



Apontamentos Teóricos

Aula 19/10/2021

Conceito de VLANs

VLAN Nativa

VLANs Privadas

Latência

Tipos de switch

Store and Forward

Cut Through

Switch assimétrico

Switch simétrico

Esquemas de buffering

Modo Access

Modo Trunk

VoIP

No switch

Referências

Aula T 02/11/2021

Configurações

No R1

SW1

No R2

No SW2

No SW3

Notas

Dividir a VLAN 30 (Private VLAN)

No SW3

No SW2

Aula T 09/11/2021

Configuração da Topologia 5 no GNS3

No R1

No SR2

No SR3

Explicação sobre a confusão entre interface vlan 99 e vlan 99 nativa

Notas

Notas sobre tipos de ligações

Aula T 16/11/2021

HOW TO STP

Exame 2020

EXAME ÉPOCA RECURSO 05FEV2019

Aula 30/11/2021

Frame Relay

Aula 07/12/2021

RSTP

Configurar o RSTP numa rede com 3 switch em ciclo

No SW1

No SW2

No SW3

Aula 14/12/2021

PPP

Ativar o encapsulamento PPP

Ping sem compressão

Ping com compressão

PPPP Multilink

Configuração do Multilink

PAP (Password Authentication Protocol)

CHAP (Challenge Handshake Authentication Protocol)

PPPoFR (PPP over Frame Relay)

Multilink PPPoFR (Multilink PPP over Frame Relay)

QinQ

Aula 21/12/2021

QinQ

Evolução

MPLS (Multiprotocol Label Switch)

Arquitetura

Operação

Configurar o MPLS

Aula 04/01/2022

Exame 13 Fev 2020

Pergunta 9

Pergunta 10

Aula 19/10/2021

Conceito de VLANs

- Podemos entender as VLANs como um conjunto de redes independentes a funcionar sobre o mesmo switch e independentes da posição geográficas
- VLAN é então um **domínio de difusão**

VLAN Nativa

- Por omissão o tráfego considerado por um switch na VLAN Nativa de um trunk, sai para esse trunk como *untaged*
- O tráfego *untaged* que entra por um trunk é considerado, pelo switch, na VLAN Nativa desse trunk

VLANs Privadas

- Um conceito importante e que também pode ser útil é o conceito de VLANs Privadas
- Uma VLAN Privada é termos várias VLANs dentro de uma VLAN ou seja, segmentar ainda mais uma rede
- Este conceito é um conceito de **L2** no modelo OSI

Latência

- A latência mede-se como o tempo que um bit demora a percorrer desde o terminal origem até ao terminal de destino
- A latência depende sempre da distância e do equipamento em si

Tipos de switch

Store and Forward

- Um switch é **store and forward** quando o mesmo lê o quadro todo de uma vez sendo que só no final é que sabe para onde tem de enviar o "pacote"

Cut Through

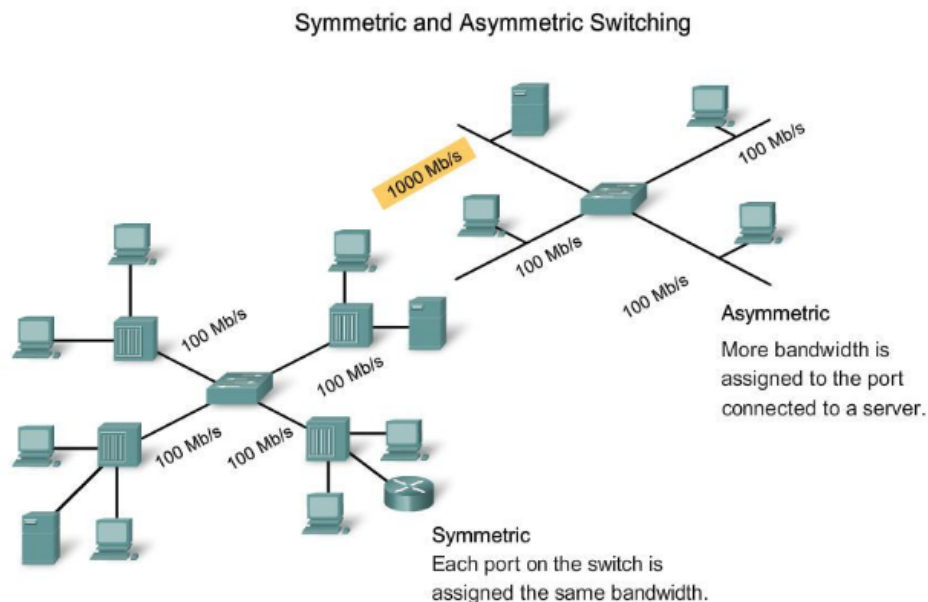
- Um switch é **cut through** quando o mesmo lê uma parte do quadro(até ao *destination address*) sabendo já aqui para onde tem de enviar o "pacote"

Switch assimétrico

- Existe mais banda larga no *uplink*

Switch simétrico

- A largura de banda que percorre os links é sempre a mesma



Esquemas de buffering

- Atualmente os switches são do tipo *shared memory*
- Este tipo de switch tem uma memória partilhada por todas as portas sendo que a quantidade de memória por porta atribuída é de maneira dinâmica

Modo Access

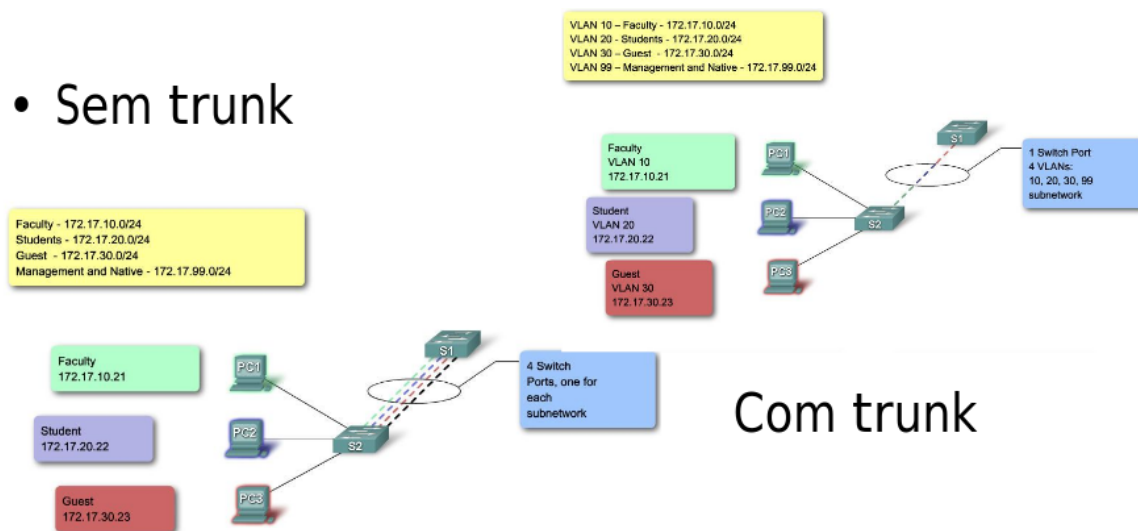
- O tráfego do switch para o PC é considerado **tráfego não marcado** -> **Modo Access**

- Ou seja, os links que estão ligados do switch aos PCs são configurados com **modo access**

Modo Trunk

- O tráfego do switch para fora é considerado **tráfego marcado** -> **Modo Trunk**
- Os links de trunk são usados para transportar tráfego de várias VLANs ao mesmo tempo, sendo que os quadros que trafegam por essa porta são identificados através da **TAG**

• Sem trunk



VoIP

- Se tivermos VoIP e um PC ligado a um switch (o PC liga a sua tomada ethernet ao telefone e o telefone liga ao switch), o switch vai mandar **tráfego não marcado** para o PC e **tráfego marcado** para o VoIP
- Sendo assim teríamos de configurar o switch de modo a enviar tráfego marcado e tráfego não marcado

No switch

- **Trafego não marcado para o PC**

```
int f0/20
switchport mode access
```

```
switchport access vlan 10
```

- **Trafego marcado para o VoIP**

```
switchport voice vlan 110
```

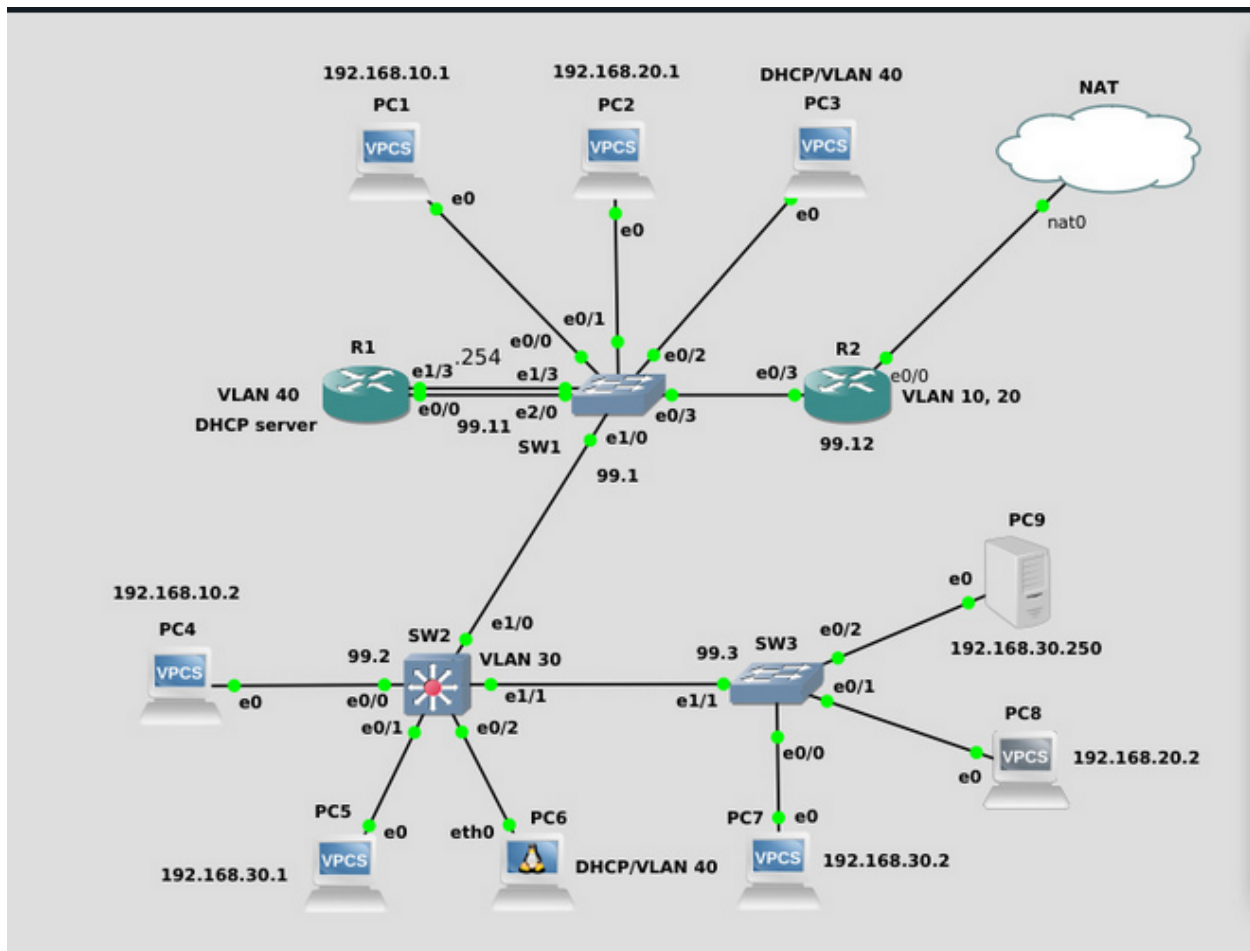
- Por fim teriamos de configurar o router de modo a trabalhar com VoIP

Referências

- <https://www.youtube.com/watch?v=3HWCqS-uU84>

Aula T 02/11/2021

- **Atenção que os equipamentos têm de ser limpos**



Configurações

- Colocou-se IPs nos VPCs e nos lpterns

No R1

- Este router é "pai" da VLAN40
- E tem tambem a VLAN99
- E é tambem servidor de DHCP
- E colocamos tambem DNS que vem do R2
- Ativar o RIP

```
conf t
hostname R1
```

```

int e1/3
ip add 192.168.40.254 255.255.255.0
no shut

int e0/0
ip add 192.168.99.11 255.255.255.0
no shut

exit
ip dhcp pool pool_VLAN
network 192.168.40.0 255.255.255.0
default-router 192.168.40.254
dns-server 192.168.99.12

router rip
network 0.0.0.0

```

SW1

- Configuramos as VLANs nos primeiros 3 comandos
- Configuramos a vlan40 na e1/3
- Configuramos a vlan99 na e2/0
- Configuramos em modo trunk na e0/3 porque o R2 tem a VLAN99 VLAN10 e VLAN20 , logo enviamos tráfego marcado porque só temos 1 cabo, logo temos de criar sub interfaces virtuais. Tem de ser trafego marcado (trunk) para suportar várias vlans
- Configuramos uma VLAN nativa no trunk (neste caso configuramos a vlan 99)
- Configurar o trunk para baixo e como é entre switches temos de meter a nativa tambem
- Usa-se este comando (`int vlan 99` e depois `ip add 192.168.99.1 255.255.255.0`) para por exemplo fazer telnet no entanto nao é necessário

```

int e0/0
sw mode access
sw access vlan 10

int e0/1
sw mode access
sw access vlan 20

int e0/2

```



```

sw mode access
sw access vlan 40

int e1/3
sw mode access
sw access vlan 40

int e2/0
sw mode access
sw access vlan 99

int e0/3
sw trunk encapsulation dot1q
sw mode trunk

int e0/3
switchport trunk native vlan 99
vlan 99

int e1/0
sw trunk encapsulation dot1q
sw trunk native vlan 99
sw mode trunk

int vlan 99
ip add 192.168.99.1 255.255.255.0

```

No R2

- Configuramos dhcp
- Configuramos o NAT outside
- Configuramos aqui as subinterfaces
 - Na porta fisica fazemos `no shut`
 - Depois criamos 3 subinterfaces , uma para cada VLAN
 - Depois temos de ter atenção à VLAN nativa do trunk (ver notas em baixo)
 - Se tivéssemos mudado a nativa para vlan 99 tínhamos de fazer o comando la em baixo que diz `dot1q 99 native`
- Colocar NAT inside
- Ativar o RIP

```

int e0/0
ip add dhcp
no shut

int e0/0
ip nat outside

int e0/3
no shut
int e0/3.10
encapsulation dot1q 10
ip add 192.168.10.254 255.255.255.0
int e0/3.20
encapsulation dot1q 20
ip add 192.168.20.254 255.255.255.0
int e0/3.99
encapsulation dot1q 99
ip add 192.168.99.12 255.255.255.0

int e0/3.99
encapsulation dot1q 99 native

int e0/3.10
ip nat inside
int e0/3.20
ip nat inside
int e0/3.99
ip nat inside
exit
access-list 10 permit any
ip nat inside source list 10 interface e0/0 overload

router rip
network 0.0.0.0
default-information originate

```

No SW2

- Configurar a VLAN nativa com o trunk
- Criar vlans
- Configurar mode access para as vlans
- Configurar trunk para o lado direito
- Configurar a VLAN30 (**começa no ip routing**) uma vez que o SW2 vai ser o *default gateway* da vlan 30

- Configurar router para acesso telnet por exemplo (nao é necessário)
- Configurar o RIP

```

int e1/0
sw trunk encapsulation dot1q
sw mode trunk
sw trunk nativ vlan 99

vlan 10
vlan 30
vlan 40
vlan 99

int e0/0
sw mode acc
sw acc vlan 10
int e0/1
sw mode acc
sw acc vlan 30
int e0/2
sw mode acc
sw acc vlan 40

int e1/1
sw tru encapsulation dot1q
sw mode trunk
sw trunk native vlan 99

ip routing
interface vlan 30
ip add 192.168.30.254 255.255.255.0
no shut

interface vlan 99
ip add 192.168.99.2 255.255.255.0
no shut

router rip
network 0.0.0.0

```

No SW3

- Configurar o trunk
- Criar VLANs
- Configurar interfaces para VLANs

- Configurar para aceder em telnet por exemplo (nao é necessário)

```
int e1/1
sw tru encapsulation dot1q
sw mode trunk
sw trunk native vlan 99

vlan 10
vlan 20
vlan 30
vlan 99

int e0/0
sw mode acc
sw acc vlan30
int e0/1
sw mode acc
sw acc vlan20
int e0/2
sw mode acc
sw acc vlan30

int vlan 99
ip add 192.168.99.3 255.255.255.0
```

Notas

- Se der erros de `full duplex` e `not full duplex` entre o Switch e os routers fazemos:

```
int e1/3
duplex full
```

- Quando se fala num trunk temos de pensar na VLAN nativa
 - Um trunk tem sempre uma vlan nativa
 - A VLAN nativa é uma vlan que não está associada explicitamente a nenhuma tag, ou seja, não tem marcação
 - **É importante mudar a vlan nativa dos trunks**
- Na configuração da VLAN30 nao podemos colocar ips nas portas do switch porque as mesmas sao de L2 então temos de criar uma interface virtual

- `ip routing`
- `interface vlan 30`
- `ip add 192.168.30.254 255.255.255.0`
- `no shut`

Dividir a VLAN 30 (Private VLAN)

- O VTP tem de estar desligado
 - O **VTP mode transparent** está a trabalhar mas não recebe as vlans
- Depois temos de dizer quais são as vlans primárias e secundárias
 - Vamos colocar o servidor na vlan primaria e os pcs na vlan secundária
 - A vlan secundária pode ser isolada e comunitária
Se colocarmos pcs numa isolada eles nao comunicam entre si, se colocarmos numa comunitária eles comunicam entre si

No SW3

- Colocar o vtp em modo transparente
- Colocar a vlan 30 a privada
- Criar a vlan31 como isolada e associamos à vlan 30
- Associar a interface e0/2 para a vlan privada
- Associar a interface e0/0 para a vlan isolada

```
conf t
vtp mode transparent

vlan 30
private-vlan primary

vlan 31
private-vlan isolated
private-vlan association 31
exit

int e0/2
switchport mode private-vlan
switchport private-vlan promiscuous
```

```
sw private-vlan mapping 30 31

int e0/0
switchport mode private-vlan
switchport private-vlan host-association
sw private-vlan mapping 30 31
```

No SW2

- Dizer que a vlan 30 é primaria e associar com a 31
- Dizer que a vlan 31 é isolada e associar à 30
- Criar a vlan31 e dizer que ela é privada e isolada
- Associar a interface e0/1 à

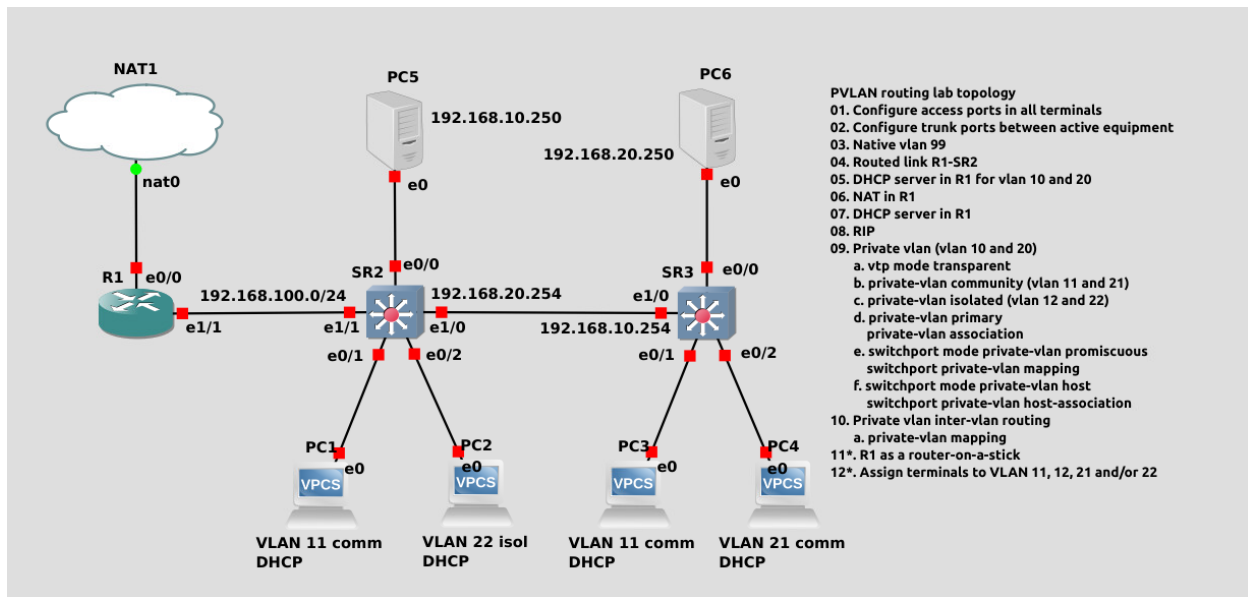
```
conf t
vtp mode transparent
vlan 30
private-vlan primary
private-vlan association 31

vlan31
private-vlan isolated
exit

int e0/1
switchport mode private-vlan
switchport private-vlan host-association 30 31
```

Aula T 09/11/2021

Configuração da Topologia 5 no GNS3



No R1

- Configurar a interface externa para ganhar IP por DHCP
- Configurar o NAT e levantar a interface e1/1 (atenção que a rede 192.168.100.0/24 é a rede entre o R1 e o SW2)
- Configurar servidor de DNS
- Criar pools de DHCP (10 e 20)
- Configurar o RIP

```

conf t
int e0/0
ip add dhcp
no shut

exit
access-list 10 permit any
int e0/0
ip nat outside
int e1/1
ip nat inside
ip nat inside source list 10 int e0/0 overload
ip add 192.168.100.1 255.255.255.0
no shut
exit

ip dns server
ip domain lookup

```

```
ip dhcp pool P00L_10
network 192.168.10.0 255.255.255.0
default-router 192.168.10.254
dns-server 192.168.100.1
ip dhcp pool P00L_20
network 192.168.20.0 255.255.255.0
default-router 192.168.20.254
dns-server 192.168.100.1
ip dhcp excluded-address 192.168.10.250
ip dhcp excluded-address 192.168.10.254
ip dhcp excluded-address 192.168.20.250
ip dhcp excluded-address 192.168.20.254

router rip
network 0.0.0.0
default-information originate
```

No SR2

- Configurar e criar a VLAN 20 visto que é este que fica responsável por ela
- Configurar e criar a VLAN99 para comunicar com o SR3
- Configurar o trunk entre SR2 e SR3
- Configurar o RIP
- Configurar a rede **.100** de modo a desligar o L2 do switch para passarmos de nível 2 para nível 3
- Configurar as private vlans
 - configurar a vlan 10 como primaria
 - associar as secundárias (11 e 12) à primária (10)
 - configurar a 11 como comunitária
 - configurar a 12 como isolada
 - configurar a vlan 20 como primária
 - associar as secundárias (21 e 22) à primária (20)
 - configurar a 21 como comunitária
 - configurar a 22 como isolada

- Configurar a porta de cima como modo promiscuo
 - dizer qual é a primaria(10) e as secundárias(11,12)
- Configurar os pcs para as private vlans
 - Colocamos o pc na vlan privada 11 (e0/1)
 - Colocamos o pc na vlan privada 22 (e0/2)
- Colocar o DHCP a funcionar nas vlans

```

conf t
ip routing
vlan 20
int vlan 20
ip add 192.168.20.254 255.255.255.0
no shut
exit

vlan 99
int vlan 99
ip add 192.168.99.2 255.255.255.0
no shut

int e1/0
sw trunk encapsulation dot1q
sw mode trunk

exit
router rip
network 0.0.0.0

int e1/1
no switchport
ip add 192.168.100.2 255.255.255.0
no shut
exit

vtp mode transparent
vlan 10
private-vlan primary
private-vlan association 11,12
vlan 11
private-vlan community
vlan 12
private-vlan isolated
vlan 20
private-vlan primary
private-vlan association 21,22
vlan 21

```

```

private-vlan community
vlan 22
private-vlan isolated

int e0/0
sw mode private-vlan promiscuous
sw private-vlan mapping 10 11,12

int e0/1
sw mode private-vlan host
sw private-vlan host-association 10 11
int e0/2
sw mode private-vlan host
sw private-vlan host-association 20 22

int vlan 20
private-vlan mapping add 21,22
ip helper-address 192.168.100.1

```

No SR3

- Configurar e criar a VLAN 10 visto que é este que fica responsável por ela
- Configurar e criar a VLAN99 para comunicar com o SR2
- Configurar o trunk entre SR3 e SR2
- Configurar o RIP
- Configurar as private vlans
 - configurar a vlan 10 como primaria
 - associar as secundárias (11 e 12) à primária (10)
 - configurar a 11 como comunitária
 - configurar a 12 como isolada
 - configurar a vlan 20 como primária
 - associar as secundárias (21 e 22) à primária (20)
 - configurar a 21 como comunitária
 - configurar a 22 como isolada
- Configurar as portas de cima como modo promiscuo
 - dizer qual é a primaria(20) e as secundárias(21,22)

- Configurar os pcs para as private vlans
 - Colocamos o pc na vlan privada 11 (e0/1)
 - Colocamos o pc na vlan privada 21 (e0/2)
- Colocar o DHCP a funcionar nas vlans

```

conf t
ip routing
vlan 10
int vlan 10
ip add 192.168.10.254 255.255.255.0
no shut
exit

vlan 99
int vlan 99
ip add 192.168.99.3 255.255.255.0
no shut
exit

int e1/0
sw trunk encapsulation dot1q
sw mode trunk
exit

router rip
network 0.0.0.0

vtp mode transparent
vlan 10
private-vlan primary
private-vlan association 11,12
vlan 11
private-vlan community
vlan 12
private-vlan isolated
vlan 20
private-vlan primary
private-vlan association 21,22
vlan 21
private-vlan community
vlan 22
private-vlan isolated

int e0/0
sw mode private-vlan promiscuous
sw private-vlan mapping 20 21,22

int e0/1
sw mode private-vlan host

```

```

sw private-vlan host-association 10 11
int e0/2
sw mode private-vlan host
sw private-vlan host-association 20 21

int vlan 10
private-vlan mapping add 11,12
ip helper-address 192.168.100.1

```

Explicação sobre a confusão entre interface vlan 99 e vlan 99 nativa

- Ao fazermos `interface vlan 99` entre os Switches de L3, estamos a criar uma rede entre switches por onde passam as vlans. Aqui como atribuidos um ip à interface também pode ser usada para acedermos ao equipamento por telnet
 - Outra coisa é a vlan nativa do trunk, ou seja, podemos ter a vlan 999 que é a nativa e associar essa ao trunk, no entanto temos de a criar na mesma com o comando `vlan 999` e fazer isto em todos os trunks existentes na rede

Notas

- `sh vlan private-vlan` -> mostra as associações entre vlans privadas
- Para os PCs terem dhcp nas vlans privadas fizemos os comandos que têm o `ip helper-address`
- Só podemos criar uma vlan isolada numa vlan primária

Notas sobre tipos de ligações

- Por exemplo, se tivermos num link a passar 3 vlans temos de criar 3 sub interfaces no router e fazer o comando `encapsulation dot1q <nr da vlan>` e depois adicionar um ip a essa subinterface
- Se tivermos um router que é o DG de uma vlan já temos de ter um ip para a interface fazendo `ip add <ip> <mask>` dentro da interface especifica e no switch que liga a ele, configurar essa ligação como access com aquela vlan especifica fazendo `sw mode access` e depois `sw access vlan <nr da vlan>`
- Se tivermos um router ligado a um switch e nao quisermos ter nenhuma vlan no router e quisermos ter uma rede com o switch temos de desligar o switchport para

passar de L2 para L3 fazendo `no switchport` depois de ter entrado na respetiva interface

- Se quisermos dizer que um switch L3 é DG de uma certa vlan fazemos `ip routing`
`vlan <nr da vlan>` `int vlan <nr da vlan>` `ip add <ip> <mask>` e `no shut`

Aula T 16/11/2021

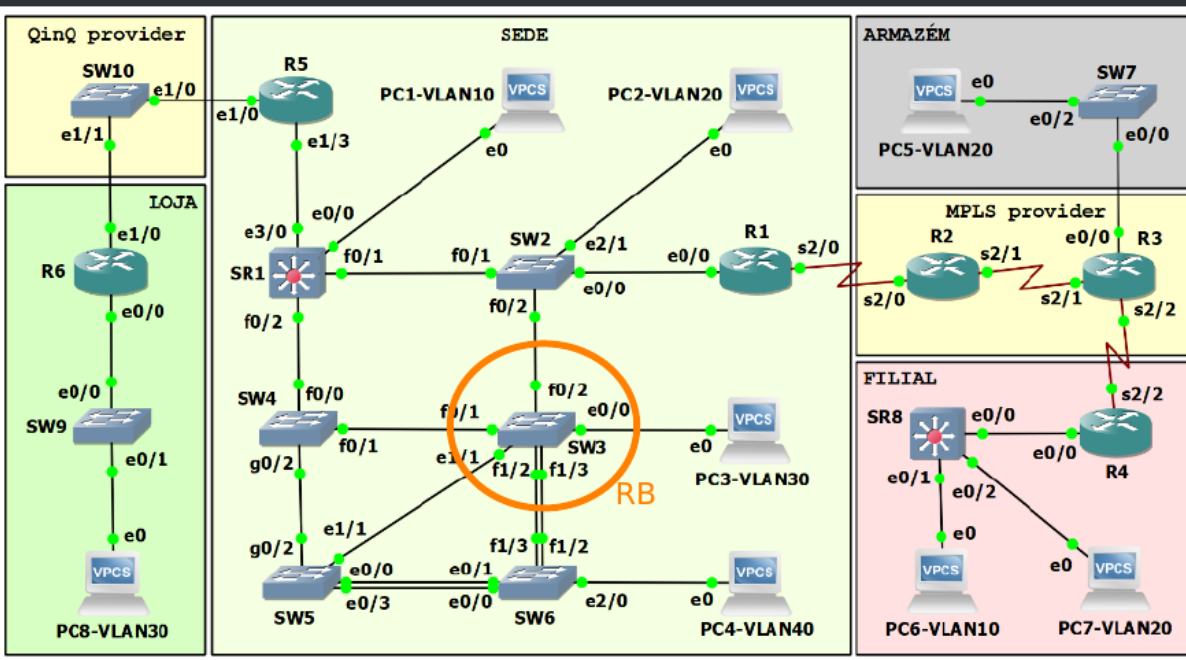
HOW TO STP

1º Eleger a Root Bridge

A eleição da RB é feita com base numa prioridade e também com base no Mac-Address(menor).

Só pode existir uma Root Bridge

Switch	MAC	Priority
SR1	aabb.cc80.0100	16384
SW2	aabb.cc80.0200	28672
SW3	aabb.cc80.0300	8192
SW4	aabb.cc80.0400	24576
SW5	aabb.cc80.0500	12288
SW6	aabb.cc80.0600	8192



- O SW3 e o SW6 têm ambos a prioridade de 8192 no entanto o MAC do SW3 é menor comparado com o MAC do SW6
- Então, colocamos logo todas as portas do SW3 como DP

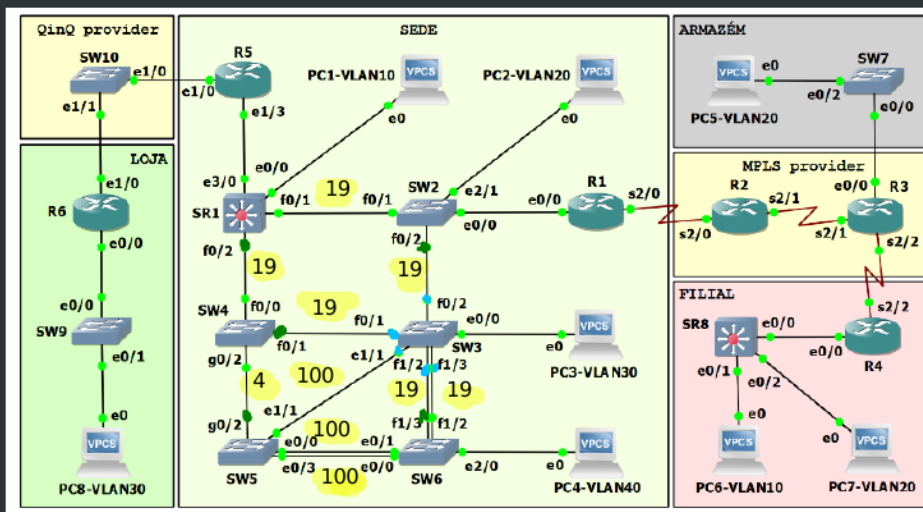
2º Determinar a distância de cada bridge até à root bridge
(A distância é a soma das distâncias entre cada bridge)
O caminho com menor custo é então a RP

Ethernet - 100
FastEthernet - 19
Giga - 4

Link Bandwidth	802.1D Cost
4 Mbps	250
10 Mbps	100
16 Mbps	62
45 Mbps	39
100 Mbps	19
155 Mbps	14
622 Mbps	6
1 Gbps	4
2 Gbps	3
10 Gbps	2

Quando existe empates para escolher qual é a *root port*,
o caminho escolhido usa o vizinho com o *bridge ID* mais baixo sendo este Bridge ID o MAC+Prioridade

Em alguns casos continua a haver um empate por exemplo se o caminho escolhido tiver
um caminho primário e um secundário, então nestes casos o desempate é feito pela porta mais baixa
do vizinho (se existir a e0/2 e a e0/3, ele iria escolher a porta mais baixa, ou seja a e0/2)



SW3 (Root Bridge)
DP (Designated Port)
RP (Root Port)

- No SR1 existe um empate, (19+19 e 19+19), então o desempate foi feito pela prioridade do SW2(28672) e do SW4(24576), sendo escolhido pelo SW4 por ser mais baixo

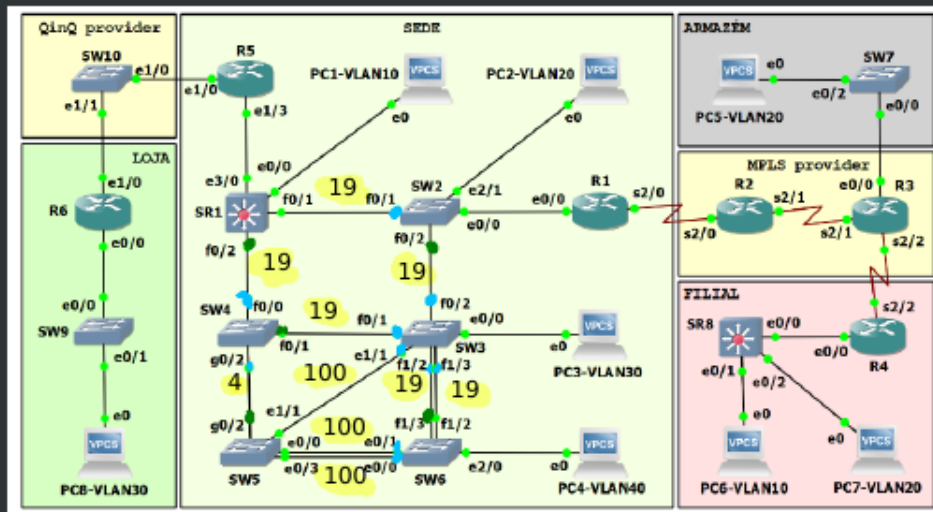
- No SW6 existe um empate, (pode ir pela f1/3 e f1/2), e como apenas temos 1 caminho, não podemos desempatar pela prioridade do SW3, então temos de desempatar pela porta mais baixa do vizinho, neste caso é a f1/2 (do SW3)

3ª Calcular o melhor caminho a partir de cada segmento para termos as DP's

O melhor é colocarmos no meio do segmento, se tivermos uma RP no segmento, automaticamente a porta em frente é DP.

Se tivermos no meio do segmento e não tivermos nenhuma RP, calculamos o melhor caminho e esse será a DP (Não contamos com o custo do segmento onde estamos)

Quando existe empate para escolher qual é a *root port*, o caminho escolhido usa o vizinho com o *bridge ID* mais baixo sendo este Bridge ID o MAC+Prioridade



SW3 (Root Bridge)

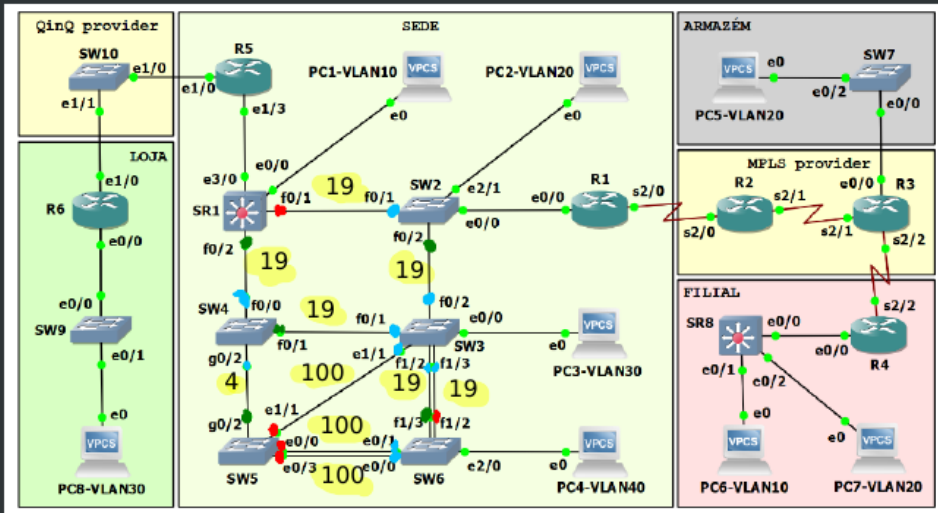
DP (Designated Port)

RP (Root Port)

- (SR1-SW2)
 - Não temos nenhuma RP, logo temos de calcular o menor custo
 - Por f0/1 do SR1 (19+19), por f0/1 SW2 (19)
 - Vamos por SW2 porque é apenas 19
- (SR1-SW4)
 - Temos uma RP, logo a porta em frente é DP
- (SW4-SW5)
 - Temos uma RP, logo a porta em frente é DP
- (SW5-SW6)
 - Não temos nenhuma RP, logo temos de calcular o menor custo
 - Por e0/0 do SW5 (100), por e0/1 do SW6 (19)
 - Vamos por e0/1 do SW6 porque é apenas 19
- (SW5-SW6)
 - Não temos nenhuma RP, logo temos de calcular o menor custo
 - Por e0/3 do SW5 (100), por e0/0 do SW6 (19)
 - Vamos por e0/0 do SW6 porque é apenas 19

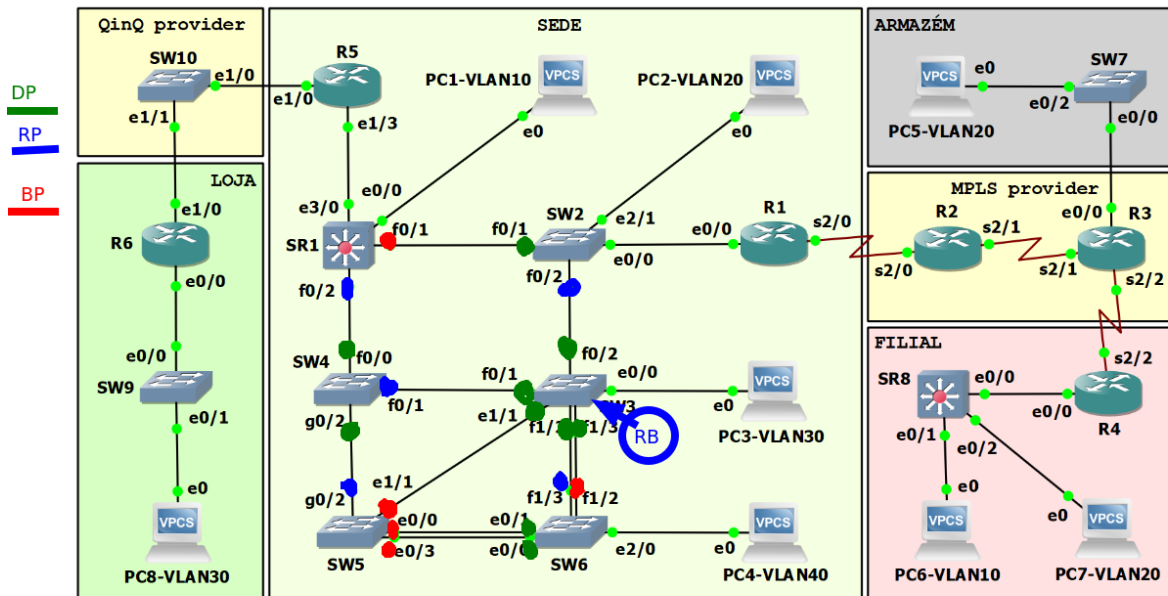
4.º Por fim bloqueamos todas as outras portas

- Estas chamam-se BP (blocked ports)
- Basicamente são as portas que sobram que não foram pintadas

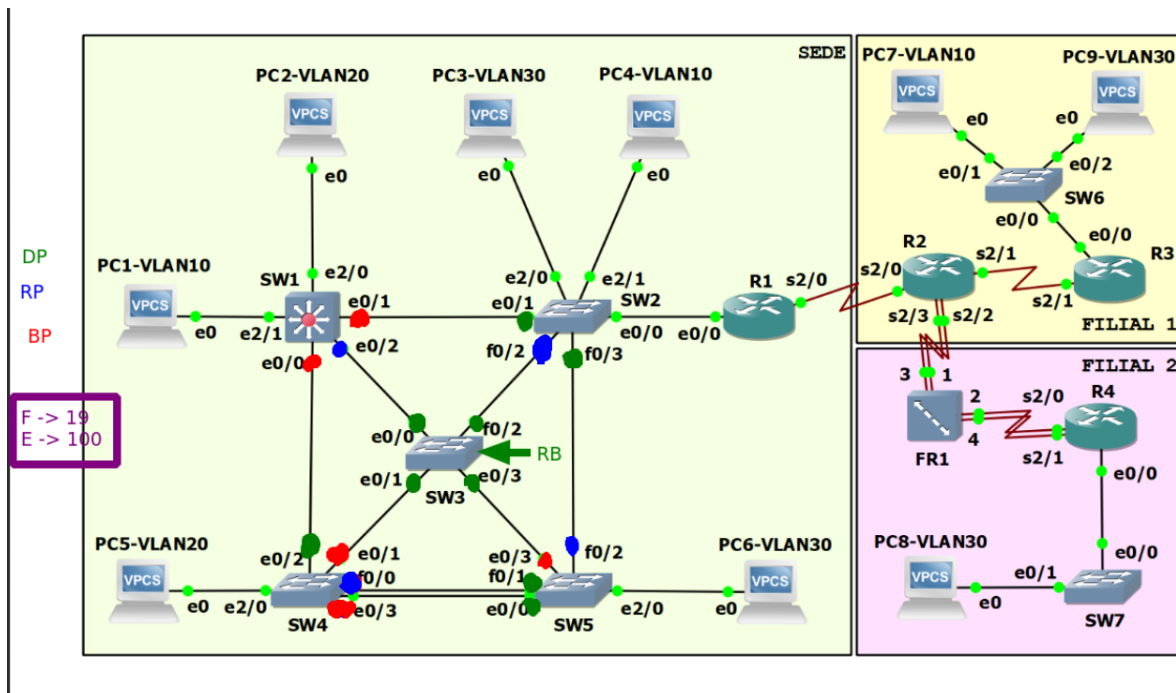


Exame 2020

- Atenção no STP conta sempre a porta do vizinho
- A **Root Bridge** é o SW3 porque a prioridade é igual ao do SW6 no entanto o MAC do SW3 é menor que o MAC do SW6
- Todas as portas do **RB** são **DP** (Designated Ports)



EXAME ÉPOCA RECURSO 05FEV2019



- É preciso ter atenção se estamos a falar de uma porta ethernet ou uma fastethernet
 - Ethernet é 100

- FastEthernet é 19

Aula 30/11/2021

- https://moodle.isec.pt/moodle/pluginfile.php/331732/mod_resource/content/4/Switch_Security_and_Monitoring.pdf
- O SPAN permite que coloquemos uma porta como se fosse um espelho de outra
 - `monitor session 1 source interface f0/1 both`
 - `monitor session 1 destination f0/24`
- RSPAN já não estou a visualizar uma porta, quero visualizar algo que é remoto

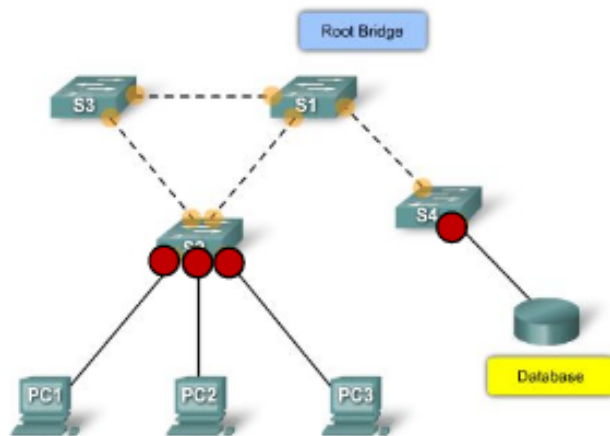
Frame Relay

- Tirar apontamentos do pdf Cisco Certified Network Associate pág. 19

Aula 07/12/2021

RSTP

- Evolução do STP
- O STP tem quatro estados (`block, listening, forward, learning`) e o RSTP tem 3 estados(`discard, listening, learning`) (pag.80)
- O RSTP é mais rápido que o STP porque não deita as interfaces todas abaixo. No processo de *Proposal/Aggrement* ele não vai bloquear todas as portas, apenas bloqueia a porta da frente do link que está a negociar
- Portas do tipo *Edge*
 - São as portas que estão viradas para os PCs
 - Temos de configurar isto como mostra em baixo com `spanning-tree portfast`



- Temos também de configurar se os trunks são point-to-point(full-duplex) ou shared(half-duplex)
 - Como os switches são full-duplex usamos o comando `spanning-tree link-type point-to-point` dentro da interface trunk
- Usamos este no TP

Configurar o RSTP numa rede com 3 switch em ciclo

No SW1

```

spanning-tree mode rapid-pvst
int range e0/1-3
sw trunk encapsulation dot1q
sw mode trunk
int e0/0
sw mode acc
spanning-tree portfast
int range e0/1-3
spanning-tree link-type point-to-point

```

No SW2

```

spanning-tree mode rapid-pvst
int range e0/1-3
sw trunk encapsulation dot1q
sw mode trunk
int e0/0
sw mode acc

```

```
spanning-tree portfast
spanning-tree link-type point-to-point
```

No SW3

```
spanning-tree mode rapid-pvst
int range e0/1-3
sw trunk encapsulation dot1q
sw mode trunk
int e0/0
sw mode acc
spanning-tree portfast
spanning-tree link-type point-to-point
```

Aula 14/12/2021

PPP

- O **PPP** é o protocolo que funciona numa linha qualquer série
- PPP Compress faz com que o quadro fique comprimido, assim os quadros ficam mais pequenos
- **tcp header compression** faz uma compressão só no cabeçalho tcp
 - Ou seja, aqui só vamos comprimir se o pacote for TCP
 - **Isto é bom quando estamos a comunicar sempre para o mesmo pc por exemplo**

Ativar o encapsulamento PPP

```
conf t
interface serial 0/0
encapsulation ppp
```

Ping sem compressão

- 192.168.1.1> ping 192.168.1.3 (sem compressão)

Capturing from - [IOU1 Serial2/0 to IOU2 Serial2/0]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1408	688.444772	192.168.1.1	192.168.1.3	ICMP	104	Echo (ping) request id=0x0
1409	688.451106	192.168.1.3	192.168.1.1	ICMP	104	Echo (ping) reply id=0x0
1410	688.456415	192.168.1.1	192.168.1.3	ICMP	104	Echo (ping) request id=0x0
1411	688.461856	192.168.1.3	192.168.1.1	ICMP	104	Echo (ping) reply id=0x0
1412	688.467351	192.168.1.1	192.168.1.3	ICMP	104	Echo (ping) request id=0x0
1413	688.477328	192.168.1.3	192.168.1.1	ICMP	104	Echo (ping) reply id=0x0
1414	688.482365	192.168.1.1	192.168.1.3	ICMP	104	Echo (ping) request id=0x0
1415	688.484577	192.168.1.3	192.168.1.1	ICMP	104	Echo (ping) reply id=0x0
1416	688.491387	192.168.1.1	192.168.1.3	ICMP	104	Echo (ping) request id=0x0
1417	688.497961	192.168.1.3	192.168.1.1	ICMP	104	Echo (ping) reply id=0x0

> Frame 1408: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface 0

> Point-to-Point Protocol

> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.3

> Internet Control Message Protocol

Ping com compressão

- 192.168.1.1> ping 192.168.1.3 (compress mppc)

Capturing from - [IOU1 Serial2/0 to IOU2 Serial2/0]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1570	954.802998	N/A	N/A	PPP Comp	58	Compressed data
1571	954.810586	N/A	N/A	PPP Comp	58	Compressed data
1572	954.816790	N/A	N/A	PPP Comp	37	Compressed data
1573	954.822309	N/A	N/A	PPP Comp	39	Compressed data
1574	954.828781	N/A	N/A	PPP Comp	36	Compressed data
1575	954.834545	N/A	N/A	PPP Comp	38	Compressed data
1576	954.840277	N/A	N/A	PPP Comp	34	Compressed data
1577	954.845601	N/A	N/A	PPP Comp	34	Compressed data
1578	954.851844	N/A	N/A	PPP Comp	32	Compressed data
1579	954.856847	N/A	N/A	PPP Comp	32	Compressed data

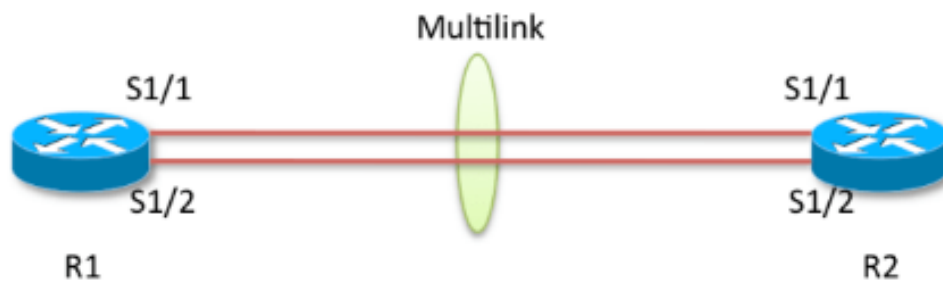
> Frame 1570: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 0

> Point-to-Point Protocol

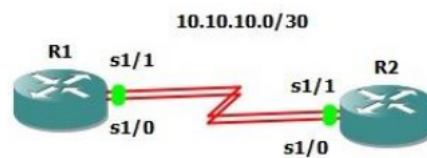
> PPP Compressed Datagram

PPPP Multilink

- A partir de determinado nível de ocupação de uma ligação a carga pode passar a ser distribuída por novas ligações estabelecidas entre os extremos se tal for possível
- Os quadros passam a ser fragmentados



Configuração do Multilink



R1#

```
int Multilink 100
ip address 10.10.10.1 255.255.255.252
ppp multilink
ppp multilink group 100
```

```
int s1/0
encapsulation ppp
ppp multilink
ppp multilink group 100
```

```
int s1/1
encapsulation ppp
ppp multilink
ppp multilink group 100
```

R2#

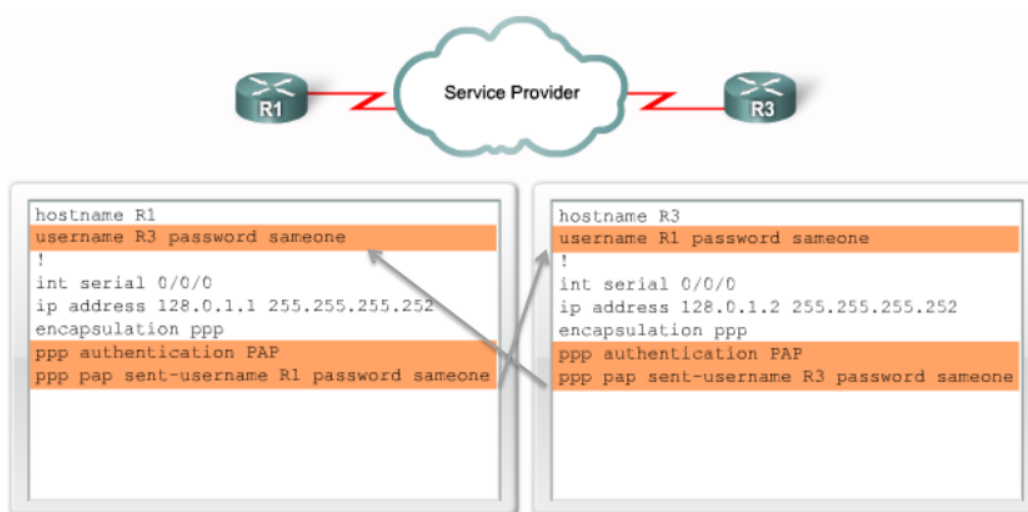
```
int Multilink 200
ip address 10.10.10.2 255.255.255.252
ppp multilink
ppp multilink group 200
```

```
int s1/0
encapsulation ppp
ppp multilink
ppp multilink group 200
```

```
int s1/1
encapsulation ppp
ppp multilink
ppp multilink group 200
```

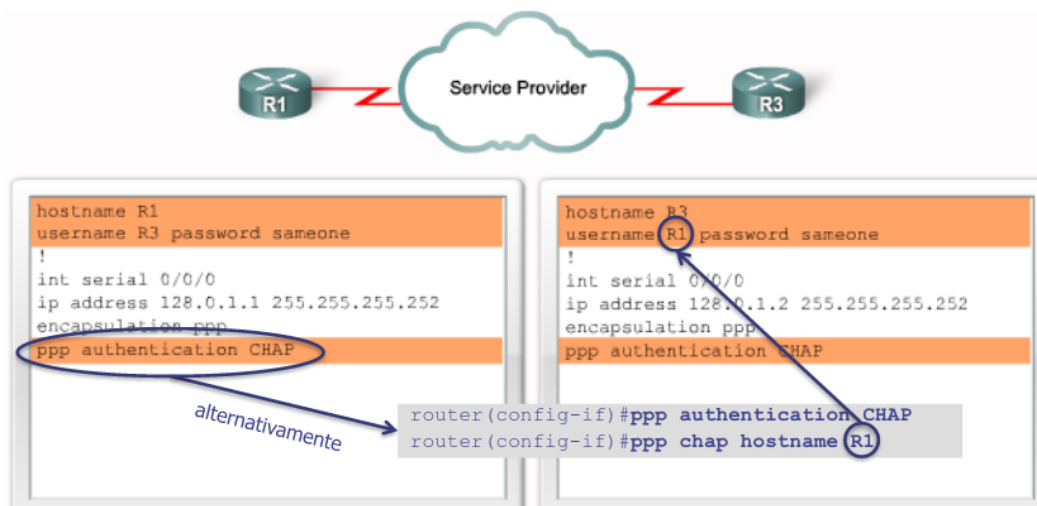
PAP (Password Authentication Protocol)

- Aqui as credenciais não ficam encriptadas
- A password pode ser diferente em cada lado

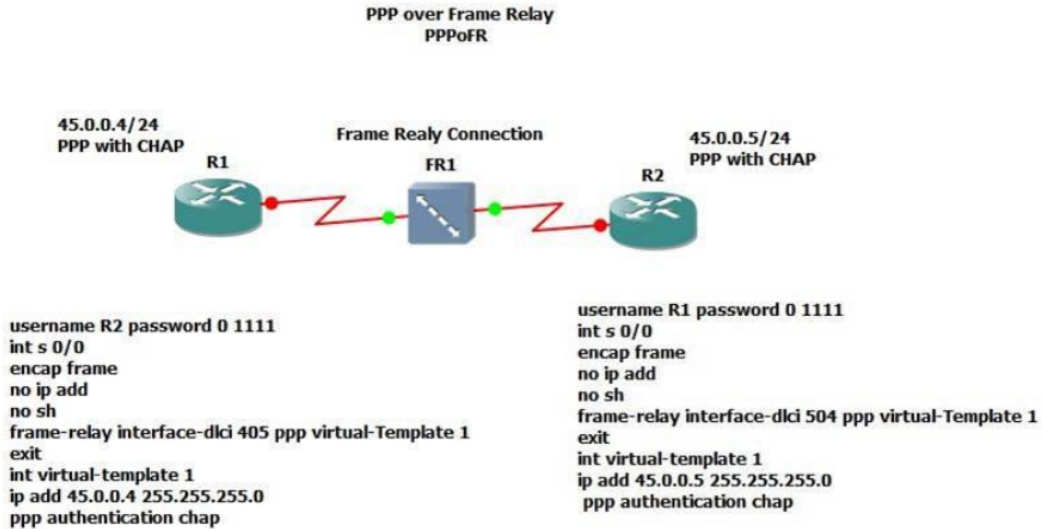


CHAP (Challenge Handshake Authentication Protocol)

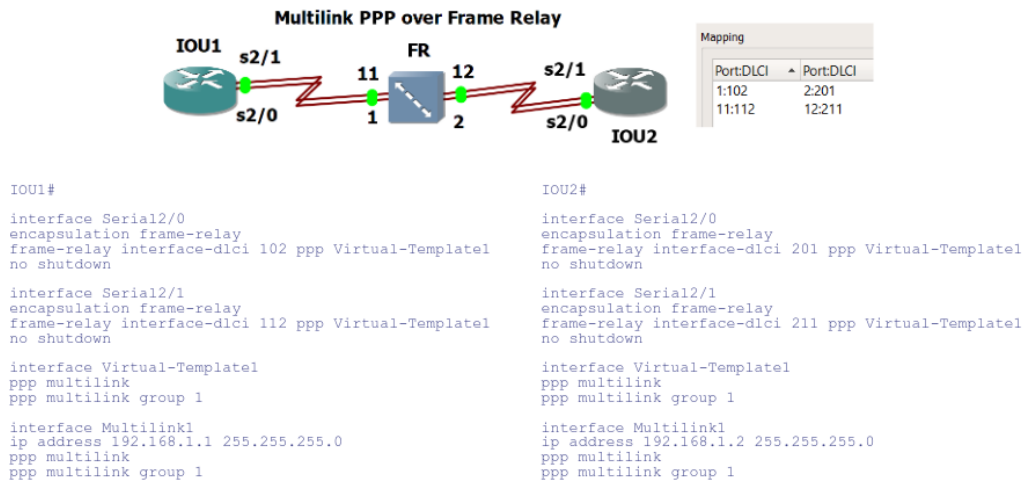
- Aqui as credenciais ficam encriptadas



PPPoFR (PPP over Frame Relay)



Multilink PPPoFR (Multilink PPP over Frame Relay)



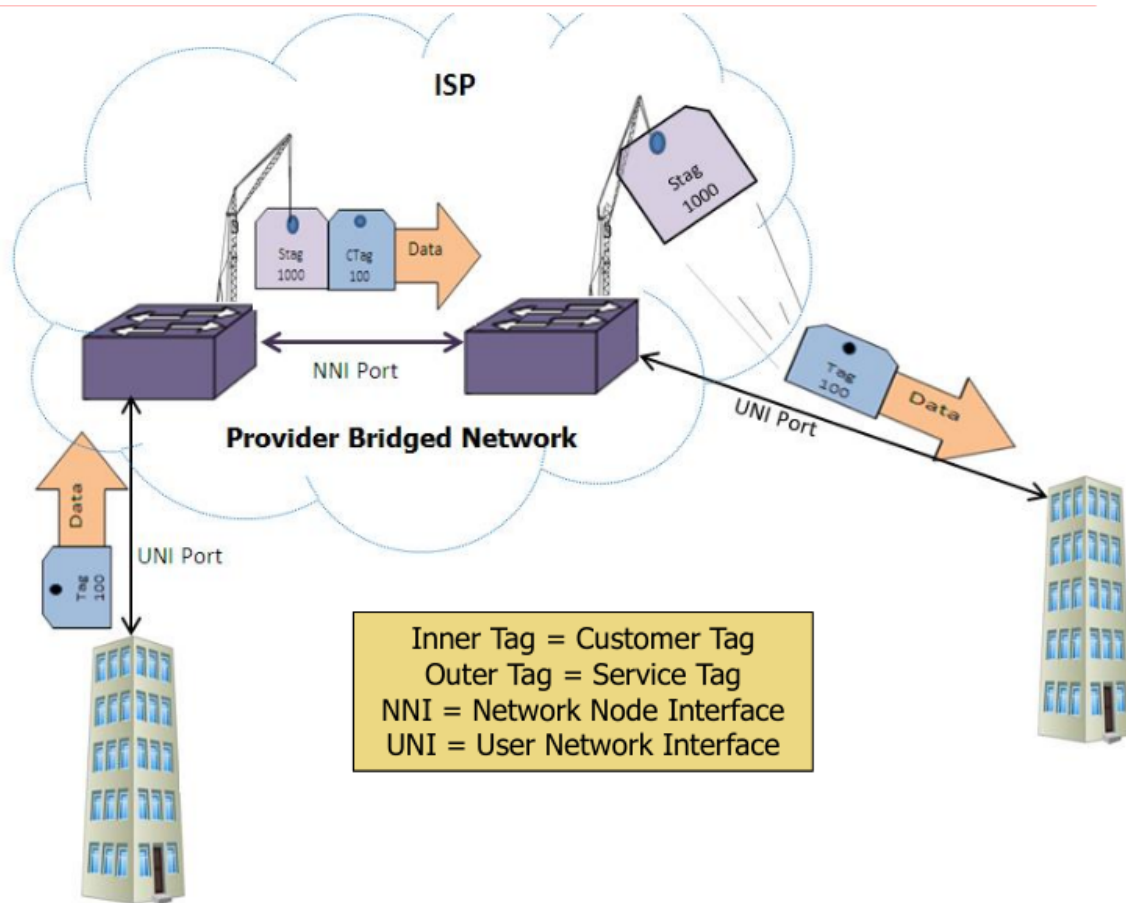
QinQ

- É conhecida por VLAN dot1q tunnel
- É basicamente termos uma vlan em cima de outra, por exemplo para ligar vlans entre empresas diferentes
- tirar print à pagina 2 do QinQ(a azul colocamos a vlan do isp e a amarelo a vlan do cliente)
- tirar print à pagina 3,4 do QinQ

Aula 21/12/2021

QinQ

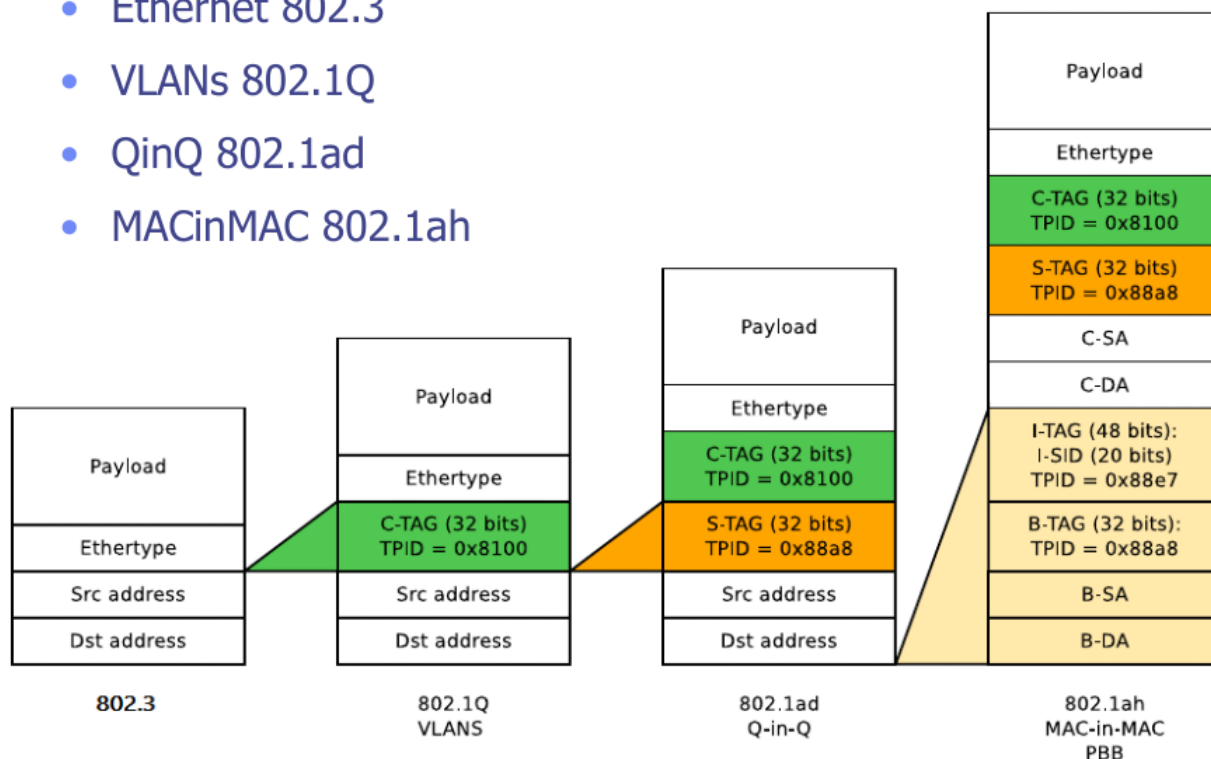
- Conhecida por VLAN dot1q tunnel
- Normalmente os *Service Providers* utilizam esta função para estabelecerem conectividade L2 (com VLANs) entre dois clientes
- **QinQ encapsula a VLAN privada da empresa na VLAN Pública, logo existe uma dupla marcação**



- Os dados saem da empresa com (apenas) a marcação 100 (inner VLAN).
 - À entrada do service provider são marcados numa porta QinQ com tag 1000 (outer VLAN).
 - Os quadros com dupla marcação circulam no service provider, de acordo com a VLAN exterior (1000).
 - À saída do service provider, numa porta QinQ, a marcação exterior (1000) é removida e os quadros recuperam a marcação interna (100).
-
- **No entanto aqui existem algumas limitações, por exemplo o facto das Provider Bridged Networks necessitarem de aprender os MACs dos seus clientes e suportarem apenas 4096 identificadores**
 - Resolvemos este problema de os endereços mac estarem a propagar para dentro do ISP com o MACinMAC

Evolução

- Ethernet 802.3
- VLANs 802.1Q
- QinQ 802.1ad
- MACinMAC 802.1ah



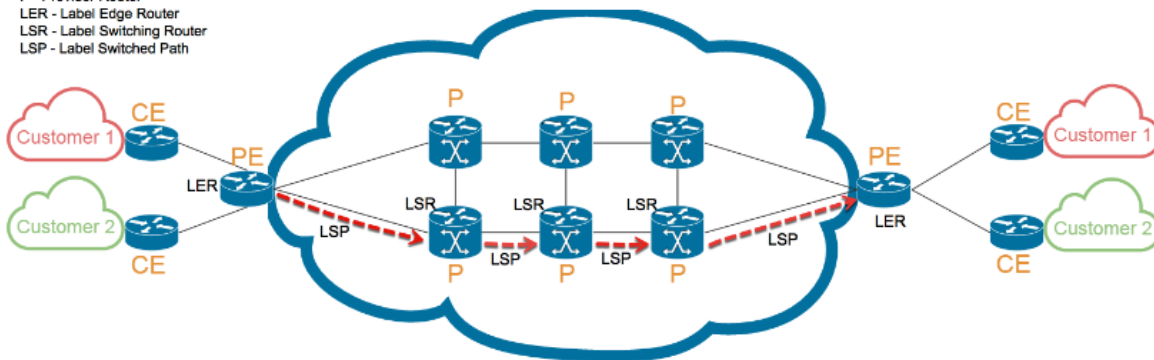
MPLS (Multiprotocol Label Switch)

- Utilizada em redes de alto-desempenho, direcionando o tráfego de um router para o próximo através da aplicação de rótulos (**labels**) aos dados, evitando as tradicionais pesquisas nas tabelas de encaminhamento
- LDP (**Label Distribution Protocol**) é o protocolo que dita quais são as labels
 - O protocolo combina as labels entre 2 routers apenas
- A tecnica dos identificadores usada no OSPF é praticamente igual no MPLS e precisamos de identificadores no MPLS
 - **Então no MPLS ele usa a maior das interfaces loopbacks ou então o maior endereço IP das interfaces físicas**
 - **Então devemos sempre criar em cada router uma interface de loopback**

Arquitetura

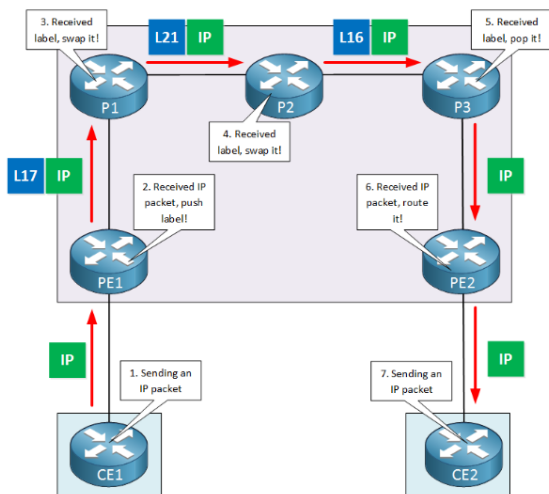
CE - Customer Edge
PE - Provider Edge
P - Provider Router
LER - Label Edge Router
LSR - Label Switching Router
LSP - Label Switched Path

MPLS Network Architecture

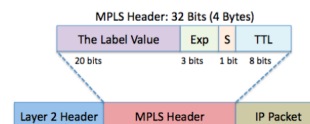


- CE (Customer Edge): último equipamento L2 ou L3 na rede do cliente, não utiliza MPLS.
- PE (Provider Edge): dispositivo situado na fronteira do ISP, acrescenta a label MPLS. Também designado por LER (Label Edge Router).
- P (Provider): interliga os routers P e PE do ISP, que comuta os quadros em função das labels ou remove-as. Também designado por LSR (Label Switch Router).

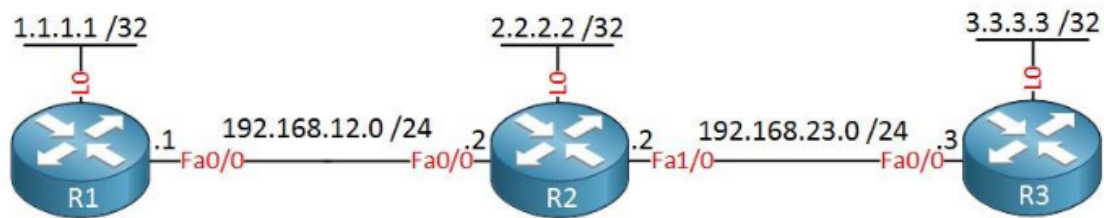
Operação



- Quando um pacote entra num LSP (Label Switch Path) é inserido um cabeçalho de 4 bytes baseado no endereço IP de destino.
- O pacote é encaminhado para os próximos routers do LSP que examinam, apenas, a informação do cabeçalho MPLS e a tabela de encaminhamento MPLS local.
- Os cabeçalhos MPLS têm, apenas, significado local, sendo substituídos em cada router do LSP.



Configurar o MPLS



- A primeira fase para o MPLS é:
 - Configurar loopback em todos os routers que vão usar MPLS
 - Ativar o OSPF (nao esquecer de colocar tambem a loopback)

• OSPF:

```

R1(config)#router ospf 1
R1(config-router)#network 192.168.12.0 0.0.0.255 area 0
R1(config-router)#network 1.1.1.1 0.0.0.0 area 0

```

```

R2(config)#router ospf 1
R2(config-router)#network 192.168.12.0 0.0.0.255 area 0
R2(config-router)#network 192.168.23.0 0.0.0.255 area 0
R2(config-router)#network 2.2.2.2 0.0.0.0 area 0

```

```

R3(config)#router ospf 1
R3(config-router)#network 192.168.23.0 0.0.0.255 area 0
R3(config-router)#network 3.3.3.3 0.0.0.0 area 0

```

- Segunda fase é configurar o LDP ao nível do processo OSPF

mpls ldp autoconfig

```
R1(config)#router ospf 1
R1(config-router)#mpls ldp autoconfig

R2(config)#router ospf 1
R2(config-router)#mpls ldp autoconfig

R3(config)#router ospf 1
R3(config-router)#mpls ldp autoconfig
```

- Terceira fase é criar os rotulos do LDP

- Rótulos LDP:

```
R1(config)#mpls label range 100 199
R2(config)#mpls label range 200 299
R3(config)#mpls label range 300 399
```

```
R1#show mpls ldp bindings
lib entry: 1.1.1.1/32, rev 4
    local binding:  label: imp-null
    remote binding: lsr: 2.2.2.2:0, label: 201
lib entry: 2.2.2.2/32, rev 8
    local binding:  label: 101
    remote binding: lsr: 2.2.2.2:0, label: imp-null
lib entry: 3.3.3.3/32, rev 6
    local binding:  label: 100
    remote binding: lsr: 2.2.2.2:0, label: 200
lib entry: 192.168.12.0/24, rev 2
    local binding:  label: imp-null
    remote binding: lsr: 2.2.2.2:0, label: imp-null
lib entry: 192.168.23.0/24, rev 10
    local binding:  label: 102
    remote binding: lsr: 2.2.2.2:0, label: imp-null
```

Aula 04/01/2022

Exame 13 Fev 2020

R1-R2-R3-R4 -> MPLS

Pergunta 9

- Primeiro ver se é o penultimo
 - se sim é logo null
 - se nao é ver o router que recebe e ver qual é a label dele

R1-R2 -> **label 202**

- É do R1 para o R2 logo é a label que o 2 usa e estamos situados no R2
R2-R1 -> **label 116**
- É do R2 para o R1 logo é a label que o 1 usa

R2-R3 -> **label 302**

- É do R2 para o R3 logo é a label que o 3 usa

R3-R2 -> **label 213**

- É a label que o 2 usa logo é a local

R3-R4 -> **null** porque é o penultimo

R4-R3 -> **312** porque é a marcação que o 3 usa

Pergunta 10

R1-R2

- Vemos o 4.4.4.4 porque é do PC1 para o PC6
 - Exterior é a **206** que é a MPLS
 - Interior é a do tunel que é a **400**

R2-R1

- Interior é a do tunel que é a **100**

- Vemos o 1.1.1.1 porque é do PC6 para o PC1
 - Exterior é **null** porque é a penultima
-

R2-R3

- Interior é a do tunel logo é **400**
- Exterior é vemos o 4.4.4.4 e vemos a marcação que o R3 usa logo é **305**

R3-R2

- Interior é a do tunel logo é **100**
 - Exterior é vemos o 1.1.1.1 e vemos a marcacao que o R2 usa logo é **208**
-

R3-R4

- Interior é a do tunel logo é **400**
- Exterior é vemos o 4.4.4.4 mas como é o penultimo salto fica a **null**

R4-R3

- Interior é a do tunel logo é **100**
 - Exterior é vemos o 1.1.1.1 e vemos a marcacao que o R3 usa logo é **307**
-