DEPARTAMENTO DE ELETRÓNICA, TELECOMUNICAÇÕES
E INFORMÁTICA

LICENCIATURA EM ENGENHARIA DE COMPUTADORES E INFORMÁTICA

ANO 2024/2025

REDES DE COMUNICAÇÕES II

LABORATORY GUIDE NO. 4:

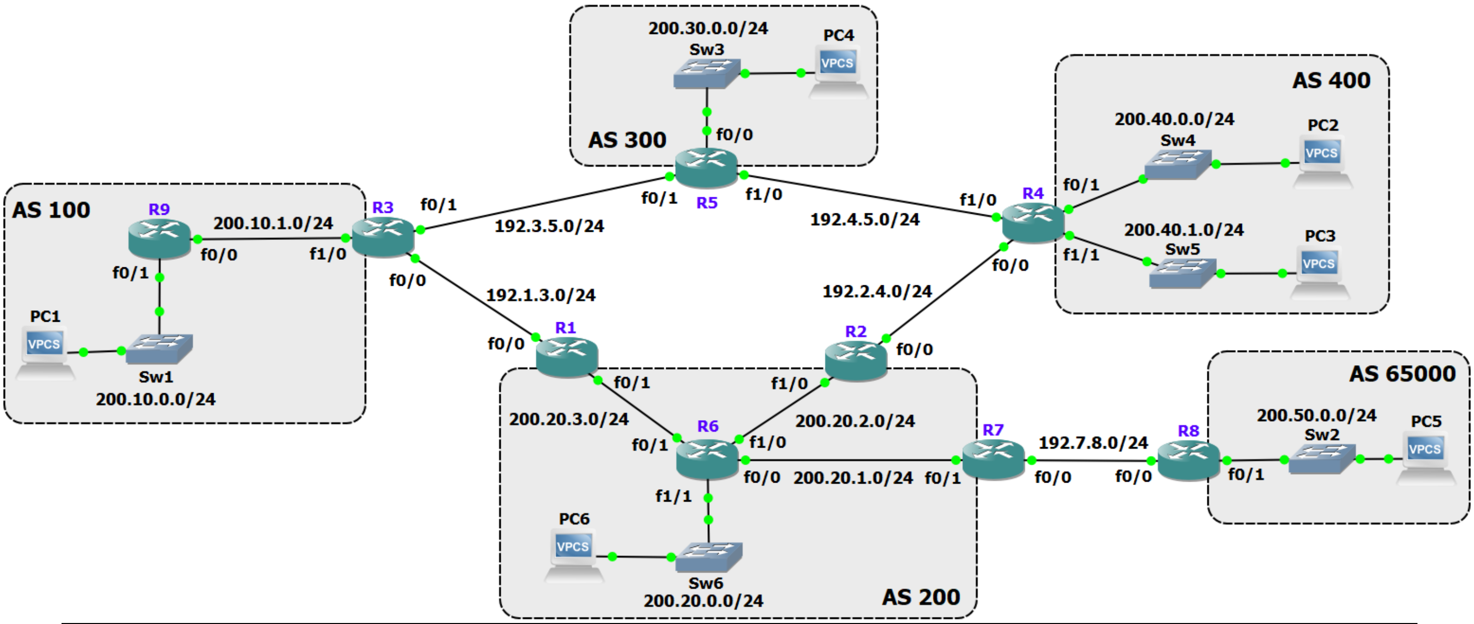
AUTONOMOUS SYSTEMS & BORDER GATEWAY PROTOCOL

In this Laboratory Guide:

- all routers should use the IOS image 15.1(4) of routers 7200 (provided in the elearning page of RC II) and with two network adapters:
  - C7200-IO-2FE in slot 0, providing 2 FastEthernet routing interfaces: `f0/0` and `f0/1`
  - PA-2FE-TX in slot 1, providing 2 FastEthernet routing interfaces: `f1/0` and `f1/1`
- all switches should use the basic Ethernet Switch available in GNS3

1. Initial IPv4 network setup

Create a GNS3 template with all equipment and links of the following network and run the template. On each interface of each router, configure an IPv4 address following the IP network address in the figure using the number of the router name as the host part of the address. On each PC, configure an IPv4 address following the IP network address in the figure (with the host part of the address equal to 100) and the IP address of its default gateway.



Configuration of IP addresses in router R6:

```
R6# configure terminal
R6(config)# interface f0/0
R6(config-if)# ip address 200.20.1.6 255.255.255.0
R6(config-if)# no shutdown
R6(config-if)# interface f0/1
R6(config-if)# ip address 200.20.3.6 255.255.255.0
R6(config-if)# no shutdown
R6(config-if)# interface f1/0
R6(config-if)# ip address 200.20.2.6 255.255.255.0
R6(config-if)# no shutdown
R6(config-if)# interface f1/1
R6(config-if)# ip address 200.20.0.6 255.255.255.0
R6(config-if)# no shutdown
R6(config-if)# end
R6# write
```

Configuration of IP address and default gateway in PC1:

```
PC1> ip 200.10.0.100/24 200.10.0.9
PC1> save
```

1.a. Check the IPv4 routing table of each router. Verify that the routing tables include all directly connected IP networks (if not, there are configuration errors that must be identified and corrected).

Check the IPv4 routing table in router R1, with or without the IP addresses of the (L)inks:
```
R1# show ip route
R1# show ip route | exclude L
```

1.b. Check (through ping) that each PC has connectivity with its default gateway (if not, there are configuration errors that must be identified and corrected).

In the Autonomous Systems (ASs) with more than one router (AS 100 and AS 200), activate the OSPFv2 routing protocol running the command `ip ospf 1 area 0` in all interfaces inside each AS.

1.c. Check the IPv4 routing tables of each router. Verify that the routers of each AS have connectivity to all IP networks of its AS but do not have connectivity to any of the networks of the other ASs.

1.d. Check (through ping) that PC1 has connectivity with the IP address of the AS 100 border router and PC6 has connectivity with the IP address of all AS 200 border routers (if not, there are configuration errors that must be identified and corrected).

2. BGP: Autonomous Systems with one Border Router

First, start a Wireshark capture in the link between routers R4 and R5. Then, configure an eBGP connection between routers R4 and R5 indicating in each peer the networks of its AS.

Configuration in router R4 of the eBGP connection between R4 and R5:
```
R4# configure terminal
R4(config)# router bgp 400
R4(config-router)# neighbor 192.4.5.5 remote-as 300
R4(config-router)# network 200.40.0.0
R4(config-router)# network 200.40.1.0
R4(config-router)# end
R4# write
```

2.a. Check (through ping) that PC4 has connectivity with PC2 and PC3 (if not, the eBGP connection configuration has errors that must be identified and corrected).

2.b. Analyze and justify the BGP messages of the Wireshark capture. In particular, check that:

- in the initial OPEN messages, each router selects its highest IP address as its Router ID, announces its Hold Time (by default, 180 seconds) and its AS number (for validation) and indicates whose capabilities are supported (identify which ones were indicated)
- in the UPDATE messages, each router announces the network prefixes belonging to its AS and each network prefix has the three well-known mandatory attributes (identify them and justify their values) and the optional non-transitive MED attribute [Footnote 1]
- KEEPALIVE messages are exchanged every 60 seconds (why?)

2.c. Analyze the IP routing tables of routers R4 and R5 and justify the new BGP entries. In particular, check that the administrative distance of network prefixes learned by eBGP is 20 and that the cost of the BGP routing paths is the value of the MED attribute received from the other AS.

2.d. Run the command `show ip bgp` in routers R4 and R5 (this command shows the information related with all network prefixes known by BGP on each router). Analize the information shown and check that it is in accordance with what you have observed in the previous **2.b** and **2.c**.

[Footnote 1] This behavior is not imposed by the BGP standard. In this CISCO implementation, when the network prefixes are explicitly indicated in the BGP process, the default behavior is that the router announces them with MED = 0.

Start now a Wireshark capture in the link between routers R3 and R5. Then, configure an eBGP connection between routers R3 and R5 in the following way:

- in router R5, you just need to add the new neighbor in the process `router bgp 300` (following the information in the figure),
- in router R3, instead of indicating the networks of its AS, redistribute the networks from the OSPF internal routing domain.

Configuration in router R3 of the eBGP connection between R3 and R5:

```
R3# configure terminal
R3(config)# router bgp 100
R3(config-router)# neighbor 192.3.5.5 remote-as 300
R3(config-router)# redistribute ospf 1
R3(config-router)# end
R3# write
```

2.e. Analyze the BGP messages of the Wireshark capture. First, check that the content of the OPEN and KEEPALIVE messages is consistent with what you have observed before. Then, justify the BGP UPDATE messages exchanged between R3 and R5. In particular, check that:

- the network prefixes announced by R5 to R3 include the prefixes learned by R5 from R4 (what is the AS_PATH attribute of these prefixes?) and, therefore, R5 assumes by default that its AS is a transit autonomous system
- the UPDATE messages sent by router R3 announce the network prefixes learned from OSPF (and, therefore, the ORIGIN attribute is INCOMPLETE) and are announced with the optional non-transitive MED attribute (which are the values?) [Footnote 2]

2.f. Analyze the IP routing tables of routers R3, R4 and R5 and justify the new BGP entries. In particular, justify the cost of the BGP routing entries in the different routers.

2.g. Run the command `show ip bgp` in routers R3, R4 and R5. Analize the information shown and check that it is in accordance with what you have observed so far.

2.h. Start a capture with Wireshark on the link between routers R3 and R5 to visualize ICMP packets. In router R3, test the connectivity with PC2 running in R3 each of the following two commands:

```
R3# ping 200.40.0.100
R3# ping 200.40.0.100 source f1/0
```

Justify the observed ICMP packets and explain why there is connectivity only when running the second command.

2.i. Test (through ping) the connectivity from PC1 (which belongs to AS 100) to any IP address belonging to AS 300 or AS 400. Check that the output is always the same. Justify why none of these connectivity tests is successful.

Configure R3 to announce itself to all other routers of its AS as the destination of a default OSPF route:

```
R3# configure terminal
R3(config)# router ospf 1
R3(config-router)# default-information originate always
R3(config-router)# end
R3# write
```

2.j. Verify that the routing table of router R9 changed accordingly. Then, repeat the connectivity tests conducted in **2.i** and explain why now all connectivity tests are successful.

[Footnote 2] This behavior is not imposed by the BGP standard. In this CISCO implementation, when the network prefixes are redistributed from an IGP routing protocol, the default behavior is that the router announces them with MED = 0 (for the directly connected networks) or MED = shortest path cost of the IGP protocol (for the not directly connected networks).

3. BGP: Autonomous Systems with multiple Border Routers

Start a Wireshark capture in the link between routers R1 and R3. Then, configure an eBGP connection between routers R1 and R3 redistributing in R1 the internal networks from the OSPF routing domain (in R3, you just need to add the new neighbor to the BGP process).

3.a. Identify and justify the three well-known mandatory attributes of all exchanged BGP UPDATE messages. Check also that R3 assumes by default that its AS is a transit autonomous system.

3.b. Analyze and justify the IP routing table of router R1.

3.c. Run the command `show ip bgp` in router R1. Analize the information shown and check that it is in accordance with what you have configured so far in all routers.

Configure an eBGP connection between routers R2 and R4 redistributing in R2 the internal networks from the OSPF routing domain (in R4, you just need to add the new neighbor to the BGP process).

3.d. Analyze and justify the IP routing tables of routers R1 and R2.

3.e. Run the command `show ip bgp` in router R2. Analize the information shown and check that it is in accordance with what you have configured so far in all routers.

3.f. Run the command `show ip bgp` in router R1 and check that its information is the same as the information observed in **3.c** (why?).

Start a Wireshark capture in the link between routers R1 and R6. Then, configure an iBGP connection between routers R1 and R2 (in both routers, you just need to add the new neighbor to the BGP process).

Addition in router R1 of an iBGP connection to R2:

```
R1# configure terminal
R1(config)# router bgp 200
R1(config-router)# neighbor 200.20.2.2 remote-as 200
R1(config-router)# end
R1# write
```

3.g. Identify and justify the three well-known mandatory attributes of all BGP UPDATE messages exchanged through the iBGP connection. Observe also that both routers:

- announce the IP prefixes learned from the other ASs with the Local Preference attribute (Which value? Why?)
- announce the IP prefixes internal to AS 200 (Why?)

3.h. Analyze the IP routing tables of router R1 and R2. Observe that these routing tables are the same as the ones observed (in **3.d**) before the configuration of the iBGP connection.

3.i. Run the command `show ip bgp` in both routers R1 and R2. Analize the information shown and check that:

- the best path (the entries identified by the symbol '>') to each internal IP prefix (i.e., each prefix belonging to AS 200) starts always in the router, and never though the BGP internal neighbor (why?)
- the best path to each external IP prefix (i.e., each prefix belonging to one of the other ASs) is always selected through the neighbor of the eBGP connection (why?)

Start a Wireshark capture in the link between routers R1 and R6. In R1 and R2, reconfigure the iBGP connection so that each router announces its internal IP address as the Next-Hop attribute to all external IP prefixes.

Configuration in router R1 with the next-hop-self option in the iBGP connection to R2:

```
R1# configure terminal
R1(config)# router bgp 200
```

```
R1(config-router)# neighbor 200.20.2.2 next-hop-self
R1(config-router)# end
R1# write
```

3.j. Analyze the BGP UPDATE messages exchanged in the iBGP connection:

- Check that the Next-Hop attribute of the external IP prefixes has changed accordingly.
- Register the external IP prefixes that were announced by each router as Withdraw Routes (this information is to be used next in **3.l**).

3.k. Analyze the IP routing tables of routers R1 and R2. Justify the routing entry on each router to each external IP prefix (recall from theory the criteria of the BGP path selection).

3.l. Run the command `show ip bgp` in both routers R1 and R2. Analize the information shown and check that it is in accordance with what you have observed in the previous **3.j** and **3.k**.

3.m. Shutdown the interface `f0/1` of router R3 simulating a link failure (<u>do not activate this interface before it is requested to do so</u>). Analyze the IP routing table of router R3. In particular, check that all IP networks belonging to all other ASs are routed in R3 through AS 200 (Why?). The conclusion is that AS 200 is configured as a transit autonomous system.

3.n. Start two Wireshark captures: one on the link R1–R6 and another on link R6–R2). Test (through ping) the connectivity from PC1 (it belongs to AS 100) to PC2 (it belongs to AS 400). Analize the observed ICMP packets and justify the connectivity failure.

One way of solving the problem observed in **3.n** is to configure a tunnel between R1 and R2 and to establish the iBGP connection between them through the tunnel.

So, start by configuring a Tunnel 0 (of type IPv4-IPv4) between interface `f0/1` of router R1 and interface `f1/0` of router R2 and assign the IP network 192.1.2.0/24 to the tunnel (configure the address 192.1.2.1 to the endpoint in R1 and the address 192.1.2.2 to the endpoint in R2).

Configuration of the endpoint of Tunnel 0 on router R1:

```
R1# configure terminal
R1(config)# interface tunnel 0
R1(config-if)# tunnel source 200.20.3.1        (the address of R1-f0/1)
R1(config-if)# tunnel destination 200.20.2.2   (the address of R2-f1/0)
R1(config-if)# tunnel mode ipip
R1(config-if)# ip address 192.1.2.1 255.255.255.0
R1(config-if)# end
R1# write
```

Then, change the iBGP connection between R1 and R2 to run through the configured tunnel.

Change in router R1 the iBGP connection to R2 to run through the tunnel:

```
R1# configure terminal
R1(config)# router bgp 200
R1(config-router)# no neighbor 200.20.2.2 remote-as 200
R1(config-router)# neighbor 192.1.2.2 remote-as 200
R1(config-router)# neighbor 192.1.2.2 next-hop-self
R1(config-router)# end
R1# write
```

3.o. Start two Wireshark captures: one on the link R1–R6 and another on link R6–R2. Check (through ping) that there is connectivity between PC1 and PC2. Analize the observed ICMP packets and justify why there is now connectivity.

3.p. Activate the interface `f0/1` of router R3 (i.e., run `no shutdown` on the interface). Check that the IP routing table of router R3 has changed accordingly.

3.q. Test (through ping) the connectivity from PC6 (which belongs to AS 200) to any IP address belonging to AS 100, 300 or 400. Check that the ping output is always the same. Justify why none of these connectivity tests is successful.

In AS 200, there are two border routers towards ASs 100, 300 and 400. Assume that the operator of AS 200 aims to use preferably R1 to forwards its internal traffic to all external IP networks.

With this aim, configure both R1 and R2 to announce themselves to all other routers of AS 200 as the destination of a default OSPF route. To give preference to R1, the external cost announced by R1 should be lower than the external cost announced by R2:

```
R1# configure terminal
R1(config)# router ospf 1
R1(config-router)# default-information originate always metric 1
R1(config-router)# end
R1# write

...
R2# configure terminal
R2(config)# router ospf 1
R2(config-router)# default-information originate always metric 2
R2(config-router)# end
R2# write
```

3.r. Analyze the IP routing table of router R6 and justify the existing Default Route.

3.s. Start two Wireshark captures: one on the link R1–R6 and another on link R6–R2. Test in PC6 (through ping) the connectivity to PC1 (belongs to AS 100) and then to PC2 (belongs to AS 400). Justify the observed ICMP packets on each capture.

So far, the internal traffic of AS 200 to external networks is routed towards R1 but for some external IP networks, R1 forwards the traffic through R2. In router R1, configure a BGP Local Preference value of 150 (highest than the default value of 100) and reset the BGP routing process:

```
R1# configure terminal
R1(config)# router bgp 200
R1(config-router)# bgp default local-preference 150
R1(config-router)# end
R1# write
R1# clear ip bgp *                         (to reset the BGP process)
```

3.t. Analyze the IP routing tables of routers R1 and R2 and verify that they have changed accordingly.

3.u. Start two Wireshark captures: one on the link R1–R6 and another on link R6–R2. Test in PC6 (through ping) the connectivity to PC2 (belongs to AS 400). Justify the observed ICMP packets on each capture.

Configure the BGP processes of routers R3 and R4 so that they announce their internal networks as a single aggregated prefix.

Configuration of R3:

```
R3# configure terminal
R3(config)# router bgp 100
R3(config-router)# aggregate-address 200.10.0.0 255.255.254.0 summary-only
R3(config-router)# end
R3# write
```

3.v. In routers R1 and R2, analyze the routing tables and the information of the command `show ip bgp`. Verify the impact of the aggregated prefix announcements on this information.

So far, AS 200 is configured as a transit AS. Assume that the operator aims to set up the AS 200 as a non-transit AS. One solution is to use filter-lists. Configure on each ASBR (i.e., R1 and R2) an access-list of type as-path with the regular expression ‘^$’ (it defines only locally originated prefixes) and apply it as an outbound filter-list to its eBGP neighbour.

Configuration of R1:
```
R1# configure terminal
R1(config)# ip as-path access-list 1 permit ^$
R1(config)# router bgp 200
R1(config-router)# neighbor 192.1.3.3 filter-list 1 out
R1(config-router)# end
R1# write
```

3.w. In routers R3 and R4, analyze the routing tables and the information shown by the command `show ip bgp`. Verify in both cases that AS 200 is configured as a non-transit AS.

Eliminate in routers R1 and R2 the last configurations to set up again AS 200 as a transit network.

Elimination of the last configuration of R1:
```
R1# configure terminal
R1(config)# router bgp 200
R1(config-router)# no neighbor 192.1.3.3 filter-list 1 out
R1(config-router)# end
R1# write
```

4. BGP: Private Autonomous Systems

The aim is to set up the required configurations so that AS 200 supports the connectivity of the private AS 65000 to any other AS:

- Configure an eBGP connection between AS 200 and the private AS 65000 in routers R7 and R8. Redistribute the networks from the OSPF internal routing domain in R7 and indicate explicitly the existing IP network in R8.
- Configuring a Tunnel 1 (of type IPv4-IPv4) between interface `f0/1` of router R1 and interface `f0/1` of router R7 and assign the IP network 192.1.7.0/24 to the tunnel (configure the address 192.1.7.1 to the endpoint in R1 and the address 192.1.7.7 to the endpoint in R7).
- Configure an iBGP connection between routers R1 and R7 through Tunnel 1 and with each router announcing its internal IP address as the Next-Hop attribute to all external IP prefixes.
- Configuring a Tunnel 2 (of type IPv4-IPv4) between interface `f1/0` of router R2 and interface `f0/1` of router R7 and assign the IP network 192.2.7.0/24 to the tunnel (configure the address 192.2.7.2 to the endpoint in R2 and the address 192.2.7.7 to the endpoint in R7).
- Configure an iBGP connection between routers R2 and R7 through Tunnel 2 and with each router announcing its internal IP address as the Next-Hop attribute to all external IP prefixes.

4.a. Check (through ping) that PC5 (that belongs to the private AS 65000) has connectivity with all other PCs (if not, the network configuration has errors that must be identified and corrected).

4.b. In router R8, justify the IP routing table and the information shown by the command `show ip bgp`.

4.c. Analyze the IP routing table of router R7 and justify the next hop addresses of the routing entries to the networks of all other ASs.

4.d. Analyze the IP routing table of router R3 and verify that there is an routing entry to the network of the private AS 65000 (the same should happen in any ASBR of any AS).

4.e. Run the command `show ip bgp` in router R3 and check that the AS_PATH attribute of the network 200.50.0.0 includes the AS number 65000 (the same happens in the ASBRs of AS 300 and AS 400).

Since 65000 is a private AS number, it cannot be included in the AS_PATH attributes of the BGP Updates sent by the ASBRs of AS 200 on their eBGP connections. To solve this issue, configure routers R1 and R2 to remove the private AS numbers to the eBGP neighbors.

Configuration of R1:
```
R1# configure terminal
R1(config)# router bgp 200
R1(config-router)# neighbor 192.1.3.3 remove-private-as
R1(config-router)# end
R1# write
```

4.f. Analyze the IP routing table of router R3 and verify that it is equal to the one observed in **4.d**.

4.g. Run the command `show ip bgp` in router R3 and check that the AS_PATH attribute of the network 200.50.0.0 does not include the private AS number. The conclusion is that the network of the private AS is seen by all other ASs as if it belongs to AS 200 (the same happens in the ASBRs of AS 300 and AS 400).

Recall that, with the configurations done so far, the internal routing of AS 200 includes a default route to R1 (configured in **3.r**). Start a Wireshark capture in the link between routers R1 and R6.

4.h. Run a ping command in PC6 (it belongs to AS 200) to PC5 (it belongs to the private AS). Justify the observed ICMP packets and explain why the routing between the two PCs is not optimal.

To solve the problem identified in **4.h**, configure router R7 to announce itself to all other AS 200 routers as the default OSPF destination to the network of the private AS.

Configuration of R7:
```
R7# configure terminal
R7(config)# ip route 200.50.0.0 255.255.255.0 192.7.8.8
R7(config)# router ospf 1
R7(config-router)# redistribute static
R7(config-router)# end
R7# write
```

4.i. Analyze the IP routing table of router R6 and justify the different OSPF external routes in the table.

4.j. Start again a Wireshark capture in the link between routers R1 and R6. Run again a ping command in PC6 to PC5. Justify the observed ICMP packets and explain why now the routing between the two PCs is optimal.

Start two Wireshark captures: one in the link R1–R6 and another in link R2–R6. Start a never-ending ping command from PC5 to PC2 (at PC5, run `ping 200.40.0.100 -t`).

4.k. Justify the ICMP packets observed in the two running captures.

Shutdown router R1 (by stop running it) to simulate a failure of R1. Wait for the reestablishment of the IP connectivity in the never-ending ping from PC5 to PC2. Then, stop (with `Ctrl+C`) the never-ending ping command.

4.l. Analize the ICMP packets observed in the two running Wireshark captures (during the failure recovery). Analyze also the IP routing table of router R7 after the IP connectivity reestablishment. Justify how the global connectivity was reestablished after the failure of R1.