

# Crescendo com Qualidade

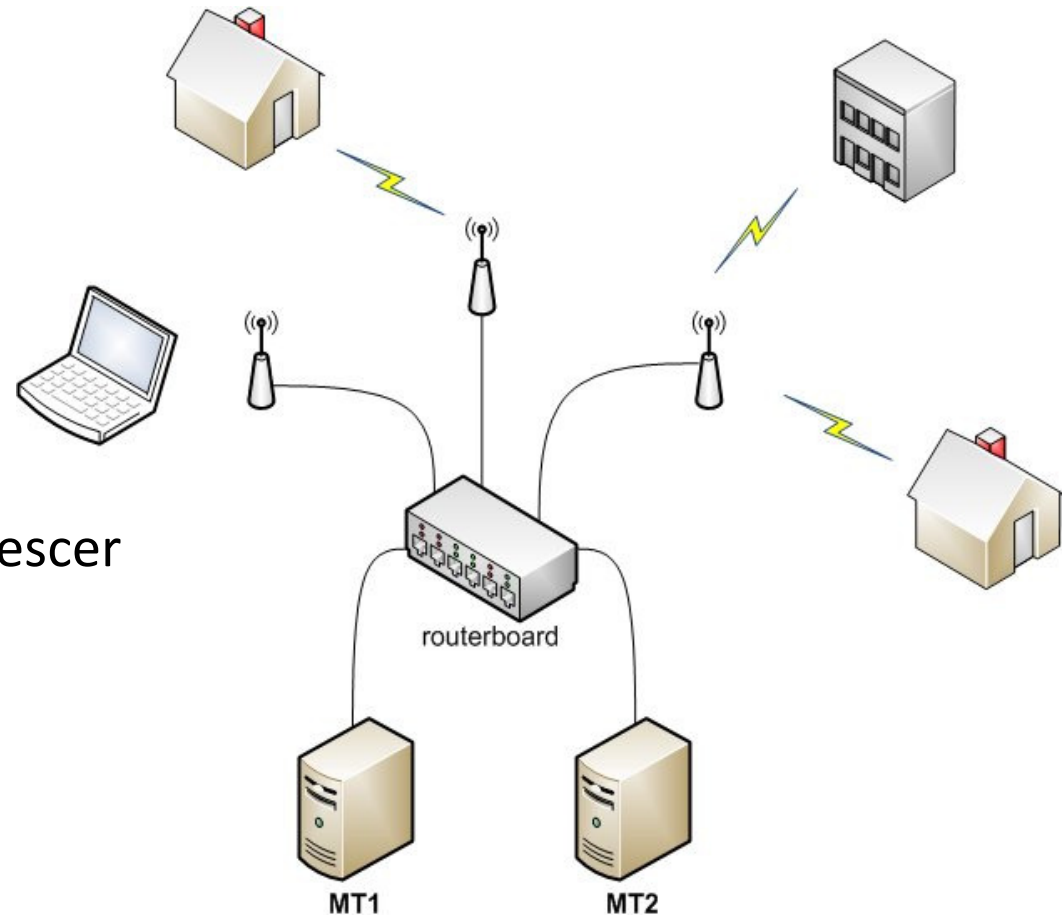
- Aperfeiçoando Bridges
- Evitando ARP spoofing
- Alta disponibilidade com VRRP



# Aperfeiçoando Bridges

## Principais impactos do crescimento

- Maior volume de tráfego
- Maior broadcast
- Maior risco devido a exposição

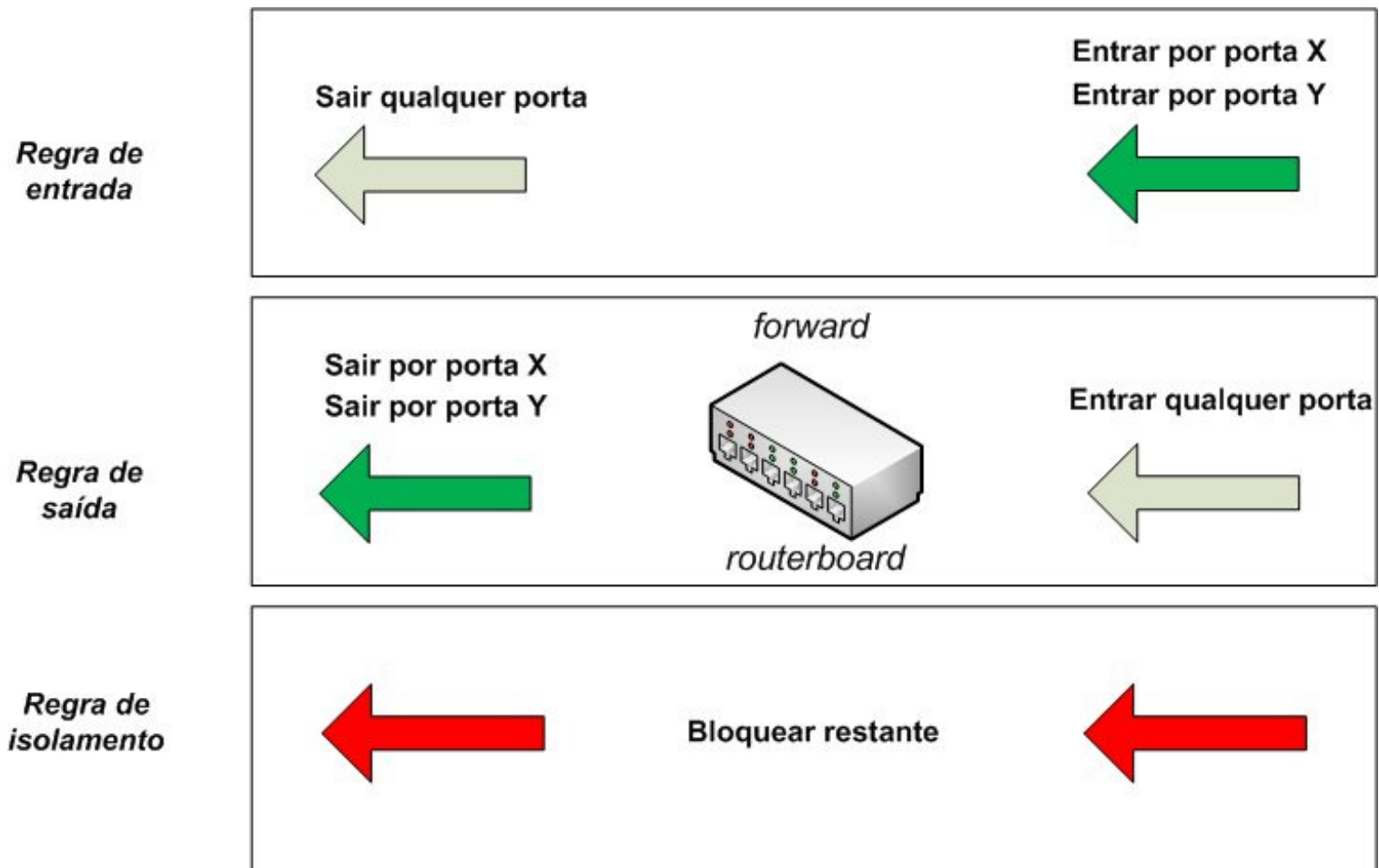


## Medidas primordiais para crescer

- Isolar comunicação intra-clientes
- Diminuir o broadcast
- Otimizar processamento total

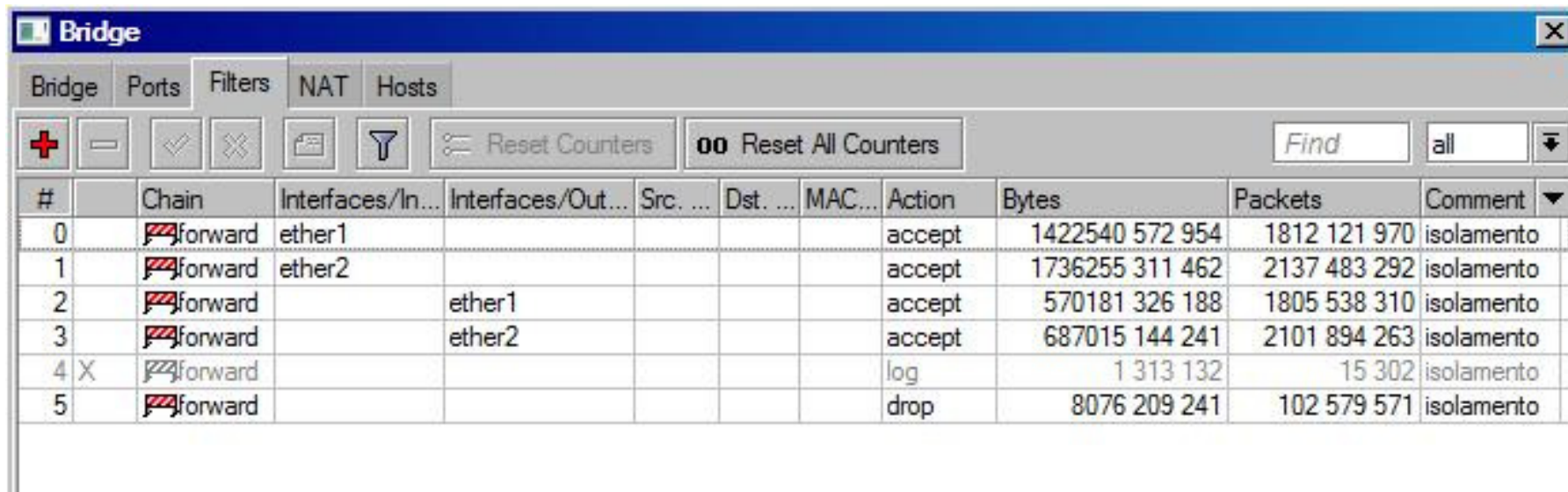
# Aperfeiçoando Bridges

## Isolamento com filtro



# Aperfeiçoando Bridges

## Isolamento com filtro



The screenshot shows the Mikrotik WinBox Bridge configuration window. The 'Filters' tab is active, displaying a table of filter rules. The table has columns for #, Chain, Interfaces/In..., Interfaces/Out..., Src..., Dst..., MAC..., Action, Bytes, Packets, and Comment. Five rules are listed, all with the action 'drop' and the comment 'isolamento'. Rule 4 is disabled, indicated by an 'X' in the first column.

#	Chain	Interfaces/In...	Interfaces/Out...	Src...	Dst...	MAC...	Action	Bytes	Packets	Comment
0	forward	ether1					accept	1422540 572 954	1812 121 970	isolamento
1	forward	ether2					accept	1736255 311 462	2137 483 292	isolamento
2	forward		ether1				accept	570181 326 188	1805 538 310	isolamento
3	forward		ether2				accept	687015 144 241	2101 894 263	isolamento
4 X	forward						log	1 313 132	15 302	isolamento
5	forward						drop	8076 209 241	102 579 571	isolamento

- reduz broadcast e exposição
- diminui comunicação entre clientes

# Aperfeiçoando Bridges

## Isolamento com filtro

Bloquear roteamento entre clientes



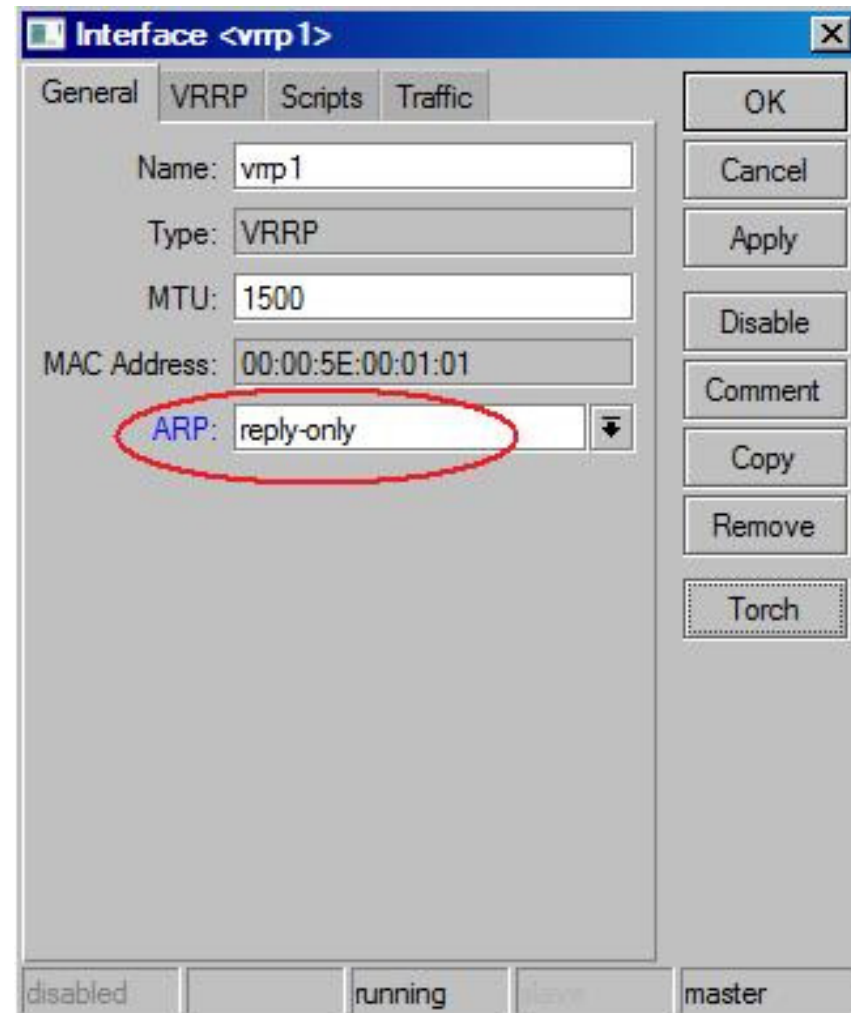
```
add action=drop chain=forward comment=Intra-Access disabled=no \  
dst-address-list=clientes src-address-list=clientes
```

# Evitando ARP spoofing

## Tabela ARP vs. Reply Only

A configuração da tabela arp do mikrotik se torna estática e fiel ao ARP (ip/mac) do cliente. Esse método simplesmente ignora as entradas ARP falsas, causada pelo ARP spoofing, garantindo maior qualidade.

*Não recomendado para redes grandes ou em crescimento, visto que exige cadastramento manual de todos os clientes na Tabela ARP do Mikrotik.*



# Evitando ARP spoofing

## Tabela ARP vs. DHCP lease

A configuração da tabela arp do mikrotik se torna fiel e evita confusões na rede, causada pelo 'envenenamento' ARP.

*Assim que o cliente recebe o ip, automaticamente é cadastrado seu ARP (ip/mac) na Tabela ARP do Mikrotik. Recomendado para todos os casos.*

DHCP Server <dhcp 1>

Name: dhcp1

Interface: vmp1

Relay:

Lease Time: 01:00:00

Address Pool: pool1

Src. Address:

Delay Threshold:

Authoritative: yes

Bootp Support

Add ARP For Leases

Always Broadcast

Use RADIUS

OK

Cancel

Apply

Disable

Copy

Remove

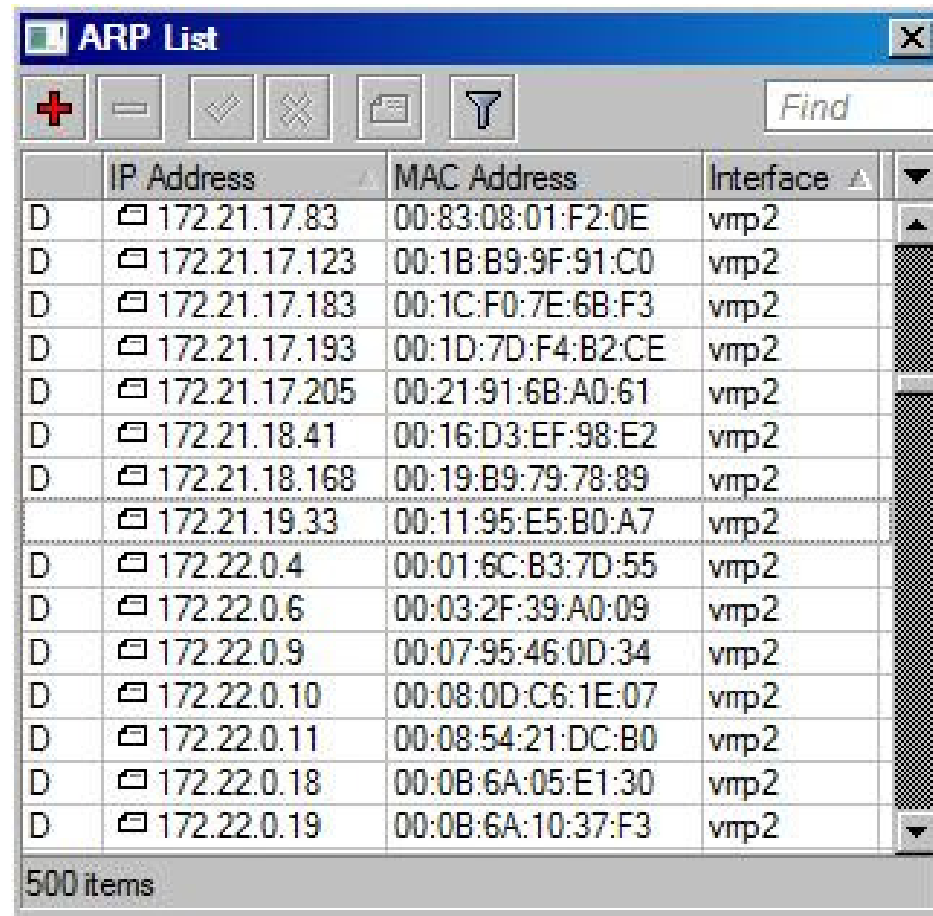
disabled

# Evitando ARP spoofing

## Algumas Considerações

Com o uso do Hotspot, a configuração do Reply Only na interface torna-se inútil.

*O Hotspot autoriza a comunicação do servidor com entradas não fixadas na Tabela ARP. Porém elas não terão o mesmo tratamento que as fixadas e poderão sofrer com o ARP spoofing na rede.*



The screenshot shows a window titled "ARP List" with a toolbar containing icons for adding, deleting, and filtering entries, along with a "Find" search box. The main area is a table with the following data:

	IP Address	MAC Address	Interface
D	172.21.17.83	00:83:08:01:F2:0E	vmp2
D	172.21.17.123	00:1B:B9:9F:91:C0	vmp2
D	172.21.17.183	00:1C:F0:7E:6B:F3	vmp2
D	172.21.17.193	00:1D:7D:F4:B2:CE	vmp2
D	172.21.17.205	00:21:91:6B:A0:61	vmp2
D	172.21.18.41	00:16:D3:EF:98:E2	vmp2
D	172.21.18.168	00:19:B9:79:78:89	vmp2
	172.21.19.33	00:11:95:E5:B0:A7	vmp2
D	172.22.0.4	00:01:6C:B3:7D:55	vmp2
D	172.22.0.6	00:03:2F:39:A0:09	vmp2
D	172.22.0.9	00:07:95:46:0D:34	vmp2
D	172.22.0.10	00:08:0D:C6:1E:07	vmp2
D	172.22.0.11	00:08:54:21:DC:B0	vmp2
D	172.22.0.18	00:0B:6A:05:E1:30	vmp2
D	172.22.0.19	00:0B:6A:10:37:F3	vmp2

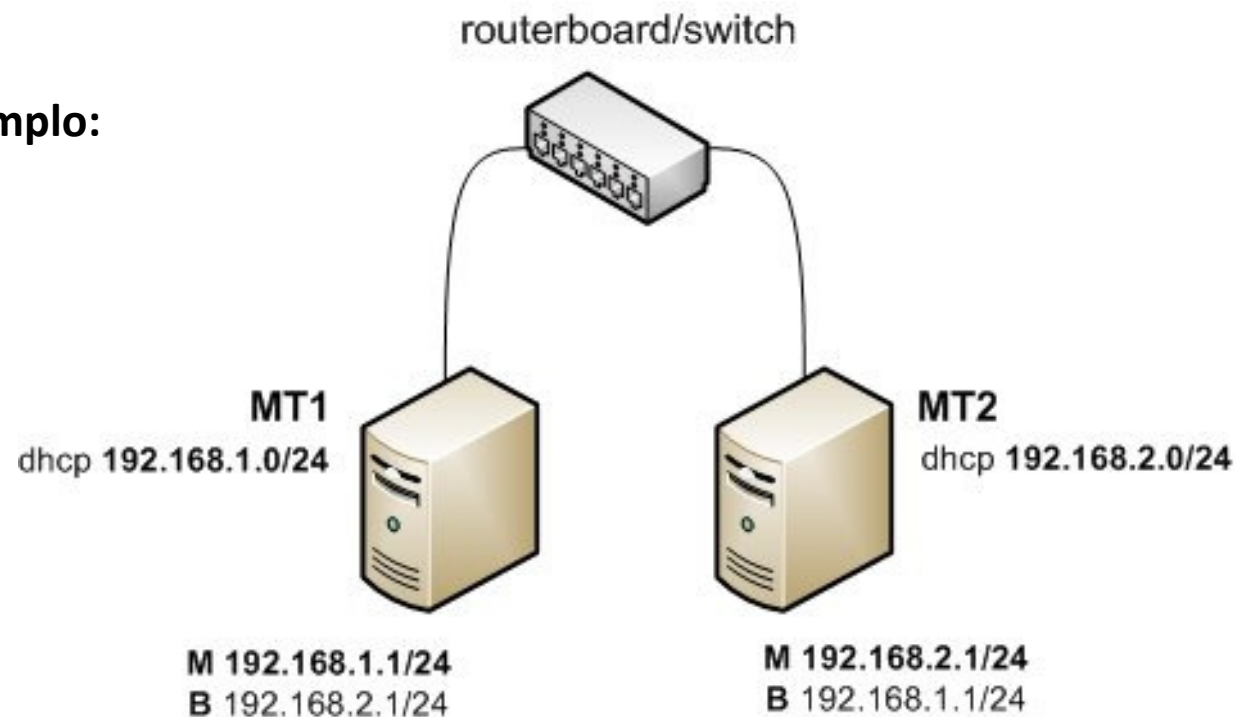
500 items

# Alta Disponibilidade

## VRRP

O objetivo é que cada servidor possa assumir todos os outros em caso de falha. Para tanto, todas as outras configurações de firewall, filas etc. devem ser respeitadas para a perfeita continuidade dos serviços.

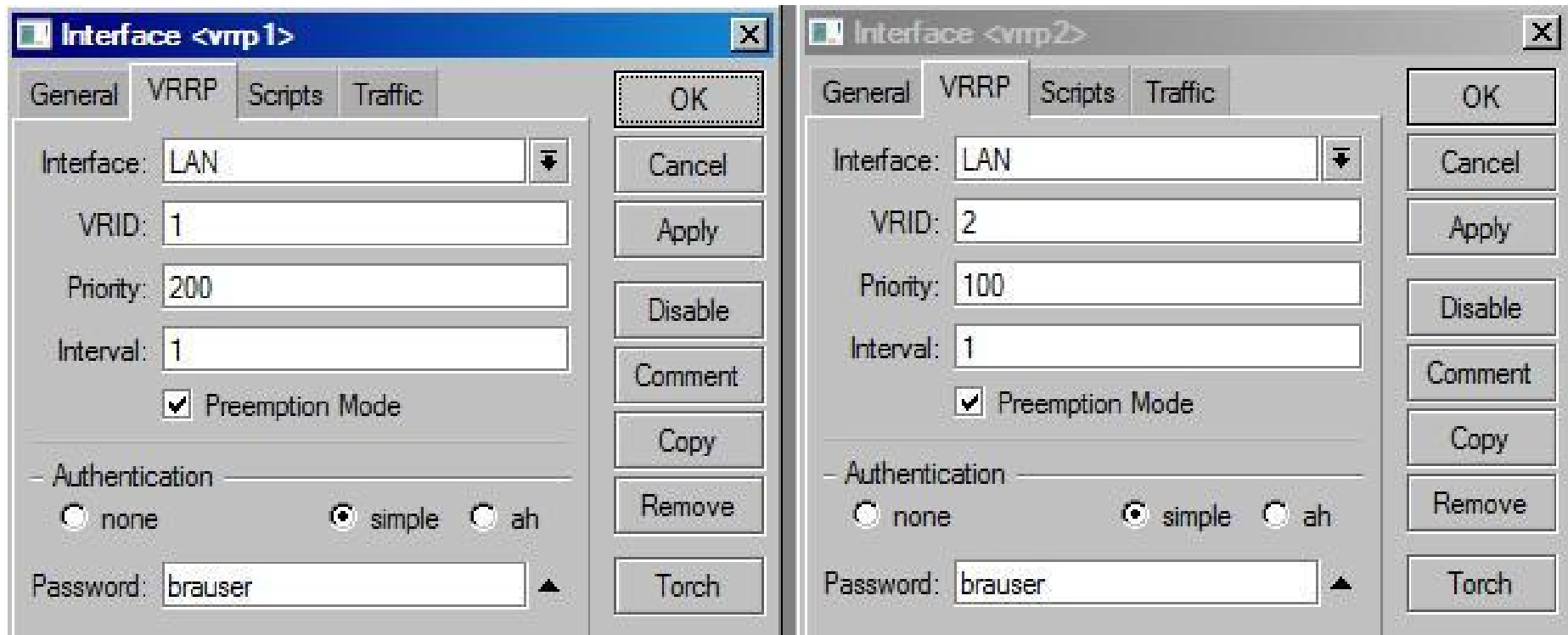
### Cenário exemplo:



# Alta Disponibilidade

## VRRP - configuração

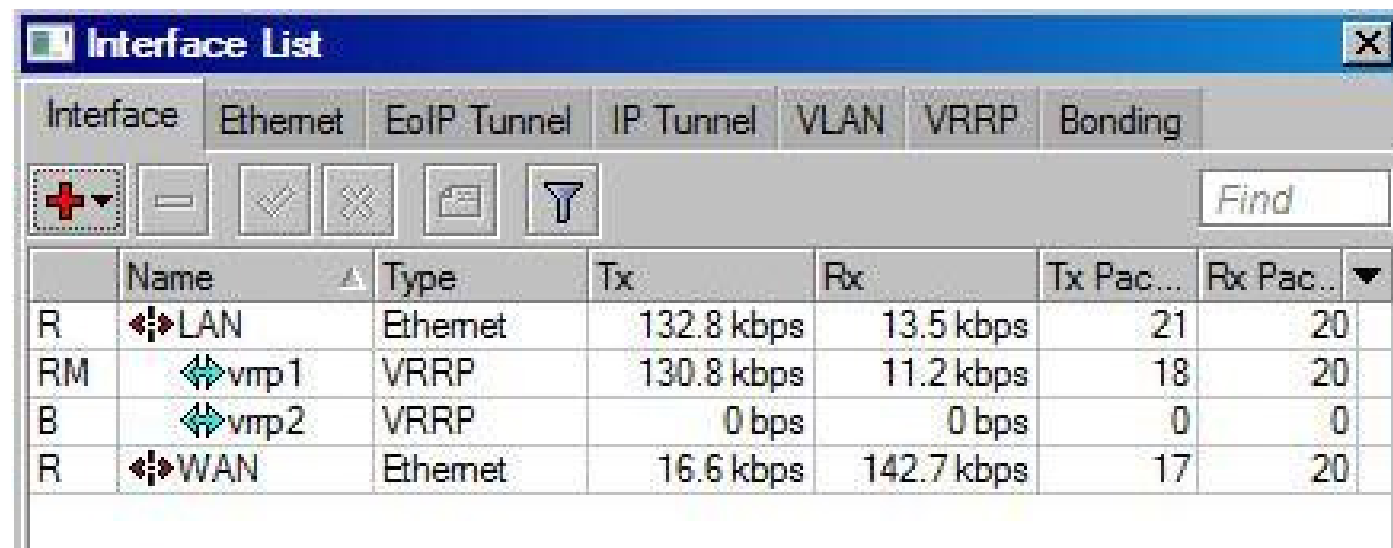
O **VRID** identifica o servidor a ser representado pela interface virtual – ela receberá o mesmo ip em todas as máquinas. **Priority** determina a interface master e a ordem de substituição em caso de *fail-over*. A autenticação do protocolo é recomendada.



# Alta Disponibilidade

## VRRP - interfaces

A interface de backup só é elegida a master quando seu respectivo servidor fica incomunicável (por tempo determinado - em **Interval**) e ela tem a prioridade máxima atual da rede.



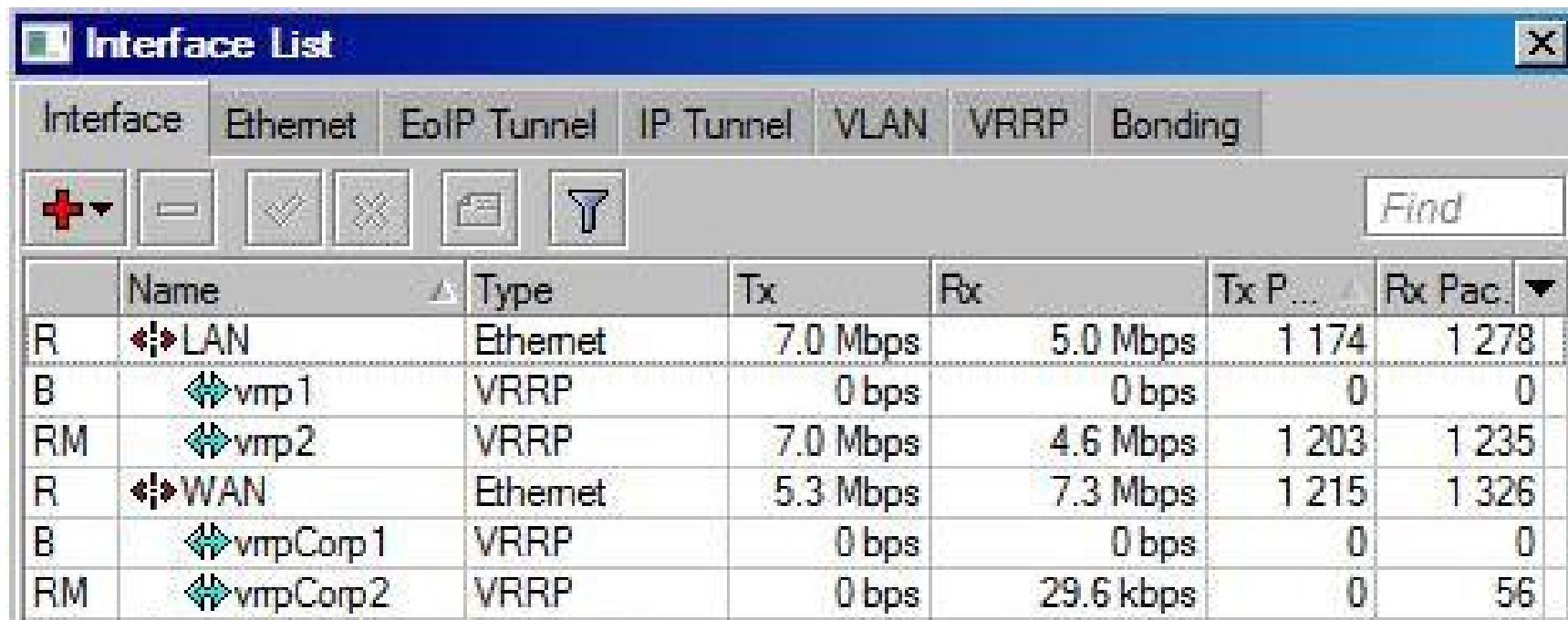
The screenshot shows a window titled "Interface List" with a tabbed interface. The "VRRP" tab is selected. Below the tabs is a toolbar with icons for adding, deleting, and filtering interfaces, along with a "Find" search box. The main area contains a table with the following data:

	Name	Type	Tx	Rx	Tx Pac...	Rx Pac..
R	LAN	Ethernet	132.8 kbps	13.5 kbps	21	20
RM	vmp1	VRRP	130.8 kbps	11.2 kbps	18	20
B	vmp2	VRRP	0 bps	0 bps	0	0
R	WAN	Ethernet	16.6 kbps	142.7 kbps	17	20

# Alta Disponibilidade

## VRRP - corporativo

É possível configurar o VRRP na interface de saída para garantir a alta disponibilidade para ips públicos. Visto que poderão existir rotas no(s) router(s) de borda para a faixa de ips em questão, a interface virtual garantirá sua integridade.



	Name	Type	Tx	Rx	Tx P...	Rx Pac.
R	LAN	Ethernet	7.0 Mbps	5.0 Mbps	1 174	1 278
B	vmp 1	VRRP	0 bps	0 bps	0	0
RM	vmp 2	VRRP	7.0 Mbps	4.6 Mbps	1 203	1 235
R	WAN	Ethernet	5.3 Mbps	7.3 Mbps	1 215	1 326
B	vmpCorp 1	VRRP	0 bps	0 bps	0	0
RM	vmpCorp 2	VRRP	0 bps	29.6 kbps	0	56

# Alta Disponibilidade

## **VRRP - considerações**

O VRRP funciona perfeitamente com Hotspots no mesmo barramento e auxiliam o provedor a balancear sua carga através do DHCP-Server.  
Tal aplicação flexibiliza a rede tornando seu crescimento fácil e transparente!

# Crescendo com Qualidade

## **Lembrem sempre de:**

- Reduzir ao máximo o tamanho das bridges.
- Usar roteamento sempre que possível.
- Procurar isolar o tráfego do cliente desde sua estação até o servidor final.

## **Lembrem sempre que:**

- Quanto maior a bridge, mais cuidado deve-se ter.
- O Hotspot é seu aliado para acompanhamento da rede.
- Basta 1 servidor DHCP por máquina em VRRP, independente de quantos servidores estiver representando.

# Crescendo com Qualidade

**Obrigado e sucesso a todos!**

Leonardo C. Rosa – Consultor em TI

[leonardo@brauser.com.br](mailto:leonardo@brauser.com.br) [msn]

(71) 2626-3735 / 9972-8523



BR08468

Leonardo C. Rosa  
BRAUSER, Brazil



*MikroTik*

