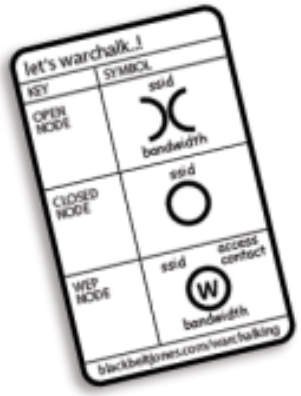
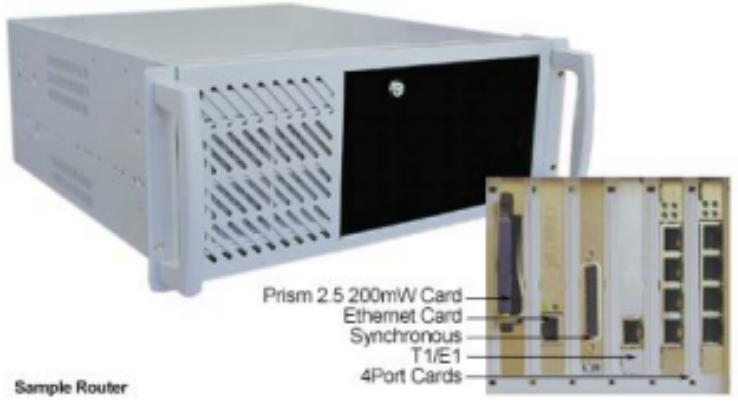


MikrotikBrasil

Consultoria e Treinamentos
Integração de Equipamentos



Sample Router

Um pouco sobre a MD Brasil Telecom (MikrotikBrasil)

- No mercado de Internet discada desde 1995
- Primeiros links Wireless de 2mbps entre 4 cidades do Interior Paulista em 2000
- Ministra treinamentos em Wireless desde 2002
- Presta serviços de consultoria em Wireless para provedores e empresas
- Representante da Mikrotik – Latvia desde 2006 representando os sistemas
- Distribuidor Oficial de Hardware Mikrotik desde janeiro de 2007
- Training Partner Mikrotik desde julho de 2007

Mikrotik RouterOS
uma pequena história de grande sucesso

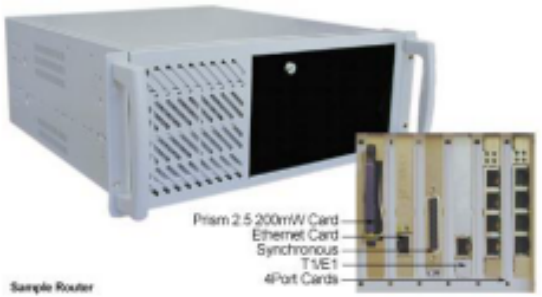
- → 1993: Primeira rede Wavelan em 915MHz em Riga, (Latvia)
- → 1995: Soluções para WISP's em vários países
- → 1996: Publicado na Internet o paper "Wireless Internet Access in Latvia"
- → 1996: Incorporada e Fundada a empresa MikroTikls
- → 2002: Desenvolvimento de Hardware próprio
- → 2007: 60 funcionários

Atualmente:
O RouterOS da Mikrotik tende a ser um padrão de fato para provedores de serviço internet podendo ser inclusive um forte concorrente com gigantes como a Cisco e outros.

O que é o Mikrotik RouterOS ?

Um poderoso sistema operacional “carrier class” que pode ser instalado em um PC comum ou placa SBC (Single Board Computer), podendo desempenhar as funções de:

- → Roteador Dedicado
- → Bridge
- → Firewall
- → Controlador de Banda e QoS
- → Ponto de Acesso Wireless modo 802.11 e proprietário
- → Concentrador PPPoE, PPtP, IPSeC, L2TP, etc
- → Roteador de Borda
- → Servidor Dial-in e Dial-out
- → Hotspot e gerenciador de usuários
- → WEB Proxy
- → Recursos de Bonding, VRRP, etc, etc.



Instalação do Mikrotik

O Mikrotik RouterOS pode ser instalado utilizando:

→ CD Iso bootável (gravado como imagem)
→ Via rede com o utilitário Netinstall

Obtendo o RouterOS

http://www.mikrotik.com/download.html

RouterOS Download

RouterBOARD 100 series
RouterBOARD 200 series
RouterBOARD 300 series
RouterBOARD 500 series
Intel/AMD PC
Other X86 compatible system

Packages for **Intel/AMD PCs**

- Combined RouterOS package
- Separate RouterOS packages *(view content)*
- ISO image
- RouterOS **2.9.48** Changelog

Optional Packages

- User manager package
- Wireless Package with new country settings

v3 Release candidate

- Combined RouterOS package
- Separate RouterOS packages *(view content)*
- ISO image
- RouterOS **3.0rc9** Changelog

Content x

- advanced-tools
- arlan
- calea
- dhcp
- gps
- hotspot
- isdn
- lcd
- ntp
- ppp
- radiolan
- routerboard
- routing
- routing-test
- rstp-bridge-test
- security
- synchronous
- system
- telephony
- thinrouter-pcipc
- ups
- user-manager
- web-proxy
- webproxy-test
- wireless
- wireless-crd
- license.txt

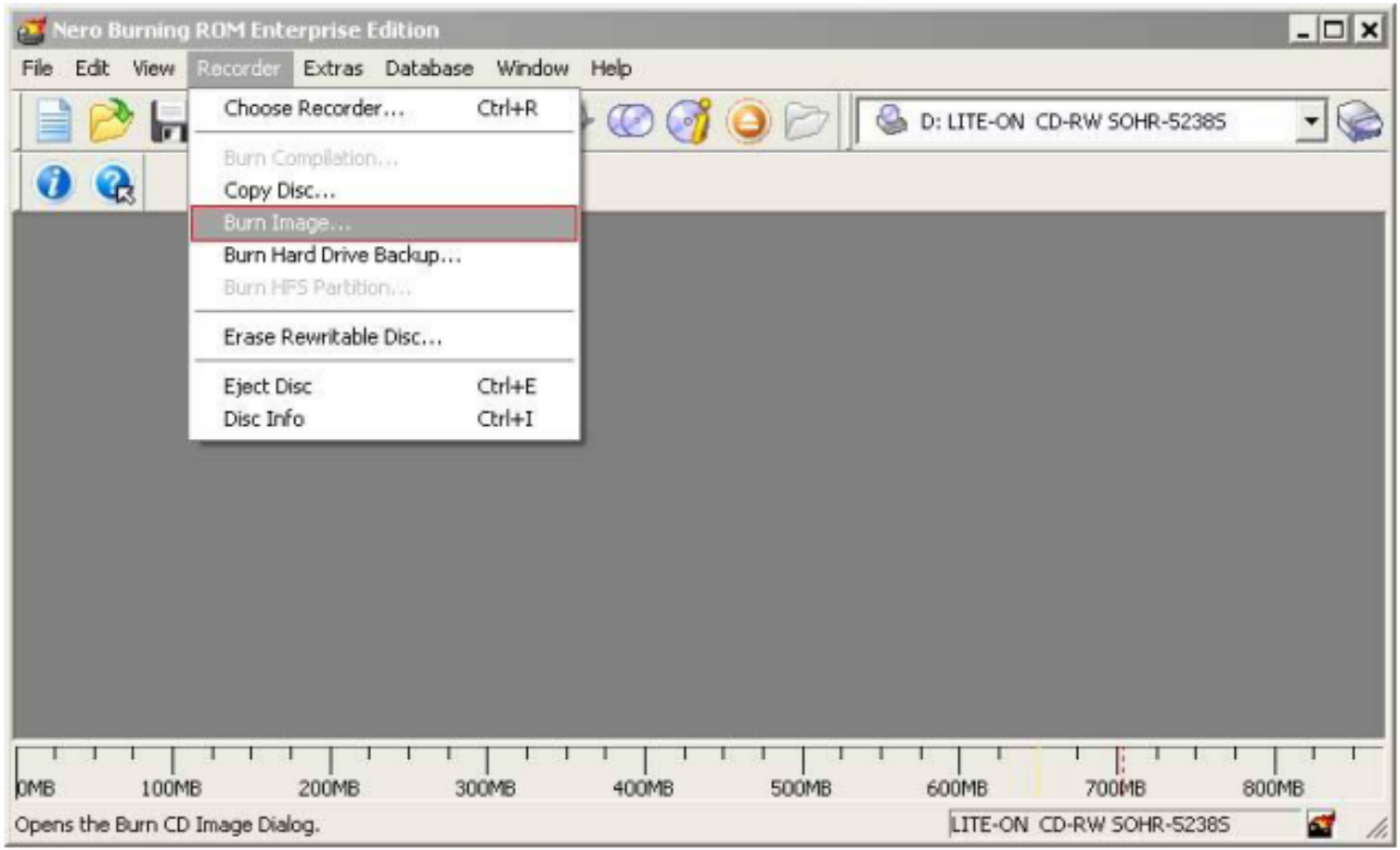
Imagem ISO – para instalação com CD

Changelog – Modificações versões

Instalando por CD

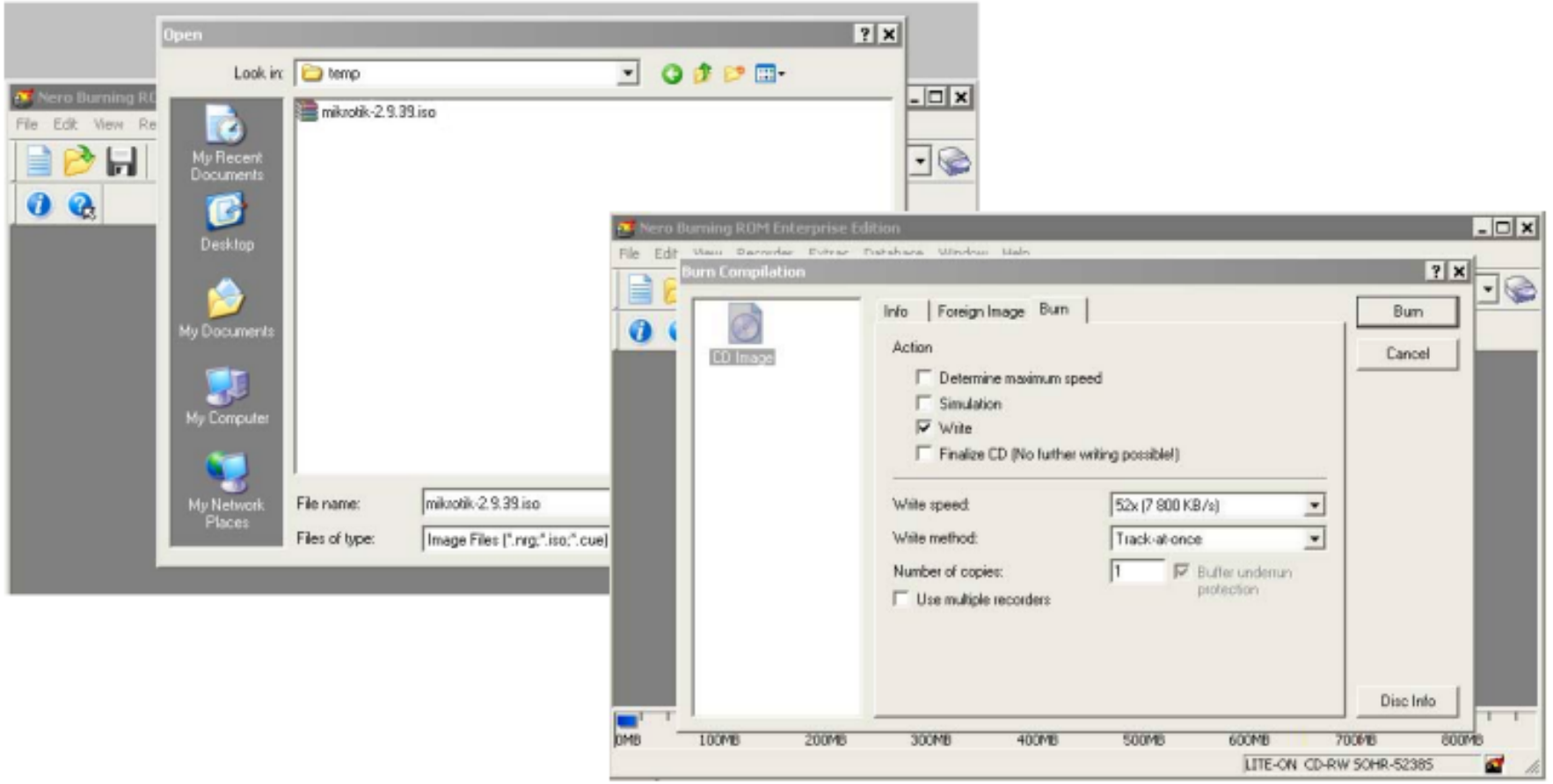
Uma vêz baixado o pacote e descompactado, precisamos gerar o CD de boot

No exemplo abaixo usamos o Nero para gravar o CD



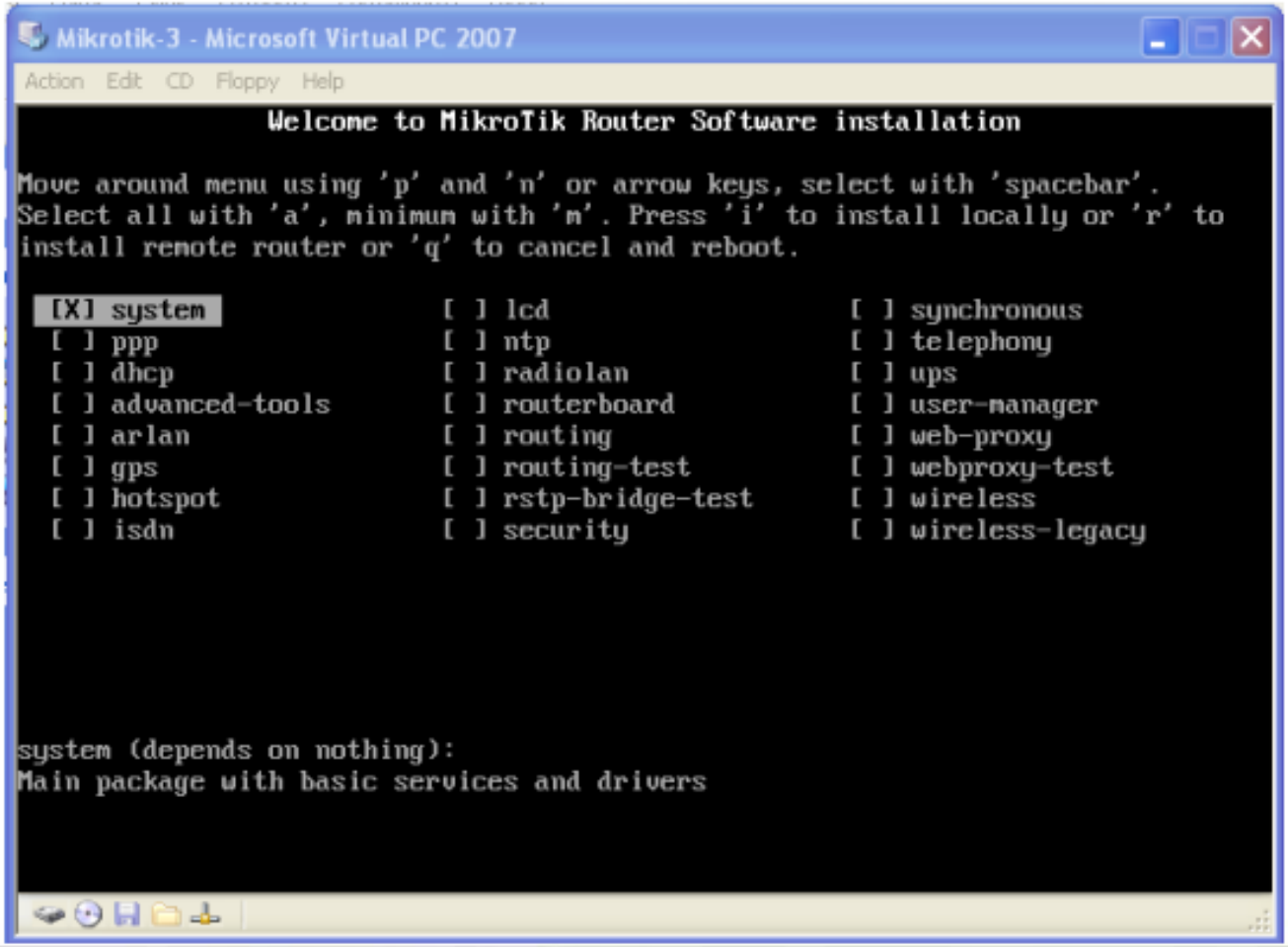
Instalando por CD

Seleciona-se a imagem .iso descompacatada e clica-se em Burn



Instalando por CD

Prepare o PC para bootar pelo CD. Após o boot será apresentada a seguinte tela:



Pacotes do RouterOS - significado

System:	Pacote principal com serviços básicos e drivers. A rigor é o único que necessáramente tem de ser instalado.
ppp:	Suporte aos serviços PPP como PPPoE, L2TP, PPtP, etc
DHCP:	DHCP cliente e DHCP servidor
advanced-tools:	ferramentas de diagnóstico, netwatch e outros utilitários
arlan:	Suporte a um tipo de placa Aironet antiga – arlan
calea:	Pacote para vigilancia de conexões (exigencia legal nos EUA)
gps:	Suporte a GPS (tempo e posição)
hotspot:	Suporte a hotspots
ISDN:	Suporte a conexões ISDN
lcd:	Suporte a display de cristal líquido
ntp:	Servidor e cliente de NTP (relógio)

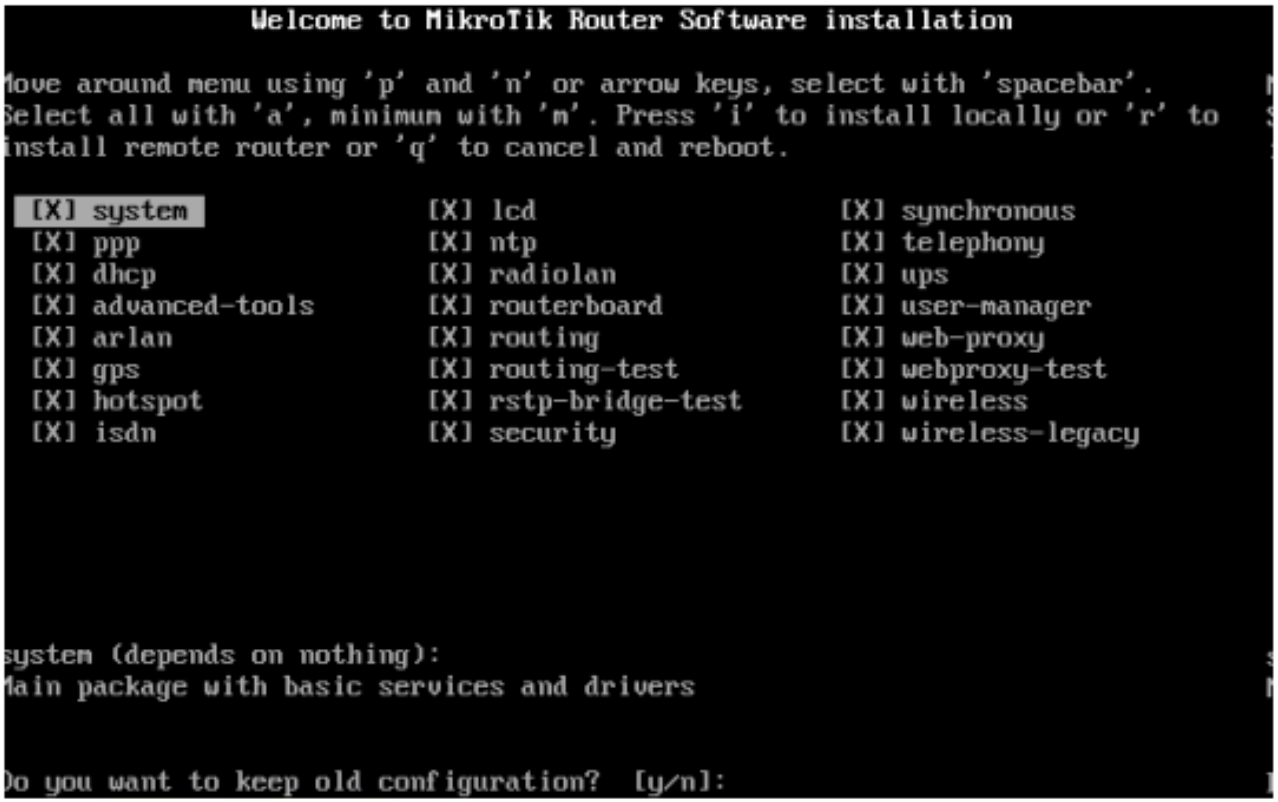
Pacotes do RouterOS - significado

radiolan:	suporte a placa Radiolan
routerboard:	utilitários para routerboard's
routing:	suporte a roteamento dinamico – protocolos RIP, OSPF e BGP
rstp-bridge-test	protocolo rstp
security:	suporte a ssh, Ipsec e conexão segura do winbox
synchronous:	suporte a placas síncronas Moxa, Cyclades PC300 e outras
telephony:	pacote de suporte a telefonia – protocolo h.323 ☹
ups:	suporte a no-breaks APC
user-manager:	serviço de autenticação user-manager
web-proxy:	Serviço de Web-Proxy
wireless:	Suporte a placas PrismII e Atheros
wireless-legacy:	Suporte a placas PrismII, Atheros e Aironet com algumas features inabilitadas

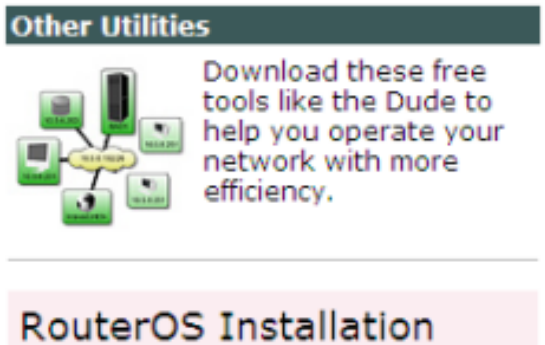
Instalando por CD

Pode-se seleccionar os pacotes desejados pressionando-se a barra de espaços ou “a” para todos. Em seguida “i” irá instalar os pacotes selecionados.

Caso haja configurações pode-se mante-las selecionando-se “y”



Instalação com Netinstall



O Netinstall tranforma uma estação de trabalho Windows em um instalador.

→ Obtem-se o programa no link www.mikrotik.com/download.html

→ Pode-se instalar em um um PC que boota via rede (configurar na BIOS)

→Pode-se instalar em uma Routerboard, configurando-a para bootar via rede

→ O Netinstall é interessante principalmente para reinstalar em routerboards quando necessário por danos a instalação inicial e quando se perde a senha do equipamento.

Instalação com Netinstall

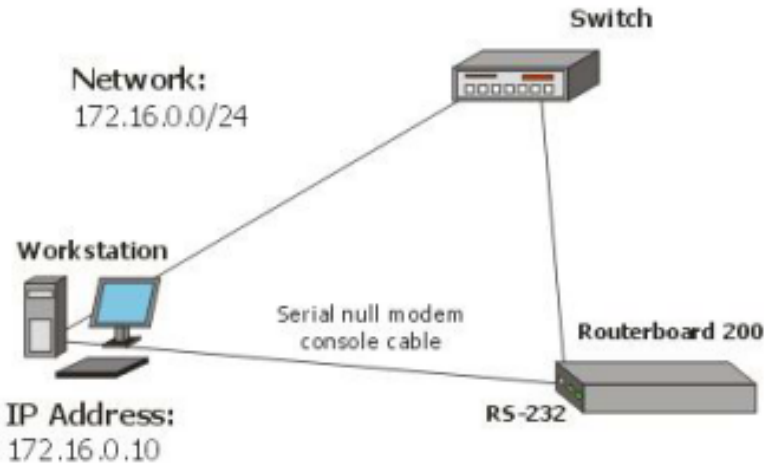
Para se instalar em uma Routerboard, inicialmente temos que entrar via serial, com um cabo null modem e os parametros:

→velocidade: 115.200 bps

→bits de dados: 8

→bits de parada: 1

→Controle de fluxo: hardware



Entra-se na Routerboard e seleciona-se

o - boot device

e depois:

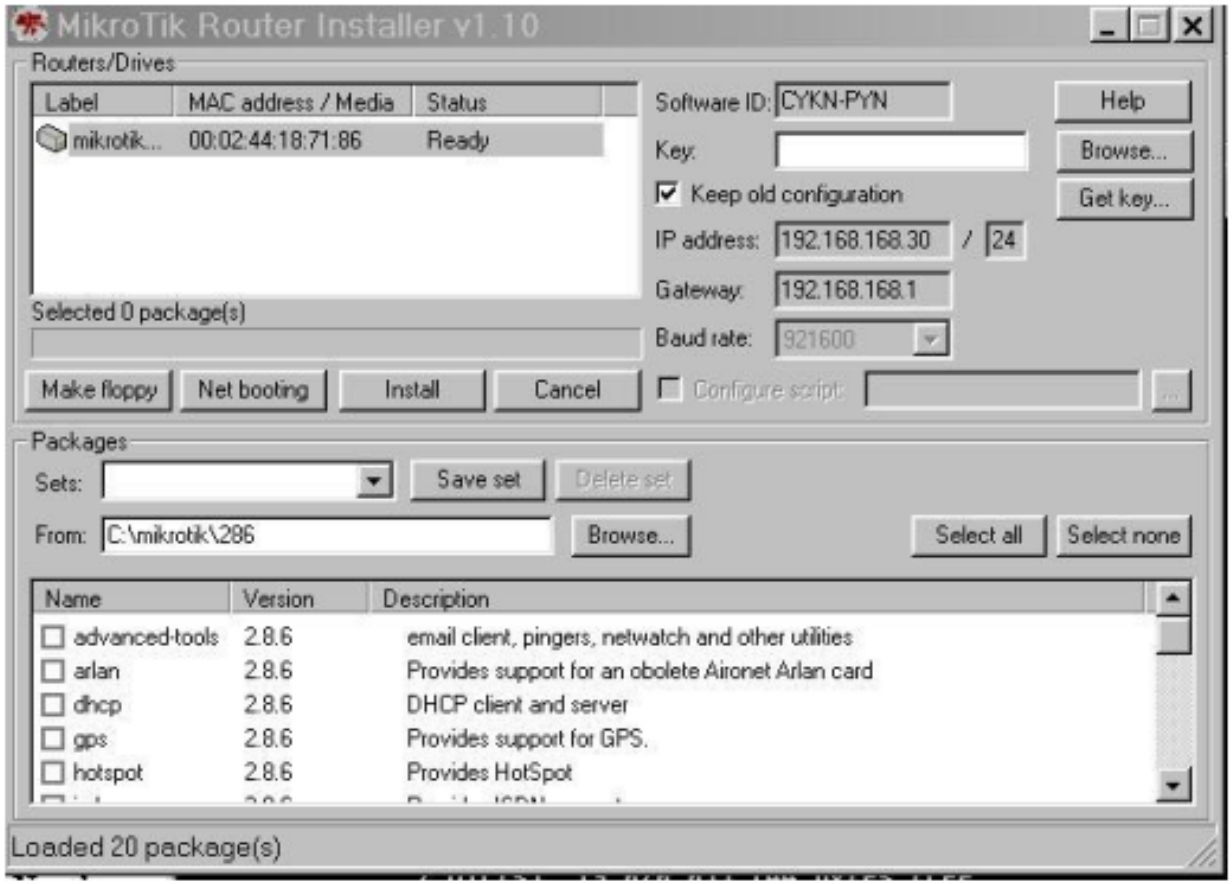
e - Etherboot

Instalação com Netinstall

→ Atribuir um IP para o Net Booting na mesma faixa da placa de rede da máquina.

→Colocar os pacotes a serem instalados na máquina.

→Bootar e selecionar os pacotes a serem instalados.



Acesso ao Mikrotik

O processo de instalação não configura um IP no Mikrotik e o primeiro acesso pode ser feito das seguintes maneiras:

→ Direto na console (no caso de PC's)

→ Via Terminal (115200/8/N/1 para routerboards e 9600/8/N/1 para PC's)

→ Via Telnet de MAC, através de outro Mikrotik ou de sistema que suporte telnet por MAC e que esteja no mesmo barramento físico de rede.

→ Via Winbox

Console do Mikrotik

Na console do Mikrotik tem-se acesso a todas as configurações por um sistema de diretórios hierárquicos pelos quais se pode navegar digitando o caminho.

Exemplo:
[admin@MikroTik] > ip
[admin@MikroTik] ip> address

Pode-se voltar um nível de diretório digitando-se ..
[admin@MikroTik] ip address> ..
[admin@MikroTik] ip>

Pode-se ir direto ao diretório raiz, digitando-se /
[admin@MikroTik] ip address> /
[admin@MikroTik] >

Console do Mikrotik

Ajuda

→ ? Mostra um help para o diretório em que se esteja – [Mikrotik] > ?

→ ? Após um comando incompleto mostra as opções disponíveis para esse comando - [Mikrotik] > interface ?

Tecla TAB

→ Comandos não precisam ser totalmente digitados, podendo ser completados com a tecla TAB

→ Havendo mais de uma opção para o já digitado, pressionar TAB 2 vezes mostra todas as opções disponíveis.

Console do Mikrotik

Print: mostra informações de configuração

```
[admin@MikroTik] interface ethernet> print
Flags: X - disabled, R - running
 #    NAME                        MTU   MAC-ADDRESS       ARP
 0  R ether1                      1500  00:03:FF:9F:5F:FD enabled
```

Pode ser usado com diversos argumentos como print status, print detail e print interval. Exemplo:

```
[admin@MikroTik] interface ethernet> print detail
Flags: X - disabled, R - running
 0  R name="ether1" mtu=1500 mac-address=00:03:FF:9F:5F:FD arp=enabled
disable-running-check=yes auto-negotiation=yes full-duplex=yes cable-
settings=default speed=100Mbps
```

Console do Mikrotik

Comando Monitor

→Mostra continuamente várias informações de interfaces

```
[admin@Escritorio] > interface ethernet monitor ether1
status: link-ok
auto-negotiation: done
rate: 100Mbps
full-duplex: yes
default-cable-setting: standard
```

Console do Mikrotik

Comandos para manipular regras

→ add, set, remove → adiciona, muda ou remove regras

→ disabled → desabilita a regra sem deletar

→ move → move algumas regras cuja ordem influencie(firewall por exemplo)

Comando export

→ exporta todas as configurações do diretório corrente acima (se estiver em /, do roteador todo)

→ pode ser copiado com o botão direito do mouse e colado em editor de textos

→ pode ser exportado para um arquivo com export file=nome do arquivo

Comando import

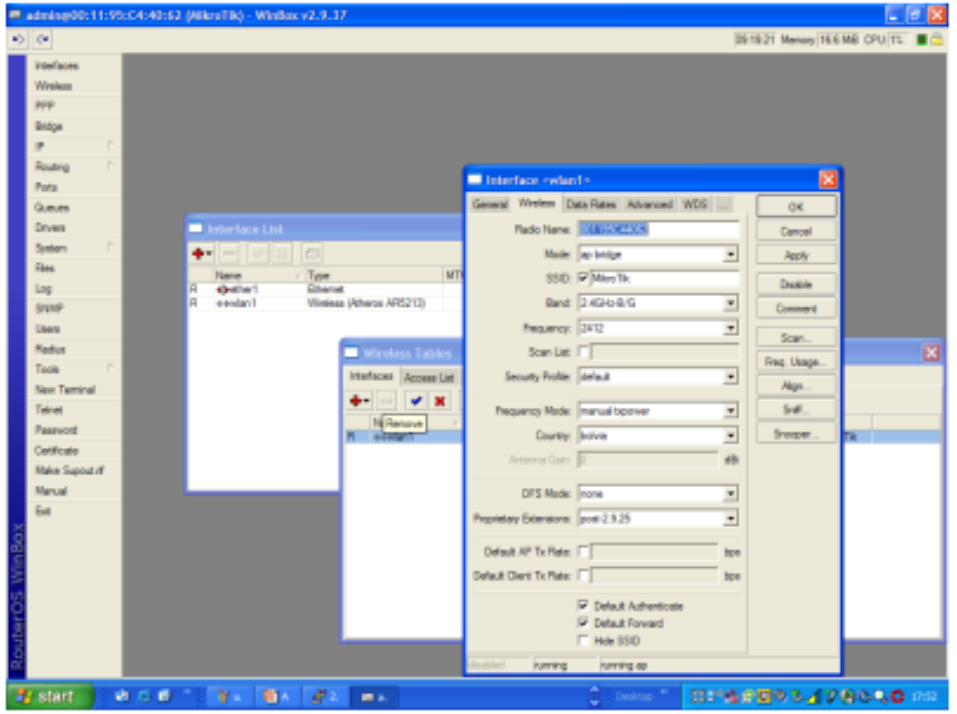
→ importa um arquivo de configurações criado pelo comando export.

Winbox

Obtem-se o Winbox na URL abaixo

ou direto em um mikrotik

www.mikrotik.com/download.html



Tools / Utilities

- Winbox configuration tool
- The Dude network monitor
- Trafr sniffer reader for linux
- Bandwidth test tool for Windows
- Neighbor viewer for Windows
- Other tools in the Archive

Interface Gráfica para administração do Mikrotik

→ Funciona em Windows e Linux (Wine)

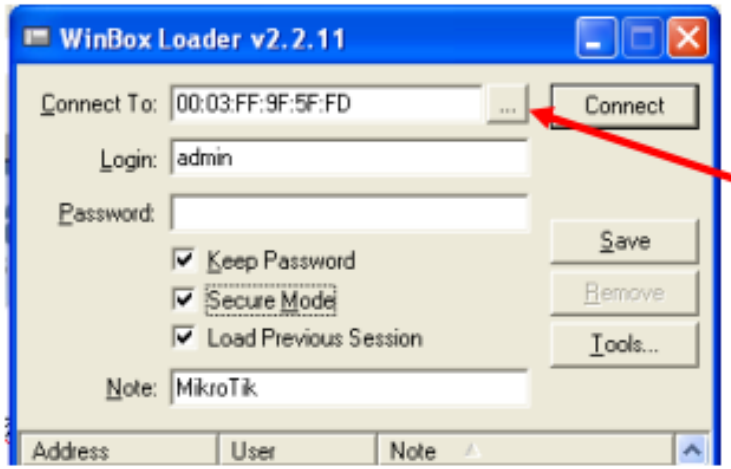
→ Utiliza porta TCP 8291

→ Se escolhido Secure mode a comunicação é criptografada

→ Quase todas as funcionalidades do terminal podem ser configuradas via WINBOX

Winbox

Com o Winbox é possível acessar um Mikrotik sem IP, através do seu MAC. Para tanto popnha os dois no mesmo barramento de rede e clique nas reticências



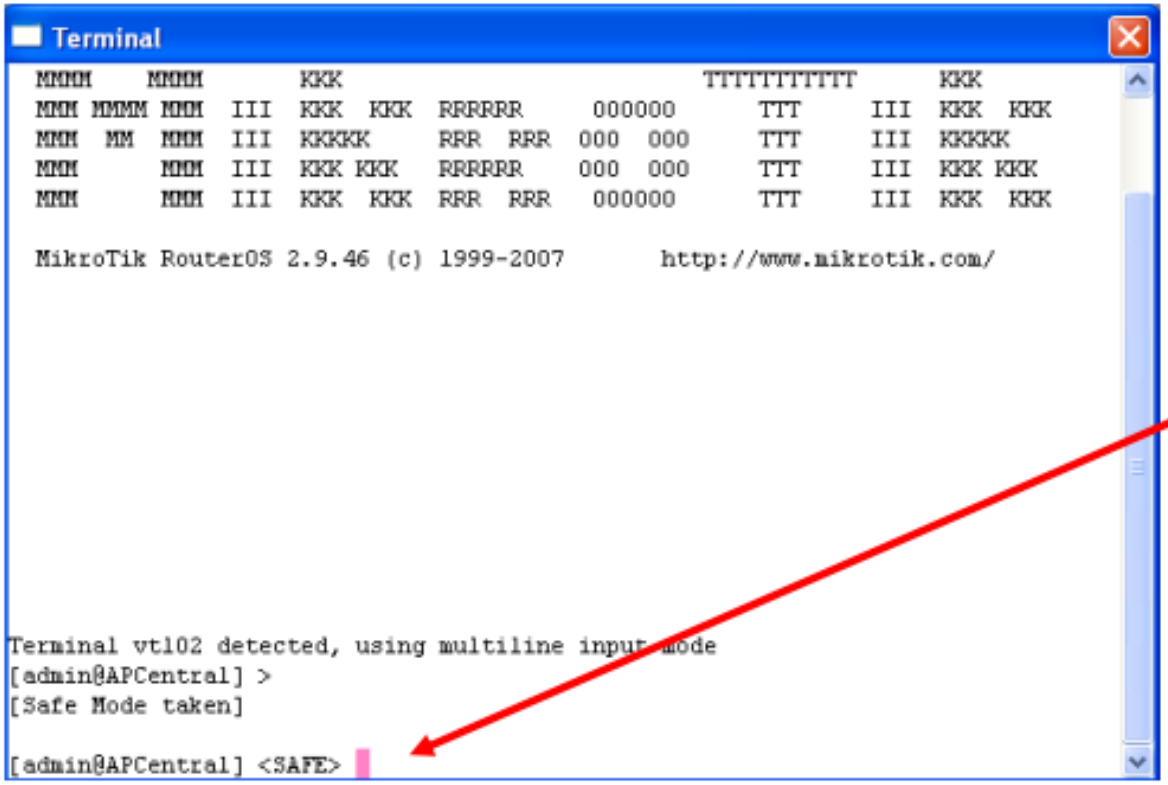
Clique para encontrar o Mikrotik

O acesso pelo MAC pode ser feito para fazer as configurações iniciais, como dar um endereço IP para o Mikrotik.

Após ter configurado um IP e uma máscara de rede. aconselha-se preferencialmente o acesso via IP que é mais estável.

Configuração no modo seguro

Pressionando-se control+X em um terminal pode-se operar o Mikrotik com a possibilidade de desfazer as configuracoes sem que elas sejam aplicadas.



Operando no modo seguro

Configuração no modo seguro

→ Se outro usuário entra no modo seguro, quando já há um nesse modo, lhe será dada a seguinte mensagem:

[admin@MKBR100] >

Hijacking Safe Mode from someone – unroll / release / don't take it [u/r/d]

u → desfaz todas as configurações anteriores feitas no modo seguro e põe a presente sessão em modo seguro

d → deixa tudo como está

r → mantém as configurações realizadas no modo seguro e põe a sessão em modo seguro. O outro usuário recebe a mensagem:

[admin@MKBR100]

Safe mode released by another user

Configuração no modo seguro

→ Todas as configurações são desfeitas caso o modo seguro seja terminado de forma anormal.

→ Control+X novamente ativa as configurações

→ Control+D desfaz todas as configurações realizadas no modo seguro.

→ Configurações realizadas no modo seguro são marcadas com uma Flag “F”, até que sejam aplicadas.

→ O histórico das alterações pode ser visto (não só no modo seguro) em /system history print

➔ Importante: O número de registros de histórico é limitado a 100. As modificações feitas no modo seguro que extrapolem esse limite não são desfeitas nem por Control+D nem pelo término anormal do modo seguro.

Manutenção do Mikrotik

- →Atualização
- →Backups
- →Acréscimo de funcionalidades
- →Detalhes do licenciamento

[MikrotikBrasil]
Routers & Wireless Systems

RouterOS Download

RouterBOARD 100 series
RouterBOARD 200 series
RouterBOARD 300 series
RouterBOARD 500 series
Intel/AMD PC
Other X86 compatible system

Packages for **Intel/AMD PCs**

- Combined RouterOS package
- Separate RouterOS packages *(view content)*
- ISO image
- RouterOS **2.9.48** Changelog

Optional Packages

- User manager package
- Wireless Package with new country settings

v3 Release candidate

- Combined RouterOS package
- Separate RouterOS packages *(view content)*
- ISO image
- RouterOS **3.0rc9** Changelog

Manutenção do Mikrotik
Atualizações

→ As atualizações podem ser feitas com o conjunto de pacotes combinados ou com os pacotes separados disponíveis no site da Mikrotik.

→ Os arquivos tem a extensão .npk e basta coloca-los no diretório raiz do Mikrotik e boota-lo para subir a nova versão.

→ O upload pode ser feito por FTP ou copiando e colando no WInbox.

[MikrotikBrasil]
Routers & Wireless Systems

Manutenção do Mikrotik
acréscimo de novas funcionalidades

RouterOS Download

RouterBOARD 100 series
RouterBOARD 200 series
RouterBOARD 300 series
RouterBOARD 500 series
Intel/AMD PC
Other X86 compatible system

Packages for **Intel/AMD PCs**

- Combined RouterOS package
- Separate RouterOS packages *(view content)*
- ISO image
- RouterOS **2.9.48** Changelog

Optional Packages

- User manager package
- Wireless Package with new country settings

v3 Release candidate

- Combined RouterOS package
- Separate RouterOS packages *(view content)*
- ISO image
- RouterOS **3.0rc9** Changelog

→ Alguns pacotes não fazem parte da distribuição normal mas podem ser instalados posteriormente. Exemplo o pacote User Manager..

→ Os arquivos também tem a extensão .npk e basta coloca-los no diretório raiz do Mikrotik e boota-lo para subir a nova versão.

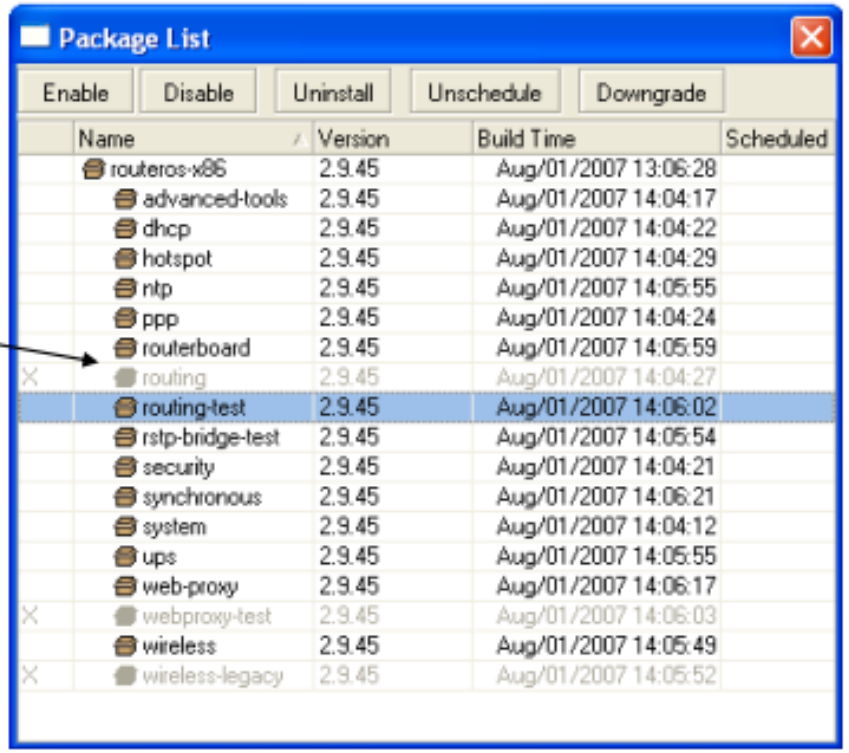
→ O upload pode ser feito por FTP ou copiando e colando no WInbox.

Manutenção do Mikrotik
Manipulação de pacotes

Alguns pacotes podem não ter sido instalados no momento da instalação ou podem estar desabilitados. Pacotes podem ser habilitados/desabilitados de acordo com as necessidades.

verifica-se e manipula-se o estado dos pacotes em / system packages

Pacote desabilitado



Se o pacote não tiver sido instalado, para faze-lo devemos encontrar o pacote de mesma versão, fazer um upload para o Mikrotik que este será automaticamente instalado

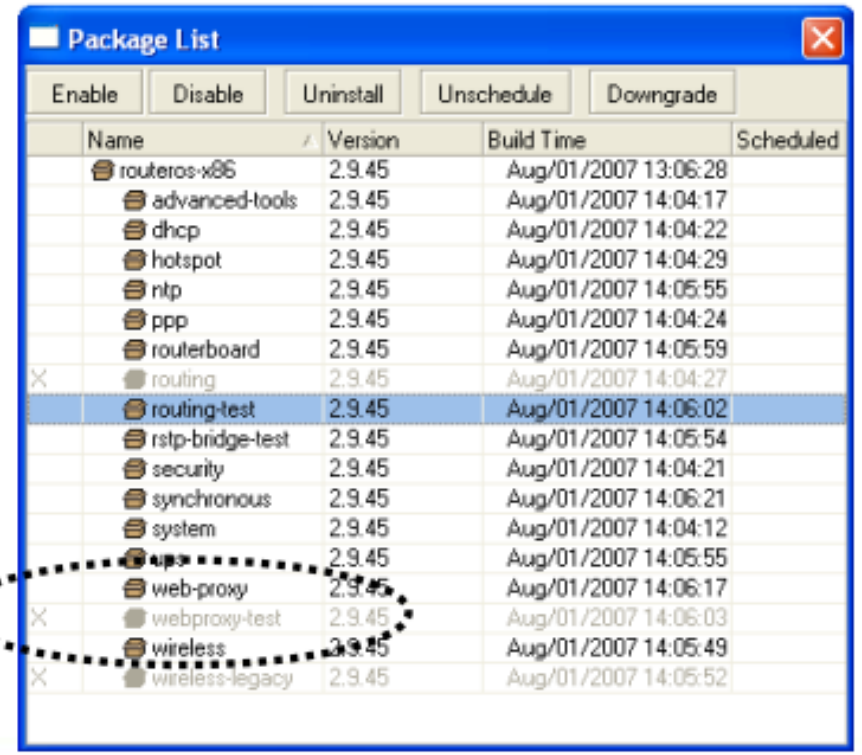
Manutenção do Mikrotik
Manipulação de pacotes

Existem os pacotes estáveis e os pacotes “test”, que estão ainda sendo reescritos e podem estar sujeitos a bugs e carencia de documentação.

Quando existem 2 iguais e um é test deve-se escolher um deles para trabalhar.

web-proxy e

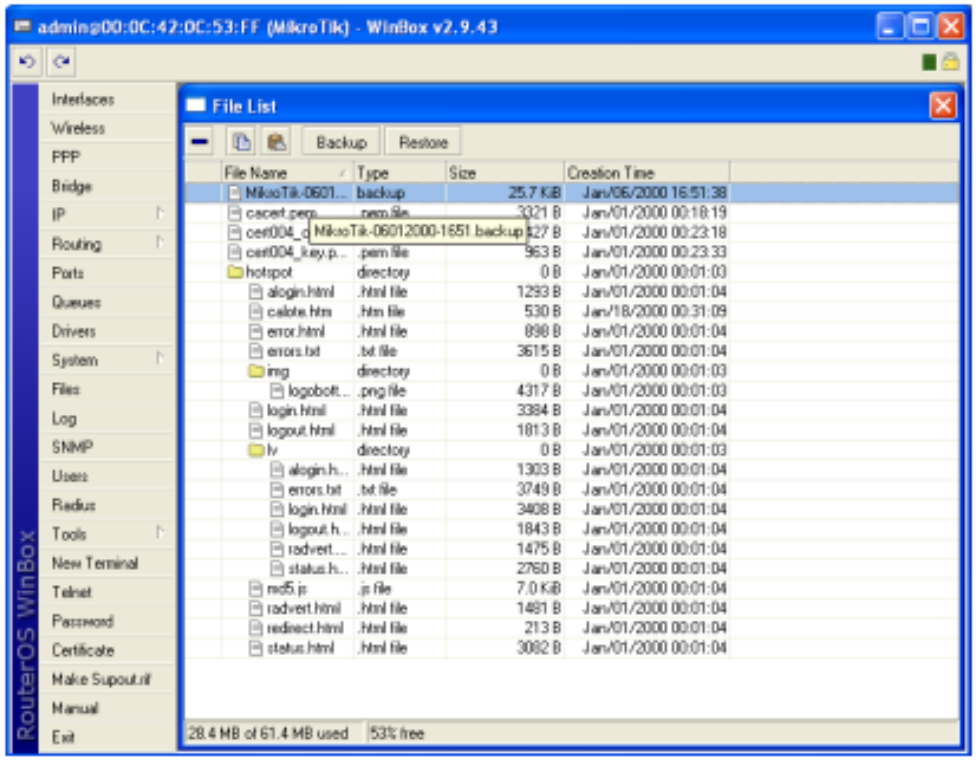
web-proxy-test



Manutenção do Mikrotik
Backup

Para efetuar o Backup, basta ir em Files e clicar em Backup copiando o arquivo para um lugar seguro.

Para restaurar, basta colar onde se quer restaurar e clicar na tecla Restore



OBS: O Backup feito dessa forma ao ser restaurado em outro hardware terá problemas com diferentes endereços MAC. Para “backupear” partes das configurações use o comando **export**

Licenciamento do Mikrotik

Detalhes de licenciamento

→ A chave é gerada sobre um software-id fornecido pelo próprio sistema

→ Fica vinculada ao HD ou Flash (e dependendo do caso da placa mãe)

→ Importante: **a formatação com ferramentas de terceiros muda o soft-id e causa a perda da licença instalada**

Política de Licenciamento

Nivel	4 (WISP)	5 (WISP)	6 (Controller)
Preços	R$ 105,00	R$ 210,00	R$ 510,00
Prazo para Upgrade	ROS v4.x	ROS v5.x	ROS v5.x
Suporte Configuração Inicial	15 dias	30 dias	30 dias
Funcionalidades			
Wireless AP	sim	sim	sim
Wireless Client and Bridge	sim	sim	sim
RIP, OSPF, BGP protocols	sim (v3 x86 = RIP, OSPF)	sim (v3 x86 = todos)	sim
EoIP tunnels	ilimitado	ilimitado	ilimitado
PPPoE tunnels	200	500	ilimitado
PPTP tunnels	200	ilimitado	ilimitado
L2TP tunnels	200	ilimitado	ilimitado
VLAN interfaces	ilimitado	ilimitado	ilimitado
P2P firewall rules	ilimitado	ilimitado	ilimitado
NAT rules	ilimitado	ilimitado	ilimitado
HotSpot active users	200	500	ilimitado
RADIUS client	sim	sim	sim
Queues	ilimitado	ilimitado	ilimitado
Web proxy	sim	sim	sim
Synchronous interfaces	sim	sim	sim
User manager active sessions	10 (v3 20)	10 (v3 50)	ilimitado

Dúvidas e esclarecimentos adicionais sobre

→ Instalação ?

→ Acesso ?

→ Manutenção ?

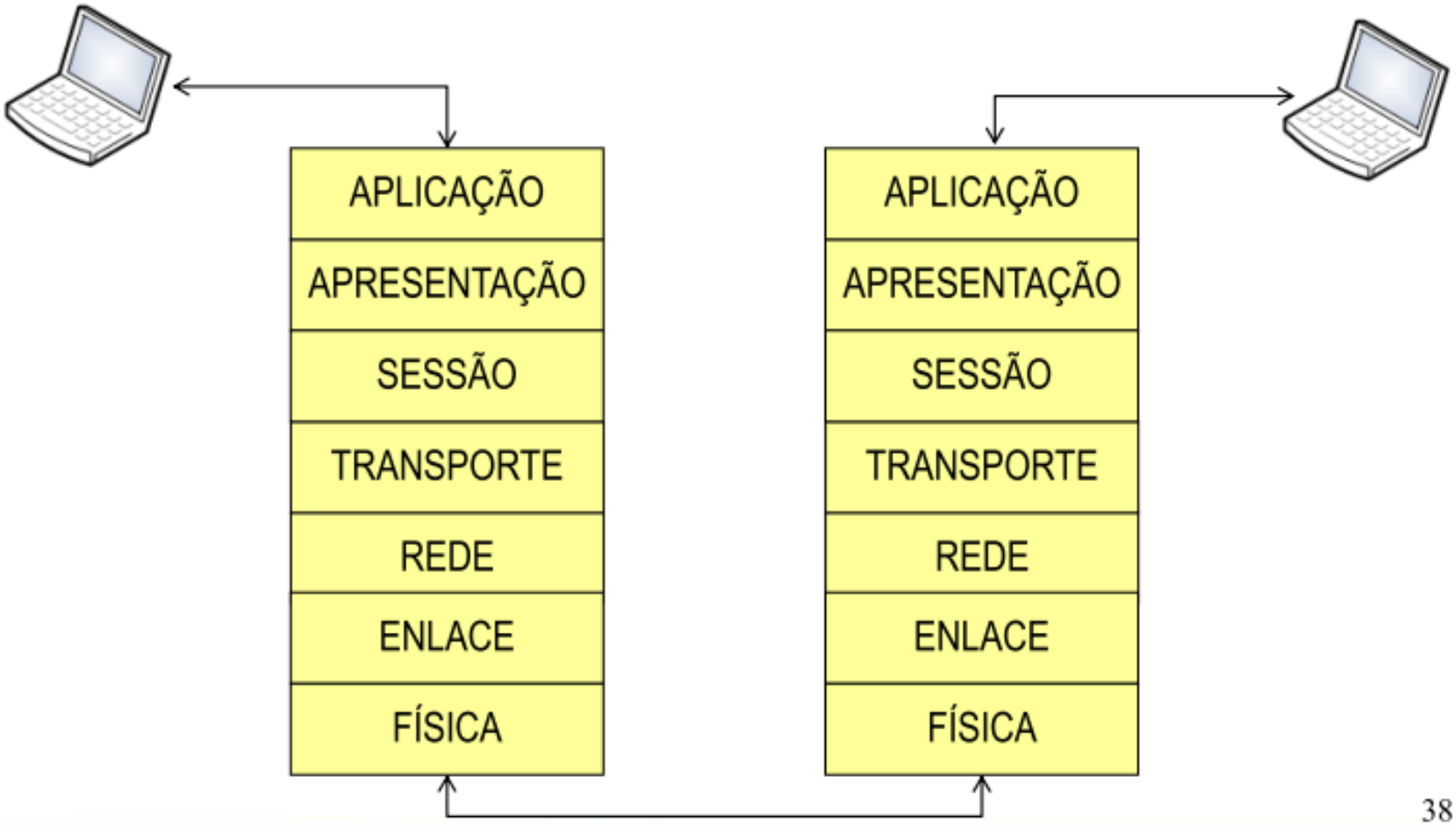
→ Licenciamento ?

Nivelamento de conceitos básicos de Redes TCP/IP e suas implementações no Mikrotik

O Modelo OSI
(Open Systems Interconnection)

APLICAÇÃO	←Camadas 7 (fornece a interface da aplicação ao usuário)
APRESENTAÇÃO	←Camada 6 (Gerencia como os dados serão apresentados)
SESSÃO	←Camada 5 (controla a comunicação entre dispositivos)
TRANSPORTE	←Camada 4 (responsável o transporte dos dados – TCP e UDP)
REDE	←Camada 3 (faz endereçamento lógico – roteamento IP)
ENLACE	←Camada 2 (detecta/corrige erros, controla fluxo, end.. físico)
FÍSICA	←Camada 1 (conexões físicas da rede, como cabos, wireless)

O Modelo OSI
(Open Systems Interconnection)



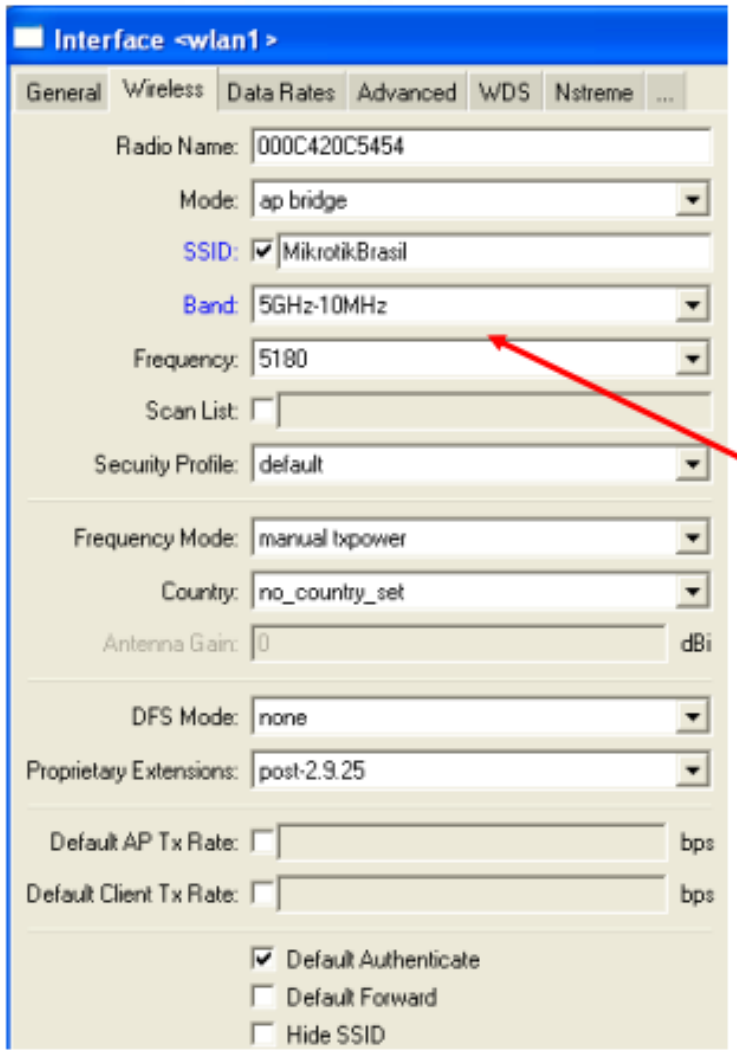
Camada I - Física

→ A camada física define as características técnicas dos dispositivos elétricos . que fazem parte da rede

→ É nesse nível que estão definidas as especificações de cabeamento estruturado, fibras óticas, etc. No caso de Wireless, é na camada I que se definem as modulações assim como a frequencia e largura de banda das portadoras

São especificações de Camada I:

RS-232, V.35, V.34, Q.911, T1, E1, 10BASE-T,100BASE-TX , ISDN, *SONET*, DSL, FHSS, DSSS, OFDM etc



Camada I - Física

Exemplo de configuração da camada física:

Escolhe-se a banda de transmissão e a forma com que o rádio irá se comportar

Exemplo de configuração física da Interface Wireless

No lado do AP

1 → Configurar o AP, definindo banda, canal, modo de operação e nome de rede

No lado dos alunos:

1 → Configurar como station, com o mesmo nome de rede e banda

2 → Na aba Wireless, no campo Radio name, colocar o seu número e nome, no seguinte padrão:

XY-SeuNome

Camada II - Enlace

→ Camada responsável pelo endereçamento físico, controle de acesso ao meio e correção de erros da camada I

→ O endereçamento físico se faz pelos endereços MAC (Controle de acesso ao meio) que são (ou deveriam ser) únicos no mundo e que são atribuídos aos dispositivos de rede

→ Bridges são exemplos de dispositivos que trabalham na camada II.

São especificações de Camada II:
Ethernet, Token Ring, FDDI, PPP, HDLC, Q.921, Frame Relay, ATM

Camada II - Enlace

Exemplo de configuração de Camada II (Enlace)

→ No AP Central: criar uma Bridge entre as interfaces Wireless

→ Bridges Verdadeiras / Bridges Falsas

Camada III - Rede

→ Responsável pelo endereçamento lógico dos pacotes

→ Transforma endereços lógicos em endereços físicos de rede

→ Determina a rota que os pacotes irão seguir para atingir o destino baseado em fatores tais como condições de tráfego de rede e prioridades.

→ Define como os dispositivos de rede se descobrem e como os pacotes são roteados ao destino final..

Estão na Camada III:

IP, ICMP, IPsec, ARP, RIP, OSPF, BGP

Protocolo IP

É um protocolo cujas funções principais são:

→ endereçamento
→ roteamento

As principais funções do protocolo IP são endereçamento e roteamento pois este fornece de uma maneira simples a possibilidade de identificar uma máquina na rede (endereço IP) e uma maneira de encontrar um caminho entre a origem e o destino (Roteamento).

Endereço IP = Número binário de 32 bits

Protocolo IP

É um protocolo cujas funções principais são:

→ endereçamento
→ roteamento

As principais funções do protocolo IP são endereçamento e roteamento pois este fornece de uma maneira simples a possibilidade de identificar uma máquina na rede (endereço IP) e uma maneira de encontrar um caminho entre a origem e o destino (Roteamento).

Endereço IP = Número binário de 32 bits

Endereçamento por Classes de IP

Classe	# Bits de rede	# Bits de Hosts	Range Decimal
Class A	8 bits	24 bits	1-126
Class B	16 bits	16 bits	128-191
Class C	24 bits	8 bits	192-223

Usando o esquema de classes era possível:

→ 126 redes “Classe A” que podiam ter até 16,777,214 hosts cada.
→ Mais 65,000 redes “Classe B” networks que podiam ter até 65,534 hosts cada
→ Mais 2 milhões de redes “Classe C” que podiam ter até 254 hosts cada.

Esquema de endereçamento CIDR

No esquema CIDR (Classless Internet Domain Routing), os computadores em uma rede fazem uso das máscaras de rede para separar computadores em sub-redes.

As máscaras de rede são tambem números binários de 32 bits, que dividimos em octetos

11111111.11111111.11111111.00000000

11111111 → 2^7 + 2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 2^1 = 255

máscara equivalente em decimal:

→ 255.255.255.0

Máscaras de rede

Além da forma binária e decimal as máscaras de rede podem ser representadas pela notação em bitmask (soma dos bits que compõe a máscara);

Exemplos:

11111111.11111111.11111111.11111111
→ decimal : 255.255.255.255 → bitmask: /32

11111111.11111111.11111111.11111100
→ decimal: 255.255.255.252 → bitmask: /30

11111111.00000000.00000000.0000000
→ decimal: 255.0.0.0 → bitmask: /8

Endereçamento de rede

Para separar computadores em sub redes é realizada uma multiplicação binária do endereço IP com a máscara de rede, sendo então calculado o endereço de rede para aquele host.

Exemplo: 200.200.200.10 com máscara 255.255.255.192 (ou /26)

	Decimal	1 octeto	2 octeto	3 octeto	4 octeto
IP	200.200.200.10	11001000	11001000	11001000	00001010
Mask	255.255.255.192	11111111	11111111	11111111	11000000
Multiplicação binária		11001000	11001000	11001000	00000000

Endereço de rede calculado → 200.200.200.0

Endereçamento de broadcast

O maior IP possivel para uma sub rede é chamado de endereço de broadcast e é o endereço para o qual se manda um pacote destinado a todos os hosts da rede.

Em uma rede os endereços de Rede e os endereços de Broadcast são reservados e não podem ser utilizados por hosts

Exemplos de endereços de rede e broadcast:

Endereço IP/mask	Rede	Broadcast
200.200.200.10/24	200.200.200.0	200.200.200.255
200.200.200.10/25	200.200.200.0	200.200.200.127
200.200.200.10/26	200.200.200.0	200.200.200.63
200.200.200.200/26	200.200.200.192	200.200.200.255

Sub Redes

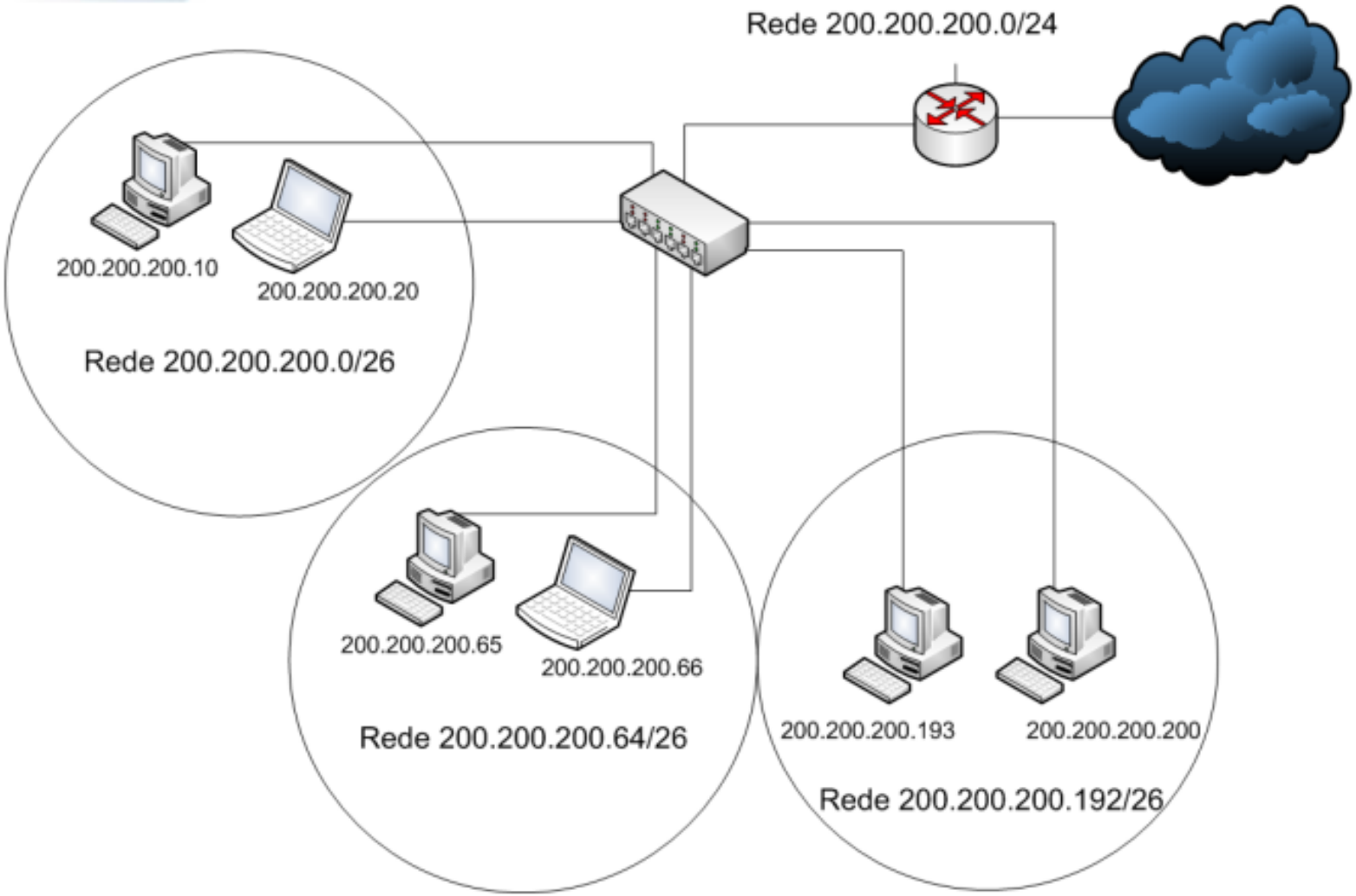
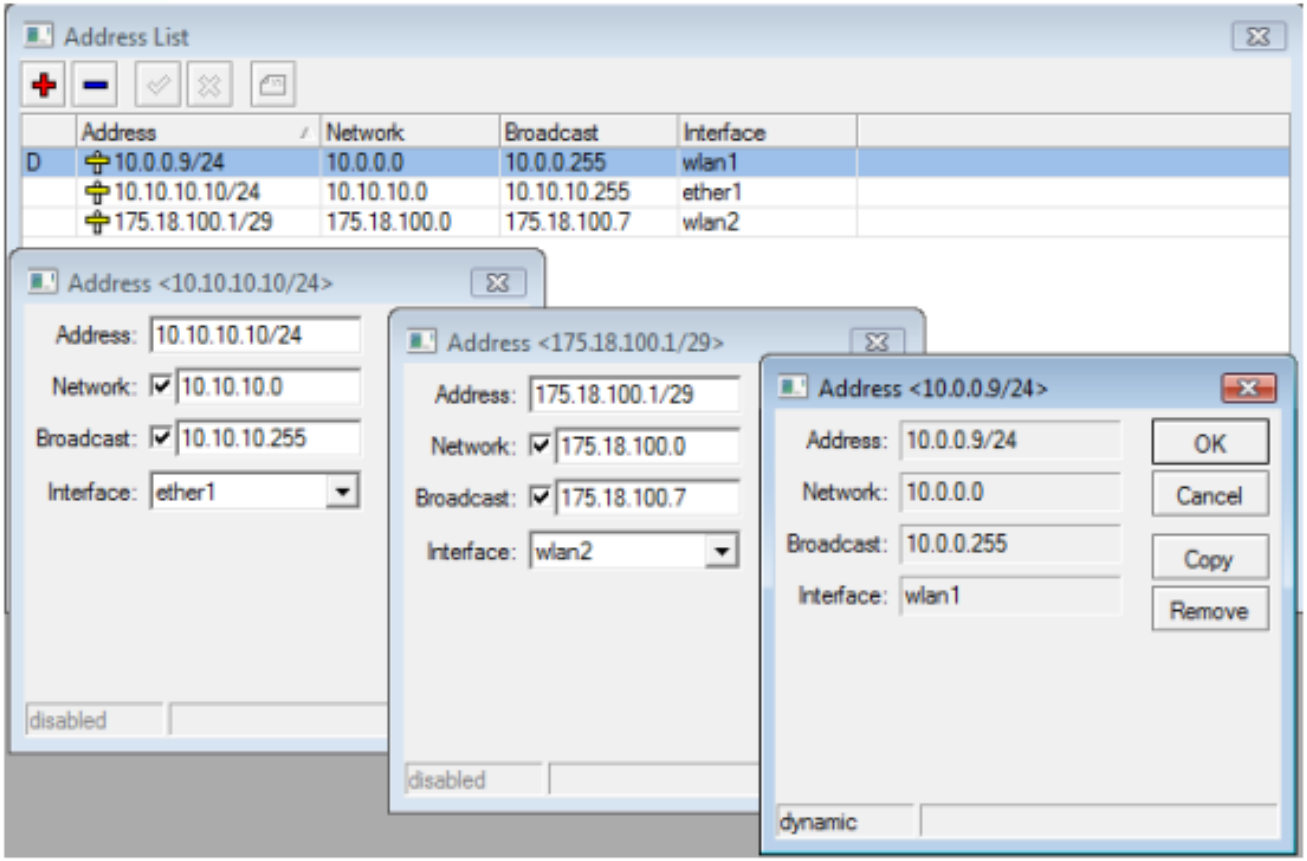

Rede 200.200.200.0/24
200.200.200.10
200.200.200.20
Rede 200.200.200.0/26
200.200.200.65
200.200.200.66
Rede 200.200.200.64/26
200.200.200.193
200.200.200.200
Rede 200.200.200.192/26

Tabela de referência IP's

Binário	Decimal	Bitmask	IP's	Hosts
11111111.11111111.11111111.11111111	255.255.255.255	/32	1	1
11111111.11111111.11111111.11111100	255.255.255.252	/30	4	2
11111111.11111111.11111111.11111000	255.255.255.248	/29	8	6
11111111.11111111.11111111.11110000	255.255.255.240	/28	16	14
11111111.11111111.11111111.11100000	255.255.255.224	/27	32	30
11111111.11111111.11111111.11000000	255.255.255.192	/26	64	62
11111111.11111111.11111111.10000000	255.255.255.128	/25	128	126
11111111.11111111.11111111.00000000	255.255.255.0	/24	256	254
…	….			
11111111.11111111.11110000.00000000	255.255.240.0	/20	4096	4094
…	…			

Endereços IP no Mikrotik



Atentar para a especificação correta da máscara de rede que determinará o endereço de rede e o de broadcast

Protocolo ARP
(Address resolution Protocol)

→ Utilizado para associar IP's com endereços físicos – faz a interface entre a camada II e a camada III.

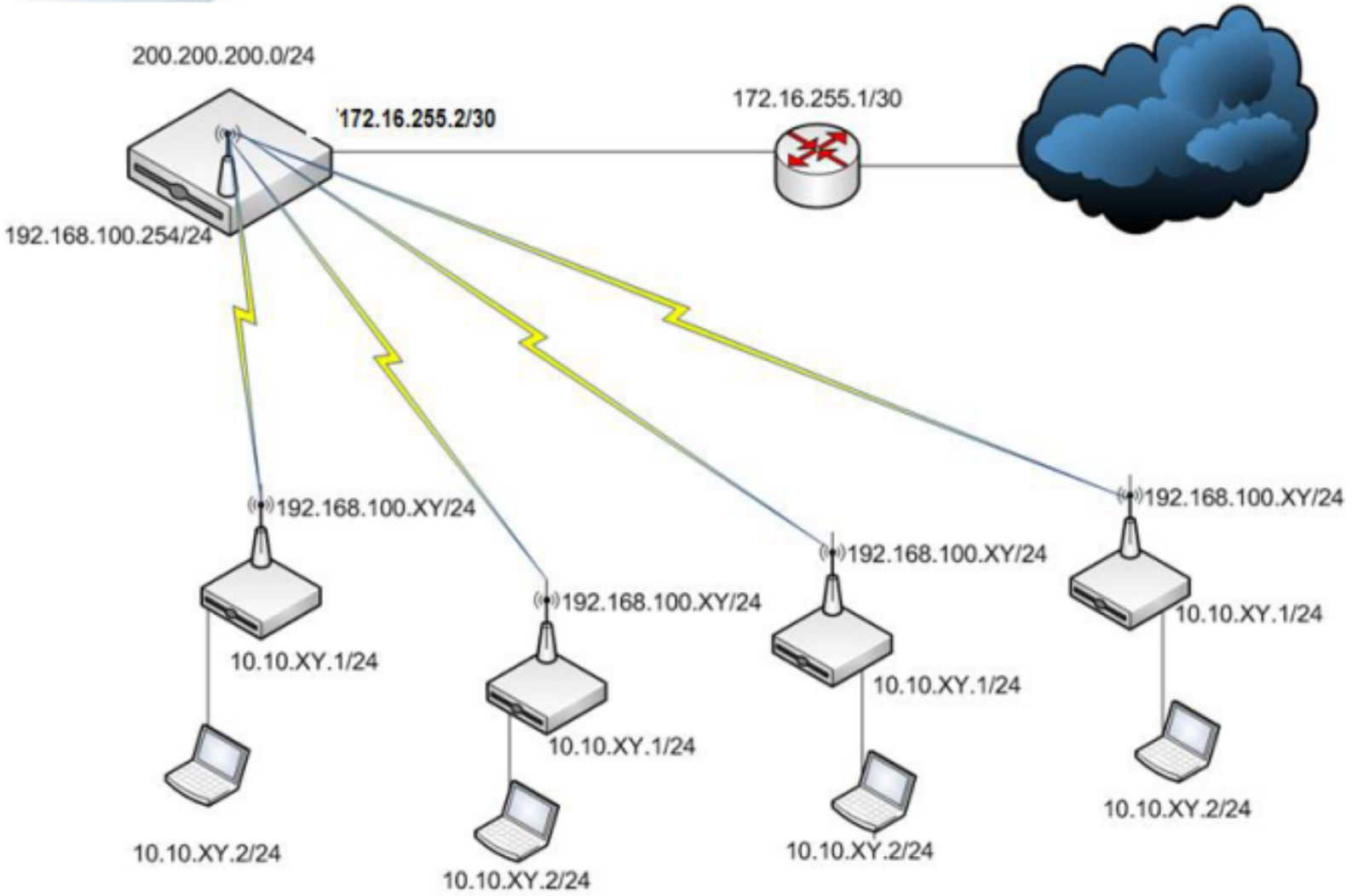
→ Funcionamento:

→ O solicitante de ARP manda um pacote de broadcast com a informação do IP de destino, IP de origem e seu MAC, perguntando sobre o MAC de destino

→ O Host que tem o IP de destino manda um pacote de retorno fornecendo seu MAC

→ Para minimizar os broadcasts devido ao ARP, são mantidas no SO, as tabelas ARP, constando o par IP – MAC

Cenário inicial do Curso



Configuração de Rede

No AP Central:

1 → Cadastrar o IP 192.168.100.254 com máscara 255.255.255.0 na wlan1

Nos alunos:

1 →Cadastrar um IP 192.168.100.XY com máscara 255.255.255.0 wlan1 do Mikrotik

2 →Como ficou sua tabela de rotas ?

Protocolo ARP
(Address resolution Protocol)

→ Observe a tabela ARP do AP

→ Consulte sua Tabela ARP

→ Torne a entrada do AP em uma entrada estática, clicando com o botão direito e “Make Static”

Roteamento

No AP Central:

1 → Cadastrar a rota default no AP Central.

Nos alunos:

1 → Cadastrar a rota default

2 → Como ficou sua tabela de rotas ?

Configuração de DNS

No AP Central:

1 → Configure o DNS apontando-o para o DNS da operadora

Nos alunos:

1 → Configure o DNS apontando para o AP Central

2 → Teste a resolução de nomes a partir da ROUTERBOARD

3 → Você quer que sua Torre resolva os nomes para o Laptop. O que tem de ser feito ?

Setup I – Roteamento estático

ectividade dos Laptops:

1 → Cadastrar o IP 10.10.XY.1/24 na Routerboard

2 → Cadastrar o IP 10.10.XY.2/24 no Laptop

3 → Cadastrar o Gateway e DNS no seu Laptop 10.10.XY.1

4 → teste as conectividades:

Laptop → Routerboard
Routerboard → AP Central
Laptop → AP Central

O que precisa ser feito para funcionar tudo ?

Camada IV - Transporte

→ No lado do remetente é responsável por pegar os dados das camadas superiores dividir em pacotes para que sejam transmitidos para a camada de rede.

→ No lado do destinatário pega os pacotes recebidos da camada de rede, remonta os dados originais e envia às camadas superiores.

Estão na Camada IV:

TCP, UDP, RTP, SCTP

Protocolo TCP

O TCP é um protocolo de transporte e executa importantes funções para garantir que os dados sejam entregues de uma maneira confiável, ou seja, sem que os dados sejam corrompidos ou alterados.

Características do protocolo TCP

→ Garante a entrega de datagramas IP

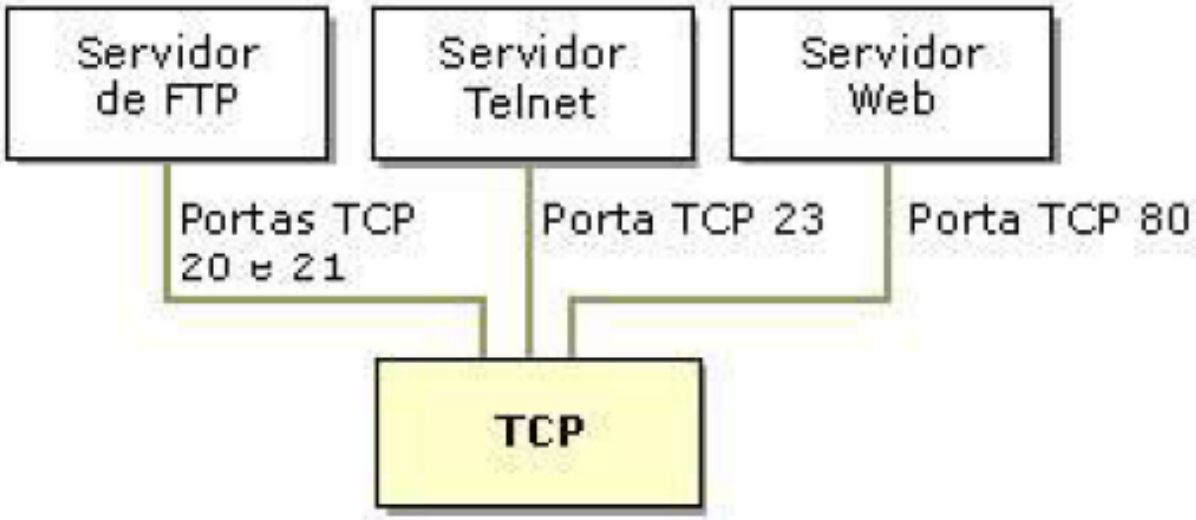
→ Executa a segmentação e reagrupamento de grandes blocos de dados enviados pelos programas e Garante o seqüenciamento adequado e entrega ordenada de dados segmentados.

→ Verifica a integridade dos dados transmitidos usando cálculos de soma de verificação

→ Envia mensagens positivas dependendo do recebimento bem-sucedido dos dados. Ao usar confirmações seletivas, também são enviadas confirmações negativas para os dados que não foram recebidos

→ Oferece um método preferencial de transporte de programas que devem usar transmissão confiável de dados baseada em sessões, como bancos de dados cliente/servidor e programas de correio eletrônico

Portas TCP



O uso do conceito de portas, permite que vários programas estejam em funcionamento, ao mesmo tempo, no mesmo computador, trocando informações com um ou mais serviços/servidores.

Portas abaixo de 1024 são registradas para serviços especiais

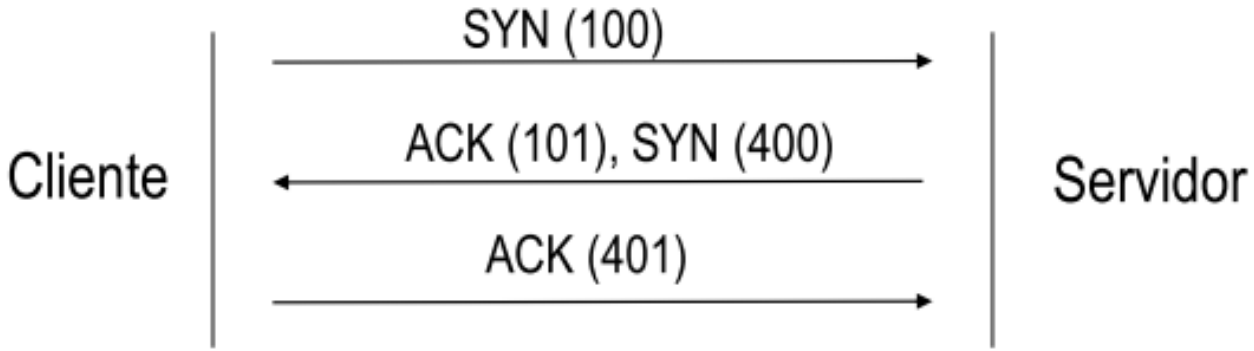
Estabelecimento de uma conexão TCP

Uma conexão TCP é estabelecida em um processo de 3 fases:

→ O "Cliente" a conexão manda uma requisição SYN contendo o número da porta que pretende utilizar e um número de sequencia inicial.

→ O "Servidor" responde com um ACK com o número sequencial enviado +1 e um pacote SYN com um outro número de sequencia

→ O "Cliente" responde com um ACK com o numero recebido do SYN +1



Enviando dados com TCP

O TCP divide o fluxo de dados em segmentos

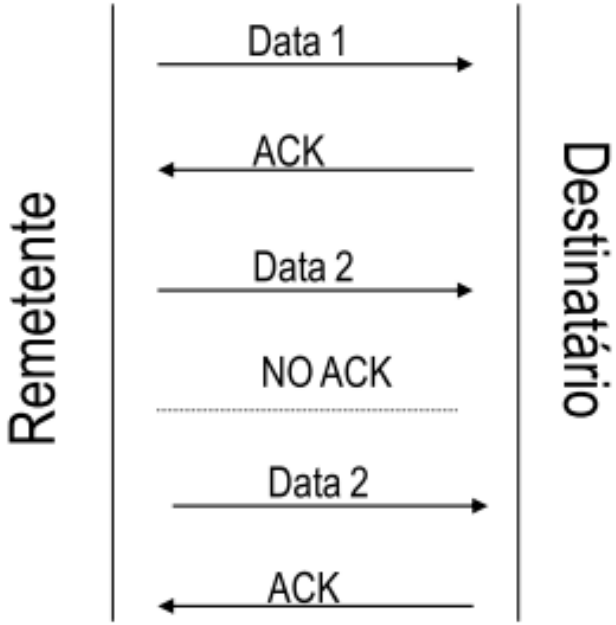
→ o remetente manda dados em segmentos com um número sequencial

→ o destinatário acusa o recebimento de cada segmento

→ o remetente manda os dados seguintes

→ se não recebe a confirmação do recebimento, manda novamente

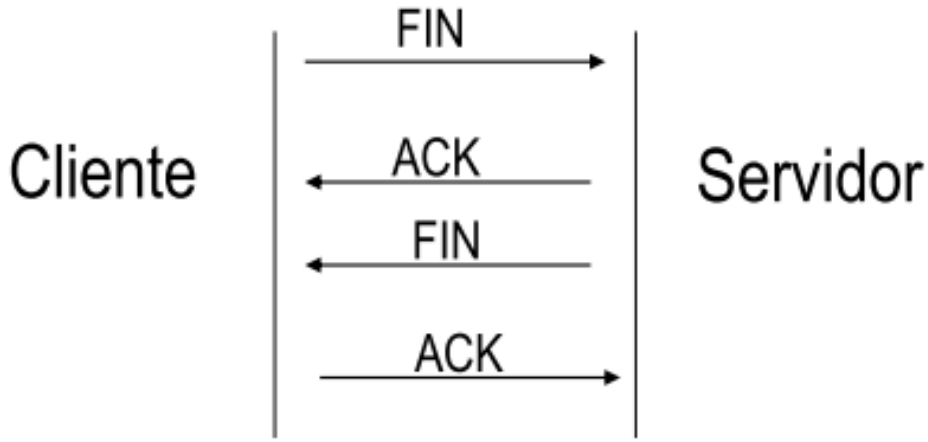
No caso da conexão ser abortada uma flag RST é mandada ao remetente



Encerrando uma conexão TCP

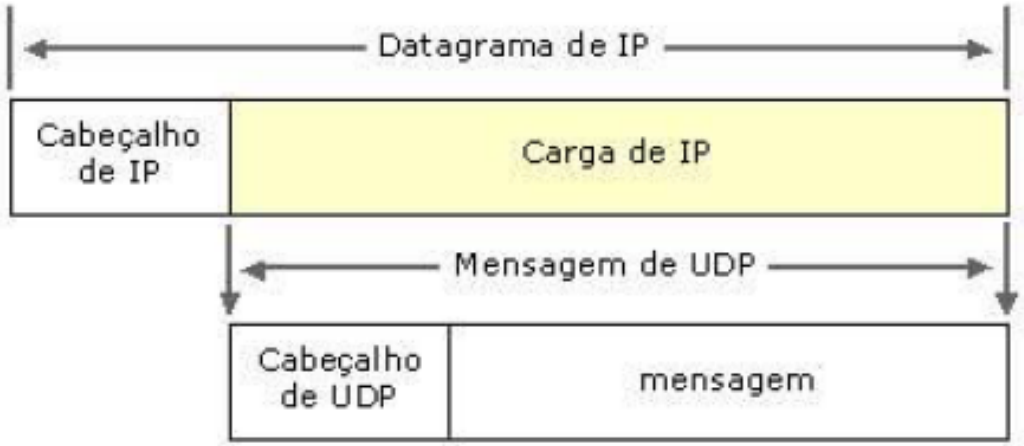
O processo de encerramento também é feito em 4 fases:

- Remetente manda um pedido de FIN
- Destinatário responde acusando o recebimento com um ACK
- Destinatário manda seu pedido de FIN
- Remetente envia um ACK



Protocolo UDP

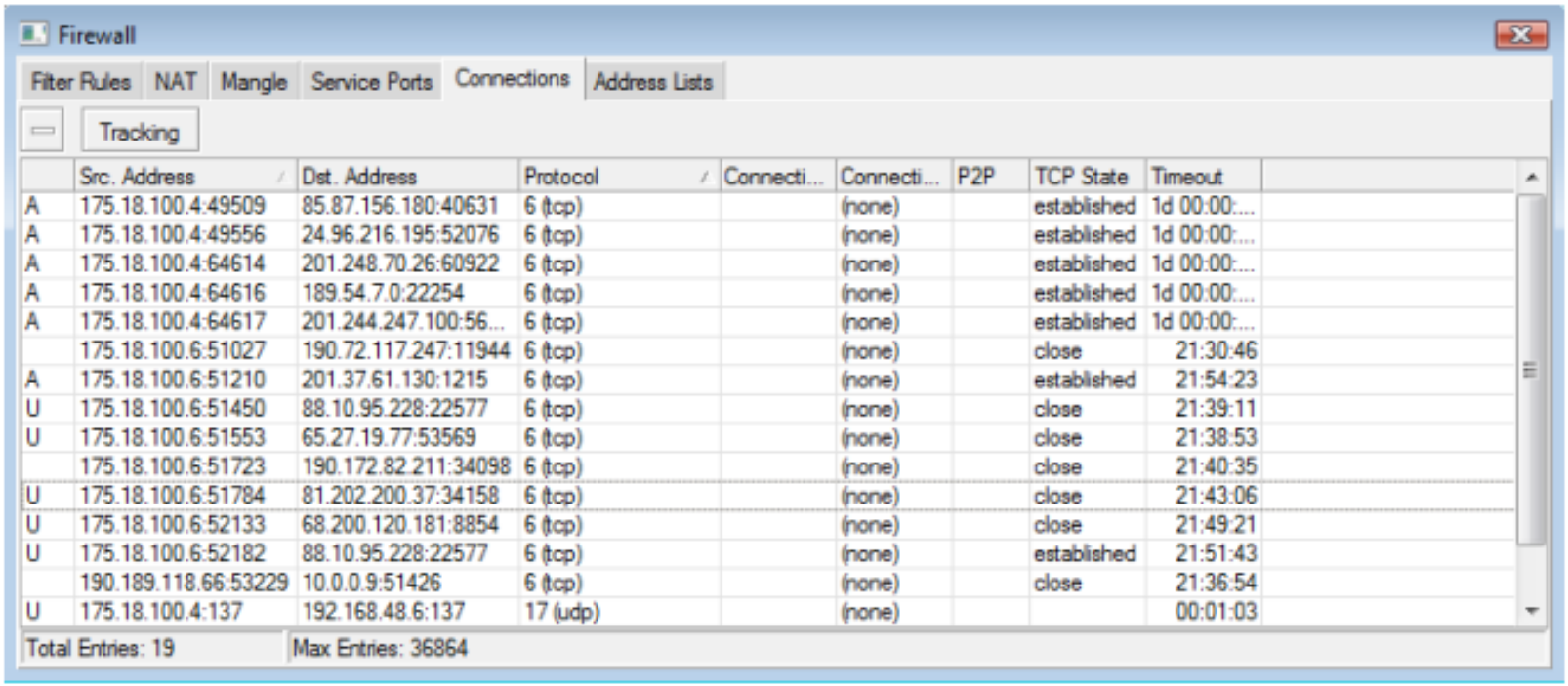
- O UDP (User Datagram Protocol) é utilizado para o transporte rápido entre hosts
- O UDP é um serviço de rede sem conexão, ou seja não garante a entrega do pacote
- Mensagens UDP são encapsuladas em datagramas IP



Comparação TCP e UDP

UDP	TCP
Serviço sem conexão. Não é estabelecida sessão entre os hosts	Serviço orientado por conexão. Uma sessão é estabelecida entre os hosts.
UDP não garante ou confirma a entrega dos dados	Garante a entrega através do uso de confirmação e entrega sequenciada dos dados
Os programas que usam UDP são responsáveis pela confiabilidade	Os programas que usam TCP tem garantia de transporte confiável de dados
Rápido, exige poucos recursos oferece comunicação ponto a ponto e ponto multiponto	Mais lento, usa mais recursos e somente dá suporte a ponto a ponto

Observe o estado de suas conexões em IP / Firewall / Connections



	Src. Address	Dst. Address	Protocol	Connecti...	Connecti...	P2P	TCP State	Timeout
A	175.18.100.4:49509	85.87.156.180:40631	6 (tcp)		(none)		established	1d 00:00:...
A	175.18.100.4:49556	24.96.216.195:52076	6 (tcp)		(none)		established	1d 00:00:...
A	175.18.100.4:64614	201.248.70.26:60922	6 (tcp)		(none)		established	1d 00:00:...
A	175.18.100.4:64616	189.54.7.0:22254	6 (tcp)		(none)		established	1d 00:00:...
A	175.18.100.4:64617	201.244.247.100:56...	6 (tcp)		(none)		established	1d 00:00:...
	175.18.100.6:51027	190.72.117.247:11944	6 (tcp)		(none)		close	21:30:46
A	175.18.100.6:51210	201.37.61.130:1215	6 (tcp)		(none)		established	21:54:23
U	175.18.100.6:51450	88.10.95.228:22577	6 (tcp)		(none)		close	21:39:11
U	175.18.100.6:51553	65.27.19.77:53569	6 (tcp)		(none)		close	21:38:53
	175.18.100.6:51723	190.172.82.211:34098	6 (tcp)		(none)		close	21:40:35
U	175.18.100.6:51784	81.202.200.37:34158	6 (tcp)		(none)		close	21:43:06
U	175.18.100.6:52133	68.200.120.181:8854	6 (tcp)		(none)		close	21:49:21
U	175.18.100.6:52182	88.10.95.228:22577	6 (tcp)		(none)		established	21:51:43
	190.189.118.66:53229	10.0.0.9:51426	6 (tcp)		(none)		close	21:36:54
U	175.18.100.4:137	192.168.48.6:137	17 (udp)		(none)			00:01:03

Total Entries: 19 | Max Entries: 36864

Fazendo uma conexao TCP

Nos alunos:

1 → Abrir uma sessão de FTP para o IP do nosso servidor de FTP

2 → Verifique a sua tabela de Connection Tracking

No AP Central:

1 → Exibir a tabela de Connection Tracking

Dúvidas ou considerações acerca de:

→ Camadas física / enlace / rede / transporte / aplicação
→ Protocolo IP / Mascaras de rede ?
→ Protocolo ARP ?
→ TCP ?
→ UDP ?

Setup II - Configuração da sala com NAT

→ Configure o mascaramento de rede

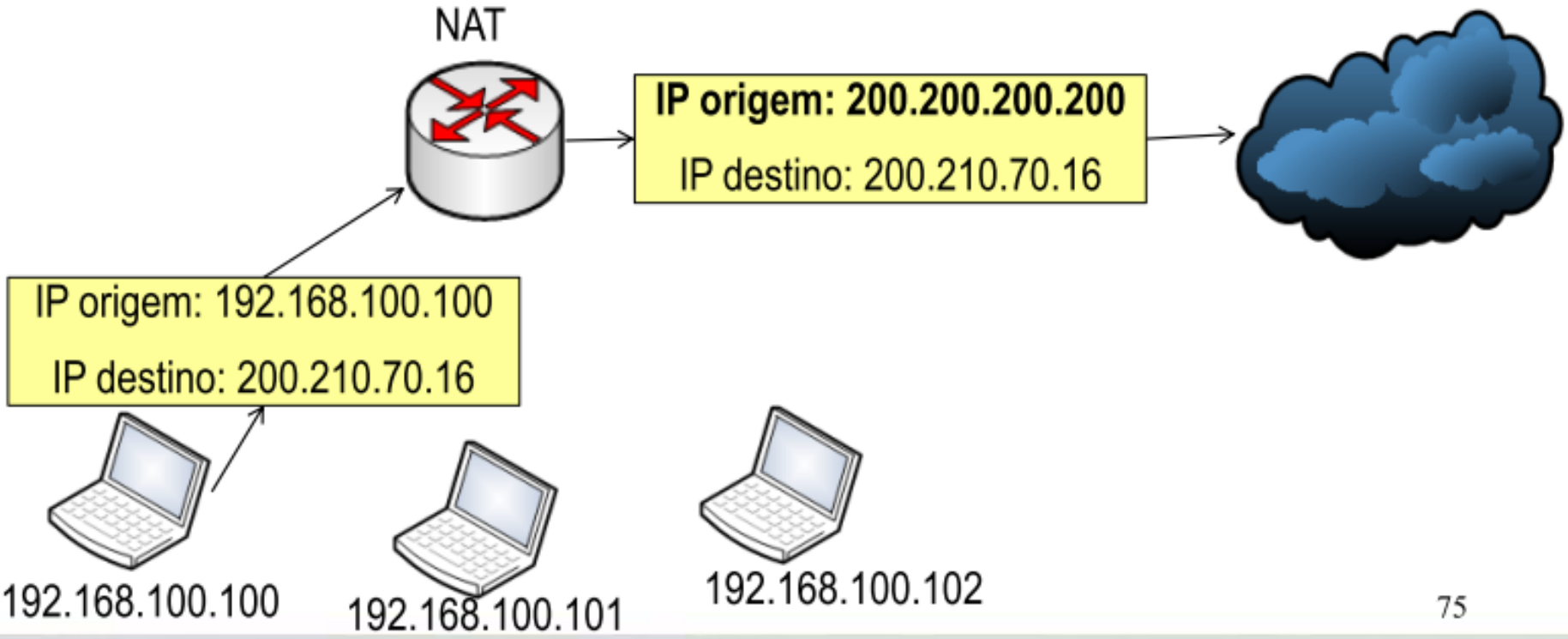
→ Teste a conectividade com o mundo exterior.

→ Apague backups anteriores eventualmente feitos e faça um backup de suas configurações

→ Salve os backups tambem no seu Laptop. Elas serão úteis durante o curso.

Mascaramento de rede

Exemplo: Um computador da rede interna 192.168.100.100 acessando www.mikrotikbrasil.com.br (200.210.70.16) através do roteador que tem IP público 200.200.200.200.



Mascaramento de rede

O mascaramento de rede é a técnica que permite que diversos computadores em uma rede compartilhem de um mesmo endereço IP. No Mikrotik o mascaramento é feito através do firewall por uma funcionalidade chamada NAT (Network Address Translation)

Todo e qualquer pacote de dados em uma rede possui um endereço IP de origem e um de destino. Para mascarar o endereço, o NAT faz a troca do IP de origem, e no retorno deste, conduz ao computador que o originou.

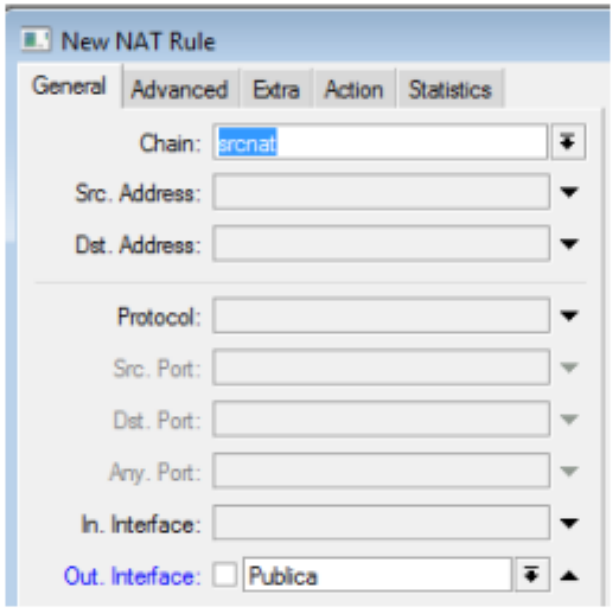
Exemplo: Um computador da rede interna 192.168.100.100 acessando www.mikrotikbrasil.com.br (200.210.70.16) através do roteador que tem IP público 200.200.200.200.

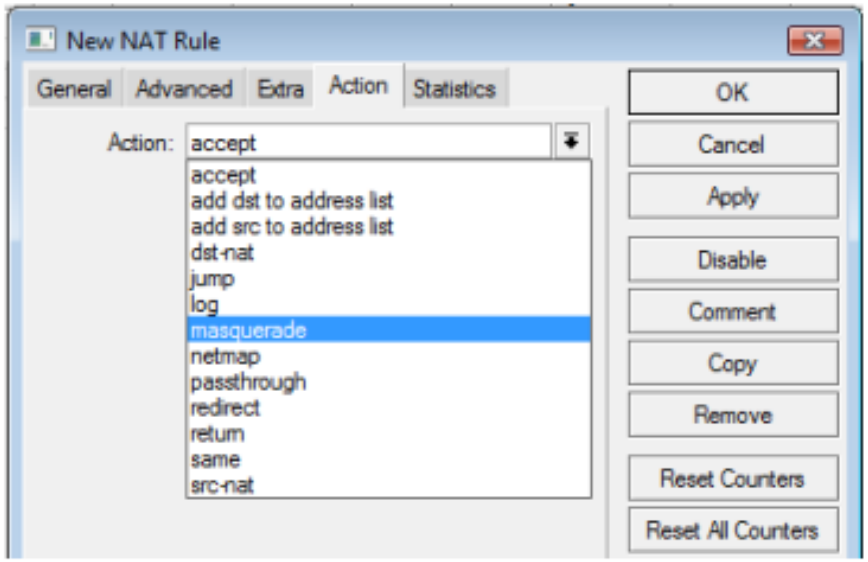
→ Destination NAT (dstnat), ou NAT de destino quando o roteador reescreve o endereço ou a porta de destino.

Mascaramento de Rede

No AP Central:

1 → Configurar o mascaramento de rede no AP Central.





Nos alunos:

3 → A partir ***do Mikrotik*** tente pingar a Internet (172.16.255.1). Funcionou ?

Mikrotik

&

Wireless

Configurações da camada Física
Bandas de operação

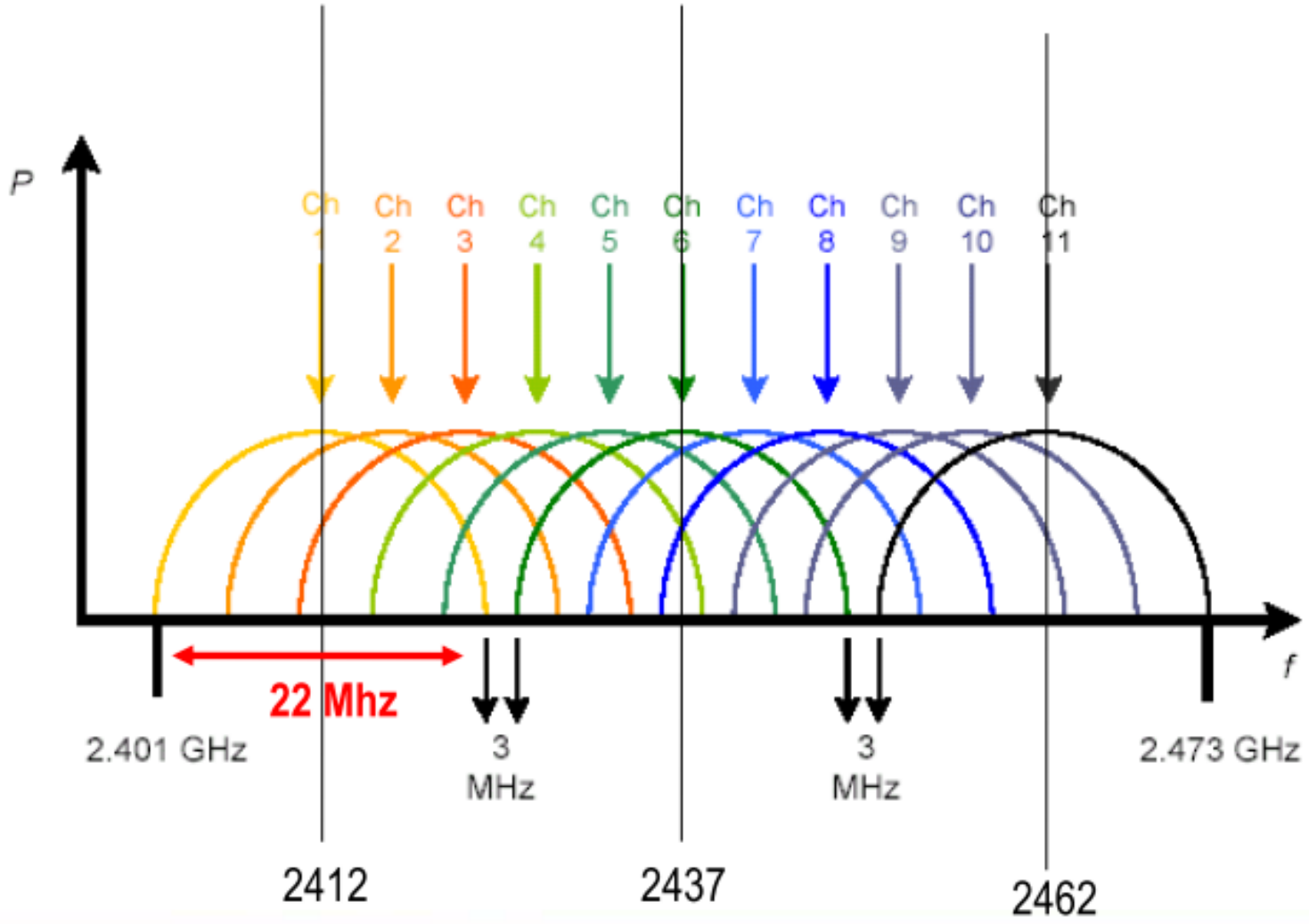
Configurações Físicas / Banda

Resumo dos padrões IEEE empregados e suas características:

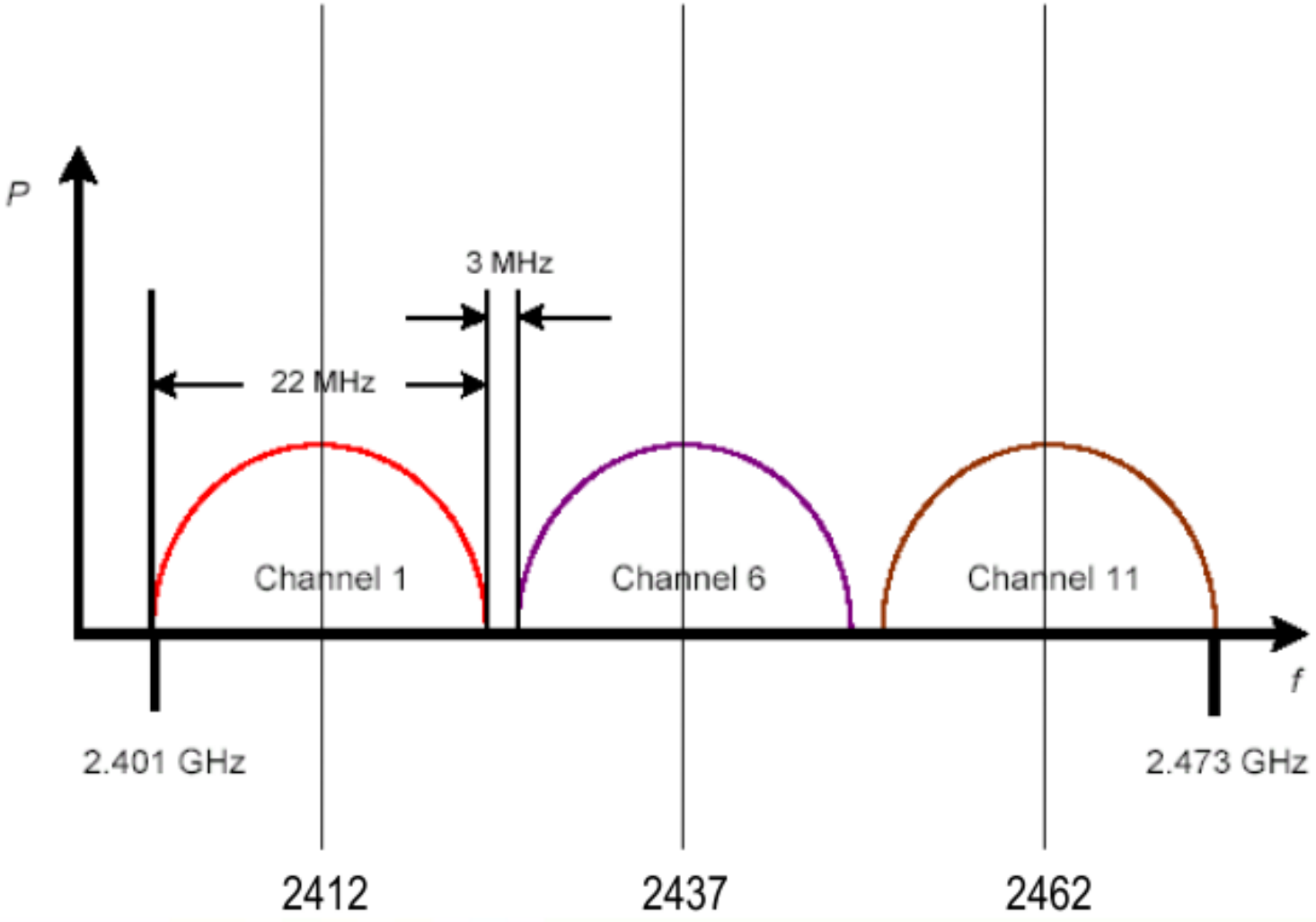
Padrão IEEE	Freqüência	Tecnologia	Velocidades
802.11b	2.4 Ghz	DSSS	1, 2, 5.5 e 11mbps
802.11g	2.4 Ghz	OFDM	6, 9, 12, 18, 24, 36 48 e 54 mbps
802.11a	5 Ghz	OFDM	6, 9, 12, 18, 24, 36 48 e 54 mbps
802.11n	2.4 Ghz e 5 Ghz	OFDM / MIMO	6,5 a 300 mpbs

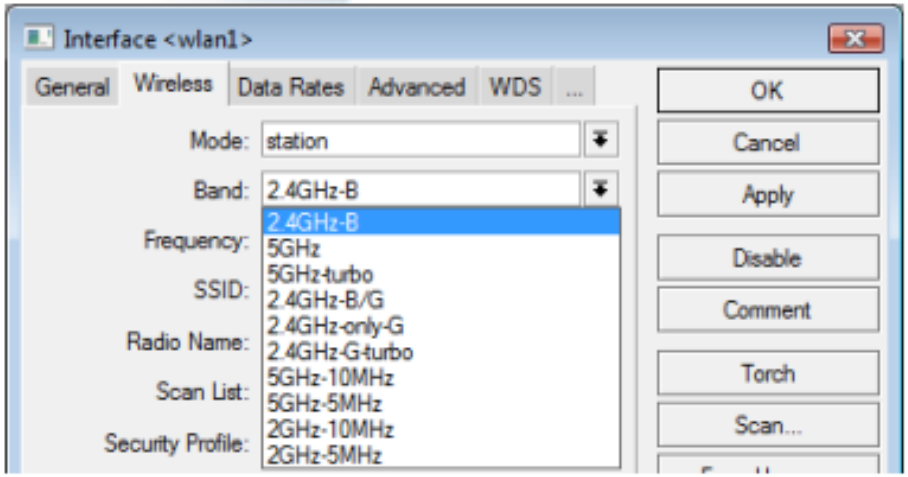
[MikrotikBrasil]
Routers & Wireless Systems

Canais em 2.4Ghz



Canais não interferentes em 2.4Ghz





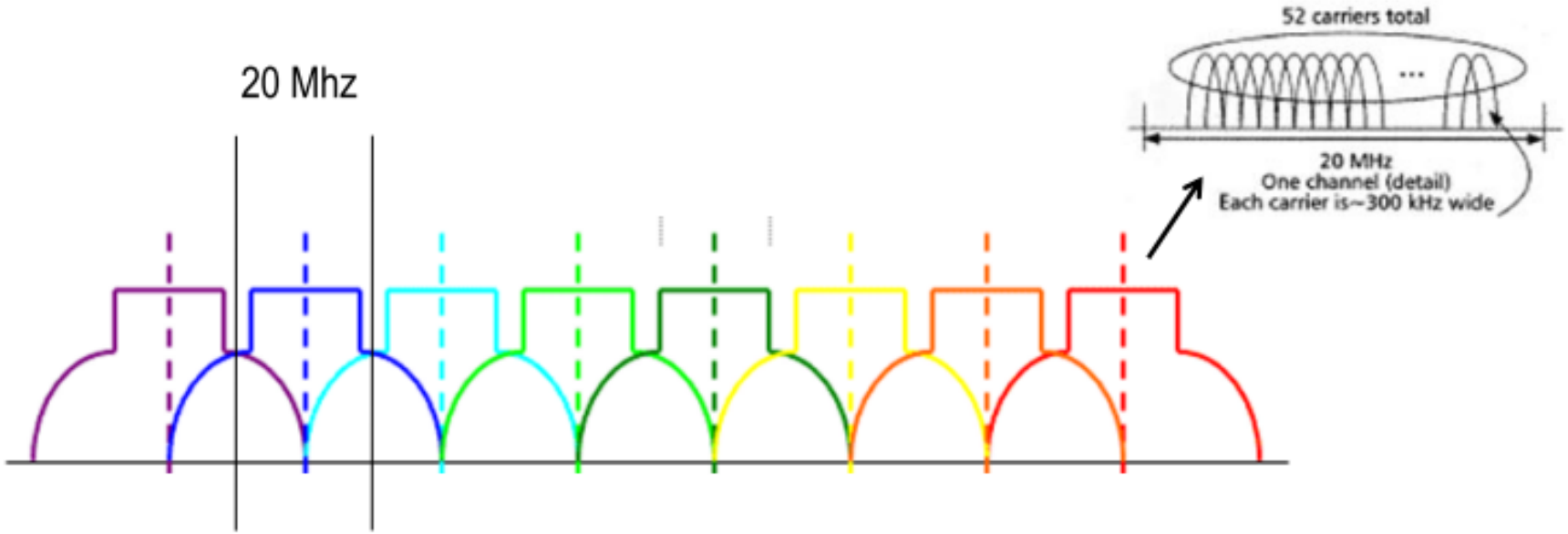
Configurações Físicas / Banda

2.4Ghz-B: Modo 802.11b, que permite velocidades nominais de 1, 2, 5.5 e 11 mbps. Utiliza espalhamento espectral em seqüência direta.

2.4Ghz-B/G: Modo misto 802.11b e 802.11g que permite as velocidades acima 802.11b e 6, 9, 12, 18, 24, 36, 48 e 54 mbps quando em G. Utiliza OFDM em 802.11g

2.4Ghz-only-G: Modo apenas 802.11g.

Canais do espectro de 5Ghz



Em termos regulatórios a faixa de 5 Ghz é dividida em 3 faixas:

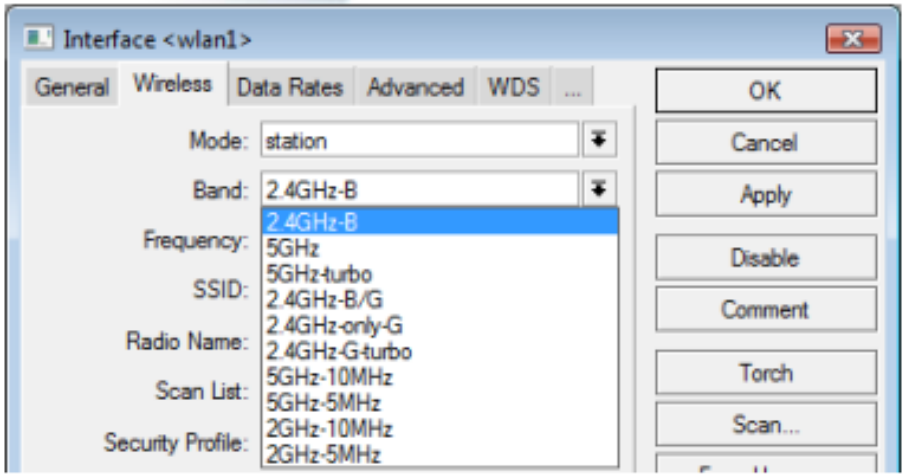
→ Faixa Baixa: 5150 a 5250 e 5250 a 5350 (Mhz)

→ Faixa Média: 5470 a 5725 (Mhz)

→ Faixa Alta: 5725 a 5850 (Mhz)

Aspectos Legais do espectro de 5Ghz

	Faixa Baixa		Faixa Média	Faixa Alta
Freqüências	5150-5250	5250-5350	5470-5725	5725-5850
Largura	100 Mhz	100 Mhz	255 Mhz	125 Mhz
canais	4 canais	4 canais	11 canais	5 canais
		Detecção de radar obrigatória	Detecção de radar obrigatória	



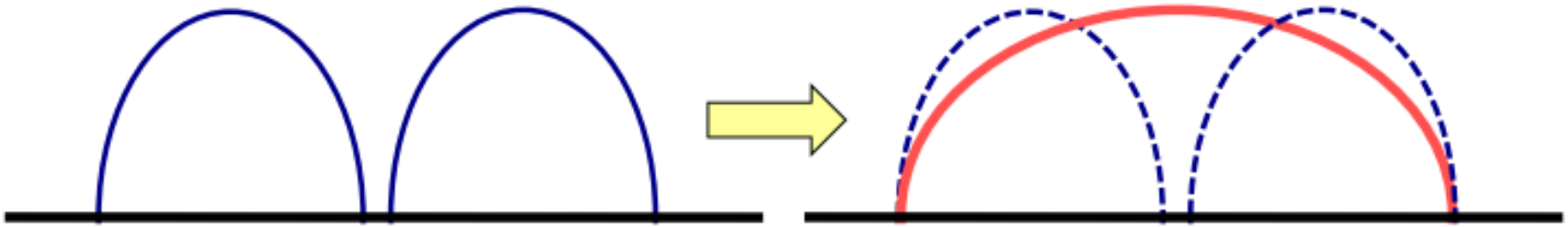
Configurações Físicas / Banda

5Ghz: Modo 802.11a – opera na faixa de 5 Ghz, baixa média e alta e permite velocidades nominais identicas ao do modo G, ou seja 6, 9, 12, 18, 24, 36, 48 e 54 mbps

Freqüência (Mhz)	5150 – 5350	5470 - 5725	5725 - 5850
Largura faixa	200 Mhz	255 Mhz	125 Mhz
Número de canais	4	11	5

Canalização em 802.11a

Modo Turbo



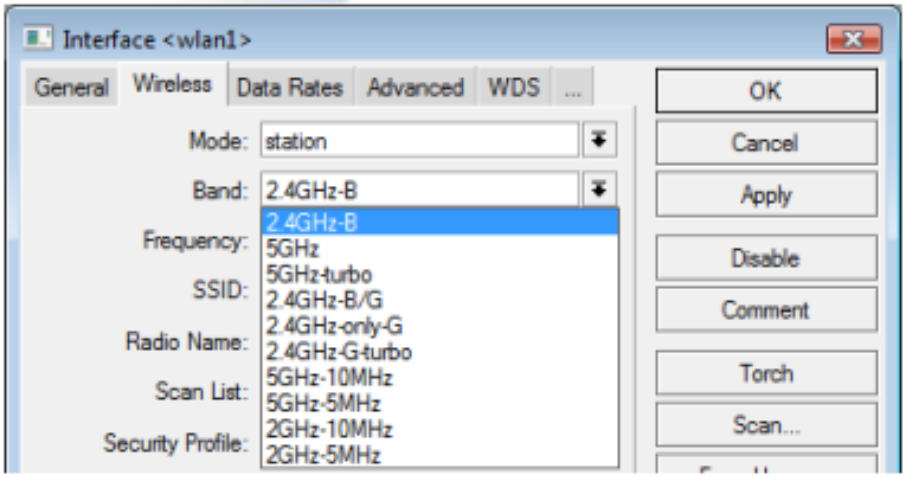
→ Maior troughput

→Menor número de canais

→Maior vulnerabilidade a interferências

→Requerida sensibilidade maior

→Diminui nível de potencia de Tx



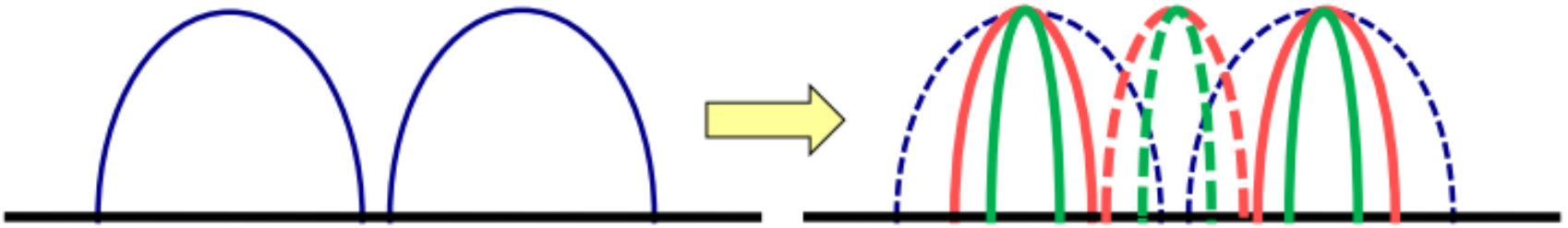
Configurações Físicas / Banda

5Ghz-turbo: Modo 802.11a – opera na faixa de 5 Ghz, baixa média e alta e permite velocidades nominais identicas ao do modo G, ou seja 6, 9, 12, 18, 24, 36, 48 e 54 mbps

Freqüência (Mhz)	5150 – 5350	5470 - 5725	5725 - 5850
Largura faixa	200 Mhz	255 Mhz	125 Mhz
Número de canais	2	5	2

Canalização em 802.11a

Modos 10 e 5 Mhz



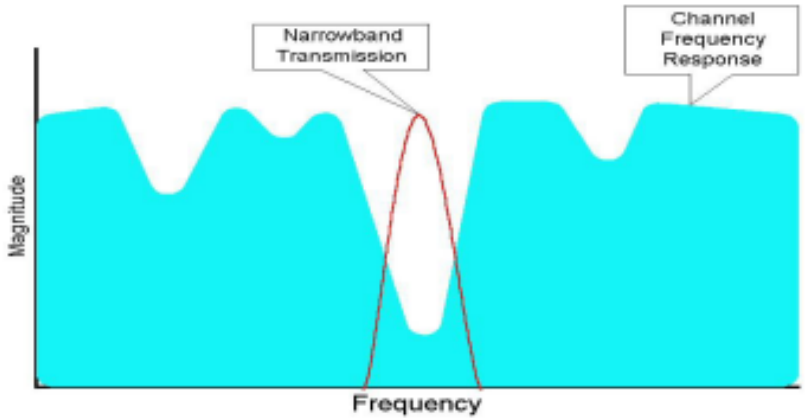
→ Menor troughput

→Maior número de canais

→Menor vulnerabilidade a interferências

→Requerida menor sensibilidade

→Aumenta nível de potencia de Tx



Faixa de 900 Mhz

No Brasil, de acordo com a resolução 506/2008, é possível a utilização da faixa de 900 Mhz sem licença. Esta faixa de freqüências tem sido empregada para aplicações com visada parcial ou até sem visada. No entanto seu emprego deve ser cuidadoso para atender a legislação..

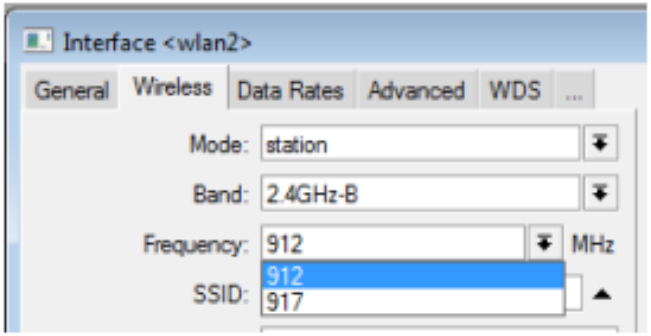
Faixas permitidas conf resol 506:

Freqüência (Mhz)	902 – 907.5	915 - 928
Largura faixa	5.5 Mhz	13 Mhz

Canais que o fabricante garante o funcionamento:

Canal 3 -> 922 Mhz (10Mhz, 5Mhz)
Canal 4 -> 917 Mhz (20Mhz, 10Mhz, 5 Mhz)
Canal 5 -> 912 Mhz (20Mhz, 10Mhz, 5 Mhz)
Canal 6 -> 907 Mhz (10Mhz, 5Mhz)

Na V3:



Variações possíveis no Brasil:

Canal 3 -> 922 Mhz (10Mhz, 5Mhz)
Canal 4 -> 917 Mhz (10Mhz, 5 Mhz)

802.11n

- → MIMO
- → Velocidades do 802.11n
- → Bonding do Canal
- → Agregaçãode Frames
- → Configuraçãodo cartão Wireless
- → Potência de TX para cartões N
- → Bridging transparente para links em N, utilizando MPLS/VPLS

MIMO

MIMO – Multiple Input and Multiple Output

SDM – Spatial Division Multiplexing

Streams espaciais múltiplos atravésde múltiplas antenas.

Configurações de antenas múltiplas para receber e transmitir:

- 1x1, 1x2, 1x3
- 2x2, 2x3
- 3x3

802.11n Data Rates

MCS Index	Spatial Streams	Modulation Type	Coding Rate	Data Rate Mb/s			
				20 MHz channel		40 MHz channel	
				800ns GI	400ns GI	800ns GI	400ns GI
0	1	BPSK	1/2	6.50	7.20	13.50	15.00
1	1	QPSK	1/2	13.00	14.40	27.00	30.00
2	1	QPSK	3/4	19.50	21.70	40.50	45.00
3	1	16-QAM	1/2	26.00	28.90	54.00	60.00
4	1	16-QAM	3/4	39.00	43.30	81.00	90.00
5	1	64-QAM	2/3	52.00	57.80	108.00	120.00
6	1	64-QAM	3/4	58.50	65.00	121.50	135.00
7	1	64-QAM	5/6	65.00	72.20	135.00	150.00
8	2	BPSK	1/2	13.00	14.40	27.00	30.00
9	2	QPSK	1/2	26.00	28.90	54.00	60.00
10	2	QPSK	3/4	39.00	43.30	81.00	90.00
11	2	16-QAM	1/2	52.00	57.80	108.00	120.00
12	2	16-QAM	3/4	78.00	86.70	162.00	180.00
13	2	64-QAM	2/3	104.00	115.60	216.00	240.00
14	2	64-QAM	3/4	117.00	130.00	243.00	270.00
15	2	64-QAM	5/6	130.00	144.40	270.00	300.00

Bonding dos Canais 2 x 20 Mhz

- → Adiciona mais 20 Mhz ao canal existente
- → O canal é colocado abaixo ou acima da freqüência principal
- → É compatível com clientes legados de 20 Mhz
  - → Conexão feita no canal principal
- → Permite utilizar taxas mais altas

Agregação de Frames

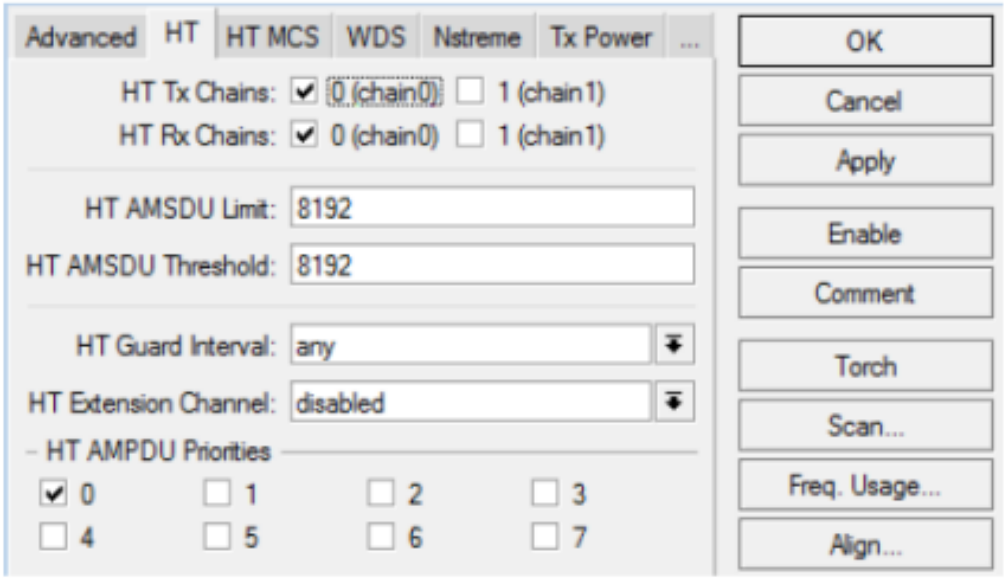
→ Combinando múltiplos frames de dados em um simples frame - diminui o overhead

→ Agregação de unidades de Serviço de dados MAC - MAC Protocol Data Units (AMPDU)

- → Usa Acknowledgement em bloco
- → Pode aumentara a latência, por default habilitado somente para tráfego de melhor esforço

→ Enviando e recebendo AMSDU-s pode aumentar o uso de processamento

Configurações



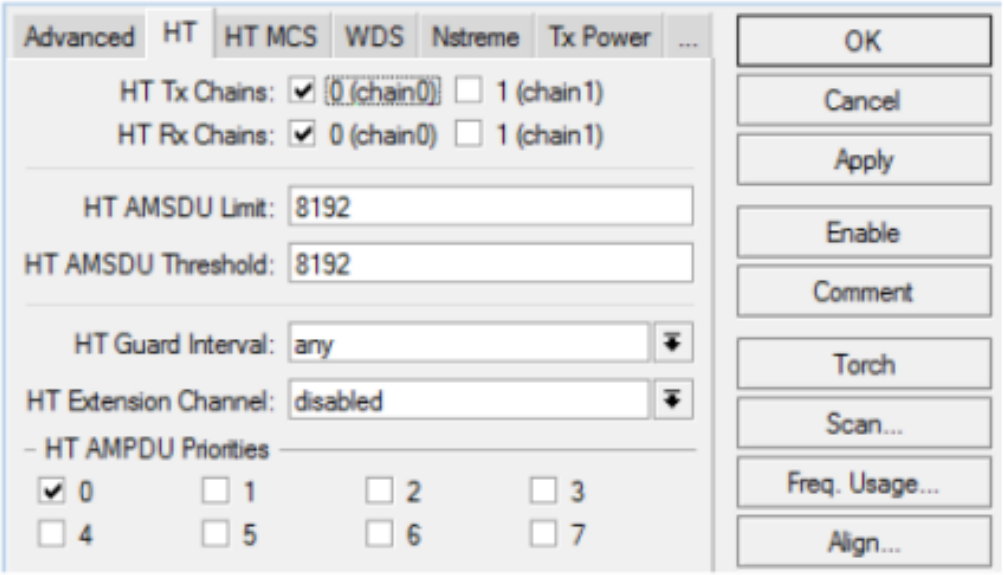
Ht-TxChains/Ht-RxChains: Qual conector da antena usar para receber e transmir

→ a configuração de antenna-mode é ignorada para cartões N.

ht-amsdu-limit: Máximo AMSDU que o dispositivo pode preparar

ht-amsdu-threshold: máximo tamanho de frame que é permitido incluir em AMSDU.

Configurações



ht-guard-interval: intervalo de guarda.

→ any: longo ou curto, dependendo da velocidade de transmissão

→ long: intervalo de guarda longo

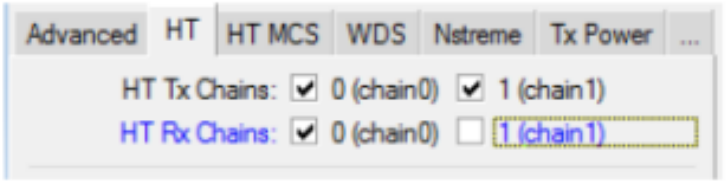
ht-extension-channel: se será usado a extensão adicional de 20 Mhz.

→ below: abaixo do canal principal

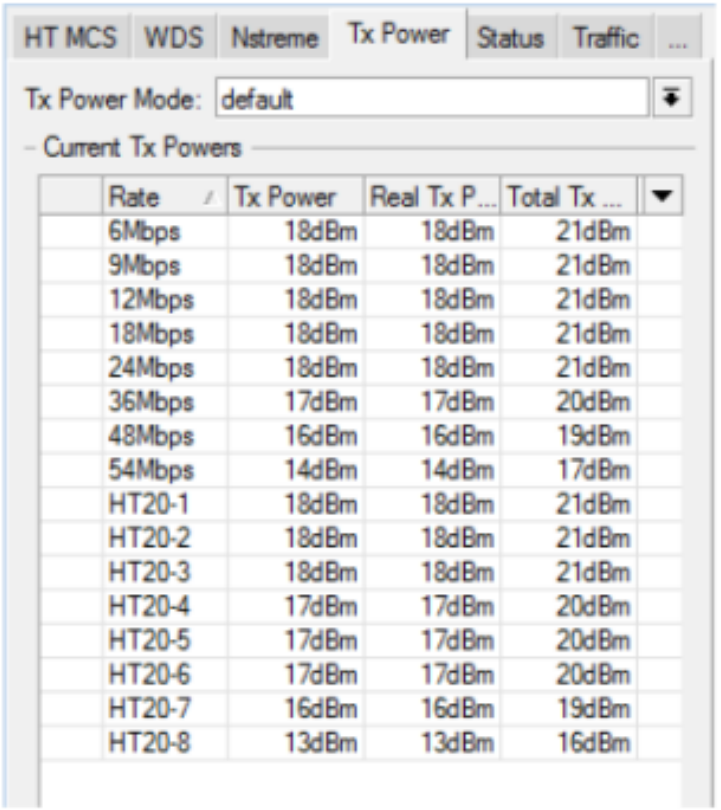
→ above: acima do canal principal

ht-ampdu-priorities:prioridades do frame para o qual AMPDU sending deve ser negociado e utilizado (agregando frames e usando acknowleddgment em bloco)

Configurações



Quando utilizando dois canais ao mesmo tempo, a potência de transmissão é dobrada (incrementada em 3 dB)



Rate	Tx Power	Real Tx P...	Total Tx ...
6Mbps	18dBm	18dBm	21dBm
9Mbps	18dBm	18dBm	21dBm
12Mbps	18dBm	18dBm	21dBm
18Mbps	18dBm	18dBm	21dBm
24Mbps	18dBm	18dBm	21dBm
36Mbps	17dBm	17dBm	20dBm
48Mbps	16dBm	16dBm	19dBm
54Mbps	14dBm	14dBm	17dBm
HT20-1	18dBm	18dBm	21dBm
HT20-2	18dBm	18dBm	21dBm
HT20-3	18dBm	18dBm	21dBm
HT20-4	17dBm	17dBm	20dBm
HT20-5	17dBm	17dBm	20dBm
HT20-6	17dBm	17dBm	20dBm
HT20-7	16dBm	16dBm	19dBm
HT20-8	13dBm	13dBm	16dBm

Configurando bridge transparente em enlaces N

→ WDS não suporta a agregação de frames e portanto não provê a velocidade total da tecnologia N.

→ EoIP incrementa overhead.

→ Para fazer bridge transparente com velocidades maiores e menos overhead em enlaces N devemos utilizar MPLS/VPLS

Configurando bridge transparente em enlaces N

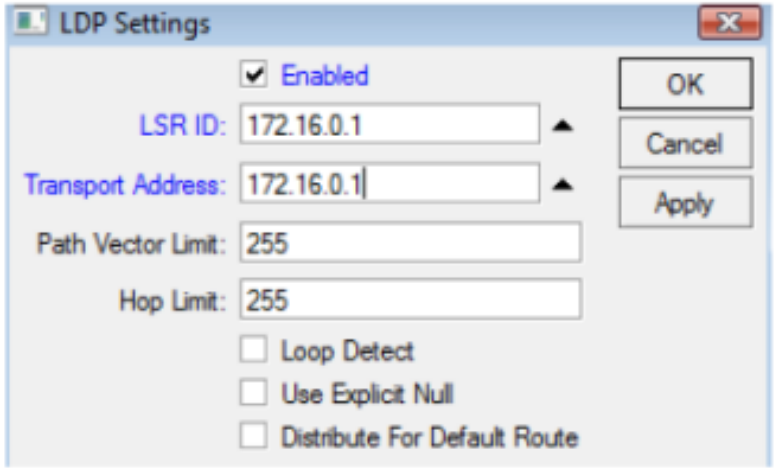
→ Estabelecer um link AP <-> Station, configurando dois IP's quaisquer.

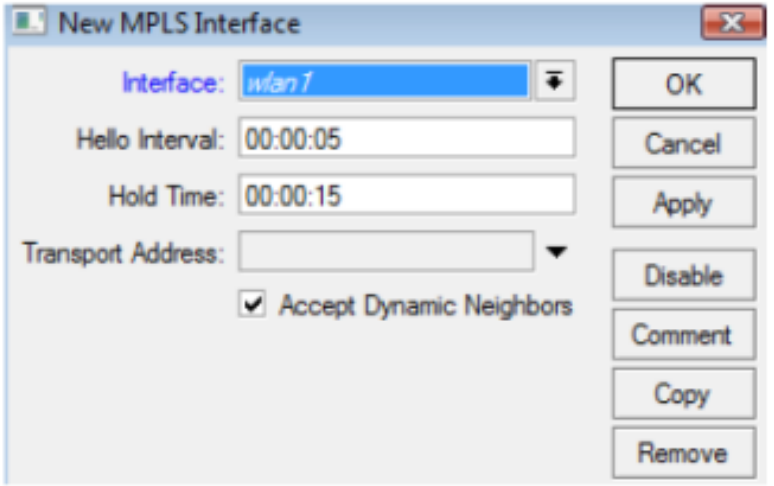
Ex. 172.16.0.1/30 e 172.16.0.2/30

→ Em ambos os lados:

→ Habilitaro LDP (Label Distribution Protocol)

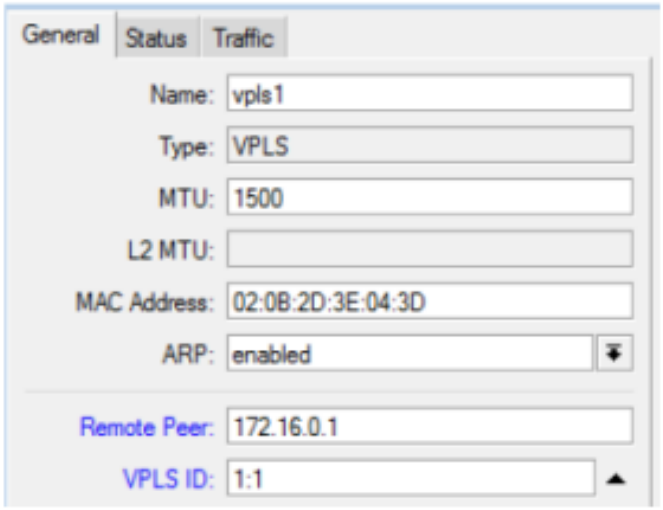
→ Adicionar a Interface wlan1

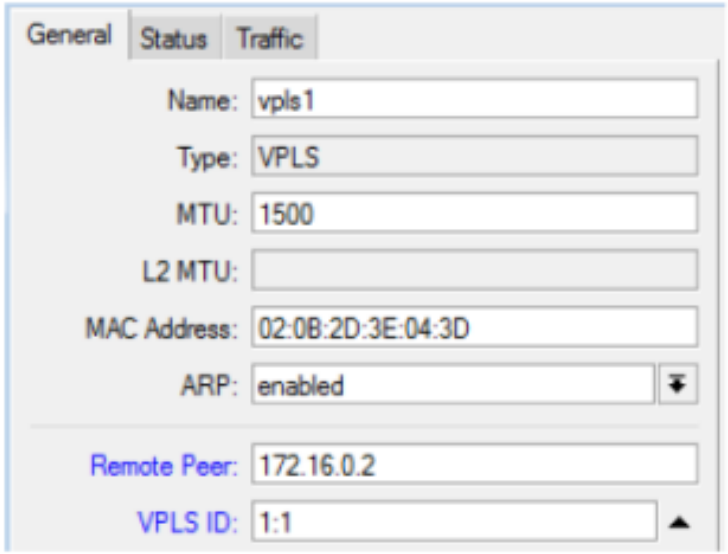




Configurando bridge transparente em enlaces N

→ Configurando o túnel VPLS em ambas as pontas





→ Criar uma Bridge entre a interface VPLS e a ethernet de saida do link

→Confirme o status do LDP e do túnel VPLS

→ mpls ld neighbor print

→ mpls forwarding-table print

→ interface vpls monitor vpls1 once

VPLS bridge e fragmentação

→ O túnel VPLS incrementao tamanho do pacote

→ Se este tamanho excede o MPLS MTU da interface de saída, é feita a fragmentação

→ Se a interface ethernet suportar um MPLS MTU de 1526 ou maior, a fragmentação pode ser evitada incrementando o MPLS MTU.

→ Uma lista das RouterBoards que suportamMPLS MTU maiores pode ser encontrada no wiki da Mikrotik

http://wiki.mikrotik.com/wiki/Manual:Maximum_Transmission_Unit_on_RouterBoards

Outdoor Setup

(Segundo Recomendações da Mikrotik Latvia)

→ Teste cada canal separadamente, antes de usar ambos ao mesmo tempo.

→ Para operação em dois canais usar polarizações diferentes para cada canal.

→ Quando utilizar antenas de polarização dupla, a isolação recomendada da antena, é no mínimo 25 dB.

Laboratório de Enlaces N

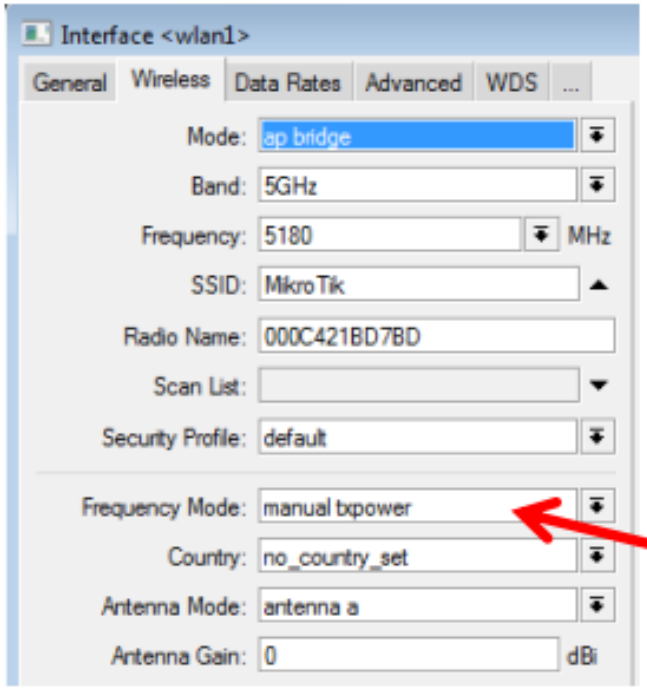
→ Estabeleça um link N com seu vizinho

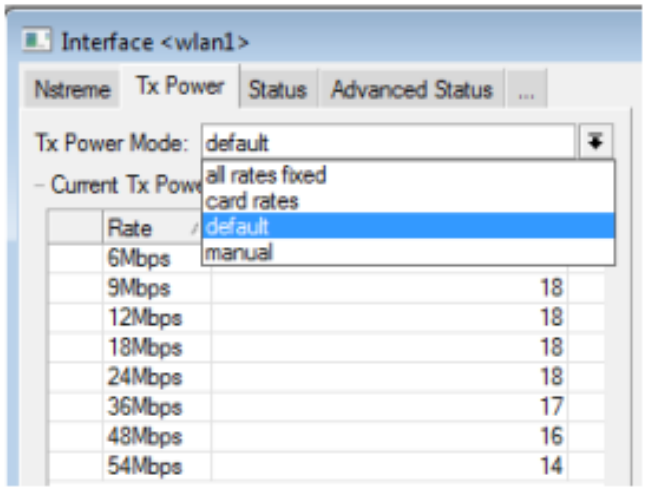
→ Teste a performance com um e dois canais

→ Crie uma bridge transparente utilizando VPLS

Configurações da camada Física
Potências

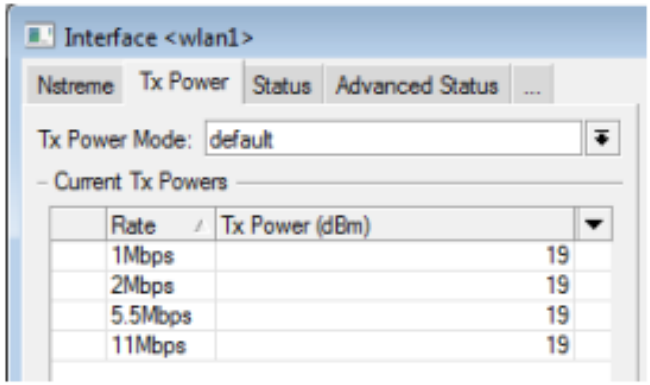
Configurações da camada Física - Potências

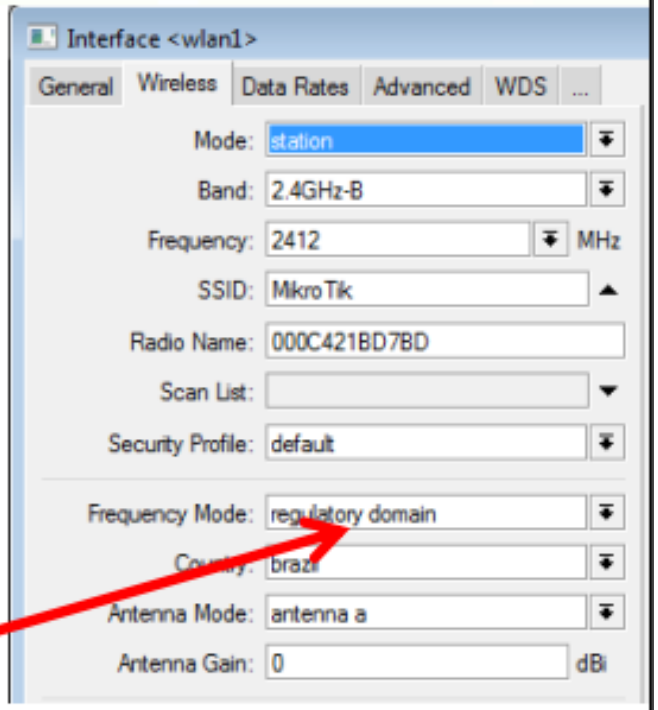




- **default:** não interfere na potencia original do cartão
- **card rates:** fixa mas respeita as variações das taxas para diferentes velocidades
- **all rates fixed:** fixa em um valor para todas velocidades
- **manual:** permite ajustar potencias diferentes para cada velocidade

Configurações da camada Física - Potências





Quando a opção **"regulatory domain"** está sendo utilizada, somente as frequencias permitidas no país selecionado em **"Country"** estarão disponíveis. Alem disso o Mikrotik Ajustará a potencia do rádio para atender a regulamentação do país, levando em conta o valor em dBi informado no campo **"Antenna Gain"**

OBS: Até a versão 3.11 tal ajuste não era feito corretamente para o Brasil.

Configurações da camada Física seleção de antenas

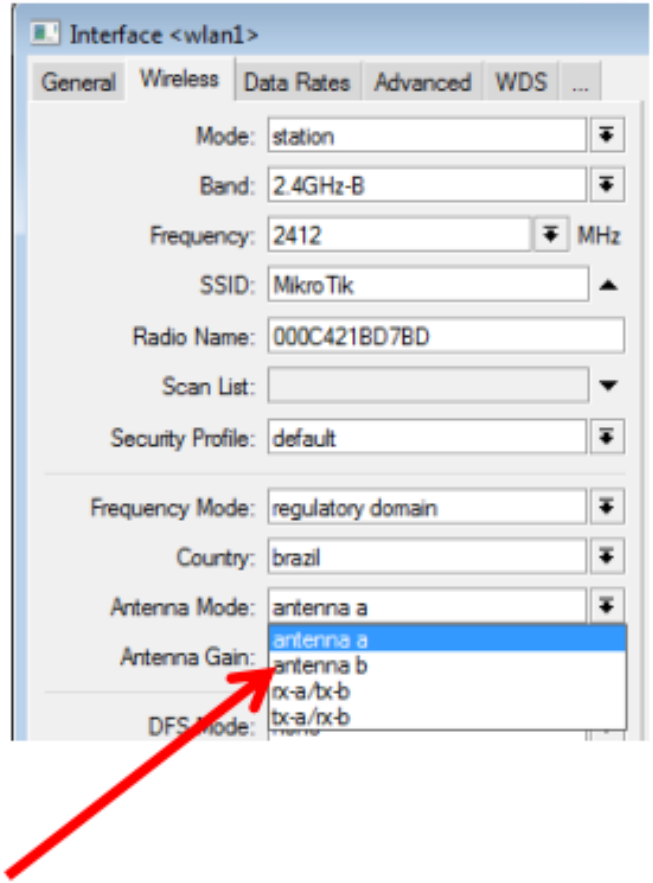
Em cartões de rádio que tem duas saidas para Antenas é possível uma ou outra.

→Antena a: utiliza a antena a (main) para tx e rx

→Antena b: utiliza a antena b (aux) para tx e rx

→ rx-a/tx/b: recepção em a e transmissão em b

→ tx-a/rx-b: transmissão em a e recepção em b



Configurações da camada Física
seleção de antenas

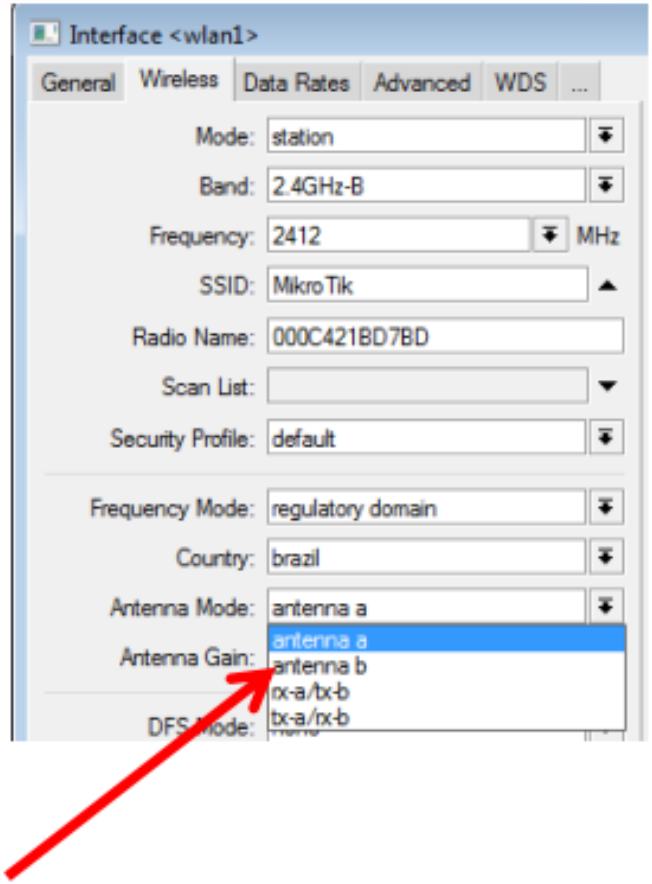
Em cartões de rádio que tem duas saidas para Antenas é possível uma ou outra.

→Antena a: utiliza a antena a (main) para tx e rx

→Antena b: utiliza a antena b (aux) para tx e rx

→rx-a/tx/b: recepção em a e transmissão em b

→tx-a/rx-b: transmissão em a e recepção em b

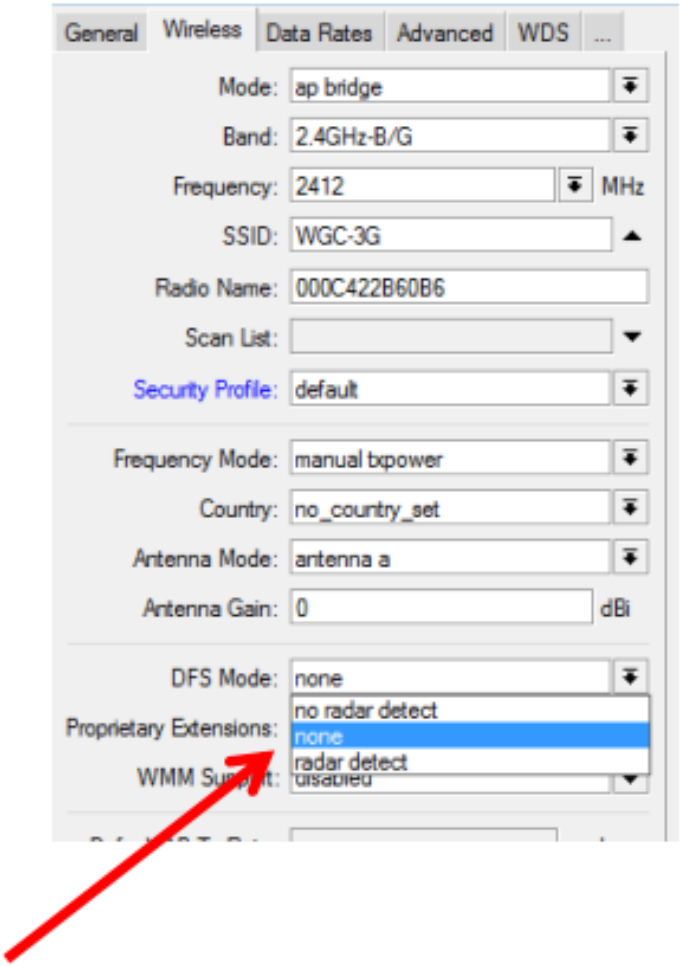


Configurações da camada Física
DFS

→ **no radar detect:** escaneia o meio e escolhe o canal em que for encontrado o menor número de redes

→ **radar detect**: escaneia o meio e espera 1 minuto para entrar em operação no canal escolhido se não for detectada a ocupação nesse canal.

O modo DFS (Seleção Dinâmica de Frequência) é obrigatório para o Brasil nas faixas de 5250-5350 e 5350-5725



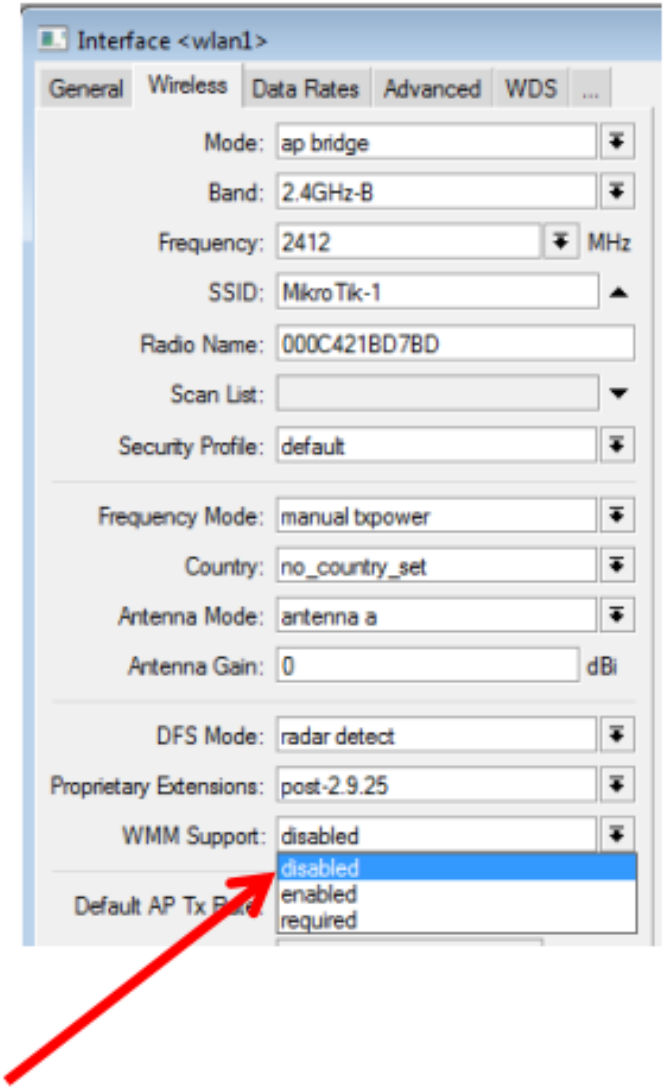
Configurações da camada Física
Prop. Extensions e WMM support

→ **Proprietary Extensions:** Opção com a única finalidade de dar compatibilidade ao Mikrotik com chipsets Centrino (post-2.9.25)

→ **WMM support**: QoS no meio físico (802.11e)

→ **enabled:** permite que o outro dispositivo use wmm

→ **required:** requer que o outro dispositio use wmm



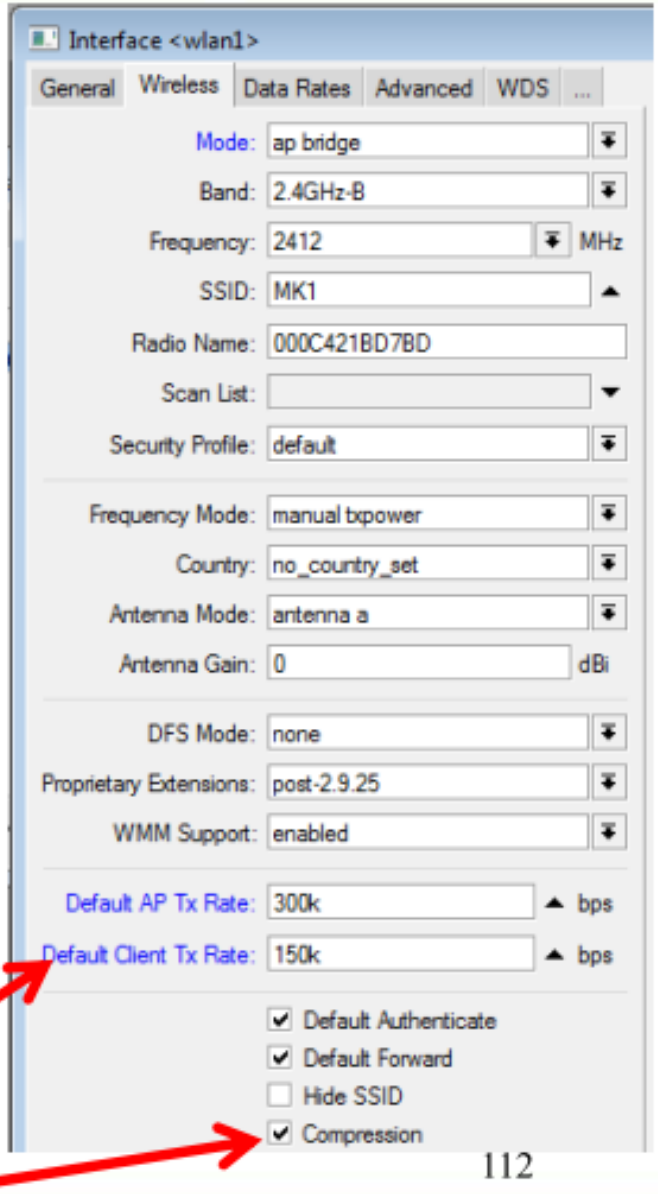
Configurações da camada Física
AP e Client Tx Rate / Compression

→ **Default AP Tx Rate:** Taxa máxima em bps que o AP pode transmitir para cada um de seus clientes. Funciona para qualquer tipo de cliente

→ **Default Client Tx Rate:** Taxa máxima em bps que o Cliente pode transmitir ao AP. Só funciona para clientes Mikrotik.

→ **Compression:** Recurso de compressão em Hardware disponível no Chipset Atheros. Melhora desempenho se o cliente possuir esse recurso. Não afeta clientes que não possuam.

(Recurso incompatível com criptografia)



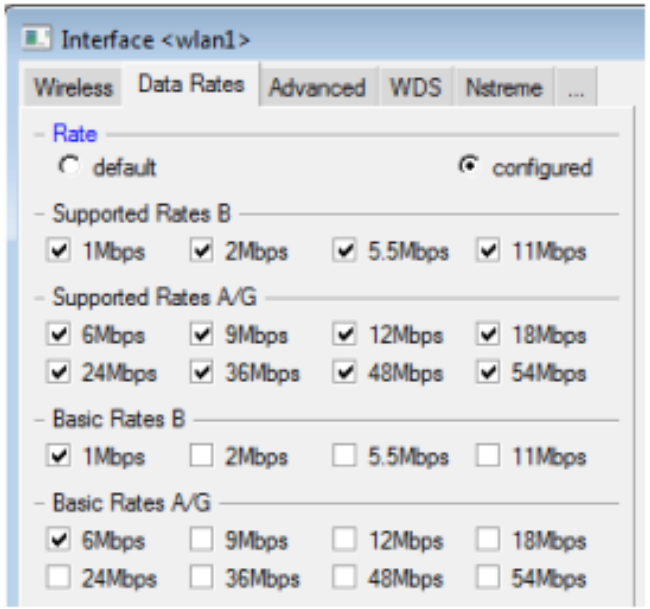
Configurações da camada Física
Data Rates

A velocidade em uma rede Wireless é definida pela modulação que os dispositivos conseguem trabalhar.

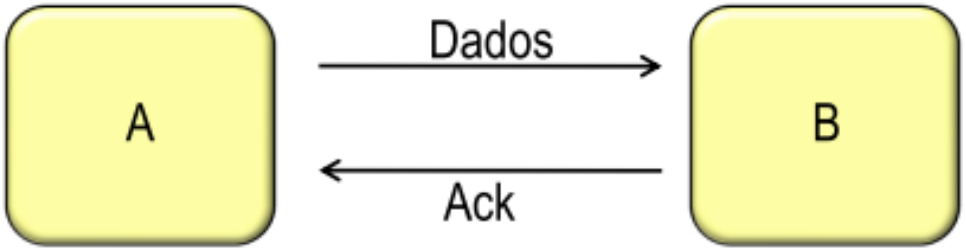
→ **Supported Rates:** São as velocidades de tráfego de dados entre AP's e clientes .

→ **Basic Rates:** São as velocidades que os dispositivos se comunicam independentemente do tráfego de dados em si (beacons, mensagens de sincronismo, etc)

Embora o próprio manual do Mikrotik aconselhe deixar as velocidades em seu default, melhores performances são conseguidas evitando trabalhar em baixas velocidades



Configurações da camada Física
Ack Timeout



O Ack Timeout é o tempo que um dispositivo Wireless espera pelo pacote de Ack que deve ser enviado para confirmar toda transmissão Wireless.

→**dynamic :** O Mikrotik calcula dinamicamente o Ack de cada cliente mandando de tempos em tempos sucessivos pacotes com Ack timeouts diferentes e analisando as respostas.

→**indoors:** valor constante para redes indoor.

→ pode ser fixado manualmente digitando-se no campo.

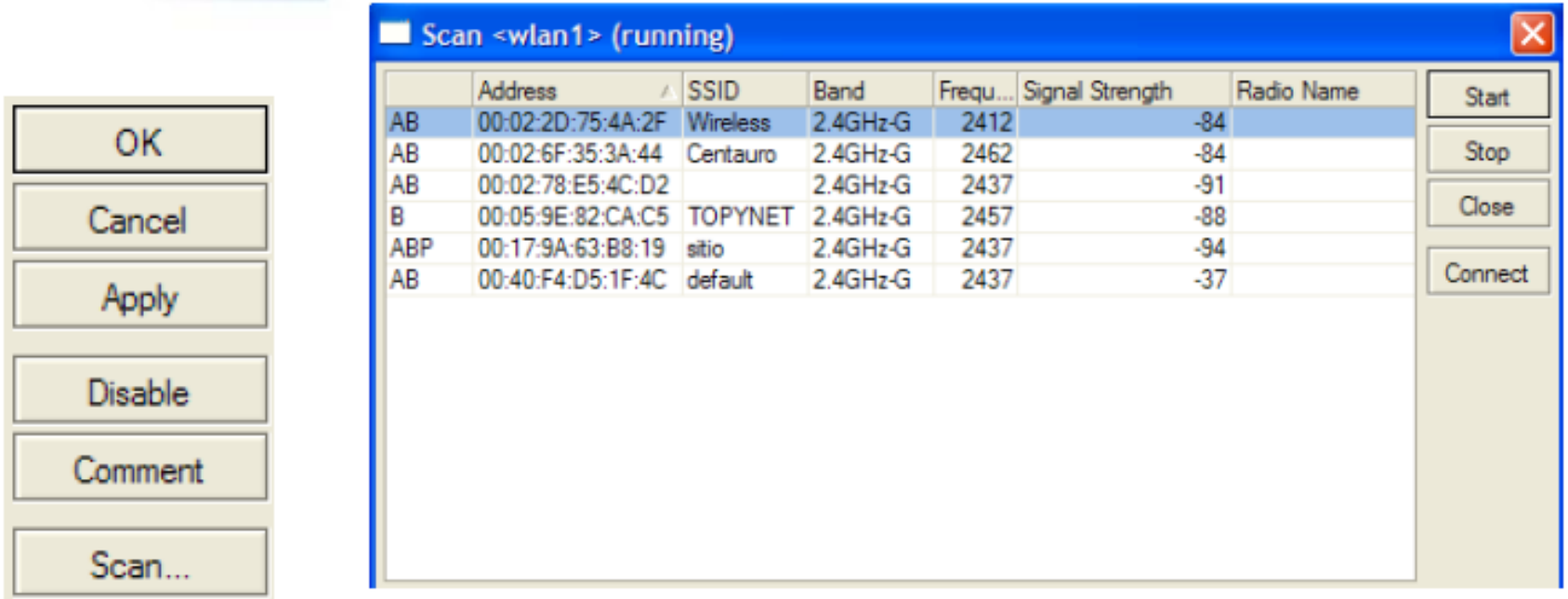
Configurações da camada Física
Valores referenciais para Ack Timeout

range	ack-timeout		
	5GHz	5GHz-turbo	2.4GHz-G
0km	default	default	default
5km	52	30	62
10km	85	48	96
15km	121	67	133
20km	160	89	174
25km	203	111	219
30km	249	137	368
35km	298	168	320
40km	350	190	375
45km	405	-	-

OBS: Valores orientativos. Valores ideais podem estar em uma faixa de +- 15 microsegundos

Ferramentas de Site Survey

Interface Wireless / Geral / Scan



Escaneia o meio (causa queda das conexões estabelecidas)

A → Ativa

B → BSS

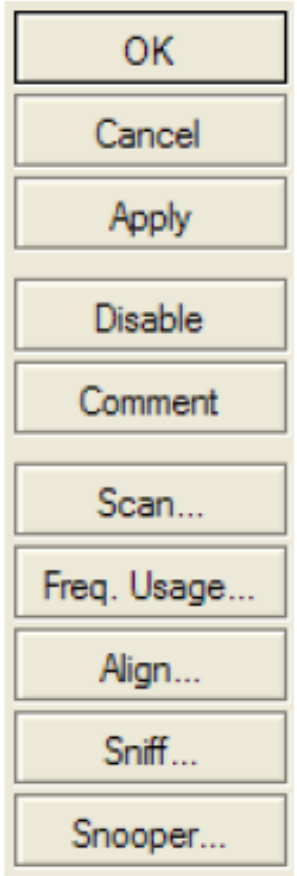
P → Protegida

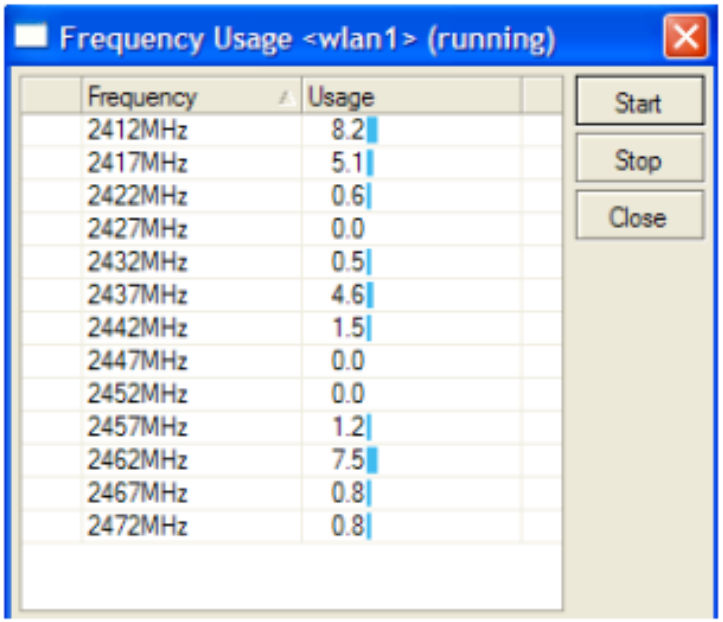
R → rede Mikrotik

N → Nstreme

Na linha de comando pode ser acessada em /interface/wireless/scan – wlan1

Interface Wireless / Geral / Uso de frequencias





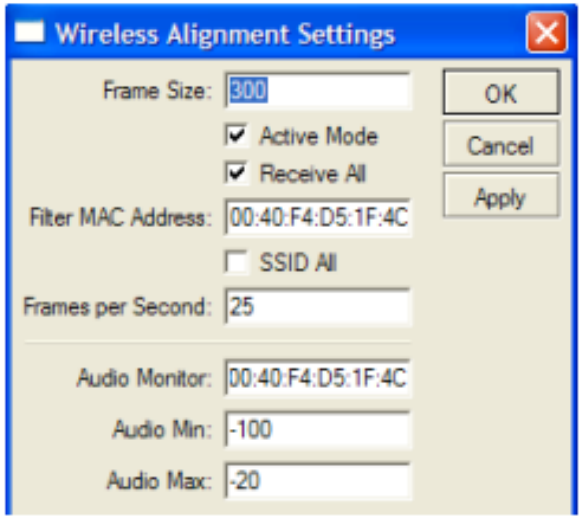
Mostra o uso das frequencias em todo o espectro, para site survey (causa queda das conexões estabelecidas)

Na linha de comando pode ser acessada em /interface/wireless/frequency-monitor wlan1

Interface Wireless / Geral / Alinhamento

Alignment <wlan1> (running)

	Address	SSID	Rx Quality	Avg. Rx Quality	Last Rx	Tx Quality	Last Tx	Correct
A	00:40:F4:D5:1F:4C	default	-45	-44	0.08	0	0.00	0%



Ferramenta de alinhamento com sinal sonoro
(Colocar o MAC do AP remoto no campo Filter e campo Audio)

Rx Quality – Potencia (dBm) do último pacote recebido

Avg. Rx Quality – Potencia média dos pacotes recebidos.

Last Rx – tempo em segundos do último pacote foi recebido

Tx Quality – Potencia do último pacote transmitido

Last Rx – tempo em segundos do último pacote transmitido

Correct – número de pacotes recebidos sem erro

OBS: Filtrar MAC do PtP

Interface Wireless / Geral / Sniffer

Sniffed Wireless Packets

Time	Interfa...	Band	Frequ...	Signal ...	Rate	Dst.	Src.	Type
1.123s	wlan1	2.4GHz-G	2437...	-48dBm	1Mbps	FF:FF:FF:FF:FF:FF	00:40:F4:D5:1F:4C	beacon
1.124s	wlan1	2.4GHz-G	2437...	-59dBm	11Mbps	00:40:F4:D5:1F:4C	00:02:2D:0C:AE:55	data
1.155s	wlan1	2.4GHz-G	2437...	-59dBm	2Mbps	00:40:F4:D5:1F:4C	00:02:2D:0C:AE:55	data null
1.156s	wlan1	2.4GHz-G	2437...	-60dBm	2Mbps	00:40:F4:D5:1F:4C	00:02:2D:0C:AE:55	data null
1.159s	wlan1	2.4GHz-G	2437...	-59dBm	2Mbps	00:40:F4:D5:1F:4C	00:02:2D:0C:AE:55	data null
1.164s	wlan1	2.4GHz-G	2437...	-59dBm	2Mbps	00:40:F4:D5:1F:4C	00:02:2D:0C:AE:55	data null
1.188s	wlan1	2.4GHz-G	2437...	-63dBm	2Mbps	FF:FF:FF:FF:FF:FF	00:02:2D:0C:AE:55	probe request
1.209s	wlan1	2.4GHz-G	2437...	-62dBm	2Mbps	FF:FF:FF:FF:FF:FF	00:02:2D:0C:AE:55	probe request
1.230s	wlan1	2.4GHz-G	2437...	-23dBm	1Mbps	FF:FF:FF:FF:FF:FF	00:40:F4:D5:1F:4C	beacon
1.234s	wlan1	2.4GHz-G	2442...	-62dBm	2Mbps	FF:FF:FF:FF:FF:FF	00:02:2D:0C:AE:55	probe request
1.256s	wlan1	2.4GHz-G	2442...	-65dBm	2Mbps	FF:FF:FF:FF:FF:FF	00:02:2D:0C:AE:55	probe request
1.263s	wlan1	2.4GHz-G	2442...	-64dBm	2Mbps	00:40:F4:D5:1F:4C	00:02:2D:0C:AE:55	ps poll
1.328s	wlan1	2.4GHz-G	2442...	-46dBm	1Mbps	FF:FF:FF:FF:FF:FF	00:40:F4:D5:1F:4C	beacon
1.435s	wlan1	2.4GHz-G	2442...	-46dBm	1Mbps	FF:FF:FF:FF:FF:FF	00:40:F4:D5:1F:4C	beacon
1.878s	wlan1	2.4GHz-G	2457...	-95dBm	1Mbps	FF:FF:FF:FF:FF:FF	00:05:9E:82:CA:C5	beacon
1.980s	wlan1	2.4GHz-G	2457...	-93dBm	1Mbps	FF:FF:FF:FF:FF:FF	00:05:9E:82:CA:C5	beacon
2.100s	wlan1	2.4GHz-G	2462...	-86dBm	2Mbps	FF:FF:FF:FF:FF:FF	00:02:6F:35:3A:44	beacon
2.160s	wlan1	2.4GHz-G	2462...	-89dBm	2Mbps	00:02:78:E2:22:9B	00:02:6F:35:3A:44	data
2.193s	wlan1	2.4GHz-G	2462...	-86dBm	2Mbps	00:06:25:02:C3:94	00:02:6F:35:3A:44	probe response
2.194s	wlan1	2.4GHz-G	2462...	-87dBm	2Mbps	00:06:25:02:C3:94	00:02:6F:35:3A:44	probe response
2.199s	wlan1	2.4GHz-G	2462...	-86dBm	2Mbps	00:06:25:02:C3:94	00:02:6F:35:3A:44	probe response
2.211s	wlan1	2.4GHz-G	2462...	-90dBm	2Mbps	FF:FF:FF:FF:FF:FF	00:02:6F:35:3A:44	beacon
2.215s	wlan1	2.4GHz-G	2462...	-87dBm	2Mbps	FF:FF:FF:FF:FF:FF	00:02:6F:35:3A:44	data
2.216s	wlan1	2.4GHz-G	2462...	-86dBm	2Mbps	FF:FF:FF:FF:FF:FF	00:02:6F:35:3A:44	data
2.217s	wlan1	2.4GHz-G	2462...	-86dBm	2Mbps	FF:FF:FF:FF:FF:FF	00:02:6F:35:3A:44	data

Ferramenta para sniffar o ambiente Wireless captando e decifrando pacotes
Muito útil para detectar ataques do tipo deauth attack e monkey jack
Pode ser arquivado no próprio Mikrotik ou passado por streaming para outro sevidor com o protocolo TZSP
Na linha de comando habilita-se em / interface wireless sniffer sniff wlan1

Interface Wireless / Geral / Snooper

Snooper <wlan1> (running)

Networks | Stations

Frequency	Band	Address	SSID	Of Freq (%)	Of Traf. (%)	Bandwidth	Net...	Stations
2412MHz	2.4GHz-B/G			11.9		926.4 kbps	1	3
2412MHz	2.4GHz-B/G	00:02:2D:75:4A:2F	Wireless	11.6	97.7	926.4 kbps		3
2417MHz	2.4GHz-B/G							
2422MHz	2.4GHz-B/G							
2427MHz	2.4GHz-B/G							
2432MHz	2.4GHz-B/G							
2437MHz	2.4GHz-B/G							
2437MHz	2.4GHz-B/G	00:40:F4:D5:1F:						
2442MHz	2.4GHz-B/G							
2447MHz	2.4GHz-B/G							
2452MHz	2.4GHz-B/G							
2457MHz	2.4GHz-B/G							
2457MHz	2.4GHz-B/G	00:05:9E:82:CA:						
2462MHz	2.4GHz-B/G							
2462MHz	2.4GHz-B/G	00:02:6F:35:3A:						
2462MHz	2.4GHz-B/G	00:02:78:E5:4C:						
2467MHz	2.4GHz-B/G							

Snooper <wlan1> (running)

Networks | Stations

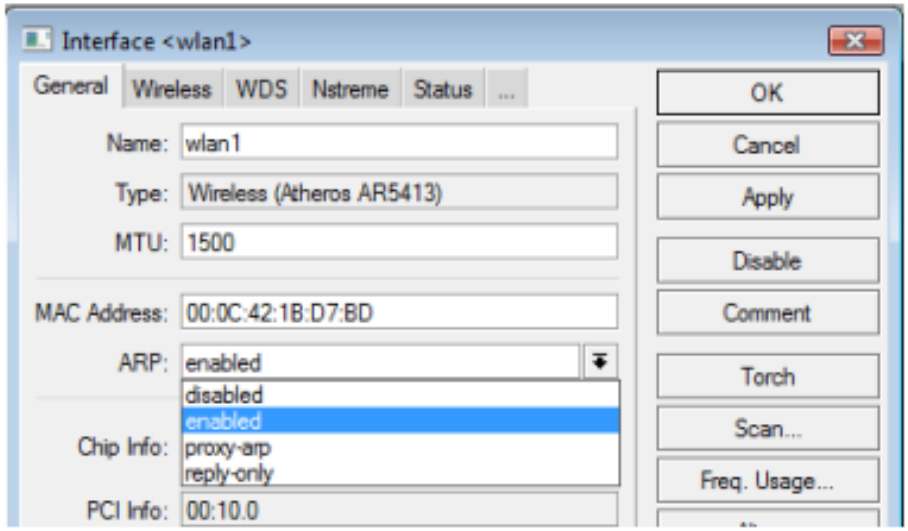
Frequency	Address	SSID	Signal	Of Freq. (%)	Of Traf. (%)	Bandwidth	Stati...
2412MHz	00:02:2D:75:4A:2F	Wireless		4.9	90.3	306.2 kbps	5
2412...	00:02:2D:53:51:98	Wireless	-93	0.0	0.0	0 bps	
2412...	00:02:2D:75:4A:2F	Wireless	-85	2.3	42.9	84.4 kbps	
2412...	00:02:78:E1:DD:65	Wireless	-88	0.1	2.2	2.8 kbps	
2412...	00:4F:62:05:8D:CF	Wireless	-84	2.3	42.9	216.2 kbps	
2412...	00:4F:62:09:20:33	Wireless	-85	0.1	2.2	2.8 kbps	
2417MHz	00:02:6F:35:94:E7		-86	0.3	21.2	9.6 kbps	
2437MHz	00:40:F4:D5:1F:4C	default		2.0	85.4	81.3 kbps	3
2437...	00:02:2D:0C:AE:55	default	-58	0.4	17.4	12.1 kbps	
2437...	00:11:F5:83:22:86	default	-35	0.0	0.0	0 bps	
2437...	00:40:F4:D5:1F:4C	default	-52	1.6	68.0	69.2 kbps	
2437MHz	00:4F:62:05:8E:B9		-87	0.0	0.0	0 bps	
2457MHz	00:05:9E:82:CA:C5	TOPYNET		0.7	53.3	5.4 kbps	1
2457...	00:05:9E:82:CA:C5	TOPYNET	-94	0.7	53.3	5.4 kbps	
2462MHz	00:02:6F:35:3A:44	Centauro		0.4	18.5	4.6 kbps	1

Com a ferramenta Snooper é possível monitorar a carga de tráfego em cada canal, por estação e por rede.

Escaneia as frequencias definidas em scan-list da interface

Configurações de Modo de Operação

Interface Wireless / Geral



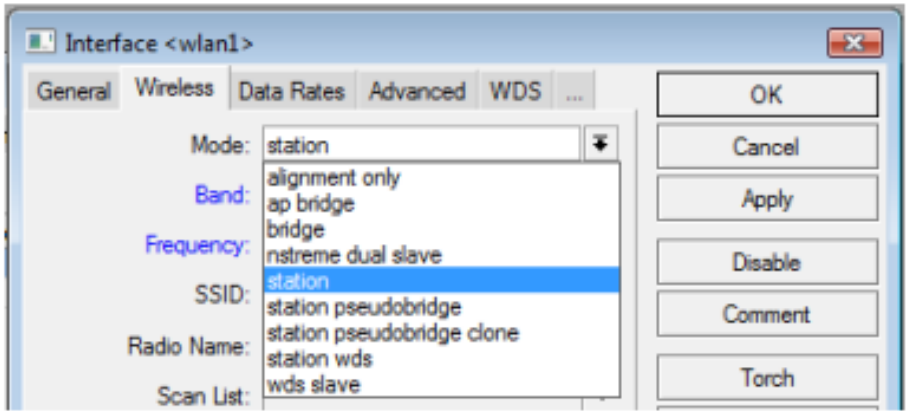
Comportamento do protocolo ARP

→ **disable:** não responde a solicitações ARP. Clientes tem de acessar por tabelas estáticas.

→ **proxy-arp:** passa o seu próprio MAC quando há uma requisição para algum host interno ao roteador.

→ **reply-only:** somente responde as requisições. Endereços de vizinhos são resolvidos estaticamente

Configurações Físicas / Modo Operação

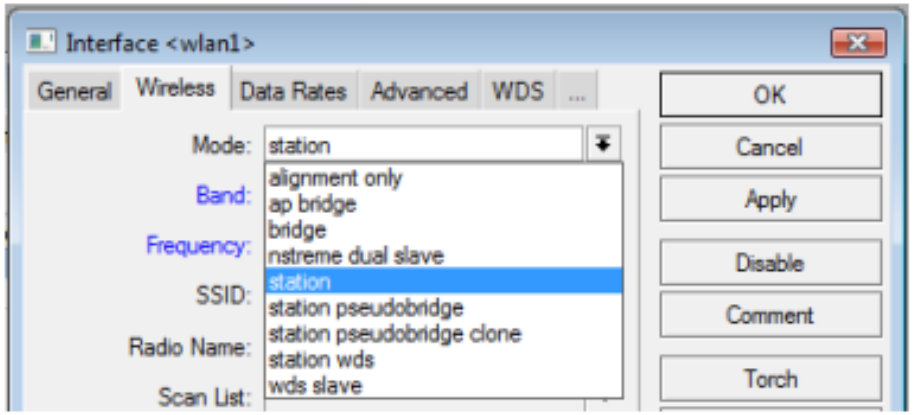


ap bridge: Modo Ponto de Acesso (AP) – repassa os MAC's do meio Wireless de forma transparente para o meio Cabeado.

bridge: Modo idêntico ao modo ap bridge, porém aceitando um cliente apenas.

station: Modo cliente de um AP – Não pode ser colocado em bridge com outras interfaces

Configurações Físicas / Modo Operação

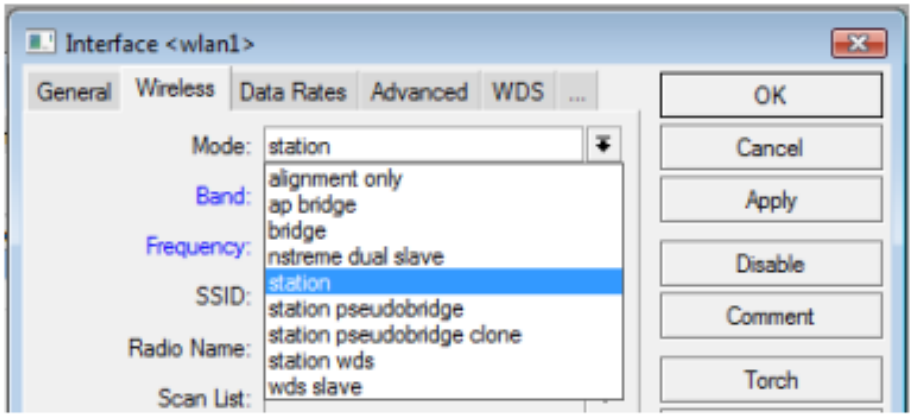


station pseudobridge: Estação que pode ser colcada em modo bridge, porém que passa ao AP sempre o seu próprio endereço MAC (uma bridge verdadeira passa os MAC's internos a ela).

station pseudobridge clone: Modo idêntico ao pseudobridge, porém que passa ao AP um MAC pré determinado do seu interior.

station wds: Modo estação, que pode ser colocado em bridge com a interface ethernet e que passa de forma transparente os MAC's internos (bridge verdadeira). É necessário que o AP esteja em modo WDS (ver tópico específico de WDS, a frente)

Configurações Físicas / Modo Operação



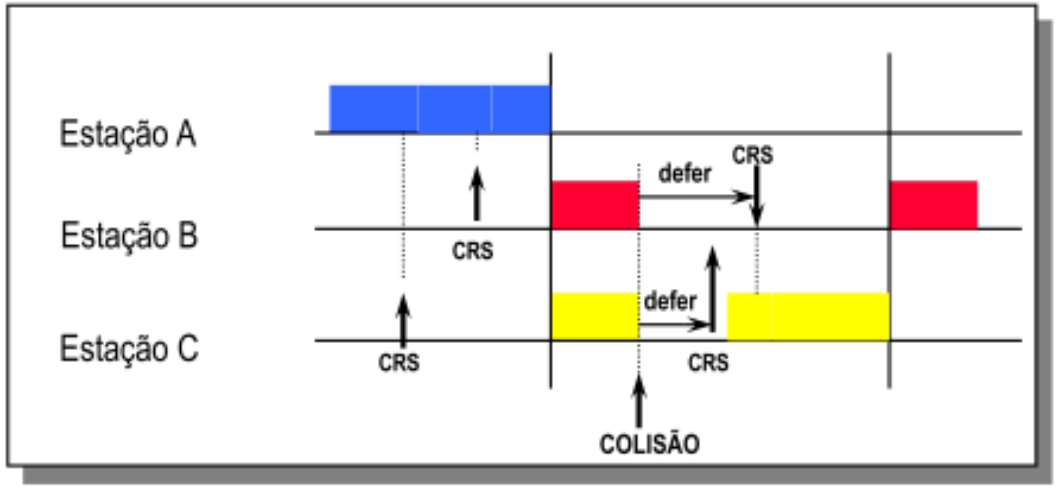
alignment only: Modo utilizado para efetuar alinhamento de antenas e monitorar sinal. Neste modo a interface Wireless "escuta" os pacotes que são mandados a ela por outros dispositivos trabalhando no mesmo canal.

wds slave: Será visto no tópico específico de WDS.

Nstreme dual slave: Visto no tópico específico de Nstreme / Nstreme Dual

Acesso ao meio físico
Protocolo Nstreme

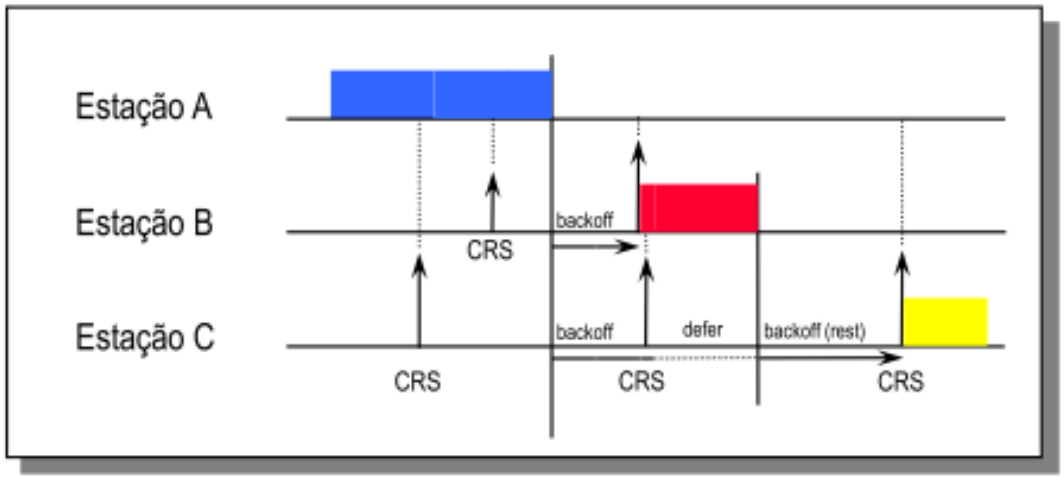
Configurações da camada Física
Como trabalha o CSMA – Carrier Sense Multiple Access



Redes Ethernet Tradicionais

Método CSMA/CD

(Collision Detection)

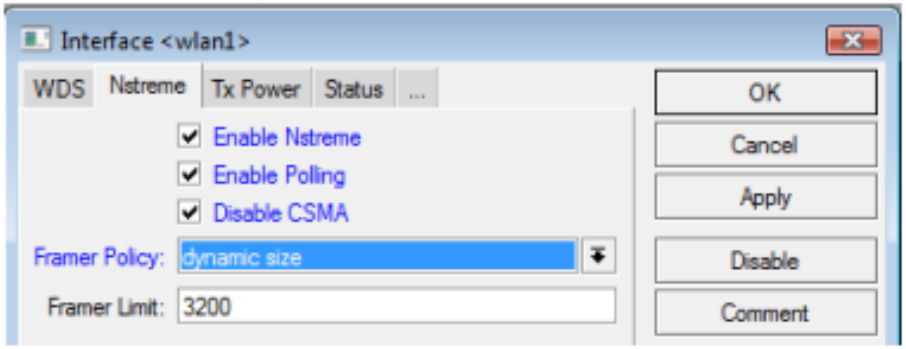


Redes Wireless 802.11

Método CSMA/CA

(Collision Avoidance)

Configurações da camada Física Nstreme



→**Enable Nstreme:** Habilita o Nstreme.

(As opções abaixo dessa só fazem sentido estando esta habilitada.)

→**Enable Polling:** Habilita o mecanismo de Polling. Recomendado

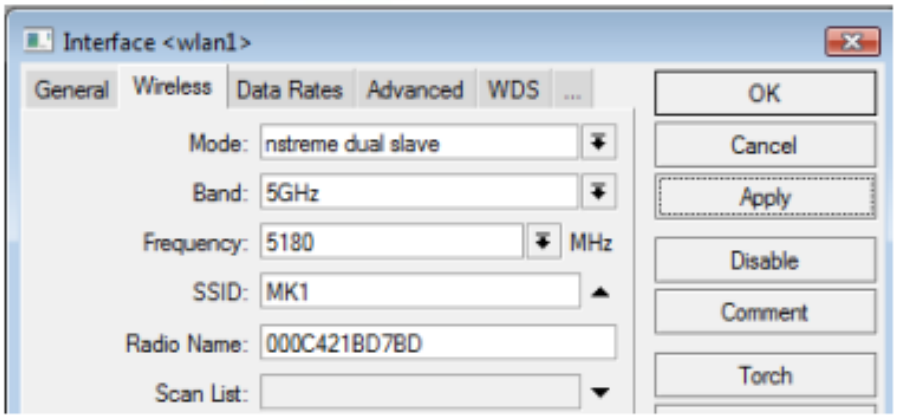
→**Disable CSMA:** Desabilita o Carrier Sense. Recomendado

→**Framer Policy:** Política em que serão agrupados os pacotes:

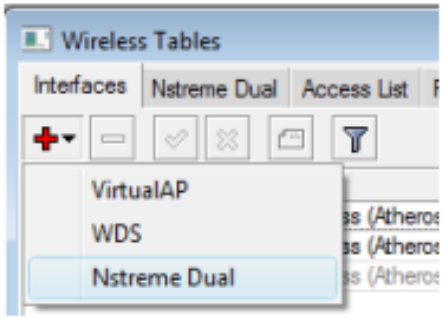
- →dynamic size: O Mikrotik determina
- →best fit: agrupa até o valor definido em Framer Limit sem fragmentar
- →exact size: agrupa até o valor definido em Framer Limit fragmentando se necessário

→ **Framer Limit:** Tamanho máximo do pacote em Bytes.

Configurações da camada Física Nstreme Dual

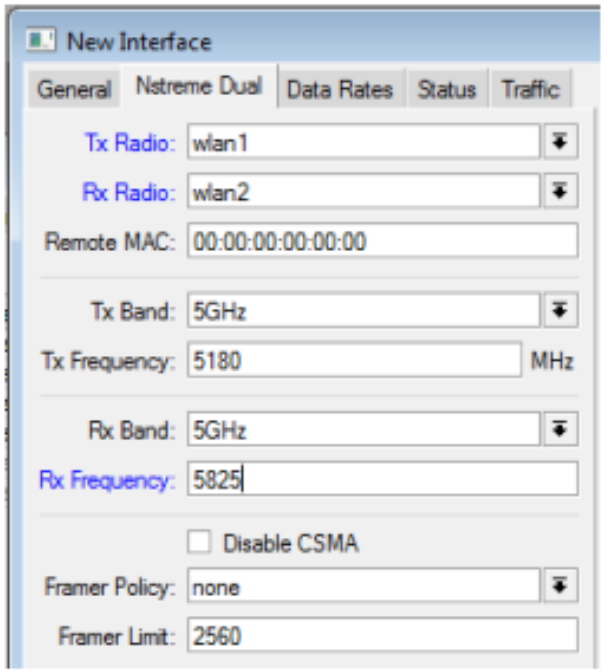


→**1 :** Passar o modo de operação das interfaces para nstreme dual slave.



→**2 :** Criar uma interface Nstreme Dual definindo quem é Tx e quem é Rx.

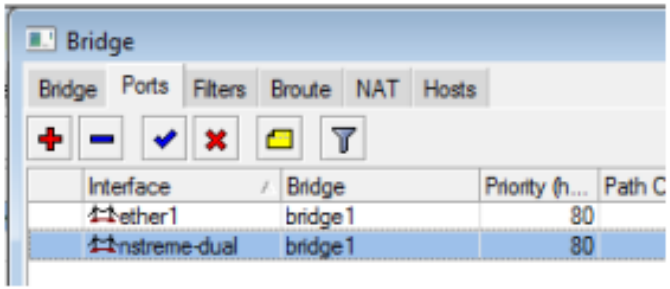
(usar canais distantes)



Configurações da camada Física
Nstreme Dual

```
[admin@MikroTik] > interface wireless nstreme-dual print
Flags: X - disabled, R - running
 0  R name="nstreme1" mtu=1500 mac-address=00:15:6D:63:05:39 arp=enabled
      disable-running-check=no tx-radio=wlan1 rx-radio=wlan2
      remote-mac=00:00:00:00:00:00 tx-band=5ghz tx-frequency=5180
      rx-band=5ghz rx-frequency=5825 disable-csma=no
```

→ **3 :** Verificar o MAC escolhido pela interface Nstreme dual e informar no lado oposto.



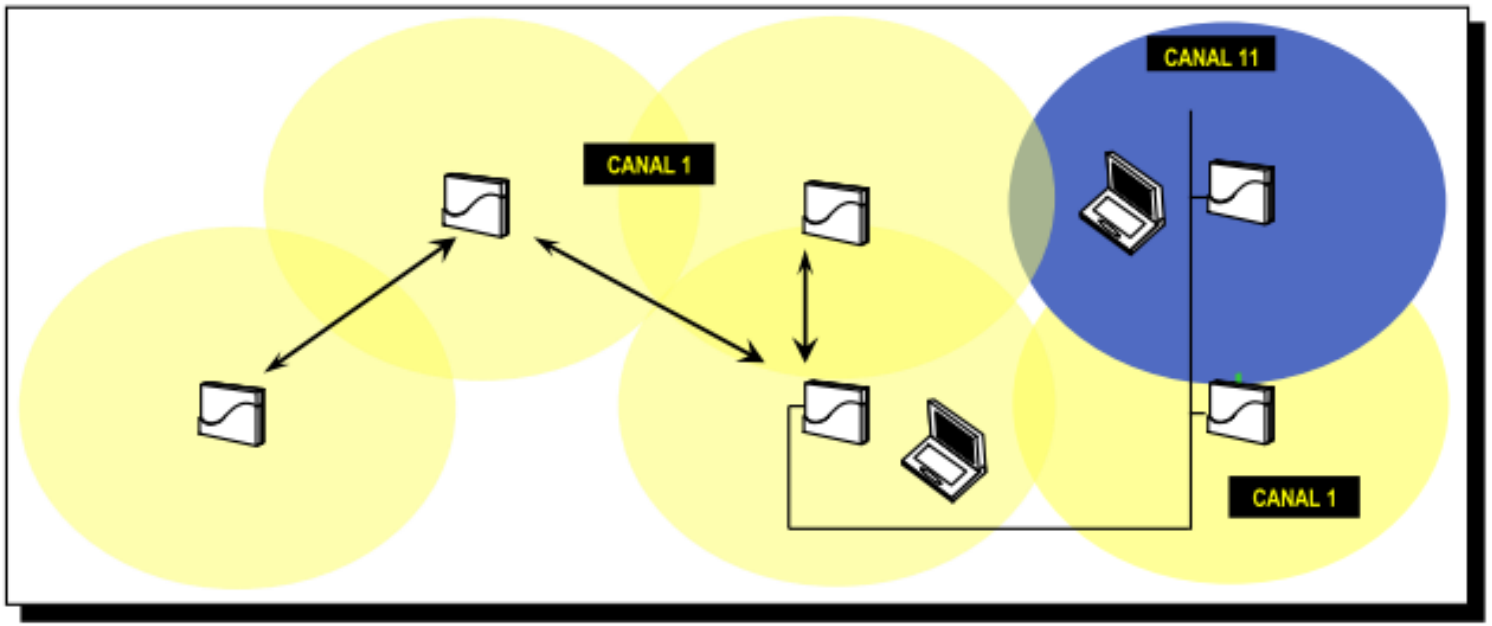
→ **4 :** Criar uma bridge entre a ethernet e a interface Nstreme Dual.

Práticas de RF recomendadas:

→ Antenas de qualidade, Polarizações invertidas, canais distantes, distância entre antenas.

WDS & Mesh WDS

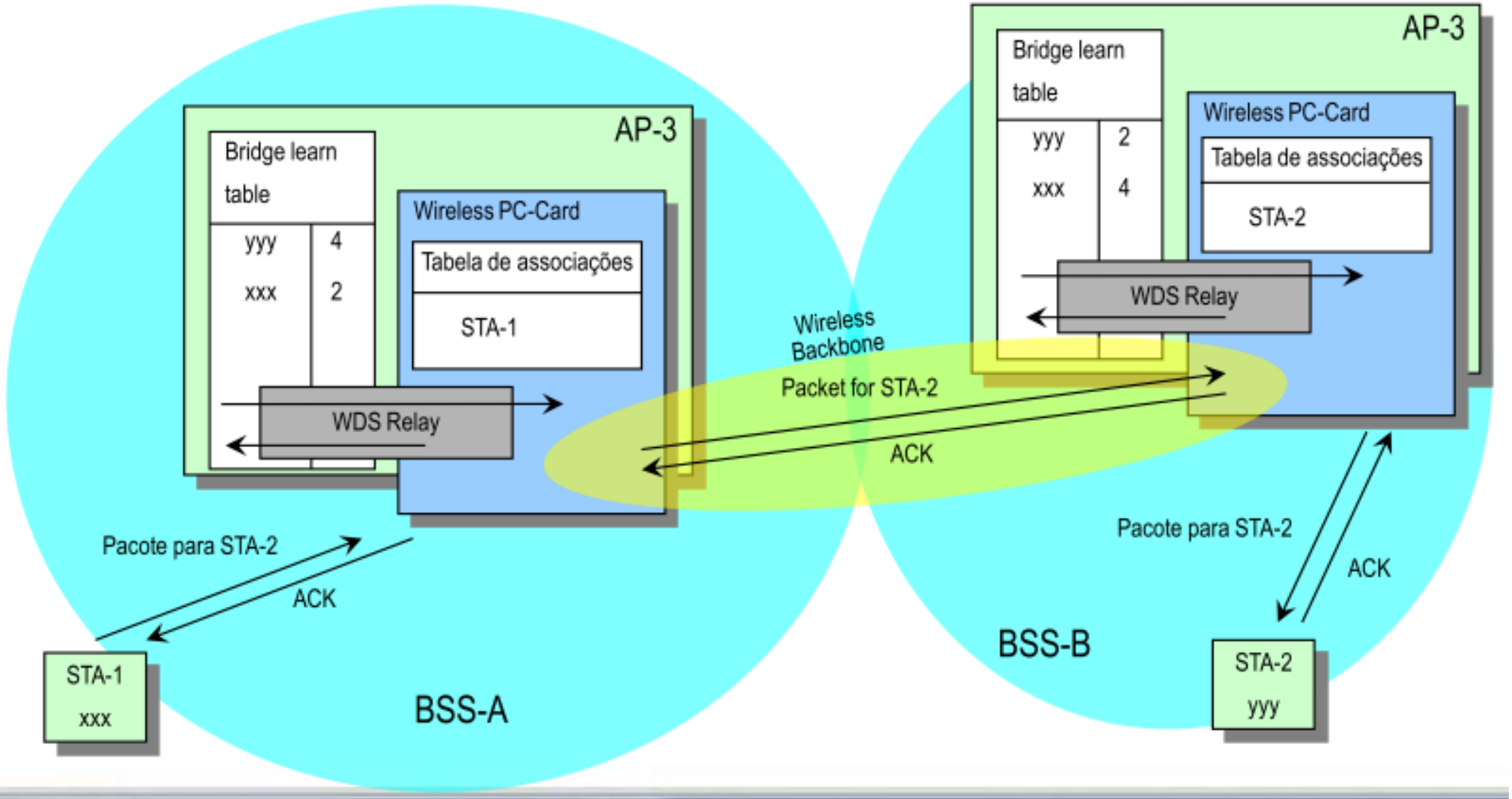
WDS : Wireless Distribution System



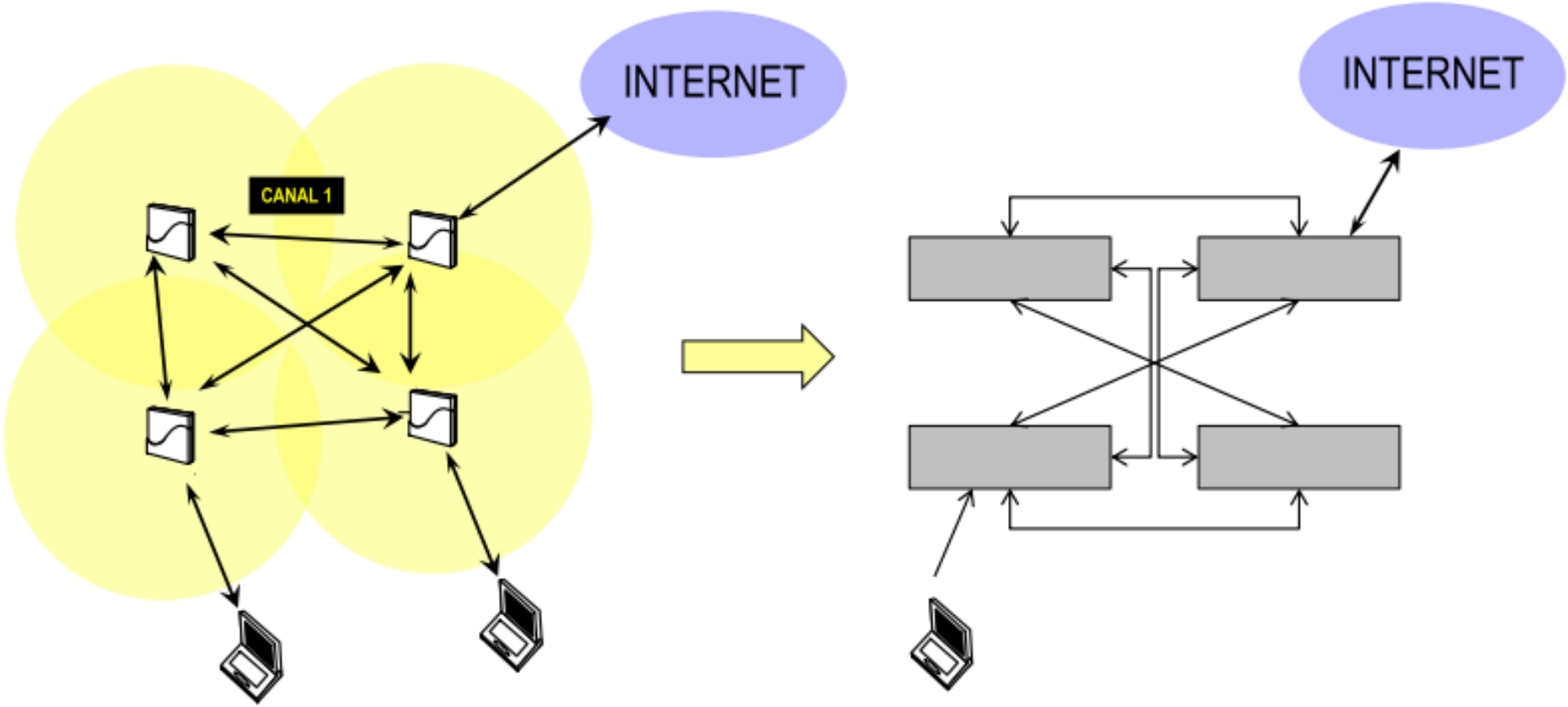
Com WDS é possível criar uma cobertura Wireless ampla e permitindo que os pacotes passem de um AP ao outro de forma transparente. Os Ap's devem ter o mesmo SSID e estarem no mesmo canal.

[MikrotikBrasil]
Routers & Wireless Systems

2 AP's com WDS

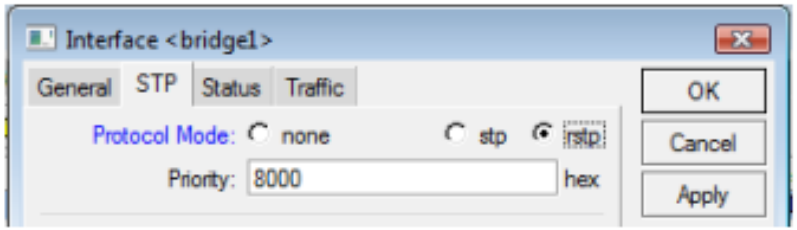


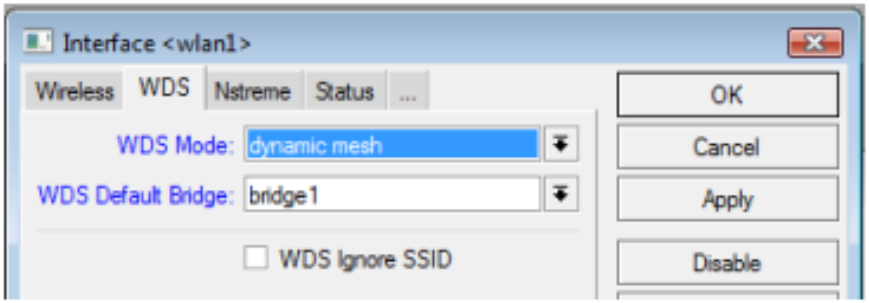
WDS : Wireless Distribution System



WDS / Mesh WDS
RSTP

Para evitar o looping na rede é necessário habilitar o protocolo STP ou RSTP. Ambos protocolos trabalham de forma semelhante sendo o RSTP mais rápido.

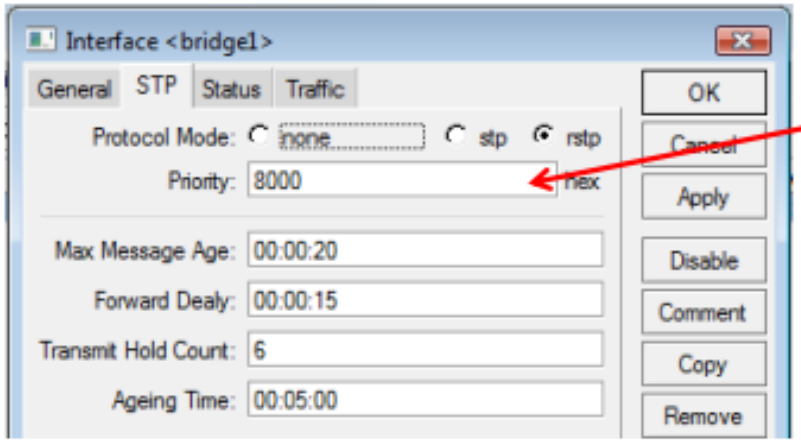




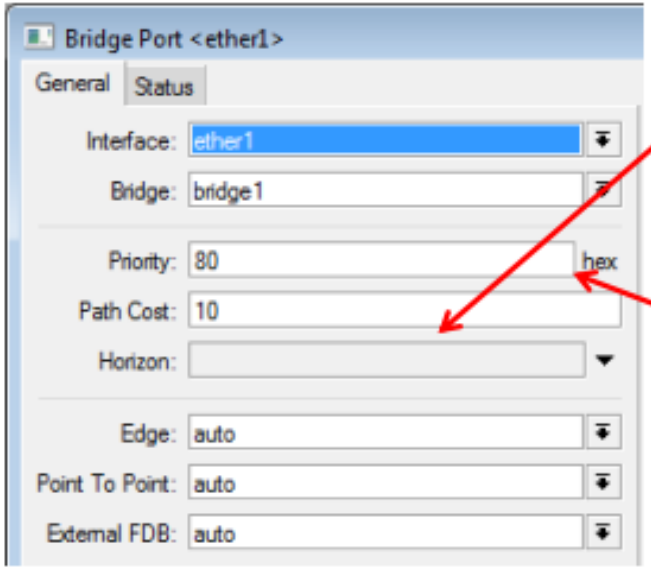
O (R)STP inicialmente elege uma root bridge e utiliza o algorítimo “breadth-first search” que quando encontra um MAC pela primeira vêz, torna o link ativo. Se o encontra outra vêz, torna o link desabilitado.

Normalmente habilitar o (R)STP já é o suficiente para atingir os resultados. No entanto é possível interferir no comportamento padrão, modificando custos, prioridades, etc.

WDS / Mesh WDS
(R)STP



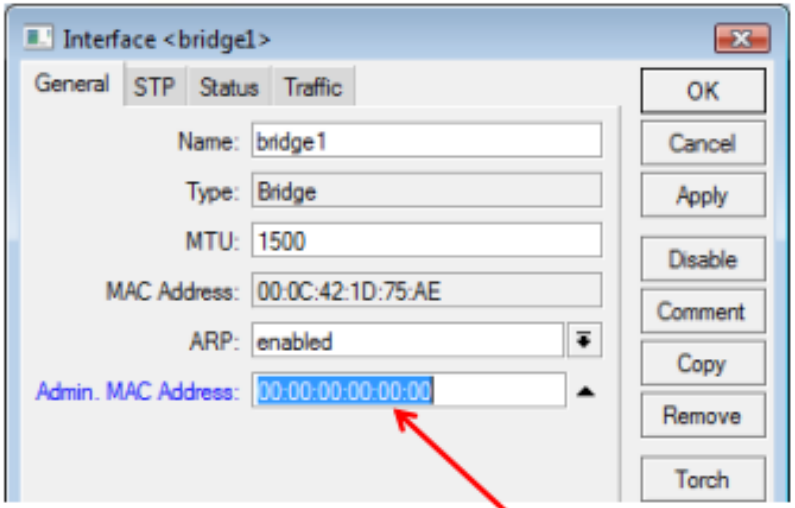
Ajustar para baixo se desejar assegurar a eleição dessa bridge como root .



Custo: permite um caminho ser eleito em lugar de outro

Prioridade: quando os custos são iguais, é eleito o de prioridade mais baixa.

WDS / Mesh WDS
(R)STP



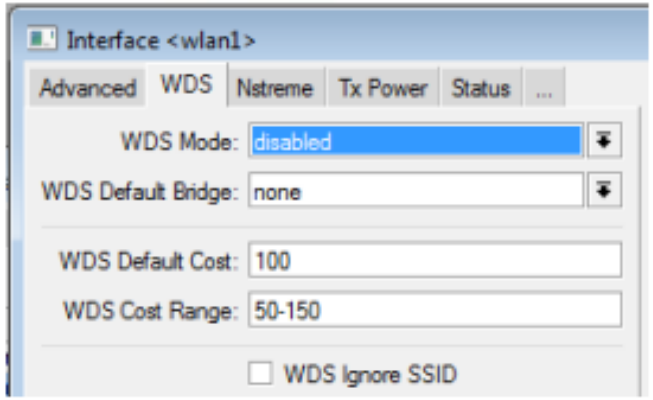
Admin MAC Address

→ A Bridge usa o endereço MAC da porta **ativa** com o menor número de porta

→ A porta Wireless está ativa somente quando existem hosts conectados a ela.

→ Para evitar que os MAC's fique variando, é possível atribuir manualmente um endereço MAC.

WDS / Mesh WDS



→ **WDS Default Bridge:** Informe aqui a bridge default.

→**WDS Default Cost:** Custo da porta da bridge do link WDS.

→ **WDS Cost Range:** Margem do custo que pode ser ajustada com base no troughput do link

Modos de WDS

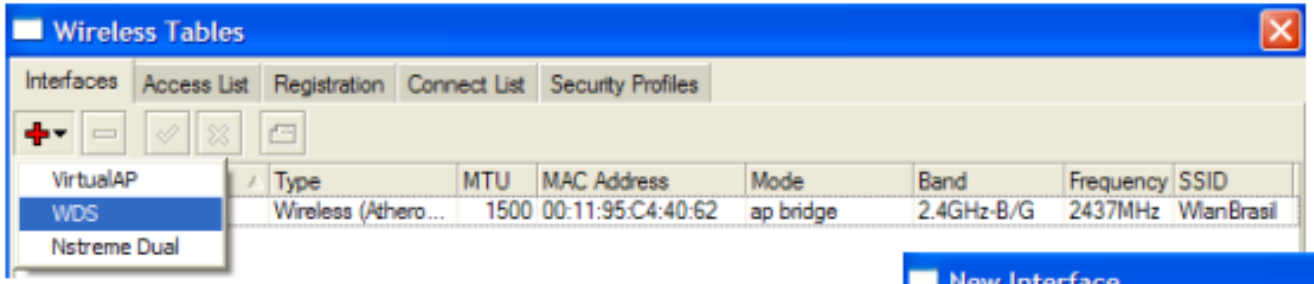
→ **dynamic:** as interfaces WDS são criadas dinamicamente quando um dispositivo em WDS encontra outro compatível (mesmo SSID e canal)

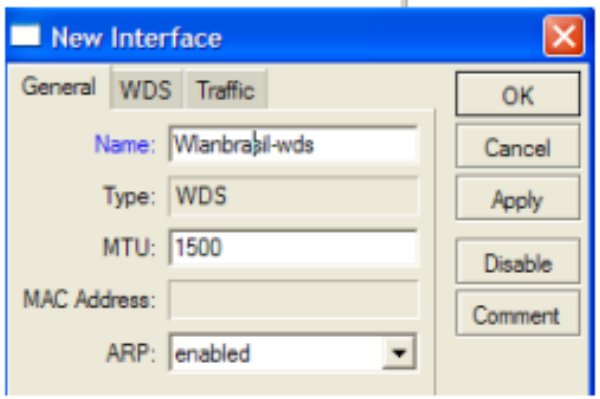
→ **static:** As interfaces tem de ser criadas manualmente com cada uma apontando para o MAC de sua "parceira"

→ **dynamic mesh:** O mesmo que dinâmica, porém com um algorítmo proprietário para melhoria do link (não compatível com outros fabricantes)

→ **static mesh:** A mesma explicação acima, porém para estátiva.

Wireless / Interfaces / WDS





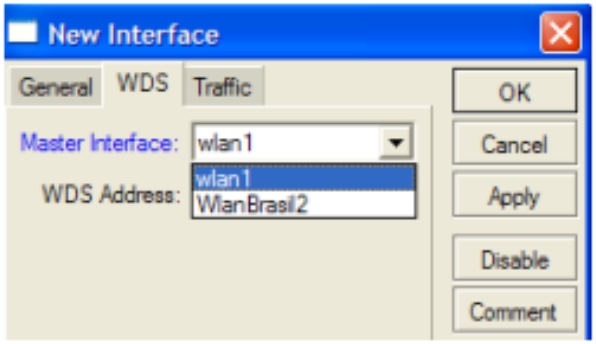
WDS:

Cria-se as interfaces WDS, dando os parametros:

→Name: Nome da rede WDS

→Master Interface: Interface sobre a qual funcionará o WDS, podendo esta inclusive ser uma interface virtual

→WDS ADDRESS: Endereço MAC que a interface WDS terá.

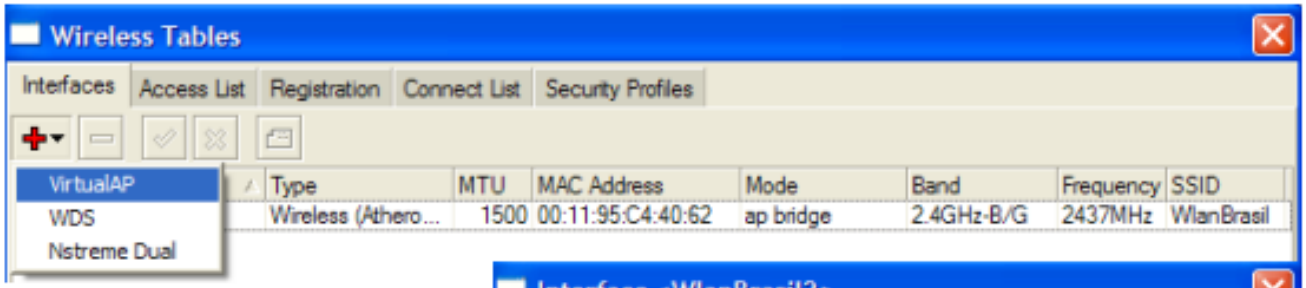


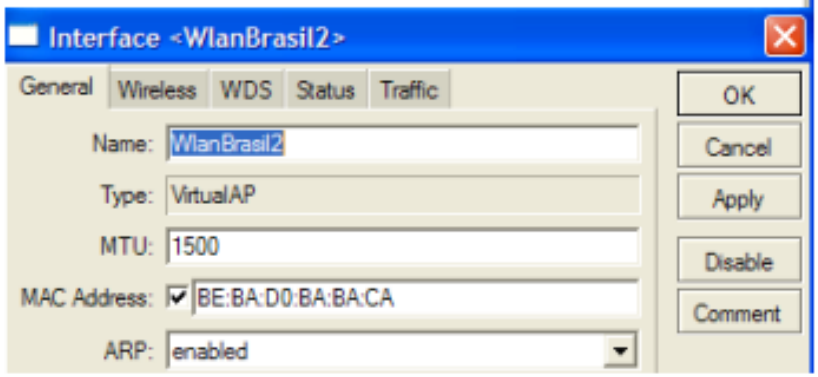
WDS / Mesh WDS
Laboratórios de WDS/Mesh

- → Link transparente com station-wds
- → Rede Mesh com WDS+RSTP
- → WDS-Slave

AP Virtual

Wireless / Interfaces





Interfaces Virtuais:

Criando interfaces virtuais podemos montar várias redes dando perfis de serviço diferentes

→Name: Nome da rede virtual

→MTU: Unidade de transferencia máxima (bytes)

→MAC Address: Dê o MAC que quiser para o novo AP !

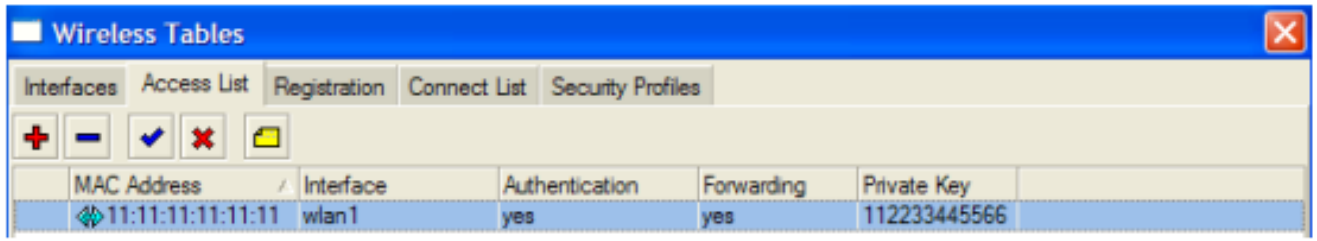
→ARP

- → Enable/Disable: habilita/desabilita
- → proxy-arp: passa seu MAC
- → reply-only

OBS: Demais configurações identicas de uma AP

Controle de Acesso

Wireless Tables / Access List

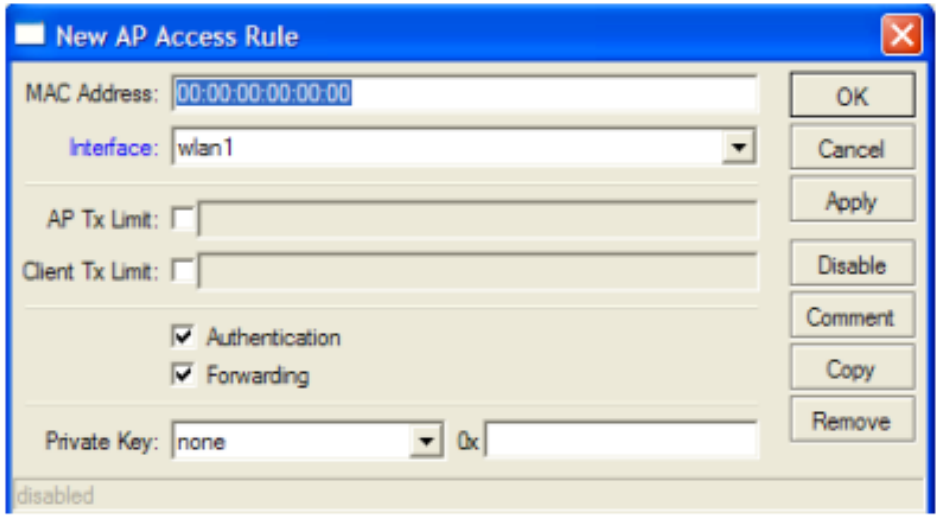


O Access List é utilizado pelo Access Point para restringir associações de clientes. Esta lista contem os endereços MAC de clientes e determina qual a ação deve ser tomada quando um cliente tenta conectar. A comunicação entre clientes da mesma interface, virtual ou real, também é controlada nos Access List.

O processo de associação ocorre da seguinte forma:

- Um cliente tenta se associar a uma interface Wlanx
- Seu MAC é procurado no acces list da interface Wlanx.
- Caso encontrada a ação especificada será tomada:
    - authenticate marcado: deixa o cliente se autenticar
    - forwarding marcado, o cliente se comunica com outros..

Wireless Tables / Access List



Private Key: Chave de criptografia

→40 bit wep
→128 bit wep
→Aes-com

Access List

MAC Address: Mac a ser liberado

Interface: Interface Real ou Virtual onde será feito o controle.

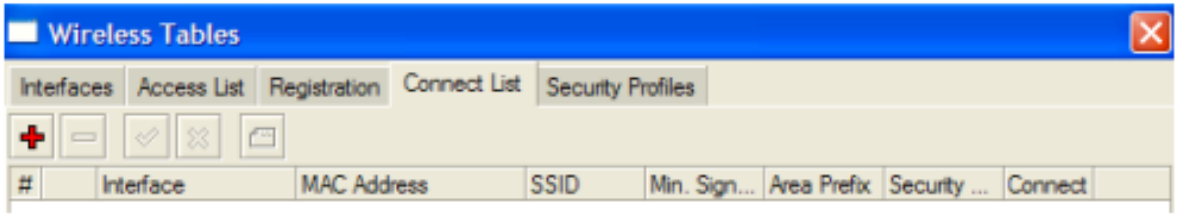
AP Tx Limit: Limite de tráfego AP → cada Cliente

Client Tx Limit: Limite de tráfego Cliente → AP (só vale para cliente Mikrotik)

Authentication: Habilitado, autentica os MAC's declarados.

Forwarding: Habilitdo permite a comunicação entre clientes habilitados (intra bss)

Wireless Tables / Connect List



A ***Connect List*** tem a finalidade de listar os pontos de Acesso que o Mikrotik configurado como cliente pode se conectar.

MAC Address: MAC do AP

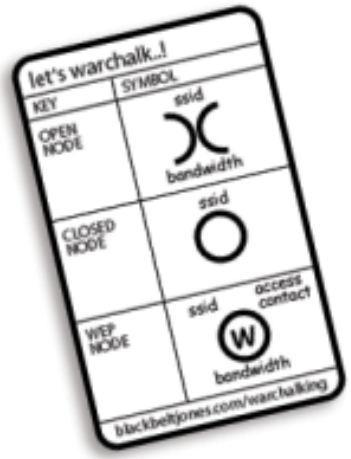
SSID: Nome da Rede

Area Prefix: String para conexão com o AP de mesma area

Security Profile: definido nos perfis de segurança.

OBS: Essa opção é interessante para evitar que o Cliente se associe em um Ponto de Acesso falso (sequestro do AP)

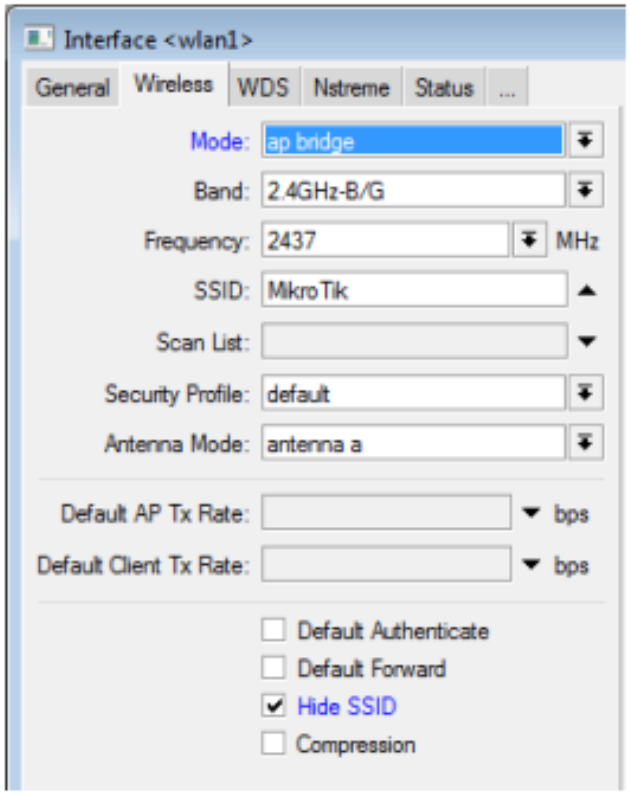
Segurança de acesso em redes sem fio



Segurança “Rudimentar”
(O que não é segurança)

1 – Nome de rede (SSID) escondido

Pontos de Acceso sem fio por padrão fazem o broadcast do seu SSID nos pacotes chamados “beacons”. Este comportamiento puede ser modificado no Mikrotik habilitando a opção Hide SSID.



Fragilidades:

→ SSID tem de ser conhecido pelos clientes

→ Scanners Passivos descobrem facilmente pelos pacores de “probe request”dos clientes.

Segurança "Rudimentar"
(O que não é segurança)

2 – Controle de MAC's

→ Descobrir MAC's que trafegam no ar é muito simples com ferramentas apropriadas

→ Airopeek para Windows

→ Kismet, Wellenreiter, etc para Linux/BSD

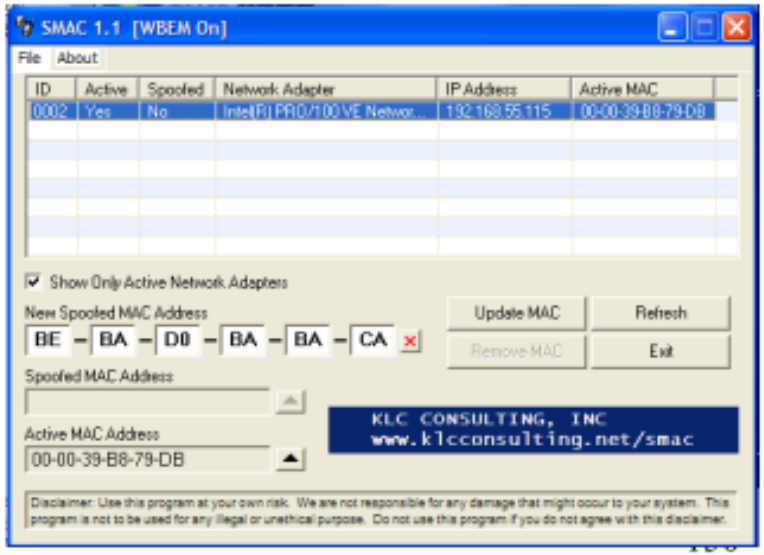
→ "Spoofar" um MAC é muito fácil, tanto em Linux como em Windows.

- FreeBSD :

ifconfig <interface> -L <MAC>

- Linux :

ifconfig <interface> hw ether <MAC>



Segurança "Rudimentar"
(O que não é segurança)

3 – Criptografia WEP

→ "Wired Equivalent Privacy" – foi o sistema de criptografia inicialmente especificado no padrão 802.11 e está baseada no compartilhamento de um segredo (semente) entre o ponto de Acesso e os clientes, usando o algorítimo RC4 para a criptografia.

→ Várias fragilidades da WEP foram reveladas ao longo do tempo e publicadas na Internet, existindo muitas ferramentas para quebrar a chave, como:

- → Airodump
- → Airreplay
- → Aircrack

→ Hoje é trivial a quebra da WEP que pode ser feita em poucos minutos com técnicas baseadas nas ferramentas acima.

Evolução dos Padrões de Segurança Wireless

+ SEGURANÇA

→WPA2 (802.11i) c/ EAP
→WPA2 (802.11i) c/ PSK
→WPA c/ AES ccm
→WPA c/ MD5
→WEP c/ TKIP
→WEP 128 bits
→WEP 64 bits

Fundamentos de Segurança

→Privacidade

→ A informação não pode ser legível por terceiros

→Integridade

→ A informação não pode ser alterada quando em transito.

→Autenticação

AP → Cliente: O AP tem que garantir que o cliente é quem diz ser.

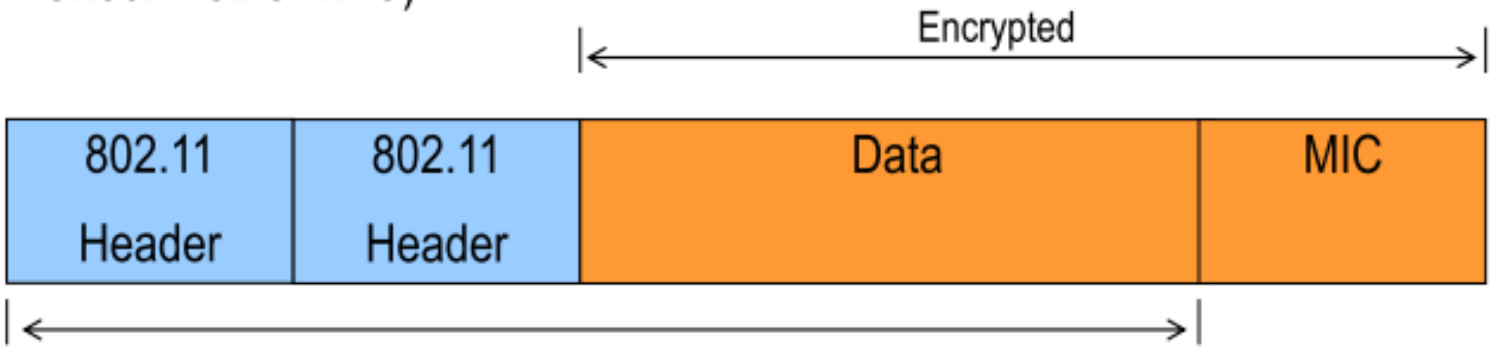
Cliente →AP: O Cliente tem que se certificar que está se conectando no AP verdadeiro. Um AP falso possibilita o chamado ataque do "homem do meio"

Privacidade e Integridade

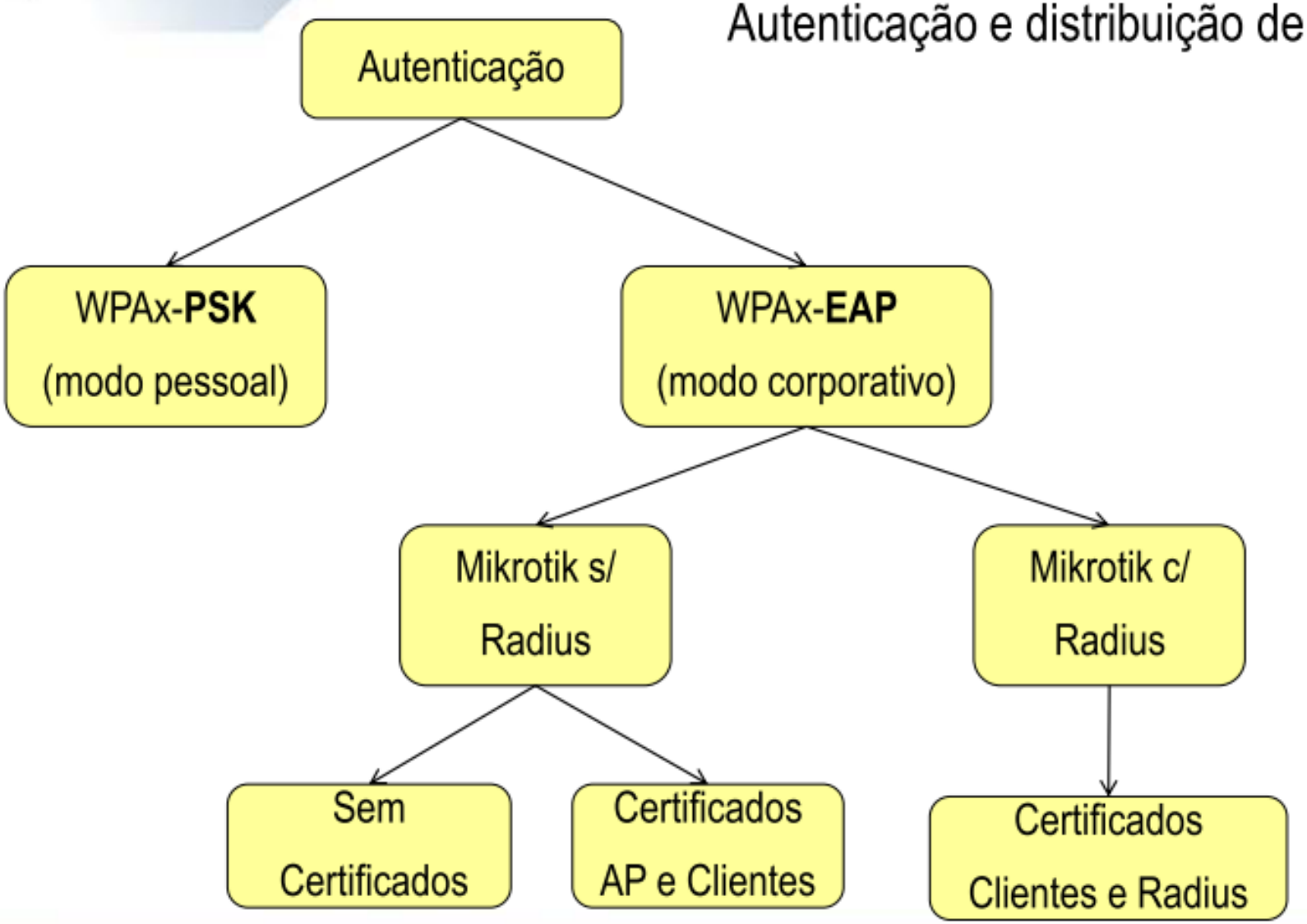
Tanto a privacidade como a integridade são garantidas por técnicas de criptografia.

→ O algorítimo de criptografia de dados em WPA é o RC4, porém implementado de uma forma bem mais segura que na WEP. E na WPA2 utiliza-se o AES.

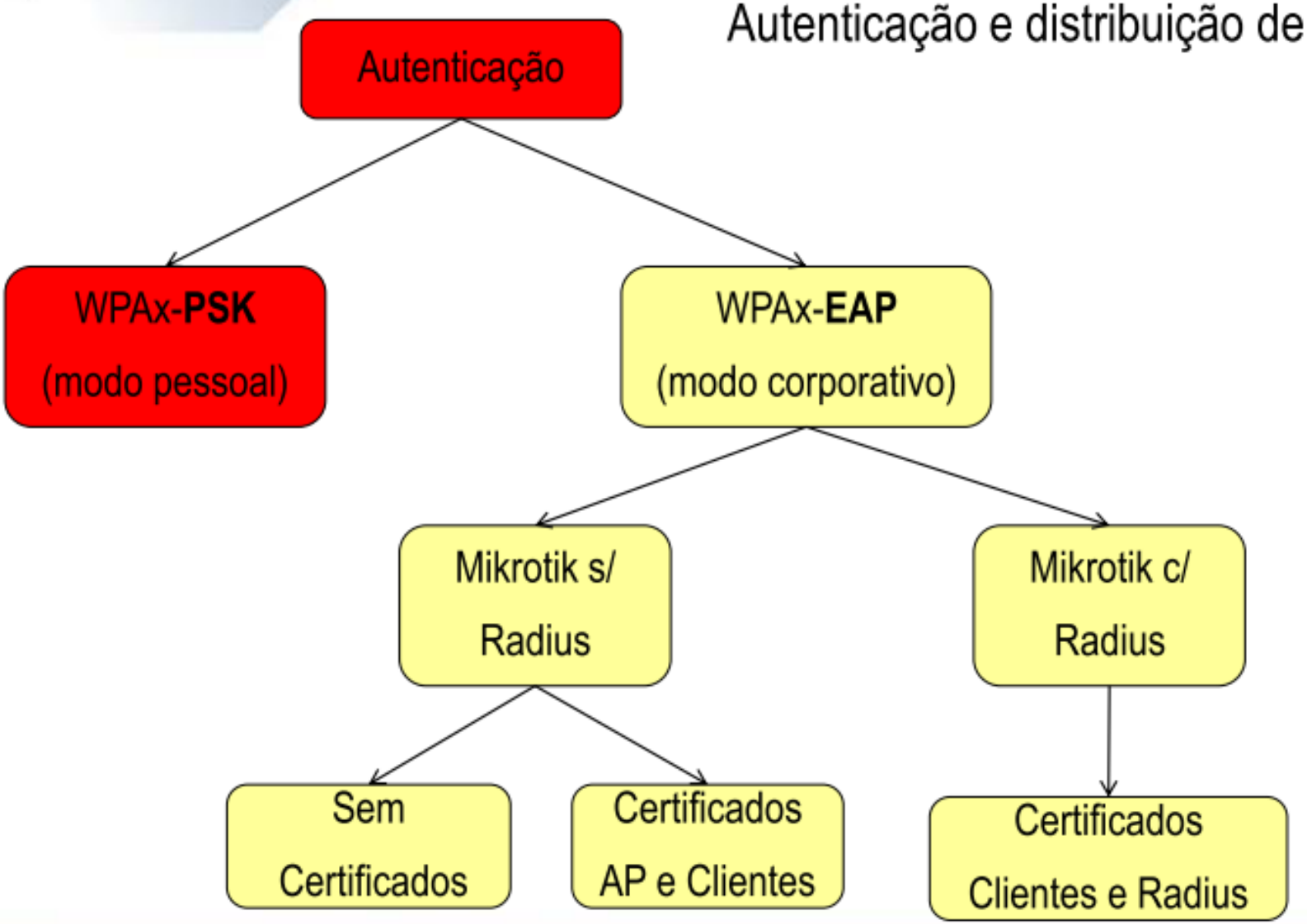
→ Para a Integridade dos dados WPA usa TKIP → Algoritimo de Hashing "Michael" e WPA2 usa CCMP (Cipher Block Chaining Message Authentication Check– CBC-MAC)



Autenticação e distribuição de chaves

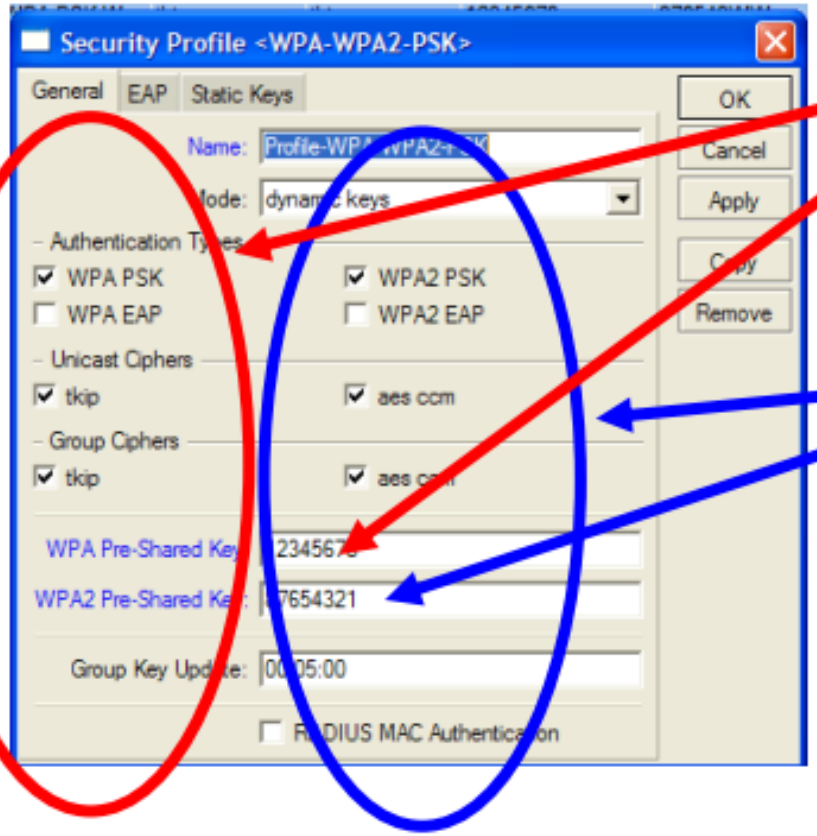


Autenticação e distribuição de chaves



Utilizando WPA/WPA2 – PSK

É muito simples a configuração de WPA/WPA2-PSK com o Mikrotik



→ **WPA - PSK**

Configure o modo de chave dinâmico,WPA PSK, e a chave pré combinada.

→ **WPA2 – PSK**

Configure o modo de chave dinâmico WPA2, PSK, e a chave pré combinada.

As chaves são alfanuméricas de 8 até 63 caracteres

WPA / WPA2 PSK é segura ?

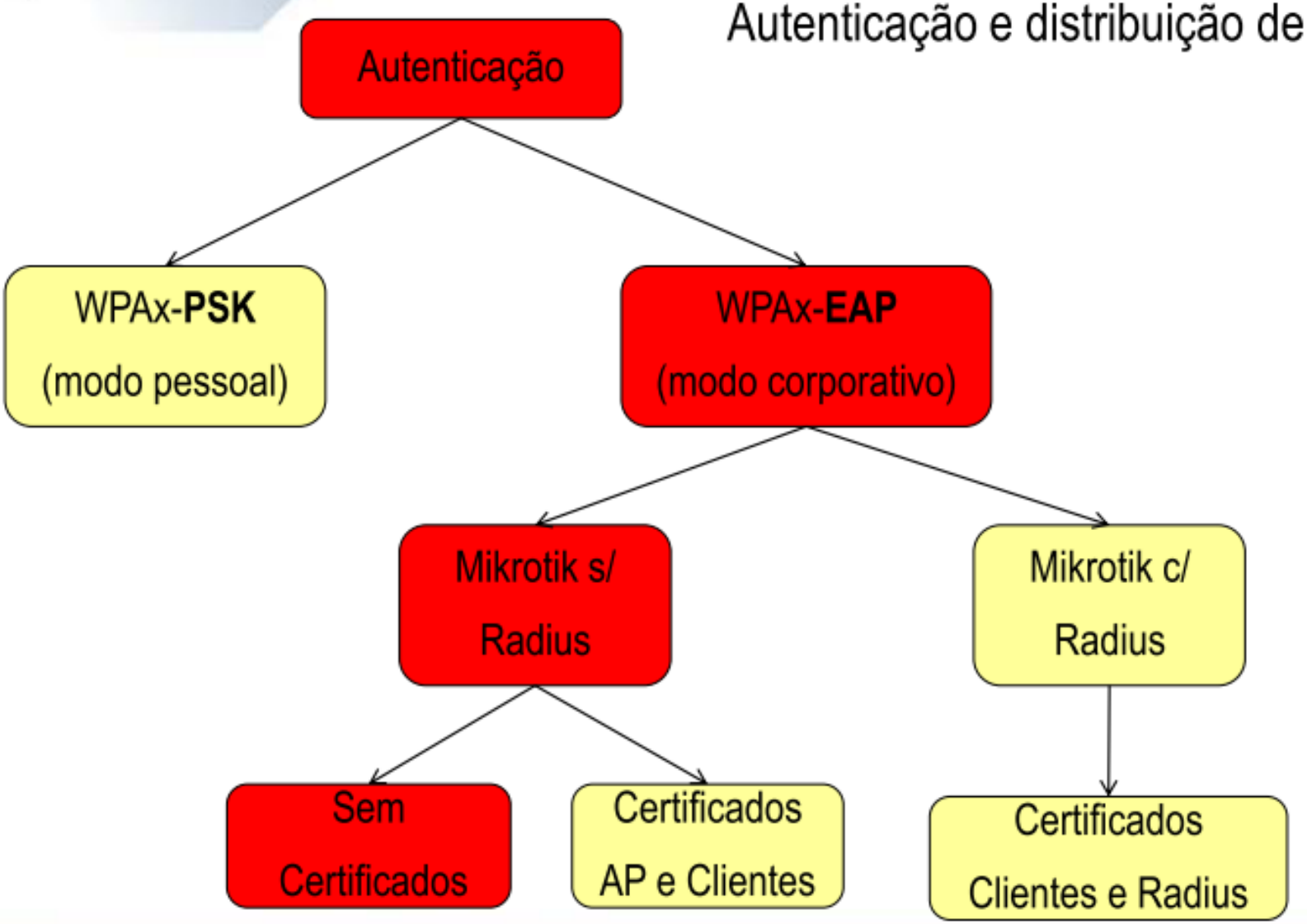
- A maneira conhecida hoje para quebrar WPA-PSK é somente por ataque de dicionário.
- Como a chave mestra - PMK combina uma contrasenha com o SSID, escolhendo palavras fortes torna o sucesso por ataque de força bruta praticamente impossível.

http://arstechnica.com/articles/paedia/wpa-cracked.ars/1

- Projeto na Internet para estudo de fragilidades da WPA/WPA2 – PSK
  - Cowpatty http://sourceforge.net/projects/cowpatty

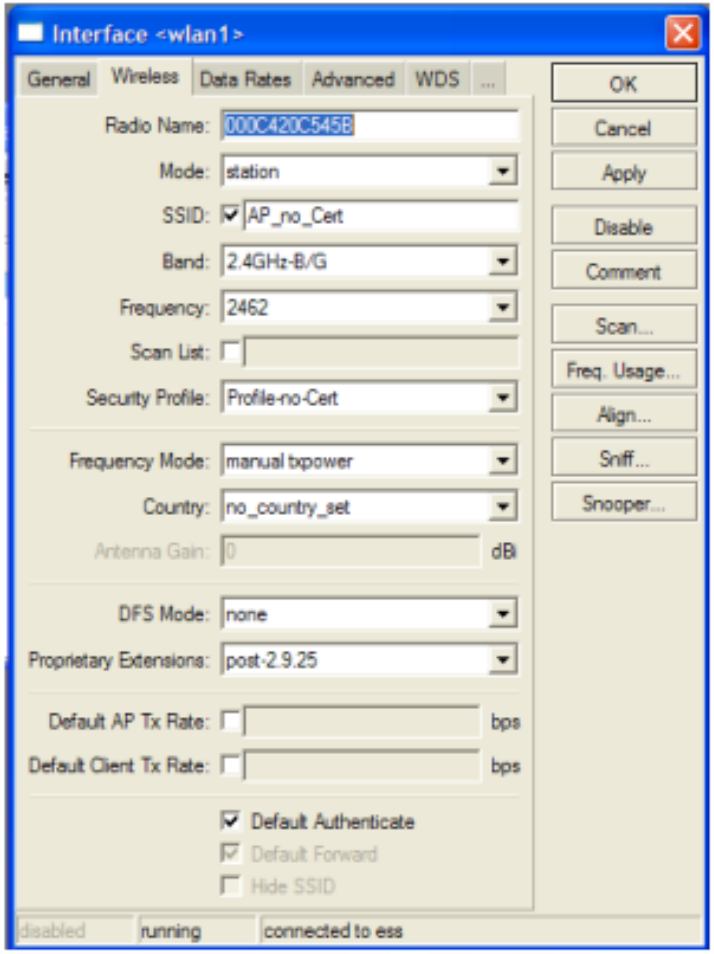
- A maior fragilidade no entanto da técnica de PSK para WISP's é que a chave se encontra em texto plano nos computadores dos clientes.

Autenticação e distribuição de chaves

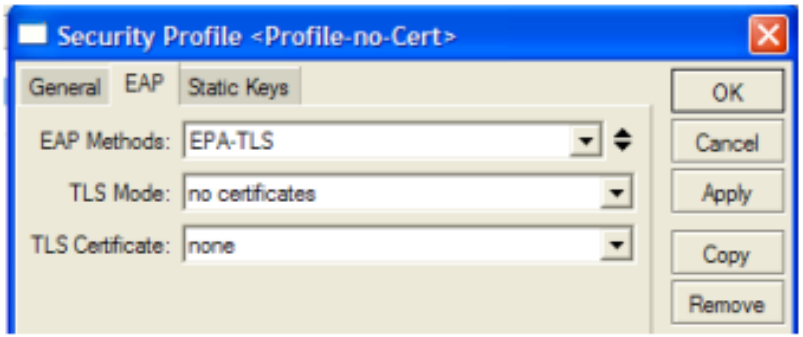


Setup with EAP-TLS – No Certificates

Station Configuration



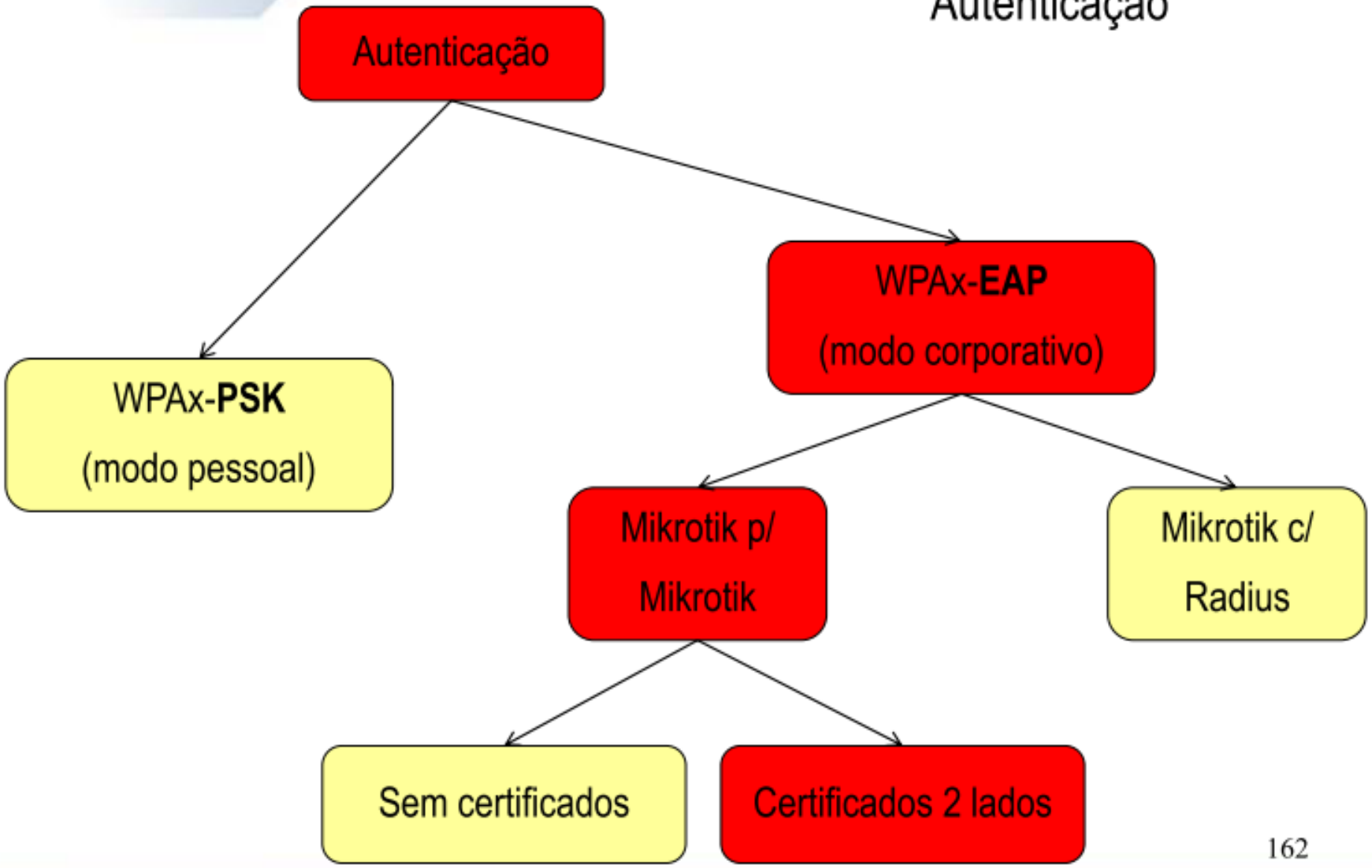
Security Profile



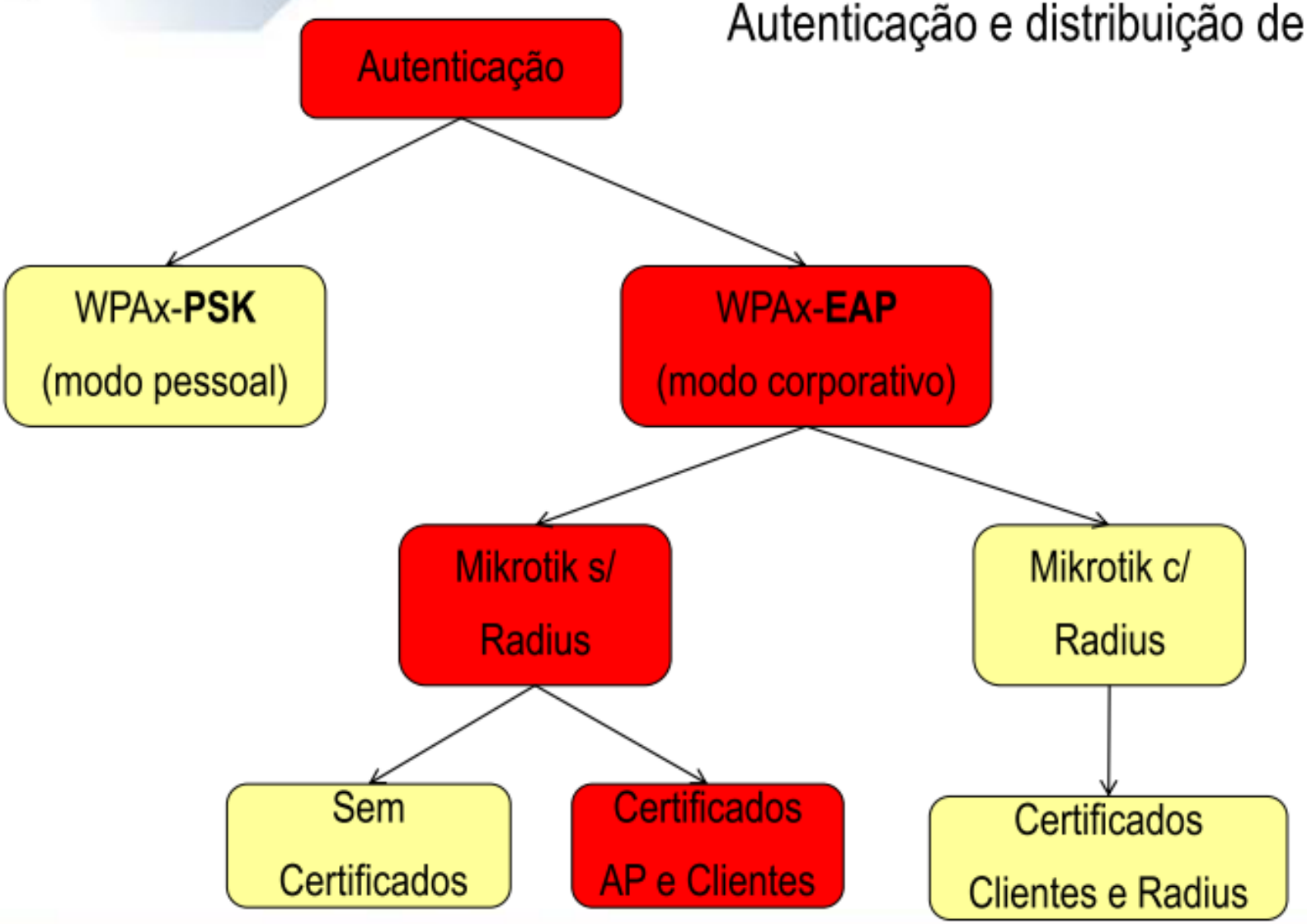
EAP-TLS sem Certificados é seguro ?

- Como resultado da negociação anonima resulta uma PMK que é de conhecimento exclusivo das duas partes e depois disso toda a comunicação é criptografada por AES (WPA2) o RC4 (WPA)
- Seria um método muito seguro se não houvesse a possibilidade de um atacante colocar um Mikrotik com a mesma configuração e negociar a chave normalmente como se fosse um equipamento da rede ☹
- Uma idéia para utilizar essa configuração de forma segura é utilizar esse método, e depois de fechado o enlace, criar um túnel criptografado PPtP ou L2TP entre os equipamentos.

Fundamentos de Segurança WPAx
Autenticação



Autenticação e distribuição de chaves



Trabalhando com Certificados

Un certificado digital é um arquivo que identifica de forma inequívoca o seu proprietário.

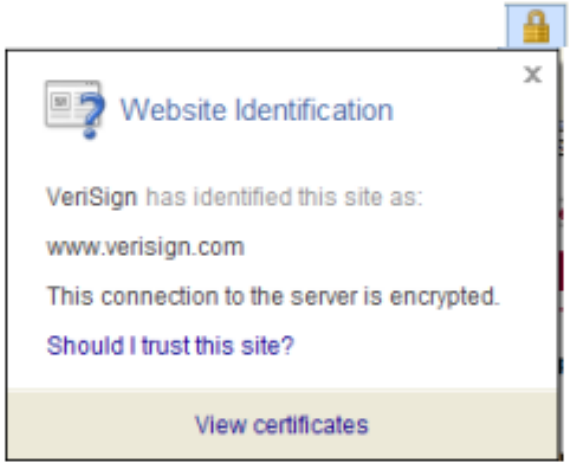
Certificados são criados por instituições emissoras chamadas de CA (Certificate Authorities)

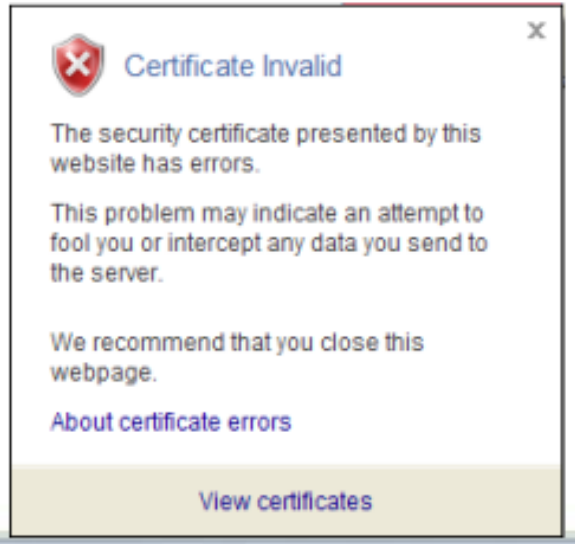
Os Certificados podem ser :

→ Assinados por uma instituição “acreditada” (Verisign, Thawte, etc)

ou

→ Certificados auto-assinados





Passos para implementação de EAP-TLS com Certificados auto assinados

Passo A → Criar a entidade Certificadora (CA)

Passo B → Criar as requisições de Certificados

Passo C → Assinar as requisições na CA

Passo D → Importar os Certificados assinados para os Mikrotiks

Passo E → Se necessário, criar os Certificados para máquinas Windows

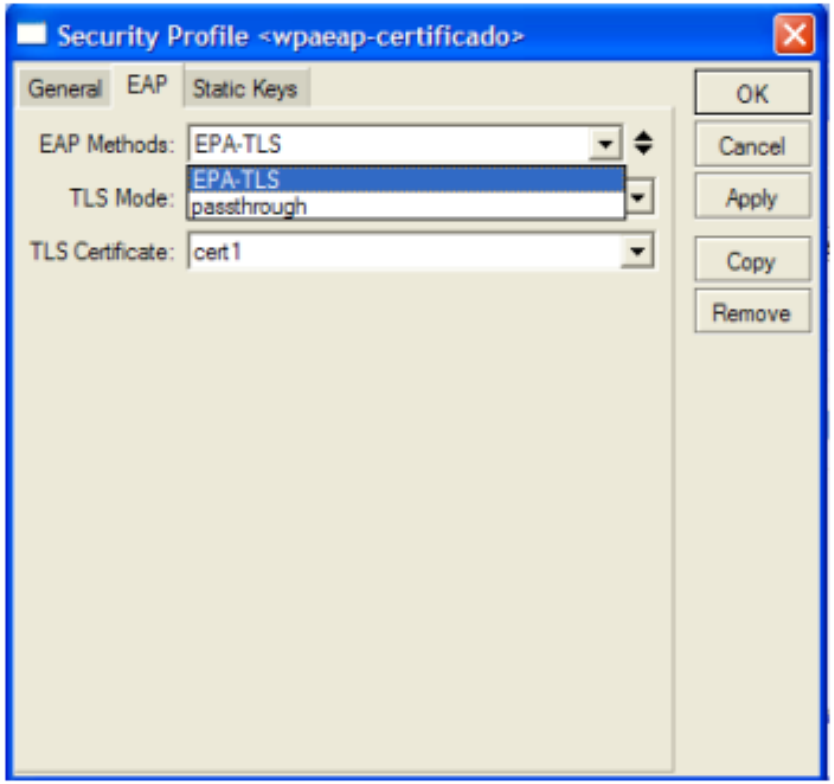
Tutoriais detalhados de como fazer isso:

http://wiki.mikrotik.com/images/2/20/AR_2007_MB_Wireless_security_Argentina_Maia.pdf

http://mum.mikrotik.com/presentations/PL08/mdbrasil.pdf

Método EAP-TLS sem Radius (em AP's e Clientes)

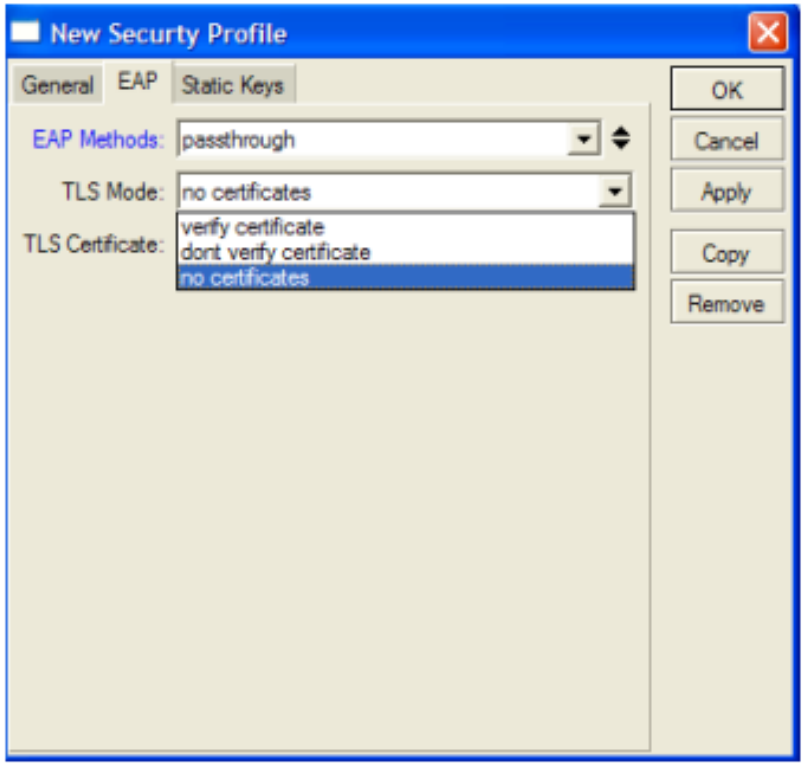
Security Profiles – Métodos de EAP



→**EAP-TLS**

Usa Certificados

Security Profiles – TLS Mode



→ verify certificates

Requer um certificado e verifica se foi firmado por uma ~CA

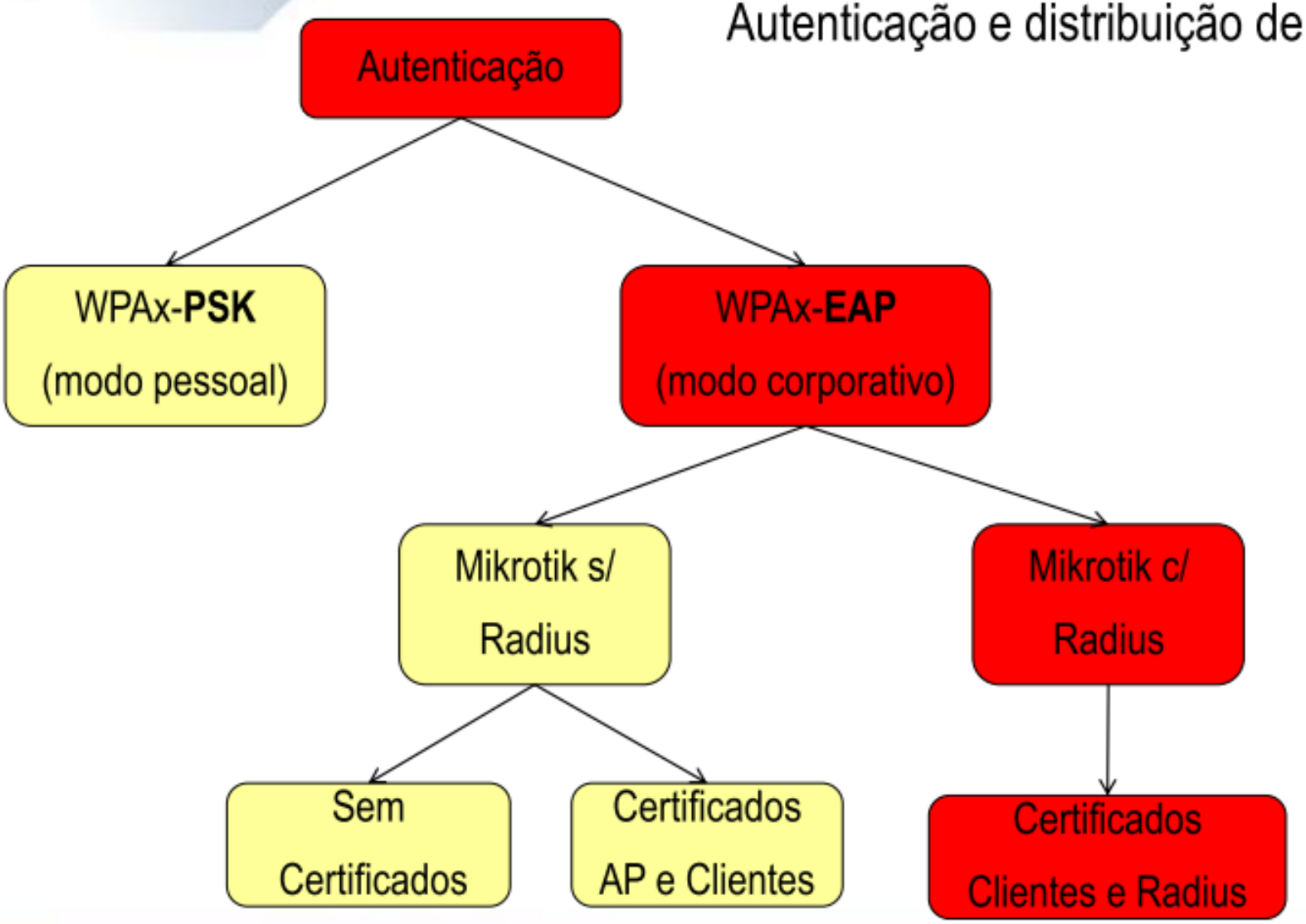
→ don't verify certificates

Requer um Certificado, porém não verifica

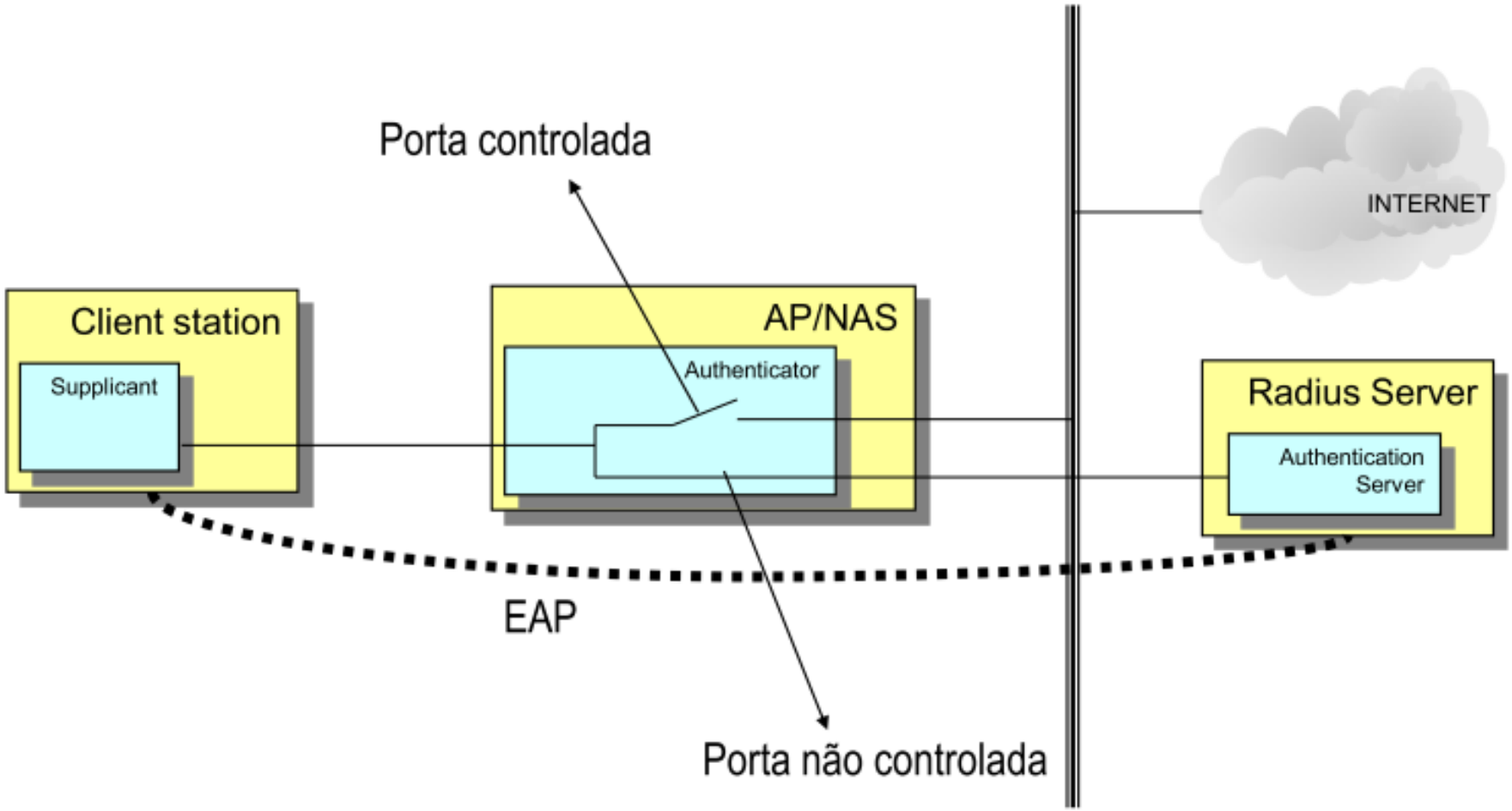
→ no certificates

Certificados são negociados dinâmicamente com o el algorítmo de Diffie-Hellman (explicado anteriormente

Autenticação e distribuição de chaves



WPAx com Radius



Tipos de EAP

EAP-TLS (EAP – Transport Layer Security)

→ O Mikrotik suporta EAP-TLS tanto como cliente como AP e ainda repassa esse método para um Servidor Radius

Provê o maior nível de segurança e necessita de Certificados nos lados do Cliente e do Servidor Radius

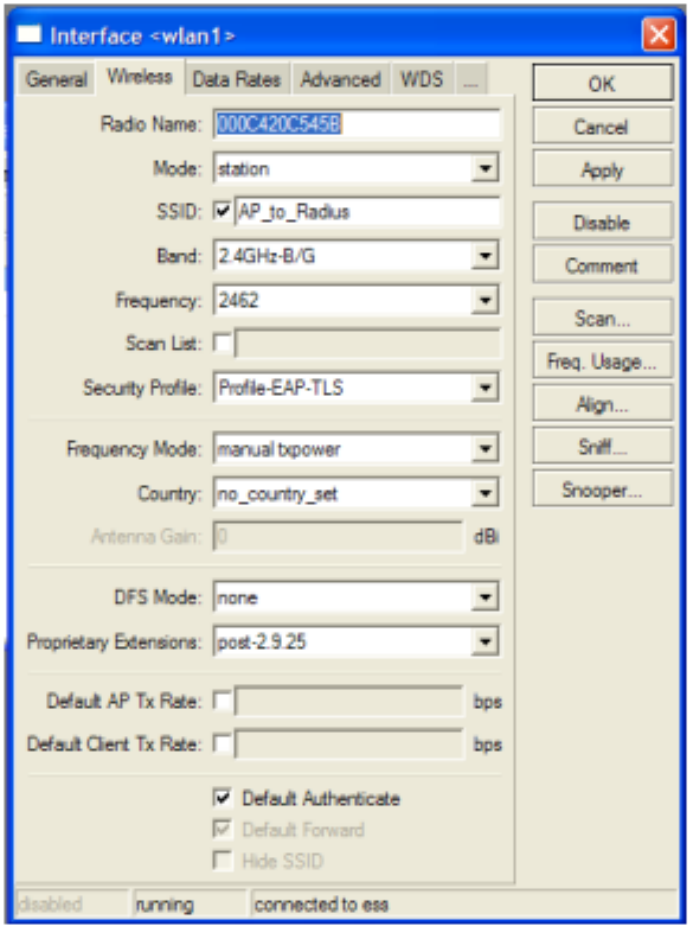
Os passos de como configurar e instalar certificados em um Servidor RADIUS podem ser obtidos em:

http://wiki.mikrotik.com/images/2/20/AR_2007_MB_Wireless_security_Argentina_Maia.pdf

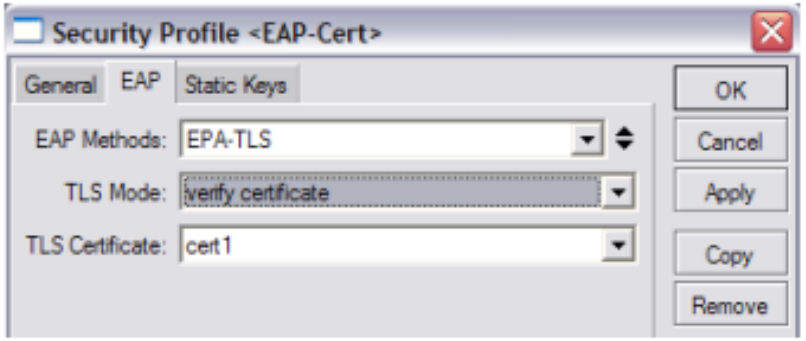
http://mum.mikrotik.com/presentations/PL08/mdbrasil.pdf

Setup with EAP-TLS + Radius Client Configuration

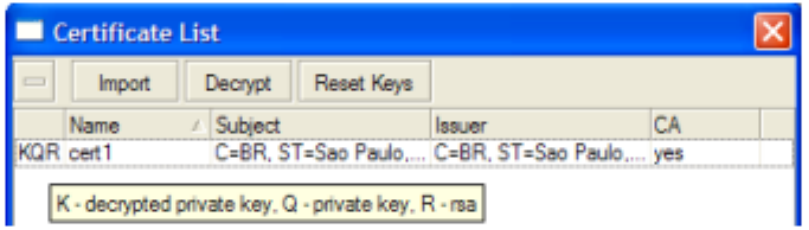
Station Configuration



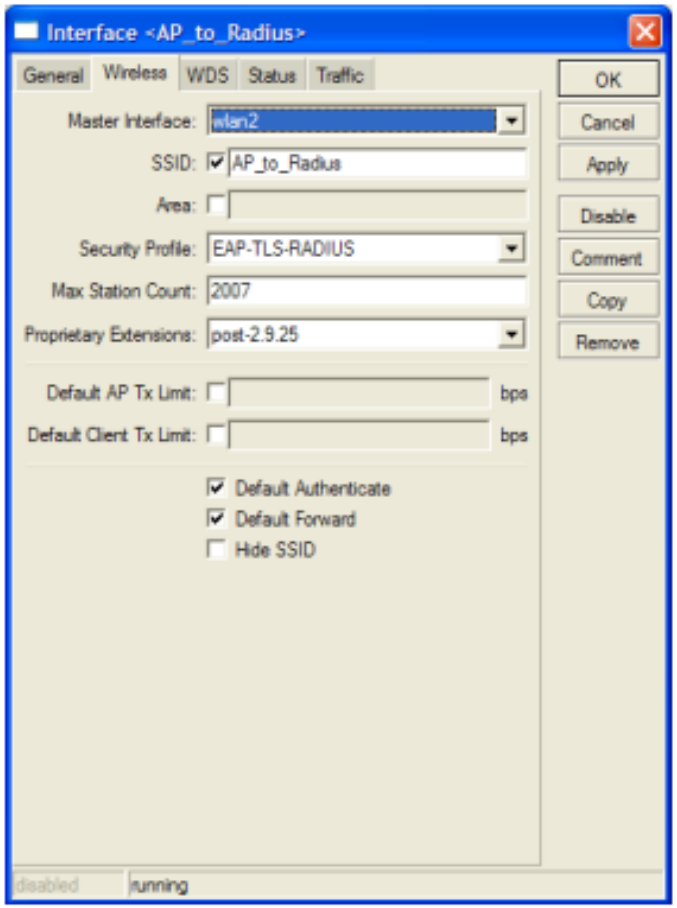
Security Profile



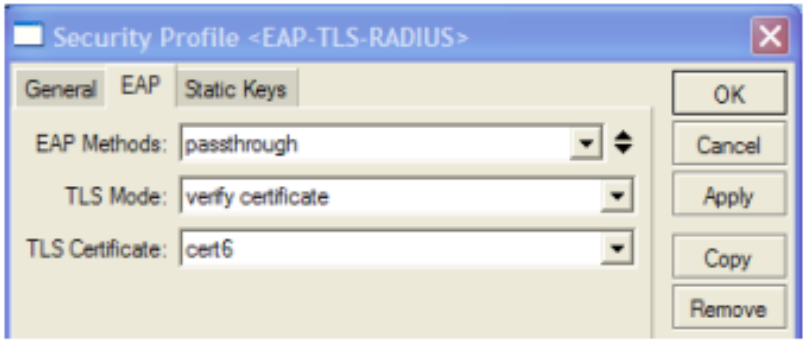
Certificate



Setup with EAP-TLS + Radius
AP Configuration



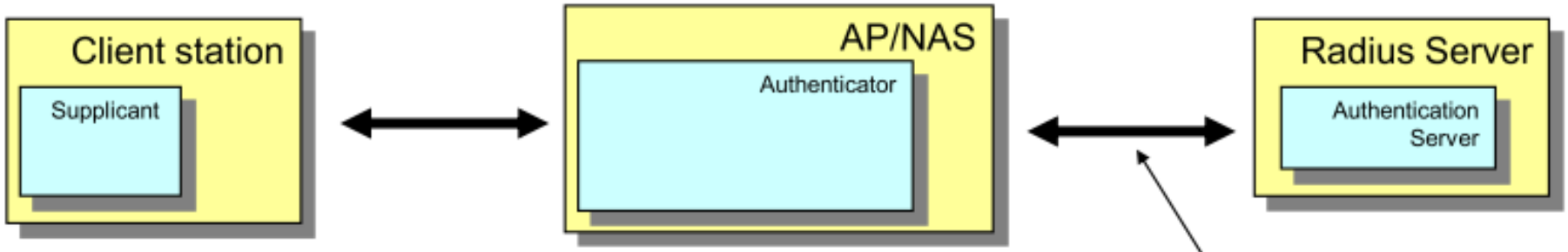
Security Profile



O método EAP-TLS + Radius é seguro ?

No se discute que o EAP-TLS é o método mais seguro que se pode obter, porém há

Um ponto que se pode levantar como uma possível fragilidade:



Existem ataques conhecidos contra o protocolo Radius.

Se um atacante tem acesso físico ao link entre o AP e o Radius

ele pode fazer ataque de força bruta para descobrir a PMK.

→ Para evitar isso há várias formas como proteger esse trecho com um tunel L2TP ou PPtP

Resumo dos métodos possíveis de implantação e seus problemas

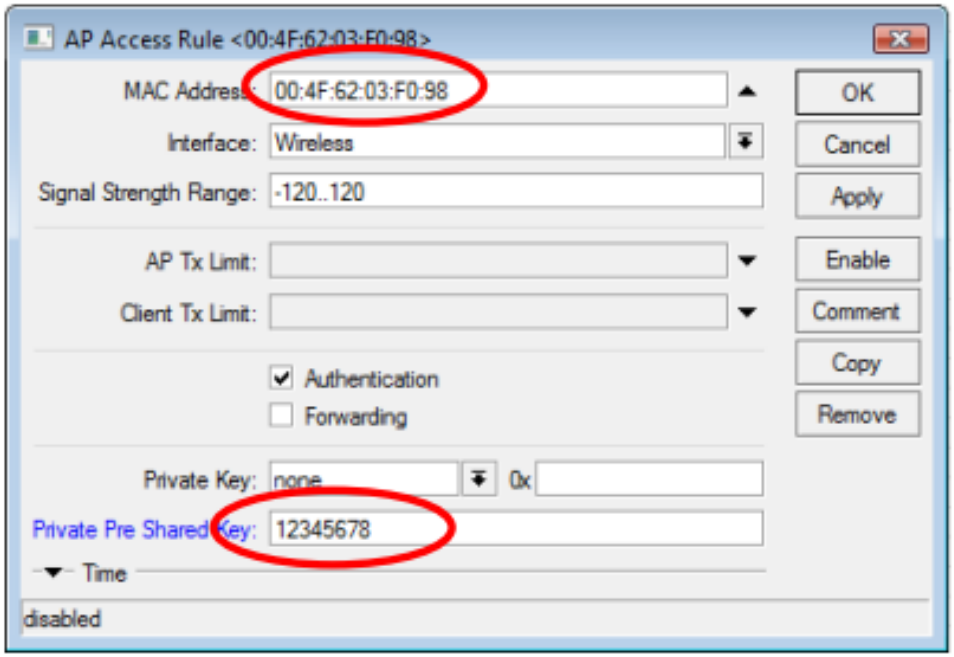
- **WPA-PSK:**
  - Chaves presentes nos clientes e acessíveis aos operadores
- **Método Sem Certificados:**
  - Passível de invasão por equipamento que tambem opere desse modo
  - Problemas com processamento
- **Mikrotik com Mikrotik com EAP-TLS**
  - Método seguro porém inviável economicamente e de implantação praticamente impossível em redes existentes.

Resumo dos métodos possíveis de implantação e seus problemas

- **Mikrotik com Radius:**
  - EAP-TTLS e EAP-PEAP:
    - Sujeito ao "homem do meio" e pouco disponível nos atuais equipamentos.
  - EAP-TLS
    - Método seguro, porém também não disponível na maioria dos equipamentos. Em "plaquinhas" é possível implementa-los.

Método alternativo Mikrotik

→ O Mikrotik na versão V3 oferece a possibilidade de distribuir uma chave WPA2 por cliente . Essa chave é configurada no Access List do AP e é vinculada ao MAC address do cliente, possibilitando que cada cliente tenha sua chave.



→ Cadastrar porém nos access lists, voltamos ao problema da chave ser visível a usuários do Mikrotik !

Método alternativo Mikrotik

→ Felizmente o Mikrotik permite que a chave seja atribuída por Radius o que torna muito interessante esse método.

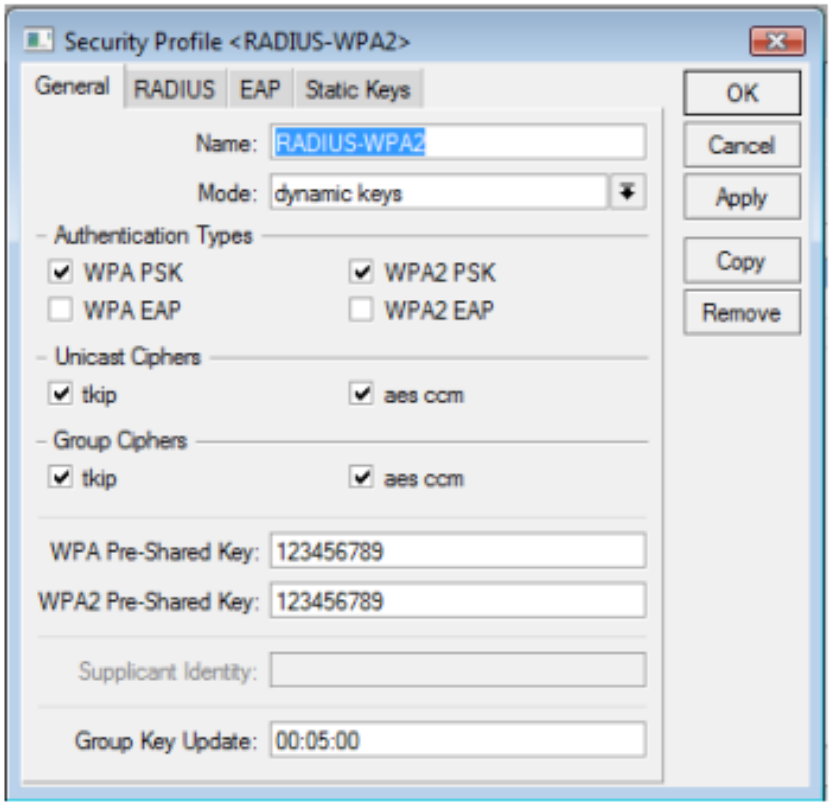
Para configurar precisamos:

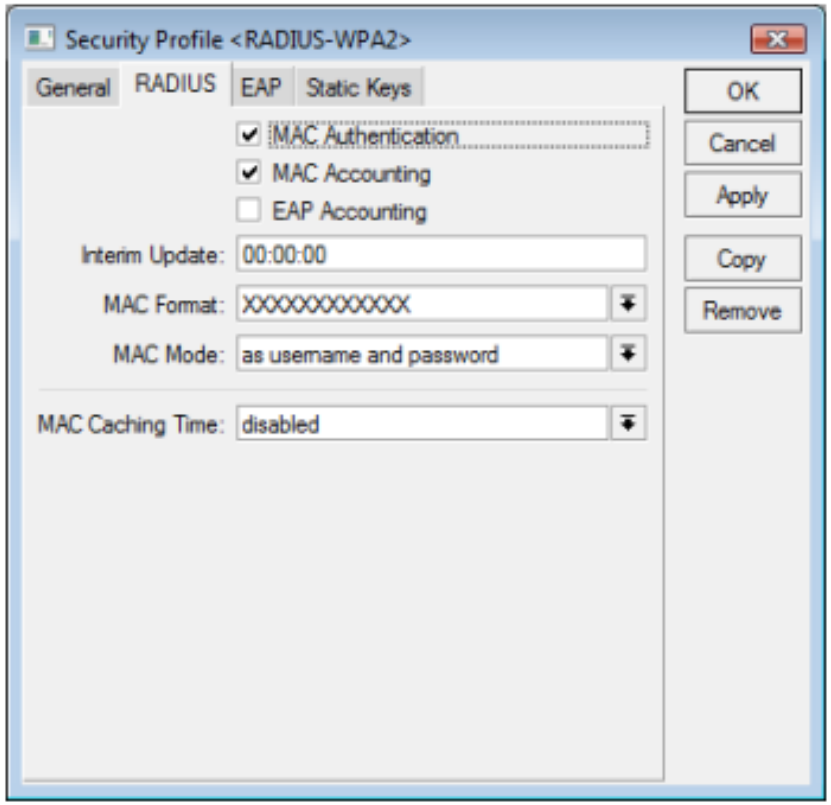
→ Criar um perfil WPA2 qualquer

→ Habilitar a autenticação via MAC no AP

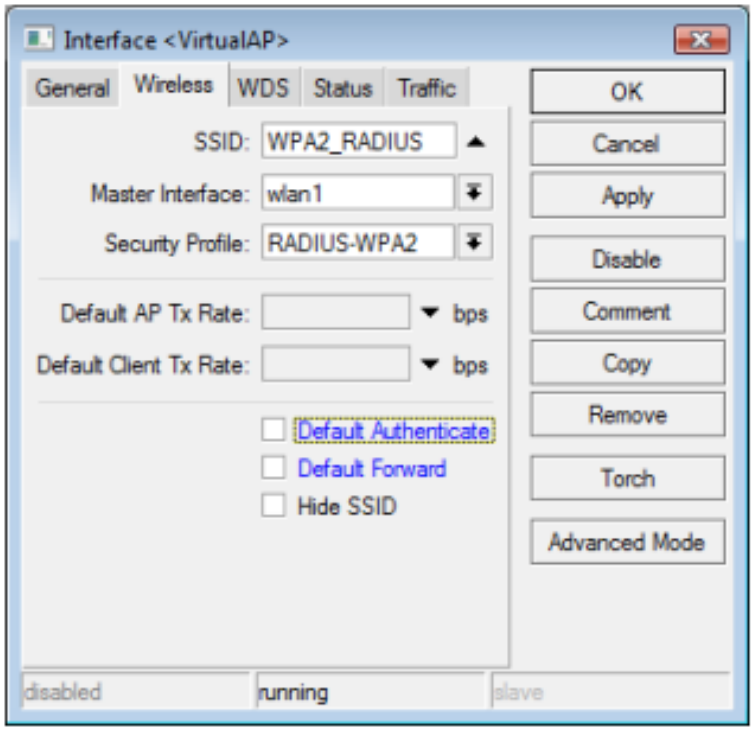
→ Ter a mesma chave configurada tanto no cliente como no Radius.

Configurando o Perfil





Configurando a Interface Wireless



Arquivo users: (/etc/freeradius)

```
# Sintaxe:
# MAC     Cleartext-Password := “MAC“
#         Mikrotik-Wireless-Psk = “Chave_PSK_de_8_a_63_caracteres“


001DE05A1749      Cleartext-Password := "001DE05A1749“
                  Mikrotik-Wireless-Psk = "12345678912“
001B779ADD5D    Cleartext-Password := "001B779ADD5D"
                  Mikrotik-Wireless-Psk = "12345678911“
001B77AF82C9      Cleartext-Password := "001B77AF82C9"
                  Mikrotik-Wireless-Psk = "12345678911"
```

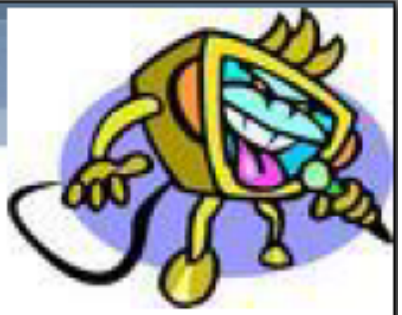
Radius (dictionary)

/usr/share/freeradius/dictionary.mikrotik

```
# MikroTik Attributes

VENDOR          Mikrotik        14988

ATTRIBUTE       Mikrotik-Recv-Limit             1       integer         Mikrotik
ATTRIBUTE       Mikrotik-Xmit-Limit             2       integer         Mikrotik
ATTRIBUTE       Mikrotik-Group                  3       string          Mikrotik
ATTRIBUTE       Mikrotik-Wireless-Forward       4       integer         Mikrotik
ATTRIBUTE       Mikrotik-Wireless-Skip-Dot1x    5       integer         Mikrotik
ATTRIBUTE       Mikrotik-Wireless-Enc-Algo      6       integer         Mikrotik
ATTRIBUTE       Mikrotik-Wireless-Enc-Key       7       string          Mikrotik
ATTRIBUTE       Mikrotik-Rate-Limit             8       string          Mikrotik
ATTRIBUTE       Mikrotik-Realm                  9       string          Mikrotik
ATTRIBUTE       Mikrotik-Host-IP                10      ipaddr          Mikrotik
ATTRIBUTE       Mikrotik-Mark-Id                11      string          Mikrotik
ATTRIBUTE       Mikrotik-Advertise-URL          12      string          Mikrotik
ATTRIBUTE       Mikrotik-Advertise-Interval     13      integer         Mikrotik
ATTRIBUTE       Mikrotik-Recv-Limit-Gigawords   14      integer         Mikrotik
ATTRIBUTE       Mikrotik-Xmit-Limit-Gigawords   15      integer         Mikrotik
ATTRIBUTE       Mikrotik-Wireless-Psk           16      string          Mikrotik

# MikroTik Values

VALUE           Mikrotik-Wireless-Enc-Algo      No-encryption           0
VALUE           Mikrotik-Wireless-Enc-Algo      40-bit-WEP              1
VALUE           Mikrotik-Wireless-Enc-Algo      104-bit-WEP             2
```

Para maiores detalhes de implementação de PSK individual por cliente ver trabalho apresentado no MUM Brasil 2008

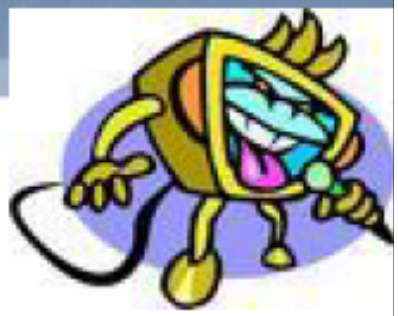
(Disponível em nosso FTP)



Firewall

com Mikrotik

Firewall

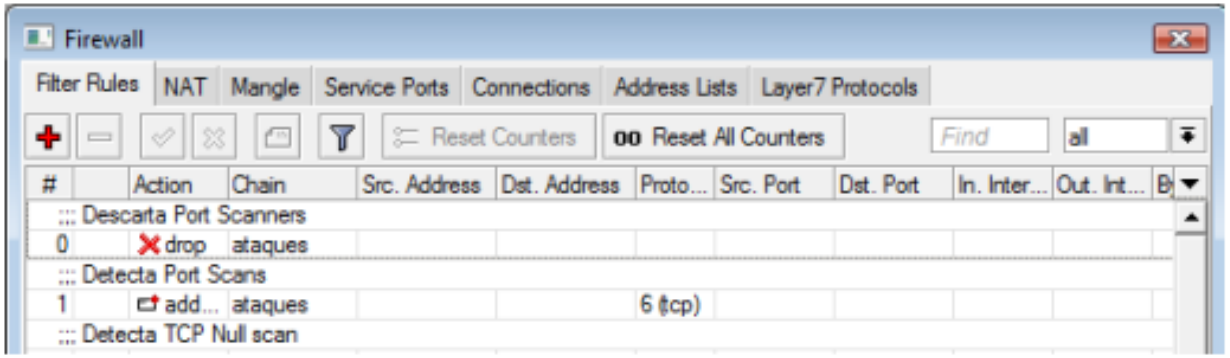


O Firewall é normalmente é usado como ferramenta de segurança para prevenir o acesso não autorizado à rede interna e ou acesso ao roteador em si, bloquear diversos tipos de ataques e controlar o fluxo de dados tanto de entrada como de saída.

Além de segurança é no Firewall que serão desempenhadas diversas funções importantes como a classificação e marcação de pacotes para uso nas ferramentas de QoS

A classificação do tráfego feita no Firewall pode ser baseada em vários classificadores como endereços MAC, endereços IP, tipos de endereços IP (broadcast, multicast, etc) portas de origem e de destino, range de portas, protocolos, Tipo do Serviço (ToS), tamanho do pacote, conteúdo do pacote, etc etc.

Firewall – visão geral



→ **Filter Rules:** é onde ficam as regras de filtros de pacotes

→ **NAT:** onde é feito a tradução de endereços (mascaramento por exemplo)

→ **Mangle:** onde é feita a marcação de pacotes, conexões e roteamento

→ **Connections:** onde são visualizadas as conexões existentes

→ **Address Lists:** lista de endereços IP inserida manual ou dinamicamente que podem ser utilizados em várias partes do Firewall

→ **Layer 7 Protocols:** Filtros de camada 7 (Aplicação)

Princípios Gerais de Firewall
Canais default

- Um Firewall opera por meio de regras de Firewall. Uma regra é uma expressão lógica que diz ao roteador o que fazer com um tipo particular de pacote.

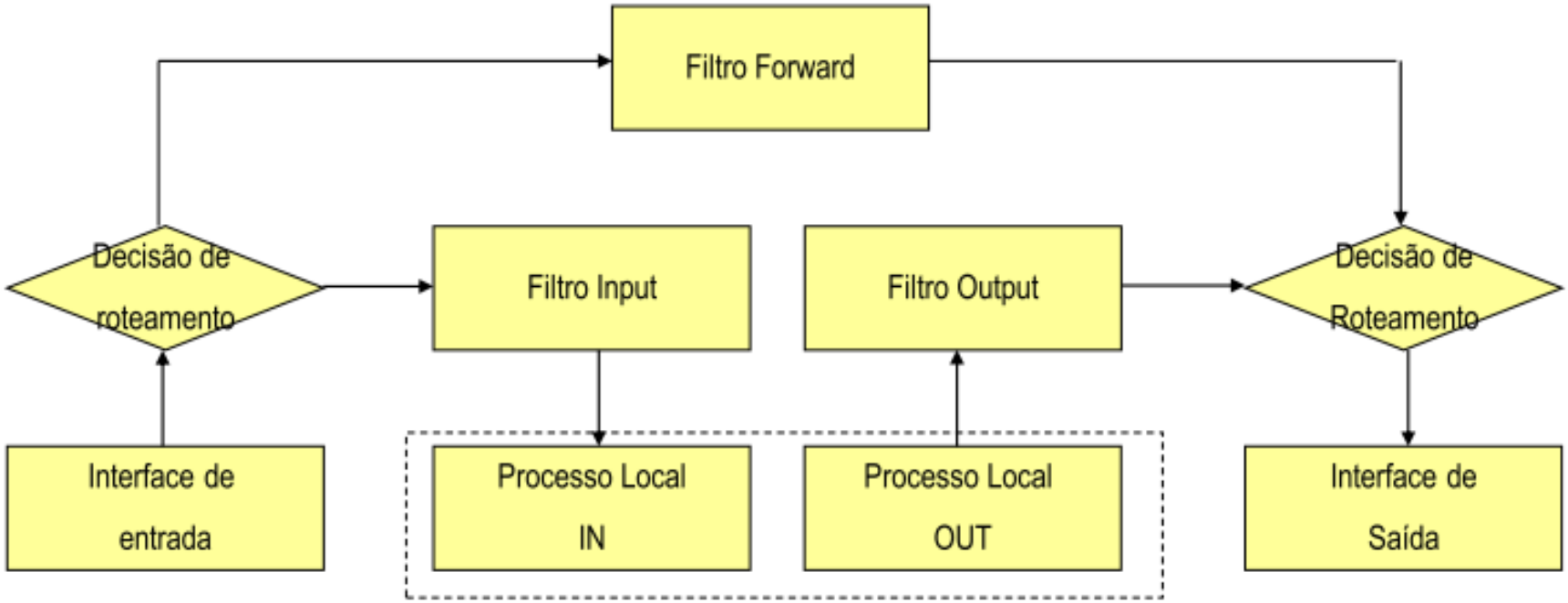
- Regras são organizadas em canais (chains) e existem 3 canais pré definidos:

  → **Input** : responsável pelo tráfego que vai **PARA** o router

  → **Forward** : responsável pelo tráfego que **PASSA** pelo router

  → **Output** : responsável pelo tráfego que **SAI** do router

Diagrama da Estrutura de Filtro



Princípios Gerais de Firewall
Regras

1 - As regras de Firewall são sempre processadas por canal, na ordem que são listadas, ou seja de cima para baixo.

2 - As regras de firewall funcionam como o que em programação chamamos de expressões condicionais , ou seja “se <condição> então <ação>”

3 – Se um pacote não atende TODAS as condições de uma regra ele passa para a regra seguinte.

Princípios Gerais de Firewall
Regras

4 – Quando o pacote atende a TODAS as condições da regra é tomada uma ação com ele, não importam as regras que estejam abaixo nesse canal, pois estas NÃO serão processadas

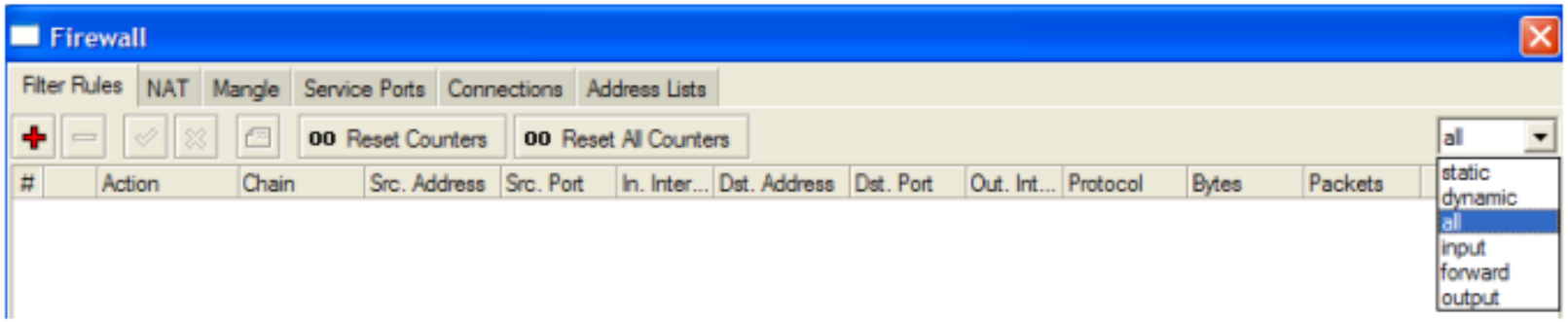
5 – Existem algumas excessões ao critério acima, que são as ações de “passthrough” (passar adiante) , log e add to address list. (visto adiante)

6 - Um pacote que não se enquadre em qualquer regra do canal, será por default aceito.

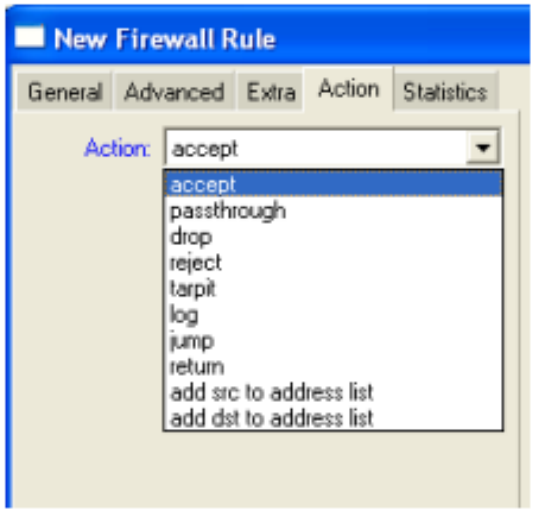
Firewall do Mikrotik – Filter Rules

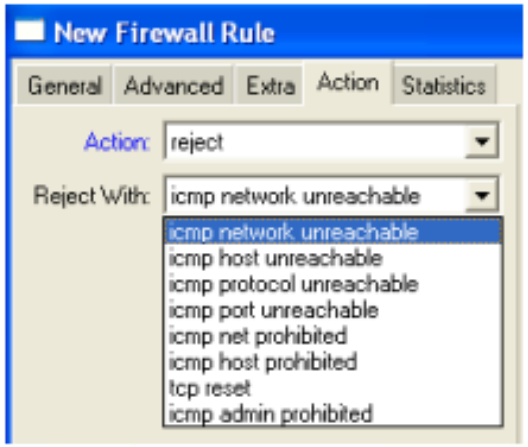
As regras de filtro podem ser organizadas e mostradas das seguintes maneiras:

→ **all:** todas
→ **dynamic:** regras dinâmicamente criadas por serviços (ex. Hotspot)
→ **input:** regras do canal input
→ **output:** regras do canal output
→ **forward:** regras do canal forward



Firewall do Mikrotik – Filter Rules





Algumas ações que se pode tomar nas regras de filtro:

→accept: aceita o pacote

→passthrough: ignora a regra (mas contabiliza) e passa para a regra seguinte

→drop: descarta silenciosamente o pacote

→reject: descarta o pacote e responde com uma mensagem de icmp ou tcp reset (ver ao lado)

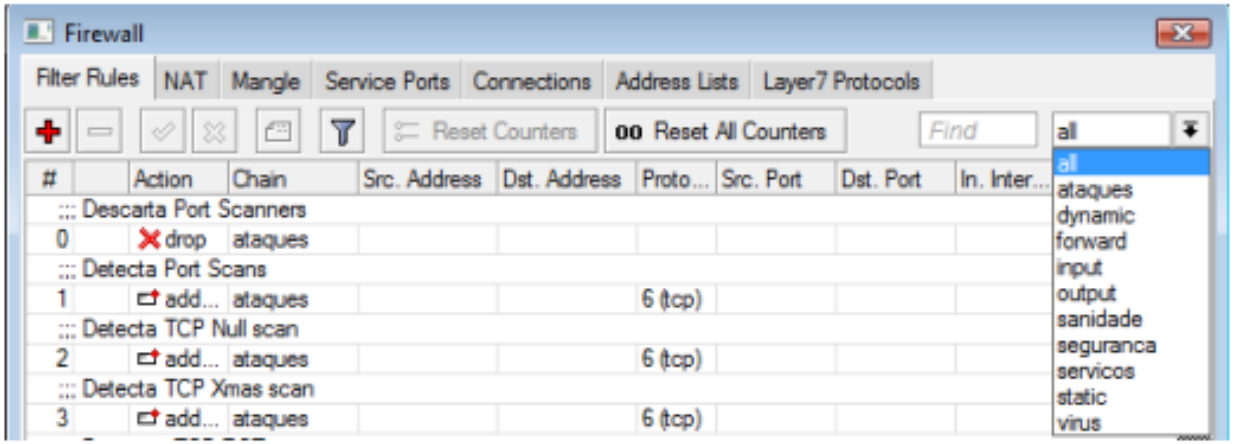
→tarpit: Respondendo com SYN/ACK ao um pacote TCP/SYN entrante, mas não conclui a conexão.

Firewall / Filtro / canais criados pelo usuário

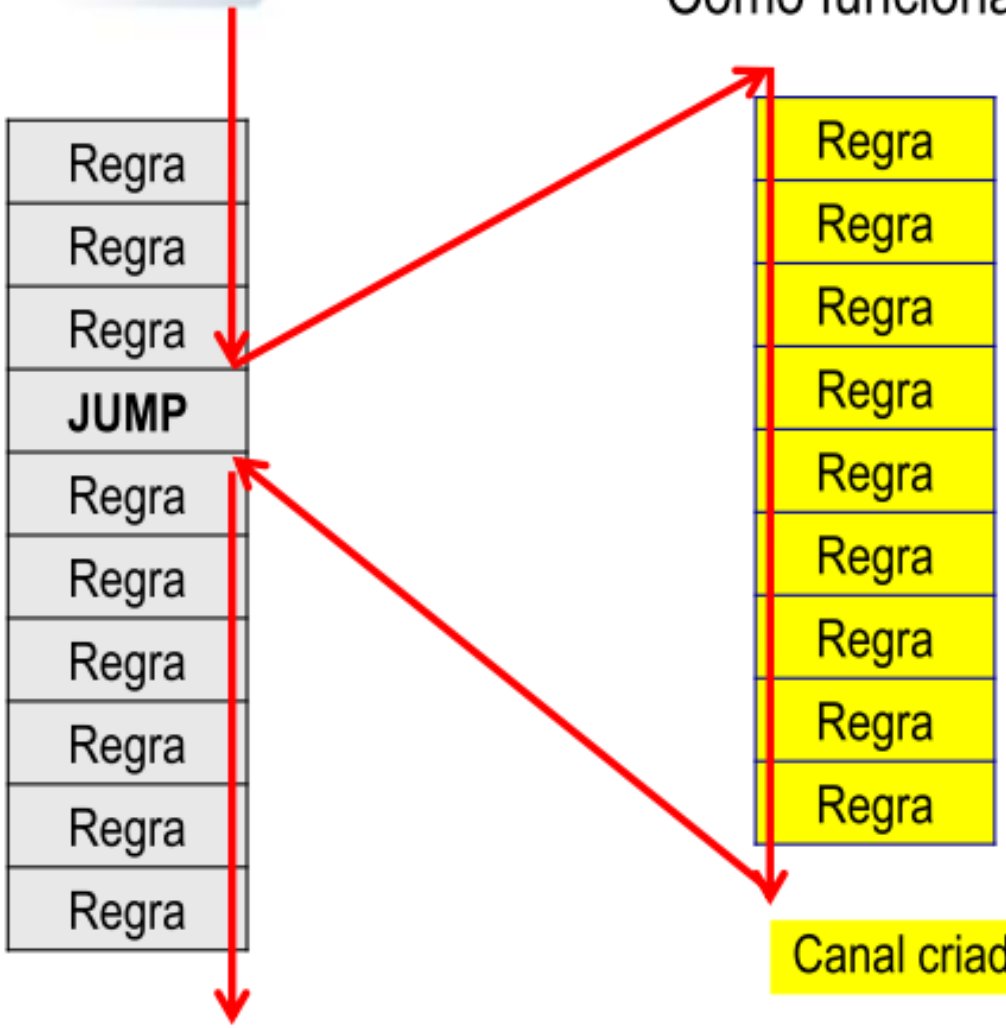
Além dos canais padrão, o administrador pode criar canais próprios, bastando dar nomes a eles. Essa prática ajuda muito na organização do Firewall.

Para utilizar um canal criado devemos desviar o fluxo através de uma ação JUMP..

No exemplo abaixo, além de input, output e forward, estão criados canais chamados sanidade, segurança, vírus, etc.

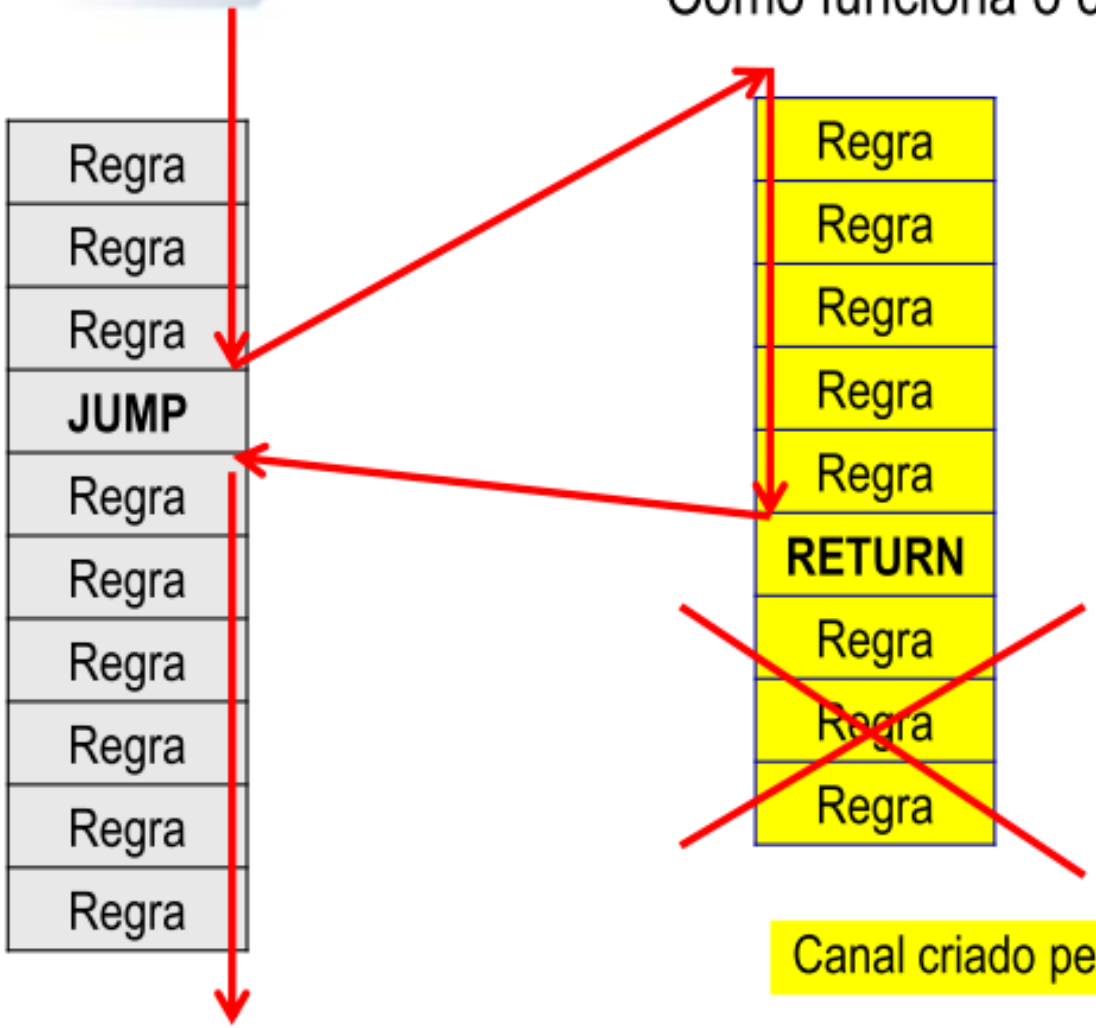


Como funciona o canal criado pelo usuário



Além dos canais padrão, o administrador pode criar canais próprios e associa-los a um canal padrão.

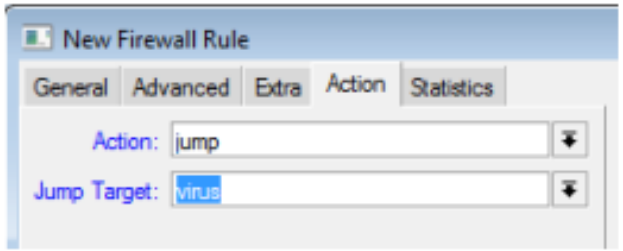
Como funciona o canal criado pelo usuário



Caso exista uma regra que tome a ação RETURN, o retorno é feito antecipadamente e as regras abaixo deste são ignoradas

Canal criado pelo usuário

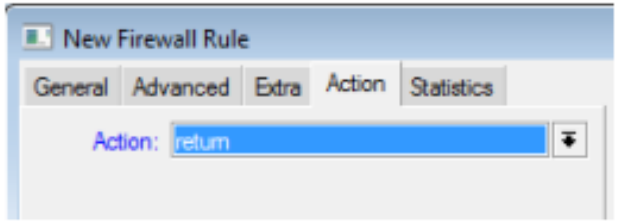
Firewall do Mikrotik – Filter Rules



Ações relativas a canais criados pelo usuário que se pode tomar nas regras de filtro:

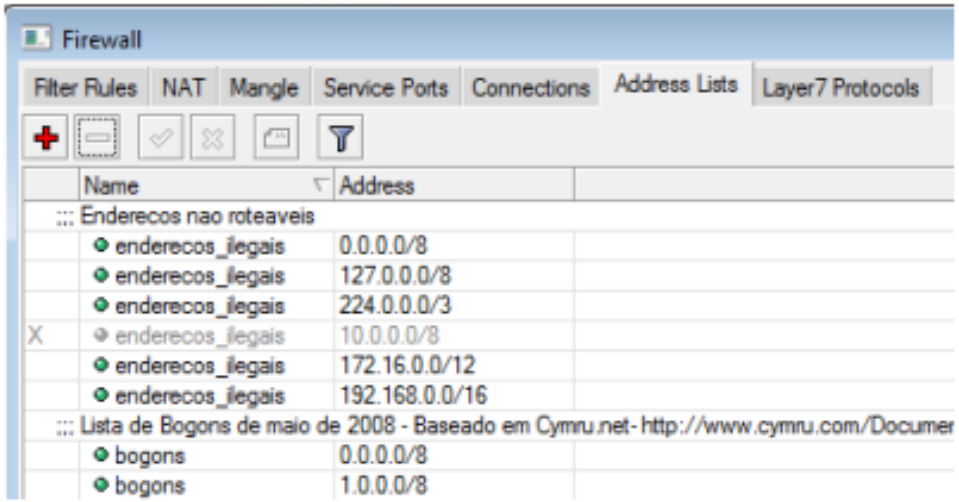
→jump: salta para o canal definido em jump-target

→Jump Target: nome do canal para onde deve saltar



→Return: Volta para o canal que chamou o jump

Firewall do Mikrotik – Address Lists

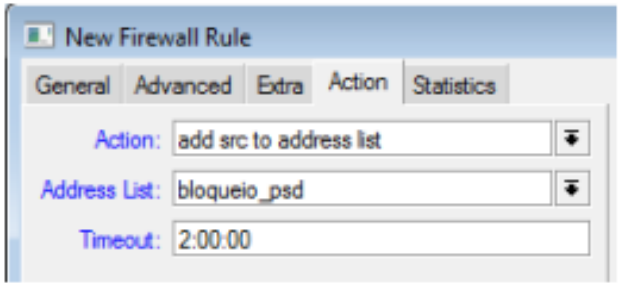


Uma Address List, ou lista de endereços é uma lista de endereços IP que pode ter várias utilizações, conforme serão vistos alguns exemplos mais adiante.

Pode-se adicionar dinamicamente entradas a essas listas no Filtro ou no Mangle.

Ações:

→add dst to address list: adiciona o IP de destino à lista



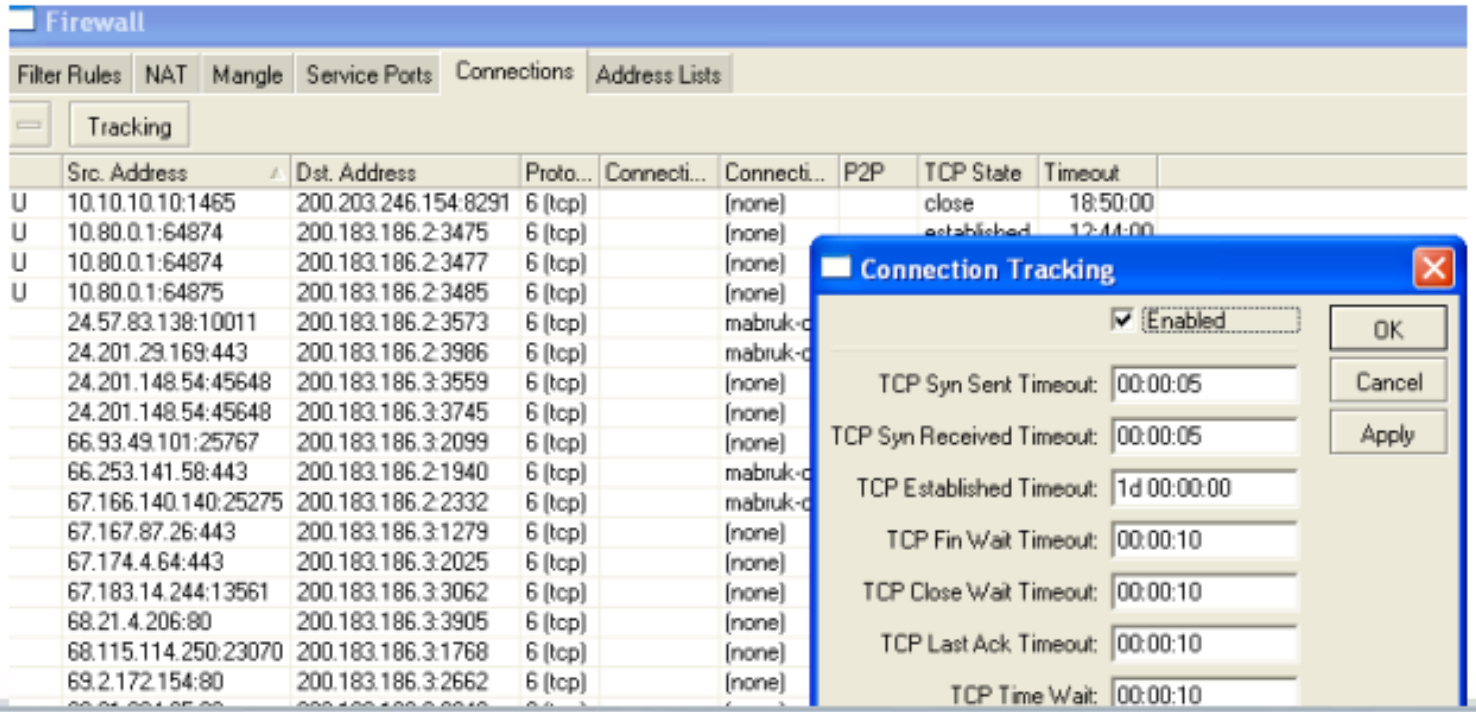
→add src to address list: adiciona o IP de origem à lista

→Address List: nome da lista de endereços

→Timeout: por quanto tempo a entrada irá permanecer

Connection Tracking

Connection Tracking (seguimento de conexões) se refere a habilidade do roteador de manter o estado da informação relativa às conexões, tais como endereços IP de origem ou destino e pares de porta, estados da conexão, tipos de protocolos e timeouts. Firewalls que fazem connection tracking são chamados de "stateful" e são mais seguros que aqueles que fazem o processamento "stateless“

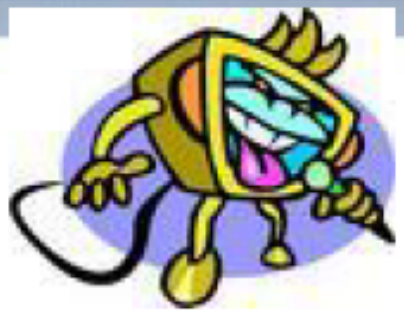


Connection Tracking

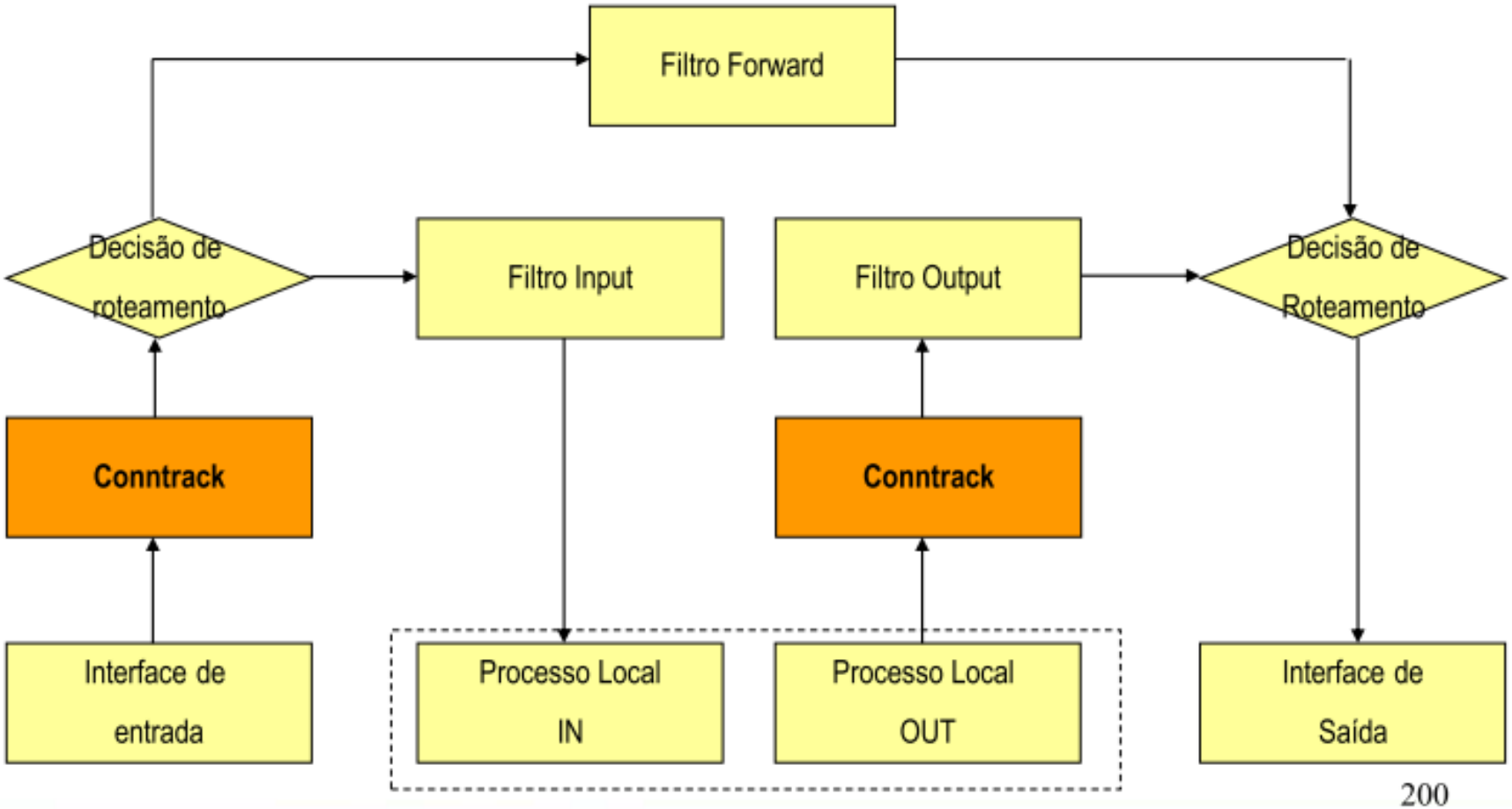
- O sistema de Connection Tracking ou Conntrack é o coração do Firewall. Ele obtem e mantém informações sobre todas as conexões ativas.

- Quando se desabilita a Função de Connection Tracking são perdidas as funcionalidades de NAT e marcação de pacotes que dependam de conexão. Pacotes no entanto podem ser marcados diretamente.

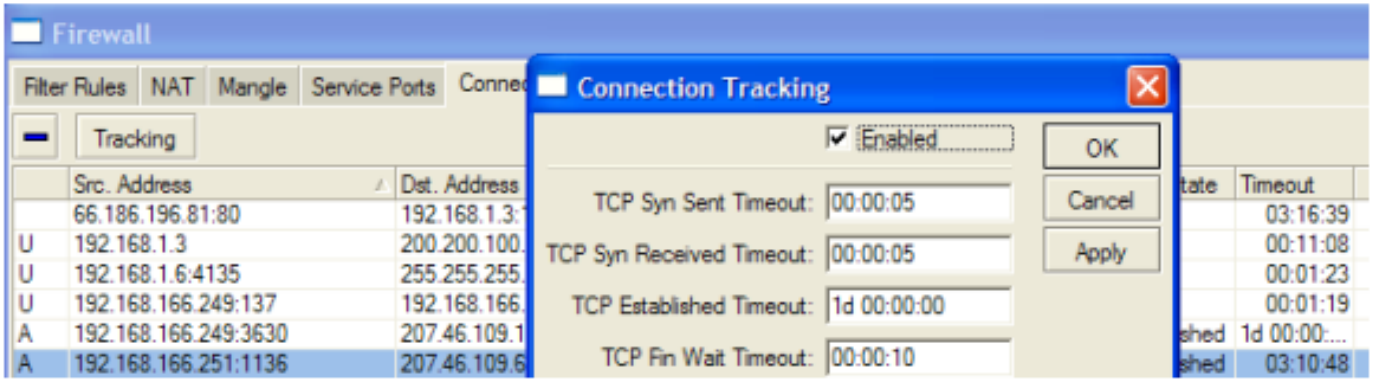
-.Conntrack é exigente de recursos de hardware. Quando o equipamento trabalha apenas como AP Bridge por exemplo, é indicado desabilita-la



Localização da Conntrack



Connection Tracking



O estado de uma conexão pode ser:

→established: significando que o pacote é parte de uma conexão já estabelecida anteriormente

→ new: significando que o pacote está iniciando uma nova conexão ou faz parte de uma conexão que ainda não trafegou pacotes em ambas direções

→ related: significando que o pacote inicia uma nova conexão, mas que essa é associada a uma conexão existente como FTP por exemplo

→invalid: significando que o pacote não pertence à nenhuma conexão conhecida nem está iniciando outra.

Firewall Filter
Protegendo o próprio Roteador e os Clientes

Princípios Básicos de Proteção

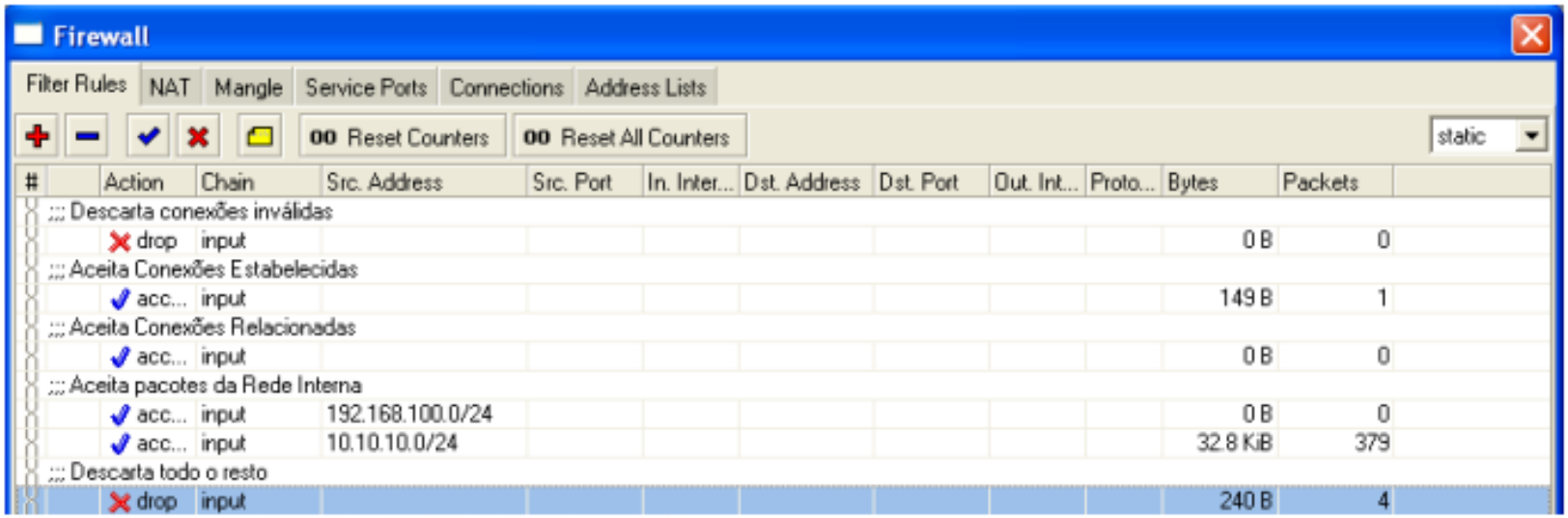
- Proteção do próprio roteador
  - tratamento das conexões e eliminação de tráfego prejudicial/inútil
  - permitir somente os serviços necessários no próprio roteador
  - prevenir e controlar ataques e acesso não autorizado ao roteador

- Proteção da rede interna
  - tratamento das conexões e eliminação de tráfego prejudicial/inútil
  - permitir somente os serviços necessários nos clientes
  - prevenir e controlar ataques e acesso não autorizado em clientes.

Regras de Firewall
tratamento de conexões

Regras no Canal Input

→ Descarta conexões inválidas
→ Aceita conexões estabelecidas
→ Aceita conexões relacionadas
→Aceita todas as conexões da rede interna
→ Descarta o restante

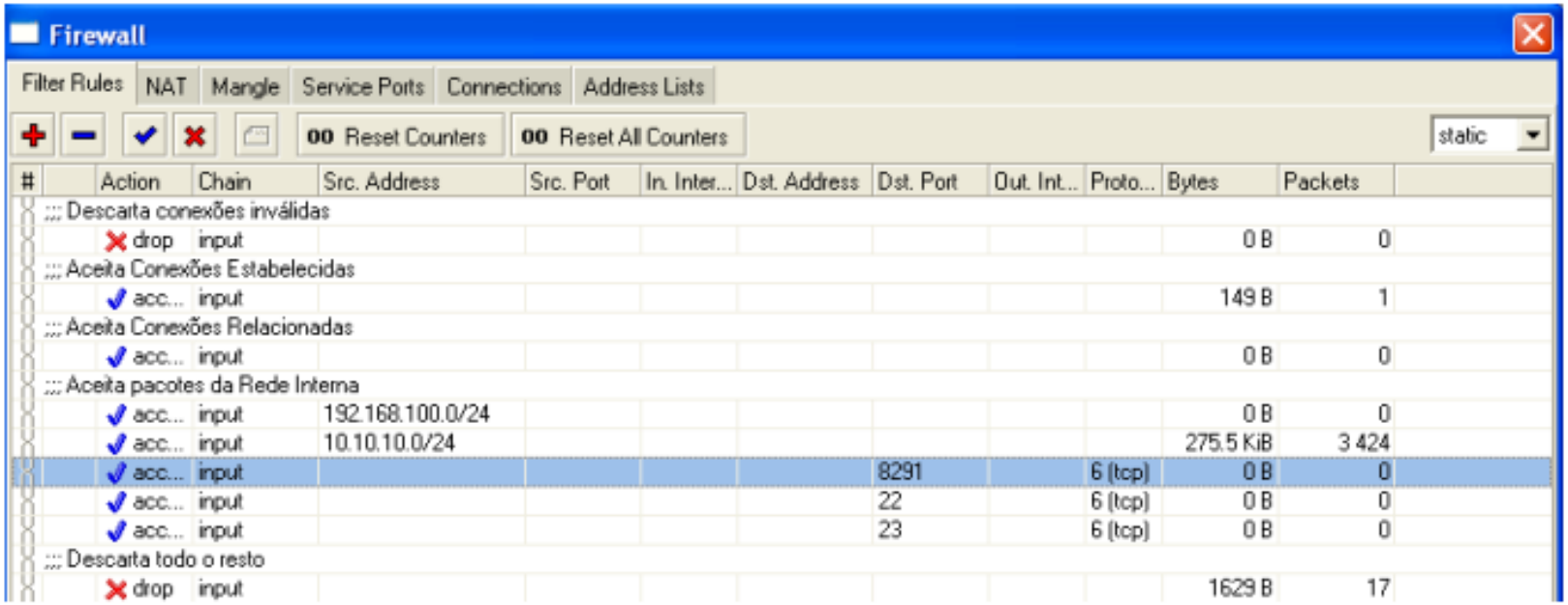


#	Action	Chain	Src. Address	Src. Port	In. Inter...	Dst. Address	Dst. Port	Out. Int...	Proto...	Bytes	Packets
;;; Descarta conexões inválidas											
	drop	input								0 B	0
;;; Aceita Conexões Estabelecidas											
	acc...	input								149 B	1
;;; Aceita Conexões Relacionadas											
	acc...	input								0 B	0
;;; Aceita pacotes da Rede Interna											
	acc...	input	192.168.100.0/24							0 B	0
	acc...	input	10.10.10.0/24							32.8 KiB	379
;;; Descarta todo o resto											
	drop	input								240 B	4

Regras de Firewall
Controle de serviços

Regras no Canal Input – cont.

→ Permitir o acesso externo ao Winbox
→ Permitir acesso externo por SSH
→ Permitir acesso externo por Telnet
→ Relocar as regras para que funcionem



#	Action	Chain	Src. Address	Src. Port	In. Inter...	Dst. Address	Dst. Port	Out. Int...	Proto...	Bytes	Packets
;;; Descarta conexões inválidas											
	drop	input								0 B	0
;;; Aceita Conexões Estabelecidas											
	acc...	input								149 B	1
;;; Aceita Conexões Relacionadas											
	acc...	input								0 B	0
;;; Aceita pacotes da Rede Interna											
	acc...	input	192.168.100.0/24							0 B	0
	acc...	input	10.10.10.0/24							275.5 KiB	3 424
	acc...	input					8291		6 (tcp)	0 B	0
	acc...	input					22		6 (tcp)	0 B	0
	acc...	input					23		6 (tcp)	0 B	0
;;; Descarta todo o resto											
	drop	input								1629 B	17

Regras de Firewall
Filtrando tráfego prejudicial/inútil

Filtros de portas de vírus

→Bloqueia portas mais populares utilizadas por vírus TCP e UDP 445 e 137-139

→No momento existem algumas centenas Trojans ativos e menos de 50 tipos de vírus ativos

→ No site da Mikrotik há uma lista com as portas e protocolos que utilizam esses vírus.

→Baixar lista de vírus Mikrotik e fazer as regras de acordo

Regras de Firewall
Filtrando tráfego indesejável e possíveis ataques

Controle de ICMP

-Internet Control Message Protocol (ICMP) é basicamente uma ferramenta para diagnóstico da rede e alguns tipos de ICMP obrigatoriamente devem ser liberados.

-Um roteador tipicamente utiliza apenas 5 tipos de ICMP (type:code), que são:

- PING – Mensagens 0:0 e 8:0
- TRACEROUTE – Mensagens 11:0 e 3:3
- PMTUD – Path MTU discovery – mensagem 3:4

Os outros tipos de ICMP podem ser bloqueados.

Regras de Firewall
Filtrando tráfego indesejável

IP's Bogons:

→ Existem mais de 4 milhões de endereços IPV4

→ Existem muitos ranges de IP restritos em redes públicas

→Existem várias ranges de IP's reservados (não usados até o momento) para propósitos específicos.

→No material do curso está disponível uma Lista de IP's Bogons atualizada em maio de 2008, baseado no site Cymru que mantém a movimentação desses IP's atualizada.

http://www.cymru.com/Documents/bogon-dd.html

IP's Privados:

→ Muitos aplicativos mal configurados geram pacotes destinados a IP's privados e é uma boa prática filtra-los.

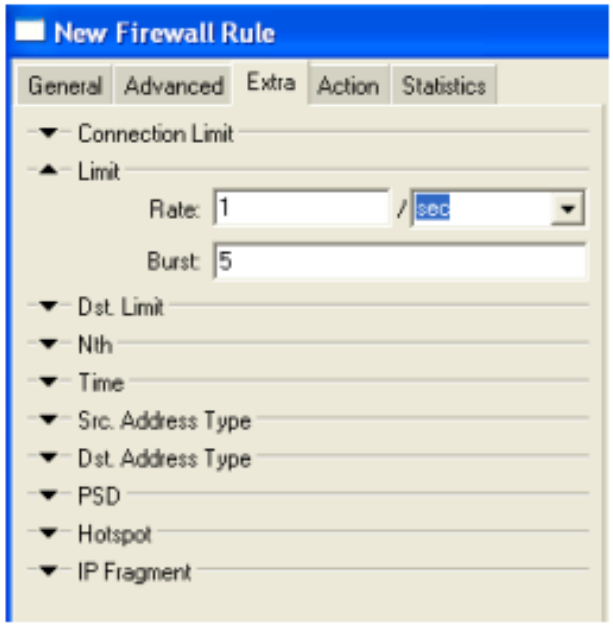
Firewall
Proteções de ataques

Ping Flood

→Ping Flood consiste usualmente de grandes volumes de mensagens de ICMP aleatórias

→É possível detectar essa condição com a regra ao lado

→Interessante associar essa regra com uma de log



Firewall - Proteções de ataques

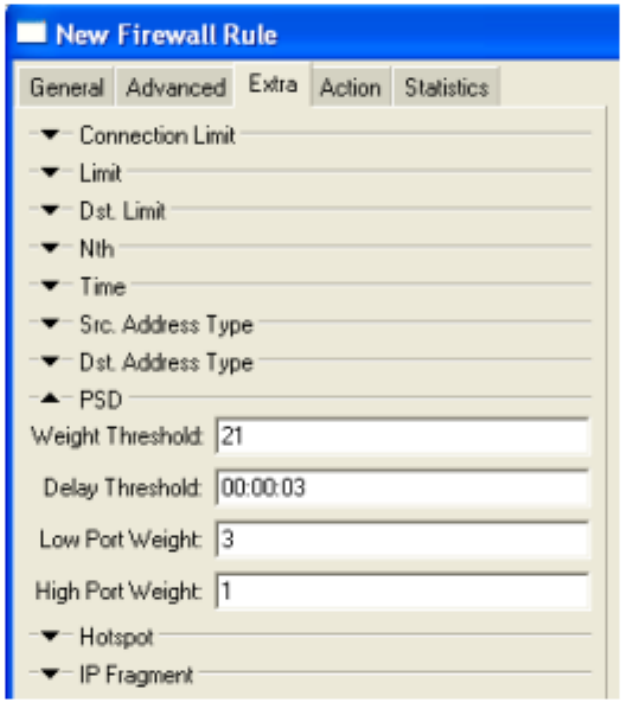
Port Scan

→Consiste no escaneamento de portas TCP e UDP

→A detecção somente é possível para ataques de TCP

→Portas baixas (0 – 1023)

→Portas altas (1024 – 65535)



Firewall - Proteções de ataques DoS

→O Principal objetivo do ataque de DoS é o consumo de recursos como CPU ou largura de banda.

→Usualmente o roteador é inundado com requisições de conexões TCP/SYN causando a resposta de TCP/SYN-ACK e a espera do pacote de TCP/ACK

→Normalmente não é intencional e é causada por vírus em clientes

→Todos IP's com mais de 10 conexões com o roteador podem ser considerados atacantes .

Firewall - Proteções de ataques DoS

Ataques DoS - cont

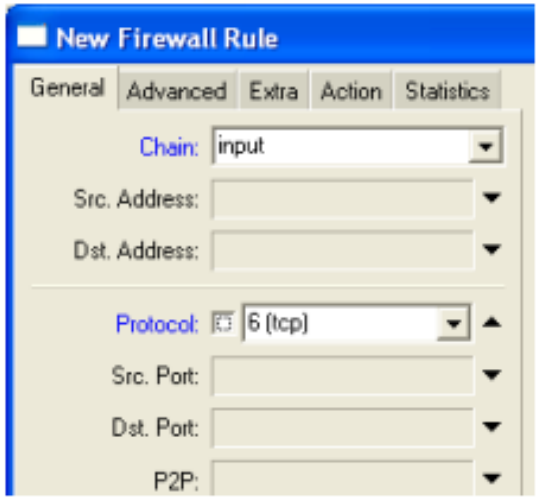
→Se simplesmente descartarmos as conexões, permitiremos que o atacante crie uma nova conexão.

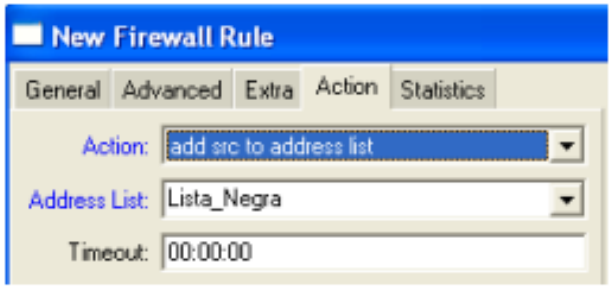
→A proteção pode ser implementada em dois estágios:

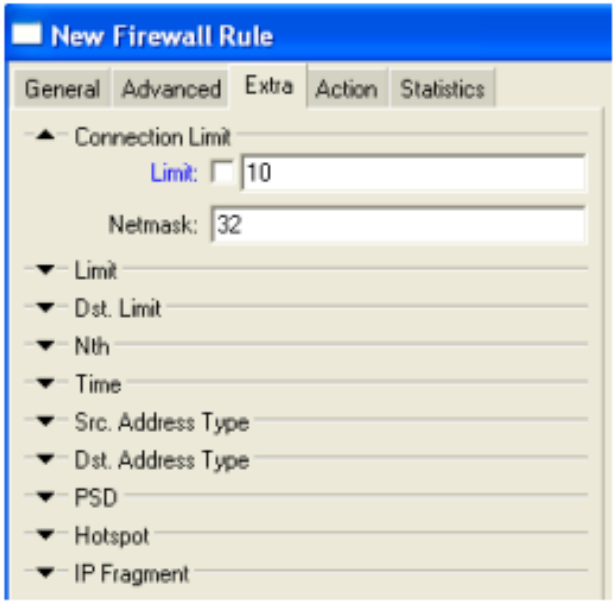
→ Detecção – criando uma lista dos atacantes DoS com base em connection limit

→Supressão – aplicando restrições aos que forem detectados.

Firewall - Proteções de ataques DoS



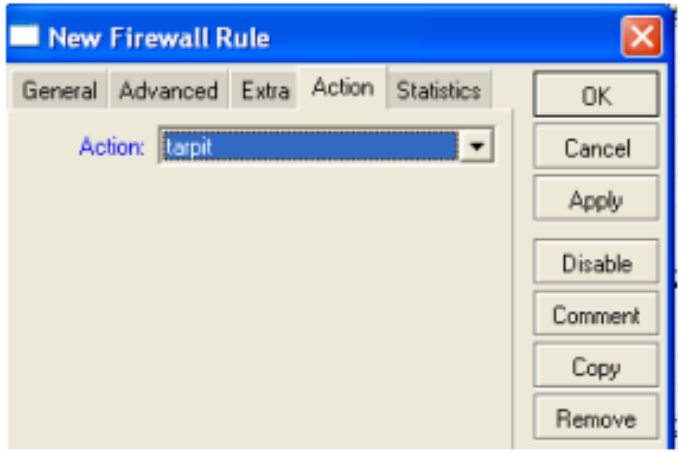




Firewall - Proteções de ataques DoS

- Com a ação tarpit aceitamos a conexão e a fechamos, não deixando no entanto o atacante trafegar.

- Esta regra deve ser colocada antes da regra de detecção ou então a address list vai reeescreve-la todo o tempo.

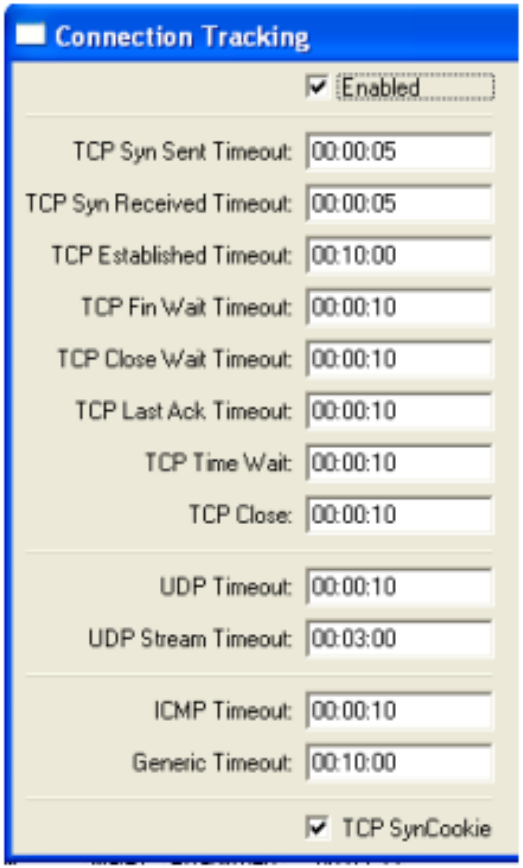


Firewall
Proteções de ataques

dDOS

→Ataques de dDos (dDoS) são bastante parecidos com os de DoS, porém partem de um grande número de hosts infectados

→A única medida que podemos tomar é habilitar a opção TCP syn cookie no connection tracking do Firewall



Firewall do Mikrotik – NAT

NAT – Network Address Translation é uma técnica que permite que hosts em uma LAN usem um conjunto de endereços IP para comunicação interna e outro para comunicação externa.

Existem dois tipos de NAT:

→ Source Nat (srcnat), ou NAT de origem, quando o roteador reescreve o IP de origem e ou a porta por um outro IP de destino.

→ Destination NAT (dstnat), ou NAT de destino quando o roteador reescreve o endereço ou a porta de destino.

Firewall do Mikrotik – NAT

As regras de NAT são organizadas em canais:

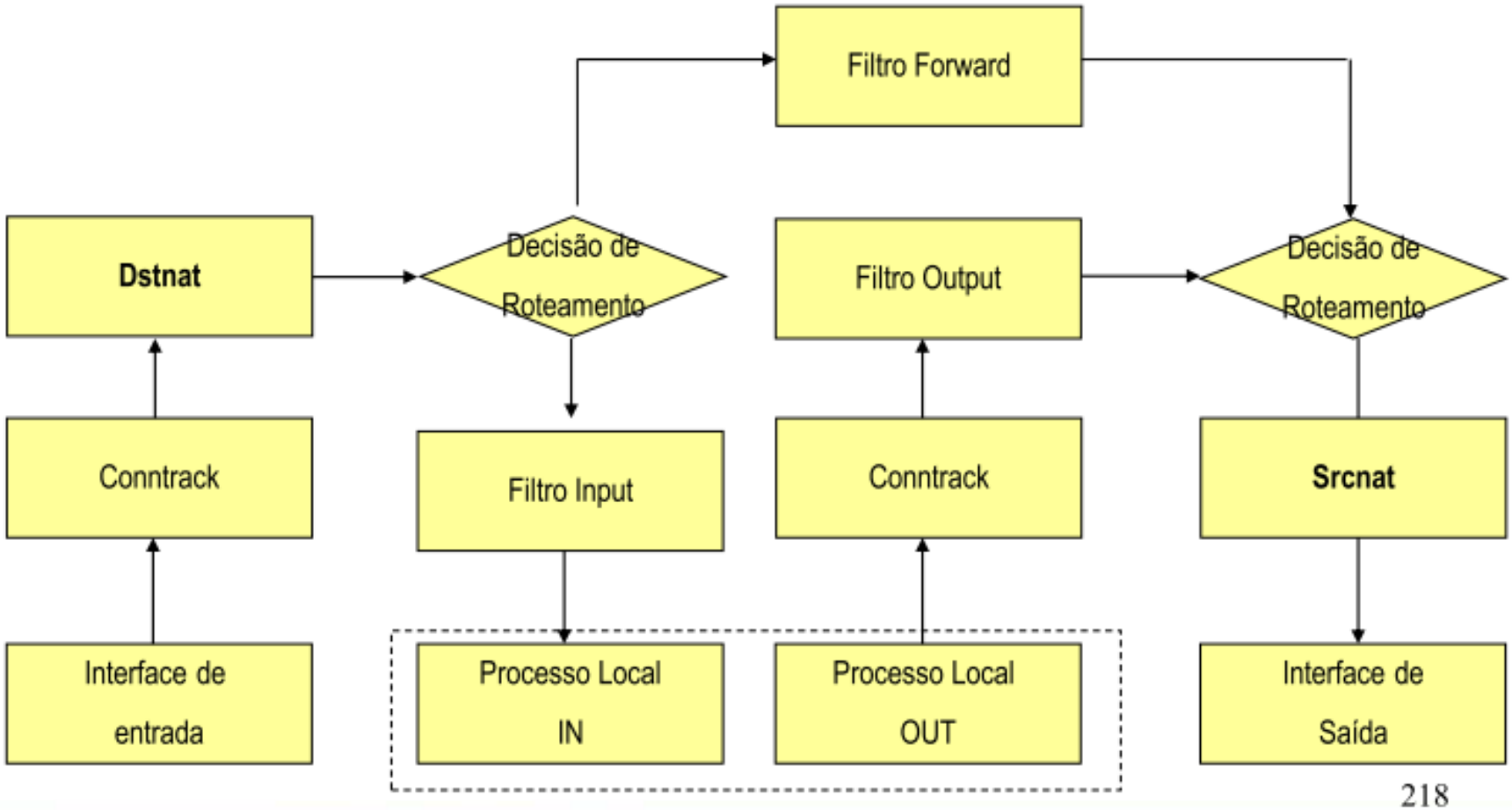
→dstnat:

Processa o tráfego mandado PARA o roteador e ATRAVÉS do roteador, antes que ele seja dividido em INPUT e FORWARD.

→src-nat:

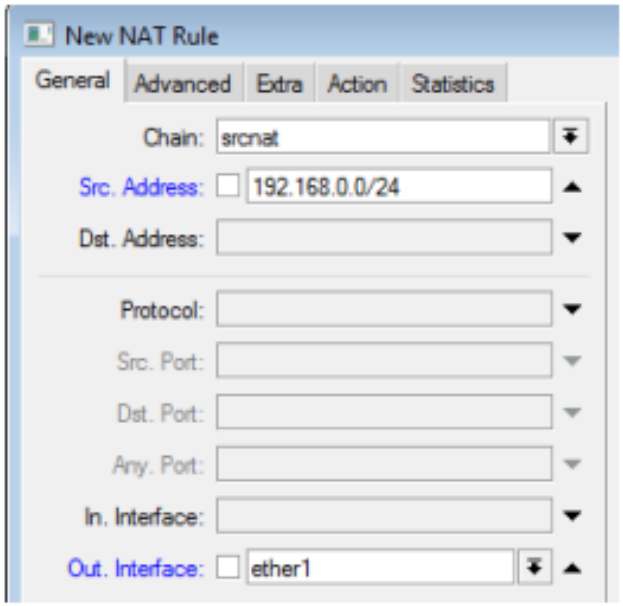
Processa o tráfego mandado a PARTIR do roteador e ATRAVÉS do roteador, depois que ele sai de OUTPUT e FORWARD

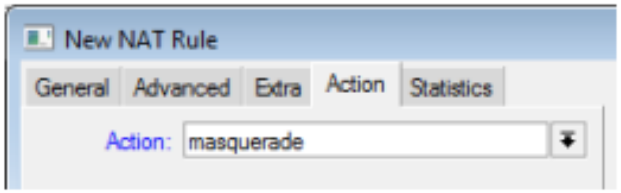
NAT


Filtro Forward
Dstnat
Decisão de Roteamento
Filtro Output
Decisão de Roteamento
Conntrack
Filtro Input
Conntrack
Srcnat
Interface de entrada
Processo Local IN
Processo Local OUT
Interface de Saída

NAT - Exemplos

Source NAT - Mascarando a rede 192.168.0.0/24 atrás do IP 200.200.200.200 que está configurado na interface ether1

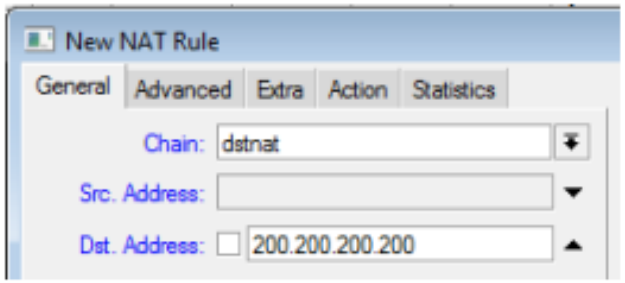


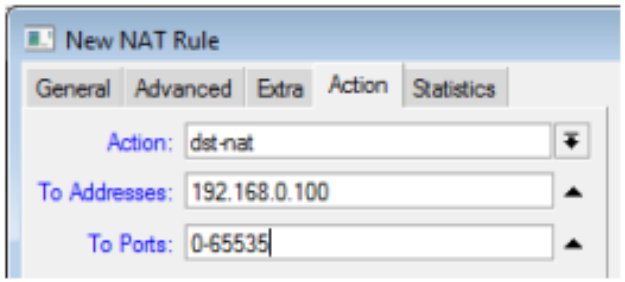


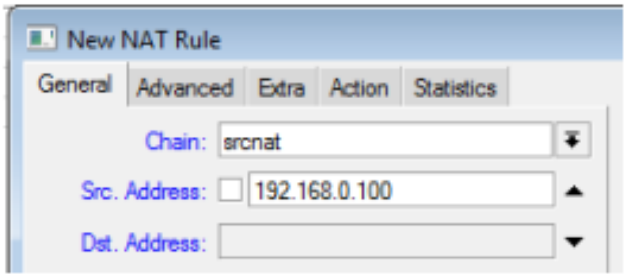
Os pacotes de qualquer host da rede 192.168.0.0/24 sairão com o IP 200.200.200.200

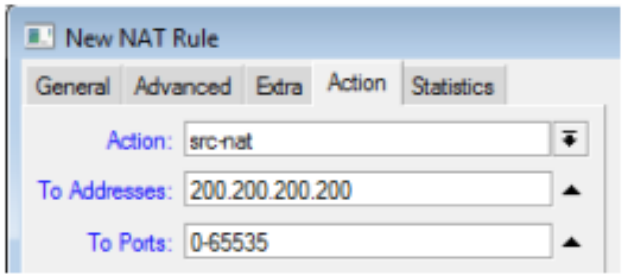
NAT - Exemplos

Destination NAT e Source NAT (1:1) – Apontando o IP 200.200.200.200 para o host interno 192.168.0.100



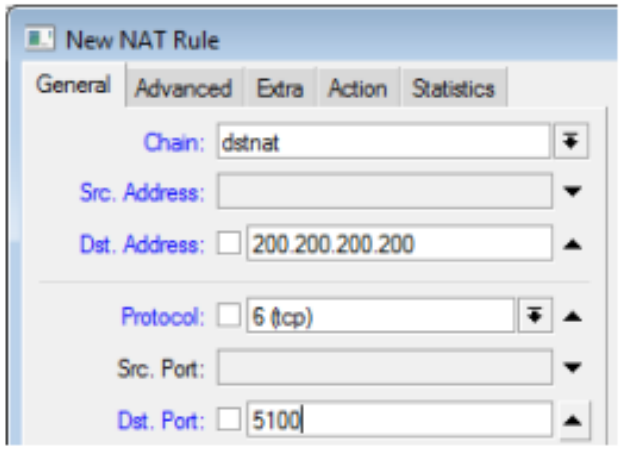


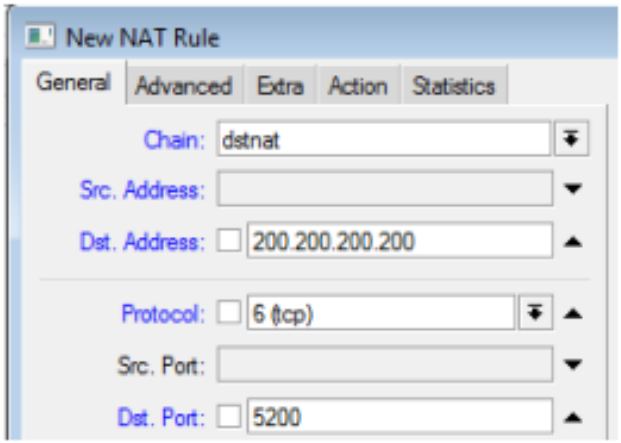


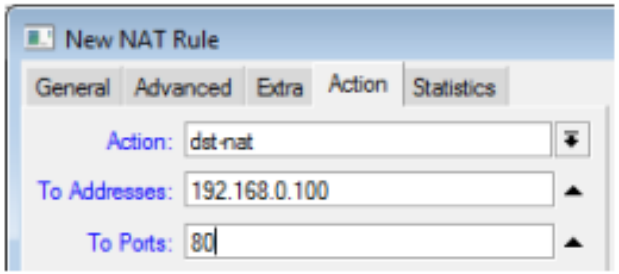


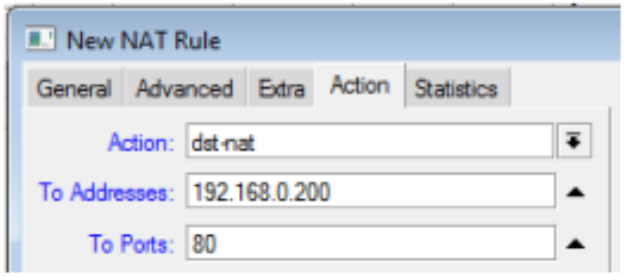
NAT - Exemplos

"Redirecionamento de Portas": Fazendo com que tudo que chegue na porta 5100 vá para o servidor WEB que está na máquina interna 192.168.0.100 e tudo que chegar na porta 5200 vá para a máquina 192.168.0.200



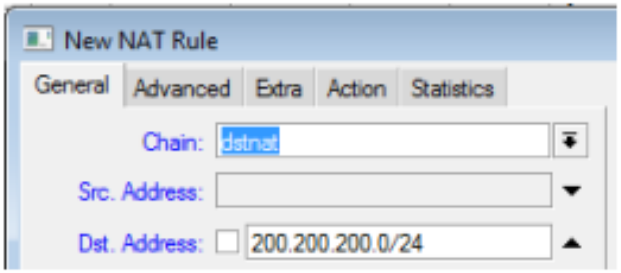


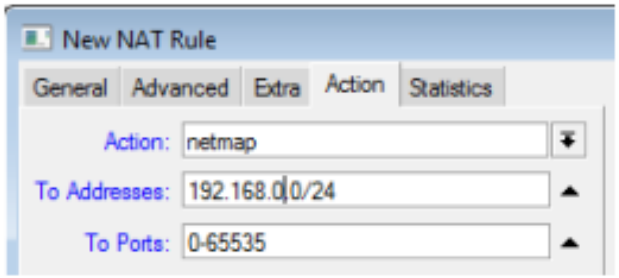


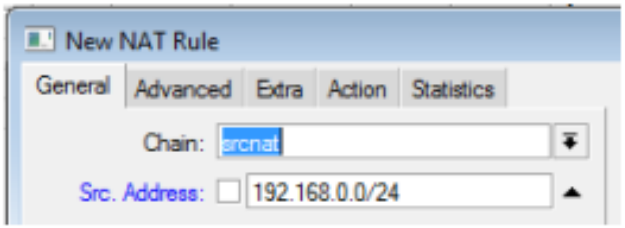


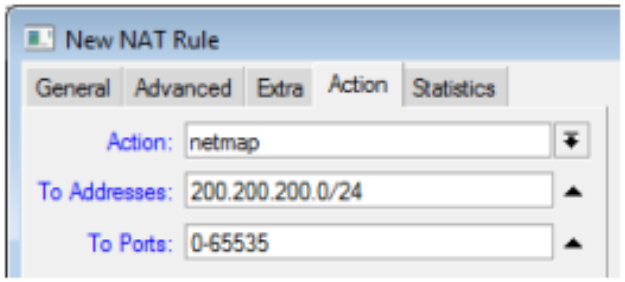
NAT - Exemplos

NAT 1:1 com netmap: Apontando a rede interna 192.168.0.0/24 para a rede pública 200.200.200.200/24









Firewall do Mikrotik – NAT

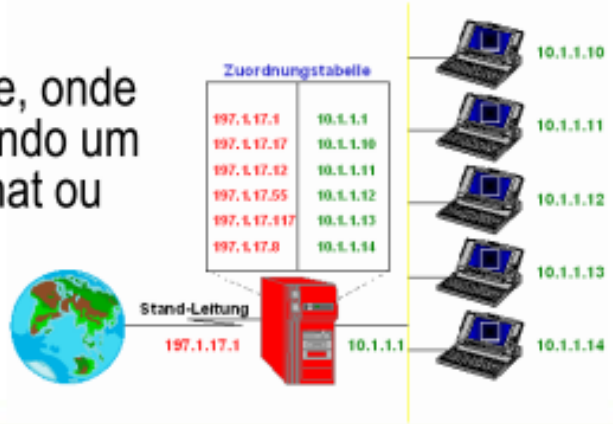
NAT Helpers

Hosts em uma rede “nateada” não possuem conectividade fim-a-fim verdadeira. Por isso alguns protocolos podem não trabalhar satisfatóriamente em alguns cenários. Serviços que requerem a iniciação de conexões TCP de for a da rede, bem como protocolos “stateless” como o UDP por exemplo, podem não funcionar.

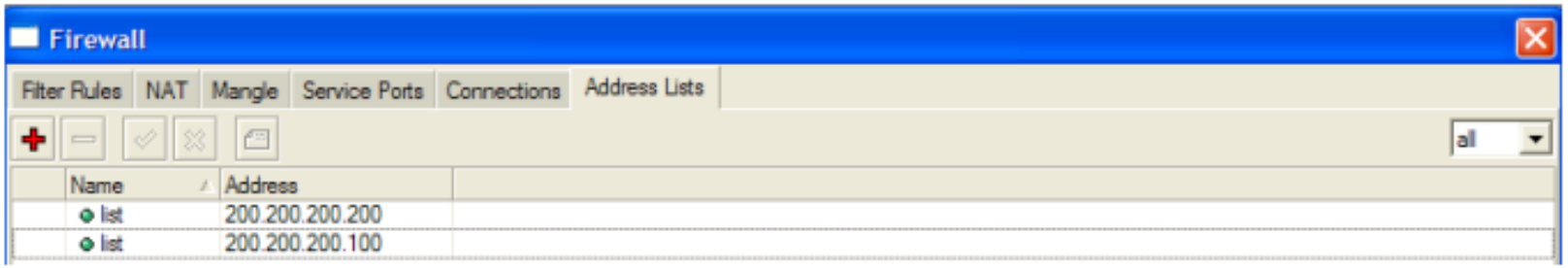
Para contornar esses problemas, a implementação de NAT no Mikrotik prevê alguns “NAT helpers” que tem a função de auxiliar nesses serviços.

Redirecionamento e Mascaramento

São formas especiais de de dstnat e srcnat respectivamente, onde não se especifica para onde vai o pacote (to-address). Quando um pacote é “nateado” como dst-nat, não importa se a ação é nat ou redirect que o IP de destino é automáticamente modificado.



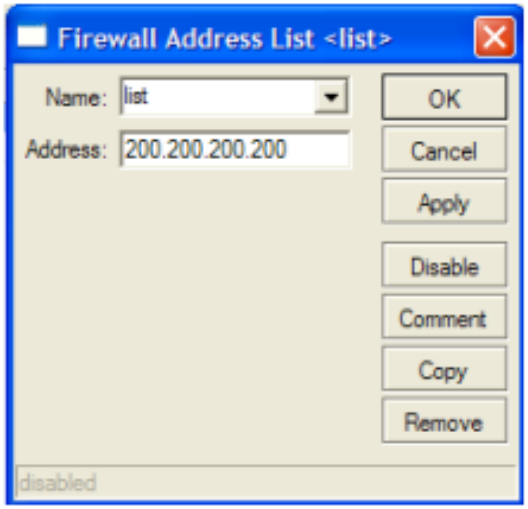
Address Lists



Address Lists permitem que o usuário crie listas de endereços IP agrupados entre si. Estes podem ser utilizados pelo filtro do Firewall, Mangle e NAT.

Os registros de Address Lists podem ser atualizados dinamicamente via action=add-src-to-address-list ou action=add-dst-to-address-list, opções encontradas em NAT, Mangle ou Filter.

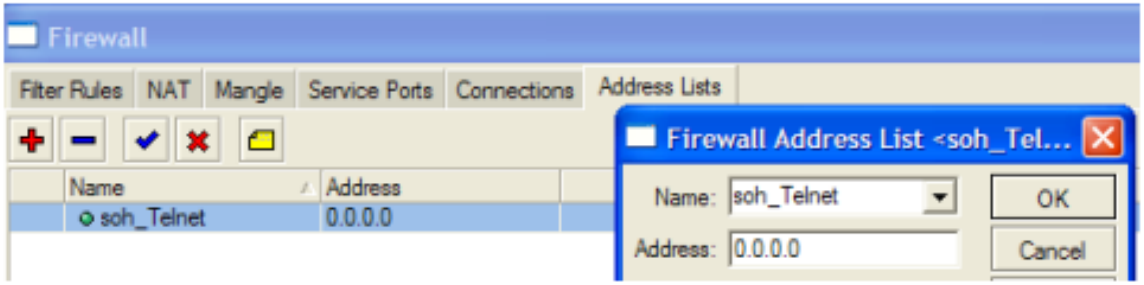
No Winbox é possível editar o nome da lista, simplesmente digitando-o



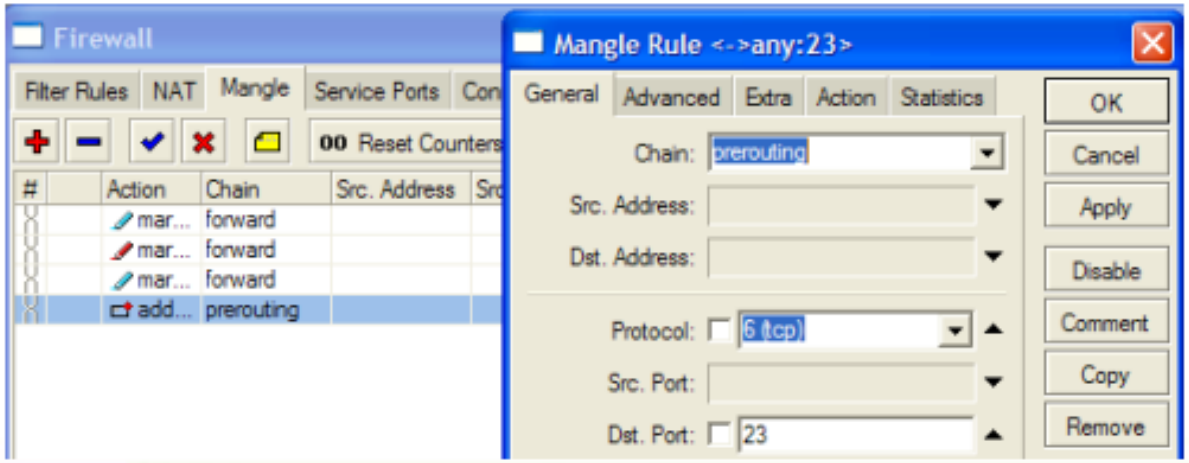
Address Lists - Exemplo

Penalizar o usuário que tentar dar um Telnet no Roteador. Fazer com que esse usuário não faça mais nada.

- cria-se as listas no Address list com o IP e da-se um nome para a lista (soh_Telnet)

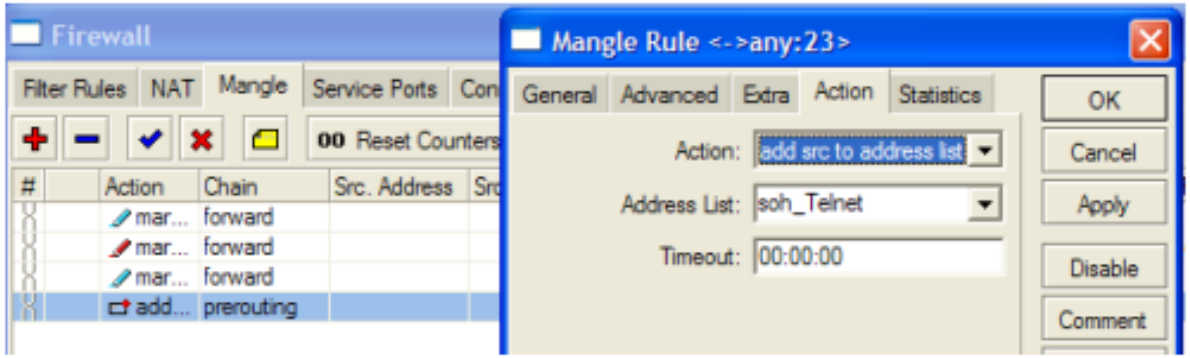


- marca-se no mangle no canal prerouting o protocolo TCP e porta 23

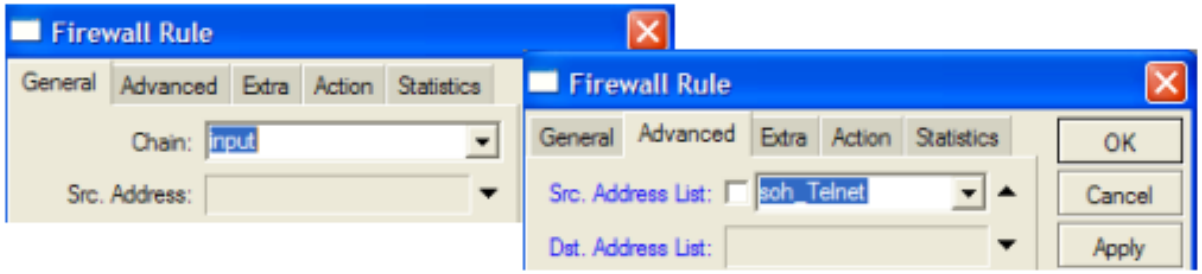


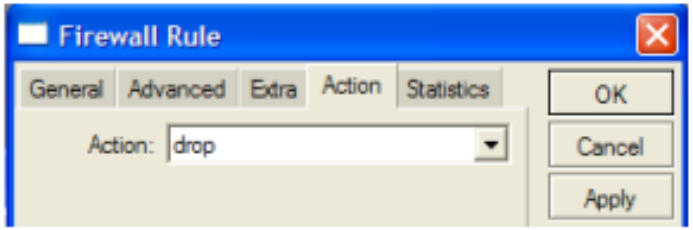
Address Lists - Exemplo

- Ainda no Mangle, adiciona-se a ação add-source ao address list chamado soh_telnet



- Nas regras de filtro, no canal input pega-se os pacotes que estão na lista soh_telnet e escolhe-se a ação drop.





Knock.exe 192.168.0.2 1234:tcp 4321:tcp

Firewall Rule <!1234>

General | Advanced | Extra | Action | Statistics

Chain: input
Src. Address:
Dst. Address:
Protocol: 6 (tcp)
Src. Port:
Dst. Port: 1234

Firewall Rule <!1234>

General | Advanced | Extra | Action | Statistics

Action: add src to address list
Address List: temp
Timeout: 00:00:15

Firewall Rule <!4321>

General | Advanced | Extra | Action | Statistics

Chain: forward
Src. Address:
Dst. Address:
Protocol: 6 (tcp)
Src. Port:
Dst. Port: 4321

Firewall Rule <!4321>

General | Advanced | Extra | Action | Statistics

Src. Address List: temp
Dst. Address List:

Firewall Rule <!4321>

General | Advanced | Extra | Action | Statistics

Action: add src to address list
Address List: liberado
Timeout: 00:00:00

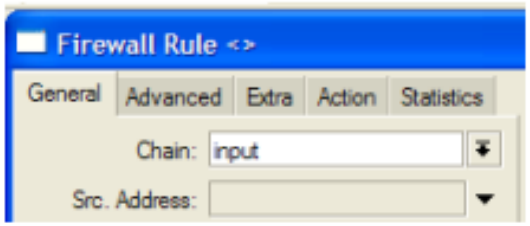
Knock.exe 192.168.0.2 1234:tcp 4321:tcp

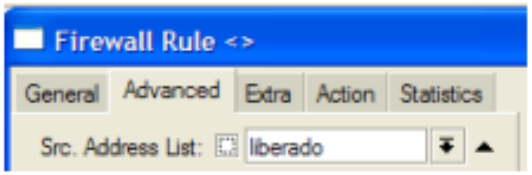
/ip firewall rule

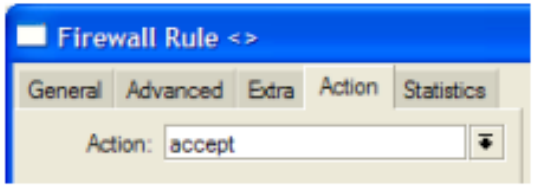
add chain=input dst-port=1234 protocol=tcp action=add-src-to-address-list address-list=temp address-list-timeout=15s

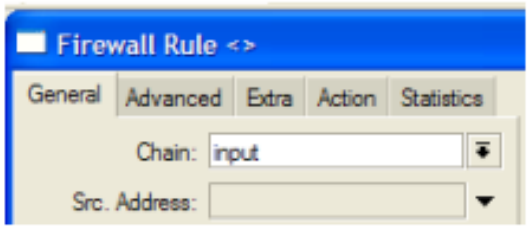
add chain=forward dst-port=4321 protocol=tcp src-address-list=temp action=add-src-to-address-list address-list=liberado address-list-timeout=15m

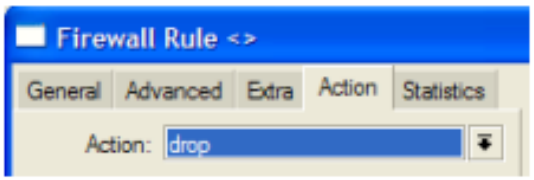
Liberando o acesso para quem estiver na lista e negando para o resto







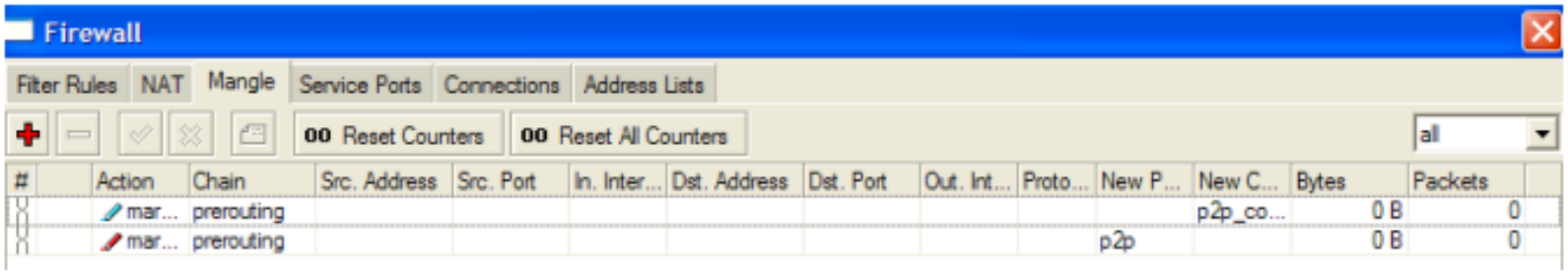




8		acc...	input								0 B	0
9		drop	input								47.1 KiB	475

FIREWALL MANGLE

Firewall do Mikrotik – Mangle



A Facilidade Mangle apresentada no RouterOS do Mikrotik permite introduzir marcas em conexões e em pacotes IP em função de comportamentos específicos.

As marcas introduzidas pelo Mangle são utilizadas em processamento futuro e delas fazem uso ferramentas como o controle de banda, ferramentas de QoS e NAT. Elas existem porém somente dentro do roteador, não sendo transmitidas para for a.

É possível porém com o Mangle alterar determinados campos no cabeçalho IP, como o ToS (type of service) e campos de TTL (Time to live)

Estrutura do Mangle

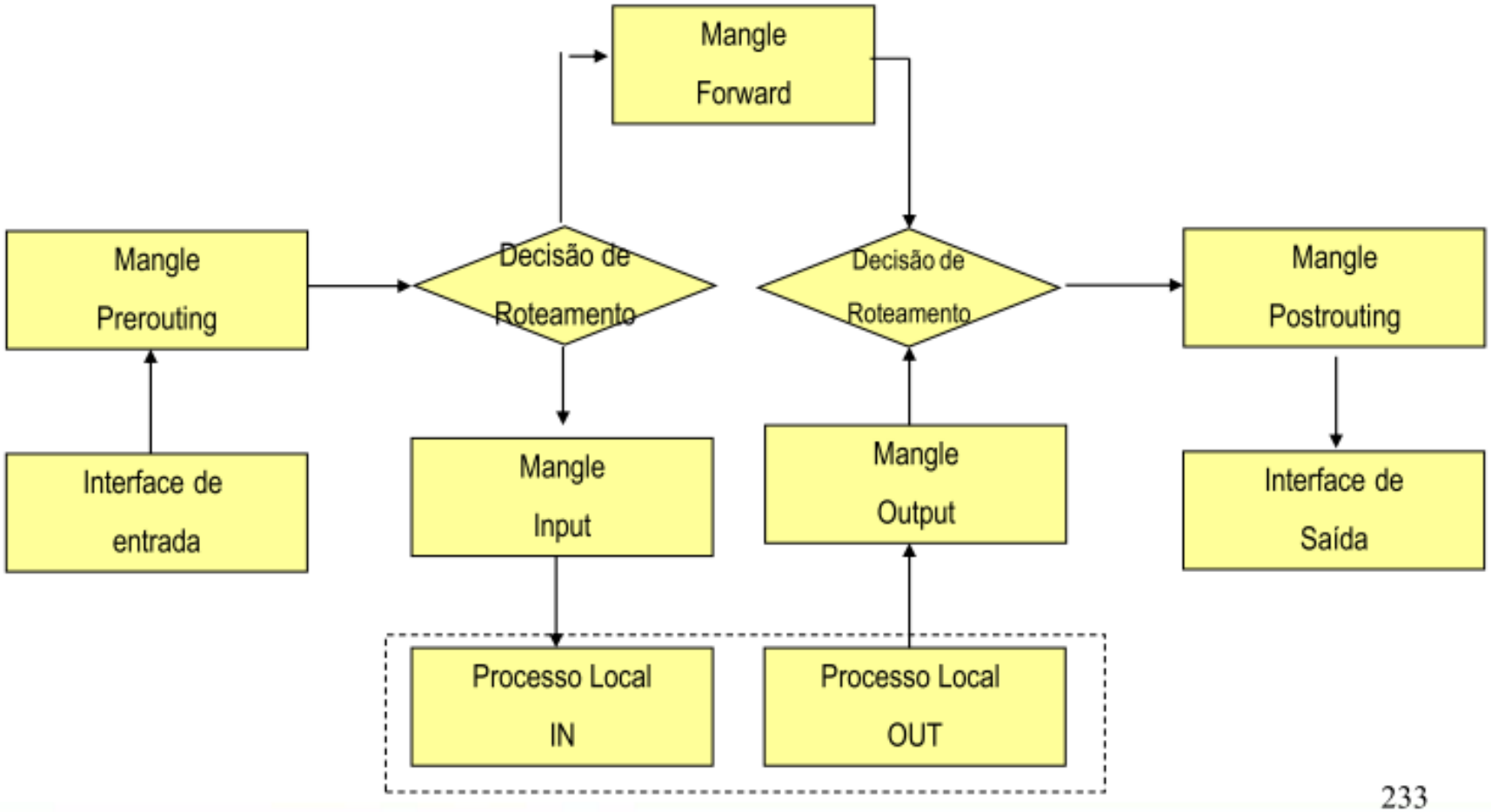
→As regras de Mangle são organizadas em canais e obedecem as mesmas regras gerais das regras de filtros, quanto a sintaxe.

→ É possível também criar canais pelo usuário

→ Há 5 canais padrão:

- → Prerouting: marca antes da fila Global-in
- → Postrouting: marca antes da fila Global-out
- → Input: marca antes do filtro de Input
- → Output: marca antes do filtro Output
- →Forward: marca antes do filtro Forward

Diagrama do Mangle



Açoes do Mangle

As opções de marcação incluem:

→mark-connection – apenas o primeiro pacote.

→mark-packet – marca um fluxo (todos os pacotes)

→mark-routing – marca pacotes para políticas de roteamento

Marcando Conexões

→Use mark-connection para identificar um ou um grupo de conexões com uma marca específica de conexão.

→ Marcas de conexão são armazenadas na tabela de connection tracking.

→Só pode haver uma marca de conexão para uma conexão.

→A facilidade Connection Tracking ajuda a associar cada pacote a uma conexão específica.

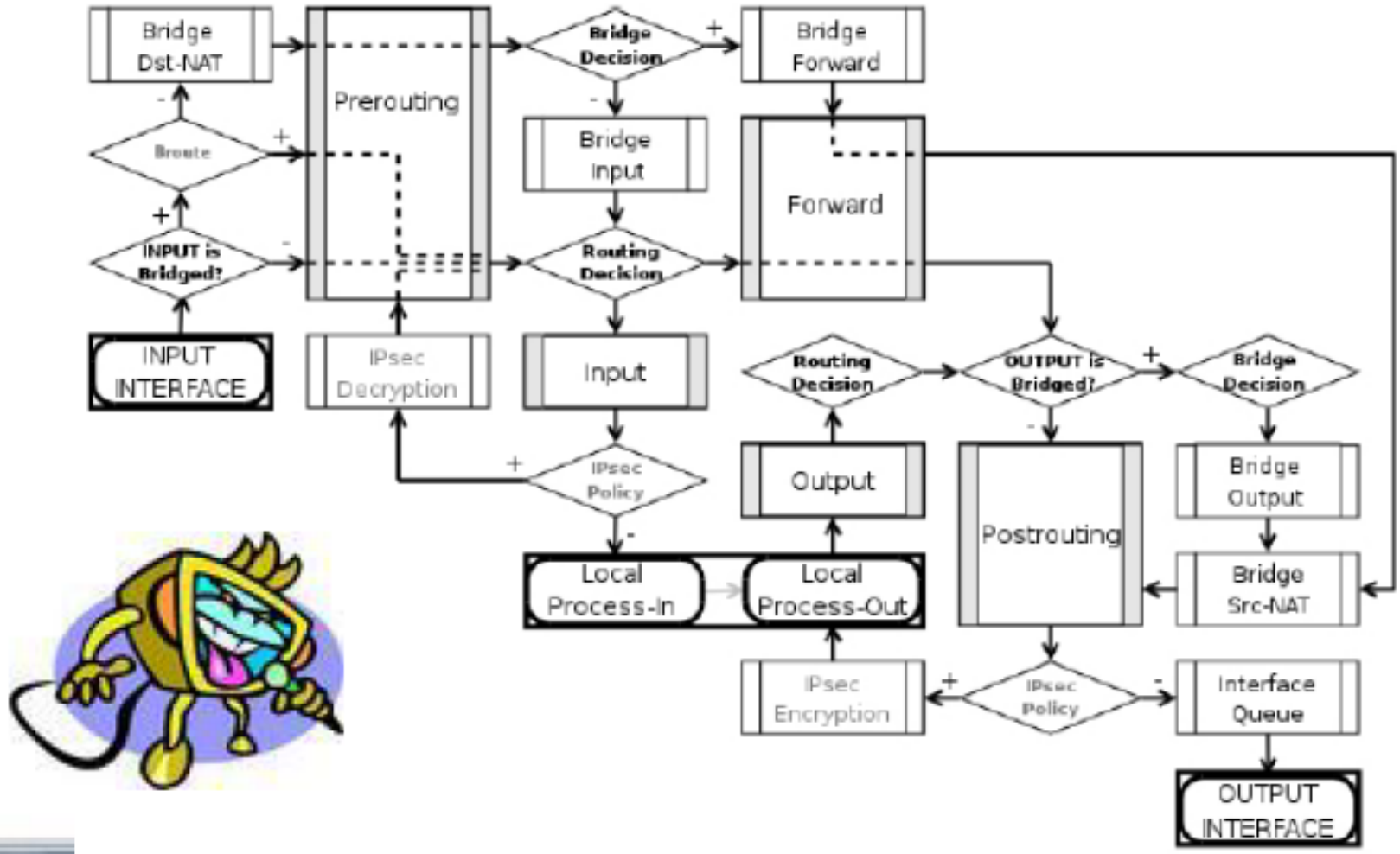
Marcando Pacotes

Pacotes podem ser marcados:

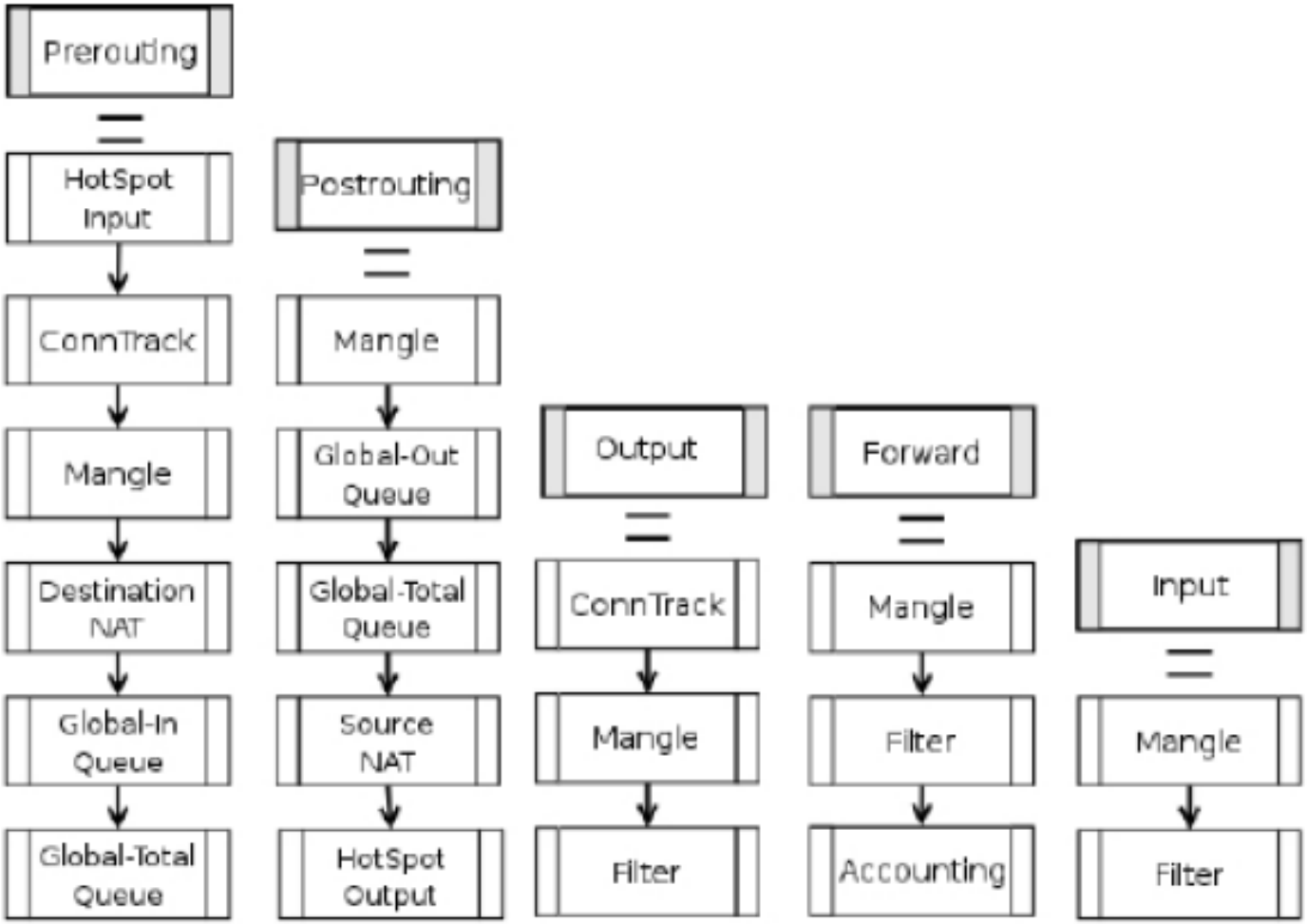
→Indiretamente, usando a facilidade de connection tracking, com base em marcas de conexão previamente criaddas (mais rápido e mais eficiente)

→Diretamente, sem o connection tracking – não é necessário marcas de conexão e o roteador irá comparar cada pacote com determinadas condições.

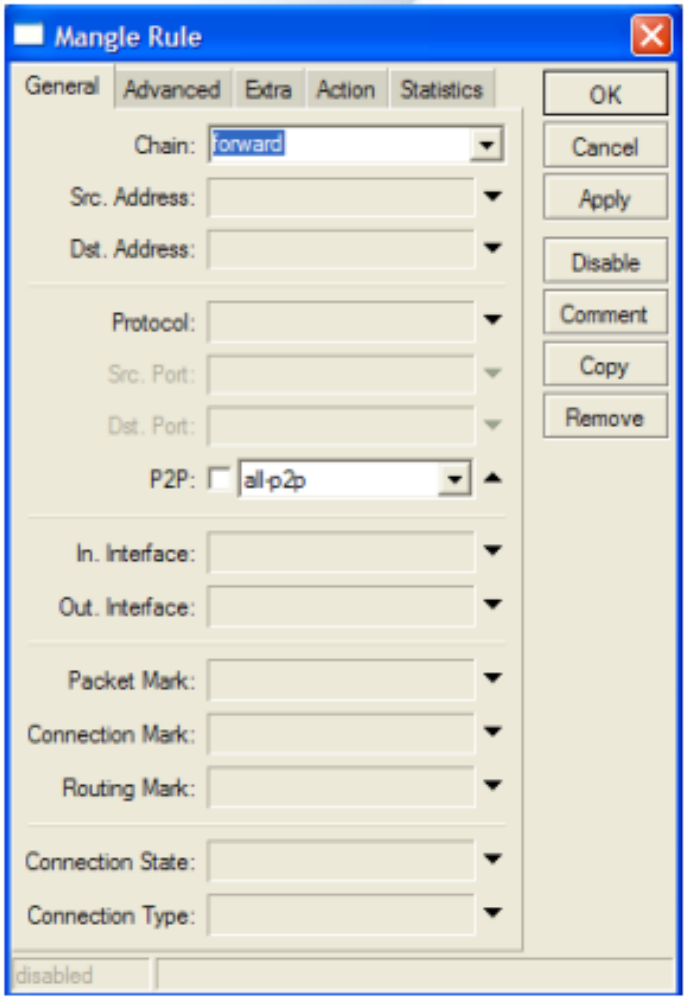
Estrutura de Firewall no Mikrotik

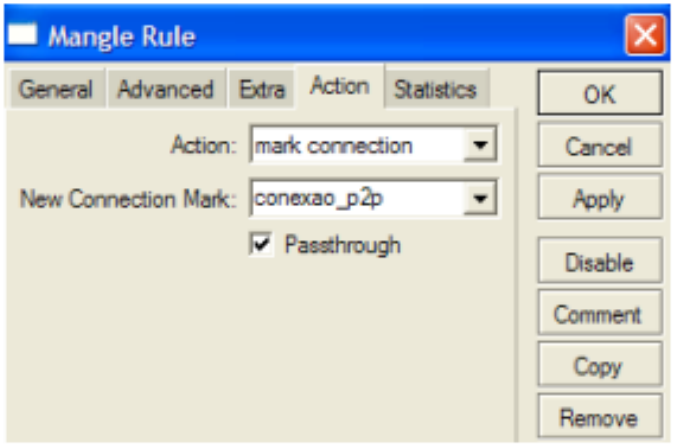


Fluxo de pacotes no Firewall



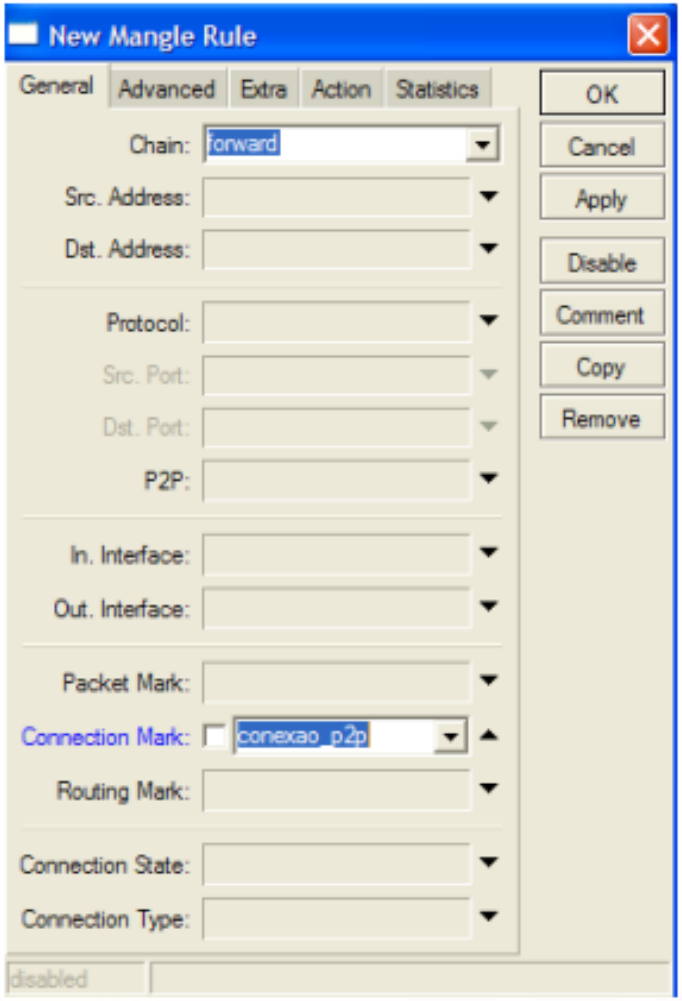
Mangle – Exemplo de marcação
Marcando a conexão P2P

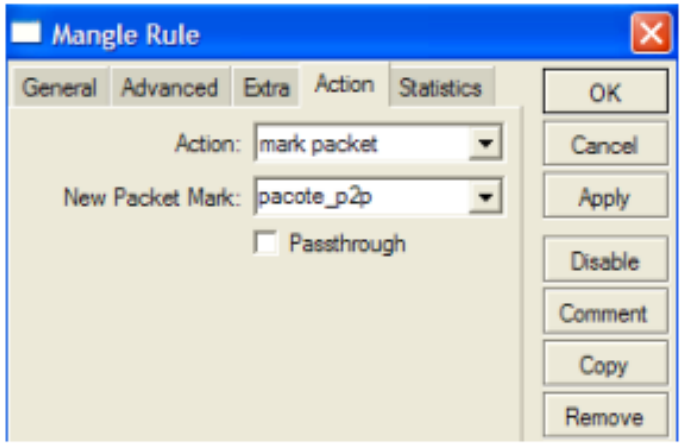





```
[admin@MikroTik] ip firewall mangle> print
Flags: X - disabled, I - invalid, D - dynamic
 0   chain=forward p2p=all-p2p action=mark-connection
new-connection-mark=marca_da_conexao passthrough=yes
```

Mangle – Exemplo de marcação
Marcando os pacotes P2P






```
[admin@MikroTik] ip firewall mangle> print
Flags: X - disabled, I - invalid, D - dynamic
 0   chain=forward p2p=all-p2p action=mark-connection new-connection-
mark=conexao_p2p passthrough=yes

 1   chain=forward connection-mark=conexao_p2p action=mark-packet new-
packet-mark=pacote_p2p passthrough=no
```

Mangle
Exemplos

Queremos dar um tratamento diferenciado a vários tipos de fluxos e

Precisamos marcar:

- → Fluxo de Navegação http e https
- → FTP
- → Email
- → MSN
- → ICMP
- → P2P
- → O que não foi marcado acima

Dúvidas ??

QoS e Limite de Banda

Largura de Banda

Em telecomunicações, a **largura da banda** ou apenas **banda** (também chamada de *débito*) usualmente se refere à *bitrate* de uma rede de transferência de dados, ou seja, a quantidade em *bits/s* que a rede suporta. A denominação *banda*, designada originalmente a um grupo de frequências é justificada pelo fato de que o limite de transferência de dados de um meio está ligado à largura da banda em *hertz*. O termo banda larga denota conexões com uma largura em *hertz* relativamente alta, em contraste com a velocidade padrão em linhas analógicas convencionais (56 kbps), na chamada conexão discada.

Limite de Banda

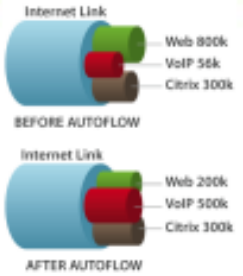
O limite de banda é o limite máximo de transferência de dados, onde também é designada sua velocidade. Por exemplo, você pode ter uma conexão de banda de 1Mbps, onde você conseguiria transportar cerca de 1 *megabit* ou aproximadamente 340 *kilobytes* por segundo.

O termo banda é frequentemente utilizado por operadoras de telecomunicações referindo-se ao limite de dados recebidos ou enviados oferecido pelo serviço num período de um mês. Ultrapassando-se esse limite, as operadoras podem aplicar cortes no limite de transferência de dados de um dado cliente.

Traffic Shaping

- ***Traffic shaping*** é um termo utilizado para definir a prática de priorização do tráfego de dados, através do condicionamento da banda de redes, a fim de otimizar o uso da largura de banda disponível.
- No Brasil, a prática passou a ser adotada pelas empresas de telefonia e PSCM. Estas empresas utilizam programas de gestão de dados que acompanham e analisam a utilização e priorizam a navegação, bloqueando ou diminuindo o tráfego de dados. A prática é comumente adotada para serviços conhecidos por demandar grande utilização da largura de banda, como os de transferência de arquivos, por exemplo, *P2P* e *FTP*.
- Os programas de *traffic shaping* podem ainda fazer logs dos hábitos dos usuários, capturar informações sobre IPs acessados, ativar gravações automáticas a partir de determinadas condutas, reduzir ou interferir na transferência de dados de cada usuário.

Qualidade de Serviço



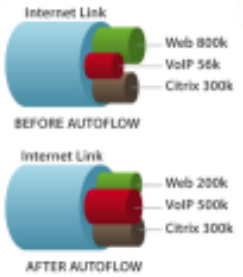
No campo das telecomunicações e redes de computadores, o termo Qualidade de Serviço (QoS), em especial nas redes de comutação de pacotes, refere-se à garantia de largura de banda ou, como em muitos casos, é utilizada informalmente para referir-se a probabilidade de um pacote circular entre dois pontos de rede.

Existem, essencialmente, duas formas de oferecer garantias de QoS. A primeira procura oferecer bastantes recursos, suficientes para o pico esperado, com uma margem de segurança substancial. É simples e eficaz, mas na prática é assumido como dispendioso, e tende a ser ineficaz se o valor de pico aumentar além do previsto.

O segundo método é o de obrigar os dispositivos a reservar os recursos, e apenas aceitar as reservas se os roteadores conseguirem servi-las com confiabilidade.

Qualidade de Serviço (QoS) significa que o(s) roteador(es) deve(m) priorizar e controlar o tráfego na rede. Diferentemente da *limitação de banda* o QoS tem a missão de racionalizar os recursos da rede, balanceando o fluxo de dados com a melhor velocidade possível, evitando o “monopólio” do canal.

Qualidade de Serviço



Os mecanismos para prover QoS do Mikrotik são:

→ limitar banda para certos IP's, subredes, protocolos, portas e outros parâmetros

→ limitar tráfego peer to peer

→ priorizar certos tipos de fluxos de dados em relação a outros

→ utilizar burst's para melhorar o desempenho de acesso WEB

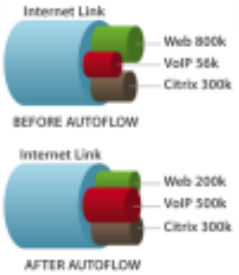
→ aplicar filas em intervalos de tempo fixos

→compartilhar a banda disponível entre os usuários de forma ponderada e dependendo da carga do canal

→ utilização de WMM – Wireless Multimídia

→ MPLS – Multi Protocol Layer Switch

Qualidade de Serviço



Os principais termos utilizados em QoS são:

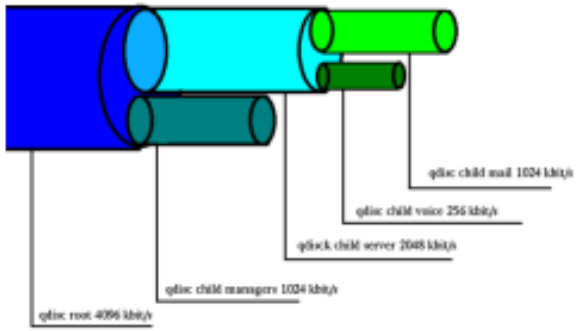
→ **queuing discipline (qdisc)** – disciplina de enfileiramento – é um algorítimo que mantém e controla uma fila de pacotes. Ela especifica a ordem dos pacotes que saem (podendo inclusive reordena-los) e detremina quais pacotes serão descartados.

→ **Limit At ou CIR (Committed Information Rate)** – Taxa de dados garantida – é a garantia de banda fornecida a um circuito/link.

→ **Max Limit ou MIR (Maximal Information Rate)** – Banda máxima que será fornecida, ou seja limite a partir do qual os pacotes serão descartados

→ **Priority** – Prioridade – é a ordem de importancia que o tráfego será processado. Pode-se determinar qual tipo de tráfego será processado primeiro.

Filas (queues)



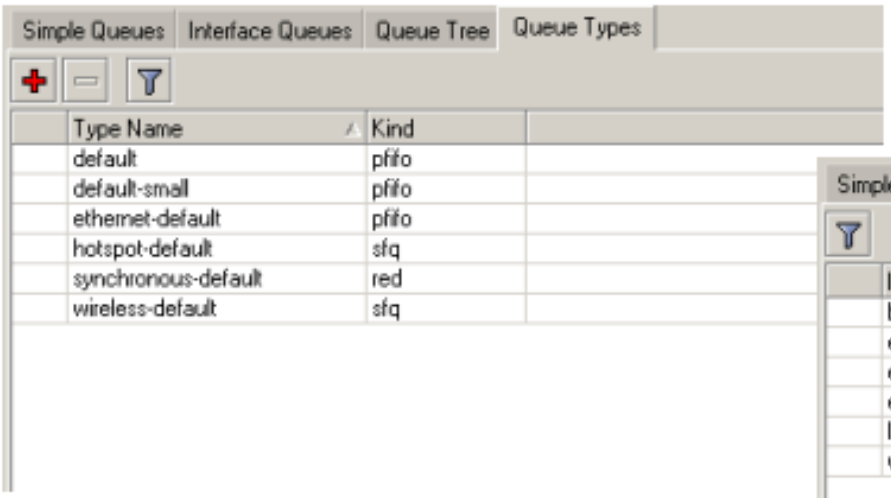
Para ordenar e controlar o fluxo de dados, é aplicada uma política de enfileiramento aos pacotes que estejam ***deixando*** o roteador, ou seja,

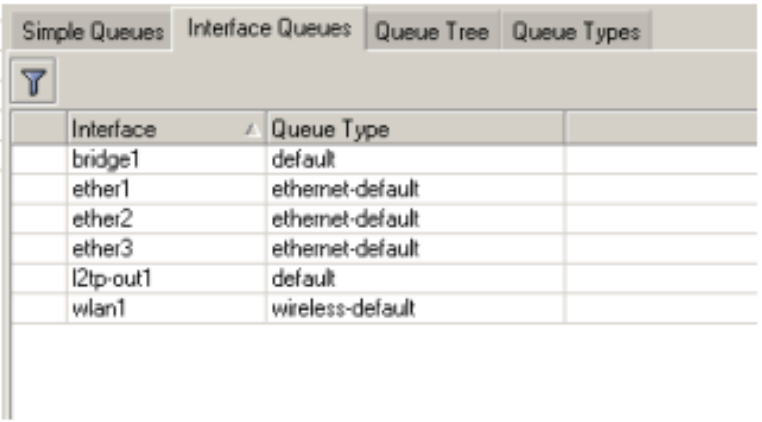
→ **As filas são aplicadas na interface onde o fluxo está saindo !**

A limitação de banda é feita mediante o descarte de pacotes. No caso de protocolo TCP, os pacotes descartados serão reenviados, de forma que não há com que se preocupar com relação à perda de dados. O mesmo não vale para UDP.

Tipos de Filas

Antes de enviar os pacotes por uma interface, eles são processados por uma disciplina de filas (*queue types*). Por padrão as disciplinas de filas são colocadas sob *queue interface* para cada interface física.





Uma vêz adicionada uma fila (em *queue tree* ou *queue simple*) para uma interface física, a fila padrão da interface (*interface default queue*), definida em *queue interface*, não será mantida. Isso significa que quando um pacote não encontra (*match*) qualquer filtro, ele é enviado através da interface com prioridade máxima.

Tipos de Filas

Disciplinas "Scheduler e Shaper"

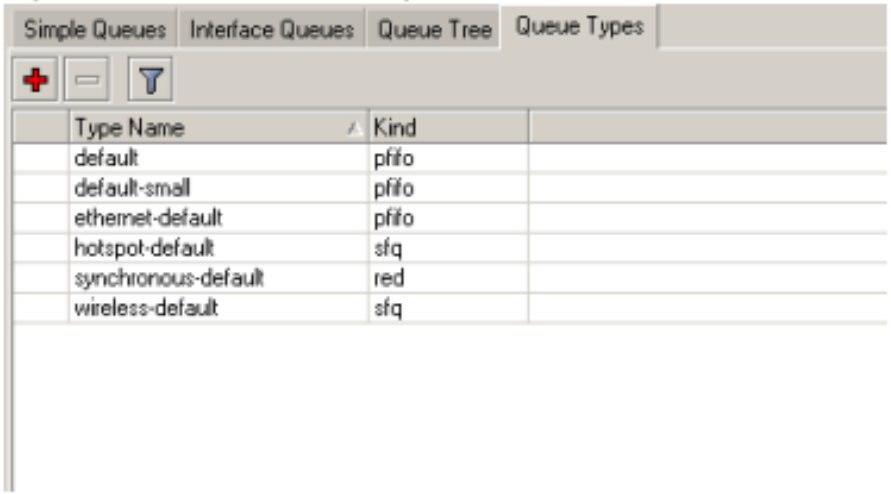
As disciplinas de filas são utilizadas para (re)enfileirar e (re)organizar pacotes na medida em que os mesmos "chegam" na interface. As disciplinas de filas são classificadas pela sua influência no fluxo de pacotes da seguinte forma:

• **schedulers** – (re)ordenam pacotes de acordo com um determinado algorítimo e descartam aqueles que se enquadram na disciplina. Disciplinas "Scheduler" são:

PFIFO, BFIFO, SFQ, PCQ, RED

• **shapers** – também fazem a limitação. São:

PCQ e HTB

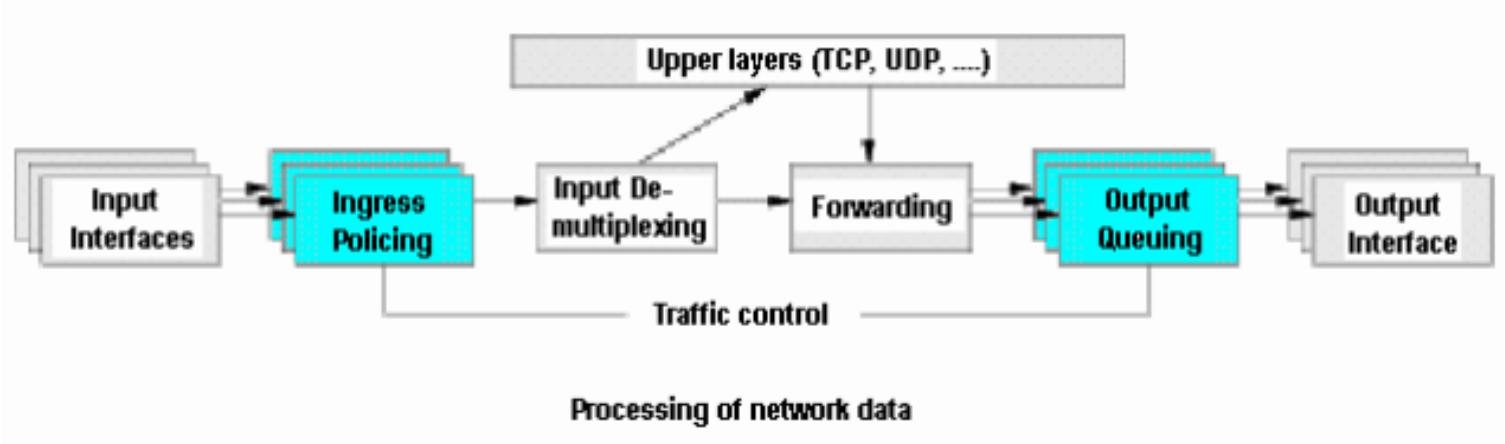


Tipos de Filas

Controle de Tráfego

O controle de tráfego é implementado através de dois mecanismos:

- Pacotes são policiados na entrada
  → pacotes indesejáveis são descartados
- Pacotes são enfileirados na respectiva interface de saída
  → pacotes podem ser atrasados, descartados ou priorizados



Controle de Tráfego

O controle de tráfego é implementado internamente por 4 tipos de componentes:

- Queuing Disciplines = qdisc
  - → algoritmos que controlam o enfileiramento e envio de pacotes.
  - → ex.: FIFO
- Classes
  - → representam "entidades de classificação de pacotes".
  - → cada classe pode estar associada a uma qdisc
- Filters
  - → utilizados para classificar os pacotes e atribuí-los as classes.
- Policers
  - → utilizados para evitar que o tráfego associado a cada filtro ultrapasse limites pré-definidos.

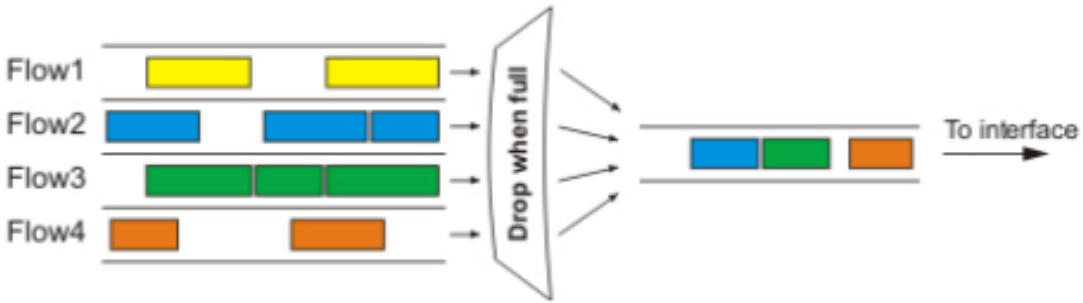
Tipos de Filas

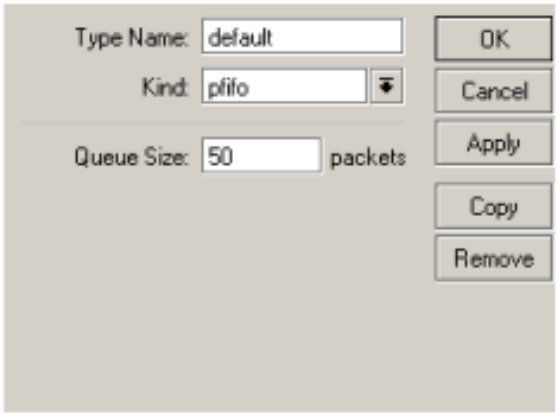
PFIFO e BFIFO

Estas disciplinas de filas são baseadas no algorítimo FIFO (First-In First-Out), ou seja, o primeiro que entra é o primeiro que sai.

A diferença entre PFIFO e BFIFO é que, um é medido em pacotes e o outro em bytes.

Existe apenas um parâmetro chamado *pfifo-limit* (*bfifo-limit*) que determina a quantidade de dados uma fila FIFO pode conter. Todo pacote que não puder ser enfileirado (se a fila está cheia) será descartado. Tamanhos grandes de fila poderão aumentar a latência, em compensação provê uma melhor utilização do canal.





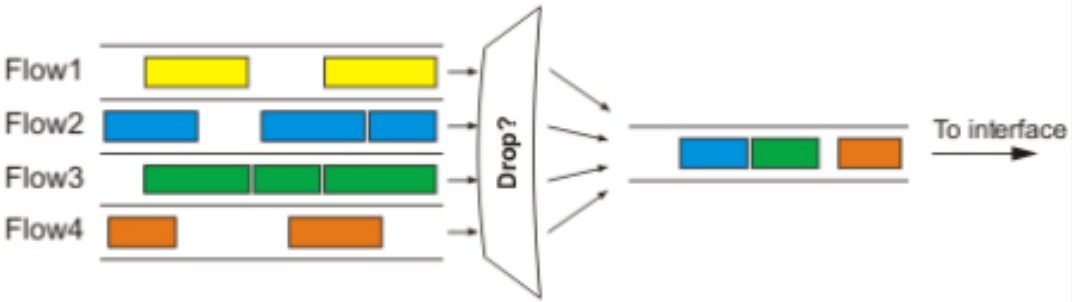
Tipos de Filas

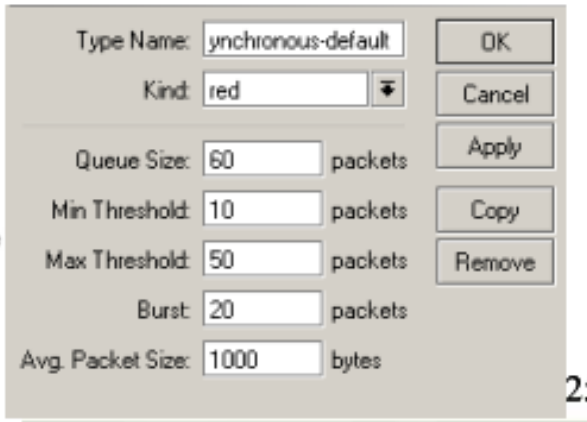
RED

RED- Random Early Detection – Detecção aleatória "antecipada" é um mecanismo de enfileiramento que tenta evitar o congestionamento do link controlando o tamanho médio da fila .

Quando o tamanho médio da fila atinge o valor configurado em *red-min-threshold*, o RED aleatóriamente escolhe um pacote para descartar. A probabilidade do número de pacotes que serão descartados cresce na medida em que a média do tamanho da fila também cresce. Se o tamanho médio da fila atinge *red-max-threshold*, os pacotes são descartados com a probabilidade máxima. Entretanto existem casos em que o tamanho real da fila (não a média) é muito maior que *red-max-threshold*, então todos os pacotes que excederem *red-limit* serão descartados.

RED é indicado em links congestionados com altas taxas de dados. Como é muito rápido funciona bem com TCP.





Tipos de Filas

SFQ

Stochastic Fairness Queuing (SFQ) – Enfileiramento Estocástico "com justiça", é um disciplina que tem a "justiça" assegurada por algoritmos de *hashing* e *round roubin*. O fluxo de pacotes pode ser identificado, exclusivamente, por 4 opções:

- *src-address*
- *dst-addess*
- *src-port*
- *dst-port*

Os pacotes podem ser classificados em 1024 sub-filas, e em seguida o algoritimo *round robin* distribui a banda disponível para estas subfilas, a cada "rodada" configurada no parâmetro *allot (bytes).*

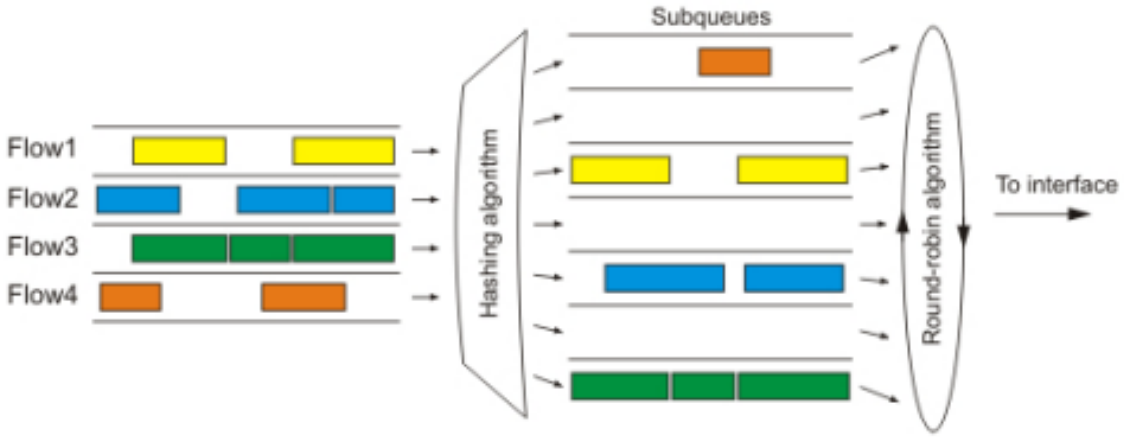
Não limita tráfego. O objetivo é equalizar os fluxos de tráfego (sessões TCP e streaming UDP) quando o link (interface) está completamente cheio. Se o link não está cheio, então não haverá fila e, portanto, qualquer efeito, a não ser quando combinado com outras disciplinas (*qdisc*).

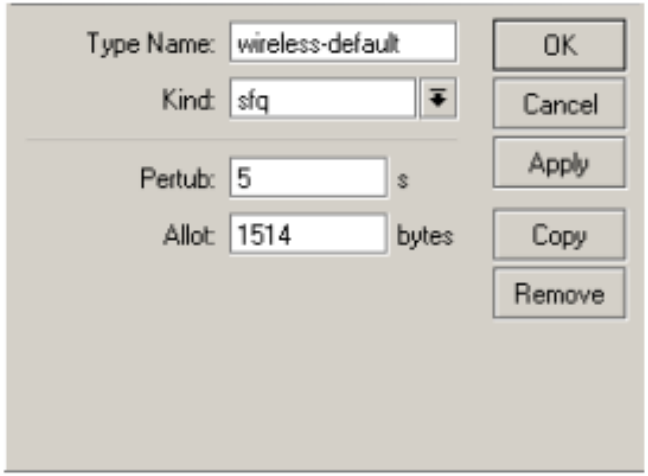
Tipos de Filas

SFQ

A fila, que utiliza SFQ, pode conter 128 pacotes e há 1024 sub-filas disponíveis.

É recomendado o uso de SFQ em links congestionados para garantir que as conexões não degradem. SFQ é especialmente indicado em conexões sem fio.



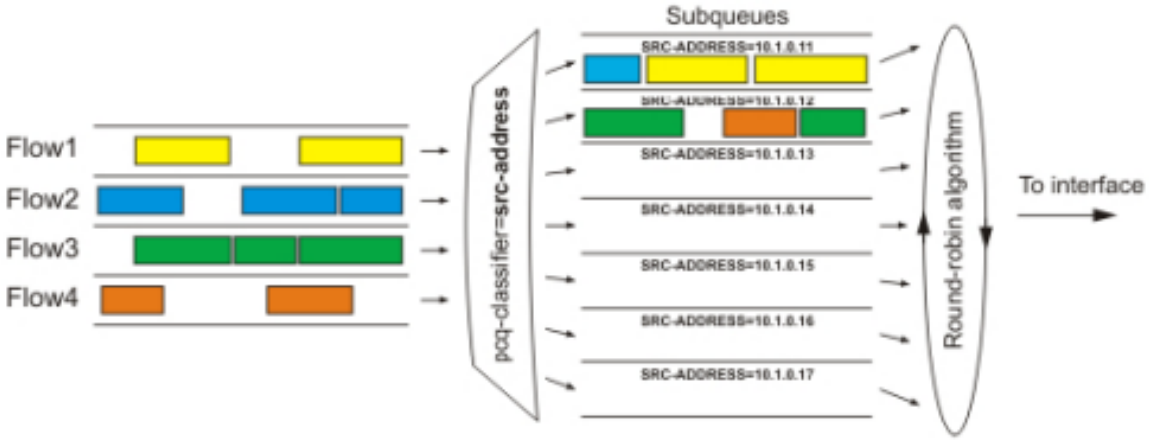


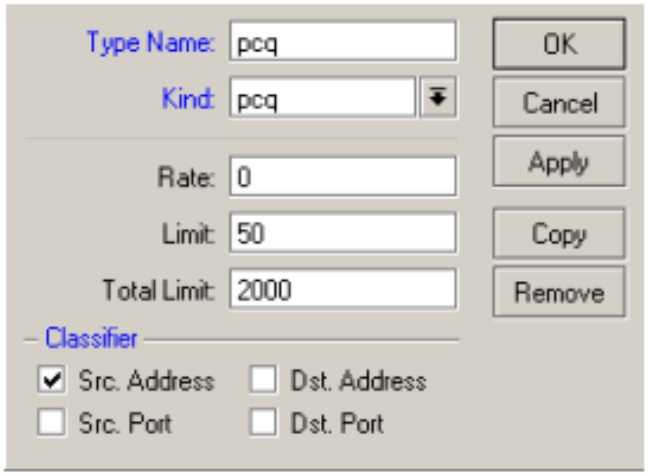
Tipos de Filas

PCQ

O PCQ - Per Connection Queuing – Enfileiramento por conexão foi criado para resolver algumas imperfeições do SFQ. É o único tipo de enfileiramento de baixo nível que pode fazer limitação sendo uma melhoria do SFQ, sem a natureza estocástica. PCQ também cria sub-filas considerando o parametro *pcq-classifier*. Cada sub-fila tem um taxa de transmissão estabelecida em *pcq-rate* e o tamanho do pacote máximo igual a *pcq-limit*. O tamanho total de uma fila a PCQ fica limitado ao que for configurado em *pcq-total-limit*.

O exemplo abaixo mostra o uso do PCQ com pacotes classificados pelo endereço de origem



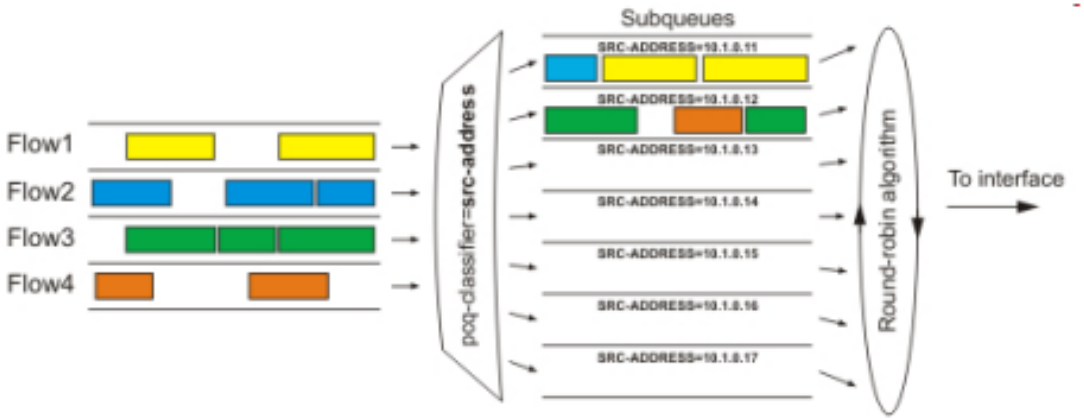


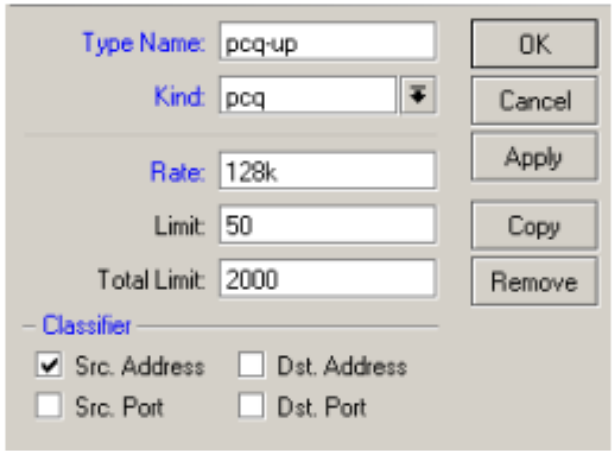
Tipos de Filas

PCQ

Se os pacotes são classificados pelo endereço de origem, então todos os pacotes com diferentes endereços serão agrupados em sub-filas diferentes. Nesse caso é possível fazer a limitação ou equalização para cada sub-fila com o parâmetro *pcq-rate*. Talvez a parte mais significante é decidir em qual interface utilizar esse tipo de disciplina. Se utilizarmos na interface local, todo tráfego da interface pública será agrupado pelo endereço de origem (e provavelmente não é o que se deseja), mas ser for empregada na interface pública todo o tráfego de nossos clientes será agrupado pelo endereço de origem, o que torna fácil equalizar ou limitar o upload dos clientes. O mesmo controle pode ser feito para downloads, mas, nesse caso será utilizado o classificador *dst-address* e configurado na interface local.

PCQ é uma boa ferramenta para controlar ou equalizar a banda entre diversos usuários com pouco trabalho de administração.



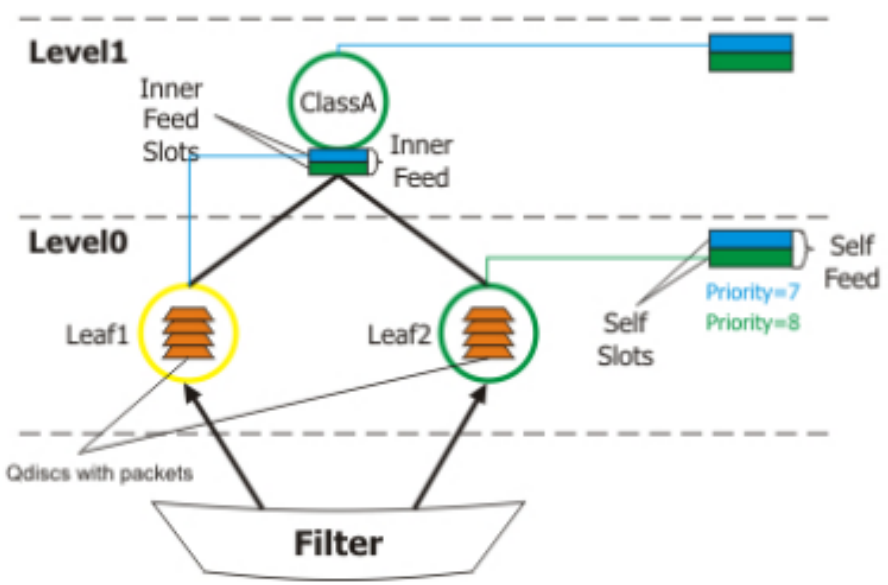


QoS - HTB

HTB (Hierarchical Token Bucket) é uma disciplina de enfileiramento hierárquica que é usual para aplicar diferentes políticas para diferentes tipos de tráfego. O HTB simula vários links um um único meio físico, permitindo o envio de diferentes tipos de tráfego em diferentes links virtuais. Em outras palavras, HTB é muito útil para limitar o *download* e *upload* de usuários de uma rede, desta forma não existe saturamento da largura de banda disponível no link físico. Além disso, no Mikrotik ROS, é utilizado o HTB para configurações de QoS.

Cada ***class*** tem um pai e pode ter uma ou mais filhas. As que não têm filhas, são colocados no ***level 0***, onde as filas são mantidas, e são chamadas de **'leaf class'**.

Cada classe na hierarquia pode priorizar e dar forma ao tráfego (***shaping***).

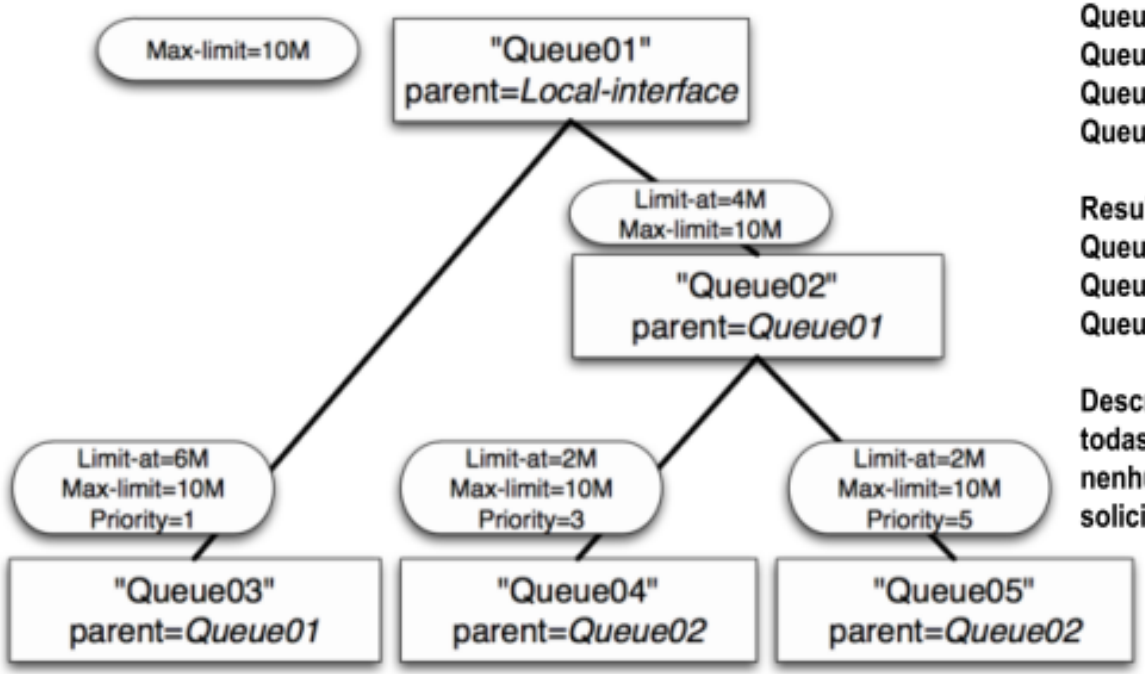


- Para "shaping" os parâmetros são:
  - → limit-at: banda garantida (CIR)
  - → max-limit: banda máxima permitida (MIR)

- Para priorizar:
  - →priority: de 1 a 8, sendo 1 a maior prioridade.
  - **Prioridade só funcionará após o limit-at ser alcançado.*

QoS - HTB

Exemplo de HTB



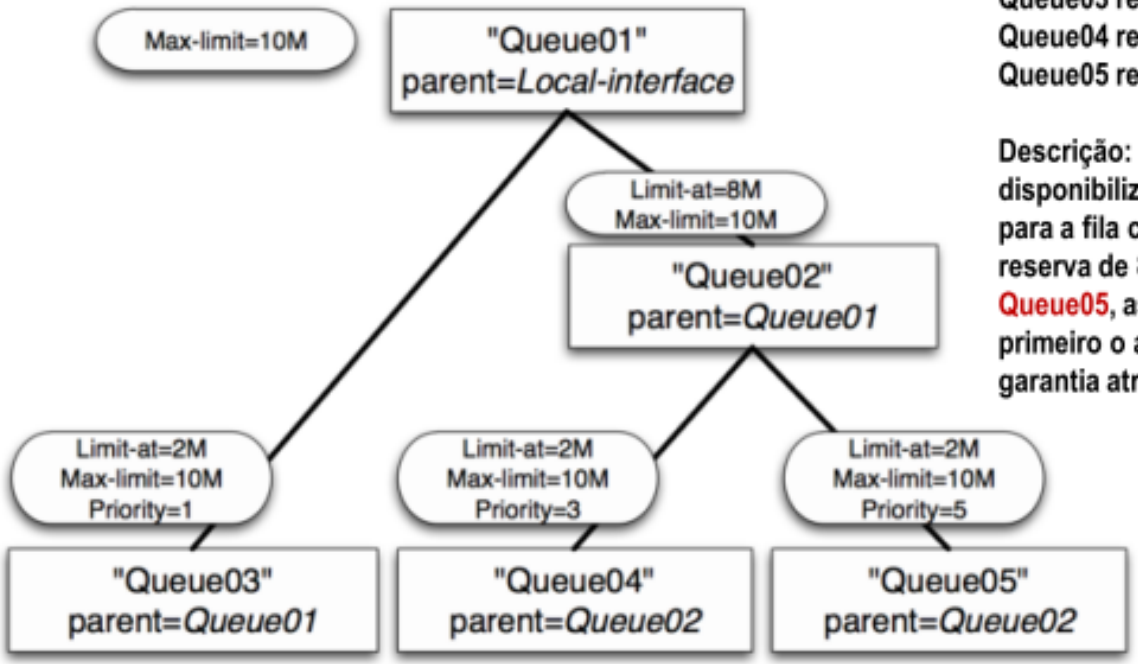
Queue01 limit-at=0Mbps max-limit=10Mbps
Queue02 limit-at=4Mbps max-limit=10Mbps
Queue03 limit-at=6Mbps max-limit=10Mbps priority=1
Queue04 limit-at=2Mbps max-limit=10Mbps priority=3
Queue05 limit-at=2Mbps max-limit=10Mbps priority=5

Resultados
Queue03 receberá 6Mbps
Queue04 receberá 2Mbps
Queue05 receberá 2Mbps

Descrição: O HTB foi configurado, de modo que, satisfazendo todas as garantias (limit-at) a filla principal (pai) não possuirá nenhuma capacidade para distribuir mais banda caso seja solicitado por uma filha.

QoS - HTB

Exemplo de HTB



Queue01 limit-at=0Mbps max-limit=10Mbps
Queue02 limit-at=8Mbps max-limit=10Mbps
Queue03 limit-at=2Mbps max-limit=10Mbps priority=1
Queue04 limit-at=2Mbps max-limit=10Mbps priority=3
Queue05 limit-at=2Mbps max-limit=10Mbps priority=5

Resultados
Queue03 receberá 2Mbps
Queue04 receberá 6Mbps
Queue05 receberá 2Mbps

Descrição: Após satisfazar todas garantias, o HTB disponibilizará mais banda, até o máximo permitido (max-limit) para a fila com maior prioridade. Mas neste caso, permitirá-se reserva de 8Mbps de *throughput* para as filas Queue04 e Queue05, as quais, a que possuir maior prioridade receberá primeiro o adicional de banda, pois a fila Queue02 possui garantia atribuida.

QoS - HTB

Termos do HTB:

→ **Filter** - um processo que classifica pacotes. Os filtros são responsáveis pela classificação de pacotes para que eles sejam colocados nas correspondentes *qdiscs*. Todos os filtros são aplicados no fila raiz HTB e classificados diretamente nas *qdiscs*, sem atravessar a árvore HTB. Se um pacote não está classificado em nenhuma das *qdiscs*, é enviado para a interface diretamente, por isso nenhuma regra HTB é aplicada aos pacotes (isso significa prioridade maior que qualquer pacote do fluxo gerido pelo HTB) .

→ **Level** - posição de uma classe na hierarquia.

→ **Class** - algoritmo de limitação no fluxo de tráfego para uma determinada taxa. Ela não guarda quaisquer pacotes (esta função só pode ser realizada por uma fila). Uma classe pode conter uma ou mais subclasses (inner class) ou apenas uma e um qdisc (leaf class).

QoS - HTB

Termos do HTB:

→ **Inner class** - uma classe que tenha uma ou mais classes filhas ligadas a ela. Não armazenam quaisquer pacotes, então *qdiscs* não podem ser associados a elas (*qdisc* e configurações de filtros são ignoradas, embora possam ser exibidos na configuração do RouterOS). Só fazem limitação de tráfego. Definição de prioridade também é ignorada.

→ **Leaf class** - uma classe que tem uma classe pai, mas ainda não tem nenhuma classe filha. ***Leaf class*** estão sempre localizadas no ***level 0*** da hierarquia.

→ **Self feed** - uma saída (fora da árvore HTB para a interface) para os pacotes de todas as classes ativas no seu nível de hierarquia. Existe uma ***self feed*** por ***level***, cada uma constituída por 8 ***self slots***, que representam as prioridades.

QoS - HTB

Termos do HTB:

→ **Auto slot** - um elemento de uma ***self feed*** que corresponde a cada prioridade. Existe um ***auto slot*** por nível. Todas as classes ativas no mesmo nível, com a mesma prioridade, são anexados a um *auto slot* que enviam os pacotes para fora.

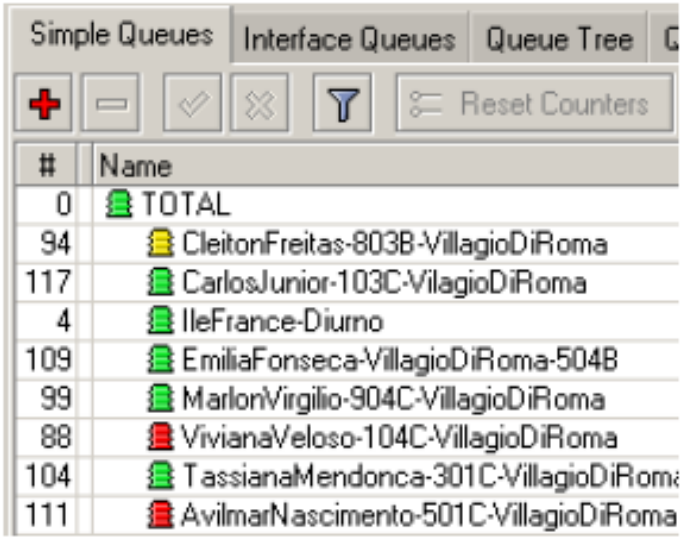
→ **Active class** (para um nível particular) - uma ***class*** que está associada a um ***auto slot*** em determinado nível.

→ **Inner feed** - semelhante a uma ***self feed***, constituídos de ***inner self slots***, presentes em cada classe interior. Existe um ***inner feed*** por ***inner class***.

→ **Inner feed slot** - similar à ***auto slot***. Cada ***inner feed*** é constituído de ***inner slots*** os quais representam uma prioridade.

QoS - HTB

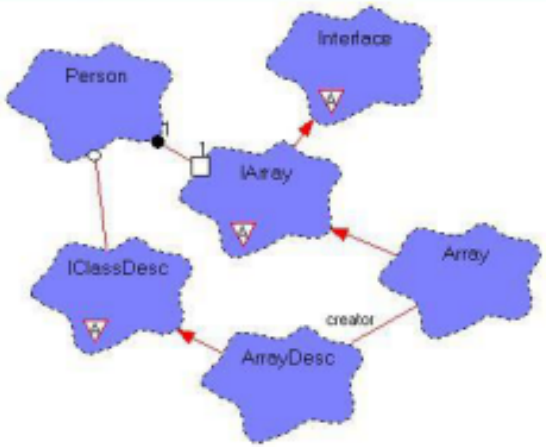
Estados das classes HTB



Cada classe HTB pode estar em um dos 3 estados, dependendo da banda que está consumindo:

- **verde –** de 0% a 50% da banda disponível está em uso.
- **amarelo** – de 51% a 75% da banda disponível está em uso.
- **vermelho** – de 76% a 100% da banda disponível está em uso. Aqui ocorre o descarte de pacotes, quando se ultrapassa o *max-limit*.

QoS - HTB



No Mikrotik ROS as estruturas do HTB podem ser anexadas a quatro locais diferentes:

Interfaces Virtuais

→**global-in** – representa todas as interfaces de entrada em geral (*INGRESS queue*). As filas atreladas à *global-in* recebem todo o tráfego entrante no roteador, antes da filtragem de pacotes.

→**global-out** – representa todas as interfaces de saída em geral (*EGRESS queue*). As filas atreladas à *global-out* recebem todo o tráfego que sai do roteador.

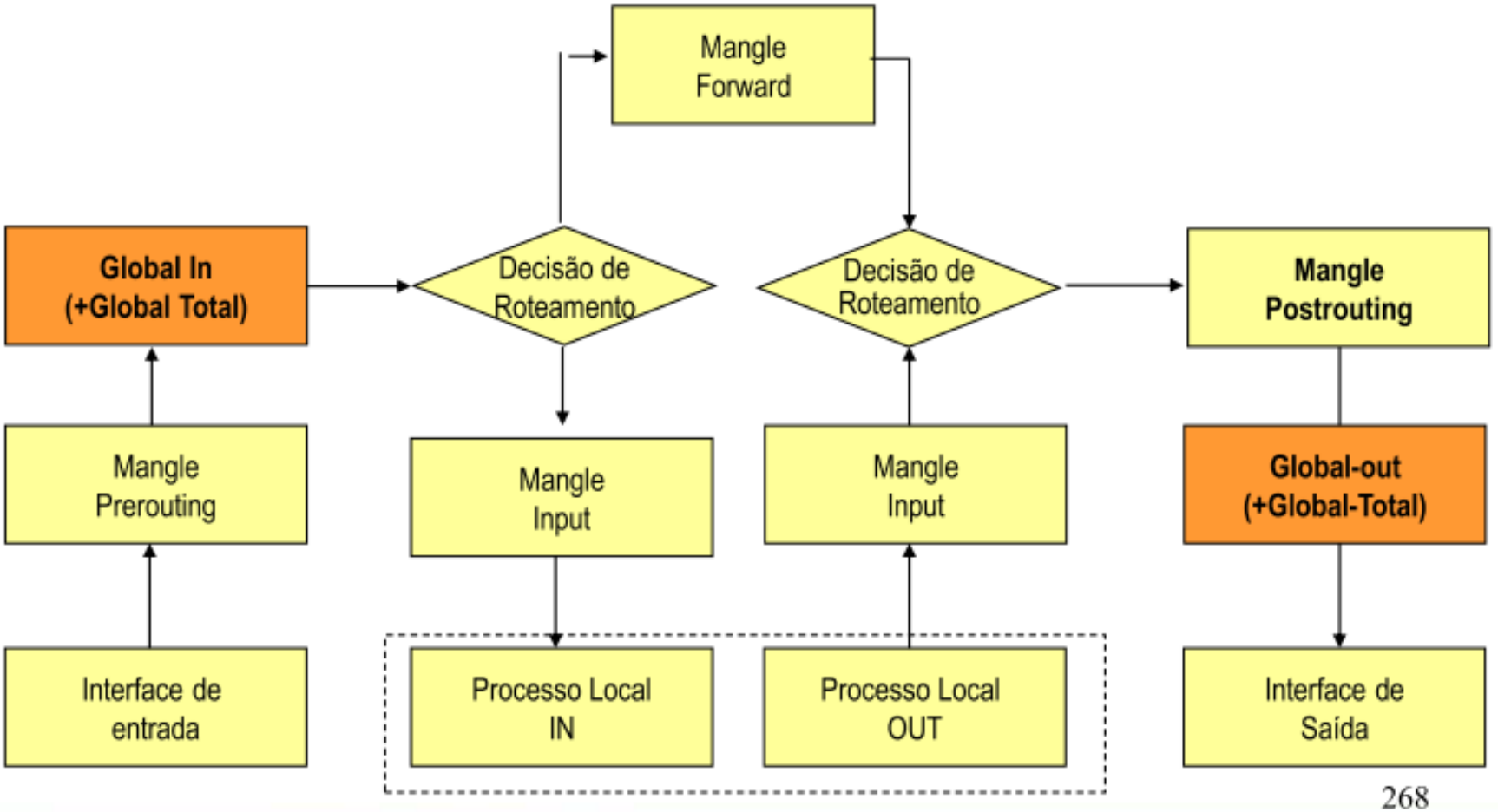
→**global-total** – representa uma interface virtual através da qual passa todo o fluxo de dados. Quando se associa uma política de filas à global-total, a limitação é feita em ambas as direções. Por exemplo se configurarmos um total-max-limit de 256kbps, teremos um total de upload+download limitado em 256 kbps, podendo haver assimetria.

Outras Interfaces

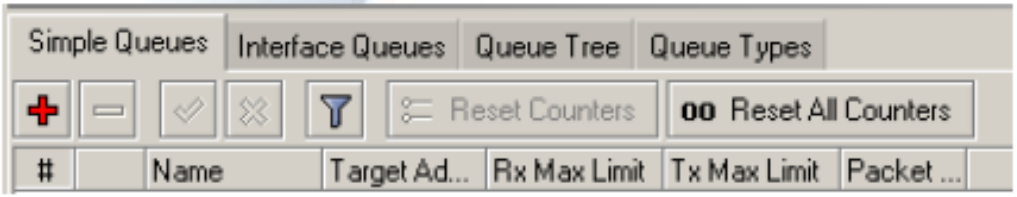
→**Interface X**- representa uma interface particular. Somente o tráfego que é configurado para sair através desta desta interface passará através da fila HTB.

QoS - HTB

Interfaces Virtuais e o Mangle



Filas Simples



- As filas simples (*simple queue*) são a maneira mais fácil de se limitar a banda de endereços IPs distintos ou sub-redes. Elas permitem configurar as velocidades de upload e download com apenas uma entrada.

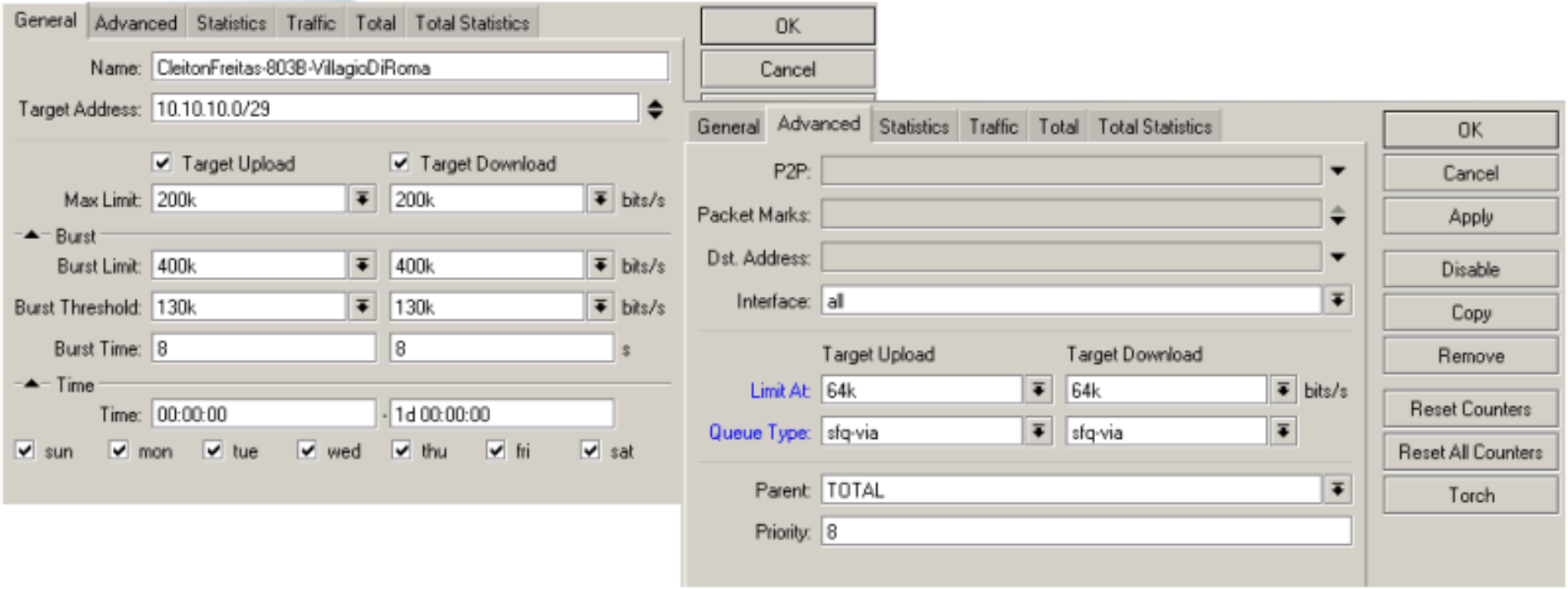
- Também podem ser usadas para configuração de aplicações de QoS.

- Os filtros de filas simples são executados completamente pelo HTB nas interfaces *global-out* (*queue 'direct'*) e *global-in* (*queue 'reverse'*)

- Os filtros "enxergam' as direções dos pacotes IP da mesma forma que apareceriam no ***Firewall***.

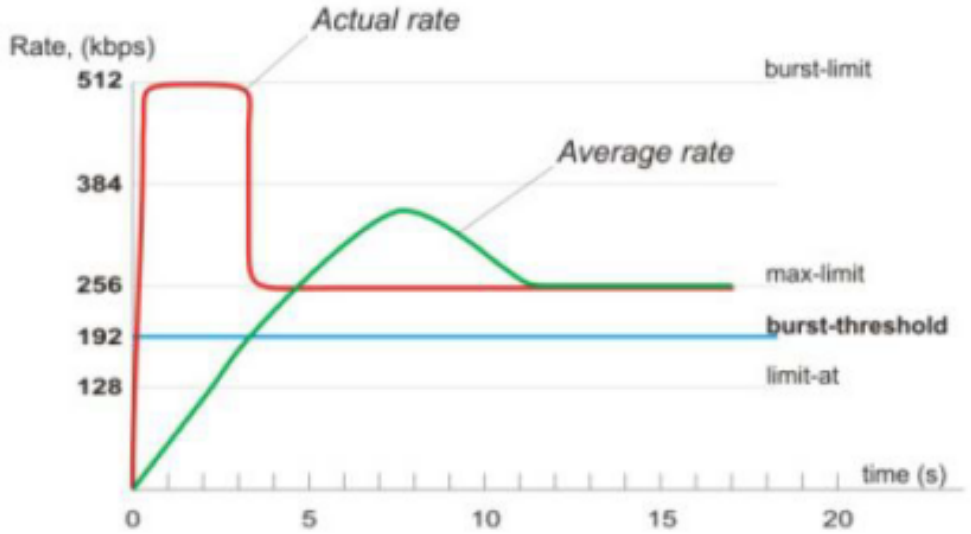
- Hotspot, DHCP e PPP criam dinamicamente filas simples.

Filas Simples



- As principais propriedades configuráveis de uma fila simples são:
  - → Limite por direção IP de origem ou destino
  - → Interface do cliente
  - → tipo de fila
  - → configurações de limit-at, max-limit, priority e burst para download e upload
  - → Horário

Como funciona o Burst

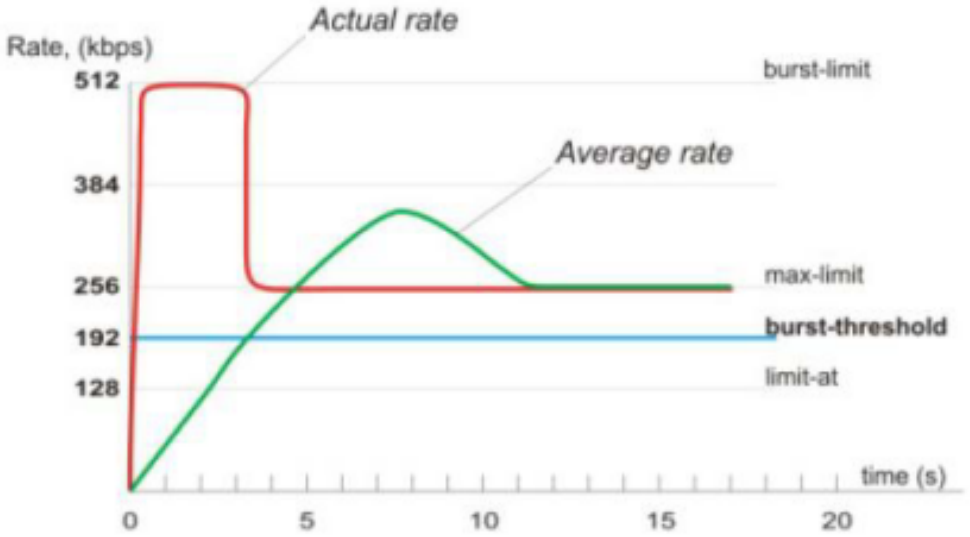


Bursts são usados para permitir altas taxas de dados por um curto período de tempo.

Os parâmetros que controlam o *Burst* são:

- → burst-limit: limite máximo que alcançará
- → burst-time: tempo que durará o burst
- → burst-threshold: patamar onde começa a limitar
- → max-limit: MIR

Como funciona o Burst



Exemplo

max-limit=256kbps

burst-time=8s

burst-threshold=192kbps

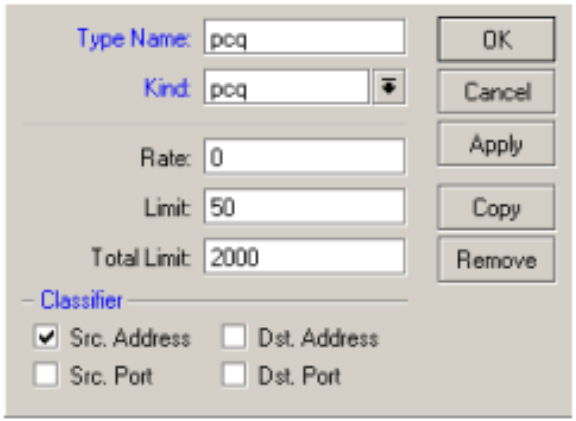
burst-limit=512kbps

É dado ao cliente inicialmente a banda burst-limit=512 kbps. O algorítimo calcula a taxa média de consumo de banda durante o burst-time de 8 segundos.

- com 1 segundo a taxa média é (0+0+0+0+0+0+0+512)/8 = 64kbps (abaixo do threshold)
- com 2 segundos já é de (0+0+0+0+0+0+512+512)/8 = 128 kbs (abaixo do threshold)
- com 3 segundos (0+0+0+0+0+512+512+512)/8 = 192 (é o ponto de inflexão – onde acaba o burst)

A partir do momento que foi atingido o ponto de inflexão o Burst é desabilitado e a taxa máxima do cliente passa a ser o max-limit.

Utilização de PCQ



PCQ – Per Connection Queue – Enfileiramento por conexão

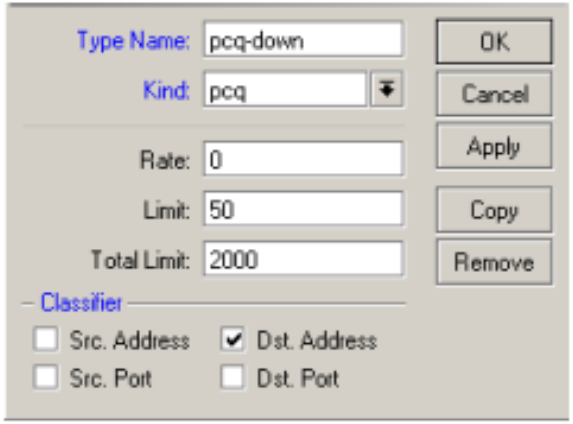
- PCQ é utilizado para equalizar a cada usuário em particular ou cada conexão em particular

- Para utilizar PCQ, um novo tipo de fila deve ser adicionado com o argumento '*kind=pcq*'

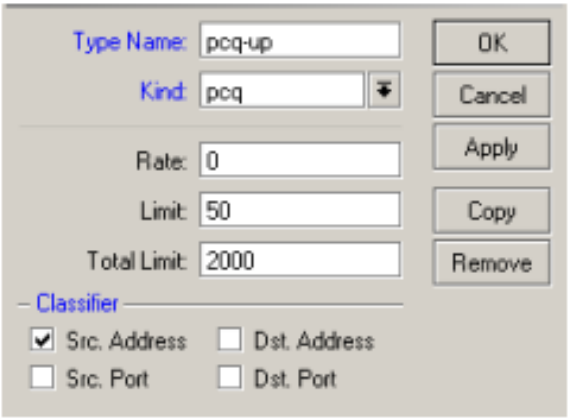
- Devem ainda ser escolhidos os parâmetros:
  - → *pcq-classifier*
  - → *pcq-rate*

Utilização de PCQ

- Com o **rate** configurado como zero, as subqueues não são limitadas, ou seja elas poderão utilizar o máximo de largura de banda disponível em max-limit

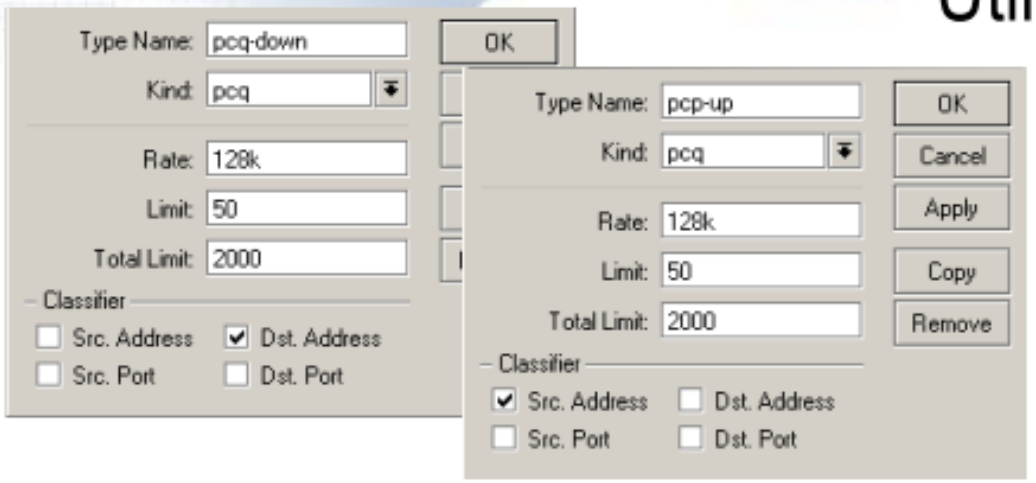


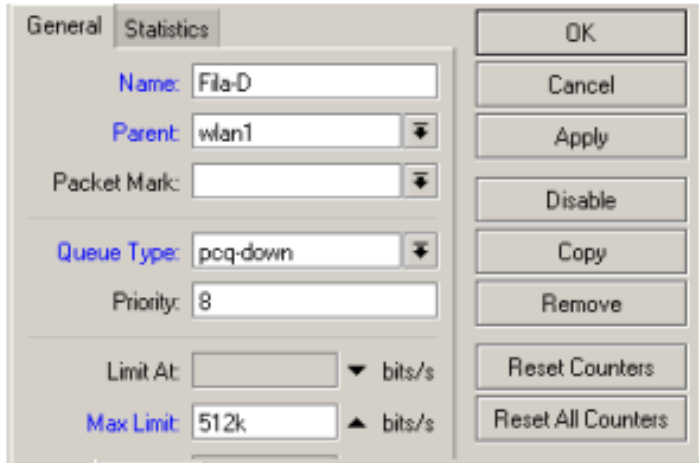
- Se configurarmos um rate para PCQ a subqueues serão limitadas nesse rate, até o total de max-limit

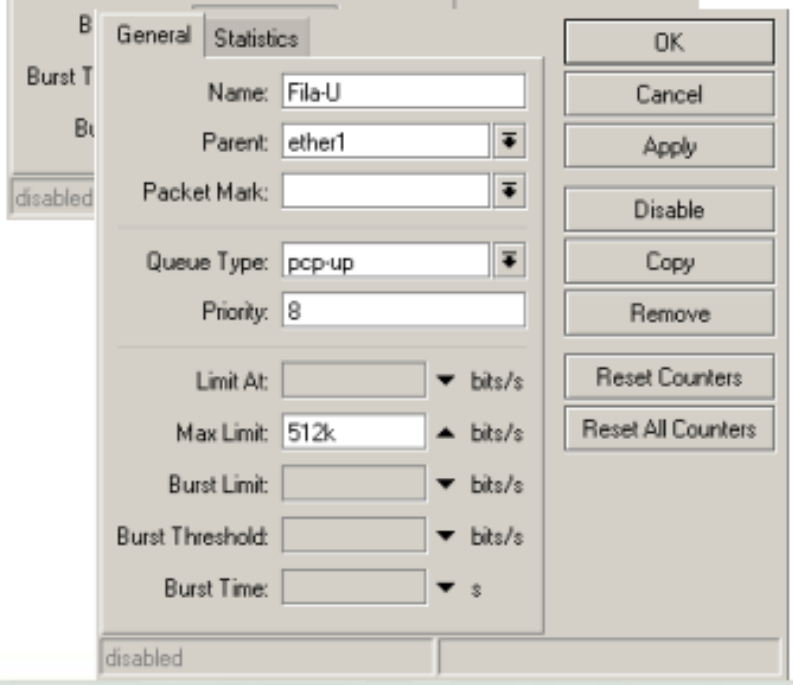


[MikrotikBrasil]
Routers & Wireless Systems

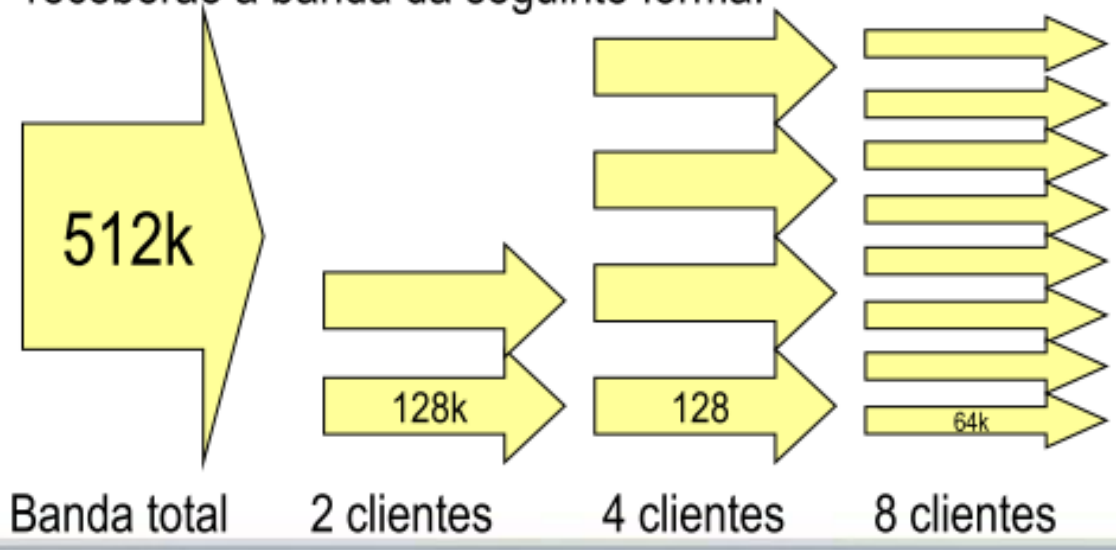
Utilização de PCQ





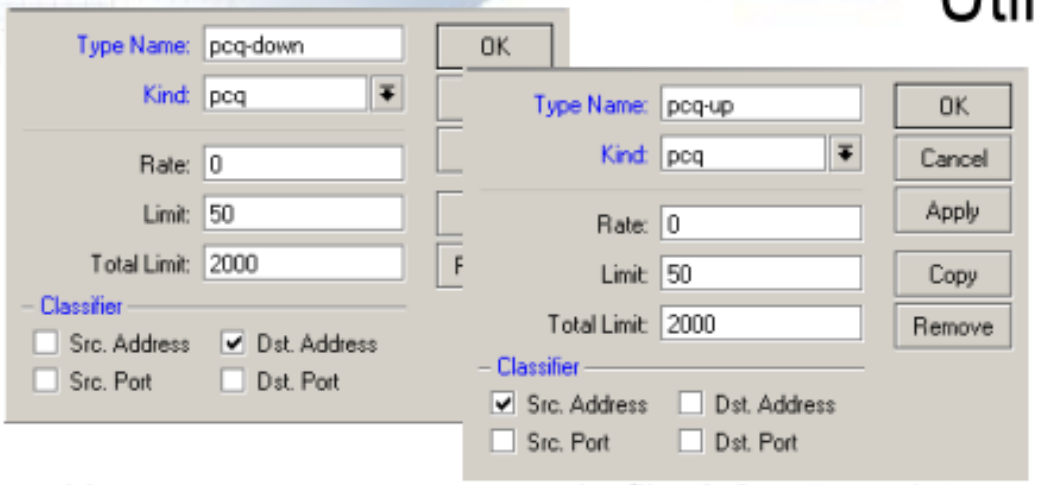


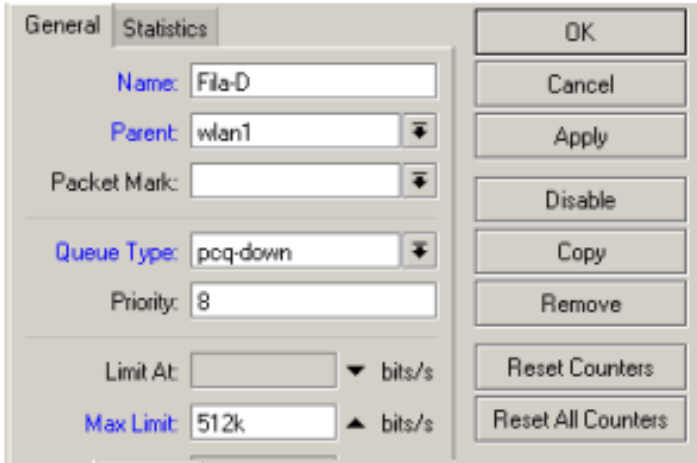
- Nesse caso, como o rate da fila é 128k, não existe limit-at e tem um total de 512k, os clientes receberão a banda da seguinte forma:

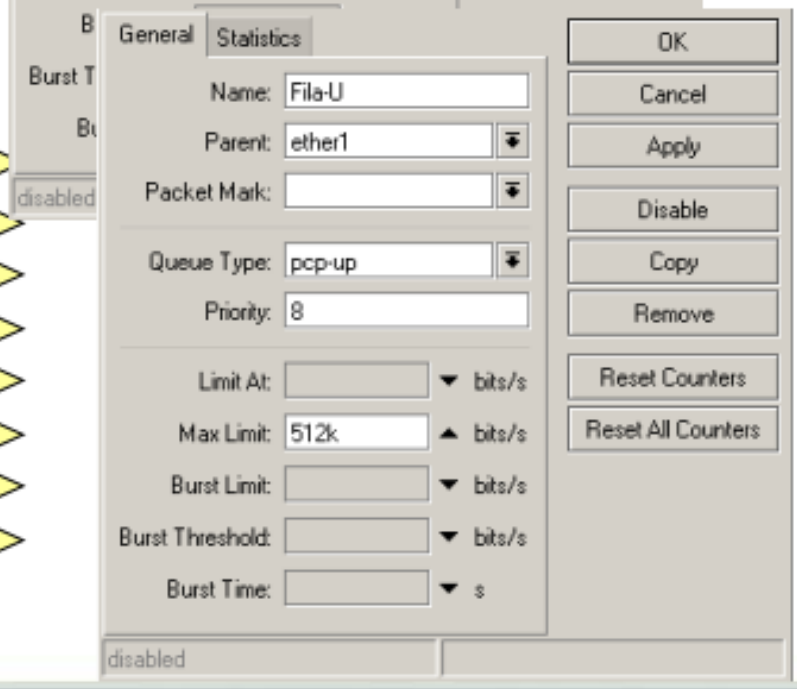


[MikrotikBrasil]
Routers & Wireless Systems

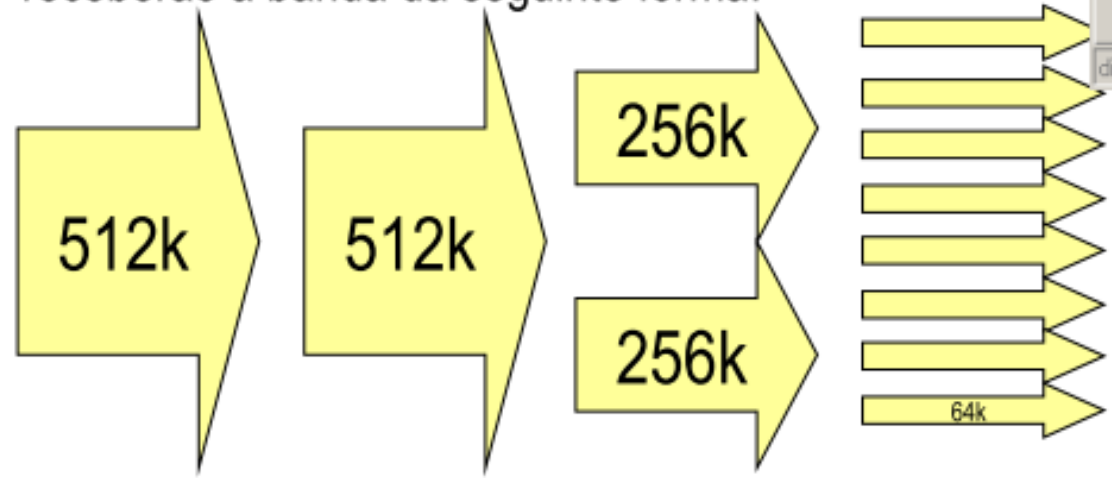
Utilização de PCQ







- Nesse caso, como o rate da fila é 0, não existe limit-at e tem um total de 512k, os clientes receberão a banda da seguinte forma:



Banda total | 1 cliente | 2 clientes | 8 clientes

Árvores de Filas

Trabalhar com árvores de filas é uma maneira mais elaborada de administrar o tráfego. Com elas é possível construir sob medida uma hierarquia de classes, onde poderemos configurar as garantias e prioridades de cada fluxo em relação à outros, determinando assim uma política de QoS para o fluxo do roteador.

Os filtros de árvores de filas são aplicados na interface especificada. Os filtros são apenas marcas que o *firewall* faz no fluxo de pacotes na opção *mangle*. Os filtros enxergam os pacotes na ordem em que eles chegam ao roteador.

É também a única maneira para adicionar uma fila em uma interface separada.

Também é possível ter o dobro de enfileiramento (exemplo: priorização de tráfego em *global-in* e/ou *global-out*, limitação por cliente na interface de saída). Se é configurado filas simples (queue simple) e árvore de filas (queue tree) no mesmo roteador, as filas simples receberão o tráfego primeiro e o classificarão.

Árvores de Filas

- As árvores de filas são configuradas em *queue tree*

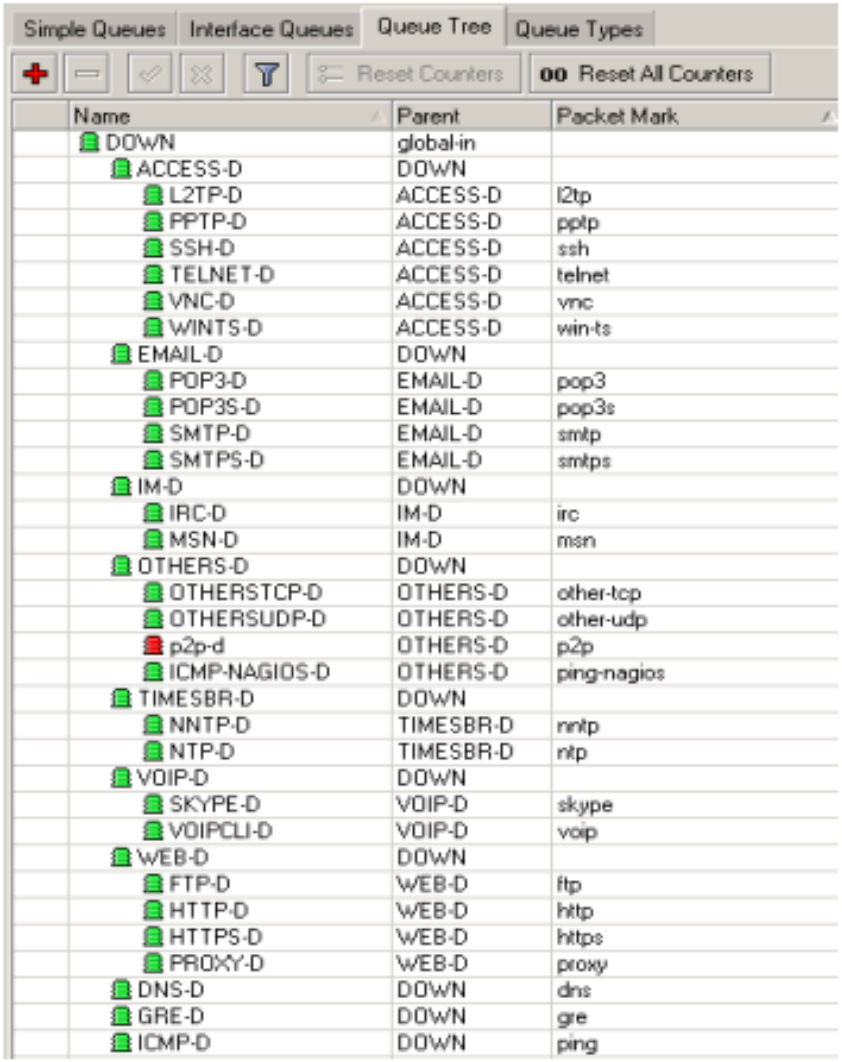
- Dentre as propriedades configuráveis se incluem;

→ Escolher uma marca de tráfego (feita no *mangle*)

→ *parent-class* ou interface de saída (incluindo as interfaces virtuais global-in e global-out)

→ Tipo de Fila (*queue type*)

→ configurações de limit-at, max-limit, priority e burst

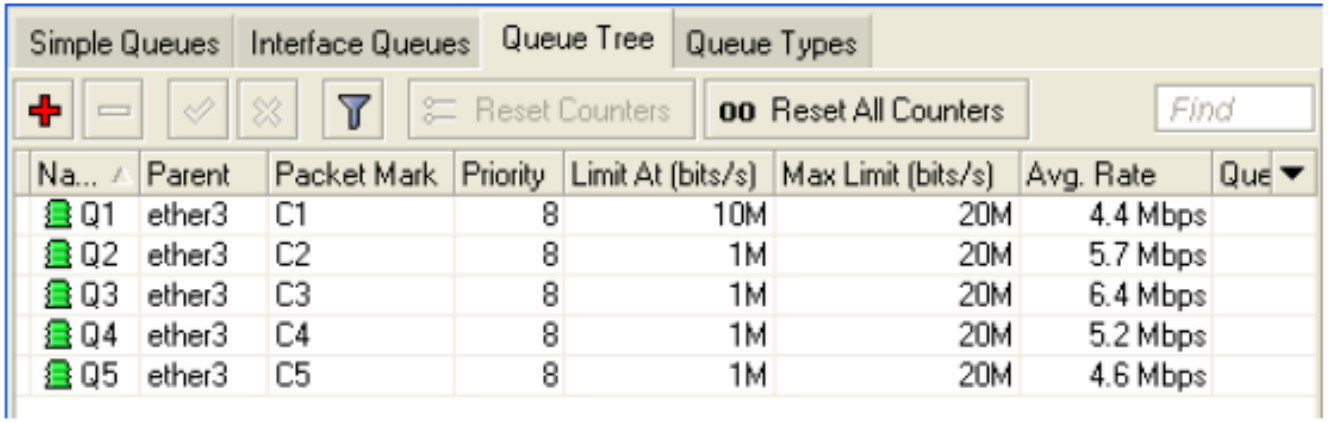


Name	Parent	Packet Mark
DOWN	global-in	
ACCESS-D	DOWN	
L2TP-D	ACCESS-D	l2tp
PPTP-D	ACCESS-D	pptp
SSH-D	ACCESS-D	ssh
TELNET-D	ACCESS-D	telnet
VNC-D	ACCESS-D	vnc
WINTS-D	ACCESS-D	win-ts
EMAIL-D	DOWN	
POP3-D	EMAIL-D	pop3
POP3S-D	EMAIL-D	pop3s
SMTP-D	EMAIL-D	smtp
SMTPS-D	EMAIL-D	smtps
IM-D	DOWN	
IRC-D	IM-D	irc
MSN-D	IM-D	msn
OTHERS-D	DOWN	
OTHERSTCP-D	OTHERS-D	other-tcp
OTHERSUDP-D	OTHERS-D	other-udp
p2p-d	OTHERS-D	p2p
ICMP-NAGIOS-D	OTHERS-D	ping-nagios
TIMESBR-D	DOWN	
NNTP-D	TIMESBR-D	nntp
NTP-D	TIMESBR-D	ntp
VOIP-D	DOWN	
SKYPE-D	VOIP-D	skype
VOIPCLI-D	VOIP-D	voip
WEB-D	DOWN	
FTP-D	WEB-D	ftp
HTTP-D	WEB-D	http
HTTPS-D	WEB-D	https
PROXY-D	WEB-D	proxy
DNS-D	DOWN	dns
GRE-D	DOWN	gre
ICMP-D	DOWN	ping

Árvores de Filas

Laboratório

Queue	Limit-At	Max-Limit
C1	10M	20M
C2	1M	20M
C3	1M	20M
C4	1M	20M
C5	1M	20M

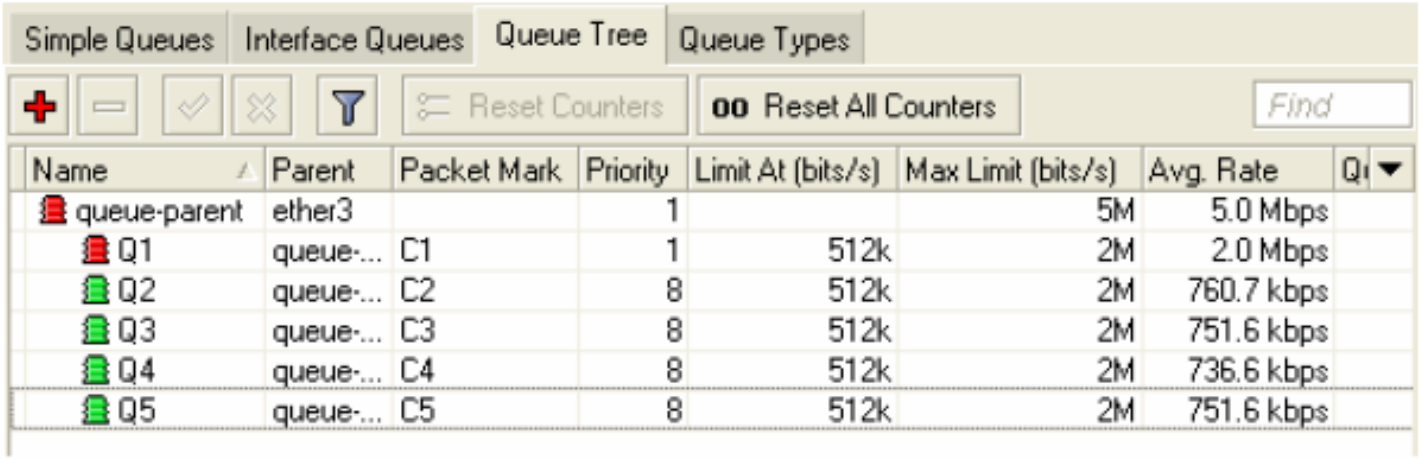


Na...	Parent	Packet Mark	Priority	Limit At (bits/s)	Max Limit (bits/s)	Avg. Rate	Que
Q1	ether3	C1	8	10M	20M	4.4 Mbps	
Q2	ether3	C2	8	1M	20M	5.7 Mbps	
Q3	ether3	C3	8	1M	20M	6.4 Mbps	
Q4	ether3	C4	8	1M	20M	5.2 Mbps	
Q5	ether3	C5	8	1M	20M	4.6 Mbps	

O roteador não conseguirá garantir a banda para C1.

Árvores de Filas

Laboratório



Name	Parent	Packet Mark	Priority	Limit At (bits/s)	Max Limit (bits/s)	Avg. Rate	Q
queue-parent	ether3		1		5M	5.0 Mbps	
Q1	queue-...	C1	1	512k	2M	2.0 Mbps	
Q2	queue-...	C2	8	512k	2M	760.7 kbps	
Q3	queue-...	C3	8	512k	2M	751.6 kbps	
Q4	queue-...	C4	8	512k	2M	736.6 kbps	
Q5	queue-...	C5	8	512k	2M	751.6 kbps	

Com *parent* (hierarquia)

Árvores de Filas

Laboratório

Simple Queues | Interface Queues | Queue Tree | Queue Types

Reset Counters | Reset All Counters | Find

Name	Parent	Packet Mark	Priority	Limit At (...	Max Limit...	Avg. Rate	Queued Byte:
queue-parent	ether3		1		5M	5.0 Mbps	0 B
-Q1	queue-parent	C1	1	512k	2M	2.0 Mbps	54.0 KiB
B1	queue-parent		8			1500.1 kbps	0 B
Q2	B1	C2	8	512k	2M	745.4 kbps	72.8 KiB
Q3	B1	C3	8	512k	2M	760.7 kbps	72.7 KiB
B2	queue-parent		8			1503.0 kbps	0 B
Q4	B2	C4	8	512k	2M	757.6 kbps	73.2 KiB
Q5	B2	C5	8	512k	2M	751.3 kbps	72.8 KiB

Mais hierarquia

C1 possui maior prioridade, portanto consegue atingir o *max-limit*, o restante da banda é divido entre as outras *leaf-queue*

Árvores de Filas

Laboratório

Simple Queues | Interface Queues | Queue Tree | Queue Types

Reset Counters | Reset All Counters | Find

Name	Parent	Packet Mark	Priority	Limit At (...	Max Limit...	Avg. Rate	Queued Byte:
queue-parent	ether3		1		5M	5.0 Mbps	0 B
-Q1	queue-parent	C1	1	512k	2M	1981.1 kbps	72.7 KiB
B1	queue-parent		8	2M	5M	2.0 Mbps	0 B
Q2	B1	C2	8	512k	2M	1003.0 kbps	72.7 KiB
Q3	B1	C3	8	512k	2M	1003.1 kbps	72.7 KiB
B2	queue-parent		8		5M	1027.2 kbps	0 B
Q4	B2	C4	8	512k	2M	509.1 kbps	72.7 KiB
Q5	B2	C5	8	512k	2M	512.1 kbps	72.7 KiB

Garantia na *inner queue*

Árvores de Filas

Laboratório

Simple Queues | Interface Queues | Queue Tree | Queue Types

00 Reset Counters | 00 Reset All Counters | Find

Name	Parent	Packet Mark	Priority	Limit At (...	Max Limit...	Avg. Rate	Queued Byte:
queue-parent	ether3		1		5M	5.0 Mbps	0 B
-Q1	queue-parent	C1	1	512k	2M	1981.2 kbps	71.3 KiB
B1	queue-parent		8	2M	5M	2.0 Mbps	0 B
Q2	B1	C2	8	512k	2M	999.9 kbps	72.7 KiB
Q3	B1	C3	8	512k	2M	1000.0 kbps	72.8 KiB
B2	queue-parent		8		5M	1024.4 kbps	0 B
Q4	B2	C4	2	512k	2M	512.2 kbps	72.7 KiB
Q5	B2	C5	2	512k	2M	512.1 kbps	72.7 KiB

Prioridade na *leaf queue*

Árvores de Filas

Laboratório

Simple Queues | Interface Queues | Queue Tree | Queue Types

00 Reset Counters | 00 Reset All Counters | Find

Name	Parent	Packet Mark	Priority	Limit At (...	Max Limit...	Avg. Rate	Queued Byte:
queue-parent	ether3		1		5M	5.0 Mbps	0 B
-Q1	queue-parent	C1	1	512k	2M	2.0 Mbps	23.7 KiB
B1	queue-parent		2	1M	5M	1024.5 kbps	0 B
Q2	B1	C2	8	512k	2M	512.2 kbps	72.7 KiB
Q3	B1	C3	8	512k	2M	512.2 kbps	72.8 KiB
B2	queue-parent		8	1M	5M	1982.0 kbps	0 B
Q4	B2	C4	4	512k	2M	993.9 kbps	72.7 KiB
Q5	B2	C5	4	512k	2M	987.9 kbps	72.7 KiB

Prioridade funciona apenas na *leaf queue*, não funciona na *inner queue*

Erros comuns:

- *leaf queue* sem *parent*
- prioridade configurada para *inner queue*

Dúvidas ??

Túneis & VPN's

VPN

Uma **Rede Particular Virtual** (**Virtual Private Network** - **VPN**) é uma rede de comunicações privada normalmente utilizada por uma empresa ou um conjunto de empresas e/ou instituições, construída em cima de uma rede de comunicações pública (como por exemplo, a Internet). O tráfego de dados é levado pela rede pública utilizando protocolos padrão, não necessariamente seguros.

VPNs seguras usam protocolos de criptografia por tunelamento que fornecem a confidencialidade, autenticação e integridade necessárias para garantir a privacidade das comunicações requeridas. Quando adequadamente implementados, estes protocolos podem assegurar comunicações seguras através de redes inseguras.

VPN

As principais características das VPN's são:

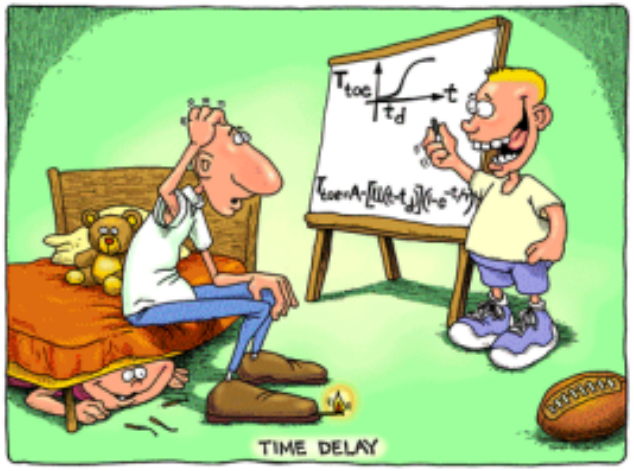
- Promover acesso seguro sobre meios físicos públicos como a Internet por exemplo.
- Promover acesso seguro sobre linhas dedicadas, wireless, etc.
- Promover acesso seguro a serviços em ambiente corporativo de correio, impressoras, etc.
- Fazer com que o usuário, na prática, se torne parte da rede corporativa remota recebendo IP's desta e perfis de segurança definidos.
- A base da formação das VPN's é o tunelamento entre dois pontos, porém tunelamento não é sinônimo de VPN.

Tunelamento

A definição de ***Tunnelling*** é a capacidade de criar túneis entre dois hosts, por onde trafegam dados.

O Mikrotik implementa diversos tipos de Tunelamento, podendo ser tanto servidor como cliente desse protocolos.

- PPP (Point to Point Protocol)
- PPPoE (Point to Point Protocol over Ethernet)
- PPtP (Point to Point Tunneling Protocol)
- L2TP (Layer 2 Tunneling Protocol)
- IPSec (IP Security)
- Túneis IPIP
- Túneis EoIP
- VPLS
- Túneis TE



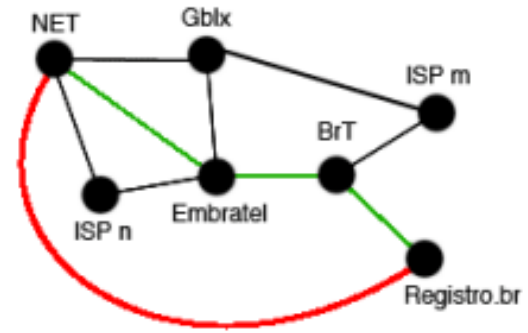
Algumas definições comuns para os serviços PPP

• MTU/MRU: unidades máximas de transmissão/recepção em bytes. Normalmente o padrão ethernet permite 1500 bytes. Em serviços PPP que precisam encapsular os pacotes, deve se definir valores menores para evitar a fragmentação.

• Keepalive Timeout: define o período de tempo em segundos após o qual o roteador começa a mandar pacotes de keepalive a cada segundo. Se nenhuma resposta de keepalive é recebida pelo período de tempo de 2 vezes o keep-alive-timeout o cliente é considerado desconectado.

• Authentication:
  - **Pap: usuário/senha passa em texto plano, sem criptografia**
  - **Chap: usuário/senha com criptografia**
  - **mschap1: versão chap da Microsoft conf. RFC 2433**
  - **mschap2: versão chap da Microsoft conf. RFC 2759**

Algumas definições comuns para os serviços PPP



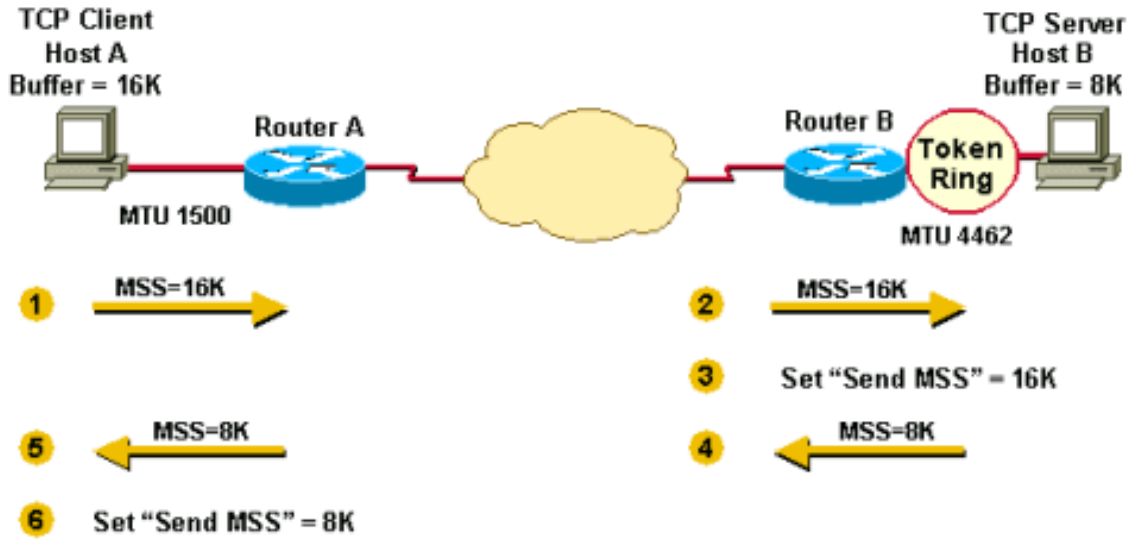
- **PMTUD**: Se durante uma comunicação alguma estação enviar pacotes IP maiores do que a rede pode suportar, ou seja, maiores que o menor MTU (Maximum Transmission Unit) do caminho, então será necessário que haja algum mecanismo para avisar que esta estação deverá diminuir o tamanho dos pacotes para que a comunicação ocorra com sucesso. O processo interativo de envio de pacotes em determinados tamanhos, a resposta dos roteadores intermediários (possivelmente com pacotes do tipo ICMP Packet Tôo Big) e a adequação do tamanho dos pacotes posteriores é chamada Path MTU Discovery ou PMTUD. Normalmente esta funcionalidade está presente em todos os roteadores comerciais e sistemas Unix Like, assim como no Mikrotik ROS.

- **MRRU:** tamanho máximo do pacote, em bytes, que poderá ser recebido no link. Se um pacote ultrapassa o valor definido ele será divido em pacotes menores, permitindo o melhor dimensionamento do túnel. Especificar MRRU significa permitir MP (Multilink PPP) sobre um túnel simples. Essa configuração é útil para o protocolo PMTU Discovery superar falhas. O MP deve ser ativado em ambos os lados (cliente e servidor).

• **Change MSS** (Máximum Segment Size Field, ou seja o tamanho máximo do segmento de dados.).

Um pacote com MSS que ultrapassa o MSS dos roteadores por onde um túnel está estabelecido deve ser fragmentado antes de enviá-lo. Em alguns casos o PMTUD está quebrado ou os roteadores não conseguem trocar as informações de maneira eficiente e causam uma série de problemas com transferência HTTP, FTP e correio eletrônico, além de mensageiros instantâneos.

Neste caso o Mikrotik ROS proporciona ferramentas onde é possível intervir e configurar uma diminuição do MSS dos próximos pacotes através do túnel visando resolver o problema.



Servidor ou Cliente PPPoE

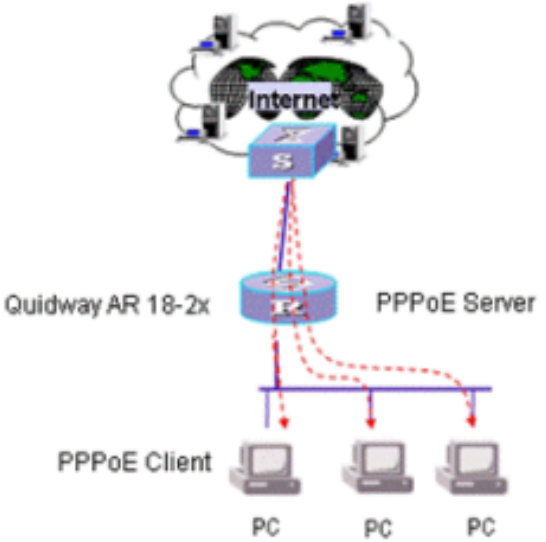
PPPoE (point-to-point protocol over Ethernet) é uma adaptação do PPP para funcionar em redes Ethernet. Pelo fato da rede Ethernet não ser ponto a ponto, o cabeçalho PPPoE inclui informações sobre o remetente e destinatário, desperdiçando mais banda (~2% a mais).

- Muito usado para autenticação de clientes com Base em Login e senha. O PPPoE estabelece a sessão e realiza a autenticação com o provedor de acesso a Internet.

- O cliente não tem IP configurado, o qual é atribuido pelo PPPoE server (concentrador), normalmente operando em conjunto com um servidor Radius. No Mikrotik ROS, não é obrigatório o uso de servidor Radius, pois o mesmo permite a criação e gerenciamento de usuários e senhas em uma tabela local (/ppp secrets).

- PPPoE, por padrão, não é criptografado (pode-se lançar mão do método MPPE, desde que o cliente suporte este método)

Servidor ou Cliente PPPoE

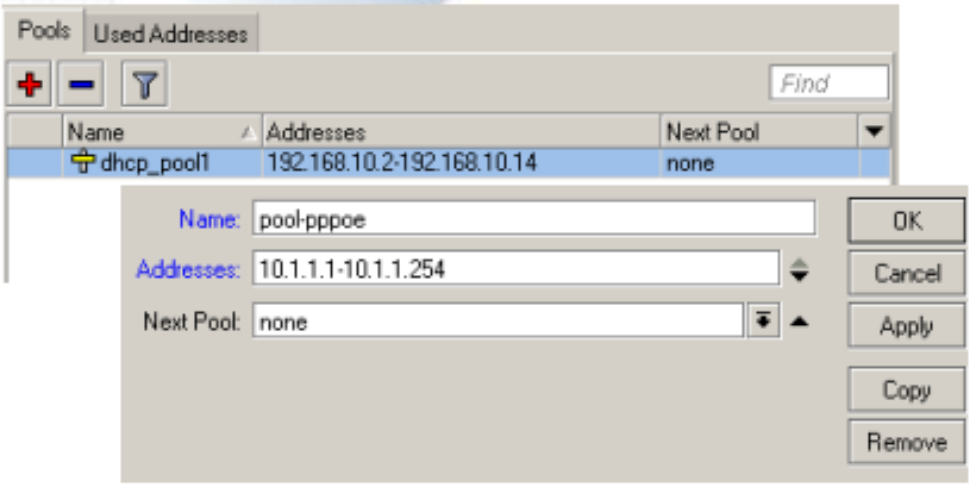


- O cliente “descobre” o servidor através do protocolo “PPPoE discover”, que tem o nome do serviço a ser utilizado.

- Precisa estar no mesmo barramento físico ou os dispositivos passarem para frente as requisições PPPoE (pppoe relay).

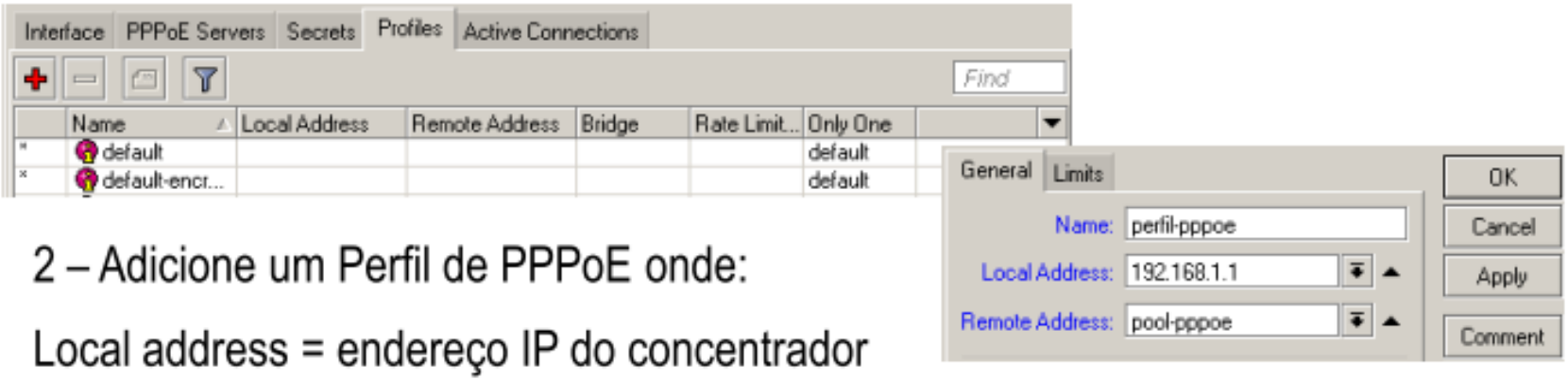
- No Mikrotik ROS o valor padrão do Keep Alive Timeout é 10, e funcionará bem na maioria dos casos. Se configurarmos para 0, o servidor não desconectará os clientes até que os mesmos solicitem ou o servidor for reiniciado.

Configuração do Servidor PPPoE



1 – Crie um pool de IP's para o PPPoE

/ip pool add name=pool-pppoe ranges=10.1.1.1-10.1.1.254

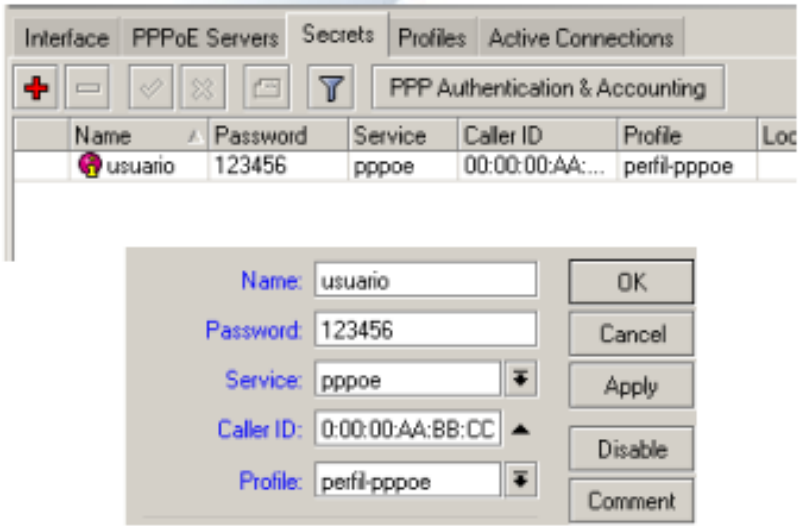


2 – Adicione um Perfil de PPPoE onde:

Local address = endereço IP do concentrador

Remote address = pool do pppoe

/ppp profile add name="perfil-pppoe" local-address=192.168.1.1 remote-address=pool-pppoe

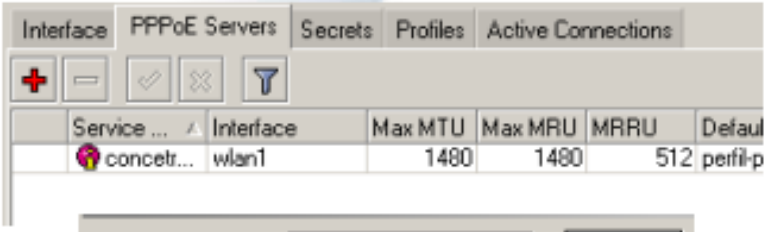


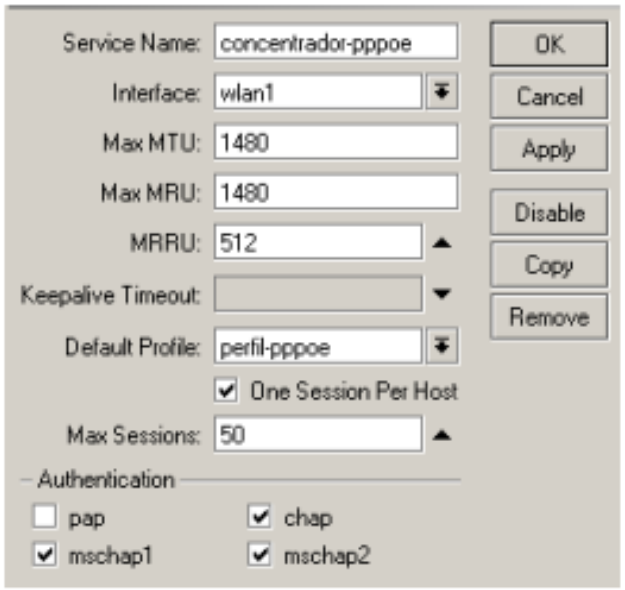
Configuração do Servidor PPPoE

3 – Adicione um usuário e senha

/ppp secret add name=usuario password=123456 service=concentrador-pppoe profile=perfil-pppoe.

Caso queira verificar o MAC-Address, adicione-o em Caller ID. Esta opção não é obrigatória, mas é um parâmetro a mais que garante segurança.





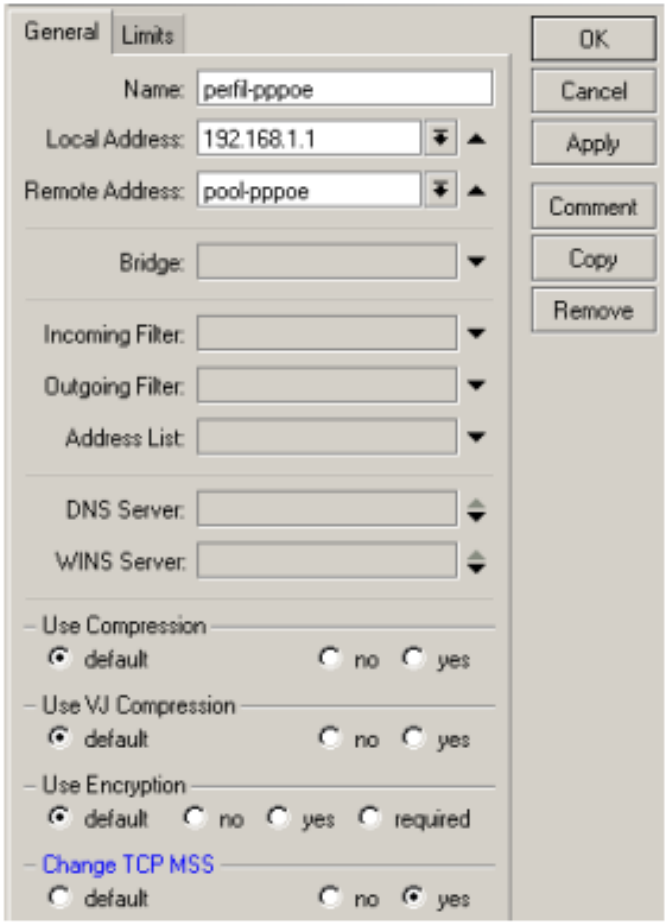
Configuração do Servidor PPPoE

4 – Adicione o PPPoE Server

→ Service Name = nome que os clientes vão procurar (pppoe-discovery).

```
/interface pppoe-server server add
    authentication=chap,mschap1,mschap2
    default-profile=perfil-pppoe disabled=no
    interface=wlan1 keepalive-timeout=10 max-
    mru=1480 max-mtu= 1480 max-sessions=50
    mrru=512 one-session-per-host=yes service-
    name=concentrador-pppoe
```

Mais sobre Perfis



→Bridge: bridge para associar ao perfil.

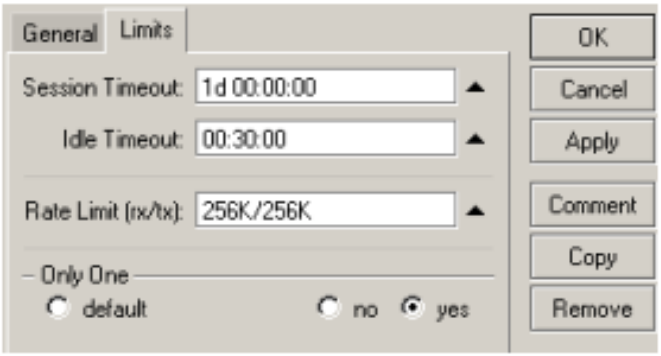
→Incoming/Outgoing Filter: nome do canal do Firewall para pacotes entrando/saindo.

→Address List: lista de endereços IPs para associar ao perfil.

→DNS Server: configuração dos servidores DNS a atribuir nos clientes. Pode se configurar mais de um endereço IP.

→ Use Compression/Encryption/Change TCPMSS: caso estejam default associam ao valor que está configurado no perfil DEFAULT-PROFILE.

Mais sobre Perfis



→ Session Timeout: é a duração máxima de uma sessão pppoe.

→ Idle Timeout: é o período de ociosidade na transmissão de uma sessão. Se não houver tráfego IP dentro do período configurado a sessão é terminada.

→Rate Limit: limitação da velocidade na forma rx-rate[/tx-rate] – rx é o upload do cliente

OBS: Pode ser usada a sintaxe: rx-rate[/tx-rate] [rx-burst-rate[/tx-burst-rate] [rx-burst-threshold[/tx-burst-threshold] [rx-burst-time[/tx-burst-time] [priority] [rx-rate-min[/tx-rate-min]]]].

→ Only One: permite apenas uma sessão para o mesmo usuário.

Mais sobre o user Database

→ Service: Especifica o servico disponível para esse cliente em particular.

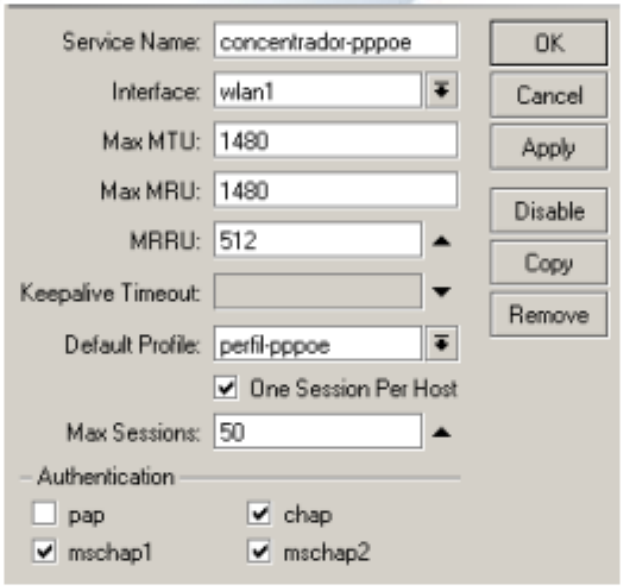
→Caller ID: MAC address do cliente

→Local Address/Remote Address: endereço IP local(servidor) e remote(cliente) que poderão ser atribuídos a um cliente em particular.

→Limit Bytes In/Out: Quantidades de Bytes que o cliente pode trafegar por sessão PPPoE

→Routes: Rotas que são criadas no lado servidor para esse cliente específico.Várias rotas podem ser adicionadas separadas por vírgula.

Detalhes adicionais do PPPoE Server



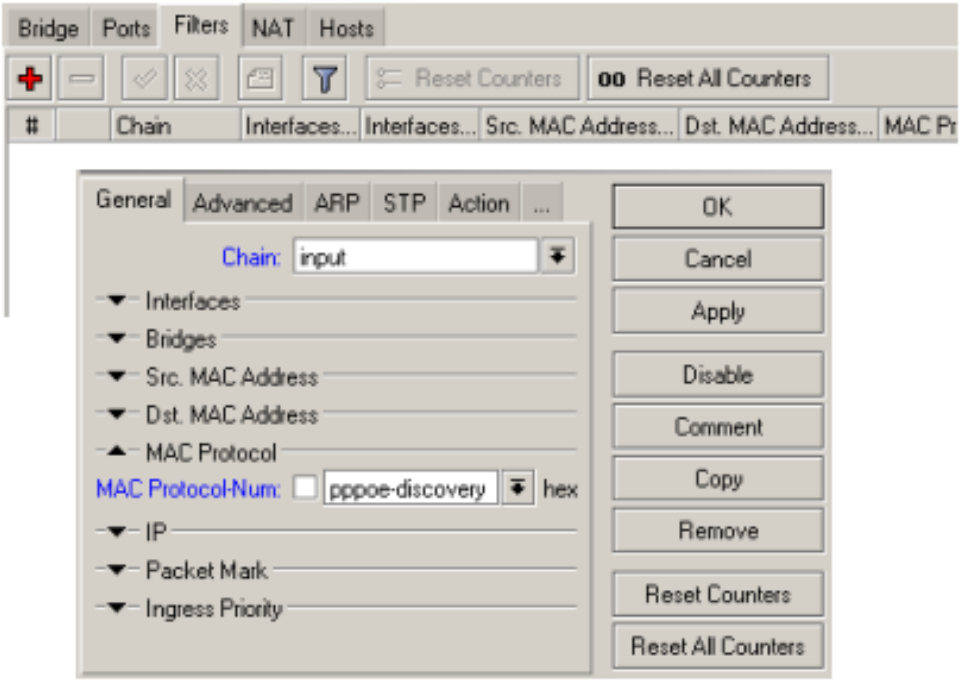
O Concentrador PPPoE do Mikrotik suporta múltiplos servidores para cada interface com diferentes nomes de serviço. Além do nome do serviço, o nome do Concentrador de Acesso pode ser usado pelos clientes para identificar o acesso em que deve se registrar.

→ Nome do Concentrador = Identidade do roteador (/system identity)

→ O valor de MTU/MRU inicialmente recomendado para o PPPoE é de 1480 bytes. Em uma rede sem fio, o servidor PPPoE pode ser configurado no Access Point. Para clientes RouterOS, a interface de rádio pode ser configurada com a MTU em 1600 bytes e a MTU da interface PPPoE em 1500 bytes. Isto otimiza a transmissão de pacotes e evita problemas associados com MTU menor que 1500 bytes. Até o momento não possuímos nenhuma maneira de alterar a MTU da interface sem fio em clientes MS Windows.

→ One session per Host: permite apenas uma sessão por host (MAC address)

→ Max Sessions: número máximo de sessões simultâneas que o Concentrador suportará.

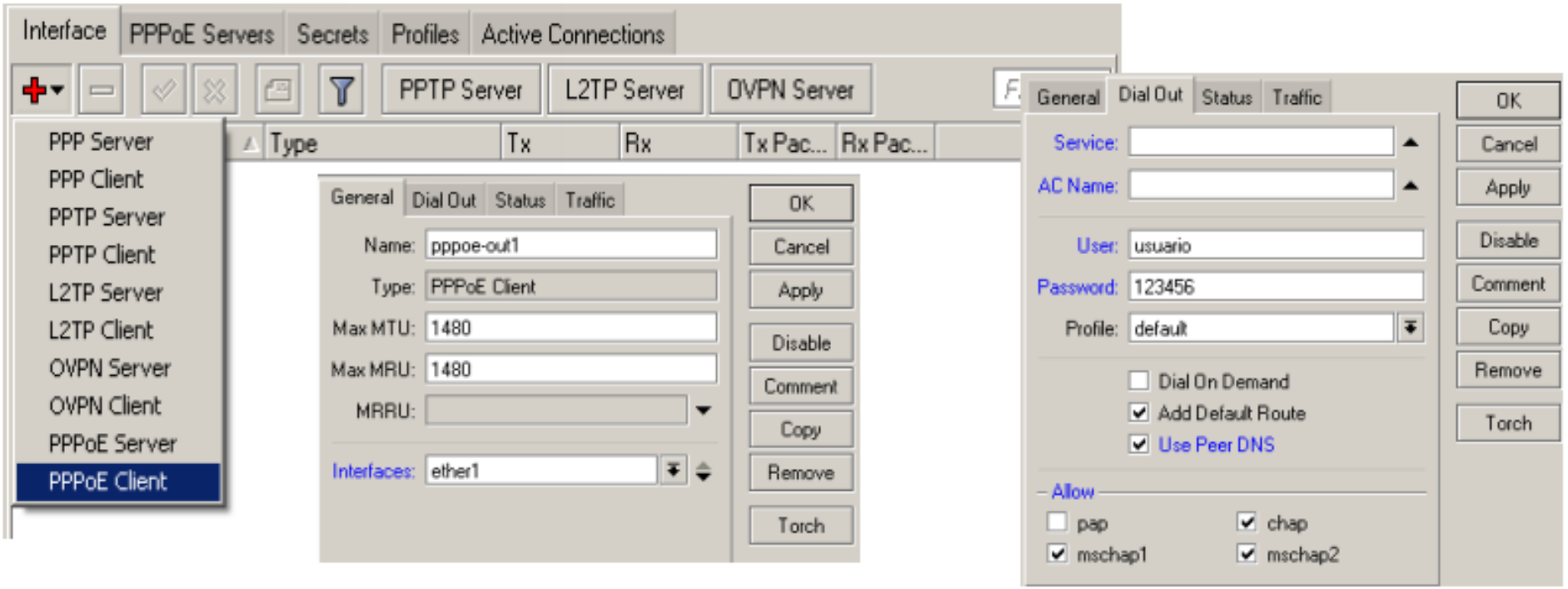


Segurança no PPPoE

→ Para assegurar um servidor PPPoE pode-se utilizar Filtros de Bridge, configurando a entrada ou repasse (depende da configuração do Mikrotik ROS) os protocolos pppoe-discovery e pppoe-session, e descartando todos os demais.

→ Mesmo que haja somente uma interface, ainda assim é possível utilizar os Fitros de Bridge, bastando para tal, criar um bridge e associar em Ports apenas esta interface. Em seguida alterar no PPPoE Server a interface que o mesmo escuta.

Configuração do PPPoE Client

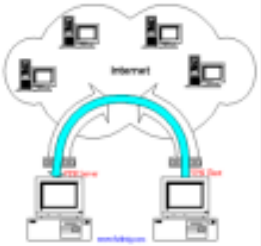


→AC Name: nome do Concentrador. Deixando em branco conecta com qualquer um.

→ Dial on Demand: disca automaticamente sempre que é gerado um tráfego de saída.

→Add default route: adiciona uma rota padrão (não usa a do servidor).

→Use Peer DNS: Usa o DNS configurado no Concentrador.



PPTP e L2TP

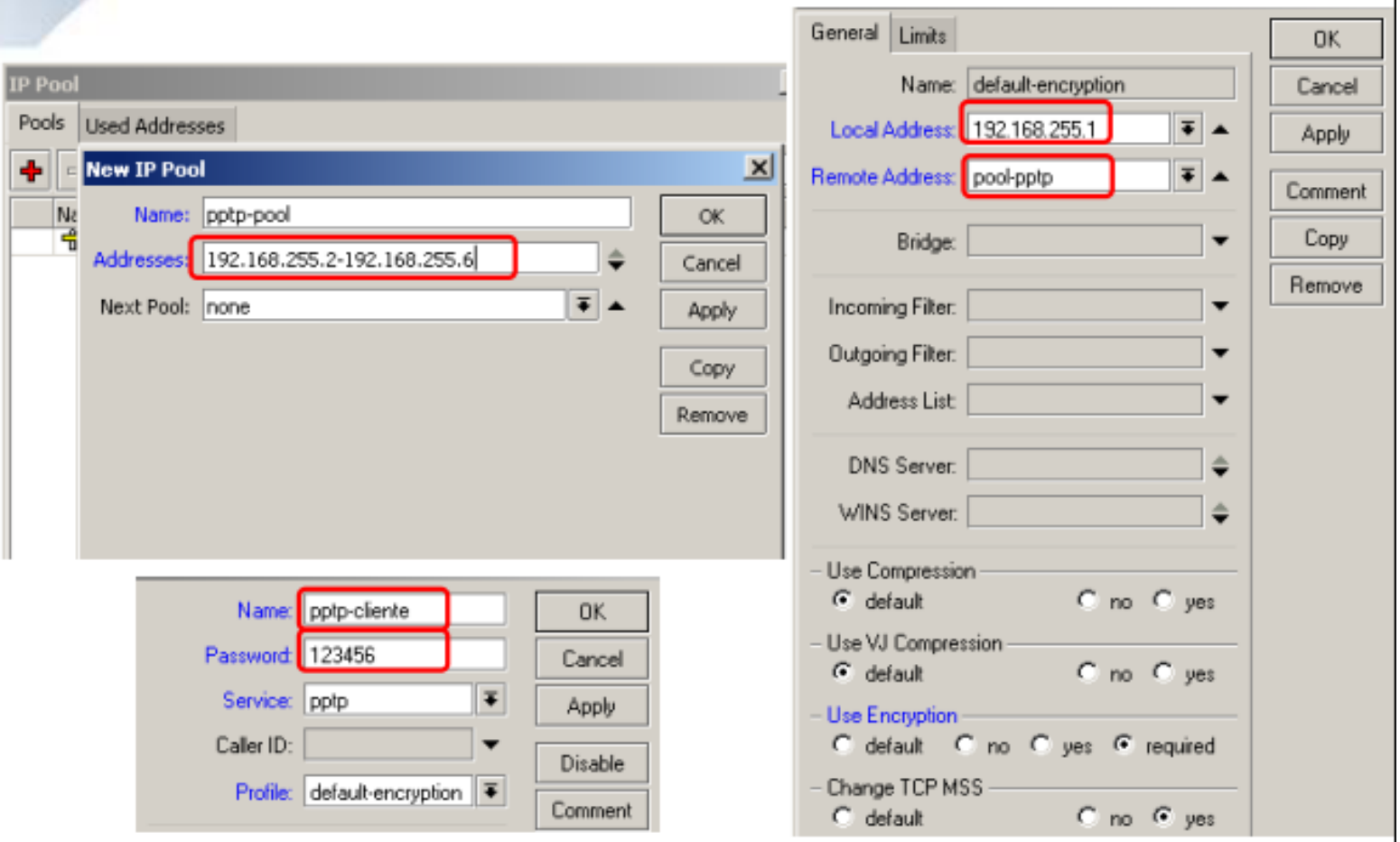
Point-to-Point Tunneling Protocol e Layer 2 Tunneling Protocol

- L2TP – Layer 2 Tunnel Protocol – Protocolo de tunelamento de camada 2 é um protocolo de tunelamento seguro para transportar tráfego IP utilizando PPP. O protocolo L2TP trabalha no *layer 2* de forma criptografada ou não e permite enlaces entre dispositivos de diferentes redes unidos por diferentes protocolos.

- O tráfego L2TP utiliza protocolo UDP tanto para controle como para pacotes de dados. A porta UDP 1701 é utilizada para o estabelecimento do link e o tráfego em si utiliza qualquer porta UDP disponível, o que significa que L2TP pode ser usado com a maioria dos *Firewalls* e *Routers*, funcionando também através de NAT.

- L2TP e PPTP possuem as mesmas funcionalidades.

Configuração do Servidor PPTP e L2TP

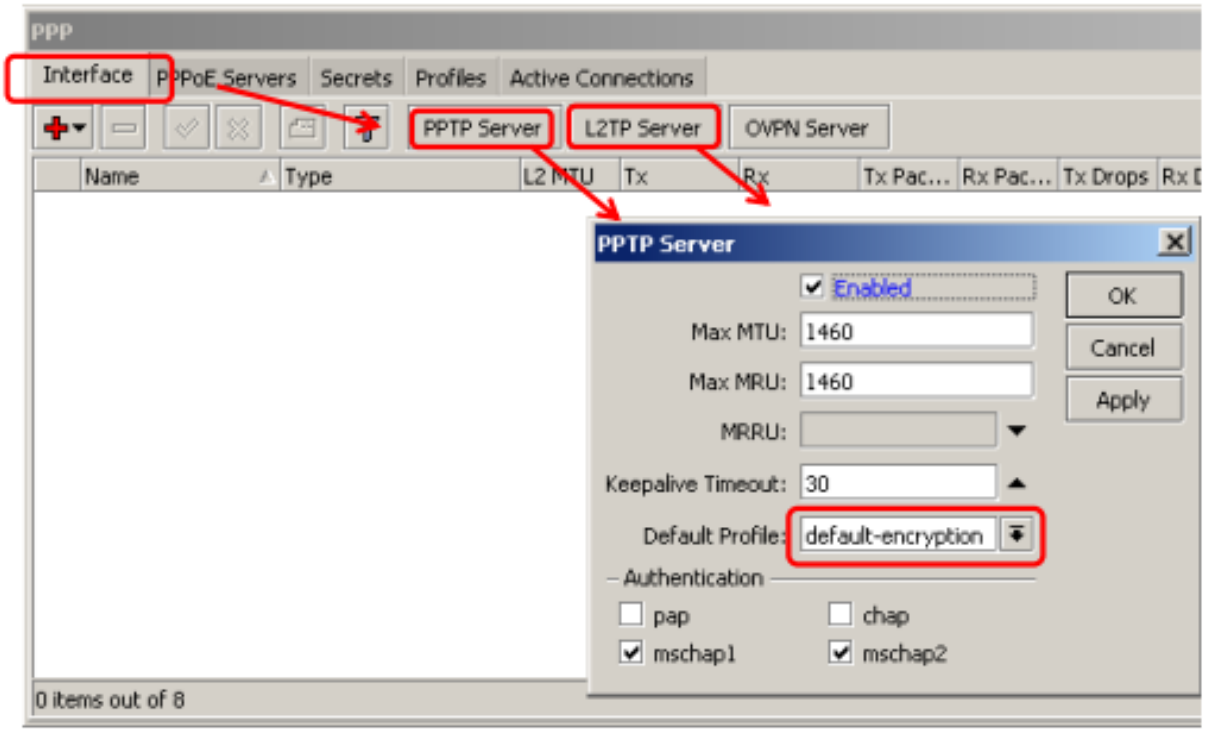


- Configure um faixa de endereços IP, em IP POOL, um perfil para o PPTP e um usuário em PPP Secrets, conforme as imagens.

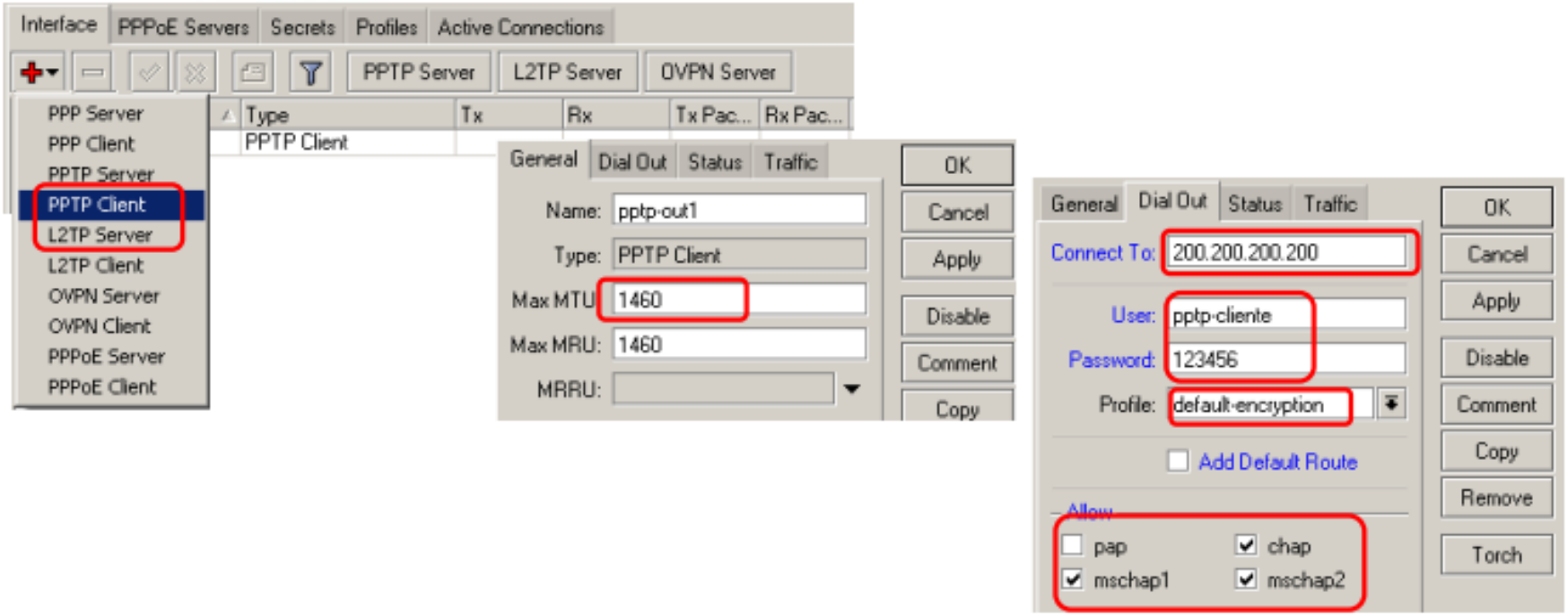
Configuração do Servidor PPTP e L2TP

- Configure os servidores PPTP e L2TP
- Atente-se para o perfil a utilizar
- Configure nos hosts locais um cliente PPTP e realize a conexão com um servidor de outra rede diferente da rede conectada.

➢ *Ex.: hosts da rede 192.168.100.0/24 conectarem-se a servidores da rede 192.168.200.0/24 e vice-versa.*

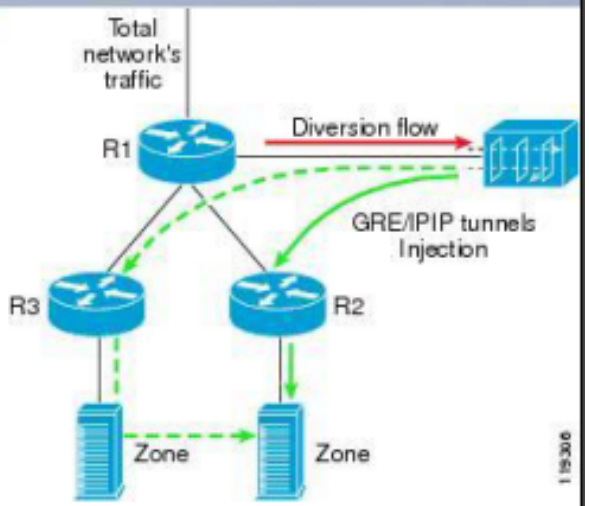


Configuração do cliente PPtP e L2TP



As configurações para o cliente PPTP ou L2TP são bastante simples, conforme observamos nas imagens.

Túneis IPIP



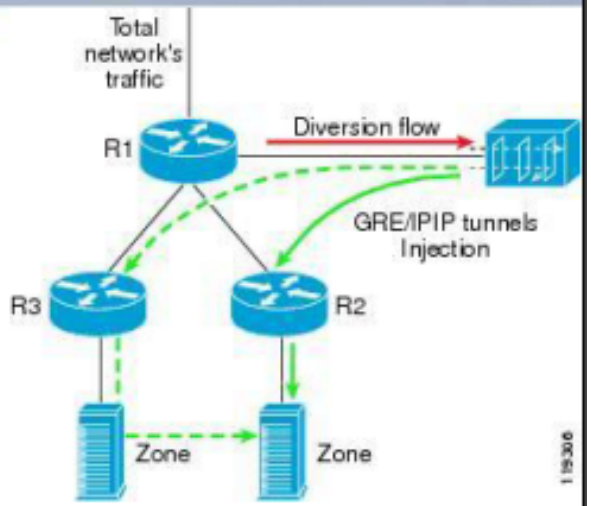
IPIP é um protocolo que encapsula pacotes IP sobre o próprio protocolo IP baseado na RFC 2003. É um protocolo simples que pode ser usado para ligar duas Intranets através da Internet usando 2 roteadores.

A Interface do túnel IPIP aparece na lista de interfaces como se fosse uma interface real.

Vários roteadores comerciais, incluindo o Cisco e roteadores baseados em Linux suportam esse protocolo.

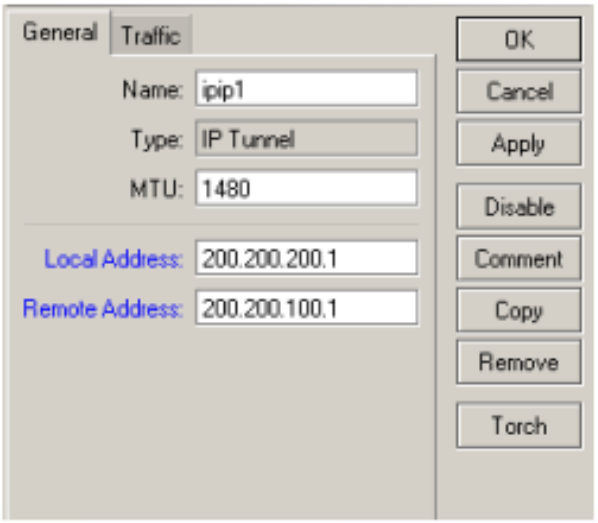
Um exemplo prático de uso de IPIP seria a necessidade de monitorar *hosts* através de um NAT, onde o túnel IPIP colocaria a rede privada disponível para o *host* que realiza o monitoramento, sem necessidade de criação de usuário e senha como nas VPNs.

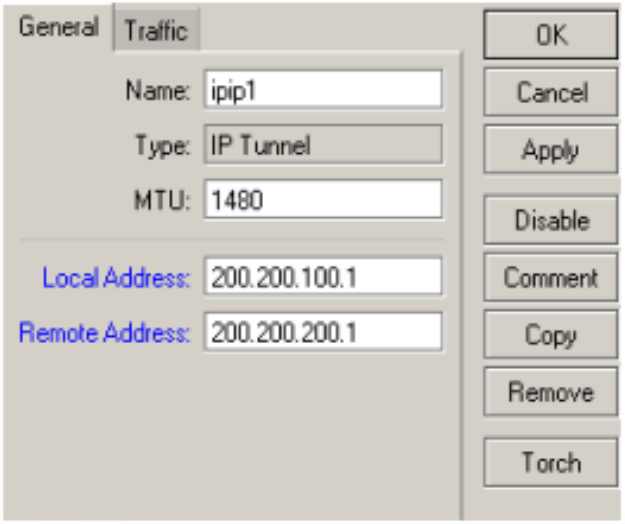
Túneis IPIP



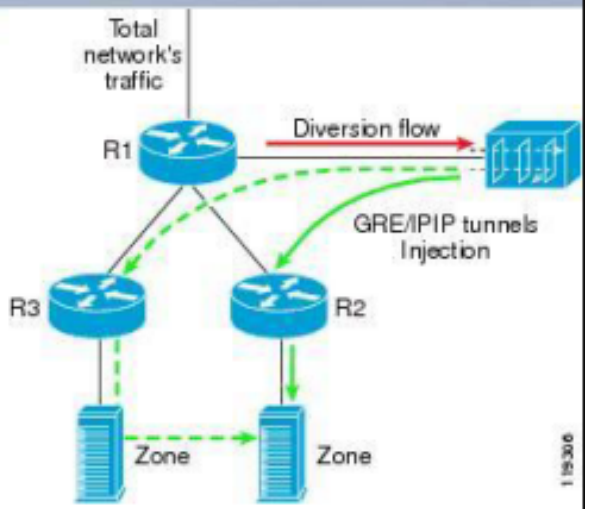
Exemplo:

Supondo que temos de unir as redes que estão por trás dos roteadores 200.200.200.1 e 200.200.100.1. Para tanto basta que criemos as interfaces IPIP em ambos, da seguinte forma:

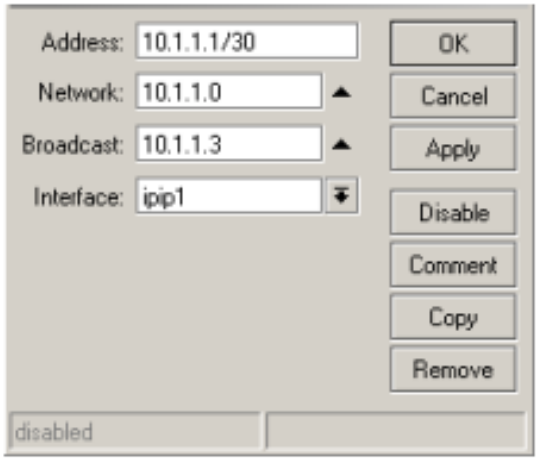


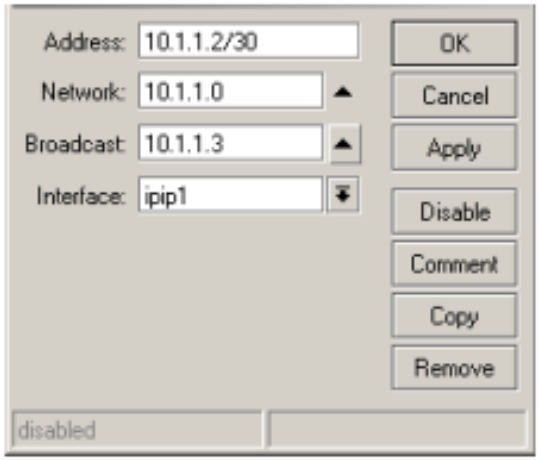


Túneis IPIP



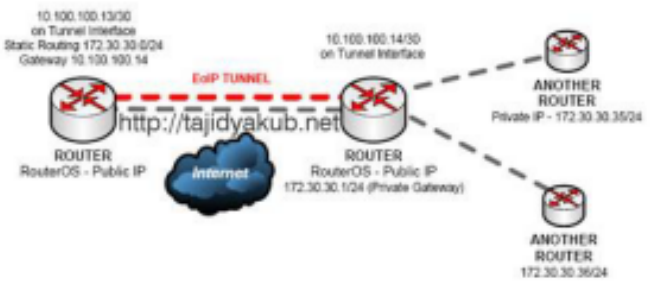
Em seguida atribui-se endereço IP às interfaces criadas (de preferência ponto a ponto)





Pronto, está criado o túnel IPIP e agora as redesfazem parte do mesmo domínio de *broadcast*.

Túneis EoIP



EoIP (Ethernet over IP) é um protocolo proprietário Mikrotik para encapsulamento de todo tipo de tráfego sobre o protocolo IP. Quando habilitada a função de *bridge* dos roteadores que estão interligados através de um túnel EoIP, todo o tráfego é passado de um lado para o outro como se houvesse um cabo de rede interligando os pontos, mesmo roteando pela Internet e por vários protocolos.

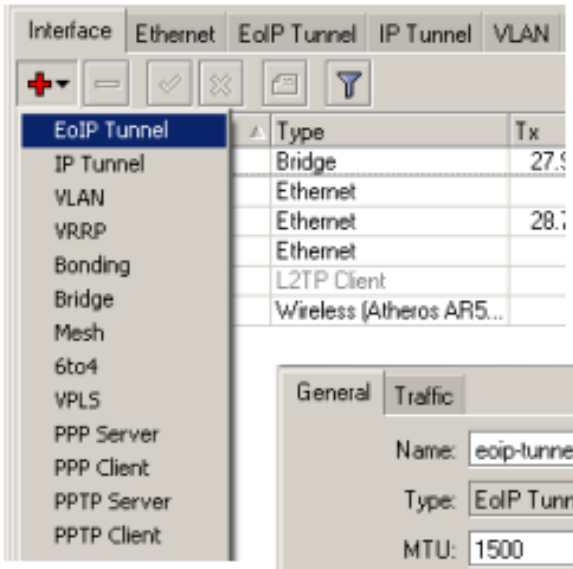
EoIP possibilita:

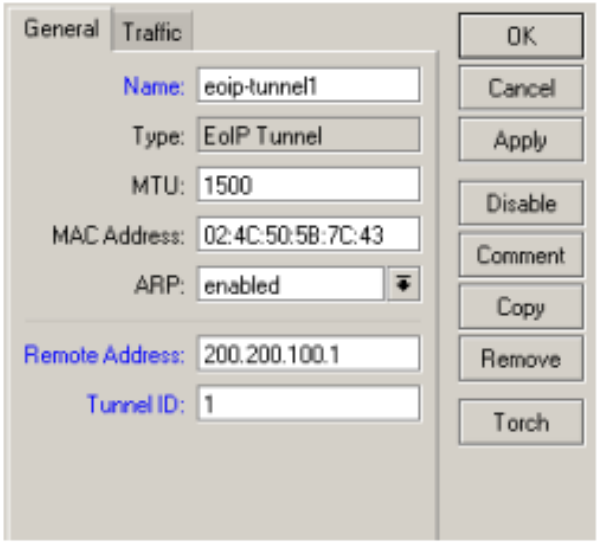
- Interligação em *bridge* de LAN's remotas através da Internet
- Interligação em *bridge* de LAN's através de túneis criptografados
- Possibilidade de "bridgear" LAN's sobre redes Ad Hoc 802.11

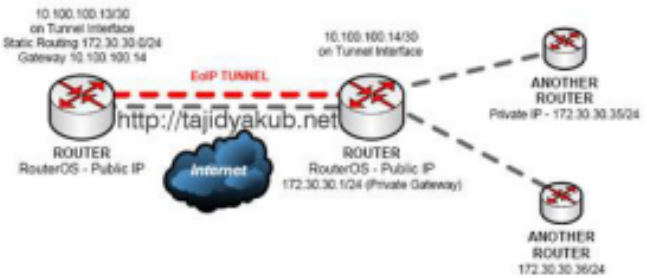
Características:

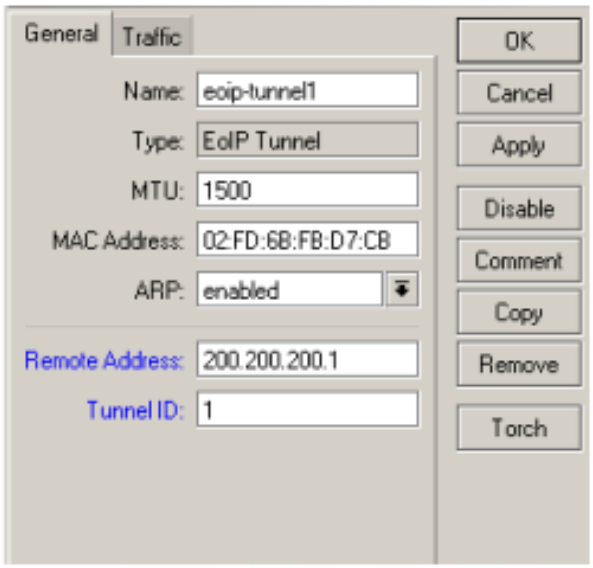
- A interface criada pelo túnel EoIP suporta todas as funcionalidades de uma interface Ethernet. Endereços IP e outros túneis podem ser configurados na interface EoIP.
- O protocolo EoIP encapsula *frames Ethernet* através do protocolo GRE.
- O número máximo de túneis suportados no Mikrotik ROS são 65536.

Túneis EoIP









Criando um túnel EoIP entre as redes que estão por trás dos roteadores 200.200.200.1 e 200.200.100.1.

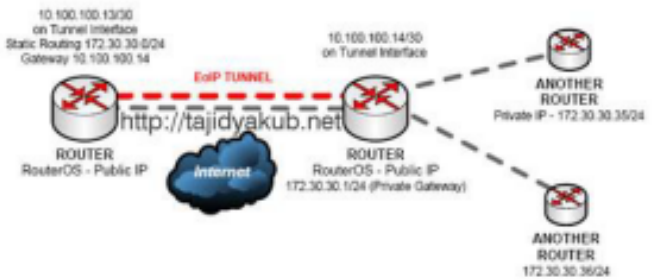
OBS:

- Os MAC's devem ser diferentes e estar entre o range 00-00-5E-80-00-00 to 00-00-5E-FF-FF-FF, pois são endereços reservados para essas aplicações.

-O MTU deve ser deixado em 1500 para evitar fragmentações.

- O túnel ID deve ser o mesmo em ambos os lados.

Túneis EoIP



Bridge | Ports | Filters | NAT | Hosts

	Interface	Bridge	Priority (h...	Path Cost	Horizon	Role
	ether2	bridge1	80	10		designated port
I	ether3	bridge1	80	10		disabled port
	wlan1	bridge1	80	10		designated port

General | Status

Interface: eoip-tunnel1
Bridge: bridge1
Priority: 80 hex
Path Cost: 10
Horizon:
Edge: auto
Point To Point: auto
External FDB: auto

OK | Cancel | Apply | Disable | Comment | Copy | Remove

- Adicione a interface EoIP à *bridge*, juntamente com a interface da rede que fará parte do mesmo domínio de *broadcast* (normalmente uma interface da rede privada – LAN).

Dúvidas ??

Hotspot no Mikrotik

Hotspot

O que é ?

Hotspot é um termo utilizado para se referir a uma área pública onde está disponível um serviço de acesso a Internet, normalmente através de uma rede sem fio Wi-Fi. Aplicações típicas incluem o acesso em Hotéis, Aeroportos, Shoppings, Universidades, etc.

O conceito de Hotspot pode ser usado no entanto para dar acesso controlado a uma rede qualquer, com ou sem fio, através de autenticação baseada em nome de usuário e senha.

Como funciona ?

Quando em uma área de cobertura de um Hotspot, um usuário que possua um Laptop e tente navegar pela WEB é arremetido para uma página do Hotspot que pede suas credenciais, normalmente usuário e senha. Ao fornece-las e sendo um cliente autorizado pelo Hotspot o usuário ganha acesso à Internet podendo sua atividade ser controldada e bilhetada.

Hotspot

Setup do Hotspot:

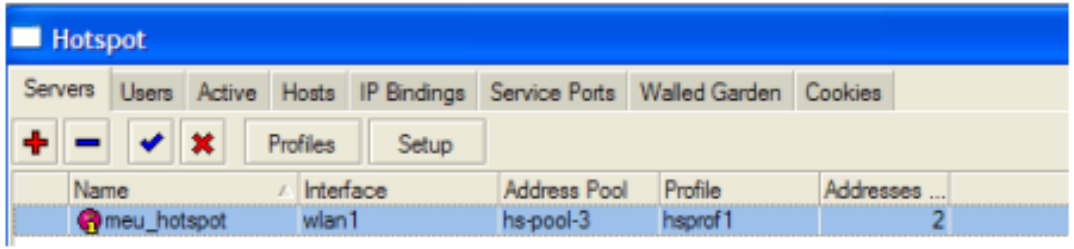
1 – Escolha a interface que vai "ouvir" o Hotspot

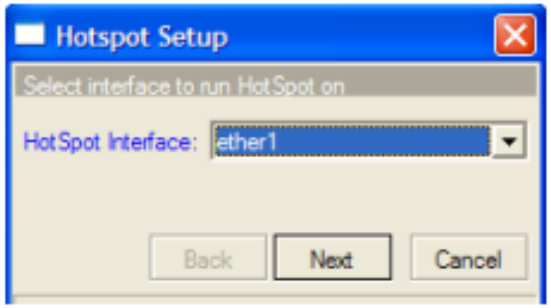
2 – Escolha o IP em que vai rodar o Hotspot e indique se a rede será mascarada

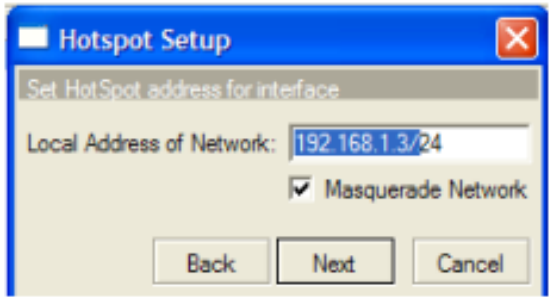
3 – Dê um pool de endereços que serão distribuidos para os usuários do Hotspot (se não tiver, crie em /ip pool)

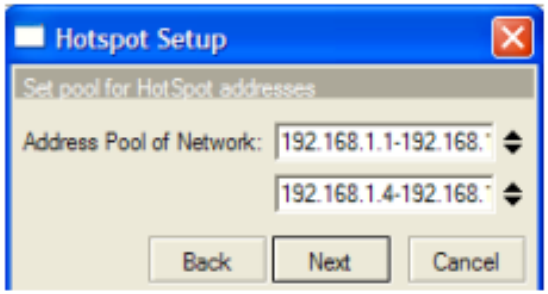
4 – Selecione um certificado, caso queira usar.

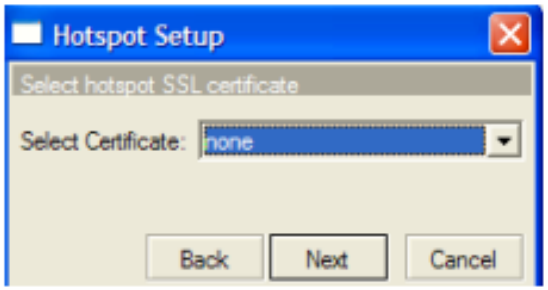
continua…











Hotspot

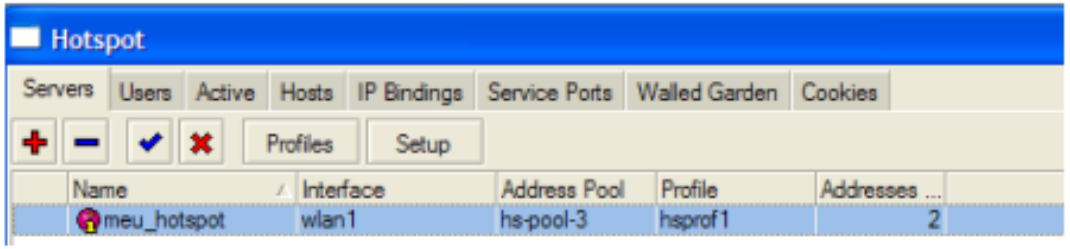
Setup do Hotspot: continuação

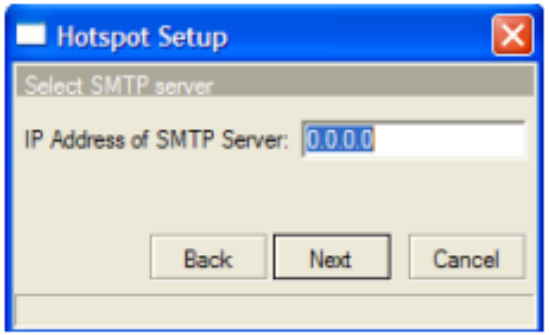
5 – Se quiser forçar a usar o seu smtp, indique o IP aqui

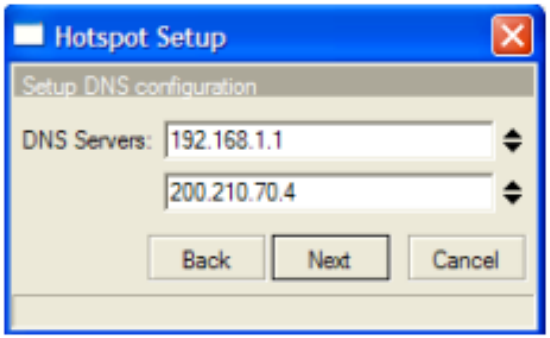
6 – Dê o endereço IP dos servidores de DNS que irão resolver os nomes para os usuários do Hotspot

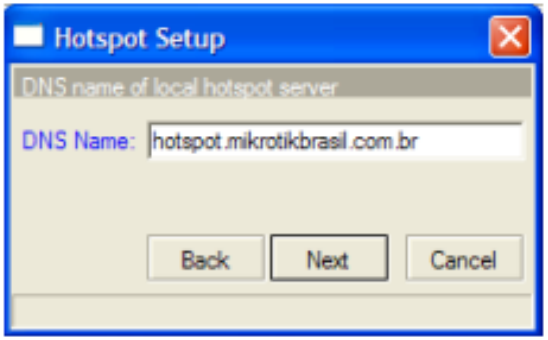
7 – Dê o nome do DNS (aparecerá no Browser dos clientes ao invés do IP)

Pronto, está configurado o Hotspot !





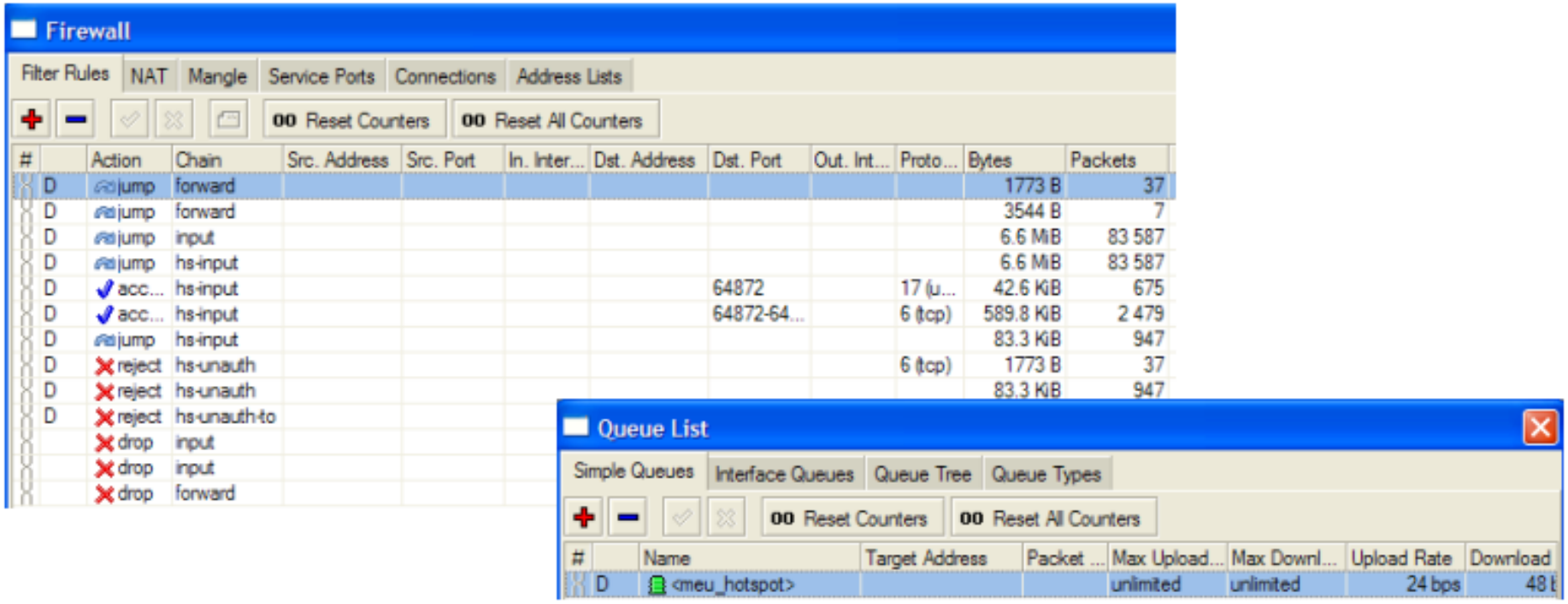




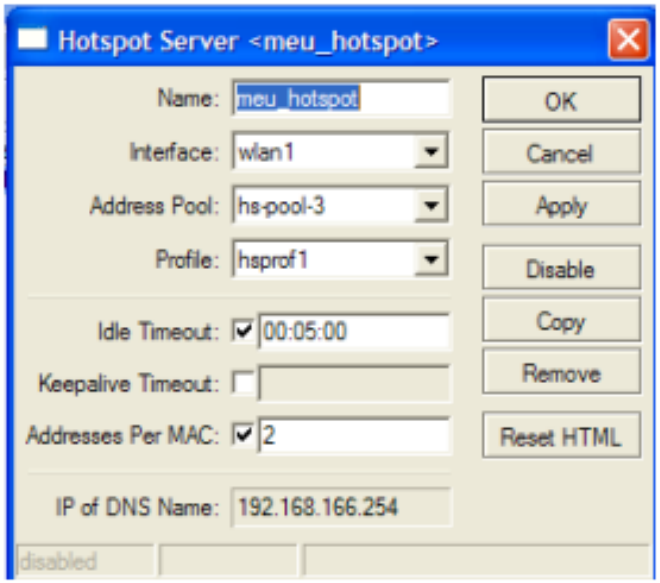
OBS: os mesmos passos acima podem ser feitos no terminal com /ip hotspot setup

Hotspot

Embora tenha sido uma configuração bastante fácil e rápida, o Mikrotik se encarregou de fazer o trabalho pesado, criando as regras apropriadas no Firewall, bem como uma fila específica para o Hotspot.



Hotspot - Detalhes de Configuração



→ **keepalive-timeout** (*time* | *none* ; default: **00:02:00**) Utilizado para detectar se o computador do cliente está ativo e encontrável. Caso nesse período de tempo o teste falhe, o usuário é tirado da tabela de hosts e o endereço Ip que ele estava usando é liberado. O tempo é contabilizado levando em consideração o momento da desconexão menos o valor configurado (2 minutos por default)

→ **idle-timeout** (*time* | *none* ; default: **none**) – máximo período de inatividade para clientes autorizados. É utilizado para detecta que clientes não estão usando redes externas (internet em geral) e que não há tráfego do cliente através do roteador. Atingindo o timeou o cliente é derrubado da lista dos hosts, o endereço IP liberado e a sessão contabilizada a menos desse valo.

→ **addresses-per-mac** (*integer* | *unlimited* ; default: **2**) – número de IP's permitidos para um particular MAC

Hotspot Server Profiles

→ **HTML Directory:**

Diretório onde estão colocadas as páginas desse Hotspot

→ **HTTP Proxy / HTTP Proxy Port**

Endereço e porta do Servidor de Web Proxy

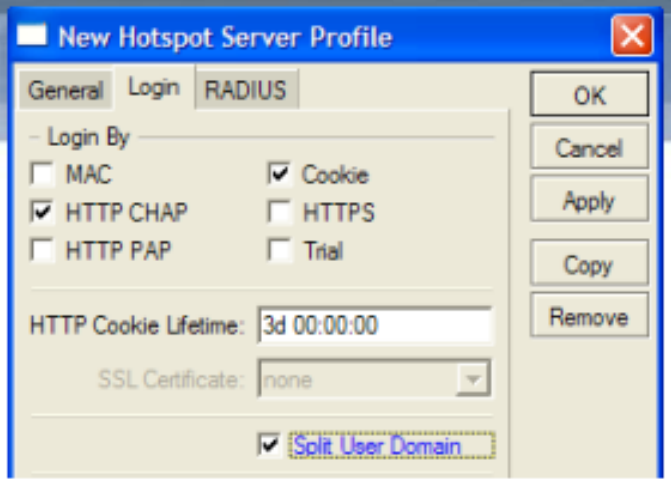
→ **SMTP Server:**

Endereço do servidor de SMTP

→ **rate-limit:**

Cria uma simple Queue para todo o Hotspot (vai após as filas dinamicas dos usuários.

Hotspot Server Profiles

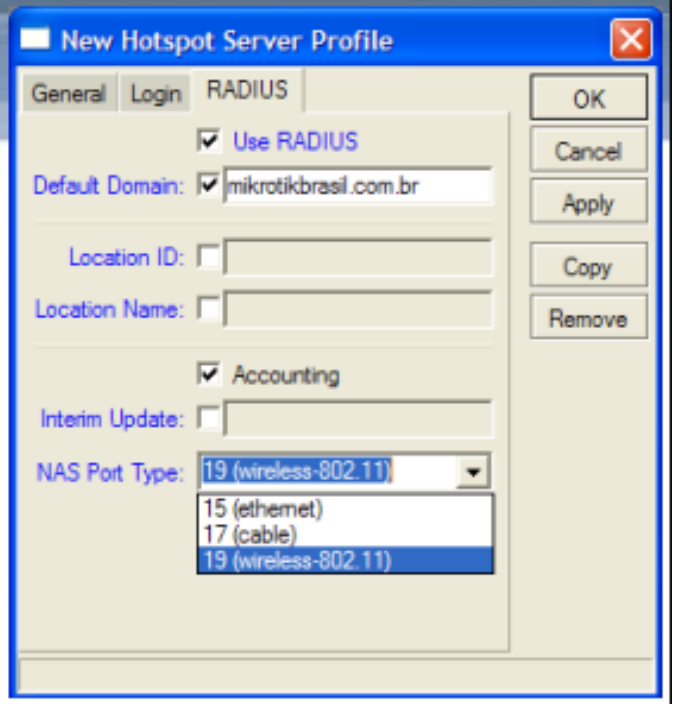


→**login-by**

- **cookie** - usa HTTP cookies para autenticar sem pedir as credenciais. Se o cliente ainda não tiver um cookie ou tiver expirado usa outro método
- **http-chap** - usa método CHAP – método criptografado
- **http-pap** - usa autenticação com texto plano – pode ser sniffado facilmente
- **https** – usa tunel SSL criptografado. Para isso funcionar, um certificado válido deve ser importado para o roteador.
- **mac** – Tenta usar o MAC dos clientes primeiro como nome de usuário. Se existir na tabela de usuários local ou em um Radius, o cliente é liberado sem username/password
- **trial** – não requer autenticação por um certo período de tempo

→**HTTP Cookie Lifetime**: tempo de vida dos Cookies

→ **Split User Domain**: corta o dominio do usuário no caso de usuário@dominio.com.br



Hotspot Server Profiles

Utilização de servidor Radius para autenticação do Hotspot
:

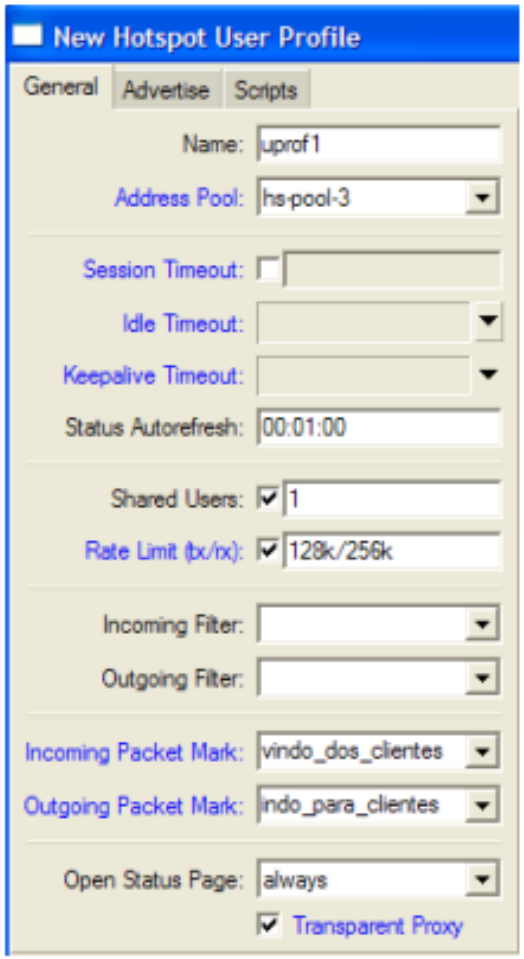
→ Location ID e Location Name: Podem ser atribuidos aqui ou no Radius – normalmente deixar em branco.

→Habilitar Accounting para fazer a bilhetagem dos usuários, com histórico de logins, desconexões, etc

→Interim Update: Frequencia de envio de informações de accounting (segundos). 0 – assim que ocorre o evento.

→NAS Port Type: Wireless, Ethernet ou Cabo

Hotspot User Profiles



Os user profiles servem para dar tratamento diferenciado a grupos de usuários, como suporte, comercial, diretoria, etc

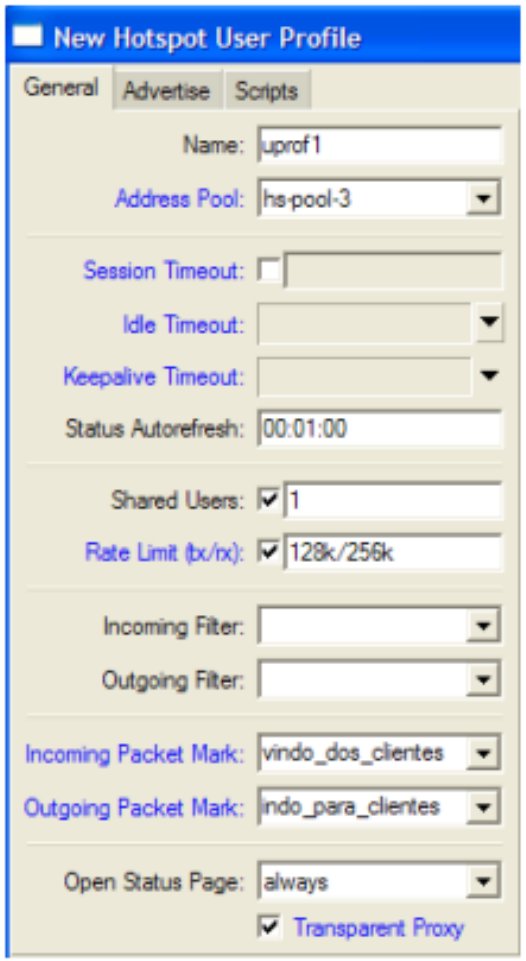
→Session Timeout: tempo máximo permitido (depois disso o cliente é derrubado)

→ Idle Timeout / Keepalive Timeout: mesma explicação anterior, no entanto agora somente para os usuários desse perfil.

→ Status Autorefresh: tempo de refresh da página de Status do Hotspot

→ Shared Users: número máximo de clientes com o mesmo username.

Hotspot User Profiles



Os perfis dos usuários podem conter os limites de velocidade implementados de forma completa, com bursts, limit-at, etc

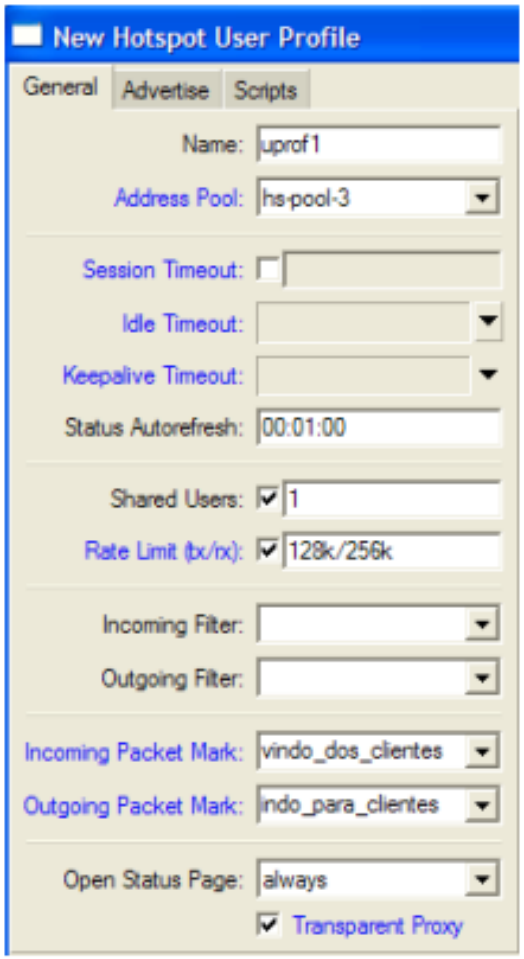
→Rate Limit:

rx-rate[/tx-rate] [rx-burst-rate[/tx-burst-rate]] [rx-burst-threshold[/tx-burst-threshold]] [rx-burst-time[/tx-burst-time]] [priority] [rx-limit-at[tx-limit-at]]

Exemplo: 128k/256k 256k/512k 96k/192k 8/8 6 32k/64k

-- 128k de upload, 256k de download
-- 256k de burst p/ upload, 512k de burst p/ download
-- 96k de threshold p/ upload, 192k de threshold p/ download
-- 8 segundos de burst time
-- 6 de prioridade
-- 32k de garantia de upload, 64k de garantia de download

Hotspot User Profiles



→Incoming Filter: nome do firewall chain aplicado aos pacotes que chegam dos usuários deste perfil

→ Outgoing Filter: nome do firewall chain aplicado aos pacotes que vão para os usuários desse perfil

→ Incoming Packet Mark: Marca colocada automáticamente em todos os pacotes oriundos de usuários desse perfil

→ Outgoing Packet Mark: Marca colocada em todos os pacotes que vão para os usuários desse perfil.

→ Open Status Page: mostra a página de status
- → http-login : para usuários normais que logam pela web
- → always ; para todos, inclusive os que logam por MAC

→ Transparent Proxy: se deve usar proxy transparente

Hotspot User Profiles

Com a opção Advertise é possível enviar de tempos em tempos popups para os usuários do Hotspot.

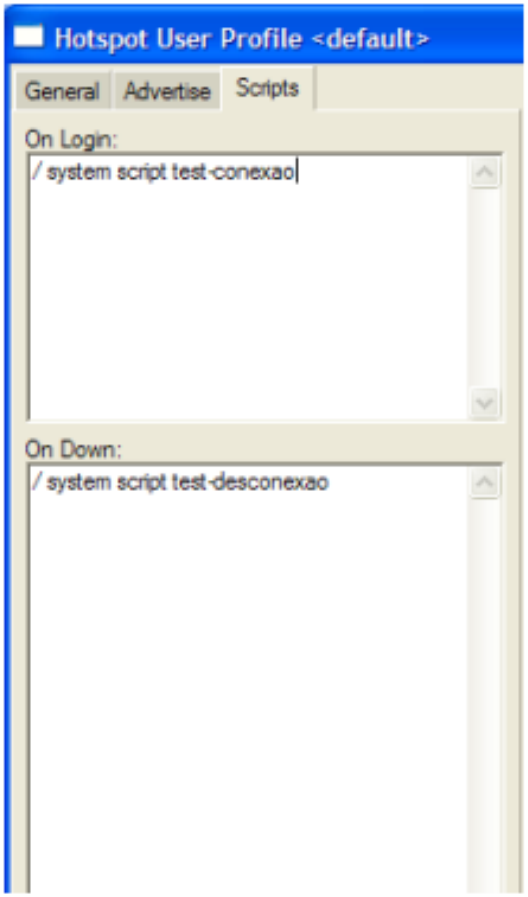
→Avertise URL: Lista das páginas que serão anunciadas. A lista é cíclica, ou seja quando a última é mostrada, começa-se novamente pela primeira.

→ Advertise Interval: Intervalos de exibição dos Popups. Depois da sequencia terminada, usa sempre o último intervalo. No exemplo, são mostradas inicialmente a cada 30 segundos, 3 vezes e depois a cada 1 hora.

→ Advertise Timeout: Quanto tempo deve esperar para o anúncio ser mostrado, antes de bloquear o acesso à rede com o "Walled-Garden"

- → pode ser configurado um tempo (default = 1 minuto)
- → nunca bloquear
- → bloquear imediatamente

Hotspot User Profile - Scripts



O mikrotik possui uma linguagem interna de scripts que podem ser adicionados para serem executados em alguma situação específica.

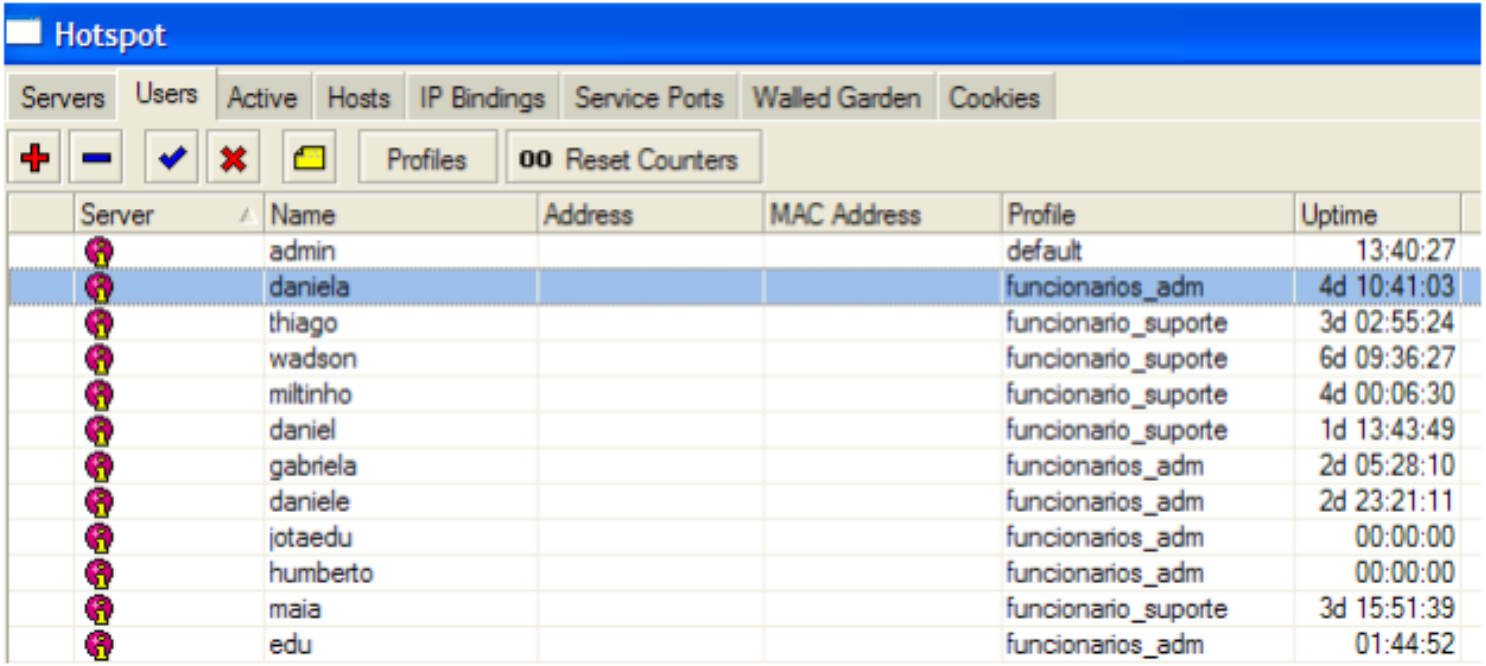
No Hotspot é possível criar scripts que executem comandos a medida que um usuário desse perfil se conecta ou se desconecta do Hotspot

-Os parâmetros que controlam essas execuções são

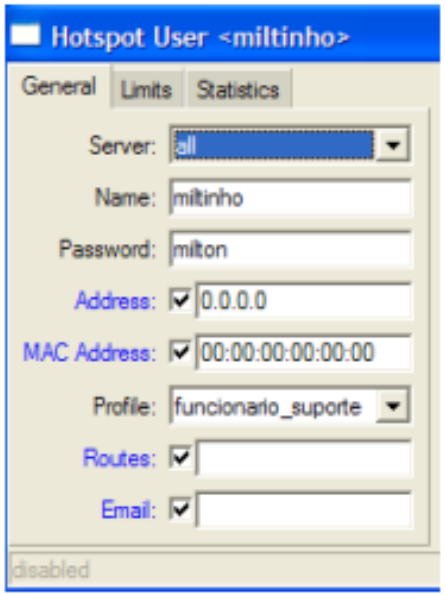
→on-login
→on-logout

Os scripts são adicionados com / system scripts add

Hotspot Users



Hotspot Users



Detalhes de cada usuário:

→ all para todos os hotspots configurados ou para um específico.

→ Name: Nome do usuário. Se o modo trial estiver habilitado o Hotspot colocará automáticamente o nome T-MAC_address. No caso de autenticação por MAC, o MAC pode ser adicionado como username (sem senha).

→Endereço IP: caso queira vincular esse usuário a um endereço fixo.

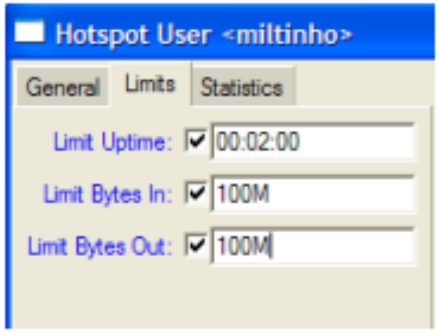
→ MAC Address: caso queira vincular esse usuário a um MAC determinado

→ Profile: perfil de onde esse usuário herda as propriedades

→Routes: rota que será adicionada ao cliente quando esse se conectar. Sintaxe endereço de destino gateway metrica. Exemplo 192.168.1.0/24 192.168.166.1 1. Várias rotas separadas por vírgula podem ser adicionadas.

→ Email: ?

Hotspot Users



→Limit Uptime: Total de tempo que o usuário pode usar o Hotspot. Útil para fazer acesso pré pago. Sintaxe hh:mm:ss. Default = 0s – sem limite.

→ Limit Bytes In: total de Bytes que o usuário pode transmitir. (bytes que o roteador recebe do usuário.

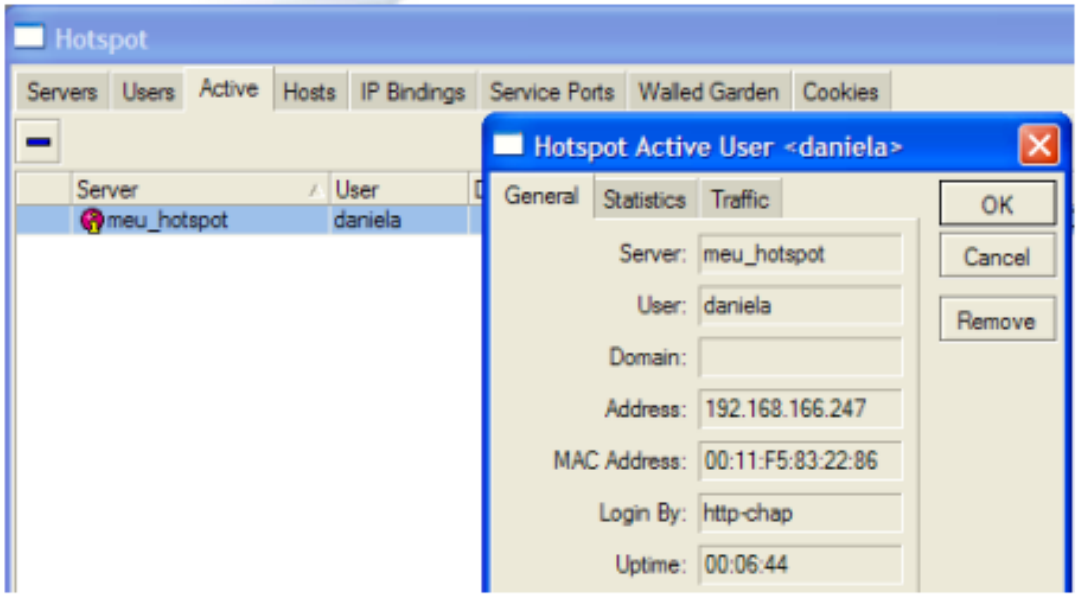
→ Limit Bytes Out: total de Bytes que o usuário pode receber. (bytes que o roteador transmite para o usuário.

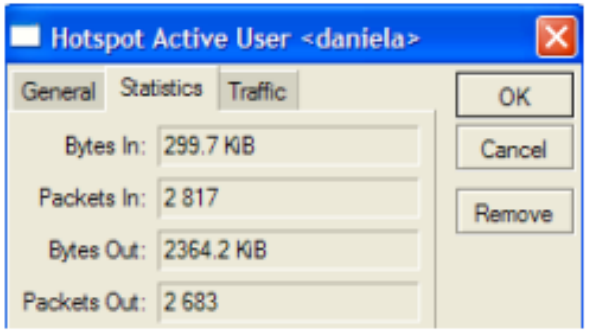
Os limites valem para cada usuário. Se um usuário já fez o download de parte de seu limite, o campo session limit vai mostrar o restante. Quando o usuário exceder seu limite será impedido de logar. As estatísticas são atualizadas cada vez que o usuário faz o logoff, ou seja enquanto ele estiver logado as estatísticas não serão mostradas.

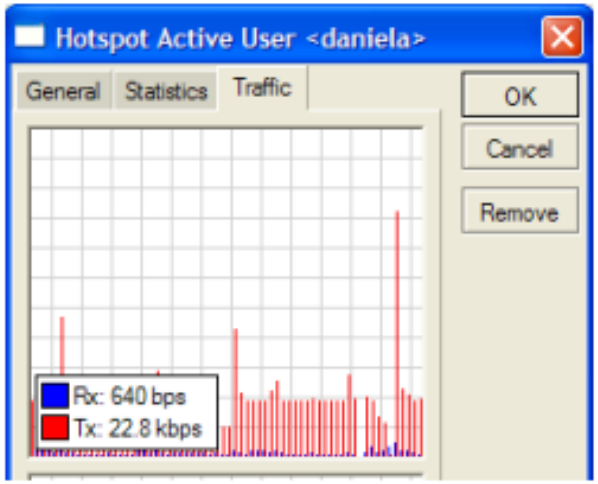
Use **/ip hotspot active** para ver as estatísticas atualizadas nas sessões correntes dos usuários.

Se um usuário tem o endereço IP especificado somente poderá haver um logado. Caso outro entre com o mesmo usuário/senha, o primeiro será desconectado.

Hotspot Active

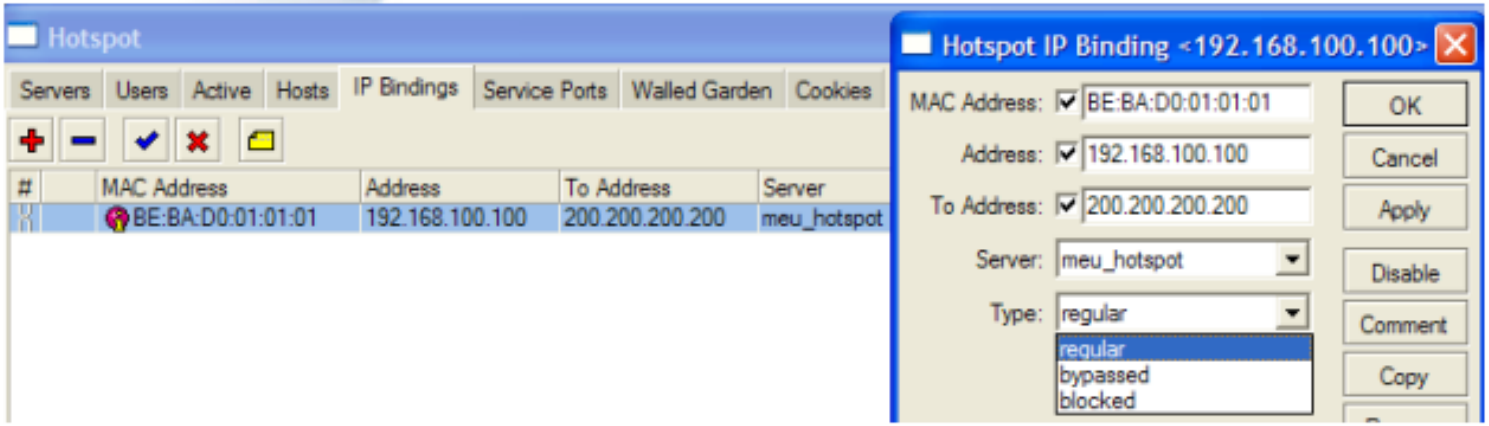






Mostra dados gerais e estatísticas de todos os usuários conectados

IP Bindings

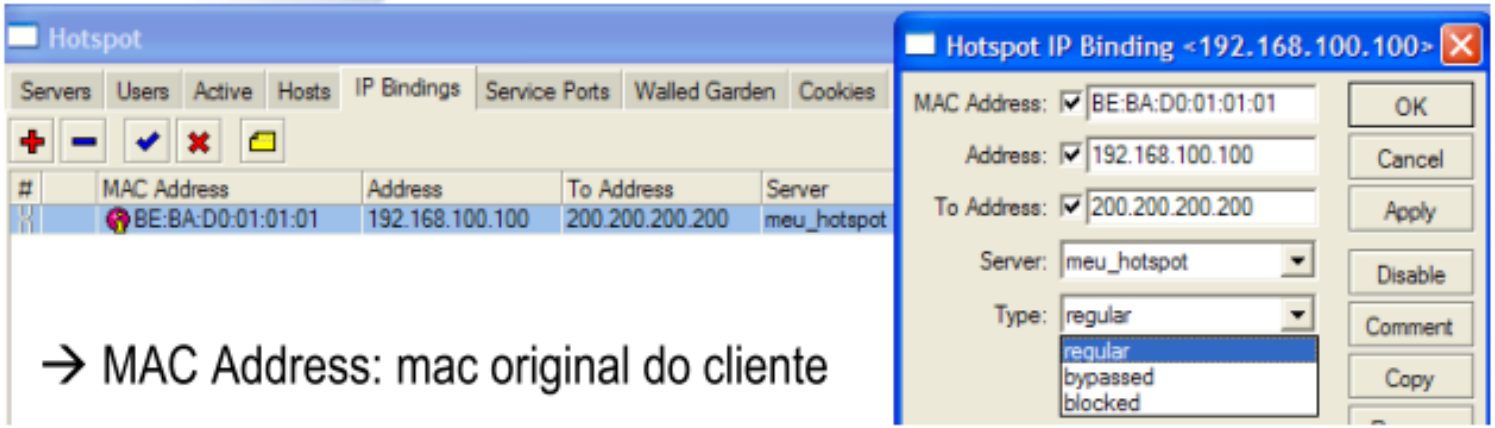


O Mikrotik por default tem habilitado o “universal client” que é uma facilidade que aceita qualquer IP que esteja configurado no cliente fazendo com ele um NAT 1:1. Esta facilidade é denominada “DAT” na AP 2500 e “eezee” no StarOS.

É possível fazer também traduções NAT estáticas com base no IP original, ou IP da rede ou no MAC do cliente. É possível também permitir a certos endereços contornarem (“by-passarem”) a autenticação do Hotspot. Ou seja sem ter de logar na rede inicialmente. Também é possível bloquear endereços

continua…

IP Bindings



→ MAC Address: mac original do cliente

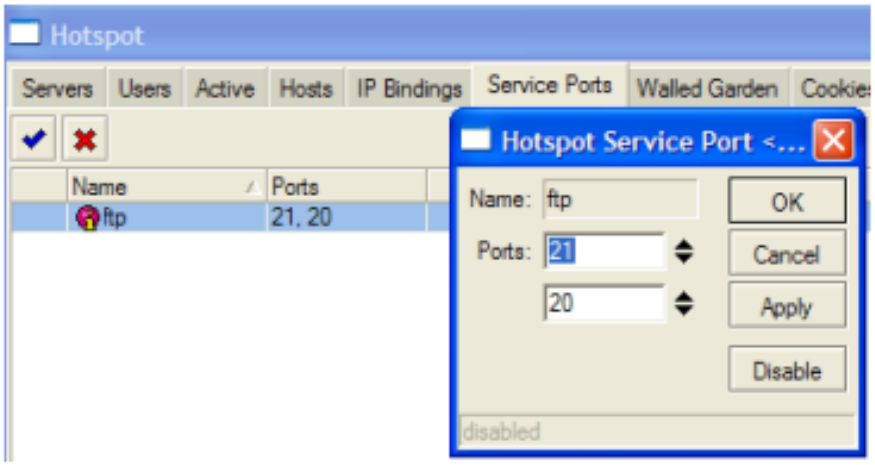
→Address: endereço IP configurado no cliente (ou rede)

→ To Address: endereço IP para o qual o original deve ser traduzido.

→Type: Tipo de Binding

- → Regular: faz uma tradução 1:1 regular
- → Bypassed: faz a tradução mas dispensa o cliente de logar no Hotspot
- → Blocked: a tradução não será feita e todos os pacotes serão descartados.

Hotspot Ports



A facilidade de NAT e NAT 1:1 do Hotspot causa problemas com alguns protocolos incompatíveis com NAT. Para que esses protocolos funcionem de forma consistente, devem ser usados os módulos “helpers”

No caso de NAT 1:1 o únco problema é com relação ao módulo de FTP que deve ser configurado para usar as portas 20 e 21.

.

Walled Garden

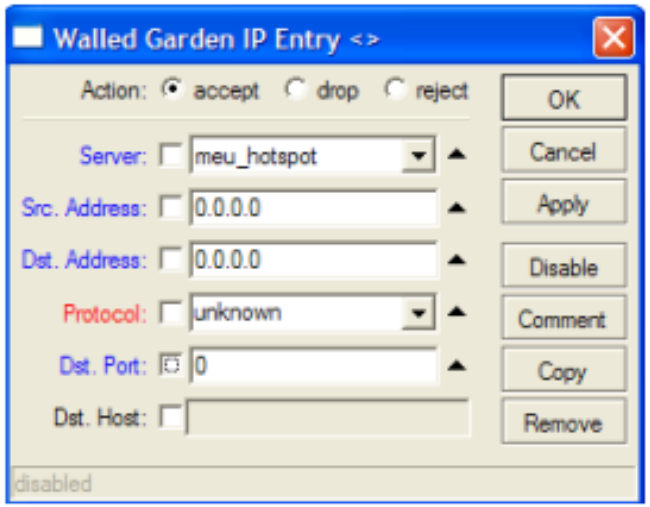
Configurando um Walled Garden ou “Jardim Murado” é possível oferecer ao usuário o acesso a determinados serviços sem necessidade de autenticação. Por exemplo em um Aeroporto poder-se-ia disponibilizar informações climáticas, horários de voos, etc sem a necessidade do usuário adquirir créditos para acesso externo.

Quando um usuário não logado no Hotspot requisita um serviço do Walled Garden o gateway não o intercepta e, no caso de http, redireciona a reuisição para o destino ou para um proxy.

Para implementar o Walled Garden para requisições http, existe um Web Proxy embarcado no Miktotik, de forma que todas as requisições de usuários não autorizados passem de fato por esse proxy.

Observar que o proxy embarcado não tem as funções de fazer cache, pelo menos por ora. Notar também que esse proxy embarcado faz parte do pacote **system** e não requer o pacote **web-proxy.**

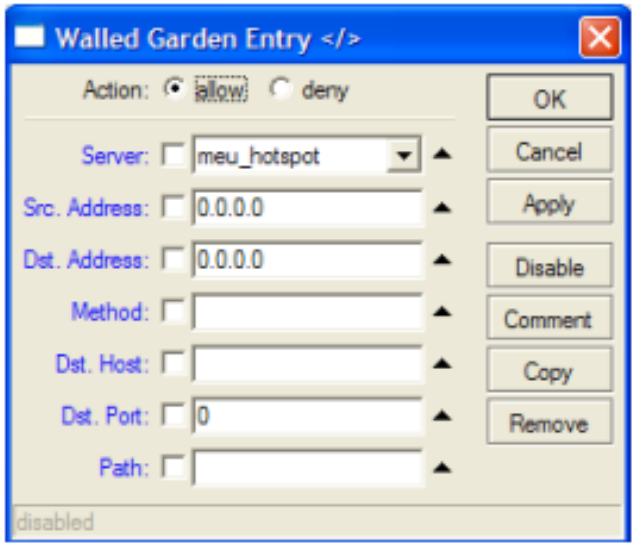
Walled Garden



É importante salientar que o Walled Garden não se destina somente a serviço WEB, mas qualquer serviço que queiramos configurar. Para tanto existem 2 menus distintos que estão acima, sendo que o da esquerda destina-se somente para HTTP e HTTPS e o da direita para outros serviços e protocolos.

No terminal o acesso ao primeiro é por /ip hotspot walled-garden e ao segundo /ip hotspot walled-garden ip

Walled Garden p/ HTTP e HTTPS



→ Action: allow ou deny – permite ou nega

→ Server: Hotspot ou Hostpots para o qual vale esse Walled Garden

→ Src Address: Endereço IP do usuário requisitante.

→ Dst Address: Endereço IP do Web Server

→ Method: método de http

→ Dst Host: nome de domínio do servidor de destino.

→ Dst Port: porta de destino que o cliente manda a solicitação.

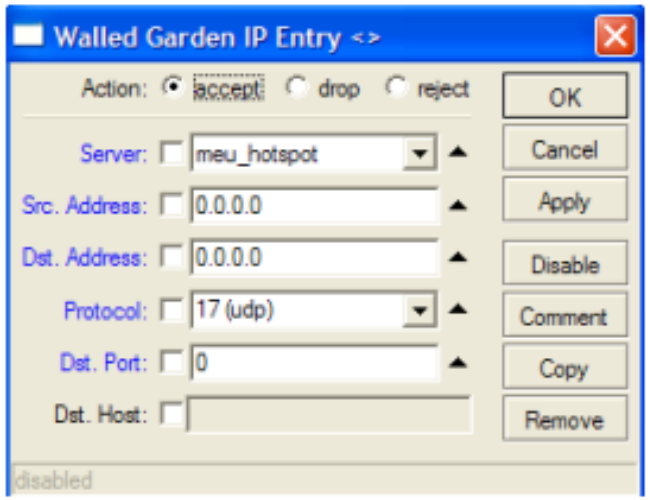
→ Path: caminho da requisição.

OBS:

- nos nomes de dominio é necessário o nome completo, podendo ser usados coringas

- aceita-se expressões regulares devendo ser iniciadas com (:)

Walled Garden p/ outros protocolos



→ Action: aceita, descarta ou rejeita o pacote

→ Server: Hotspot ou Hostpots para o qual vale esse Walled Garden

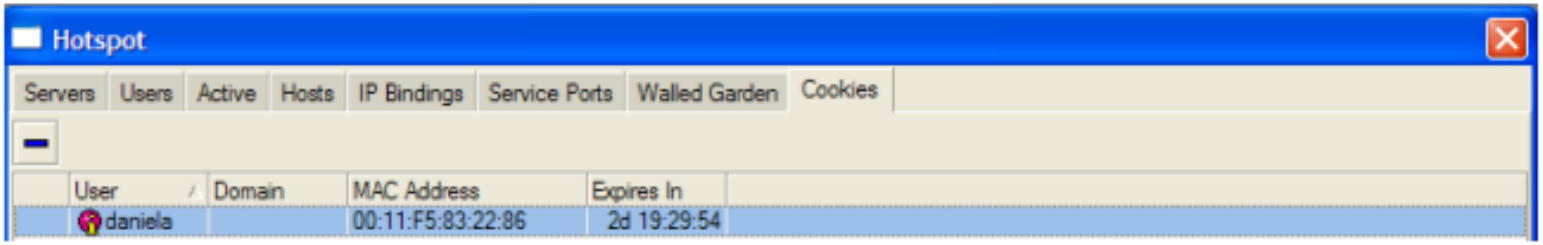
→ Src Address: Endereço IP de origem do usuário requisitante.

→ Protocol: Protocolo a ser escolhido da lista

→Dst Port: Porta TCP ou UDP que está sendo requisitadao

→ Dst Host: Nome de domínio do WEB server

Hotspot - Cookies



→Quando configurado o login por Cookies, estes ficam armazenados no Hotspot, com o nome do usuário, MAC e o tempo de validade.

→ Enquanto estiverem válidos o usuário não precisa passar o par usuário/senha

→ Podem ser deletados (-) forçando assim o usuário fazer nova autenticação

Personalizando o Hotspot

Páginas do Hotspot

As páginas do Hotspot são totalmente configuráveis e além disso é possível criar conjuntos totalmente diferentes das páginas do Hotspot para vários perfis de usários especificando diferentes diretórios html raiz) /ip hotspot profile html-directory.

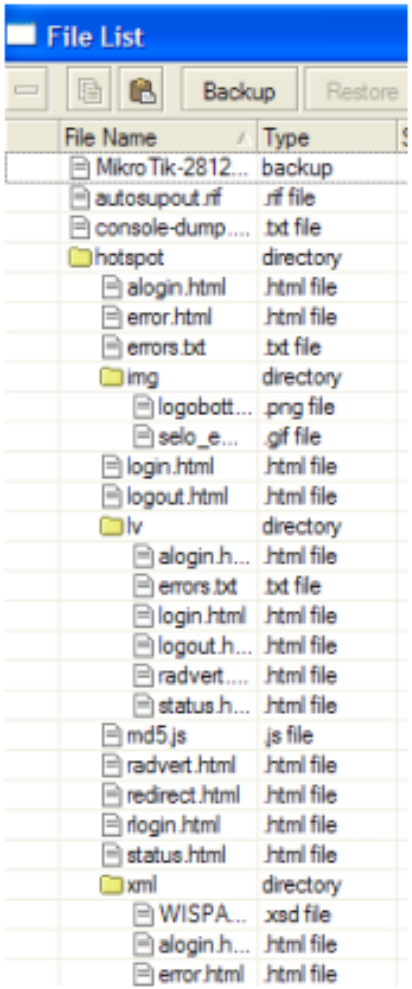
Principais páginas que são mostradas aos usuários:

→ **redirect.html** – redireciona o usuário a uma página específica

→ **login.html** – Página de login que pede ao usuário o login e senha. Esta página tem os seguintes parametros:

- **username / password**
- **dst** – URL original que o usuário solicitou antes do redirecionamento (será aberta após o login com sucesso)
- **popup** – se será aberto uma janela de pop-up quando o usuário se logar com sucesso.

Personalizando o Hotspot



Páginas do Hotspot

As páginas do Hotspot são totalmente configuráveis e podem ser editadas em qualquer editor html, sendo depois atualizadas no mikrotik.

É possível criar conjuntos totalmente diferentes de páginas do Hotspot para vários perfis de usários especificando diferentes diretórios html raiz) /ip hotspot profile html-directory.

Essa possibilidade, associada a criação de AP's virtuais possibilita que em uma mesma área pública o detentor da infraestrutura possa fornecer serviço a vários operadores, utilizando os mesmos equipamentos.

Hotspot com https

→ Criar o certificado em uma máquina Unix com o Script:

```
#!/bin/sh
SERVER=hotspot.mikrotikbrasil.com.br
PRIVATE_KEY=$SERVER.key
CERTIFICATE_FILE=$SERVER
VALID_DAYS=1095
openssl genrsa -des3 -out $PRIVATE_KEY 1024
openssl req -new -x509 -days $VALID_DAYS -key $PRIVATE_KEY -out
$CERTIFICATE_FILE
```

→Importar o Certificado em / certificate import

Dúvidas ??

User Manager

MikroTik
RouterOS User Manager

- Status
- Routers
- Credits
- Users
- Sessions
- Customers
- Reports
- Logs
- Logout

Search users

Search

Active users: 0 Show

Active sessions: 0 Show

Add users

Number of users: 1
Rate limits:
Uptime limit: 0s
Prepaid: 30segundos (1.00)
Generate CSV file
Generate vouchers
Users per page: 1
Add

User Manager

O que é o User Manager ?

É um sistema de gerenciamento de usuários que pode ser utilizado para controlar
→ Usuários de Hotspot
→Usuários PPP (PPtP e PPPoE)
→ Usuários DHCP
→ Usuários Wireless em Geral
→ Usuários do sistema RouterOS em si

User Manager

Como implementar (2.9.x)

→ Fazer o download do pacote / FTP para o Router / Reboot
→Criar o primeiro “subscriber” (somente no terminal)

[admin@MikrotikBrasil] tool user-manager customer> add login="admin" password=“1234" permissions=owner

→ Na V3 não é necessário criar – usuário padrão admin, senha em branco.
→Logar via WEB com o usuário e senhas criados acima em:

http://IP_do_Router/userman

User Manager - Conceitos

Customers, Subscribers e Users

Customers são os provedores de serviço. Eles tem acesso à interface WEB para manipular os usuários (users) créditos e roteadores.

Um ***Subscriber*** é um ***Customer*** com permissões de "dono"

Os ***Subscribers*** tem conhecimento de tudo que acontece com seus sub-customers, créditos, usuários, roteadores, sessões, etc. No entanto um subscriber não tem acesso aos dados de outros subscribers.

Users são os pobres mortais que usam os serviços oferecidos pelos Customers

User Manager – Algumas características

→Cada Subscriber pode criar vários Customers, personalizando telas de login para os usuários, permissões que os Customers tem, Modelos de "Voucher", etc

→Voucher é o cartão de login/senha que pode ser gerado em lote para o atendimento de um Hotel, por exemplo

→É possível implementar esquemas de criação de login pelo usuário com pagamento por cartão de crédito via PayPal ou Autorize.net

→É possível configurar na mesma máquina o User Manager e o Hotspot, possibilitando uma solução única para prestar serviço em Hotel com uma máquina rodando Mikrotik apenas.

Exemplo de implementação de User Manager com Hotspot

No Router:

/ ip hotspot profile set hsprof1 use-radius=yes

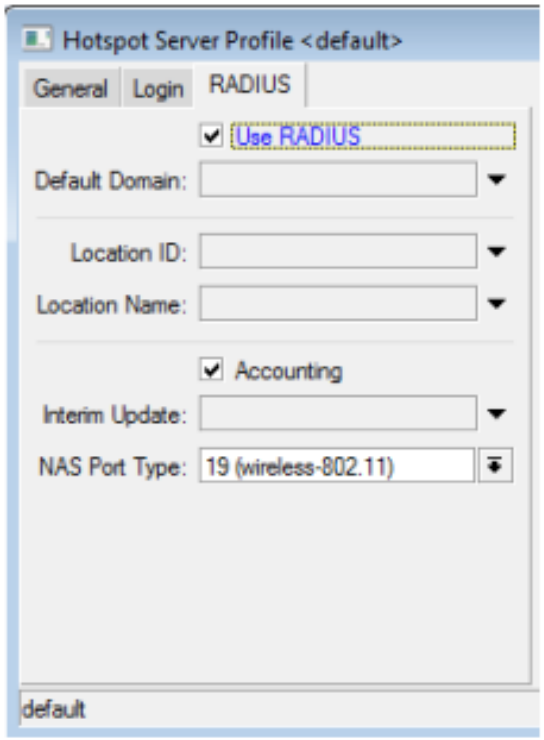
/ radius add service=hotspot address=x.x.x.x secret=123456

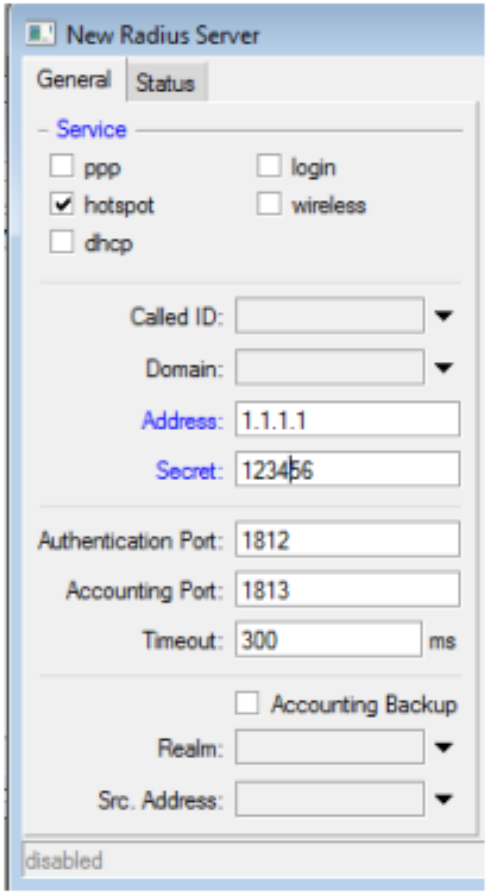
No User Manager:

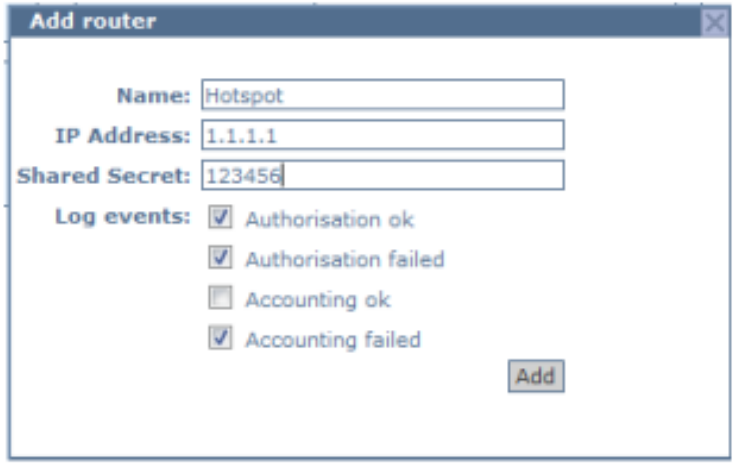
/ tool user-manager router add subscriber=MikrotikBrasil ip-address=10.5.50.1 shared-secret=123456

No caso, para usar somente uma máquina, basta apontar o mesmo IP x.x.x.x que ela será o Hotspot e ao mesmo tempo o User Manager

Exemplo de implementação de User Manager com Hotspot







Dúvidas ??

Roteamento

Mikrotik RouterOS suporta dois tipos de roteamento:

→ Roteamento Estático: As rotas criadas pelo usuário através de inserção de rotas pré definidas em função da topologia da rede

→ Roteamento Dinâmico: As rotas são geradas automáticamente através de algum agregado de endereçamento IP ou por protocolos de roteamento

O Mikrotik suporta ECMP - Equal Cost Multipath Routing (Roteamento por multicaminhos com mesmo Custo), que é um mecanismo que permite rotear pacotes através de vários links e permite balanceamento de carga.

É possível ainda no Mikrotik se estabelecer Políticas de Roteamento (Policy Routing) dando tratamento diferenciado a vários tipos de fluxo a critério do adminstrador.

Políticas de Roteamento

Existem algumas regras que devem ser seguidas para se estabelecer uma política de roteamento:

→ As políticas podem ser por marca de pacotes, por classes de endereços Ip e portas.

→ A marca dos pacotes deve ser adicionada no Firewall, no módulo Mangle com **routing-mark**

→ Aos pacotes marcados será aplicada uma política de roteamento, dirigindo-os para um determinado gateway.

→ É possivel utilizar política de roteamento quando se utiliza mascaramento (NAT)

Políticas de Roteamento

Observações Importantes:

Uma aplicação típica de Políticas de Roteamento é trabalhar com dois links direcionando parte do tráfego por um e parte por outro. Por exemplo a canalização de aplicações peer-to-peer por um link “menos nobre”

É impossível porém reconhecer o tráfego peer-to-peer do a partir do primeiro pacote, mas tão somente após as conexões estabelecidas, o que impede o funcionamento dos programas P2P em caso de NAT de origem.

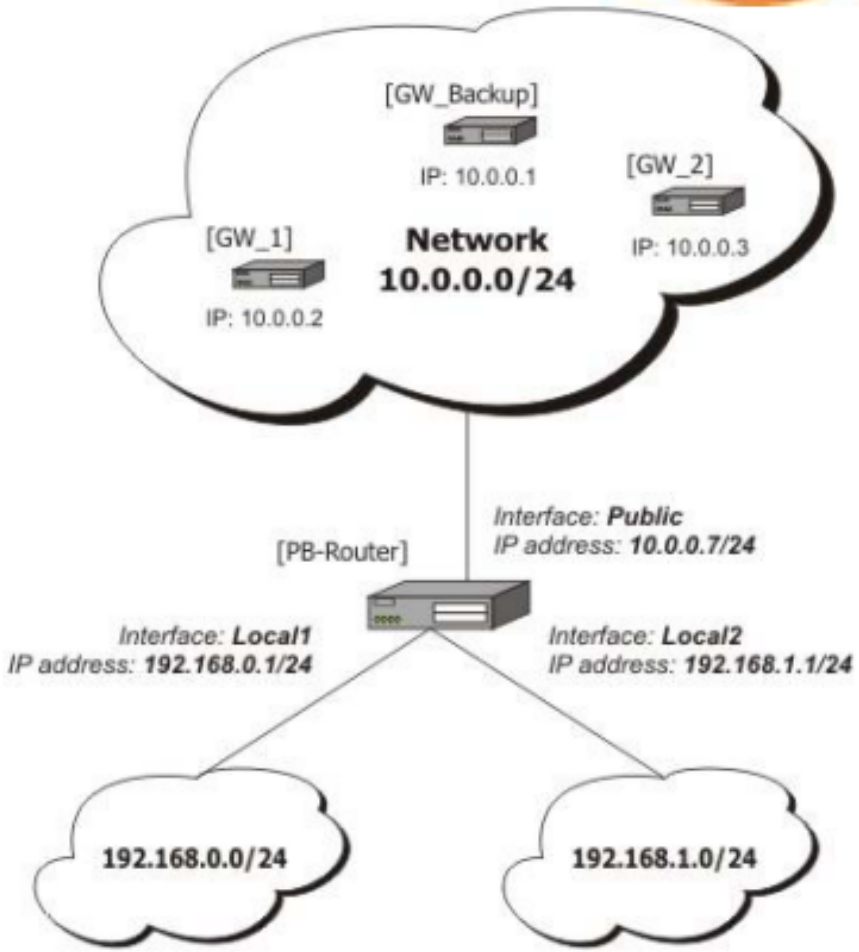
A estratégia nesse caso é colocar como gateway default o link “menos nobre”, marcar o tráfego conhecido e “nobre” (HTTP, DNS, POP3, SMTP, etc) e desvia-lo para o link “nobre”. Todas as outras aplicações, incluido o P2P, irão para o link “não nobre”.

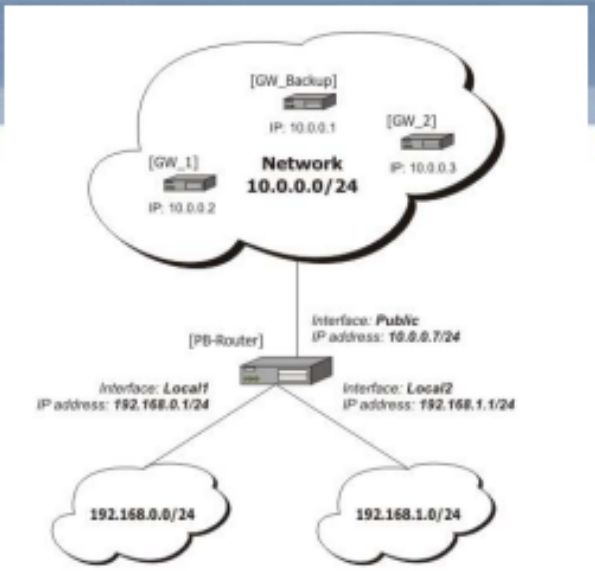
Exemplo de Política de Roteamento

Na situação normal queremos que a rede:

→ **192.168.0.0/24**, use o gateway GW_1,
→ **192.168.1.0/24**, use o gateway GW_2

No caso de falha aos pings do GW_1 ou do GW_2, queremos automáticamente rotear para o GW_Backup.





Exemplo de Política de Roteamento

1. Marcar pacotes da rede 192.168.0.0/24 com **new-routing-mark=net1**, e pacotes da rede 192.168.1.0/24 com **new-routing-mark=net2**:

ip firewall mangle> add src-address=192.168.0.0/24 action=mark-routing new-routing-mark=net1 chain=prerouting

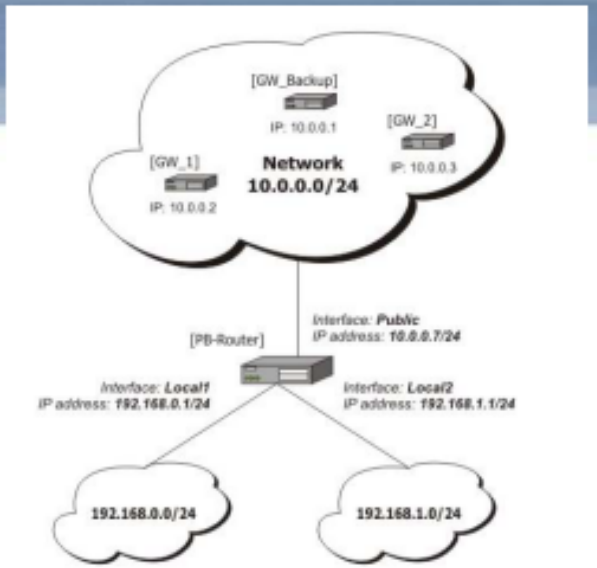
ip firewall mangle> add src-address=192.168.1.0/24 action=mark-routing new-routing-mark=net2 chain=prerouting

2. Rotear os pacotes da rede 192.168.0.0/24 para o gateway GW_1 (10.0.0.2), pacotes da rede 192.168.1.0/24 para o gateway GW_2 (10.0.0.3), usando as correspondentes marcas de pacotes. Se GW_1 ou GW_2 falharem (não responder a pings), rotear para GW_Backup (10.0.0.1):

ip route> add gateway=10.0.0.2 routing-mark=net1 check-gateway=ping

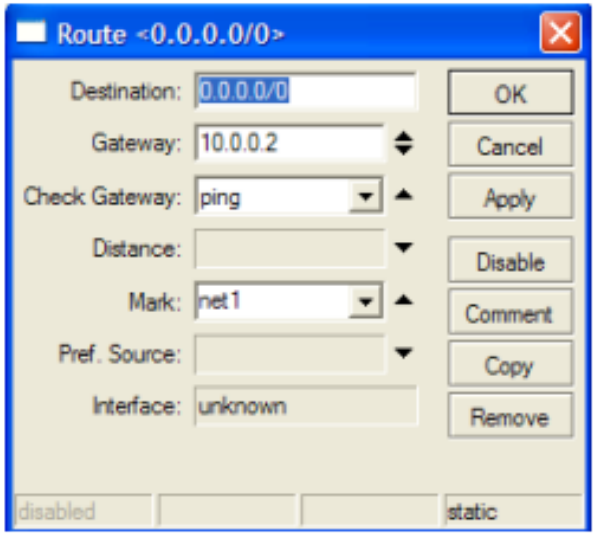
ip route> add gateway=10.0.0.3 routing-mark=net2 check-gateway=ping

ip route> add gateway=10.0.0.1



Exemplo de Política de Roteamento

Com Winbox:



Balanceamento de Carga com PCC

O recurso PCC (per connection classifier) está disponível a partir da V3.24

Balanceamento de Carga com PCC

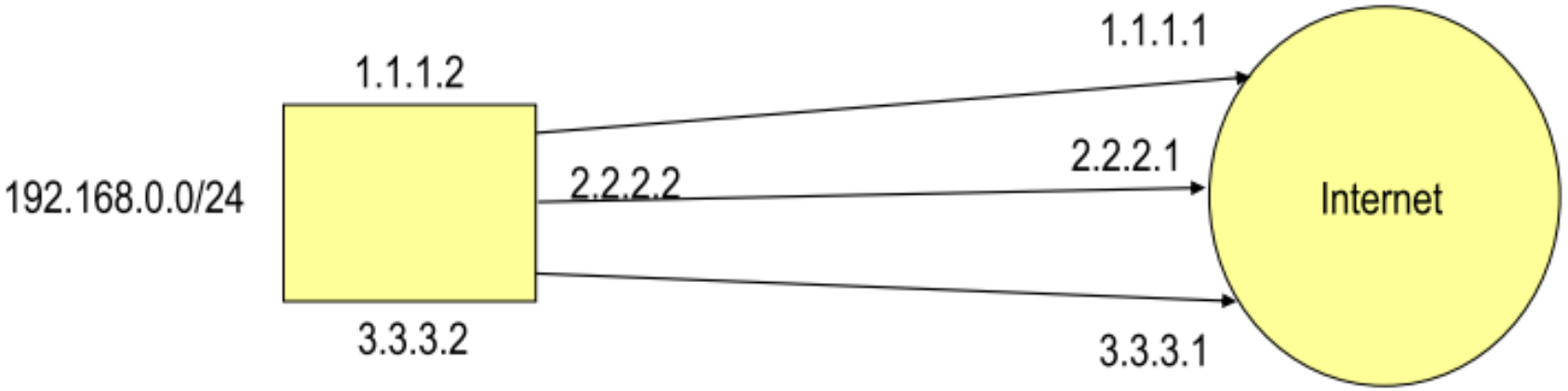
O recurso PCC (per connection classifier) está disponível a partir da V3.24

Balanceamento de Carga com PCC

O recurso PCC (per connection classifier) está disponível a partir da V3.24

Balanceamento de Carga com PCC

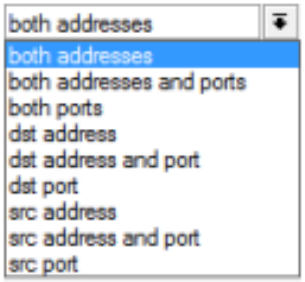
Exemplo para 3 Links



Balanceamento com PCC

PCC = Per connection Classifier (Classificador por conexão). Com o PCC é possível dividir o tráfego em fluxos distintos, em função de um critério de classificação. Os parametros de configuração são:

→ Classificador::

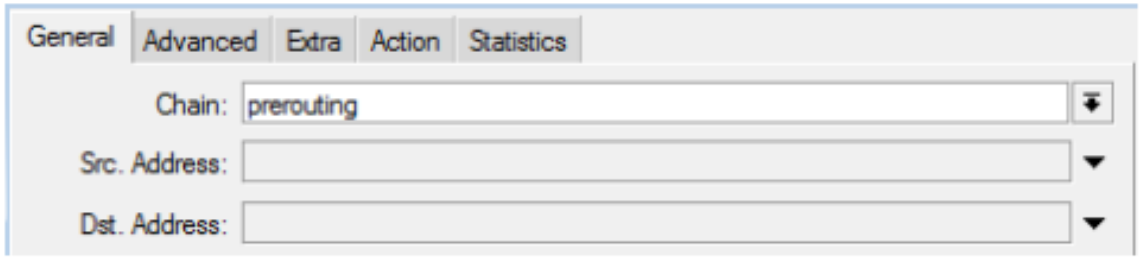


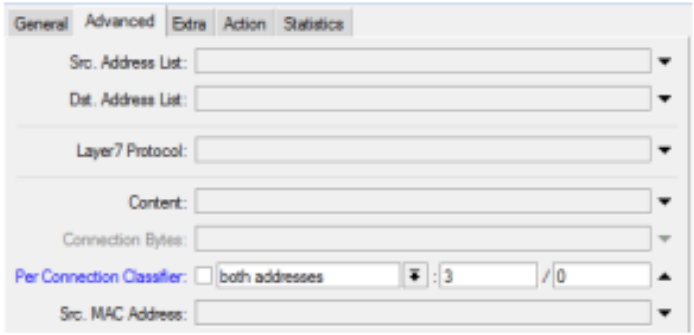
→ Denominador: Número de canais por onde serão divididos os fluxos

→ Contador. Determina o número do canal que será utilizado.

Balanceamento com PCC

Exemplo para balanceamento de 3 links





Balanceamento com PCC

Exemplo para balanceamento de 3 links

General | Advanced | Extra | Action | Statistics

Chain: prerouting

Src. Address:

Dst. Address:

General | Advanced | Extra | Action | Statistics

Src. Address List:

Dst. Address List:

Layer7 Protocol:

Content:

Connection Bytes:

Per Connection Classifier: both addresses : 3 / 1

Src. MAC Address:

General | Advanced | Extra | Action | Statistics

Action: mark connection

New Connection Mark: Link2_con

Passthrough

Balanceamento com PCC

Exemplo para balanceamento de 3 links

General | Advanced | Extra | Action | Statistics

Chain: prerouting

Src. Address:

Dst. Address:

General | Advanced | Extra | Action | Statistics

Src. Address List:

Dst. Address List:

Layer7 Protocol:

Content:

Connection Bytes:

Per Connection Classifier: both addresses : 3 / 2

Src. MAC Address:

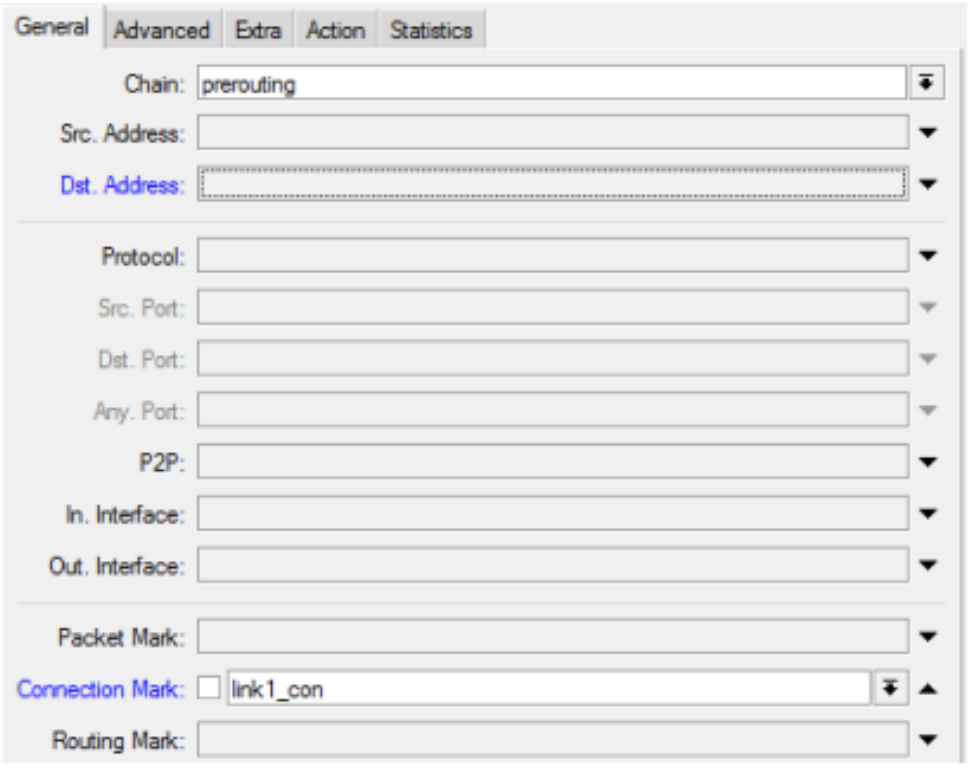
General | Advanced | Extra | Action | Statistics

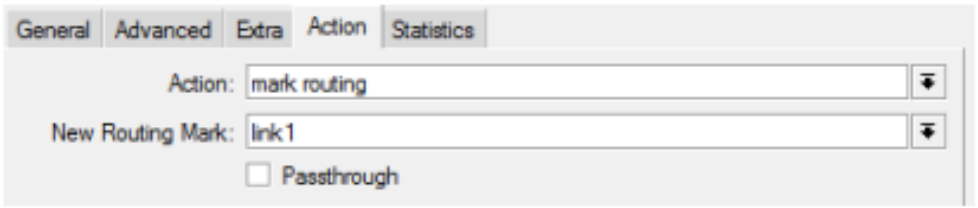
Action: mark connection

New Connection Mark: Link3_con

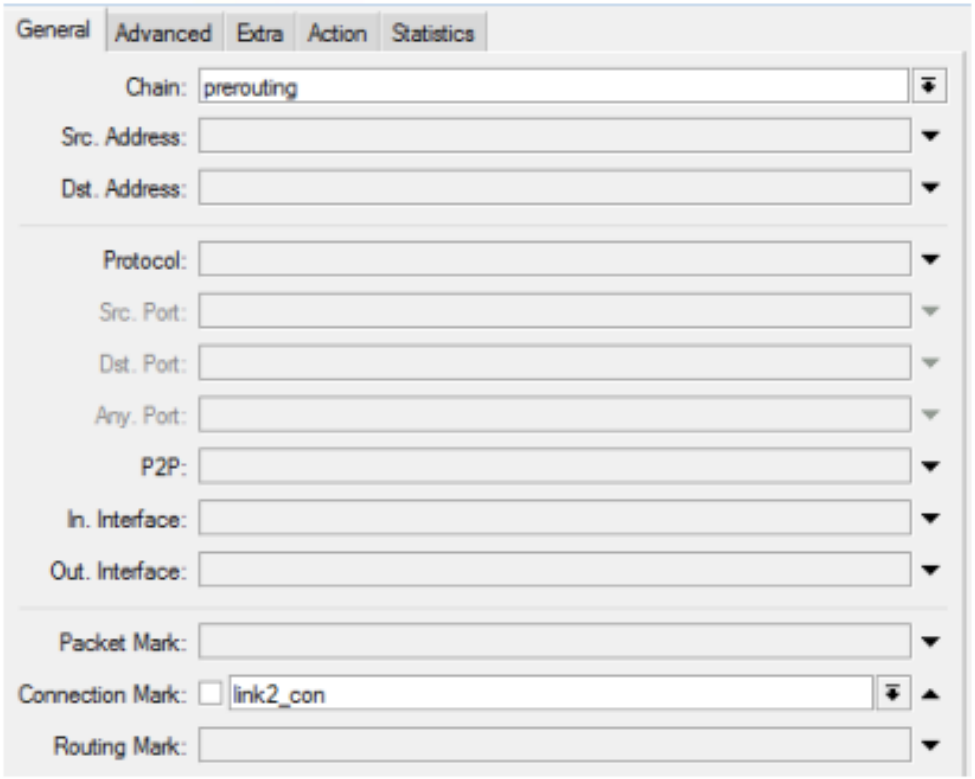
Passthrough

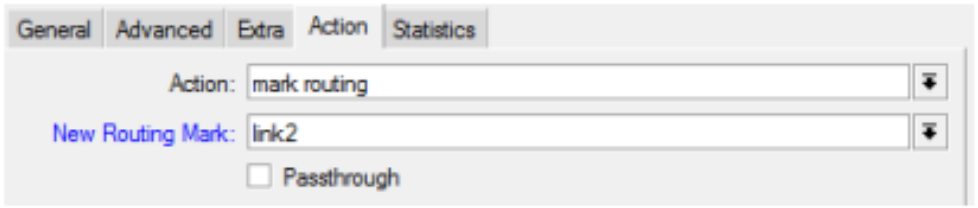
Marcação de rotas



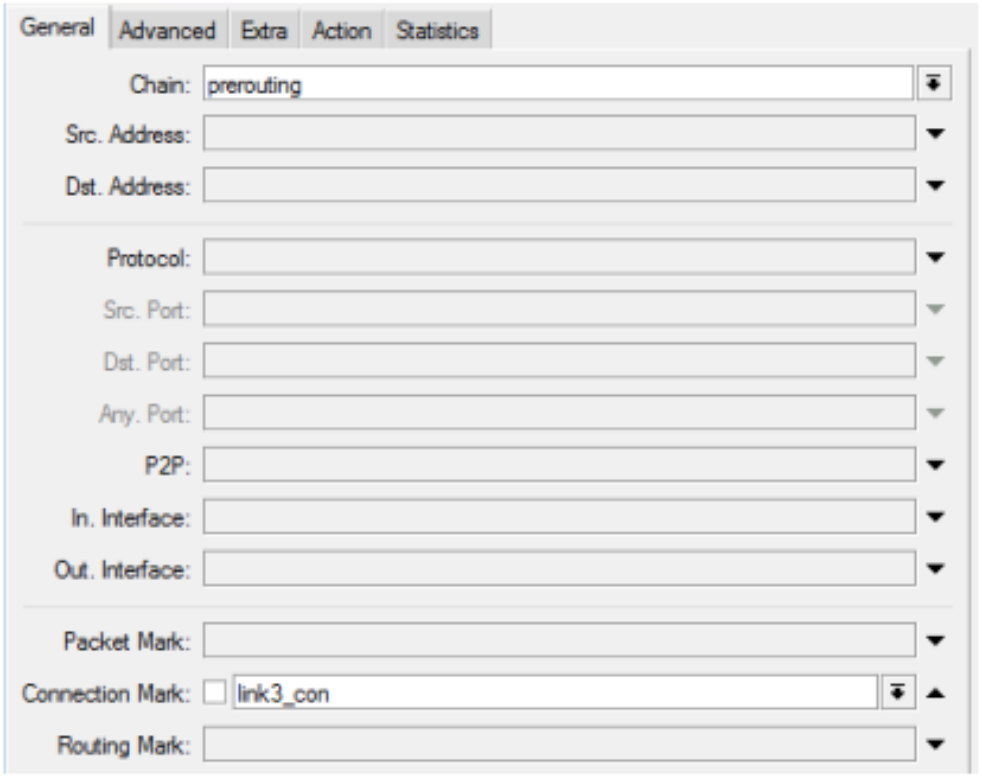


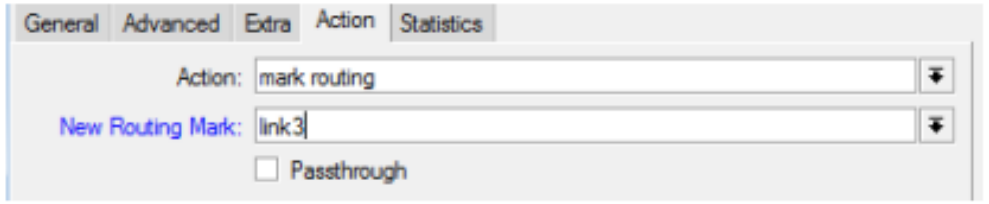
Marcação de rotas





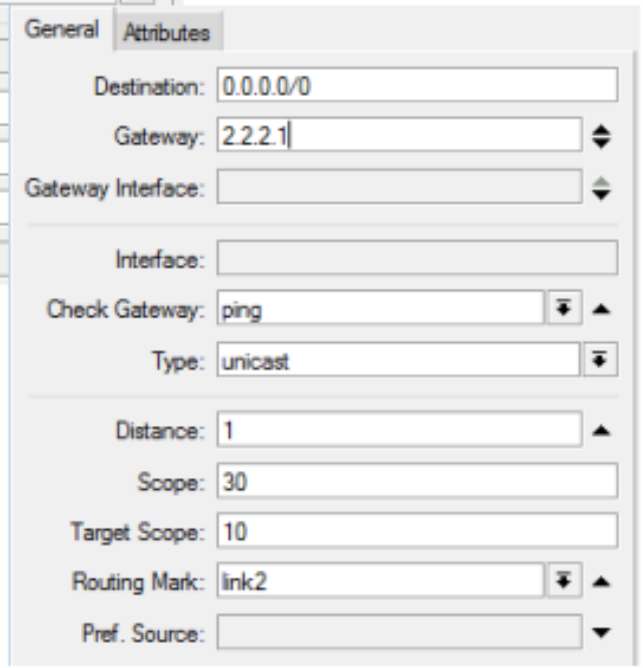
Marcação de rotas

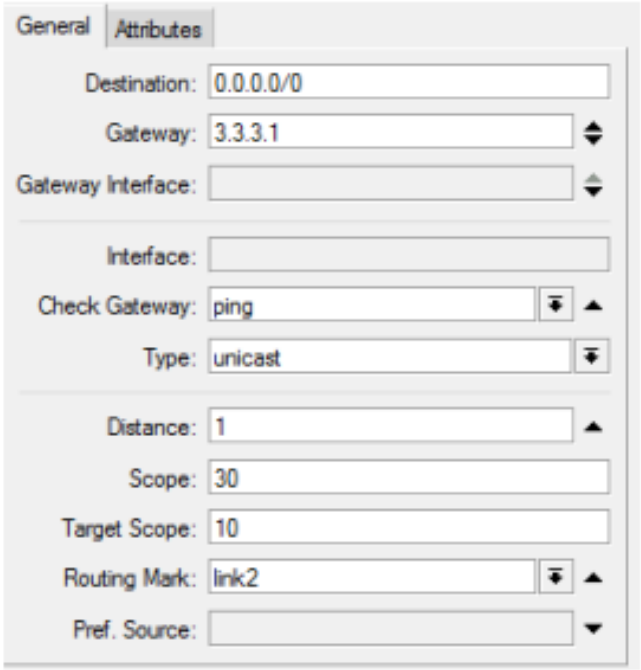




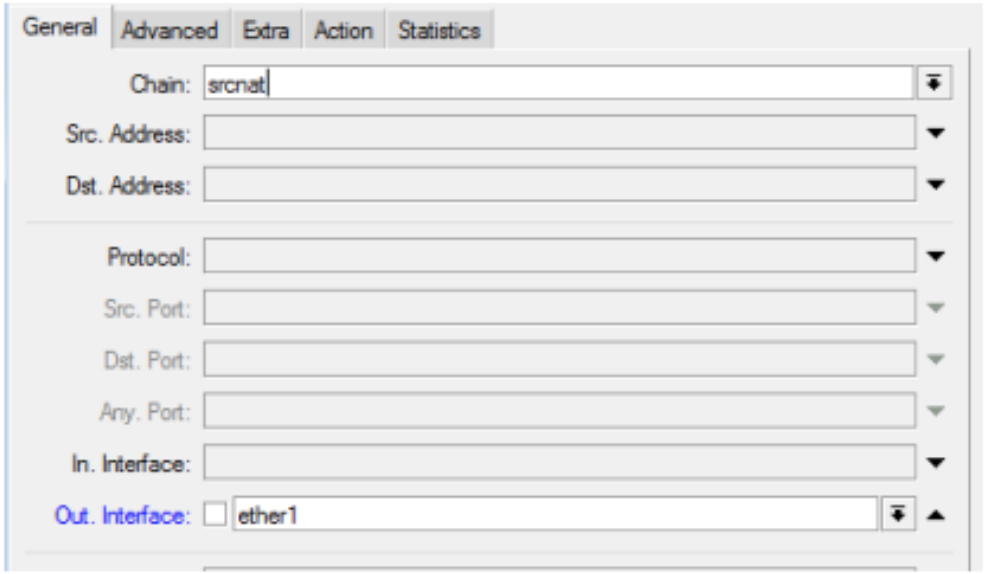
Rotas

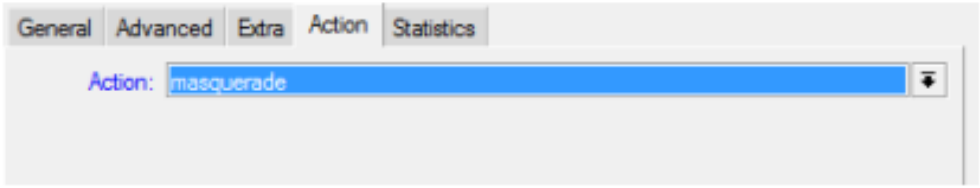

General
Attributes
Destination: 0.0.0.0/0
Gateway: 1.1.1.1
Gateway Interface:
Interface:
Check Gateway: ping
Type: unicast
Distance:
Scope: 30
Target Scope: 10
Routing Mark: link1
Pref. Source:


General
Attributes
Destination: 0.0.0.0/0
Gateway: 2.2.2.1
Gateway Interface:
Interface:
Check Gateway: ping
Type: unicast
Distance: 1
Scope: 30
Target Scope: 10
Routing Mark: link2
Pref. Source:

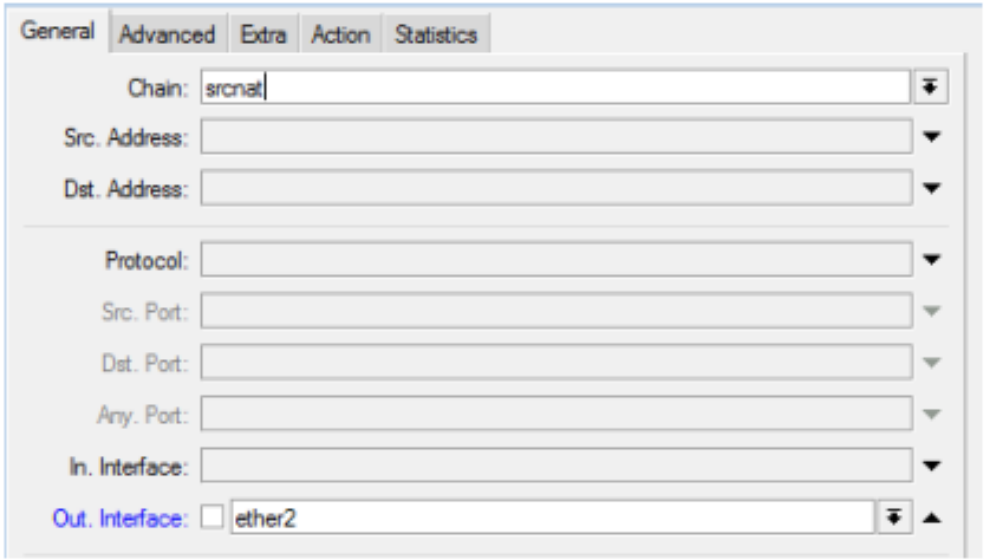

General
Attributes
Destination: 0.0.0.0/0
Gateway: 3.3.3.1
Gateway Interface:
Interface:
Check Gateway: ping
Type: unicast
Distance: 1
Scope: 30
Target Scope: 10
Routing Mark: link2
Pref. Source:

Nat


General
Advanced
Extra
Action
Statistics
Chain:
srcnat
Src. Address:
Dst. Address:
Protocol:
Src. Port:
Dst. Port:
Any. Port:
In. Interface:
Out. Interface:
ether1

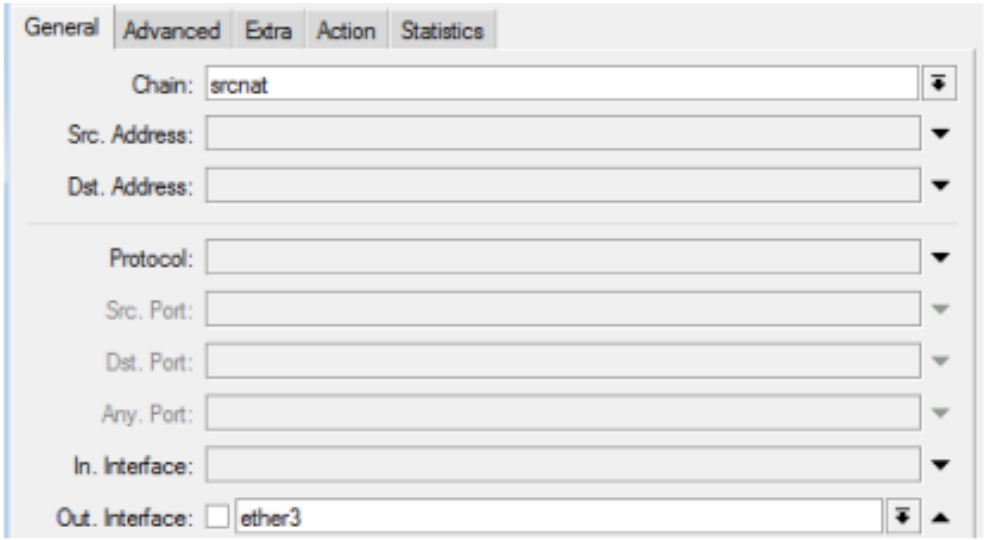

General
Advanced
Extra
Action
Statistics
Action:
masquerade

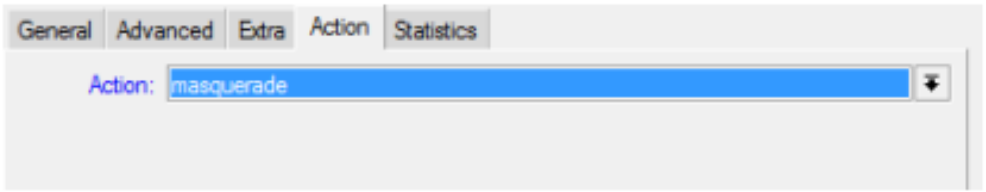
Nat


General
Advanced
Extra
Action
Statistics
Chain:
srcnat
Src. Address:
Dst. Address:
Protocol:
Src. Port:
Dst. Port:
Any. Port:
In. Interface:
Out. Interface:
ether2


General
Advanced
Extra
Action
Statistics
Action:
masquerade

Nat


General
Advanced
Extra
Action
Statistics
Chain: srcnat
Src. Address:
Dst. Address:
Protocol:
Src. Port:
Dst. Port:
Any. Port:
In. Interface:
Out. Interface: ether3


General
Advanced
Extra
Action
Statistics
Action: masquerade

Roteamento Dinâmico

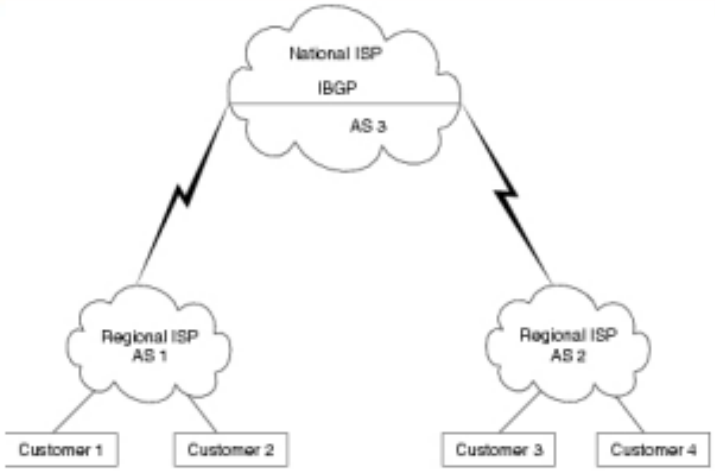
O Mikrotik RouterOS suporta os seguintes protocolos de roteamento:

→ RIP versão 1 e RIP versão 2
→ OSPF versão 2
→ BGP versão 4

- Versões em desenvolvimento do Mikrotik dão suporte a versões mais recentes desses protocolos, mas ainda em fase beta.

- O uso de roteamento dinamico permite implementar redundância e balanceamento de carga de forma automática e é uma forma de se fazer uma rede semelhante às redes conhecidas como Mesh, porém de forma estática.

Roteamento BGP



O protocolo BGP (Border Gateway Protocol) é destinado a fazer comunicação entre Autonomous Systems diferentes, podendo ser considerado como o coração da Internet.

O BGP mantém uma tabela de “prefixos” de rotas contendo as informações de “encontrabilidade” de redes (NLRI – Network Layer Reachbility Information) entre os AS’s.

A versão corrente do BGP é a versão 4, especificada na RFC 1771.

OSPF

O protocolo **Open Shortest Path First** (Abra primeiro o caminho mais curto) é um protocolo do tipo "link-state". Ele usa o algorítimo de Dijkstra para calcular o caminho mais curto para todos os destinos.

O OSPF distribui informações de roteamento entre os roteadores que participem de um mesmo AS (Autonomous System) e que tenham obviamente o protocolo OSPF habillitado.

Para que isso aconteça todos os roteadores tem de ser configurados de uma maneira coordenada e devem ter o mesmo MTU para todas as redes anunciadas pelo protocolo OSPF.

O protocolo OSPF é iniciado depois que é adicionado um registro na lista de redes. As rotas são "aprendidas" e instaladas nas tabelas de roteamento dos roteadores.

artigo da Cisco sobre OSPF: http://www.cisco.com/warp/public/104/1.html#t3

Tipos de roteadores em OSPF

O OSPF define 3 tipos de roteadores:

→ Roteadores internos a uma área

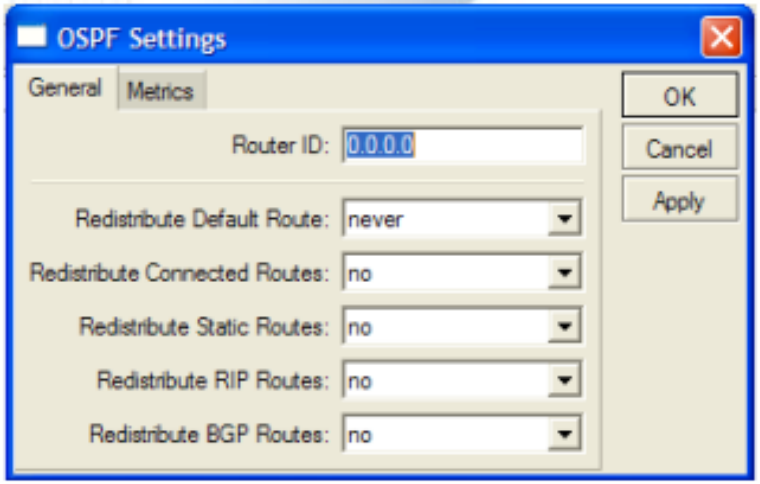
→ Roteadores de backbone (dentro da área 0)

→ Roteadores de borda de área (ABR)

→Roteadores ABR ficam entre 2 áreas e deve "tocar" a área 0

→ Roteadores de borda com Autonomous System (ASBR)

→ São os roteadores que participam do OSPF mas fazem a comunicação com um AS



OSPF Settings

Router ID: IP do roteador. Caso não especificado o roteador utiliza o maior endereço IP que exista na interface.

Redistribute Default Route: Especifica como deve ser distribuida a rota default

→ never: nunca distribui

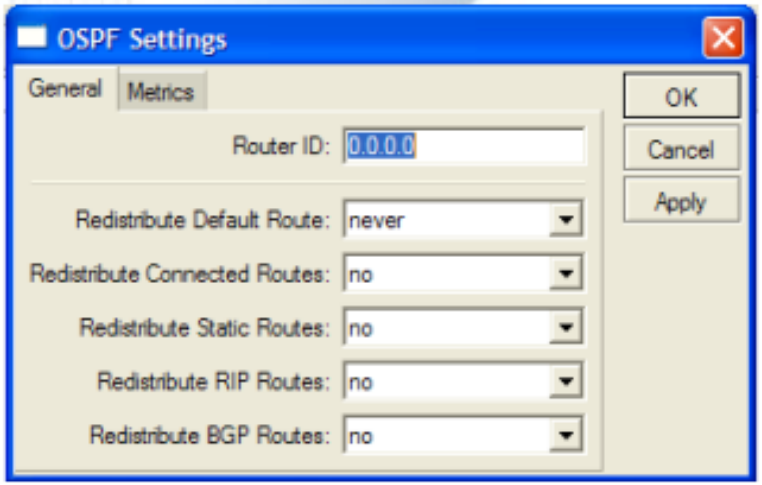
→ if installed (as type 1): envia (com métrica 1) se tiver sido instalada como rota estática ou adicionada por DHCP ou PPP

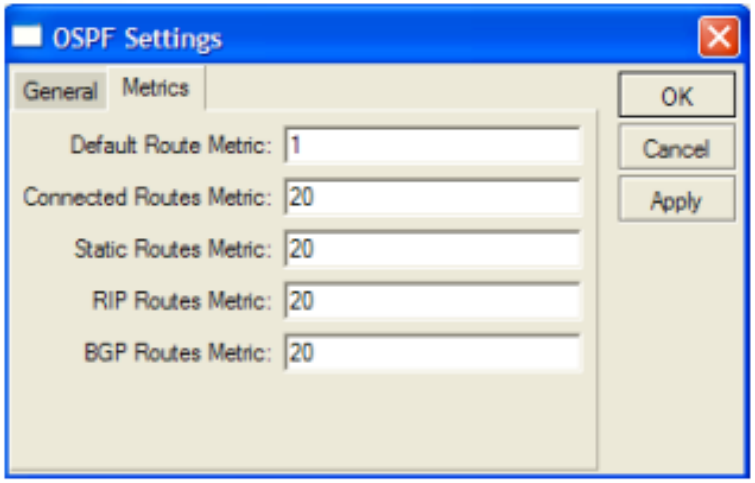
→ if installed (as type 2): envia (com métrica 2) se tiver sido instalada como rota estática ou adicionada por DHCP ou PPP

→ always (as type 1): sempre, com métrica 1

→ always (as type 2): sempre, com métrica 2

OSPF Settings





Redistribute Connected Routes: Caso habilitado, o roteador irá redistribuir todas as rotas relativas a redes que estejam diretamente conectadas a ele (sejam alcançáveis)

Redistribute Static Routes: Caso habilitado, distribui as rotas estáticas cadastradas em /ip route

Redistribute RIP: Caso habilitado, redistribui as rotas “aprendidas’ por RIP

Redistribute BGP: Caso habilitado, redistribui as rotas “aprendidas’ por BGP

Na aba Metrics, é possivel mudar o custo que serão exportadas as diversas rotas

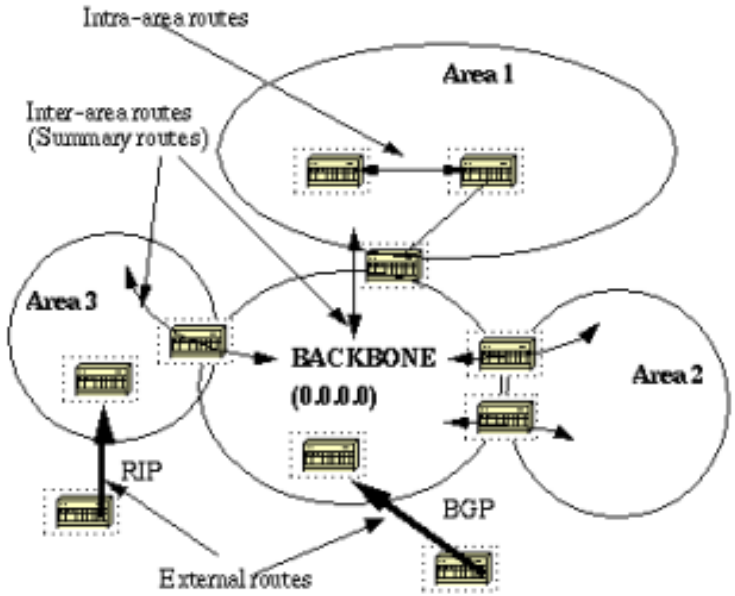
Áreas de OSPF

O protocolo OSPF permite que vários roteadores sejam agrupados entre si. Cada grupo formado é chamado de área e cada área roda uma cópia do algorítimo básico, e que cada área tem sua própria base de dados do estado de seus roteadores.

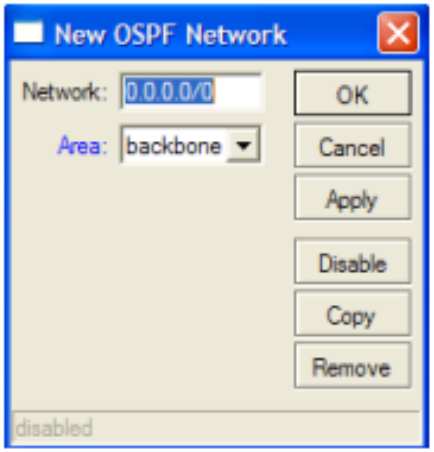
A divisão em áreas é importante pois como a estrutura de uma área só é visível para os participantes desta, o tráfego é sensivelmente reduzido.

É aconselhável utilizar no máximo 60 a 80 roteadores em cada área..

Acessa-se as opções de área em / routing ospf area



Rede OSPF

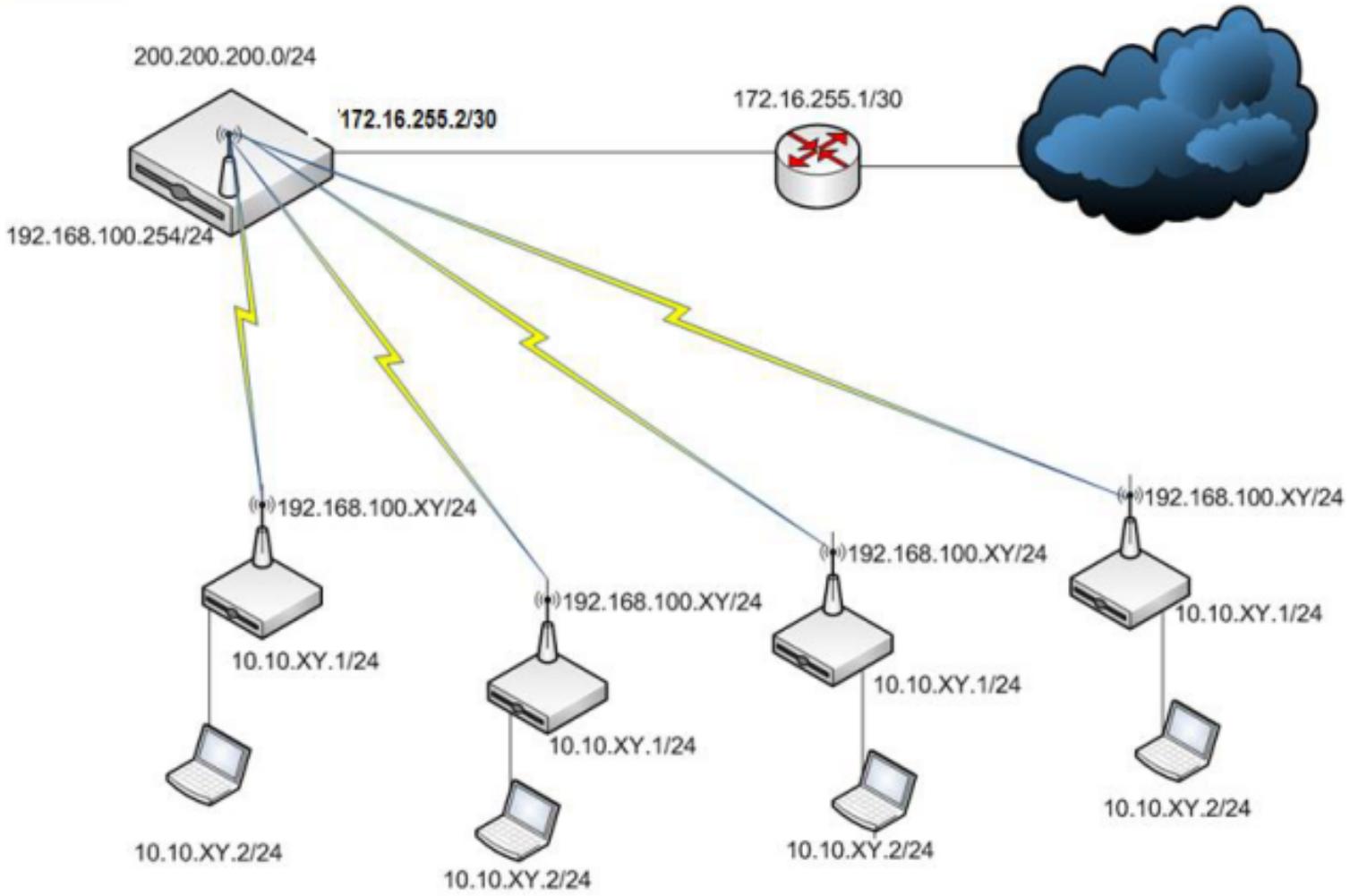


Define-se aqui a Rede OSPF, com os seguintes parametros:

- Área: Área do OSPF associada

- Network: Endereço IP/Máscara, associado. Permite definir uma ou mais interfaces associadas a uma área. Somente redes conectadas diretamente podem ser adicionadas aqui.

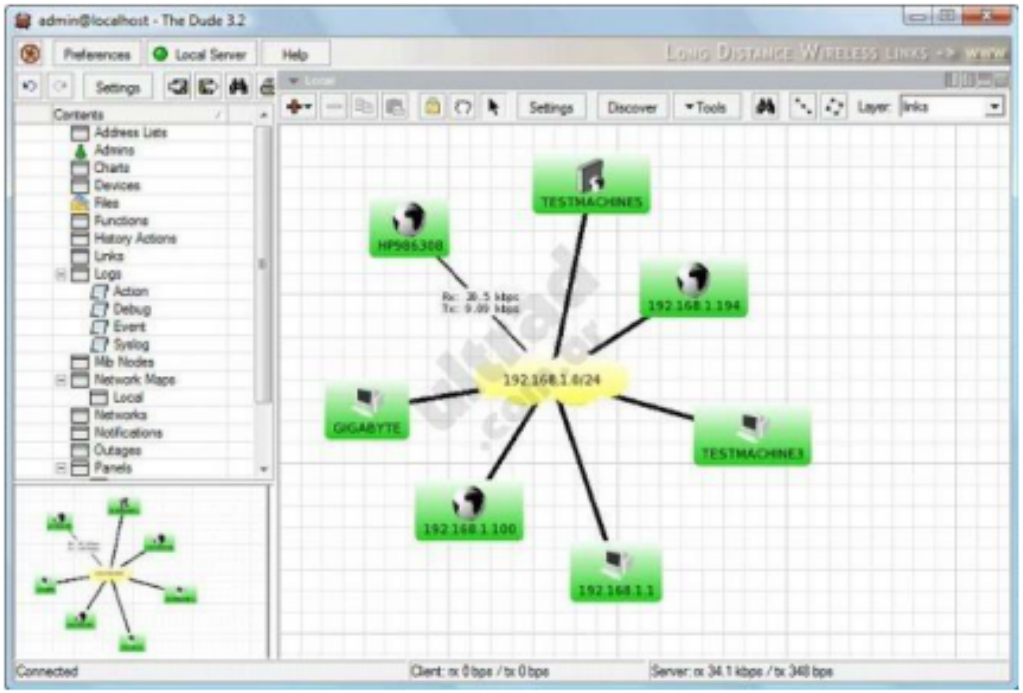
OSPF


200.200.200.0/24
172.16.255.2/30
172.16.255.1/30
192.168.100.254/24
192.168.100.XY/24
192.168.100.XY/24
192.168.100.XY/24
192.168.100.XY/24
10.10.XY.1/24
10.10.XY.1/24
10.10.XY.1/24
10.10.XY.1/24
10.10.XY.2/24
10.10.XY.2/24
10.10.XY.2/24
10.10.XY.2/24

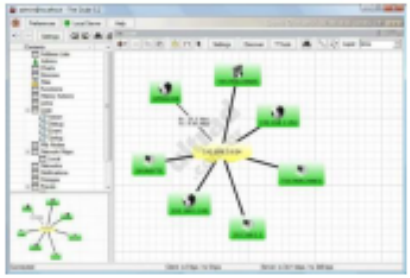
Dúvidas ??

The Dude

“O Cara”



O que é o DUDE



Como ferramenta de Monitoramento:

→ Fornece informações acerca de quedas e restabelecimentos de redes, serviços, assim como uso de recursos de equipamentos.

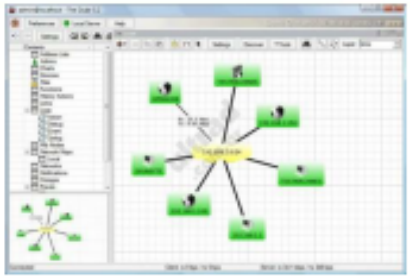
→ Permite o mapeamento da rede com gráficos da topologia da rede e relacionamentos lógicos entre os dispositivos

→ Notificações via audio/vídeo/email acerca de eventos

→ Gráfico de serviços mostrando, latencia, tempos de resposta de DNS, utilização de banda, informações físicas de links, etc.

→ Monitoramento de dispositivos não RouterOS com SNMP..

O que é o DUDE



Como ferramenta de Gerenciamento:

→ Possibilidade de utilizar ferramentas para acesso direto a dispositivos da rede a partir do diagrama da mesma.

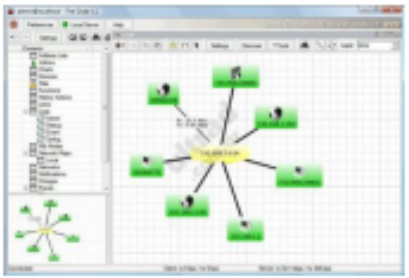
→ Acesso direto a dispositivos Mikrotik RouterOS através do Winbox

→ Armazenamento de histórico de eventos (logs) de toda a rede, com momentos de queda, restabelecimentos, etc.

→ Possibilidade de utilizar SNMP também para a tomada a tomada de decisões (SNMP set)

(V. MUM Czech Republic 2009 – Andrea Coppini)

Instalando o DUDE



Instalando no WIndows:

→ Fazer o download, clicar no executável e responder sim para todas perguntas ☺

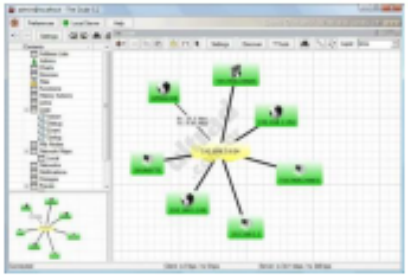
Instalando no Linux:

→ Instalar o Wine e a partir dai proceder como no Windows.

Instalando em uma Routerboard ou PC com Mikrotik

→ Baixar o pacote referente a arquitetura específica, enviar para o equipamento via ftp ou Winbox e bootar o mesmo

Instalação em Routerboards



O espaço em disco consumido pelo DUDE é considerável devido, entre outras coisas, aos gráficos e logs a serem armazenados. Assim, no caso de instalação em Routerboards é aconselhavel o uso daquelas que possuam possibilidade de armazenamento adicional, como

→ RB 433UAH – aceita HD externo via USB

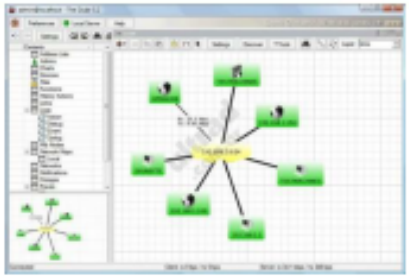
→ RB 450G – aceita micro SD

→ RB 600A – aceita micro SD

→ RB 1000 – aceita flash card

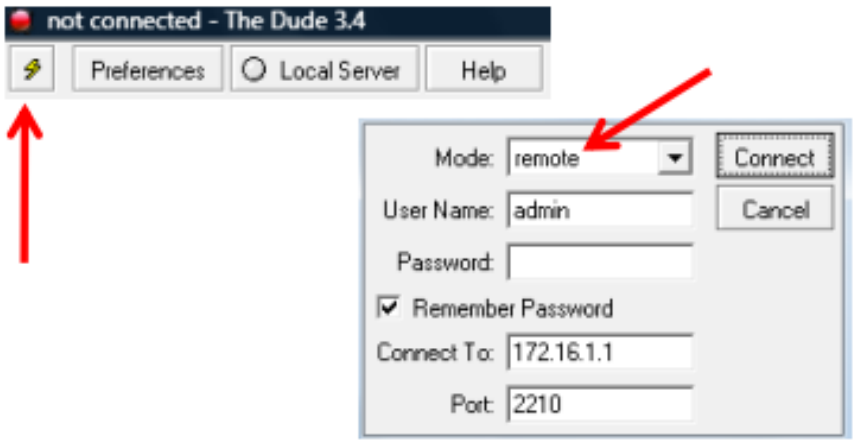
OBS: É possivel instalar em equipamentos sem as capacidades acima, porém poderão ocorrer problemas de perda de dados e impossibilidade e efetuar backup.

Começando usar o DUDE

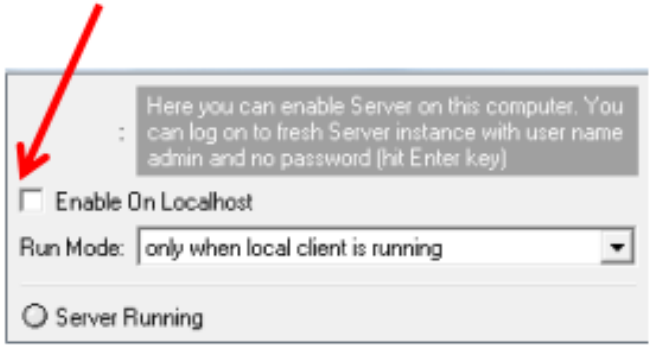


A instalação do DUDE em Windows ou Linux sempre instala o Cliente e o Servidor e no primeiro uso ele sempre irá tentar usar o Servidor Local (localhost).

Caso queira se conectar em outro DUDE (por exemplo instalado em outra Routerboard) clique em



Para desabilitar o Servidor Local:

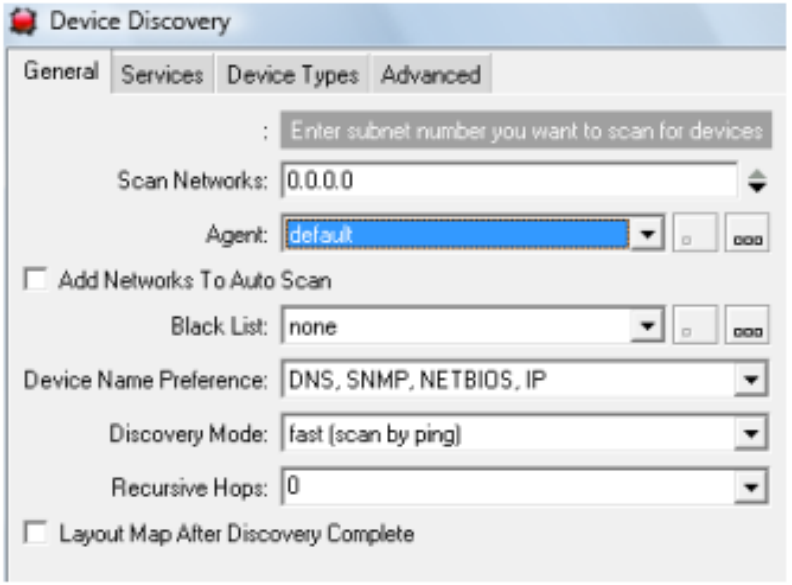


Começando usar o DUDE

Auto Discovery

O auto discovery permite que o Servidor DUDE localize os dispositivos de seu segmento de rede, através de provas de ping, arp, snmp, etc e por serviços.

Outros segmentos de redes que tenham Mikrotiks podem tambem ser mapeados por seus vizinhos (neighbours)

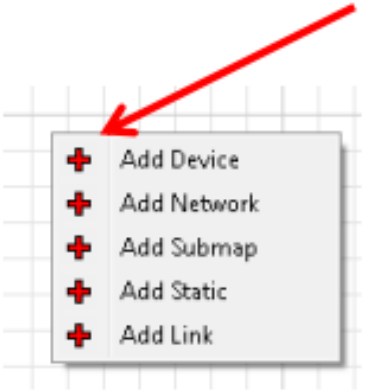


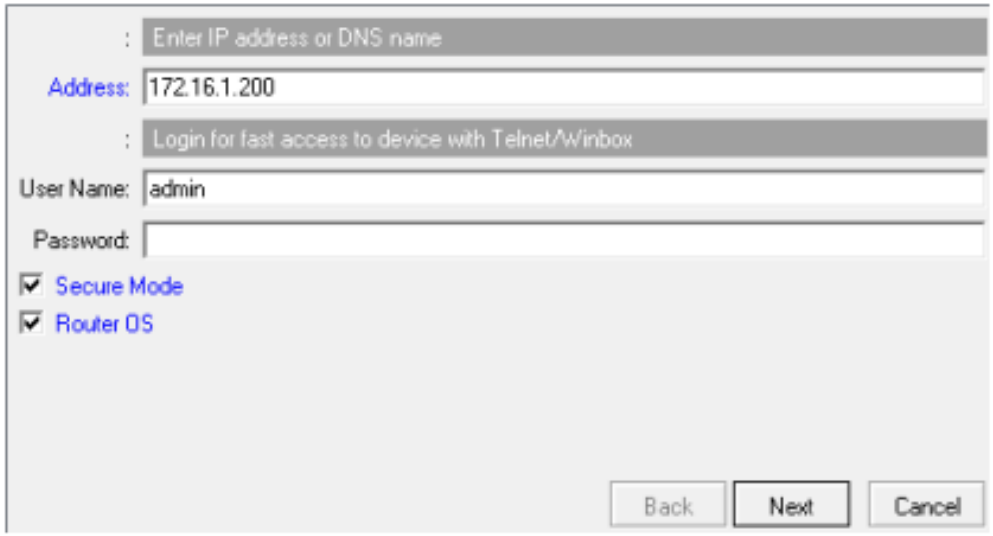
Conselho amigo: Se vai usar o DUDE para fazer um bom controle de sua rede esqueça o auto discovery !

Começando o desenho da Rede

Adicionando dispositivos

O Mikrotik tem um Wizard para a criação de dispositivos. Informe o IP e, se for Mikrotik clique em RouterOS

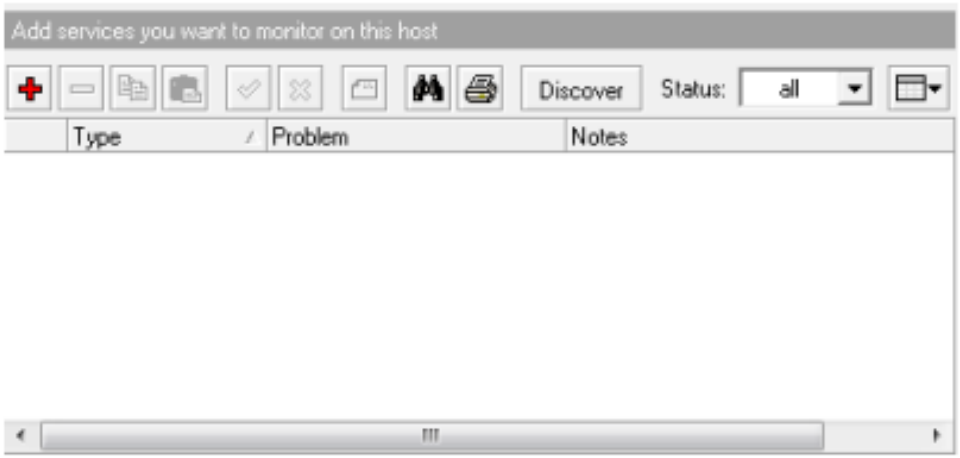


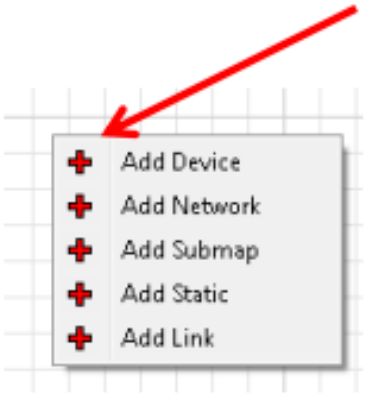


Começando o desenho da Rede

Adicionando dispositivos

Em seguida descubra os serviços que estão rodando nesse equipamento.



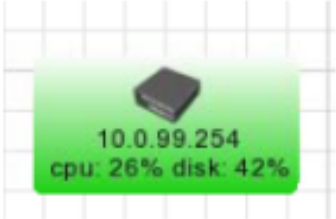


Aproveite esse momento para refletir quanta coisa inútil e insegura pode estar rodando em sua rede ☺ Desabilite tudo que for desnecessário.

Começando o desenho da Rede

Adicionando dispositivos

O dispositivo está criado.



Clique no dispositivo criado para ajustar vários parametros, mas principalmente:

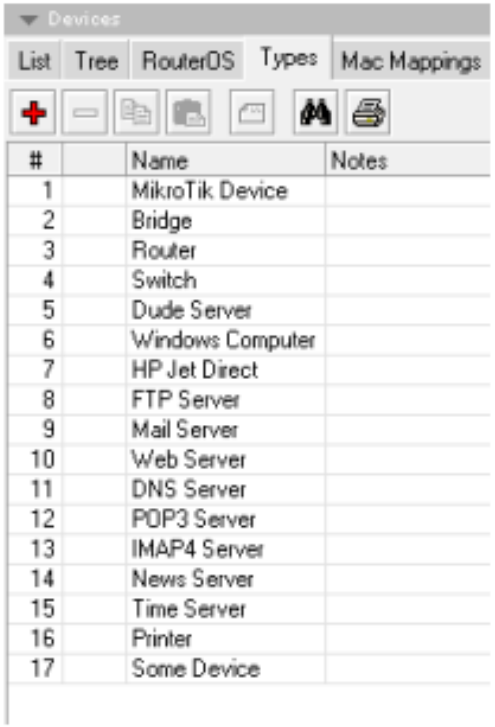
→Nome para exibição

→Tipo do dispositivo

Começando o desenho da Rede

Adicionanddo dispositivos não pré definidos

O DUDE possui vários dispositivos pré definidos mas pode-se criar novos dispositivos customizados para que o desenho realmente reflita a realidade prática.



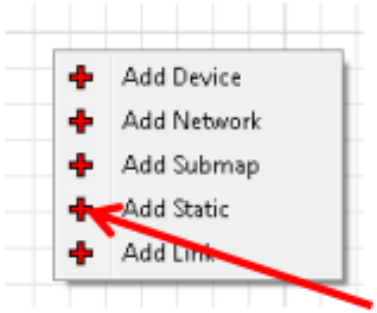
#		Name	Notes
1		MikroTik Device	
2		Bridge	
3		Router	
4		Switch	
5		Dude Server	
6		Windows Computer	
7		HP Jet Direct	
8		FTP Server	
9		Mail Server	
10		Web Server	
11		DNS Server	
12		POP3 Server	
13		IMAP4 Server	
14		News Server	
15		Time Server	
16		Printer	
17		Some Device	

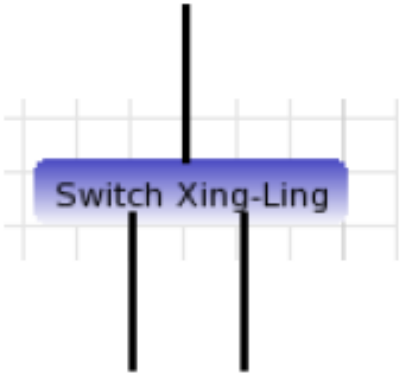
Por razões de produtividade é aconselhável que todos os dipositivos existentes na rede sejam criados com suas propriedades específicas antes do desenho da rede, mas nada impede que isso seja feito depois.

Começando o desenho da Rede

Adicionando dispositivos estáticos

Quando a rede possui elementos não configuráveis por IP (switches L2 não gerenciáveis por exemplo), é necessário criar dispositivos estáticos para fazer as ligações.



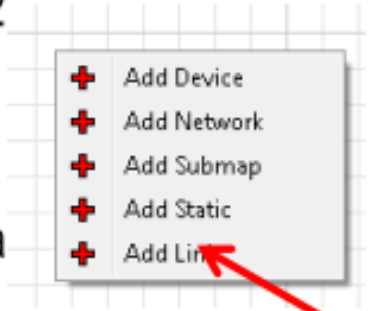


Com isso pode-se completar o diagrama de rede de forma mais realista e parecida com a rede real.

Começando o desenho da Rede

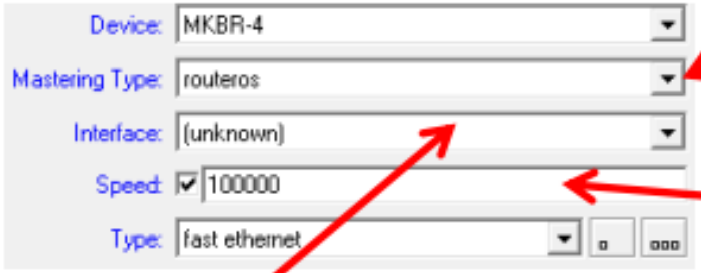
Criando os Links entre dispositivos

No mapa, clicar com o botão direito, selecionar Add Link e ligar os 2 dispositivos informando:



Mastering Type:

→ RouterOS: Se o dispositivo for Mikrotik, habilita a escolha da Interface para mostrar velocidades e estado do link.



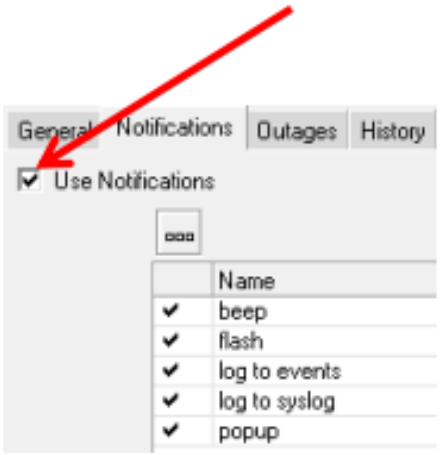
Informando a velocidade máxima do link, ativa a sinalização do estado do mesmo.

→ SNMP: para outros dispositivos que tenham suporte a snmp.

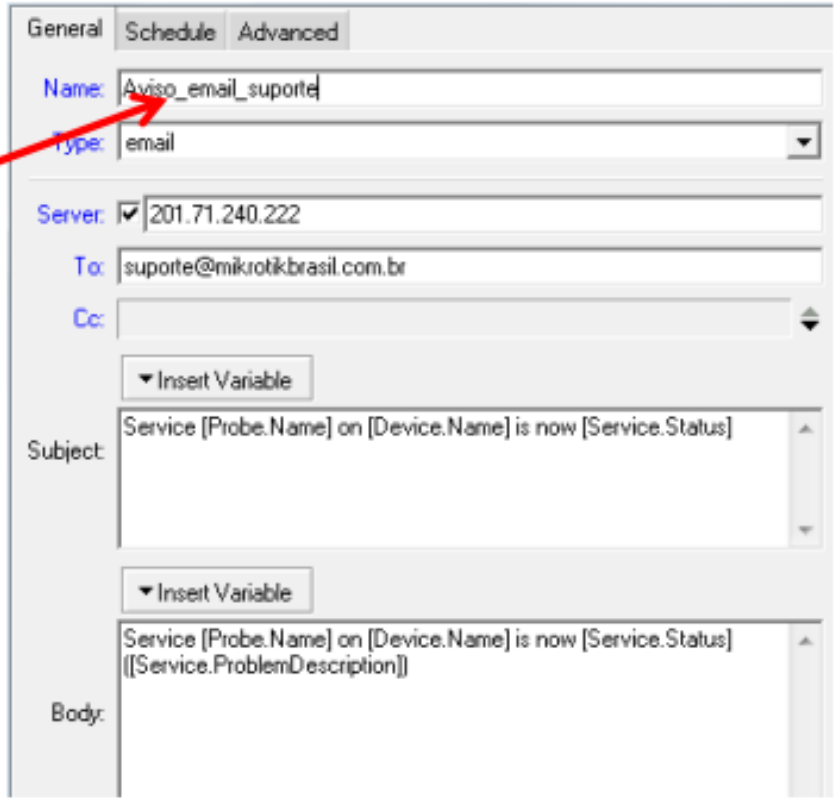
→ Simple: somente traça a linha mas não mostra informações.

Notificações

Duplo clique no dispositvo / clique no serviço e na guia notificação informar o tipo de notificação.

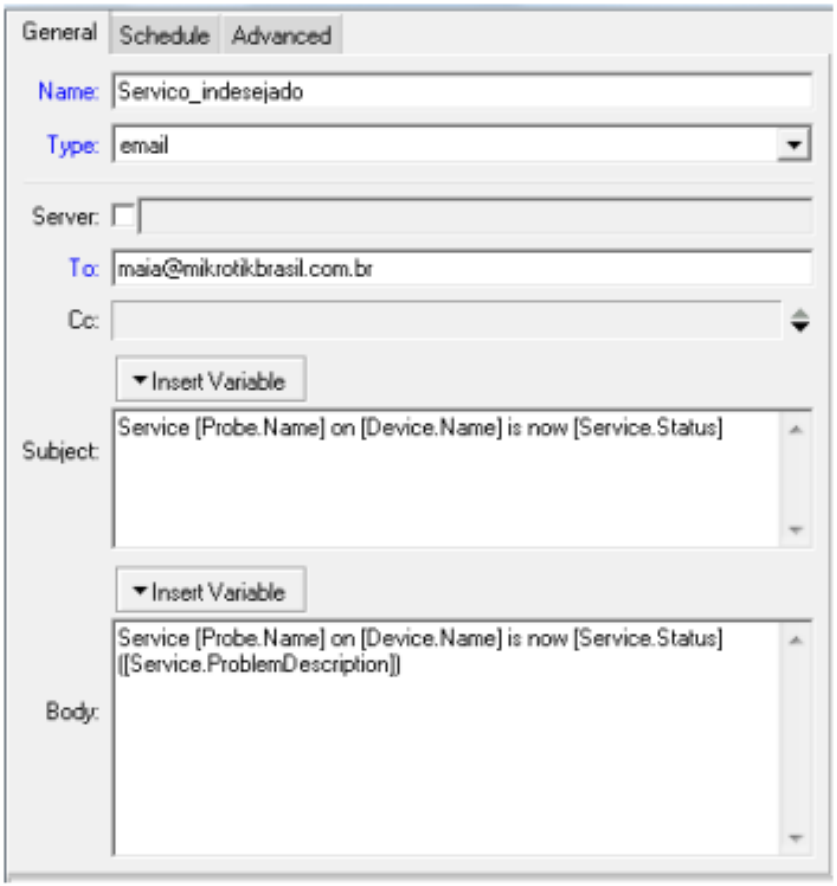


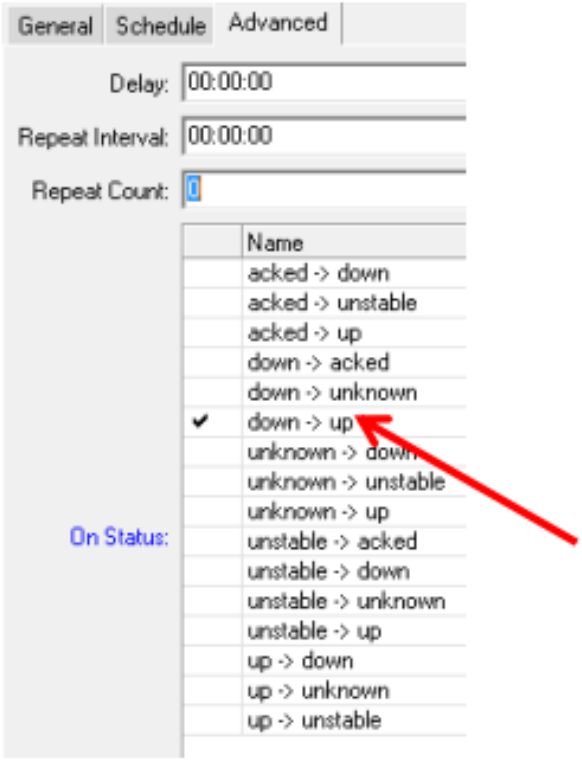
Criando novos tipos de notificação



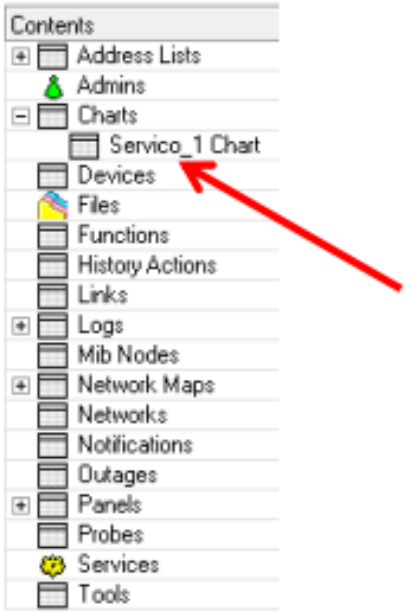
Notificações“ao contrario”

Úteis quando se quer monitorar serviços que não devem estar ativos





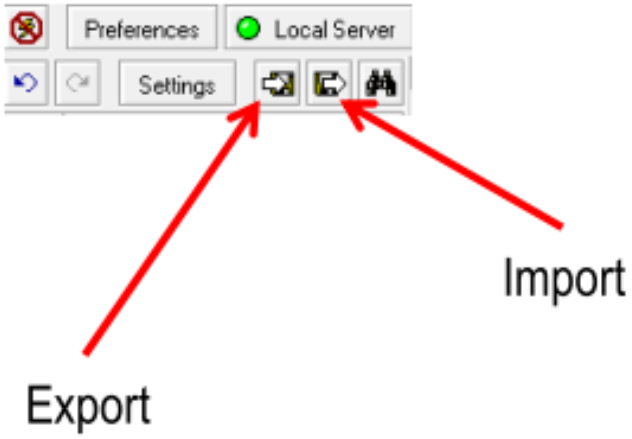
Gráficos de uso / performance, etc

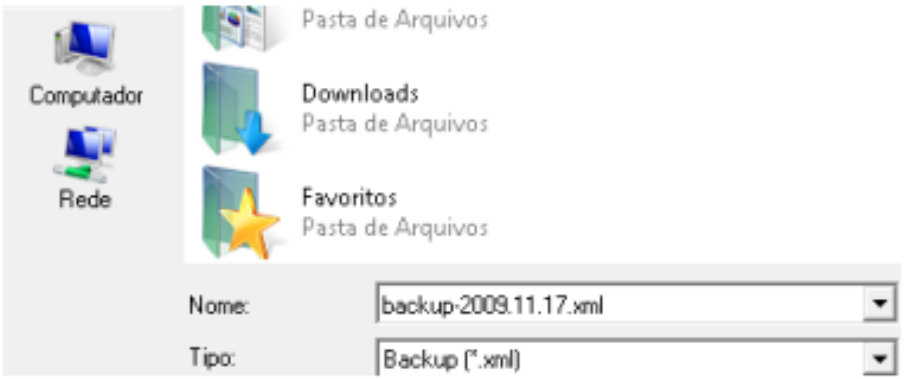


Salvando as configurações

As configurações são salvas automaticamente na medida em que são feitas.

Para ter um backup externo, use o export que será gerado um XML com todas as configurações que por sua vez podem ser importadas em outro DUDE.





Dúvidas ??

WEB - Proxy

WEB - Proxy

O Web Proxy possibilita o armazenamento de objetos Internet (dados disponíveis via protocolos HTTP e FTP) em um sistema local.

Navegadores Internet usando web-proxy podem acelerar o acesso e reduzir o consumo de banda.

Quando configurar o Web proxy, certifique-se que apenas os clientes da rede local utilizarão o mesmo, pois uma configuração aberta permitirá o acesso externo, trazendo problemas graves de segurança.

Com o Web Proxy é possível criar filtros de acesso a conteúdo indesejável, tornando a navegação mais segura aos clientes.

Um web proxy em execução, mesmo sem cache, pode ser útil como um firewall HTTP e FTP (negar acesso a determinados tipos de arquivo, como por exemplo MP3) ou ainda para redirecionar os pedidos de proxy externos.

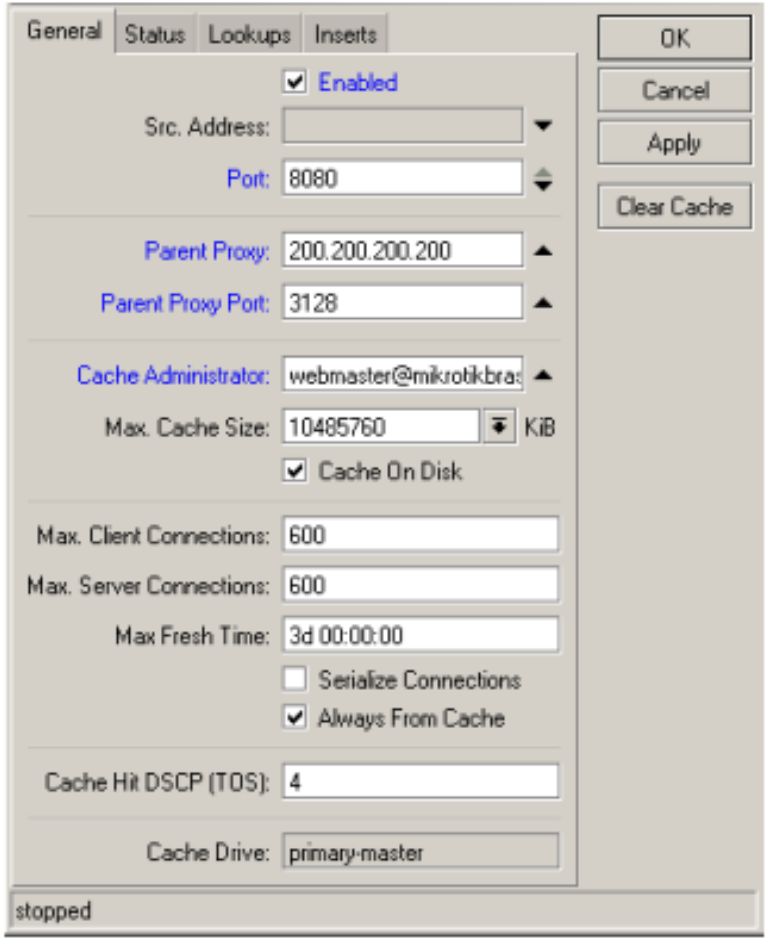
WEB - Proxy

O MikroTik RouterOS implementa um web-proxy com as seguintes características:

→ HTTP proxy
→ Transparent proxy. Onde é transparente e HTPP ao mesmo tempo
→ Lista de Acesso por origem, destino, URL e métodos de requisição
→ Lista de Acesso Cache (especifica os objetos que poderão ou não ser "cacheados")
→ Lista de Acesso Direto (especifica quais recursos deverão ser acessados diretamente - através de outro web-proxy)
→ Sistema de Logging

WEB - Proxy

Web-Proxy configurado para 10 GiB de cache, escutando na porta 8080:



- Clear Cache – Serve para esvaziar o cache armazenado (dependendo do tamaho do cache esta opção poderá ser bastante lenta).

- Enable – Utilizado para habilitar ou desabilitar o web-proxy.

- Src.Address - poderá ficar em branco. Em caso de uma hierarquia de proxy, este será o endereço IP utilizado pelo protocolo ICP. O src.address quando deixado em branco (0.0.0.0/0) será automaticamente configurado pela tabela de roteamento.

WEB - Proxy

- Port - A porta onde o web-proxy escutará.

- Parent Proxy - Utilizado para indicar o IP de um servidor proxy “pai” numa hierarquia de proxy.

- Parent Proxy Port - A porta que o parent proxy “escuta”.

- Cache Administrator - Um nome ou endereço de e-mail para exibição no caso de avisos emitidos aos clientes.

- Max. Cache Size - Tamanho máximo em kiBytes que o cache atingirá.

- Cache on Disk - Habilita o proxy a armazenar o cache em disco. Caso fique desabilitado o armazenamento será na RAM (Random Access Memory).

WEB - Proxy

• Max Client Connections - número máximo de conexões simultâneas de clientes permitidas no proxy. Após antigido o limite configurado todas as novas conexões serão rejeitadas.

• Max Server Connections - número máximo de conexões simultâneas do proxy para servidores externos. Todas as novas conexões serão colocadas em espera até que algumas das conexões ativas sejam encerradas.

• Max Fresh Time: um limite máximo de quanto tempo objetos sem um termo explícito de validade serão consideradas atuais (depois de quanto o tempo o proxy deverá realizar uma nova consulta e atualizar os objetos).

• Serialize Connections: Não habilitar múltiplas conexões ao servidor para múltiplas conexões do cliente, quando possível (servidor suportar conexões HTTP persistentes). Os clientes serão atendidos em princípio pelo método FIFO; o próximo cliente é processado quando a transferência para a sessão anterior for concluída. Se um cliente está inativo por algum tempo (no máximo 5 segundos, por padrão), o servidor irá interromper a conexão e abrir outra.

WEB - Proxy

• Always From Cache - ignorar pedidos de atualização dos clientes, caso o conteúdo seja considerado atual.

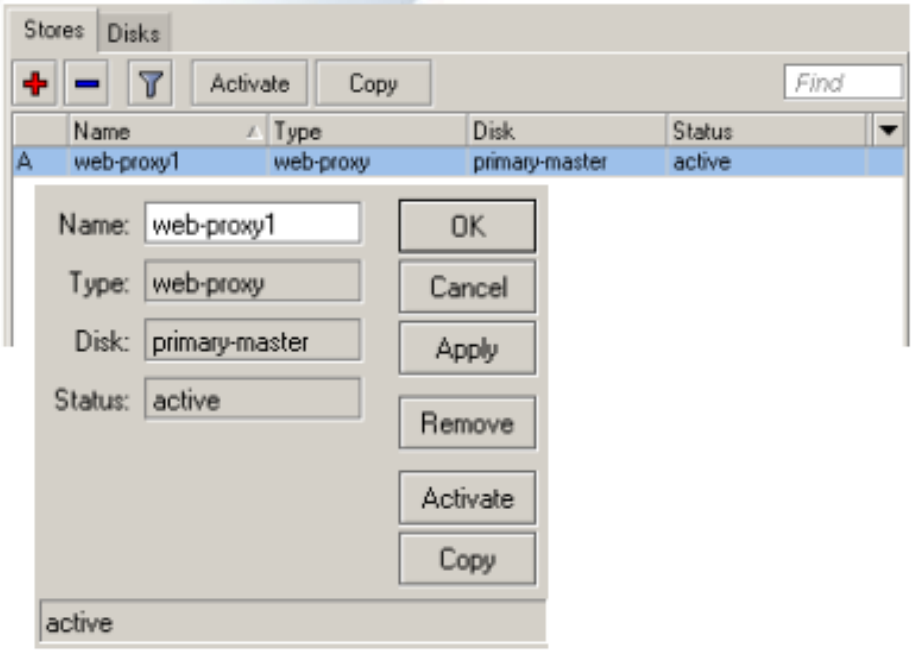
• Cache Hit DSCP (TOS) - Marca automaticamente hits do cache com o valor DSCP configurado.

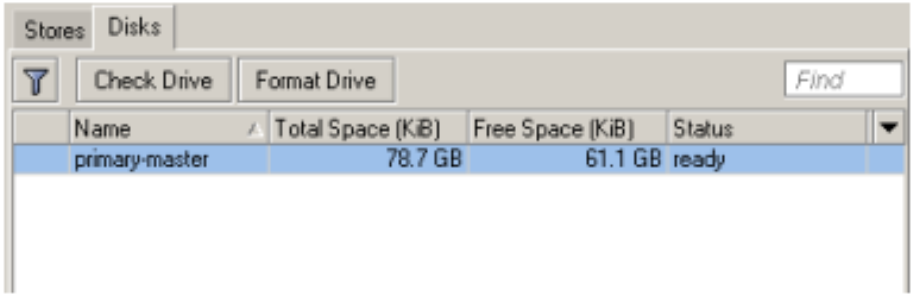
• Cache Drive - exibe o disco que está em uso para o armazenamento dos objetos em cache. Para configurar o disco é necessário acessar o menu **Stores**.

•OBSERVAÇÃO:

O web proxy escuta todos os endereços IP que estão configurados no servidor.

WEB - Proxy





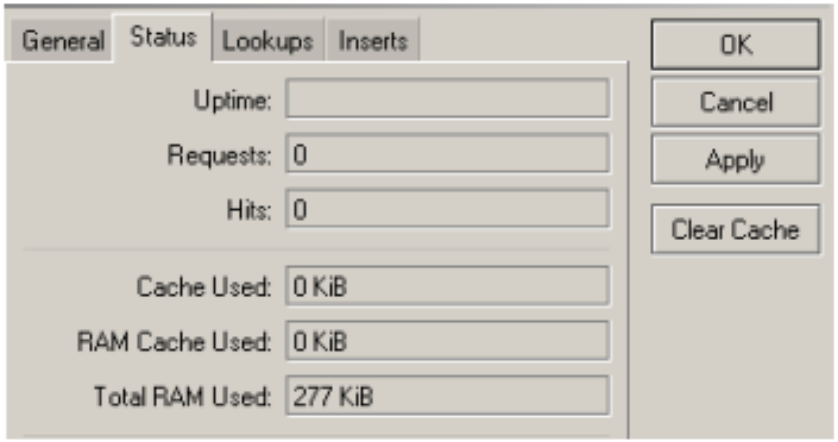
Stores

Submenu:/stores

Com esta opção podemos gerenciar a mídia onde será armazenado os objetos do cache.

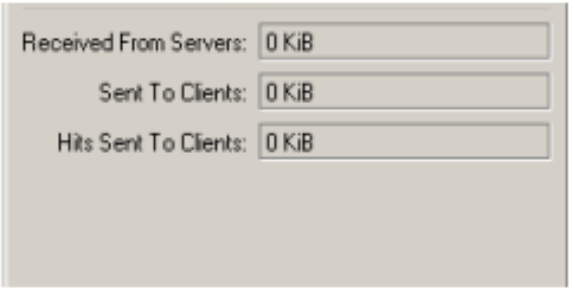
- Possível adicionar mais de 1 disco.
- Copiar o conteúdo de um disco para outro.
- Realizar checagen do disco para verificação de bad blocks.
- Realizar formatação do disco, desde que não seja onde o sistema está instalado.

Monitorando o Web-Proxy



- Uptime - o tempo transcorrido desde que o proxy foi ativado.
- Requests - total de requisições dos clientes ao proxy.
- Hits - número de requisições dos clientes atendidas diretamente do cache, pelo proxy.
- Cache Used – a quantidade do disco (ou da RAM se o cache é armazenado apenas na mesma) utilizada pelo cache.
- RAM Cache Used – quantidade da RAM utilizada pelo cache.
- Total RAM Used - a quantidade da RAM utilizada pelo proxy (excluindo tamanho da RAM Cache).

Monitorando o Web-Proxy



- Received From Servers - quantidade de dados, em kiBytes, recebidos de servidores externos
- Sent To Clients - quantidade de dados, em kiBytes, enviado aos clientes.
- Hits Sent To Clients - quantidade, em kiBytes, de cache hits enviado aos clientes.

Barra de Status – Exibe informações do estado do web proxy

- stopped - proxy está desabilitado e inativo
- running - proxy está habilitado e ativo
- formatting-disk - o disco do cache está sendo formatado
- checking-disk - checando o disco que contêm o cache para corrigir erros e inconsistências do mesmo.
- invalid-address - proxy está habilitado, mas não está ativo, porque o endereço IP é inválido (deverá ser alterado o endereço IP ou porta)

Monitorando o Web-Proxy

Lista de Conexões

Submenu: ***/ip proxy connections***

Descrição

Este menu contem uma lista das conexões ativas do proxy

Descrição das Propriedades

dst-address – endereço IP que os dados passaram através do proxy

protocol - nome do protocolo

rx-bytes - quantidade de bytes recebidos remotamente

src-address - endereço IP das conexões remotas

Monitorando o Web-Proxy

Lista de Conexões

State

idle - esperando próximo cliente

resolving - resolvendo nome DNS

rx-body - recebendo quadro HTTP

rx-header - recebendo cabeçalho; ou esperando próxima requisição do cliente

tx-body - transmitindo quadro HTTP

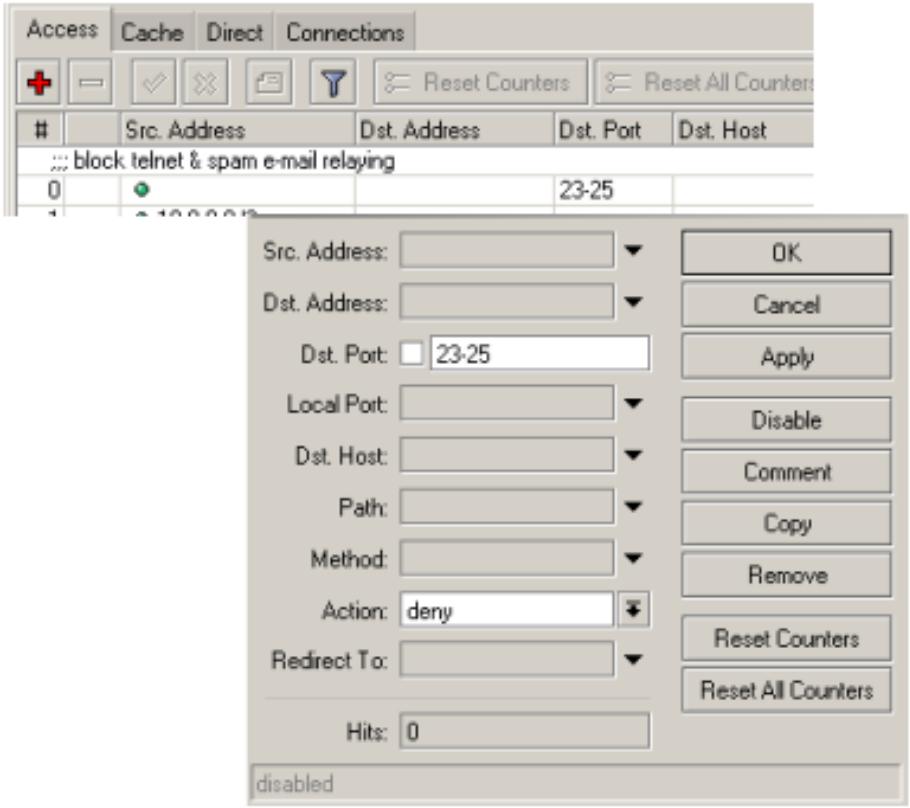
tx-header - transmitindo cabeçalho HTTP

tx-bytes - quantidade de bytes enviados remotamente

Access List

Submenu: /ip proxy access

A Lista de Acesso é configurada da mesma forma que as regras de firewall. As regras são processadas de cima para baixo. O primeiro "matching" da regra especifica a tomada de decisão para a conexão. Existe um total de 6 classificadores para especificar a regra.



Descrição das propriedades

- src-address - endereço IP de origem do pacote.
- dst-address - endereço de destino do pacote.
- dst-port (port{1,10}) - uma porta ou uma lista de portas para onde o pacote é destinado.

WEB - Proxy

Access List

• local-port (port) - especifica a porta do web-proxy que recebe os pacotes. Este valor deve corresponder a porta que o web-proxy está escutando.

• dst-host (wildcard) - Endereço IP ou nome DNS utilizado para realizar a conexão (pode ser apenas uma parte da URL)

• path (wildcard) - nome da página requisita dentro do servidor (ex. o nome de uma página web ou um documento que está hospedado no servidor)

• method (any | connect | delete | get | head | options | post | put | trace) - Método HTTP usado nas requisições (veja a seção Métodos HTTP no final deste documento).

• action (allow | deny; default: allow) - especifica a ação de negar ou liberar os pacotes que atravessam o web-proxy.

Access List

Nota

• Por padrão, é aconselhável configurar uma regra para prevenir requisições nas portas 443 e 563 (conexões através de SSL e NEWS).

• As opções dst-host e path, corresponde a uma string completa (ex.: não existirá um “matching” para "example.com" se for configurado apenas "example").

• O uso de curingas também é possível: '*' (combina um número qualquer de caracteres) e '? '(combina um caractere qualquer).

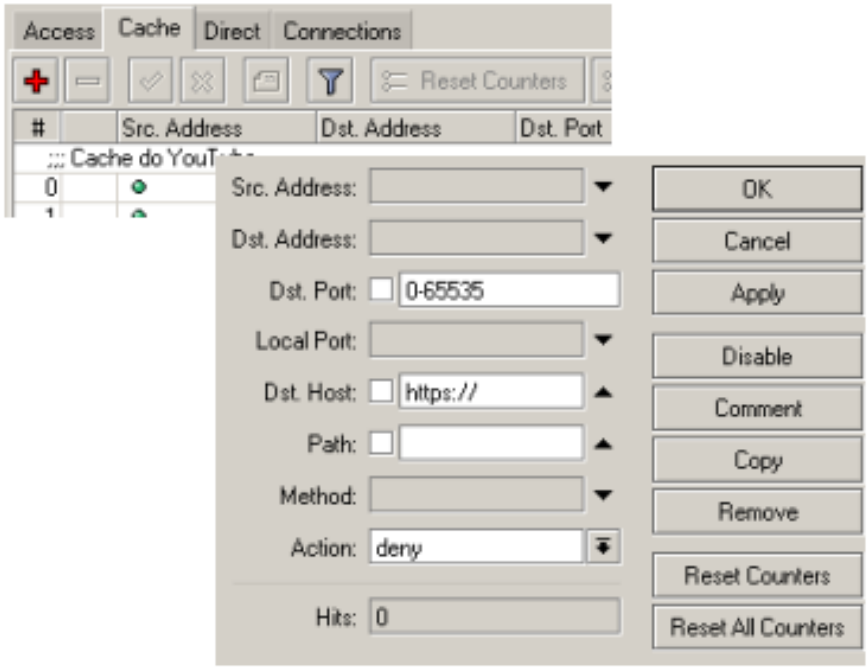
• Expressões regulares também são permitidas, e deverão iniciar por 2 pontos (':') como no exemplo:

/ip proxy access add dst-host=":\\.mp\[3g\]$" action=deny

Lista de Gerenciamento do Cache

Submenu: /ip proxy cache

A Lista de Gerenciamento do Cache especifica como as requisições (domínios, servidores, páginas) serão "cacheadas" ou não pelo servidor web-proxy. Esta lista lista é implementada da mesma forma que a Lista de Acesso. A ação padrão é "cachear" os objetos se não existir nenhuma regra.



Descrição das propriedades

- src-address (IP address/netmask) - IP de origem do pacote.
- dst-address (IP address/netmask) - IP de destino do pacote.
- dst-port (port{1,10}) - uma lista de portas que o pacote é destinado.
- local-port (port) - especifica a porta do web-proxy, a qual, o pacote foi recebido. Este valor deverá corresponder a porta que o web-proxy está escutando.

Lista de Gerenciamento do Cache

• dst-host (wildcard) - Endereço IP ou nome DNS utilizado para realizar a conexão (pode ser apenas uma parte da URL)

• path (wildcard) - nome da página requisita dentro do servidor (ex. o nome de uma página web ou um documento que está hospedado no servidor)

• method (any | connect | delete | get | head | options | post | put | trace) - Método HTTP usado nas requisições (veja a seção Métodos HTTP no final deste documento).

• action (allow | deny; default: allow) – especifica a ação a ser tomada quando um "matching" ocorrer.

allow - "cacheia" o objeto de acordo com a regra.
deny – não "cacheia" o objeto de acordo com a regra.

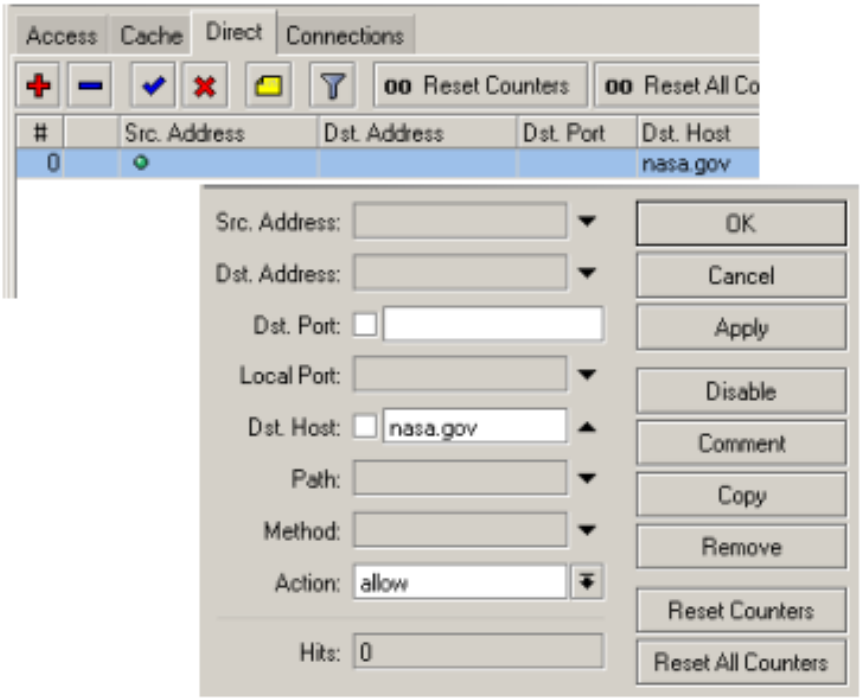
WEB - Proxy

Lista de Acesso Direto

Submenu: /ip proxy direct

Descrição

Quando um Parent Proxy está configurado, é possível passar a conexão ao mesmo ou tentar transmitir a requisição diretamente ao servidor de destino. A lista de Acesso Direto é configurada da mesma forma que a Lista de Acesso, com exceção do argumento da ação.



Descrição das propriedades

- src-address (IP address/netmask) - IP de origem do pacote.
- dst-address (IP address/netmask) - IP de destino do pacote.
- dst-port (port{1,10}) - uma lista de portas que o pacote é destinado.
- local-port (port) - especifica a porta do web-proxy, a qual, o pacote foi recebido. Este valor deverá corresponder a porta que o web-proxy está escutando.

Lista de Acesso Direto

- dst-host (wildcard) - Endereço IP ou nome DNS utilizado para realizar a conexão (pode ser apenas uma parte da URL)

- path (wildcard) - nome da página requisita dentro do servidor (ex. o nome de uma página web ou um documento que está hospedado no servidor)

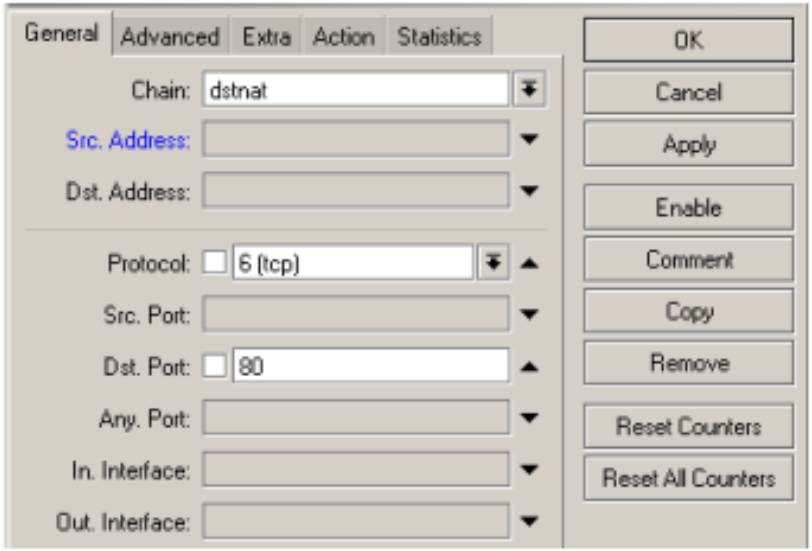
- method (any | connect | delete | get | head | options | post | put | trace) - Método HTTP usado nas requisições (veja a seção Métodos HTTP no final deste documento).

Nota

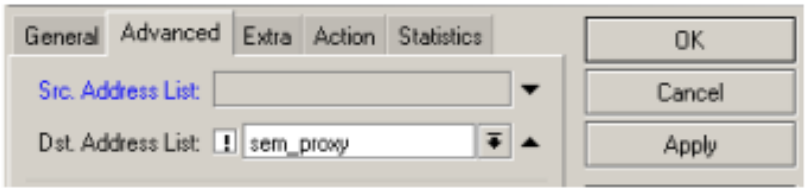
- action (allow | deny; default: allow) – especifica a ação a ser tomada quando um "matching" ocorrer.

Diferentemente da Lista de Acesso, a Lista de Acesso Direto tem a ação padrão "deny". Esta ação ocorre quando não são especificadas regras nas requisições.

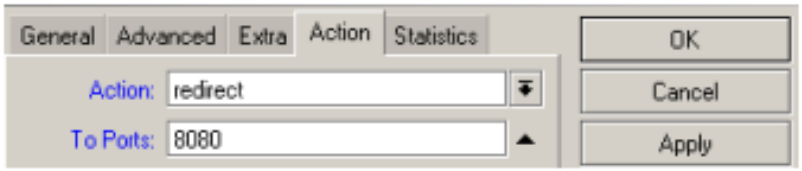
Regra de firewall para redirecionar ao web-proxy local.



1 – Utiliza-se a opção firewall nat e insere uma nova regra para protocolo TCP e porta de destino 80;

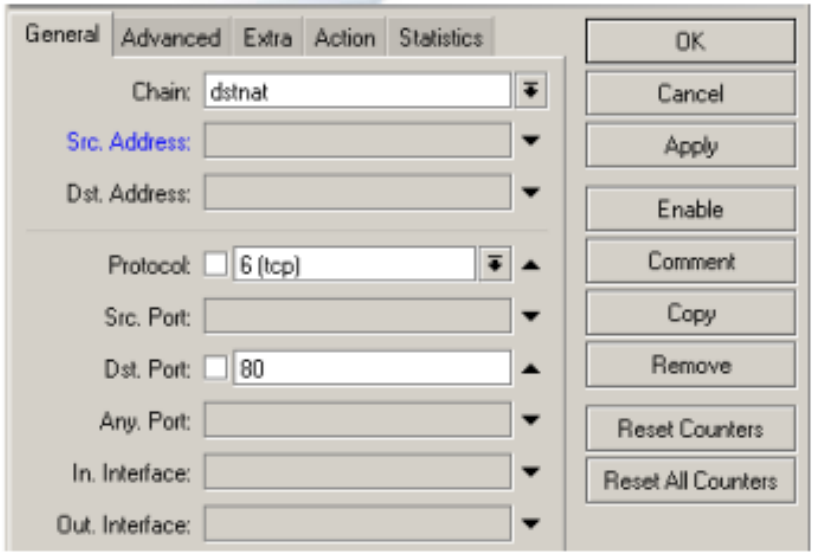


2 – Na guia Advanced, insira uma lista de endereços IP, os quais não serão redirecionados ao web-proxy;

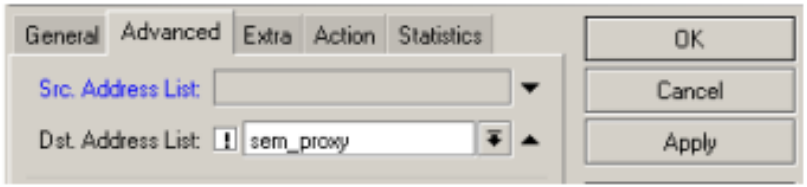


3 – Na guia Action, será a configurada a ação de redirect para a porta 8080, onde o web-proxy está escutando.

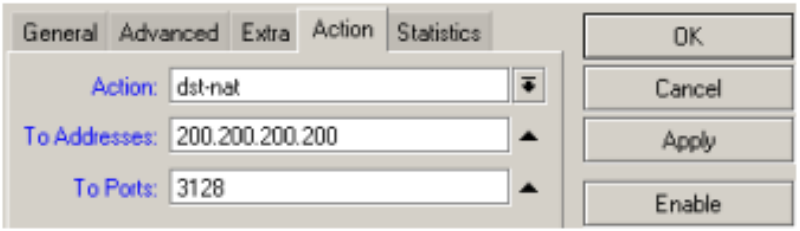
Regra de firewall para redirecionar para um web-proxy externo.



1 – Utiliza-se a opção firewall nat e insere uma nova regra para protocolo TCP e porta de destino 80;



2 – Na guia Advanced, insira uma lista de endereços IP, os quais não serão redirecionados ao web-proxy;

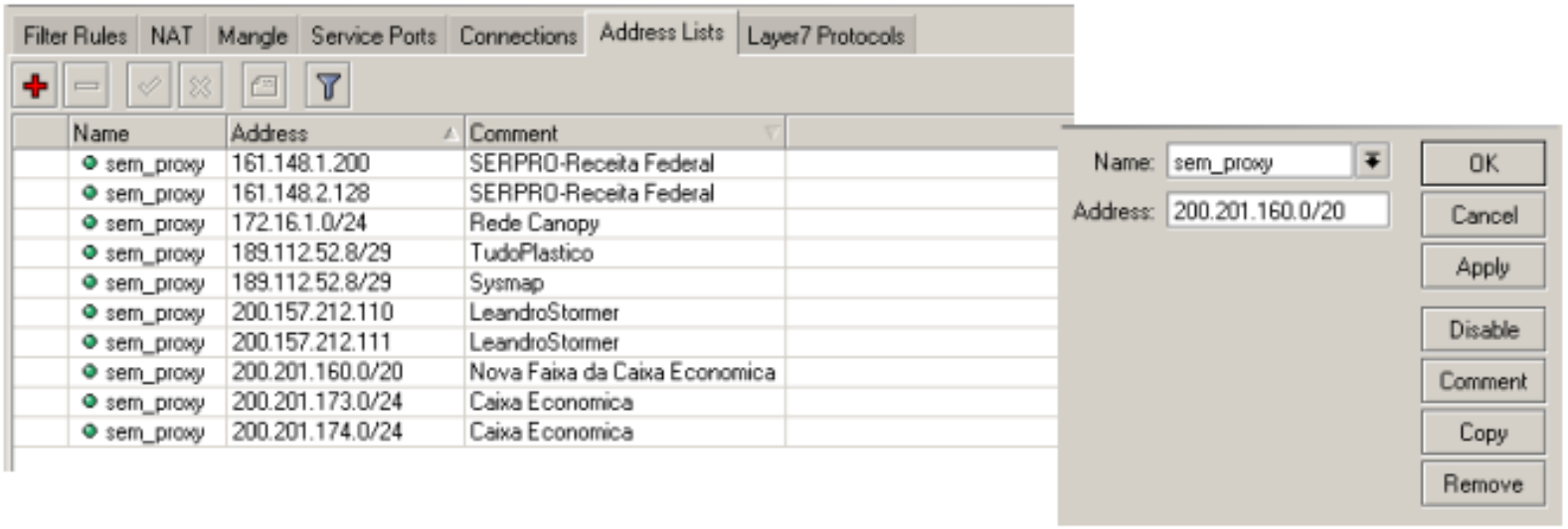


3 – Na guia Action, será a configurada a ação de dst-nat para o IP e a porta onde o web-proxy externo está escutando.

WEB - Proxy

Lista de endereços IP, os quais não farão parte das regras de redirect ou dst-nat.

Submenu: /ip firewall adress-list

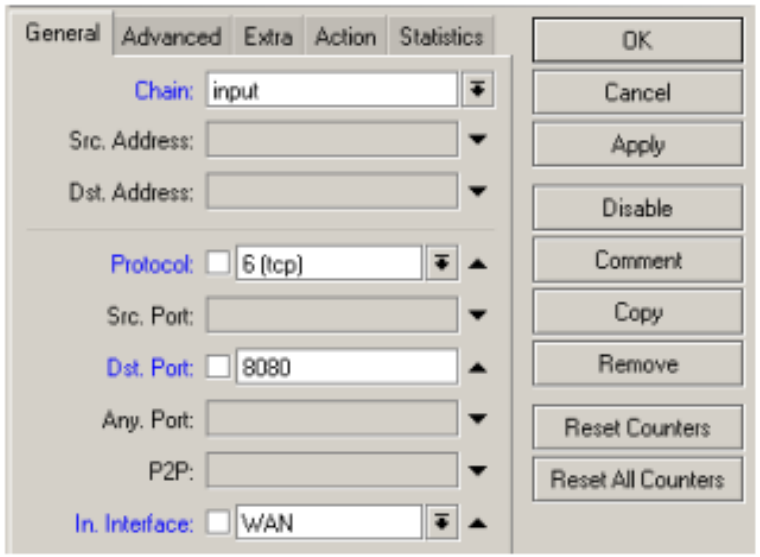


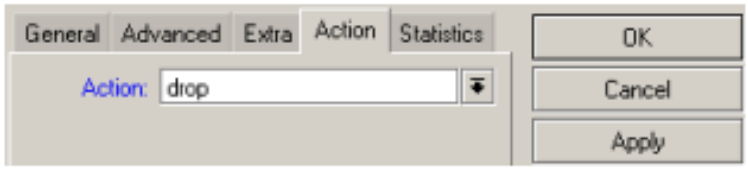
Filtro de firewall para proteger o acesso ao web-proxy

Submenu: /ip firewall filter

/ip firewall filter

add action=drop chain=input comment="" disabled=no dst-port=8080 in-interface=WAN protocol=tcp





Métodos HTTP

Descrição

OPTIONS

Este método é uma requisição de informações sobre as opções da comunicação disponível entre o cliente e o servidor (web-proxy) identificadas por Request – URI (Uniform Resource Identifier, é um termo genérico para todos os tipos de nomes e endereços aos quais referem-se os objetos da WEB. A URL é um tipo de URI). Este método permite que o cliente determine as opções e (ou) as requisições associadas a um recurso sem iniciar qualquer recuperação da comunicação.

GET

Este método recupera qualquer informação identificada pelo Request-URI. Se o Request-URI refere-se a um processo de tratamento de dados a resposta ao método GET deverá conter os dados produzidos pelo processo, e não o código fonte do processo ou procedimento(s), a menos que o código fonte seja o resultado do processo.

O método GET pode tornar-se um GET condicional se o pedido inclui uma mensagem If-Modified-Since, If-Unmodified-Since, If-Match, If-None-Match ou If-Range no cabeçalho do pacote. O método GET condicional é utilizado para reduzir o tráfego de rede com a especificação de que a transferência da conexão deverá ocorrer apenas nas circunstâncias descritas pela(s) condição(ões) do cabeçalho do pacote.

Métodos HTTP

Descrição

O método GET pode tornar-se um GET parcial se o pedido inclui uma mensagem Range no cabeçalho do pacote. O método GET parcial é destinado a reduzir o uso desnecessário de rede, solicitando apenas partes dos objetos sem transferência dos dados já realizada pelo cliente. A resposta a uma solicitação GET pode ser "cacheada" somente se ela preencher os requisitos para cache HTTP.

HEAD

Este método compartilha todas as características do método GET exceto pelo fato de que o servidor não deve retornar uma message-body na resposta. Este método recupera a meta informação do objeto intrínseco à requisição, que conduz a uma ampla utilização da mesma para testar links de hipertexto, acessibilidade e modificações recentes.

As respostas a uma requisição HEAD podem ser "cacheadas" da mesma forma que as informações contidas nas respostas podem ser utilizadas para atualizar o cache previamente identificados pelo objeto.

Métodos HTTP
Descrição

POST

Esse método solicita que o servidor de origem aceite uma requisição do objeto, subordinado a um novo recurso identificado pelo Request-URI. A verdadeira ação realizada pelo método POST é determinada pelo servidor de origem e normalmente é dependente da Request-URI. Respostas ao método POST não são “cacheadas”, a menos que a resposta inclua Cache-Control ou Expires no cabeçalho do pacote.

PUT

Esse método solicita que o servidor de destino forneça uma Request-URI. Se existe outro objeto sob a Request–URI especificada, o objeto deve ser considerado como atualizado sobre a versão residente no servidor de origem. Se a Request-URI não está apontando para um recurso existente, o servidor origem devem criar um recurso com a URI.

Se a requisição passa através de um cache e as Request-URI identificam um ou mais objetos no cache, essas inscrições devem ser tratadas como atualizáveis (antigas). Respostas a este método não são “cacheadas”.

Métodos HTTP
Descrição

TRACE

Este método invoca remotamente um loop-back na camada de aplicação da mensagem de requisição. O destinatário final da requisição deverá responder a mensagem recebida para o cliente uma resposta 200 (OK) no corpo da mesma. O destinatário final não é a origem nem o primeiro servidor proxy a receber um MAX-FORWARD de valor 0 na requisição. Uma requisição TRACE não inclui um objeto. As respostas a este método não devem ser "cacheadas".

Dúvidas ??

Laboratório Final

→ Abram um terminal

→ system reset-configuration

[MikrotikBrasil]
Routers & Wireless Systems

Obrigado !

Edson Xavier Veloso Jr.
edson@mikrotikbrasil.com.br

Sérgio Souza
sergio@mikrotikbrasil.com.br

Wardner Maia
maia@mikrotikbrasil.com.br