# Projeto Final
# Arquitetura de Redes Avançadas

Universidade de Aveiro

Márcia Pires, Tomás Martins

# Projeto Final
# Arquitetura de Redes Avançadas

Departamento de Eletrónica, Telecomunicações e Informática

Universidade de Aveiro

Márcia Pires, Tomás Martins

(88747) marcia.pires@ua.pt
(89286) tomasfilipe7@ua.pt

janeiro de 2021

# Conteúdo

# Capítulo 1

# Introdução

No âmbito da cadeira de Arquitetura de Redes Avançadas foi desenvolvido um projeto com o objetivo de implementar uma rede com dois operadores e dois clientes corporativos, correndo serviços de VoIP e *data*, assumindo o papel de engenheiro pertecente à equipa de engenharia de cada operador. Esta implementação foi desenvolvida e testada no GNS3.

Esta implementação baseia-se nos conteúdos lecionados e adquiridos ao longo do semestre na respetiva cadeira, visando uma solução ótima e racional, servindo este relatório para explicar todas as escolhas de engenharia tomadas.

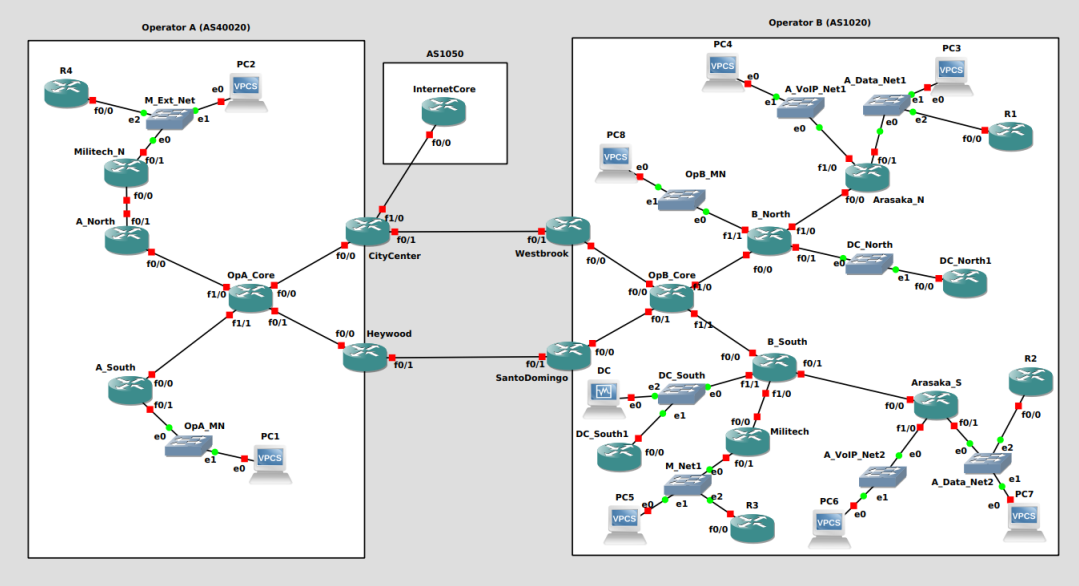


Figura 1.1: Esquema da rede implementada.

# Capítulo 2

# Endereçamento IPv4

| Nome da rede | Endereço |
|---|---|
| **Operador A** | |
| OpA_Core <---> CityCenter | 10.10.0.0/30 |
| OpA_Core <---> Heywood | 10.10.0.4/30 |
| OpA_Core <---> A_North | 10.10.0.8/30 |
| OpA_Core <---> A_South | 10.10.0.12/30 |
| OpA_Core <---> Militech_N | 10.10.0.16/30 |
| Militech_N | 193.136.200.0/23 |
| OperatorA_Media_Network | 100.200.1.0/24 |

Figura 2.1: Tabela de endereçamento IPv4 do Operador A.

| Nome da rede | Endereço |
|---|---|
| **Operador B** | |
| OpB_Core <---> Westbrook | 10.10.128.0/30 |
| OpB_Core <---> SantoDomingo | 10.10.128.4/30 |
| OpB_Core <---> B_North | 10.10.128.8/30 |
| OpB_Core <---> B_South | 10.10.128.12/30 |
| OpB_Core <---> Arasaka_N | 10.10.128.16/30 |
| OpB_Core <---> Arasaka_S | 10.10.128.20/30 |
| OpB_Core <---> Militech | 10.10.128.24/30 |
| Militech | 193.136.202.0/23 |
| Arasaka_N Data | 193.136.1.0/24 |
| Arasaka_N VoIP | 193.136.2.0/24 |
| Arasaka_S Data | 193.136.3.0/24 |
| Arasaka_S VoIP | 193.136.4.0/24 |
| OperatorB_Media_Network | 10.20.1.0/24 |
| Datacenter North | 200.100.2.0/24 |
| Datacenter South | 200.100.4.0/24 |

Figura 2.2: Tabela de endereçamento IPv4 do Operador B.

| Nome da rede | Endereço |
|---|---|
| **Outros** | |
| Tunnels | 10.10.224.0/30 |
| External BGP CityCenter - WestBrook | 4.4.4.0/30 |
| External BGP CityCenter - SantoDomingo | 4.4.4.4/30 |
| External BGP CityCenter - InternetCore | 4.4.4.8/30 |
| Internet_1 | 3.3.3.0 |
| Internet_2 | 2.2.2.0 |
| Loopback Westbrook | 10.10.192.4/32 |
| Loopback SantoDomingo | 10.10.192.5/32 |
| Loopback OpB_Core | 10.10.192.6/32 |
| Loopback B_North | 10.10.192.7/32 |
| Loopback B_South | 10.10.192.8/32 |
| Loopback Arasaka_N | 10.10.192.9/32 |
| Loopback Arasaka_S | 10.10.192.10/32 |
| Loopback CityCenter | 10.10.192.1/32 |
| Loopback Heywood | 10.10.192.1/32 |
| Loopback OpA_Core | 10.10.192.2/32 |
| Loopback A_North | 10.10.192.3/32 |
| Loopback A_South | 10.10.192.4/32 |

Figura 2.3: Tabela de endereçamento IPv4 das restantes ligações.

# Capítulo 3

# Mecanismos básicos e BGP

### 3.0.1 OSPF

Por forma a estabelecer conexão entre todos os routers do **Operador B (AS1020)**, foram ativados **quatro processos de OSPF** no total. Desta maneira, ao não incluir todos os routers no mesmo processo de OSPF, é evitado o aparecimento de tabelas de routing em routers onde não é necessário e só resultaria em sobrecarga.

O router B_North faz a ligação com o lado norte do Operador e portanto inclui uma ligação com a respetiva *Media Network*, uma ligação com a Arasaka *Corporation* Norte (processo 2 de OSPF) e outra com o Datacenter Norte (processo 4 de OSPF). Este mesmo router, B_North, tem ativo o processo 1 de OSPF em direção ao router OpB_Core e é através desse processo que faz a redistribuição dos outros processos de OSPF. Por sua vez, o router Arasaka_N onde corre o processo 2 de OSPF, define as interfaces direcionadas para a rede de VoIP e de Data como *passive-interfaces*.

O router B_South bastante se assemelha ao router B_North: a ligação ao Datacenter Sul também corre o processo 4 de OSPF; a ligação com a Arasaka *Corporation* Sul o processo 2 de OSPF e agora, a ligação com a Militech *Corporation* com o processo 3. Este também tem ativo o processo 1 em direção ao router OpB_Core em que permite a redistribuição dos outros processos. Tal como acontece no router equivalente a Norte, o router Arasaka_S define as interfaces direcionadas para a rede de VoIP e de Data como *passive-interfaces*.

O router do core, OpB_Core, e os routers de Westbrook e SantoDomingo têm o processo 1 de OSPF ativos e redistribuem-no para o protocolo de BGP.

Já no Operador A (AS40020), existem **três processos de OSPF**. No router A_North, que está ligado à Militech, está ativo o processo 3 de OSPF, ajudando desta maneira a que não existam *loops* dada a existência de um túnel no router de Militech. Por sua vez, no router A_South, na ligação com a respetiva *Media Network*, corre o processo 2 de OSPF. Ambos os routers, A_North e A_South, têm ativo o processo 1 de OSPF em direção ao core, e é através dele que é feita a redistribuição dos outros processos.

Assim, no router do core, OpA_Core, e nos routers de CityCenter e Heywood, está ativo o processo 1 de OSPF e redistribuem-no para o protocolo BGP.

### 3.0.2 BGP

O protocolo BGP é usado para encaminhar o tráfego entre Sistemas Autónomos (AS) e dentro dos mesmos. Assim sendo, por forma a conectar os **três diferentes Sistemas Autónomos presentes (AS1020, AS40020, AS1050)**, foi utilizado **eBGP** entre Heywood - SantoDomingo, CityCenter - Westbrook e CityCenter - InternetCore. E, de forma a estabelecer relações dentro da mesma AS, foi utilizado **iBGP**: no Operador A entre CityCenter, Heywood, Core (sendo este o router que faz a interconexão), Operador A Norte e Operador A Sul; e no Operador B entre Westbrook, SantoDomingo, Core (também aqui faz a interconexão), Operador B Norte e Operador B Sul. Estas relações de iBGP são estabelecidas com interfaces Loopbacks de forma a manter as relações independentemente do estado físico das interfaces.

O AS1050, correspondente à "Internet Core"foi criado de modo a que este pudesse anunciar múltiplos prefixos de redes para o Operador A e Operador B, através dos seus vizinhos BGP.

**Restrições de rastreamento**

- O **tráfego de VoIP** pertencente a Arasaka e Militech, entre operadores, deve ser **sempre** encaminhado através da ligação **CityCenter <-> Westbrook**:

  Para tal foi criada uma *ip access list*, tanto no router de CityCenter quanto no de Westbrook, que apenas dá *permit* às redes que queremos que sejam encaminhadas por esta ligação, ou seja, as de tráfego VoIP de Arasaka e Militech. Essa *ip access list* foi anunciada por BGP para os vizinhos.

- O **tráfego de Data e o tráfego para a "Internet Core"**, entre operadores, deve ser sempre encaminhado através da ligação **Heywood <-> SantoDomingo**:

  Neste caso, também foi criada uma *ip access list*, tanto no router de Heywood quanto no de SantoDomingo, que apenas dá *permit* às redes que queremos que sejam encaminhadas por esta ligação, ou seja, as de tráfego de Data. Também esta *ip access list* foi anunciada por BGP para os vizinhos. Para assegurar que o tráfego para a "Internet Core"também fosse encaminhado por esta ligação, no router de SantoDomingo, acrescentou-se uma *default route* que encaminha, para a interface direcionada para a ligação com Heywood, todos os pacotes com endereço de destino desconhecido (ou, neste caso, que será pertencente à "Internet Core"). Também no router de CityCenter existe uma *default route* com o mesmo objetivo, desta vez com a interface direcionada diretamente para a "Internet Core".

# Capítulo 4

# Provisionamento de serviços de redes corporativas

Para que os *branches* Norte e Sul de Arasaka, dentro do Operador B, se interconectassem usando a mesma sub-rede, foi criada uma **VPN MPLS** entre os routers B_North e B_South. Em cada um desses routers foi preciso definir uma VRF VPN bem como definir a interface direcionada para Arasaka, Norte e Sul respetivamente, com essa VPN. Para que a VPN fosse distribuída dentro do BGP, foi preciso definir ambos B_North e B_South como vizinhos e enviar ambas as comunidades. Foi também necessário redistribuir o processo OSPF, o 2 neste caso, dentro da VRF VPN. Por fim, para que a VPN tenha total conectividade, foi preciso uma rota estática tanto em B_North quanto em B_South para a respetiva VPN, e redistribuir essa rota através do processo de OSPF. Foram ainda definidas outras duas rotas estáticas em cada router, uma para a rede de VoIP e outra para a rede de Data, com direção ao router OpB_Core.

Uma vez que ambos os operadores providenciam um serviço para Militech e ambos têm apenas um único ponto de acesso à "Internet Core", que é o router B_South, foi criado um **túnel do modo ipip** entre o router Militech_N (do Operador A) e o router Militech (do Operador B). Desta forma, quando o router Militech_N quiser aceder à Internet, o tráfego é encaminhado pelo túnel até ao router Militech e, a partir daí segue o caminho até à Internet, através do router B_South. Tal acontece porque o router Militech_N tem uma *default route* que encaminha o tráfego de endereço IP desconhecido, ou seja, para a Internet, através do túnel.

# Capítulo 5

# Provisionamento de serviços VoIP

Apesar de na versão final do projeto e na respetiva apresentação, o serviço VoIP não estar funcional nem mesmo completo, tudo foi devido a um problema de transferência de configurações de máquinas virtuais entre computadores. No entanto, dado que trabalhamos para tal, achámos por bem incluir esta nossa parte do trabalho no relatório em que, no mínimo, pudéssemos explicar qual a lógica implementada.

A nossa rede possuía **2 SIP Proxys** , um para cada operador e **3 Linphones**, 2 deles no Operador B e outro no Operador A. Cada SIP Proxy, tinha o objetivo de gerir as ligações efetuadas no seu operador (Proxy 1 para o Operador B e Proxy 2 para o Operador A), enquanto os Linphones serviam para se comunicar entre si.

Aos Linphones do Operador B, foram atribuidos os números **289101000** e **234101000**. Ao Linphone do Operador A, foi atribuido o **289102000**.

Os SIP Proxy, são configurados através de 2 ficheiros principais, *"sip.conf"*, que serve para anunciar os sistemas conhecidos pelo Proxy, e *"extensions.conf"*, que irá conter as instruções para o Proxy executar, quando receber uma ligação com determinadas extensões.

No caso do *"sip.conf"*, cada Proxy iria conter a informação dos Linphones do seu operador, assim como a informação relativa ao outro Proxy.

No ficheiro *"extensions.conf"*, já diferem um pouco, pois apesar de ambos redirecionarem as chamadas para os seus respetivos Linphones, no caso do Proxy1, se este não conhecesse o número da ligação, iria reencaminhar a ligação para o Proxy2. Este por sua vez, iria verificar se conhecia o número da ligação e se não fosse o caso, iria simular uma chamada de voz em que seriam ditos os números marcados pelo cliente (Uma simulação do redirecionamento para a Internet).

```
[Militech_AN]
type=friend
host=dynamic
secret=labcom
context=phones
mailbox=4000@voicemail_project
allow=all

[Proxy_1]
type=peer
host=193.136.2.101
secret=labcom
context=phones
username=Proxy_2
```

Figura 5.1: Ficheiro "sip.conf"do Proxy2.

```
  GNU nano 3.2                          /etc/asterisk/extensions.conf

; use that particular application in this file, the dial plan.
; "core show functions" will list all dialplan functions
; "core show function <COMMAND>" will show you more information about
; one function. Remember that function names are UPPER CASE.

[phones]

exten => _289101.,1,Dial(SIP/Arasaka_BS,10)
exten => _289101.,2,PlayBack(vm-goodbye)
exten => _289101.,3,HangUp()

exten => _234101.,1,Dial(SIP/Arasaka_BN,10)
exten => _234101.,2,PlayBack(vm-goodbye)
exten => _234101.,3,HangUp()

exten => _X.,1,Dial(SIP/${EXTEN}@Proxy_2,10)
```

Figura 5.2: Ficheiro "extensions.conf"do Proxy1.

# Capítulo 6

# Provisionamento de serviços de Datacenter

No Datacenter Sul do Operador B foi estrategicamente colocado um **servidor DNS** (DC) que atua como um servidor *master* para o **domínio "burn-city.org"**. Para implementar o serviço de CDN, este servidor DNS redireciona os seus clientes para o Datacenter mais próximo segundo a sua localização: pedidos de resolução vindos de Arasaka Norte são enviados para o Datacenter Norte (representado pelo router DC_North1, sem *ip routing*) e pedidos de resolução vindos de Arasaka Sul ou Militech, seja do Operador A ou Operador B, são enviados para o Datacenter Sul (representado pelo router DC_South1 também sem *ip routing*).

Este servidor DNS contém um ficheiro chamado "Arasaka.acl"que contém três ACLs: "AN"que inclui os terminais de Arasaka Norte; "AS"que inclui os terminais de Arasaka Sul e "Militech"com os terminais da corporação Militech. No ficheiro */etc/bind/named.conf.local* foram definidas quais zonas são retornadas a cada cliente: a view "ArasakaN"que dá *match* com os clientes da ACL "AN"; a view "ArasakaS"que dá *match* com os clientes da ACL "AS"e por fim a view "Militech"que dá *match* com os clientes da ACL "Militech". Em cada uma destas views é referenciado um ficheiro: *"burn-city.org-arasakan.db"*, *"burn-city.org-arasakas.db"* e *"burn-city.org-militech.db"* respetivamente. É então, em cada um destes ficheiros, definida a zona onde se inclui o endereço IP do Datacenter ao qual os clientes farão os seus pedidos.

Existem quatros routers: R1, R2, R3 e R4 que servem para testar o funcionamento dos Datacenter, podendo ser efetuado o *ping burn-city.org* com sucesso.

# Capítulo 7

# Conclusões

Através deste relatório explicamos de forma detalhada a nossa implementação do projeto final, incluindo os pontos que consideramos mais pertinentes, aqueles em que tivemos mais dificuldades e o porquê das nossas escolhas de engenharia para chegar a uma implementação final otimizada e simples. Consideramos que a maioria dos objetivos foi alcançada com sucesso e que conseguimos implementar uma rede bem fundamentada com base nos conhecimentos adquiridos ao longo da cadeira de Arquitetura de Redes Avançadas.