuming that all routers have learned about the destination network via RIPv2, then each router will have calculated a metric for each available path to reach the destination network based on the sum of the costs of the individual links along the path. The path R1-R3-R4 has a lower metric (cost) of 3 (sum of the costs of links f2/0-s0/0-f1/0). Therefore, R1 chooses the path R1-R3-R4 to reach the destination network. R1-R2-R4 is another possible path to reach the destination network. However, in this case, R1-R2-R4 has a higher metric (cost) of 4 (sum of the costs of links f0/0-f0/1 and f1/0-f2/0-s0/0). So, the path R1-R3-R4 has a lower metric (cost) of 3 (sum of the costs of links f2/0-s0/0-f1/0). Therefore, R1 chooses the path with the lowest metric (cost), which is R1-R3-R4, to reach the destination network.

Problem 4.

4.a Open Shortest Path First (OSPF).

Open Shortest Path First (OSPF) is a type of routing protocol that utilizes a link-state algorithm to determine the most optimal path between a source and destination router.

Configuring OSPF routers involves specifying the correct number of networks with appropriate IP addresses, masks, and areas for each router. OSPF uses areas to improve network scalability, reduce routing traffic, and enable efficient use of network resources. In general, it is recommended to divide the network into multiple areas to prevent the flooding of OSPF updates and to make it easier to summarize routes.

When deciding how to divide the network into areas, it is important to consider the network topology, the size of the network, and the amount of traffic that will be generated. Generally, the backbone area (Area 0) should be used to interconnect multiple areas in a hierarchical fashion. This approach helps to prevent unnecessary routing updates and ensures that routes are propagated only to the appropriate areas.

The choice of metric used by OSPF to select the best path is based on the OSPF cost metric. The cost metric is calculated based on the bandwidth of the link, and is inversely proportional to the bandwidth. In other words, a higher bandwidth link will have a lower cost metric and be preferred over a lower bandwidth link.

Overall, when configuring OSPF routers, it is important to carefully consider the network topology and to use areas appropriately. This will help to ensure efficient use of network resources and provide optimal routing for network traffic (Cisco, 2022).

Figure 13. Ping from PC1 to PC2 (configuration for OSPF).

<u>**4.b** Testing scenarios.</u>

All configurations for OSPF have been done. It was done ping from PC1 to PC2(look the Figure 13). I have used a traceroute command from PC1 to PC2 to see which routing path has been picked by OSPF. It was picked the route R1-R2-R4 (Look to the Figure 14). This root R1-R2-R4 is more efficient than others as it has higher bandwidth then others. So, the root R1-R2-R4 has higher bandwidth. For this reason, OSPF algorithm picked this route as it identifies the most efficient route based on the highest available bandwidth, prioritizing the route with the best bandwidth performance.

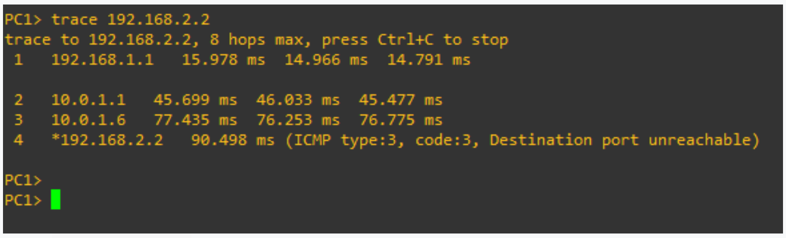


Figure 14. Traceroute PC1 to PC2 (configuring OSP)

After it, I have started a continuous ping between PC1 and PC2 and shut down active router interfaces, R1, R2, R4. Please look to the Figure 14. It was lost three packets. After it, the new route (R1-R4) has been found and it starts working in normal way (look to the Figure 15).

```
PC1    PC2    R1
84 bytes from 192.168.2.2 icmp_seq=1 ttl=61 time=92.078 ms
84 bytes from 192.168.2.2 icmp_seq=2 ttl=61 time=91.706 ms
84 bytes from 192.168.2.2 icmp_seq=3 ttl=61 time=93.040 ms
84 bytes from 192.168.2.2 icmp_seq=4 ttl=61 time=92.767 ms
84 bytes from 192.168.2.2 icmp_seq=5 ttl=61 time=91.665 ms

PC1> trace 192.168.2.2
trace to 192.168.2.2, 8 hops max, press Ctrl+C to stop
 1   192.168.1.1   15.507 ms  15.180 ms  15.006 ms
 2   10.0.1.1   46.086 ms  45.668 ms  45.984 ms
 3   10.0.1.6   76.159 ms  75.726 ms  76.666 ms
 4   *192.168.2.2   91.088 ms (ICMP type:3, code:3, Destination port unreachable)

PC1> ping 192.168.2.2 -c 1000
84 bytes from 192.168.2.2 icmp_seq=1 ttl=61 time=92.284 ms
84 bytes from 192.168.2.2 icmp_seq=2 ttl=61 time=91.492 ms
84 bytes from 192.168.2.2 icmp_seq=3 ttl=61 time=92.072 ms
84 bytes from 192.168.2.2 icmp_seq=4 ttl=61 time=90.657 ms
84 bytes from 192.168.2.2 icmp_seq=5 ttl=61 time=91.855 ms
84 bytes from 192.168.2.2 icmp_seq=6 ttl=61 time=91.507 ms
84 bytes from 192.168.2.2 icmp_seq=7 ttl=61 time=75.712 ms
84 bytes from 192.168.2.2 icmp_seq=8 ttl=61 time=92.334 ms
84 bytes from 192.168.2.2 icmp_seq=9 ttl=61 time=91.244 ms
84 bytes from 192.168.2.2 icmp_seq=10 ttl=61 time=92.019 ms
84 bytes from 192.168.2.2 icmp_seq=11 ttl=61 time=92.238 ms
84 bytes from 192.168.2.2 icmp_seq=12 ttl=61 time=91.766 ms
84 bytes from 192.168.2.2 icmp_seq=13 ttl=61 time=91.775 ms
84 bytes from 192.168.2.2 icmp_seq=14 ttl=61 time=90.702 ms
84 bytes from 192.168.2.2 icmp_seq=15 ttl=61 time=91.644 ms
84 bytes from 192.168.2.2 icmp_seq=16 ttl=61 time=90.981 ms
84 bytes from 192.168.2.2 icmp_seq=17 ttl=61 time=91.869 ms
84 bytes from 192.168.2.2 icmp_seq=18 ttl=61 time=91.255 ms
84 bytes from 192.168.2.2 icmp_seq=19 ttl=61 time=92.352 ms
84 bytes from 192.168.2.2 icmp_seq=20 ttl=61 time=91.289 ms
84 bytes from 192.168.2.2 icmp_seq=21 ttl=61 time=91.980 ms
84 bytes from 192.168.2.2 icmp_seq=22 ttl=61 time=91.483 ms
84 bytes from 192.168.2.2 icmp_seq=23 ttl=61 time=92.704 ms
84 bytes from 192.168.2.2 icmp_seq=24 ttl=61 time=92.188 ms
84 bytes from 192.168.2.2 icmp_seq=25 ttl=61 time=91.408 ms
84 bytes from 192.168.2.2 icmp_seq=26 ttl=61 time=75.572 ms
192.168.2.2 icmp_seq=27 timeout
192.168.2.2 icmp_seq=28 timeout
192.168.2.2 icmp_seq=29 timeout
84 bytes from 192.168.2.2 icmp_seq=30 ttl=61 time=60.339 ms
84 bytes from 192.168.2.2 icmp_seq=31 ttl=61 time=62.155 ms
84 bytes from 192.168.2.2 icmp_seq=32 ttl=61 time=61.371 ms
84 bytes from 192.168.2.2 icmp_seq=33 ttl=61 time=62.597 ms
84 bytes from 192.168.2.2 icmp_seq=34 ttl=61 time=62.074 ms
84 bytes from 192.168.2.2 icmp_seq=35 ttl=61 time=61.787 ms
84 bytes from 192.168.2.2 icmp_seq=36 ttl=61 time=61.721 ms
84 bytes from 192.168.2.2 icmp_seq=37 ttl=61 time=61.669 ms
84 bytes from 192.168.2.2 icmp_seq=38 ttl=61 time=60.683 ms
84 bytes from 192.168.2.2 icmp_seq=39 ttl=61 time=62.015 ms
84 bytes from 192.168.2.2 icmp_seq=40 ttl=61 time=61.837 ms
84 bytes from 192.168.2.2 icmp_seq=41 ttl=61 time=61.414 ms
84 bytes from 192.168.2.2 icmp_seq=42 ttl=61 time=61.629 ms
84 bytes from 192.168.2.2 icmp_seq=43 ttl=61 time=60.518 ms
```

Figure 15. Interfaces have been shut down (cconfiguring OSPF)

The new route R1-R4 has been picked by OSPF algorithm (look to the Figure 16) as it is the most efficient route: the bandwidth on the link between R1 and R4 is higher (10000 kbps) than the bandwidth on the link between R1, R3, and R4 (1544 kbps).

```
*Mar  1 00:45:25.131: %SYS-5-CONFIG_I: Configured from console by console
R1#
*Mar  1 00:49:32.231: %OSPF-5-ADJCHG: Process 1, Nbr 10.0.1.5 on FastEthernet0/1 from FULL to DOWN, Neighbor Down: Dead timer expired
R1#traceroute 192.168.2.2

Type escape sequence to abort.
Tracing the route to 192.168.2.2

  1 10.0.1.14 40 msec 32 msec 24 msec
  2 192.168.2.2 48 msec 40 msec 52 msec
R1#
```

Figure 16. Trace route <u>after</u> shut down active router interfaces (configuring OSPF)

Problem 5.

Static routing is the simplest and easiest to configure, but it is not scalable and requires manual configuration of all routes. This makes it inefficient for large and complex networks where frequent changes occur. In case of failure, static routes must be updated manually, leading to network downtime and packet loss (Par, 2023).

RIPv2 is easier to configure than OSPF, but it is not as efficient for large networks because it consumes more bandwidth due to frequent updates. It is better suited for smaller networks that do not require a high level of reliability. In case of failure, RIPv2 can take a longer time to converge, leading to packet loss and downtime (Lazaros, 2023).

OSPF is more complex to configure than RIPv2 and static routing, but it is highly scalable and efficient for larger networks. It consumes less bandwidth because it sends updates only when changes occur and converges faster than RIPv2, reducing downtime and packet loss. In case of failure, OSPF can quickly reroute traffic to an alternate path, ensuring high availability and reducing packet loss. For example, I have done all configuration for OSPF and after it shut down router interfaces, it showed that it was lost 3 packets comparing RIPv2 (Lazaros, 2023).

In conclusion, each of these routing methods has its own advantages and disadvantages, and the best choice depends on the network size, complexity, reliability requirements, and resources available. Static routing is suitable for simple networks with a few routers, while RIPv2 is better for small networks that do not require high reliability or for medium-sized networks with frequent topology changes. OSPF is ideal for large and complex networks that require high reliability and availability.

References:

1. Par D. S. (2023) “Routing operation: Static routes 14 January 2023”. FORMIP. Available at: https://formip.com/en/routing-operation-static-routes (accessed 23 March 2023) .

2. Lazaros A. (2023) “Comparison of OSPF vs RIP/RIPv2 Routing Protocols in IP Networks”. NetworksTraining. Available at: https://www.networkstraining.com/ospf-vs-rip-ripv2/ (accessed 23 March 2023).

3. Cisco. (2022) “Understand Open Shortest Path First (OSPF) - Design Guide”. Available at: https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html (accessed 23 March 2023).