Universidade de Aveiro

Final Project

Departamento de Electrónica, Telecomunicações e Informática

Advanced Networks Architecture

Diogo Ferreira, Luís Leira
76504, 76514
diogodanielsoaresferreira@ua.pt, luisleira@ua.pt

January 8, 2018

Contents

Chapter 1

Introduction

This report is done in the scope of the course of Advanced Networks Architecture, in Departamento de Electrónica, Telecomunicações e Informática in Universidade de Aveiro.

On this report we will explain in detail our implementation and engineering choices of the final project of the course.

The first section is dedicated to the addressing of the entities used in the implementation, accordingly to what was proposed in the assignment. The addressing includes IPv4 and IPv6 networks.

On the second section we explain how we manage to achieve the routing inside the ISP PT2, and its interaction with the external peers, mainly with an explanation of BGP and OSPF routing and filters applied to the routes.

On the next section, we describe the MPLS implementation with two bi-directional channels and a VPN for a corporate client.

On the next section, it is explained how we achieved to connect multiple clients through a VoIP service from different companies, with a SIP Proxy inside the ISP PT2, and redirecting all other calls to an external SIP Proxy.

On the next section, we explain how do we created a CDN with conditional DNS, and how do we applied load balancing in the servers, using *SNMP* and a *python* script.

Finally, in the last section it is described how it is implemented the ATM Core in a triangle configuration in the ethernet core of the ISP PT2.

Chapter 2

Implementation

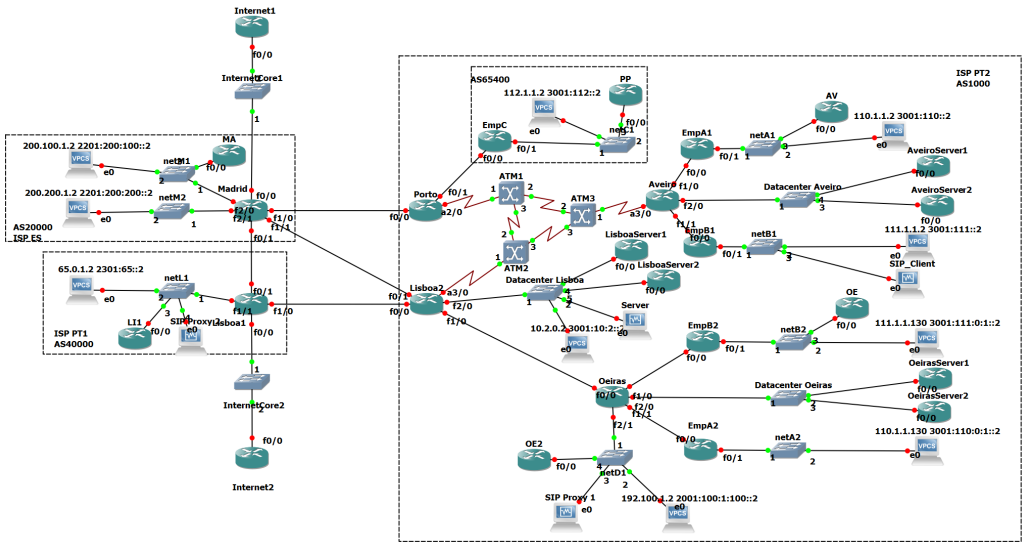

Figure 2.1: GNS3 project topology screenshot.

2.1 Addressing

2.1.1 IPv4

Inside the ISP PT2, public IP addresses were used for the Net A1, A2, B1, B2, C, D1 and a secondary network for Datacenter Lisboa. The networks have the following addresses:

- Net A1 - 110.1.1.0/25
- Net A2 - 110.1.1.128/25
- Net B1 - 111.1.1.0/25
- Net B2 - 111.1.1.128/25
- Net C - 112.1.1.0/24
- Net D1 - 192.100.1.0/25
- Datacenter Lisboa (public) - 192.100.1.128/25
- Interconnection between EmpC and Porto - 4.4.4.24/30 (does not need to be accessible by the outside, but it is to follow the same range of subnets for EBGP)

The private IP addresses were used for the networks of all datacenters (Aveiro, Oeiras and Lisboa), point-to-point links and loopback interfaces.

- Datacenter Lisboa (private) - 10.2.0.0/24
- Datacenter Aveiro - 10.2.1.0/24
- Datacenter Oeiras - 10.2.2.0/24
- ATM point-to-point - 10.0.0.0/24 (divided in subnets /30)
- Other point-to-point links - 10.0.1.0/24 (divided in subnets /30)
- Loopbacks - 10.0.2.0/24 (divided in subnets /32)

Outside the ISP PT2, the interconnections among the AS are done with the network 4.4.4.4/26 (subdivided in /30 subnets).

Inside ISP PT1, the network used is 65.0.1.0/24. Inside the ISP ES, the networks used are, 200.100.1.0/24 for M2 and 200.200.1.0/24 for M1.

The internet core has two subnets, one connected to ISP ES and other connected to ISP PT1. The internet connected to ISP ES has the subnet 2.2.2.1/25, while the one connected to ISP PT1 has the subnet 2.2.2.128/25.

2.1.2 IPv6

For IPv6, the networks follow the same pattern from the IPv4 networks, to ease the debug when dealing with both protocols. The networks that need to be accessible by the outside have the following networks:

- Net A1 - 3001:110::1/64
- Net A2 - 3001:110:0:1::/64
- Net B1 - 3001:111::/64
- Net B2 - 3001:111:0:1::/64
- Net C - 3001:112::/48
- Net D1 - 2001:100:1:100::/64
- Datacenter Lisboa (publicly accessible subnet) - 2001:100:1:101::/64
- Interconnection between EmpC and Porto - 2001:4:4::18/126 (does not need to be accessible by the outside, but it is to follow the same range of subnets for EBGP)

The IPv6 addresses for the networks of all datacenters (Aveiro, Oeiras and Lisboa), point-to-point links and loopback interfaces do not need to be accessible by the outside of the AS.

- Datacenter Lisboa (private) - 3001:10:2::/48
- Datacenter Aveiro -3001:10:2:1::/64
- Datacenter Oeiras -3001:10:2:2::/64
- ATM point-to-point - 2001:100:1:10::/64 (divided in subnets /126)
- Other point-to-point links - 2001:100:1:1::/64 (divided in subnets /126)
- Loopbacks - 2001:100:1:2::/64 (divided in subnets /128)

Outside the ISP PT2, the interconnections among the AS are done with the network 2001:4:4/48 (subdivided in /126 subnets).

Inside the ISP PT1, the network used in 2301:65:0::/48. Inside the ISP ES, the networks used are, 2201:200:100::/48 for M1 and 2201:200:200::/48 for M2.

The internet core has two subnets, one connected to ISP ES and other connected to ISP PT1. The internet connected to ISP ES has the subnet 2001:2:2::/80 and the one connected to ISP PT1 has the subnet 2001:2:2:1::/80.

2.2 Routing

2.2.1 Routing accordingly to ISP networking good practices

The following configurations apply to both IPv4 and IPv6.
The routers with EBGP and with peering relations are:

- Madrid - Internet1
- Lisboa1 - Internet2
- Madrid - Lisboa1
- Madrid - Lisboa2
- Madrid - Porto
- Lisboa1 - Lisboa2
- Porto - EmpC

All IBGP peering relations are established with loopback interfaces, to maintain the IBGP relations independently of the interfaces. Inside the ISP PT2 there are four routers with IBGP, and they are all interconnected in a full mesh: Porto, Lisboa2, Aveiro and Oeiras. Aveiro and Oeiras have IBGP to be able to forward packets to Porto or Lisboa2 according to the destination AS (MP-BGP second constraint).

In ISP PT2 there are five OSPF processes among the networks.

The Aveiro router has one OSPF process for the Emp A1 network and other for the Emp B1 (processes number 2 and 3 respectively). The Emp A1 and Emp B1 have the OSPF process with a passive-interface in the direction of the network (A1 or B1). Both OSPF processes are redistributed into OSPF 1 with metric-type 1. The interface with the Aveiro Datacenter is also running OSPF 1, as a passive-interface. The Aveiro router announces a default route for both processes.

For the Oeiras router, the same pattern is followed. Emp B2 and Emp A2 have each one an OSPF process. These two routers have the OSPF process in the direction of the network (B2 or A2) as a passive-interface. The Oeiras Datacenter and Net D1 are integrated in OSPF 1 as passive-interfaces. Both OSPF processes are redistributed into OSPF 1 with metric-type 1. The Oeiras router announces a default route for both processes.

Other possible routing alternative would be to include all routers on the same OSPF process. However, it would overload the Emp routers with the core routing table, and it would make them aware of all the network, which could be a security issue.

Porto and Lisboa routers have OSPF 1 active and redistribute it to the BGP protocol. It is also announced a default route to IBGP peers by Lisboa2 and Porto. This default route is announced by BGP and not by OSPF because if a packet destination is not on the OSPF routing table, it will be sent to the internet with BGP, so Aveiro and Oeiras routers conceptually separate the routes to internal networks (OSPF) from the routes to external networks (BGP).

The routes sent to EBGP peers are filtered, being only sent the addresses for Net A (1 and 2), Net B (1 and 2), Net C, Net D and the public accessible subnet from Lisboa Datacenter. By doing this, it assures that if a configuration of a new network is done by mistake on Aveiro or Oeiras routers, it does not send it to the internet without an explicit prefix-list entry, allowing more control over the internal networks. Because the AS is non-transit, is also required to send only internal routes from the AS or routes from AS 65400.

Porto announces a default route to the AS 65400, and both Porto and Lisboa remove the private AS from the routes sent to the internet.

Madrid and Lisboa1 announce default routes to Lisboa2 and Porto. Other alternative for this would be to define static routes on the ISP PT2 to Madrid and Lisboa1. While the first option is dynamic, it assumes that the peers are trustworthy. The second option does not depend on announcements made by external routers, but if an external router is not turned on, the static route will continue to route traffic to that router.

Loopbacks are used to create the IBGP connections and they can not be included in the BGP route exchange, so they must be learned through OSPF. Because of that, route-map is applied between all IBGP's (Lisboa2, Porto, Aveiro and Oeiras) to not allow the announcement of the loopbacks to its BGP peers.

To not allow that misconfigurations in Aveiro and Oeiras routers interfere with the regular routing processes of Lisboa and Porto, it is applied a distribute-list to the OSPF process to deny the reception of any default route sent by the Aveiro or Oeiras routers sent to Lisboa2 and Porto routers.

2.2.2 MP-BGP routing constraints

To apply the first routing rule (IP traffic towards Internet should be preferably routed via ISP PT1), it is applied a route-map in Lisboa2 to the

neighbor Lisboa1 that sets the local preference of all routes learned from that router to 200 (higher than the default 100). Porto also needs to apply a route-map to the Madrid neighbor, to set the local preference of the routes learned from the ISP ES, except the default route, to 200. This leads to Porto choosing its route to Madrid as primary route. Because Lisboa2 also needs send the traffic to Madrid without going through Porto, it is added a set weight 100 to the route-map applied in Lisboa2 to neighbor Lisboa1. This way, Porto and Lisboa2 do not need to send traffic to each other when sending packets to Madrid. But if the traffic is going to other AS, it is routed preferably to Lisboa2.

To apply the second routing rule (IP traffic towards all AS20000 networks, should be preferably routed via Porto from Aveiro, and via Lisboa1 from Oeiras), it is applied an access-list in Aveiro to the neighbor Porto to higher the local preference to 300 from all routes learned with destination to ISP ES. The same route-map is applied in Oeiras to the neighbor Lisboa2. This way, Oeiras routes all packets to ISP ES to Lisboa2 and Aveiro to Porto. Other possible option would be to define communities in Lisboa and Porto routers, and change the local preference based on communities, but the overhead of sending and checking a community is unnecessary.

To apply the third routing rule (IP traffic for remote SIP proxy 2 (to network netL1) can not be routed via Porto using the direct peering link to ISP ES), it is applied a prefix-list in Porto to the neighbor Madrid to deny all the routes from the SIP Proxy 2 network. This way, there are no routes learned from Porto to the SIP Proxy network. If, for any reason, Porto has a default-route to Madrid (Lisboa2 router must be down), and SIP Packets are routed to Porto, the packets would still go to Madrid. To avoid that, it is also applied a route-map to the interface to deny the sending of packets with SIP Proxy 2 network as destination.

2.3 MPLS

The routers with MPLS configured and their interfaces are Lisboa2, Porto, Aveiro e Oeiras.

To configure two bi-directional channels between the branches of client B with dedicated bandwidth of 20 Mbps it was first configured on the routers where the traffic goes (Aveiro, Lisboa2 and Oeiras) MPLS Traffic-Engineering for OSPF, to allow OSPF to announce MPLS labels. Then, on each interface where the traffic goes, it was configured 100 000 Kbit/s as the maximum reservable bandwidth, total and per flow. On Aveiro router it was configured two tunnels with destination the IP of the loopback interface of Oeiras router.

Both tunnels have 20 000 Kbit/s of bandwidth. To route the traffic to the tunnel interface, it was needed to create an extended access-list, used by a route-map applied to the interface connected to Emp B1, that redirects all the traffic from Emp B1 network to Emp B2 network. On Oeiras, symmetrical configurations were done: two tunnels were configured to Aveiro loopback, an extended access-list was created and a route-map using the access-list was applied to the interface to route all traffic from the Emp B2 network to Emp B1. Initially, IPv4 and IPv6 traffic was redirected to the tunnel. On the final GNS3 project version, because of an ATM bug on the routers, the IPv6 traffic over the IPv4 MPLS tunnel would not go through the ATM network correctly, so now the IPv6 traffic between the Emp B tunnels does not goes into the tunnel.

An MPLS VPN was also deployed for client A, interconnecting Aveiro and Oeiras branches. In Aveiro and Oeiras router it is needed to define a VRF VPN, and it is also needed to define the interface to Emp A with that VPN. For the VPN's to have connectivity, it is needed to define the VPN neighbor (Oeiras - Aveiro) and send both communities. Then it is needed to redistribute the routes learned from the VPN (redistribute the OSPF process). For the VPN's to have global connectivity, it is needed to have a static route from Oeiras and Aveiro to the respective VPN, and to redistribute the static route to the OSPF process. Finally, it is needed to define a static route for the VPN routing tables. On this case, it was defined that the VPN from Oeiras would have as static default route the Lisboa router, while the VPN from Aveiro would have the Porto router as the static default route.

2.4 SIP

The ISP PT2 SIP Proxy server is located in Net D and it is used as a SIP proxy for corporate clients of companies A and B. It was configured three client for each company, each one using both extensions (e.g. Client 1 of Emp A has the extensions 234100001 and 234110001). With this configuration, the clients can make calls between them. Two SIP clients were also configured (one in Lisboa Datacenter, other in EmpB1) to test the SIP functionalities.

To enable the forwarding of calls, it was configured another SIP Proxy on ISP PT1. The proxies are configured as peers, with a static host, and the ISP PT2 proxy is configured to redirect all other calls (all extensions not known) to the external proxy. The external proxy is configured to receive all calls and answer with a playback message to ease the tests and to not be needed a new virtual machine to test the reception of the calls from the external proxy.

2.5 CDN

A DNS server located in the Lisboa Datacenter acts as a master server (zone) for the domain acacdn.com. It redirects clients to the closest Datacenter according to their location. The DNS server contains a file with two ACLs, one named "AV" that includes terminals in Aveiro (110.1.1.0/25, 111.1.1.0/25 and 10.2.1.0/24) and another named "OE" that includes terminals in Oeiras (110.1.1.128/25, 111.1.1.128/25, 192.100.1.0/25 and 10.2.2.0/24). Then, the definition of the zones are conditioned by the views "aveiro", "oeiras" and "lisboa". The first will match the clients from "AV" and the corresponding file "aracdn.com-aveiro-symlink". The second will match the clients from "OE" and the corresponding file "aracdn.com-oeiras-symlink". The last one will match the clients from "any" (all other internal or external terminals) and the corresponding file "aracdn.com-lisboa-symlink". Each file refers to a symlink that binds the configuration file from each zone.

To enable load balancing in the decision process of DNS, each datacenter will have two servers. Each DNS configuration file is a symlink that points to another file. Each datacenter will have two files, one pointing to each server. We have made a *python* script that uses SNMP to get informations about each server. The SNMP is configured on each server from the datacenters with the version 3, with an user defined and a password. The CDN server is the only host that is allowed to read information from those servers using SNMP.

The *script* requests the number of packets in and out from the servers, on each interface that is used for the DNS requests. If the router or the interface is down, or if the sum of the packets sent and received is higher than the server on the same datacenter, the file binding is changed to the other server. With that, if one server has more traffic than the other server in the same datacenter, load balancing is done to assure that the traffic is always equalized between both servers.

2.6 ATM

The three ATM switches deployed in a triangle configuration are connected directly among them and each one to a different router. Assuming ATM1, ATM2 and ATM3: the first one is connected to Porto, the second to Lisboa2 and the last one to Aveiro.

Each one of these three routers (Porto, Lisboa2 and Aveiro) establishes a point-to-point connection among each other through the ATM core. Each one has two sub-interfaces into the ATM interface that connects to the cor-

responding ATM switch (described before) and each sub-interface with one PVC assigned, besides the OSPF and MPLS configurations needed (and BGP).

Porto's two PVCs have assigned the values 101/0 and 102/0, Lisboa2 assigned the values 102/0 and 103/0 and Aveiro assigned the values 101/0 and 103/0. So, it can be seen in the following way:

- 101/0 is assigned between Porto, ATM1, ATM3 and Aveiro.
- 102/0 is assigned between Porto, ATM1, ATM2 and Lisboa2.
- 103/0 is assigned between Lisboa2, ATM2, ATM3 and Aveiro.

Each PVC uses aal5snap encapsulation to forward the IP and IPv6 packets throught the ATM network.

Chapter 3

Conclusion

On this report we explained our implementation of the final project of the course Advanced Networks Architecture, with all the main goals and the engineering choices behind the implementation. All the proposed objectives for the project were achieved, along with an extra objective, that was ATM. With this implementation, we explained how to implement routing, VoIP, tunneling through MPLS, CDN with load balancing done using *SNMP* and ATM inside an AS.