



# Fluxo dos Pacotes (Packet Flow)

## Completo, Simples e Útil

---

# João Krieger

---



**CREA-SC**  
Conselho Regional de Engenharia,  
Arquitetura e Agronomia de Santa Catarina

**LANTastic**  
Network Software



**Microsoft**  
**CERTIFIED**  
*Technology  
Specialist*

---

**MikroTik**  
CERTIFIED CONSULTANT

**MikroTik**  
CERTIFIED TRAINER

---

**Academia MT**  
Cursos e Serviços MikroTik

# Conteúdo

---

1. Modelos OSI e TCP/IP (Revisão)
2. Diagrama do Fluxo dos Pacotes
3. Firewall
  1. Filter / NAT / Mangle / Raw / Connections
4. Dicas pro Dia a Dia

# Modelo OSI e TCP/IP



7	APLICAÇÃO	APLICAÇÃO	
6	APRESENTAÇÃO	<b>DADOS</b> HTTP, HTTPS DNS, DHCP, FTP	5
5	SESSÃO	SSH, TELNET	
4	TRANSPORTE	<b>Porta TCP e UDP</b> 22, 80, 443	4
3	REDE	<b>IP</b> 172.30.1.1	3
2	ENLACE	<b>MAC</b> 6C:3B:6B:40:0D:53	2
1	FÍSICA	<b>bits</b> 1110101010110111	1

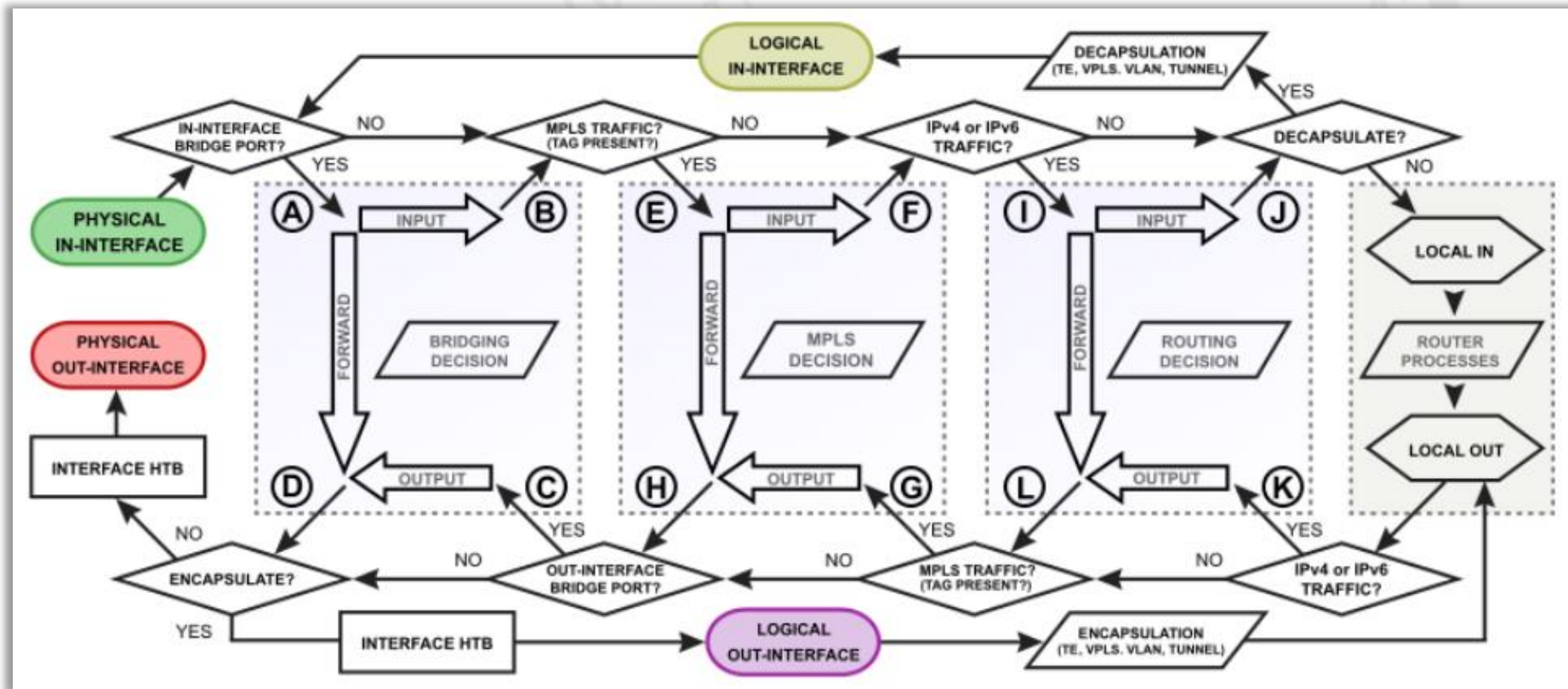
# Camada 3, Rede - Cabeçalho IPv4

Versão (Version)	Tamanho do Cabeçalho (IHL)	Tipo de Serviço (ToS)	Tamanho Total (Total Length)	
Identificação (Identification)		Flags	Deslocamento do Fragmento (Fragment Offset)	
Tempo de Vida (TTL)	Protocolo (Protocol)	Soma de verificação do Cabeçalho (Checksum)		
Endereço de Origem ( <i>Source Address</i> )				
Endereço de Destino ( <i>Destination Address</i> )				
Opções + Complemento (Options + Padding)				

# Diagrama do Fluxo de Pacotes

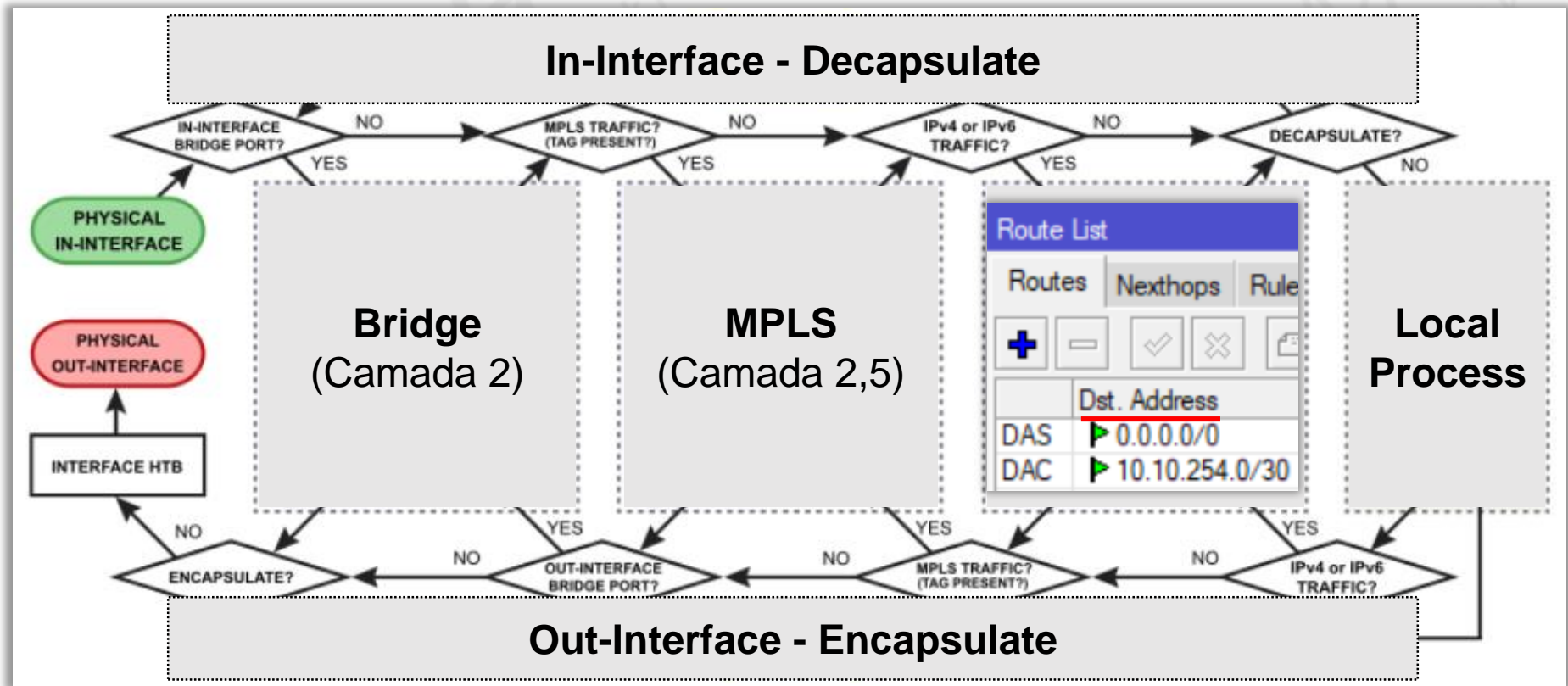
- **Porque é necessário conhecê-lo?**
  1. Para sabermos **quando, porque e onde passam os pacotes** no RouterOS
  2. Resolver tarefas mais complicadas como bloqueios
  3. Fazer redirecionamentos, marcações e classificações
  4. Priorizar tráfego e fazer QoS
  5. Criar políticas de roteamento
  6. E ...

# Diagrama em Blocos do Fluxo de Pacotes



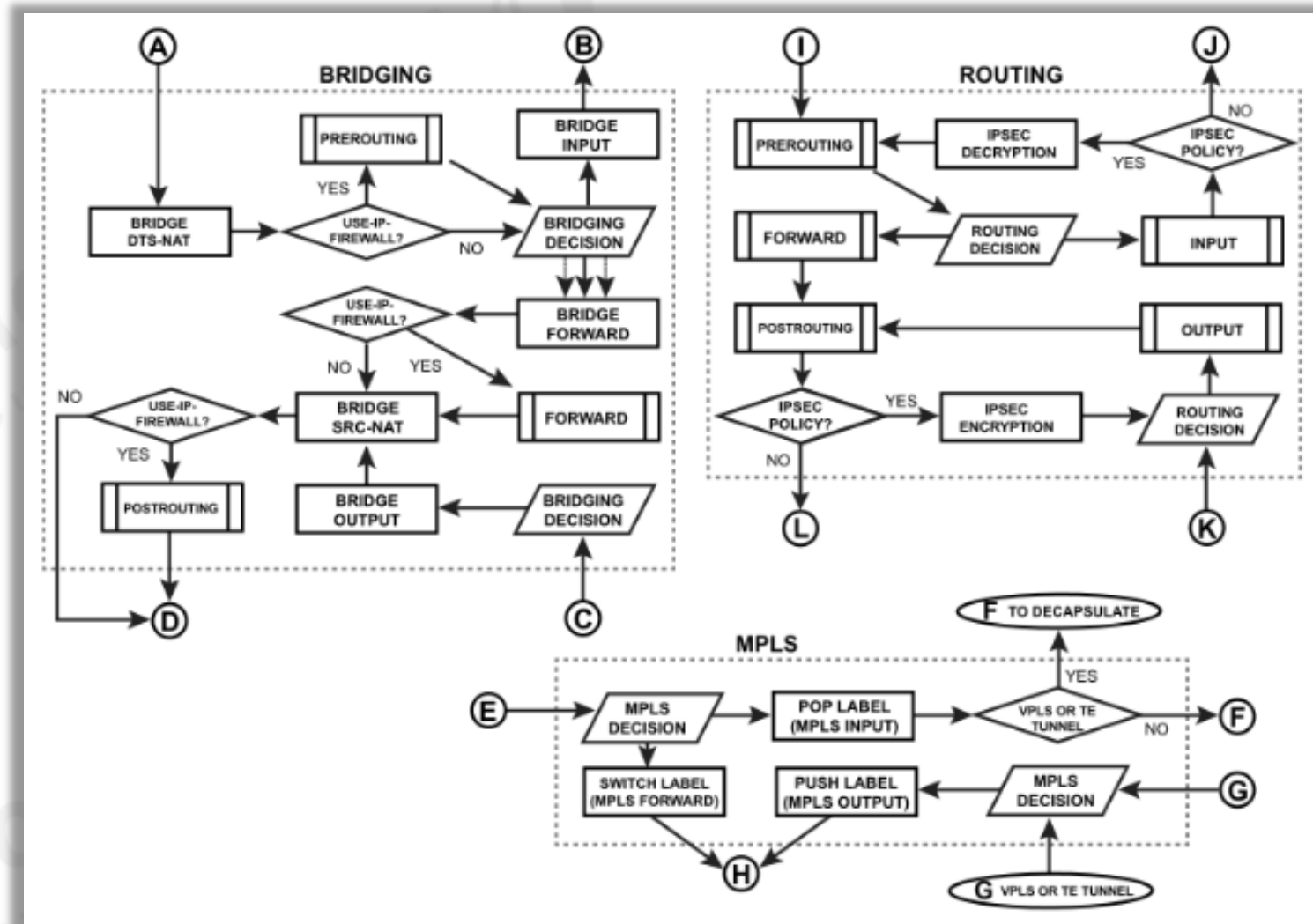
[https://wiki.mikrotik.com/wiki/Manual:Packet\\_Flow](https://wiki.mikrotik.com/wiki/Manual:Packet_Flow)

# Fluxo de Pacotes em Blocos Simples

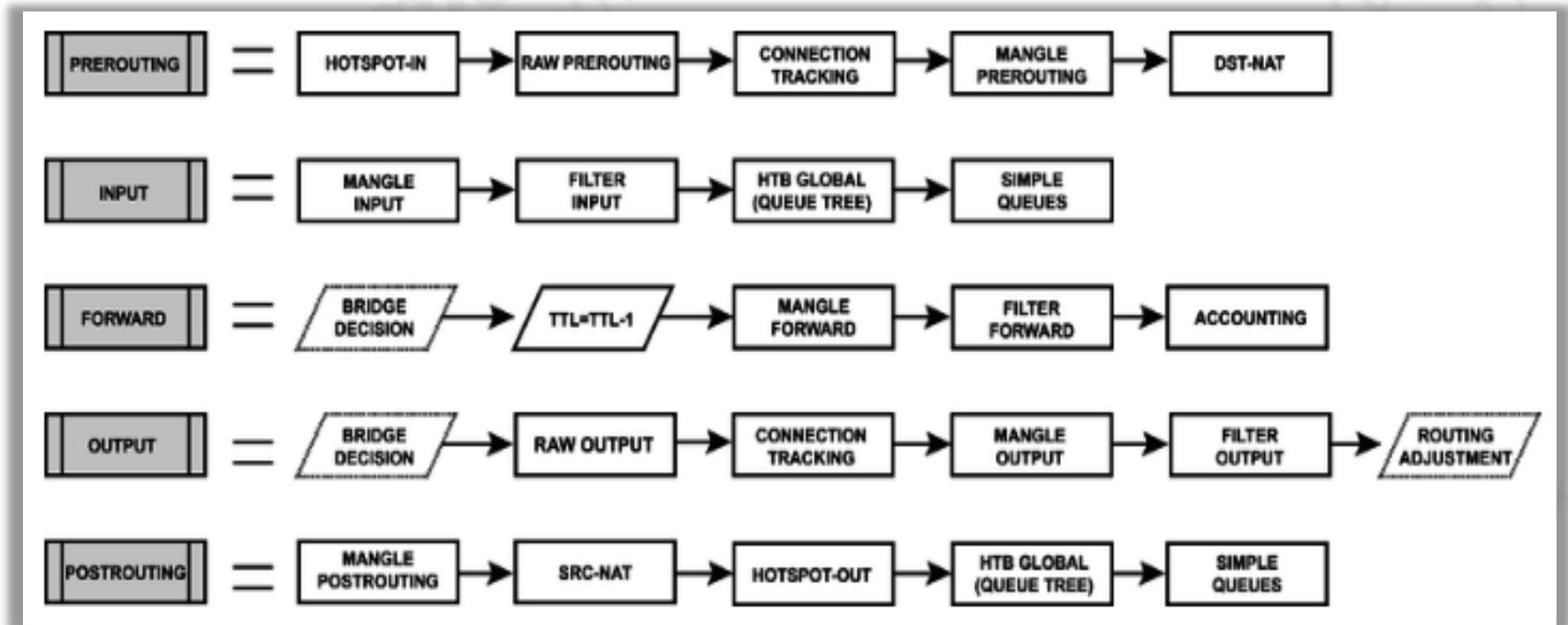




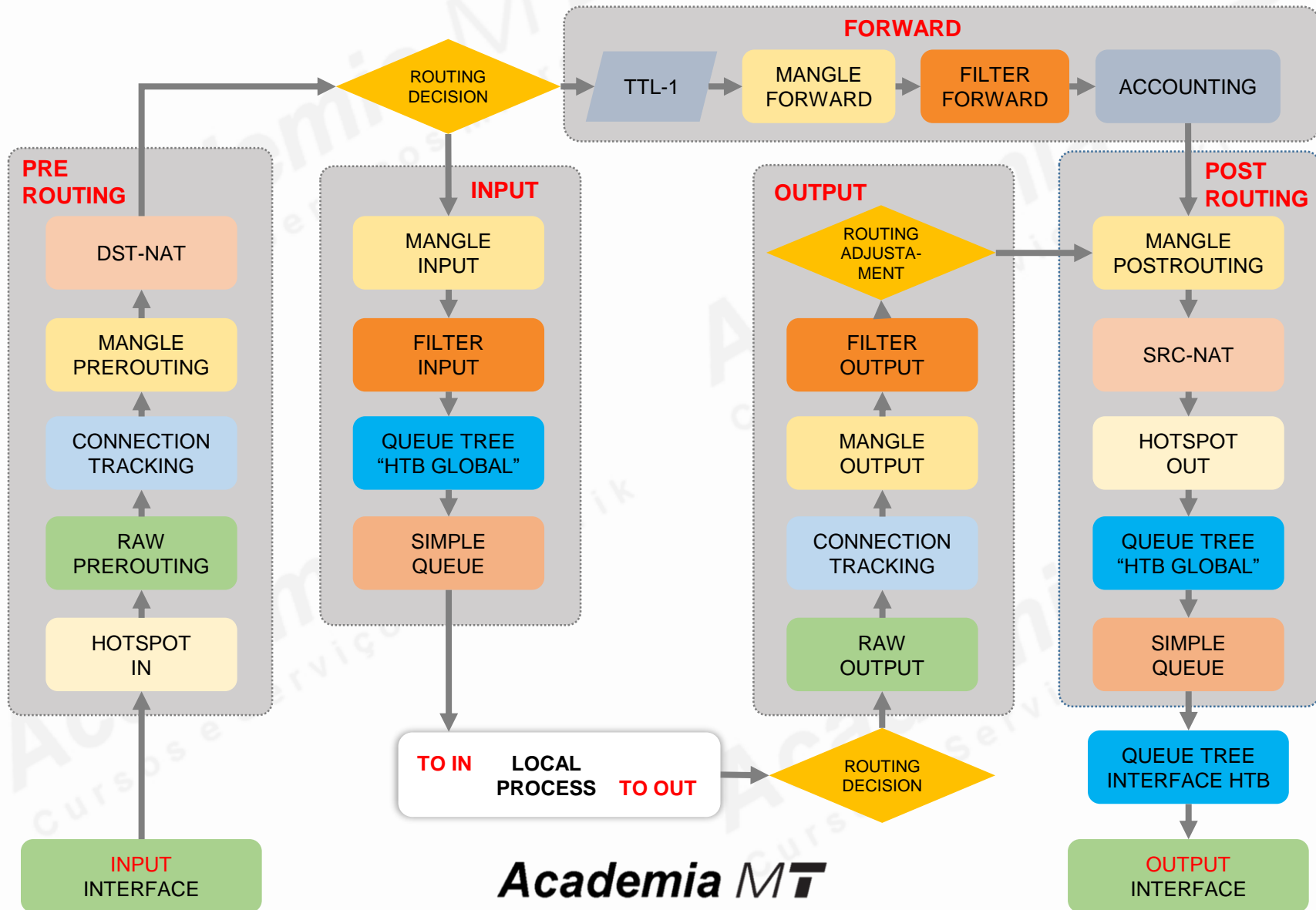
# Decisões Expandidas



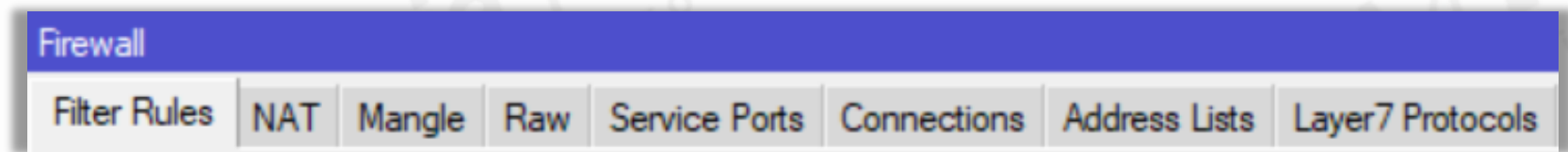
# Chains (corrente) de Fluxo dos Pacotes



# Fluxo dos Pacotes IP Completo



# Tabelas em /ip firewall



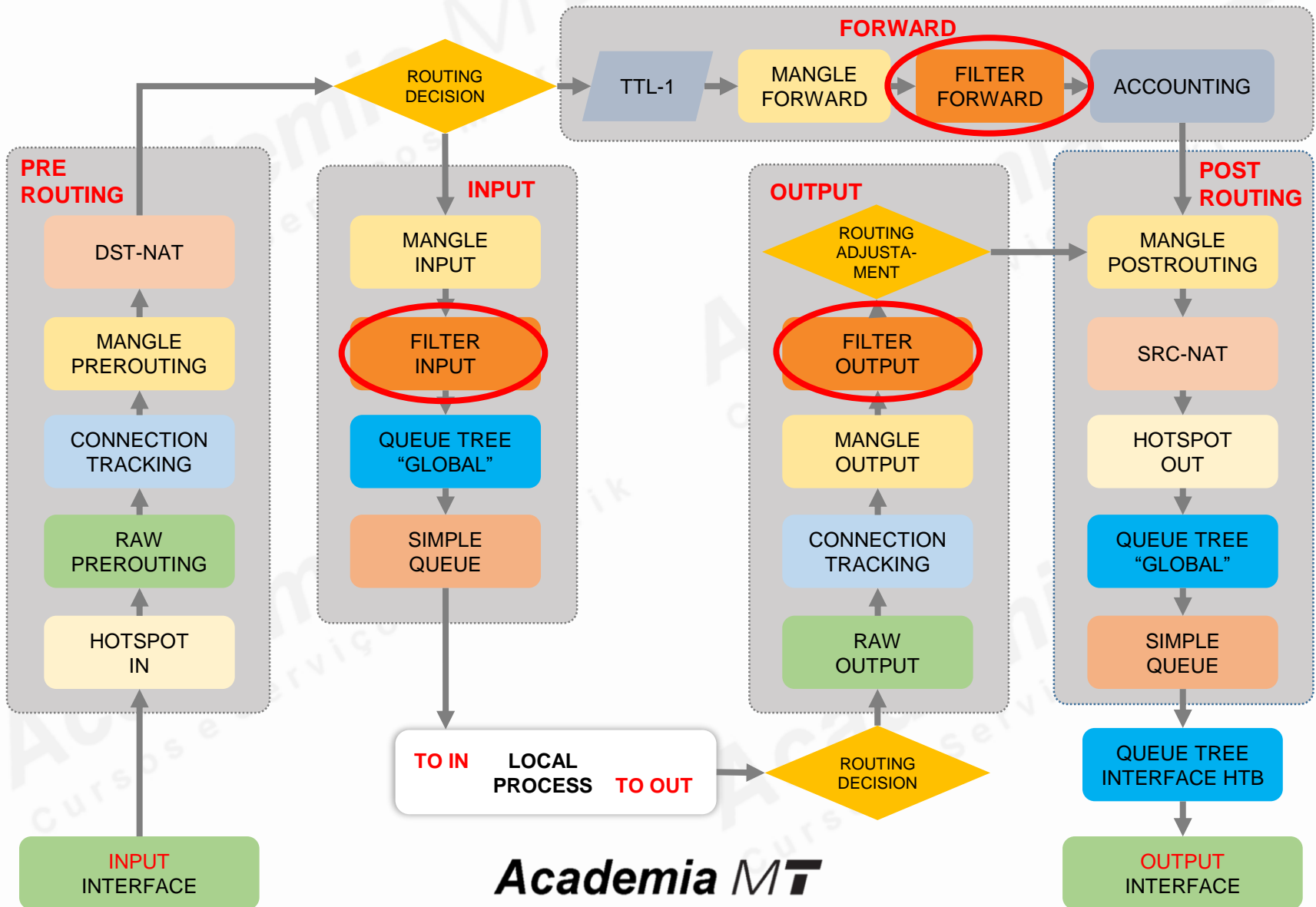
1. **Filter Rules:** Filtra pacotes
2. **NAT:** Traduz endereços e portas
3. **Mangle:** Marca conexões, pacotes e roteamento, também pode alterar campos no cabeçalho
4. **Raw:** Salta a Conntrack, protege e agiliza
5. **Connections:** Rastreia conexões (ConnTrack)

`/ip firewall filter add chain=`

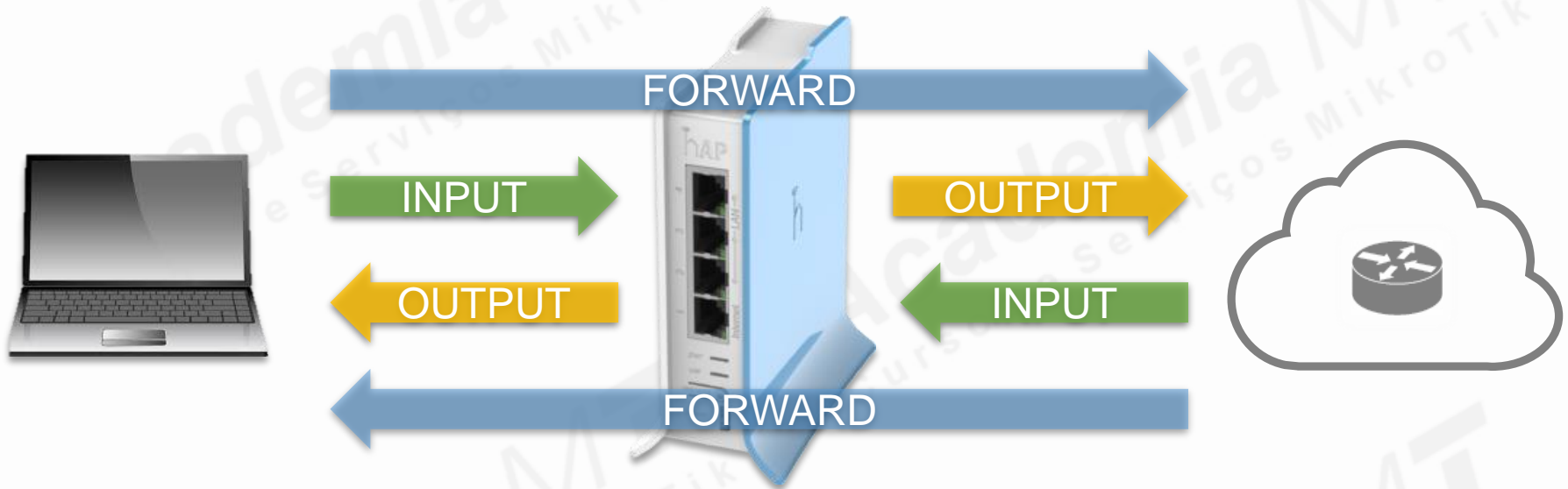
The screenshot shows the 'New Firewall Rule' configuration window. The 'Chain' dropdown menu is open, displaying the following options:

Chain
forward
input
output

# /ip firewall filter add chain=



# /ip firewall filter add chain=

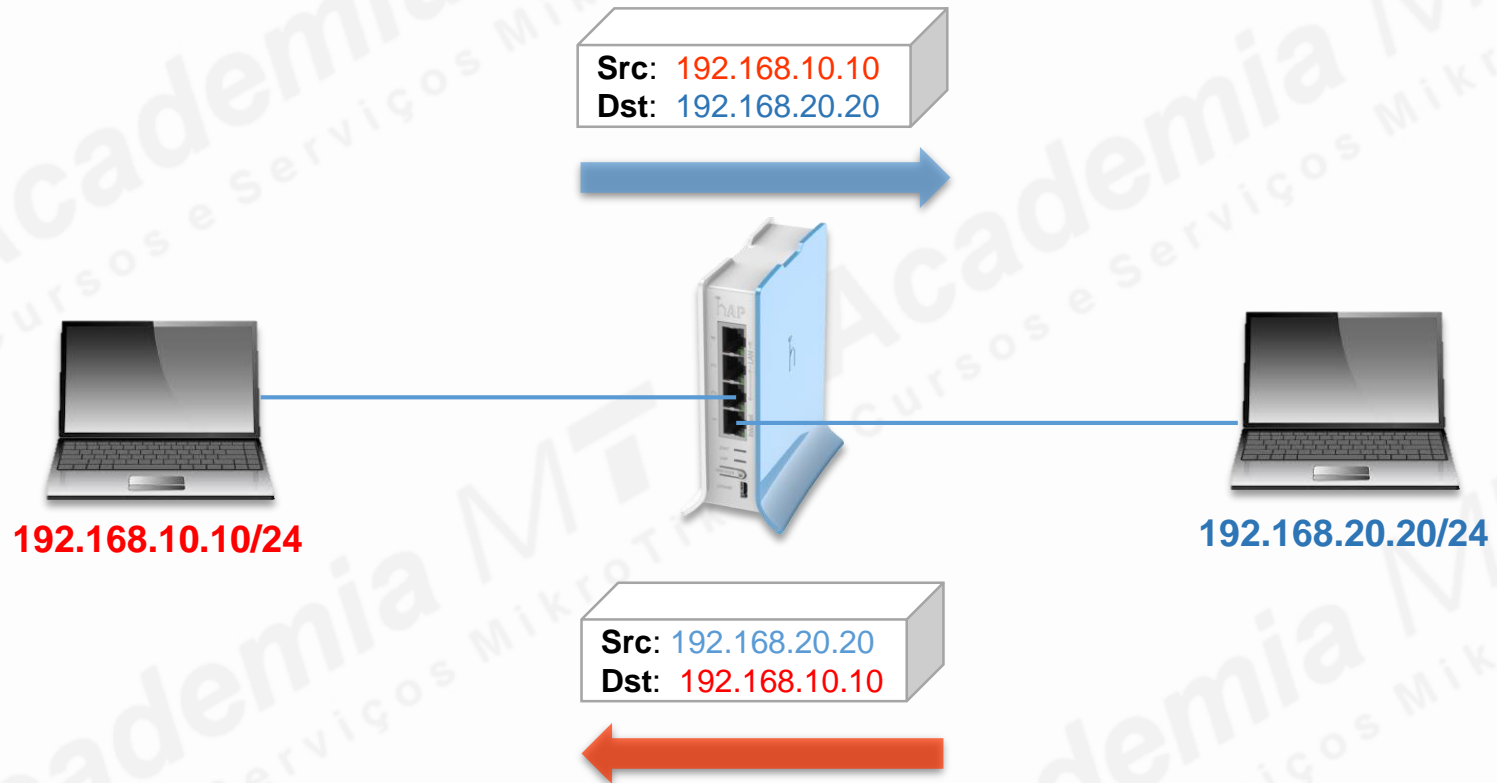


**FORWARD** – Pacote vem de fora e passa ATRAVÉS DO ROUTER

**INPUT** – Pacote vem de fora e vai PARA O ROUTER

**OUTPUT** – Pacote é ORIGINADO NO ROUTER

# /ip firewall connection





# Conexão Estabelecida

The screenshot shows the Mikrotik WinBox Firewall interface. The 'Connections' tab is selected, and the 'Tracking' button is active. A table lists various connections, with the first one highlighted in blue and a red box around it. A detailed view of this connection is shown in a pop-up window.

	Src. Address	Dst. Address	Protocol	Timeout	TCP State	Orig./Repl. Rate	Orig./Repl. Bytes
SAC	172.30.1.198:13089	172.30.1.1:80	6 (tcp)	00:04:59	established	12.0 kbps/61.8 kbps	7.2 KiB/28.5 KiB
SACs	172.30.1.198:13080						1569 B/1843 B
SACs	172.30.1.198:13083						1785 B/3875 B
SACs	172.30.1.198:13084						1785 B/9.4 KiB
SAC	172.30.1.198:13086						7.8 KiB/29.6 KiB
SACs	172.30.1.198:13087						2699 B/6.2 KiB
SACs	172.30.1.198:51007						12.8 KiB/8.0 KiB
SACs	172.30.1.198:51008						2910 B/2217 B
SACs	172.30.1.198:53168						3178 B/2986 B
SACs	172.30.1.198:53169						8.5 KiB/5.2 KiB
SC	172.30.1.198:53732						68 B/174 B
SACs	172.30.1.198:54450						3092 B/2217 B
SACs	172.30.1.198:55891						1501 B/1549 B
SACs	172.30.1.198:57365						887 B/1212 B
SACs	172.30.1.198:61098						2137 B/3450 B
SACs	172.30.1.198:61100						7.2 KiB/53.7 KiB
SACs	172.30.1.198:64243						2481 B/2305 B
SACs	172.30.1.198:64403						4610 B/4012 B
SACs	172.30.1.198:64404						3707 B/3490 B
SACs	172.30.1.198:65061						803 B/860 B
SACs	172.30.1.198:65105						3226 B/3012 B
SC	192.168.15.2:36332						61 B/77 B
SC	192.168.15.2:42237						68 B/174 B
SC	192.168.15.2:45181						58 B/74 B
SC	192.168.15.2:52368						75 B/91 B

**Connection <172.30.1.198:13089->172.30.1.1:80>**

General | Statistics

Src. Address: 172.30.1.198:13089

Dst. Address: 172.30.1.1:80

Reply Src. Address: 172.30.1.1:80

Reply Dst. Address: 172.30.1.198:13089

Protocol: 6 (tcp)

Connection Type:

Connection Mark:

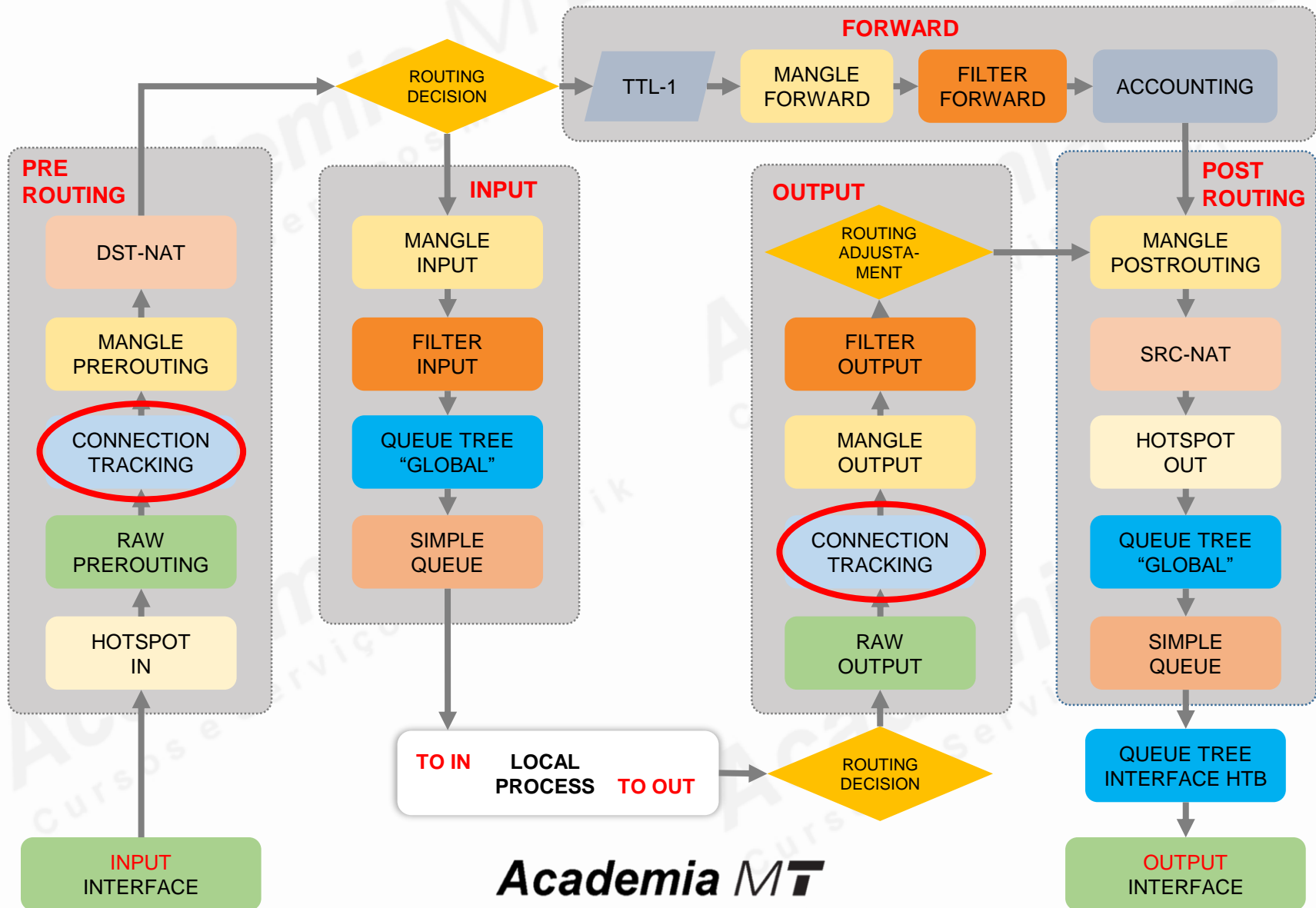
Timeout: 00:04:59

TCP State: established

expected | seen reply | assured | confirmed | dying | fasttrack | srcnat | dstnat

OK | Remove

# Fluxo de Pacotes Connection Tracking



`/ip firewall nat add chain=`

**New NAT Rule**

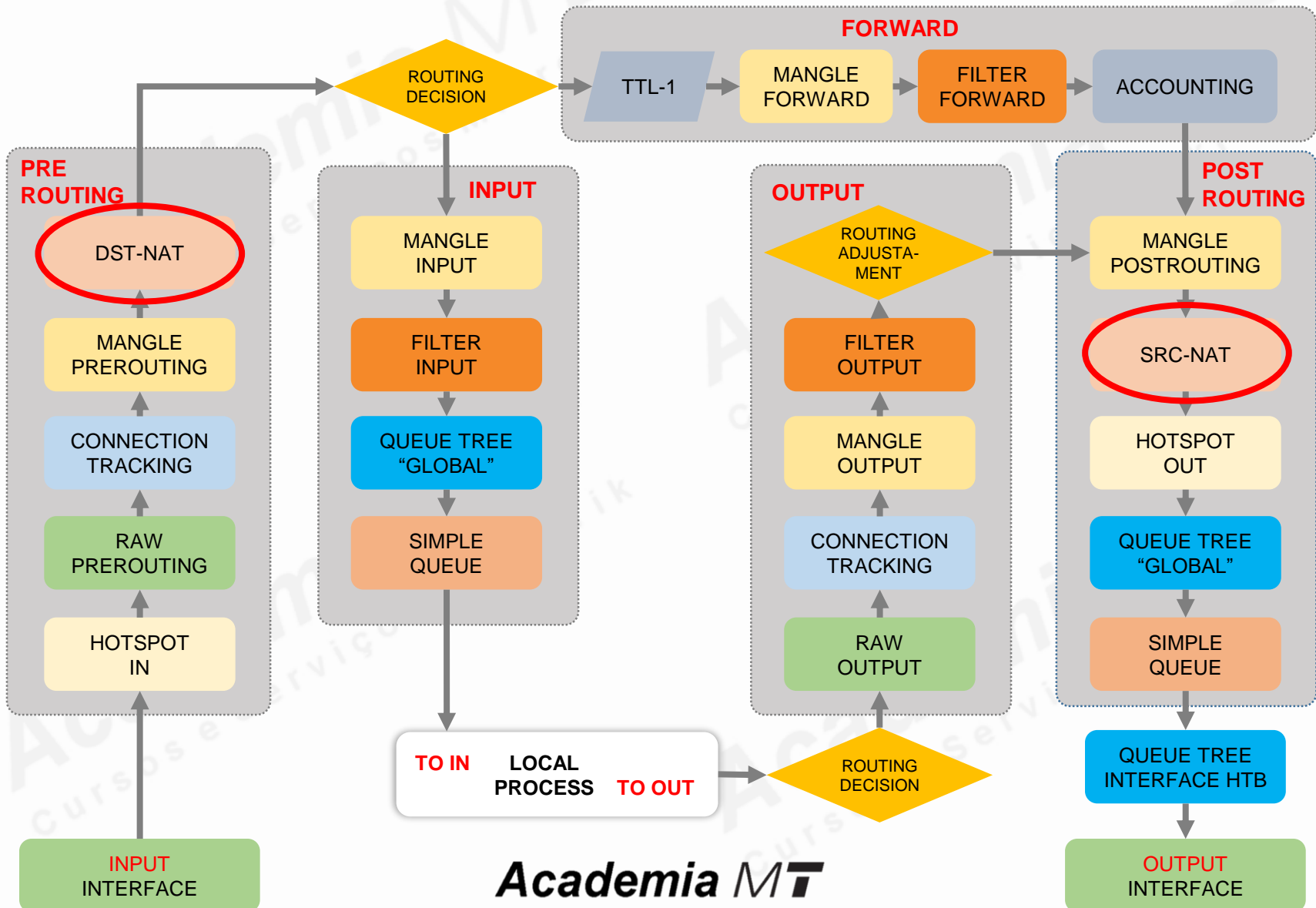
General | Advanced | Extra

Chain: srcnat

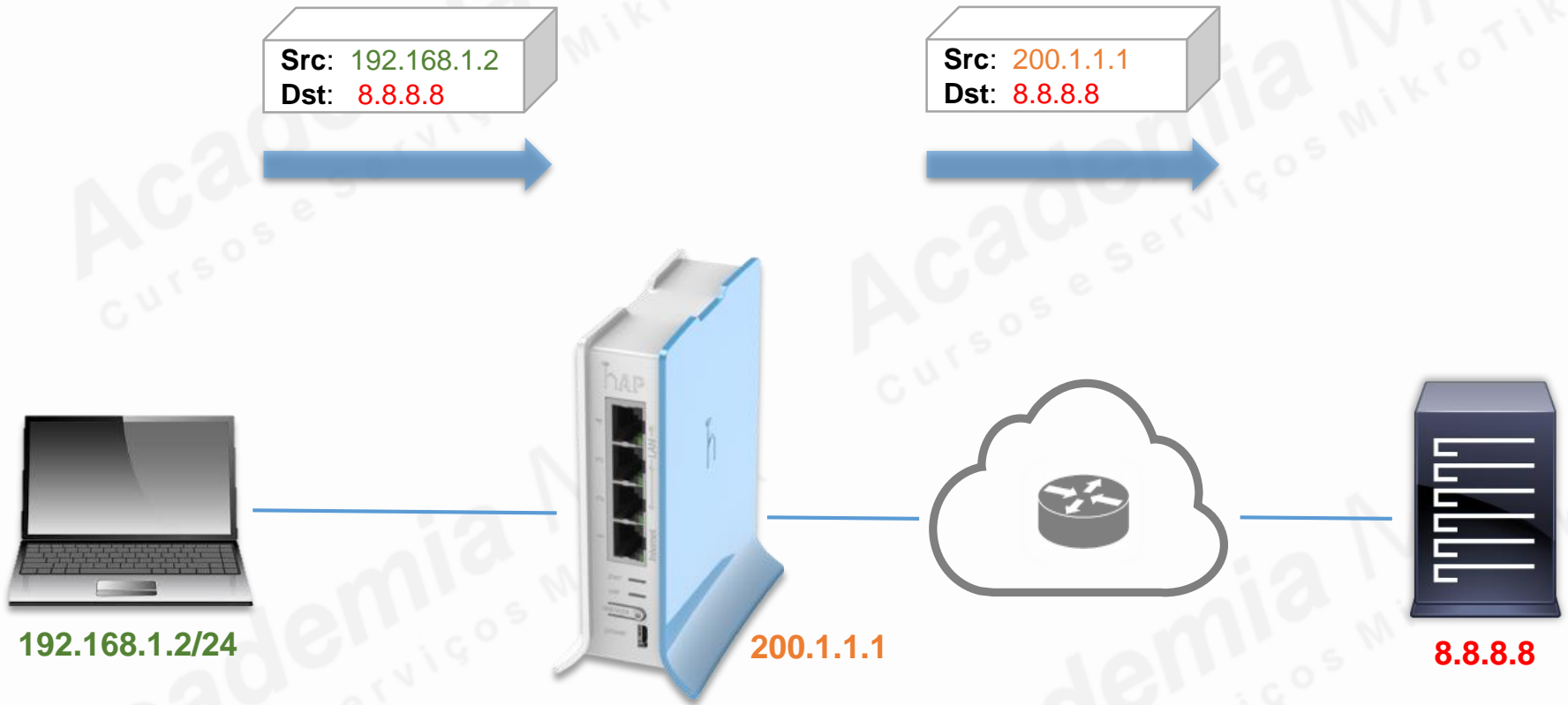
Src. Address: dstnat

srcnat

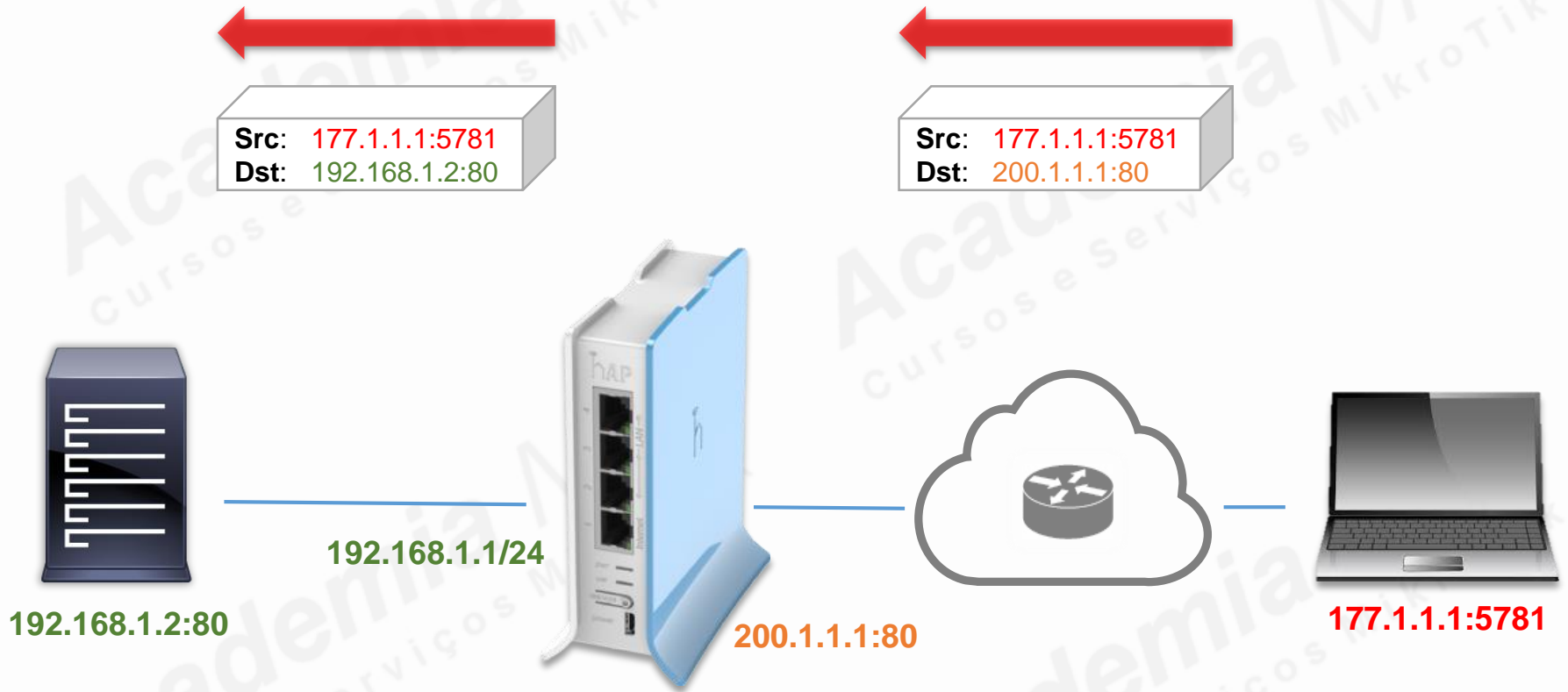
# Fluxo de Pacotes src-nat e dst-nat



# /ip firewall nat add chain=srcnat



# /ip firewall nat add chain=dstnat



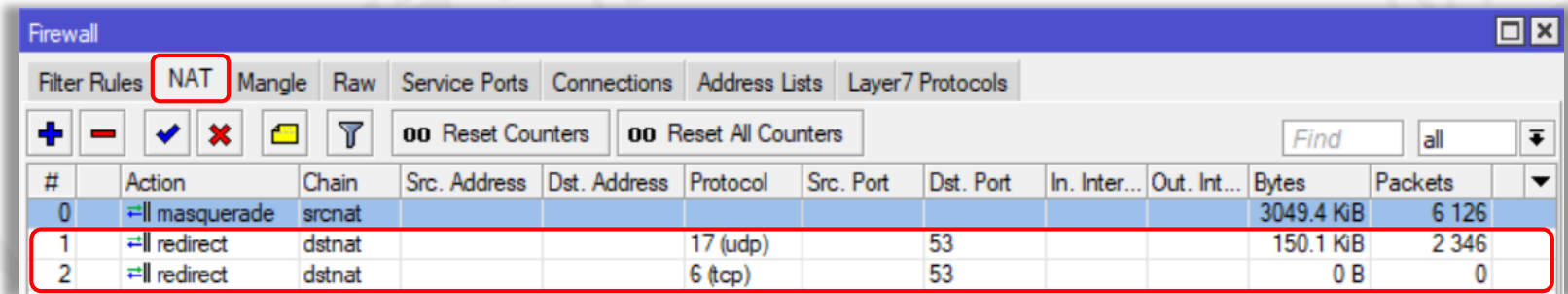
# /ip firewall nat add chain=dstnat

DICA

## Objetivo

- Usar a `action=redirect` pra enviar ao próprio Router as consultas DNS

```
/ip firewall nat
add action=redirect chain=dstnat dst-port=53 protocol=udp
add action=redirect chain=dstnat dst-port=53 protocol=tcp
```



The screenshot shows the Mikrotik WinBox interface for the Firewall NAT tab. The 'NAT' tab is selected and highlighted with a red box. Below the tab, there are buttons for adding (+), removing (-), enabling (checkmark), disabling (cross), and other actions. A search bar and 'Find' button are also visible. The main table displays the configured NAT rules:

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	masquerade	srcnat								3049.4 KiB	6 126
1	redirect	dstnat			17 (udp)		53			150.1 KiB	2 346
2	redirect	dstnat			6 (tcp)		53			0 B	0

# /ip firewall mangle add chain=

New Mangle Rule

General Advanced Extra Action

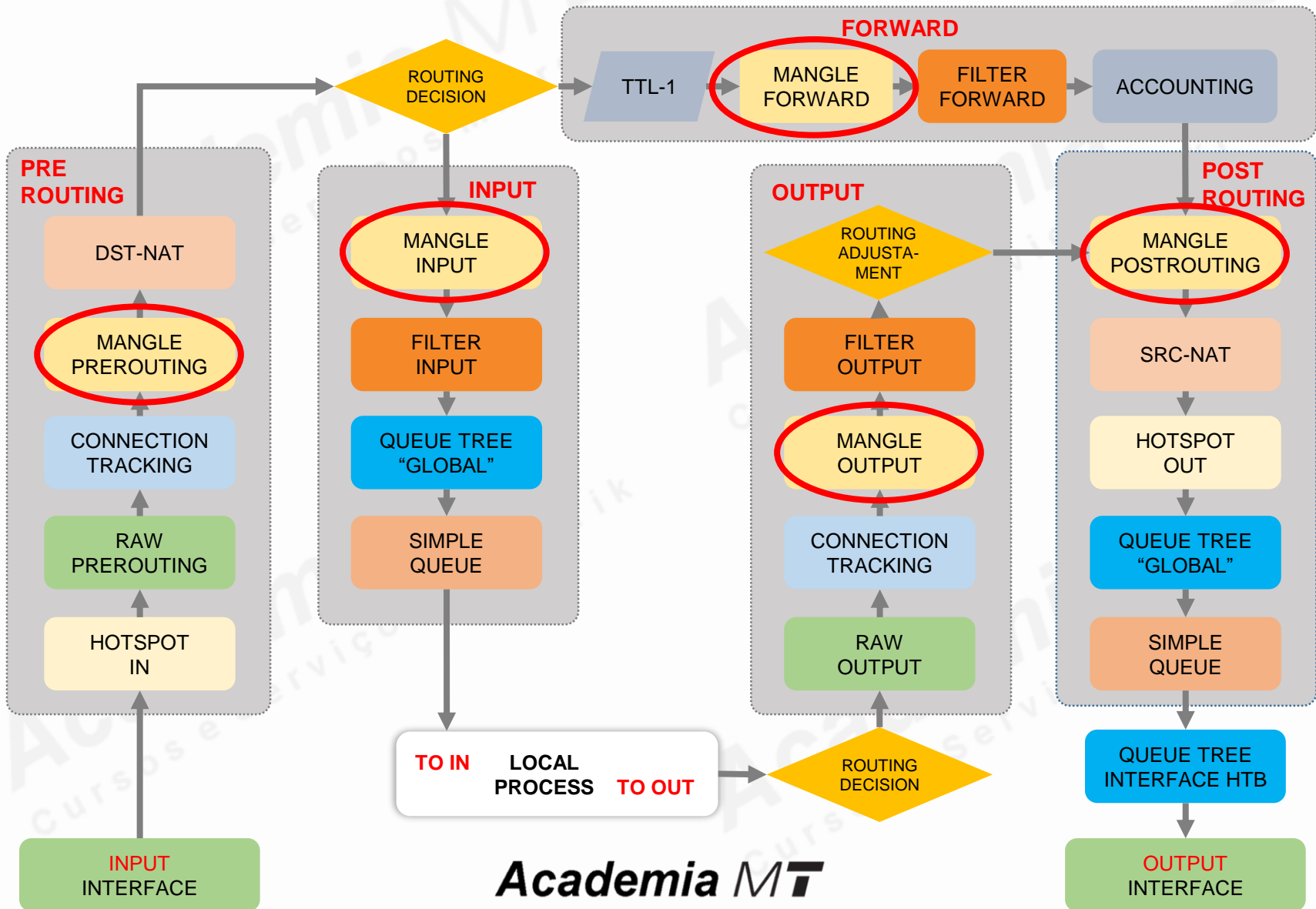
Chain: prerouting

Src. Address: input  
output  
postrouting  
prerouting

Dst. Address: postrouting  
prerouting



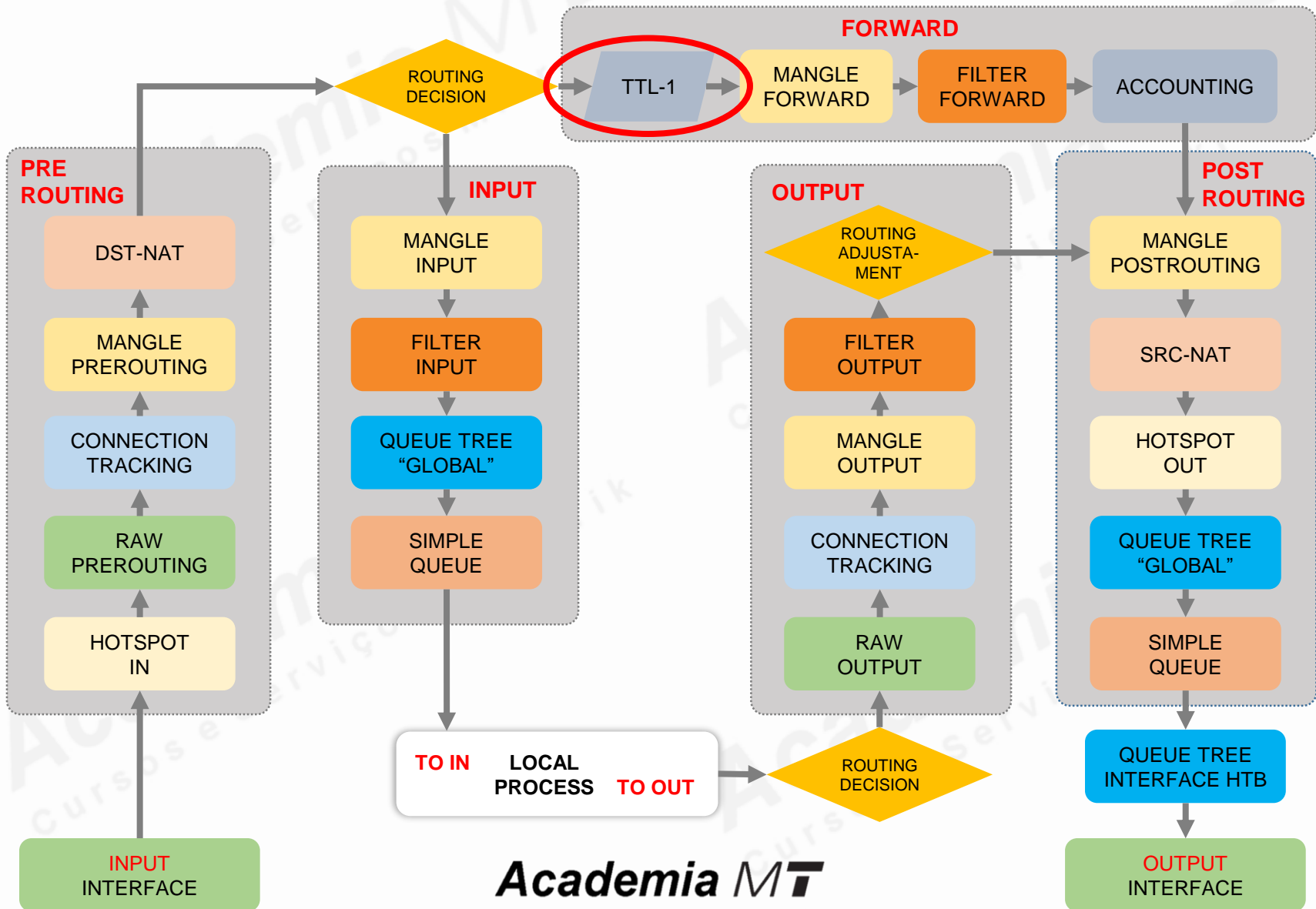
# Fluxo de Pacotes Mangle



# Camada 3, Rede - Cabeçalho IPv4

Versão (Version)	Tamanho do Cabeçalho (IHL)	Tipo de Serviço (ToS)	Tamanho Total (Total Length)	
Identificação (Identification)		Flags	Deslocamento do Fragmento (Fragment Offset)	
Tempo de Vida (TTL)		Protocolo (Protocol)	Soma de verificação do Cabeçalho (Checksum)	
Endereço de Origem (Source Address)				
Endereço de Destino (Destination Address)				
Opções + Complemento (Options + Padding)				

# Fluxo de Pacotes TTL-1

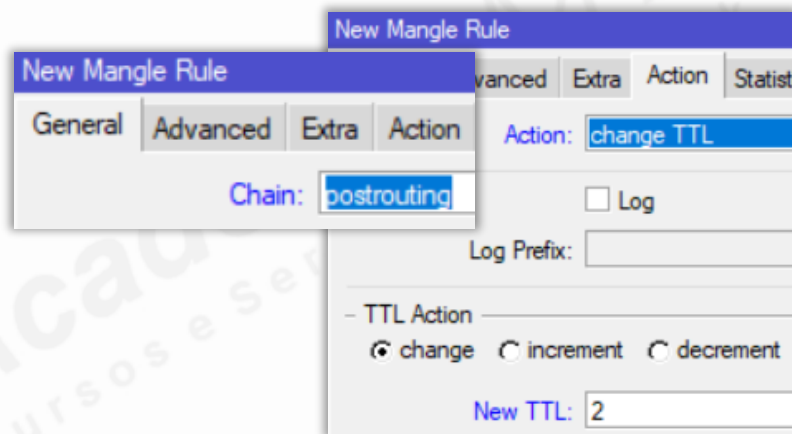
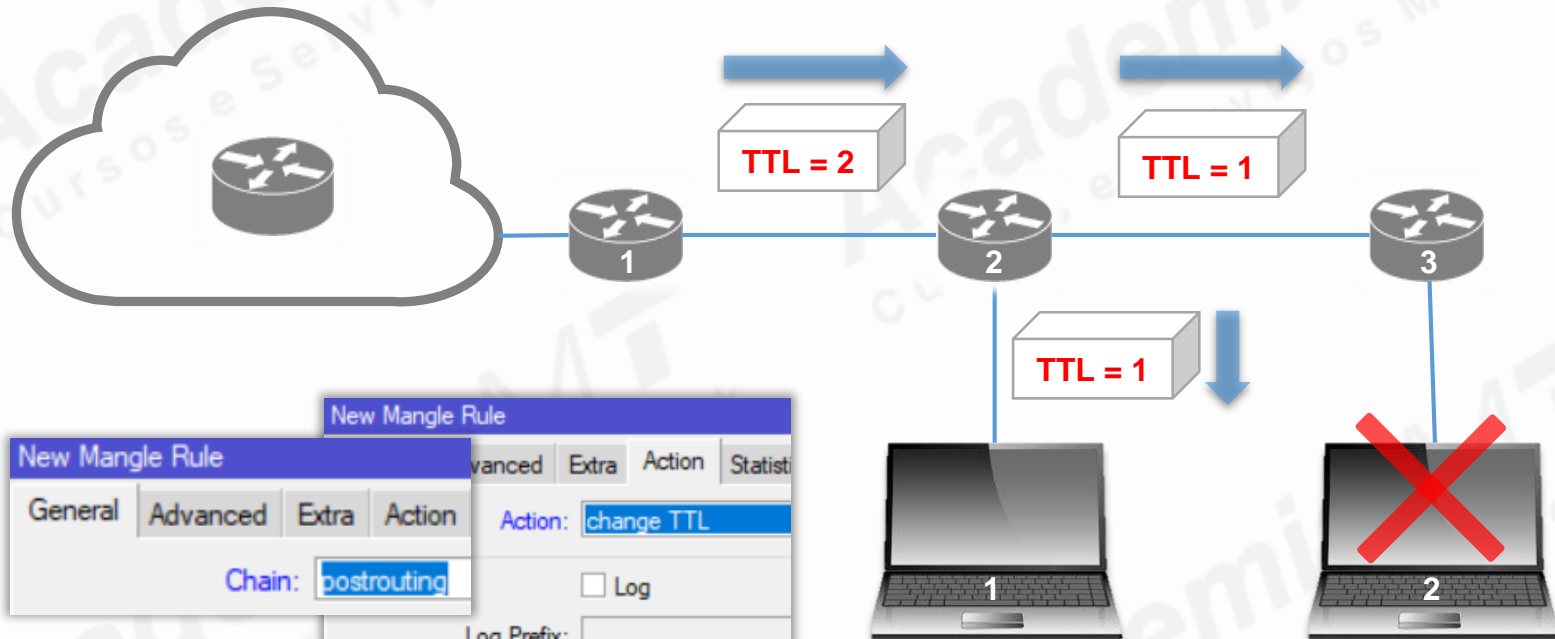


# /ip firewall mangle set action=change-ttl

## Objetivo

- Não redistribuir Internet ao acrescentar um novo Router

DICA

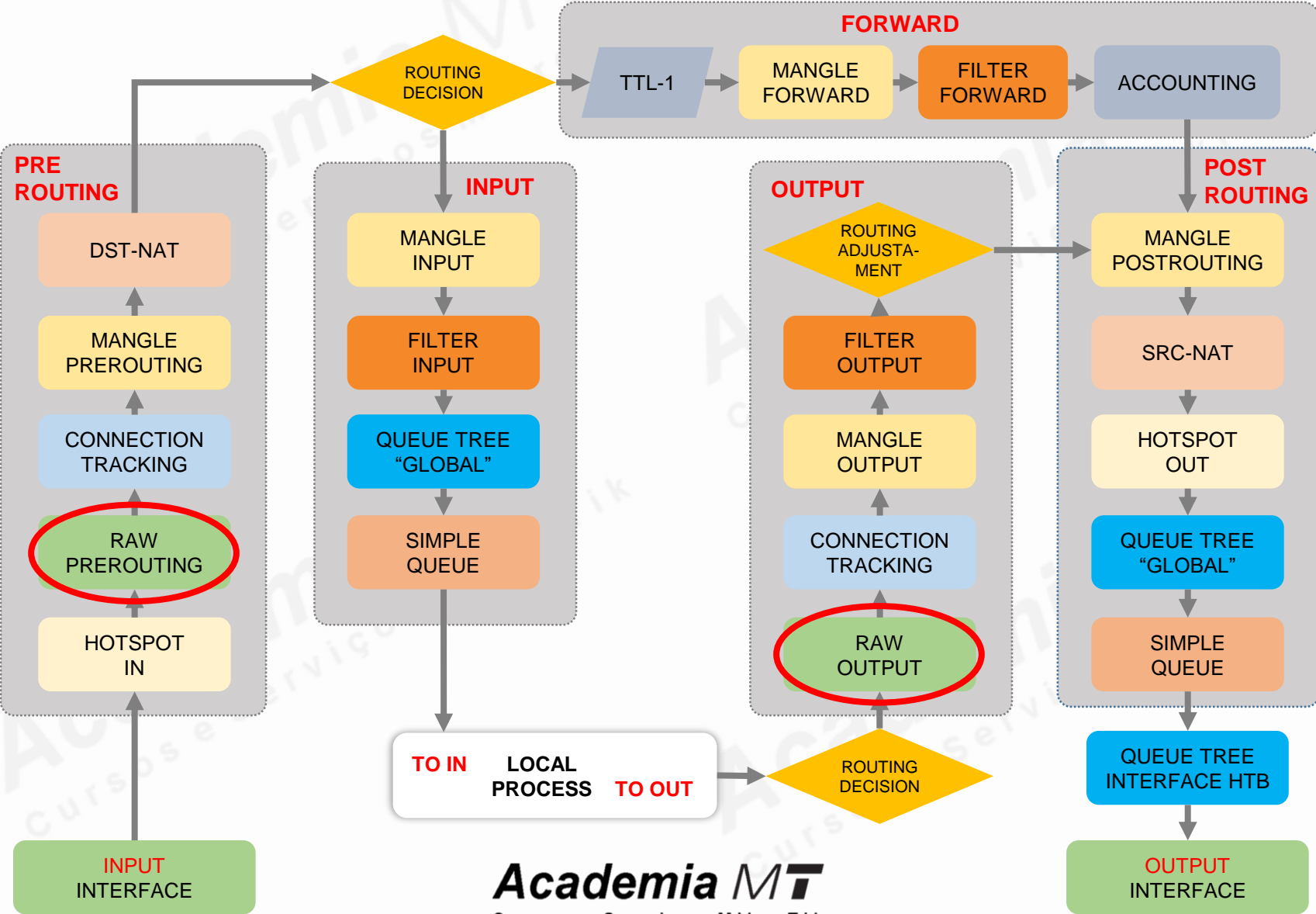


`/ip firewall raw add chain=`

The screenshot shows the 'New Raw Rule' configuration window. The 'Chain' dropdown is set to 'prerouting' and the 'Src. Address' dropdown is set to 'prerouting'. Both dropdowns are highlighted with red boxes.

Field	Value
Chain:	prerouting
Src. Address:	prerouting

# Fluxo de Pacotes Raw



# /ip firewall raw set action=drop

DICA

## Objetivos

- Bloquear **Spoofing** (falsificação) dos IPs Rede Local
- Estar em conformidade com a RFC 2827 ou **BCP 38** criadas 2000)
- Diminuir em quase 100% o número de Ataques para a Internet

## Comandos

```
/interface list add name=LAN
/interface list member add interface=ether3_LAN list=LAN
/ip firewall address-list add address=192.168.1.0/24 list=REDE_LOCAL
/ip firewall raw
add action=drop chain=prerouting comment="Anti Spoofing - BCP 38" \
  in-interface-list=LAN src-address-list=!REDE_LOCAL
```

# /ip firewall raw set action=accept e drop

DICA

## Objetivos

- Aceitar **50 Pings** por segundo e dropar o resto
- Consumir menos processamento em um ataque de **Ping Flood**

## Comandos

```
/ip firewall raw
```

```
add action=accept chain=prerouting comment="50 Pings por segundo" limit=\
50,5:packet protocol=icmp
add action=drop chain=prerouting comment="Ping" protocol=icmp
```



# /ip firewall raw set action=drop

DICA

## Objetivos

- Bloquear acessos vindos da WAN para serviços privados
- Prevenir ataques de Amplificação, DoS e Flooding, ao Router e para a Rede Local

## Comandos

```
/ip firewall raw
```

```
add chain=prerouting in-interface=WAN action=drop protocol=udp dst-port="53,123,161,1900" comment="Previne Amplificação de DNS, NTP, SNMP e SSDP"
```

```
add chain=prerouting in-interface=WAN action=drop protocol=tcp dst-port="22,23,53,80,2000,8080" comment="Portas Mais Visadas"
```

# /ip firewall raw set action=drop

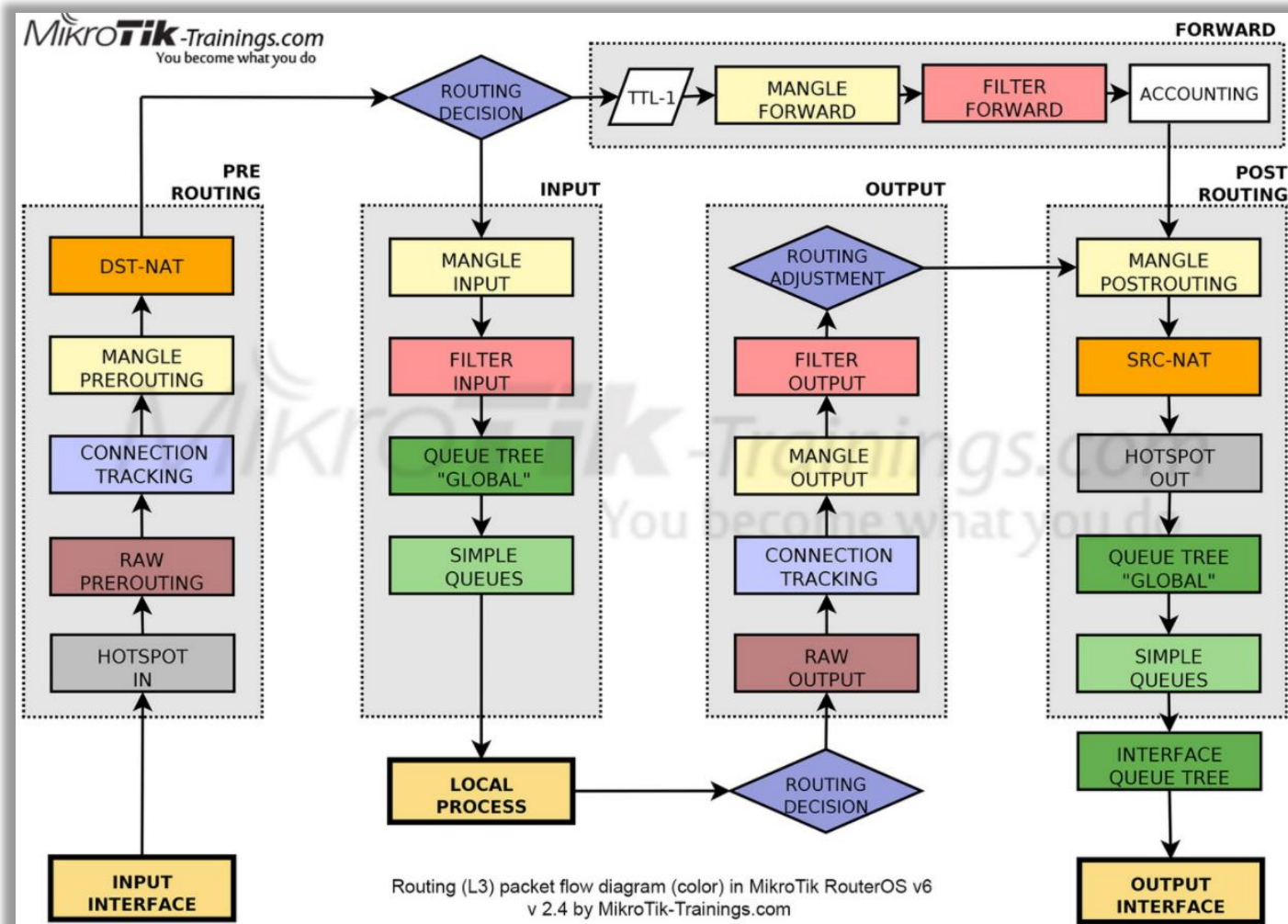
DICA

## Objetivo

- Bloquear Prefixos BOGONS

```
/ip firewall address-list
add address=0.0.0.0/8 comment="Auto Identificacao" list=BOGONS
add address=10.0.0.0/8 comment="Privada - Verifique se voce necessita" \
  disabled=yes list=BOGONS
add address=127.0.0.0/8 comment="Loopback" list=BOGONS
add address=169.254.0.0/16 comment="Link Local - APIPA" list=BOGONS
add address=172.16.0.0/12 comment="Privada - Verifique se voce necessita" \
  disabled=yes list=BOGONS
add address=192.168.0.0/16 comment="Privada - Verifique se voce necessita" \
  disabled=yes list=BOGONS
add address=192.0.2.0/24 comment="Reservada - TestNet1" list=BOGONS
add address=192.88.99.0/24 comment="6to4 Relay Anycast" list=BOGONS
add address=198.18.0.0/15 comment="Teste NIDB" list=BOGONS
add address=198.51.100.0/24 comment="Reservada - TestNet2" list=BOGONS
add address=203.0.113.0/24 comment="Reservada - TestNet3" list=BOGONS
add address=224.0.0.0/4 comment="Multicast - Verifique se voce necessita" \
  disabled=yes list=BOGONS
/ip firewall raw
add action=drop chain=prerouting comment="dst BOGONS" dst-address-list=BOGONS
```

# Crédito



<https://www.mikrotik-trainings.com/docs#form>

# Conteúdo Abordado



1. Modelos OSI e Híbrido (Revisão)
2. Diagrama do Fluxo dos Pacotes
3. Firewall
  1. Filter / NAT / Mangle / Raw / Connections
4. Dicas pro Dia a Dia

# ***Academia MT***

Cursos e Serviços MikroTik

---

## **Obrigado!**

---

## **João Krieger**

**48 9-9982-8707**

**krieger@academiamt.com.br**

---

# Treinamentos MikroTik

