CRS3xx:
Recursos básicos e avançados de switching para a construção de redes layer 2 resilientes e de alto desempenho

MikroTik

(MUM BR 2019)
Foz do Iguaçu

Sobre o apresentador

- **Nome:** João Alberto Barbosa de Oliveira
- **Minicurriculum:**
  - **Fundador da Pro Networks**
  - Pós Graduado em gestão e segurança em redes de computadores – UEG 2016;
  - Consultor e Instrutor Oficial com todas as certificações Mikrotik;
  - Gerente de Redes nas empresas Radar WISP LTDA e InternetUP;
  - Instrutor Parceiro – Redes Brasil
  - Certificações Extras: Exin Ethical Hacking Foundation;

pronetworks

MikroTik
CERTIFIED TRAINER

Cronograma

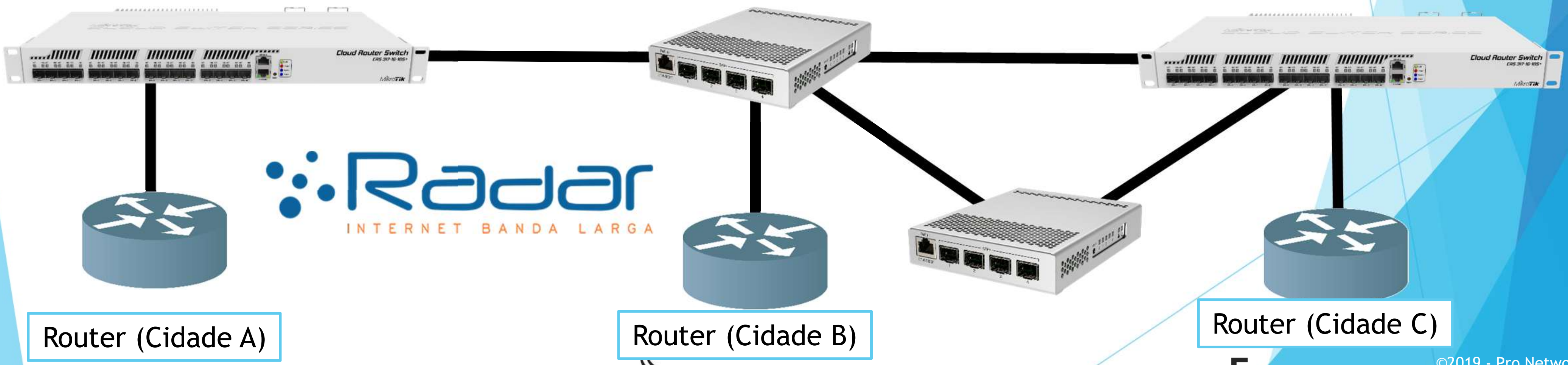
- Case Real de uso em Backbone;
- Introdução à série CRS 3xx;
- Hardware Offload;
- VLAN's;
- LACP;
- Port Mirroring;
- Prevenindo ataques de "MAC Flooding";
- DHCP Snooping;
- BPDU Guard;
- Limitação de Tráfego;
- MPLS Hardware Offload

Objetivos:

- Difundir as características dessa fantástica linha de switches;
- Desmistificar que é possível desfrutar de performance e estabilidade em redes comutadas em L2;
- Todos os recursos aqui apresentados serão recursos possíveis via HARDWARE;
- Propagar a MANEIRA CORRETA de configurar alguns recursos.

Case de backbone: ISP Radar Internet

- Backbone óptico com 10 e 20Gbps;
- Mais de 240 dispositivos com RouterOS, sendo 30 Switchs CRS3xx;
- 650km de backbone óptico;



Router (Cidade A)

Router (Cidade B)

Router (Cidade C)

Introdução à Série CRS3xx

- Switches com excelente custo x benefício;
- Aplicáveis desde redes de acesso até backbones;
- Opções com portas de até 40Gbps;
- Switches com características de roteador;
- **Comutação em Hardware (**Atende cenários mais exigentes);

MikroTik

CRS326-24G-2S+RM

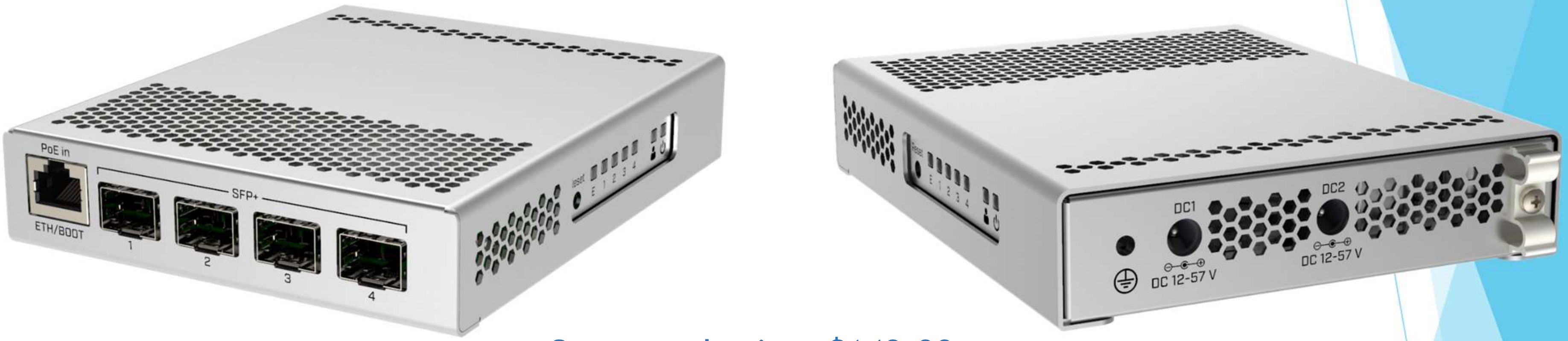
Suggested price: $139.00

Principais Características:

- 2 portas SFP+ (10Gbps);
- 24 portas ethernet 100/1000;
- Aimentação PoE;
- Útil para redes ópticas/Acesso

MikroTik

CRS305-1G-4S+IN



Suggested price: $149.00

- 1 porta ethernet 100/1000;
- 4 portas SFP+ (10Gbps);
- Alimentação via PoE;
- Alimentação DC Redundante;
- Design compacto e baixíssimo consumo de energia;

CRS 317

Suggested price: $399.00

- 16 portas de SFP+ (10Gbps);
- Fonte Redundante;
- Excelente para Backbones/Datacenters;
- Capacidade máxima de switching: 322 Gbps
- MPLS Hardware Offload;

CRS326-24S+2Q+RM

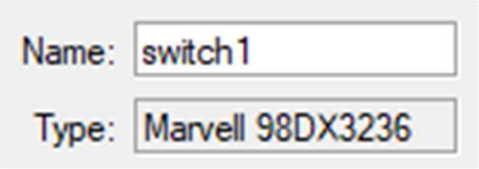
Suggested price: $499.00

- 24 portas (SFP+) de 10Gbps;
- 2 Portas (QSFP+) de 40Gbps;
- Capacidade máxima de switching: 640 Gbps
- Excelente para Backbones/Datacenters;

MikroTik

CRS 3xx conta com o poder...

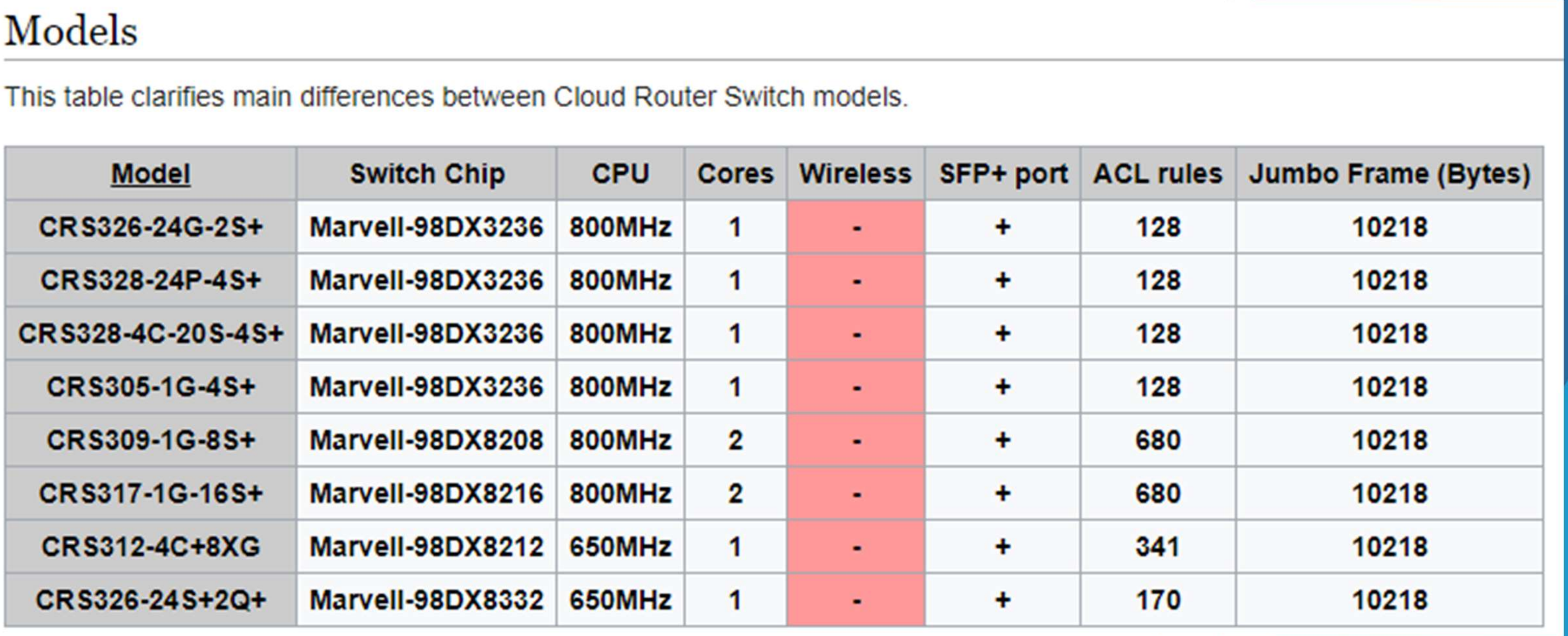
MARVELL®


Name: switch1

Type: Marvell 98DX3236

MikroTik

Características base:

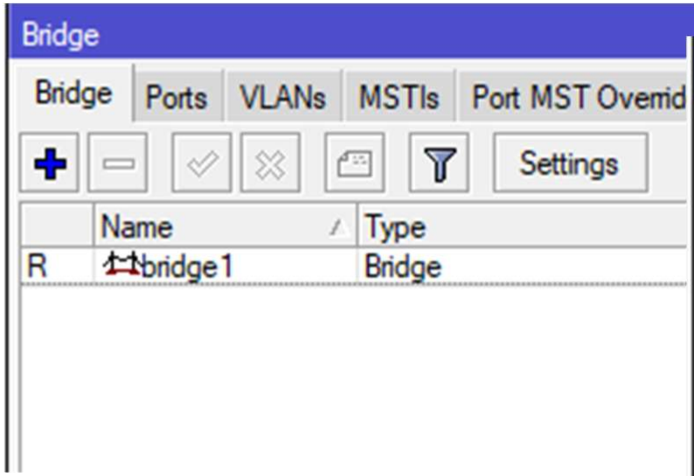


Models

This table clarifies main differences between Cloud Router Switch models.

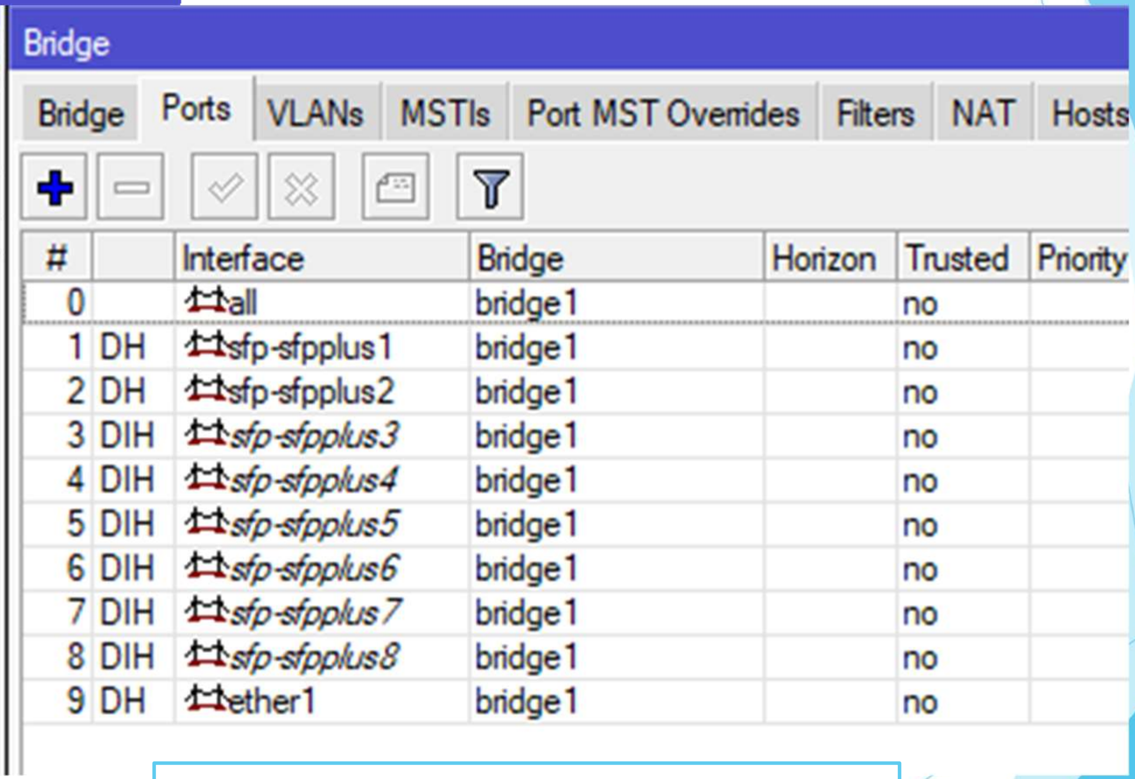
Model	Switch Chip	CPU	Cores	Wireless	SFP+ port	ACL rules	Jumbo Frame (Bytes)
CRS326-24G-2S+	Marvell-98DX3236	800MHz	1	-	+	128	10218
CRS328-24P-4S+	Marvell-98DX3236	800MHz	1	-	+	128	10218
CRS328-4C-20S-4S+	Marvell-98DX3236	800MHz	1	-	+	128	10218
CRS305-1G-4S+	Marvell-98DX3236	800MHz	1	-	+	128	10218
CRS309-1G-8S+	Marvell-98DX8208	800MHz	2	-	+	680	10218
CRS317-1G-16S+	Marvell-98DX8216	800MHz	2	-	+	680	10218
CRS312-4C+8XG	Marvell-98DX8212	650MHz	1	-	+	341	10218
CRS326-24S+2Q+	Marvell-98DX8332	650MHz	1	-	+	170	10218

Como Geralmente as pessoas fazem...



	Name	Type
R	bridge1	Bridge

1° Cria uma Bridge



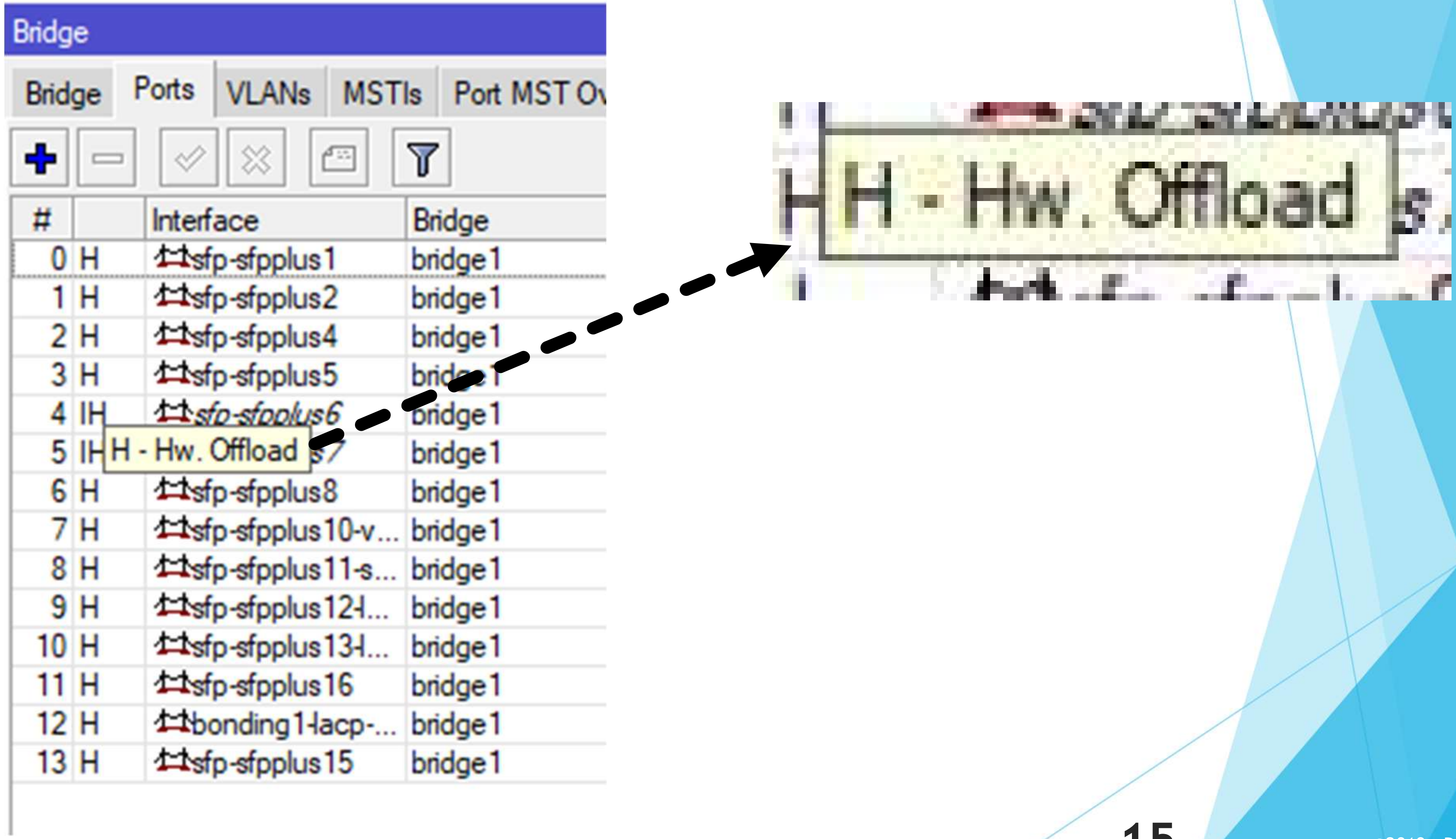
#		Interface	Bridge	Horizon	Trusted	Priority
0		all	bridge1		no	
1	DH	sfp-sfpplus1	bridge1		no	
2	DH	sfp-sfpplus2	bridge1		no	
3	DIH	sfp-sfpplus3	bridge1		no	
4	DIH	sfp-sfpplus4	bridge1		no	
5	DIH	sfp-sfpplus5	bridge1		no	
6	DIH	sfp-sfpplus6	bridge1		no	
7	DIH	sfp-sfpplus7	bridge1		no	
8	DIH	sfp-sfpplus8	bridge1		no	
9	DH	ether1	bridge1		no	

2° Adiciona Todas as portas na Bridge

MikroTik

CONTE-ME MAIS SOBRE ESSE SEU...
"SWITCHZÃO"
imgflip.com

Hardware Offload



Bridge

Bridge | Ports | VLANs | MSTIs | Port MST Ov

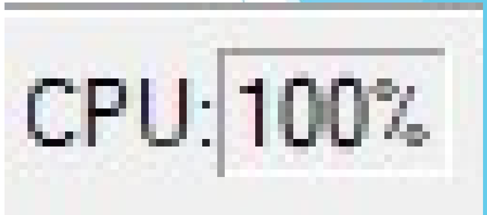
#		Interface	Bridge
0	H	sfp-sfpplus1	bridge1
1	H	sfp-sfpplus2	bridge1
2	H	sfp-sfpplus4	bridge1
3	H	sfp-sfpplus5	bridge1
4	IH	*sfp-sfpplus6*	bridge1
5	IH	s7	bridge1
6	H	sfp-sfpplus8	bridge1
7	H	sfp-sfpplus10-v...	bridge1
8	H	sfp-sfpplus11-s...	bridge1
9	H	sfp-sfpplus12-l...	bridge1
10	H	sfp-sfpplus13-l...	bridge1
11	H	sfp-sfpplus16	bridge1
12	H	bonding1-lacp-...	bridge1
13	H	sfp-sfpplus15	bridge1

H - Hw. Offload

H - Hw. Offload

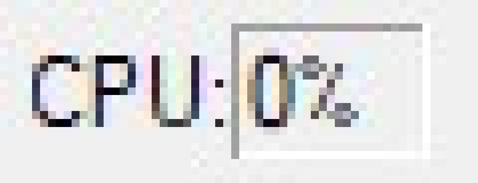
Hardware Offload

SEM Hardware Offload



CPU: 100%

COM Hardware Offload

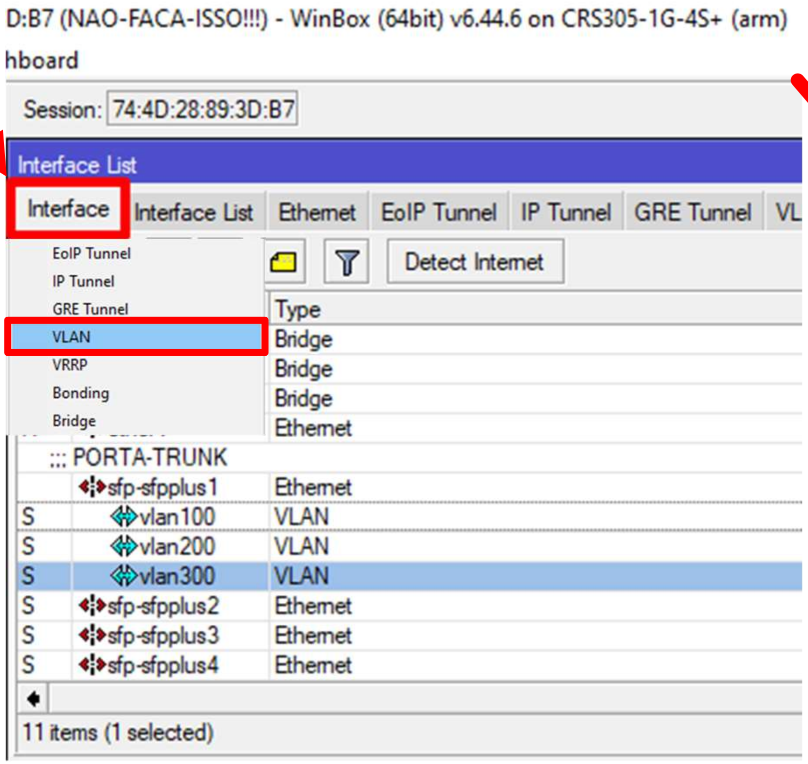


CPU: 0%

O SEGREDO É...
NÃO PERDER O HARDWARE OFFLOAD
imgflip.com

VLANs

JAMAIS FAÇA ISSO!



D:B7 (NAO-FACA-ISSO!!!) - WinBox (64bit) v6.44.6 on CRS305-1G-4S+ (arm)

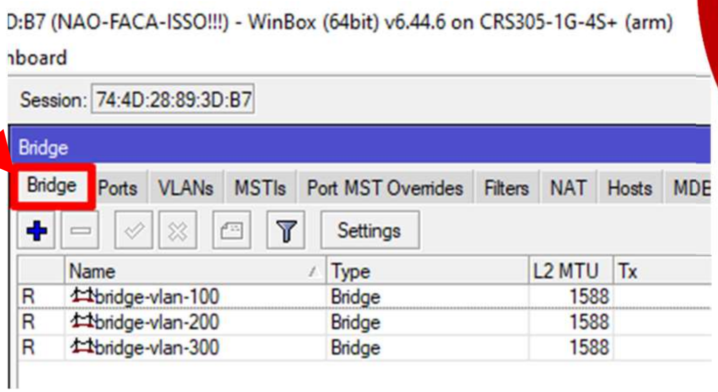
hboard

Session: 74:4D:28:89:3D:B7

Interface List

	Name	Type
		Bridge
		Bridge
		Bridge
		Ethernet
	;;; PORTA-TRUNK	
	sfp-sfpplus1	Ethernet
S	vlan100	VLAN
S	vlan200	VLAN
S	vlan300	VLAN
S	sfp-sfpplus2	Ethernet
S	sfp-sfpplus3	Ethernet
S	sfp-sfpplus4	Ethernet

11 items (1 selected)



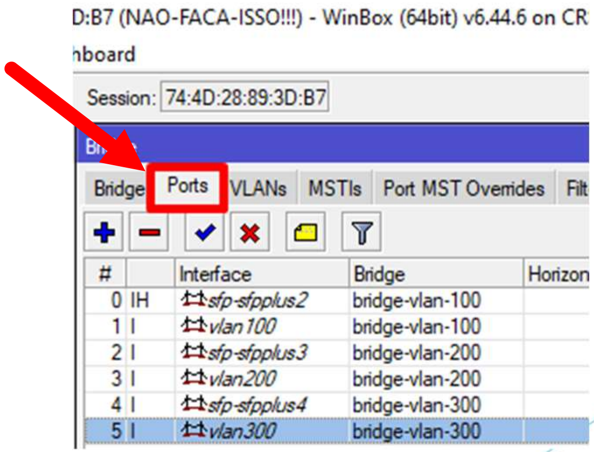
D:B7 (NAO-FACA-ISSO!!!) - WinBox (64bit) v6.44.6 on CRS305-1G-4S+ (arm)

hboard

Session: 74:4D:28:89:3D:B7

Bridge

	Name	Type	L2 MTU	Tx
R	bridge-vlan-100	Bridge	1588	
R	bridge-vlan-200	Bridge	1588	
R	bridge-vlan-300	Bridge	1588	

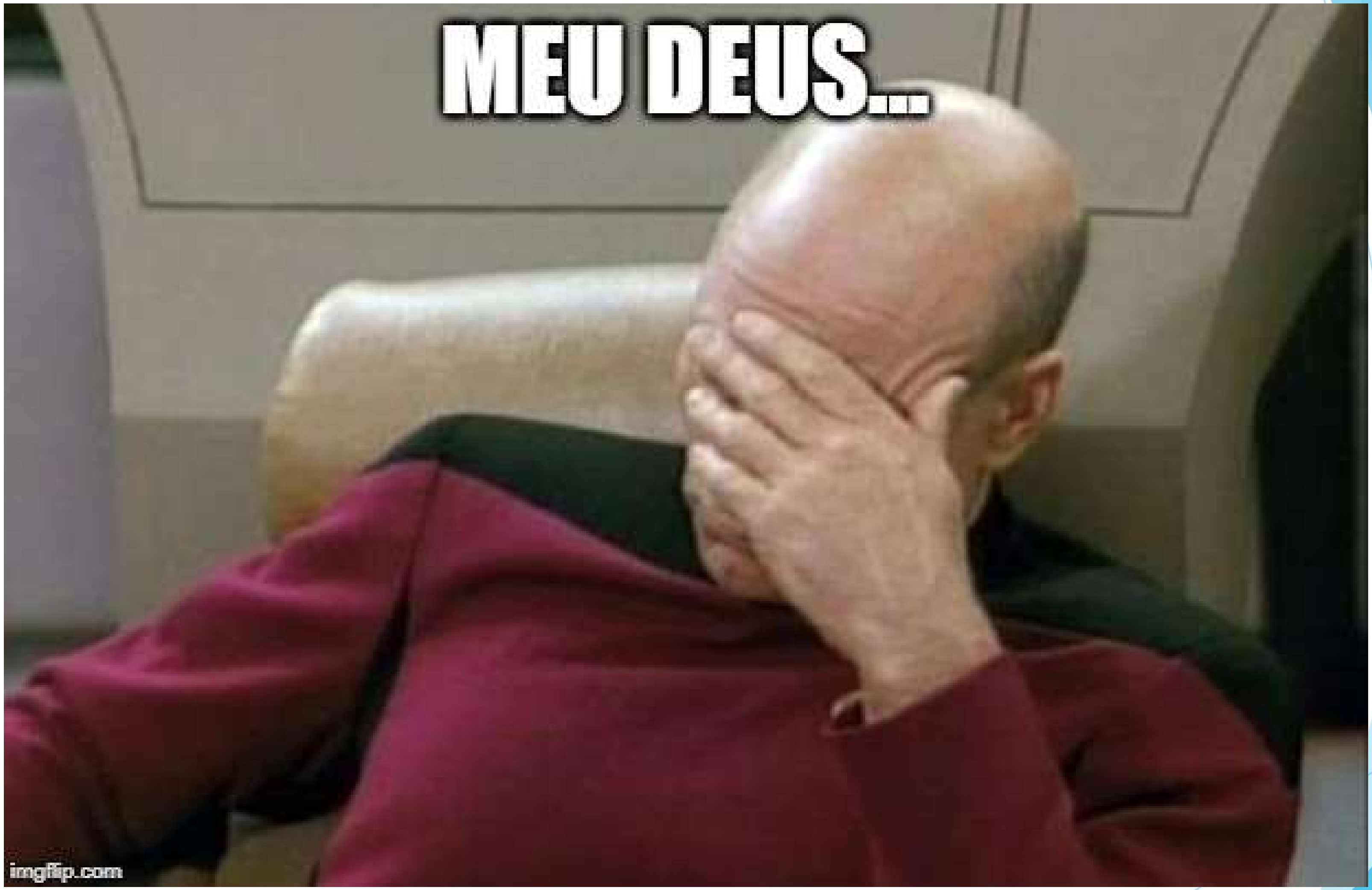


D:B7 (NAO-FACA-ISSO!!!) - WinBox (64bit) v6.44.6 on CR

hboard

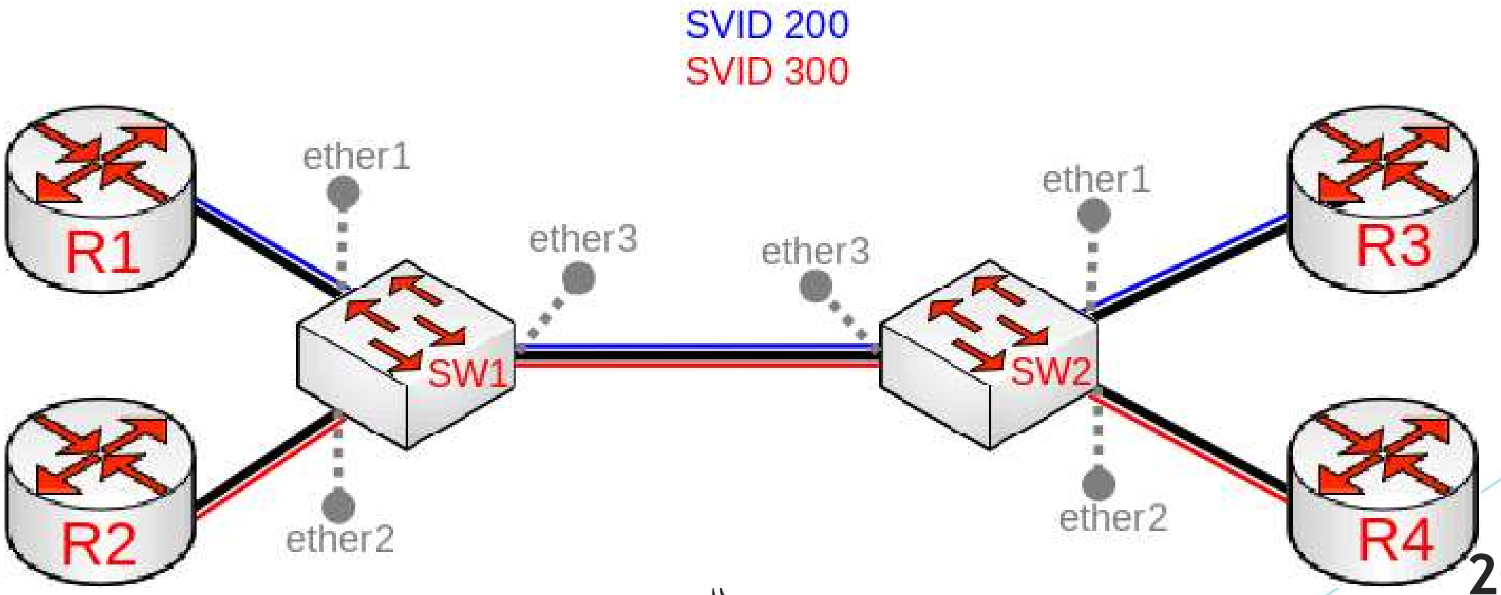
Session: 74:4D:28:89:3D:B7

#		Interface	Bridge	Horizon
0	IH	sfp-sfpplus2	bridge-vlan-100	
1	I	vlan100	bridge-vlan-100	
2	I	sfp-sfpplus3	bridge-vlan-200	
3	I	vlan200	bridge-vlan-200	
4	I	sfp-sfpplus4	bridge-vlan-300	
5	I	vlan300	bridge-vlan-300	


MEU DEUS...
imgflip.com

VLANs (Tagged)

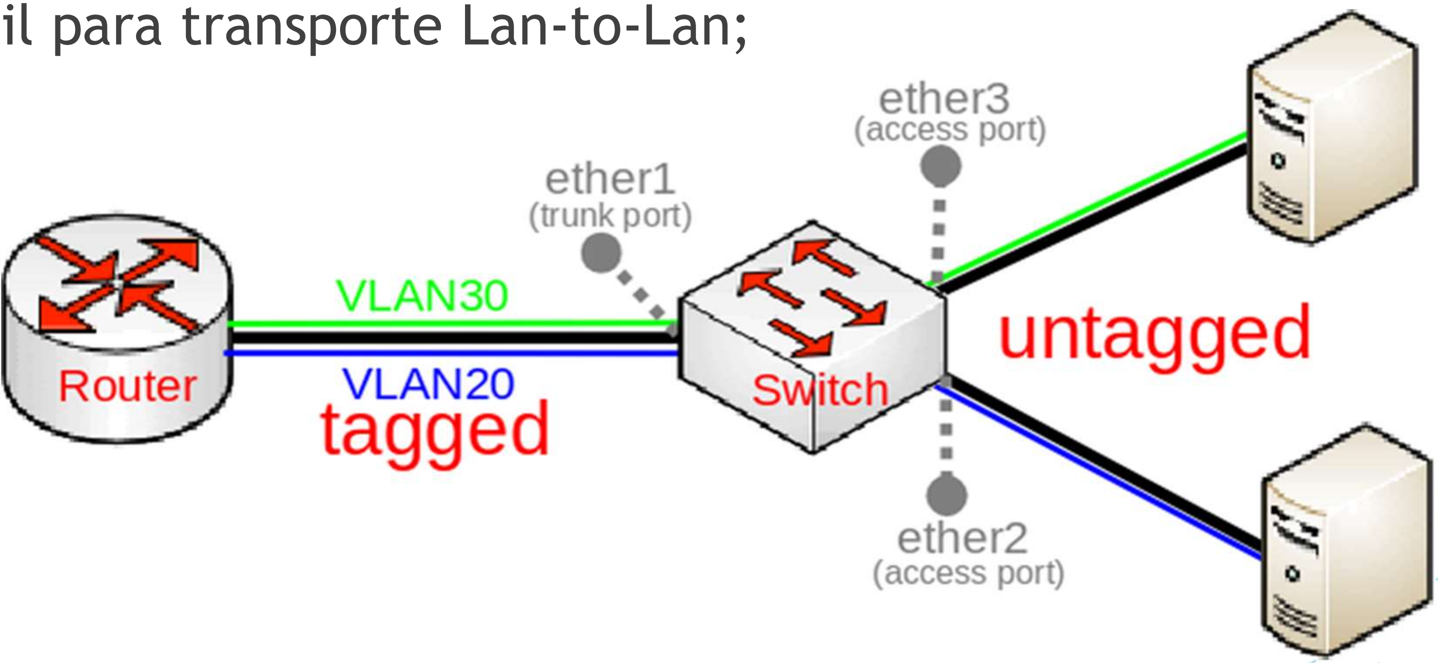
- O switch espera já receber frames com alguma Tag;
- Útil para isolar domínios de broadcast/gerencia;
- Útil para transportes Lan-to-Lan;



MikroTik

VLANs (Untagged)

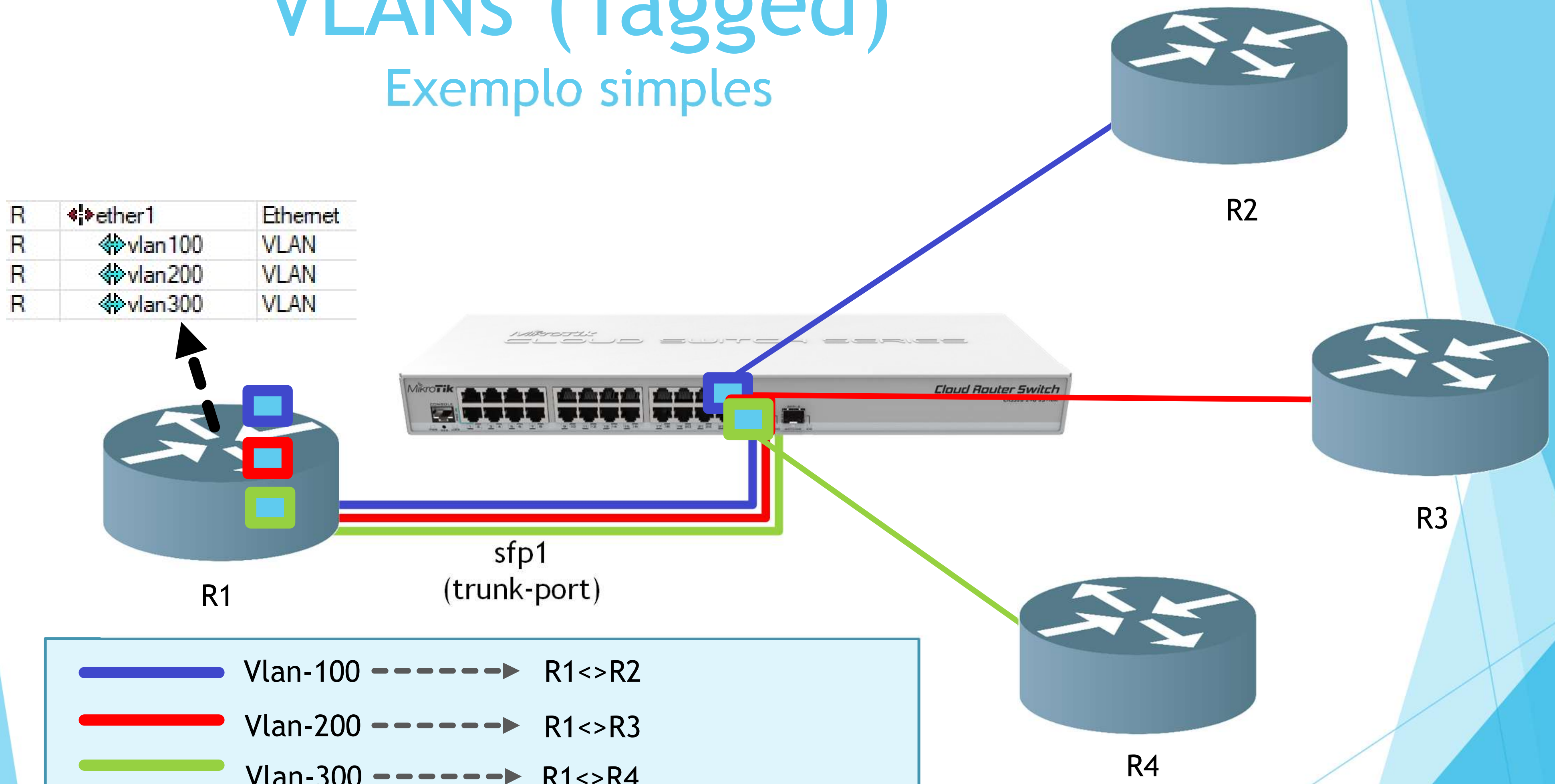
- O switch recebe ou remove um “Tag” do Frame;
- Uso em redes de acesso/servidores/gerencia;
- Útil para transporte Lan-to-Lan;



MikroTik

VLANs (Tagged)

Exemplo simples



R	ether1	Ethernet
R	vlan100	VLAN
R	vlan200	VLAN
R	vlan300	VLAN

🟦 Vlan-100 ------▶ R1<>R2

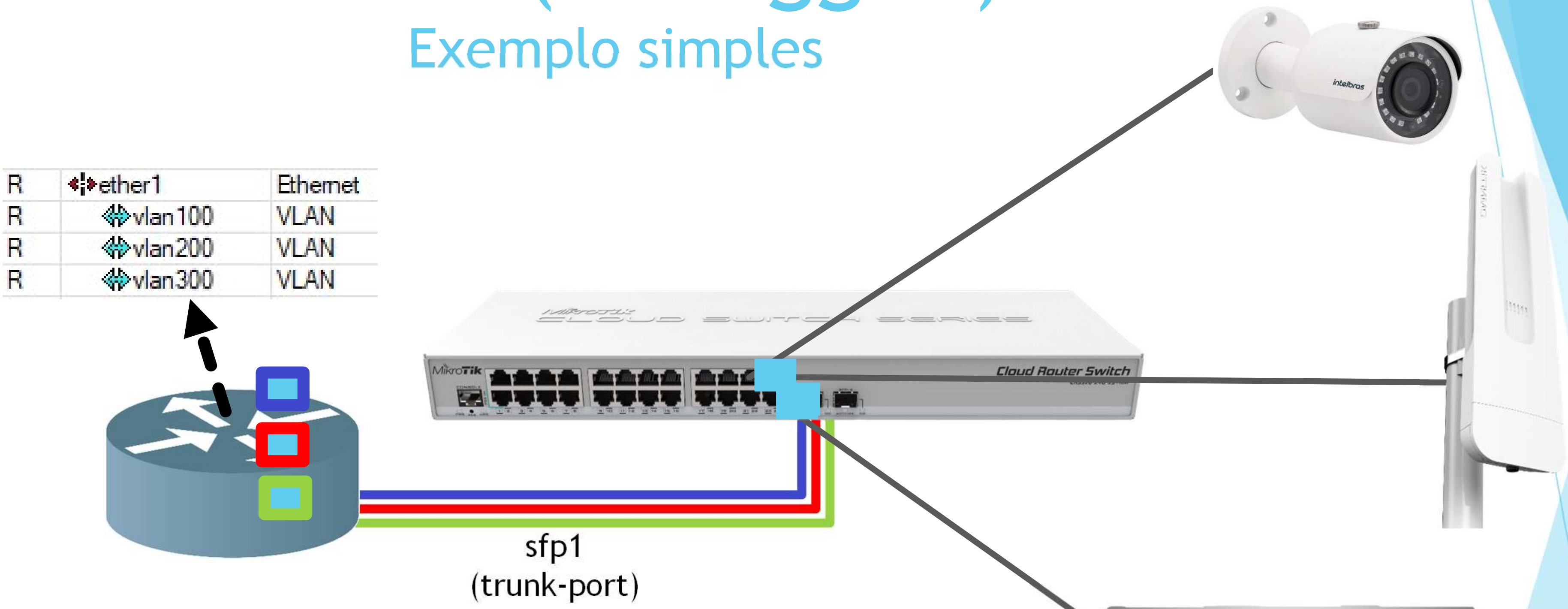
🟥 Vlan-200 ------▶ R1<>R3

🟩 Vlan-300 ------▶ R1<>R4

🟦 Payload

VLANs (Untagged)

Exemplo simples



```
R   ether1      Ethernet
R     vlan100   VLAN
R     vlan200   VLAN
R     vlan300   VLAN
```

🟦 Vlan-100 ------▶ Camera

🟥 Vlan-200 ------▶ OmniTIK

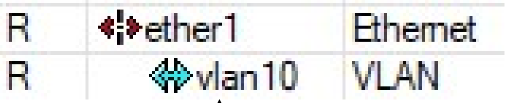
🟩 Vlan-300 ------▶ DELL Server

■ Payload

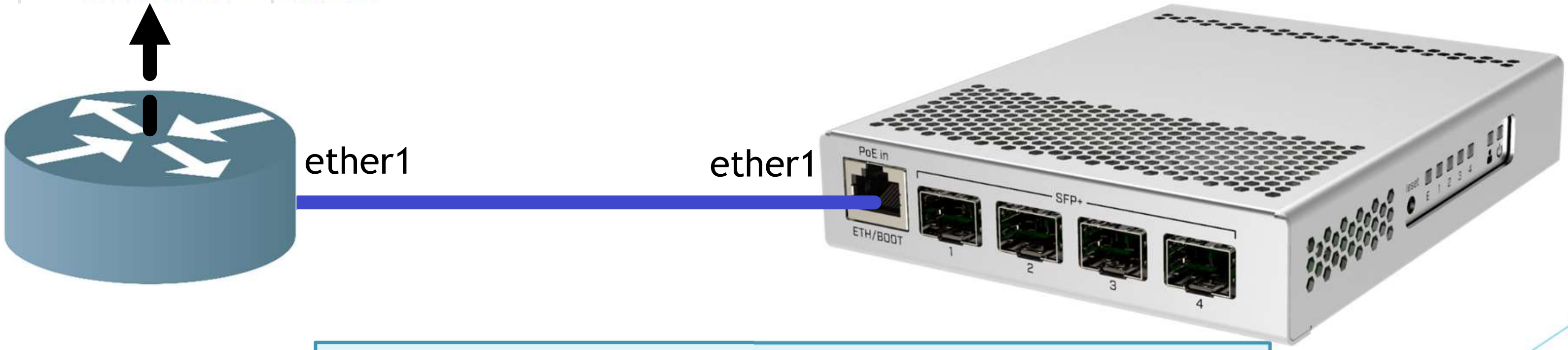
VLAN de Gerencia (tagged)

Exemplo

- Objetivo:
  - Filtrar a gerencia do Switch em modo “tagged” pela VLAN ID 10 sobre via ether1;



R	ether1	Ethernet
R	vlan10	VLAN

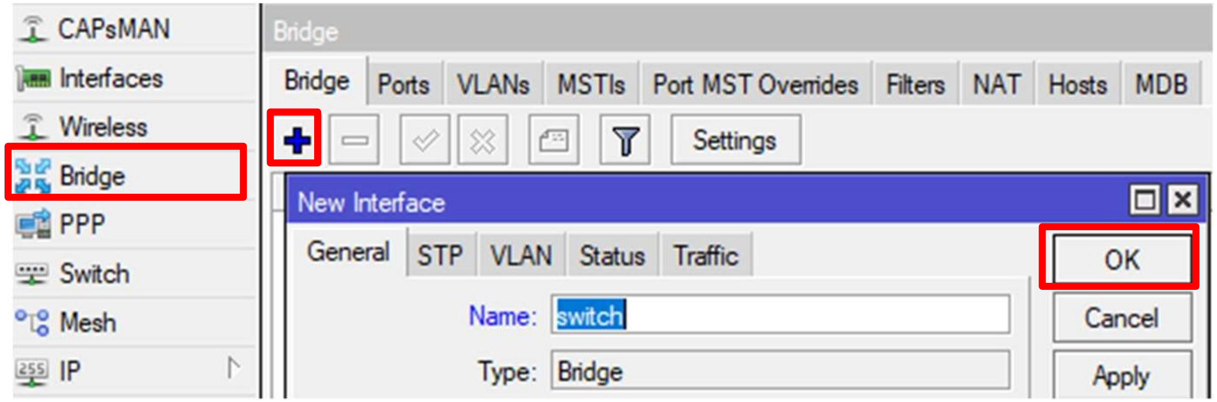


Vlan-10 (tagged) ----> Gerencia

VLAN de Gerencia (tagged)

Exemplo

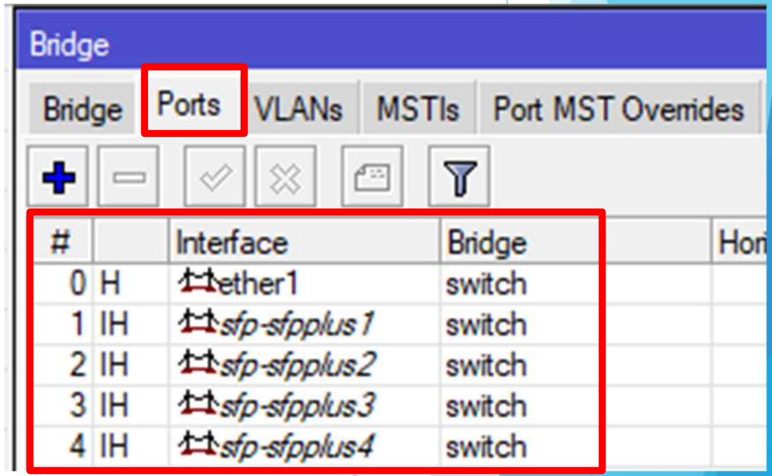
1- Criar uma bridge



Name: switch

Type: Bridge

2- Vincular as portas à Bridge



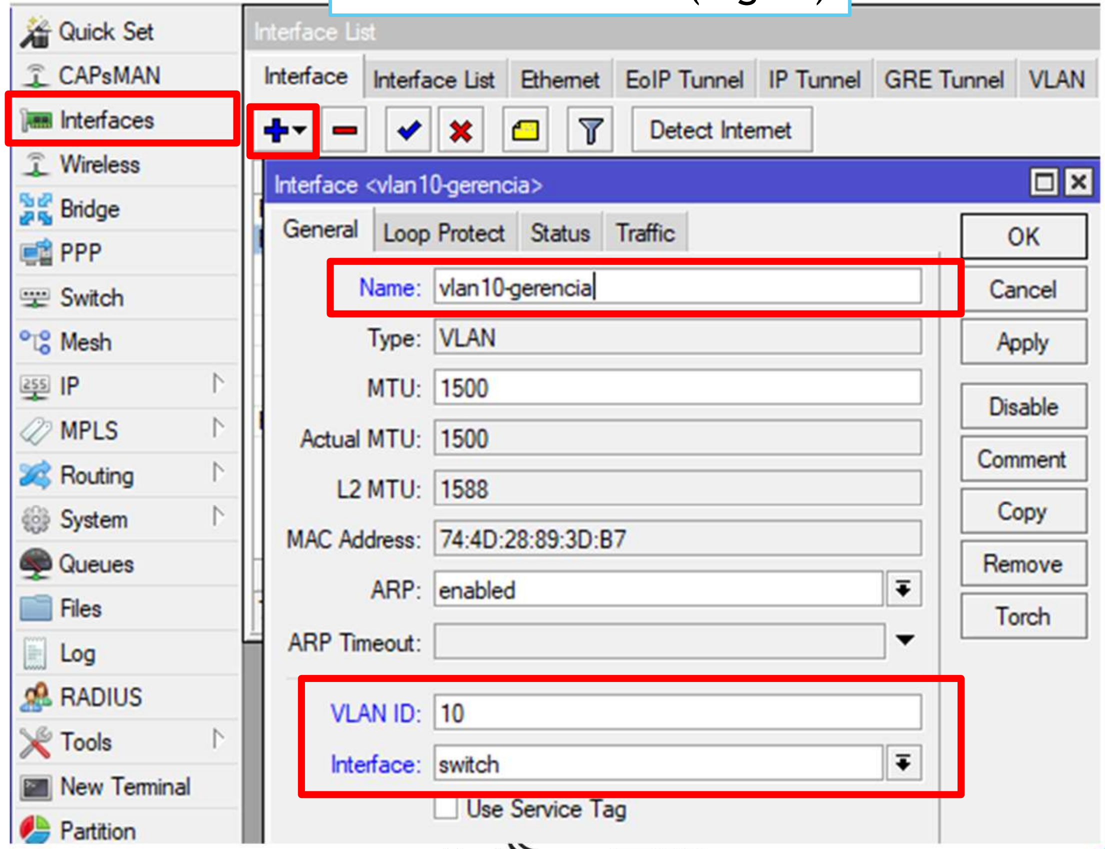
#		Interface	Bridge	Hori
0	H	ether1	switch	
1	IH	sfp-sfpplus1	switch	
2	IH	sfp-sfpplus2	switch	
3	IH	sfp-sfpplus3	switch	
4	IH	sfp-sfpplus4	switch	

MikroTik

VLAN de Gerencia (tagged)

Exemplo

3- Criar uma vlan (lógica)



Name: vlan10-gerencia

Type: VLAN

MTU: 1500

Actual MTU: 1500

L2 MTU: 1588

MAC Address: 74:4D:28:89:3D:B7

ARP: enabled

ARP Timeout:

VLAN ID: 10

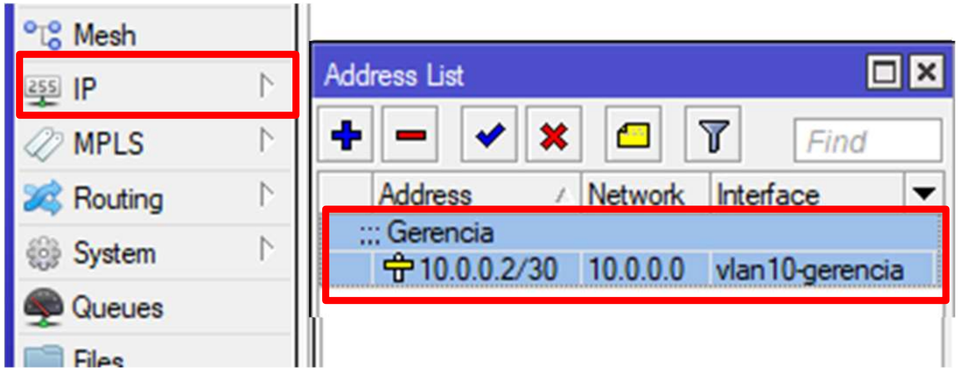
Interface: switch

□ Use Service Tag

VLAN de Gerencia (tagged)

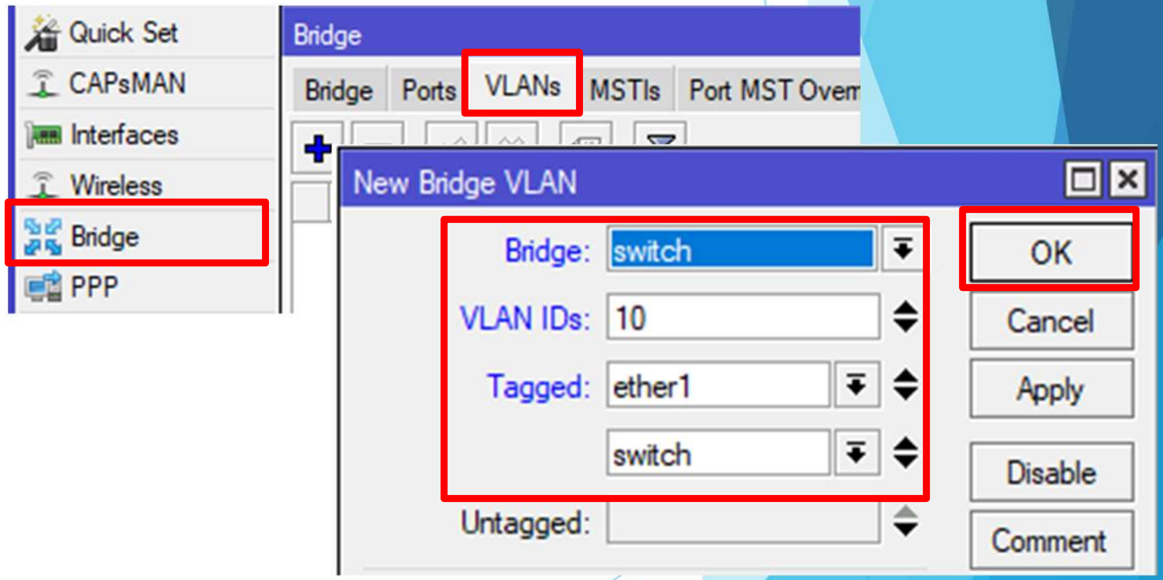
Exemplo

4- Adicionar o IP de Gerencia à VLAN criada



Address	Network	Interface
::: Gerencia		
10.0.0.2/30	10.0.0.0	vlan10-gerencia

5- Marcar essa VLAN como "Tagged" nas respectivas interfaces;



Bridge: switch

VLAN IDs: 10

Tagged: ether1

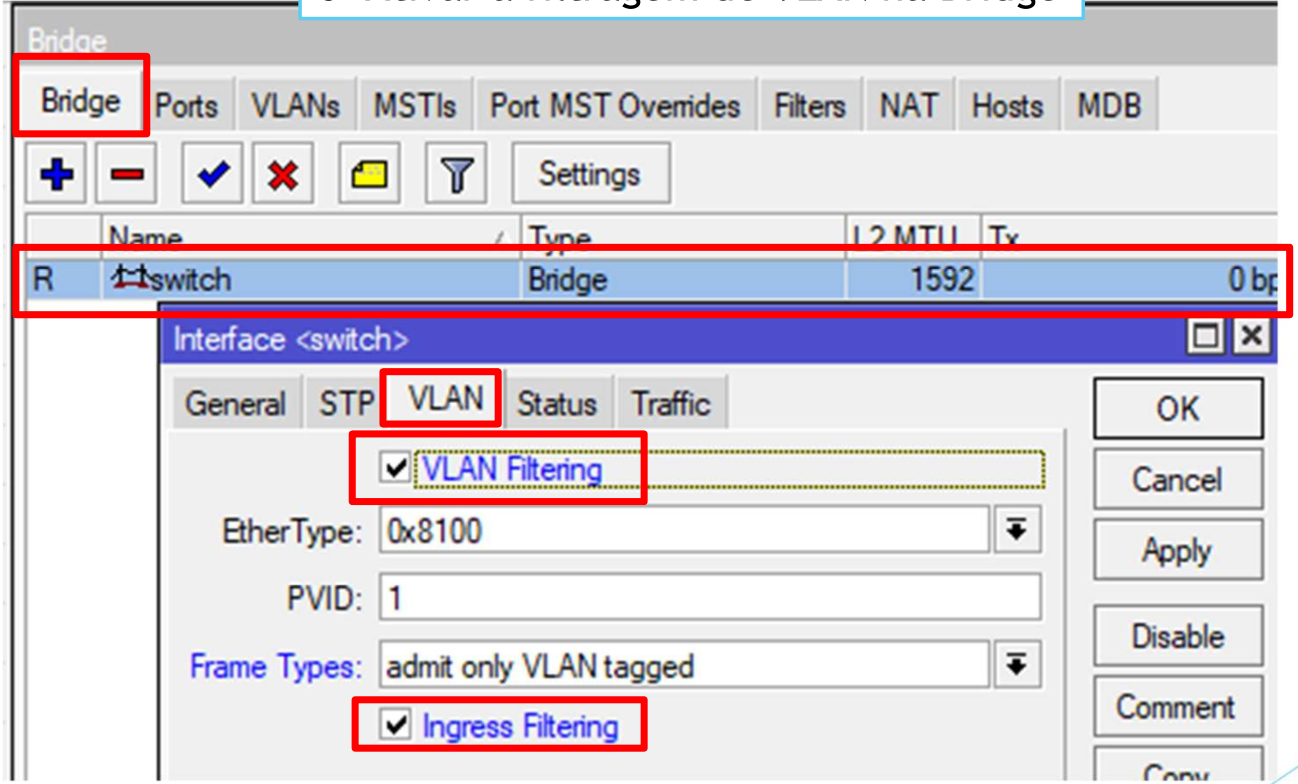
switch

Untagged:

VLAN de Gerencia (tagged)

Exemplo

6- Ativar a filtragem de VLAN na Bridge



	Name	Type	L2 MTU	Tx
R	switch	Bridge	1592	0 bp

☑ VLAN Filtering

EtherType: 0x8100

PVID: 1

Frame Types: admit only VLAN tagged

☑ Ingress Filtering

VLAN de Gerencia (Considerações finais)

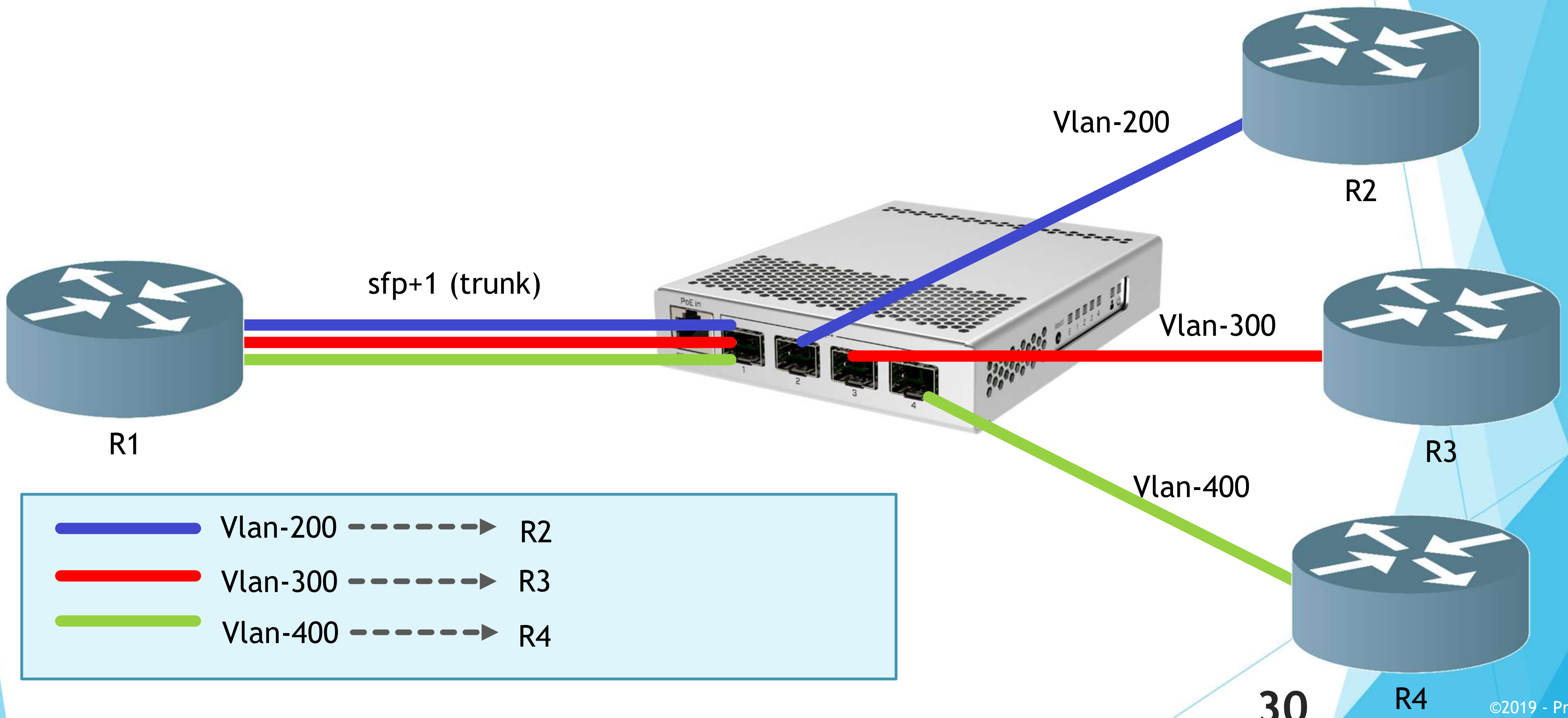
- Preferencialmente faça essa configuração antes das demais

(se possível em bancada);

- Ficar atento à erros (eles podem custar caro);
- Usar o “Safe mode” e “RoMON para testes/gerencia;
- A Mikrotik recomenda realizar a ativação do “Vlan Filtering” usando cabo serial (se possível);

VLANs (Tagged)

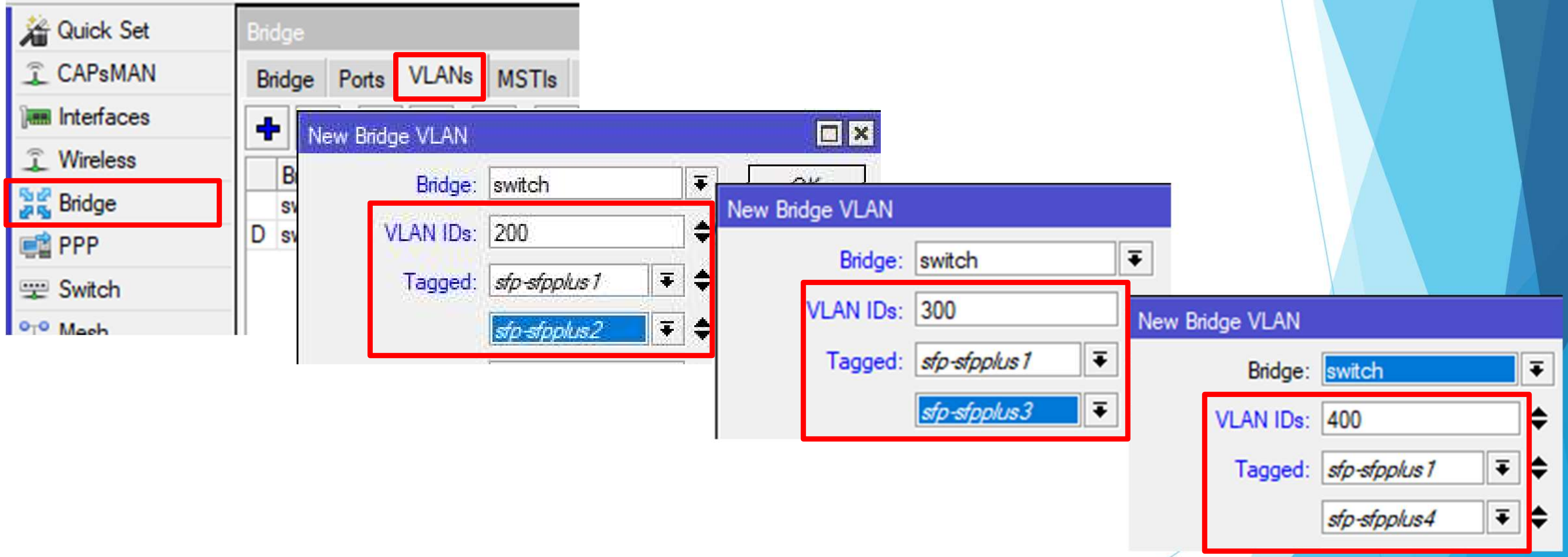
Como Fazer?


sfp+1 (trunk)
R1
Vlan-200
R2
Vlan-300
R3
Vlan-400
R4
🟦 Vlan-200 - - - - - - → R2
🟥 Vlan-300 - - - - - - → R3
🟩 Vlan-400 - - - - - - → R4

VLANs (Tagged)

Como Fazer?

1- Criar os grupos de portas que permitirão a passagem das VLANs tipo “Tagged”



New Bridge VLAN

Bridge: switch

VLAN IDs: 200

Tagged: sfp-sfpplus1

sfp-sfpplus2

New Bridge VLAN

Bridge: switch

VLAN IDs: 300

Tagged: sfp-sfpplus1

sfp-sfpplus3

New Bridge VLAN

Bridge: switch

VLAN IDs: 400

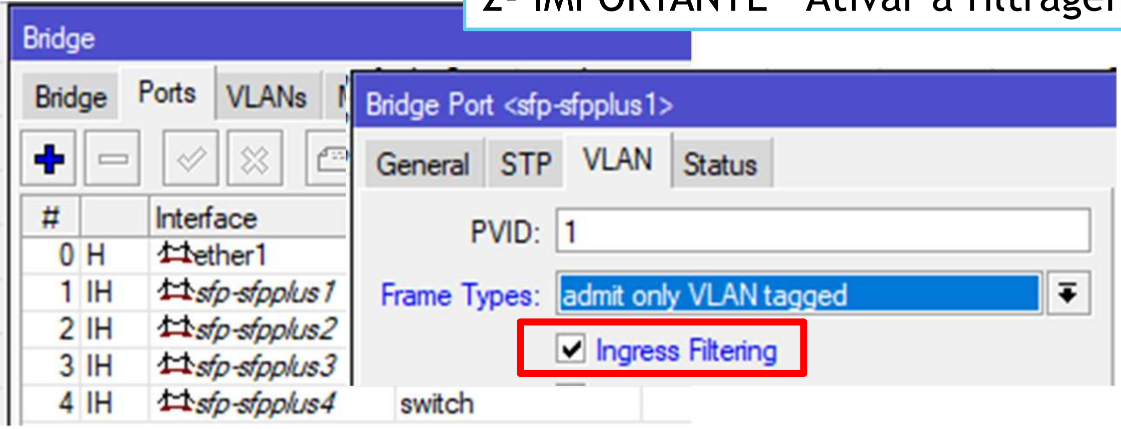
Tagged: sfp-sfpplus1

sfp-sfpplus4

VLANs (Tagged)

Como Fazer?

2- IMPORTANTE – Ativar a filtragem nas respectivas portas físicas



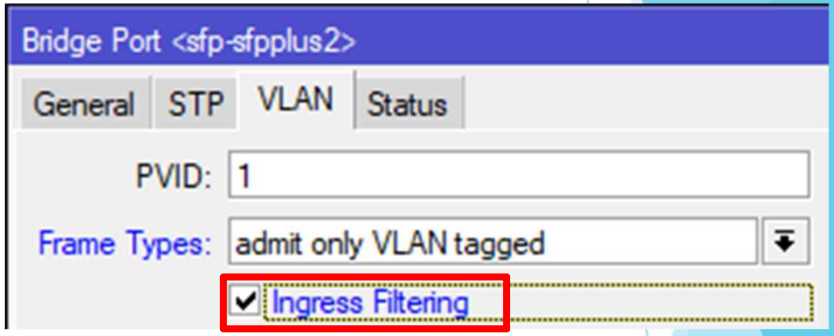
#		Interface	
0	H	ether1	
1	IH	sfp-sfpplus1	
2	IH	sfp-sfpplus2	
3	IH	sfp-sfpplus3	
4	IH	sfp-sfpplus4	switch

Bridge Port <sfp-sfpplus1>

PVID: 1

Frame Types: admit only VLAN tagged

☑ Ingress Filtering

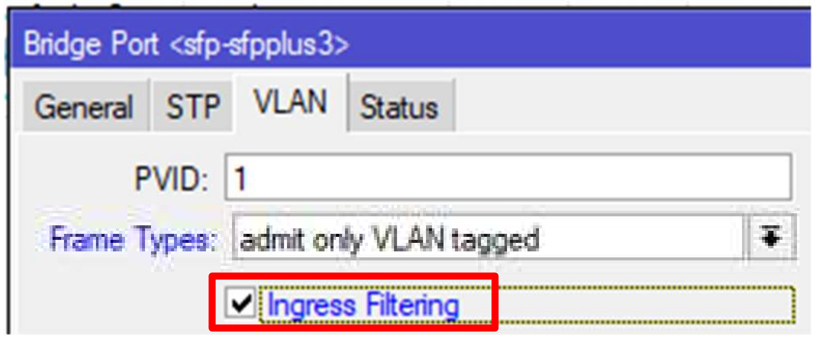


Bridge Port <sfp-sfpplus2>

PVID: 1

Frame Types: admit only VLAN tagged

☑ Ingress Filtering

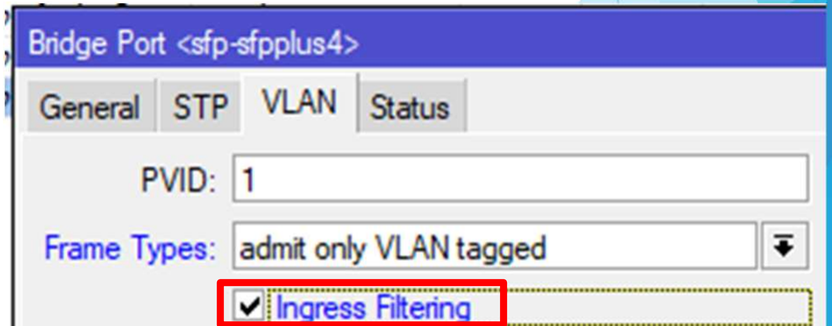


Bridge Port <sfp-sfpplus3>

PVID: 1

Frame Types: admit only VLAN tagged

☑ Ingress Filtering



Bridge Port <sfp-sfpplus4>

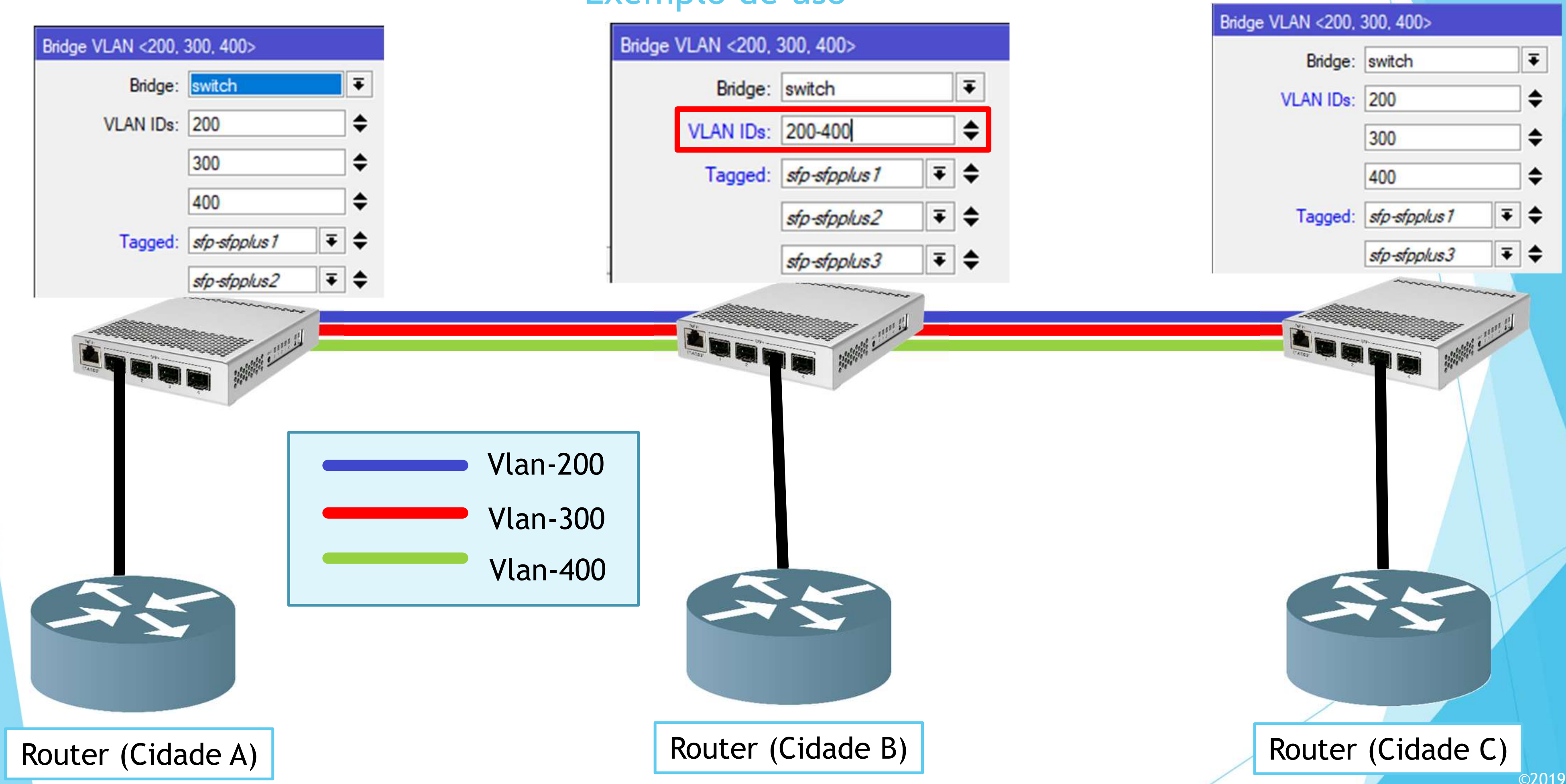
PVID: 1

Frame Types: admit only VLAN tagged

☑ Ingress Filtering

VLANs (Tagged)

Exemplo de uso



Bridge VLAN <200, 300, 400>

Bridge: switch

VLAN IDs: 200
300
400

Tagged: sfp-sfpplus1
sfp-sfpplus2

Bridge VLAN <200, 300, 400>

Bridge: switch

VLAN IDs: 200-400

Tagged: sfp-sfpplus1
sfp-sfpplus2
sfp-sfpplus3

Bridge VLAN <200, 300, 400>

Bridge: switch

VLAN IDs: 200
300
400

Tagged: sfp-sfpplus1
sfp-sfpplus3

🟦 Vlan-200
🟥 Vlan-300
🟩 Vlan-400

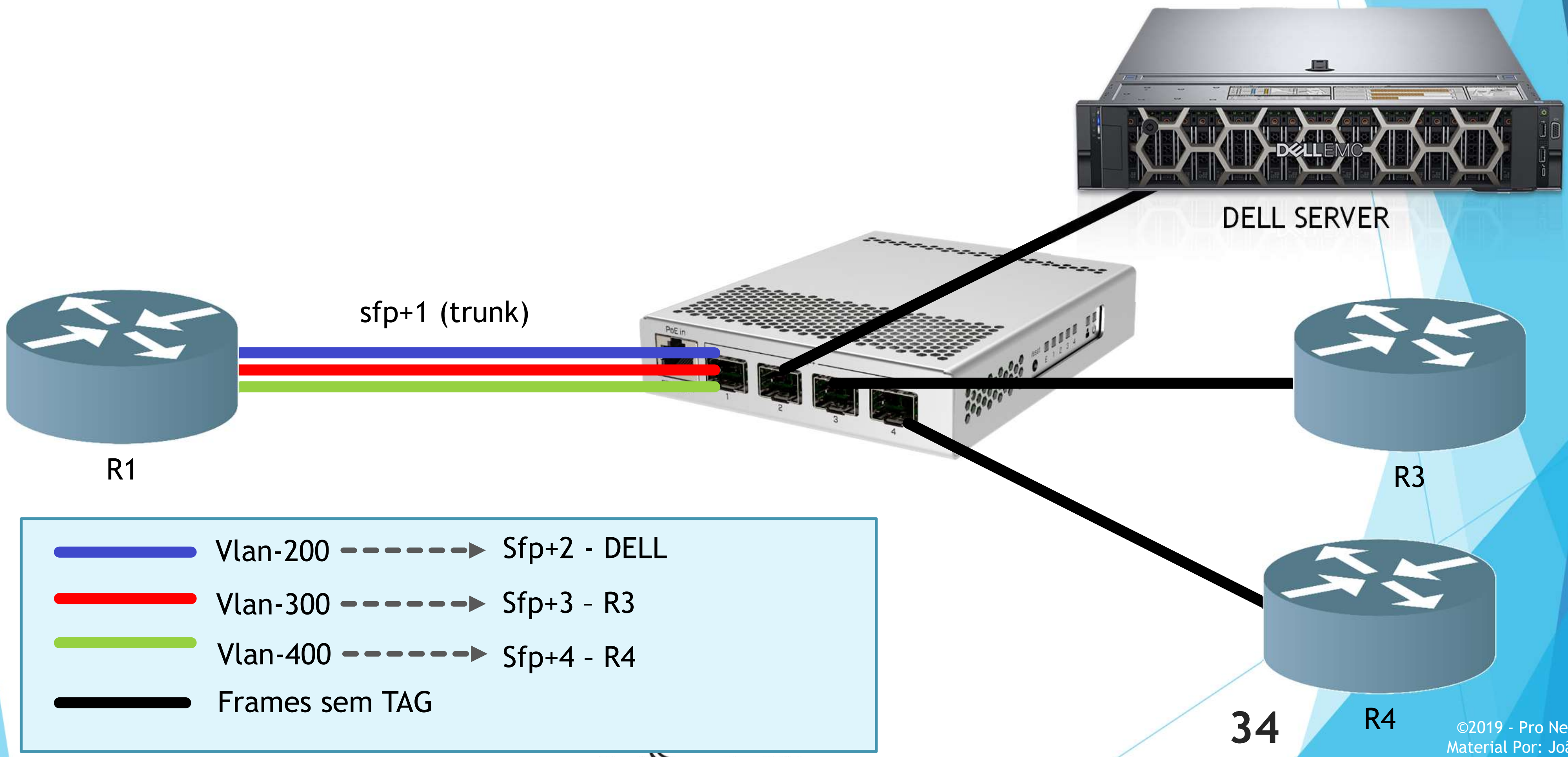
Router (Cidade A)

Router (Cidade B)

Router (Cidade C)

VLANs (Untagged)

Como Fazer?



🟦 Vlan-200 ------▶ Sfp+2 - DELL

🟥 Vlan-300 ------▶ Sfp+3 – R3

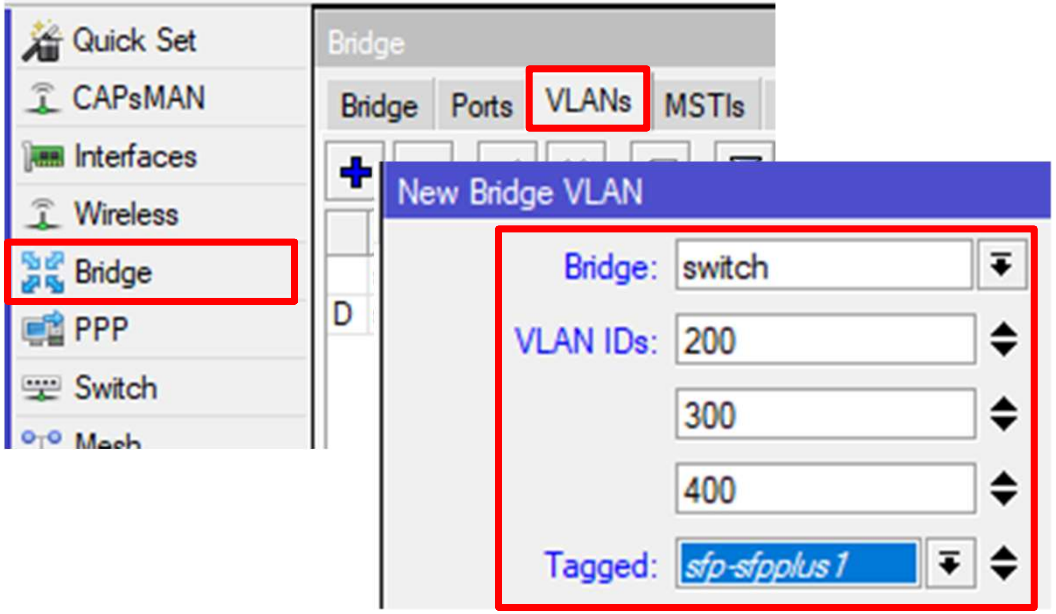
🟩 Vlan-400 ------▶ Sfp+4 – R4

⬛ Frames sem TAG

VLANs (Untagged)

Como Fazer?

1- Adicionar a Trunk Port e VLANs Tagged



Bridge: switch

VLAN IDs: 200

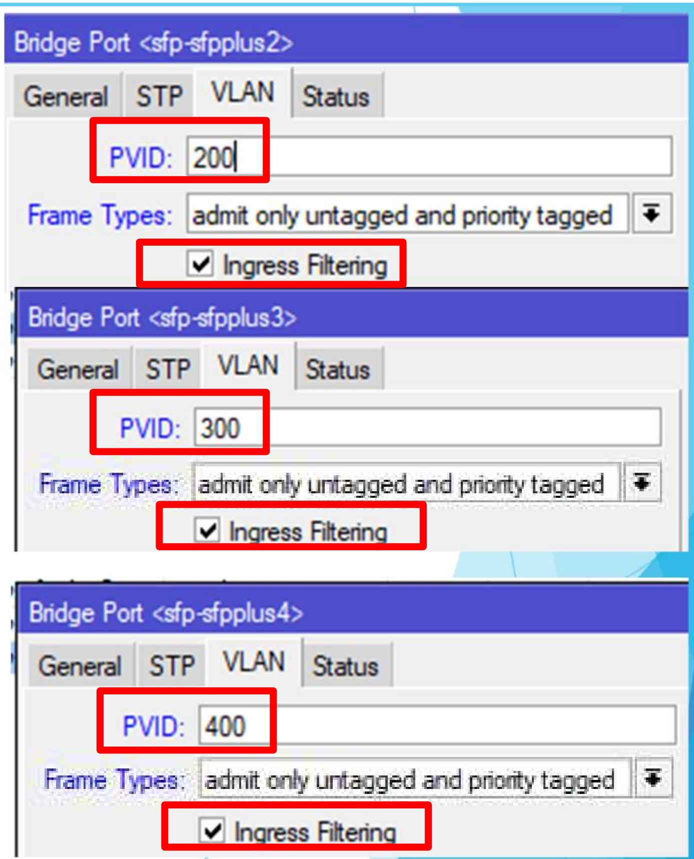
300

400

Tagged: sfp-sfpplus1

Menu “Bridge > Ports”

2- EM PVID dizer qual tratará frames “Untagged”



Bridge Port <sfp-sfpplus2>

PVID: 200

Frame Types: admit only untagged and priority tagged

☑ Ingress Filtering

Bridge Port <sfp-sfpplus3>

PVID: 300

Frame Types: admit only untagged and priority tagged

☑ Ingress Filtering

Bridge Port <sfp-sfpplus4>

PVID: 400

Frame Types: admit only untagged and priority tagged

☑ Ingress Filtering

VLANs

Considerações Gerais

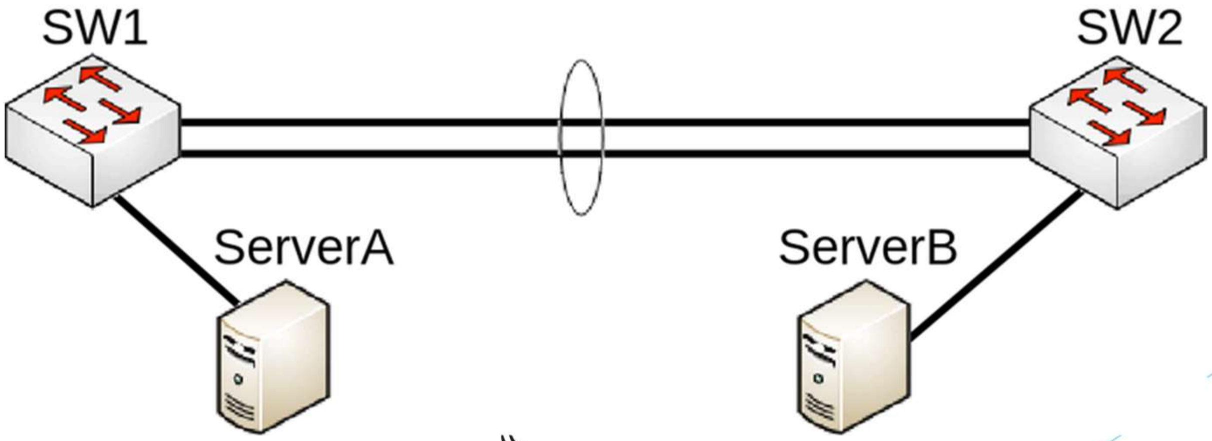
- ✓ Sempre usar “ingress filtering” nas interfaces para garantir o isolamento de broadcast;
- ✓ Essas configurações são válidas exclusivamente para a série CRS3xx (modo hardware);
- ✓ Existem diferentes formas de se configurar (dependendo do hardware/serie);

MikroTik

LACP

(Link Aggregation Control Protocol)

- Útil para agregar 1 ou mais circuitos/Interfaces;
- Possibilidade de transportar VLANs (Tagged ou Untagged);
- Proporciona também HA;
- É possível agregar até 8 portas pro grupo;
- Sempre observar o “Hash” correto para seu cenário;

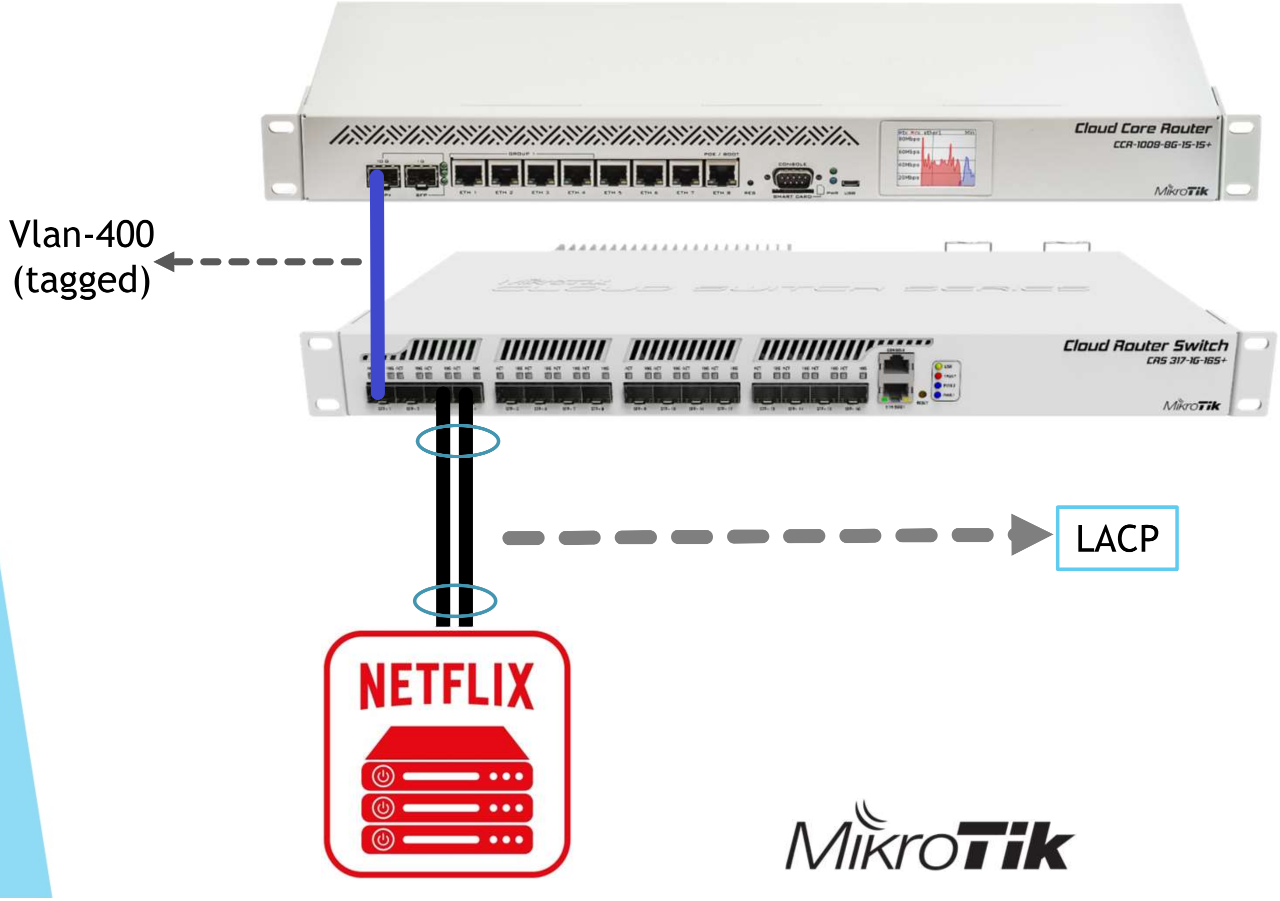


MikroTik

LACP

(Caso de uso)

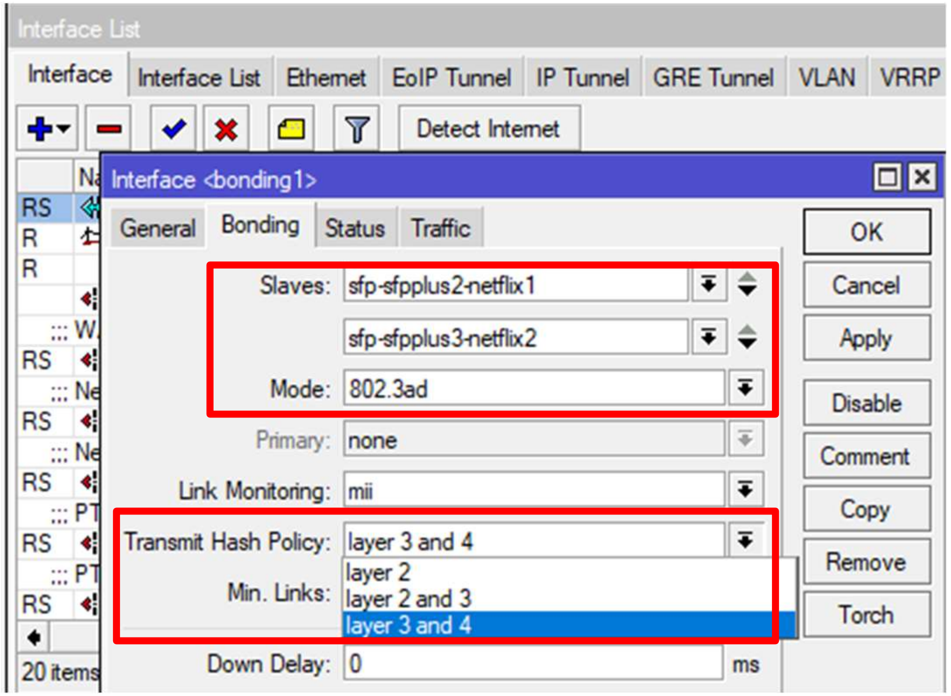
- Exemplo com CDN (Netflix) (LACP + VLAN)



LACP

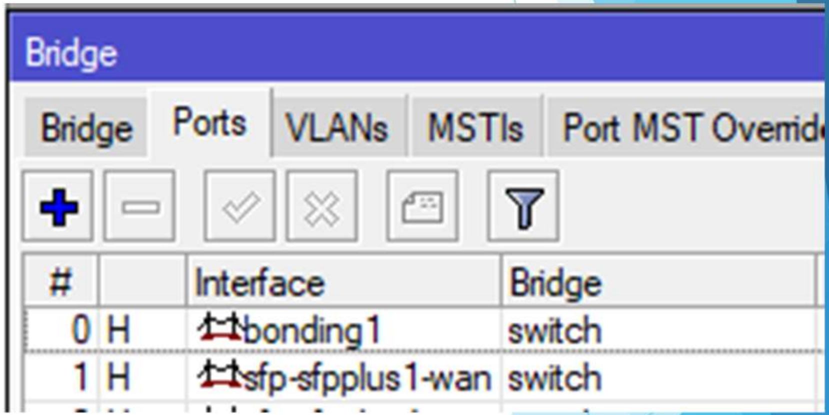
(Como fazer?)

1- Criar uma interface "Bonding" no modo 802.3ad



Slaves: sfp-sfpplus2-netflix1
sfp-sfpplus3-netflix2
Mode: 802.3ad
Primary: none
Link Monitoring: mii
Transmit Hash Policy: layer 3 and 4
layer 2
layer 2 and 3
layer 3 and 4
Min. Links:
Down Delay: 0 ms

2- Adicionar o Bonding na Bridge



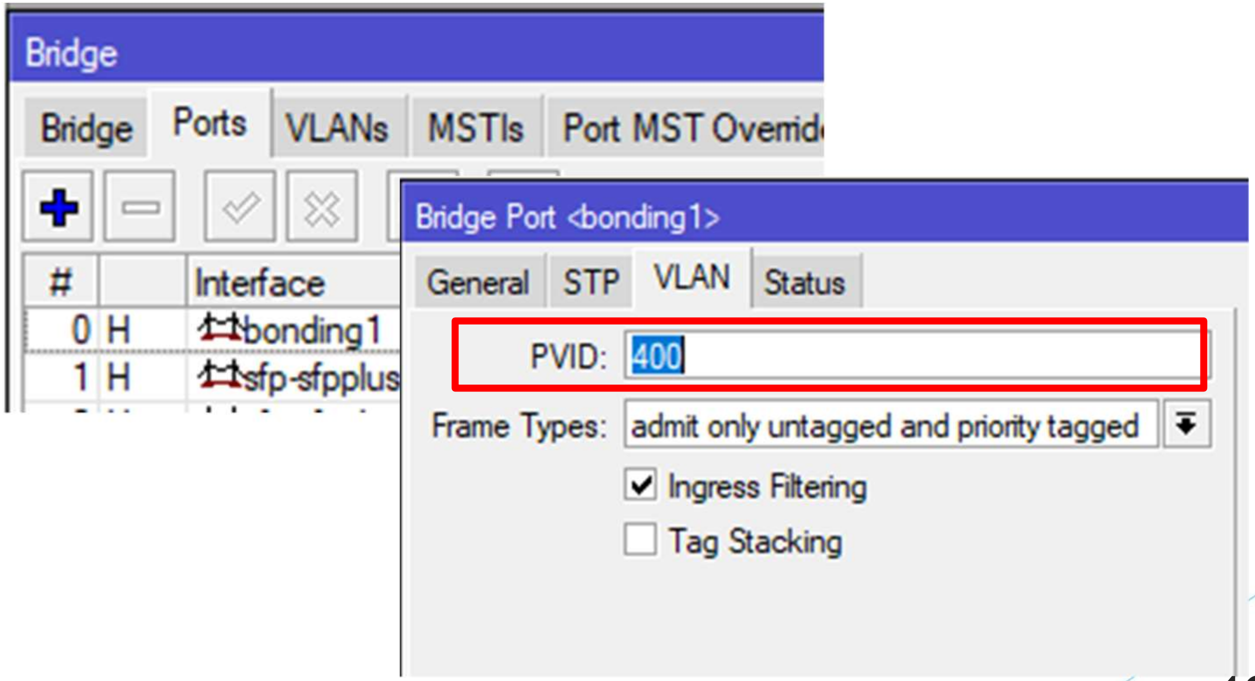
#		Interface	Bridge
0	H	bonding1	switch
1	H	sfp-sfpplus1-wan	switch

*É possível também em modo "balance-xor"

LACP

(Como fazer?)

3- Colocar o PVID 400 (untagged) no Bonding



PVID: 400

Frame Types: admit only untagged and priority tagged

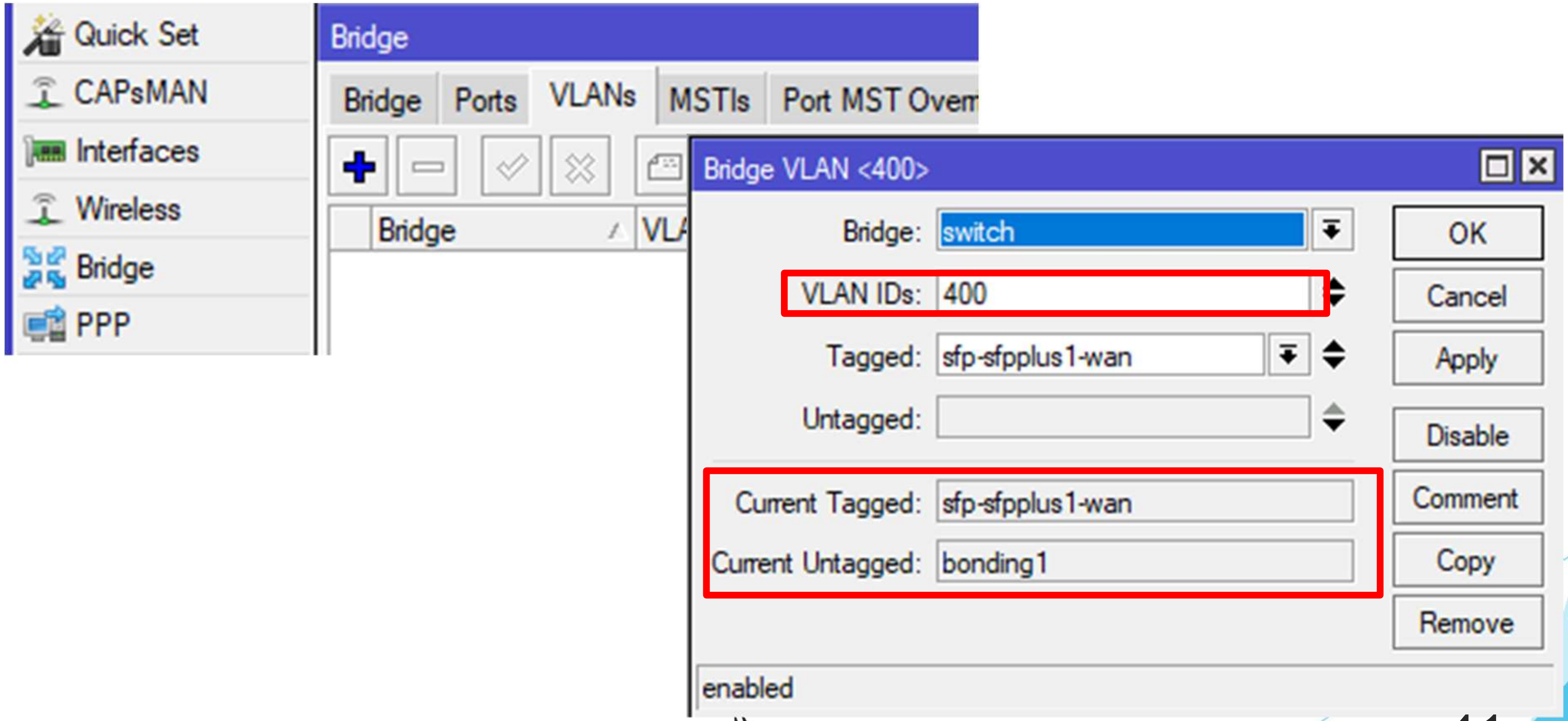
☑ Ingress Filtering

□ Tag Stacking

LACP

(Como fazer?)

4- Marcar a porta Trunk como VID 400 "tagged"



Bridge VLAN <400>

Bridge: switch

VLAN IDs: 400

Tagged: sfp-sfpplus1-wan

Untagged:

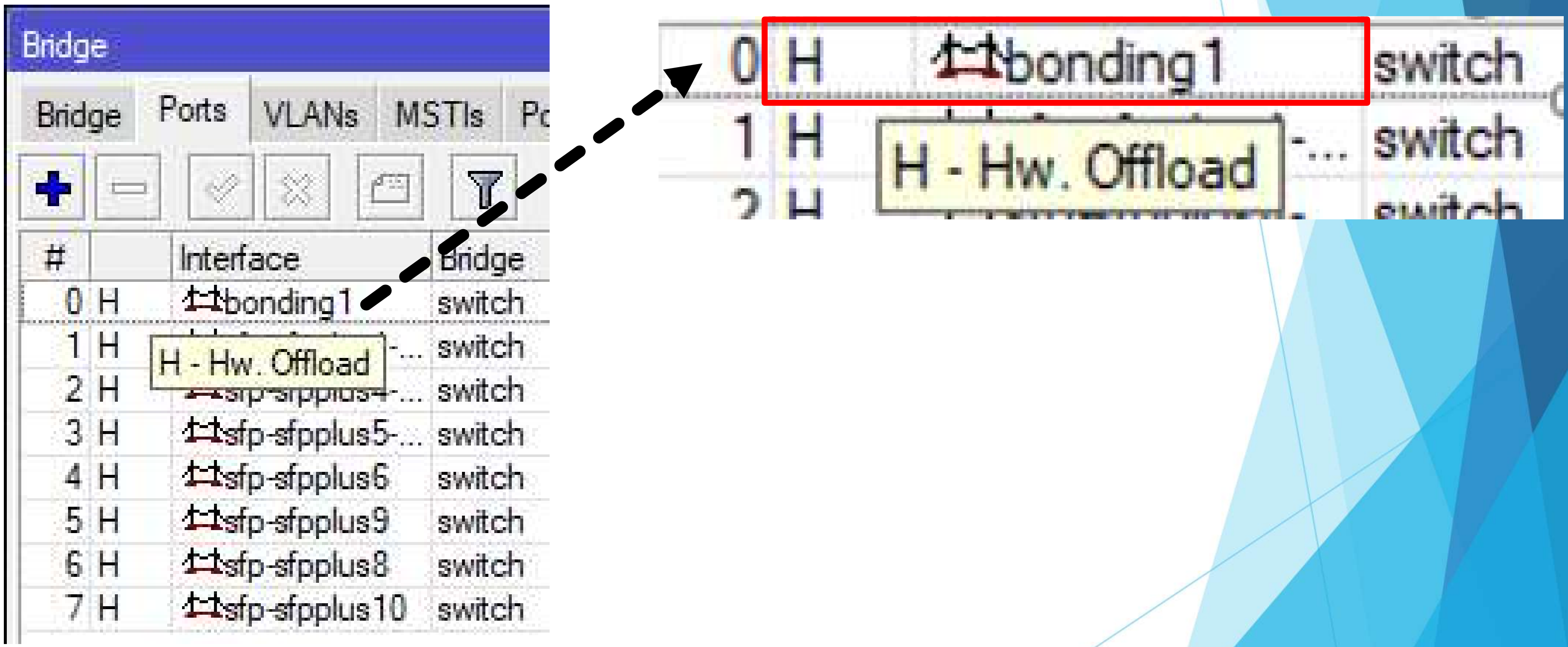
Current Tagged: sfp-sfpplus1-wan

Current Untagged: bonding1

enabled

LACP

(Resultado)



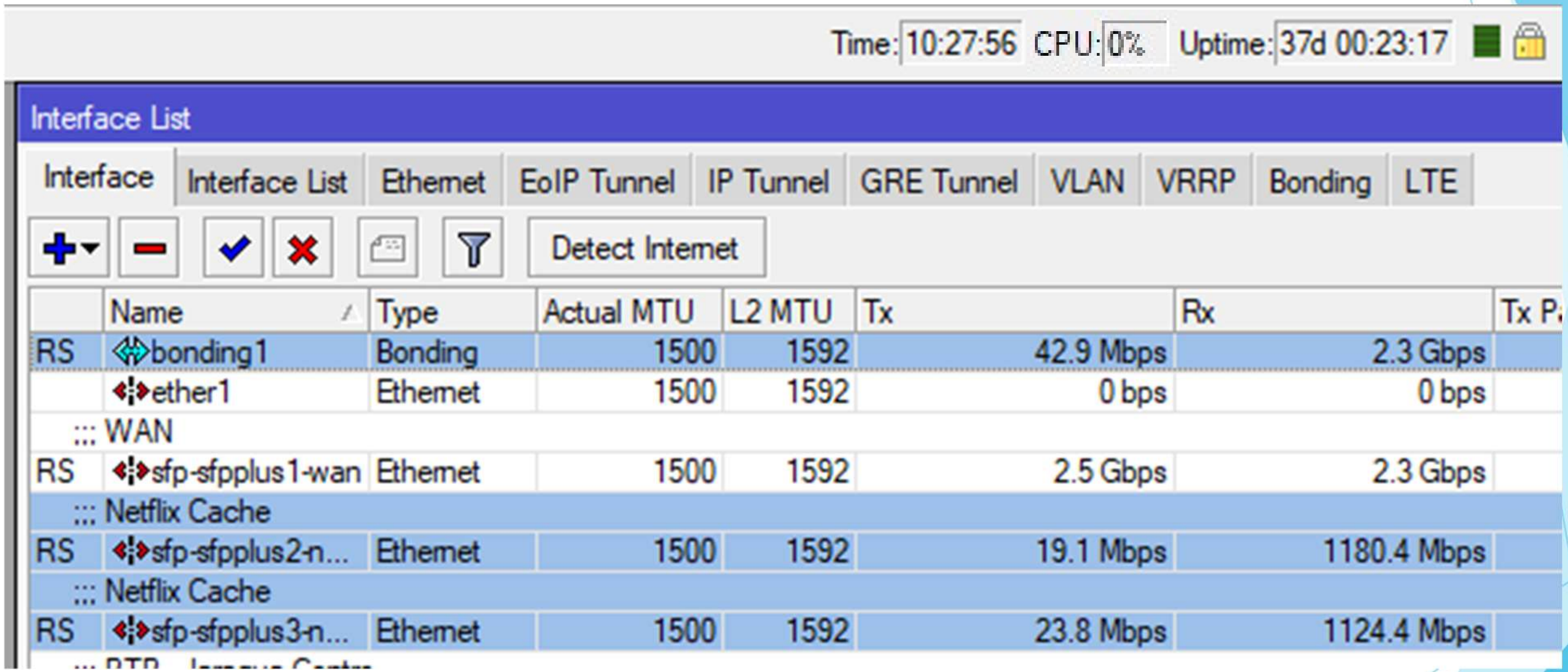
#		Interface	Bridge
0	H	bonding1	switch
1	H	-...	switch
2	H	sfp-sfpplus4-...	switch
3	H	sfp-sfpplus5-...	switch
4	H	sfp-sfpplus6	switch
5	H	sfp-sfpplus9	switch
6	H	sfp-sfpplus8	switch
7	H	sfp-sfpplus10	switch

0	H	bonding1	switch
1	H	-...	switch
2	H		switch

H - Hw. Offload

LACP

(Resultado)



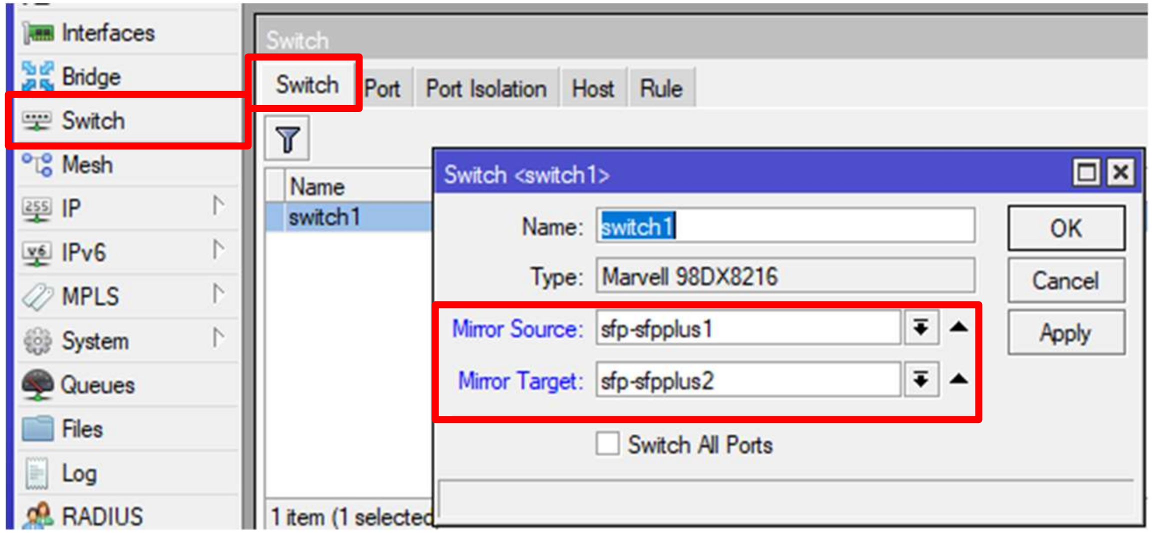
Time: 10:27:56 CPU: 0% Uptime: 37d 00:23:17

Interface List

	Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx P
RS	bonding1	Bonding	1500	1592	42.9 Mbps	2.3 Gbps	
	ether1	Ethernet	1500	1592	0 bps	0 bps	
	::: WAN						
RS	sfp-sfpplus1-wan	Ethernet	1500	1592	2.5 Gbps	2.3 Gbps	
	::: Netflix Cache						
RS	sfp-sfpplus2-n...	Ethernet	1500	1592	19.1 Mbps	1180.4 Mbps	
	::: Netflix Cache						
RS	sfp-sfpplus3-n...	Ethernet	1500	1592	23.8 Mbps	1124.4 Mbps	

Port Mirroring (espelhamento de portas)

- O Chip permite que haja o “espelhamento” de pacotes a uma determinada(s) porta/vlans/MACs;
- Útil para análises avançadas com algum packet sniffer (Ex: Wireshark)
- Interessante para analisar comportamentos de ataques.



Name: switch1

Type: Marvell 98DX8216

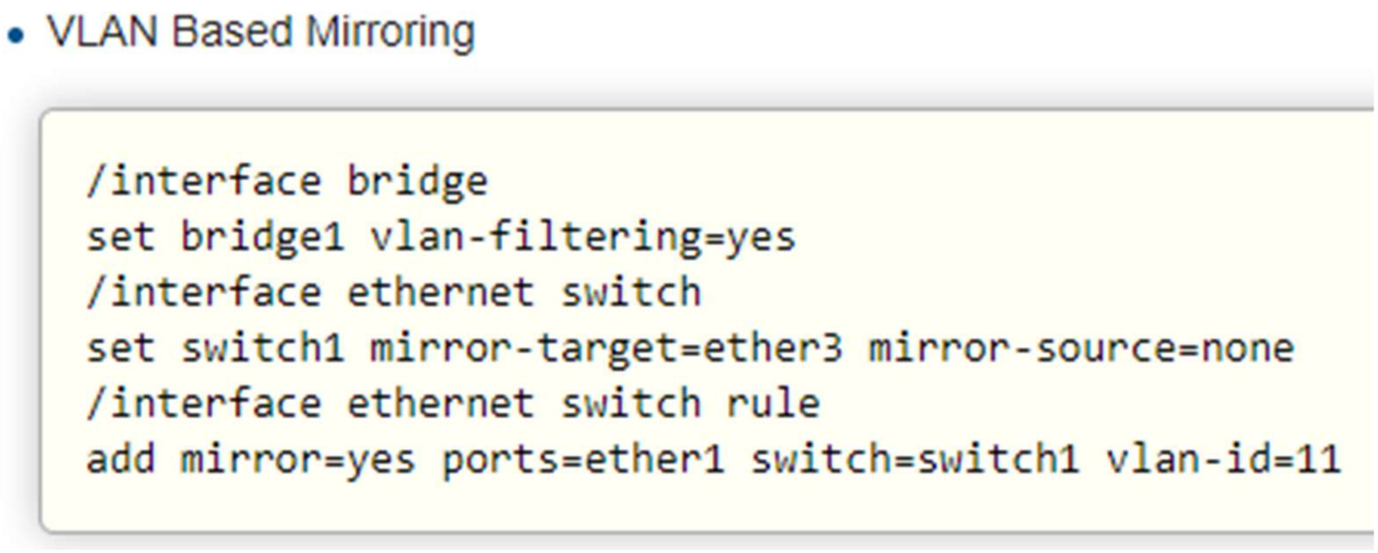
Mirror Source: sfp-sfpplus1

Mirror Target: sfp-sfpplus2

□ Switch All Ports

Port Mirroring (espelhamento de portas)

- Exemplo com base em VLANs

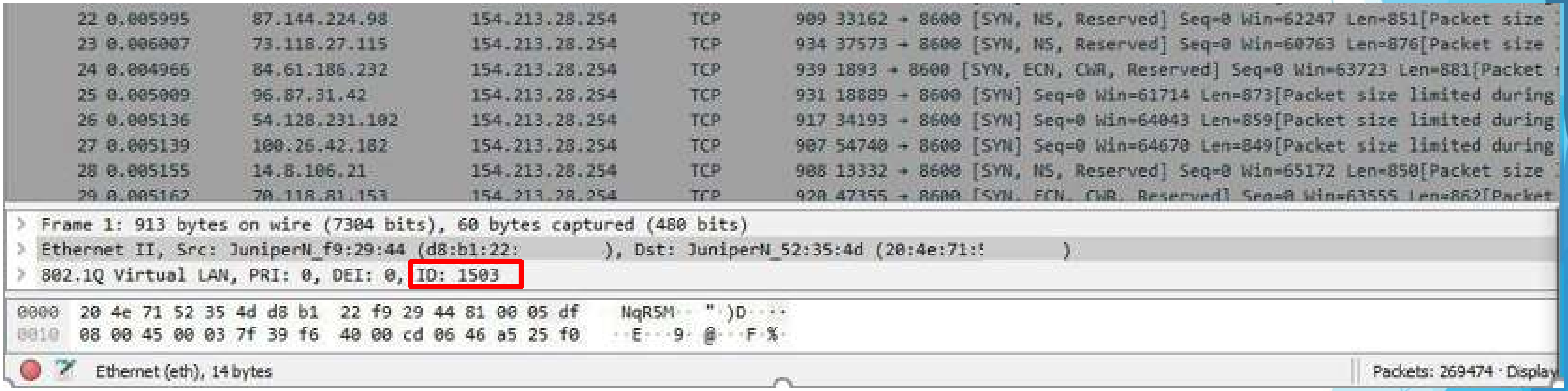


- VLAN Based Mirroring

```
/interface bridge
set bridge1 vlan-filtering=yes
/interface ethernet switch
set switch1 mirror-target=ether3 mirror-source=none
/interface ethernet switch rule
add mirror=yes ports=ether1 switch=switch1 vlan-id=11
```

Mais em: https://wiki.mikrotik.com/wiki/Manual:CRS3xx_series_switches#Mirroring

Port Mirroring (exemplo real de analise)



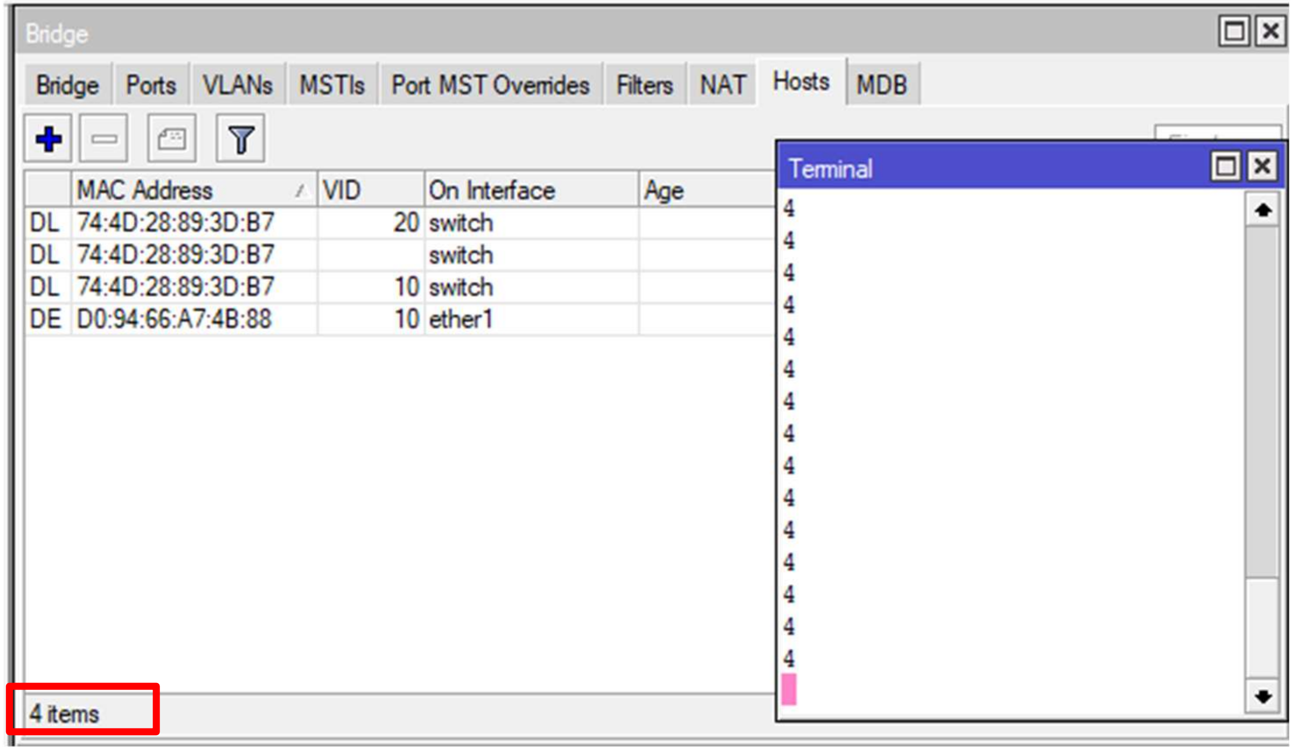
```
    22 0.005995      87.144.224.98       154.213.28.254       TCP      909 33162 → 8600 [SYN, NS, Reserved] Seq=0 Win=62247 Len=851[Packet size
    23 0.006007      73.118.27.115       154.213.28.254       TCP      934 37573 → 8600 [SYN, NS, Reserved] Seq=0 Win=60763 Len=876[Packet size
    24 0.004966      84.61.186.232       154.213.28.254       TCP      939 1893 → 8600 [SYN, ECN, CWR, Reserved] Seq=0 Win=63723 Len=881[Packet
    25 0.005009      96.87.31.42         154.213.28.254       TCP      931 18889 → 8600 [SYN] Seq=0 Win=61714 Len=873[Packet size limited during
    26 0.005136      54.128.231.102      154.213.28.254       TCP      917 34193 → 8600 [SYN] Seq=0 Win=64043 Len=859[Packet size limited during
    27 0.005139      100.26.42.182       154.213.28.254       TCP      907 54740 → 8600 [SYN] Seq=0 Win=64670 Len=849[Packet size limited during
    28 0.005155      14.8.106.21         154.213.28.254       TCP      908 13332 → 8600 [SYN, NS, Reserved] Seq=0 Win=65172 Len=850[Packet size
    29 0.005162      70.118.81.153       154.213.28.254       TCP      920 47355 → 8600 [SYN, ECN, CWR, Reserved] Seq=0 Win=63555 Len=862[Packet

> Frame 1: 913 bytes on wire (7304 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: JuniperN_f9:29:44 (d8:b1:22:        ), Dst: JuniperN_52:35:4d (20:4e:71:        )
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1503

0000  20 4e 71 52 35 4d d8 b1  22 f9 29 44 81 00 05 df    NqR5M·· "·)D····
0010  08 00 45 00 03 7f 39 f6  40 00 cd 06 46 a5 25 f0   ··E···9· @···F·%·

Ethernet (eth), 14 bytes                                                                  Packets: 269474 · Display
```

Mac Flooding
(antes de um ataque)

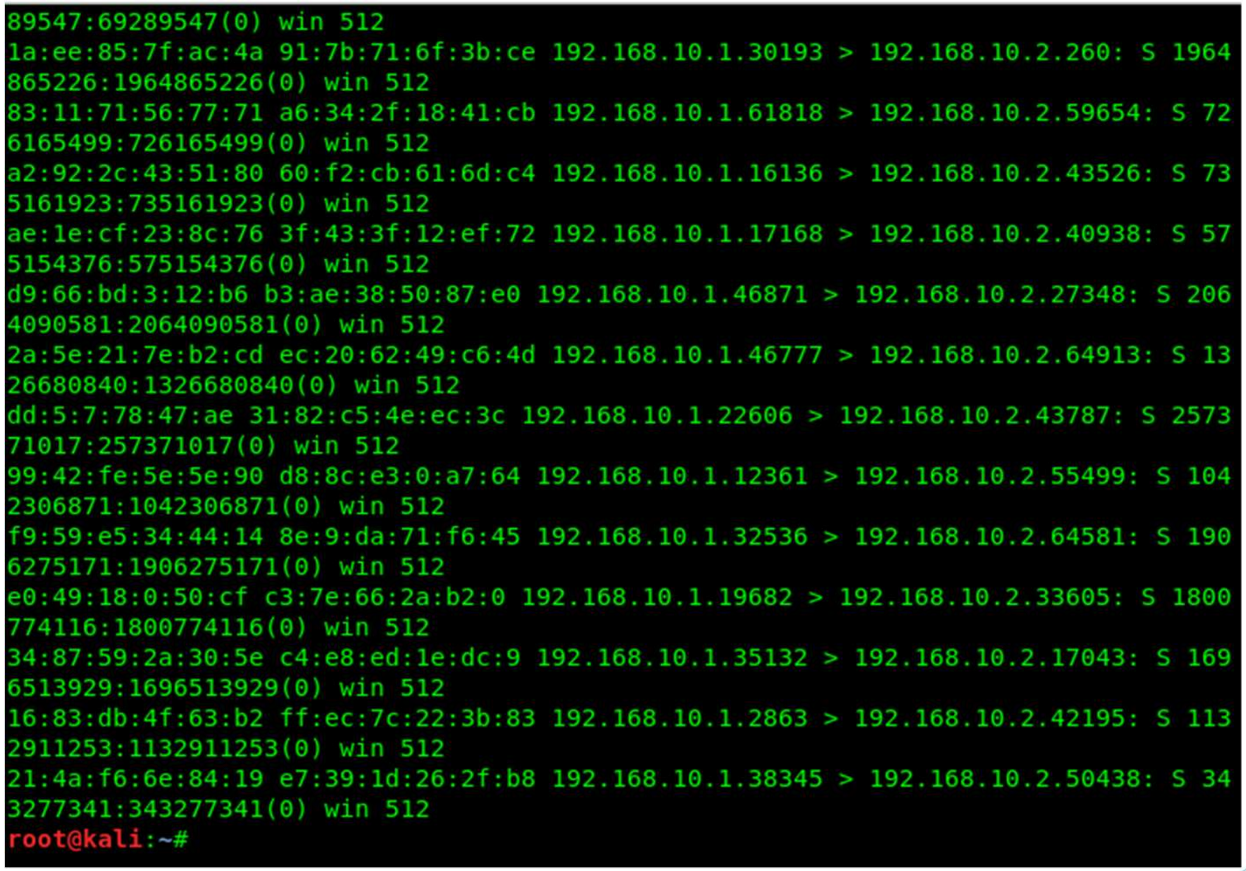


	MAC Address	VID	On Interface	Age
DL	74:4D:28:89:3D:B7	20	switch	
DL	74:4D:28:89:3D:B7		switch	
DL	74:4D:28:89:3D:B7	10	switch	
DE	D0:94:66:A7:4B:88	10	ether1	

4 items

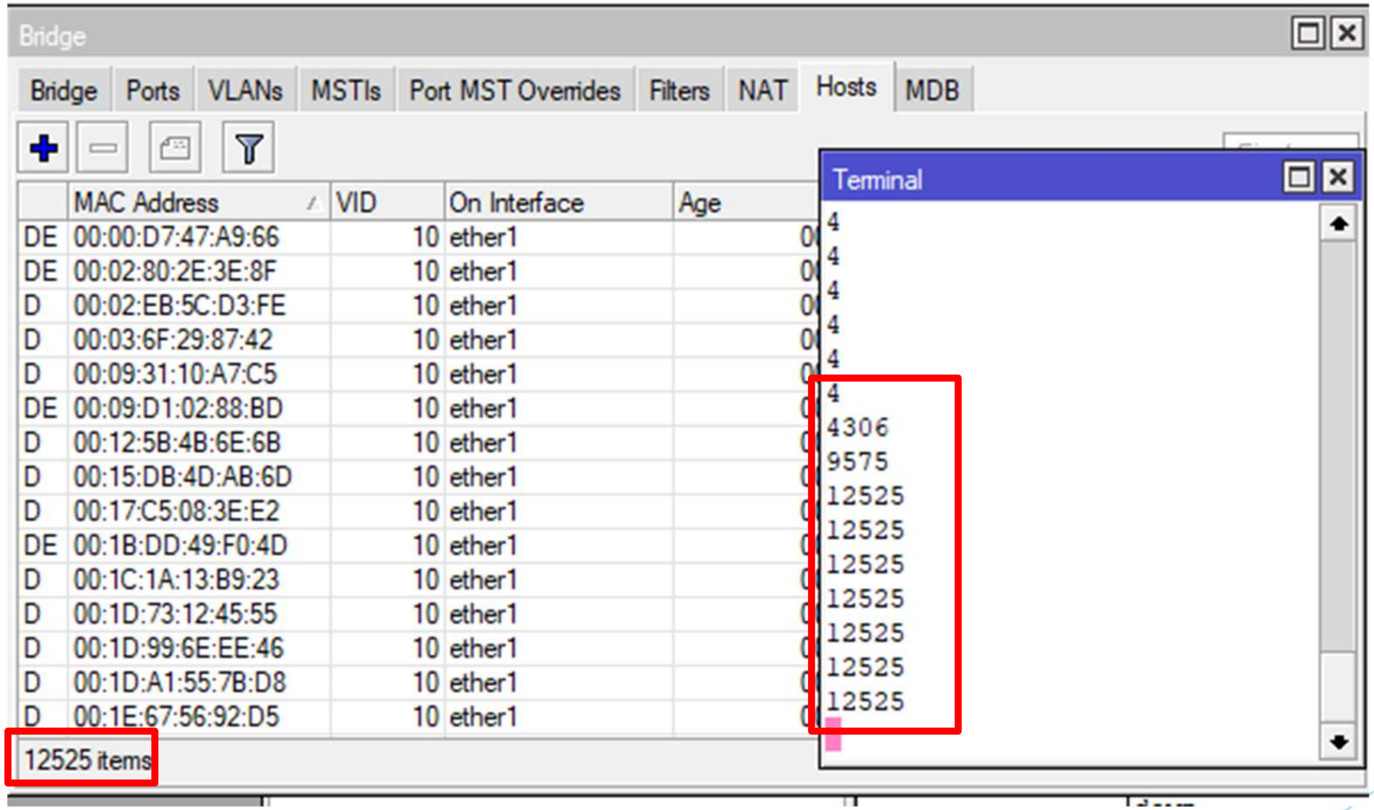
```
4
4
4
4
4
4
4
4
4
4
4
4
4
4
4
```

Mac Flooding (durante um ataque)



```
89547:69289547(0) win 512
1a:ee:85:7f:ac:4a 91:7b:71:6f:3b:ce 192.168.10.1.30193 > 192.168.10.2.260: S 1964
865226:1964865226(0) win 512
83:11:71:56:77:71 a6:34:2f:18:41:cb 192.168.10.1.61818 > 192.168.10.2.59654: S 72
6165499:726165499(0) win 512
a2:92:2c:43:51:80 60:f2:cb:61:6d:c4 192.168.10.1.16136 > 192.168.10.2.43526: S 73
5161923:735161923(0) win 512
ae:1e:cf:23:8c:76 3f:43:3f:12:ef:72 192.168.10.1.17168 > 192.168.10.2.40938: S 57
5154376:575154376(0) win 512
d9:66:bd:3:12:b6 b3:ae:38:50:87:e0 192.168.10.1.46871 > 192.168.10.2.27348: S 206
4090581:2064090581(0) win 512
2a:5e:21:7e:b2:cd ec:20:62:49:c6:4d 192.168.10.1.46777 > 192.168.10.2.64913: S 13
26680840:1326680840(0) win 512
dd:5:7:78:47:ae 31:82:c5:4e:ec:3c 192.168.10.1.22606 > 192.168.10.2.43787: S 2573
71017:257371017(0) win 512
99:42:fe:5e:5e:90 d8:8c:e3:0:a7:64 192.168.10.1.12361 > 192.168.10.2.55499: S 104
2306871:1042306871(0) win 512
f9:59:e5:34:44:14 8e:9:da:71:f6:45 192.168.10.1.32536 > 192.168.10.2.64581: S 190
6275171:1906275171(0) win 512
e0:49:18:0:50:cf c3:7e:66:2a:b2:0 192.168.10.1.19682 > 192.168.10.2.33605: S 1800
774116:1800774116(0) win 512
34:87:59:2a:30:5e c4:e8:ed:1e:dc:9 192.168.10.1.35132 > 192.168.10.2.17043: S 169
6513929:1696513929(0) win 512
16:83:db:4f:63:b2 ff:ec:7c:22:3b:83 192.168.10.1.2863 > 192.168.10.2.42195: S 113
2911253:1132911253(0) win 512
21:4a:f6:6e:84:19 e7:39:1d:26:2f:b8 192.168.10.1.38345 > 192.168.10.2.50438: S 34
3277341:343277341(0) win 512
root@kali:~#
```

Mac Flooding (durante um ataque)

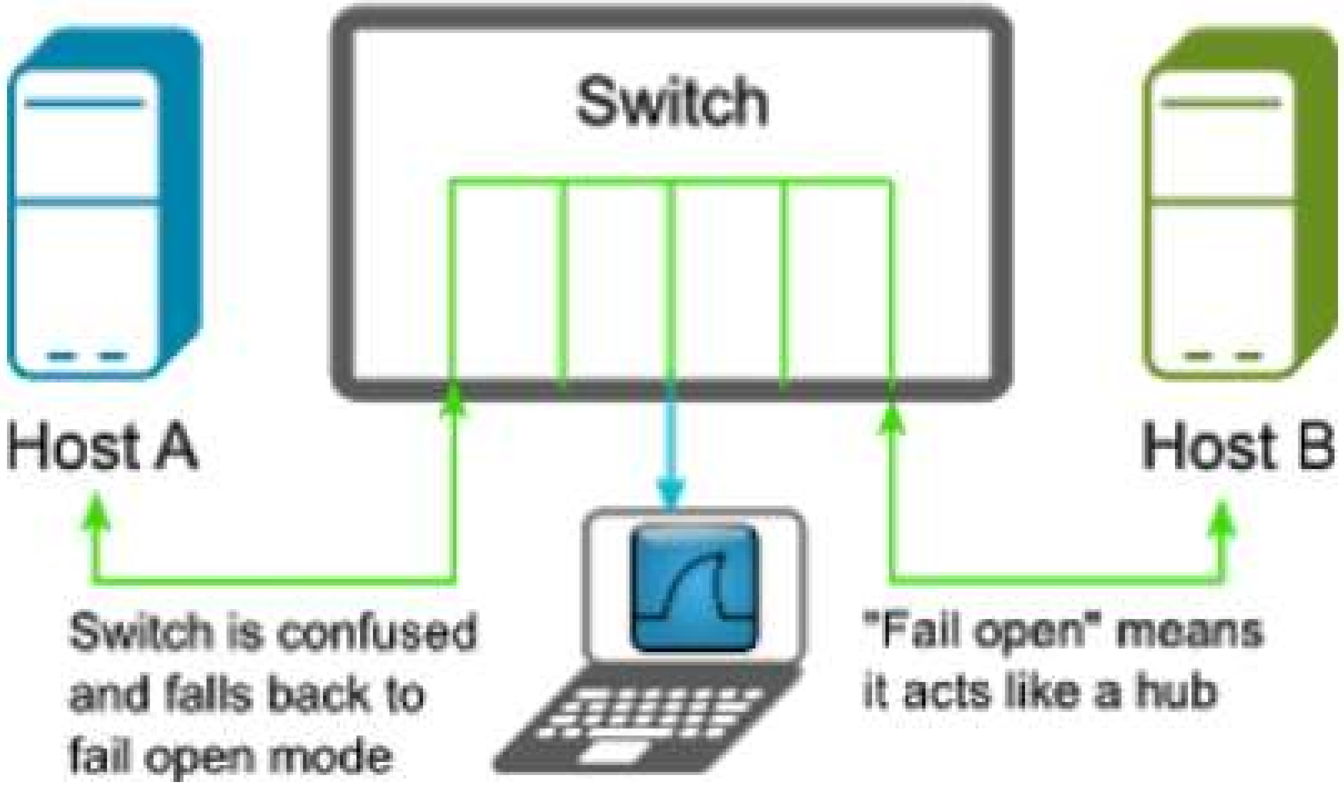


	MAC Address	VID	On Interface	Age
DE	00:00:D7:47:A9:66	10	ether1	0
DE	00:02:80:2E:3E:8F	10	ether1	0
D	00:02:EB:5C:D3:FE	10	ether1	0
D	00:03:6F:29:87:42	10	ether1	0
D	00:09:31:10:A7:C5	10	ether1	0
DE	00:09:D1:02:88:BD	10	ether1	0
D	00:12:5B:4B:6E:6B	10	ether1	0
D	00:15:DB:4D:AB:6D	10	ether1	0
D	00:17:C5:08:3E:E2	10	ether1	0
DE	00:1B:DD:49:F0:4D	10	ether1	0
D	00:1C:1A:13:B9:23	10	ether1	0
D	00:1D:73:12:45:55	10	ether1	0
D	00:1D:99:6E:EE:46	10	ether1	0
D	00:1D:A1:55:7B:D8	10	ether1	0
D	00:1E:67:56:92:D5	10	ether1	0

12525 items

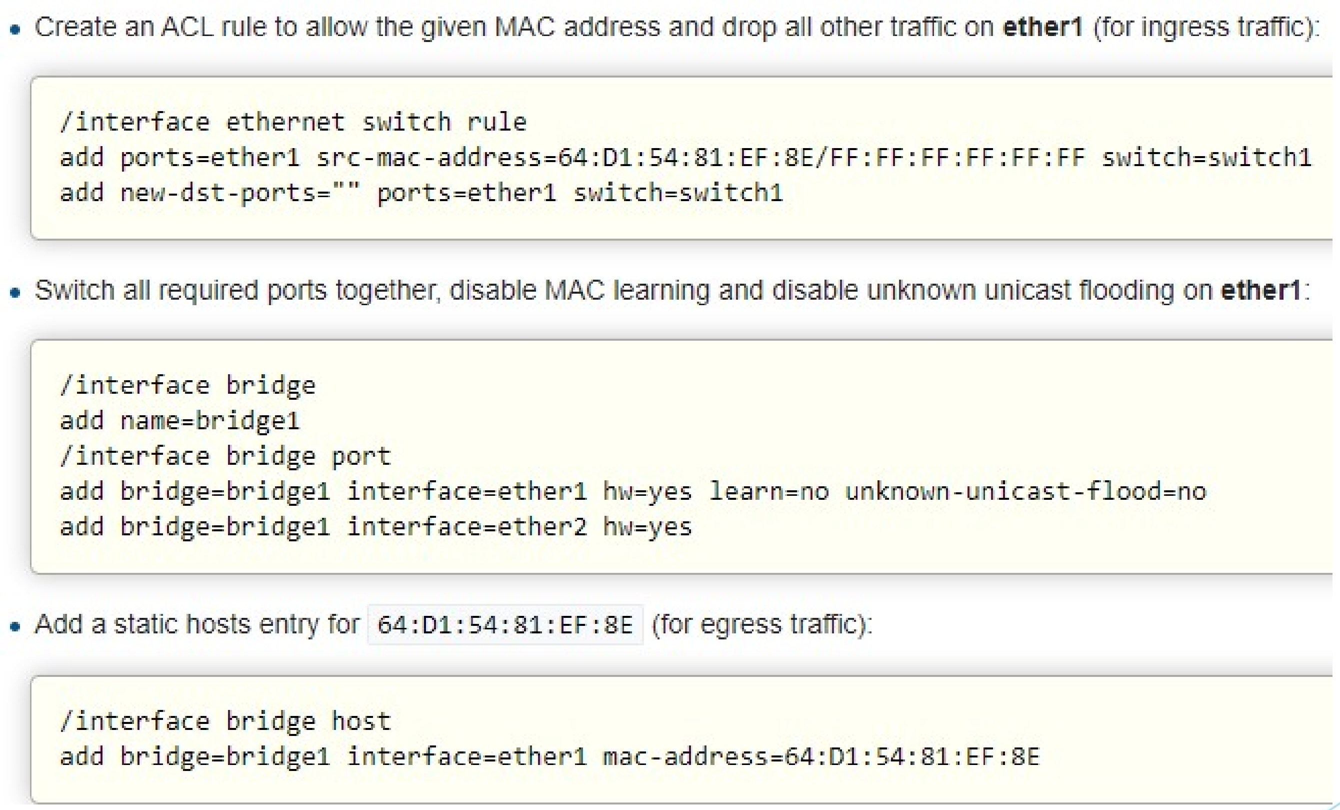
```
4
4
4
4
4
4
4306
9575
12525
12525
12525
12525
12525
12525
12525
```

Mac Flooding (após um ataque)


Switch
Host A
Host B
Switch is confused and falls back to fail open mode
"Fail open" means it acts like a hub

https://rumyittips.com/cam-flow-attack-on-switch-network/

Mac Flooding (alternativa)



- Create an ACL rule to allow the given MAC address and drop all other traffic on **ether1** (for ingress traffic):

```
/interface ethernet switch rule
add ports=ether1 src-mac-address=64:D1:54:81:EF:8E/FF:FF:FF:FF:FF:FF switch=switch1
add new-dst-ports="" ports=ether1 switch=switch1
```

- Switch all required ports together, disable MAC learning and disable unknown unicast flooding on **ether1**:

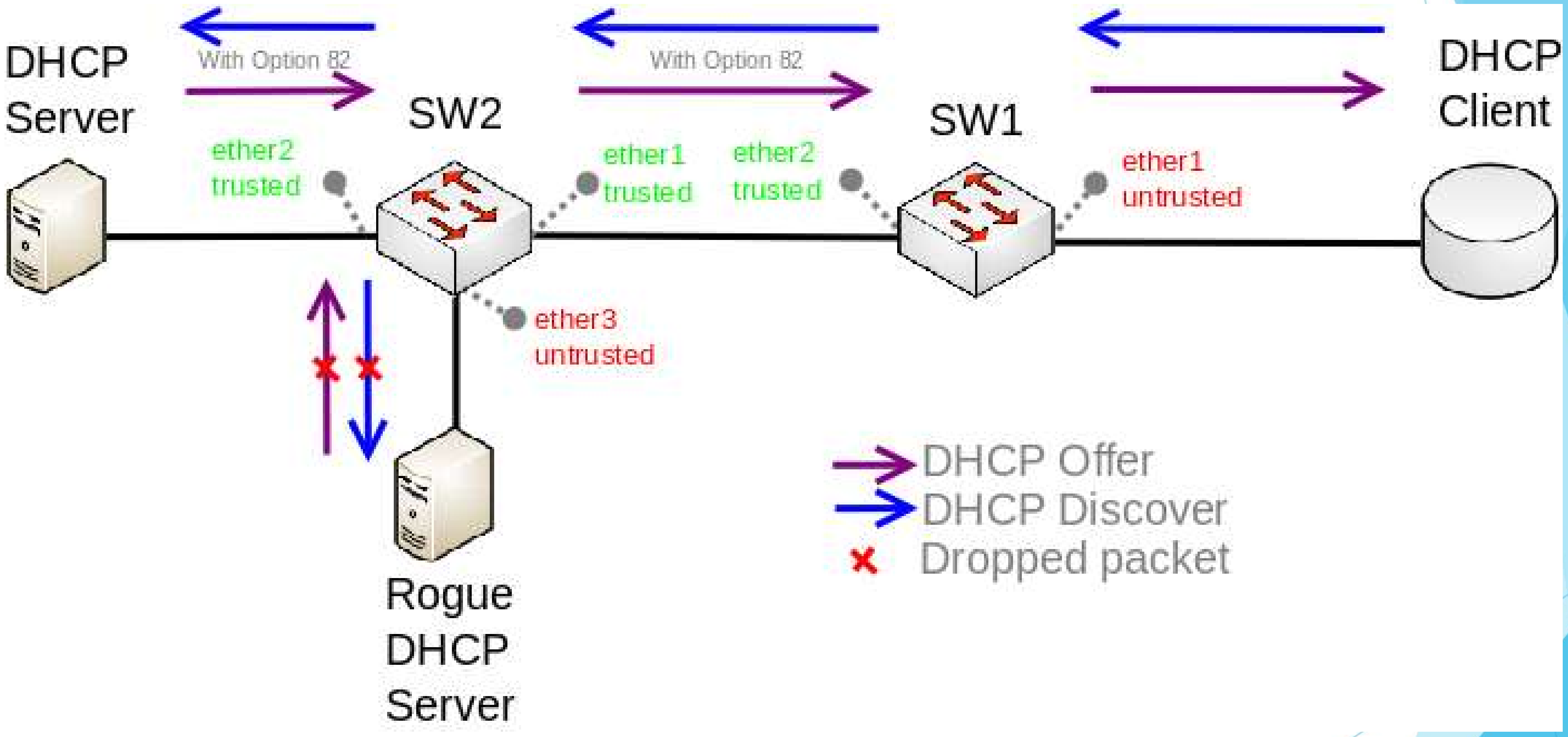
```
/interface bridge
add name=bridge1
/interface bridge port
add bridge=bridge1 interface=ether1 hw=yes learn=no unknown-unicast-flood=no
add bridge=bridge1 interface=ether2 hw=yes
```

- Add a static hosts entry for `64:D1:54:81:EF:8E` (for egress traffic):

```
/interface bridge host
add bridge=bridge1 interface=ether1 mac-address=64:D1:54:81:EF:8E
```

Mais em: https://wiki.mikrotik.com/wiki/Manual:CRS3xx_series_switches#Port_Security

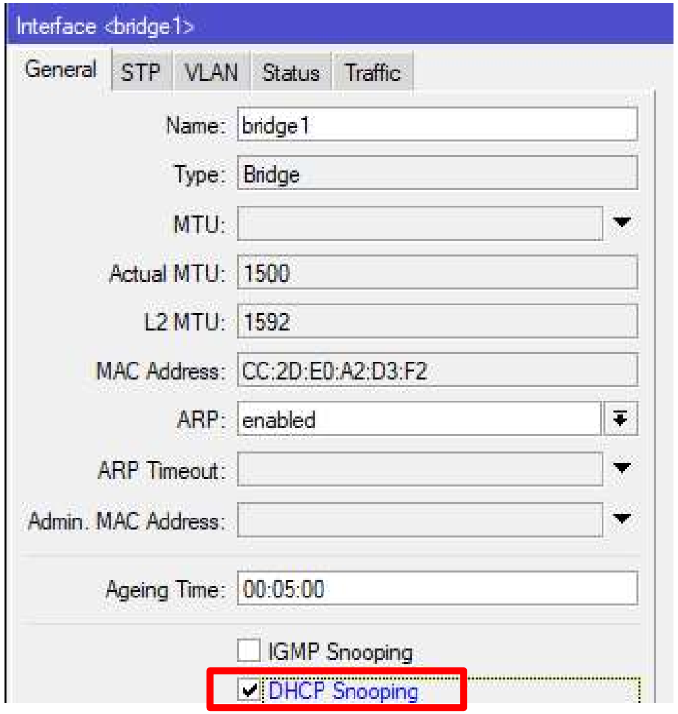
DHCP Snooping



Fonte: https://wiki.mikrotik.com/wiki/File:Dhcp_snooping.png

DHCP Snooping

1- Habilitar a opção na Bridge

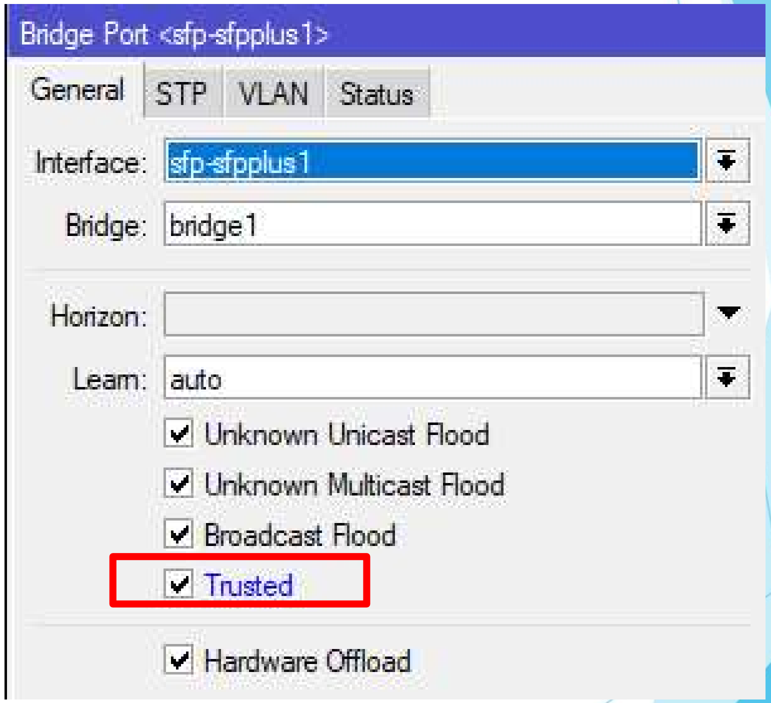


Interface <bridge1>

Name: bridge1
Type: Bridge
MTU:
Actual MTU: 1500
L2 MTU: 1592
MAC Address: CC:2D:E0:A2:D3:F2
ARP: enabled
ARP Timeout:
Admin. MAC Address:
Ageing Time: 00:05:00

☐ IGMP Snooping
☑ DHCP Snooping

2- Marcar as portas que são confiáveis



Bridge Port <sfp-sfpplus1>

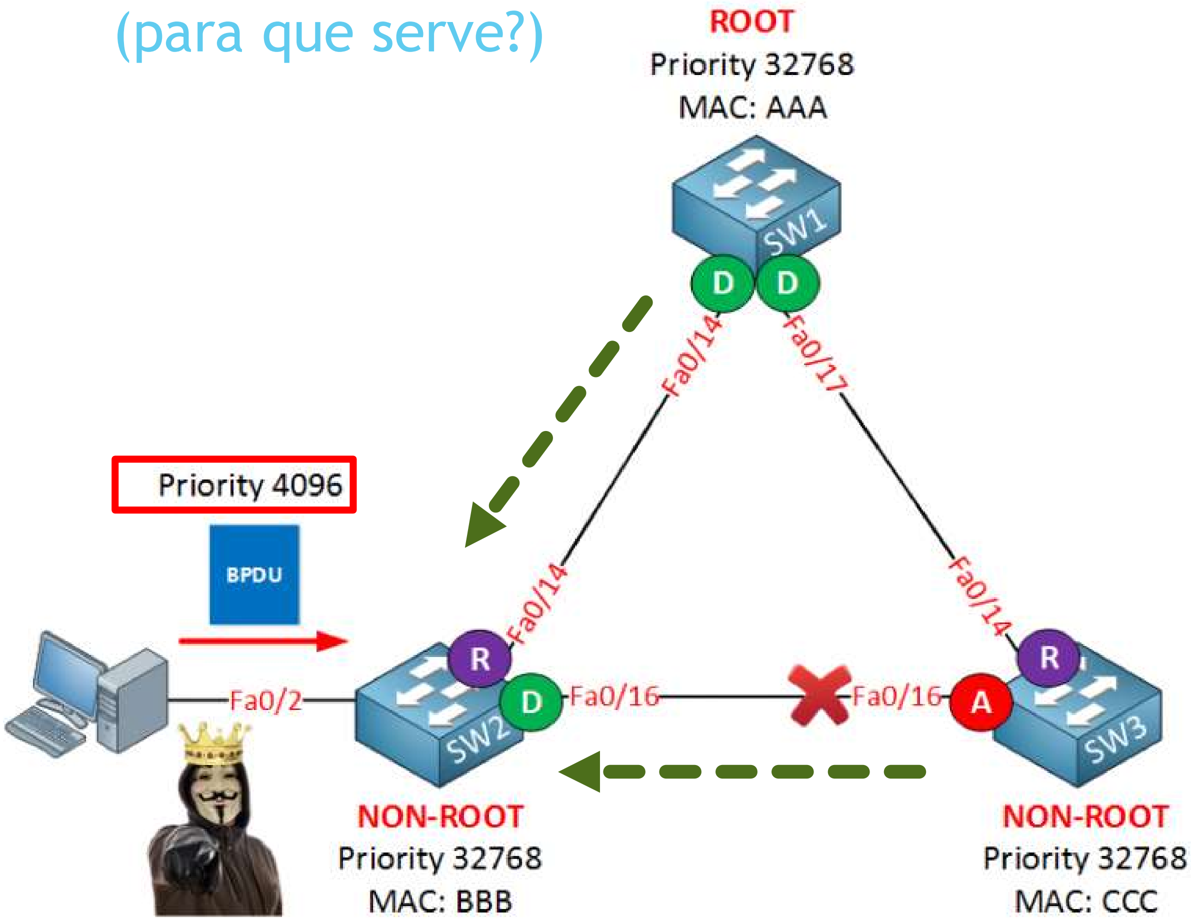
Interface: sfp-sfpplus1
Bridge: bridge1
Horizon:
Learn: auto

☑ Unknown Unicast Flood
☑ Unknown Multicast Flood
☑ Broadcast Flood
☑ Trusted
☑ Hardware Offload

MikroTik

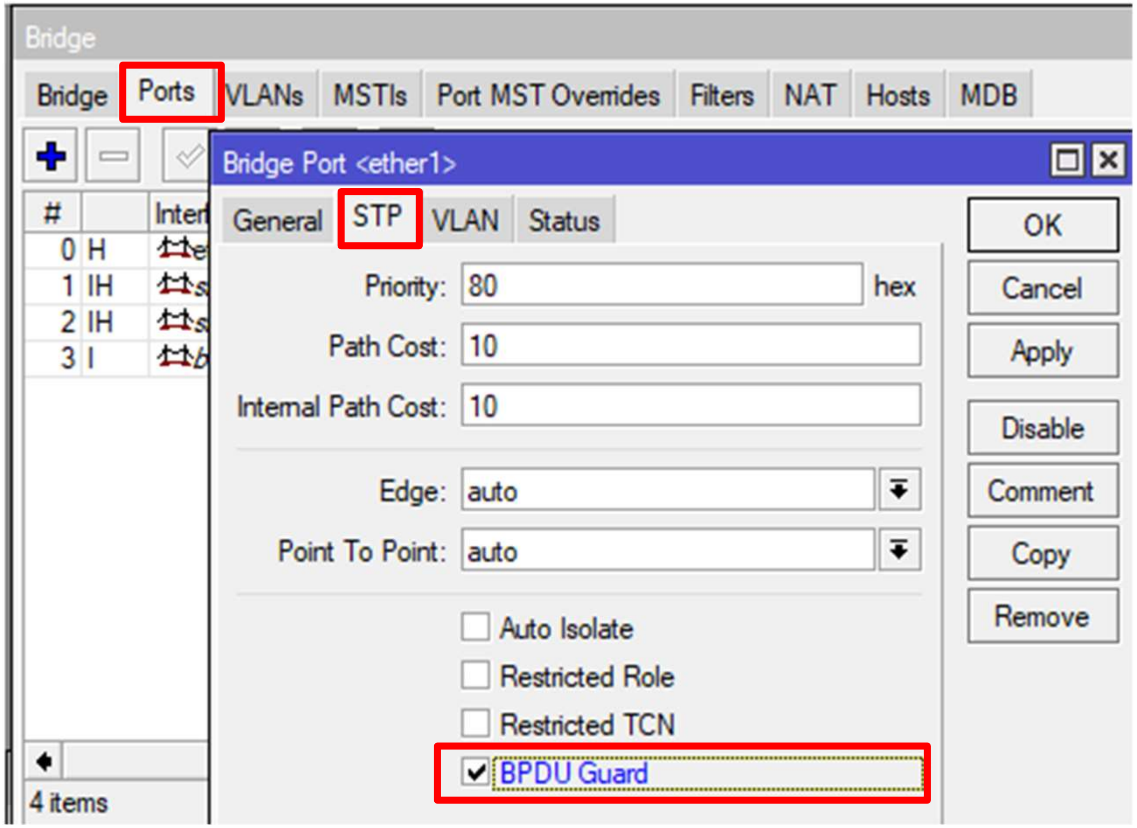
BPDU Guard

(para que serve?)



Fonte: https://networklessons.com/cisco/ccie-routing-switching-written/spanning-tree-bpduguard

BPDU Guard



Priority: 80 hex

Path Cost: 10

Internal Path Cost: 10

Edge: auto

Point To Point: auto

□ Auto Isolate

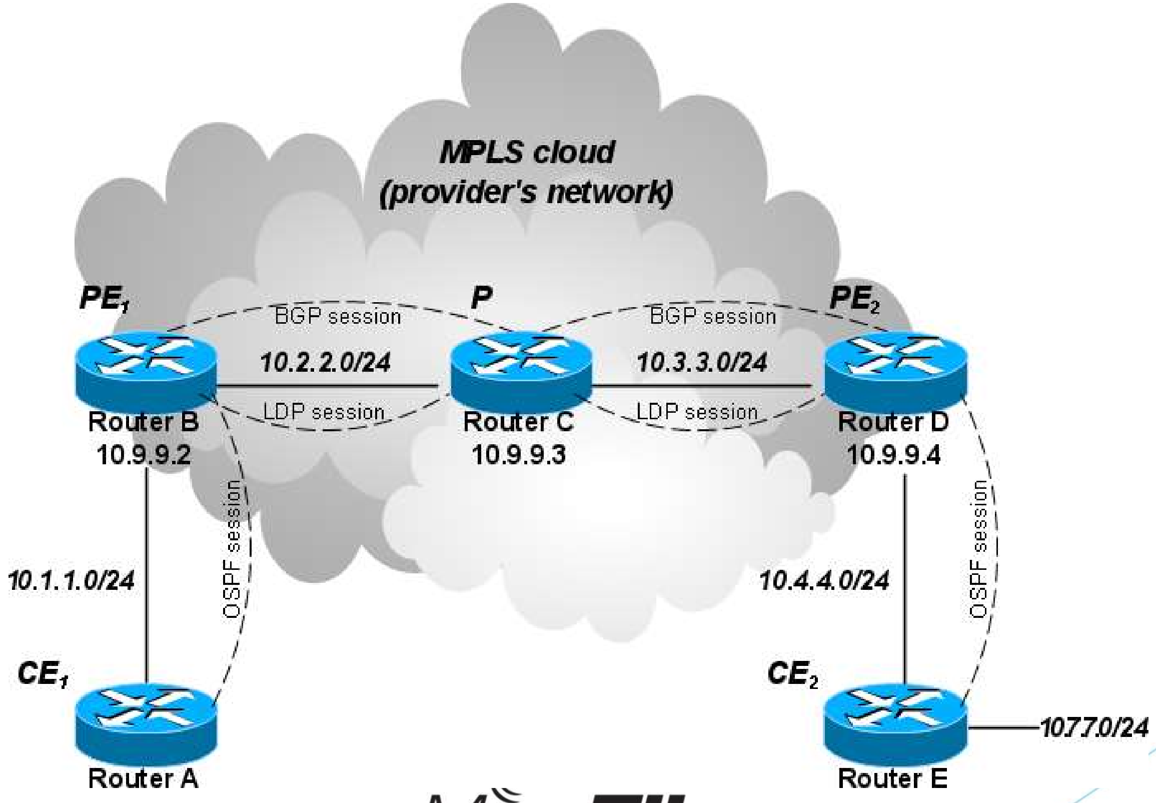
□ Restricted Role

□ Restricted TCN

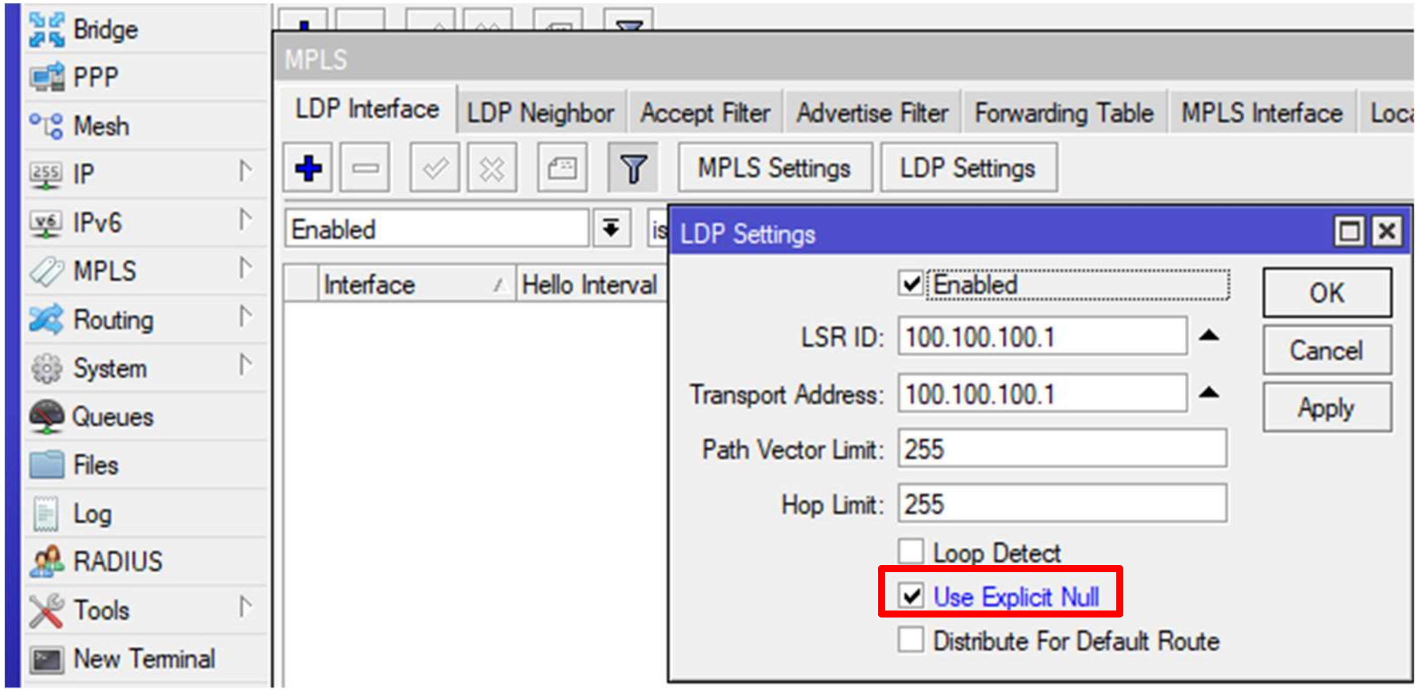
☑ BPDU Guard

MPLS Hardware Offload

- Em uma nuvem MPLS, é necessário que o Switch Comute os Labels;
- Não se aplica ao processo de POP/PHP;
- Necessário ser um “P”, se caso antecipar um destino é necessário ter “Explicit Null”;



MPLS Hardware Offload



LDP Settings

☑ Enabled

LSR ID: 100.100.100.1

Transport Address: 100.100.100.1

Path Vector Limit: 255

Hop Limit: 255

□ Loop Detect

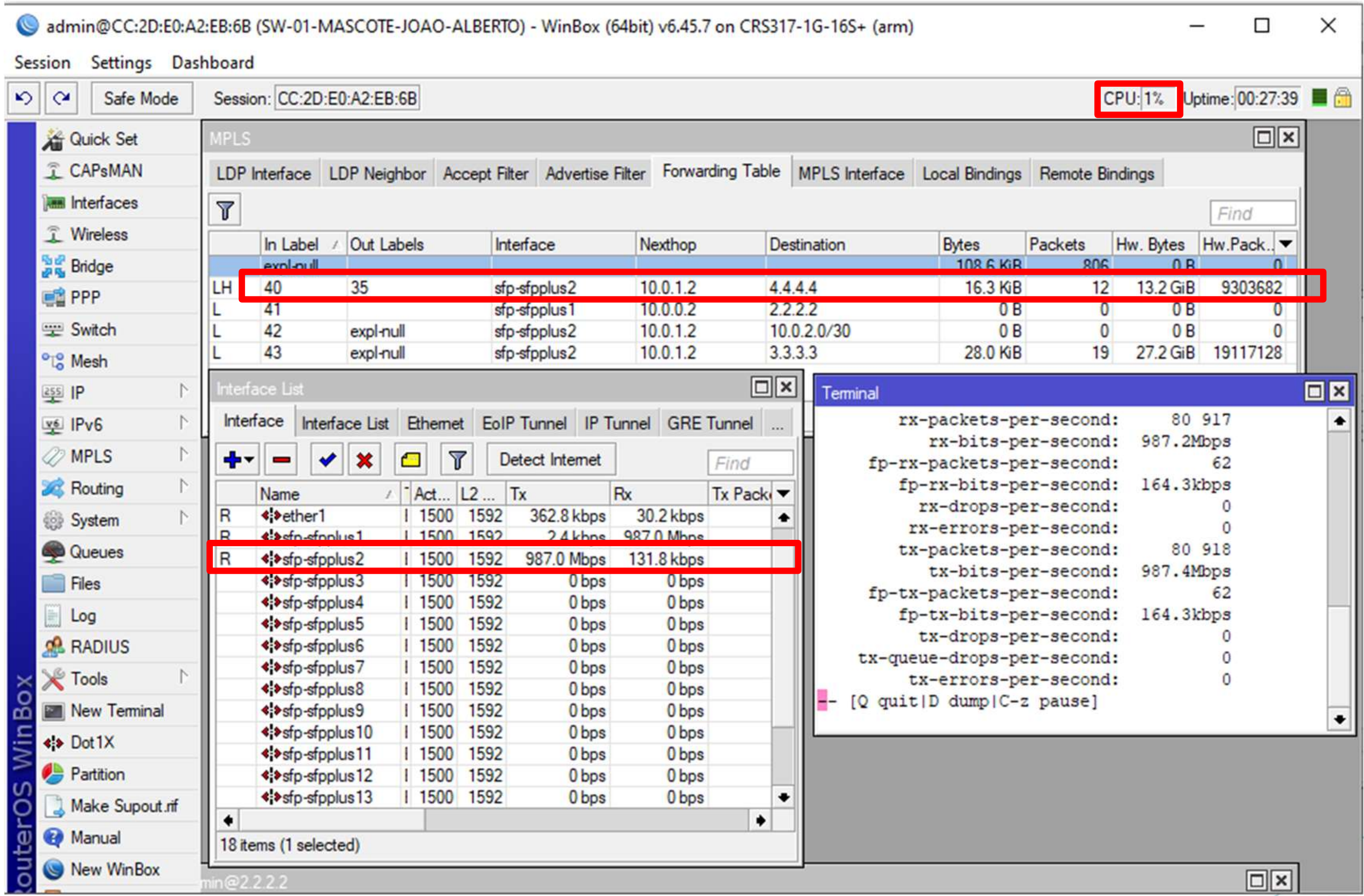
☑ Use Explicit Null

□ Distribute For Default Route

⚠ Atualmente este Recurso funciona apenas para as Routerboards:

CRS317-1G-16S+RM e CRS309-1G-8S+IN

MPLS Hardware Offload



admin@CC:2D:E0:A2:EB:6B (SW-01-MASCOTE-JOAO-ALBERTO) - WinBox (64bit) v6.45.7 on CRS317-1G-16S+ (arm)

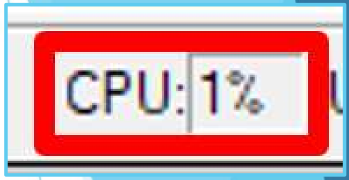
Session: CC:2D:E0:A2:EB:6B CPU: 1% Uptime: 00:27:39

	In Label	Out Labels	Interface	Nexthop	Destination	Bytes	Packets	Hw. Bytes	Hw.Pack..
	expl-null					108.6 KiB	806	0 B	0
LH	40	35	sfp-sfpplus2	10.0.1.2	4.4.4.4	16.3 KiB	12	13.2 GiB	9303682
L	41		sfp-sfpplus1	10.0.0.2	2.2.2.2	0 B	0	0 B	0
L	42	expl-null	sfp-sfpplus2	10.0.1.2	10.0.2.0/30	0 B	0	0 B	0
L	43	expl-null	sfp-sfpplus2	10.0.1.2	3.3.3.3	28.0 KiB	19	27.2 GiB	19117128

	Name		Act...	L2 ...	Tx	Rx	Tx Pack
R	ether1		1500	1592	362.8 kbps	30.2 kbps	
R	sfp-sfpplus1		1500	1592	2.4 kbps	987.0 Mbps	
R	sfp-sfpplus2		1500	1592	987.0 Mbps	131.8 kbps	
	sfp-sfpplus3		1500	1592	0 bps	0 bps	
	sfp-sfpplus4		1500	1592	0 bps	0 bps	
	sfp-sfpplus5		1500	1592	0 bps	0 bps	
	sfp-sfpplus6		1500	1592	0 bps	0 bps	
	sfp-sfpplus7		1500	1592	0 bps	0 bps	
	sfp-sfpplus8		1500	1592	0 bps	0 bps	
	sfp-sfpplus9		1500	1592	0 bps	0 bps	
	sfp-sfpplus10		1500	1592	0 bps	0 bps	
	sfp-sfpplus11		1500	1592	0 bps	0 bps	
	sfp-sfpplus12		1500	1592	0 bps	0 bps	
	sfp-sfpplus13		1500	1592	0 bps	0 bps	

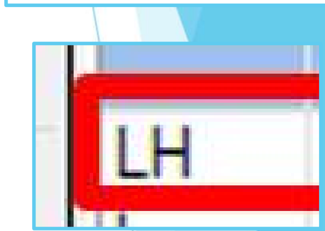
18 items (1 selected)

```
        rx-packets-per-second:      80 917
           rx-bits-per-second:   987.2Mbps
     fp-rx-packets-per-second:          62
        fp-rx-bits-per-second:   164.3kbps
          rx-drops-per-second:           0
         rx-errors-per-second:           0
        tx-packets-per-second:      80 918
           tx-bits-per-second:   987.4Mbps
     fp-tx-packets-per-second:          62
        fp-tx-bits-per-second:   164.3kbps
          tx-drops-per-second:           0
    tx-queue-drops-per-second:           0
         tx-errors-per-second:           0
-- [Q quit|D dump|C-z pause]
```

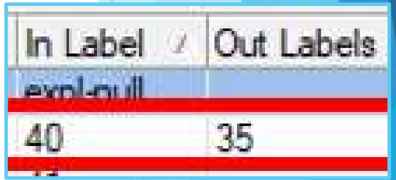


CPU: 1%

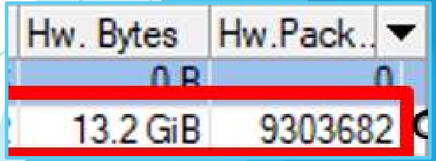
987.2Mbps



LH

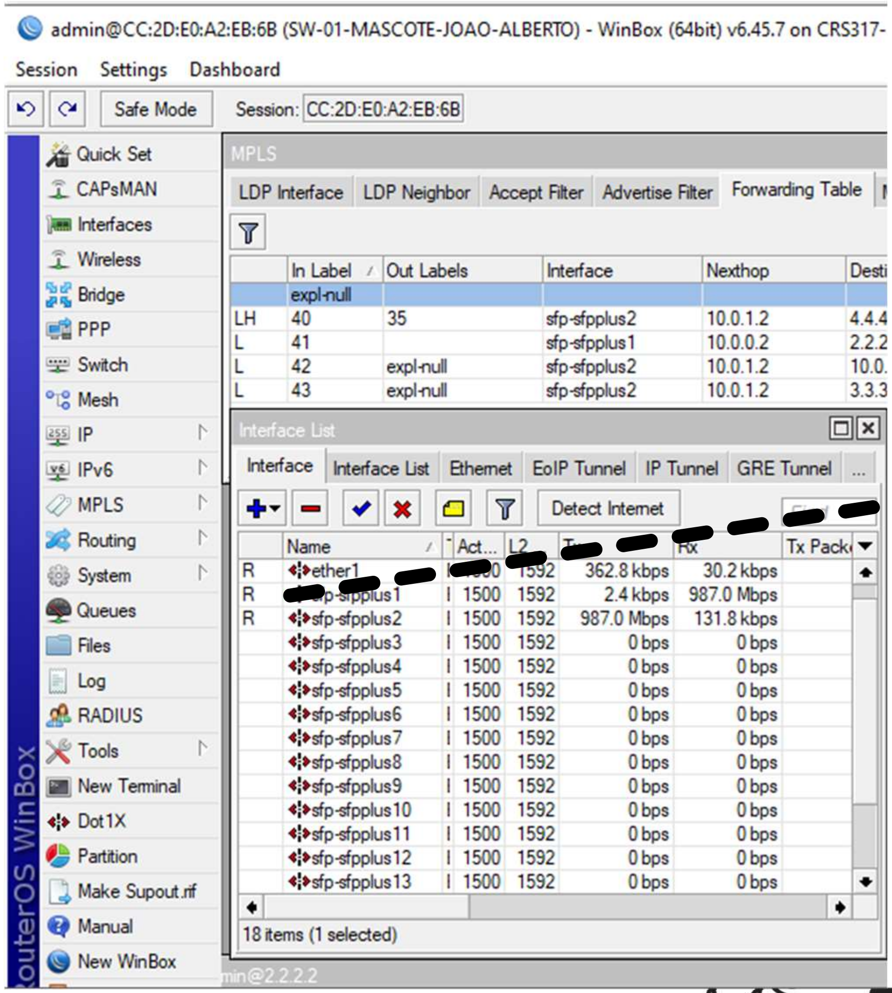


In Label	Out Labels
expl-null	
40	35



Hw. Bytes	Hw.Pack..
0 B	0
13.2 GiB	9303682

MPLS Hardware Offload

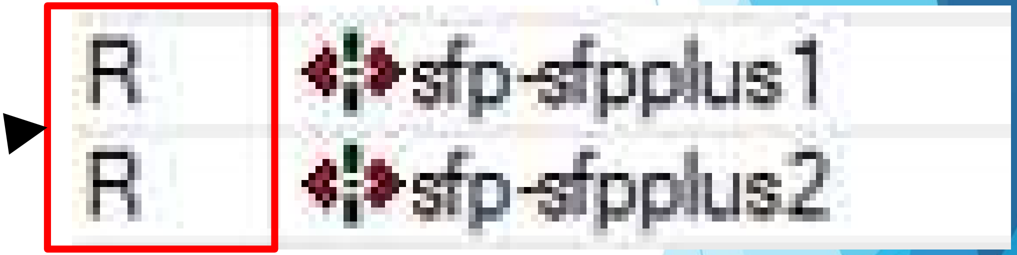


admin@CC:2D:E0:A2:EB:6B (SW-01-MASCOTE-JOAO-ALBERTO) - WinBox (64bit) v6.45.7 on CRS317-

	In Label	Out Labels	Interface	Nexthop	Desti
	expl-null				
LH	40	35	sfp-sfpplus2	10.0.1.2	4.4.4
L	41		sfp-sfpplus1	10.0.0.2	2.2.2
L	42	expl-null	sfp-sfpplus2	10.0.1.2	10.0.
L	43	expl-null	sfp-sfpplus2	10.0.1.2	3.3.3

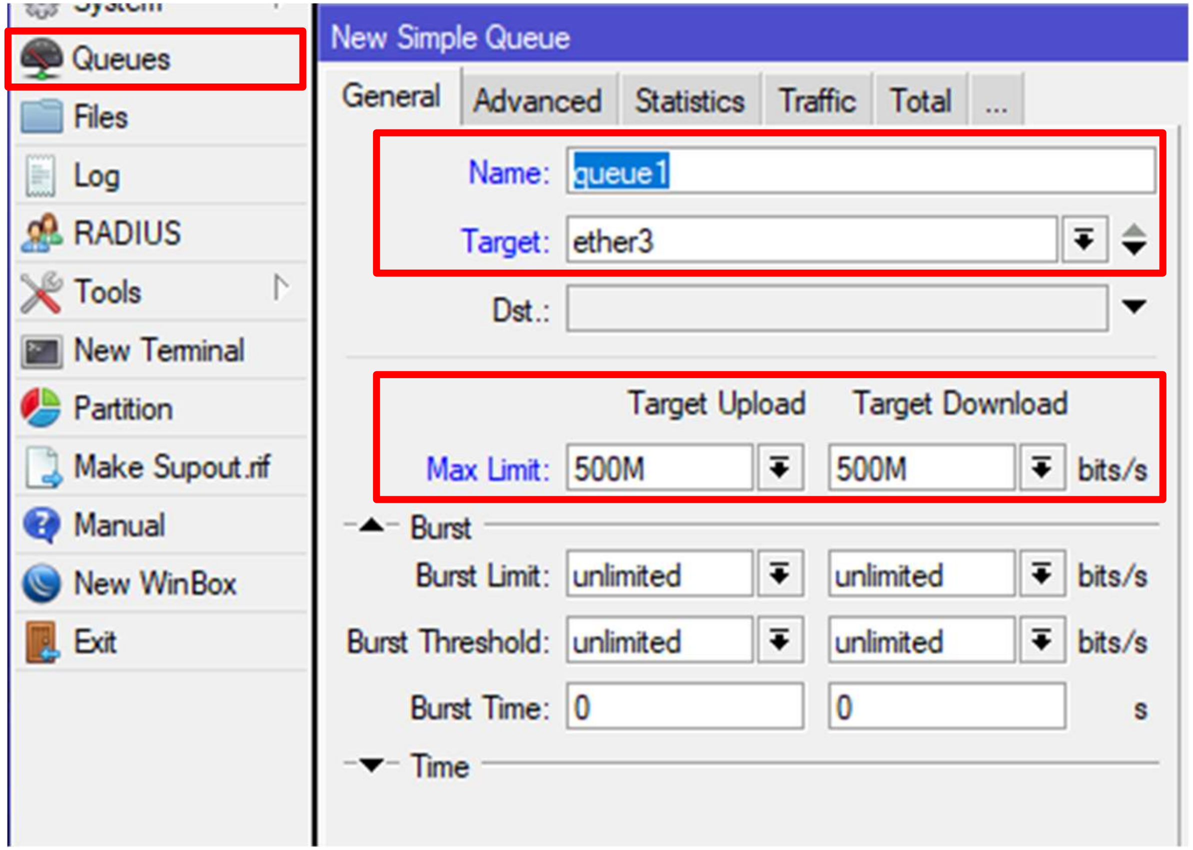
	Name		Act...	L2	Tx	Rx	Tx Pack
R	ether1	I	1500	1592	362.8 kbps	30.2 kbps	
R	sfp-sfpplus1	I	1500	1592	2.4 kbps	987.0 Mbps	
R	sfp-sfpplus2	I	1500	1592	987.0 Mbps	131.8 kbps	
	sfp-sfpplus3	I	1500	1592	0 bps	0 bps	
	sfp-sfpplus4	I	1500	1592	0 bps	0 bps	
	sfp-sfpplus5	I	1500	1592	0 bps	0 bps	
	sfp-sfpplus6	I	1500	1592	0 bps	0 bps	
	sfp-sfpplus7	I	1500	1592	0 bps	0 bps	
	sfp-sfpplus8	I	1500	1592	0 bps	0 bps	
	sfp-sfpplus9	I	1500	1592	0 bps	0 bps	
	sfp-sfpplus10	I	1500	1592	0 bps	0 bps	
	sfp-sfpplus11	I	1500	1592	0 bps	0 bps	
	sfp-sfpplus12	I	1500	1592	0 bps	0 bps	
	sfp-sfpplus13	I	1500	1592	0 bps	0 bps	

18 items (1 selected)



Limitação de Tráfego

JAMAIS FAÇA ISSO NO SWITCH!



Name: queue1

Target: ether3

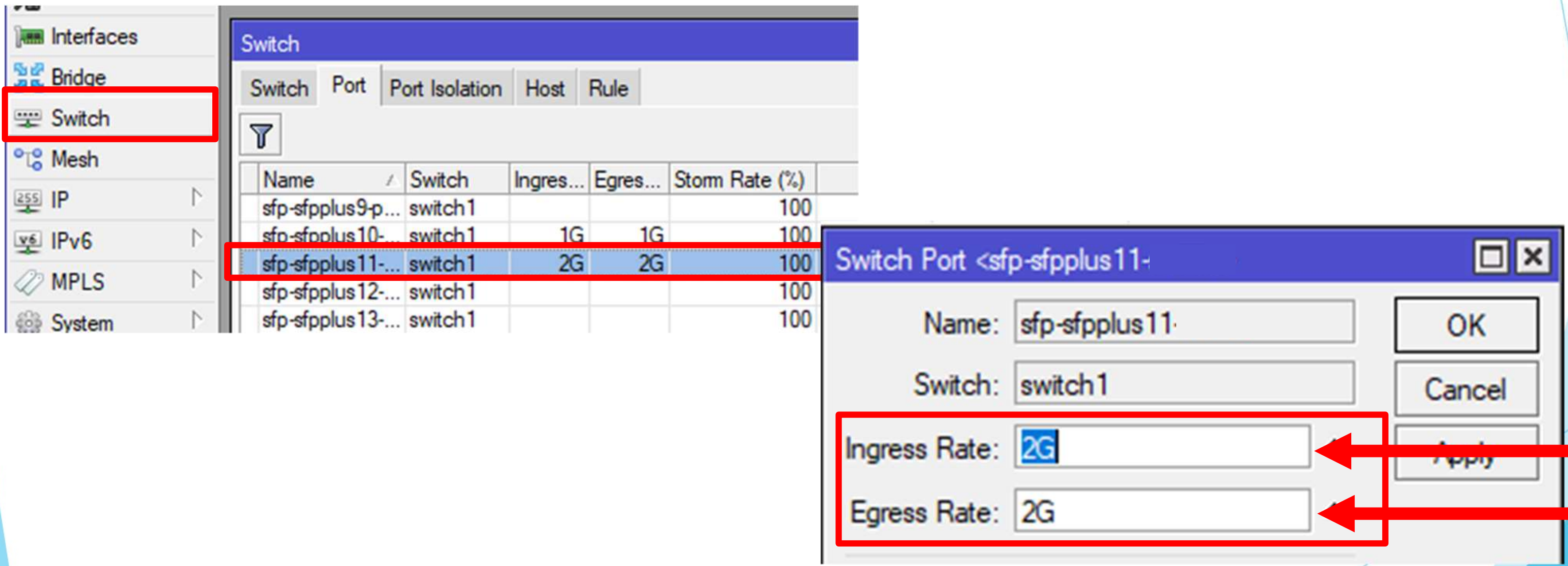
Dst.:

	Target Upload	Target Download	
Max Limit:	500M	500M	bits/s
Burst			
Burst Limit:	unlimited	unlimited	bits/s
Burst Threshold:	unlimited	unlimited	bits/s
Burst Time:	0	0	s

Time

Limitação de tráfego

- Plenamente possível em Hardware;
- Possibilidade de limitar tráfego acima de 1Gbps com muita facilidade



Name	Switch	Ingres...	Egres...	Storm Rate (%)
sfp-sfpplus9-p...	switch1			100
sfp-sfpplus10-...	switch1	1G	1G	100
sfp-sfpplus11-...	switch1	2G	2G	100
sfp-sfpplus12-...	switch1			100
sfp-sfpplus13-...	switch1			100

Name: sfp-sfpplus11-

Switch: switch1

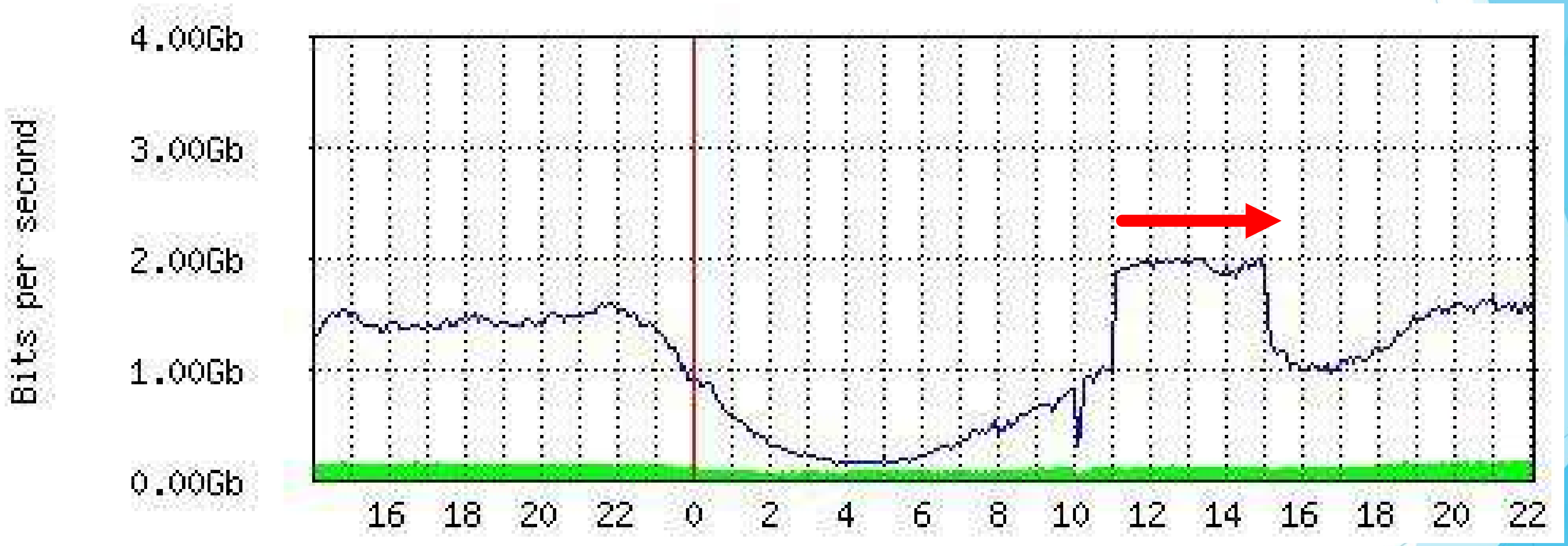
Ingress Rate: 2G

Egress Rate: 2G

Upload (cliente)

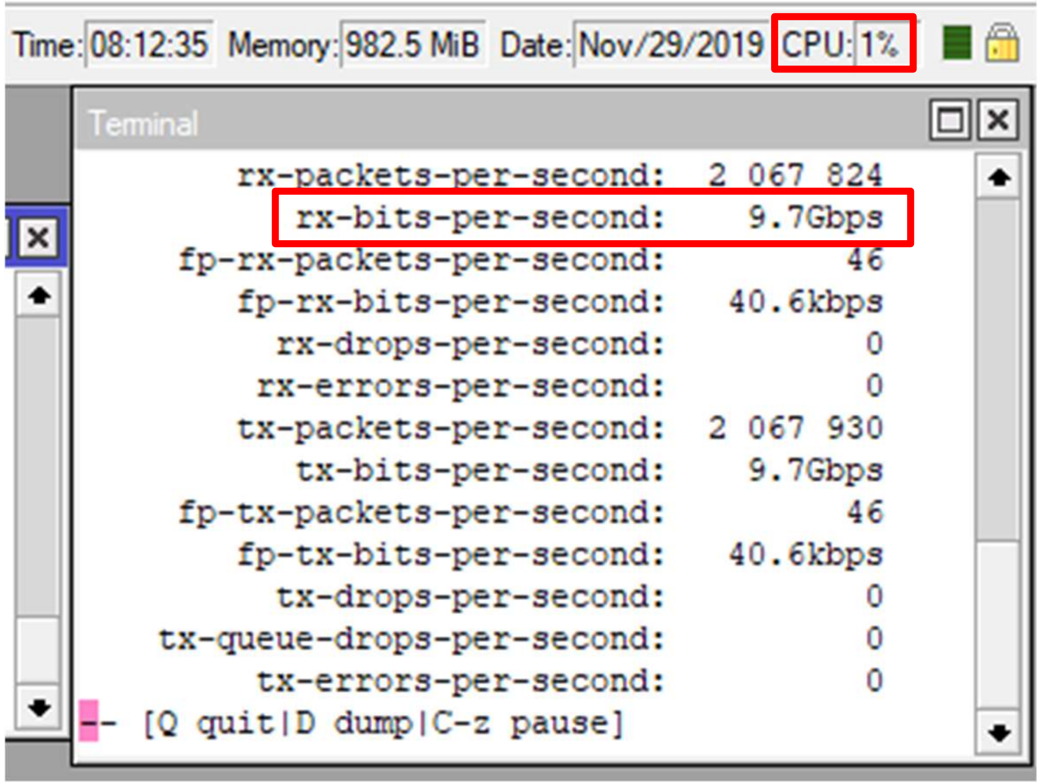
Download (cliente)

Limitação de tráfego (resultado)



Resultado Real

(preservando o Hardware offload)

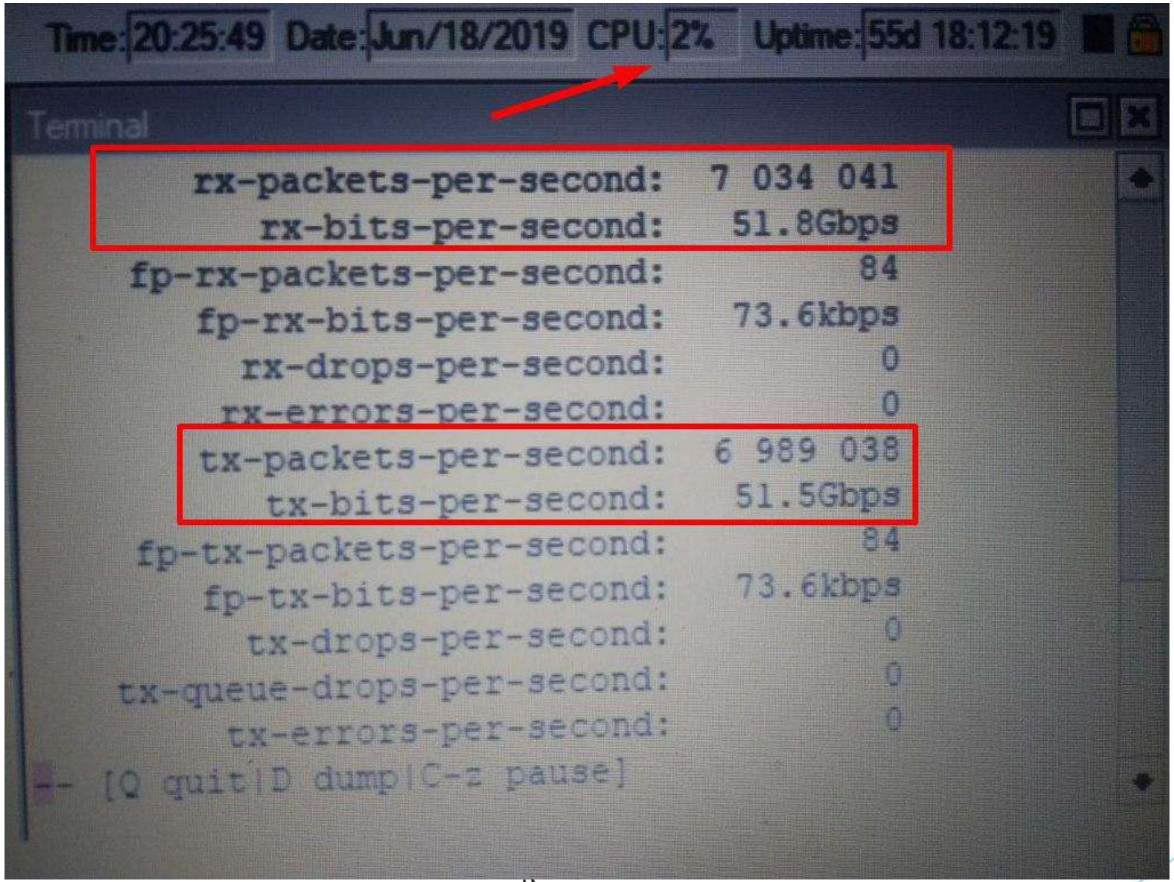


Time: 08:12:35 Memory: 982.5 MiB Date: Nov/29/2019 CPU: 1%

```
      rx-packets-per-second:  2 067 824
         rx-bits-per-second:    9.7Gbps
   fp-rx-packets-per-second:         46
      fp-rx-bits-per-second:   40.6kbps
        rx-drops-per-second:          0
       rx-errors-per-second:          0
      tx-packets-per-second:  2 067 930
         tx-bits-per-second:    9.7Gbps
   fp-tx-packets-per-second:         46
      fp-tx-bits-per-second:   40.6kbps
        tx-drops-per-second:          0
  tx-queue-drops-per-second:          0
       tx-errors-per-second:          0
-- [Q quit|D dump|C-z pause]
```

Resultado Real

(preservando o Hardware offload)



```
Time: 20:25:49  Date: Jun/18/2019  CPU: 2%  Uptime: 55d 18:12:19
```

```
     rx-packets-per-second:   7 034 041
        rx-bits-per-second:     51.8Gbps
  fp-rx-packets-per-second:           84
     fp-rx-bits-per-second:    73.6kbps
       rx-drops-per-second:            0
      rx-errors-per-second:            0
     tx-packets-per-second:   6 989 038
        tx-bits-per-second:     51.5Gbps
  fp-tx-packets-per-second:           84
     fp-tx-bits-per-second:    73.6kbps
       tx-drops-per-second:            0
 tx-queue-drops-per-second:            0
      tx-errors-per-second:            0
-- [Q quit|D dump|C-z pause]
```

Referências e informações adicionais:

- https://wiki.mikrotik.com/wiki/Manual:CRS3xx_series_switches
- https://wiki.mikrotik.com/wiki/Manual:Bridge_VLAN_Table
- https://youtu.be/CKgyf9N-wR0 -> (Overview da CRS326-24S+2Q+)

Dúvidas??
Obrigado!

pronetworks

Radar
INTERNET BANDA LARGA

MikroTik

Redes Brasil