



Universidade do Minho
Escola de Engenharia

REDES DE ACESSO E NÚCLEO
ENGENHARIA DE TELECOMUNICAÇÕES E INFORMÁTICA

29 DE ABRIL DE 2022

TP2 - ENGENHARIA DE TRÁFEGO COM MPLS

Autores:

Hugo Miguel Miranda Reynolds - a83924@alunos.uminho.pt

Inês Barreira Marques - a84913@alunos.uminho.pt

Rui Filipe Ribeiro Freitas - pg47639@alunos.uminho.pt

Tiago João Pereira Ferreira - pg47692@alunos.uminho.pt

Índice

1	Introdução	3
2	Fundamentos	4
2.1	Familiarização com o ambiente Cisco Modelling Labs	4
3	Desenvolvimento	5
3.1	Topologia	5
3.2	Reconfiguração do protocolo OSPF	7
3.3	Criação e configuração de túneis MPLS	8
3.4	Balanceamento de tráfego MPLS	10
3.5	Políticas de encaminhamento	11
4	Testes e discussão de resultados	12
4.1	Túneis	12
4.2	Políticas de encaminhamento	14
5	Conclusão	16

Lista de Figuras

1	Topologia.	5
2	Exemplo de configuração de uma interface.	7
3	Exemplo de configuração do router OSPF.	8
4	Caminho dos túneis.	9
5	Criação e configuração do túnel 4.	9
6	Comando show ip route para o router 5.	10
7	Políticas de encaminhamento.	11
8	Informações do túnel 2.	12
9	Informações do túnel 4.	13
10	Comando show ip route para o endereço IP 10.0.1.2.	13
11	Servidor TCP.	14
12	Cliente TCP.	14
13	Servidor UDP.	14
14	Cliente UDP.	14
15	Captura de tráfego TCP.	15
16	Captura de tráfego UDP.	15

Lista de Tabelas

1	Atribuição de Endereços IP	6
2	Largura de Banda entre as ligações	6

1 Introdução

No âmbito da unidade curricular de redes de acesso e núcleo foi proposto o desenvolvimento de uma topologia que usasse a engenharia de tráfego MPLS. É pedido que se configure uma solução simples que permita balancear tráfego de um cliente origem para um cliente destino por 2 caminhos alternativos escolhidos e definidos explicitamente. De modo a realizar este trabalho de forma organizada foi dividido o trabalho em 7 etapas.

A primeira etapa da realização deste trabalho tratou-se da familiarização com o ambiente Cisco Modelling Labs visto ser uma ferramenta nova e de pouco conhecimento por parte do grupo. A segunda etapa consistiu na elaboração da topologia a utilizar, identificando os routers LSR e LER e configurando as várias interfaces da topologia. Na terceira etapa foi configurado o protocolo OSPF de modo a que este passasse a anunciar informação útil para a engenharia de tráfego MPLS. Relativamente à quarta etapa foi necessário definir um sistema final de origem e de destino, ambos fora do domínio MPLS, conectados por 2 caminhos distintos. Na quinta etapa foi forçado o balanceamento de tráfego MPLS entre os 2 percursos LSP com a proporção de tráfego em cada caminho de 50%. Na etapa 6 foi testada a solução desenvolvida e demonstrado o seu correto funcionamento. Quanto à 7ª e última etapa foi proposta uma solução de engenharia de tráfego em que o tráfego HTTP na porta 80 ou 8080 fosse por um percurso e o tráfego UDP por outro. Para além disso foi testado o funcionamento com auxílio da ferramenta *netcat* de modo a introduzir tráfego na rede para controlar o fluxo de pacotes nas interfaces.

2 Fundamentos

2.1 Familiarização com o ambiente Cisco Modelling Labs

De modo a realizar o trabalho, foi necessária uma adaptação inicial à ferramenta Cisco Modelling Labs. Foi necessário identificar as principais características básicas de interfaces Ethernet sendo estas: interfaces Ethernet sobre cobre e interfaces Ethernet sobre fibra óptica.

- **Ethernet sobre Cobre:** Existem 2 categorias básicas de cabo Ethernet: cabo trançado e trançado sólido. O cabo Ethernet trançado tende a funcionar melhor para uso em Desktops. É mais flexível e resiliente do que o cabo ethernet sólido e mais fácil de trabalhar, mas funciona apenas com distâncias curtas. O cabo ethernet sólido destina-se a execuções mais longas em uma posição fixa. No contexto do CML podemos usar os equipamentos CSR 1000V e CAT 8000V que consistem num router virtual de produção em ambientes de *cloud* pública e privada. O CSR 1000v tem desempenho limitado ao encaminhar tráfego. As taxas de transferência alcançadas são 1,6 Mb/s ao passar o tráfego por meio de um dispositivo CSR 1000v e 1,52 Mb/s quando encadeado em dois dispositivos CSR 1000v. O Catalyst 8000V tem desempenho limitado ao encaminhar o tráfego. As taxas de transferência alcançadas são 11,1 Mbits/s ao passar o tráfego por meio de um dispositivo Catalyst 8000V e 10,8 Mbits/s quando encadeado em dois dispositivos Catalyst 8000V. Ambos os equipamentos podem ser suscetíveis a aplicações sobre fios de cobre devido aos seus baixos níveis de transferências de sinal.
- **Ethernet sobre Fibra Ótica:** A Single Mode Fiber é um tipo comum de fibra ótica usada para transmitir em distâncias muito longas. É um dos dois tipos de fibra ótica, sendo o outro Multimode Fiber. Uma SMF é um único fio de fibra de vidro usado para transmitir um único modo ou raio de luz. Esta tecnologia funciona principalmente com os cabos de fibra ótica que conectam dispositivos a uma distância de 10 km e suporta 10 Mbps. Um equipamento suscetível a esta interface pode ser o equipamentos IOSv que é uma implementação da Cisco IOS que suporta até 16 interfaces GigabitEthernet. O IOSv fornece funcionalidade completa de plano de controle e plano de dados da camada 3. A comutação de camada 2 não é suportada, mas os encapsulamentos de camada 2, como EoMPLS e L2TPv3, são suportados.

3 Desenvolvimento

3.1 Topologia

Na figura 1 é apresentada a topologia proposta para este trabalho prático. Os routers R1 e R5 foram definidos como LER. Este tipo de routers, para além de terem funções de encaminhamento e controlo são também responsáveis pela rotulação de pacotes à entrada do domínio MPLS e pela remoção das etiquetas à saída do domínio, mantendo a semântica de um pacote IP. Os restantes routers foram definidos como LSR em que este tipo de routers tem como objetivo o encaminhamento de pacotes baseados em etiquetas. Sempre que recebe um pacote, o LSR altera a etiqueta e passa o pacote para o próximo LSR até que chegue a um LER.

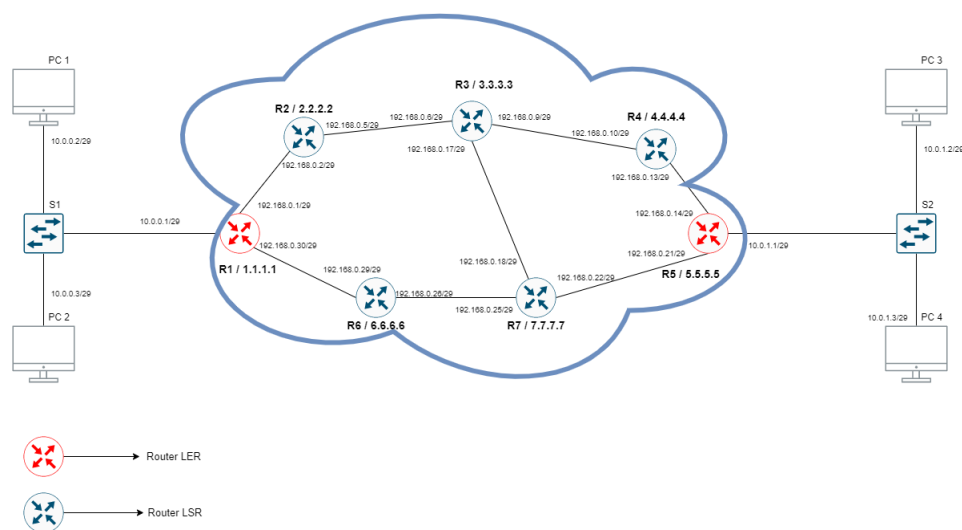


Figura 1: Topologia.

Na tabela abaixo é apresentada uma tabela com os endereços IP atribuídos às ligações entre os routers. Quanto aos endereços das redes locais foram atribuídos os endereços 10.0.0.2/29 e 10.0.0.3/29 à rede da esquerda e os endereços 10.0.1.2/29 e 10.0.1.3/29 à rede da direita.

Ligação	IpRede	Gama de valores	IpDifusão
R1-R2	192.168.0.0	192.168.0.1 - 192.168.0.2	192.168.0.3
R2-R3	192.168.0.4	192.168.0.5 - 192.168.0.6	192.168.0.7
R3-R4	192.168.0.8	192.168.0.9 - 192.168.0.10	192.168.0.11
R4-R5	192.168.0.12	192.168.0.13 - 192.168.0.14	192.168.0.15
R3-R7	192.168.0.16	192.168.0.17 - 192.168.0.18	192.168.0.19
R5-R7	192.168.0.20	192.168.0.21 - 192.168.0.22	192.168.0.23
R7-R6	192.168.0.24	192.168.0.25 - 192.168.0.26	192.168.0.27
R6-R1	192.168.0.28	192.168.0.29 - 192.168.0.30	192.168.0.31

Tabela 1: Atribuição de Endereços IP

Na tabela 2 estão especificadas as larguras de banda das ligações entre os vários componentes da topologia. A largura de banda representa a taxa máxima de transferência de dados possível numa determinada ligação. Esta foi introduzida manualmente no laboratório Cisco Modeling Labs, selecionando a ligação e introduzindo o valor da largura de banda em Kbps.

Ligação	Largura de Banda
R1-R2	1Gbps
R2-R3	1Gbps
R3-R4	2Gbps
R4-R5	2Gbps
R3-R7	1Gbps
R5-R7	2Gbps
R7-R6	1Gbps
R6-R1	1Gbps
R1-S1	1Gbps
S1-PC1	1Gbps
S1-PC2	1Gbps
R5-S2	1Gbps
S2-PC3	1Gbps
S2-PC4	1Gbps

Tabela 2: Largura de Banda entre as ligações

3.2 Reconfiguração do protocolo OSPF

Terminada a configuração do protocolo de estado de ligação OSPF foi necessário realizar uma reconfiguração do mesmo de modo a que este passasse a anunciar informação útil para a engenharia de tráfego MPLS. Para isso realizaram-se um conjunto de comandos nos routers MPLS. Na configuração de todos os routers foi necessário realizar o comando:

- `mpls traffic-eng tunnels`

Posteriormente, foi também necessário configurar todas as interfaces que pudessem vir a pertencer a um túnel. Na figura 2 é apresentada uma configuração exemplo que corresponde à interface Ethernet 0/0 do router R1.



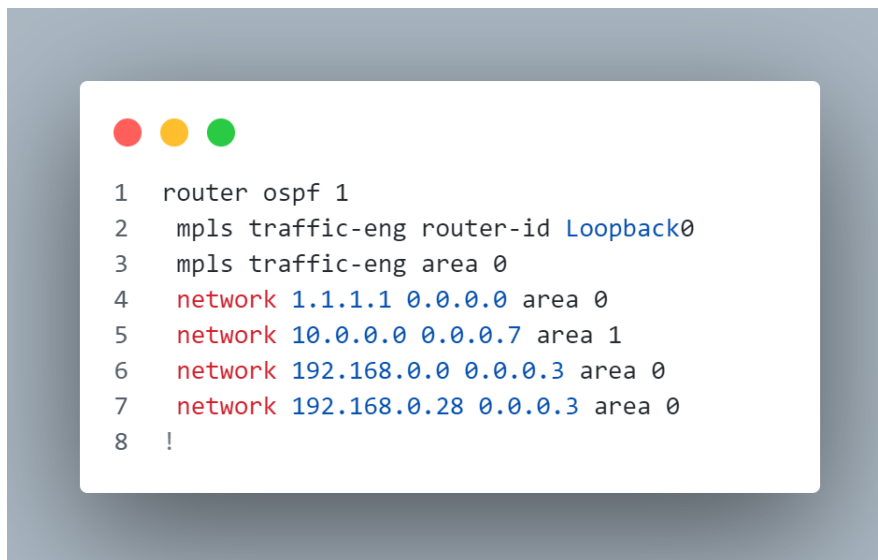
```
1 interface GigabitEthernet0/0
2 ip address 192.168.0.1 255.255.255.252
3 ip access-group 100 in
4 ip access-group 100 out
5 duplex auto
6 speed auto
7 media-type rj45
8 mpls traffic-eng tunnels
9 mpls ip
10 ip rsvp bandwidth 1000000
11 !
```

Figura 2: Exemplo de configuração de uma interface.

Quanto aos comandos `ip access-group` estes serão explicados numa secção mais à frente pois dizem respeito às políticas de encaminhamento de tráfego. Os comandos `mpls traffic-eng tunnels` e o `mpls ip` são definidos em todas as interfaces que pertencem ao domínio MPLS e são usados para a sua configuração. Relativamente ao `ip rsvp bandwidth 1000000` é

onde é definida a largura de banda máxima que pode ser reservada pelo túnel, sendo que neste caso foram reservados 1Gbps.

Depois de terminada a configuração das interfaces, foi necessário configurar os routers OSPF como demonstrado na figura seguinte que corresponde ao router R1.

A screenshot of a terminal window with a light blue background. At the top left, there are three colored circles: red, yellow, and green. Below them, a list of configuration commands is displayed, each preceded by a line number from 1 to 8. The commands are: 1 router ospf 1, 2 mpls traffic-eng router-id Loopback0, 3 mpls traffic-eng area 0, 4 network 1.1.1.1 0.0.0.0 area 0, 5 network 10.0.0.0 0.0.0.7 area 1, 6 network 192.168.0.0 0.0.0.3 area 0, 7 network 192.168.0.28 0.0.0.3 area 0, and 8 !.

```
1 router ospf 1
2 mpls traffic-eng router-id Loopback0
3 mpls traffic-eng area 0
4 network 1.1.1.1 0.0.0.0 area 0
5 network 10.0.0.0 0.0.0.7 area 1
6 network 192.168.0.0 0.0.0.3 area 0
7 network 192.168.0.28 0.0.0.3 area 0
8 !
```

Figura 3: Exemplo de configuração do router OSPF

Na configuração OSPF realizada em todos os túneis foi necessário inserir os primeiros comandos que dizem respeito à configuração do MPLS incluindo a área OSPF e o router-id e depois identificar as redes do router: o endereço loopback, a rede local com IP 10.0.0.0/29 e as redes de ligação com os routers vizinhos 192.168.0.0/30 e 192.168.0.28/30 assim como as áreas a que estes pertecem.

3.3 Criação e configuração de túneis MPLS

Depois de efetuada a configuração do MPLS nos diferentes routers foram implementados quatro túneis, dois com o sistema de origem R1 e sistema de destino R5 e outros dois com sistema de origem R5 e sistema de destino R1, sendo que R1 e R5 são routers do tipo LER.

O primeiro túnel tem como caminho o R5-R4-R3-R2-R1, o segundo túnel R1-R2-R3-R4-R5, o terceiro R5-R7-R6-R1 e o quarto R1-R6-R7-R5. Os diferentes caminhos encontram-se representados na figura seguinte.

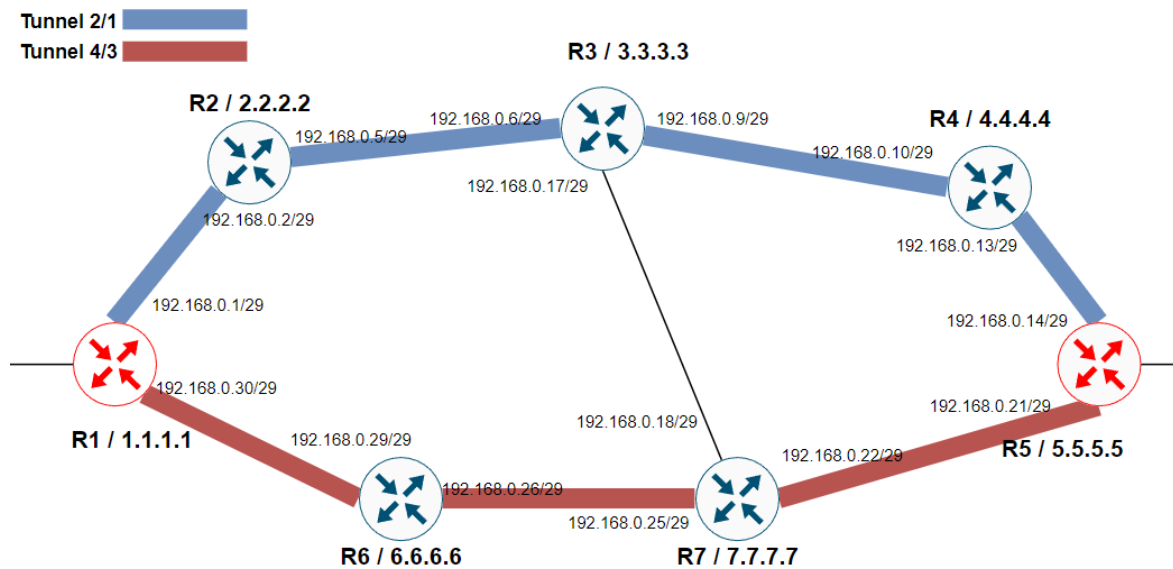


Figura 4: Caminho dos túneis.

A figura seguinte diz respeito à criação e configuração do quarto túnel, que tem como origem o router R1 e destino o router R5.

```

1 interface Tunnel4
2   ip unnumbered Loopback0
3   ip access-group 101 in
4   ip access-group 101 out
5   tunnel mode mpls traffic-eng
6   tunnel destination 5.5.5.5
7   tunnel mpls traffic-eng autoroute announce
8   tunnel mpls traffic-eng priority 1 1
9   tunnel mpls traffic-eng bandwidth 256000
10  tunnel mpls traffic-eng path-option 5 explicit name R1-R5-2
11  tunnel mpls traffic-eng path-option 10 dynamic
12  no routing dynamic
13  !
14  ip explicit-path name R1-R5-2 enable
15    next-address 6.6.6.6
16    next-address 7.7.7.7
17    next-address 5.5.5.5
18  !

```

Figura 5: Criação e configuração do túnel 4.

Dos comandos apresentados na figura anterior é importante salientar os seguintes:

- **ip access-group 101 out** : diz ao túnel que tipo de tráfego pode encaminhar;
- **tunnel destination 5.5.5.5** : indica o destino final do túnel;
- **tunnel mpls traffic-eng autoroure announce** : diz ao router à cabeça para tratar o túnel como um link diretamente ligado à cauda;
- **tunnel mpls traffic-eng priority 1 1** : tem como objetivo indicar a prioridade do túnel, o primeiro valor corresponde ao setup-priority e o segundo a hold-priority;
- **tunnel mpls traffic-eng bandwidth 256000** : define a largura de banda disponível para o túnel;
- **tunnel mpls traffic-eng path-option 5 explicit name R1-R5-2** : este comando é definido como prioritário, quando comparado com o caminho dinâmico, uma vez que possui um valor de path options inferior ao do dinâmico, isto significa que sempre que possível, este é escolhido em relação ao outro. Neste caso o caminho prioritário seria o R1-R5-2, explicitado na figura acima através do comando ip explicit-path;
- **mpls traffic-eng path-option 10 dynamic** : este comando foi realizado com o intuito de fornecer uma caminho alternativo ao caminho do ponto anterior caso este por algum motivo não esteja operacional.

3.4 Balanceamento de tráfego MPLS

Com os túneis criados foi necessário balancear o tráfego que passa nos túneis. Esse balanceamento foi realizado colocando os atributos setup-priority e hold-priority iguais em ambos os túneis. De modo a comprovar o correto balanceamento de tráfego foi utilizado o comando show ip route para o router 5. Na imagem seguinte pode verificar-se que o *traffic share count* está a 1 em ambos os túneis, o que significa que o balanceamento do tráfego está corretamente implementado.

```
R1#show ip route 5.5.5.5
Routing entry for 5.5.5.5/32
  Known via "ospf 1", distance 110, metric 5, type intra area
  Last update from 5.5.5.5 on Tunnel2, 01:51:33 ago
  Routing Descriptor Blocks:
    5.5.5.5, from 5.5.5.5, 01:51:33 ago, via Tunnel2
      Route metric is 5, traffic share count is 1
    * 5.5.5.5, from 5.5.5.5, 01:51:33 ago, via Tunnel4
      Route metric is 5, traffic share count is 1
```

Figura 6: Comando show ip route para o router 5.

3.5 Políticas de encaminhamento

Conforme pedido no enunciado, foi necessário realizar políticas de encaminhamento para o tráfego gerado na rede. No túnel 2 não pode ser encaminhado tráfego UDP entre as portas 16384 e 32767 e no túnel 4 não pode ser encaminhado tráfego HTTP que use as portas 80 ou 8080.

Para implementar as políticas abordadas no parágrafo anterior foram usadas access lists. Na figura 7 é possível observar a implementação das mesmas.

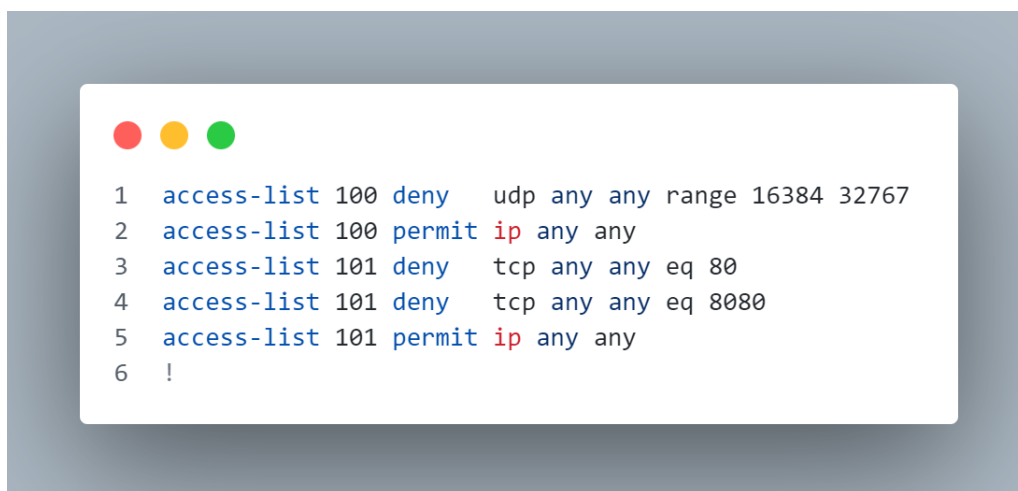


Figura 7: Políticas de encaminhamento.

Como é possível verificar na imagem anterior foram criadas 2 access lists, uma para a interface do túnel superior e outra para a interface do túnel inferior. No túnel 2 que corresponde ao túnel superior, é pretendido que tráfego UDP entre as portas 16384 e 32767 não seja encaminhado. Para isso foi usado o comando "deny udp any any range 16384 32767". Em seguida foi realizado o comando "permit ip any any" com o objetivo de que todo o tráfego que não fosse o anterior pudesse ser encaminhado por esta interface.

Quanto à segunda access list, que diz respeito ao túnel 4, esta foi criada com o objetivo de não permitir o encaminhamento TCP nas portas 80 e 8080 cujo comando é "deny tcp any any eq 80/8080". Nesta interface foi utilizado também o comando "permit ip any any" com o mesmo objetivo do utilizado no túnel 2.

4 Testes e discussão de resultados

4.1 Túneis

Para testar a solução previamente implementada pelo grupo, foi acessado a um dos routers em que os túneis foram criados, (ex:Router R1) e foi escrito o comando "show mpls traffic-eng tunnels", e pode ver-se que os ambos os túneis desse router se encontram "up" e que possuem como caminho prioritário, o caminho explícito definido anteriormente na configuração do mesmo.

Na figura seguinte é apresentado o output do comando "show mpls traffic-eng tunnels" relativo ao túnel 2.

```
Name: R1_t2 (Tunnel2) Destination: 5.5.5.5
Status:
  Admin: up      Oper: up      Path: valid      Signalling: connected
  path option 5, type explicit R1-R5 (Basis for Setup, path weight 4)

Config Parameters:
  Bandwidth: 256000 kbps (Global) Priority: 1 1 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute: enabled LockDown: disabled Loadshare: 256000 bw-based
  auto-bw: disabled

Active Path Option Parameters:
  State: explicit path option 5 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled

InLabel : -
OutLabel : GigabitEthernet0/0, 31
RSVP Signalling Info:
  Src 1.1.1.1, Dst 5.5.5.5, Tun_Id 2, Tun_Instance 20
RSVP Path Info:
  My Address: 192.168.0.1
  Explicit Route: 192.168.0.2 192.168.0.5 192.168.0.6 192.168.0.9
                  192.168.0.10 192.168.0.13 192.168.0.14 5.5.5.5
```

Figura 8: Informações do túnel 2.

Com a utilização do comando "show ip route" é possível obter informações sobre o túnel, como o estado, que neste caso se encontra ativo e funciona, a largura de banda reservada, que é de 256 Mbps, a prioridade que possui os atributos a 1 1. Para além disso podemos observar o caminho realizado pelo túnel em que na nossa topologia corresponde ao caminho superior.

De seguida é apresentado o mesmo comando mas com as informações do túnel 4.

```

Name: R1_t4                                     (Tunnel4) Destination: 5.5.5.5
Status:
  Admin: up          Oper: up          Path: valid          Signalling: connected
  path option 5, type explicit R1-R5-2 (Basis for Setup, path weight 3)
  path option 10, type dynamic

Config Parameters:
  Bandwidth: 256000 kbps (Global) Priority: 1 1 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute: enabled LockDown: disabled Loadshare: 256000 bw-based
  auto-bw: disabled
Active Path Option Parameters:
  State: explicit path option 5 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled

InLabel : -
OutLabel : GigabitEthernet0/1, 19
RSVP Signalling Info:
  Src 1.1.1.1, Dst 5.5.5.5, Tun_Id 4, Tun_Instance 25
RSVP Path Info:
  My Address: 192.168.0.30
  Explicit Route: 192.168.0.29 192.168.0.26 192.168.0.25 192.168.0.22
                  192.168.0.21 5.5.5.5

```

Figura 9: Informações do túnel 4.

Com as informações obtidas anteriormente podemos salientar o estado do túnel que se encontra ativo e é possível observar que existem 2 hipóteses possíveis que o túnel pode utilizar no seu caminho, um caminho explícito e um caminho dinâmico sendo que este último como é de uma prioridade mais baixa apenas é utilizado caso ocorra algum erro no caminho explícito. É também possível observar a largura de banda reservada e o caminho que o túnel está a percorrer sendo que na nossa topologia corresponde ao caminho inferior.

Outro comando que foi utilizado para testar o correto funcionamento dos túneis foi o "show ip route IP_DEST", em que o IP_DEST corresponde ao ip destino desejado. Como exemplo, no R1 foi executado o comando com o ip 10.0.1.2 e foi obtido o seguinte resultado.

```

R1#show ip route 10.0.1.2
Routing entry for 10.0.1.0/29
  Known via "ospf 1", distance 110, metric 4, type inter area
  Last update from 5.5.5.5 on Tunnel4, 00:14:47 ago
  Routing Descriptor Blocks:
    5.5.5.5, from 5.5.5.5, 00:14:47 ago, via Tunnel4
      Route metric is 4, traffic share count is 1
    * 5.5.5.5, from 5.5.5.5, 00:14:47 ago, via Tunnel2
      Route metric is 4, traffic share count is 1

```

Figura 10: Comando show ip route para o endereço IP 10.0.1.2.

Como se pode verificar o router encaminha o tráfego para o ip 10.0.1.2 pelo túneis 2 e 4. Para além disso é possível retirar informações relativamente ao balanceamento de tráfego com ambos os fatores a 1 indicando que o tráfego é distribuído igualmente por ambos.

4.2 Políticas de encaminhamento

Após realizarmos as políticas de encaminhamento foi necessário testar de modo a comprovar o seu funcionamento. Para realizar os testes foi necessário uma ferramenta que colocasse o tráfego pretendido na rede em que a utilizada pelo grupo foi o netcat devido a ser uma ferramenta já conhecida e dominada. Nas figuras seguintes é demonstrado um servidor e um cliente netcat no qual ambos trocam mensagens entre si utilizando o protocolo de encaminhamento especificado assim como a porta.

```
PC3:~$ nc -l -p 8080
ola
tudo bem
sim
e contigo
█
```

Figura 11: Servidor TCP.

```
PC1:~$ nc 10.0.1.2 8080
ola
tudo bem
sim
e contigo
█
```

Figura 12: Cliente TCP.

Como as políticas de encaminhamento foram utilizadas tanto no tráfego TCP como UDP foi necessário fazer uma ligação cliente-servidor também com o protocolo UDP cujo resultado da troca de pacotes é demonstrado de seguida.

```
PC4:~$ nc -l -u -p 17000
ola
tudo bem
sim e contigo
█
```

Figura 13: Servidor UDP.

```
PC2:~$ nc -u 10.0.1.3 17000
ola
tudo bem
sim e contigo
█
```

Figura 14: Cliente UDP.

De modo a observar por onde o tráfego era encaminhado no router R1 foi utilizado a ferramenta *Packet Capture* do CML em ambas as interfaces de saída de modo a observar se o tráfego estava a ser encaminhado corretamente. De seguida pode observar-se uma captura realizada na interface Ethernet 0/0 em que era suposto esta não permitir o tráfego UDP entre as portas 16384 e 32767 e permitir o tráfego TCP.

No.	Time	Source	Destination	Protocol	Length	Info
62	47.993464	10.0.0.2	10.0.1.2	TCP	79	34669 → 8080 [PSH, ACK] Seq=5 Ack=1 Win=64256 Len=9 TSval=4191104873 TSecr=2242153462
63	47.997255	10.0.1.2	10.0.0.2	TCP	66	8080 → 34669 [ACK] Seq=1 Ack=14 Win=65216 Len=0 TSval=2242156692 TSecr=4191104873
64	49.563359	10.0.0.2	10.0.1.2	TCP	74	34669 → 8080 [PSH, ACK] Seq=14 Ack=1 Win=64256 Len=4 TSval=4191106443 TSecr=2242156692
65	49.569725	10.0.1.2	10.0.0.2	TCP	66	8080 → 34669 [ACK] Seq=1 Ack=18 Win=65216 Len=0 TSval=2242158262 TSecr=4191106443
72	52.643788	10.0.0.2	10.0.1.2	TCP	80	34669 → 8080 [PSH, ACK] Seq=18 Ack=1 Win=64256 Len=10 TSval=4191109523 TSecr=2242158262
73	52.648090	10.0.1.2	10.0.0.2	TCP	66	8080 → 34669 [ACK] Seq=1 Ack=28 Win=65216 Len=0 TSval=2242161342 TSecr=4191109523

Figura 15: Captura de tráfego TCP.

O tráfego demonstrado anteriormente foi filtrado para apresentar somente o TCP, no entanto foi observado que nenhum pacote UDP foi transmitido visto que estes foram encaminhados pela interface Ethernet 0/1 em que a captura realizada nesta interface é apresentada na figura seguinte.

No.	Time	Source	Destination	Protocol	Length	Info
93	81.276467	10.0.0.3	10.0.1.3	UDP	60	60584 → 17000 Len=4
99	87.058327	10.0.0.3	10.0.1.3	UDP	60	60584 → 17000 Len=14
105	90.618731	10.0.0.3	10.0.1.3	UDP	60	60584 → 17000 Len=4
140	123.059084	10.0.0.3	10.0.1.3	UDP	60	42728 → 17000 Len=4
158	135.658665	10.0.0.3	10.0.1.3	UDP	60	40557 → 17000 Len=4
181	153.677875	10.0.0.3	10.0.1.3	UDP	60	52029 → 17000 Len=4
196	164.389806	10.0.1.3	10.0.0.3	UDP	51	17000 → 52029 Len=9
201	169.147494	10.0.0.3	10.0.1.3	UDP	60	52029 → 17000 Len=14

Figura 16: Captura de tráfego UDP.

5 Conclusão

O principal objetivo deste trabalho foi a implementação do protocolo MPLS numa topologia, bem como a familiarização com a ferramenta Cisco Modeling Labs. Usando esta ferramenta, foi possível desenvolver a topologia proposta no enunciado, bem como a implementação do protocolo MPLS. Foram criados diferentes túneis com o intuito de encaminhar tráfego através de etiquetas, que é a principal característica do MPLS, ao contrário das redes tradicionais que encaminham o tráfego baseado no ip. Foram criadas também políticas de encaminhamento, em que um túnel fica responsável por encaminhar o tráfego HTTP e outro pelo tráfego UDP.

No final da criação e configuração dos túneis e das diferentes políticas de encaminhamento, foram realizados vários testes de conectividade e performance de modo a comprovar o bom funcionamento da solução desenvolvida pelo grupo. Após a realização dos mesmos, o grupo ficou satisfeito com os resultados obtidos, uma vez que estes foram positivos, uma vez que os túneis estavam “up” e a encaminhar tráfego segundo as políticas estabelecidas.

Com isto, o grupo considera que o trabalho realizado foi um sucesso e que os objetivos propostos no enunciado foram cumpridos com sucesso.