

**“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)

Figure 22 - R6 LocPrf 200

# 

# 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 requirements.

The topology consists of 8 AS’s and 16 routers. Each AS has some public IP addresses to be advertised to other AS’s via eBGP, configured on the next section of this work. Each router has also its router ID matching the address from its Loopback0.

The image below summarises the architecture of the project:

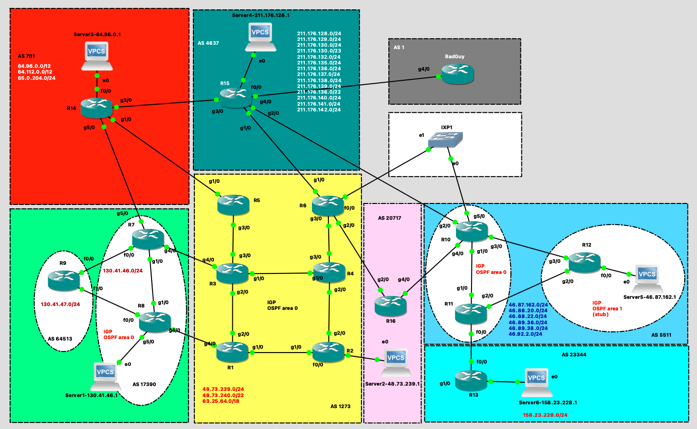


Figure 1 - Network topology

|  |  |  |
| --- | --- | --- |
| **Color Area** | **AS** | **Device** |
| Yellow | 1273 | R1, R2, R3, R4, R5, R6 |
| Green | 17390 | R7, R8, Server 1 |
| Green | 64513 | R9 |
| Blue | 5511 | R10, R11, R12, Server 5 |
| Cyan | 23344 | R13, Server 6 |
| Red | 701 | R14, Server 3 |
| Dark green | 4637 | R15, Server 4 |
| Pink | 20717 | R16, Server 2 |

Table 1 - Topology AS areas and Devices

To configure the IP addresses for all the interfaces of the 16 routers, we created a configuration file for each. We set up their hostname, the interfaces for their Loopback interfaces (0 and 1), the ones for each of their ports and the OSPF network settings.

As an example these were the following OSPF settings for Router 1:

*router ospf 1*

*log-adjacency-changes*

*router-id 10.1.1.1*

*passive-interface Loopback0*

*passive-interface Loopback1*

*network 10.1.1.1 0.0.0.0 area 0*

*network 10.1.2.0 0.0.0.3 area 0*

*network 10.1.3.0 0.0.0.3 area 0*

All routers had only one OSPF area (Backbone Area 0) except for AS 5511 (routers 10,11,12), which needed the backbone (Area 0) and one stub area (Area 1).

On AS 5511, Router 10 and 11 were Area Border Routers and Router 12 was on Area 1. Therefore, all links to R12 were on Area 1 and the rest on Area 0.

Verified OSPF neighbors successfully on R10, R11 and R12:

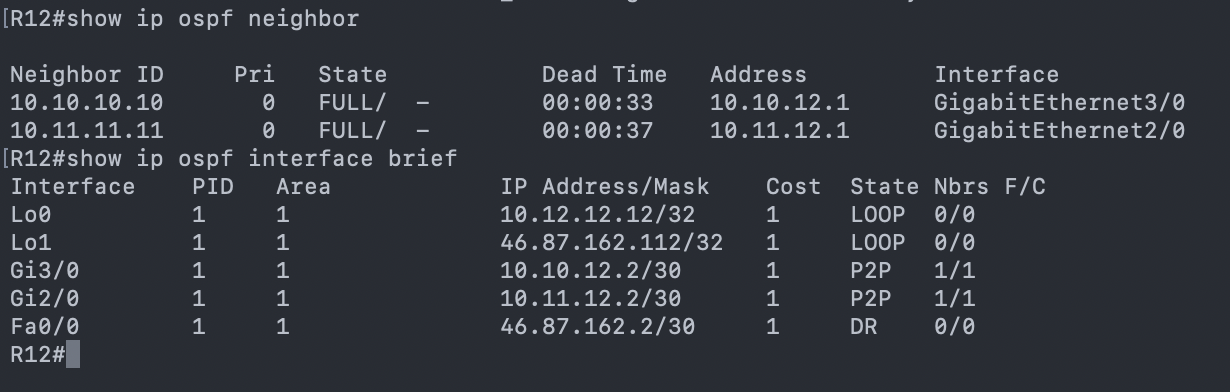


Figure 2 - OSPF neighbors with R12

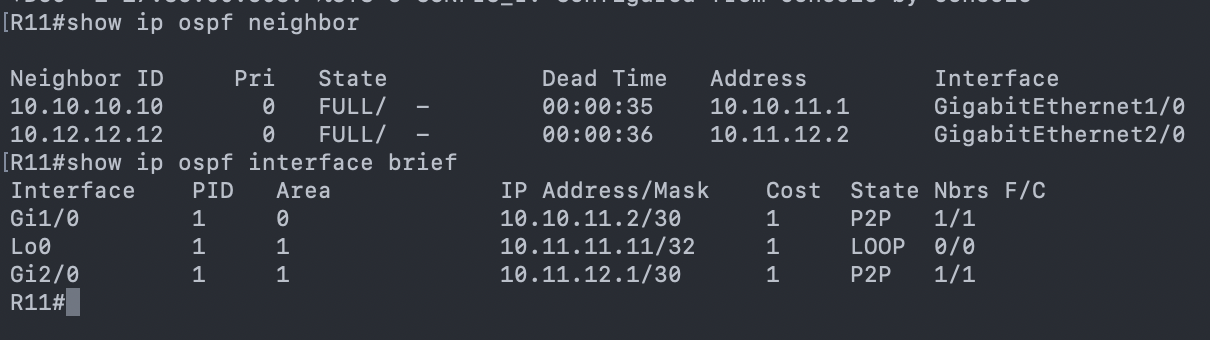


Figure 3 - OSPF neighbors with R11

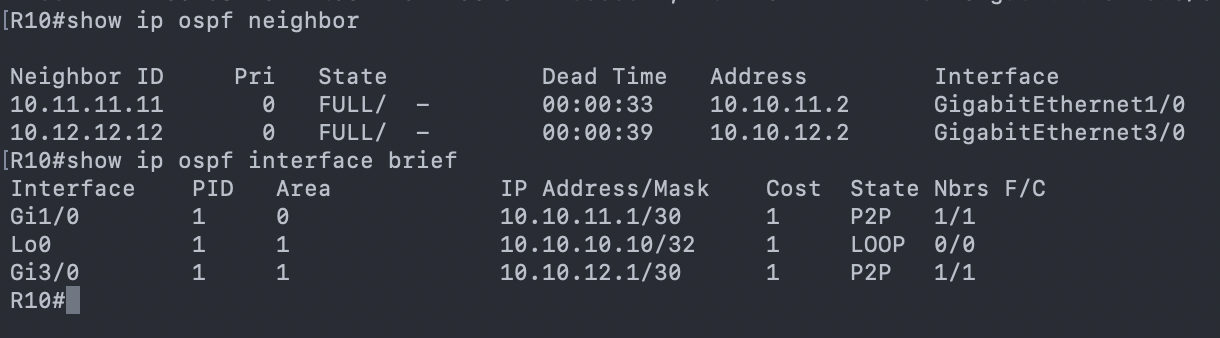


Figure 4 - OSPF neighbors with R10

On R10 we confirmed the R11 and R12 were registered OSPF neighbours. Only the internal link to R11 was in Area 0, the Loopback and the link to R12 were both in Area 1. On R11 we checked the same behaviour, with R10 and R12 as neighbours and on R12 all links were on Area 1 as required.

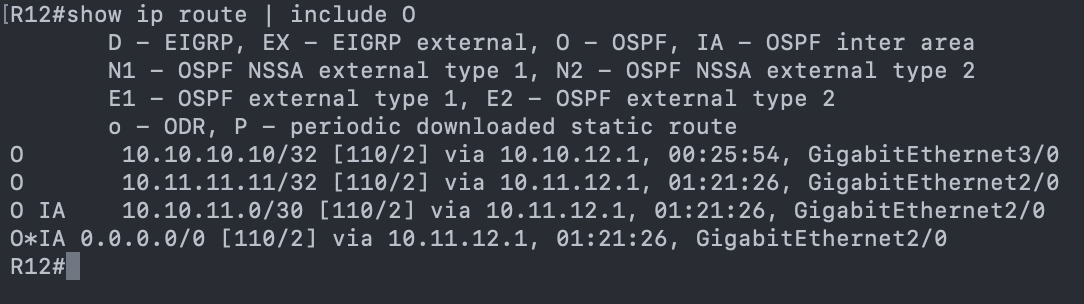


Figure 5 - OSPF routes on R12 FIB

Using the command “show ip route” on R12 (which is located in Area 1), we can see all the routes learned through OSPF.  
Routes marked with “O” are intra-area routes, meaning they were learned from within the same OSPF area (Area 1). In this case, these include the loopback networks of R10 and R11, which are advertised into Area 1.

Routes marked with “O IA” are inter-area routes, meaning they were learned from a different OSPF area. For example, the entry: “O IA 10.10.11.0/30 via 10.11.12.1” shows that R12 is learning the network 10.10.11.0/30 (which belongs to Area 0) through the ABR R11, via its link 10.11.12.1.

Because Area 1 is configured as a stub area, R12 also receives a default route (0.0.0.0/0) generated by the ABR. This forces all traffic from Area 1 that does not match a more specific prefix to be forwarded toward Area 0 (the backbone).

##### 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.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Local Router** | **Local AS** | **Neighbor Router** | **Neighbor AS** | **Peering Type** | **Interface** |
| R14 | AS701 | R5 | AS1273 | eBGP | g1/0-g1/0 |
| R14 | AS701 | R7 | AS17390 | eBGP | g5/0-g5/0 |
| R14 | AS701 | R15 | AS4637 | eBGP | g3/0-g3/0 |
| R7 | AS17390 | R3 | AS1273 | eBGP | g4/0-g4/0 |
| R7 | AS17390 | R8 | AS17390 | iBGP | g1/0-g1/0 |
| R7 | AS17390 | R9 | AS17390 | iBGP | f0/0-f0/0 |
| R8 | AS17390 | R9 | AS17390 | iBGP | f0/0-f1/0 |
| R8 | AS17390 | R1 | AS1273 | eBGP | g4/0-g4/0 |
| R5 | AS1273 | R3 | AS1273 | iBGP | g3/0-g3/0 |
| R3 | AS1273 | R4 | AS1273 | iBGP | g1/0-g1/0 |
| R3 | AS1273 | R1 | AS1273 | iBGP | g2/0-g2/0 |
| R1 | AS1273 | R2 | AS1273 | iBGP | g1/0-g1/0 |
| R2 | AS1273 | R4 | AS1273 | iBGP | g2/0-g2/0 |
| R4 | AS1273 | R6 | AS1273 | iBGP | g3/0-g3/0 |
| R6 | AS1273 | R16 | AS20717 | eBGP | g2/0-g2/0 |
| R6 | AS1273 | R15 | AS4637 | eBGP | g1/0-g1/0 |
| R16 | AS20717 | R10 | AS5511 | eBGP | g4/0-g4/0 |
| R10 | AS5511 | R15 | AS4637 | eBGP | g2/0-g2/0 |
| R10 | AS5511 | R11 | AS5511 | iBGP | g4/0-g1/0 |
| R10 | AS5511 | R12 | AS5511 | iBGP | g3/0-g3/0 |
| R11 | AS5511 | R13 | AS23344 | eBGP | f0/0-f0/0 |
| R11 | AS5511 | R12 | AS5511 | iBGP | g2/0-g2/0 |
| R15 | AS4637 | BadGuy | AS1 | eBGP | f0/0-g4/0 |
| IXP1 | - | R6 | AS1273 | eBGP | e1-f0/0 |
| IXP1 | - | R10 | AS5511 | eBGP | e0-g5/0 |

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.**

In this lab topology, the only neutral public peering interconnection is between R6(AS1273) and R10(AS5511) over the shared IXP1 LAN. Only these routers have direct Layer-2 connections into the IXP1 fabric, making them the only participants of the public peering exchange. The exchange is neutral because it is not owned by either AS, it simply provides a Layer-2 environment where independent Ases can establish eBGP sessions.

It is called a neutral peering point because it is not owned or operated by any of the ASes participating in the exchange. The IXP provides equal, neutral access to all connected networks, allowing them to peer without relying on a transit provider. Neutral IXPs promote fairness, reduce costs, and simplify interconnection policies.

Real-world examples of neutral public interconnection points include AMS-IX(Amsterdam), Linx(London, and DE-CIX Frankfurt. These IXPs are among the largest in the world and function as neutral, shared peering environments for hundreds of networks.

1. **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 appropriate eBGP sessions. On every AS and belonging router we started by registering the static routes with the prefixes to be announced via BGP. We then configured the BGP session to have the ID of the belonging AS and the router ID in question to match the Lo0 interface of said router. Its neighbours were defined identifying the AS to which they belong to and finally the network to be announced via BGP. Next, we present an example of the commands ran for R1:

*enable*

*conf t*

*! static routes*

*ip route 130.41.47.0 255.255.255.0 Null0*

*! BGP configuration*

*router bgp 64513*

*bgp router-id 10.9.9.9*

*no synchronization*

*bgp log-neighbor-changes*

*neighbor 130.41.46.9 remote-as 17390*

*neighbor 130.41.46.9 soft-reconfiguration inbound*

*neighbor 130.41.46.5 remote-as 17390*

*neighbor 130.41.46.5 soft-reconfiguration inbound*

*network 130.41.47.0 mask 255.255.255.0*

*no auto-summary*

*end*

*wr*

This protocol has two variants, iBGP for the links within the same AS and eBGP for the links connecting different AS’s. For AS 1273, and to avoid a full mesh type configuration, we needed to configure 2 route reflectors on R3 and R4 in order to forward external routes to the rest of the routers of the AS (R1, R2, R5 and R6 registered as clients).

Server subnet public IPs were listed in the internet routing table and were announced with the “network” command, together with Lo1 to allow reachability 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 2 – eBGP neighbors configuration

Testing and validation involved running the following commands:

*show ip bgp*

*show ip bgp summary*

*show ip route bgp*

*show ip bgp neighbors 10.6.6.6 received-routes*

##### 

##### 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

#### 

**OBJECTIVES**

* Aggregate IP prefixes when possible and adverXse only the aggregate route on eBGP sessions.
* We should not have adverXsed prefixes longer than /24 in the internet rouXng table
* The internet peering’s should accept a maximum of 50 prefixes
* We should not have private ASs in the middle from an AS path aoribute
* The AS 23344 has only one peering to the internet and want to receive only the default route from the eBGP peering

##### 

##### Practical Questions:

1. Aler applying your prefix-list or route-map, compare the output of show ip bgp and show ip bgp neighbors <ip> adverXsed-routes. Explain the differences you observe referring to the **Adj- RIB-In, Adj-RIB-Out, and Loc-RIB** tables.  
2. Why is the control from the number of prefixes adverXsed to the internet a good pracXce?  
3. What is the **private AS number range** in BGP? Describe some scenarios where using private ASNs can be useful.

4. Assume that you successfully configured prefix filtering. Based on the **BGP path selecXon rules**, explain why R12 selects a specific path for the prefix 65.0.204.0/24. Use the following output as reference (hop://www.cisco.com/en/US/tech/tk365/technologies\_tech\_note09186a0080094431.shtml):

R12#sh ip bgp 65.0.204.0  
BGP routing table entry for 65.0.204.0/24, version 18717 Paths: (2 available, best #2, table Default-IP-Routing-Table)

Advertised to update-groups: 2

4637 701, (received & used)  
10.10.10.10 (metric 2) from 10.10.10.10 (10.10.10.10)

Origin IGP, metric 0, localpref 100, valid, internal 1273 701, (received & used)

48.73.240.17 from 48.73.240.17 (10.6.6.6)  
Origin IGP, localpref 100, valid, external, best

5. Imagine that one of your prefixes was not selected as the best path in your lab. Based on the **BGP decision process**, propose a configuraXon change (e.g., adjusXng local preference, MED, or weight) that would alter the selecXon. JusXfy your answer by showing the relevant command(s) and predicXng the impact on the rouXng table.

#### 

## PHASE 4 - INFLUENCE THE INTERNET ROUTING

The main objective of this phase is to control how traffic flows between Autonomous Systems by manipulating BGP attributes. Unlike previous phases, where routing decisions were determined naturally by IGP metrics or default BGP behaviour, this stage focuses on actively shaping the internet routing path to ensure predictable, stable, and symmetric traffic.

To achieve this, we define polices that influences the BGP decision process both inbound (how our AS selects external routes) and outbound (how other ASes select the routes we advertise). This is done using mechanisms such as local preference, AS-path prepending, prefix-lists, and route-maps. By applying these policies consistently along the entire path, we ensure that AS20717 becomes the preferred transit AS in both directions, creating coherent and predictable routing behaviour across the internet topology.

The selected BGP attributes (Local Preference, AS-Path Prepending, prefix-list and route-maps) were chosen because they are the standard and most effective mechanisms used in real ISP environments to influence routing decisions without breaking BGP fundamental behaviour.

Example:

ip prefix-list FROM\_AS20717 seq 5 permit 0.0.0.0/0 le 32

route-map RM\_PREF\_AS20717\_IN permit 10

match ip address prefix-list FROM\_AS20717

set local-preference 200

router bgp 1273

neigneighbor 48.73.240.22 route-map RM\_PREF\_AS20717\_IN in

neighbor 48.73.240.17 send-community both

To confirm the configuration was right we used show ip bgp to ensure that routes through AS20717 are marked as the best.

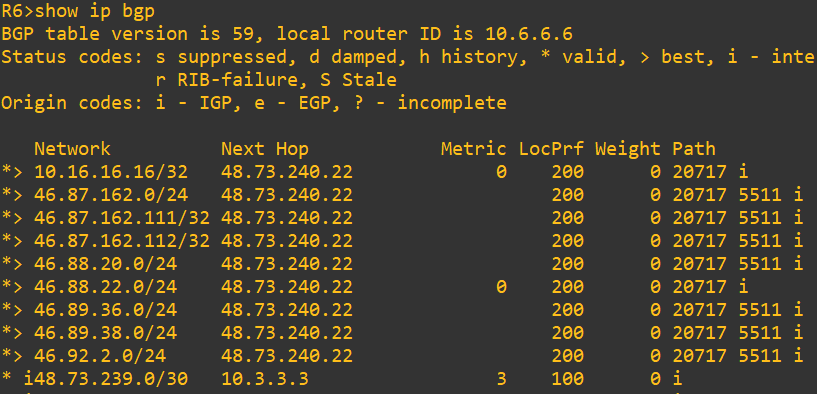


Figure 22 – R6 LocPrf 200

The field LocPrf shows that the route through AS20717 is marked as the best since as a higher preference that the other paths, then Using show ip bgp | include 20717 we can filter just the path that include the AS20717

Uma imagem com texto, captura de ecrã, menu

Os conteúdos gerados por IA podem estar incorretos.

Figure 23 – R6 BGP ips filtered to AS20717

### Using show ip bgp neighbours 48.73.240.22 advertised-routes we see what R6 advertise to R16

### Uma imagem com texto, captura de ecrã, menu, Tipo de letra Os conteúdos gerados por IA podem estar incorretos.

Figure 24 – R6 advertised-routes to R16

Finaly to make sure that the chosen path is the one we want we run traceroute 46.88.20.1 which one of the ips of R10 we see that it has 2 hops the first one belongs to R16 and the last one is the ip we wanted which belongs to AS5511 where R10 is situated.

Uma imagem com texto, captura de ecrã, Tipo de letra

Os conteúdos gerados por IA podem estar incorretos.

Figure 25 – R6 route to R10

##### Practical Questions

**1. Describe in your report the policy options you used to implement the routing policies (include all the details of the configurations (e.g., prefix-list, route-map, etc).**

In order to enforce the required BGP routing policies between AS1273, AS20717 and AS5511, a set of policy-control mechanisms was deployed using prefix-lists, route-maps, and neighbor-specific inbound policy application.

Prefix-lists- were used to match the routes received from specific external ASes, allowing the router to classify which should receive modified BGP attributes.

Defined on R6 and R10:

ip prefix-list FROM\_AS20717 seq 5 permit 0.0.0.0/0 le 32

This prefix-list matches all routes learned from AS20717, enabling us to apply policy to all its prefixes. This ensures every prefix from AS20717 is eligible for the inbound policy.

Route-Maps- was implemented to modify the LOCAL\_PREFERENCE attribute for a specific neighbor.

Defined on R6 and R10:

route-map RM\_PREF\_AS20717\_IN permit 10

match ip address prefix-list FROM\_AS20717

set local-preference 200

This increase LOCAL\_PREF for routes coming from AS20717 to 200 which is higher than the default (100), this makes AS20717 the preferred inbound path within AS1273 and AS5511.

The route-map is applied inbound on the EBGP session with AS20717.

On R6:

neighbor 48.73.240.22 route-map RM\_PREF\_AS20717\_IN in

On R10:

neighbor 46.88.20.2 route-map RM\_PREF\_AS20717\_IN in

This makes all routes learned from AS20717 enter BGP table with LOCAL\_PREF = 200, making these routes preferred over those learned from AS4637

**2.** **Provide command output screenshots that demonstrate the successful application of the configured policies.**

**Uma imagem com texto, captura de ecrã, Tipo de letra

Os conteúdos gerados por IA podem estar incorretos.**

Figure 26 – R10 route to R6

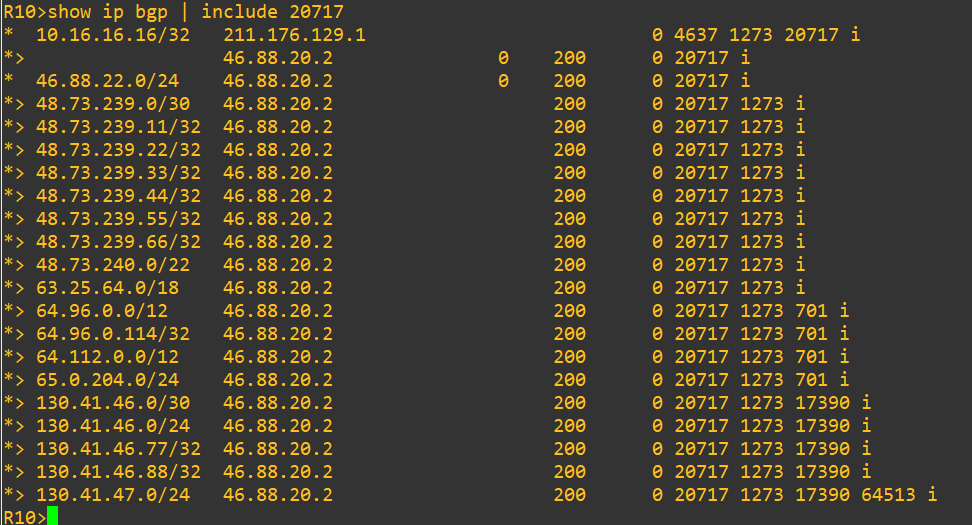
****

Figure 27 – R10 bgp ips

**3. Discuss other alternative to achieve the same results and comment on their relative pros and cons, compared to your implementation.**

One alternative we could have used is AS-PATH prepending, artificially lengthening the AS-PATH the router advertise to make a route look less preferred to external BGP neighbours.

Pros:

* Very simple to implement.
* Only influences inbound traffic (remote AS will prefer other paths).
* Simple to apply on a per-peer basis.

Cons:

* Not deterministic, remote ASes may ignore long AS paths if they use local-pref, making prepend irrelevant.
* Can require multiple prepends or trial-and-error.
* Scales poorly, if many prefixes need different behaviours, prepend rules become messy.

## 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/>