

7.

2	1.339749	192.168.1.100	192.168.1.1	ICMP	98 Echo (ping) request	id=0x37ba, seq=1/256, ttl=64 (reply in 3)
3	1.354677	192.168.1.1	192.168.1.100	ICMP	98 Echo (ping) reply	id=0x37ba, seq=1/256, ttl=255 (request in 2)
4	2.375027	192.168.1.100	192.168.1.1	ICMP	98 Echo (ping) request	id=0x38ba, seq=2/512, ttl=64 (reply in 5)
5	2.389328	192.168.1.1	192.168.1.100	ICMP	98 Echo (ping) reply	id=0x38ba, seq=2/512, ttl=255 (request in 4)
6	3.408603	192.168.1.100	192.168.1.1	ICMP	98 Echo (ping) request	id=0x39ba, seq=3/768, ttl=64 (reply in 7)
7	3.422752	192.168.1.1	192.168.1.100	ICMP	98 Echo (ping) reply	id=0x39ba, seq=3/768, ttl=255 (request in 6)
8	4.441691	192.168.1.100	192.168.1.1	ICMP	98 Echo (ping) request	id=0x3aba, seq=4/1024, ttl=64 (reply in 9)
9	4.457446	192.168.1.1	192.168.1.100	ICMP	98 Echo (ping) reply	id=0x3aba, seq=4/1024, ttl=255 (request in 8)
10	5.478197	192.168.1.100	192.168.1.1	ICMP	98 Echo (ping) request	id=0x3bba, seq=5/1280, ttl=64 (reply in 11)
11	5.492784	192.168.1.1	192.168.1.100	ICMP	98 Echo (ping) reply	id=0x3bba, seq=5/1280, ttl=255 (request in 10)

Observando a captura do wireshark acima podemos ver que os pacotes ICMP Echo Request são enviados periodicamente com um intervalo de aproximadamente 1 segundo. O campo Sequence Number permite identificar cada pedido e associa-lo ao respectivo Echo Reply, depois o ping calcula o RTT subtraindo o instante de envio do request ao instante de recepção do reply com o mesmo número de sequencia

8.

- a. PC Ethernet/MAC address: 00:50:79:66:68:00
- b. Router Ethernet/MAC address: ca:01:19:20:00:08
- c. Hexadecimal code (Type field of Ethernet header) that identifies an IP datagram: 0x0800
- d. Hexadecimal code (Protocol field of IP header) that identifies na ICMP packet: 0x01
- e. Hexadecimal code (Type field of ICMP header) that identifies the two ICMP packet types (Echo Request and Echo Reply): 0x08 (Echo Request) 0x00 (Echo Reply)

11

```
PC1> arp
ca:01:19:20:00:08 192.168.1.1 expires in 112 seconds
```

O endereço IP do Router tem o endereço Ethernet ca:01:19:20:00:08 associado

13

## ARP Request

## Ethernet header

Origin MAC/Ethernet/Hardware Address: 00:50:79:66:68:00

Destination MAC/Ethernet/Hardware Address: ff:ff:ff:ff:ff:ff

## ARP Packet

Origin MAC/Ethernet/Hardware Address: 00:50:79:66:68:00

Origin IP Address: 192.168.1.100

## ARP Response

## Ethernet header

Origin MAC/Ethernet/Hardware Address: ca:01:19:20:00:08

Destination MAC/Ethernet/Hardware: 00:50:79:66:68:00

## ARP Packet

Origin MAC/Ethernet/Hardware Address: ca:01:19:20:00:08

Origin IP Address: 192.168.1.1

Destination MAC/Ethernet/Hardware Address: 00:50:79:66:68:00

Destination IP Address: 192.168.1.100

14.

Demora 120 segundos para desaparecer da ARP table

18.

## ARP

Padding: 00000000000000000000000000000000000000

## ICMP

Padding: 000000000000000000000000

20.

Executando o comando “ping 192.168.1.200” é possível ver o padding em ambos os pacotes ICMP, em que nos dois o padding é 000000000000000000000000

24.

a. cada pacote é fragmentado em 2 ou 3 fragmentos porque o tamanho máximo é 1500 bytes

b. Identification: valor igual em todos os fragmentos para identificar os conjuntos

Flag: 0x1 – More Fragments: indica que existem fragmentos a seguir e 0x0 indica o ultimo fragmento

Offset: Para ordenar os pacotes

c. Se enviarmos 2000 bytes de dados os pacotes são fragmentados em dois fragmentos o primeiro com 1514 bytes (14 bytes do Ethernet header, 20 bytes do IP header, 8 bytes do ICMP header e 1472 bytes de dados) e o segundo com 528 bytes (14 bytes do Ethernet header, 20 bytes do IP header e 528 bytes de dados)

Se enviarmos 3100 bytes de dados os pacotes são fragmentados em dois fragmentos o primeiro com 1514 bytes (14 bytes do Ethernet header, 20 bytes do IP header, 8 bytes do ICMP header e 1472 bytes de dados) o segundo também com 1514 bytes (14 bytes do Ethernet header, 20 bytes do IP header e 1480 bytes de dados) e o último com 182 (14 bytes do Ethernet header, 20 bytes do IP header e 148 bytes de dados)

## Parte 2

### 2.1

```
R1#show ip route
Codes: L - local, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, FastEthernet0/0
L       192.168.1.1/32 is directly connected, FastEthernet0/0
    192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, FastEthernet2/0
L       192.168.3.1/32 is directly connected, FastEthernet2/0
```

Usando o comando show ip route conseguimos ver que a rede 192.168.1.0/24 está conectada à interface f0/0 e 192.168.1.1 é o endereço local da interface. Relativamente à interface f2/0 podemos ver que 192.168.3.0/24 é a rede conectada e 192.168.3.1 o endereço da interface.

### 2.2

```
PC1> ping 192.168.3.33    PC3> ping 192.168.1.100
No gateway found          No gateway found
```

Em ambos os pings executados não é possível observar qualquer pacote no wireshark e no terminal aparece a mensagem no gateway found, isto porque, quando fazemos ping para outra rede os pacotes são enviados para a default gateway, para que o ping seja bem sucedido temos que configurar uma default gateway para ambos os PC's

## 2.3

```
PC3> ping 192.168.1.100
192.168.1.100 icmp_seq=1 timeout
192.168.1.100 icmp_seq=2 timeout
192.168.1.100 icmp_seq=3 timeout
192.168.1.100 icmp_seq=4 timeout
192.168.1.100 icmp_seq=5 timeout
```

→	56	430.825744	192.168.3.33	192.168.1.100	ICMP	98 Echo (ping) request	id=0x9bf8, seq=1/256, ttl=63 (reply in 61)
	59	432.821957	192.168.3.33	192.168.1.100	ICMP	98 Echo (ping) request	id=0x9df8, seq=2/512, ttl=63 (reply in 67)
←	61	433.841138	192.168.1.100	192.168.3.33	ICMP	98 Echo (ping) reply	id=0x9bf8, seq=1/256, ttl=64 (request in 56)
	63	434.835714	192.168.3.33	192.168.1.100	ICMP	98 Echo (ping) request	id=0x9ff8, seq=3/768, ttl=63 (reply in 72)
	66	436.849792	192.168.3.33	192.168.1.100	ICMP	98 Echo (ping) request	id=0xa1f8, seq=4/1024, ttl=63 (reply in 77)
	67	436.864742	192.168.1.100	192.168.3.33	ICMP	98 Echo (ping) reply	id=0x9df8, seq=2/512, ttl=64 (request in 59)
	70	438.867066	192.168.3.33	192.168.1.100	ICMP	98 Echo (ping) request	id=0xa3f8, seq=5/1280, ttl=63 (reply in 82)
	72	439.889959	192.168.1.100	192.168.3.33	ICMP	98 Echo (ping) reply	id=0x9ff8, seq=3/768, ttl=64 (request in 63)
	77	442.919436	192.168.1.100	192.168.3.33	ICMP	98 Echo (ping) reply	id=0xa1f8, seq=4/1024, ttl=64 (request in 66)
	82	445.938437	192.168.1.100	192.168.3.33	ICMP	98 Echo (ping) reply	id=0xa3f8, seq=5/1280, ttl=64 (request in 70)

Ao executar o ping do PC3 para o PC1 ocorre timeout, acontece porque, como a default gateway já está definida no PC3, o ping consegue chegar ao PC1, no entanto, como o PC1 não tem gateway definida ele não consegue responder então ocorre um timeout

## 2.4

```
PC1> ping 192.168.3.33
84 bytes from 192.168.3.33 icmp_seq=1 ttl=63 time=30.209 ms
84 bytes from 192.168.3.33 icmp_seq=2 ttl=63 time=31.279 ms
84 bytes from 192.168.3.33 icmp_seq=3 ttl=63 time=31.413 ms
84 bytes from 192.168.3.33 icmp_seq=4 ttl=63 time=32.251 ms
84 bytes from 192.168.3.33 icmp_seq=5 ttl=63 time=31.278 ms
```

Agora com a Default Gateway do PC1 configurada o ping já ocorre com sucesso

### ICMP Echo Request

Ethernet packet header      Source MAC Address: 00:50:79:66:68:00

“Owner”: PC1

Destination MAC Address: ca:01:28:b0:00:08

“Owner”: f0/0

IP packet header      Source IP Address: 192.168.1.100  
                              “Owner”: PC1  
                              Destination IP Address: 192.168.3.33  
                              “Owner”: PC3

## ICMP Echo Reply

Ethernet packet header      Source MAC Address: ca:01:28:b0:00:08  
                                      “Owner”: f0/0  
                                      Destination MAC Address: 00:50:79:66:68:00  
                                      “Owner”: PC1  
  
IP packet header      Source IP Address: 192.168.3.33  
                              “Owner”: PC3  
                              Destination IP Address: 192.168.1.100  
                              “Owner”: PC1

## 2.5

```
R1#show arp
Protocol Address      Age (min)  Hardware Addr  Type   Interface
Internet 192.168.1.1      -         ca01.28b0.0008  ARPA   FastEthernet0/0
Internet 192.168.1.100    11        0050.7966.6800  ARPA   FastEthernet0/0
Internet 192.168.3.1      -         ca01.28b0.0038  ARPA   FastEthernet2/0
Internet 192.168.3.33     11        0050.7966.6802  ARPA   FastEthernet2/0
```

Analizando a ARP table podemos ver que estão presentes os endereços IP e MAC dos PC's e interfaces que foram utilizados e por qual interface qual interface se chega a esse endereço

## 2.6

## ICMP Echo Request

Ethernet packet header      Source MAC Address: ca:01:28:b0:00:38  
   "Owner": f2/0  
   Destination MAC Address: 00:50:79:66:68:02  
   "Owner": PC3

IP packet header              Source IP Address: 192.168.1.100  
   "Owner": PC1  
   Destination IP Address: 192.168.3.33  
   "Owner": PC3

## ICMP Echo Reply

Ethernet packet header      Source MAC Address: 00:50:79:66:68:02  
   "Owner": PC3  
   Destination MAC Address: ca:01:28:b0:00:38  
   "Owner": f2/0

IP packet header              Source IP Address: 192.168.3.33  
   "Owner": PC3  
   Destination IP Address: 192.168.1.100  
   "Owner": PC1

## 2.7

4	28.110227	ca:01:28:b0:00:08	Broadcast	ARP	60 Who has 192.168.1.10? Tell 192.168.1.1
6	32.131609	ca:01:28:b0:00:08	Broadcast	ARP	60 Who has 192.168.1.10? Tell 192.168.1.1
7	36.154803	ca:01:28:b0:00:08	Broadcast	ARP	60 Who has 192.168.1.10? Tell 192.168.1.1

Como 192.168.1.10 é um endereço desconhecido que pertence a uma rede diferente do PC3, ele envia um ARP request para a default gateway aí o router encaminha para a rede da esquerda por este endereço pertencer à mesma mas como este endereço não existe, não ocorre qualquer resposta, ocorrendo um timeout.

## 2.8

2	0.746358	Private_66:68:02	Broadcast	ARP	64	Who has 192.168.3.1? Tell 192.168.3.33
3	0.760917	ca:01:28:b0:00:38	Private_66:68:02	ARP	60	192.168.3.1 is at ca:01:28:b0:00:38
4	0.776501	192.168.3.33	194.100.1.1	ICMP	98	Echo (ping) request id=0x2f05, seq=1/256, ttl=64 (no response found!)
5	0.792118	192.168.3.1	192.168.3.33	ICMP	70	Destination unreachable (Host unreachable)
6	1.809192	192.168.3.33	194.100.1.1	ICMP	98	Echo (ping) request id=0x3005, seq=2/512, ttl=64 (no response found!)
7	1.824234	192.168.3.1	192.168.3.33	ICMP	70	Destination unreachable (Host unreachable)
8	2.845514	192.168.3.33	194.100.1.1	ICMP	98	Echo (ping) request id=0x3105, seq=3/768, ttl=64 (no response found!)
9	2.860470	192.168.3.1	192.168.3.33	ICMP	70	Destination unreachable (Host unreachable)
10	3.880939	192.168.3.33	194.100.1.1	ICMP	98	Echo (ping) request id=0x3205, seq=4/1024, ttl=64 (no response found!)
11	3.895046	192.168.3.1	192.168.3.33	ICMP	70	Destination unreachable (Host unreachable)
12	4.911731	192.168.3.33	194.100.1.1	ICMP	98	Echo (ping) request id=0x3305, seq=5/1280, ttl=64 (no response found!)
13	4.926850	192.168.3.1	192.168.3.33	ICMP	70	Destination unreachable (Host unreachable)

O PC3 não conhece a rede do endereço então manda para a gateway, como o router não conhece a rede manda uma mensagem de volta de Destination unreachable host

## 2.10

```
R1#show ip route
Codes: L - local, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, FastEthernet0/0
L       192.168.1.1/32 is directly connected, FastEthernet0/0
    192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, FastEthernet2/0
L       192.168.3.1/32 is directly connected, FastEthernet2/0
```

É igual à routing table obtida no ponto 2.1

## 2.11



3	19.484843	Private_66:68:00	Broadcast	ARP	64 Who has 192.168.1.1? Tell 192.168.1.100
4	19.499215	ca:01:28:b0:00:08	Private_66:68:00	ARP	60 192.168.1.1 is at ca:01:28:b0:00:08
5	19.515210	192.168.1.100	192.168.3.150	ICMP	98 Echo (ping) request id=0x7e0a, seq=1/256, ttl=64 (no response found!)
7	21.527143	192.168.1.100	192.168.3.150	ICMP	98 Echo (ping) request id=0x800a, seq=2/512, ttl=64 (no response found!)
8	23.539130	192.168.1.100	192.168.3.150	ICMP	98 Echo (ping) request id=0x820a, seq=3/768, ttl=64 (no response found!)
9	25.548948	192.168.1.100	192.168.3.150	ICMP	98 Echo (ping) request id=0x840a, seq=4/1024, ttl=64 (no response found!)
10	27.559106	192.168.1.100	192.168.3.150	ICMP	98 Echo (ping) request id=0x860a, seq=5/1280, ttl=64 (no response found!)

192.168.3.150 é um endereço de outra rede então o PC1 envia para a Default Gateway um ARP, como o router conhece a rede envia para o lado direito onde esta rede está, como o endereço não é encontrado então ocorre timeout. Se isto fosse feito do outro lado do R1, ou seja, na mesma rede que o endereço que se procura, ia ser enviado um ARP request em Broadcast mas como não é encontrado ocorre um erro not reachable

## 2.12

20	253.575415	192.168.1.100	192.168.2.254	ICMP	98 Echo (ping) request id=0x5198, seq=1/256, ttl=64 (no response found!)
21	253.621049	192.168.1.1	192.168.1.100	ICMP	70 Destination unreachable (Host unreachable)
22	254.646014	192.168.1.100	192.168.2.254	ICMP	98 Echo (ping) request id=0x5298, seq=2/512, ttl=64 (no response found!)
23	254.661601	192.168.1.1	192.168.1.100	ICMP	70 Destination unreachable (Host unreachable)
24	255.684805	192.168.1.100	192.168.2.254	ICMP	98 Echo (ping) request id=0x5398, seq=3/768, ttl=64 (no response found!)
25	255.699795	192.168.1.1	192.168.1.100	ICMP	70 Destination unreachable (Host unreachable)
26	256.708341	192.168.1.100	192.168.2.254	ICMP	98 Echo (ping) request id=0x5498, seq=4/1024, ttl=64 (no response found!)
27	256.723040	192.168.1.1	192.168.1.100	ICMP	70 Destination unreachable (Host unreachable)
28	257.745623	192.168.1.100	192.168.2.254	ICMP	98 Echo (ping) request id=0x5598, seq=5/1280, ttl=64 (no response found!)
29	257.760479	192.168.1.1	192.168.1.100	ICMP	70 Destination unreachable (Host unreachable)

O PC1 não conhece a rede então envia para a Default Gateway como o R1 não tem essa rede na routing table então envia de volta com o erro Destination unreachable. Se a experiencia ocorresse do outro lado do R1 ou seja na rede 192.168.3.0/24, por exemplo fazendo ping do PC3 para 102.168.2.254, como o PC3 também não conhece a rede manda para a Default Gateway como o R1 tem essa rede na sua routing table então envia de volta com o erro Destination unreachable tal como na experiencia anterior.

## 2.13

```

R1#show ip route
Codes: L - local, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, FastEthernet0/0
L       192.168.1.1/32 is directly connected, FastEthernet0/0
S       192.168.2.0/24 [1/0] via 192.168.3.254
    192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, FastEthernet2/0
L       192.168.3.1/32 is directly connected, FastEthernet2/0

```

```

R2#show ip route
Codes: L - local, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

S       192.168.1.0/24 [1/0] via 192.168.3.1
    192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, FastEthernet0/0
L       192.168.2.254/32 is directly connected, FastEthernet0/0
    192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, FastEthernet2/0
L       192.168.3.254/32 is directly connected, FastEthernet2/0

```

Podemos ver que foi adicionada no routing table do R1 a linha “S 192.168.2.0/24 [1/0] via 192.168.3.254”, ou seja, tem uma rota estática para alcançar a rede 192.168.2.0/24 e para lá chegar primeiro tem que ir até 192.168.3.254, já na routing table do R2 foi adicionada a linha “S 192.168.1.0/24 [1/0] via 192.168.3.1”, ou seja, tem uma rota estática para alcançar a rede 192.168.1.0/24 e para lá chegar primeiro tem que ir até 192.168.3.1

```

PC1> ping 192.168.2.22
84 bytes from 192.168.2.22 icmp_seq=1 ttl=62 time=76.701 ms
84 bytes from 192.168.2.22 icmp_seq=2 ttl=62 time=61.132 ms
84 bytes from 192.168.2.22 icmp_seq=3 ttl=62 time=47.100 ms
84 bytes from 192.168.2.22 icmp_seq=4 ttl=62 time=71.876 ms
84 bytes from 192.168.2.22 icmp_seq=5 ttl=62 time=61.242 ms

```

Com a rotas estáticas definidas, é possível estabelecer conectividade

Ao executar ping 192.168.2.22 -T 1 apenas chega ao R1 pois quando chega o TTL é reduzido a zero e o router responde com um mensagem ICMP Time-to-live exceeded, ao executar ping 192.168.2.22 -T 2 já consegue chegar ao R2 mas não ao destino, quando passa pelo R1 o TTL é reduzido a 1 e quando chega ao R2 o TTL é reduzido a zero e a mensagem é descartada pelo router que envia uma mensagem ICMP Time-to-live exceeded, por último ao executar 192.168.2.22 -T 3 já consegue chegar ao PC3 e estabelecer conectividade pois o TTL necessário para chegar ao PC3 é 3

## 2.15

(i) Ao executar o comando “trace 192.168.2.22 -P 1” o pacote ICMP request é enviado com TTL=1, o qual é reduzido para 0 ao chegar ao R1, o qual envia para o PC1 um ICMP Time-to-live exceeded, o endereço de origem neste pacote é a interface do router que enviou a mensagem, assim o PC1 sabe qual o endereço da interface do R1, após isso o TTL é aumentado para 2 o que permite chegar até ao R2 no qual é reduzido para 0 (já tendo sido reduzido para 1 no R1) então o R2 envia para o PC1 um ICMP Time-to-live exceeded, o endereço o endereço de origem neste pacote é a interface do router que enviou a mensagem, assim o PC1 sabe qual o endereço da interface do R2

(ii)

2	11.764780	192.168.1.100	192.168.2.22	ICMP	106 Echo (ping) request id=0x702f, seq=0/0, ttl=1 (no response found!)
3	11.779346	192.168.1.1	192.168.1.100	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
4	11.779346	192.168.1.100	192.168.2.22	ICMP	106 Echo (ping) request id=0x702f, seq=0/0, ttl=1 (no response found!)
5	11.795107	192.168.1.1	192.168.1.100	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
6	11.810319	192.168.1.100	192.168.2.22	ICMP	106 Echo (ping) request id=0x702f, seq=0/0, ttl=1 (no response found!)
7	11.825054	192.168.1.1	192.168.1.100	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
8	11.840977	192.168.1.100	192.168.2.22	ICMP	106 Echo (ping) request id=0x702f, seq=0/0, ttl=2 (no response found!)
9	11.886156	192.168.3.254	192.168.1.100	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
10	11.901731	192.168.1.100	192.168.2.22	ICMP	106 Echo (ping) request id=0x702f, seq=0/0, ttl=2 (no response found!)
11	11.947034	192.168.3.254	192.168.1.100	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
12	11.962405	192.168.1.100	192.168.2.22	ICMP	106 Echo (ping) request id=0x702f, seq=0/0, ttl=2 (no response found!)
13	12.007595	192.168.3.254	192.168.1.100	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
14	12.007595	192.168.1.100	192.168.2.22	ICMP	106 Echo (ping) request id=0x702f, seq=0/0, ttl=3 (reply in 15)
15	12.068197	192.168.2.22	192.168.1.100	ICMP	106 Echo (ping) reply id=0x702f, seq=0/0, ttl=62 (request in 14)
16	12.083748	192.168.1.100	192.168.2.22	ICMP	106 Echo (ping) request id=0x712f, seq=0/0, ttl=3 (reply in 17)
17	12.144375	192.168.2.22	192.168.1.100	ICMP	106 Echo (ping) reply id=0x712f, seq=0/0, ttl=62 (request in 16)
18	12.159528	192.168.1.100	192.168.2.22	ICMP	106 Echo (ping) request id=0x712f, seq=0/0, ttl=3 (reply in 19)
19	12.219922	192.168.2.22	192.168.1.100	ICMP	106 Echo (ping) reply id=0x712f, seq=0/0, ttl=62 (request in 18)

O PC1 envia três pacotes ICMP Echo Request com TTL=1, três pacotes com TTL=2 e três pacotes com TTL=3 que é o TTL necessário para estabelecer conectividade

(iii)

O PC1 para o processo de aumentar o TTL quando recebe o pacote ICMP Echo Reply

## 2.16

```
PC1> trace 192.168.2.22 -P 1
trace to 192.168.2.22, 8 hops max (ICMP), press Ctrl+C to stop
 1  192.168.1.1    15.318 ms  15.430 ms  15.429 ms
 2  192.168.3.254  46.077 ms  45.639 ms  45.385 ms
 3  192.168.2.22   60.442 ms  61.067 ms  60.318 ms
```

```
PC1> trace 192.168.2.254 -P 1
trace to 192.168.2.254, 8 hops max (ICMP), press Ctrl+C to stop
 1  192.168.1.1    15.468 ms  15.611 ms  15.380 ms
 2  192.168.2.254  45.572 ms  46.046 ms  45.969 ms
```

Ao executar “trace 192.168.2.22 -P 1” o numero de saltos a fazer é maior pois o TTL é reduzido no R1 e no R2 não permitindo chegar ao PC4 sendo necessário um TTL=3 para alcança-lo, já ao executar “trace 192.168.2.254 -P 1” o número de saltos é menor pois como 192.168.2.254 é interface do R2 mesmo o TTL sendo reduzido no R2 consegue alcançar o destino em apenas dois saltos