Academia MT

Cursos e Serviços MikroTik

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

Linux Professional Institute
LPIC-2

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

Camada 3, Rede - Cabeçalho IPv4

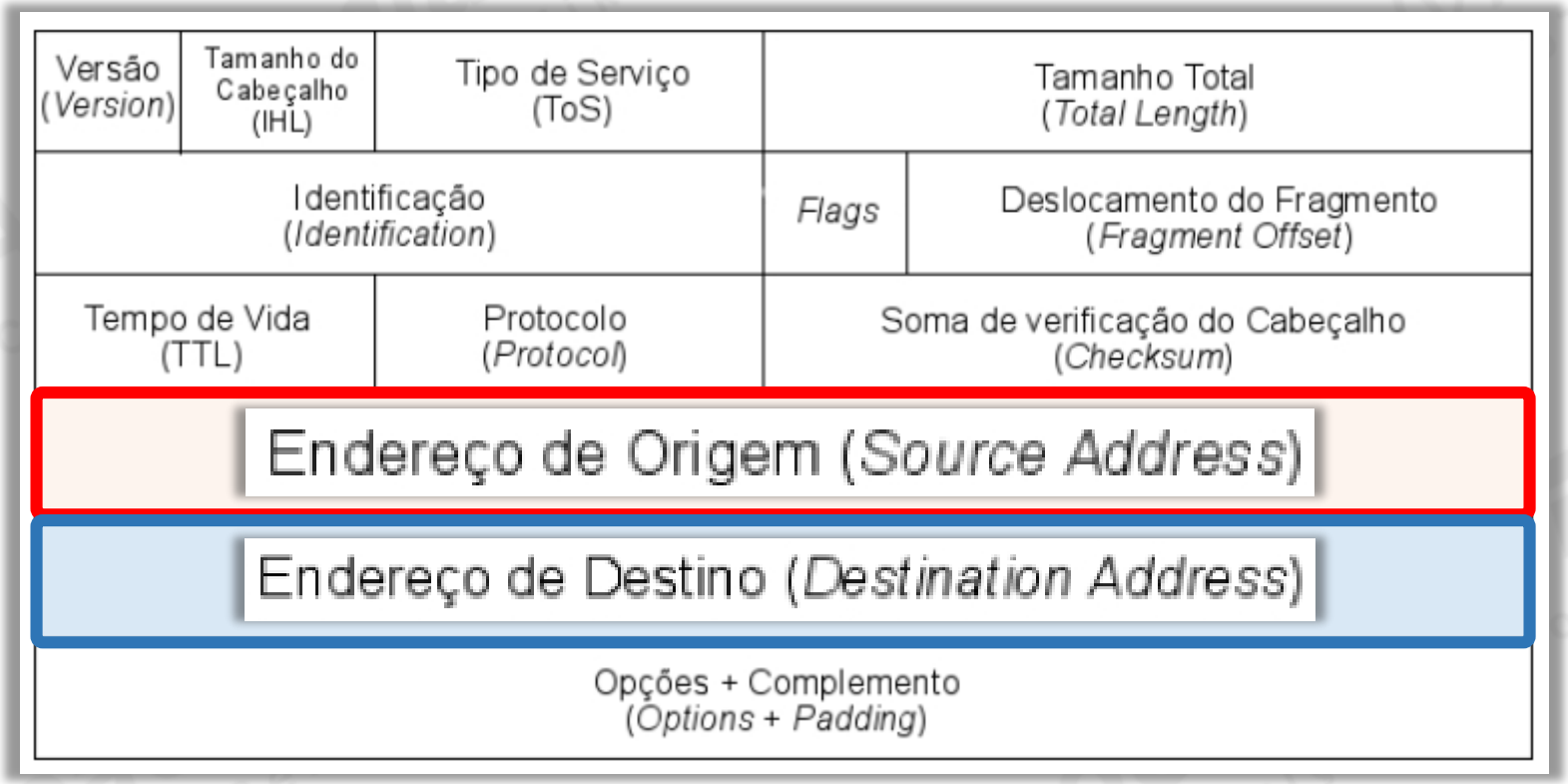
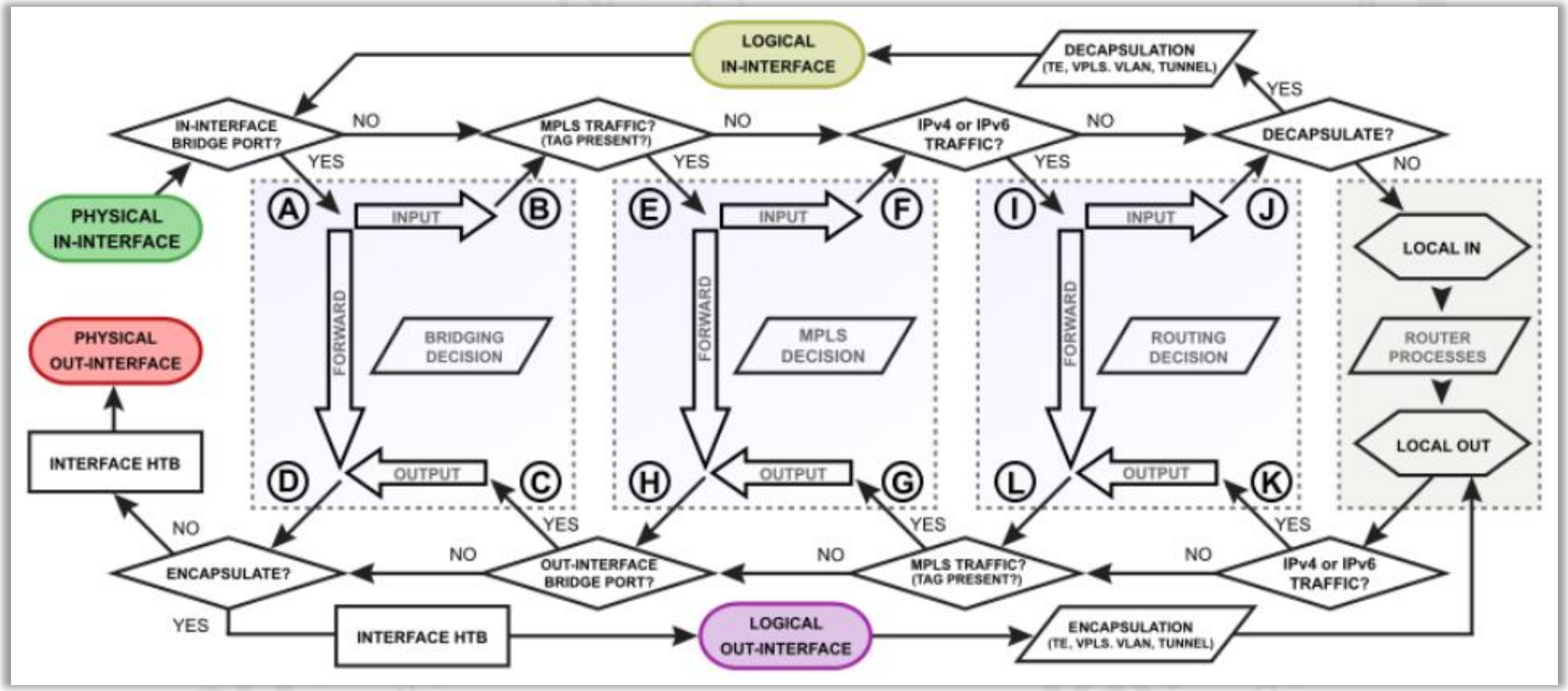


Diagrama do Fluxo de Pacotes

- **Porque é necessário conhecê-lo?**

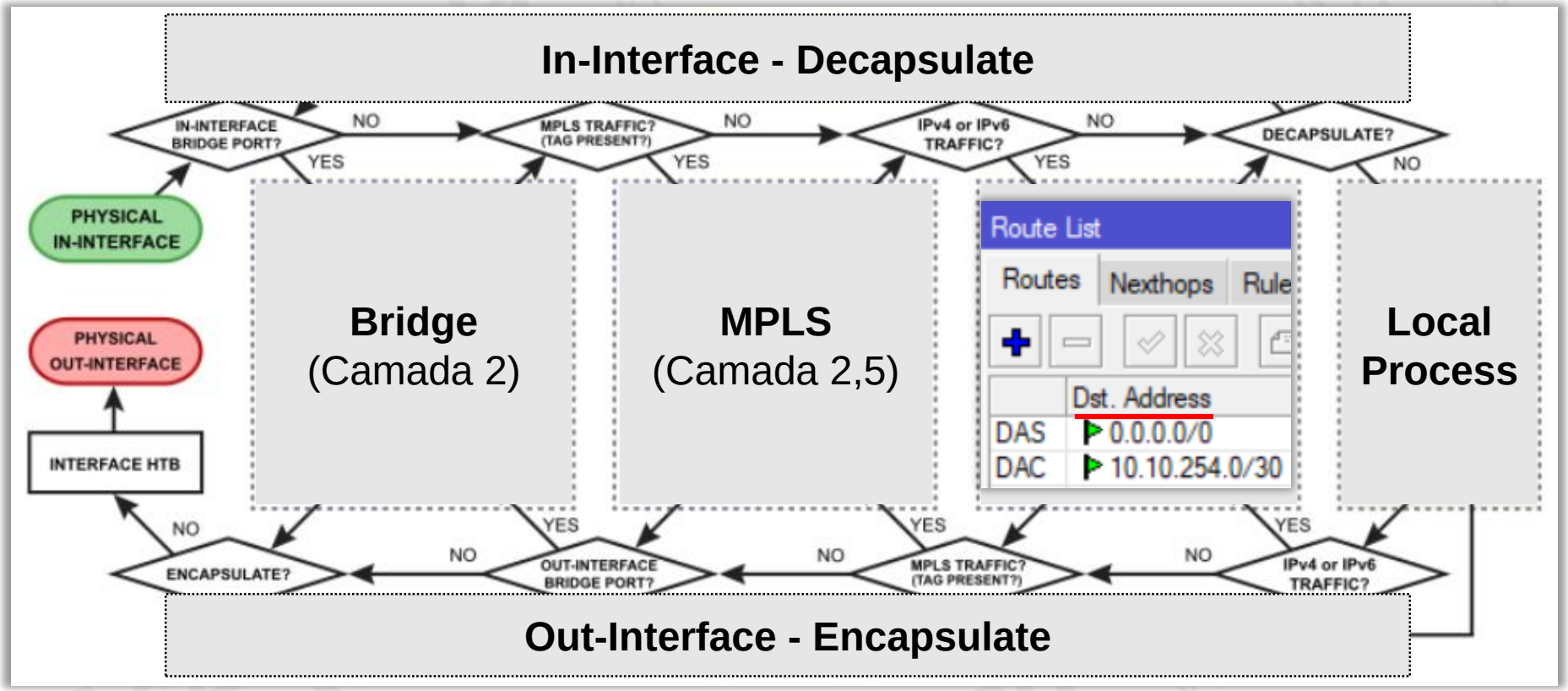
1. Para sabermos quando, porque e onde passam os pacotes no RouterOS
2. Resolver tarefas mais complicadas como bloqueios
3. Fazer redirecionamentos, marcações e classificações
4. Priorizar tráfego e fazer QoS
5. Criar políticas de roteamento
6. E …

Diagrama em Blocos do Fluxo de Pacotes

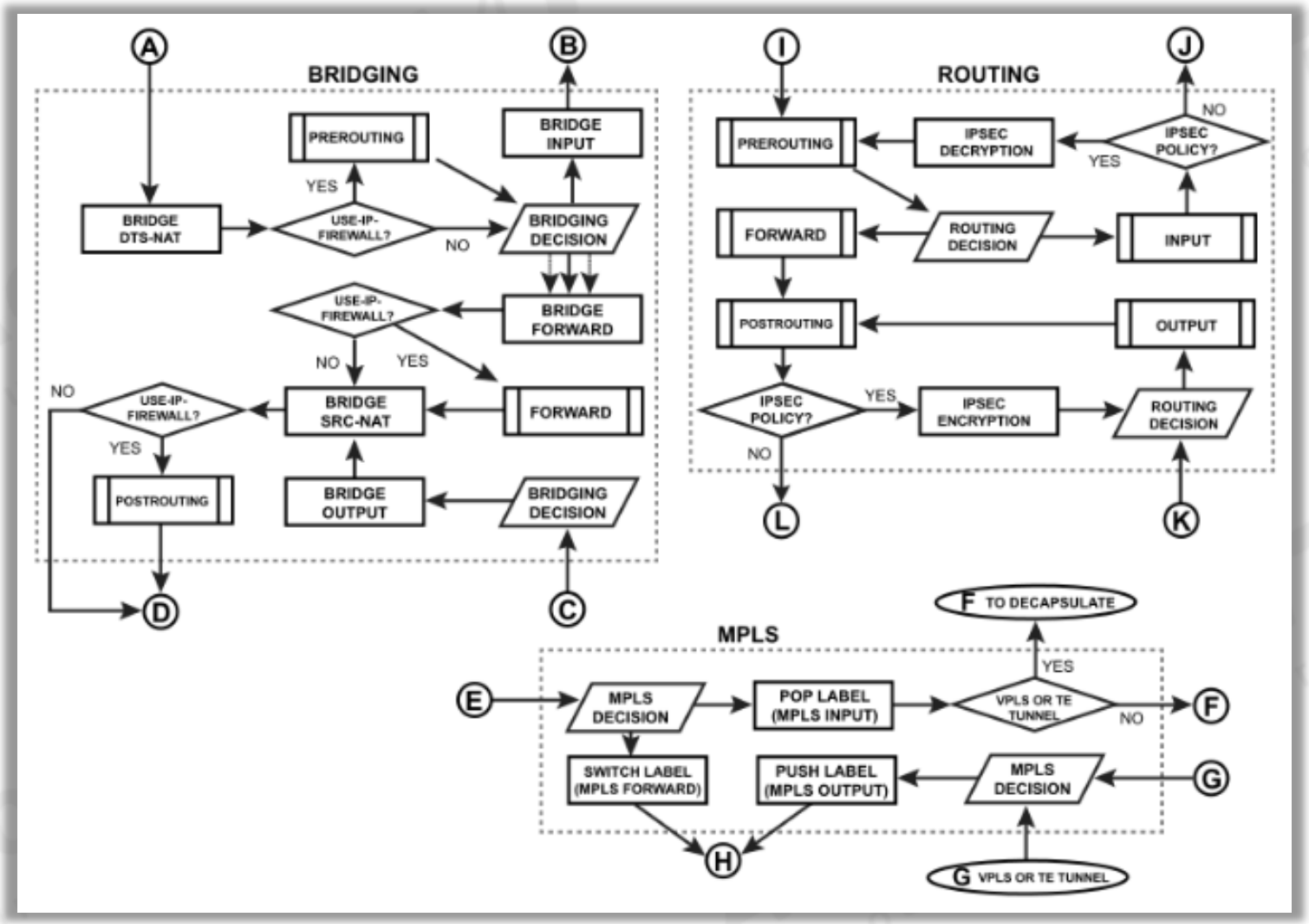


https://wiki.mikrotik.com/wiki/Manual:Packet_Flow

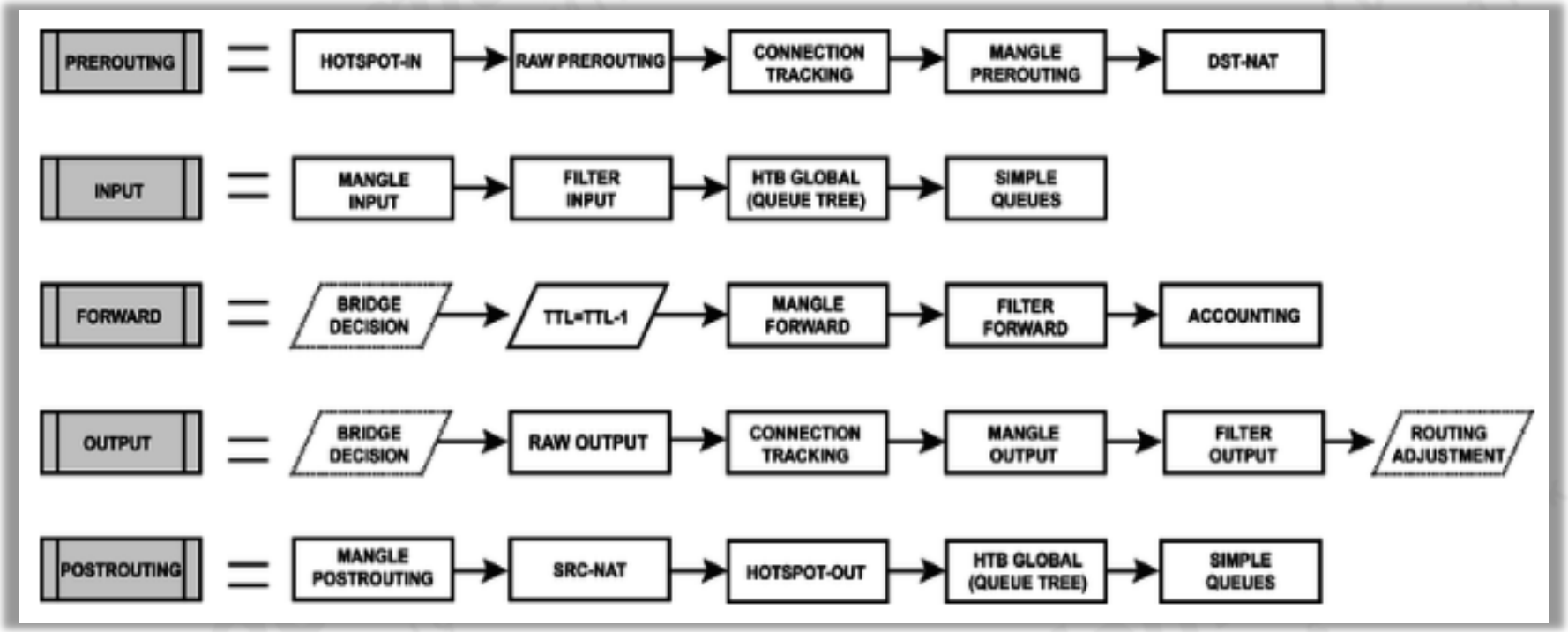
Fluxo de Pacotes em Blocos Simples



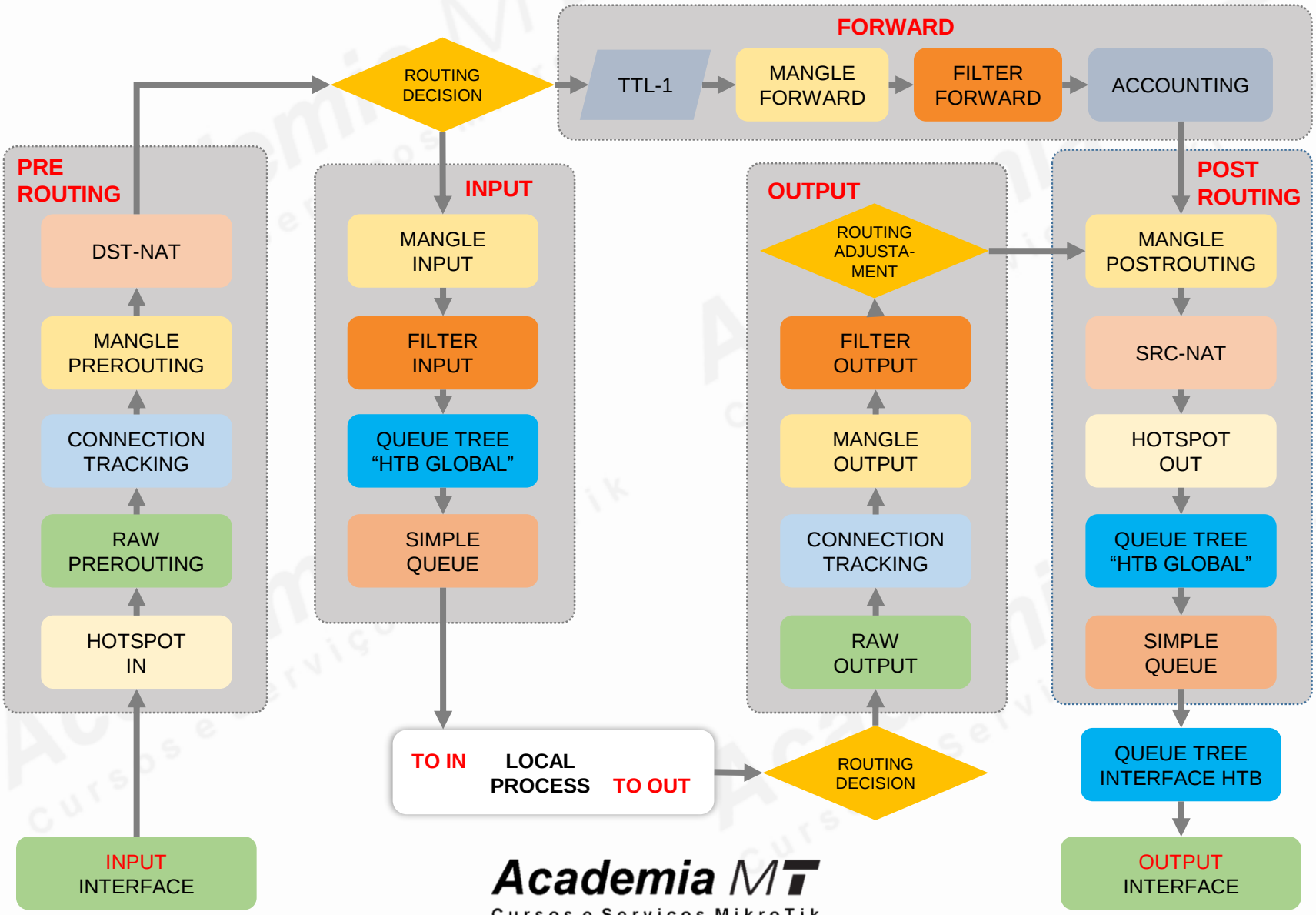
Decisões Expandidas



Chains (corrente) de Fluxo dos Pacotes

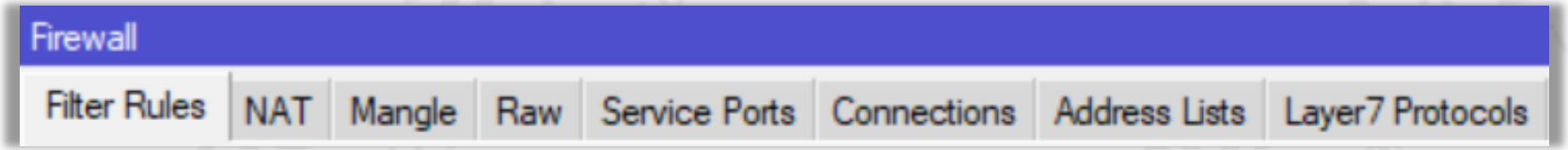


Fluxo dos Pacotes IP Completo



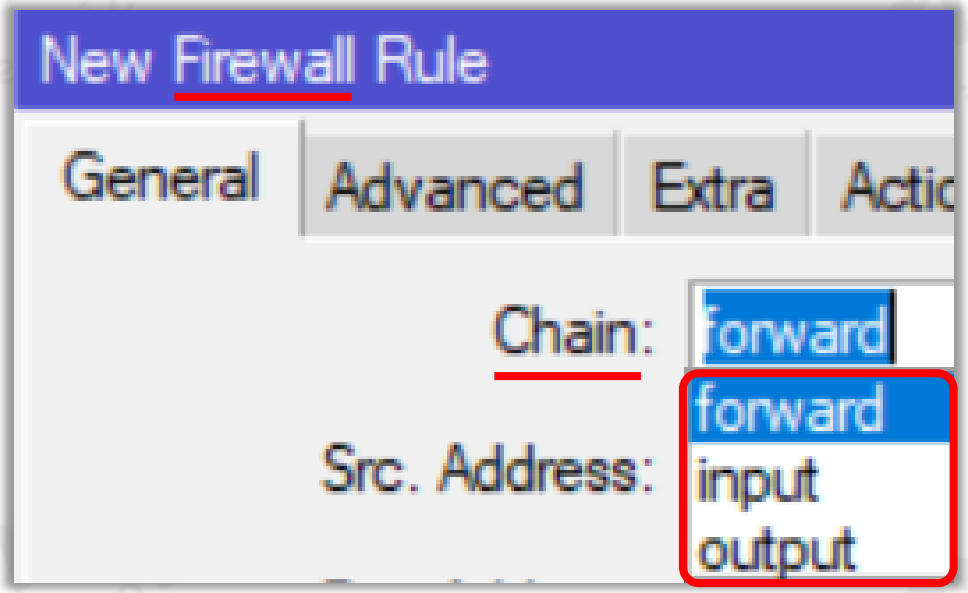
Academia MT
Cursos e Serviços MikroTik

Tabelas em /ip firewall

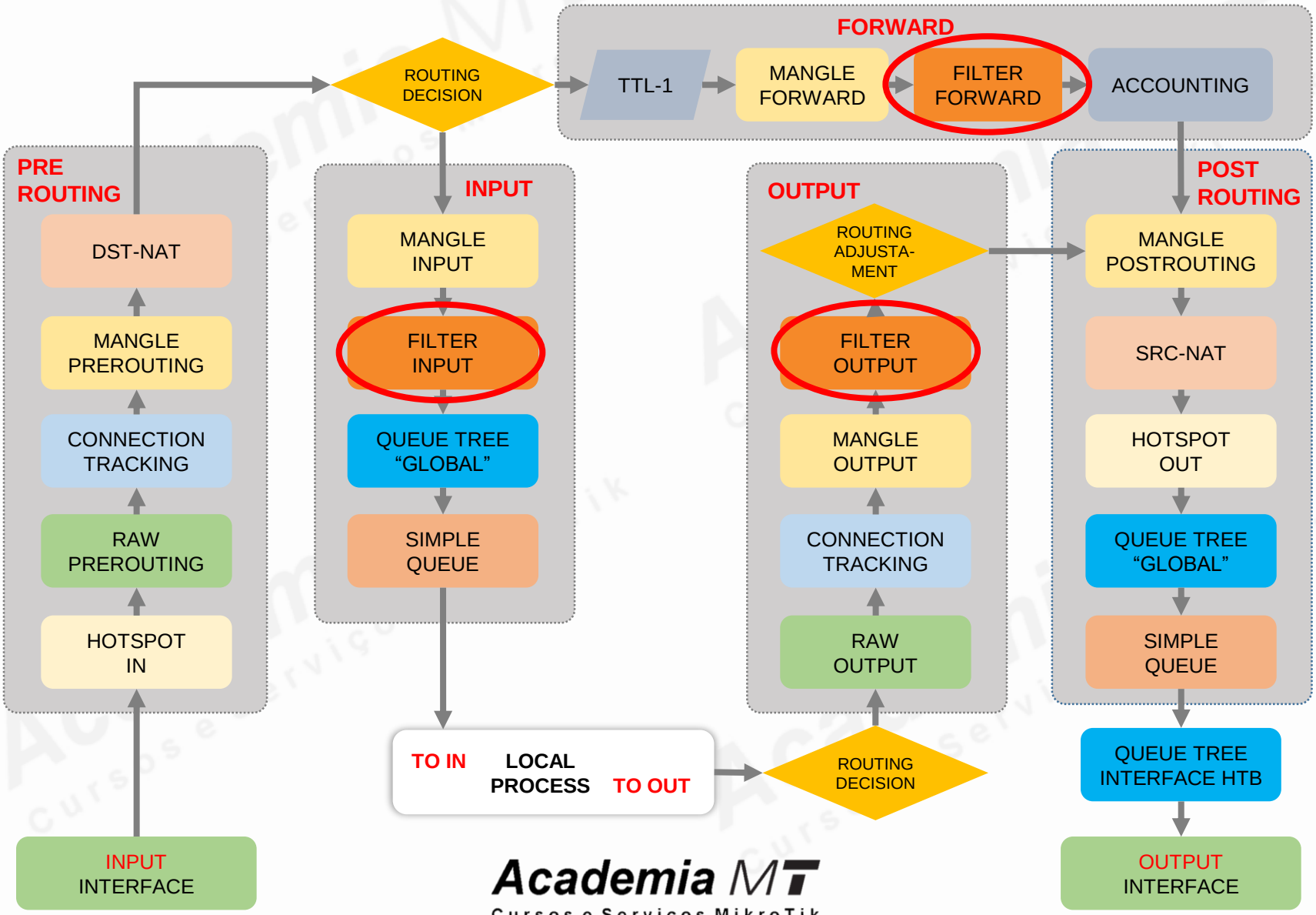


1. **Filter Rules**: Filtra pacotes
2. **NAT**: Traduz endereços e portas
3. **Mangle**: Marca conexões, pacotes e roteamento, também pode alterar campos no cabeçalho
4. **Raw:** Salta a Conntrack, protege e agiliza
5. **Connections**: Rastreia conexões (ConnTrack)

/ip firewall filter add chain=

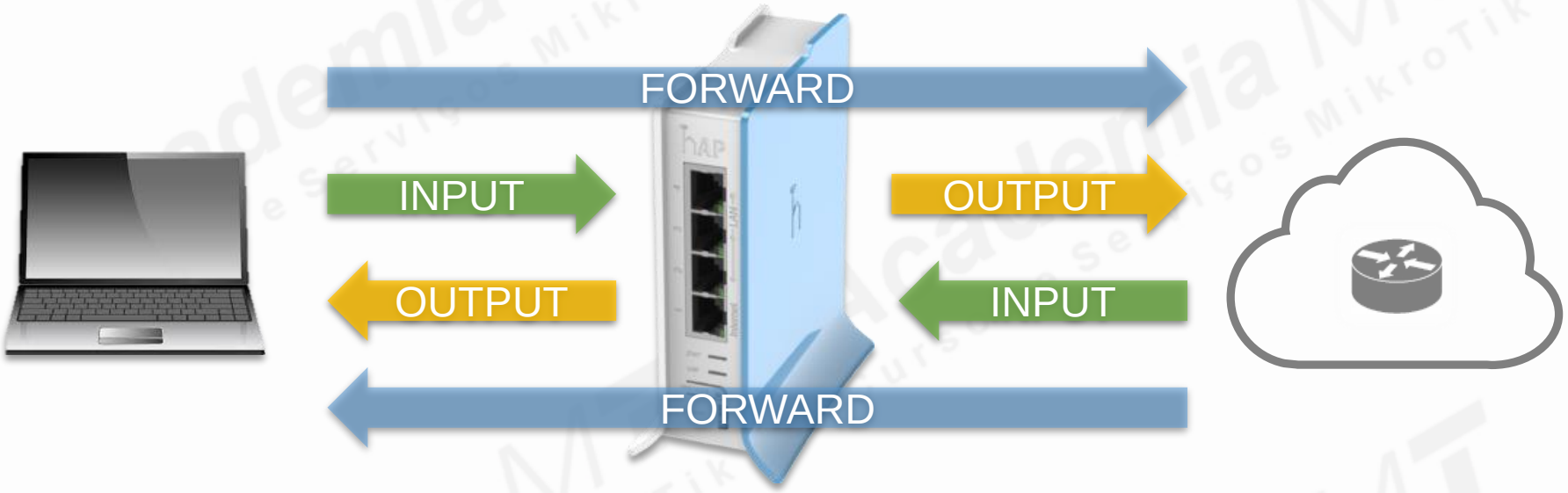


/ip firewall filter add chain=



Academia MT
Cursos e Serviços MikroTik

/ip firewall filter add chain=

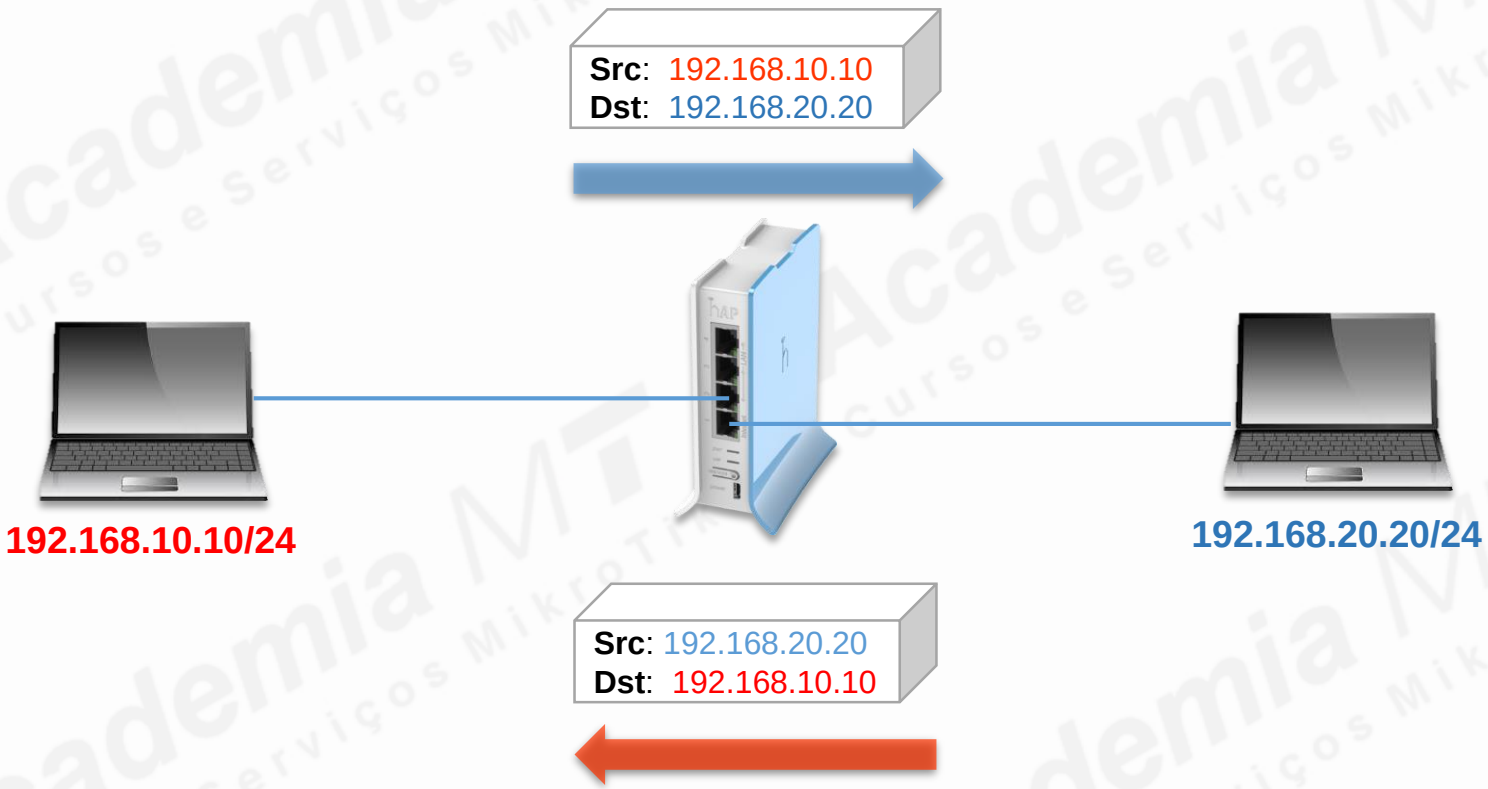


FORWARD – Pacote vem de fora e passa **ATRAVÉS DO ROUTER**

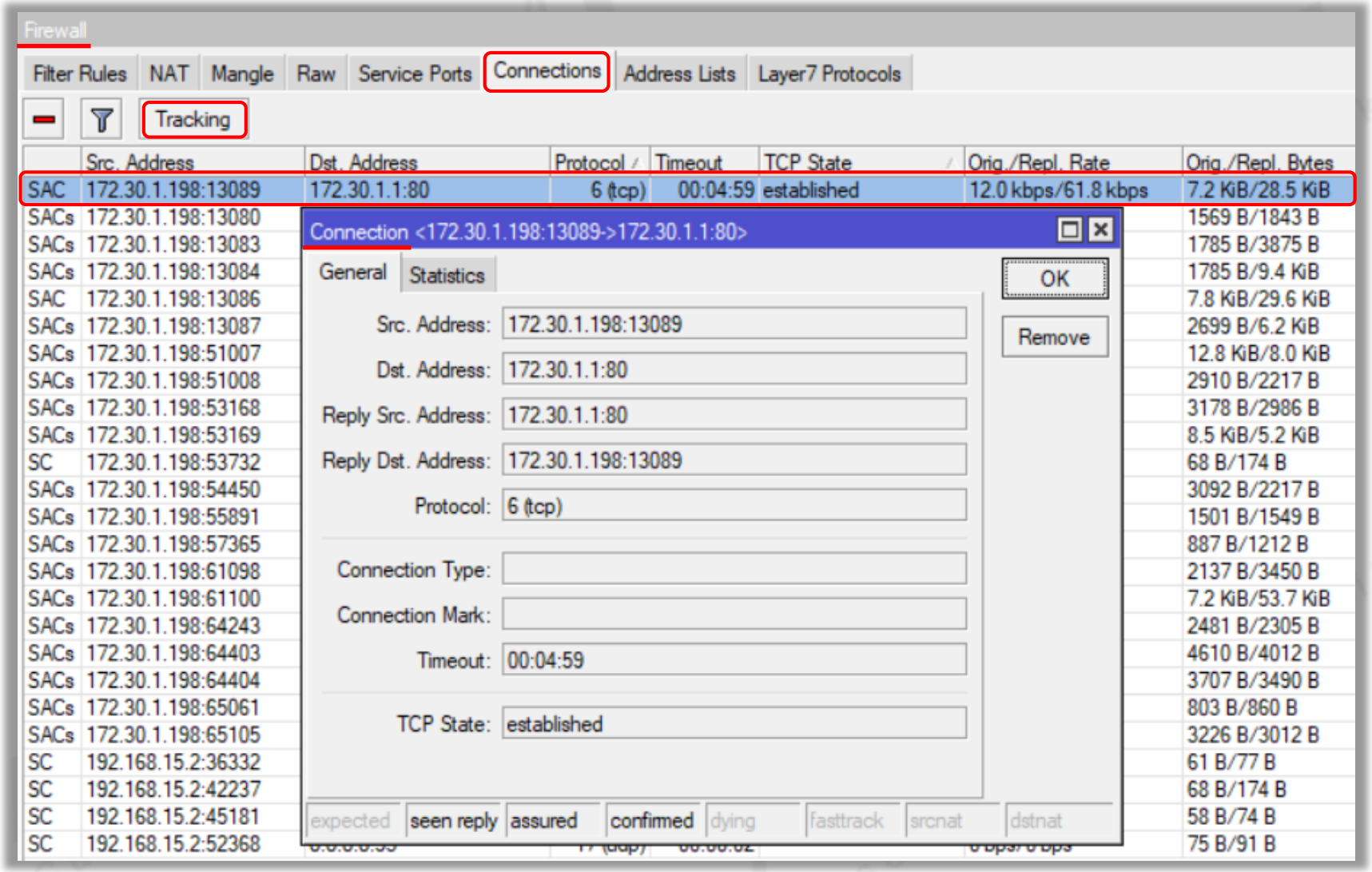
INPUT – Pacote vem de fora e vai **PARA O ROUTER**

OUTPUT – Pacote é **ORIGINADO NO ROUTER**

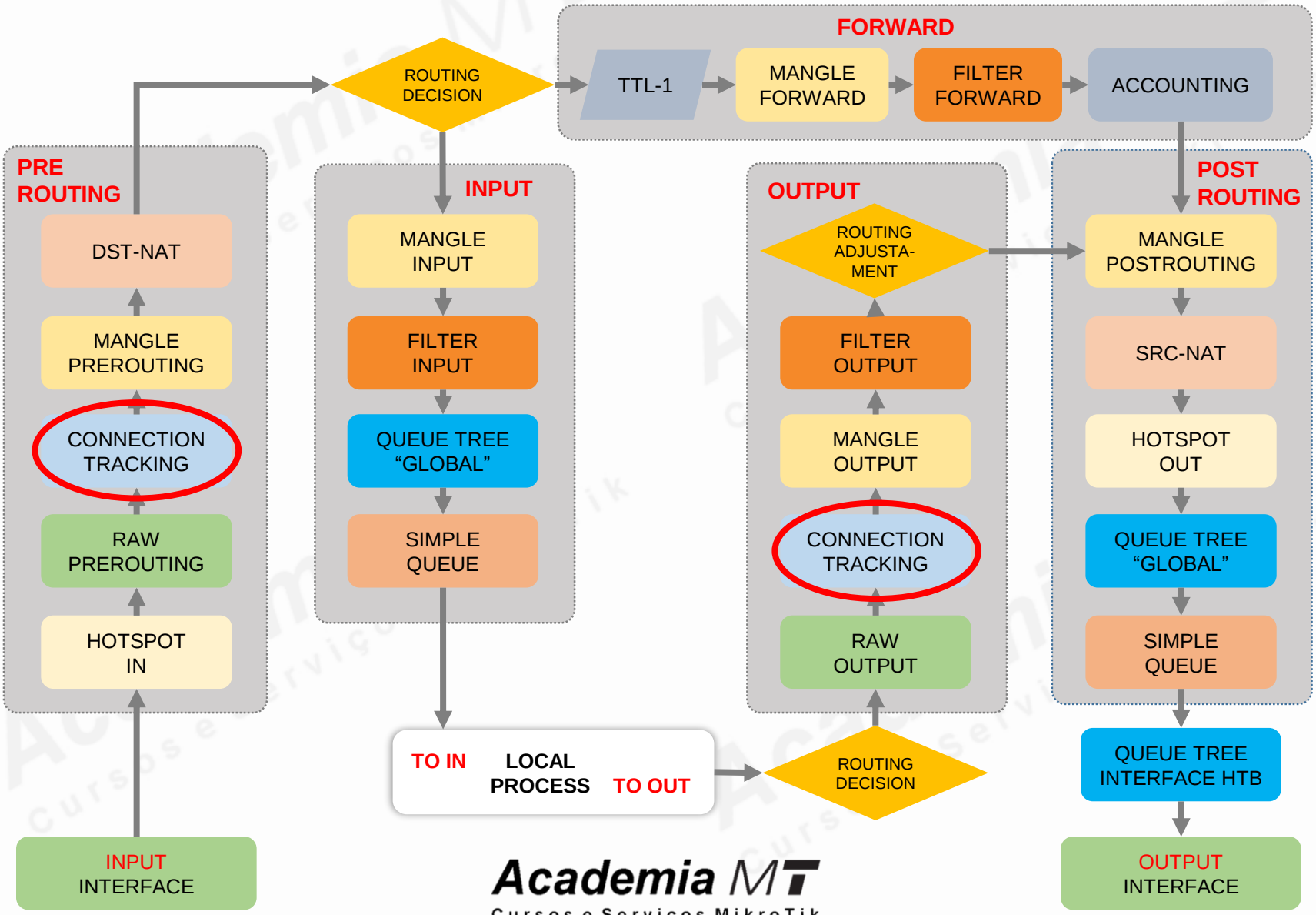
/ip firewall connection



Conexão Estabelecida

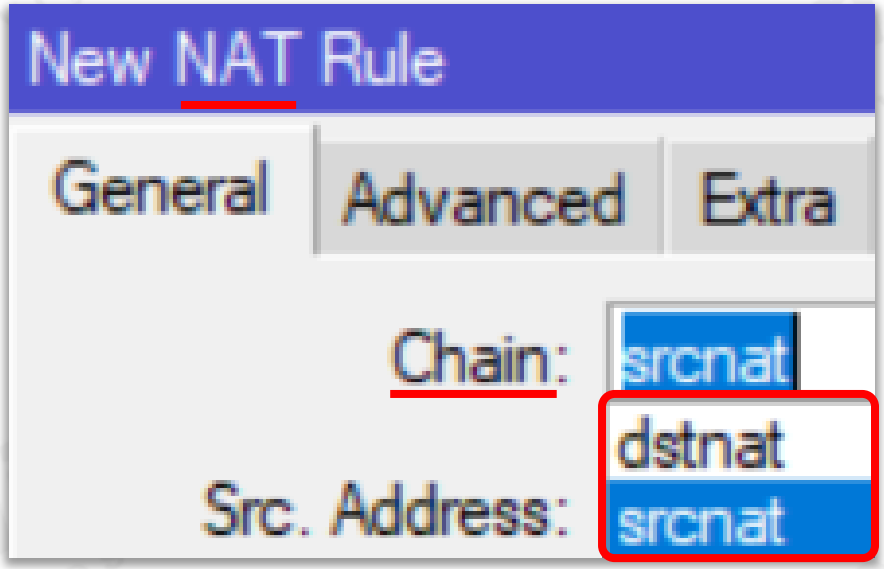


Fluxo de Pacotes Connection Tracking

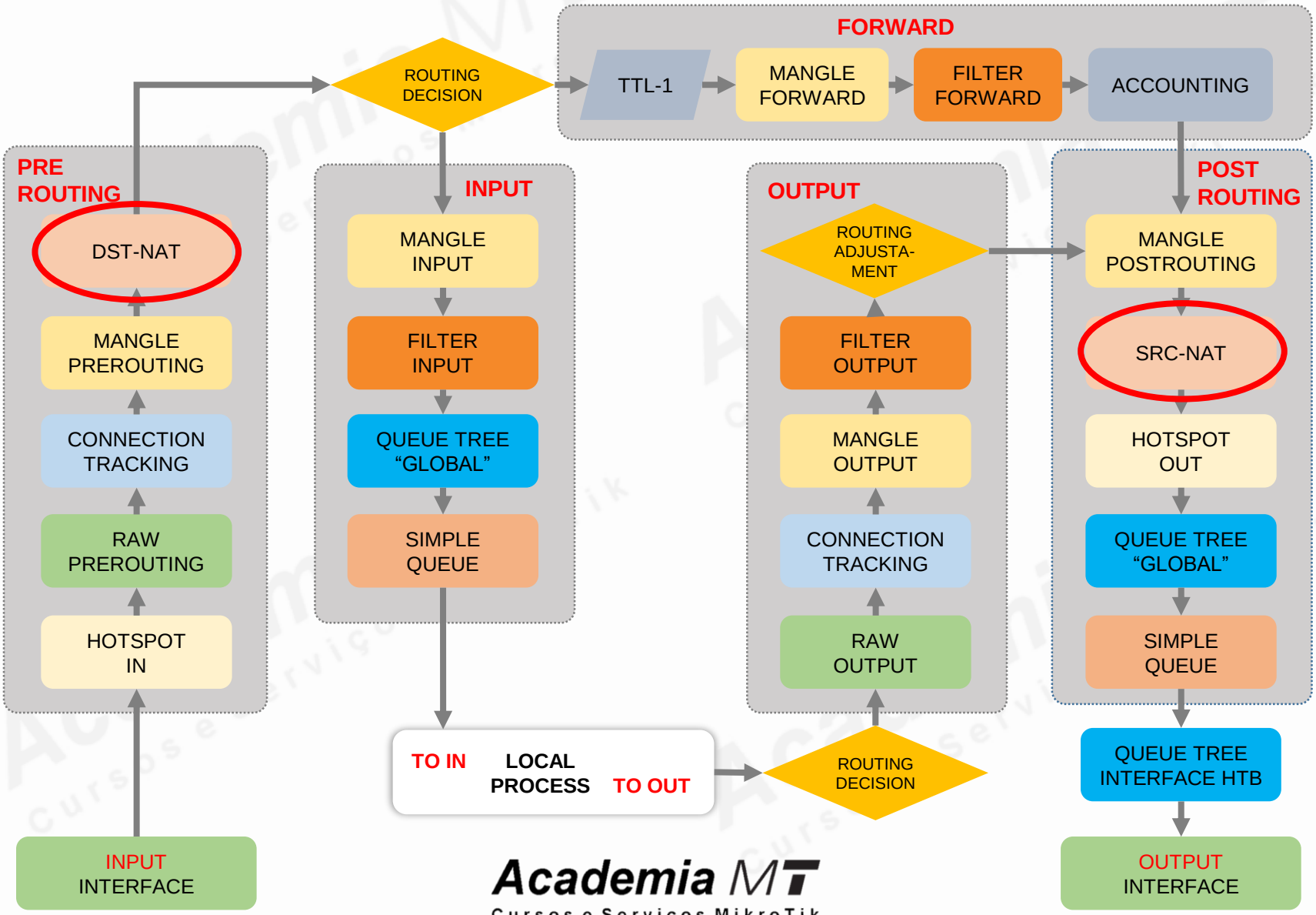


Academia MT
Cursos e Serviços MikroTik

/ip firewall nat add chain=

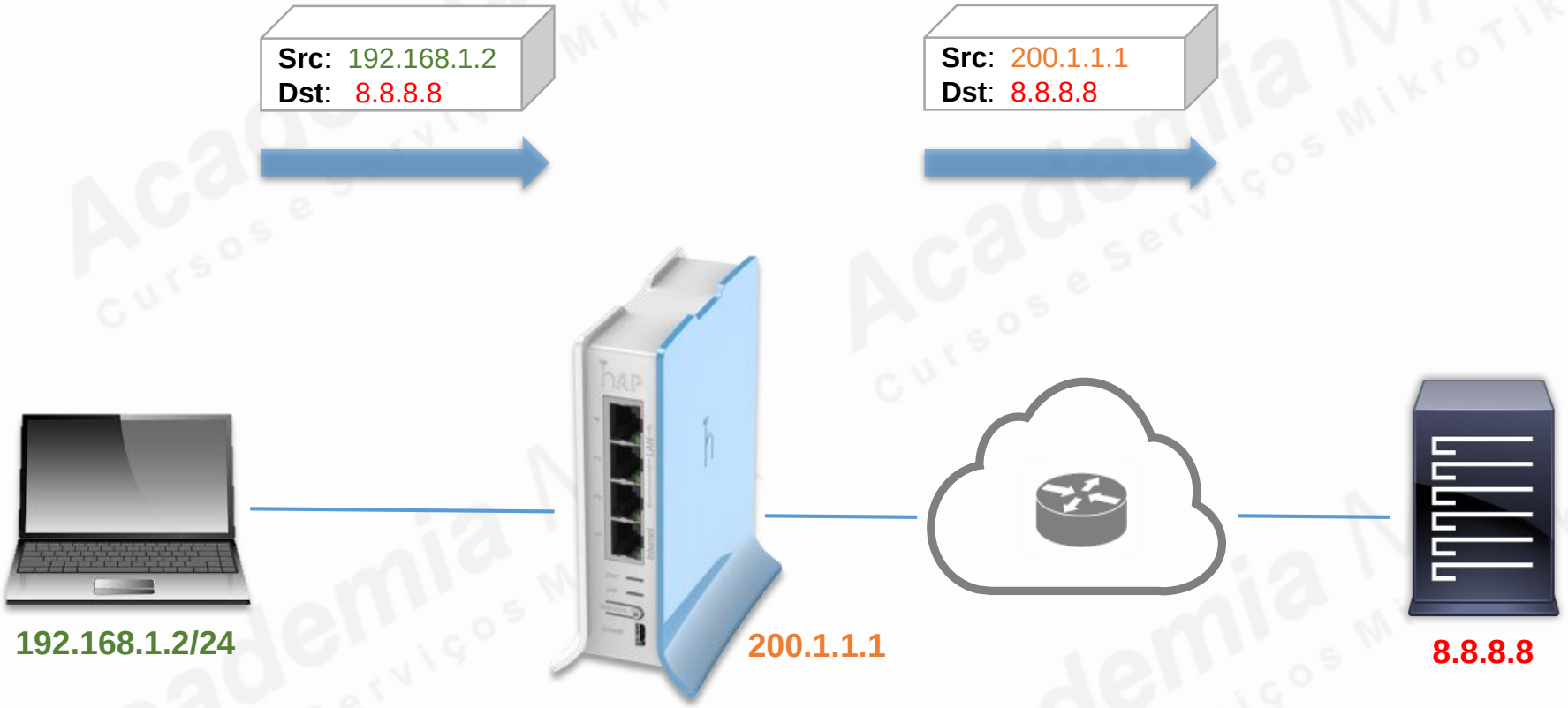


Fluxo de Pacotes src-nat e dst-nat

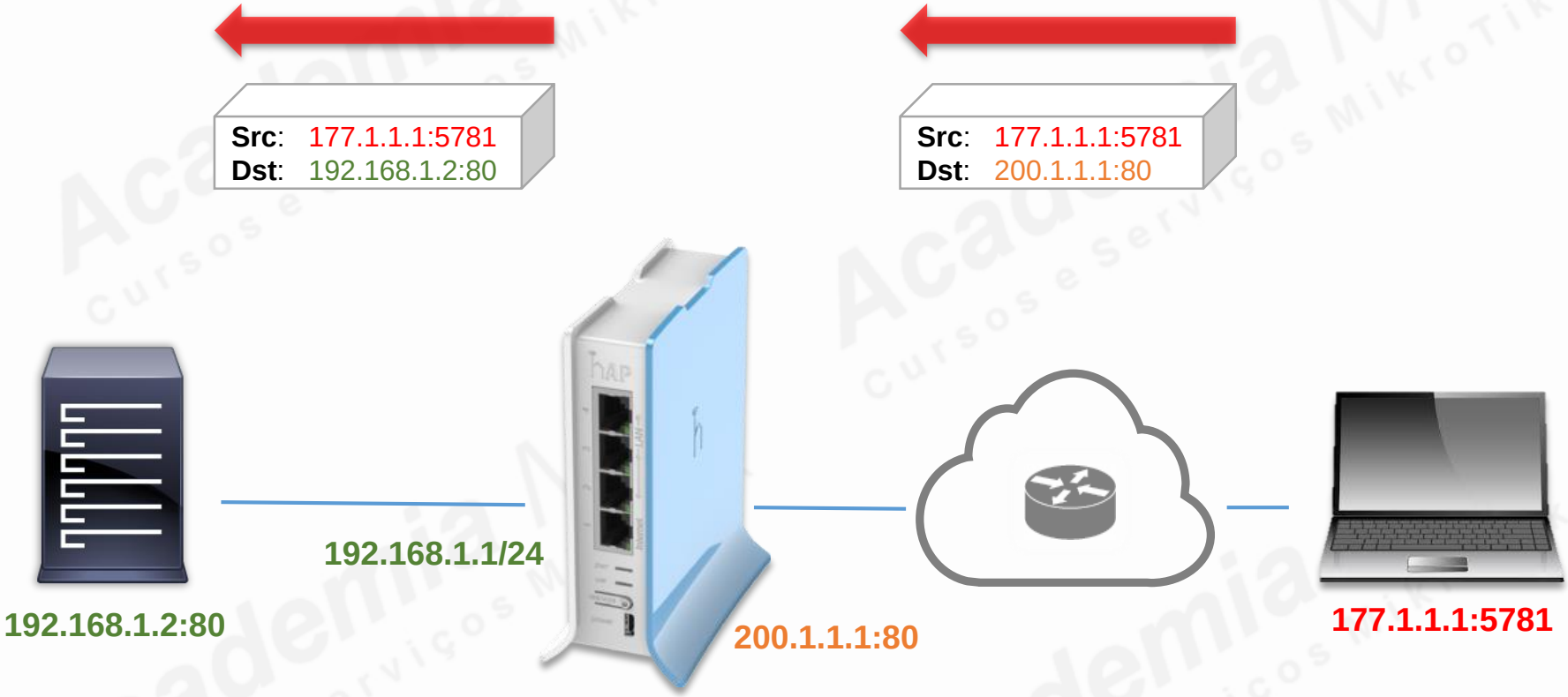


Academia MT
Cursos e Serviços MikroTik

/ip firewall nat add chain=srcnat



/ip firewall nat add chain=dstnat



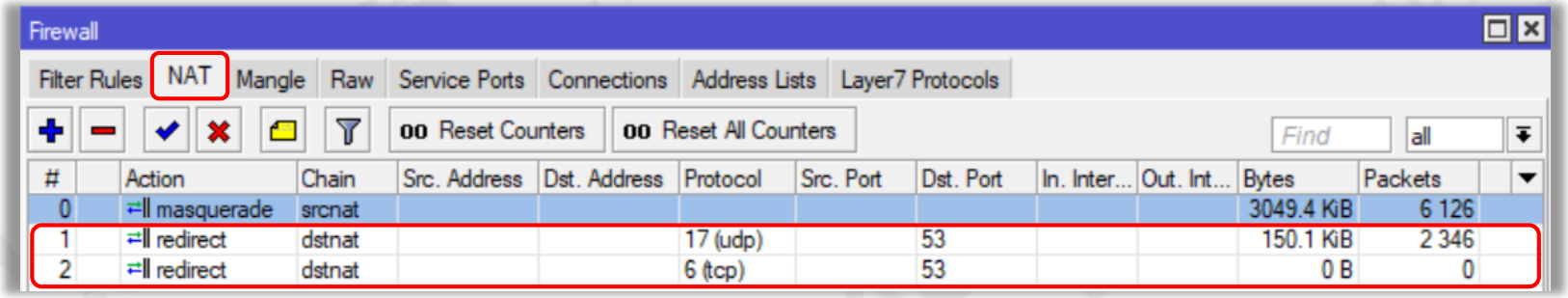
/ip firewall nat add chain=dstnat

DICA

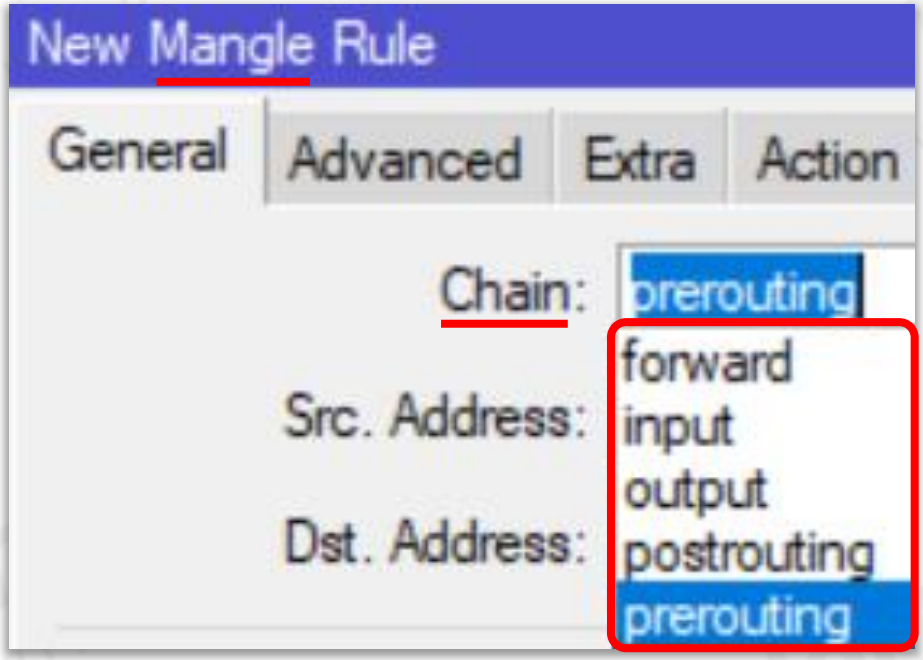
Objetivo

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

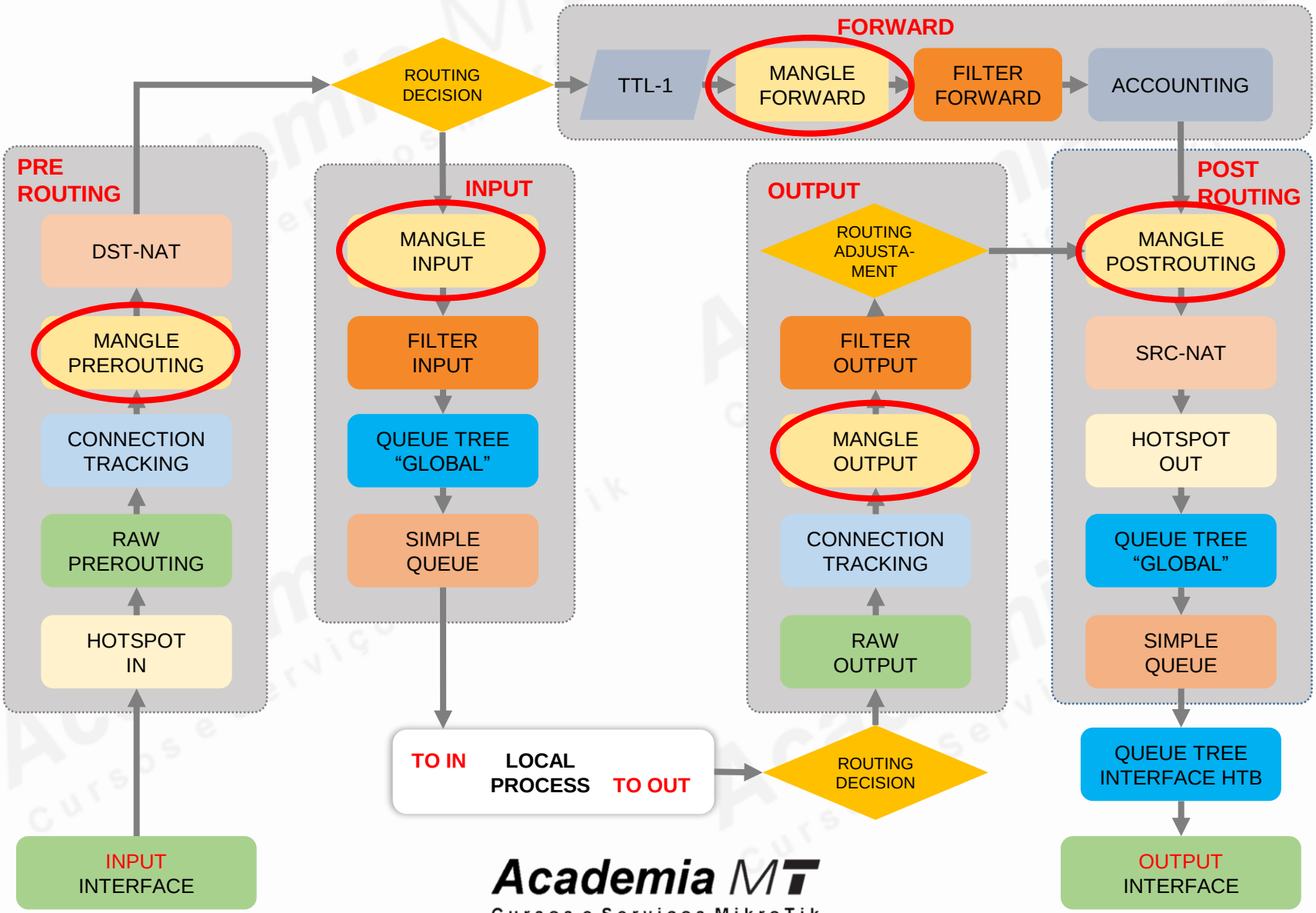
```
/ip firewall nat
add action=redirect chain=dstnat dst-port=53 protocol=udp
add action=redirect chain=dstnat dst-port=53 protocol=tcp
```



/ip firewall mangle add chain=

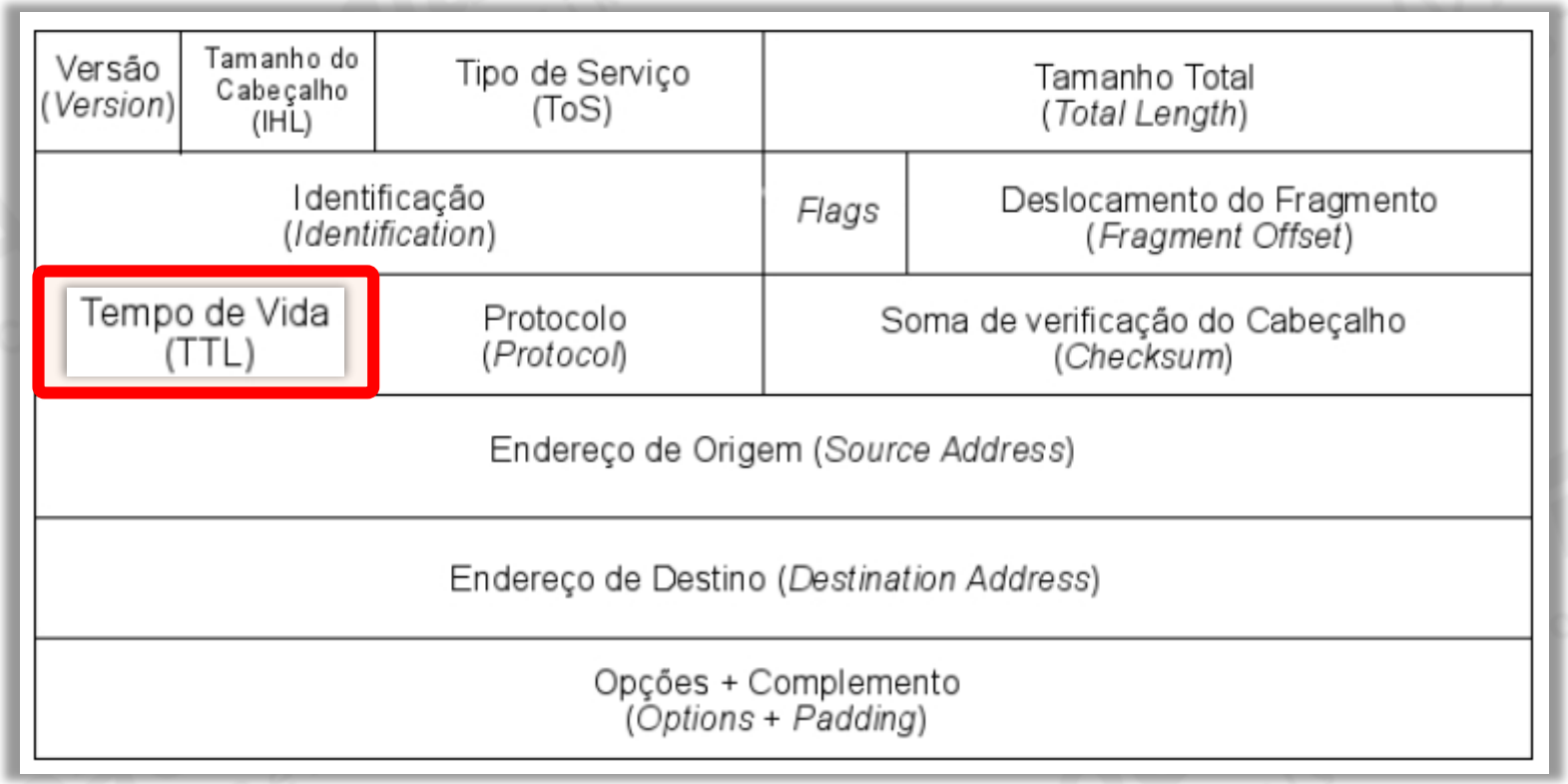


Fluxo de Pacotes Mangle

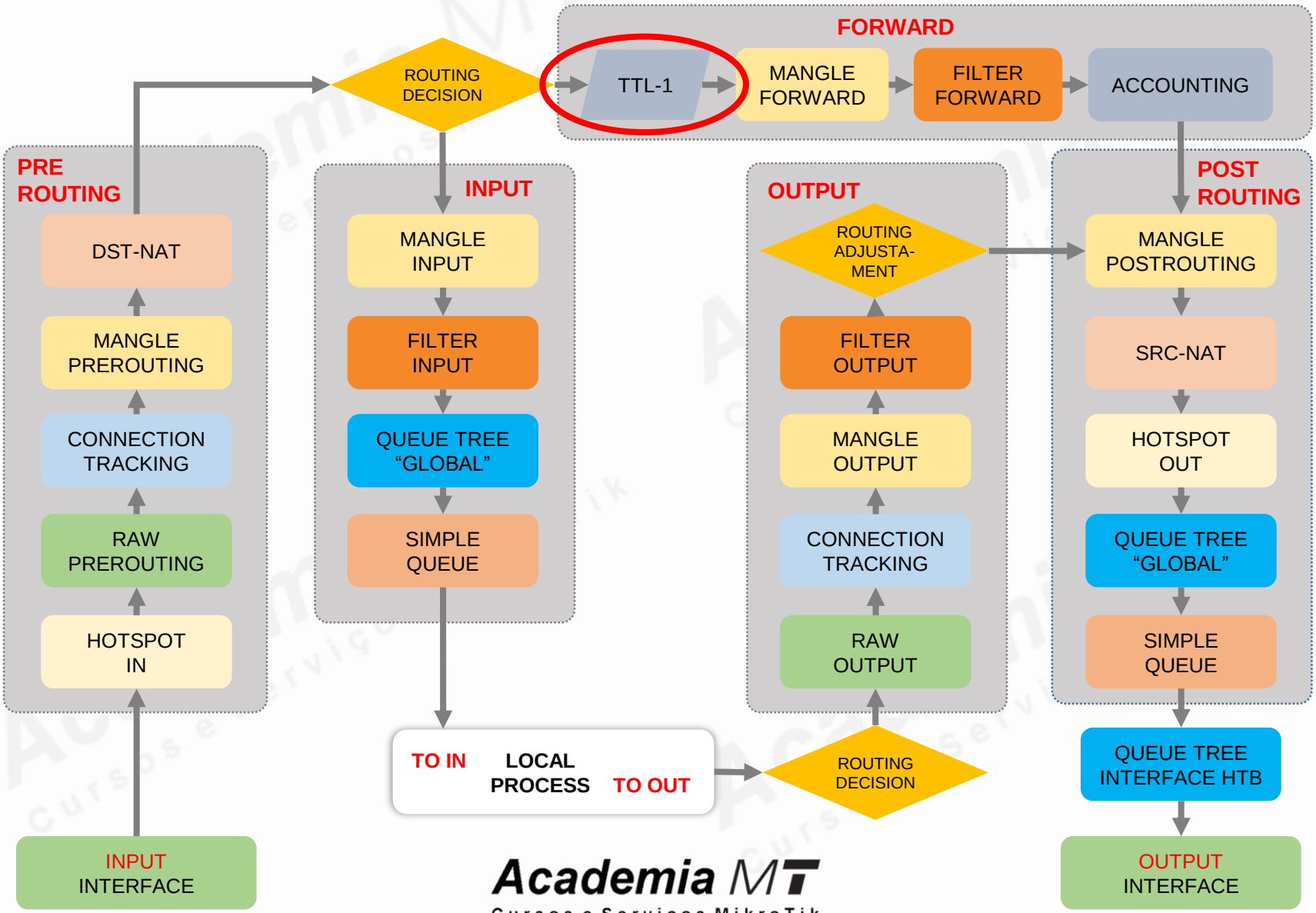


Academia MT
Cursos e Serviços MikroTik

Camada 3, Rede - Cabeçalho IPv4



Fluxo de Pacotes TTL-1



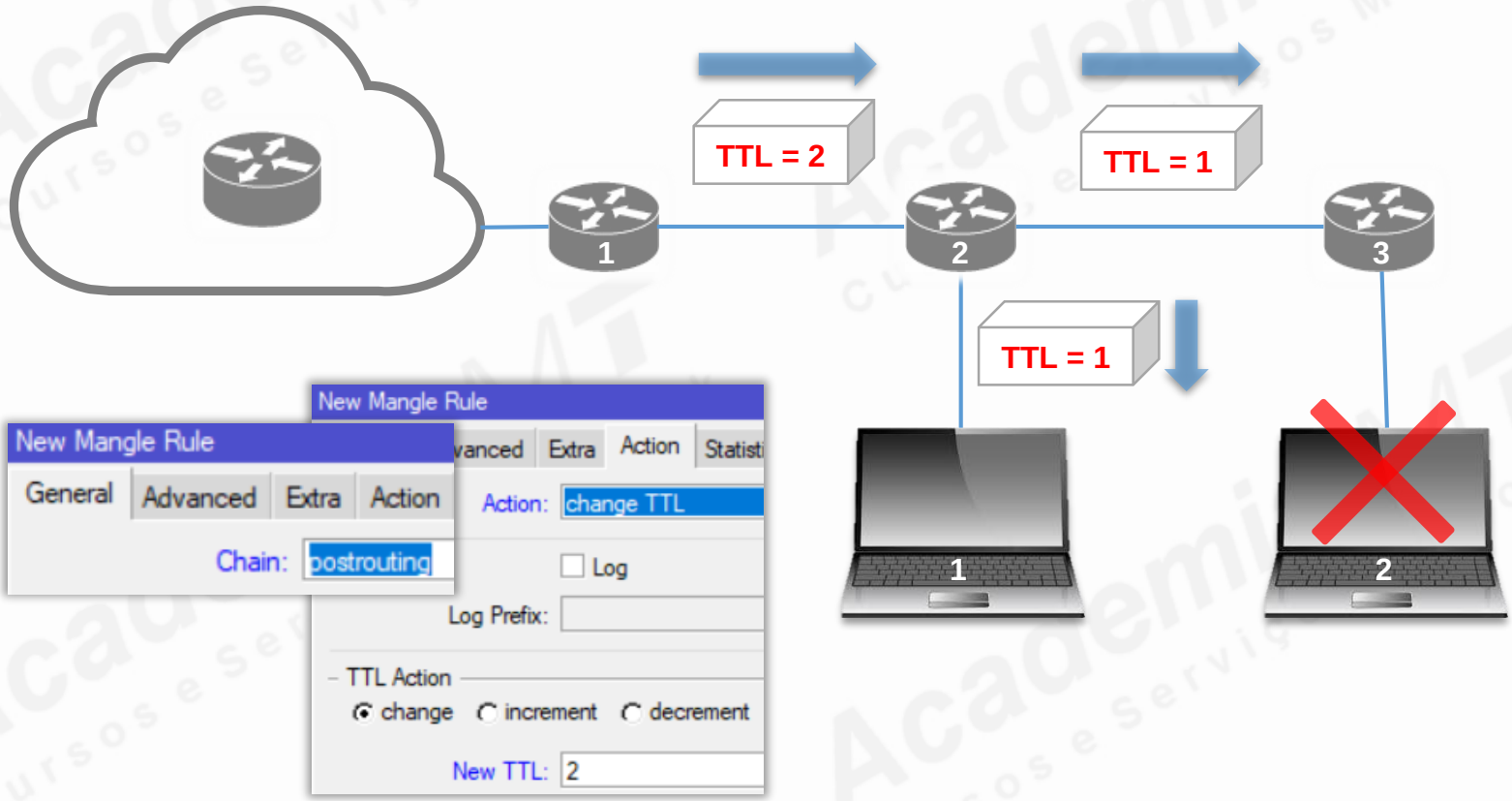
Academia MT
Cursos e Serviços MikroTik

/ip firewall mangle set action=change-ttl

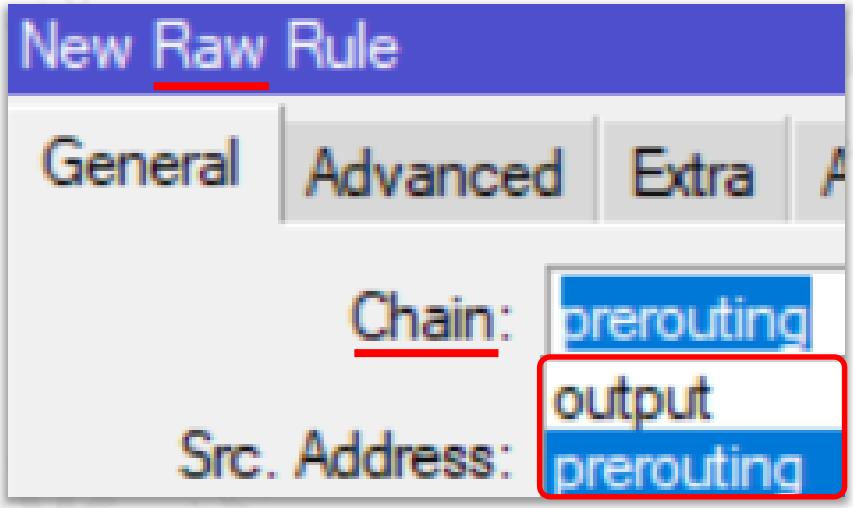
Objetivo

- Não redistribuir Internet ao acrescentar um novo Router

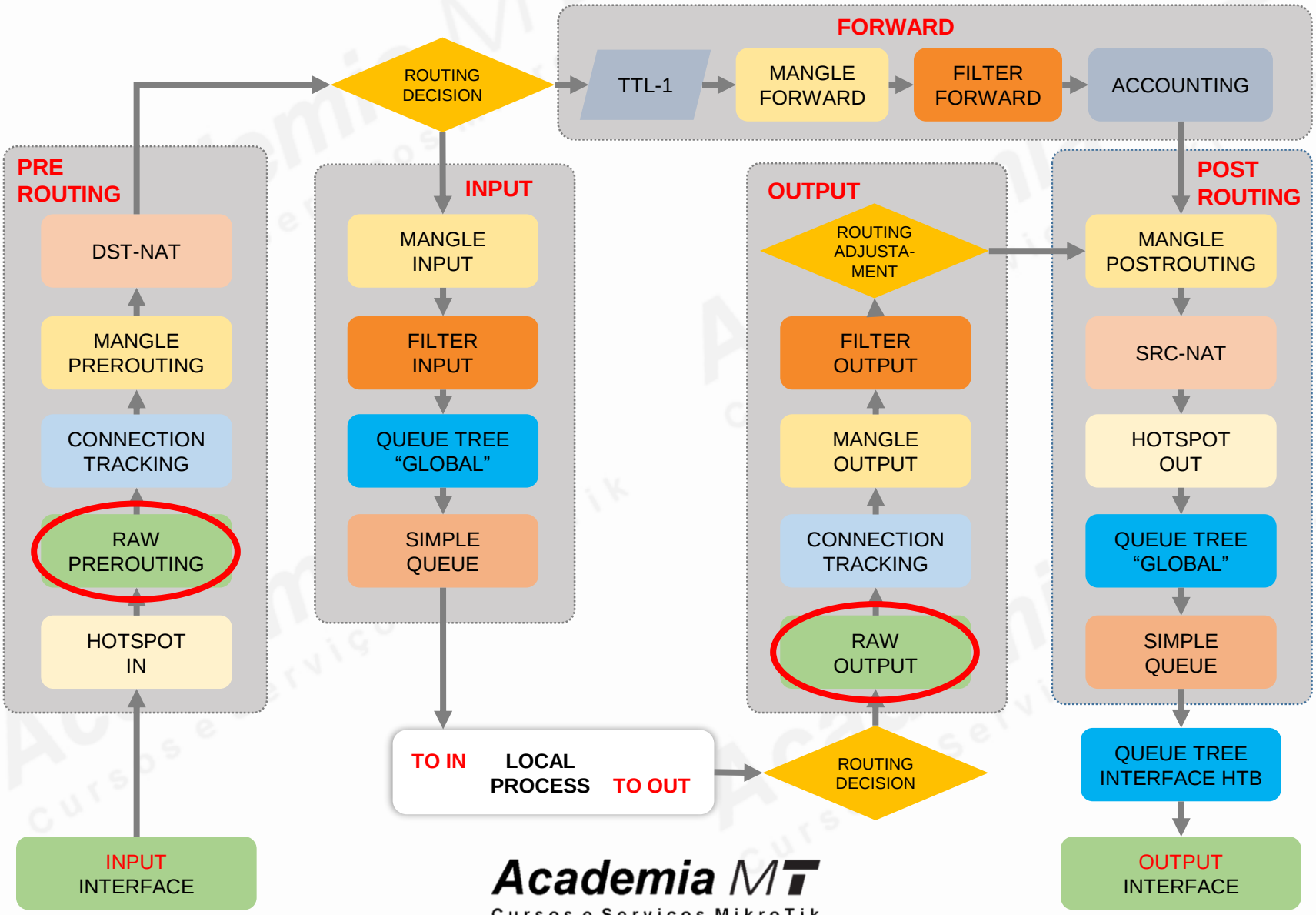
DICA



/ip firewall raw add chain=



Fluxo de Pacotes Raw



Academia MT
Cursos e Serviços MikroTik

/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 servicos 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

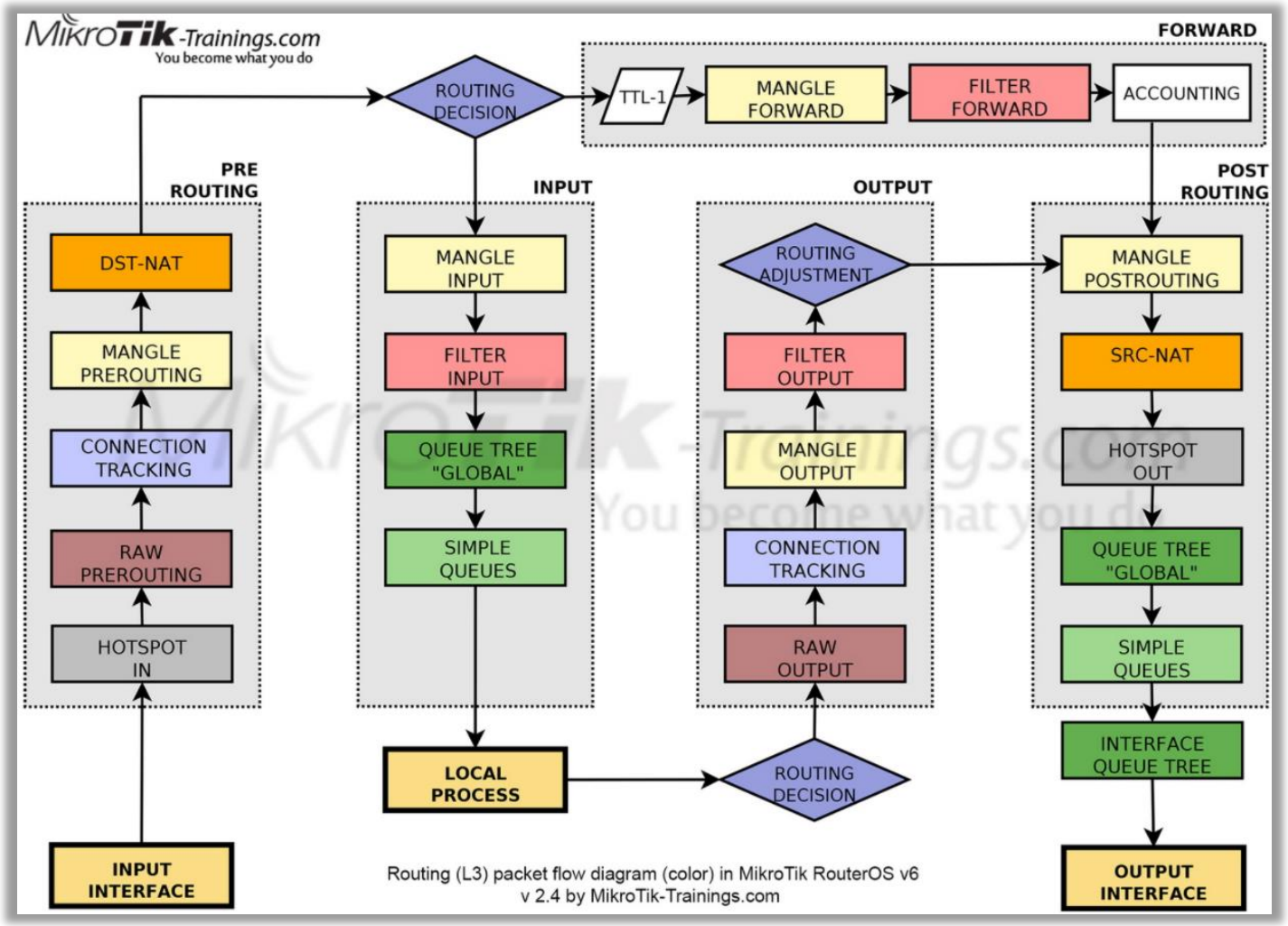
DICA

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

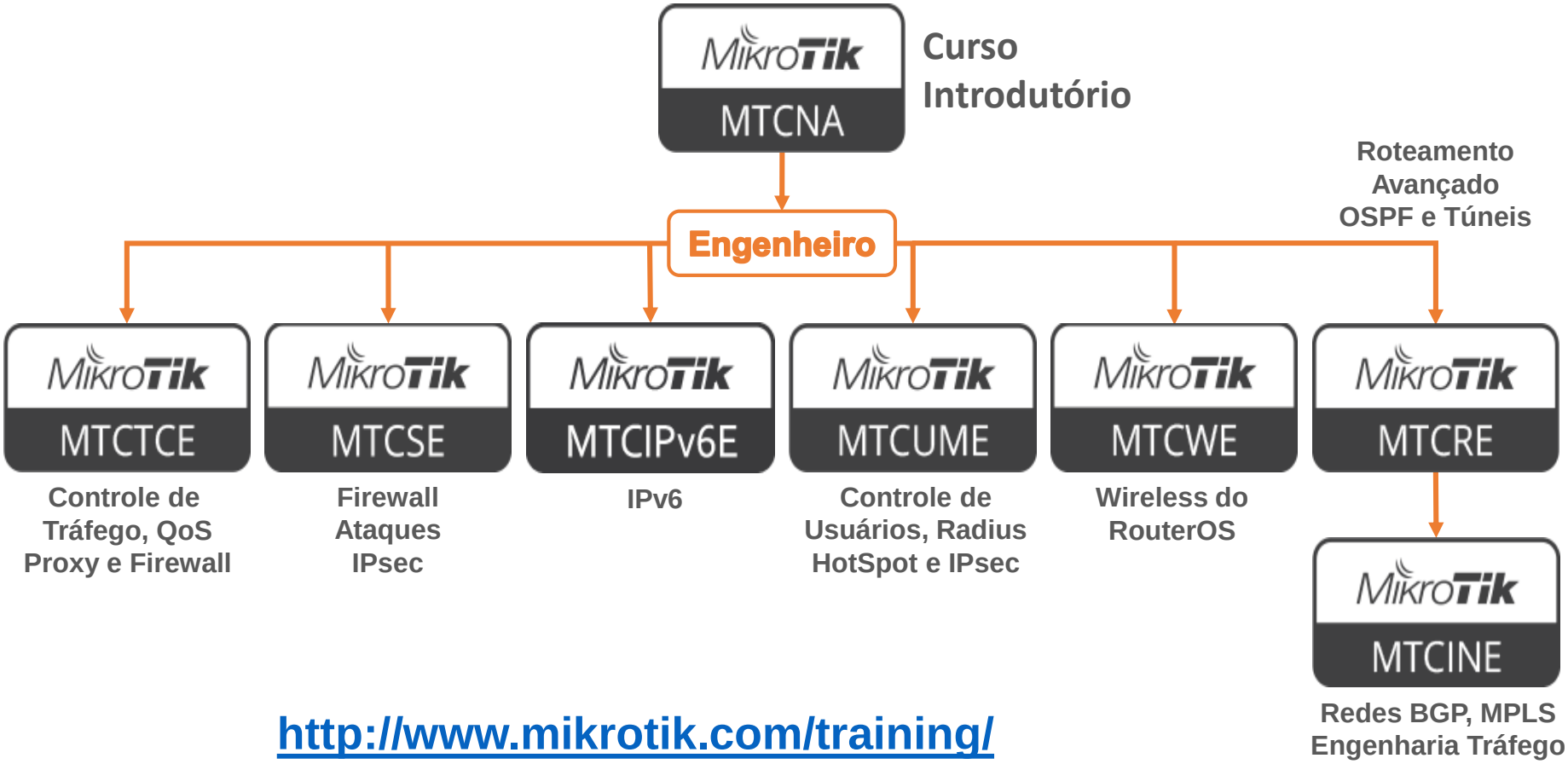
Obrigado!

João **Krieger**

48 9-9982-8707

krieger@academiamt.com.br

Treinamentos MikroTik



http://www.mikrotik.com/training/