Linnéuniversitetet
Kalmar Växjö

Report

Assignment 4: Network Topology And Routing

Author: Yuyao Duan
Supervisor: Ola Flygt,
Hemant Ghayvat
Semester: Spring 2022
Discipline: Computer Network
Course code: 1DV701

Table of Contents

1 Problem 1

a) Completed topology screenshot:

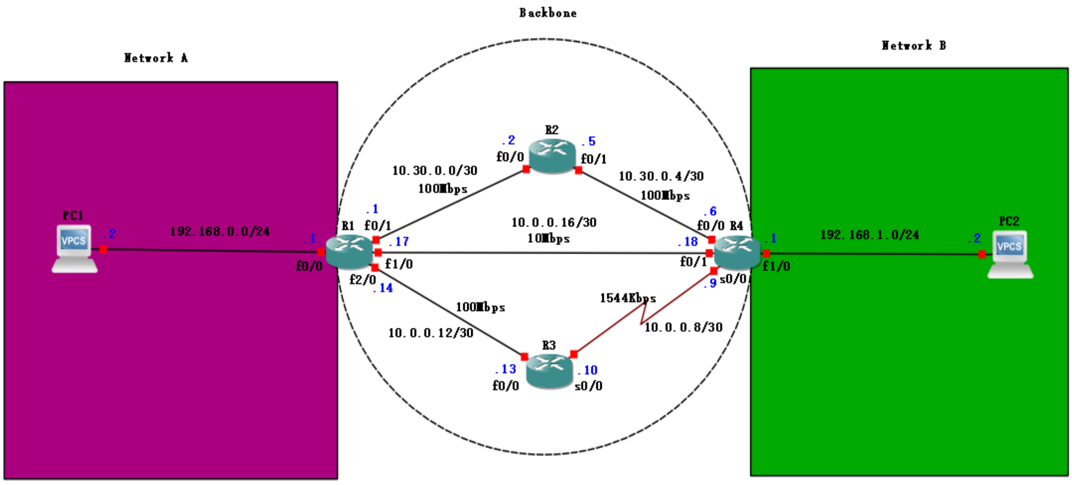

Figure 1. Screenshot from GNS3 with a completed topology

b) Screenshots of pings:

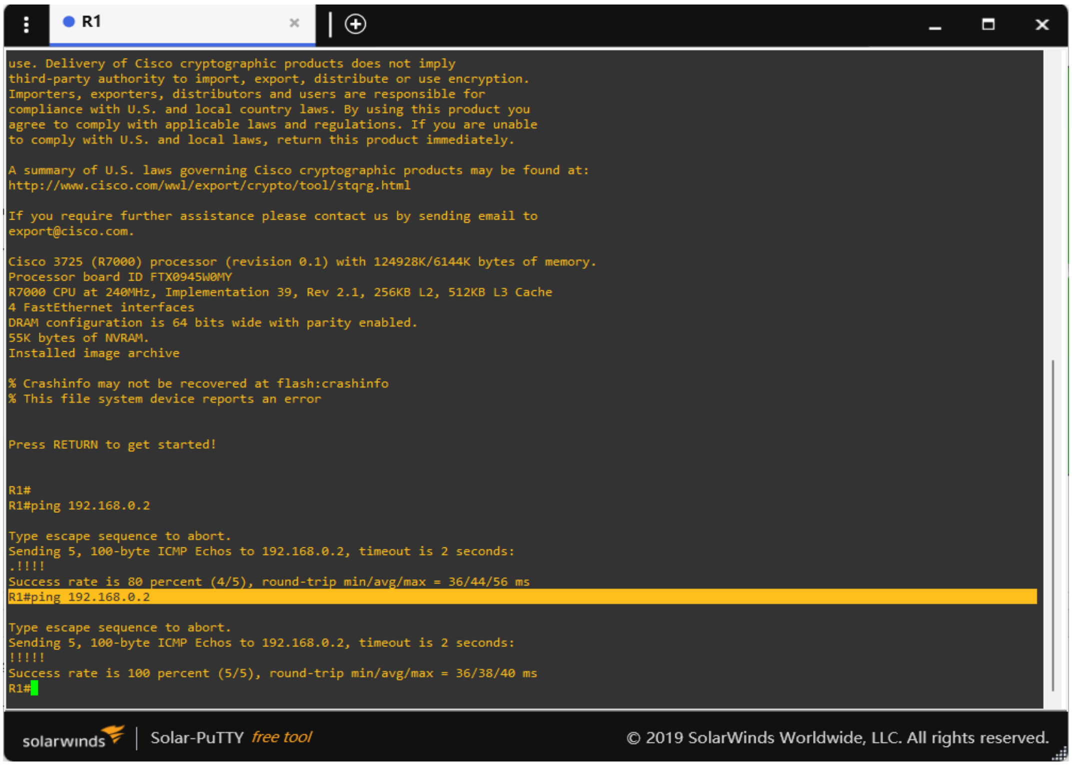

Figure 2. Ping from R1 to PC1

Figure 3. Ping from R1 to R4

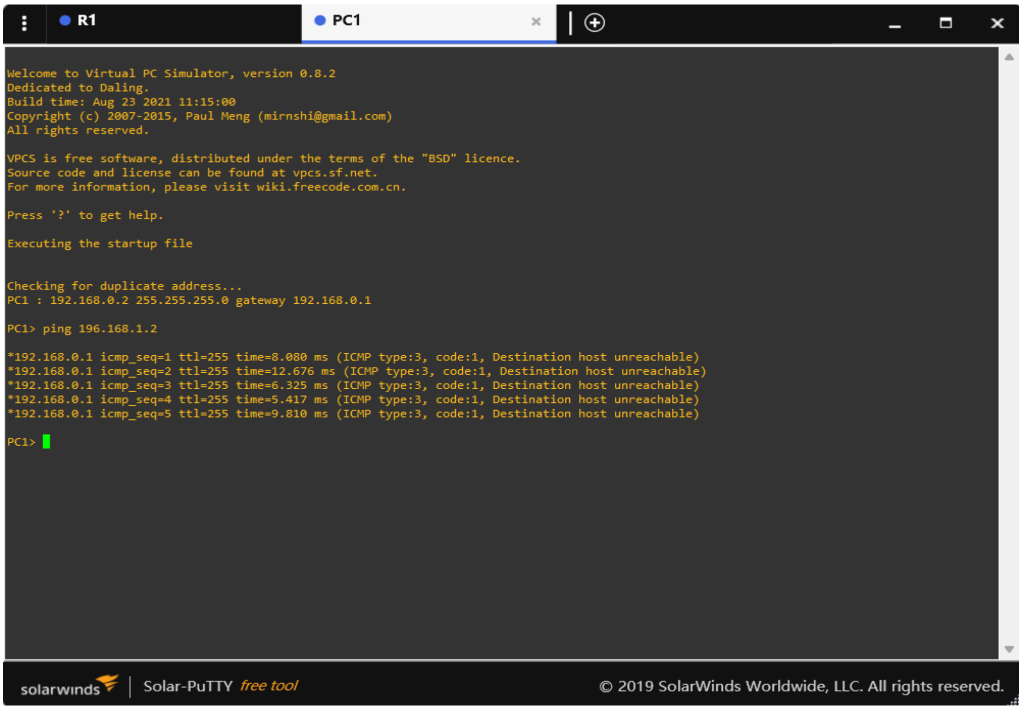

Figure 4. Ping from PC1 to PC2

c) ***An explanation of NM-1FE-TX and WIC-1T abbreviations and why these modules are chosen among the available alternatives. Make sure to describe the properties of each type of interface.***

NM-1FE-TX： 10/100 Mbps Fast Ethernet Network Module, 100 Base-TX. The feature of NM-1FE-TX include following: RJ-45 100 Base-TX interface (no MII port) 10 or 100 Mbps speed, auto sensing; Full or half duplex, auto-negotiating (at 10 Mbps and 100 Mbps); ISL is supported in hardware, requires "Plus" Feature set.

WIC-1T: One port serial (DB60, Cisco 60-pin "5-in-1" connector). Supports Max sync speed 2 Mbps. Does not support hot swap.

The reason that these two modules are chosen is due to the structure of this network demanding three types of bandwidths: 100Mbps, 10Mbps, and 1544Kbps. By using NM-1FE-TX, it can auto sense and auto-negotiate between 100Mbps and 10Mbps which are needed for up and middle lines; By using WIC-1T, it can realize the serial connection with max speed 2 Mbps which is very suitable for the connection between R3 and R4.

d) Answer to the following question: what is the practical difference between a /24 and a /30 subnet?

A /24 subnet indicates using mask 255.255.255.0 which contains 256 addresses and 254 available hosts. By comparison, a /30 subnet indicates using mask 255.255.255.252 which contains 4 addresses and 2 available hosts.

The practical reason for using different subnets is due to the fact of the network's situation. For Network A and B, there are normally more devices demanding for IP address, therefore /24 subnet is more suitable. For Backbone, /30 subnet is more suitable since the communication between routers do not demand more than 2 host addresses, more than /30 subnetting can be considered as wasting addresses.

2 Problem 2

a) Explain each of the parameters of the ip route command:

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

[ip]: Specifies the IP route prefix for the destination.
[mask]: Specifies the prefix mask for the destination.
[router_interface]: Specifies the interface of another hop or the next interface's ip address.
[metric]: Specifies the metric of the route. The default metric is 6. Valid range is from 1–255.

b) Ping between VPCS:

Figure 5. Ping from PC1 to PC2

Figure 6. Trace route

For this question, the middle route R1 to R4 is selected for creating the static routing, the reason for this selection is that there are less routers (2 routers compared to other two routes with 3 routers) on this route from PC1 to PC2 which is more efficient since there may exist less possibility of device failure.

c) Shutdown interfaces:

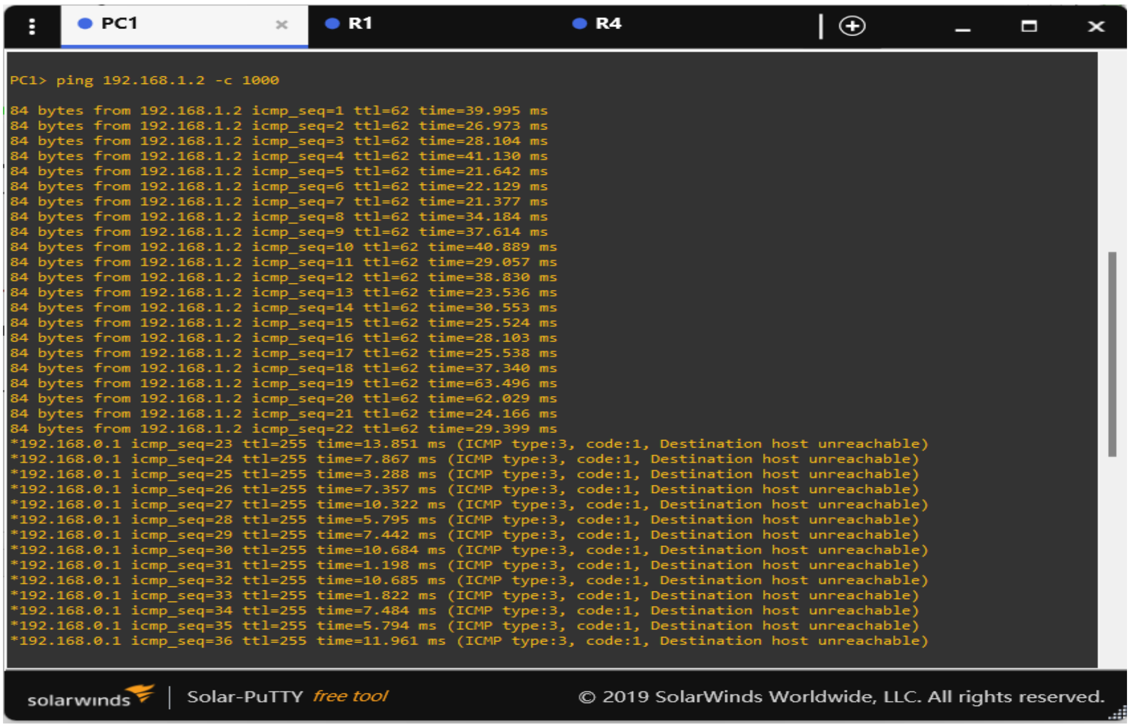

Figure 8. Observation ping failure after shutdown the interfaces

During this observation, both of the active router interfaces on both sides of R1 and R4 were shut down after pinging PC2 starting. As we can see, once the interfaces were closed, the pings turned to be above unreachable.

d) configure the remaining two possible routing paths between PC-1 and PC-2:

For this task, all three routes had been configured. The up route “R1→R2→R4” was configured with metric 1; the middle route “R1→R4” was configured with metric 2; the down route “R1→R3→R4” was configured with metric 3.

Figure 9. Observation packets lost after shutdown the interfaces

During this observation, the first used route is “R1→R2→R4”, the command for shutdown both interfaces of R1 and R4 were prepared in advance in the terminal (only waiting for press Enter). After entering “shut” for R1, the unreachable error appeared; then after entering “shut” for R4, the timeout error occurred. Then immediately the new route was picked, and it turns to normal.

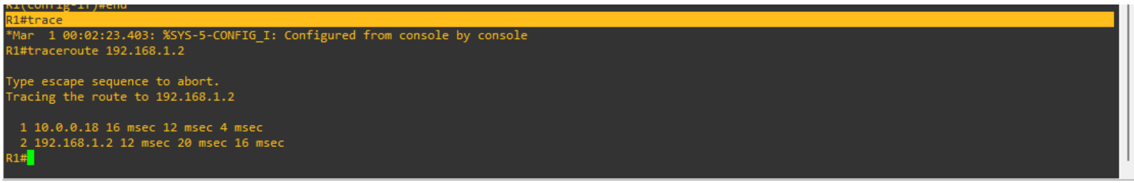

Figure 10. Traceroute after shutdown “R1→R2→R4”

From the above traceroute, we can find that after shutdown the route “R1→R2→R4”, the middle route “R1→R4” was immediately picked for forwarding the rest packets. The reason for this is due to the “metric” parameter used. The metric for “R1→R2→R4” is “1”; “R1→R4” is “2”; “R1→R3→R4” is “3”, which the metric can be considered as a “priority level”. The lower the number is, the higher the priority it has. This explains why after shutdown “R1→R2→R4”, the middle route “R1→R4” was selected.

3 Problem 3

a) Configure RIPv2 for the routers and traceroute:

Figure 11. Traceroute PC1 to PC2 after configuring RIPv2

As we can see, after finishing the configuration for RIPv2, the middle route "R1→R4" was picked as the most efficient one. This is due to the fact that RIPv2's algorithm considering the optimal route by hop count i.e. the route with the lowest hop count will be considered as the most efficient route [1]. This explains why the middle route "R1→R4" was selected instead of using "R1→R3→R4" or "R1→R2→R4".

b) Shutdown the active route and identify which route will be picked:

```
Executing the startup file


Checking for duplicate address...
PC1 : 192.168.0.2 255.255.255.0 gateway 192.168.0.1

PC1> ping 192.168.1.2

192.168.1.2 icmp_seq=1 timeout
192.168.1.2 icmp_seq=2 timeout
84 bytes from 192.168.1.2 icmp_seq=3 ttl=62 time=38.481 ms
84 bytes from 192.168.1.2 icmp_seq=4 ttl=62 time=35.272 ms
84 bytes from 192.168.1.2 icmp_seq=5 ttl=62 time=29.153 ms

PC1> ping 192.168.1.2 -c 100

84 bytes from 192.168.1.2 icmp_seq=1 ttl=62 time=39.005 ms
84 bytes from 192.168.1.2 icmp_seq=2 ttl=62 time=28.499 ms
84 bytes from 192.168.1.2 icmp_seq=3 ttl=62 time=37.078 ms
84 bytes from 192.168.1.2 icmp_seq=4 ttl=62 time=34.217 ms
84 bytes from 192.168.1.2 icmp_seq=5 ttl=62 time=37.922 ms
84 bytes from 192.168.1.2 icmp_seq=6 ttl=62 time=40.153 ms
84 bytes from 192.168.1.2 icmp_seq=7 ttl=62 time=41.234 ms
84 bytes from 192.168.1.2 icmp_seq=8 ttl=62 time=39.882 ms
84 bytes from 192.168.1.2 icmp_seq=9 ttl=62 time=36.748 ms
*192.168.0.1 icmp_seq=10 ttl=255 time=11.109 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.0.1 icmp_seq=11 ttl=255 time=13.651 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.0.1 icmp_seq=12 ttl=255 time=10.413 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.0.1 icmp_seq=13 ttl=255 time=7.548 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.0.1 icmp_seq=14 ttl=255 time=7.673 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.0.1 icmp_seq=15 ttl=255 time=11.707 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.0.1 icmp_seq=16 ttl=255 time=3.797 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.0.1 icmp_seq=17 ttl=255 time=1.973 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.0.1 icmp_seq=18 ttl=255 time=3.979 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.0.1 icmp_seq=19 ttl=255 time=5.464 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.0.1 icmp_seq=20 ttl=255 time=2.734 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.0.1 icmp_seq=21 ttl=255 time=7.277 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.0.1 icmp_seq=22 ttl=255 time=10.868 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.0.1 icmp_seq=23 ttl=255 time=10.142 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.0.1 icmp_seq=24 ttl=255 time=9.702 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.0.1 icmp_seq=25 ttl=255 time=8.665 ms (ICMP type:3, code:1, Destination host unreachable)
84 bytes from 192.168.1.2 icmp_seq=26 ttl=61 time=33.689 ms
84 bytes from 192.168.1.2 icmp_seq=27 ttl=61 time=36.324 ms
84 bytes from 192.168.1.2 icmp_seq=28 ttl=61 time=43.891 ms
84 bytes from 192.168.1.2 icmp_seq=29 ttl=61 time=48.065 ms
84 bytes from 192.168.1.2 icmp_seq=30 ttl=61 time=48.446 ms
84 bytes from 192.168.1.2 icmp_seq=31 ttl=61 time=49.505 ms
84 bytes from 192.168.1.2 icmp_seq=32 ttl=61 time=47.720 ms
```

Figure 12. Observation packets lost after shutdown the interfaces (RIPv2)

Again, during this observation, the command for shutdown the interfaces were prepared in advance in the R1's and R4's terminal to keep this observation as accurate as possible. As we can see, there were 16 packets lost before a new route was selected.

```
PC1> trace 192.168.1.2
trace to 192.168.1.2, 8 hops max, press Ctrl+C to stop
 1   192.168.0.1   9.187 ms  10.118 ms  9.276 ms
 2   10.30.0.2   19.472 ms  20.616 ms  20.668 ms
 3   10.30.0.6   30.153 ms  29.628 ms  29.887 ms
 4   *192.168.1.2   50.110 ms (ICMP type:3, code:3, Destination port unreachable)

PC1>
```

Figure 13. Traceroute after shutdown "R1→R4"

As we can see, after shutdown the first efficient route, the up route "R1→R2→R4" was selected. The reason for this route was selected instead of using bottom route "R1→R3→R4" (even both have same hop count) due to the fact that "R1→R2→R4" has higher bandwidth with 100Mbps along the way. By comparison, the route "R1→R3→R4" has very low bandwidth between R3 and R4 with only 1544 Kbps. Therefore, "R1→R2→R4" was selected as the second option after the first route failed.

4 Problem 4

a) Implementing OSPF dynamic routing protocol:

According to the OSPF algorithm, it uses areas to simplify administration and optimize traffic and resource utilization [2]. Without using areas, it can be very challenging to manage routers. An area indicates a logical grouping of contiguous network and routers, and all routers in the same area having same topology table (and don't know the routers in other areas) [2]. The main advantage to use areas in an OSPF network including: reducing the router tables on the routers (memory burden); less time demand for SFP algorithm since routers need to recalculate their link state database only when there is typology change within their own area; routing updates are reduced [2]. In OSPF, if there are multiple routes to a network with the same route type, the metric will be calculated as cost based on the bandwidth is used for selecting the best route i.e. the route with the lowest value for cost is chosen as the best route [3].

In OSPF network, each area must be connected to the backbone area (also known as area 0) [2]. All routers inside an area must have the same area ID in orer to become OSPF neighbours [2]. This provide the answer for dividing the areas. Based on this understanding, backbone area in this assignment should be assigned with area 0. Also, assigning backbone area with "area 0" can enable the network to switch route in case one route with connection failure.

Figure 14. PC1 ping PC2 after configuring all networks

b) Repeat all testing scenarios from Problem 3

Figure 15. Traceroute PC1 to PC2 after configuring OSPF

From the above observation we can find that OSPF selected tthe up route “R1→R2→R4” as the most efficient one. This is due to the fact that OSPF’s algorithem considering the optimal route by highest bandwidth i.e. the route with the best bandwidth performance will be considered as the most efficient route.

Therefore, in the following observation, interfaces of the route “R1→R2→R4” will be shutdown. Again the shutdown commands will be prepared in advance in the terminals of R1 and R1 and just waiting for press Enter button.

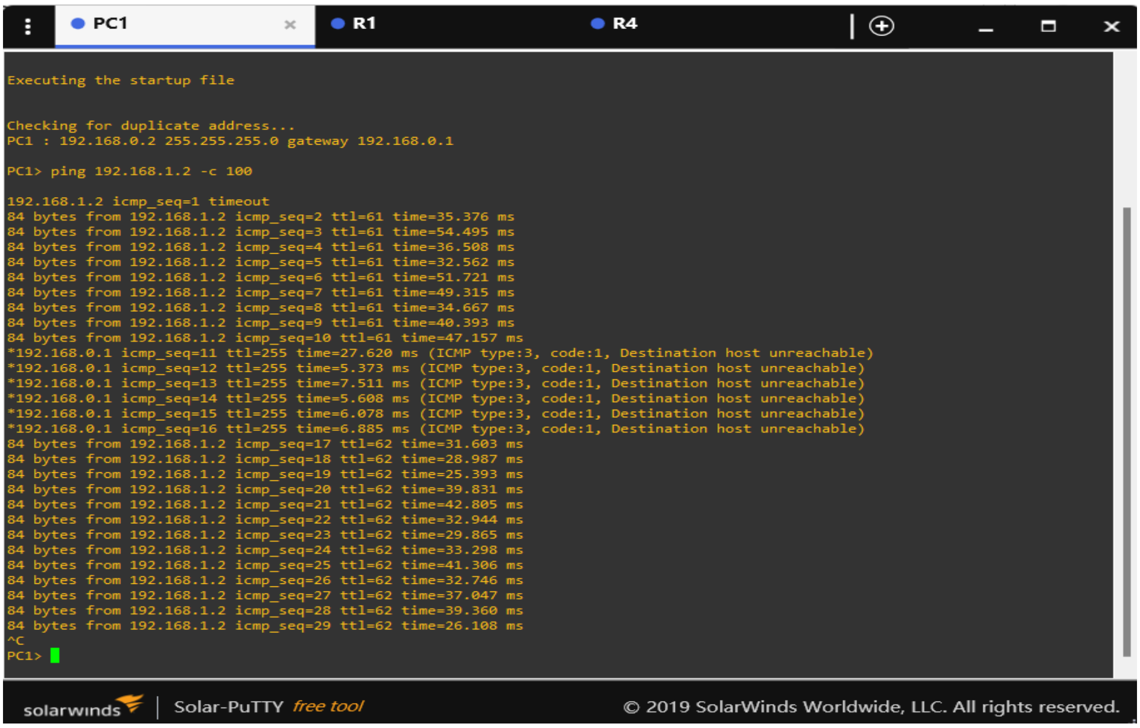

Figure 16. Observation packets lost after shutdown the interfaces (OSPF)

As we can see that there were 6 packets lost before switching to a new route. The following figure shows that the new route is the middle route “R1→R4”.

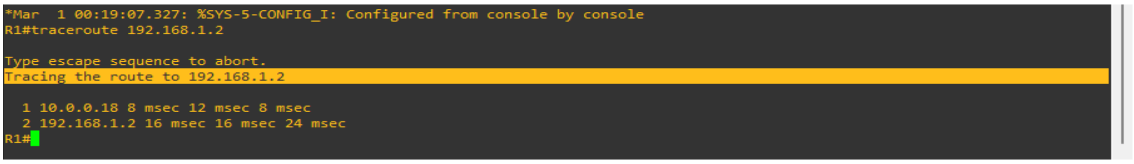

Figure 17. Traceroute PC1 to PC2 after shutdown “R1→R2→R4”

From the above observation, after shutdown the first efficient route, the middle route “R1→R4” was selected. The reason for this route was selected instead of using bottom route “R1→R3→R4” due to the fact that “R1→R4” has higher bandwidth with

10Mbps along the way. By comparison, the route "R1→R3→R4" has very low bandwidth between R3 and R4 with only 1544 Kbps. So in general, "R1→R4" has better bandwidth than the route "R1→R3→R4".

5 Problem 5

In this section, the three routing method: static routing, RIPv2 routing, and OSPF routing method will be discussed and summarized. The aim of this part is to have a deep understanding of the three routing methods in terms of configuration complexity, configuration time, efficiency and number of packets lost in case of failure.

Static Routing Method: Implementing Static Routing demands manual configuration which indicates that this method with very low feasibility for large networks due to the time- and labour-consuming [4]. This method is more suitable for small networks and the advantage of static routing is that it does not need complicated routing algorithm and normally contributing better security performance [4]. In case of connection failure, static routing with the best performance regarding packet lost among RIPv2 and OSPF which has smallest number of packet lost (2 lost) compared to RIPv2 (16 lost) and OSPF (6 lost).

RIPv2 Routing Method: Compared to Static Routing Method, the configuration process of RIPv2 is much easier and requires less effort. RIPv2 utilizes Distance-Vector Routing Protocol which indicates that it selects priority route based on the distance metric. During the observation of Problem 3, the most efficient route from RIPv2 is the middle route which has 2 hops compared to other two alternatives with 3. However, the limitation of this method is that the maximum hop counts is 15 [5], which means RIPv2 cannot be applied in case of a large network with many routers in between. An obvious disadvantage of RIPv2 is that it has most lost packets compared to static routing and OSPF when encountering connection failure.

OSPF Routing Method: The configuration for OSPF is also much easier compared to Static Routing. This method implements the link-state routing algorithm [6]. It uses the link state information that is available in the routers, which will help to analyze different sources like the speed, cost and path congestion while identifying the shortest path [6]. The topology will determine the routing table for routing decisions [6]. The merit of OSPF is that it can handle the error detection by itself and it applies multicast addressing for routing in a broadcast domain [6]. The metric of OSPF is bandwidth of the network and there is no hop count limitation for this method [6]. Compared to RIPv2, OSPF has much less lost packets in the case of connection failure.

OSPF is a good compromise in terms of configuration complexity, efficiency, number of packet loss compared to Static and RIPv2 Routing methods.

Reference

[1] TechRepublic, "Cisco administration 101: Know the basics about RIPv2", [2022-03-19], url: [https://www.techrepublic.com/article/cisco-administration-101-know-the-basics-about-ripv2/]

[2] Geek-University, "*OSPF areas explained*", [2022-03-19], url: [https://geek-university.com/ospf-areas-explained/]

[3] Networkworld, "*How does OSPF select the best route on Cisco routers and does load balancing work across multiple paths?*", [2022-03-19], url: [https://www.networkworld.com/article/2344467/how-does-ospf-select-the-best-route-on-cisco-routers-and-does-load-balancing-work-acros.html]

[4] Geeksforgeeks, "*Difference between Static and Dynamic Routing*", [2022-03-19], url: [https://www.geeksforgeeks.org/difference-between-static-and-dynamic-routing/]

[5] Geeksforgeeks, "*Differences between RIPv1 and RIPv2*", [2022-03-19], url: [https://www.geeksforgeeks.org/differences-between-ripv1-and-ripv2/]

[6] Geeksforgeeks, "*Difference between RIP and OSPF*", [2022-03-19], url: [https://www.geeksforgeeks.org/difference-between-rip-and-ospf/]