

**“BGP ROUTING CONFIGURATIONS”**LAB Project Nº 2

Report for “*Redes de Internet”* curricular unit

on the Bachelor Course of Informatics and Computer Engineering

**Group 3 authors:**

Diogo Bicho - nº41504

Tomás Pereira - nº49486

Margarida Pascoal - nº50929

**Professor:** Eng. Luís Mata

<< This page was intentionally left blank >>

# Index

[Index 3](#_Toc214979630)

[Figures List 3](#_Toc214979631)

[Tables List 4](#_Toc214979632)

[1. Introduction 5](#_Toc214979633)

[2. Development 5](#_Toc214979634)

[PHASE 1 – IGP CONFIGURATION 5](#_Toc214979635)

[PRACTICAL QUESTIONS 8](#_Toc214979636)

[PHASE 2 - iBGP AND eBGP WITHOUT ROUTING POLICIES 11](#_Toc214979637)

[Practical Questions: 12](#_Toc214979638)

[PHASE 3 - ROUTING POLICIES IMPLEMENTATION 12](#_Toc214979639)

[Practical Questions: 13](#_Toc214979640)

[PHASE 4 - INFLUENCE THE INTERNET ROUTING 13](#_Toc214979641)

[PHASE 5 - SECURITY PRACTICES 14](#_Toc214979642)

[Practical Questions 15](#_Toc214979643)

[3. Conclusion 15](#_Toc214979644)

[4. References 16](#_Toc214979645)

# Figures List

[Figure 1 - Network topology 7](#_Toc211809387)

[Figure 2 - VLAN creation overview 12](#_Toc211809388)

[Figure 3 - RPVST mode enabling 12](#_Toc211809389)

[Figure 4 - VLAN 1 RB reassignment command 15](#_Toc211809390)

[Figure 5 - VLAN 1 RB 15](#_Toc211809391)

[Figure 6 - VLAN 1 RB after configuration 16](#_Toc211809392)

[Figure 7 - VLAN Tag specification 17](#_Toc211809393)

[Figure 8 - Ethernet Frame 18](#_Toc211809394)

[Figure 9 - Subinterfaces configuration 23](#_Toc211809395)

[Figure 10 - Hostname configuration 23](#_Toc211809396)

[Figure 11 - Banner for Router A configuration 23](#_Toc211809397)

[Figure 12 - VLAN configuration on trunk ports 24](#_Toc211809398)

[Figure 13 - Ping test after prunning intended blocked VLANs 26](#_Toc211809399)

[Figure 14 - VLAN brief for Swacesso A 30](#_Toc211809400)

[Figure 15 - Trunked interfaces on switch fabric 31](#_Toc211809401)

[Figure 16 - VLAN configuration Swacesso B 31](#_Toc211809402)

[Figure 17 - Conectivity tests on switch fabric 31](#_Toc211809403)

[Figure 18 - OSPF neighbor Router 1 35](#_Toc211809404)

[Figure 19 - IP routes on Router 1 35](#_Toc211809405)

[Figure 20 - IP protocol on Router 1 36](#_Toc211809406)

[Figure 21 - Router 1 ping to simulated core 36](#_Toc211809407)

# 

# Tables List

[Table 1 - VLAN creation and assignment 7](#_Toc211809409)

[Table 2 - Switch port allocation 9](#_Toc211809410)

[Table 3 - Port Analysis STP Vlan 1 10](#_Toc211809411)

[Table 4 - Port Analysis STP Vlan 32 10](#_Toc211809412)

[Table 5 - Port Analysis STP Vlan 31 11](#_Toc211809413)

[Table 6 - Port Analysis STP Vlan 33 11](#_Toc211809414)

[Table 7 - Port Analysis RSTP Vlan 32 13](#_Toc211809415)

[Table 8 - Port Analysis RSTP Vlan 31 14](#_Toc211809416)

[Table 9 - Port Analysis RSTP Vlan 33 14](#_Toc211809417)

[Table 10 - IP segmentation on PCs 20](#_Toc211809418)

[Table 11- VLAN configuration for switch fabric 27](#_Toc211809419)

# Introduction

This lab report document is focused on the implementation and validation of BGP protocol configurations.

Each phase includes objectives, implementation details, and validation evidence, developed on a GNS3 (Graphical Network Simulator-3) portable project file (.gns3project) which is appended to the comprehension of this report.

# Development

To achieve the requirements for this assignment we used the following environment:

• GNS3 (Graphical Network Simulator-3)

• Devices: Cisco switches/routers

• Connections: Ethernet interfaces between switches/routers

• Host Machines: PCs connected to specific switches for connectivity testing

#### 

## PHASE 1 – IGP CONFIGURATION

On the first stage of this work, we worked on configuring the Interior Gateway Protocol (IGP) the topology would be running on – in this case OSPF. An IGP is connected to Interior routers, i.e. devices living on the same Autonomous System (AS).

We started by setting up the interfaces as per the Table 1 - IP addressing provided on the essay requirement.

The topology consists of 8 AS’s and 16 routers. Each AS has some public IP address to be advertised to other AS’s via eBGP. Each router has its router ID matching the address from its Loopback0.

The image below summarises the architecture of the project:

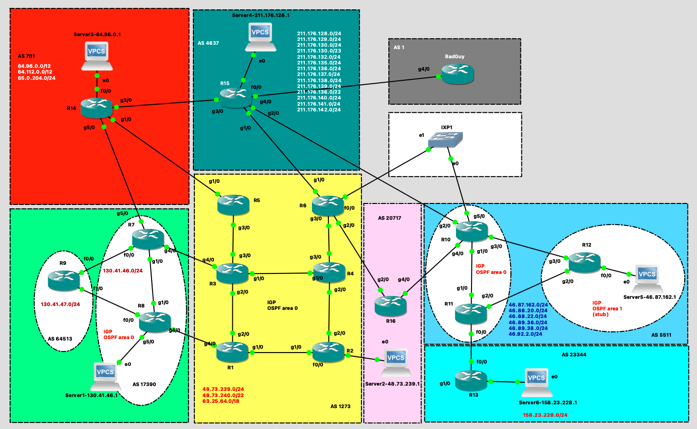
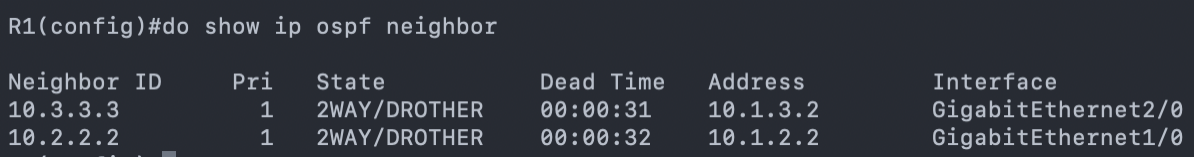


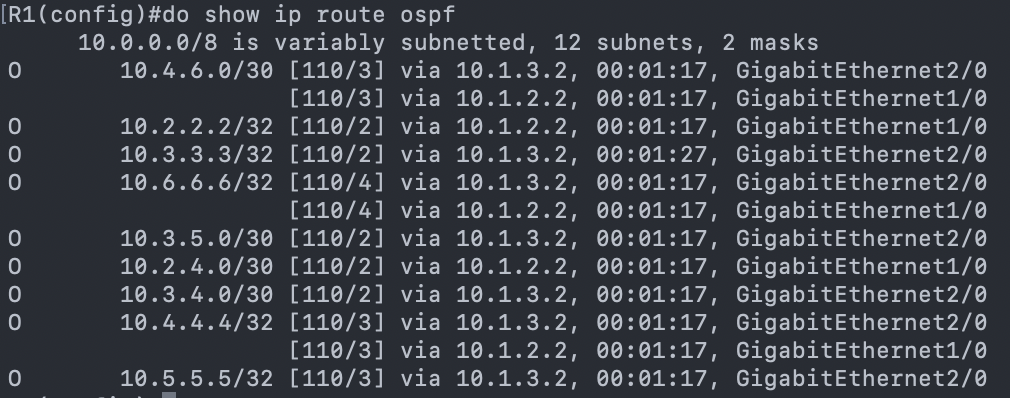
Figure 1 - Network topology

|  |  |  |
| --- | --- | --- |
| **Color Area** | **AS** | **Device** |
| Amarelo | 1273 | R1, R2, R3, R4, R5, R6 |
| Verde | 17390 | R7, R8, Server 1 |
| Verde | 64513 | R9 |
| Azul | 5511 | R10, R11, R12, Server 5 |
| Azul claro | 23344 | R13, Server 6 |
| Vermelho | 701 | R14, Server 3 |
| Verde escuro | 4637 | R15, Server 4 |
| Rosa | 20717 | R16, Server 2 |

* Configure the IP addresses for all the interfaces, as per the Table 1 - IP addressing
* Configure the OSPF as per the design rules on the ASes
* Implement the OSPF mulX-area topology in AS 5511: area 0 and area 1 (stub).
* Test the private infrastructure connecXvity’s inside the ASes
* Test the interfaces connecXvity between the ASes
* Save this project phase as RI\_25\_26\_GROUP<ID>\_phase1

Verified OSPF neighbors successfully on R1:



Checked OSPF routes and loopbacks:

We can see the different routes this Router has on its FIB and that they were “learned” by OSPF protocol due to the letter “O” on the beginning of each line.

On Router 12, in Area 1, a default route (0.0.0.0/0) is present checked with ‘show ip route’:

PROF VAI MUDAR ENUNCIADO POIS N É POSSIVEL ACONTECER

##### PRACTICAL QUESTIONS

1. Create a comprehensive table presenting all the connectivity tests carried out and the respective outcome (*e.g.,* success, failure). You don’t need to provide exhaustive snapshots for all test results. Choose only three example cases, from different ASes, to include in your report and briefly comment on each selected case.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Test** | **Source** | **Destination** | **Path** | **Result** |
| ping | R7 (AS 17390) | R8 (AS 17390) | AS 17390 | Success |
| ping | R8 (AS 17390) | R1 (AS 1273) | Via eBGP only | Failed |
| ping | R1 (AS 1273) | R2 (AS 1273) | AS 1273 | Success |
| ping | R6 (AS 1273) | R1 (AS 1273) | AS 1273 | Success |
| ping | R12 (AS 5511) | Server5 (AS 5511) | AS 5511 | Success |
|  |  |  |  |  |

1. Use the hops://bgp.tools/ to identify the ASes entities involved in the lab topology.

|  |  |  |
| --- | --- | --- |
| **AS** | **Area color** | **Entities** |
| 17390 | Verde | IBM |
| 64513 | Verde | Private ASN |
| 701 | Vermelho | Verison Business |
| 4637 | Verde escuro | Telstra Global |
| 5511 | Azul | Orange S.A. |
| 20717 | Rosa | DE-CIX Marseille Route Servers |
| 23344 | Azul claro | Disney Worldwide Services, Inc. |
| 1 | Cinza | Level 3 Parent, LLC |
| 1273 | Amarelo | Vodafone Group PLC |

1. Explain the concept of an Autonomous System (AS) in the Internet architecture and provide examples associated with the Portuguese Internet ecosystem.

An Autonomous System (AS) contains routers under a single administrative domain, i.e., it is a set of routers and IP networks managed by a single entity. Normally each AS is assigned a globally unique 16-bit or 32-bit AS number (ASN) which is registered by IANA (Internet Assigned Numbers Authority) and distributed by Regional Internet Registries (RIRs).

All routers within an AS typically run the same Interior Gateway Protocol (IGP) (e.g., OSPF, IS-IS, EIGRP) to exchange routing information within a domain. The communication between different AS’s is done thanks to EBGP.

Considering the context of EBGP, there are different types of AS: **Providers**, which give upstream connectivity to **Customers** and **Peers** which normally occurs to exchange routing information without financial compensation, normally between ISPs or an ISP and a customer.

Examples in the Portuguese Internet ecosystem would be: AS3243 – MEO / Altice Portugal, AS12353 – Vodafone Portugal, AS15525 – Claranet Portugal, AS9186 – ONI Telecom, AS20940 – Claranet

1. Classify each AS in the lab project as Tier-1 or Tier-2. For each classification, describe the evidence you find in the lab topology that justifies it.

|  |  |  |  |
| --- | --- | --- | --- |
| **AS** | **Area color** | **Entities** | **Tier** |
| 17390 | Green | IBM | 2 |
| 64513 | Green | Private ASN | 2 |
| 701 | Red | Verison Business | 1 |
| 4637 | Dark green | Telstra Global | 1 |
| 5511 | Blue | Orange S.A. | 1 |
| 20717 | Pink | DE-CIX Marseille Route Servers | 2 (Transit) |
| 23344 | Blue cyan | Disney Worldwide Services, Inc. | 2 |
| 1 | Grey | Level 3 Parent, LLC | 2 |
| 1273 | Yellow | Vodafone Group PLC | 1 |

P REVER!!!

1. Create a table showcasing all the peering relations established in the provided topology.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **AS A** | **Area color** | **AS B** | **Type** | **Evidence** |
| 17390 | Green | 1273 | eBGP | R7/R3 and R8/R1 |
| 17390 | Green | 701 | eBGP | R7/R14 |
| 64513 | Green |  |  |  |
| 701 | Red |  |  |  |
| 4637 | Dark green |  |  |  |
| 5511 | Blue |  |  |  |
| 20717 | Pink |  |  |  |
| 23344 | Blue cyan |  |  |  |
| 1 | Grey |  |  |  |
| 1273 | Yellow |  |  |  |

1. Explain how a Tier-2 benefits from peering instead of buying everything from a Tier-1.

Tier-2 networks:

* Reduce transit costs (sending traffic via Tier-1 is expensive)
* Improve latency (shorter paths via peering)
* Increase redundancy (multiple peer paths)
* Improve performance for local/regional users

Peering = cheaper, faster, more reliable.

1. Identify the neutral public peering interconnections in this lab topology. Elaborate on why they are called neutral and provide examples of real-world implementations of such public interconnections.
2. Explain the role of R12 in AS 5511, and how are its interfaces divided between the OSPF areas involved.

R12 is an ABR connecting Area 0 (backbone) to Area 1 (stub). Interfaces to Area 0 are: R10 link, R11 (both backbone routers) and Loopback0. Area 1 interface is the 46.87.162.0/24 subnet. The purpose of an ABR is to separate backbone from a stub area, advertising a route into Area 0.

An ABR connects routers from multiple areas (including the backbone), and its responsible to exchange routing information.

1. Explain what a stub area is and discuss the resulting advantages and potential limitations. In your discussion, please detail under what conditions would multi-area OSPF be preferred over a single backbone area in real networks.

A stub area is a special type of OSPF area created to reduce the amount of routing information a router must process and store. In a stub area Type 5 LSAs (External routes) are not allowed, instead the ABR (Area Border Router) injects a default route into the area. This is common in small or remote branches because it minimizes the LSDB size and CPU load on routers with limited resources.

Advantages:

* Reduces routing table size- Since no external routes enter the area, routers rely on a single default route for outside destinations.
* Less LSA flooding- No Type 5 LSAs, lower link-state overhead, faster convergence inside the area.
* Lower CPU and memory usage- The LSDB is smaller, and SPF recalculations are simpler.

Limitations:

* No external routes are allowed- If visibility of external prefixes inside the area is needed, a stub area will not work.
* Cannot contain an ASBR- A stub area cannot host a router that redistributes external routes, because that would violate the “no Type 5 LSAs” rule.
* All routers must agree- Every router in the area must be configured as a stub.
* Single-exit expectation- Stub areas work best when there is ONE ABR providing a clean default route. If a stub area has multiple exit points, routing may be sub-optimal.

When multi-Area OSPF is preferred:

Scalability Limits- Large flat (single-area) topologies can cause, Large LSDBs, High CPU use on routers and longer convergence times, Multi-area OSPF reduces these by dividing the network and SPF domains.

* + Geographic Distribution- If the network spans over many remote sites, regions, or countries, dividing them into areas:
    - localizes link failures
    - reduces LSA flooding
    - isolates topology changes to smaller regions.
  + Security and Administrative Separation- Different departments, customers, or service types can be isolated logically.
  + Optimizing Routing for Branch Offices- Branch or remote sites often benefit from:
    - Stub areas (simple connectivity via default route)
    - NSSA areas (when redistribution is needed near the edge)

Limiting the impact of instability- A flapping link in one area does not cause SPF recalculation in all areas, only inside that area.

1. Discuss why the subnet 46.87.162.0/24 was not placed on the backbone area, considering the OSPF design principles.

That subnet was allocated to server 5 (an end user) and the OSPF principles state that Access/edge or end-user networks should be in non-backbone areas.

## PHASE 2 - iBGP AND eBGP WITHOUT ROUTING POLICIES

Border Gateway Protocol (BGP) is a routing protocol to exchange information between different networks. In this case BGP manages communication between the different Autonomous Systems.

On this stage, we configured BGP process for each AS and on the case of external links we established an eBGP session.

Inside AS 1273 we also need iBGP with route-reflectors (R3/R4).

• Inside the AS 1273 you will establish iBGP sessions between the clients and the two route reflectors,

R3 and R4 to avoid the full mesh

• Server subnet public IPs are listed in the internet routing table.

• Implement connectivity between the ASes from any routers using the Lo1 and from any server

|  |  |  |  |
| --- | --- | --- | --- |
| Area AS | Color | Neighbors AS | Neighbor’s Color |
| 701 | Red | 1273 | Yellow |
| 4637 | Dark green |
| 17390 | Light Green |
| 1273 | Yellow | 701 | Red |
| 4637 | Dark green |
| 17390 | Light green |
| 20717 | Pink |
| 4637 | Dark green | 701 | Red |
| 1273 | Yellow |
| 5511 | Blue |
| 1730 | Light green | 1273 | Yellow |
| 701 | Red |
| 20717 | Pink | 1273 | Yellow |
| 5511 | Blue |
| 23344 | Cyan | 5511 | Blue |
| 1 | Grey | 4637 | Dark green |

Table 10 – eBGP neighbors configuration

Testing and validation involved running the following commands:

*show ip bgp*

*show ip bgp summary*

*show ip neighbours*

##### 

##### Practical Questions:

1. How is the BGP next hop reachability solved inside an AS?

Inside an AS, BGP next-hop reachability is provided by the IGP(OSPF, per example).

BGP does not discover next hops on its own, when a router receives a BGP route, it installs it only if the NEXT\_HOP address is reachable in the routing table via the IGP.

Bgp relies entirely on the IGP to make the BGP next-hop reachable, internal routers must have an IGP route to the next-hop IP, or the BGP route will be rejected.

1. Why is it a good practice to use the loopback IP address in the iBGP sessions?

Using a loopback IP address for iBGP sessions is considered best practice because it makes the BGP session stable, reliable, and independent of physical interfaces.

Stability- Loopbacks never go down unless the router goes down.

Redundancy and Resilience- If you use a physical interface for BGP, the session depends on that specific link. With a loopback, any path in the IGP can be used to reach the loopback, If one links fails, traffic reroutes through another path, the BGP session survives internal failures.

Simpler network design- Loopbacks provide a stable, unique identifier for the router.

1. Create and present a detailed table with all the connectivity tests performed using the TCLSH procedure, as previously outlined.
2. In the following Local-RIB table output example, how many routes were installed for the destination 46.87.162.0/24? Justify your response explaining the decision process in BGP.
3. What would have happened in case you didn’t configure the next-hop-self on the iBGP peering definitions? What reasons explain why BGP doesn’t set the next-hop-self as a default setting?

If you do not configure next-hop-self on an iBGP router that receives routes from an eBGP peer:

By default, when a router redistributes a route from eBGP to iBGP, the next hop is not changed. So the next hop remains the external router’s IP.

If the internal routers do not have an IGP route to that external next-hop address, the route will be rejected because “next-hop is not reachable”, will lose connectivity to the advertised prefix and have incomplete routing table. This caused blackholes or missing routes inside the AS.

Why doesn’t BGP use next-hop-self by default, BGP is designed to preserve accurate routing and policy. The original design philosophy of BGP is:

“Do not modify attributes unless explicitly configured by the operator.”

The external next hop carries important information, such as proximity to the destination, exit point selection and routing policies. Automatically overwriting the next hop would hide this information and reduce routing control.

1. How are the route prefixes propagated inside the AS when you have route reflectors configured?

With route reflectors, route prefixes propagate through the RR, which reflects iBGP-learned routes between its clients and peers, eliminating the need for a full iBGP mesh inside the AS.

1. Simulate and explain using Wireshark the BGP messages associated to each BGP state (see: hops://www.ciscopress.com/arXcles/arXcle.asp?p=2756480&seqNum=4).

#### 

## PHASE 3 - ROUTING POLICIES IMPLEMENTATION

#### 

In this phase, was to implement and test the network communication rules for Company A. The following rules were put into place:

• Accounting and Secretariat networks must not communicate with any other internal or external network/VLAN.

• IT network must be able to communicate with the internal VLANs and outside Company A.

• The equipment in the VLAN Network Management of Company A must be able to communicate with each other.

To follow these rules we first started by creating subinterfaces on Router A for interface Fa0/1.

This was sufficient to stop them from communicating with the outside and inside, as stopping router reach they can’t use tagging to communicate outside of themselves.

##### 

##### Practical Questions:

3. Provide short command outputs proving each rule is satisfied/blocked as required

The following ping tests concluded that:

* Accounting cannot communicate with no other device outside of its local network (PC7 example).
* Secretariat cannot communicate outside of its network as well.
* IT can communicate with the router and therefore outside networks.

#### 

## PHASE 4 - INFLUENCE THE INTERNET ROUTING

The main objectives of this phase are to implement the VLANS and addressing plan for Company B, to build the Layer 2 interconnection with the ISP using VLANs 90 and 95, and to ensure redundancy and loop-free operation through the correct configuration of Spanning Tree Protocol.

**3. Explain the chosen RB priorities and observed blocked ports.**

The root bridge priorities were deliberately configured to control STP root election and traffic flow for each VLAN:

SwDistribution-1 was assigned the lowest priority for VLAN 90,making it the root bridge for Company A’s VLAN

SwDistribution-2 was configured with the lowest priority for VLAN 95, making it the root bridge for Company B’s VLAN.

This design ensures that each company’s VLAN has a clearly defined root within the ISP distribution layer, simplifying traffic forwarding and fault recovery.

Observed blocked ports correspond to redundant paths that would otherwise create loops between the distribution and core switches. These ports remain in a blocking or alternate state until a failure occurs on the active link, at which point Rapid STP quickly reconverges to restore connectivity.

## PHASE 5 - SECURITY PRACTICES

The goal of this phase was to establish a stable routing configuration between the routers using static routes, then migrate the topology to a single-area OSPF routing protocol to achieve global connectivity and redundancy across the ISP core.

Additionally, router R2’s Loopback (8.8.8.8/32) was configured to simulate Internet connectivity.

##### Practical Questions

**1. Can corporate PCs ping the ISP router before OSPF? Justify.**

Before OSPF is configured, corporate PCs can only ping the ISP router if proper static routes are manually configured on both the corporate routers and the ISP routers.

If the static routes are missing or incomplete, the packets will reach the nearest router but will not be able to find a valid return path from the ISP back to the company network.

Therefore, without dynamic routing, connectivity is limited to directly connected networks. Full reachability between companies and the ISP core only becomes possible once OSPF dynamically advertises all subnets across routers.

# Conclusion

In conclusion, this project provided practical experience in implementing VLANs, STP/RSTP, inter-VLAN routing, and OSPF in a simulated enterprise environment. Through progressive configuration and testing network segmentation we successfully reinforced our understanding of Layer 2 and Layer 3 operations, troubleshooting, and configuring networks.

# References

[1] BGP Tools. @ONLINE., November 2025. URL <https://bgp.tools/>

[2] Cisco Systems. @ONLINE., 2025. URL <https://www.cisco.com/>

[3] Cisco Press. Routing TCP/IP Volume II (BGP,MPLS, Advanced IGP). Jeff Doyle, 2nd Edition. @ONLINE., 2005. URL <https://www.ciscopress.com/>