Instituto Politécnico de Tomar

Escola Superior de Tecnologia de Tomar

Engenharia Informática

Projeto de Redes – Trabalho Prático Nº 2

2014/2015

Trabalho realizado por:

Dário Mendes Nº 17337

Ricardo Cruz Nº 17808

Índice

1 Introdução

Uma rede local de dados é normalmente organizada hierarquicamente, dividindo se em camadas. A cada camada correspondem determinadas funções que operam de acordo com a sua finalidade. O modelo de projeção mais usual consiste em dividir a rede em três camadas hierárquicas:

- Acesso – efetua a interface com os dispositivos terminais e é normalmente constituída por *switches* L2 e *access points*.
- Distribuição - agrega os dados provenientes da camada de acesso antes de serem encaminhados para o core. É também utilizada para segmentar a rede em vários domínios de *broadcast*, e para concretizar políticas de encaminhamento. Nesta camada são utilizados *switches* L3.
- Core - é utilizada para ligar os recursos partilhados, assim como para fazer a interface entre a rede local e a rede pública. São normalmente utilizados *switches* L3 de elevado desempenho e/ou Routers.

Proceder ao desenvolvimento da rede local com esta organização por camadas hierárquicas resulta em implicações no aumento:

- Da escalabilidade.
- Da redundância.
- Do desempenho.
- Da segurança.
- Da facilidade de gestão.

2 Objetivos

Projeção e concretização das camadas de acesso e de distribuição das redes locais de dados.

3 Topologia da Rede

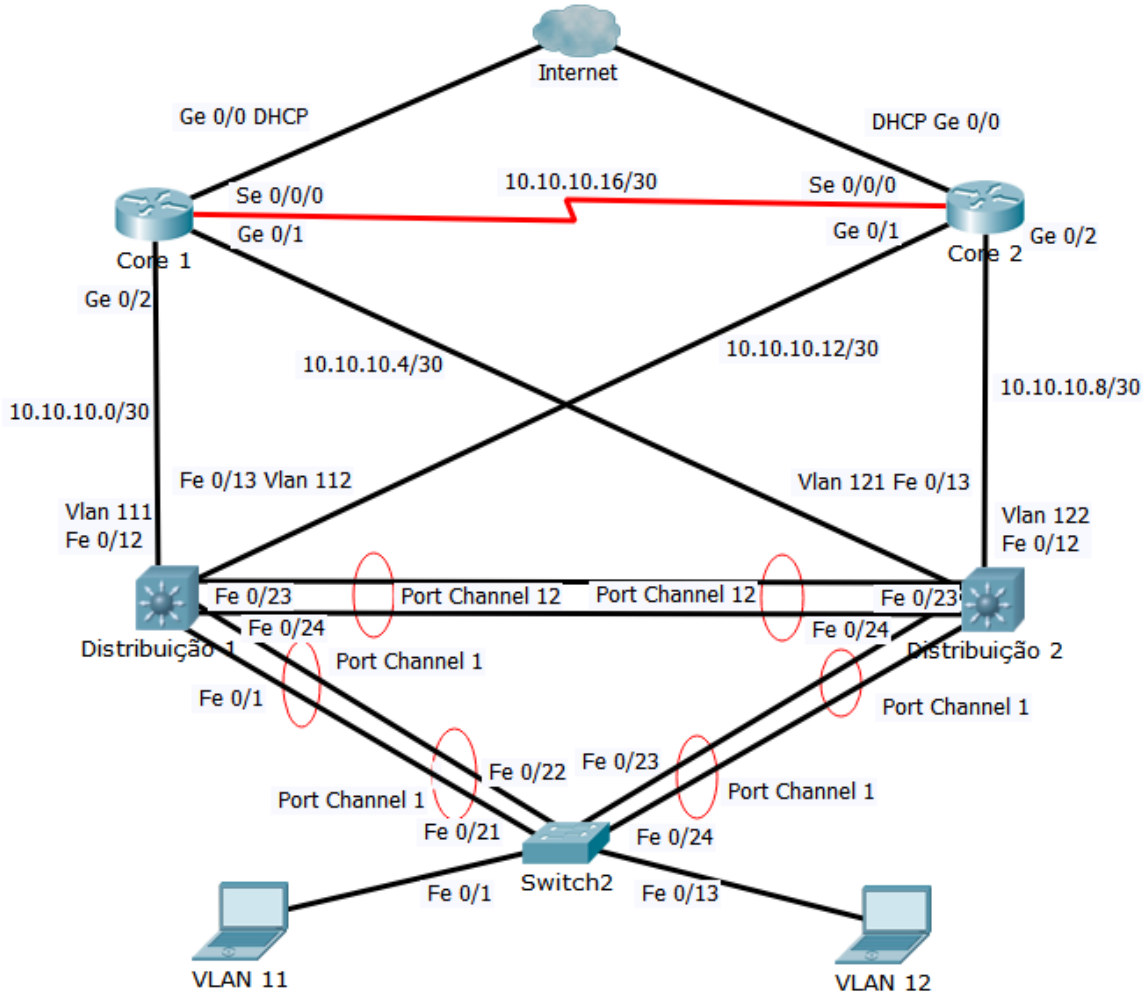

Figura 1: camadas de acesso, de distribuição e Core.

Distribuição 1:

Fe 0/12 – 10.10.10.1 /30

Fe 0/13 – 10.10.10.13 /30

Distribuição 2:

Fe 0/12 – 10.10.10.9 /30

Fe 0/13 – 10.10.10.5 /30

Core 1:

Se 0/0/0 – 10.10.10.17 /30

Ge 0/1 – 10.10.10.6 /30

Ge 0/2 – 10.10.10.2 /30

Core 2:

Se 0/0/0 – 10.10.10.18 /30

Ge 0/1 – 10.10.10.4 /30

Ge 0/2 – 10.10.10.10 /30

4 Procedimentos

4.1 Configurações

Inicialmente procedeu-se à criação das vlan's no switch de acesso.

```
vlan 11
vlan 12
vlan 21
vlan 22
vlan 99
```

A atribuição da identificação das Vlans segue a ideologia seguinte: Vlan 1x e Vlan 1x+1, sendo que x representa o numero do grupo da Rede a ser utilizada.

Configuração das portas FastEthernet. As portas 1 a 12 correspondem ao acesso da Vlan 11 e as 13 a 15 correspondem ao acesso da Vlan 12.

```
interface range FastEthernet0/1-12
switchport access vlan 11
switchport mode access
!
interface range FastEthernet0/13-15
switchport access vlan 12
switchport mode access
```

Foi utilizado o LACP (*Link Aggregation Control Protocol*) de maneira a agregar as portas 21 e 22 no Port-channel1 e as portas 23 e 24 no Port-channel2. Recorreu-se ao modo "trunk" de maneira a associar na *frame* as *vlans* correspondentes a cada Port-channel. Cada Port-Channel vai ser, posteriormente configurado em cada uma das Distribuições 1 e 2 de modo a que haja conexão com o Acesso.

```
interface FastEthernet0/21
switchport trunk allowed vlan 11,12,21,22,99
switchport mode trunk
channel-group 1 mode active
!
interface FastEthernet0/22
switchport trunk allowed vlan 11,12,21,22,99
switchport mode trunk
channel-group 1 mode active
!
interface FastEthernet0/23
switchport trunk allowed vlan 11,12,21,22,99
switchport mode trunk
channel-group 2 mode active
!
interface FastEthernet0/24
switchport trunk allowed vlan 11,12,21,22,99
switchport mode trunk
channel-group 2 mode active
!
interface Port-channel1
switchport trunk allowed vlan 11,12,21,22,99
switchport mode trunk
!
interface Port-channel2
switchport trunk allowed vlan 11,12,21,22,99
switchport mode trunk
```

Procedeu-se à criação das Vlans anteriores nos switchs de distribuição também. Isto vai permitir o encaminhamento de tráfico tendo em conta a Vlan em que este circula.

```
vlan 11
vlan 12
vlan 21
vlan 22
vlan 99
```

Depois foram configurados os Port-Channel que iram coagir com os Port-Channels configurados anteriormente no switch de Acesso. Aqui são permitidos os acessos às Vlans criadas, nas suas portas especificas.

```
interface FastEthernet0/1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 11,12,99
switchport mode trunk
channel-group 1 mode active
!
interface FastEthernet0/2
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 11,12,99
switchport mode trunk
channel-group 1 mode active
!
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 21,22,99
 switchport mode trunk
 channel-group 2 mode active
!
interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 21,22,99
 switchport mode trunk
 channel-group 2 mode active
!
interface FastEthernet0/23
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 11,12,21,22,99
switchport mode trunk
channel-group 12 mode active
!
interface FastEthernet0/24
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 11,12,21,22,99
switchport mode trunk
channel-group 12 mode active
!
interface Port-channel1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 11,12,99
switchport mode trunk
!
interface Port-channel12
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 11,12,21,22,99
switchport mode trunk
```

Em cada um dos Switch Layer 3 foram configuradas três interfaces. Cada interface diz respeito a uma Vlan (11, 12 e a Vlan de gestão 99). Estas interfaces respeitam a sub-rede 172.16.11.10 /24

Distribuição 1:

```
interface vlan11
ip address 172.16.11.1 255.255.255.0
!
interface vlan12
ip address 172.16.12.1 255.255.255.0
!
interface vlan99
ip address 172.16.99.100 255.255.255.0
```

Distribuição 2:

```
interface vlan11
ip address 172.16.11.2 255.255.255.0
!
interface vlan12
ip address 172.16.12.2 255.255.255.0
!
interface vlan99
ip address 172.16.99.101 255.255.255.0
```

De modo a evitar loops na rede e a prevenir uma possível inabilitação de um dos switch de distribuição, passou-se a implementar a configuração do MSTP (Multiple Spanning-Tree Protocol) no qual vão ser criadas cinco instancias uma para cada Vlan existente na rede, tanto do Grupo 1 como do Grupo 2 incluindo a Vlan de gestão.

```
spanning-tree mode mst
spanning-tree extend system-id
!
spanning-tree mst configuration
name region
instance 11 vlan 11
instance 12 vlan 12
instance 21 vlan 21
instance 22 vlan 22
instance 99 vlan 99
```

Definiu-se que a Distribuição 1 seria a default Root Bridge para as Vlans 11 e 99, como tal, para evitar quaisquer equívocos nesse acontecimento recorreu-se a atribuição das prioripadades estáticas seguintes:

```
spanning-tree mst 11,99 priority 4096
spanning-tree mst 12 priority 8192
```

Do mesmo modo foi decidido que a Distribuição 2 seria a default Root Bridge para a Vlan 12

```
spanning-tree mst 12 priority 4096
spanning-tree mst 11,99 priority 8192
```

4.2 Mecanismos de Segurança

No *switch de Acesso* procederam-se as seguintes configurações de mecanismos de segurança:

- **Port security** – este mecanismo limita o numero de dispostivos que podem aceder a uma só porta. Neste caso ficou decidido que apenas dois dispositivos poderão ter acesso a uma determinada porta e, caso esta restrição seja violada, o Port Security está configurado para bloquear dada porta durante 300 segundos.

```
errdisable recovery cause psecure-violation
errdisable recovery interval 300
!
interface range FastEthernet 0/1-15
switchport port-security maximum 2
switchport port-security violation shutdown
```

- **DHCP Snooping** – garante a integridade IP num *switch Layer* 2. Faz com que hosts só possam utilizar os endereços IP que lhes estão associados e apenas servidores DHCP autorizados podem ser acedidos.

```
ip dhcp snooping
ip dhcp snooping vlan 11 12
!
interface range FastEthernet0/21-24
```

```
ip dhcp snooping trust
!
interface Port-channel1
ip dhcp snooping trust
!
interface Port-channel2
ip dhcp snooping trust
```

- **IP Source Guard -** permite bloquear o tráfego de rede indesejado a partir de endereços IP que não foram atribuídos pelo servidor DHCP confiável. Este mecanismo descarta pacotes que possuem endereços não confiáveis de acordo com a tabela do DHCP.

```
interface range FastEthernet 0/1-15
ip verify source vlan dhcp-snooping
```

- **Dynamic ARP Inspection -** verifica protocolo de endereço (ARP) assegurando que apenas os *request* e *response* válidos sejam transmitidos. Este mecanismo previne ARP *spoofing attacks.*

```
ip arp inspection
!
interface range FastEthernet0/21-24
ip arp inspection trust
!
interface Port-channel1
ip arp inspection trust
!
interface Port-channel2
ip arp inspection trust
```

- **ARP Rate Limiting Control** – Limita os pacotes ARP que podem ser transmitidos por porta. Este mecanismo previne ataques de DoS através do envio de grandes quantidades de mensagens ARP.

```
interface range FastEthernet0/1-15
ip arp inspection limit rate 20
```

- **Storm Control -** torna a rede mais robusta quando o número de pacotes de broadcast, multicast ou unicast criam excesso de tráfego numa determinada porta. Este excesso pode causar problemas de desempenho na rede ou mesmo a que a rede fique inoperacional.

Como medida de segurança, na eventualidade de ocorrer uma "Storm", a porta em questão é desligada.

```
interface range FastEthernet0/1-15
storm-control broadcast level 25.00
storm-control multicast level 25.00
storm-control unicast level 50.00
storm-control action shutdown
```

- **Spanning Tree BPDU Filter and Guard** - As portas de acesso não recebem nem enviam BPDU's (Bridge Protocol Data Unit). Caso ocorra transmissão de BPDU's a porta em questão é desligada.

```
interface range FastEthernet0/1-15
spanning-tree bpdufilter enable
spanning-tree bpduguard enable
```

4.3 Configuração da camada de distribuição e da camada Core.

Configuração do HSRP (Hot Standby Router Protocol) com os mesmos IP.

Switch de distribuição 1:

```
interface Vlan11
standby 0 ip 172.16.11.254
standby 0 priority 100
standby 0 preempt delay minimum 300
!
interface vlan12
standby 0 ip 172.16.12.254
standby 0 priority 10
standby 0 preempt delay minimum 300
!
```

HSRP no Switch de distribuição 2:

```
interface Vlan11
standby 0 ip 172.16.11.254
standby 0 priority 10
standby 0 preempt delay minimum 300
!
interface Vlan12
standby 0 ip 172.16.12.254
standby 0 priority 100
standby 0 preempt delay minimum 300
```

Para a *vlan 11 e 12* foi configurado um servidor DHCP em cada um dos *switches* de distribuição de maneira a que cada *host* que se conecte ao *switch* de acesso adquira um endereço IPv4 de forma automática.

```
ip dhcp pool vlan11
network 172.16.11.0 255.255.255.0
dns-server 8.8.8.8
default-router 172.16.11.254
lease 3
!
ip dhcp pool vlan12
network 172.16.12.0 255.255.255.0
dns-server 8.8.8.8
default-router 172.16.12.254
lease 3
```

Configuração das interfaces Fe 0/12 e 0/13 nos *switch* de distribuição para a ligação com os routers da camada core.

Distribuição 1:

```
vlan 111
vlan 112
!
interface Vlan111
ip address 10.10.10.1 255.255.255.252
!
interface Vlan112
ip address 10.10.10.13 255.255.255.252
!
interface FastEthernet0/12
switchport access vlan 111
switchport mode access
!
interface FastEthernet0/13
switchport access vlan 112
switchport mode access
```

Distribuição 2:

```
vlan 121
vlan 122
!
interface Vlan121
ip address 10.10.10.5 255.255.255.252
!
interface Vlan122
ip address 10.10.10.9 255.255.255.252
!
```

```
interface FastEthernet0/12
switchport access vlan 122
switchport mode access
!
interface FastEthernet0/13
switchport access vlan 121
switchport mode access
```

De seguida procedeu-se à ativação do encaminhamento nos *switches* de distribuição recorrendo ao OSPF.

Distribuição 1:

```
ip routing
!
log-adjacency-changes
router ospf 10
network 10.10.10.0 0.0.0.3 area 0
network 10.10.10.12 0.0.0.3 area 0
network 172.16.11.0 0.0.0.255 area 0
network 172.16.12.0 0.0.0.255 area 0
```

Distribuição 2:

```
ip routing
!
log-adjacency-changes
router ospf 10
network 10.10.10.4 0.0.0.3 area 0
network 10.10.10.8 0.0.0.3 area 0
network 172.16.11.0 0.0.0.255 area 0
network 172.16.12.0 0.0.0.255 area 0
```

Foram implementadas as interfaces dos routers da camada core.

Core 1:

```
interface Loopback0
ip address 192.168.100.1 255.255.255.255
no shut
!
interface GigabitEthernet0/0
ip address dhcp
no shut
!
interface GigabitEthernet0/1
ip address 10.10.10.6 255.255.255.252
no shut
!
```

```
interface GigabitEthernet0/2
ip address 10.10.10.2 255.255.255.252
no shut
!
interface Serial0/0/0
ip address 10.10.10.17 255.255.255.252
no shut
```

Core 2:

```
interface Loopback0
ip address 192.168.100.2 255.255.255.255
no shut
!
interface GigabitEthernet0/0
ip address dhcp
no shut
!
interface GigabitEthernet0/1
ip address 10.10.10.14 255.255.255.252
no shut
!
interface GigabitEthernet0/2
ip address 10.10.10.10 255.255.255.252
no shut
!
interface Serial0/0/0
ip address 10.10.10.18 255.255.255.252
no shut
```

De seguida configurou-se o OSPF para cada router da camada core.

Core 1:

```
router ospf 10
router-id 192.168.100.1
redistribute static
network 10.10.10.0 0.0.0.3 area 0
network 10.10.10.4 0.0.0.3 area 0
network 10.10.10.16 0.0.0.3 area 0
```

Core 2:

```
router ospf 10
router-id 192.168.100.2
redistribute static
network 10.10.10.8 0.0.0.3 area 0
network 10.10.10.12 0.0.0.3 area 0
network 10.10.10.16 0.0.0.3 area 0
```

Por fim, foi configurado o NAT overload em cada core, desta forma os IP de cada host que pretendam aceder à rede publica são traduzidos no porto de saída do router.

```
interface GigabitEthernet0/0
ip nat outside
!
interface GigabitEthernet0/1
ip nat inside
!
interface GigabitEthernet0/2
ip nat inside
!
interface Serial0/0/0
ip nat inside
!
access-list 1 permit any
!
ip nat inside source list 1 interface GigabitEthernet0/0 overload
```

5 Testes

Teste ao LACP

Port Channel 1:

Procedimento - desligar o cabo na porta 22 no switch da camada de acesso:

Resultado esperado – Po1 assumido pela porta 21.

```
Switch#shou spanning-tree vlan 11

MST11
  Spanning tree enabled protocol mstp
  Root ID    Priority    4107
             Address     501c.bf38.ec00
             Cost        100000
             Port        64 (Port-channel2)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32779  (priority 32768 sys-id-ext 11)
             Address     c414.3cd9.9400
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface          Role Sts Cost      Prio.Nbr Type
------------------ ---- --- --------- -------- --------------------------------
Fa0/3              Desg FWD 2000000   128.3    P2p
Po1                Altn BLK 100000    128.56   P2p
Po2                Root FWD 100000    128.64   P2p


Switch#
*Mar  1 01:15:47.011: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed state to down
*Mar  1 01:15:48.017: %LINK-3-UPDOWN: Interface FastEthernet0/23, changed state to down
Switch#shou spanning-tree vlan 11

MST11
  Spanning tree enabled protocol mstp
  Root ID    Priority    4107
             Address     501c.bf38.ec00
             Cost        100000
             Port        64 (Port-channel2)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32779  (priority 32768 sys-id-ext 11)
             Address     c414.3cd9.9400
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface          Role Sts Cost      Prio.Nbr Type
------------------ ---- --- --------- -------- --------------------------------
Fa0/3              Desg FWD 2000000   128.3    P2p
Po1                Altn BLK 200000    128.56   P2p
Po2                Root FWD 100000    128.64   P2p
```

Resultado - a comunicação Po1 e Po2 manteve-se.

Estado – Passou o teste.

Port Channel 2:

Procedimento – desligar desligar o cabo na porta 23 no switch da camada de acesso.

Resultado esperado – Po2 assumido pela porta 23.

```
Switch#shou spanning-tree vlan 12

MST12
  Spanning tree enabled protocol mstp
  Root ID    Priority    4108
             Address     501c.bf0f.f280
             Cost        100000
             Port        56 (Port-channel1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32780  (priority 32768 sys-id-ext 12)
             Address     c414.3cd9.9400
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface          Role Sts Cost      Prio.Nbr Type
------------------ ---- --- --------- -------- --------------------------------
Po1                Root FWD 100000    128.56   P2p
Po2                Altn BLK 100000    128.64   P2p


Switch#
*Mar  1 00:59:12.843: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/21, changed state to down
*Mar  1 00:59:13.850: %LINK-3-UPDOWN: Interface FastEthernet0/21, changed state to down
Switch#shou spanning-tree vlan 12

MST12
  Spanning tree enabled protocol mstp
  Root ID    Priority    4108
             Address     501c.bf0f.f280
             Cost        100000
             Port        56 (Port-channel1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32780  (priority 32768 sys-id-ext 12)
             Address     c414.3cd9.9400
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface          Role Sts Cost      Prio.Nbr Type
------------------ ---- --- --------- -------- --------------------------------
Po1                Root FWD 100000    128.56   P2p
Po2                Altn BLK 200000    128.64   P2p
```

Resultado - a comunicação Po2 manteve-se.

Estado – Passou o teste.