Arquitetura de Redes Avançada

Relatório

Bruno Aguiar, 80177
José Moreira, 79671

NOTA: Esquema do projeto na última página

1. Basic mechanisms and Inter-Operator border agreements

1.1 Endereçamento IP

Nesta parte inicial do projeto foram atribuídos endereços a todas as redes das operadoras e BGP Peering links. Foi também criada uma rede no core da Internet de forma a testar a conectividade entre as operadoras à Internet.

OPERADOR A (AS 40020)

Militech External Net	193.136.200.1/23
Point-To-Point Network *(Militech-N, A-North)*	10.10.1.8/30
Operator A's Core	10.10.1.0/29
Operator A's Media Network	100.200.1.0/24

REDES EXTERNAS:

External BGP Peering Link *(CityCenter, Internet)*	2.3.4.0/24
Internet's Core network for testing purposes	194.194.194.0/24
External BGP Peering Link *(CityCenter, Westbrook)*	4.4.4.4/30
External BGP Peering Link *(Heywood, SantoDomingo)*	4.4.4.0/30

OPERADOR B (AS 1020)

Operator B's Core	10.10.0.0/29
Operator B's Media Network	10.20.1.0/24
Arasaka VoIP Net 1	193.136.2.0/24
Arasaka Data Net 1	193.136.0.0/24
Datacenter North	200.100.2.0/24
Datacenter South	200.100.4.0/24
Militech Net 1	193.136.202.0/23
Arasaka VoIP Net 2	193.136.3.0/24
Arasaka Data Net 2	193.136.1.0/24

1.2 BGP Neighboring

O passo seguinte foi estabelecer relações de BGP Interno e Externo entre os routers intra-operador e inter-operador, respetivamente.

Foi definido que, no operador A, os routers A_North, A_South, CityCenter e HeyWood deveriam correr o processo BGP, enquanto no operador B os routers WestBrook, SantoDomingo, B_North e B_South.

Os routers Militech_N, Militech, Arasaka_N e Arasaka_S são routers que tratam os clientes corporativos e não estão propriamente na fronteira entre os dois operadores e a Internet, onde o BGP é usado para estabelecer relações de vizinhança entre dos ISPs (Internet Service Providers), e por isso não se configuraram processos de BGP neles.

Os routers A_North, A_South, B_North e B_South, não estão na vizinhança dos dois operadores, então vão apenas estabelecer relações de BGP Interno (iBGP) com routers no mesmo Sistema Autónomo (AS), ou seja, com o mesmo Número de AS.

Como exemplo, a configuração BGP para o router A_North:

```
router bgp 40020
 neighbor 10.10.1.2 remote-as 40020 ! iBGP neighboring
 neighbor 10.10.1.3 remote-as 40020 ! iBGP neighboring
 neighbor 10.10.1.4 remote-as 40020 ! iBGP neighboring
```

Já nos routers CityCenter, WestBrook, HeyWood e SantoDomingo, como são vizinhos de routers de outro operador, com um número de AS diferente, mas também vizinhos de routers no mesmo AS, vão estabelecer relações de eBGP e iBGP, dependendo do router vizinho.

Exemplo do router CityCenter:

```
router bgp 40020
 bgp log-neighbor-changes
 neighbor 2.3.4.6 remote-as   1     ! eBGP neighboring
 neighbor 4.4.4.6 remote-as   1020  ! eBGP neighboring
 neighbor 10.10.1.1 remote-as 40020 ! iBGP neighboring
 neighbor 10.10.1.2 remote-as 40020 ! iBGP neighboring
 neighbor 10.10.1.3 remote-as 40020 ! iBGP neighboring
```

1.3 Configuração do Atributo Next-Hop-Self:

Numa sessão eBGP, um router muda por padrão o atributo next-hop de uma rota BGP quando algum outro router eBGP envia uma rota para ele. No entanto, um dos problemas com o iBGP é que um router iBGP não muda o endereço IP do next-hop se o NLRI tiver um next-hop diferente de 0.0.0.0, podendo causar problemas de acessibilidade na rede. Foi então necessário que alguém que estivesse na fronteira entre AS diferentes lhe anunciasse as rotas externas.

Como os routers CityCenter, WestBrook, HeyWood e SantoDomingo possuem ligações eBGP, foram configurados como Route Reflectors:

Exemplo da configuração para o CityCenter:

```
router bgp 40020
 neighbor 10.10.1.1 next-hop-self
 neighbor 10.10.1.2 next-hop-self
 neighbor 10.10.1.3 next-hop-self
```

1.4 eBGP e iBGP com OSPF:

O BGP é o protocolo de escolha quando é necessário controlar que tráfego entra e sai da rede AS e pôr em prática contratos legais entre operadoras, no entanto os protocolos existentes de IGP's (como o OSPF) são mais rápidos a lidar com mudanças na topologia de uma dada rede e permitem mais escalabilidade. Devido a este factor, a decisão foi implementar o OSPF dentro dos Sistemas Autónomos de ambos os operadores.

Além dos routers a correr o processo de BGP, desta vez, também os routers que lidam com os clientes corporativos (Arasaka_N e Arasaka_S) foram configurados com o processo OSPF.

Exemplo do Router A_South a anunciar as suas redes no processo OSPF interno ao Operador A:

```
router ospf 1
 network 10.10.0.0 0.0.255.255 area 0
 network 100.200.1.0 0.0.0.255 area 0
```

Nos Routers Militech_N e Militech acabou por se retirar o processo de OSPF, que foi substituído rotas estáticas, para a tentativa de implementação de MPLS VPN (ver mais à frente sobre "*Provisioning of Corporate networking Services*".

Por vezes era necessário redistribuir rotas BGP para um IGP, devido aos routers que não participam nos processos de BGP e que precisam de saber as rotas que estão a ser anunciadas por BGP.

Devido a esse problema, decidiu-se então fazer a redistribuição de rotas BGP para OSPF
Nos routers de fronteira, que estabelecem sessões de eBGP *peering*: CityCenter, HeyWood, SantoDomingo e WestBrook.

Exemplo do router de Fronteira WestBrook:

```
router ospf 2
 redistribute bgp 1020 subnets
```

1.5 Redistribuição de Rotas OSPF para BGP:

Como se verificou anteriormente, foi decidido não incorporar BGP nos routers que lidam com os clientes corporativos, no entanto, é necessário redistribuir essas redes para o ambiente BGP, por isso fez-se o processo de redistribuição dessas mesmas redes nos routers iBGP, nomeadamente os routers A_North, A_South, B_North e B_South.

Exemplo do router B_North:

```
router bgp 1020
 redistribute ospf 2
```

1.6 Propagação de rotas privadas e restrições de rotas:

Nenhum dos Sistemas Autónomos deve anunciar as suas rotas privadas ou default para a Internet! Também se deve negar as rotas default vindas de outras AS. Além destas restrições obrigatórias padrão, foi anunciado o seguinte conjunto de restrições:

- O Tráfego inter-operador VoIP pertencente a Arasaka e Militech deve ser sempre encaminhado pela ligação CityCenter <=> WestBrook
- O Tráfego de dados e o tráfego para a Internet deve ser sempre encaminhado pela ligação HeyWood <=> SantoDomingo.

De modo a implementar este conjunto de políticas de restrição foi utilizada a filtragem de Rotas com Prefix *Lists*.

Analisando Router a Router a implementação das *Prefix Lists* bloqueadas de anunciar:

Nota: A sublinhado estão as rotas restringidas de acordo com o conjunto de restrições específicas para este projeto (ver tabela de mapeamento dos endereços das redes para os nomes das mesmas em "Endereçamento IP").

CityCenter:

```
ip prefix-list priv-network seq 10 deny 10.0.0.0/8 le 32
ip prefix-list priv-network seq 12 deny 172.16.0.0/12 le 32
ip prefix-list priv-network seq 14 deny 192.168.0.0/16 le 32
ip prefix-list priv-network seq 15 deny 100.200.1.0/24
ip prefix-list priv-network seq 16 deny 0.0.0.0/0
ip prefix-list priv-network seq 100 permit 0.0.0.0/0 le 32

ip prefix-list external-network seq 16 deny 0.0.0.0/0
ip prefix-list external-network seq 100 permit 0.0.0.0/0 le 32

router bgp 40020
 neighbor 4.4.4.6 prefix-list external-network in
 neighbor 4.4.4.6 prefix-list priv-network out
```

WestBrook:

```
ip prefix-list external-network seq 16 deny 0.0.0.0/0
ip prefix-list external-network seq 100 permit 0.0.0.0/0 le 32
!
ip prefix-list priv-network seq 10 deny 10.0.0.0/8 le 32
ip prefix-list priv-network seq 11 deny 193.136.0.0/24
ip prefix-list priv-network seq 12 deny 172.16.0.0/12 le 32
ip prefix-list priv-network seq 13 deny 193.136.1.0/24
ip prefix-list priv-network seq 14 deny 192.168.0.0/16 le 32
ip prefix-list priv-network seq 15 deny 200.100.2.0/24
ip prefix-list priv-network seq 16 deny 0.0.0.0/0
```

```
ip prefix-list priv-network seq 17 deny 200.100.4.0/24
ip prefix-list priv-network seq 100 permit 0.0.0.0/0 le 32
```

HeyWood:

```
ip prefix-list external-network seq 100 permit 0.0.0.0/0 le 32
!
ip prefix-list priv-network seq 10 deny 10.0.0.0/8 le 32
ip prefix-list priv-network seq 12 deny 172.16.0.0/12 le 32
ip prefix-list priv-network seq 14 deny 192.168.0.0/16 le 32
ip prefix-list priv-network seq 15 deny 193.136.200.0/23
ip prefix-list priv-network seq 16 deny 0.0.0.0/0
ip prefix-list priv-network seq 100 permit 0.0.0.0/0 le 32
```

SantoDomingo:

```
ip prefix-list external-network seq 100 permit 0.0.0.0/0 le 32
!
ip prefix-list priv-network seq 10 deny 10.0.0.0/8 le 32
ip prefix-list priv-network seq 11 deny 193.136.2.0/24
ip prefix-list priv-network seq 12 deny 172.16.0.0/12 le 32
ip prefix-list priv-network seq 13 deny 193.136.3.0/24
ip prefix-list priv-network seq 14 deny 192.168.0.0/16 le 32
ip prefix-list priv-network seq 15 deny 193.136.202.0/23
ip prefix-list priv-network seq 16 deny 0.0.0.0/0
ip prefix-list priv-network seq 100 permit 0.0.0.0/0 le 32
```

Nestes dois últimos routers foi permitido receber as rotas default de modo a que essas rotas sejam encaminhadas em direção à Internet.

De modo a que estas Prefix Lists tenham efeito prático, precisam de ser configuradas nos processos de encaminhamento, nomeadamente no processo BGP e anunciar ao seu *peer* a sua política de restrições.

Exemplo de configuração das Prefix Lists no BGP, no router HeyWood:

```
router bgp 40020
 neighbor 4.4.4.2 prefix-list external-network in
 neighbor 4.4.4.2 prefix-list priv-network out
```

1.7 Encaminhamento de Rotas padrão para a Internet:

Como se sabe, o Internet Core deve receber as rotas padrão, que não pertencem a nenhum dos dois AS conhecidos. Sabe-se também que essas mesmas rotas devem ser encaminhadas pela ligação HeyWood <=> SantoDomingo. De modo a que esse encaminhamento seja bem sucedido para o AS 1020 (Operador B) é preciso configurar o Router SantoDomingo para anunciar as rotas default para o AS 40020. Para que o AS 40020 reencaminhe, depois, para a Internet.

Assim sendo, inseriu-se a seguinte configuração no router SantoDomingo:

```
router ospf 2
 default-information originate always
```

No AS 40020, foi necessário também de configurar o router CityCenter para anunciar as rotas default presentes no seu AS para a Internet:

```
router ospf 1
 default-information originate always
```

Estando as rotas no router do CityCenter, é preciso encaminhá-las em direção à Internet, ou seja, a um Router que represente a Internet (o router nomeado como "Internet", no nosso projeto). Para isso foi criada uma nova sessão BGP entre estes dois routers e definimos o Router Internet como router que recebe as rotas padrão, criando também um novo Sistema Autônomo nele (AS 1):

```
 router bgp 1
  neighbor 2.3.4.5 remote-as 40020
  neighbor 2.3.4.5 default-originate
```

Assim, qualquer rota padrão que não seja conhecida pelos sistemas AS 40020 e AS 1020 irá sempre ser encaminhada para o router Internet. Caso essa rota tenha origem, ou vem do AS 1020, ela passará sempre pela ligação HeyWood <=> SantoDomingo:

Exemplo de um *traceroute* feito do PC (Router com o *routing* desligado) R7 para um PC na Internet com o IP `194.194.194.1`:

```
R7# traceroute 194.194.194.1
Type escape sequence to abort.
Tracing the route to 194.194.194.1
VRF info: (vrf in name/id, vrf out name/id)
  1 193.136.202.1 28 msec 12 msec 16 msec ! Militech gateway
  2 10.10.0.13 56 msec 24 msec 48 msec ! B_South F1/0
  3 10.10.0.4 56 msec 52 msec 80 msec ! SantoDomingo F0/0
  4 4.4.4.1 152 msec 76 msec 108 msec ! HeyWood F1/0
  5 10.10.1.4 92 msec 76 msec 72 msec ! CityCenter F0/0
  6 2.3.4.6 84 msec 104 msec 100 msec ! Internet F1/1
  7 194.194.194.1 124 msec 84 msec 128 msec ! Internet F1/0
```

1.8 Domínios de trânsito

Neste trabalho, foi considerado também quem deveria ser um domínio de trânsito ou não.

No Operador A, considerou-se que este deveria de ser um domínio de trânsito, isto porque é um meio de transmissão entre a Internet e o Operador B.

O Operador B possui apenas ligações com o Operador A e nenhuma ligação direta com a Internet. Assim, caso um terceiro Sistema Autónomo, com ligação à Internet e ao operador B, queira comunicar com o Operador A, por exemplo, comunica diretamente via internet.

Foram então feitas as devidas alterações na configuração nos *border routers* do AS 1020, como mostrado no exemplo do Router SantoDomingo:

```
ip as-path access-list 1 permit ^$
route-map routes-out permit 10
match as-path 1
router bgp 1020
  address-family ipv4 unicast
  neighbor 4.4.4.1 route-map routes-out out
```

1. Provisioning of Corporate Networking Services

2.1 "Arasaka requested its North and South branches inside Operator B (AS1020) to be interconnected using the same subnet"

Para o primeiro ponto decidiu-se implementar a tecnologia MPLS RSVP-TE estabelecendo assim um túnel entre as sub-redes da mesma *subnet* (`193.136.1.0/22`).

O MPLS RSVP-TE é uma tecnologia muito usada para reservar recursos que nos foram pedidos e por causa disso, decidiu-se implementar esse requerimento usando esta mesma tecnologia. Um desses recursos que podemos reservar de modo a implementar uma política de Qualidade de Serviço é a largura de banda. Para este projeto não foi dado algum tipo de requisito especial, no entanto, foi atribuido 40% da largura de banda das ligações entre routers aos túneis de MPLS RSVP-TE, sendo que cada túnel (neste caso só temos um) irá ajustar automaticamente a sua largura de banda utilizada. Os Routers onde foi implantado o túnel foram os Arasaka_S e Arasaka_N. O túnel é feito de modo dinâmico, portanto o caminho é gerado automaticamente e pode se reajustar mediante as condições da rede.

Os Routers (e interfaces) escolhidos de modo a implementar o caminho dinâmico foram os Routers Arasaka_S (F1/1, F0/0, F0/1), B_South (F1/1 e F0/0), SantoDomingo (F0/0), WestBrook (F0/0), B_North (F0/0, F0/1) e Arasaka_N (F0/1, F1/0 e F1/1), através da configuração do comando `mpls traffic-eng tunnels` na configuração e em cada interface acima citada. Também foi necessário configurar os comandos `mpls traffic-eng area 0` e `mpls traffic-eng router-id Loopback 0` na configuração geral desses Routers (Foram criados também endereços de Loopback para esses mesmos Routers) e `ip rsvp bandwidth percent 40` em cada interface dita anteriormente.

A implementação seguinte foi estabelecer o túnel dinâmico em cada um dos Routers Arasaka_S e Arasaka_N. Exemplo de implementação no Router Arasaka_S:

```
interface Tunnel1
 ip unnumbered Loopback0
```

```
 tunnel mode mpls traffic-eng
 tunnel destination 10.10.2.6
 tunnel mpls traffic-eng path-option 1 dynamic
 tunnel mpls traffic-eng auto-bw

ip route 193.136.2.0 255.255.255.0 tunnel1
ip route 193.136.0.0  255.255.255.0 tunnel1
```

A rota estática foi necessária para reencaminhar o tráfego vindo da rede Arasaka Data Net 2 e da Arasaka VoIP Net 2 para o túnel.

2.2 "Both operators provide a service to Militech: its traffic in a specific network inside both operators, and it has a single access point to the "Internet Core" which is the B_South router;"

Neste segundo ponto, procurou-se implementar a tecnologia MPLS VPN e formar uma overlay network entre o Router A_North e B_South, que opera através MP-BGP e VRF. Da mesma maneira que as VLANs implementam camadas lógicas/virtuais sobre uma LAN física, as VRFs procuram implementar tabelas de encaminhamento e de forwarding de modo a estabelecer redes lógicas sobre uma rede física. Assim, seria possível formar uma rede virtual entre o A_North e o B_South.

Neste projeto, não foi possível uma implementação funcional do MPLS VPN para este ponto. Quando os pacotes chegavam ao router A_North ou B_South, vindos das redes Militech External Net ou Militech Net 1, não eram reencaminhados ao destino (não saíam do router), mas será descrito de qualquer forma os passos tomados.

Primeiro, foi decidido remover o processo OSPF dos Routers Militech_N e Militech e das interfaces F0/1 do Router A_North e F1/0 do Router B_South, já que são as ligações que recebem o tráfego vindo dessas redes que pretendemos estabelecer o MPLS VPN.

Nos Routers Militech_N e Militech implementou-se rotas estáticas de modo a encaminhar o tráfego para os Routers A_North e B_South.

Exemplo para o Militech:

```
ip route 0.0.0.0 0.0.0.0 10.10.0.13 ! F1/0 B_South
```

Nos routers A_North e B_South também se colocaram rotas estáticas de modo a obter conexão total com essas mesmas redes e foram configuradas as restantes interfaces com OSPF.

Exemplo para o B_South:

```
ip route 193.136.202.0 255.255.254.0 FastEthernet1/0 ! F1/0
Militech


interface FastEthernet0/1
```

```
 ip ospf 2 area 0

interface FastEthernet1/1
 ip ospf 2 area 0

interface FastEthernet0/0
 ip ospf 2 area 0
```

Para completar, distribuíram-se essas mesmas rotas no processo OSPF e BGP:

Exemplo para o B_South:

```
router ospf 2
 redistribute static subnets

router bgp 1020
 redistribute static
```

Foi ativado também o protocolo `mpls ip` na configuração dos seguintes routers (e interfaces): Routers A_North (F0/0), B_South (F0/0), CityCenter (F0/0, F1/0) e WestBrook (F1/0 e F0/0).

Foi implementada a seguinte configuração no router A_North, em que o `10.10.2.1` é o endereço de Loopback do Router B_South:

```
ip vrf VPN-Militech
 rd 200:1
 route-target export 200:1
 route-target import 200:1

interface FastEthernet0/1
 ip vrf forwarding VPN-Militech
 ip address 10.10.1.10 255.255.255.252

router  bgp 40020
 bgp router-id 10.10.10.10
 neighbor 10.10.2.1 remote-as 1020
 neighbor 10.10.2.1 update-source Loopback0
 address-family vpnv4
 neighbor 10.10.2.1 activate
 neighbor 10.10.2.1 send-community both
 address-family ipv4 vrf VPN-Militech
 redistribute connected
```

Uma configuração semelhante foi também implementada no router B_South.

De modo a tentar obter conectividade inter-routing global, inseriram-se também as seguintes rotas estáticas:

Router A_North:

```
ip route vrf VPN-Militech 193.136.202.0 0.0.1.255 F0/0
global
```

Router B_South:

```
ip route vrf VPN-Militech 193.136.200.0 0.0.1.255 F0/0
global
ip route vrf VPN-Militech 0.0.0.0 0.0.0.0 F0/0 global
```

2. Provisioning of VoIP services

Para esta parte do projeto instalaram-se dois SIP servers, um na rede Operator B's Media Network (Proxy 1) e outro na rede Operator A's Media Network (Proxy 2). O Proxy 1 irá atender as chamadas internas e reencaminhar para o Proxy 2 todas as outras.

Até à apresentação não foi possível testar o VoIP, visto que eram encontrados problemas a configurar o endereço de IP da máquina virtual do Linphone ao inserir o comando `sudo ip addr add 10.20.1.10/24 dev enp0s3.` Isto porque o utilizador `labcom` não estava na lista de `sudoers`. O professor, durante a apresentação, sugeriu tentar com o comando `su`, de modo a ativarmos a root shell. Foi então possível testar, apenas posteriormente à apresentação, o VoIP com o Linphone. Na prática não é possível reencaminhar as chamadas para o Proxy 2, mas é possível atender as chamadas no Proxy 1.

Primeiro configurou-se o servidor Proxy 1 em `/etc/asterisk/sip.conf` criando-se 3 "utilizadores": o Arasaka_N, o Arasaka_S e o Militech, que são os clientes corporativos, do lado do Operador B.

Exemplo do Arasaka_N:

```
[Arasaka_N]
type=friend      ; informa o Asterisk que planeamos fazer chamadas para o telefone e
                 ; receber chamadas
host=dynamic     ; informa ao Asterisk que o telefone irá nos dizer onde está na rede, em
                 ; vez de estar definido estaticamente
secret=labcom    ; uma password segura
context=phones   ; define que canal é que a chamada irá entrar, definido em
                 ; extensions.conf
allow=all        ; aceitar todos os codecs
```

Foi também configurado o Proxy 1 para reencaminhar tráfego para o Proxy 2:

```
[SIProxy2]
type=peer
host=100.200.1.10 ; endereço do Proxy 2
secret=labcom
username=SIProxy2
```

O passo seguinte foi configurar o ficheiro `/etc/asterisk/extensions.conf`, que possui o fluxo de execução das operações a tomar quando se recebe ou se reencaminha as chamadas.

A configuração para o comportamento de quando se recebe uma chamada para o Arasaka_N é descrita como:

```
#Arasaka_N
exten => _234101.,1,Answer(500)
exten => _234101.,2,PlayBack(vm-received)
exten => _234101.,3,SayDigits(${EXTEN:3})
exten => _234101.,n,PlayBack(vm-goodbye)
exten => _234101.,n,Hangup()
```

Para reencaminhar as chamadas externas, configuramos da seguinte maneira:

```
#External
exten => _.,1,Dial(SIP/${EXTEN}@SIProxy2,10)
exten => _X.,n,Hangup()
```

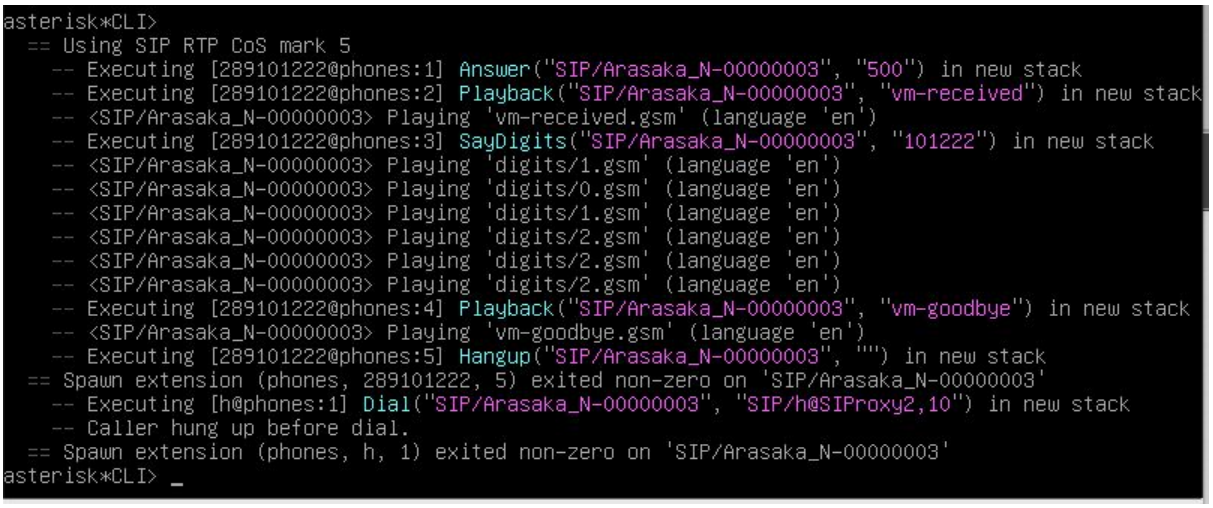
No outro lado, no Proxy 2, ao ficheiro `/etc/asterisk/sip.conf` foi adicionada a seguinte configuração:

```
[SIProxy2]
type=peer
host= 10.20.1.10  ; endereço do Proxy 1
secret=labcom
username=SIProxy2
```

No ficheiro `/etc/asterisk/extensions.conf,` uma configuração semelhante ao ficheiro do Proxy 1 foi feita:

```
[phones]
#External
exten => _X.,1,Answer(500)
exten => _X.,2,PlayBack(vm-received)
exten => _X.,3,SayDigits(${EXTEN:3})
exten => _X.,n,PlayBack(vm-goodbye)
exten => _X.,n,Hangup()
```

Exemplo de uma chamada para o Arasaka_N:



3. Provisioning of Datacenter Services

Relativamente aos Datacenters, o operador B oferece dois, um na zona norte, e outro na zona sul. Devido aos contratos estabelecidos entre o operador, e as empresas Militech e Arasaka, ficou definido que o Datacenter localizado na zona sul responderá a todos os pedidos efetuados por qualquer rede Militech e ainda aos pedidos de Arasaka_S, que está mais próxima do datacenter em questão, e que o Datacenter localizado na zona norte responderá apenas ao pedidos efetuados efetuados por Arasaka_N, devido a sua proximidade com o datacenter em questão. Para isto ocorrer, foi então criado um servidor DNS, e o domínio a ser utilizado será “burn-city.org”. Na configuração deste servidor, foi criado o ficheiro ACL, com um conjunto de BIND Access Control Lists que atribuem às redes IPv4 que pretendemos que obtenham resposta de um dado datacenter um determinado identificador, como por exemplo:

```
acl AN {
     193.136.2.0/24;
     193.136.0.0/24;
};
```

Exemplo representativo de Arasaka_N.

Após a criação deste ficheiro, é necessário carregá-lo para a configuração BIND.
Posteriormente, foram criadas “views”, que nos permite atribuir um servidor a cada conjunto de redes, definido pelo identificador acima abordado.

```
view “arasaka_n” {
     match-clients{AN;};
     recursion no;
     zone “burn-city.org” {
```

```
        type master;
        file "/etc/bind/burn-city.org-arasaka_n.bd";
    };
};
```

Exemplo representativo de Arasaka_N.

Por fim, é necessário a criação dos ficheiros que contêm a informação das máquinas em que o servidor atua.

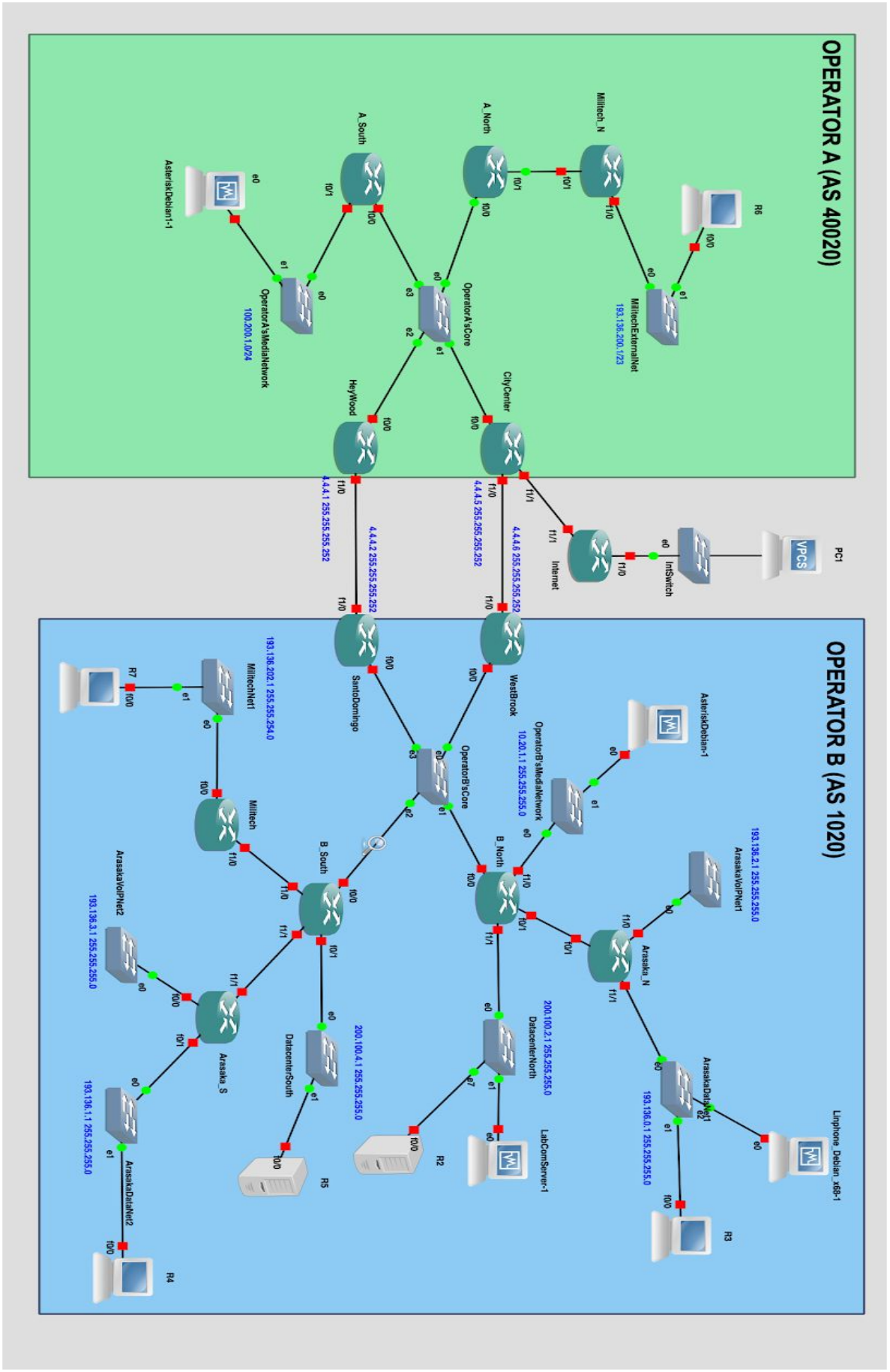
```
$TTL 604800
$ORIGIN burn-city.org.
@    IN   SOA  ns1.burn-city.org. adm.burn-city.org. (
               2 ; Serial
               604800 ; Refresh
               86400 ; Retry
               2419200 ; Expire
               604800 ) ; Negative Cache TTL
     IN   NS   ns1.burn-city.org.
     IN   A    200.100.2.10
ns1  IN   A    200.100.2.2
```

Exemplo representativo de Arasaka_N.

A partir deste momento, é possível efetuar ping de um qualquer terminal pertencente à rede Arasaka Data Net 1 ou Arasaka VoIP Net 1, que será respondido pelo Datacenter North. Seguidamente foram efetuados os mesmos passos para implementar nas restantes redes, tendo em conta que para as restantes, o Datacenter a utilizar será o Datacenter South.

4. Conclusão

Olhando para a realização do projeto, concluímos que fizemos um projeto robusto e consistente, no entanto gostaríamos de ter atingido a funcionalidade total no VoIP e no MPLS VPN, coisa que infelizmente não conseguimos. Faltou também por implementar a componente SDN.


OPERATOR A (AS 40020)
OPERATOR B (AS 1020)
R6
Milltech_N
A_North
A_South
AsteriskDebian1-1
MilltechExternalNet
193.136.200.1/23
OperatorA'sCore
OperatorA'sMediaNetwork
100.200.1.0/24
HeyWood
CityCenter
4.4.4.1 255.255.255.252
4.4.4.5 255.255.255.252
4.4.4.2 255.255.255.252
4.4.4.6 255.255.255.252
PC1
VPCS
InetSwitch
Internet
SantoDomingo
WestBrook
OperatorB'sCore
OperatorB'sMediaNetwork
10.20.1.1 255.255.255.0
AsteriskDebian-1
B_North
B_South
Arasaka_N
Arasaka_S
193.136.2.1 255.255.255.0
ArasakaVoIPNet1
ArasakaVoIPNet2
193.136.3.1 255.255.255.0
ArasakaDataNet1
193.136.0.1 255.255.255.0
ArasakaDataNet2
193.136.1.1 255.255.255.0
Linphone Debian x68-1
R3
R4
200.100.2.1 255.255.255.0
DatacenterNorth
LabComServer-1
R2
200.100.4.1 255.255.255.0
DatacenterSouth
R5
193.136.202.1 255.255.254.0
MilltechNet1
Milltech
R7