Provedor Completo com Mikrotik
Tudo o que você precisa

Túlio Ernandez Cabral

Índice

Apresentação

Olá tudo bom? Gostaria de me apresentar antes de começarmos a falar deste livro. Meu nome é Túlio, sou o autor desta obra, quando que na verdade essa obra foi construída por muitos, por pessoas anônimas ou declaradas mais com um único objetivo. Compartilhar a informação de forma gratuita e aprender com outros.

No inicio de 2005 eu montei meu primeiro sistema wireless através de um ap d-link, compartilhando uma conexão adsl para 3 computadores, era um sistema para uso particular.

O fascínio foi instantâneo, surgindo a ideia de montar um provedor wireless, então comecei a pesquisar equipamentos profissionais e que pode-se me propor um maior controle sobre a administração de tráfego e usuários.

Comprei um zinwell g120 e junto veio a frustração. Um equipamento que os vendedores vendiam dizendo que fazia divisão de banda QoS enfim, o que parecia um bom negócio erá um improviso e muito complicado, eu queria algo mais completo, que houve-se como eu ter acesso a gráficos de tráfego, bloqueio fácil de clientes e gerenciamento mais completo.

O mikrotik era um sistema ainda fora dos holofotes, poucos sabiam como configura-lo e as informações disponíveis estavam em outra língua, os Wikis engatinhavam os fóruns estavam com mais “?” que “!” , era um ambiente hostil e inexplorado porém promissor.

Comecei a estudar o sistema, tentando e errando, comecei instalando o mikrotik em um servidor virtual, as evoluções foram poucas, depois adquiri um pc velho para usá-lo exclusivamente para teste, foi então que comecei a evoluir.

Em meados de 2006 eu já estava usando o mikrotik como ap em minha própria residência conectando 3 computadores e compartilhando uma conexão adsl de 300kbps.

O meu sistema ainda engatinhava, estava vazio e faltava muito para conseguir um sistema ideal, porém já poderia entrar no mercado com um bom gerenciamento de banda e controle sofre o fluxo de tráfego.

Ainda em 2006 convidei um amigo para entrar em uma sociedade era uma oportunidade de dividir os custos do investimento inicial e poderia aplicar meus conhecimentos em campo, iniciei com uma antena e um rádio montado sobre uma caixa hermética em uma torre de 3 mts, o sistema era estável e me surpreendia com ele a cada dia. A empresa foi crescendo e adquirindo novos clientes apenas com o boca a boca.

Em junho de 2007 já tinha um sistema com dois links adsl, 3 antenas setoriais 3 rádios e uma torre de 16 metros de altura com aproximadamente 80 clientes, a empresa prosperava e a demanda aumentava a cada dia.

Porém como estava em uma sociedade vieram problemas que ocorriam desde a fundação da empresa que posteriormente seria também o motivo do falecimento de um da mesma.

A sociedade foi desfeita, os equipamentos vendidos, os clientes ressarcidos e o desgosto pelo empreendedorismo foi o desfecho deste episódio em minha vida.

Porém a paixão pelo sistema continuava, comecei a prestar consultoria para pessoas queriam aprender como utilizar o mikrotik, como montar, enfim pensei em escrever um e-book com cara de manual porém não passava de um relato vivenciado de toda um aprendizado sobre internet sem fio utilizando o sistema Mikrotik.

Aproveitando melhor o livro

Este livro é destinado à profissionais da área de tecnologia da informação, administradores de rede, empresários, para pessoas que pensam em montar seu próprio ISP e para leigos que não sabem nada ;).

Escrito em uma linguagem de fácil assimilação, o livro apresenta uma didática própria, descaracterizando o cunho exclusivamente técnico e evidenciando antes de tudo a vivência do autor com a tecnologia aqui explorada.

Dividido em 3 partes que poderíamos denominar de antes durante e depois do mikrotik, para aqueles que já dominam a tecnologia wireless e querem apenas evoluir para o mikrotik podem ir direto ao item 10 do índice que fala sobre o mikrotik.

Se você não tem familiaridade com o sistema Mikrotik , aconselho que faça a configuração até o item 10.12, que resume-se a instalação do sistema para funcionar em hotspot.

Você estará controlando banda, inserindo e removendo clientes. Estará pronto para prover internet usando o mikrotik, porém recomendo que passe um período se adaptando e conhecendo mais as configurações que você fez ate o item 10.12, para depois começar a inserir regras, scripts, marcações de pacotes, rotas etc e finalizar as configurações adicionais.

Em todo instante estarei dando exemplos práticos e comentando as configurações descritas.

O livro é repleto de figuras totalizando mais de 120 imagens que ajudaram na configuração de todo o sistema assim como o seu entendimento.

Na pasta arquivos suporte você encontrará duas apostilas de autores diferentes que ajudarão no seu aprendizado, os arquivos são:

1. montando caixa hermética – aqui o autor descreve detalhadamente como montar o mikrotik em uma caixa hermética baseado em um PC comum.
2. mikrotik_detalhado – Uma apostila detalhada sobre o sistema, o autor é bastante minucioso
3. manual oficial – é o manual completo disponibilizado pela mikrotik

Sistema Wireless

Um sistema wireless ao pé da letra um sistema sem fio, em inglês sua tradução vem do wire (cabo, fio) + less (livre), ou seja é um sistema que funciona através de outros meios que dispense a utilização de cabos, seja 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 como por exemplo um controle remoto ou uma transmissão de longa distância como exemplo as informações que são enviadas por satélites.
A tecnologia wireless é utilizada comumente nos equipamentos de telecomunicações, como celulares, telefones sem fio, walktalk e gps.

Wireless network

Atualmente os sistemas de rede sem fio tem se tornado um grande atrativo devido ao baixo custo de viabilização e à praticidade no instante em que um usuário final não precisará se incomodar com cabos, *hubs*, 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 proprietária da empresa Wi-Fi Alliance que designou o padrão IEEE 802.11, dentro deste padrão trabalha dentro da frequência de 2.,4 e 5 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.

Detalhes dos padrões b/g retirados retirados do site wikpédia

802.11b

Alcança uma velocidade de 11 Mbps padronizada pelo IEEE e uma velocidade de 22 Mbps, oferecida por alguns fabricantes não padronizados. Opera na freqüência de 2.4 GHz. 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 802.11b e oferece uma velocidade de 54 Mbps. Funciona dentro da frequência de 2,4 GHz. Tem os mesmos inconvenientes do padrão 802.11b (incompatibilidades com dispositivos de diferentes fabricantes). As vantagens também são as velocidades). Usa autenticação WEP estática. 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 um tópico de interesse a muitas pessoas que pensam em instalar uma rede sem fio.
Os motivos para estes interesses são muitos, pois como uma rede sem fio está disponível a um numero de pessoas indefinidas, pois o sinal de rádio muitas vezes podem ser captadas por usuários indesejados dos quais alguns podem ser invasores e fazer um bom estrago em sua rede.
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.

O que preciso para ter um provedor de internet a radio

A tecnologia atual propiciou a popularização dos serviços antes restrito à grandes empresas, a 8 anos atrás um provedor de acesso a internet requeria um grande investimento em infra-estrutura tornando-se um serviço exclusivo que na maioria das vezes as teles dominavam.

Hoje o sol nasce para todos, para você prover internet não precisa grandes equipamentos mainframe ou coisa do gênero, basta apenas um roteador e pronto claro que deve-se guardar as devidas proporções, pois o nível de distribuição restringe-se ao nivel de infra-estrutura que você possui.

Então você deve está se perguntando e o que preciso para montar meu provedor de acesso a internet ou ISP (*Internet Service Provider*).

Bom vamos listar por tópico para você se organizar.

Iremos listar os equipamentos que este e-book se refere.

Inicialmente você precisará de uma conexão de internet, como estamos falando de provedor e não compartilhamento de conexão adsl recomendamos que você adquira junto as operadoras um link próprio com a internet, ou um link dedicado.
Os valores cobrados pelas teles variam muito e inclusive são negociáveis, geralmente os preços são muito parecidos porém a qualidade do serviço vai variar de acordo com a

garantia de banda que a tele oferece.

No capitulo principais fornecedores você encontrará os links das teles e os serviços prestados.

2 . roteador para gerenciar e distribuir a conexão, neste tópico subdividiremos em partes para que você possa montar ou adquiri o routerboard à sua preferência.

Montagem do router :

Leia em arquivos suporte / montando caixa hermetica.pdf

Itens necessários:

1. Computador ou router board
2. Placa Wireless
3. Placa Ethernet
4. Caixa hermética
5. Antenas
6. Torre
7. Escada
8. Sistema para verificação do sinal

Os itens listados não constam cabos, pigtails, régua de alimentação e nobreak pois esses itens são dedutivos no momento da própria construção do sistema.
Abaixo descrevemos cada item descrevendo sua utilidade.

Computador :

apenas placa mãe, processador, memória, HD e fonte de alimentação (drive de cd-room,e monitor apenas para instalação inicial)

Computador com routerOS montado em caixa hermética.

Placas de rádios compatíveis com o routerOS:

O mikrotik trabalha com uma lista de hardware compatíveis, no brasil você encontrará muitos produto 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 mais encontradas e testadas:
DWL-G520 / ag530
Senao NMP-8602 (mini PCI você precisará de um adaptador para transformar em PCI)

Placa d-link dwl-g520 com chipset Atheros AR5213

Placa ethernet(necessário estar dentro da lista de drivers da mikrotik:

Essa interface receberá o link com a sua internet, geralmente só há a necessidade de utilização de um link.

O chipset mais encontrado e compatível com o Mikrotik é o RealTek RTL8129

Placa ethernet

Caixa Hermética:

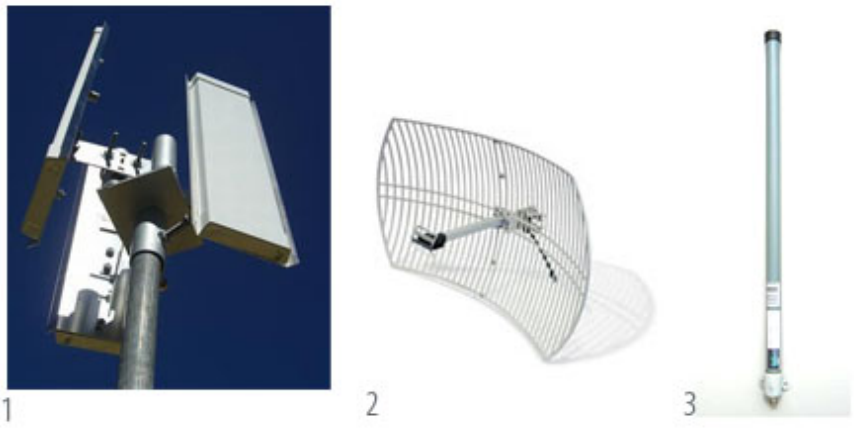
A caixa hermética será a base do seu router ou seja ela conterá todos os itens descritos acima, geralmente recomendamos caixas com o tamanho igual ou superior a 40 cm.

Imagem da caixa hermética

Antenas:

As antenas é a parte principal do seu sistema, ao trabalhar com o mikrotik as opções e formatação de seu sistema irradiante será conforme sua necessidade. Ex. Você poderá usar 4 antenas setoriais de 90º cobrindo a área de 360º ou se preferir utilizar 3 setoriais de 120º, ou setorial para cobrir uma determinada área e uma direcional para fechar um enlance com um repetidor, enfim, quem vai definir como e quando utilizar vai ser você.

Obs: não recomendamos a utilização de omni devido a baixa capacidade de irradiação. Antenas setoriais é a melhor solução para seu sistema, além de cobrir uma área maior que as direcionais.



Principais antenas utilizadas no provedor via rádio: 1) Painel setorial, 2) Parábola vazada (direcional), 3) omni

Torre:

A torre ou local onde será instalado as suas antenas deve ser alta e ultrapassar as barreiras iniciais, existem no mercado 2 tipo de torre que são as mais comuns entre os provedores, estas torres são:
Torre Estaiada : são torres de base modular ou triangular de 35cm à 40cm de lado. Estas torres são indicadas quando a altura ideal mínima ultrapassa 15mts e quando é necessário a subida periódica de técnicos, onde o reparo poderá ser feito em cima da torre sem a necessidade de descer o equipamento.
Torre telescópica: São torres muito útil prática e barata, exigindo menor habilidade para instalar. Essas torres alcançam até 12 mts sendo que a cada 3 mts você terá a opção de usar estais (ou cordas de sustentação) que deixará a torre estável e resistente aos ventos.
Além destas duas torres existe também a **torre autoportante.** são torres que têm sua base maior que o seu ápice havendo um afunilamento gradual relacionado a sua altura. Estas torres têm a vantagem de ocupar uma área útil menor que as estaiadas pois não são necessários as estaias para mantê-la estável, além de permitir a subida e o reparo na própria torre. A desvantagem deste tipo de torre é o seu preço que é muito maior que as ostras duas citadas.

1) torre Estaiada 2) torre autoportante 3) torre telescópica

Escada:

Uma escada telescópica será de muita utilidade quando você for verificar o sinal em sacadas, telhados e lugares altos, recomendamos escadas a partir de 6mts levando em conta a média do pé direito de de 3mts em uma casa típica do Brasil, caso tenha um pavimento você poderá subir no telhado a partir do térreo.

Sistema para verificação de sinal no cliente:

Definiremos como sistema pois assim é composto de mais de um equipamento.

Um sistema para verificar o sinal em seu cliente será muito útil e quanto mais completo mais fácil será a sua vida quando você estiver procurando sua torre.

Existe um tópico falando só sobre este assunto.

Torre

A torre será seu principal aliado no que diz respeito a distância que você vai alcançar com seu provedor, é claro que quanto mais alta a torre melhor correto? Correto, porém uma torre deve ser maior que as barreiras existente no local, não existe necessidade de você construir um monumento de 30 mts de altura em uma cidade plana e com edificações inferiores a 12 mts. Estude direito o local e a topologia da área de atuação do seu provedor.

Ainda sobre a altura da torre, é fato que quanto mais alta for, mais longe o seu sinal chegará, como foi discutido anteriormente, lembrando sempre que enquanto a zona de fresnel estiver livre de barreira maior a possibilidade de realizar um enlance mais distante, na tabela abaixo você poderá comparar as distâncias alcançadas x a altura da sua antena, levando em consideração que esses valores não são exatos e a distância vai

depender de muitos fatores como potência do rádio, tipo de antena e qualidade da mesma.

Dist6ancia	***Altura da Antena (m)***
1,6km	3,6 m
4,8km	8,1m
8km	10,5m
12km	14,4m
16km	17m
24km	25m
32km	34,5m

fonte:HyperLink Tecnchnologies, Inc.

Atualmente o google eath é uma boa ferramenta para verificação de altura, lembrando que a altura dada pela ferramenta não eh precisa, mais lhe dará uma base para você projetar sua torre.

Existem muitas maneiras de você adquirir sua torre, uma delas é você ir à um serralheiro, com um esboço em mãos e pedir para ele construir para você os módulos, esta forma é pouco recomendável, pois você correrá o risco de construir algo fora do padrão e a economia será muito baixo além do tempo que o serralheiro irá gastar, mais tempo para supervisionar o serviço e ainda a possibilidade de ficar mal feito, fora que você terá que buscar parafusos, cabos, sistema de balizamento enfim, se seu intuído não é vender torres então compre-a pronta, atualmente existem empresas e pessoas no próprio mercado livre que estão fornecendo torre estaiada em módulos de 2mts e construídas dentro dos padrões da abnt, esses módulos ficam em torno de 150 reais.

Se você tem uma boa laje ou uma caixa d'agua alta, você já terá uma vantagem que lhe propiciará uma economia muito grande.

Atualmente existem torres telescópica que oferecem mais de 20mts de altura, essas torres são fáceis de instalar e de fazer a manutenção, a desvantagem é que você precisará descer ela completamente caso precise realizar algum reparo nos equipamentos, porém como estamos nos baseando em um equipamento que não deve parar isso ocorrerá muito raramente eu garanto por experiência própria, em um ano de atividade nunca precisei subir na torre para fazer qualquer reparo no sistema, apenas verificávamos a ação do tempo na torre para tomar medidas cautelares de segurança.

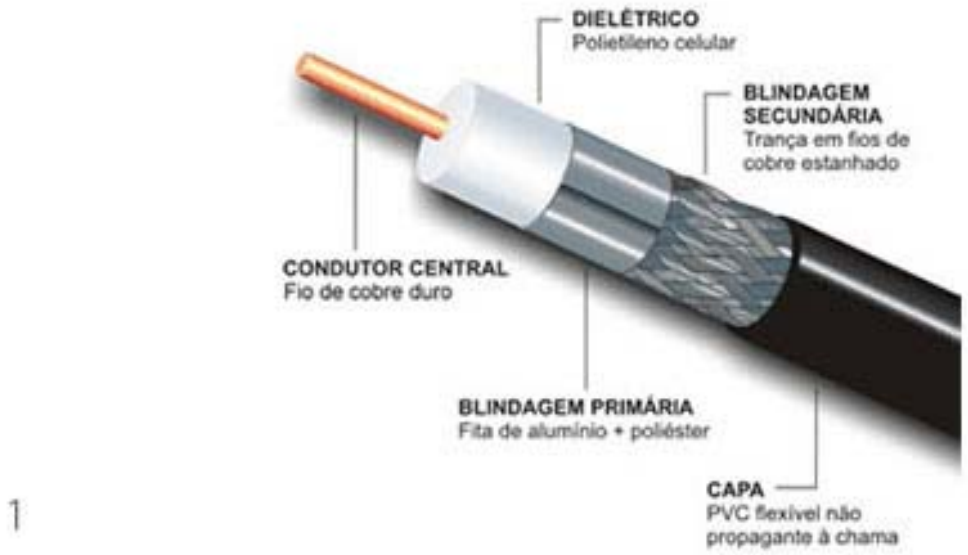
Disponibilizamos o link dos fornecedores no parte Principais Fornecedores

Cabos

Os cabos são de suma importância para o bom funcionamento de um sistema wireless, do mercado existem dois tipos principais de cabos são eles o recg 58 e rgc 213 alem do tradicional cat5 utilizado em rede wired ou cabeada e que também será muito usado.
A principal diferença entre os cabos rgc58 e rgc213 é a atenuação ou seja a perda de sinal relativa ao tamanho do mesmo, além é claro o diferença de valores o rgc213 chega a ser quase 8x mais caro que o rgc58 do cabo veja a tabela com a atenuação dos dois cabos.

Tipo de Cabo	Factor de Velocidade	1.2 Ghz	2.4 Ghz	5.8 GHz
RG-58	66%	0.692 dB/m	1.056 dB/m	1.692 dB/m
RG-213/214	82%	0.331 dB/m	0.499 dB/m	0.938

Em suma, o rgc58 oferece quase 2x mais “resistência” ao sinal, aumentando a perda do mesmo e possibilitando a existência de ruídos porém é 8x mais barato.



Desenho de cabo rgc

“Então p/ o padrão B e G (2,4Ghz) a interferência máxima para condução do sinal sem perdas significativas é aproximadamente 4dB, o que permite o uso de cerca de 4metros de cabo RG-58 e 8metros de cabo RG-213.

Para um elance com a finalidade apenas de recepção do sinal e navegação na internet a perda pode ser superior 7dB o que nos dá 6,5metros de RG-58 e 14metros de RG-213.”

Bom mais quando usar o rgc58 e o rgc213? A resposta é simples, você não vai implantar o rgc213 em todos os seus clientes, até porque ficaria caro e o cabo rgc213 é mais complicado para trabalhar pois o mesmo é muito grosso, outro motivo é que para o cliente só será necessário você estabelecer a conexão com a internet permitindo grandes perdas de sinal com a atenuação do cabo, diferente da sua base que terá que ter a melhor saída de sinal possível.

Para o cliente essa perda é irrelevante quando se faz o teste de sinal e se consegue um sinal possível de navegar dentro da velocidade contratada, eu já usei 30mts de rgc58 em um cliente e nunca tive problemas com ele, porém o nível de sinal caiu bastante, na prática tive uma perda de mais de aproximadamente 30db o que seria inviável caso o cliente estivesse muito longe.

Outra vantagem de utilizar o rgc58 é que o mesmo dispensa a utilização de pigtail fazendo conexão direta com as placas pci dos clientes.

Porém na base o ideal é que se use o rgc213, pois esse é o sistema que fará a irradiação principal e nós queremos que o sinal saia com o mínimo de resistência possível, para que possamos ter uma maior eficiência na nossa irradiação.

Além da utilização do cabo rgc213, na minha base utilizava tamanhos não superiores a 2 mts, o que aumentava as chances de ir mais longe.

Conectores:

- Conector N Femea P/ Rgc213
Os conectores N Femea servem para conexão de pigtail e algumas antenas que oferecem o conector N macho para sua conexão, vale observar que a maioria das antenas oferecem conector N Femea .

Conector N Femea P/ Rgc213

- Conector N Macho P/ Rgc213

Os conectores N Macho são comumente usado para conexão em antenas que oferecem conector N Femea para encaixe

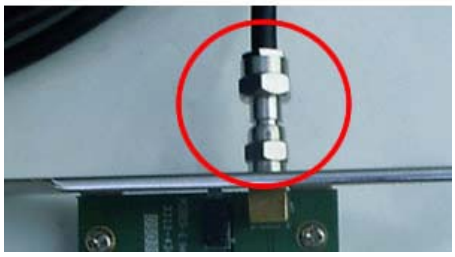
Conector N Macho P/ Rgc213

- Conector N Macho P/ Rgc58

Conector N Macho P/ Rgc58

- Conector Sma P/ Placa Wireless P/ Rgc58

este conector dispensa o uso de Pigtail conectando diretamente as placas wireless do cliente.



Conector Sma P/ Placa Wireless P/ Rgc58

- Pigtail

Os pigtails são utilizados para converter o padrão Rgc213 para o padrão sma utilizado na maioria das placas wireless, Porém alguns fabricantes utilizam outros padrões, como TNC Reverso utilizado em alguns produtos da linksys ou senão.

Modelo de pigtail ac/ufl

Montando o Cabo

Bom você já sabe quais os cabos comprar e quando usar.
Agora veremos como montar e testar se o cabo esta ok.

1

As montagens dos cabos são relativamente fáceis.
Um cabo RGC é composto por 6 elementos descritos de “a” à “f” que serão montados conforme instrução abaixo.

1. primeiro você adicionará os itens de “a” ao “c” no cabo começando pela porca(a), depois a arruela(b) e por último o anel de borracha(c).
2. Corte cerca de 3 cm do cabo deixando aparecer a malha de aço
3. dobre a malha de aço sobre o anel de borracha(c) e corte o excesso com uma tesoura
4. adicione o item “d”pressionando a malha de acho na borracha
5. corte agora a segunda proteção de plastico deixando cerca de 5mm além do ultimo anel de aço ou item “d”coberto como ilustrado na imagem acima
6. deixe mais 5 mm da haste de cobre para fora e insira o conector de cobre ou item “e” soldando-o em seguida
7. Enrosque o conector f ao conector a com o auxílio de duas chaves de boca.

Repita o procedimento para qualquer conector os elementos são os mesmos.

Testando o Cabo

Com o auxílio de um multímetro você checará o cabo com o conector, pegue um dos pólos do multímetro e encoste na parte de metal externa do conector, com o outro pólo encoste na haste interna caso feche curto já sabe, o cabo foi mal feito.

Cuidados após montagem dos conectores.

Na ponta do cabo que será conectado à antena externa vede com fita de auto-fusão os conectores para evitar entrada de água e consequentemente crie curto no sistema.

Cabo CAT

Cabo UTP é um dos mais usados para a criação de redes de computadores baseadas em fios. Seu desenvolvimento foi fruto dos trabalhos da Electrical Industrial American (EIA) e da Telecomunications Industrial American (TIA), que pesquisaram o desenvolvimento de um meio de comunicação eficiente para redes. Após essa definição, a Bell Laboratories trabalhou no desenvolvimento do cabo UTP (Unshilded Twisted Par).

Nas redes padrão Ethernet praticamente são só usados cabos UTP CAT 5. Isso quer dizer que esse tipo de cabo é composto por quatro pares de fios e opera à freqüência de 100 MHz.

A foto abaixo mostra os pares de fio. Repare que eles são combinações das cores laranja, azul, verde e marrom com correspondentes na cor branca. Assim, um fio na cor azul tem como par um fio nas cores azul e branco. Um fio na cor verde tem como par um fio nas cores verde e branco, e assim por diante:

É mais comum encontrar cabos UTP com revestimento na cor azul, no entanto, não é difícil encontrar cabos em outras cores.

Fonte:http://www.infowester.com/tutcabosredes.php

Cabo utp com conector rj45

Quando Utilizar o Cabo UTP?

Boa pergunta, porém apesar de ser um provedor a rádio em algum lugar desse provedor você precisará ligar um cabo correto? Além disto quando você precisar disponibilizar internet em um edifício toda a rede vai ser cabeada, pois as redes wi-fi foram projetadas para ambientes indoor.

Para fazer um cabo UTP será necessário:

- alicate de crimpagem
- Conectores RJ-45
- Cabo UTP padrão CAT 5

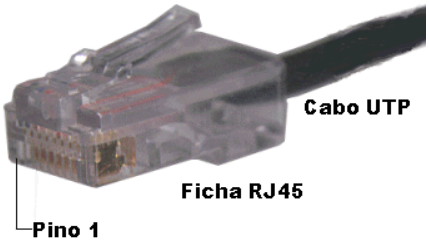
Quando for comprar o cabo verifique se o mesmo os pares estão em cores diferentes, puchando a capa protetora para trás você poderá ver os pares de fio, alguns fornecedores vendem cabos com apenas das cores o que vai dificultar e muito sua vida quando for separar os fios.

Fazendo um cabo direto:

Fazer um cabo UTP não tem mistério algum, basta inserir os fios no conector seguindo uma sequência da norma EIA/TIA 568A e depois crimpar com o alicate de crimpagem, para criação do cabo direto o procedimento deve ser o mesmo nas duas extremidades do cabo, seguindo a norma EIA/TIA 568A, para as duas pontas.

Sequência EIA/TIA 568A:

1. Verde-Branco
2. verde
3. Laranja-Branco
4. Azul
5. Azul-Branco

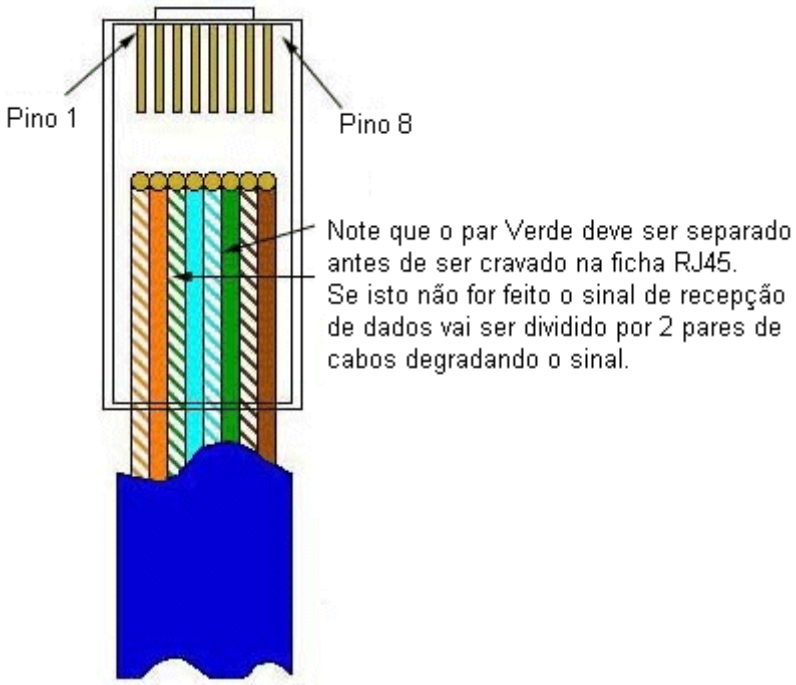


6. Laranja
7. Marrom-Branco
8. Marrom

Fazendo um cabo Crossover

Para fazer um cabo Crossover você terá apenas que modificar uma das pontas do cabo seguindo a norma EIA/TIA 568B.
Desta forma você terá uma das pontas formatado como o cabo direto e na outra como o cabo cross.

1. Laranja-Branco
2. Laranja
3. Verde-Branco
4. Azul
5. Azul-Branco
6. Verde
7. Marrom-Branco
8. Marrom



O cabo crossover servirá para você fazer a primeira conexão com o mikrotik com o seu computador afim de acessar o WinBox e realizar as configurações iniciais.

Antenas

A antena é o elemento principal do seu provedor, ela será responsável pela emissão do sinal. Atualmente o Brasil hoje produz suas próprias antenas através de empresas genuinamente brasileiras, porém como esse mercado têm crescido e sem controle algum existem empresas ou pessoas fabricando antena em fundo de quintal e falando o que

quer, para impedir os golpistas de plantão, a Anatel agência que regula a telecomunicação no país, emite um certificado de homologação para as antenas fabricadas no brasil, esse certificado atesta a qualidade dos produtos e evita que você leve gato por lebre .

Existem muitos modelos de antenas porém vamos citar as mais usadas afim de evitar que nos aprofundemos em assuntos que não faram diferenças, caso queira estudar mais sobre antenas a internet está repleta de artigos, inclusive em português que trata do assunto com mais formalidade.
Modelos usados pelo seu provedor.

Principais Modelos

1. Parábola Vazada (direcional)
2. Painel Setorial
3. Omni

É importante entender os aspectos físicos das antenas e para isso vou ilustrar com uma metáfora muito usadas pelos autores quando querem explicar a eficiência de cada antena, basta lembrar que as antenas são responsáveis pela focalização da energia e não pela produção ou amplificação da mesma.

A antena omni é uma antena projetada para emitir o sinal em 360 graus, diferente das direcionais e setoriais que emitem sua onda centralizada em um determinado ângulo, agora entrando na metáfora, imagine que a onda de rádio é a luz de uma lanterna, agora imagina que esta lanterna não tem um elemento refletor, sua luz vai ser jogado para todos os lados, porém a distância que a luz irá percorrer será reduzida, agora imagina essa lanterna com um refletor usando a mesma fonte de luz, a luz será concentrada em um ponto único alcançando distancias maiores porem em uma unica área de atuação.

As antenas citadas tem funções específicas no seu provedor que serão:

1) Direcional – as antenas direcionais são usados na maioria das vezes nos clientes,

estas antenas possuem uma potência muito superior às omnis e setoriais chegando a 30db, porém é necessário que ela esteja apontada exatamente para a antena em sua base, outra utilidade destas antenas é na criação de um ponto a ponto, onde geralmente utiliza-se duas direcionais afim de obter um enlance em distâncias maiores, a grande dificuldade desta modalidade é regular as antenas de forma que uma fique virada para outra, imagine você fazendo isso a 20 km de distância.

2) Omni – estas antenas são utilizadas por grande parte dos provedores de acesso caseiro, ou por locais públicos de acesso como hot-spot onde a área de abrangência é pequena e livre de barreiras.
   A principal vantagem desta antena é o baixo custo de aquisição aliado à utilização de pontos de acessos baratos, você conseguirá cobrir uma uma boa quantidade de pessoas porém se resumirá a uma área restrita. Muitos vendedores falam que seu produto tem um alcance de até 5km com este tipo de antena, acho pouco provável essa façanha a não ser que no raio destes 5km não exista nenhuma barreira e mesmo assim precisaria ver para crer. Inclusive alguns fabricantes sérios indicam o seu uso para interno.
3) Painel-Setorial - esta antena você irá usar em sua base pois além de cobrir uma área de até 90 graus definido pela sua abertura horizontal (existem fabricantes que produzem de 120 e 180 graus porém no brasil os produtos homologados vão até 90 graus) e um um logo alcance a depender do ganho supera os 10km de distância.
   Para você cobrir 360 graus você fará o uso de 4 antenas e 4 rádios ou poderá fazer uso de um divisor ou splitter (não recomendado).

O que é Mikrotik?

O mikrotik é um routerOS , ou seja um sistema operacional desenvolvido para realizar a tarefa de um roteador.
Desenvolvido pela MikroTikls empresa fundada em 1995 em Riga capital da Lativia região próximo à Rússia. A mikrotik nome comercial da empresa, desenvolve sistema para solução em conectividade como ISP (Internet Service Provider), administração de rede e serviço de conexão sem fio.
O sistema foi desenvolvido para funcionar em 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.

Principais Características

- Performance otimizada com o protocolo proprietário NSTREME
- Alta disponibilidade com o protocolo VRRP
- Possibilidade de agregar interfaces (bonding)
- Interface melhorada
- Poucas exigências de recursos de hardware
- Inúmeras novas funcionalidades
- Qualidade de serviço avançado
- Firewall "stateful"
- Protocolo Spanning Tree em bridge com filtros.
- Alta velocidade com 802.11a/b/g com criptografia WEP/WPA
- WDS e APs Virtuais
- Portal Captativo (Hotspot) com acesso Plug & Play
- Roteamento com os protocolos RIP, OSPF e BGP
- Acesso remoto com amigável aplicativo Windows - Winbox e administração Web
- Administração por telnet, mac-telnet, ssh e console
- Configuração e monitoramento em tempo real
-

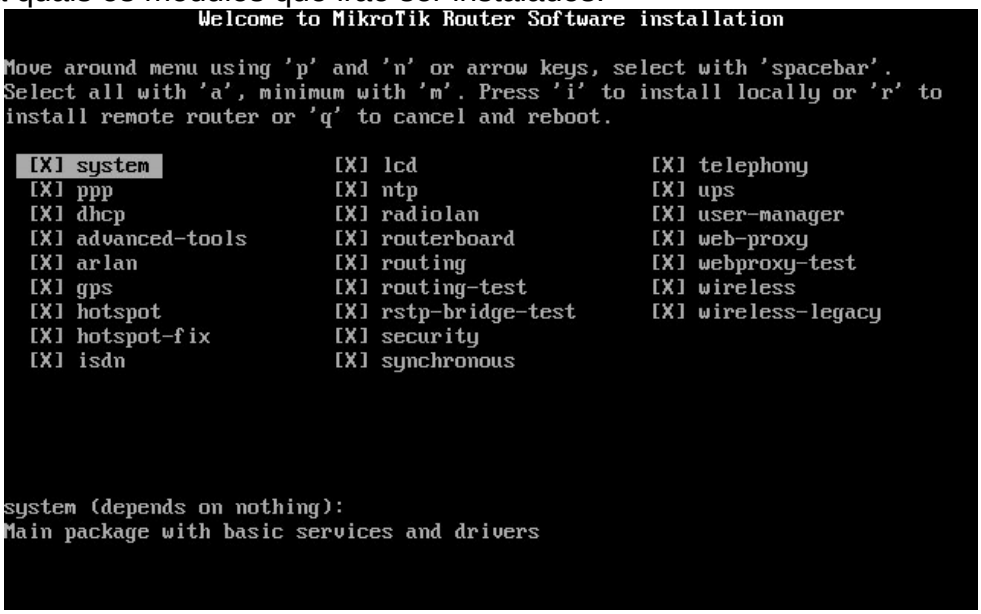
Preparando a Caixa Hermética

A montagem detalhada do Mikrotik na caixa hermética você encontrará em **arquivos suporte/montando caixa hermetica.pdf**

Instalando o Mikrotik

Com o PC já preparado com os hardwares listados, vamos inserir o cd do mikrotik e dar o boot pelo driver de Cdrom.

O sistema detectará o OS Linux e preparará para a instalação parando nesta tela onde você dirá quais os módulos que irão ser instalados.



Pessoalmente instalo todos os módulos apesar de não usá-los por completo, como uso um HD com muito espaço, o mikrotik instalado com todos os seus módulos não ultrapassa 30 mb, então prefiro instalar todos que fazer o Downgrade mais tarde pra usar algum serviço que não pretendia usar no início.

Então na tela de instalação aperte a **tecla "a"** (para selecionar todos os módulos) e depois aperte enter a **tecle "i"**para que ele faça a instalação diretamente no HD.

2) Quando perguntar se gostaria de manter a configuração antiga (keep old configuration?), **tecle "n"** para dizer que não, afinal estamos instalando pela primeira vez ;).
3) A instalação informará que todos os dados do seu hd serão apagados se você tem certeza que o HD pode perder os dados **tecle "Y"** e vamos lá
4) No final da instalação ele informará que o mesmo foi instalado e que você deverá **Tecle "enter"** para que ele possa fazer o reboot.
5) Retire o cd do driver e coloque o sistema para fazer o boot pelo HD.

6) Se tudo deu certo aparecerá a tela de login você usará o **login“admin” tecle “enter”** sem senha tecle **“enter”** novamente

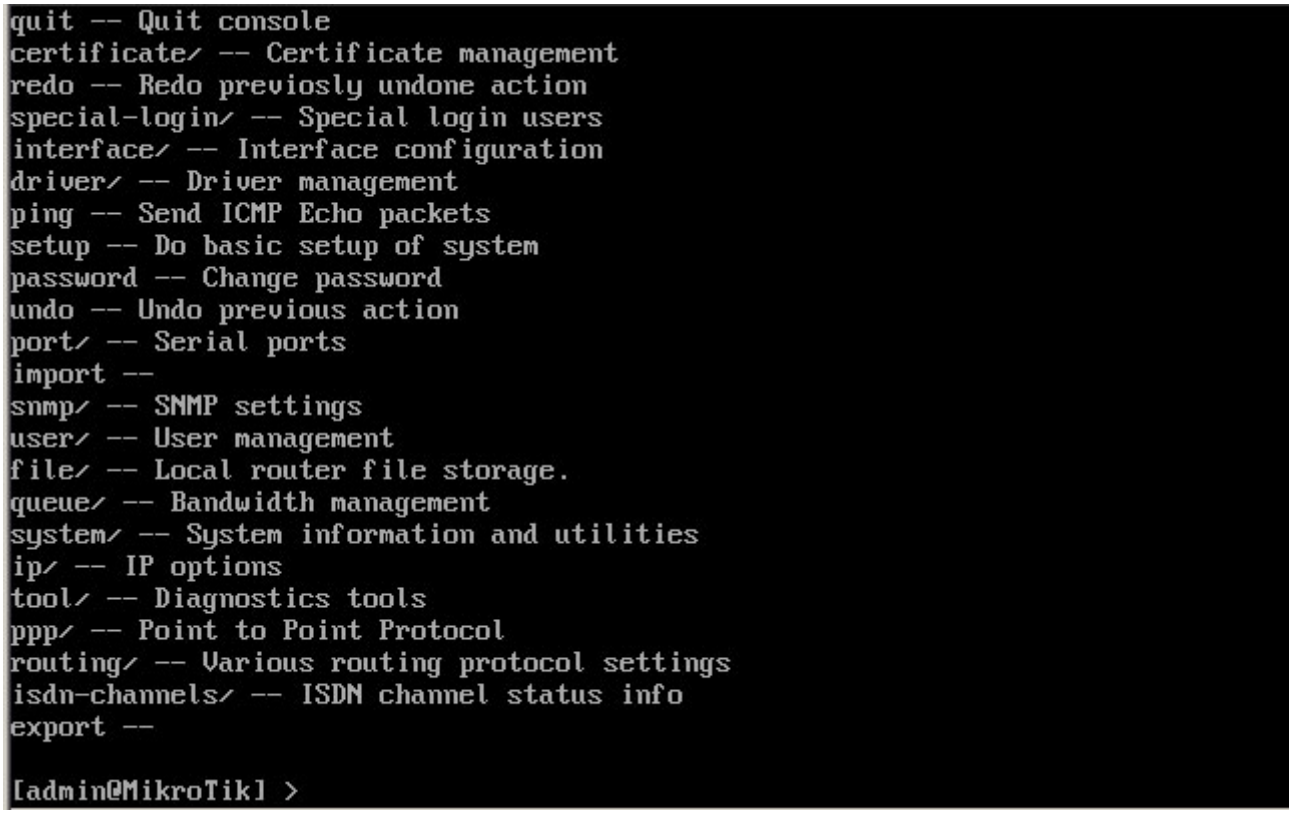
7) O sistema perguntará se você quer que exiba a licença, ao menos que tenha curiosidade tecle “y” do contrário **tecle “n”** e vamos ao que interessa.

Comandos Básicos

Bom agora vamos aprender alguns comandos básicos do sistema no terminal

O Mikrotik é um sistema fácil, para você que nunca viu e tem dúvidas porque não começar com uma **“?”** isso mesmo, quando você tecla interrogação ele vai passar todos os serviços disponíveis parecido com o dir do DOS.

Então vamos lá conhecer alguns serviços que nos interessa. **Tecle “?”** isso mesmo quando você aperta a interrogação aparecerá todos os comandos existentes naquele diretório, e seguindo a mesma lógica para os subdiretórios.



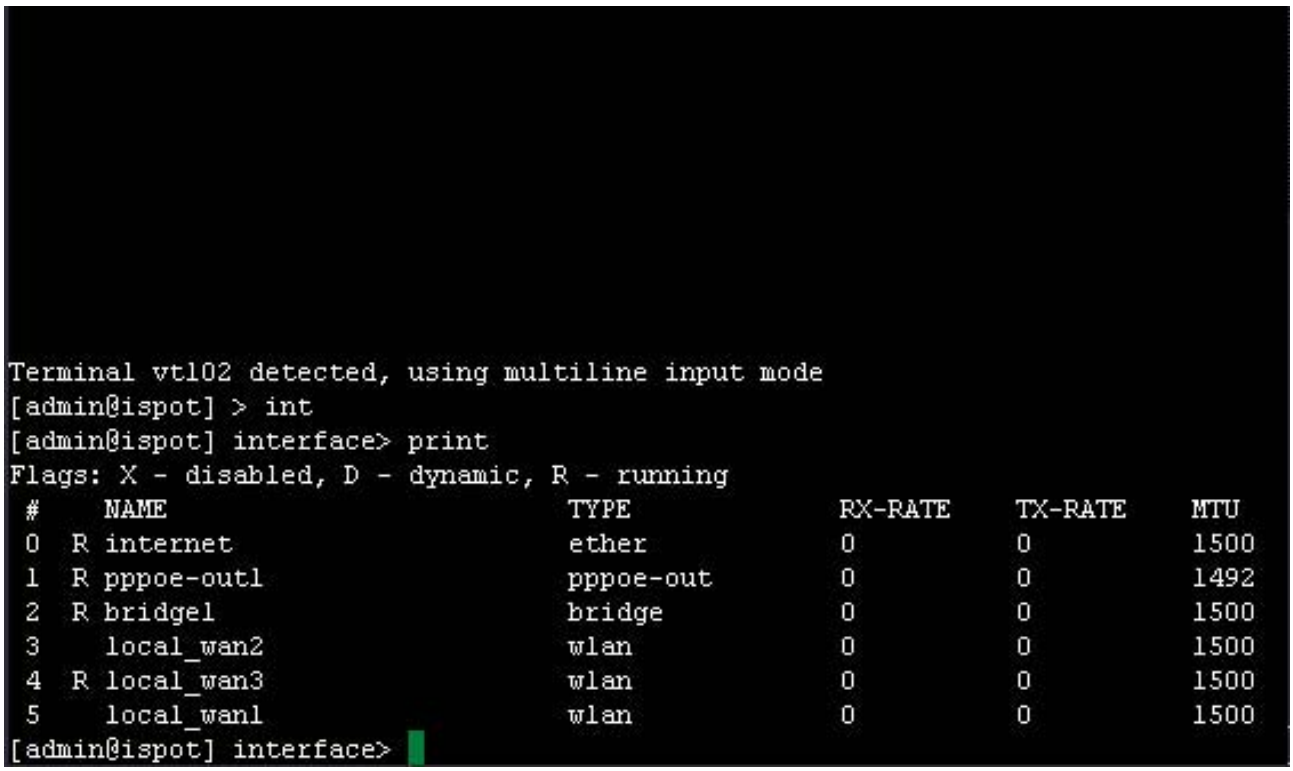
Antes de começarmos a listar os serviços existe um comando muito importante que se chama **“print”** com este comando você lista as opções de um determinado serviço, outro comando importante é a **“/”** com ela você retorna para o primeiro nível de comando, mais adiante veremos esses comandos na prática.

quit: tecle quit para sair do console e voltar para tela de login
certificate: o mikrotik possibilita a utilização de chaves de segurança e criptografia como ssl para proteger e dar maior confiabilidade aos serviços que você por ventura venha prover, como hotspot ou rede pública, esses certificados garantem maior confiabilidade para as pessoas que venham a usar os seus serviços. Obs (nunca usei por isso só vou citar).
Redo: este comando serve para você desfazer uma alteração e para refazer você digitará **Undo** para vizualizar o histórico vá para /system history print.
Interfaces: comando bastante usado para listar e configurar as interfaces que estão instaladas no MK.
Ping: assim como funciona com o DOS esse serviço enviara pacotes para m determinado endereço afim de obter um retorno ou ver a latência do mesmo.
Setup: este comando fará a configuração básica do sistema, como configurar ip, gateway entre outros, como não vamos usar e faremos a configuração individual.

Bom o resto dos comandos veremos no próprio winbox, pois o console reflete justamente o que temos no winbox.

Listando as interfaces instaladas no sistema

Tecle “interfaces” e depois t**ecle “print”** ficando assim “**interfaces print”** e enter ele listará todas as interfaces que você colocou como as interfaces disponíveis no seu sistema

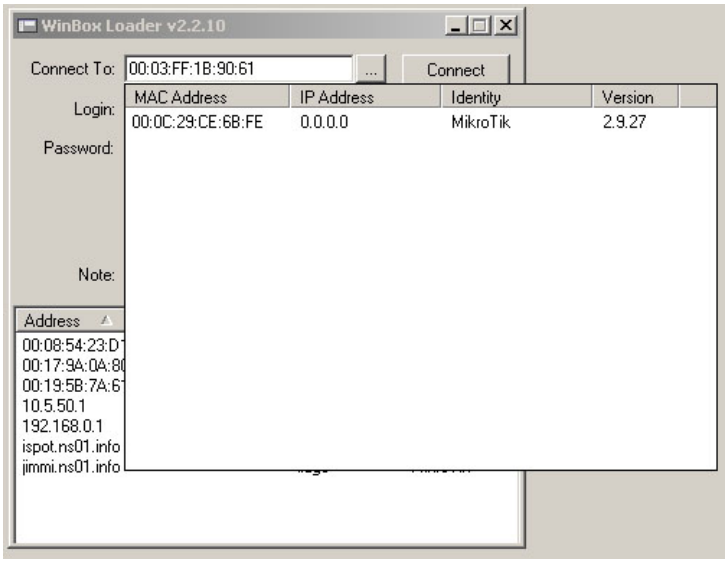


Se você instalou corretamente as placas e se elas forem compatíveis com os chipsets listados provavelmente aparecerá o nome **ether** para as placas **“ethernet”** e para as placas wireless **“wlan”.**

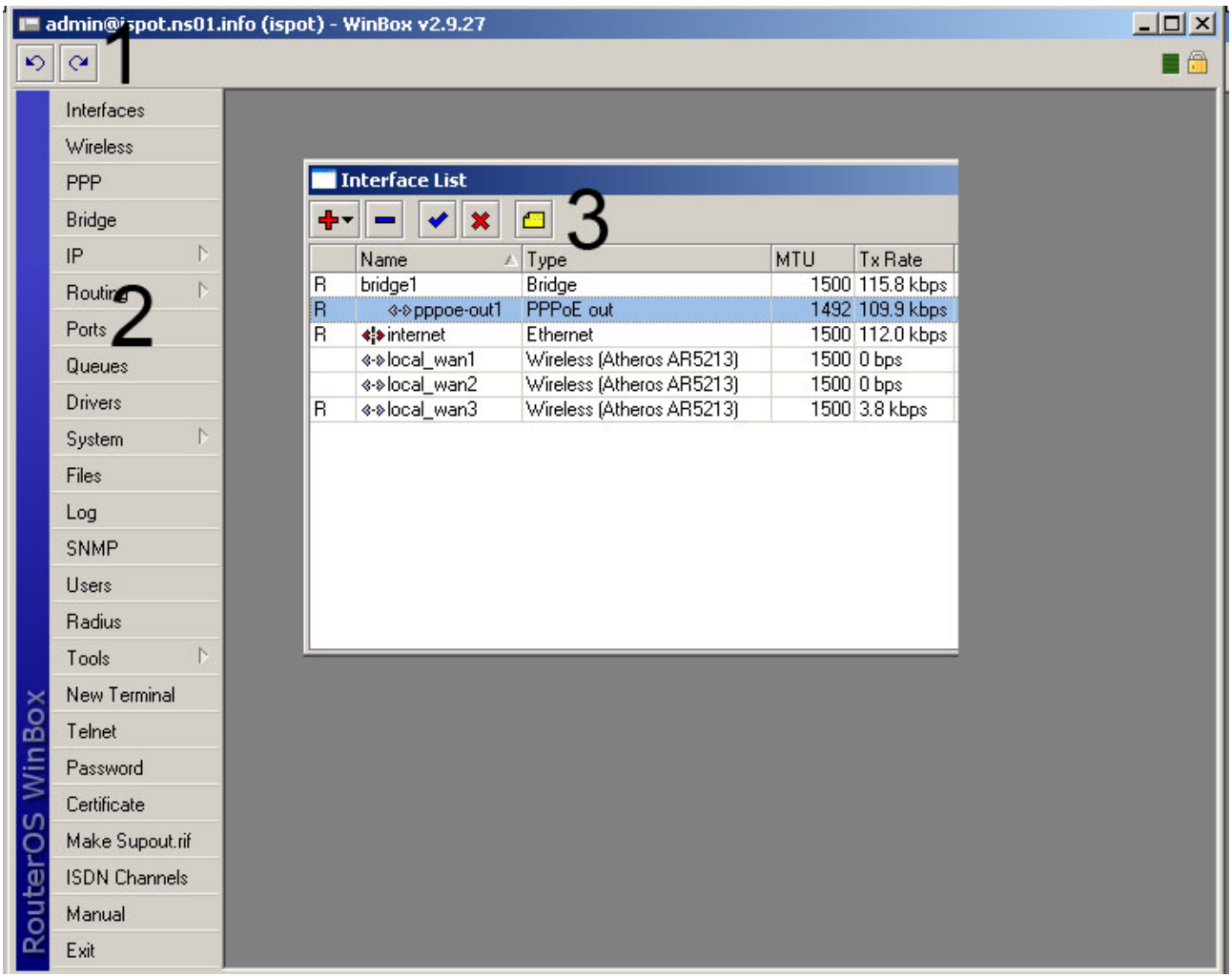
Winbox

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

Antes de acessar o mikrotik via interface gráfica é importante que você faça a conexão do sistema mikrotik com o computador remoto via **cabo UTP em *crossover***, desta forma o sistema reconhecerá o **mac** da sua placa no mikrotik automaticamente.
Para isso basta clicar nos 3 pontinhos ao lado do connect to e aparecerá uma lista das interfaces disponíveis.



Entendendo a tela do winbox

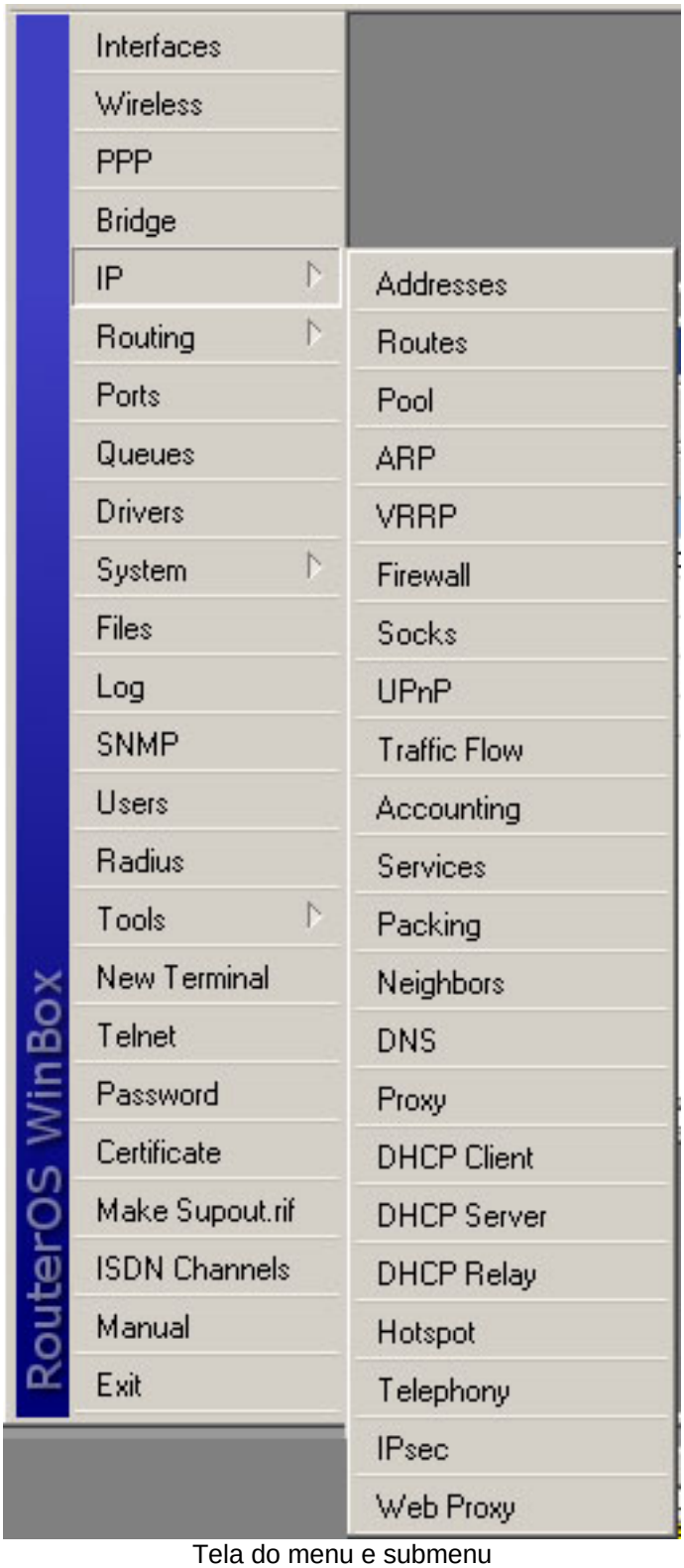


1) Botões Rendo e Undo

Os botões Rendo e Undo funcionam para desfazer ou refazer uma alteração rescente feita no sistema.

2) A tela do winbox é dividido em menu a esquerda, e sub-menu quando aparece a setinha ao lado do menu.

Fazendo uma comparação com o terminal, os comandos iniciais estão todos representados aqui, logo quando você estiver procurando algum tutorial específico e você encontre apenas em comandos, o caminho a ser seguido é o mesmo ex:
para visualizar as interfaces no terminal de comando você deverá acessar “**interfaces print”** se lembra? Então o sistema mostrará todas interfaces instaladas, no winbox só precisará ir no menu interfaces e todas as interfaces estarão listadas também.



Tela do menu e submenu

3) Botões de ações:

Os botões a seguir representam respectivamente:

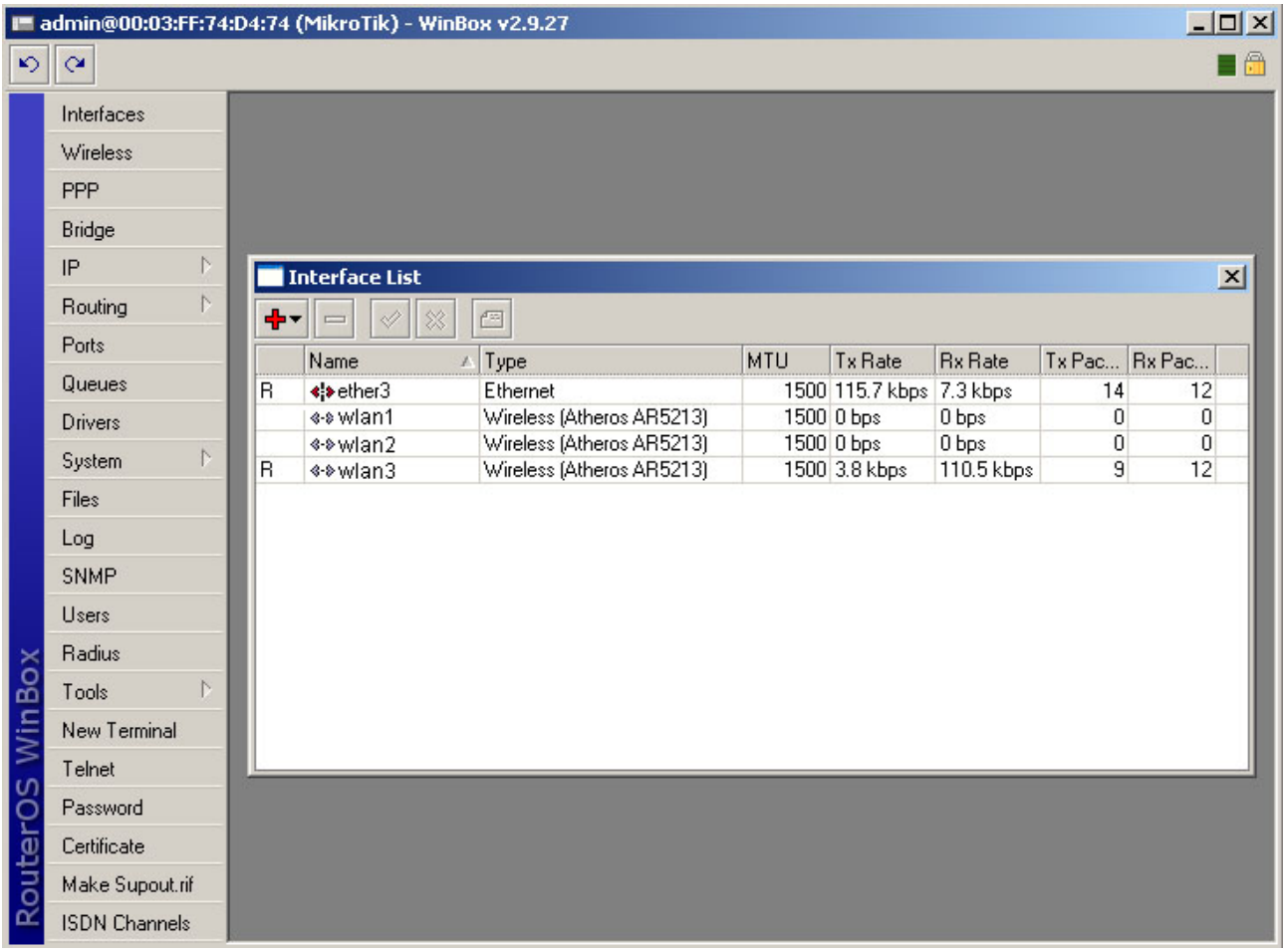
1. o sinal de mais significa que poderão ser adicionado novas entradas
2. o sinal de menos removerá uma entrada selecionada

3. o botão “v” check habilita uma entrada desabilitada (as entradas desabilitadas estarão em cinza)
4. o botão “x” desabilita uma entrada habilitada
5. o botão “lembrete” faz um comentário em uma determinada entrada.

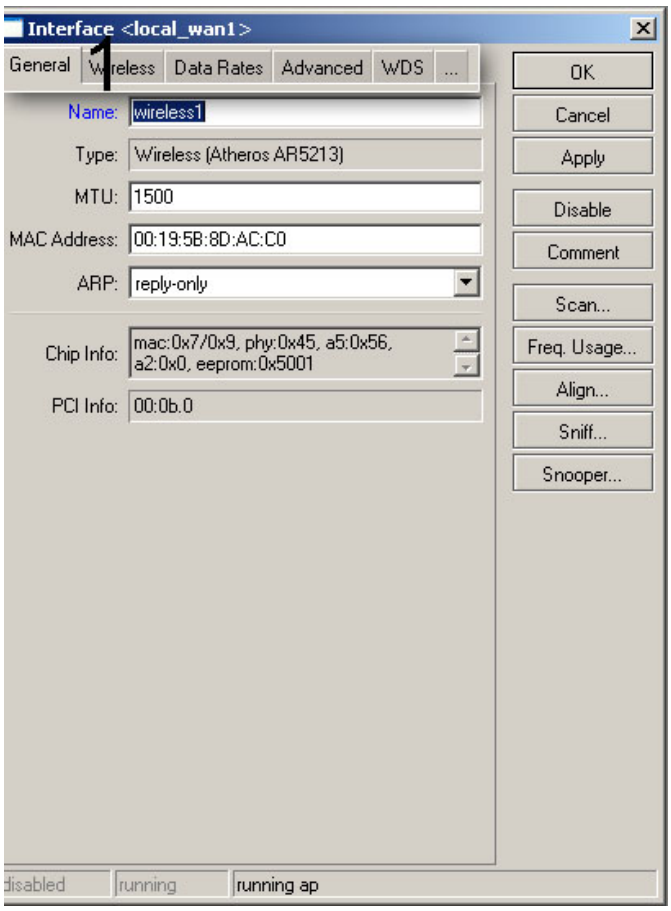
Configuração

Todas as configurações do mikrotik dar-se-á pelo próprio winbox, para o melhor aproveitamento deveremos seguir as etapas exatamente como o livro sugere, após a configuração você poderá altear o sistema ao seu gosto.

Configurando as Interfaces



Sua interfaces serão apresentadas nesta tela, as interfaces wireless são apresentadas como wlan e estarão desabilitadas, você deve clicar 2x sobre a interface wlan1 abrindo as configurações desta interface realizando as seguintes modificações para que ele se comporte como ap ou acesses point:

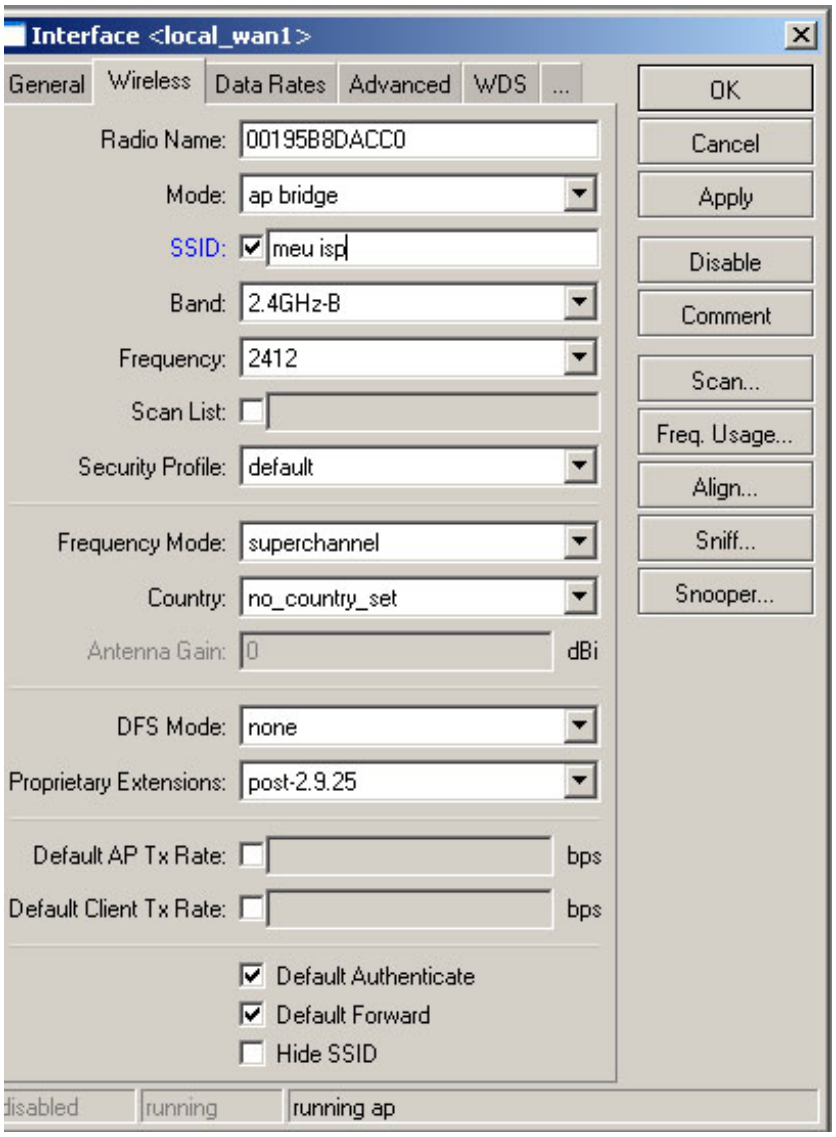


Dado dois cliques na interface você terá a tela acima, na aba general em destaque com o número 1 é a primeira área a ser configurada, vamos listar os nomes e as funções dos principais campos a serem alterados:

Aba General

1. **Name:** em name você colocará um nome para sua interface, esse nome será apresentado na tela principal de interfaces. Está função é muito importante para você organizar seu sistema.
2. **Type:** mostra o modelo da interface instalada
3. **MTU:** “Unidade Máxima de transferência” não mexe deixa como está.
4. **ARP:** ou “Address Resolution Protocol ” serve para buscar um endereço físico (mac) a partir de um endereço IP.
   Marque reply-only:
   As configurações disponíveis são:
   disable: não responde a solicitações ARP
   proxy-arp: passa o seu próprio MAC
   reply-only: repassa as requisições.
5. Mac-Address: é o endereço físico da interface atual.
6. Chip-Info: informações sobre o chip da interface.
7. Pci-Info: informações sobre a unidade pci que está ocupando no sistema.

Aba Wireless

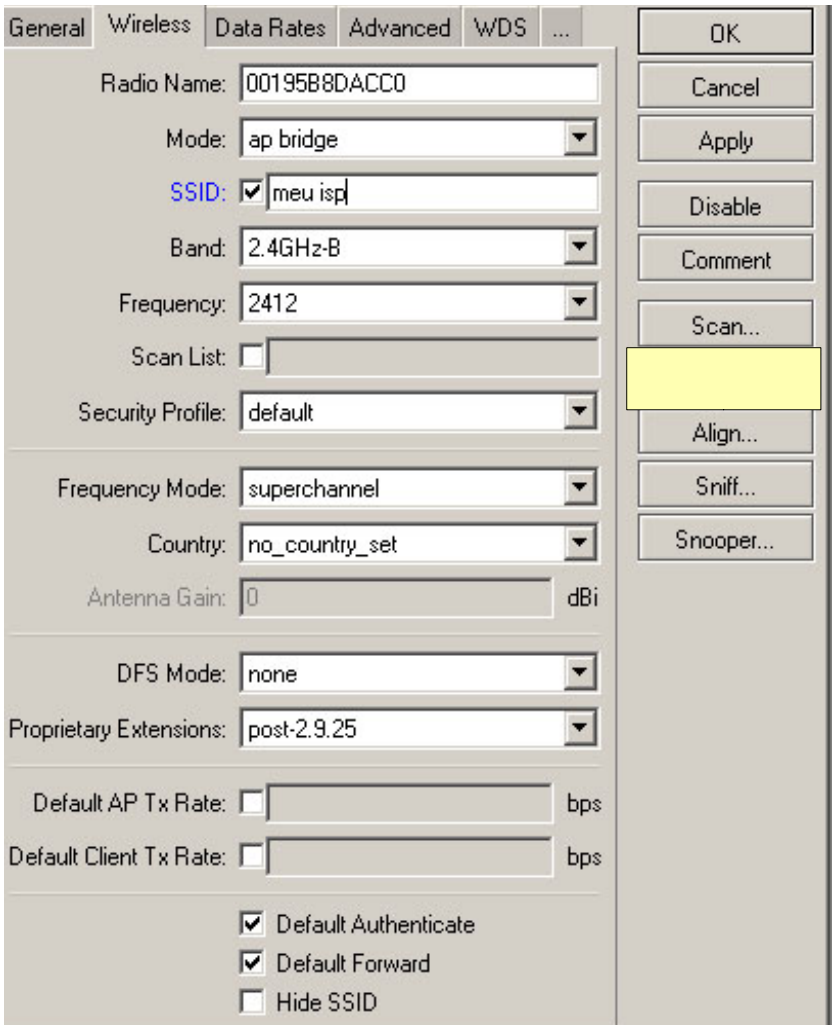


Na aba wireless serão feitas as configurações básicas do sistema no que diz respeito a conexão wi-fi configure como está na imagem.

1. **Radio Name:** O nome usado para identificar a interface
2. **Mode:** o modo de funcionamento do rádio ou para que função você quer destinar a ele, se você já tem alguma familiaridade com os aps normais você se identificará com algumas funções.
   Configure para Ap-Bridge pois nossa intenção é distribuir a internet.
   - **Station:** modo cliente
   - **Station WDS:** possibilita repassar os endereços realizando um bridge transparente.
   - **Ap-Bridge:** Funciona como um acsess-point repassando os endereços transparentemente.
   - **Bridge:** como o nome sugere, faz apenas o papel de bridge
   - **alignment-only:** para realizar alinhamento de antenas apenas.
   - 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.

3. **SSID:** serve para dar nome a sua rede, ou seja as pessoas que captarem seu sinal estarão enxergando o que você escrever aqui, caso você deixe desmarcado não será possível enxergar seu nome nas redes wireless disponíveis.
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 quase absoleto e é usando apenas para realizar ptp por alcançãr maiores distâncias porém devido a sua restrita velocidade resumida em 2mbps ela tem sido deixada para traz, quanto a banda "b" já chega a 11mbps se tornando viável para tráfego mais intenso de dados além de ser estável e e segundo algumas pessoas consegue um alcance maior que a banda g que por ventura suporta até 54mbps. Então ficaremos com a banda b
5. **Frequency:** a frequencia 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. Para você saber como estão sendo usados os canais de outros aps no local onde você irá atuar basta você clicar no botão scan no lado direito da tela de configuração da interface, e ele vai lhe mostrar todos os sinais captados pela sua antena. Ou você poderá usar o Freq. Usage logo abaixo do Scan para que você possa ver os canais que não estão sendo usados.



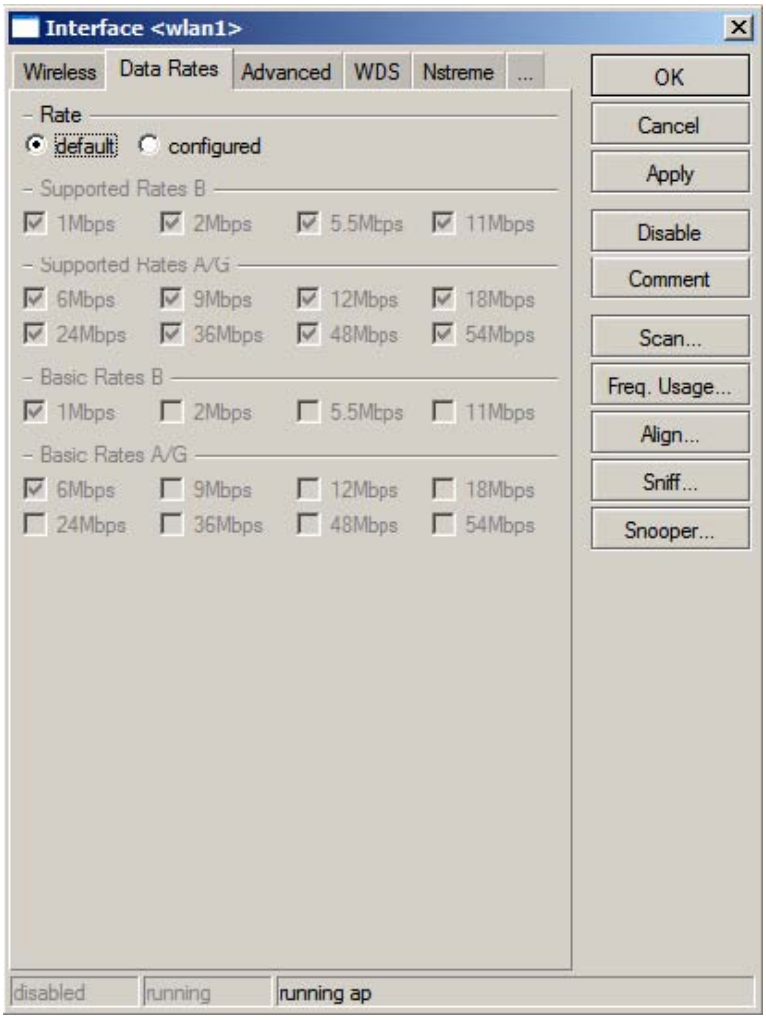
6. **Scan List:** Scaneia uma lista de frequências, não utilizaremos este recurso
7. **Security Profile**: Prefiro não utilizar nenhum meio de segurança externa pois você bloqueará possíveis clientes que captarem o seu sinal evitando que eles entrem no site de autenticação do seu hotspot e visualize seu hotsite perdendo desta forma m ótimo canal de comunicação, caso você queira usar um sistema de Autenticação como WPA você deve ir no menu wireless / na aba security (veremos a configuração de segurança mais adiante)e configurar um profile com os protocolos de segurança que você definir.
8. **Frequency Mode:** o modo de frequencia assim como os canais permitidos mudam para cada país, este recurso permite que o mikrotik trabalhe dentro dos parâmetros do país selecionado. Aqui usaremos superchannel uma vez que os equipamentos utilizados são homologados e suas frequências e canais de funcionamento estão 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.

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 cada cliente para esta interface.
12. **Default Authenticate:** estabelece a autenticação padrão para os clientes se conectarem ao ap.
13. **Default Forward:** desmarque está opção caso não queira que os clientes se enxerguem na rede é preferivel em um isp que os clientes não tenham acesso a rede local podendo acessar os computadores dos outros clientes.
14. **Hide SSID:** caso marcado o nome da rede em broadcast será omitido aos clientes.

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.



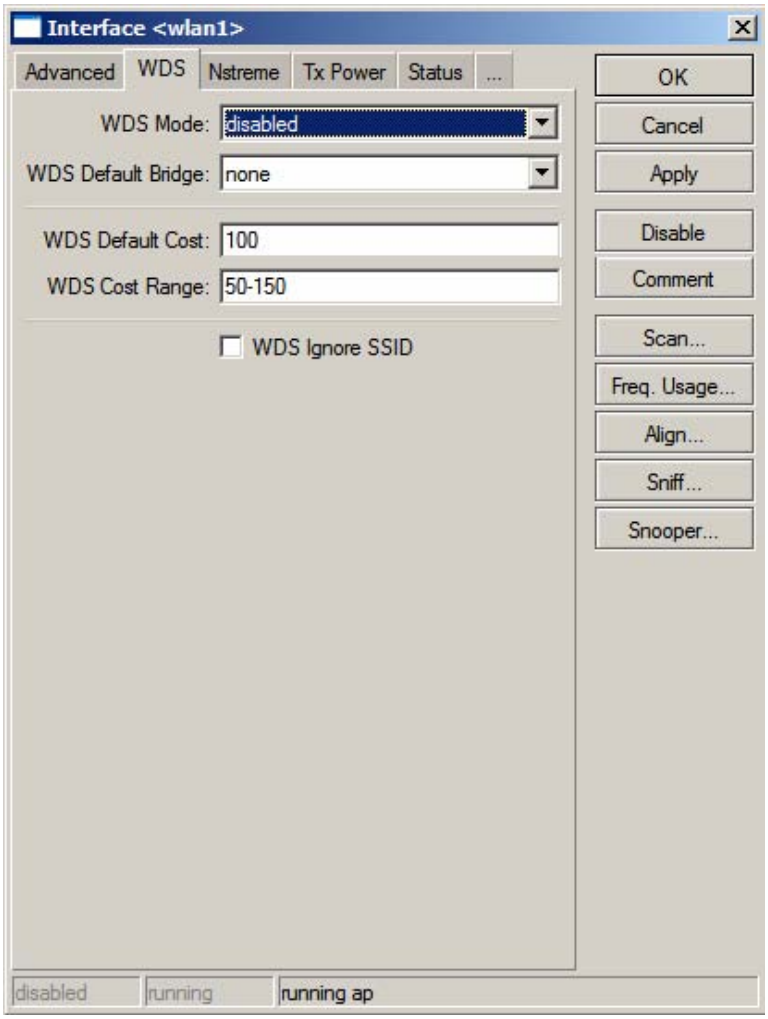
Aba Advanced

Nesta aba você fara as configurações detalhadas do AP. Não iremos nos aprofundar mais nesta área para sermos diretos e evidenciarmos apenas o foco deste manual que é a instalação do mikrotik e sua configuração básica e melhorarmos nosso processo cognitivo.

caso queira mais detalhes sobre o assunto busque nos **arquivos suporte /mikrotik detalhado.pdf.**

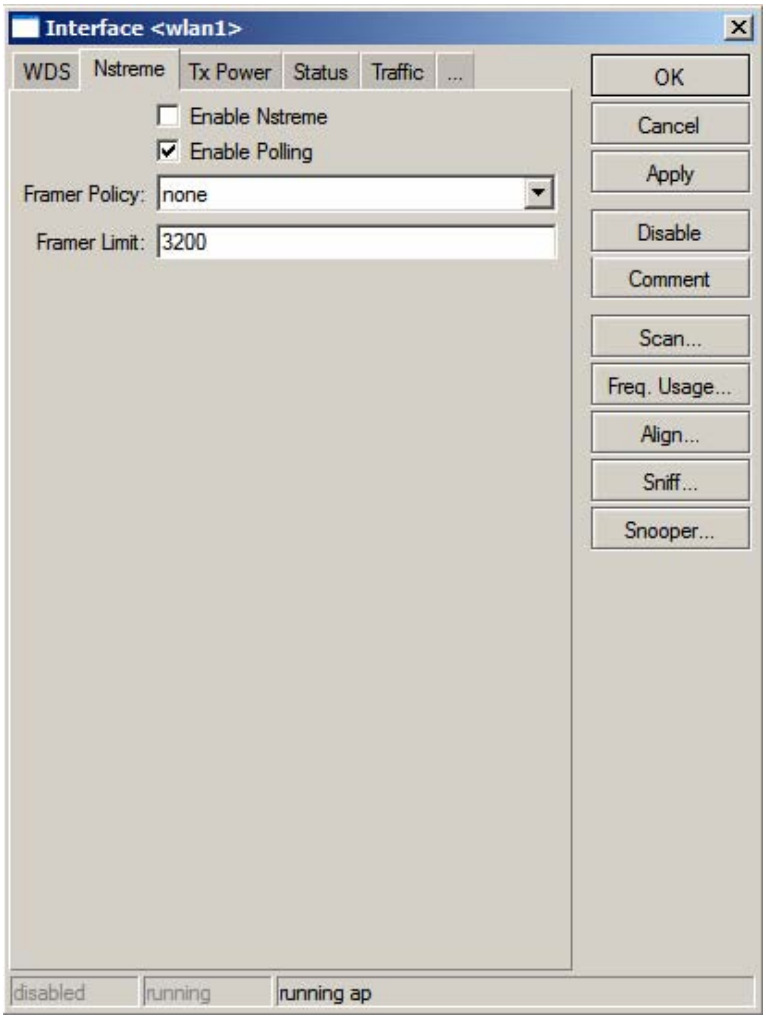
Aba WDS

Está área define se a interface fará o wds sistema de distribuição sem fio, esse sistema serve para repetir o sinal por outro ap, voltaremos a explicar como realizar o wds na parte sobre o mesmo deste livro, deixe tudo como esta e vamos para próxima aba.



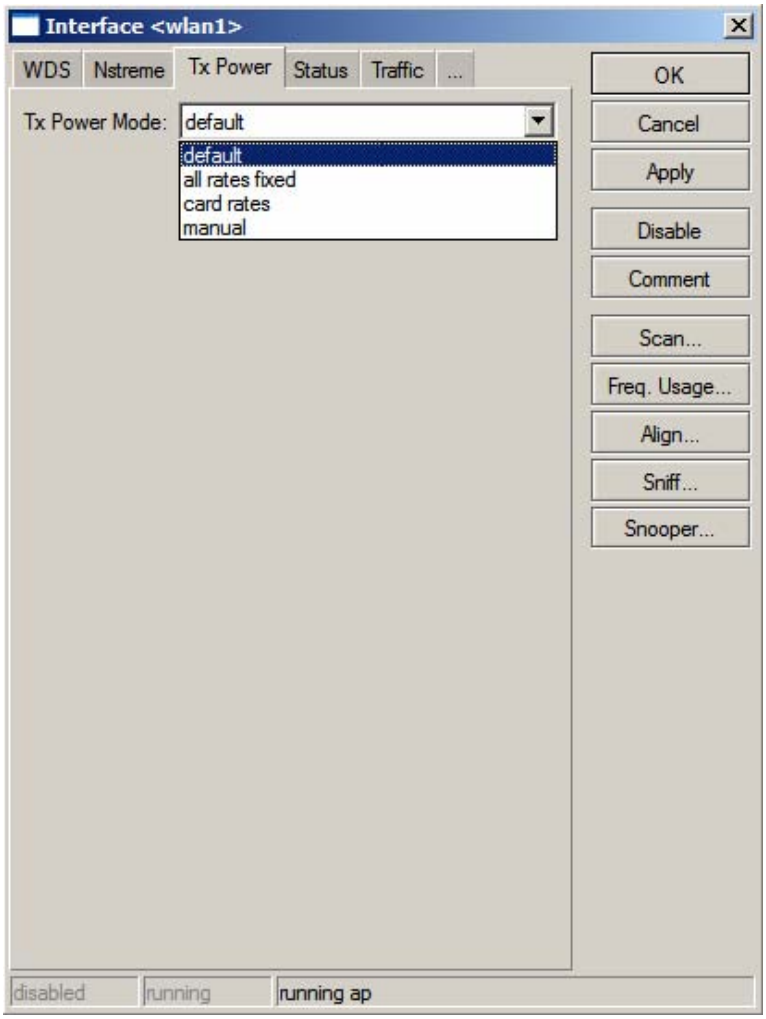
Aba Nstreme

Mais uma vez não precisaremos configurar nada aqui, por se tratar de um protocolo proprietário da mikrotik não marcaremos por falta de compatibilidade com outros deixaremos apenas **Enable Polling** marcado esse protocolo evita colisões com nós escondidos na rede.



Aba Tx-Power

Aqui nos interessa e muito, pois aqui definiremos a potência das placas instaladas em 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 que a mesma oferece até 30 dbm, porém na prática a atheros ar5213 só chega até 23 dbm ou 200mw de potência, que para nosso sistema já é um ótimo negócio, é muita potência e o suficiente para atender nossos cliente a uma distância média de até 5 km com painel setorial de 21dbi, onde foi testado na prática por mim porém acredito que ele alcança distâncias maiores.



Em **Tx Power Mode** marque all rates fixed e coloque 23 no campo abaixo.

Veja a tabela de conversão de dbm para sua respectiva potência.

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

Aba Status:

Oferecerá todos o status da interface, informando:

1. Band: banda de operação da interface.
2. Freqüência: o canal utilizado.

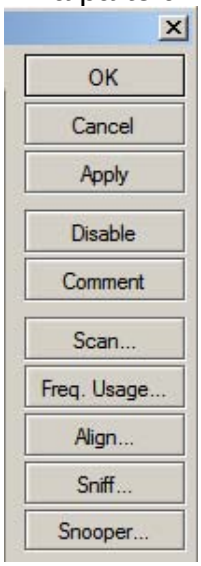
3. Registered Clients: clientes registrados
4. Authenticated Clients: clientes autenticados
5. Overall Tx CCQ: ou qualidade de conexão do cliente, onde mostrará o valor em porcentagem da qualidade de transmissão do link.
6. Ack Timeout: o tempo limite de requisição de um pacote
7. Noise Floor: ruído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

Aba Traffic

Mostra graficamente o uso total do seu link

Finalizando

Após concluir as configurações desta interface clique no botão aply e enable depois clique no botão ok esses botões se encontram na parte direita.



Repita o procedimento para todos as outras interfaces wireless, você poderá mudar os ssid de cada inerface caso queira visualiza-las separadamente algo que recomendo, depois de tudo configurado você poderá utilizar o mesmo ssid.
Qual a vantagem de usar o mesmo SSID? Caso você opte em utilizar o mesmo SSID os clientes que se conectarem a sua rede conectarão à interface com o melhor sinal automaticamente.

Pronto a partir deste ponto você já deverá enxergar sua conexão wireless no seu computador particular, caso ele tenha um dispositivo wi-fi instalado.

Pode desconectar o cabo do seu computador e acessar o winbox pela interface wireless

Criando uma conexão PPoE

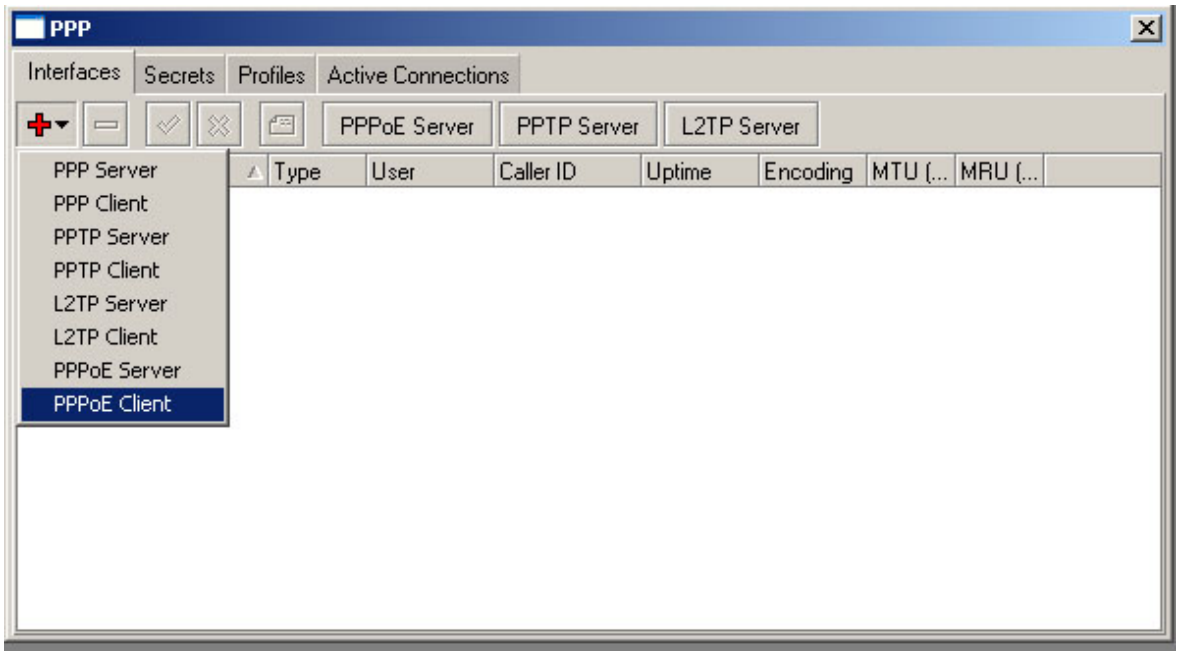
Como estamos montando um roteador iremos entender que o seu modem ADSL estará

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.

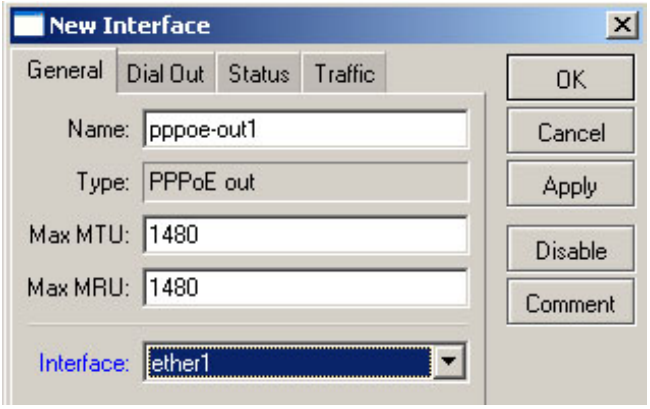
Menu PPP / interfaces

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



Escolha a opção PPPoE cliente e configure da seguinte forma:

Aba General

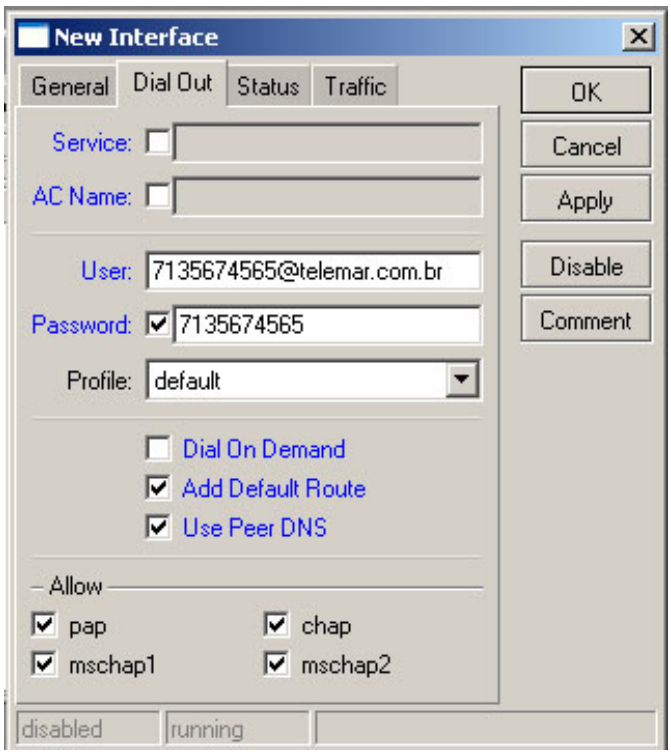


Name: escolha um nome da sua conexão PPPoE, esse nome é apenas para organizar suas interfaces

1. Max MTU – assim como nas outras interfaces vista esse número define a unidade de transferência máxima deixe em default assim como o MAX MRU

2. Interface: coloque a interface ethernet que esta conectado ao seu modem **ATENÇÃO: essa interface será alterada para bridge após agende criar a mesma no próximo tópico.**

Aba Dial Out:



Aqui você colocará as informações do seu ISP, alguns ISP não existe a necessidade de autenticação para isso você só precisa de um número de telefone comercial.

1. **Service:** não precisa marcar.
2. **AC Name:** Não precisa marcar.
3. **User:** o número de autenticação que a telemar fornece como login.
4. **Password:** a senha que a telemar fornece, no caso da velox é o mesmo número de telefone sem necessidade do @telemar.com.br
5. Dial On Demand: precisa que você faça a conexão manualmente desmarque, pois queremos que ele volte a discar caso sistema caia.
6. O resto deixa como está na imagem acima não me aprofundarei em cada itém.

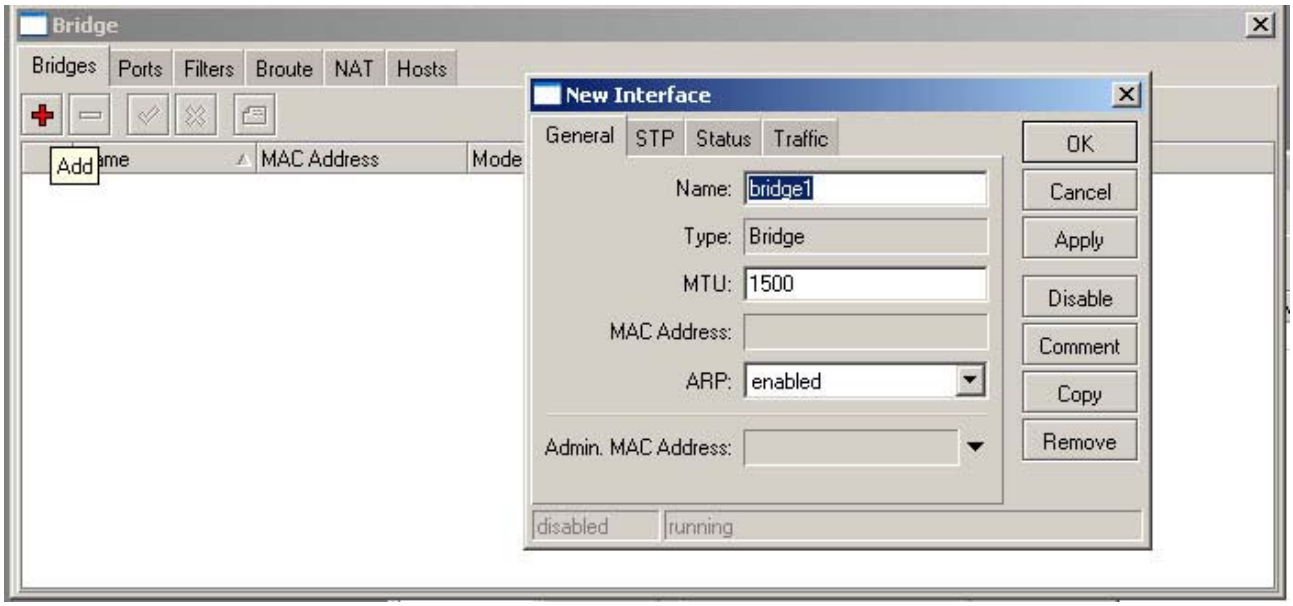
Pronto clique em **apply** e depois em **enable** para habilitar a interface e que ele comece a fazer a conexão, você pode acompanhar o andamento da conexão no roda pé da tela que você está (PPPoe interface). O status são **dialing** / **stabilished** e **connected** quando você estará conectado ao velox no caso.

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.

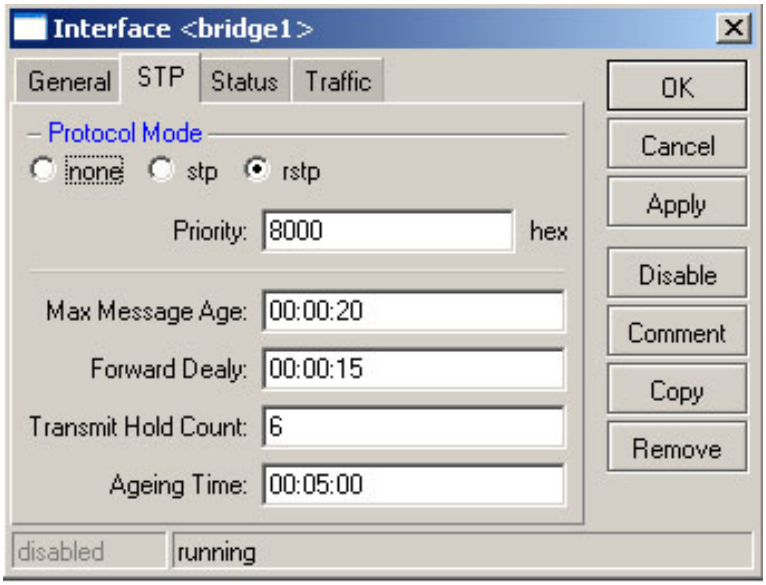


Aba General

1. **Name -** assim como se repete em todas as adições de interfaces o nome será apenas uma forma de apelidar uma interface afim de que tenha uma maior organização sobre seu sistema.
2. **Type -** o tipo de interface
3. **MTU -** deixa default
4. **MAC -** Address: será automático e definido pelo sistema.
5. **ARP –** deixa em enable
6. **Admin. MAC –** deixa em branco como está.

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 sugere inclusive a criação de uma rede mesh,

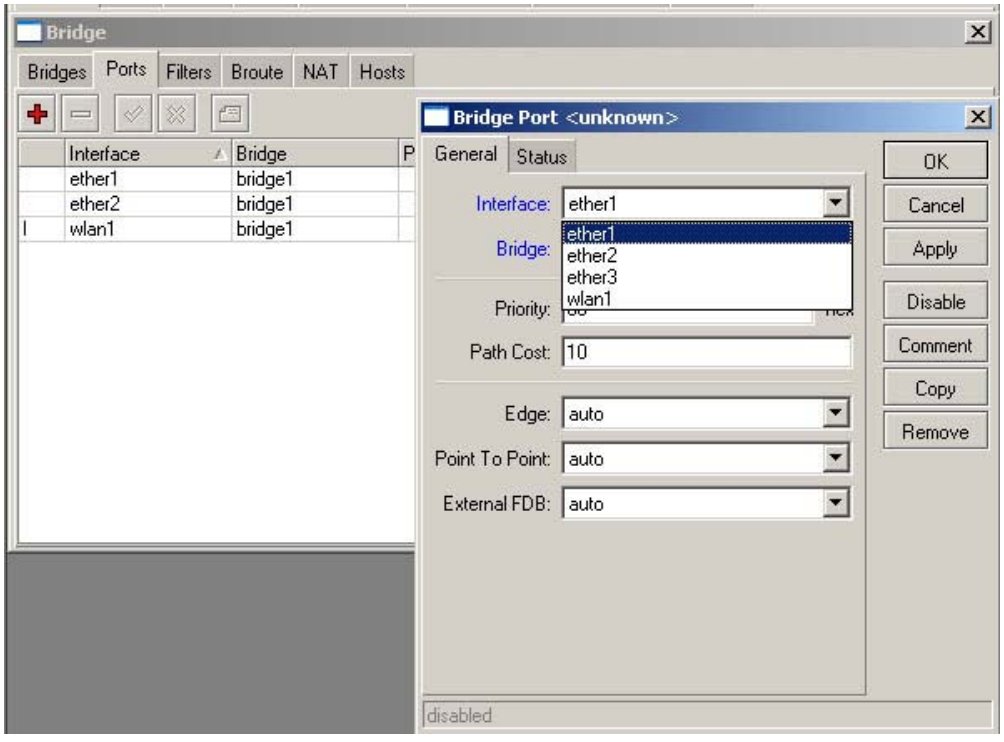


então a configuração ficará como da imagem acima, você só precisará marcar o protocolo rstp e o resto ficará em defaut.

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

Ainda em Bridge vamos para a aba Ports

Aba Ports

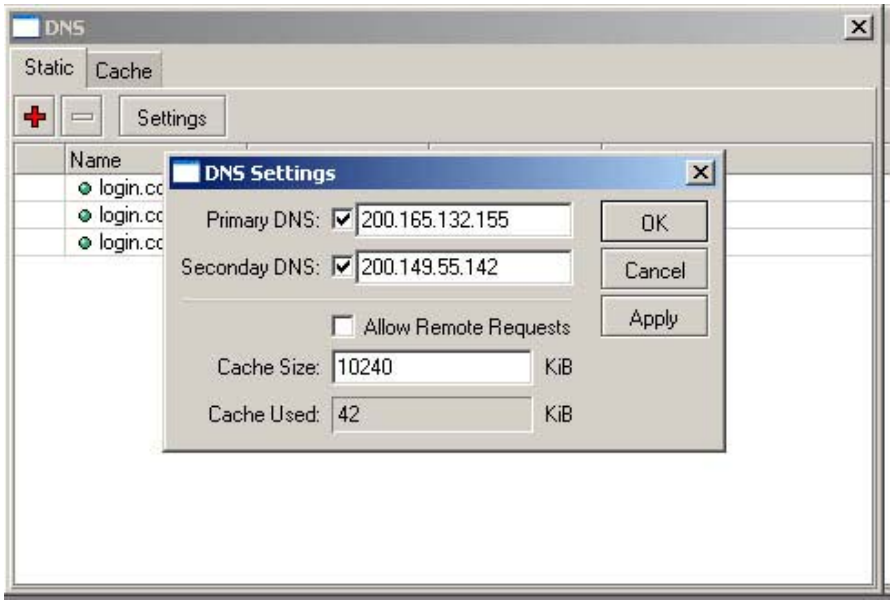


Na Aba ports clique no botão “+” para adicionarmos as portas de todas as interfaces que já foram configuradas anteriormente.

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

Configurando o DNS

O DNS neste manual será o do seu ISP, para saber o DNS do provedor de internet você precisará usar seu discador convencional, ir para o comando do DOS e entrar com o comando i**pconfig/all** então você terá acesso ao DNS do seu servidor.
O DNS abaixo é do velox e já foi testado em dois estados diferentes no nordeste, caso o seu serviço de internet seja o velox você poderá estar tesando o mesmo.



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

Aba Static

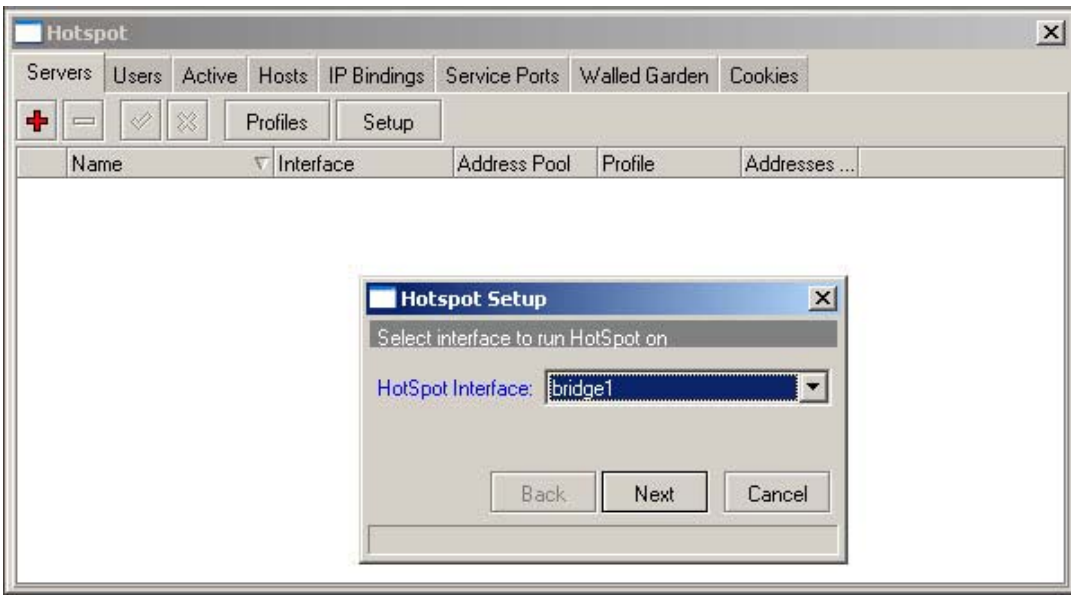
1. Primary DNS – coloque o DNS primário que você conseguiu.
2. Secondary DNS – coloque o DNS Secundário que você conseguiu.
3. Cache Size – O tamano do cache para o DNS fará uma armazenamento eporário das ultimas páginas visitadas pelos clientes em um cache de até 10mb no caso como é KiB cada 1mb = 1024 KiB então 10mb = 10240 KiB

Configurado o DNS você clica em apply e depois OK, vamos para o próximo passo.

Configurando Hotspot

A configuração de um Hotspot é simples e os passos a seguir serão bem intuitivos.

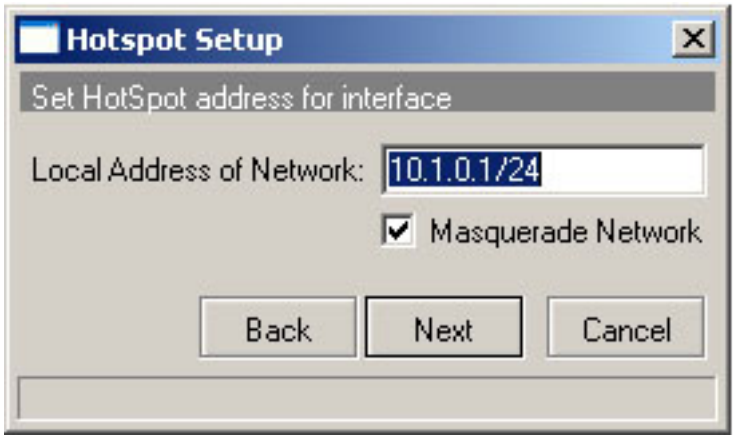
Vá para o menu **Ip** submenu **Hotspot**



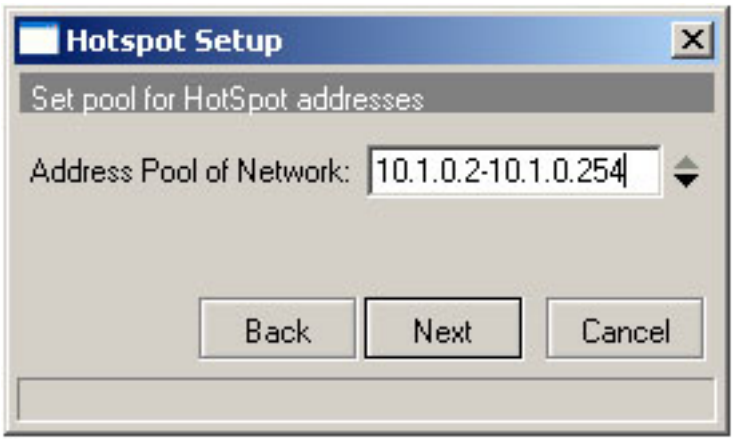
Aba Servers

Nesta parte configuraremos o servidor de hotspot para tanto clique no botão setup e seguiremos os passos até o fim desta etapa.

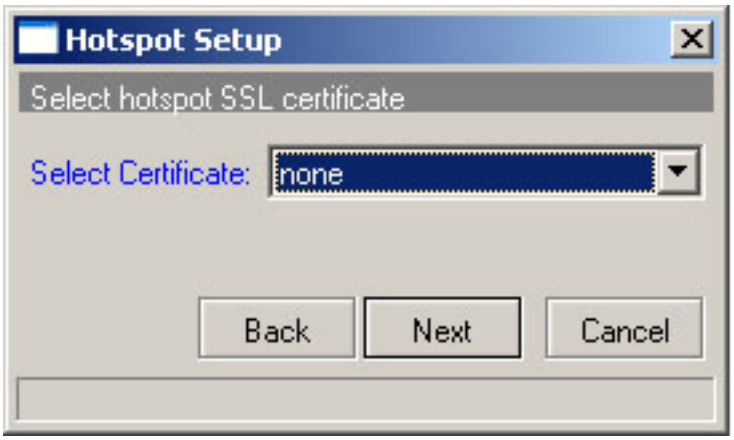
1. **Passo 1 [Select Interface to run Hotspot on]**, você deverá selecionar a interface que fizemos a bridge anteriormente. Clique em **next**
2. **Passo 2 [set HotSpot address for interface]**, aqui você definirá o ip da rede e sua máscara, neste caso uma máscara de 24 bits me dará uma faixa de 254 ips uma máscara de 22 bits me dará 1022 ips então quando vc for definir o tamanho de sua rede você colocará o ip da sua interface e no final você utilizara uma “/” e o tamanho da sua rede em bits. Assim como na figura abaixo com uma máscara de subrede de 254 ips. Clique em **next**



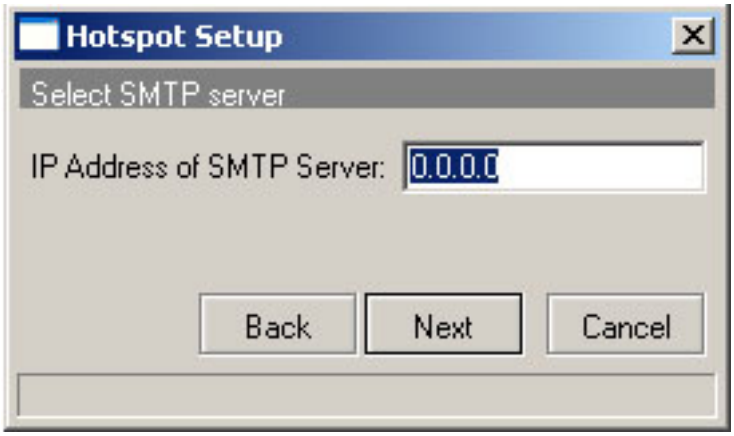
3. **Passo 3 [Set pool for HotSpot address]** o pool é justamente a faixa de ips que estarão disponíveis para os clientes, ele será definido automaticamente a partir do ip e máscara de subrede que você definiu no passo 2. Clique em **next**



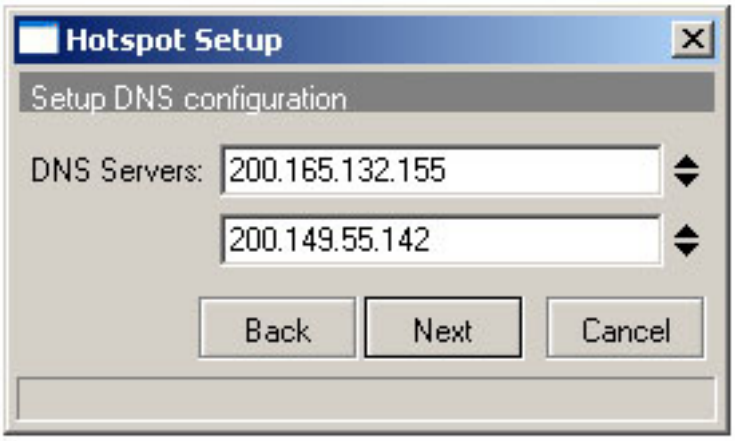
4. **Passo 4 [Select hotspot SSL certificate]**, a certificação digital é uma forma de garantir que o seu sistema é seguro para os usuários, o sistema mikrotik trabalha com certificação digital. Como não trabalharemos com certificação digital deixe esta opção em **none** e clique em **next.**



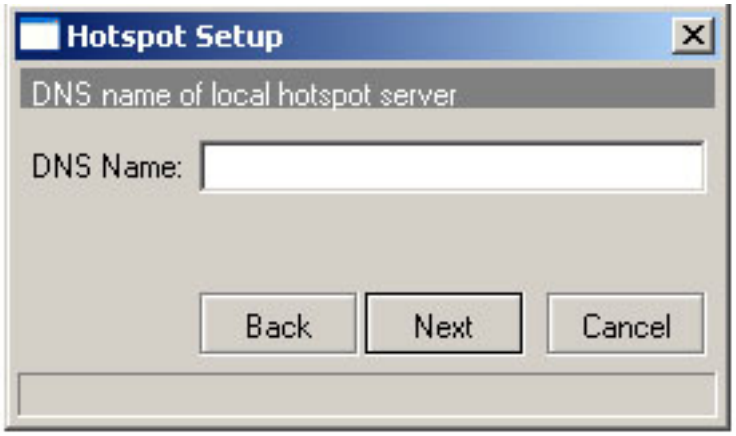
5. **Passo 5 [Select SMTP server],** essa configuração não abortará serviços de SMTP, por tanto deixe o ip em 0.0.0.0 e clique em next.



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



7. **Passo 7 [DNS name of local hotspot server]** – deixe em branco e clique em **next**



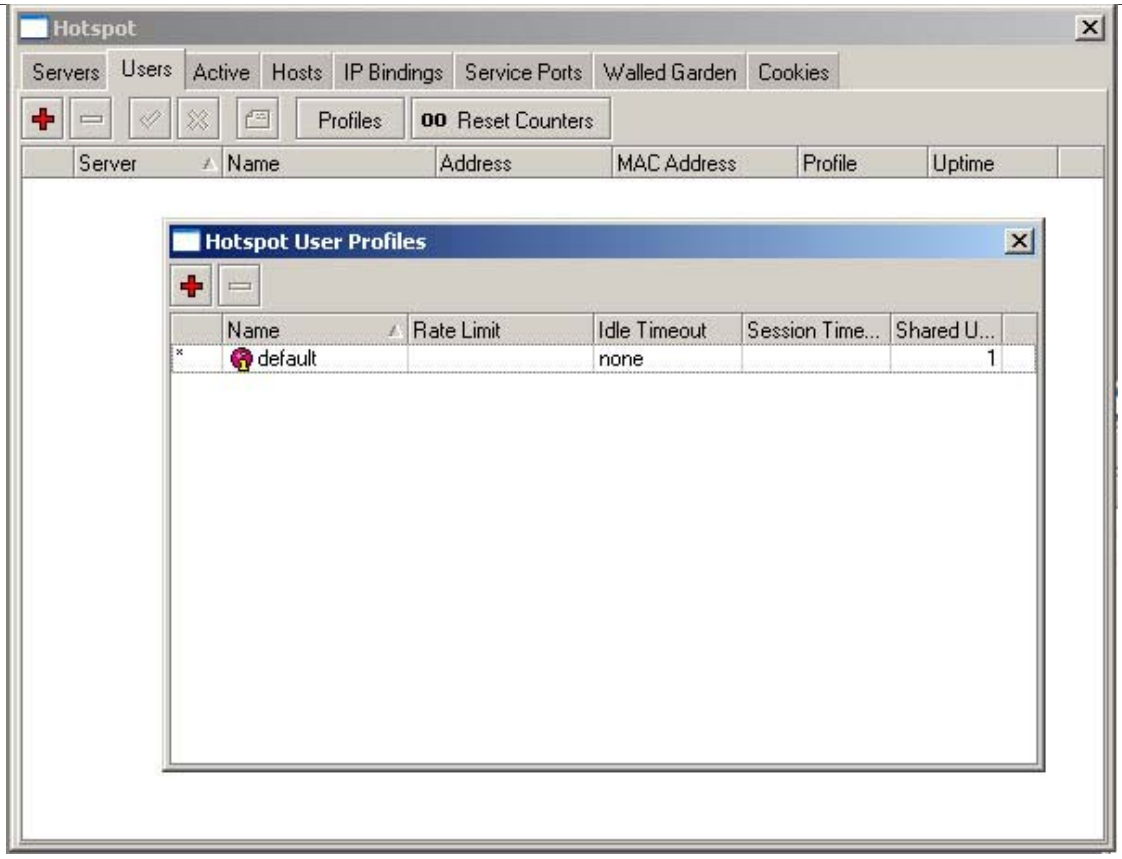
8. **Passo 8 [Create local HotSpot user]** – deixe em branco e clique em next para finalizarmos a configuração do hotspot.

Criando Perfis (limitação de banda)

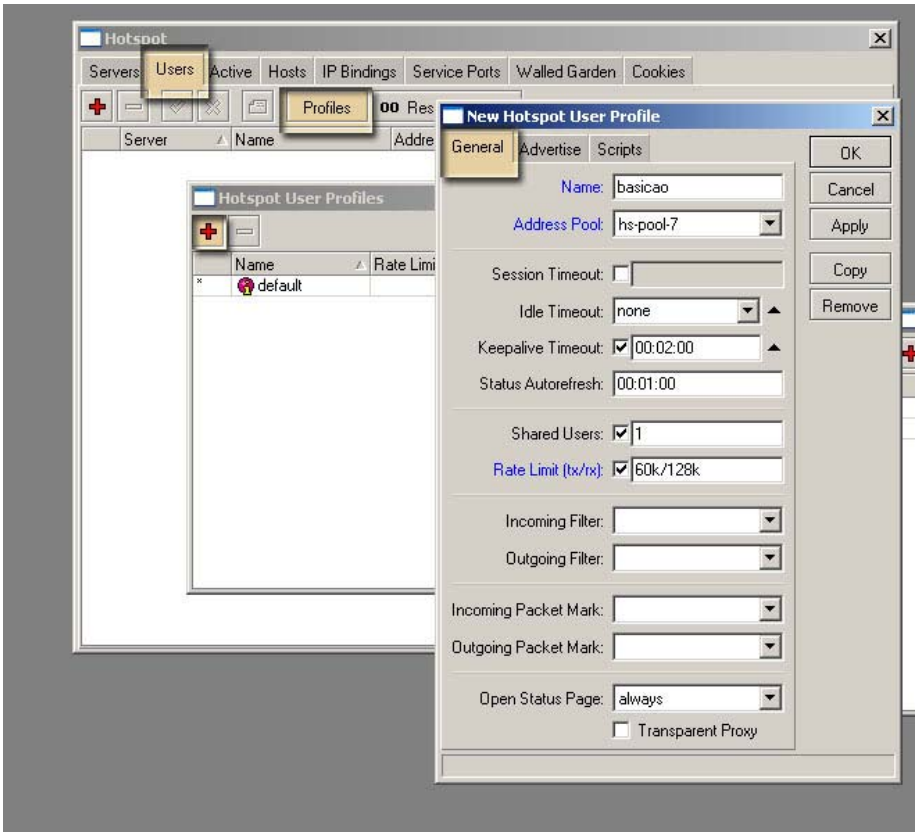
Os perfis no hotspot define como um grupo que será destinado aquele perfil vai acessar a internet exemplo.
Seu ISP vai fornecer dois tipos de acesso um básico de 128k/64k e um avançado de 256k/64k, cada cliente que aderir a sua empresa escolherá um plano e você atribuirá

àquele cliente o perfil que ele caracteriza o plano escolhido.

Criando um perfil.

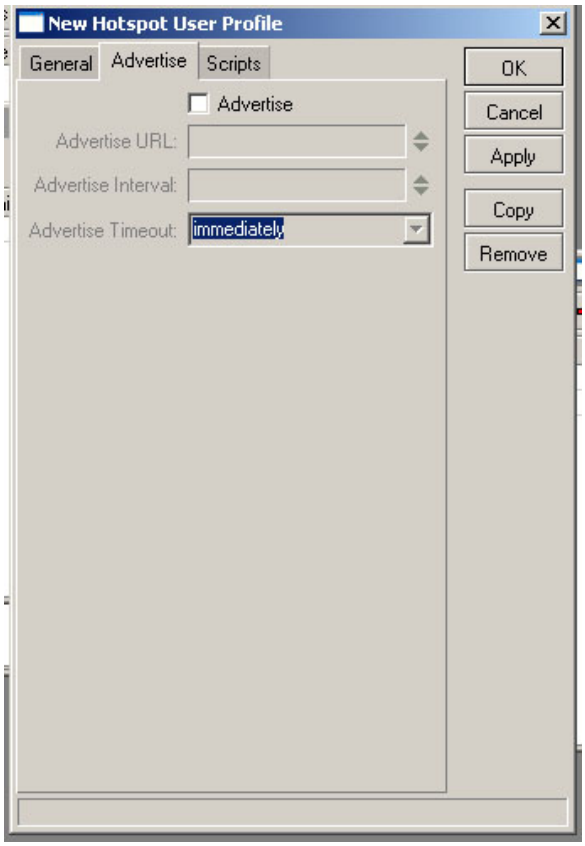


1. No menu **Hotspot** vá para a aba **Users** e clique em **profile**.
2. Dentro de **Hotspot User Profile** clique no sinal "**+**" para criarmos um novo profile



3. **Aba General**
    1. **Name** – o nome do seu plano ou como você quiser chamar
    2. **address pool** – coloque o pool criado no processo de configuração do hotspot, provavelmente só haverá um pool.
    3. **Session Timeout** – Tempo permitido para o cliente quando inspirado ele é derrubado pelo sistema.
    4. **Idle Timeout** – tempo para sistema em espera, deixe em none
    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. A configuração deve ser velocidade de transmissão / velocidade de recepçã ou seja upload/download e as velocidades serão definidas em k colocando no final da velocidade. Ex: 128k/256k 128 kbps para upload e 256 kbps para download.

4. **Aba advertise** Pronto aqui você configurou o básico do perfil e já poderá adicionar novos usuários, o que veremos a seguir não é necessário configurar apenas ficará como explicação.
   Essa função é muito interessante, 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.



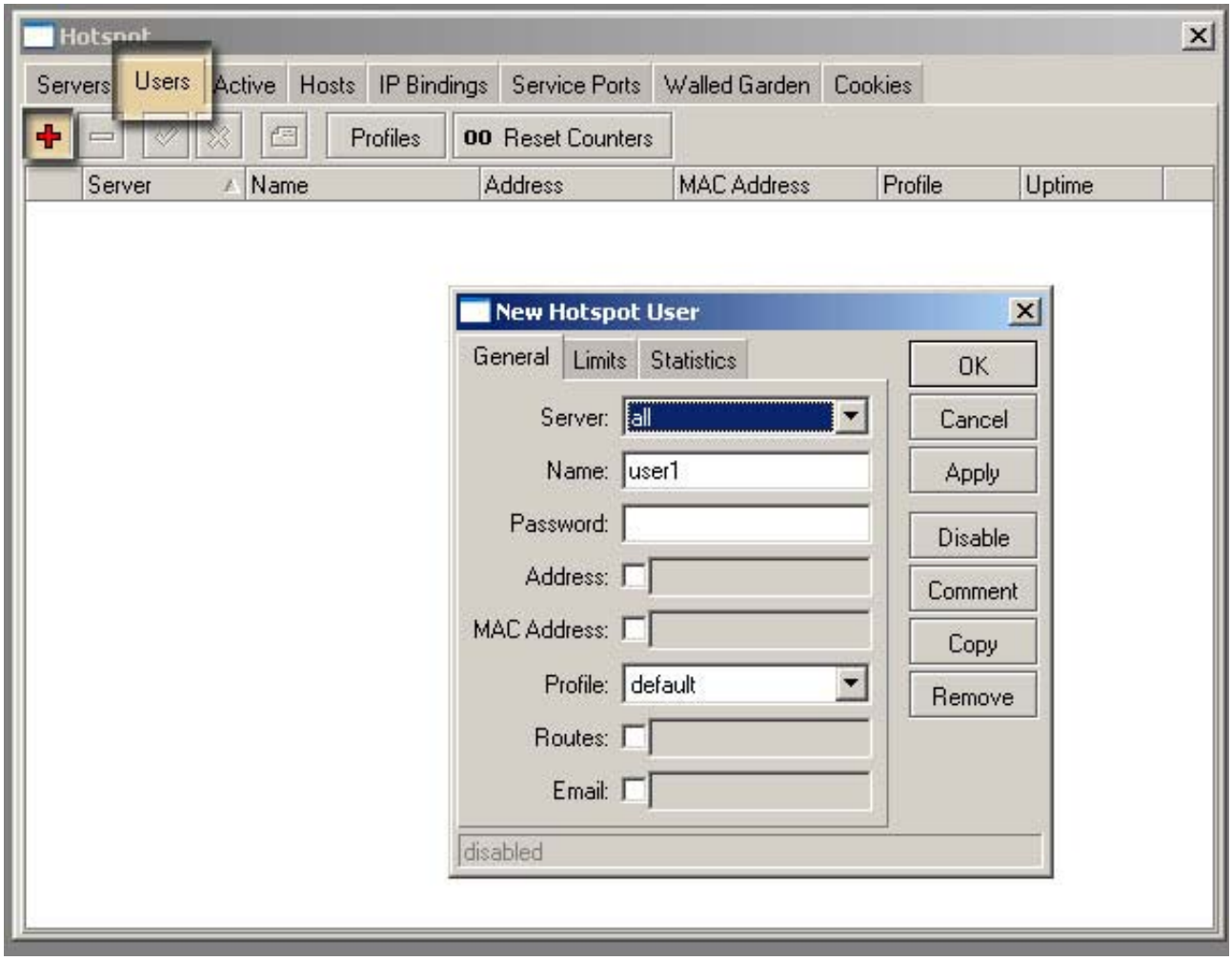
    1. **Advertise URL** – página que será exibida para o cliente poderá ser mais de uma seguindo uma sequência.
    2. **Advertise Interval** – Intervalo para exibição do pop-up.

3. **Advertise Timeout** – advertência para bloqueio de suário.

5. Ok configuramos o perfil você poderá inserir quantos perfis quiser conforme seu ISP, antão clique em **apply** e depois em **Ok.**

Administrando 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

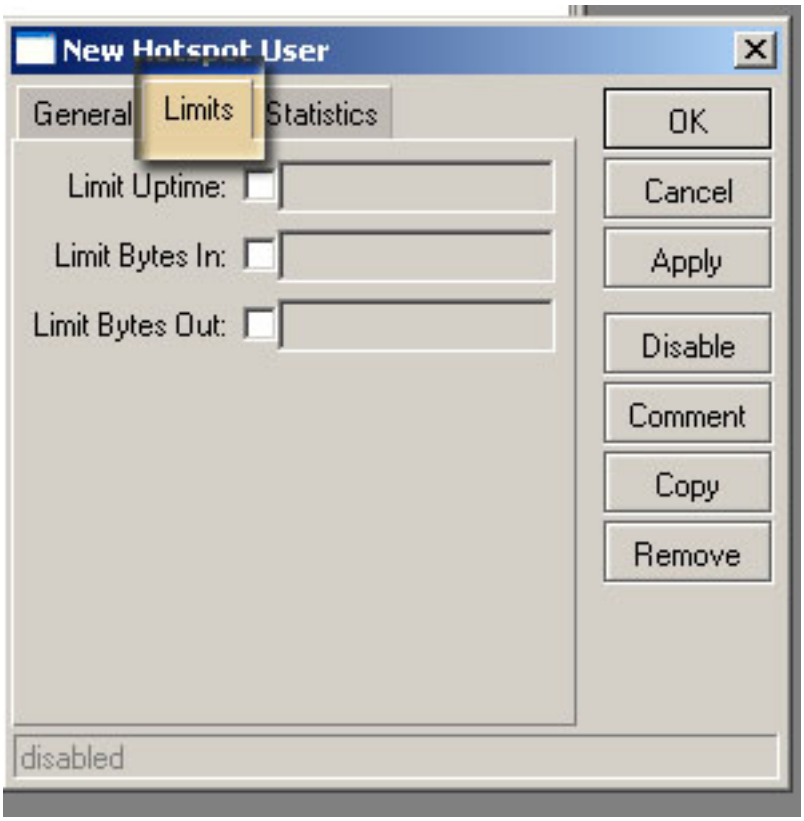
1. Server – escolha o servidor hotspot que criamos ou pode deixar em all
2. Name – nome do usuário, ele se logará com o nome que você definir aqui
3. Password – senha para o name você poderá deixar em branco ou poderá preencher e repassar para o seu cliente.
4. Address – não marque essa opção deixe que o mikrotik atribua automaticamente um ip para o seu cliente.
5. MAC Address – caso você tenha o mac do seu cliente você poderá adicionar amarrando o mac ao login. Desta forma fica quase impossível mais de uma pessoa

se logar com o mesmo Name ou o mesmo MAC, pois em share user dentro de profile nos configuramos apenas para um usuário se lembra?

6. Profile – escolha o profile que você acabou de criar, de acordo com o plano do seu cliente.
7. Routes - deixe em branco – define uma rota especifica para o cliente
8. e-mail - deixe em branco – coloca o email do cliente

Aba Limits

Aqui você tem mais uma opção de serviço para seus clientes, você poderá estabelecer um contrato mensal de dados trafegados assim como poderá limitar o tempo de uso dos seus clientes. Um serviço interessante caso queira criar pacotes pré-pagos ou ou oferecer um serviço de teste para um futuro cliente.



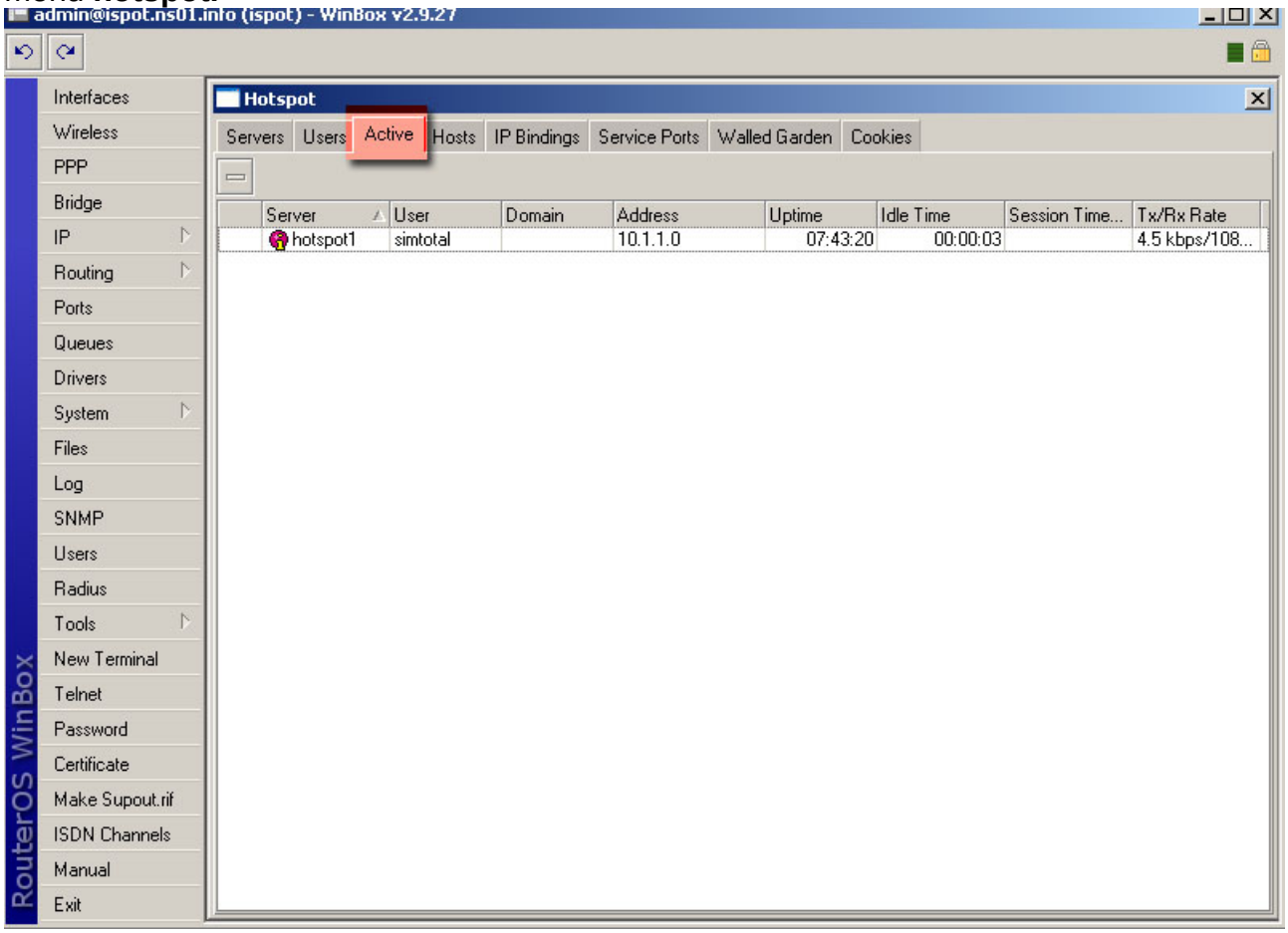
1. Limit Uptime – limita o tempo de conexão do seu cliente
2. Limit Bytes In – Limita quanto seu cliente poderá dar de upload
3. Limit Bytes Out – Limita quanto seu cliente poderá download

Pronto com seu cliente já poderá navegar no seu sistema, a criação de contas de usuários no mikrotik é bastante prático e intuitivo, agora vamos ver e administrar quem está conectado.

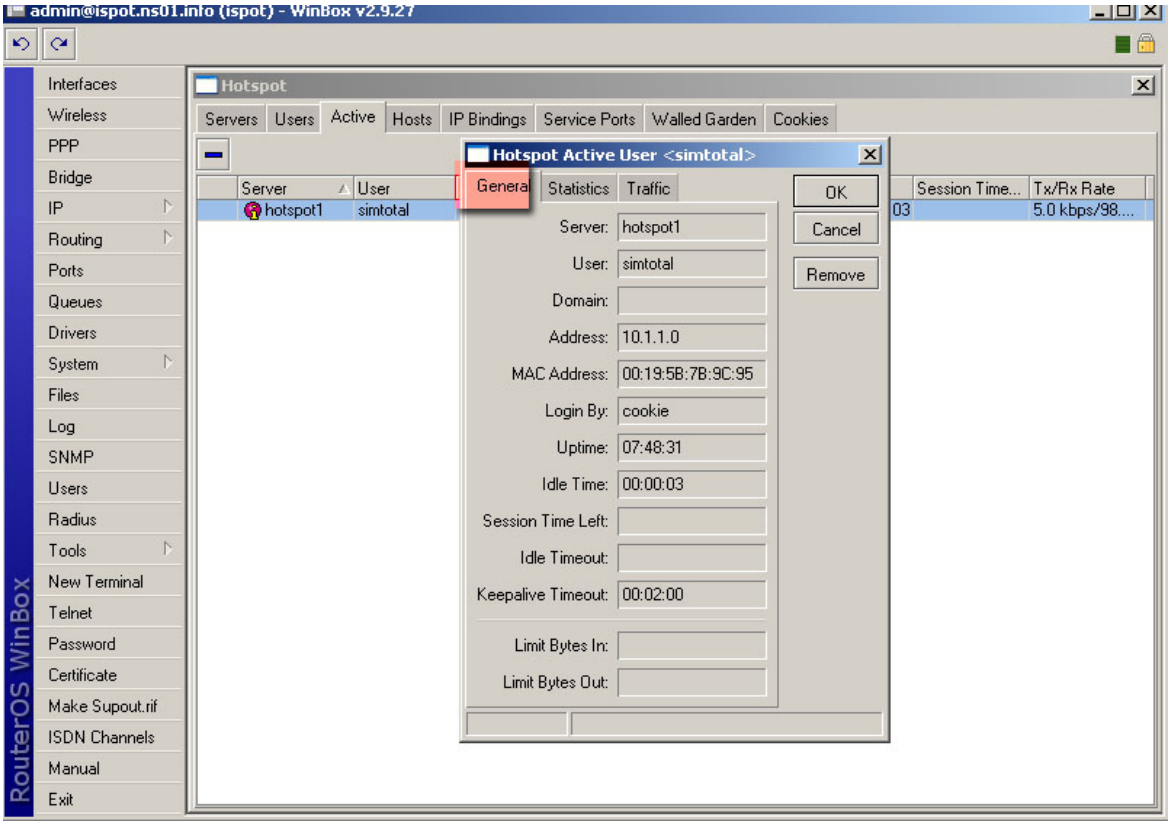
Quem está conectado?

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.



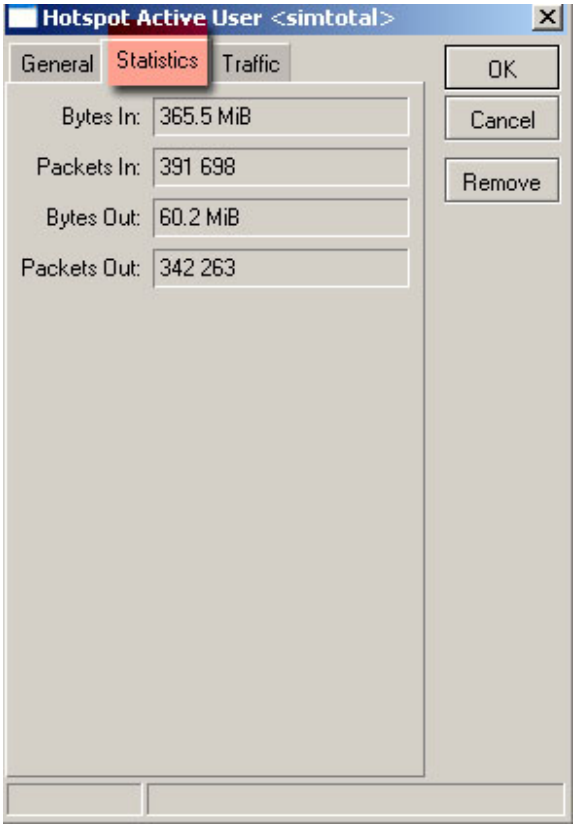
Se você der dois cliques no cliente você terá:

Aba General

1. Server – servidor hotspot que ele está conectado.
2. User – nome do usuário conectado.
3. Address – endereço atribuído para este cliente.
4. MAC Address – Endereço físico da placa wireless do cliente (casso você ainda não tenha o mac do cliente você poderá copiar e colar o endereço quando ele estiver online)
5. Login By – define como o cliente se logou. O mikrotik deixa um cook nos computadores dos clientes não exigindo que ele digite toda vez que for acessar a internet seu login e senha, o tempo de expiração assim como a possibilidade de não ter o cook poderão ser configurados.
6. Uptime – tempo de conexão
7. Idle Time – tempo ocioso sem atividade

Aba Statistic

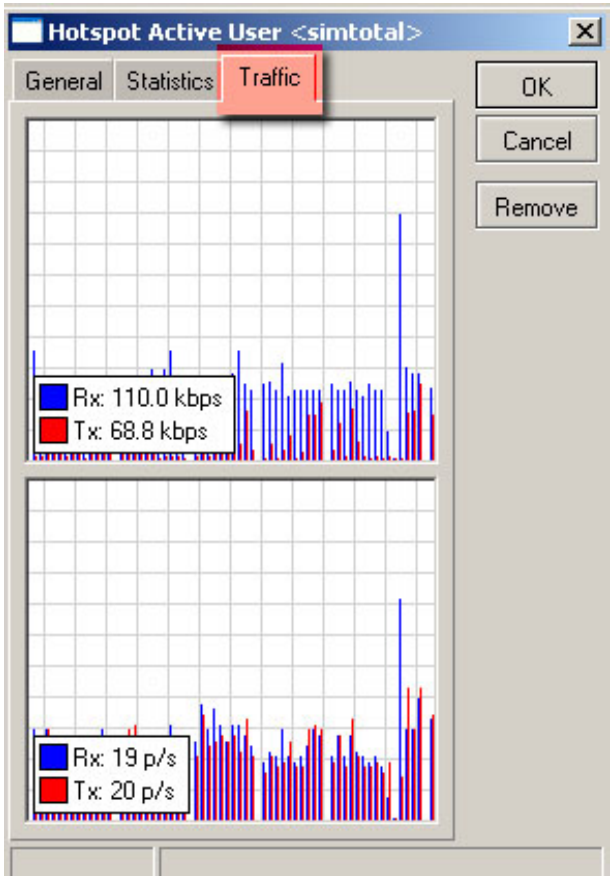
A aba statistics mostrará o tráfego geral do cliente selecionado.



1. Bytes In – bytes recebidos pelo servidor upload do cliente
2. Bytes Out – bytes enviados para o servidor download do cliente

Aba Trafic

A aba trafic mostra o uso atual do link pelo cliente selecionado em um gráfico.
A parte de cima do grafico mostra a quantidade de bytes por segundo quanto que o gráfico de baixo mostra pacotes por segundo.

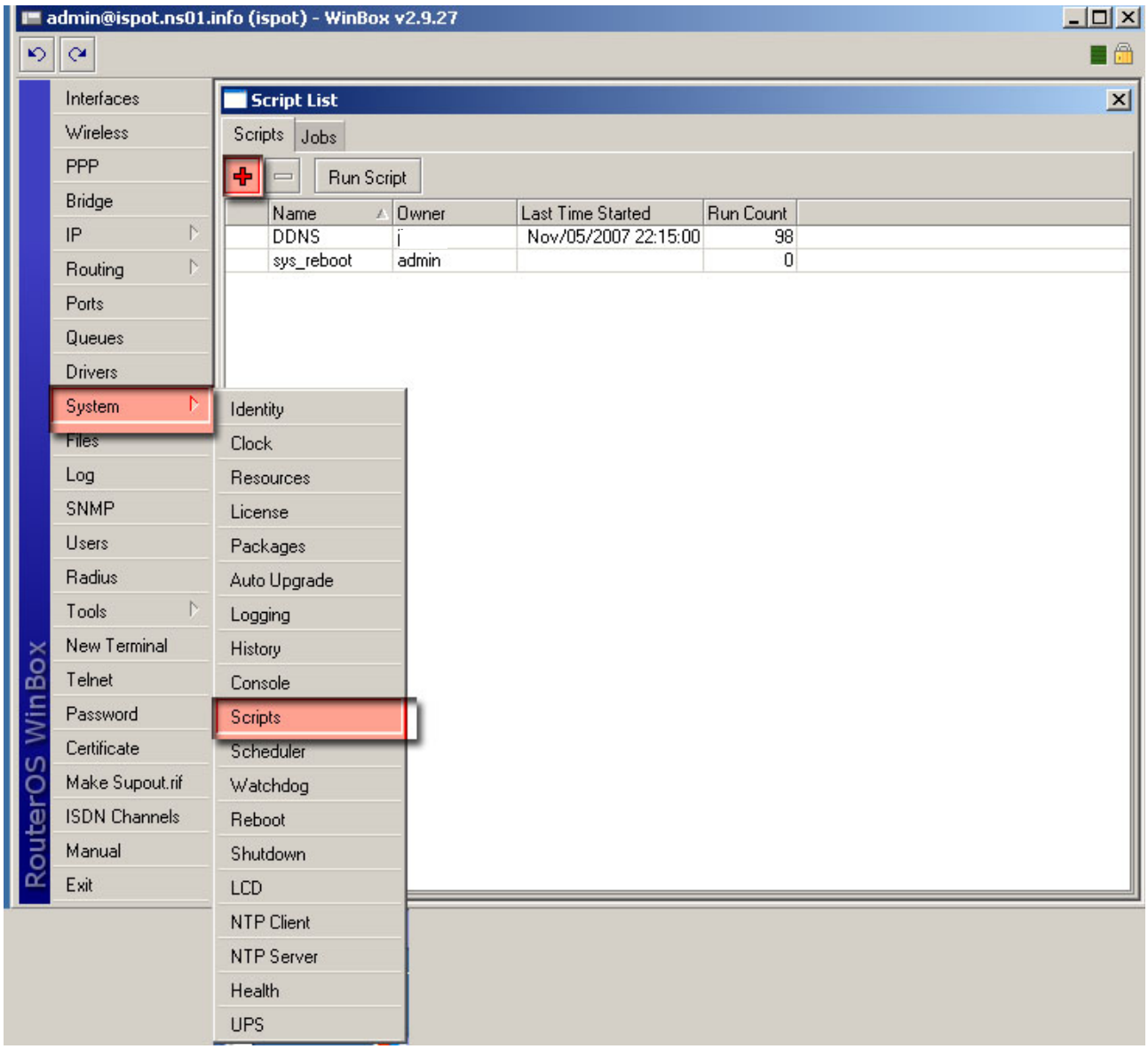


Acessando Remotamente

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/ eles oferecem servidor ddns gratuito.

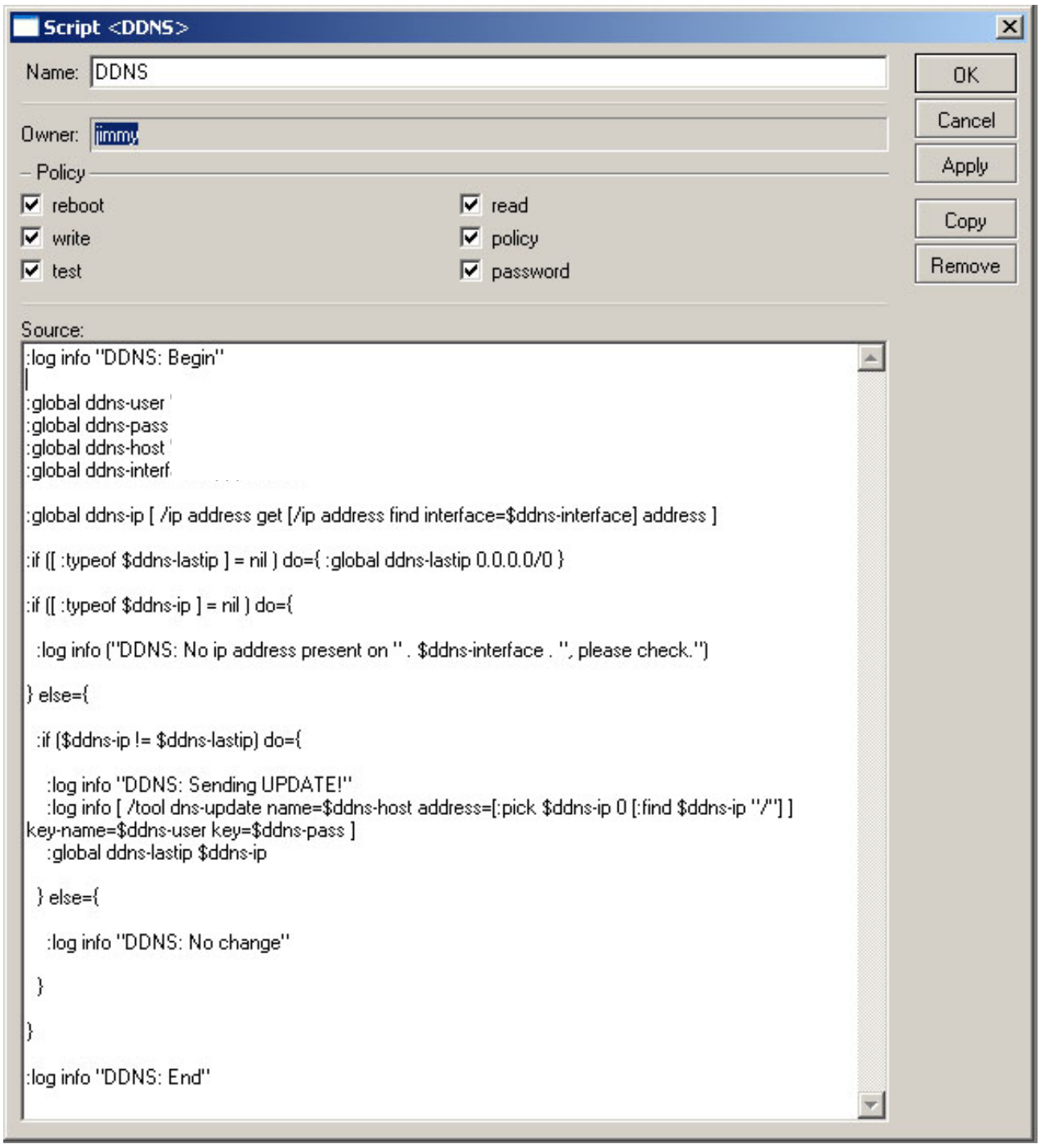
Após realizar o cadastro iremos configurar um script para que o mikrotik atualize o ip atual no servidor ddns.

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 abaixo


Script <DDNS>
Name: DDNS
Owner: jimmy
Policy
reboot
write
test
read
policy
password
OK
Cancel
Apply
Copy
Remove
Source:
:log info "DDNS: Begin"
:global ddns-user
:global ddns-pass
:global ddns-host
:global ddns-interf
:global ddns-ip [/ip address get [/ip address find interface=$ddns-interface] address]
:if ([:typeof $ddns-lastip] = nil) do={ :global ddns-lastip 0.0.0.0/0 }
:if ([:typeof $ddns-ip] = nil) do={
:log info ("DDNS: No ip address present on " . $ddns-interface . ", please check.")
} else={
:if ($ddns-ip != $ddns-lastip) do={
:log info "DDNS: Sending UPDATE!"
:log info [/tool dns-update name=$ddns-host address=[:pick $ddns-ip 0 [:find $ddns-ip "/"]]
key-name=$ddns-user key=$ddns-pass]
:global ddns-lastip $ddns-ip
} else={
:log info "DDNS: No change"
}
}
:log info "DDNS: End"

Para adiconar o script copie o texto abaixo e cole na tela do script como na figura mudando apenas os dados que estão em negrito

---

```
:log info "DDNS: Begin"

:global ddns-user "nome do seu usuário no change ip"
:global ddns-pass "senha do seu usuário no change ip"
:global ddns-host "seu endereço no changeip"
:global ddns-interface "pppoe-out1"

:global ddns-ip [ /ip address get [/ip address find interface=$ddns-interface] address ]

:if ([ :typeof $ddns-lastip ] = nil ) do={ :global ddns-lastip 0.0.0.0/0 }

:if ([ :typeof $ddns-ip ] = nil ) do={

  :log info ("DDNS: No ip address present on " . $ddns-interface . ", please check.")

} else={

  :if ($ddns-ip != $ddns-lastip) do={

    :log info "DDNS: Sending UPDATE!"
    :log info [ /tool dns-update name=$ddns-host address=[:pick $ddns-ip 0 [:find $ddns-ip "/"] ] key-
name=$ddns-user key=$ddns-pass ]
    :global ddns-lastip $ddns-ip

  } else={

    :log info "DDNS: No change"

  }

}

:log info "DDNS: End"
```

Explicando os campos em negrito:

Quando você cria um usuário no chande ip geralmente o nome do seu usuário será seu endereço DDNS.

Iremos simular uma conta de nome usuario e senha 1234 então as configurações ficariam assim:

:global ddns-user "usuario"
:global ddns-pass "1234"
:global ddns-host "usuario.ns01.info" (neste caso o domínio que escolhi foi o ns01.info, você terá outras opções de domínio quando for criar sua conta no changeip)
:global ddns-interface "pppoe-out1" (aqui colocamos a interface PPPOE que faz a conexão com a internet)

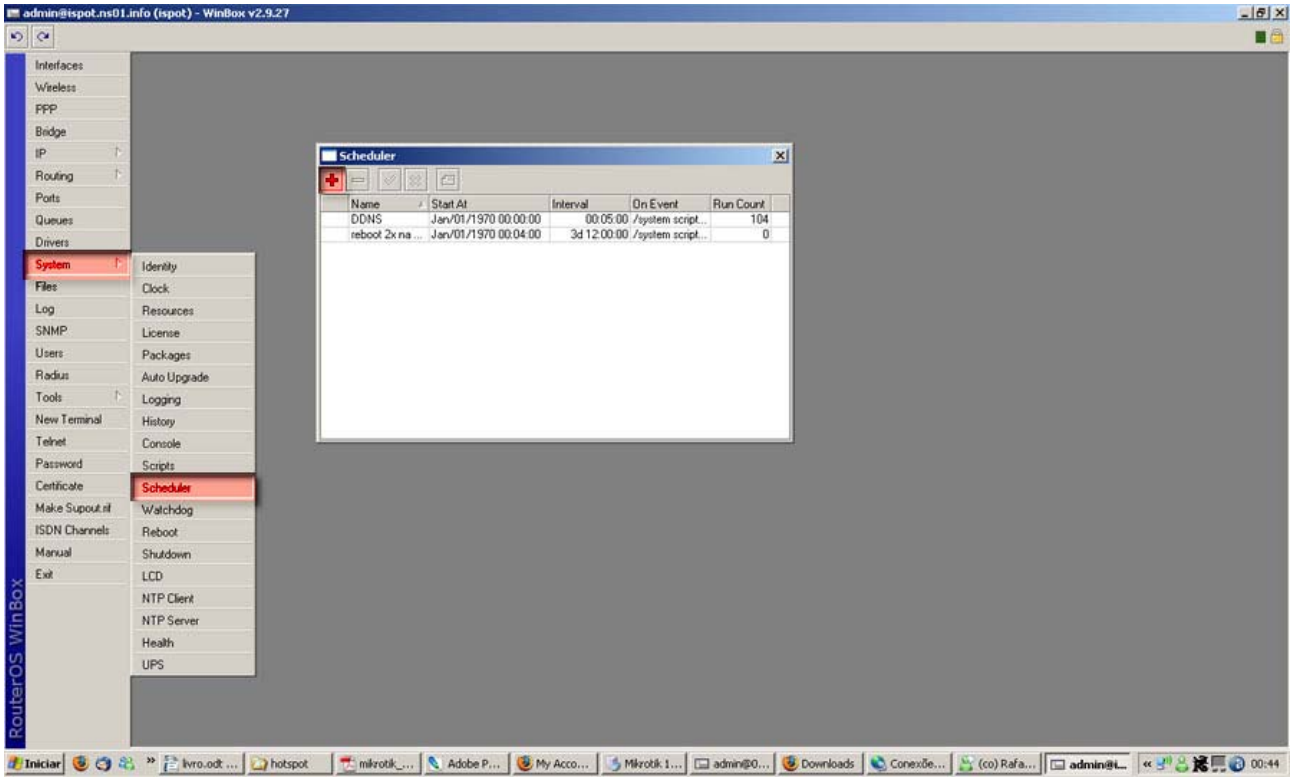
Criamos o script que estará atualizando o servidor ddns com o ip do adsl uma vez que este ip é dinâmico. Clique em apply e depois em ok.

Para rodar o Script basta clicar em Run ao lado do sinal (+), porém como não estaremos sempre na frente do computador faremos com que o mikrotik rode esse script

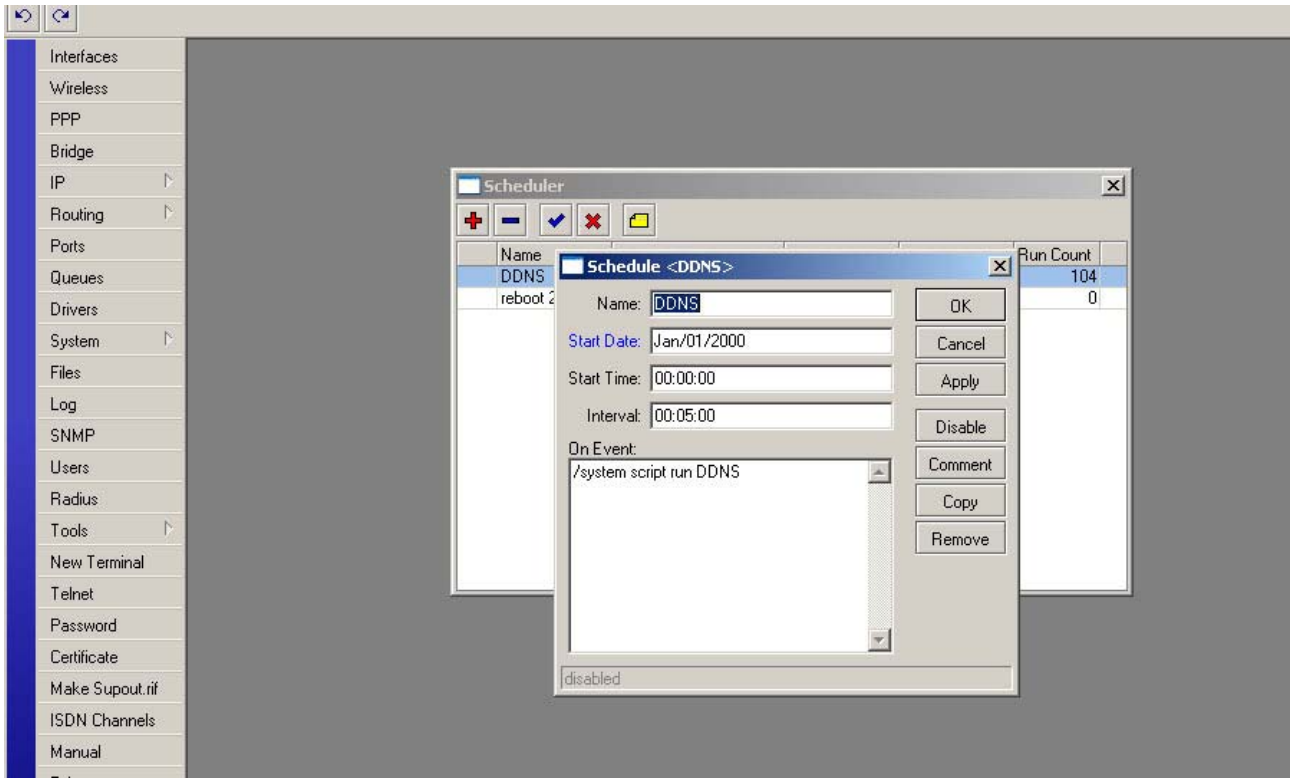
automaticamente.

Automatizando o script

Vá para o menu **system, scheduler** e clique no sinal de **“+”** para adicionarmos um novo agendamento de tarefa.



Em schedule configure da seguinte forma:



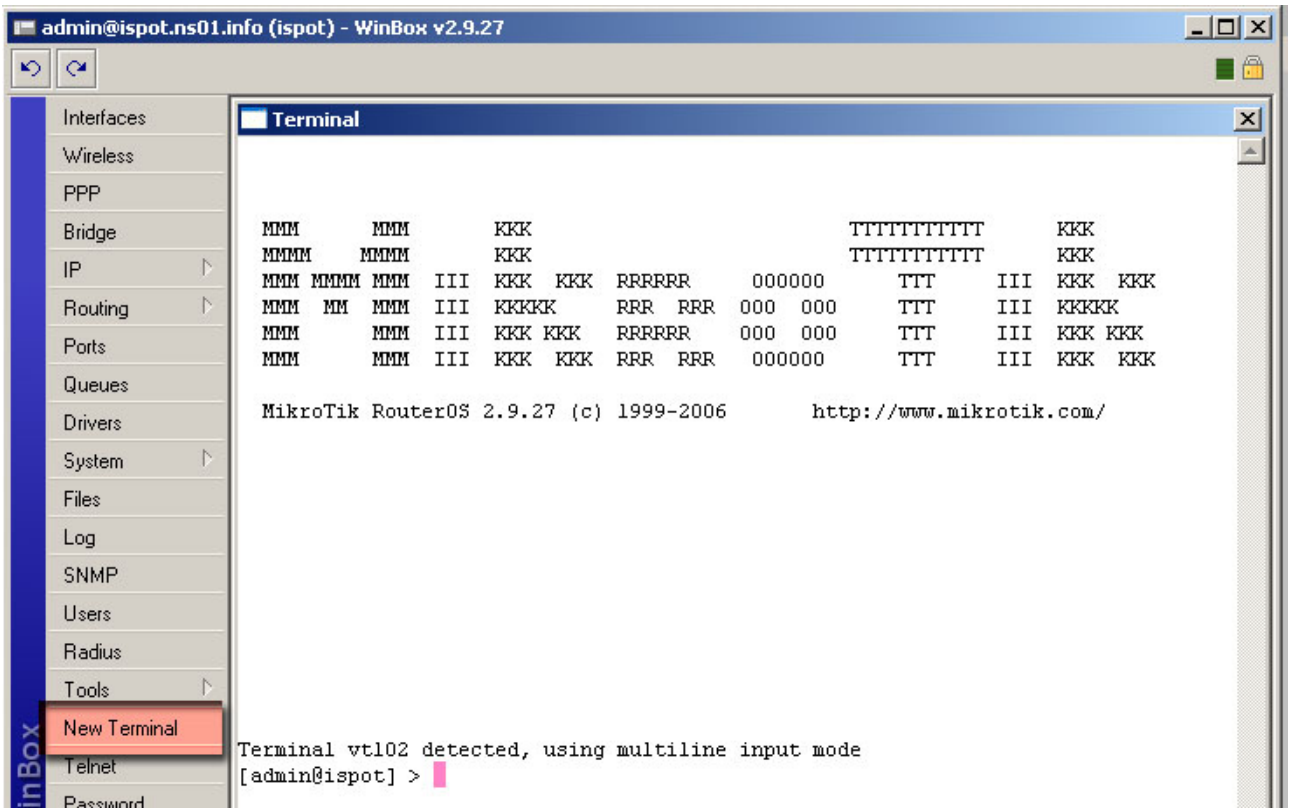
1. Name – coloque um nome para o seu agendamento ao seu gosto
2. Start Date – dia que o agendamento começará a rodar , coloque um dia antes ao dia atual, recomendo que veja se a data e hora do seu sistema estão corretos, para isso basta cessar o menu **system** e o submenu **clock.**
3. Start Time – hora que iniciará o agendamento, coloque 00:00:00 para começar imediatamente.
4. Interval – intervalo que o script ira rodar, colocaremos de 5 em 5 minutos para que tenhamos sempre o ddsn atualizado coloque 00:05:00.
5. em on event escreva (/system script run DDNS) o DDS é o nome que demos ao script anteriormente se lebra? Caso não se lembre o nome que deu volte para o menu script e reveja.
6. Clique em **aply**, **enable** e **ok**.

Agora basta você acessar o winbox com o nome do seu domínio, ex: usuario.ns01.info logando ao sistema de qualquer canto do planeta.

Firewall

O Firewall do mikrotik será realizado através de regras próprias, o nível de otimização é quase infinito, você poderá bloquear qualquer tipo de acesso ao mikrotik.

Para facilitar a inserção de todas as regras você poderá inserir tudo via terminal para isso acesse Menu New Terminal



Quando acessamos um terminal é a mesma coisa do console de comando inicial se lembra? Aquela tela preta com letras em branco que aparece logo depois de instalar o Mikrotik. Mais agora temos a vantagem de estar operando em ambiente gráfico e podemos copiar as linhas de comando e colar, muitos tutoriais que você encontrará na

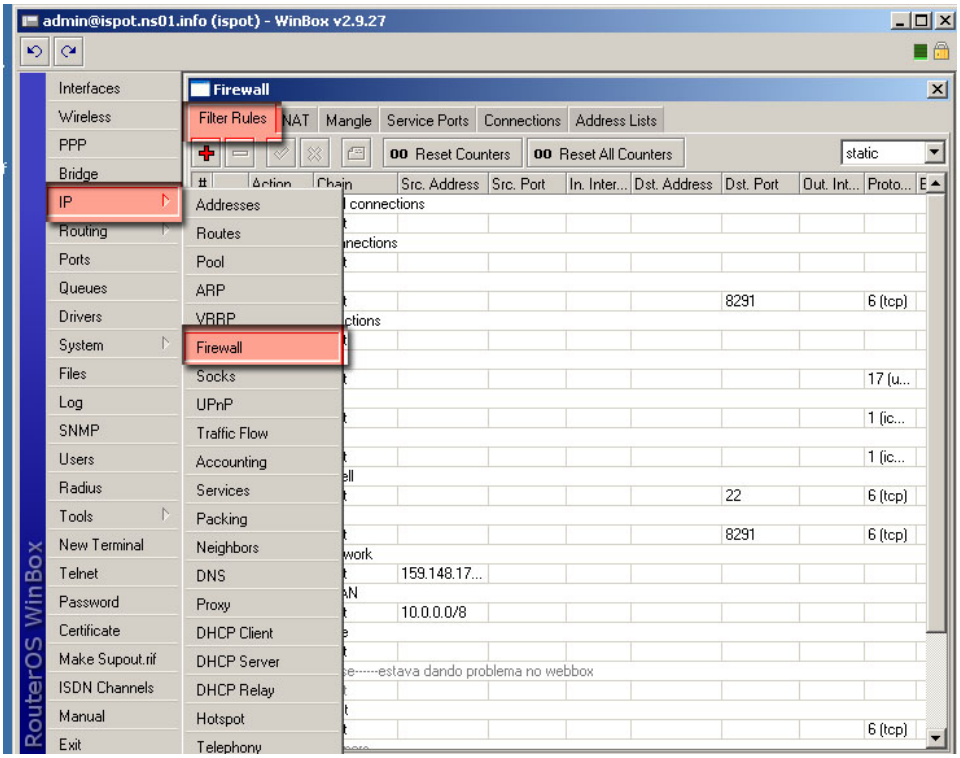
internet ofereceram essa forma de você trabalhar.

Copie todas as regras de Firewall aqui e cole no terminal, clicando com o botão direito sobre a tela do mesmo e clicando na opção past.

```
/ ip firewall filter
add chain=input connection-state=established comment="Accept established connections"
add chain=input connection-state=related comment="Accept related connections"
add chain=input connection-state=invalid action=drop comment="Drop invalid connections"
add chain=input protocol=udp action=accept comment="UDP" disabled=no
add chain=input protocol=icmp limit=50/5s,2 comment="Allow limited pings"
add chain=input protocol=icmp action=drop comment="Drop excess pings"
add chain=input protocol=tcp dst-port=22 comment="SSH for secure shell"
add chain=input protocol=tcp dst-port=8291 comment="winbox"
add chain=input action=log log-prefix="DROP INPUT" comment="Log everything else"
```

Explicando um pouco cada item.

Observe que o comando na primeira linha (/ ip firewall filter) fazendo uma analogia com a parte gráfica é a mesma coisa de menu **IP** depois submenu **Firewall** e depois ele entra na Aba **Filter** Rules.



Cada linha que começa com o nome add chain significa que você está clicando no sinal “+” então vamos explicar cada item.

1. Linha 2 Accept established connections – toda entrada de conexão estabelecida serão aceitas.
2. Linha 3 Accept related connections – Toda entrada de conexões relatadas serão

aceitas.

3. Linha 4 Drop invalid connections – toda entrada que não estiver na opção anterior serão expulsas.
4. Linha 5 UDP – entrada de protocolo UDP serão aceitas
5. Linha 6 Allow limited pings – entrada de protocolo ICMP com ping em no máximo 50/5s,2
6. Linha 7 Drop excess pings – Ping com ping alto serão dropados superior ao valor citado na linha acima
7. Linha 8 SSH for secure shell – permite conexão SSH para porta 22
8. Linha 9 Winbox – permite a entrada do winbox
9. As ultimas linhas abaixo refere-se a banir ações como Bruteforce, ele expulsa possíveis invasores que usam boot para ficar enviando login e senha na tentativa de acerto e insão no seu sistema.

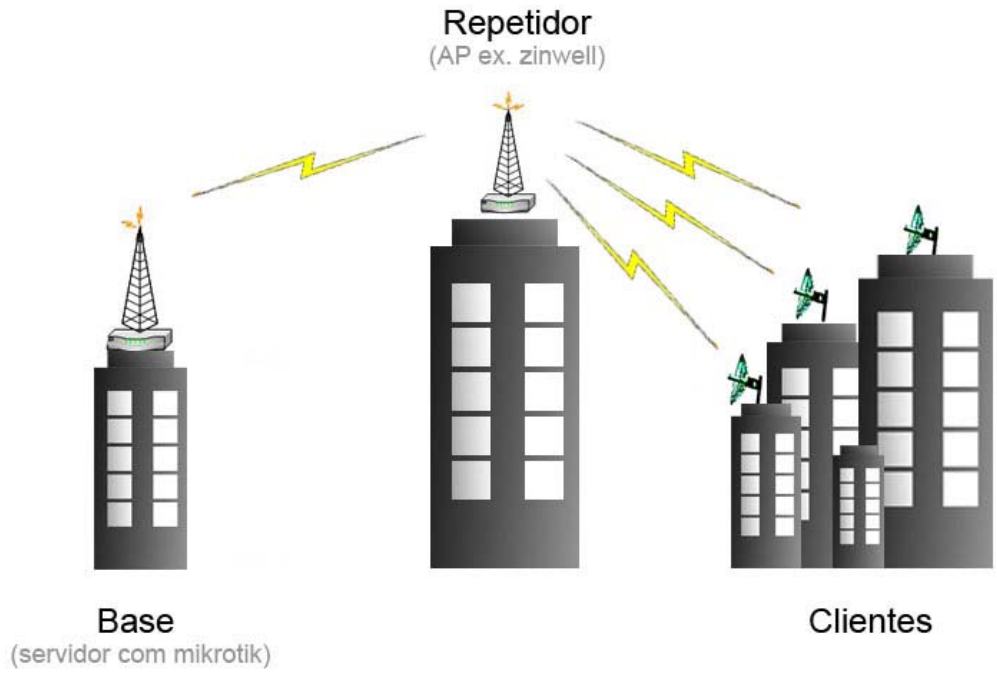
```
add chain=input protocol=tcp dst-port=22 src-address-list=black_list action=drop comment="drop ssh brute forcers" disabled=no
add chain=input protocol=tcp dst-port=22 connection-state=new src-address-list=ssh_stage3 action=add-src-to-address-list address-list=black_list address-list-timeout=1d comment="" disabled=no
add chain=input protocol=tcp dst-port=22 connection-state=new src-address-list=ssh_stage2 action=add-src-to-address-list address-list=ssh_stage3 address-list-timeout=1m comment="" disabled=no
add chain=input protocol=tcp dst-port=22 connection-state=new src-address-list=ssh_stage1 action=add-src-to-address-list address-list=ssh_stage2 address-list-timeout=1m comment="" disabled=no
add chain=input protocol=tcp dst-port=22 connection-state=new action=add-src-to-address-list address-list=ssh_stage1 address-list-timeout=1m comment="" disabled=no
```

WDS – Repetindo seu sinal

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 o sinal da sua base.

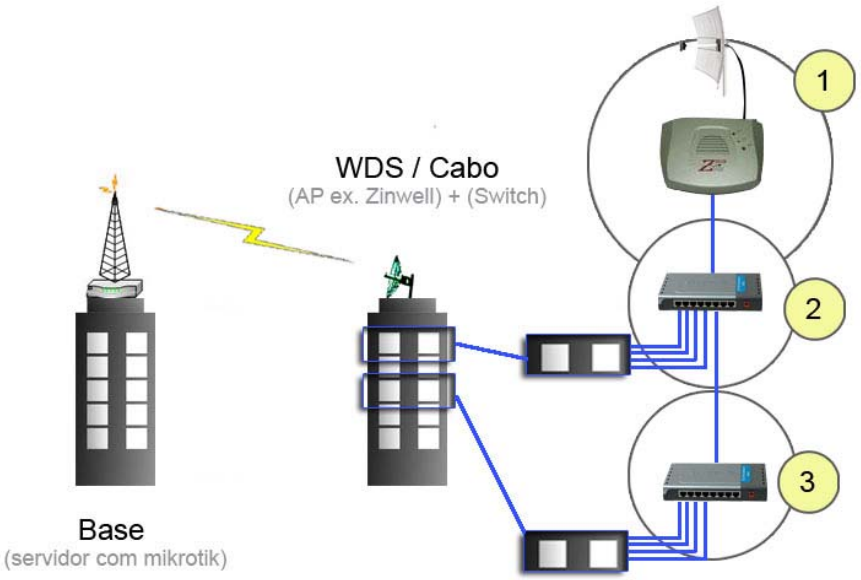
As possibilidades do WDS são muitas veja três exemplos a seguir:

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



base e repetir para a área não coberta.

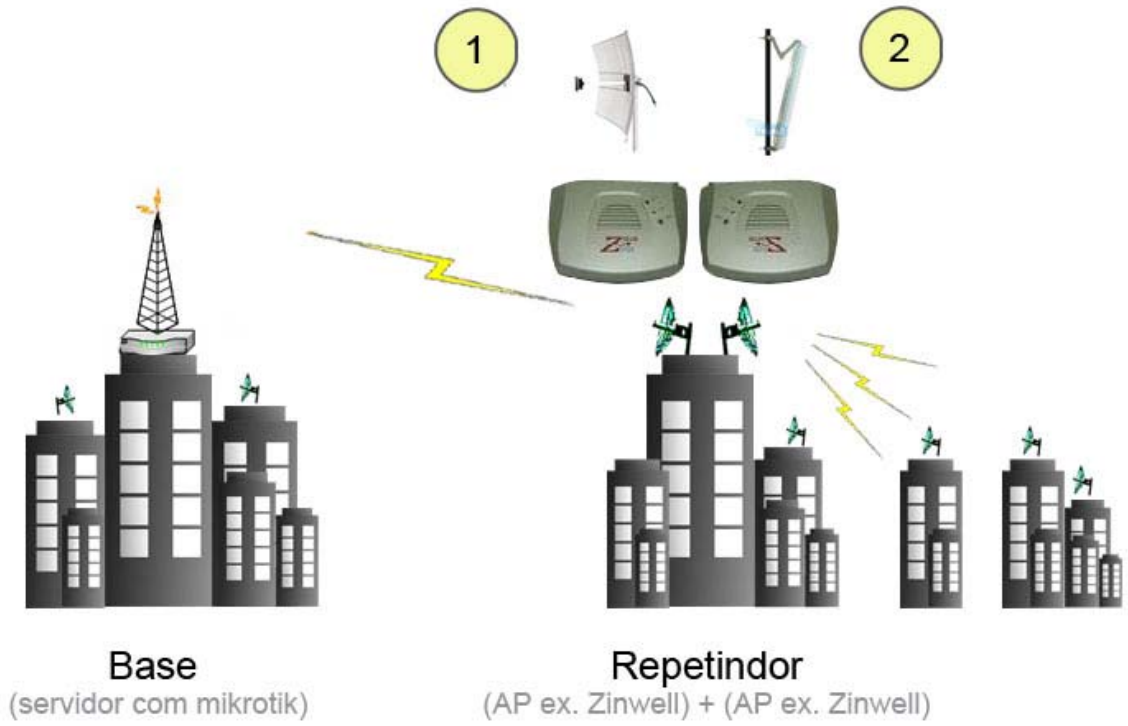
2. Em alguns casos você disponibilizará o serviço de internet para edifícios, como o sistema WI-FI não foi projetado para ultrapassar barreiras você não poderá cobrir todas as residências via wireless, então você usará um AP para receber o sinal de rádio e repassar para os usuários via cabo utilizando 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 Ziwell g120.
2. O AP Zinwell repassa o link via cabo para um Switch de 8 portas que estará no ultimo andar do edifício, repassando para os moradores e descendo mais um cabo para o penúltimo andar.
3. Mais um Switch receberá o sinal via cabo do Swtch do apartamento superior e repassará para os moradores deste andar, descendo mais um cabo pro andar inferior e mais um switch, repetindo o procedimento para todos os andares.

3. Realizar elances a grandes distâncias, este procedimento é indicado quando você quer repetir o sinal em um local distante da sua base levando sua internet a locais distântes.



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 Splintter (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.

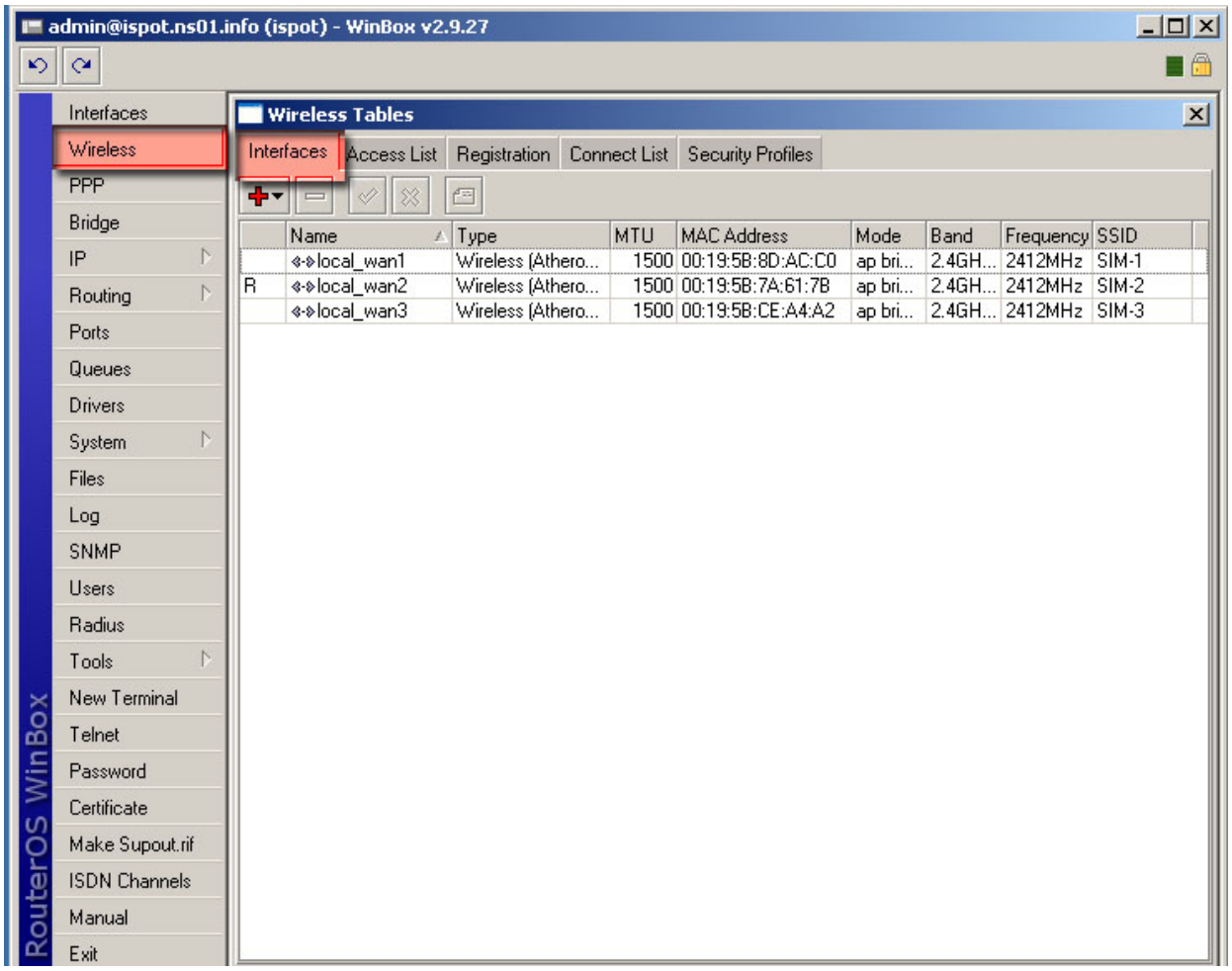
Configurando o WDS no Mikrotik e no AP

Como nós já vimos a utilização do WDS agora só resta fazer as configurações do mikrotik e dos Aps.

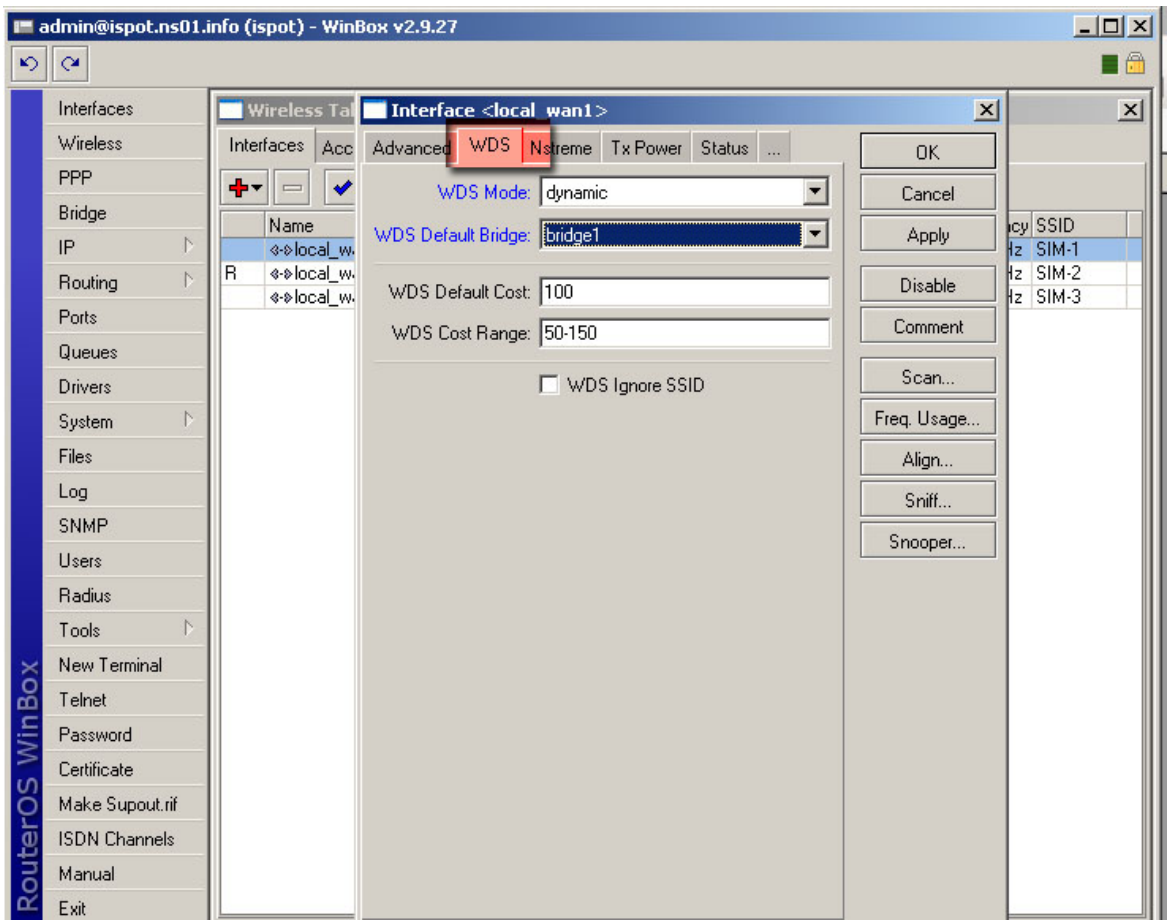
Mikrotik:

Configurando o Mikrotik para trabalhar em WDS

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.



3. Na interface selecionada vá para aba WDS e configure da seguinte maneira:
    1. **WDS Mode -** em WDS mode você terá dois modos de operação, o Dynamic e o Static, o primeiro modo fará o WDS dinâmico ou seja ele se comunicará com qualquer AP que estiver configurado para receber o sinal do seu Mikrotik, quanto que o Static você terá que adicionar manualmente os AP's que se comunicarão com sua base. Desta forma trabalharemos com **WDS Dynamic** pois queremos que essa comunicação seja automática 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. Essa função é importante para você especificar links diferentes para determinadas áreas, se você tivesse uma interface ether com um link exclusivo para esta interface você poderia enviar este link para que fosse repetido em outro local.
    3. WDS Defalt Cost – 100
    4. WDS Cost Range- 50-150
    5. WDS Ignore SSID – deixe essa opção marcada

Configurando seu Um AP comum

A configuração do seu AP vai seguir o mesmo passo independente da marca ou modelo, é necessário apenas que ele tenha a função WDS, os testados até então foiram o **Zinwell g120** e o **Edimax EW7209** porém existem outros modelos que aceitam o trabalhar em WDS porém não tem como garantir se irá funcionar.

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 da sua interface wireless 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.

A configuração para o WDS estático você encontrará na pasta de suporte no arquivo Mikrotik detalhado.

Limitando P2P

É fato que os P2P's são as pragas para os provedores, e os usuários destes serviços são considerados os have users aquele cliente que ninguém quer e é obrigado a tê-los.
Neste tópico jogaremos um balde de água fria na diversão deles (deixar o computador 24hs por dia com o e-mule, kazaa, shareaza e afins ligado e consumindo seu link) e o melhor sem que eles saibam.
Existem 1000 maneiras para você informar ao cliente que a culpa do id baixo ou de baixas velocidades em serviços p2p não é culpa do provedor e sim do próprio serviço p2p.
Uma das maneiras é dizer que o serviço p2p depende da quantidade de fontes disponíveis pois sabemos que o p2p é um serviço de toma-la-dá-cá, outra maneira e informar que o governo federal está com o programa anti-pirataria que obriga os provedores a bloquearem as portas para estes serviços, e por fim e desta vez você não estará metindo, você informará que o sistema é protegido por um Firewall Obrigatório para manter a segurança dos clientes na rede e o Firewall bloqueia estes tipos de serviços por serem um antro de vírus.
Enfim use sua criatividade pois você vai precisar no momento em que um have user destes te pentelhar e começar a falar mal do seu serviço, conveça-o a utilizar o serviço de download pelo browser.
Bom como você irá administrar isso vai ser problema seu, apenas dei uma dica de como manter seu sistema funcionando bem para a maioria dos seus clientes que usam a internet para visitar sites, ler e-mails ou até mesmo jogar.

Para a configuração via terminal como vimos anteriormente basta você copiar o código e colar no terminal

```
/ ip firewall mangle
/ip firewall mangle
add chain=prerouting p2p=all-p2p action=mark-connection
new-connection-mark=conexao-p2p passthrough=yes comment="CONTROLE DO P2P" disabled=no
add chain=prerouting connection-mark=conexao-p2p action=mark-packet new-packet-mark=pacotes-p2p
passthrough=yes comment="" disabled=no
add chain=prerouting p2p=all-p2p action=mark-routing new-routing-mark=p2p passthrough=no comment=""
disabled=no

/ip firewall filter
add chain=forward p2p=all-p2p src-address-list=!p2p-sem-bloqueio action=drop comment="BLOQUEIO DO
P2P" disabled=yes

/ queue tree
add name="\[P2P\] - Download" parent=global-in packet-mark=pacotes-p2p limit-at=0 queue=default
priority=8 max-limit=64000 burst-limit=0 burst-threshold=0 burst-time=0s disabled=no
add name="\[P2P\] - Upload" parent=global-out packet-mark=pacotes-p2p limit-at=0 queue=default
priority=8 max-limit=64000 burst-limit=0 burst-threshold=0 burst-time=0s disabled=no

/ system script
add name="liberar-p2p" source="/ip firewall filter disable \[/ip firewall filter find p2p=all-p2p\]" \
policy=ftp,reboot,read,write,policy,test,winbox
add name="bloquear-p2p" source="/ip firewall filter enable \[/ip firewall filter find p2p=all-p2p\]" \
policy=ftp,reboot,read,write,policy,test,winbox

/ system scheduler
add name="bloquear-p2p" on-event=bloquear-p2p start-date=aug/31/2007 start-time=08:00:00 interval=1d
comment="" disabled=no
add name="liberar-p2p" on-event=liberar-p2p start-date=aug/31/2007 start-time=21:00:00 interval=1d
comment="" disabled=no
```

Explicando:

```
/ip firewall mangle
add chain=prerouting p2p=all-p2p action=mark-connection
new-connection-mark=conexao-p2p passthrough=yes comment="CONTROLE DO P2P" disabled=no
add chain=prerouting connection-mark=conexao-p2p action=mark-packet new-packet-mark=pacotes-p2p
passthrough=yes comment="" disabled=no
add chain=prerouting p2p=all-p2p action=mark-routing new-routing-mark=p2p passthrough=no comment=""
disabled=no
```

Marcações

As marcações servem para determinar no sistema o destino de determinados serviços para posteriormente poder definir suas premissas dentro do sistema.
As marcações são muito usadas para especificar uma rota de um determinado serviço para outro link.
Neste caso marcamos a conexão, tráfego e rota do serviço p2p.

1. a primeira marcação faz referência as conexões realizada pelo serviço p2p.
2. A segunda marcação fará a marcação dos pacotes ou seja do tráfego
3. A terceira marcação fará a rota ou o caminho que este serviço deverá tomar

Apenas para lembrar cada marcação é reconhecida pelo comando “add” que significa

adicionar. Então quando falo a primeira regra é onde começa o primeiro “add”.

Bloqueio Firewall

```
/ip firewall filter
add chain=forward p2p=all-p2p src-address-list=!p2p-sem-bloqueio action=drop comment="BLOQUEIO DO P2P" disabled=yes
```

O firewall dropará das conexões que o cliente p2p tetar estabelecer.
Desta forma o p2p não funciona uma vez que ele depende das conexões para realizar a troca de arquivos.

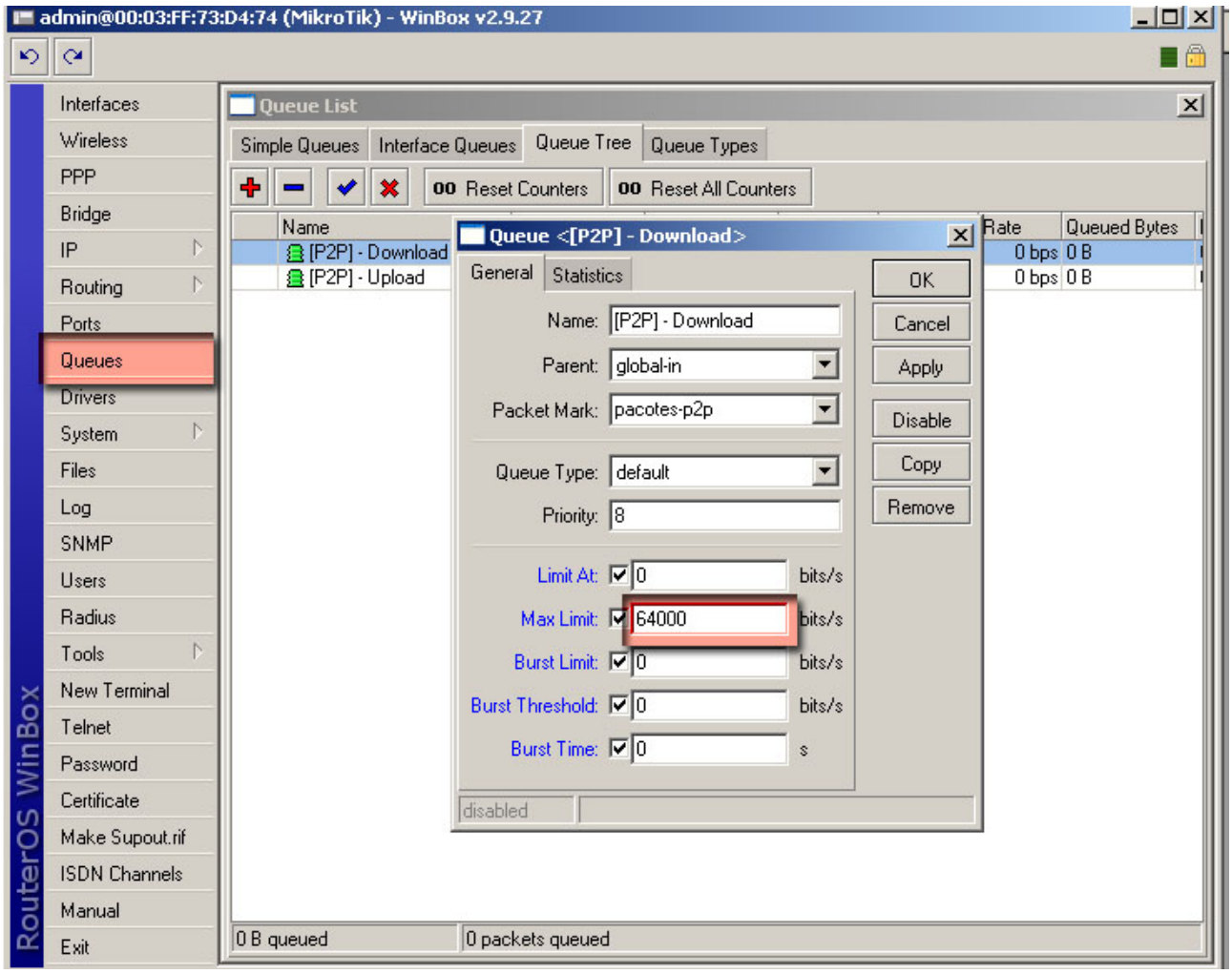
Queue

O queue fará o controle da banda que será disponibilizado para os serviços de p2p.

```
/ queue tree
add name="\[P2P\] - Download" parent=global-in packet-mark=pacotes-p2p limit-at=0 queue=default priority=8 max-limit=64000 burst-limit=0 burst-threshold=0 burst-time=0s disabled=no
add name="\[P2P\] - Upload" parent=global-out packet-mark=pacotes-p2p limit-at=0 queue=default priority=8 max-limit=64000 burst-limit=0 burst-threshold=0 burst-time=0s disabled=no
```

1. A primeira regra é usado para controlar o a taxa de download do p2p, originalmente o serviço está configurado para 64k “max-limit=64000” para alterar o valor do download do p2p para seus clientes você deverá alterar o valor 64000 à sua necessidade.
   ex. Caso queira dispor 100k para seu cliente você deverá por 100000 ficando assim max-limit=100000.
2. O segundo queue refere-se a taxa de upload assim como acontece no download basta alterar o valor do max-limit para mudar a quantidade de banda disponibilizada para este serviço.

Caso você queira alterar o limite de download e upload pelo winbox acesse o menu queue, de dois cliques sobre as regras e altere onde tem max-limit.
Veja as configurações na figura abaixo.



Scripts

A função dos scripts aqui será ativar e desativar o bloqueio total do p2p, muito útil quando seu ISP estiver com muitos clientes online.

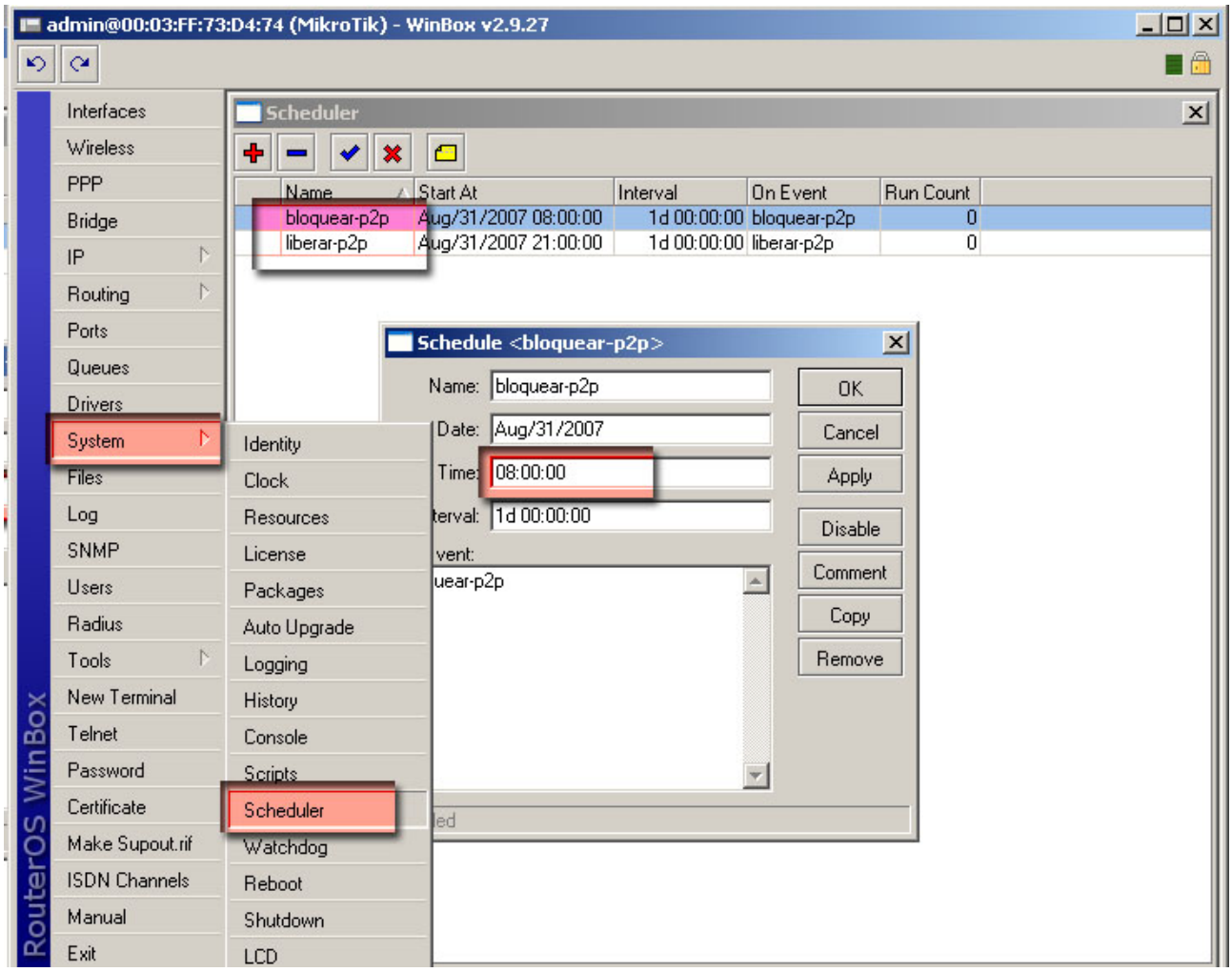
```
/ system script
add name="liberar-p2p" source="/ip firewall filter disable \[/ip firewall filter find p2p=all-p2p\]" \
policy=ftp,reboot,read,write,policy,test,winbox
add name="bloquear-p2p" source="/ip firewall filter enable \[/ip firewall filter find p2p=all-p2p\]" \
policy=ftp,reboot,read,write,policy,test,winbox
```

Scheduler ou Agendamento

```
/ system scheduler
add name="bloquear-p2p" on-event=bloquear-p2p start-date=aug/31/2007 start-time=08:00:00 interval=1d
comment="" disabled=no
add name="liberar-p2p" on-event=liberar-p2p start-date=aug/31/2007 start-time=21:00:00 interval=1d
comment="" disabled=no
```

O agendamento ativa o serviço de bloqueio total ou seja o script feito no tópico acima em horários críticos, geralmente em horários onde o maior número de usuários estão conectado.
Observe que o horário aqui está setado para iniciar as 08:00:00 e terminar as 21:00:00,

caso queira mudar o horário de ativação do serviço você deverá mudar o campo start-time da regra abaixo ou você poderá acessar o menu **system scheduler** e realizar essa alteração no próprio agendamento dando dois cliques nas regras, **bloquear-p2p** e **liberar-p2p**.

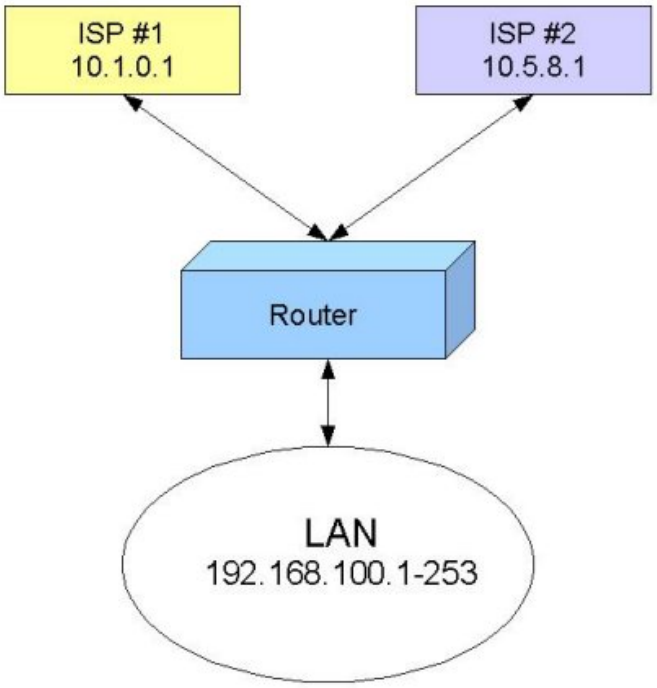


Load Balance (utilizando mais de um link no mesmo sistema)

Balanceamento de carga é a técnica utilizada para dividir os recursos de um sistema de forma a não sobrecarrega-lo, no caso do mikrotik é o direcionamento dos caminhos que os links devem seguir afim de aumentar a capacidade do mesmo.

No mikrotik você poderá adicionar mais de um link de internet definindo rotas especificas para atender determinado número de pessoas, aumentando a capacidade do seu servidor e garantindo a qualidade do mesmo.

Outra prática comum ao load balance é determinar uma rota exclusiva com um link próprio para os serviços de http e e-mail, que são serviços básicos e não requerem muita banda usado pela maioria dos seus usuários.



O balanceamento de carga que iremos realizar consiste em colocar duas adsl (ISP1 e ISP2) e definir rotas diferentes para cada adsl 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 ISP #1 ou ISP#2.
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 (temos 254 endereços para atribuir ao clientes)

Os grupos ficaram divididos na seguinte faixa de ips.

• **Grupo A** 192.168.100.1 até 192.168.100.126 -

• **Grupo B** 192.168.100.128 até 192.168.100.253

• O **gateway** será 192.168.100.254

Todas as as máquinas dos usuários terá o IP do grupo (A ou B), Com a máscara de rede, 255.255.255.0, e gateway padrão 192.168.100.254 para ambas.

Após ter definido os grupos e como eles estarão divididos, nós podemos escolher quem usará cada IP

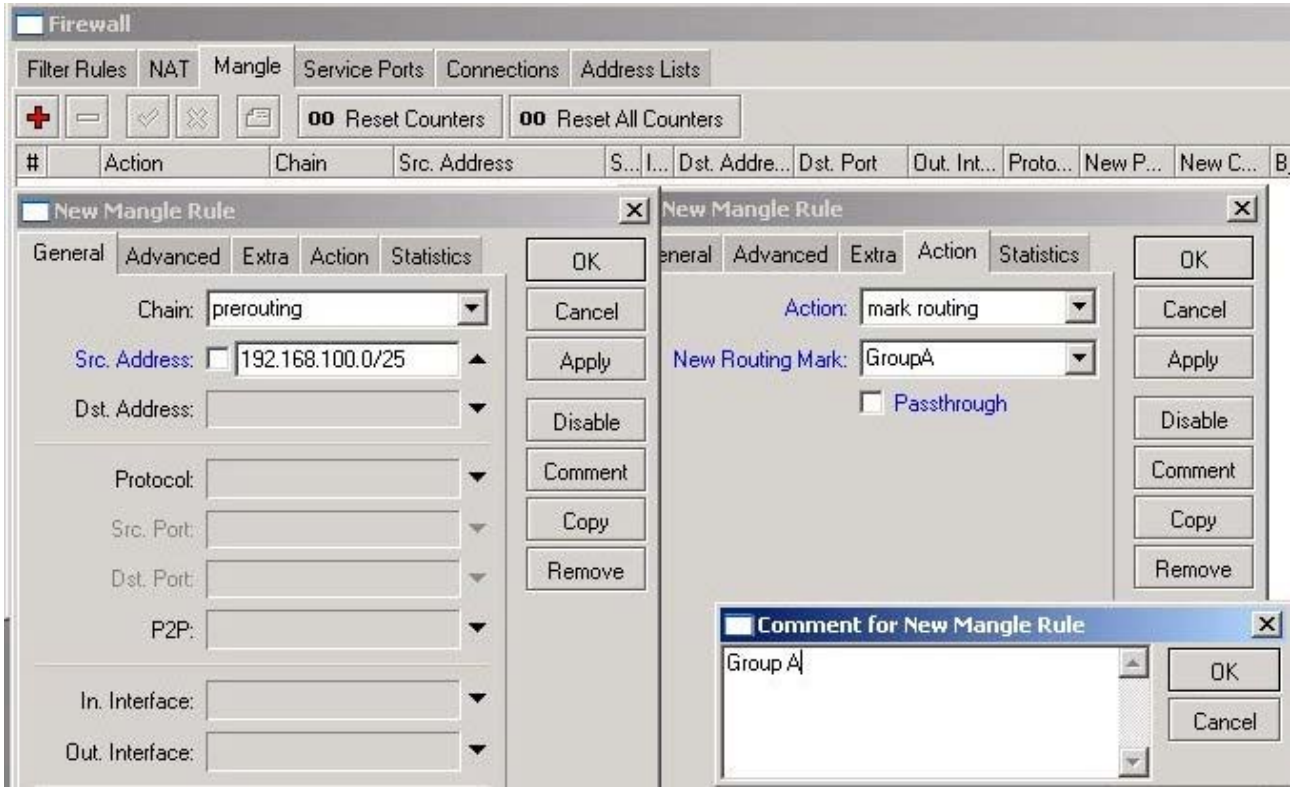
• O grupo A é 192.168.100.0 /25, isto é, endereços de 192.168.100.1 até 126

• O grupo B é 192.168.100.128 /25, isto é, endereços de 192.168.100.129 até 253

Configurando a regra Mangle

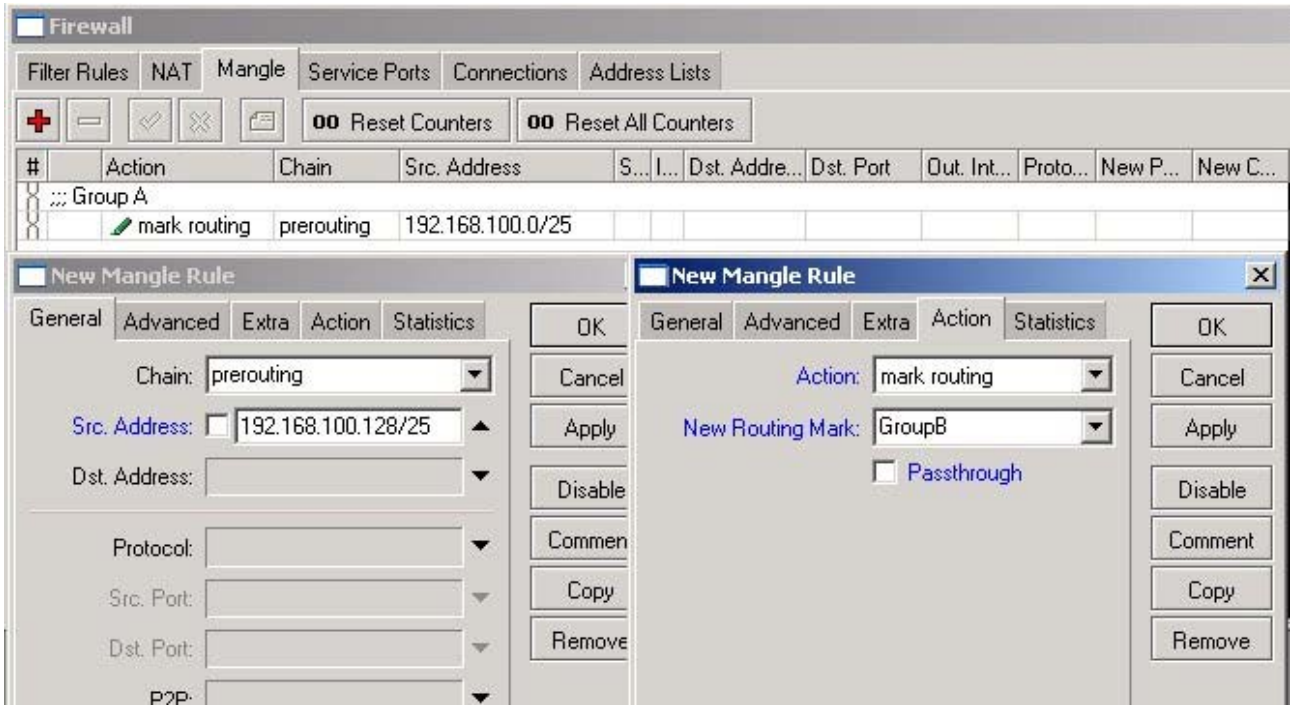
Marcaremos os pacotes do grupo A

1. **Aba General** > Chain: prerouting e Src. Address: 192.168.100.0 /25
2. **Aba Action** > Action:mark routing e new routing mark: escreva **“GroupA”**.
3. Adicione um comentário para você se organizar.



Marcação dos pacotes para o Grupo B

1. **Aba General** > Chain: prerouting e Src. Address: 192.168.100.128 /25
2. **Aba Action** > Action: mark routing e new routing mark: escreva **“GroupB”**

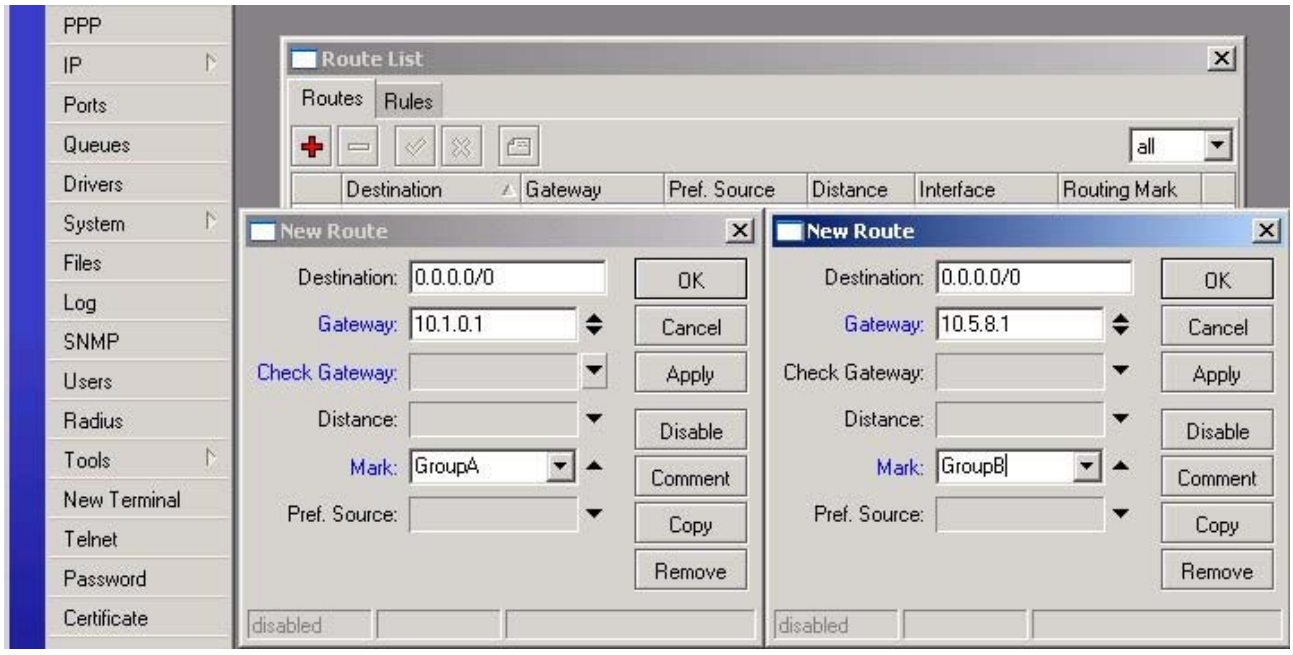


Todo tráfego gerado pelo servidor terá os Ips marcados como **GroupA** e **GroupB**, usaremos essas marcações mais afrente para atribuir rotas especificas.

Especificando as rotas:

Acesse o Menu **IP** submenu **Route.**

Clique no sinal de **"+"** para adicionar novas rotas e configure como estabelecido na imagem abaixo, lembre-se que os endereços aqui deverão ser os IPS do seu ADSL que deverão estar configurados como router.



Finalizando o tutorial você fará o mascaramento de sua rede basta apenas criar uma regra de NAT.

Criando a máscara de rede

Vá para o menu IP e submenu Firewall. acesse a **aba nat** clique no sinal de **“+”**e configure conforme a figura abaixo.

Aba General

1. **Aba General** > Chain: Src. Address 192.168.100.0/24
2. **Aba Action >** Action masquerade

Teste a configuração

Teste para GroupA

Em um computador com com o IP do GroupA abra o console de comando do DOS e digite: **“C:\>tracert -d 8.8.8.8”** claro que sem as aspas e sem o c:>

deverá aparecer a seguinte resposta mudando apenas o ip do ISP que provavelmente não será 10.1.0.1 a não ser que você configure no modem.

Tracing route to 8.8.8.8 over a maximum of 30 hops

Tracing route to 8.8.8.8 over a maximum of 30 hops

```
1     2 ms     2 ms     2 ms  192.168.100.254
2    10 ms     4 ms     3 ms  10.1.0.1
...
```

Teste para GroupA

Em um computador com com o IP do GroupB abra o console de comando do DOS e digite: **“C:\>tracert -d 8.8.8.8”**

deverá aparecer a seguinte resposta mudando apenas o ip do ISP que provavelmente não será 10.1.0.1 a não ser que você configure no modem.

Tracing route to 8.8.8.8 over a maximum of 30 hops

```
1     2 ms     2 ms     2 ms  192.168.100.254
2    10 ms     4 ms     3 ms  10.5.8.1
...
```

Acabamos de mostrar uma forma de fazer o balanceamento de carga existem outras, posteriormente postaremos e enviaremos via e-mail para você outras maneiras.

Acabamos nossa explicação sobre o Mikrotik, existindo dúvidas envie um e-mail para o autor zona13793@yahoo.com.br.

Kit Cliente

O que chamamos de Kit Cliente?

São os equipamentos necessários para que possamos instalar o sistema na casa de um Cliente.

O Kit é composto basicamente de?

1. **Antena** – recomendo antenas direcionais de 24dbi para clientes mais distantes e para clientes próximos caso não consiga estabelecer o um elance estável você poderá usar uma solução de antena direcional de 16dbi, esteticamente são menos chamativas e mais fáceis de manipular.

   Preço médio **R$ 70,00**

2. **Placa Wireless** – A placa Wireless fará a conexão com a antena recebendo o sinal do servidor.
   No mercado existem muitos modelos e preços que variam de R$ 50,00 á R$ 150,00, os modelos mais baratos geralmente não são tão bons, procure as placas equipadas com o Chipset Atheros ou Ralink, posso recomendar pois essas placas foram testadas na prática e sem dúvida o ganho com elas é significativo. O Chipset não é a marca da placa é apenas o chip que equipa os equipamentos de diversas marcas, como a g-link ou linksys.

   Preço médio **R$ 70,00**

3. **Cabo RGC-58** – São indicados para instalação em clientes pelo baixo custo, a metragem deve ser tirada no próprio cliente, evite levar cabo pronto você perderá muito muito cabo e dinheiro.

   Preço médio p/metro **R$ 3,00**

4. Conectores – você precisará de dois conectores para o cabo um **Conector N Macho P/ Rgc58** dependendo do conector da antena você deverá adquirir o **Conector N Femea P/ Rgc58** conector e para conectar nas placas wireless o **Conector Sma P/ Rgc58**.

   Preço médio Conector N **R$ 10,00**
   Preço médio Conector sma **R$ 7,00**

5. **Tubo Galvanizado** – O tubo galvanizado servirá de suporte para seus clientes, compre o tubo mais grosso para suporte de antena, em casas especializadas em antenas de TV você encontra-rá com facilidade. Esses tubos são relativamente caros, eles são comprados de 3mts você poderá cerrar o tubo em 2 para elances com mais facilidade.

   Preço médio **R$ 30,00**

6. **Suporte Pata Tubo** – Vale apena falar aqui do suporte pois o mesmo tabém é relativamente caro para a função que tem, Preço médio **R$ 15,00**

Então, temos um preço médio de do Kit completo de R$ 205,00, o preço pode variar conforme o fornecedor, marca, quantidade e frete, essa variação pode chegar a 40 % para menos e 20 % para mais.

Esse custo geralmente geralmente é cobrado do cliente como custo de instalação, você poderá fornecer esses equipamentos em sistema de comodato, ficando com os equipamento caso haja desistência por parte do cliente.

Verificando o Sinal em um Cliente

A verificação de viabilidade não é uma tarefá tão simples, não pela cobrança intelectual mais sim pela exigência física e de certa forma arriscada, é imprescindível equipamentos de segurança para essa tarefa.

Não existe calculo que substitua o bom teste prático, mais existe o bom senso, elance muito longos, ou barreiras em demasia. Enfim você terá este feeling na prática, enquanto isso você irá tentar(e isso é bom), em qualquer lugar afinal você não vai querer dizer não aos seus primeiros clientes.

Você deverá estar dotado dos seguintes equipamentos:

1. **Notebook** – equipamento necessário devido a sua portabilidade e a possibilidade de você levar para os locais sem necessidade de ponto de energia.
2. **Placa wireless USB com conector SMA** – A edimax disponibiliza um equipamento com estas especificações. O modelo é EW-7318USG.
3. **Cabo para conexão USB/Antena** – faça um cabo rgc58 de até 3 metros para você levar junto e fazer a conexão usb/antena, recomendo até 3mts pois a resistencia do cabo não terá influência na tentativa de pegar um pico de sinal que seja.
4. **Escada** – não precisava nem falar, vale apenas dizer que o ideal são escadas de aluminio de até 3mts, essas escadas são leves e darão conta de quase todo o serviço.
5. **Netstumbler** – essa sem dúvida é uma ferramente que vale apena falar, o Netstumbler é um software para verificar a existência de sinal Wi-Fi.
   Ele lhe mostrará toda as informações disponíveis sobre o sinal e você poderá mensurar a viabilidade da instalação do sistema em determinado cliente.
   Disponibilizei um tópico só sobre o netstumbler abaixo.
6. **Google earth** – Essa ferramenta é outra mão na roda, com o software google earth você terá maior noção de direção poderá ver a distância da sua torre para o ponto do cliente, poderá visualizar altura do terreno, existência de edificações e muito mais, instale encontre sua torre e já comece a reconhecer o terreno.
7. **GPS** – Ao se distanciar da torre, entrando e saindo de beco, você provavelmente perderá o senso de direção, isso acontece mesmo você tomando conhecimento do terreno pelo google-earth, o GPS lhe dará a sua localização em relação a torre e com o auxílio de uma bússola provavelmente você direcionará sua antena para o local certo.
8. **Binóculos** – Pense que você tem uma torre vazada de 40 cm de largura se encontrando a 1km de distância da mesma. Você não enxergará nem o vulto dela.

Após você se situar no local com o auxílio do GPS e bússola é só mirar o binóculos para a localização indicada e logo logo você verá, claro que vai depender e muito do alcance do seu binóculos.

Os equipamentos listados acima não são obrigatórios, já tive a experiência de ir na residência do cliente com um computador desktop na mão e uma placa Wireless instalada (no dia seguinte providenciei um notebook), assim como já fechei muitos elances sem o auxílio de binóculos e GPS, porém devo ter perdido alguns possíveis elance por estar procurando a antena em direção errada, enfim já tomei muita queda de telhado, mais antes de tudo isso me rendeu experiência e alguns vexames até que cheguei a um patamar onde o trabalho de verificação de sinal já tinha se tornado rotina e sem dúvida menos laborioso, além de mostrar mais profissionalismo perante o cliente.

É recomendável que você faça esse serviço com o auxílio de outra pessoa, afinal seu cliente não vai estar disponível para segurar a escada, passar ferramenta e subir em telhado.

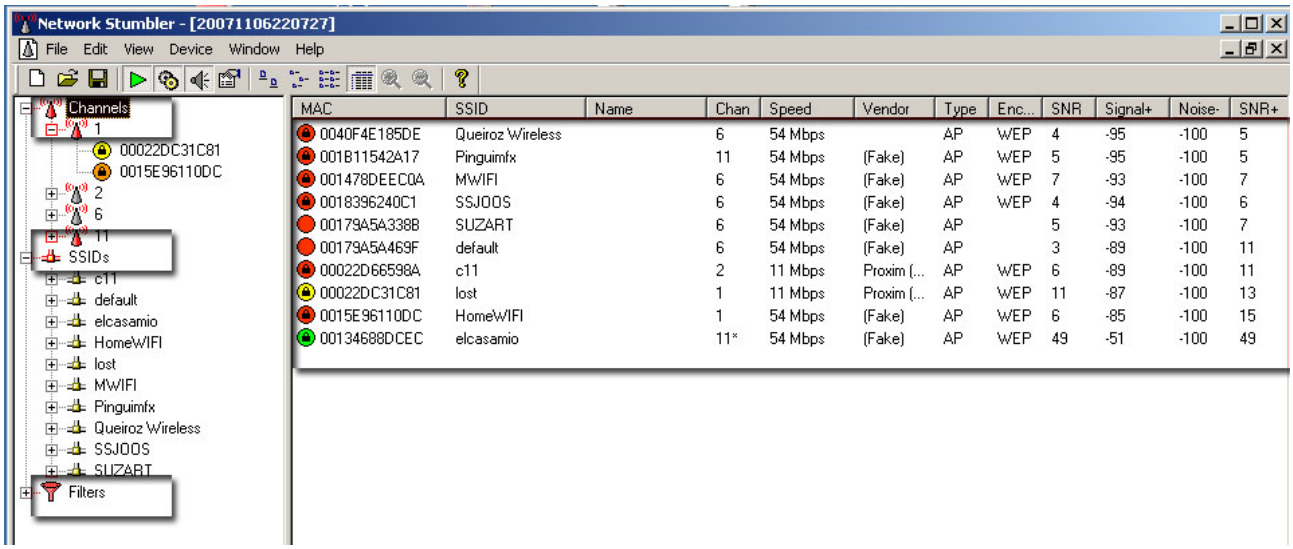
Netstumbler

É uma ferramenta para detecção de redes wireless nos padões 802.11b, 802.11a e 802.11g,
O sistema é compatível com o Windows sendo importante tê-lo instalado no seu notebook de verificação de sinal, tanto como nos computadores dos clientes afim de diagnosticar a qualidade do sinal.

O Netstumbler é utilizado para:

1. Wardriving (técnica usada para detectar redes utilizando um veículo)
2. Verificação de configurações de rede Wi-Fi
3. Encontrar as localizações coberta por uma determinada rede.
4. Detectar a causa de uma possível interferência.
5. Detectar pontos de acesso irregulares.
6. Alinhamento de antenas.

Conhecendo o Netstumbler

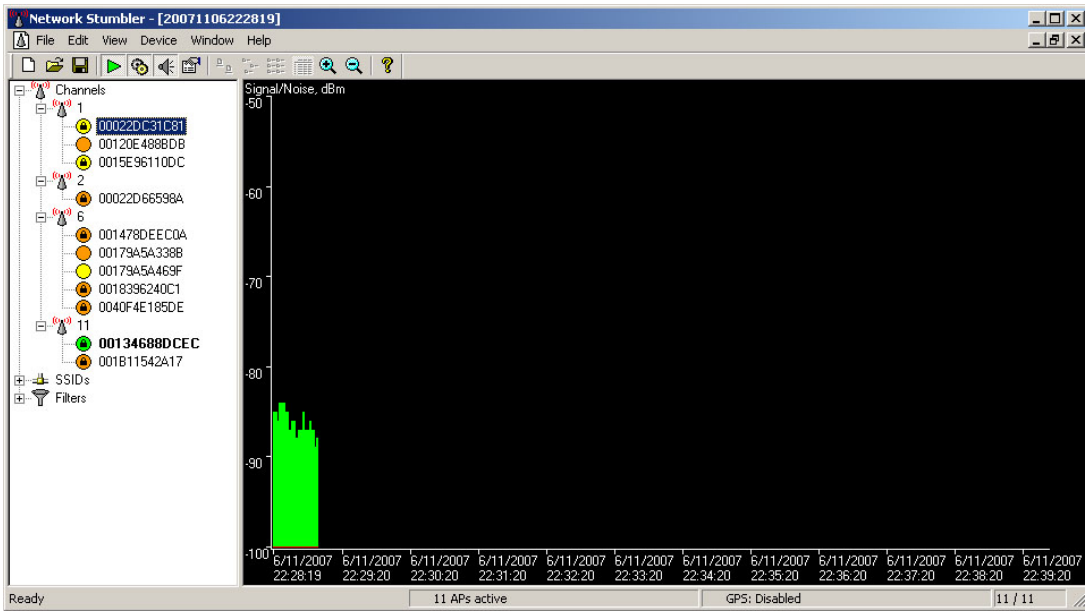


O sistema é simples e direto, do lado esquerdo você terá os filtros para as redes detéctadas, você poderá listar as redes por **Channel** (canal), por SSID, ou utilizar filtros mais específicos na parte filter, ex. Mostrar apenas APs com criptografia.
Do lado direito teremos todos os APs disponíveis inicialmente ele mostrara todos sem filtro algum, e os dados relevantes ao AP que são:

MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR	Signal+	Noise-	SNR+
0040F4E185DE	Queiroz Wireless		6	54 Mbps		AP	WEP	4	-95	-100	5
001B11542A17	Pinguimfx		11	54 Mbps	(Fake)	AP	WEP	5	-95	-100	5
001478DEEC0A	MWIFI		6	54 Mbps	(Fake)	AP	WEP	7	-93	-100	7
0018396240C1	SSJOOS		6	54 Mbps	(Fake)	AP	WEP	4	-94	-100	6
00179A5A338B	SUZART		6	54 Mbps	(Fake)	AP		5	-93	-100	7
00179A5A469F	default		6	54 Mbps	(Fake)	AP		3	-89	-100	11
00022D66598A	c11		2	11 Mbps	Proxim (...	AP	WEP	6	-89	-100	11
00022DC31C81	lost		1	11 Mbps	Proxim (...	AP	WEP	11	-87	-100	13
0015E96110DC	HomeWIFI		1	54 Mbps	(Fake)	AP	WEP	6	-85	-100	15
00134688DCEC	elcasamio		11*	54 Mbps	(Fake)	AP	WEP	49	-51	-100	49

1. MAC – o endereço físico dos APS encontrados
2. SSID – As identidades dos APS na rede
3. Chan – O canal de operação
4. Speed – velocidade do ap, quando é 11Mbps significa que aquele ap esta operando em 802.11b e quando for 54Mbps 802.11g.
5. Vendor – Fabricante do AP
6. Type – Tipo de interface, na maioria das vezes é AP, mais você pode detectar redes Ad-Hoc por exemplo.
7. Encyption – Tipode criptografia usado pela interface.
8. SNR – Qualidade do sinal quanto maior melhor.
9. Signal+ - Qualidade do sinal em uma escala que vai de -100 à 0, quanto menos negativo melhor ou quando mais próximo do zero, geralmente um sinal para que você possá estabelecer ma conexão é a partir de -70.
10. Noise – Quantidade de ruido, quanto mais próximo do -100 melhor, quando está no -100 significa que não existe ruído no sinal

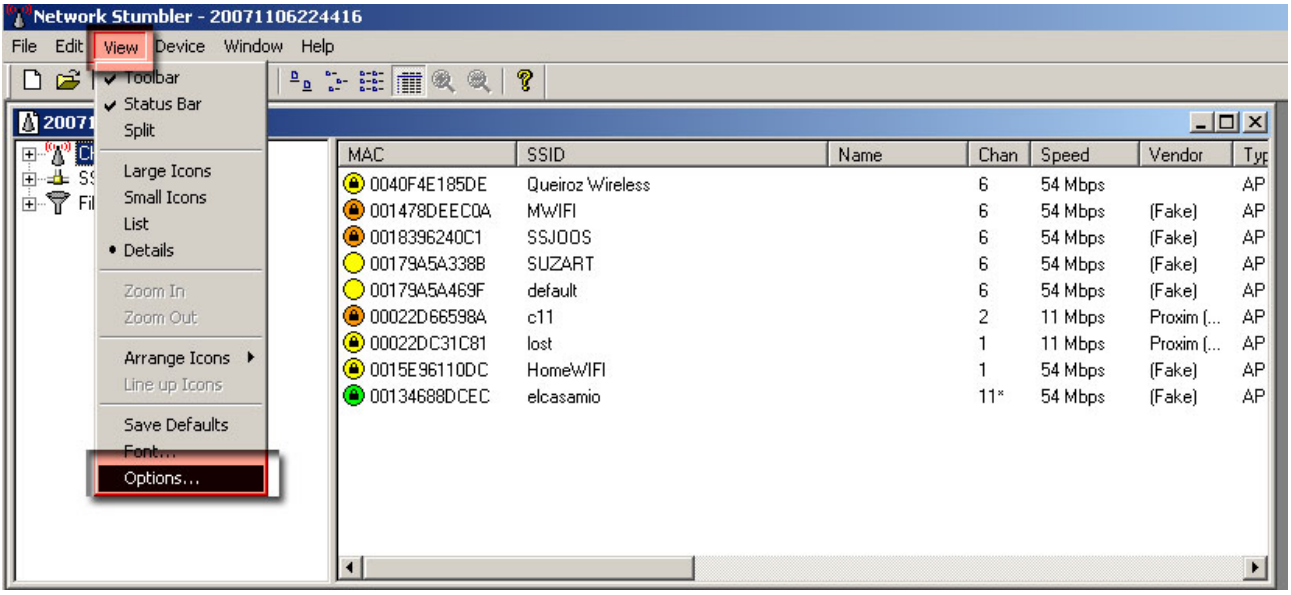
Gráficos de sinal



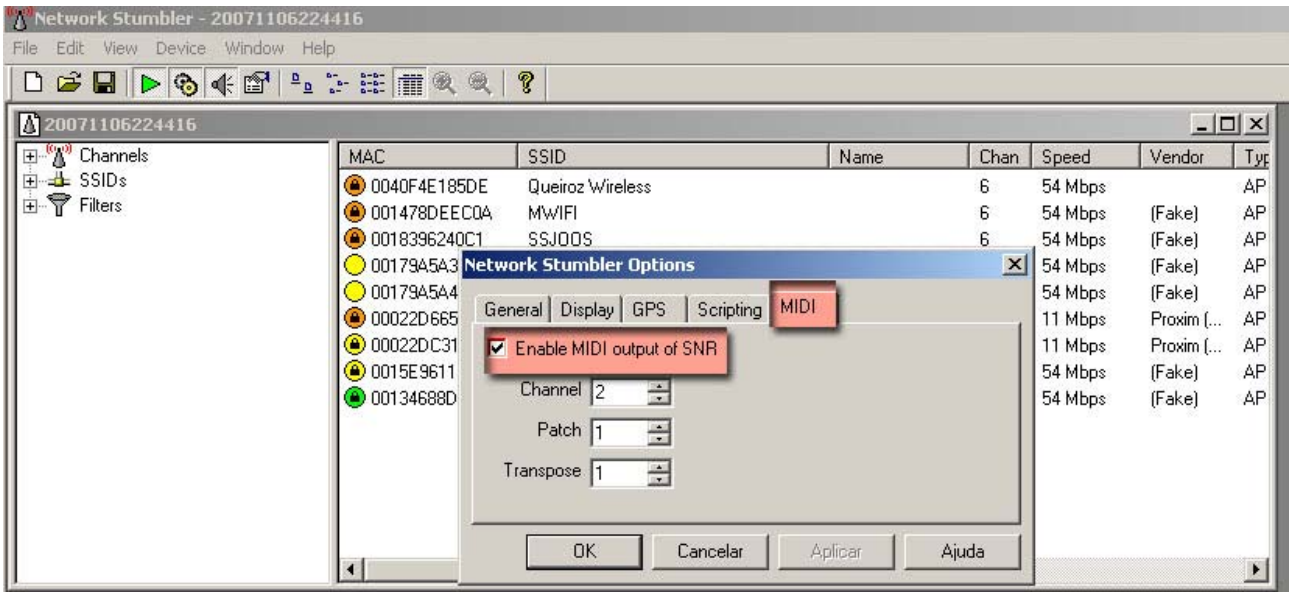
Para que possa visualizar o gráfico do sinal de um determinado AP você precisará expandir(clicar no sinal de “+”) os níveis do menu da esquerda, como mostra a imagem acima.

O menu Channel foi expandido depois o menu referente ao canal 1 e depois o AP clicando no seu MAC, caso você queira visualizar seu ap pelo nome você deverá expandir o menu SSID.
Com o gráfico na tela, direcione a antena a antena para torre e busque o ponto exato de elance através do pico máximo do gráfico, lembrando que quanto mais próximo de zero melhor.

Você poderá fazer o alinhamento das antenas utilizando um **sistema sonoro** do próprio Netstumbler, liberando sua atenção visual para a torre.
Para isso acesse o menu **view** e depois **options**.



Na tela de **options** acesse a **aba Midi** marcando **Enable MIDI output of SNR.**



Como efetuar a cobrança

Para você que está iniciando seu provedor, ou até mesmo já tenha um, existe uma empresa chamada F2B, é uma espécie de banco virtual, essa empresa disponibiliza todos os meios de pagamento para você de forma simples e sem burocracia e qualquer pessoa poderá abrir uma conta tanto física quanto jurídica.

Você tem todo o controle financeiro, recebendo por email confirmação de pagamento, opção de emitir boleto (inclusive inserir sua logo) enviando para seu cliente por email ou carta, poderá agendar cobrança mensal, cadastrar clientes, gerenciar todo movimento financeiro.

Vantagens:

1. Não existem as taxas de um banco comum.
2. Não será cobrado CPMF
3. Poderá transferir o dinheiro para conta física ou jurídica.
4. Disponibiliza sistema de integração de cobrança para seu Site
5. Burocracia 0
6. Disponibiliza um cartão de débito para você usar o dinheiro disponível sem necessidade de transferência para uma conta física (imagine as possibilidades).

Existem outras vantagens que você terá que visitar o site para saber mais detalhes sobre o F2B e sem dúvidas é uma mão na roda para driblar a burocracia dos bancos brasileiros.
Para maiores informações acesse www.f2b.com.br .

Questões Legais

Texto retirado do site da ABRANET Associação brasileira dos provedores de Internet

COMO MONTAR UM PROVEDOR DE ACESSO VIA RÁDIO

Contribuições ao Tema

A Abranet possui um grupo de trabalho em formação que vai atuar diretamente nesta área, não somente nas questões de SCM, mas de outras pertinentes a regulamentação, quanto ao SCM.

- As empresas que comercializam serviços de Telecom atuam basicamente em duas frentes:
  - Serviços de Telefonia (STFC - Serviço de Telefonia Fixa Comutada)
  - Serviços de dados
  - Nas concessões de STFC, que é um serviço de interesse público as empresas compradoras (tanto as "incumbents" quanto as "espelhos"), receberam autorizações de operar serviços de dados, estas operadoras,portanto podem realizar conexões dedicadas, ligando o “ponto A com ponto B” por quaisquer meios, utilizando radiofreqüência ou não.

O Serviço de transmissão de dados, em caráter privado, contava com várias denominações (SRTT / SLE etc...) com a Lei 9472 de 06 de julho de 1997 criou-se o SCM - Serviço de Comunicação Multimídia que veio a englobar todas estas atividades (mais informações sobre a Lei 9472 podem ser visualizadas no site da ANATEL - www.anatel.gov.br)

Mas o que tem haver isto com nosso negocio de Provedor de acesso?

É necessário desenvolver em paralelo, para que possamos entender as dicotomias e onde na verdade estes temas, Provedor de acesso x SCM se encontram.

Com a insatisfação dos clientes, principalmente dos heavy users com a banda estreita, o mercado banda larga começou a crescer, e tivemos um movimento de crescimento deste serviço, nas grandes cidades, o ADSL tomou conta de certa maneira deste mercado, mas um movimento diferente, na realidade não muito programado pelas teles começou a surgir, principalmente, nas pequenas/médias cidades onde as redes ADSL não estavam contempladas a “priori”, o ACESSO VIA RADIO 2.4 Ghz, no inicio com um custo razoável e agora relativamente barato.

Os provedores não só criaram/adaptaram uma tecnologia, (inicialmente puramente indoor) para operar outdoor como começaram a desenvolver ferramentas, como controle de banda, cachês, roteamentos alternativos que fizeram com que as redes de rádio 2.4 Ghz, começassem a ter QoS (Nível de Qualidade) superior as redes ADSL.

Vejamos, portanto o inicio da invasão rádio 2.4 (anterior ao efetivo conhecimento e aplicação da Legislação SCM), mas os legisladores de certa maneira, visionaram esta invasão.

Gostaríamos de frisar, que a outorga SCM, a priori, não tem nada a haver com operação de rádio freqüência, uma empresa outorgada pela Anatel pode, ou não, utilizar este meio (rádio freqüência) para ligar o “ponto A ao ponto B”, (pois se utilizar fibra ótica, par trancado, coaxial) não irá necessitar desta autorização, quando uma empresa tem a outorga ela tem a prerrogativa de pedir ou não, uso de rádio freqüência, no caso para rádio freqüência licenciada exclusiva ou não. Um erro comum, que vamos esclarecer á seguir e a confusão á despeito de ser as freqüências de 2.4 e 5.8 freqüências "Livres" portanto, livres de licença para operação.

Freqüência Licenciada divide-se em:

1. **Exclusiva** - Basicamente de operadoras celulares, ou seja, elas adquirem via leilão, estas freqüências, serão proprietárias na exploração deste serviço, tem território delimitado e são onerosas.
2. **Não exclusivas** – Citamos um exemplo: A “Telecom A” pode operar um enlace a 15 Ghz em Manaus para atender um cliente de 4 Mbs e a “ Telecom B” pode estar usando esta mesma freqüência pra atender um outro em Curitiba, as estações tem de estar registradas e pagam a Anatel uma taxa de otimização de rádio freqüência (IPPUR) (que é calculado via uma fórmula que se encontra no site da Anatel), ou seja, geram custos em toda a sua utilização.

Freqüências 'Livres “ou não”Licenciadas”.

Copiados do FCC (órgãos americanos), são nomeados ISM (Industrial and Service Mode) foram estabelecidas para que organismos como polícia, bombeiros etc, tivessem acesso a comunicação de uma maneira menos "burocrática", sua característica principal e a necessidade de estarem homologadas, cadastradas no órgão regulador, mas, não pagam pela otimização deste espectro.

Na realidade o que queremos ressaltar, é que quando a Anatel “lacra”, (e estão lacrando!), seu provedor por estar prestando serviço de rádio, o foco não é na freqüência e sua utilização, está na permissão ou não de sua empresa em prestar Serviço de Telecomunicação.

A Lei de SCM vem a regular a relação entre o ISP e seu cliente, com a ANATEL ele tem somente duas; uma regulatória que se exaure no momento que o órgão concede a licença, e outra fiscalizadora, em que o cerne da questão (esta somente se à parte básica da rede estiver ok).

Finalizando, toda empresa que liga “ponto A ao ponto B”, para acesso IP (Internet) ou dados privados tem que estar regular (SCM) para prestar este serviço.

Perguntasmais Freqüentes:

1 -E muito caro?

A outorga custa R$9.000,00 (nove mil reais), o pagamento é efetuado para a ANATEL via

um boleto, quando da publicação no diário oficial da união, pode ser utilizada em todo o território nacional.

2 - O que preciso?

A empresa deve estar:

1. Constituída segundo as leis Brasileiras com sede e administração no País;
2. Com todas as condições de idoneidade perante o Poder Público (seja quanto a licitações, impostos ou permissões).
3. Documentos necessários:
    1. Contrato Social com o objeto compatível com a autorização
    2. Cópia do CNPJ
    3. Inscrição Municipal
    4. Inscrição Estadual
    5. Registro no CREA, assinado por um responsável técnico que seja engenheiro eletrônico, eletricista ou engenheiro de telecomunicações.
    6. Certidões Negativas da Fazenda Federal, Estadual eMunicipal
    7. Prova de regularidade Junto ao INSS e FGTS

3 – Como proceder?

Inicialmente você vai precisar elaborar um projeto muito simples, com auxílio de um engenheiro de confiança.

5 -Mas meu serviço de rádio é pequeno, será que compensa SCM só pra regularizá-lo?

O SCM não é só pra regularizar rádio, (leia a íntegra da lei no site da Anatel) e verá que ele abre um leque enorme de serviços hoje e no futuro, além de ter descontos em links e outros serviços junto as Teles, por ser uma empresa de Telecom também.

Principais fornecedores:

Diversos

Especializados nos principais produtos para sistema wireless (cabos, caixa hermética, antenas, conectores, torres e afins) vale apena conferir

1. http://gtnet.com.br/
2. http://www.americanexplorer.com.br/
3. http://www.sat5.com.br/
4. http://loja.tray.com.br/loja/loja.php?loja=14629
5. http://www.orbitech.com.br/
6. http://www.orbitech.com.br/
7. http://www.orbitech.com.br/

Escadas

1. http://www.escafort.com.br/

Fabricantes de antenas no Brasil

1. http://www.tsm.com.br/
2. http://www.idealantenas.com.br/
3. http://www.aquario.com.br/
4. http://www.glink.com.br/

Firmeware

1. http://www.aprouter.com.br/

Torres

1. http://www.apioinstalacoes.com.br
2. http://www.radiotech.com.br/torres/torres.htm
3. http://www.towercom.com.br/

Link e Ips dedicado

1. http://www.ipdedicado.com.br/
2. http://www.cttelecom.com.br/
3. http://www.embratel.com.br/Embratel02/cda/portal/0,2997,MG_P_652,00.html

Criação de interface para discador PPPOE

1. http://www.embrap.com.br/

Consultoria em certificação SCM

1. http://www.scmconsultoria.com.br/

Free DDNS

1. http://www.changeip.com/

Tutoriais

1. http://svcglobal.com/antena/index.html (construa sua própria torre de alumínio)
2. http://www.xe1rcs.org.mx/galeria/torre/ (instalando uma antena tipo estaiada)
3. http://www.egidy.de/wifi/wusb54g/ (improvisando uma antena externa)
4. http://www.engadget.com/2005/11/15/how-to-build-a-wifi-biquad-dish-antenna/2
1. http://www.saunalahti.fi/elepal/antenna2.html
2. http://koti.mbnet.fi/zakifani/biquad/
3. http://martybugs.net/wireless/biquad/
4. http://martybugs.net/wireless/biquad/double.cgi
5. http://koti.mbnet.fi/zakifani/biquad/
6. http://under-linux.org/forums/wireless/92921-construindo-antenas-bi-quad.html
7. http://www.paramowifix.net/antenas/EnlacesAntenas.html
8. http://www.usbwifi.orcon.net.nz/
9. http://under-linux.org/forums/antenas/95638-fotos-aquario-12dbi-60-graus-

desmontado.html

Links diversos

10. http://under-linux.org/wiki/index.php/Tutoriais/Wireless
11. www.mikrotik.com
12. www.mikrotik.com.br
13. http://www.mundowifi.com.br/
14. http://wireless.gumph.org/content/3/7/011-cable-connectors.html (todos os tipos de conectores)
15. https://capivara.warchalking.com.br
16. http://www.infowester.com

Conclusão

Esta é a primeira versão de uma obra inacabada, o mundo em torno do sistema mikrotik é mais vasto e com inúmeras possibilidades de configuração do que foi apresentado neste e-book, peço desculpas aos meus leitores por qualquer equívoco da minha parte.

Esta é uma versão beta sem revisão os erros de concordância e ortografia serão minimizados em um proxima versão.

Áqueles que estão comprando este e-book estarão recebendo as atualizações gratuitamente via e-mail para tanto entre em contato com o autor pelo e-mail zona13793@yahoo.com.br com o título “quero receber atualizações” colocando o seu nome completo no e-mail.

Criticas sugestões e elogios para: Túlio Ernandez Cabral. zona13793@yahoo.com.br

Salvador Bahia
07 de novembro de 2007