

Relatório de ARA

Arquitetura de Redes Avançada

Mestrado Integrado em Engenharia de
Computadores e Telemática



universidade de aveiro
theoria poiesis praxis

Renato Valente - 89077
Jacinto Luflakio - 89162

Índice

Índice	2
1 - Configuração da Rede de comunicação	3
1.1 - BGP P2P	3
1.2 - Operador A (AS40020)	3
1.3 - Operador B (AS1020)	3
2 - Mecanismos básicos e acordos de fronteira entre operadores	4
2.1 - Full connectivity in and between AS	4
2.2 - Routing constraints	4
3 - Serviços da rede corporativa	5
3.1 - Arasaka's subnet	5
3.2 - Single access to internet core	5
4 - Serviços VoIP	6
5 - Serviços de Datacenter	8

1 - Configuração da Rede de comunicação

1.1 - BGP P2P

Network	ipv4 Address
CityCenter - Westbrook	4.4.4.0/30
Heywood - SantoDomingo	4.4.4.4/30
internet	4.4.4.8/30

1.2 - Operador A (AS40020)

Network	ipv4 Address
A_North - Militech_N	10.10.2.0/30
Operator_A's_Core	10.10.0.0/28
Operator_A's_Media_Net	100.200.1.0/24
Militech_External_Net	193.136.200.0/23

1.3 - Operador B (AS1020)

Network	ipv4 Address
B_North - Arasaka_N	10.10.2.12/30
B_South - Militech	10.10.2.16/30
B_South - Arasaka_S	10.10.2.20/30
Operator_B's_Core	10.10.1.0/28
Operator_B's_Media_Net	10.20.1.0/24
Arasaka_Data_Voip_1	193.136.0.0/24
Arasaka_Data_Voip_2	193.136.1.0/24
Arasaka_Dara_Net_1	193.136.2.0/24
Arasaka_Data_Net_2	193.136.3.0/24
Datacenter_North_Network	200.100.2.0/24
Datacenter_South_Network	200.100.4.0/24
Militech_Net_1	193.136.202.0/23

2 - Mecanismos básicos e acordos de fronteira entre operadores

2.1 - Full connectivity in and between AS

Dentro de cada AS, para cada rede temos um protocolo de roteamento (ospf) diferente ativo, estes protocolos são então redistribuídos pelo protocolo de roteamento do core que por sua vez é redistribuído por BGP para a outra AS. O facto de cada rede ter o seu protocolo ospf previne que as restantes redes se espalhem para as redes dos clientes. Foi também ativado a default route nos routers do core ligados a essas redes, assim permitindo que o tráfego seja encaminhado para os routers do core que conhecem as rotas para as outras redes.

2.2 - Routing constraints

Para permitir que apenas o tráfego VoIP fosse roteado através da ligação CityCenter - Westbrook foram criadas access-lists que permitiam que apenas as redes VoIP e de media de cada operador fossem anunciadas pelo respetivo router fronteira superior (CityCenter ou Westbrook). Quanto ao restante das redes, também através de access-lists, são anunciadas pelos outros routers fronteira (Heywood e SantoDomingo). A rede usada para ligações ponto a ponto é impedida de ser anunciada por todos os routers fronteira. Na ligação entre CityCenter e a internet foi feita uma simulação de uma terceira AS do lado da internet. Esta nova AS envia informações de certas redes. Para evitar que estas redes se propaguem para dentro da rede do operador A foi criada uma access-list que impede todo o tipo de redes provenientes da internet de entrar nas suas tabelas de encaminhamento.

3 - Serviços da rede corporativa

3.1 - Arasaka's subnet

Para interconectar a rede Arasaka na mesma subnet, foi criada uma VPN-MPLS, como Arasaka usa ospf para mapear a topologia da rede as interfaces dos routers north e south com ligação aos routers do cliente também tem o mesmo protocolo de ospf ativo. Foi ativado bgp (ibgp) nos routers core, north e south, assim podendo anunciar as rotas de cada ponta da rede Arasaka. Também foi ativado mpls nas interfaces que ligam os routers north e south ao core, assim podendo identificar através das labels de que parte da rede de Arasaka vem os pacotes.

3.2 - Single access to internet core

Como todo o tráfego em direção à internet (redes não conhecidas pelas duas ASs) tem de roteado pelo router CityCenter, foi criada uma rota estática que redireciona todo o tráfego de dentro da rede em direção a uma rede desconhecida pelas ASs para a interface conectada ao internet core. De maneira a que os outros routers redirecionem o tráfego para o router CityCenter foi ativado no mesmo a default route, esta informação é então propagada por ospf para os routers do core. Como as default routes não são anunciadas por bgp criamos uma rota estática semelhante à do CityCenter no router SantoDomingo, para o router Heywood, e ativamos a default route no mesmo.

Para o tráfego da rede Militech do operador A em direção ao internet core passar sempre pelo router south do operador B foi criado um túnel entre os routers Militech de cada operador (apesar de este não funcionar, pois os routers não sabem as rotas de um para o outro). No router CityCenter foi criado uma route map para encaminhar todo o tráfego, proveniente do internet core, para a rede Militech do operador A pelo túnel que foi configurado entre o router CityCenter e o router Militech do operador B.

4 - Serviços VoIP

Foi implementada a criação de VoIP (Voice over IP) em ambos os AS's, fornecendo através do Proxy 1, com SIP (Session Initiation Protocol), conectividade para os clientes internos e forward para todas as outras chamadas.

No Asterisk server localizado no AS B criamos algumas contas de usuários e a configuração do Proxy 2 situado no AS A como um par com do IP host remoto. (Figura 1)

No Asterisk server localizado no AS A configuramos o Proxy 1 como par. (Figura 2)

Para ambos os Proxy's adicionamos conteúdo no ficheiro extensions.conf, no Proxy 1, adicionamos os números das empresas às respetivas redes. Para todas as outras chamadas que não constam na lista, serão redirecionadas para o Proxy 2. Foi adicionado um número para chamadas de teste. (Figura 3) O Proxy 2 aceita todas as chamadas que recebe, e estas são atendidas pelo atendedor automático que diz os números do número marcado. (Figura 4)

```
[Server2]
type=peer
host=100.200.1.100
secret=labcom
context=public
username=Server1

[ArasakaVoipS]
type=friend
host=dynamic
secret=labcom
context=public
allow=all

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

Figura 1. Configuração SIP do ficheiro sip.conf do Proxy 1

```
[Server1]
type=peer
host=10.20.1.100
secret=labcom
context=public
```

Figura 2. Configuração SIP do ficheiro sip.conf do Proxy 2

```
[public]
exten => 10,1,Answer(500)
exten => 10,n,Playback(demo-congrats)
exten => 10,n,Playback(vm-goodbye)
exten => 10,n,Hangup()

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

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

exten => _X.,1,Dial(SIP/${EXTEN}@Server2,10)
```

Figura 3. Configuração do ficheiro extensions.conf do Proxy 1

```
[public]

exten => _X.,1,Answer(500)
exten => _X.,n,Playback(vm-recieved)
exten => _X.,n,SayDigits(${EXTEN}:3)
exten => _X.,n,Playback(vm-goodbye)
exten => _X.,n,HangUp()
```

Figura 4. Configuração do ficheiro extensions.conf do Proxy 2

5 - Serviços de Datacenter

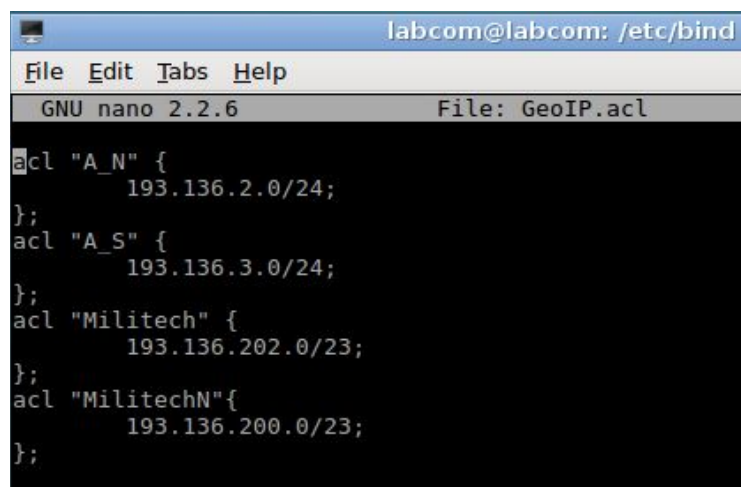
Criação de um serviço de roteamento CDN (Content Distribution Protocol) para clientes do Operador B, para isso implementamos um serviço de DNS sob o nome do domínio de “burn-city.org”.

Clientes têm alguns privilégios de conexão ao servidor em que iram ser sempre enviados para os Datacenter mais próximos (definido geograficamente), ou seja, clientes da network Arasaka North irão ser enviados para o Datacenter North e clientes da network Arasaka South irão ser enviados para o Datacenter South .

Para este mapeamento construímos um banco de dados com ACL's que contêm um conjunto de ip's. (Figura 5)

Usamos as ACL's criadas na configuração das zonas para encaminhar os clientes para Datacenter mais próximo. (Figura 6)

Cada zona tem o seu próprio ficheiro que aponta para o seu respetivo Datacenter. (Figuras 7, 8, 9 e 10)



```
labcom@labcom: /etc/bind
File Edit Tabs Help
GNU nano 2.2.6 File: GeoIP.acl

acl "A_N" {
    193.136.2.0/24;
};
acl "A_S" {
    193.136.3.0/24;
};
acl "Militech" {
    193.136.202.0/23;
};
acl "MilitechN"{
    193.136.200.0/23;
};
```

Figura 5. Configuração das ACL's


```

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

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

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

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

```

Figura 6. Configuração das Zonas no ficheiro named.conf.local

```

GNU nano 2.2.6      File: burn-city.org-Arasaka_N.db
$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        200.100.2.101
ns1       IN      A        200.100.4.100

```

Figura 7. Configuração da Zonas Arasaka_N

```

GNU nano 2.2.6      File: burn-city.org-Arasaka S.db
$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        200.100.4.101
ns1        IN      A        200.100.4.100

```

Figura 8. Configuração da Zonas Arasaka_S

```

GNU nano 2.2.6      File: burn-city.org-Militech.db
$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        200.100.4.101
ns1        IN      A        200.100.4.100

```

Figura 9. Configuração da Zonas Militech

```

GNU nano 2.2.6      File: burn-city.org-MilitechN.db
$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        200.100.4.101
ns1        IN      A        200.100.4.100

```

Figura 10. Configuração da Zonas MilitechN

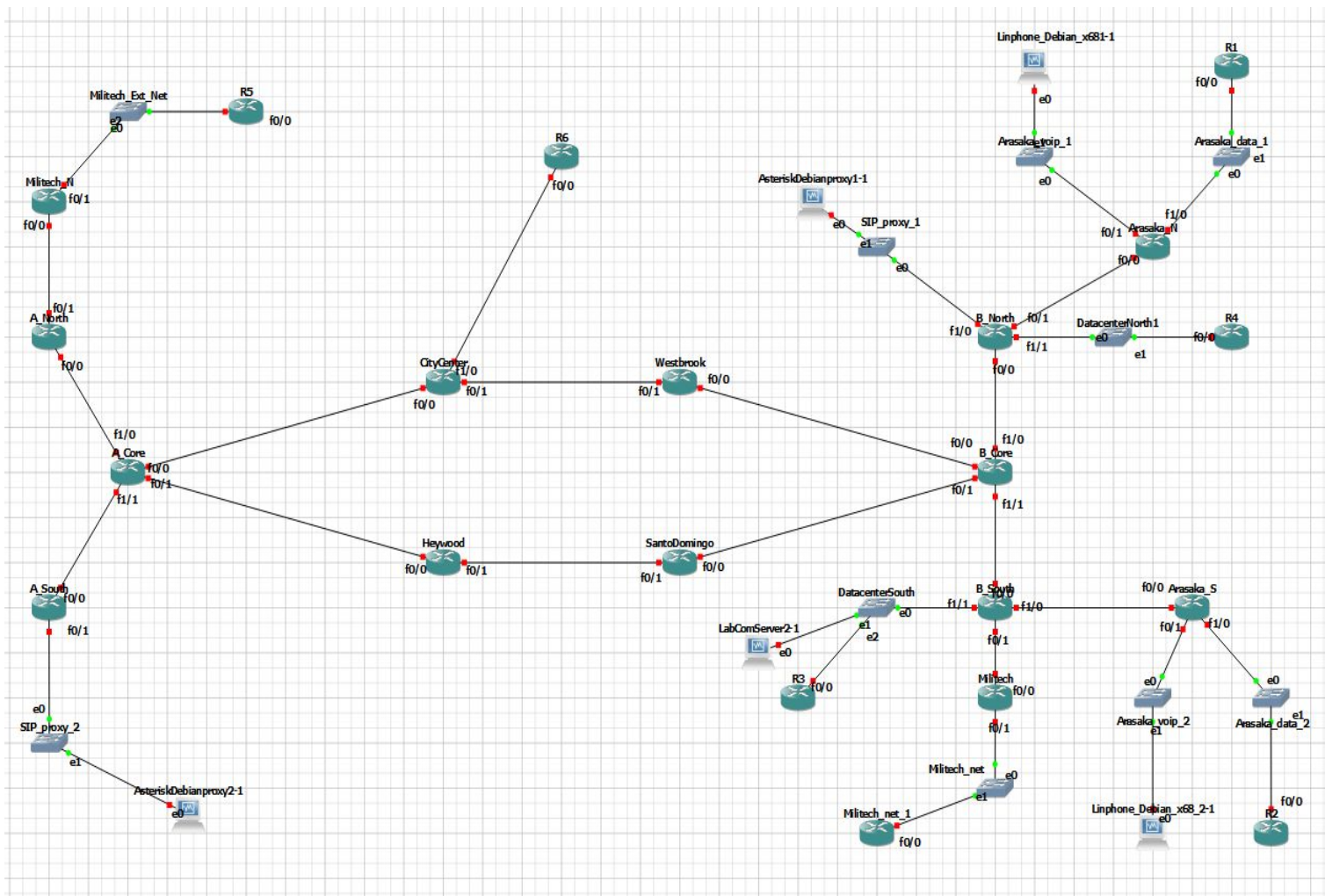


Figura 11. Desenho da Rede