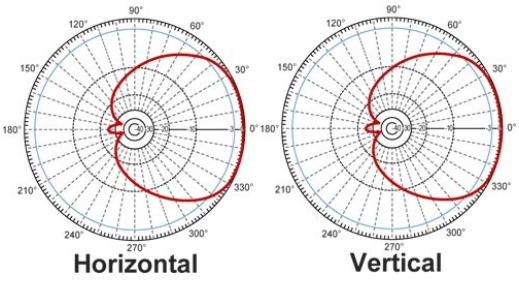
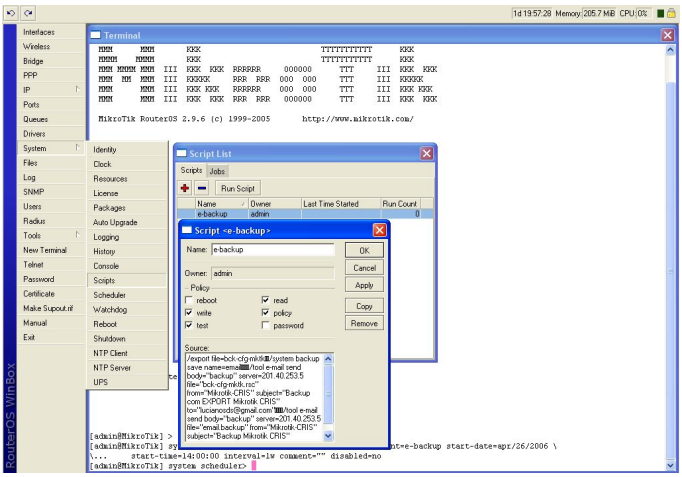
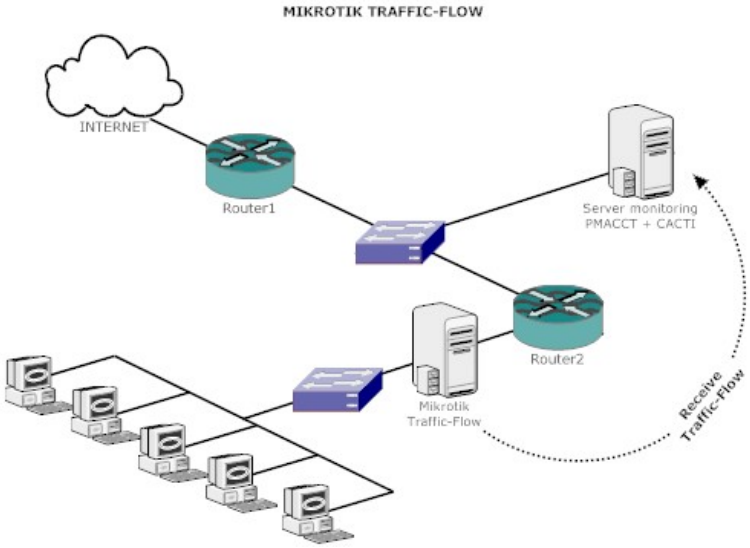
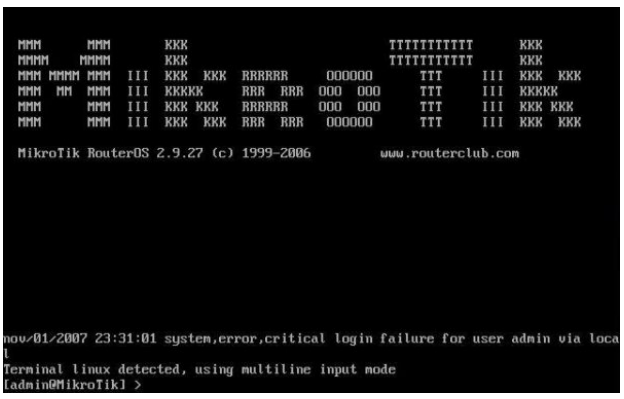
CURSO MIKROTIK 2.9.X









Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

ÍNDICE

Alfamaster

Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

Rafael Galdino

Formado em marketing estrategico pela FPPD (Faculdade Paraibana de Processamento de Dados).
trabalha com rede desde 2002, onde começou como suporte Técnico do provedor DIGINET www.digi.com.br , passando por outros provedores como: Neoline, Openline etc...
Teve o primeiro provedor WISP em 2003, e teve o primeiro contato com o Sistema Mikrotik em 2005, desde lá trabalha implementando regras e aperfeiçoamentos com regras de firewall e outros ajustes para melhorar o desempenho de redes do tipo Wireless.
A mais de 3 anos mechendo com o Mikrotik já implementou cerca de 40 provedores.
Onde da Suporte e sempre implementando melhorias.
Na rede Wireless tem experiência por ter tido contato com equipamentos Top de linha, como Terabeam, Nanostation, Mikrotik etc..É moderador de diversas comunidades Mikrotik no orkut e também tem grande participação em comunidades relacionadas como: Wireless Brasil e Wifi Hacking.

Agradecimentos

Primeiramente a Deus por me dar forças nos piores momentos e sempre me ajudar, a minha esposa Sheila, que muitas noites sentiu a minha falta na cama por eu estar estudando ou configurando servidores até umas 3 ou 4 da manhã.
A Luiz Roberto "comunidades sobre mikrotik ORKUT", um cara que sempre me ajudou e sempre batemos juntos no aspecto mikrotik. com vasta experiência, sempre conversarmos, sempre mudamos umas regras um ajudando o outro.
ao Lucky "comunidade wireless brasil ORKUT", por ter me ajudado nas duvídas sobre o que é SCM, o que é de direito e o que não é, sobre APS, etc... um cara fantastico.
Ao George Almeida e Lorran "comunidade Wifi Hacking ORKUT" por terem aberto minha cabeça sobre segurança, onde eu com minha cabeça dura achava que tudo era seguro, mas me provaram coisas imaginaveis sobre falhas e bugs.
entre outros como meus amigos: Fernandinho "HIPERNET", Marcio Lucena "Supernet", Flávio "NetSpeed", Claúdio "Alfamaster", Keitel Werner "UPLINK", Mago "MaisNet" e a todos que me ajudaram diretamente ou indiretamente a conclusão dessa apostila .


Lucky


Luiz Roberto


George Almeida


Lorran

Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

O QUE É WIFI (WIRELESS)

Nada mais é que um sistema sem fio, em inglês sua tradução vem do wire (cabo, fio) + less (livre), é um sistema que funciona através de ondas eletro-magnéticas, rádio ou infra-vermelho.

A comunicação sem fio serve para levar uma informação de um elemento emissor à um elemento receptor, podendo ser uma transmissão de curta distância ou uma transmissão de longa distância como exemplo as informações que são enviadas por satélites.
A tecnologia wireless é utilizada em equipamentos de telecomunicações, como celulares, telefones sem fio, walktalk e gps.
Atualmente os sistemas de rede sem fio tem se tornado um grande atrativo devido ao baixo custo e à praticidade no instante em que um usuário final não precisará se incomodar com cabos, switchs, e outros equipamentos que antes eram necessários quando se queria disponibilizar a internet em sua residência ou casa.
Hoje o mercado disponibiliza equipamentos relativamente baratos e de fácil configuração, tornando esta realidade mais próxima de uma boa parcela de usuários de internet.

Padrões atuais Wi-fi

Wi-Fi ou Wireless Fidelity, é uma marca da empresa Wi-Fi Alliance que designou o padrão IEEE 802.11, dentro deste padrão trabalha dentro da frequência de 2,4Ghz e 5,8 Ghz com a capacidade de atingir taxas de transferências de até 54mbs. Os padrões adotados mundialmente se concentram nos 802.11 b/g padronizando a utilização da tecnologia no mundo.

802.11B

Alcança uma velocidade de 11 Mbps padronizada pelo IEEE, oferecida por alguns fabricantes não padronizados. Opera na freqüência de 2.4GHz. Inicialmente suporta 32 utilizadores por ponto de acesso. Um ponto negativo neste padrão é a alta interferência tanto na transmissão como na recepção de sinais, porque funcionam a 2,4 GHz equivalentes aos telefones móveis, fornos microondas e dispositivos Bluetooth.
O aspecto positivo é o baixo preço dos seus dispositivos, a largura de banda gratuita bem como a disponibilidade gratuita em todo mundo. O 802.11b é amplamente utilizado por provedores de internet sem fio.

802.11G

Baseia-se na compatibilidade com os dispositivos 802.11g e oferece uma velocidade de 54 Mbps. Funciona dentro da frequência de 2,4 GHz. As vantagens também são as velocidades. Torna-se por vezes difícil de configurar, como Home Gateway devido à sua freqüência de rádio e outros sinais.

Segurança

A segurança numa rede wireless é muito interessante a pessoas que pensam em instalar uma rede sem fio.
Um comitê do padrão 802.11 definiu o WEP (wireless equivalent privacy) esse processo que impede a invasão por pessoas não autorizadas a rede é baseado em chaves de permissão do qual apenas pessoas autorizadas e com o conhecimento desta poderá acessar a rede protegida. Existe outros meios de segurança, afim de evitar o acesso não autorizado a rede, WPA, Controle de Mac etc..

Alfamaster

Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

O que é Mikrotik?

O Mikrotik é um routerOS , ou seja o routerOS é um sistema operacional desenvolvido para realizar a tarefa de um roteador, o nome MIKROTIK se dar aos equipamentos.
Desenvolvido pela MikroTikls empresa em Riga capital da Letônia região dos países baltícos próximo à Rússia. A mikrotik nome comercial da empresa, desenvolve sistema para solução em conectividade como ISP (Internet Service Provider).
O sistema foi desenvolvido para computadores tradicionais baseado em plataforma x86, devido a esta vantagem o usuário poderá dimensionar um roteador com a configuração que desejar, além de custar menos que os roteadores profissionais no mercado.

Em poucas palavras é um sistema operacional, que pode ser instalado em um PC comum

ou Placas SBC (Single Board Computer), podendo executar funções de:

Roteador Dedicado

Bridge

Firewall

Controlador de Banda e QOS

Ponto de Acesso Wireless em modos: A/B/G e prioritário

Concentrador VPN “pppoe, pptp, ipsec, L2TP etc..”

Roteador de Borda

Hotspot, Web Proxy entre outros.

Bastente Utilizado em Provedores Wireless pela praticidade e pela quantidade de materiais

disponivéis na internet, bem como técnicos que tranformam uma rede simples numa

arquitetura profissional e de qualidade, com recursos infinitos e em sempre atualização.

Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

Instalação do Sistema

Existe 3 formas de instalar o sistema:
*Via disquete "já obsoleto"
*Via CD-ROM
*Via Netinstall

Instalando o Mikrotik VIA CD

Coloca-se o PC para dar o boot pela unidade de cd Para selecionar todos os Pacotes da instalação

aperta a tecla “A” Em seguida a tecla “i”, depois a tecla “Y”

SYSTEM: Pacote Principal, com os serviços fundamentais para funcionamento,drivers etc..

PPP: Suporte aos serviços de VPN, PPPoE, L2TP, PPtP, etc

DHCP: DHCP cliente e DHCP servidor

ADVANCED-TOOLS: ferramentas de diagnóstico, netwatch, e outros...

ARLAN: Suporte a placas da Aironet

GPS: Suporte a GPS

HOTSPOT: Suporte a Hotspots

ISDN: suporte a conexões ISDN

LCD: suporte a Display de cristal liquído

NTP: Servidor e cliente de NTP (Relógio)

RÁDIOLAN: Suporte a placa Radiolan

ROUTERBOARD: utilitários para Routerboard

ROUTING: Suporte a roteamento Dinâmico – Protocolos RIP, OSPF e BPG

ROUTING-TEST: suporte a roteamento Dinâmico “em teste”

RSTP-BRIDGE-TEST: Protocolo RSTP

SECURITY: Suporte a SSH, Ipsec e conexões seguras do winbox

SYNCHRONOUS: Suporte a Placas sécronas Moxa, Cyclades PC300 e outras

TELEPHONY: suporte a telefonia protocol h.323 VoIP

UPS: Suporte a no-breaks APC

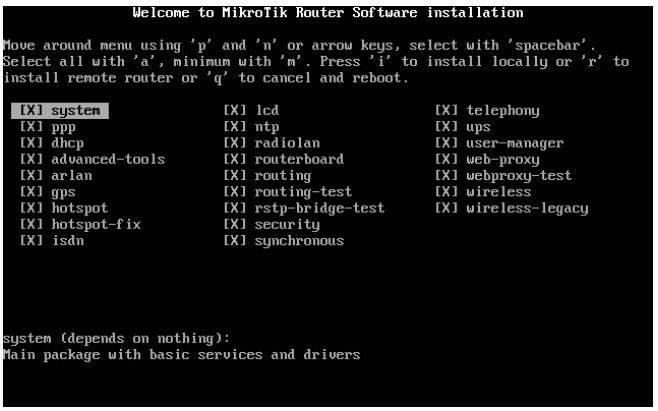
USER-MANAGER: Serviço de autenticação User-Manager

WEBPROXY: Serviço de Web-proxy

WEBPROXY-TEST: Serviço de Web-proxy “em teste”

WIRELESS: suporte a places prismll e atheros

WIRELESS-LEGACY: Suporte a Placas Prismll, atheros e aironet com algumas features inabilitadas



Se a instalação foi feita com sucesso aparecerá

a tela de login você usará o login“admin” sem senha

Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

Instalação com Netinstall

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

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

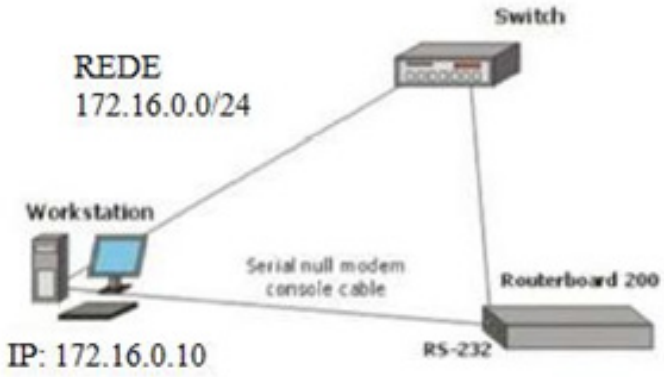
→ Pode-se instalar em um um PC que da BOOT via rede (configurar na BIOS)

→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.

Para se instalar em uma Routerboard, 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

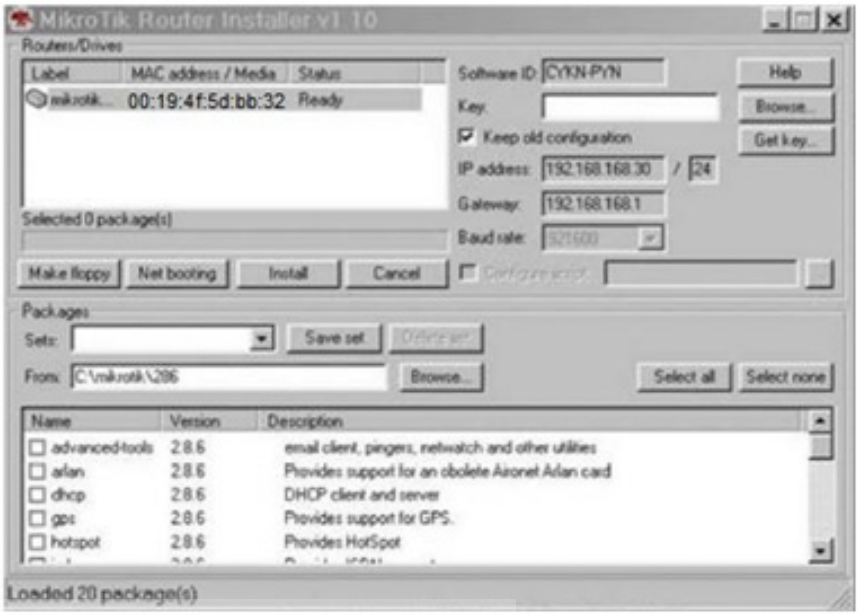


Entra-se na Routerboard e seleciona-se

o - boot device

e - Etherboot

e depois:



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

→Colocar os pacotes a serem instalados na máquina.

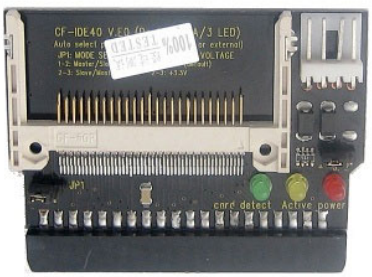
→Bootar e selecionar os pacotes a serem instalados.

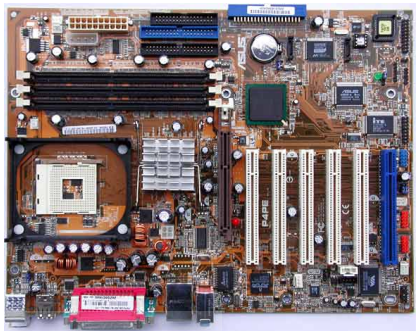
Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

Hardware Compatíveis

O mikrotik trabalha com uma lista de hardware compatíveis, no brasil você encontrará muitos produtos compatíveis geralmente dotado com o chipset atheros, cisco ou intersil.
Neste link você poderá consultar toda a lista de hardware compatível:
http://www.mikrotik.com/testdocs/ros/2.9/guide/driverlist.php
Algumas placas Wireless encontradas e testadas:
DWL-G520 / ag530
Senao NMP-8602 (mini PCI você precisará de um adaptador para transformar em PCI)
EnGenius EPI3601S
Greatek WL-2454G
Tp-Link WN551G
Tp-Link WN651G

Placas de rede Ethernet
Realtek 8139d
Dlink DFE-520Tx
Dlink DGE-530Tx
Placas E1 e T1





Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

O processo para acessar pela primeira vez um mikrotik
pode ser feito das seguintes formas:
•direto no console (se for um PC)
•via terminal
•via telnet de mac, atravez de outro mikrotik ou de sistema que suporte telnet por Mac
•via Winbox

CONSOLE

```
quit -- Quit console
certificate/ -- Certificate management
redo -- Redo previosly undone action
special-login/ -- Special login users
interface/ -- Interface configuration
driver/ -- Driver management
ping -- Send ICMP Echo packets
setup -- Do basic setup of system
password -- Change password
undo -- Undo previous action
port/ -- Serial ports
import --
snmp/ -- SNMP settings
user/ -- User management
file/ -- Local router file storage.
queue/ -- Bandwidth management
system/ -- System information and utilities
ip/ -- IP options
tool/ -- Diagnostics tools
ppp/ -- Point to Point Protocol
routing/ -- Various routing protocol settings
isdn-channels/ -- ISDN channel status info
export --

[admin@MikroTik] >
```

Print: com este comando você lista as opções naquela tela: "informações. dados"**.**
/ : serve para voltar para o menu raiz
.. : serve para voltar um menu acima
quit: para sair do console e ficar na tela de login
Interfaces: comando usado para listar as interfaces que estão instaladas no MK.
Ping: P**ara efetuar ping para algum ip ou host**
Setup: este comando fará a configuração como configurar ip, gateway entre outros**.**

Verificando as placas instaladas no Mikrotik

No console do mikrotik digite:
interfaces
depois : print

```
Terminal vt102 detected, using multiline input mode
[admin@ispot] > int
[admin@ispot] interface> print
Flags: X - disabled, D - dynamic, R - running
 #    NAME                TYPE            RX-RATE    TX-RATE    MTU
 0  R internet            ether           0          0          1500
 1  R pppoe-out1          pppoe-out       0          0          1492
 2  R bridge1             bridge          0          0          1500
 3    local_wan2          wlan            0          0          1500
 4  R local_wan3          wlan            0          0          1500
 5    local_wan1          wlan            0          0          1500
[admin@ispot] interface>
```

Se você instalou corretamente as placas e se elas forem compatíveis com os chipsets listados provavelmente aparecerá o nome ether para as placas “ethernet” e para as placas wireless “wlan”.

Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

Winbox

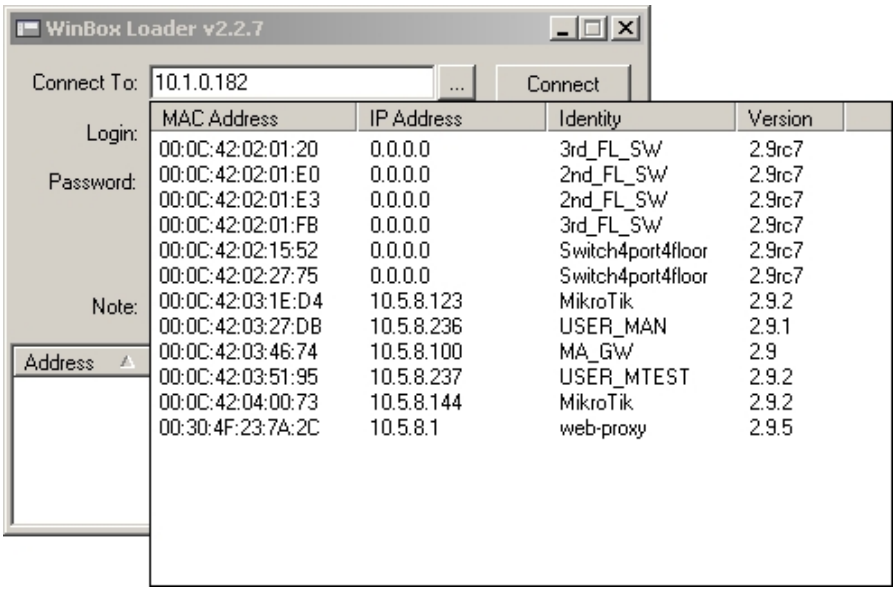
O winbox você baixa no endereço: http://www.mikrotik.com/download/winbox.exe

Para acessa-lo pela primeira vez tem que usar um cabo cross, ou ligar o mikrotik a um switch, para ter acesso.

Connect To: é o endereço de ip ou host do mikrotik para acessar, pode usar também MAC

Login: nome do usuario

Password: senha



Keep Password: Salvar a senha

Secure mode: Para criptografar o acesso

Load Previous session: lêr a ultima seção

O mikrotik pode ser baixado também pelo navegador usando a porta padrão 80

http://IP_do_Mikrotik

Alfamaster

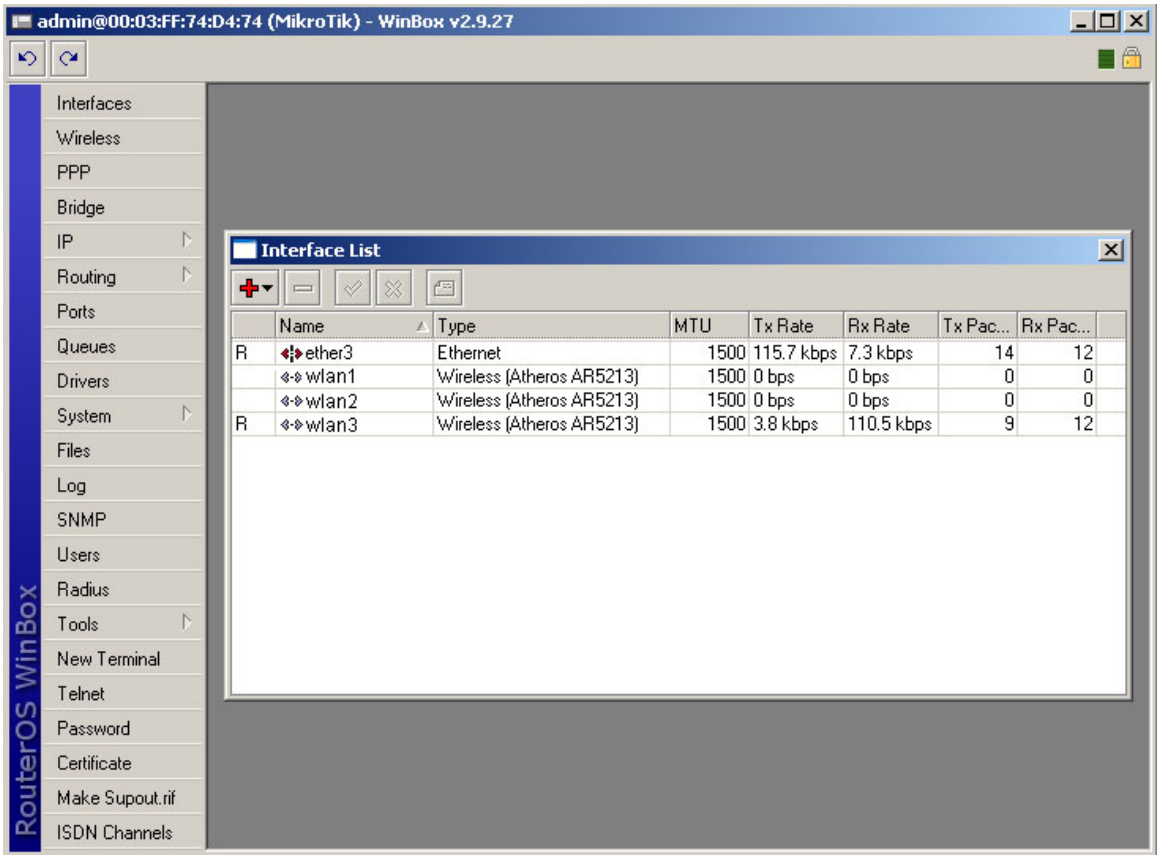
Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

1. o sinal + significa que poderão ser adicionado novas regras
2. o sinal - removerá uma regra selecionada
3. o botão “v” habilita uma regra desabilitada (as entradas desabilitadas estarão em cinza)
4. o botão “x” desabilita uma regra habilitada
5. o botão “comment” faz um comentário em uma determinada regra.

Configuração das Interfaces

Para uma melhor configuração do servidor deve-ser feito um cronograma do que será feito

o sistema será: servidor? load balance? roteador de borda? faixas de ips?que link será utilizado?



Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

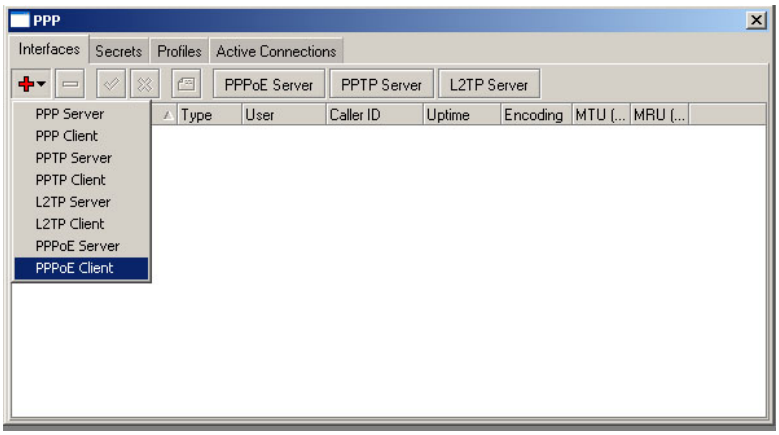
em modo bridge e quem fará a discagem será o próprio Mikrotik.

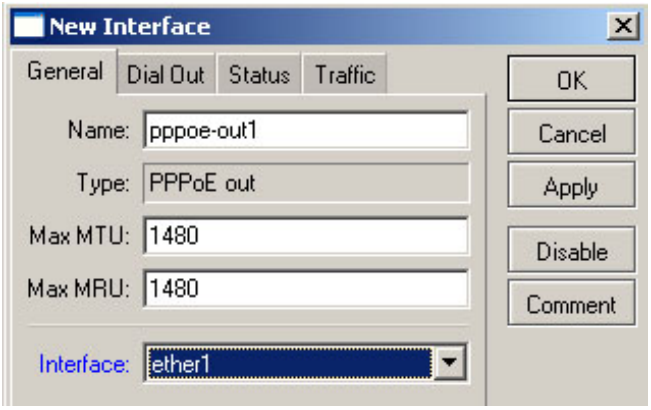
Agora na interface ether você deverá conectar o cabo de rede que sai do seu modem adsl para o mikrotik, obs esse cabo é normal.

Menu PPP / interfaces

você dará um clique no botão de “+” localizado na parte superior esquerda.

Escolha a opção PPPoE cliente e configure da seguinte forma:



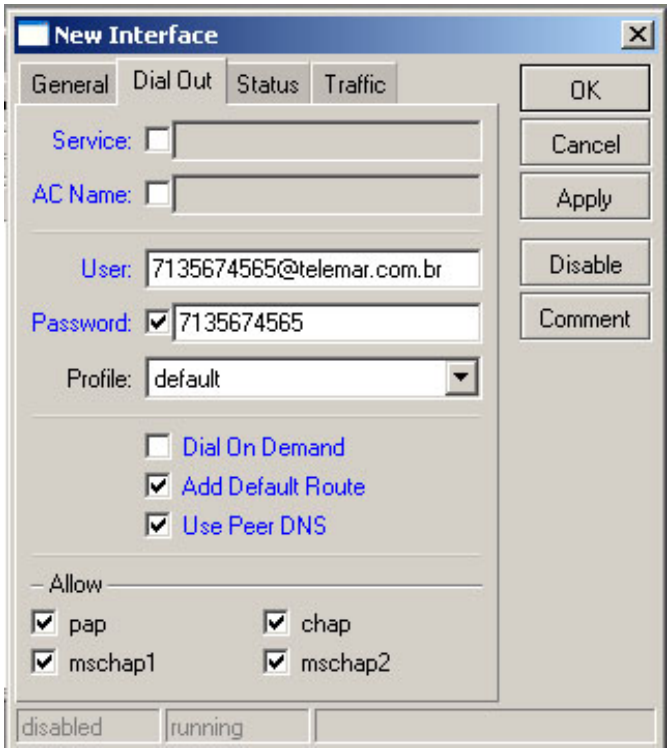


Name: coloque um nome tipo: LINK, ou WAN

1. Max MTU / MRU – deixe a default 1480 ou então 1500
2. Interface - escolha a placa que está ligada ao modem.

Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

Aba Dial Out:



Aqui você colocará as informações do seu login de acesso.

1. **Service:** não precisa colocar nada.
2. **AC Name:** Não precisa colocar nada
3. **User:** o seu login de acesso.
4. **Password:** a senha de acesso
5. **Dial On Demand:** discar por demanda, no nosso caso deixar desmarcado para a conexão sempre fica ativa e não precisar conectar manualmente.
6. **Add Default Route:** adiciona uma rota padrão para essa conexão
7. **Use Peer DNS:** Utiliza essa conexão para pegar os endereços de DNS,

   podemos deixar desmarcado caso queira colcoar manualmente os DNS em IP / DNS

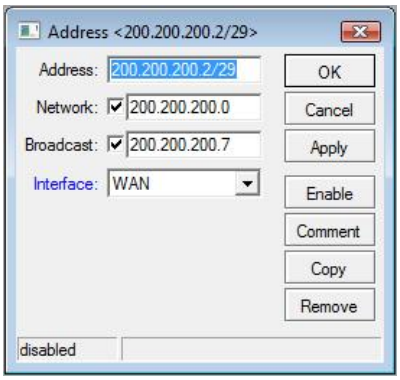
8. **Allow:** Deixar marcado todas as formas de protocolos.

Pronto clique em **apply** e depois em **enable** para habilitar a interface e que ele comece a fazer a conexão, você pode verificar o status da conexão no rodapé se você está (PPPoe interface). O status são
dialing ..... Discando
stabilished ..... Estabelecida
connected ..... Conectado
disconnected ..... Desconectado

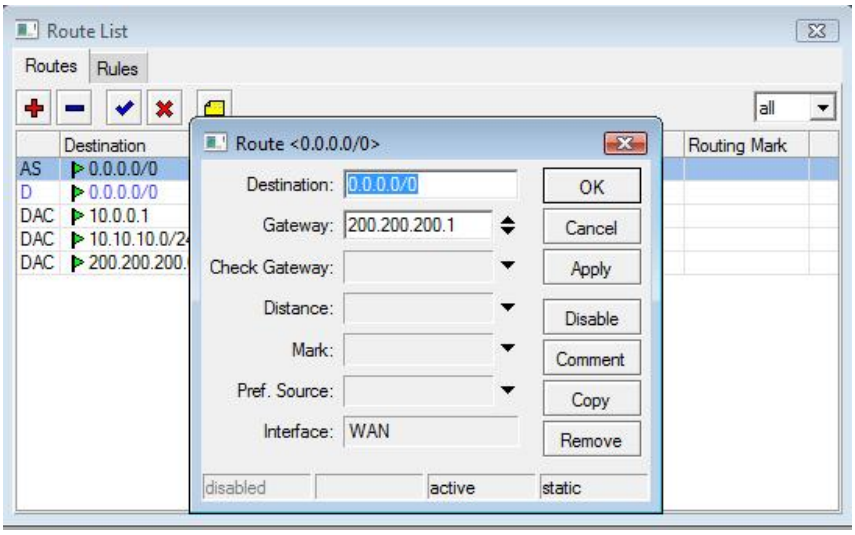
Usando IP statico (LINK DEDICADO)

O uso de Ip dedicado por provedores vem sido mais usado, pela garantia de banda e também pela qualidade. Vamos configurar nosso mikrotik usando o ip: 200.200.200.2/29 e o nosso gateway será o 200.200.200.1 (Roteador Cisco)

Vamos em IP ADDRESS e Adidiona-se o IP
Lembrar de colocar a interface correta, fazer logo após um teste simples de ping no terminal do mikrotik para o IP do gateway "200.200.200.1" ele tem que responder

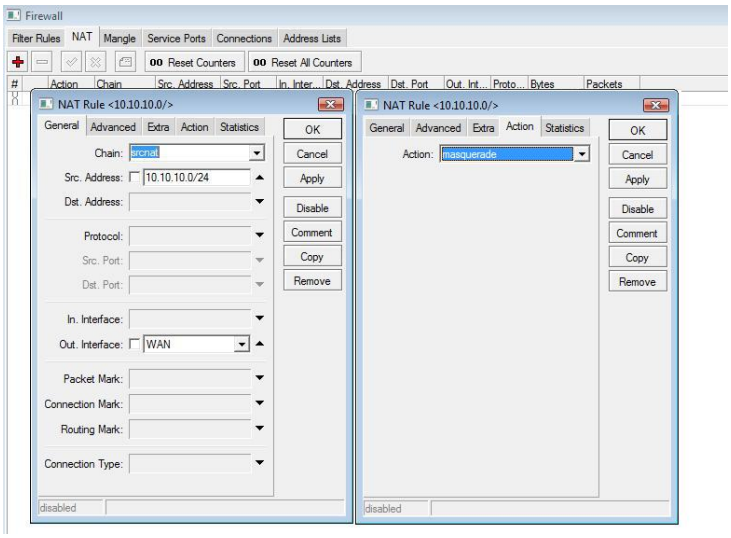


Após ir em IP ROUTE



Aperta em + e adiciona-se o gateway igual a figura acima, quando apertar em APPLY ele vai mostrar abaixo se está ACTIVE "ATIVO" e em Interface ele já mostra se realmente fechou o link.

Para finalizar o acesso O NAT no firewall
IP FIREWALL NAT e adiciona-se a seguinte regra Onde:chain: srcnat "origem"Src.Address: 10.10.10.0/24 "ip dos clientes
Out.Interface: LINK"interface onde tem internet"
Action: Masquarede "mascarar" após essa configuração a rede10.10.10.0/24 será integrada a rede WAN, sendo que a WAN
está sendo "NATEADA"para a rede Local.



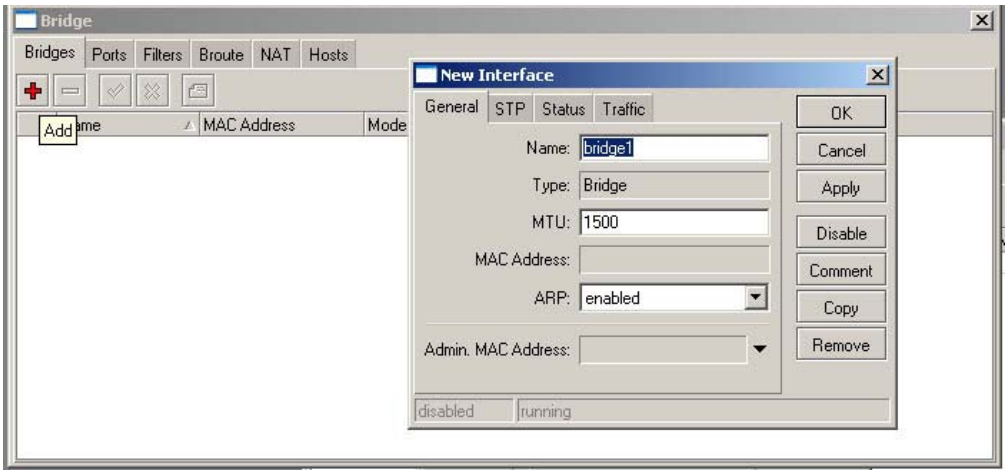
Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

Bridge Transparente

Com as configurações das principais interfaces iremos centralizar todas elas numa interface que fará o bridge transparente repassando todo o trafego para esta interface.

Menu Bridge

Clique no menu Bridge e depois no sinal de “+” da aba Bridges para adicionarmos uma nova interface.

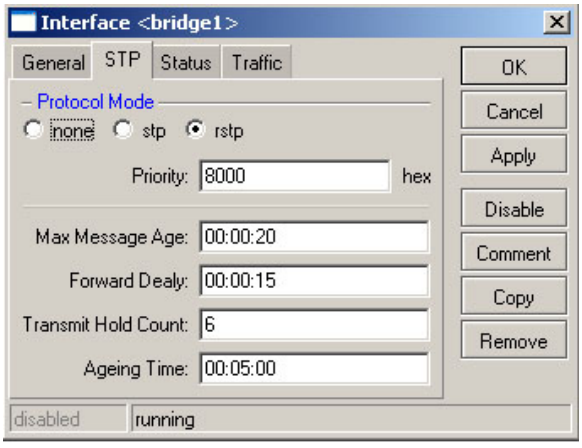


Aba General

1. **Name -** é o nome dado a interface
2. **Type -** o tipo de interface
3. **MTU -** deixa default
4. **MAC -** Address: será automático e definido pelo sistema.
5. **ARP –** deixa em enable ou Reply-only se for fazer controle de IP X MAC
6. **Admin. MAC –** deixa em branco como está. ou colocar um mac caso queira

Aba STP

O protocolo STP (Spanning Tree Protocol) foi criado para recuperar uma conexão perdida, o protocolo RSTP (Rapid Spanning Tree Protocol), é a evolução do STP com a função de buscar o melhor caminho para a continuação dos dados, esse protocolo é uma especie de uma rede tipo mesh,



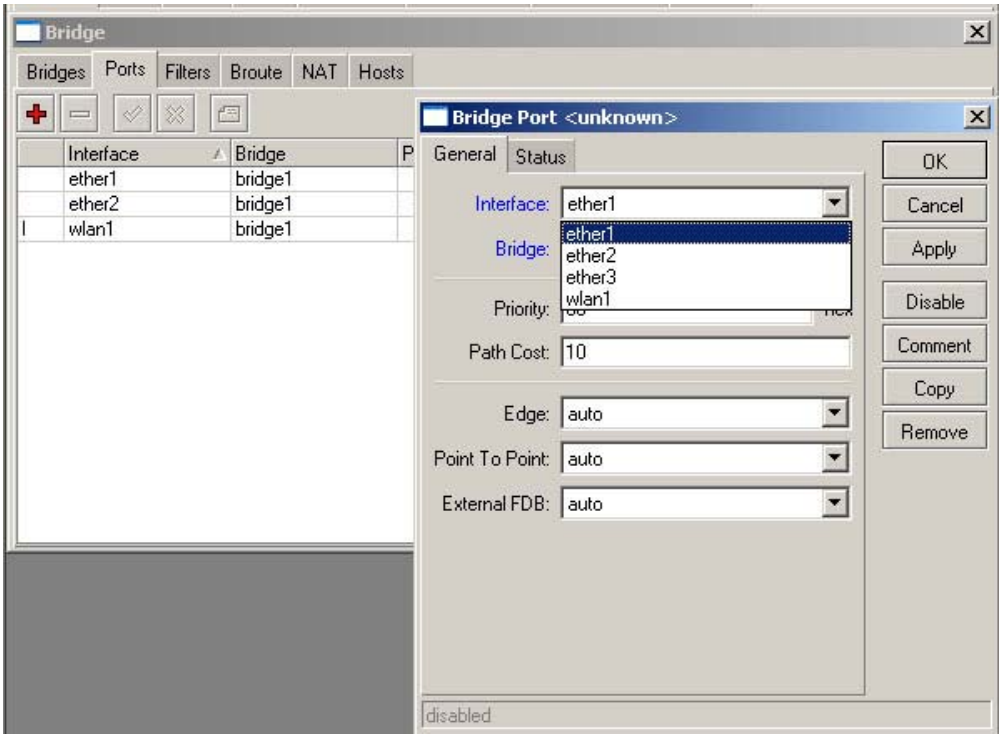
Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

então a configuração ficará como da imagem acima, você só precisará marcar o protocolo rstp e o resto ficará em defaut.

Concluímos a bridge clique em **Aplly**, **enable** e depois **OK.**

Ainda em Bridge vamos para a aba Ports

Aba Ports



Na Aba ports clique no botão “+” para adicionarmos as Interfaces que farão parte da bridge

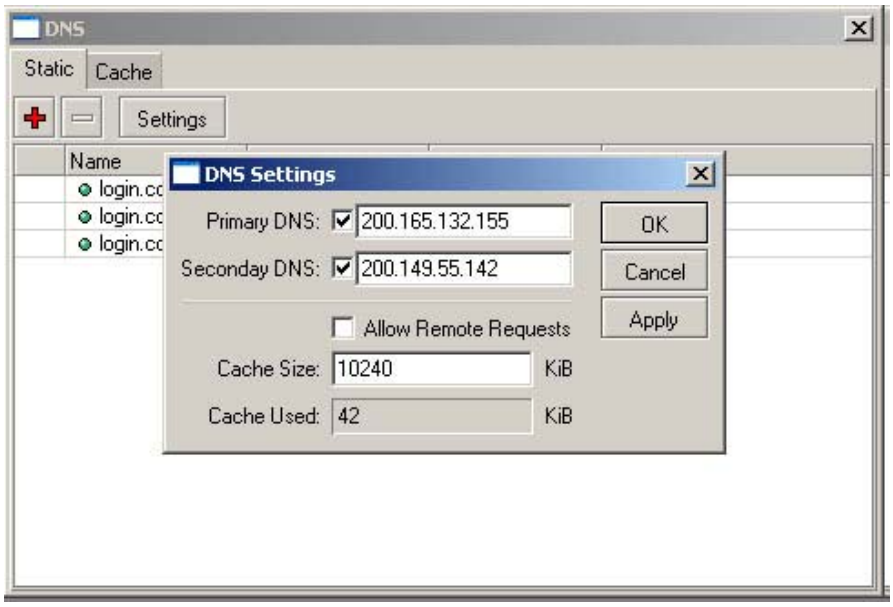
- Clique em Interface e depois coloque as interface da lista clique no botão apply e depois no botão Ok, repita o procedimento para todas as interfaces existentes.

Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

Configurando o DNS

O DNS será o do seu ISP, o DNS abaixo é do velox, você pode usar também um OpenDNS

208.67.222.222 e 208.67.220.220

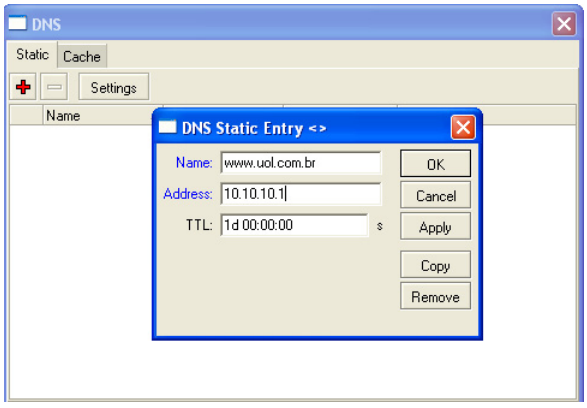


Para configurar o DNS acesse o menu IP depois o sub-menu DNS.

Aba Static clique em SETTINGS

1. Primary DNS – coloque o DNS primário.
2. Secondary DNS – coloque o DNS Secundário.
3. Allow Remote Request - deixar marcado para permitir requisições remotas.
4. Cache Size – O tamano do cache para o DNS fará uma armazenamento temporário das ultimas páginas visitadas pelos clientes em um cache de até 10mb no caso como é KiB cada 1mb = 1024 KiB então 10mb = 10240 KiB

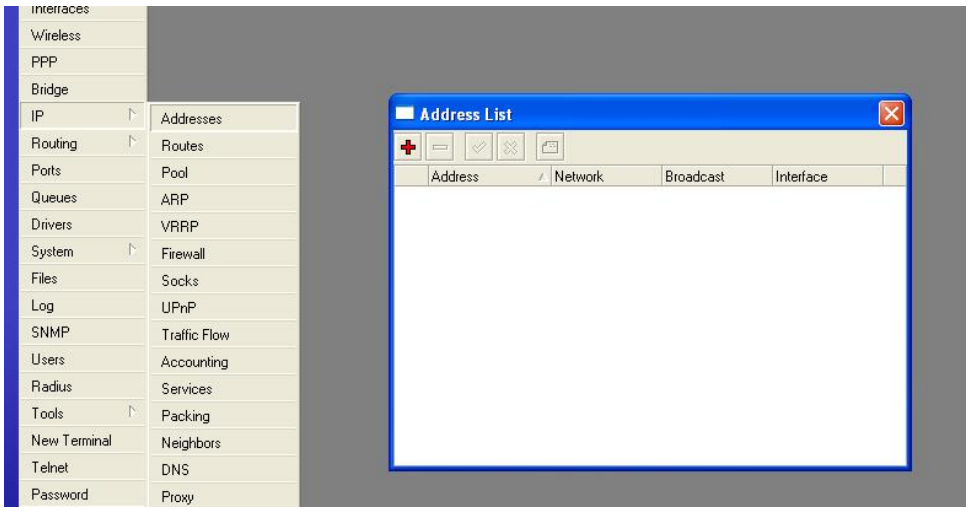
isto faz com que o site adicionado em static seja redirecionado para o ip abaixo .
é uma espécie de resolução do site localmente



Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

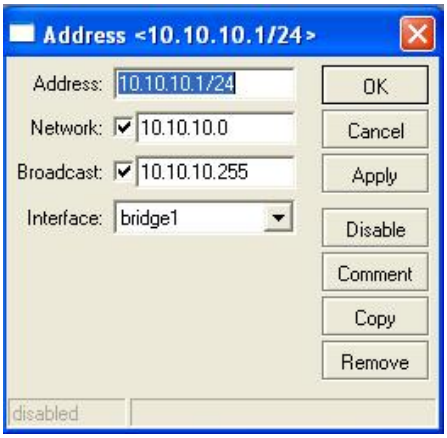
Configurar IP

Para colocar um ip a interface você vai em: IP ADDRESS
como estamos trabalhando com uma bridge, vamos atribuir um ip para a mesma.



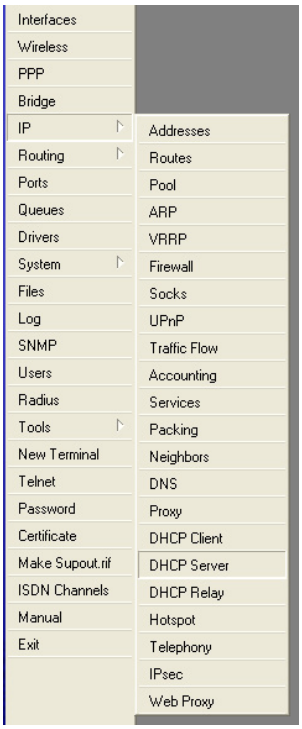
vamos colocar o ip 10.10.10.1/24
o mikrotik se encarregará de colocar a rede e o broadcast, lembrando-se de escolher a interface.

caso vc não saiba qual classe colocar você pode colocar da seguinte forma:
10.10.10.1/255.255.255.0 que o mikrotik converte automaticamente para a faixa escolhida.

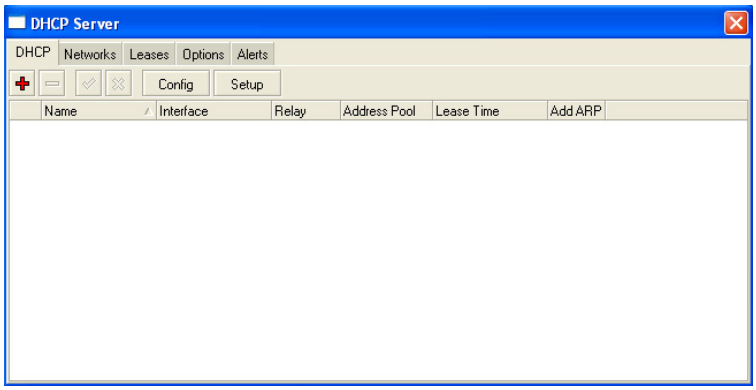


Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

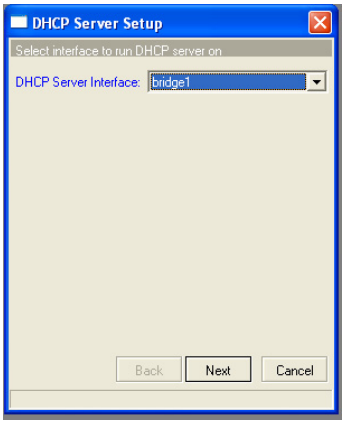
Configurar um servidor DHCP



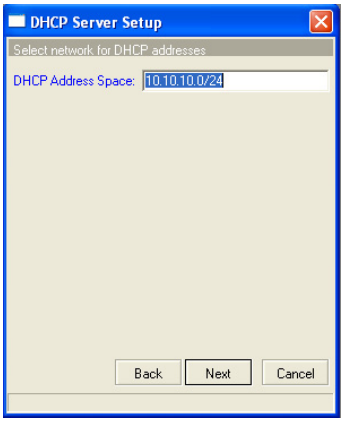
Vamos no Menu IP / DHCP-SERVER
Depois utilizaremos o Wizard do mikrotik apertando no botão SETUP



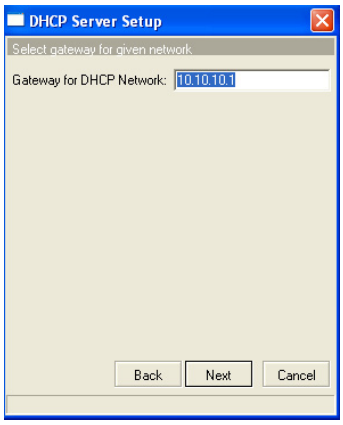
Segue os Seguintes Passos Abaixo:
Escolhe qual interface vai ser a Server de DHCP



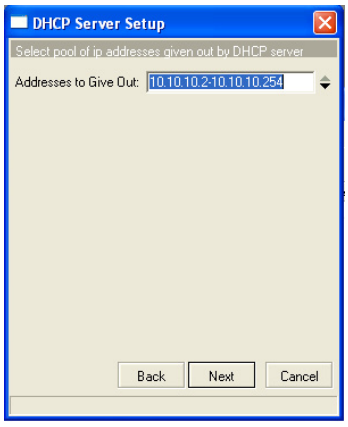
Escolhe a interface



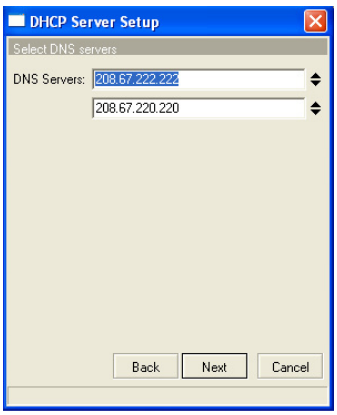
escolhe a classe de ips



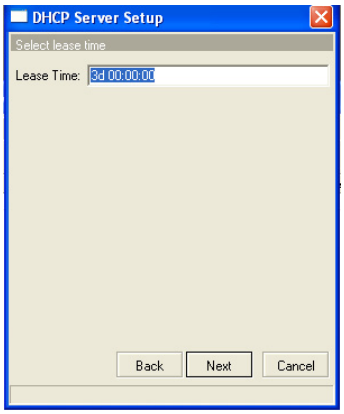
escolhe o gateway



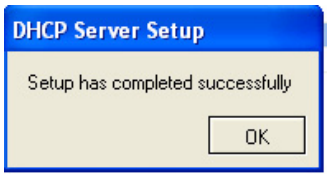
os ips que serão atribuidos



Escolhe os DNS



O tempo do Lease

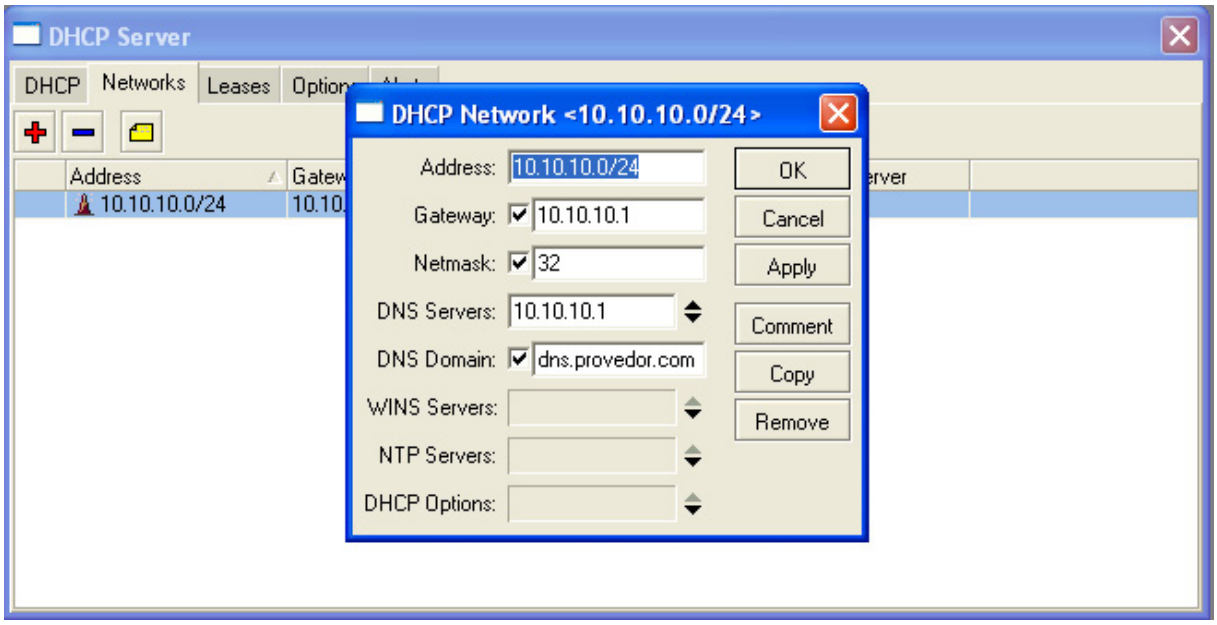


Configurado com sucesso

Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

Network

Nessa parte você pode deixar o dhcp configurado dessa forma



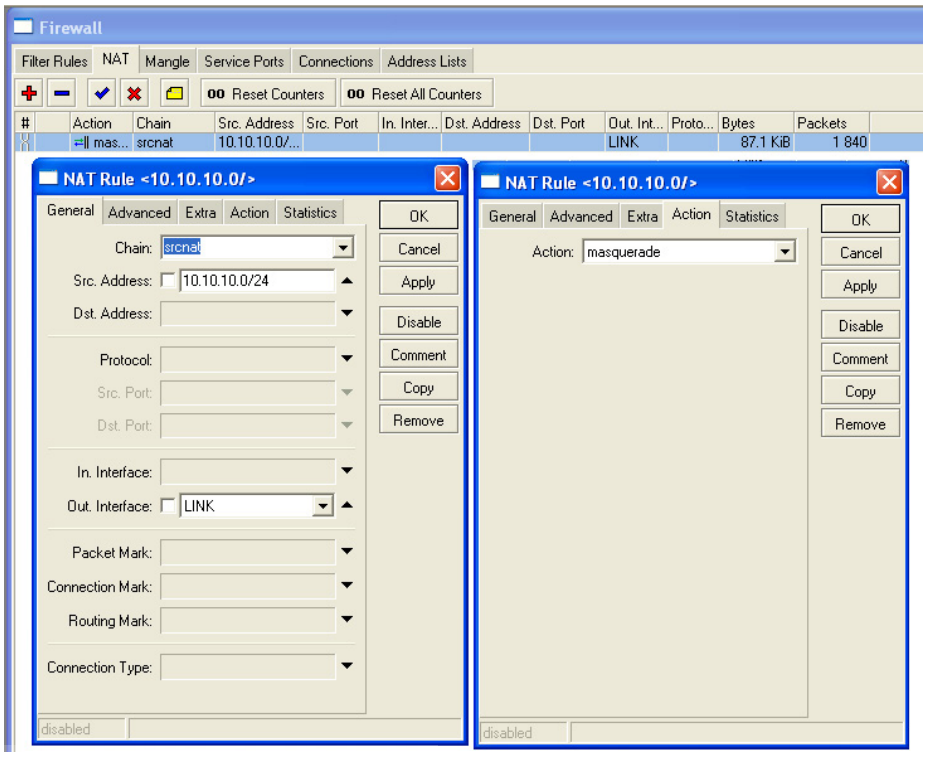
Address: endereço da rede
Gateway: endereço da placa do mikrotik
Netmask: 32 para ficar mascara fechada 255.255.255.255 ou em branco para ficar 255.255.255.0
Dns Servers: ip do mikrotik, para não aparecer no cliente o ip do dns usado no server
Dns Domain: nome do server dns, caso visto no ipconfig /all

NAT

Para finalizar o acesso O NAT no firewall
IP FIREWALL NAT e adiciona-se a seguinte regra

Onde:
chain: srcnat "origem"
Src.Address: 10.10.10.0/24
"ip dos clientes
Out.Interface: LINK
"interface onde tem internet"
Action: Masquarede "mascarar"

após essa configuração a rede 10.10.10.0/24 será integrada a rede LINK, sendo que a LINK está sendo "NATEADA" para a rede Local.



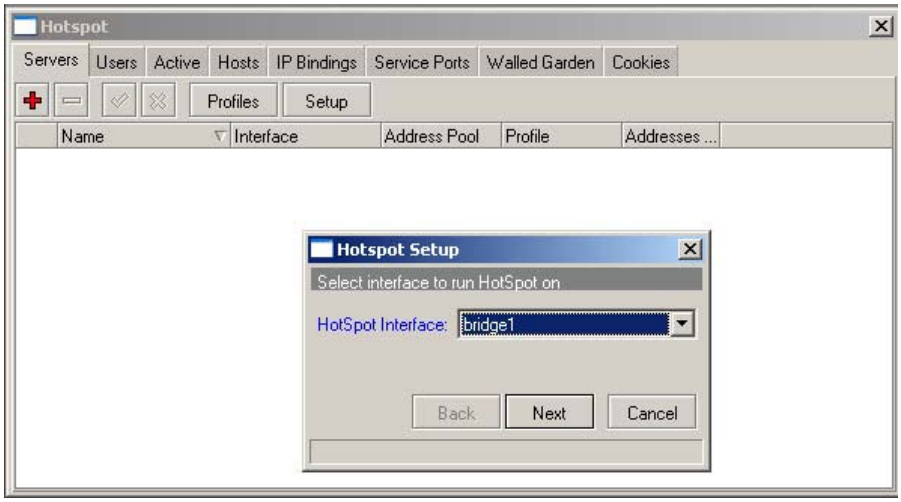
Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

Configurando Hotspot

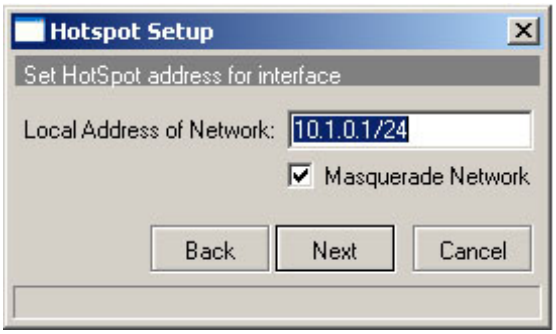
A configuração de um Hotspot é simples e os passos a seguir serão bem intuitivos.
Vá para o menu Ip submenu Hotspot

Aba Servers

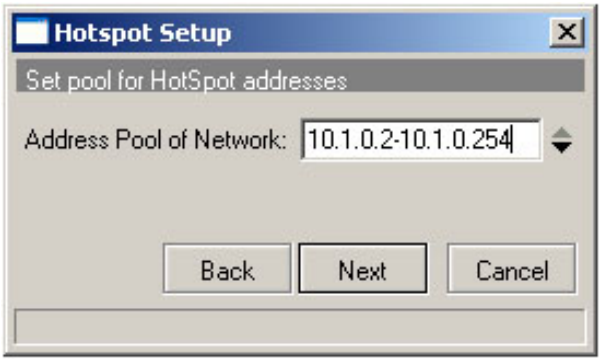
Nesta parte configuraremos o servidor de hotspot usando o botão setup.



1. **[Select Interface to run Hotspot on]**, você deverá selecionar a interface que terá o hotspot, escolhemos a bridge anteriormente criada. depois Clique em **next**
2. **[set HotSpot address for interface]**,escolha o ip da rede e sua máscara, Escolha Assim como na figura abaixo com uma máscara /24. Clique em **next**

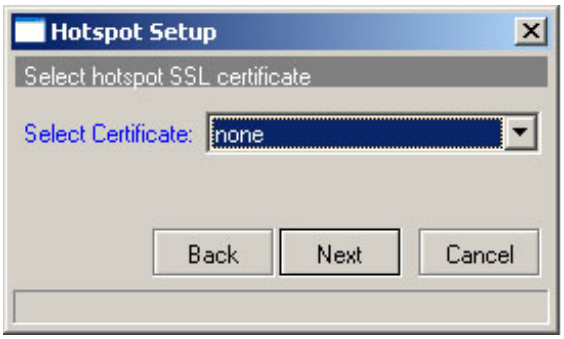


3. **Passo 3 [Set pool for HotSpot address]** o pool é justamente a faixa de ips que estarão disponíveis para os clientes, ele será definido automaticamente a partir do ip e máscara de subrede que você definiu no passo 2. Clique em **next**

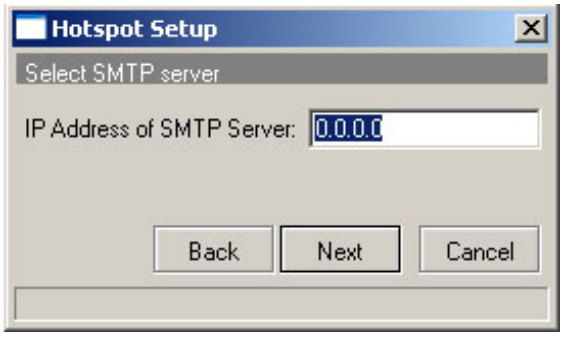


Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

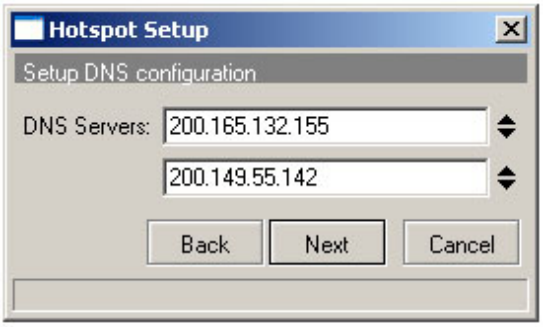
4. [Select hotspot SSL certificate], a certificação digital é uma forma degarantir que o seu sistema é seguro para os usuários, o sistema mikrotik trabalhacom certificação digital. clique em **next**



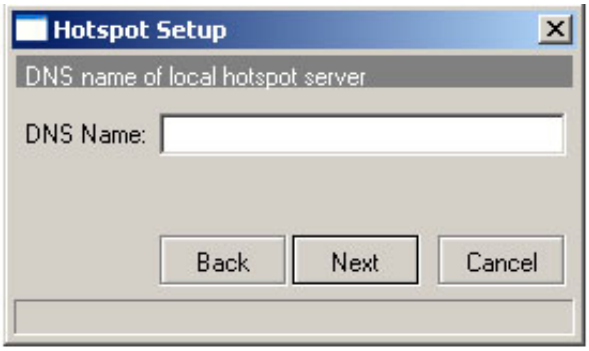
5. **[Select SMTP server],** essa configuração não abortará serviços de SMTP, por tanto deixe o ip em 0.0.0.0 e clique em **next**



6. [Setup DNS configuration], como já haviamos configurado o DNS anteriormente o sistema preencherá sozinho com o DNS já atribuído. Clique em **next**



7. [DNS name of local hotspot server] – é o endereço que ira aparecer quando forem redirecionado para a tela de login no navegador, deixe em branco ou coloque um nome e clique em **next**

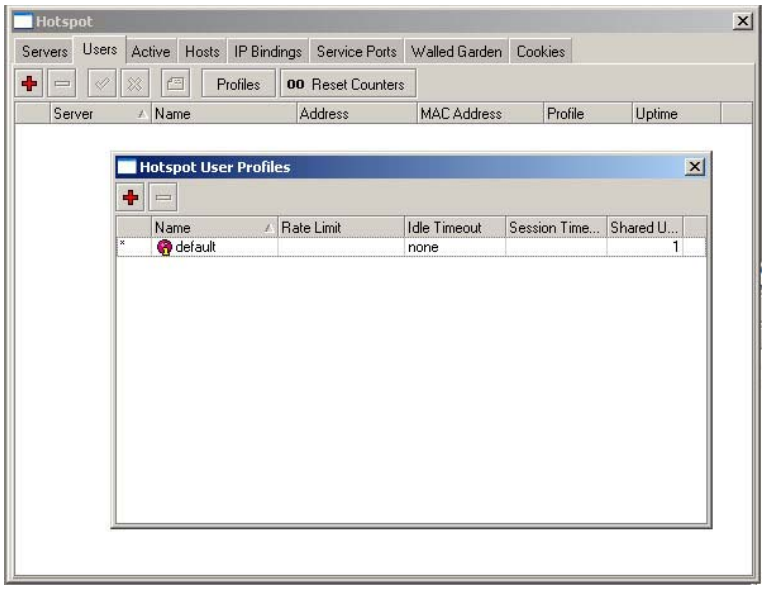


Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

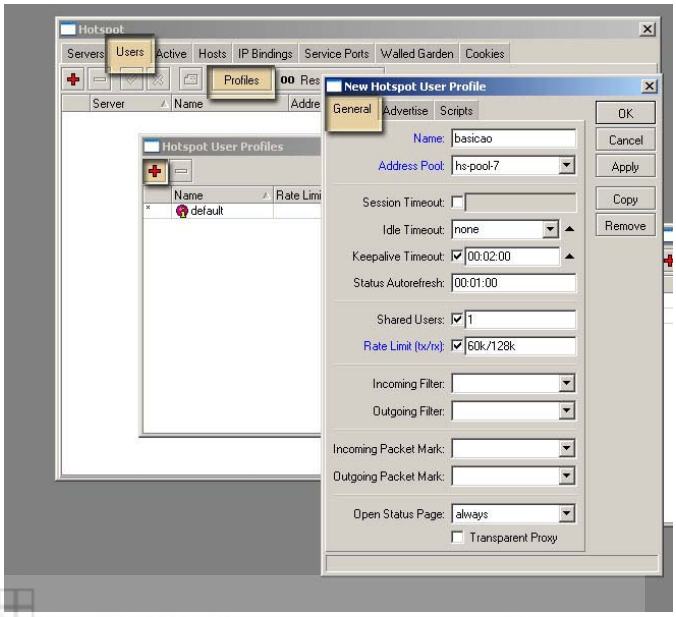
8.**[Create local HotSpot user]** – coloque uma senha para a conta admin para poder acessar pela primeira vez, depois clique em **next**

Criando Perfis

Os perfis no hotspot serve para definir uma configuração para determinados grupos, serve por exemplo um controle de banda.
Vamos configurar o Servidor para fornecer dois tipos de acesso um básico de 64k/128k e um avançado de 64k/256k.

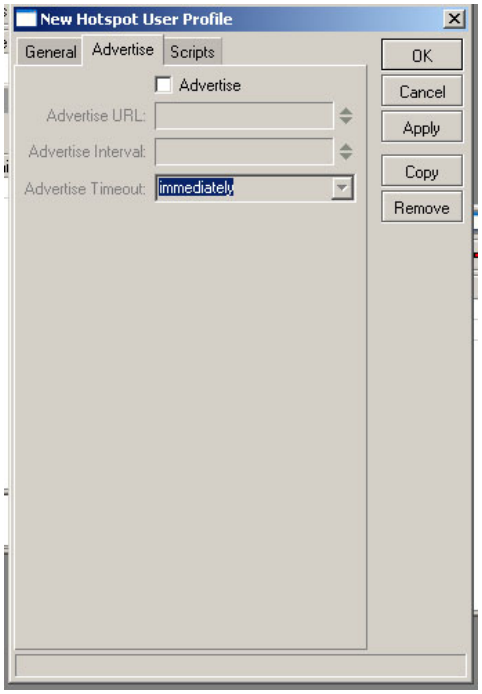


1. No menu **Hotspot** vá para a aba **Users** e clique em **profile**.
2. Dentro de **Hotspot User Profile** clique no sinal "**+**" para criarmos um novo profile



Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

3. **Aba General**
   1. **Name** – o nome do seu plano, Ex: 128K
   2. **address pool** – coloque a faixa de ip que foi criada no inicio.
   3. **Session Timeout** – Tempo permitido para o cliente quando inspirado ele é derrubado pelo sistema.
   4. **Idle Timeout** – tempo de inatividade para o sistema derrubar a conexão
   5. **Keepalive Timeout**: - coloque 00:02:00
   6. **Status Autorefresh:** - período que o sistema atualiza todos os dados do hotspot.
   7. **Shared Users:** número de usuários permitidos para o mesmo username, esta função compartilhará o mesmo usuário para o número de clientes que você definir. Caso não queira mais de 1 log por user mesmo clonando mac as apenas um usuário estará conectado.
   8. **Rate Limit (tx/rx):** Limitação da velocidade. primeiro Upload depois Download
      Ex: 128k/256k 128 kbps para upload e 256 kbps para download.
   9. **Aba advertise:** ela envia de tempo em tempo pop-up para os clientes que estiverem neste perfil, pode ser muito útil para publicidade e comunicação com os seus cliente.

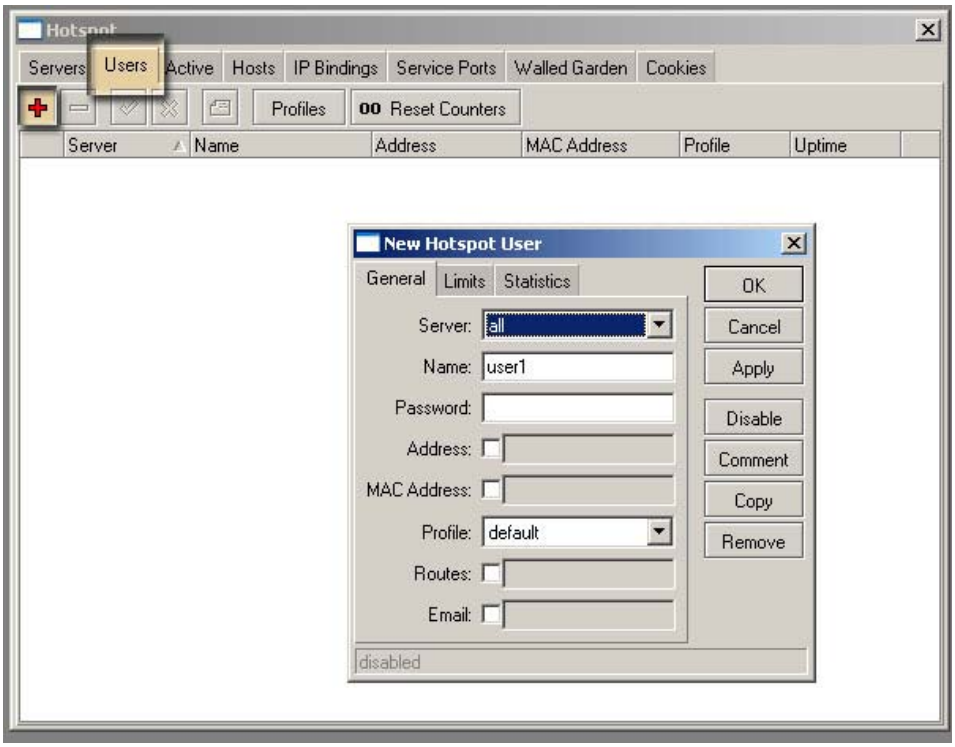


1. **Advertise URL** – página que será exibida para o cliente poderá ser mais de uma seguindo uma sequência.
2. **Advertise Interval** – Intervalo para exibição do pop-up.
3. **Advertise Timeout** – Quanto tempo deve-se esperar para o anúncio ser mostrado,antes de bloquear o acesso a rede pode ser:
   Never = Nunca
   Immediately = Imediato
   Tempo = Ex: 1 minuto.

Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

Criando Usuários

Após termos criado o profile vamos adicionar nossos clientes e definindo o seu perfil, assim como ver dados relevante sobre o mesmo como tempo de uso, quantidade de pacotes trafegado, e muitas outas opções.
Menu **hotspot** aba **users** sinal de **"+"**.

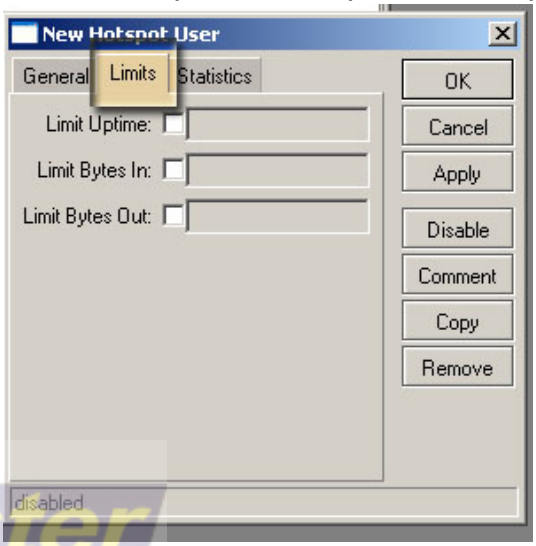


Aba general

1. **Server** – escolha o servidor hotspot que criamos ou pode deixar em all
2. **Name** – nome do usuário, ele se logará com esse nome.
3. **Password** – senha para o cliente você poderá deixar em branco ou poderá
4. **Address** – endereço de ip para o cliente
5. **MAC Address** – o mac do cliente você poderá adicionar amarrando o mac ao login.
6. **Profile** – escolha o profile com a velocidade do cliente.
7. **Routes** - deixe em branco – define uma rota especifica para o cliente
8. **e-mail** - deixe em branco – coloca o e-mail do cliente

você poderá estabelecer um contrato mensal de dados trafegados, ou poderá limitar o tempo de uso dos seus clientes. Um serviço ideal para Hotéis ou locais que vendam pacotes Pré-pagos

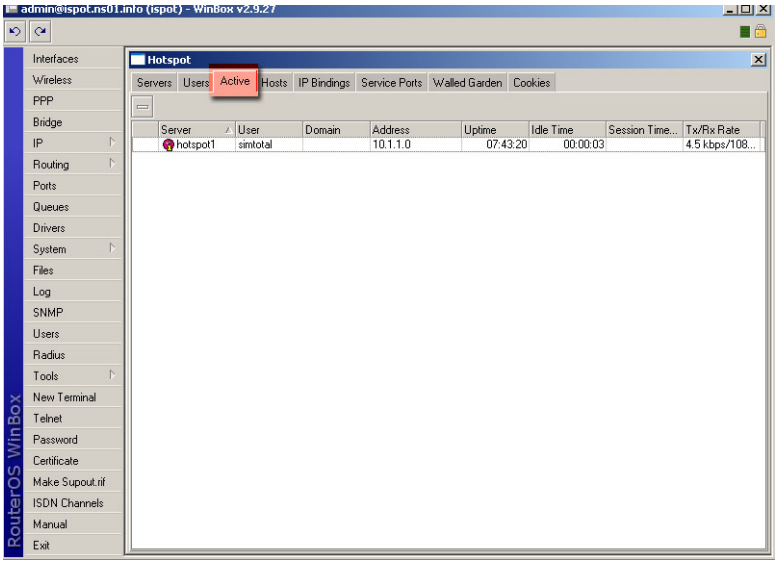
1.**Limit Uptime** – limita o tempo de conexão do seu cliente
2.**Limit Bytes In** – Limita quanto seu cliente poderá dar de download
3.**Limit Bytes Out** – Limita quanto seu cliente poderá de upload



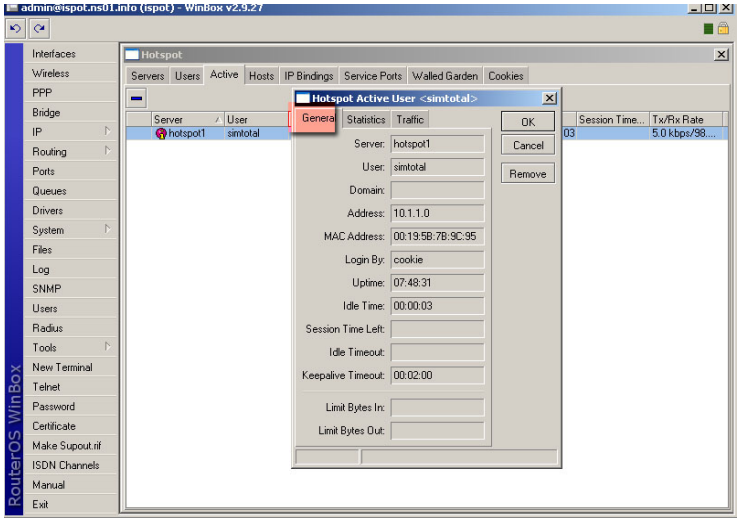
Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

Quem está On-Line "CONECTADO"

O mikrotik permite que você possa ver quem está conectado, quanto tempo aquele cliente está conectado, quanto tempo de uso e quanto foi o tráfego dele.
Vá para a aba **active** do menu **Hotspot**



Todos os clientes que estiverem na aba active significam que estão conectados, aqui você verá quem estar conectado, qual o endereço ip quanto tempo ele está ativo quanto tempo ele está inativo e qual a sua taxa de transferência e de recebimento.



Clicando duas vezes no cliente você verá:

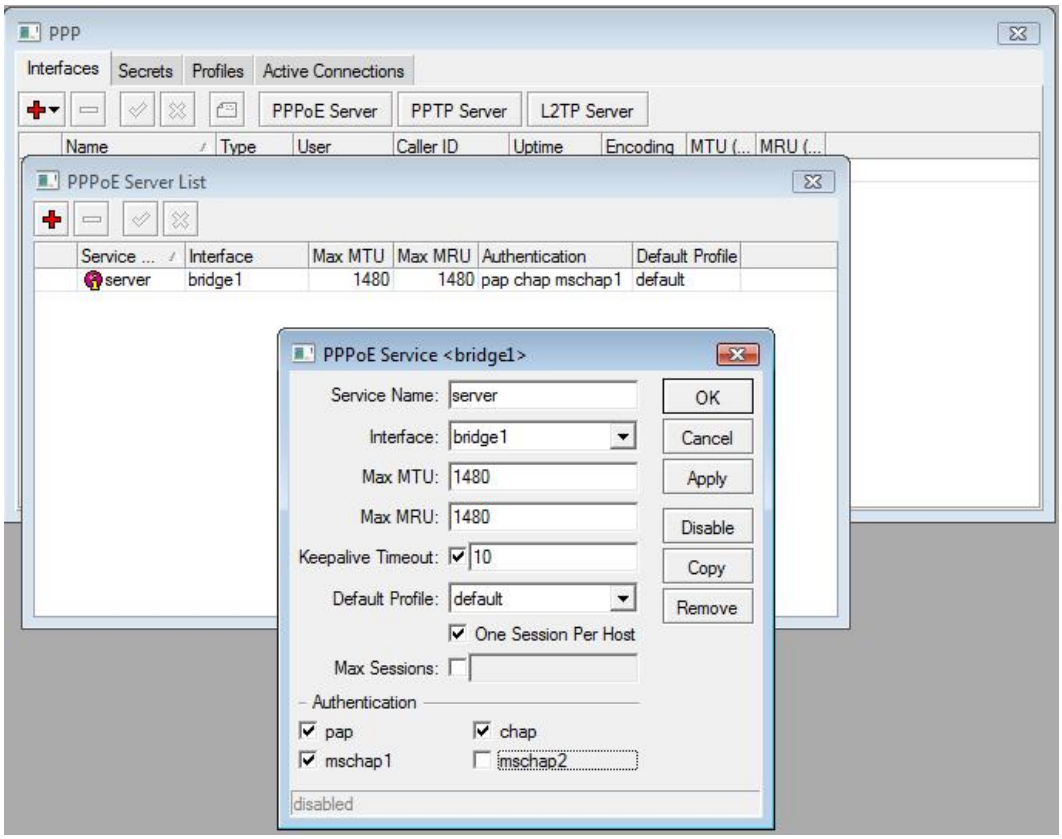
1. **Server** – servidor hotspot que ele está conectado.
2. **User** – nome do usuário conectado.
3. **Address** – endereço de ip.
4. **MAC Address** – Endereço físico da placa do cliente
5. **Login By** – define como o cliente se logou. O mikrotik deixa um cookie nos clientes não exigindo que ele digite toda vez que for acessar a internet seu login e senha, o tempo de expiração pode ser configurado.
6. **Uptime** – tempo de conexão
7. **Idle Time** – tempo ocioso da conexão

Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

SERVIDOR PPPoE

PPPoE (Point-to-Point Protocol over Ethernet) é um protocolo para conexão de usuários em uma rede, é uma VPN onde não tem interferência de meios externos. vamos configurar nosso servidor em:

PPP / PPPoE Server



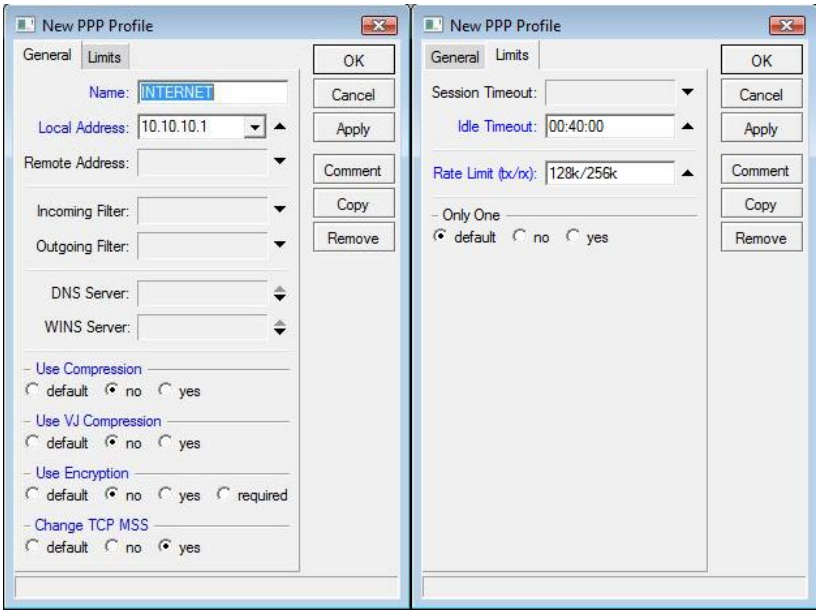
1 Service name: Coloca-se um nome para o servidor
2 Interface: Escolhe a interface dos clientes
3 Max MTU: Deixar 1480 ou escolher um valor entre 1360-1492
4 Max MRU: Deixar 1480 ou escolher um valor entre 1360-1492
5 Keepalive timeout: É o tempo para se conectar, caso não conecte é derrubado
6 Default Profile: Deixar Default "Iremos abordar na proxíma pagína"
7 One Session per host: Deixar marcado caso queria apenas um cliente com o mesmo nome
8 Max Session: defini a quantidade maxima de clientes
9 Authentication: deixar marcados todos, exceto o MSCHAP2, por ter uma falha de segurança caso queiram saber pesquisem sobre ASLEAP

Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

Profile PPPOE

Iremos fazer um profile do pppoe para poder atribuir umas mudanças no PPPoE e também para colocarmos o gateway ao invéz de colocar no secret.

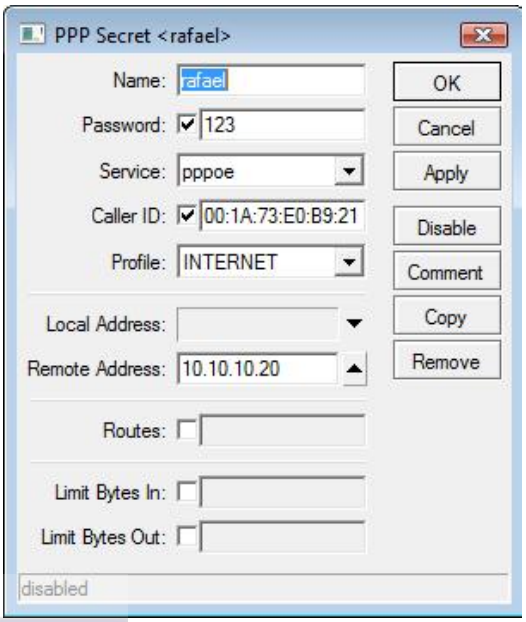
PPP / PROFILE



1 Name: coloca-se um nome para o profile Ex: INTERNET
2 Local Address: coloca-se o ip do gateway, no caso o ip da placa dos clientes
3 Use Compression: NO "não usar compresão"
4 Use VJ compression: NO "não usar compresão"
5 Use Encryption: no "não usar encripitação"
6 Change TCP MSS: Yes "tamanho máximo de segmento"
7 Idle Timeout: Tempo para derrubar a conexão caso haja inatividade
8 Rate Limit (tx/rx): Serve para prender a velocidade do profile, mas no nosso caso não iremos usar pois iremos prender a velocidade no Queue Simple, para podermos fazer as pagínas de gráficos dos clientes

CRIAR UMA CONTA DE USUÁRIO

Cadastrar em: **PPP / SECRET / +**



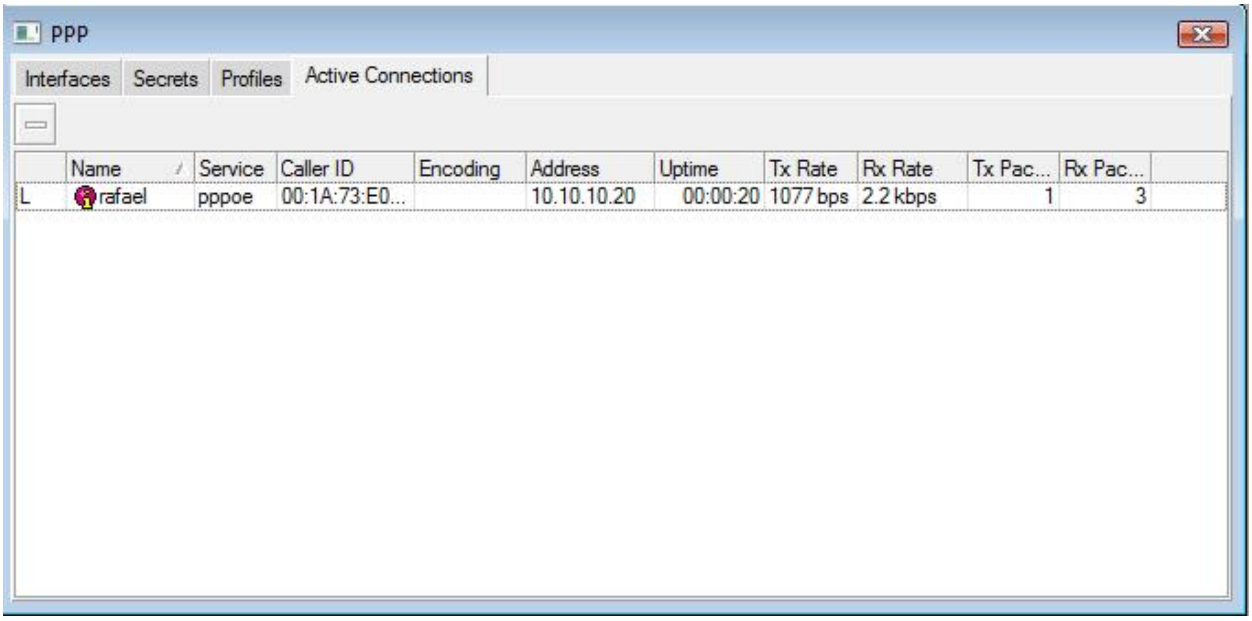
1 Name: nome do cliente
2 Password: senha da conta
3 Service: PPPOE ou ANY
4 Caller ID: MAC,serve para prender user+senha+mac
5 Profile: INTERNET o profile criado anteriormente
para evitarmos de clocar sempre o local Address
6 Remote Address: Endereço de IP do cliente

Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

Active connections

Serve para verificar os clientes que estão conectados e também derrubar as conexões, monitorar tráfego etc..

PPP / ACTIVE CONNECTIONS

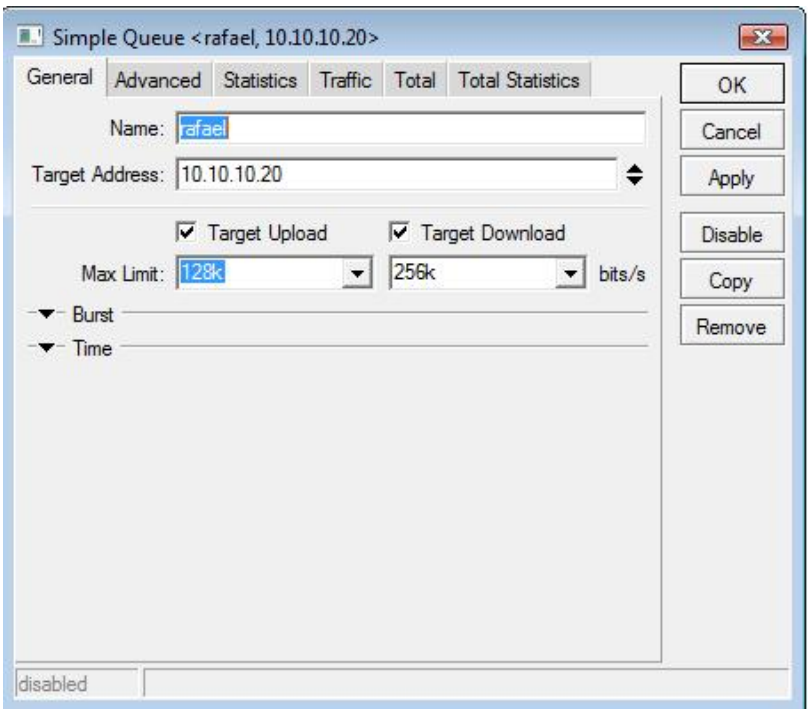


Para desconectar um cliente do Pppoe seleciona o cliente e aperta no -
para pingar para um cliente clica com o direito emcima do cliente e escolhe PING

CONTROLE DE BANDA

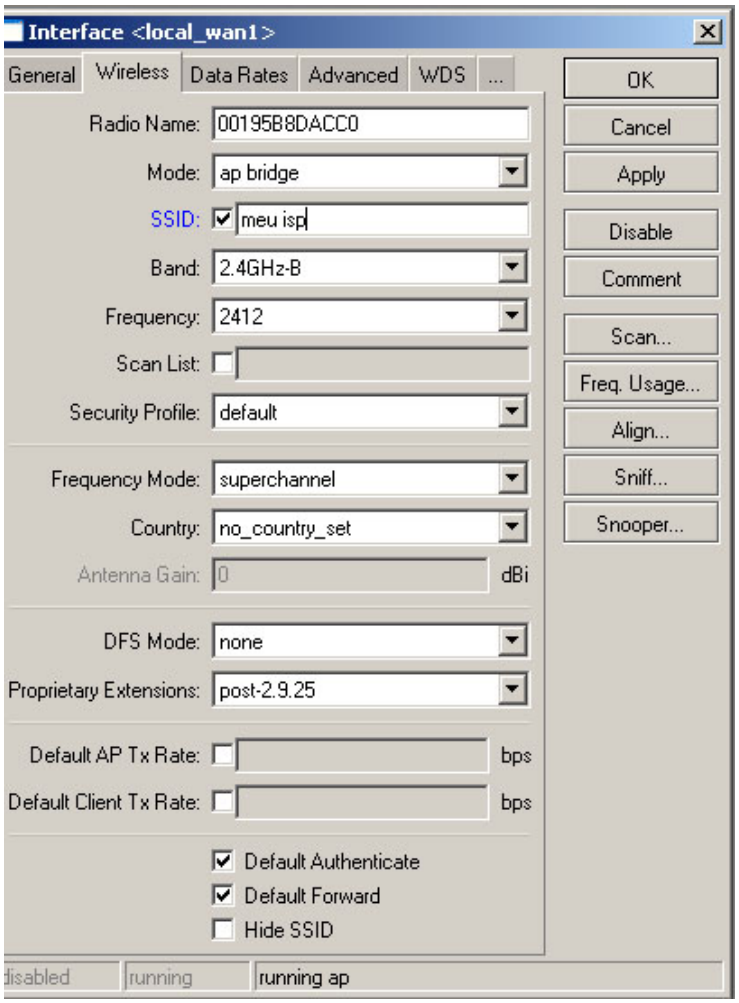
vamos cadastrar o ip dessa conta para ter a velocidade de 128k de up e 256k de download
vamos em QUEUE SIMPLE

1 Name: Nome do cliente
2 Target Address: ip do cliente
3 Max Limit: respectivamente velocidade de Up e Down



Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

INTERFACE WIRELESS



Na aba wireless serão feitas as configurações básicas do sistema na conexão wi-fi configure como está na imagem.

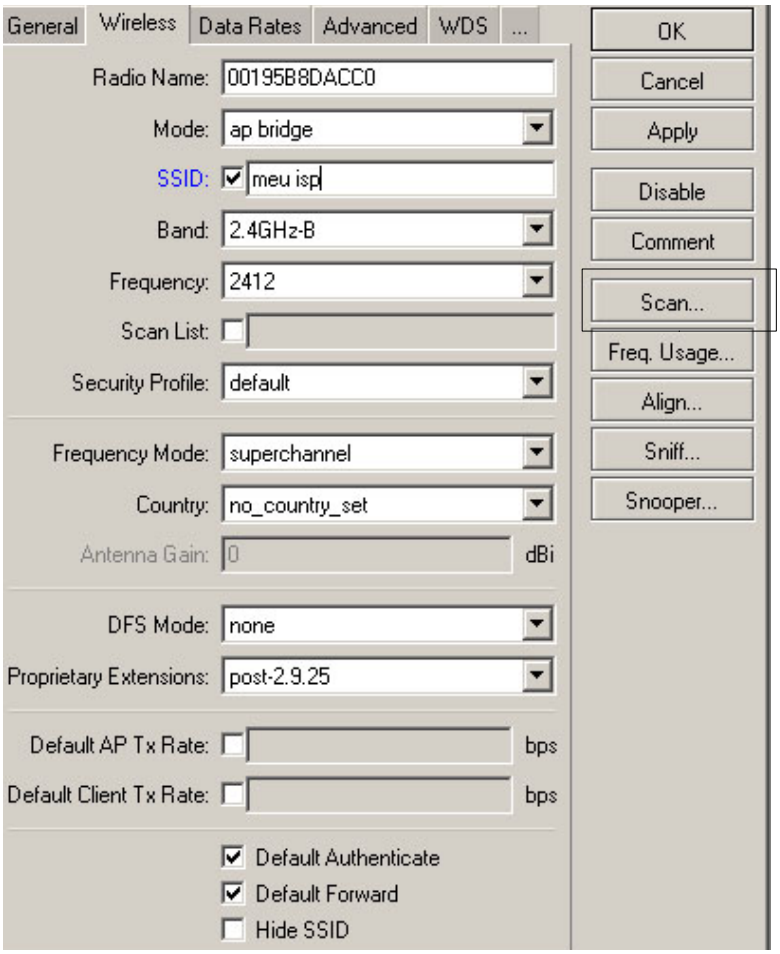
1. **Radio Name:** O nome usado para identificar a interface "atravez de outro mikrotik"
2. **Mode:** o modo de funcionamento do rádio para a função que você quer destinar a ele.

- **Station:** modo cliente
- **Station WDS:** possibilita repassar os endereços realizando um bridge transparente.
- **Ap-Bridge:** Funciona como um access-point
- **Bridge:** faz apenas o papel de bridge
- **alignment-only:** para realizar alinhamento de antenas.
- **Nstreme-dual-slave:** para funcionar em Nstreme, protocolo proprietário da mikrotik.

Wds-slave: retransmite o sinal de um outro ap que esteja em wds principal.

Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

3. **SSID:** serve para dar nome a sua rede, ou seja as pessoas que captarem seu sinal estarão enxergando esse nome.
4. **Band:** as bandas já foram descritas anteriormente mais vamos relembrar apenas o que é importante, a banda de 2.4ghz"b" e "g" é a banda usada por quase todos os laptops , computadores e placas wi-fi existentes no mercado, a banda de 5.8ghz banda "a" é usando apenas para realizar ptp por alcançar maiores trefégos.
5. **Frequency:** a frequência usada aqui determinará em que canal você estará trabalhando. Vale falar que sinais iguais causam ruído e perda de sinal, então busque um canal ainda não utilizado ou utilize um canal que menos houver no local. Você poderá usar o Freq. Usage logo abaixo do Scan para que você possa ver os canais que não estão sendo usados.



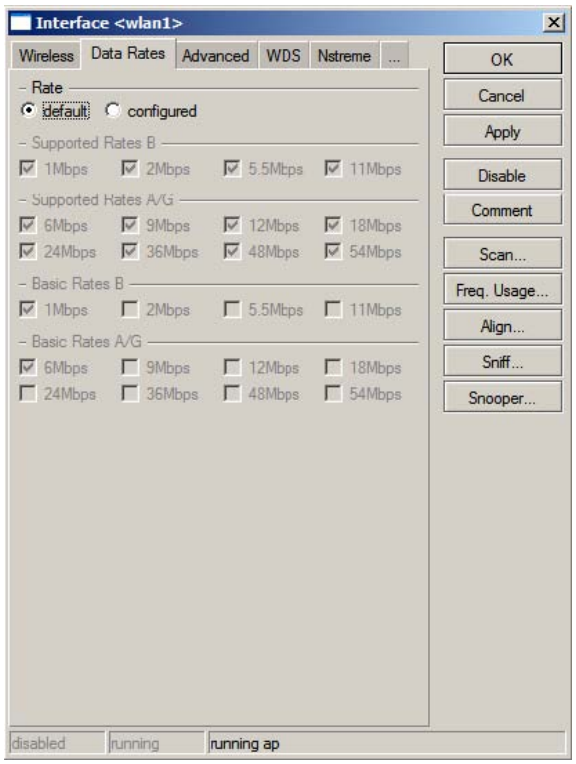
6.Scan List: Scaneia uma lista de frequências, não utilizaremos este recurso
7.Security Profile: serve para você colocar uma criptografia, seja WEP ou WPA no menu WIRELESS / SECURITY PROFILES
8. Frequency Mode: o modo de frequência escolhe entre canais normais entre 1 e 11 ou usar o superchannel, onde tem se os chamados Overlap de canais, onde chega a 74 canais Aqui usaremos manual Tx Power, para não ter erro na hora de colocar um canal onde as placas dos clientes não encontre e não funcione dentro do estabelecido em lei. Em frequency mode teremos 3 tipos de operações:
superchannel – operá na potência e canais definida pelo administrador
Manual Tx Power – o administrador terá apenas a possibilidade de alterar a potência e os canais serão controlados pela região escolhida.
Regulatory domain - Tanto a potência como os canais serão disponibilizados conforme o permitido no país selecionado.

Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

9. **DFS Mode:** Dynamic Frequency Selection, ou seleção dinâmica de frequência, como o próprio nome sugere esta função buscará a frequência menos utilizada automaticamente. Esse recurso não é utilizado pelo fato de não sabermos em que canal estamos operando no momento podendo dificultar ao tentar analisar seu sinal por um canal específico.
10. **Proprietary extensions:** não utilizaremos faz referência a versão e compatibilidade do mikrotik .
11. **Default AP Tx Rate:** estabelece a velocidade máxima fornecida para esta interface.
12. **Default CLIENT Tx Rate:** a velocidade máxima fornecida para cada cliente na interface.
13. **Default Authenticate:** estabelece a autenticação padrão para os clientes se conectarem ao ap, Controle de mac, se for ativar deixar marcada
14. **Default Forward:** uma especie de block relay, para evitar os clientes se enchergarem
15. **Hide SSID:** caso marcado o nome da rede será escondida.

Aba data rates

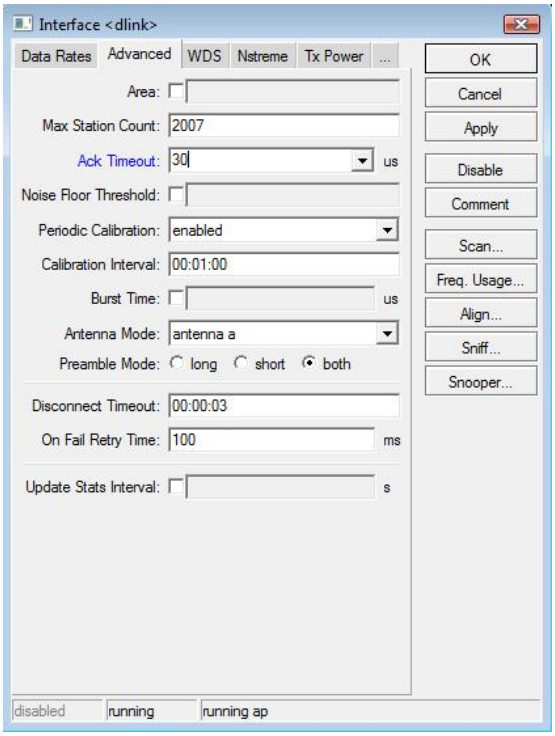
Aqui você poderá definir as taxas máximas e mínimas de transmissão padrões para cada banda, deixaremos em default pois usaremos a taxa de transmissão suportada pela banda b que é de até 11mbps**,** na pratíca 5,4Mbps Full



Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

ADVANCED

Está área define os ajustes mais avançados, como ack, tempo de calibração, ajuste de nível de ruído etc...



1 Área: não precisa colocar nada
2 Max Station Count: quantidade maxíma de clientes "teoricamente"
3 Ack Timeout: serve para otimizar o throughput de uma transmissão ao máximo, tempo de espera de um pacote, ajuda a otmizar os dados. temos as seguintes configurações:
Dynamic: ajusta automaticamente, porém se um cliente estiver ruim prejudica o resto
Indoors: para redes em ambientes fechados
Manualmente: como a tabela ao lado

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	268
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 (801.11a/b)	30	409	22	204	109	409	n/a	n/a
5212 (802.11a/b/g)	25	409	22	204	30	409	52	409

4 Noise Floor Threshold: nível de ruído em um ambiente "em dbm" valor entre : 0~127
5 periodic calibration: para assegurar a performace do chipset sob as condiçõesde temperatura
6 Calibration Interval: intervalo da verificação de calibração default= 1 minuto
7 Burst time: tempo em micro segundos de um cartão transmitir continuamente opção válido para os cartões: AR5001 AR5000. padrão: sem nada
8 Antena Mode: escolher A, usar apenas a ou apenas b se for ligar na saida auxiliar: MAIN
9 Preample mode: usar Both, pois é o modo de Pre-ambulo de irradiação
10 Disconnect Timeout: Valor ao qual o cliente é considerado desconectado**,** padrão: 3s
11 On Fail Retry Time: intervalo de tempo para repetir alguma comunicação por falha padrão 100ms
12 Update starts Interval: Atualização das estatisticas da interface. padrão: 10 s

Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

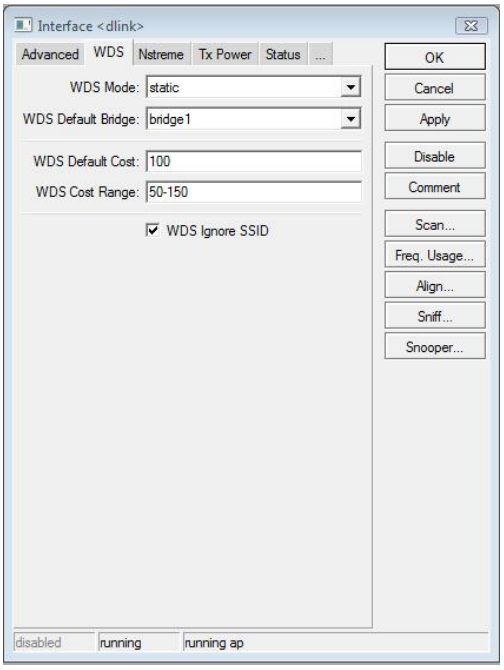
WDS

Está área define se a interface fará o wds, sistema de distribuição sem fio, esse sistema serve para repetir o sinal para outro ap, e/ou fazer um Ponto a Ponto,

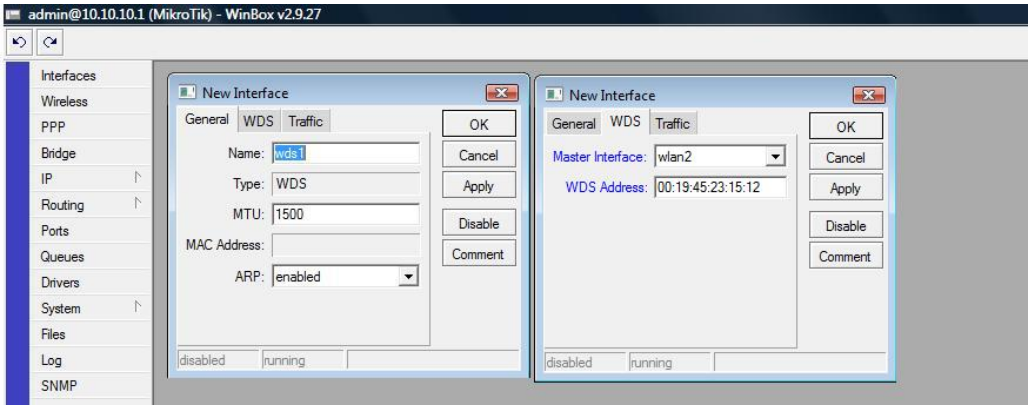
Para configurar a interface para aceitar WDS deixamos da seguinte forma:

1 WDS MODE: Static "so WDS cadastrados"
2 **WDS Default Bridge:** escolha a bridge criada
3 **WDS Igonore SSID:** deixar marcado, para ignorar o ssid e fechar o wds

Obs: em Rádios com chipset realtek deve usar no modo AP+WDS, pois apenas como WDS ele não fecha o ponto a ponto.

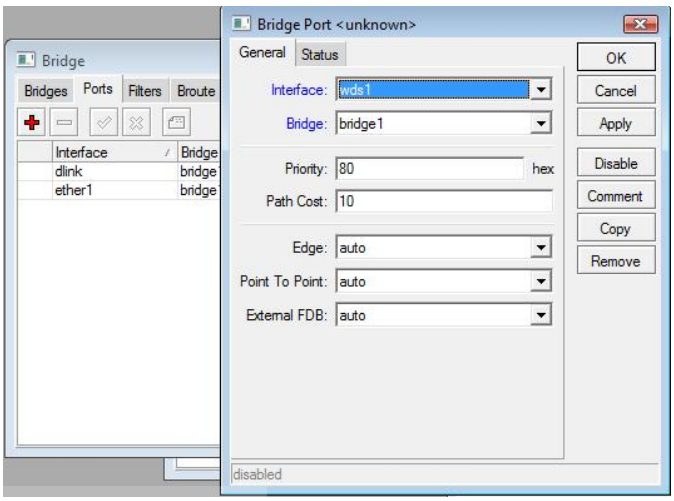


Para fazer o WDS vc deve ir em INTERFACE / +



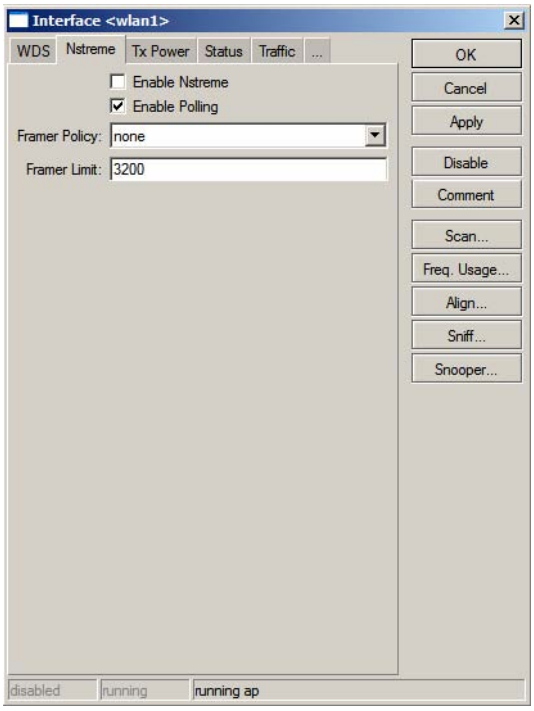
1-Name: dê um nome a essa interface WDS
2 Master Interface: a placa Wireless que fará o WDS
3 WDS Address: endereço mac do equipamento remoto

agora vamos colocar essa WDS na Bridge **BRIDGE / PORT** e adiciona a WDS
após isso você pode ver se o WDS está ativo, em INTERFACE você verifica se está com a letra R ao lado da interface.



Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

NSTREME é um protocolo prioritário da mikrotik para fazer um ponto a ponto utilizando duas placas, sendo uma para TX e outra para RX, como não iremos trabalhar com ela deixaremos apenas Enable Polling marcado esse protocolo evita colisões com nós escondidos na rede.



Aba Tx-Power

Aqui definiremos a potência das placas instaladas no nosso sistema.
Como muitos fabricantes para atender as normas locais ou para aumentar a vida útil dos seus equipamentos acabam rebaixando a potência dos mesmos, nas placas wireless que usamos sua potência é de 17dbm ou seja 50mw esse valor deve ser checado, quanto tem algumas que chega a oferece até 30 dbm, porém na prática a atheros ar5213 só chega até 23 dbm ou 200mw de potência, que para nós já é um ótimo negócio.

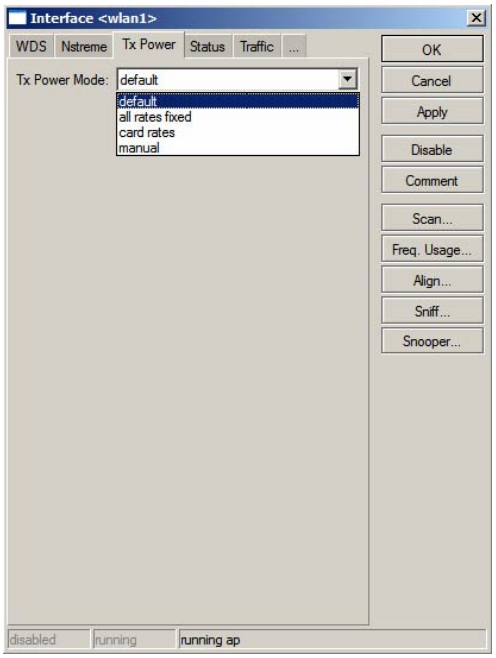


Tabela de Potências

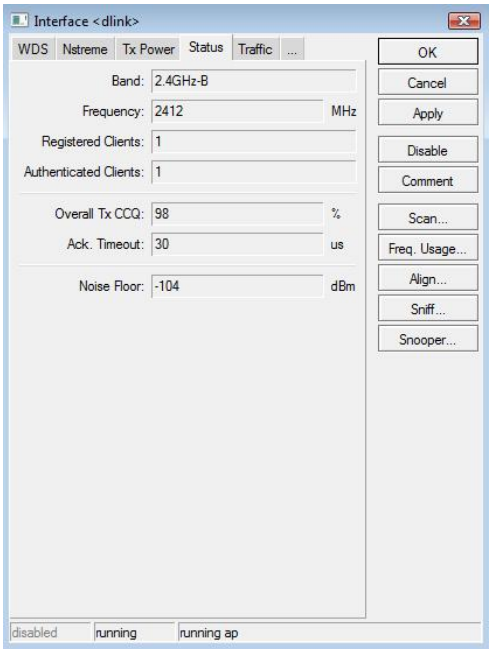
17dBm = 50mW
18dBm = 63mW
20dBm = 100mW
22dBm = 150mW
23dBm = 200mW
24dBm = 250mW
25dBm = 316mW
26dBm = 400mW

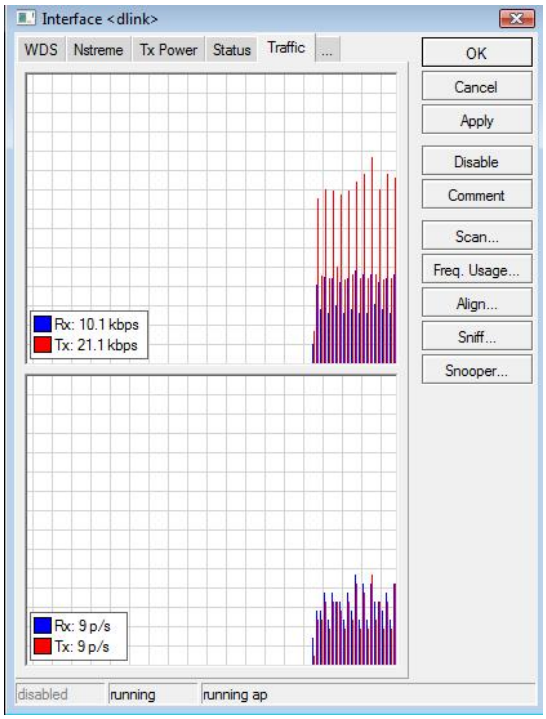
Escolha a opção **All rates fixed** e escolha a potência desejada
Lembrando que nem sempre potência demais é sinal de qualidade no link

Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

Aba Status

1. **Band:** Banda utilizada
2. **Frequency:** Freqüência utilizada "Canal"
3. **Registered Clients:** clientes registrados
4. **Authenticated Clients:** clientes conectados
5. **Overall Tx CCQ:** ou qualidade de conexão do cliente, onde mostrará o valor em porcentagem da qualidade de transmissão do link.
6. **Ack Timeout:** o tempo limite de requisição de um pacote
7. **Noise Floor:** ruído do sistema quanto mais próximo de -100 melhor ou seja não existe ruído.





Na aba Trafic mostra o trafégo da interface

Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

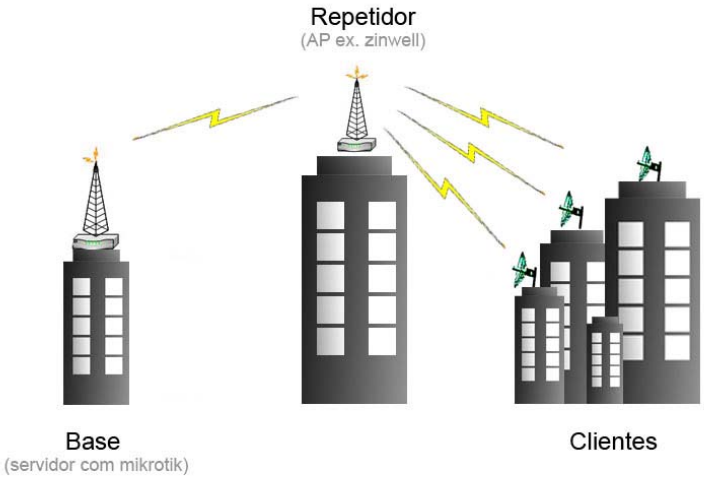
Fazendo um ponto a ponto em WDS com Rádios AP

WDS é a sigla para sistema de distribuição sem fio, consiste em desenvolver um sistema com mais de um AP repetindo e distribuindo o sinal da sua base.

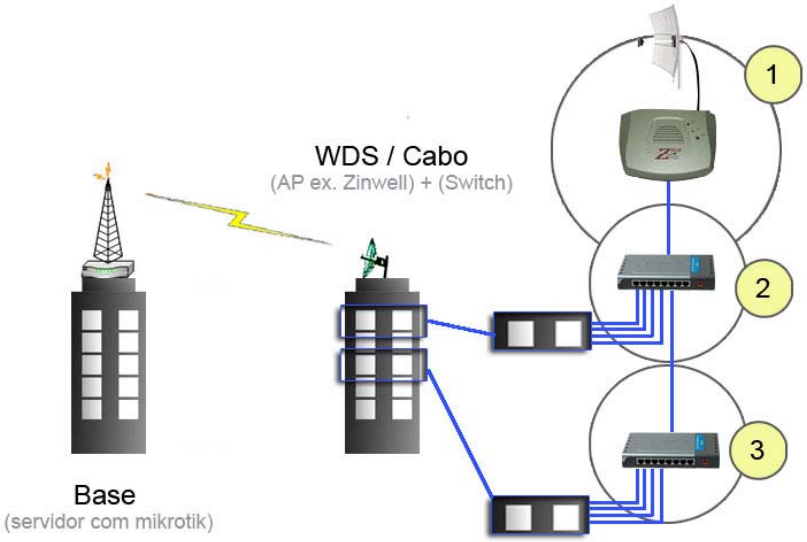
As possibilidades do WDS são muitas veja três exemplos a seguir:

1. Você quer enviar o sinal para uma área de sombra ou atrás de uma barreira, colocando um repetidor em em um ponto que seja possível captar o sinal da sua

.



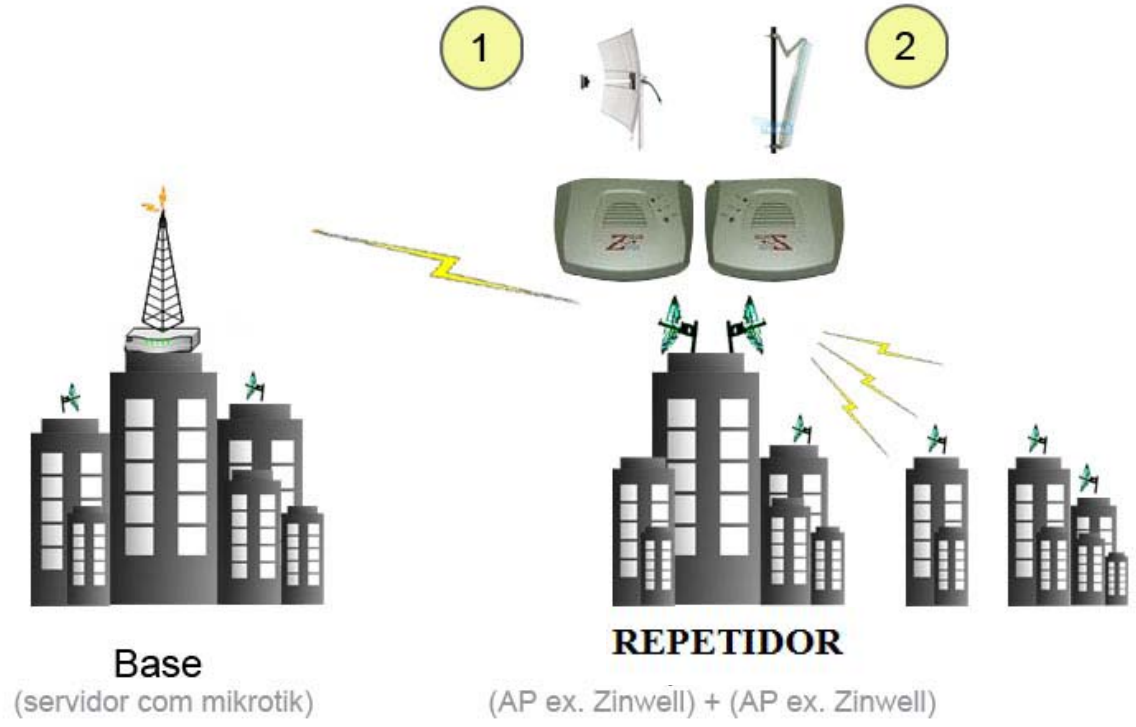
2. Em alguns casos você disponibilizará o serviço de internet para edifícios, como o sistema WI-FI não foi projetado para ultrapassar barreiras você não poderá cobrir todas as residências via wireless, então você usará um AP para receber o sinal de rádio e repassar para os usuários via cabo utilizando switch veja o modelo a seguir.



No exemplo acima a Base envia o sinal para um edifício supostamente de cinco andares e quatro apartamentos por andar então o esquema funciona desta forma:

1. Antena direcional recebe o sinal da base e repassa para o AP, no exemplo usamos um Zinwell g120.
2. O AP Zinwell repassa o link para um Switch de 8 portas e dele liga-se via cabo de rede os computadores ou outros Switchs para mais clientes.

Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

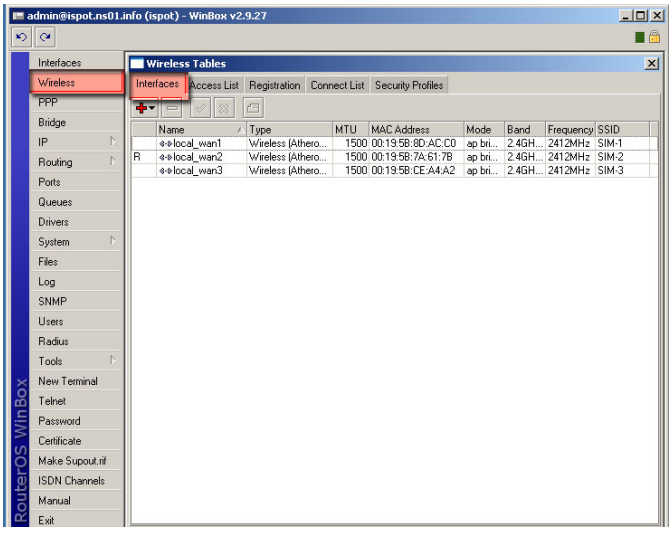


1. Um AP receberá o sinal (zinwell + direcional) e um segundo AP repassará o sinal (zinwell + setorial ou omni), você poderá usar também apenas um AP utilizando um Splitter (divisor de sinal) porém você terá perda do seu sinal.

Com este sistema você repassará os IP's da sua base (Mikrotik) para todos os clientes conectados via cabo, fazendo o gerenciamento e sabendo quem está conectado, ficando idêntico as conexões diretas.

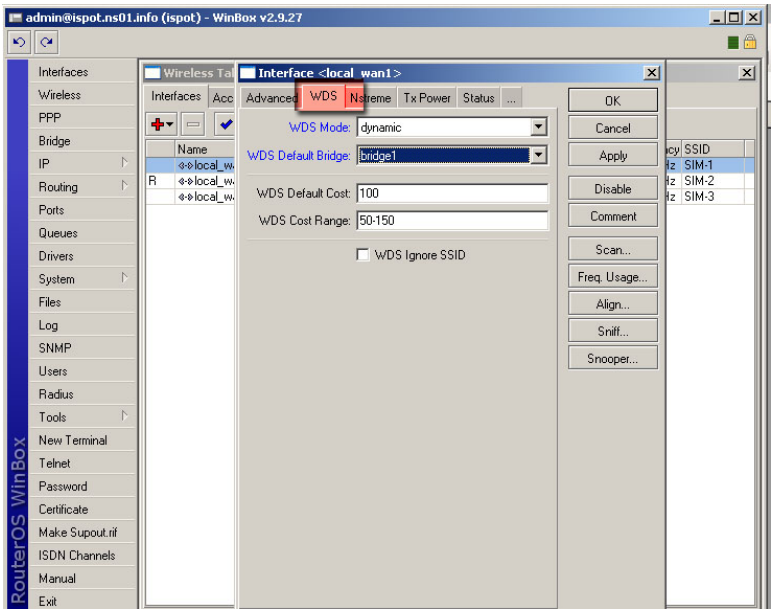
Configurando o WDS no Mikrotik e no AP

1. Acesse o menu Wireless



2. Na aba interface teremos apenas as interfaces wireless de dois cliques em qualquer interface para que possamos fazer as configurações da mesma.

Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com



3. Na interface selecionada vá para aba WDS e configure da seguinte maneira:
   1. **WDS Mode - WDS STATIC**
   pois queremos que essa comunicação seja setada evitando maiores configurações.
   2. **WDS Default Bridge** – Aqui estabeleceremos qual a interface que estará repassando o link para seu rádio, como estabelecemos uma bridge que concentra todos as interfaces então selecionaremos ela.
   3. WDS Defalt Cost – 100
   4. WDS Cost Range- 50-150
   5. WDS Ignore SSID – deixe essa opção marcada

Configurando o AP

A configuração do seu AP vai seguir o mesmo passo independente da marca ou modelo, é necessário apenas que ele tenha a função WDS.

Configurações

1. **MODO:** AP+WDS
2. **NOME:** “A sua escolha”
3. **SSID:** “A sua Escolha”
4. **canal** “o mesmo da sua interface no mikrotik”
5. **No menu WDS** marcar “Ativar WDS” e adicionar o endereço mac do Mikrotik

Feito as configurações o seu mikrotik vai exibir a interface wds do seu AP no menu interfaces.

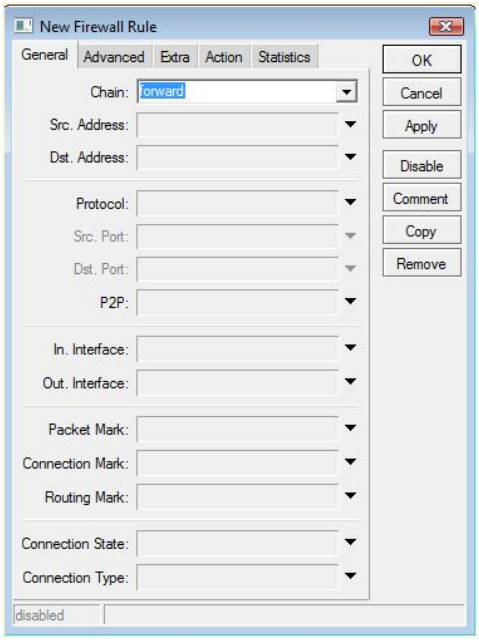
O WDS dinâmico tem a vantagem de por exemplo você criar uma rede dinâmica de repetidores, inclusive no WIKI oficial da mikrotik o autor deste procedimento refere-se a ele como rede MESH, porém se você está em um ambiente com vários provedores não é aconselhado por se tratar do mikrotik receber WDS não cadastrados.

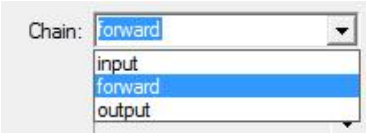
Alfamaster
Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

Firewall

O firewall do mikrotik é o coração do sistema, onde iremos fazer regras de direcionamentos, bloqueios, filtros etc..
ele é dividido em 3 partes
Filter: onde vc faz os filtros bloqueios ou relata uma ação
Nat: onde vc faz redirecionamentos
Mangle: onde vc faz marcações QOS e redirecionamentos

Vamos começar pelo FILTER, e entender cada menu
iremos fazer um bloqueio para um cliente, da porta 80

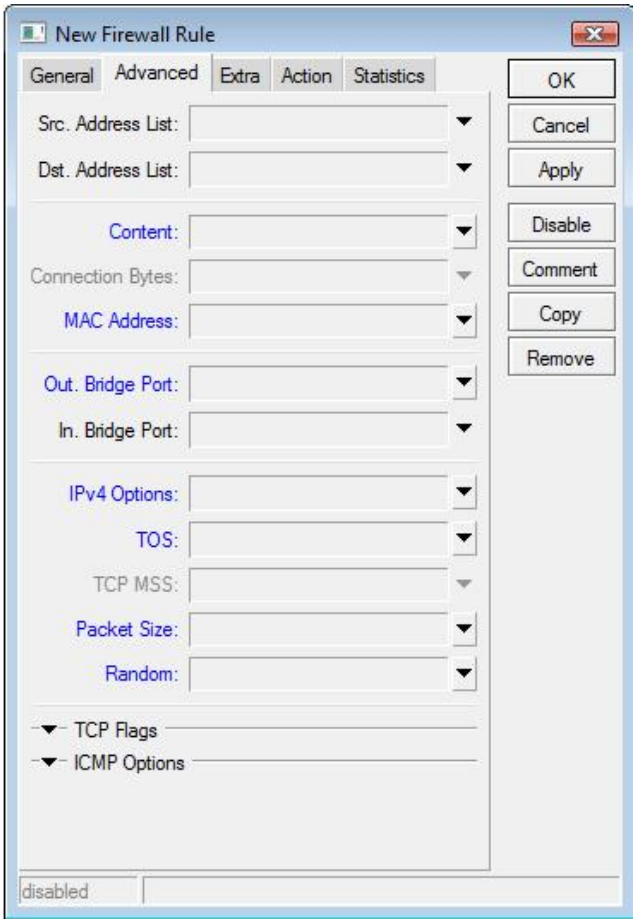


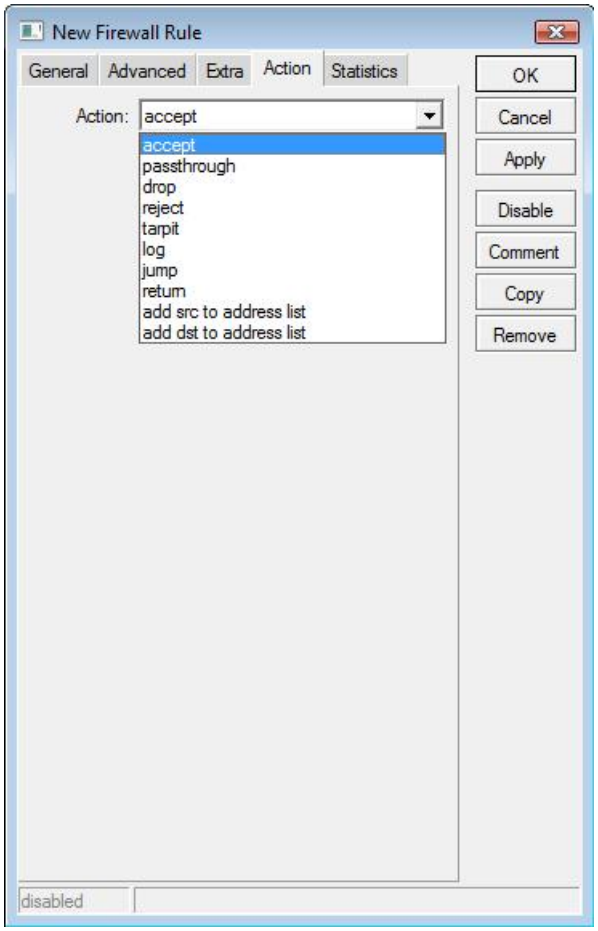


→ **Input** : responsável pelo tráfego que vai **PARA** o router
→ **Forward** : responsável pelo tráfego que **PASSA** pelo router
→ **Output** : responsável pelo tráfego que **SAI** do router

Src.Address: IP de Origem ex: um ip da rede interna que vamos fazer a regra
Dst.Address: ip de destino, ou em branco para todos
Protocolo: Tcp, Udp, Icmp se deixar em branco será todos os protocolos
Src.Port: Porta de Origem
Dst.Port: Porta de Destino
P2P: é a junção de todas as portas utilizadas pelos programas p2p
In.Interface: Interface de entrada, serve para aplicarmos so para essa interface a regra
Out.Interface: Interface de saída, serve para aplicarmos so para essa interface a regra
Packet Mark: Pacote marcado em mangle
Connection Mark: Coneção marcada em Mangle
Routing Mark: Rota marcada em Mangle
Connection state: serve para informar se a conexão está:**related:** relatada **new:** nova
invalid: invalida **estabilished:** estabelecida
Connection Type: serve para informar o tipo seja: ftp, tftp, etc..

Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com





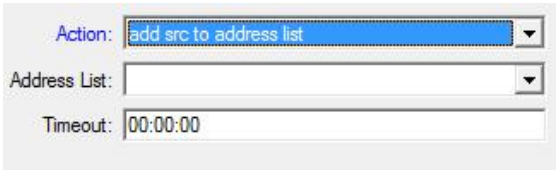
Aba Advanced

Src.Address List: Ip de origem, porém é uma lista criada em IP / FIREWALL / Address List
Dst.Address List: Ip de destino, porém é uma lista criada em IP / FIREWALL / Address List
Content: um nome em especifico no pacote "usado geralmente para cache full: X-HIT"
MAC Address: para usar um mac na regra
TCP FLAGS é onde pode se fazer regras com ack,fin,syc etc..
ICMP Oprtions: onde se faz os cortes do que é permitido no ICMP: ping, tracert etc..

Aba Action

Accept: aceita o pacote
Passthrough: ignora a regra (mas contabiliza)e passa para a regra seguinte
Drop: Rejeita o pacote
Reject: Rejeita e responde com um erro ICMP ver tabela:
Tapit: captura e segura conexões TCP, respondendo com SYN/ACK ao pacote TCP/SYN entrante
Log: serve para logar tudo nessa regra
Jump: serve para pular regras, quase não é mais utilizado
Return: retorna para uma regra acima
Add Src.to address list: Adiciona origem a Address List
Add Dst.to addrress list: Adiciona o destino a Address List

Address list: nome da regra
timeout: tempo que vai ficar catalogado



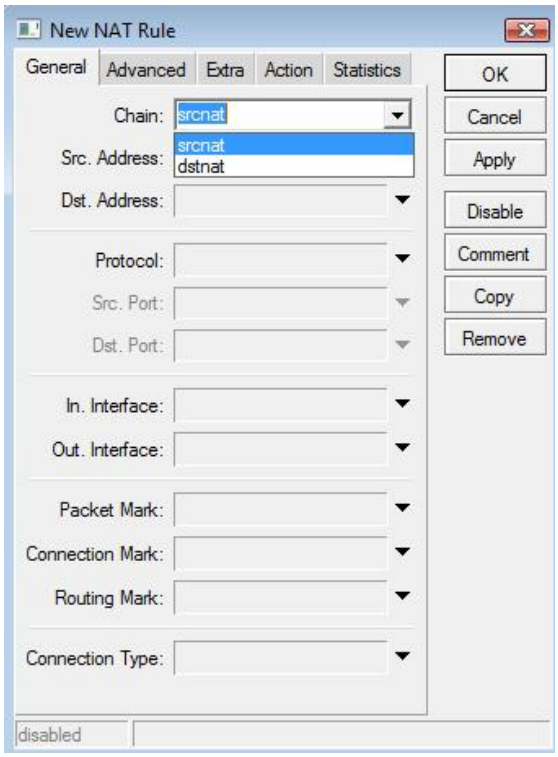
O interessante de adicionar a address list, pois pode ser feito regras de bloqueios para pessoas mal intencionadas, como acesso ssh ao servidor etc..

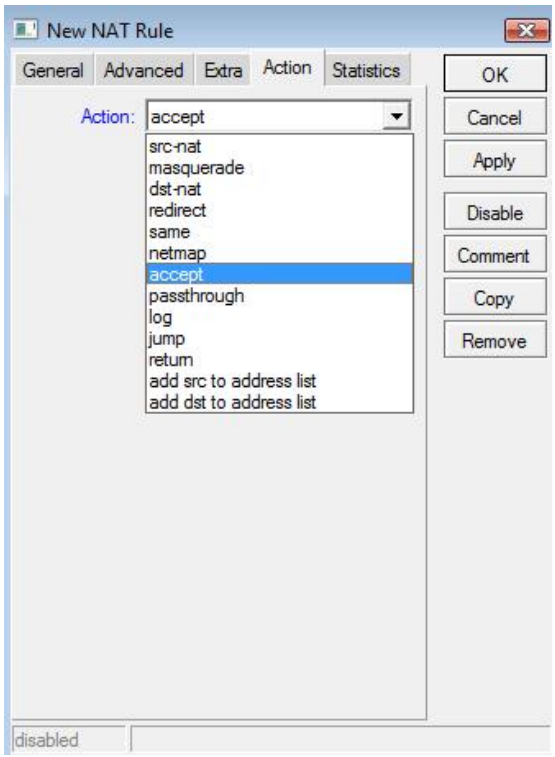
Alfamaster

Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

FIREWALL NAT

O firewall NAT tem quase todas as funções que citamos no Filter porém as ações são diferentes:





Chain SRCNAT: Determina a origem
Chain DSTNAT: Determina o destino

Action
Src-Nat: serve para redirecionar de uma origem
Masquarede: serve para fazer uma nat, mascarar
Dst-Nat: serve para redirecionar para um destino
Netmap: serve para fazer um repasse de conexão **"ex: ip válido"**
Redirect: redireciona para determinada porta "porta essa no servidor"
Passthrough: ignora a regra (mas contabiliza)e passa para a regra seguinte
Log: Faz o log da regra
Jump: serve para pular regras, quase não é mais utilizado
Return: Retorna a regra "não mais utilizado"
Add Src to Address list: Adiciona a Origem em Address List
Add Dst to Address list: Adiciona a Destino em Address List

Exemplo: fazer um redirecionamento de VNC para o cliente 10.10.10.40, sabendo que a porta do VNC é a 5900 e que a interface de entrada será LINK

/ ip firewall nat add chain=dstnat in-interface=LINK protocol=tcp dst-port=5900 action=dst-nat to-addresses=10.10.10.40 to-ports=5900 comment="" disabled=no

Fazer um nat da Interface LINK para a os clientes, ip dos clientes: 10.10.10.0/24

/ ip firewall nat add chain=srcnat out-interface=LINK src-address=10.10.10.0/24 action=masquerade comment="" disabled=no

Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

Fazer um redirecionamento da Porta 80 para a porta do web-proxy na porta 3128, ip dos clientes: 10.10.10.0/24

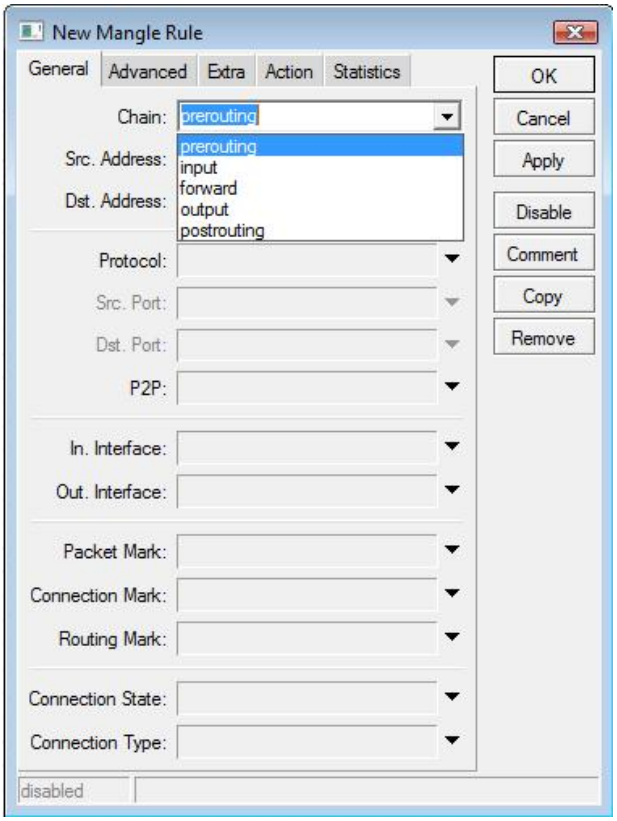
/ ip firewall nat add chain=dstnat src-address=10.10.10.0/24 protocol=tcp dst-port=80 action=redirect to-ports=3128 disabled=no

Fazer um redirecionamento para acessar um rádio de ip 10.10.10.254 "porta 80" utilizando a porta 4040 da rede externa.

/ ip firewall nat add chain=dstnat in-interface=LINK protocol=tcp dst-port=4040 action=dst-nat to-addresses=10.10.10.254 to-ports=80 disabled=no

Mangle

Mangle é a função mais importante do Firewall na minha opinião, nela você poderá marcar pacotes, fazer rotas distintas, fazer marcações em conjunto com o FILTER RULES para bloqueio de invasor etc, e é utilizado para fazer a marcação para LOAD BALANCE.
não é diferente do Filter e Nat, porém as actions são diferentes também.

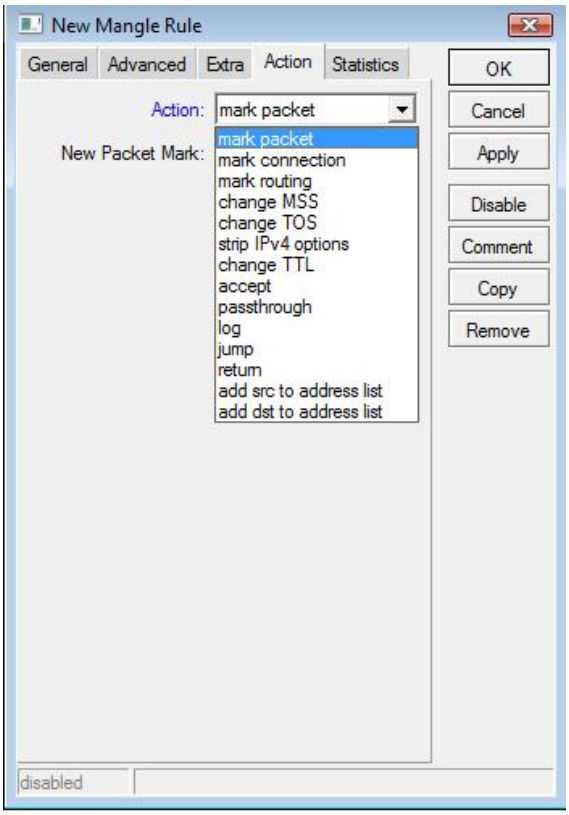


Chain

1 Prerouting: marca antes da fila global-in "o mais utilizado por está no começo das regras"
2 Postrouting: marca antes da fila global-out
3 Input: marca antes do filtro de input
4 Output: marca antes do filtro de output
5 Forward: marca antes do filtro Forward

Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

actions



Action
Mark Packet: serve para marcar todos os Pacote
Mark Connection: serve para marcar o primeiro pacote "cataloga em Connections"
Mark Routing: serve para Marcar uma rota "ex: load balance"
Change MSS: serve para mudar o tamanho de um segmento TCP, Padrão:1360
Change TTL: serve para ocultar a rota de um tracert
Add Src to Address list: Adiciona a Origem em Address List
Add Dst to Address list: Adiciona a Destino em Address List

Fazer a marcação da coneção e de pacotes da porta tcp 443 "HTTPS"

/ ip firewall mangle add chain=prerouting protocol=tcp dst-port=443 action=mark-connection new-connection-mark=443 passthrough=yes comment="HTTPS" disabled=no

agora marcar o pacote:
/ ip firewall mangle add chain=prerouting connection-mark=443 action=mark-packet new-packet-mark=https passthrough=yes comment="" disabled=no

com isso podemos agora fazer um QOS, priorizando uma quantidade de banda para esse pacote para isso é bom fazer para todas as portas mais utilizadas como:
1863 MSN, 443 Https, 23 FTP, 80 HTTP, 25 SMTP, 110 POP3, 5060 Voip, 53 DNS, etc...
o valor de banda disponivel para essas marcações é feita em Queue Tree, lembre-se de quando colocar em em queue tree colocar o limite para não ficar aberto a banda.

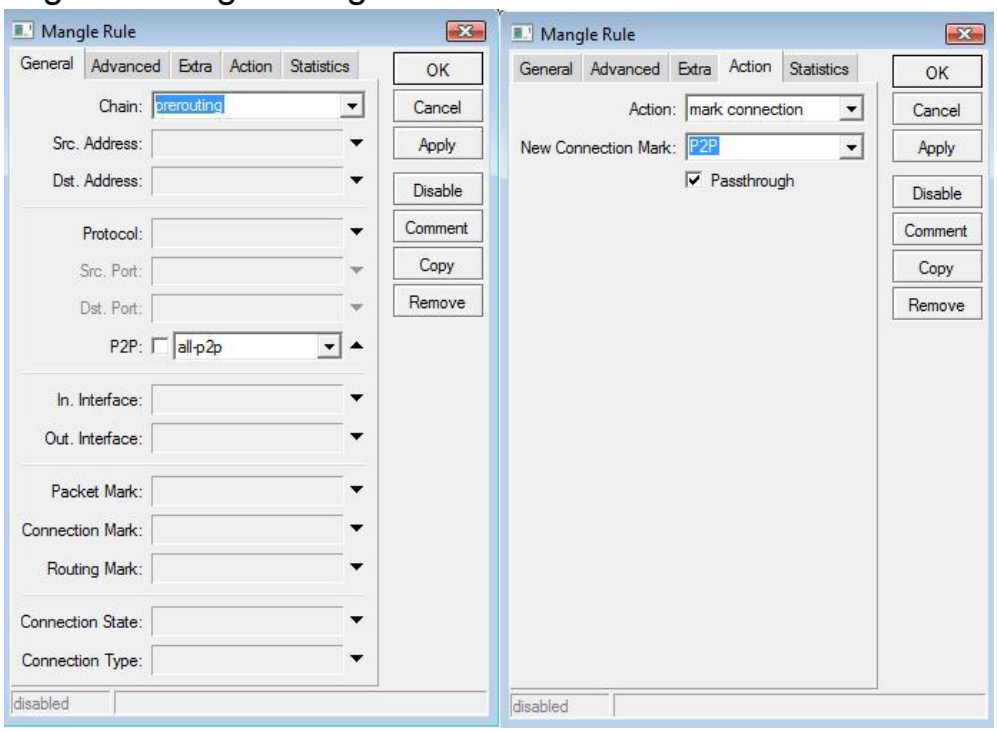
Criar um controle para P2P e limitar

vamos primeiramente marcar a conexão

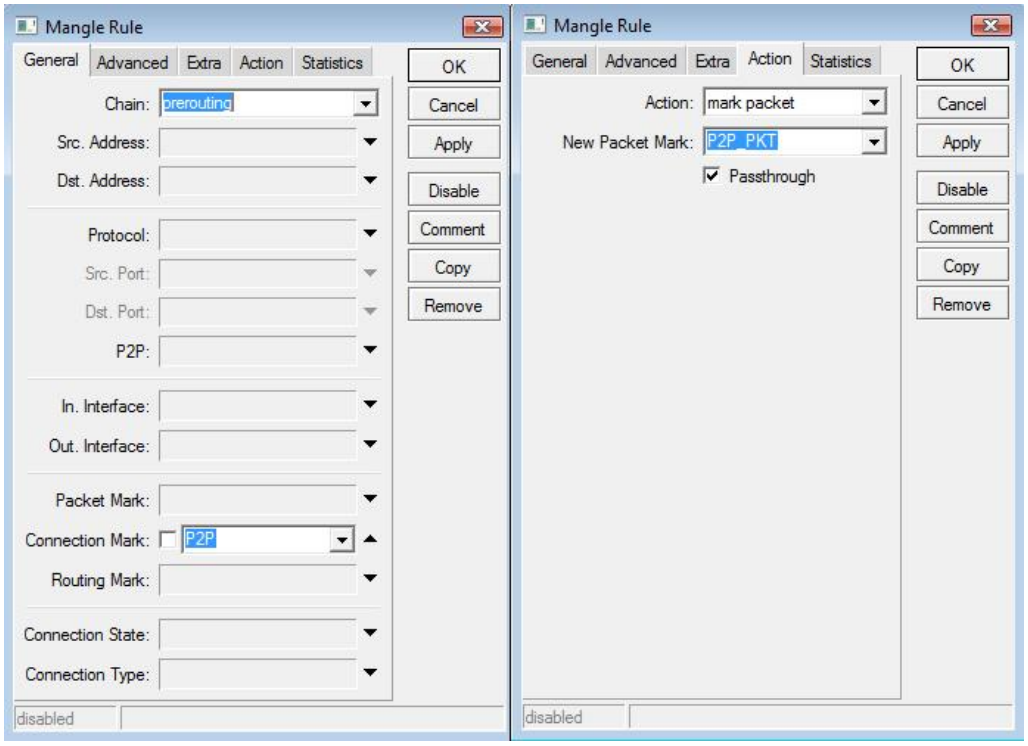
/ ip firewall mangle add chain=prerouting p2p=all-p2p action=mark-connection new-connection-mark=P2P passthrough=yes comment="P2P" disabled=no

Agora iremos marcar o pacote:
/ ip firewall mangle add chain=prerouting connection-mark=P2P action=mark-packet new-packet-mark=P2P_PKT passthrough=yes comment="" disabled=no

A primeira regra ficará igual a figura abaixo:



E a segunda regra ficará assim:



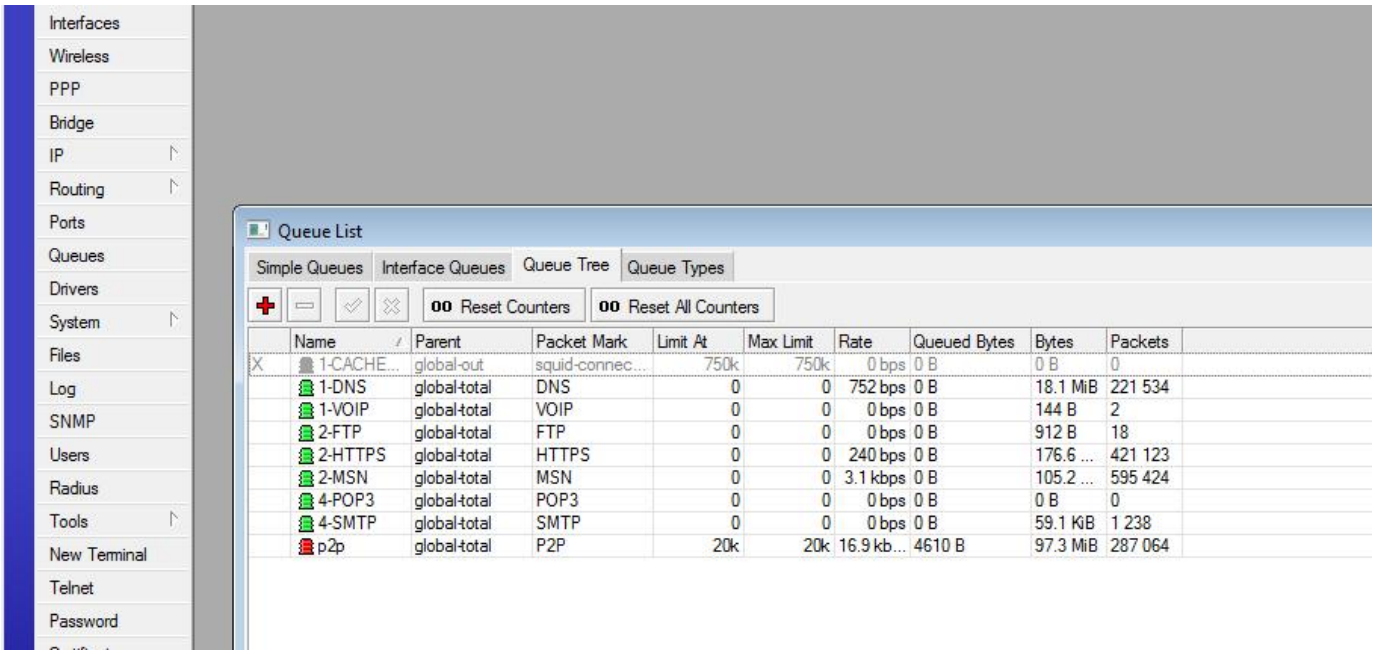
O ideal é marcar todas as conexões do menu P2P: fasttrack (kazaa),gnutella,edokkey etc...
após feito isso vamos em queue tree para prender a velocidade a qual esses pacotes irão trafégar.

Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

QUEUE Controle de Banda

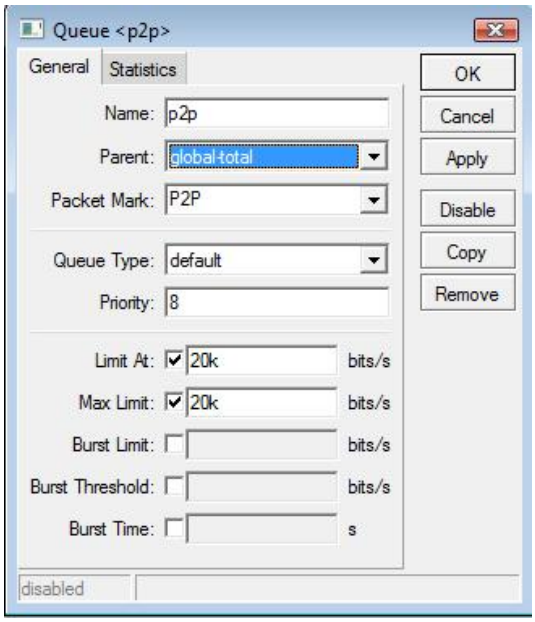
O queue fará o controle da banda que será disponibilizado para os serviços marcados em mangle sendo feito em QUEUE TREE, e para um controle de banda para um IP em QUEUE SIMPLE.
Vamos configurar um controle de banda para a regra de P2P que criamos, vamos então em:

/ QUEUE / QUEUE TREE



Clica-se no + e vamos criar o controle para o pacote P2P_PKT

Name: Nome da regra
Parent:qual fila? entrada ou saida?
global in: controle de entrada
global out: controlde de saida
global total: controle entrada e saida juntos
Packet Mark: qual pacote vai ser feito a regra
Queue Type: deixar em default
priority:número de prioridade de 1 até 9
Limit At: limitado até
Max.Limit: maximo permitido
Burst Limit: velocidade de inicio
Burst threshold: velocidade intermediaria
Bust Time: tempo da velocidade de inicio

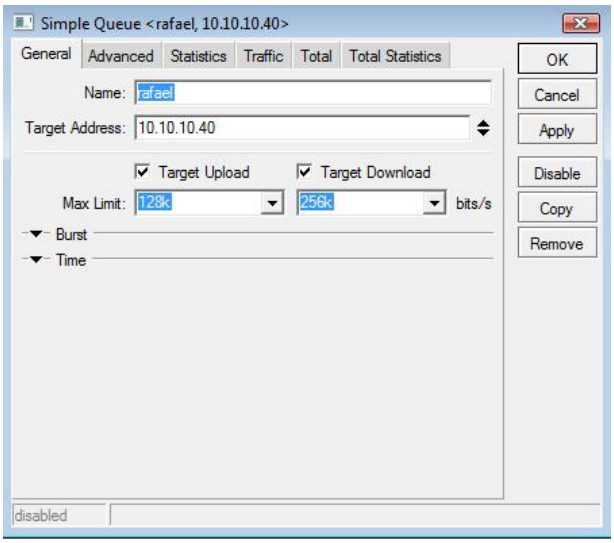


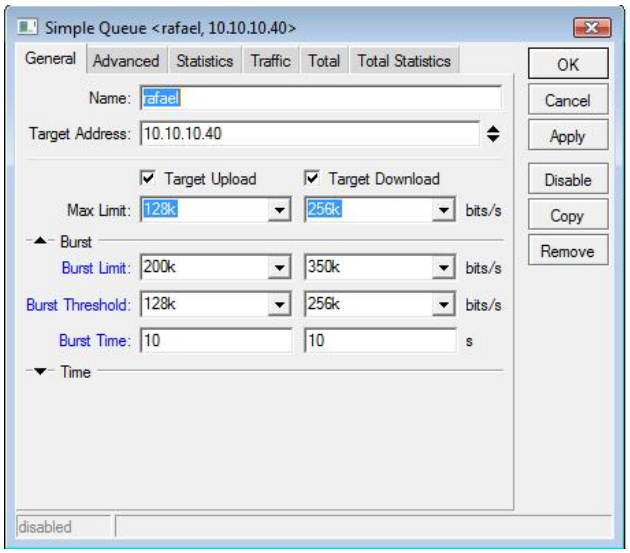
Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

Queue Simple

É onde iremos prender a velocidade dos clientes utilizando o Ip, prendemos a velocidade de upload "envio de dados" e de Download "recebimento de dados", normalmente o Upload é mais baixo do que o download, geralmente utiliza-se metade de download para upload, lembrando não colocar abaixo de 64K para upload afim de não ter problema com clientes, que postam fotos em orkut ou que mandam anexos em e-mails.

vamos prender a velocidade do ip 10.10.10.40 do cliente Rafael para 128k de up e 256 de down.
caminho: **QUEUE SIMPLE / +** a figura da direita está configurada, a da esquerda tem uma diferença





Name: nome do cliente
Target Address: endereço de ip do cliente
Target Upload e target Download: devem está marcados
Max Limit upload: velocidade maxíma de upload usar k para kilobyte e m para megabyte
Max Limit download: velocidade maxíma de download
BURST: serve para dar um aumento inicial na velocidade num determinado tempo
Burst limit: até onde vc quer que ele chegue no caso 200k e 350k
Burst threshold: velocidade intermédiaria, ele vai voltar para essa velocidade.
Burst Time: tempo que a velocidade inicial ficará. nesse caso 10 segundos
TIME: esse menu não utilizaremos pois ela so fará o controle de banda nesse tempo estipulado

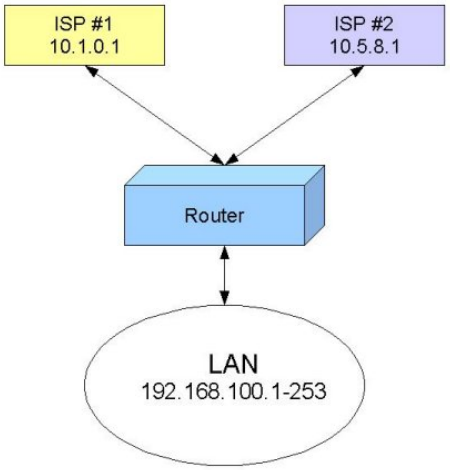
A aba Advanced não iremos utilizar, porém ela pode fazer um controle de banda para os pacotes marcados em Mangle, mas como os QOS deve ser antes do controle de banda do cliente então não iremos utilizar

Alfamaster
Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

Load Balance

(utilizando mais de um link no mesmo sistema)

Balanceamento de carga é a técnica utilizada para dividir os recursos de um sistema deforma a não sobrecarrega-lo, no caso do mikrotik podemos fazer de duas formas: Por rotas estaticas, que é o direcionamento do cliente para determinado links, definindo rotas especificas. outra forma é a soma de link, utilizando por NTH, que é a divisão dos pacotes e repassando para a LAN somada, esse segundo exige mais regras por ter que fazer rotas estaticas para bancos e alguns serviços.



O balanceamento de carga que iremos realizar consiste em colocar Dois links (ISP1 e ISP2) e definir rotas diferentes para cada LINK agrupando seus clientes por endereço IP. Você precisará de duas placas de rede disponíveis uma para cada ISP

Se você tiver certo número de clientes, você pode agrupá-los por endereços de IP. Então, dependendo do IP address da fonte, o tráfego passará para o ISP1 ou ISP2.
Essa não é a melhor forma de realizar um balanceamento, porém é fácil a sua execução e entendimento, dando-lhe a possibilidade de manter algum controle.

Partiremos do princípio que os endereços da sua rede estarão configurados nesta faixa 192.168.100.0/24 irá utilizar o ISP1 e 192.168.200.0/24 vai utilizar o ISP2

Os grupos ficaram divididos na seguinte faixa de ips.

• **Grupo A** 192.168.100.0/24 • **Grupo B** 192.168.200.0/24

• O **gateway** será 192.168.100.1 e o 192.168.200.1

o IP dos Modems serão: 10.1.0.1 e 10.5.8.1

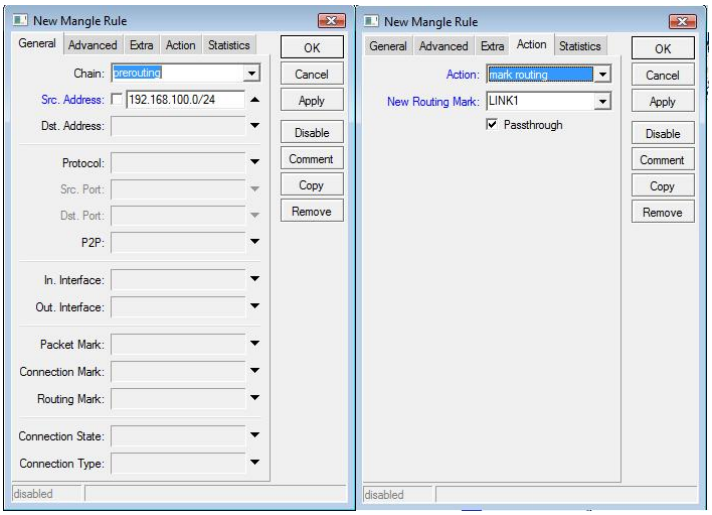
após isso irremos marcar em mangle a rota para os clientes do grupo A tenha a Rota para sair pelo

Link ISP1 e o grupo B saia pelo Link ISP2

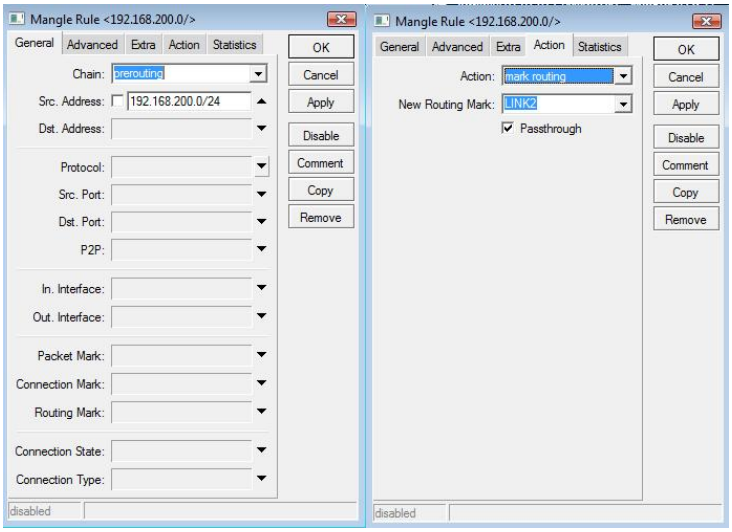
Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

Marcaremos os pacotes do grupo A

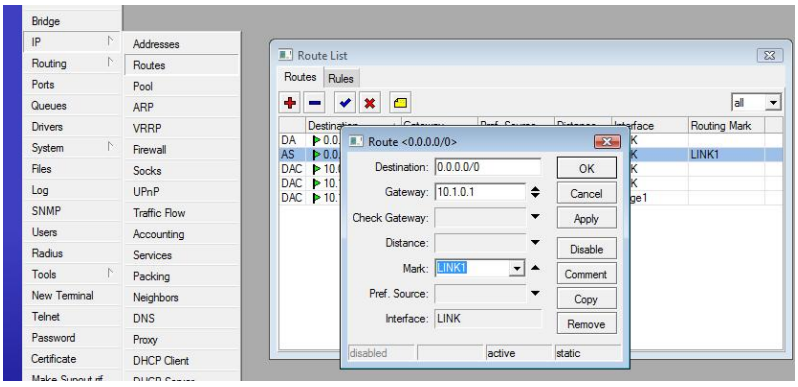
1. **Aba General** > Chain: prerouting e Src. Address: 192.168.100.0 /24
2. **Aba Action** > Action:mark routing e new routing mark: escreva **LINK1”**.

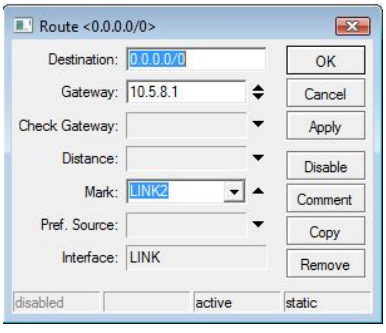


Fazemos a mesma coisa para o grupo B colocando o ip e new rotuing: LINK2



Agora iremos fazer as rotas de saida, o caminho: IP / ROUTE





Gateway: coloca o ip do modem 10.1.0.1 e em Mark: LINK1, e repete-se para o segundo link

colocanodo o ip 10.5.8.1 e Mark: LINK2, após isso fazer apenas uma regra de Nat "masquared"

para os dois links.

Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

Load Balance por NTH "soma e link"

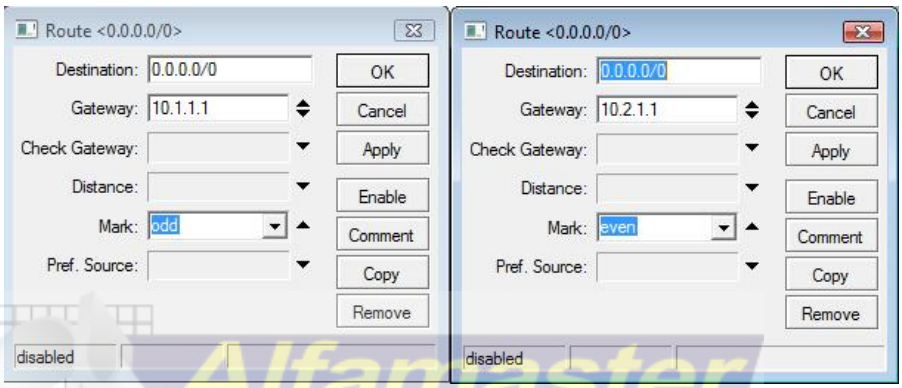
Nessa forma os links Entrantes WAN serão marcados em mangle e fazendo a soma para a interface LAN, recomendado usar uma maquina para fazer esse serviço, utilizar outra maquina para ser o firewall, pois senão não terá algumas regras de QOS funcional. load balance tem que ser feito em uma maquina dedicada, por esse sistema da o nome Roteador de Borda.
Primeiramente iremos ter ips distintos na WAN, no caso se for usar ADSL, cada modem tem que estar em faixas de ip diferente, e no modem ativar o DMZ para o ip que iremos usar no Mikrotik, o DMZ é o para deixar esse host com acesso irrestrito, no caso as portas são todas redirecionadas.
Iremos usar os ips nos modens: 10.1.1.1 e 10.2.1.1, iremos usar uma placa de rede apenas WAN e iremos utilizar um Switch de 8 portas na wan, para ligar os links nele.
1 Passo: colocar os ips na interface WAN: 10.1.1.2/24 e 10.2.1.2/24

Fazer um teste pingando para o Ip dos modens.
esse exemplo temos cada link sendo de 1 mega, para somar e termos 2 Megas
Após isso faremos as marcações em mangle

/ ip firewall mangle add chain=prerouting in-interface=bridge1 connection-state=new nth=1,1,0 action=mark-connection new-connection-mark=pacote_1 passthrough=yes disabled=no
/ip firewall mangle add chain=prerouting in-interface=bridge1 connection-mark=pacote_1 action=mark-routing new-routing-mark=odd passthrough=no disabled=no

/ip firewall mangle add chain=prerouting in-interface=bridge1 connection-state=new nth=1,1,1 action=mark-connection new-connection-mark=pacote_2 passthrough=yes disabled=no
/ip firewall mangle add chain=prerouting in-interface=bridge1 connection-mark=pacote_2 action=mark-routing new-routing-mark=even passthrough=no disabled=no

dessa forma iremos dividir TUDO em dois pacotes, sendo um para um link e outro para o outro, caso vc tenha um link de 1 mega e outro de 2 megas, terá que fazer 3 marcações para ficar:
1mega + 1 mega + 1 mega : 3 Megas, para o link que tem dois megas vc fará duas regras de marcação e para o de um mega apenas um.
agora iremos Adicionar as rotas em: **IP / ROUTE**



Alfamaster

Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

NAT DO LOAD

Após ser adicionado as rotas dos pacotes agora vamos fazer o nat:

/ ip firewall nat add chain=srcnat connection-mark=odd action=src-nat to-addresses=10.0.0.2 to-ports=0-65535 comment="Balanceamento de carga" disabled=no

/ ip firewall nat add chain=srcnat connection-mark=even action=src-nat to-addresses=10.2.2.2 to-ports=0-65535 comment="" disabled=no

após isso o mikrotik já estara somando, lembrar que se for preciso de que determinado serviço, ou site de bancos não passe pelo load balance passe direto vc tem que marcar o site ou a porta para redirecionar para um link desses, também é interessante colocar um gateway padrão para o mikrotik não depender apenas do load.

o calculo de NTH será da seguinte forma:

2 pacotes "2 links"--> 1.1.0 1.1.1

3 pacotes "3 links"--> 2.2.0 2.2.1 2.2.2

4 pacotes "4 links"--> 3.3.0 3.3.1 3.3.2 3.3.3

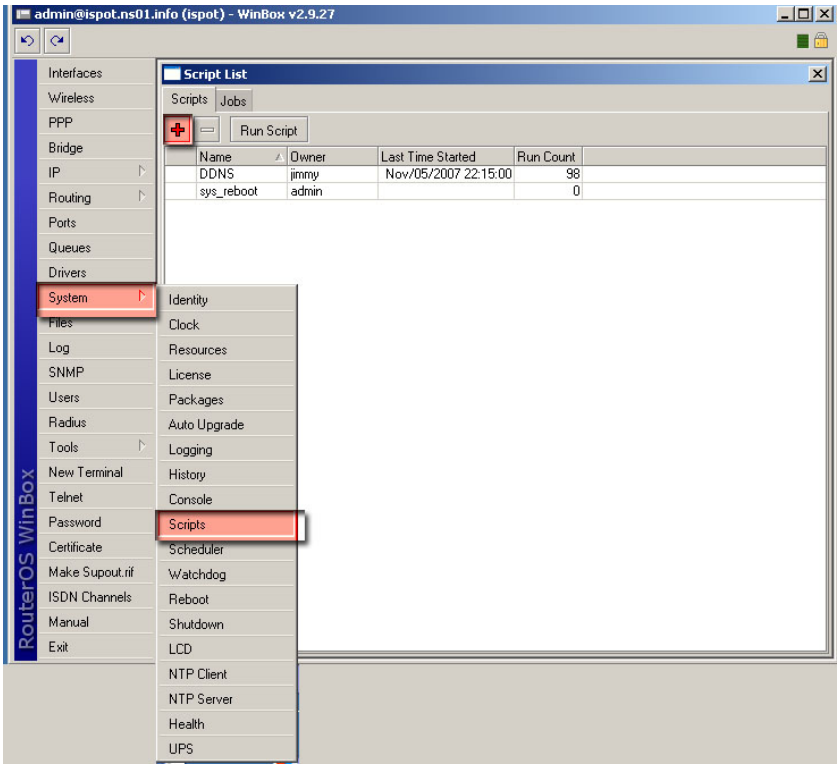
5 pacotes "5 links"--> 4.4.0 4.4.1 4.4.2 4.4.3 4.4.4

Acessando Remotamente VIA REDE EXTERNA

O mikrotik poderá ser acessado de qualquer lugar do mundo, para isso você só precisará se cadastrar em um servidor ddns no site https://www.changeip.com/ caso você não tenha um ip real, ou se caso tenha queira acessar via HOST "nome".

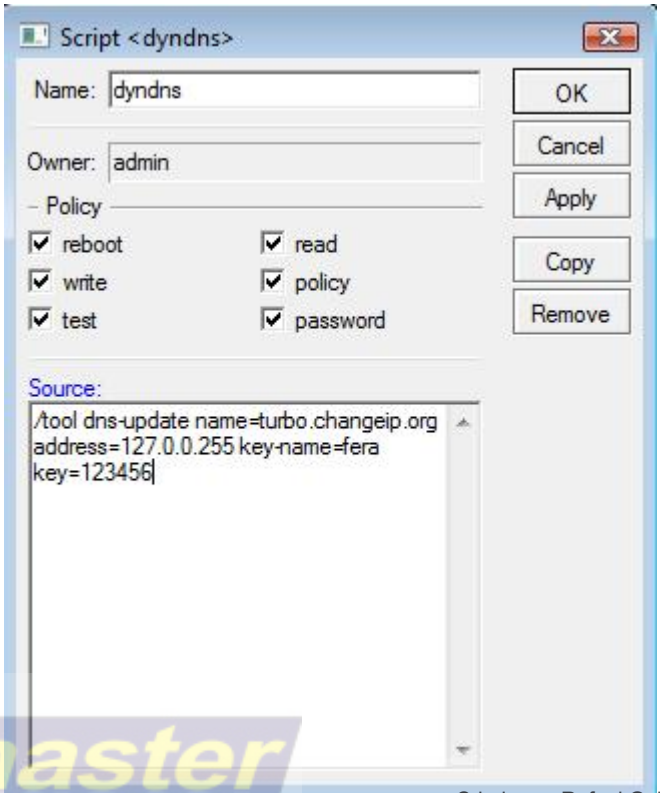
Após realizar o cadastro iremos configurar um script para que o mikrotik atualize o ip atual no servidor ddns.

Acesse o menu **system** submenu **script**



Na aba scripts clique no sinal “+”na

tela do script:



1. Name – nome do script

2. Policy - marque todos os campos de

policy como na figura

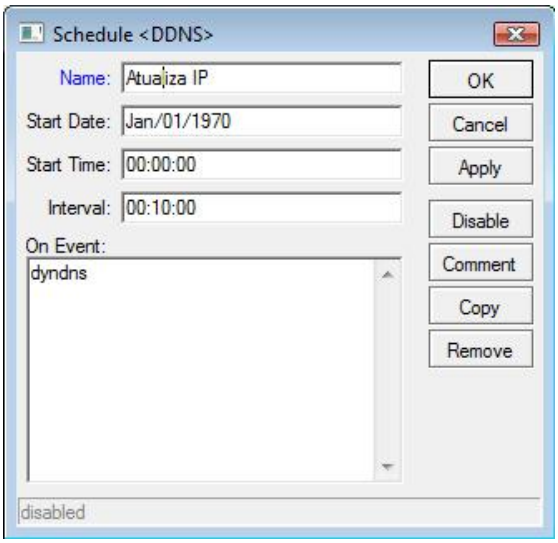
Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com

A regra seria a seguinte:

/tool dns-update name=turbo.changeip.org address=127.0.0.255
key-name=turbo key=123456

Onde: Turbo.changeip.org é o nome que vc criou no cadastro de sua conta no site
Turbo: é o nome de usuario para logar no site
123456: é a senha de acesso ao site.

Após isso para testar vc pode ir no botão Run Script, mas para a regra ficar sendo executada de tempos e tempos vamos precisar fazer o agendamento desse script, para isso iremos em: **SYSTEM / SCHUDLER**



Onde
Name: nome da regra
Start Date: data que irá começar
Start Time: Hora que irá começar
Interval: intervalo de tempo da regra
On Event: Qual evento irá ser executado

Criada por Rafael Galdino
sup.rafaelgaldino@gmail.com