ECOLE
POLYTECHNIQUE
DE BRUXELLES

IRELE - MA1 Electrical Engineering

ELEC-H417

Report Lab 1
Dynamic Routing

Authors :

Amaury ARICO

Alexis BOLLENGIER

Emmeran COLOT

Sefa GÖNEN

Professor :

Jean-Michel DRICOT

Assistant :

Navid LADNER

Academic year :

2024 - 2025

Contents

1 Mission 0 - Initial Topology Setup

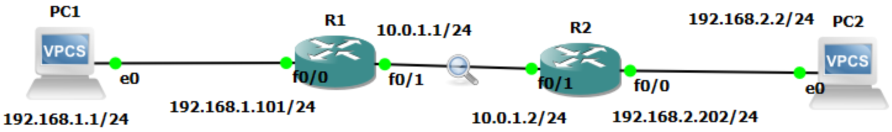


Figure 1.1: Initial topology

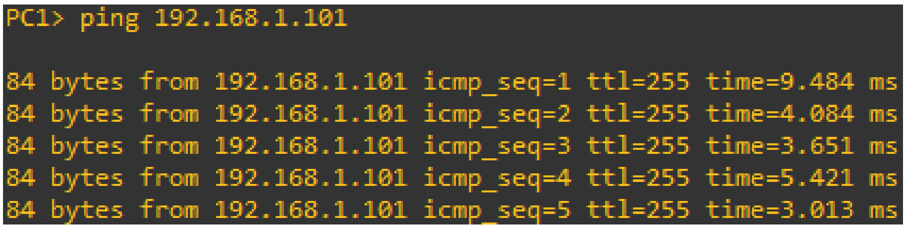
1.1 Question - Why does inter-router communication fail initially ?

Why does inter-router communication fail initially ?

At this stage of the lab, you should be able to ping device at a distance of 1 (i.e. directly connected) but not further devices (distance ≥ 2). Why ? In addition, please provide a proof (if any) to underline your answer (e.g. screenshot).

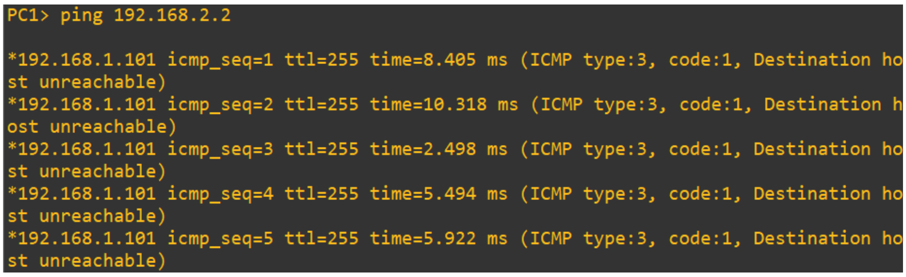
We can't ping devices at a distance ≥ 2 because the routers don't know how to reach these devices (addresses not in the routing table).

Here are some screenshots proving it :



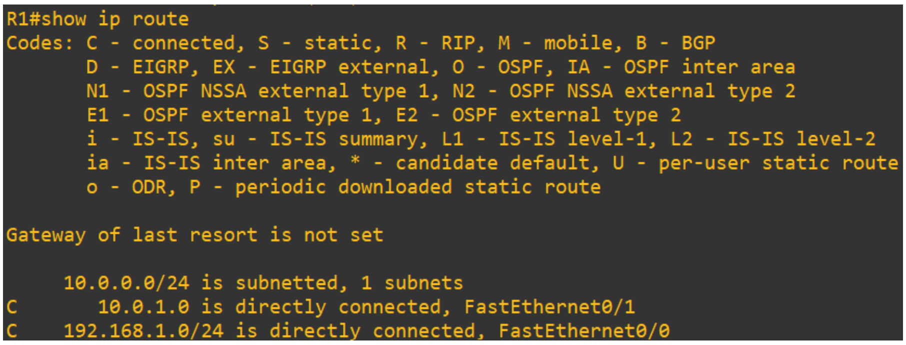
```
PC1> ping 192.168.1.101

84 bytes from 192.168.1.101 icmp_seq=1 ttl=255 time=9.484 ms
84 bytes from 192.168.1.101 icmp_seq=2 ttl=255 time=4.084 ms
84 bytes from 192.168.1.101 icmp_seq=3 ttl=255 time=3.651 ms
84 bytes from 192.168.1.101 icmp_seq=4 ttl=255 time=5.421 ms
84 bytes from 192.168.1.101 icmp_seq=5 ttl=255 time=3.013 ms
```

Figure 1.2: Ping from PC1 (192.168.1.1) to R1 (192.168.1.101)



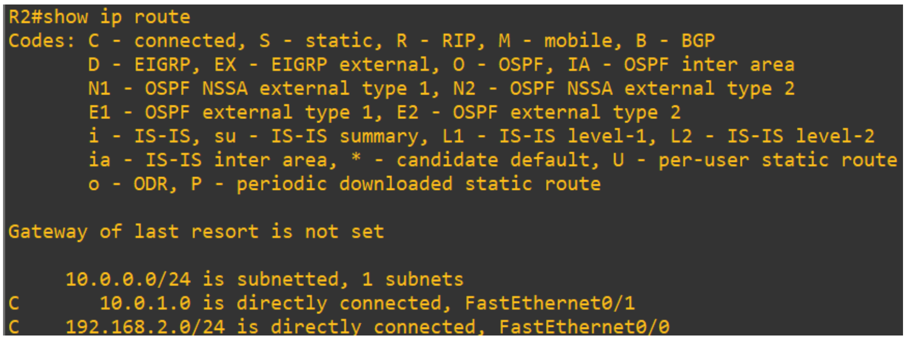
```
PC1> ping 192.168.2.2

*192.168.1.101 icmp_seq=1 ttl=255 time=8.405 ms (ICMP type:3, code:1, Destination ho
st unreachable)
*192.168.1.101 icmp_seq=2 ttl=255 time=10.318 ms (ICMP type:3, code:1, Destination h
ost unreachable)
*192.168.1.101 icmp_seq=3 ttl=255 time=2.498 ms (ICMP type:3, code:1, Destination ho
st unreachable)
*192.168.1.101 icmp_seq=4 ttl=255 time=5.494 ms (ICMP type:3, code:1, Destination ho
st unreachable)
*192.168.1.101 icmp_seq=5 ttl=255 time=5.922 ms (ICMP type:3, code:1, Destination ho
st unreachable)
```

Figure 1.3: Ping from PC1 (192.168.1.1) to PC2 (192.168.2.2)



```
R1#show ip route
Codes: C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.0.1.0 is directly connected, FastEthernet0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
```

Figure 1.4: Routing table of R1



```
R2#show ip route
Codes: C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.0.1.0 is directly connected, FastEthernet0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

Figure 1.5: Routing table of R2

2

Mission 1 - Configuring RIPv2

2.1 Question - RIP the Limits : Can PC1 finally reach PC2 ?

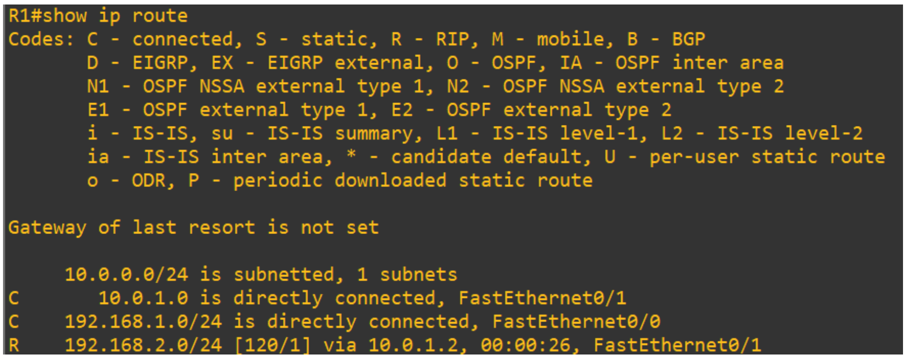
RIP the Limits : Can PC1 finally reach PC2 ?

After activating the RIP protocol on the first router only, can you ping from PC1 to PC2 and vice-versa ?

Why ? What should you do to solve this problem (*and do it*)?

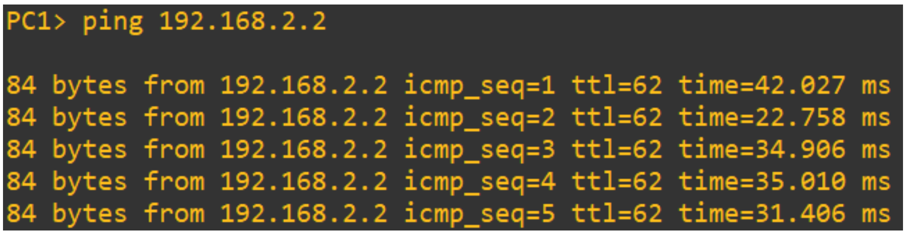
No we can't ping from **PC1 to PC2**/PC2 to PC1 because the router **R1**/R2 doesn't know how to access **PC2**/PC1 (no routing information).

To solve this, we just need to configure the RIP protocol for R2. After configuring it, we can ping and the routing tables are updated :



```
R1#show ip route
Codes: C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.0.1.0 is directly connected, FastEthernet0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
R    192.168.2.0/24 [120/1] via 10.0.1.2, 00:00:26, FastEthernet0/1
```

Figure 2.1: Routing table of R1 after configuring RIPv2



```
PC1> ping 192.168.2.2

84 bytes from 192.168.2.2 icmp_seq=1 ttl=62 time=42.027 ms
84 bytes from 192.168.2.2 icmp_seq=2 ttl=62 time=22.758 ms
84 bytes from 192.168.2.2 icmp_seq=3 ttl=62 time=34.906 ms
84 bytes from 192.168.2.2 icmp_seq=4 ttl=62 time=35.010 ms
84 bytes from 192.168.2.2 icmp_seq=5 ttl=62 time=31.406 ms
```

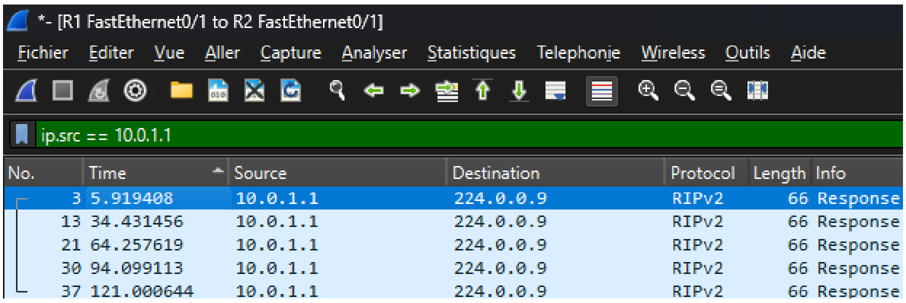
Figure 2.2: Ping from PC1 to PC2

2.2 Question - Wireshark : What's Hiding in the RIP Packets?

Wireshark : What's Hiding in the RIP Packets?

At what frequency RIP packets are send ? Is it send only once, periodic (and if so, at which frequency), sporadic (i.e. randomly) ? What interesting information do you find in those packets (Put a Wireshark screenshot in your report and highlight these information on it) ?

The RIP packets are sent periodically, approximately every 30 seconds (see figure 2.3).


*- [R1 FastEthernet0/1 to R2 FastEthernet0/1]
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

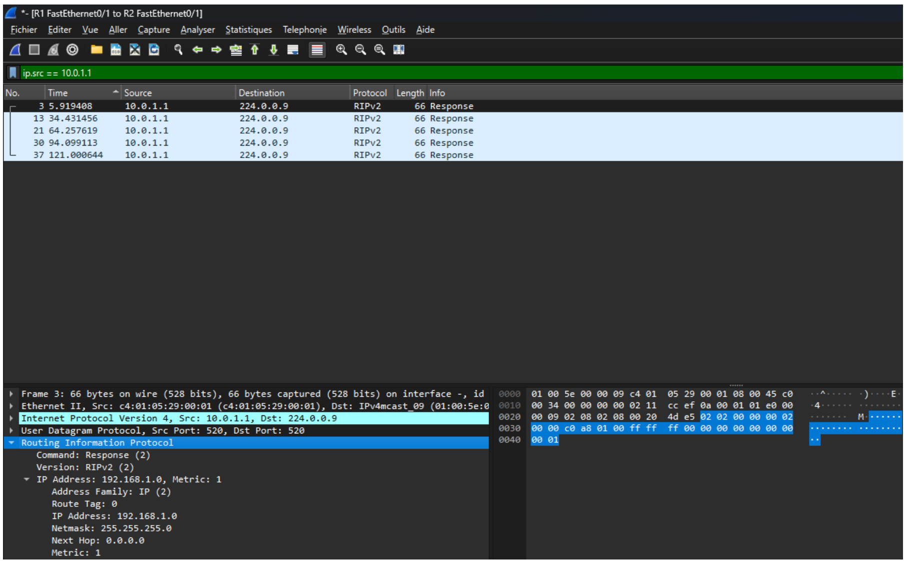
ip.src == 10.0.1.1

```
No.  Time          Source     Destination  Protocol  Length Info
   3 5.919408      10.0.1.1   224.0.0.9    RIPv2         66 Response
  13 34.431456     10.0.1.1   224.0.0.9    RIPv2         66 Response
  21 64.257619     10.0.1.1   224.0.0.9    RIPv2         66 Response
  30 94.099113     10.0.1.1   224.0.0.9    RIPv2         66 Response
  37 121.000644    10.0.1.1   224.0.0.9    RIPv2         66 Response
```

Figure 2.3: Wireshark screenshot. Listening to packets between R1 and R2 (subnet 10.0.1.0/24). Filtered to show packets sent by R1

The figure 2.4 shows the content of the RIP packet. We can find in it [1] :

- **IP address** : IP address of the network that the router serves (in this case R1 serves 192.168.1.0)
- **Netmask** : The subnet mask of that network (in this case /24)
- **Next hop** : The IP address of the next router along the path to destination (0.0.0.0 means that the network 192.168.1.0/24 is directly connected to R1)
- **Metric** : The number of hops to the destination (1 in this case)


*- [R1 FastEthernet0/1 to R2 FastEthernet0/1]
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

ip.src == 10.0.1.1

```
No.  Time          Source     Destination  Protocol  Length Info
   3 5.919408      10.0.1.1   224.0.0.9    RIPv2         66 Response
  13 34.431456     10.0.1.1   224.0.0.9    RIPv2         66 Response
  21 64.257619     10.0.1.1   224.0.0.9    RIPv2         66 Response
  30 94.099113     10.0.1.1   224.0.0.9    RIPv2         66 Response
  37 121.000644    10.0.1.1   224.0.0.9    RIPv2         66 Response
```

```
> Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface -, id
> Ethernet II, Src: c4:01:05:29:00:01 (c4:01:05:29:00:01), Dst: IPv4mcast_09 (01:00:5e:0
> Internet Protocol Version 4, Src: 10.0.1.1, Dst: 224.0.0.9
> User Datagram Protocol, Src Port: 520, Dst Port: 520
v Routing Information Protocol
    Command: Response (2)
    Version: RIPv2 (2)
  v IP Address: 192.168.1.0, Metric: 1
      Address Family: IP (2)
      Route Tag: 0
      IP Address: 192.168.1.0
      Netmask: 255.255.255.0
      Next Hop: 0.0.0.0
      Metric: 1
```

```
0000  01 00 5e 00 00 09 c4 01  05 29 00 01 08 00 45 c0   ··^····· ·)····E·
0010  00 34 00 00 00 00 02 11  cc ef 0a 00 01 01 e0 00   ·4······ ········
0020  00 09 02 08 02 08 00 20  4d e5 02 02 00 00 00 02   ·······  M·······
0030  00 00 c0 a8 01 00 ff ff  ff 00 00 00 00 00 00 00   ········ ········
0040  00 01                                              ··
```

Figure 2.4: Wireshark screenshot. Listening to packets between R1 and R2. The content of one RIP packet sent by R1 is shown in the bottom left

[1] Information on the fields found from this website : `infocenter.nokia.com/public/7750SR222R1A/index.jsp?topic=/com.nokia.Unicast_Guide/rip_packet_form-ai9exj5yo9.html`

2.3 Bonus question - One-way communication

One-way communication

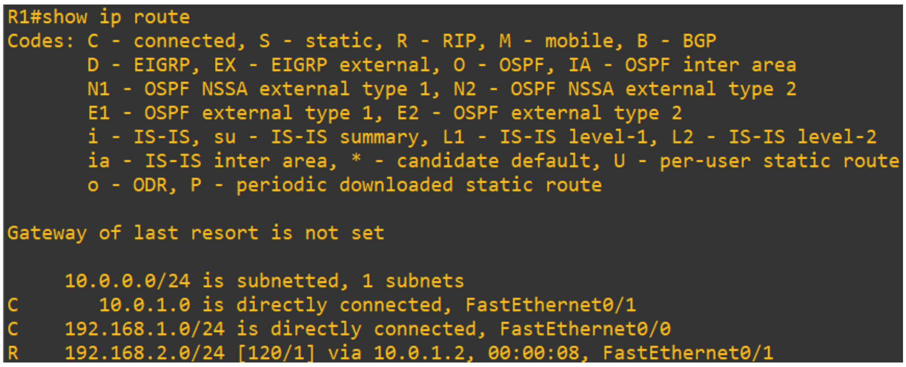
What can you do to make a one way communication (i.e. ping PC1→PC2 works but not PC2→PC1) ?

If we want to do PC1 → PC2, we need to remove the subnet of PC1 (192.168.1.0) from the RIP database of R1. So the result is that my router R1 doesn't share the fact that it serves the network 192.168.1.0 but it receives the information from R2 that a network 192.168.2.0 exists.

Command to do that :

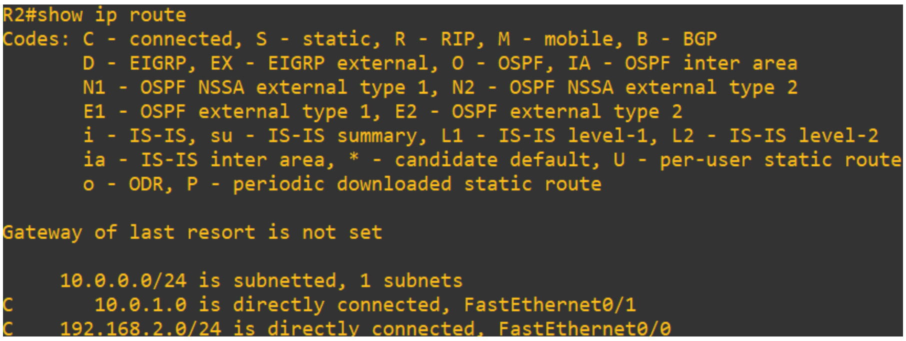
```
R1#conf t
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#no network 192.168.1.0
R1(config-router)#end
R1#write
```

Results :



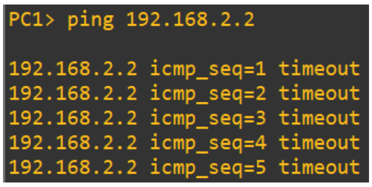
```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.0.1.0 is directly connected, FastEthernet0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
R    192.168.2.0/24 [120/1] via 10.0.1.2, 00:00:08, FastEthernet0/1
```

Figure 2.5: Routing table of R1 after removing the network 192.168.1.0 from the RIP database of R1



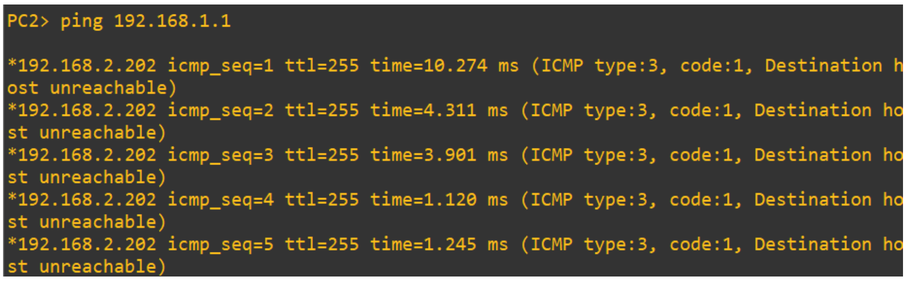
```
R2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.0.1.0 is directly connected, FastEthernet0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

Figure 2.6: Routing table of R2 after removing the network 192.168.1.0 from the RIP database of R1



```
PC1> ping 192.168.2.2

192.168.2.2 icmp_seq=1 timeout
192.168.2.2 icmp_seq=2 timeout
192.168.2.2 icmp_seq=3 timeout
192.168.2.2 icmp_seq=4 timeout
192.168.2.2 icmp_seq=5 timeout
```

Figure 2.7: Ping from PC1 to PC2. Timeout because no response from PC2 (one way communication PC1 → PC2)



```
PC2> ping 192.168.1.1

*192.168.2.202 icmp_seq=1 ttl=255 time=10.274 ms (ICMP type:3, code:1, Destination h
ost unreachable)
*192.168.2.202 icmp_seq=2 ttl=255 time=4.311 ms (ICMP type:3, code:1, Destination ho
st unreachable)
*192.168.2.202 icmp_seq=3 ttl=255 time=3.901 ms (ICMP type:3, code:1, Destination ho
st unreachable)
*192.168.2.202 icmp_seq=4 ttl=255 time=1.120 ms (ICMP type:3, code:1, Destination ho
st unreachable)
*192.168.2.202 icmp_seq=5 ttl=255 time=1.245 ms (ICMP type:3, code:1, Destination ho
st unreachable)
```

Figure 2.8: Ping from PC2 to PC1. Unreachable (one way communication PC1 → PC2)

3

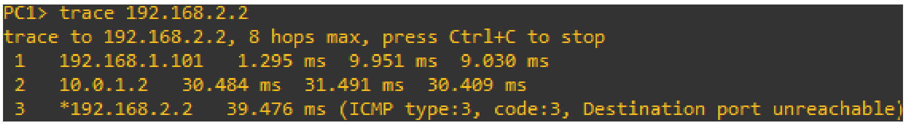
Mission 2 - Route Discovery

3.1 Question - Sanity check

Sanity check

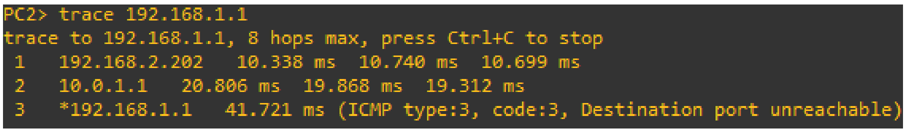
Make use of the trace command to find the route between both PCs. What is the path and its length (it is straightforward) ?

The results of the **trace** command for both PCs :



```
PC1> trace 192.168.2.2
trace to 192.168.2.2, 8 hops max, press Ctrl+C to stop
 1   192.168.1.101   1.295 ms  9.951 ms  9.030 ms
 2   10.0.1.2   30.484 ms  31.491 ms  30.409 ms
 3   *192.168.2.2   39.476 ms (ICMP type:3, code:3, Destination port unreachable)
```

Figure 3.1: Traceroute from PC1 to PC2



```
PC2> trace 192.168.1.1
trace to 192.168.1.1, 8 hops max, press Ctrl+C to stop
 1   192.168.2.202   10.338 ms  10.740 ms  10.699 ms
 2   10.0.1.1   20.806 ms  19.868 ms  19.312 ms
 3   *192.168.1.1   41.721 ms (ICMP type:3, code:3, Destination port unreachable)
```

Figure 3.2: Traceroute from PC2 to PC1

The routers R1 and R2 forms the path between both PCs. The length of this path is 2 (packets go through 2 routers).

3.2 Question - How does Traceroute reveal the path between devices ?

How does Traceroute reveal the path between devices ?

By analysing carefully your trace command using Wireshark (do not hesitate to capture all the three links), you should be able to understand how it works. Explain in details how the traceroute command works (and interesting observations you can make). What are the layer 3 protocols used and why ?

The traceroute command works as following :

1. If the first router's IP address isn't already associated with a MAC address, first PC sends an ARP request.

2. First PC sends an UDP packet to the destination with a source TTL (Time-To-Live) of 1.

3. Packet arrives at the first router, decrements the source TTL by one : 1 → 0. If the TTL is zero, the router sends back an ICMP response (Time to live exceeded in transit) to the first PC.

4. First PC resends an UDP packet to the destination but this time it increments the previous source TTL by one (1 → 2) so that the packet reaches the second router but not yet the destination.

   Remark : before incrementing the TTL, the first PC resends two times the packet (so at the end, three packets with TTL of 1 have been sent).

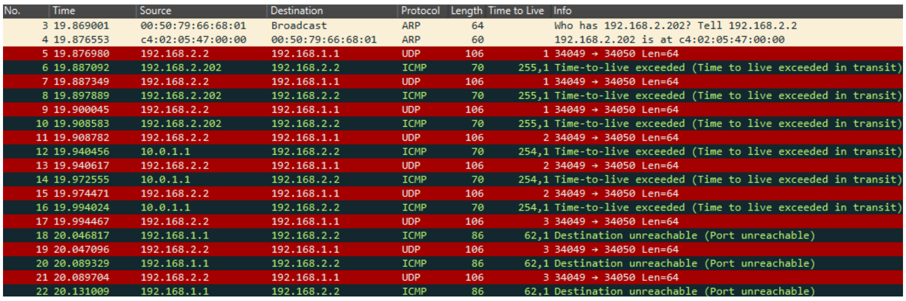
5. And this goes on until the source TTL is high enough that the UDP packet arrives at the destination. When this happens, the destination PC sends an ICMP response (Port unreachable) to the first PC. Also the first step can be repeated at this stage but this time for the destination PC.

Observations :

- Traceroute uses UDP and not TCP, this command doesn't search to establish a reliable connection (connectionless).
- Traceroute command is an iterative process. It starts from a very low TTL packet and stops when the TTL is enough. This is done for capturing the routers forming the path from source to destination.
- We can use the Traceroute command to test the latency for each node in the path.

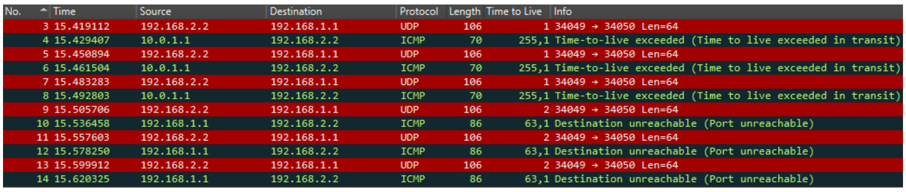
There are 3 protocols from the layer 3 used in traceroute :

- **ARP** or Address Resolution Protocol : it is used by the PCs to link the IP address to the MAC address of the routers they are directly connected to.
- **IPv4** : it is used for sending the UDP and ICMP packets from the source to the destination.
- **ICMP** : it is used for indicating the source that the TTL isn't high enough or indicating that the packet arrived at the destination.



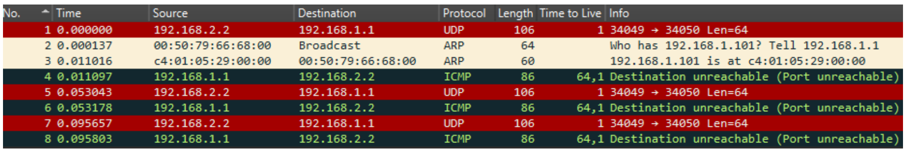
```
No.   Time       Source             Destination        Protocol Length Time to Live Info
    3 19.869001  00:50:79:66:68:01  Broadcast          ARP        64             Who has 192.168.2.202? Tell 192.168.2.2
    4 19.876553  c4:02:05:47:00:00  00:50:79:66:68:01  ARP        60             192.168.2.202 is at c4:02:05:47:00:00
    5 19.876980  192.168.2.2        192.168.1.1        UDP       106           1 34049 → 34050 Len=64
    6 19.887092  192.168.2.202      192.168.2.2        ICMP       70       255,1 Time-to-live exceeded (Time to live exceeded in transit)
    7 19.887349  192.168.2.2        192.168.1.1        UDP       106           1 34049 → 34050 Len=64
    8 19.897889  192.168.2.202      192.168.2.2        ICMP       70       255,1 Time-to-live exceeded (Time to live exceeded in transit)
    9 19.900045  192.168.2.2        192.168.1.1        UDP       106           1 34049 → 34050 Len=64
   10 19.908583  192.168.2.202      192.168.2.2        ICMP       70       255,1 Time-to-live exceeded (Time to live exceeded in transit)
   11 19.908782  192.168.2.2        192.168.1.1        UDP       106           2 34049 → 34050 Len=64
   12 19.940456  10.0.1.1           192.168.2.2        ICMP       70       254,1 Time-to-live exceeded (Time to live exceeded in transit)
   13 19.940617  192.168.2.2        192.168.1.1        UDP       106           2 34049 → 34050 Len=64
   14 19.972555  10.0.1.1           192.168.2.2        ICMP       70       254,1 Time-to-live exceeded (Time to live exceeded in transit)
   15 19.974471  192.168.2.2        192.168.1.1        UDP       106           2 34049 → 34050 Len=64
   16 19.994024  10.0.1.1           192.168.2.2        ICMP       70       254,1 Time-to-live exceeded (Time to live exceeded in transit)
   17 19.994467  192.168.2.2        192.168.1.1        UDP       106           3 34049 → 34050 Len=64
   18 20.046817  192.168.1.1        192.168.2.2        ICMP       86        62,1 Destination unreachable (Port unreachable)
   19 20.047096  192.168.2.2        192.168.1.1        UDP       106           3 34049 → 34050 Len=64
   20 20.089329  192.168.1.1        192.168.2.2        ICMP       86        62,1 Destination unreachable (Port unreachable)
   21 20.089704  192.168.2.2        192.168.1.1        UDP       106           3 34049 → 34050 Len=64
   22 20.131009  192.168.1.1        192.168.2.2        ICMP       86        62,1 Destination unreachable (Port unreachable)
```

Figure 3.3: Traceroute from PC2 to PC1. Wireshark link between PC2 and R2



```
No.   Time       Source             Destination        Protocol Length Time to Live Info
    3 15.419112  192.168.2.2        192.168.1.1        UDP       106           1 34049 → 34050 Len=64
    4 15.429407  10.0.1.1           192.168.2.2        ICMP       70       255,1 Time-to-live exceeded (Time to live exceeded in transit)
    5 15.450894  192.168.2.2        192.168.1.1        UDP       106           1 34049 → 34050 Len=64
    6 15.461504  10.0.1.1           192.168.2.2        ICMP       70       255,1 Time-to-live exceeded (Time to live exceeded in transit)
    7 15.483283  192.168.2.2        192.168.1.1        UDP       106           1 34049 → 34050 Len=64
    8 15.492803  10.0.1.1           192.168.2.2        ICMP       70       255,1 Time-to-live exceeded (Time to live exceeded in transit)
    9 15.505706  192.168.2.2        192.168.1.1        UDP       106           2 34049 → 34050 Len=64
   10 15.536458  192.168.1.1        192.168.2.2        ICMP       86        63,1 Destination unreachable (Port unreachable)
   11 15.557603  192.168.2.2        192.168.1.1        UDP       106           2 34049 → 34050 Len=64
   12 15.578250  192.168.1.1        192.168.2.2        ICMP       86        63,1 Destination unreachable (Port unreachable)
   13 15.599912  192.168.2.2        192.168.1.1        UDP       106           2 34049 → 34050 Len=64
   14 15.620325  192.168.1.1        192.168.2.2        ICMP       86        63,1 Destination unreachable (Port unreachable)
```

Figure 3.4: Traceroute from PC2 to PC1. Wireshark link between R2 and R1



No.	Time	Source	Destination	Protocol	Length	Time to Live	Info
1	0.000000	192.168.2.2	192.168.1.1	UDP	106	1	34049 → 34050 Len=64
2	0.000137	00:50:79:66:68:00	Broadcast	ARP	64		Who has 192.168.1.101? Tell 192.168.1.1
3	0.011016	c4:01:05:29:00:00	00:50:79:66:68:00	ARP	60		192.168.1.101 is at c4:01:05:29:00:00
4	0.011097	192.168.1.1	192.168.2.2	ICMP	86	64,1	Destination unreachable (Port unreachable)
5	0.053043	192.168.2.2	192.168.1.1	UDP	106	1	34049 → 34050 Len=64
6	0.053178	192.168.1.1	192.168.2.2	ICMP	86	64,1	Destination unreachable (Port unreachable)
7	0.095657	192.168.2.2	192.168.1.1	UDP	106	1	34049 → 34050 Len=64
8	0.095803	192.168.1.1	192.168.2.2	ICMP	86	64,1	Destination unreachable (Port unreachable)

Figure 3.5: Traceroute from PC2 to PC1. Wireshark link between R1 and PC1

4

Mission 3 - Redundancy and dynamic re-routing

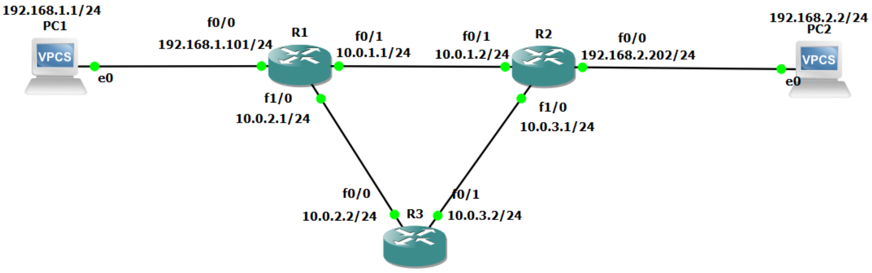


Figure 4.1: New topology of the network

4.1 Question - What is the route

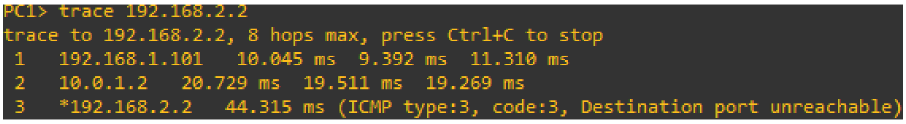
What is the route

What is the current route (IPs and devices) ? Did the route change (compared to mission 2: RIPv2) and why ?

After adding a third router and configuring it, the route from PC1 to PC2 is (as seen in the figure 4.2) :

- **PC1** (192.168.1.1) → **R1** (192.168.1.101) → **R2** (10.0.1.2) → **PC2** (192.168.2.2)

This route is the same as in the mission 2, see figure 3.1. It didn't change because it is the shortest route from PC1 to PC2. If the packets did go through the third router R3, it will take one more hop for the packets to arrive at PC2



```
PC1> trace 192.168.2.2
trace to 192.168.2.2, 8 hops max, press Ctrl+C to stop
 1   192.168.1.101   10.045 ms  9.392 ms  11.310 ms
 2   10.0.1.2   20.729 ms  19.511 ms  19.269 ms
 3   *192.168.2.2   44.315 ms (ICMP type:3, code:3, Destination port unreachable)
```

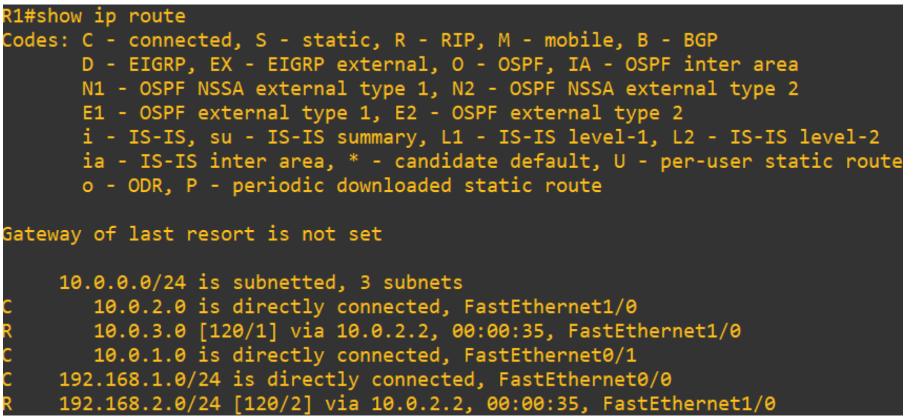
Figure 4.2: Traceroute from PC1 to PC2 for the new topology

4.2 Question - What changes in the routing table after a network link failure ?

What changes in the routing table after a network link failure ?

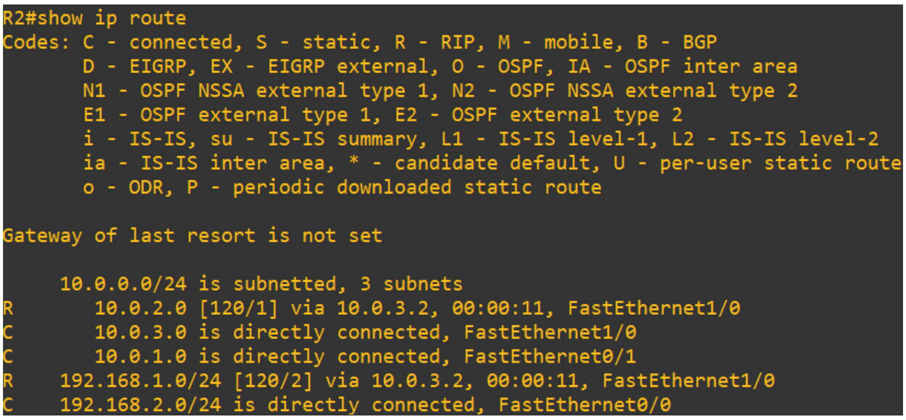
Display the routing table of your routers. What have changed ? How much time has it taken to change ? What could happen if you do a ping between PC1 and PC2 before the changes takes place ? What is the current route and its length ? Did the route change and why ?

The new routing tables for each router :



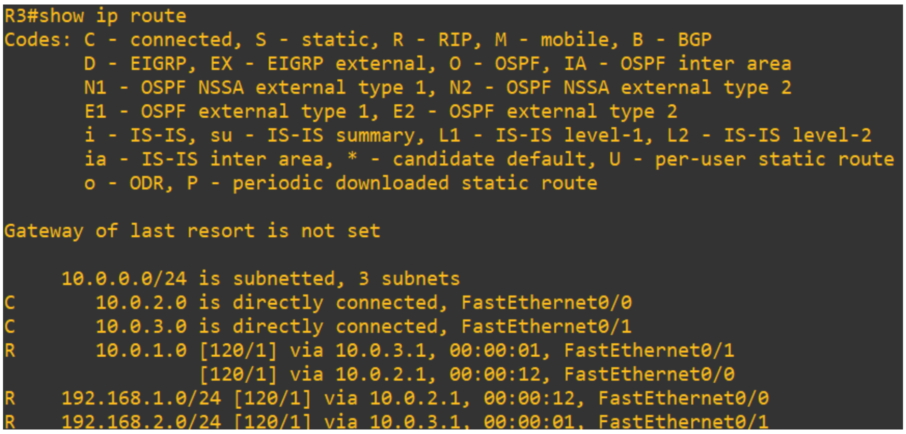
```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 3 subnets
C       10.0.2.0 is directly connected, FastEthernet1/0
R       10.0.3.0 [120/1] via 10.0.2.2, 00:00:35, FastEthernet1/0
C       10.0.1.0 is directly connected, FastEthernet0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
R    192.168.2.0/24 [120/2] via 10.0.2.2, 00:00:35, FastEthernet1/0
```

Figure 4.3: Routing table of R1 after updating the broken link



```
R2#show ip route
Codes: C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 3 subnets
R       10.0.2.0 [120/1] via 10.0.3.2, 00:00:11, FastEthernet1/0
C       10.0.3.0 is directly connected, FastEthernet1/0
C       10.0.1.0 is directly connected, FastEthernet0/1
R    192.168.1.0/24 [120/2] via 10.0.3.2, 00:00:11, FastEthernet1/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

Figure 4.4: Routing table of R2 after updating the broken link



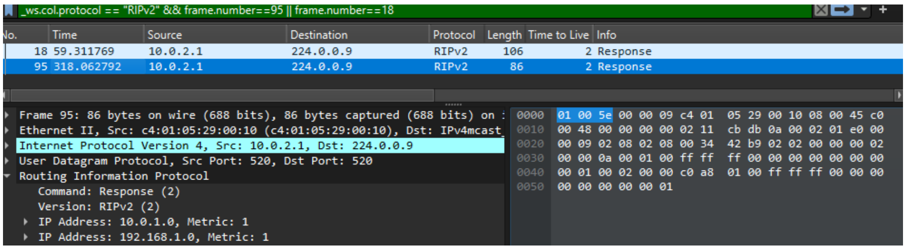
```
R3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 3 subnets
C       10.0.2.0 is directly connected, FastEthernet0/0
C       10.0.3.0 is directly connected, FastEthernet0/1
R       10.0.1.0 [120/1] via 10.0.3.1, 00:00:01, FastEthernet0/1
                 [120/1] via 10.0.2.1, 00:00:12, FastEthernet0/0
R    192.168.1.0/24 [120/1] via 10.0.2.1, 00:00:12, FastEthernet0/0
R    192.168.2.0/24 [120/1] via 10.0.3.1, 00:00:01, FastEthernet0/1
```

Figure 4.5: Routing table of R3 after updating the broken link

Only two things have changed for the router R1 and R2 :

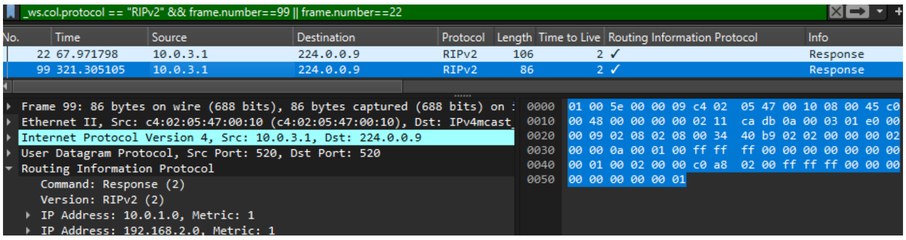
- In order to access the subnet of the PCs, the routers now go through R3 (for example, R1 needs to take R3 to get to 192.168.2.0)
- There is now only one path to access the subnet between the routers and R3 (for example, before the change R1 could access 10.0.3.0 via R2 or R3)

The change took approximately 260 seconds for R1 and for R2 after deleting the link in gns3.



```
_ws.col.protocol == "RIPv2" && frame.number==95 || frame.number==18

No.  Time        Source     Destination  Protocol  Length  Time to Live  Info
  18 59.311769   10.0.2.1   224.0.0.9    RIPv2     106                2  Response
  95 318.062792  10.0.2.1   224.0.0.9    RIPv2      86                2  Response

Frame 95: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on
Ethernet II, Src: c4:01:05:29:00:10 (c4:01:05:29:00:10), Dst: IPv4mcast_
Internet Protocol Version 4, Src: 10.0.2.1, Dst: 224.0.0.9
User Datagram Protocol, Src Port: 520, Dst Port: 520
Routing Information Protocol
   Command: Response (2)
   Version: RIPv2 (2)
   IP Address: 10.0.1.0, Metric: 1
   IP Address: 192.168.1.0, Metric: 1

0000  01 00 5e 00 00 09 c4 01  05 29 00 10 08 00 45 c0
0010  00 48 00 00 00 00 02 11  cb db 0a 00 02 01 e0 00
0020  00 09 02 08 02 08 00 34  42 b9 02 02 00 00 00 02
0030  00 00 0a 00 01 00 ff ff  ff 00 00 00 00 00 00 00
0040  00 01 00 02 00 00 c0 a8  01 00 ff ff ff 00 00 00
0050  00 00 00 00 00 01
```

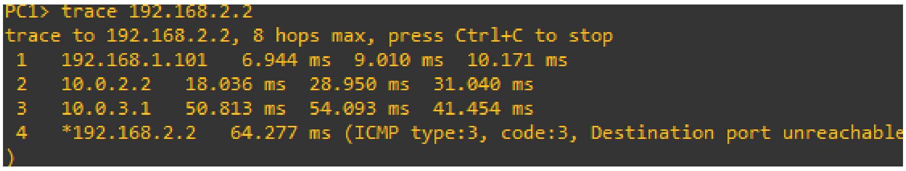
Figure 4.6: Wireshark screenshots. Listening to link between R1 and R3. Bottom left shows RIPv2 content sent by R1. Deleted link around t=60 seconds



```
_ws.col.protocol == "RIPv2" && frame.number==99 || frame.number==22

No.  Time        Source     Destination  Protocol  Length  Time to Live  Routing Information Protocol  Info
  22 67.971798   10.0.3.1   224.0.0.9    RIPv2     106                2  ✓                             Response
  99 321.305105  10.0.3.1   224.0.0.9    RIPv2      86                2  ✓                             Response

Frame 99: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on
Ethernet II, Src: c4:02:05:47:00:10 (c4:02:05:47:00:10), Dst: IPv4mcast_
Internet Protocol Version 4, Src: 10.0.3.1, Dst: 224.0.0.9
User Datagram Protocol, Src Port: 520, Dst Port: 520
Routing Information Protocol
   Command: Response (2)
   Version: RIPv2 (2)
   IP Address: 10.0.1.0, Metric: 1
   IP Address: 192.168.2.0, Metric: 1

0000  01 00 5e 00 00 09 c4 02  05 47 00 10 08 00 45 c0
0010  00 48 00 00 00 00 02 11  ca db 0a 00 03 01 e0 00
0020  00 09 02 08 02 08 00 34  40 b9 02 02 00 00 00 02
0030  00 00 0a 00 01 00 ff ff  ff 00 00 00 00 00 00 00
0040  00 01 00 02 00 00 c0 a8  02 00 ff ff ff 00 00 00
0050  00 00 00 00 00 01
```

Figure 4.7: Wireshark screenshots. Listening to link between R2 and R3. Bottom left shows RIPv2 content sent by R2. Deleted link around t=60 seconds

The current path is the following (inverse for PC2 to PC1) with length three (packets go through 3 routers):



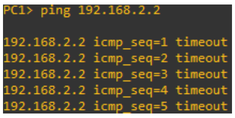
```
PC1> trace 192.168.2.2
trace to 192.168.2.2, 8 hops max, press Ctrl+C to stop
 1   192.168.1.101   6.944 ms  9.010 ms  10.171 ms
 2   10.0.2.2   18.036 ms  28.950 ms  31.040 ms
 3   10.0.3.1   50.813 ms  54.093 ms  41.454 ms
 4   *192.168.2.2   64.277 ms (ICMP type:3, code:3, Destination port unreachable
)
```

Figure 4.8: Trace command from PC1 to PC2

- **PC1** → **R1** (192.168.1.101) → **R3** (10.0.2.2) → **R2** (10.0.3.1) → **PC2** (192.168.2.2)

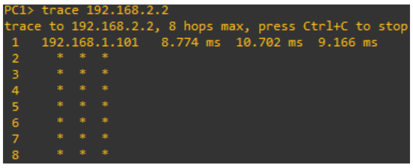
As we can see, the route did in fact change after the link between R1 and R2 has been broken. The RIP updated the routing table of each router after the destruction of the link

If we do a ping between PC1 and PC2 before the changes take place, we have no response from PC2 (see figure 4.9) because the first router didn't update the routing table and tries to send the packets through the broken link. We can see more clearly with the trace command (figure 4.10) that we don't get an answer from R2.



```
PC1> ping 192.168.2.2

192.168.2.2 icmp_seq=1 timeout
192.168.2.2 icmp_seq=2 timeout
192.168.2.2 icmp_seq=3 timeout
192.168.2.2 icmp_seq=4 timeout
192.168.2.2 icmp_seq=5 timeout
```

Figure 4.9: Ping from PC1 to PC2 with broken link and no changes in routing tables



```
PC1> trace 192.168.2.2
trace to 192.168.2.2, 8 hops max, press Ctrl+C to stop
 1   192.168.1.101   8.774 ms  10.702 ms  9.166 ms
 2     *  *  *
 3     *  *  *
 4     *  *  *
 5     *  *  *
 6     *  *  *
 7     *  *  *
 8     *  *  *
```

Figure 4.10: Trace from PC1 to PC2 with broken link and no changes in routing tables

4.3 Bonus Question

Bonus Question

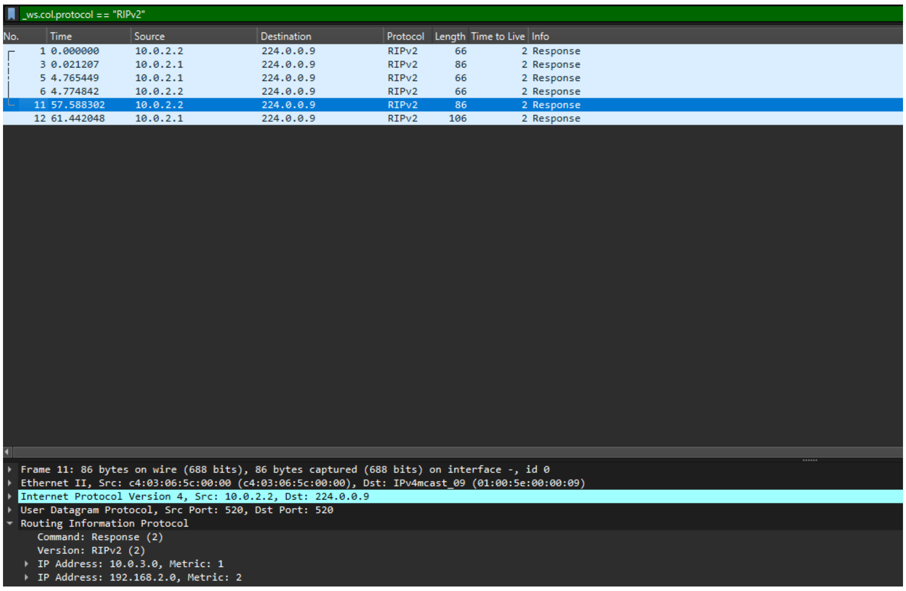
If you have looked carefully to the RIP packets, you should have noticed that the RIP packet does not contain all the router's routing table, but only a subset of the routing table. What part of the routing table is not send and why ?

The routers don't send the part of the routing tables that corresponds to a network which is directly connected to another router. For example, R3 doesn't tell R1 that it can serve the networks 192.168.1.0/24 and 10.0.1.0/24 because R1 is directly connected to these networks. However, R3 tells R1 that it is serving the networks 10.0.3.0/24 and 192.168.2.0/24.

Remark : routers don't send the network with which they communicate (in the previous case, neither R1 or R3 send to each other the fact that they serve the network 10.0.2.0, it is the subnet that connects them)

Why the routers do that ? The routers don't send these parts because the metrics associated with these networks will be always higher than the metric for a router direclty connected to it.

In fact, it is rather the router that is directly connected to a subnet that advertises it to other routers. The goal is to set up the shortest path from one network to another.

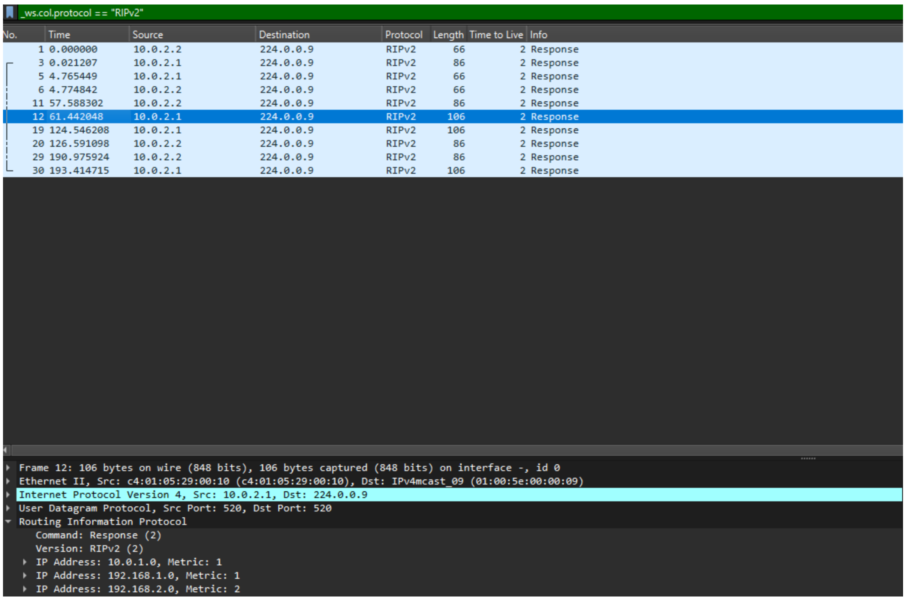


_ws.col.protocol == "RIPv2"

No.	Time	Source	Destination	Protocol	Length	Time to Live	Info
1	0.000000	10.0.2.2	224.0.0.9	RIPv2	66	2	Response
3	0.021207	10.0.2.1	224.0.0.9	RIPv2	86	2	Response
5	4.765449	10.0.2.1	224.0.0.9	RIPv2	66	2	Response
6	4.774842	10.0.2.2	224.0.0.9	RIPv2	66	2	Response
11	57.588302	10.0.2.2	224.0.0.9	RIPv2	86	2	Response
12	61.442048	10.0.2.1	224.0.0.9	RIPv2	106	2	Response

```
▸ Frame 11: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface -, id 0
▸ Ethernet II, Src: c4:03:06:5c:00:00 (c4:03:06:5c:00:00), Dst: IPv4mcast_09 (01:00:5e:00:00:09)
▸ Internet Protocol Version 4, Src: 10.0.2.2, Dst: 224.0.0.9
▸ User Datagram Protocol, Src Port: 520, Dst Port: 520
▾ Routing Information Protocol
    Command: Response (2)
    Version: RIPv2 (2)
  ▸ IP Address: 10.0.3.0, Metric: 1
  ▸ IP Address: 192.168.2.0, Metric: 2
```

Figure 4.11: Wireshark screenshot. Listening to link between R1 and R3. Bottom left shows RIPv2 content sent from R3



_ws.col.protocol == "RIPv2"

No.	Time	Source	Destination	Protocol	Length	Time to Live	Info
1	0.000000	10.0.2.2	224.0.0.9	RIPv2	66	2	Response
3	0.021207	10.0.2.1	224.0.0.9	RIPv2	86	2	Response
5	4.765449	10.0.2.1	224.0.0.9	RIPv2	66	2	Response
6	4.774842	10.0.2.2	224.0.0.9	RIPv2	66	2	Response
11	57.588302	10.0.2.2	224.0.0.9	RIPv2	86	2	Response
12	61.442048	10.0.2.1	224.0.0.9	RIPv2	106	2	Response
19	124.546208	10.0.2.1	224.0.0.9	RIPv2	106	2	Response
20	126.591098	10.0.2.2	224.0.0.9	RIPv2	86	2	Response
29	190.975924	10.0.2.2	224.0.0.9	RIPv2	86	2	Response
30	193.414715	10.0.2.1	224.0.0.9	RIPv2	106	2	Response

```
> Frame 12: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface -, id 0
> Ethernet II, Src: c4:01:05:29:00:10 (c4:01:05:29:00:10), Dst: IPv4mcast_09 (01:00:5e:00:00:09)
> Internet Protocol Version 4, Src: 10.0.2.1, Dst: 224.0.0.9
> User Datagram Protocol, Src Port: 520, Dst Port: 520
v Routing Information Protocol
      Command: Response (2)
      Version: RIPv2 (2)
    > IP Address: 10.0.1.0, Metric: 1
    > IP Address: 192.168.1.0, Metric: 1
    > IP Address: 192.168.2.0, Metric: 2
```

Figure 4.12: Wireshark screenshot. Listening to link between R1 and R3. Bottom left shows RIPv2 content sent from R1