Protocolos de Roteamento Dinâmicos

Nome: Luiza Kuze Gomes Disciplina: RCO786202

PARTE 1 - RIP

6. Anote as rotas do pc0 para o pc1 e pc2: "traceroute 10.0.1.20" e "traceroute 10.0.2.20"

```
root@pc0:/# traceroute 10.0.1.20
traceroute to 10.0.1.20 (10.0.1.20), 30 hops max, 60 byte packets
    10.0.0.1 (10.0.0.1) 0.116 ms 0.041 ms
                                                     0.020 \text{ ms}
                                0.047 \text{ ms}
2 10.0.10.2 (10.0.10.2)
                                            0.032 <u>ms</u>
                                                        0.031 \text{ ms}
    10.0.1.20 (10.0.1.20)
                                0.120 \text{ ms}
                                            0.070 ms
                                                        0.066 \, \text{ms}
root@pc0:/# traceroute 10.0.2.20
traceroute to 10.0.2.20 (10.0.2.20), 30 hops max, 60 byte packets
    10.0.0.1 (10.0.0.1) 0.092 ms 0.020 ms 0.017 ms
    10.0.11.2 (10.0.11.2)
                               0.041~\mathrm{ms}
                                            0.026 \text{ ms} - 0.024 \text{ ms}
                                0.045 \text{ ms}
    10.0.2.20 (10.0.2.20)
                                            0.035 \, \text{ms}
                                                        0.035 \, \text{ms}
```

7. Anote as tabelas de roteamento de todos os roteadores: route

```
root@pcO:/# route
Kernel IP routing table
                                                 Flags Metric Ref
                                                                      Use Iface
Destination
                                Genmask
                Gateway
default
                10.0.0.1
                                 0.0.0.0
                                                                        0 eth0
                                                 UG
10.0.0.0
                                                 Ш
                                                              Ó.
                0.0.0.0
                                 255,255,255,0
                                                                        0 eth0
root@pcO:/#
```

8. Interprete as tabelas de roteamento, diferenciando entrega direta e indireta

- Rota Default (Gateway padrão): Para qualquer destino desconhecido, o PC0 encaminhará os pacotes para o gateway 10.0.0.1 (R0), utilizando a interface eth0.
- Rota direta para 10.0.0.0/24: Os pacotes destinados à rede 10.0.0.0/24 (onde o próprio PC0 está) serão entregues diretamente, sem passar por nenhum roteador.

Então:

- Entregas diretas na rede local (10.0.0.0/24).
- Entregas indiretas para outras sub-redes usando o gateway padrão (10.0.0.1).
- 9. Vamos provocar a queda de um enlace, em seguida restabelecer e analisar todo o processo.
 - 1. Deixe um ping entre o pc0 e pc2 rodando.
 - 2. Deixe o Wireshark rodando na interface eth2 do R2.
 - 3. Desative o enlace R0-R2. No R2 execute: ifconfig eth1 down ou ip link set eth1 down

```
root@R2:/# ifconfig eth1 down
root@R2:/# █
```

5. Qual o tempo aproximado, medido no relógio, para reativação das repostas do ping?

Aproximadamente 3 minutos

6. Anote o número de sequência do último ping com sucesso antes da "derrubada" do enlace e o primeiro após o retorno do funcionamento normal do ping.

```
64 bytes from 10.0.2.20; icmp_seq=24 tt1=62 time=0.107 Ms
64 bytes from 10.0.2.20; icmp_seq=25 tt1=62 time=0.093 ms
64 bytes from 10.0.2.20; icmp_seq=26 tt1=62 time=0.111 ms
64 bytes from 10.0.2.20; icmp_seq=27 tt1=62 time=0.119 ms
64 bytes from 10.0.2.20; icmp_seq=28 tt1=62 time=0.111 ms
64 bytes from 10.0.2.20; icmp_seq=29 tt1=62 time=0.107 ms
64 bytes from 10.0.2.20; icmp_seq=30 tt1=62 time=0.082 ms
64 bytes from 10.0.2.20; icmp_seq=31 tt1=62 time=0.128 ms
64 bytes from 10.0.2.20; icmp_seq=31 tt1=62 time=0.116 ms
64 bytes from 10.0.2.20; icmp_seq=33 tt1=62 time=0.116 ms
64 bytes from 10.0.2.20; icmp_seq=34 tt1=62 time=0.113 ms
64 bytes from 10.0.2.20; icmp_seq=35 tt1=62 time=0.113 ms
64 bytes from 10.0.2.20; icmp_seq=35 tt1=62 time=0.137 ms
65 bytes from 10.0.2.20; icmp_seq=35 tt1=62 time=0.137 ms
66 bytes from 10.0.2.20; icmp_seq=36 tt1=62 time=0.137 ms
67 bytes from 10.0.2.20; icmp_seq=36 tt1=62 time=0.137 ms
68 bytes from 10.0.2.20; icmp_seq=36 tt1=62 time=0.137 ms
69 bytes from 10.0.2.20; icmp_seq=36 tt1=62 time=0.137 ms
60 bytes from 10.0.2.20; icmp_seq=36 tt1=62 time=0.137 ms
60 bytes from 10.0.2.20; icmp_seq=36 tt1=62 time=0.137 ms
61 bytes from 10.0.2.20; icmp_seq=36 tt1=62 time=0.137 ms
62 bytes from 10.0.2.20; icmp_seq=36 tt1=62 time=0.137 ms
63 bytes from 10.0.2.20; icmp_seq=36 tt1=62 time=0.113 ms
64 bytes from 10.0.2.20; icmp_seq=36 tt1=62 time=0.113 ms
65 bytes from 10.0.2.20; icmp_seq=36 tt1=62 time=0.113 ms
66 bytes from 10.0.2.20; icmp_seq=36 tt1=62 time=0.113 ms
67 bytes from 10.0.2.20; icmp_seq=36 tt1=62 time=0.113 ms
68 bytes from 10.0.2.20; icmp_seq=36 tt1=62 time=0.113 ms
69 bytes from 10.0.2.20; icmp_seq=36 tt1=62 time=0.113 ms
60 bytes from 10.0.2.20; icmp_seq=36 tt1=62 time=0.113 ms
61 bytes from 10.0.2.20; icmp_seq=30 tt1=62 time=0.113 ms
62 bytes from 10.0.2.20; icmp_seq=30 tt1=62 time=0.113 ms
63 bytes from 10.0.2.20; icmp_seq=30 tt1=62 time=0.113 ms
64 bytes from 10.0.2.20; icmp_seq=30 tt1=62 time=0.113 ms
64 bytes from 10.0.2.20; icmp_seq=30 tt1=62 time=0.113 ms
64 bytes from 10
```

Último número de sequência antes da derrubada: 36 Primeiro número de sequência após o retorno: 202

7. Anote a nova rota do pc0 para o pc2 e a compare com a mesma rota obtida anteriormente: traceroute 10.0.2.20.

```
root@pc0:/# traceroute 10.0.2.20
traceroute to 10.0.2.20 (10.0.2.20), 30 hops max, 60 byte packets
1 10.0.0.1 (10.0.0.1) 0.128 ms 0.035 ms 0.019 ms
2 10.0.10.2 (10.0.10.2) 0.047 ms 0.032 ms 0.031 ms
3 10.0.12.2 (10.0.12.2) 0.062 ms 0.044 ms 0.044 ms
4 10.0.2.20 (10.0.2.20) 0.070 ms 0.056 ms 0.057 ms
root@pc0:/#
```

8. Anote novamente as tabelas de roteamento de todos os roteadores:

- 10. Reative o enlace R0-R2. No R2 execute: ifconfig eth1 up ou ip link set eth1 up
 - 1. Em algum momento o ping deixou de funcionar? Não.
 - 2. Aguarde por volta de uns 2 minutos e anote novamente a rota do pc0 para o pc2: traceroute 10.0.2.20

Voltou para como estava antes.

```
root@pc0:/# traceroute 10.0.2.20
traceroute to 10.0.2.20 (10.0.2.20), 30 hops max, 60 byte packets
1 10.0.0.1 (10.0.0.1) 0.084 ms 0.018 ms 0.016 ms
2 10.0.11.2 (10.0.11.2) 0.037 ms 0.025 ms 0.025 ms
3 10.0.2.20 (10.0.2.20) 0.046 ms 0.036 ms 0.035 ms
root@pc0:/#
```

- 11. Identifique e aponte as diferenças entre as rotas com e sem a queda de enlace. Obs: estão relacionados com a interface desativada.
 - Rota inicial:

 $PC0 \rightarrow R0 \rightarrow R2 \rightarrow PC2$. O enlace direto entre **R0** e **R2** estava funcionando, então o protocolo RIP escolheu este caminho como a rota mais curta.

- Durante a Queda do Enlace:

 $PC0 \rightarrow R0 \rightarrow R1 \rightarrow R2 \rightarrow PC2$. O tráfego foi redirecionado através de **R1**, usando a rota alternativa propagada pelo RIP.

- 12. A partir das mensagens do Wireshark responda:
 - É possível usar o filtro rip, para limpar a visualização.

- Clique sobre a mensagem e expanda o campo *Routing Information Protocol* na janela central, será possível visualizar mensagens do tipo *IP Address: 10.0.12.0, Metric: 16*
- Os roteadores são identificados por seus IPs.
- O campo *Metric* indica o número de saltos do roteador em questão até a rede destino.
 - 1. Tente compreender as mensagens RIPv2 trocadas desde o início explicando-as.

Request (Mensagem No. 1): A primeira mensagem capturada é um **RIP Request** enviado por **10.0.12.2** para o endereço multicast **224.0.0.9**. Este é um pedido de atualização de rotas.

Responses (Mensagem No. 2): As respostas são mensagens **RIP Response** trocadas entre os roteadores (como 10.0.12.1 e 10.0.12.2).

2. Justifique/explique o valor das métricas (1, 2, 3, ..., 16).

O RIP tem métricas que determinam o número máximo de saltos permitidos que são 15. Quando tem a métrica 16 significa que o destino é inalcançável. Pegando somente dois pacotes para exemplificar:

Métrica do primeiro pacote após queda de enlace:

- Métrica 16: Indica que a rota não está disponível (inalcançável).

```
Wireshark Packet 1 --

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface -, id 0

Ethernet II, Src: 42:00:aa:00:00:0a (42:00:aa:00:00:0a), Dst: IPv4mcast_09 (01:00:5e:00:00:09)

Internet Protocol Version 4, Src: 10.0.12.2, Dst: 224.0.0.9

User Datagram Protocol, Src Port: 520, Dst Port: 520

Routing Information Protocol
Command: Request (1)
Version: RIPv2 (2)

Address not specified, Metric: 16
Address Family: Unspecified (0)
Route Tag: 0
Netmask: 0.0.0.0
Next Hop: 0.0.0.0
```

Métricas do segundo pacote (ao se recuperar da derrubada):

- Métrica 2: A dois saltos de distância.
- Métrica 1: Diretamente conectada.

```
Wireshark Packet 2--

Frame 2: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface -, ic

Ethernet II, Src: 42:00:aa:00:00:0b (42:00:aa:00:00:0b), Dst: 42:00:aa:00:00:0a (42:00:a)

Internet Protocol Version 4, Src: 10.0.12.1, Dst: 10.0.12.2

Routing Information Protocol

Command: Response (2)

Version: RIPV2 (2)

IP Address: 10.0.0.0 Metric: 2

Address Family: IP (2)

Route Tag: 0

IP Address: 10.0.0.0

Netmask: 255.255.255.55.0

Next Hop: 0.0.0.0

Metric: 2

IP Address: 10.0.1.0

Netmask: 255.255.255.55.0

Next Hop: 0.0.0.0

Metric: 1

IP Address: 10.0.1.0

Netmask: 255.255.255.55.0

Next Hop: 0.0.0.0

Metric: 1

IP Address: 10.0.10.0

Netmask: 255.255.255.255.0

Next Hop: 0.0.0.0

Metric: 1

IP Address: 10.0.10.0

Netmask: 255.255.255.255.255

Next Hop: 0.0.0.0

Metric: 1

IP Address: 10.0.11.0

Netmask: 255.255.255.255.255

Next Hop: 0.0.0.0

Metric: 1

IP Address: 10.0.11.0

Netmask: 255.255.255.255.255

Next Hop: 0.0.0.0

Metric: 1

IP Address: 10.0.11.0

Netmask: 255.255.255.255.255

Next Hop: 0.0.0.0

Metric: 2
```

3. Qual o intervalo aproximado na troca de mensagens?

Aproximadamente 30 segundos.

4. Qual o número (No.) da mensagem onde a rede apresentou problemas com rotas (obs: retire o filtro rip e procure no número de sequência dos pings (seq) os números anotados no item 15.1).

Como eu já havia fechado o Wireshark anteriormente, não consegui obter os dados do experimento inicial. Tentei fazê-lo, mas percebi que desta vez nem mesmo apareceu o erro "Destination Host Unreachable" ou "Destination Net Unreachable". Isso indica que, nesse novo experimento, o RIP pode ter demorado um pouco para convergir, mas agora já conhece as rotas novamente, e os pacotes estão sendo encaminhados corretamente.

```
traceroute to 10.0.1.20 (10.0.1.20), 30 hops max, 60 byte packets
    10.0.0.1 (10.0.0.1) 0.098 ms 0.023 ms 0.017 ms
   10.0.10.2 (10.0.10.2)
                            0.051 ms 0.030 ms 0.028 ms
    10.0.1.20 (10.0.1.20)
                            0.100 ms
                                       0.043 ms 0.043 ms
root@pc0:/# traceroute 10.0.2.20
traceroute to 10.0.2.20 (10.0.2.20), 30 hops max, 60 byte packets
    10.0.0.1 (10.0.0.1) 0.108 ms 0.023 ms 0.024 ms
    10.0.11.2 (10.0.11.2)
                            0.061 ms
                                       0.034 \text{ ms} - 0.031 \text{ ms}
    10.0.2.20 (10.0.2.20)
                            0.061 \text{ ms}
                                       0.045 \text{ ms} - 0.043 \text{ ms}
```

5. Quais e quantas mensagens (número) são trocadas entre os roteadores para restabelecer as rotas?

Entre os roteadores, o RIP troca mensagens de atualização (RIP Response) periodicamente, a cada 30 segundos por padrão.

6. Pesquise o significado do endereço 224.0.0.9.

É o endereço multicast utilizado pelos roteadores RIP.

PARTE 2 - OSPF

6. Anote as rotas do pc0 para o pc1 e pc2: traceroute 10.0.1.20 e traceroute 10.0.2.20

```
raceroute to 10.0.2.20 (10.0.2.20), 30 hops max, 60 byte packets
1 10.0.0.1 (10.0.0.1) 0.113 ms 0.032 ms 0.030 ms
2 10.0.11.2 (10.0.11.2) 0.072 ms 0.041 ms 0.028 ms
3 10.0.2.20 (10.0.2.20) 0.054 ms 0.040 ms 0.041 ms
root@pc0:/#
root@pc0:/#
traceroute 10.0.1.20
traceroute to 10.0.1.20 (10.0.1.20), 30 hops max, 60 byte packets
1 10.0.0.1 (10.0.0.1) 0.124 ms 0.036 ms 0.030 ms
2 10.0.10.2 (10.0.10.2) 0.070 ms 0.053 ms 0.048 ms
3 10.0.1.20 (10.0.1.20) 0.103 ms 0.070 ms
root@pc0:/#
```

- 7. Vamos provocar a queda de um enlace, em seguida restabelecer e analisar todo o processo.
 - 1. Deixe um ping entre o pc0 e pc2 rodando.
 - 2. Deixe o Wireshark rodando na interface eth2 do R2.
 - 3. Desative o enlace R0-R2. No R2 execute: ifconfig eth1 down ou ip link set eth1 down
 - 4. Monitorando o ping, aguarde até o retorno das repostas ao mesmo. É comum praticamente não percebermos falhas.
 - 5. Anote novamente a rota do pc0 para o pc2: traceroute 10.0.2.20

```
rootepc0;/# traceroute 10.0.2.20
raceroute to 10.0.2.20 (10.0.2.20), 30 hops max, 60 byte packets
   10.0.0.1 (10.0.0.1)
                             0.088 ms 0.042 ms
2 10.0.10.2 (10.0.10.2)
3 10.0.12.2 (10.0.12.2)
                               0.038 ms 0.027 ms
                                0.049 ms
                                            0.040 \text{ ms}
   10,0,2,20 (10,0,2,20)
                                0.059 \text{ ms}
                                            0.049 \, \text{ms}
oot@pc0:/# traceroute 10.0.1.20
traceroute to 10.0.1.20~(10.0.1.20), 30~{
m hops} max, 60~{
m byte} packets
    10.0.0.1 (10.0.0.1) 0.080 ms 0.018 ms 0.027 ms
    10.0.10.2 (10.0.10.2) 0.040 ms 0.027 ms 0.040 ms
                                0.056 ms
                                            0.040 \text{ ms}
```

6. Reative o enlace R0-R2. No R2 execute: if config eth1 up ou ip link set eth1 up

```
root@pc0:/# traceroute 10.0.2.20
traceroute to 10.0.2.20 (10.0.2.20), 30 hops max, 60 byte packets
1 10.0.0.1 (10.0.0.1) 0.127 ms 0.038 ms 0.033 ms
2 10.0.11.2 (10.0.11.2) 0.082 ms 0.047 ms 0.047 ms
3 10.0.2.20 (10.0.2.20) 0.095 ms 0.077 ms 0.071 ms
root@pc0:/# traceroute 10.0.1.20
traceroute to 10.0.1.20 (10.0.1.20), 30 hops max, 60 byte packets
1 10.0.0.1 (10.0.0.1) 0.101 ms 0.026 ms 0.018 ms
2 10.0.10.2 (10.0.10.2) 0.044 ms 0.030 ms 0.028 ms
3 10.0.1.20 (10.0.1.20) 0.055 ms 0.041 ms 0.041 ms
```

- 8. A partir das mensagens do Wireshark responda:
- É possível usar o filtro ospf, para limpar a visualização.
- Perceba que com o protocolo OSPF, diferentemente do RIP, não há trocas periódicas de mensagens do protocolo de roteamento.
- Só haverá trocas quando o protocolo sentir necessidade de alguma mudança de rota, por exemplo, com a queda de um enlace.
 - 1. Quais as mensagens trocadas pelo protocolo OSPF são observadas no WireShark? Observe o trecho de mensagens onde não houve respostas ao ping.

139 75.031840	10.0.12.2	10.0.12.1	0SPF	122 LS Update
140 76.019937	10.0.12.1	224.0.0.5	0SPF	78 LS Acknowledge
141 80.000127	10.0.12.1	224.0.0.5	0SPF	82 Hello Packet
142 80.026910	10.0.12.2	224.0.0.5	0SPF	82 Hello Packet
143 90.000143	10.0.12.1	224.0.0.5	OSPF	82 Hello Packet
144 90.026930	10.0.12.2	224.0.0.5	0SPF	

2. Qual o tempo aproximado para a total recuperação das rotas?

Mínimo, questão de poucos segundos.

3. As mensagens trocadas pelos roteadores são distintas quando comparadas ao uso do RIP?

Sim, o RIP utiliza as simples mensagens "Request" e "Response". No OSPF, as mensagens também incluem: "Hello Packet", "LS Update" e "LS Acknowledge".

4. Explique as mensagens "Hello Packet", "LS Update" e "LS Acknowledge".

Hello Packets: Para detectar e manter vizinhos ativos.

LS Update (Link-State Update): Para compartilhar informações sobre alterações de estado dos enlaces.

LS Acknowledge: Para confirmar o recebimento de atualizações de estado.

5. Houve diferença no tempo de atualização das rotas quando comparado ao RIP? Explique?

O tempo de atualização no RIP:

- Periodicidade Fixa: RIP envia atualizações a cada 30 segundos, independente das alterações na rede.
- Lento para Convergir: Alterações na topologia demoram bastante até serem reconhecidas.

O tempo de atualização no OSPF:

- Atualizações Sob Demanda: OSPF envia LS Updates apenas quando há alteração na topologia da rede.
- Convergência Rápida: Algoritmo de Dijkstra permite o cálculo extremamente rápido.
- Hello Packet: Permite detectar falhas rapidamente.