2.a)



Nova entrada do R1 e R2.

As novas entradas nas tabelas de encaminhamento surgem porque os endereços IPv4 configurados nas interfaces Tunnel 0 de R1 e R2 pertencem à rede 192.1.2.0/24.

2.b)

No ping do R1 para 192.1.2.2, os pacotes ICMP são capturados na rede 192.1.4.0. Não é capturado nenhum pacote na rede 192.1.5.0, pois como o ping é para o tunnel e o tunnel foi configurado a partir da interface 192.1.4.1, não passa assim pacotes por 192.1.5.0.

Mesmo que OSPF sugira que 192.2.4.2 (tunnel destination) possa ser alcançado via 192.1.5.0, o tráfego deste túnel específico não usará essa rota porque a sua origem foi explicitamente definida para ser 192.1.4.1.



Nos pacotes capturados, é possível ver a passagem pelo tunnel do pacote.

2.c)

Apenas é visível ping requests na captura de 192.1.4.0 . Isto acontece porque o tunnel foi definido para fazer comunicação apenas pelas interfaces configuradas (192.1.4.1 e 192.2.4.2).

Neste caso a interface 192.2.4.2 está desligada, tornando impossível realizar um ping para o tunnel. Há outras maneiras de chegar ao R2, mas como o ping é para o túnel, não é possível receber resposta.

2.d) e 2.e)

R1 consulta sua tabela de roteamento para encontrar o melhor caminho para 200.2.2.2.

Como o OSPF está ativo e as interfaces Loopback são anunciadas, R1 sabe como alcançar 200.2.2.2.

Existem dois caminhos principais de R1 para R2 na rede física:

* 1. R1 -> R4 -> R2
  2. R1 -> R5 -> R3 -> R2

O OSPF escolherá o caminho com o menor custo. R1 encaminhará o pacote pela sua interface f0/1 (192.1.4.1) em direção a R4.

Uma imagem com texto, software, Software de multimédia, captura de ecrã

Os conteúdos gerados por IA podem estar incorretos.

R1-R4 // R1-R5

A principal mudança é que o tunnel source agora é um endereço de Loopback (200.1.1.1). Este endereço é virtual e está sempre "up" enquanto o router R1 estiver funcionando, independentemente do estado de qualquer interface física individual.

**Benefício Principal: Resiliência.** Se a interface f0/1 de R1 (que leva a R4) falhasse, mas a interface f1/0 (que leva a R5) estivesse funcionando, R1 ainda poderia alcançar 200.2.2.2 através de R5->R3->R2. OSPF atualizaria a rota para 200.2.2.2, e o túnel continuaria a funcionar, agora usando o caminho alternativo, sem precisar de reconfiguração do túnel em si. Isso contrasta com a configuração anterior (2.b), onde se a interface física 192.1.4.1 falhasse, o túnel falharia imediatamente porque o tunnel source estaria inativo.

Uma imagem com texto, software, Software de multimédia, Tipo de letra

Os conteúdos gerados por IA podem estar incorretos.

R1-R4 // R1-R5

R1-R5 recebe os pacotes, pois a interface f1/0 de R2 está desligada.

2.f)

Este pacote ICMP (que é um pacote IP) é agora encapsulado dentro de um cabeçalho GRE e, em seguida, dentro de um novo cabeçalho IP (o cabeçalho de transporte ou "outer header").

**Cabeçalho GRE:** Será adicionado entre o cabeçalho IP externo e o pacote IP interno. Uma das funções importantes do cabeçalho GRE é identificar o tipo de protocolo do payload que ele está carregando (neste caso, IPv4).

**Protocolo: 47 (GRE)**. Este é o número de protocolo IP que indica que o payload deste pacote externo é um pacote GRE

Os pacotes são observados na rede 192.1.4.0/24 pela mesma razão da pergunta anterior.

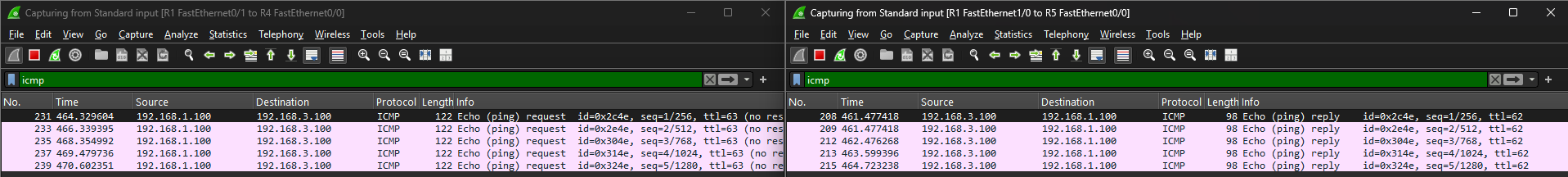
***R1(config)# ip route 192.168.3.0 255.255.255.0 tunnel 0***

A rota estática para 192.168.3.0 através do Tunnel0 substitui a rota OSPF previamente aprendida porque as rotas estáticas têm uma Distância Administrativa (AD) padrão de 1, enquanto as rotas OSPF têm uma AD padrão de 110. O router sempre prefere a rota com a menor Distância Administrativa quando existem múltiplas fontes de roteamento para o mesmo prefixo de destino.

2.g)

O tráfego de PC1 para PC2 não utiliza o túnel porque R1 não tem uma rota que direcione o tráfego para a rede do PC2 através do Tunnel0. R1 usa a rota OSPF aprendida para a rede do PC2.

2.h)



R1-R4 Requests // Replys R1-R5

**Pacote ICMP Echo Request (PC1 -> PC3):**

1. PC1 (192.168.1.100) envia o Echo Request para PC3 (192.168.3.100). **O gateway de PC1 é R1**.
2. R1 recebe o pacote. O destino é 192.168.3.100.
3. R1 consulta sua tabela de roteamento. A rota 192.168.3.0 através do tunnel 0 corresponde ao destino.
4. R1 decide que a interface de saída é Tunnel0. Portanto, R1 encapsula o pacote ICMP original:
5. R1 encaminha o pacote encapsulado pela sua interface física que leva ao melhor caminho para 200.2.2.2 (f0/1 via R4).

**Na captura da rede 192.1.4.0/24 (R1-R4):**Será visto o pacote encapsulado (com IPs externos 200.1.1.1 -> 200.2.2.2).

1. R2 recebe o pacote encapsulado, desencapsula-o e vê o pacote interno **destinado a 192.168.3.100**.
2. R2 encaminha o pacote ICMP original para R3 (via OSPF).
3. R3 encaminha para PC3.

**Pacote ICMP Echo Reply (PC3 -> PC1):**

É enviado pela rede física **sem encapsulamento**, seguindo o melhor caminho OSPF. R3 envia para R5, e R5 envia para R1.

Este cenário demonstra que a decisão de usar um túnel é tomada hop-by-hop com base na tabela de roteamento do roteador que está processando o pacote. Uma rota estática em R1 para usar o túnel não implica automaticamente que R2 usará o túnel para o tráfego de retorno, a menos que uma configuração correspondente exista em R2.