Relatório Projeto de ARA 2020/2021

Introdução

Neste relatório iremos abordar a construção de uma rede entre 2 operadores, que possuem 2 clientes que podem comunicar entre si e com o exterior. Esta rede possui também serviços VoIP e ainda Datacenters.

Desenho de rede

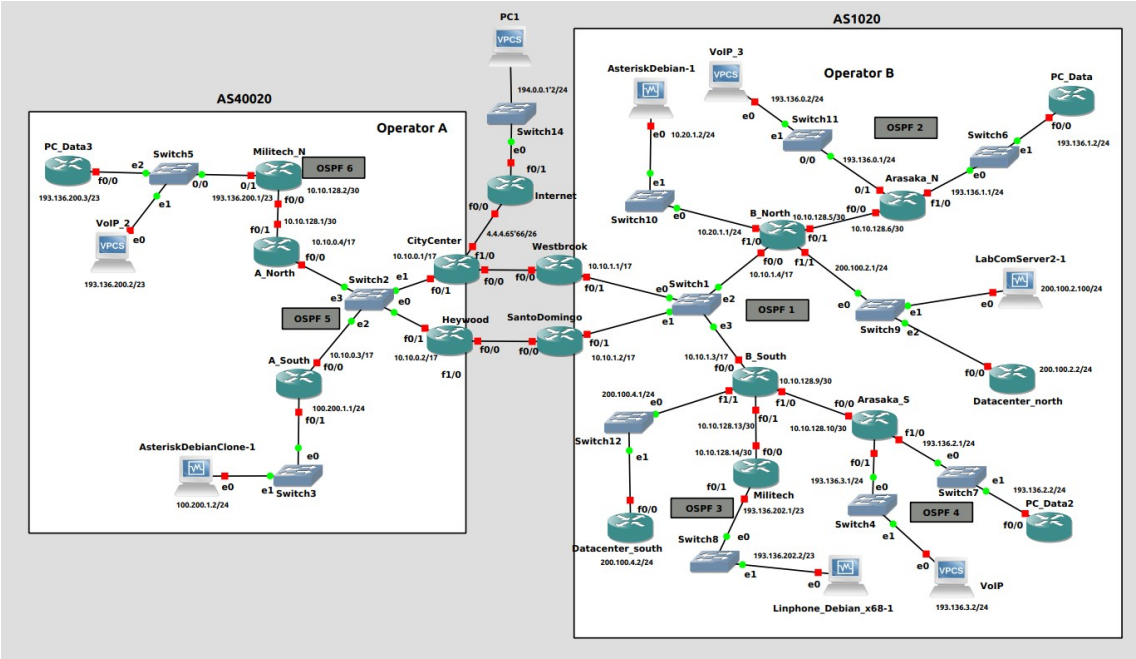

Figura 1: Desenho da rede

Basic mechanisms and Inter-Operator border agreements

Após montarmos a rede, o nosso primeiro objetivo foi ter conectividade total dentro de cada *Autonomous System*. Para isso, implementamos um mecanismo básico de routing, o OSPF. Como os endereços do Core não podem ser anunciados e reconhecidos pelos diferentes clientes (*Arasaka* e *Militech*), tivemos que criar diferentes processos de OSPF.

Pedro Gonçalves 88859
Pedro Silva 89228

Assim, teríamos o Core com um identificador específico de OSPF, no caso do Operador B, OSPF 1, onde colocaríamos todas as redes associadas ao Core, incluindo os Datacenters e os serviços VoIP. Para cada empresa, associámos as suas redes a outro identificador de OSPF. Para que todo o Core conhecesse todas as redes do seu AS, nos routers fronteira entre o Core e as empresas, B_North e B_South no Operador B, no OSPF do Core fizemos uma redistribuição dos processos de OSPF com outro identificador, fazendo com que o Core conhecesse todas as redes das empresas, mas que os clientes não conhecessem o Core.

```
router ospf 1
 redistribute ospf 3
 redistribute ospf 4
 network 10.10.0.0 0.0.127.255 area 0
 network 200.100.4.0 0.0.0.255 area 0
!
router ospf 3
 network 10.10.128.12 0.0.0.3 area 0
!
router ospf 4
 network 10.10.128.8 0.0.0.3 area 0
```

Figura 2: Redistribuição de OSPF no Router B_South

Desta maneira, para obtermos conectividade entre os clientes, tivemos que adicionar uma rota estática aos routers destes, de modo a enviarem tudo o que não conheciam para o router do Core do AS.

Para obtermos conectividade entre ambos os operadores, implementámos 2 relações *Border Gateway Protocol,* uma entre *Citycenter* e *Westbrook*, outra entre *Heywood* e *Santo Domingo*.

De forma a passar todas as redes públicas aprendidas por OSPF de um AS para o outro, necessitamos ainda de inserir o comando ‘redistribute ospf X match internal external 1 external 2’ (em que X é o processo de OSPF adjacente).

Para obtermos conectividade com a Internet, implementámos 1 relação *Border Gateway Protocol* entre o Citycenter e o Router Internet, que é a fronteira do AS da Internet.

Posteriormente, como os Autonomous Systems não devem anunciar rotas privadas para os seus vizinhos nem devem anunciar *default routes*, utilizamos uma filtragem de rotas com *distribute lists.*

Pedro Gonçalves 88859
Pedro Silva 89228

```
ip access-list standard fIn-default
 deny   0.0.0.0
 permit any
ip access-list standard fOut-priv-default
 deny   0.0.0.0
 deny   10.0.0.0 0.255.255.255
 deny   172.16.0.0 0.15.255.255
 deny   192.168.0.0 0.0.255.255
 permit any
```

Figura 3: Proibição de redes privadas e default routes

De seguida, tivemos que anunciar as rotas da Internet entre todos os routers fronteira, pois, visto que queremos mandar o tráfego para a Internet pela ligação *Heywood – Santo Domingo*, o *Heywood* terá que conhecer as rotas anunciadas pela Internet. A solução passa pela implementação de *Internal BGP* entre *Heywood* e *Citycenter,* que leva a que *Heywood* conheça todas as rotas aprendidas pelo *Citycenter.*

Inicialmente todo o tráfego estava a ir pela ligação *Heywood - Santo Domingo* devido ao facto dos Routers do Core A e Core B terem default routes para essa ligação. Para encaminharmos o tráfego VoIP pela ligação *Citycenter – Westbrook*, tivemos que adicionar *Policy Based Routing*. Para isso, utilizamos uma *access-list* onde especificamos a rede destino, neste caso as redes VoIP, utilizando de seguida um Route-Map para forçar o tráfego a ir pela ligação correta.

```
access-list 101 permit ip any host 193.136.200.2
access-list 102 permit ip any host 100.200.1.2
!
route-map VoIPRouting permit 10
 match ip address 101
 match ip address 102
 set ip next-hop 10.10.1.1
```

Figura 4: Route-map para encaminhar o tráfego do VoIP pela ligação Citycenter - Westbrook

Pedro Gonçalves 88859
Pedro Silva 89228

Como está referido no enunciado, ambos os operadores fornecem os seus serviços a *Militech,* mas esta empresa tem apenas um ponto de acesso ao Internet Core, que é através do Router *B_South.* Isto implica que quando o *Militech_N* pretende fazer um pedido à Internet, tem que comunicar com o *Militech* do Operador B, e este último é que fará o pedido ao Internet Core. Para isso, serão necessários 2 túneis.

O primeiro túnel que desenvolvemos é um túnel GRE IPv4 e tem como origem o Router *Militech_N* do Operador A, e como destino o Router *Militech* do Operador B. Quando o Router *Militech_N* recebe tráfego com destino para o Internet Core, encaminha esse tráfego para o túnel 1. Quando o tráfego chega ao *Militech*, é reencaminhado para o Internet Core como se o pedido fosse efetuado pelo próprio *Militech*.

O segundo túnel que desenvolvemos também é um túnel GRE IPv4 que vai desde o Router Internet até ao Router *Militech*. Quando a Internet recebe tráfego que vai para *Militech_N*, encaminha para o túnel 2.

```
interface Tunnel1
 ip address 10.10.128.22 255.255.255.252
 tunnel source 193.136.202.1
 tunnel destination 193.136.200.1
!
interface Tunnel2
 ip address 10.10.128.26 255.255.255.252
 tunnel source 193.136.202.1
 tunnel destination 194.0.0.1
```

Figura 5: Configuração dos túneis no Router Militech

Provisioning of VoIP services

Relativamente ao serviço de VoIP, de que todos os clientes do Operador B beneficiam, começámos por adicionar 2 proxys (AsteriskDebian e AsteriskDebianClone), o primeiro, na rede do Operador B e o segundo na do Operador A, e também o servidor que vai permitir que esta comunicação seja feita (LinphoneDebian).

Pedro Gonçalves 88859
Pedro Silva 89228

Em seguida configurámos a proxy 1 de forma a saber para onde fazer o encaminhamento das chamadas e a proxy 2 para poder responder às mesmas. Esta configuração foi feita de modo a que apenas as chamadas feitas para Arasaka (234101xxx e 289101xxx) e Militech (289102xxx) tenham resposta.

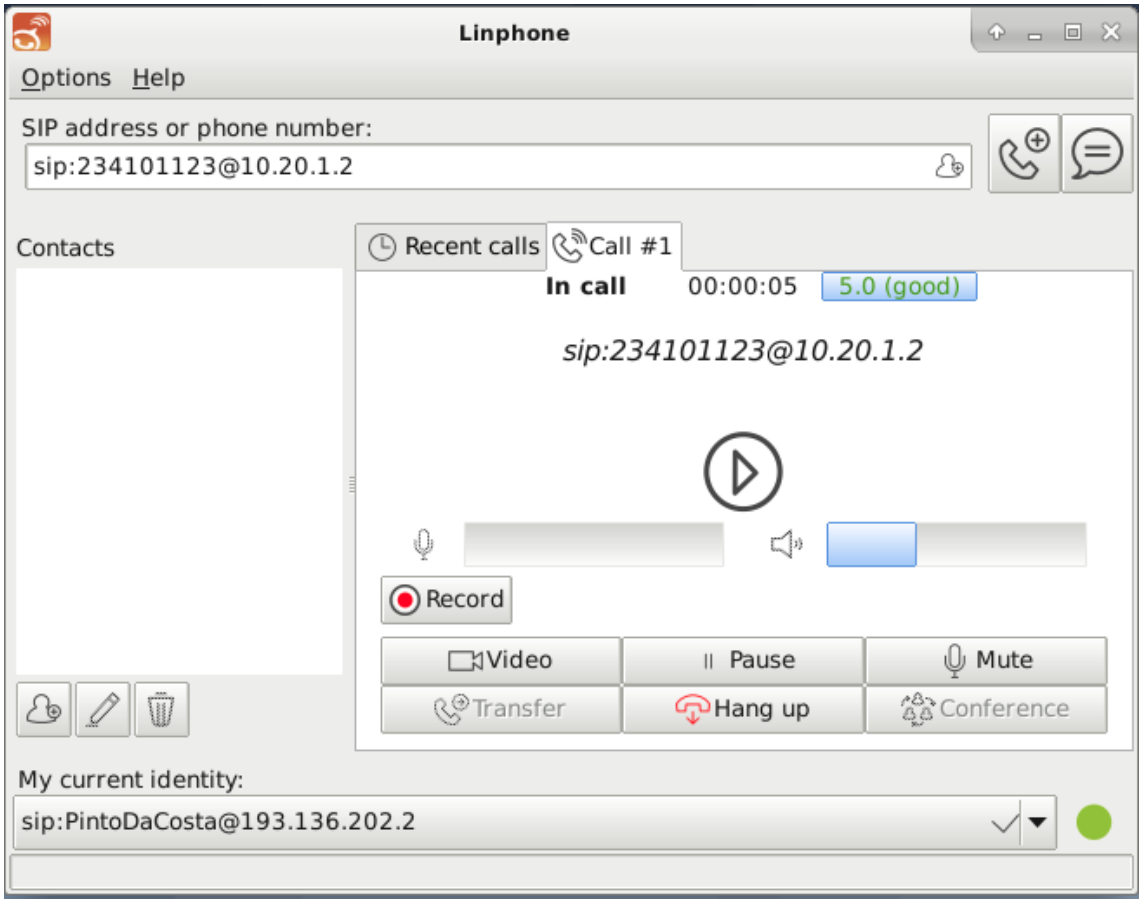

Figura 6: Telefonema da Proxy 1 para a Proxy 2

Provisioning of Datacenter Services

Iniciámos esté tópico com a configuração dos Datacenters e dos PCs, como Routers sem capacidade de routing.

Em seguida passámos para a configuração do servidor DNS, este é essencialmente uma máquina virtual onde adicionamos os vários ficheiros e as respetivas configurações.

Pedro Gonçalves 88859
Pedro Silva 89228

O ficheiro GeoIP.acl que contém as *access-lists*, o ficheiro named.conf que relaciona cada prefixo da *access-list* com um determinado ficheiro, no nosso caso AN (Arasaka_N) com o ficheiro 'burn-city.org-north.db' e AS (Arasaka_S) e MT (Militech) com o ficheiro 'burn-city.org-south.db'.

Por fim configurámos estes 2 ficheiros, o primeiro de forma a que qualquer PC de Arasaka_N que queira aceder ao domínio 'burn-city.org' o faça através do Datacenter geograficamente mais perto (Datacenter North) e qualquer PC de Arasaka_S o faça através do Datacenter South.

Podemos então fazer um ping de qualquer PC_Data para o domínio 'burn-city.org' e reparar que do PC_Data3 e PC_Data2 (Militech_N e Arasaka_S respetivamente) o tráfego é enviado para o Datacenter South (200.100.4.2) e do PC_Data (Arasaka_N) é enviado para o Datacenter North (200.100.2.2).

```
PC_Data3#ping burn-city.org

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.100.4.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 116/138/180 ms
```

Figura 7: Ping para o domínio 'burn-city.org' do PC_Data3

Conclusão

Este projeto solidificou os nossos conhecimentos em relação ao modo como os operadores funcionam e deu-nos uma noção de como funciona o encaminhamento de rotas, as vantagens das CDN's e de como se efetua as ligações de voz sobre IP.

Pedro Gonçalves 88859
Pedro Silva 89228