

Boas práticas para obter o máximo de desempenho com equipamentos da MikroTik.



Redes Brasil

Informações sobre o palestrante

Nome: Francisco Ribeiro de Souza Neto

Resumo:

- Trabalha com telecomunicações desde 2005.
- Possui todas as certificações da MikroTik (MTCNA,MTCRE,MTCWE,MTCINE,MTCTCE,MTCUME,MTCIPv6E).
- Consultor e instrutor oficial MikroTik.
- Consultor e instrutor oficial Ubiquiti.

Objetivos da apresentação

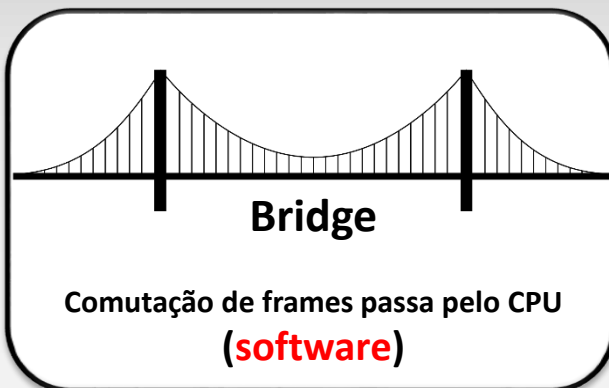
- Mostrar uma série de funcionalidades e recursos que irão te ajudar a usar 100% da capacidade de seus equipamentos.
- Fazer uma explicação detalhada sobre cada um dos tópicos, para que você consiga definir quando e onde utilizar tais recursos.



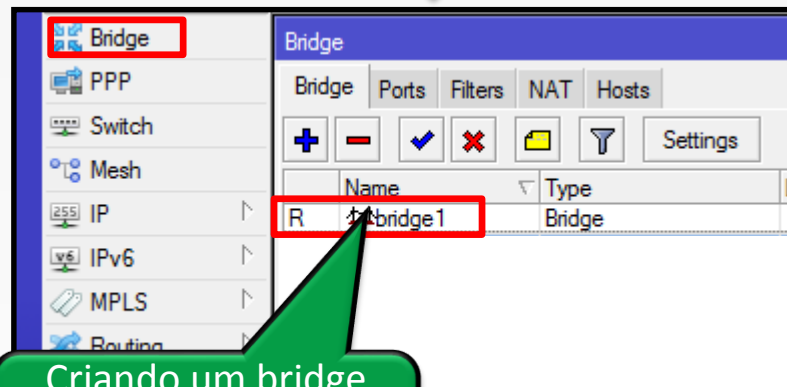
Agenda

- Bridge X Switch;
- Connection tracking (conntrack);
- Fasttrack;
- Tabela RAW;
- FastPath;

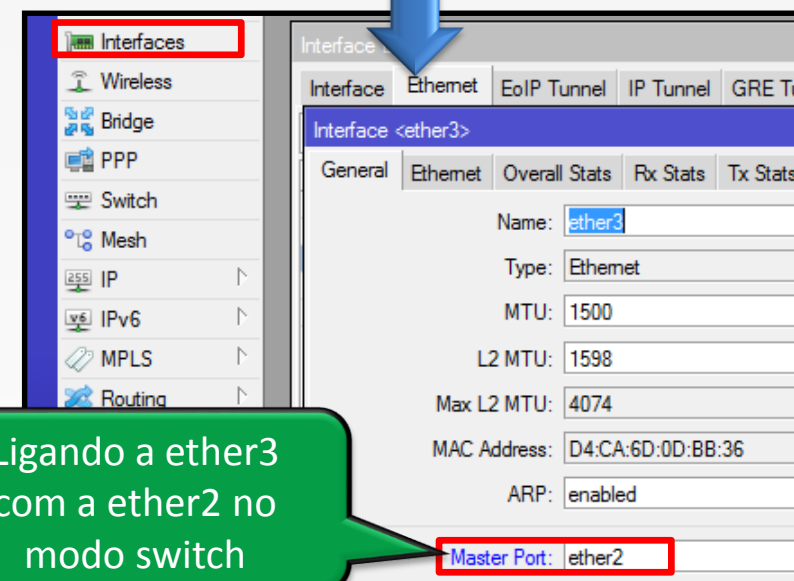
Bridges e Switchs



- Trabalham na camada 2
- Comutação de frames acontece em um nível diferente.



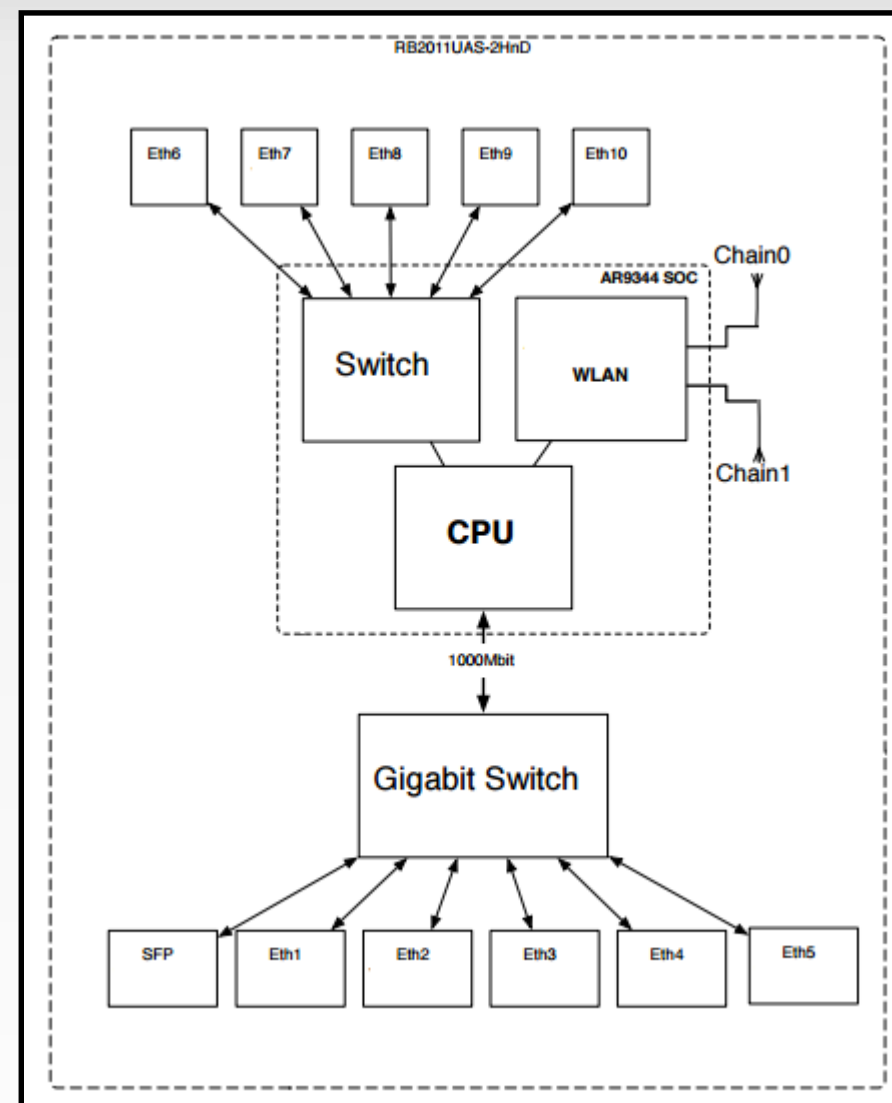
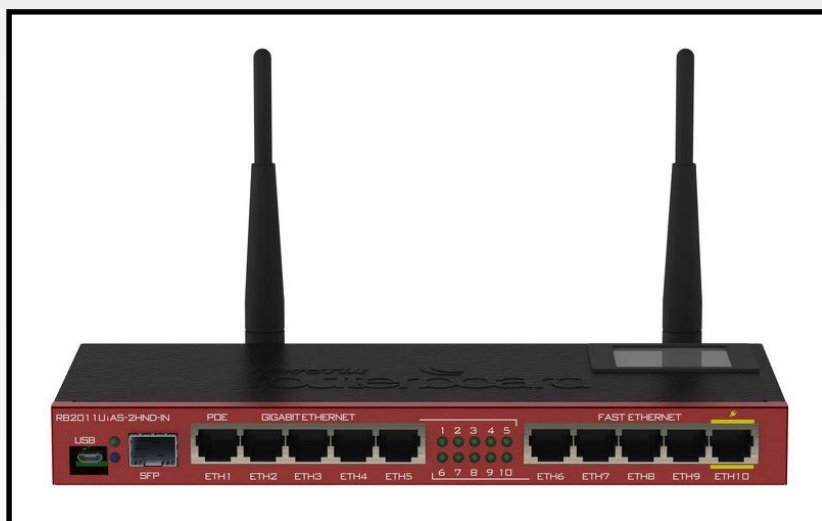
Criando um bridge para futura inclusão de interfaces



Ligando a ether3 com a ether2 no modo switch

Diagrama de bloco resumido

RB2011UiAS-2HnD-IN

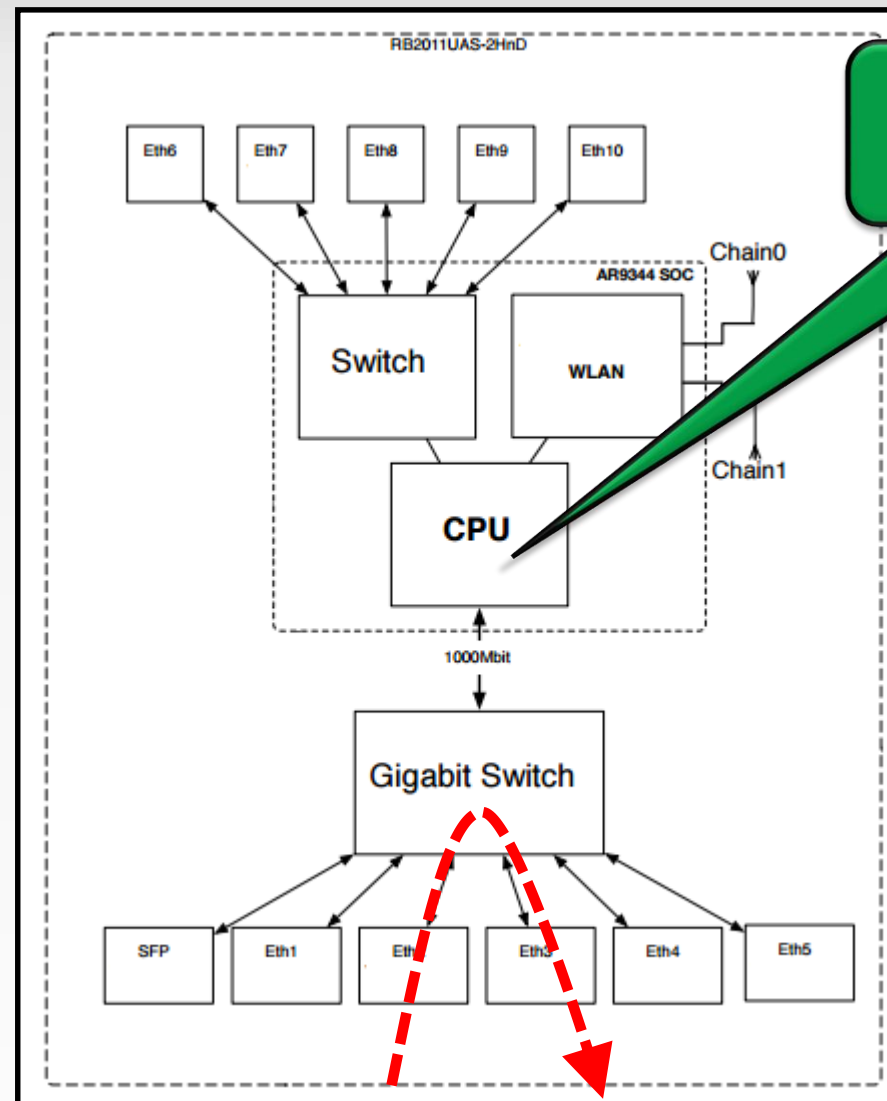


Usando a funcionalidade de switch

Onde usar o modo switch



Mesmo segmento de rede.



O tráfego não passa pela CPU.

Usando a funcionalidade de bridge

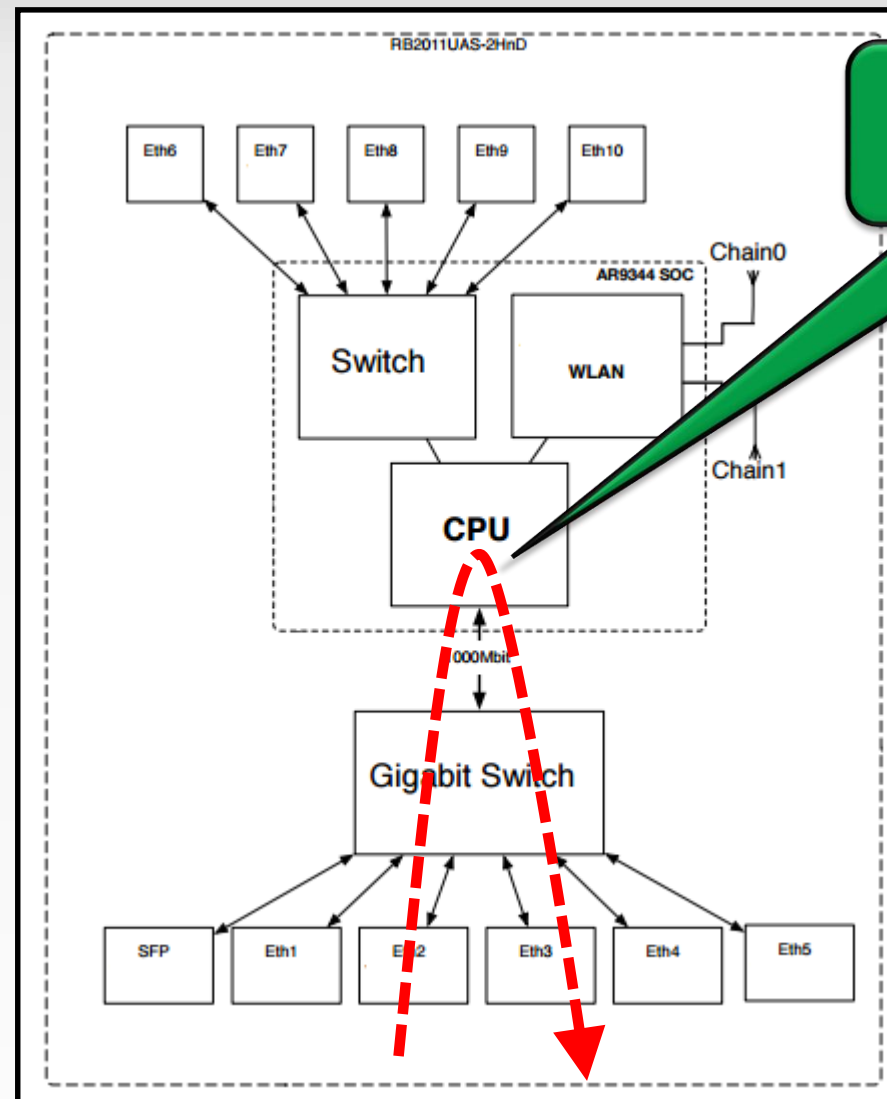
Redes Brasil

Onde usar o modo bridge



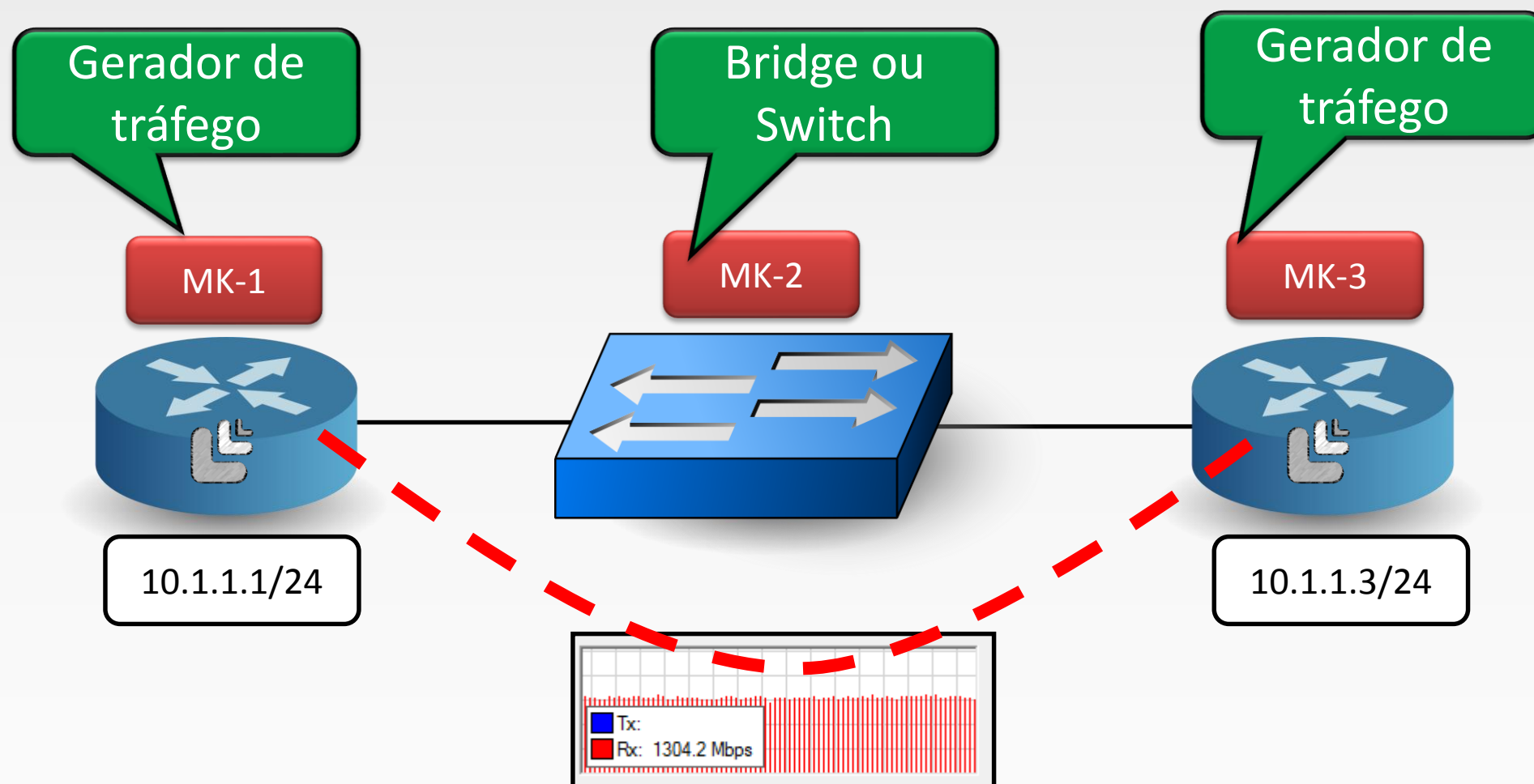
- ❖ Firewall
- ❖ QoS avançado
- ❖ Torch

Mesmo segmento de rede.



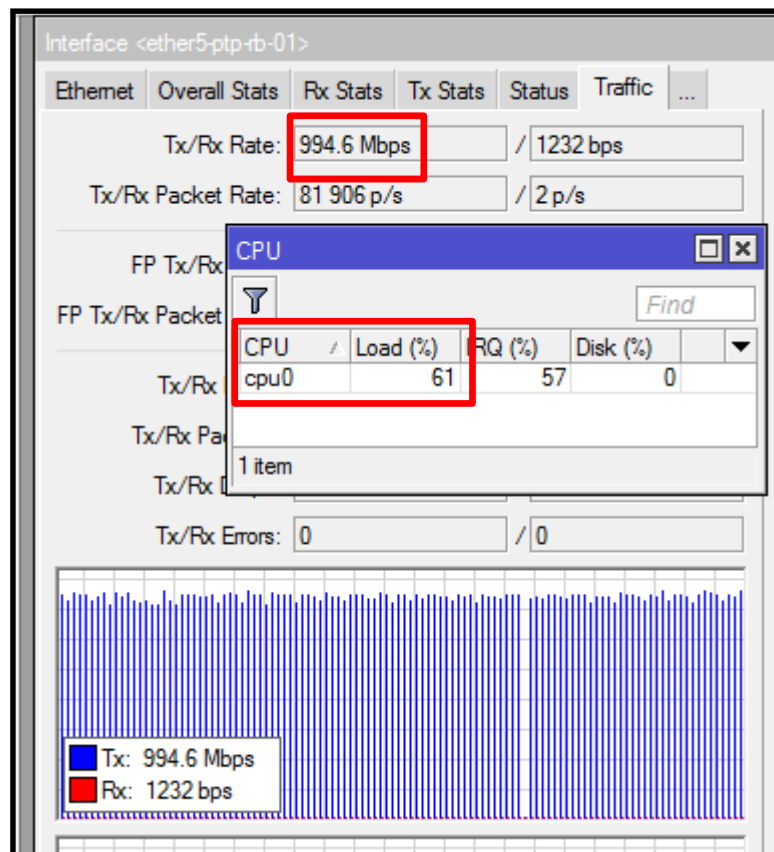
O tráfego passa pela CPU.

Testes de bancada Bridge e Switch

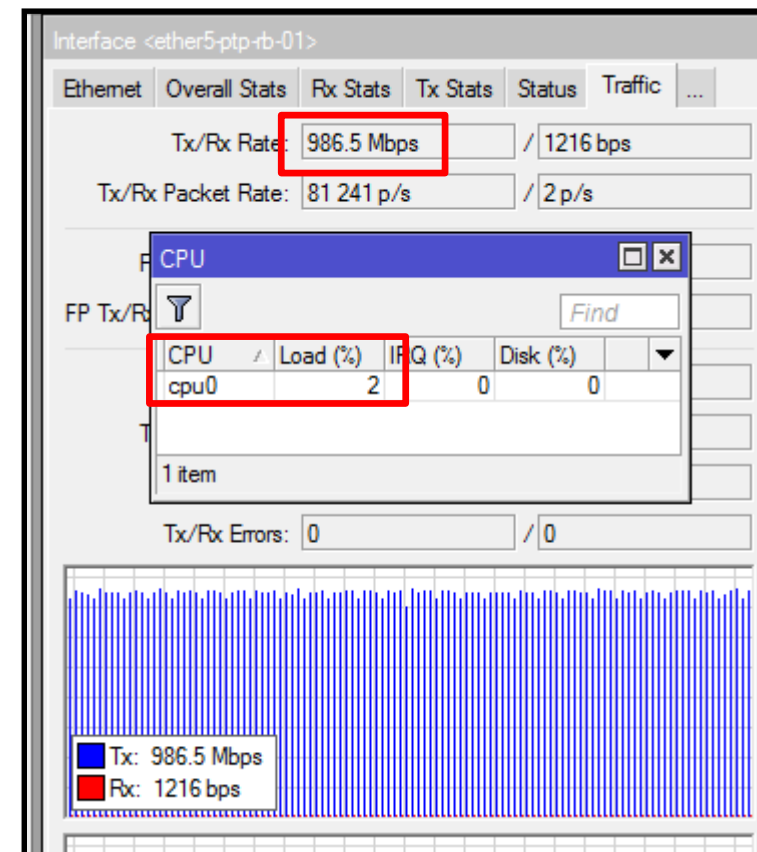


Testes de bancada Bridge e Switch

Bridge

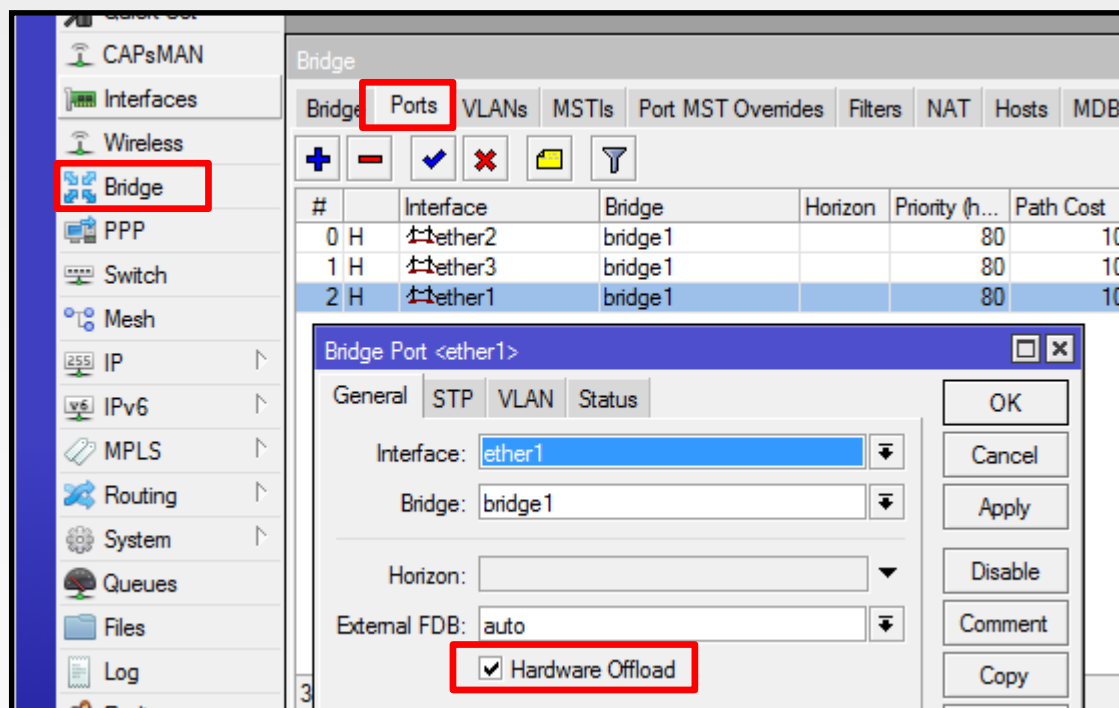


Switch



Vídeo com teste de desempenho <https://www.youtube.com/watch?v=tNEhExMOJyw>

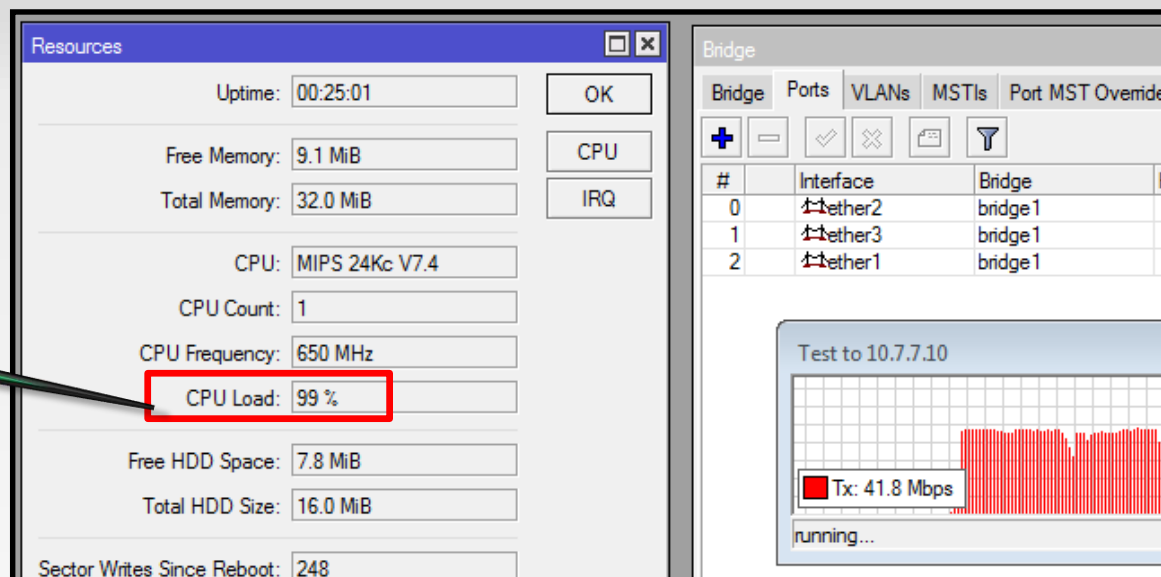
Bridge Hardware Offloading



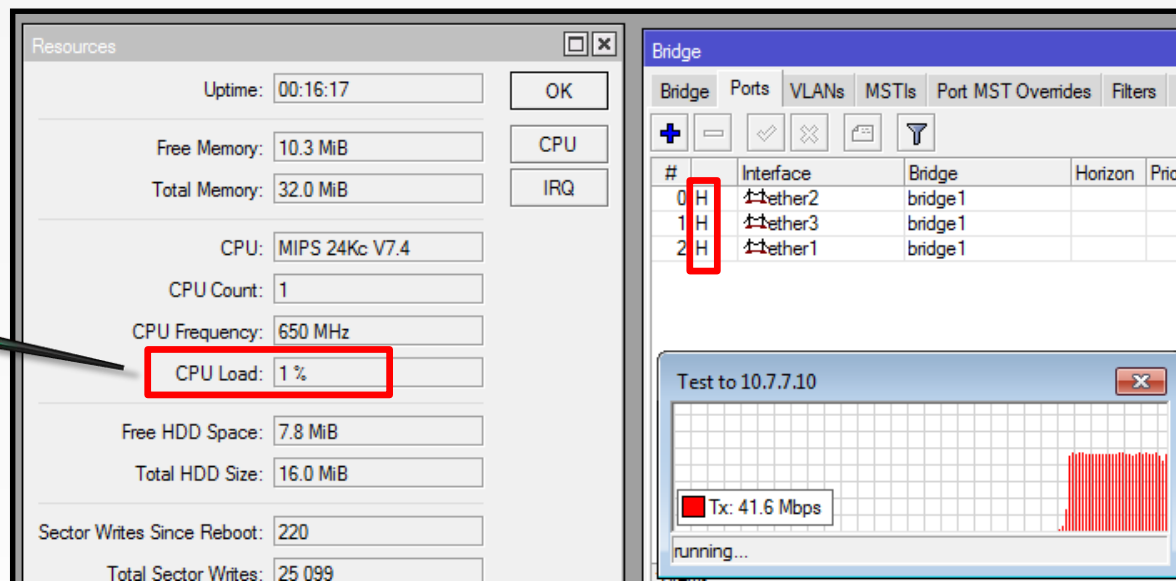
- A partir da versão v6.40rc29 o RouterOS conta com a funcionalidade de **Bridge Hardware Offloading**.
- Com esse recurso uma bridge terá a capacidade de fazer encaminhamento Layer2 usando o switch chip.

Resultados com hw-offload

Sem hardware-offload

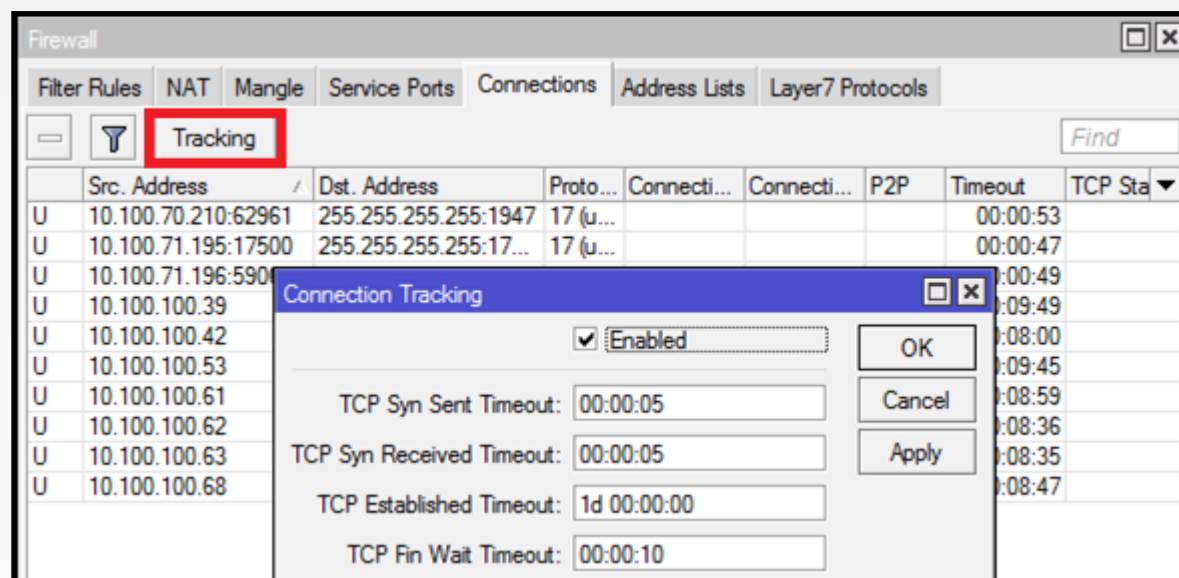


Com hardware-offload



Connection Tracking

- Utilizando a connection tracking o firewall consegue armazenar os estados das conexões.



Connection Tracking

Cuidado com Connection Tracking (Conntrack).

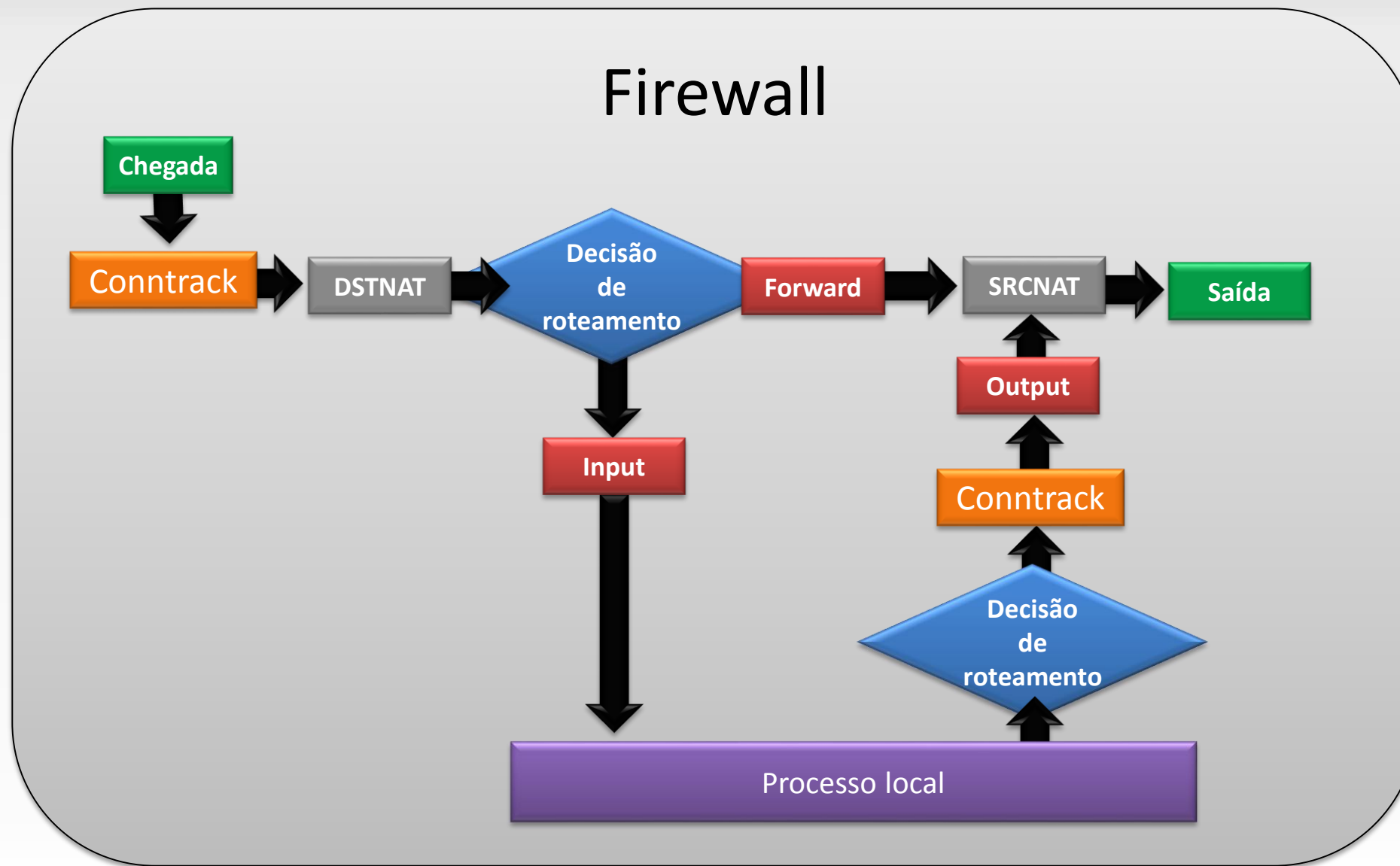


Ajuda em algumas tarefas.



Rouba seu CPU

Localização da Connection Tracking



Quando preciso da conntrack habilitada?

➤ NAT

➤ firewall:

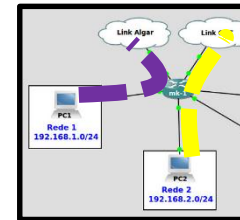
- connection-bytes
- connection-mark
- connection-type
- connection-state
- connection-limit
- connection-rate
- layer7-protocol
- p2p
- new-connection-mark
- tarpit

➤ p2p matching in simple queues

Para que serve marcas de conexões?



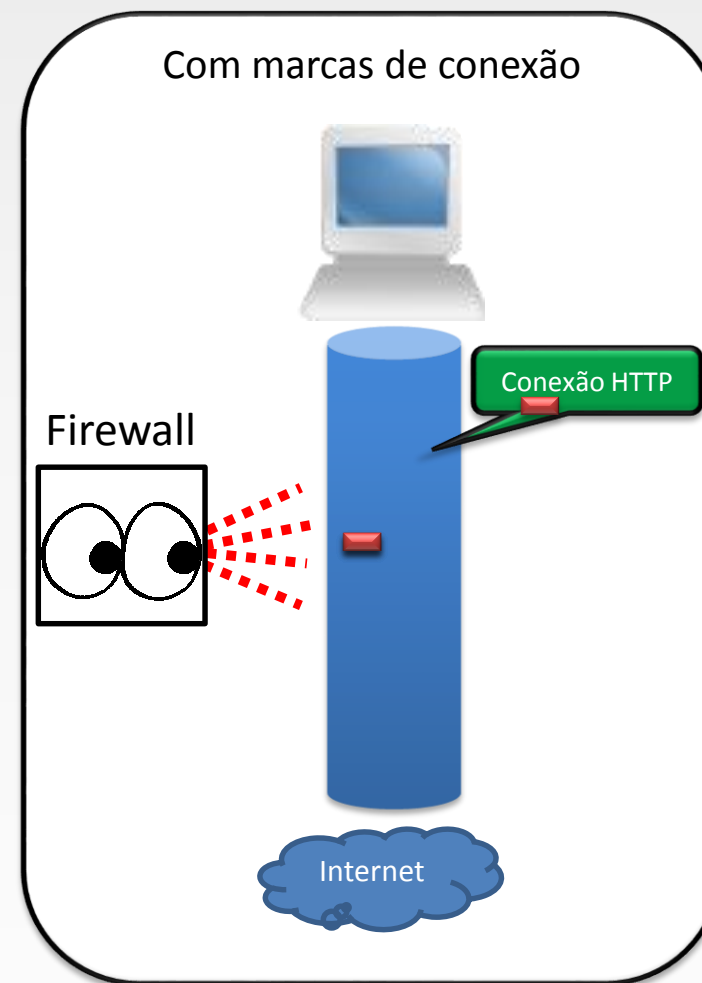
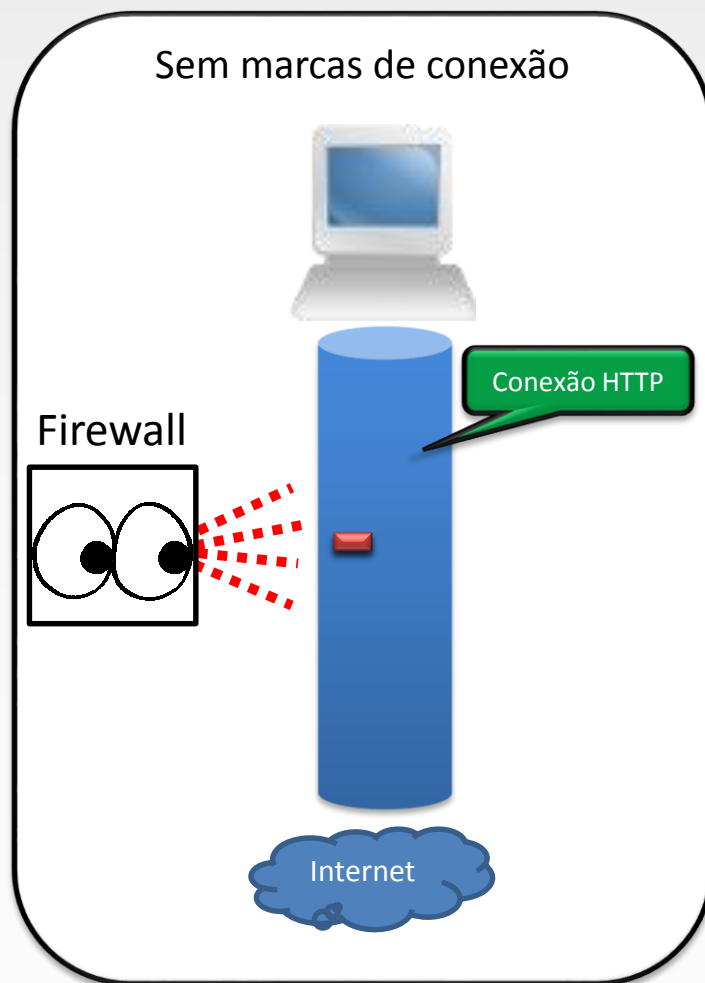
Marcas de pacotes



Marcas de roteamento

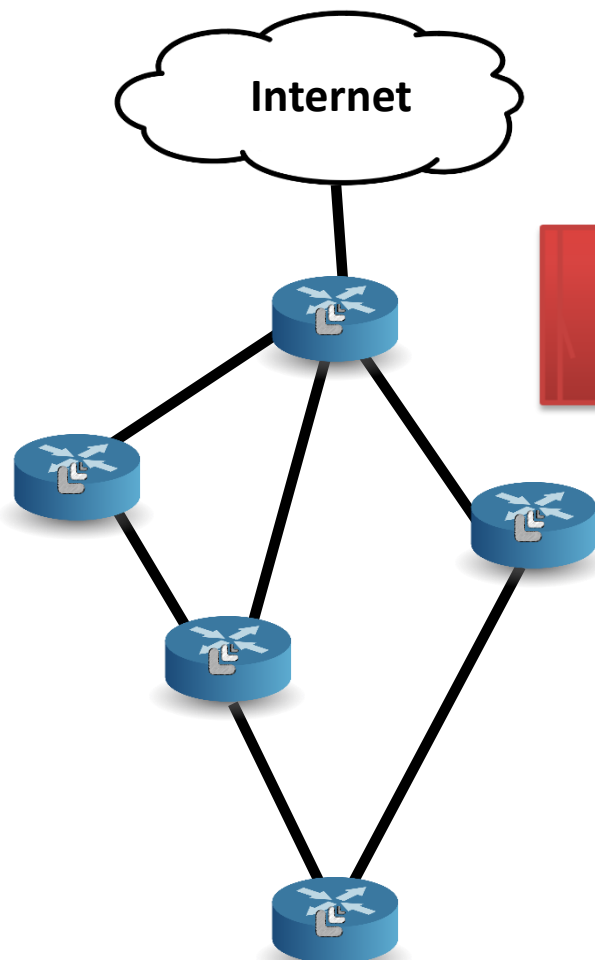
- Auxiliar as marcas de pacotes e marcas de roteamento
- Evitar que todos os pacotes sejam inspecionados no firewall
- Economia de uso de recursos da CPU
- Ajudar em algumas políticas de roteamento

Marcas de conexão



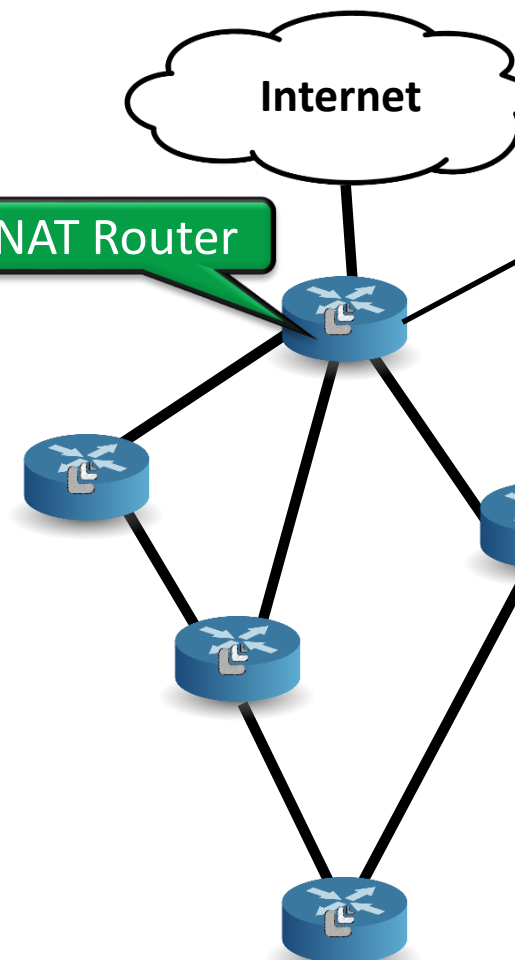
Onde posso desabilitar?

IPs públicos



Conntrack desabilitada
em todos os roteadores

IPs privados



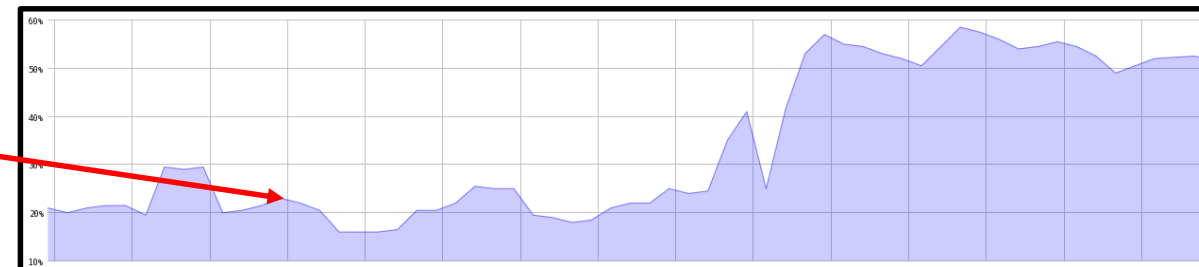
Conntrack
habilitada

Conntrack
desabilitada

Consumo de CPU

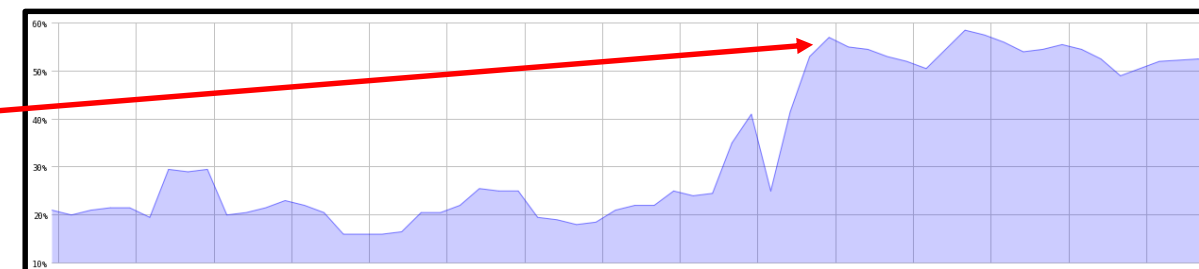
Contrack desabilitada

CPU:	ARMv7	CPU
CPU Count:	2	IRQ
CPU Frequency:	1400 MHz	
CPU Load:	22 %	
Free HDD Space:	88.5 MiB	
Total HDD Size:	128.3 MiB	
Architecture Name:	arm	
Board Name:	RB3011UiAS	



Contrack habilitada

CPU:	ARMv7	CPU
CPU Count:	2	IRQ
CPU Frequency:	1400 MHz	
CPU Load:	63 %	
Free HDD Space:	88.5 MiB	
Total HDD Size:	128.3 MiB	
Architecture Name:	arm	
Board Name:	RB3011UiAS	



Ainda precisa parcialmente do NAT ?

Fasttrack



Sem controle de banda



Sem filtros no firewall

No-track

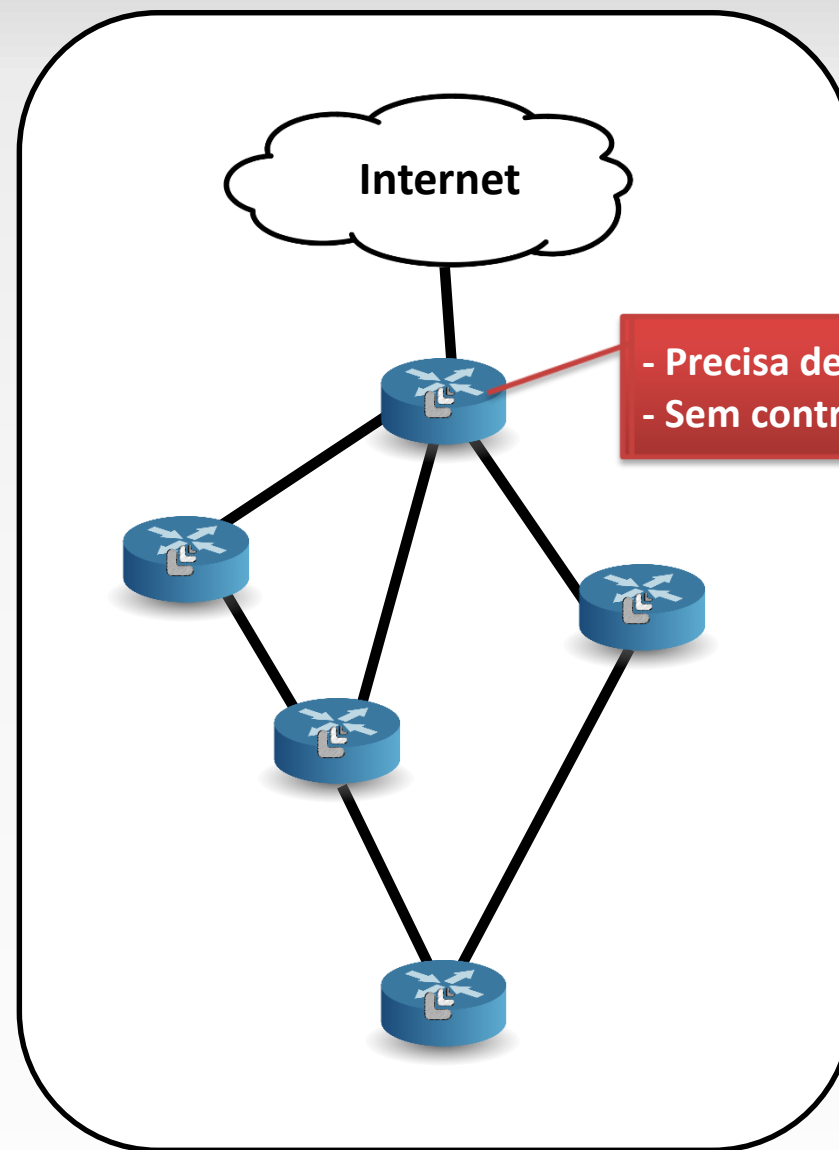


Controle de banda



Filtros de firewall

Onde aplicar fasttrack ?



- Precisa de NAT
- Sem controle de banda e outros recursos

➤ Com o recurso de Fasttrack ativo os pacotes irão fazer um bypass dos seguintes recursos.

- Firewall
- Connection tracking
- Simple queues e queue tree com parent=global
- IP accounting
- IPSec
- Hotspot
- Universal client
- VRF

FastTrack	
Without	With
360Mbps	890Mbps
CPU 100%	CPU 86%
44% CPU on firewall	6% CPU on firewall
* tested on RB2011 with single TCP stream	

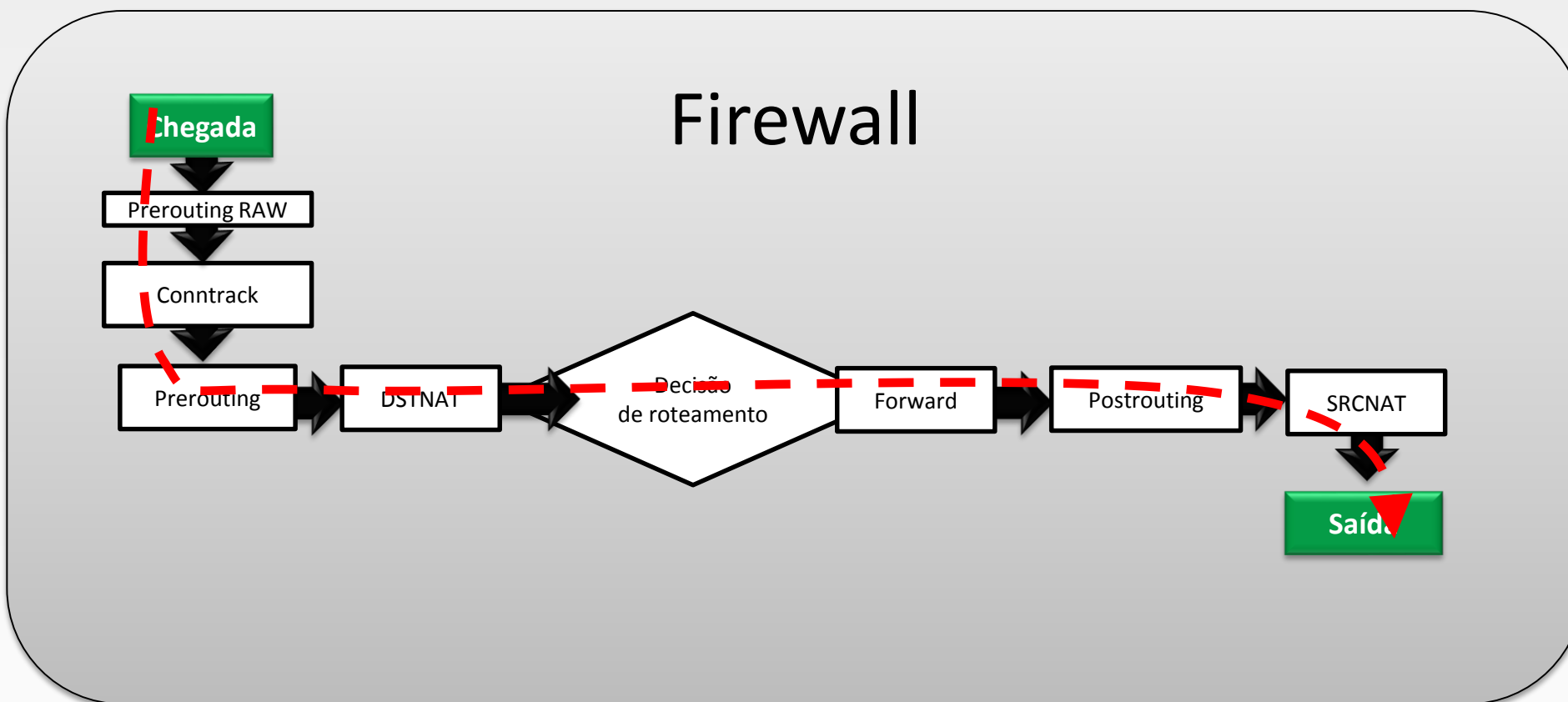
➤ Ativando Fasttrack você pode aumentar em até 5x a performance do roteador.

➤ Para mais informações visite <http://wiki.mikrotik.com/wiki/Manual:IP/Fasttrack>

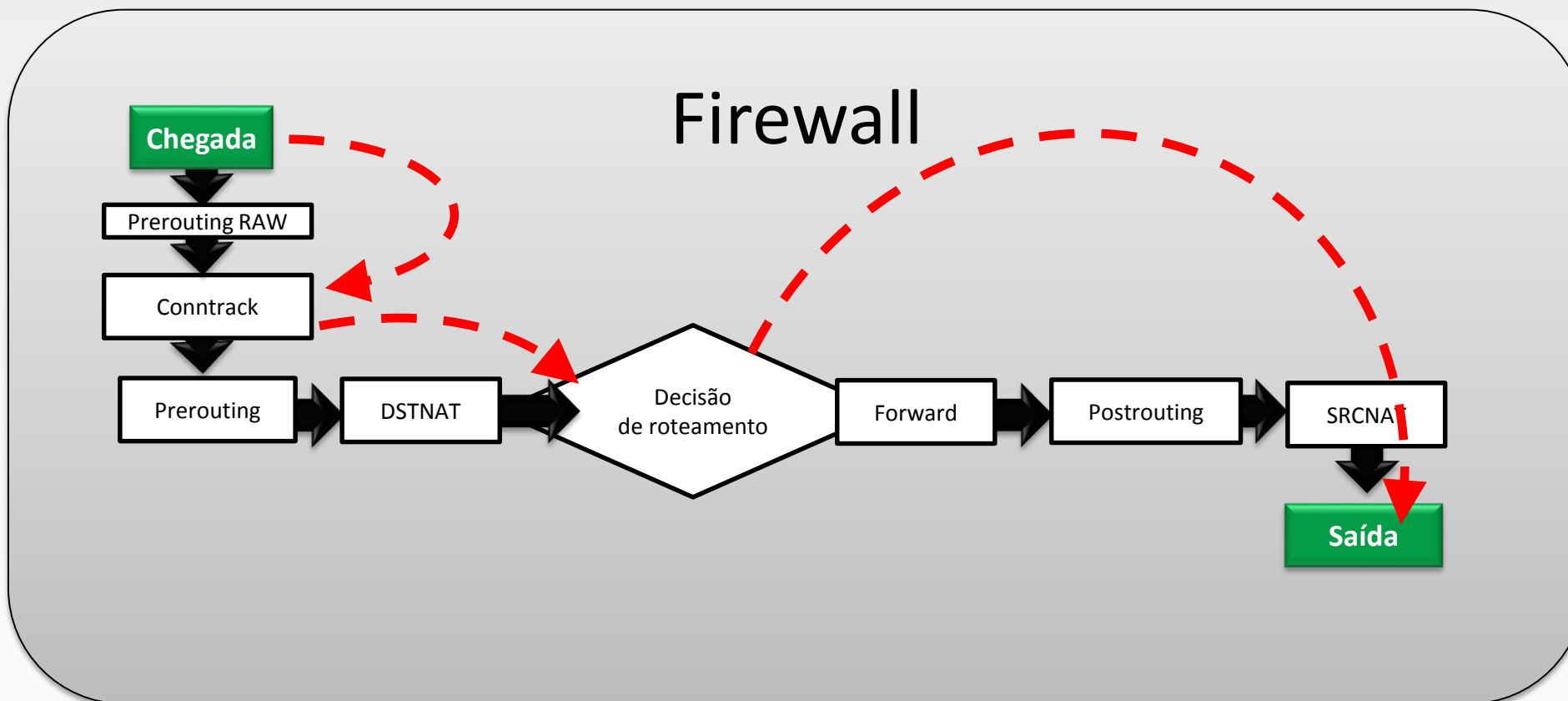
Comandos

```
/ip firewall filter  
add chain=forward action=fasttrack-connection connection-state=established,related
```

Fluxo do firewall sem fasttrack



Analogia do fluxo com fasttrack



Regra para Fasttrack

New Firewall Rule

General Advanced Extra Action Statistics

Chain: **forward**

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

P2P:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State: ☐ invalid ☒ established ☒ related ☐ new ☐ untracked

Connection NAT State:

New Firewall Rule

General Advanced Extra Action Statistics

Action: **fasttrack connection**

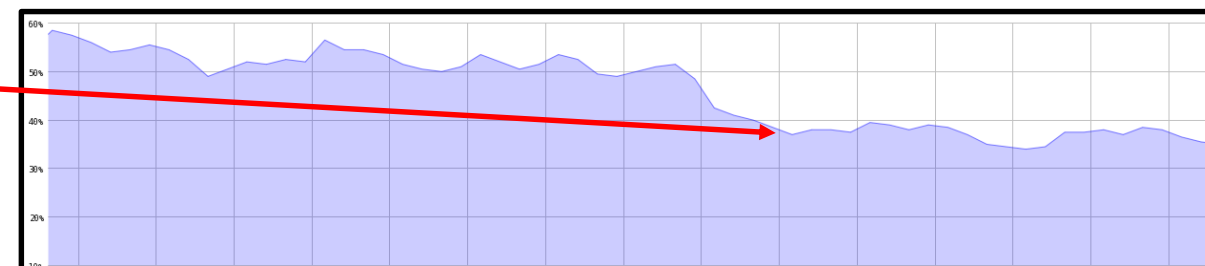
☐ Log

Log Prefix:

Consumo de CPU

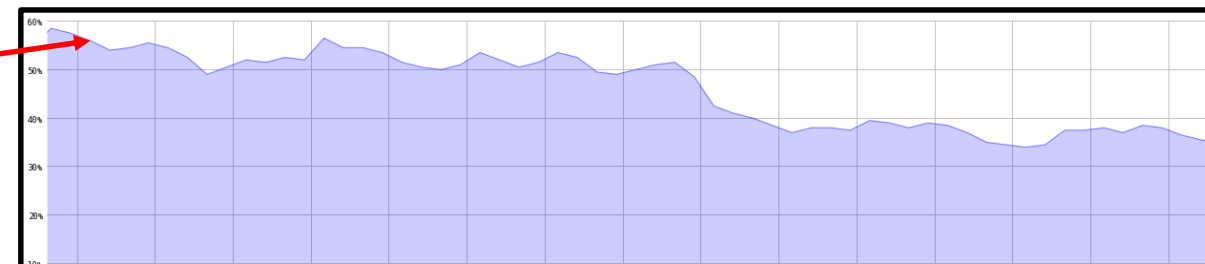
Com Fasttrack

CPU:	ARMv7	CPU
CPU Count:	2	IRQ
CPU Frequency:	1400 MHz	
CPU Load:	36 %	
Free HDD Space:	88.5 MiB	
Total HDD Size:	128.3 MiB	
Architecture Name:	arm	
Board Name:	RB3011UiAS	

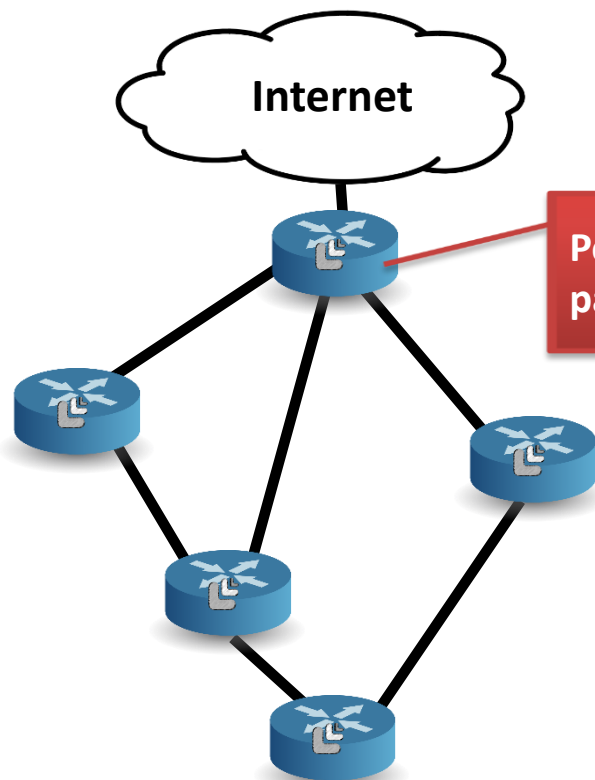


Sem Fasttrack

CPU:	ARMv7	CPU
CPU Count:	2	IRQ
CPU Frequency:	1400 MHz	
CPU Load:	63 %	
Free HDD Space:	88.5 MiB	
Total HDD Size:	128.3 MiB	
Architecture Name:	arm	
Board Name:	RB3011UiAS	

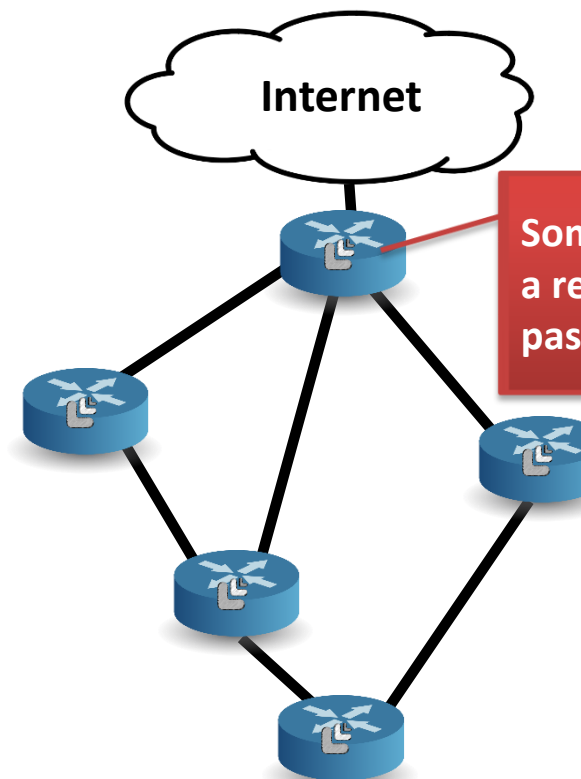


Onde aplicar a ação no-track ?



Pouco tráfego precisa passar pela contrack

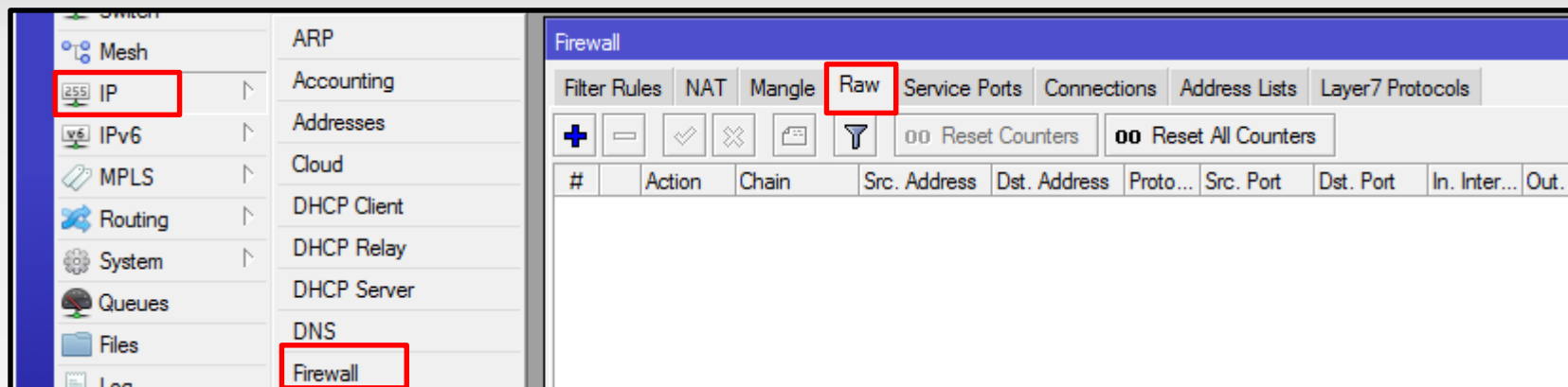
Grande parte do tráfego usa IPs públicos
Pequena parte do tráfego usa IPs privados



Somente tráfego destinado a redirecionamento irá passar pela contrack

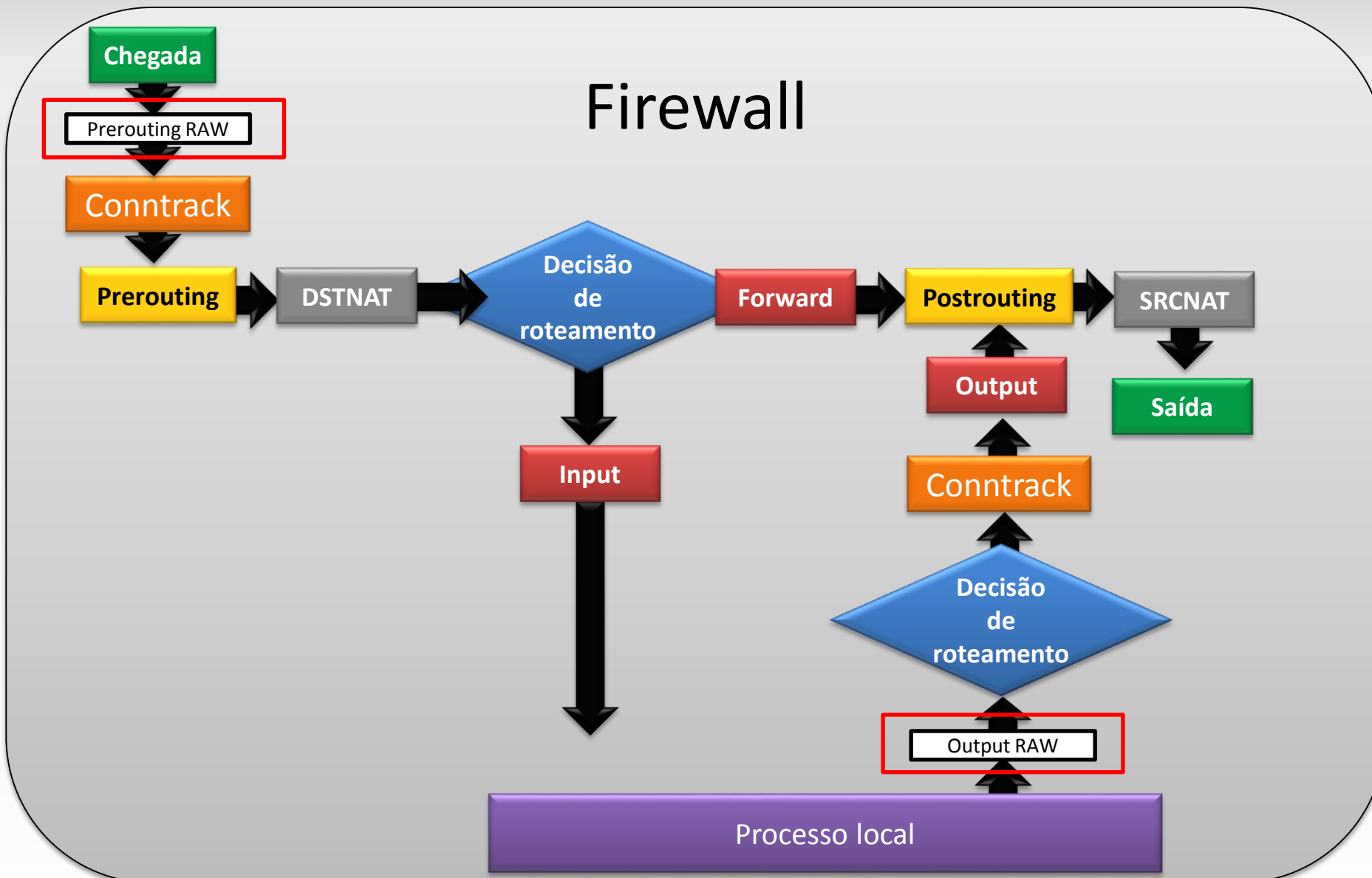
Precisa ativar NAT nos roteadores internos para fazer algum tipo de redirecionamento.
Ex: Pág de bloqueio

Tabela RAW



- A tabela RAW pode ser usada para fazer um bypass ou drop de pacotes antes que os pacotes cheguem até a connection tracking e com isso consegue reduzir drasticamente a sobrecargas na CPU.
- Filtros contra ataque de DoS e ou DDoS devem preferivelmente ser aplicados na tabela RAW.
- As ações mais comuns da tabela RAW são:
 - Drop: Usada para dropar pacotes antes que ele avance para processos internos.
 - No track: Usada para fazer com que pacotes façam um bypass da connection tracking.

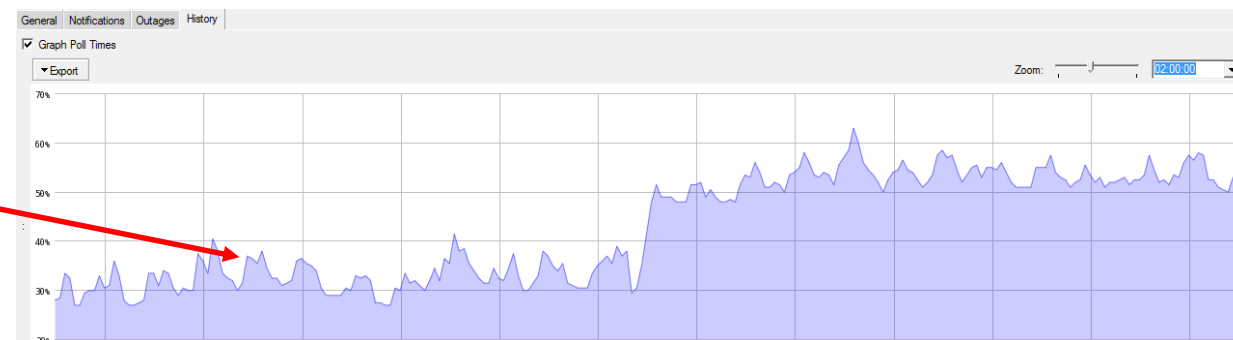
Canais da tabela RAW



Consumo de CPU

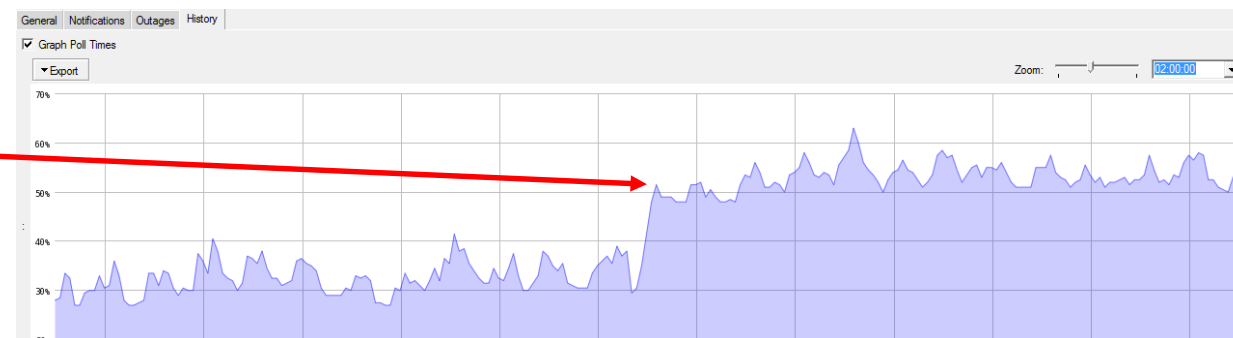
Com no-track

CPU: ARMv7 CPU
CPU Count: 2 IRQ
CPU Frequency: 1400 MHz
CPU Load: 34 %
Free HDD Space: 88.5 MiB
Total HDD Size: 128.3 MiB
Architecture Name: am
Board Name: RB3011UiAS



Sem no-track

CPU: ARMv7 CPU
CPU Count: 2 IRQ
CPU Frequency: 1400 MHz
CPU Load: 56 %
Free HDD Space: 88.5 MiB
Total HDD Size: 128.3 MiB
Architecture Name: am
Board Name: RB3011UiAS



Problemas ao cair vários túneis PPPoE

➤ Mais de 120 mil entradas na conntrack

↔ cppoeb-seb...	PPPoE Serv...	1480
↔ cppoeb-seb...	PPPoE Serv...	1480
↔ cppoeb-seb...	PPPoE Serv...	1480
↔ cppoeb-seb...	PPPoE Serv...	1480
↔ cppoeb-seb...	PPPoE Serv...	1480
↔ cppoeb-sara...	PPPoE Serv...	1480
↔ cppoeb-san...	PPPoE Serv...	1480
↔ cppoeb-san...	PPPoE Serv...	1480
↔ cppoeb-san...	PPPoE Serv...	1480
↔ cppoeb-san...	PPPoE Serv...	1480
↔ cppoeb-san...	PPPoE Serv...	1480
↔ cppoeb-san...	PPPoE Serv...	1480
↔ cppoeb-san...	PPPoE Serv...	1480
↔ cppoeb-sam...	PPPoE Serv...	1480
↔ cppoeb-sam...	PPPoE Serv...	1480
↔ cppoeb-sam...	PPPoE Serv...	1480
↔ cppoeb-salv...	PPPoE Serv...	1480
↔ cppoeb-ruth...	PPPoE Serv...	1480

ems out of 85: (95 selected)

Free Memory: 1152.3 MiB PCI

Total Memory: 1939.3 MiB USB

CPU: tilegx CPU

CPU Count: 16 IRQ

CPU Frequency: 1200 MHz

CPU Load: 92 %

Free HDD Space: 417.5 MiB

Total HDD Size: 512.0 MiB

Architecture Name: tile

Board Name: CCR1016-12G

Version: 6.39.2 (stable)

bridging	15	0.0
cpu0		90.5
cpu1		84.5
cpu2		89.5
cpu3		76.5
cpu4		70.5
cpu5		90.5
cpu6		77.0
cpu7		77.0
cpu8		83.5
cpu9		28.5
cpu10		59.0
cpu11		96.5
cpu12		67.0
cpu13		60.0
cpu14		73.5
cpu15		91.5
ethernet	9	0.5

ethernet	13	0.0
firewall	2	87.5
firewall	1	86.5
firewall	13	86.0
firewall	8	80.5
firewall	15	80.5
firewall	10	80.0
firewall	7	78.0
firewall	12	77.5
firewall	5	77.0
firewall	11	77.0
firewall	9	76.5
firewall	6	75.0
firewall	14	74.0
firewall	4	71.5
firewall	0	61.5
firewall	3	55.0

➤ Roteador ficava travado por mais de 10 minutos

Problemas ao cair vários túneis PPPoE

Filter Rules	NAT	Mangle	Raw	Service Ports	Connections	Address Lists	Layer7 Protocols				
#	Action	Chain	Src. Address	Dst. Address	Pr...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
... Deixa pacotes destinados aos IPs privados passarem pela conntrack											
0	✓ acc...	prerouting								2250.5 MiB	2 487 184
... Passa IPs publicos fora da conntrack para Upload											
1	no track	prerouting								14.0 GiB	74 974 123
... Passa IPs publicos fora da conntrack para Download											
2	no track	prerouting								95.7 GiB	87 501 235

- Pouco mais de 5 mil entradas na Conntrack
- Sem travamentos

DR	↔	pppoe-doris...	PPPoE Serv...	1480
DR	↔	pppoe-edg...	PPPoE Serv...	1480
DR	↔	pppoe-edi...	PPPoE Serv...	1480
DR	↔	pppoe-edia...	PPPoE Serv...	1480
DR	↔	pppoe-edim...	PPPoE Serv...	1480
DR	↔	pppoe-edim...	PPPoE Serv...	1480
DR	↔	pppoe-ediv...	PPPoE Serv...	1480
DR	↔	pppoe-ediv...	PPPoE Serv...	1480
DR	↔	pppoe-ediv...	PPPoE Serv...	1480
DR	↔	pppoe-ediv...	PPPoE Serv...	1480
DR	↔	pppoe-edm...	PPPoE Serv...	1480
DR	↔	pppoe-edn...	PPPoE Serv...	1480
DR	↔	pppoe-eds...	PPPoE Serv...	1480
DR	↔	pppoe-edu...	PPPoE Serv...	1480
DR	↔	pppoe-edu...	PPPoE Serv...	1480
DR	↔	pppoe-edu...	PPPoE Serv...	1480
DR	↔	pppoe-edu...	PPPoE Serv...	1480
DR	↔	pppoe-eli...	PPPoE Serv...	1480
DR	↔	pppoe-eli...	PPPoE Serv...	1480

845 items out of 862 (150 selected)

CPU:	tilegx	CPU
CPU Count:	16	IRQ
CPU Frequency:	1200 MHz	
CPU Load:	27%	
Free HDD Space:	417.5 MiB	
Total HDD Size:	512.0 MiB	
Architecture Name:	tile	
Board Name:	CCR1016-12G	
Version:	6.39.2 (stable)	

cpu0	5.0
cpu1	14.5
cpu2	9.5
cpu3	11.5
cpu4	5.0
cpu5	6.0
cpu6	5.5
cpu7	13.0
cpu8	10.5
cpu9	16.5
cpu10	12.5
cpu11	12.5
cpu12	4.5
cpu13	20.5
cpu14	20.5

Regras de no-track

Firewall							
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols							
oo Reset Counters oo Reset All Counters							
#	Action	Chain	Src. Address List	Dst. Address List	Bytes	Packets	Comment
0	✓ accept	prerouting		passar-pela-contrack	151.2 KiB	789	Deixa pacotes destinados a exeções passarem pela contrack
1	✓ accept	prerouting	passar-pela-contrack		1267.5 KiB	11 441	Deixa pacotes originados a exeções passarem pela contrack
2	no track	prerouting			91.4 GiB	96 421 095	Faz bypass de todo restante

Comandos

```
/ip firewall raw
```

```
add action=accept chain=prerouting comment="Deixa pacotes destinados a exeções passarem pela contrack" dst-address-list=passar-pela-contrack
```

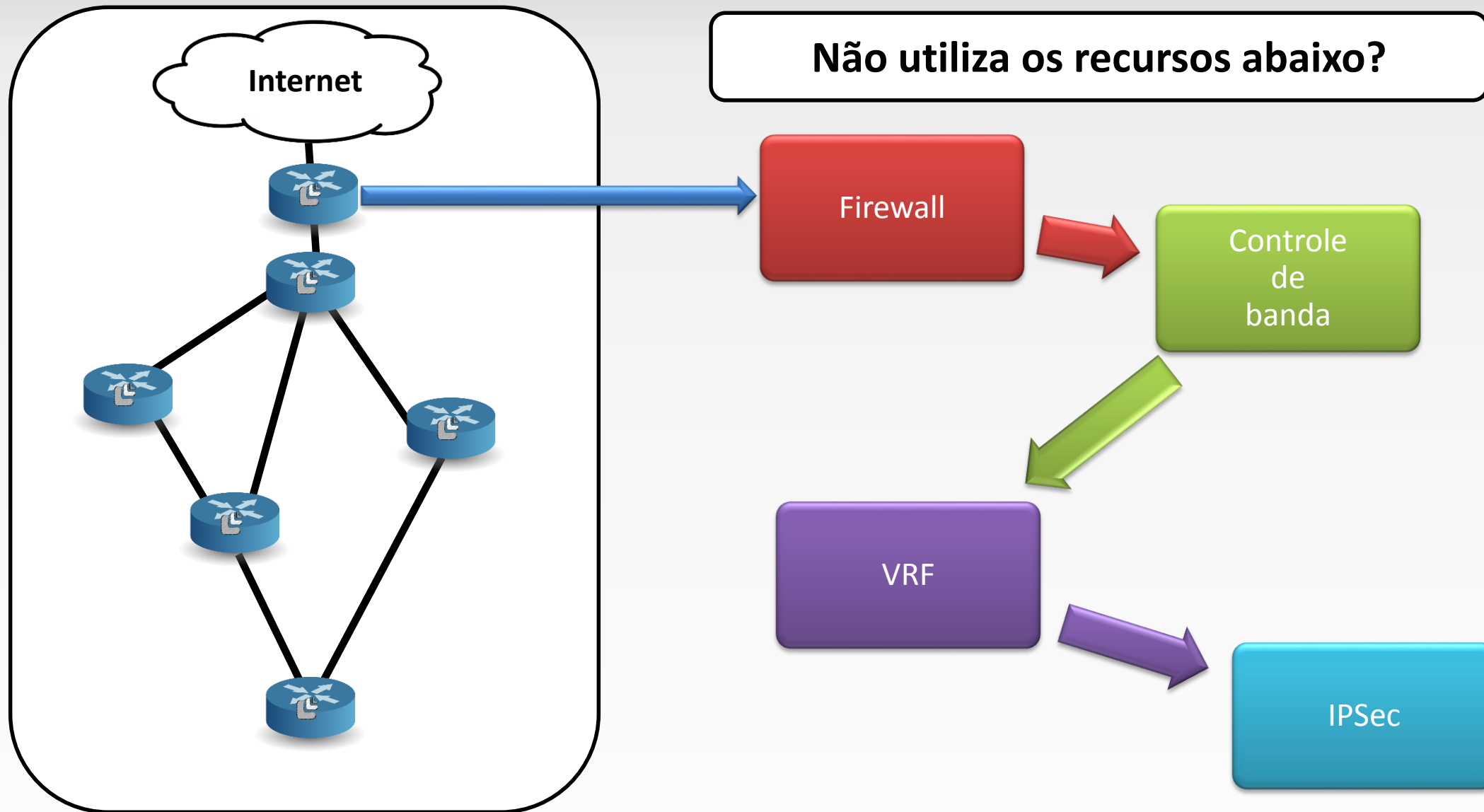
```
add action=accept chain=prerouting comment="Deixa pacotes originados a exeções passarem pela contrack" src-address-list=passar-pela-contrack
```

```
add action=notrack chain=prerouting comment="Faz bypass de todo restante"
```

Resumo para ter mais desempenho.

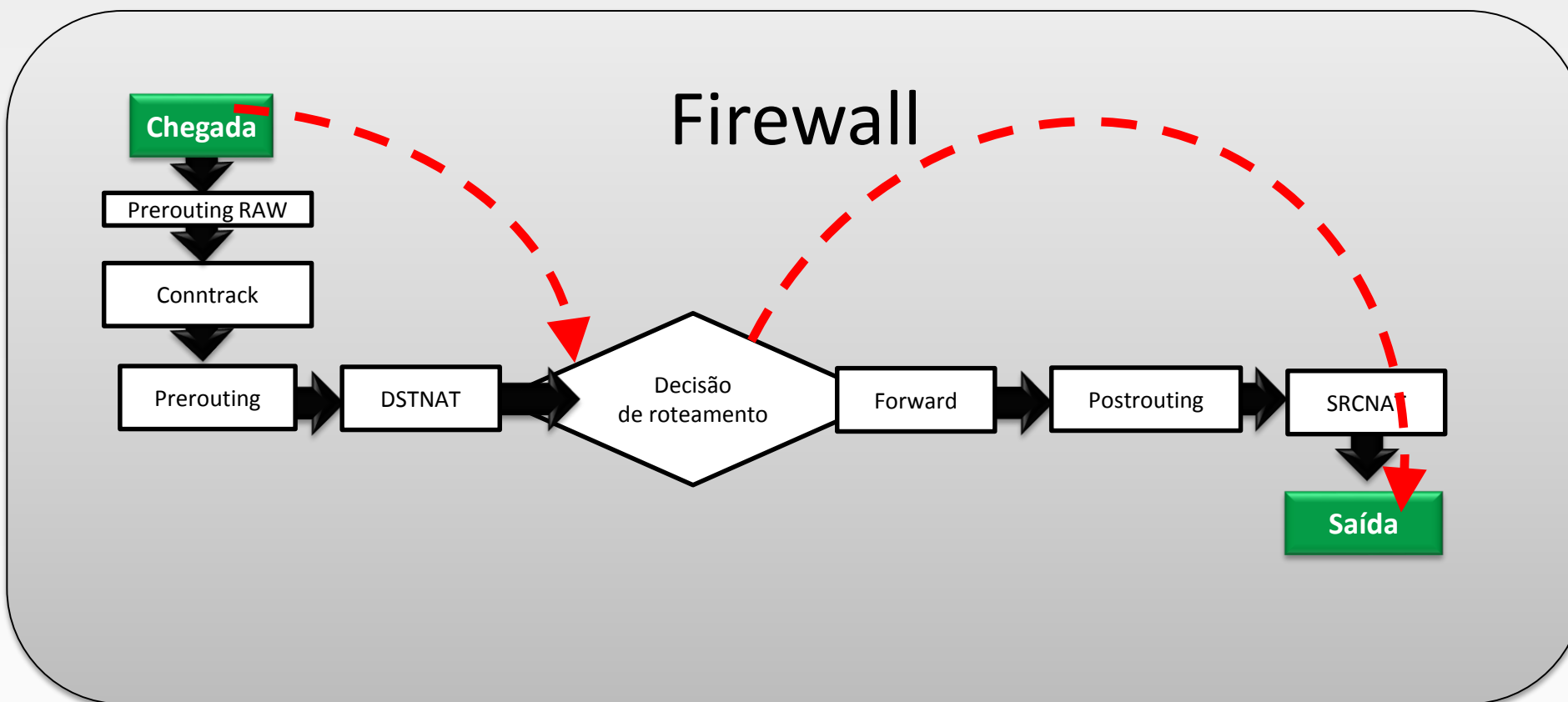


Onde aplicar o FastPath?



- A função de **fastpath** permite encaminhar pacotes sem processamento adicional no Kernel Linux.
- Com essa funcionalidade ativada conseguimos melhorar significativamente a velocidade de encaminhamento de pacotes e reduzir muito a sobrecarga no CPU.
- Fastpath será automaticamente usado se as condições abaixo forem satisfeitas.
 - firewall rules não estar configurado.;
 - firewall address lists não estar configurado.;
 - Simple e queue trees with parent=global não estar configurado.;
 - no mesh, metarouter interface configuration;
 - sniffer, torch and traffic generator is not running;
 - connection tracking não estar ativa;
 - ip accounting is disabled (/ip accounting enabled=no);
 - VRFs are not set (/ip route vrf is empty);
 - Hotspot is not used (/ip hotspot has no interfaces);
 - IpSec policies não estar configurado. (ROS v6.8);
 - /tool mac-scan is not actively used;
 - /tool ip-scan is not actively used;
 - route cache must be enabled

Analogia do fluxo com fastpath



Testes de performance com fastpath.

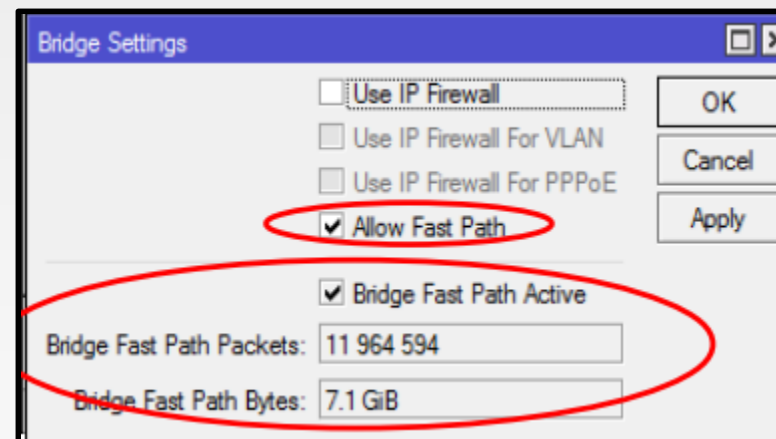
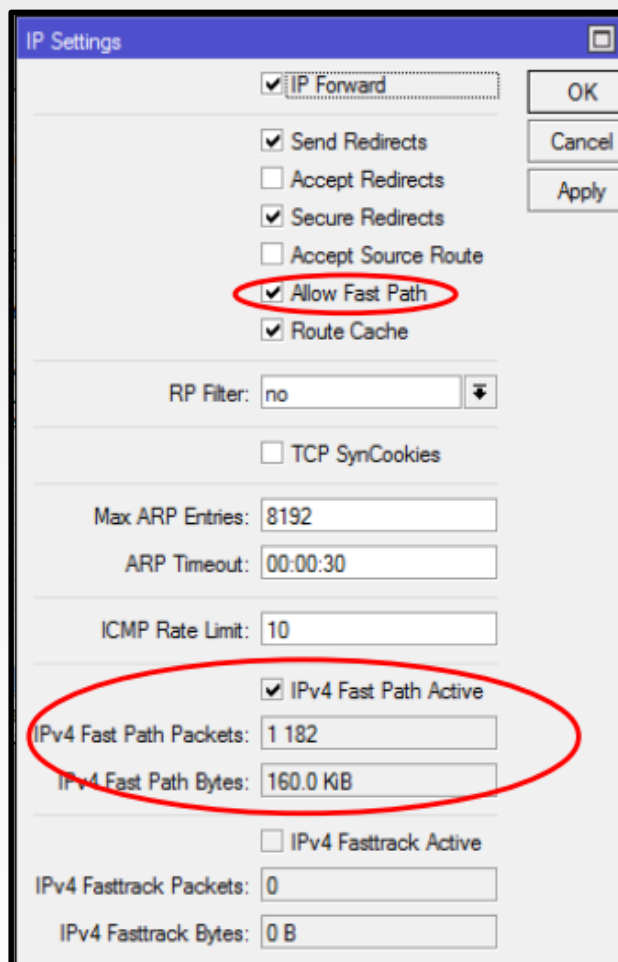


RB3011UiAS-RM		IPQ-8064 All port test					
Mode	Configuration	1518 byte		512 byte		64 byte	
		kpps	Mbps	kpps	Mbps	kpps	Mbps
Bridging	none (fast path)	325.0	3,946.8	939.8	3,849.4	1,530.2	783.5
Bridging	25 bridge filter rules	325.0	3,946.8	384.2	1,573.7	348.6	178.5
Routing	none (fast path)	325.0	3,946.8	939.8	3,849.4	1,437.6	736.1
Routing	25 simple queues	325.0	3,946.8	419.6	1,718.7	419.7	214.9
Routing	25 ip filter rules	202.0	2,453.1	204.1	836.0	188.4	96.5

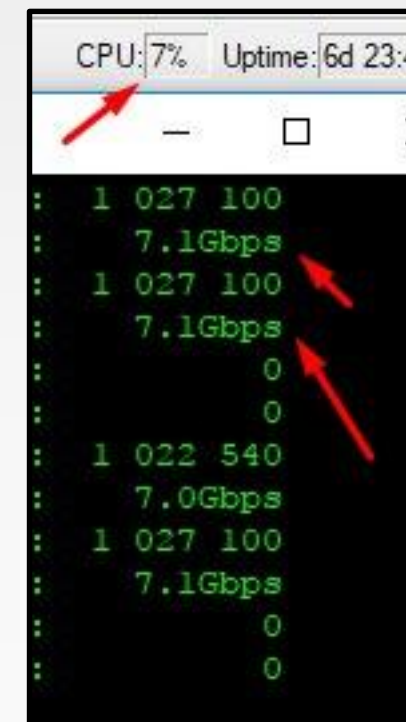


RB1100Dx4		AL21400 1G all port test					
Mode	Configuration	1518 byte		512 byte		64 byte	
		kpps	Mbps	kpps	Mbps	kpps	Mbps
Bridging	none (fast path)	606.5	7,365.3	1,736.4	7,112.3	5,509.7	2,821.0
Bridging	25 bridge filter rules	606.5	7,365.3	1,107.8	4,537.5	1,153.2	590.4
Routing	none (fast path)	606.5	7,365.3	1,736.4	7,112.3	5092.3	2,607.3
Routing	25 simple queues	606.5	7,365.3	933.6	3,824.0	960.3	491.7
Routing	25 ip filter rules	543.7	6,602.7	561.8	2,301.1	564.6	289.1

Ativando FastPath



Roteador com FastPath







www.redesbrasil.com



Redes Brasil

Página no

The Facebook logo, consisting of the word "facebook" in white lowercase letters on a blue rectangular background.

facebook

Canal do

The YouTube logo, consisting of the words "You" and "Tube" in white, with "Tube" inside a white rounded rectangle, all on a red rectangular background.

YouTube