Arquitetura de Redes Avançadas

Relatório de Projeto 2020/2021

Mestrado Integrado em Engenharia de Computadores e Telemática
Departamento de Electrónica, Telecomunicações e Informática
Universidade de Aveiro

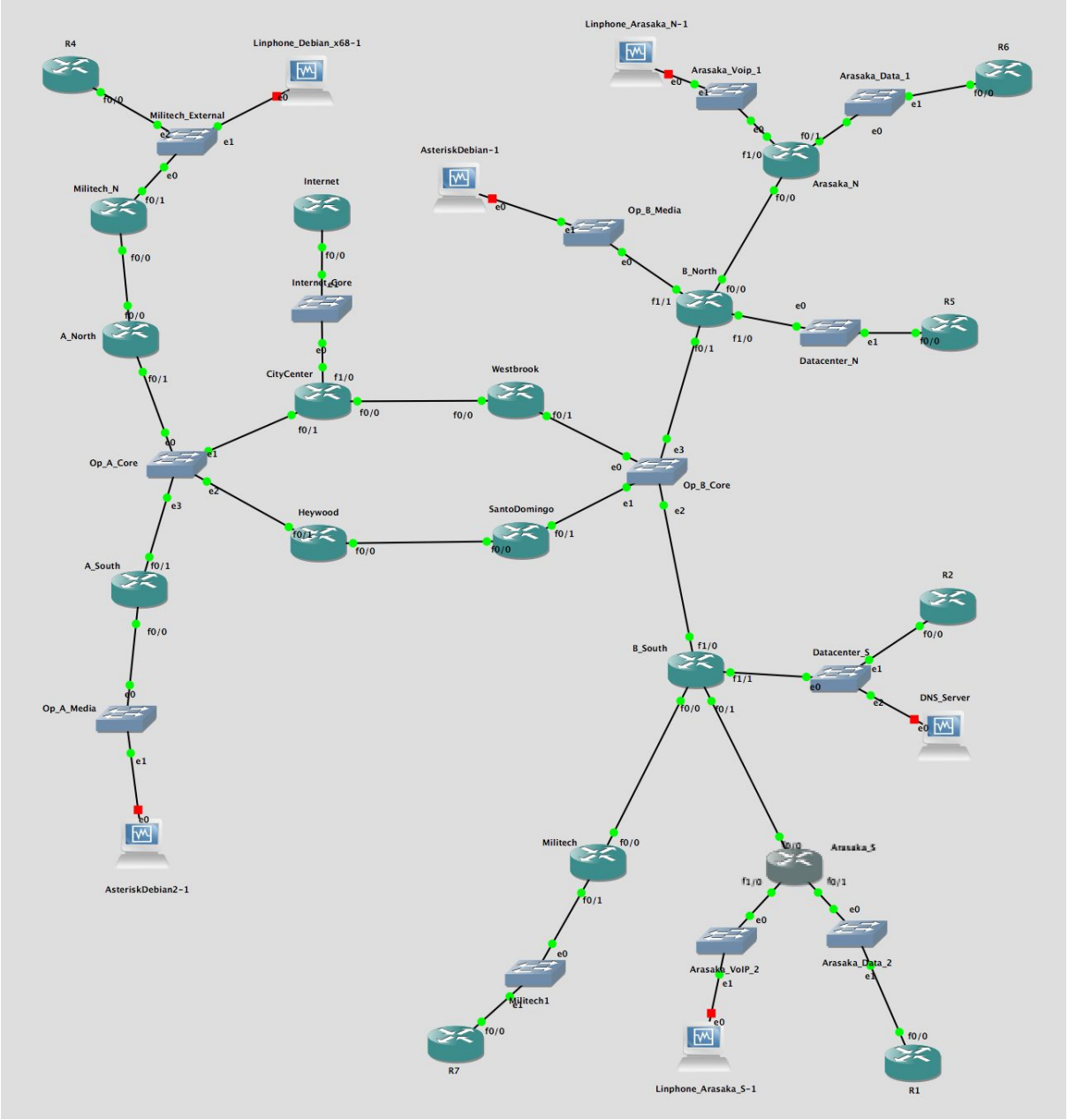
Rui Miguel da Silva Oliveira - 89216 - P1
Rui Pedro Pereira Santos - 89293 - P4

Introdução

No contexto da disciplina de Arquitetura de Redes, foi proposto projetar e configurar uma rede com dois operadores e dois clientes, ambos executando comunicações de voz e dados.
Neste relatório serão explicadas as decisões de engenharia que foram seguidas na construção do projeto.

Desenvolvimento

Desenho da rede



Endereços IP

Op. B Loopbacks	10.10.0.0/24
Op. B Core	10.10.1.0/24
B_South - Militech	10.10.2.0/30
B_South - Arasaka_N	10.10.2.8/30
B_North - Arasaka_N	10.10.2.12/30
Op. A Loopbacks	10.10.128.0/24
Op. A Core	10.10.129.0/24
A_North - Militech_N	10.10.130.12/30
CityCenter - Westbrook	4.4.4.0/30
Heywood - SantoDomingo	4.4.4.4/30
CityCenter - Internet	4.4.4.8/30
Arasaka_Data_1	193.136.0.0/24
Arasaka_VoIP_1	193.136.1.0/24
Arasaka_Data_2	193.136.2.0/24
Arasaka_VoIP_2	193.136.3.0/24
Militech1	193.136.200.0/24
Militech_External	193.136.202.0/24
Datacenter_N	200.100.2.0/24
Datacenter_S	200.100.4.0/24
Op_A_Media	100.200.1.0/24
Op_B_Media	10.20.1.0/24
Tunel Militech_N - Militech	10.10.20.0/30
Tunel CityCenter - Militech	10.10.30.0/30
Internet Network	8.8.8.0/24

Mecanismos básicos e acordos de fronteira entre operadores

Border Gateway Protocol (BGP)

Para haver conectividade entre terminais, mecanismos de routing entre redes precisam de ser estabelecidos. Para encaminhar o tráfego entre os Sistemas Autônomos (AS), utilizámos o Border Gateway Protocol (BGP).
Entre routers fronteira, as rotas foram trocadas usando *External Border Gateway Protocol (eBGP)* e as relações de vizinhança foram estabelecidas entre os IPs dos links ponto a ponto. Assim, apenas pares diretamente conectados estabeleceram vizinhanças eBGP entre eles.
Dentro dos Sistemas Autónomos foi utilizado o Open Shortest Path First (OSPF) para fazer o routing e foram utilizados diversos processos para que as empresas não conhecessem os IPs do *core* do Operador. Assim, foram configuradas rotas default para o router de *core* (routers As e Bs) que contêm tanto os processos OSPF do core como o da empresa e foram redistribuídas as rotas do ospf da empresa no OSPF do *core*.

Internet

A internet é representada pelo router Internet que contém o AS2020. Este router contém também a rede 8.8.8.0/24 que é anunciada por BGP para o AS40020 que depois a anuncia para o AS1020 também por BGP.
No operador A, a conexão com a Internet é feita pelo router CityCenter e este foi configurado para anunciar por ospf 1 uma rota por defeito para ele mesmo, podendo depois encaminhar o tráfego para a Internet.
No operador B, sempre que o destino de um pacote fôr desconhecido, este deverá ser encaminhado para o router SantoDomingo que depois tem uma rota por defeito para o router Heywood quando não conhece o destino do pacote. No operador B foi escolhido o router SantoDomingo como destino por defeito em vez do Westbrook visto que este tráfego, que não é conhecido, não é VoIP e portanto deve passar entre Heywood e SantoDomingo.

Preferências no routing entre operadores

Para satisfazer as preferências estabelecidas no enunciado do projeto relativamente ao tráfego entre operadores foram implementadas 2 communities em cada um dos 4 routers eBGP's. O uso de communities tem algumas vantagens relativamente a outros mecanismos como o simples bloqueio de certas redes no BGP como o facto de haver uma rota alternativa no caso da ligação preferida "cair". Achámos que seria bastante importante assegurar que o tráfego tinha sempre rotas para o seu destino e portanto optou-se por utilizar communities.
As communities foram aplicadas num route map contendo as prefix lists: *voip_prefix_list* e *no_voip_prefix_list*. Tal como o nome indica, na *voip_prefix_list* foram permitidas as redes relativas ao voip e negadas todas as restantes. Na prefix list *no_voip_prefix_list* foram negadas as redes de voip e permitidas as restantes.
O route map *routes-in* recebe as communities do eBGP a que está ligado e define as local-preferences de acordo com a localização do router.

No código seguinte está representado um excerto das configurações relativas às referidas preferências configuradas no router CityCenter:

```
ip prefix-list no_voip_prefix_list seq 10 deny 193.136.0.0/23 le 32
ip prefix-list no_voip_prefix_list seq 12 deny 10.20.1.0/24 le 32
ip prefix-list no_voip_prefix_list seq 14 deny 10.10.0.0/16 le 32
ip prefix-list no_voip_prefix_list seq 100 permit 0.0.0.0/0 le 32
!
ip prefix-list voip_prefix_list seq 10 permit 193.136.0.0/23 le 32
ip prefix-list voip_prefix_list seq 12 permit 10.20.1.0/24 le 32
ip prefix-list voip_prefix_list seq 100 deny 0.0.0.0/0 le 32
no cdp log mismatch duplex
!
route-map westbrook-citycenter_rm permit 10
match ip address prefix-list voip_prefix_list
set community 1020:1
!
route-map westbrook-citycenter_rm permit 20
match ip address prefix-list no_voip_prefix_list
set community 1020:2
!
route-map routes-in permit 10
match community 1
set local-preference 22
!
route-map routes-in permit 20
match community 2
set local-preference 111
```

Provisionamento de serviços de rede corporativa

MPLS/VPN

Visto que o cliente Arasaka solicitou que suas filiais norte e sul dentro da Operadora B (*AS1020*) fossem interconectadas usando a mesma sub-rede, considerámos que uma VPN MPLS seria uma boa solução nesse sentido. Assim o primeiro passo para o conseguir foi criar uma VRF nos routers Arasaka e associá-la às interfaces. Posteriormente, a família de endereços *vpnv4* foi configurada em ambos os *routers*, de modo que, por meio do *MP-BGP (Multi-Protocol Border Gateway Protocol)*, as rotas entre as filiais do cliente A pudessem ser trocadas. Foi também necessário ativar o *MPLS* nos routers *B_North* e *B_South* para que os pacotes pudessem ser encaminhados através de *Multi-Protocol Label Switching (MPLS)*.

Após estas etapas, a conectividade entre as filiais (Arasaka) será estabelecida e uma MPLS Virtual Private Network (MPLS-VPN) será criada (os pacotes entre as filiais serão encaminhados por meio de MPLS). Para que as filiais do cliente A tenham conectividade com o exterior, foram estabelecidas rotas estáticas para o interior da VPN a apontar para o *router fronteira* mais próximo.

As rotas estáticas também foram redistribuídas via OSPF.

ip route 0.0.0.0 0.0.0.0 FastEthernet0/0 10.10.2.9
ip route 193.136.0.0 255.255.255.0 FastEthernet1/0
ip route 193.136.2.0 255.255.255.0 FastEthernet0/1

Para adicionar uma rota padrão à VPN-1 usando a tabela de encaminhamento global para encontrar o próximo salto usamos a rota seguinte:

ip route vrf VPN-1 0.0.0.0 0.0.0.0 10.10.2.9 global

Acesso único à Internet do *Militech* (Túnel GRE/IP)

A empresa Militech tem um único acesso à Internet que é feito no router B_South. Para isso foi necessário colocar um túnel do Militech_N (Operador A) para o Militech (Operador B). O tipo de túnel escolhido foi gre/ip tendo este a vantagem de ser uma forma segura de transportar os pacotes.
Quando os pacotes regressam da Internet para o Militech_N devem ser encaminhados por outro túnel gre/ip entre o CityCenter e o Militech. Para encaminhar os pacotes, foi implementado um route map que fazia com que todos os pacotes cujo destino fosse a rede do Militech fossem por este túnel:

```
access-list 102 permit ip any 193.136.200.0 0.0.2.255
!
route-map netParaMil permit 10
 match ip address 102
 set interface Tunnel2
!
```

Provisionamento de serviços VoIP

Foi também implementado um serviço Voice over IP (VoIP) - Session Initiation Protocol (SIP) no operador B através do SIP Proxy 1.
Usando o Asterisk como servidor/proxy SIP no AsteriskDebian, algumas contas de utilizador foram criadas e configuradas:

```
[ArasakaVoipN]
type=friend
host=dynamic
secret=labcom
context=phones
allow=all

[ArasakaVoipS]
type=friend
host=dynamic
secret=labcom
contect=phones
allow=all

[Militech]
type=friend
host=dynamic
secret=labcom
context=phones
allow=all

[AsteriskDebian2]
type=peer
host=100.200.1.2
defaultuser=AsteriskDebian
secret=labcom
context=phones
```

Em ambos os Proxies, foram definidos os contextos no ficheiro extensions.conf. No AsteriskDebian optou-se por associar os diferentes números aos respetivos nomes. No caso dos números pertencerem ao Militech ou não estarem referidos, são redirecionados para o Proxy2 (AsteriskDebian2):

```
[public]

exten => 234101777,1000,Dial(SIP/ArasakaVoipN,10)
exten => 289101777,1000,Dial(SIP/ArasakaVoipS,10)
exten => 289102777,1000,Dial(SIP/Militech,10)

exten => _234101.,1,Answer(500)
exten => _234101.,n,Playback(demo-congrats)
exten => _234101.,n,Playback(vm-goodbye)
exten => _234101.,n,Hangup()

exten => _289101.,1,Answer(500)
exten => _289101.,n,Playback(demo-congrats)
exten => _289101.,n,Playback(vm-goodbye)
exten => _289101.,n,Hangup()

exten => _X.,1,Dial(SIP/${EXTEN}@AsteriskDebian2,10)
```

A configuração do ficheiro sip.conf do Proxy2 é bastante semelhante à do Proxy1, mudando apenas o nome e o IP do último utilizador. O ficheiro extensions.conf é também muito semelhante, mudando apenas o Dial para as configurações dos números do Militech.

Provisionamento de serviços de datacenter

Para fornecer um serviço de encaminhamento *Content Distribution Protocol (CDN)* para clientes corporativos, foi proposta a implementação de um serviço *DNS*, capaz de direcionar clientes para o datacenter mais próximo de acordo com sua localização, ou seja:

- Terminais *Militech* e *Arasaka_S* para o *datacenter* do sul do operador B
- Terminais *Arasaka_N* para o *datacenter* do norte do operador B.

Já que o *DNS*, por si só, não pode tomar uma decisão com base numa localização geográfica, um banco de dados foi construído onde um conjunto de IPs de rede foi mapeado da seguinte maneira:

```
acl ARASAKA_N {
        193.136.1.0/24;
        193.136.3.0/24;
};
acl ARASAKA_S {
        193.136.0.0/24;
        193.136.2.0/24;
};
acl MILITECH {
        193.136.200.0/24;
};
acl MILITECH_N {
        193.136.202.0/24;
};
```

Agora que todos os IPs estão mapeados consoante a sua localização geográfica, resta escolher para onde encaminhar as solicitações.

```
view "datacenter_north" {
 match-clients { ARASAKA_N; };
 recursion no;
 zone "burn-city.org" {
 type master;
 file "/etc/bind/burn-city.org-datacenter_north.db";
 };
};

view "datacenter_south" {
 match-clients { MILITECH; MILITECH_N; ARASAKA_S; };
 recursion no;
 zone "burn-city.org" {
 type master;
 file "/etc/bind/burn-city.org-datacenter_south.db";
 };
};
```

Cada zona tem seu próprio ficheiro de zona, que aponta para o respectivo datacenter:

```
$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 200.100.4.3
ns1 IN A 200.100.4.2
```

```
$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 200.100.2.2
ns1 IN A 200.100.4.2
```

Conclusão

Com este projeto conseguimos entender como uma rede “aparentemente simples” entre dois operadores se pode tornar complexa quando temos diversas restrições e diferentes tipos de comunicação.
A nossa implementação foi pensada para a rede ser o mais resiliente e compacta possível. Assim, a rede deverá suportar falhas e cada equipamento deve saber apenas o essencial/necessário para comunicar com o resto da rede.
Excluindo a parte relativa ao SND fizemos todos os restantes serviços (VoIP, DNS e MPLS/VPN).

Consideramos, deste modo, que ambos os elementos do grupo contribuíram igualmente no desenvolvimento do projeto.

Nota: Tal como indicado nas normas da entrega do projeto, a submissão não irá conter nenhuma máquina virtual na topologia do gns3 para poder ser testado nos computadores dos docentes, no entanto os ficheiros de configuração das mesmas estarão num directorio à parte.
(Para efeitos de teste: seguir topologia indicada no capítulo com o desenho da rede)