

Bem vindo ao Portal Under-Linux! O maior Portal sobre Linux e Tecnologia da Informação do Brasil! Você ainda não é **registrado**? Pois não perca seu tempo e **crie já seu usuário**. É rápido e fácil! E você terá muitas vantagens: Além de participar do maior fórum de tecnologia do país, ainda terá seu próprio Blog para escrever sobre os seus temas favoritos, e criar uma verdadeira comunidade à sua volta. E você ainda poderá crescer (e enriquecer) profissionalmente, interagindo com os milhares de usuários de nosso Portal, profissionais de TI e diversas empresas da área de tecnologia que estão sempre online no Under-Linux.Org.

Senhores, o Portal Under-Linux.Org ficará indisponível por período indeterminado para manutenção no dia 08/05/2011 a partir das 03:00 da manhã.

[Ver código-fonte](#) [Ver histórico](#) [Discussão](#)

Mikrotik
De Under-Linux.Org Wiki

Guia passo-a-passo do Mikrotik



Tabela de conteúdo

- 1 Prefácio
- 2 Configurações iniciais
- 3 Configurando o Mikrotik (LINK ou MODEM ROTEADO)
- 4 A PRÓPOSTA DOS TÓPICOS
- 5 Como amarrar IP/MAC
- 6 Configurando o WEB-PROXY
- 7 Controle de banda
- 8 Acesso remoto a outro Mikrotik
- 9 Controle P2P (MUITO BOM)
- 10 BACKUP e restauração
- 11 Limitar conexões por cliente
- 12 Servidor PPPoE e Cadastro de Clientes
- 13 Amarrar faixa de IP no DHCP
- 14 Configurando o HOTSPOT
- 15 Configurações dos cartões Wireless
- 16 Entendendo cada função do menu do WINBOX
 - 16.1 SUB-MENU IP
 - 16.2 SUB-MENU ROUTING
 - 16.3 SUB-MENU SYSTEM
- 17 Instalação do MIKROTIK (Link Dedicado)
 - 17.1 Colocando ip Dedicado no cliente
 - 18 Configurando Servidor de Hora Automático
 - 19 Lista de SCRIPTS e AGENDAMENTOS úteis
 - 20 Configurando Liberação Automática de Banda por hora determinada
 - 21 LOADBALANCE - Visão Geral e Aplicação
 - 22 LOADBALANCE - IPD X IPD
 - 22.1 IPD(DEDICADO)
 - 22.2 Tratamento de portas
 - 23 LOADBALANCE - DIVIDINDO CARGA DE FORMA PERSONALIZADA ENTRE OS LINKS
 - 23.1 Tratamento de portas
 - 24 Mk como AP-bridge
 - 25 FIREWALL
 - 26 Gráficos em Tempo Real do Mikrotik
 - 27 Sobre o autor

Navegação

- Página principal
- Portal comunitário
- Eventos atuais
- Mudanças recentes
- Página aleatória
- Padrão

Pesquisa

Ferramentas

- Páginas afluentes
- Alterações relacionadas
- Páginas especiais
- Link permanente

Prefácio

ÚLTIMA ATUALIZAÇÃO: 25-03-2008

Restruturando este passo a passo, busco mais uma vez facilitar para os novatos deste excelente sistema, ensinando aqui mesmo, o básico para fazer um servidor mikrotik funcionar. Apresento o início, aquilo que não gostam de ensinar, sem omissão, sem enrolação. Para todos aqueles que querem aprender ou conhecer o mikrotik, aqui está a forma mais simples de "rodar" um servidor básico para aprendizagem ou mesmo para iniciar suas experiências. Lembre-se, estou dizendo o básico e isso não significa "o servidor". Para os "aventureiros", não recomendo colocar um servidor mikrotik, não configurado (com configurações básicas), em produção (em funcionamento no provedor). Tenho visto muita gente se decepcionando com o mikrotik, pelo simples fato de conseguir configurar o básico (que irei apresentar abaixo) e achar que é tudo. Um servidor, para rodar perfeitamente, precisa de no mínimo, configurações "obrigatórias", para evitar os velhos problemas conhecidos (perdas de pacotes, lentidão, etc). Falo eu CATVBRASIL (David), que já atendi mais de 500 empresas por todo o Brasil, Argentina, Chile, USA, Itália, Portugal e etc... Lembre-se, conhecimento é tudo... Estudem bastante e assim que possível, se especializem, façam treinamentos (existem vários), tirem suas dúvidas, participem do forum do under-linux (um dos mais completos do Brasil, em termos de mikrotik) e etc....

Busquei neste passo a passo, ajudar, de certa forma, aqueles que sentem dificuldade para realizar simples tarefas neste SO, Mikrotik. Basicamente a estrutura de todo este passo-a-passo é a fácil execução dos procedimentos, orientados por simples textos e imagens.

Agradeço a todos, que colaboraram direta ou indiretamente pela realização deste.

É expressamente proibida a VENDA ou qualquer outra forma de remuneração por meio deste material. É permitido divulgar, colaborar, inserir artigos ou correções neste material. Não esqueça de indicar o autor e a origem do material.

Desenvolvi este manual passo-a-passo, para auxiliar a todos iniciantes ou não deste excelente sistema operacional para roteadores.

ATENÇÃO: É GRÁTIS!! TUDO QUE ESTÁ AQUI É GRÁTIS!! DAI DE GRAÇA O QUE RECEBEU DE GRAÇA!!

Configurações iniciais

Parte retirada do treinamento a distância de mikrotik - CATVBRASIL

CONFIGURANDO UM SERVIDOR MIKROTIK BÁSICO (MÉTODO RELÂMPAGO)

Para configurar um servidor Mikrotik é muito fácil e rápido e você pode configurá-lo em 2 minutos no máximo!!! Consideramos que este servidor não terá placas wireless, apenas 2 placas ethernets (1 de entrada e 1 de saída).

Para colocar um servidor Mikrotik, precisamos configurar apenas:

IP>ADDRESS (define o endereço IP para a interface de entrada e de saída)

IP>ROUTES (define o gateway de saída)

IP>DNS (define o DNS primário e secundário)

REGRA DE NAT (IP>FIREWALL>NAT) (define o NAT mascarado)

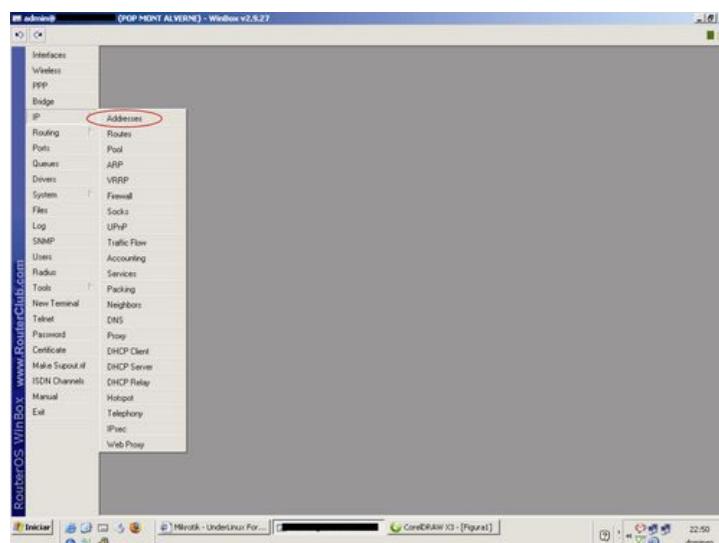
SOMENTE ESTAS CONFIGURAÇÕES SÃO NECESSÁRIAS PARA LEVANTAR UM SERVIDOR MIKROTIK BÁSICO. ESTE SERVIDOR JÁ ESTARÁ "FUNCIONANDO". NOTEM QUE EU DISSE "FUNCIONANDO" APENAS. FUNCIONAR NÃO É TUDO!!!

Configurando o Mikrotik (LINK ou MODEM ROTEADO)

Vamos lá mãos a obra!!

1º passo: **CONFIGURAR O ENDEREÇO (ADDRESS):**

Abra o menu IP > ADDRESS



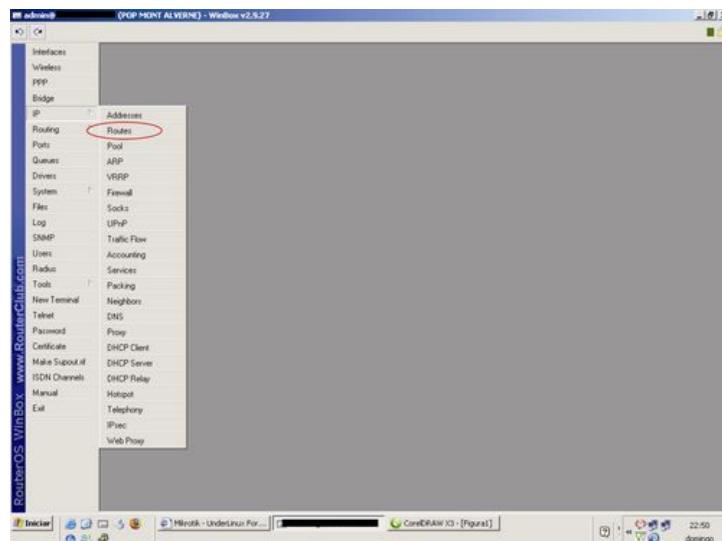
Crie um novo endereço IP (dentro da faixa do seu link ou modem, com a máscara de rede). Não esqueça de definir a interface correta a qual seu roteador ou modem está ligado, caso contrário não funcionará.



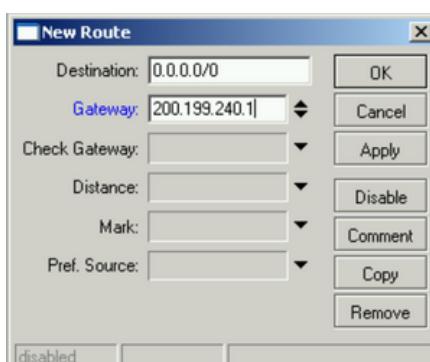
Após criar o endereço, e clicar em OK, automaticamente os endereços de network e broadcast serão preenchidos. Estes endereços são criados automaticamente de acordo com a máscara de rede.

2º passo: CONFIGURAR A ROTA DE SAÍDA (ROUTER):

Abra o menu IP > ROUTES

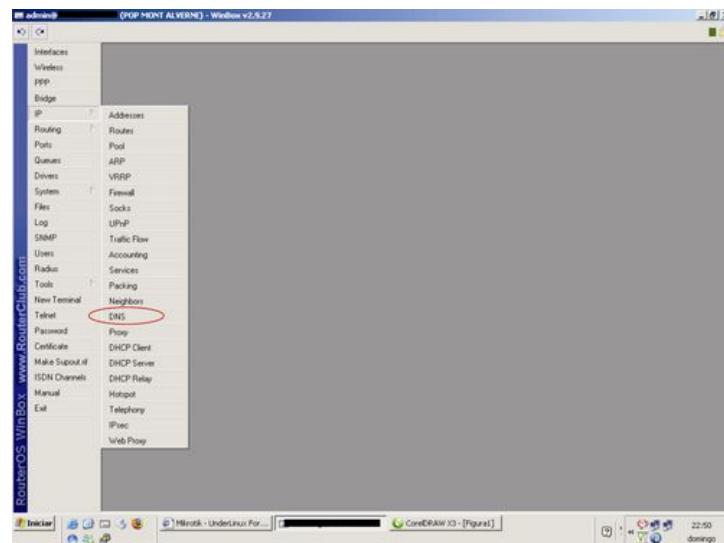


Crie uma nova rota, e defina apenas o endereço de gateway (este é o endereço do seu roteador ou modem). Não é necessário colocar a máscara de rede. Note que se estiver tudo certo, o campo "interface" desta nova regra, será preenchido automaticamente (com a interface onde está ligado seu modem ou roteador)



3º passo: CONFIGURAR O DNS:

Abra o menu IP > DNS

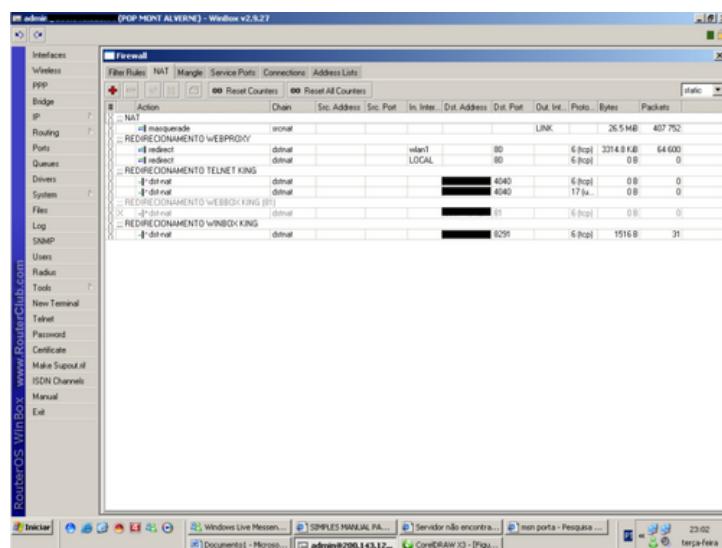


Abra o botão "settings" e configure o DNS primário e secundário do seu link.

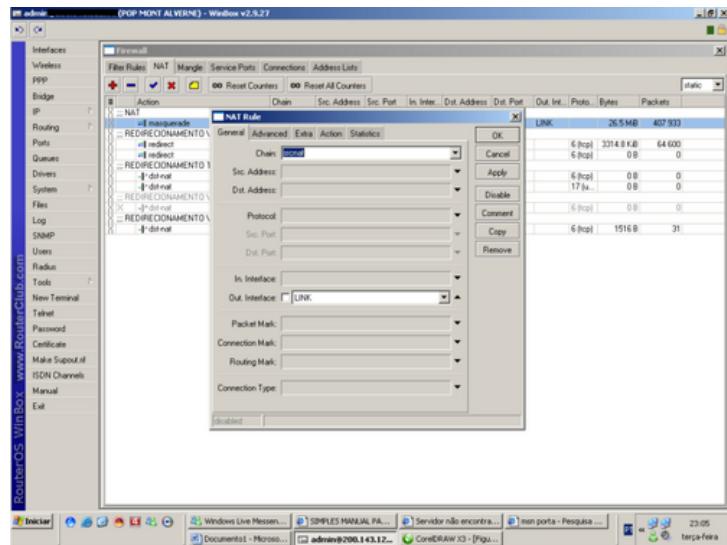


4º passo: CONFIGURANDO O NAT:

Abra o menu IP > FIREWALL > NAT

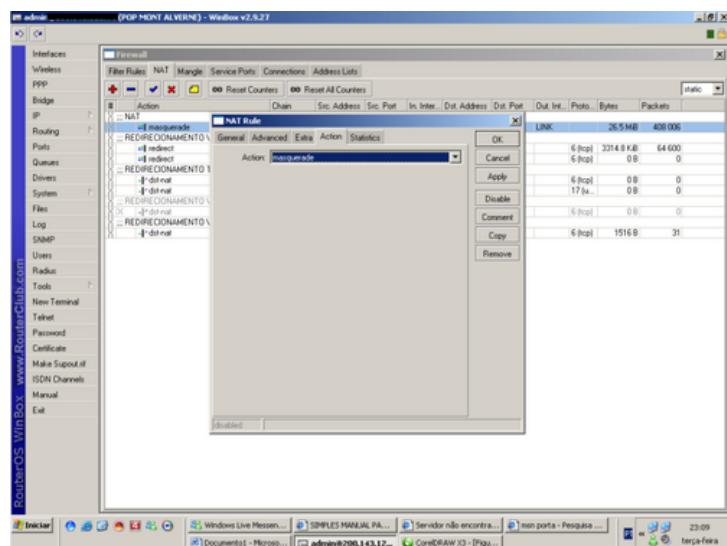


Crie uma nova regra



Em "CHAIN" escolha a opção "srcnat", em OUT INTERFACE (SAÍDA), não precisa escolher a interface de saída.

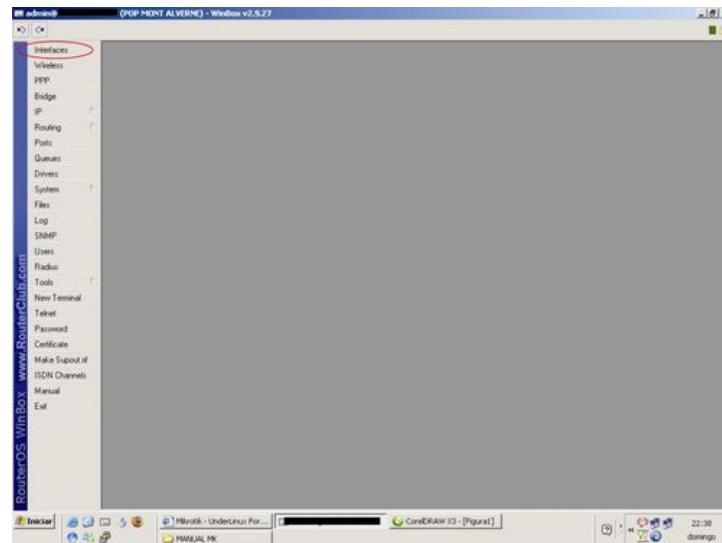
Na aba "ACTION", escolha a opção "MASQUERAD".



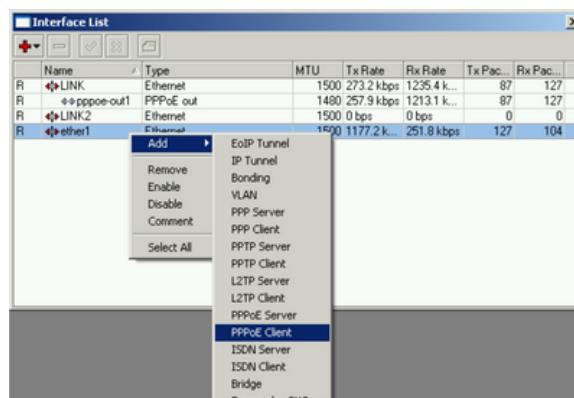
EXTRA

Passo adicional: **CONFIGURANDO UM MK COM ADSL - MODEM EM BRIDGE:**

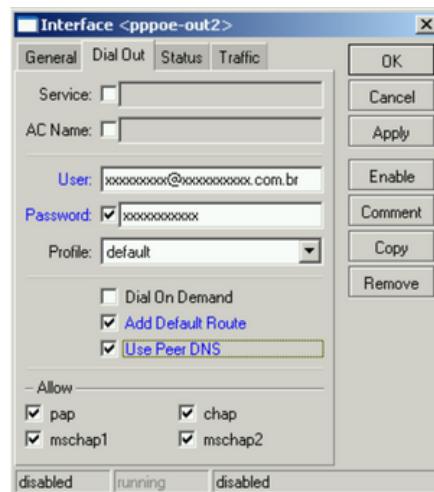
Abra o menu INTERFACE



Clique com o botão direito, em cima da interface do ADSL, e escolha a opção "PPPOE CLIENT"



Na aba DIAL OUT, configure os campos:



*USER: nome de usuário da cont ADSL (xxxxxxxx@operadora.com.br)

*PASSWORD: senha da conta ADSL

Deixar marcado as opções:

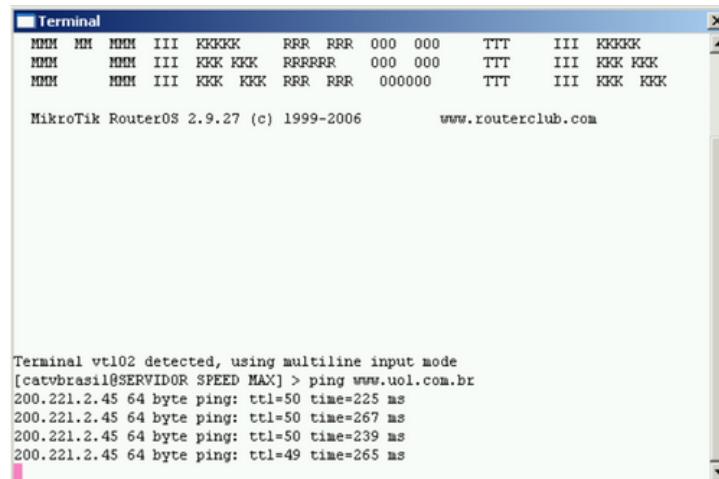
*ADD DEFAULT ROUTER

*USER PEER DNS

Mantendo estas duas opções marcadas, você não irá precisar configurar o IP e a ROTA (deve-se pular os passos 1 e 2 deste artigo). Dando um OK, automaticamente o discador PPPoE irá se conectar e já estará pronto para trabalhar.

5º passo: CERTIFICANDO QUE TUDO ESTÁ FUNCIONANDO PERFEITAMENTE:

Bom, como saber se tudo que foi configurado está funcionando perfeitamente? No winbox, há uma opção chamada "new terminal" que como o próprio nome sugere, é um terminal de comando do mikrotik. Lá temos vários comandos (podemos verificar, apenas apertando "?", dentre eles o conhecido "ping". Para testar a funcionalidade de nosso servidor mikrotik, basta "pingar" um endereço qualquer (www.uol.com.br) e verificar se há resposta. Havendo resposta, nosso servidor já está "navegando" na internet, caso não haja resposta, significa que há algum problema na configuração (bastando iniciar novamente este manual e verificar onde está acontecendo o erro)... Podemos também através do comando de ping, verificar o "estado" de nosso roteador, link, dns, etc etc...



```
Terminal
NMNM NM NMNM IIII KKKKKK RRRR RRRR 000 000 TTT IIII KKKKKK
NMNM NMNM IIII KKK KKK RRRRRR 000 000 TTT IIII KKK KKK
NMNM NMNM IIII KKK KKK RRR RRR 000000 TTT IIII KKK KKK

MikroTik RouterOS 2.9.27 (c) 1999-2006 www.routerclub.com

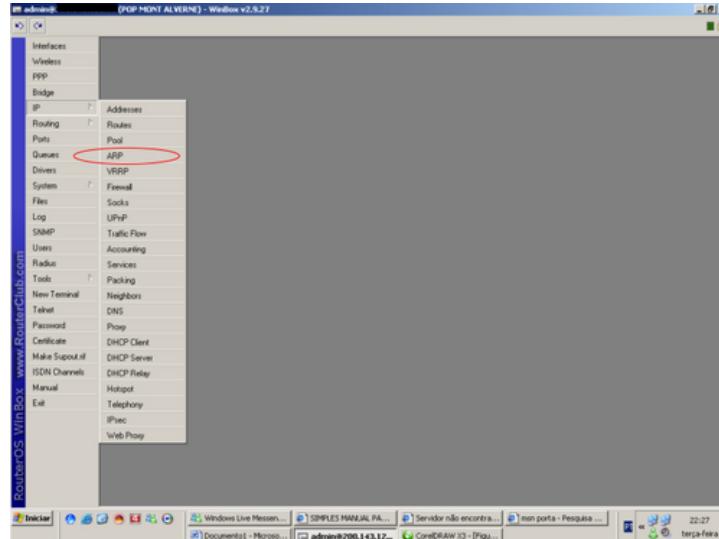
Terminal vt102 detected, using multiline input mode
[catvbrasil@SERVIDOR SPEED MAX] > ping www.uol.com.br
200.221.2.45 64 byte ping: ttl=50 time=225 ms
200.221.2.45 64 byte ping: ttl=50 time=267 ms
200.221.2.45 64 byte ping: ttl=50 time=239 ms
200.221.2.45 64 byte ping: ttl=49 time=265 ms
```

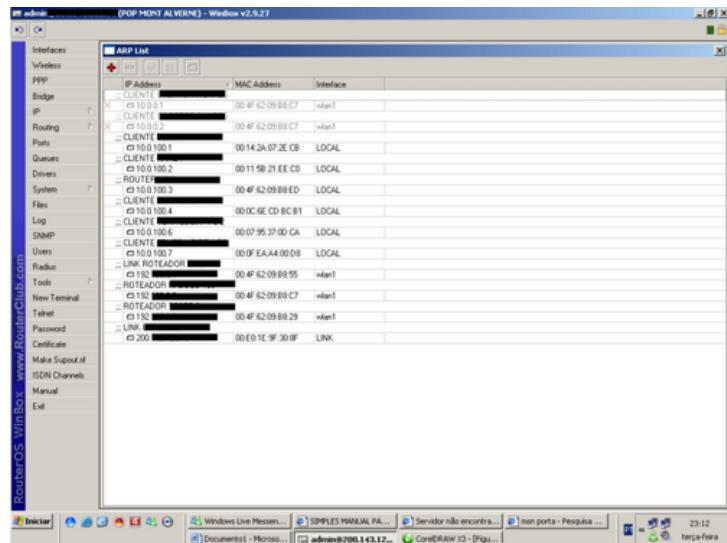
A PROPOSTA DOS TÓPICOS

Abaixo, apresento várias soluções e regras procuradas por muitos, de uma forma simples e descomplicada. A proposta abaixo é resolver algumas das dúvidas cotidianas. Já vi muita gente falando no forum que configurou seu servidor com as regras e soluções abaixo e não ficou "aquele" servidor. Quero lembrar mais uma vez, que as regras e soluções apresentadas abaixo, funcionam perfeitamente, mas não são a solução completa. Elas resolvem algumas coisas, mas para um servidor funcionar perfeitamente, é necessário outras configurações...

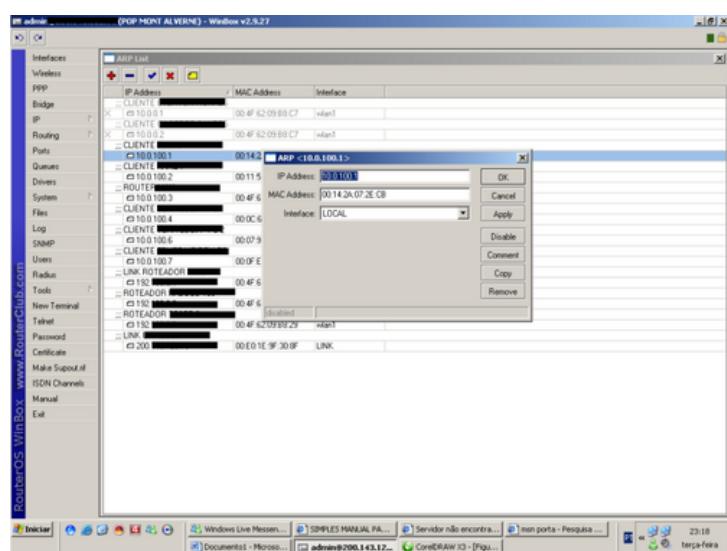
Como amarrar IP/MAC

Acesse o menu IP, ARP





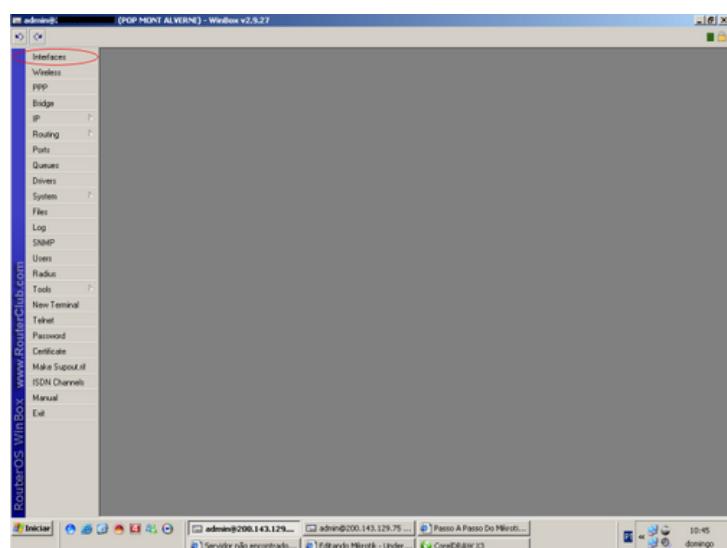
Crie uma nova "ARP" (botão "+")

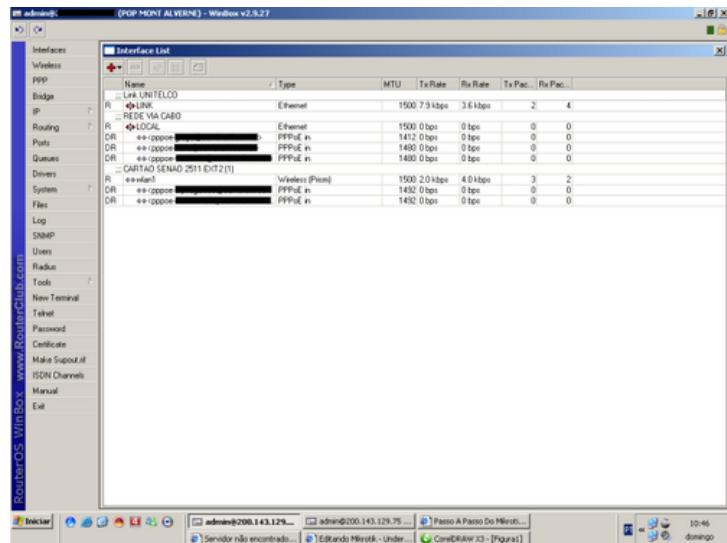


Digite o IP da máquina a qual quer amarrar, o MAC ADDRESS e a INTERFACE a qual a máquina será ligada.

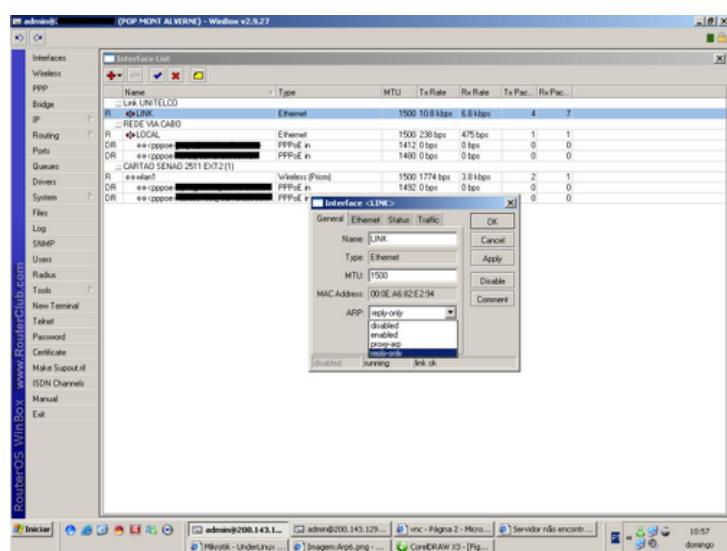
Em COMMENT, dê o nome desta ARP, como no exemplo acima.

Acesse o menu, INTERFACES



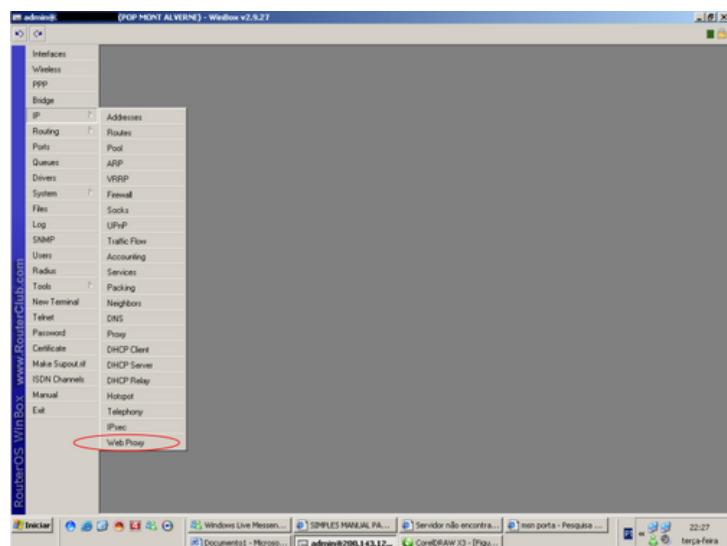


Como último procedimento, você deve habilitar em sua interface, o ARP para reply-only.

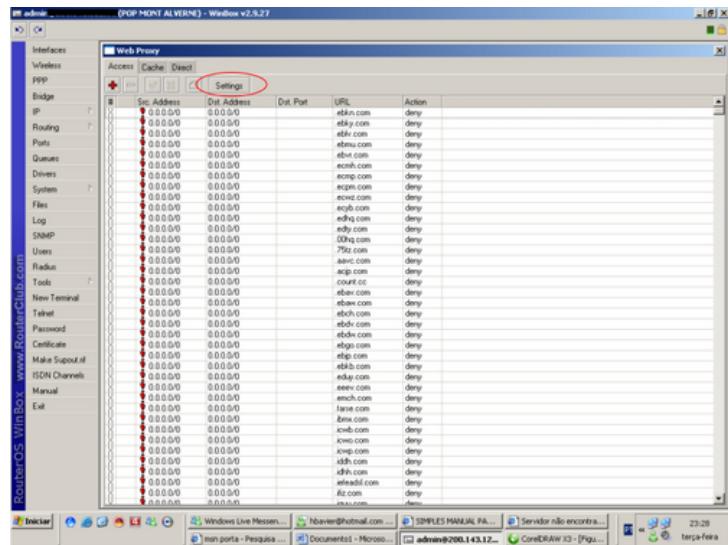


Configurando o WEB-PROXY

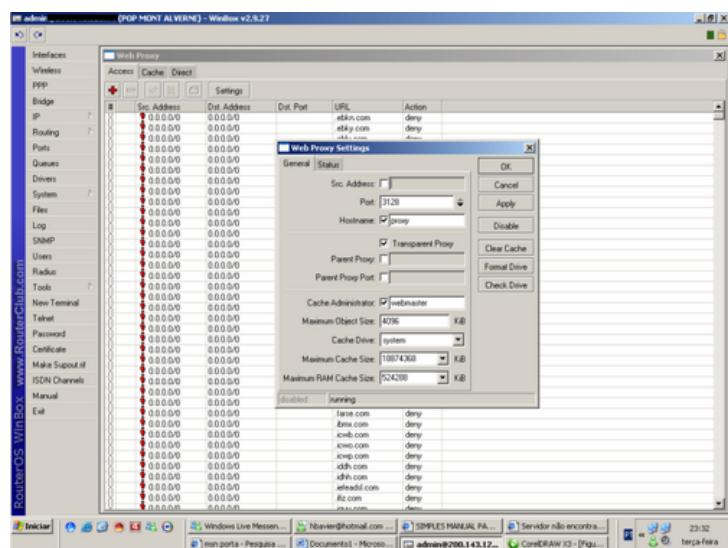
Acesse o menu IP, WEB-PROXY



Clique no botão "SETTINGS"



Deverá aparecer uma tela como esta



Configure de acordo com suas necessidades...

SRC-ADDRESS = Deixe em branco

PORT = Escolher a porta do seu web-proxy

TRANSPARENT PROXY = Deixe marcado para proxy transparente

PARENT PORT = Deixe em branco

PARENT PROXY PORT = Deixe em branco

CACHE ADMINISTRATOR = Deixe como está

MAXIMUM OBJECT SIZE = Deixe como está

CACHE DRIVE = Deixe como "system"

MAXIMUM CACHE SIZE = Define o tamanho do seu cache, varia de acordo com o tamanho do seu HD

MAXIMUM RAM CACHE SIZE = Define o tamanho máximo de sua memória RAM para o cache

Após configurar estes parâmetros, aperte a tecla "ENABLE"

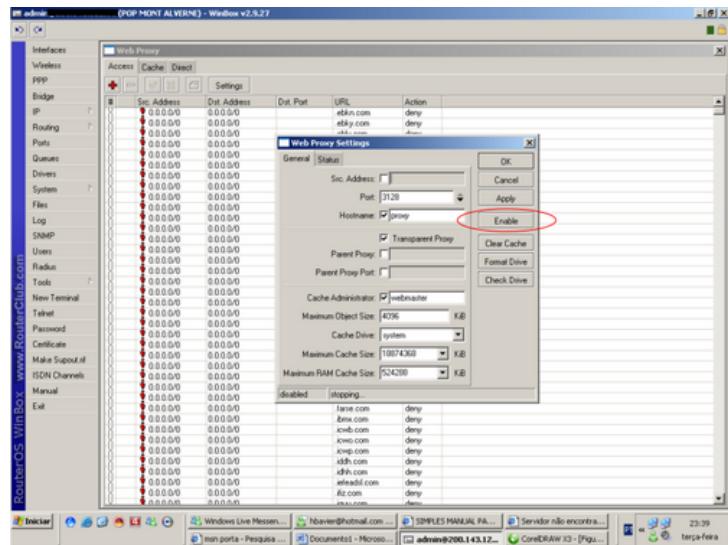
NÃO se deve fazer CACHE de PÁGINAS DINÂMICAS (bancos, globo.com, etc etc...)

Duas regras devem ser colocadas na aba "CACHE" do Web-Proxy para esse efeito:

IP / WEB-PROXY / CACHE

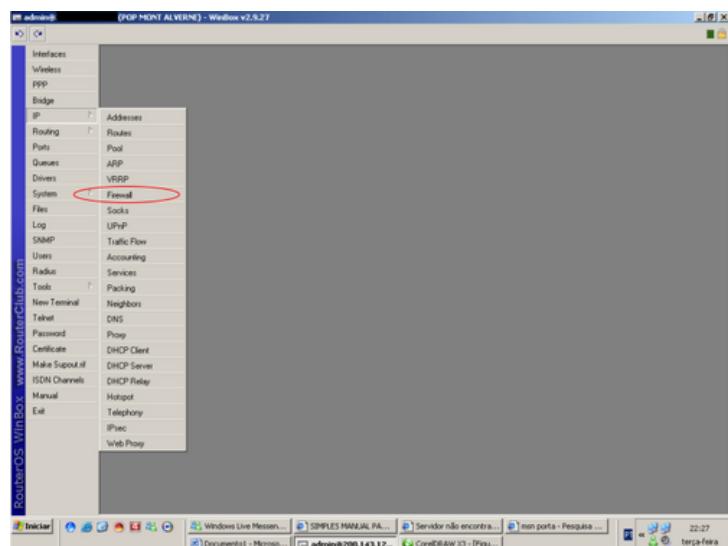
Crie uma nova regra (botão "+")

```
add url=":cgi-bin \?" action=deny comment="no cache dynamic http pages" disabled=no
add url="https://" action=deny comment="no cache dynamic https pages" disabled=no
```

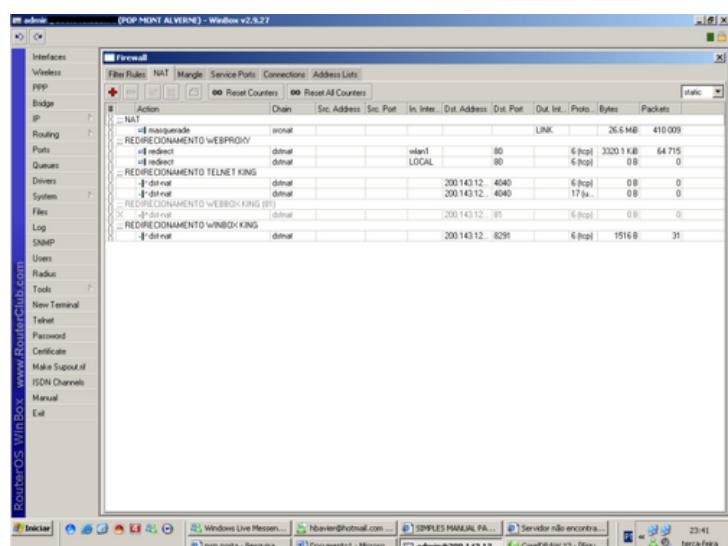


O segundo passo para nosso WEB-PROXY funcionar é criar um regra para redirecionar as requisições primeiramente para o proxy, para isso:

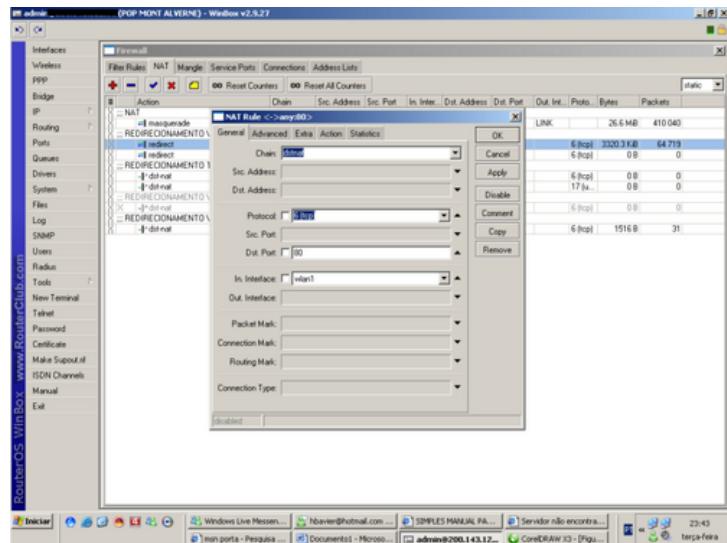
Acesse IP, FIREWALL



Escolha a aba "NAT"



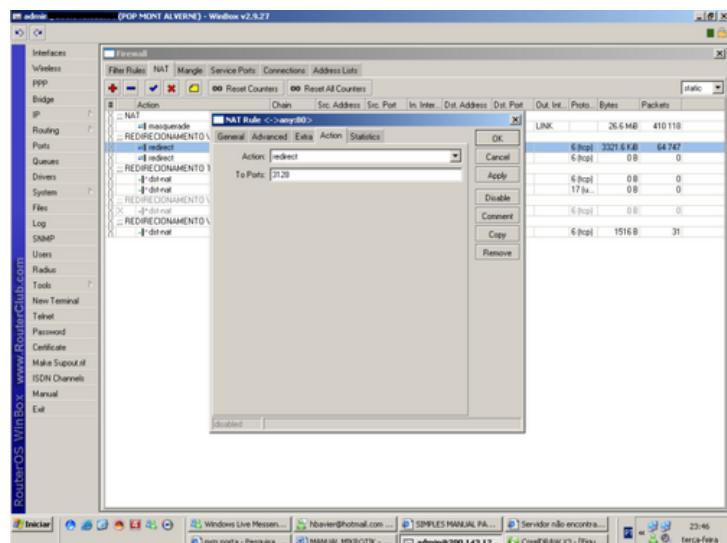
Crie uma nova regra (botão "+")



Crie a regra da seguinte forma:

```
*CHAIN = DSTNAT
*PROTOCOL = 6 (TCP)* <r> *DST. PORT = 80
*IN. INTERFACE = INTERFACE DOS CLIENTES
```

Vá na aba "ACTION"

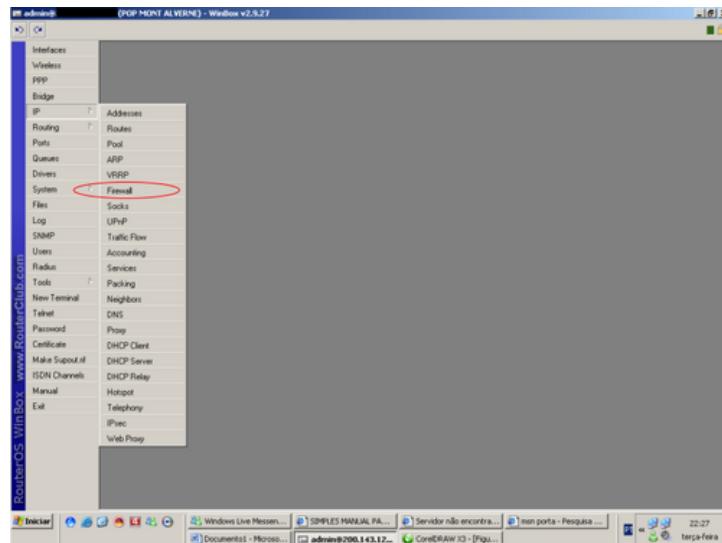


Escolha em "ACTION" a opção "REDIRECT" e em "TO PORT" escolha a porta do seu proxy (definida anteriormente no começo deste tópico).

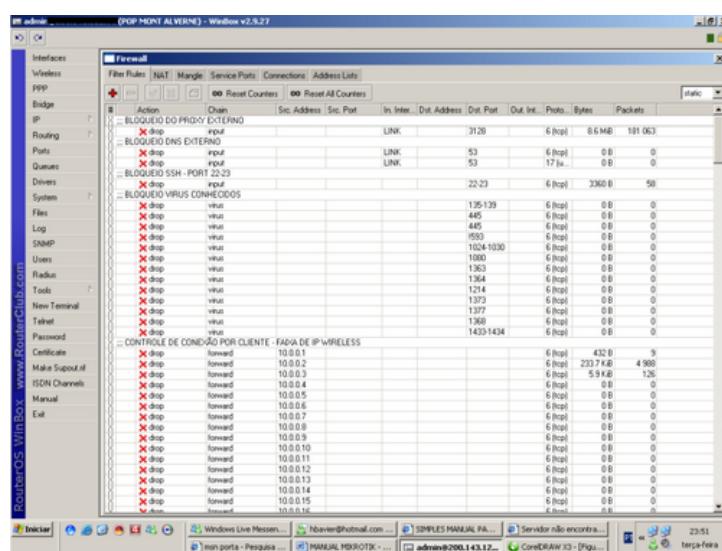
É interessante realizar uma regra para cada interface de assinantes. Neste caso como possuo duas interfaces (LAN/WLAN), criei duas regras, uma para cada interface.

É importante criar uma regra de bloqueio externo ao web-proxy. Caso você não crie esta regra, ela sobreencarregará o seu proxy, travando até mesmo seu serviço. Siga abaixo:

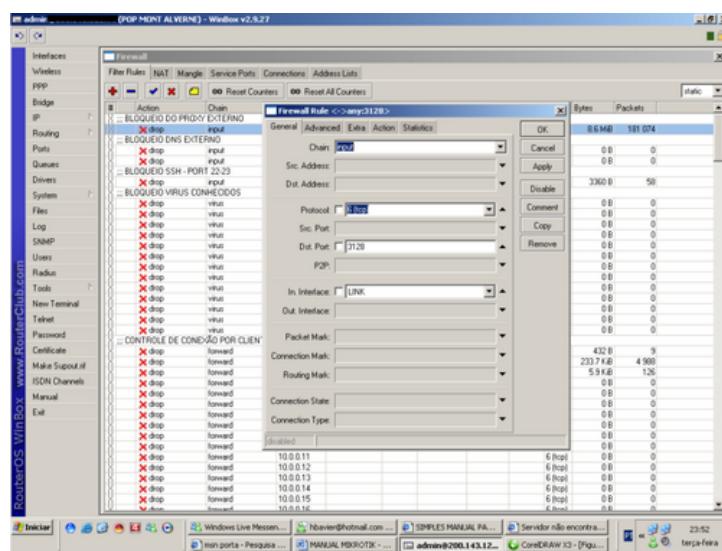
Acesse o menu IP, FIREWALL



Acesse a aba "FILTER RULES"



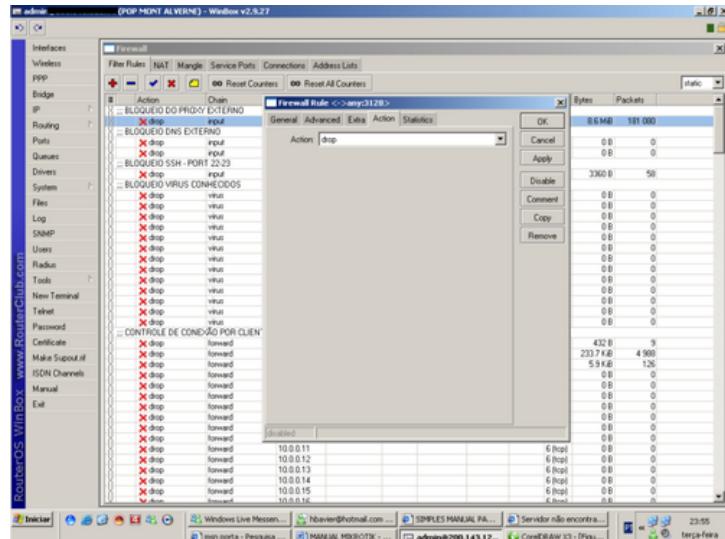
Crie uma nova regra (botão "+")



Segue a configuração:

CHAIN = INPUT
*PROTOCOL = 6 (TCP)
*DST PORT = PORTA DO SEU WEB-PROXY
*IN. INTERFACE = INTERFAC DE SAÍDA (LINK DE INTERNET)

Acesse a aba "ACTION"



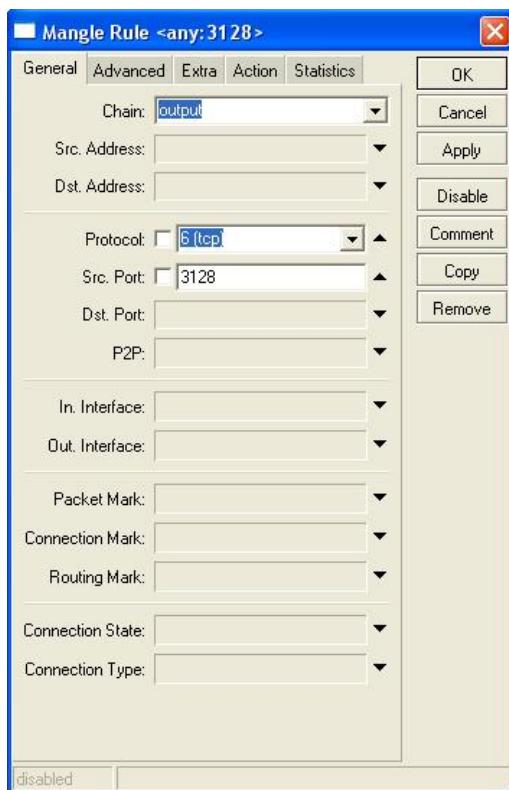
Em "ACTION" escolha a opção "drop".

EM COMMENT você pode dar um nome a regra, que neste caso foi apelidado de "BLOQUEIO DO PROXY EXTERNO".

Com este passo-a-passo, você criou e habilitou o seu web-proxy e também tornou mais eficiente, bloqueando o acesso externo a ele.

CACHE FULL

IP > FIREWALL > MANGLE > +



Mangle Rule <any:3128>

General Advanced Extra Action Statistics

Src. Address List: [dropdown]
Dst. Address List: [dropdown]

Content: X-Cache: HIT

Connection Bytes: [dropdown]
MAC Address: [dropdown]

Out. Bridge Port: [dropdown]
In. Bridge Port: [dropdown]

IPv4 Options:
TOS: [dropdown]
TCP MSS: [dropdown]
Packet Size: [dropdown]
Random: [dropdown]

TCP Flags
ICMP Options

disabled

OK Cancel Apply Disable Comment Copy Remove

Mangle Rule <any:3128>

General Advanced Extra Action Statistics

Action: mark connection
New Connection Mark: Cache-Connection
 Passthrough

disabled

OK Cancel Apply Disable Comment Copy Remove

Mangle Rule

General Advanced Extra Action Statistics

Chain: output

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

P2P:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark: Cache-Connection

Routing Mark:

Connection State:

Connection Type:

disabled

OK Cancel Apply Disable Comment Copy Remove

Mangle Rule

General Advanced Extra Action Statistics

Action: mark packet

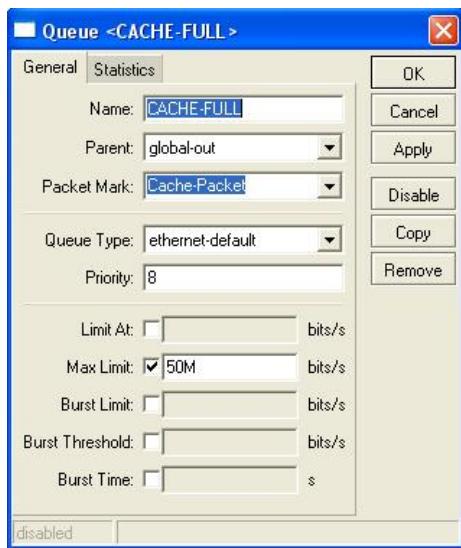
New Packet Mark: Cache-Packet

Passthrough

disabled

OK Cancel Apply Disable Comment Copy Remove

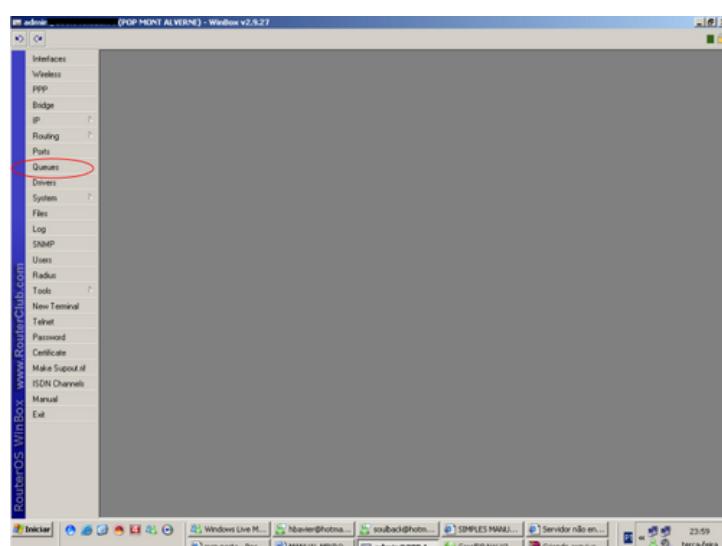
QUEUES > +



Eu Explico depois

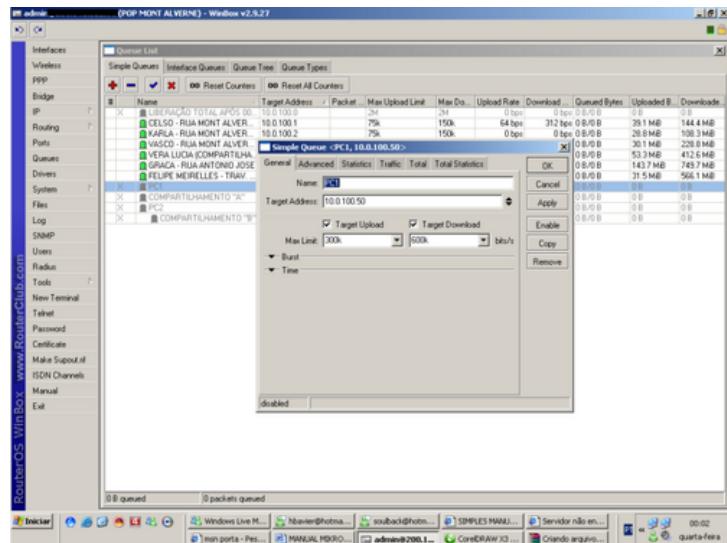
Controle de banda

Acesse no menu, QUEUE



Name	Target Address	Packet At	Max Upload Limit	Max Do	Upload Rate	Download	Queued Bytes	Uploaded B	Download B
LIBERACAO TOTAL AP01 90	19.0.100.0	24	24	0 bps	0 bps	0 b/s	0 B	0 B	0 B
CELSO - RUA MONT ALVER.	19.0.100.1	75k	150k	60 bps	480 bps	0 b/s	144.4 MB	0 B	0 B
PC1 - RUA MONT ALVER.	19.0.100.2	75k	150k	60 bps	480 bps	0 b/s	28.8 MB	0 B	0 B
VASCO - RUA MONT ALVER.	19.0.100.3	300k	600k	0 bps	0 bps	0 b/s	30.1 MB	220.6 MB	0 B
VERA LUCIA COMPARTILHA.	19.0.100.4,10.0.	300k	600k	0 bps	0 bps	0 b/s	53.1 MB	412.6 MB	0 B
GRACA - RUA ANTONIO JOSE	19.0.100.5	300k	600k	480 bps	568 bps	0 b/s	143.7 MB	745.6 MB	0 B
FELIPE MERILLELES - TRAV.	19.0.100.7	75k	150k	0 bps	0 bps	0 b/s	31.5 MB	566.1 MB	0 B
PC2 - RUA MONT ALVER.	19.0.100.40	300k	600k	0 bps	0 bps	0 b/s	0 B	0 B	0 B
COMPARTILHAMENTO "A"	19.0.100.50,10.0.	300k	600k	0 bps	0 bps	0 b/s	0 B	0 B	0 B
PC2	19.0.100.51	300k	600k	0 bps	0 bps	0 b/s	0 B	0 B	0 B
COMPARTILHAMENTO "B"	19.0.100.50	300k	600k	0 bps	0 bps	0 b/s	0 B	0 B	0 B

Crie um novo controle de banda (botão "+")



Configure como abaixo:

- *NAME = Nome do "dono" da configuração – Nome do cliente
- *TARGET ADDRESS = IP que irá controlar a banda
- *TARGET UPLOAD – MAX LIMIT = Taxa de upload (Colocar "k" Minúsculo no final)
- *TARGET DOWNLOAD – MAX LIMIT = Taxa de download (Colocar "K" minúsculo no final)

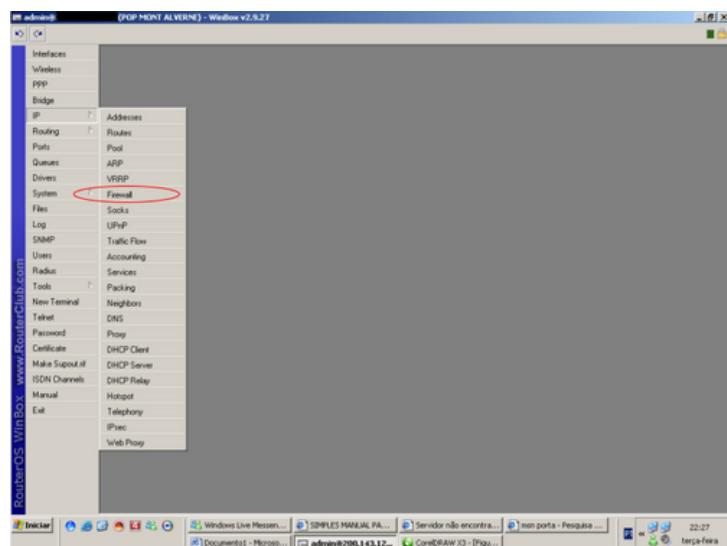
Controle de banda concluído. Somente isso é necessário.

Acesso remoto a outro Mikrotik

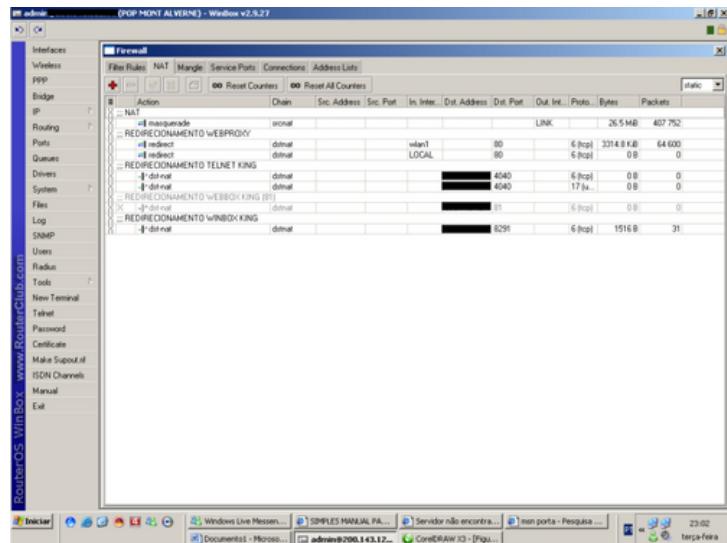
PS: Para ter acesso a rádios AP em sua rede, você deverá habilitar a função “ATIVAR GERENCIAMENTO PELA PORTA WAN” do seu rádio.

Simples. Basta criar três regras no firewall. Segue abaixo:

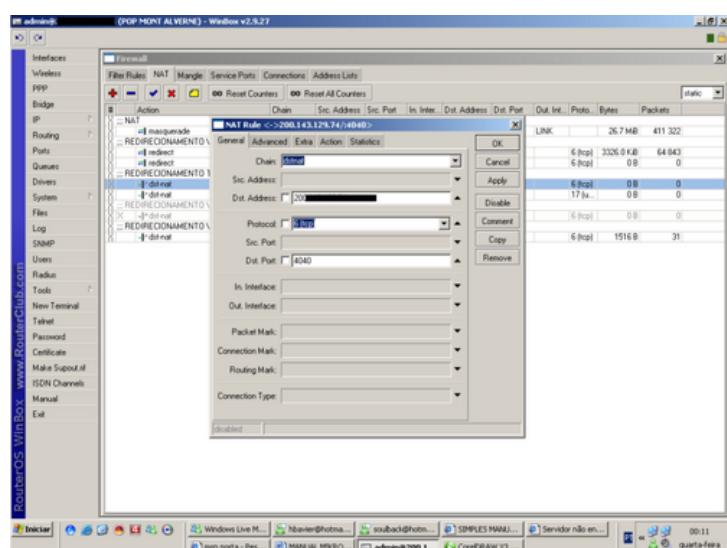
Acesse o menu IP, FIREWALL



Clique na aba “NAT”



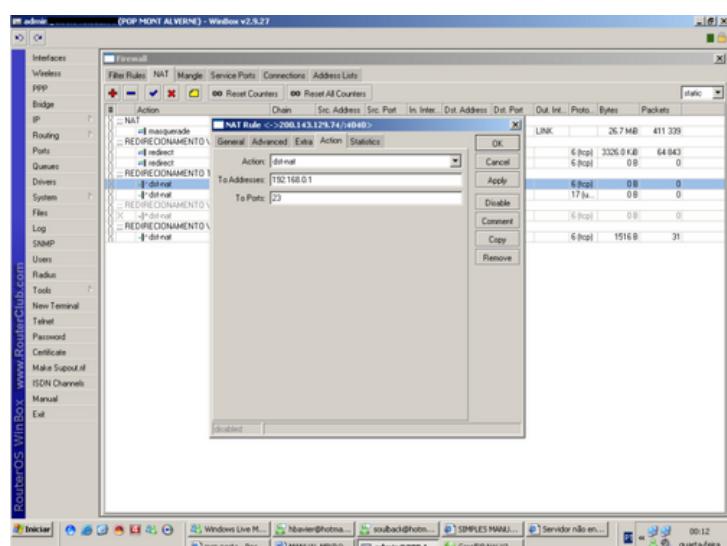
Crie uma nova regra (botão "+")



Siga os procedimentos de configuração abaixo:

- *CHAIN = DSTNAT
- *DST. ADDRESS = Endereço IP do MK principal
- *PROTOCOL = 6 (TCP)
- *DST. PORT = 4040 (Porta padrão do Firewall)

Abra a aba "ACTION"



Siga as configuração abaixo:

*ACTION = DSTNAT

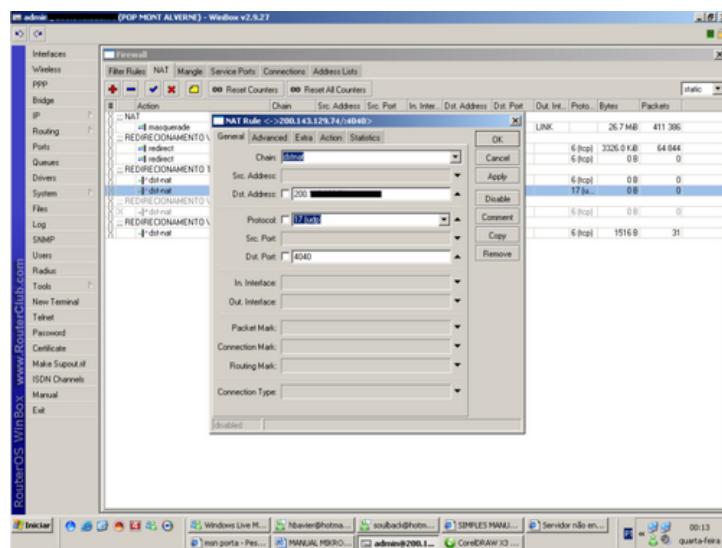
*O ADDRESS = Endereço IP do AP que deseja acessar.

*TO PORT = Porta de acesso do AP

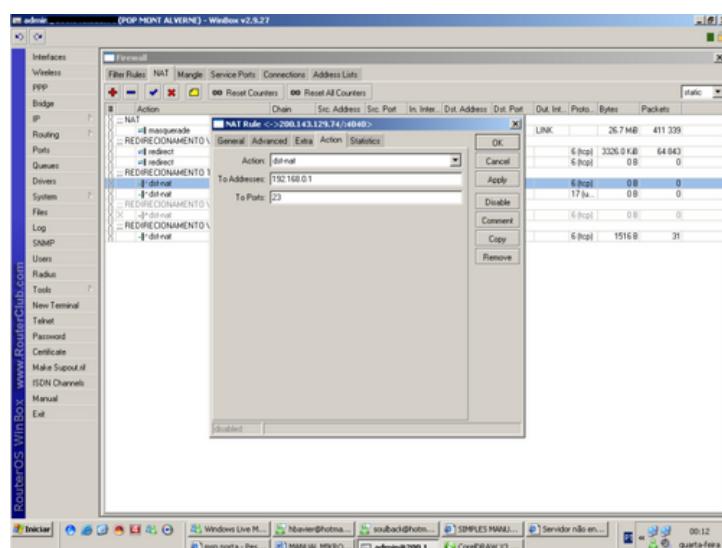
Confirme e dê um nome em COMMENT para sua regra.

Se o AP que você deseja acessar for um outro AP Mikrotik, você deverá escolher a porta padrão TELNET (23). Se for um AP rádio, escolha a porta padrão HTTP (80) ou outra escolhida no rádio.

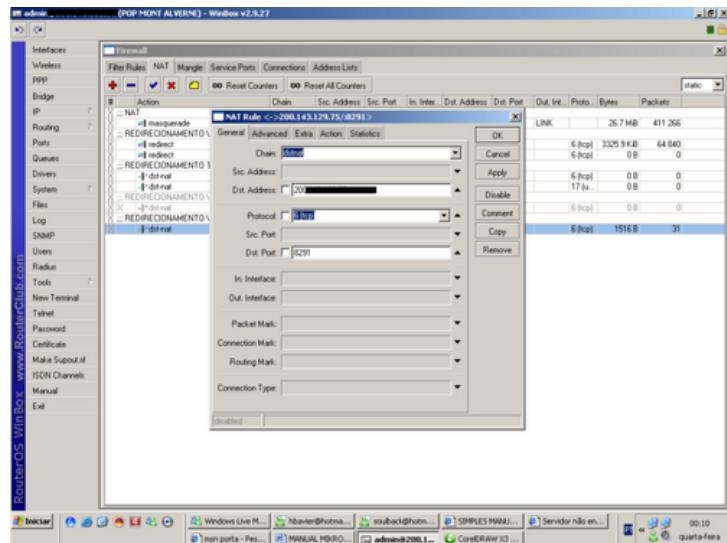
Você deverá criar uma segunda regra:



Repetindo o mesmo procedimento acima, mas desta vez, alterando apenas o protocolo para 17 (UDP).



Salve tudo e crie a terceira regra.

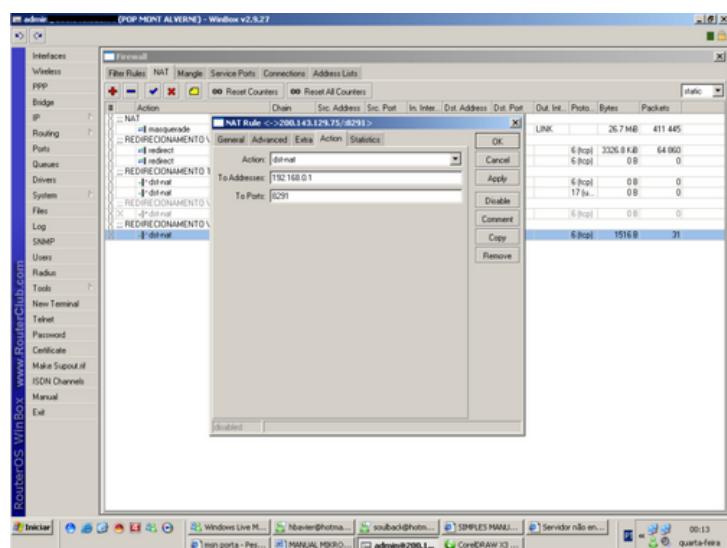


Nesta regra, você irá definir um endereço IP para seu AP. Verifique com sua operadora quais endereços IP você tem e quais estão sobrando.

Cria a regra como abaixo:

- *CHAIN = DSTNAT
- *DST. ADDRESS = Endereço IP livre, a qual será atribuído ao seu rádio ou AP MIKROTIK.
- *PROTOCOL = 6 (TCP)
- *DST. PORT = Porta de acesso ao AP ou rádio. Se você for acessar outro AP pelo WINBOX, selecione a porta 8291 (PORTA PADRÃO DO WINBOX), se você for acessar um rádio, a porta padrão é a 80 ou outra pré-definida do rádio.

Abra a aba "ACTION"



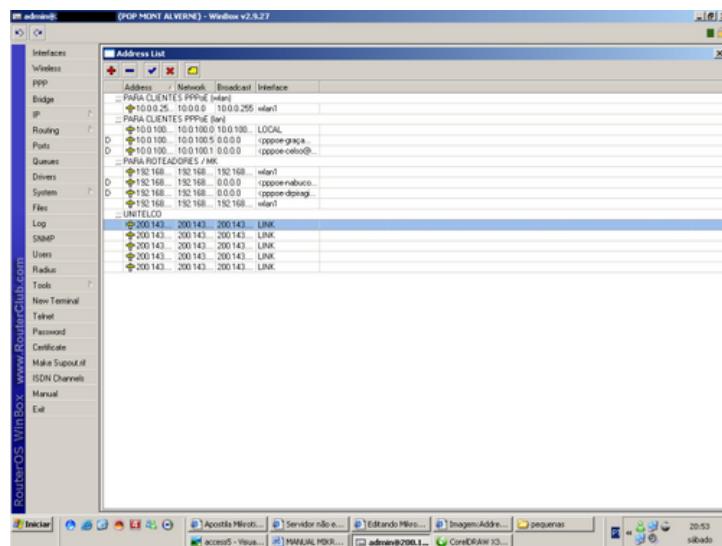
Nesta aba você irá configurar da seguinte forma:

- *ACTION = DST-NAT
- *TO ADDRESS = Endereço IP do seu rádio ou AP (endereço de IP da rede interna)
- *TO PORT = Porta padrão para o WINBOX (AP MIKROTIK) ou porta padrão para rádios, porta 80 (ou outra definida).

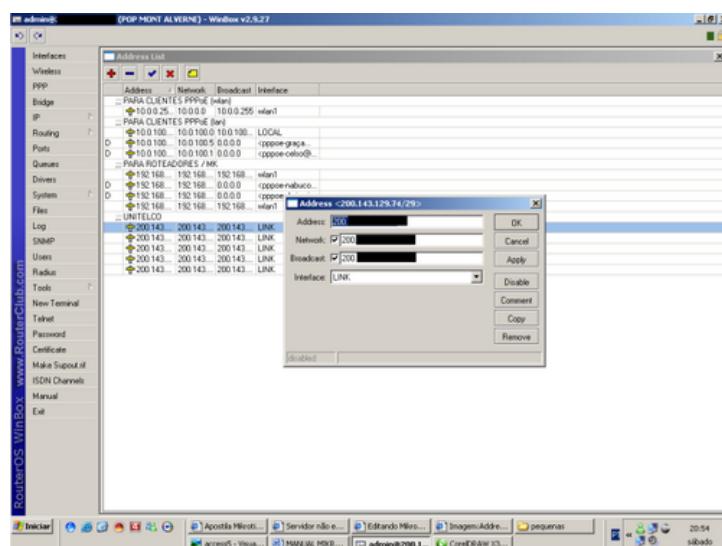
Pronto!!! Para ter acesso a AP MIKROTIK, vá no WINBOX, digite o IP válido definido acima, senha e login. Para ter acesso a rádios, abra o internet explorer, digite o endereço IP válido definido acima... Abrirá um box para senha e login... Digite-as e seja feliz!!!

Não esquecer de adicionar os IP's válidos que serão usados para os rádios na ADDRESS LIST. Como??

Acesse o menu IP, ADDRESS LIST



Crie uma nova lista de endereços (botão "+")

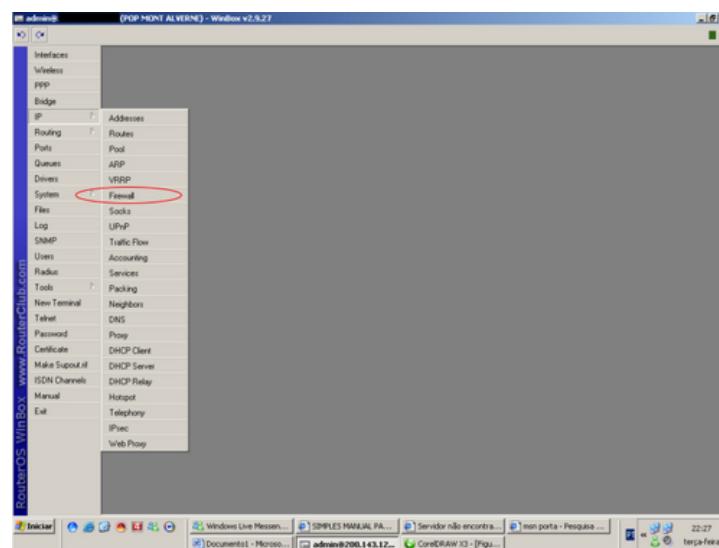


De acordo com seu link, coloque o novo IP válido, o Ip da "NETWORK e o IP do BROADCAST. Defina também a interface (Neste caso, a interface de saída da internet)

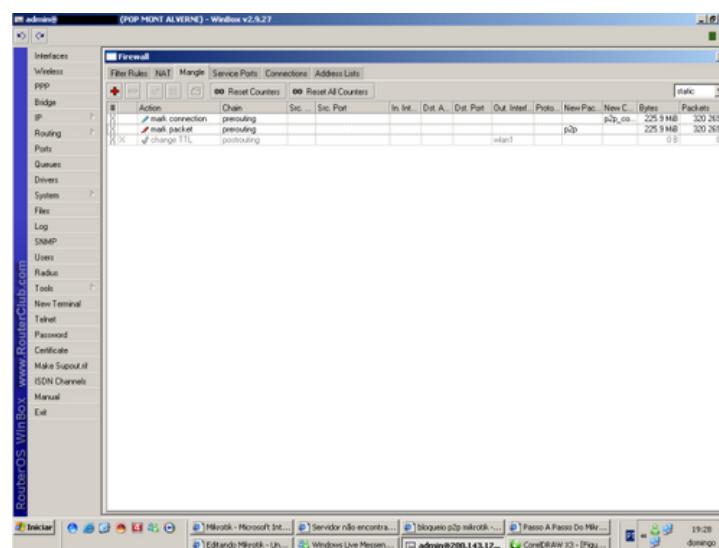
Controle P2P (MUITO BOM)

Aqui você irá aprender a controlar (shape) o tráfego P2P, marcando pacotes, facilmente. Basta apenas 4 regrinhas, 2 no firewall e 2 no queue. Então vamos lá:

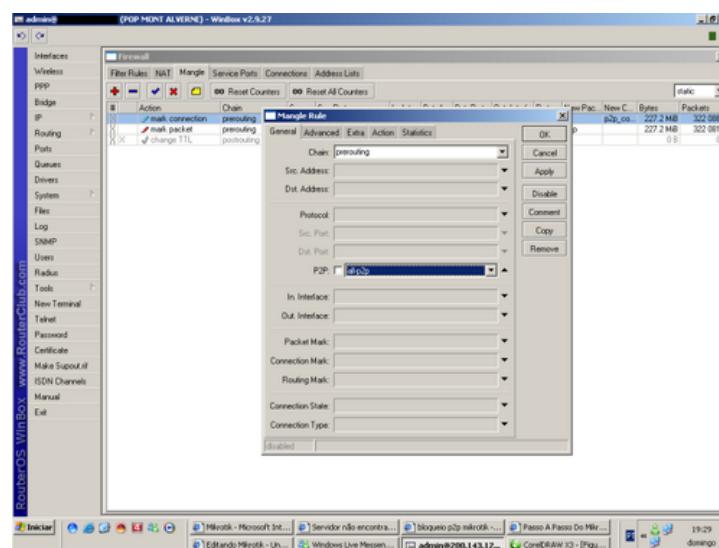
Acesse o menu IP, FIREWALL



Escolha a aba, MANGLE

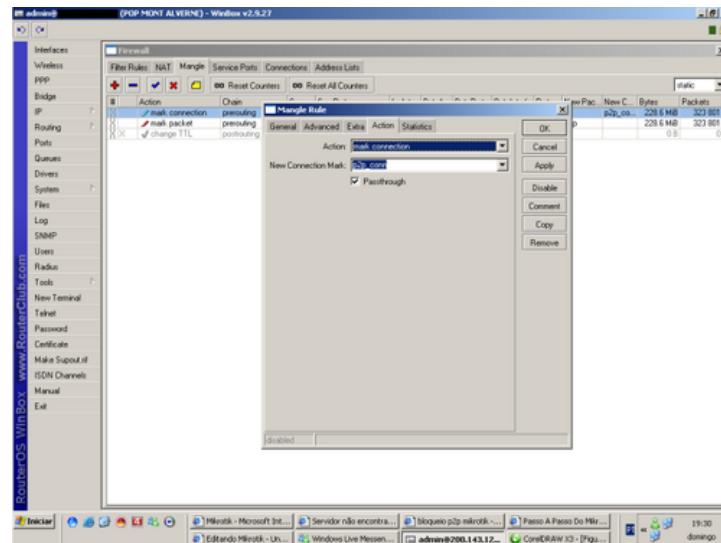


Crie uma nova regra (botão "+")



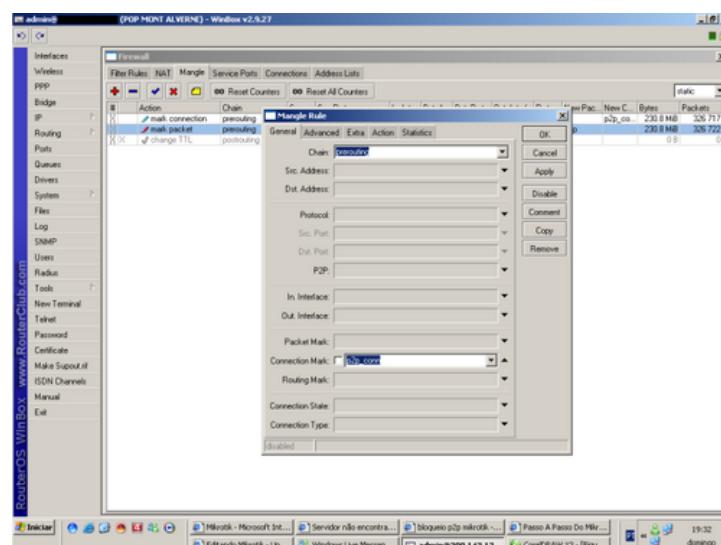
No campo "CHAIN", escolha "PREROUTING". No campo "P2P", escolha "all-p2p".

Abra a aba "ACTION"



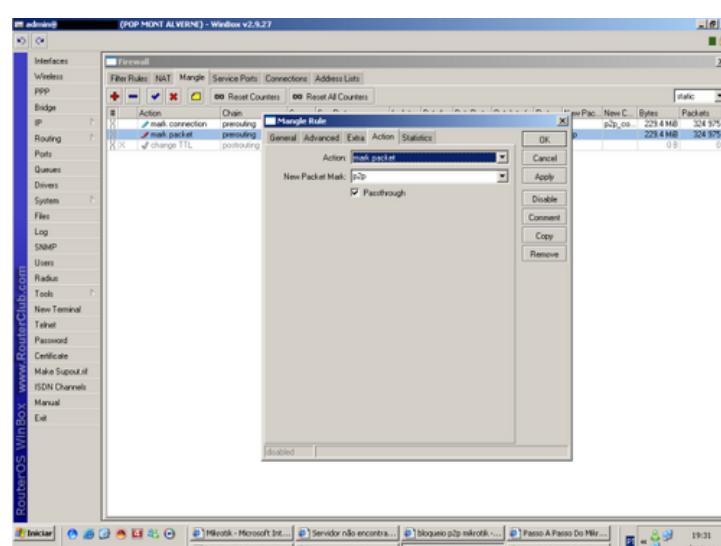
No campo "ACTION", escolha "MARK CONNECTION". No campo "NEW CONNECTION MARK", dê um nome a sua nova marcação de pacotes (no exemplo, demos o nome de "p2p_conn"). Deixe a opção "PASSTHROUGH" ligada. Confirme.

Crie uma nova regra (botão "+")



No campo "CHAIN", escolha "PREROUTING". No campo "CONNECTION MARK" escolha a opção com o nome definido acima (no nosso caso foi "p2p_conn").

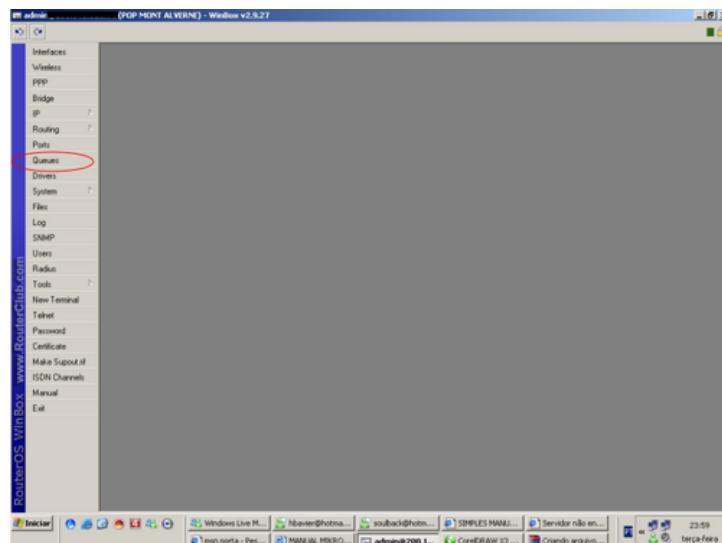
Abra a aba "ACTION"



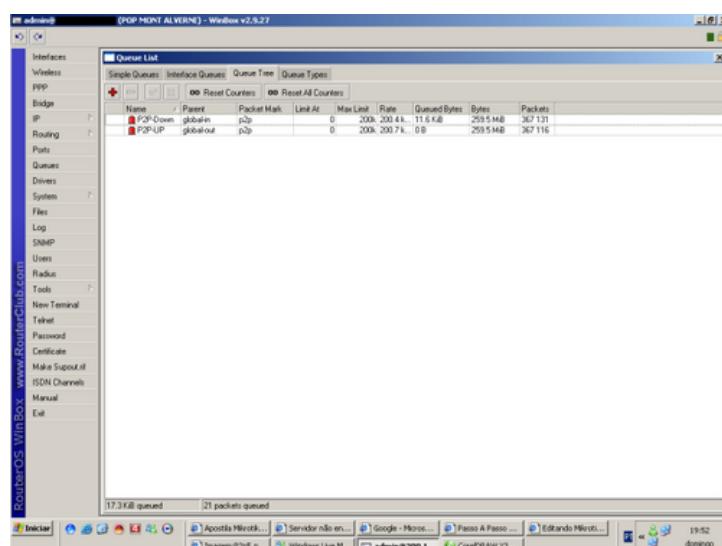
No campo "ACTION", escolha "MARK PACKET", no campo "NEW PACKET MARK", defina outro nome (no nosso caso, ficou como "p2p"). Confirme.

Após criar estas duas regras no firewall, será necessário criar mais duas regras no queue. Para isso:

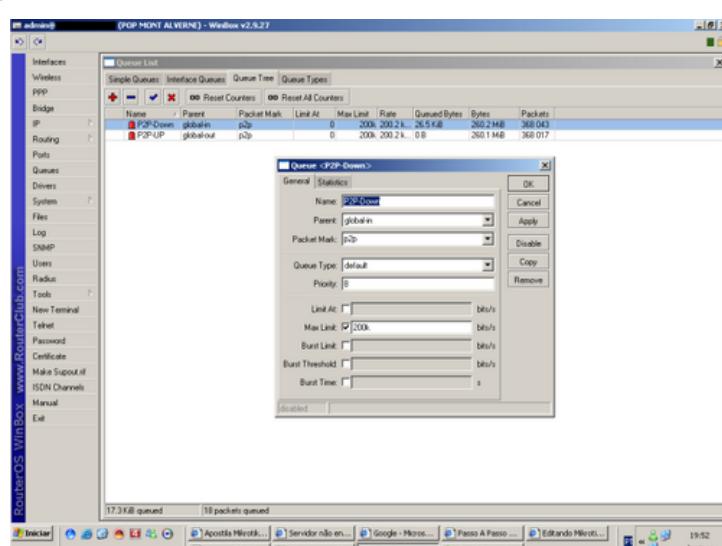
Abra o menu, QUEUE



Abra a aba "QUEUE TREE"



Crie uma nova regra (botão "+")



Defina de acordo com a figura.

*NAME = Defina um nome para a regra

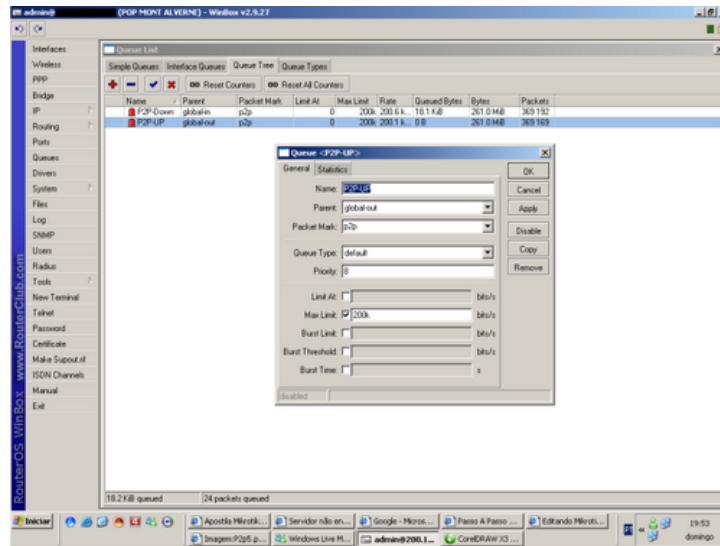
*PARENT = Escolha "GLOBAL-IN"

*PACKET MARK = Escolha a opção do nome escolhido acima. Aparecerá aqui o nome definido na regra do firewall

*QUEUE TYPE = DEFALT
 *PRIORITY = 8
 *MAX LIMIT = Define o limite máximo de banda reservado para o P2P. No nosso caso, é um total de 200k para p2p

Confirme...

Crie uma nova regra (botão "+")



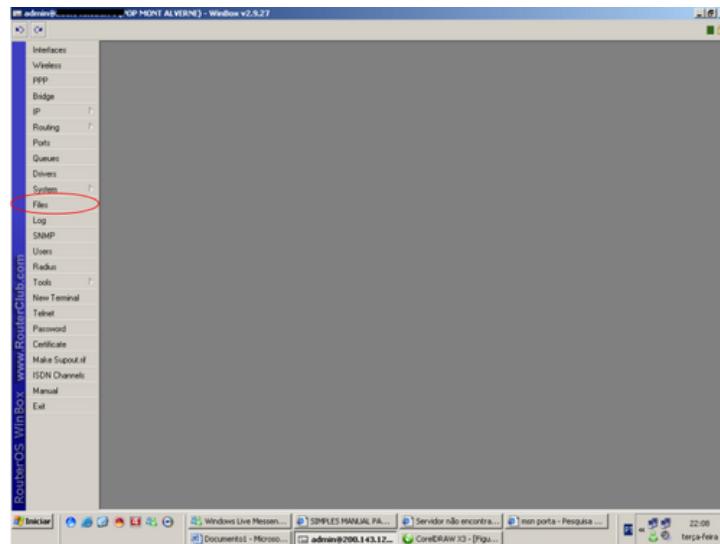
Defina de acordo com a figura.

*NAME = Defina um nome para a regra
 *PARENT = Escolha "GLOBAL-OUT"
 *PACKET MARK = Escolha a opção do nome escolhido acima. Aparecerá aqui o nome definido na regra do firewall
 *QUEUE TYPE = DEFALT
 *PRIORITY = 8
 *MAX LIMIT = Define o limite máximo de banda reservado para o P2P. No nosso caso, é um total de 200k para p2p
 align="justify">>Confirme...

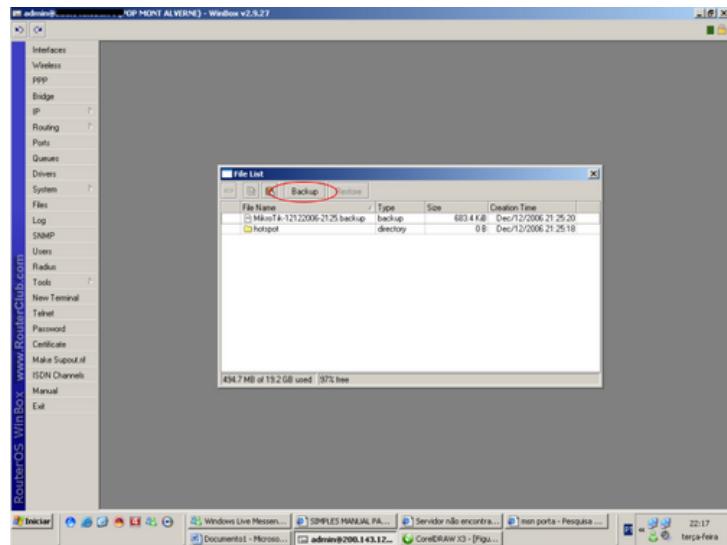
Pronto!!! Moleza!!! Agora o tráfego P2P, será limitado por marcação de pacotes. Esta regra é muito eficiente!!

BACKUP e restauração

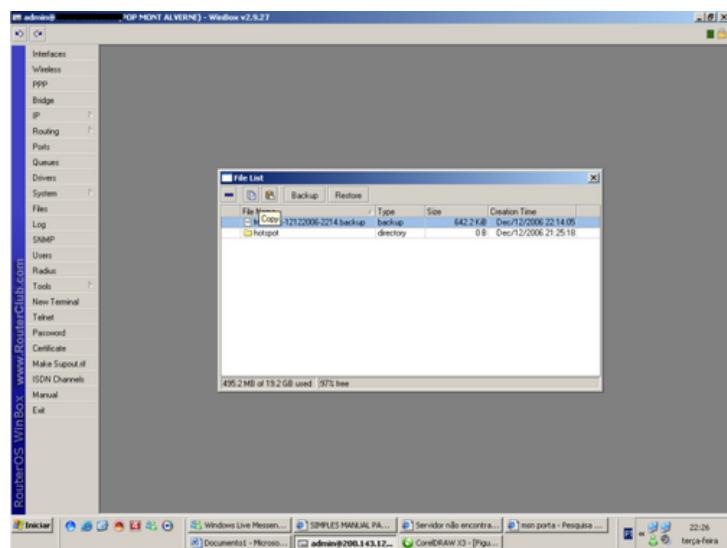
Abra o menu, FILES



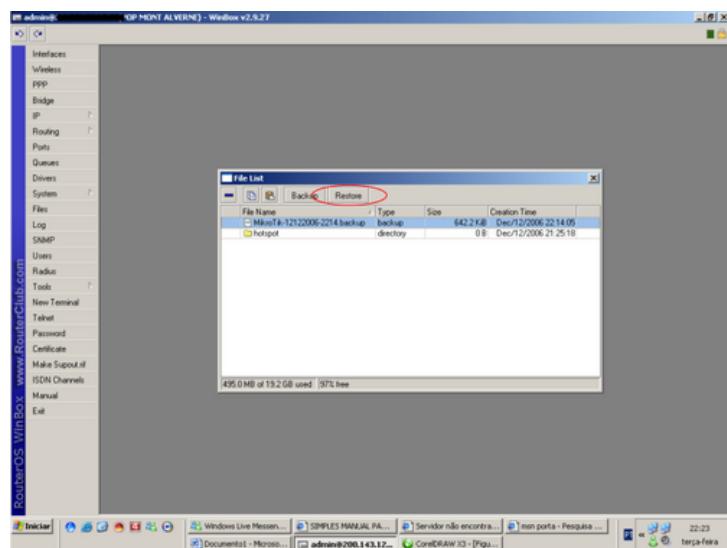
Para criar uma cópia de backup, clique em "BACKUP"



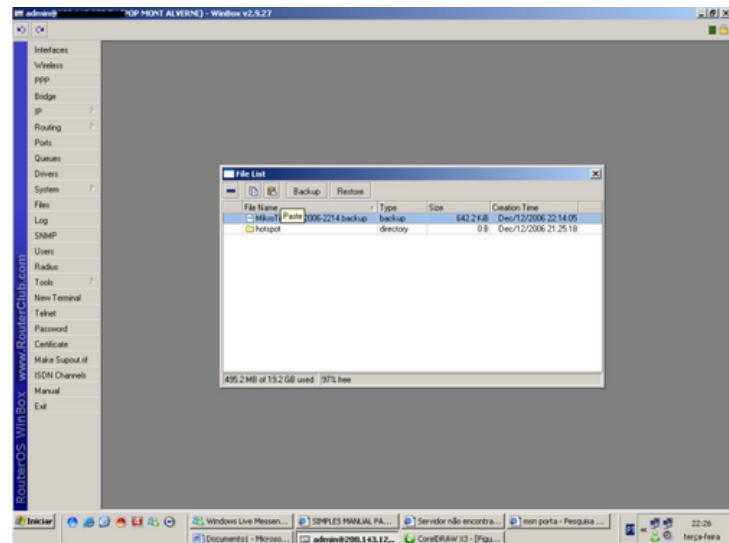
Em "FILE NAME", aparecerá o novo BACKUP. Esta cópia estará armazenada no HD do MIKROTIK. Para copiar este backup em outro computador, clique em "copy" (como na figura) e cole em qualquer pasta no windows.



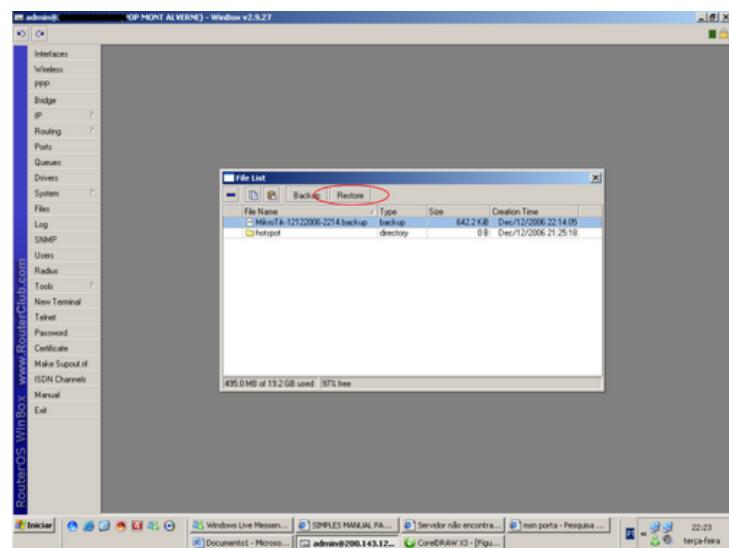
Para restaurar o seu backup, escolha a cópia desejada na "FILE NAME" e clique em "RESTORE", como abaixo.



Você também poderá restaurar uma cópia de backup, que encontra-se no seu windows, por exemplo. Para isso, no seu sistema operacional, selecione o arquivo do backup e com botão direito do mouse, escolha "COPIAR" (COPY). Vá na janela de backup do seu MIKROTIK e clique em "paste" (como na figura).



Selecione esta nova cópia do backup (aparecerá na lista) e aperte em "RESTORE"



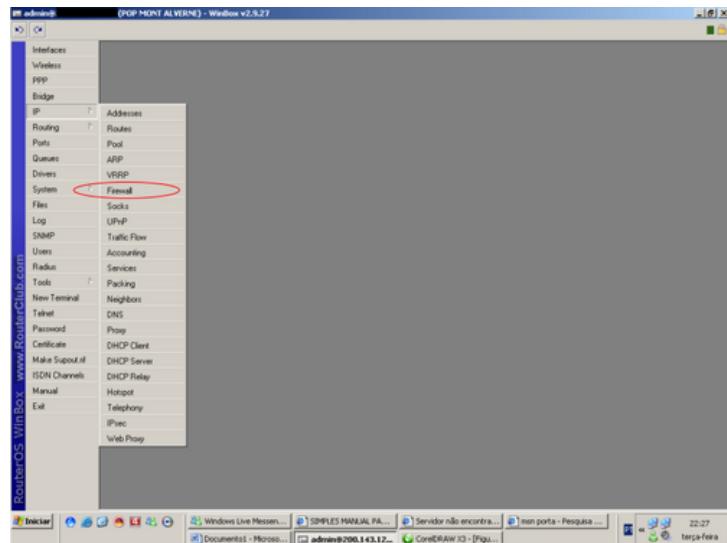
Após realizar a restauração do backup, reinicie o seu MIKROTIK.

Estamos tratando apenas de backup realizados pela "winbox", seja ele remotamente ou no próprio servidor.

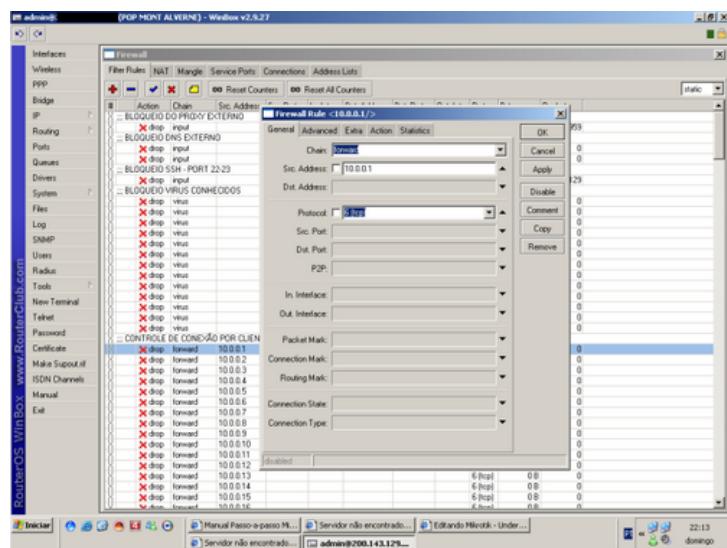
Limitar conexões por cliente

Simplérrimo!!

Acesse o menu IP, FIREWALL



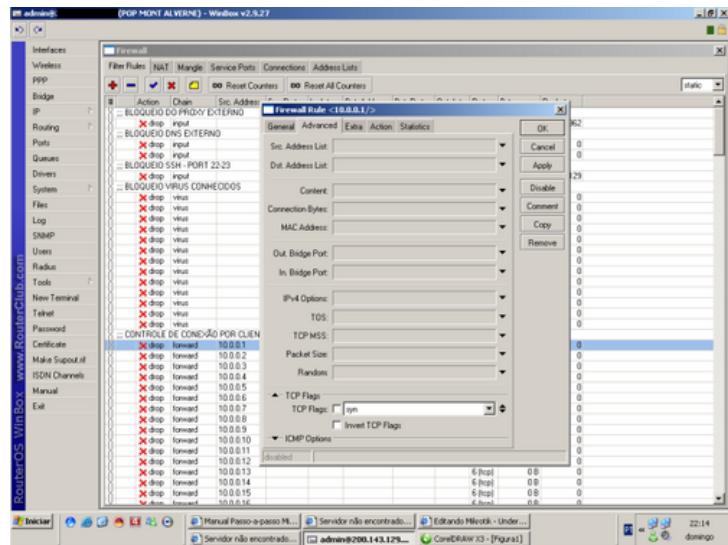
Na aba "FILTER RULES", crie uma nova regra (botão "+").



Configure da seguinte forma:

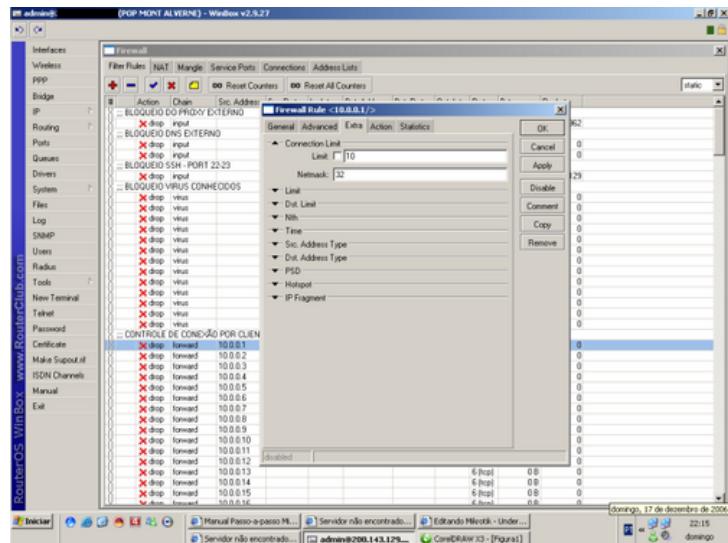
CHAIN = FORWARD
 SRC. ADDRESS = ENDEREÇO DO CLIENTE A QUAL APLICARÁ O LIMITE.
 PROTOCOL = 6 (TCP)

Agora abra a aba "ADVANCED"



Em "TCP FLAGS", escolha a opção "SYN" (este comando é responsável pelo recebimento da requisição de conexão do cliente e também pelo aviso de que a porta está ou não disponível)

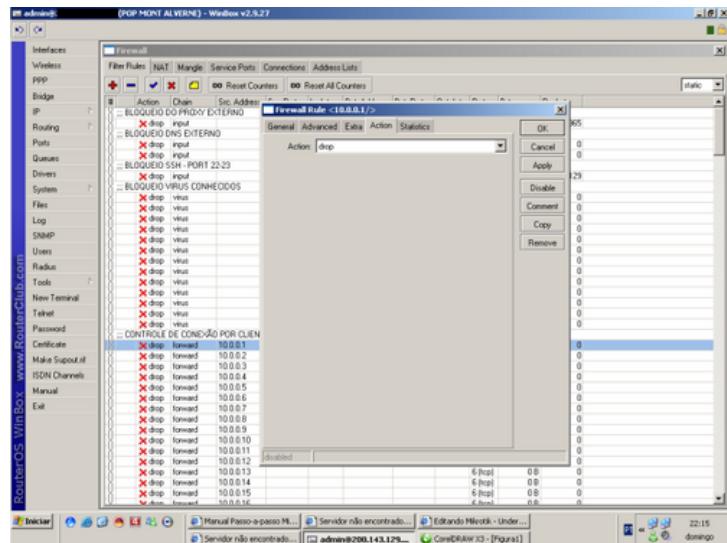
Abra a aba "EXTRA"



Em "CONNECTION LIMIT" / "LIMIT", defina o número de conexões máximas para este cliente.

No campo "NETMASK", defina a máscara 32 (32 significa que a regra será aplicada apenas a este IP)

Agora abra a aba "ACTION"



EM "ACTION", escolha a opção "DROP".

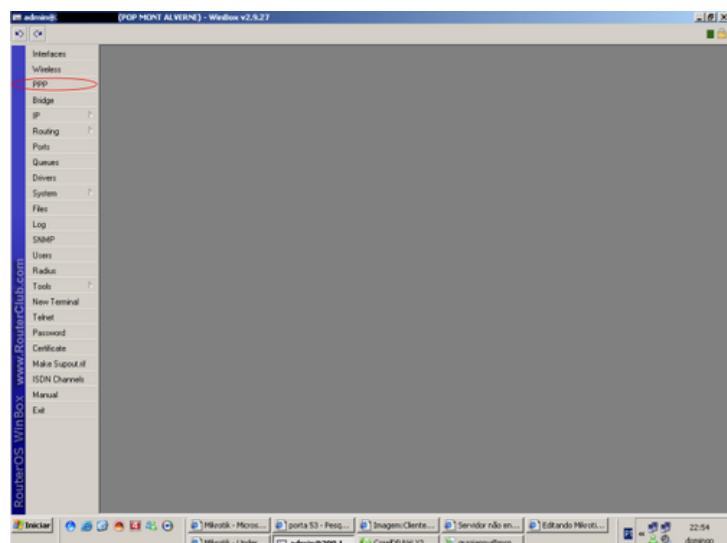
Basicamente esta regra libera N conexões simultâneas para o cliente, bloqueando requisições de conexões acima do limite.

Configure de acordo com suas necessidades

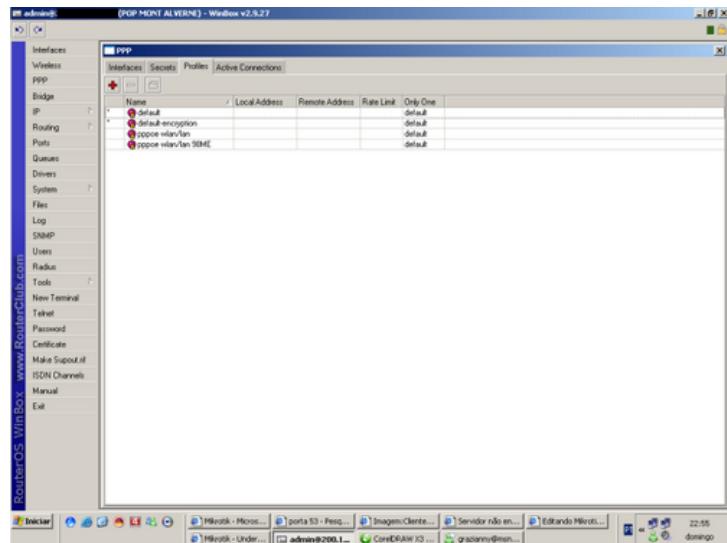
Caso deseje aplicar a regra para um range de IPs completo, configure o IP XXX.XXX.XXX.0 e o NETMASK para 24.

Servidor PPPoE e Cadastro de Clientes

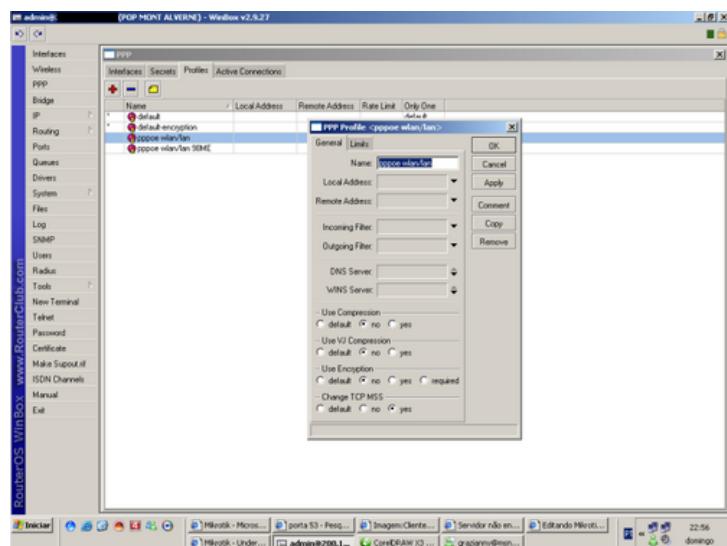
Abra o menu PPP



Clique na aba "PROFILES"



Crie um novo profile (botão "+")

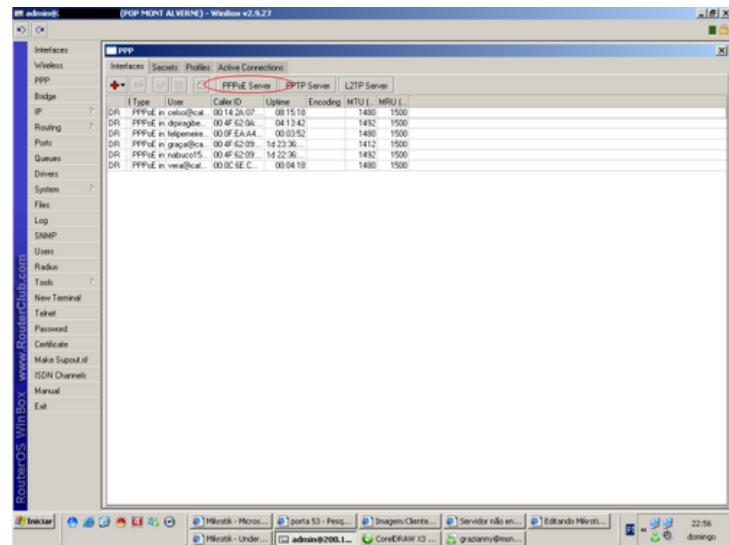


Configure este novo profile de acordo com suas necessidades. Basicamente configure assim:

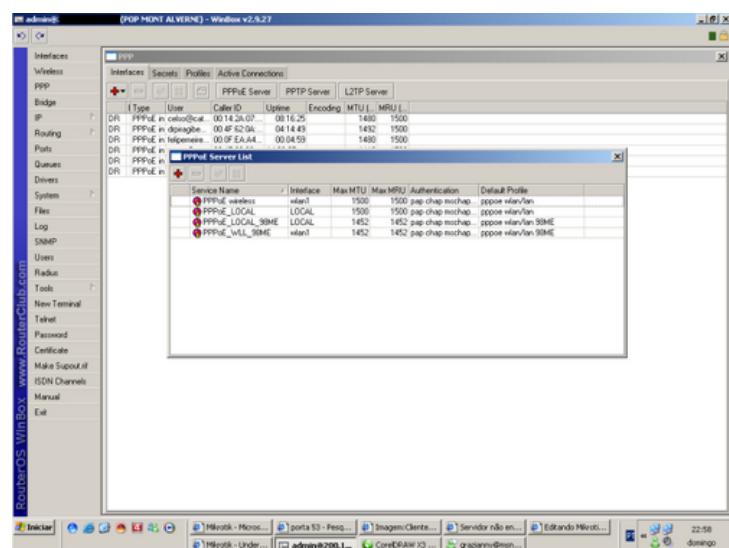
NAME = Nome do profile.
 USE COMPRESSION = NO
 USE VJ COMPRESSION = NO
 USE ENCRYPTION = NO
 CHANGE TCP MSS = YES

O outros campos deixe em branco, conforme a figura acima.

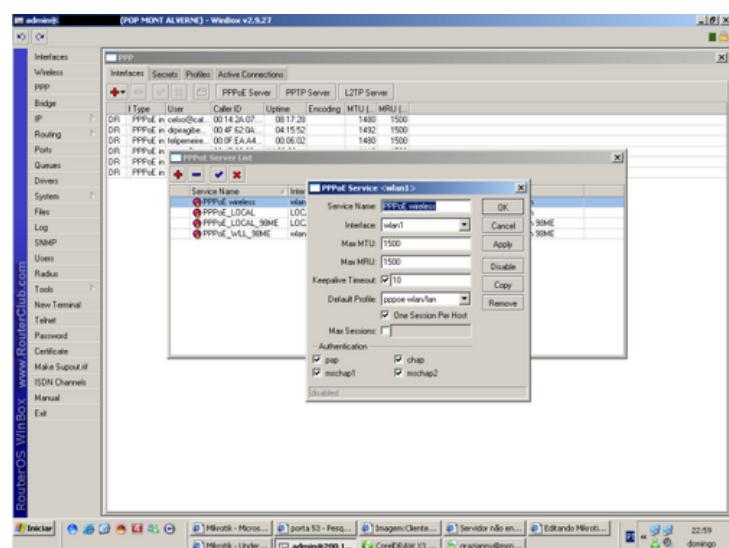
Confirme e abra a aba "INTERFACES" (na janela PPP mesmo) e clique no botão "PPPoE SERVER".



Na janela "PPPoE SERVER LIST", crie um novo servidor (botão "+")



Configure de acordo com suas necessidades. Basicamente como abaixo:



Parâmetros:

SERVICE NAME = Nome do servidor PPPoE.

INTERFACE = Interface com que este servidor irá trabalhar.

MAX MTU = Taxa máxima de transmissão. Basicamente deixe em 1500 para clientes com winxp pra cima e 1452 para clientes com win98 pra baixo e clientes que utilizam discador RASPPPOE.

MAX MRU = Taxa máxima de recepção. Configurar conforme acima.

KEEPALIVE TIMEOUT = Tempo máximo quem uma conexão retornará um erro. Basicamente deixe em 10.

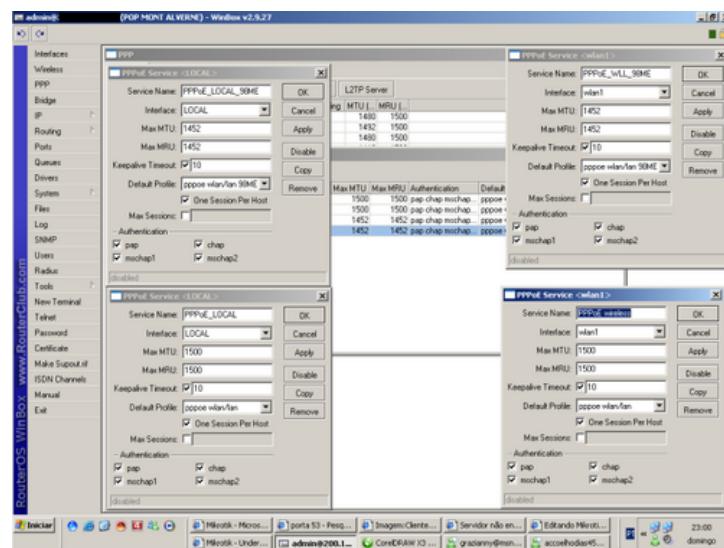
DEFAULT PROFILE = Lembra do profile que você criou? É aqui que todas estas configurações ficarão incorporados a ele. Basicamente o profile é um atalho de todas estas configurações.

ONE SESSION PER HOST = Esta opção permite que login e senha de um cliente (cadastro no servidor pppoe), conecte por vez. Isto é interessante, pois evita que várias pessoas conectem ao mesmo tempo com apenas um login e senha. Deixe marcado.

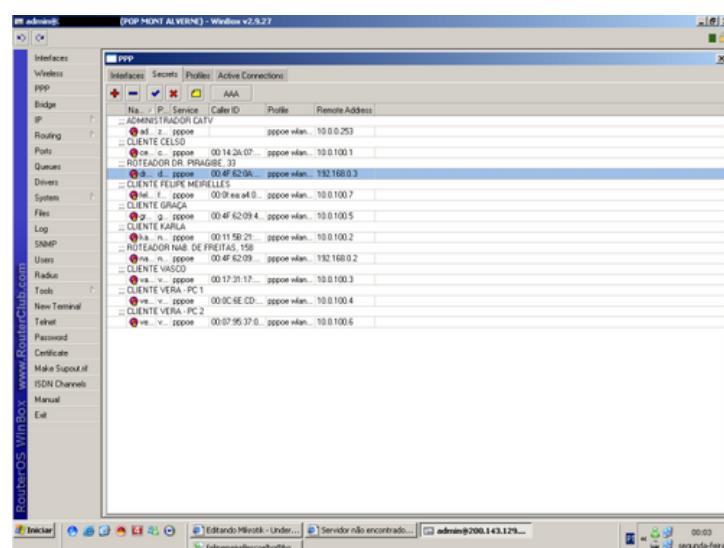
MAX SESSION = Define o número máximo de conexões a este servidor. Basicamente deixe em branco mesmo.

AUTENTICATION = Para haver compatibilidade com todos os serviços de discagem disponíveis, deixe todas marcadas.

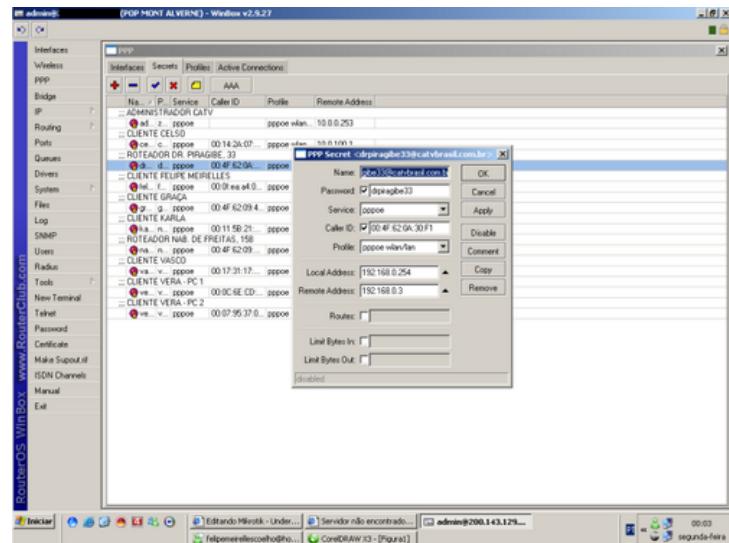
Você poderá criar vários servidores PPPoE. Cada um atendendo uma determinada interface e um determinado sistema operacional, como no exemplo abaixo:



Para cadastrar clientes é bem fácil. Após criar seu servidor PPPoE, basta clicar na aba "SECRETS"



Para criar uma nova conta, aperte no botão "+"



Configure de acordo com suas necessidades:

NAME = Login do assinante. Pode conter @xxxxxxxx.com.br ou não.

PASSWORD = Senha de acesso.

SERVICE = Escolha PPPoe.

CALLER ID = Define qual MAC Adress ficará amarrado esta conexão

PROFILE = Define o profile que será amarrado esta conexão.

REMOTE ADDRESS= Endereço do Gateway (normalmente a faixa de IP utilizada com final 254)

LOCAL ADDRESS = Endereço IP desta máquina (preferencialmente dentro da faixa de IP do LOCAL ADDRESS)

ROUTERS = Define roteamento. Deixar em branco.

LIMIT BYTES IN = Limita o número de bytes de entrada. Deixar em branco.

LIMIT BYTES OUT = Limita o número de bytes de saída.

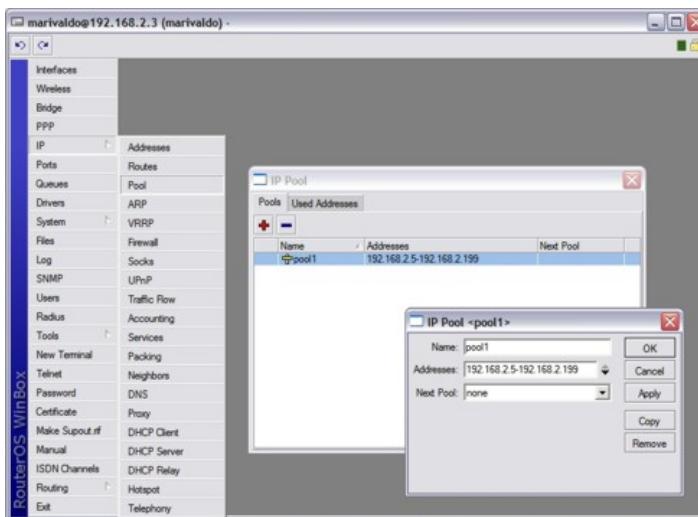
Confirme tudo e pronto. No computador do cliente basta criar uma conexão PPPoE com esta senha e login e mandar conectar.

Amarrar faixa de IP no DHCP

Um dos recursos mais interessantes em rede é o DHCP, ainda hoje eu me pergunto como os administradores conseguem trabalhar sem ele, pois ele faz todo o trabalho de configuração da interface de rede, seja ela Linux, Windows ou outra qualquer, com o DHCP você pode alterar as configurações de gateway, DNS, faixa de IP do cliente e máscara tudo sem precisar ir na casa dele, você altera no Mikrotik e pede pro cliente reparar a rede ou reiniciar o computador e está resolvido.

Resolvi dar minha contribuição neste wiki sobre esse assunto que tanto gosto e convivo todos os dias.

Comece clicando na opção IP -> POOL



Clique no botão "+" e adicione o pool1.

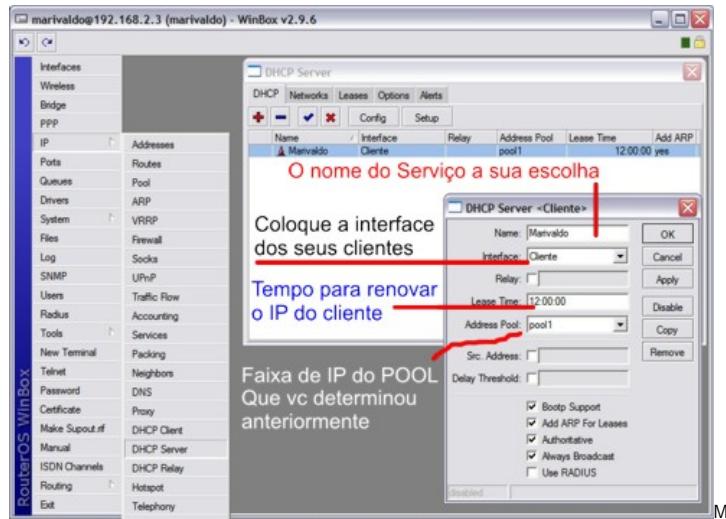
Em address: você coloca a faixa de rede que quer atribuir aos clientes.

Ex: 192.168.2.5-192.168.2.199 está bem claro não?

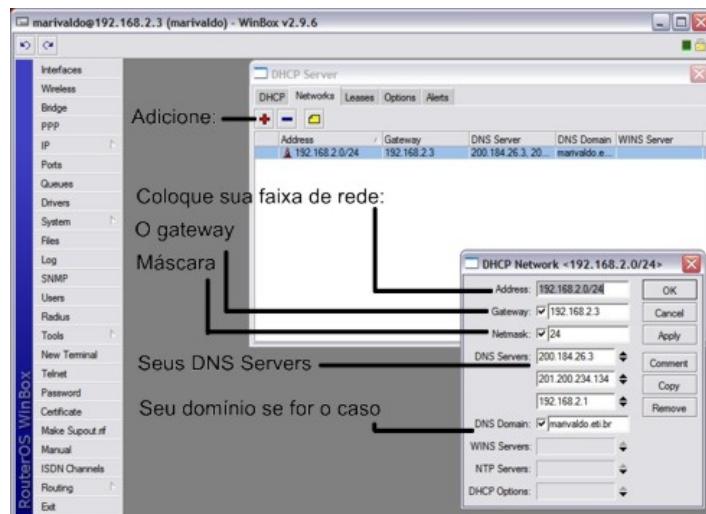
Clique em OK.

Depois clique em IP -> DHCP Server:

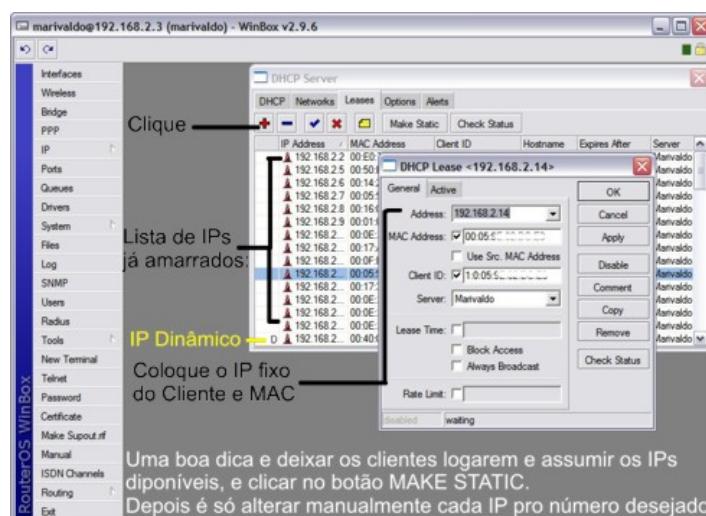
Clique no botão "+" e adicione o SERVER:



No mesmo menu, clique na ABA "Networks" :



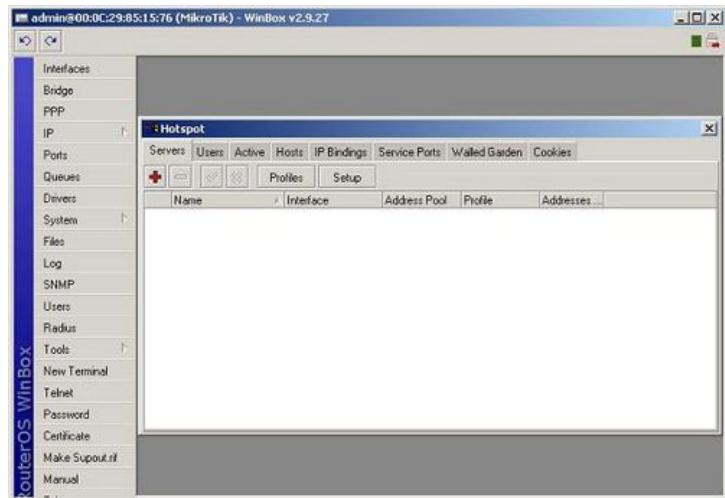
Clique na aba Leases: É nela que vc vai amarrar os IPs no DHCP



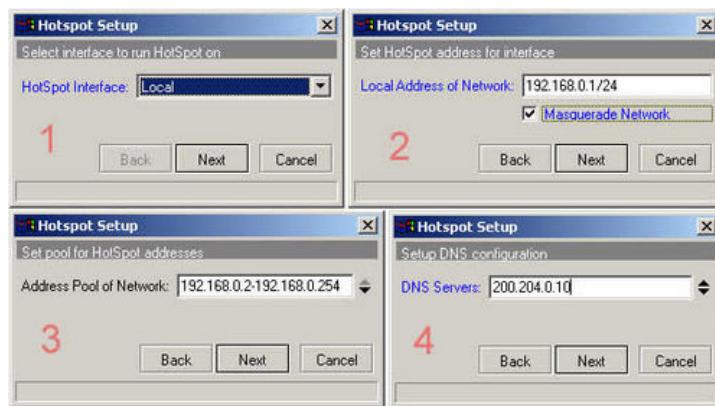
Pronto seu DHCP Server está ativado.

Configurando o HOTSPOT

Para configurar um Hotspot utilizando o Winbox, é necessário que as interfaces estejam configuradas e online. Vá para o menu IP -> Hotspot:



Em seguida, clique em Setup. As imagens a seguir mostram as principais telas de configurações:



Na imagem 1, você irá selecionar em qual interface estão os clientes do Hotspot. Na imagem 2, você pode aceitar o endereço padrão da interface ou atribuir um outro para o Hotspot. Na imagem 3, escolha a faixa de IPs que os cliente usarão e por último, defina um DNS válido para esta rede.
Ao final destes passos, você terá que criar o primeiro usuário para acessar o Hotspot. O próprio assistente sugere o usuário Admin, digite uma senha para ele e o assistente concluirá a configuração.

Agora, você já pode testar, dentro da rede local, basta tentar acessar qualquer endereço externo, digite o usuário e senha e pronto.

Somente uma coisa que quero adicionar, é que todo sempre tem a dificuldade de linkar o hotspot com o web-proxy.... ai todos achão que estão errando na configuração e acabam lotando os fóruns de tópicos.... Pessoal para funcionar o HOTSPOT com o WEB-PROXY precisa criar uma regra para a requisição ir para a porta do hotspot e não pra porta 80 direto... -> IP -> FIREWALL -> NAT ->

add -> chain=pre-hotspot src-address=IP da Rede dos Clientes Protocol=6(tcp) Dst.Port=80 In. interface=Interface dos clientes " Na guia Extra va em Hotspot e selecione a opção "auth" e na guia Action deixe em Action=redirect To Ports=Porta do Web-proxy .

Configurações dos cartões Wireless

<p />Olá pessoal, vou ensinar aos poucos como criar um AP em modo Bridge Para que os clientes se conectem a sua rede, somente desejo que não liguem para os Prints, pois meu monitor é de 14' preto e branco ai sai meio cortada.....

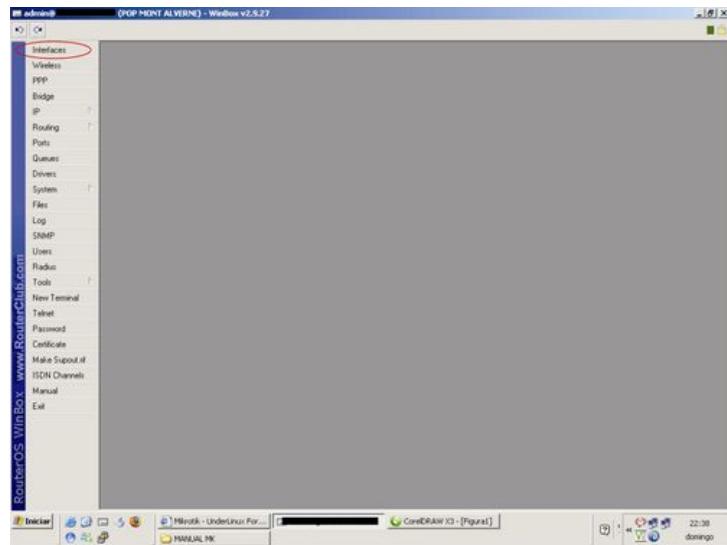
Arquivo: Imagem1.PNG

<p />Primeiramente clique na opção Wireless, habilite o cartão, e de um duplo-clique nele. <p />em Name: de um nome para ele, lembrando que isto não é o nome que o Ap receberá. <p />em ARP deixe Reply-only se for controlar via arp list. de OK...

<p />Continua....

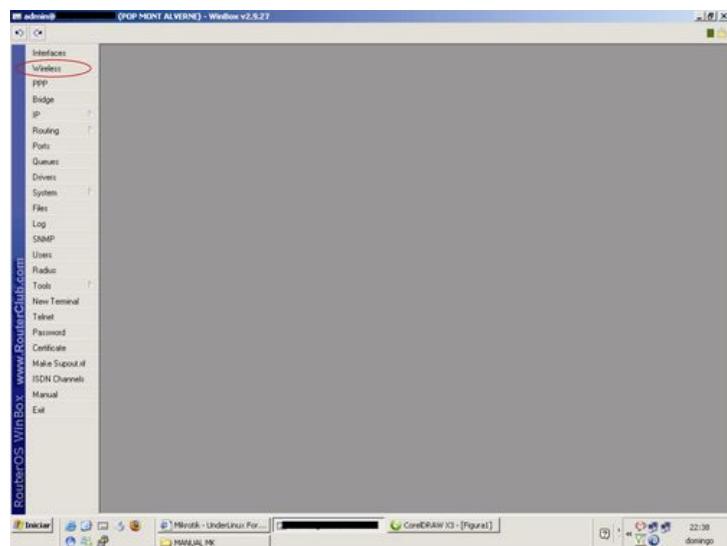
Entendendo cada função do menu do WINBOX

Em construção

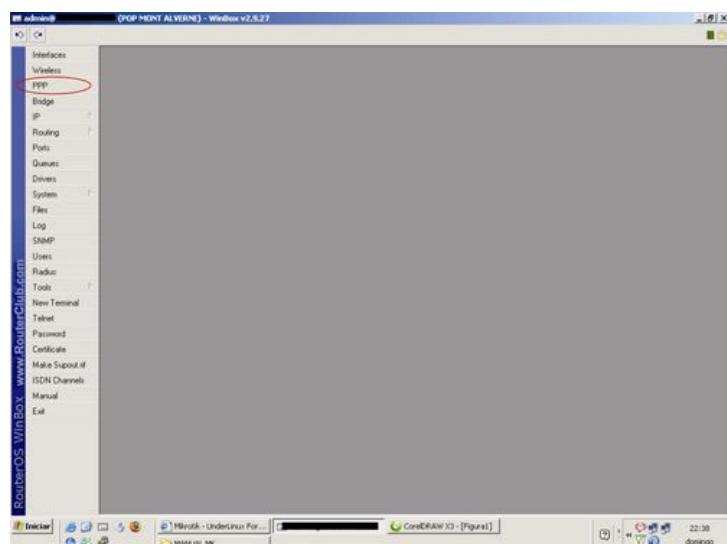


O primeiro menu do lado esquerdo chama-se " Interfaces ", é nele que se consegue enxergar os dispositivos fisicos conectados ao mikrotik, tais como placas de rede, placas wireless e etc ... é neste menu também que se cadastra a interfaces virtuais como PPoE server, bridge, virtualap e etc ... basta apenas clicar no Sinal de "+" e adicionar a interface desejada.

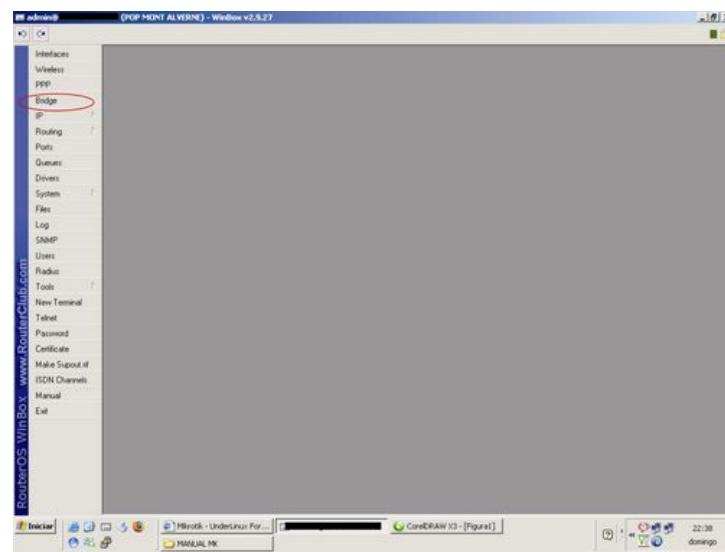
Responde também pelo comando " interface " no terminal do mikrotik.



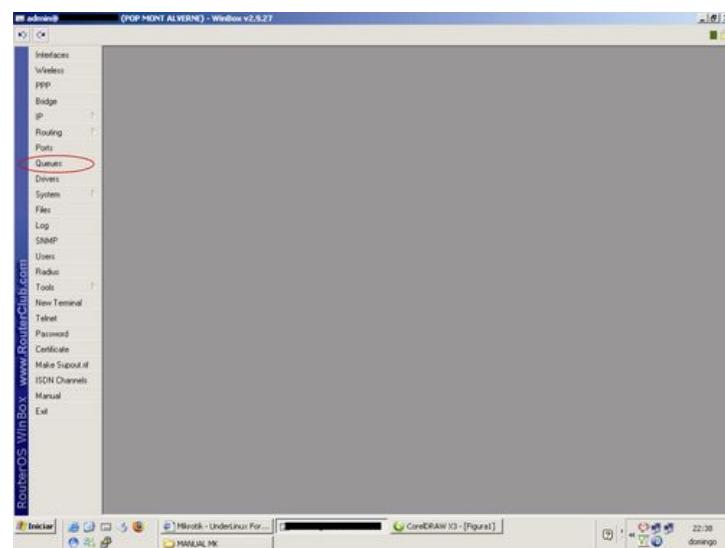
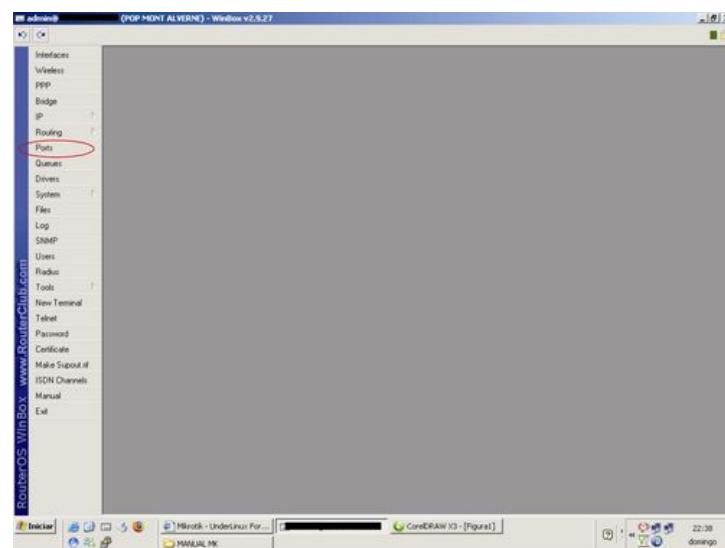
O segundo menu, - Wireless - É nele que se pode abilitar e desabilitar as interfaces wireless (Como cartões PCMCIA - Car Mini-PCI Wireless (Basta apenas clicar no Sinal de "+" e adicionar a interface desejada.)



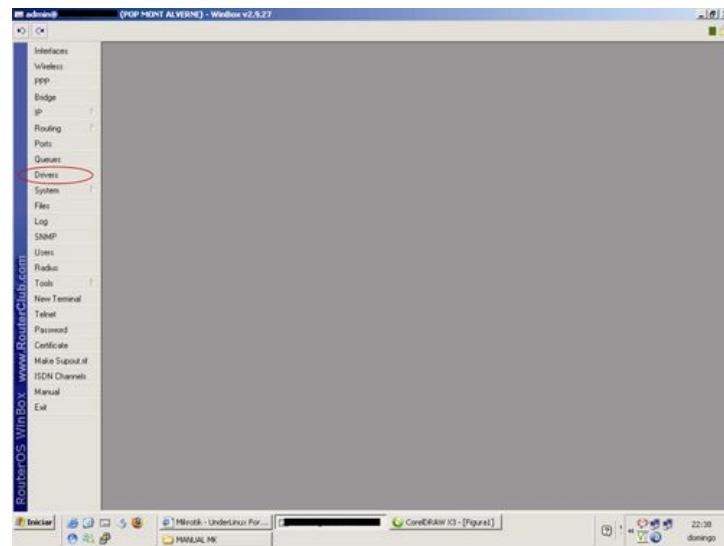
O terceiro menu, - PPP - É nele que se pode criar, editar e remover conexões PPPoe PPTP e L2TP, também é onde se configura servidores dos mesmos serviços, configura senhas para discadores dos seus clientes e adiciona perfis de discagem.



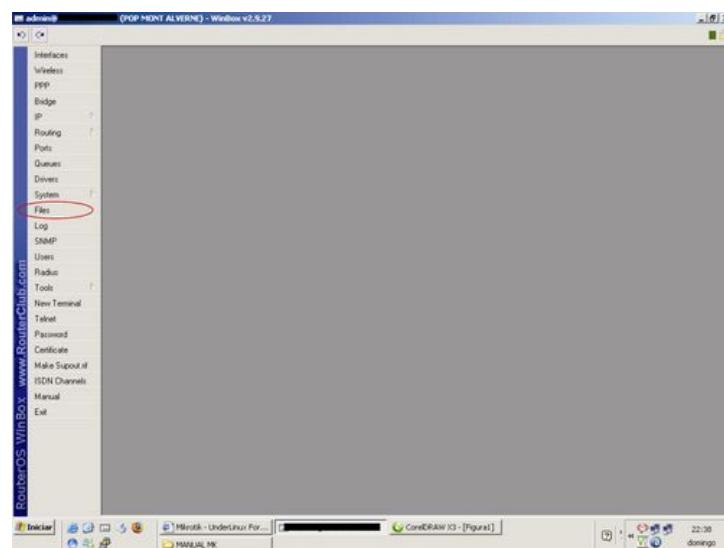
O quarto menu, - Bridge - É nele que se pode criar, editar e remover Bridges (Pontes entre as interfaces).



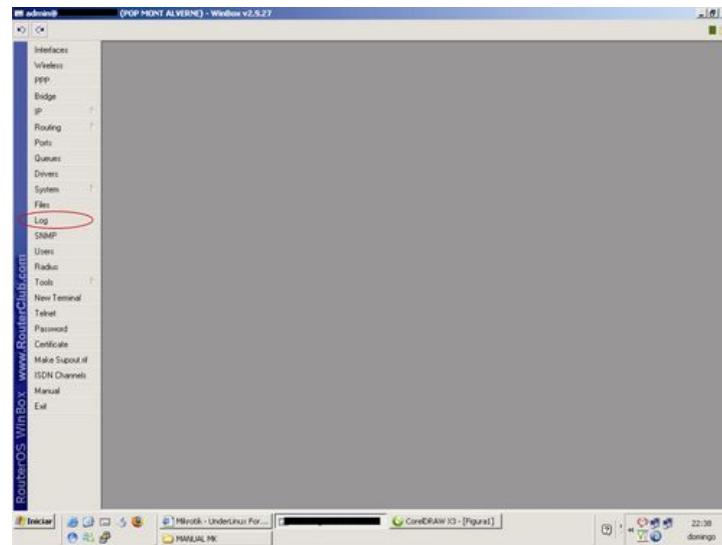
O sexto menu, - Queues - É nele que se limita velocidade por IP ou faixa de IPs ou também por Interface.



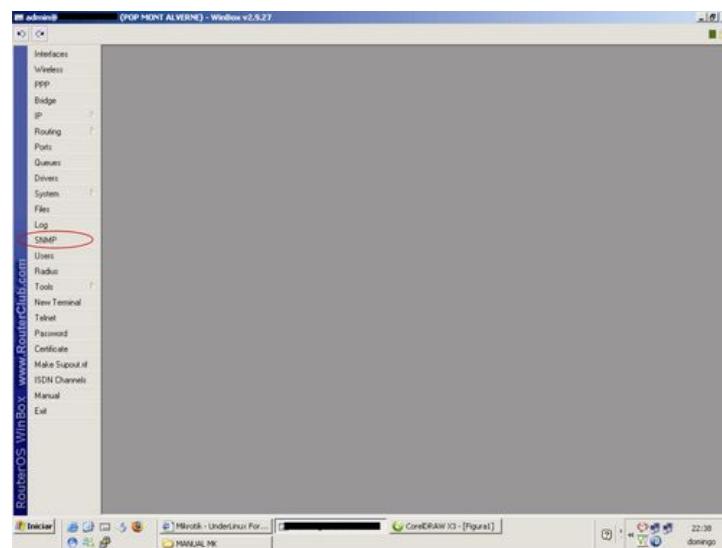
O sétimo menu, - Drivers - É onde se obtém a lista de drivers de Cartões Wireless e Placas de Rede.



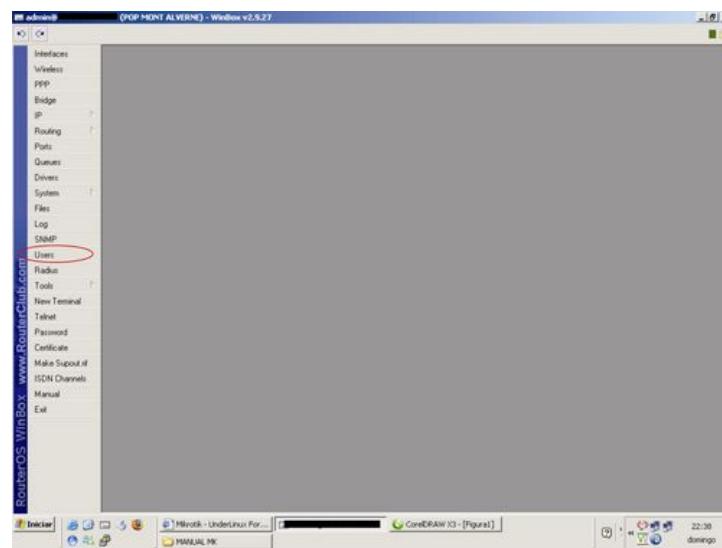
O oitavo menu, - Files - Abre um navegador no qual pode-se ver os arquivos que estão no HD, também é onde se cria Backup e restaura os mesmos.



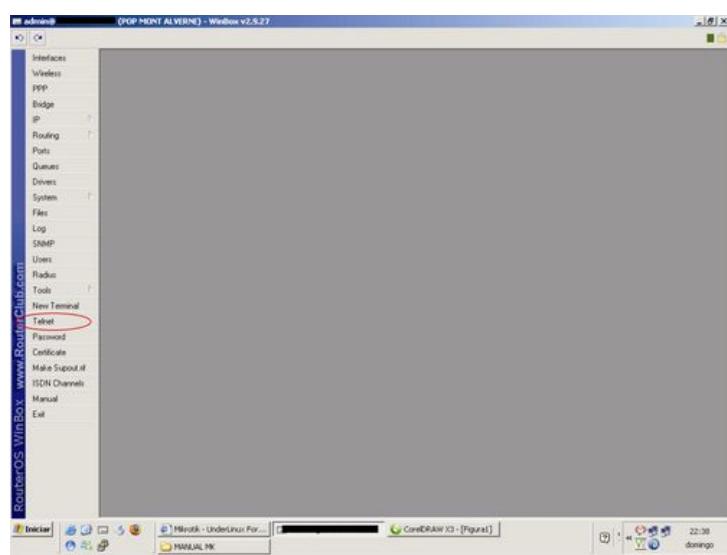
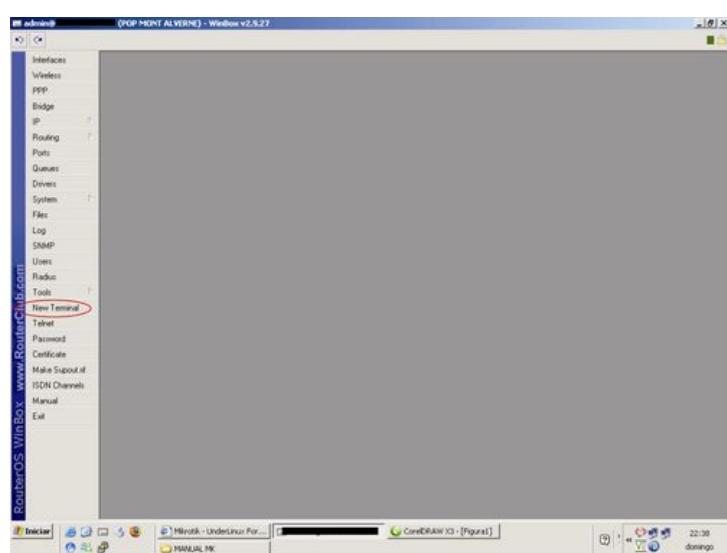
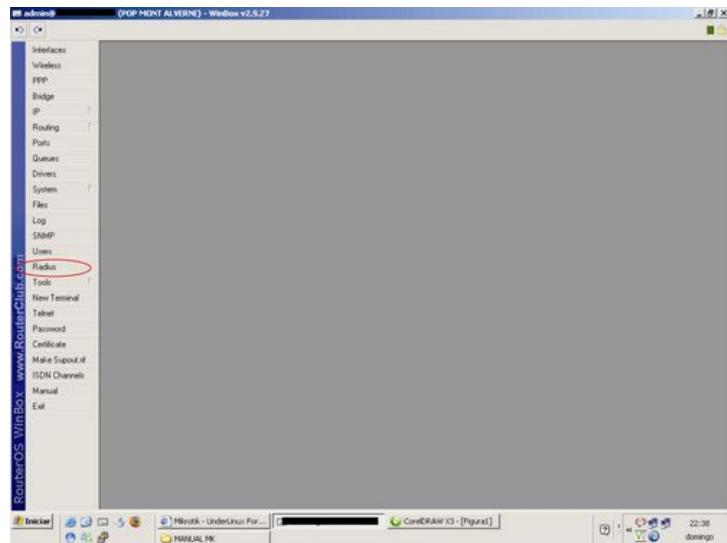
O nono menu, - Log - É onde se ver o log do seu sistema.

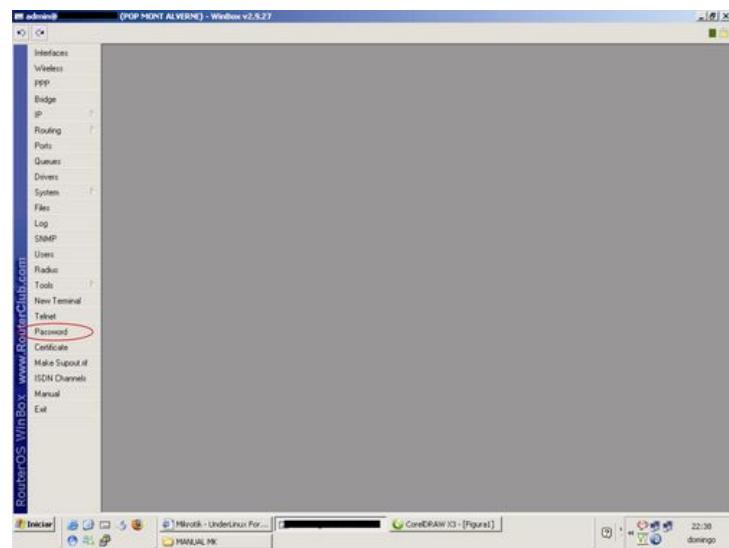


O décimo menu, - SMNP - É onde se configura o smnp communitydo seu sistema.

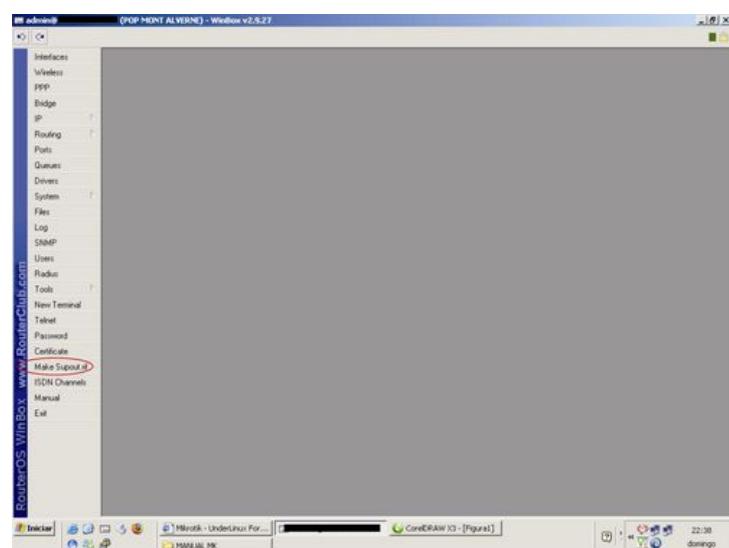
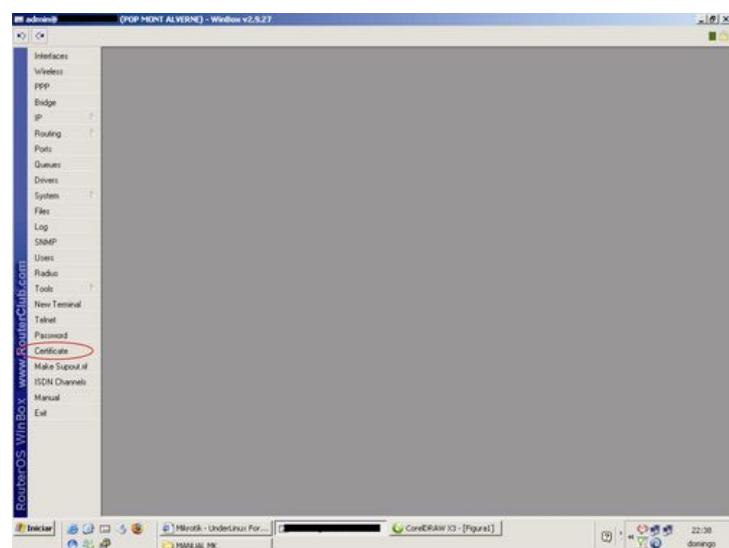


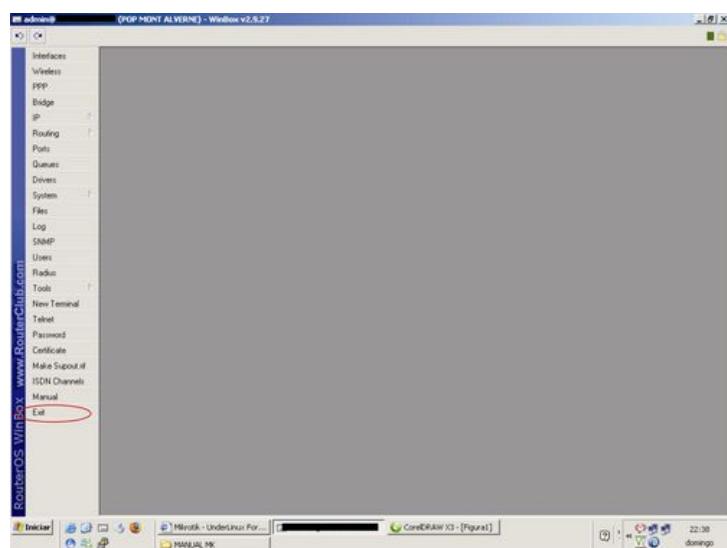
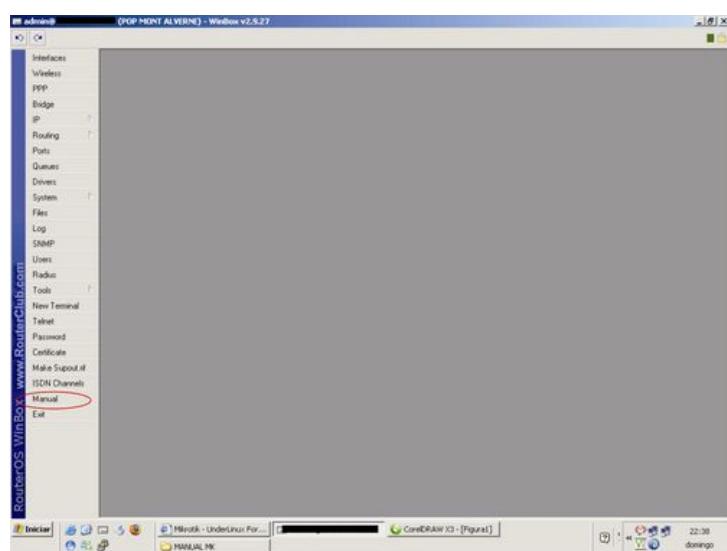
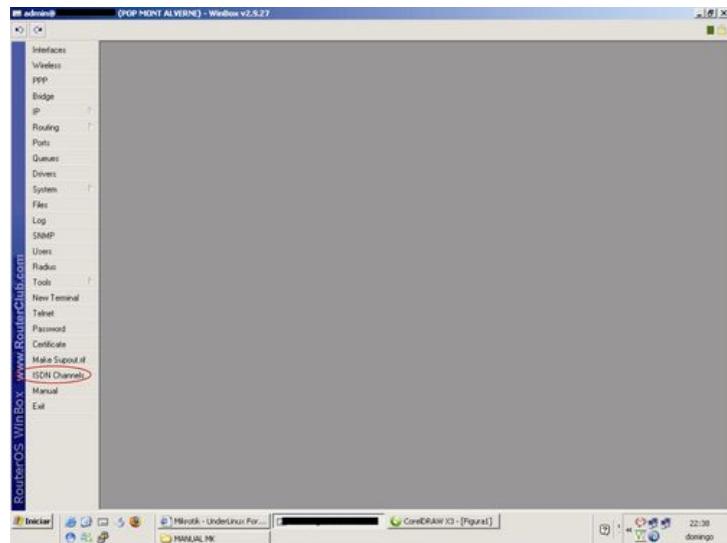
O décimo-primeiro menu, - users - É onde se cadastra e remove usuários do sistema.





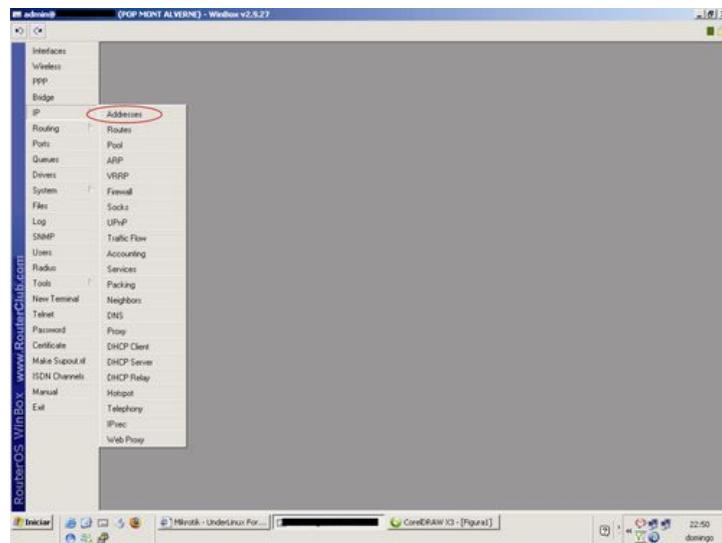
O Décimo-Quinto menu, - Password - é onde se altera a senha do seu Mikrotik



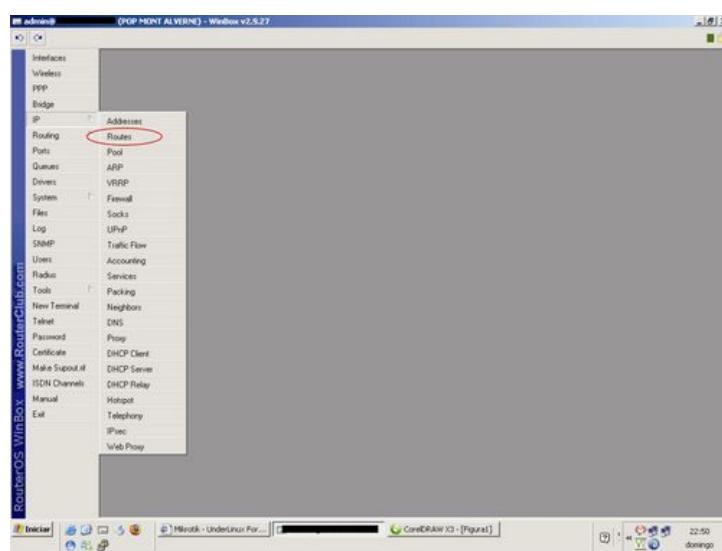


O vigésimo, - Exit - Fecha a sua sessão do Winbox.

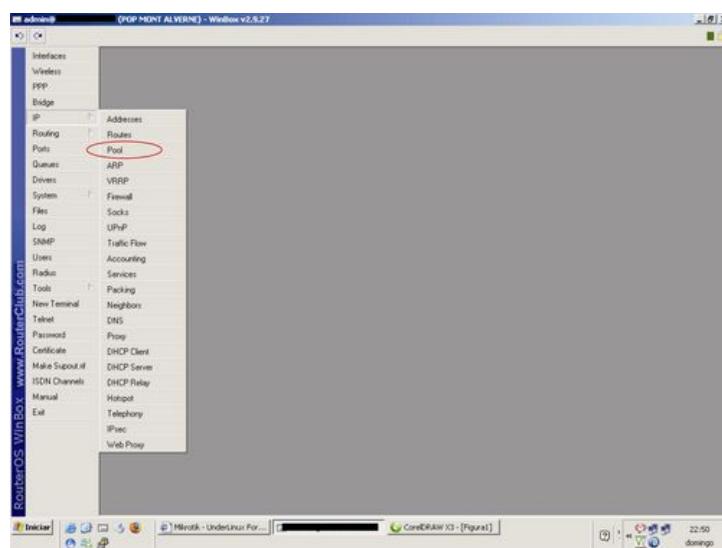
SUB-MENU IP

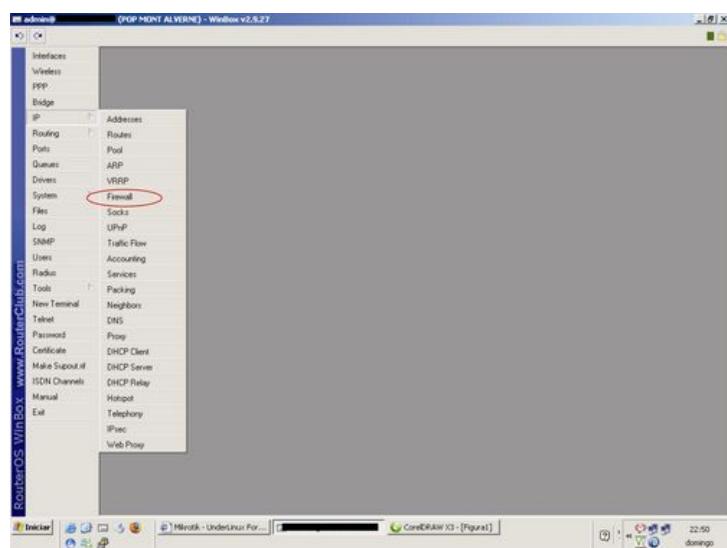
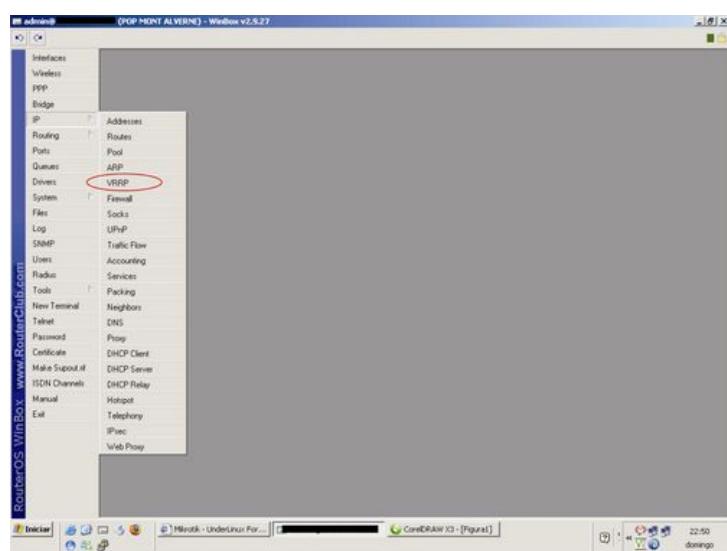
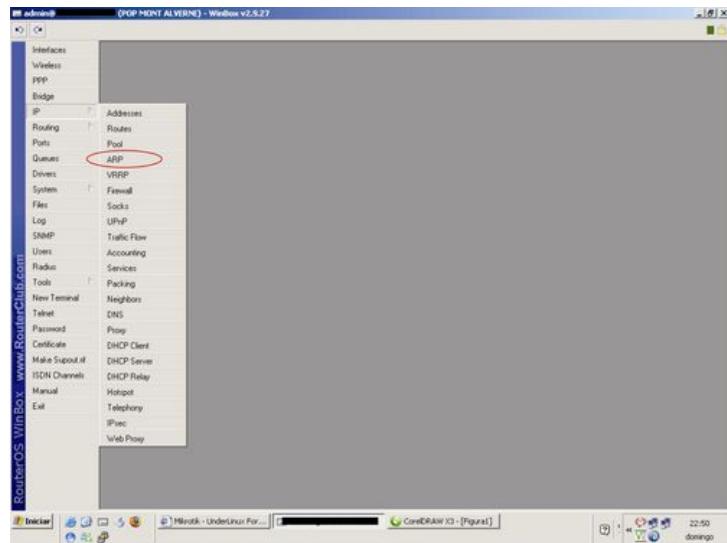


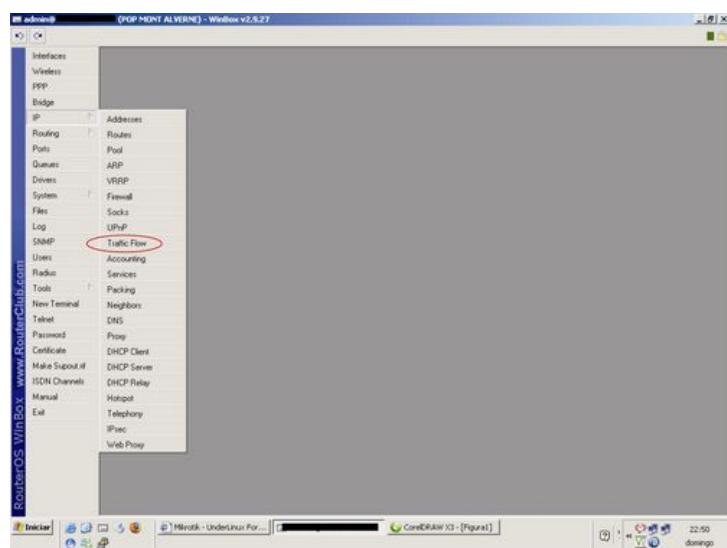
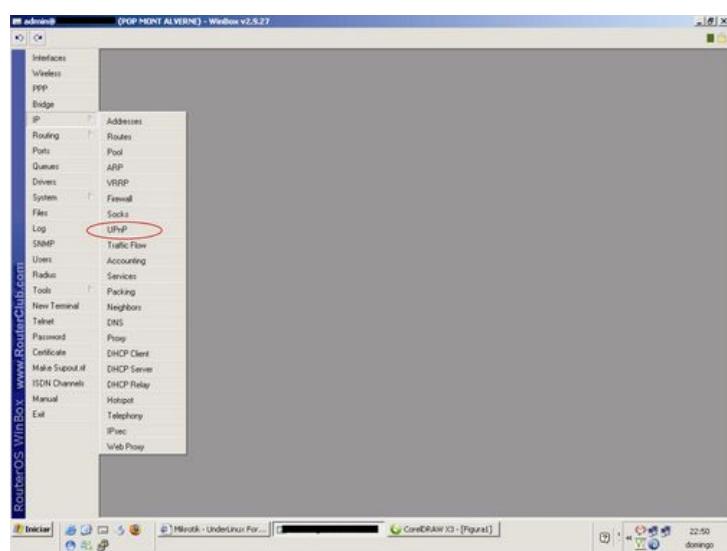
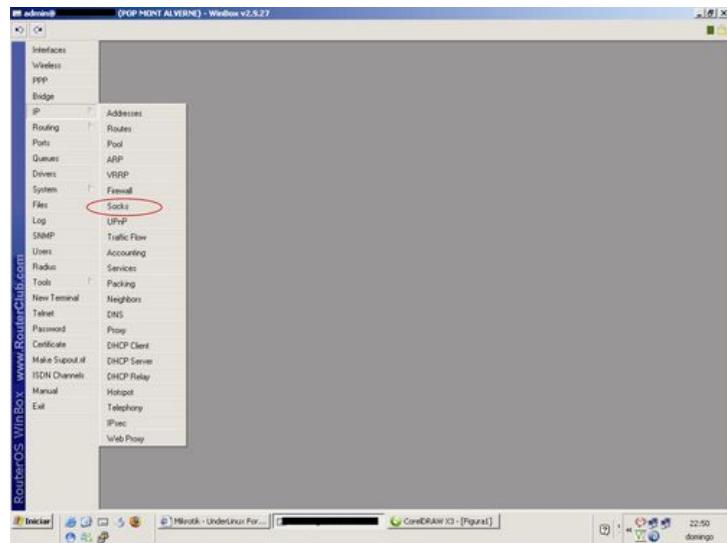
address: onde se adiciona endereços as interfaces de rede.

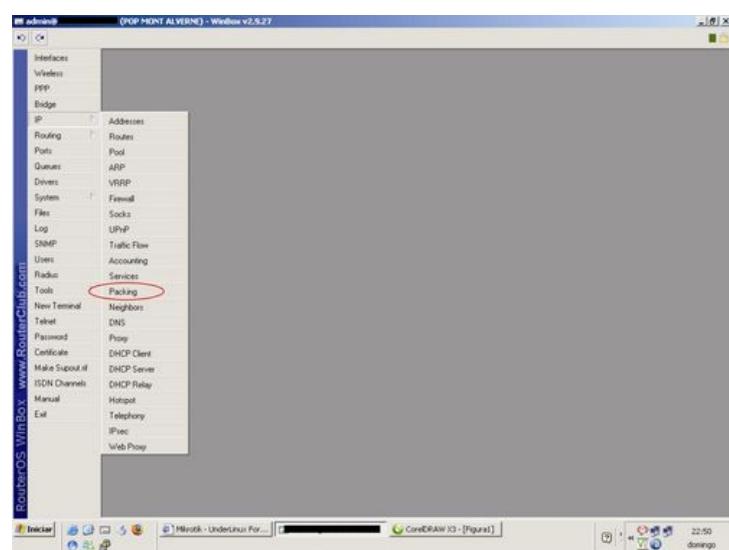
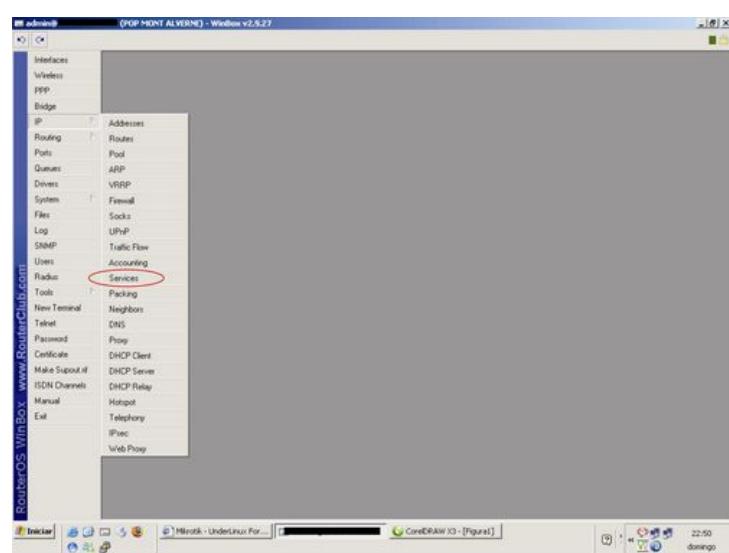
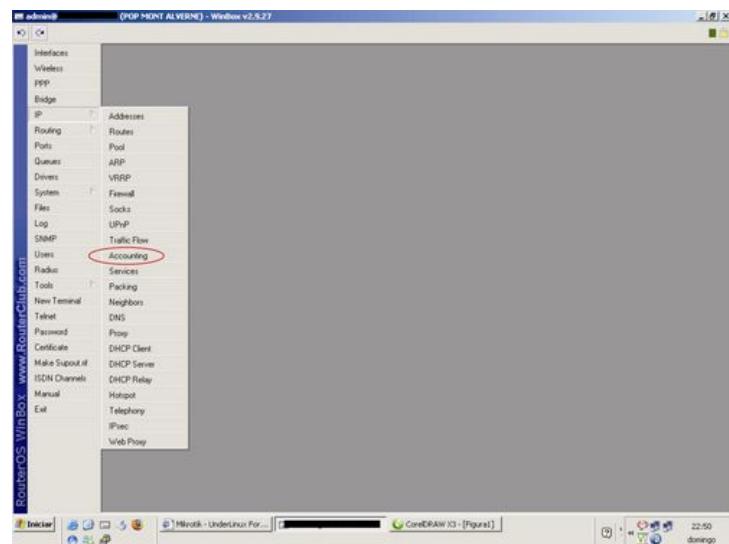


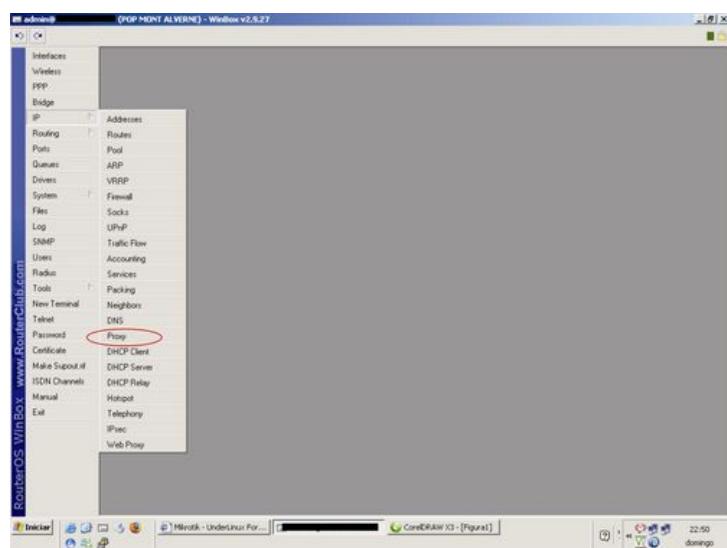
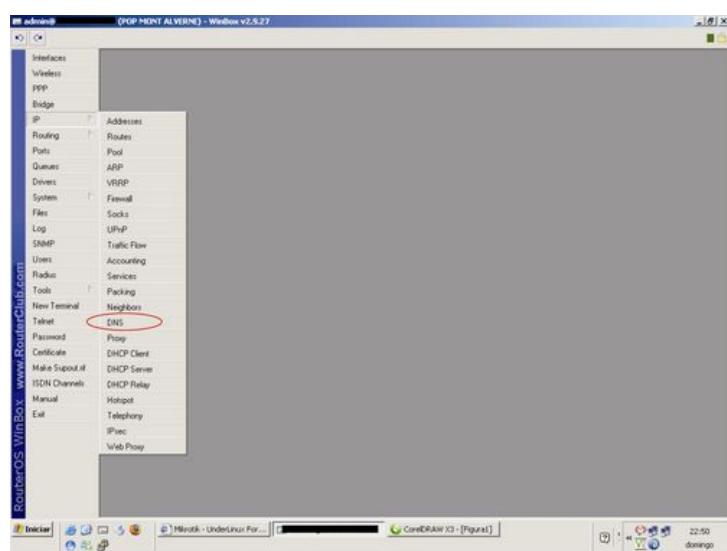
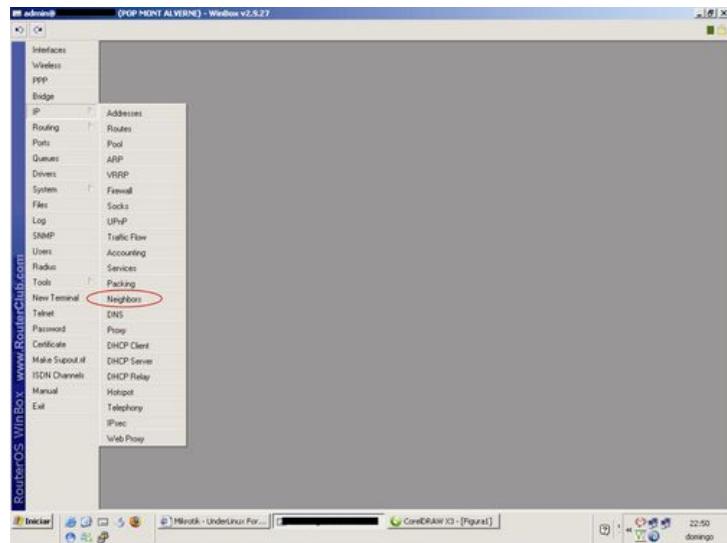
Routes: onde se coloca as rotas estáticas e regras de roteamento.

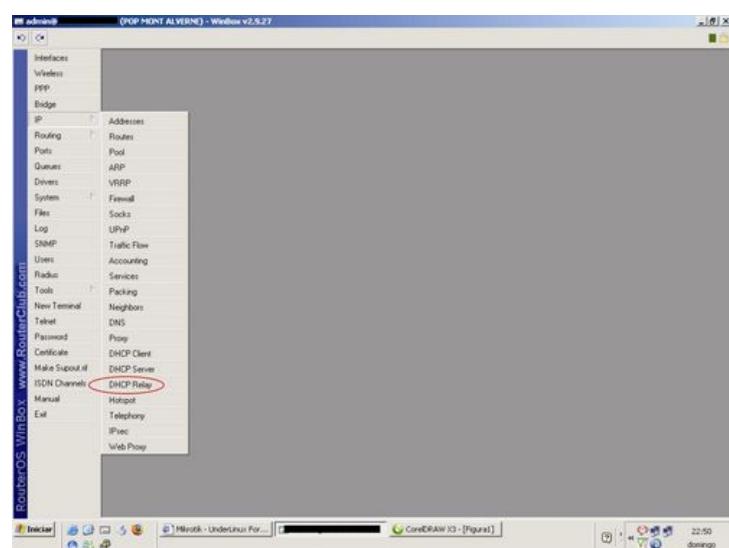
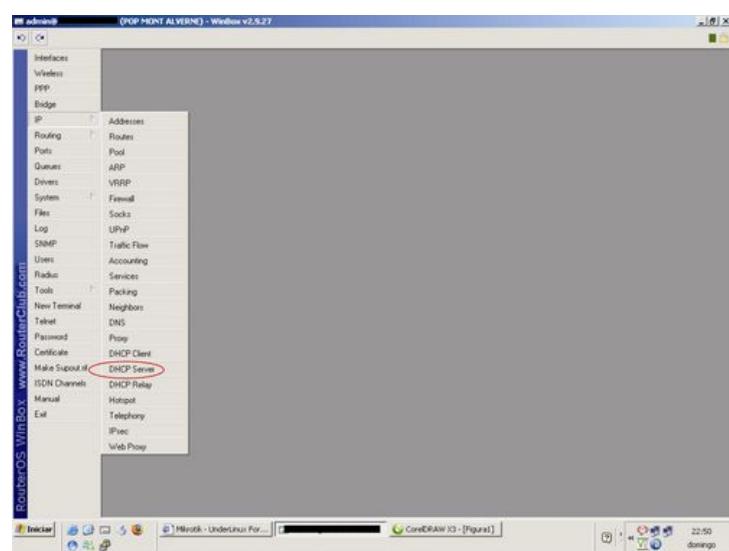
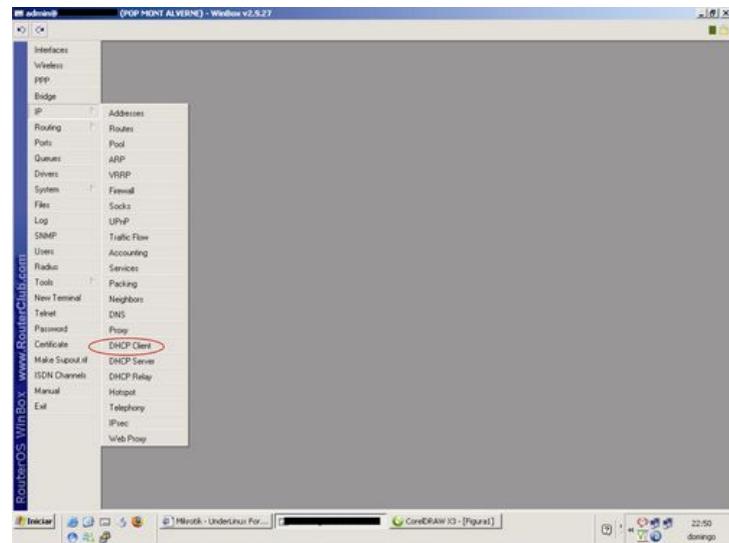


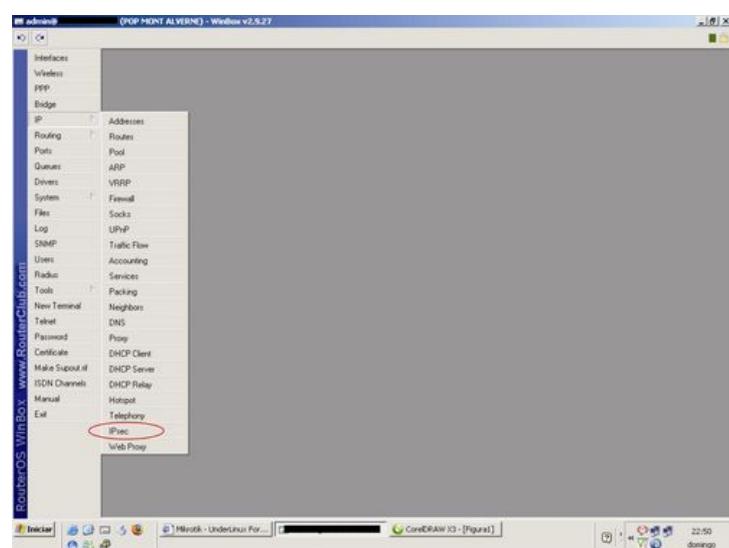
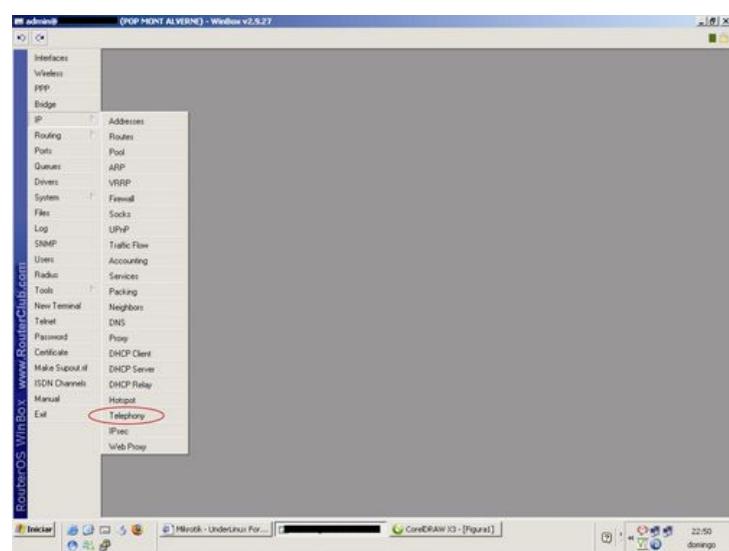
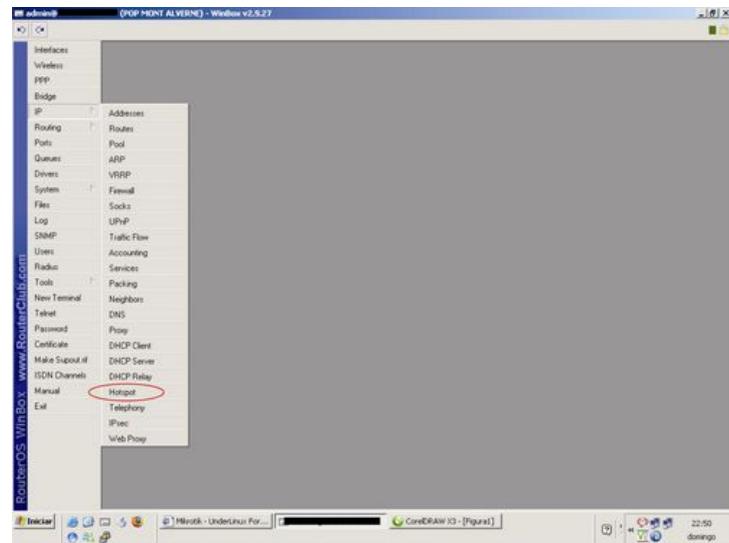


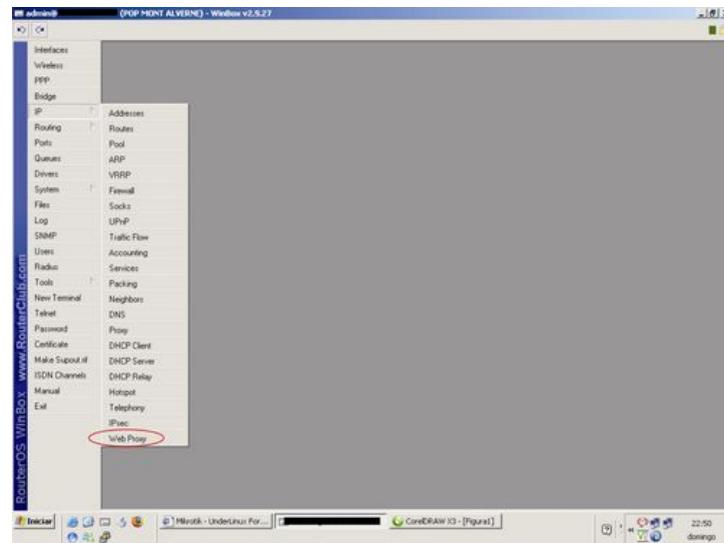




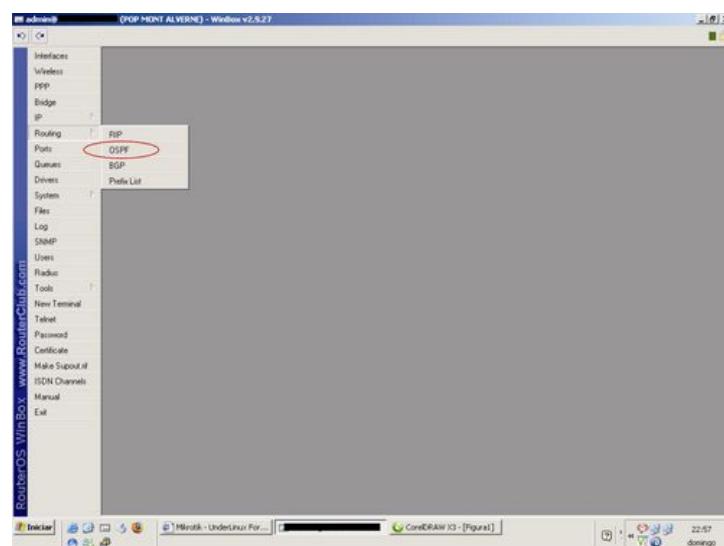
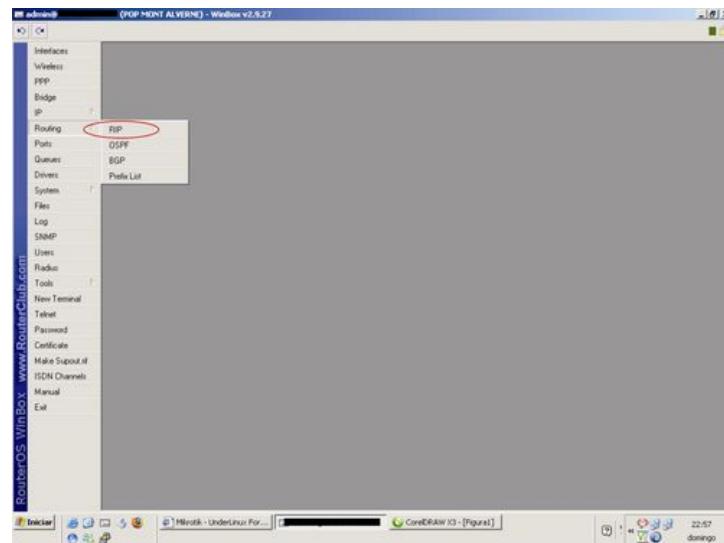


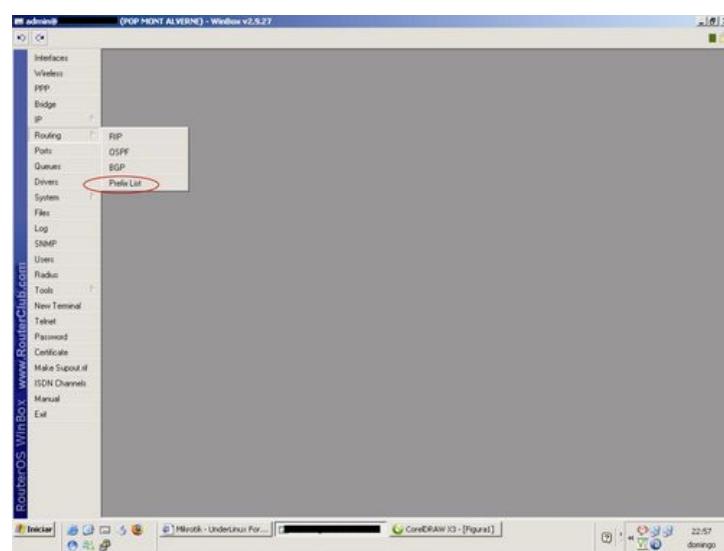
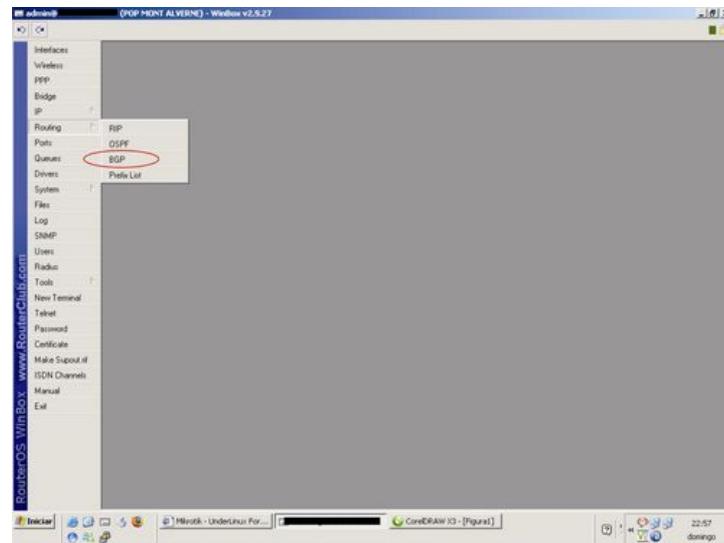




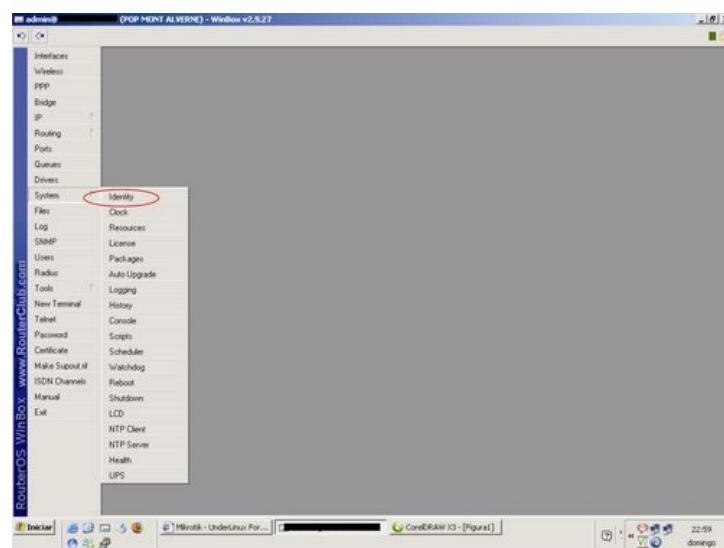


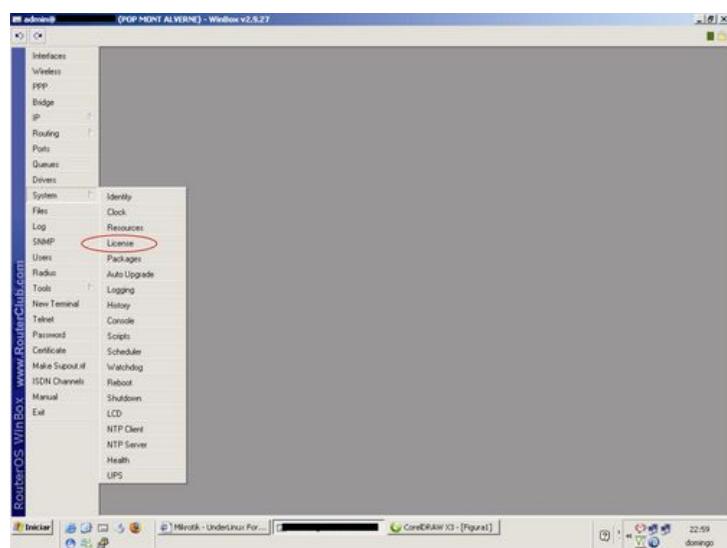
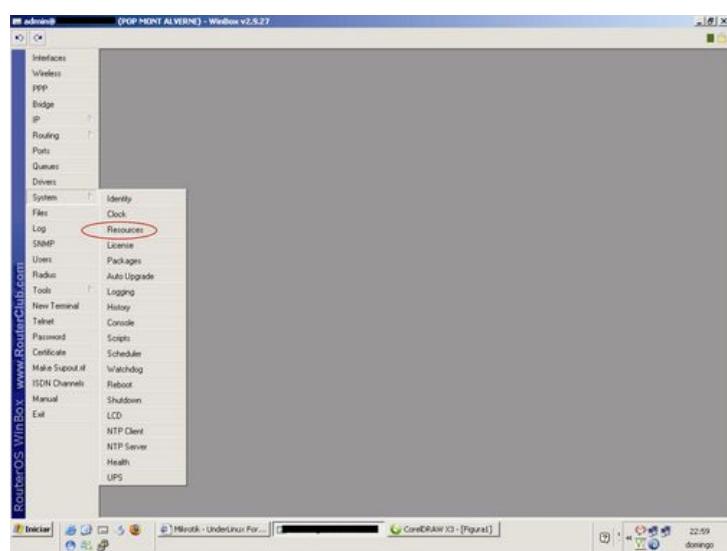
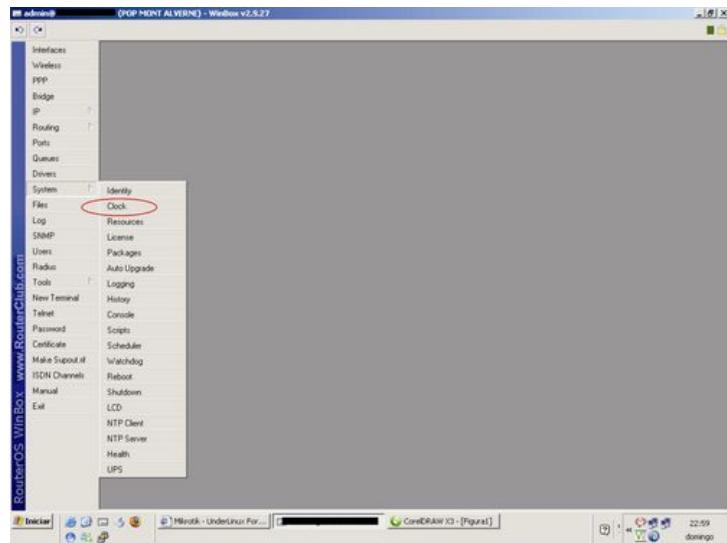
SUB-MENU ROUTING

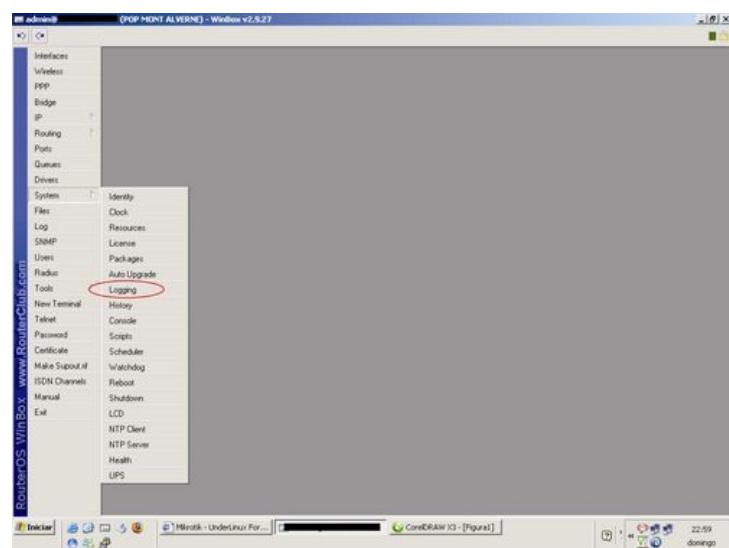
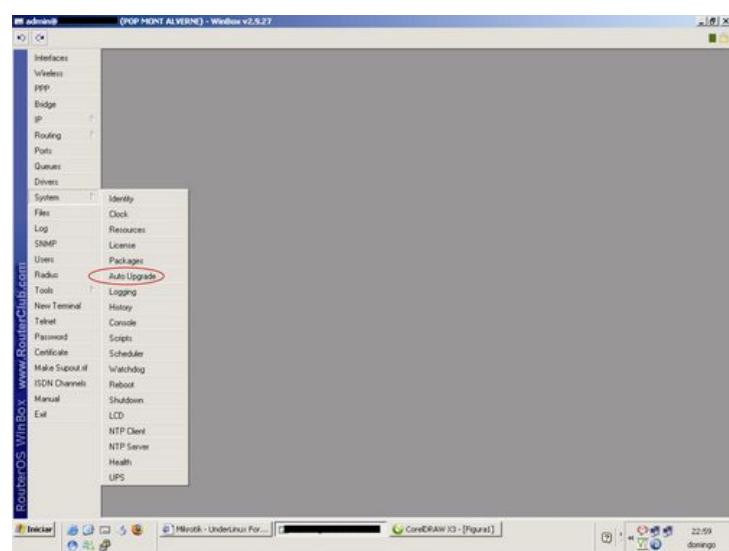
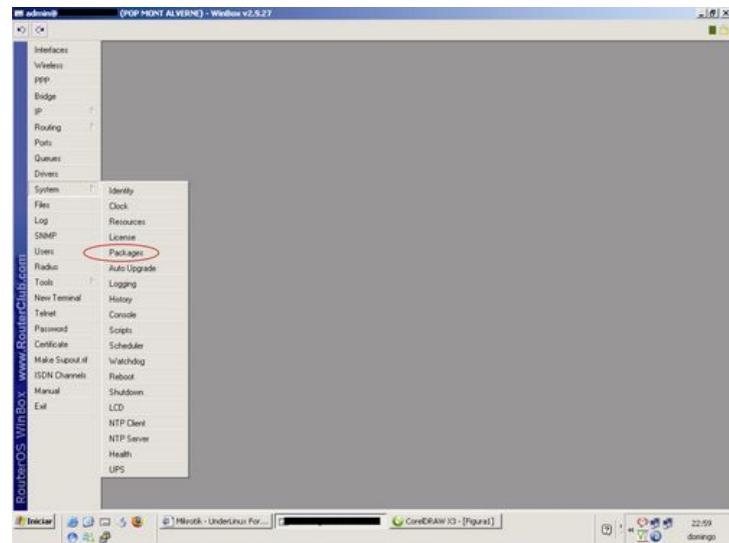


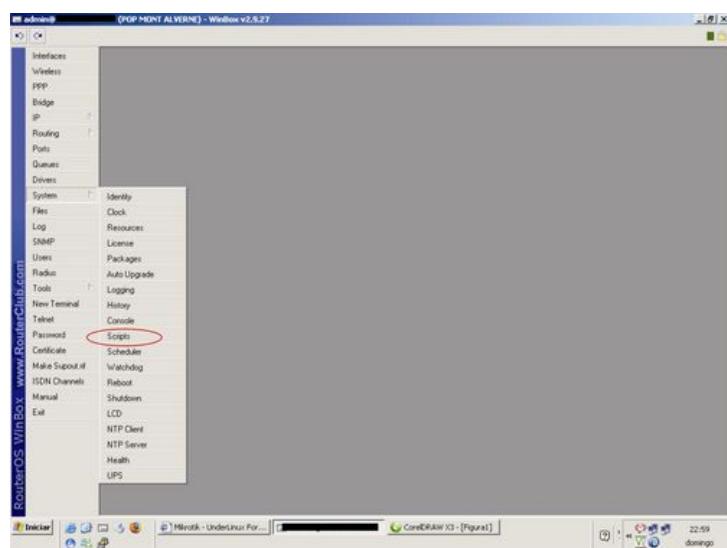
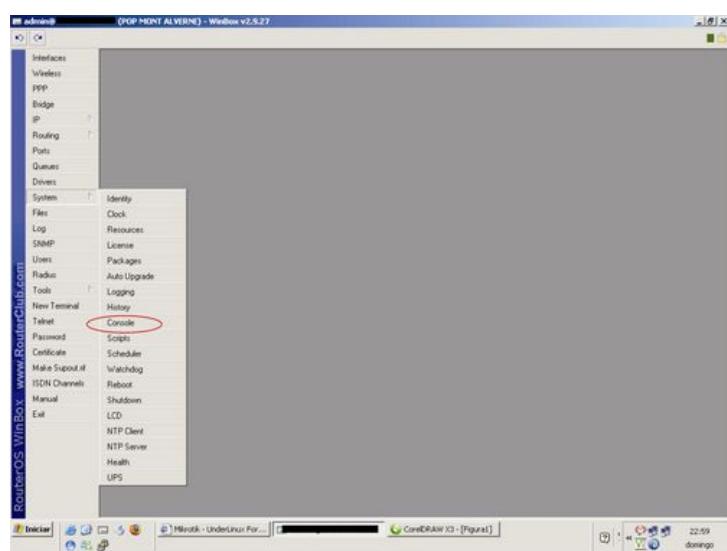
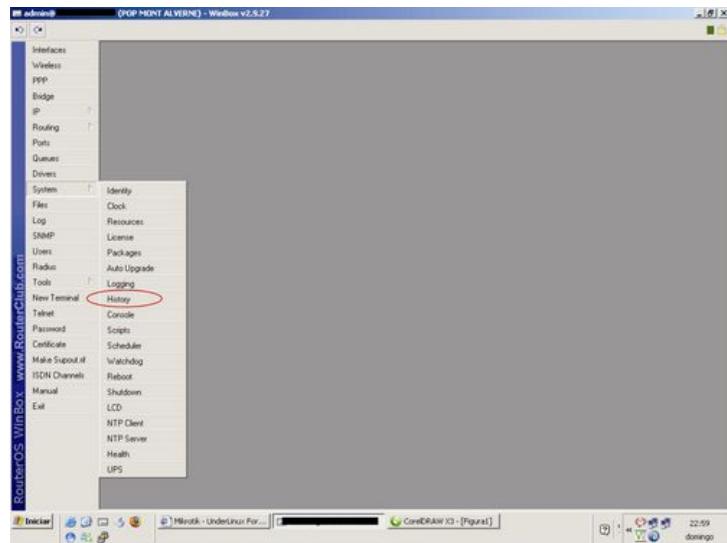


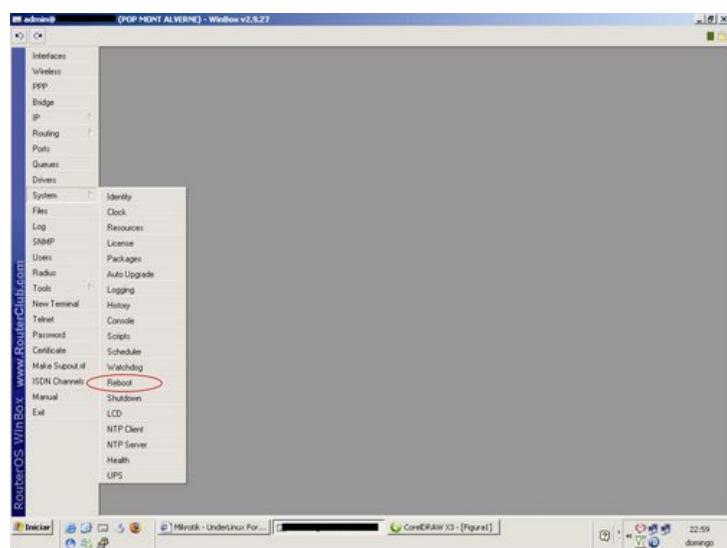
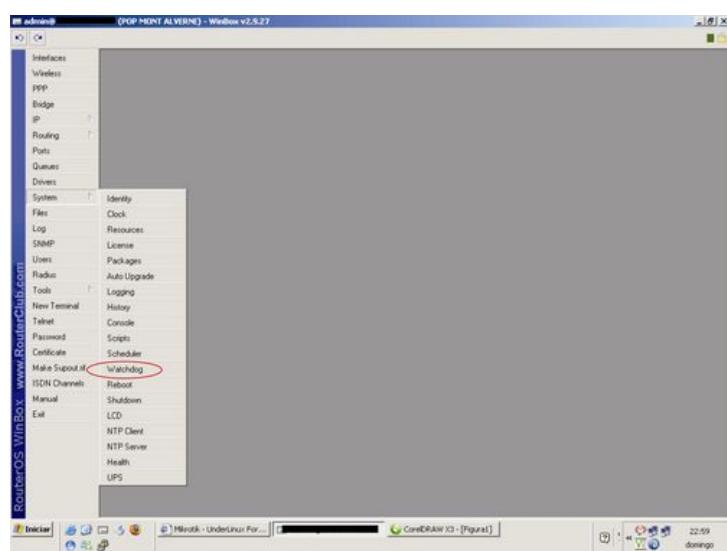
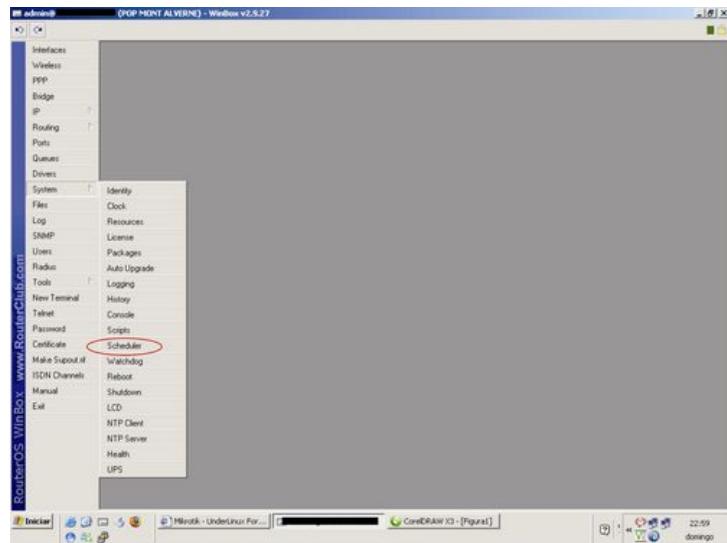
SUB-MENU SYSTEM

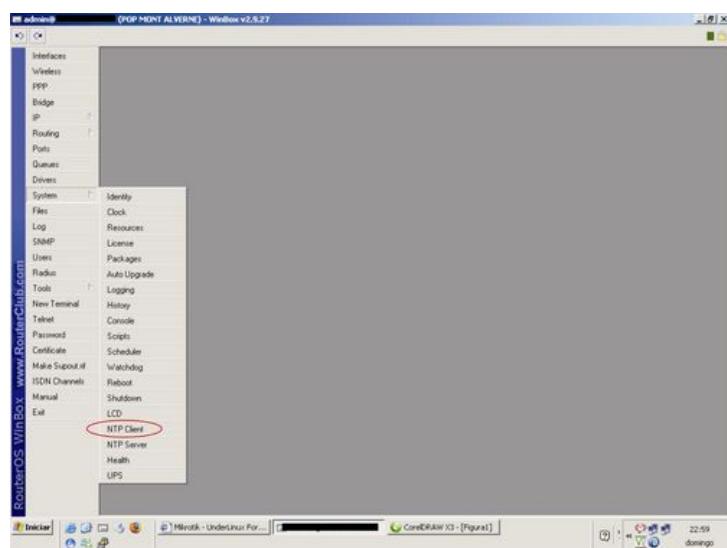
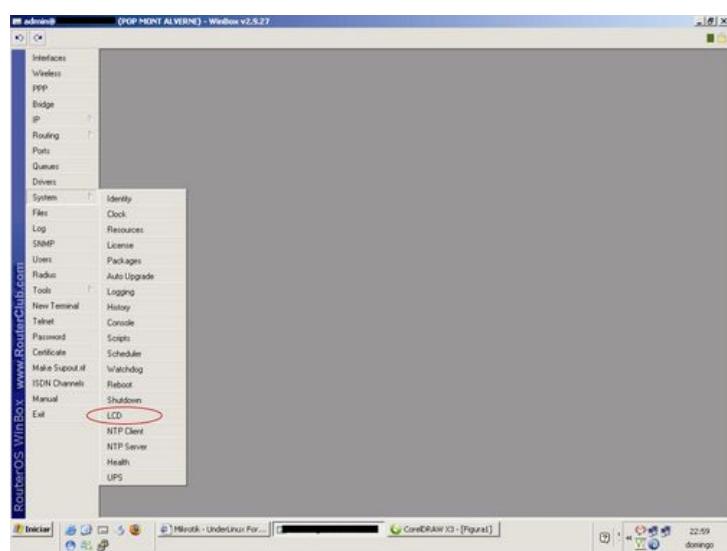
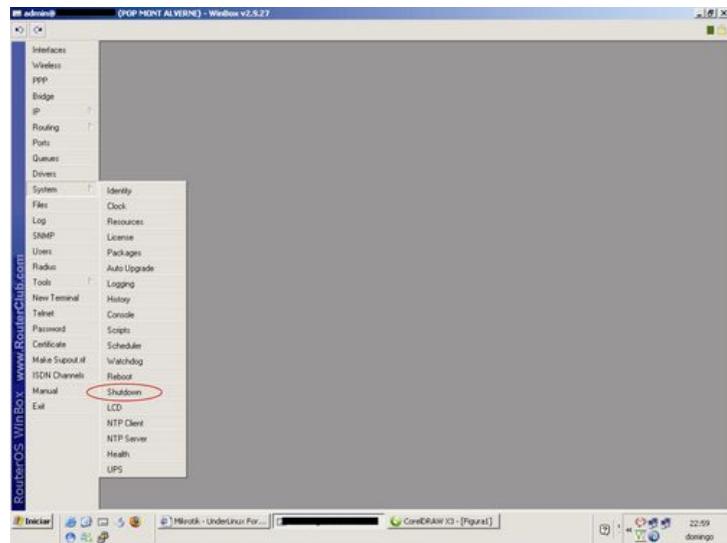


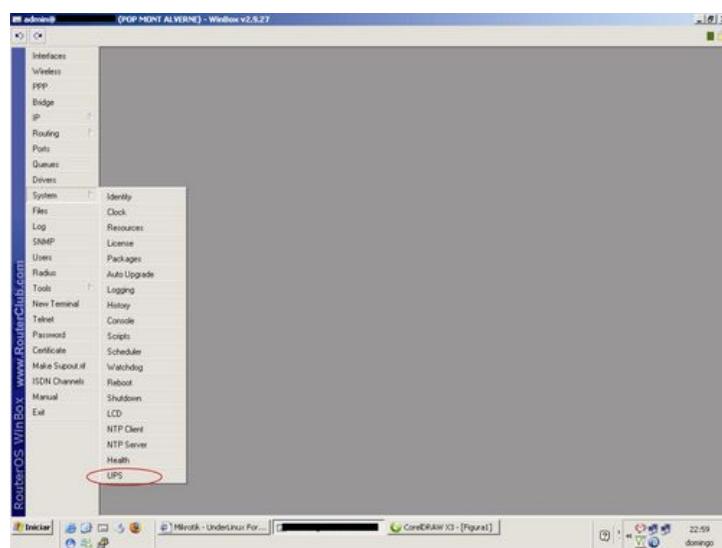
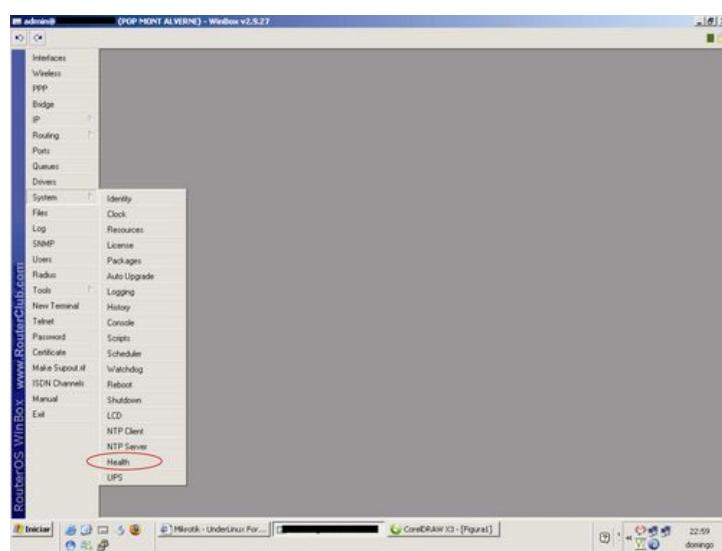
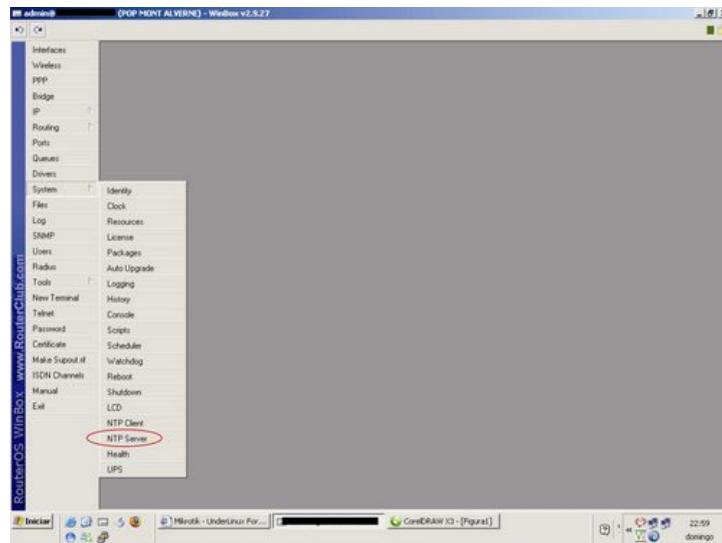












Instalação do MIKROTIK (Link Dedicado)

Utilizo link dedicado da brasil telecon, funciona assim, eles dao por exemplo 128 ips = faixa de 201.2.180.1 até 201.2.180.127, sendo o 201.2.180.1 o gateway, entao eh soh colocar o ip no servidor 201.2.180.2, e gateway e pronto..

Colocando ip Dedicado no cliente

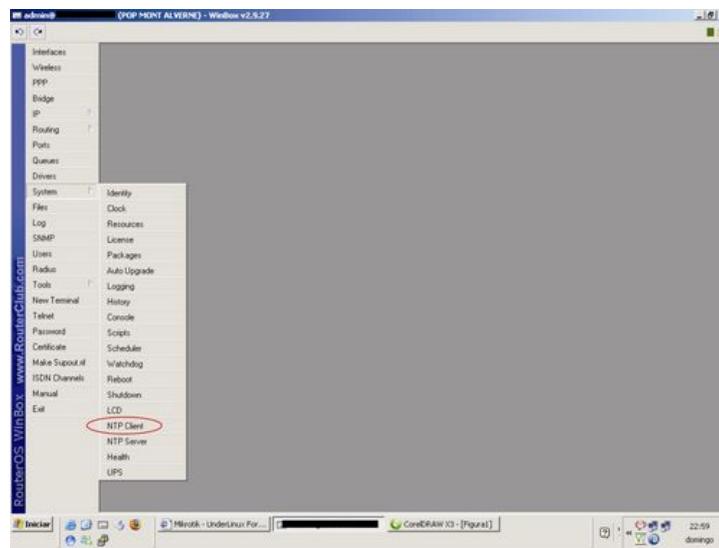
Se o cliente quer ip dedicado, cadastro ele na rede interna ex: 192.168.2.50 e adiciono mais um ip na interface do link 201.2.180.10 e faco uma regrinha no /ip firewall nat

```
add chain=dstnat dst-address=201.2.180.10 protocol=tcp dst-port=0-65535 \
action=dst-nat to-addresses=192.168.2.50 to-ports=0-65535 \
comment="Direcionando IP 192.168.2.50 para 201.2.180.10" disabled=no
```

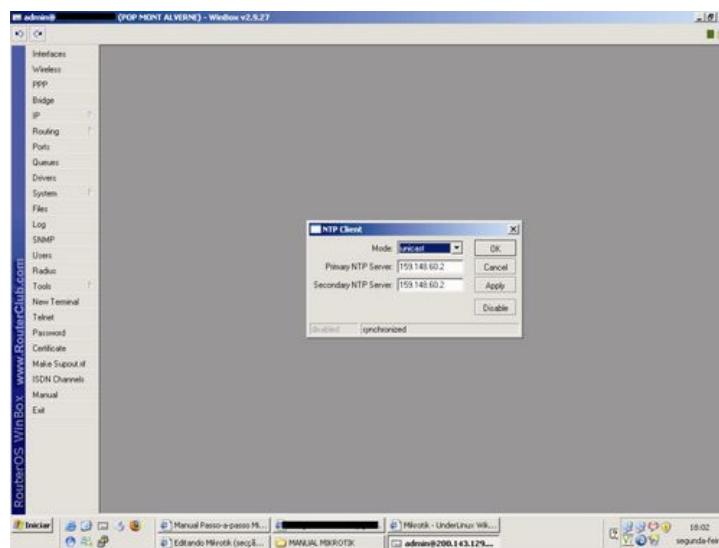
Configurando Servidor de Hora Automático

Aqui você irá aprender a configurar servidores NTP (network time protocol) automaticamente no mikrotik, via servidor de internet... Muito útil para quem trabalha com regras baseadas no horário e não pode ter hora errada, adianta ou atrasada.

Primeiro procedimento, abra o menu "NTP CLIENT"

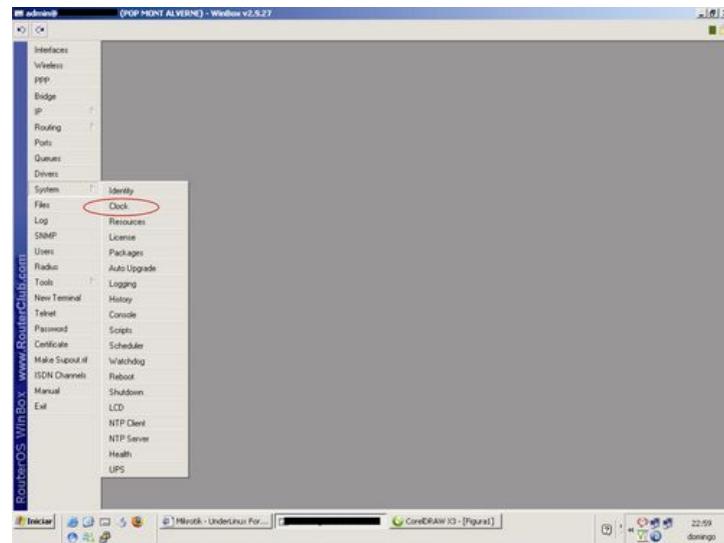


Configure como abaixo:

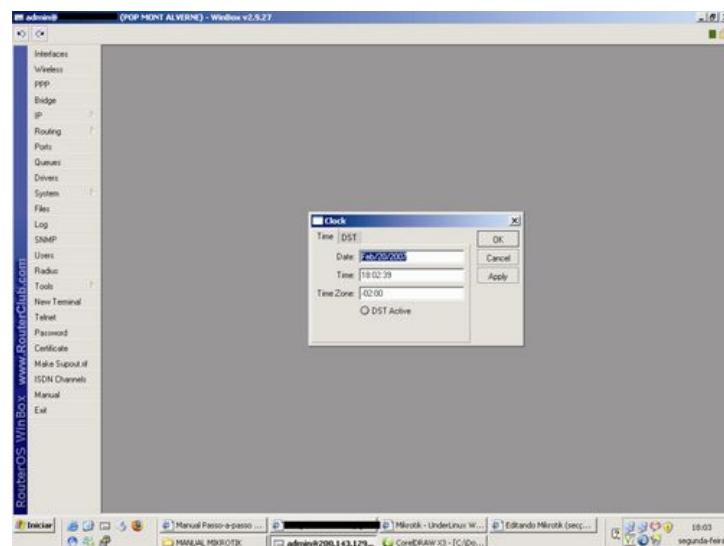


MODE - Escolha a opção "UNICAST"
PRIMARY NTP SERVER = 159.148.60.2
SECONDARY NTP SERVER = 159.148.60.2

Após configurar, aperte o botão ENABLE.
Abra o menu "CLOCK".



Configure o campo "Time Zone" de acordo com o fuso horário da sua cidade.



Você deve se basear no horário mundial (Greenwich). Aqui no Rio de Janeiro, é -2:00 de diferença.

Pronto!! Agora não precisa mais se preocupar com a hora certa do seu sistema!!!

Lista de SCRIPTS e AGENDAMENTOS úteis

Lista de Scripts prontos!!

TODOS OS SCRIPTS DEVEM SER INSERIDOS VIA WINBOX NO MENU SYSTEM>SCRIPTS OU VIA "NEW TERMINAL" /system script

SCRIPT PARA REBOOTAR AUTOMATICAMENTE

```
add name="reboot" source="/system reboot" \
policy=ftp,reboot,readonly,policy,test,winbox,password
```

SCRIPT PARA BACKUP AUTOMÁTICO DO MIKROTIK

```
add name="backup_diario" source="/sys ba sav name=mk_bkp.backup" \
policy=ftp,reboot,readonly,write,policy,test,winbox,password
```

SCRIPTS PARA HABILITAR E DESABILITAR TODA A BANDA

DESABILITA

```
add name="queue_disable" source="/queue simple { disable \[find \
```

```
name=LIBERA_TUDO\] }" \
policy=ftp,reboot,read,write,policy,test,winbox,password
```

HABILITA

```
add name="queue_enable" source="/queue simple { enable \[find \
name=LIBERA_TUDO\] }" \
policy=ftp,reboot,read,write,policy,test,winbox,password
```

AGENDAMENTOS ÚTEIS

Devem ser aplicados via winbox (menus system>scheduler) ou via "new terminal" em / system scheduler

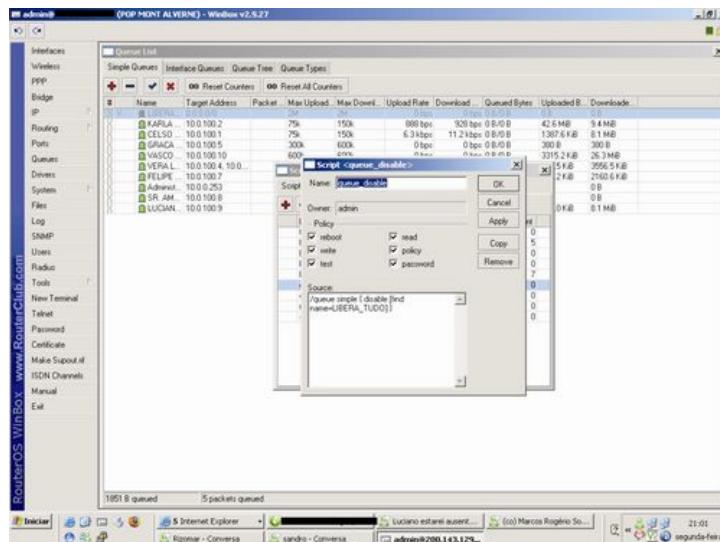
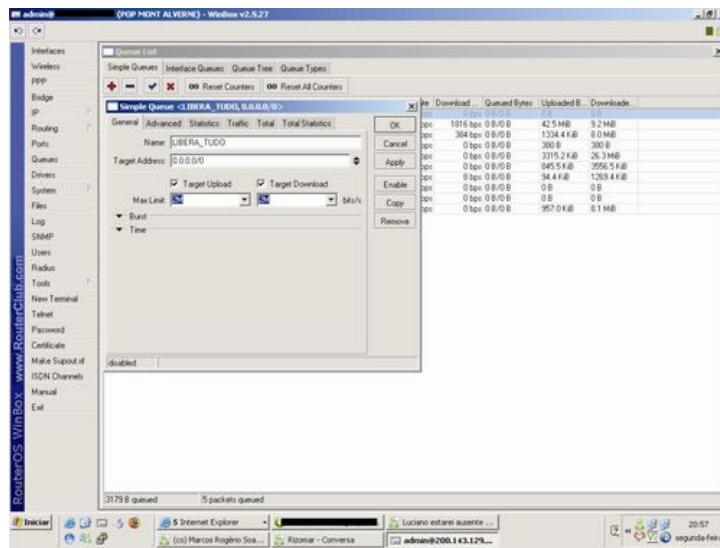
AGENDAMENTO PARA REBOOT DE 15 EM 15 DIAS

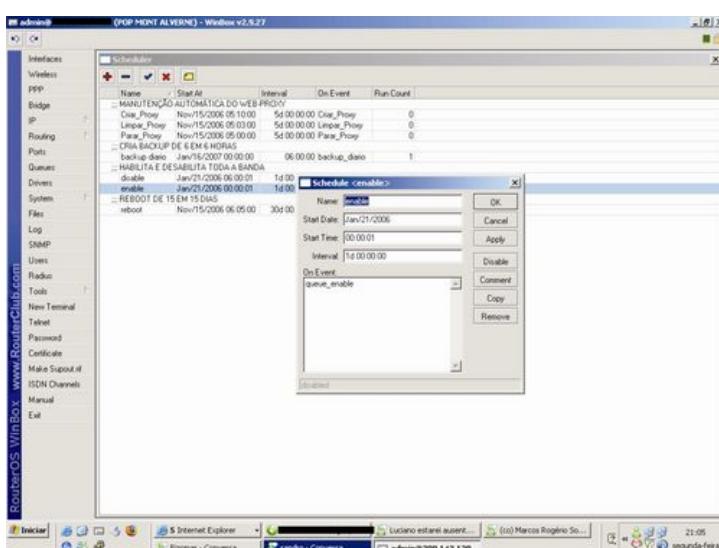
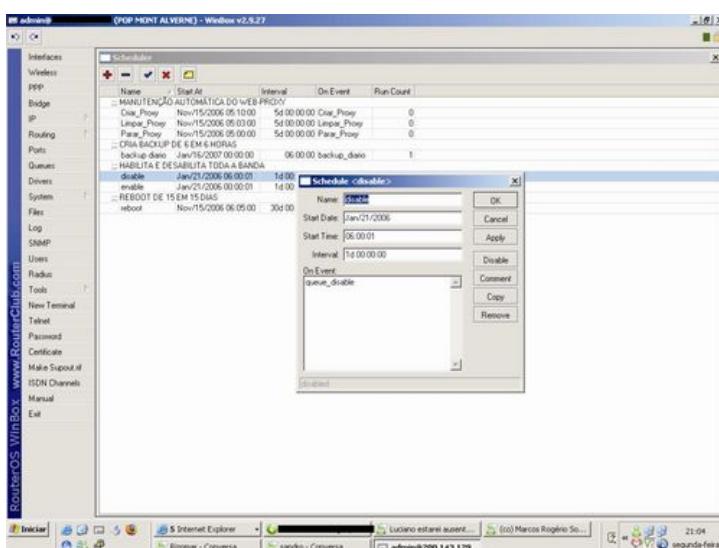
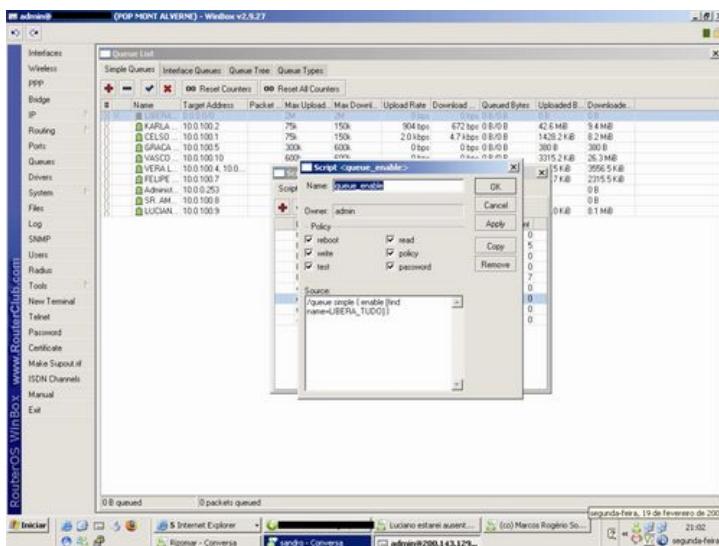
```
add name="reboot" on-event=reboot start-date=nov/15/2006 start-time=06:05:00 \
interval=4w2d comment="REBOOT DE 15 EM 15 DIAS" disabled=no
```

AGENDAMENTO PARA BACKUP AUTOMÁTICO DE 6 EM 6 HORAS

```
add name="backup diario" on-event=backup_diario start-date=jan/16/2007 \
start-time=00:00:00 interval=6h comment="CRIA BACKUP DE 6 EM 6 HORAS" \
disabled=no
```

Configurando Liberação Automática de Banda por hora determinada





LOADBALANCE - Visão Geral e Aplicação

Balanceamento de carga

Todo o hardware tem o seu limite, e muitas vezes o mesmo serviço tem que ser repartido por várias máquinas, sob pena de se tornar congestionado. Estas soluções podem-se especializar em pequenos grupos sobre os quais se faz um balanceamento de carga: utilização do CPU, de armazenamento, ou de rede. Qualquer uma delas introduz o conceito de clustering, ou server farm, já que o balanceamento será, provavelmente, feito para vários servidores.

Balanceamento de armazenamento (storage)

O balanceamento do suporte de armazenamento permite distribuir o acesso a sistemas de ficheiros por vários discos (software/hardware RAID), pelo que derivam ganhos óbvios em tempos acesso. Estas soluções podem ser dedicadas ou existir em cada um dos servidores do cluster.

Soluções
RAID
Storage Area Network

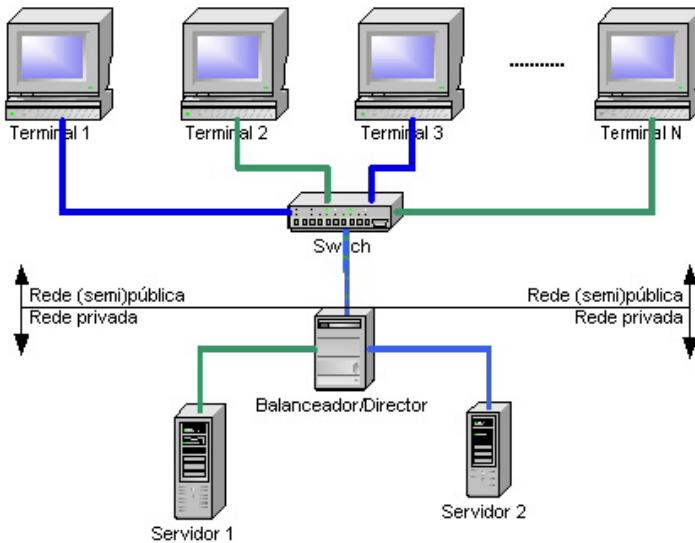


Figura 1 - Balanceamento de carga (NAT).

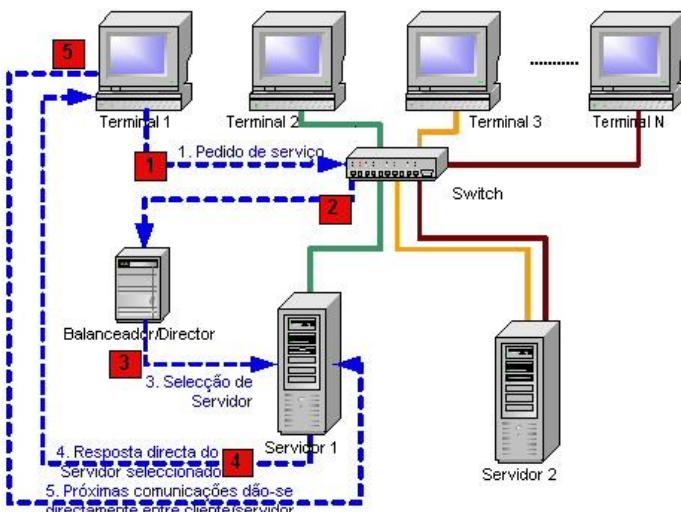


Figura 2 - Balanceamento de carga (Direct Routing).

Balanceamento de rede

O balanceamento da utilização da rede passa sobretudo por reencaminhar o tráfego por caminhos alternativos a fim de descongestionar os acessos aos servidores. Este balanceamento pode ocorrer a qualquer nível da camada OSI.

A Figura 1 sugere a existência de um mecanismo/dispositivo responsável pelo balanceamento (director). Na verdade, ele pode existir sob várias formas, dependendo do(s) serviço(s) que se pretende balancear. Este director serve também de interface entre o cluster de servidores e os clientes do(s) serviço(s) - tudo o que os clientes conhecem é o endereço semi-público deste servidor. Esta abordagem (clássica) é algo limitada, em termos de escalabilidade, ao número de tramas que o director consegue redireccionar, principalmente devido à velocidade dos buses das placas de rede. Existem, no entanto, outras soluções mais complexas que tiram melhor partido das características do protocolo TCP/IP em conjunto com routing especializado (NAT, IP Tunneling, Direct Routing).

Exemplo Um exemplo de um site a utilizar técnicas de balanceamento de carga é a própria Wikimedia Foundation e os seus projectos. Em Junho de 2004, a carga era balanceada usando uma combinação de:

Round robin DNS, que distribui os pedidos uniformemente para um dos três servidores de cache Squid;

Estes servidores de cache usam os tempos de resposta para distribuir os pedidos para cada um dos sete servidores de páginas. Em média, os servidores Squid já têm em cache páginas suficientes para satisfazer 75% dos pedidos sem sequer consultar os servidores de páginas; Os scripts PHP que formam a aplicação distribuem a carga para um de vários servidores de base de dados dependendo do tipo do pedido, com as atualizações indo para um servidor primário e as consultas para um ou mais servidores secundários.

Soluções (software) Existem soluções que operam exclusivamente em apenas algumas camadas (níveis) do Modelo OSI:

Balancamento de CPU

Este tipo de balanceamento é efectuado pelos sistemas de processamento distribuído e consiste, basicamente, em dividir a carga total de processamento pelos vários processadores no sistema (sejam eles locais ou remotos).

*Fonte: [Wikipedia](#)

Aplicação:

Tenho visto muitas pessoas confusas, quanto a aplicação do loadbalance... Alguns sugerem colocar lo 5 ou 10 links, pelo fato de ser "melhor"... Para que todos possam aproveitar o máximo dos recursos do loadbalance e também não gastar dinheiro desnecessariamente, deixemos claro as seguintes coisas:

Loadbalance, como o próprio nome diz é "**BALANÇAMENTO DE CARGA**" ou seja, divisão de carga da sua rede entre os links... Muitas pessoas se enganam e acham que loadbalance soma link (1mb + 1mb = 2mb), o que não é verdade... Para ter o máximo de desempenho em uma técnica de loadbalance, devemos primeiramente analizar as necessidades de cada rede, para assim, criar um loadbalance com o máximo de desempenho para nossa rede...

Ligaçāo externa (<http://www.wikimedia.org>)

LOADBALANCE - IPD X IPD

LOADBALANCE - ADSL X IPD
LOADBALANCE - ADSL X ADSL

IPD(IP DEDICADO)

```
/ ip firewall mangle
add chain=prerouting in-interface= Link1 connection-state=new nth=1,1,0 action=mark-connection
new-connection-mark=Link1 passthrough=yes comment="Balanceamento de carga" disabled=no
add chain=prerouting in-interface= Link1 connection-mark=Link1 action=mark-routing
new-routing-mark=Link1 passthrough=no comment="" disabled=no
add chain=prerouting in-interface= Link2 connection-state=new nth=1,1,1 action=mark-connection
new-connection-mark=Link2 passthrough=yes comment="" disabled=no
add chain=prerouting in-interface= Link2 connection-mark=Link2 action=mark-routing
new-routing-mark=Link2 passthrough=no comment="" disabled=no
```

```
/ ip firewall nat
add chain=srcnat out.interface= Link1 Actoin=Link1 comment="Nat Link1" disabled=no
add chain=srcnat out.interface= Link2 Actoin=Link2 comment="Nat Link2" disabled=no
```

```
/ ip route
add dst-address=0.0.0.0/0 gateway=192.168.254.254 scope=255 target-scope=10 routing-mark=Link1
comment="Gateway adsl1" disabled=no
add dst-address=0.0.0.0/0 gateway=192.168.253.253 scope=255 target-scope=10 routing-mark=Link2
comment="Gateway adsl2" disabled=no
add dst-address=0.0.0.0/0 gateway=192.168.254.254 scope=255 target-scope=10 comment="principal" disabled=yes
```

Tratamento de portas

```
/ ip firewall mangle
add chain=prerouting protocol=tcp dst-port=80 action=mark-routing new-routing-mark=link2
passthrough=yes \
comment="HTTP no link2" disabled=no
add chain=prerouting routing-mark=link2 action=mark-packet new-packet-mark=link2 passthrough=yes \
comment="Pacotes marcados do Link2" disabled=no

add chain=prerouting protocol=tcp dst-port=443 action=mark-routing new-routing-mark=link2
passthrough=yes \
comment="HTTPS no Link2" disabled=no
add chain=prerouting routing-mark=link2 action=mark-packet new-packet-mark=link2 passthrough=yes \
comment="Pacotes marcados do Link2" disabled=no

add chain=prerouting protocol=tcp dst-port=1863 action=mark-routing new-routing-mark=link2
passthrough=yes \
comment="MSN no Link2" disabled=no
add chain=prerouting routing-mark=link2 action=mark-packet new-packet-mark=link2 passthrough=yes \
comment="Pacotes marcados do Link2" disabled=no

add chain=prerouting protocol=tcp dst-port=21 action=mark-routing new-routing-mark=link1
passthrough=yes \
comment="FTP no link1" disabled=no
add chain=prerouting routing-mark=link1 action=mark-packet new-packet-mark=link1 passthrough=yes \
comment="Pacotes marcados do Link1" disabled=no

add chain=prerouting protocol=tcp dst-port=22 action=mark-routing new-routing-mark=link1
passthrough=yes \

```

```

comment="SSH no Link1" disabled=no
add chain=prerouting routing-mark=link1 action=mark-packet new-packet-mark=link1 passthrough=yes \
comment="Pacotes marcados do Link1" disabled=no

add chain=prerouting protocol=tcp dst-port=23 action=mark-routing new-routing-mark=link1
passthrough=yes \
comment="TELNET" disabled=no
add chain=prerouting routing-mark=link1 action=mark-packet new-packet-mark=link1 passthrough=yes \
comment="Pacotes marcados do Link1" disabled=no

add chain=prerouting protocol=tcp dst-port=25 action=mark-routing new-routing-mark=link1
passthrough=yes \
comment="SMTP" disabled=no
add chain=prerouting routing-mark=link1 action=mark-packet new-packet-mark=link1 passthrough=yes \
comment="Pacotes marcados do Link1" disabled=no

add chain=prerouting protocol=tcp dst-port=53 action=mark-routing new-routing-mark=link1
passthrough=yes \
comment="DNS" disabled=no
add chain=prerouting routing-mark=link1 action=mark-packet new-packet-mark=link1 passthrough=yes \
comment="Pacotes marcados do Link1" disabled=no

add chain=prerouting protocol=tcp dst-port=110 action=mark-routing new-routing-mark=link1
passthrough=yes \
comment="POP3" disabled=no
add chain=prerouting routing-mark=link1 action=mark-packet new-packet-mark=link1 passthrough=yes \
comment="Pacotes marcados do Link1" disabled=no

add chain=prerouting protocol=tcp dst-port=1080 action=mark-routing new-routing-mark=link1
passthrough=yes \
comment="" disabled=no
add chain=prerouting routing-mark=link1 action=mark-packet new-packet-mark=link1 passthrough=yes \
comment="Pacotes marcados do Link1" disabled=no

add chain=prerouting protocol=tcp p2p=all-p2p action=mark-routing new-routing-mark=link1
passthrough=yes \
comment="p2p no link1" disabled=no
add chain=prerouting routing-mark=link1 action=mark-packet new-packet-mark=link1 passthrough=yes \
comment="Pacotes marcados do Link1" disabled=no

```

Autor: SHTURBO-INTERNET (<http://www.shturbo.com.br>)

LOADBALANCE - DIVIDINDO CARGA DE FORMA PERSONALIZADA ENTRE OS LINKS

Tratamento de portas

```

/ ip firewall mangle
add chain=prerouting protocol=tcp dst-port=80 action=mark-routing new-routing-mark=link2
passthrough=yes \
comment="HTTP no link2" disabled=no
add chain=prerouting routing-mark=link2 action=mark-packet new-packet-mark=link2 passthrough=yes \
comment="Pacotes marcados do Link2" disabled=no

add chain=prerouting protocol=tcp dst-port=443 action=mark-routing new-routing-mark=link2
passthrough=yes \
comment="HTTPS no Link2" disabled=no
add chain=prerouting routing-mark=link2 action=mark-packet new-packet-mark=link2 passthrough=yes \
comment="Pacotes marcados do Link2" disabled=no

add chain=prerouting protocol=tcp dst-port=1863 action=mark-routing new-routing-mark=link2
passthrough=yes \
comment="MSN no Link2" disabled=no
add chain=prerouting routing-mark=link2 action=mark-packet new-packet-mark=link2 passthrough=yes \
comment="Pacotes marcados do Link2" disabled=no

add chain=prerouting protocol=tcp dst-port=21 action=mark-routing new-routing-mark=link1
passthrough=yes \
comment="FTP no link1" disabled=no
add chain=prerouting routing-mark=link1 action=mark-packet new-packet-mark=link1 passthrough=yes \
comment="Pacotes marcados do Link1" disabled=no

add chain=prerouting protocol=tcp dst-port=22 action=mark-routing new-routing-mark=link1
passthrough=yes \
comment="SSH no Link1" disabled=no
add chain=prerouting routing-mark=link1 action=mark-packet new-packet-mark=link1 passthrough=yes \
comment="Pacotes marcados do Link1" disabled=no

add chain=prerouting protocol=tcp dst-port=23 action=mark-routing new-routing-mark=link1
passthrough=yes \
comment="TELNET" disabled=no
add chain=prerouting routing-mark=link1 action=mark-packet new-packet-mark=link1 passthrough=yes \
comment="Pacotes marcados do Link1" disabled=no

add chain=prerouting protocol=tcp dst-port=25 action=mark-routing new-routing-mark=link1
passthrough=yes \
comment="SMTP" disabled=no
add chain=prerouting routing-mark=link1 action=mark-packet new-packet-mark=link1 passthrough=yes \
comment="Pacotes marcados do Link1" disabled=no

```

```

comment="Pacotes marcados do Link1" disabled=no

add chain=prerouting protocol=tcp dst-port=53 action=mark-routing new-routing-mark=link1
passthrough=yes \
comment="DNS" disabled=no
add chain=prerouting routing-mark=link1 action=mark-packet new-packet-mark=link1 passthrough=yes \
comment="Pacotes marcados do Link1" disabled=no

add chain=prerouting protocol=tcp dst-port=110 action=mark-routing new-routing-mark=link1
passthrough=yes \
comment="POP3" disabled=no
add chain=prerouting routing-mark=link1 action=mark-packet new-packet-mark=link1 passthrough=yes \
comment="Pacotes marcados do Link1" disabled=no

add chain=prerouting protocol=tcp dst-port=1080 action=mark-routing new-routing-mark=link1
passthrough=yes \
comment="" disabled=no
add chain=prerouting routing-mark=link1 action=mark-packet new-packet-mark=link1 passthrough=yes \
comment="Pacotes marcados do Link1" disabled=no

add chain=prerouting protocol=tcp p2p=all-p2p action=mark-routing new-routing-mark=link1
passthrough=yes \
comment="p2p no link1" disabled=no
add chain=prerouting routing-mark=link1 action=mark-packet new-packet-mark=link1 passthrough=yes \
comment="Pacotes marcados do Link1" disabled=no

```

Autor: SHTURBO-INTERNET (<http://www.shturbo.com.br>)

Mk como AP-bridge

Primeiro você vai em interface e veja se a placa wireless e a ethernet estão ativas (se tiver esmaecida (cinza) clique nela e enable). Feito Isto vá em bridge e clique no "+" e crie uma bridge . Ainda no menu bridge clique em port vai aparecer suas placas de redes. Assim basta clicar em cada placa de rede e adicionar o nome da bridge criada.

Depois disso você adiciona um ip para a bridge e exclui os ips anteriores das placas. Pronto, seu Access Point mikrotik foi criado.

FIREWALL

Gráficos em Tempo Real do Mikrotik

primeiro vá em IP=>SERVICES,modifique a aporta do serviço WWW. no meu caso usei 809. pois vc poderá precisar da porta 80 para algum servidor web na sua rede e outra,impedira que outros fique fucando seu MT.

Logo apos vá em TOOLS=>GRAPHING

Adicione as rules que vc tem nescessidade:

Queue Rules:monitora as regras de velocidade de seus clientes.

Interfaces Rules:Monitora as interfaces de rede do seu MT

Resource Rules :Monitora CPU,MEMORY e UPTIME do seu MT.

Agora o teste,digite no seu navegador op ip do seu MT junto scom a porta do seu MT.no meu caso <http://192.168.0.254:809> .não esqueça da porta que vc modificou em IP=>SERVICES.

Veja que ai vc têm algumas opções ,mas vá no que interessa em GRAPHS. escolha qual grafico vc deseja verificar. clique em cima da opção que o grafico sera mostrado.

DICA:vcê pode bloquear esta porta para o uso externo em:

IP=>FIREWALL=>FILTER RULES

Adicione uma nova regra e deixe assim.

CHAIN:forward PROTOCOL:tcp DST PORT:(porta que vc modificou para servico www) IN INTERFACE:(interface da internet) ACTION:drop.

Use o programa (cliente DDNS) da winco tecnologia para monitorar seus MT que estão por ai sem ip fixo.

ander_bj{NOSPAM}hotmail.com

Sobre o autor

David Marcony, conhecido como CATVBRASIL, é professor oficial da Mikrotik desde 2009, também é consultor oficial da Mikrotik desde 2008. Pesquisador de tecnologias, já participou de diversos treinamentos, trabalha com wireless e mikrotik. Ministra treinamentos oficial por todo o Brasil e também consultorias especializadas a várias empresas.

Abaixo meus contatos:

David Marcony - **catvbrasil** - Training Oficial Mikrotik

MIKROTIK, VOIP, IPTV - Consultoria & Treinamento

Telefones:

Todos os meus números mudaram!!

21-2233-8124

21-7719-4073 (nextel)

83*101357 (nextel ID)

catvbrasil@hotmail.com

www.catvbrasil.com.br



David Marcony, conhecido como CATVBRASIL



Certificado Oficial de Trainer and Pather da Mikrotik



Certificado Oficial MTCNA pela FS INTERNET, empresa séria, 75% de acertos, sem consulta e prova em inglês



Certificado Oficial MTCTCE diretamente pela Mikrotik Internacional, 75% de acertos sem consulta. Prova e treinamento em Ingles realizado em Dallas (Texas - EUA)

Obtida de "<http://under-linux.org/wiki/Mikrotik>"

0

The advertisement features the 'Microwave' logo with a signal icon. It says 'DISTRIBUIDOR OFICIAL MIKROTIK' and 'OS MELHORES PREÇOS DO MERCADO'. On the right, it shows a white 'CPE MIKROTIK SXT' device with the text 'PREÇO ESPECIAL DE LANÇAMENTO! R\$265,00'. A small note below says '* Valor em até 3x no Boleto e 4x no Cartão de Crédito. Sem juros!'.

Fale Conosco Under-Linux.Org Condições de Uso Sobre FAQ Topo

Todos horários são GMT -3. Hora atual: 23:32