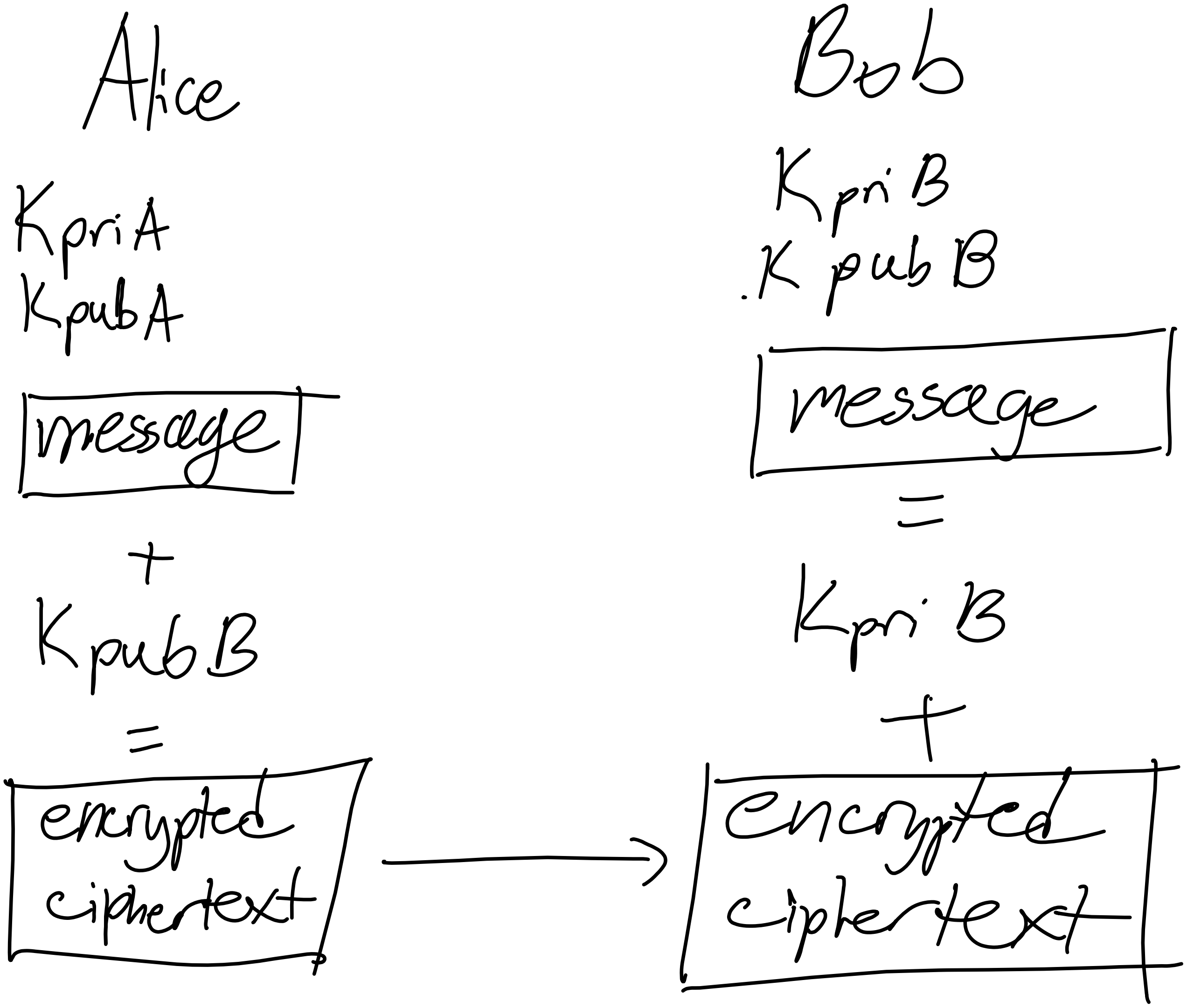
HW2

Part 1

1. Confidentiality refers to an adversary cannot find out who sent the message or to whom it will reach. Integrity refers to the adversary not being able to change the message without it having noticeable effect. You can have confidentiality without integrity by sending a message that when tampered with will just be lost and losing only integrity. You can have integrity without confidentiality by sending a cleartext message that will show signs if it is tampered with.

2. A non-forgeable, verifiable document requires that the signature require some near-impossible task that the other party can use a process to see if it is genuine. In the past, special inks and codes were used to protect documents, but now digital signatures are used. Digital signatures use a one-way hashing encryption algorithm that is near-impossible to forge and a low compute time, decryption algorithm that can be used to verify the message bits that matches the signature of the party sending it.

3.
    a. No, without a public key that Alice can use to create her own signature she cannot send a message that can be verified by Bob with the hash function.
    b.



4.

   a. You would need sequence numbers in order to send the correct NACK to the sender to make sure that particular data is sent again.
   b. The receiver would need a timer to make sure the sender didn't send the data and the NACK needed to be sent again.
   c. The sender would send a packet of data to the receiver with a unique sequence number. The receiver would only send a NACK if it received a packet with an unexpected sequence number. The receiver would set a timer for the NACKs and resend when it times out. The NACK-only protocol would fail in flow control since the receiver never sends a message to the sender if it is overloaded.

5.

S would send packet to AS 100 since it is the only link available. AS 100 would then run a check to see the shortest way to D using inter and intra domain algorithms, Distance Vector and Link State. AS 100 will see that the response time from AS 200 to interior router R4 is faster than routing iBGP through R2 and R3 and thus send the packet to AS 200 R5. AS 200 will use interdomain eBGP to send the packet back through AS 100 where the packet is received by gateway router R4. R4 will then send the packet to D.

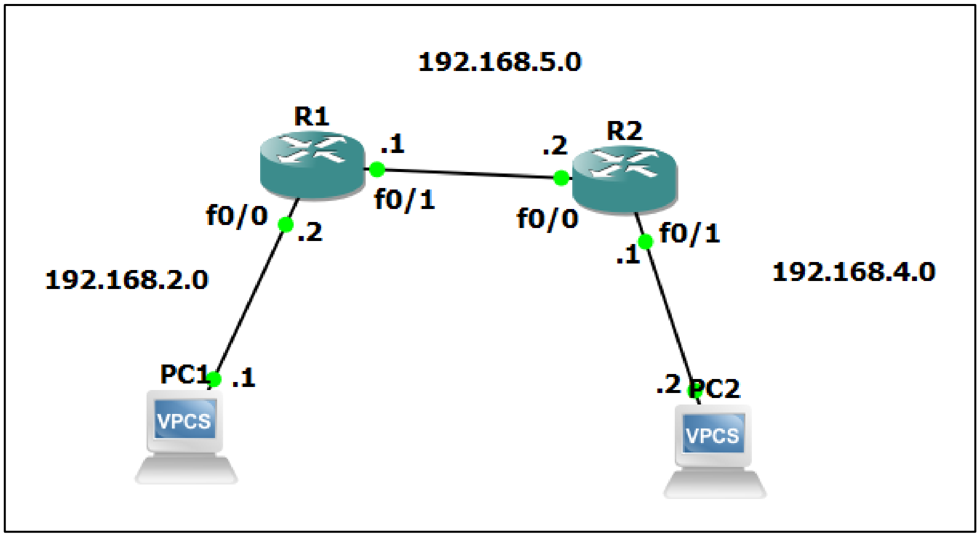
6.

This routing will use a greedy algorithm to find the shortest path from the source to the sink. It will only look at the available choices for nodes yet to be visited and will always choose the least weighted path. While the links are bidirectional, we assume the arrows are the way to the sink aka the next node will know where to go to get to the sink node.

The resulting path would be s, 3, 4, 7, 1 with a weight of 5, 4, 30, 10. This is not an optimal, but a greedy solution.

Part 2

1.



a.

Panther ID is 002074252.

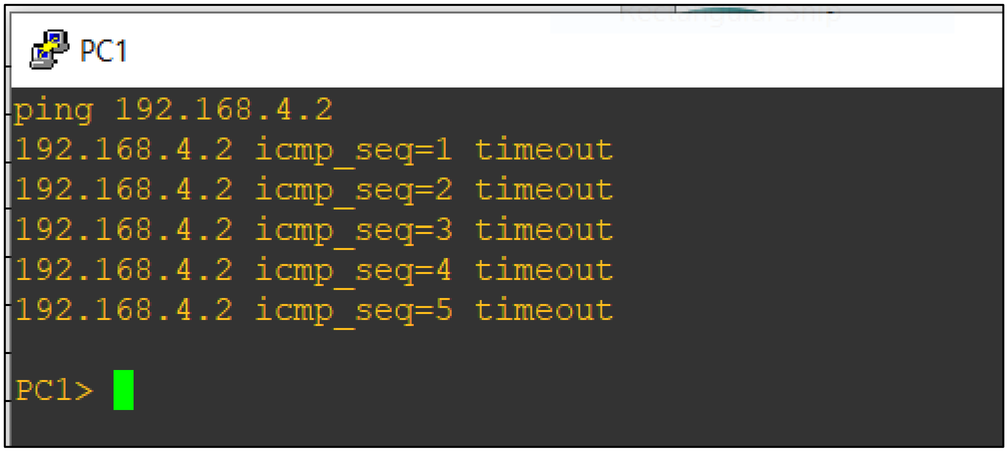
There are 3 subnets.

1 subnet between PC1 and R1.0, 192.168.2.0

1 subnet between R1.1 and R2.0, 192.168.5.0

1 subnet between PC2 and R2.1, 192.168.4.0 (used next number to avoid conflicts)

IP Address	MAC Address	Hostname
192.168.2.1	00:50:79:66:68:00	PC1
192.168.2.2	c803.282c.0001	R1.0
192.168.5.1	c803.282c.0010	R1.1
192.168.5.2	c804.29dc.0001	R2.0
192.168.4.1	c804.29dc.0010	R2.1
192.168.4.2	00:50:79:66:68:01	PC2

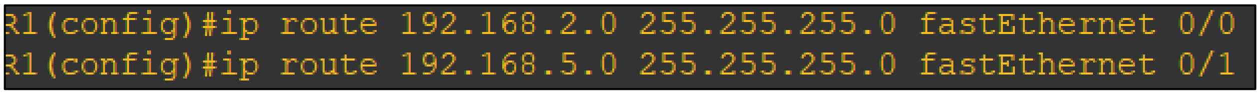


```
ping 192.168.4.2
192.168.4.2 icmp_seq=1 timeout
192.168.4.2 icmp_seq=2 timeout
192.168.4.2 icmp_seq=3 timeout
192.168.4.2 icmp_seq=4 timeout
192.168.4.2 icmp_seq=5 timeout

PC1>
```

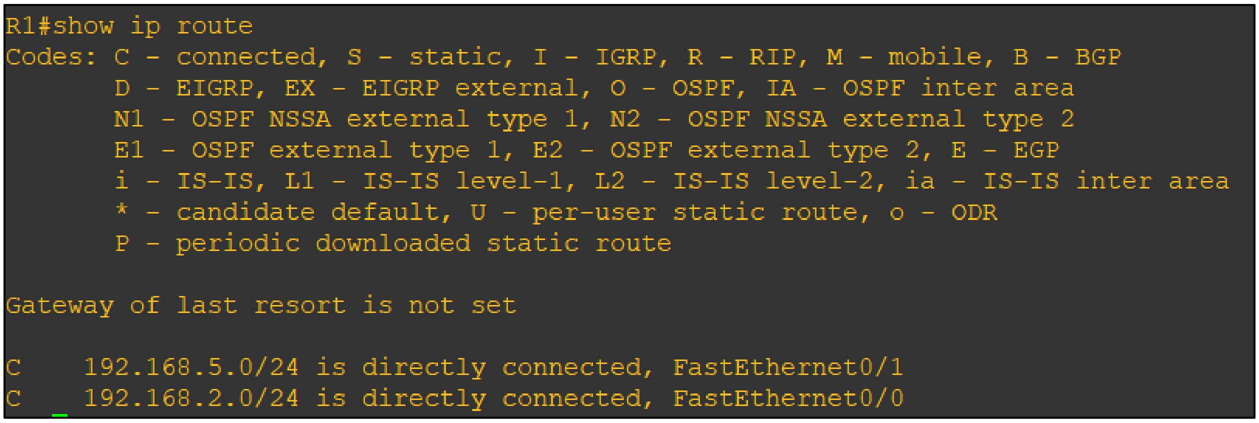
Our ping results in a timeout since while physically connected, there are no routes between PC1 and PC2 that can deliver the ICMP packet. We need to config the routers to route through the subnets.

b.

For R1:

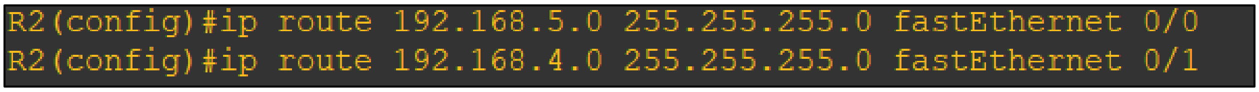


```
R1(config)#ip route 192.168.2.0 255.255.255.0 fastEthernet 0/0
R1(config)#ip route 192.168.5.0 255.255.255.0 fastEthernet 0/1
```

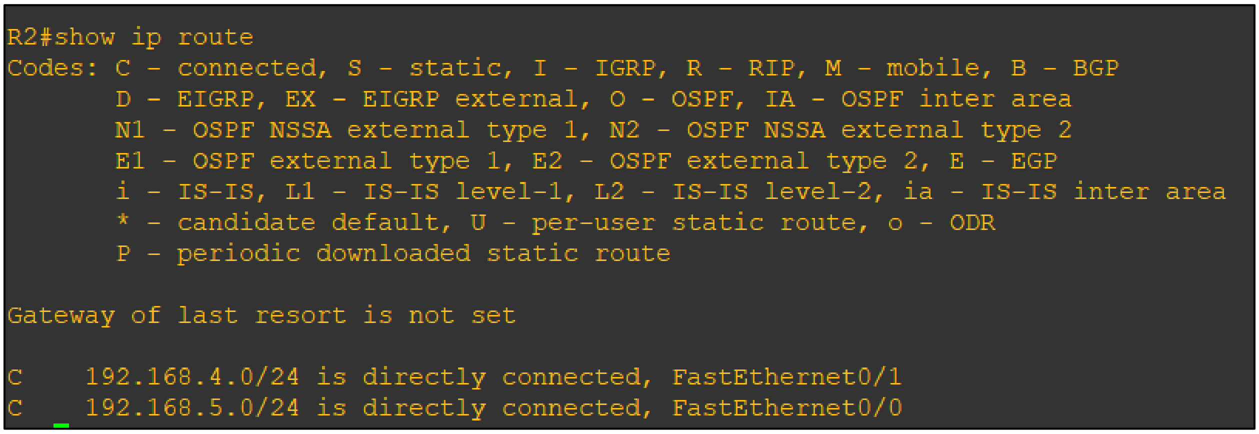


```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP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

Gateway of last resort is not set

C    192.168.5.0/24 is directly connected, FastEthernet0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

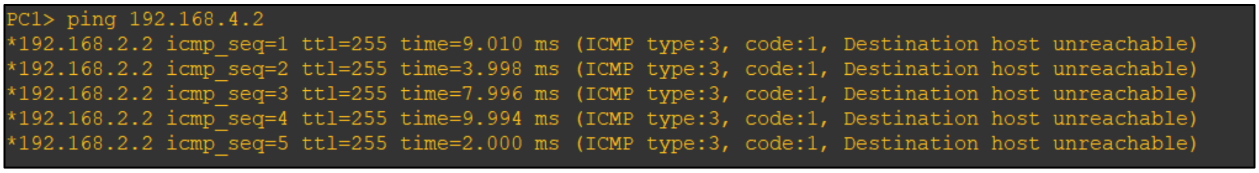
For R2:



```
R2(config)#ip route 192.168.5.0 255.255.255.0 fastEthernet 0/0
R2(config)#ip route 192.168.4.0 255.255.255.0 fastEthernet 0/1
```



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

Gateway of last resort is not set

C    192.168.4.0/24 is directly connected, FastEthernet0/1
C    192.168.5.0/24 is directly connected, FastEthernet0/0
```

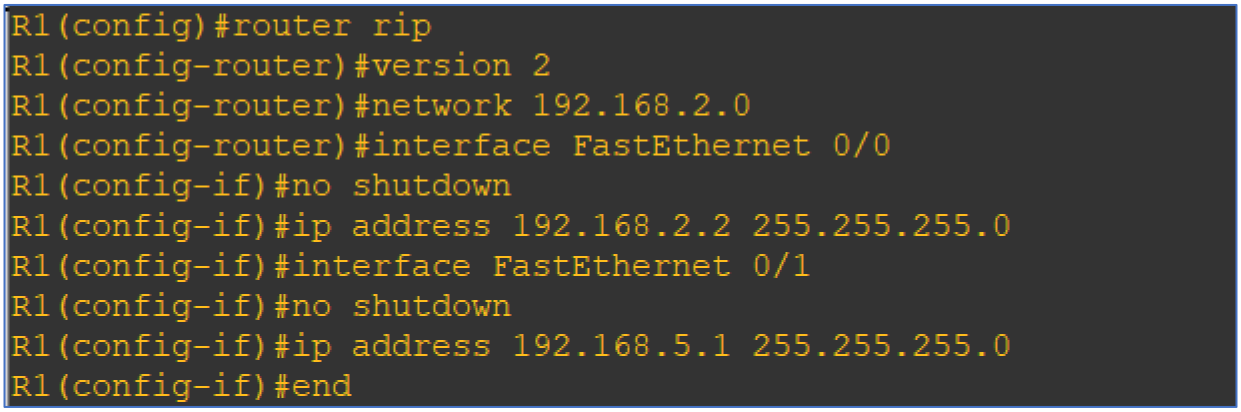


```
PC1> ping 192.168.4.2
*192.168.2.2 icmp_seq=1 ttl=255 time=9.010 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.2.2 icmp_seq=2 ttl=255 time=3.998 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.2.2 icmp_seq=3 ttl=255 time=7.996 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.2.2 icmp_seq=4 ttl=255 time=9.994 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.2.2 icmp_seq=5 ttl=255 time=2.000 ms (ICMP type:3, code:1, Destination host unreachable)
```

Here we have configured the routes required to reach the destination ip address 192.168.4.2 (PC2). Destination host unreachable is expected behavior since that indicates to the ping that the destination host was found and is the end of route.

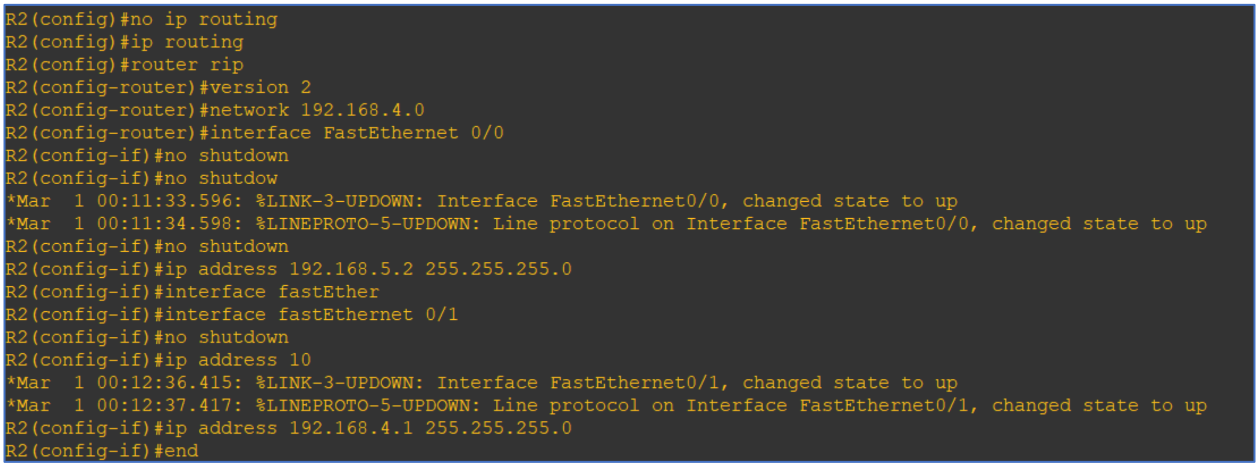
c.

For R1:

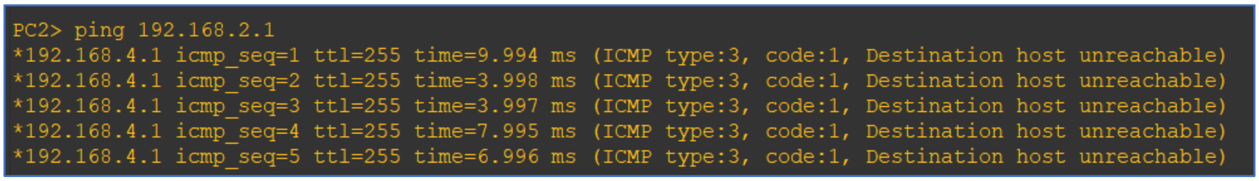


```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 192.168.2.0
R1(config-router)#interface FastEthernet 0/0
R1(config-if)#no shutdown
R1(config-if)#ip address 192.168.2.2 255.255.255.0
R1(config-if)#interface FastEthernet 0/1
R1(config-if)#no shutdown
R1(config-if)#ip address 192.168.5.1 255.255.255.0
R1(config-if)#end
```

For R2:



```
R2(config)#no ip routing
R2(config)#ip routing
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 192.168.4.0
R2(config-router)#interface FastEthernet 0/0
R2(config-if)#no shutdown
R2(config-if)#no shutdow
*Mar  1 00:11:33.596: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:11:34.598: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R2(config-if)#no shutdown
R2(config-if)#ip address 192.168.5.2 255.255.255.0
R2(config-if)#interface fastEther
R2(config-if)#interface fastEthernet 0/1
R2(config-if)#no shutdown
R2(config-if)#ip address 10
*Mar  1 00:12:36.415: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:12:37.417: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
R2(config-if)#ip address 192.168.4.1 255.255.255.0
R2(config-if)#end
```



```
PC2> ping 192.168.2.1
*192.168.4.1 icmp_seq=1 ttl=255 time=9.994 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.4.1 icmp_seq=2 ttl=255 time=3.998 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.4.1 icmp_seq=3 ttl=255 time=3.997 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.4.1 icmp_seq=4 ttl=255 time=7.995 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.4.1 icmp_seq=5 ttl=255 time=6.996 ms (ICMP type:3, code:1, Destination host unreachable)
```

Here we configured with rip routing and successfully reach PC1 from PC2 with a ping. I deleted my entire configurations for R1, R2 to make sure to get the right result.