universidade de aveiro
theoria poiesis praxis

# ARQUITETURA COMUNICAÇÕES

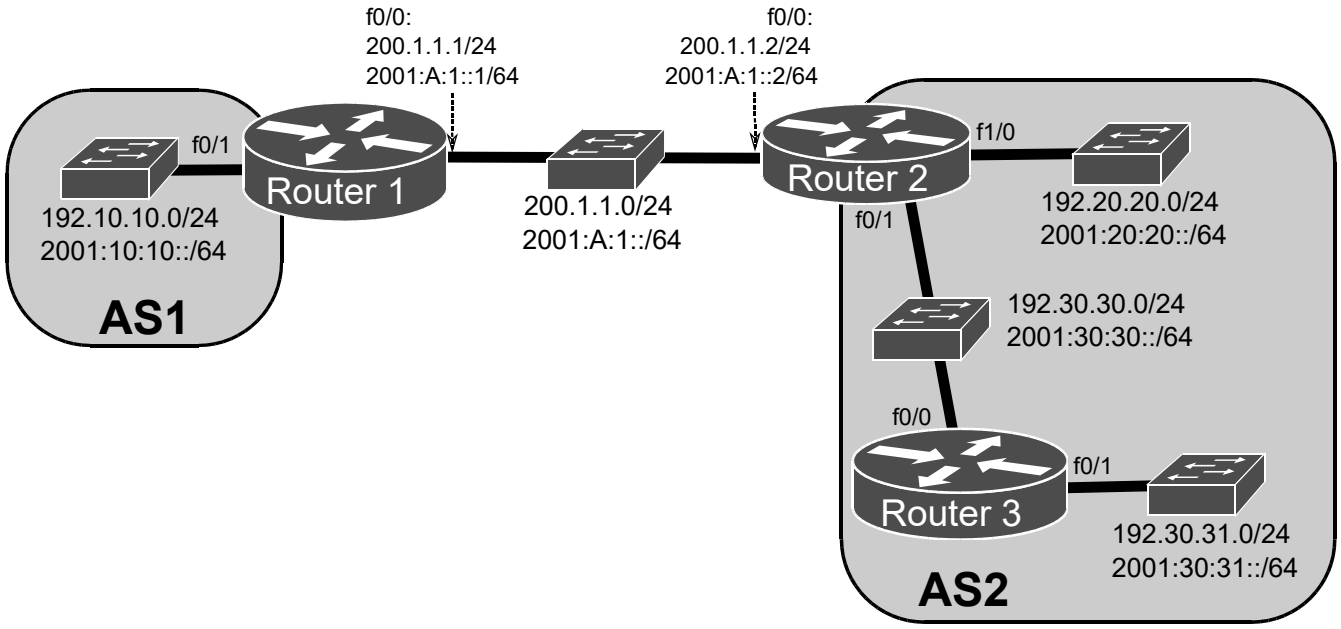
## LABORATORY GUIDE

## BGP AND MPLS

### Objectives

- Introduction to BGP and MPLS

# Introduction to BGP




1. Assemble and configure (only IPv4 addresses) the above depicted network with two Autonomous Systems (AS). Start a packet capture on link R1-R2 (with TCP filter). The internal routing protocol in AS2 is OSPF (network 192.20.20.0 is not included in the process. Router 2 announces a default route.). The AS exchange routes using BGP. Routing configurations:

```
Router1(config)# router bgp 1
Router1(config-router)# neighbor 200.1.1.2 remote-as 2
Router1(config-router)# network 192.10.10.0
---
Router2(config)# router ospf 1
Router2(config-router)# network 192.30.30.0 0.0.0.255 area 0
Router2(config-router)# default-information originate always
Router2(config)# router bgp 2
Router2(config-router)# neighbor 200.1.1.1 remote-as 1
Router2(config-router)# redistribute ospf 1
Router2(config-router)# network 192.20.20.0 !Explicit inclusion. Not in OSPF 1.
---
Router3(config)# router ospf 1
Router3(config-router)# network 192.30.30.0 0.0.0.255 area 0
Router3(config-router)# network 192.30.31.0 0.0.0.255 area 0
```

Understand/explain the purpose off all commands.

Analyze the content of the captured BGP packets (and associated TCP acknowledgments) and identify the BGP packet types, their purposes and periodicity. Analyze the IPv4 routing tables and test full connectivity. Explain how IPv4 routes are announced to remote BGP peers.

2. While capturing packets on link R1-R2, disable Router 3's f0/1 interface (shutdown) to simulate a link failure. Wait a couple of minutes, and enable again the interface (no shutdown) .

Analyze the captured packets, and identify how a network unreachability is announced to a remote BGP peer. And how a newly available network is announced to a remote BGP peer.

3. Change Router 2 BGP configurations in order that networks 192.30.30.0/24 and 192.30.31.0/24 are announced as an aggregate:

```
Router2(config)# router bgp 2
Router2(config-router)# aggregate-address 192.30.30.0 255.255.254.0 summary-only
```

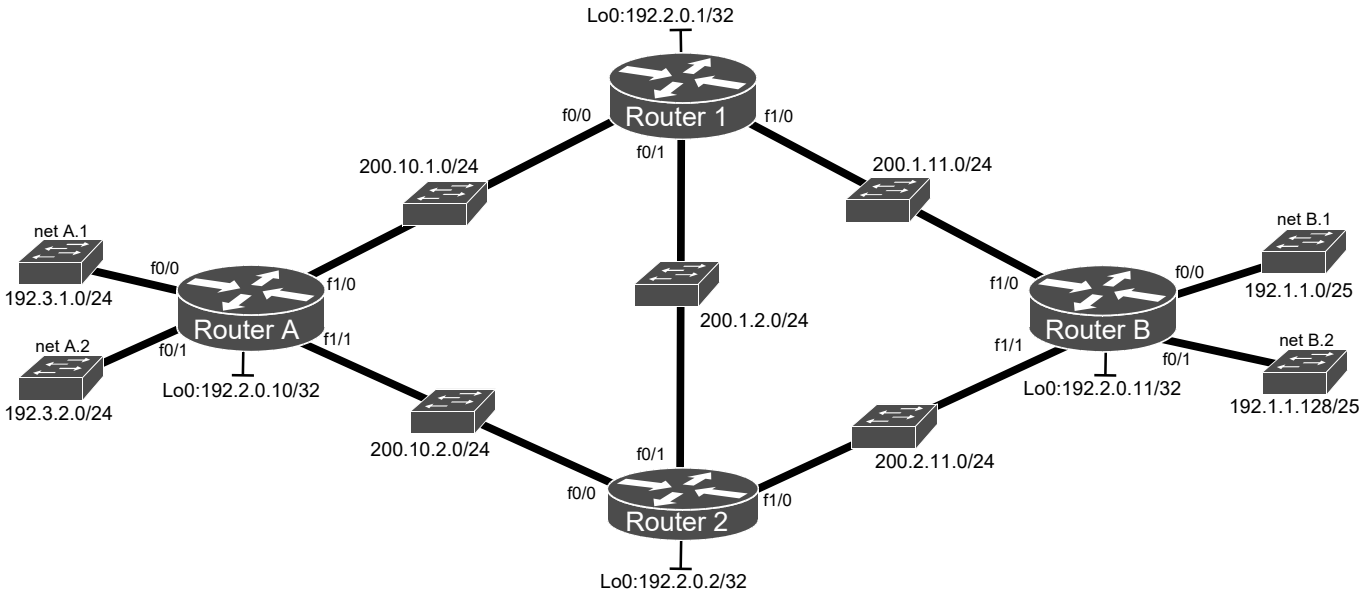
Analyze the routing tables of all routers. Analyze how the network aggregate is announced to the remote BGP peer (identify relevant BGP attributes). Identify the main advantage of network aggregates.

4. While capturing packets on link R1-R2 and with the networks aggregation active, disable Router 3's f0/1 interface (`shutdown`) to simulate a link failure. Wait a couple of minutes, and enable again the interface (`no shutdown`) .

Compare the results with the ones obtained in experiment 2.

5. Simulate now a link failure on Router 2's f0/1 interface. Compare the results and captured packets with the ones obtained in experiments 2 and 4. Identify one disadvantage of using network aggregates in BGP.

**I**




# 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 ph 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
```

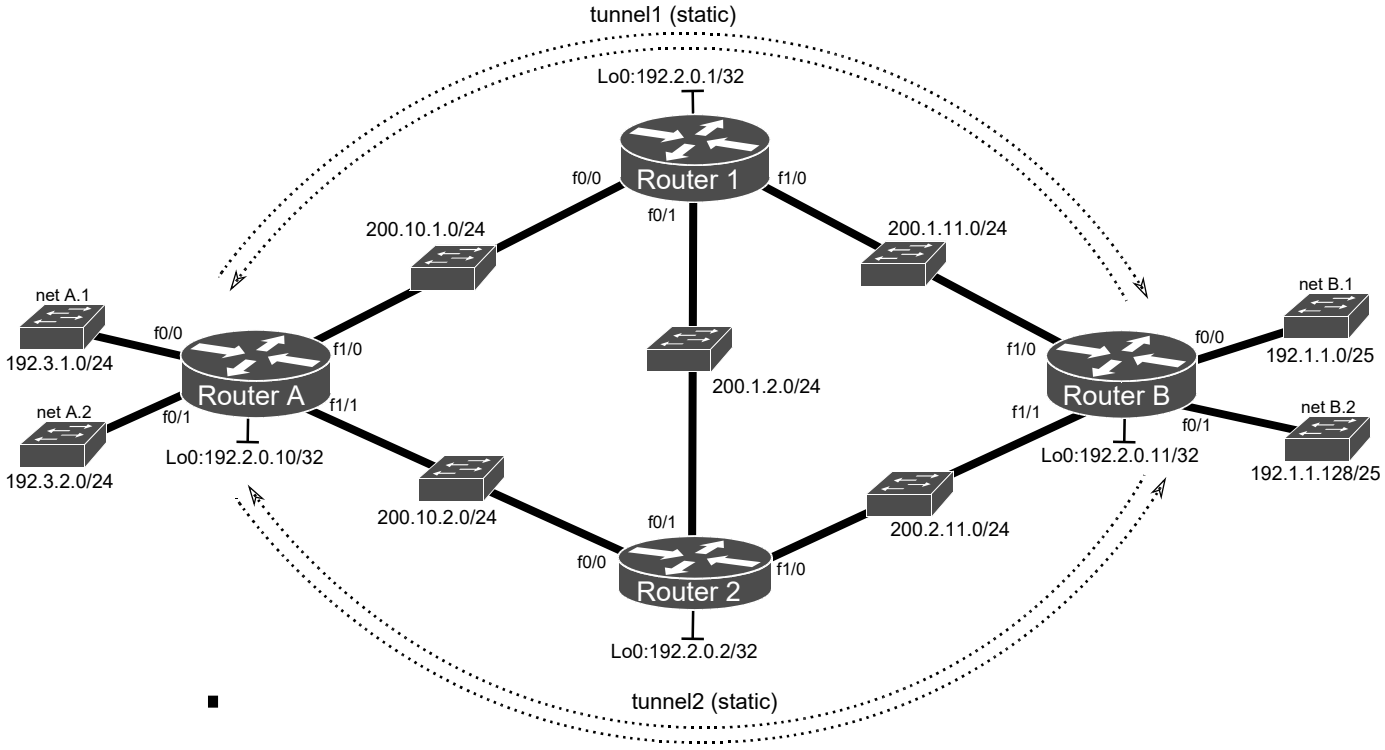
Make similar (symmetric) configurations on RouterB.

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?

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 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.