ARQUITETURA DE REDES AVANÇADAS

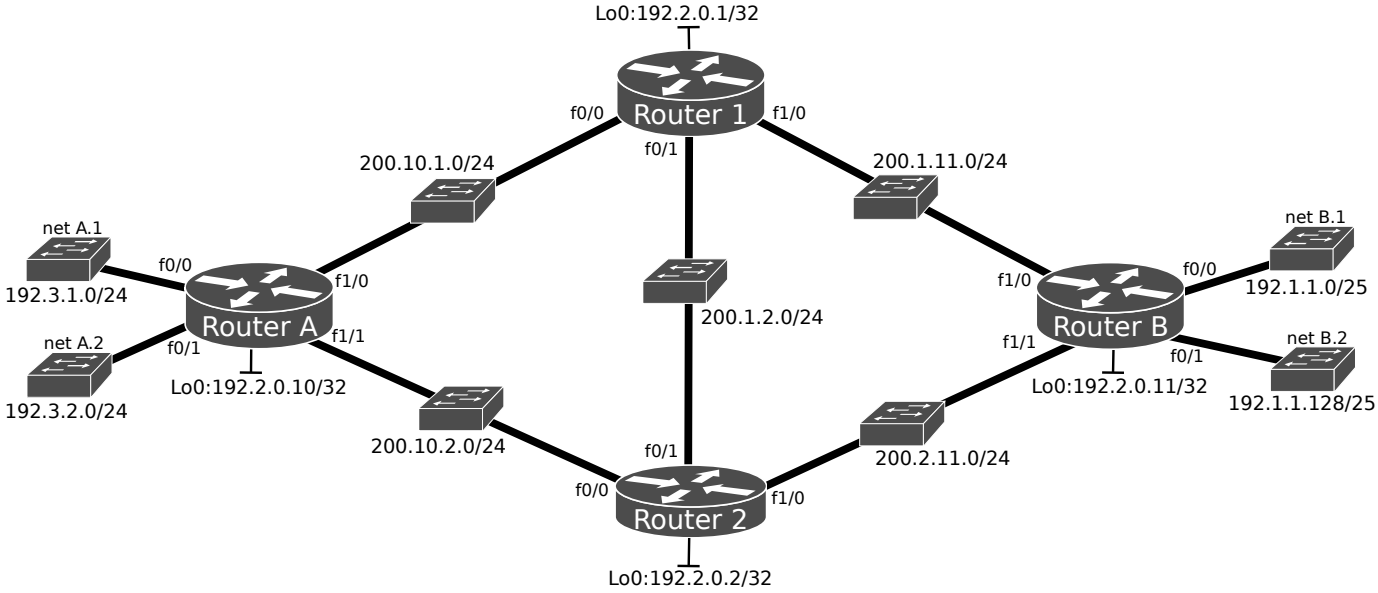
LABORATORY GUIDE

MPLS

Objectives

- LDP protocol
- RSVP-TE protocol
- MPLS basic configuration and traffic engineering support
- MPLS-TE tunnels
- MPLS VPN (MP-BGP and VRF instances)

MPLS with LDP



1. Set up and configure the above depicted network. For all IP addresses not defined in the figure the last byte is equal to the network ID plus the router number/letter (use A=10, B=11). Configure OSPF routing protocol in all interfaces (**including the Loopback interfaces**) considering a single area (`ip ospf 1 area 0`). Verify the correctness of the IPv4 routing tables to assure total connectivity (`show ip route`, `show ip route | sec exclude ^L`).

2. Start a capture of IP packets on links RA-R2 and R1-RB. At each router,

Enable (if not already active) ***Cisco Express Forwarding*** in general configuration mode: *`ip cef`*

Enable **MPLS (LDP)** in general configuration mode and in each physical interface: *`mpls ip`*

Note 1: The LSRs must have (up) Loopback interfaces with an address mask of 32 bits and these interfaces must be reachable with the global IP routing table.

Note 2: When you activate MPLS, LDP is automatically turned on and labels start being advertised (default mode: downstream unsolicited).

Note 3: Cisco's routers have by default MPLS Penultimate Hop Popping (*PHP*) mechanism active.

Analyze the captured packets (UDP and TCP), particularly those belonging to the LDP protocol, in order to see the label advertising process.

Using the command `show mpls ldp neighbor` identify the LDP neighbors and check if all their interfaces are being properly announced.

3. Using the `show ip route` command, check the routing tables at each router.

Use the `show mpls forwarding-table` command to check the MPLS forwarding table, which is the label switching equivalent of the IP routing table for standard IP routing: it contains inbound and outbound labels and descriptions of the packets.

Use the `show mpls ip binding` and `show mpls ldp bindings` commands to see the label bindings associated to each destination (MPLS binding table).

4. Start captures also on links RA-R1 and R2-RB. From Router A ping using source f0/0 (and traceroute) the loopback0, f0/0 and f0/1 interfaces of Router B, and vice-versa. Analyze the ICMP packets, namely the added MPLS header and respective label. Compare the observed labels with the ones observed on Router A and Router B MPLS binding tables and all routers MPLS forwarding tables.

MPLS with RSVP-TE

5.**Disable MPLS (LDP) in general configuration mode and in each physical interface:** ***no mpls ip***

Stop all captures, and start new captures on links RA-R2 and R1-RB.

Enable MPLS (RSVP-TE) in general configuration mode and in each physical interface:

```
mpls traffic-eng tunnels
```

Enable traffic engineering features on **OSPF** in order to announce Multiprotocol Label Switching (MPLS) traffic engineering (TE) link information by entering the following commands on the OSPF configuration mode of all routers:

```
mpls traffic-eng area 0
mpls traffic-eng router-id Loopback 0
```

Use the command `clear ip ospf process` to reinitialize the OSPF process in each router (one at a time).

Note that OSPF floods TE topology and resource information using type 10 Link-State Advertisements (also called Opaque LSAs). Analyze the OSPF packets that were captured.

Using the commands

```
show ip ospf mpls traffic-eng link
show ip ospf database opaque-area
```

verify the TE relevant networks/interfaces being announced and received via OSPF by each router. The *show ip ospf mpls traffic-eng link* command shows the links advertised by OSPF at a given router, including the RSVP characteristics. The *show ip ospf database opaque-area* command shows the OSPF database restricted part corresponding to Type 10 LSAs, showing the database that is used by the MPLS TE process to calculate TE routes for tunnels.

6. Enable RSVP by entering in each physical interface

```
ip rsvp bandwidth 512 512
```

(these are the values of the reservable bandwidth in each interface, total and per flow).

Note that RSVP is used to establish and maintain LSP tunnels based on the calculated path using PATH and RSVP RESV messages. The RSVP protocol specification has been extended so that the RESV messages also distribute label information.

Set up tunnels two **static tunnels** between RA and RB to be used for TE: tunnel 1 and tunnel 2 with explicit paths (next figure).

In order to configure these tunnels, enter the following commands on RouterA:

```
RouterA(config)#interface tunnel 1
RouterA(config-if)#ip unnumbered Loopback0
RouterA(config-if)#tunnel destination 192.2.0.11
RouterA(config-if)#tunnel mode mpls traffic-eng
RouterA(config-if)#tunnel mpls traffic-eng bandwidth 150
            ! Specification of the tunnel bandwidth (Kbit/s)
RouterA(config-if)#tunnel mpls traffic-eng path-option 1 explicit name path1
RouterA(config)#interface tunnel 2
RouterA(config-if)#ip unnumbered Loopback0
RouterA(config-if)#tunnel destination 192.2.0.11
RouterA(config-if)#tunnel mode mpls traffic-eng
RouterA(config-if)#tunnel mpls traffic-eng bandwidth 150
RouterA(config-if)#tunnel mpls traffic-eng path-option 1 explicit name path2
```

```
RouterA(config)#ip explicit-path name path1 enable
RouterA(cfg-ip-expl-path)#next-address 200.10.1.1          !Router1
RouterA(cfg-ip-expl-path)#next-address 200.1.11.11         !RouterB
RouterA(config)#ip explicit-path name path2 enable
RouterA(cfg-ip-expl-path)#next-address 200.10.2.2          !Router2
RouterA(cfg-ip-expl-path)#next-address 200.2.11.11         !RouterB
```

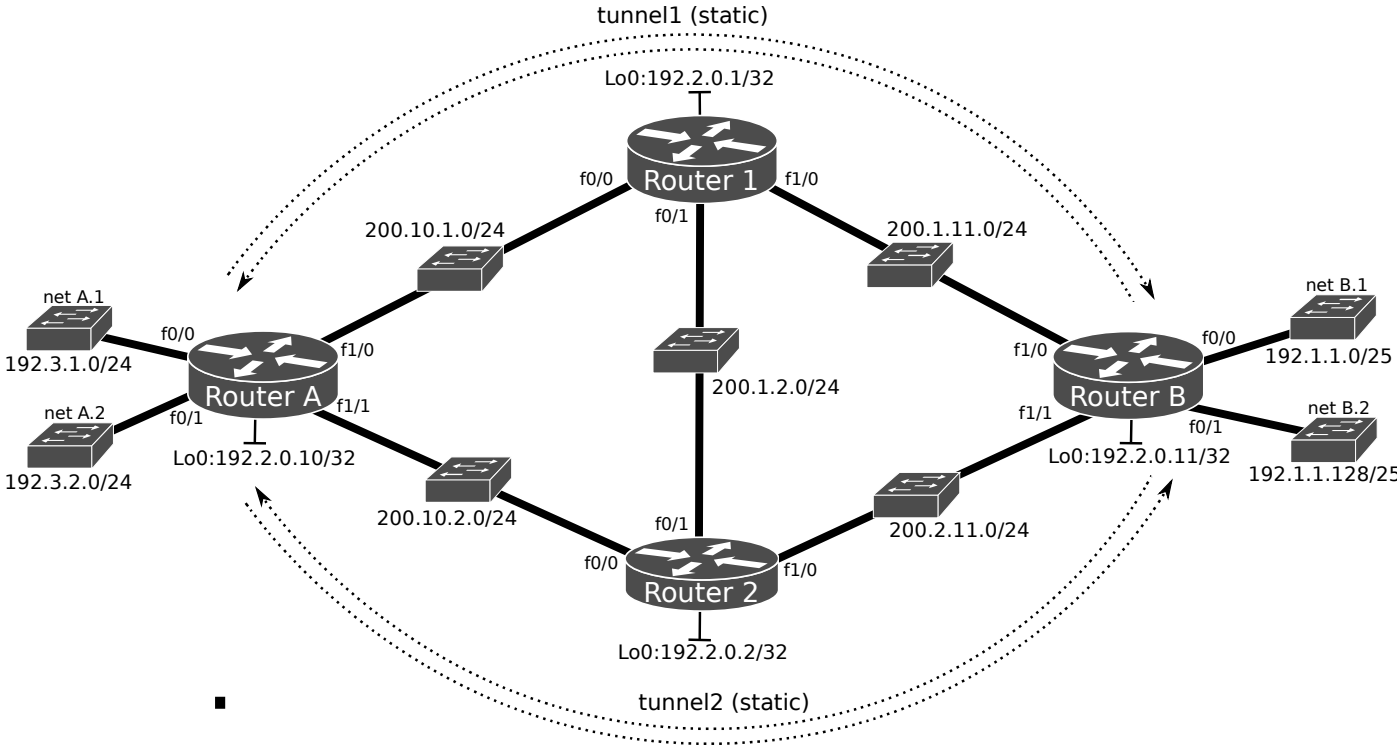
Make similar (symmetric) configurations on RouterB.

Use the

```
show mpls traffic-eng tunnels
```

command (in all routers) to see the tunnels status, paths, and negotiated MPLS labels. Check the routing tables of the different routers and explain their contents. Analyze the RSVP packets that were captured, paying special attention to the TE extensions of the RSVP messages (EXPLICIT ROUTE, LABEL REQUEST, LABEL).

Troubleshooting: If the tunnel status is down due to an error finding a node on the path, use the command `clear ip ospf process` to reinitialize the OSPF process in each router (one at a time).



7. Configure two static routes in Router A to forward traffic to net B.1 via tunnel 1 and traffic to net B.2 via tunnel 2:

```
ip route 192.1.1.0 255.255.255.128 tunnel1
ip route 192.1.1.128 255.255.255.128 tunnel2
```

Configure two static routes in Router B to forward traffic to net A.1 via tunnel 1 and traffic to net A.2 via tunnel 2:

```
ip route 192.3.1.0 255.255.255.0 tunnel1
ip route 192.3.2.0 255.255.255.0 tunnel2
```

Start a capture of packets on links RA-R1, RA-R2, R1-RB and R2-RB. From Router A ping (and traceroute) Router B's f0/0 and f0/1 interfaces and from Router B ping Router A's f0/0 and f0/1 interfaces. Explain the contents of captured ICMP/IP packets and additional MPLS headers.

8. In Routers A and B, remove all static routes and include the following commands in the MPLS tunnels configurations:

```
Router(config)#interface tunnel 1
Router(config-if)# tunnel mpls traffic-eng autoroute announce
Router(config)#interface tunnel 2
Router(config-if)# tunnel mpls traffic-eng autoroute announce
```

Analyze and explain RouterA and RouterB routing tables.

Note that the `tunnel mpls traffic-eng autoroute announce` command announces the presence of a tunnel via routing protocol.

From Router A ping (and traceroute) Router B's f0/0 and f0/1 interfaces and from Router B ping Router A's f0/0 and f0/1 interfaces. Verify that both tunnels are being used (alternately) to transmit data between Routers A and B. Explain the result?

tunnel 1 tem metrica de 3 (tunnel+loopback+rede) tunnel 2 metrica 5 vai preferir o tunnel1

~~9.~~ Now, at Router A enter the following command in tunnel 2:

```
tunnel mpls traffic-eng autoroute metric 5
```

Justify the changes on the routing table of Router A (next-hop for net B.1 and net B.2).

Now, at Router A enter the following command in tunnel 1 and tunnel 2:

tunnel 1 e 2 tem metrica de 22 (tunnel+loopback+rede) então prefere ir por routing

```
tunnel mpls traffic-eng autoroute metric 20
```

Justify the changes on the routing table of Router A (next-hop for net B.1 and net B.2).

~~10.~~ Now, we want to set up two **dynamic tunnels** (tunnel 3 and tunnel 4) to be used for TE between Router A and Router B:

```
RouterA(config)#interface tunnel 3
RouterA(config-if)#ip unnumbered Loopback0
RouterA(config-if)#tunnel destination 192.2.0.11
RouterA(config-if)#tunnel mode mpls traffic-eng
RouterA(config-if)#tunnel mpls traffic-eng autoroute announce
RouterA(config-if)#tunnel mpls traffic-eng bandwidth 150
RouterA(config-if)#tunnel mpls traffic-eng path-option 1 dynamic
...
RouterA(config)#interface tunnel 4
RouterA(config-if)#ip unnumbered Loopback0
RouterA(config-if)#tunnel destination 192.2.0.11
RouterA(config-if)#tunnel mode mpls traffic-eng
RouterA(config-if)#tunnel mpls traffic-eng autoroute announce
RouterA(config-if)#tunnel mpls traffic-eng auto-bw         !bandwidth is automatically adjusted
RouterA(config-if)#tunnel mpls traffic-eng path-option 1 dynamic
```

Make similar (symmetric) configurations on RouterB. Check (`show mpls traffic-eng tunnels`) if the dynamic tunnels have been set up through the shortest path between Routers A and B or not.

~~11.~~ Disable the RA-R1 link (Router A's f1/0 interface: `shutdown`) and check again the status of the different tunnels (`show mpls traffic-eng tunnels, show ip interface brief`). What happened to the static and dynamic tunnels? Explain the advantages (and disadvantages) of dynamic tunnels.

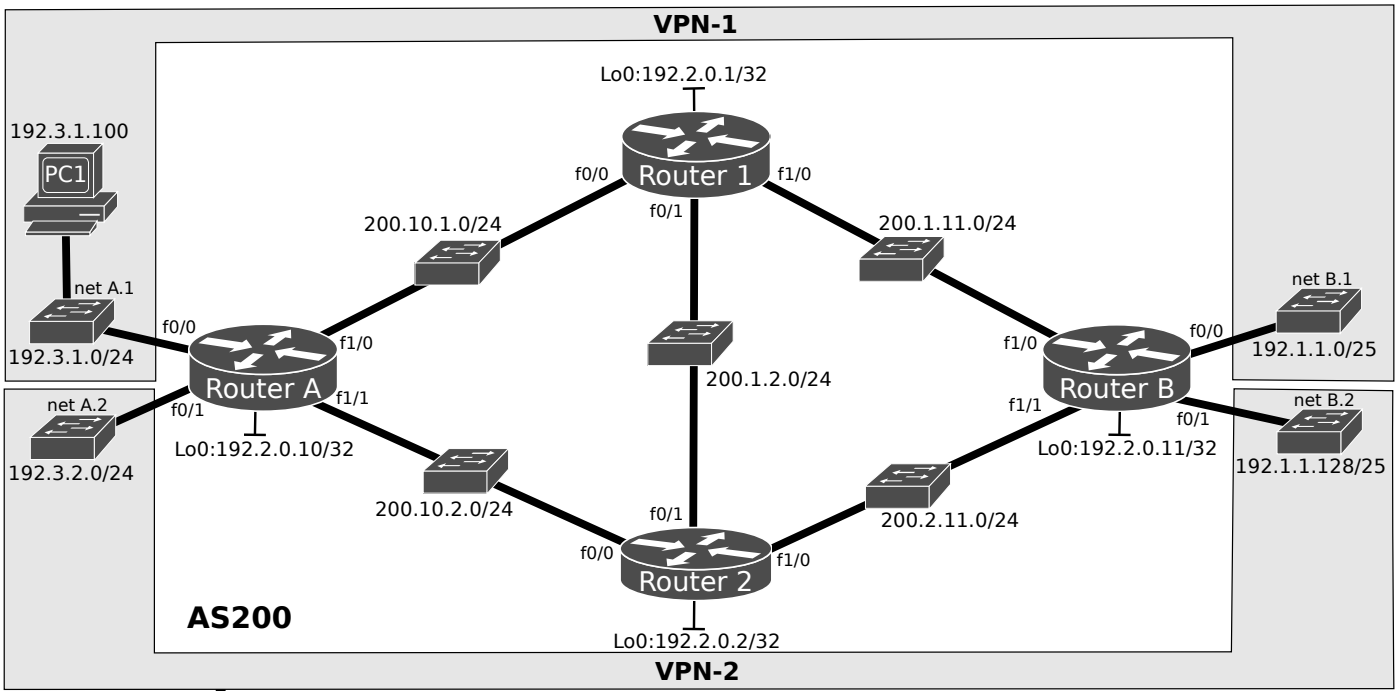
MPLS-VPN (with MP-BGP and VRF)

~~12.~~ **Disable all previously configured tunnels in Routers A and B:**

```
Router(config)#interface range tunnel 1-4
Router(config-if-range)#shutdown
```

Disable relevant MPLS (RSVP-TE) and OSPF commands in all Routers:

```
Router(config)#no mpls traffic-eng tunnels
Router(config)#interface range FastEthernet 0/0-1
Router(config-if-range)#no mpls traffic-eng tunnels
Router(config-if-range)#no ip rsvp bandwidth 512 512
Router(config)#interface range FastEthernet 1/0-1
Router(config-if-range)#no mpls traffic-eng tunnels
Router(config-if-range)#no ip rsvp bandwidth 512 512
Router(config)#router ospf 1
Router(config-router)#no mpls traffic-eng router-id Loopback0
Router(config-router)#no mpls traffic-eng area 0
```



~~13.~~ Assuming that net A.1 and net B.1 belong to VPN-1 and that net A.2 and net B.2 belong to VPN-2, define two VRF instances (one per VPN) with the respective route distinguisher and route targets (the VPNs do no exchange routes – export/import only their one routes). For Router A:

```
RouterA(config)#ip vrf VPN-1
RouterA(config-vrf)#rd 200:1
RouterA(config-vrf)#route-target export 200:1
RouterA(config-vrf)#route-target import 200:1
RouterA(config)#ip vrf VPN-2
RouterA(config-vrf)#rd 200:2
RouterA(config-vrf)#route-target export 200:2
RouterA(config-vrf)#route-target import 200:2
```

Associate each one of the network interfaces to the respective VRF instance (VPN):

```
RouterA(config)#interface FastEthernet0/0
RouterA(config-if)#ip vrf forwarding VPN-1
```

```
RouterA(config-if)#ip address 192.3.1.10 255.255.255.0     !Addresses must be re-configured
RouterA(config-if)#interface FastEthernet0/1
RouterA(config-if)#ip vrf forwarding VPN-2
RouterA(config-if)#ip address 192.3.2.10 255.255.255.0     !Addresses must be re-configured
```

Activate OSPF (`ip ospf 1 area 0`) for all Router interfaces **except** the ones connected to networks net A.* and net B.*.

Enable **MPLS (LDP)** in general configuration mode and in each physical interface (`mpls ip`) **except** the ones connected to networks net A.* and net B.*. Use the `show mpls ip binding` and `show mpls forwarding-table` commands to see the MPLS label bindings and forwarding table.

Start captures on links RA-R1, RA-R2, R1-RB, and R2-RB.

```
RouterA(config)#router bgp 200
RouterA(config-router)#bgp router-id 10.10.10.10           !router-id must be defined
RouterA(config-router)#neighbor 192.2.0.11 remote-as 200
RouterA(config-router)#neighbor 192.2.0.11 update-source Loopback0
!
RouterA(config-router)#address-family vpnv4
RouterA(config-router-af)#neighbor 192.2.0.11 activate
RouterA(config-router-af)#neighbor 192.2.0.11 send-community both
!
RouterA(config-router)#address-family ipv4 vrf VPN-1
RouterA(config-router-af)# redistribute connected
RouterA(config-router)#address-family ipv4 vrf VPN-2
RouterA(config-router-af)#redistribute connected
```

Make similar/symmetric configurations on RouterB.

Analise the global and VRF specific VRF instance routing tables and MP-BGP state/routes:

```
#show ip route
#show ip route vrf VPN-1
#show ip route vrf VPN-2
!
#show ip bgp all
#show ip bgp vpnv4 all          !VPNv4 address family routes
#show ip vrf detail
```

Analyze the captured packets, namely BGP UPDATES (see EXTENDED_COMMUNITIES and MP_REACH_NLRI attributes). Explain how the different routes are associated with a specific VPN/VRF. Use the `show mpls ip binding` and `show mpls forwarding-table` commands to see the MPLS label bindings and forwarding table, associated to each new VPN destination.

From Router A ping Router B's f0/0 and f0/1 interfaces (using the respective VPN/VRF), and vice-versa.

```
RouterA# ping vrf VPN-1 192.1.1.11
RouterA# ping vrf VPN-2 192.1.1.129
!
RouterB# ping vrf VPN-1 192.3.1.10
RouterB# ping vrf VPN-2 192.3.2.10
```

Analyzing the captured ICMP packets (MPLS headers), together with the MPLS binding and forwarding tables, explain how the path and the destined VPN is defined with the (two) MPLS additional headers.

Global and VRF inter-routing

~~14.~~ Configure PC1, start a capture on network 200.10.1.0/24, and test the connectivity from PC1 to Router1's Lo0 interface. Explain the results by analyzing the Ipv4 routing tables on Router A and Router 1:

```
RouterA#show ip route                  !RouterA's global routing table
RouterA#show ip route vrf VPN-1        !RouterA's VRF VPN-1 routing table
Router1#show ip route                  !Router1's global routing table. Doesn't have a VRF!
```

A entrada do 192.2.0.1 não está no VPN-1 routing table

~~15.~~ To add a default route from the VPN-1 to Router1 using the global routing table to find the next-hop, configure on Router A:

```
RouterA(config)# ip route vrf VPN-1 0.0.0.0 0.0.0.0 200.10.1.1 global
```

Perform a ping from PC1 to Router1's Lo0 interface and analyze the captured packets. Re-analyze RouterA's routing tables. Explain the results (lack of connectivity).

~~16.~~ To add a route to network 192.3.1.0/24 from Router A's global routing table and announce it to Router1 (via OSPF redistribution):

```
RouterA(config)#ip route 192.3.1.0 255.255.255.0 FastEthernet0/0
RouterA(config)#router ospf 1
RouterA(config-router)#redistribute static subnets
```

Re-analyze RouterA's and Router1's routing tables. Perform a ping from PC1 to Router1's Lo0 interface and analyze the captured packets. Explain the results (connectivity).

Note: For scenarios where the VRF terminals are not directly connect to a global router, it is possible to define an IP static route defining an output interface and next-hop IP address (VPN inner-router), simultanesly (e.g., `ip route 192.4.1.0 255.255.255.0 FastEthernet0/0 192.3.1.254`).