RECOMP Sprint 2 Report – Group 5

Isaac Santos – 1181242

André Teixeira – 1190384

Wimy Carvalho – 1161297

Matija Zupanc - 1240290



Table of contents

[Introduction 2](#_Toc656323325)

[Routing configuration between branches 3](#_Toc1461360530)

[GRE Configuration 3](#_Toc48074560)

[Between Oporto and Warsaw 3](#_Toc632638007)

[Between Oporto and Munich 3](#_Toc2017252754)

[Port Security Configuration 4](#_Toc1661345855)

[ACLs 5](#_Toc1916685241)

[PAT 9](#_Toc2018042732)

[IPv6 9](#_Toc925476441)

[1) IPv6 Subnet Planning 9](#_Toc1806200731)

[3) Dynamic Routing with IPv6 11](#_Toc2065591883)

[4) IPv6 Security Considerations 11](#_Toc1939364337)

[5) Transition and Coexistence with IPv4 12](#_Toc258498158)

[6) Conclusion 12](#_Toc516532642)

[OSPF Configuration 12](#_Toc527668763)

[EIGRP Configuration 13](#_Toc1763157770)

# Introduction

In this report it will be detailed an expansion in the configuration for the network created for 3 sites of the hypothetical company *“RECOMP Corporation WAN”* in the previous sprint. These new configurations are mainly concerned with creating a safe environment, making sure that the users have their needed accesses while keeping vulnerabilities in check.

# Routing configuration between branches

To enable communication between branches we must configure the routes between branches. This was done with the following commands.

|  |
| --- |
| Oporto |
| ip route 10.27.68.0 255.255.254.0 192.0.2.110  ip route 10.27.70.0 255.255.255.0 192.0.2.110  ip route 10.27.71.0 255.255.255.128 192.0.2.110  ip route 10.27.71.128 255.255.255.192 192.0.2.110  ip route 172.21.72.0 255.255.255.0 192.0.2.110  ip route 172.21.73.0 255.255.255.0 192.0.2.110 |
| Warsaw |
| ip route 10.27.68.0 255.255.254.0 192.0.2.110  ip route 10.27.70.0 255.255.255.0 192.0.2.110  ip route 10.27.71.0 255.255.255.128 192.0.2.110  ip route 10.27.71.128 255.255.255.192 192.0.2.110  ip route 172.21.72.0 255.255.255.0 192.0.2.110  ip route 172.21.73.0 255.255.255.0 192.0.2.110 |
| Munich |
| ip route 10.27.68.0 255.255.254.0 193.136.60.150  ip route 10.27.70.0 255.255.255.0 193.136.60.150  ip route 10.27.71.0 255.255.255.128 193.136.60.150  ip route 10.27.71.128 255.255.255.192 193.136.60.150  ip route 192.168.154.0 255.255.255.0 193.136.60.150  ip route 192.168.155.0 255.255.255.0 193.136.60.150 |

|  |  |
| --- | --- |
| MLS1 | MLS2 |
| ip route 0.0.0.0 0.0.0.0 10.27.71.193 | ip route 0.0.0.0 0.0.0.0 10.27.71.197 |

# GRE Configuration

Two GRE tunnels were created for the relations between routers. One was created between Oporto and Warsaw, and another between Oporto and Munich. Here follow their configurations.

### Between Oporto and Warsaw

Using the network 1.0.0.0/30, the configuration is as follows:

|  |  |
| --- | --- |
| Oporto | Warsaw |
| interface Tunnel 0  ip address 10.0.0.1 255.255.255.252  tunnel source G0/0/0  tunnel destination 192.0.2.97  tunnel mode gre ip  no shutdown | interface Tunnel 0  ip address 10.0.0.2 255.255.255.252  tunnel source G0/0/0  tunnel destination 209.165.200.129  tunnel mode gre ip  no shutdown |

### Between Oporto and Munich

Using the network 1.0.0.4/30, the configuration is as follows:

|  |  |
| --- | --- |
| Oporto | Munich |
| interface Tunnel 1  ip address 10.0.0.5 255.255.255.252  tunnel source G0/0/0  tunnel destination 193.136.60.147  tunnel mode gre ip  no shutdown | interface Tunnel 1  ip address 10.0.0.6 255.255.255.252  tunnel source G0/0/0  tunnel destination 209.165.200.129  tunnel mode gre ip  no shutdown |

A screenshot of a computer program

Description automatically generated A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated A screenshot of a computer program

Description automatically generated

# Port Security Configuration

To configure Port Security, the following configurations were done on each of the switches available ports:

|  |
| --- |
| Oporto – SW1 and SW2 |
| interface range f0/5-20  switchport mode access  switchport port-security  switchport port-security maximum 2  switchport port-security mac-address sticky  switchport port-security violation shutdown |
| Warsaw – SW1 |
| interface range f0/1-20  switchport mode access  switchport port-security  switchport port-security maximum 2  switchport port-security mac-address sticky  switchport port-security violation shutdown |
| Munich – SW1 |
| interface range f0/1-20  switchport mode access  switchport port-security  switchport port-security maximum 2  switchport port-security mac-address sticky  switchport port-security violation shutdown |

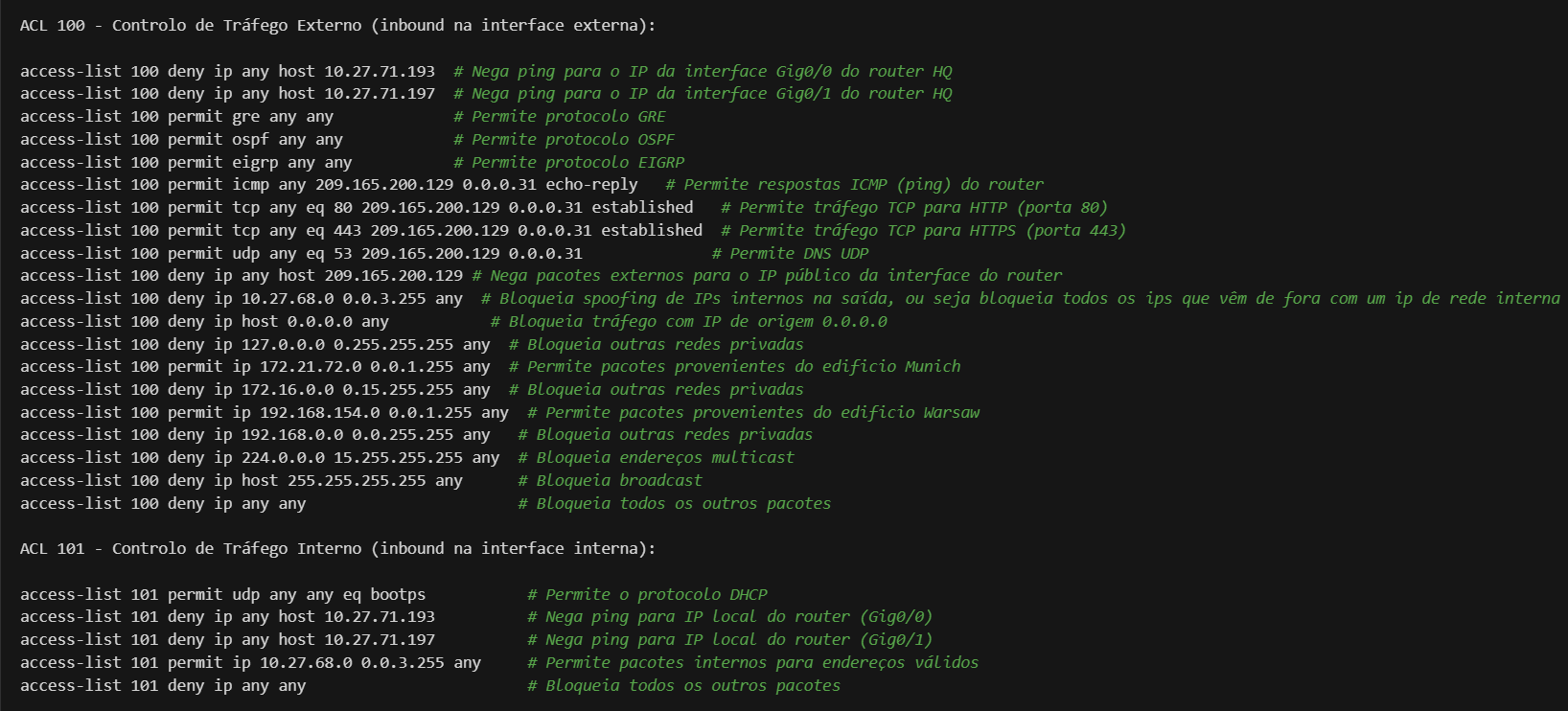
This set of commands, performed on each of the available interface in each switch, enables port security on all the applied interfaces, limiting them to a maximum of 2 MAC addresses connected to them, and performing a shutdown on the violation of that limit. Finally, the mac-address sticky command makes sure that each MAC address is dynamically learned and retained in that interface, to keep track of the configured maximum.

# ACLs

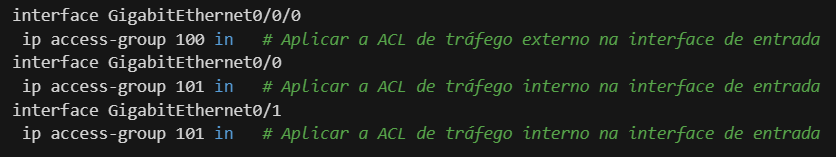
In this section, it was requested that internal and external spoofing be blocked on the routers of the three buildings. Furthermore, all traffic directed to the routers was blocked, with the exception of what is necessary for the implemented functionalities to continue operating. Finally, it was requested that the remaining traffic be allowed.

In order to block unwanted traffic and prevent spoofing, rules for access-lists (ACLs) were created, which were configured on the routers in each building. These rules are:

* **Oporto**



These ACLs were applied to the respective interfaces with the commands:



* ACL 100

Controls incoming traffic on the public interface (GigabitEthernet0/0).

Allows essential protocols such as GRE, OSPF, EIGRP and ICMP (echo-reply).

Allows HTTP, HTTPS and DNS connections to the Oporto public network.

Blocks spoofing of internal addresses and unauthorized private networks.

Ensures that only authorized traffic from other branches is allowed

* ACL 101

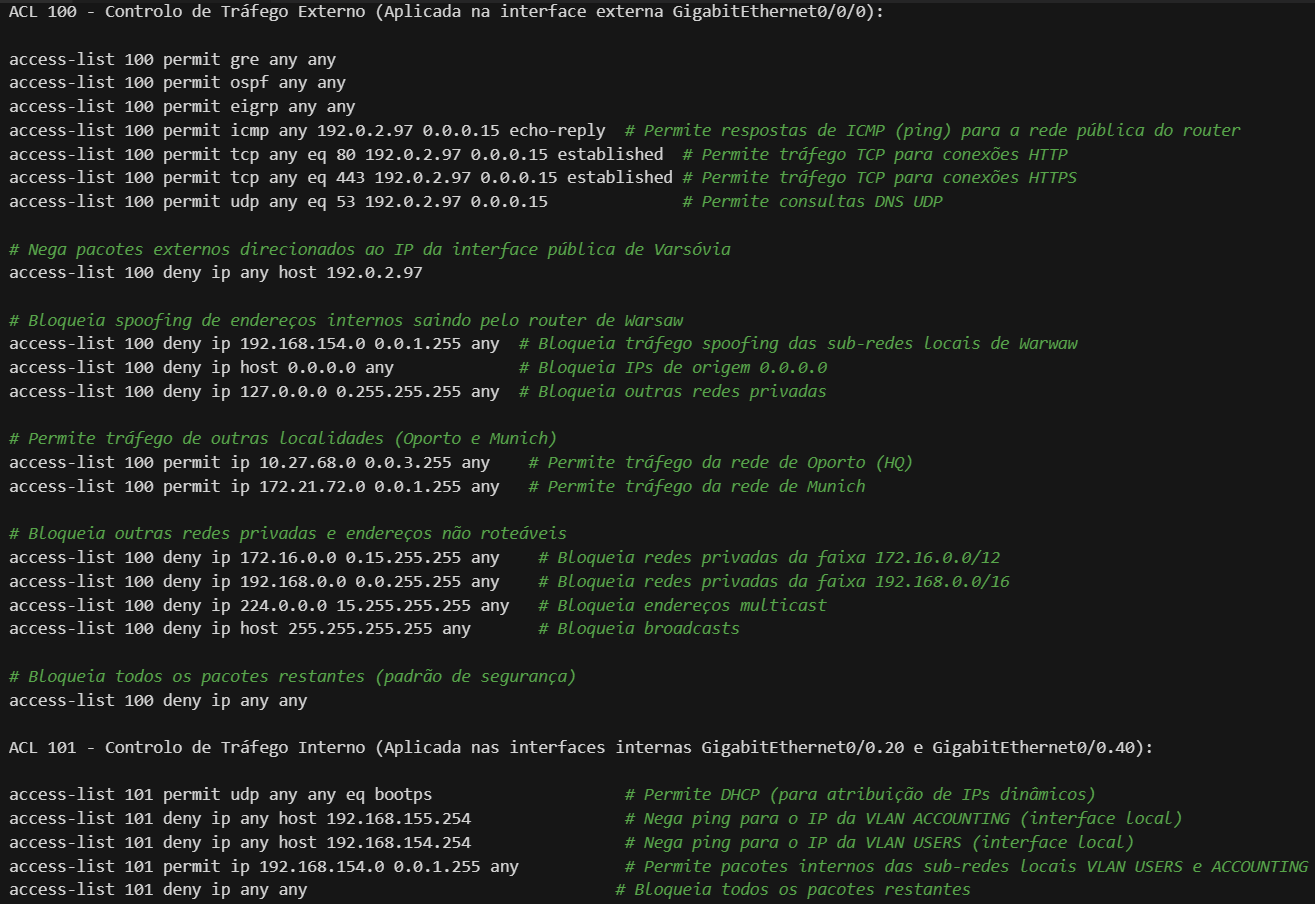
Controls incoming traffic on internal interfaces (VLAN STAFF, VLAN ACCOUNTING, VLAN HR and VLAN USERS).

Allows DHCP traffic for automatic IP configuration.

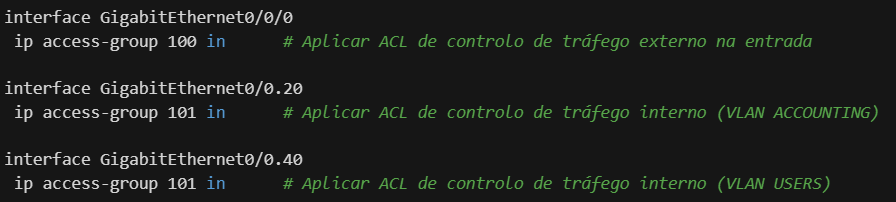
Restricts ping to local interface IPs and blocks unauthorized packets.

Ensures that only valid traffic from the internal network is allowed.

* **Warsaw**



These ACLs were applied to the respective interfaces with the commands:



* ACL 100:

Controls incoming traffic on the public interface (GigabitEthernet0/0/0).

Allows essential protocols such as GRE, OSPF, EIGRP and ICMP (echo-reply).

Allows HTTP, HTTPS and DNS connections to the Warsaw public network.

Blocks spoofing of internal addresses and unauthorized private networks.

* ACL 101:

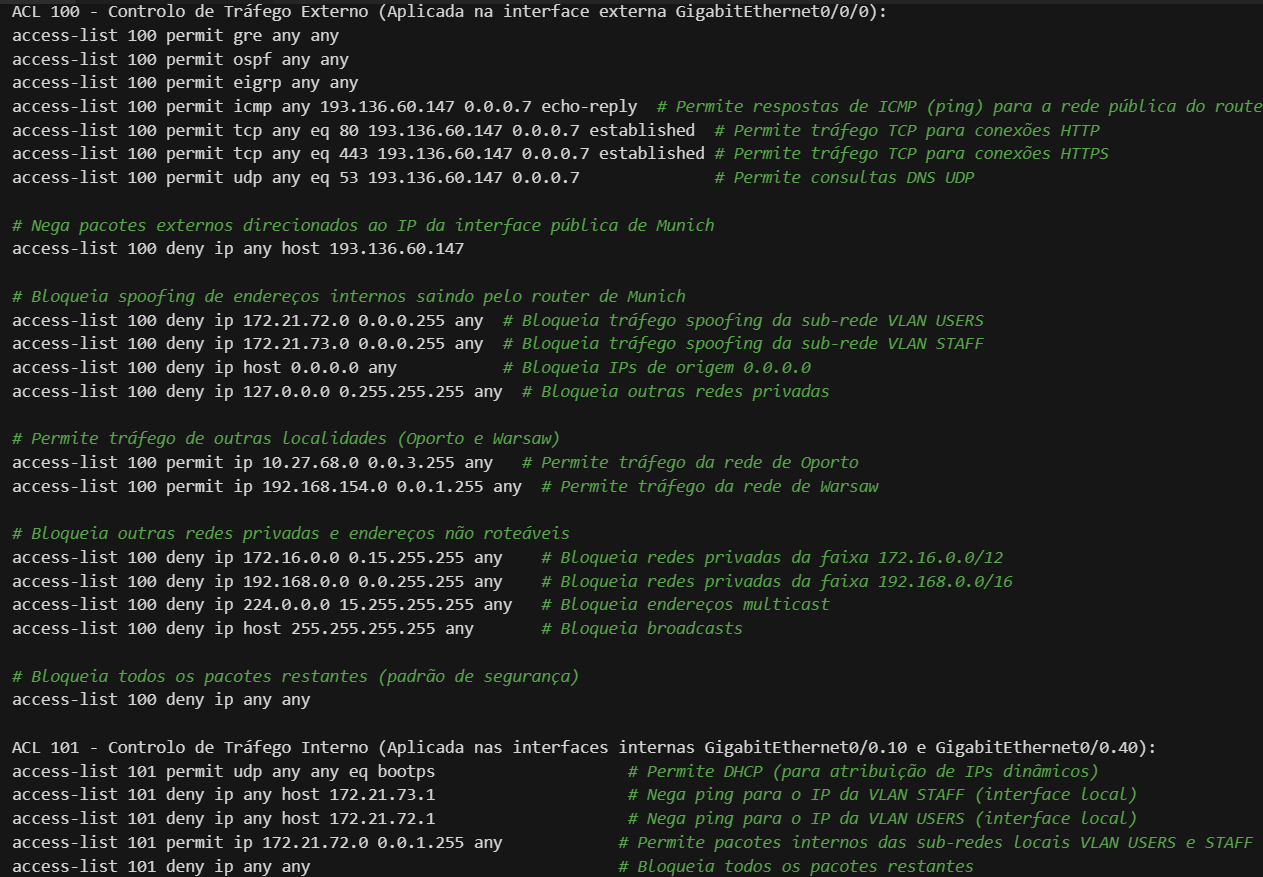
Controls incoming traffic on the internal VLAN ACCOUNTING and VLAN USERS interfaces.

Allows DHCP traffic for automatic IP configuration.

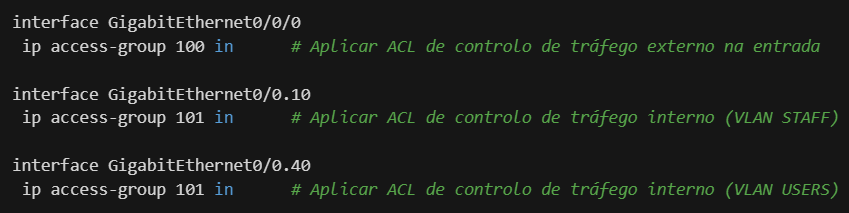
Restricts ping to the IP of local interfaces and blocks unauthorized packets.

These ACL settings protect the Warsaw router by restricting external traffic and securing internal subnets according to project security guidelines.

* **Munich**



These ACLs were applied to the respective interfaces with the commands:



* ACL 100:

Controls incoming traffic on the public interface (GigabitEthernet0/0/0).

Allows essential protocols such as GRE, OSPF, EIGRP and ICMP (echo-reply).

Allows HTTP, HTTPS and DNS connections to the Munich public network.

Blocks spoofing of internal addresses and unauthorized private networks.

* ACL 101:

Controls incoming traffic on internal VLAN STAFF and VLAN USERS interfaces.

Allows DHCP traffic for automatic IP configuration.

Restricts ping to the IP of local interfaces and blocks unauthorized packets.

These ACL settings provide security to the Munich router by limiting external traffic and protecting internal subnets.

# PAT

PAT – Port Address Translation is a type of network address translation protocol that uses additional help of port number to allow multiple users to share one public address. When the router receives traffic that needs to go through internet/public network it converts its local IP address to a public one.

To enable communication between branches and allow users to access the internet a PAT protocol was also implemented with the following commands

|  |
| --- |
| Oporto |
| ip nat inside source list 101 interface GigabitEthernet0/0/0 overload  interface GigabitEthernet0/0/0  ip nat outside  interface GigabitEthernet0/1  ip nat inside  interface GigabitEthernet0/0  ip nat inside |
| Warsaw |
| ip nat inside source list 101 interface GigabitEthernet0/0/0 overload  interface GigabitEthernet0/0/0  ip nat outside  interface GigabitEthernet0/0.20  ip nat inside  interface GigabitEthernet0/0.40  ip nat inside |
| Munich |
| ip nat inside source list 101 interface GigabitEthernet0/0/0 overload  interface GigabitEthernet0/0/0  ip nat outside  interface GigabitEthernet0/0.10  ip nat inside  interface GigabitEthernet0/0.40  ip nat inside |

# IPv6

RECOMP Corporation is planning to migrate from IPv4 to IPv6 to meet the growing scalability and network requirements. During the transition process, both protocols (IPv4 and IPv6) must coexist. This report presents configuration recommendations to support IPv6 in each branch and ensure a smooth transition between protocols.

## IPv6 Subnet Planning

Prefix **2001:db8::/32:** This prefix is reserved by the IETF (Internet Engineering Task Force) for documentation and examples, as a "fictitious network" for teaching and testing purposes. It should not be used in production since it is designated for documentation. For a real environment, the organization should request an IPv6 prefix from an Internet Service Provider (ISP).

For the IPv6 addressing structure, RECOMP should use a **/48 prefix** for each location, subdivided into /64 subnets for each internal VLAN, allowing each VLAN network to have unique IPv6 addresses. Below are the suggested IPv6 prefixes for each location:

* **Oporto**: **2001:db8:10::/48**
  + The suffix 10 was chosen to identify Oporto's network.
  + The /48 mask means the first 48 bits of the address define the network, leaving the remaining bits to create subnets.
  + Below this /48 prefix, multiple /64 subnets can be created for the VLANs in Oporto.
    - VLAN STAFF: **2001:db8:10:10::/64**
    - VLAN ACCOUNTING: **2001:db8:10:20::/64**
    - VLAN HR: **2001:db8:10:30::/64**
    - VLAN USERS: **2001:db8:10:40::/64**
* **Warsaw**: **2001:db8:11::/48**
  + The suffix 11 was used to identify the Warsaw network.
  + Each VLAN in Warsaw receives a new suffix, allowing unique IPv6 networks for each department or VLAN.
    - VLAN ACCOUNTING: **2001:db8:11:20::/64**
    - VLAN USERS: **2001:db8:11:40::/64**
* **Munich**: **2001:db8:12::/48**
  + The suffix 12 identifies Munich's network.
  + This /48 prefix can be divided into /64 subnets, creating specific identifiers for VLANs at this location.
    - VLAN STAFF: **2001:db8:12:10::/64**
    - VLAN USERS: **2001:db8:12:40::/64**

These subnets should be consistently applied across all branches to facilitate routing and management.

**In a Real Environment**

For a real corporate network, the company should:

* Obtain an IPv6 prefix from an ISP, which may be a /48 for large companies or a /56 for smaller companies.
* Subdivide this prefix for internal networks, maintaining hierarchy as described, to facilitate internal routing and management.

1. IPv6 Address Allocation for Devices

To distribute IPv6 addresses to devices, we recommend two approaches:

1. **SLAAC (Stateless Address Autoconfiguration):**

* Allows devices to automatically configure their IPv6 addresses based on prefixes announced by routers.
* Used for networks that do not require strict IP control, such as general-use networks (e.g., VLAN USERS).

1. **DHCPv6:**

* Used for centralized control, such as in the ACCOUNTING network segments, where more careful management of IP addresses is needed.
* DHCPv6 enables device tracking and offers additional options, such as DNS assignment.

Each VLAN should be configured to support IPv6 address distribution according to each network's management and security needs.

## Dynamic Routing with IPv6

To ensure connectivity and efficient routing between locations, RECOMP should implement dynamic routing with IPv6. The recommendations are:

* **OSPFv3**: Recommended for routing within each location, with specific areas for local networks and GRE tunnels connecting locations.
  + **Area 0** for tunnels between Oporto and Warsaw, and between Oporto and Munich.
  + **Area 1** for local networks in Oporto.
  + **Area 2** for local networks in Warsaw.
  + **Area 3** for local networks in Munich.
* **EIGRP for IPv6**: Should be configured on GRE tunnel interfaces to ensure connectivity between locations (Oporto-Munich and Oporto-Warsaw) and facilitate redistribution between OSPF and EIGRP.

## IPv6 Security Considerations

The introduction of IPv6 brings new security challenges. We recommend the following measures:

* **RA Guard and DHCP Guard**: To prevent unauthorized router announcements and DHCP attacks, which could compromise the network.
* **IPv6 ACLs**: As with IPv4, ACLs should be configured to control IPv6 traffic. IPv6 ACLs should include:
  + Blocking unnecessary multicast addresses.
  + Controlling traffic between VLANs and internal networks.
  + Restricting access to routers and other critical devices.

## Transition and Coexistence with IPv4

During the transition, we recommend using a **dual-stack configuration** (simultaneous support for IPv4 and IPv6) on all devices and routers until the network is ready to operate exclusively with IPv6. This will allow:

* **Continuous access** to services that still rely on IPv4.
* **Monitoring and adjustments** for IPv6 performance and security in a controlled environment.

## Conclusion

Implementing IPv6 will provide greater flexibility and scalability for RECOMP Corporation. This transition plan considers the security, routing, and address management requirements for a seamless coexistence with IPv4. We recommend a period of testing and monitoring, with regular updates to ensure the migration is effective and secure.

# OSPF Configuration

In this section, it was requested to configure the OSPF router-ID on Oporto and Warsaw routers to 1.1.1.1 and 2.2.2.2, respectively. Assign Oporto's tunnel interface to Warsaw in area 0 and local networks to area 1, ensuring OSPF is also configured on Oporto's MLS’s and assign Warsaw's tunnel interface to Oporto in area 0 and local networks to area 2.

|  |  |
| --- | --- |
| Oporto | Warsaw |
| **Router HQ** router ospf 1  router-id 1.1.1.1  network 10.0.0.0 0.0.0.3 area 0  network 10.27.71.192 0.0.0.3 area 1  network 10.27.71.196 0.0.0.3 area 1  redistribute eigrp 1 subnets  **MLS1** router ospf 1  router-id 3.3.3.3  network 10.27.71.192 0.0.0.3 area 1  network 10.27.68.0 0.0.1.255 area 1  network 10.27.70.0 0.0.0.255 area 1  network 10.27.71.0 0.0.0.127 area 1  network 10.27.71.128 0.0.0.63 area 1  **MLS2**  router ospf 1  router-id 4.4.4.4  network 10.27.71.196 0.0.0.3 area 1  network 10.27.68.0 0.0.1.255 area 1  network 10.27.70.0 0.0.0.255 area 1  network 10.27.71.0 0.0.0.127 area 1  network 10.27.71.128 0.0.0.63 area 1 | router ospf 1  router-id 2.2.2.2  network 10.0.0.0 0.0.0.3 area 0  network 192.168.154.0 0.0.0.255 area 2  network 192.168.155.0 0.0.0.255 area 2 |

# EIGRP Configuration

In this section, we will demonstrate the commands necessary to make the EIGRP configuration. It was requested to configure EIGRP in the Oporto tunnel interface, Munich's tunnel interface, and local networks.

|  |  |
| --- | --- |
| Oporto | Munich |
| router eigrp 1  network 10.0.0.4 0.0.0.3  network 10.27.71.192 0.0.0.3  network 10.27.71.196 0.0.0.3  redistribute ospf 1 metric 10000 10 255 1 1500 | router eigrp 1  network 10.0.0.4 0.0.0.3  network 172.21.72.0 0.0.0.255  network 172.21.73.0 0.0.0.255 |

# Conclusion

The commands used greatly improved the security of complete network. The communication between users was also greatly enhanced to allow them to communicate between different branches and access internet. It is also more efficient because of blocking unnecessary and unwanted traffic.