Redes de Internet (RI) 2025-2026

LAB Project Nº 2 -BGP ROUTING CONFIGURATIONS

Contents

1. INTRODUCTION 3

2. PROJECT REPORT STRUCTURE AND GRADING 3

3. LAB ENVIRONMENT SETUP 4

3.1. SIMULATION SOFTWARE 4

3.2. NETWORK TOPOLOGY OVERVIEW 4

3.3. LAB CONFIGURATION GUIDELINES 5

4. EXPERIMENTAL WORK 6

4.1. PHASE 1 - IGP CONFIGURATION 6

4.1.1. OBJECTIVES 6

4.1.2. IMPLEMENTATION 7

4.1.3. TEST AND VALIDATION 7

4.1.4. PRACTICAL QUESTIONS 9

4.2. PHASE 2 - iBGP AND eBGP WITHOUT ROUTING POLICIES 10

4.2.1. OBJECTIVES 10

4.2.2. IMPLEMENTATION 10

4.2.1. TEST AND VALIDATION 11

4.2.2. PRACTICAL QUESTIONS 13

4.3. PHASE 3 - ROUTING POLICIES IMPLEMENTATION 14

4.3.1. OBJECTIVES 14

4.3.2. IMPLEMENTATION 14

4.3.3. TEST AND VALIDATION 14

4.3.4. PRACTICAL QUESTIONS 15

4.4. PHASE 4 - INFLUENCE THE INTERNET ROUTING 16

4.4.1. OBJECTIVES 16

4.4.2. IMPLEMENTATION 16

4.4.3. TEST AND VALIDATION 16

4.4.4. PRACTICAL QUESTIONS 16

4.5. PHASE 5 - SECURITY PRACTICES 17

4.5.1. OBJECTIVES 17

4.5.2. IMPLEMENTATION 17

4.5.3. TESTING AND VALIDATION 18

4.5.4. PRACTICAL QUESTIONS 18

5. APPENDICES 19

5.1. IP ADDRESSING FOR LAB TOPOLOGY 19

5.2. TCLSH (TOOL CONTROL LANGUAGE) SHELL FOR TESTING. 22

1. INTRODUCTION

Welcome to the BGP for Internet Configuration project. In this project, you will build a topology representing an ecosystem of several Autonomous Systems (ASes), representing different Internet Service Providers (ISPs). The BGP is used as exterior gateway protocol, and you will implement the routing between the ASes. You will be guided through creating routing policies, gaining hands-on experience with BGP's flexibility, and learning best practices for designing and applying BGP as an internet protocol. By the end of this lab, you will be able to:

- Follow best practices for implementing BGP both within and between Autonomous Systems (ASes).
- Configure BGP for internet addressing advertisement and control, utilizing BGP's policy features.
- Implement BGP within an Autonomous System using a scalable approach.
- Understand the fundamental security considerations involved in BGP deployment.

BGP is essential for internet networks, and the skills gained with this project apply directly to network engineering. Tackle each task carefully and ask questions if needed.

2. PROJECT REPORT STRUCTURE AND GRADING

Organize your report according to the five main sections of this lab, which are summarized next:

1. IGP Configuration
2. Basic iBGP and eBGP Configuration without Routing Policies
3. Routing Policies Implementation
4. Scalability and Routing Simplification
5. Security Practices

Each section will have a relative weight in the final grading of 15%, 15%, 30%, 20% and 20%, respectively. In each section, follow the corresponding sequence of assigned tasks for implementation and answer carefully the practical questions within each section. Please present your results in a clear and consistent manner to facilitate understanding.

Key report delivery requisites:

- Include an Introduction and Conclusions section
- Include an Index for the report sections
- Provide comprehensive answers to all practical questions
- Ensure clear justifications for each answer, with well-documented reasoning
- Include configuration snapshots, when relevant, to support your responses

The **maximum number of pages in the delivered report is 60**, which includes indexes, introduction, and conclusion. Ensure every group member participates in completing the required tasks and submit your group lab report on Moodle, check the deadlines!

Note: Plagiarism or copying configurations from other students will result in a zero grade for the project.

3. LAB ENVIRONMENT SETUP

This section presents the guidelines for the lab project execution, including the presentation of the lab software to be used and the experimental topology proposed.

3.1. SIMULATION SOFTWARE

This lab utilizes the following environment:

- Simulation Software: GNS3 (Graphical Network Simulator-3)
- Devices: Cisco routers (series 7200)
- Connections: Ethernet interfaces between routers
- Host Machines: PCs connected to specific routers for testing connectivity

To start GNS3 and load the lab you should:

1. Launch GNS3 after ensuring you have properly installed the application.~~;~~
2. Go to File > Import project~~;~~
3. Select the provided .gns3 project file for this lab~~;~~
4. Wait for the project to load and verify that you see 16 routers in the topology.

3.2. NETWORK TOPOLOGY OVERVIEW

In Figure 1, the proposed lab topology is presented, including 8 autonomous systems and 16 routers. The architecture represents a Tier 1 and Tier 2 ASes with their respective downstream clients.

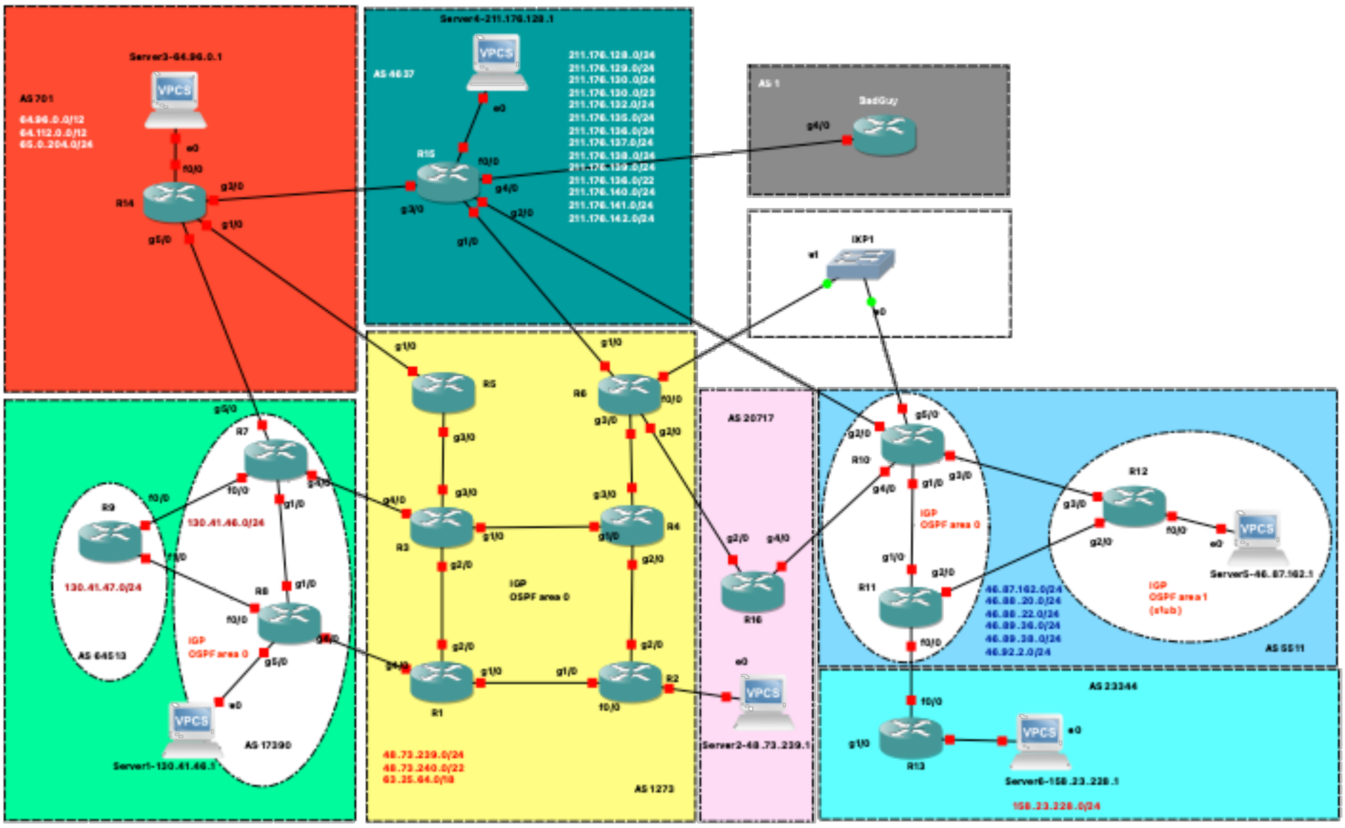


FIGURE 1 - NETWORK TOPOLOGY DIAGRAM

The ASes have some public IP addresses that will be advertised between ASes by eBGP. The AS 1 is intentionally misconfigured to inject Bogon prefixes - IP address ranges that should not be routed on the public internet - into BGP. This serves as an example of poor BGP deployment practices. Except for AS 1 and its direct peers, configure the rest of the network topology following standard BGP engineering practices, such as prefix filtering, route validation, and secure peering agreements.

The owner of AS 17390 decided to implement inside his network a division and attribute a private AS to R9. This part of the network is under testing, and this motivates the reason for the private AS allocation. Private ASs should not be present in the AS path attribute sent to the internet. During this lab implementation, you will need to have this in consideration and avoid propagating a private AS in your advertisements to the internet. For more info on the private AS you can consult the https://datatracker.ietf.org/doc/html/rfc6996.

3.3. LAB CONFIGURATION GUIDELINES

Next, the main guidelines for the project implementation will be provided, starting with general principles and then transitioning to specific instructions that should be observed while configuring the Interior Gateway Protocol (IGP) and the Exterior Gateway Protocol (EGP).

General Engineering and Configuration Rules:

- Save your router configuration often `#write mem`.
- Save your PC configuration often with the `VPCS> save`
- Do not use any static routes, default routes, or policy routing unless otherwise specified.
- The vPCs can have in some situations some abnormal behaviour you may need to individually stop and then start the vPC.
- All the PC's and servers, represents an AS client with a public IP address from the respective AS.
- In case of high CPU on the GNS3, run the idle PC in the several routers from the topology.
- For router configuration, right-click on the router and select "Console" to open the CLI:
    - Enter privileged EXEC mode: `enable`
    - Enter global configuration mode: `configure terminal`

IP Addressing Configuration Guidelines

- All the routers must have a loopback 0 (lo0) with the following convention R<ID> lo0 = 10.<ID>.<ID>.<ID> (ex: R5, loopback 0 = 10.5.5.5/32).
- Configure the router IDs with the IP address from Lo0.
- All the routers must have a loopback 1 (lo1) with a public IP address from the respective AS where is part and will help on the connectivity verifications (see IP addressing from lab topology).
- For all the ethernet interfaces with /30 (point to point) choose the OSPF network type that will allow the fastest convergence on neighbour relations establishment.

IGP Configuration Guidelines

- Use OSPF as the Interior Gateway Protocol (IGP) for this project.
- Use OSPF process id=1 (router ospf 1) in the routers where you configure OSPF.

- OSPF process should not try to establish a neighbour adjacency through interfaces where adjacencies are not expected (ex: loopbacks or connections inter AS).
- You should not send LSAs outside each OSPF domain, example AS 1273 should not send, in any situation, OSPF messages to AS 701, 4637 or 5511.
- AS 5511 adopts a multi-area OSPF design for its internal IGP. Routers R10 and R11 form part of the backbone (Area 0), while R12 acts as an Area Border Router (ABR) linking Area 0 to Area 1. The subnet 46.87.162.0/24, where Server5 is located, is placed in Area 1, which is configured as a **stub area**.
- In AS 5511, R12 advertises a default route into Area 1, instead of propagating all external LSAs. The other public prefixes of AS 5511 — 46.88.20.0/24, 46.88.22.0/24, 46.89.36.0/24, 46.89.38.0/24, and 46.92.2.0/24 — remain visible only in Area 0, where they are distributed among the backbone routers and subsequently exported to the Internet through eBGP.

EGP Configuration Guidelines

- You will use the BGP as the EGP for this project.
- The public IP addresses should not be distributed to the IGP. Your IGP is used to advertise the private IPs from your internal AS infrastructure and allows the resolution from the BGP next hop prefixes. The iBGP sessions will distribute the public IP routes inside the AS.
- You should use the BGP next-hop-self in the iBGP sessions to resolve the next-hop from the BGP prefixes.
- iBGP sessions should use the Lo0 for the session establishment and as BGP router ID.
- On the eBGP neighbor sessions configuration, you should use the IP address from the physical interfaces between the peering routers.
- For scalability in the number of iBGP sessions, inside the AS1273, you should implement a route reflector on R3 and R4.

4. EXPERIMENTAL WORK

This section includes five subsections; each associated to an experimental work phase, each including practical questions that must be thoroughly addressed in the project report.

4.1. PHASE 1 - IGP CONFIGURATION

4.1.1. OBJECTIVES

- 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 multi-area topology in AS 5511: area 0 and area 1 (stub).
- Test the private infrastructure connectivity’s inside the ASes
- Test the interfaces connectivity between the ASes
- Save this project phase as RI_25_26_GROUP<ID>_phase1

4.1.2. IMPLEMENTATION

1. Configure the interfaces on each router according to the Table 1 scheme provided. Here's an example for R1:

```
interface Loopback0
ip address 10.1.1.1 255.255.255.255
```

2. Configure GigabitEthernet interfaces (repeat for each interface):

```
interface GigabitEthernet0/0
ip address 10.1.2.1 255.255.255.252
no shutdown
```

3. Save the configuration:

```
end
write memory
```

Repeat this process for all routers, using the appropriate IP addresses from the topology diagram.

4.1.3. TEST AND VALIDATION

1. VERIFY BASIC CONNECTIVITY

After configuring all interfaces, verify basic connectivity. Example, ping the directly connected interfaces:

```
R1# ping 10.1.2.2
```

2. Repeat similar tests between directly connected routers to ensure basic IP connectivity.
3. Verify the route path between the source and destination to confirm the routing is aligned with the requirements and your expectation

```
R1# traceroute 10.1.2.2
```

4. Implement the OSPF configurations across each AS as the IGP. As an example, the configuration OSPF for the Multi-Area Configuration in AS 5511 is depicted:

- Backbone Routers (R10 and R11 – Area 0 only):

```
router ospf 1
 router-id 10.10.10.10      ! Example for R10, use Loopback0
 network 10.10.11.0 0.0.0.3 area 0
 network 10.10.12.0 0.0.0.3 area 0
 network 10.10.10.10 0.0.0.0 area 0   ! Loopback0
!
router ospf 1
 router-id 10.11.11.11      ! Example for R11
 network 10.10.11.0 0.0.0.3 area 0
 network 10.11.12.0 0.0.0.3 area 0
 network 10.11.11.11 0.0.0.0 area 0   ! Loopback0
```

- Backbone Routers (R10 and R11 - Area 0 only):

```
router ospf 1
```

```
 router-id 10.12.12.12
!
 ! Interfaces toward R10 and R11 (backbone)
 network 10.10.12.0 0.0.0.3 area 0
 network 10.11.12.0 0.0.0.3 area 0
 network 10.12.12.12 0.0.0.0 area 0   ! Loopback0
!
 ! Interface toward Server LAN (46.87.162.0/24)
 network 46.87.162.0 0.0.0.255 area 1
!
 ! Configure Area 1 as stub
 area 1 stub
```

5. On the router in Area 1, verify that a default route (0.0.0.0/0) is present in the OSPF database instead of all external prefixes.

```
R12# show ip ospf database summary
R12# show ip route ospf
```

6. Inside the AS's running the IGP protocol verify the neighbour relations and the interfaces that are part of the process.

```
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.3.3.3          0   FULL/  -        00:00:35    10.1.3.2        GigabitEthernet2/0
10.2.2.2          0   FULL/  -        00:00:30    10.1.2.2        GigabitEthernet1/0
```

```
R1#sh ip ospf interface brief
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Lo0          1     0               10.1.1.1/32        1     LOOP  0/0
Gi2/0        1     0               10.1.3.1/30        1     P2P   1/1
Gi1/0        1     0               10.1.2.1/30        1     P2P   1/1
```

7. Inside the AS's running the IGP you should be able to ping all the internal IPs including the loopback 0 from all the routers inside the AS.

8. Configure the vPC with the respective IP addresses, gateway, name and save.

```
Server1> ip 130.41.46.1/30 130.41.46.2
Server1> save
```

9. SAVE YOUR PROGRESS

Once you've completed the initial setup and verified connectivity:

- Save all router configurations: `write memory` on each router and save on the vPC
- Save your GNS3 project: File > Save project as

10. TROUBLESHOOTING TIPS

- Verify that all interfaces are in "up/up" state using `show ip interface brief`

- Check for typos in IP addresses and subnet masks
- Ensure that you've saved configurations on all devices
- Verify the OSPF neighbours’ relationship `show ip ospf summary`

4.1.4. 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.
2. Use the https://bgp.tools/ to identify the ASes entities involved in the lab topology.
3. Explain the concept of an Autonomous System (AS) in the Internet architecture and provide examples associated with the Portuguese Internet ecosystem.
4. 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.
5. Create a table showcasing all the peering relations established in the provided topology.
6. Explain how a Tier-2 benefits from peering instead of buying everything from a Tier-1.
7. 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.
8. Explain the role of R12 in AS 5511, and how are its interfaces divided between the OSPF areas involved.
9. 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.
10. Discuss why the subnet 46.87.162.0/24 was not placed on the backbone area, considering the OSPF design principles.

4.2. PHASE 2 - iBGP AND eBGP WITHOUT ROUTING POLICIES

4.2.1. OBJECTIVES

- Establish eBGP sessions between the AS's
- 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

4.2.2. IMPLEMENTATION

1. To configure the BGP on the router you should define the respective local AS, the router-id and individually configure the neighbours

```
router bgp 701
      !
      bgp router-id 10.14.14.14
      bgp log-neighbor-changes
      !
      neighbor 64.112.0.2 remote-as 1273
      neighbor 64.112.0.2 soft-reconfiguration inbound
```

The soft-reconfiguration inbound allows you to see the individual adj-RIB-in table from each peer and will be useful to understand the prefixes that were sent by the neighbours. It will also allow you to apply the policy rules during this lab, without the need to hard reset the BGP session.

2. The BGP only advertise routes that are installed on the routing table. To allow the peer routers from an AS to advertise its prefixes, you can add a static route pointing to null. You can consult the chapter Route Summarization from https://www.ciscopress.com/articles/article.asp?p=2756480&seqNum=13:

```
ip route 64.96.0.0 255.240.0.0 Null
ip route 64.112.0.0 255.240.0.0 Null0
ip route 65.0.204.0 255.255.255.0 Null0
```

3. advertise the subnets via BGP with the command network. Remember that mask should exactly match the prefix from the routing table:

```
router bgp 701
      network 64.96.0.114 mask 255.255.255.255
      network 64.96.0.0 mask 255.240.0.0
      network 64.112.0.0 mask 255.240.0.0
      network 65.0.204.0 mask 255.255.255.0
      no auto-summary
```

4. To facilitate the number of configurations, you can define an **iBGP peer-group** config template and apply the peer-group config to the iBGP neighbours:

```
router bgp 1273
   no synchronization
   bgp router-id 10.1.1.1
   !
   neighbor iBGP peer-group
   neighbor iBGP remote-as 1273
   neighbor iBGP update-source Loopback0
   neighbor iBGP next-hop-self
   neighbor iBGP soft-reconfiguration inbound
   !
   neighbor 10.3.3.3 peer-group iBGP
   neighbor 10.4.4.4 peer-group iBGP
```

5. For scalability and to avoid the full mesh in the AS1273, R3 and R4 must be defined as route reflectors routers, you should define the remaining neighbours as route reflectors clients. Moreover, beware that you will have to configure both route reflectors with the same cluster-id.

```
router bgp 1273
   no synchronization
   bgp router-id 10.3.3.3
   bgp cluster-id 1273
   !
   neighbor iBGP peer-group
   neighbor iBGP remote-as 1273
   neighbor iBGP update-source Loopback0
   neighbor iBGP route-reflector-client
   neighbor iBGP next-hop-self
   neighbor iBGP soft-reconfiguration inbound
   !
   neighbor iBGP_RR peer-group
   neighbor iBGP_RR remote-as 1273
   neighbor iBGP_RR update-source Loopback0
   neighbor iBGP_RR soft-reconfiguration inbound
   !
   neighbor 10.1.1.1 peer-group iBGP
   neighbor 10.2.2.2 peer-group iBGP
   neighbor 10.4.4.4 peer-group iBGP_RR
   neighbor 10.5.5.5 peer-group iBGP
   neighbor 10.6.6.6 peer-group iBGP
```

4.2.1. TEST AND VALIDATION

The following commands and checks are indicative, you should run in the different routers from the topology and interpret the output to confirm if you are getting the expected result (ex: prefixes that you expect, number of peering's and respective status).

1. Verify the BGP peer status

```
    R1#sh ip bgp summ
    BGP router identifier 10.1.1.1, local AS number 1273
    BGP table version is 100, main routing table version 100
    55 network entries using 7260 bytes of memory
    111 path entries using 5772 bytes of memory
    12/10 BGP path/bestpath attribute entries using 2016 bytes of memory
    8 BGP rrinfo entries using 192 bytes of memory
    8 BGP AS-PATH entries using 192 bytes of memory
    0 BGP route-map cache entries using 0 bytes of memory
    0 BGP filter-list cache entries using 0 bytes of memory
    Bitfield cache entries: current 3 (at peak 4) using 96 bytes of memory
    BGP using 15528 total bytes of memory
    BGP activity 55/0 prefixes, 615/504 paths, scan interval 60 secs

    Neighbor        V    AS    MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
    10.3.3.3        4    1273    260     242 100 0 0 03:34:47 49
    10.4.4.4        4    1273    242     224 100 0 0 03:34:35 49
    48.73.240.2     4    17390   565     335 100 0 0 05:17:31 8
```

2. Verify the prefixes received and sent from or to a determined neighbour

```
R3#show ip bgp neighbors 10.6.6.6 received-routes
BGP table version is 39, local router ID is 10.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,r RIB-failure,
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i46.87.162.0/24   10.6.6.6                 0    100      0 20717 5511 i
*>i46.88.20.0/24    10.6.6.6                 0    100      0 20717 5511 i
*>i46.88.22.0/24    10.6.6.6                 0    100      0 20717 5511 i
*>i46.89.36.0/24    10.6.6.6                 0    100      0 20717 5511 i
*>i46.89.38.0/24    10.6.6.6                 0    100      0 20717 5511 i
*>i46.92.2.0/24     10.6.6.6                 0    100      0 20717 5511 i
(...)
```

```
    R3#show ip bgp neighbors 10.6.6.6 advertised-routes
    BGP table version is 117, local router ID is 10.3.3.3
    Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,r RIB-
failure, S Stale
    Origin codes: i - IGP, e - EGP, ? - incomplete

       Network          Next Hop            Metric LocPrf Weight Path
    *>i10.0.0.0         10.6.6.6                 0    100      0 4637 1 ?
    *>i46.87.162.0/30   10.6.6.6                 0    100      0 5511 i
    *>i46.87.162.0/24   10.6.6.6                 0    100      0 5511 i
    *>i46.87.162.110/32 10.6.6.6                 0    100      0 5511 i
    *>i46.92.2.0/24     10.6.6.6
```

3. Verify the prefixes received and sent from or to a determined neighbour, notably the prefixes installed on the Loc-RIB BGP table:

```
   R9#show ip bgp
   BGP table version is 46, local router ID is 10.9.9.9
   Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,r RIB-
failure, S Stale
   Origin codes: i - IGP, e - EGP, ? - incomplete

      Network          Next Hop            Metric LocPrf Weight Path
   * 46.87.162.0/24    130.41.46.5                              0 17390 1273 20717 5511 i
   *>                  130.41.46.9                              0 17390 1273 20717 5511 i
   46.88.20.0/24       130.41.46.5                              0 17390 1273 20717 5511 i
   *>                  130.41.46.9                              0 17390 1273 20717 5511 i
   46.88.22.0/24       130.41.46.5                              0 17390 1273 20717 5511 i
   *>                  130.41.46.9                              0 17390 1273 20717 5511 i
   * 46.89.36.0/24     130.41.46.5                              0 17390 1273 20717 5511 i
   *>                  130.41.46.9                              0 17390 1273 20717 5511 i
     46.89.38.0/24     130.41.46.5                              0 17390 1273 20717 5511 i
   (…)
```

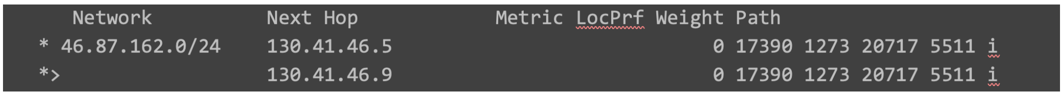
4. By the end of this chapter, you should be able to run the TCLSH (Tool Control Language) Shell for testing. When the BGP will be in place, from all the routers, using the Lo1 public IP addresses as source address, you should be able to ping all the Lo1 interfaces from the other routers and the public IPs from the servers. See the TCLSH script on the appendix TCLSH (Tool Control Language) Shell for testing.

5. SAVE YOUR PROGRESS

- Save all router configurations: `write memory` on each router
- Save this project phase as RI_25_26_GROUP<ID>_phase2

4.2.2. PRACTICAL QUESTIONS

1. How is the BGP next hop reachability solved inside an AS?
2. Why is it a good practice to use the loopback IP address in the iBGP sessions?
3. Create and present a detailed table with all the connectivity tests performed using the TCLSH procedure, as previously outlined.
4. 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.



```
     Network          Next Hop            Metric LocPrf Weight Path
  * 46.87.162.0/24    130.41.46.5                              0 17390 1273 20717 5511 i
  *>                  130.41.46.9                              0 17390 1273 20717 5511 i
```

5. 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?
6. How are the route prefixes propagated inside the AS when you have route reflectors configured?
7. Simulate and explain using Wireshark the BGP messages associated to each BGP state (see: https://www.ciscopress.com/articles/article.asp?p=2756480&seqNum=4).

4.3. PHASE 3 - ROUTING POLICIES IMPLEMENTATION

4.3.1. OBJECTIVES

- Aggregate IP prefixes when possible and advertise only the aggregate route on eBGP sessions.
- We should not have advertised prefixes longer than /24 in the internet routing 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 attribute
- The AS 23344 has only one peering to the internet and want to receive only the default route from the eBGP peering

4.3.2. IMPLEMENTATION

1. You should verify in each AS, the possibility to summarize the prefixes. When possible, the command aggregate will allow to advertise the summarized prefix only. You can apply this approach on the ASes with one peer router only, such as in this example:

```
router bgp 64513
   aggregate-address 130.41.47.0 255.255.255.0 summary-only
```

2. On the ASes with more than one router, the Lo1 interfaces are advertised in the iBGP and you need these prefixes for the internal routing, but you don't want them to be advertised to other ASes. To accomplish this, you can create an access list restricting the prefixes to advertise to the eBGP peers, specifying only the prefixes with mask /24 or lower (this blocks the masks /32) of the Lo1 interfaces).

```
ip prefix-list PREF_LIST_ADV_SUMM seq 5 permit <prefix add/mask> le <24>
…
router bgp 1273
   neighbor 48.73.240.6 prefix-list PREF_LIST_ADV_SUMM out
```

3. After changing or applying an out peering policy (ex: prefix-list application, route-map), you need to soft restart the peer to apply the policy changes:

```
R3#clear ip bgp 48.73.240.6 soft out
```

4.3.3. TEST AND VALIDATION

1. On each router, you can inspect the **AS_PATH attribute** of prefixes with the following commands:

```
R3#show ip bgp 211.176.129.0
R3#show ip bgp
```

These commands allow you to verify whether any advertised prefixes contain **private AS numbers** (64512–65535 or 4200000000–4294967294).

2. If private ASNs appear in the AS_PATH, they must be removed before advertising prefixes to external peers, since private ASNs are not valid in the global Internet. This can be achieved by applying the following command on the appropriate eBGP sessions:

```
neighbor 130.41.46.10 remove-private-as
```

3. SAVE YOUR PROGRESS
   - Save all router configurations: `write memory` on each router
   - Save this project phase as RI_25_26_GROUP<ID>_phase3

4.3.4. PRACTICAL QUESTIONS

1. After applying your prefix-list or route-map, compare the output of show ip bgp and show ip bgp neighbors <ip> advertised-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 advertised to the internet a good practice?
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 selection rules**, explain why R12 selects a specific path for the prefix `65.0.204.0/24`. Use the following output as reference (http://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 configuration change (e.g., adjusting local preference, MED, or weight) that would alter the selection. Justify your answer by showing the relevant command(s) and predicting the impact on the routing table.

4.4. PHASE 4 - INFLUENCE THE INTERNET ROUTING

4.4.1. OBJECTIVES

- Enable authentication on eBGP peerings in **AS701**.
- Filter Bogon prefixes received from the “BadGuy” router.
- Apply **Remote Triggered Black Hole (RTBH)** filtering to mitigate a DoS attack within **AS1273**.

4.4.2. IMPLEMENTATION

1. Create prefix-lists to specify which networks are advertised to external peers.
2. Create route-maps that match these lists and apply BGP attributes (e.g., local-preference, AS-path prepending).
3. Apply policy to neighbors: inbound and outbound. This involves setting how your AS prefers routes learned from external peers and which prefixes your AS announces and with what attributes.
4. In case you need to use regular expressions, the following link can help to test the logic: https://regex101.com/. You can find some examples from most common regular expressions in https://conference.apnic.net/22/docs/tut-routing-pres-bgp-bcp.pdf.

4.4.3. TEST AND VALIDATION

1. Use show ip bgp to check that routes through AS20717 are marked as best.
2. Use show ip bgp regexp to filter and verify specific paths (e.g., routes containing 20717).
3. Confirm that outbound advertisements are controlled using:

```
show ip bgp neighbors <ip> advertised-routes
```

4. Perform traceroute tests from routers in AS1273 and AS511 to confirm traffic flows through AS20717.
5. SAVE YOUR PROGRESS:
   - Save all router configurations: write memory on each router
   - Save this project phase as RI_25_26_GROUP<ID>_phase4

4.4.4. 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*).
2. Provide command output screenshots that demonstrate the successful application of the configured policies.
3. Discuss other alternative to achieve the same results and comment on their relative pros and cons, compared to your implementation.

4.5. PHASE 5 - SECURITY PRACTICES

4.5.1. OBJECTIVES

- Activate the MD5 authentication on all the eBGP peering's on the AS701. This a good practice for all the peers nevertheless for the lab proposes will be ok to test on this AS only.
- Filter the Bogon prefixes on the peer routers from AS 1273. The BadGuy router is advertising Bogons (see: https://conference.apnic.net/22/docs/tut-routing-pres-bgp-bcp.pdf).
- Implement Remote Triggered Black Hole (RTBH) filtering - a popular and effective technique for the mitigation of denial-of-service (DoS) attack on **AS1273** coming from the prefix `63.96.0.115` https://www.cisco.com/c/dam/en_us/about/security/intelligence/blackhole.

4.5.2. IMPLEMENTATION

1. Configure MD5 Authentication on eBGP Peerings (AS701). MD5 authentication ensures that only peers using the same shared password can establish a BGP session. This prevents unauthorized peers from injecting routes.

```
router bgp 701
  neighbor 64.112.0.2 remote-as 1273
  neighbor 64.112.0.2 password BGPpass123
```

2. Apply the same configuration on the neighbor router (AS1273), using the same password. If the passwords do not match, the session will fail with an **Authentication failure** error.
3. To filter Bogon Prefixes in AS1273, define a prefix-list for Bogons (example):

```
ip prefix-list BOGONS deny 10.0.0.0/8
ip prefix-list BOGONS deny 172.16.0.0/12
ip prefix-list BOGONS deny 192.168.0.0/16
ip prefix-list BOGONS permit 0.0.0.0/0 le 32
```

4. Then, apply the prefix list filtering on each neighbor session:

```
router bgp 701
  neighbor 64.112.0.2 remote-as 1273
  neighbor 64.112.0.2 prefix-list BOGONS in
```

5. Now, on R14 simulate the bot attacker:

```
interface Loopback2
ip address 63.96.0.115 255.255.255.255
```

6. To deploy RTBH Filtering in AS1273 you will configure **R4 as the trigger router** to filter the prefix `63.96.0.115`.

```
R4#
ip route 64.96.0.115 255.255.255.255 Null0 tag 66
router bgp 1273
redistribute static
neighbor iBGP send-community
neighbor iBGP route-map black-hole-trigger out
...
```

```
    ip prefix-list BH seq 5 permit 64.96.0.115/32
    ...
    route-map black-hole-trigger permit 10
    match ip address prefix-list BH
    set local-preference 200
    set origin igp
    set community no-export
    set ip next-hop 192.0.2.1
```

7. On all edge routers of AS1273 implement the black hole route. The IP address 192.0.2.1 is reserved for use in test networks and is not used as a deployed. The uRPF (`ip verify unicast reverse-path`) ensures packets with spoofed source addresses are dropped at peering interfaces.

```
    ip route 192.0.2.1 255.255.255.255 Null0

    interface GigabitEthernet1/0
    ip verify unicast reverse-path
```

4.5.3. TESTING AND VALIDATION

1. Use show ip bgp summary to confirm that the eBGP sessions in AS701 are in the Established state after applying the MD5 authentication.
2. Use show ip bgp to check that Bogon prefixes from "BadGuy" do not enter the local BGP table in AS 1273.
3. From R14, ping Server2 using source IP `64.96.0.115` to check if the RTBH filtering is working out as expected.
4. On R5–R3, run a Wireshark capture to monitor ICMP traffic
5. SAVE YOUR PROGRESS:
    - Save all router configurations: write memory on each router
    - Save this project phase as RI_25_26_GROUP<ID>_phase5

4.5.4. PRACTICAL QUESTIONS

1. How does MD5 authentication improve the security of BGP sessions? What happens if it is not enabled?
2. Which Bogon ranges did you filter in your lab, and why must they not appear in the global routing table?
3. Explain how RTBH was implemented in AS1273. Include a diagram showing how the trigger router propagates the blackhole route.
4. Describe the role of uRPF in validating traffic source addresses and preventing spoofing.
5. What impact would the attack from 64.96.0.115 have on AS1273 if RTBH was not deployed?

5. APPENDICES

5.1. IP ADDRESSING FOR LAB TOPOLOGY

TABLE 1 - IP ADDRESSING

Router	Interface	Private IP Address	Public IP Address
R1	Lo0	10.1.1.1/32	
	Lo1		48.73.239.11/32
	g1/0	10.1.2.1/30	
	g2/0	10.1.3.1/30	
	g4/0		48.73.240.1/30
R2	Lo0	10.2.2.2/32	
	Lo1		48.73.239.22/32
	f0/0		48.73.239.2/30
	g1/0	10.1.2.2/30	
	g2/0	10.2.4.1/30	
R3	Lo0	10.3.3.3/32	
	Lo1		48.73.239.33/32
	g1/0	10.3.4.1/30	
	g2/0	10.1.3.2/30	
	g3/0	10.3.5.1/30	
	g4/0		48.73.240.5/30
R4	Lo0	10.4.4.4/32	
	Lo1		48.73.239.44/32
	g1/0	10.3.4.2/30	
	g2/0	10.2.4.2/30	
	g3/0	10.4.6.1/30	
R5	Lo0	10.5.5.5/32	
	Lo1		48.73.239.55/32
	g1/0		64.112.0.2/30
	g3/0	10.3.5.2/30	
R6	Lo0	10.6.6.6/32	
	Lo1		48.73.239.66/32
	f0/0		48.73.240.17/30
	g1/0		48.73.240.13/30
	g2/0		48.73.240.21/30

Router	Interface	Private IP Address	Public IP Address
	g3/0	10.4.6.2/30	
R7	Lo0	10.7.7.7/32	
	Lo1		130.41.46.77/32
	f0/0		130.41.46.9/30
	g1/0	10.7.8.1/30	
	g4/0		48.73.240.6/30
	g5/0		64.112.0.6/30
R8	Lo0	10.8.8.8/32	
	Lo1		130.41.46.88/32
	f0/0		130.41.46.5/30
	g1/0	10.7.8.2/30	
	g4/0		48.73.240.2/30
	g5/0		130.41.46.2/30
R9	Lo0	10.9.9.9/32	
	Lo1		130.41.47.99/32
	f0/0		130.41.46.10/30
	f1/0		130.41.46.6/30
R10	Lo0	10.10.10.10/32	
	Lo1		46.87.162.110/32
	g1/0	10.10.11.1/30	
	g2/0		211.176.129.2/30
	g3/0	10.10.12.1/30	
	g4/0		46.88.20.1/30
R11	Lo0	10.11.11.11/32	
	Lo1		46.87.162.111/32
	f0/0		46.88.20.5/30
	g1/0	10.10.11.2/30	
	g2/0	10.11.12.1/30	
R12	Lo0	10.12.12.12/32	
	Lo1		46.87.162.112/32
	f0/0		46.87.162.2/30
	g2/0	10.11.12.2/30	
	g3/0	10.10.12.2/30	
	g5/0		48.73.240.18/30
R13	Lo0	10.13.13.13/32	

Router	Interface	Private IP Address	Public IP Address
	Lo1		158.23.228.113/32
	f0/0		46.88.20.6/30
	g1/0		158.23.228.2/30
R14	Lo0	10.14.14.14/32	
	Lo1		64.96.0.114/32
	f0/0		64.96.0.2/30
	g1/0		64.112.0.1/30
	g3/0		64.112.0.9/30
	g5/0		64.112.0.5/30
R15	Lo0	10.15.15.15/32	
	Lo1		211.176.128.115/32
	f0/0		211.176.128.2/30
	g1/0		48.73.240.14/30
	g2/0		211.176.129.1/30
	g3/0		64.112.0.10/30
	g4/0		211.176.129.5/30
R16	Lo0	10.16.16.16/32	
	Lo1		
	g2/0		48.73.240.22/30
	g4/0		48.88.20.2/30
Badguy	Lo0	10.66.66.66/32	
	g4/0		211.176.129.6/30
Server1	e0		130.41.46.1/30
Server2	e0		48.73.239.1/30
Server3	e0		64.96.0.1/30
Server4	e0		211.176.128.1/30
Server5	e0		46.87.162.1/30
Server6	e0		158.23.228.1/30

5.2. TCLSH (TOOL CONTROL LANGUAGE) SHELL FOR TESTING.

```
R9#tclsh
R9(tcl)#
foreach address {
48.73.239.11
48.73.239.22
48.73.239.33
48.73.239.44
48.73.239.55
48.73.239.66
130.41.46.77
130.41.46.88
130.41.47.99
46.87.162.110
46.87.162.111
46.87.162.112
158.23.228.113
64.96.0.114
211.176.128.115
130.41.46.1
48.73.239.1
64.96.0.1
211.176.128.1
46.87.162.1
158.23.228.1
} {ping $address source lo1}
```