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

©2019 - Pro Networks - Material Por: João Aberto Barbosa de Oliveira

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

©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

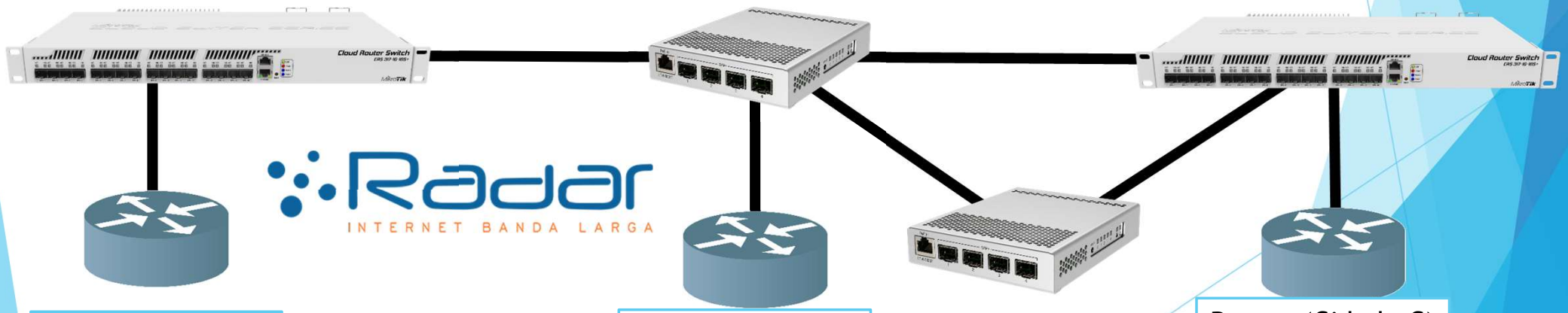
Objetivos:

- 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.

©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

Case de backbone: ISP Radar Internet

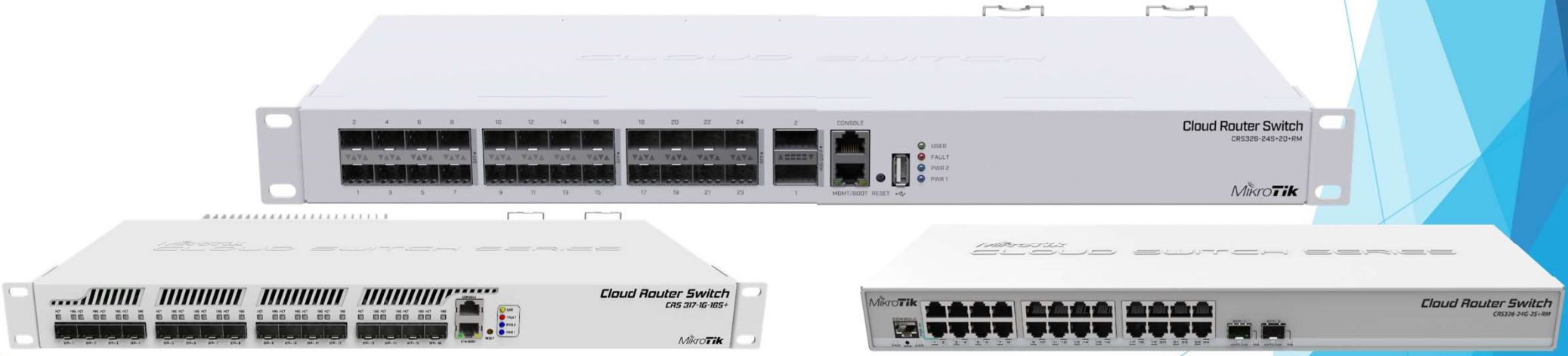
- Backbone óptico com 10 e 20Gbps;
- Mais de 240 dispositivos com RouterOS, sendo 30 Switchs CRS3xx;
- 650km de backbone óptico;



©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

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

©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

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

©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

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;

MikroTik

©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

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;

©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

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

©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

CRS 3xx conta com o poder...

MARVELL®

Name: switch1

Type: Marvell 98DX3236

MikroTik

©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

Características base:

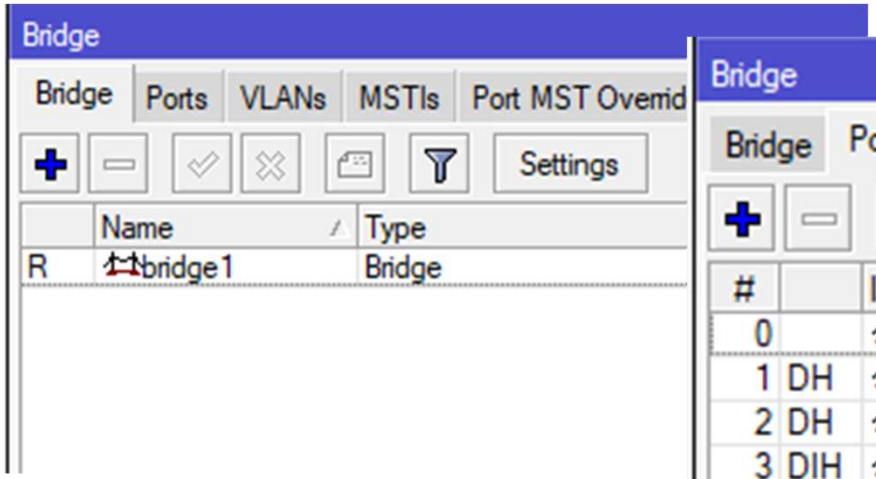
Models

This table clarifies main differences between Cloud Router Switch models.

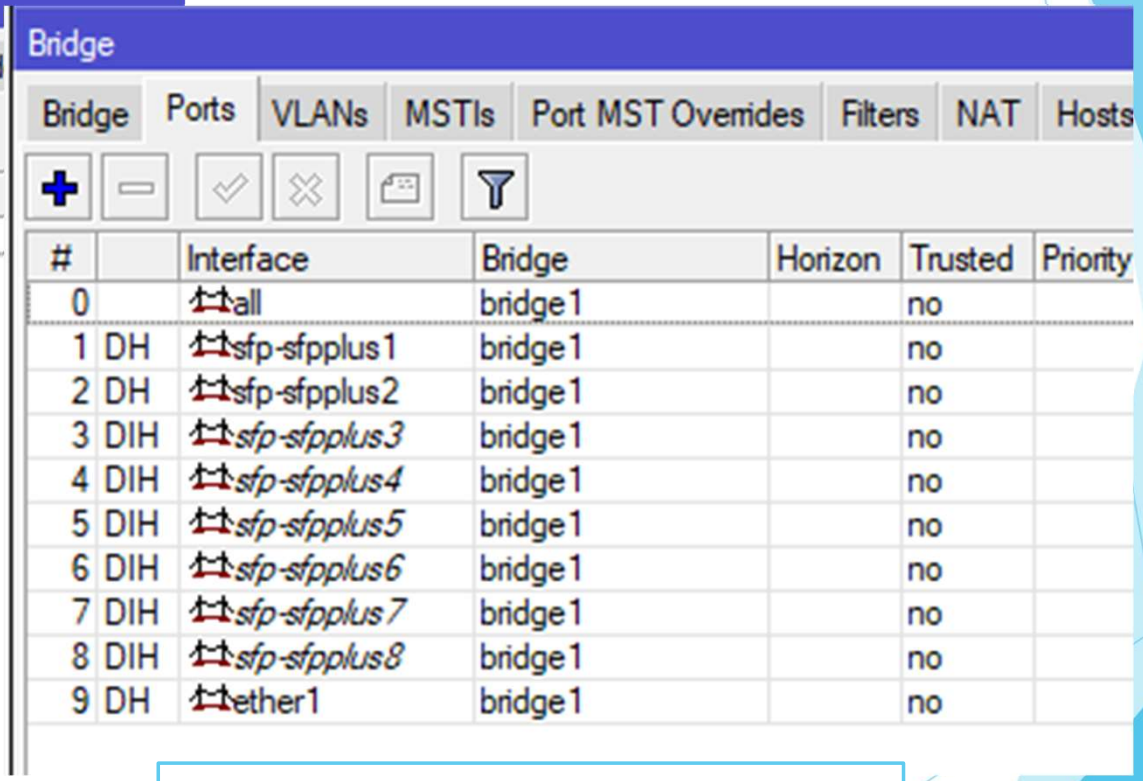
Model	Switch Chip	CPU	Cores	Wireless	SFP+ port	ACL rules	Jumbo Frame (Bytes)
CRS326-24G-2S+	Marvell-98DX3236	800MHz	1	-	+	128	10218
CRS328-24P-4S+	Marvell-98DX3236	800MHz	1	-	+	128	10218
CRS328-4C-20S-4S+	Marvell-98DX3236	800MHz	1	-	+	128	10218
CRS305-1G-4S+	Marvell-98DX3236	800MHz	1	-	+	128	10218
CRS309-1G-8S+	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

©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

Como Geralmente as pessoas fazem...

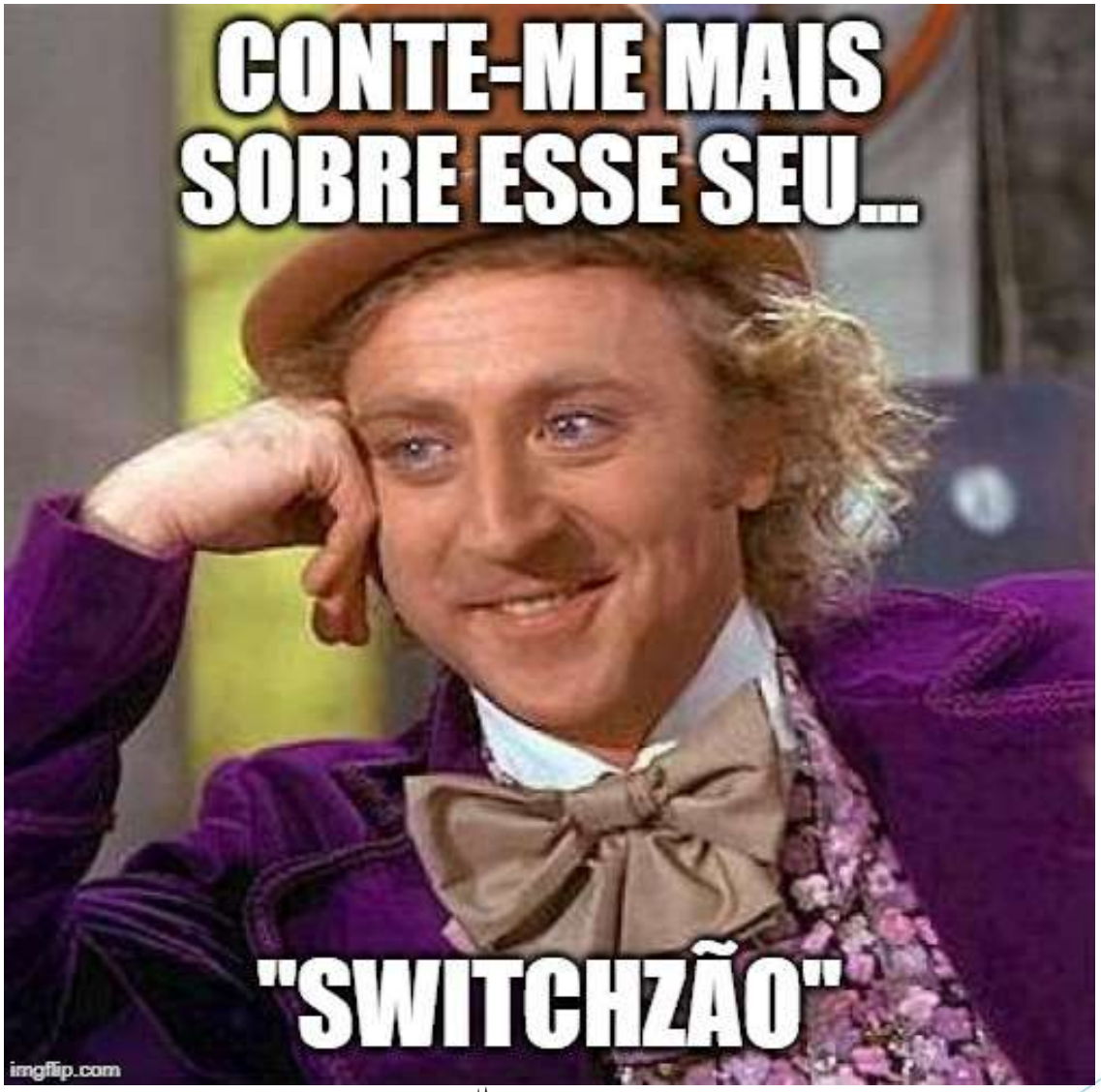


1° Cria uma Bridge



2° Adiciona Todas as portas na Bridge

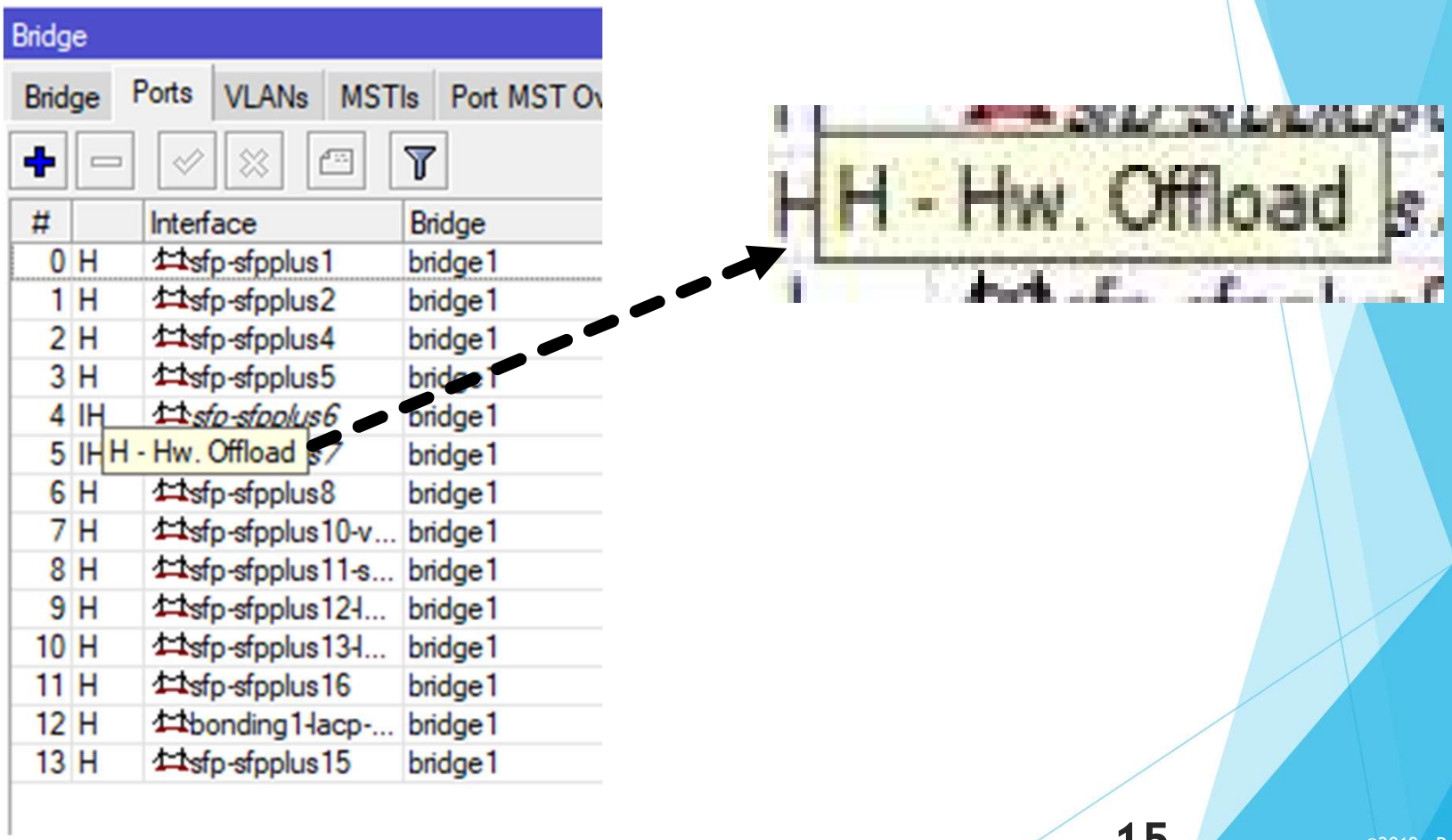
©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira



MikroTik

©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

Hardware Offload



©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

Hardware Offload

SEM Hardware Offload ----▶ CPU: 100%

COM Hardware Offload -----▶ CPU: 0%

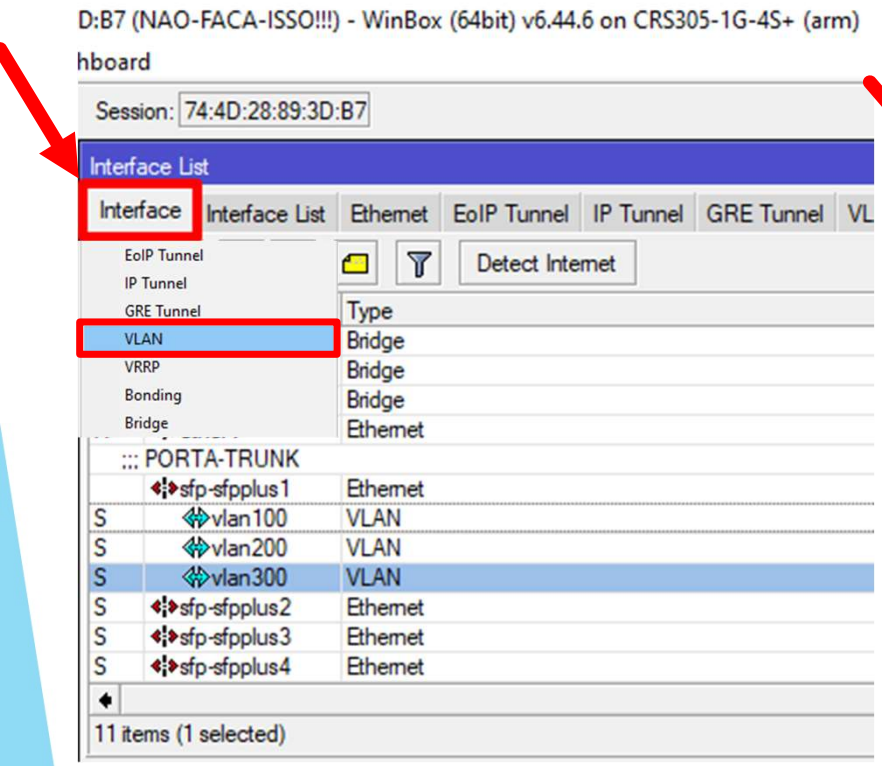
MikroTik

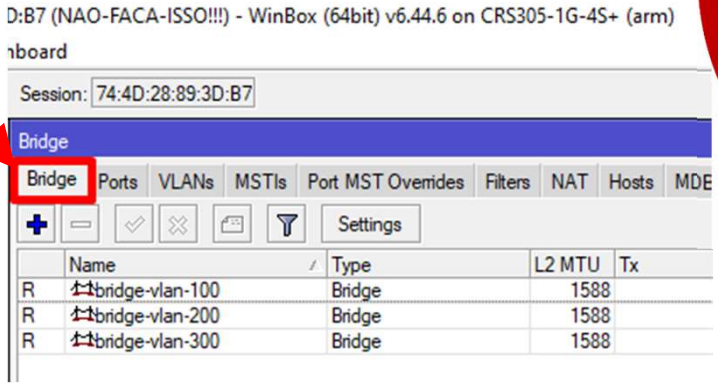
©2019 - Pro Networks -
Material Por: João Aberto Barbosa de Oliveira

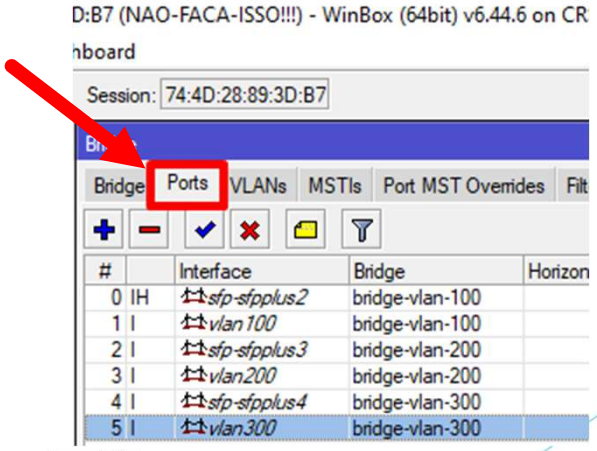
©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

VLANs

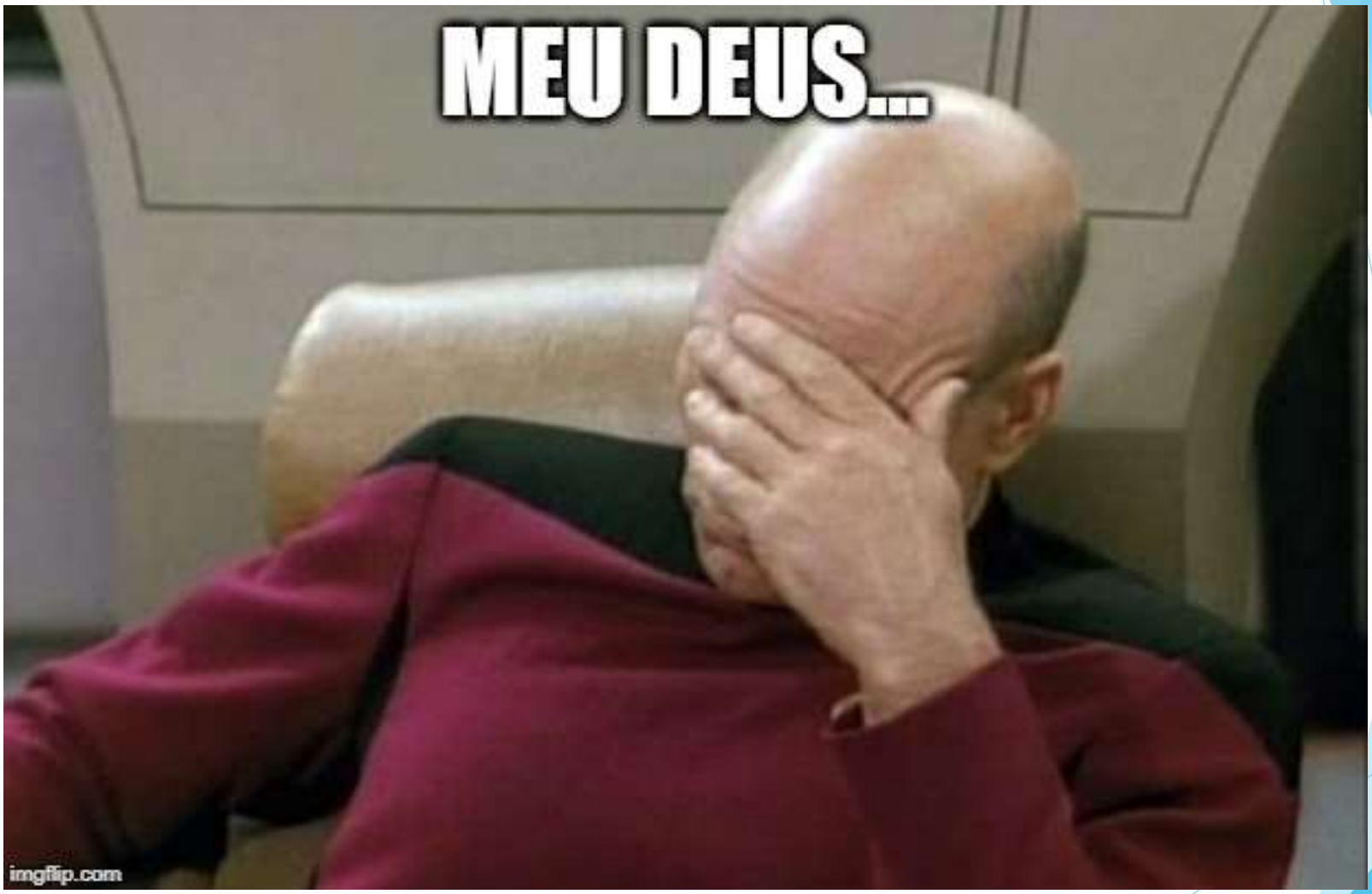
JAMAIS FAÇA ISSO!







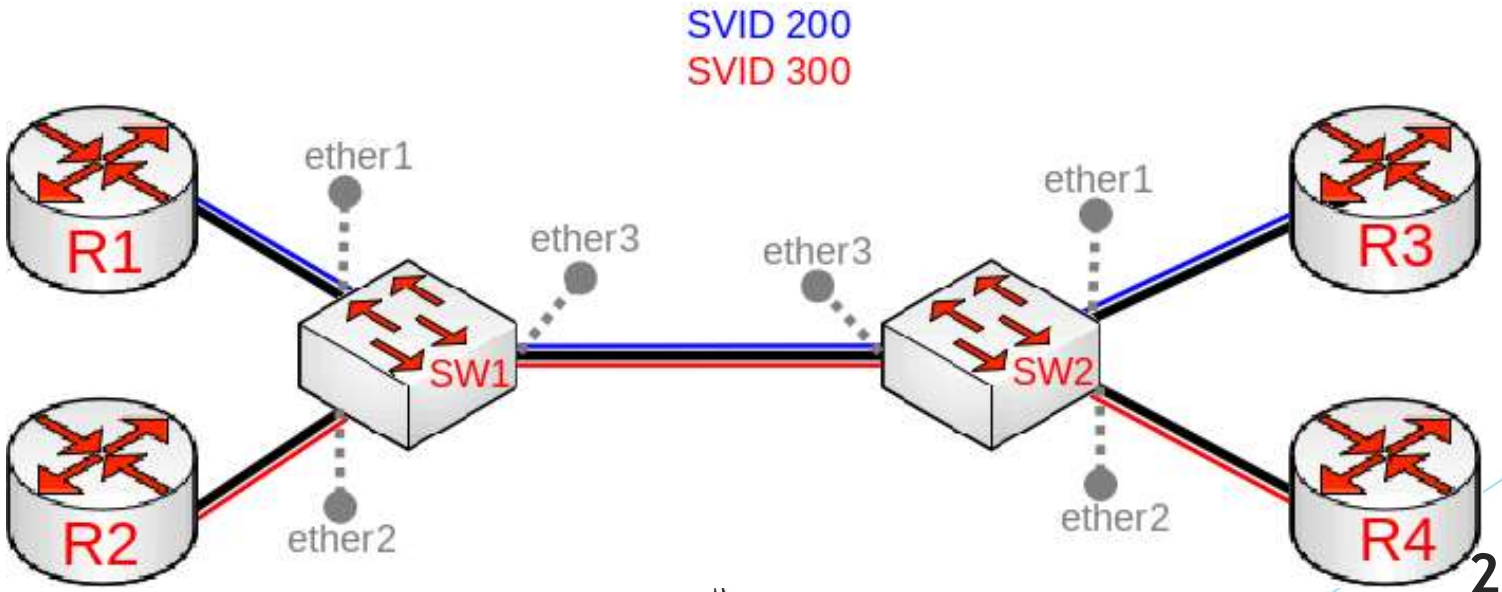
©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira



©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

VLANs (Tagged)

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

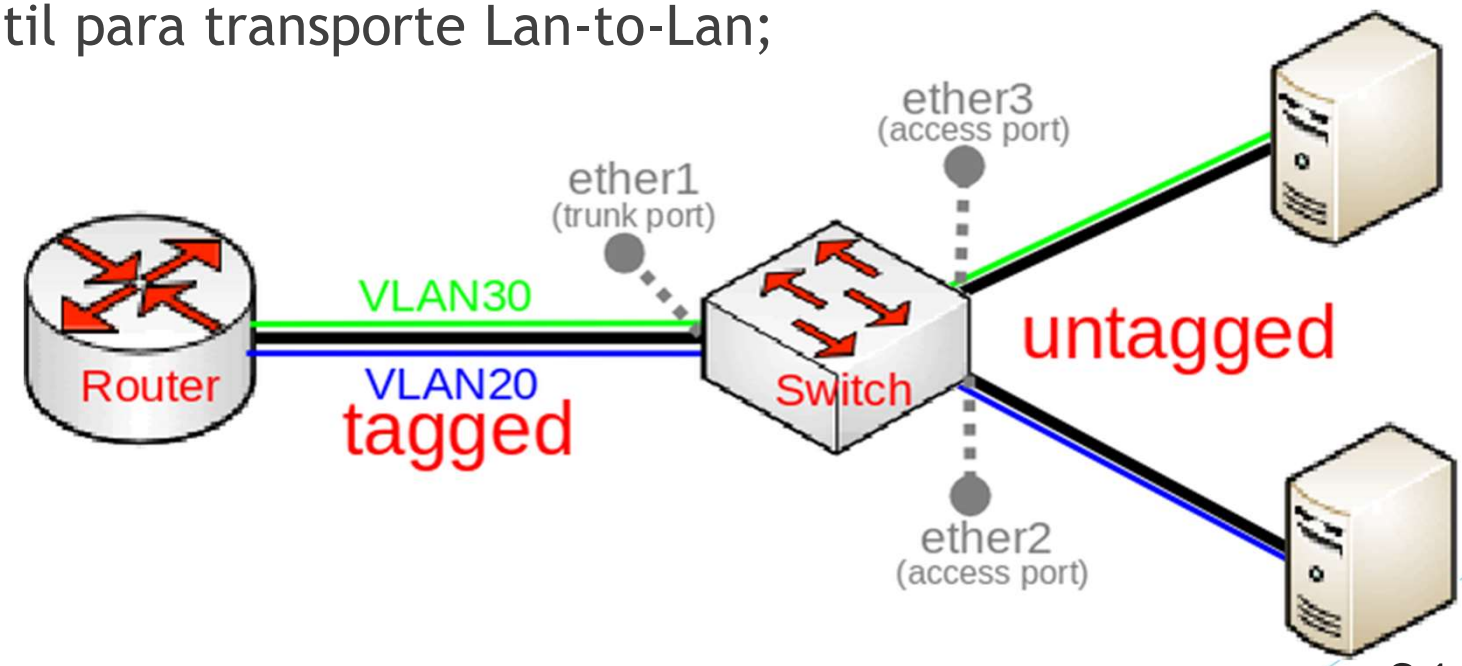


MikroTik

©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

VLANs (Untagged)

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

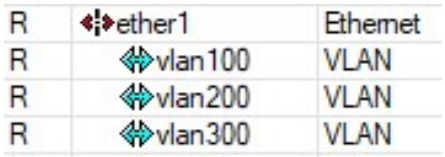


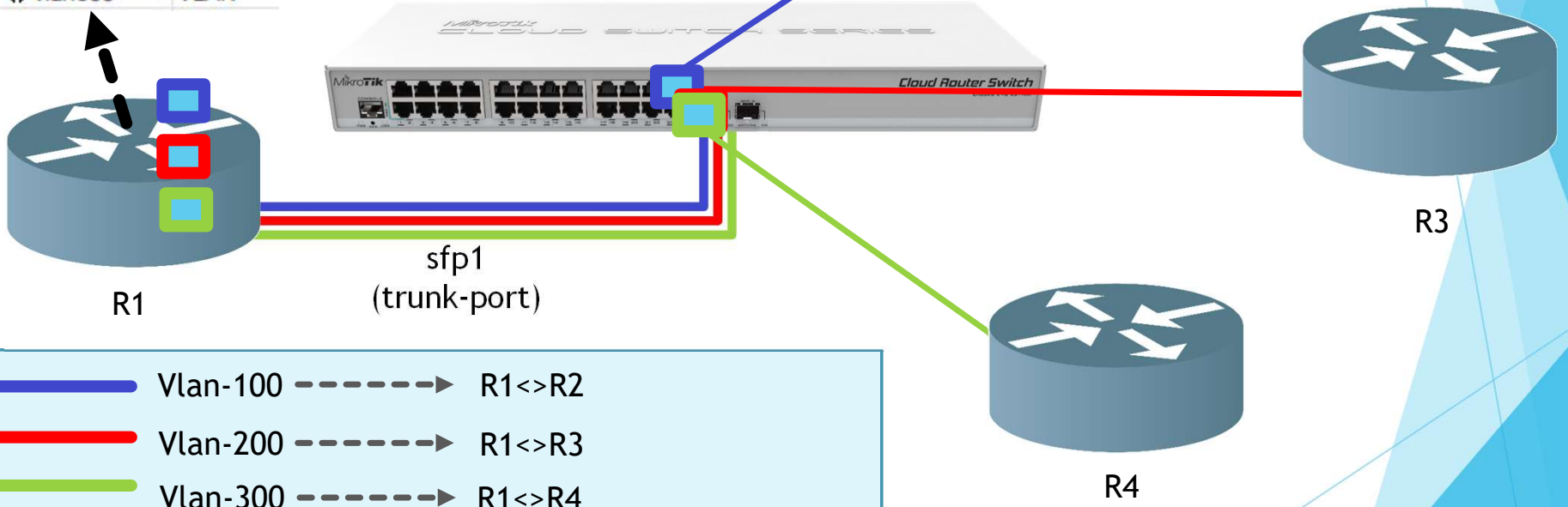
MikroTik

©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

VLANs (Tagged)

Exemplo simples





Vlan-100 ------> R1<>R2

Vlan-200 ------> R1<>R3

Vlan-300 ------> R1<>R4

Payload

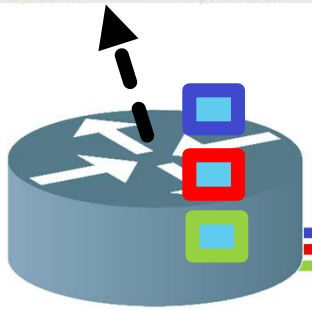
MikroTik

©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

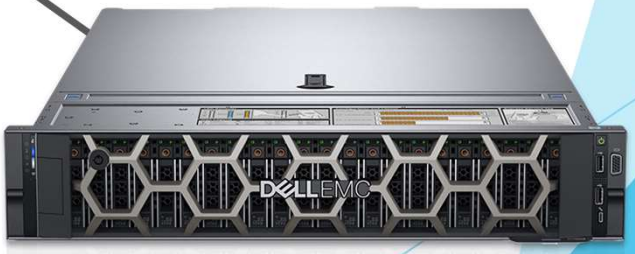
VLANs (Untagged)

Exemplo simples

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



sfp1
(trunk-port)



Vlan-100 ------> Camera

Vlan-200 ------> OmniTIK

Vlan-300 ------> DELL Server

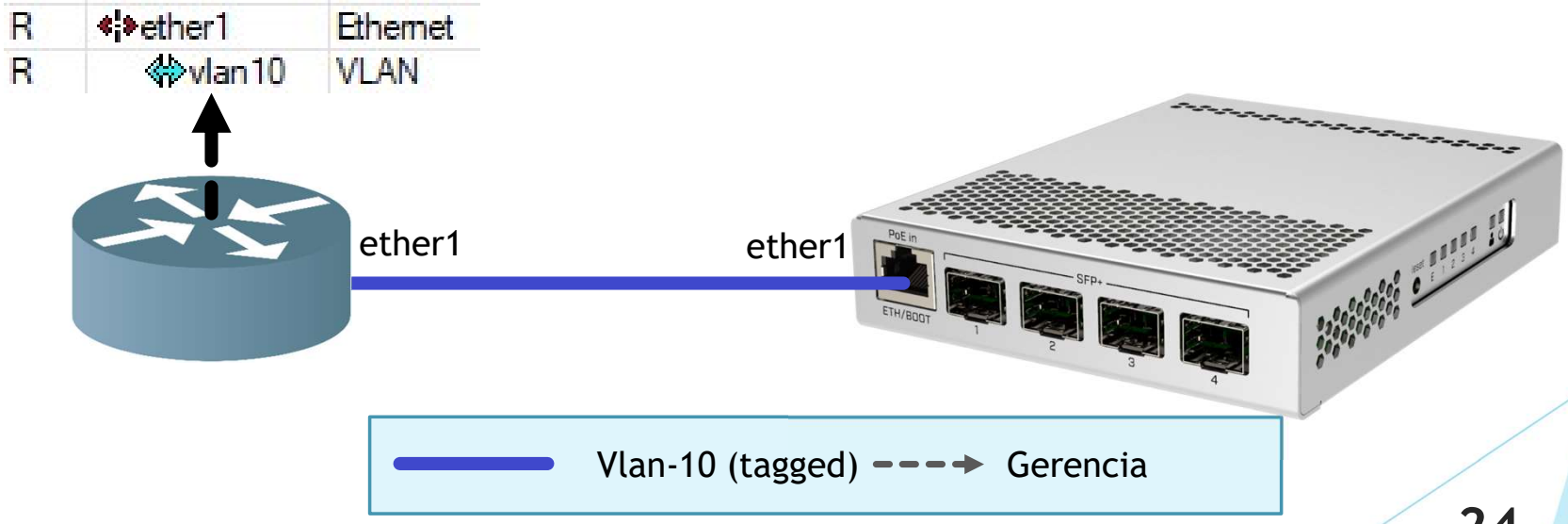
Payload

MikroTik

©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

VLAN de Gerencia (tagged)
Exemplo

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

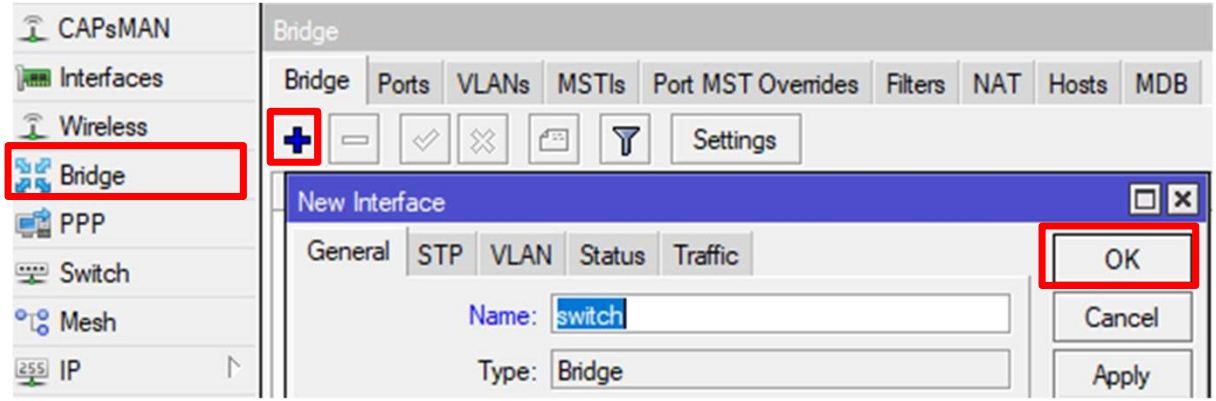


©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

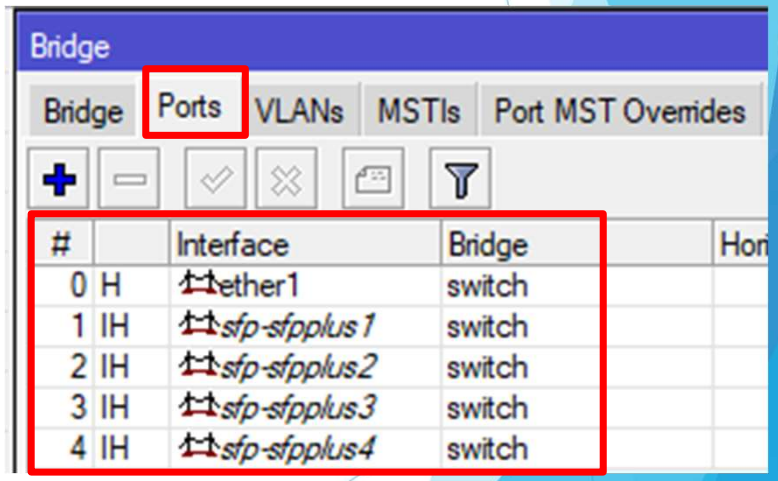
VLAN de Gerencia (tagged)

Exemplo

1- Criar uma bridge



2- Vincular as portas à Bridge

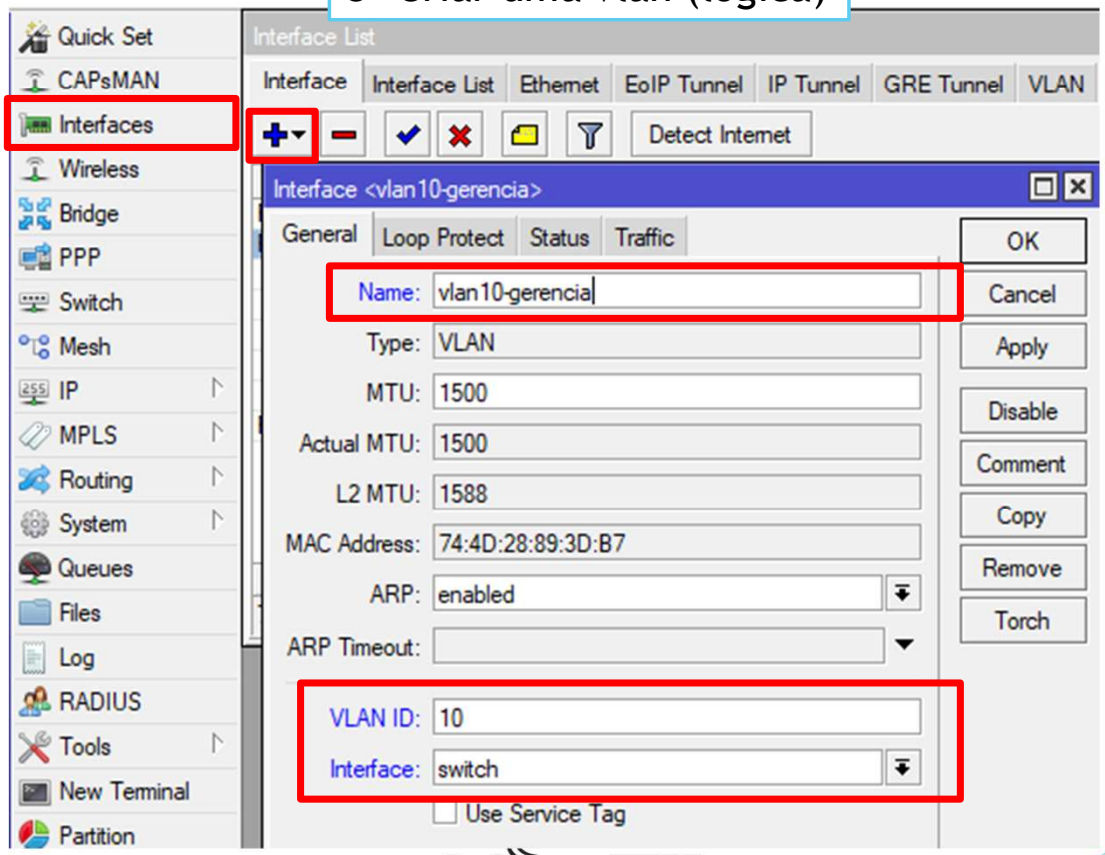


©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

VLAN de Gerencia (tagged)

Exemplo

3- Criar uma vlan (lógica)



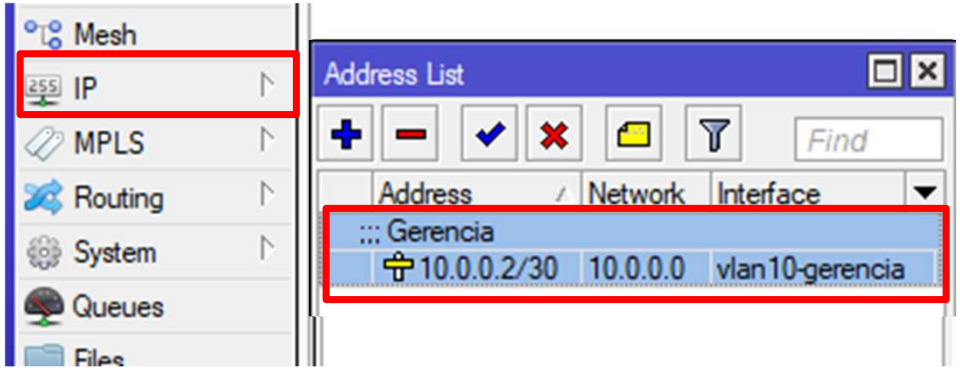
MikroTik

©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

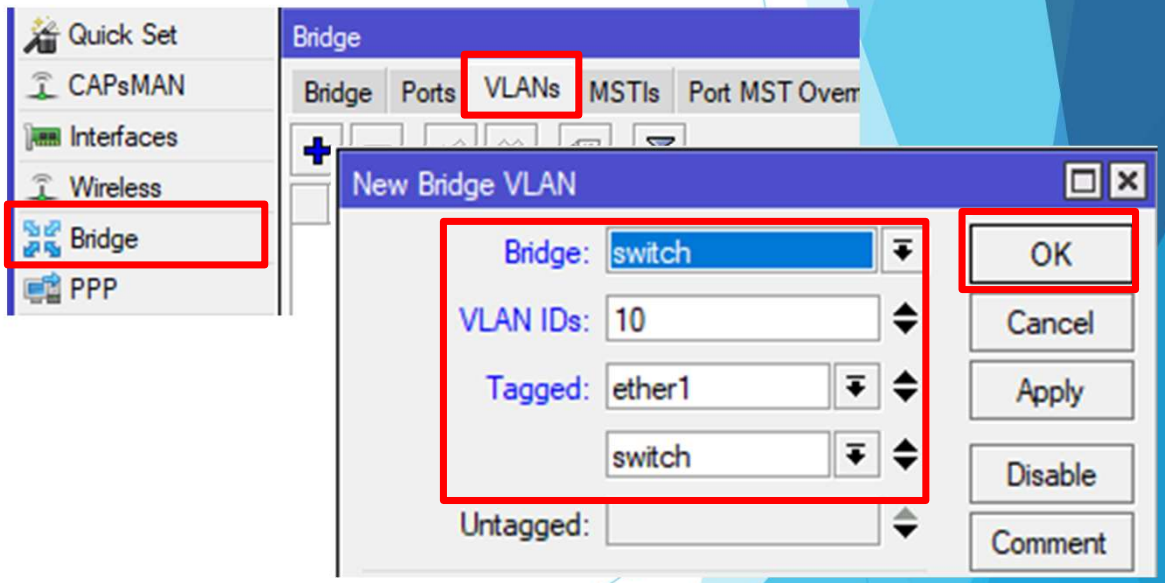
VLAN de Gerencia (tagged)

Exemplo

4- Adicionar o IP de Gerencia à VLAN criada



5- Marcar essa VLAN como “Tagged” nas respectivas interfaces;

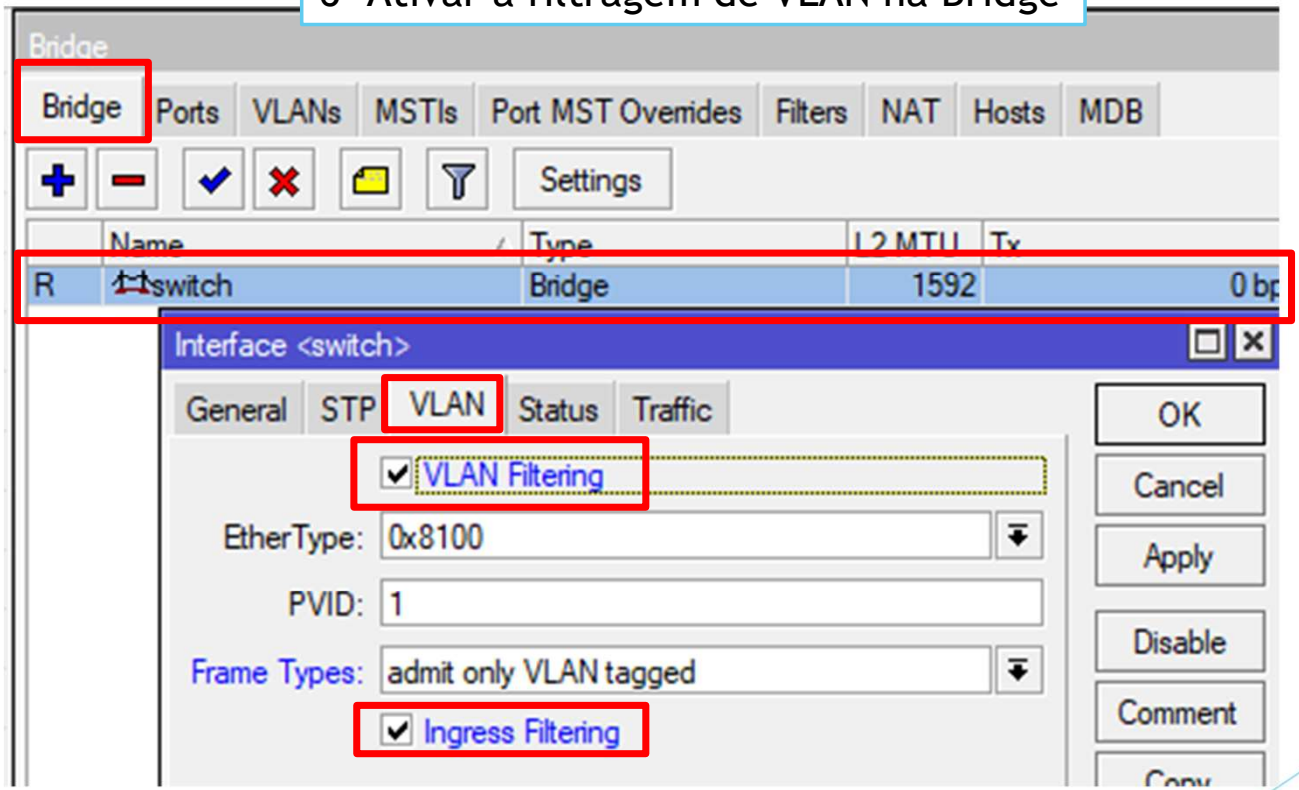


©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

VLAN de Gerencia (tagged)

Exemplo

6- Ativar a filtragem de VLAN na Bridge



©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

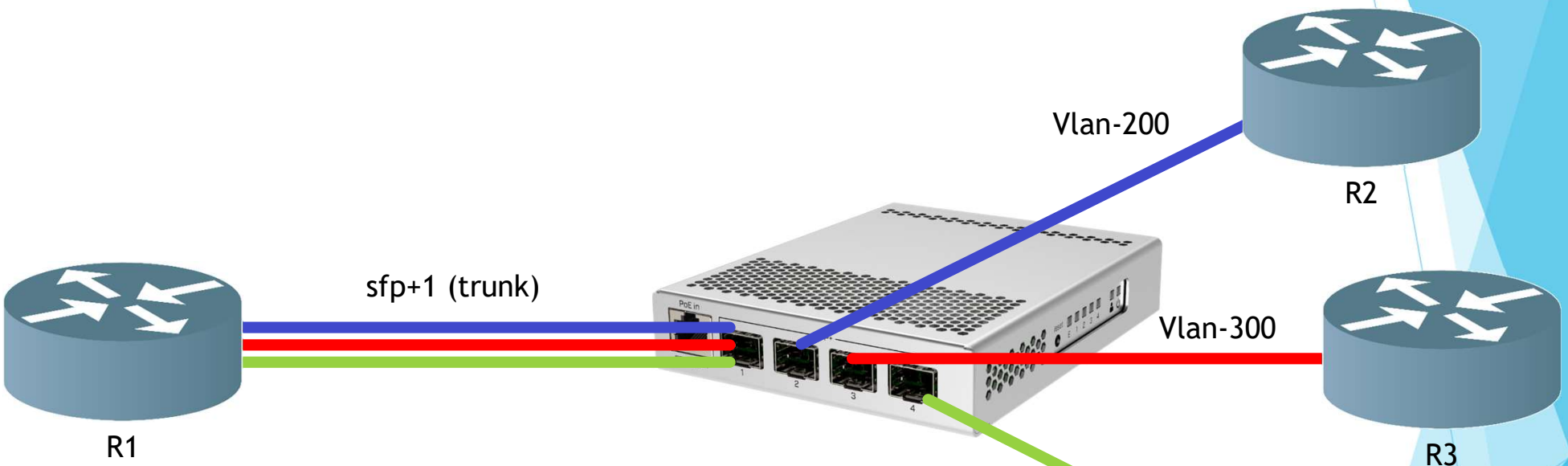
VLAN de Gerencia (Considerações finais)

- 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);

©2019 - Pro Networks -
Material Por: João Aberto Barbosa de Oliveira

VLANs (Tagged)

Como Fazer?



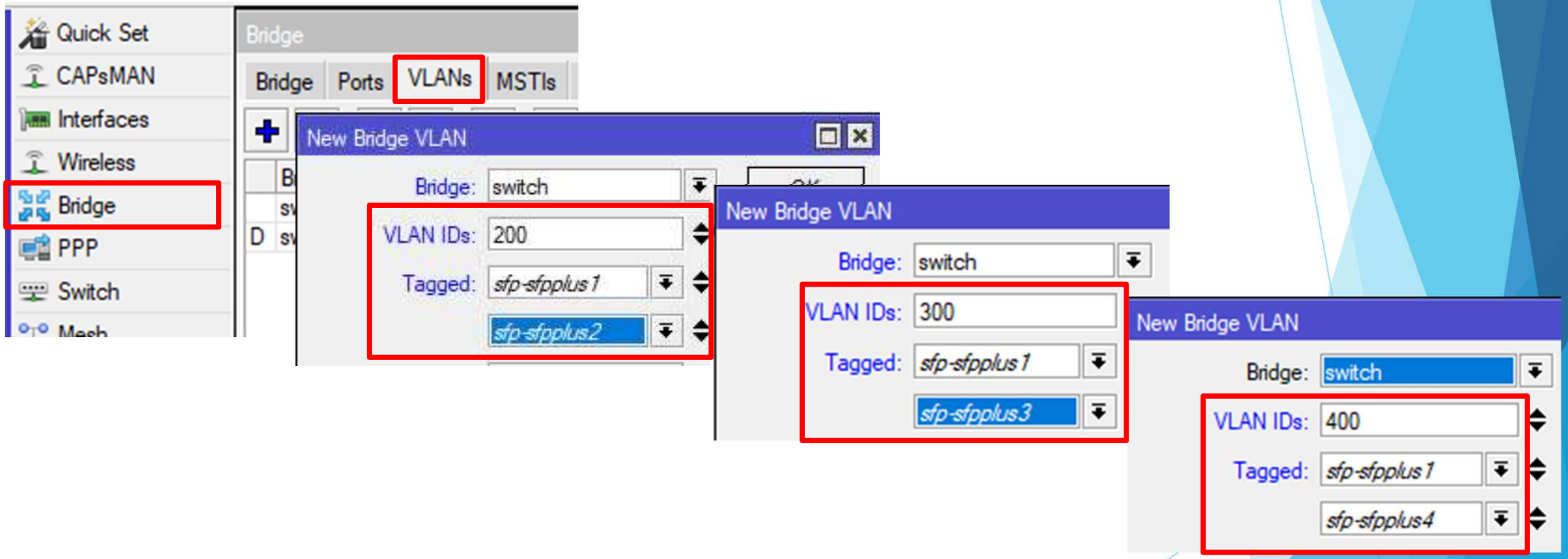
MikroTik

©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

VLANs (Tagged)

Como Fazer?

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

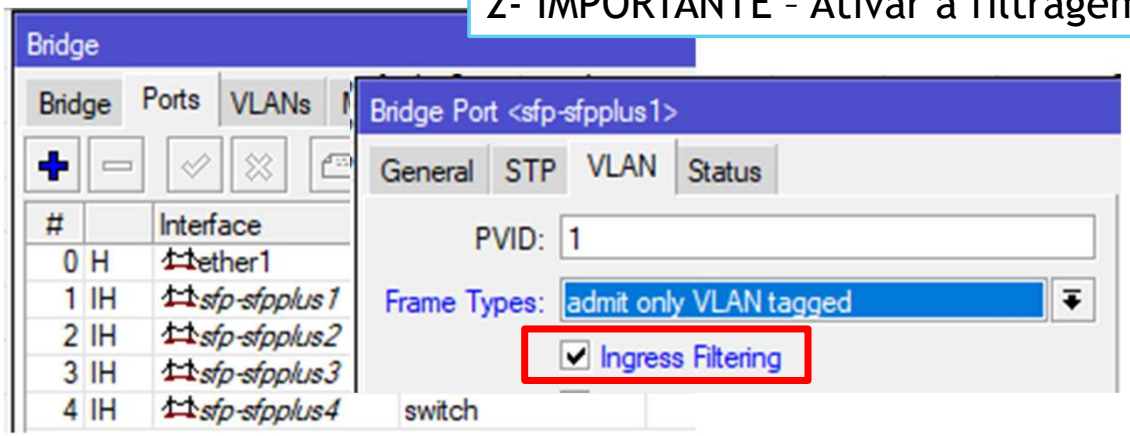


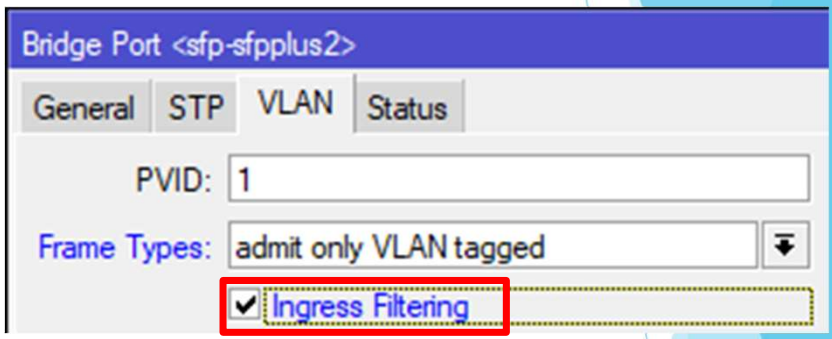
©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

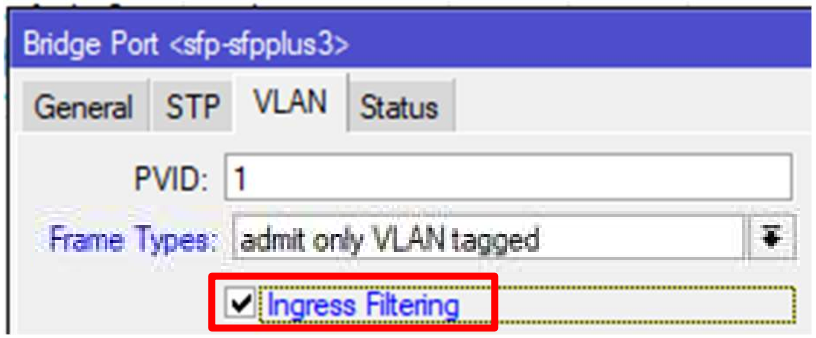
VLANs (Tagged)

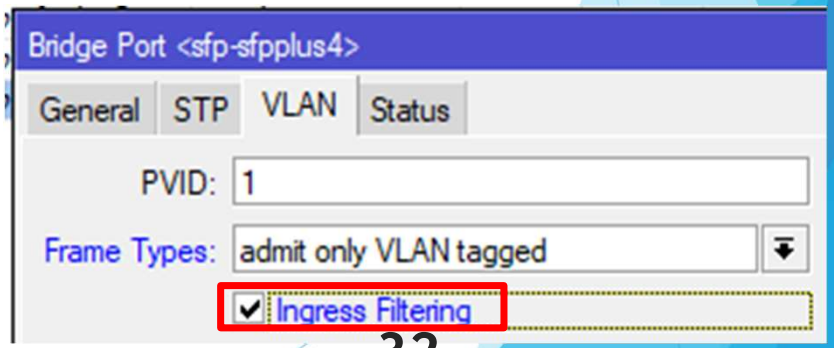
Como Fazer?

2- IMPORTANTE – Ativar a filtragem nas respectivas portas físicas





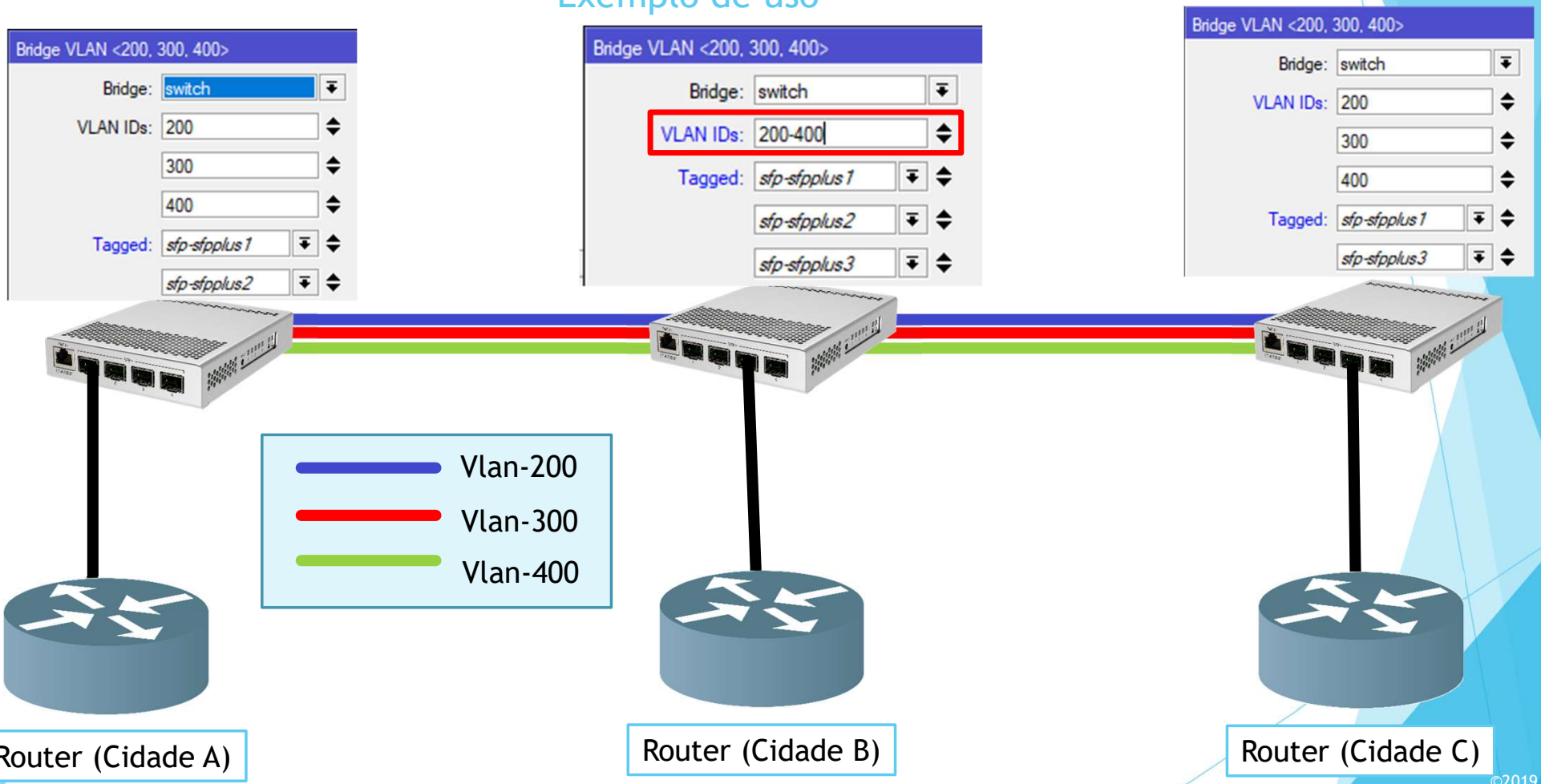




©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

VLANs (Tagged)

Exemplo de uso

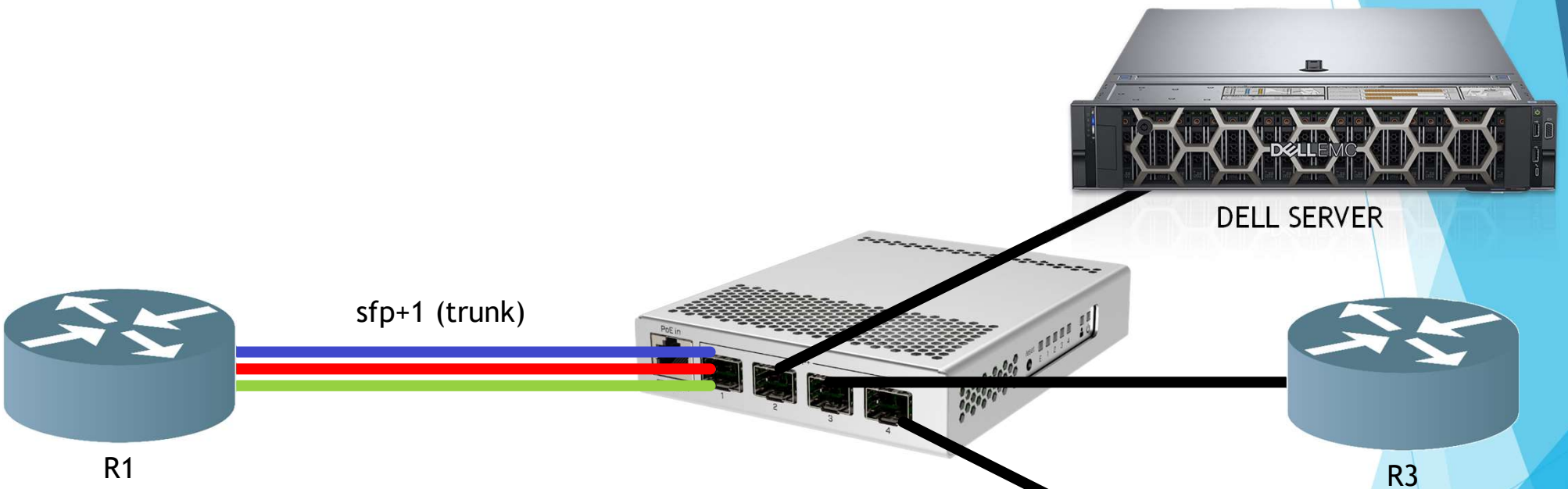


MikroTik

©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

VLANs (Untagged)

Como Fazer?



- Vlan-200 ------> Sfp+2 - DELL
- Vlan-300 ------> Sfp+3 – R3
- Vlan-400 ------> Sfp+4 – R4
- Frames sem TAG

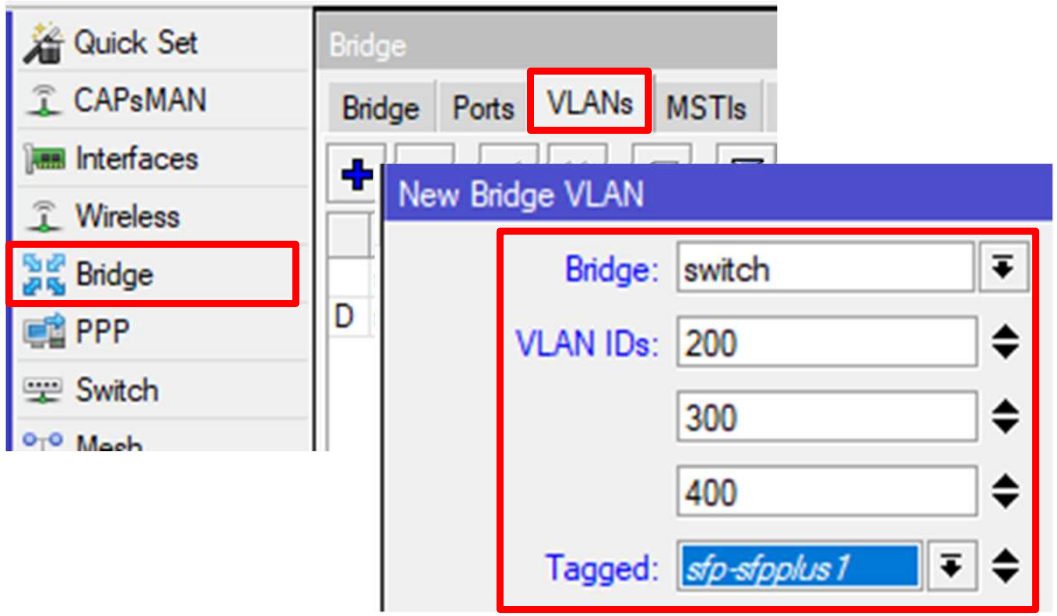
MikroTik

©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

VLANs (Untagged)

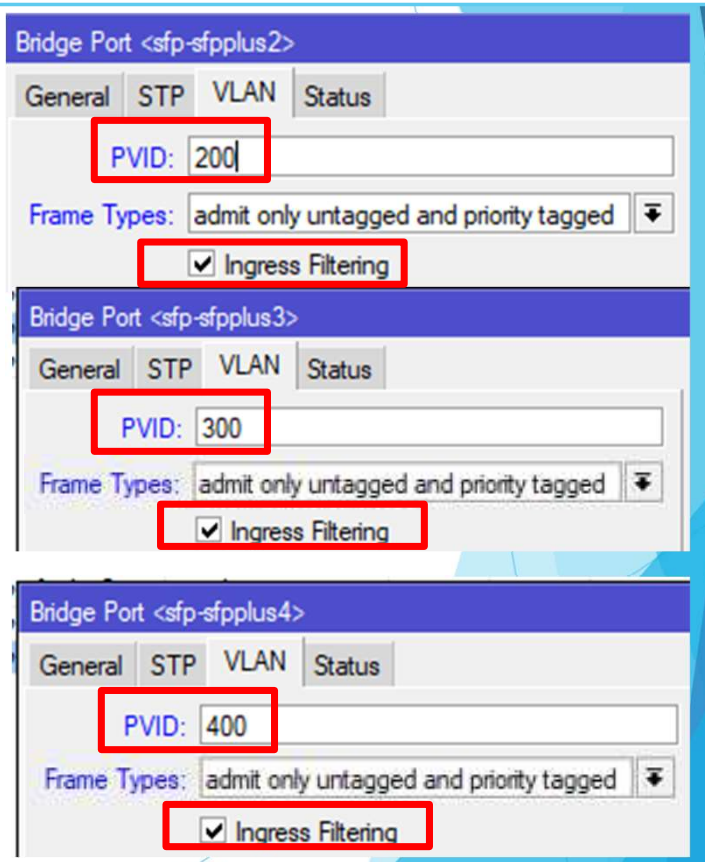
Como Fazer?

1- Adicionar a Trunk Port e VLANs Tagged



Menu “Bridge > Ports”

2- EM PVID dizer qual tratará frames “Untagged”



©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

VLANs

Considerações Gerais

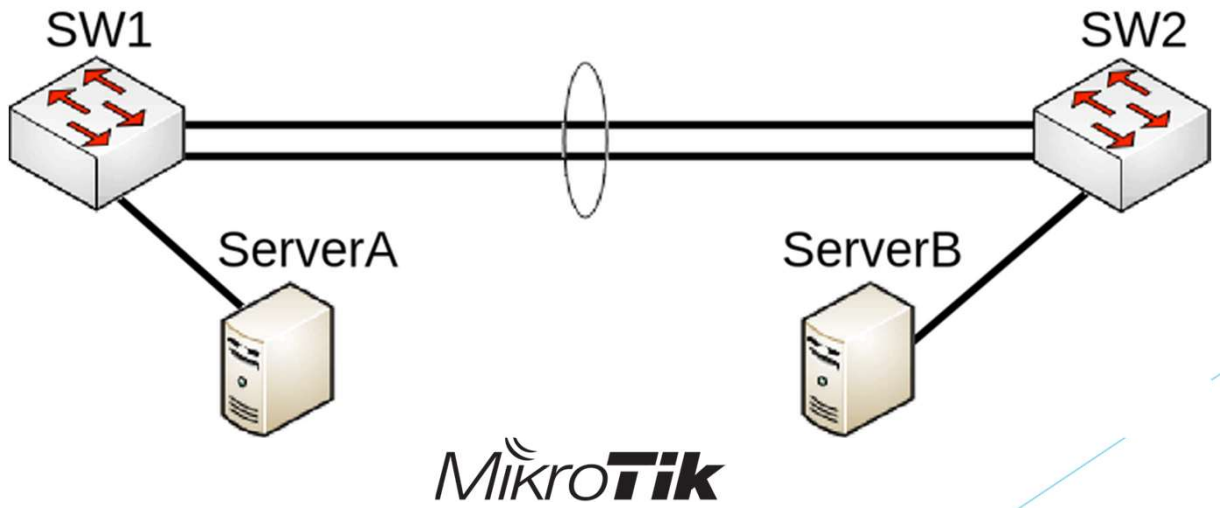
- ✓ Sempre usar “ingress filtering” nas interfaces para garantir o isolamento de broadcast;
- ✓ Essas configurações são válidas exclusivamente para a série CRS3xx (modo hardware);
- ✓ Existem diferentes formas de se configurar (dependendo do hardware/serie);

MikroTik

©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

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;

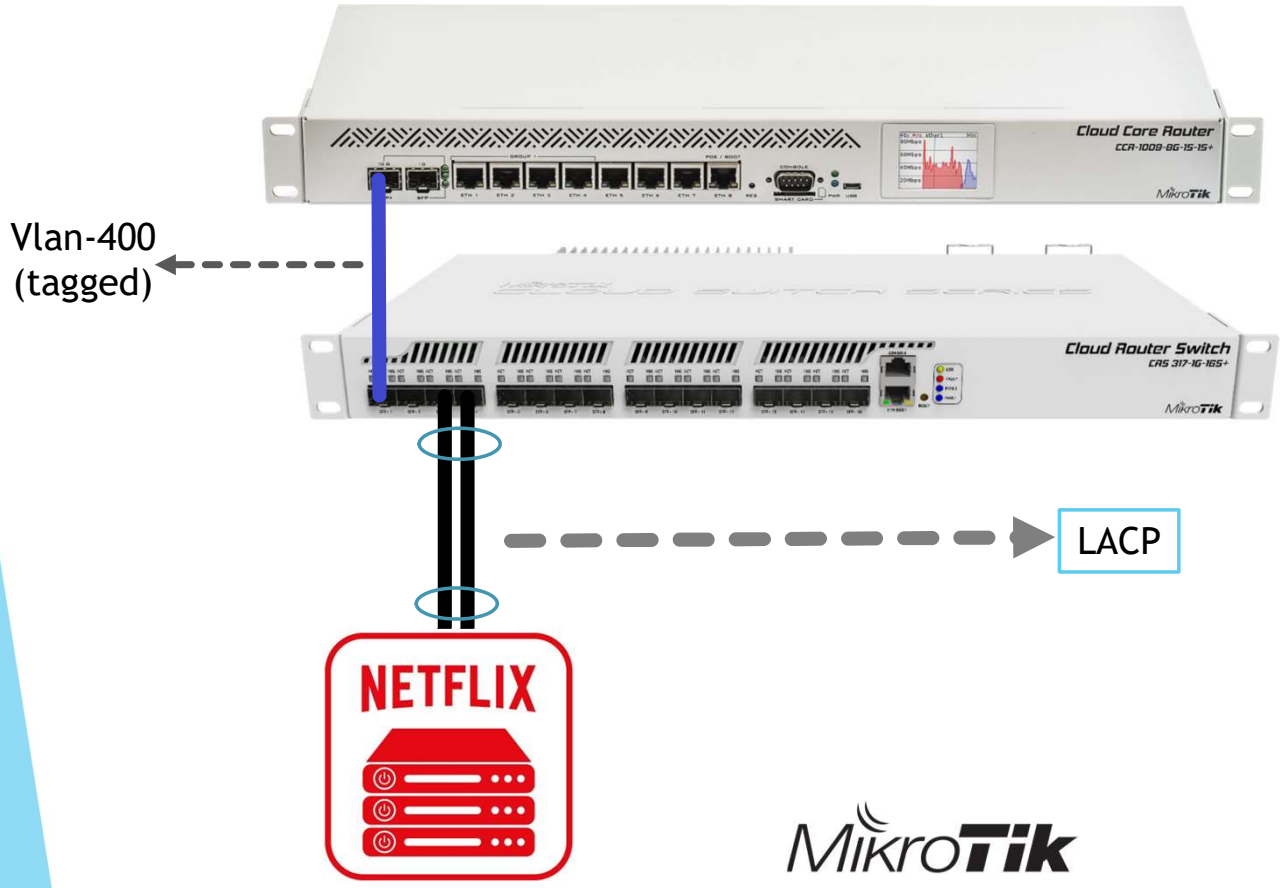


©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

LACP

(Caso de uso)

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

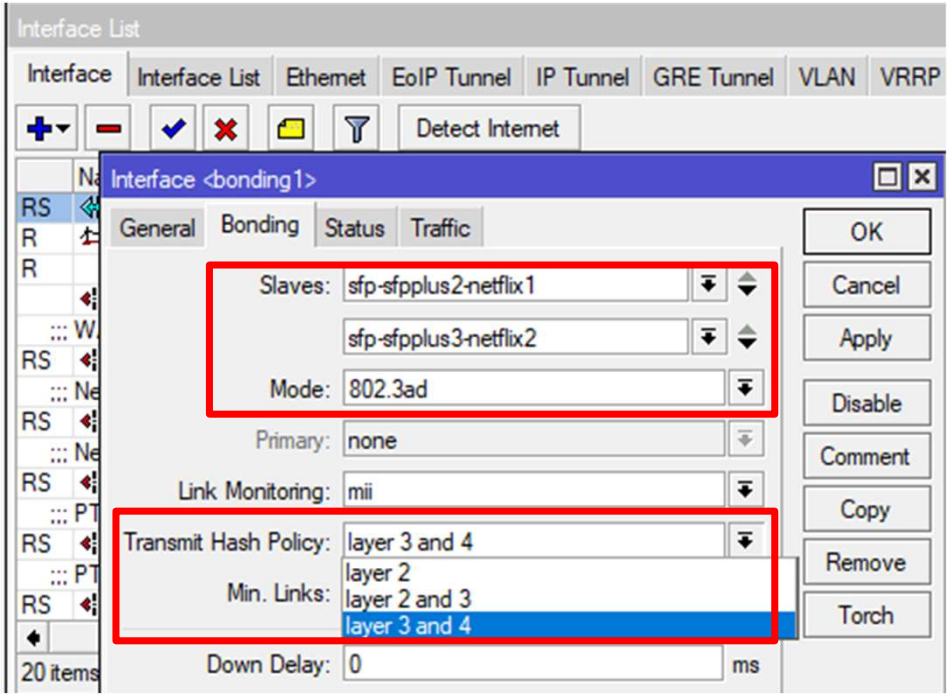


©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

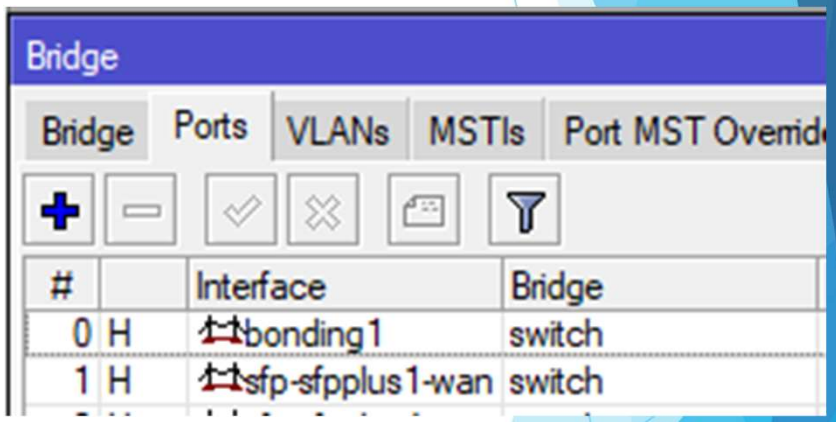
LACP

(Como fazer?)

1- Criar uma interface “Bonding” no modo 802.3ad



2- Adicionar o Bonding na Bridge



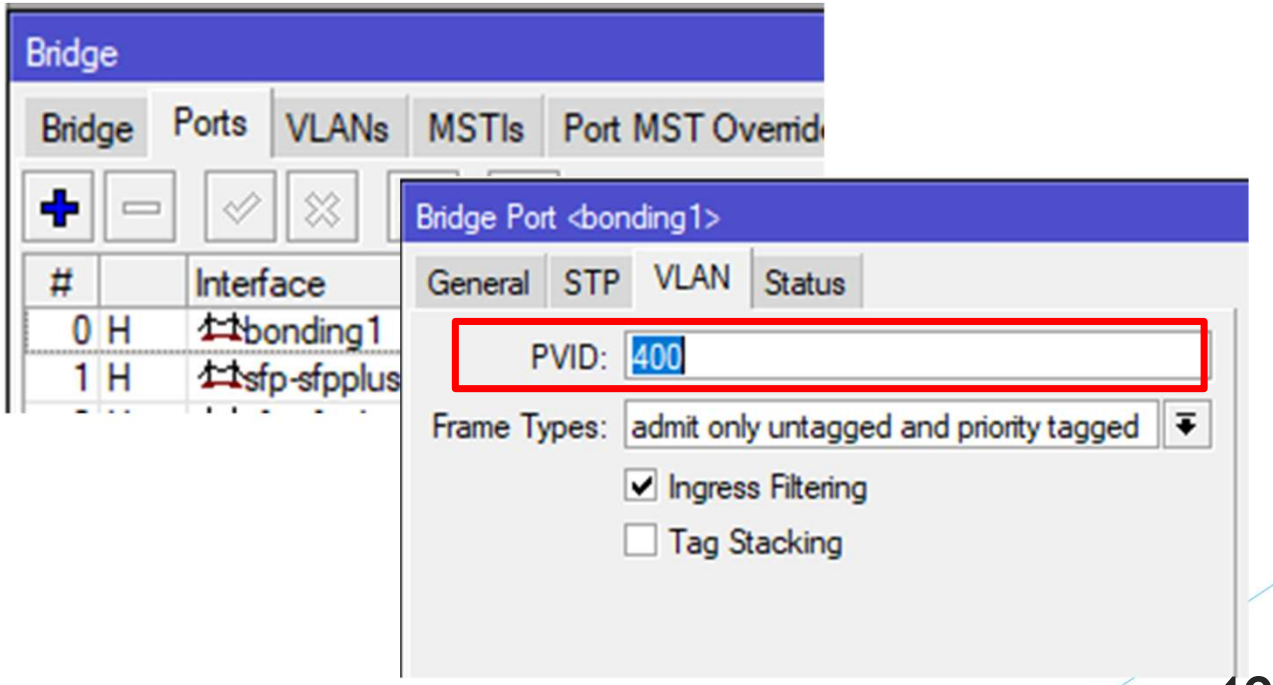
*É possível também em modo “balance-xor”

©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

LACP

(Como fazer?)

3- Colocar o PVID 400 (untagged) no Bonding

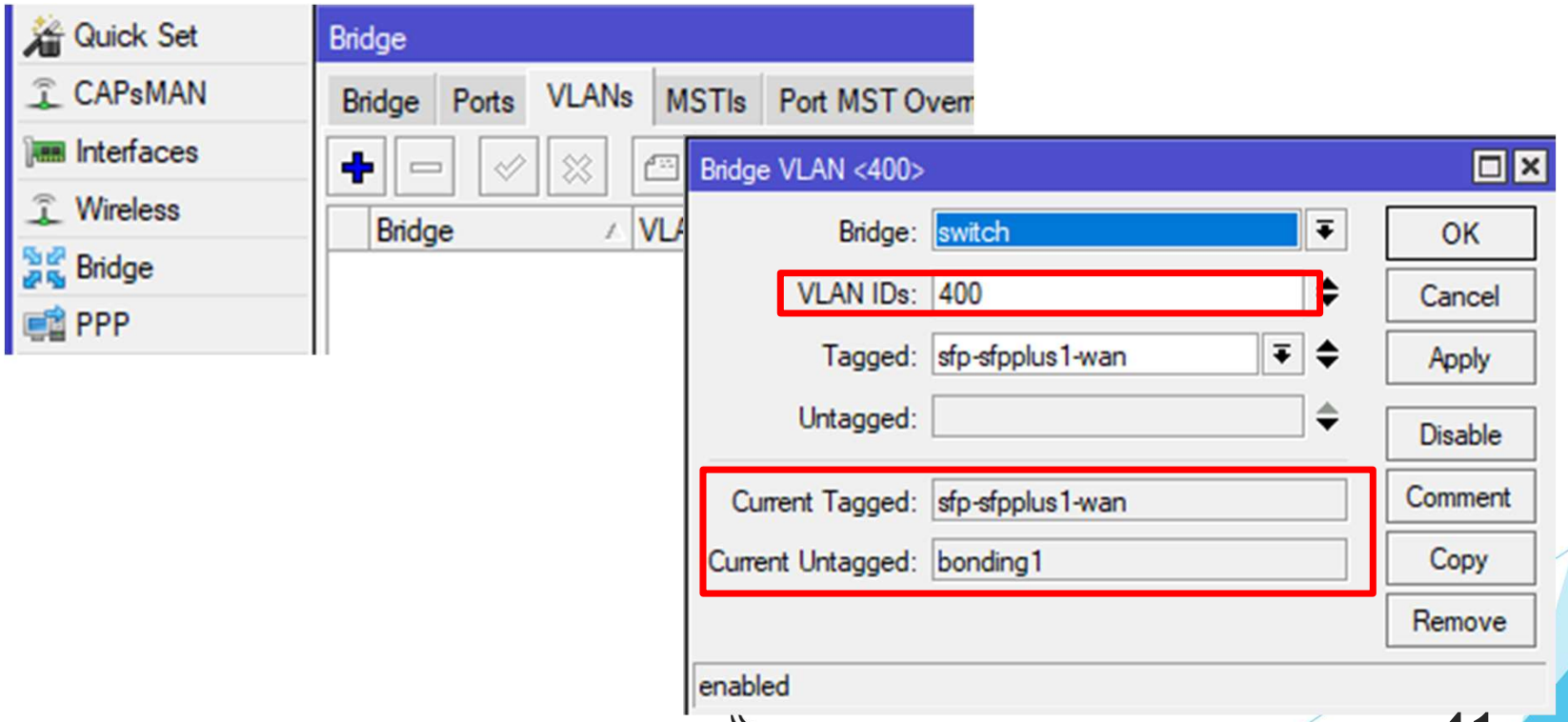


©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

LACP

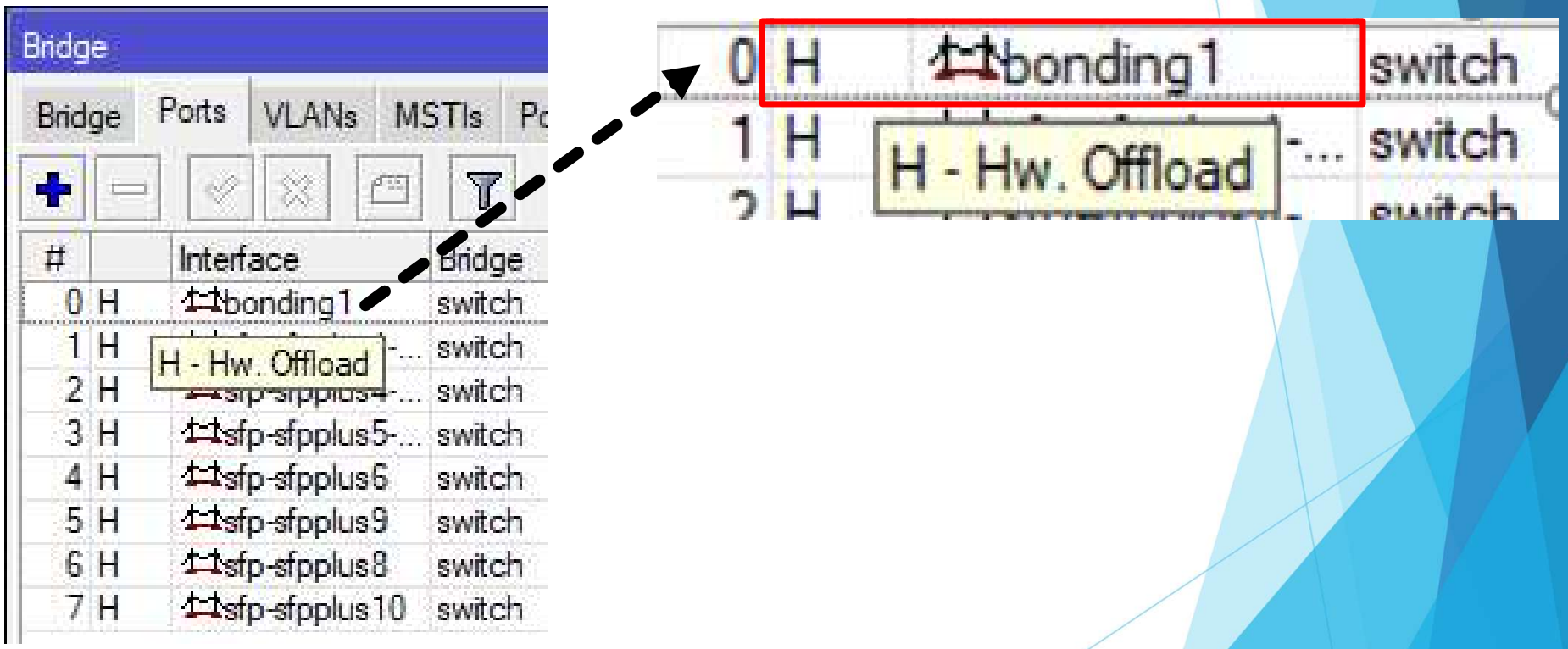
(Como fazer?)

4- Marcar a porta Trunk como VID 400 “tagged”



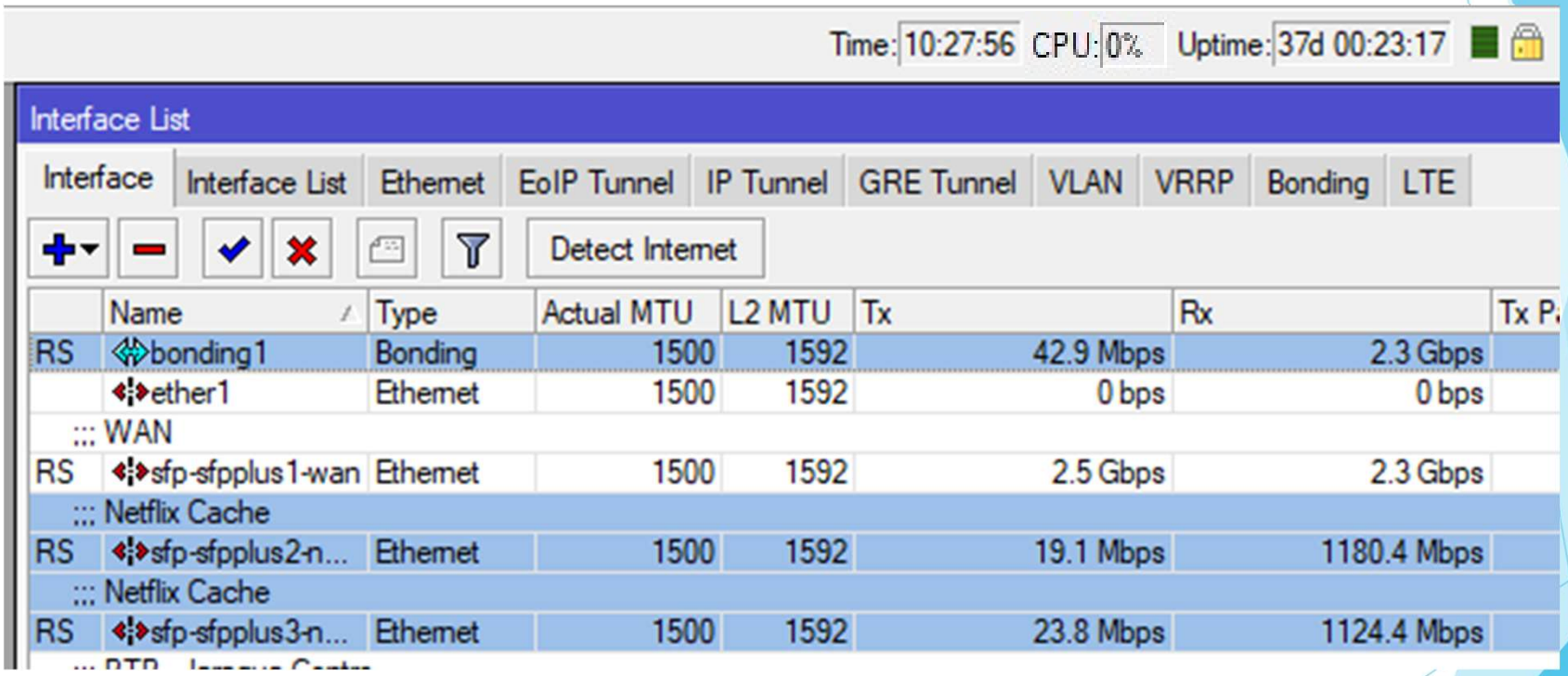
©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

LACP
(Resultado)



©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

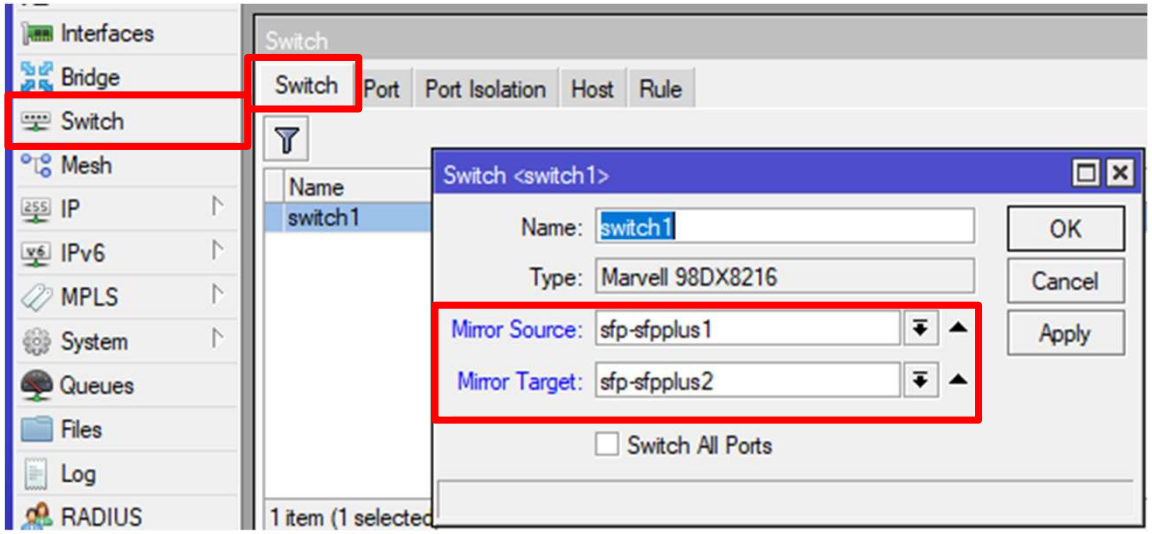
LACP
(Resultado)



©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

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.



©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

Port Mirroring (espelhamento de portas)

- Exemplo com base em VLANs

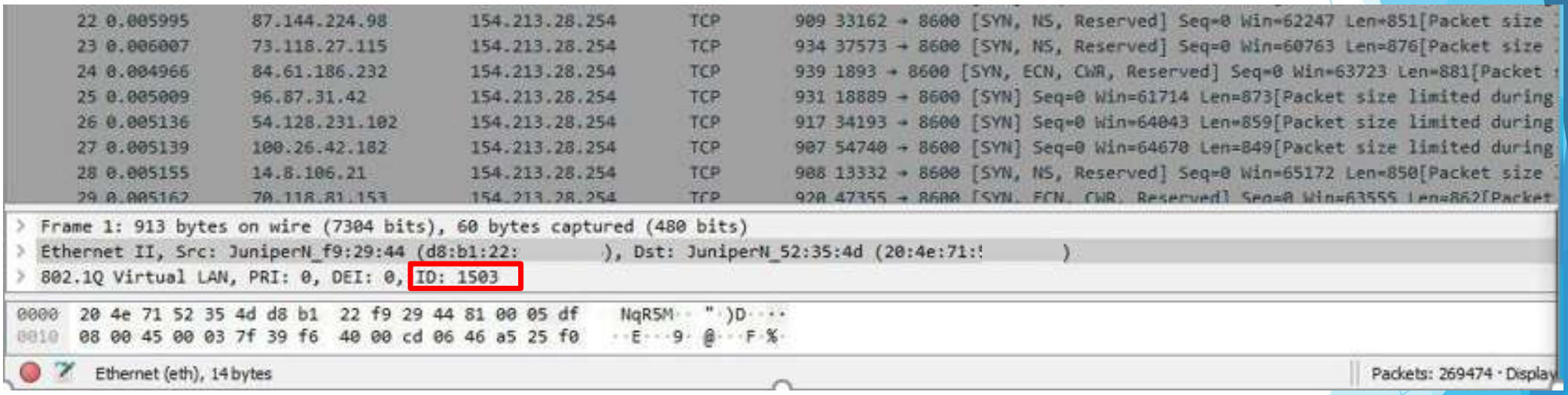
  - VLAN Based Mirroring

```
/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

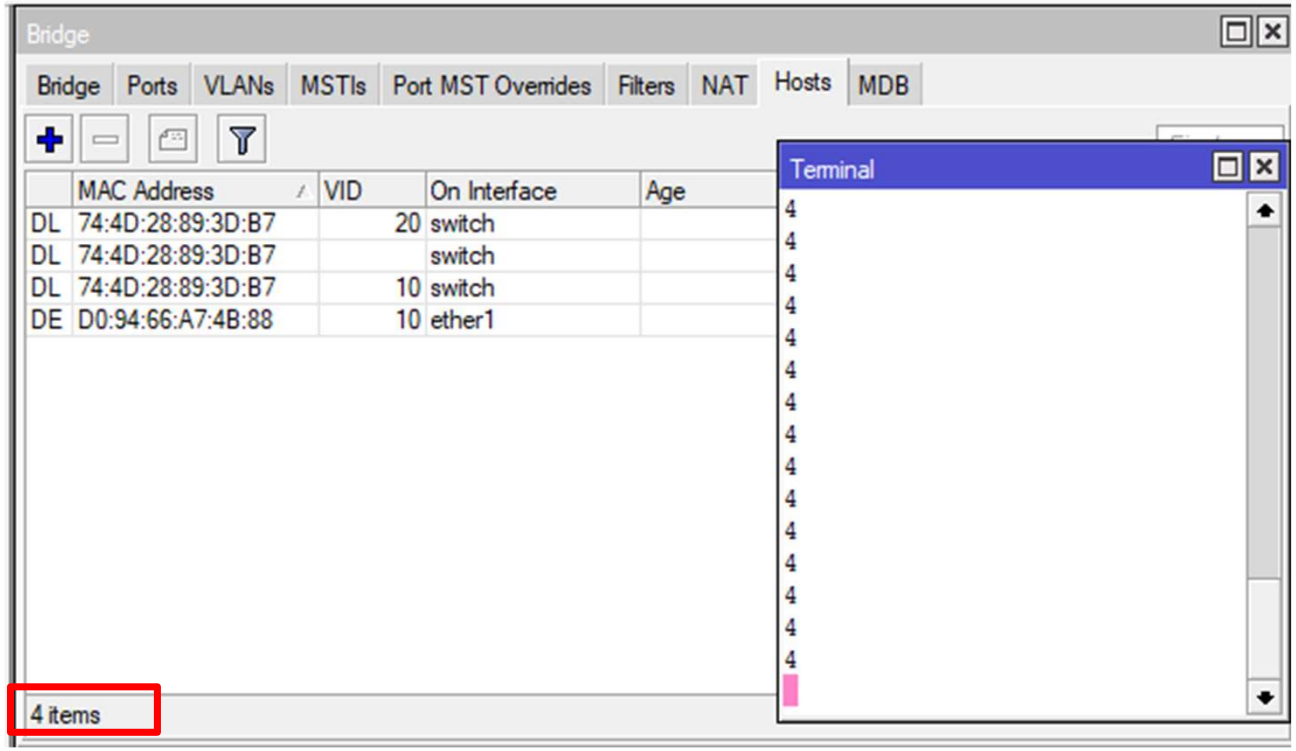
©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

Port Mirroring
(exemplo real de analise)



©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

Mac Flooding
(antes de um ataque)



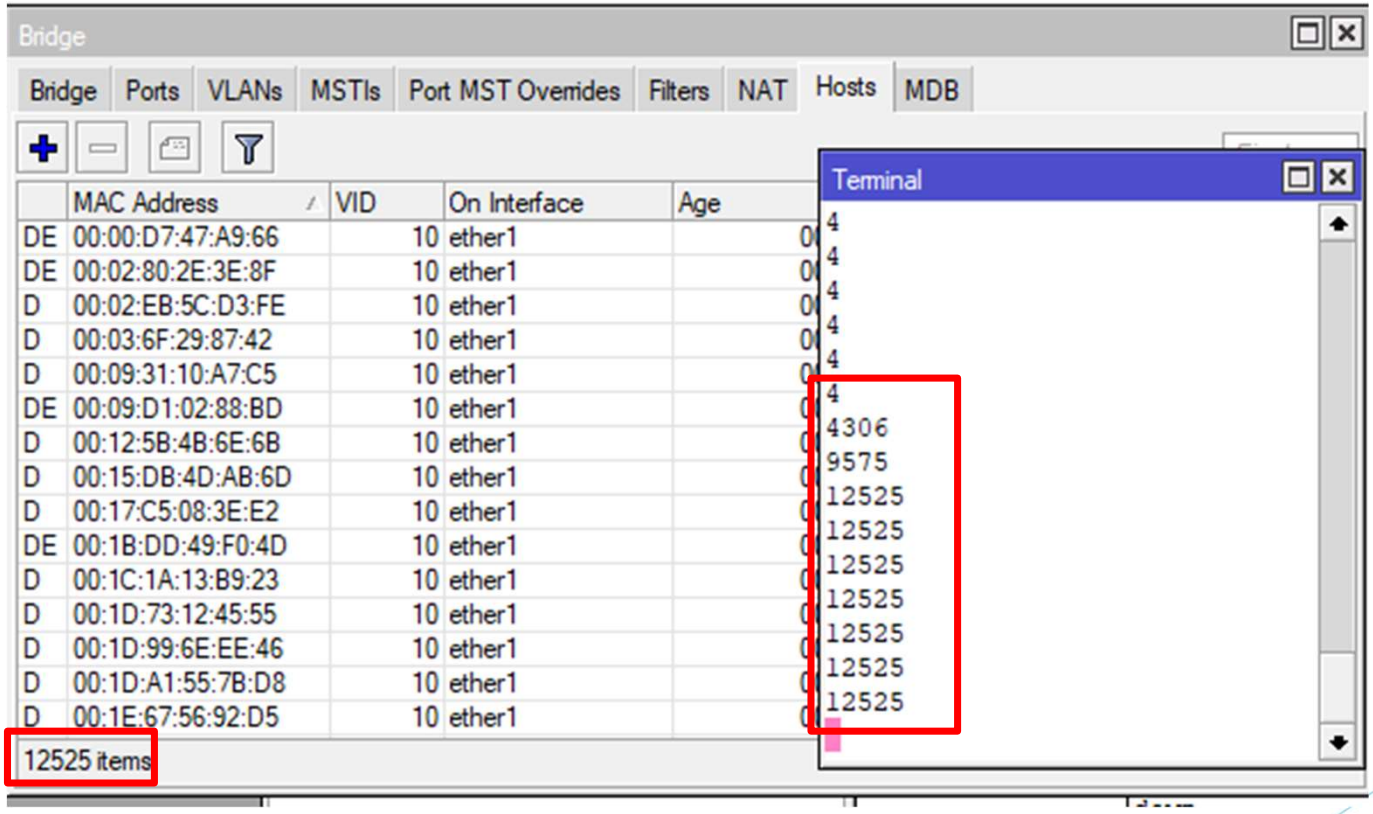
©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

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:~#
```

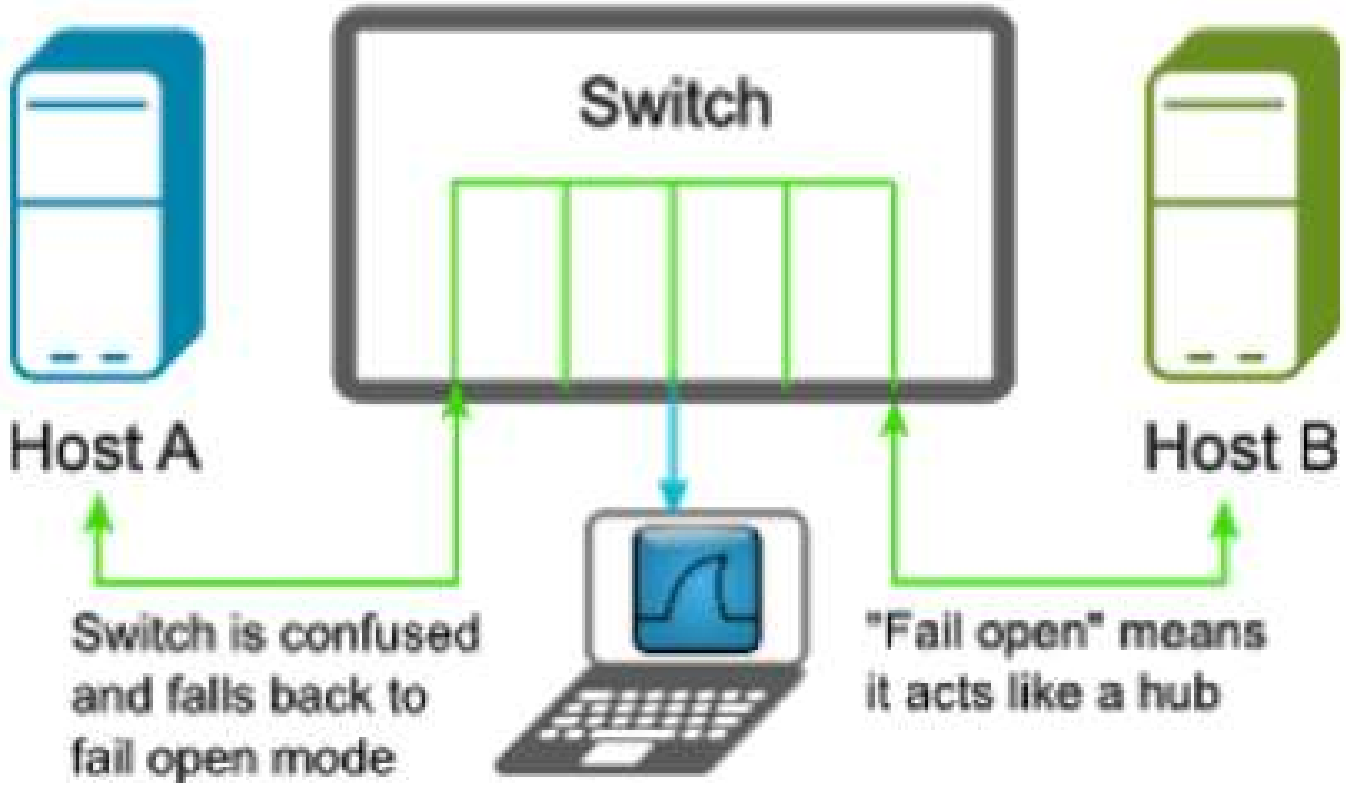

©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

Mac Flooding
(durante um ataque)



©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

Mac Flooding (após um ataque)



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

MikroTik

©2019 - Pro Networks - Material Por: João Aberto Barbosa de Oliveira

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
```

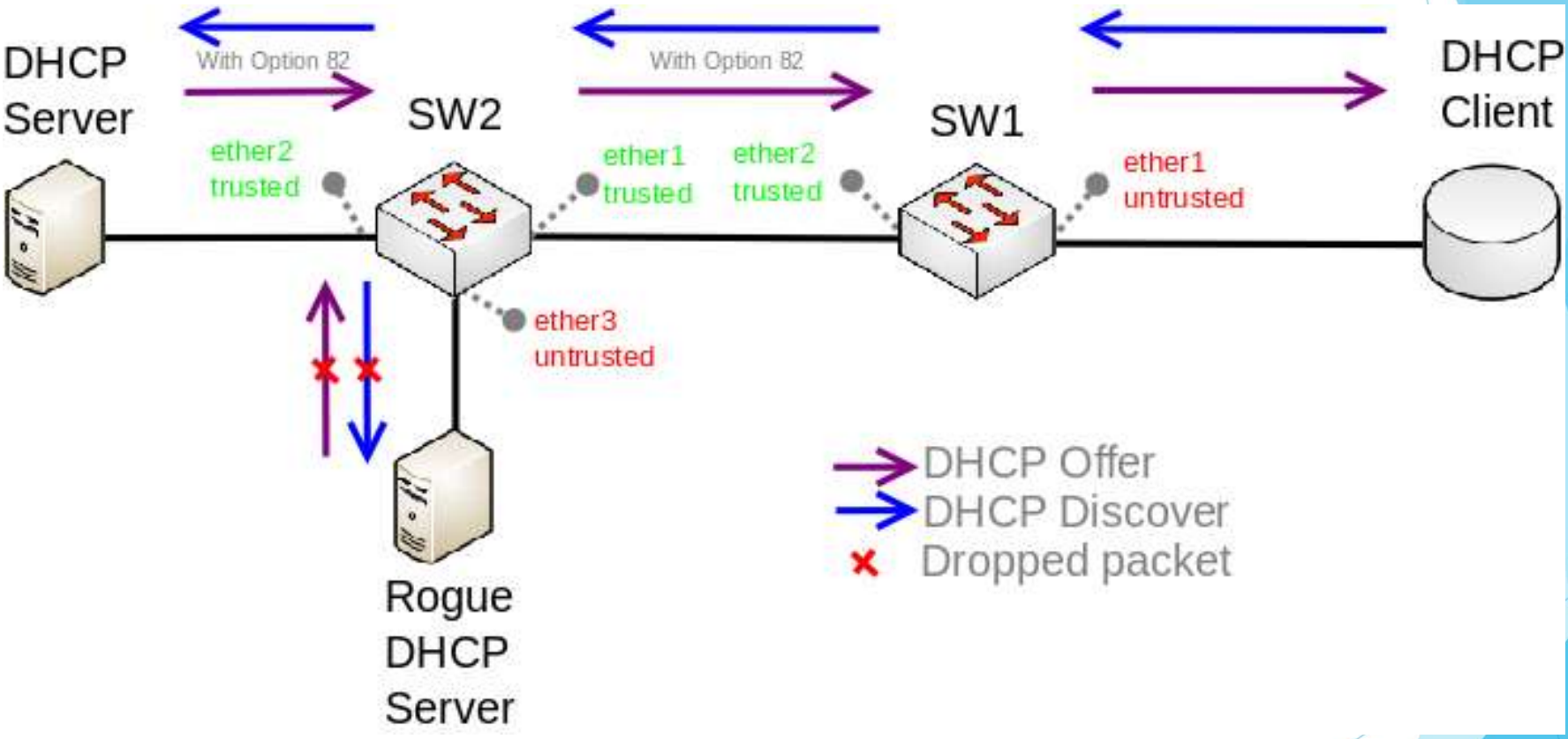
- Add a static hosts entry for `64:D1:54:81:EF:8E` (for egress traffic):

```
/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

©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

DHCP Snooping

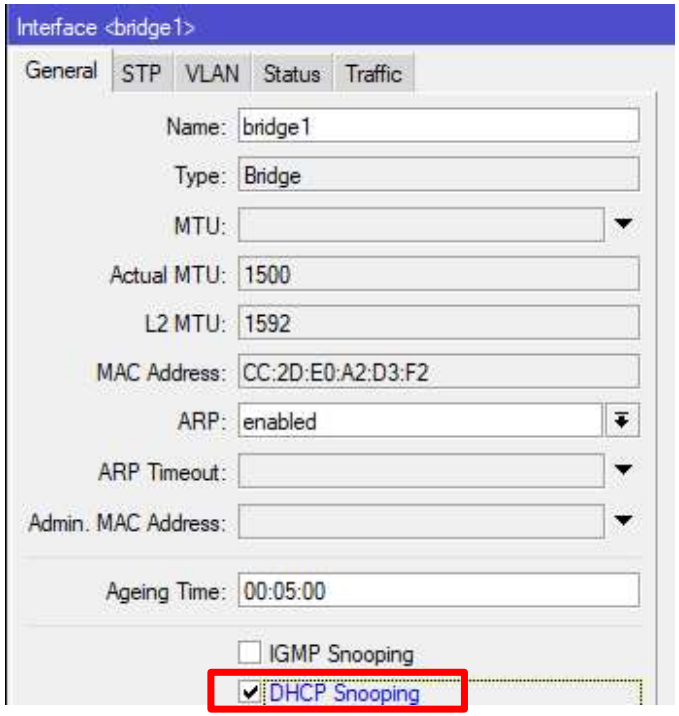


Fonte: https://wiki.mikrotik.com/wiki/File:Dhcp_snooping.png

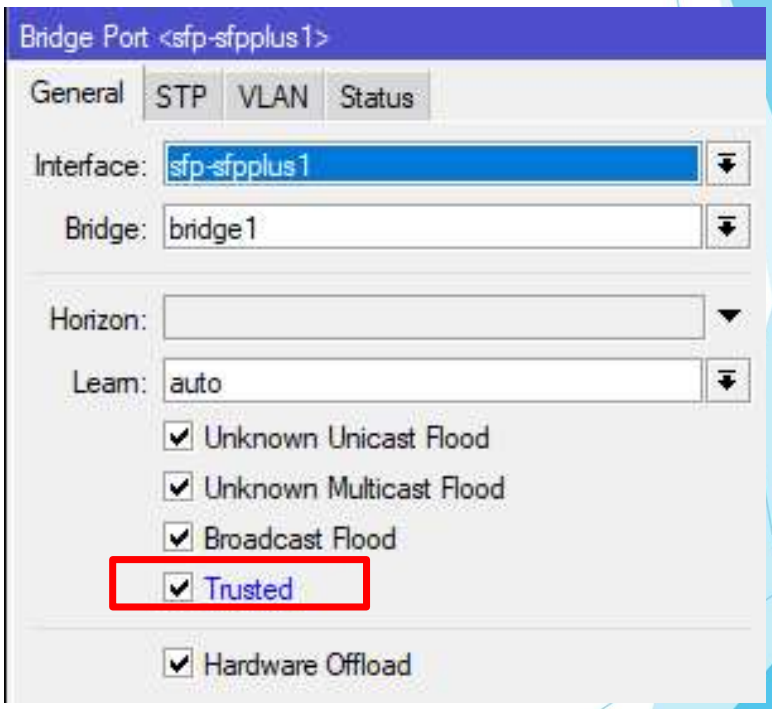
©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

DHCP Snooping

1- Habilitar a opção na Bridge



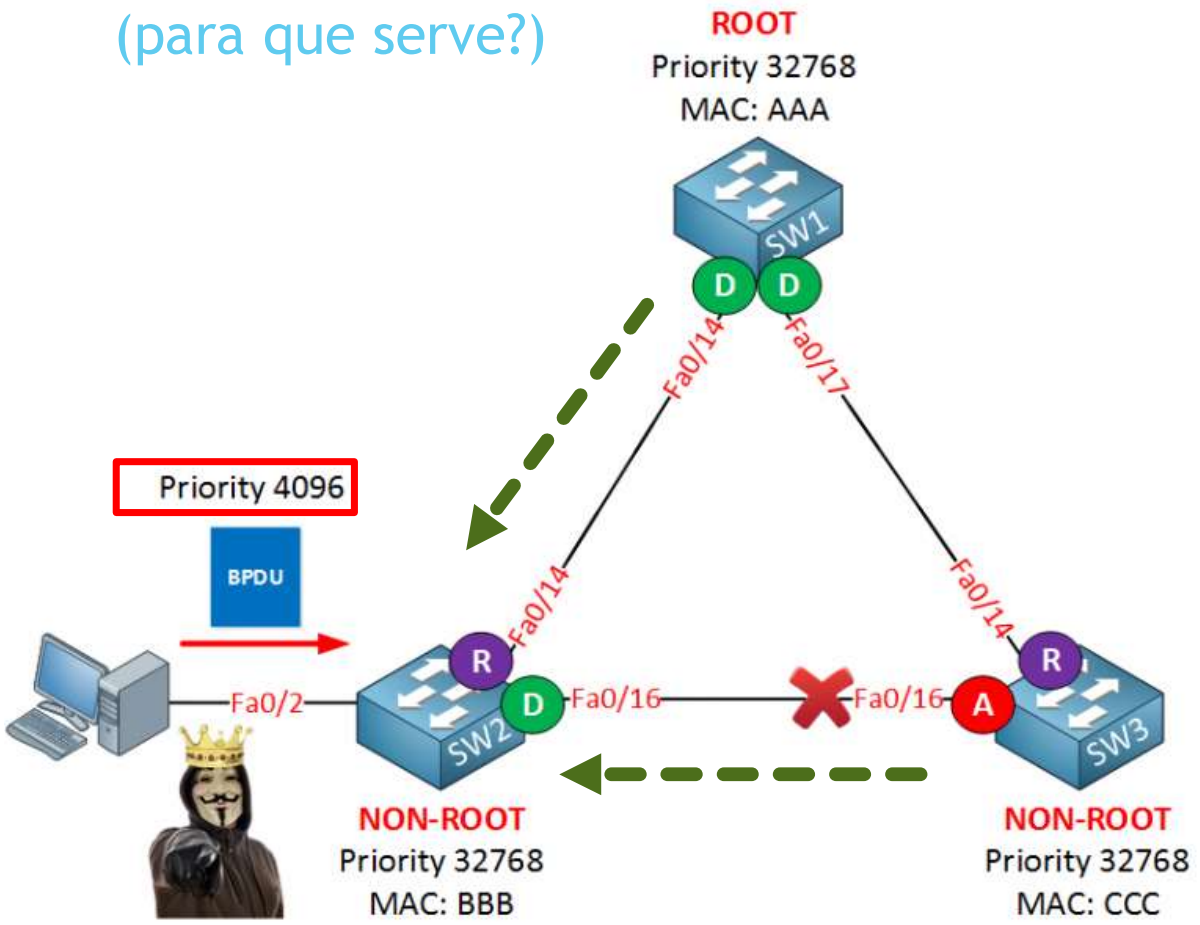
2- Marcar as portas que são confiáveis



©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

BPDU Guard

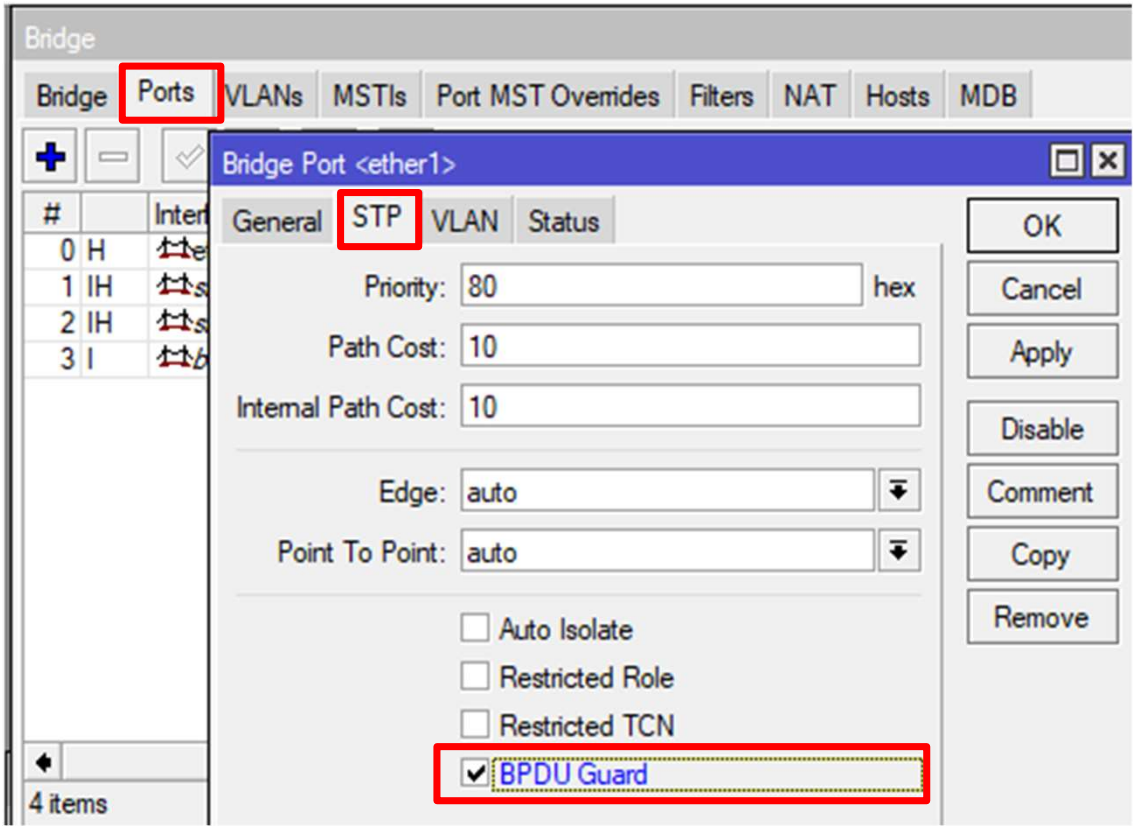
(para que serve?)



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

©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

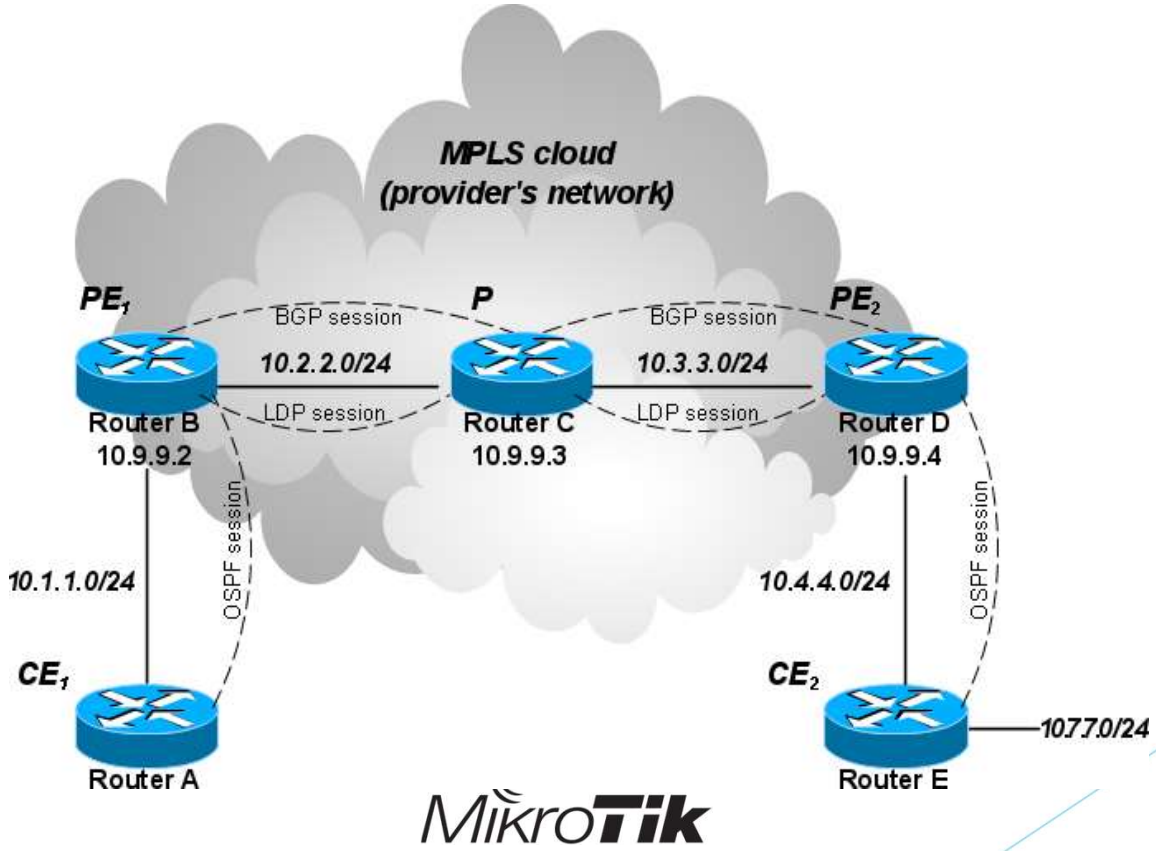
BPDU Guard



©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

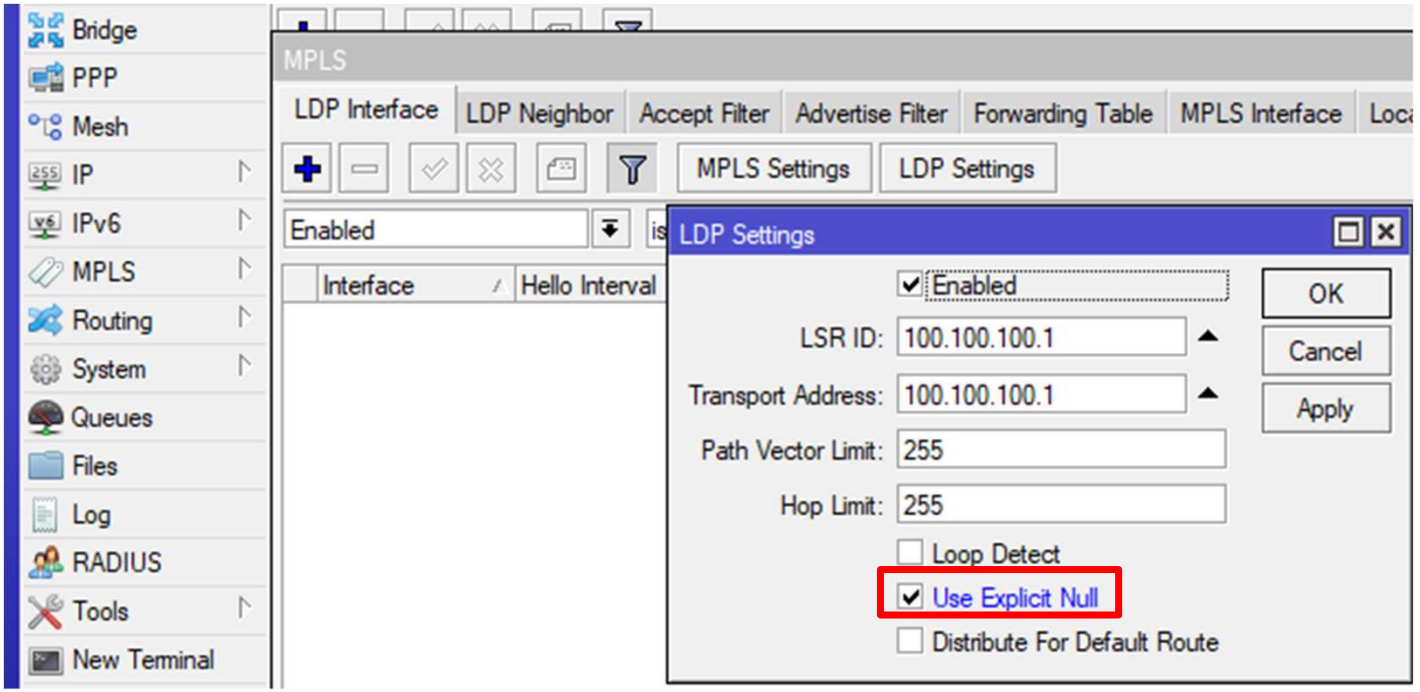
MPLS Hardware Offload

- 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”;



©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

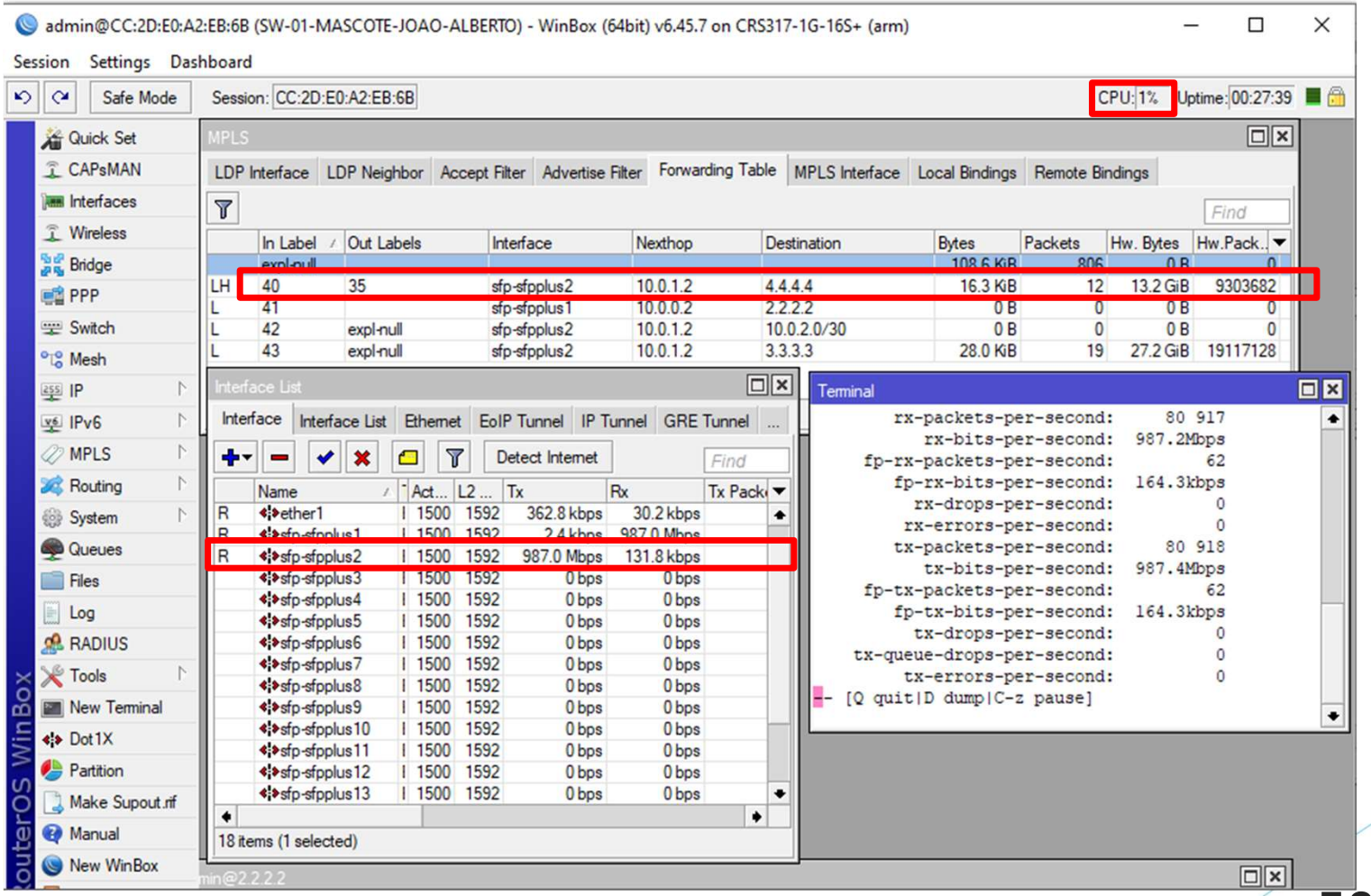
MPLS Hardware Offload

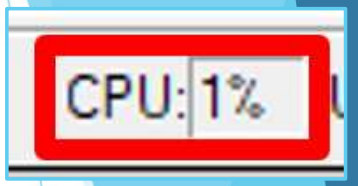


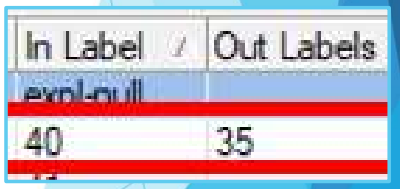
Atualmente este Recurso funciona apenas para as Routerboards:
CRS317-1G-16S+RM e CRS309-1G-8S+IN

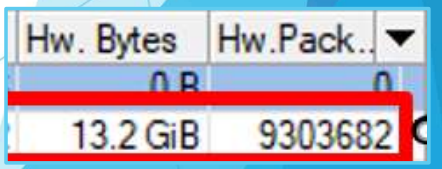
©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

MPLS Hardware Offload



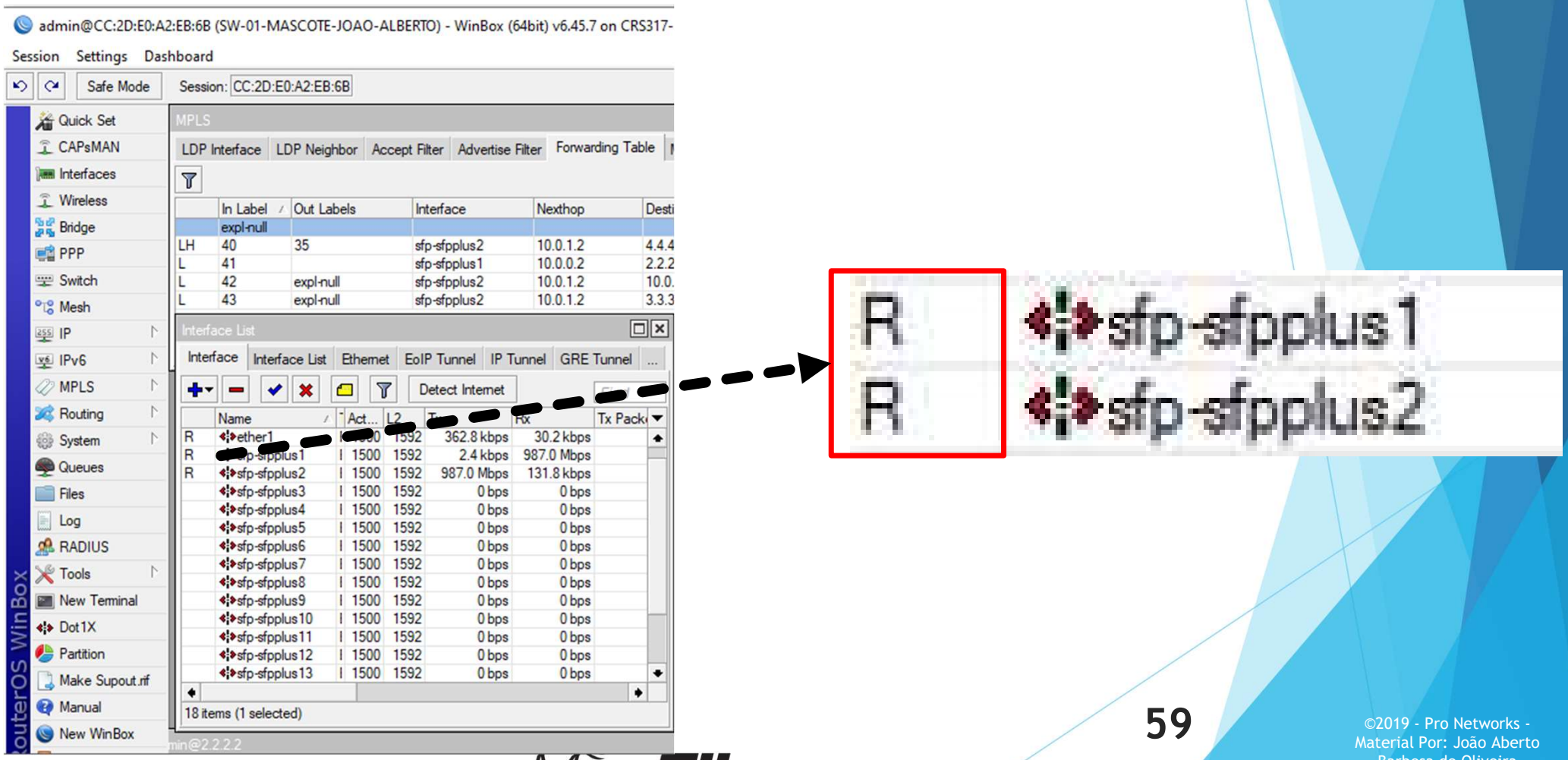






©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

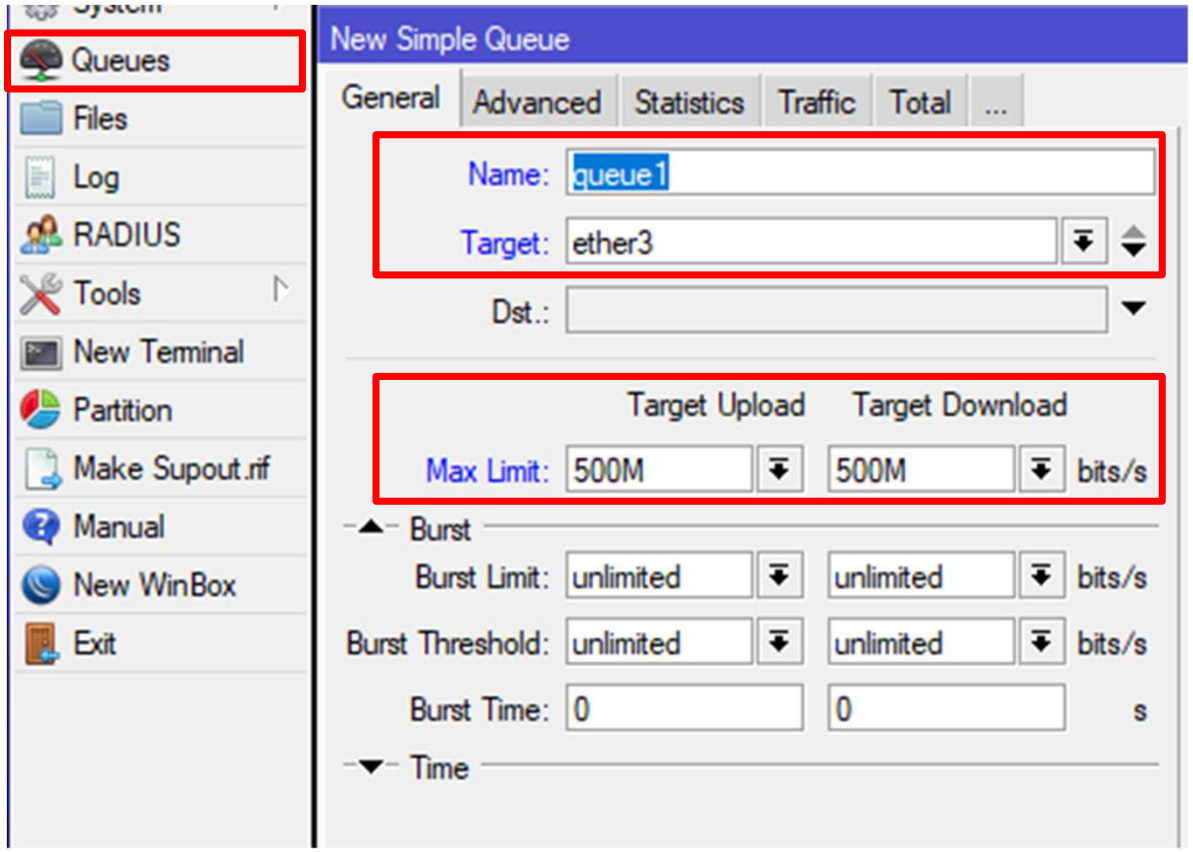
MPLS Hardware Offload



©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

Limitação de Tráfego

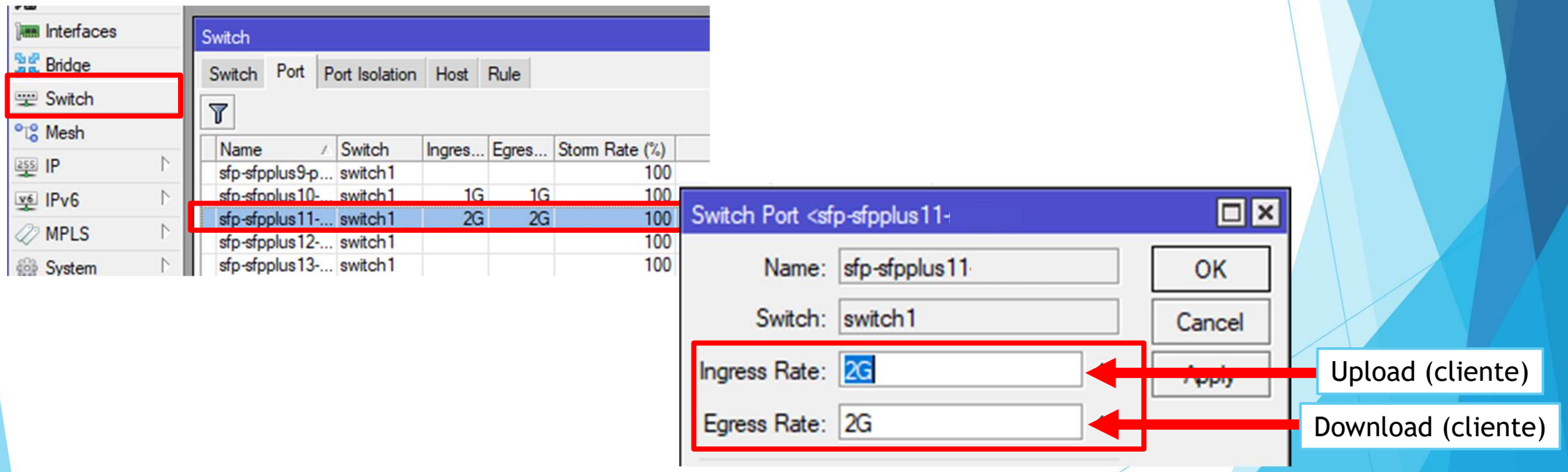
JAMAIS FAÇA ISSO NO SWITCH!



©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

Limitação de tráfego

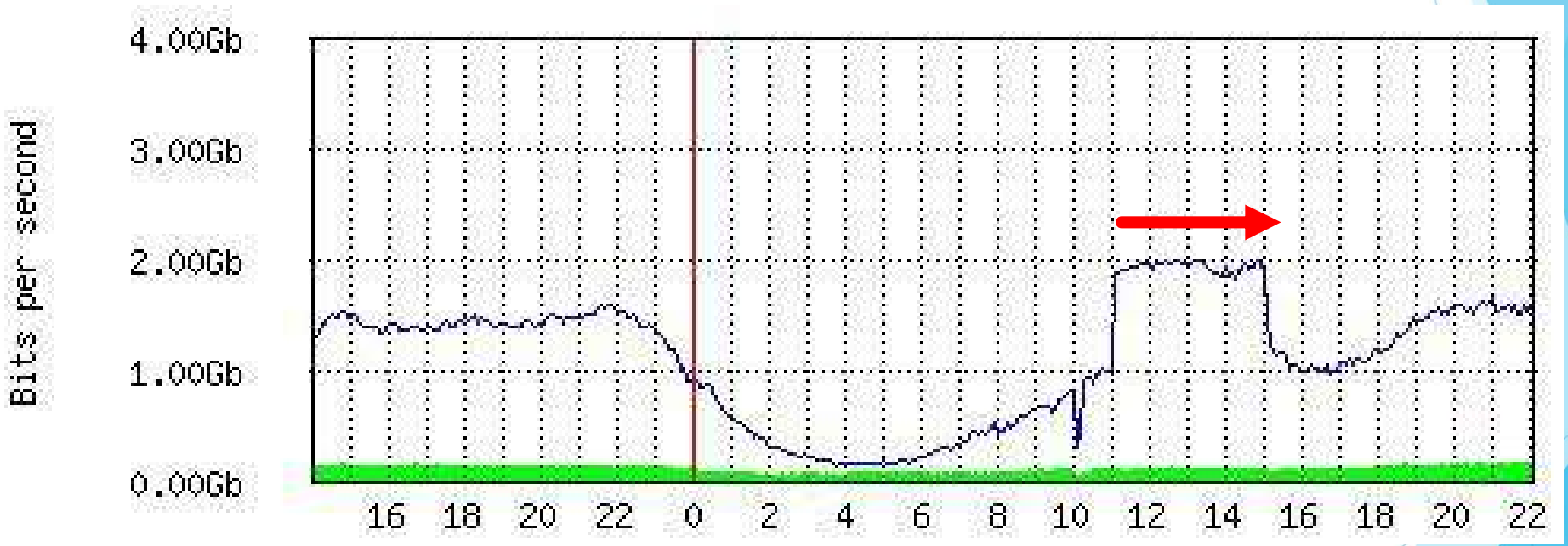
- Plenamente possível em Hardware;
- Possibilidade de limitar tráfego acima de 1Gbps com muita facilidade



MikroTik

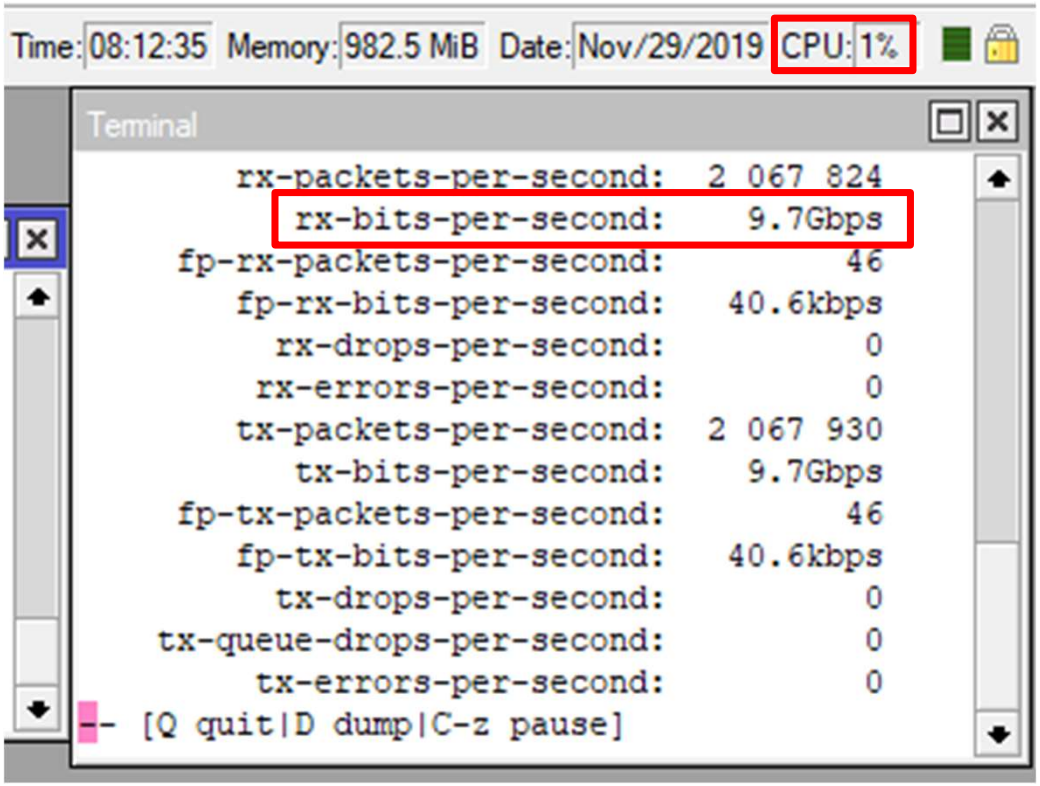
©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

Limitação de tráfego (resultado)



©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

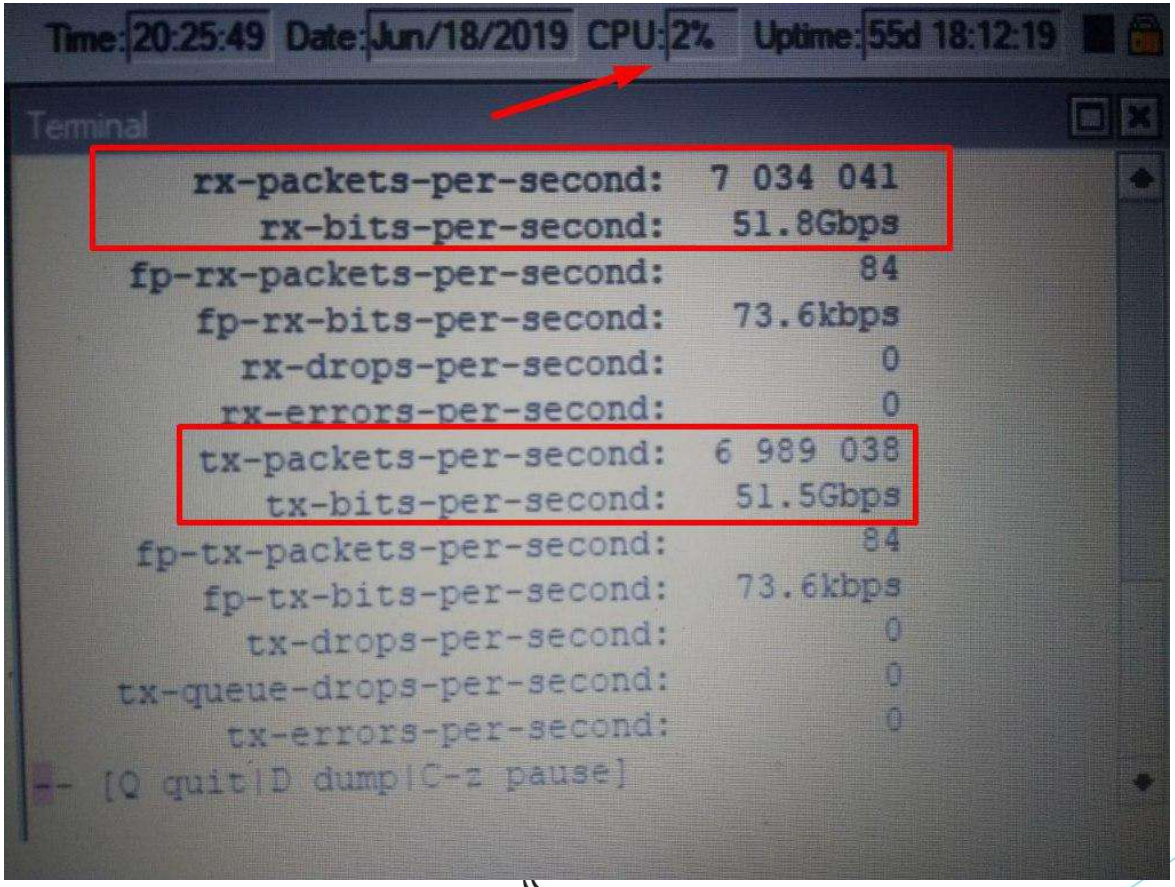
Resultado Real
(preservando o Hardware offload)



MikroTik

©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

Resultado Real
(preservando o Hardware offload)



©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

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+)

©2019 - Pro Networks -
Material Por: João Aberto
Barbosa de Oliveira

Dúvidas??
Obrigado!

pronetworks

Radar
INTERNET BANDA LARGA

MikroTik

Redes Brasil