First Project
Networks Architecture and Management

Authors: Filipe Pires [85122] & João Alegria [85048]
Teaching Staff: António Nogueira

Table of Contents

Introduction

With the expantion of XPTO Lda in Aveiro, an engineering services company in the area of IoT (Internet of Things), and its creation of a new branch in Porto, a set of challenges have rizen regarding the internal networks. Our job as network engineers for this project was to analyse the current state of the company's infrastructures' architecture, plan the integration of the new building in Aveiro and assure the quality and security of the whole network, including the connection between branches.

This project assignment was proposed by professor António Nogueira of the Department of Electronics, Telecommunications and Informatics within the scope of the Networks Architecture and Management subject, belonging to the bachelor's degree in Informatics Engineering. The main goal was to learn, in a practical manner, the processes around executing a technical design, configuration and test of a telecommunications network. The case study is a fictitious company and the actual application of the content present in this report was done through the network software simulator GNS3 in a small scale.

The structure of this report is present on the first page's Table of Contents. Our work focuses on presenting the results of the entire network analysis and the expansion planning, along with detailed explanations for the reasons of our decisions. Visual aid is presented whenever appropriate and possible and it is assumed that the reader has knowledge about the content of this assignment's instructions (1).

1. Network Architecture

In this first chapter we discuss the architecture chosen for company XPTO's new infrastructures.
After considering several factors we adopted a hybrid topology, as we belive to be the best fit for the company's case. This hybrid topology consists in a Tree topology, where the Core Switches Layer 3 (SWL3) work as the root nodes, combined with a Mesh topology, where the devices of a department are all connected to each other (2). Figure 1 helps the reader understand this.
It is important to state that this network planning is not fully mesh-based, as there is no parallel connection between redundant SWL3 (e.g. Core1 and Core2, or New1 and New2) and therefore the total number of physical channels to link n devices is not equal to n(n-1)/2. The purpose of our decision is simply to make sure that the network keeps working in case of local failures. This is more visible inside subnetworks such as the New Datacenter.
Regarding the tree-based approach, we found it appropriate since a hierarchy makes the network easier to manage and reduces the points in need of defence against outside threats. As mentioned before, the Core SWL3 are the root nodes of the network tree and the switches, terminals and storage units are considered the tree leafs.

1.1. Logical Network

Figure 1 is the diagram that aims to represent the network under the layer 3 of the OSI model. Here are present the Routers, SWL3s and also Switches Layer 2 (though not frequently present in this sort of diagrams, but used for visualization purposes). The Logical Network Diagram also shows the VLANs created, the subnets and respective masks and the IP addresses (3).

The entire network is configured with OSPF. The reason we adopted this protocol was that it helped maintain the simplicity of configurations while allowing fast internal communications. We distributed OSPF areas according to the logical and physical distribution of the new facilities. I.E. each department and building would have a dedicated OSPF area. The backbone (area 0) is, as one may imagine, the one with the Core SWL3, and the remaining areas are named after the VLAN they hold (Datacenter and DMZ) or with a symbolic value ease to recall (New Building). This keeps the network organized.
All connections are configured as trunk – meaning that they are prepared to carry data from multiple LANs or VLANs across a single interconnect between switches or routers. However, we applied restrictions to each link allowing only a specific set of VLANs to pass packets. The allowed VLANs are: 1, the default one; 1002-1005, Cisco's default ones; and the specific interconnect VLANs. We decided to do so as this strategy offers more security to the network and allows the possibility of easily adding more VLANs to the list.
As the reader can observe in the diagram, the connection between the entry points on both company sites and the ISP 1 have one IPSec VPN tunnel configured. This tunnel exists to provide a secure and direct connected between company sites. More about this is described in chapter 3.
Since it was not very ease to represent the application of a Wi-Fi connection for the entire Aveiro facility, we decided to do so by placing the VLAN dedicated for that job over the New Building icon – this has the intent to pass the idea that the VLAN will be available for the entire network and can be accessed anywere inside the building. This VLAN was configured in the following SWL3: Cores, DMZ, NewBuildings, NewDatacenter.
VLAN configurations are discussed in section 1.3 and the IP addressing decisions described in chapter 2.

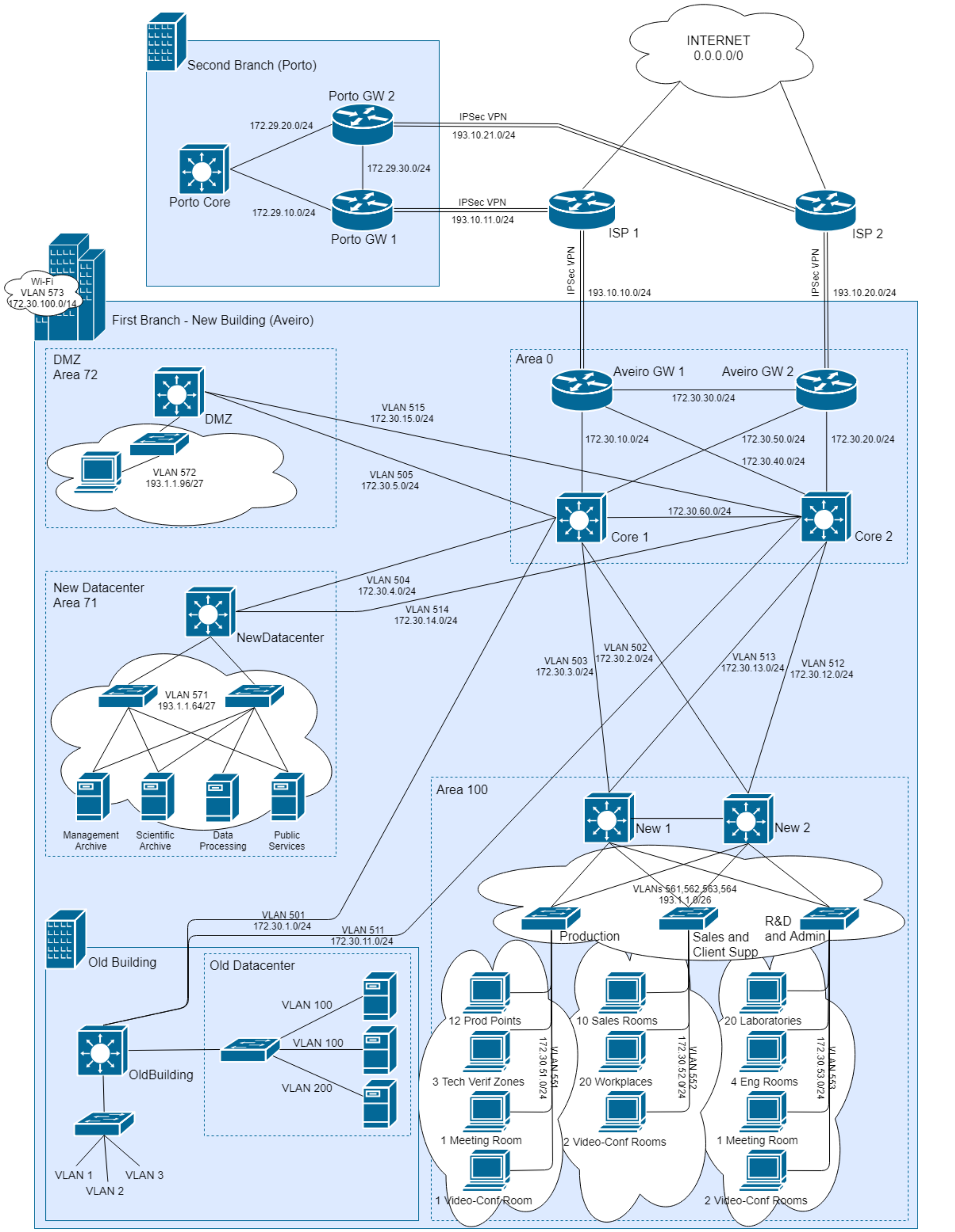

Figure 1: Logical Network Diagram (4).

1.2. Physical Mapping

Figure 2, on the other hand, shows the physical network diagram of XPTO's new infrastructures. Here, we enter in a more technical visualization of the network, as it is a useful asset to visually document the physical connections on the network for the company's IT staff. The focus here is on which ports are used by each device and what is the exact topology of the physical links between the devices.
As it is easy to understand, the figure is a screenshot taken from a virtual representation of the network made inside GNS3. This representation is a simplified version of the network for performance reasons but it is still configured to deal with most of the real network's complexity.

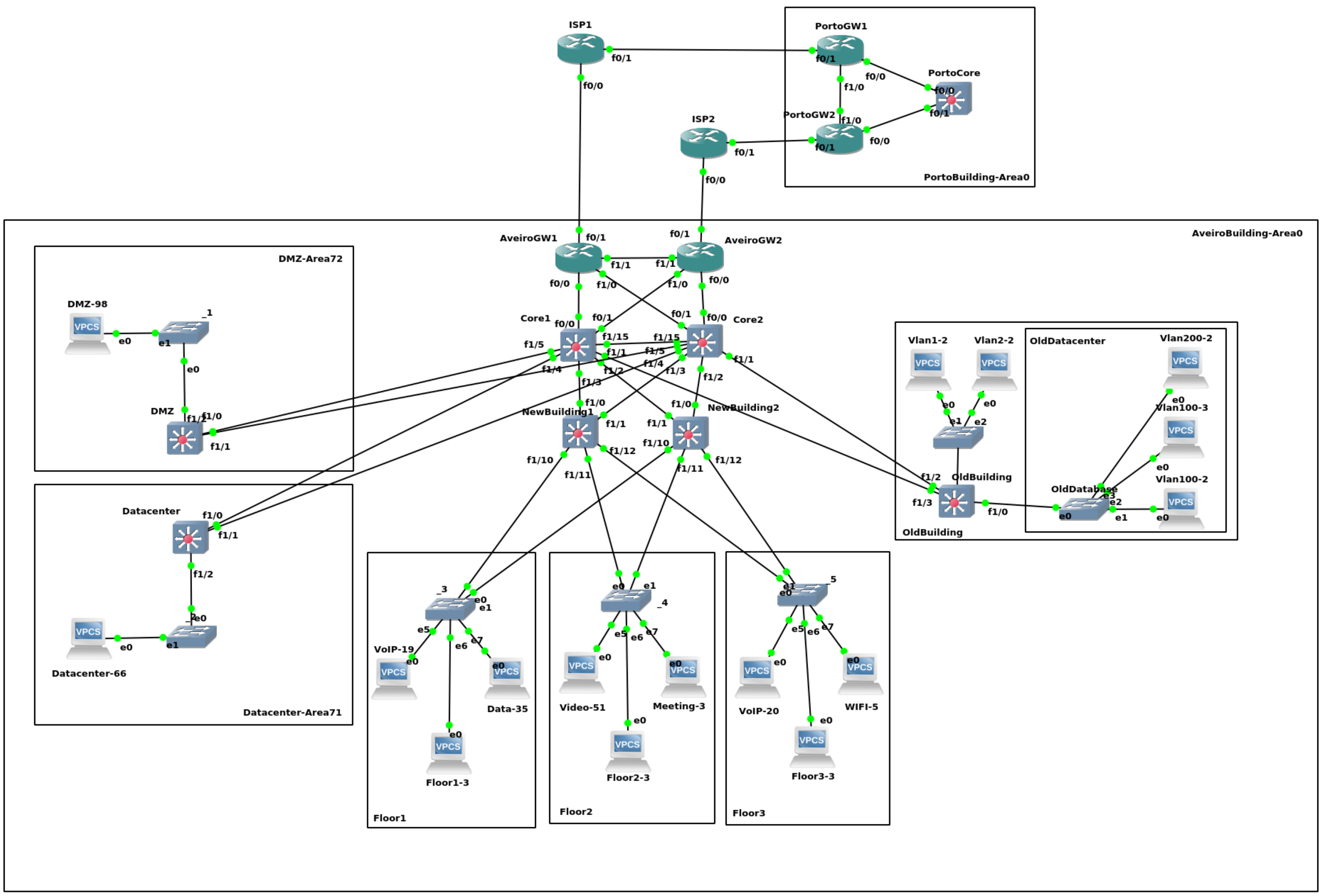

Figure 2: Physical Network Diagram.

A physical mapping such as the one on the figure usual gives the information about how are the devices physically connected. However, as it was a detail not directly linked to our project, we decided to avoid adding unnecessary complexity to the diagram. Nevertheless we decided to still address the issue without great depth.
As the new building will reuse the old infrastructures, we believe that a hybrid strategy would be the best solution, combining copper cables potentially already installed with new fiber optics capable of dealing with larger amounts of data flows and packet transitions. Regarding wireless communications, the ideal would be to follow the IEEE 802.11 standard.

1.3. Local Networks

The table presented below shows the definition of the virtual local networks created for the company's new infrastructures. The names given to them have a simple structure for reading purposes and many are related to the IP addresses used within them (e.g. VLAN 503 holds the subnetwork 172.30.3.0/24 , 2002:A:A:3:: / 64). The reason we adopted the use of many VLANs was that it made the configurations more dynamic and it enabled the logical grouping of end-stations physically dispersed on the network.

VLAN	Subnet
1, 2, 3	Old Building
100, 200	Old Datacenter
501	Core1 - Old Building
502	Core1 - New Building 2
503	Core1 - New Building 1
504	Core1 - New Datacenter
505	Core1 - DMZ
511	Core2 - Old Building
512	Core2 - New Building 2
513	Core2 - New Building 1
514	Core2 - New Datacenter
515	Core2 - DMZ
551	1st Floor
552	2nd Floor
553	3rd Floor
561	Voice Services over IP
562	Data Services over IP
563	Video Services over IP (video-conf. Rooms)
564	Meeting Rooms (meetings, reception, lounge, etc.)
571	New Datacenter
572	DMZ
600	Wi-Fi

2. Addresses Definition and Configuration

The analysis of the requirements for the expansion of the company lead us to carefully distribute all IP addresses the best possible way. In many of the subnetworks we left some room for further expansion, preventing the company from having to refactor the address configuration in case of necessity.

2.1. Addressing Schemes

Below are presented 3 addressing tables developed by us and followed during the configuration and testing of the entire network. These tables are useful to understand the distribution of addresses throughout each section.

IP Tables

The public IPv4 addresses were distributed as follows:

Public IPv4 Address / Mask	Subnet
193.1.1.0 / 28	Meeting Rooms (meetings, reception, lounge, etc.)
193.1.1.16 / 28	Voice Services over IP
193.1.1.32 / 28	Data Services over IP
193.1.1.48 / 28	Video Services over IP (video-conf. Rooms)
193.1.1.64 / 27	New Datacenter
193.1.1.96 / 27	DMZ
193.1.1.128 / 25	NAT
193.10.10.0 / 24	AveiroGW1 - ISP1
193.10.11.0 / 24	PortoGW1 - ISP1
193.10.20.0 / 24	AveiroGW2 - ISP2
193.10.21.0 / 24	PortoGW2 - ISP2

The private IPv4 addresses follow the same class as the IPs assigned in the old building. All new private addresses start with 172.30.X.Y, where X is the subnet identifier and Y is the id of a terminal from the subnet. Each subnetwork will then have 255 IPs available for internal communications.

Private IPv4 Address / Mask	Subnet
172.29.10.0 / 24	PortoCore - PortoGW1
172.29.20.0 / 24	PortoCore - PortoGW2
172.29.30.0 / 24	PortoGW1 - PortoGW2
172.30.1.0 / 24	Core1 - OldBuilding
172.30.2.0 / 24	Core1 - NewBuilding2
172.30.3.0 / 24	Core1 - NewBuilding1
172.30.4.0 / 24	Core1 - Datacenter
172.30.5.0 / 24	Core1 - DMZ
172.30.10.0 / 24	Core1 - AveiroGW1
172.30.11.0 / 24	Core2 - OldBuilding
172.30.12.0 / 24	Core2 - NewBuilding2
172.30.13.0 / 24	Core2 - NewBuilding1
172.30.14.0 / 24	Core2 - Datacenter
172.30.15.0 / 24	Core2 - DMZ
172.30.20.0 / 24	Core2 - AveiroGW2
172.30.30.0 / 24	AveiroGW1 - AveiroGW2
172.30.40.0 / 24	AveiroGW1 - Core2
172.30.50.0 / 24	AveiroGW2 - Core1
172.30.60.0 / 24	Core1 - Core2
172.30.51.0 / 24	1st Floor
172.30.52.0 / 24	2nd Floor
172.30.53.0 / 24	3rd Floor
172.30.100.0 / 24	Wi-Fi

IPv6 were distributed with a similar strategy of the one used for the IPv4 private addresses. Internal addresses start with 2002:A:A:X::Y (or 2002:B:B:X::Y, for the Porto site), where X is the subnet identifier and Y is the id of a terminal. The first addresses are dedicated to the external communications through IPv6.

IPv6 Address / Mask	Subnet
A:A:A:10:: / 64	AveiroGW1 - ISP1
A:A:A:20:: / 64	AveiroGW2 - ISP2
A:A:A:11:: / 64	PortoGW1 - ISP1
A:A:A:21:: / 64	PortoGW2 - ISP2
2002:A:A:1:: / 64	Core1 - OldBuilding
2002:A:A:2:: / 64	Core1 - NewBuilding2
2002:A:A:3:: / 64	Core1 - NewBuilding1
2002:A:A:4:: / 64	Core1 - Datacenter
2002:A:A:5:: / 64	Core1 - DMZ
2002:A:A:10:: / 64	Core1 - AveiroGW1
2002:A:A:11:: / 64	Core2 - OldBuilding
2002:A:A:12:: / 64	Core2 - NewBuilding2
2002:A:A:13:: / 64	Core2 - NewBuilding1
2002:A:A:14:: / 64	Core2 - Datacenter
2002:A:A:15:: / 64	Core2 - DMZ
2002:A:A:20:: / 64	Core2 - AveiroGW2
2002:A:A:30:: / 64	AveiroGW1 - AveiroGW2
2002:A:A:51:: / 64	1^{st} Floor
2002:A:A:52:: / 64	2^{nd} Floor
2002:A:A:53:: / 64	3^{rd} Floor
2002:A:A:60:: / 64	Core1 - Core2
2002:A:A:61:: / 64	Voice Services over IP
2002:A:A:62:: / 64	Data Services over IP
2002:A:A:63:: / 64	Video Services over IP (video-conf. Rooms)
2002:A:A:64:: / 64	Meeting Rooms (meetings, reception, lounge, etc.)
2002:A:A:71:: / 64	New Datacenter
2002:A:A:72:: / 64	DMZ
2002:A:A:100:: / 64	Wi-Fi
2002:B:B:10:: /64	PortoCore - PortoGW1
2002:B:B:20:: /64	PortoCore - PortoGW2
2002:B:B:30:: / 64	PortoGW1 - PortoGW2

IP Configuration

Here we present an example of the configurations applied to the network. The following commands were executed in Core 1 and in Aveiro Gateway 1 and reffer to the interfaces f1/3 and f0/1 respectively, responsible for communications between Core 1 and New Building 1 and Aveiro Gateway 1 and ISP 1, respectively.
The configuration of Core 1's interface is similar to the ones with the remaining internal areas (DMZ, Datacenter, etc.), and these are also executed (with adjustments) in Core 2. Whereas the Gateway's interface configuration is meant to show the differences in commands for the outside communications.

```
# Core 1

conf t
ip routing
ipv6 unicast-routing
ip cef
end

conf t
int f1/3
switchport mode trunk
switchport trunk allowed vlan 1,503,1002-1005
interface Vlan503
ip address 172.30.3.1 255.255.255.0
ipv6 address 2002:A:A:3::1/64
no shut
no autostate
end
write
```

```
# Aveiro GW 1

conf t
ipv6 unicast-routing
int f0/1
ip address 193.10.10.2 255.255.255.0
ipv6 address A:A:A:10::2/64
no shut
end
write
```

2.2. Routing Configuration and Transition Mechanisms

Regarding the configurations of the routing inside the network, as it has been previously mentioned, we made OSPF the elected protocol. The fact that it has no limitations in hop counts and has better load balancing made it an appropriate choice to the new infrastructures of XPTO. For IPv6 we used OSPFv3.
As the old infrastructures had RIP implemented, we configured a translation mechanism between the new devices and the old one.
The following commands are the ones we ran to configure the protocol throughout the network. Here are only a few examples, as they repeat themselves often, changing only a few details. We also include the commands executed in the Core SWL3 for the RIP-to-OSPF translation.

```
# Core1

conf t
ipv6 router ospf 1
router-id 1.1.1.1
int f0/0
ip ospf 1 area 0
ipv6 ospf 1 area 0
end

conf t
router rip
version 2
no auto-summary
redistribute ospf 1 metric 10
network 172.30.1.0
network 172.30.2.0
network 172.30.3.0
network 172.30.4.0
network 172.30.5.0
exit
router ospf 1
redistribute rip metric 10 subnets
end
write
```

2.3. Private Addressing Translation Mechanisms

Network Address Translation is an essential tool in every private network. The NAT protocol offers a simple way of assigning public addresses to terminals inside an organization or company. As the reader has seen in tables previously mentioned, our private address range was 172.30.0.0 for the new infrastructures and we kept the 172.31.0.0 range for the old infrastructures. The main purpose of the use of this protocol was to allow terminals inside the network to access resources outside of it and receive responses from the destinations.
Source NAT was brought to the matter as the protocol had to be configured in more than one device. SNAT allowed us to ensure the IP translation of all packets, even in case of local failures.
Once again, we present a few lines of commands executed during the configuration of the network.

```
# Aveiro GW 1

conf t
int f0/0
ip nat inside
int f0/1
ip nat outside
end

conf t
access-list 1 permit 172.30.0.0 0.0.255.255
access-list 1 permit 172.31.0.0 0.0.255.255
ip nat pool POOLR 193.1.1.128 193.1.1.255 netmask
255.255.255.128
ip nat Stateful id 3
primary 172.30.10.1
peer 172.30.20.1
mapping-id 10
end
conf t
ip nat inside source list 1 pool POOLR mapping-id 10
overload
end
write
```

3. QoS and Security

3.1. Quality of Service Policies

As the dimension of the company is increased in great scale, the need to treat different traffics in different ways became one of our priorities. To do so, we created 2 traffic classes, which are assigned to every packet and define how should the network deal with them in terms of response delay, bandwidth and priority.

These were the characteristics and requirements defined for each class:
- **Premium**: used for VoIP; will be marked with a DSCP value of 46 (EF).
- **Best-Effort**: used all remaining traffic.
- The premium class should be forwarded with the lowest delay possible up to a maximum of 40% of the link bandwidth during periods of congestion.
- Best-effort class should be policed to 16 kbps.

In order to classify traffic into the different classes, 1 extended access lists was defined at SWL3 NewBuildings. We tested the performance of our solution by establishing a connection between a VoIP terminal and the ouside world.
Following is the code executed when configuring the access lists and defining the classes.

```
# NewBuilding1

conf t
access-list 101 permit ip 193.1.1.16 0.0.0.15 any
access-list 101 deny ip any any
class-map match-all EF
match access-group 101
exit
policy-map SETDSCP
class EF
set ip dscp 46
end
conf t
class-map match-all PREMIUM
match ip dscp 46
exit
class-map match-all BEST-EFFORT
match ip dscp 0
end
conf t
policy-map EDGE
class PREMIUM
priority percent 40
class BEST-EFFORT
police 16000 2000 2000 conform-action set-dscp-transmit
0
end
write
conf t
int vlan503
service-policy output EDGE
int vlan513
service-policy output EDGE
int vlan561
service-policy input SETDSCP
end
write
```

3.2. Secure Connection Configuration

Although security was not the focus of this project, an important aspect of it was a requisite for the final solution: establishing a secure connection between the two company sites, Aveiro and Porto. The most appropriate way to do so was to configure a site-to-site communication tunnel where transfered packets are encrypted – an IPSec VPN Tunnel. Although only one VPN was configured, two tunnels were established within it for redundancy and security reasons, as there are two ways to enter both company sites.
The configuration of our secure tunnel is presented below and was executed in all Router Gateways.

```
# AveiroGW1

conf t
crypto isakmp policy 30
authentication pre-share
crypto isakmp key xpto-sitecom address 193.10.11.2
crypto ipsec transform-set authT ah-sha-hmac
crypto ipsec transform-set cipherT esp-des
crypto ipsec transform-set auth_ciphT ah-sha-hmac esp-des
crypto ipsec profile ipsec-profile-01
set transform-set authT cipherT auth_ciphT
end
write
```

```
conf t
interface Tunnel 0
ip nat outside
ip unnumbered FastEthernet0/1
tunnel source 193.10.10.2
tunnel destination 193.10.11.2
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec-profile-01
ip route 193.2.2.0 255.255.255.0 Tunnel0
ipv6 route ::/0 A:A:A:10::1
end
write
```

Conclusion

To conclude this report we would like to list the aspects that did not have a linear solution, to evaluate the final results and to name possible future improvements to the network.
Distributing the IP addresses throughout the network and configuring the OSPF protocol was relatively simple. The connection with the RIP protocol gave us a few struggles, as the translation required a strong knowledge about the protocols and forced us to learn more about them. The same happened with the tunnel between the company sites, but in this case,as the solution was a simplified version, we managed to establish the tunnel in what we believe to be a secure way. The quality of service policies were not as linear as the IPs configuration but it did not occupy much of our development time.
The overall evaluation of the network’s final version is satisfactory and we finish this project delivering a fully functional network simulated in GNS3. The project files are attached to this report.
Considering future work around the network, we believe that the focus should be on the new company site in Porto and perhaps on the development of firewalls for XPTO.

Bibliography

1. **Nogueira, António.** First Project, Networks Architecture and Management. *Elearning.* [Online] 2019.

2. Computer Networks: Types of Network Topology. *Study Tonight.* [Online] [Cited: 04 13, 2018.] https://www.studytonight.com/computer-networks/network-topology-types.

3. **Kabalani, Sal.** Logical and Physical Network Diagrams. *Quora.* [Online] 03 24, 2017. [Cited: 04 12, 2019.] https://www.quora.com/What-is-the-difference-between-a-logical-network-diagram-and-a-physical-network-diagram-When-would-you-use-each-type.

4. **Kerns, John.** Network Documentation Series: Physical Diagram. *PacketPushers.* [Online] 06 03, 2015. [Cited: 04 12, 2019.] https://packetpushers.net/network-documentation-series-physical-diagram-2/.

Appendix

All configuration executed in the GNS3 network simulation are present in this chapter so that the reader may analyse in case of need.

```
# AveiroGW1
conf t
ipv6 unicast-routing
int f0/0
ip nat inside
ip address 172.30.10.1 255.255.255.0
ipv6 address 2002:A:A:10::1/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
int f0/1
ip nat outside
ip address 193.10.10.2 255.255.255.0
ipv6 address A:A:A:10::2/64
no shut
int f1/1
no switchport
ip nat inside
ip address 172.30.30.1 255.255.255.0
ipv6 address 2002:A:A:30::1/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
int f1/0
no switchport
ip nat inside
ip address 172.30.40.1 255.255.255.0
ipv6 address 2002:A:A:40::1/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
end
conf t
ip route 0.0.0.0 0.0.0.0 193.10.10.1
router ospf 1
default-information originate always metric 5
exit
ipv6 router ospf 1
router-id 1.0.1.0
default-information originate always metric 10
end
conf t
access-list 1 permit 172.30.0.0 0.0.255.255
access-list 1 permit 172.31.0.0 0.0.255.255
ip nat pool POOLR 193.1.1.128 193.1.1.255 netmask
255.255.255.128
ip nat Stateful id 3
primary 172.30.10.1
peer 172.30.20.1
mapping-id 10
end
conf t
ip nat inside source list 1 pool POOLR mapping-id 10
overload
end
write

conf t
crypto isakmp policy 30
authentication pre-share
crypto isakmp key xpto-sitecom address 193.10.11.2
crypto ipsec transform-set authT ah-sha-hmac
crypto ipsec transform-set cipherT esp-des
crypto ipsec transform-set auth_ciphT ah-sha-hmac esp-des
crypto ipsec profile ipsec-profile-01
set transform-set authT cipherT auth_ciphT
end
write
conf t
interface Tunnel 0
ip nat outside
ip unnumbered FastEthernet0/1
tunnel source 193.10.10.2
tunnel destination 193.10.11.2
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec-profile-01
ip route 193.2.2.0 255.255.255.0 Tunnel0
ipv6 route ::/0 A:A:A:10::1
end
write
```

```
# AveiroGW2
conf t
ipv6 unicast-routing
int f0/0
ip nat inside
ip address 172.30.20.1 255.255.255.0
ipv6 address 2002:A:A:20::1/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
int f0/1
ip nat outside
ip address 193.10.20.2 255.255.255.0
no shut
int f1/0
no switchport
ip nat inside
ip address 172.30.50.1 255.255.255.0
ipv6 address 2002:A:A:50::1/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
```

```
int f1/1
no switchport
ip nat inside
ip address 172.30.30.2 255.255.255.0
ipv6 address 2002:A:A:30::2/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
end
conf t
router ospf 1
default-information originate always metric 10
exit
ipv6 router ospf 1
router-id 2.0.2.0
default-information originate always metric 5
end
conf t
access-list 1 permit 172.30.0.0 0.0.255.255
access-list 1 permit 172.31.0.0 0.0.255.255
ip nat pool POOLR 193.1.1.128 193.1.1.255 netmask
255.255.255.128
ip nat Stateful id 2
backup 172.30.20.2
peer 172.30.10.1
mapping-id 10
end
conf t
ip nat inside source list 1 pool POOLR mapping-id 10
overload
end
write
conf t
crypto isakmp policy 30
authentication pre-share
crypto isakmp key xpto-sitecom address 193.10.21.2
crypto ipsec transform-set authT ah-sha-hmac
crypto ipsec transform-set cipherT esp-des
crypto ipsec transform-set auth_ciphT ah-sha-hmac esp-des
crypto ipsec profile ipsec-profile-01
set transform-set authT cipherT auth_ciphT
end
write
conf t
interface Tunnel 0
ip nat outside
ip unnumbered FastEthernet0/1
tunnel source 193.10.20.2
tunnel destination 193.10.21.2
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec-profile-01
ip route 193.2.2.0 255.255.255.0 Tunnel0
end
write
conf t
interface Tunnel 1
tunnel source f0/1
ipv6 address 2002:C10A:1402::2/48
tunnel mode ipv6ip 6to4
no shut
exit
ipv6 route 2002:C10A::/32 Tunnel1
ipv6 route ::/0 2002:C10A:1502::2
ip route 0.0.0.0 0.0.0.0 193.10.20.1
end
write
```

```
# PortoGW1
conf t
ipv6 unicast-routing
int f0/0
ip nat inside
ip address 172.29.10.1 255.255.255.0
ipv6 address 2002:B:B:10::1/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
int f0/1
ip nat outside
ip address 193.10.11.2 255.255.255.0
ipv6 address A:A:A:11::2/64
no shut
int f1/0
no switchport
ip nat inside
ip address 172.29.30.1 255.255.255.0
ipv6 address 2002:B:B:30::1/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
end
conf t
ip route 0.0.0.0 0.0.0.0 193.10.11.1
router ospf 1
default-information originate always metric 5
exit
ipv6 router ospf 1
router-id 1.0.1.0
default-information originate always metric 10
end

conf t
crypto isakmp policy 30
authentication pre-share
crypto isakmp key xpto-sitecom address 193.10.10.2
crypto ipsec transform-set authT ah-sha-hmac
crypto ipsec transform-set cipherT esp-des
crypto ipsec transform-set auth_ciphT ah-sha-hmac esp-des
crypto ipsec profile ipsec-profile-01
set transform-set authT cipherT auth_ciphT
end
write
conf t
interface Tunnel 0
ip nat outside
```

```
ip unnumbered FastEthernet0/1
tunnel source 193.10.11.2
tunnel destination 193.10.10.2
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec-profile-01
ip route 193.1.1.0 255.255.255.0 Tunnel0
ipv6 route ::/0 A:A:A:11::1
end
write

conf t
access-list 1 permit 172.29.0.0 0.0.255.255
ip nat pool POOLR 193.2.2.128 193.2.2.255 netmask
255.255.255.128
ip nat Stateful id 3
primary 172.29.10.1
peer 172.29.20.1
mapping-id 10
end
conf t
ip nat inside source list 1 pool POOLR mapping-id 10
overload
end
write
```

```
# PortoGW2
conf t
ipv6 unicast-routing
int f0/0
ip nat inside
ip address 172.29.20.1 255.255.255.0
ipv6 address 2002:B:B:20::1/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
int f0/1
ip nat outside
ip address 193.10.21.2 255.255.255.0
no shut
int f1/0
no switchport
ip nat inside
ip address 172.29.30.2 255.255.255.0
ipv6 address 2002:B:B:30::2/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
end
conf t
router ospf 1
default-information originate always metric 10
exit
ipv6 router ospf 1
router-id 2.0.2.0
default-information originate always metric 5
end
conf t
crypto isakmp policy 30
authentication pre-share
crypto isakmp key xpto-sitecom address 193.10.20.2
crypto ipsec transform-set authT ah-sha-hmac
crypto ipsec transform-set cipherT esp-des
crypto ipsec transform-set auth_ciphT ah-sha-hmac esp-des
crypto ipsec profile ipsec-profile-01
set transform-set authT cipherT auth_ciphT
end
write
conf t
interface Tunnel 0
ip nat outside
ip unnumbered FastEthernet0/1
tunnel source 193.10.21.2
tunnel destination 193.10.20.2
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec-profile-01
ip route 193.1.1.0 255.255.255.0 Tunnel0
end
write
conf t
interface Tunnel 1
tunnel source f0/1
ipv6 address 2002:C10A:1502::2/48
tunnel mode ipv6ip 6to4
no shut
exit
ipv6 route 2002:C10A::/32 Tunnel1
ipv6 route ::/0 2002:C10A:1402::2
ip route 0.0.0.0 0.0.0.0 193.10.21.1
end
write

conf t
access-list 1 permit 172.29.0.0 0.0.255.255
ip nat pool POOLR 193.2.2.128 193.2.2.255 netmask
255.255.255.128
ip nat Stateful id 2
backup 172.29.20.1
peer 172.29.10.1
mapping-id 10
end
conf t
ip nat inside source list 1 pool POOLR mapping-id 10
overload
end
write
```

```
# Core1
vlan database
vlan 501
vlan 502
vlan 503
vlan 504
vlan 505
```

```
vlan 560
vlan 600
exit
conf t
ip routing
ipv6 unicast-routing
ip cef
ipv6 router ospf 1
router-id 1.1.1.1
end
conf t
ip route 0.0.0.0 0.0.0.0 193.10.10.1 60
int f0/0
ip nat inside
ip address 172.30.10.2 255.255.255.0
ipv6 address 2002:A:A:10::2/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
int f0/1
ip nat inside
ip address 172.30.50.2 255.255.255.0
ipv6 address 2002:A:A:50::2/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
int f1/1
switchport mode trunk
switchport trunk allowed vlan 1,501,1002-1005
int f1/2
switchport mode trunk
switchport trunk allowed vlan 1,502,600,1002-1005
int f1/3
switchport mode trunk
switchport trunk allowed vlan 1,503,600,1002-1005
int f1/4
switchport mode trunk
switchport trunk allowed vlan 1,504,600,1002-1005
int f1/5
switchport mode trunk
switchport trunk allowed vlan 1,505,600,1002-1005
int f1/15
switchport
switchport mode trunk
switchport trunk allowed vlan 1,560,600,1002-1005
int vlan560
ip nat inside
ip address 172.30.60.1 255.255.255.0
ipv6 address 2002:A:A:60::1/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
no autostate
interface Vlan501
ip nat inside
ip address 172.30.1.1 255.255.255.0
ipv6 address 2002:A:A:1::1/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
no autostate
interface Vlan502
ip nat inside
ip address 172.30.2.1 255.255.255.0
ipv6 address 2002:A:A:2::1/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
no autostate
interface Vlan503
ip nat inside
ip address 172.30.3.1 255.255.255.0
ipv6 address 2002:A:A:3::1/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
no autostate
interface Vlan504
ip nat inside
ip address 172.30.4.1 255.255.255.0
ipv6 address 2002:A:A:4::1/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
no autostate
interface Vlan505
ip nat inside
ip address 172.30.5.1 255.255.255.0
ipv6 address 2002:A:A:5::1/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no autostate
no shut
interface Vlan600
ip nat inside
ip address 172.30.100.1 255.255.255.0
ipv6 address 2002:A:A:100::1/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no autostate
no shut
end
conf t
router rip
version 2
no auto-summary
redistribute ospf 1 metric 10
network 172.30.1.0
network 172.30.2.0
network 172.30.3.0
network 172.30.4.0
network 172.30.5.0
exit
router ospf 1
redistribute rip metric 10 subnets
end
write
```

```
# Core2
vlan database
vlan 511
vlan 512
vlan 513
vlan 514
vlan 515
vlan 560
vlan 600
exit
conf t
ip routing
ipv6 unicast-routing
ip cef
ipv6 router ospf 1
router-id 2.2.2.2
end
conf t
ip route 0.0.0.0 0.0.0.0 193.10.20.1
int f0/0
ip nat inside
ip address 172.30.20.2 255.255.255.0
ipv6 address 2002:A:A:20::2/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
int f0/1
ip nat inside
ip address 172.30.40.2 255.255.255.0
ipv6 address 2002:A:A:40::2/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
int f1/1
switchport mode trunk
switchport trunk allowed vlan 1,511,1002-1005
int f1/2
switchport mode trunk
switchport trunk allowed vlan 1,512,600,1002-1005
int f1/3
switchport mode trunk
switchport trunk allowed vlan 1,513,600,1002-1005
int f1/4
switchport mode trunk
switchport trunk allowed vlan 1,514,600,1002-1005
int f1/5
switchport mode trunk
switchport trunk allowed vlan 1,515,600,1002-1005
int f1/15
switchport
switchport mode trunk
switchport trunk allowed vlan 1,560,600,1002-1005
int vlan560
ip nat inside
ip address 172.30.60.2 255.255.255.0
ipv6 address 2002:A:A:60::2/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no autostate
no shut
interface Vlan511
ip nat inside
ip address 172.30.11.1 255.255.255.0
ipv6 address 2002:A:A:11::1/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
no autostate
interface Vlan512
ip nat inside
ip address 172.30.12.1 255.255.255.0
ipv6 address 2002:A:A:12::1/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
no autostate
interface Vlan513
ip nat inside
ip address 172.30.13.1 255.255.255.0
ipv6 address 2002:A:A:13::1/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
no autostate
interface Vlan514
ip nat inside
ip address 172.30.14.1 255.255.255.0
ipv6 address 2002:A:A:14::1/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
no autostate
interface Vlan515
ip nat inside
ip address 172.30.15.1 255.255.255.0
ipv6 address 2002:A:A:15::1/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
no autostate
interface Vlan600
ip nat inside
ip address 172.30.100.2 255.255.255.0
ipv6 address 2002:A:A:100::2/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no autostate
no shut
end
conf t
router rip
version 2
no auto-summary
redistribute ospf 1 metric 20
network 172.30.11.0
network 172.30.12.0
network 172.30.13.0
network 172.30.14.0
```

```
network 172.30.15.0
exit
router ospf 1
redistribute rip metric 20 subnets
end
write
```

```
# NewBuilding1
vlan database
vlan 503
vlan 513
vlan 551
vlan 552
vlan 553
vlan 561
vlan 562
vlan 563
vlan 564
vlan 600
exit
conf t
ip routing
ipv6 unicast-routing
ipv6 router ospf 1
router-id 11.11.11.11
end
conf t
int f1/0
switchport mode trunk
switchport trunk allowed vlan 1,503,600,1002-1005
int f1/1
switchport mode trunk
switchport trunk allowed vlan 1,513,600,1002-1005
int f1/10
switchport mode trunk
switchport trunk allowed vlan 1,551,561-564,600,1002-
1005
int f1/11
switchport mode trunk
switchport trunk allowed vlan 1,552,561-564,600,1002-
1005
int f1/12
switchport mode trunk
switchport trunk allowed vlan 1,553,561-564,600,1002-
1005
int f1/15
switchport
switchport mode trunk
switchport trunk encapsulation dot1q
interface Vlan600
ip nat inside
ip address 172.30.100.3 255.255.255.0
ipv6 address 2002:A:A:100::3/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no autostate
no shut
interface Vlan503
ip nat inside
ip address 172.30.3.2 255.255.255.0
ipv6 address 2002:A:A:3::2/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
no autostate
interface Vlan513
ip nat inside
ip address 172.30.13.2 255.255.255.0
ipv6 address 2002:A:A:13::2/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
no autostate
interface Vlan551
ip nat inside
ip address 172.30.51.1 255.255.255.0
ipv6 address 2002:A:A:51::1/64
ip ospf 1 area 100
ipv6 ospf 1 area 100
no shut
no autostate
interface Vlan552
ip nat inside
ip address 172.30.52.1 255.255.255.0
ipv6 address 2002:A:A:52::1/64
ip ospf 1 area 100
ipv6 ospf 1 area 100
no shut
no autostate
interface Vlan553
ip nat inside
ip address 172.30.53.1 255.255.255.0
ipv6 address 2002:A:A:53::1/64
ip ospf 1 area 100
ipv6 ospf 1 area 100
no shut
no autostate
interface Vlan561
ip nat outside
ip address 193.1.1.17 255.255.255.240
ipv6 address 2002:A:A:61::1/64
ip ospf 1 area 100
ipv6 ospf 1 area 100
no shut
no autostate
interface Vlan562
ip nat outside
ip address 193.1.1.33 255.255.255.240
ipv6 address 2002:A:A:62::1/64
ip ospf 1 area 100
ipv6 ospf 1 area 100
no shut
no autostate
interface Vlan563
ip nat outside
ip address 193.1.1.49 255.255.255.240
ipv6 address 2002:A:A:63::1/64
```

```
ip ospf 1 area 100
ipv6 ospf 1 area 100
no shut
no autostate
interface Vlan564
ip nat outside
ip address 193.1.1.1 255.255.255.240
ipv6 address 2002:A:A:64::1/64
ip ospf 1 area 100
ipv6 ospf 1 area 100
no shut
no autostate
end
write
conf t
access-list 101 permit ip 193.1.1.16 0.0.0.15 any
access-list 101 deny ip any any
class-map match-all EF
match access-group 101
exit
policy-map SETDSCP
class EF
set ip dscp 46
end
conf t
class-map match-all PREMIUM
match ip dscp 46
exit
class-map match-all BEST-EFFORT
match ip dscp 0
end
conf t
policy-map EDGE
class PREMIUM
priority percent 40
class BEST-EFFORT
police 16000 2000 2000 conform-action set-dscp-transmit 0
end
write
conf t
int vlan503
service-policy output EDGE
int vlan513
service-policy output EDGE
int vlan561
service-policy input SETDSCP
end
write


# NewBuilding2
vlan database
vlan 502
vlan 512
vlan 551
vlan 552
vlan 553
vlan 561
vlan 562
vlan 563
vlan 564
vlan 600
vlan 570
exit
conf t
ip routing
ipv6 unicast-routing
ipv6 router ospf 1
router-id 12.12.12.12
end
conf t
int f1/0
switchport mode trunk
switchport trunk allowed vlan 1,502,600,1002-1005
int f1/1
switchport mode trunk
switchport trunk allowed vlan 1,512,600,1002-1005
int f1/10
switchport mode trunk
switchport trunk allowed vlan 1,551,561-564,600,1002-
1005
int f1/11
switchport mode trunk
switchport trunk allowed vlan 1,552,561-564,600,1002-
1005
int f1/12
switchport mode trunk
switchport trunk allowed vlan 1,553,561-564,600,1002-
1005
int f1/15
switchport
switchport mode trunk
switchport trunk encapsulation dot1q
interface Vlan600
ip nat inside
ip address 172.30.100.4 255.255.255.0
ipv6 address 2002:A:A:100::4/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no autostate
no shut
interface Vlan502
ip nat inside
ip address 172.30.2.2 255.255.255.0
ipv6 address 2002:A:A:2::2/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
no autostate
interface Vlan512
ip nat inside
ip address 172.30.12.2 255.255.255.0
ipv6 address 2002:A:A:12::2/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
no autostate
interface Vlan551
ip nat inside
ip address 172.30.51.2 255.255.255.0
```

```
ipv6 address 2002:A:A:51::2/64
ip ospf 1 area 100
ipv6 ospf 1 area 100
no shut
no autostate
interface Vlan552
ip nat inside
ip address 172.30.52.2 255.255.255.0
ipv6 address 2002:A:A:52::2/64
ip ospf 1 area 100
ipv6 ospf 1 area 100
no shut
no autostate
interface Vlan553
ip nat inside
ip address 172.30.53.2 255.255.255.0
ipv6 address 2002:A:A:53::2/64
ip ospf 1 area 100
ipv6 ospf 1 area 100
no shut
no autostate
interface Vlan561
ip nat outside
ip address 193.1.1.18 255.255.255.240
ipv6 address 2002:A:A:61::2/64
ip ospf 1 area 100
ipv6 ospf 1 area 100
no shut
no autostate
interface Vlan562
ip nat outside
ip address 193.1.1.34 255.255.255.240
ipv6 address 2002:A:A:62::2/64
ip ospf 1 area 100
ipv6 ospf 1 area 100
no shut
no autostate
interface Vlan563
ip nat outside
ip address 193.1.1.50 255.255.255.240
ipv6 address 2002:A:A:63::2/64
ip ospf 1 area 100
ipv6 ospf 1 area 100
no shut
no autostate
interface Vlan564
ip nat outside
ip address 193.1.1.2 255.255.255.240
ipv6 address 2002:A:A:64::2/64
ip ospf 1 area 100
ipv6 ospf 1 area 100
no shut
no autostate
end
write
conf t
access-list 101 permit ip 193.1.1.16 0.0.0.15 any
access-list 101 deny ip any any
class-map match-all EF
match access-group 101
exit
policy-map SETDSCP
class EF
set ip dscp 46
end
conf t
class-map match-all PREMIUM
match ip dscp 46
exit
class-map match-all BEST-EFFORT
match ip dscp 0
end
conf t
policy-map EDGE
class PREMIUM
priority percent 40
class BEST-EFFORT
police 16000 2000 2000 conform-action set-dscp-transmit 0
end
write
conf t
int vlan502
service-policy output EDGE
int vlan512
service-policy output EDGE
int vlan561
service-policy input SETDSCP
end
write
```

```
# Datacenter
vlan database
vlan 504
vlan 514
vlan 571
vlan 600
exit
conf t
ip routing
ipv6 unicast-routing
ipv6 router ospf 1
router-id 71.71.71.71
end
conf t
int f1/0
switchport mode trunk
switchport trunk allowed vlan 1,504,600,1002-1005
int f1/1
switchport mode trunk
switchport trunk allowed vlan 1,514,600,1002-1005
int f1/10
switchport mode trunk
switchport trunk allowed vlan 1,571,600,1002-1005
int f1/2
switchport mode access
switchport access vlan 571
interface Vlan600
ip nat inside
ip address 172.30.100.5 255.255.255.0
ipv6 address 2002:A:A:100::5/64
```

```
ip ospf 1 area 0
ipv6 ospf 1 area 0
no autostate
no shut
interface Vlan504
ip nat inside
ip address 172.30.4.2 255.255.255.0
ipv6 address 2002:A:A:4::2/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
no autostate
interface Vlan514
ip nat inside
ip address 172.30.14.2 255.255.255.0
ipv6 address 2002:A:A:14::2/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
no autostate
interface Vlan571
ip nat outside
ip address 193.1.1.65 255.255.255.224
ipv6 address 2002:A:A:71::1/64
ip ospf 1 area 71
ipv6 ospf 1 area 71
no shut
no autostate
end
write

# DMZ
vlan database
vlan 505
vlan 515
vlan 572
vlan 600
exit
conf t
ip routing
ipv6 unicast-routing
ipv6 router ospf 1
router-id 72.72.72.72
end
conf t
int f1/0
switchport mode trunk
switchport trunk allowed vlan 1,505,1002-1005
int f1/1
switchport mode trunk
switchport trunk allowed vlan 1,515,1002-1005
int f1/10
switchport mode trunk
switchport trunk allowed vlan 1,572,600,1002-1005
interface Vlan600
ip nat inside
ip address 172.30.100.6 255.255.255.0
ipv6 address 2002:A:A:100::6/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no autostate
no shut
interface Vlan505
ip nat inside
ip address 172.30.5.2 255.255.255.0
ipv6 address 2002:A:A:5::2/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
no autostate
interface Vlan515
ip nat inside
ip address 172.30.15.2 255.255.255.0
ipv6 address 2002:A:A:15::2/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
no autostate
interface Vlan572
ip nat outside
ip address 193.1.1.97 255.255.255.224
ipv6 address 2002:A:A:72::1/64
ip ospf 1 area 72
ipv6 ospf 1 area 72
no shut
no autostate
end
write

# ISP1
conf t
ip cef
int f0/0
ip address 193.10.10.1 255.255.255.0
ipv6 address A:A:A:10::1/64
no shut
int f0/1
ip address 193.10.11.1 255.255.255.0
ipv6 address A:A:A:11::1/64
no shut
end
conf t
ip route 193.2.2.0 255.255.255.0 193.10.11.2
ip route 193.1.1.0 255.255.255.0 193.10.10.2
ipv6 route 2002:B:B::/48 A:A:A:11::2
ipv6 route 2002:A:A::/48 A:A:A:10::2
end
write

# ISP2
conf t
ip cef
int f0/0
ip address 193.10.20.1 255.255.255.0
no shut
int f0/1
```

```
ip address 193.10.21.1 255.255.255.0
no shut
end
conf t
ip route 193.2.2.0 255.255.255.0 193.10.21.2
ip route 193.1.1.0 255.255.255.0 193.10.20.2
end
write
```

```
# PortoCore
conf t
ip routing
ipv6 unicast-routing
ip cef
ip route 0.0.0.0 0.0.0.0 193.10.11.1
int f0/0
ip address 172.29.10.2 255.255.255.0
ipv6 address 2002:B:B:10::2/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
int f0/1
ip address 172.29.20.2 255.255.255.0
ipv6 address 2002:B:B:20::2/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
no shut
int lo0
ip address 193.2.2.1 255.255.255.128
ipv6 address 2002:B:B:B::1/64
ip ospf 1 area 0
ipv6 ospf 1 area 0
ip ospf network point-to-point
ipv6 ospf network point-to-point
no shut
end
write
```

```
# Old Building
vlan database
vlan 1
vlan 2
vlan 3
vlan 100
vlan 200
vlan 501
vlan 511
exit
conf t
interface range fastEthernet 1/0 - 3
switchport mode trunk
switchport trunk encapsulation dot1q
interface Vlan1
ip address 172.31.1.1 255.255.255.0
no shut
no autostate
interface Vlan2
ip address 172.31.2.1 255.255.255.0
no shut
no autostate
interface Vlan3
ip address 172.31.3.1 255.255.255.0
no shut
no autostate
interface Vlan100
ip address 172.31.100.1 255.255.255.0
no shut
no autostate
interface Vlan200
ip address 172.31.200.1 255.255.255.0
no shut
no autostate
interface Vlan501
ip address 172.30.1.2 255.255.255.0
no shut
no autostate
interface Vlan511
ip address 172.30.11.2 255.255.255.0
no shut
no autostate
end
conf t
ip routing
router rip
version 2
no auto-summary
network 172.31.0.0
network 172.30.1.0
network 172.30.11.0
end
write
```