universidade de aveiro

Departamento de Eletrónica, Telecomunicações e Informática

Arquitetura de Redes Avançada

Projeto Prático

Rodrigo Santos, 89180
Francisco Petronilho, 89241

Introduction

This report was done for the final project of the course Advanced Network Architecture, in Departamento de Eletrónica, Telecomunicações e Informática in Universidade de Aveiro. We will explain in detail the implementation and engineering choices done in the project.

The first section will briefly explain the IPv4 addressing of the entities according to what was proposed.

In the second section we explain the basic mechanisms and Inter-Operator border agreements, where we talk about the routing inside and between the operators and the Internet Core, according to the scenario constraints and inter-operator routing constraints proposed.

The third section is dedicated to the provisioning of corporate networking services. Finally, the provisioning of VoIP services(section 4) and datacenter services(section 5) are explained.

Implementation

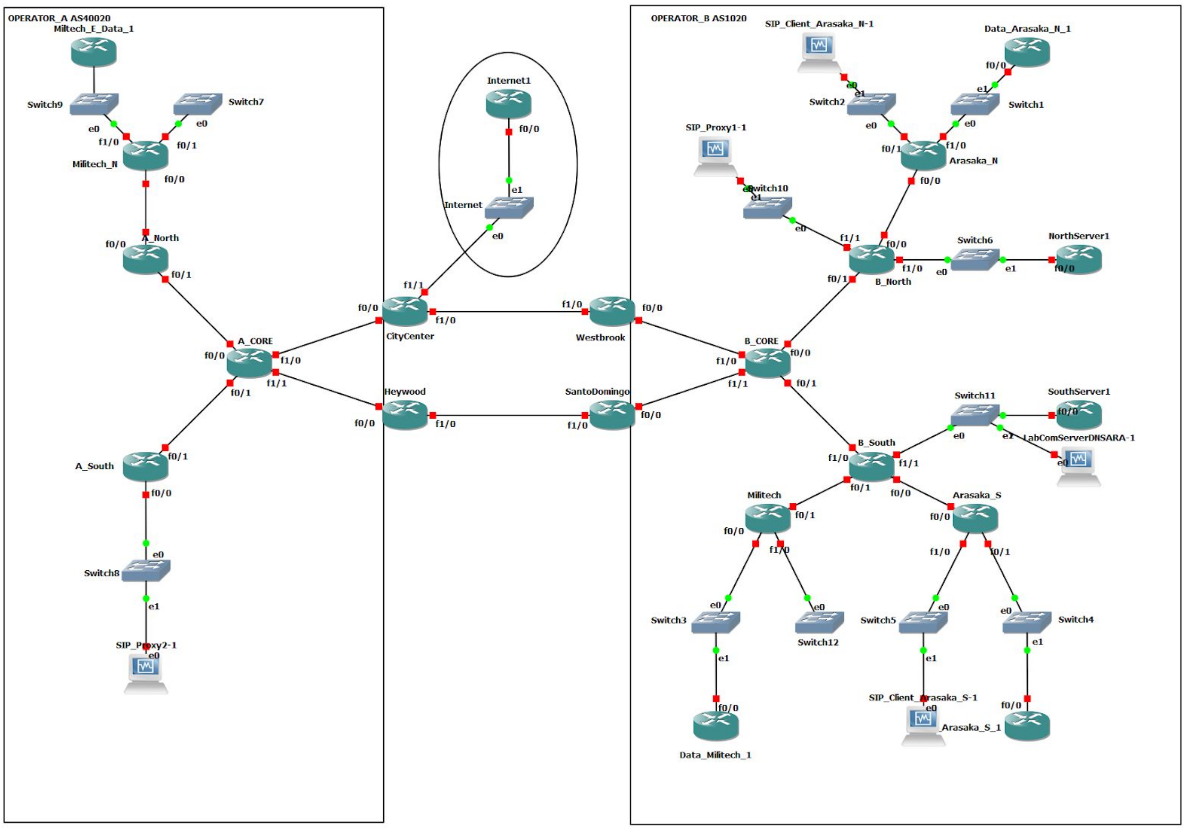

Figure 1: GNS3 project screenshot

Addressing

Inside operator A, public IP addresses were used on the Militech External Net and Operator A's Media Network. The networks use the following addresses:

- Militech External Net Data – 193.136.200.0/24
- Militech External Net VoIP - 193.136.201.0/24
- Operator A's Media Network - 100.200.1.0/24

Inside operator B, public IP addresses were used for the Arasaka Corporation networks, and the datacenter networks. The networks use the following addresses:

- Arasaka Data Net 1 - 193.136.100.0/24
- Arasaka VoIP Net 1 - 193.136.101.0/24
- Arasaka Data Net 2 - 193.136.102.0/24
- Arasaka VoIP Net 2 - 193.136.103.0/24
- Militech Net 1 VoIP – 193.136.202.0/24
- Militech Net 1 Data - 193.136.203.0/24
- Datacenter North - 200.100.2.0/24
- Datacenter South - 200.100.4.0/24

The private networks used for the core, internal point-to-point links and loopback interfaces in both operators were 10.10.0.0/16, also, on operator B the media network used is the private network 10.20.1.0/24.

All the external BGP peering links use the network 4.4.4.0/26. A router Internet1 was set to simulate traffic from the Internet with different network prefixes.

Basic mechanisms and Inter-Operator border agreements

Routers eBGP peering relations:

- Westbrook ← → CityCenter
- SantoDomingo ← → Heywood
- Internet1 ← → CityCenter

Inside operator A there are 4 routers with iBGP and 5 in operator B, all established with loopback interfaces, to maintain the iBGP relation regardless of the interfaces. Inside each operator the routers with iBGP are interconnected in a full mesh. The core routers in both operators (A_CORE and B_CORE) have iBGP to be able to forward traffic according to the destination and the constraints implemented that will be explained ahead.

In order to provide full connectivity between operator B (AS1020), operator A (AS 40020) and the Internet Core, it was necessary to activate and configure BGP in the border routers from operator B and operator A as well as both the Core routers inside operator B and A. The path to the Internet Core is acquired through this protocol, where as a result of the eBGP peering relations between the border routers an AS-PATH is obtained with the information on how to proceed routing. This path is then announced through iBGP to the Core routers. Both Core routers announce a default route through the OSPF process to the AS corporations inside the AS, this way all traffic to a network outside the AS is routed towards the Core of the AS and from there routed using BGP routes to the Internet, or the other AS.

Each operator has an OSPF process (100), both border routers from each operator have OSPF active and redistribute it to the BGP protocol. In operator B the redistribution is done for internal (OSPF) routes, external type 1 and 2 routes. More information in the Provisioning of Corporate Networking Services section.

Furthermore to ensure the correct use of eBGP policies, filtering is done in the border routers from both operators to make sure no private networks are going out the operator they belong to or being received in another operator and the default routes are also denied when entering an AS. This is accomplished through the use of prefix-lists denying private and default networks to be announced by BGP.

To implement the required routing constraints for inter-operator VoIP and data traffic, BGP communities were created in each border router, route-maps were created and assigned with a community and a Local Preference value to meet the routing constraints. For the routers Westbrook and CityCenter VoIP routes learned from each other a Local Preference value of 111 was set, and 22 to all other routes. Values were set the other way around for routers SantoDomingo and Heywood, 111 for all routes other than VoIP, and 22 for VoIP routes. The communities in each border router are sent to its eBGP peer. This way, the core routers will always forward traffic to the correct path, as long as both links are up, otherwise, connectivity is still ensured as Local Preference doesn't prohibit traffic flow and VoIP and data traffic can still circulate in both inter-operator links.

Provisioning of Corporate Networking Services

For the interconnection of Arasaka's north and south branches inside operator B, a VRF VPN was created in which reside all the networks from those two branches. Once the VPN is set both branches can communicate, but communication outside the VPN is lost, to fix this, in both Arasaka_N and Arasaka_S routers a default route was created for traffic leaving the VRF VPN to be routed towards B_NORTH and B_SOUTH, respectively, this doesn't fix connectivity problem yet. To ensure connectivity static routes were created for Arasaka's networks, and redistributed through the OSPF process. By doing this, in order to communicate with networks outside operator B, border routers Westbrook and SantoDomingo have to redistribute the OSPF external type 2 routes to the BGP process.

To implement Militech's Internet Core access point as B_South router, a tunnel was created between Militech_N and Militech routers in which traffic with destination to the Internet Core belonging to Militech branch in operator A is routed through. Once traffic reaches the B_South router through the tunnel it is routed to the Internet Core, using the routes it has learned by OSPF.

To identify the traffic that is supposed to be routed to the tunnel, a route-map changes the next-hop of the routes announced via iBGP, according to the AS Path of each route, if the route came through the AS 1020 it means that it came from the internet and the next-hop is changed. All the routes to the internet will have the same next-hop, when this next-hop is used a static route will send it through the tunnel.

Provisioning of VoIP services

To provide VoIP services to all corporate customers from Operator B(AS1020) there is a SIP proxy server(SIP Proxy 1) on Operator B's Media Network. This proxy server has three clients configured one for each Arasaka branch(234101xxx and 289101xxx) and one for Militech Net 1(289102xxx). This allows the clients to make calls between them. Any number that belongs to the assigned telephone numbers of Arasaka and Militech corporations are redirected to the respective client, if the proxy server can't reach the client the server will send an automatic answer, in this answer the server says the digits of the number that the client is trying to call.

If a number does not belong to any of the corporations(234101XXX, 289101XXX or 289102XXX) the call will be forwarded. For this another SIP proxy(SIP Proxy 2) was configured on Operator A. The proxies were configured as peers with a static host, the SIP Proxy 1 will redirect calls that are trying to reach numbers that it doesn't recognize(all the numbers that are not from Arasaka or Militech Corporations). The external proxy was configured to receive all calls and answer with a playback message to facilitate the testing.

Since SIP Proxy 1 is in a private network and BGP blocks all private routes between operators, SIP Proxy 2 can't communicate with SIP Proxy 1. To solve this issue a tunnel was created between A_South and Arasaka_N routers using the VoIP assigned IP's to make sure traffic is correctly(according to the constraints) routed between operators. When SIP Proxy 2 sends a packet to SIP Proxy 2 a static route in A_South sends it through the tunnel. The opposite, from SIP Proxy 1 to SIP Proxy 2 doesn't use the tunnel because SIP Proxy 2 has a public IP that is announced between operators.

Provisioning of Datacenter Services

The provisioning of the datacenter services is guaranteed by a DNS server located in the Datacenter South that acts as a master server for the domain burn-city.org. This server provides Arasaka Corporation a privileged connection to these services by ensuring that the resolution requests from the corporation are always sent to the closest datacenter. All other traffic associated with the datacenter service is always resolved to the Datacenter South.

To redirect clients from Arasaka corporation to the closest datacenter according to their location, the DNS server contains a file with two ACL's one named "North" and the other named "South". The North ACL includes terminals from the North branch of the Arasaka corporation and the Datacenter North, the South ACL contains the terminals from the South branch of the Arasaka Corporation and the Datacenter South.

The definition of the zones are conditioned by the views “north” and “south”. The view “north” matches the clients from the ACL “North" with the file “burn-city.org-north.db” and, the view “south” matches the clients from the ACL “South” and “any”(all other clients) with the file “burn-city.org-south.db”. Each file contains the configuration from each zone using the corresponding datacenter(North or South).

To resolve traffic from Militech to the Datacenter South we decided to use “any” in the view “south” since it will achieve the same goal and allow the Operator B to provide datacenter services to future client corporations without any additional configuration(unless those corporations also need privileged connections).

Conclusion

To conclude in this project many different protocols and technologies learned in practical classes were used to accomplish and implement the requirements and objectives of the project. With it we got a better understanding of all these technologies and also a better, in real life view, of network engineering problems and how to overcome them.

All of the main points of the project were implemented with the exception of SDN Services (Open vSwitch).