Advanced Network Architecture Project
2018/2019
Projeto de melhoria

Diogo Guedes, nmec: 76318

Teachers: Rui Aguiar, Daniel Corujo

Contents

1) IPv4 Addresses

P2P networks	IPv4 Address	Broadcast Address
p2p: Aveiro ↔ EmpA1	10.0.128.0/30	10.0.128.3/30
p2p: Aveiro ↔ EmpB1	10.0.128.4/30	10.0.128.7/30
p2p: Lisboa2 ↔ Oeiras	10.0.128.8/30	10.0.128.11/30
P2p: Oeiras ↔ EmpC	10.0.128.16/30	10.0.128.19/30
ISP PT2 ↔ Ethernet Core	10.0.0.0/17	10.0.127.255/17
netD1	192.168.1.0/25	192.168.1.255/25
Vlans Oeiras		
EmpA2	192.168.1.248/30	192.168.1.251/30
EmpB2	192.168.1.252/30	192.168.1.255/30
Corporates		
Corporate Client A1	110.1.1.0/25	110.1.1.127/25
Corporate Client A2	110.1.1.128/25	110.1.1.255/25
Corporate Client B1	111.1.1.0/25	111.1.1.127/25
Corporate Client B2	111.1.1.128/25	111.1.1.255/25
Corporate Client C	112.1.1.0/24	112.1.1.255/24
Datacenters		
Datacenter Lisboa	10.2.128.0/17	10.2.128.255/17
Datacenter Oeiras	10.2.0.0/18	10.2.63.255/18
Datacenter Aveiro	10.2.64.0/18	10.2.127.255/18
ISP PT1 (AS40000)		
netL1	65.0.1.0/24	65.0.1.255/24
ISP ES (AS20000)		
netM1	190.100.1.0/24	190.100.1.255/24
netM2	190.200.1.0/24	190.200.1.255/24
External BGP peering links		
Madrid ↔ Lisboa2	5.4.4.0/30	5.4.4.3/30

Madrid ↔ Porto	5.4.4.4/30	5.4.4.7/30
Lisboa1 ↔ Lisboa2	5.4.4.8/30	5.4.4.11/30
Lisboa1 ↔ Madrid	5.4.4.12/30	5.4.4.15/30
Internet Core		
Internet Core	2.2.2.0/24	2.2.2.255/24

Loopback interfaces:

Routers	IPv4 Address
EmpB1	192.168.2.1/32
Aveiro	192.168.2.2/32
Lisboa2	192.168.2.3/32
Oeiras	192.168.2.4/32
EmpA1	192.168.2.5/32
Porto	192.168.2.6/32
EmpA2	192.168.2.7/32
EmpB2	192.168.2.8/32
EmpC	192.168.2.9/32

2) BGP and OSPF configuration

The ISP-PT2 is a multi-homed transit AS, so it's going to route traffic coming from external ASs like 20000, 40000 and from the private AS 65400. The core network of the ISP-PT2 will run:

- iBGP for keeping track of all the routes to client networks and to networks in other ASs. A full mesh will be used to connect the 4 routers
- OSPF for MPLS LSPs, to define the most efficient paths inside the network. The OSPF process will not be aware of any external networks except for the datacenters.

To connect with external public ASs, the routers Porto and Lisboa2 will run eBGP, and to connect to the private AS 65400 the router Oeiras will also run eBGP in the apropriate interface.
The ISP-PT2 core network will connect to its clients through OSPF. The client networks will run OSPF, and the routes learned from this protocol will be redistributed to iBGP in order to make these networks reachable. Datacenters will run OSPF with the ISP-PT2 routers in the same process as the core (process 1).

The ISP-PT2 will run OSPF process 1 for the core network and separate OSPF processes for each client, so:

- Corporate A will have OSPF process 2
- Corporate B will have OSPF process 3
- Corporate C is connected via eBGP so no OSPF process

This way the OSPF process for the core network will not have unnecessary routes from external networks.

The interface that connects Oeiras to netD will be running two OSPF processes: one for Corporate A (id = 2) and one for Corporate B (id = 3).
In order to create MPLS VPN for Corporate A and B, that are connected to the same interface in the Oeiras router, 2 sub-interfaces are needed, one for each:

- f1/0.2: 192.168.1.2, vlan 2
- f1/0.3: 192.168.1.3, vlan 3

The network clients will have a default gateway to the PE router which they are attached to because the associated OSPF process doesn't have external routes.
Because the AS65400 is a private AS, the AS number has to be removed from the AS-Path attribute of each announced route to external ASs. The only public AS that will have the private AS number in the AS-path (of the routes advertised by the private AS) is the AS of the ISP that it is connected to it. In order for the private AS number to be removed from routes going outside the ISP-PT2, the command

```
neighbor <int-ip> remove-private-as all
```

- was used in the ISP-PT2 ASBR routers (Porto and Lisboa2), by specifying the interface IPs of the external ASs ASBRs directly connected to them. This way all route updates, which have the private AS number in the AS-path attribute, to the external ASs ASBRs will have the private AS number removed.

The Internet Core network is advertised via BGP.

a) IP traffic towards Internet should be always routed via ISP PT1.

In order for all traffic to go to the Internet Core network through Lisboa2, the following commands were configured in this router:

```
Lisboa2# conf t
Lisboa2# ip prefix-list internet-destination seq 10 permit 2.2.2.0/24

Lisboa2# route-map route-through-lisboa2 permit 10
Lisboa2# match ip address prefix-list internet-destination
Lisboa2# set local-preference 200
Lisboa2# route-map route-through-lisboa2 permit 20

Lisboa2# conf t
Lisboa2# router bgp 1000
Lisboa2# address-family ipv4 unicast
Lisboa2# neighbor 5.4.4.9 route-map route-through-lisboa2 in
```

- every route being advertised from the internet core to the Lisboa2 router will have local preference 200. The local preference is exchanged with all iBGP peers, so the Lisboa2 router is the only router to have to be configured

b1) IP traffic towards all AS20000 networks, should be preferably routed via Lisboa2 from Oeiras,

```
Oeiras# ip prefix-list as20000-destination seq 10 permit 190.100.1.0/24
Oeiras# ip prefix-list as20000-destination seq 20 permit 190.200.1.0/24

Oeiras# !! Route-map to send traffic through porto
Oeiras# route-map route-through-lisboa2 permit 10
Oeiras# match ip address prefix-list as20000-destination
Oeiras# !! default local preference is 100
Oeiras# set local-preference 110
Oeiras# route-map route-through-lisboa2 permit 20

Oeiras# !! Update neighbor relationships with the route-map
Oeiras# router bgp 1000
Oeiras# address-family ipv4 unicast
Oeiras# neighbor 192.168.2.3 route-map route-through-lisboa2 in
```

b2) IP traffic towards all AS20000 networks, should be preferably routed via Porto from Aveiro,

```
Aveiro# ip prefix-list as20000-destination seq 10 permit 190.100.1.0/24
Aveiro# ip prefix-list as20000-destination seq 20 permit 190.200.1.0/24
Aveiro# !! Route-map to send traffic through porto
```

```
Aveiro# route-map route-through-porto permit 10
Aveiro# match ip address prefix-list as20000-destination
Aveiro# !! default local preference is 100
Aveiro# set local-preference 110
Aveiro# route-map route-through-porto permit 20

Aveiro# !! Update neighbor relationships with the route-map
Aveiro# router bgp 1000
Aveiro# address-family ipv4 unicast
Aveiro# neighbor 192.168.2.6 route-map route-through-porto in
```

c) IP traffic for remote SIP proxy 2 (to network netL1) must be routed via Porto using the direct peering link to ISP ES

Policy-based routing with Route Maps was used to send traffic from SIP proxy 2 network to network netL1. Policy-based routing is applied to the incoming packets on Lisboa2 (interface f2/0), in order for the ones coming from SIP proxy 2 network and going to netL1 to be sent to the Porto router :

```
Lisboa2# ip access-list extended 101
Lisboa2# permit ip 112.1.1.0 0.0.0.255 65.0.1.0 0.0.0.255

Lisboa2# route-map SIP2-to-netL1-through-Porto permit 10
Lisboa2# match ip address 101
Lisboa2# !set ip next-hop 192.168.2.6
! next hop router Porto
Lisboa2# set ip next-hop 10.0.0.2
Lisboa2# route-map SIP2-to-netL1-through-Porto permit 20

!! apply route-map to interface where the packets from the SIP proxy 2
Lisboa2# network are received
Lisboa2# conf t
Lisboa2# int f2/0
Lisboa2# ip policy route-map SIP2-to-netL1-through-Porto
```

The Porto router also needs to be configured in order for the traffic to not go back to the Lisboa2 router:

```
Porto# ip access-list extended 101
Porto# permit ip 112.1.1.0 0.0.0.255 65.0.1.0 0.0.0.255

Porto# route-map SIP2-to-netL1-through-Porto permit 10
Porto# match ip address 101
Porto# set ip next-hop 5.4.4.5
```

```
Porto# route-map SIP2-to-netL1-through-Porto permit 20

Porto# network are received
Porto# conf t
Porto# int f1/1
Porto# ip policy route-map SIP2-to-netL1-through-Porto
```

This way only the routes coming from netC (where SIP proxy 2 is located) and towards to netL will be necessarily routed through Porto.
Note: I matched all IP addresses of the netL1 network instead of only the SIP proxy 2 IP address because I'm not able to implement VoIP.

d) Packets from AS65400 should be routed to the Internet as generic, but should be routed via Lisbon2 to reach netM1

```
Lisboa2# conf t
Lisboa2# ip access-list extended 102
Lisboa2# permit ip 112.1.1.0 0.0.0.255 190.100.1.0 0.0.0.255

Lisboa2# route-map AS65400-to-netM1-through-Lisboa2 permit 10
Lisboa2# match ip address 102
Lisboa2# set ip next-hop 5.4.4.9
Lisboa2# route-map AS65400-to-netM1-through-Lisboa2 permit 20

Lisboa2# int f2/0
Lisboa2# ip policy route-map AS65400-to-netM1-through-Lisboa2
```

However, because only one route-map can be applied an interface, I had to merge both route-maps (c) and d)) in the Lisboa2 router:

```
Lisboa2# ! SIP proxy 2 network to netL1
Lisboa2# route-map AS65400-routemap permit 10
Lisboa2# match ip address 101
Lisboa2# set ip next-hop 10.0.0.2
! AS 65400 to netM1
Lisboa2# route-map AS65400-routemap permit 20
Lisboa2# match ip address 102
Lisboa2# set ip next-hop 5.4.4.9
Lisboa2# route-map AS65400-routemap permit 30

Lisboa2# int f2/0
Lisboa2# ip policy route-map AS65400-routemap
```

2) MPLS configuration

a) External AS transit traffic should be routed (between Lisboa2 and Porto) over a MPLS tunnel, with reserved bandwidth of 30Mbps.

The MPLS RSVP is going to be running in the Core ISP-PT2 network with bandwidth up to 100Mbps that can be used by MPLS TE tunnels. The bandwidth had to be higher than the requisite for 30Mbps bandwidth for the MPLS tunnel between Porto and Lisboa2.
The tunnel that's going to route external AS transit between Porto and Lisboa2 is going to be a static tunnel. Route-maps were used to send the appropriate traffic (from AS40000 to AS20000 and vice-versa) through the MPLS tunnel.

b) Deploy a MPLS VPN for Corporate client A (interconnecting Aveiro and Oeiras branches),and test this with proper packet tracing.

NetA1 and NetA2 belong to VPN-1. The VRFs are configured in the Provider Edge routers of the ISP-PT2 core network that are connected to the Corporate As networks.

Because the interfaces shutdown when the vrfs are connected to them, the OSPF running in them is also removed and BGP will have no way to know about routes to Corporate networks. In order to make BGP aware of the Corporate networks I tried to configure OSPF in the VFRs and redistribute it to BGP however the error "VRF specified does not match existing router" didn't allow me to do so.
I tried the following configurations, but in order to have full connectivity between all locations I removed these configurations from the routers:

- Aveiro router configuration:

```
Aveiro# !! interface to EmpA1
Aveiro# int f1/0
Aveiro# ip vrf forwarding VPN-1
Aveiro# ip address 10.0.128.1 255.255.255.252

Aveiro# router bgp 1000
Aveiro# address-family vpnv4
Aveiro# neighbor 192.168.2.4 activate
Aveiro# neighbor 192.168.2.4 send-community both

Aveiro# address-family ipv4 vrf VPN-1
Aveiro# !! ospf process 2 within vrf
Aveiro# router ospf 2 vrf VPN-1
Aveiro# address-family ipv4 vrf VPN-1
Aveiro# redistribute ospf 100 metric 1
Aveiro# vrf selection source 110.1.1.0 255.255.255.128 vrf VPN-1
```

```
Aveiro# int f1/0
Aveiro# ip vrf select source
```

- Oeiras router configuration:

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

!! sub-interface to EmpA2
int f1/0.2
ip vrf forwarding VPN-1
ip address 192.168.1.249 255.255.255.252
```

3) CDN configuration

To provide redirection, the service bind9 was used with the following configurations:

- aracdn.com-aveiro.db

```
$TTL 604800
$ORIGIN aracdn.com.
@     IN    SOA   nsl.aracdn.com.   adm.aracdn.com. (
                        2                 ; Serial
                     604800         ; Refresh
                     86400          ; Retry
                     2419200        ; Expire
                     604800 )       ; Negative Cache TTL
      IN    NS    nsl.aracdn.com.
      IN    A     10.2.64.10
nsl   IN    A     10.2.64.10
```

- aracdn.com-lisboa.db

```
$TTL 604800
$ORIGIN aracdn.com.
@     IN    SOA   nsl.aracdn.com.   adm.aracdn.com. (
                        2                 ; Serial
                     604800         ; Refresh
                     86400          ; Retry
                     2419200        ; Expire
                     604800 )       ; Negative Cache TTL
      IN    NS    nsl.aracdn.com.
```

```
      IN    A     10.2.128.2
nsl   IN    A     10.2.64.10
```

- aracdn.com-oeiras.db

```
$TTL 604800
$ORIGIN aracdn.com.
@     IN    SOA   nsl.aracdn.com.   adm.aracdn.com. (
                        2                 ; Serial
                     604800         ; Refresh
                     86400          ; Retry
                     2419200        ; Expire
                     604800 )       ; Negative Cache TTL
      IN    NS    nsl.aracdn.com.
      IN    A     10.2.0.2
nsl   IN    A     10.2.64.10
```

- named.conf.local

```
view "aveiro" {
      match-clients{110.1.1.0/25; 111.1.1.0/25;};
      allow-recursion{any;};
      zone "aracdn.com"{
            type master;
            file "/etc/bind/aracdn.com-aveiro.db";
      };
};
view "oeiras"{
      match-clients{110.1.1.128/25; 111.1.1.128/25; 112.1.1.0/24;};
      allow-recursion{any;};
      zone "aracdn.com"{
            type master;
            file "/etc/bind/aracdn.com-oeiras.db";
      };
};
view "lisboa"{
      match-clients{any;};
      allow-recursion{any;};
      zone "aracdn.com"{
            type master;
            file "/etc/bind/aracdn.com-lisboa.db";
      };
};
```