RECOMP Sprint 3 Report – Group 5

Isaac Santos – 1181242

André Teixeira – 1190384

Wimy Carvalho – 1161297

Matija Zupanc - 1240290

ISEP INSTITUTO SUPERIOR DE ENGENHARIA DO PORTO

Table of contents

Introduction

In Sprint 3, we are challenged to implement a DMZ, configure internal servers, and perform security adjustments while integrating technologies such as VLANs, HSRP, OSPF, and QoS. This report presents the execution of the proposed tasks, highlighting the importance of each step in ensuring efficiency, security, and connectivity within the simulated environment.

DMZ

In this section, the creation of a DMZ on the Porto website was requested, and a new switch was requested connected to the Porto router. This new switch was asked to add the following servers: (DNS Server, FTP Server, HTTP Server, Email Server, IoT Server). In addition, OSPF was also requested to be reconfigured to take into account the new network, as well as the PAT configuration.

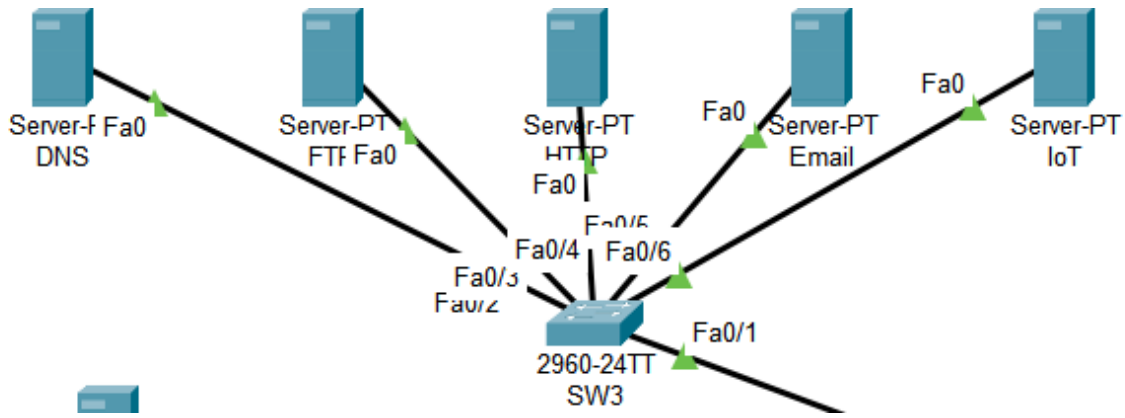

Figure 1 DMZ

Static IPs were assigned to all servers created from the block: 192.168.G.0/27 (G being our group number), with the Subnet Mask: 255.255.255.224.

Note: Our group is number 5.

Device	Static IP
Router Oporto	192.168.5.1
DNS Server	192.168.5.2
FTP Server	192.168.5.3
HTTP Server	192.168.5.4
Email Server	192.168.5.5
loT Server	192.168.5.6

To configure OSPF on the router, the following settings were made:

- Router Oporto:
  router ospf 1
  router-id 1.1.1.1
  network 10.0.0.0 0.0.0.3 area 0
  network 10.27.68.0 0.0.3.255 area 1
  network 192.168.5.0 0.0.0.31 area 1
  network 10.27.71.193 0.0.0.15 area 1

- MLS1:
  router ospf 1
  router-id 3.3.3.3
  network 10.27.68.0 0.0.3.255 area 1
  network 192.168.5.0 0.0.0.31 area 1
  network 10.27.71.193 0.0.0.15 area 1

- MLS2:
  router ospf 1
  router-id 4.4.4.4
  network 10.27.68.0 0.0.3.255 area 1
  network 192.168.5.0 0.0.0.31 area 1
  network 10.27.71.193 0.0.0.15 area 1

To configure the PAT, the following settings were made on the Oporto router:

```
no access-list 10

access-list 10 permit 10.27.68.0 0.0.3.255

access-list 10 permit 192.168.5.0 0.0.0.31

ip nat inside source list 10 interface Gig0/0/0 overload

interface Gig0/0
 ip nat inside

interface Gig0/1
 ip nat inside

interface Gig0/0/0
 ip nat outside

interface Gig0/2
 ip nat inside
```

Figure 2 PAT

Explanation:

- no access-list 10: Removes any existing access list numbered 10 to start fresh.
- access-list 10 permit 10.27.68.0 0.0.3.255: Allows traffic from the 10.27.68.0/22 network.
- access-list 10 permit 192.168.5.0 0.0.0.31: Allows traffic from the 192.168.5.0/27 network.
- ip nat inside source list 10 interface Gig0/0/0 overload: Configures NAT Overload for addresses matched by access list 10, translating them to the IP address of the Gig0/0/0 interface.
- interface Gig0/0 to interface Gig0/2: Configures NAT roles for interfaces. ip nat inside designates interfaces as internal (inside the network), and ip nat outside designates external (outside the network).

Internal Servers

Syslog

When setting up the Syslog server, we connected a new switch (SW4) to both MLS (Multi-Layer Switch) switches (MLS1 and MLS2) and configured the necessary settings. Before configuring the switches, we created a new subnetwork with the address 10.27.71.208/28. Below are the necessary configurations that were performed on the switch (SW4) and the MLS switches (MLS1 and MLS2), as well as the router (HQ).

SW4
interface FastEthernet0/1 switchport access vlan 50 switchport trunk native vlan 50 switchport mode trunk interface FastEthernet0/2 switchport access vlan 50 switchport trunk native vlan 50 switchport mode trunk interface FastEthernet0/3 switchport access vlan 100 switchport mode access

A new VLAN (VLAN 100) was introduced to enable a secure and stable connection to the server. The interfaces connected to the MLS switches (FastEthernet0/1 and FastEthernet0/2) were configured as trunk ports using native VLAN 50. The interface connected to the server (FastEthernet0/3) uses VLAN 100 and is set to access mode.

MLS1	**MLS2**
interface Vlan100 ip address 10.27.71.211 255.255.255.240 Standby 100 priority 110 standby 100 preempt router ospf 1 network 10.27.71.208 0.0.0.15 area 1	interface Vlan100 ip address 10.27.71.212 255.255.255.240 Standby 100 priority 90 standby 100 preempt router ospf 1 network 10.27.71.208 0.0.0.15 area 1

Both MLS1 and MLS2 have IP addresses configured under VLAN 100. In the HSRP (Hot Standby Router Protocol) configuration, MLS1 has a higher priority (110) compared to MLS2 (90). Both

switches have preemption enabled. Additionally, we set up a new network in the OSPF (Open Shortest Path First) configuration.

BR1

```
logging on
logging 10.27.71.210
logging trap debugging
```

In the HQ router, we enabled logging to the Syslog server with the IP address 10.27.71.210 using the above commands.

HTML

To include the branch name in the webpage, the following code was used in the index.html file. This code displays a welcome message in blue color with a font size of 3, centered on the webpage, with the branch name "Oporto" highlighted.

index.html

```
<html> <center><font size='+3'
color='blue'>Welcome to
Oporto</font></center> </html>
```

The same was done for branches Warsaw and Munich where the text is changed according to the location the server is located.

FTP

On the FTP server, a new user was created with the following properties:

username	password	permission
recomp5	recomp5	RWDNL

For this account, we opted to grant all permissions (Read, Write, Delete, Rename, List) because it is the main account used for maintaining and editing everything on this server.

Email

For the email server, three new users were created: Oporto, Warsaw, and Munich. The domain for all users is mail.recomp2425m1b05.recomp.com, and the password used for all accounts is recomp5.

Others

We enabled the **IoT** and **Syslog** services on the Oporto branch, and the **DNS** service was enabled across all three branches (Oporto, Warsaw, and Munich).

DNS configuration in Oporto

After adding the DMZ zone, we proceeded to configure it by adding DNS records to the DNS server to route incoming traffic from users across the Oporto branch. We also configured forwarding of DNS queries to the default DNS server (8.8.8.8).

No.	Name	Type	Detail
0	.	NS	ns
1	ftp.porto.recomp2425m1b05.recomp.com	A Record	192.168.5.3
2	munich.recomp2425m1b05.recomp.com	NS	ns.munich.recomp2425m1b05.recomp.com
3	ns	A Record	8.8.8.8
4	ns.munich.recomp2425m1b05.recomp.com	A Record	192.168.200.2
5	warsaw.recomp2425m1b05.recomp.com	NS	ns.warsaw.recomp2425m1b05.recomp.com
6	ns.warsaw.recomp2425m1b05.recomp.com	A Record	192.168.100.2
7	oporto.recomp2425m1b05.recomp.com	A Record	192.168.5.4
8	ns.recomp2425m1b05.recomp.com	A Record	192.168.5.2
9	iot.recomp2525m1b05.recomp.com	A Record	192.168.5.6
10	www.iot.recomp2525m1b05.recomp.com	CNAME	iot.recomp2425m1b05.recomp.com
11	mail.recomp2425m1b05.recomp.com	A Record	192.168.5.5
12	www.porto.recomp2425m1b05.recomp.com	CNAME	oporto.recomp2425m1b05.recomp.com

DNS configuration in Warsaw

Because of the addition of subnetwork 192.168.100.5/27, we had to modify the router configuration. The server was attributed IP address of 192.168.100.2.

Warsaw

```
interface GigabitEthernet0/1
ip address 192.168.100.1 255.255.255.224
ip access-group 101 in
ip nat inside

router ospf 1
network 192.168.100.5 0.0.0.31 area 2
```

In Warsaw branch, DNS configuration included setting the warsaw.recomp2425m1b05.recomp.com domain to resolve to the IP address 192.168.100.2. Additionally, the www.warsaw.recomp2425m1b05.recomp.com CNAME record was created to redirect to the main warsaw.recomp2425m1b05.recomp.com domain. The website is hosted on another

No.	Name	Type	Detail
0	.	NS	ns
1	ns	A Record	192.168.5.2
2	warsaw.recomp2425m1b05.recomp.com	NS	ns.warsaw.recomp2425m1b05.recomp.com
3	warsaw.recomp2425m1b05.recomp.com	A Record	192.168.100.2
4	www.warsaw.recomp2425m1b05.recomp.com	CNAME	warsaw.recomp2425m1b05.recomp.com

DNS configuration in Munich

The server was put in a subnetwork 192.168.200.5/27.

Munich

```
interface GigabitEthernet0/1
ip address 192.168.200.1 255.255.255.224
ip access-group 101 in
ip nat inside

router eigrp 1
network 92.168.200.5 0.0.0.31
```

In the Munich branch, the DNS configuration included setting the munich.recomp2425m1b05.recomp.com domain to resolve to the IP address 192.168.200.2. A CNAME record was also added for the www.munich.recomp2425m1b05.recomp.com domain, pointing to the main munich.recomp2425m1b05.recomp.com domain.

No.	Name	Type	Detail
0	.	NS	ns
1	munich.recomp2425m1b05.recomp.com	NS	ns.munich.recomp2425m1b05.recomp.com
2	munich.recomp2425m1b05.recomp.com	A Record	192.168.200.2
3	ns	A Record	192.168.5.2
4	www.munich.recomp2425m1b05.recomp.com	CNAME	munich.recomp2425m1b05.recomp.com

IoT

Porto

To ensure proper functioning of IoT devices we had to configure layer 2 and both layer 3 switches.

SW4

```
interface FastEthernet0/21
switchport access vlan 101
switchport mode access
```

The interface FastEthernet0/21 on switch SW4 is configured for VLAN 101 in access mode, allowing it to connect to IoT devices.

MLS1	MLS2

```
ip dhcp excluded-address 10.27.71.225
10.27.71.226

ip dhcp pool VLAN101-IOT
network 10.27.71.224 255.255.255.240
default-router 10.27.71.225
dns-server 192.168.5.2
domain-name RECOMP2425M1B05

interface Vlan101
mac-address 0001.42ce.8006
ip address 10.27.71.225 255.255.255.240

router ospf 1
network 10.27.71.224 0.0.0.15 area 1
```

```
ip dhcp excluded-address 10.27.71.225
10.27.71.226

ip dhcp pool VLAN101-IOT
network 10.27.71.224 255.255.255.240
default-router 10.27.71.226
dns-server 192.168.5.2
domain-name RECOMP2425M1B05

interface Vlan101
mac-address 0001.42ce.8006
ip address 10.27.71.225 255.255.255.240

router ospf 1
network 10.27.71.224 0.0.0.15 area 1
```

In the MLS1 and MLS2 configuration, IP addresses 10.27.71.225 and 10.27.71.226 are excluded from the DHCP pool to avoid conflicts. A DHCP pool for VLAN101 is created with network 10.27.71.224/28, default router 10.27.71.225, and DNS server 192.168.5.2. The VLAN101 interface is configured with a specific MAC address and IP address 10.27.71.225/28. The network 10.27.71.224/28 is added to OSPF area 1 for routing.

Warsaw

Similar configurations were applied in the Warsaw branch, focusing primarily on the router.

Warsaw

```
ip dhcp excluded-address 192.168.100.33

ip dhcp pool VLAN101-IOT
network 192.168.100.32 255.255.255.224
default-router 192.168.100.33
dns-server 192.168.100.2

interface GigabitEthernet0/0.101
encapsulation dot1Q 101
ip address 192.168.100.33 255.255.255.224

router ospf 1
network 192.168.100.32 0.0.0.31 area 2
```

In the Warsaw router configuration, IP address 192.168.100.33 is excluded from the DHCP pool. A DHCP pool for VLAN101 is created with network 192.168.100.32/27, default router 192.168.100.33, and DNS server 192.168.100.2. The GigabitEthernet0/0.101 sub-interface is configured with dot1Q encapsulation for VLAN 101 and IP address 192.168.100.33/27. The network 192.168.100.32/27 is added to OSPF area 2.

SW1 (Warsaw)

```
interface FastEthernet0/21
switchport access vlan 101
switchport mode access
```

The FastEthernet0/21 interface on SW1 is configured for VLAN 101 in access mode.

Munich

Similarly, configurations were applied in the Munich branch for both the router and switch to enable IoT devices.

Munich

```
ip dhcp excluded-address 192.168.200.33

ip dhcp pool VLAN101-IOT
network 192.168.200.32 255.255.255.224
default-router 192.168.200.33
dns-server 192.168.200.2

interface GigabitEthernet0/0.101
encapsulation dot1Q 101
ip address 192.168.200.33 255.255.255.224

router eigrp 1
network 192.168.200.32 0.0.0.31
```

In the Munich router configuration, IP address 192.168.200.33 is excluded from the DHCP pool. A DHCP pool for VLAN101 is created with network 192.168.200.32/27, default router 192.168.200.33, and DNS server 192.168.200.2. The GigabitEthernet0/0.101 sub-interface is configured with dot1Q encapsulation for VLAN 101 and IP address 192.168.200.33/27. The network 192.168.200.32/27 is added to EIGRP 1 for routing.

SW1 (Munich)

```
interface FastEthernet0/21
switchport access vlan 101
switchport mode access
```

The FastEthernet0/21 interface on SW1 is configured for VLAN 101 in access mode.

QoS Oporto

1. Routing - To match any dynamic routing traffic (EIGRP, OSPF) that could be generated in the network.

Router Oporto:
class-map match-any ROUTING
match protocol eigrp
match protocol ospf

2. Protocols - To match any DNS, FTP, SMTP or POP3 traffic that could be generated in the network.

Router Oporto:
class-map match-any PROTOCOLS
match protocol DNS
match protocol FTP
match protocol SMTP
match protocol POP3

3. Accounting- To match any traffic coming from the accounting network.

Router Oporto:
Ip access-list standard accountingacl
permit 10.27.70.0 0.0.0.255
deny any

class-map match-any ACCOUNTING
match access-group name accountingacl

4. AccountingHTTPS - To match all traffic coming from the accounting network and matching the HTTPS protocol.

Router Oporto:
Ip access-list standard accountingacl
permit 10.27.70.0 0.0.0.255
deny any

class-map match-all ACCOUNTINGHTTPS

match access-group name accountingacl
match protocol https

5. HR - To match any traffic coming from the HR network.

Router Oporto:
Ip access-list standard hracl
permit 10.27.71.0 0.0.0.127
deny any

class-map match-any HR
match access-group name hracl

6. Staff - To match any traffic coming from the staff network.

Router Oporto:
Ip access-list standard staffacl
permit 10.27.71.128 0.0.0.63
deny any

class-map match-any STAFF
match access-group name staffacl

7. Staff-HTTP - To match any traffic coming from the staff network.

Router Oporto:
class-map match-all STAFFHTTP
match access-group name staffacl
match protocol http

8. Users - To match any traffic coming from the staff network.

Router Oporto:
Ip access-list standard usersacl
permit 10.27.68.0 0.0.1.255
deny any

class-map match-any USERS
match access-group name usersacl

9. Default - To handle all traffic that doesn't match the criteria of the previous groups

No configuration needed for default.

Traffic Shaping

Router Oporto:

```
policy-map OPORTOPOLICY
class ROUTING
set ip dscp ef
class PROTOCOLS
set ip dscp af11
class ACCOUNTING
set ip dscp af11
class ACCOUNTINGHTTPS
set ip dscp af11
class HR
set ip dscp af32
class STAFF
set ip dscp af11
class STAFFHTTP
set ip dscp af11
class USERS
set ip dscp af32
class class-default
set ip dscp af21

interface g0/0/0
service-policy output OPORTOPOLICY
```

On the Warsaw and Munich routers the following configurations need to be applied:

```
class-map match-any ROUTING
match ip dscp ef
class-map match-any PROTOCOLS
match ip dscp af11
class-map match-any ACCOUNTING
match ip dscp af11
class-map match-all ACCOUNTINGHTTPS
match ip dscp af11
class-map match-any HR
```

match ip dscp af32
class-map match-any STAFF
match ip dscp af11
class-map match-any STAFFHTTP
match ip dscp af11
class-map match-any USERS
match ip dscp af32
class-map match-all class-default
match ip dscp af32

policy-map WAROPOSHAPING/ policy-map MUNOPOSHAPING
class ROUTING
priority percent 20

class PROTOCOLS
bandwidth remaining percent 50
random-detect dscp-based

class ACCOUNTINGHTTPS
bandwidth remaining percent 50
random-detect dscp-based

class ACCOUNTING
bandwidth remaining percent 50
random-detect dscp-based

class STAFFHTTP
bandwidth remaining percent 50
random-detect dscp-based

class STAFF
bandwidth remaining percent 50
random-detect dscp-based

class HR
bandwidth remaining percent 50
random-detect dscp-based

class USERS
bandwidth remaining percent 50
random-detect dscp-based

class class-default
fair-queue
random-detect

interface g0/1
service-policy input WAROPOSHAPING/ service-policy output MUNOPOSHAPING
interface g0/0
service-policy input WAROPOSHAPING/ service-policy output MUNOPOSHAPING

QoS Warsaw

1. Routing - To match any dynamic routing traffic (EIGRP, OSPF) that could be generated in the network.

Router Warsaw:
class-map match-any ROUTING
match protocol eigrp
match protocol ospf

2. Protocols - To match any DNS, FTP, SMTP or POP3 traffic that could be generated in the network.

Router Warsaw:
class-map match-any PROTOCOLS
match protocol DNS
match protocol FTP
match protocol SMTP
match protocol POP3

3. Accounting- To match any traffic coming from the accounting network.

Router Warsaw:
Ip access-list standard accountingacl
permit 192.168.155.0 0.0.0.255
deny any

class-map match-any ACCOUNTING
match access-group name accountingacl

4. AccountingHTTPS - To match all traffic coming from the accounting network and matching the HTTPS protocol.

Router Warsaw:
class-map match-all ACCOUNTINGHTTPS
match access-group name accountingacl
match protocol https

5. Users - To match any traffic coming from the staff network.

Router Warsaw:
Ip access-list standard usersacl
permit 192.168.154.0 0.0.0.255
deny any

class-map match-any USERS
match access-group name usersacl

6. Default - To handle all traffic that doesn't match the criteria of the previous groups

No configuration needed for default.

Traffic Shaping

Router Warsaw:
policy-map WARSAWPOLICY
class ROUTING
set ip dscp ef
class PROTOCOLS
set ip dscp af11
class ACCOUNTING
set ip dscp af11
class ACCOUNTINGHTTPS
set ip dscp af11
class USERS
set ip dscp af32
class class-default
set ip dscp af21

```
interface g0/0/0
service-policy output WARSAWPOLICY
```

On the Oporto and Munich routers the following configurations need to be applied:

```
class-map match-any ROUTING
match ip dscp ef
class-map match-any PROTOCOLS
match ip dscp af11
class-map match-any ACCOUNTING
match ip dscp af11
class-map match-all ACCOUNTINGHTTPS
match ip dscp af11
class-map match-any USERS
match ip dscp af32
class-map match-all class-default
match ip dscp af21

policy-map OPOWARSHAPING/ policy-map MUNWARSHAPING
class ROUTING
priority percent 20

class PROTOCOLS
bandwidth remaining percent 30
random-detect dscp-based

class ACCOUNTINGHTTPS
bandwidth remaining percent 50
random-detect dscp-based

class ACCOUNTING
bandwidth remaining percent 50
random-detect dscp-based

class USERS
bandwidth remaining percent 50
random-detect dscp-based

class class-default
fair-queue
random-detect
```

interface g0/1
service-policy input OPOWARSHAPING / service-policy output MUNWARSHAPING
interface g0/0
service-policy input OPOWARSHAPING / service-policy output MUNWARSHAPING

QoS Munich

1. Routing - To match any dynamic routing traffic (EIGRP, OSPF) that could be generated in the network.

Router Munich:
class-map match-any ROUTING
match protocol eigrp
match protocol ospf

2. Protocols - To match any DNS, FTP, SMTP or POP3 traffic that could be generated in the network.

Router Munich:
class-map match-any PROTOCOLS
match protocol DNS
match protocol FTP
match protocol SMTP
match protocol POP3

3. Staff - To match any traffic coming from the staff network.

Router Munich:
Ip access-list standard staffacl
permit 172.21.73.0 0.0.0.255
deny any

class-map match-any STAFF
match access-group name staffacl

4. Staff-HTTP - To match all traffic coming from the staff network and matching the HTTP protocol.

Router Munich:
class-map match-all STAFFHTTP
match access-group name staffacl
match protocol http

5. Users - To match any traffic coming from the staff network.

Router Munich:
Ip access-list standard usersacl
permit 172.21.72.0 0.0.0.255
deny any

class-map match-any USERS
match access-group name usersacl

6. Default - To handle all traffic that doesn't match the criteria of the previous groups

No configuration needed for default.

Traffic Shaping

Router Munich:
policy-map MUNICHPOLICY
class ROUTING
set ip dscp ef
class PROTOCOLS
set ip dscp af11
class STAFF
set ip dscp af11
class STAFFHTTP
set ip dscp af11
class USERS
set ip dscp af32
class class-default
set ip dscp af21

interface g0/0/0
service-policy output MUNICHPOLICY

On the Oporto and Warsaw routers the following configurations need to be applied:
class-map match-any ROUTING
match ip dscp ef
class-map match-any PROTOCOLS
match ip dscp af11
class-map match-any STAFF
match ip dscp af11
class-map match-all STAFFHTTP
match ip dscp af11

```
class-map match-any USERS
match ip dscp af32
class-map match-all class-default
match ip dscp af21

policy-map OPOMUNSHAPING/ policy-map WARMUNSHAPING
class ROUTING
priority percent 20

class PROTOCOLS
bandwidth remaining percent 20
random-detect dscp-based

class STAFFHTTP
bandwidth remaining percent 50
random-detect dscp-based

class STAFF
bandwidth remaining percent 50
random-detect dscp-based

class USERS
bandwidth remaining percent 50
random-detect dscp-based

class class-default
fair-queue
random-detect

interface g0/1
service-policy input OPOMUNSHAPING / service-policy output WARMUNSHAPING
interface g0/0
service-policy input OPOMUNSHAPING / service-policy output WARMUNSHAPING
```

QoS Clarification

In order to avoid redundancy in explanation, this section is used to detail the reasoning behind the QoS configuration in each of the routers.

A class map is defined through the “class-map [match type] [Name]” command. This defines that traffic corresponding to matches defined below it is classified into the class-map. The match type match-any specifies that any match condition satisfied is enough to match, while match-all requires that every condition needs to be satisfied to match.

To create a group matching a specific traffic type, like the dynamic routing traffic or a specific protocols traffic described in the ROUTING and PROTOCOLS groups for example, the command “match protocol [name of protocol]” is used.

To match a group from a given network, like in the STAFF or ACCOUNTING or STAFFHTTP and ACCOUNTINGHTTPS, it is first required to create an ACL for that specific network. Then, the command “match access-group name [ACL Name]” can be used to match the incoming traffic into the class map.

In order to create/modify a policy map using the created class maps, the command “policy-map [Name]” was used. Below it, each of the created class maps are set using the command “class [Name of existing class map]”, followed by the command “set ip dscp [dscp value]”, to determine the priority of the traffic, values EF (Expedited forwarding) for high priority, af11 (Assured Forwarding) for low drop probability, af21 for medium drop probability and af32 for lower priority traffic.

For incoming traffic, class maps were created to match the dscp traffic type, using the command “match ip dscp [value]”. Then, a policy map was created, configuring each class map’s priority traffic, using the command “priority percent [value]” to determine the priority traffic percentage in the case of the first class, and the commands “bandwidth remaining percent [value]” and “random-detect dscp-based”, the first command to configure the percentage of traffic from the remaining traffic not already configured, and the second one to manage congestion through selectively dropping packets based on their dscp value. Finally, class-default handles traffic not matched in the other class maps, using the “fair-queue” command to distribute resources evenly between traffic types, and “random-detect” to manage congestion with no given focus (unlike “dscp-based”).

In order to apply the service-policy into outwards traffic, the command “service-policy output [Policy Name]” is applied. For inwards traffic, we use the same command with input instead of output.

Security Issues

DNS vulnerabilities

The DNS configuration detailed in this work could lead to a few particular vulnerabilities, like DNS Spoofing, DDoS attacks, DNS Tunneling or Hijacking. To mitigate these issues, DNSSEC technology could be installed in the routers.

DNCSEC, meaning DNS Security is a collection of security protocols to protect the integrity and authenticity of DNS traffic, through implementation of digital signatures to DNS records, ensuring integrity and authenticity of data.

DHCP Snooping

In order to defend DHCP attacks, DHCP snooping can be implemented, to ensure only trusted ports can use the DHCP functionality. In order to do this, the following commands should be performed in each switch:

```
ip dhcp snooping
interface range f0/x-y
ip dhcp snooping trust
interface range f0/w-z
no ip dhcp snooping trust
no ip dhcp snooping information option
```

With x-y being the range of trusted ports and w-z the range of not trusted ports.

Security for Devices and Services

Centralized services such as DNS, FTP, HTTP and IoT can present significant vulnerabilities and can become potential attack if not properly secured. To mitigate these risks, the following measures should be implemented:

DNS Security (DNSSEC)

For DNS service, we can protect DNS queries and responses from spoofing and cache poisoning attacks by using the DNSSEC which ensures data integrity and authenticity by using cryptographic signatures.

Secure FTP and HTTP Services

For HTTP services, we can enforce the use of HTTPS (TLS/SSL encryption) to secure data in transit and prevent man-in-the-middle attacks.

For FTP services, we can enforce the use of FTPS (FTP Secure) to encrypt file transfers.

Service Monitoring and Logging

Service monitoring and logging are critical components of a secure and reliable network infrastructure. They ensure the detection of potential security threats, enable system health analysis, and support troubleshooting. For practical implementation, centralized logging and secure monitoring solutions must be deployed across the entire infrastructure.

IoT Device Isolation

Internet of things (IoT) devices while offering immense functionality, often present significant security risks, placing IoT devices in a dedicated VLAN and applying Access Control List (ACLs) to restrict communication and disable unused ports or services on IoT devices to minimize attack surfaces are critical measures to improve network security while maintaining network performance and compliance.

IoT Device Isolation improves network security by:

- Containing security risks associated with IoT devices.
- Preventing attackers from moving laterally across the network.
- Reducing the attack surface by disabling unused ports/services.
- Ensuring compromised devices have limited impact on critical systems.

By implementing these measures, the network can ensure the confidentiality, integrity, and availability of critical services, while minimizing potential vulnerabilities and attack surfaces.

Conclusion

The conclusion of Sprint 3 of the RECOMP project reflects the application of advanced networking techniques to meet the requirements of a modern corporate infrastructure. The implementation of the DMZ, the configuration of services such as DNS, FTP, and HTTP, and the security measures adopted illustrate the commitment to best practices in network administration. Furthermore, the use of protocols such as OSPF and the integration of QoS demonstrate the ability to optimize the network's performance and reliability. Through this project, it was possible to consolidate essential technical skills, preparing participants for real-world challenges in networking and cybersecurity.