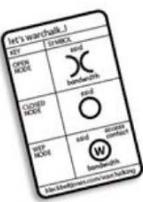


[MikrotikBrasil]
Routers & Wireless Systems


www.warchalking.org

MikrotikBrasil
Consultoria Treinamentos e Equipamentos





Sample Router

1

[MikrotikBrasil]
Routers & Wireless Systems

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



2

Reprodução não autorizada

[MikrotikBrasil]
Routers & Wireless Systems

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.



3

[MikrotikBrasil]
Routers & Wireless Systems

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
- Ministrava 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

4

APOSTILA DO CURSO MIKROTIK BRASIL EM 2007

[MikrotikBrasil]
Routers & Wireless Systems

MikrotikBrasil - OEM Sales Program

South America

Solution Box
Matheu, Argentina
Stocks: RB100, RB500 series, R52, accessories
Tel: (54-11) 4011-1200
Web: <http://www.solutionbox.com.ar>
Email: info[at]solutionbox.com.ar

ISECOM S.A.
Rosario, Mendoza y Cordoba, Argentina
Stocks: RB100, RB500, R52, accessories
Tel: 54.351.4244897
Web: <http://www.isecom.com.ar/>
Email: matiasjimenez[at]isecom.com.ar

Microcom Argentina S.A.
Rosario, Argentina
Stocks: RB100, RB500, RB44, R52, accessories
Tel: +54 3461 452852
Web: <http://www.microcom.com.ar/>
Email: s.tabellone[at]microcom.com.ar

InterCity SRL
Rio Cuarto, Argentina
Web: <http://www.intercity.net.ar/>

MD Brasil - Servicos de Telecomunicacoes Ltda
Sao Paulo, Brazil
Stocks: RB100, RB500, R52, accessories, RouterOS software
Tel: +55 17 33447277
Web: <http://www.mikrotikbrasil.com.br/>
Email: vendas[at]mikrotikbrasil.com.br

→

5

[MikrotikBrasil]
Routers & Wireless Systems

MikrotikBrasil – South America Distributors

MD Brasil - Servicos de Telecomunicacoes Ltda
Sao Paulo, Brazil
Stocks: RB100, RB500, R52, accessories, RouterOS software
Tel: +55 17 33447277
Web: <http://www.mikrotikbrasil.com.br/>
Email: vendas[at]mikrotikbrasil.com.br

Laserwifi.com
Torres Medellin, Colombia
Stocks: RB100, RB500 series, R52, accessories
Tel: (574)262.9404 301.3326.0628
Web: <http://www.laserwifi.com/>

TELKUS LTDA.
Cartagena, Colombia
Stocks: RB100, RB500, R52, RouterOS, accessories
Tel: 575 672 2304
Web: <http://www.telkuscol.com/>
Email: info[at]telkus-ip.com

ISC Conex
Caracas, Venezuela
Stocks: RB100, RB500 series, accessories
Tel: +58 (212) - 516-1714
Web: <http://www.isccnex.com/>
Email: info[at]isccnex.com

→

6

Reprodução não autorizada

APOSTILA DO CURSO MIKROTIK BRASIL EM 2007

[MikrotikBrasil]
Routers & Wireless Systems

Training Partners in Americas

Americas

WISP-Training
Web: <http://www.wisp-training.com/>

Bluemon Networks, LLC.
Reston, Virginia, US
Tel: (703) 787-7700
Web: <http://www.bluemontraining.com/>

QuickLink Wireless
Simpsonville, KY, US
Tel: 800-405-9865
Web: <http://www.quicklinkwireless.com>

Index Datacom, S.A. de C.V. I.
Los Mochis Sinaloa, Mexico
Tel: +52 668 812 5212
Web: <http://www.mikrotik-mexico.com.mx>
e-mail: [ecommerce\[at\]index.com.mx](mailto:ecommerce[at]index.com.mx)

MD Brasil Telecomunicações Ltda - São Paulo / SP
Bebedouro/SP, Brasil
Tel: +55 17 3344 7277
Web: <http://www.mikrotikbrasil.com.br>
e-mail: [contato\[at\]mikrotikbrasil.com.br](mailto:contato[at]mikrotikbrasil.com.br)

Certificate
TR0021
This is to certify, that
Wardner Maia
is a MikroTik Certified Trainer
15-06-2007

←

[MikrotikBrasil]
Routers & Wireless Systems

Processo de Homologação da RB133

4. RESULTADOS DOS ENSAIOS DA RESOLUÇÃO 365

Foto 4 – Setup com analisador de espectro

Foto 5 – Setup: Medidas de DFS

Versões indoor e outdoor

Wardner Maia
maia@mikrotikbrasil.com.br




8

Reprodução não autorizada

[MikrotikBrasil]
Routers & Wireless Systems

Instalação do Mikrotik

O Mikrotik RouterOS pode ser instalado utilizando:

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

9

[MikrotikBrasil]
Routers & Wireless Systems

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

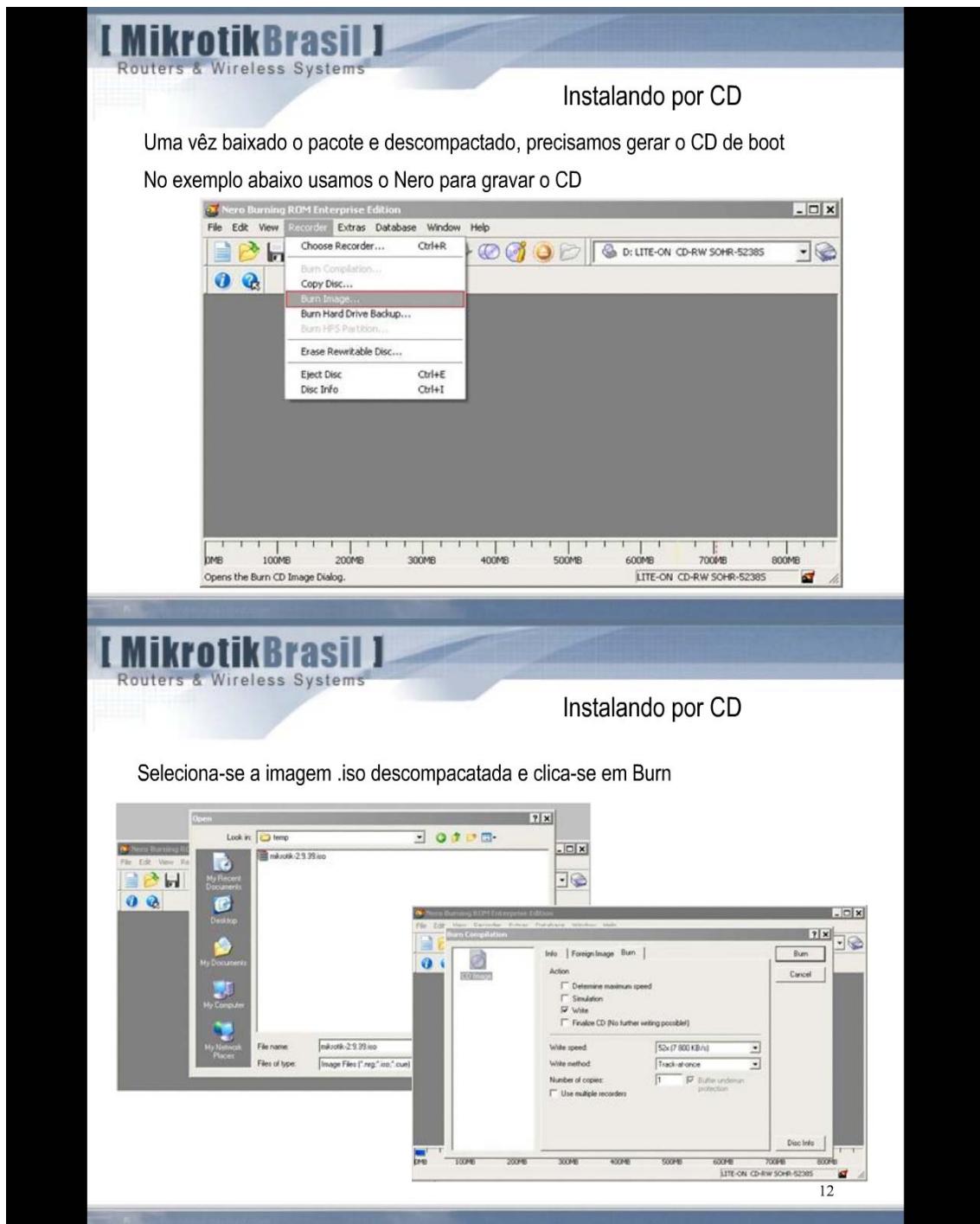
Content

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

Imagen ISO – para instalação com CD
Changelog – Modificações versões

10

APOSTILA DO CURSO MIKROTIK BRASIL EM 2007



Reprodução não autorizada

APOSTILA DO CURSO MIKROTIK BRASIL EM 2007



Instalando por CD

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

Mikrotik-3 - Microsoft Virtual PC 2007

Action Edit CD Floppy Help

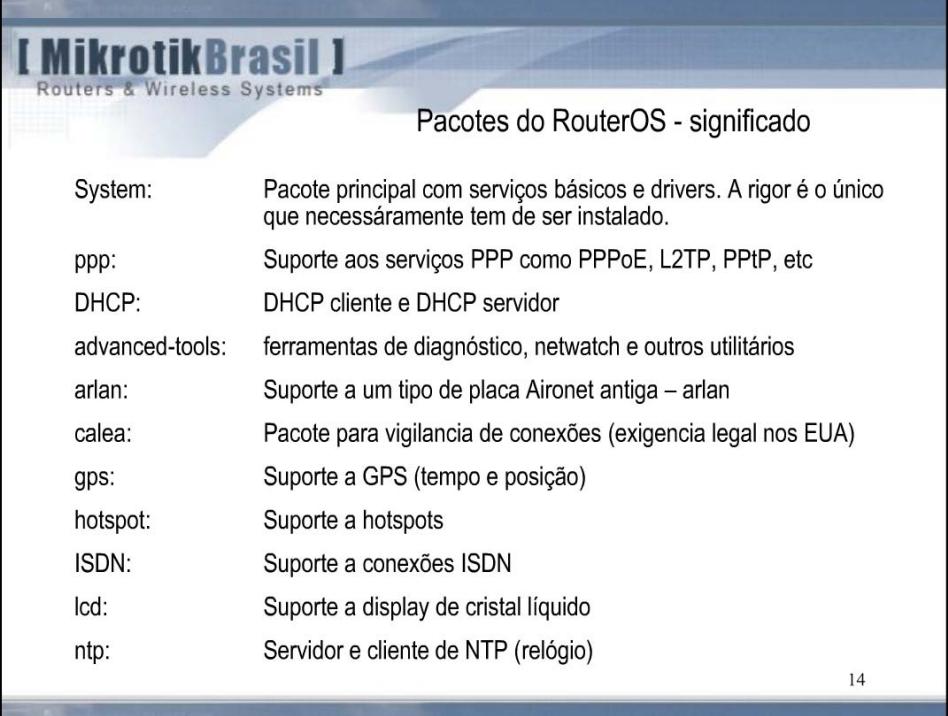
Welcome to MikroTik Router Software installation

Move around menu using 'p' and 'n' or arrow keys, select with 'spacebar'.
Select all with 'a', minimum with 'm'. Press 'i' to install locally or 'r' to
install remote router or 'q' to cancel and reboot.

[] system	[] lcd	[] synchronous
[] ppp	[] ntp	[] telephony
[] dhcp	[] radiolan	[] ups
[] advanced-tools	[] routerboard	[] user-manager
[] arlan	[] routing	[] web-proxy
[] gps	[] routing-test	[] webproxy-test
[] hotspot	[] rstp-bridge-test	[] wireless
[] isdn	[] security	[] wireless-legacy

system (depends on nothing):
Main package with basic services and drivers

13



Pacotes do RouterOS - significado

System:	Pacote principal com serviços básicos e drivers. A rigor é o único que necessariamente 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 vigilância 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)

14

Reprodução não autorizada

APOSTILA DO CURSO MIKROTIK BRASIL EM 2007

[MikrotikBrasil]
Routers & Wireless Systems

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

15

[MikrotikBrasil]
Routers & Wireless Systems

Instalando por CD

Pode-se selecionar 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"

The screenshot shows a terminal window titled "Welcome to MikroTik Router Software installation". It displays a menu for selecting packages to install. The packages listed are: system, lcd, synchronous, ppp, ntp, telephone, dhcp, radiolan, ups, advanced-tools, routerboard, user-manager, arлан, routing, web-proxy, gps, routing-test, webproxy-test, hotspot, rstp-bridge-test, wireless, isdn, security, and wireless-legacy. The "system" package is selected (indicated by a checked checkbox). The menu also includes instructions: "Move around menu using 'p' and 'n' or arrow keys, select with 'spacebar'. Select all with 'a', minimum with 'm'. Press 'i' to install locally or 'r' to install remote router or 'q' to cancel and reboot." At the bottom, it says "system (depends on nothing): Main package with basic services and drivers" and asks "Do you want to keep old configuration? [y/n]".

16

Reprodução não autorizada

[MikrotikBrasil]
Routers & Wireless Systems

Instalação com Netinstall

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

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

→ Pode-se instalar em 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.

17

[MikrotikBrasil]
Routers & Wireless Systems

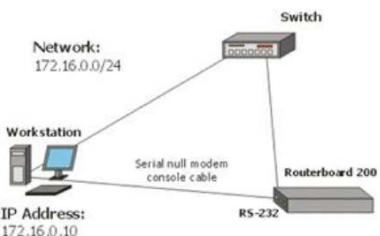
Instalação com Netinstall

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



18

The screenshot shows the MikroTik Router Installer v1.10 interface. The main window title is "Instalação com Netinstall". It displays a table of drives with one entry: "mikrotik... 00:02-44:18:71:86 Ready". Configuration fields include "Software ID: CYKN-PyN", "IP address: 192.168.168.30 / 24", "Gateway: 192.168.168.1", and "Baud rate: 921600". Below this is a "Selected 0 package(s)" section and a "Packages" section listing several software packages:

Name	Version	Description
advanced-tools	2.8.6	email client, pingers, netwatch and other utilities
airan	2.8.6	Provides support for an obsolete Aironet Airon card
dhcp	2.8.6	DHCP client and server
gps	2.8.6	Provides support for GPS.
hotspot	2.8.6	Provides HotSpot

At the bottom left of the window, it says "Loaded 20 package(s)".

Text instructions on the left side of the slide:

- 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.

19

The screenshot shows a web browser window with the MikroTik logo at the top. The main content area has the heading "Acesso ao Mikrotik".

Text below the heading:

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

20

APOSTILA DO CURSO MIKROTIK BRASIL EM 2007



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] >
```

21



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.

22

Reprodução não autorizada

APOSTILA DO CURSO MIKROTIK BRASIL EM 2007

The screenshot shows the MikroTik Console interface. At the top, the MikrotikBrasil logo is visible. Below it, the title "Console do Mikrotik" is displayed. The main content area contains several command-line examples:

Print command output:

```
[admin@MikroTik] interface ethernet> print
Flags: X - disabled, R - running
# NAME MTU MAC-ADDRESS ARP
0 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
```

23

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
```

24

Reprodução não autorizada

[MikrotikBrasil]
Routers & Wireless Systems

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.

25

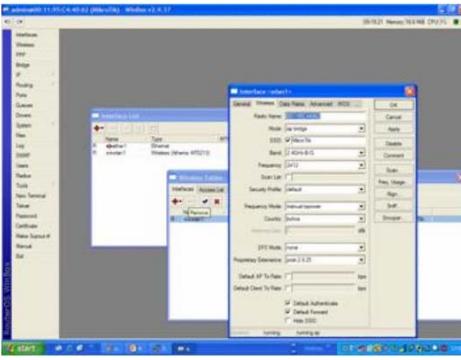
[MikrotikBrasil]
Routers & Wireless Systems

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
- Traf 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

26

Reprodução não autorizada

[MikrotikBrasil]
Routers & Wireless Systems

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.

27

[MikrotikBrasil]
Routers & Wireless Systems

Manutenção do Mikrotik

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

28

APOSTILA DO CURSO MIKROTIK BRASIL EM 2007

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.

29

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 acréscimo de novas funcionalidades

→ 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.

30

Reprodução não autorizada

15

[MikrotikBrasil]
Routers & Wireless Systems

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

Name	Version	Build Time	Scheduled
routeros-x86	2.9.45	Aug/01/2007 13:06:28	
advanced-tools	2.9.45	Aug/01/2007 14:04:17	
dhcp	2.9.45	Aug/01/2007 14:04:22	
hotspot	2.9.45	Aug/01/2007 14:04:23	
ntp	2.9.45	Aug/01/2007 14:05:55	
ppp	2.9.45	Aug/01/2007 14:04:24	
routerboard	2.9.45	Aug/01/2007 14:05:59	
routing	2.9.45	Aug/01/2007 14:04:27	
routing-test	2.9.45	Aug/01/2007 14:06:02	
rstp-bridge-test	2.9.45	Aug/01/2007 14:05:54	
security	2.9.45	Aug/01/2007 14:04:21	
synchronous	2.9.45	Aug/01/2007 14:06:21	
system	2.9.45	Aug/01/2007 14:04:12	
ups	2.9.45	Aug/01/2007 14:05:55	
web-proxy	2.9.45	Aug/01/2007 14:06:17	
web-proxy-test	2.9.45	Aug/01/2007 14:05:03	
wireless	2.9.45	Aug/01/2007 14:05:49	
wireless-legacy	2.9.45	Aug/01/2007 14:05:52	

31

[MikrotikBrasil]
Routers & Wireless Systems

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

Name	Version	Build Time	Scheduled
routeros-x86	2.9.45	Aug/01/2007 13:06:28	
advanced-tools	2.9.45	Aug/01/2007 14:04:17	
dhcp	2.9.45	Aug/01/2007 14:04:22	
hotspot	2.9.45	Aug/01/2007 14:04:23	
ntp	2.9.45	Aug/01/2007 14:05:55	
ppp	2.9.45	Aug/01/2007 14:04:24	
routerboard	2.9.45	Aug/01/2007 14:05:59	
routing	2.9.45	Aug/01/2007 14:04:27	
routing-test	2.9.45	Aug/01/2007 14:06:02	
rstp-bridge-test	2.9.45	Aug/01/2007 14:05:54	
security	2.9.45	Aug/01/2007 14:04:21	
synchronous	2.9.45	Aug/01/2007 14:06:21	
system	2.9.45	Aug/01/2007 14:04:12	
ups	2.9.45	Aug/01/2007 14:05:55	
web-proxy	2.9.45	Aug/01/2007 14:06:17	
web-proxy-test	2.9.45	Aug/01/2007 14:05:03	
wireless	2.9.45	Aug/01/2007 14:05:49	
wireless-legacy	2.9.45	Aug/01/2007 14:05:52	

APOSTILA DO CURSO MIKROTIK BRASIL EM 2007

[MikrotikBrasil]
Routers & Wireless Systems

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 "backuper" partes das configurações use o comando export

Versão 2.9 ou versão 3.x ??

Atualmente estamos no final da série 2.9.x e partindo para a v3, que está em fase de "release candidate"

Diferenças básicas das versões :

2.9.x	→ Linux Kernel 2.4.31
3.x	→ Linux Kernel 2.6.20

Compatibilidade de Hardware na v3:

- Suporte a SMP (multiprocessamento)
- Suporte a discos SATA
- RAM máxima aumentada de 1 GB para 2 GB
- Várias interfaces de rede novas suportadas
- Descontinuados alguns suportes e hardwares antigos

Reprodução não autorizada

[MikrotikBrasil]
Routers & Wireless Systems

Licenciamento do Mikrotik

Detalhes de licenciamento

- A chave é gerada sobre um software-id fornecido pelo próprio sistema
- Fica vinculada ao HD ou Flash
- A licença pode ser “colada” na janela de terminal ou enviada por ftp
- Esse HD / Flash pode ser montado em qualquer outro computador aproveitando a licença
- Importante: **a formatação com ferramentas de terceiros faz perder a licença instalada**

35

[MikrotikBrasil]
Routers & Wireless Systems

Política de Licenciamento

- As Licenças nunca expiram
- Podem ser ser atualizadas para a última versão do próximo release. ex: 2.9.x → 3beta → 3.x
- Podem ser usadas várias interfaces
- Uma licença por máquina

Level number	0 (FREE)	1 (DEMO)	2 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Controller)
Software only	free, no key	registration required	volume only	\$45 (WISP4)	\$95 (WISP5)	\$250 (WISP6)
Installed on IDE Flash	-	-	volume only	\$85 (WISP4)	\$135 (WISP5)	\$299 (WISP6)
Features						
Upgradable To	-	no upgrades	ROS v3.x	ROS v3.x	ROS v4.x	ROS v4.x
Initial Config Support	-	-	-	15 days	30 days	30 days
Wireless AP	24h limit	-	-	yes	yes	yes
Wireless Client and Bridge	24h limit	-	yes	yes	yes	yes
RIP, OSPF, BGP, protocols	24h limit	-	yes (v3 x86 = RIP) RIP, OSPF	yes (v3 x86 = RIP, OSPF)	yes (v3 x86 = RIP, OSPF)	yes
EoIP tunnels	24h limit	1	unlimited (V3 = 1)	unlimited	unlimited	unlimited
PPPoE tunnels	24h limit	1	200 (V3 = 1)	200	500	unlimited
PTP tunnels	24h limit	1	200 (V3 = 1)	200	unlimited	unlimited
L2TP tunnels	24h limit	1	200 (V3 = 1)	200	unlimited	unlimited
VLAN interfaces	24h limit	1	unlimited (V3 = 1)	unlimited	unlimited	unlimited
P2P firewall rules	24h limit	1	unlimited (V3 = 1)	unlimited	unlimited	unlimited
NAT rules	24h limit	1	unlimited	unlimited	unlimited	unlimited
HotSpot active users	24h limit	1	1	200	500	unlimited
Radius client	24h limit	-	yes	yes	yes	yes
Queues	24h limit	1	unlimited	unlimited	unlimited	unlimited
Web proxy	24h limit	-	yes	yes	yes	yes
Synchronous interfaces	24h limit	-	-	yes	yes	yes
User manager active sessions	24h limit	1	10 (v3 10)	10 (v3 20)	10 (v3 50)	Unlimited

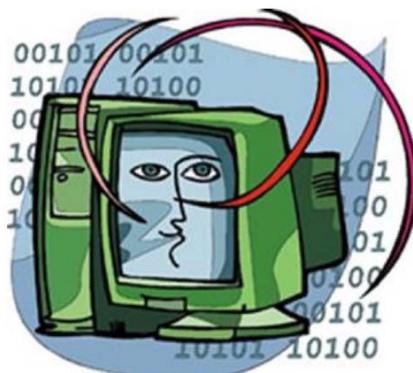
36

Dúvidas e esclarecimentos adicionais sobre

- Instalação ?
- Acesso ?
- Manutenção ?
- Licenciamento ?

37

Revisão de TCP/IP



38

[MikrotikBrasil]
Routers & Wireless Systems

O Modelo OSI (Open Systems Interconnection)

APLICAÇÃO
APRESENTAÇÃO
SESSÃO
TRANSPORTE
REDE
ENLACE
FÍSICA

← Camadas 4, 5 e 6 (sessão, apresentação e aplicação)
← Camada 4 (garante o transporte dos dados – TCP e UDP)
← Camada 3 (faz endereçamento lógico – roteamento IP)
← Camada 2 (detecta/corre erros, controla fluxo, end.. físico)
← Camada 1 (conexões físicas da rede, como cabos, wireless)

39

[MikrotikBrasil]
Routers & Wireless Systems

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.931, T1, E1, 10BASE-T, 100BASE-TX , ISDN, SONET, DSL, FHSS, DSSS, OFDM etc

40

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

41

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

42

Protocolo IP

É um protocolo de endereçamento 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).

43

Endereçamento IP

O Protocolo TCP/IP utiliza 4 sequências de 8 bits (octetos) para representação dos endereços IP e máscaras

Exemplo :

11000000.10101000.00000001.00000001, em notação binária,
convertida para decimal fica:

$$\begin{array}{rcl} 11000000 \rightarrow 2^7+2^6 & = 128+64 & = 192 \\ 10101000 \rightarrow 2^7+2^5+2^3 & = 128+32+8 & = 168 \\ 00000001 \rightarrow 2^0 & & = 1 \\ 00000001 \rightarrow 2^0 & & = 1 \end{array}$$

→ 192.168.1.1

44

Máscaras de Sub-Rede

As máscaras de rede servem para, em conjunto com o endereço IP, separar grupos de computadores. Da mesma forma que os IP's as máscaras de rede utilizam octetos, no entanto variando os últimos bits:

11111111.11111111.11111111.11111111 => /32
11111111 em decimal é : $2^7 + 2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0 = 255$
máscara equivalente em decimal : 255.255.255.255

11111111.11111111.11111111.11111100 => /30
11111100 em decimal é: $2^7 + 2^6 + 2^5 + 2^4 + 2^3 + 2^2 = 252$
máscara equivalente em decimal: 255.255.255.254

11111111.00000000.00000000.00000000 => /8
00000000 em binário é: 0
máscara equivalente em decimal: 255.0.0.0

45

Endereços IP e máscaras de sub rede

- Endereços IP podem, em conjunto com as máscaras de rede ser utilizados para agrupar conjuntos de computadores em sub-redes.
 - em uma rede, estando os computadores na mesma subrede eles se comunicam diretamente pelo barramento de rede (hub ou switch)
 - estando em redes diferentes a comunicação é passada ao gateway da rede (roteador)
- Roteadores tratam endereçamentos IP, fazendo os pacotes chegarem a seus destinos finais.

46

APOSTILA DO CURSO MIKROTIK BRASIL EM 2007



Quantos hosts cabem em uma Sub-Rede ?

- O endereçamento de rede se dá por uma multiplicação binária efetuada entre o endereço IP e a máscara de rede que determina se os computadores estão na mesma subrede.
- Por definição toda rede tem seu IP inicial reservado para o endereço de rede e o seu maior IP para o endereço de broadcast da rede, ou seja para onde irão ser enviadas toda a comunicação que seja para todos IP's da rede.
- Esses endereços não podem ser utilizados para hosts

Exemplo :

A Rede 192.168.1.128/26 tem os IPs reservados 192.168.1.128 como endereço de rede e 192.168.1.255 como endereço de broadcast, podendo ter apenas 62 hosts

47



IP x mascaramento de rede

O Mascaramento de rede serve para subdividir grupos de computadores em diversas redes e faz isso multiplicando de forma binária o endereço IP pela máscara de rede:

Quando um computador envia um pacote para outro, o protocolo IP precisa inicialmente saber se:

- Estão na mesma rede → envia pacote para o barramento de rede
- Estão em redes diferentes → envia para o roteador

Como o protocolo “sabe” se os computadores estão na mesma rede ?

- Exemplo 1 : 200.200.200.10/26 → 200.200.200.20/26
- Exemplo 2 : 200.200.200.10/26 → 200.200.200.200/26

48

APOSTILA DO CURSO MIKROTIK BRASIL EM 2007



Routers & Wireless Systems

200.200.200.10/26 → 200.200.200.20/26

	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	10000000
Multiplicação binária		11001000	11001000	00001010	00000000

	Decimal	1 octeto	2 octeto	3 octeto	4 octeto
IP	200.200.200.20	11001000	11001000	11001000	00010100
Mask	255.255.255.192	11111111	11111111	11111111	10000000
Multiplicação binária		11001000	11001000	11001000	00000000

Resultados iguais → Mesma Rede

49



Routers & Wireless Systems

200.200.200.10/26 → 200.200.200.200/26

	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	10000000
Multiplicação binária		11001000	11001000	00001010	00000000

	Decimal	1 octeto	2 octeto	3 octeto	4 octeto
IP	200.200.200.200	11001000	11001000	11001000	11001000
Mask	255.255.255.192	11111111	11111111	11111111	10000000
Multiplicação binária		11001000	11001000	11001000	10000000

Resultados diferentes → Redes diferentes

50

Reprodução não autorizada

APOSTILA DO CURSO MIKROTIK BRASIL EM 2007



Máscaras de Sub-Rede

Resumo

255.255.255.255 => 11111111.11111111.11111111.11111111 => /32
255.255.255.254 => 11111111.11111111.11111111.11111110 => /31
255.255.255.252 => 11111111.11111111.11111111.11111100 => /30
255.255.255.248 => 11111111.11111111.11111111.11111000 => /29
255.255.255.240 => 11111111.11111111.11111111.11110000 => /28
255.255.255.224 => 11111111.11111111.11111111.11100000 => /27
255.255.255.192 => 11111111.11111111.11111111.11000000 => /26
255.255.255.128 => 11111111.11111111.11111111.10000000 => /25
255.255.255.0 => 11111111.11111111.11111111.00000000 => /24
....
255.255.0.0 => 11111111.11111111.00000000.00000000 => /16
....
255.0.0.0 => 11111111.00000000.00000000.00000000 => /8

51



Espaço de subredes

Bits	Decimal	Sub-redes	Hosts/subrede	Hosts disponíveis
/24	255.255.255.0	1	254	254
/25	255.255.255.128	2	126	252
/26	255.255.255.192	4	62	248
/27	255.255.255.224	8	30	240
/28	255.255.255.240	16	14	224
/29	255.255.255.248	32	6	192
/30	255.255.255.252	64	2	128

52

Reprodução não autorizada

Tipos de tráfego em uma Rede

Unicast:

Tráfego destinado a um host apenas

Broadcast:

Tráfego destinado a todos os hosts da mesma rede. Redes remotas podem ser unidas através de túneis e serem parte do mesmo “domínio de Broadcast”

Multicast :

Tráfego destinado a hosts previamente “inscritos” para receberem o tráfego multicast. Os dispositivos de rede devem ter capacidade de propagar o tráfego multicast.

53

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

54

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

55

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.

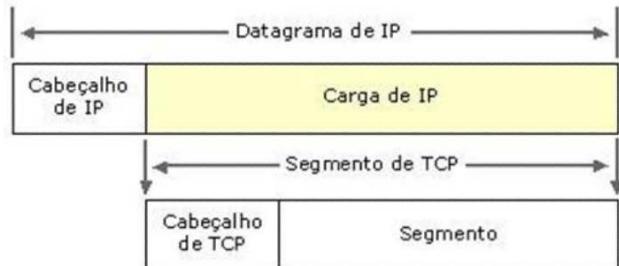
56

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

57

TCP



Os segmentos TCP são encapsulados e
enviados em datagramas IP

58

[MikrotikBrasil]
Routers & Wireless Systems

Portas TCP

```
graph TD; FTP[Servidor de FTP] --- PortasTCP[Portas TCP 20 e 21]; Telnet[Servidor Telnet] --- PortaTCP23[Porta TCP 23]; Web[Servidor Web] --- PortaTCP80[Porta TCP 80]; PortasTCP --- TCP[TCP]; PortaTCP23 --- TCP; PortaTCP80 --- 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

59

[MikrotikBrasil]
Routers & Wireless Systems

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

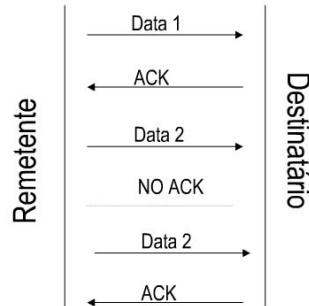
```
sequenceDiagram; participant Cliente; participant Servidor; Cliente->>Servidor: SYN (100); activate Servidor; Servidor-->>Cliente: ACK (101), SYN (400); activate Cliente; Cliente-->>Servidor: ACK (401); deactivate all;
```

60

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

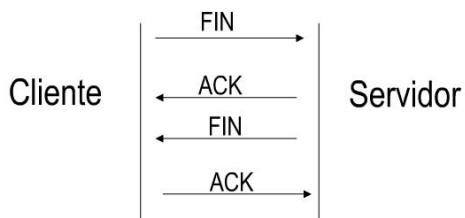


61

Encerrando uma conexão TCP

O processo de encerramento também é feito em 4 fases:

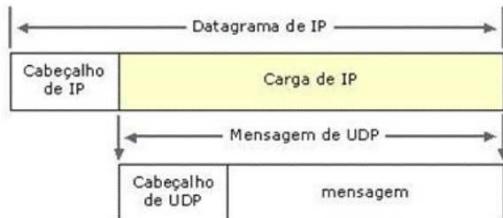
- Remetente manda um pedido de FIN
- Destinatário responde acusando o recebimento com um ACK
- Destinatário manda seu pedido de FIN
- Remetente envia um ACK



62

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



63

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

64

Dúvidas ou considerações acerca de:

- Camadas física / enlace / rede / transporte / aplicação
- Protocolo IP / Mascaramento de rede ?
- Protocolo ARP ?
- TCP ?
- UDP ?

65

Mikrotik
&
Wireless



Setup Básico do AP do Curso

- 1 → Configurando o DHCP client
- 2 → Configurando uma AP básica
- 3 → Configurando um IP na Wireless
- 4 → Configurando um DHCP server
- 5 → Fazendo o mascaramento de rede

67

Setup Básico I – Usando DHCP

- 1 → Conectar o Mikrotik ao AP do Curso
- 2 → Configurar um DHCP client
- 3 → Criar um IP na placa de rede do Mikrotik
- 4 → Configurar um DHCP server
- 5 → Obter um IP para seu Laptop.
- 6 → Fazer o mascaramento
- 7 → Navegar

68

[MikrotikBrasil]
Routers & Wireless Systems

Setup Básico I – Usando IP's estáticos

- 1 → Conectar o Mikrotik a AP do Curso
- 2 → Adicionar um IP na interface Wireless
- 3 → Criar uma rota default
- 4 → Configurar o DNS
- 5 → Permitir DNS para rede interna
- 6 → Criar um IP na placa de rede do Mikrotik
- 7 → Configurar um IP, gateway e DNS na placa do Laptop
- 8 → Testar a conectividade com o Mikrotik
- 9 → Fazer uma regra de NAT de origem
- 10 → navegar

69

[MikrotikBrasil]
Routers & Wireless Systems

Interface Wireless / Geral

Name: Nome da Interface ; Type: Wireless ; MTU: Unidade máxima de transferencia (bytes)
MAC Address: Endereço MAC da Interface ; Chip Info / PCI Info: Informações da placa
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

70

[MikrotikBrasil]
Routers & Wireless Systems

Interface Wireless / Geral / Scan

Scan <wlan1> (running)

Address	SSID	Band	Frequ...	Signal Strength	Radio Name
AB 00:02:2D:75:4A:2F	Wireless	2.4GHz-G	2412	-84	
AB 00:02:6F:35:3A:44	Centaur	2.4GHz-G	2462	-84	
AB 00:02:78:E5:4C:D2		2.4GHz-G	2437	-81	
B 00:05:9E:82:CA:C5	TOPYNET	2.4GHz-G	2457	-88	
ABP 00:17:9A:63:B8:19	atio	2.4GHz-G	2437	-84	
AB 00:40:F4:D5:1F:4C	default	2.4GHz-G	2437	-87	

OK Cancel Apply Disable Comment Scan... Freq. Usage... Align... Sniff... Snooper... Start Stop Close Connect

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

71

[MikrotikBrasil]
Routers & Wireless Systems

Interface Wireless / Geral / Uso de frequencias

Frequency Usage <wlan1> (running)

Frequency	Usage
2412MHz	8.2
2417MHz	5.1
2422MHz	0.6
2427MHz	0.0
2432MHz	0.5
2437MHz	4.6
2442MHz	1.5
2447MHz	0.0
2452MHz	0.0
2457MHz	1.2
2462MHz	7.5
2467MHz	0.8
2472MHz	0.8

OK Cancel Apply Disable Comment Scan... Freq. Usage... Align... Sniff... Snooper... Start Stop Close

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

72

Wireless Alignment Settings

Frame Size: 600
 Active Mode
 Receive All
Filter MAC Address: 00:40:F4:D5:1F:4C
 SSID All
Frames per Second: 25
Audio Monitor: 00:40:F4:D5:1F:4C
Audio Min: -100
Audio Max: 20

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 Tx – tempo em segundos do último pacote transmitido

Correct – número de pacotes recebidos sem erro

OBS: Filtrar MAC do PtP

73

Time	Interfa	Band	Frequ	Signal	Rate	Det	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...	-55dBm	11Mbps	00:40:F4:D5:1F:4C	00:02:D0:0C:AE:55	data
1.155s	wlan1	2.4GHz-G	2437...	-55dBm	2Mbps	00:40:F4:D5:1F:4C	00:02:D0:0C:AE:55	data null
1.156s	wlan1	2.4GHz-G	2437...	-60dBm	2Mbps	00:40:F4:D5:1F:4C	00:02:D0:0C:AE:55	data null
1.159s	wlan1	2.4GHz-G	2437...	-55dBm	2Mbps	00:40:F4:D5:1F:4C	00:02:D0:0C:AE:55	data null
1.164s	wlan1	2.4GHz-G	2437...	-55dBm	2Mbps	00:40:F4:D5:1F:4C	00:02:D0:0C:AE:55	data null
1.188s	wlan1	2.4GHz-G	2437...	-53dBm	2Mbps	FF:FF:FF:FF:FF:FF	00:02:D0:0C:AE:55	probe request
1.209s	wlan1	2.4GHz-G	2437...	-62dBm	2Mbps	FF:FF:FF:FF:FF:FF	00:02:D0:0C: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:D0:0C:AE:55	probe request
1.256s	wlan1	2.4GHz-G	2442...	-55dBm	2Mbps	FF:FF:FF:FF:FF:FF	00:02:D0:0C:AE:55	probe request
1.263s	wlan1	2.4GHz-G	2442...	-64dBm	2Mbps	00:40:F4:D5:1F:4C	00:02:D0:0C: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	00:02:70:E2:22:98	00:02:6F:35:3A:44	data
2.193s	wlan1	2.4GHz-G	2462...	-85dBm	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 sniff wlan1

74

APOSTILA DO CURSO MIKROTIK BRASIL EM 2007

[MikrotikBrasil]
Routers & Wireless Systems

Interface Wireless / Geral / Snooper

Frequency	Address	SSID	Of Freq (%)	Of Traf. (%)	Bandwidth	Net	Stations
2.4GHz-B/G	00:02:D7:5A:2F	Wireless	11.9	97.7	926.4 kbps	1	3
2.4GHz-B/G	00:40:F4:D5:1F:4C						
2.4GHz-B/G	00:02:D0:53:91:98	Wireless	4.9	0.0	306.2 kbps	5	
2.4GHz-B/G	00:02:D0:53:91:98	Wireless	85.0	0.0	0 bps		
2.4GHz-B/G	00:02:78:E1:D0:65	Wireless	85.2	2.2	84.4 kbps		
2.4GHz-B/G	00:02:78:E1:D0:65	Wireless	88.0	2.2	2.8 kbps		
2.4GHz-B/G	00:02:78:E1:D0:65	Wireless	84.2	2.3	216.2 kbps		
2.4GHz-B/G	00:02:62:09:20:33	Wireless	85.0	2.2	2.8 kbps		
2.4GHz-B/G	00:02:6F:35:94:E7	Wireless	86.0	0.3	21.2		
2.4GHz-B/G	00:02:6F:35:94:E7	default	2.0	85.4	81.3 kbps	3	
2.4GHz-B/G	00:02:2D:0C:AE:55	default	58.0	17.4	12.1 kbps		
2.4GHz-B/G	00:11:F5:03:22:86	default	35.0	0.0	0 bps		
2.4GHz-B/G	00:40:F4:D5:1F:4C	default	52.1	68.0	69.2 kbps		
2.4GHz-B/G	00:4F:62:05:9E:B9	TOPYNET	87.0	0.0	0 bps		
2.4GHz-B/G	00:05:9E:82:CA:C5	TOPYNET	0.7	53.3	5.4 kbps	1	
2.4GHz-B/G	00:05:9E:82:CA:C5	TOPYNET	94.0	0.7	5.4 kbps		
2.4GHz-B/G	00:02:6F:35:3A:44	Centaur	0.4	18.5	4.6 kbps		

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

Escaneia as frequências definidas em scan-list da interface

75

[MikrotikBrasil]
Routers & Wireless Systems

Interface Wireless / Wireless

Radio Name: apelido qualquer para a interface Wireless

Mode: modo de operação
 -station: modo cliente de AP. Não pode ser “bridgeado”. Não passa os MAC's internos, mas somente o seu.
 -station wds: estação que pode ser “bridgeada”, passando transparentemente os MAC's AP precisa estar em WDS
 -ap-bridge: Modo Access Point normal
 -modo ponto de acesso para suportar um cliente somente (Links Ponto a Ponto)
 -alignment-only: modo para alinhar antenas e monitorar sinal.
 -nstream-dual-slave: Para enlaces em modo nstream dual
 -wds-slave: trabalha como ponto de acesso escravo, adaptando-se a um WDS mestre (adapta-se às configurações da mestre)

SSID: Nome de Rede

Band: Banda e modo de operação
 -2.4GHz-b: 802.11b até 11 mbps
 -2.4GHz-b/g: 802.11b até 11mbps e 802.11g até 54 mbps (modo misto)
 -2.4GHz-only-g: 802.11g até 54mbps (somente clientes g)
 -2.4GHz-g-turbo: modo proprietário Atheros até 108mbps
 -5GHz: 802.11a até 54mbps
 -5GHz-turbo: Modo proprietário Atheros até 108mbps
 -2.GHz-10MHz: Modo “cloacking”, utiliza cana de 10 MHZ
 -2.GHz-5MHz: Modo “cloacking”, utiliza cana de 5 MHZ
 -5.GHz-10MHz: Modo “cloacking”, utiliza cana de 10 MHZ
 -5.GHz-10MHz: Modo “cloacking”, utiliza cana de 5 MHZ

76

Reprodução não autorizada

[MikrotikBrasil]
Routers & Wireless Systems

Uso Correto dos Canais em 900 Mhz

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)

77

[MikrotikBrasil]
Routers & Wireless Systems

Interface Wireless / Wireless

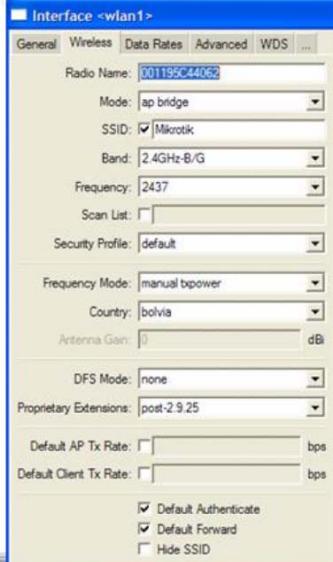
Frequency: Frequencia de trabalho em função da banda escolhida e do domínio regulatório

Scan List: lista de frequencias a serem escaneadas
- Quando a interface está configurada como cliente, serão “procuradas” AP’s que estiverem nessa lista.
- Por default serão buscadas as frequencias do domínio regulatório.
- Pode-se forçar o escaneamento de frequencias específicas, colocando-as separadas por vírgula.

Security Profile: perfil de segurança
- Perfil de segurança podem ser criados/alterados em Wireless/security profiles

Frequency Mode:
- regulatory domain: somente são permitidas o uso das frequencias do país indicado no campo Country, sendo que a potencia máxima de transmissão EIRP será limitada de acordo com a legislação, considerando-se o Ganhos de antena indicado no campo Antenna Gain
- manual-tx-power: os canais permitidos são os do país selecionado mas a potencia é informada pelo operador.
- superchannel: somente possível com a licença superchannel. Todos os canais e potencias suportados pelo hardware serão permitidos

78



Interface Wireless / Wireless

Country: País de operação

Antenna Gain: Ganho da antena em dB

DFS Mode: modo se seleção dinâmica de frequência.

- none: Não usa DFS
- no-radar-detect: O AP escaneia os canais da "scan-list" e escolhe para operar na menor frequência detectada
- radar-detect: O AP escaneia a partir da "scan-list" e escolhe a menor frequência detectada. Se durante 60 segundos não é detectado nesse canal ela começa a operar nesse canal, caso contrário continua escaneando sempre pelos canais menos ocupados.
- OBS: No Brasil é necessário DFS para operar de 5250-5350 e 5470-5725 e existem valores mínimos em dBm que, se detectados não é permitida a operação nesses canais (art. 50 da resolução 365/2004 da Anatel)

Proprietary extensions: Método para inserir informações adicionais (proprietárias MikroTik) nos pacotes Wireless a fim de contornar problemas de compatibilidade com versões antigas (antes da 2.9.25) com novos cartões Intel - Centrino

- pre-2.9.25: Inclui extensões na forma aceita por versões mais antigas do RouterOS. Incompatível com clientes Centrino
- post-2.9.25: Extensões aceitas a partir dessa versão e compatível com todos os clientes conhecidos até o momento.

79

Interface Wireless / Wireless

Default AP Tx Rate: Estabelece a taxa máxima, em bps, que cada cliente pode ter de download

Default Client TX Rate: Estabelece a taxa máxima, em bps, que cada cliente pode enviar ao AP – só funciona para cliente também MikroTik.

Default Authenticate: (default-authentication) Especifica a ação padrão a ser adotada pela AP para os clientes Wireless que não estejam declarados na access list (controle de MAC). Para os equipamentos configurados como clientes, especifica a ação a ser adotada para os AP's que não estejam na Connect List.

- yes: Como AP, deixa o cliente se associar, mesmo se não estiver declarado nas access list. Como cliente, associa-se a qualquer AP, mesmo que não esteja na connect list

Default Forward: (default-forwarding) Determina se poderá haver comunicação entre clientes conectados na mesma interface Wireless. Esse bloqueio é feito na camada 2 de enlace e portanto independente de IP. (algumas AP's tem esse recurso como IntraBSS relay)

- yes (marcado): permite a comunicação
- No (desmarcado) não permite a comunicação.

OBS: Quando as interfaces estão em Bridge, pode haver comunicação entre clientes de interfaces diferentes, mesmo com esse recurso habilitado.

Hide SSID: Determina se o AP vai divulgar o nome da Rede em broadcast através de "beacons"

- yes (marcado): não divulga, somente respondendo aos clientes que enviarem os "probe requests"
- no (desmarcado): divulga o nome da rede.

80

[MikrotikBrasil]
Routers & Wireless Systems

Interface Wireless / Data Rates

Nesta Tela é possível configurar as Taxas de transmissão Suportadas e as taxas Básicas, sendo que:

Taxas Suportadas:
São todas as taxas que o cartão que está sendo configurado suporta.

Taxas Básicas:
São as taxas mínimas suportadas por todos os dispositivos Wireless presentes na rede.

OBS: recomenda-se deixar sempre as taxas básicas no mínimo (1mbps)

81

[MikrotikBrasil]
Routers & Wireless Systems

Interface Wireless / Advanced

Area: String alfanumérica utilizada para descrever um Access Point. O clientes compararam esse valor com o que estiver configurado em sua Area Prefix e se a string toda ou pelo menos os primeiros caracteres coincidirem é estabelecida a associação.

Max Station Count: Número máximo de estações que podem se conectar no AP. Limite teórico de 2007.

Ack Timeout: Tempo de expiração (timeout) do pacote de confirmação de recebimento (acknowledgment) enviado por uma estação
 - dynamic: ajuste dinâmico. O roteador manda pacotes variáveis e em função da resposta procura ajustar ao timeout ideal
 - indoors: para redes indoor.
 - pode ser ajustado manualmente (valor inteiro em microsegundos) digitando-se diretamente na interface.

Noise Floor Threshold: Piso de ruído do ambiente (em dBm).

82

APOSTILA DO CURSO MIKROTIK BRASIL EM 2007

[MikrotikBrasil]
Routers & Wireless Systems

Valores sugeridos de 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	-	-

Chipset version	5ghz		5ghz-turbo		2ghz-b		2ghz-g	
	default	max	default	max	default	max	default	max
5000 (5.2GHz only)	30	204	22	102	N/A	N/A	N/A	N/A
5211 (802.11a/b)	30	409	22	204	109	409	N/A	N/A
5212 (802.11a/b/g)	25	409	22	204	30	409	52	409

OBS: Esses valores são meramente referenciais e devem ser ajustados em função do hardware empregado e do ambiente

83

[MikrotikBrasil]
Routers & Wireless Systems

Interface Wireless / Advanced

Periodic Calibration: Para assegurar a performance do chipsets sob diversas condições de temperatura ambiente o Mikrotik faz calibrações periódicas.

Calibration Interval: Intervalo em segundos entre as calibrações periódicas. Default = 60 segundos.

Burst Time: Tempo em micro segundos que o cartão wireless pode transmitir continuamente. Essa opção só é válida para chipsets Atheros AR5000, AR5001X e AR5001X+. A variável de leitura burst-support, acessível via terminal mostra a capacidade ou não do suporte a essa opção

Antena Mode: Permite a escolha da antena.
 - antena a/b: escolhe uma das antenas a ou b

Preamble Mode: Escolhe o modo do Preamble (comunicação inicial e de sincronização)
 - long: Padrão compatível com 802.11 em geral (mais抗igo -128 bits)
 - short: Padrão suportado por alguns cartões mais modernos, porém não compatível com 802.11. Utilizando short -56 bits, há aumento (pequeno) de performance.
 - both: ambos são suportados

84

Reprodução não autorizada

[MikrotikBrasil]
Routers & Wireless Systems

Interface Wireless / Advanced

Compression: Quando habilitada a compressão (em modo AP-bridge ou bridge), permite que um cliente que tenha a mesma capacidade de compressão habilitada comunique-se com a AP comprimindo os dados (compressão de hardware) melhorando a performance. Esta ação não afeta clientes que não tenham capacidades de compressão.

- A capacidade ou não de compressão de um dispositivo wireless pode ser vista em /interface wireless info print.

Disconnect Timeout: Valor em segundos acima do qual um cliente é considerado desconectado.
Default = 3 segundos.

On Fail Retry Time: Intervalo de Tempo após o qual é repetida a comunicação para um dispositivo Wireless cuja comunicação tenha falhado.
Default = 100 ms

Update Stats Interval: Periodicidade de atualização das estatísticas da interface.
Default = 10 s

85

[MikrotikBrasil]
Routers & Wireless Systems

Interface Wireless / WDS

WDS Mode:

Modo de operação em WDS. Neste modo de operação todos os AP's tem de estar configuradas com o mesmo nome de rede e utilizando o mesmo canal. Além da comunicação entre AP's, o WDS permite que se conectem em qualquer das AP's estações Wireless.

- disabled: WDS desabilitado
- static: As estações WDS ficam atreladas umas às outras de forma estática, com cada uma referenciando o MAC de sua parceira.
- dynamic: Uma vez estabelecido o enlace, a rede WDS é criada automática e dinamicamente.

- Quando em modo dinâmico um dispositivo perde o link, a interface dinâmica desaparece e se há algum endereço IP configurado nessa interface, o estado desta é mudado para "unknown". Quando o link volta esse estado não muda permanecendo "unknown". Por isso não se aconselha a colocar IPs em interfaces WDS dinâmicas. Ao invés disso, utilize a default Bridge para permitir que quando o link volte a interface seja colocada automaticamente na Bridge.

- Tendo em vista que WDS pressupõe mesmo canal em todos AP's, fica incompatível o uso de DFS.

86

[MikrotikBrasil]
Routers & Wireless Systems

Interface Wireless / WDS

WDS Default Bridge: Uma vez criada uma Bridge em /interface bridge add as AP's configuradas em WDS podem fazer parte desta, bastando indicar neste combo. Para WDS dinâmico é recomendável que todas as interfaces estejam sobre a mesma Bridge.

WDS Default Cost: No caso de redes malhadas (Mesh) feitas com WDS pode-se definir custos diferentes para diversos trajetos, dando preferências a determinadas rotas de forma manual.

WDS Cost Range: Indicação da faixa de custos que serão empregados na rede mesh.

WDS Ignore SSID: Uma vez habilitada essa opção, as AP's irão criar links com qualquer outra AP que esteja configurada na mesma frequência, independentemente do SSID configurado nas mesmas.
Default = no.

87

[MikrotikBrasil]
Routers & Wireless Systems

Interface Wireless / Nstreme

Nstreme
Nstreme é um protocolo proprietário (não 802.11) MikroTik que tem por objetivo estabelecer links de performance melhorada quando comparado ao padrão Wi-Fi Normal. Desenhado principalmente a links ponto a ponto mas podendo também ser utilizado em ambientes multiponto, desde que todos os clientes também tenham nstreme habilitado (obviamente todos mikrotik)

Enable Polling: No modo Polling as transmissões das estações são coordenadas pelo AP evitando as colisões por nó escondido. Não é utilizando o método CSMA/CA comum das redes Wi-Fi.

Framer Policy: Método utilizado para combinar pacotes em um quadro maior e com isso diminuir o overhead da comunicação, aumentando consequentemente a performance

- none: não combina os pacotes
- best-fit: coloca o maior número de pacotes possíveis em um frame, até que o limite estabelecido em framer-limit seja atingido. Não fragmenta pacotes.
- exact-size: põe quantos pacotes for possível em um quadro, até que o limite estabelecido em framer-limit seja atingido, mesmo que seja necessário fragmentar
- dynamic-size: escolhe o melhor tamanho do quadro dinamicamente.

Framer Limit: Tamanho máximo do quadro. Default = 3200 bytes

88

Tx Power:
Interface utilizada para configurar a potencia de transmissão – valores de -30 dBm a 30 dBm, default = 17 dBm.

- all-rates-fixed: utiliza a mesma potencia configurada em Tx Power para todas as velocidades.
- card-rates: utiliza as velocidades próprias dos firmware dos cartões.
- default: utiliza a potencia default (17 dBm)
- manual-table: permite a configuração de diversas potencias em função da taxa de trasnmissão.

OBS:
A possibilidade de alterar a potencia do cartão normalmente é utilizada para diminuir a potencia nominal do mesmo e não aumenta-la.

WDS Cost Range: Indicação da faixa de custos que serão empregados na rede mesh.

WDS Ignore SSID: Uma vez habilitada essa opção, as AP's irão criar links com qualquer outra AP que esteja configurada na mesma frequencia, independentemente do SSID configurado nas mesmas.
Default = no.

89

Status: Mostra informações sobre o status do AP

Band: Frequencia e modo de operação

Frequencia: Canal utilizado

Registered Clients: Clientes registrados

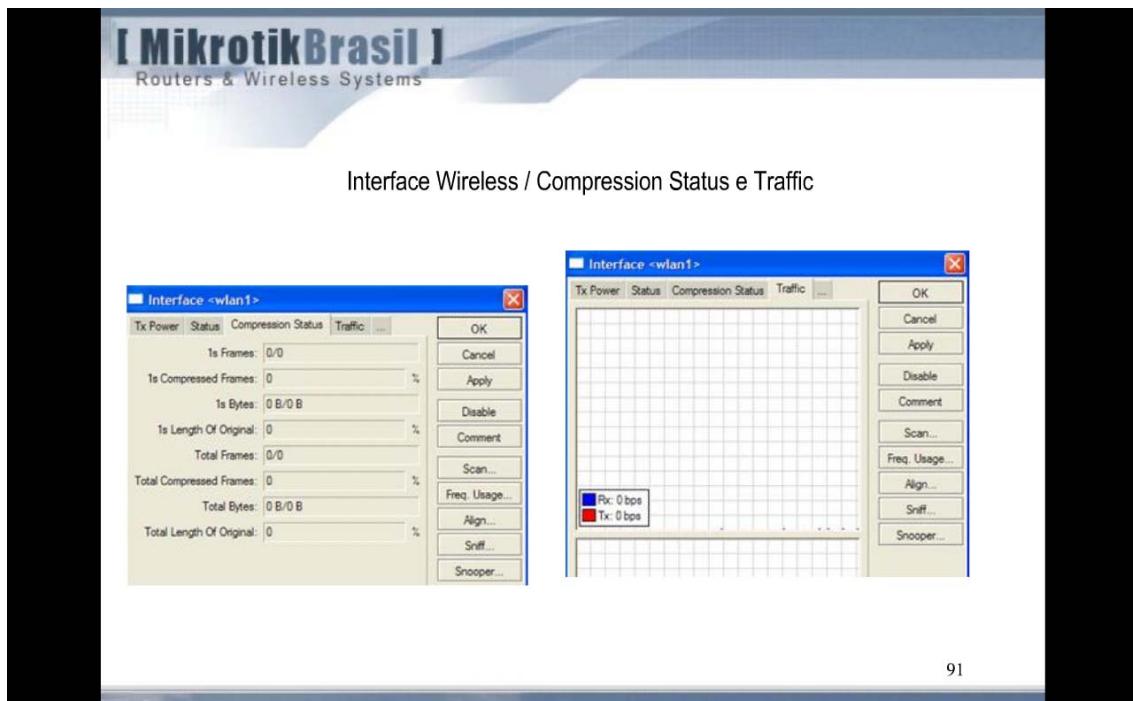
Authenticated Clients: Clientes autenticados

Overall Tx CCQ: Valor em porcentagem que mostra a eficiencia da Banda de transmissão em relação à máxima banda teórica disponível no link. Esse valor é calculado com base nos pacotes Wireless que são retransmitidos no meio físico. Quanto mais retransmissões, menor a eficiencia.

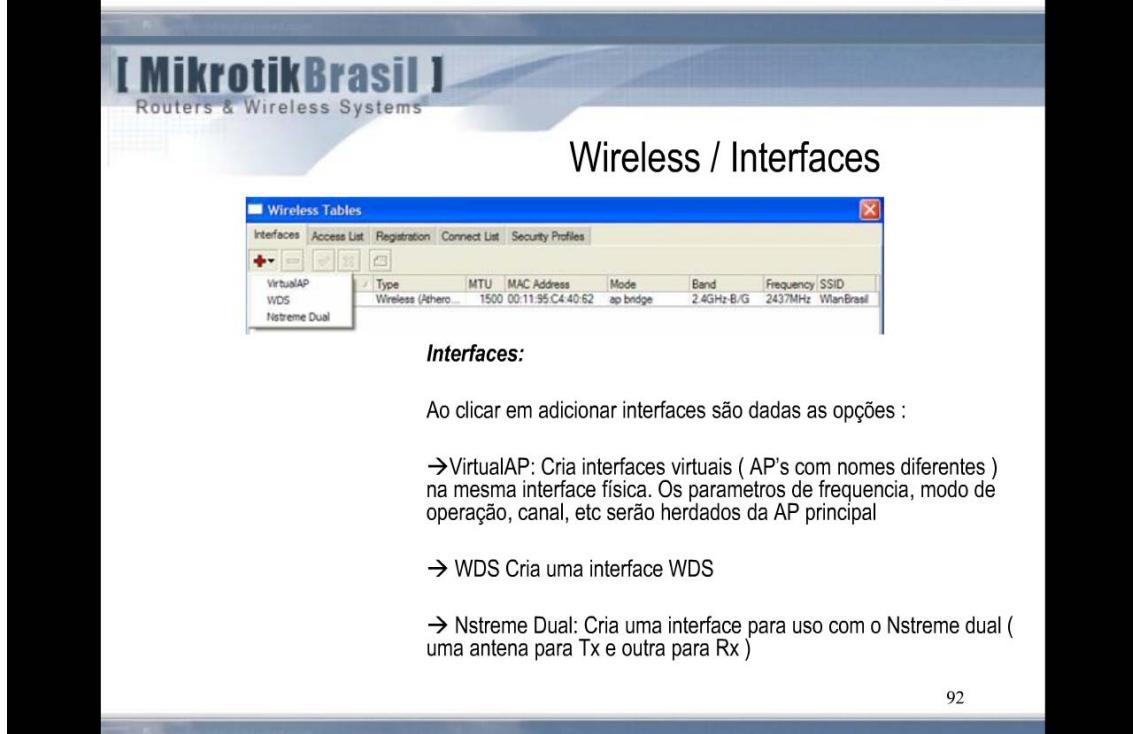
Ack Timeout: tempo de expiração do ACK em microsegundos

Noise Floor: Piso de ruído em dBm

90



91



92

Reprodução não autorizada

[MikrotikBrasil]
Routers & Wireless Systems

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

93

[MikrotikBrasil]
Routers & Wireless Systems

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.

94

NStreme dual é um protocolo proprietário Mikrotik em que se usa duas antenas, sendo uma para Transmissão e outra para Recepção.

→ Tx/Rx Radio: especifica-se as interfaces de Tx e Rx

→ Tx/Rx Banda e Frequências: especifica-se as Bandas de Tx e Rx que podem inclusive ser de frequências diferentes (ex. 2.4 para Tx e 5.7 para Rx)

→ Framer Policy:

- best-fit: pacotes são agrupados em frames, sem fragmentação
- exact-size: pacotes são agrupados em frames, com fragmentação se necessário

Com NStreme dual é possível escolher as velocidades de transmissão e recepção e ainda monitorar o status das conexões

[MikrotikBrasil]
Routers & Wireless Systems

Wireless Tables / Access List

MAC Address	Interface	Authentication	Forwarding	Private Key
00:11:11:11:11:11	wlan1	yes	yes	112233445566

O Access List é utilizado pelo Access Point para restringir associações de clientes. Esta lista contém 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 access 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..

97

[MikrotikBrasil]
Routers & Wireless Systems

Wireless Tables / Access List

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: Habilitado permite a comunicação entre clientes habilitados (intra bss)

98

[MikrotikBrasil]
Routers & Wireless Systems

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 área

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)

99

[MikrotikBrasil]
Routers & Wireless Systems

Wireless Tables / Security Profiles

Na tabelas **Security Profiles** são definidos os perfis de segurança da parte Wireless que podem ser utilizados no RouterOS

Name: nome que aparecerá em outras telas, referenciando esse perfil

Mode: Modo de operação

- dynamic keys: gera chaves dinâmicas automaticamente
- static-keys-required: criptografa todos os pacotes e somente aceita pacotes criptografados
- static-keys-optional: se existe uma chave privada estática de estação (static-sta-private-key), esta será utilizada. Caso contrário, estando a estação no modo AP, não será utilizada criptografia e em modo estação usará se estiver setada a static-transmit-key

[MikrotikBrasil]
Routers & Wireless Systems

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

101

[MikrotikBrasil]
Routers & Wireless Systems

Wireless Tables / Security Profiles

Wireless Tables

Interfaces | Access List | Registration | Connect List | Security Profiles

Name	Mode	Auth. Mode	Unicast Ciphers	Group Ciphers	WPA Pre-Shared ...	WPA2 Pre-S...
default	none					

Authentication Types:

WPA: Método não padrão IEEE utilizado durante algum tempo pela indústria para evitar problemas do WEP

WPA2: Método compatível com 802.11i do IEEE.

PSK: Pré Shared Key – Chave compartilhada entre dois dispositivos.

EAP: Extensive Authentication Protocol

OBS: O AP irá divulgar todos os modos de autenticação marcados aqui e as estações escolherão o método considerado mais seguro. Exemplo, WPA EAP ao invés de WPA PSK.

New Security Profile

General	EAP	Static Keys
Name: profile1	Mode: dynamic keys	
<input checked="" type="checkbox"/> WPA PSK	<input checked="" type="checkbox"/> WPA2 PSK	
<input type="checkbox"/> WPA EAP	<input type="checkbox"/> WPA2 EAP	
<input checked="" type="checkbox"/> skip	<input type="checkbox"/> aes ccm	
<input checked="" type="checkbox"/> skip	<input type="checkbox"/> aes ccm	
WPA Pre-Shared Key:		
WPA2 Pre-Shared Key:		
Group Key Update:	00:05:00	
<input type="checkbox"/> RADIUS MAC Authentication		

APOSTILA DO CURSO MIKROTIK BRASIL EM 2007

The screenshot shows the MikroTik Wireless Tables / Security Profiles interface. On the left, there is a list of security profiles: default (Mode: none). On the right, two windows are displayed: a 'New Security Profile' dialog and a 'New Security Profile' dialog for the EAP tab.

General Tab (Left):

- Name: profile1
- Mode: dynamic keys
- Authentication Types:
 - WPA PSK (checked)
 - WPA EAP (unchecked)
 - WPA2 PSK (checked)
 - WPA2 EAP (unchecked)
- Unicast Ciphers:
 - tkip (checked)
 - aes ccm (unchecked)
- Group Ciphers:
 - tkip (checked)
 - aes ccm (unchecked)
- WPA Pre-Shared Key: [empty field]
- WPA2 Pre-Shared Key: [empty field]
- Group Key Update: 00:05:00
- RADIUS MAC Authentication: [unchecked]

EAP Tab (Right):

- EAP Methods: passthrough (selected)
- EPA-TLS (disabled)
- TLS Mode: verify certificate (selected)
- TLS Certificate: none

Reprodução não autorizada

The screenshot shows the MikroTik configuration interface. At the top, there's a banner for 'MikrotikBrasil Routers & Wireless Systems'. Below it, a window titled 'Wireless Tables / Security Profiles / Static Keys' is open. This window has tabs for 'Wireless Tables' (selected), 'Interfaces', 'Access List', 'Registration', 'Connect List', and 'Security Profiles'. Under 'Wireless Tables', there's a table with columns: Name, Mode, Auth. Mode, Unicast Ciphers, Group Ciphers, WPA Pre-Shared Key, and WPA2 Pre-Shared Key. One row is visible: 'default' with 'Mode: none'. A second window, 'Security Profile <profile1>', is also open. It has tabs for 'General' (selected) and 'EAP'. Under 'General', there are fields for 'Key 0' through 'Key 3', each set to 'none' with a hex value '0x'. There's also a 'Transmit Key:' dropdown set to 'key 0' and a 'St. Private Key:' dropdown set to 'none'. On the right side of this window are buttons for 'OK', 'Cancel', 'Apply', 'Copy', and 'Remove'. The number '105' is displayed at the bottom right of the interface.

Dúvidas ??

106

[MikrotikBrasil]
Routers & Wireless Systems

Bonding

Bonding é uma técnica que permite agrregar múltiplas interfaces ethernet ou “ethernet-like” em um link virtual único, possibilitando assim aumento do throughput e ainda contingenciamento.

The diagram shows two routers, R1 and R2, connected via their respective wlan1 and wlan2 interfaces. These interfaces are bonded together to form a single tunnel interface (loop-tunnel1 and loop-tunnel2) with tunnel-id 1 and 2 respectively. The configuration for bonding1 on R1 is as follows:

```
bonding1:
  slaves: 192.168.0.1/24,loop-tunnel1,loop-tunnel2
  mode: balance-rr
  link-monitoring: arp
  arp-ip-targets: 192.168.0.2
```

The configuration for bonding1 on R2 is as follows:

```
bonding1:
  slaves: 192.168.0.2/24,loop-tunnel1,loop-tunnel2
  mode: balance-rr
  link-monitoring: arp
  arp-ip-targets: 192.168.0.1
```

107

[MikrotikBrasil]
Routers & Wireless Systems

Bonding

- active-backup - provides link backup. Only one slave can be active at a time. Another slave becomes active only, if first one fails.
- balance-alb - adaptive load balancing. It includes balance-tlb and received traffic is also balanced. Device driver should support for setting the mac address, then it is active. Otherwise balance-alb doesn't work. No special switch is required.
- balance-rr - round-robin load balancing. Slaves in bonding interface will transmit and receive data in sequential order. Provides load balancing and fault tolerance.

108

Bonding

- balance-tlb - Outgoing traffic is distributed according to the current load on each slave. Incoming traffic is received by the current slave. If receiving slave fails, then another slave takes the MAC address of the failed slave. Doesn't require any special switch support.
- balance-xor - Use XOR policy for transmit. Provides only failover (in very good quality), but not load balancing, yet.
- broadcast - Broadcasts the same data on all interfaces at once. This provides fault tolerance but slows down traffic throughput on some slow machines.

109

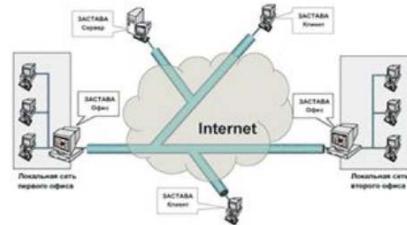
Túneis & VPN's com Mikrotik



[MikrotikBrasil] Routers & Wireless Systems

VPN's

As principais funções das VPN's são:



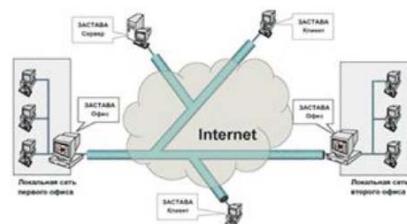
- Promover acesso seguro sobre meios físicos públicos como a Internet por exemplo
- Promover acesso seguro sobre linhas dedicadas, wireless, etc.
- Promover acesso seguro a serviços em ambiente corporativo de Correio, impressoras, etc
- Fazer com que o usuário na prática se torne parte da rede corporativa 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.

111

[MikrotikBrasil] Routers & Wireless Systems

Tunelamento



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

112

[MikrotikBrasil]
Routers & Wireless Systems

Algumas definições comuns para os serviços PPP

-MTU/MRU: tamanhos máximos dos pacotes de transmissão/Recepção em bytes. Normalmente a ethernet permite 1500 bytes. Em serviços PPP que precisam encapsular os pacotes, deve se definir valores menores para que não haja fragmanetação.

- 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: o par usuário/senha passa em texto plano, sem autenticação
- Chap: usuário/senha com criptografia
- mschap1: versão chap da Microsoft conf. RFC 2433
- mschap2: versão chap da Microsoft conf. RFC 2759

113

[MikrotikBrasil]
Routers & Wireless Systems

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

- 1 MSS=16K → Router A
- 2 Router B → MSS=16K
- 3 Set "Send MSS" = 16K
- 4 Router B → MSS=8K
- 5 Router B → Host A
- 6 Set "Send MSS" = 8K

O exemplo abaixo demonstra como baixar o MSS via MANGLE do Firewall:

```
[admin@MikroTik] > /ip firewall mangle add out-interface=pppoe-out protocol=tcp tcp-flags=syn action=change-mss new-mss=1300 chain=forward
[admin@MikroTik] > /ip firewall mangle print
Flags: X - disabled, I - invalid, D - dynamic
0 chain=forward out-interface=pppoe-out protocol=tcp tcp-flags=syn
action=change-mss new-mss=1300
```

114

[MikrotikBrasil]
Routers & Wireless Systems



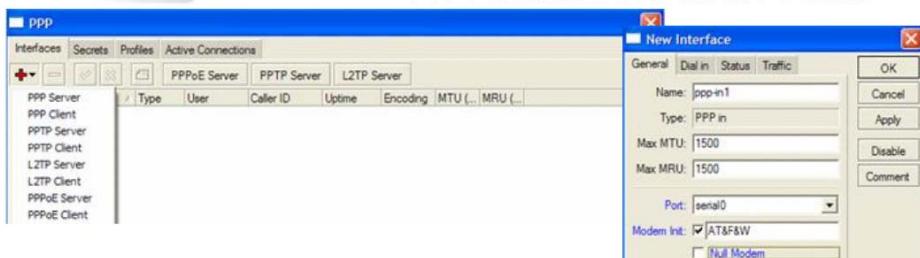
Servidor ou Cliente PPP

O Mikrotik pode ser configurado para ser um servidor PPP, com a opção PPP Server. Clientes remotos (dial up por exemplo) podem ser autenticados no próprio Mikrotik, utilizando a base de dados local em /user ou através de um servidor Radius especificado em /ip ppp

Também é possível configura-lo para discar para um servidor dial up sob demanda tornando-o um Cliente de Dial Up

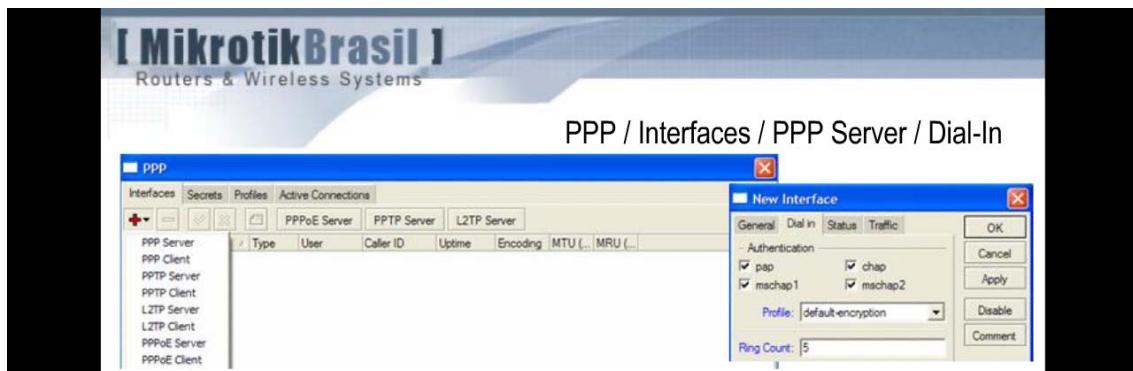
115

PPP / Interfaces / PPP Server / General



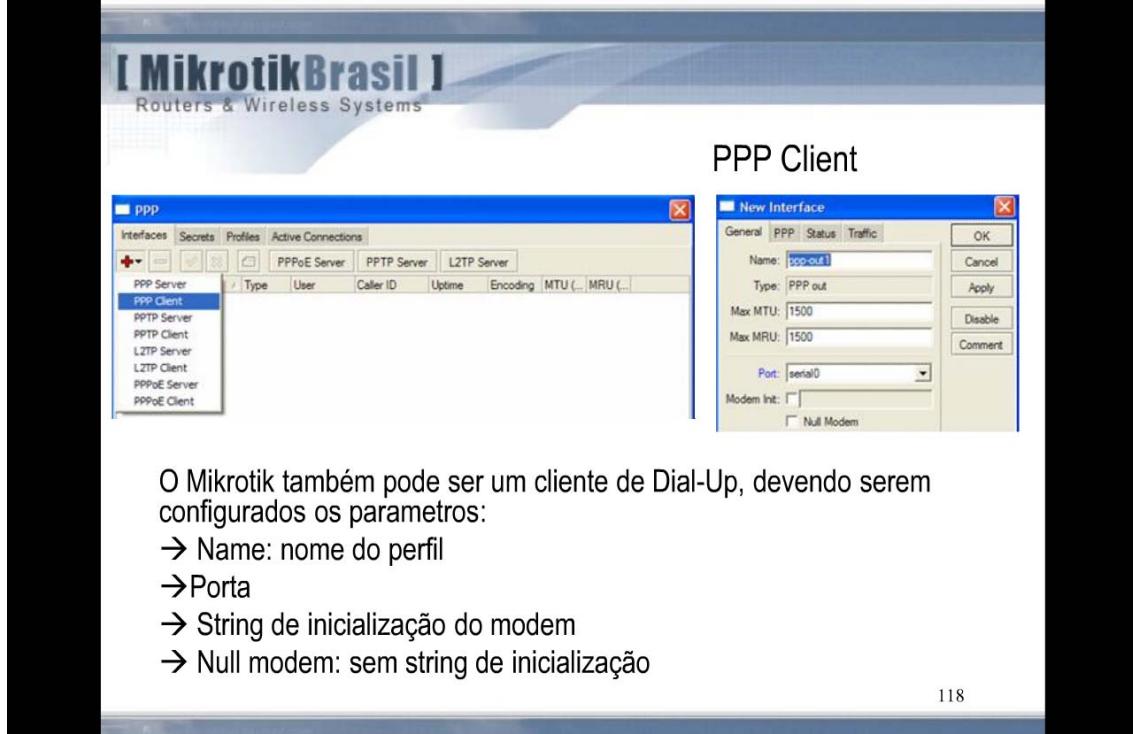
Name: Nome do perfil
→ Port: porta serial
→ Modem Init: string de inicialização a ser passada para um modem
→ Null Modem: não passa strings

116



Profile: escolhe o perfil de segurança definido em /ppp profiles
 Ring Count: número de toques antes do atendimento

117



O Mikrotik também pode ser um cliente de Dial-Up, devendo serem configurados os parametros:

- Name: nome do perfil
- Porta
- String de inicialização do modem
- Null modem: sem string de inicialização

118

Reprodução não autorizada

[MikrotikBrasil]
Routers & Wireless Systems

Configuração do PPP Client

The screenshot shows two windows from the MikroTik Winbox interface. On the left is the 'PPP' window with tabs for Interfaces, Secrets, Profiles, and Active Connections. The 'Interfaces' tab is selected, showing a list of interfaces including PPP Client, PPTP Client, L2TP Client, and PPPoE Client. The 'PPP Client' item is highlighted. On the right is the 'New Interface' dialog for a PPP client, with tabs for General, PPP, Status, and Traffic. The 'General' tab is selected, showing fields for Phone (0211733445000), Dial Command (ATDT), User (wlanbrasil), Password (senha), Profile (default-encryption), and checkboxes for Dial On Demand, Add Default Route, and Use Peer DNS. Below these are 'Allow' checkboxes for pap, chap, mschap1, and mschap2.

Configuração do Dial-out:

- Phone: número a ser discado
- Dial Command: string a ser enviada ao modem local
- User / Password: usuário e senha no servidor remoto
- Profile: perfil de segurança definido em /ppp profiles
- Dial On Demand: discar sempre que algum aplicativo tentar usar saída
- Add Default Route: usa a rota default configurada em / ip rout
- Use Peer DNS: usa os servidores de DNS definidos no servidor remoto.

119

Servidor ou Cliente PPPoE

PPPoE – Point to Point Protocol over Ethernet– Extensão do protocolo PPP, porém sobre o meio físico Ethernet.

- Muito usado para autenticação de clientes com Base em Login e senha
- O Cliente não tem IP configurado que é dado pelo PPPoE Server, normalmente por um servidor Radius
- PPPoE não é criptografado
- O Cliente “descobre” o servidor através de um 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)

120

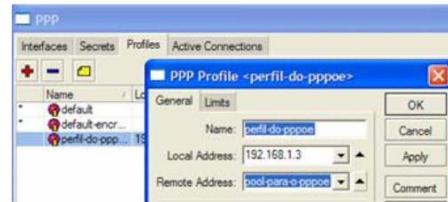
[MikrotikBrasil]
Routers & Wireless Systems

Configuração do Servidor PPPoE

1 – Crie um pool de IP's para o PPPoE
`/ip pool add name=pool-para-o-pppoe ranges=10.0.0.1-10.0.0.100`



2 – Adicione um Perfil de PPPoE onde
 → Local address = endereço Ip do Concentrador
 → Remote address = pool do pppoe
`/ppp profile add name="perfil-do-pppoe" local-address=192.168.1.3 remote-address=pool-para-o-pppoe`



121

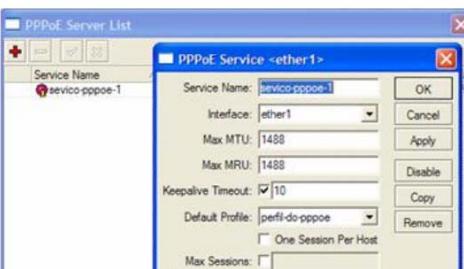
[MikrotikBrasil]
Routers & Wireless Systems

Configuração do Servidor PPPoE

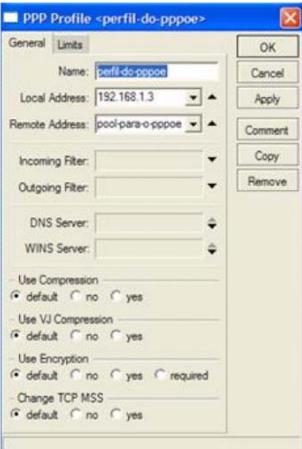
3 – Adicione um usuário e senha
`/ppp secret add name=wlanbrasil password=123 service=servico-pppoe1 profile=perfil-do-pppoe`



4 – Adicione o PPPoE Server
 → Nome do serviço = nome que os clientes vão procurar
`/interface pppoe-server server add service-name=servico-pppoe1 interface=ether1 default-profile=perfil-do-pppoe`



122



Mais sobre Perfis

- Incoming/Outgoing Filter: nome do canal do Firewall para pacotes entrantes/sairantes. O canal ppp deve ser manualmente adicionado e regras com action=jump e jump-target=ppp devem ser adicionadas para que o filtro funcione. Ver Firewall.
- Rate Limit: limitação da velocidade na forma 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]]]. Do ponto de vista do roteador rx é o upload do cliente.
- Use Compression/Encryption/TCPMSS: caso estejam default pegam o que estiver configurado na Interface.

123



Mais sobre o user Database

- Service: Especifica o serviço disponível para esse usuário em particular.
- Caller ID: MAC address do cliente
- Limit Bytes In/Out: Quantidades de Bytes que o cliente pode trafegar por sessão PPPoE
- Routes: Rotas que são criadas no lado do servidor para esse cliente específico. Sintaxe: dst-address gateway metric. Várias rotas podem ser adicionadas separadas por vírgula.

124



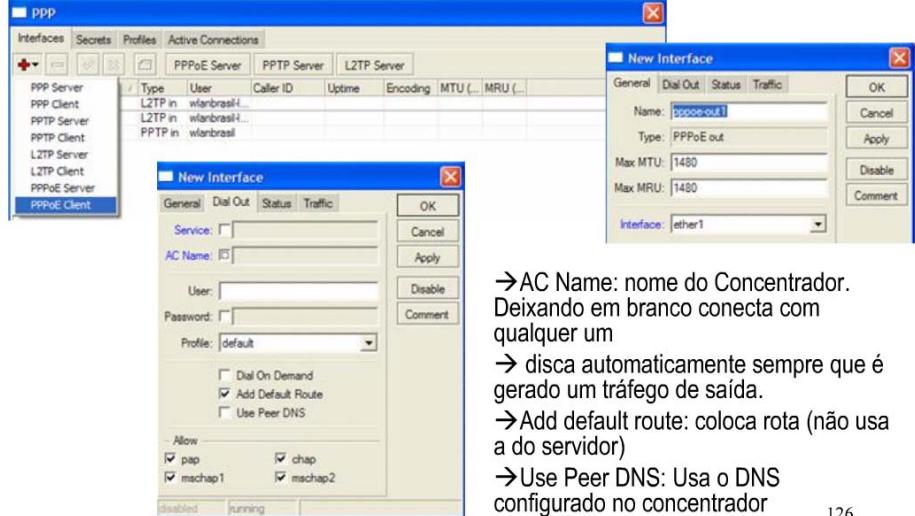
Detalhes adicionais do PPPoE Server

- 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 do acesso = Identidade do roteador (/system identity)
- O valor de MTU/MRU recomendado para o PPPoE é de 1480 bytes

→ One session per Host: somente um conecta com o mesmo usuário/senha (corrigir)

→ Max Sessions: número máximo de sessões por usuário/senha (corrigir)

125



Configuração do PPPoE Client

- AC Name: nome do Concentrador. Deixando em branco conecta com qualquer um
- disca automaticamente sempre que é gerado um tráfego de saída.
- Add default route: coloca rota (não usa a do servidor)
- Use Peer DNS: Usa o DNS configurado no concentrador

126

[MikrotikBrasil]
Routers & Wireless Systems

Segurança no PPPoE

Para assegurar um servidor PPPoE pode-se utilizar Filtros de Bridge, deixando somente passar os protocolos pppoe-discovery e pppoe-session, e descartando todos os outros.

Mesmo que haja somente uma interface, ainda assim é possível utilizar os Filtros de Bridge.

127

[MikrotikBrasil]
Routers & Wireless Systems

Servidor ou Cliente PPtP

PPtP – Point to Point Tunneling Protocol – Protocolo de tunelamento ponto a ponto é um protocolo desenvolvido pela Microsoft que pode ou não ser criptografado e que tem as principais aplicações:

- Formação de túneis seguros entre dois routers pela Internet
- Para linkar de forma transparente Intranets ou LAN's
- Para usuários remotos se logarem no ambiente corporativo da empresa de forma segura mesmo em locais públicos como Hotspots por exemplo.

128

The screenshot shows two windows from the MikroTik Winbox interface:

- Top Window (PPP Secret):** Shows a list of secrets. One entry is selected: "Name: wlan-pptp", "Password: 123", "Service: pptp", "Profile: default".
- Bottom Window (PPTP Server):** Shows settings for the PPTP server. "Enabled" is checked, "Max MTU: 1460", "Max MRU: 1460", "Keepalive Timeout: 30", and "Default Profile: default-encryption".

Configuração do Servidor PPPtP

- 1 – Adicione um usuário

```
/ppp secret add name=wlan-pptp
password=123 local-
address=10.0.0.1
Remote-address=10.0.0.2
```
- 2 – Habilite o PPtP Server

```
/ppp pptp-server server> set
enable=yes
```

Está pronto !

129

The screenshot shows two windows from the MikroTik Winbox interface:

- Top Window (PPP):** Shows a list of services. "PPTP Client" is selected.
- Bottom Window (New Interface):** Shows the configuration for a new PPTP interface. "Name: pptp-out", "Type: PPTP out.", "Max MTU: 1460", and "Max MRU: 1460".
- Bottom Window (New Interface):** Shows the configuration for a new PPTP client interface. "Server Address: 0.0.0.0", "User: ", "Password: ", "Profile: default-encryption", and checkboxes for "Allow: pap, mschap1" and "chap, mschap2".

Configuração do PPtP Client

Adicionando pelo terminal :

```
/ interface pptp-client add user=wlan-
client-pptp password=123 connect-to
200.200.200.200 disabled=no
```

130

*

Reprodução não autorizada

L2TP



L2TP – Layer 2 Tunneling Protocol – Protocolo de tunelamento de camada 2

L2TP 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.

Como exemplo, um usuário conectado em um RAS de uma companhia telefônica pode se conectar ao backbone de um provedor de acesso que lhe atribui banda e endereçamento IP próprio.

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 atrás de NAT.

131

Configuração do L2TP Server

1- Adicionar um usuário L2TP user:
`/ppp secret add name=wlanbrasil-l2tp
password=123 local-address=10.0.0.1
remote-address=10.0.0.2
(pode-se amarrar ip's de origem,
bytes, etc)`

2. Habilitar o servidor L2TP
`/interface l2tp-server server set
enabled=yes`

132

[MikrotikBrasil]
Routers & Wireless Systems

Configuração do L2TP Cliente

Configurar o Mikrotik como Cliente de um servidor L2TP é muito simples conforme mostram as telas ao lado.

Na linha de comando seria :

```
/ interface l2tp-client> add user=wlanbrasil-l2tp  
password=senha connect-to=200.200.200.200
```

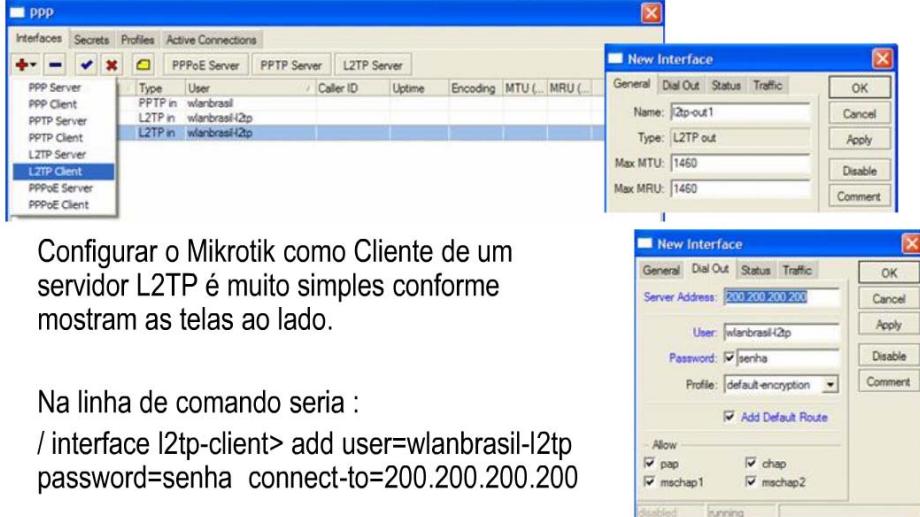
Túneis IPIP

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 routers.

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

Vários Roteadores comerciais, incluindo o Cisco suportam esse protocolo

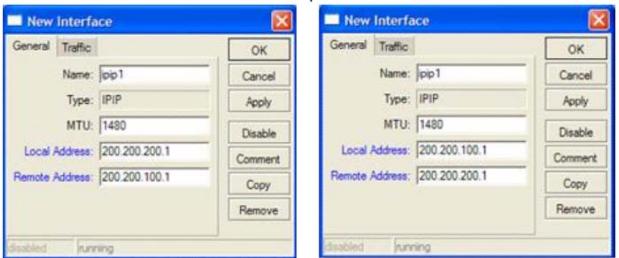
134



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 routers, da seguinte forma:

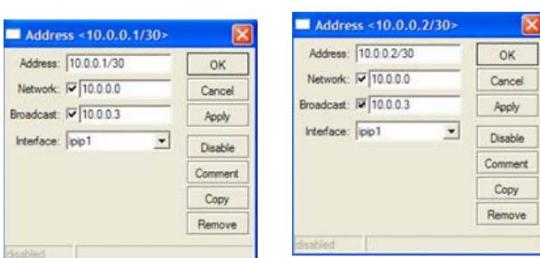


135

Túneis IPIP



Em seguida atribui-se às interfaces criadas IP's (de preferencia ponto a ponto)



Pronto, está criado o Túnel IPIP e agora as redes fazem parte do mesmo domínio de Broadcast.

136

[MikrotikBrasil]

Routers & Wireless Systems

Túneis EoIP

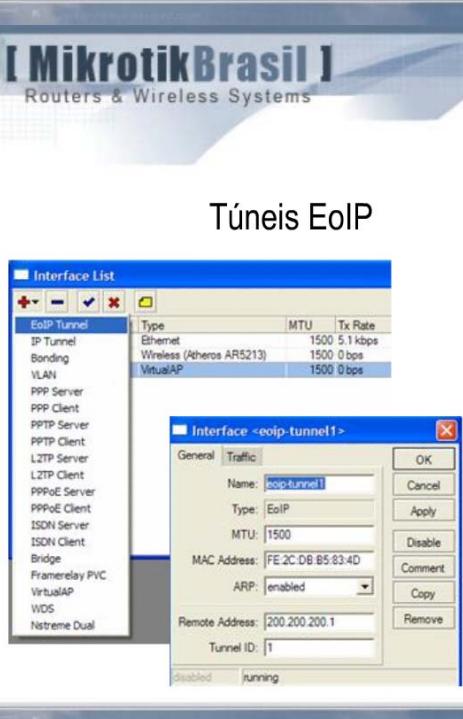


137

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 passando 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 "bridgegear" LAN's sobre redes Ad Hoc 802.11



138

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.

[MikrotikBrasil]
Routers & Wireless Systems

Dúvidas ??

139

[MikrotikBrasil]
Routers & Wireless Systems



Firewall

com Mikrotik



140

Firewall



O Firewall é normalmente 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.

141

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

142

[MikrotikBrasil]
Routers & Wireless Systems

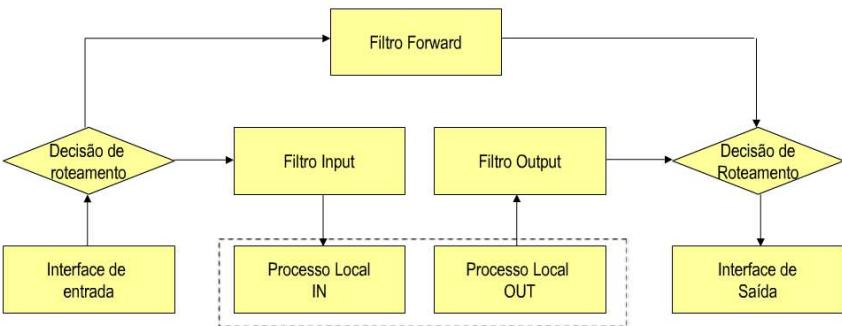


Diagrama da Estrutura de Filtro

O diagrama mostra o fluxo de dados em um roteador MikroTik. Os dados entram pela "Interface de entrada", passam por uma "Decisão de roteamento", e são processados no "Filtro Input". O resultado é dividido entre o "Processo Local IN" (que alimenta o "Filtro Forward") e o "Processo Local OUT" (que alimenta o "Filtro Output"). O "Filtro Forward" alimenta o "Filtro Output". Ambos os filtros alimentam uma segunda "Decisão de Roteamento", que resulta na saída pela "Interface de Saída".

143

[MikrotikBrasil]
Routers & Wireless Systems



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.

144

[MikrotikBrasil]
Routers & Wireless Systems



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 - A excessão ao critério acima pode ser feita quando está disponível a opção "passthrough" (passar adiante)

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

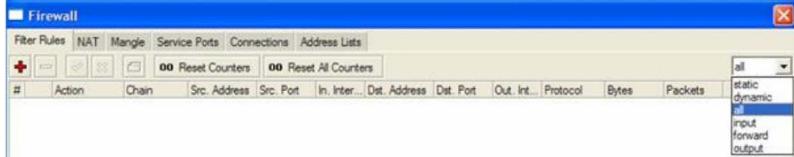
145

[MikrotikBrasil]
Routers & Wireless Systems

Firewall do Mikrotik – Filter Rules

Nesta tela são pode-se visualizar todas as regras que o Firewall está processando.

Basicamente as regras se dividem em estáticas e dinâmicas podem ser visualizadas separadamente. Também podem ser visualizadas em separado os canais input, output e forward.



146

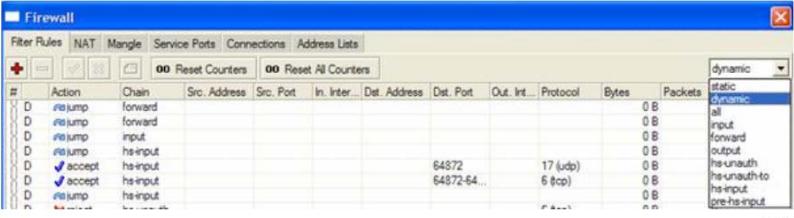
[MikrotikBrasil]
Routers & Wireless Systems

Firewall do Mikrotik – Filter Rules

A medida que são criados ou ativados serviços novos que demandam regras dinâmicas no Firewall, são também criados canais dinâmicos que aparecem na lista de opção de regras de filtros.

No exemplo abaixo aparecem os canais hs-input, hsunauth, referentes à ativação de um Hotspot nesse Router.

Observar que a ordem das regras pode ser alterada para visualização, clicando na opção a ordenar, mas para efeito de processamento a ordem é a que aparece quando clicamos em #



147

[MikrotikBrasil]
Routers & Wireless Systems

Firewall do Mikrotik – Filter Rules

New Firewall Rule

Action	accept
accept	passthrough
drop	reject
reject	tarpit
log	ping
ping	return
return	add src to address list
	add dst to address list

As ações que se pode tomar nas regras de filtro são:

- 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)



148

[MikrotikBrasil]
Routers & Wireless Systems

Firewall do Mikrotik – Filter Rules

As ações que se pode tomar nas regras de filtro são:

→tarpit: captura e segura conexões TCP, respondendo com SYN/ACK ao pacote TCP/SYN entrante.

→return: devolve o controle para o canal original de onde foi feito um salto de jump

→add dst to address list: adiciona o IP de destino a uma Address List

→add src to address list: adiciona o IP de origem a uma Address List

149

[MikrotikBrasil]
Routers & Wireless Systems

Princípios Gerais de Firewall

Canais definidos pelo usuário



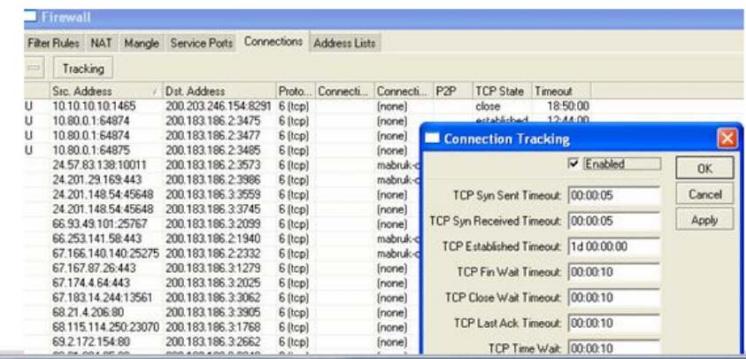
- Canais definidos pelo usuário podem ser adicionados, sendo que nesse caso devem ser feitos direcionamentos para um dos canais, input, output e forward através das regras de action=jump e jump-target
- Podem ser adicionados qualquer número de canais.
- A criação de canais torna a administração e entendimento do Firewall mais fáceis
- Esses canais ajudam a melhorar a performance reduzindo o número de regras processadas por pacote.

150

MikrotikBrasil
Routers & Wireless Systems

Connection Tracking

Connection Tracking (seguimento de conexões) se refere à 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".



151

MikrotikBrasil
Routers & Wireless Systems

Connection Tracking



- O sistema de Connection Tracking ou Conntrack é o coração do Firewall. Ele obtém 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.
- Cada entrada na tabela conntrack representa a troca de dados bidirecional.
- Conntrack é exigente de recursos de hardware. Quando o equipamento trabalha apenas como AP Bridge por exemplo, é indicado desabilitá-la

152

Localização da Conntrack

```

graph TD
    IF[Interface de Entrada] --> FForward[Filtro Forward]
    FForward --> D1{Decisão de roteamento}
    D1 --> FInput[Filtro Input]
    FInput --> Conntrack1[Conntrack]
    Conntrack1 --> D2{Decisão de Roteamento}
    D2 --> FOutput[Filtro Output]
    FOutput --> Conntrack2[Conntrack]
    Conntrack2 --> IFSAIDA[Interface de Saída]
    subgraph ProcessoLocal [Processo Local]
        direction LR
        P1[Processo Local IN] --- P2[Processo Local OUT]
    end
    P1 -.-> FInput
    P2 -.-> FOutput
    
```

153

Connection Tracking

Src. Address	Dest. Address
66.186.196.81:80	192.168.1.3
U 192.168.1.3	200.200.100
U 192.168.1.6:4135	255.255.255
U 192.168.166.249:137	192.168.166
A 192.168.166.249:3630	207.46.109.1
A 192.168.166.251:1136	207.46.109.6

Enabled

TCP Syn Sent Timeout: 00:00:05

TCP Syn Received Timeout: 00:00:05

TCP Established Timeout: 1d 00:00:00

TCP Fin Wait Timeout: 00:00:10

154

[MikrotikBrasil]
Routers & Wireless Systems

Regras de Firewall Proteção do próprio Roteador

Regras no Canal Input

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

The screenshot shows the Winbox Firewall Filter Rules window with the following rules listed:

#	Action	Chain	Src. Address	Src. Port	In. Inter...	Dst. Address	Dst. Port	Out. Int...	Proto...	Bytes	Packets
1	drop	input								0 B	0
2	acc...	input								149 B	1
3	acc...	input								0 B	0
4	acc...	input								0 B	0
5	acc...	input	192.168.100.0/24							32.8 kB	379
6	drop	input								240 B	4

Regras no Canal Input – cont.

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

The screenshot shows the Winbox Firewall Filter Rules window with the following rules listed, including new entries for Winbox, SSH, and Telnet:

#	Action	Chain	Src. Address	Src. Port	In. Inter...	Dst. Address	Dst. Port	Out. Int...	Proto...	Bytes	Packets
1	drop	input								0 B	0
2	acc...	input								149 B	1
3	acc...	input								0 B	0
4	acc...	input	192.168.100.0/24							0 B	0
5	acc...	input	10.10.10.0/24							275.5 kB	3424
6	acc...	input					8291	6 (tcp)	0 B	0	
7	acc...	input					22	6 (tcp)	0 B	0	
8	acc...	input					23	6 (tcp)	0 B	0	
9	drop	input								1629 B	17

[MikrotikBrasil]
Routers & Wireless Systems

Regras de Firewall Proteção do próprio Roteador

Proteções Básicas de um Roteador

Filtros de Firewall não filtram camada de MAC e por isso é necessário desabilitar MAC telnet e MAC Winbox pelo menos na Interface pública.

Deve-se desabilitar o “network discovery” também para que o Roteador não se revele mais (/ip neighbor discovery menu)

157

[MikrotikBrasil]
Routers & Wireless Systems

Regras de Firewall Proteção do próprio Roteador

Proteções Básicas de um Roteador

É importante lembrar ainda que, para a proteção interna de um Roteador é necessário controlar os serviços que estão habilitados neste.

Acesse /ip services e desabilite tudo que não for utilizado.

Name	Port	Available From
ftp	21	0.0.0.0/0
ssh	22	0.0.0.0/0
telnet	23	0.0.0.0/0
www	80	0.0.0.0/0
www-ssl	443	0.0.0.0/0

158

Reprodução não autorizada

[MikrotikBrasil]
Routers & Wireless Systems

Regras de Firewall Proteção da Rede Interna

Regras primeiras no Canal Forward

- Descarta conexões inválidas
- Aceita conexões estabelecidas
- Aceita conexões relacionadas

The screenshot shows the Winbox Firewall interface with the 'Filter Rules' tab selected. It displays a list of rules with their actions, chains, source addresses, destination ports, and statistics. The rules are:

- ... Descarta conexões inválidas (drop input)
- ... Aceita Conexões Estabelecidas (acc... input)
- ... Aceita Conexões Relacionadas (acc... input)
- ... Aceita pacotes da Rede Interna (acc... input)
- ... Descarta todo o resto (drop input)

Statistics for the first three rules are shown: 149 B bytes and 1 packet for the established connections rule.

[MikrotikBrasil]
Routers & Wireless Systems

Regras de Firewall Proteção da Rede Interna

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

160

[MikrotikBrasil]
Routers & Wireless Systems

Regras de Firewall Proteção da Rede Interna

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.
- Pode-se encontrar informações sobre esses endereços em <http://www.completeswhois.com/bogons>

Bloqueia endereços IP "bogons":

```
add chain=forward src-address=0.0.0.0/8 action=drop
add chain=forward dst-address=0.0.0.0/8 action=drop
add chain=forward src-address=127.0.0.0/8 action=drop
add chain=forward dst-address=127.0.0.0/8 action=drop
add chain=forward src-address=224.0.0.0/3 action=drop
add chain=forward dst-address=224.0.0.0/3 action=drop
```

161

[MikrotikBrasil]
Routers & Wireless Systems

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



162



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)



163



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 .

164

[MikrotikBrasil]
Routers & Wireless Systems

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.

165

[MikrotikBrasil]
Routers & Wireless Systems

Firewall - Proteções de ataques DoS

The image shows three separate windows of the MikroTik Winbox interface, each titled "New Firewall Rule".
1. The first window (left) shows the "General" tab with fields for Chain (set to "input"), Src. Address, Dist. Address, Protocol (set to "6 (tcp)", with a note "SRC.DST: 192.168.1.100-255.255.255.255"), Src. Port, Dist. Port, and P2P. The "Action" tab is visible at the top right.
2. The second window (top right) shows the "Action" tab with Action set to "add src to address list", Address List set to "Lista_Negra", and Timeout set to "00:00:00".
3. The third window (bottom right) shows the "Connection Limit" tab with Limit set to "10" and Netmask set to "32". Other options like Dst. Limit, Nlh, Time, and various address types are listed below.
166

[MikrotikBrasil]
Routers & Wireless Systems

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 reescrever-la todo o tempo.



167

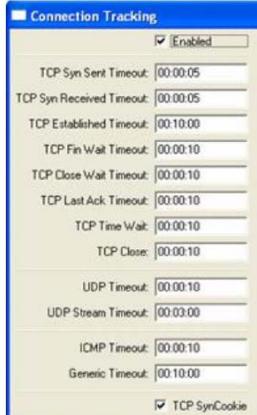
[MikrotikBrasil]
Routers & Wireless Systems

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



168

[MikrotikBrasil] Routers & Wireless Systems

Filter Rules - Exemplos

• Permitir apenas 20 conexões simultâneas para cada cliente:

```
/ip firewall filter add
chain=forward
protocol=tcp tcp-
flags=syn connection-
limit=20,32 action=drop
```

169

[MikrotikBrasil] Routers & Wireless Systems

Filter Rules - Exemplos

Na verdade o interessante é limitar a partir da porta 1024 e ainda evitar algumas de certos serviços, por exemplo:

- 1863 (MSN)
- 3128 (Squid – nosso caso)
- 5600 (VNC)
- 5900 (VNC)

Etc...

170

[MikrotikBrasil]

Routers & Wireless Systems

Filter Rules – canais definidos pelo usuário

Exemplo de canal criado para 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.

171

[MikrotikBrasil]

Routers & Wireless Systems

Filter Rules – canais definidos pelo usuário

Exemplo de canal criado para ICMP

- Crie um canal ICMP
- Aceite os 5 tipos de ping indicados
- Negue o resto
- Crie uma ação “jump” no canal input
- Crie a mesma ação “jump”, agora no canal forward

172

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.



173

Firewall do Mikrotik – NAT

As regras de NAT são organizadas em canais:

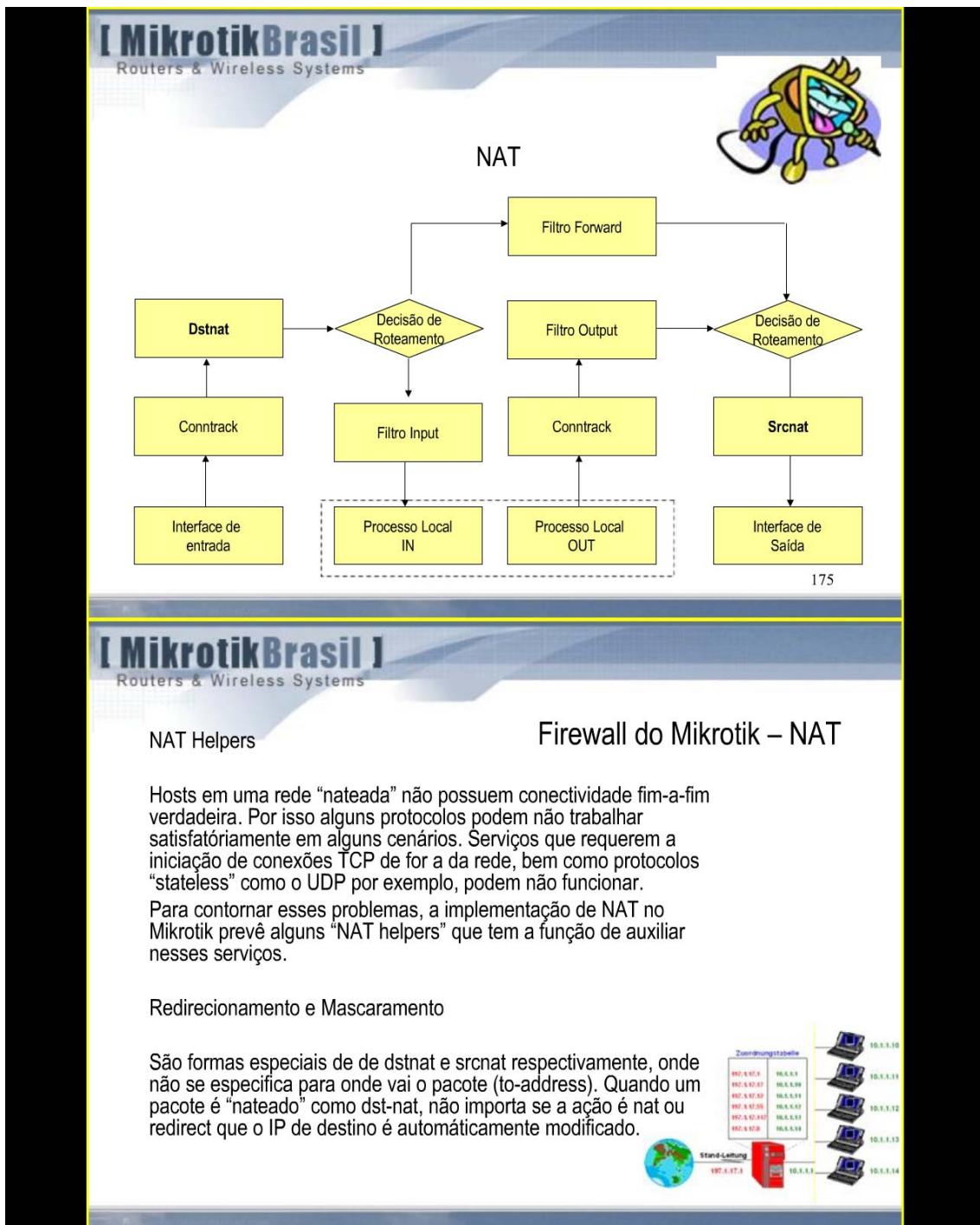
→ dstnat:

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

174



[MikrotikBrasil]
Routers & Wireless Systems

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

→ Regra única fazendo Masquerade
add chain=srcnat out-interface=ether1 src-address=192.168.0.0/24 action=masquerade

Destination NAT – Apontando o IP 200.200.200.200 para o host interno 192.168.0.100

→ Regra permitindo acesso de redes externas ao servidor interno
add chain=dstnat dst-address=200.200.200.200 action=dst-nat to-addresses=192.168.0.100

→ Regra permitindo acesso do servidor interno para redes externas tendo seu endereço trocado pelo IP público
add chain=srcnat src-address=192.168.0.109 action=src-nat to-addresses=200.200.200.200

177

[MikrotikBrasil]
Routers & Wireless Systems

NAT - Exemplos

Exemplo de Destination NAT com WInbox

– Apontando o IP 200.200.200.200 para o host interno 192.168.0.100

The image shows four windows of the Winbox 'New NAT Rule' dialog:

- New NAT Rule (Top Left):** Chain: 'dstnat', Src. Address: empty, Det. Address: '200.200.200' (with a dropdown menu showing '200 200 200 200').
- New NAT Rule (Top Right):** Action: 'dst-nat', To Addresses: '192.168.0.100', To Ports: '0-65535'.
- NAT Rule <192.168.0.100/> (Bottom Left):** General tab, Chain: 'srcnat', Src. Address: '192.168.0.100'.
- NAT Rule <192.168.0.100/> (Bottom Right):** Action: 'src-nat', To Addresses: '200.200.200.200', To Ports: '0-65535'.

NAT 1:1

– Apontando a rede interna 192.168.0.0/24 para a rede pública 200.200.200.200/24

```

add chain=dslnat dst-address=200.200.200.1-200.200.200.254 action=netmap to-addresses=192.168.0.1-192.168.0.254 to-ports=0-65535
add chain=srcnat src-address=192.168.0.0/24 action=netmap to-addresses=200.200.200.0-200.200.200.254 to-ports=0-65535

```

179

Service Ports

Name	Ports
ftp	21
gre	
h323	
irc	6667
pptp	
quake3	
http	80

Alguns protocolos de rede não são compatíveis com NAT devido a alguma informação adicional sobre os reais endereços ou portas presentes dentro do conteúdo do pacote.

O conteúdo do pacote não é conhecido nos procedimentos de NAT, já que ele "olha" apenas IP, UDP e cabeçalhos TCP e nunca dentro dos mesmos.

Para que esses protocolos possam trabalhar corretamente, um "auxiliador de seguimento de conexões" - connection tracking helper é necessário para contornar esses problemas. É possível habilitar esses helpers e é aconselhável desabilitá-los caso não seja usados para melhorar a performance do roteador. Notar que não é possível introduzir helpers, mas tão somente habilitá-los ou desabilitá-los

180

[MikrotikBrasil]
Routers & Wireless Systems

FIREWALL MANGLE

181

[MikrotikBrasil]
Routers & Wireless Systems

Firewall do Mikrotik – Mangle

The screenshot shows the 'Firewall' window with the 'Mangle' tab selected. There are two entries listed:

#	Action	Chain	Src. Address	Src. Port	In. Inter...	Dst. Address	Dst. Port	Out. Int...	Proto...	New P...	New C...	Bytes	Packets
1	mark	prerouting							p2p_co...	0 B	0	0 B	0
2	mark	prerouting							p2p_co...	0 B	0	0 B	0

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 fora.

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)

182

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

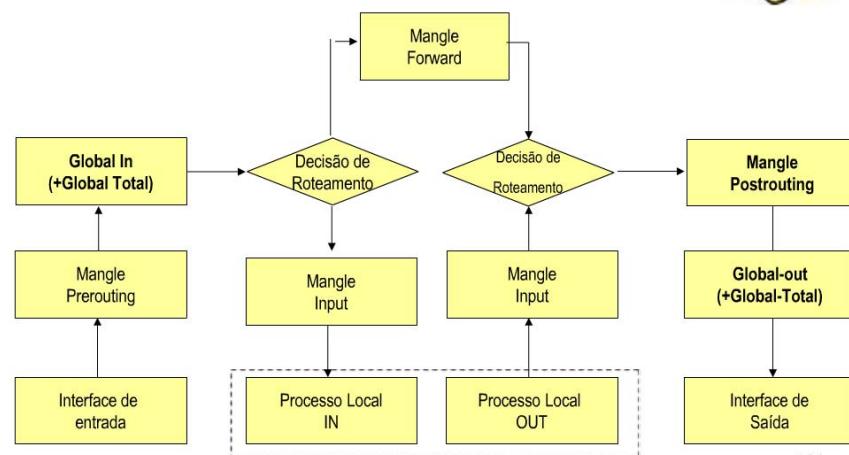
→ Há 5 canais padrão:

- 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

183



MANGLE E QUEUE



184

Ações 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

185

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.

186

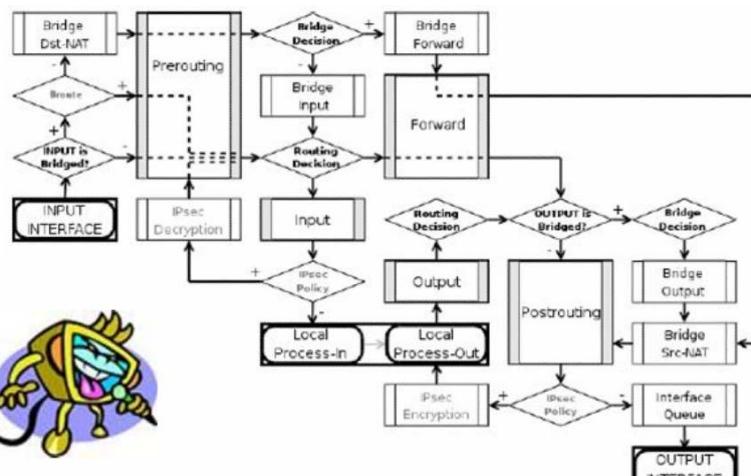
Marcando Pacotes

Pacotes podem ser marcados:

- Indiretamente, usando a facilidade de connection tracking, com base em marcas de conexão previamente criadas (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.

187

Estrutura de Firewall no Mikrotik



[MikrotikBrasil]
Routers & Wireless Systems

Fluxo de pacotes no Firewall

```

graph TD
    Prerouting[Prerouting] --> HotSpotInput[HotSpot Input]
    HotSpotInput --> ConnTrack1[ConnTrack]
    ConnTrack1 --> Mangle1[Mangle]
    Mangle1 --> DestinationNAT[Destination NAT]
    DestinationNAT --> GlobalInQueue[Global-In Queue]
    GlobalInQueue --> GlobalTotalQueue[Global-total Queue]
    GlobalTotalQueue --> SourceNAT[Source NAT]
    SourceNAT --> HotSpotOutput[HotSpot Output]
    HotSpotOutput --> Postrouting[Postrouting]
    Postrouting --> Mangie[ConnTrack]
    Mangie --> GlobalOutQueue[Global-Out Queue]
    GlobalOutQueue --> Output[Output]
    Output --> Forward[Forward]
    Forward --> ConnTrack2[ConnTrack]
    ConnTrack2 --> Mangle2[Mangle]
    Mangle2 --> Filter1[Filter]
    Filter1 --> Accounting[Accounting]
    Accounting --> Input[Input]
    Input --> Filter2[Filter]
    Filter2 --> Mangle3[Mangle]
    Mangle3 --> Filter3[Filter]
  
```

189

[MikrotikBrasil]
Routers & Wireless Systems

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
  
```

190

[MikrotikBrasil]
Routers & Wireless Systems

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
```

191

[MikrotikBrasil]
Routers & Wireless Systems

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

192

[MikrotikBrasil]
Routers & Wireless Systems

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

193

[MikrotikBrasil]
Routers & Wireless Systems

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

[MikrotikBrasil]
Routers & Wireless Systems

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.

The screenshot shows the Winbox interface for MikroTik. It includes several windows: a main Firewall window with a list of rules, a detailed view of a Mangle Rule (Action: add src to address list, Address List: soh_telnet), and two Firewall Rule windows (Chain: input, Action: drop). There is also a small cartoon illustration of a hand knocking on a door.

195

[MikrotikBrasil]
Routers & Wireless Systems

Address Lists - Exemplo

Protegendo o acesso externo ao roteador com uma lista dinâmica.

- Baixar o utilitário knock.exe :
<http://www.zeroflux.org/proj/knock/files/knock-cygwin.zip>
- Utilização :
Knock.exe <IP Address> port:protocol port:protocol
port:protocol...

196

[MikrotikBrasil]
Routers & Wireless Systems

Knock.exe 192.168.0.2 1234:tcp 4321:tcp



■ Firewall Rule <11234>
General Advanced Extra Action Statistics
Chain: input
Src. Address:
Dst. Address:
Protocol: 6 (tcp)
Src. Port:
Dst. Port: 1234

■ Firewall Rule <11234>
General Advanced Extra Action Statistics
Action: add src to address list
Address List: temp
Timeout: 00:00:15

■ Firewall Rule <14321>
General Advanced Extra Action Statistics
Chain: forward
Src. Address:
Dst. Address:
Protocol: 6 (tcp)
Src. Port:
Dst. Port: 4321

■ Firewall Rule <14321>
General Advanced Extra Action Statistics
Src. Address List: temp
Dst. Address List:
Action: add src to address list
Address List: liberado
Timeout: 00:00:00

197

[MikrotikBrasil]
Routers & Wireless Systems

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
```

198

Reprodução não autorizada

[MikrotikBrasil]
Routers & Wireless Systems



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

■ Firewall Rule <>
General Advanced Extra Action Statistics
Chain: input
Src. Address:

■ Firewall Rule <>
General Advanced Extra Action Statistics
Src. Address List: liberado

■ Firewall Rule <>
General Advanced Extra Action Statistics
Action: accept

■ Firewall Rule <>
General Advanced Extra Action Statistics
Action: drop

	acc... input	drop input		
8	✓		0 B	0
9	✗		47.1 kB	475

199

[MikrotikBrasil]
Routers & Wireless Systems

Dúvidas ??

200

[MikrotikBrasil]
Routers & Wireless Systems

QoS & Controle de Banda



201

[MikrotikBrasil]
Routers & Wireless Systems

Qualidade de Serviço

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

Os mecanismos para prover QoS do Mikrotik são:

- limitar banda para certos IP's, subredes, protocolos, portas e outros parametros
- 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

202

Qualidade de Serviço cont.

Para ordenar e controlar o fluxo de dados, é aplicada uma política de enfileiramento aos pacotes que estejam deixando o Roteador através de uma interface real (as filas são aplicadas na interface de saída, considerando o fluxo de tráfego), ou em uma das 3 interfaces virtuais adicionais (global-in, global-out e global-total)

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.

Os principais termos utilizados para descrever o nível de QoS para aplicações de rede são:

- **queuing discipline (qdisc)** – disciplina de enfileiramento – é um algoritmo que mantém e controla uma fila de pacotes. Ela especifica a ordem dos pacotes que saem (podendo inclusive reordená-los) e determina quais pacotes serão descartados.
- **Limit At ou CIR (Committed Information Rate)** – Taxa de dados garantida – é a velocidade mínima que se fornece a um circuito.

203

QoS -cont.

- **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 importância que o tráfego será processado. Pode-se determinar qual tipo de tráfego será processado primeiro
- **Contention Ratio** – Razão de Contenção – é a relação em que a banda será compartilhada entre usuários. Por exemplo um contention rate de 1:4 significa que a banda total alocada pode ser compartilhada entre 4 usuários.

204

Tipos de Filas

Antes de enviar os dados 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.

Queue List	
	Type Name
[+]	default
	default-small
	ethernet-default
	hotspot-default
	pcq-fairinha-down
	pcq-fairinha-up
	queue1
	synchronous-default
	wireless-default

Queue List	
Interface	Queue Type
Local	wireless-default
Public	ethernet-default
bonding1	default
ether1	ethernet-default
ether2	ethernet-default
wlan2	wireless-default

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

205

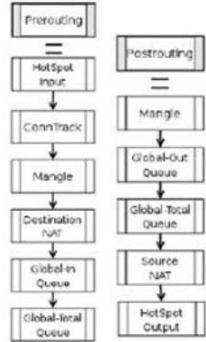
Qualidade de Serviço

Interfaces Virtuais

Além das interfaces reais, são definidas 3 interfaces virtuais no RouterOS::

- **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-in queueing” é executado logo após o mangle and dst-nat
- **global-out** – representa todas as interfaces de saída em geral. As filas associadas à essa interface precedem aquelas associadas a uma interface específica.
- **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.



206

[MikrotikBrasil]
Routers & Wireless Systems

Qualidade de Serviço

Interfaces Virtuais

Além das interfaces reais, são definidas 3 interfaces virtuais no RouterOS::

- **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-in queueing” é executado logo após o mangle and dst-nat
- **global-out** – representa todas as interfaces de saída em geral. As filas associadas à essa interface precedem aquelas associadas a uma interface específica.
- **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.

```

graph TD
    HotSpotInput[HotSpot Input] --> Conntrack[Conntrack]
    Conntrack --> Mangle[Mangle]
    Mangle --> DestinationNAT[Destination NAT]
    DestinationNAT --> GlobalInQueue[Global-in Queue]
    GlobalInQueue --> GlobalTotalQueue[Global-total Queue]
    GlobalTotalQueue --> SourceNAT[Source NAT]
    SourceNAT --> HotSpotOutput[HotSpot Output]
    GlobalOutQueue[Global-out Queue] --> GlobalTotalQueue
    GlobalTotalQueue --> GlobalOutQueue
  
```

207

[MikrotikBrasil]
Routers & Wireless Systems

Diagrama de fluxo de pacotes RouterOS:

- Entrada:** n interfaces de entrada convergem para a pilha **Global-in**.
- Processamento:** A pilha **Global-in** converge para a pilha **Global-total**. A pilha **Global-total** contém os seguintes componentes:
 - Conntrack
 - Mangle
 - Destination NAT
 - Global-in Queue (que converge para a pilha **Global-total**)
- Saída:** A pilha **Global-total** converge para a pilha **Global-out**. A pilha **Global-out** contém os seguintes componentes:
 - Global-total Queue (que converge para a pilha **Global-out**)
 - Source NAT
 - HotSpot Output

208

MikrotikBrasil
Routers & Wireless Systems

Tipos de Filas

Disciplinas “Scheduler e Shaper”

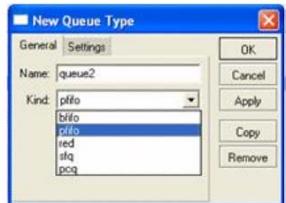
As disciplinas de filas são classificadas pela sua influencia no fluxo de pacotes da seguinte forma:

- **schedulers** – apenas reordenam 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



209

MikrotikBrasil
Routers & Wireless Systems

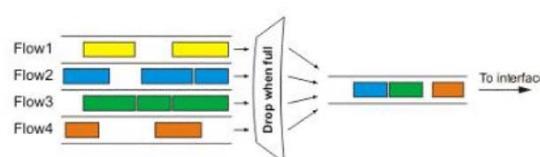
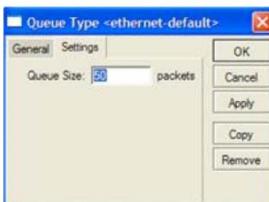
Tipos de Filas

PFIFO and BFIFO

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

A diferença entre o PFIFO e o BFIFO é que um é medido em pacotes e o outro em Bytes. Existe apenas um parametro chamado **pfifo-limit (bfifo-limit)** que determina a quantidade de dados uma fila FIFO pode ter. Todo pacote que não puder ser enfileirado (se a fila está cheia) será descartado. Tamanhos grandes de fila poderão aumentar a latênciâa.

Recomenda-se o uso desse tipo de fila em links não congestionados

210

MikrotikBrasil

Routers & Wireless Systems

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 aleatoriamente 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 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 e somente para controle de TCP (não funciona bem para UDP).

Queue Type <synchronous-default>

General	Settings	OK
Queue Size:	50	Cancel
Min Threshold:	10	Apply
Max Threshold:	50	Copy
Burst:	20	Remove

MikrotikBrasil

Routers & Wireless Systems

Tipos de Filas

SFQ

Stochastic Fairness Queuing (SFQ) – Enfileiramento Estocástico “com justiça”

Não limita tráfego. O objetivo é equalizar os fluxos de tráfego (sessões TCP e streaming UDP) quando o link está completamente cheio.

A “justiça” do SFQ é assegurado por algoritmos de hashing e round-robin.

Algoritmos de hashing dividem o tráfego da sessão em um número limitado de sub-filas. Depois de atingido o tempo em segundos configurado em **sfq-perturb** o algoritmo de hashing muda e divide a sessão em outras subfilas. O algoritmo round-robin reenfilerá essas sub-filas conforme configurado em **pcq-allot bytes**.

É recomendada a utilização desse tipo de fila para controle de P2P.

Queue Type <hotspot-default>

General	Settings	OK
Perfub:	5	Cancel
Allot:	1514	Apply
		Copy
		Remove

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 parâmetro **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

Queue Type <minha_fila_pcq>	
General Settings	
Rate:	128k
Limit:	50
Total Limit:	2000
Classifier	
<input checked="" type="checkbox"/> Src. Address	<input type="checkbox"/> Dst. Address
<input type="checkbox"/> Src. Port	<input type="checkbox"/> Dst. Port

213

Tipos de Filas

PCQ - continuação

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.

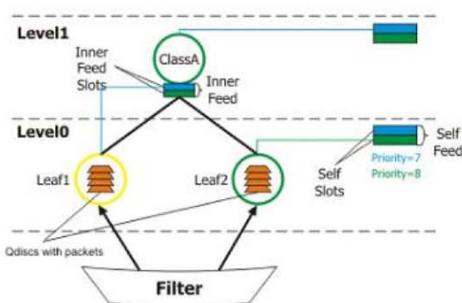
PCQ é uma boa ferramenta para controlar ou equalizar a banda entre diversos usuários com pouco trabalho de administração.

Queue Type <minha_fila_pcq>	
General Settings	
Rate:	128k
Limit:	50
Total Limit:	2000
Classifier	
<input checked="" type="checkbox"/> Src. Address	<input type="checkbox"/> Dst. Address
<input type="checkbox"/> Src. Port	<input type="checkbox"/> Dst. Port

214

QoS - HTB

HTB (Hierarchical Token Bucket) é uma disciplina de enfileiramento hierárquica que é usual para aplicar diferentes políticas para diferentes tipos de tráfego. Geralmente é possível apenas se fazer uma fila para uma interface, mas no Mikrotik as filas são associadas ao HTB e assim podem “herdar” determinadas propriedades de uma fila “pai”. Como exemplo, poderíamos configurar um total máximo de banda para um grupo de trabalho e então distribuir essa banda entre os seus membros. :



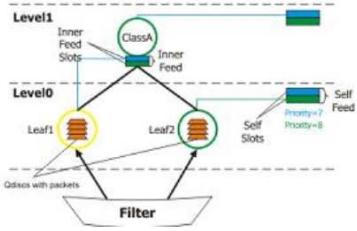
Explicação sucinta

- No nível 1 a classe “pai” está ligada as classes filhas.
- Nas classes filhas no nível 0, os pacotes recebem um tratamento determinado pelo Filtro e pela disciplina de fila a ela associada(fifo, bfifo, etc.)
- De acordo com esse tratamento, os pacotes são classificados, reordenados e se for o caso descartados.
- Se as classes filhas estão dentro do seu limit-at podem trafegar, independente da classe pai, caso contrário ficam submetidas a disponibilidade desta..

215

QoS - HTB

- Cada classe tem um “pai” e pode ter ou não classes “filhas”



- Se não tiver ‘filhas’ é colocada no nível 0
- Cada classe pode priorizar ou dar forma (“shaping”) ao tráfego
- 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 máxima prioridade

216

QoS - HTB

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

- **verde** - a classe está com a velocidade igual ou melhor que limit-at. Nesse estado a classe já está associada a seu slot de saída com sua prioridade correspondente. É permitido à classe satisfazer seu próprio limit-at independentemente das limitações da classe pai. Por exemplo se a classe tem limit-at=512kbps e sua classe pai tem max-limit-at=128kbps, a sua velocidade poderá chegar até 512kbps.
- **amarela** – nesse caso a classe está com o banda real maior que limit-at e igual ou menor que max-limit. Nesse caso a classe pede à classe pai para usar mais banda, que permitirá o uso se dispuzer de banda. Porém se a classe pai tiver outra classe pai e estiver no estado verde, permite o uso. Se estiver em amarelo pede à sua classe pai superior (avô da primeira) e assim por diante.
- **vermelha** – estando em vermelha, ou seja quando foi excedido o max-limit a classe não pode pedir banda à sua classe pai.

217

Filas Simples

- As Filas simples (simple queue) são a maneira mais fácil de se controlar a velocidade dos clients. Elas permitem configurar as velocidades de upload e download com apenas uma entrada.
- Na Hierarquia HTB estão localizadas justamente debaixo de 'root'
- 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.
- Hotspots e PPP criam dinamicamente filas simples

218

[MikrotikBrasil]
Routers & Wireless Systems

Filas Simples

Simple Queue <fila-simples-teste>

General		Advanced	Statistics	Traffic	Total	Total Statistics
Name:	fila-simples-teste					
Target Address:						
<input checked="" type="checkbox"/> Target Upload		<input checked="" type="checkbox"/> Target Download				
Max Limit:	128k	256k	bits/s			
Burst						
Burst Limit:	unlimited	512k	bits/s			
Burst Threshold:	unlimited	192k	bits/s			
Burst Time:	0	8	s			
Time						

OK Cancel Apply Disable Copy Remove

-As 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 bursts para download e upload
→ configurações de limit-at, max-limit, priority e bursts para velocidade agregada

219

[MikrotikBrasil]
Routers & Wireless Systems

Como funciona o Burst

Rate, (kbps)

Actual rate

burst-limit

Average rate

max-limit

burst-threshold

limit-at

time (s)

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

Os parametros 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

220



Como funciona o Burst

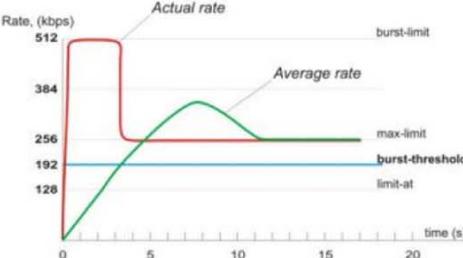
Exemplo
 max-limit=256kbps
 burst-time=8s
 burst-threshold=192kbps
 burst-limit=512kbps

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

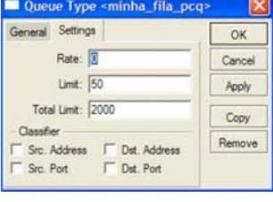
- com 1 segundo a taxa média é $(0+0+0+0+0+0+512)/8 = 64\text{ kbps}$ (abaixo do threshold)
- com 2 segundos já é de $(0+0+0+0+0+512+512)/8 = 128\text{ kbps}$ (abaixo do threshold)
- com 3 segundos $(0+0+0+0+512+512+512)/8 = 192$ (é o ponto de inflexão – onde acaba o burst)

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

221



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

222

MikrotikBrasil

Routers & Wireless Systems

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

The first window shows the General tab with Name: 'minha_fila_pcq' and Kind: 'pcq'. The second window shows the Settings tab with Rate: 0, Limit: 50, and Total Limit: 2000. The third window shows the Settings tab with Rate: 128000, Limit: 50, and Total Limit: 2000. All three windows have Classifier settings for Src. Address (checked) and Src. Port (unchecked). The third window also has Dest. Address (checked) and Dest. Port (unchecked).

223

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:

The diagram illustrates bandwidth distribution. A large arrow labeled '512k' represents the total bandwidth. It branches into two arrows labeled '128k' (representing the queue rate), which further branch into four arrows labeled '128' (representing the bandwidth per client), which finally branch into eight arrows labeled '64k' (representing the bandwidth per client). Below the diagram, the 'New Queue' configuration window is shown, setting up a queue named 'minha_fila_pcq' under 'Total_da_Banda' with a rate of 128k.

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

Exemplo de utilização de PCQ

- Equalização de Bandas para um determinado número de usuários, sendo
 - 64kbps download
 - 32kbps upload

1 - Criando as filas PCQ

```

add name="pcq_download" kind=pcq pcq-rate=64000 pcq-limit=50 pcq-classifier=dst-address pcq-total-limit=2000
add name="pcq_upload" kind=pcq pcq-rate=32000 pcq-limit=50 pcq-classifier=src-address pcq-total-limit=2000

```

OBS: Limit é o número máximo de pacotes por subqueue e Total Limit o número máximo de pacotes pela queue

Exemplo de utilização de PCQ

```

add name="pcq_download/pcq_upload" target-address=192.168.0.0/24 interface=all parent=none direction=both priority=8 \
queue=pcq_upload/pcq_download limit-at=32000/64000 max-limit=32000/64000 total-queue=default-small disabled=no

```

227

Criando uma fila Simples

```

add name="pcq_download/pcq_upload" target-address=192.168.0.0/24 interface=all parent=none direction=both priority=8 \
queue=pcq_upload/pcq_download limit-at=32000/64000 max-limit=32000/64000 total-queue=default-small disabled=no

```

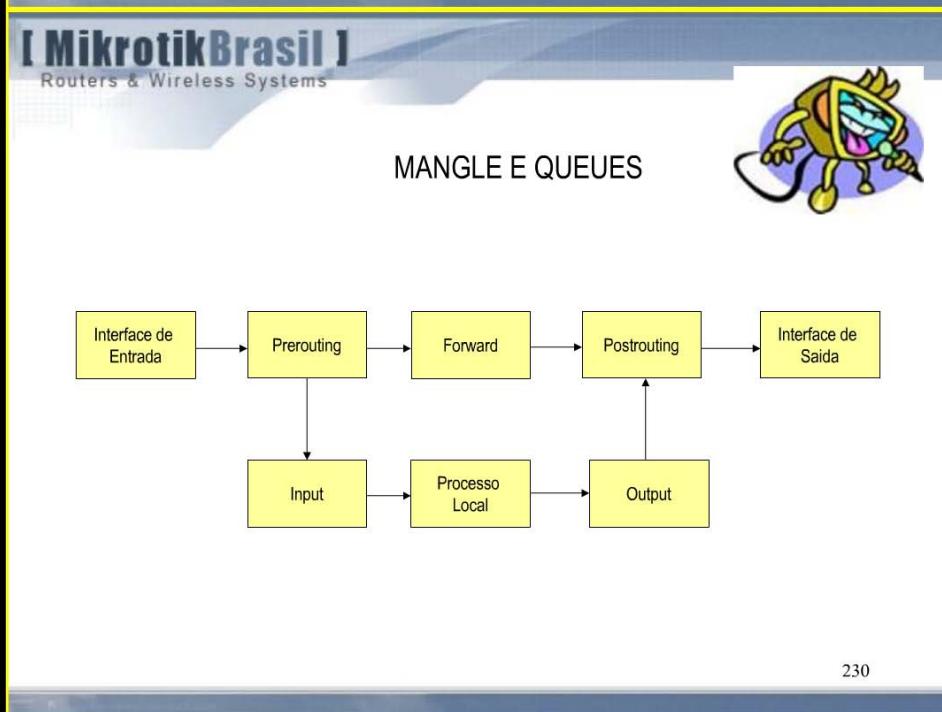
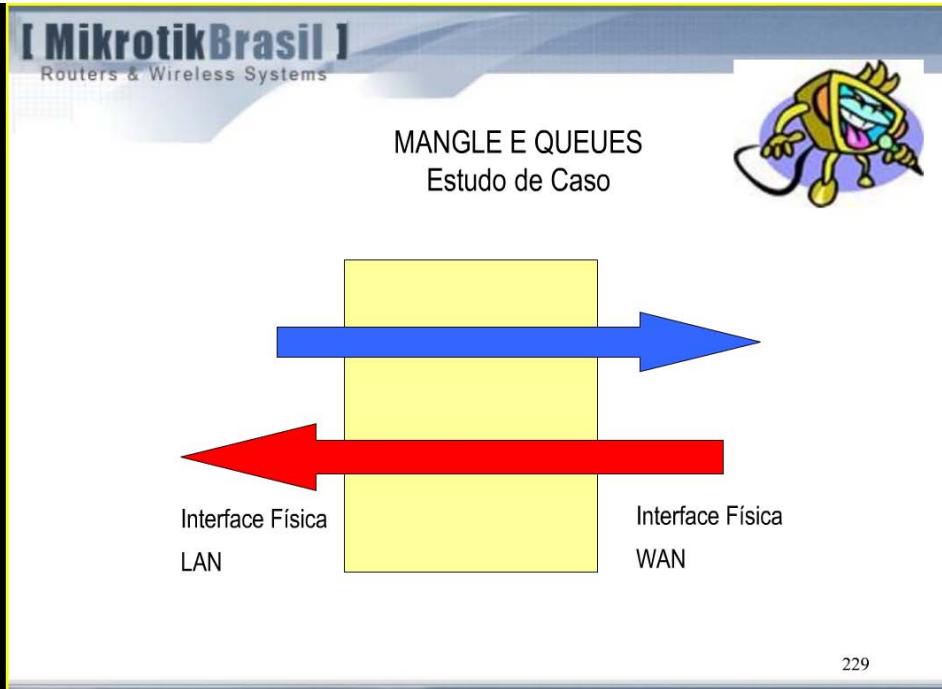
Exemplo de utilização de PCQ

```

queue=pcq_upload/pcq_download limit-at=32000/64000 max-limit=32000/64000 total-queue=default-small disabled=no

```

228



[MikrotikBrasil]
Routers & Wireless Systems

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.

- Os filtros de árvores de filas são aplicados na interface especificada. Os filtros são apenas marcas que o Firewall faz nos fluxos de pacotes na opção "Mangle". Os filtros enxergam os pacotes na ordem em que eles chegaram ao roteador.

- Os filtros nas interfaces global-in e global-out são executados antes dos filtros simples. Note-se que as filas simples estão separadas em 2 partes: 'direct' em global-out e 'reverse' em global-in.

- Se são feitas configurações com duplo enfileiramento (exemplo em ambas interfaces virtuais), considerar que não poderá ter mais que o mínimo da limitações ativas.

231

[MikrotikBrasil]
Routers & Wireless Systems

Árvores de Filas

- As árvores de filas são configuradas em /queue tree

Queue <-p2pconf>

General	Statistics
Name: p2pconf	
Parent:	global-in
Packet Mark:	p2p
Queue Type:	default
Priority:	8
Limit At:	bits/s
Max Limit:	<input checked="" type="checkbox"/> 1024 bits/s
Burst Limit:	bits/s
Burst Threshold:	bits/s
Burst Time:	s
disabled	

OK Cancel Apply Disable Copy Remove

232

Exemplo de QoS utilizando Queue Tree

(Marcando o VoIP)

```
/ ip firewall mangle  
add chain=prerouting protocol=udp src-port=10000-20000 action=mark-connection new-connection-mark=voipC passthrough=yes comment="VoIP" disabled=no  
  
add chain=prerouting protocol=udp src-port=5060 action=mark-connection new-connection-mark=voipC passthrough=yes comment="" disabled=no  
  
add chain=prerouting dst-address=200.200.200.200 action=mark-connection new-connection-mark=voipC passthrough=yes comment="Asterisk" disabled=no
```

233

Exemplo de QoS utilizando Queue Tree

(Marcando o VoIP – continuação)

```
/ ip firewall mangle  
  
add chain=prerouting tos=184 action=mark-connection new-connection-mark=voipC  
passthrough=yes comment="" disabled=no  
  
add chain=prerouting connection-mark=voipC action=change-tos new-tos=184 comment=""  
disabled=no  
  
add chain=prerouting connection-mark=voipC action=mark-packet new-packet-mark=voip  
passthrough=no comment="" disabled=no
```

234

Exemplo de QoS utilizando Queue Tree

(Marcando ICMP, HTTP e HTTPS)

/ip firewall mangle

```
add chain=prerouting src-address=192.168.1.0/24 protocol=icmp action=mark-connection new-connection-mark=icmpC passthrough=yes comment="ICMP da rede interna" disabled=no
```

```
add chain=prerouting connection-mark=icmpC action=mark-packet new-packet-mark=icmp passthrough=no comment="" disabled=no
```

```
add chain=prerouting protocol=tcp dst-port=80 action=mark-connection new-connection-mark=httpC passthrough=yes comment="http" disabled=no
```

235

Exemplo de QoS utilizando Queue Tree

(HTTP e HTTPS - continuação)

/ip firewall mangle

```
add chain=prerouting protocol=tcp dst-port=443 action=mark-connection new-connection-mark=httpsC passthrough=yes comment="https" disabled=no
```

```
add chain=prerouting protocol=udp dst-port=443 action=mark-connection new-connection-mark=httpsC passthrough=yes comment="https" disabled=no
```

```
add chain=prerouting protocol=udp dst-port=53 action=mark-connection new-connection-mark=httpsC passthrough=yes comment="dns" disabled=no
```

```
add chain=prerouting connection-mark=httpC action=mark-packet new-packet-mark=http passthrough=no comment="" disabled=no
```

236

i

i

Exemplo de QoS utilizando Queue Tree

(Marcando o p2p)

```
add chain=prerouting p2p=all-p2p action=mark-connection new-connection-mark=p2pC  
passthrough=yes comment="P2P" disabled=no
```

```
add chain=prerouting protocol=tcp p2p=all-p2p connection-limit=40,32 action=mark-  
connection new-connection-mark=p2pCL passthrough=yes comment="" disabled=no
```

```
add chain=prerouting connection-mark=p2pC action=mark-packet new-packet-mark=p2p  
passthrough=no comment="" disabled=no
```

```
add chain=prerouting connection-mark=p2pCL action=mark-packet new-packet-mark=p2p  
passthrough=no comment="" disabled=no
```

237

Exemplo de QoS utilizando Queue Tree

(Medidores)

```
add chain=prerouting dst-address=209.160.32.66 action=mark-connection new-connection-  
mark=medidoresC passthrough=yes comment="Medidores" disabled=no
```

```
add chain=prerouting dst-address=200.140.120.29 action=mark-connection new-connection-  
mark=medidoresC passthrough=yes comment="" disabled=no
```

```
add chain=prerouting dst-address=200.141.254.61 action=mark-connection new-connection-  
mark=medidoresC passthrough=yes comment="" disabled=no
```

```
add chain=prerouting dst-address=64.247.18.18 action=mark-connection new-connection-  
mark=medidoresC passthrough=yes comment="" disabled=no
```

238

Exemplo de QoS utilizando Queue Tree

(Medidores - continuação)

```
add chain=prerouting dst-address=200.150.160.39 action=mark-connection new-connection-mark=medidoresC passthrough=yes comment="" disabled=no
```

```
add chain=prerouting dst-address=62.81.199.129 action=mark-connection new-connection-mark=medidoresC passthrough=yes comment="" disabled=no
```

```
add chain=prerouting dst-address=212.71.8.6 action=mark-connection new-connection-mark=medidoresC passthrough=yes comment="" disabled=no
```

```
add chain=prerouting connection-mark=medidoresC action=mark-packet new-packet-mark=medidores passthrough=no comment="" disabled=no
```

239

Exemplo de QoS utilizando Queue Tree

(Acessos Remotos)

```
add chain=prerouting protocol=tcp dst-port=5900-5999 action=mark-connection new-connection-mark=vncC passthrough=yes comment="Acessos remotos" disabled=no
```

```
add chain=prerouting protocol=tcp dst-port=3389 action=mark-connection new-connection-mark=vncC passthrough=yes comment="" disabled=no
```

```
add chain=prerouting protocol=tcp dst-port=22 action=mark-connection new-connection-mark=vncC passthrough=yes comment="" disabled=no
```

```
add chain=prerouting protocol=tcp dst-port=23 action=mark-connection new-connection-mark=vncC passthrough=yes comment="" disabled=no
```

```
add chain=prerouting connection-mark=vncC action=mark-packet new-packet-mark=vnc passthrough=no comment="" disabled=no
```

240

Exemplo de QoS utilizando Queue Tree

(FTP e MSN)

```
add chain=prerouting protocol=tcp dst-port=21 action=mark-connection new-connection-mark=ftpC passthrough=yes comment="FTP" disabled=no
```

```
add chain=prerouting connection-mark=ftpC action=mark-packet new-packet-mark=ftp passthrough=no comment="" disabled=no
```

```
add chain=prerouting protocol=tcp dst-port=6891-6901 action=mark-connection new-connection-mark=msnC passthrough=yes comment="MSN" disabled=no
```

```
add chain=prerouting protocol=udp dst-port=6891-6901 action=mark-connection new-connection-mark=msnC passthrough=yes comment="" disabled=no
```

241

Exemplo de QoS utilizando Queue Tree

(MSN - continuação)

```
add chain=prerouting protocol=tcp dst-port=1863 action=mark-connection new-connection-mark=msnC passthrough=yes comment="" disabled=no
```

```
add chain=prerouting protocol=udp dst-port=1863 action=mark-connection new-connection-mark=msnC passthrough=yes comment="" disabled=no
```

```
add chain=prerouting protocol=udp dst-port=5190 action=mark-connection new-connection-mark=msnC passthrough=yes comment="" disabled=no
```

```
add chain=prerouting connection-mark=msnC action=mark-packet new-packet-mark=msn passthrough=no comment="" disabled=no
```

242

Exemplo de QoS utilizando Queue Tree

(Streamings)

```
add chain=prerouting protocol=tcp dst-port=554 action=mark-connection new-connection-mark=rtspC passthrough=yes comment="Streamings: rtsp e ms-streaming" disabled=no
```

```
add chain=prerouting protocol=udp dst-port=554 action=mark-connection new-connection-mark=rtspC passthrough=yes comment="" disabled=no
```

```
add chain=prerouting protocol=udp dst-port=8554 action=mark-connection new-connection-mark=rtspC passthrough=yes comment="" disabled=no
```

243

Exemplo de QoS utilizando Queue Tree

(Streamings - continuação)

```
add chain=prerouting protocol=tcp dst-port=1755 action=mark-connection new-connection-mark=rtspC passthrough=yes comment="" disabled=no
```

```
add chain=prerouting protocol=udp dst-port=1755 action=mark-connection new-connection-mark=rtspC passthrough=yes comment="" disabled=no
```

```
add chain=prerouting connection-mark=rtspC action=mark-packet new-packet-mark=rtsp passthrough=no comment="" disabled=no
```

244

Exemplo de QoS utilizando Queue Tree

(E-mail)

```
add chain=prerouting dst-address=200.200.200.100 protocol=tcp dst-port=25 action=mark-connection new-connection-mark=mailC passthrough=yes comment="E-mail" disabled=no
```

```
add chain=prerouting dst-address=200.200.200.100 protocol=tcp dst-port=110 action=mark-connection new-connection-mark=mailC passthrough=yes comment="" disabled=no
```

```
add chain=prerouting connection-mark=mailC action=mark-packet new-packet-mark=mail passthrough=no comment="" disabled=no
```

245

Exemplo de QoS utilizando Queue Tree

(UDP e Outros)

```
add chain=prerouting protocol=udp action=mark-connection new-connection-mark=outrosUDPc passthrough=yes comment="Outros UDP" disabled=no
```

```
add chain=prerouting connection-mark=outrosUDPc action=mark-packet new-packet-mark=outrosUDP passthrough=no comment="" disabled=no
```

```
add chain=prerouting action=mark-connection new-connection-mark=outrosC passthrough=yes comment="Outros" disabled=no
```

```
add chain=prerouting connection-mark=outrosC action=mark-packet new-packet-mark=outros passthrough=no comment="" disabled=no
```

246

Exemplo de QoS utilizando Queue Tree

/ queue tree

```
add name="QoS" parent=global-total packet-mark="" limit-at=0 queue=default priority=8 max-limit=20M burst-limit=0 burst-threshold=0 burst-time=0s disabled=no
```

```
add name="voip" parent=QoS packet-mark=voip limit-at=500000 queue=default priority=1 max-limit=1000000 burst-limit=0 burst-threshold=0 burst-time=0s disabled=no
```

```
add name="outros" parent=QoS packet-mark=outros limit-at=0 queue=default priority=8 max-limit=10000000 burst-limit=0 burst-threshold=0 burst-time=0s disabled=no
```

```
add name="icmp" parent=QoS packet-mark=icmp limit-at=1000000 queue=default priority=1 max-limit=2000000 burst-limit=0 burst-threshold=0 burst-time=0s disabled=no
```

247

Exemplo de QoS utilizando Queue Tree

/ queue tree

```
add name="p2p" parent=QoS packet-mark=p2p limit-at=0 queue=default priority=8 max-limit=512000 burst-limit=0 burst-threshold=0 burst-time=0s disabled=no
```

```
add name="vnc" parent=QoS packet-mark=vnc limit-at=256000 queue=default priority=2 max-limit=512000 burst-limit=0 burst-threshold=0 burst-time=0s disabled=no
```

```
add name="http" parent=QoS packet-mark=http limit-at=2000000 queue=default priority=3 max-limit=100000000 burst-limit=0 burst-threshold=0 burst-time=0s disabled=no
```

```
add name="msn" parent=QoS packet-mark=msn limit-at=1000000 queue=default priority=3 max-limit=2000000 burst-limit=0 burst-threshold=0 burst-time=0s disabled=no
```

248

Exemplo de QoS utilizando Queue Tree

/ queue tree

```
add name="medidores" parent=QoS packet-mark=medidores limit-at=1000000 queue=default priority=2 max-limit=4000000 burst-limit=0 burst-threshold=0 burst-time=0s disabled=no
```

```
add name="streamings" parent=QoS packet-mark=rtsp limit-at=1000000 queue=default priority=2 max-limit=5000000 burst-limit=0 burst-threshold=0 burst-time=0s disabled=no
```

```
add name="email" parent=QoS packet-mark=mail limit-at=600000 queue=default priority=3 max-limit=10000000 burst-limit=0 burst-threshold=0 burst-time=0s disabled=no
```

249

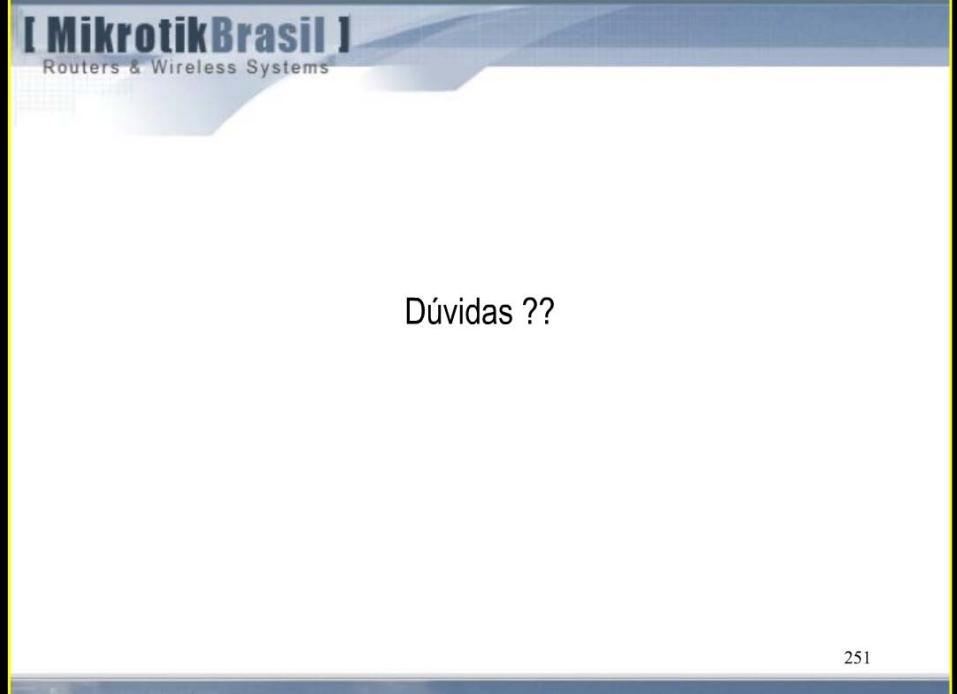
Exemplo de QoS utilizando Queue Tree

/ queue tree

```
add name="outrosUDP" parent=QoS packet-mark=outrosUDP limit-at=2000000 queue=default priority=3 max-limit=10000000 burst-limit=0 burst-threshold=0 burst-time=0s disabled=no
```

```
add name="ftp" parent=QoS packet-mark=ftp limit-at=2000000 queue=default priority=3 max-limit=10000000 burst-limit=0 burst-threshold=0 burst-time=0s disabled=no
```

250



[MikrotikBrasil]
Routers & Wireless Systems

off the mark
www.offthemark.com by Mark Parisi

Shoo!
OUT OF OUR
HOTSPOT!

© Mark Parisi, Permission required for use.

Hotspot
no
Mikrotik

Reprodução não autorizada

[MikrotikBrasil]
Routers & Wireless Systems

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 fornecer-las e sendo um cliente autorizado pelo Hotspot o usuário ganha acesso à Internet podendo sua atividade ser controlada e bilhetada.

253

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 distribuídos para os usuários do Hotspot (se não tiver, crie em /ip pool)

4 – Selecione um certificado, caso queira usar.
continua...

Hotspot

Name	Interface	Address Pool	Profile	Addresses
meu_hotspot	wlan1	hs-pool-3	hsprof1	2

Hotspot Setup

Select interface to run HotSpot on:
HotSpot Interface: ether1

Hotspot Setup

Local Address of Network: 192.168.1.3/24
 Masquerade Network

Hotspot Setup

Set pool for HotSpot addresses:
Address Pool of Network: 192.168.1.1-192.168.1.254
192.168.1.4-192.168.1.254

Hotspot Setup

Select hotspot SSL certificate:
Select Certificate: none

254

[MikrotikBrasil]
Routers & Wireless Systems

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

255

[MikrotikBrasil]
Routers & Wireless Systems

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.

256

Reprodução não autorizada

[MikrotikBrasil]
Routers & Wireless Systems

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 detectar 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

257

[MikrotikBrasil]
Routers & Wireless Systems

Hotspot Server Profiles

→ **rate-limit** (*text* ; default: **""**)
 A limitação de velocidade tem a sintaxe:

rx-rate[/tx-rate] [rx-burst-rate[/tx-burst-rate] [rx-burst-threshold[/tx-burst-threshold] [rx-burst-time[/tx-burst-time]]]]]

Exemplo: 150k/300k 512k/512k 350k/350k 100/100

- rx é o upload do cliente e tx é o download do cliente.
 - As velocidades podem ser números com opcionais 'k' (1.000 s) e 'M' para kilo e Mega.
 - Se tx rate não é especificado, tem o mesmo valor de rx-rate.
 - O mesmo para tx-burst-rate, tx-burst-threshold e tx-burst-time.
 - Se ambos rx-burst-threshold e tx-burst-threshold não são especificados (mas burst-rate sim), rx-rate e tx-rate são usados como burst thresholds.
 - Se ambos rx-burst-time e tx-burst-time não são especificados, 1s é usado como default

[MikrotikBrasil]
Routers & Wireless Systems

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 domínio do usuário no caso de usuário@dominio.com.br.

259

[MikrotikBrasil]
Routers & Wireless Systems

Hotspot Server Profiles

Utilização de servidor Radius para autenticação do Hotspot

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

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

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

→ NAS Port Type: Wireless, Ethernet ou Cabo

260

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: período de inatividade (acesso externo)
- Keepalive Timeout: se o computador está “vivo” e tem conectividade
- Status Autorefresh: tempo de refresh da página de Status do Hotspot
- Shared Users: número máximo de clientes com o mesmo username.
- Rate Limit: mesma sintaxe explanada em Server Profiles

261

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 automaticamente 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

262

[MikrotikBrasil]
Routers & Wireless Systems

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

263

[MikrotikBrasil]
Routers & Wireless Systems

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

264

The screenshot shows two parts of the MikroTik Web Interface. The top part displays a list of 'Hotspot Users' with columns for Server, Name, Address, MAC Address, Profile, and Uptime. The bottom part shows the configuration details for a specific user named 'miltinho'.

Hotspot Users List:

Server	Name	Address	MAC Address	Profile	Uptime
admin	admin			default	13:40:27
daniela	daniela			funcionarios_adm	4d 10:41:03
thiago	thiago			funcionario_suporte	3d 02:55:24
wadson	wadson			funcionario_suporte	6d 09:36:27
miltinho	miltinho			funcionario_suporte	4d 00:06:30
daniel	daniel			funcionario_suporte	1d 13:43:49
gabriela	gabriela			funcionarios_adm	2d 05:28:10
daniele	daniele			funcionarios_adm	2d 23:21:11
jotaedu	jotaedu			funcionarios_adm	00:00:00
humberto	humberto			funcionarios_adm	00:00:00
maia	maia			funcionario_suporte	3d 15:51:39
edu	edu			funcionarios_adm	01:44:52

Hotspot User <miltinho> Configuration:

- General tab settings:
 - Server: all
 - Name: miltinho
 - Password: milton
 - Address: 0.0.0.0
 - MAC Address: 00:00:00:00:00:00
 - Profile: funcionario_suporte
 - Routes:
 - Email:
- Statistics tab (disabled)

Details of each user:

- all para todos os hotspots configurados ou para um específico.
- Name: Nome do usuário. Se o modo trial estiver habilitado o Hotspot colocará automaticamente 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 métrica. Exemplo 192.168.1.0/24 192.168.166.1 1. Várias rotas separadas por vírgula podem ser adicionadas.
- Email: ?

265

266



Hotspot User <miltinho>

General	Limits	Statistics
Limit Uptime: <input checked="" type="checkbox"/> 00:02:00		
Limit Bytes In: <input checked="" type="checkbox"/> 100M		
Limit Bytes Out: <input checked="" type="checkbox"/> 100M		



Hotspot User <miltinho>

General	Limits	Statistics
Uptime: 4d 00:06:30		
Bytes In: 34.6 MB		
Packets In: 420 833		
Bytes Out: 354.4 MB		
Packets Out: 524 232		

Hotspot Users

→ Limit Uptime: Total de tempo que o usuário pode usar o Hotspot. Util 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).

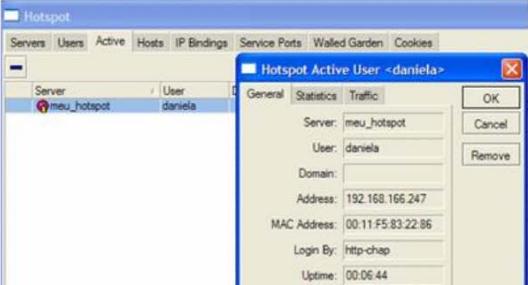
→ Limit Bytes Out: total de Bytes que o usuário pode receber. (bytes que o roteador transmite para o usuário).

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.

267

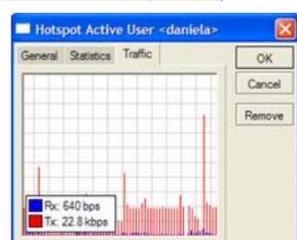


Hotspot

- Servers
- Users
- Active**
- Hosts
- IP Bindings
- Service Ports
- Walled Garden
- Cookies

Hotspot Active User <daniela>

General	Statistics	Traffic
Server: meu_hotspot	Bytes In: 299.7 kB	OK
User: daniela	Packets In: 2 817	Cancel
Domain:	Bytes Out: 2364.2 kB	Remove
Address: 192.168.166.247	Packets Out: 2 683	
MAC Address: 00:11:F5:83:22:86		
Login By: Http-chap		
Uptime: 00:06:44		



Hotspot Active User <daniela>

General Statistics Traffic

Rx: 640 bps Tx: 22.8 kbps

Hotspot Active

Mostra dados gerais e estatísticas de todos os usuários conectados

268

The screenshot shows the MikroTik IP Bindings configuration interface. On the left, there is a list of IP bindings with columns for MAC Address, Address, To Address, and Server. One entry is selected: MAC Address BE:BA:D0:01:01:01, Address 192.168.100.100, To Address 200.200.200.200, and Server meu_hotspot. On the right, a detailed configuration dialog for this binding is open. It shows the MAC Address (BE:BA:D0:01:01:01), Address (192.168.100.100), To Address (200.200.200.200), Server (meu_hotspot), and Type (regular). The Type dropdown menu is open, showing options: regular, bypassed, and blocked.

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...
269

The screenshot shows the same MikroTik IP Bindings configuration interface as before, but with several annotations pointing to specific fields:

- 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. Se for uma rede, é o endereço inicial da tradução.
- 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.

270



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 único problema é com relação ao módulo de FTP que deve ser configurado para usar as portas 20 e 21.

271



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 requisição para o destino ou para um proxy.

Para implementar o Walled Garden para requisições http, existe um Web Proxy embarcado no Mikrotik, 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**.

272

The screenshot shows two windows side-by-side under the 'Walled Garden' section:

- Walled Garden Entry </>**: This window is for HTTP and HTTPS rules. It includes fields for Action (allow or deny), Server (set to 'meu_hotspot'), Src. Address, Dst. Address, Method, Dst. Host, Dst. Port, and Path. A note at the bottom says 'disabled'.
- Walled Garden IP Entry </>**: This window is for other protocols. It includes fields for Action (accept, drop, reject), Server (set to 'meu_hotspot'), Src. Address, Dst. Address, Protocol (set to 'unknown'), Dst. Port, and Dst. Host. A note at the bottom says 'Enabled'.

Below the windows, there is explanatory text and terminal commands:

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

273

The screenshot continues with the following text and configuration window:

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 domínio é necessário o nome completo, podendo ser usados coringas
- aceita-se expressões regulares devendo ser iniciadas com (:)

274

[MikrotikBrasil]
Routers & Wireless Systems

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 requisitada
 → Dst Host: Nome de domínio do WEB server

275

[MikrotikBrasil]
Routers & Wireless Systems

Hotspot – Walled Garden

Notes

Wildcard properties (**dst-host** and **dst-path**) match a complete string (i.e., they will not match "example.com" if they are set to "example"). Available wildcards are '*' (match any number of any characters) and '?' (match any one character). Regular expressions are also accepted here, but if the property should be treated as a regular expression, it should start with a colon (':').

Small hints in using regular expressions:

- \ symbol sequence is used to enter \ character in console
- .\ pattern means . only (in regular expressions single dot in pattern means any symbol)
- to show that no symbols are allowed before the given pattern, we use ^ symbol at the beginning of the pattern
- to specify that no symbols are allowed after the given pattern, we use \$ symbol at the end of the pattern

You can not use **path** property for HTTPS requests as router can not (and should not - that is what the HTTPS protocol was made for!) decrypt the request.

276



The screenshot shows the MikroTik Web Interface with the title 'Hotspot - Cookies'. Below it is a table with one row containing the user 'daniela', MAC address '00:11:F5:83:22:86', and an expiration time of '2d 15:29:54'.

→ 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

277



The screenshot shows the MikroTik Web Interface with the title 'Personalizando o Hotspot'. Below it is a section titled 'Páginas do Hotspot' with a detailed description of how to customize hotspot pages for different user profiles.

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

Para tanto crie os diretórios, copie as páginas default e edite-as a vontade, fazendo o upload destas em /files Available Servlet Pages

Main HTML servlet pages, which are shown to user:

- **redirect.html** - redirects user to another url (for example, to login page)
- **login.html** - login page shown to a user to ask for username and password. This page may take the following parameters:
 - **username** - username
 - **password** - either plain-text password (in case of PAP authentication) or MD 5 hash of chap-id variable, password and CHAP challenge (in case of CHAP authentication)
 - **dst** - original URL requested before the redirect. This will be opened on successfull login
 - **popup** - whether to pop-up a status window on successfull login

278

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 usuários 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.

279

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

280

The screenshot shows the MikroTik RouterOS User Manager interface. At the top left is the MikrotikBrasil logo. On the right, there is a large text area with the question "Dúvidas ??". Below this, the page number "281" is visible. The main content area is titled "User Manager". It features two side-by-side boxes: "Search users" on the left and "Add users" on the right. The "Search users" box contains a search input field and a "Search" button. The "Add users" box has fields for "Number of users", "Rate limits", "Uptime limit", and "Prepaid". It also includes checkboxes for "Generate CSV file" and "Generate vouchers", and a dropdown for "Users per page". At the bottom right of the interface is a small user icon.

282

[MikrotikBrasil]
Routers & Wireless Systems

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

Requisitos:

- Pacotes do User Manager e do RouterOS devem ter a mesma versão.
- Roda em x86. Quando dessa edição da apostila, a versão para MIP's estava parada na 2.9.26.
- O roteador precisa ter pelo menos 32 MB de RAM e 2MB de espaço livre em disco

283

[MikrotikBrasil]
Routers & Wireless Systems

User Manager



Como implementar

- 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
```

→ Logar via WEB com o usuário e senhas criados acima em:

http://IP_do_Router/userman

284

[MikrotikBrasil]
Routers & Wireless Systems

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

285

[MikrotikBrasil]
Routers & Wireless Systems

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.

286

[MikrotikBrasil]
Routers & Wireless Systems



User Manager como autenticador do sistema

No Roteador:

```
/ user aaa set use-radius=yes  
/ user aaa set default-group=full  
/ radius add service=login address=x.x.x.x secret=123456
```

No User Manager

```
/ tool user-manager customer add login="MikrotikBrasil" password="1234"  
permissions=owner  
/ tool user-manager router add subscriber=MikrotikBrasil ip-address=x.x.x.x shared-  
secret=123456
```

OBS: A Base de usuários local será consultada antes e depois o User Manager.

287

[MikrotikBrasil]
Routers & Wireless Systems



User Manager + DHCP

No Router:

```
/ ip dhcp-server set dhcp1 use-radius=yes  
/ radius add service=dhcp address=y.y.y.y secret=123456
```

No User Manager:

```
/ tool user-manager customer add login="MikrotikBrasil" password="1234"  
permissions=owner  
/ tool user-manager router add subscriber=MikrotikBrasil ip-address=x.x.x.x shared-  
secret=123456  
/ tool user-manager user add add subscriber=MikrotikBrasil  
username="00:01:29:27:81:95" ip-address=192.168.100.2
```

288

[MikrotikBrasil]
Routers & Wireless Systems

User Manager + PPPoE



No Router:

```
/ interface pppoe-server server add interface=ether1 service-name=MikroTik one-session-per-host=yes disabled=no  
/ ppp aaa set use-radius=yes  
/ ppp profile set default local-address=192.168.0.1  
/ radius add service=ppp address=y.y.y.y secret=123456
```

No User Manager:

```
/ tool user-manager customer add login="MikrotikBrasil" password="1234" permissions=owner  
/ tool user-manager router add subscriber=MikrotikBrasil ip-address=x.x.x.x shared-secret=123456  
/ tool user-manager user add username=demo password=demo subscriber=MikrotikBrasil ip-address=192.168.0.2
```

289

[MikrotikBrasil]
Routers & Wireless Systems

User Manager + Hotspot
(Solução única para Hotéis)



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 customer add login="MikrotikBrasil" password="1234" permissions=owner  
/ tool user-manager router add subscriber=MikrotikBrasil ip-address=10.5.50.1 shared-secret=123456  
/ tool user-manager user add username=demo password=demo subscriber=MikrotikBrasil
```

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

Em seguida pode-se criar planos e senhas em batch, fornecendo-as ao Hotel, de preferência gerenciadas por algum aplicativo simples em Windows.

290

Dúvidas ??

291

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 automaticamente 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 administrador.

292

ECMP



Este mecanismo de roteamento habilita o roteamento de pacotes em vários links com custo igual, assegurando um certo balanceamento de carga. Com ECMP podem ser usados mais de um gateway para um destino.

Com ECMP habilitado um novo gateway é escolhido para cada novo par de IP's origem/destino. Por exemplo uma conexão FTP é aberta para um servidor usará um link, enquanto que uma segunda conexão para outro servidor usará o próximo link.

As rotas ECMP podem ser criadas por protocolos de roteamento (RIP ou OSPF) ou adicionando uma rota estática com múltiplos gateways separados por vírgula. O tráfego pode ser ponderado entre links diferentes usando o mesmo gateway mais de uma vez. Por exemplo, se temos um link de 1 mega e outro de dois megas e queremos que os pacotes saiam nessa proporção, declaramos o gateway de 2 megas duas vezes.

293

ECMP



- ECMP não significa redundância, pois não cuida do estado dos links.
- ECMP não é um protocolo voltado à conexão, o que pode significar problemas de downloads interrompidos.

Para que o ECMP seja habilitado basta adicionar vários gateways para a mesma rota, por exemplo:

```
/ip route add gateway=192.168.0.1, 192.168.1.1, 192.168.1.1
```

No exemplo acima, indiretamente o gateway 192.168.1.1 terá "peso 2", ou seja de 3 pacotes, 1 irá pelo primeiro link e dois pelo segundo.

294

[MikrotikBrasil]
Routers & Wireless Systems

Exemplo de ECMP

Temos que rotear os pacotes da rede 192.168.0.0/24 por dois links distintos:

- 10.1.0.1 de 2 mbps
- 10.1.1.1 de 4 mbps

A solução para “balancear” o link é configurar um gateway com o primeiro link e dois com o segundo.

```
/ip route add gateway=10.1.0.1, 10.1.1.1, 10.1.1.1
```

295

[MikrotikBrasil]
Routers & Wireless Systems

Exemplo de ECMP

Temos que rotear os pacotes da rede 192.168.0.0/24 por dois links distintos:

- 10.1.0.1 de 2 mbps
- 10.1.1.1 de 4 mbps

A solução para “balancear” o link é configurar um gateway com o primeiro link e dois com o segundo.

```
/ip route add gateway=10.1.0.1, 10.1.1.1, 10.1.1.1
```

No Winbox :

296

[MikrotikBrasil]
Routers & Wireless Systems



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 possível utilizar política de roteamento quando se utiliza mascaramento (NAT)

297

[MikrotikBrasil]
Routers & Wireless Systems



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”.

298

[MikrotikBrasil]
Routers & Wireless Systems

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 automaticamente rotear para o GW_Backup.

[MikrotikBrasil]
Routers & Wireless Systems

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
```

[MikrotikBrasil]
Routers & Wireless Systems

Exemplo de Política de Roteamento

Com Winbox:

Three windows showing route configuration:

- Route <0.0.0.0/0>:
 - Destination: 0.0.0.0/0
 - Gateway: 10.0.0.2
 - Check Gateway: ping
 - Distance: 1
 - Mark: net1
 - Pref. Source: static
 - Interface: unknown
- Route <0.0.0.0/0>:
 - Destination: 0.0.0.0/0
 - Gateway: 10.0.0.3
 - Check Gateway: ping
 - Distance: 1
 - Mark: net2
 - Pref. Source: static
 - Interface: unknown
- Route <0.0.0.0/0>:
 - Destination: 0.0.0.0/0
 - Gateway: 10.0.0.1
 - Check Gateway: ping
 - Distance: 1
 - Mark: static
 - Pref. Source: static
 - Interface: unknown

301

[MikrotikBrasil]
Routers & Wireless Systems

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 dinâmico 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.

302

Reprodução não autorizada

[MikrotikBrasil]
Routers & Wireless Systems

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 Reachability Information) entre os AS's.

Ao contrário de outros protocolos, o BGP não se utiliza de métricas para encontrar o melhor caminho, mas sim de políticas administrativas.

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

303

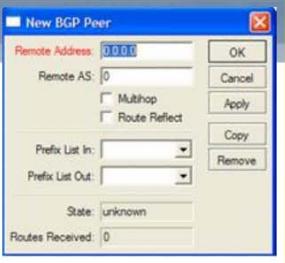
[MikrotikBrasil]
Routers & Wireless Systems

BGP - Settings

- AS: número do Autonomous System Number atribuído por uma entidade que gerencia esses números (No caso da América Latina, a LACNIC). Os números AS vão de 1 a 65356
- Router ID: string de identificação do Roteador, na forma de um número IP
- Redistribute Connected: Se o roteador deve distribuir as rotas a ele conectadas diretamente
- Redistribute Static: Se o roteador deve distribuir as rotas estáticas nele configuradas.
- Redistribute RIP: Se deve distribuir as rotas “aprendidas” por RIP
- Redistribute OSPF: Se deve distribuir as rotas aprendidas por OSPF

304

BGP - Peer



É necessário especificar pelo menos um Peer com o qual se quer trocar informações de roteamento, sendo que para a troca acontecer uma conexão TCP tem que ser estabelecida (porta179)

- Remote AS: número do AS remoto
- Multihop: Caso habilitada, essa opção permite sessões BGP mesmo em segmentos não diretamente conectados. Porém a sessão não será estabelecida caso a única rota para o endereço do Peer seja a rota default 0.0.0.0/0
- Route Reflect: route reflect é uma técnica para evitar que um roteador de um AS tenha que repassar as tabelas de roteamento para todos os roteadores internos ao AS permitindo que o que receber passe adiante, sem necessidade de um esquema "full mesh" (<http://www.faqs.org/rfcs/rfc2796.html>)

305

BGP - Peer



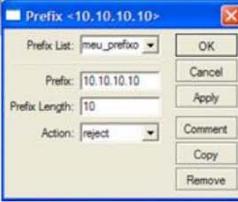
- Prefix List In: Nome da lista de prefixo para filtragem de pacotes entrantes.
- Prefix List Out: Nome da lista de prefixo para filtragem de pacotes entrantes "saintes".
- State: Mostra o estado do BGP
- Route Received: número de rotas recebidas de outros Peer's BGP

306

MikrotikBrasil
Routers & Wireless Systems



Prefix List



As listas de Prefixo podem ser adicionadas ao roteador com a opção /routing prefix-list add para que sejam usadas posteriormente pelos protocolos Rip ou pelo BGP

- Prefix List: Nome dado à lista de prefixo
- Prefixo: identificador da rede em forma de IP
- Prefix Length: tamanho do prefixo
- Action: Ação à ser tomada

307

MikrotikBrasil
Routers & Wireless Systems

OSPF



O protocolo **Open Shortest Path First** (Abra primeiro o caminho mais curto) é um protocolo do tipo "link-state". Ele usa o algoritmo 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 habilitado.

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>

308

[MikrotikBrasil]
Routers & Wireless Systems

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

309

[MikrotikBrasil]
Routers & Wireless Systems

OSPF Settings

OSPF Settings

Router ID: 0.0.0.0

Redistribute Default Route: never

Redistribute Connected Routes: no

Redistribute Static Routes: no

Redistribute RIP Routes: no

Redistribute BGP Routes: no

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

Redistribute Default Route: Especifica como deve ser distribuída 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

310

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 possível mudar o custo que serão exportadas as diversas rotas

311

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 algoritmo 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

312

[MikrotikBrasil]
Routers & Wireless Systems

Áreas “Stub” em OSPF

Áreas “Stub”

O OSPF permite que certas áreas sejam configuradas como áreas do tipo “stub” (áreas de topo)

Redes externas, cujas rotas são redistribuídas de outros protocolos para dentro do OSPF, não podem ser propagadas em uma área definida como “stub”.

O roteamento a partir dessas áreas para o mundo exterior é obrigatoriamente baseada em uma rota default.

A configuração de uma área como Stub, reduz as bases de dados que o OSPF precisa manter, exigindo consequentemente menos requisitos de memória dos roteadores dessas áreas.

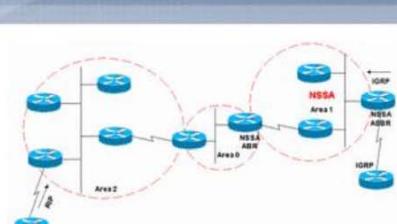
Mais detalhes em:
<http://www.cisco.com/warp/public/104/1.html#t31>

313

[MikrotikBrasil]
Routers & Wireless Systems

Áreas “NSSA” em OSPF

Áreas “NSSA”



A área chamada NSSA – “not-so-stubby area”, que pode ser traduzida por “área não assim tão stub”, ou “stub, pero no mucho” ☺ de acordo com a RFC 1587 é uma modificação no conceito de área stub que permite a injeção de rotas externas de uma forma controlada.

A redistribuição de rotas dentro de uma NSSA cria um tipo de anúncio de estado de link (LSA) chamado como tipo 7, que só pode existir em uma área NSSA, não podendo ser propagado pelo domínio todo do OSPF. Para que anúncios sejam propagáveis no domínio OSPF é necessário que eles sejam do tipo 5.

Um roteador de borda, que faz a comunicação entre um NSSA e outras áreas pode ou não propagar esses anúncios, dependendo de estar ou não configurado como “tradutor” do tipo 7 para o tipo 5.

314

[MikrotikBrasil]
Routers & Wireless Systems

Áreas “NSSA” em OSPF

No diagrama acima, se a área 1 é definida como uma área stub, as rotas IGRP não podem ser propagadas para dentro do domínio do OSPF porque áreas stub não permitem a propagação de rotas externas.

Porém se definirmos a área 1 como NSSA, as rotas IGRP poderão adentrar o OSPF e entrarão como do tipo 7, sendo propagadas para as outras áreas somente se a política do roteador de borda (NSSA ABR) assim permitir (e propagará como tipo 5).

Por outro lado as rotas RIP que entram na área 2 não serão permitidas na área 1. Áreas NSSA não permitem anúncios do tipo 5, agindo nesse caso como “stub’s”.

Mais detalhes em: <http://www.cisco.com/warp/public/104/nssa.html#intro>

315

[MikrotikBrasil]
Routers & Wireless Systems

Áreas de OSPF

- Name: nome a ser dado à Área
- Área ID: IP identificador da área. A área default com IP 0.0.0.0 é a área de backbone. O Backbone OSPF sempre contém todos os roteadores de borda das outras áreas, sendo o responsável por distribuir informações de roteamento à elas. Todas áreas tem de “tocar” logicamente o backbone, podendo ser por um link virtual.

316

[MikrotikBrasil]
Routers & Wireless Systems

Áreas de OSPF

-Type: tipo da área
→ stub: área configurada como “stub”
→ nssa: área configurada como “nssa”

-Translator Role:
→ translate never: nunca faz a tradução do tipo 7 para tipo 5.
→ translate always: faz sempre
→ translate candidate: pode ou não fazer a tradução

Maiores informações no artigo
<http://www.cisco.com/warp/public/104/nssa.html#intro>

317

[MikrotikBrasil]
Routers & Wireless Systems

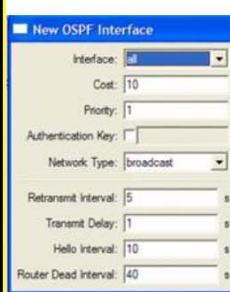
Rede OSPF

Define-se aqui a Rede OSPF, com os seguintes parâmetros:

- 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.

318

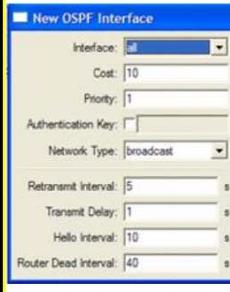


OSPF - Interface

Para simplesmente rodar o OSPF, não é necessário qualquer configuração da Interface. Essa facilidade existe no RouterOS para um refino mais aprofundado das propriedades do OSPF.

- Interface: Interface onde vai rodar o OSPF
- Cost: custo da Interface (métrica)
- Priority: roteadores com esse valor mais alto terão prioridade sobre outros
- authentication key: senha de autenticação (texto) caso os roteadores estejam usando autenticação.
- Network Type: tipo da rede
 - ponto a ponto
 - multiponto
 - Broadcast: tipicamente Ethernet
 - nbma (non broadcast multiple address): tipicamente Frame Relay e X25

319



OSPF - Interface

→ **Retransmit Interval**: tempo entre anuncios de perda de link. Quando um roteador manda um anuncio de estado de link (LSA) para seu vizinho, ele mantém o LSA até que receba de volta a confirmação (acknowledgment). Caso não receba em tempo, retransmite o LSA. O valor recomendado para redes Broadcast é 5 segundos e para ponto a ponto 10 segundos.

→ **Transmit Delay**: intervalo de tempo para transmissão de LSA.

→ **Hello Interval**: Intervalo de tempo entre os pacotes "hello" que o roteador manda na interface. Quanto menor o intervalo hello, mais rápidas serão detectadas as modificações na topologia da rede, com o consequente aumento do tráfego. Este valor obrigatoriamente deve ser o mesmo em cada adjacência.

→ **Router Dead Interval**: Especifica o intervalo de tempo após o qual um vizinho é considerado "morto". O intervalo é anunciado nos pacotes hello e seu valor tem de ser obrigatoriamente o mesmo para todos os roteadores da rede.

i

OSPF – Virtual Link

Conforme estabelecido na RFC do OSPF, a área de backbone deve ser contígua. No entanto é possível definir áreas de forma que o backbone não seja contíguo, porém com a conectividade assegurada por links virtuais.

Os links virtuais podem ser configurados entre dois roteadores através de uma área comum chamada de área transito, sendo que uma das áreas interligadas deve tocar fisicamente o backbone.

O protocolo trata dois roteadores ligados por um link virtual como se estivessem ligados por uma rede ponto a ponto não numerada.

Os parâmetros de configuração são:

- Neighbor ID: IP do roteador vizinho
- Transit Area: Área de transito

OBS: não é possível fazer links virtuais entre áreas "stub" 321

Router ID	Address	State	State Changes
10.6.0.1	10.2.0.5	Full	4
10.7.0.3	10.7.0.3	2-Way	2
10.7.0.7	10.7.0.7	2-Way	4
10.7.0.10	10.2.0.6	2-Way	0
10.7.0.11	10.7.0.11	2-Way	3
10.7.0.12	10.7.0.12	2-Way	19
10.7.0.99	10.7.0.99	2-Way	2
10.7.0.100	10.7.0.100	2-Way	5
10.7.0.101	10.7.0.101	2-Way	3
10.7.0.108	10.7.0.108	Full	5
10.7.0.254	10.7.0.254	Full	5

OSPF – Neighbors

Conforme estabelecido na RFC do OSPF, a área de backbone deve ser contígua. No entanto é possível definir áreas de forma que o backbone não seja contíguo, porém com a conectividade assegurada por links virtuais.

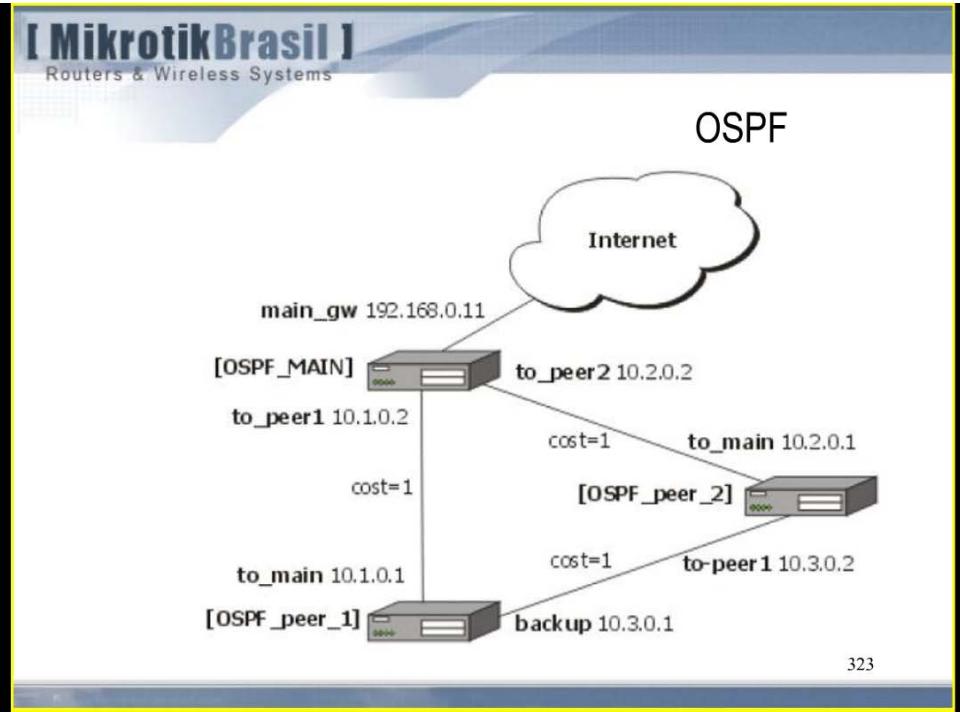
Os links virtuais podem ser configurados entre dois roteadores através de uma área comum chamada de área transito, sendo que uma das áreas interligadas deve tocar fisicamente o backbone.

O protocolo trata dois roteadores ligados por um link virtual como se estivessem ligados por uma rede ponto a ponto não numerada.

Os parâmetros de configuração são:

- Neighbor ID: IP do roteador vizinho
- Transit Area: Área de transito

OBS: não é possível fazer links virtuais entre áreas "stub" 322



323



324

OSPF

Setar distribute-default como if-installed-as-type-2, redistribute-connected como as-type-1 e redistribute-static como as-type-2. Metric-connected, metric-static, metric-rip, metric-bgp deixar como zero.

```
[admin@OSPF_MAIN] routing ospf> print
router-id: 0.0.0.0
distribute-default: if-installed-as-type-2
redistribute-connected: as-type-1
redistribute-static: as-type-2
redistribute-rip: no
redistribute-bgp: no
metric-default: 1
metric-connected: 0
metric-static: 0
metric-rip: 0
metric-bgp:
```

325

OSPF

Defina nova área OSPF de nome local_10 com área id = 0.0.0.1

```
[admin@OSPF_MAIN] routing ospf area> print
Flags: X - disabled, I - invalid
#
#      NAME          AREA-ID
0      backbone      0.0.0.0
1      local_10      0.0.0.1 no 1
```

Adicione as redes conectadas com a área local_ao na rede OSPF:

```
[admin@OSPF_MAIN] routing ospf network> print
```

Flags: X - disabled, I - invalid

```
#
#      NETWORK        AREA
0      10.1.0.0/24   local_10
1      10.2.0.0/24   local_10
```

326

[MikrotikBrasil]
Routers & Wireless Systems

OSPF

No Peer-1 configure redistribute-connected as as-type-1 e Metric-connected, metric-static, metric-rip, metric-bgp como zero.

```
[admin@OSPF_peer_1] routing ospf> print
router-id: 0.0.0.0
distribute-default: never
redistribute-connected: as-type-1
redistribute-static: no
redistribute-rip: no
redistribute-bgp: no
metric-default: 1
metric-connected: 0
metric-static: 0
metric-rip: 0
metric-bgp: 0
```

Adicione a mesma área local_10 nesse roteador. Siga os mesmos procedimentos para o Peer2

[MikrotikBrasil]
Routers & Wireless Systems

OSPF

```
(admin@OSPF MAIN] ip route> print
Flags: X - disabled, I - invalid, D - dynamic, J - rejected,
C - connect, S - static, r - rip, o - ospf, b - bgp
# DST-ADDRESS          G GATEWAY          DISTANCE INTERFACE
0 Io 192.168.0.0/24      110
1 DC 192.168.0.0/24      r 0.0.0.0      0      main_gw
2 Do 10.3.0.0/24         r 10.2.0.1     110      to_peer_2
                           r 10.1.0.1
3 Io 10.2.0.0/24         110
4 DC 10.2.0.0/24         r 0.0.0.0      0      to_peer_2
5 Io 10.1.0.0/24         110
6 DC 10.1.0.0/24         r 0.0.0.0      0      to_peer_1
```

[MikrotikBrasil]
Routers & Wireless Systems

OSPF

```
[admin@OSPF peer 1] ip route> print
Flags: X - disabled, I - invalid, D - dynamic, J - rejected,
C - connect, S - static, r - rip, o - ospf, b - bgp
#      DST-ADDRESS      G GATEWAY          DISTANCE INTERFACE
0 Do 192.168.0.0/24    r 10.1.0.2          110      to_main
1 Io 10.1.0.0/24           110
2 DC 10.3.0.0/24    r 0.0.0.0          0      backup
3 Do 10.2.0.0/24    r 10.1.0.2          110      to_main
4 Io 10.1.0.0/24    r 10.3.0.2          110      backup
5 DC 10.1.0.0/24    r 0.0.0.0          0      to_main
-----
```

329

[MikrotikBrasil]
Routers & Wireless Systems

OSPF

```
[admin@OSPF peer 2] ip route> print
Flags: X - disabled, I - invalid, D - dynamic, J - rejected,
C - connect, S - static, r - rip, o - ospf, b - bgp
#      DST-ADDRESS      G GATEWAY          DISTANCE INTERFACE
0 Do 192.168.0.0/24    r 10.2.0.2          110      to_main
1 Io 10.3.0.0/24           110
2 DC 10.3.0.0/24    r 0.0.0.0          0      to_peer_1
3 Io 10.2.0.0/24           110
4 DC 10.2.0.0/24    r 0.0.0.0          0      to_main
5 Do 10.1.0.0/24    r 10.3.0.1          110      to_peer_1
                           r 10.2.0.2          110      to_main
```

330

[MikrotikBrasil]
Routers & Wireless Systems

OSPF

331

[MikrotikBrasil]
Routers & Wireless Systems

OSPF

We should change cost value in both routers: OSPF_peer_1 and OSPF_peer_2 to 50. To do this, we need to add a following interface:

```

[admin@OSPF_peer_1] routing ospf interface> add interface=backup cost=50
[admin@OSPF_peer_1] routing ospf interface> print
  0 interface=backup cost=50 priority=1 authentication-key=""
    retransmit-interval=5s transmit-delay=1s hello-interval=10s
    dead-interval=40s

[admin@OSPF_peer_2] routing ospf interface> add interface=to_peer_1 cost=50
[admin@OSPF_peer_2] routing ospf interface> print
  0 interface=to_peer_1 cost=50 priority=1 authentication-key=""
    retransmit-interval=5s transmit-delay=1s hello-interval=10s
    dead-interval=40s

```

332

[MikrotikBrasil]
Routers & Wireless Systems

Dúvidas ??

333

[MikrotikBrasil]
Routers & Wireless Systems

Scripting Host e Ferramentas
Complementares do
Mikrotik



334

[MikrotikBrasil]
Routers & Wireless Systems

Scripting Host



O Mikrotik possui uma poderosa linguagem interna de Scripts com a qual diversas ações e tarefas de manutenção podem ser executadas a partir da ocorrência de eventos diversos.

Os scripts podem ser executados tanto pelo agendador de tarefas como por outras ferramentas como o monitoramento de tráfego e o netwatch.

Os comandos de configuração são comandos padrão do RouterOS e as expressões são precedidas de ":" a acessíveis de todos os sub-menus.

335

[MikrotikBrasil]
Routers & Wireless Systems

Scripting Host - Variáveis



O Mikrotik RouterOS suporta dois tipos de variáveis – globais (disponíveis para todo o sistema) e locais (acessível somente ao contexto do script). Uma variável pode ser referenciada pelo símbolo de '\$', seguido pelo nome da variável, com exceção dos comandos **set** e **unset** que tomam o nome da variável sem o '\$'.

Os nomes das variáveis podem ser compostos de letras, números e do símbolo '-'. Toda variável deve ser obrigatoriamente declarada antes de ser utilizada nos scripts.

Existem 4 tipos de declarações que podem ser feitas:

global – variáveis globais podem ser acessadas por todos os scripts e logins de console no mesmo roteador. Entretanto elas não são mantidas depois de reboots

local – variáveis declaradas como locais não são compartilhadas com outros scripts e seu valor é perdido sempre que o script é finalizado.

336

[MikrotikBrasil]
Routers & Wireless Systems



Scripting Host - Variáveis

As variáveis também podem ser declaradas como:

variáveis indexadoras de loop – definidas dentro de uma declaração **for** e **foreach**, essas variáveis são utilizadas apenas para um bloco **do** de comandos e são removidas quando o comando é completado.

variáveis de monitor – alguns comandos **monitor** que tem uma parte **do** também podem introduzir variáveis.

Para obter uma lista de variáveis disponíveis use o comando **:environment print**

É possível atribuir um novo valor a uma variável dentro do script usando o comando **:set** seguido do nome da variável sem o \$ e o novo valor. Também pode-se eliminar uma variável com **:unset**. Nesse caso, se a variável é local, é perdida e se é global fica mantida, porém inacessível pelo script corrente.

337

[MikrotikBrasil]
Routers & Wireless Systems



Scripting Host - Variáveis

```
[admin@Hotspot] > :global variavel-global "abcd"  
[admin@Hotspot] > :local variavel-local "1234"  
[admin@Hotspot] > :put $variavel-global  
abcd  
[admin@Hotspot] > :put $variavel-local  
1234  
[admin@Hotspot] > :environment print  
Global Variables  
variavel-global=abcd  
Local Variables  
variavel-local=1234
```

338



Scripting Host
Inserindo os Scripts

Os scripts ficam armazenados em /system script. As propriedades são as seguintes:

- Name: nome que vai ser chamado o script
- Policy: são as políticas de segurança aplicáveis
- Run Count: quantas vezes o script rodou. Valor volátil quando o roteador é reiniciado.
- Owner: usuário criador do script
- Last Time Started: Data e hora da última execução do script
- A Facilidade JOB é utilizada para manipular tarefas ativas o que estejam previamente agendadas em /system scheduler

339



Scripting Host
Exemplos

Façamos um script simples para monitorar o estado de uma interface de rede ether1 a cada 10 segundos e fazer com que seja mandado para o log qualquer inatividade desta.

Script para monitorar:

```
:global estado-da-interface;
/interface ethernet monitor ether1 once do={:set
estado-da-interface $status;
:if ($status="no link") do={log message="O link
caiu!!!!";}
```



340

[MikrotikBrasil]
Routers & Wireless Systems

Scripting Host Exemplos

Em seguida colocamos no Agendador de Tarefas para que dispare o script Monitora_Lan a cada 10 segundos. Equivalente na linha de comando:

```
/ system script
add name="Monitora_Lan" source="{:global estado-da-interface;/interface ethernet
monitor ether1 once do={:set estado-da-interface $status};:if(!($status=no-link) do={log
message="O link caiu!!!!" }"

/scheduler
add name="Monitora_Lan" on-event=Monitora_Lan start-date=jan/01/1970 start-
time=00:00:00 interval=10s comment="" disabled=no
```

Para popular a tabela ARP

```
/ system script
add name="popula_ARP" code=":{foreach i in [/ip arp find dynamic=yes interface=wlan1]
do={ /ip arp add copy-from=$i }"

/scheduler
add name="popula_ARP" on-event=Monitora_Lan start-date=jan/01/1970 start-
time=00:00:00 interval=1d comment="" disabled=no
```

342

[MikrotikBrasil]
Routers & Wireless Systems

Scripting Host
Exemplos

Scripts que podem ser baixados em <http://wiki.mikrotik.com/wiki/Scripts>

- Filter a command output
- Enable and Disable P2P connections
- [Send Backup email](#)
- Limiting a user to a given amount of traffic (using firewall)
- Limiting a user to a given amount of traffic II (using queues)
- Limiting a user to a given amount of traffic with user levels (using queues)
- Generate bogons firewall chain based on routing-marks
- Generate routes for stress testing BGP functionality
- Set global and local variables
- Dynamic DNS Update Script for ChangelP.com
- Reset Hotspot user count
- Use SSH to execute commands (DSA key login)
- Audible signal test
- ECMP Failover Script
- Sending text out over a serial port
- Setting static DNS record for each DHCP lease
- Improved Netwatch

343

[MikrotikBrasil]
Routers & Wireless Systems



SCRIPTS - ANEXOS

Comandos e Operadores

344

[MikrotikBrasil]
Routers & Wireless Systems

Scripting Host – Comandos e valores de retorno



Alguns comandos são úteis quando os resultados de suas saídas podem ser utilizados como argumentos em outros comandos. Os valores de retorno de comandos no entanto não aparecem na tela do terminal e para serem obtidos devem ser colocados entre colchetes []. Após a execução o valor de retorno do comando será o valor do conteúdo desses colchetes. Esse procedimento é chamado de substituição de comando.

Entre os comandos que produzem valores de retorno estão:

- **find**: retorna uma referência a um ítem em particular
- **ping** retorna o número de pings com sucesso,
- **time** retorna o tempo,
- **inc** e **decr** retornam o novo valor de uma variável
- **add** que retorna o número interno de um ítem novo criado.

345

[MikrotikBrasil]
Routers & Wireless Systems

Scripting Host – Comandos e valores de retorno



Exemplo de utilização de find:

```
[admin@Hotspot] >
[admin@Hotspot] > /interface
[admin@Hotspot] interface> find type=ether
[admin@Hotspot] interface>
[admin@Hotspot] interface> :put [find type=ether]
*1
[admin@Hotspot] interface>
```

Exemplo de um comando servindo de argumento para outro:

```
[admin@Hotspot] interface> enable [find type=ether]
[admin@Hotspot] interface>
```

346

MikrotikBrasil
Routers & Wireless Systems



Scripting Host – Operadores

Na console do RouterOS podem ser feitos cálculos simples com números, endereços IP's, Strings e listas. Para obter o resultado de uma expressão coloque os argumentos entre parenteses

- → menos unário – inverte o sinal de um dado valor.
- → menos binário – subtrai dois números, dois IP's ou um IP e um número
- ! → NOT – NÃO lógico. Operador unário que inverte um dado valor booleano
- / → divisão. Operador Binário – divide um número por outro (dá um número como resultado) ou divide um tempo por um número (dá um tempo como resultado).
- . → concatenação. Operador Binário – concatena 2 strings ou anexa uma lista a outra, ou ainda anexa um elemento à uma lista.
- ^ → operador XOR (OU exclusivo). Os argumentos e os resultados são endereços IP
- ~ → inversão de bit. Operador unário que inverte bits em um endereço IP
- * → multiplicação. Operador Binário, que pode multiplicar dois números ou um valor de tempo por um número

347

MikrotikBrasil
Routers & Wireless Systems



Scripting Host – Operadores

- & → bitwise AND (E). Os argumentos e resultados são endereços IP
- && → AND (operador booleano E). Operador Binário – os argumentos e resultados são valores lógicos.
- + → mais binário. Adiciona dois números, dois valores de tempo um número e um endereço IP.
- < → menor. Operador Binário que compara dois números, dois valores de tempo ou dois IP's. Retorna um valor booleano.
- << → deslocamento à esquerda. Operador Binário que desloca um endereço IP com um dado tamanho de bits. O primeiro argumento é o IP e o segundo um inteiro. O resultado é outro IP
- <= → menor ou igual. Operador Binário que compara 2 números ou 2 valores de tempo ou dois IP's. O resultado é um valor booleano.
- > → maior. Operador Binário que compara 2 números, ou 2 valores de tempo ou dois IP's, retornando um valor booleano
- >= → maior ou igual. Operador Binário que compara 2 números, ou 2 valores de tempo ou dois IP's, retornando um valor booleano
- >> - deslocamento à direita. Operador Binário que desloca um endereço IP com um dado tamanho de bits. O primeiro argumento é o IP e o segundo um inteiro. O resultado é outro IP
- | - bitwise OR. Os argumentos e resultados são ambos endereços IP
- || - OR (operador booleano OU). Operador Binário. Os argumentos e resultados são valores lógicos.

348

[MikrotikBrasil]
Routers & Wireless Systems

Scripting Host – Operadores



Exemplos:

Ordem de operadores e de avaliação:

```
[admin@MikroTik] ip firewall rule forward> :put (10+1-6*2=11-12=2+(-3)=-1)
false
[admin@MikroTik] ip firewall rule forward> :put (10+1-6*2=11-12=(2+(-3)=-1))
true
[admin@MikroTik] ip firewall rule forward
```

NÃO lógico

```
[admin@MikroTik] interface> :put (!true)
false
[admin@MikroTik] interface> :put (!(2>3))
true
[admin@MikroTik] interface>
```

349

[MikrotikBrasil]
Routers & Wireless Systems

Scripting Host – Operadores



Exemplos:

Inversão de bits

```
[admin@MikroTik] interface> :put (~255.255.0.0)
0.0.255.255
[admin@MikroTik] interface>
```

Soma

```
[admin@MikroTik] interface> :put (3ms + 5s)
00:00:05.003
[admin@MikroTik] interface> :put (10.0.0.15 + 0.0.10.0)
cannot add ip address to ip address
[admin@MikroTik] interface> :put (10.0.0.15 + 10)
10.0.0.25
[admin@MikroTik] interface>
```

350

[MikrotikBrasil]
Routers & Wireless Systems



Scripting Host – Comandos

O RouterOS apresenta vários comandos internos de console e expressões (ICE) que não dependem de qual diretório se esteja no menu.

Esses comandos não mudam as configurações diretamente, mas são úteis para automatizar vários processos de manutenção.

A lista completa das ICE pode ser acessada digitando : e em seguida dois tab's

```
[admin@Hotspot] interface> :
```

```
beep      execute global local put toarray tonum while
delay     find if log resolve tobool tostr
do        for len nothing set toid totime
environment foreach list pick time toip typeof
```

351

[MikrotikBrasil]
Routers & Wireless Systems



Scripting Host – Comandos

list – lista todos comandos
resolve – faz uma busca por um nome de domínio
execute – roda um script em separado
local – atribui um valor para uma variável local
global – declara e atribui um valor para uma variável global
set – Muda as propriedades do item
put – apresenta os argumentos na tela
while – executa um comando enquanto uma condição é verdadeira
if – executa um comando se uma condição é verdadeira
do – executa um comando
time – retorna o tempo que um comando levou para ser executado
for – executa um comando para um range de valores inteiros
foreach – executa um comando para cada um dos argumentos de uma lista
delay – pausa a execução por um determinado tempo

352

[MikrotikBrasil]
Routers & Wireless Systems



Scripting Host – Comandos

typeof – retorna o tipo do valor
len – retorna o número de elementos no valor
tostr – converte um argumento para uma string
tobool – converte um argumento para verdadeiro
tonum – converte um argumento para um valor inteiro
totime – converte um argumento para um valor de intervalo de tempo
toip -- converte um argumento para um endereço IP
toarray – converte um argumento para um valor de array
nothing – não faz nada e não retorna nada – comando extremamente útil 😊
pick – retorna um range de caracteres de strings ou valores de arrays
find – Localiza items pelo valor
log – manda mensagem para os logs
beep – produz um sinal audível se for suportado hardware.
environment/ -- lista de todas as variáveis

353

[MikrotikBrasil]
Routers & Wireless Systems



Scripting Host – Comandos Especiais

Monitor
É possível acessar valores que são mostrados pela maioria das ações **monitor**, através dos Scripts. Um comando **monitor** que tem um parametro **do** pode ser fornecido tanto pelo nome do script (**/system scripts**), ou pela execução de comandos de console.

Get
A maior parte dos comandos **print** produzem valores que são acessíveis a partir dos scripts. Esses comandos **print** tem um correspondente comando **get** no mesmo nível de menu. O comando **get** aceita um parametro quando trabalhando com números regulares ou dois parametros quando trabalhando com listas

354

[MikrotikBrasil]
Routers & Wireless Systems

Scripting Host
Caracteres Especiais



→ # é usado como comentário. Linha é ignorada
→ ; usado para colocar múltiplos comandos em uma só linha
→ Caso se precise usar os caracteres especiais {}"\'\$, como strings normais, eles devem ser precedidos de uma barra \. Exemplo \\, significa o caractere \
→ \a campainha, código do caractere 7
→ \b backspace, código do caractere 8
→ \f alimentação de página, código do caractere 12
→ \n nova linha, código do caractere 10
→ \r enter, código do caractere 13
→ \t tabulação, código do caractere 9
→ \v tabulação vertical, código do caractere 11
→ _ espaço, código do caractere 32

355

[MikrotikBrasil]
Routers & Wireless Systems



Monitoramento da Rede - Netwatch



A Ferramenta Netwatch monitora o estado de hosts da rede, mandando pacotes de ping's para uma lista de endereços IP especificados.

É possível especificar para cada IP, intervalos de ping e scripts de console, possibilitando assim que sejam feitas ações em função da mudança de estado de hosts.

356

[MikrotikBrasil]
Routers & Wireless Systems

Monitoramento da Rede - Netwatch

→ Host: Endereço IP do host que será monitorado

→ Interval: Intervalo em que o host será “pingado”. Por default 1 segundo.

→ Timeout: Se nenhuma resposta for recebida nesse tempo, o host será considerado “down”.

→ Na aba Up, deve ser colocado o nome do script de console que será executado quando o estado do host **mudar** de “desconhecido” ou down para up.

→ Na aba Down, deve ser colocado o nome do script de console que será executado quando o estado do host **mudar** de “desconhecido” ou up para down

357

[MikrotikBrasil]
Routers & Wireless Systems

Monitoramento da Rede - Netwatch

O estado dos hosts pode ser visto acima:

→ Status: up, down ou unknown (desconhecido)

→ Since: Indica quando o estado do host mudou pela última vez.

É importante conhecer o nome exato das variáveis de mudança de estado, pois elas serão usadas na lógica dos scripts:

→ up-script: nome do script que é executado quando o estado muda para up

→ down-script: nome do script que é executado quando o estado muda para down

358

[MikrotikBrasil]
Routers & Wireless Systems



Exemplo de aplicação de Netwatch

Queremos que um o gateway default de uma rede seja alterado, caso o gateway em uso tenha problemas

```
[admin@MikroTik] system script> add name=gw_1 source={/ip route set { [/ip route find dst 0.0.0.0] gateway 10.0.0.1}}
```

```
[admin@MikroTik] system script> add name=gw_2 source={/ip route set {[/ip route find dst 0.0.0.0] gateway 10.0.0.217}}
```

```
[admin@MikroTik] system script> /tool netwatch
```

```
[admin@MikroTik] tool netwatch> add host=10.0.0.217 interval=10s timeout=998ms up-script=gw_2 down-script=gw_1
```

359

[MikrotikBrasil]
Routers & Wireless Systems



Monitor de Porta Serial - Sigwatch

O utilitário “Sigwatch” permite o monitoramento do estado da porta serial, gerando eventos no sistema quando há alteração do estado destas. O acesso a essa facilidade somente pode ser feito pelo Terminal, não estando disponível no Winbox.

Os parametros a configurar são:

- **name**: nome do ítem a ser monitorado pelo Sigwatch
- **on-condition**: em qual situação deve ser tomada alguma ação para esse ítem (default =on):
 - **on**: dispara se o estado do pino muda para ativo
 - **off**: dispara quando o estado do pino muda para inativo
 - **change**: dispara sempre que o estado do pino muda.

360

[MikrotikBrasil]
Routers & Wireless Systems



Monitor de Porta Serial - Sigwatch

→ **port**: nome da porta serial a monitorar

→ **script**: nome do script a disparar para esse ítem

→ **signal**: nome do sinal ou número do pino (para DB9 padrão) a monitorar (default=rts)

- **dtr**: Data Terminal Ready (pino 4)
- **rts**: Request to Send (pino 7)
- **cts**: Clear to Send (pino 8)
- **dcd**: Data Carrier Detect (pino 1)
- **ri**: Ring Indicator (pino 9)
- **dsr**: Data Set Ready (pino 6)

361

[MikrotikBrasil]
Routers & Wireless Systems



Monitor de Porta Serial - Sigwatch

→ **state**: último estado do sinal monitorado

→ **log**: (yes|no): se deve ser adicionada uma mensagem na forma *name-of-sigwatch-item*:
signal changed [to high | to low] à facilidade do System-Info sempre que esse ítem do sigwatch for disparado (default=no)

→ **count**: contador (só leitura) que indica o número de vezes que sigwatch foi ativado. Zera quando o roteador é reiniciado

OBS: O Sigwatch pode disparar um script previamente colocado em system/scripts ou seu código fonte pode ser digitado diretamente na linha de chamada do script.

362

[MikrotikBrasil]
Routers & Wireless Systems

Monitor de Porta Serial - Sigwatch



Exemplo: Desejamos monitorar se na porta serial1 do Roteador há sinal de CTS.

```
[admin@Hotspot] tool sigwatch> add name="monitor_da_serial" port=serial0 pin=8 on-condition=change log=no
```

363

[MikrotikBrasil]
Routers & Wireless Systems

Traffic Monitor



A ferramenta "traffic monitor" é utilizada para executar scripts de console, sempre que o tráfego em uma dada interface ultrapasse um valor determinado.

Parametros de configuração:

- Name: Nome do ítem
- Interface: Interface que será monitorada
- Traffic: se é tráfego transmitido ou recebido
- Threshold: limite em bps que dispara o gatilho
- Trigger: Se o gatilho é disparado quando o valor ultrapassa o Threshold ou cai abaixo ou o somente atinge (subindo ou descendo)
- On Event: script a ser executado.

New Traffic Monitor

Name: <input type="text" value="mon1"/>
Interface: <input type="text" value="ether1"/>
Traffic: <input checked="" type="radio"/> transmitted <input type="radio"/> received
Trigger: <input checked="" type="radio"/> above <input type="radio"/> below <input type="radio"/> always
Threshold: <input type="text" value="0"/>
On Event:

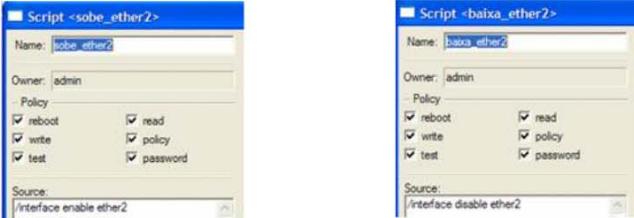
364

[MikrotikBrasil]
Routers & Wireless Systems

Traffic Monitor

Exemplo: Queremos monitorar o tráfego entrante em um roteador com duas interfaces de rede ether1 e ether2. Quando o tráfego exceder 15kbps na ether1 vamos habilitar a ether2, que será desabilitada quando o tráfego recuar para menos de 12kbps

- Primeiro vamos criar os scripts de subida e descida

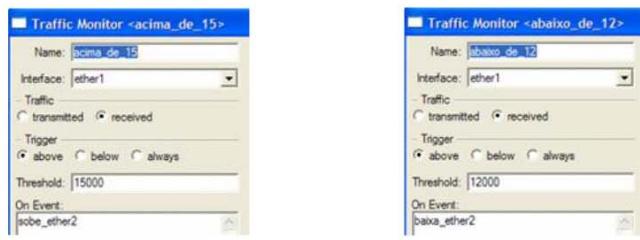


365

[MikrotikBrasil]
Routers & Wireless Systems

Traffic Monitor

Agora vamos definir as ações: quando o tráfego passa de 15kbps ativa a interface, mas só quando cai abaixo de 12 kbps é que desabilita



366



Traffic Monitor

Vamos conferir como ficou na linha de comando:

```
/ system script  
  
add name="sobe_ether2" source="/interface enable ether2"  
add name="baixa_ether2" source="/interface disable ether2  
  
/ tool traffic-monitor  
  
add name="acima_de_15" interface=ether1 traffic=received trigger=above  
threshold=15000 on-event=sobe_ether2  
  
add name="abaixo_de_12" interface=ether1 traffic=received trigger=above  
threshold=12000 on-event=baixa_ether2
```

367

Dúvidas ??

368

WEB - Proxy



369

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 poderá também criar filtros de acesso a conteúdo indesejável, tornando a navegação mais segura aos clientes.

370

[MikrotikBrasil]
Routers & Wireless Systems

WEB - Proxy

O MikroTik RouterOS implementa um web-proxy com as seguintes características:

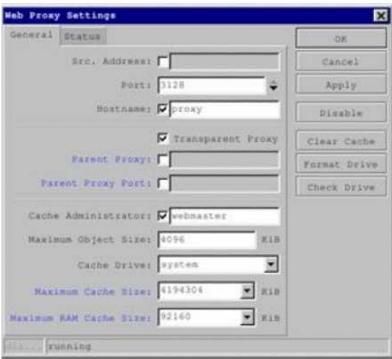
- HTTP proxy
- Transparent proxy. Onde é transparente e HTPP ao mesmo tempo
- Lista de Acesso por origem, destino, URL e métodos de requisição
- Lista de Acesso Cache (especifica os objetos que poderão ou não ser "cacheados")
- Lista de Acesso Direto (especifica quais recursos deverão ser acessados diretamente e também através de outro web-proxy)
- Sistema de Logging

371

[MikrotikBrasil]
Routers & Wireless Systems

WEB - Proxy

Web-Proxy configurado para 4 GiB de cache, escutando na porta 3128:



The screenshot shows the 'Web Proxy Settings' dialog box. Under the 'General' tab, the 'Bind Address' is set to an empty field, 'Port' is set to 3128, and 'Hostname' is set to 'proxy'. The 'Transparent Proxy' checkbox is checked. Under the 'Cache' tab, 'Cache Administrator' is set to 'webmaster', 'Maximum Object Size' is 4096 KIB, 'Cache Drive' is 'system', 'Maximum Cache Size' is 4194304 KIB, and 'Maximum RAM Cache Size' is 92160 KIB. Buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Clear Cache', 'Format Drive', and 'Check Drive' are visible.

- Clear Cache – Serve para esvaziar o cache armazenado (dependendo do tamaho do cache esta opção poderá ser bastante lenta).
- Check Drive – Verifica a integridade da mídia de armazenamento, procurando por "Bad Blocks".
- Enable/Disable – Utilizado para habilitar ou desabilitar o web-proxy.

372

[MikrotikBrasil]

Routers & Wireless Systems

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.
- Port – A porta onde o web-proxy escutará.
- Hostname – Um nome de host para ser exibido no caso de avisos emitidos aos clientes.
- Transparent Proxy – Habilita transparente proxy
- Parent Proxy – Utilizado para indicar o IP de outro servidor proxy numa hierarquia de proxy.
- Parent Proxy Port – Porta onde o web-proxy escuta no Parent.

373

[MikrotikBrasil]

Routers & Wireless Systems

WEB - Proxy

- Cache Administrator -Um nome ou endereço de e-mail para exibição no caso de avisos emitidos aos clientes.
- Maximum Object Size – O tamanho máximo de um objeto armazenado no cache. Se você deseja aumentar a velocidade mais do que deseja economizar banda, é aconselhável manter este valor baixo.
- Cache Drive – A mídia onde o web-proxy armazenará o cache. Em caso de apenas uma mídia instalada no sistema será SYSTEM. Quando utilizado uma mídia secundária, a opção a escolher na lista suspensa é SECONDARY. Quando utilizando esta opção, deveremos utilizar o botão FORMAT DRIVE.

374

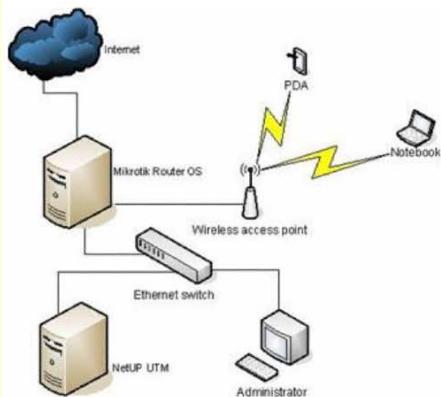
WEB - Proxy

- Maximum Cache Size – Tamanho máximo que o cache atingirá.
- Maximum RAM Cache Size – O tamanho máximo da RAM que o web-proxy alocara para utilização do web-proxy.
- OBS. - Vale lembrar que, em média, cada GB de cache necessita de 15 a 20 MB de RAM, então basta fazermos os cálculos no momento de configurar o sistema.
- Lembramos também que o Mikrotik RouterOS na versão 2.9.x suporta até 1 GB de RAM.

375

WEB - Proxy

Status do Web-Proxy



status (read-only: text; default: stopped) – exibe as informações do servidor web-proxy.

stopped - web-proxy está inativo.

rebuilding-cache – o web-proxy está ativo e operando. O conteúdo armazenado (cache) está em verificação.

running - web-proxy está ativo e operando.

stopping - web-proxy entrando em modo inativo (max 10s).

clearing-cache - web-proxy está inativo, e os arquivos do cache serão removidos.

376

[MikrotikBrasil]
Routers & Wireless Systems

WEB - Proxy

Status do Web-Proxy

status (read-only: text; default: stopped) – exibe as informações do servidor web-proxy.

stopped - web-proxy está inativo.

rebuilding-cache – o web-proxy está ativo e operando. O conteúdo armazenado (cache) está em verificação.

running - web-proxy está ativo e operando.

377

[MikrotikBrasil]
Routers & Wireless Systems

WEB - Proxy

Status do Web-Proxy

stopping - web-proxy entrando em modo inativo (max 10s).

clearing-cache - web-proxy está inativo, e os arquivos do cache serão removidos.

creating-cache - web-proxy está inativo e a estrutura do cache está em criação.

dns-missing - web-proxy está ativo, mas não está rodando porque o DNS é desconhecido ou não foi configurado apropriadamente.

378

[MikrotikBrasil]
Routers & Wireless Systems

WEB - Proxy

- creating-cache - web-proxy está inativo e a estrutura do cache está em criação.
- dns-missing - web-proxy está ativo, mas não está rodando porque o DNS é desconhecido ou não foi configurado apropriadamente.
- invalid-address - web-proxy está ativo, mas não está rodando porque o endereço IP ou a porta configurados são inválidos.
- invalid-cache-administrator - web-proxy está ativo, mas não está rodando porque o Cache-Administrator configurado é inválido.
- invalid-hostname – web-proxy está ativo, mas não está rodando porque o hostname configurado é inválido. Deverá ser consultado o log do sistema. Este erro deverá ser enviado a Mikrotik Latvia.
- reserved-for-cache (integer) – tamanho máximo do cache acessível ao web-proxy.

379

[MikrotikBrasil]
Routers & Wireless Systems

WEB - Proxy

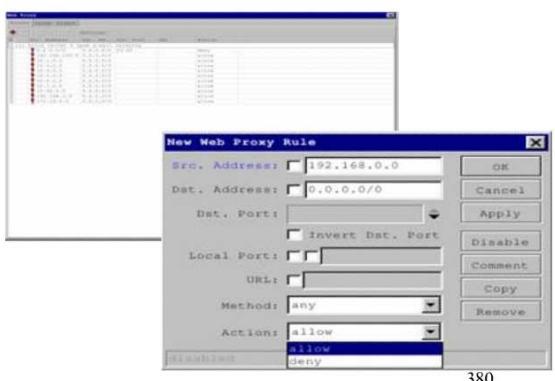
Access List

Submenu: /ip web-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

action (allow | deny; default: allow) – especifica a ação de negar ou liberar os pacotes que chegam ao web-proxy.



380

WEB - Proxy

- 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..
- method (any | connect | delete | get | head | options | post | put | trace) – Método HTTP usado nas requisições (veja a seção Métodos HTTP no final deste documento).
- src-address (IP address/netmask) – endereço IP de origem do pacote.
- url (wildcard) – A URL da requisição HTTP.
- Nota:
 - Por padrão, é aconselhável configurar uma regra para prevenir requisições nas portas 443 e 563 (conexões através de SSL e NEW\$).
 - A opção URL, 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 web-proxy access> add url=":\\.mp\[3g\]\$" action=deny

381

WEB - Proxy

- 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..
- method (any | connect | delete | get | head | options | post | put | trace) – Método HTTP usado nas requisições (veja a seção Métodos HTTP no final deste documento).
- src-address (IP address/netmask) – endereço IP de origem do pacote.
- url (wildcard) – A URL da requisição HTTP.
- Nota:
 - Por padrão, é aconselhável configurar uma regra para prevenir requisições nas portas 443 e 563 (conexões através de SSL e NEW\$).
 - A opção URL, 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 web-proxy access> add url=":\\.mp\[3g\]\$" action=deny

382

[MikrotikBrasil]
Routers & Wireless Systems

Lista de Gerenciamento do Cache

Submenu: /ip web-proxy cache

Descrição

A Lista de Gerenciamento do Cache especifica como as requisições (domínios, servidores, páginas) serão “cacheadas” ou não pelo servidor web-proxy. Esta 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

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.

dst-address (IP address/netmask) – IP de destino do pacote.

383

[MikrotikBrasil]
Routers & Wireless Systems

- 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.
- method (any | connect | delete | get | head | options | post | put | trace) – método HTTP usado na requisição.
- src-address (IP address/netmask) – IP de origem do pacote.
- url (wildcard) – a URL da requisição HTTP.

Lista de Acesso Direto

Submenu: /ip web-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.

384

[MikrotikBrasil]
Routers & Wireless Systems

Descrição das Propriedades

action (allow | deny; default: allow) - especifica a ação a ser tomada quando um “matching” ocorrer.

allow – resolve as requisições em “matching” localmente “bypassando” o parent proxy.

deny – resolve as requisições em “matching” através do parent proxy. Se nenhum parent proxy está configurado o efeito é o mesmo de allow.

dst-address (IP address/netmask) – IP de destino do pacote.

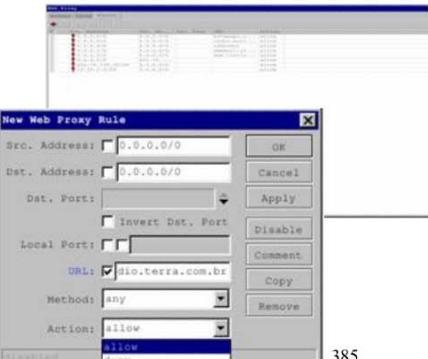
dst-port (port{1,10}) - uma lista de portas que o pacote é destinado.

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.

method (any | connect | delete | get | head | options | post | put | trace) – método HTTP usado na requisição.

src-address (IP address/netmask) – IP de origem do pacote.

url (wildcard) – a URL da requisição HTTP.



385

[MikrotikBrasil]
Routers & Wireless Systems

Nota

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.

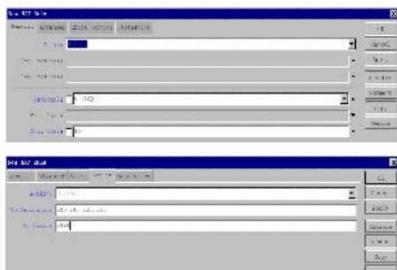


- 1 – Utiliza-se a opção firewall nat e insere uma nova regra
- 2 – Na guia Advanced, insira uma lista de endereços IP, os quais não serão redirecionados ao web-proxy.
- 3 – Na guia Action, será a configurada a ação de redirect para a porta 3128, onde o web-proxy está escutando.

386

[MikrotikBrasil]
Routers & Wireless Systems

Regra de firewall para redirecionar para um web-proxy externo.



4 – Utiliza-se a opção firewall nat e insre uma nova regra.

5 – Na guia Action, uma ação de dst-nat para o IP e porta onde o web-proxy externo estará escutando.

Lista de endereços IP, os quais não farão parte das regras de redirect ou dst-nat.



387

[MikrotikBrasil]
Routers & Wireless Systems

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.

388

APOSTILA DO CURSO MIKROTIK BRASIL EM 2007

Métodos HTTP	Descrição
<ul style="list-style-type: none">• GET<ul style="list-style-type: none">• 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.• 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.	389
<ul style="list-style-type: none">• HEAD<ul style="list-style-type: none">• 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.	390

Reprodução não autorizada

- 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.

391

- 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”.
- 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”.

392

Balanceamento de Carga melhorado com Mikrotik



393



Balanceamento de Carga com NTH

Conforme pudemos ver até agora existem diversos métodos para se fazer balanceamento de carga, cada um com suas particularidades.

Um dos problemas que ocorre quando queremos平衡ar o tráfego utilizando duas ou mais operadoras diferentes é com relação ao funcionamento de diversos serviços dependentes da manutenção conexão, como por exemplo https, serviços de mensagens e outros.

O Mikrotik apresenta um atributo no Mangle que auxilia na marcação de pacotes que é o NTH (n-ésimo). O NTH tem o objetivo de encontrar a n-ésimo pacote recebido por uma regra. Seu uso é definido pelos parâmetros:

nth (every, counter, packet)

394



Balanceamento de Carga com NTH

Nth (every, counter, packet)

São três números inteiros que significam :

→ every: encontra cada pacote de número every+1. Exemplo, se every = 1, a regra encontrará o segundo pacote.

→ counter: especifica qual contador utilizar. É um número aleatório que deve ser escolhido de 0 a 15, devendo ser o mesmo para um grupo que se queira balancear.

→ packet: a regra encontra o pacote com esse número. Obviamente esse número deverá estar entre 0 e every.

395



Balanceamento de Carga com NTH

Exemplo, para平衡ear 3 links:

nth = 2,3,0 2,3,1 2,3,2

- o primeiro pacote encontra a regra 2,3,0 (por causa do 0).
- o segundo pacote encontra a regra 2,3,1 (por causa do 1)
- o terceiro encontra a regra 2,3,2 (por causa do 2)
- a cada every+1 o contador é zerado, iniciando o processo novamente.

396



Balanceamento de Carga com NTH

Para balancear 2 links:

→ nth = 1,2,0 1,2,1

Para balancear 4 links:

→ nth = 3,3,0 3,3,1 3,3,2 3,3,3

Para balancear 7 links:

→ nth = 6,15,0 6,15,1 6,15,2 6,15,3 6,15,4 6,15,5 6,15,6

397



Balanceamento de Carga com NTH

Para balancear 2 links:

→ nth = 1,2,0 1,2,1

Para balancear 4 links:

→ nth = 3,3,0 3,3,1 3,3,2 3,3,3

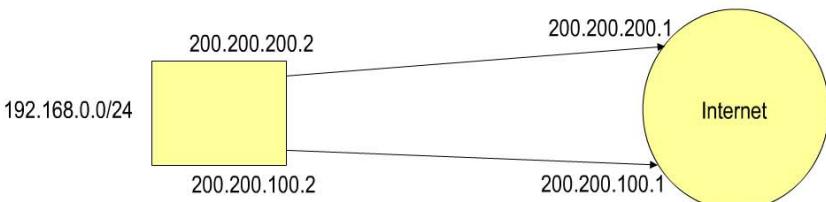
Para balancear 7 links:

→ nth = 6,15,0 6,15,1 6,15,2 6,15,3 6,15,4 6,15,5 6,15,6

398


Balanceamento de Carga com NTH


Exemplo para 2 Links



```

    graph LR
      Host[Host] --- I1[200.200.200.2]
      Host --- I2[200.200.100.2]
      I1 --- Central(( ))
      I2 --- Central
      Central --- Internet((Internet))
      Internet --- I3[200.200.200.1]
      Internet --- I4[200.200.100.1]
  
```

/ ip address
add address=192.168.0.1/24 network=192.168.0.0 broadcast=192.168.0.255 interface=Local
add address=200.200.200.2/30 network=200.200.200.0/30 broadcast=200.200.200.3 interface=wan2
add address=200.200.100.2/30 network=200.200.100.0/30 broadcast=200.200.100.3 interface=wan1

399


Balanceamento de Carga com NTH


Mangle Rule

General	Advanced	Extra	Action	Statistics
Chain: prerouting			Action: mark connection	
Src. Address:			New Connection Mark: <input type="text" value="primeira"/>	<input checked="" type="checkbox"/> Passthrough
Dest. Address:				
Protocol:				
Src. Port:				
Dest. Port:				
P2P:				
In. Interface: Local				
Out. Interface:				
Packet Mark:				
Connection Mark:				
Routing Mark:				
Connection State: new				
Connection Type:				

Mangle Rule

General	Advanced	Extra	Action	Statistics
Nth				
Every: <input type="text" value="1"/>	Counter: <input type="text" value="1"/>	Packet: <input type="text" value="0"/>		
Time				

Exemplo para 2 Links

- 1 marca-se a conexão no canal prerouting, pela interface Local e estado da conexão "new"
- 2 Marca-se a conexão com a etiqueta "primeira" e manda passar adiante
- 3 Na aba "Extra" marca-se o atributo NTH

400

Balanceamento de Carga com NTH



Mangle Rule

General Advanced Extra Action Statistics

Chain: prerouting
Action: mark routing
New Routing Mark: primeira_rota
Passthrough

Src. Address: Det. Address: Protocol: P2P: In. Interface: Local Out. Interface: Packet Mark: Connection Mark: Routing Mark: Connection State: Connection Type:

Exemplo para 2 Links – continuação:

→4 no canal prerouting, na Interface Local, escolhe-se agora as conexões que tem a marca "primeira"

→5 Toma-se a ação "mark routing" dando-se o nome de "primeira_rota". Isso significa que todos os pacotes pertencentes à conexão "primeira" serão rotulados com a marca de roteamento "primeira_rota". Não se usa passthrough pois a ação já foi tomada e esse pacote para de ser examinado.

401

Balanceamento de Carga com NTH



Mangle Rule

General Advanced Extras Action Statistics

Action: mark connection
New Connection Mark: segunda
Passthrough

Src. Address: Det. Address: Protocol: P2P: In. Interface: Local Out. Interface: Packet Mark: Connection Mark: Routing Mark: Connection State: new Connection Type:

Exemplo para 2 Links – continuação.

→6 Faz-se o mesmo para a conexão seguinte, utilizando agora o atributo NTH = 1,1,1 e a marca de conexão "segunda"

402

Mangle Rule

General Advanced Extra Action Statistics

Chain: **segunda**

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

P2P:

In. Interface: Local

Out. Interface:

Packet Mark:

Connection Mark: **segunda**

Routing Mark:

Connection State:

Connection Type:

Mangle Rule

General Advanced Extra Action Statistics

Action: **mark routing**

New Routing Mark: **segunda_rota** Passthrough

NAT Rule

General Advanced Extra Action Statistics

Chain: **segunda**

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark: **segunda**

Routing Mark:

Connection Type:

NAT Rule

General Advanced Extra Action Statistics

Action: **src-nat**

To Addresses: **200.200.100.2**

To Ports: **0-65535**

Exemplo para 2 Links – continuação:

→7 Finalizando a etapa de marcação, faz-se o mesmo procedimento de marcar os pacotes pertencentes à conexão “segunda” colocando-se a marca de rota “segunda_rota”

Exemplo para 2 Links – continuação:

→10 É necessário agora fazer as regras de NAT de forma que as conexões marcadas como primeira sejam “nateadas pelo IP da WAN1



Balanceamento de Carga com NTH



NAT Rule

General		Advanced	Extra	Action	Statistics
Chain:	WAN1				
Src. Address:					
Dst. Address:					
Protocol:					
Src. Port:					
Dst. Port:					
In. Interface:					
Out. Interface:					
Packet Mark:					
Connection Mark:	segunda				
Routing Mark:					
Connection Type:					

NAT Rule

General		Advanced	Extra	Action	Statistics
Action:	src-nat				
To Addresses:	200.200.200.2				
To Ports:	0-65535				

Exemplo para 2 Links – continuação:

→ 11 Da mesma forma, as conexões marcadas como segunda devem ser "nateadas pelo endereço IP da WAN2

405

Balanceamento de Carga com NTH



New Route

Destination:	0.0.0.0/0	
Gateway:	200.200.100.1	
Check Gateway:		
Distance:		
Mark:	primeira_rota	
Pref. Source:		

New Route

Destination:	0.0.0.0/0	
Gateway:	200.200.200.1	
Check Gateway:		
Distance:		
Mark:	segunda_rota	
Pref. Source:		

Exemplo para 2 Links – continuação:

→ 12 Cria-se então as rotas default apontando para o primeiro e segundo link, dependendo da marcação recebida previamente.

→ 13 Finalmente cria-se uma rota default apontando para qualquer um dos links, com a finalidade de mandar os pacotes não marcados, no caso o tráfego do próprio roteador.

406

[MikrotikBrasil]
Routers & Wireless Systems

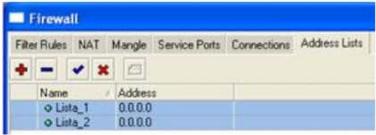
Balanceamento de Carga com NTH, com conexões persistentes por usuário



Nesse caso, nosso objetivo é fazer o balanceamento entre 2 links, mas forçando que as conexões dos mesmos usuários saiam sempre pelo mesmo link.

Fazemos isso, utilizando a técnica do NTH combinada com as Address Lists do Firewall.

→ 1 Adicionamos duas Address List's no Firewall



407

[MikrotikBrasil]
Routers & Wireless Systems

Balanceamento de Carga com NTH, com conexões persistentes por usuário



→2 Fazemos agora com que todas as conexões novas oriundas dos usuários contidos na Lista_1 sejam marcadas com a marca “primeira” e em seguida fazemos com que os pacotes dessa conexões recebam a marca de rota “primeira_rota”

408

[MikrotikBrasil]
Routers & Wireless Systems

Balanceamento de Carga com NTH, com conexões persistentes por usuário

Regra 1

409

Regra 2

410

[MikrotikBrasil]
Routers & Wireless Systems

Balanceamento de Carga com NTH, com conexões persistentes por usuário

→3 O mesmo fazemos agora para as conexões novas oriundas dos usuários contidos na Lista_2.

Marcamos as conexões com a marca “segunda” e em seguida fazemos com que os pacotes dessa conexões recebam a marca de rota “segunda_rota”

411

[MikrotikBrasil]
Routers & Wireless Systems

Balanceamento de Carga com NTH, com conexões persistentes por usuário

Mangle Rule

General Advanced Extra Action Statistics

Chain: prerouting

Src. Address: []

Dst. Address: []

Protocol: []

Src. Port: []

Dst. Port: []

P2P: []

In. Interface: Local

Out. Interface: []

Packet Mark: []

Connection Mark: []

Routing Mark: []

Connection State: new

Connection Type: []

Mangle Rule

General Advanced Extra Action Statistics

Src. Address List: Lista_2

Dst. Address List: []

Content: []

Connection Byter: []

MAC Address: []

Out. Bridge Port: []

In. Bridge Port: []

IPv4 Options: []

TOS: []

TCP MSS: []

Packet Size: []

Random: []

TCP Flags: []

ICMP Options: []

Action: mark connection

New Connection Mark: segunda

Passthrough:

OK Cancel Apply Disable Comment Copy Remove

Regra 3

412

[MikrotikBrasil]
Routers & Wireless Systems

Balanceamento de Carga com NTH, com conexões persistentes por usuário



Mangle Rule

General Advanced Extra Action Statistics

Chain: **lserouting**

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

P2P:

In. Interface: Local

Out. Interface:

Packet Mark:

Connection Mark: **segunda**

Routing Mark:

Connection State:

Connection Type:

Action: mark routing

New Routing Mark: **segunda, rot**

Passthrough

OK Cancel Apply Disable Comment Copy Remove

Regra 4

413

[MikrotikBrasil]
Routers & Wireless Systems

Balanceamento de Carga com NTH



Mangle Rule

General Advanced Extra Action Statistics

Chain: **lserouting**

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

P2P:

In. Interface: Local

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Connection State: **new**

Connection Type:

Action: mark connection

New Connection Mark: **segunda**

Passthrough

Mangle Rule

General Advanced Extra Action Statistics

Connection Limit

Limit

Dst. Limit

Nth

Every: 1

Counter: **1**

Packet: **0**

Time

Fazemos agora as marcações, desta vez utilizando o NTH.

Nestas regras irão passar todos os clientes que não estiverem já inscritos em listas.

Regra 5

414

[MikrotikBrasil]
Routers & Wireless Systems

Balanceamento de Carga com NTH



Mangle Rule

General Advanced Extra Action Statistics

Chain: prerouting
Action: add-addr-to-address-list
Address List: Lista_1
Timeout: 1d 00:00:00

OK Cancel Apply Disable Comment Copy Remove

415

Mangle Rule

General Advanced Extra Action Statistics

Action: mark-routing
New Routing Mark: primeira_rota
Passthrough

OK Cancel Apply Disable Comment Copy Remove

416

Agora, os usuários que foram marcados com uma marca de conexão específica, são inscritos em uma lista.

No caso, primeira → Lista_1

Regra 6

Ainda na marca de conexão primeira, marca-se a rota primeira_rota

Regra 7

[MikrotikBrasil]
Routers & Wireless Systems

Balanceamento de Carga com NTH



Mangle Rule

General Advanced Extra Action Statistics

Chain: **l2routing**

Src. Address: []

Det. Address: []

Protocol: []

Src. Port: []

Det. Port: []

P2P: []

In. Interface: Local

Out. Interface: []

Packet Mark: []

Connection Mark: []

Routing Mark: []

Connection State: new

Connection Type: []

Mangle Rule

Action: mark connection

New Connection Mark: **segunda**

Passthrough

Mangle Rule

General Advanced Extra Action Statistics

▼ Connection Limit

▼ Limit

▼ Det. Limit

▲ Nth

Every: 1

Counter: 1

Packet: 1

417

Repetimos tudo de novo
utilizando no entanto o NTH =
1,1,1

Regra 8

[MikrotikBrasil]
Routers & Wireless Systems

Balanceamento de Carga com NTH



Mangle Rule

General Advanced Extra Action Statistics

Chain: **l2routing**

Src. Address: []

Det. Address: []

Protocol: []

Src. Port: []

Det. Port: []

P2P: []

In. Interface: Local

Out. Interface: []

Packet Mark: []

Connection Mark: **segunda**

Routing Mark: []

Connection State: []

Connection Type: []

Mangle Rule

Action: add src to address list

Address List: **Lista_2**

Timeout: 1d 00:00:00

OK Cancel Apply Disable Comment Copy Remove

Adiciona-se agora os usuários na
Lista_2

Regra 9

418

[MikrotikBrasil]
Routers & Wireless Systems

Balanceamento de Carga com NTH



Mangle Rule

General Advanced Extra Action Statistics

Chain: **balanceout**

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

P2P:

In. Interface: Local

Out. Interface:

Packet Mark:

Connection Mark: **segunda**

Routing Mark:

Connection State:

Connection Type:

Mangle Rule

General Advanced Extra Action Statistics

Action: **mark routing**

New Routing Mark: **segunda_nota**

Passthrough

Regra 10

419

[MikrotikBrasil]
Routers & Wireless Systems

Balanceamento de Carga com NTH



NAT Rule

General Advanced Extra Action Statistics

Chain: **segunda**

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark: **segunda**

Routing Mark:

Connection Type:

NAT Rule

General Advanced Extra Action Statistics

Action: **src-nat**

To Addresses: **200.200.100.2**

To Ports: **0-65535**

Regra 11

→ Faz-se normalmente as regras de NAT de forma que as conexões marcadas como primeira sejam "nateadas pelo IP da WAN1

420

[MikrotikBrasil]
Routers & Wireless Systems

Balanceamento de Carga com NTH



NAT Rule

General	Advanced	Extra	Action	Statistics
Chain: forward			Action: src-nat	
Src. Address:			To Addresses: 200.200.200.2	
Dest. Address:			To Ports: 0-65535	
Protocol:				
Src. Port:				
Dest. Port:				
In. Interface:				
Out. Interface:				
Packet Mark:				
Connection Mark: segunda				
Routing Mark:				
Connection Type:				

Regra 12

→ O mesmo para as conexões marcadas como segunda, que devem ser “nateadas pelo endereço IP da WAN2

421

[MikrotikBrasil]
Routers & Wireless Systems

Balanceamento de Carga com NTH



New Route

Destination: 0.0.0.0/0	Gateway: 200.200.100.1
Check Gateway:	
Distance:	
Mark: primeira_rota	
Pref. Source:	

New Route

Destination: 0.0.0.0/0	Gateway: 200.200.200.1
Check Gateway:	
Distance:	
Mark: segunda_rota	
Pref. Source:	

Exemplo para 2 Links – continuação:

→ 13 Cria-se então as rotas default apontando para o primeiro e segundo link, dependendo da marcação recebida previamente.

→ 14 Finalmente cria-se uma rota default apontando para qualquer um dos links, com a finalidade de mandar os pacotes não marcados.

422



Balanceamento de Carga com NTH, utilizando links de velocidades diferentes

Quando temos vários links de velocidades diferentes e queremos balanceá-los de forma ponderada podemos fazê-lo utilizando a seguinte lógica:

- Somamos os valores das velocidades de todos os links.
- Dividimos o valor encontrado pela velocidade do menor link
- O valor encontrado menos 1 será o valor de every.
- O valor de packet irá variar de zero até esse valor encontrado menos 1

423



Balanceamento de Carga com NTH, utilizando links de velocidades diferentes

Exemplo: temos 4 links de velocidades de 512, 1024, 1024 e 2048 kbps e queremos balanceá-los:

Total da Banda = $512 + 1024 + 1024 + 2048 = 4608$

Equivalência de link = $4608/512 = 9$ (é como se tivéssemos 9 links de 512kbps)

Escolhemos os seguintes valores de NTH: 8,1,0 ; 8,1,1 ; 8,1,2 ; 8,1,3 ; 8,1,4 ; 8,1,5 ; 8,1,6 ; 8,1,7, 8,1,8

Seguindo a mesma lógica do que foi feito para dois links, no mangle, marcamos as conexões e rotas de 1 a 8.

Promovemos então o balanceamento direcionando 1 conexão para o link1, 2 para o link2, 2 para o link3 e 4 para o link4, totalizando $4+2+2+1 = 9$ conexões.

424

[MikrotikBrasil]
Routers & Wireless Systems

Dúvidas ??

425

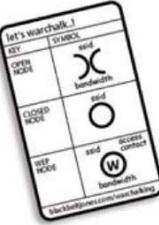
[MikrotikBrasil]
Routers & Wireless Systems

mum
Argentina 
September 7-8th, 2007


www.warchalking.org

Seguridad de redes
Inalámbricas

Eng. Wardner Maia

Let's warchalk!


426



Introducción

MD Brasil – Tecnologia da Informação Ltda
→ Proveedor de Internet desde 1995
→ Redes Inalambricas desde 2000

MD Brasil – Telecomunicações Ltda
→ Suministra entrenamientos en Wireless desde 2002
→ Mayorista de Productos Mikrotik
→ Entrenamientos en Mikrotik desde 2007

Red Global Info
→ La más grande red de Proveedores de Brasil. Presente en más de 450 ciudades.

427



Introducción

Público-alvo:

- Proveedores de Servicio de Internet que hacen uso de tecnologia de acceso inalámbrico fijo baseado en equipos Wi-Fi

Objetivos:

- Abordaje de los aspectos teóricos de seguridad inalámbrica
- Análisis Crítico de los actuales modelos empleados por Proveedores
- Maneras de emplear WPA2-TLS con RouterOS para garantizar la Seguridad
- Ataques de capa 2 e el reto de proteger contra tal tipo de ataques

428

[MikrotikBrasil]
Routers & Wireless Systems



“El poder de las patatas”



Entre 43 redes inalámbricas situadas en la región financiera más importante en Sao Paulo, solamente 8 tenían las configuraciones "recomendadas" de seguridad.

IT Magazine - Info Exame
Artículo publicado en 2002

429

[MikrotikBrasil]
Routers & Wireless Systems



“El poder de las patatas”



Las medidas “recomendadas” de seguridad según el autor eran:

- Nombre de la red escondido
- Control de direcciones MAC
- Encriptación WEP

430

[MikrotikBrasil]
Routers & Wireless Systems

Encuesta sobre seguridad de WISP's realizada en 2002

Segurança provedores 2002

Método de Segurança	Porcentaje
Nenhuma Medida	56%
Controle de MAC - ACL	24%
Controle de MAC + IP	12%
PPPoE	5%
WEP	1%
Controle de MAC - Radius	2%

431

[MikrotikBrasil]
Routers & Wireless Systems

Seguridad “Rudimentaria”
(lo que NO es Seguridad)

1 – SSID escondido

Puntos de Acceso Inalámbricos por defecto hacen broadcasts de los SSID en paquetes llamados “Beacons”. Este comportamiento puede ser modificado y el Punto de Acesso configurado para enviar Strings vacías o ninguna información.

Esconder el nombre de la Red ayuda, pero no puede significar seguridad porque

- SSID's están presentes en texto plano nas computadoras de los clientes
- Escaneadores pasivos pueden escuchar las pruebas de los clientes (probe requests) quando buscan su Red y adivinar el SSID
- Hay equipos que tienen problemas para conectar cuando el AP no hace el broadcast del SSID

432

[MikrotikBrasil]
Routers & Wireless Systems

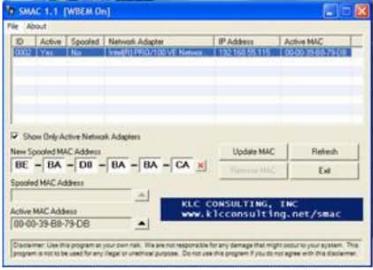
Seguridad “Rudimentaria” (lo que NO es Seguridad)

2 – Filtrado de direcciones MAC

- Descubrir MAC's permitidos es posible con escaneadores pasivos
 - Airopeek para Windows
 - Kismet, Wellenreiter, etc for Linux/BSD
- Falsificar una MAC es muy sencillo con Unix
y lo mismo para Windows

- FreeBSD :
ifconfig <interface> -L <MAC>

- Linux :
ifconfig <interface> hw ether <MAC>



SMAC 1.1 [WBEM On]

ID	Active	Spoofted	Network Adapter	IP Address	Active MAC
0x00	Yes	No	Intel(R) PRO/1000 MT Desktop	192.168.0.115	00:00:90:0B:79:06

Show Only Active Network Adapters

New Spoofted MAC Address: 0E - BA - DB - BA - BA - CA

Update MAC Refresh

Spoofted MAC Address: 00:00:90:0B:79:06

Active MAC Address: 00:00:90:0B:79:06

KLC CONSULTING, INC
www.klcconsulting.net/smac

Disclaimer: Use this program at your own risk. We are not responsible for any damage that might occur to your system. This program is not to be used for any illegal or unethical purposes. Do not use this program if you do not agree with this disclaimer.

433

[MikrotikBrasil]
Routers & Wireless Systems

Seguridad “Rudimentaria” (lo que NO es Seguridad)

3 – Encriptación WEP

- “Wired Equivalent Privacy” – es un sistema de cifrado estándar de la 802.11 pero su utilizacióin no es mandatoria.
- Esta basada en un secreto compartido por las partes y encriptacion con el algoritmo RC4 – Pude ser de 40 e 128 bit.
- 40 bit WEP puede ser crackeada sin hacer uso de técnica sofisticada – solamente un ataque de diccionario quiebra la WEP en menos de 24 horas !
- 104 bit WEP na práctica no puede ser quebrada por ataque de diccionario solamente. Pero...

434

[MikrotikBrasil]
Routers & Wireless Systems

Comprometiendo la WEP (en definitivo)

Articulos publicados na Internet justo al comienzo del uso de WEP mostrando las fragilidades existentes

1 – University of Berkeley – “Intercepting Mobile Communications: The insecurity of 802.11”
Borisov, Nikita, Goldberg e Wagner
<http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf>

2 – University of Maryland – “Your 802.11 Wireless Network has no Clothes.”
Arbaugh, Shankar e Wan
<http://www.cs.umd.edu/~waa/wireless.pdf>

3 – Security Focus – “Weaknesses in the Key Scheduling Algorithm of RC4”
Fluhrere, Martin e Shamir
http://downloads.securityfocus.com/library/rc4_ksaproc.pdf

435

[MikrotikBrasil]
Routers & Wireless Systems

Comprometiendo la WEP (en definitivo)

4 – Articulo publicado en 2005 por Andrea Bittau describiendo un ataque basado en Fragmentación y otras técnicas de ataques inductivos – WEP crakeada en menos de 5 minutos !
<http://www.toorcon.org/2005/conference.html?id=3www.aircrack-ng.org/doku.php?id=fragmentation&DokuWiki=71f9be8def4d820c6a5a4ec475dc6127>

5 – Muy bueno soporte en la net para crackear la WEP

The FEDs can own your WLAN too
<http://www.tomsnetworking.com/Sections-article111.php>

How to crack WEP
<http://www.tomsnetworking.com/Sections-article118.php>

Breaking 104 bit WEP in less than 60 seconds
<http://eprint.iacr.org/2007/120.pdf>

436

[MikrotikBrasil]
Routers & Wireless Systems

Comprometiendo la WEP (en definitivo)

5 – Muy bueno soporte en la net para crackear la WEP

You Tube Vídeo (en español !!)
<http://www.youtube.com/watch?v=PmVtJ1r1pmc>

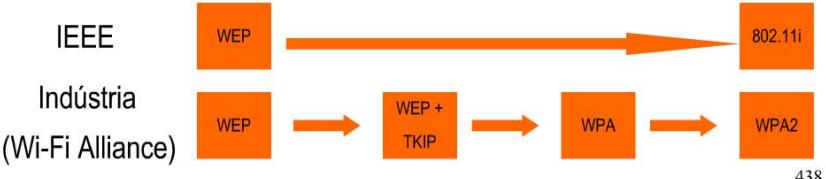


YouTube
Broadcast Yourself! Videos Categories Search
Crackear WEP 2wire infinitum en menos de 2 minutos
Airodump... aireplay... aircrack... root@...
iwconfig001 IEEE80211 /aircrack -p /root/capturas/kyokom-02.cap
Con poco mas de 16.000 iv's generados en menos de 2 minutos arrancamos aircrack-piv
/aircrack-piv ./ ruta del .cap/kyokom-02.cap
debian 437

[MikrotikBrasil]
Routers & Wireless Systems

IEEE 802.11i

- Motivado por los problemas de WEP el IEEE ha creado el Grupo de Trabajo – 802.11i cuya tarea principal era hacer una nueva norma de facto segura.
- Antes de la conclusión del grupo 802.11i (que demoró bastante) la Industria creó un estándar propio - el WPA (Wireless Protected Access)
- En junio del 2004 por fin el stándar fue aprobado y la Industria le dio el nombre de WPA2, compatible con 802.11i .y con WPA



```
graph LR; IEEE[WEP] --> 802_11i[802.11i]; IA[WEP] --> WT[WT-PSK]; WT --> WPA[WPA]; WPA --> WPA2[WPA2]
```

IEEE
Indústria
(Wi-Fi Alliance)

802.11i

WEP

WEP + TKIP

WPA

WPA2

438

Objectivos de 802.11i

→ Autentificación

AP → Cliente: El AP tiene que garantizar que el cliente es quien dice ser
Client → AP: El Cliente tiene que garantizar que el AP es verdadero y no un AP engañoso (man-in-the-middle attack)

→ Privacidad

→ La información no es legible por terceros.

→ Integridad

→ La información no puede ser alterada en transito.

439

Como trabaja 802.11i

802.11i tiene 3 partes

- Suplicant (Solicitante, Cliente)
- Authenticator (Autenticador, AP)
- Authentication Server (Servidor de Autenticación, RADIUS)

Y es hecha por una combinación de protocolos:

- 802.1X – A Port Based Network Access Control
- EAP – Extensible Authentication Protocol
- RADIUS – Remote Access Dial In User Service

440

[MikrotikBrasil]
Routers & Wireless Systems

Variantes de 802.11i

El proceso de autenticación puede ser de 2 maneras:

- Home Mode: (modo casero, personal)
 - Pre Shared Key (PSK)
- Enterprise Mode: (modo corporativo)
 - 802.1X/EAP

		WPA	WPA2
Modo Corporativo	Autenticación	802.1X / EAP	802.1X / EAP
	Cifrado	TKIP/MIC	AES-CCMP
Modo Personal	Autenticación	PSK	PSK
	Cifrado	TKIP/MIC	AES-CCMP

441

[MikrotikBrasil]
Routers & Wireless Systems

802.11i PSK

```

    graph TD
        subgraph Client [Client]
            P1[Passphrase (PSK)] --> PMK1["PMK = f ( passphrase, SSID )"]
            PMK1 --> PMK2["256-bit pairwise master key (PMK)"]
            PMK2 --> D1[Derive PTK]
            D1 --> S1[Check MIC]
            S1 --> I1[Install Key  
Begin encrypting]
        end
        subgraph AP [AP]
            P2[Passphrase (PSK)] --> PMK3["PMK = f ( passphrase, SSID )"]
            PMK3 --> PMK4["256-bit pairwise master key (PMK)"]
            PMK4 --> D2[Derive PTK,  
Check MIC]
            D2 --> S2[OK, install MIC]
            S2 --> I2[Install Key  
Begin encrypting]
        end
        D1 <--> D2
        S1 <--> S2
        I1 <--> I2
    
```

Una "llave Maestra" llamada PMK – Pairwise Master Key es creada por un hash entre la Passphrase y el SSID. La PMK es guardada en el Registro de Windows o en supplicant.conf en Linux.

Otra llave llamada PTK - Pairwise Transient Key es creada de manera dinámica después de un proceso de handshake de 4 vías. PTK es única a cada sesión.

442

[MikrotikBrasil]
Routers & Wireless Systems

Privacidad con 802.11i

Privacidad

- Después de la autenticación, los dos lados – AP y Cliente tienen la misma PMK – Pairwise Master Key que se mantiene durante toda la sesión
- Para la transmisión de datos, es hecha una derivación de la PMK y una PTK – Pairwise Transient Key **única para cada cliente** es utilizada para encriptación.

443

[MikrotikBrasil]
Routers & Wireless Systems

Integridad con 802.11i

Una parte de la PTK tiene la función de proteger los datos para que no sean alterados cuando en transito – es el MIC - Message Integrity Check (MIC). Con el MIC, para todo paquete el transmisor calcula un hash de los datos con una llave secreta – Temporal Integrity Key.

MIC = hash(packet, temporal integrity key)

WPA usa TKIP → Algoritmo de Hashing “Michael”

WPA2 uses CCMP → Cipher Block Chaining Message Authentication Check– CBC-MAC

The diagram illustrates the structure of an 802.11i frame. It consists of four main fields: 802.11 Header (blue), Encrypted Data (orange), Data (orange), and MIC (orange). A horizontal bracket above the Data field indicates the entire frame is Encrypted. A horizontal bracket below the 802.11 Header and Data fields indicates they are Authenticated by MIC.

444

[MikrotikBrasil]
Routers & Wireless Systems

Utilizando WPA/WPA2 – PSK con Mikrotik RouterOS

445

[MikrotikBrasil]
Routers & Wireless Systems

Utilizando WPA/WPA2 – PSK

Es muy sencilla la configuracion de WPA/WPA2-PSK con Mikrotik

→WPA - PSK
Configure el modo de llave dinámico, WPA PSK, y la llave compartida.

→ WPA2 - PSK
Configure el modo de llave dinámico, WPA PSK, y la llave compartida.

Las llaves son alfanumericas de 8 hasta 63 caracteres

446

General Tab	Static Keys Tab
- Authentication Types: ✓ WPA PSK ☐ WPA EAP	WPA2 PSK ☐ WPA2 EAP aes com
- Unicast Ciphers: ✓ skip	aes com
- Group Ciphers: ✓ skip	
WPA Pre-Shared Key: 23456789	
WPA2 Pre-Shared Key: 1234567890	
Group Key Update: 0/15.00	
RADIUS MAC Authentication	

¿ Cuanto segura es WPA / WPA2 PSK ?

- La manera conocida hoy de crackear WPA-PSK es solamente por un ataque de diccionario.
- Como la llave maestra - PMK combina una contraseña con el SSID, escogiendo dos palabras fuertes, hace ineficientes los diccionarios precompilados
- No hay diferencias en la manera y nivel de dificultad para crackear WPA-PSK o WPA2-PSK, porque el mecanismo que genera la PMK es el mismo. Solamente cambia el MIC.
- Herramienta para quiebra de WPA/WPA2 – PSK
 - Cowpatty <http://sourceforge.net/projects/cowpatty>.
- La mayor fragilidad de PSK para WISP's es que la llave se encuentra em texto plano nas computadoras dos clientes

447

¿ Cuán segura es WPA / WPA2 PSK ?

Cuando el atacante tiene la llave PMK es posible:

- Ganar acceso no autorizado
- Falsificar um Punto de acceso y hacer el ataque del “hombre del medio” (man-in-the-middle)

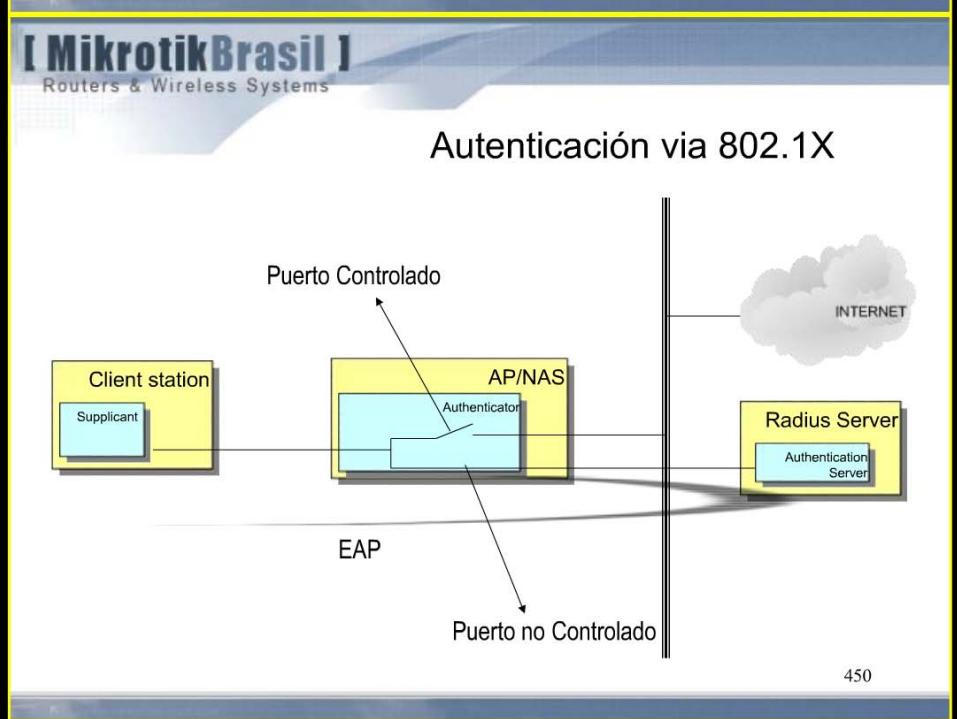
Recomendaciones para WISP's

- Solo use PSK se tiene **absoluta certeza** que las llaves están protegidas (equipos clientes del proveedor)
- No olvides que las llaves PSK están em **texto plano** dentro de los boxes Mikrotik (hasta para read-only user)

448



449



450

EAP

EAP es un protocolo para identificación de usuarios o hosts originalmente diseñado para Protocolo Punto a Punto (PPP)

```
graph LR; CS[Client station  
Suplicant] <--> AP[AP/NAS  
Authenticator]; AP <--> RS[Radius Server  
Authentication Server]
```

EAP over LAN EAP over RADIUS

Soporta diferentes tipos de autenticación. Los más comunes son: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-LEAP, EAP-MD5 etc

451

Tipos de EAP

EAP Type	Open/ Proprietary	Mutual Auth	Authentication Credentials		Key Material	User Name In Clear
			Supplicant	Authenticator		
TLS	Open	Yes	Certificate	Certificate	Yes	Yes
TTLS	Open	Yes	Username/Pwd	Certificate	Yes	No
PEAP	Open	Yes	Username/Pwd	Certificate	Yes	No
LEAP	Proprietary	Yes	Username/Pwd		Yes	Yes

452

[MikrotikBrasil]
Routers & Wireless Systems

Tipos de EAP

LEAP: (Lightweight EAP)

Es un protocolo propietario de Cisco patentado antes mismo de 802.11i and WPA.
Es basado en nombre de usuario y contraseña que se envía sin protección.
Esta metodología descuida la protección de las credenciales durante la fase de autenticación del usuario con el servidor.
Trabaja con variados tipos de clientes pero solo con AP Cisco.

→ Tool to crack LEAP: Asleap - <http://asleap.sourceforge.net/>

OBS: Mikrotik no soporta LEAP

453

[MikrotikBrasil]
Routers & Wireless Systems

Tipos de EAP

PEAP: (Protected EAP) and EAP-TTLS (EAP tunneled TLS)

PEAP y TTLS son parecidos- TTLS es compatible con otros protocolos como LEAP y hacen uso de Certificados de Autenticidad en lado del Servidor y usuario contraseña en lado cliente. Autenticación sigue la orden:

- 1 – El Servidor manda un EAP request
- 2 – Cliente manda una identidade (lo que sea) - un Tunel TLS es creado
- 3 – Dentro del tunel, el cliente pasa usuário y contraseña

El problema con TTLS y PEAP es el “hombre del medio”

OBS: Mikrotik no soporta TTLS y PEAP

454

[MikrotikBrasil]
Routers & Wireless Systems

Tipos de EAP

EAP-TLS (EAP – Transport Layer Security)

→ Es el tipo de EAP que Mikrotik soporta

Provee mayor nivel de seguridad y necesita certificados en los dos lados – Cliente y Servidor.

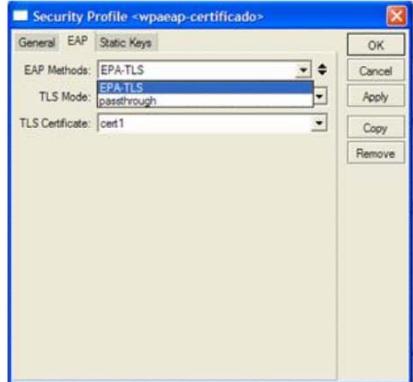
Los Certificados pueden ser instalados:

- En AP y Clientes
- En Clientes y Servidor Radius
- Sin Certificados !

455

[MikrotikBrasil]
Routers & Wireless Systems

Security Profiles – EAP Methods



→ **EAP-TLS**
Usa Certificados

→ **passthrough**
Manda para un Servidor Radius (funciona como dispositivo 802.1X) – solo para Puntos de Acceso.

456

[MikrotikBrasil]
Routers & Wireless Systems

Security Profiles – TLS Mode

→ verify certificates
Requiere un certificado y verifica si fue firmado por una Certificadora

→ don't verify certificates
Requiere un certificate, pero no verifica

→ no certificates
Certificados son negociados dinámicamente con el algoritmo de Diffie-Hellman (explicado adelante)

457

[MikrotikBrasil]
Routers & Wireless Systems

¿¿ Trabajar con EAP-TLS pero sin Certificados ??

458

[MikrotikBrasil]
Routers & Wireless Systems

Diffie-Hellmann (Without Certificates)

Side A

Secret number x

Generator g

Prime number p

$K(a) = g^x \pmod{p}$

$K(a), g, p$

Side B

1. Cada lado escoge un número secreto x y y – llaves privadas.

2. Lado A empieza seleccionando un número primo muy alto (p) y un pequeño entero – el generador (g)

3. Lado A calcula usando aritmética modular la clave pública, $K(a)$:
 $\rightarrow K(a) = g^x \pmod{p}$

4. Lado A manda para o lado B la clave pública, el número primo (p), y el generador (g)

459

[MikrotikBrasil]
Routers & Wireless Systems

Diffie-Hellmann (Without Certificates)

Side A

Secret number x

Generator g

Prime number p

$K(a) = g^x \pmod{p}$

$K(a), g, p$

Side B

Generator g

Prime number p

Secret number y

$K(b) = g^y \pmod{p}$

$K(b)$

5. Lado B hace un calculo similar con su clave secreta, el primo y el generador para obtener su clave pública.

6. Lado B manda para lado A la clave pública.

7. Ahora los dos lados pueden calcular una misma clave compartida
 \rightarrow Shared key = $K(b)^x \pmod{p}$
 \rightarrow Shared key = $K(a)^y \pmod{p}$

460

The diagram illustrates the Diffie-Hellmann key exchange process. Side A and Side B both start with a secret number (x and y respectively), a generator (g), and a prime number (p). Side A calculates $K(a) = g^x \pmod{p}$ and sends $K(a), g, p$ to Side B. Side B calculates $K(b) = g^y \pmod{p}$ and sends $K(b)$ to Side A. Both sides then calculate the shared key: Side A calculates $\text{Key} = K(b)^x \pmod{p}$ and Side B calculates $\text{Key} = K(a)^y \pmod{p}$. The resulting keys are shown to be the same value.

**Diffie-Hellmann
(Without Certificates)**

8. Los dos cálculos producen valores exactamente iguales – propiedad de aritmética modular
9. La clave calculada es usada como PMK e inicia el proceso de encriptación

461

The screenshot shows the "Station Configuration" window for an interface named "wlan1". Under the "General" tab, the "Security Profile" is set to "Profile-no-Cert". The "Security Profile" window shows the "EAP Method" is set to "EAP-TLS" and the "TLS Mode" is "no certificates".

Setup with EAP-TLS – No Certificates

Station Configuration

Security Profile

462

[MikrotikBrasil]
Routers & Wireless Systems

Setup with EAP-TLS – No Certificates

AP Configuration

Interface <AP_no_Cert>

General | Wireless | WDS | Status | Traffic

Master Interface: wlan2
SSID: AP_no_Cert
Area:
Security Profile: EAP-TLS-NoCert
Max Station Count: 2007
Proprietary Extension: post-2.9.25
Default AP Tx Limit: bps
Default Client Tx Limit: bps
 Default Authenticate
 Default Forward
 Hide SSID

OK Cancel Apply Disable Comment Copy Remove

Security Profile

Security Profile <EAP-TLS-NoCert>

General | EAP | Static Keys

EAP Methods: EAP-TLS
TLS Mode: no certificates
TLS Certificate: none

OK Cancel Apply Copy Remove

463

[MikrotikBrasil]
Routers & Wireless Systems

¿ Cuanto seguro es EAP-TLS sin Certificados ?

- Como resultado de la negociación anónima resulta una PMK y después toda la comunicación es encriptada por AES (WPA2) o RC4 (WPA)
- Sería todo muy seguro si no hubiera la posibilidad de un hacker meter un Mikrotik con la misma configuración y negociar la clave normalmente 😞
- Una idea para hacer esa configuración de forma segura es después de cerrar el enlace, hacer un túnel PPTP o L2TP entre los equipos.

464

The slide has a yellow border and features the MikrotikBrasil logo at the top left. The title 'Implantando EAP-TLS con Certificados' is centered. In the bottom right corner, there is a small numerical value '465'. The main content area contains text about digital certificates and two screenshots of browser certificate dialogs.

Un certificado digital es un fichero que identifica su propietario de manera única. Certificados son creados por instituciones emisoras llamadas de CA (Certificate Authorities)

Certificados pueden ser :

- Firmados por una institución "acreditada" (Verisign, Thawte, etc)
- o
- Certificados auto-firmados

465

[MikrotikBrasil]
Routers & Wireless Systems

Implantando EAP-TLS con Certificados

Creando la CA - Certificate Authority

→ En una máquina Linux con OpenSSL modifique el fichero openssl.conf con los datos que se usarán en los Certificados que serán generados

/etc/ssl/openssl.conf

dir	= ./MikrotikBrasil_CA
countryName_default	= BR
stateOrProvinceName_default	= Sao Paulo
organizationName_default	= MikrotikBrasil_Private_Network

467

[MikrotikBrasil]
Routers & Wireless Systems

Implantando EAP-TLS con Certificados

Creando la CA - Certificate Authority – cont.

→ Modifique el script creador de la CA (CA.sh) para el mismo directorio.

CATOP=./MikrotikBrasil_CA

→ Corra el con la opcion –newca

```
root@wlanbrasil:/etc/ssl# ./misc/CA.sh –newca
CA certificate filename (or enter to create)
```

→ Pressione <enter> e contesta a las preguntas

468

[MikrotikBrasil]
Routers & Wireless Systems

Implantando EAP-TLS con Certificados

Creando la CA - Certificate Authority – cont.

→ El Certificado fue creado y se encuentra en:

/etc/openssl/MikrotikBrasil_CA/cacert.pem

→ Una Clave protegida con DES también está en::

/etc/openssl/MikrotikBrasil_CA/cakey.pem

469

[MikrotikBrasil]
Routers & Wireless Systems

Implantando EAP-TLS con Certificados

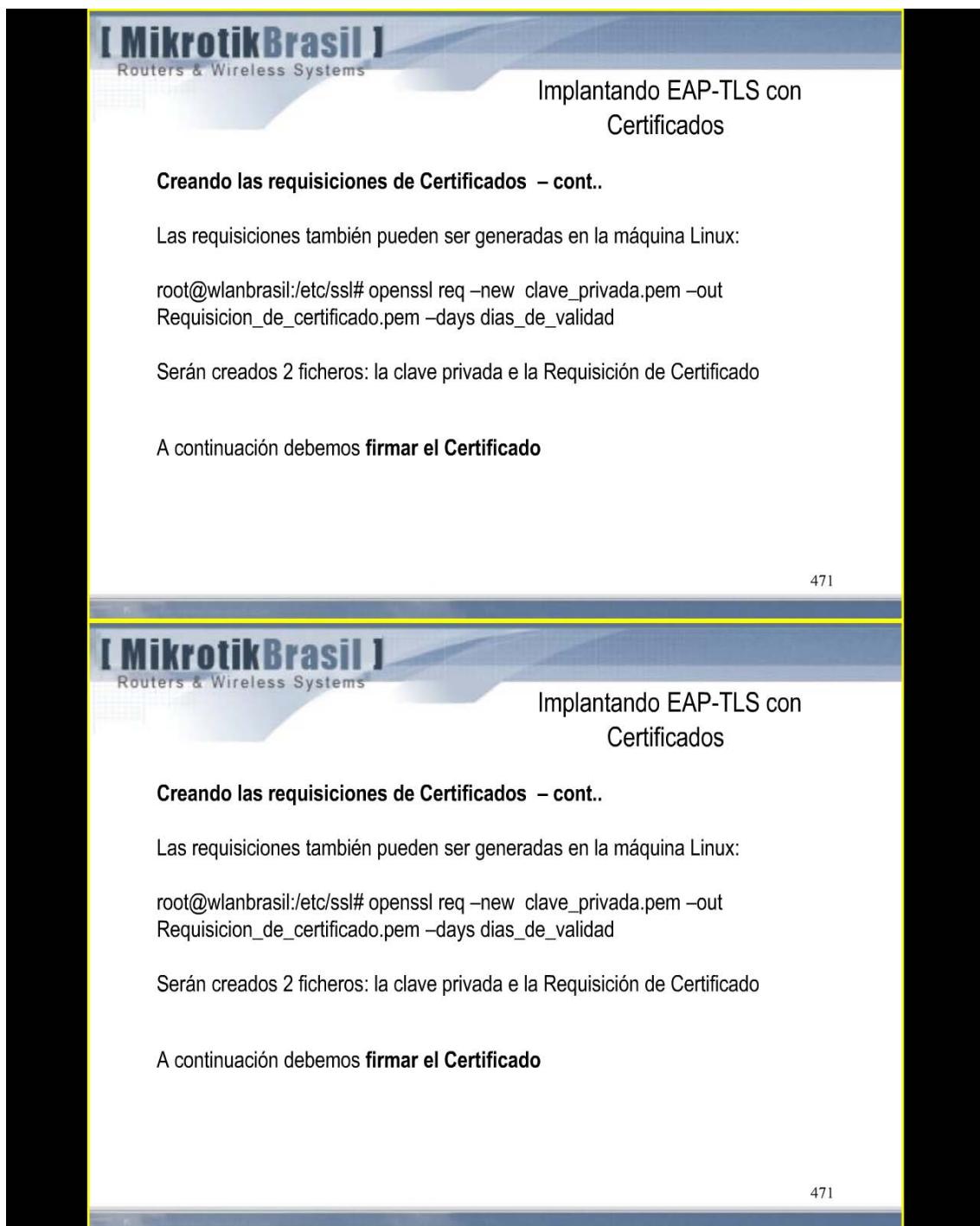
Creando las requisiciones de Certificados

Pueden ser creadas en propio Mikrotik con :

/ certificates create-certificate-request

```
[admin@MikroTik] certificate>
create-certificate-request decrypt edit find get import print remove reset-certificate-cache set
[admin@MikroTik] certificate> create-certificate-request
certificate request file name: certificate-request-01.pem
file name: private-key-01.pem
passphrase: *****
verify passphrase: *****
rsa key bites: 1024
country name: BR
state or province name: Sao Paulo
locality name: Bebedouro
organization name: Mikrotik Brasil Corp.
organization unit name: Wireless Security
common name: hotspot.mikrotikbrasil.com.br
email address: maia@mikrotikbrasil.com.br
challenge password: *****
unstructured address: www.mikrotikbrasil.com.br
[admin@MikroTik] certificate>
```

470



[MikrotikBrasil]
Routers & Wireless Systems

Implantando EAP-TLS con Certificados

Creando las requisiciones de Certificados – cont..

Las requisiciones también pueden ser generadas en la máquina Linux:

```
root@wlanbrasil:/etc/ssl# openssl req -new clave_privada.pem -out Requisicion_de_certificado.pem -days dias_de_validad
```

Serán creados 2 ficheros: la clave privada e la Requisición de Certificado

A continuación debemos **firmar el Certificado**

471



[MikrotikBrasil]
Routers & Wireless Systems

Implantando EAP-TLS con Certificados

Creando las requisiciones de Certificados – cont..

Las requisiciones también pueden ser generadas en la máquina Linux:

```
root@wlanbrasil:/etc/ssl# openssl req -new clave_privada.pem -out Requisicion_de_certificado.pem -days dias_de_validad
```

Serán creados 2 ficheros: la clave privada e la Requisición de Certificado

A continuación debemos **firmar el Certificado**

471

[MikrotikBrasil]
Routers & Wireless Systems

Implantando EAP-TLS con Certificados

Asignando las requisiciones de Certificados

Las requisiciones creadas en RouterOS o en la máquina Linux se firma con

```
root@wlanbrasil:/etc/ssl# openssl ca -config ./openssl.conf -policy policy_anything -out /certificado_asignado.pem -infiles /requisicion_de_certificado.pem
```

Ahora el fichero de requisición puede ser deletado porque será utilizado solo el certificado_asignado.pem

472

[MikrotikBrasil]
Routers & Wireless Systems

Implantando EAP-TLS con Certificados

Importando el Certificado para Mikrotik

via Winbox



Después de la Importación



Para importar la clave es necesaria la misma contraseña que se utilizó en la creación

473

[MikrotikBrasil]
Routers & Wireless Systems

Implantando EAP-TLS con Certificados

Importando el Certificado para Mikrotik

via Winbox

Después de la Importación

Para importar la clave es necesaria la misma contraseña que se utilizó en la creación

473

[MikrotikBrasil]
Routers & Wireless Systems

Utilización de EAP-TLS con Certificados
en AP y Clientes

474

Reprodução não autorizada

[MikrotikBrasil]
Routers & Wireless Systems

Utilización de EAP-TLS (AP con Certificado) Configuración del AP

AP Configuration

Security Profile

Certificate

475

[MikrotikBrasil]
Routers & Wireless Systems

Utilización de EAP-TLS (AP con Certificado) Configuración del Cliente

Station Configuration

Security Profile

Certificate

476

Implantando EAP-TLS + Radius

477

Implantando EAP-TLS + Radius

Creando Certificado para instalar en el Servidor RADIUS (1/1)

El Certificado para Radius puede ser creado de la misma manera que otros certificados, pero es mejor que se utilice la opción –nodes

Se no se utiliza la opción –nodes toda vez que se inicia Radius tiene que digitar la clave privada.

openssl req -nodes -new -keyout key_file.pem -out req_file.pem -days 365

Se firma como los otros y está listo !

478

Implantando EAP-TLS + Radius

Instalando el Certificado en el Servidor RADIUS (1/1)

→ Ponga las cosas en sus lugares correctos:

```
root@radius:/usr/local/etc/raddb# mv certs certs.old  
root@radius:/usr/local/etc/raddb# mkdir certs  
root@radius:/usr/local/etc/raddb# mv /root/radius_cert_key.pem ./certs  
root@radius:/usr/local/etc/raddb# mv /root/cacert.pem ./certs
```

→ Crea el parámetro de Diffie-Hellman:

```
root@radius:/usr/local/etc/raddb# dd if=/dev/random of=./certs/random count=2  
root@radius:/usr/local/etc/raddb# openssl dhparam -check -text -5 -512 -out  
./certs/dh
```

→ Chequea si todo se encuentra en su lugar

```
root@radius:/usr/local/etc/raddb# ls ./certs  
cacert.pem dh radius_cer_key.pem random
```

479

Implantando EAP-TLS + Radius

Configurando el Servidor RADIUS (1/4)

→ Edite el fichero clients.conf con la lista de AP's (NAS's) que utilizarán el Radius

```
root@radius:/usr/local/etc/raddb# aee clients.conf  
client 192.168.100.1/32 {  
    secret          = 123456  
    shortname      = AP1  
}
```

→ Edit radiusd.conf

```
root@radius:/usr/local/etc/raddb# aee radiusd.conf
```

```
user = nobody  
group = nogroup
```

480

Implantando EAP-TLS + Radius

Configurando el Servidor RADIUS (2/4)

Editing radiusd.conf - cont

```
authorize {  
    preprocess  
    chap  
    mschap  
    suffix  
    eap  
    files  
}
```

481

Implantando EAP-TLS + Radius

Configurando el Servidor RADIUS (3/4)

Configure el fichero users

```
root@radius:/usr/local/etc/raddb# aee radiusd.conf
```

DEFAULT	Auth-Type = EAP
	Tunnel-Type = 13,
	Tunnel-Medium-Type = 6,
	Tunnel-Private-Group-Id = 1

482

[MikrotikBrasil]
Routers & Wireless Systems

Implantando EAP-TLS + Radius

Configurando el Servidor RADIUS (4/4)

→ Edite eap.conf

```
root@radius:/usr/local/etc/raddb# aee eap.conf
default_eap_type = tls
tls
{
    private_key_file = ${raddbdir}/certs/radius_cert_key.pem
    certificate_file = ${raddbdir}/certs/radius_cert_key.pem
    CA_file = ${raddbdir}/certs/cacert.pem
    dh_file = ${raddbdir}/certs/dh
    random_file = ${raddbdir}/certs/cacert.pem
}
```

→Finalmente inicia el Radius Server

```
root@radius:/usr/local/etc/raddb# ./radiusd -X
```

483

[MikrotikBrasil]
Routers & Wireless Systems

Station Configuration

The window shows the configuration for Interface <wlan1>. The General tab is selected, displaying fields for Radio Name (000000000000), Mode (station), SSID (AP_to_Radius), Band (2.4GHz B/G), Frequency (2462), Scan List (None), Security Profile (Profile-EAP-TLS), Frequency Mode (manual txpower), Country (no_country_set), Antenna Gain (0 dB), DFS Mode (none), Proprietary Extensions (post-2.9.25), Default AP Tx Rate (11 bps), Default Client Tx Rate (11 bps), and checkboxes for Default Authenticate, Default Forward, and Hide SSID.

Setup with EAP-TLS + Radius Client Configuration

Security Profile

The dialog box shows the Security Profile <EAP-Cert>. It has tabs for General, EAP, and Static Keys. Under EAP, the method is set to EAP-TLS and the TLS mode is verify certificate. Under TLS Certificate, the certificate is set to cert1. Buttons include OK, Cancel, Apply, Copy, and Remove.

Certificate

The dialog box shows a Certificate List with one entry: KQR cert1. The details are: Name / Subject: C=BR, ST=Sao Paulo..., Issuer: CA. Below the table is a note: K - decrypted private key, Q - private key, R - na.

484

[MikrotikBrasil]
Routers & Wireless Systems

Setup with EAP-TLS + Radius AP Configuration

The screenshot shows the 'Interface - AP_to_Radius' configuration window. Under the 'General' tab, the 'Master Interface' is set to 'wireless'. The 'SSID' is 'AP_to_Radius'. The 'Security Profile' dropdown is set to 'EAP-TLS-RADIUS'. Other settings include 'Max Station Count: 2007', 'Proprietary Extensions: post-2.9.25', and 'Default AP Tx Unit: 1 bps' and 'Default Client Tx Unit: 1 bps'. Buttons for OK, Cancel, Apply, Disable, Comment, Copy, and Remove are visible.

Security Profile

The screenshot shows the 'Security Profile <EAP-RADIUS>' configuration window. The 'EAP Methods' dropdown is set to 'passthrough'. The 'TLS Mode' is 'verify certificate' and the 'TLS Certificate' is 'cert1'. Buttons for OK, Cancel, Apply, Copy, and Remove are visible.

Security Profile

The screenshot shows the 'Security Profile <EAP-TLS-RADIUS>' configuration window. The 'EAP Methods' dropdown is set to 'passthrough'. The 'TLS Mode' is 'verify certificate' and the 'TLS Certificate' is 'certS'. Buttons for OK, Cancel, Apply, Copy, and Remove are visible.

485

Backbone con EAP-TLS +Radius

The diagram illustrates a mesh network backbone. A 'Mesh Node' is connected to a 'Radius Server', which is connected to a 'Database'. The 'Radius Server' also has a connection to a 'Certificates' icon (represented by a starburst). A callout box labeled 'Ubicación IP "Certificada", Ancho de Banda, Rutas, etc.' points to the 'Mesh Node'. Below the backbone, a large mesh network is shown as a grid of nodes connected by lines, each containing a lock icon, representing secured connections.

486

[MikrotikBrasil]
Routers & Wireless Systems

¿ Cuanto seguro es EAP-TLS + Radius ?

No se discute que EAP-TLS es el método más seguro, pero la única cosa que se podría argumentar es cuanto al link entre AP y Radius.



→ Hay ataques conocidos contra Radius. Si un atacante tiene acceso físico a el link entre AP y Radius, el puede hacer un ataque de diccionario para descobrir la PMK.

→ Para evitar puede-se proteger de muchas maneras, como con un tunel L2TP con IPSec entre Radius y AP.

487

802.11i

X

WISP's

488

[MikrotikBrasil]
Routers & Wireless Systems

Volviendo al pasado – En 2002 Los WISP's en Brasil
Con las medidas “apropiadas”

Segurança provedores 2002

Medida	Porcentaje
Nenhuma Medida	56%
Controle de MAC - ACL	24%
Controle de MAC + IP	12%
PPPoE	5%
WEP	1%
Outros	2%

Se consideraban muy seguros...

489

[MikrotikBrasil]
Routers & Wireless Systems

Soluciones para ultima milla

Para tratar de asegurar el servicio en la última milla, muchos proveedores utilizan las soluciones:

- Túneles PPPoE
- Autenticación Hotspot

A continuación vamos a hacer un análisis crítico de los dos modelos cuando empleados con objetivos de seguridad.

490

Encuesta realizada en septiembre de 2007

Proveedores que responderan a la Encuesta: 74

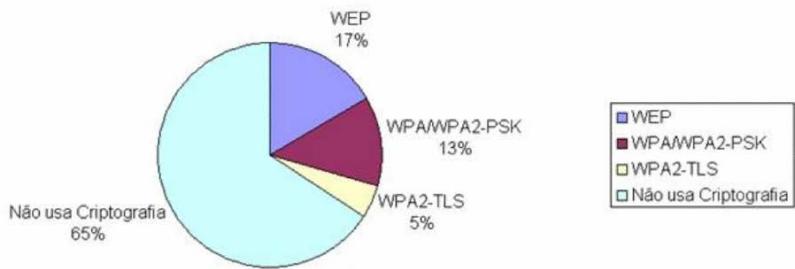
Numero de Clientes atendidos: 52.385

Total de Link contratado: 585.6 mbps

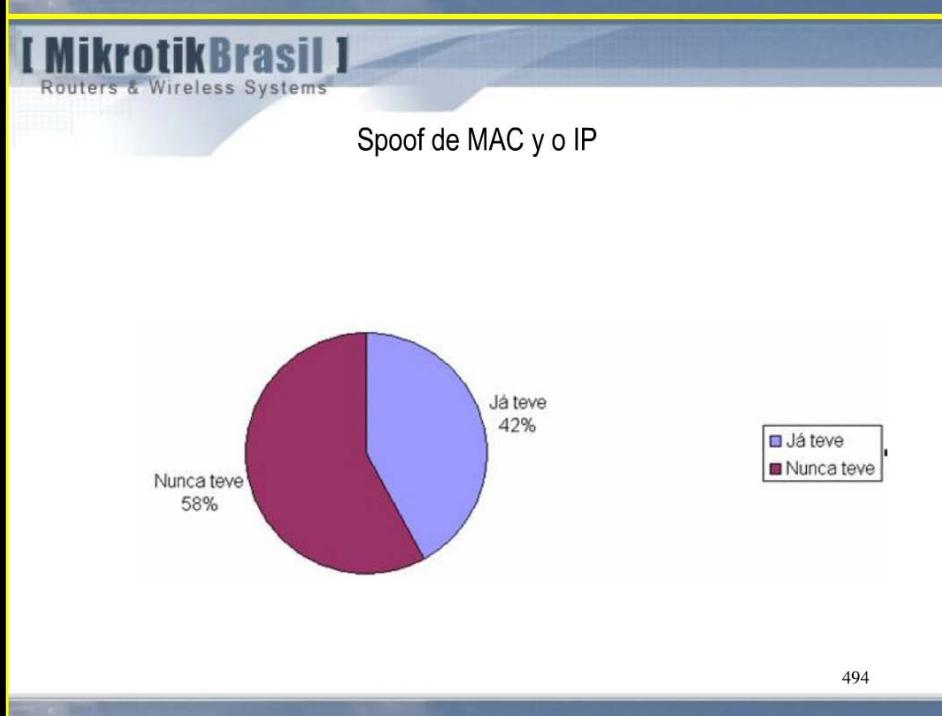
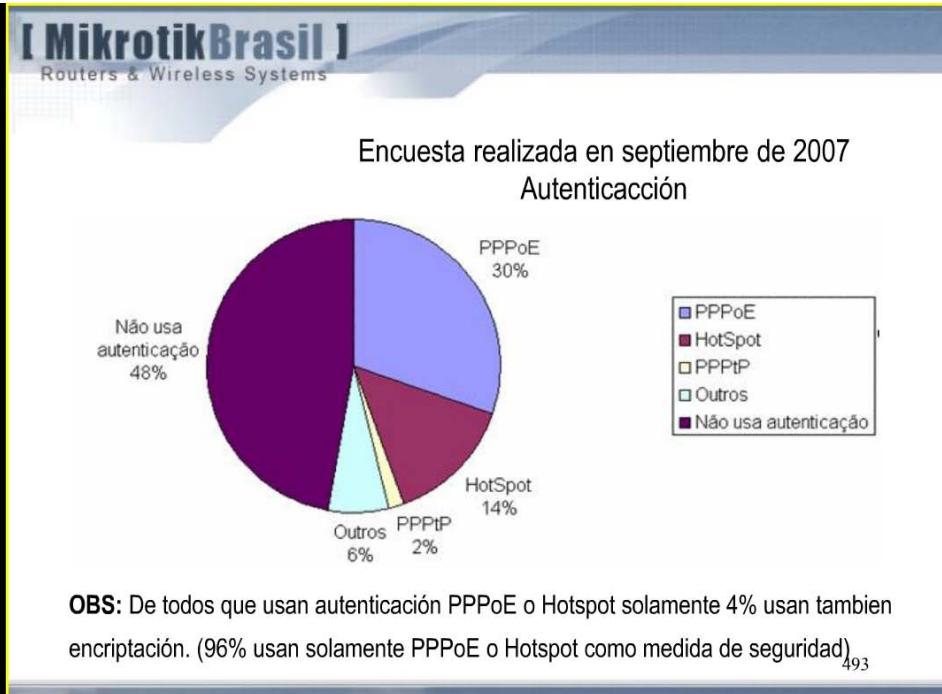
Los resultados fueran compilados de manera ponderada por el numero de clientes atendidos. Por ejemplo, la respuesta de un proveedor que tiene 1000 clientes vale 10 veces a de un que tiene 100 clientes.

491

Encuesta realizada en septiembre de 2007
Encriptación



492



Soluciones (no 80211i) para la última milha

Para tratar de asegurar el servicio en la última milla, muchos proveedores utilizan las soluciones:

- Túneles PPPoE
- Autenticación Hotspot

A continuación vamos a hacer un análisis crítico de los dos modelos cuando empleados con objetivos de seguridad.

495

Túneles PPPoE aspectos generales

- PPPoE : originalmente desarrollado para redes alambradas .
- El PPPoE Server (PPPoEd) escucha las solicitudes de PPPoE clients que utilizan el protocolo PPPoE discovery.
- PPPoE por defecto no es encriptado – puede ser configurado si el cliente soporta encriptación.
- User/password puede ser protegido empleando de método CHAP authentication. PAP passes in plain text.

496

Tuneles PPPoE aspectos generales

- La interface que "escucha" las requisiciones PPPoE no deben tener configurado IP "roteado". Se lo tiene es posible pasar a largo de la autenticación PPPoE configurando de forma manual um IP de la grade.
- Como otros tuneles, los valores de MTU and MRU deben ser modificados.
- PPPoE es sensible a variaciones de señal
- En máquinas Windows es necesario a instalación de un marcador, lo que representa trabajo administrativo.

497

PPPoE y Seguridad

- Un atacante que falsifique una dirección MAC no logra navegar, pero causa muchos problemas para el usuario verdadero.
- Quando el concentrador PPPoE está corriendo en la misma máquina del AP, un MAC falso causa la negación de servicio al usuario verdadero quando este intenta conectarlo.
- Lo más grave que tiene PPPoE es que **el usuario no autentica el Servidor**. Por ese motivo un ataque del tipo "hombre del medio" puede facilmente ser implementado. Basta que un atacante ponga un AP falso en una posición privilegiada y accione um PPPoE Server para capturar las requisiciones PPPoE discover de los clientes y aceptar cualquier usuario/contraseña que sea.

498

Hotspots aspectos generales

- Originalmente fueron desarrollados para dar servicio de conexión a Internet en Hoteles, Shoppings, etc. Con el tiempo, WISP's hacen uso de Hotspots como medio para autenticar usuarios.
- La interfaz configurada como Hotspot escucha las solicitudes de navegación y pide usuario/contraseña.
- Mikrotik puede autenticar en la base local o en un Radius externo.
- Con Certificados digitales en el box Mikrotik se puede configurar un Hotspot con https.

499

Hotspots y Seguridad

- Una vez que un usuario se ha autenticado y su par IP + MAC sea descubierto y falsificado por un atacante, el atacante gana acceso sin tener usuario/contraseña. El punto de acceso no "ve" dos, pero solo un usuario. El servicio se queda malo para los dos (pero lo atacante sabe el motivo) y no hay conflicto.
- Cuando se trabaja sin Certificados, el ataque del "hombre del medio" puede ser hecho como en PPPoE porque el cliente no autentica el Hotspot.
- Trabajando con Certificados se puede en el primer acceso instalar en la máquina del cliente el Certificado y enseñar al Cliente los riesgos de aceptar un Certificado diferente.

500

PPPoE x Hotspot & seguridad - conclusiones

- PPPoE tiene muchas ventajas porque trabaja en capa 2 y no hay tráfico IP.
Muchos problemas como virus, broadcasts, etc no existen en una planta basada en PPPoE
- El ataque del "hombre del medio" es muy sencillo de implementar contra los WISP's que usan PPPoE. No hay mucho por hacer para evitar esto..
- Hotspots tambien son vulnerables pero si son bien configurados e instalados con Certificados digitales pueden evitar el "hombre del medio" pero los usuarios tienen que tener conocimiento de una serie de prácticas.
- Los dos son excelentes herramientas de ayuda para la administración de la Red, principalmente cuando trabajando en conjunto com Radius.
- **PPPoE y Hotspot ayudan, pero no significan seguridad !!!**

501

Seguridad – conclusiones (casi) finales

Seguridad en el medio Inalámbrico que cumpla los principios básicos de

- Autenticación
- Confidencialidad
- Integridad de datos

Solo se consigue con la utilización de una estructura basada en 802.11i con EAP-TLS implementada con Certificados Digitales + Radius.

Otras implementaciones como la formación de VPN's entre los clientes y un Concentrador son eficaces pero en escala de implementación pueden mostrarse inefectivas.

502

¿ Porque los WISP's no utilizan 802.11i ?

WISP's dicen que no utilizan 802.11i por los motivos abajo:

- Mucha Complejidad
 - (con Mikrotik todo es muy sencillo!!)
- Por ser un padrón abierto se esperan problemas de seguridad para el futuro
 - (puede ser una verdad, pero la realidad es hoy)
- Equipos antigos no permiten encriptación.
 - (Mikrotik permite varios profiles. Hasta WEP puede ser una buena salida)
- Antiguos problemas de Wep hacen criptografía no creíble
 - (Las diferencias son muchas. No hay comparación)
- Problemas de performance cuando se usa encriptación.
 - (Nuevos Chipsets Atheros tienen encriptación por hardware, no hay problemas de performance)

503

Servicio afectado por ataques de capa 2

504

Servicio afectado por ataques de capa 2

IEEE 802.11i se preocupó con

- Autenticación
- Confidencialidad
- Integridad

Desafortunadamente 802.11i no se preocupó con la **disponibilidad** del servicio.

El Servicio Wi-Fi puede ser comprometido con dos tipos de ataque:

- Basados en alto poder de RF (verdaderamente un ataque de capa 1)
- Basados nel protocolo 802.11

505

Ataque al medio fisico



506

[MikrotikBrasil]
Routers & Wireless Systems

Servicio afectado por ataques de capa 2

→ Basados en alto poder de RF (Jamming)

No hay nada que hacer en Mikrotik. La única medida posible es llamar las autoridades responsables por el espectro radioelectrico.

Un buen proyecto de RF puede ayudar mucho.

→ Basados en el protocolo 802.11

Son basados en debilidades del protocolo 802.11 muy dependente de MAC address

Hay muchas herramientas disponibles en la Internet que pueden ser usadas para

Ataques com. Void11, airreplay, etc.

www.wlanbrasil.com.br/downloads/seguranca/cd1.iso

www.wlanbrasil.com.br/downloads/seguranca/cd2.iso

507

[MikrotikBrasil]
Routers & Wireless Systems

Proceso de asociación

```

graph TD
    S1((State 1:  
Unauthenticated  
Unassociated)) -- "Successful authentication" --> S2((State 2:  
Authenticated  
Unassociated))
    S2 -- "Deauthentication" --> S1
    S2 -- "Disassociation" --> S3((State 3:  
Authenticated  
Associated))
    S3 -- "Successful authentication or reassociation" --> S2
    S3 -- "Deauthentication" --> S1
  
```

802.11 Types and Subtypes

00 - Protocol Version	0000 - Management Frame Type	01 - Control Frame Type	10 - Data Frame Type
0000 - association request	0000 - association response	0010 - power save poll	0000 - data
0001 - reassocation request	0001 - reassocation response	0011 - RTS	0001 - data + CF-ACK
0010 - reassociation response	0010 - probe request	0100 - CTS	0010 - data + CF-poll
0100 - probe response	0101 - probe response	1101 - ACK	0011 - data + CF-ACK + CF-poll
1001 - disassociation	1010 - disassociation	1110 - CF-end	0101 - NULL (no data)
1011 - authentication	1100 - authentication	1111 - CF-end + CF-ACK	0101 - CF-ACK (no data)
1100 - deauthentication	1100 - deauthentication		0110 - CF-poll (no data)
			0111 - CF-ACK + CF-poll (no data)

508

Ataque de Deauth

1 – El atacante utiliza alguna herramienta como airopeek, kismet, wellenreiter, para descubrir :

- El MAC del AP
- El MAC del Cliente
- Canal de RF

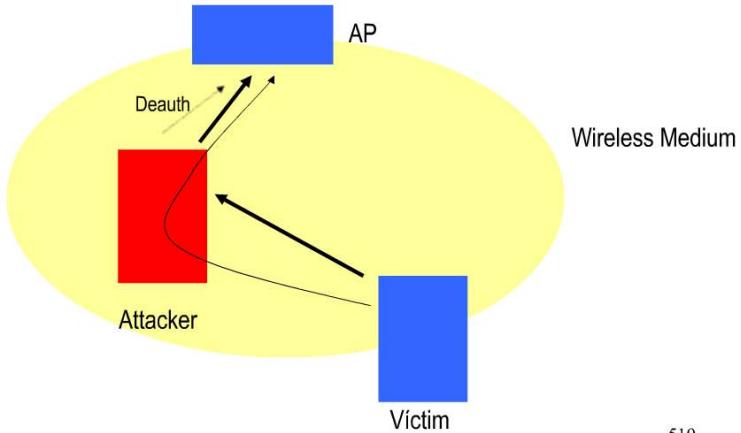
2 – Lanza paquetes de deauth en el aire

- NO necesita de potencia alta
- NO necesita asociación
- NO necesita estar en la tabla de MAC's

Solo tiene que tener una tarjeta inalámbrica apropiada que permite inyección de paquetes, como Prism, Atheros, Ralink, etc y el driver apropiado.

509

Hombre del medio “in aire” (Monkey Jack attack)



510

[MikrotikBrasil]
Routers & Wireless Systems

Contramedidas para De-auth Attack con Mikrotik

Modificación del Protocolo

- Con una modificación del protocolo 802.11 este tipo de ataque puede ser evitado.
- La idea es basada en que los equipos no obedezcan paquetes de deauth
- Hay que ver si la modificación tiene impactos para otras cosas
- Teniendo en cuenta que Nstreme es un protocolo propietario quizás Mikrotik pueda implementar
- Abajo hay un link para un artículo que describe los problemas y propone soluciones

<http://sysnet.ucsd.edu/~bellardo/pubs/usenix-sec03-80211dos-slides.pdf>

511

[MikrotikBrasil]
Routers & Wireless Systems

Contramedidas para De-auth Attack con Mikrotik

La primera cosa que tiene que hacer es estar seguro que estás con este tipo de ataque
Los paquetes inalámbricos pueden ser sniffados en /interface/wireless/sniffer

Sniffed Wireless Packets

Time	Interfa...	Band	Frequ...	Signal ...	Rate	Dst.	Src.	Type
1.043s	wlan2	2.4GHz-G	2462...	-50dBm	1Mbps	FF:FF:FF:FF:FF:FF	00:0C:42:0C:54:1D	beacon
1.061s	wlan2	2.4GHz-G	2462...	-87dBm	11Mbps	FF:FF:FF:FF:FF:FF	00:02:78:E5:4C:97	beacon
1.102s	wlan2	2.4GHz-G	2462...	-86dBm	11Mbps	FF:FF:FF:FF:FF:FF	00:02:78:E5:4C:97	beacon
1.120s	wlan2	2.4GHz-G	2462...	-91dBm	1Mbps	00:0C:42:0C:54:5B	02:0C:42:0C:53:1B	deauthentication
1.121s	wlan2	2.4GHz-G	2462...	-46dBm	1Mbps	FF:FF:FF:FF:FF:FF	00:0C:42:0C:54:5B	probe request
1.146s	wlan2	2.4GHz-G	2462...	-59dBm	1Mbps	FF:FF:FF:FF:FF:FF	00:0C:42:0C:54:1D	beacon
1.193s	wlan2	2.4GHz-G	2462...	-86dBm	11Mbps	00:60:1D:22:F2:4D	00:02:78:E5:4C:97	data

El paquete de tipo “deauthentication” principalmente en gran número muestra que la red está sufriendo un ataque deauth
Verifique principalmente los MAC's de origen y destino.

512

[MikrotikBrasil]
Routers & Wireless Systems

Contramedidas para De-auth Attack con Mikrotik

Los modos de operación que emplean ancho de 10 y 5 Mhz. no son afectados por las herramientas de deauth

Nosotros testamos en la práctica con Void11 y air-replay.

Si el ataque esta siendo hecho en un link Punto a Punto cámbialo para 10 o 5 Mhz puede ser una buena solución.

513

[MikrotikBrasil]
Routers & Wireless Systems

Contramedidas para De-auth Attack con Mikrotik

Como los ataques son hechos utilizando el AP MAC, una salida es cambiar el MAC en el Mikrotik

Esta puede no ser considerada una medida elegante de seguridad, pero un trabajo puede ayudar que el atacador descubra el nuevo MAC.

514

Contramedidas para De-auth Attack con Mikrotik

Seguridad por “obscuridad”

Utilizando AP's Virtuales que no hacen nada, pero solo lanzan broadcasts con SSID's y MAC's puedes crear un ambiente muy difícil de ser sniffado.

- Con Mikrotik puedes tener AP's virtuales con diferentes direcciones MAC
- Puedes con scripts adicionales crear, habilitar y desabilitar dinámicamente muchas más AP's virtuales con muchos MAC's.

OBS: La idea es parecida con que lo hace el Script Perl llamado “Fake AP”

<http://www.blackalchemy.to/project/fakeap>.

515

Muchas Gracias !

Paldies !

Obrigado !

Wardner Maia

maia@mikrotikbrasil.com.br

516

