ankaa
wireless solutions

GUIA EXCLUSIVO DE REFERÊNCIA

MikroTik™

COMO ACESSAR O ROUTEROS MIKROTIK

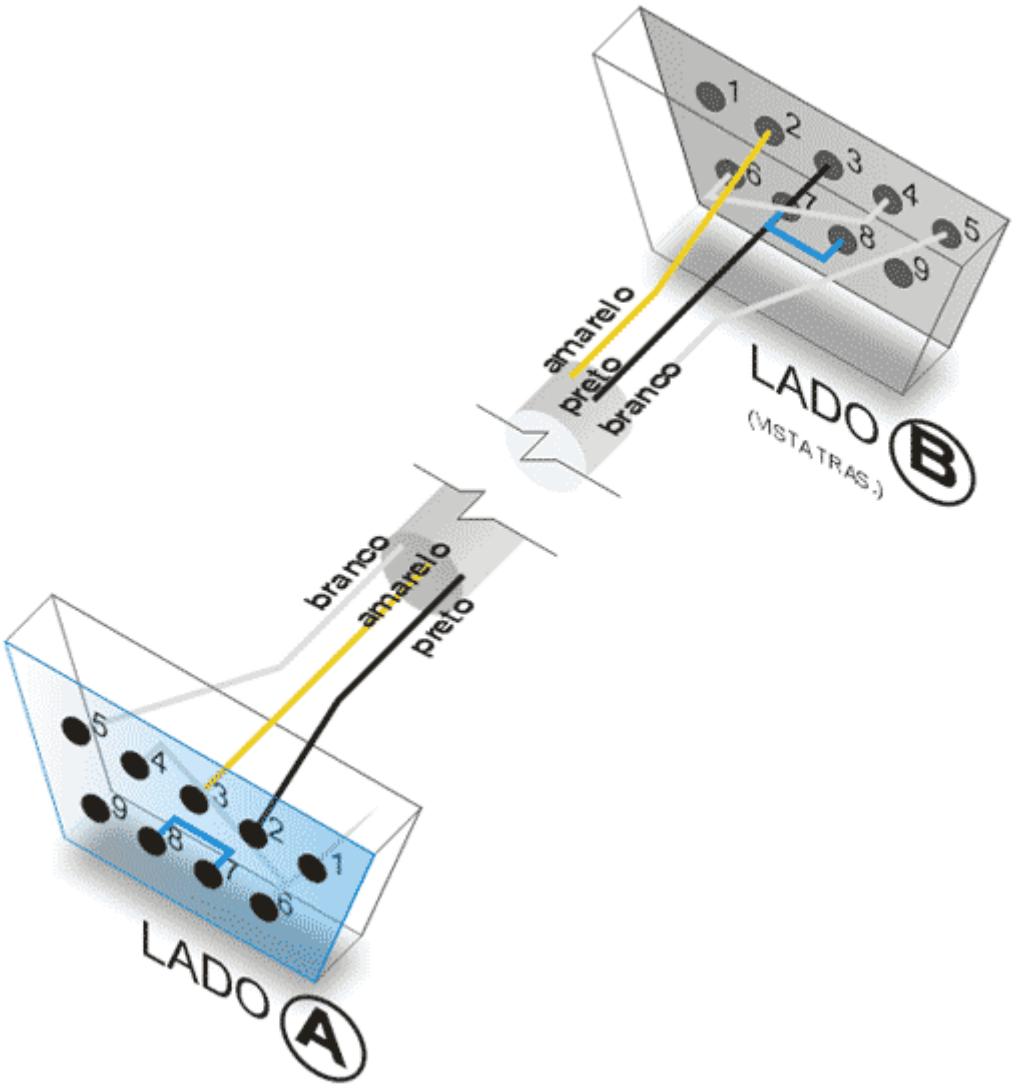
O roteador RouterOS pode ser acessado das seguintes maneiras:

- Monitor e teclado
- Terminal Serial (default 8 / N / 1 – velocidade 9600)
- Telnet
- Telnet de MAC
- SSH
- Interface Gráfica Winbox em windows
- Interface Gráfica Winbox em Linux com Wine

ACESSO VIA TERMINAL

- **Primeiro acesso**:
  - Pode ser no próprio box, via serial, SSH ou telnet
  - Usuário: admin
  - Senha: (em branco)

- Configuração do Cabo Serial – Conector DB9



- **Ajuda**
  - ?: Mostra um help para o diretório em que se esteja
    [Mikrotik] > ?
  - ? Após um comando incompleto: Mostra as opções adicionais disponíveis.
    [Mikrotik] > interface ?

- **Navegação nos níveis de diretório**
  - [Mikrotik] > interface {enter}
  - [Mikrotik] interface > wireless {enter}
  - [Mikrotik] interface wireless > print {enter}
  - Pode-se ir diretamente com / interface wireless print
  - / Para voltar na raiz

- **Tecla TAB**
  - Comandos não precisam ser totalmente digitados, podendo ser completados com a tecla TAB
  - Havendo mais de uma opção para o já digitado, se pressionar TAB duas vezes mostra as opções.

Comandos mais comuns

- **Print**: Pode ser usado com diversos argumentos como:
  - print status
  - print detail
  - print interval, etc

- **Monitor**: Usado repetidamente mostra o status
  / interface wireless monitor wlan1

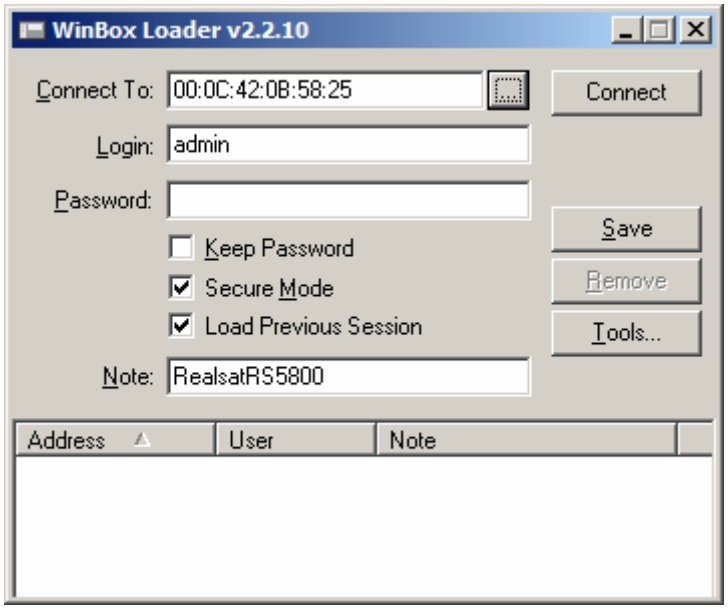
- **Manipulação de regras**
  - add: adiciona regras
  - set: muda regras
  - remove: remove regras
  - disable: desabilita a regra sem apaga-la
  - move: move algumas regras cuja ordem influencie (firewall por exemplo)

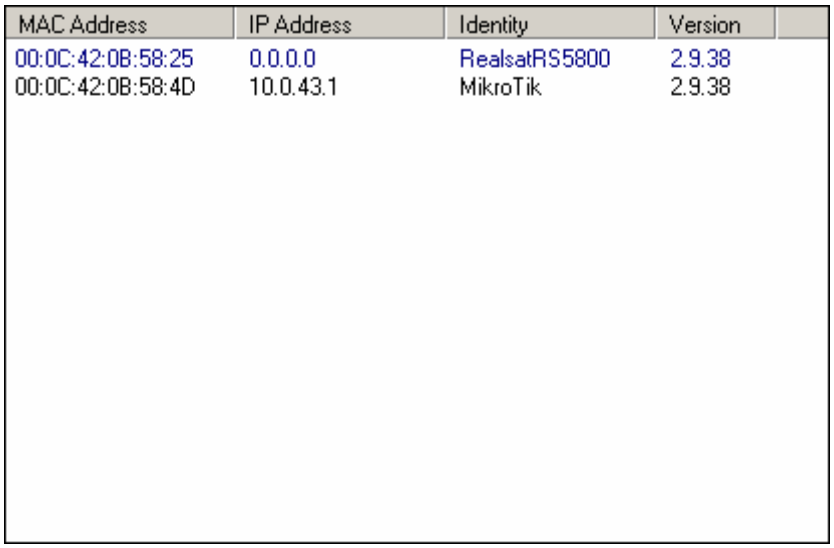
- **export**: exporta todas as configurações do diretório corrente acima (se estiver em /, do roteador todo). O resultado pode ser copiado com o botão direito do mouse e colado em editor de textos.

ACESSO VIA WINBOX GUI

Interface Gráfica para administração do Mikrotik
- Funciona em Windows e Linux (Wine)
- Utiliza a porta TCP 8291

Para Download: http://www.mikrotik.com/download/winbox.exe





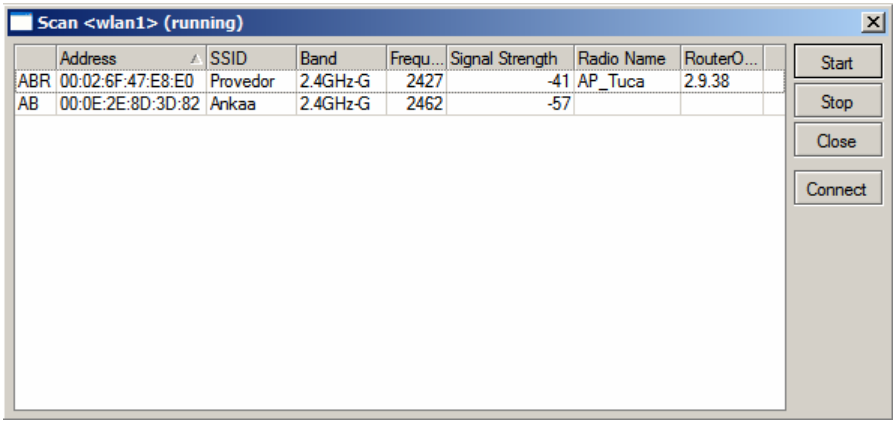
Significado dos ícones:

- Adicionar novas entradas
- Remover entradas existentes
- Habilitar o item
- Desabilitar o item
- Acrescentar ou adicionar comentários
- Desfazer a ação
- Refazer a ação

INTERFACE WIRELESS

Botão – Scan

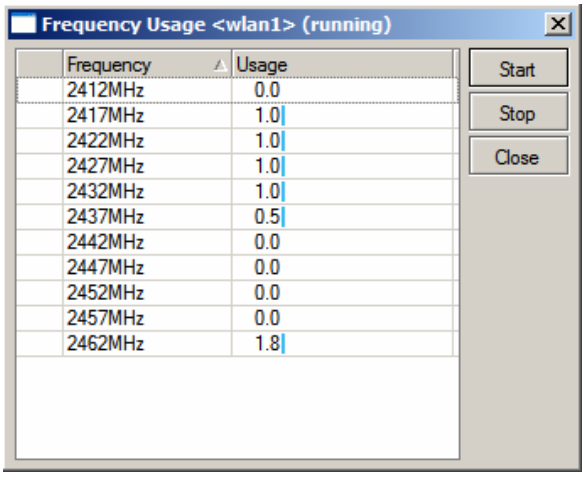
Escaneia o meio (causa queda das conexões estabelecidas)
A – Ativa
B – BSS
P – Protegida
R – Rede Mikrotik
N – Nstreme



Botão – Freq. Usage

Mostra o uso as freqüências em todo o espectro, para site survey

Obs.: Ao utilizar esta opção, a conexão estabelecida é interrompida.

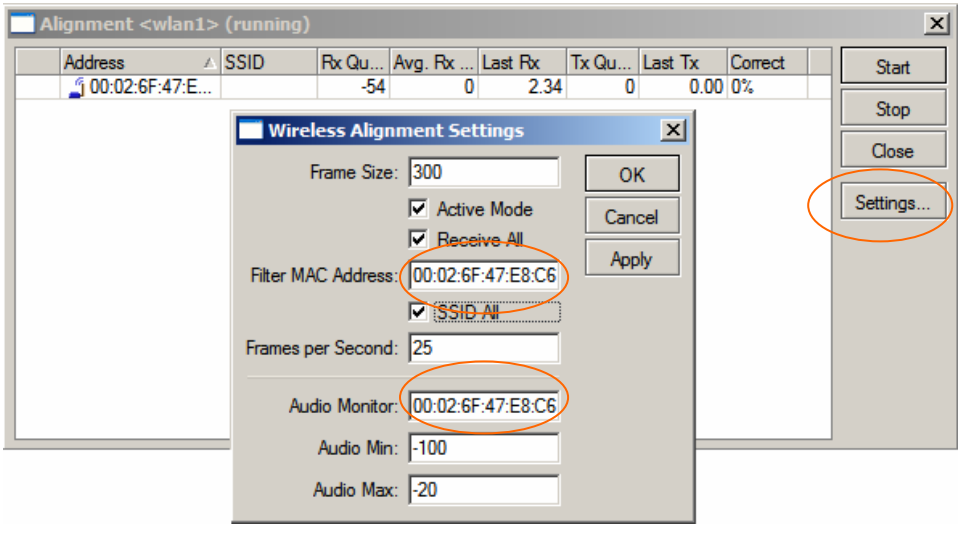


Botão - Align

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

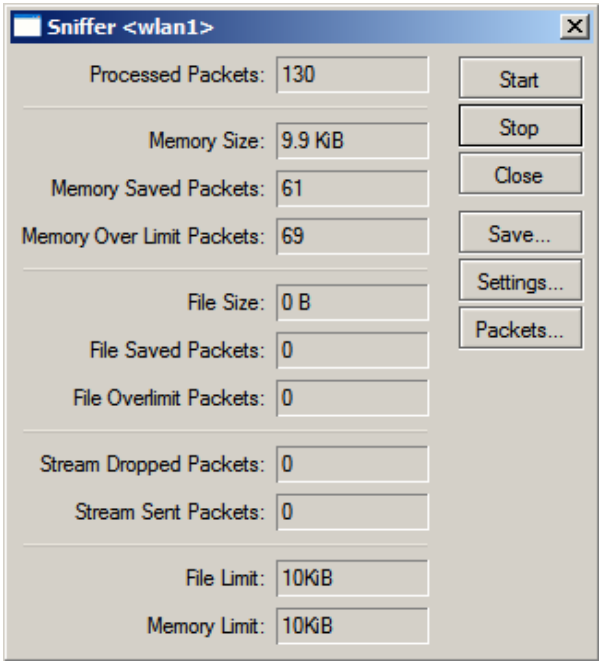
Obs.: Ao utilizar esta opção, a conexão estabelecida é interrompida.

Rx Quality – Potência (dBm) do último pacote recebido
Avg. Rx Quality – Potência média dos pacotes recebidos
Last Rx – Tempo em segundos do último pacote recebido
Tx Quality – Potência do último pacote transmitido
Last Tx – Tempo em segundos do ultimo pacote transmitido



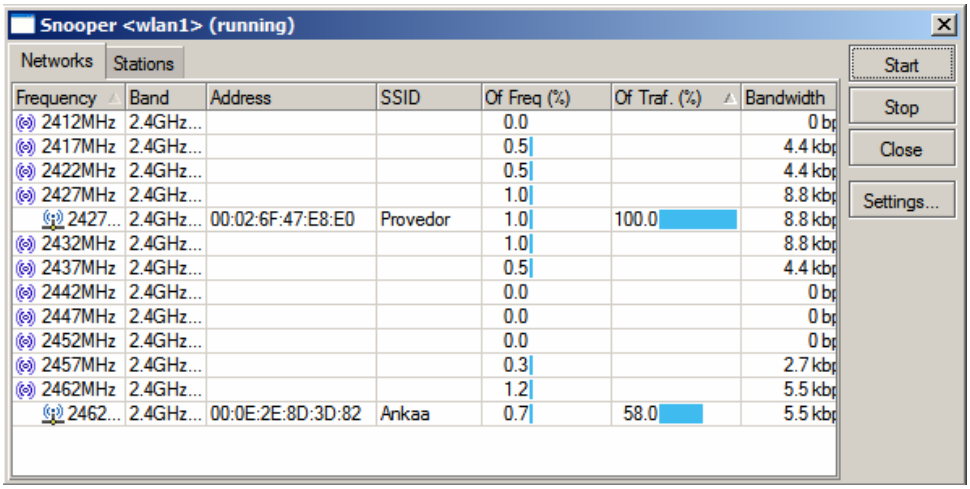
Botão – Sniff

Ferramenta para sniffar o ambiente wireless captando e decifrando pacotes
Muito útil para detectar ataques do tipo deauth attack e monkey jack.
Pode ser arquivado no próprio Mikrotik ou passado por streaming para outro servidor com protocolo TZSP

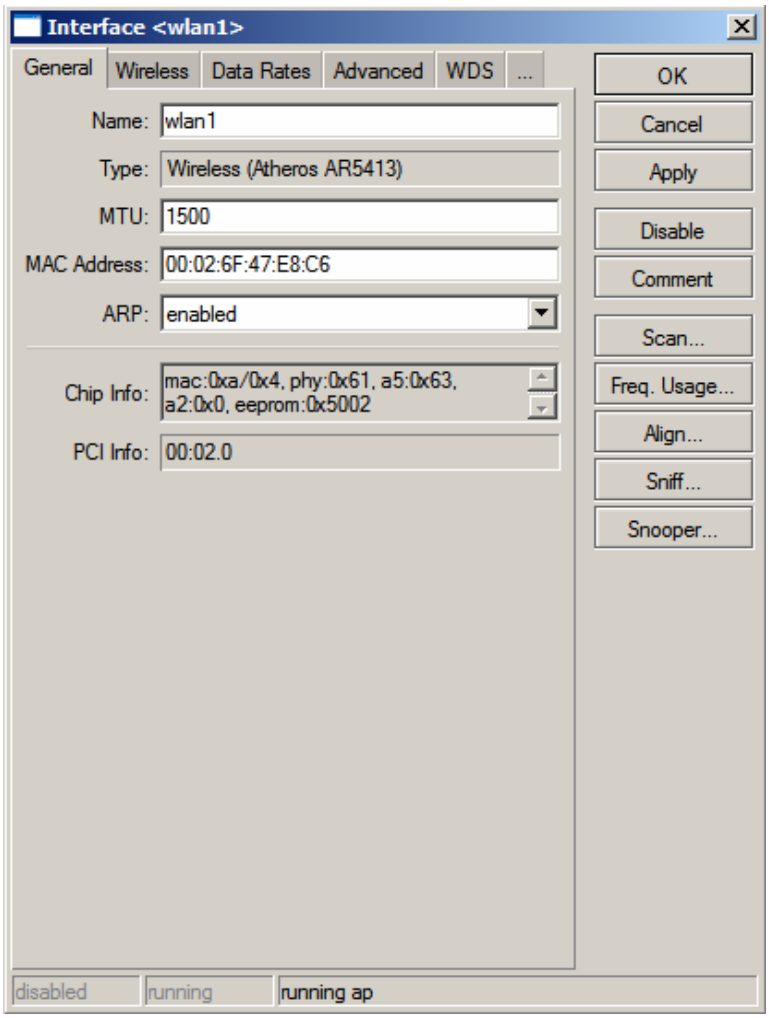


Botão – Snooper

Com a ferramenta Snooper é possível monitorar a carga de tráfego em cada canal, por estação ou por rede.
Esta opção escaneia as freqüências definidas em scan-list da interface.



Guia – General



Name: Nome da Interface.

Type: wireless.

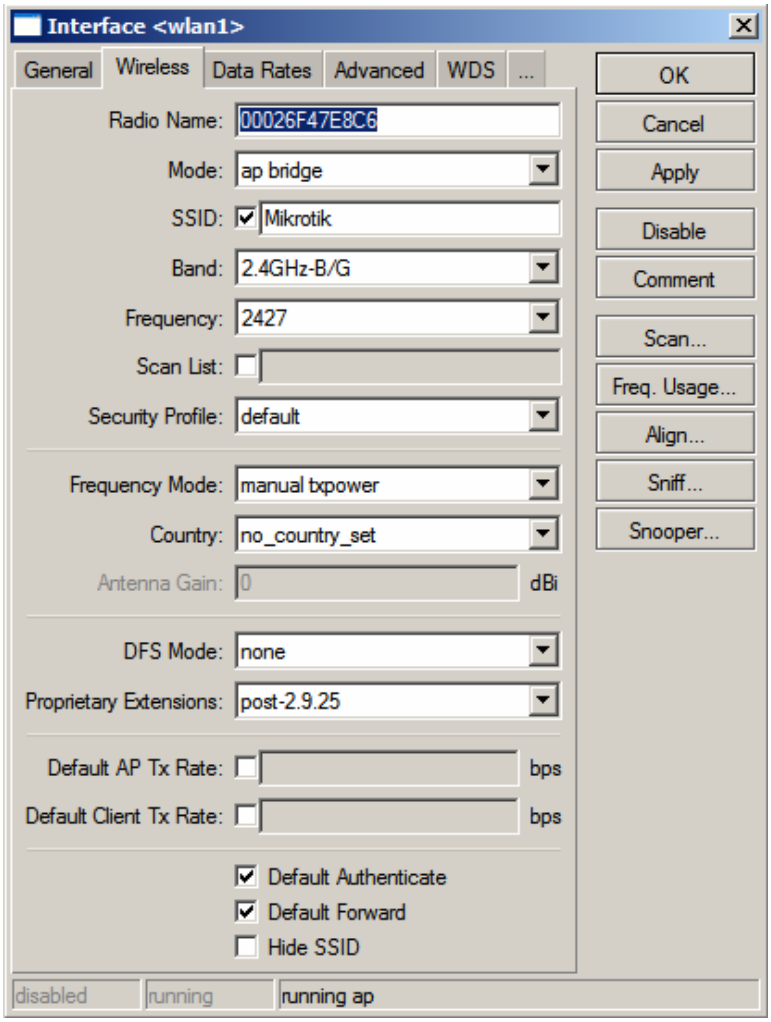
MTU: Unidade máxima de transferência (bytes).

MAC Address: Endereço MAC da interface.

Chip Info / PCI Info: Informações da placa;

ARP: - **disable**: não responde a solicitações ARP. Clientes tem que acessar tabelas estáticas;
- **proxy-arp**: passa o seu próprio MAC quando há uma requisição para algum host interno ao roteador;
- **reply-only**: somente responde as requisições. Endereços de vizinhos são resolvidos estaticamente.

Guia – Wireless



Radio Name: apelido usado para identificar a interface.

Mode: Modo de operação.

- **station**: modo cliente de AP. Não pode ser "bridgeado". Não passa os MACs internos, mas somente o seu;
- **station wds**: estação que pode ser "bridgeada", passando transparentemente os MACs. AP precisa estar em WDS;
- **ap-bridge**: Modo Access Point normal;
- modo ponto de acesso para suportar um cliente somente (links ponto a ponto);
- **alignment-only**: modo para alinhar antenas e monitorar sinal;
- **nstreme-dual-slave**: para enlaces em modo nstreme dual;
- **wds-slave**: trabalha como ponto de acesso escravo, adaptando-se a um WDS mestre (adapta-se às configurações da mestre).

SSID: Nome de rede.

Band: Banda e modo de operação.
- **2.4Ghz-b**: 802.1b até 11mbps;
- **2.4Ghz-b/g**: 802.11b até 11mbps e 802.11g até 54mbps (modo misto);
- **2.4Ghz-only-g**: 801.11g até 54mbps (somente clientes g);
- **2.4Ghz-g-turbo**: modo proprietário Atheros até 108mbps;
- **5Ghz:** 802.11a até 54mbps;
- **5Ghz-turbo**: Modo proprietário Atheros até 108mbps;
- **2.Ghz-10Mhz**: Modo "cloacking", utiliza canal de 10Mhz;
- **2.Ghz-5Mhz**: Modo "cloacking", utiliza canal de 5Mhz;
- **5.Ghz-10Mhz**: Modo "cloacking", utiliza canal de 10Mhz;
- **5.Ghz-5Mhz**: Modo "cloacking", utiliza canal de 5Mhz.

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

Scan List: lista de freqüências a serem escaneadas.
- Quando a interface está configurada como cliente, serão "procuradas" APs que estiverem nessa lista;
- Por default, serão buscadas as freqüências do domínio regulatório;
- Pode-se forçar o escaneamento de freqüências especificas, colocando-as separadas por vírgula.

Secutity Profile: Perfil de segurança. Perfis de segurança podem ser criados/alterados em Wireless/Security profiles.

Frequency Mode:
- **Regulatory domain**: somente são permitidas o uso das freqüências do país indicado no campo Country, sendo que a potência máxima de transmissão EIRP será limitada de acordo com a legislação, considerando-se o ganho de antena indicado no campo Antenna Gain;
- **Manual-tx-power**: os canais permitidos são os do país selecionado mas a potência é informada pelo operador;
- **superchannel**: somente possível com a licença superchannel. Todos os canais e potências suportados pelo hardware serão permitidos.

Country: País de operação.

Antenna Gain: Ganho da antena em dBi.

DFS Mode: Modo de seleção dinâmica de freqüência.
- **none**: Não usa DFS;
- **no-radar-detect:** O AP escaneia os canais da "scan-list" e escolhe para operar na menor freqüência detectada;
- **radar-detect**: O AP escaneia a partir da "scan-list" e escolhe a menos freqüência detectada. Se durante 60 segundos não é detectado nesse canal, ela começa a operar nesse canal, caso contrário continua escaneando sempre pelos canais menos ocupados.

Observação: No Brasil é necessário DFS para operar de 5250-5350 e 5470-5725 e existem valores mínimos em dBm que, se detectados não é permitida a operação nesses canais (art. 50 da resolução 365/2004 da Anatel).

Proprietary extensions: Método para inserir informações adicionais (proprietárias Mikrotik) nos pacotes Wireless a fim de contornar problemas de compatibilidade com versões antigas (antes da 2.9.25) com novos cartões Intel – Centrino.
- **pré-2.9.25**: Inclui extensões da forma aceita por versões mais antigas do RouterOS. Incompatível com clientes Centrino;

- **post-2.9.25**: Extensões aceitas a partir dessa versão e compatível com todos os clientes conhecidos até o momento.

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

Default Client Tx Rate: Estabelece a taxa máxima, em bps que cada cliente pode enviar ao AP – Só funciona para cliente, também, Mikrotik.

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

Yes: Como AP, deixa o cliente se associar, mesmo se não estive declarado na Access List. Como cliente, associa-se a qualquer AP, mesmo que não esteja na Connect List.

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

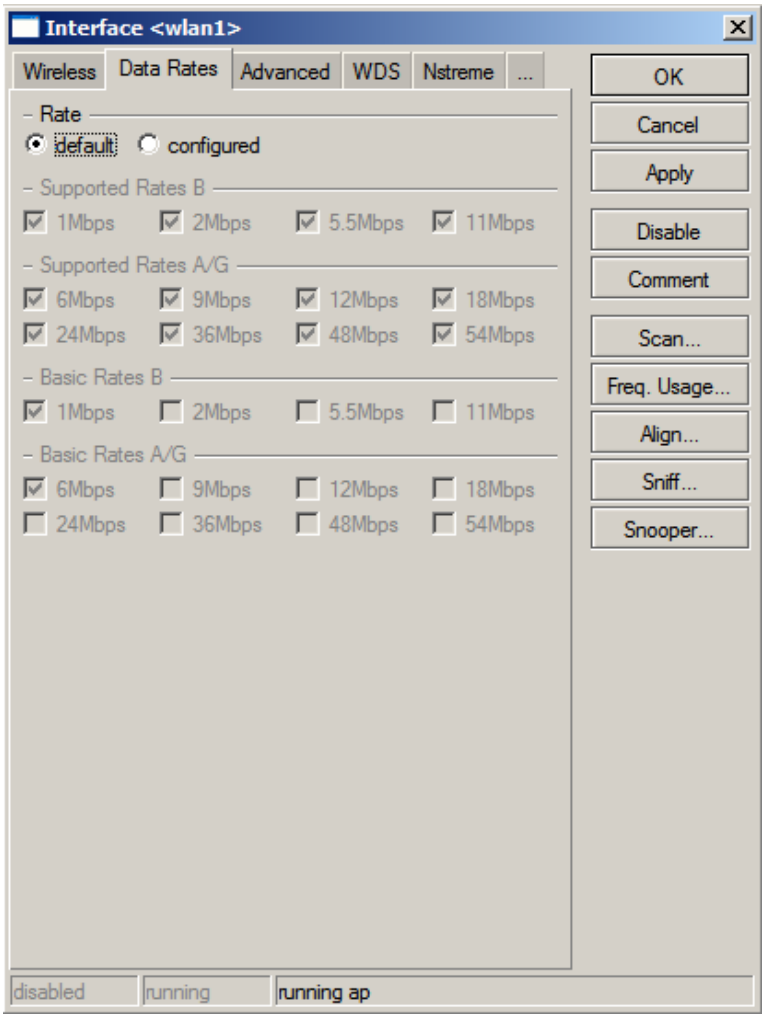
- **Yes** (marcado): permite a comunicação;
- **No** (desmarcado): Não permite a comunicação.

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

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

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

Guia – Data Rates



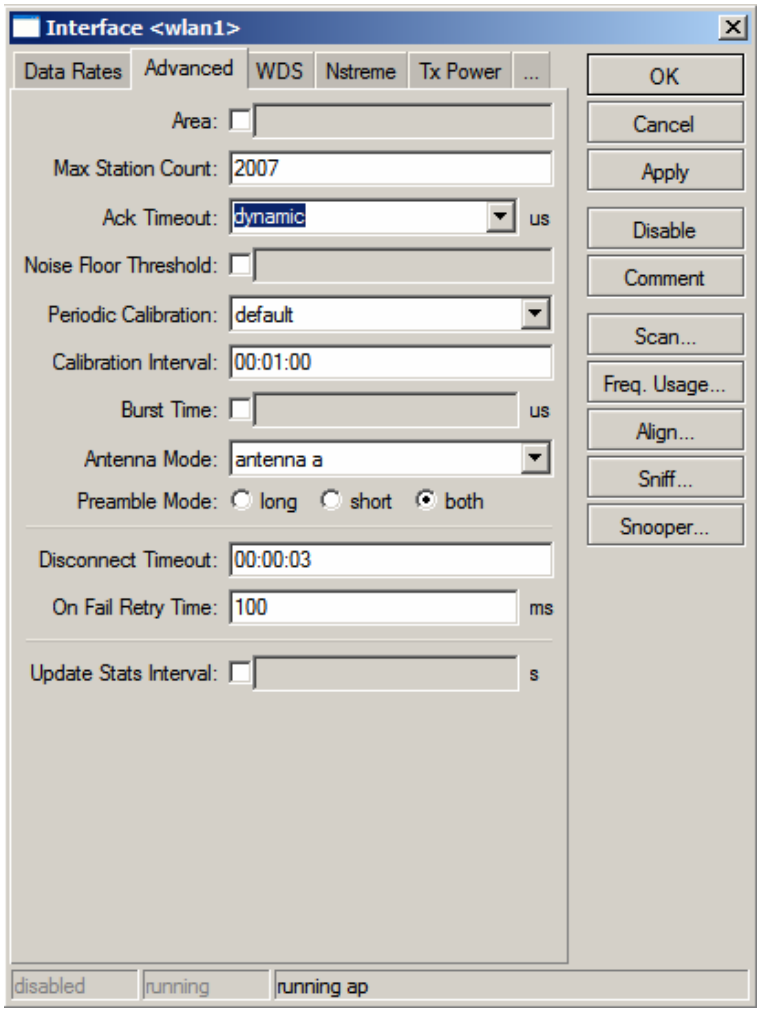
Nesta tela é possível configurar as Taxas de transmissão suportadas e as Taxas Básicas, sendo que:

- **Taxas Suportadas (Supported Rates)**: São todas as taxas que o cartão que está sendo configurado suporta.

- **Taxas Básicas (Basic Rates)**: São as taxas mínimas suportadas por todos os dispositivos Wireless presentes na rede

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

Guia – Advanced



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

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

Ack Timeout: Tempo de expiração (timeout) do pacote de confirmação de recebimento (acknowledgment) enviado por uma estação

- dynamic: ajuste dinâmico. O roteador manda pacotes variáveis e em função da resposta procura ajustar ao timeout ideal.
- indoors: para redes indoor.
- pode ser ajustado manualmente (valor inteiro em microssegundos) digitando-se diretamente na interface.

Valores sugeridos de Ack-Timeout

Range	Ack-timeout		
	5Ghz	5Ghz-turbo	2.4Ghz-G
0Km	default	default	default
5Km	52	30	62
10Km	85	48	96
15Km	121	67	133
20Km	160	89	174
25Km	203	111	219
30Km	249	137	268
35Km	298	168	320
40Km	350	190	375
45Km	405	-	-

Chipset version	5Ghz		5Ghz-turbo		2Ghz-b		2Ghz-g	
	Default	Max	Default	Max	Default	Max	Default	Max
5000 (5.2Ghz only)	30	204	22	102	n/a	n/a	n/a	n/a
5211 (801.11a/b)	30	409	22	204	109	409	n/a	n/a
5212 (802.11a/b/g)	25	409	22	204	30	409	52	409

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

Noise Floor Threshold: Piso de ruído do ambiente (em dBm).
Observação: Não localizamos documentação suficiente para esclarecer a utilidade prática desta opção. Em princípio deve trabalhar com cartões que tenham a opção de detecção de noise floor – noise-floor-control

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

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

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

Antena Mode: Permite a escolha da antena.
- antena a/b: escolhe uma das antenas a ou b
- tx-a/rx-b: usa a antena A para TX e a B para RX
- tx-b/rx-a: usa a antena B para TX e a A para RX

Preamble Mode: escolhe o modo do preâmbulo (comunicação inicial e de sincronização).
- long: padrão compatível com 802.11 em geral (mais antigo)
- short: padrão suportado por alguns cartões mais modernos; porem não compatível com 801.11. Utilizando short, há aumento (pequeno) de performance.
- both: ambos são suportados

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

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

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

Default = 3 segundos

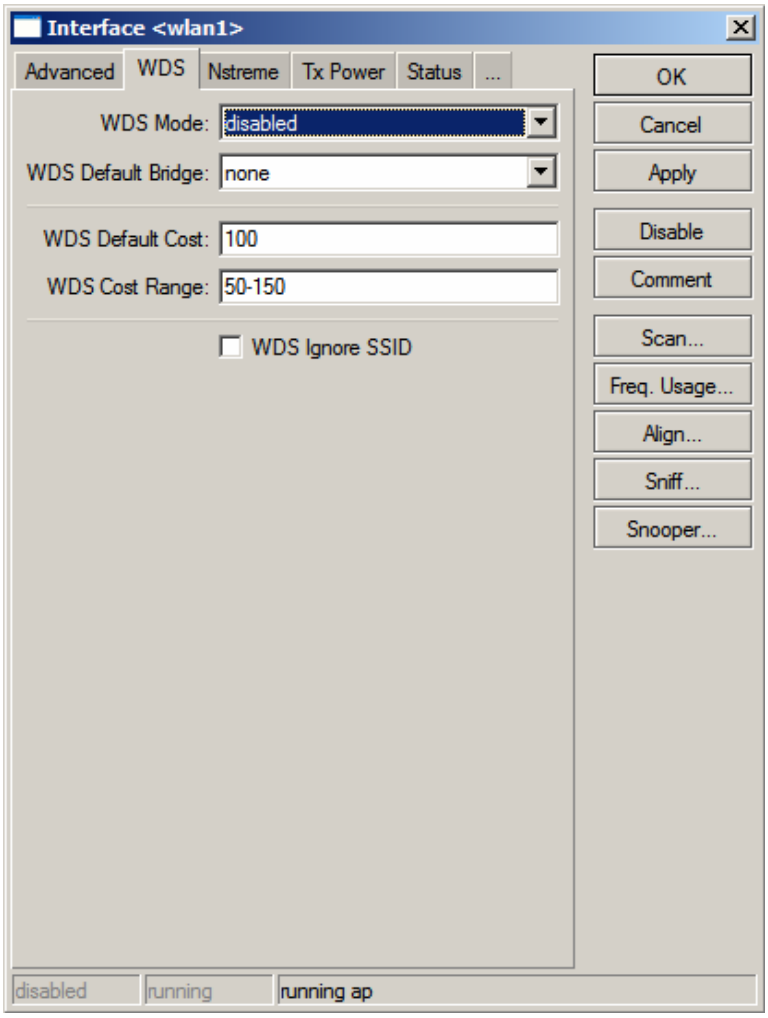
On Fail Retry Time: Intervalo de tempo após o qual é repetida a comunicação para um dispositivo wireless cuja comunicação tenha falhado.

Default: 100ms

Update Stats Interval: Periodicidade de atualização das estatísticas da interface.

Default = 10s

Guia – WDS



WDS Mode: Neste modo de operação todos os APs tem que estar configurados com o mesmo nome de rede e utilizando o mesmo canal. Além da comunicação entre APs, o WDS permite que se conectem em qualquer dos APs estações wireless

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

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

Tendo em vista que WDS pressupõe mesmo canal em todos os APs, fica incompatível o uso de DFS.

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

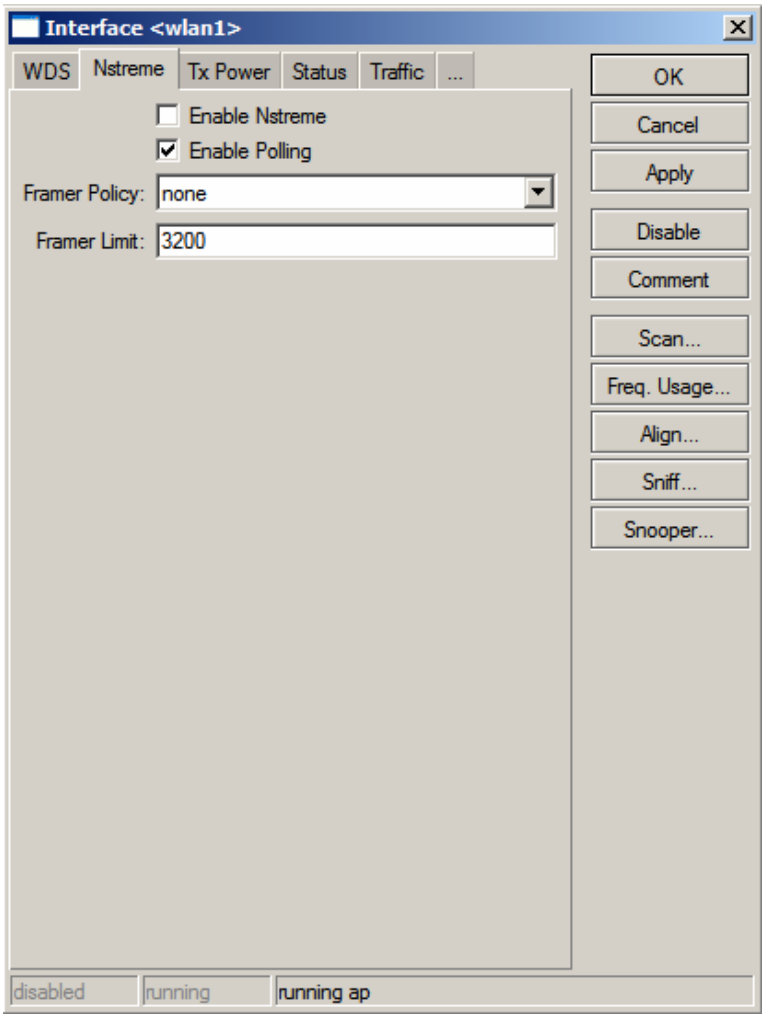
WDS Default Cost: No caso de redes malhadas (Mesh) feitas com WDS podem-se definir custos diferentes para diversos trajetos, dando preferências a determinadas rotas de forma manual.

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

WDS Ignore SSID: Uma vez habilitada essa opção, os APs irão criar links com qualquer outro AP que esteja configurado na mesma freqüência, independente do SSID configurado nas mesmas.

Default = No.

Guia – Nstreme



Nstreme é um protocolo proprietário Mikrotik (não 802.11) que tem por objetivo estabelecer links de desempenho melhorado quando comparado ao padrão Wi-fi Normal. Destinado principalmente a links ponto-a-ponto, mas podendo, também, ser utilizado em ambientes multiponto, desde que todos tenham nstreme habilitado (obviamente todos Mikrotik).

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

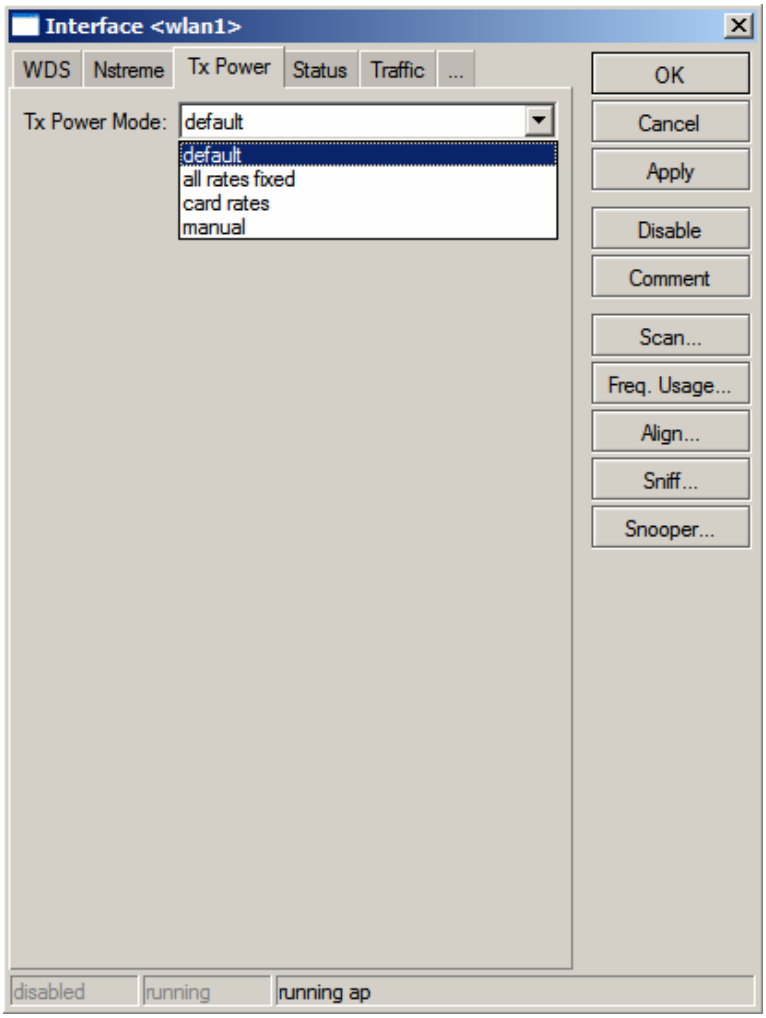
Framer Policy: Método utilizado para combinar pacotes em um quadro maior e com isso diminuir o overhead da comunicação, aumentando consequentemente a performance.

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

Framer Limit: Tamanho máximo do quadro.

Default = 3200 bytes

Guia – Tx Power



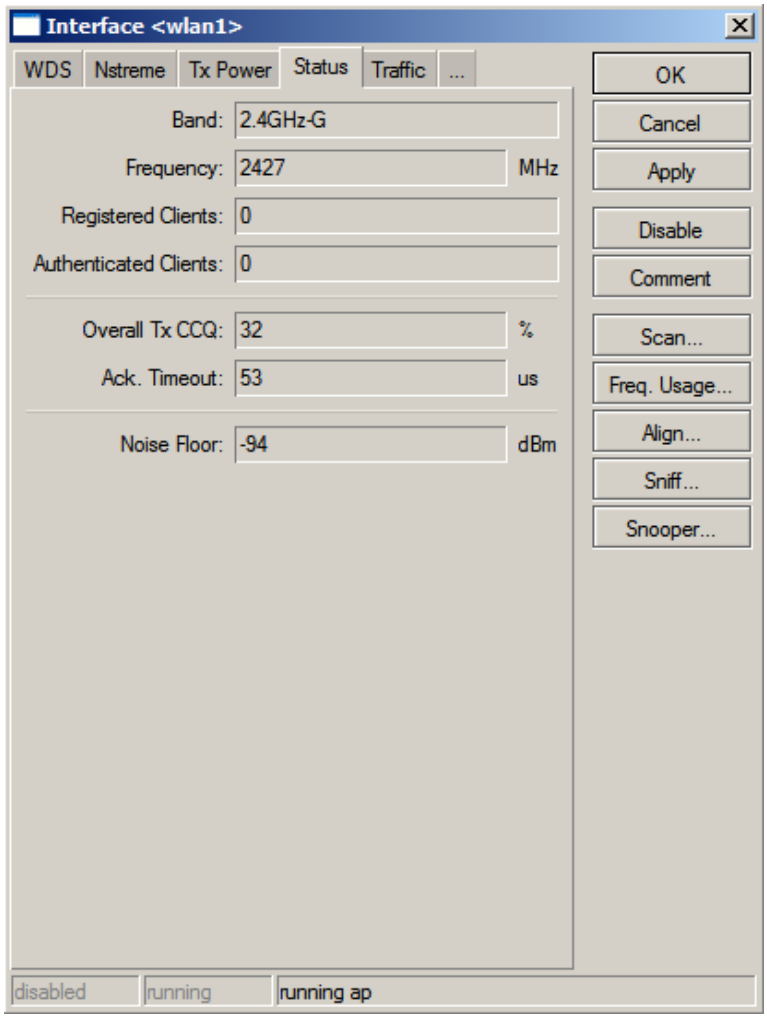
Tx Power Mode: Interface utilizada para configurar a potência de transmissão – valores de -30dBm a 30dBm

Default = 17dBm

- All-rates-fixed: utiliza a mesma potência configurada em Tx Power para todas as velocidades.
- Card-rates: utiliza as velocidades próprias dos firmwares dos cartões
- Default: utiliza a potência default (17dBm)
- Manual-table: permite a configuração de diversas potências em função da taxa de transmissão.

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

Guia – Status



Mostra informações sobre o status do AP

- **Band**: Freqüência e modo de operação

- **Freqüência**: Canal utilizado

- **Registered Clients**: Clientes registrados

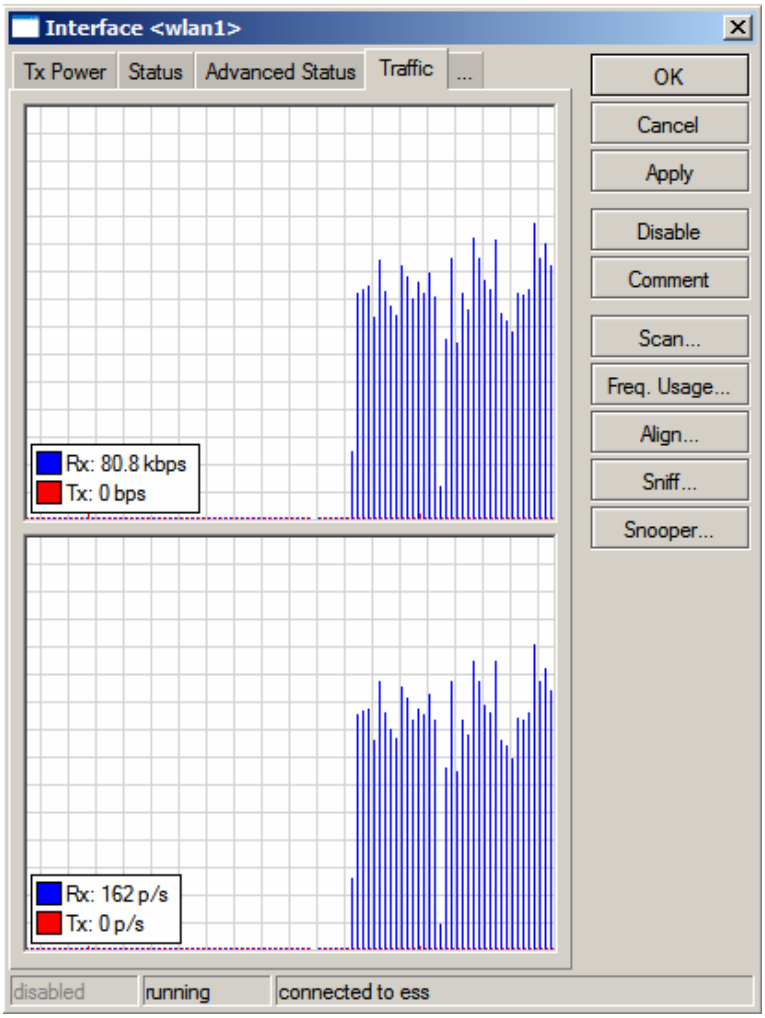
- **Authenticated Clients**: Clientes autenticados

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

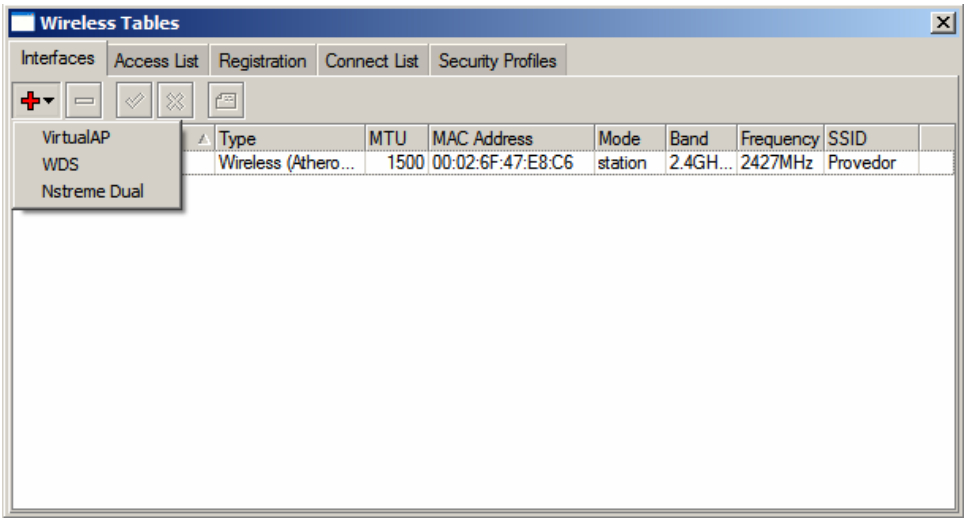
- **Ack Timeout**: Tempo de expiração do ACK em microssegundos.

- **Noise Floor**: Piso de ruído em dBm.

Guia – Traffic



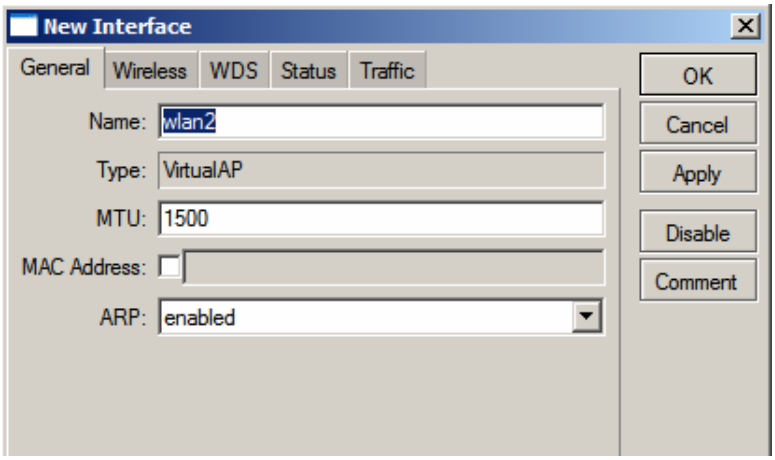
Menu Wireless – Interfaces



Ao clicar em adicionar interfaces, são dadas as opções:

- **VirtualAP**: Cria interfaces virtuais (APs com nomes diferentes) na mesma interface física. Os parâmetros de freqüência, modo de operação, canal, etc., serão herdados do AP principal.

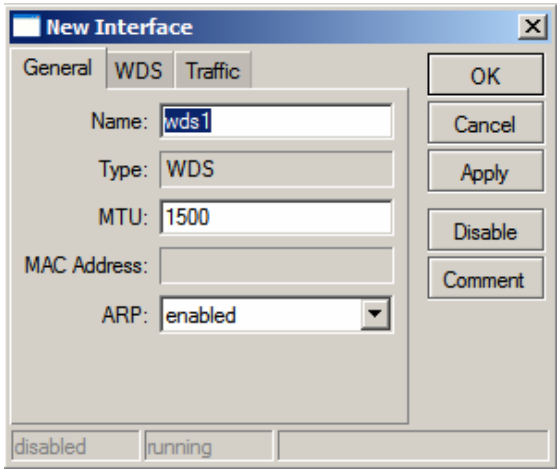
Criando interfaces virtuais, podemos montar várias redes dando perfis de serviços diferentes.

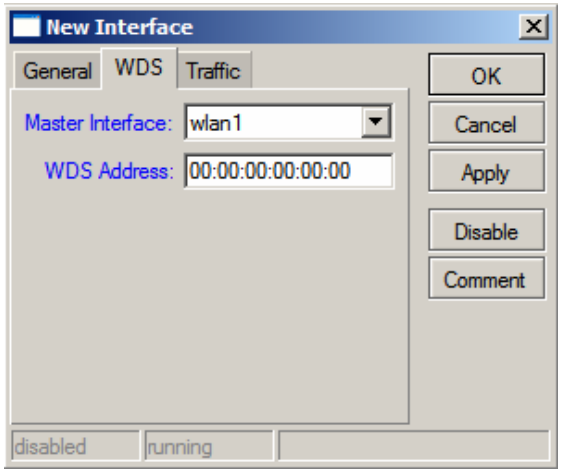


- Name: Nome da rede virtual
- MTU: Unidade de transferência máxima (bytes)
- MAC Address: Dê o MAC que quiser para o novo AP
- ARP
  - Enable/Disable: Habilita/Desabilita
  - Proxy-arp: passa seu MAC
  - Reply-only

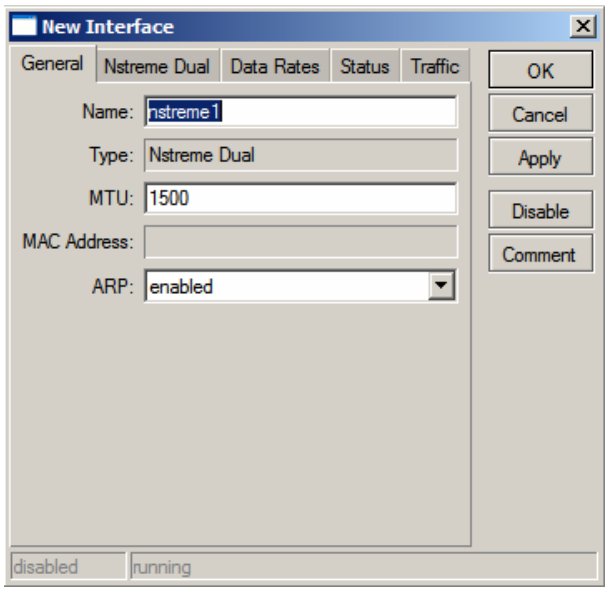
Observação: Demais configurações idênticas de uma AP

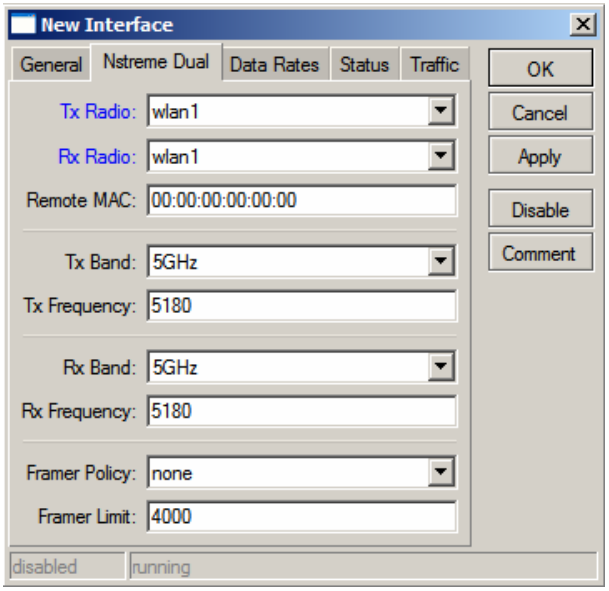
- **WDS**: Cria uma interface WDS dando os parâmetros:
    - Name: Nome da rede WDS
    - Master Interface: Interface sobre a qual funcionará o WDS, podendo esta inclusive ser uma interface virtual
    - WDS Address: endereço MAC que a interface terá.





- **Nstreme Dual**: Cria uma interface para uso como Nstreme dual utilizando duas antenas (uma antena para Tx (Transmissão) e outra para Rx (Recepção)).

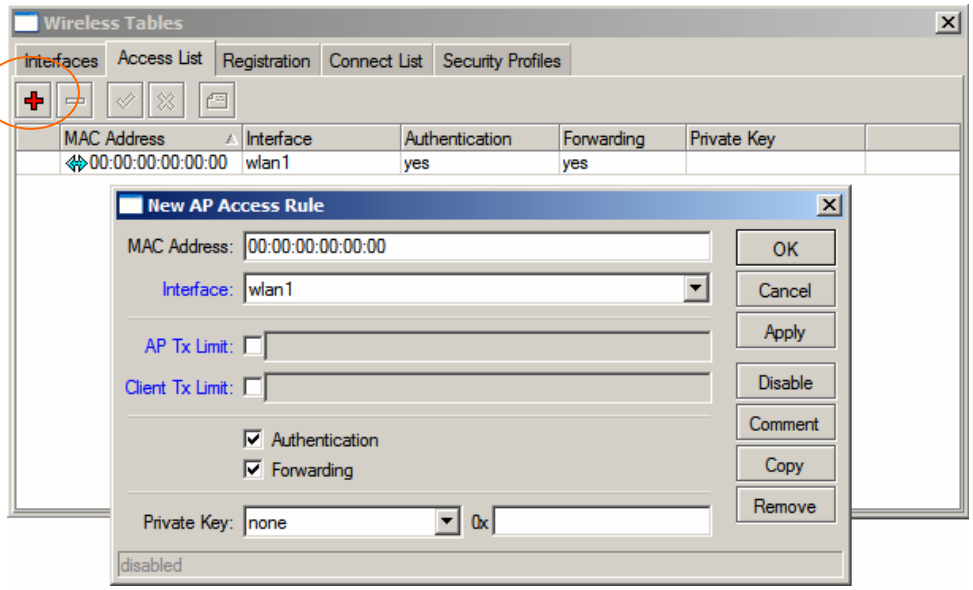




- Tx Rádio: especifica-se as interfaces de Tx.
- Rx Rádio: especifica-se as interfaces de Rx.
- Tx/Rx Band e Frequency: Especifica-se a Banda de Tx e Rx que podem inclusive ser de frquencias diferentes (2.4Ghz para Tx e 5.8Ghz para Rx)
- Framer Policy:
    - Best-fit: pacotes são agrupados em frames, sem fragmentação
    - exact-size: pacotes são agrupados em frames, com fragmentação se necessário.

Observação: Com Nstreme dual é possível escolher as velocidades de transmissão e recepção e ainda monitorar o status das conexões.

Menu Wireless – Access List

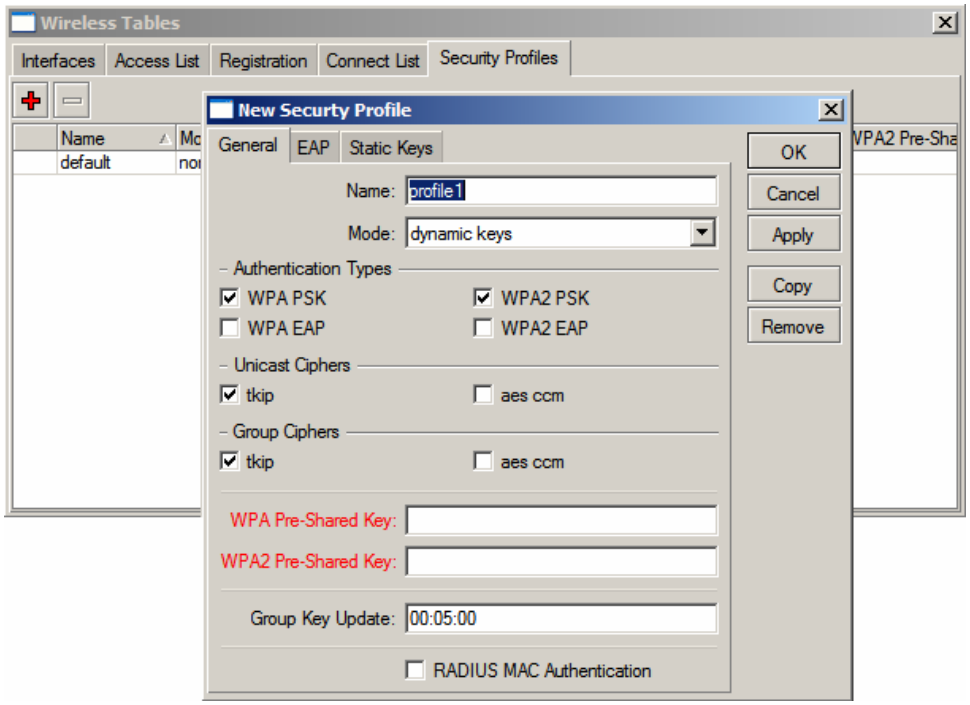


O Access List é utilizado pelo Access Point para restringir associações de clientes. Esta lista contém os endereços MAC de clientes e determina qual a ação deve ser tomada quando um cliente tenta conectar. A comunicação entre clientes da mesma interface, virtual ou real, também é controlada nos Access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

- Um cliente tenta se associar a uma interface WlanX
- Seu MAC é procurado no Access List da interface WlanX
- Caso encontrada a ação especificada será tomada:
    - Authentication marcado: deixa o cliente se autenticar
    - Forwarding marcado, o cliente se comunica com outros

- **MAC Address**: MAC a ser liberado
- **Interface**: Interface Real ou Virtual onde será feito o controle
- **AP Tx Limit**: Limite de tráfego do AP para o Cliente
- **Client Tx Limit**: Limite de tráfego do Cliente para o AP (apenas se cliente Mikrotik)
- **Authentication**: Habilitado, autentica os MACs declarados.
- **Forwarding**: Habilitado, permite a comunicação entre clientes habilitados (intra bss)
- **Private Key**: Chave de criptografia
    - 40bit wep
    - 128 bit wep
    - Aes-com

Menu Wireless – Security Profiles

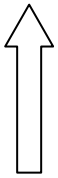


Na tabela Security Profiles são definidos os perfis de segurança da parte Wireless que poder ser utilizados no RouterOS.

- **Name**: Nome que aparecerá em outras telas, referenciando esse perfil.
- **Mode**: Modo de operação
  - dynamic keys: gera chaves dinâmicas
  - static-keys-required: criptografia todos os pacotes e somente aceita pacotes criptografados.
  - static-keys-optional: se existe uma chave privada estática de estação (static-sta-private-key), esta será utilizada. Caso contrário, estando a estação no modo AP, não será utilizada criptografia e em modo estação usará se estiver setada a static-transmit-key.
- **Authentication Types**

Evolução dos padrões de Segurança wireless

+ SEGURANÇA



- WPA2 (802.11i) com EAP
- WPA2 (802.11i) com PSK
- WPA com AES ccm
- WPA com MD5
- WEP com TKIP
- WEP 128 bits

- WPA: Métido não padrão IEEE utilizado surante algum tempo pela indústria para evitar problemas do WEP
- WPA2: Método compatível com 802.11i do IEEE
- PSK (Pré Shared Key): chave compartilhada entre dois dispositivos.
- EAP: Extensive Authentication Protocol

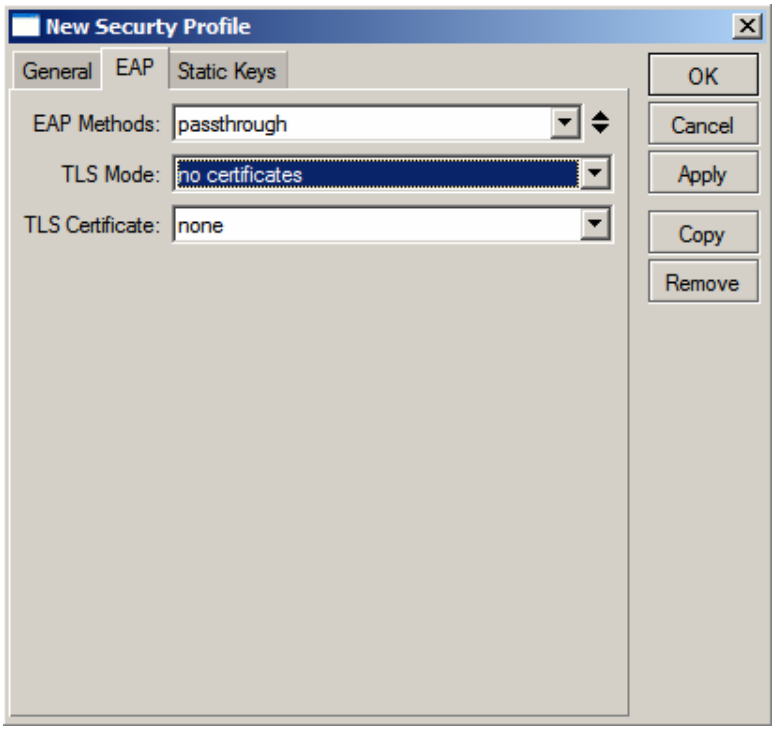
Observação: O AP irá divulgar todos os modos de autenticação marcados aqui e as estações escolherão o método considerando mais seguro.
Exemplo: WPA EAP ao invés de WPA PSK

- **Unicast Chipers**

- TKIP: Protocolo de integridade de chave Temporal. Método utilizado durante algum tempo para contornar problemas da WEP (Proxim implementa como WEP Plus).
- AES CCM: Método de criptografia WPA mais seguro, que utiliza algoritimo AES.
- PSK (Pré Shared Key): chave compartilhada entre dois dispositivos.
- EAP: Extensive Authentication Protocol

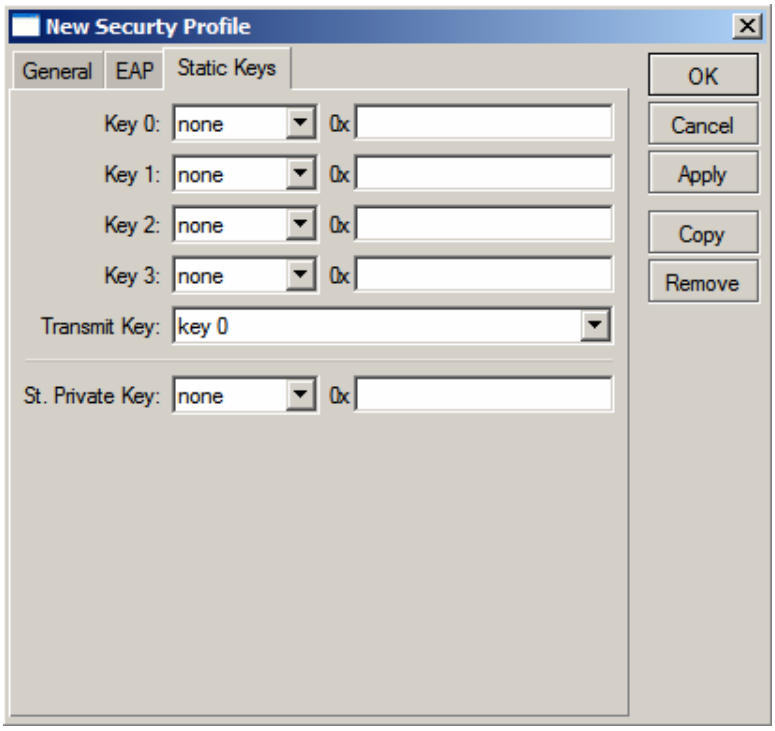
Observação: O AP irá divulgar todos os modos de autenticação marcados aqui e as estações escolherão o método considerando mais seguro.
Exemplo: WPA EAP ao invés de WPA PSK

- **Métodos EAP**



- Passtrough: Repassa o pedido de autenticação para um Servidor Radius (esta opção somente é usada em APs)
- EAP/TLS: Utiliza um Certificado TLS (Transport Layer Certificate)
- TLS Mode:
  - No-certificate: Certificados são negociados dinamicamente utilizando o algoritmo de Deffie-Helmman.
  - Don't-verify-certificate: exige o certificado, porém não o confere com uma entidade certificadora.
  - Verify-certificate: exige e verifica o certificado.
- TLS Certificate: Habilita um certificado importado em /Certificates

- **Static Keys**: Utilizado em caso de WEP



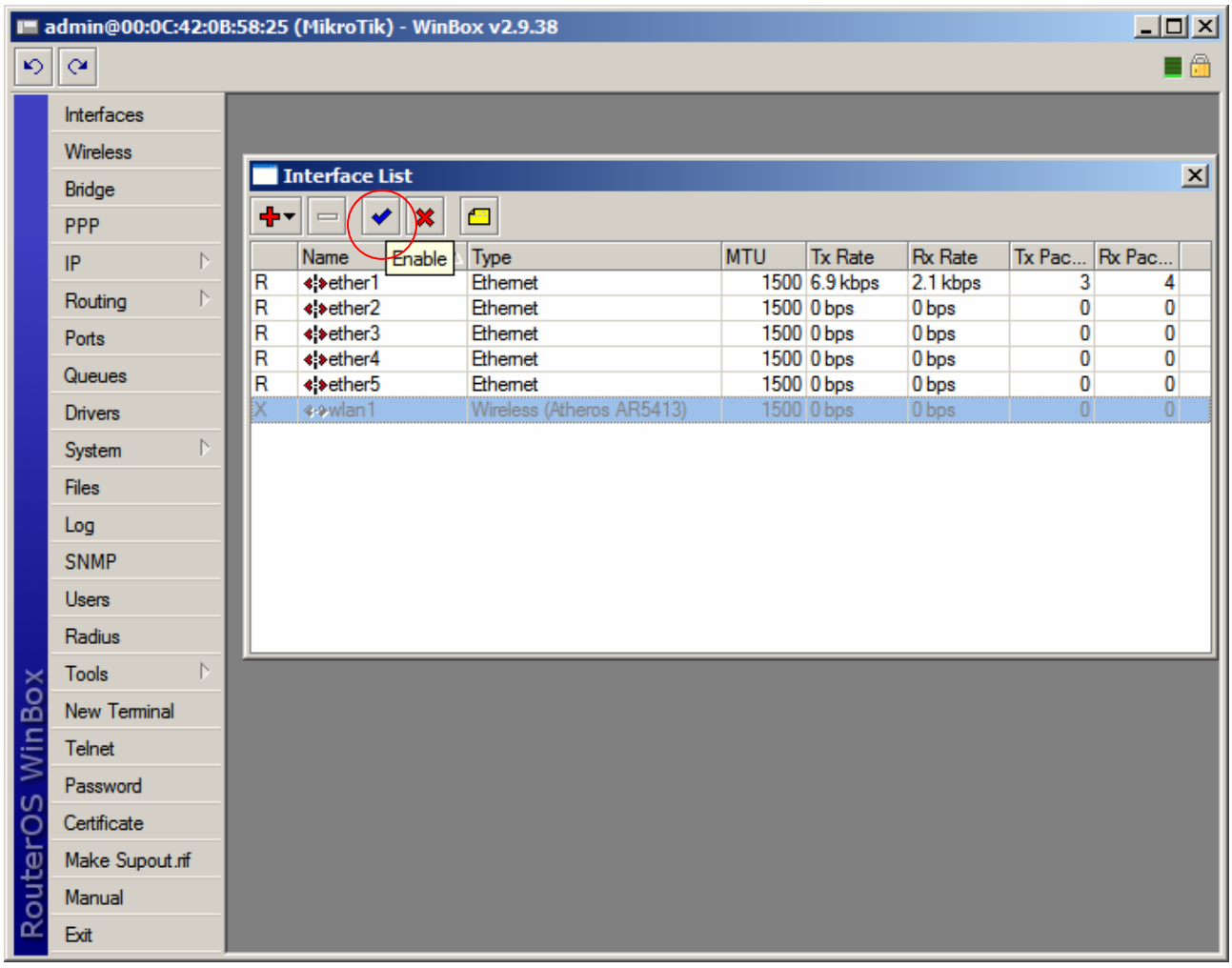
AP-BRIDGE

Bridge ou ponte, é um dispositivo que liga duas redes que usam protocolos distintos, ou dois segmentos da mesma rede que usam o mesmo protocolo, por exemplo ethernet ou token ring.

Uma bridge ignora os protocolos utilizados nos dois segmentos que liga, já que opera a um nível muito baixo do modelo OSI (nível 2); somente envia dados de acordo com o endereço do pacote. Este endereço não é o endereço IP (internet protocol) mas o MAC (media access control) que é único para cada placa de rede. Os únicos dados que são permitidos atravessar uma bridge são dados destinados a endereços válidos no outro lado da ponte. Desta forma é possível utilizar uma bridge para manter um segmento da rede livre dos dados que pertencem a um outro segmento.

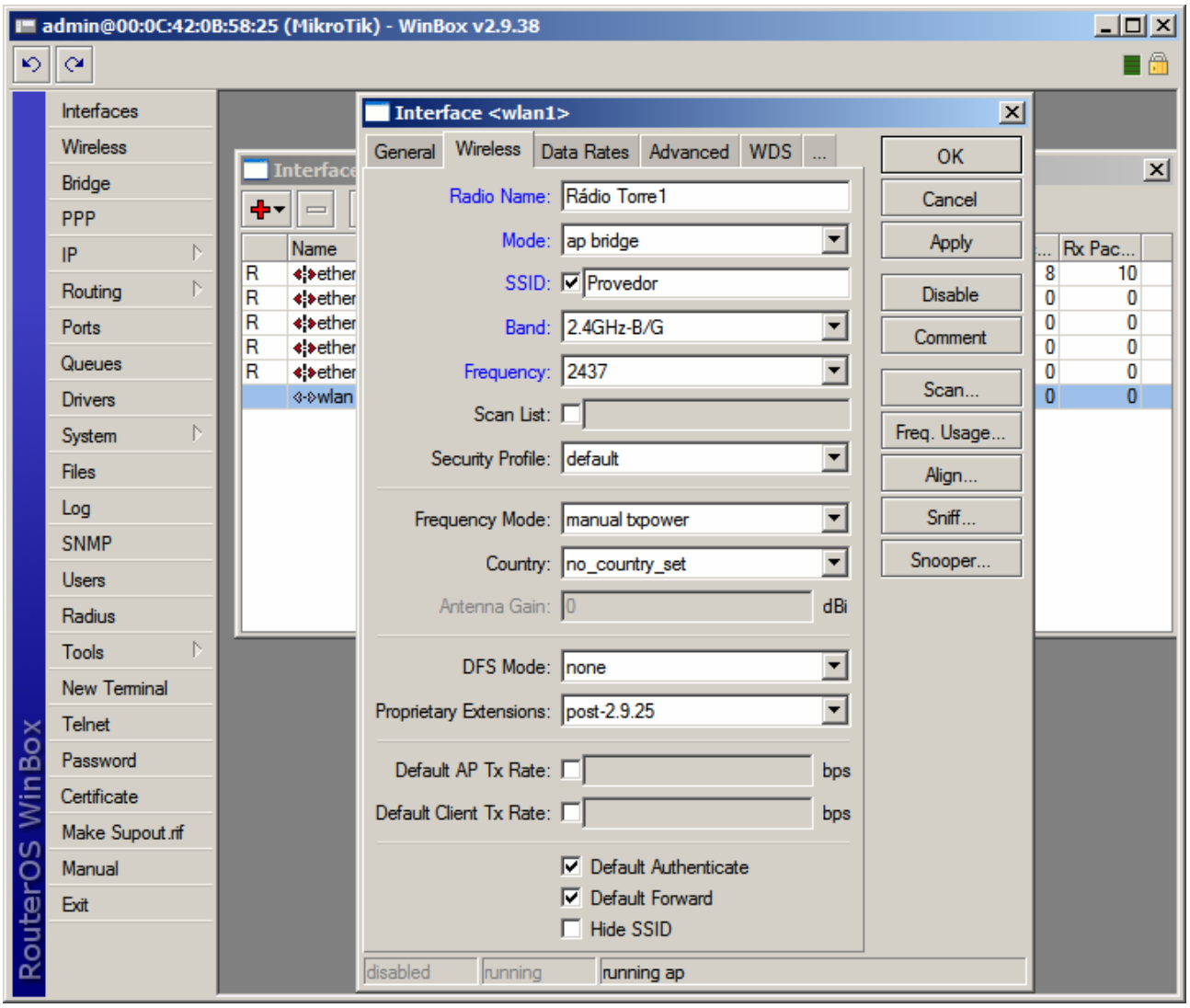
Configurando AP-Bridge no Mikrotik:

- Clique no menu Interfaces.
- Clique na interface Wlan desejada e clique no botão Habilitar



- Dê um clique duplo na interface habilitada
- Na guia Wireless, configure as opções:

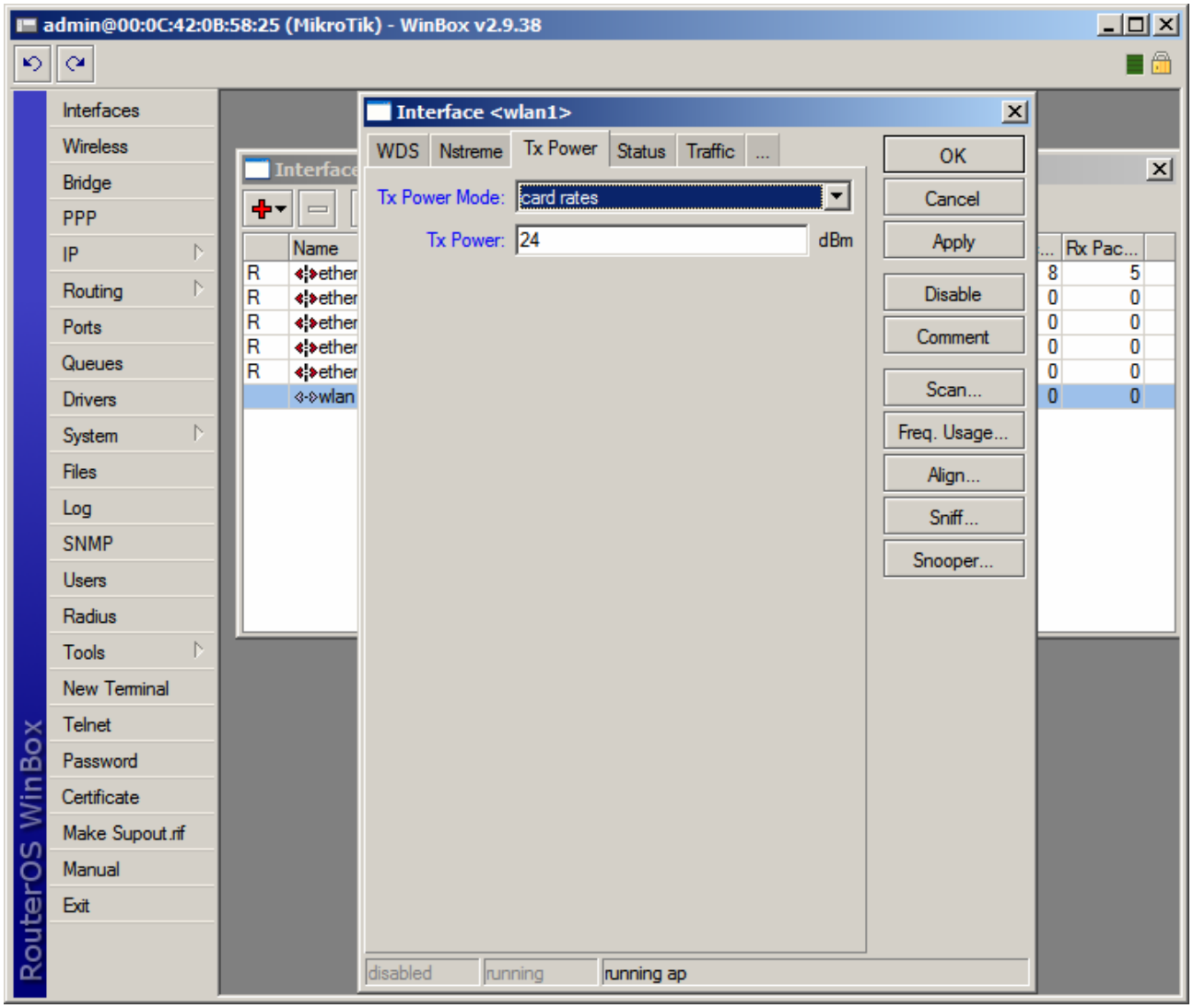
- Opção Radio Name: Coloque nessa opção o nome que você deseja que o Rádio tenha na rede.
- Opção Mode: AP Bridge
- Opção Band: Escolha a Banda de Operação desejada
- Opção Frequency: Canal de operação do equipamento
- Clique no botão “OK”



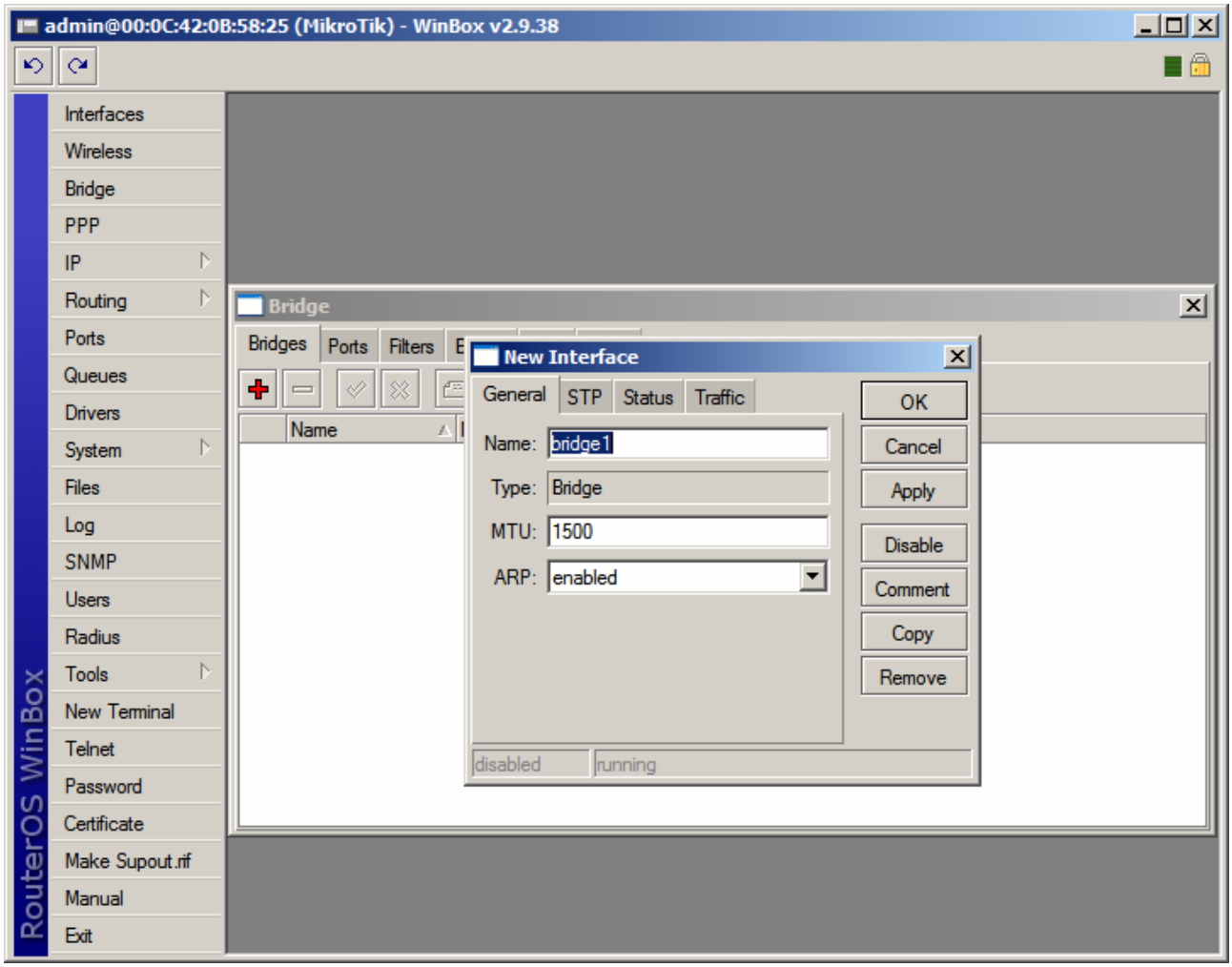
- Clique na guia “Tx Power” para escolher a potência do cartão, considerando:

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

Obs: Verifique a potência máxima permitida para o cartão utilizado antes de fazer a alteração.

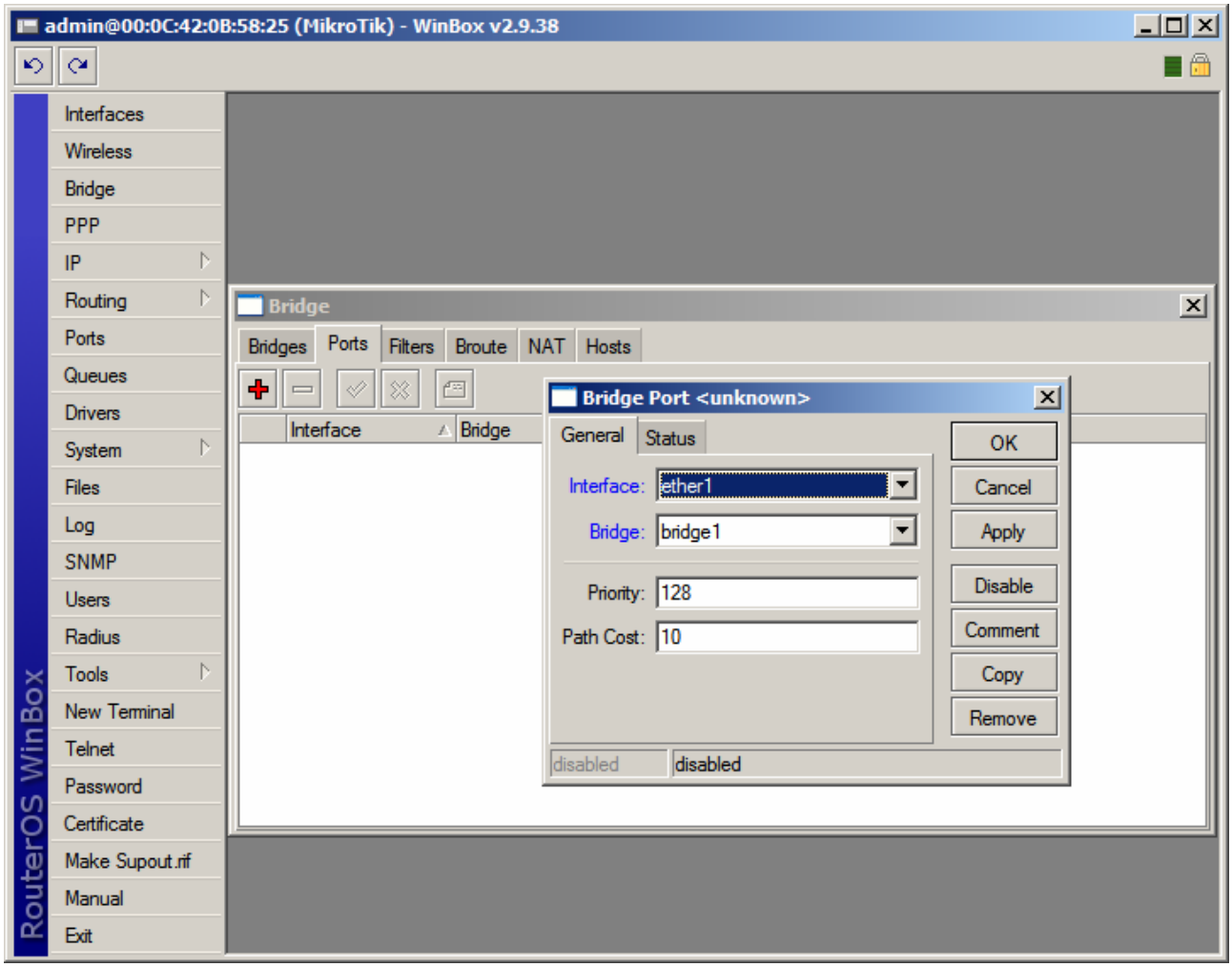


- Clique no Menu “Bridge”
- Clique em “Adicionar”
- Na guia General, na opção Name, digite um nome para a sua nova interface bridge. Em nosso exemplo, manteremos o nome default: bridge1



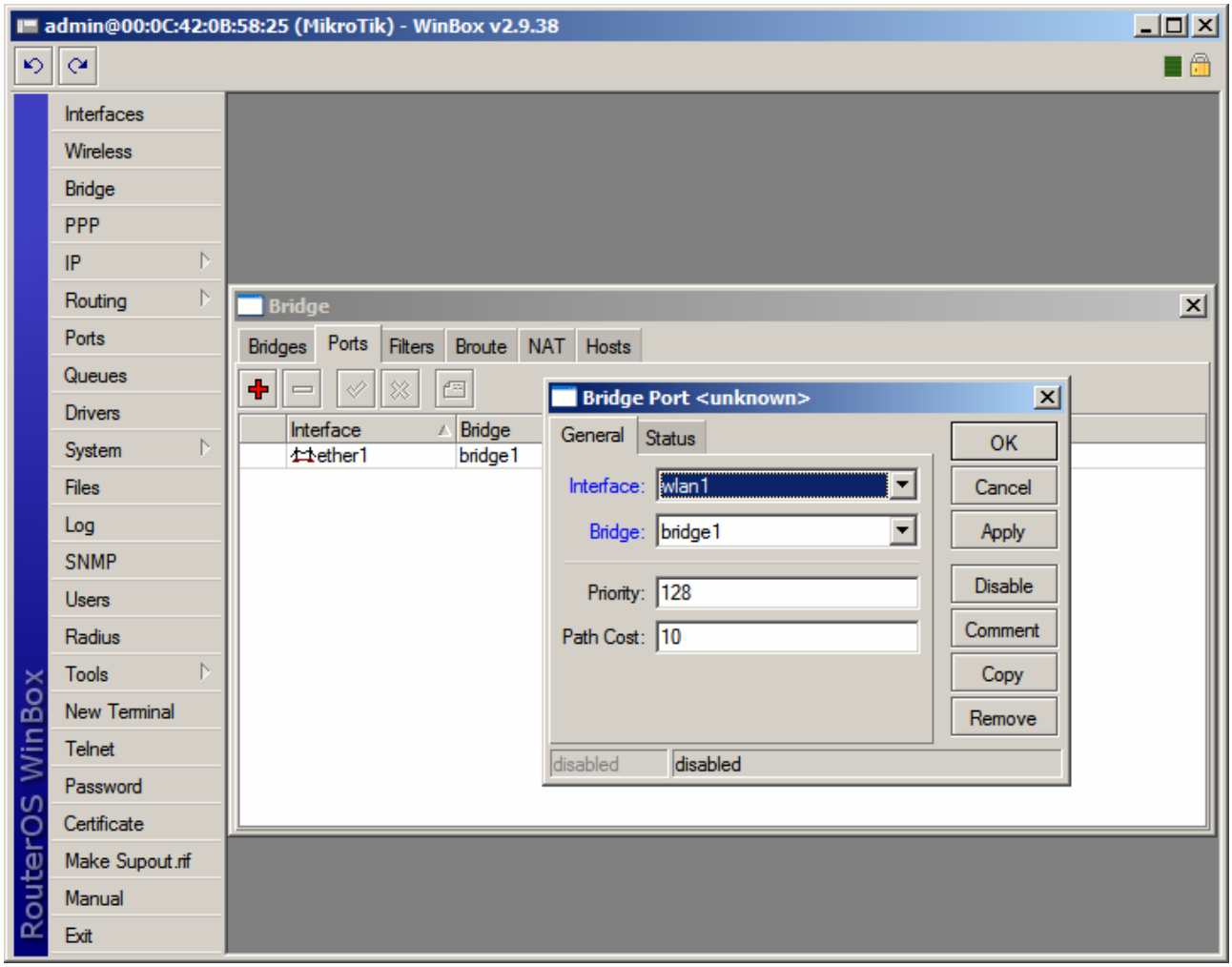
- Clique no botão “OK”

- Clique na guia Ports
- Clique em Adicionar
- Na opção Interface, selecione a opção “ether1”
- Na opção Bridge, deixe como “bridge1”



- Clique no botão OK

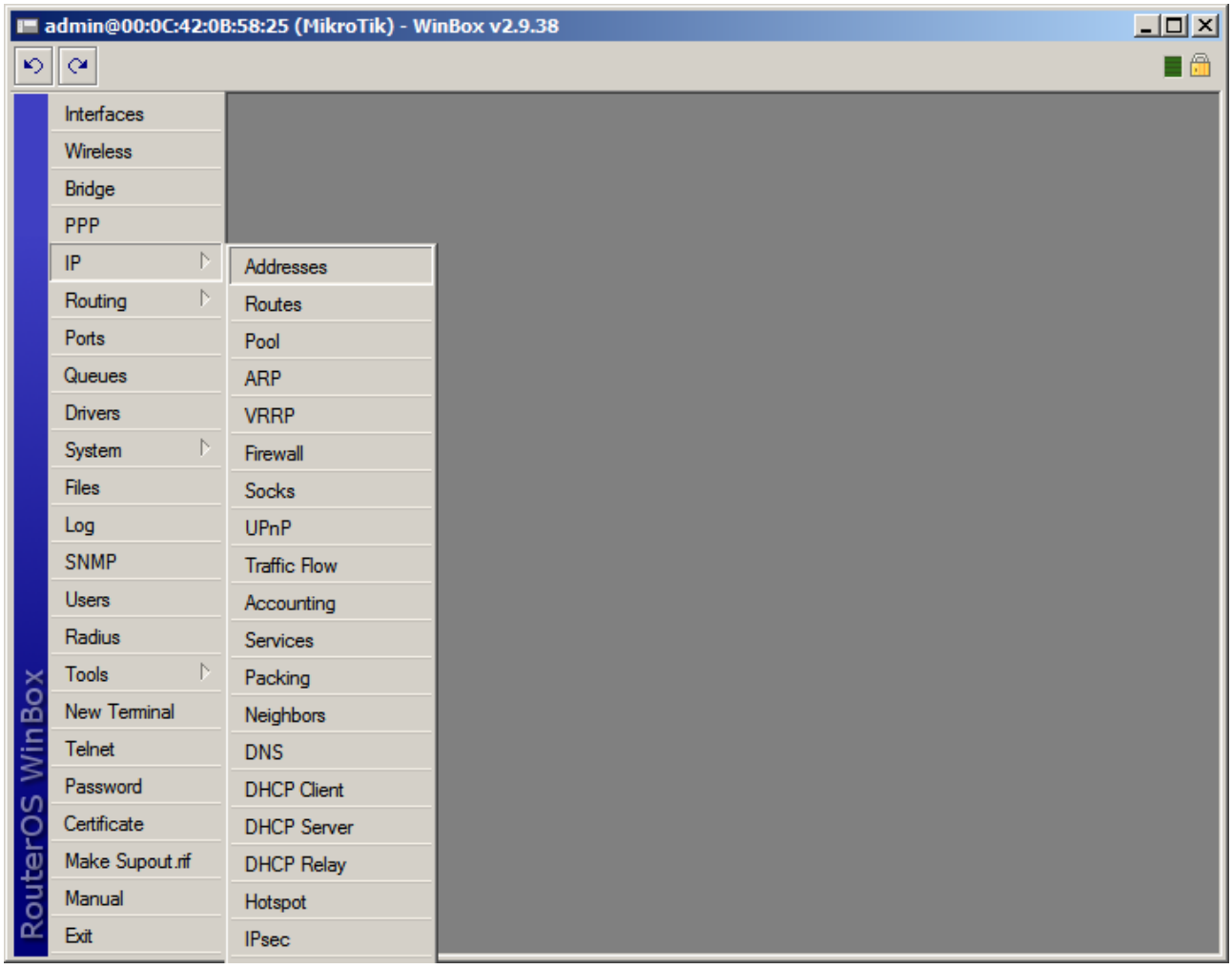
- Clique na guia Ports, novamente
- Clique em Adicionar nova entrada
- Na opção Interface, selecione a opção “wlan1”
- Na opção Bridge, deixe como “bridge1”



- Clique no botão OK

Atribuir um IP a interface Bridge

- Clique no menu “IP”
- Clique na opção “Addresses”

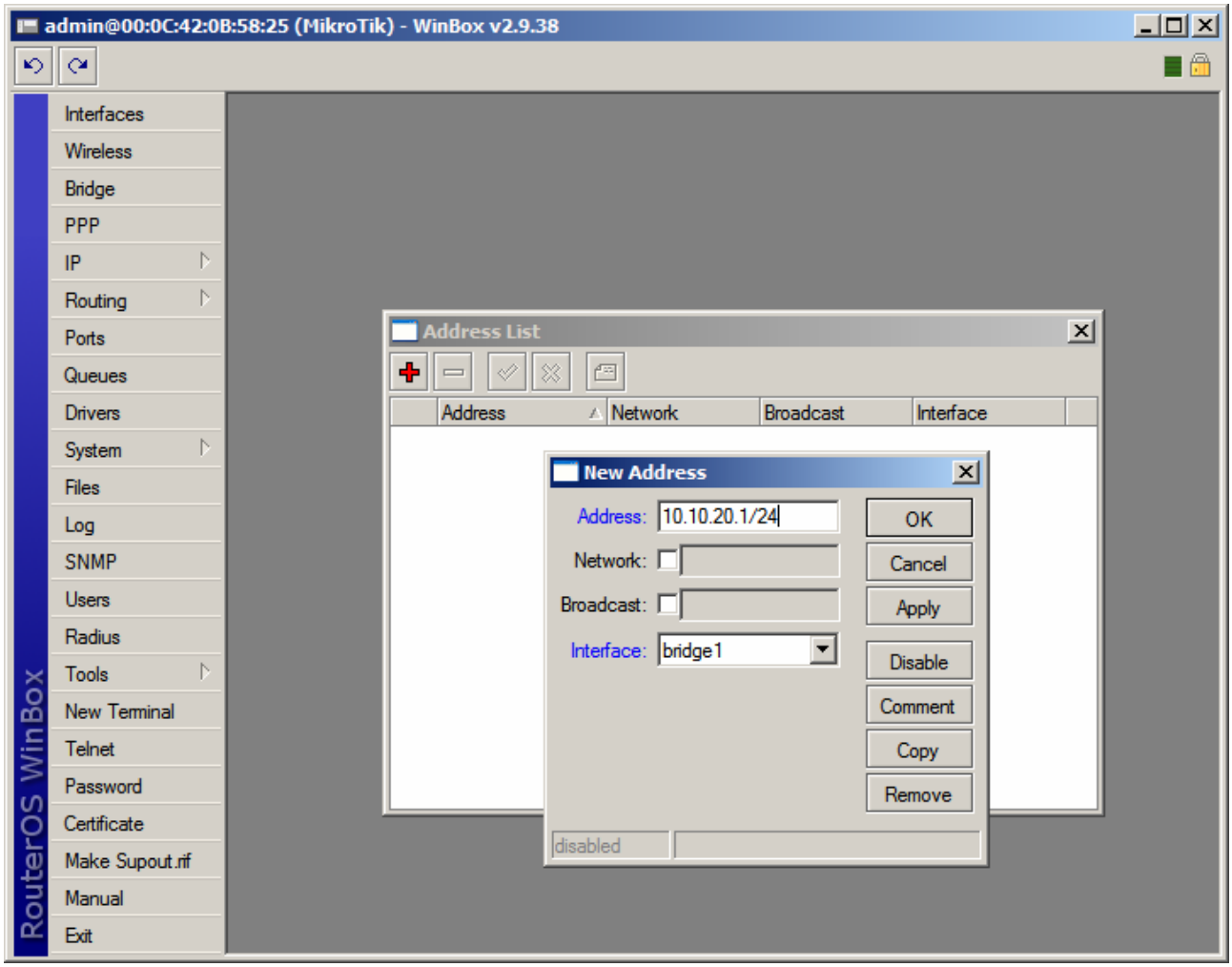


- Clique no botão “Adicionar”
- Coloque o IP que você deseja com os bits correspondentes (veja tabela na última imagem)

Ex.: 192.168.0.1/24 (255 IPs)
192.168.0.1/29 (6 IPs)

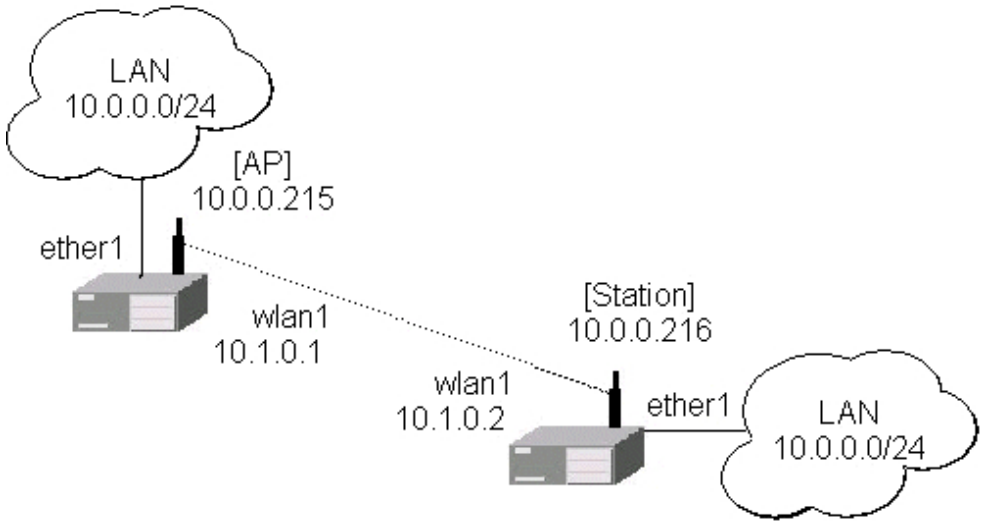
Decimal	Bits	Common Use
255.255.255.252	30	2 Host Subnet
255.255.255.248	29	6 Host Subnet
255.255.255.240	28	14 Host Subnet
255.255.255.224	27	30 Host Subnet
255.255.255.192	26	32 Host Subnet
255.255.255.128	25	126 Host Subnet
255.255.255.0	24	254 Host Net/Subnet
255.255.254.0	23	510 Host Subnet
255.255.252.0	22	1.022 Host Subnet
255.255.248.0	21	2.046 Host Subnet
255.255.240.0	20	4.094 Host Subnet
255.255.224.0	19	8.190 Host Subnet
255.255.192.0	18	16.382 Host Subnet
255.255.128.0	17	32.766 Host Subnet
255.255.0.0	16	65.534 Host Net/Subnet
255.254.0.0	15	131.070 Host Subnet
255.252.0.0	14	262.142 Host Subnet
255.248.0.0	13	524.286 Host Subnet
255.240.0.0	12	1.048.574 Host Subnet
255.224.0.0	11	2.097.150 Host Subnet
255.192.0.0	10	4.194.302 Host Subnet
255.128.0.0	9	8.388.606 Host Subnet
255.0.0.0	8	16.777.214 Host Subnet

- Em Interface, escolha a bridge criada anteriormente.



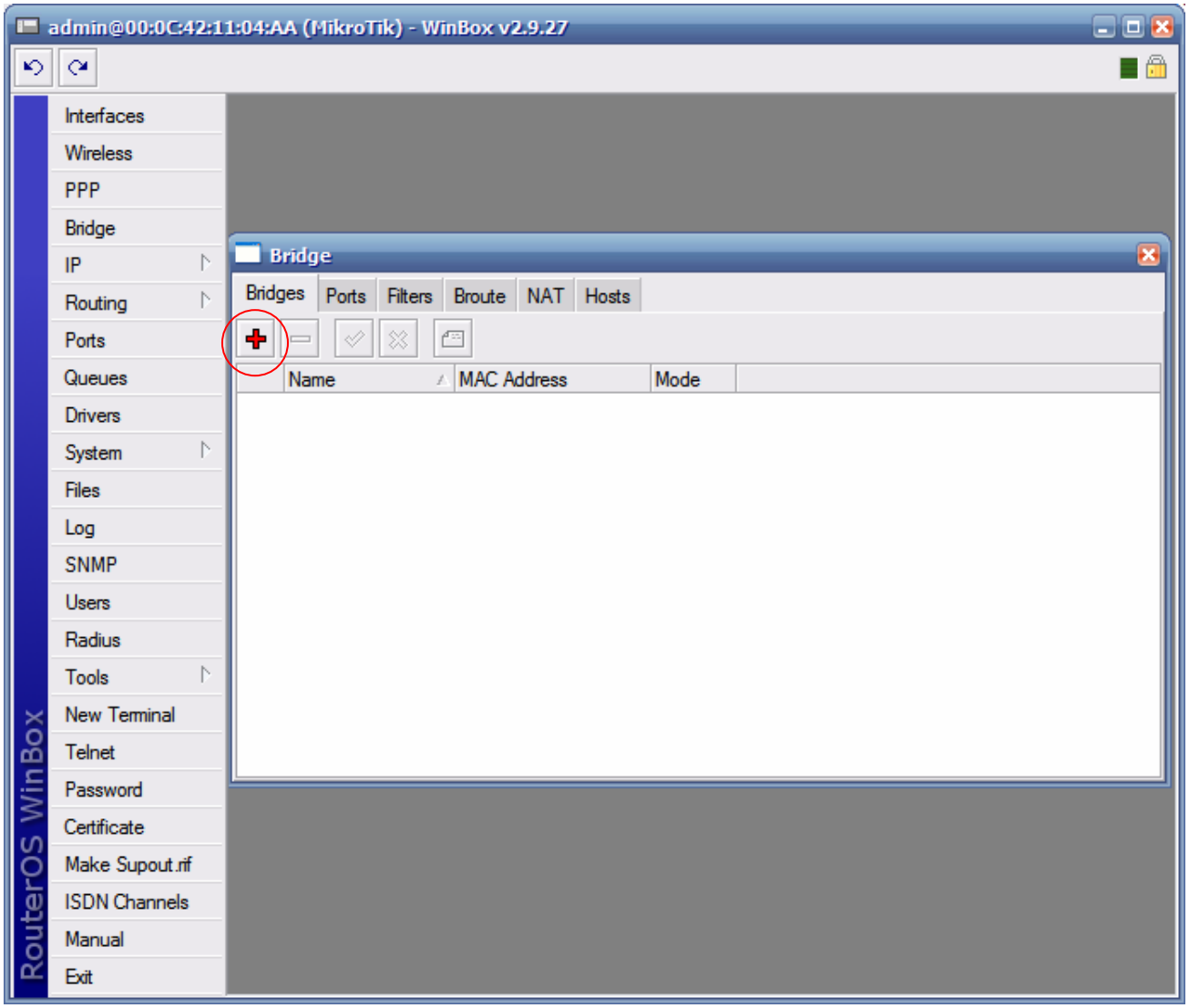
- Clique no botão OK

BRIDGE TRANSPARENTE ENTRE DOIS PONTOS UTILIZANDO WDS

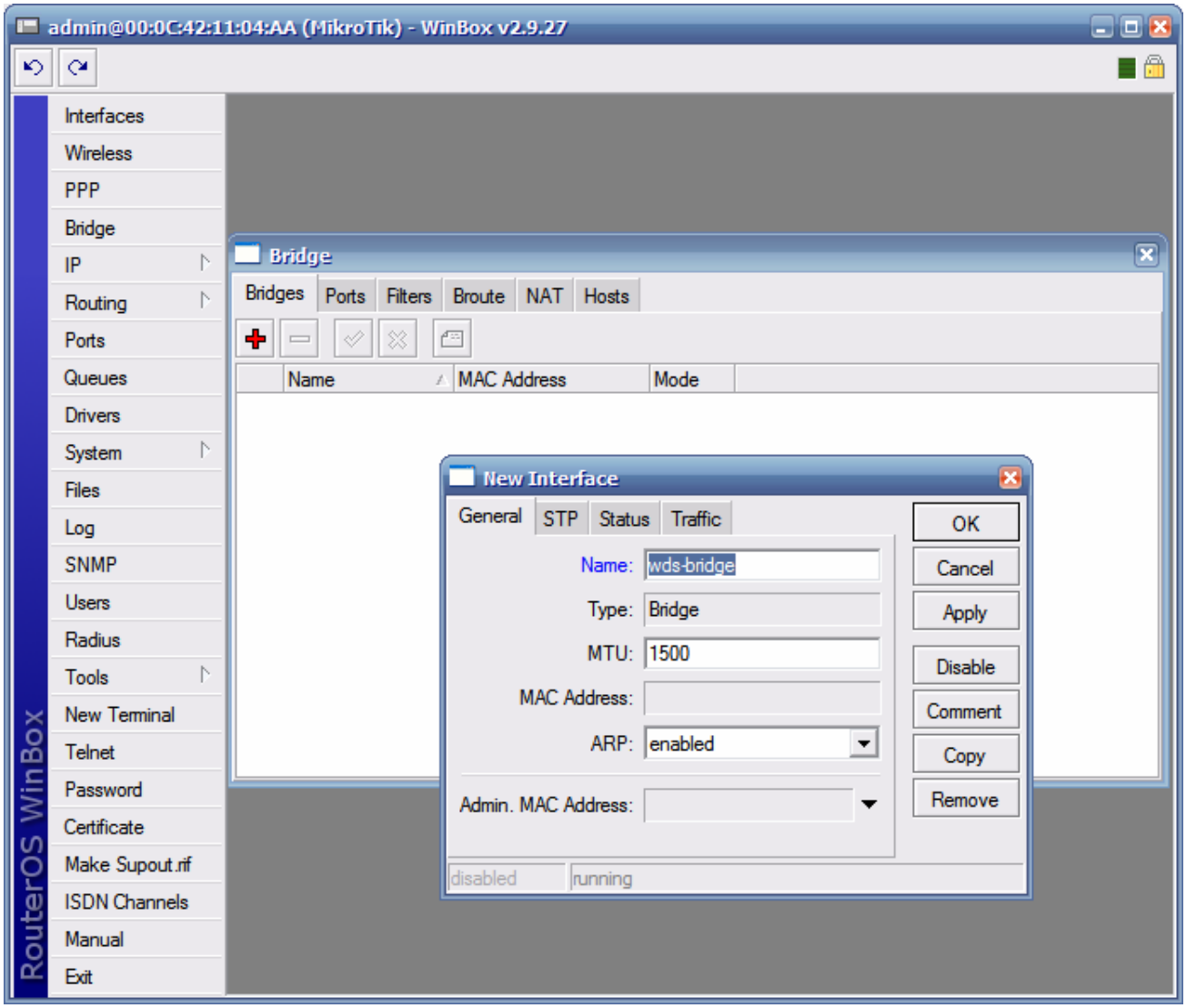


RÁDIO 1

Crie uma interface bridge
Clique no menu Bridge
Clique em adicionar para que uma nova interface bridge seja criada.



No campo Name, digite o nome da interface bridge (exemplo: wds-bridge)

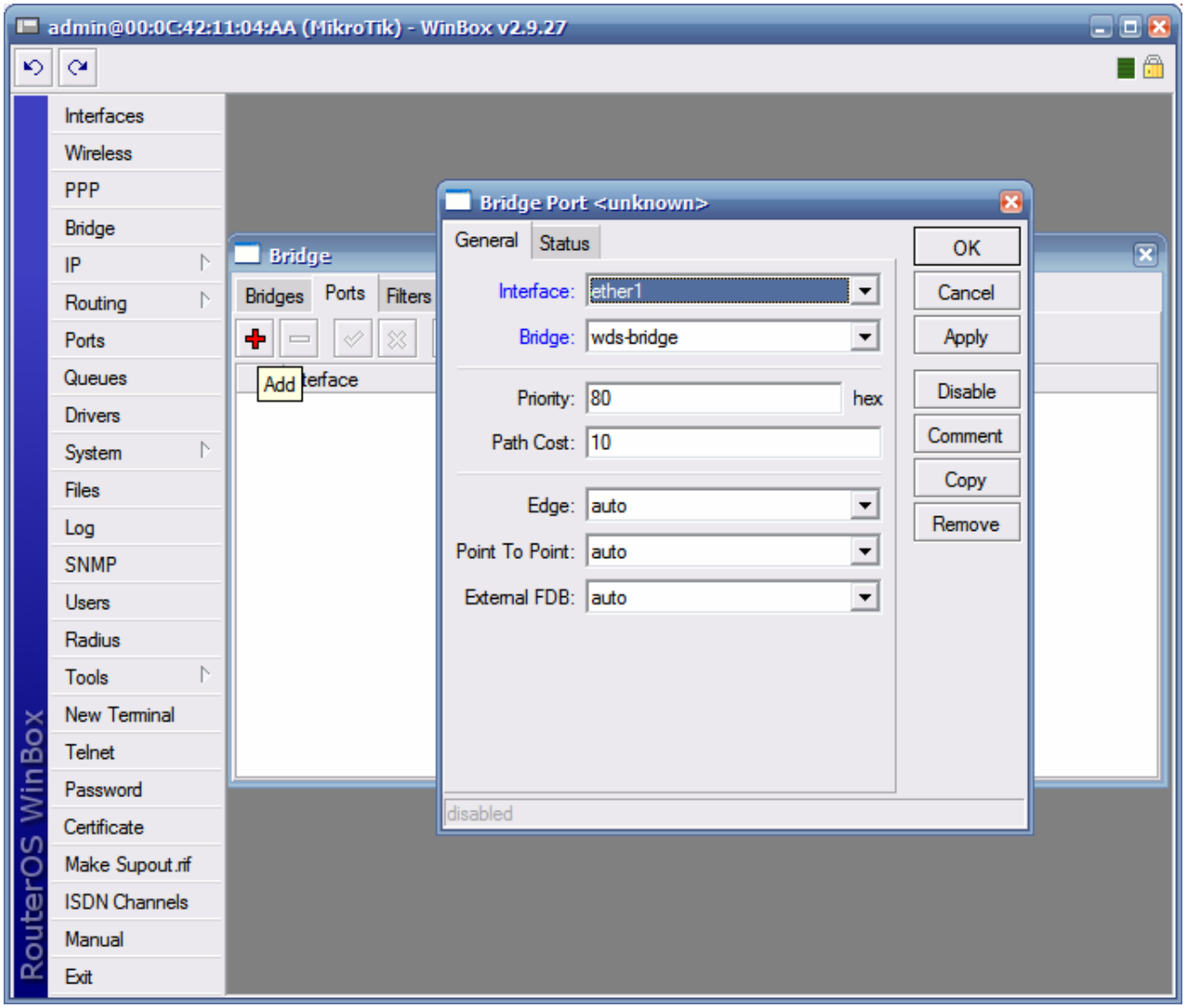


Clique no botão OK

- Clique na guia Ports

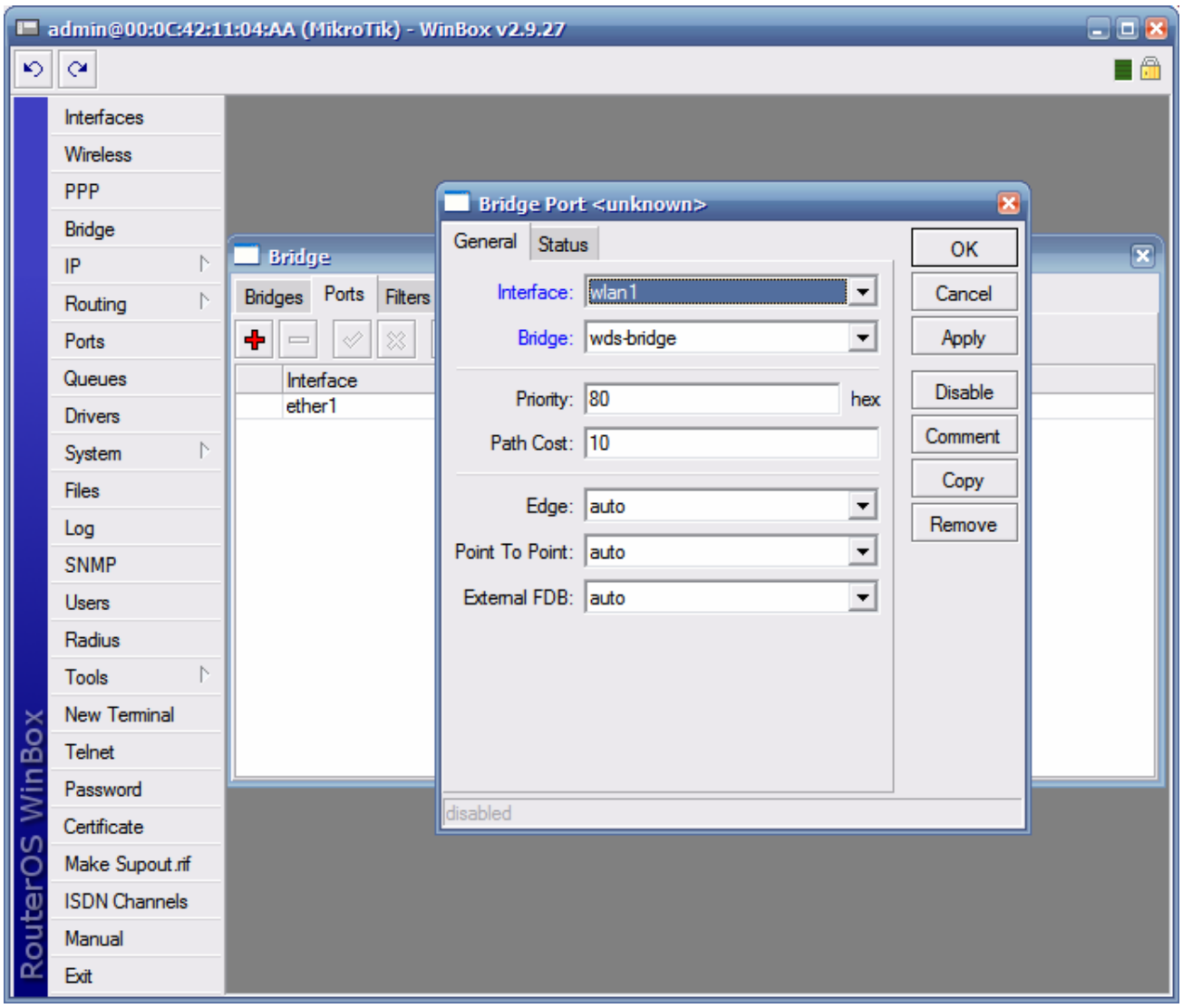
Será necessário adicionar as portas Ether1 e Wlan1 à bridge criada

- Clique em adicionar
- Em Interface, escolha ether1
- Em Bridge, escolha a bridge criada: wds-bridge



- Clique no botão OK

- Clique novamente em adicionar
- Em Interface, escolha wlan1
- Em Bridge, escolha a bridge criada: wds-bridge



- Clique no botão OK

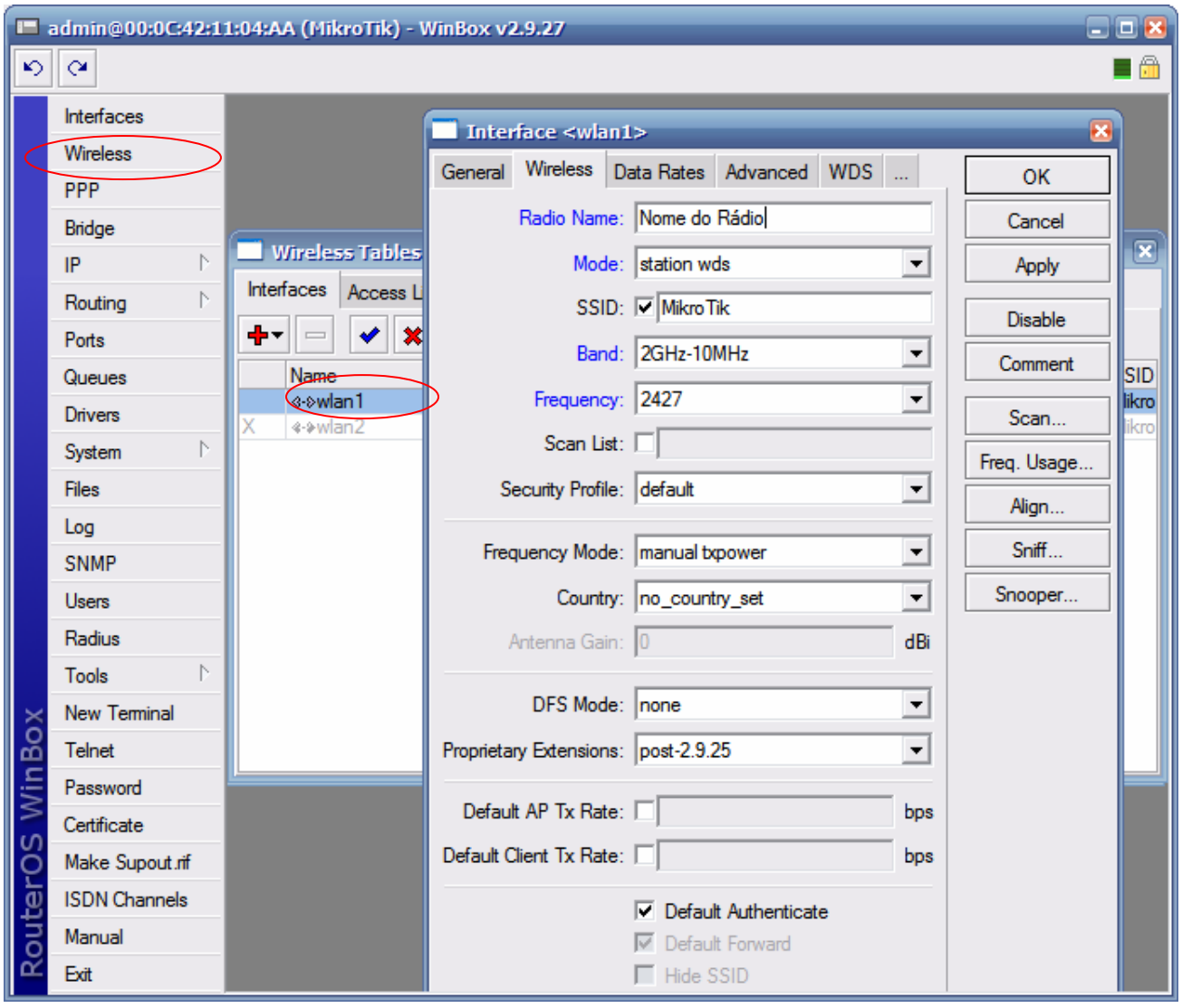
Para que haja comunicação entre os dois equipamentos, um roteador deve ser configurado como AP (station WDS) e o outro deve ser configurado como Station

CONFIGURAÇÃO DO AP (STATION WDS)

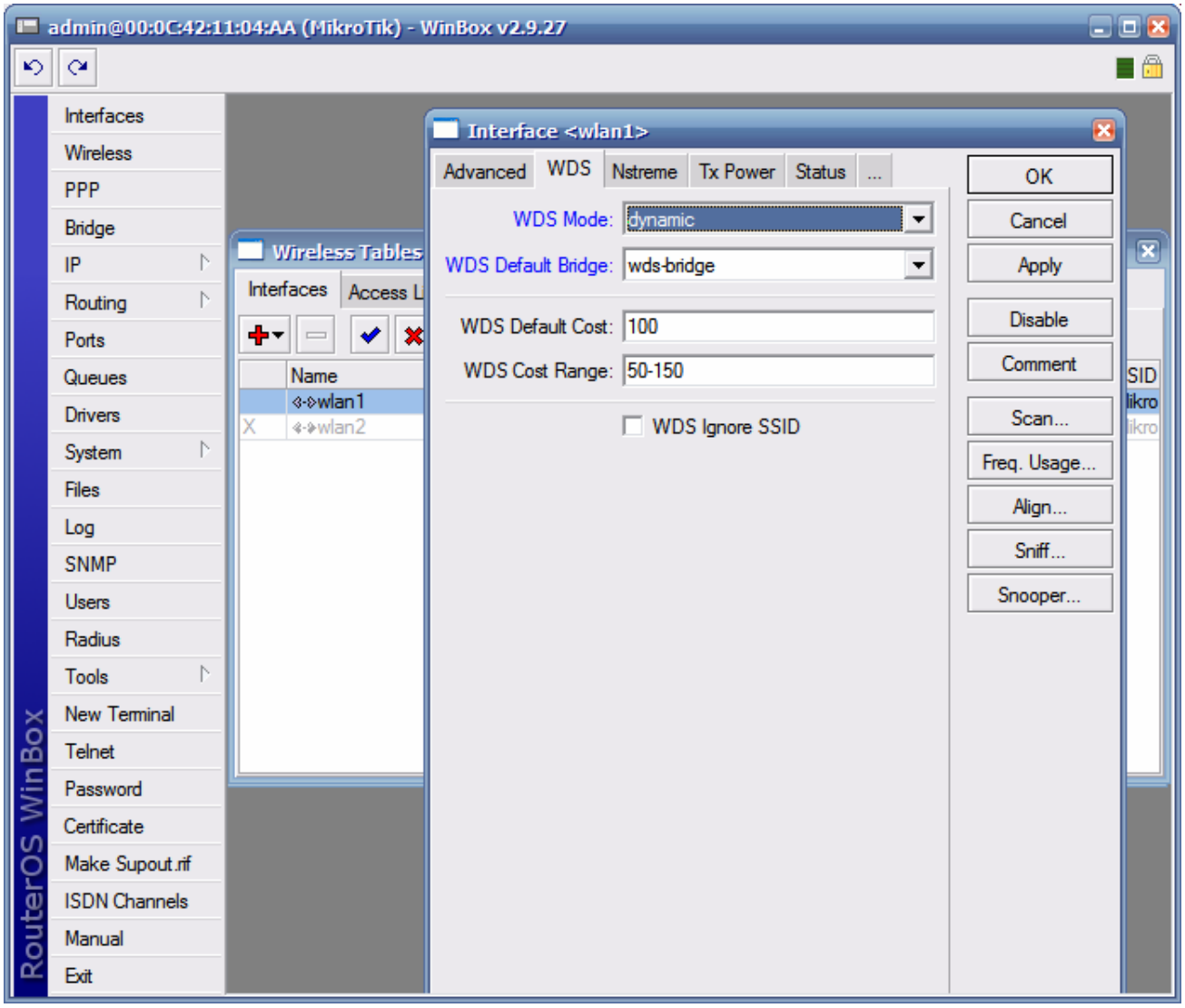
- Clique no menu Wireless
- Dê um clique duplo na interface wlan1

Na guia Wireless, configure os seguintes campos:
- Radio name: Digite o nome do rádio
- Mode: Escolha a opção station wds
- SSID: digite um SSID
- Band: Escolha a banda 2Ghz – 10Mhz (para trabalhar em 900Mhz)
- Frequency: Escolha o canal 2427 (Canal 4)

Obs: Para trabalhar com 900Mhz, deve-se usar somente os canais de 3 a 6.

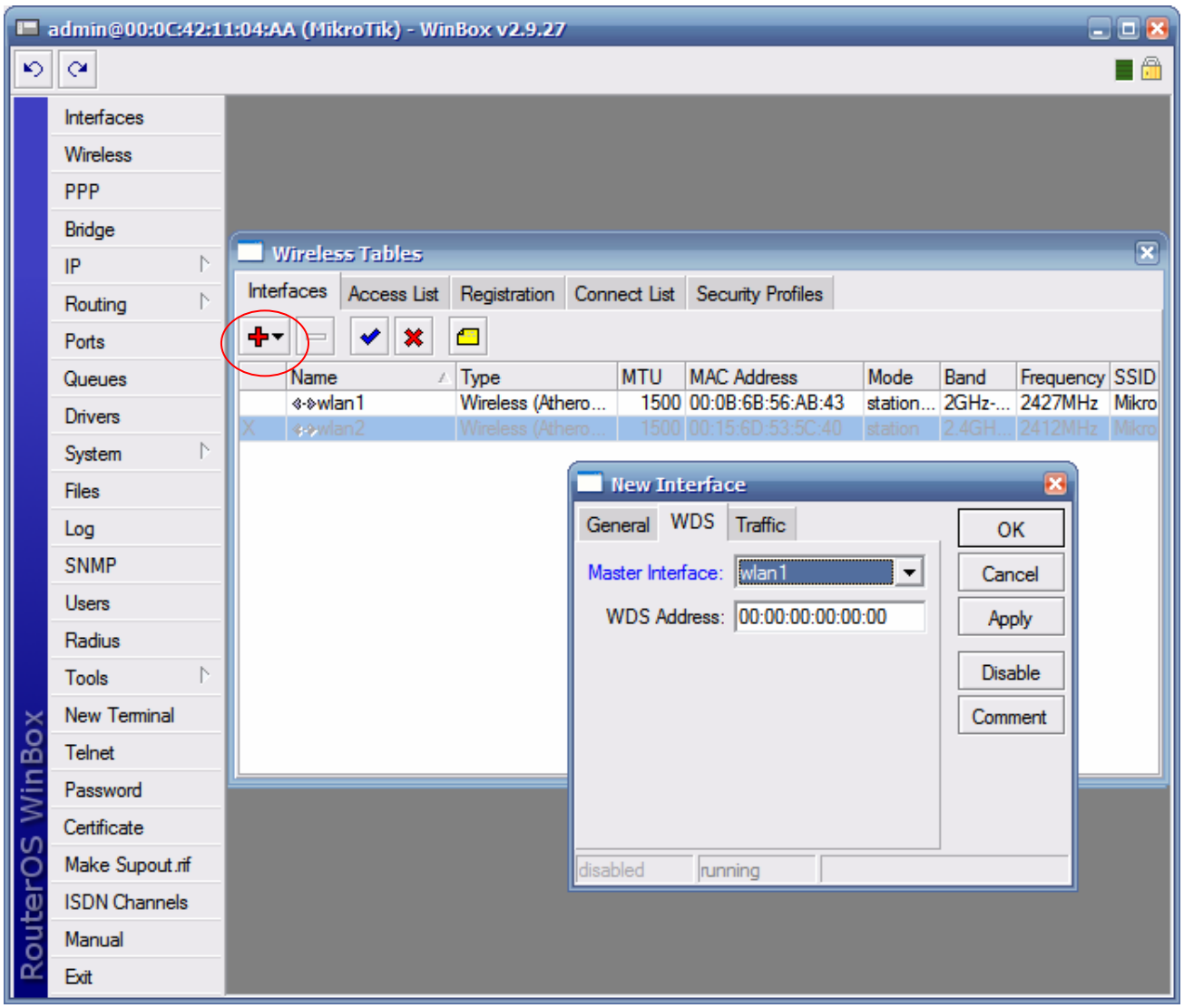


- Localize a guia WDS e clique nela
- No campo WDS Mode, escolha a opção dynamic
- No campo WDS Default Bridge, escolha a bridge criada (wds-bridge)

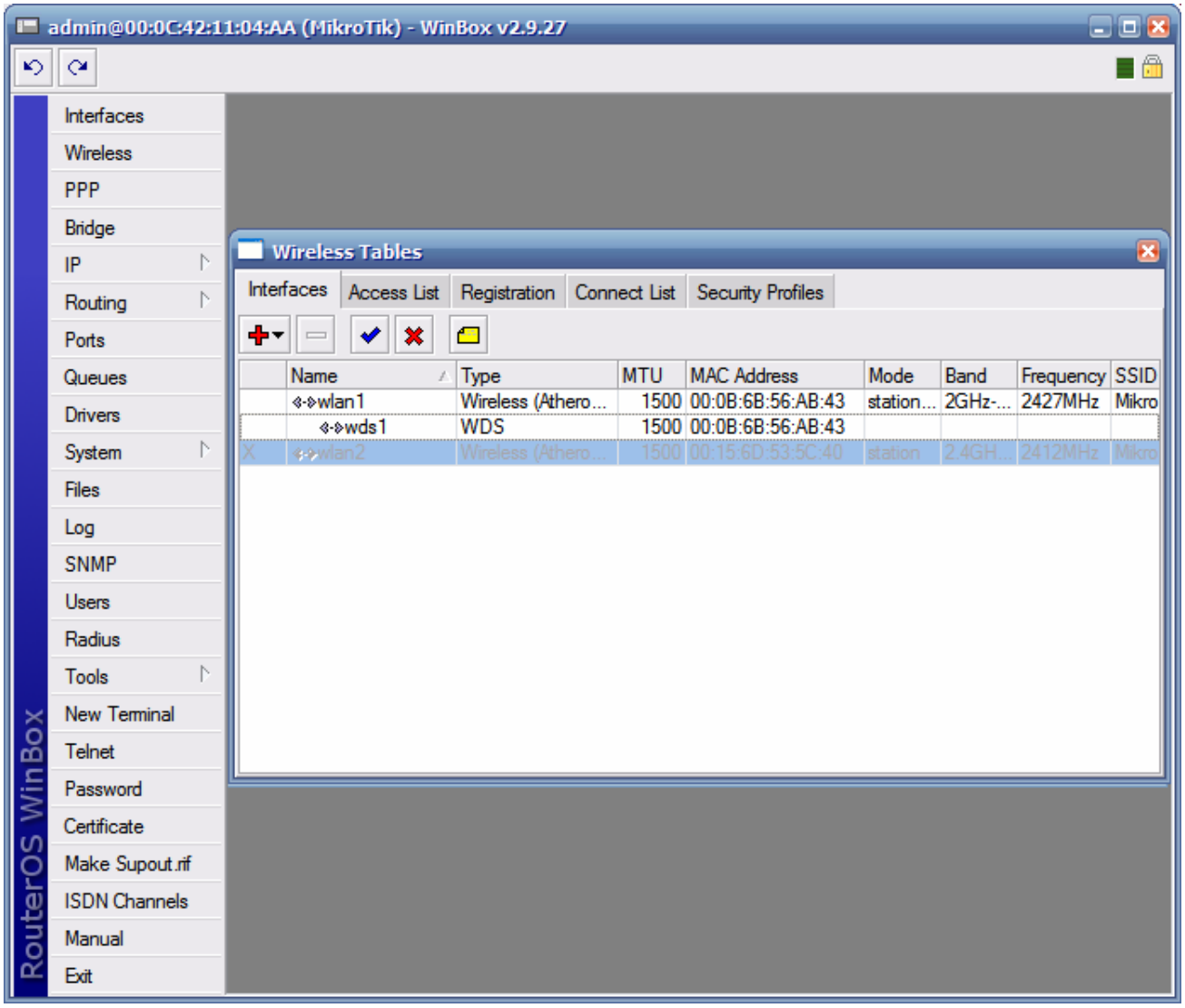


- Clique no botão OK

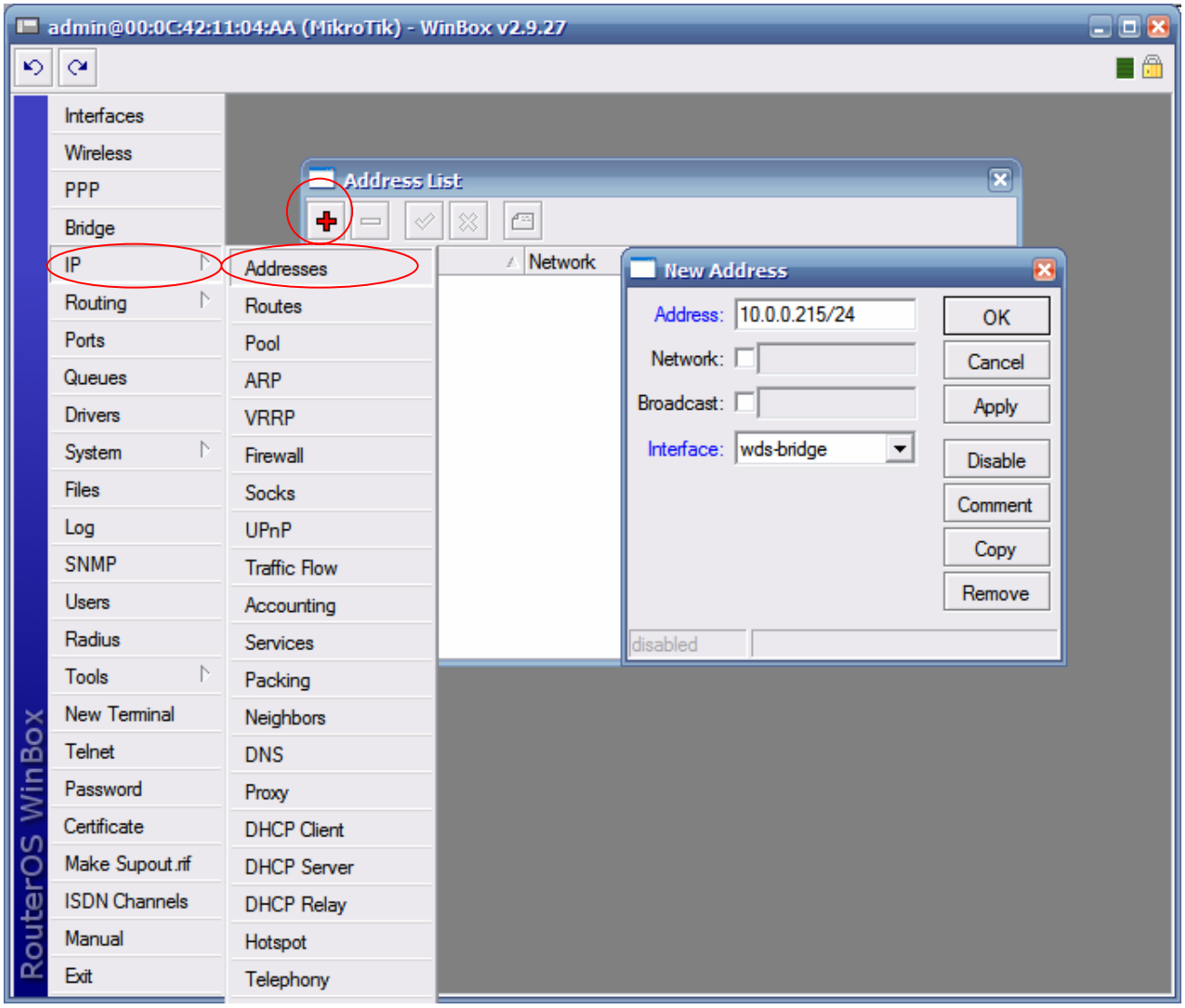
- Clique em adicionar
- Escolha a opção WDS
- Em Master Interface, escolha a opção wlan1



- Clique no botão OK



- Adicione o IP da interface Bridge
- Clique no menu IP
- Clique na opção Addresses
- Clique em adicionar
- Digite o IP 10.0.0.215/24
- Em Interface, escolha a bridge criada (wds-bridge)

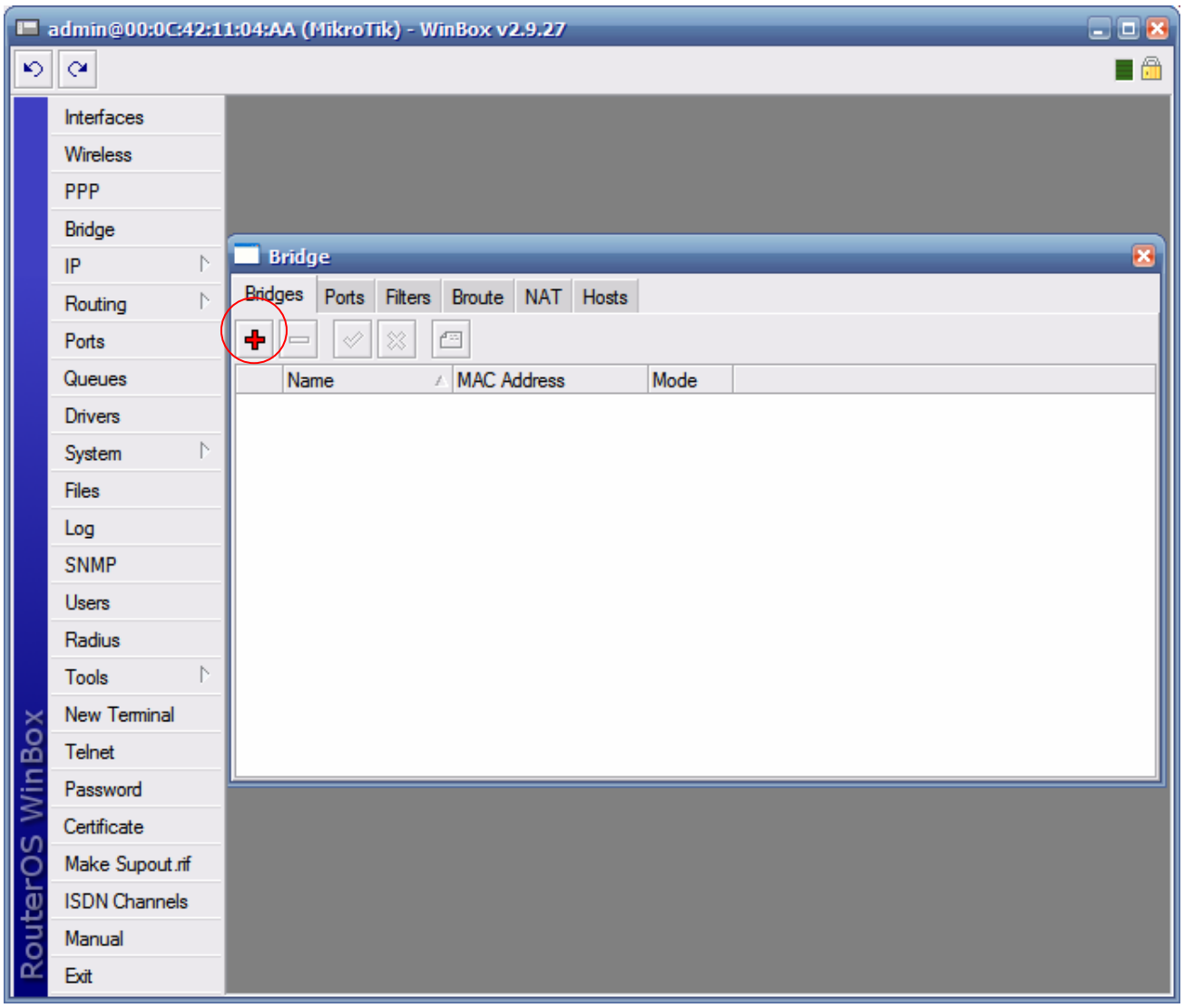


- Clique no botão OK

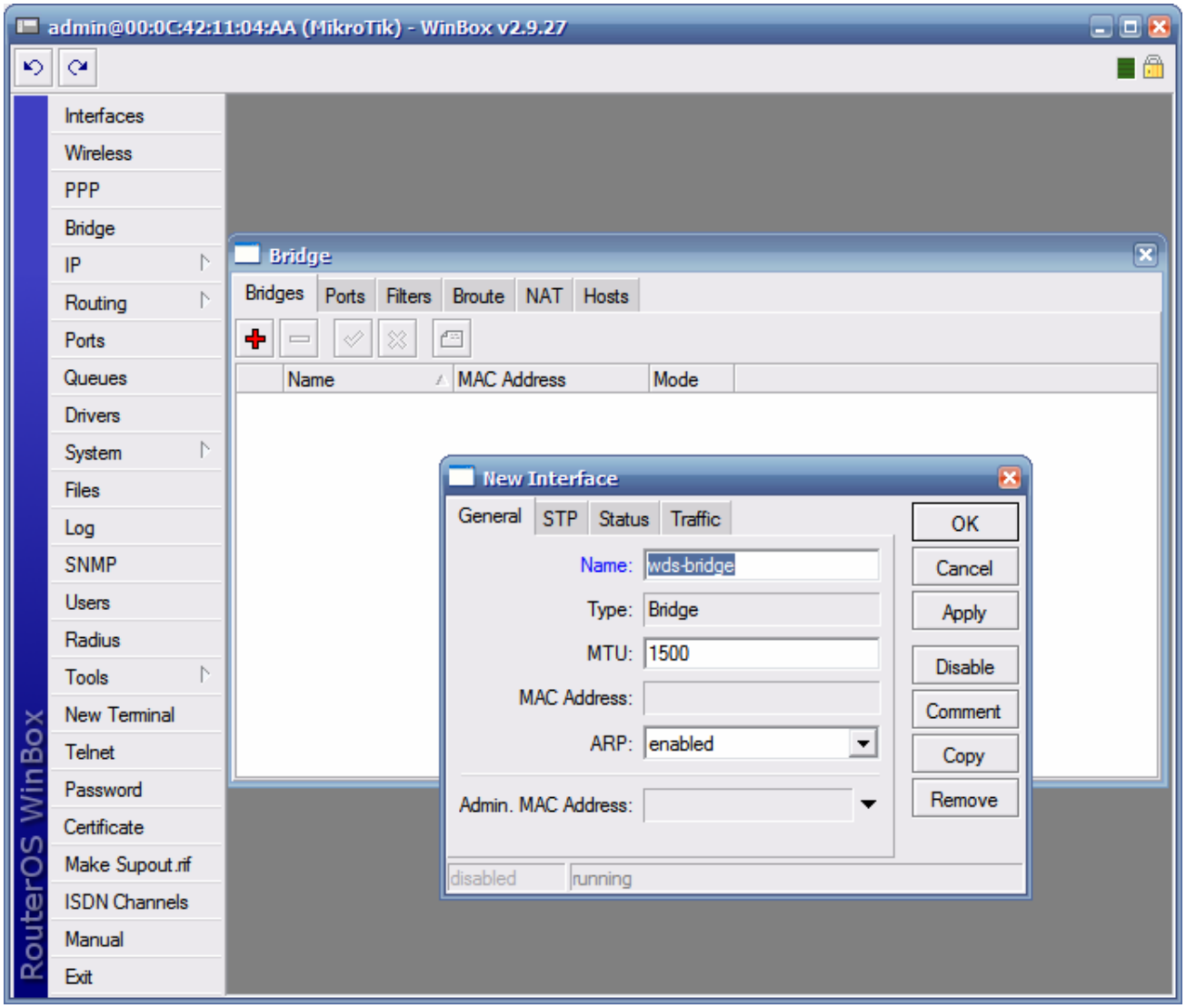
RÁDIO 2

Para a configuração do outro ponto (bridge), configure como abaixo:

- Crie uma interface bridge
- Clique no menu Bridge
- Clique em adicionar para que uma nova interface bridge seja criada.



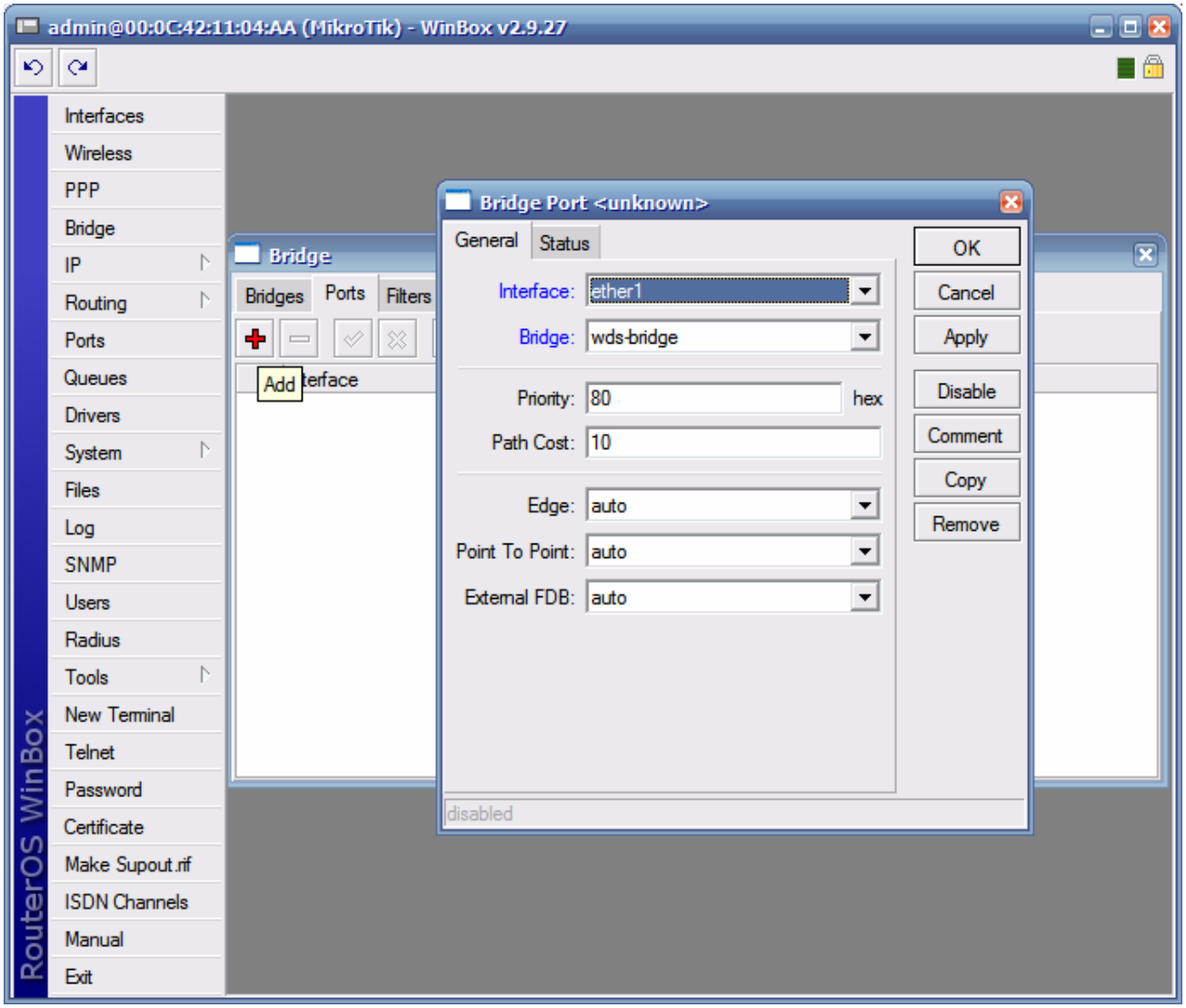
- No campo Name, digite o nome da interface bridge (exemplo: wds-bridge)



- Clique no botão OK

- Clique na guia Ports

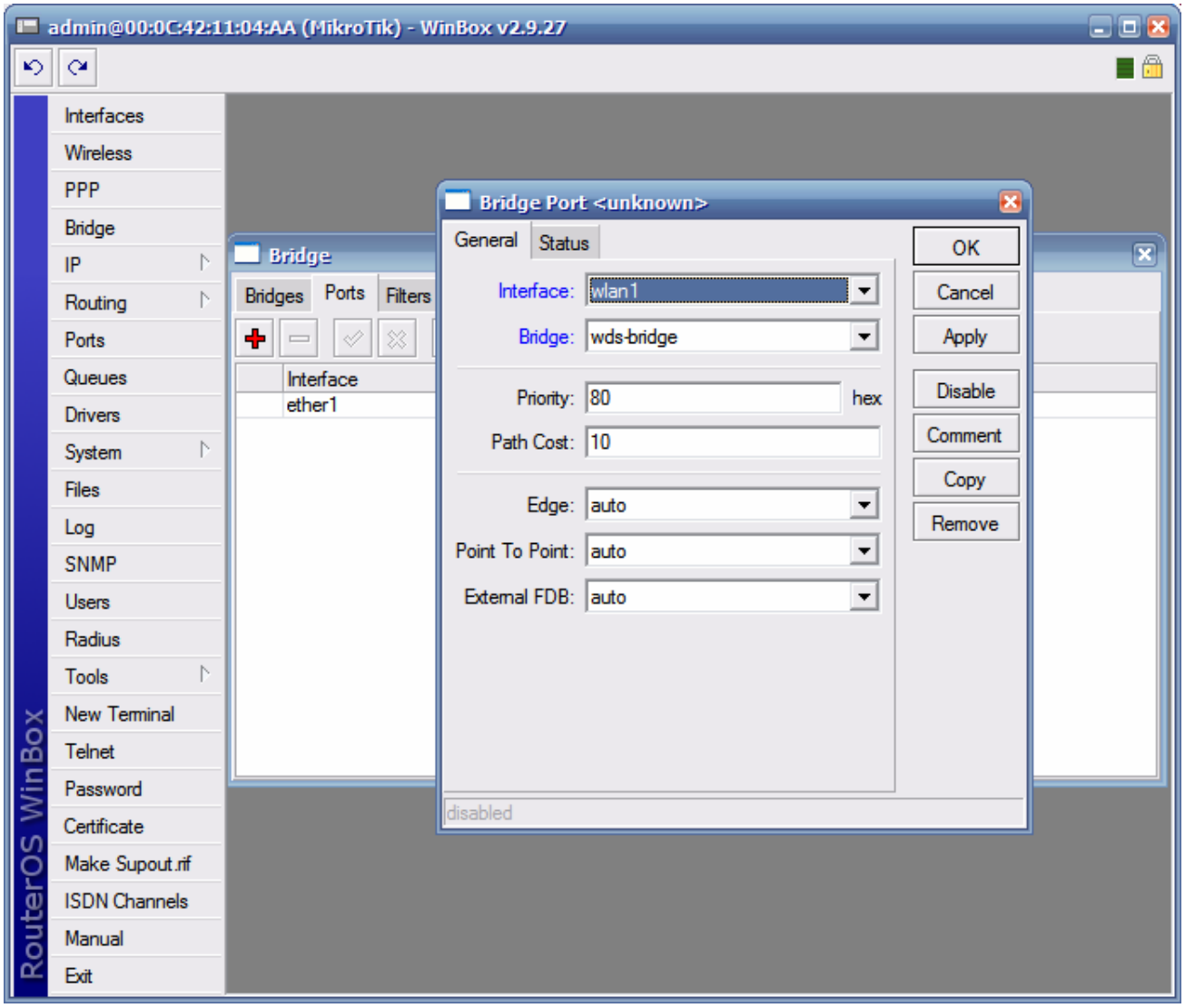
Será necessário adicionar as portas Ether1 e Wlan1 à bridge criada
- Clique em adicionar
- Em Interface, escolha ether1
- Em Bridge, escolha a bridge criada: wds-bridge



- Clique no botão OK

Clique novamente em adicionar

- Em Interface, escolha wlan1
- Em Bridge, escolha a bridge criada: wds-bridge

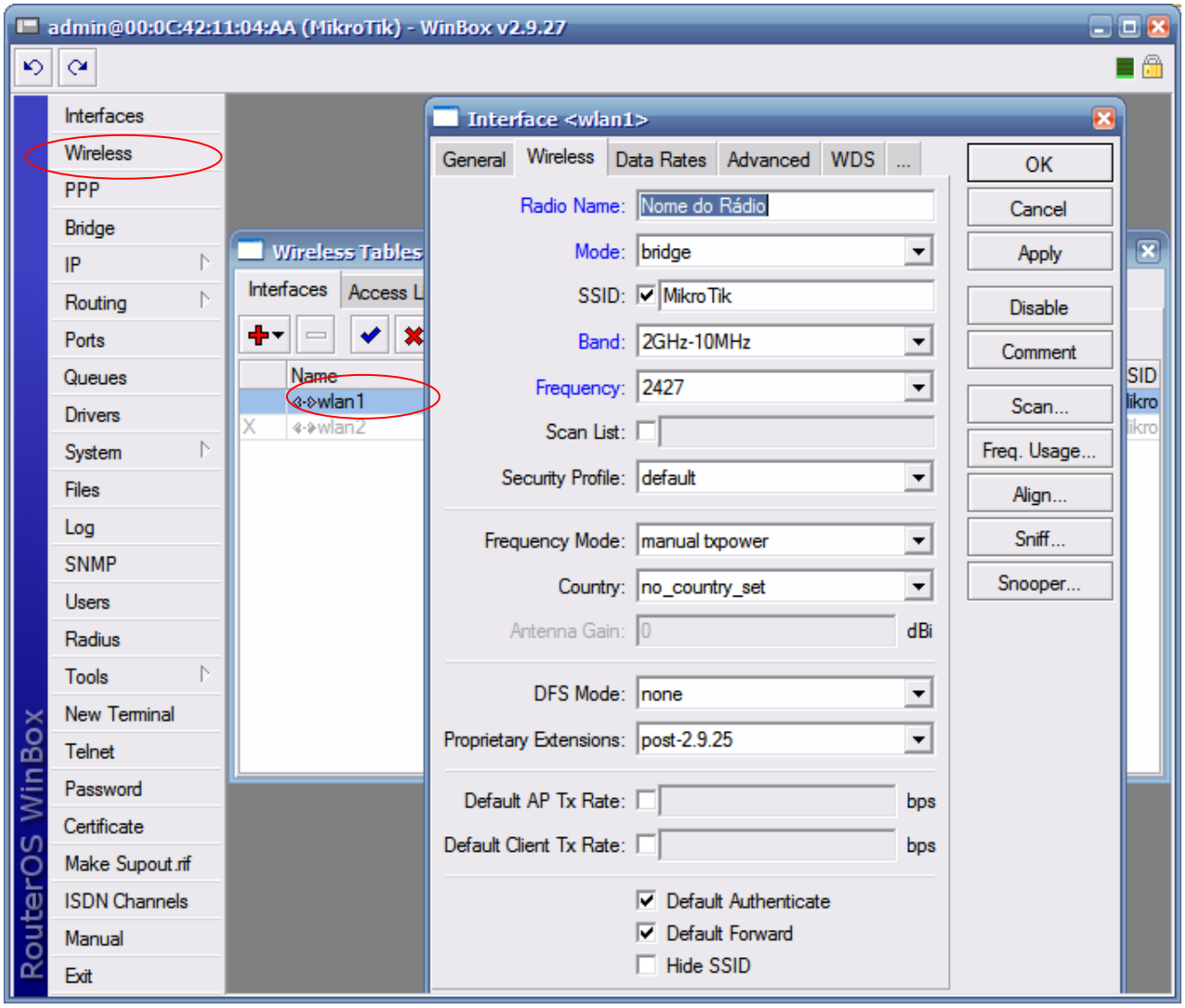


- Clique no botão OK

Para que haja comunicação entre os dois equipamentos, um roteador deve ser configurado como AP (station WDS) e o outro deve ser configurado como Station

CONFIGURAÇÃO DO CLIENTE (BRIDGE)

- Clique no menu Wireless
- Dê um clique duplo na interface wlan1

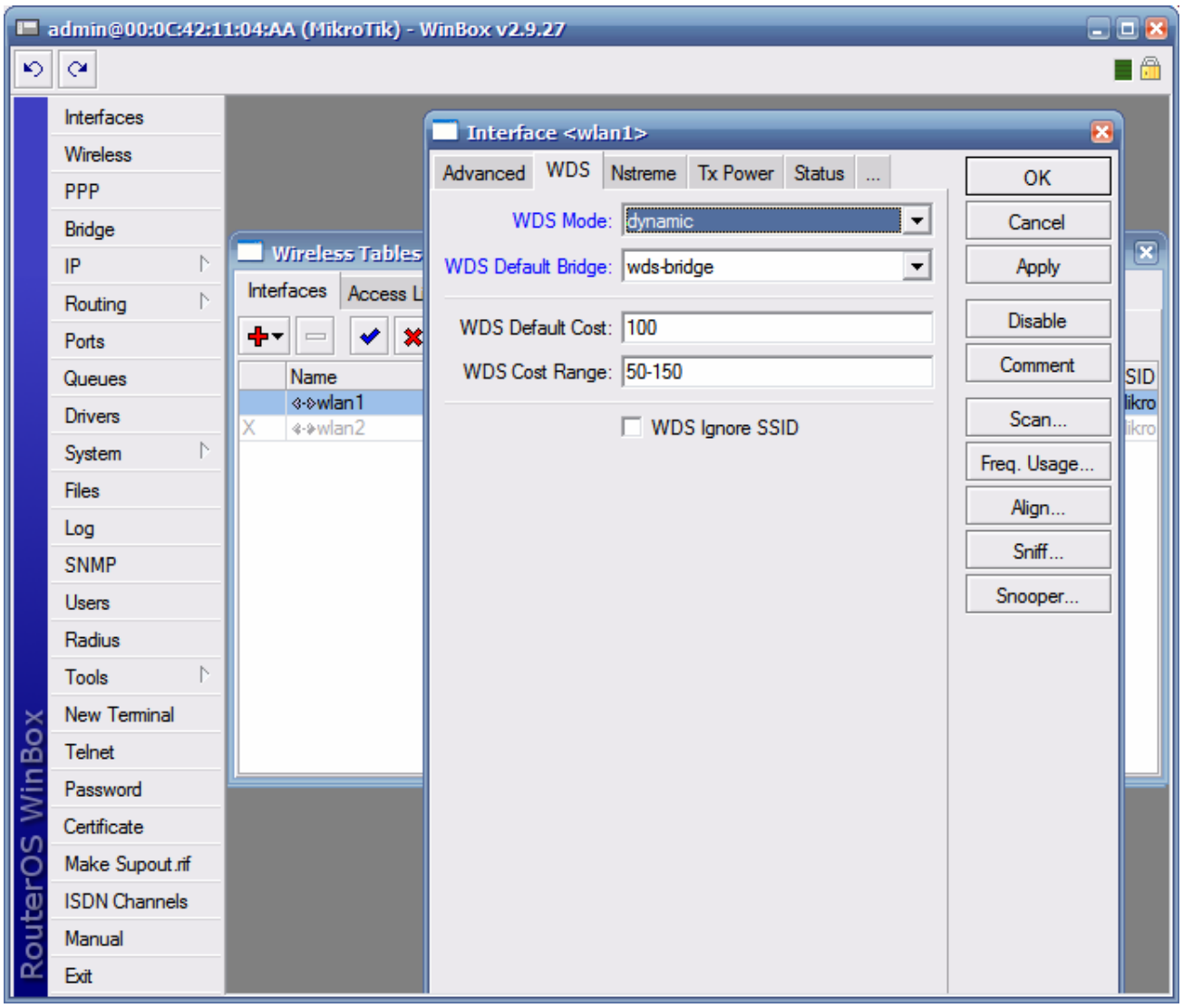


Na guia Wireless, configure os seguintes campos:

- Radio name: Digite o nome do rádio
- Mode: Escolha a opção bridge
- SSID: digite o mesmo SSID do Rádio 1
- Band: Escolha a banda 2Ghz – 10Mhz (para trabalhar em 900Mhz)
- Frequency: Escolha o canal 2427 (Canal 4)

Obs: Para trabalhar com 900Mhz, deve-se usar somente os canais de 3 a 6.

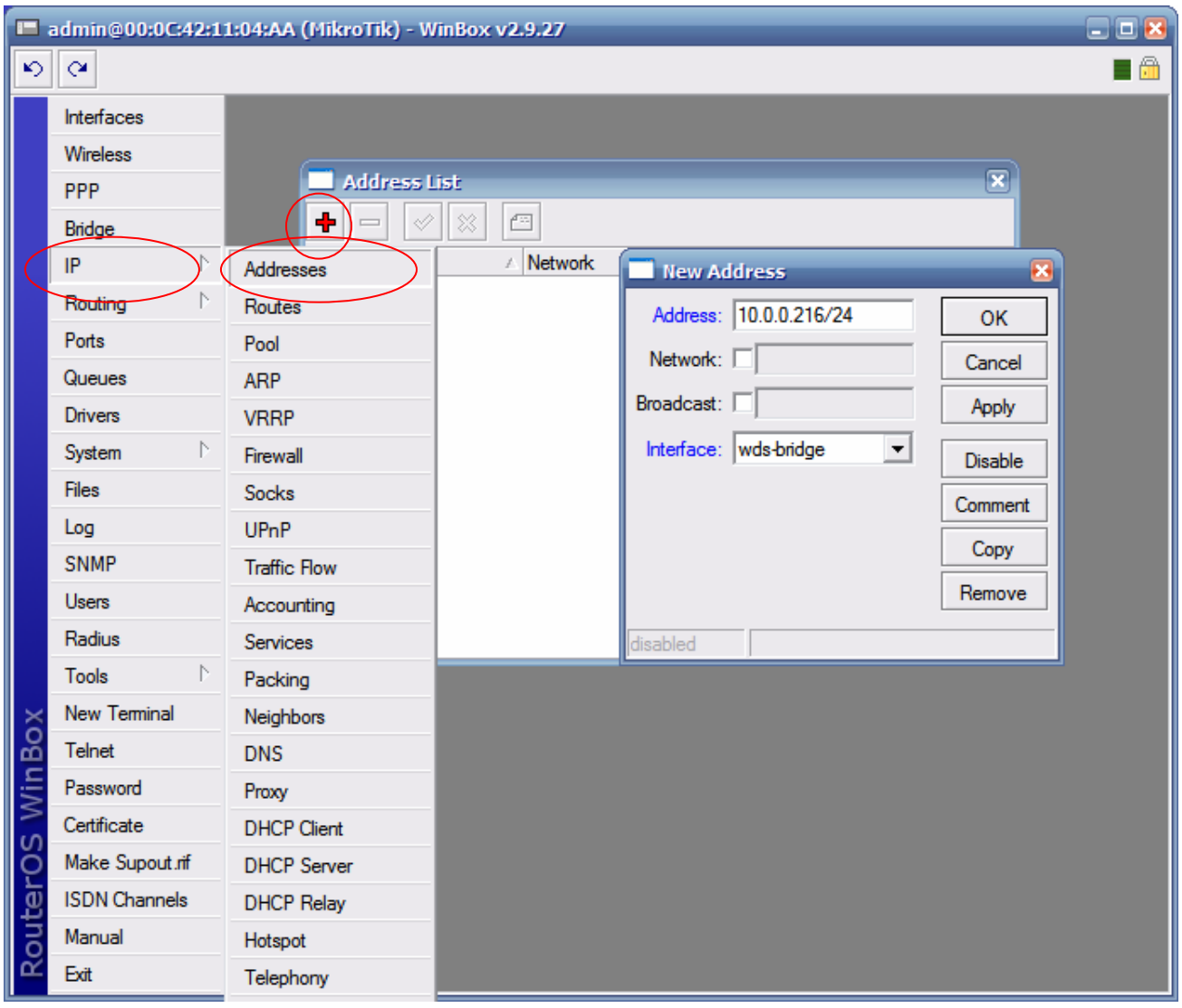
- Localize a guia WDS e clique nela
- No campo WDS Mode, escolha a opção dynamic
- No campo WDS Default Bridge, escolha a bridge criada (wds-bridge)



- Clique no botão OK

Adicione o IP da interface Bridge

- Clique no menu IP
- Clique na opção Addresses
- Clique em adicionar
- Digite o IP 10.0.0.216/24
- Em Interface, escolha a bridge criada (wds-bridge)

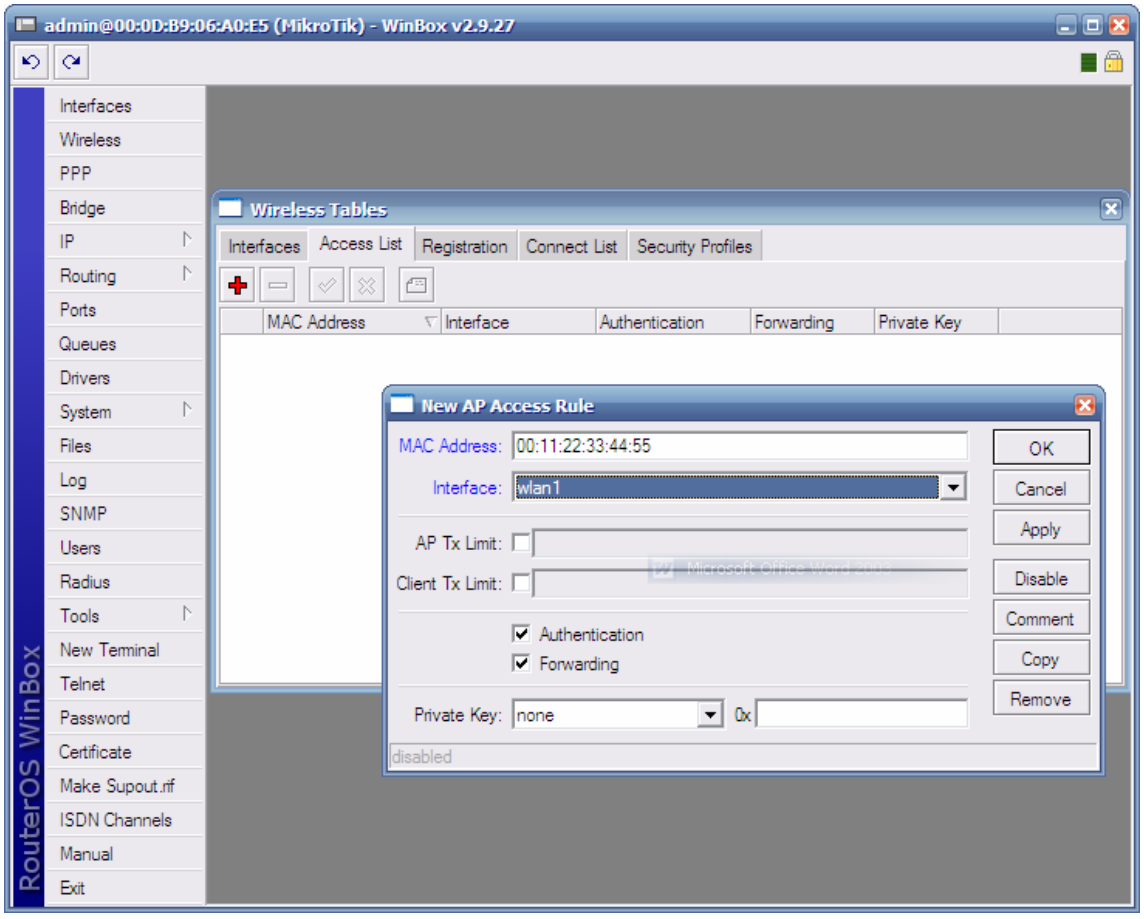


- Clique no botão OK

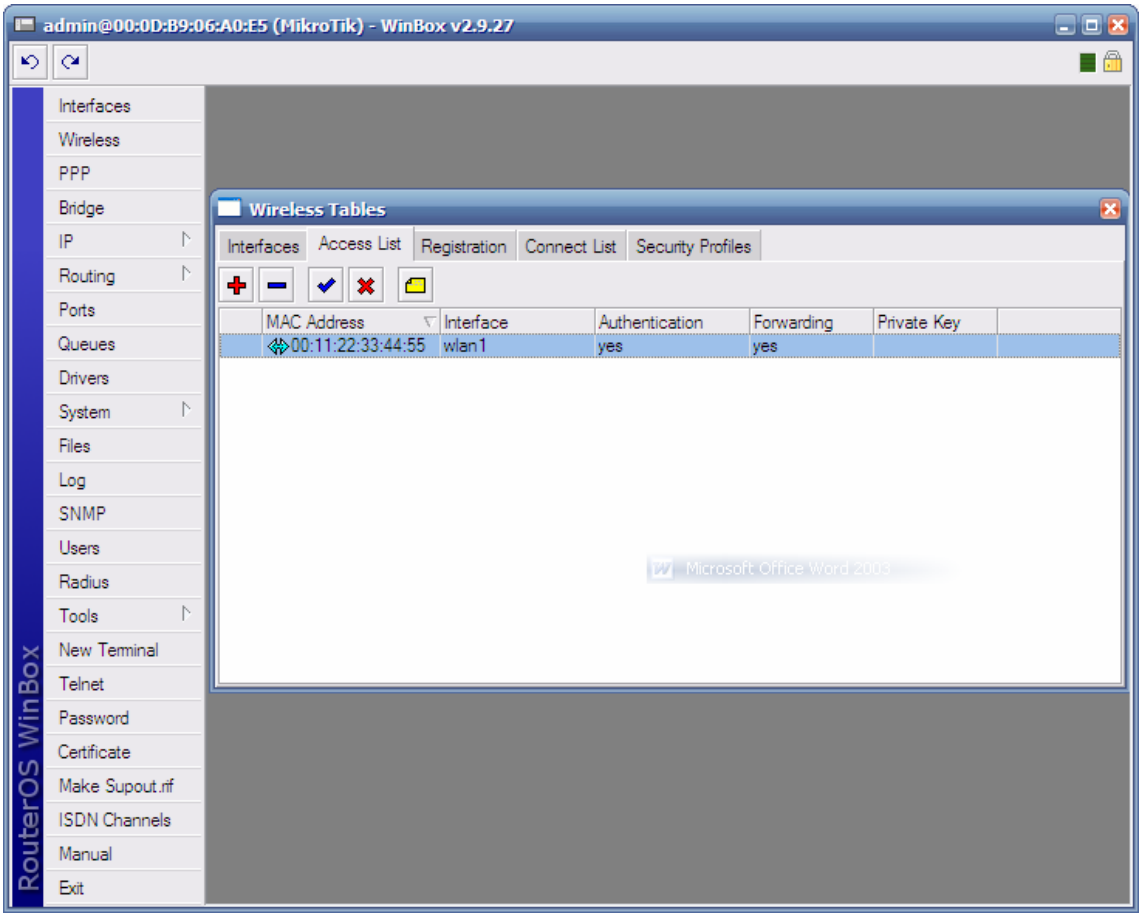
A configuração está completa.

CONTROLE DE CLIENTES APENAS POR MAC

- Clique no menu “Wireless”
- Clique na guia “Access List”
- Clique em “+” para adicionar uma nova regra
- Em “MAC Address”, digite o MAC da placa do cliente
- Escolha a interface onde o cliente estará conectado em “Interface”

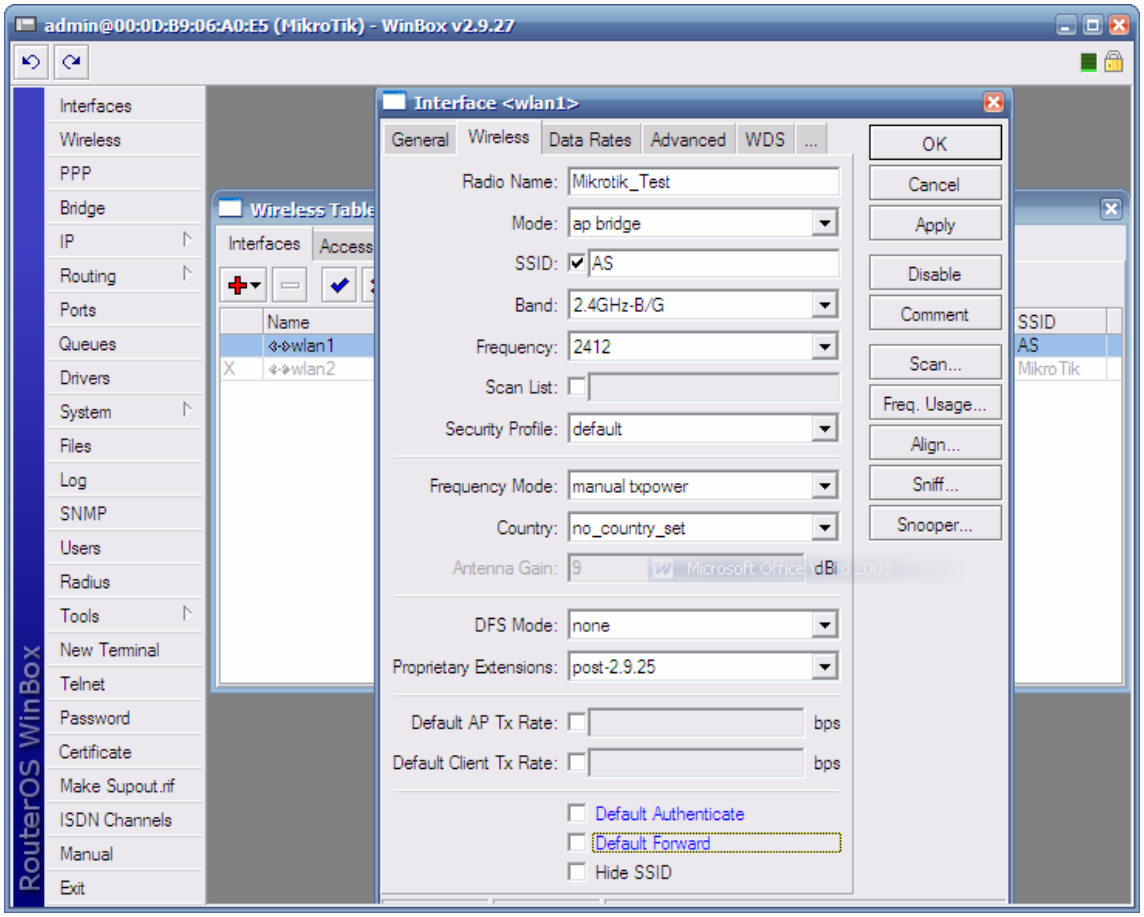


- Clique no botão OK



- Basta repetir os últimos passos até cadastrar todos os usuários.

- Clique na guia “Interfaces”
- Dê um clique duplo na interface que você quer ativar o controle por MAC
- Na guia “Wireless”, desative as opções:
    - “Default Authenticate”
    - “Default Forward” (impede que os clientes se vêem na interface)

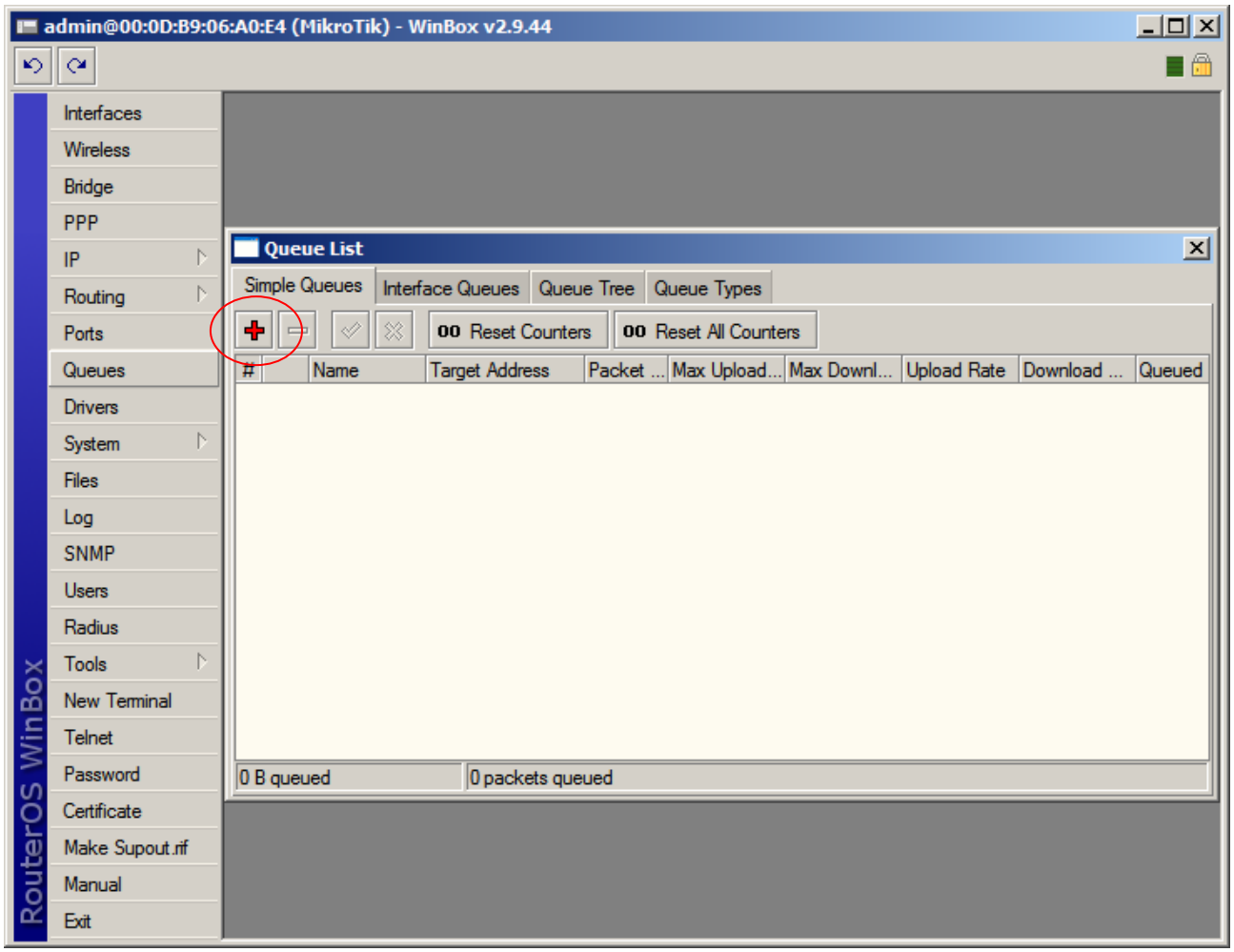


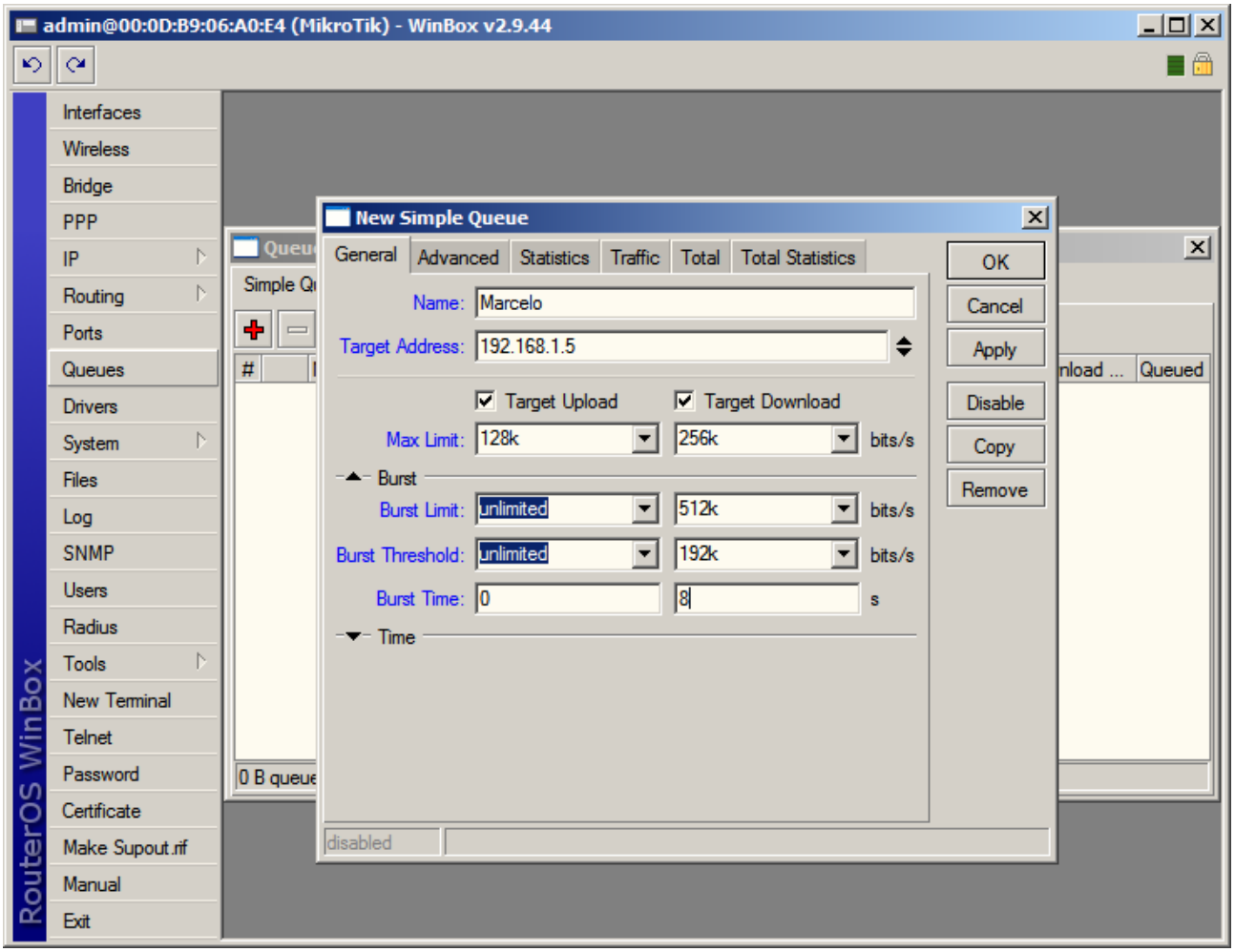
- Clique no botão OK

CONTROLE DE BANDA – Simple Queue

As Filas simples (Simple Queue) é a meneira mais fácil de se controlar a velocidade dos clientes. Elas permitem configurar as velocidades de upload e download com apenas uma entrada.

- Clique no Menu “Queues”
- Clique em “Adicionar”





As propriedades configuráveis de uma fila simples são:
- Limite por direção IP de origem ou destino
- Interface do cliente
- Tipo de fila
- Configurações de limit-at, max-limit, priority e bursts para download e upload
- Configurações de limit-at, max-limit, priority e bursts para velocidade agregada

COMO FUNCIONA O BURST

Bursts são usados para permitir altas taxas de dados por um curto período de tempo.
Os parâmetros que controlam o Burst são:
- burst-limit: limite máximo que alcançará
- burst-time: tempo que durará o burst
- burst-threshold: patamar onde começa a limitar
- max-limit: MIR

Exemplo:
Max-limit=256kbps
Burst-time=8s
Burst-threshold=192kbps
Burst-limit=512kbps

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

- com 1 segundo a taxa média é (0+0+0+0+0+0+0+512)/8 = 64kbps (abaixo do threshold)
- com 2 segundos já é de (0+0+0+0+0+0512+512)/8 = 128kbps (abaixo do threshold)
- com 3 segundos (0+0+0+0+0+512+512+512)/8 = 192kbps (é o ponto de inflexão – onde acaba o burst)

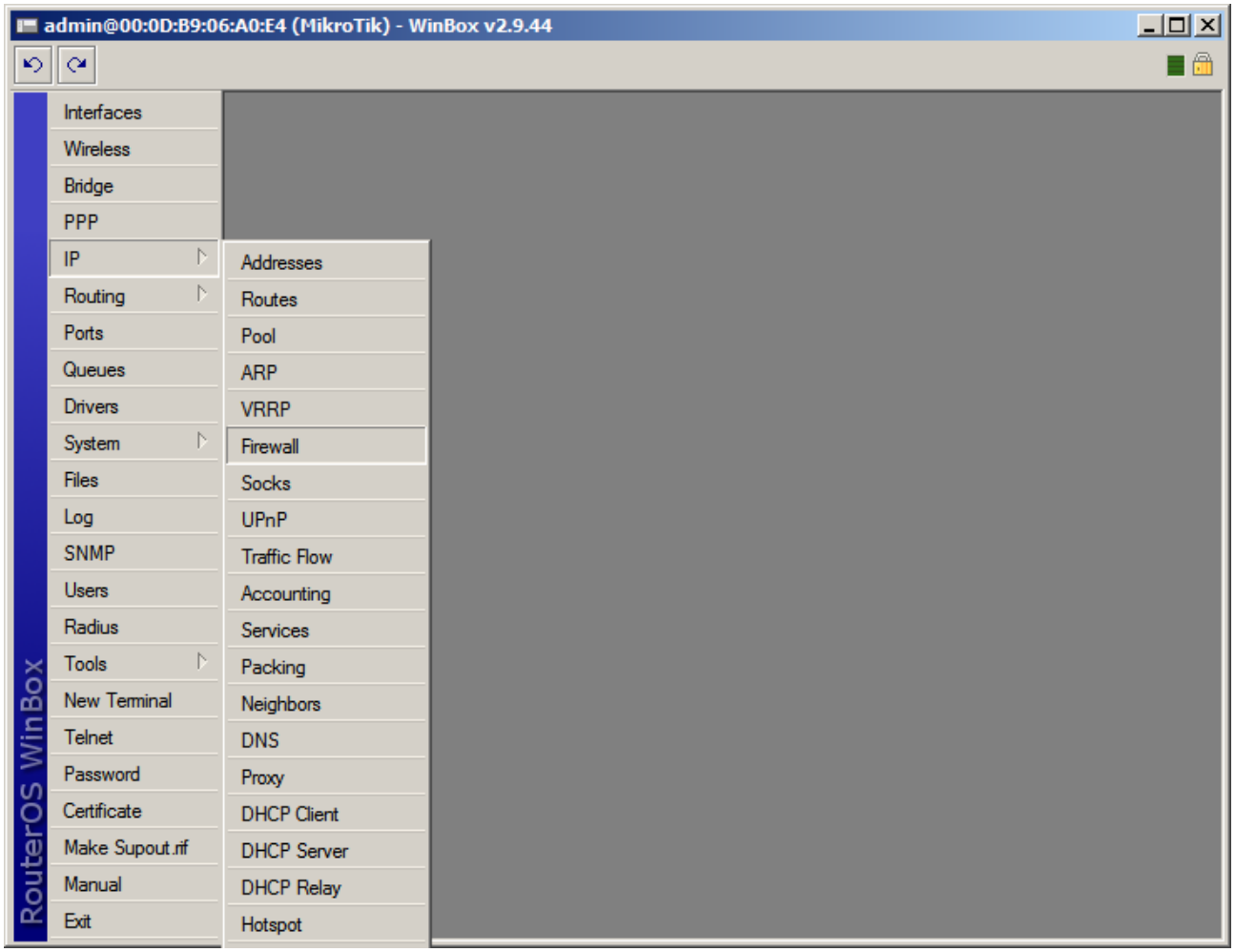
A partir do momento que foi atingido o ponto de inflexão, o Burst é desabilitado e a taxa máxima do cliente passa a ser o max-limit

LIMITAÇÃO DE BANDA PARA P2P

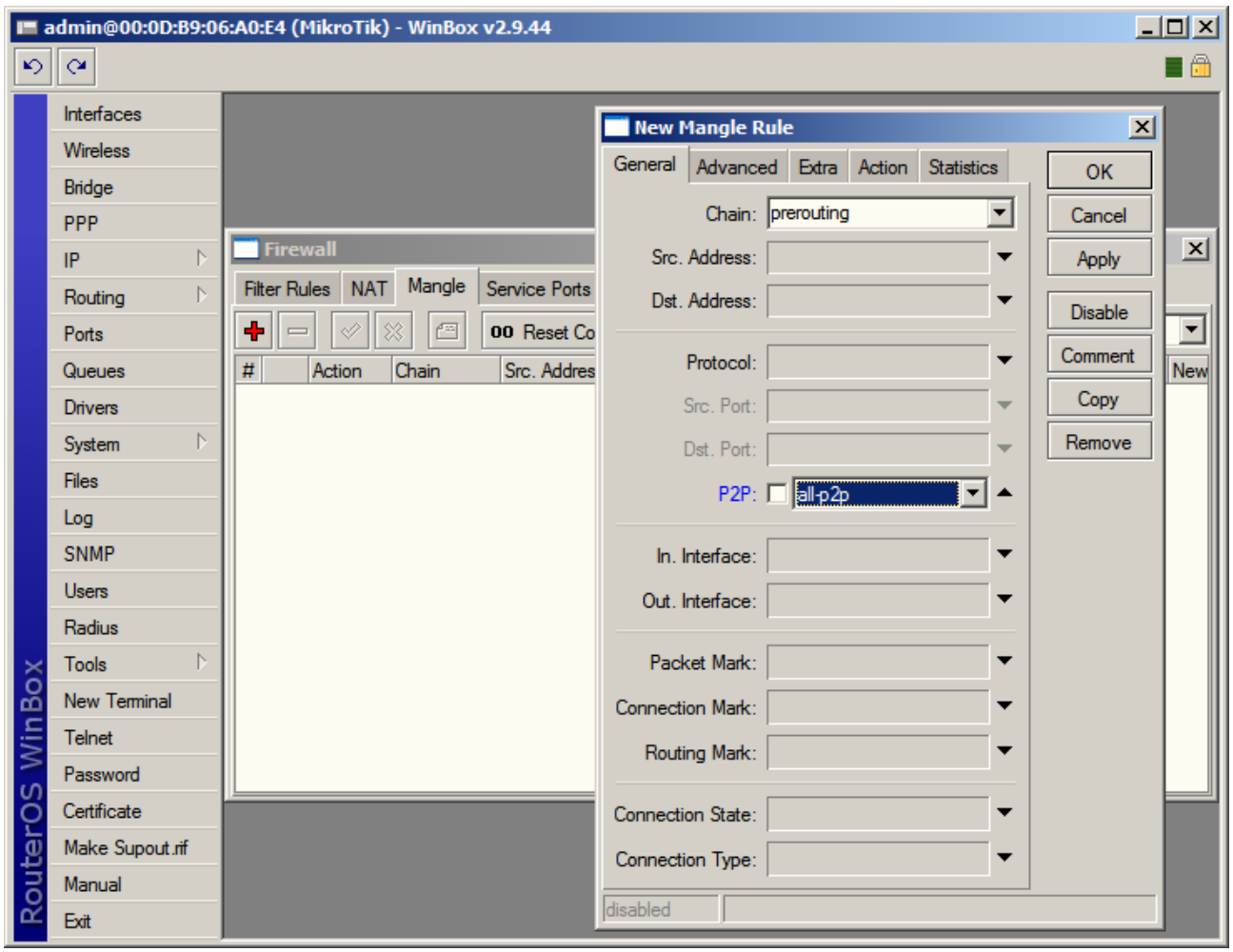
Para fazer a limitação de banda para P2P deverá ser usado algumas regras utilizando o Firewall e o Queue

FIREWALL

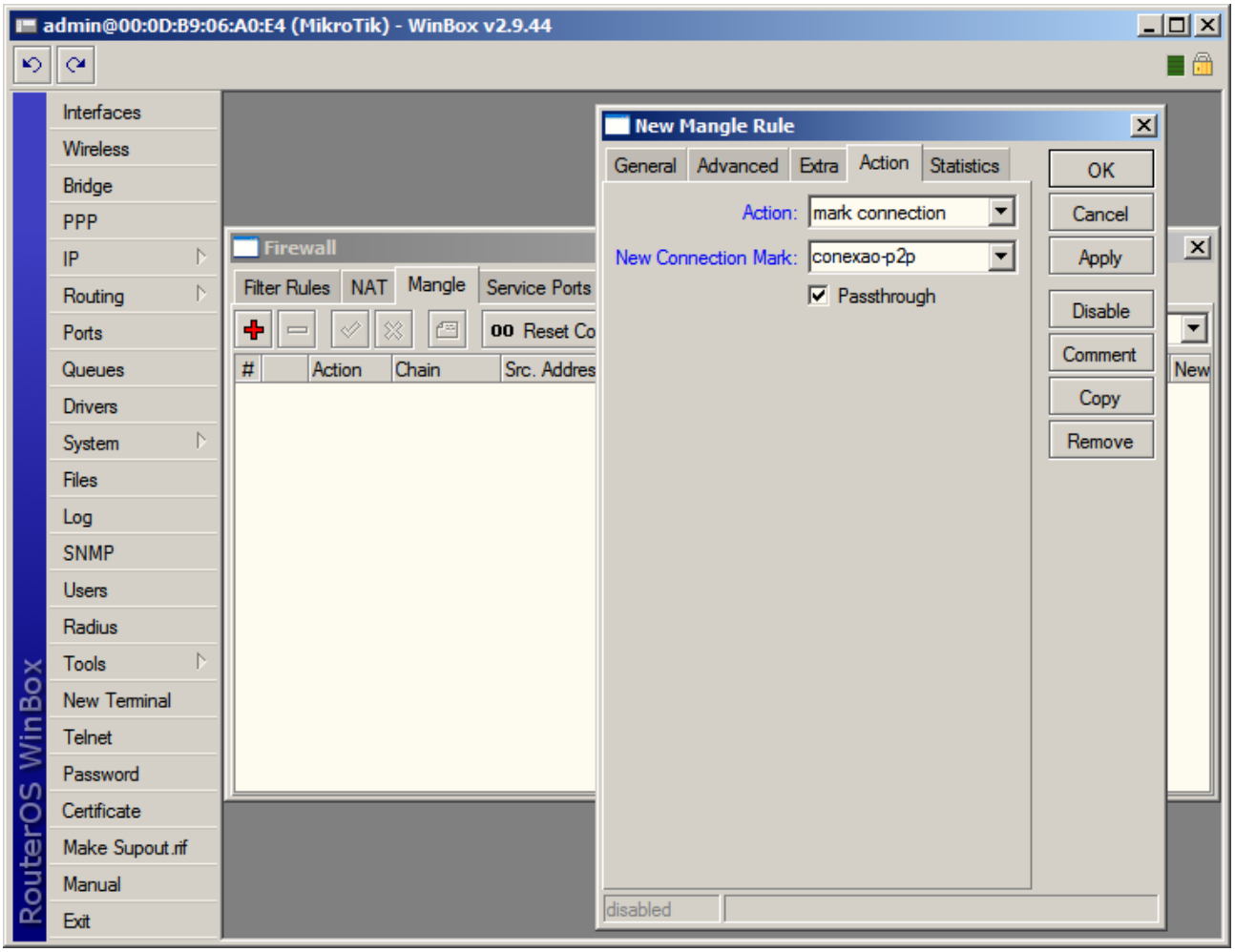
- Clique no menu “IP”
- Clique na opção “Firewall”



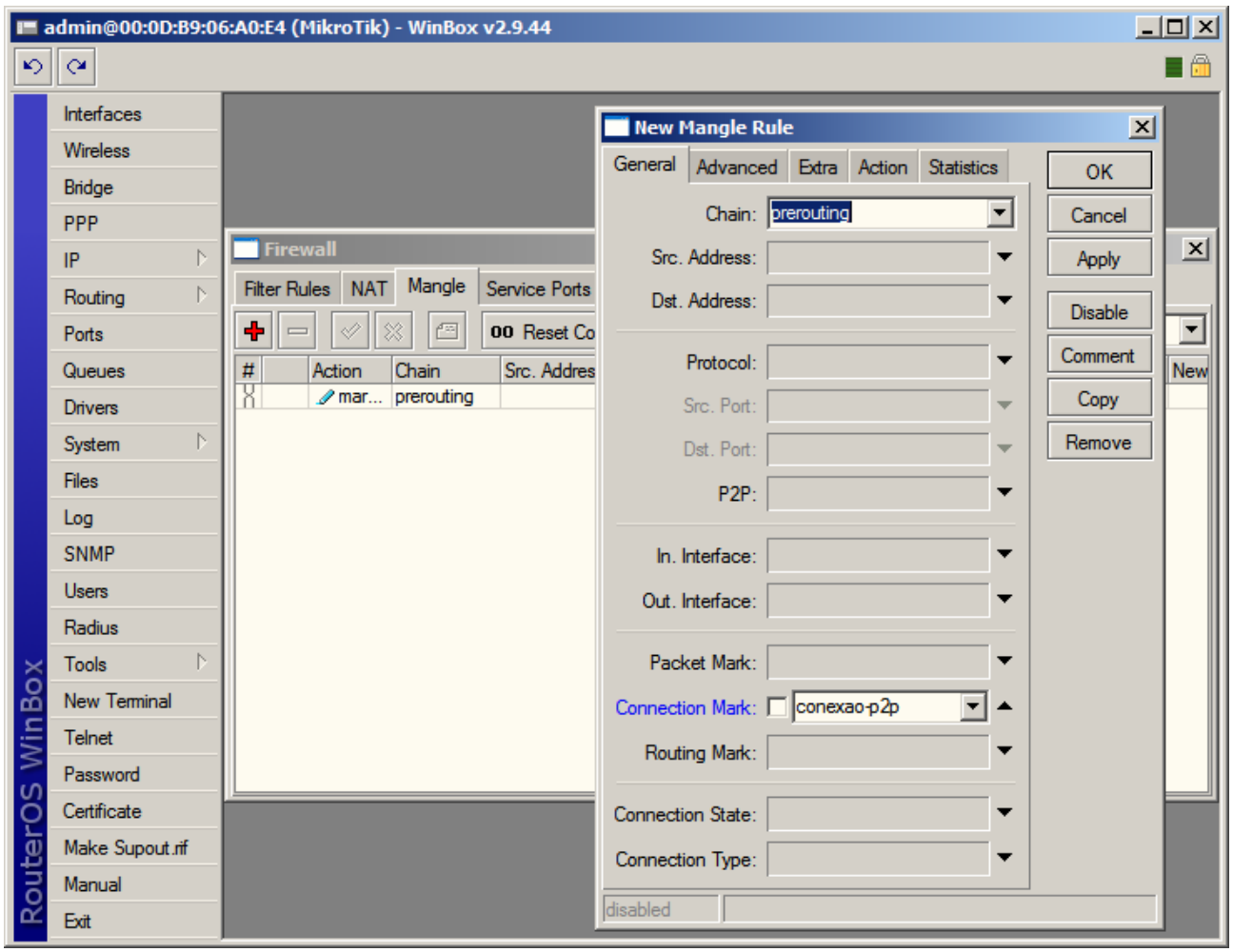
- clique na guia “Mangle”
- na Guia “General”, na opção “Chain”, escolha a opção “prerouting”
- na opção “P2P”, escolha a opção “all-p2p”



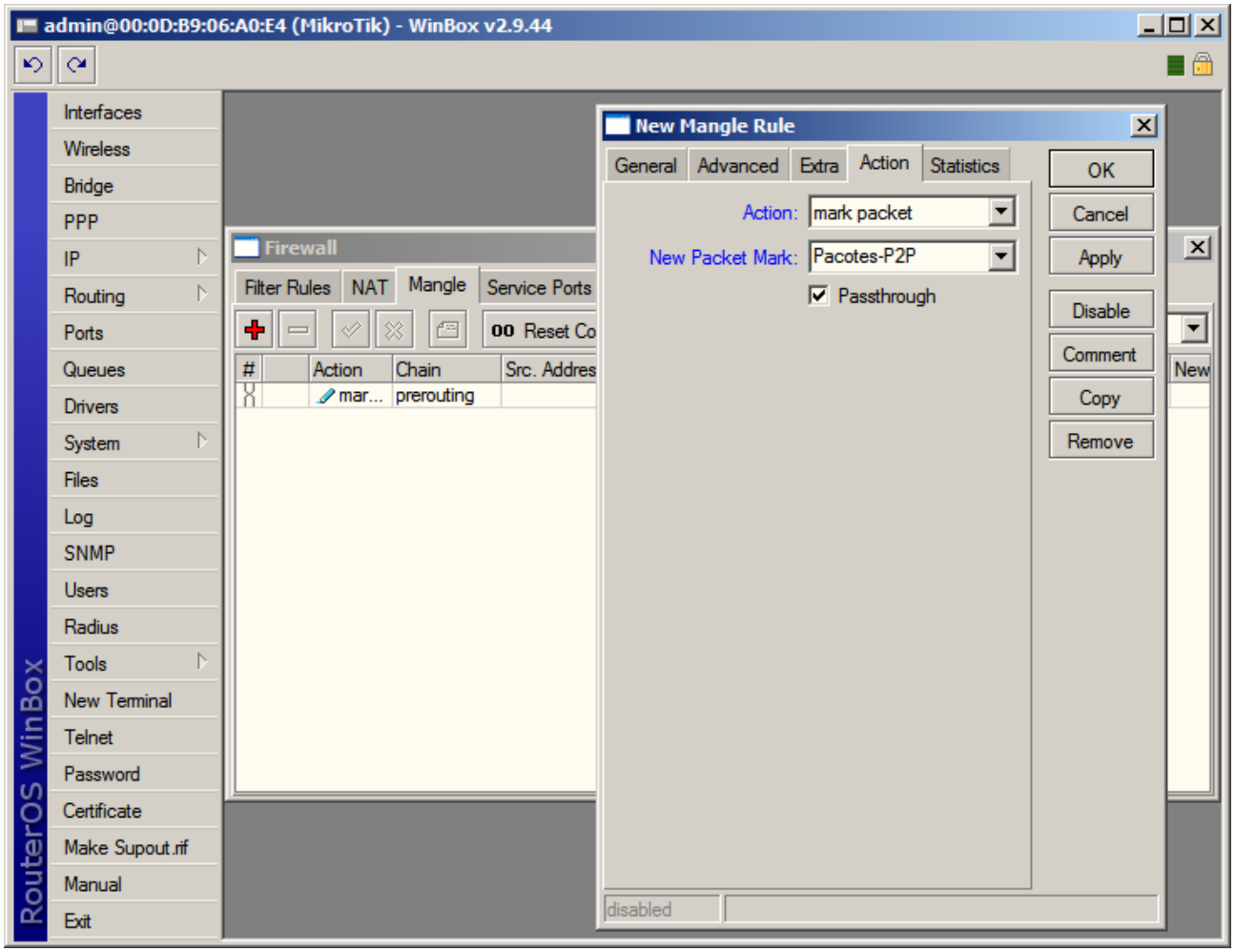
- Clique na guia “Action”
- Na opção “Action”, escolha “mark connection”
- Na opção “New Connection Mark”, digite um nome para a marcação da conexão
- Mantenha a opção “Passthrough” ativada
- Clique no botão “OK”



- Clique novamente em “Adicionar”
- Na guia “General”, na opção “Chain”, escolha a opção “prerouting”
- Na opção “Connection Mark”, escolha a marcação criada na regra anterior.

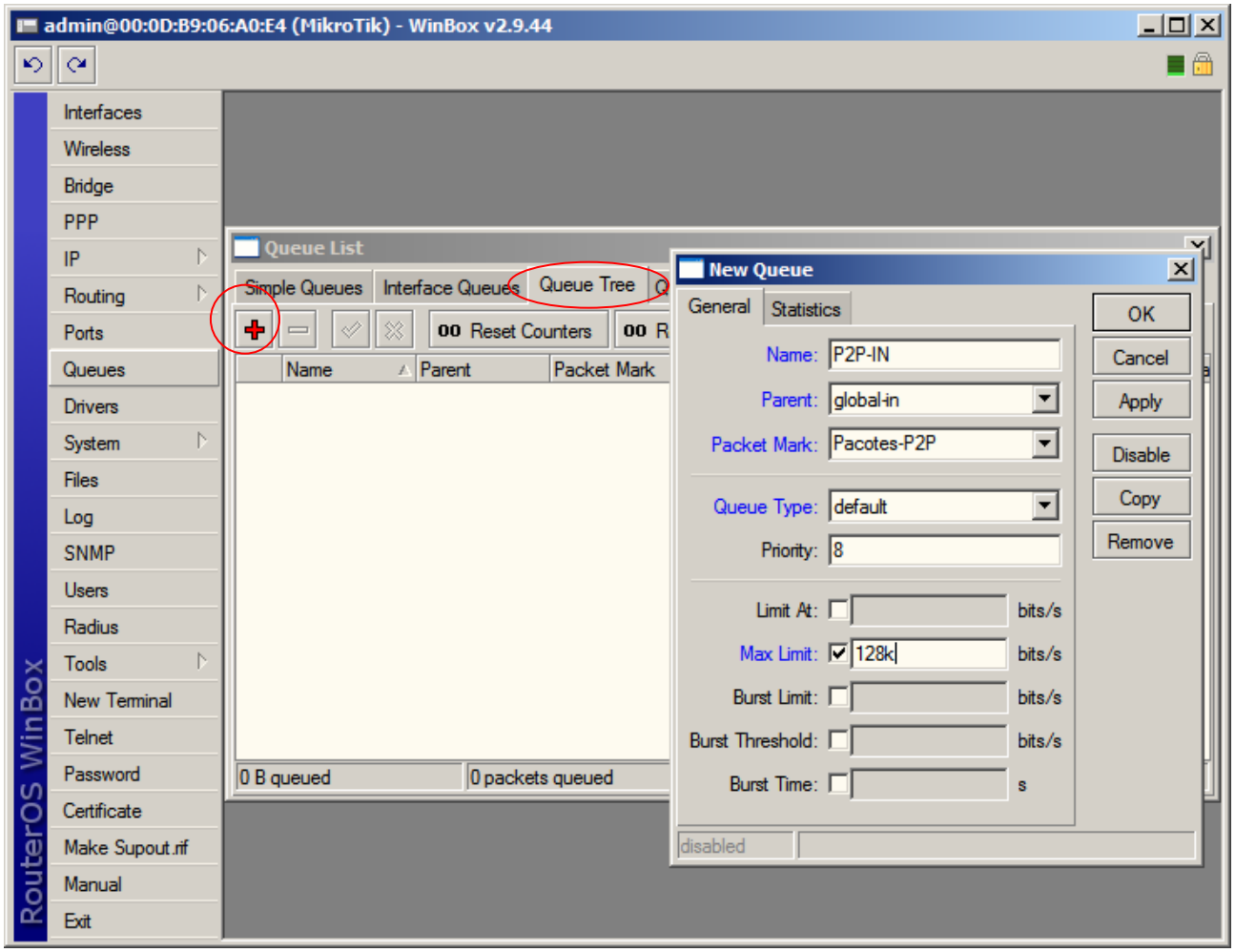


- Clique na guia “Action”
- Na opção “Action”, escolha a opção “mark packet”
- Na opção “New Packet Mark”, digite um nome para a marcação dos pacotes
- Clique no botão “OK”

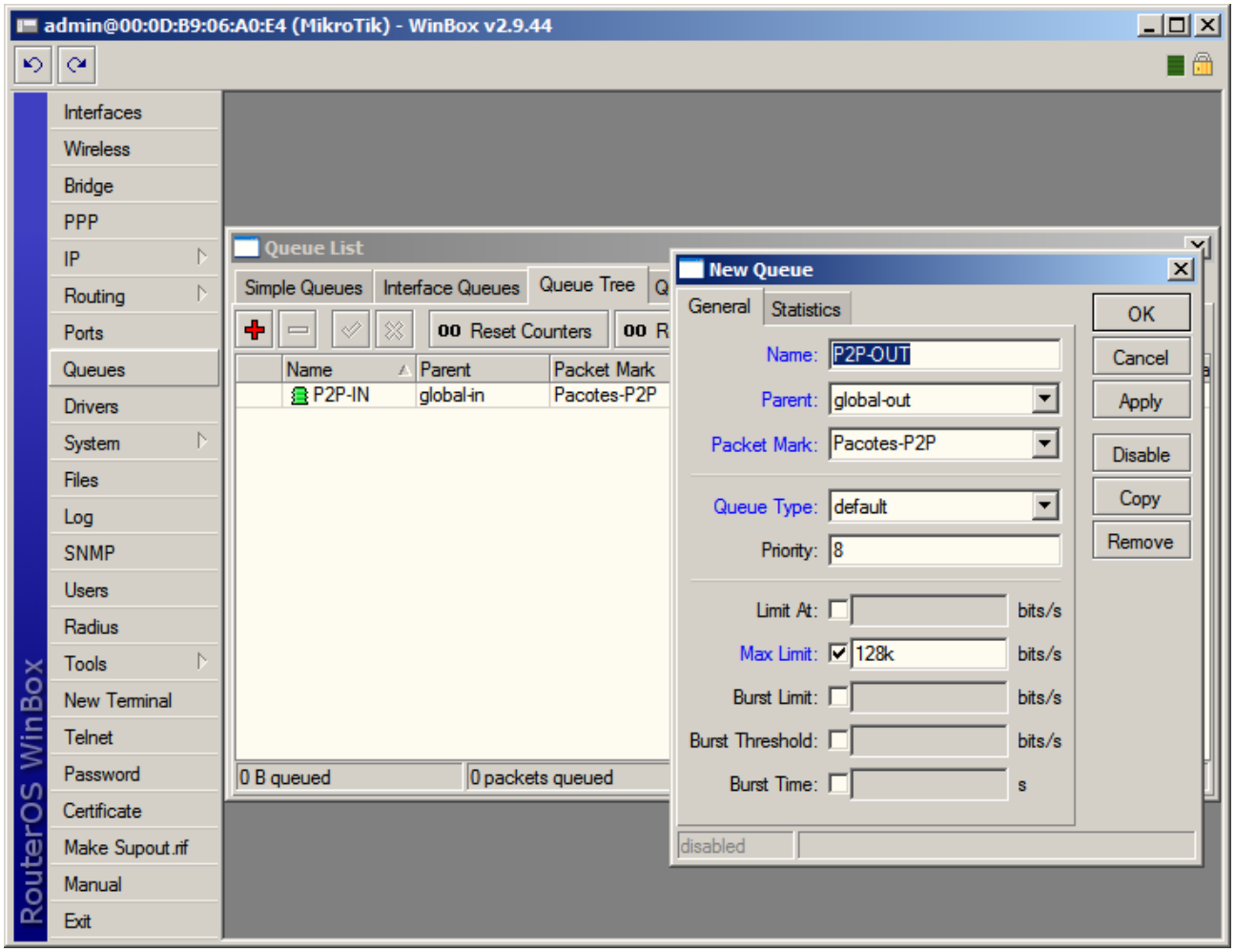


QUEUE

- Clique no menu “Queue”
- Clique na guia “Queue Tree”
- Clique em “Adicionar”
- Na guia “General”, na opção “Name”, digite um nome para a regra
- Na opção “Parent”, escolha a opção “global-in”
- Na opção “Packet Mark”, escolha a marcação dos pacotes criada anteriormente
- Na opção “Queue Type”, escolha a opção “default”
- Na opção “Priority”, permaneça com o número 8
- Na opção “Max Limit”, digite o limite máximo permitido (utilize “k” (minúsculo) ou “M” (maiúsculo) após sua opção)
- Clique no botão “OK”



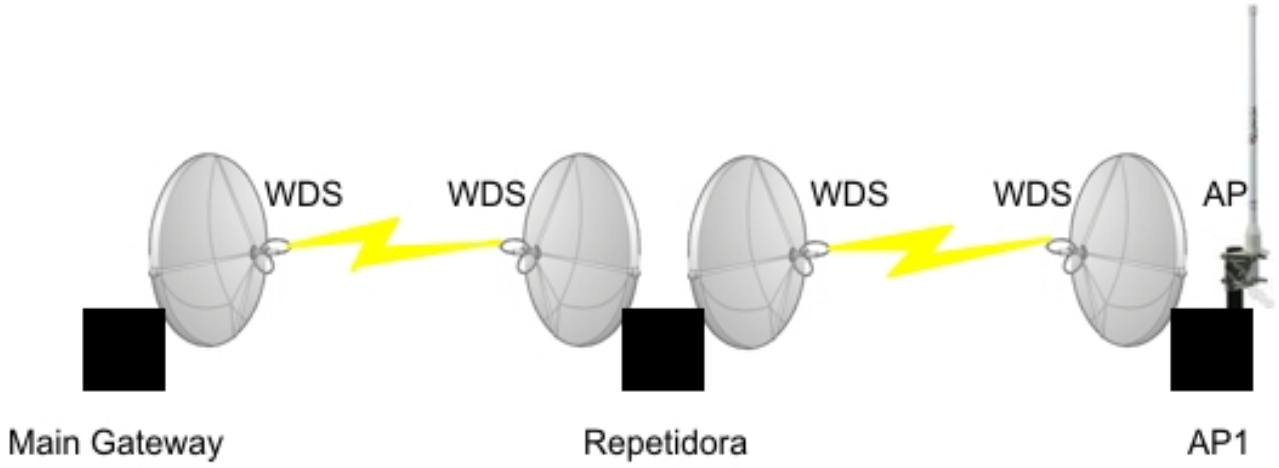
- Clique novamente em “Adicionar”
- Na guia “General”, na opção “Name”, digite um nome para a regra
- Na opção “Parent”, escolha a opção “global-out”
- Na opção “Packet Mark”, escolha a marcação dos pacotes criada anteriormente
- Na opção “Queue Type”, escolha a opção “default”
- Na opção “Priority”, permaneça com o número 8
- Na opção “Max Limit”, digite o limite máximo permitido (utilize “k” (minúsculo) ou “M” (maiúsculo) após sua opção)
- Clique no botão “OK”



REPETIDORA WIRELESS – UTILIZANDO WDS

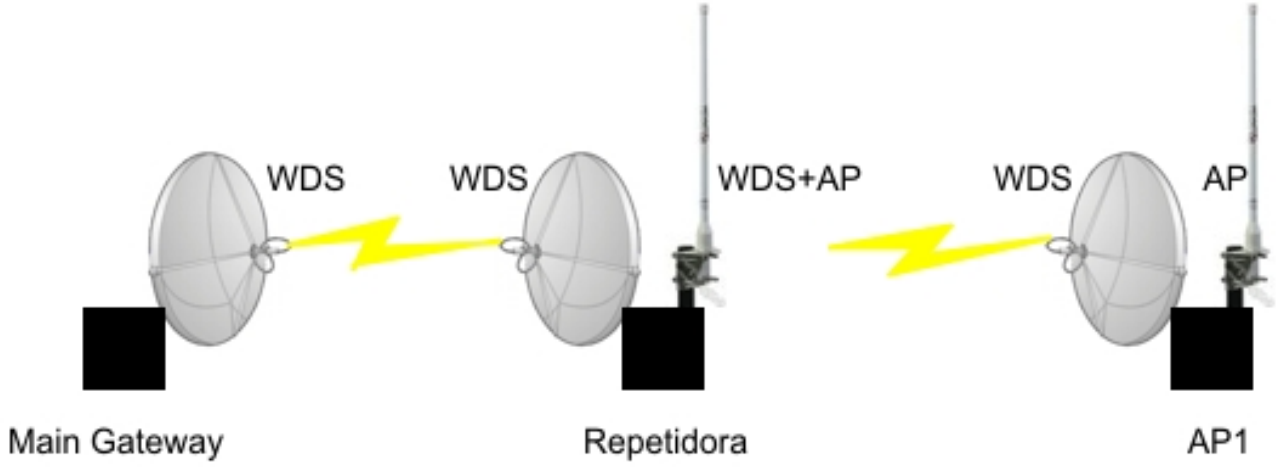
Este exemplo mostra como configurar um repetidor wireless. O repetidor wireless estende a escala de um WLAN existente em vez de adicionar mais pontos de acesso. Considere a disposição da rede:

CASO 1



Conforme imagem acima, usaremos duas interfaces wireless (duas antenas) no router repetidor. Os links WDS serão estabelecidos entre o 'Main gateway' e o 'repetidor ', e entre o 'repetidor' e o 'AP1' (os usuários finais são conectados na omni do AP1).

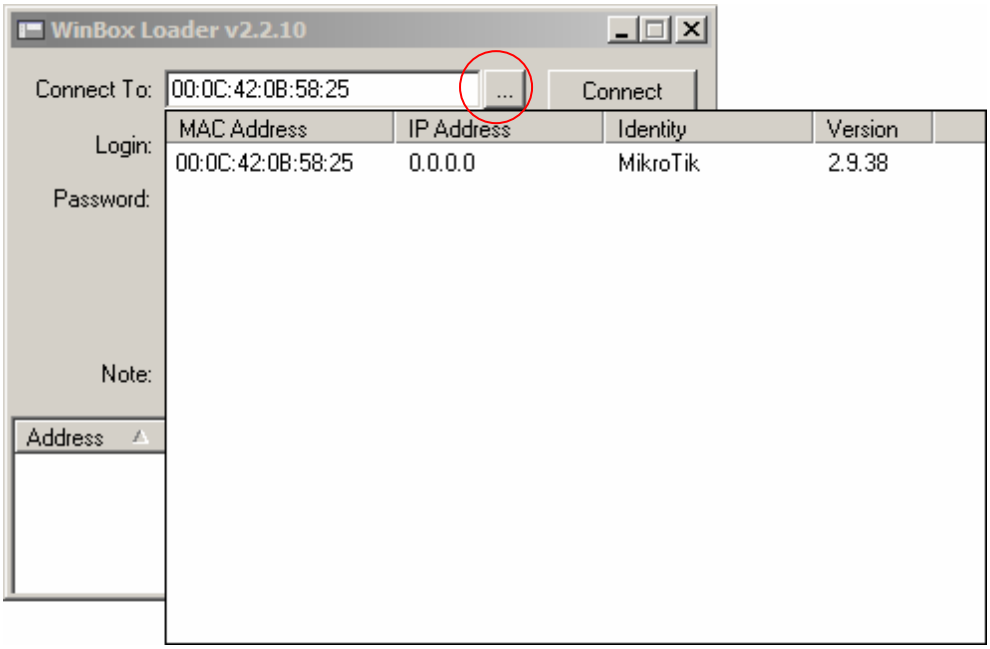
CASO 2



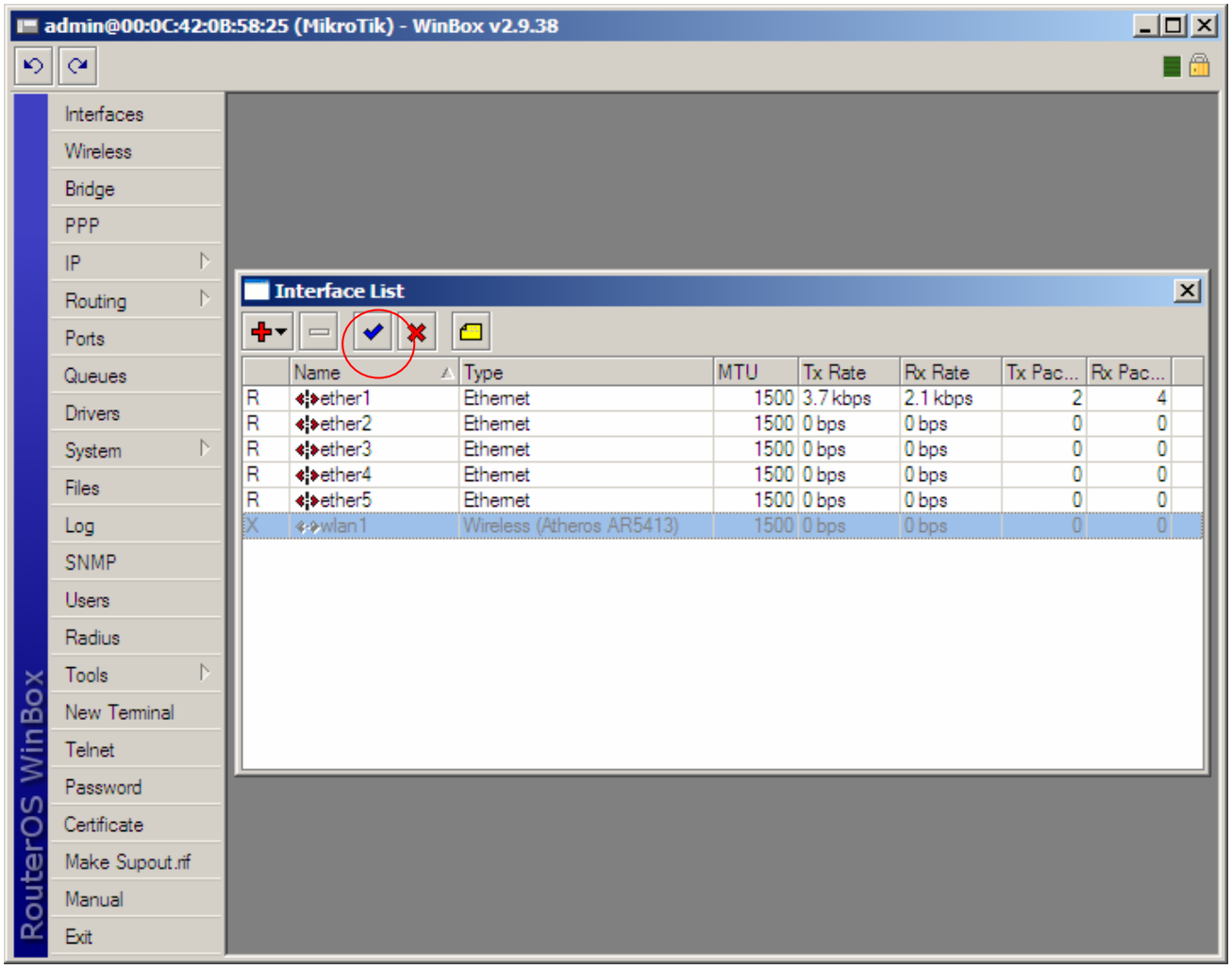
Conforme esta outra imagem, usaremos duas interfaces wireless (duas antenas) no router repetidor. Os links WDS serão estabelecidos entre o 'Main gateway' e o 'repetidor ', e entre o 'repetidor' e o 'AP1', sendo que os usuários finais poderão se conectar na antena omni da repetidora e na antena omni do AP1.

Configuração do Equipamento 1 - Main Gateway

- Acesse o RouterOS “Main Gateway” através do Winbox



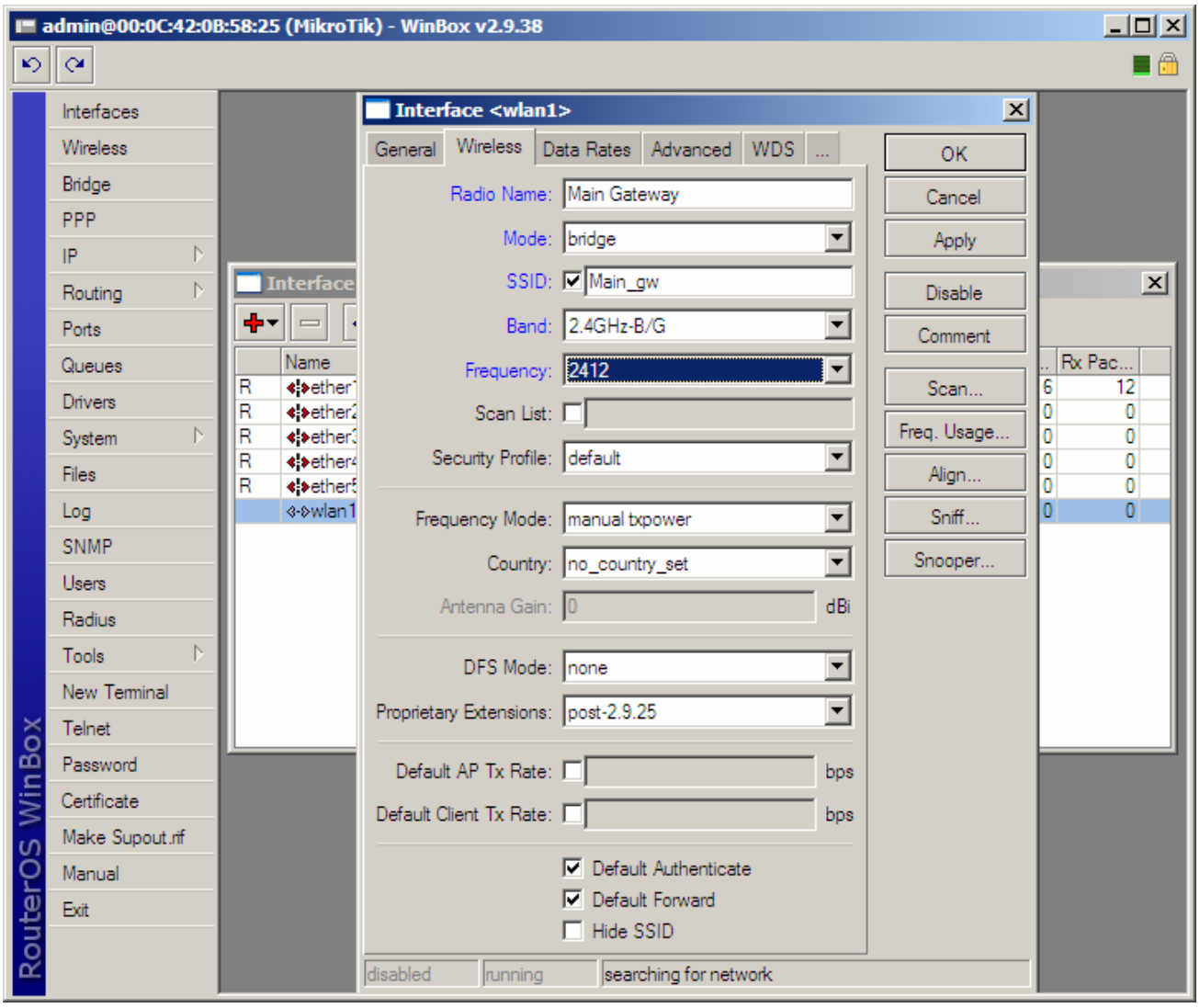
- Clique no menu Interface
- Habilite a interface wireless



Configure a interface wireless, dando um clique duplo nela
- Clique na guia Wireless
- Em Radio Name, digite um nome para identificação da interface;
- Em Mode, escolha a opção bridge;
- Em SSID, digite um nome para identificação da interface na Rede;
- Em Band, escolha a banda desejada, em nosso caso: 2.4Ghz-B/G (deverá ser a mesma banda escolhida na outra ponta do enlace);
- Em Frequency, escolha o canal que melhor lhe convier (deverá ser o mesmo canal escolhido na outra ponta do enlace).

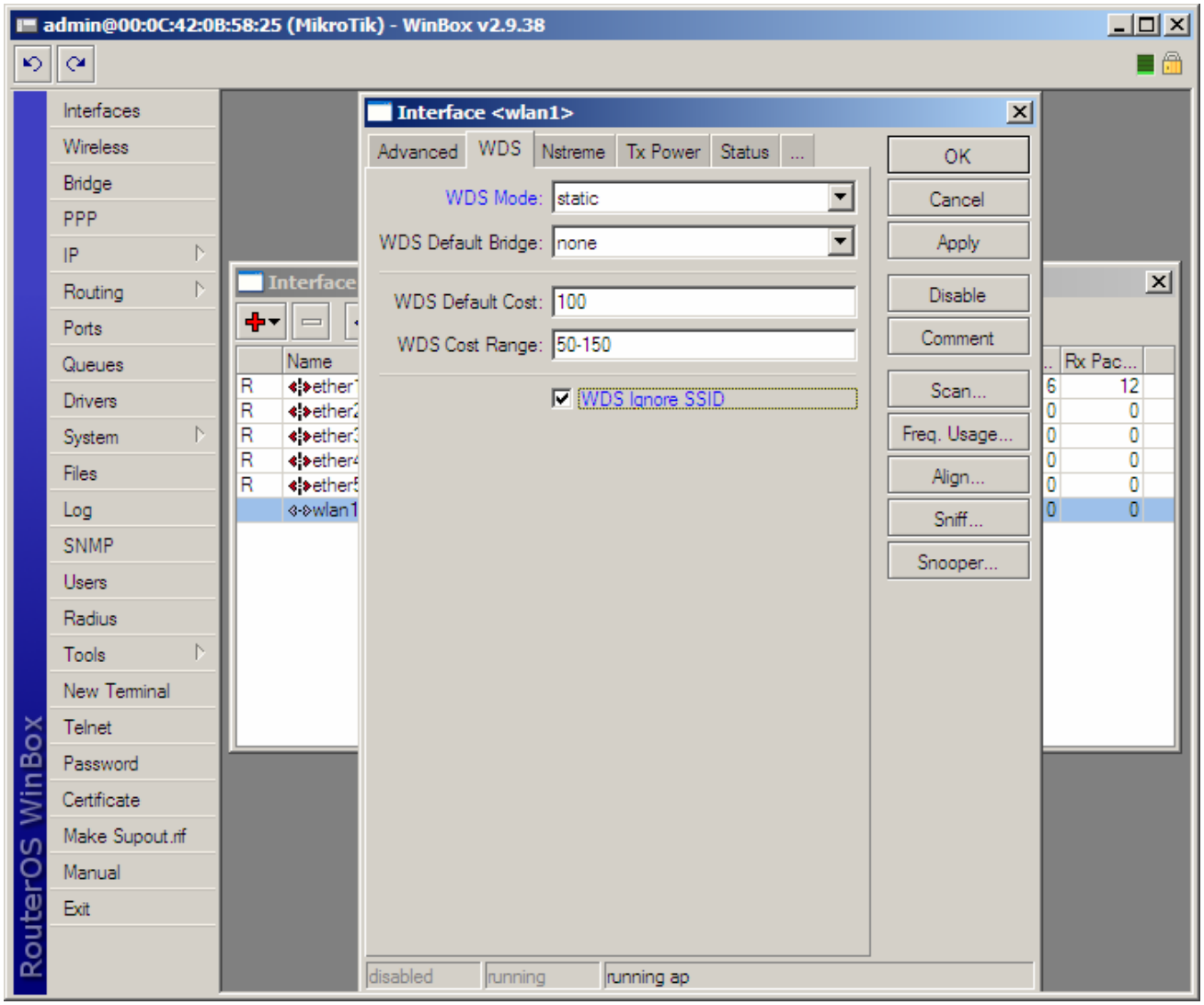
Observação importante: As disposições dos canais são importantes para que haja o mínimo de interferência possível. Utilize:

- Enlace 1 = Canal 1
- Enlace 2 – Canal 6
- Enlace 3 = Canal 11



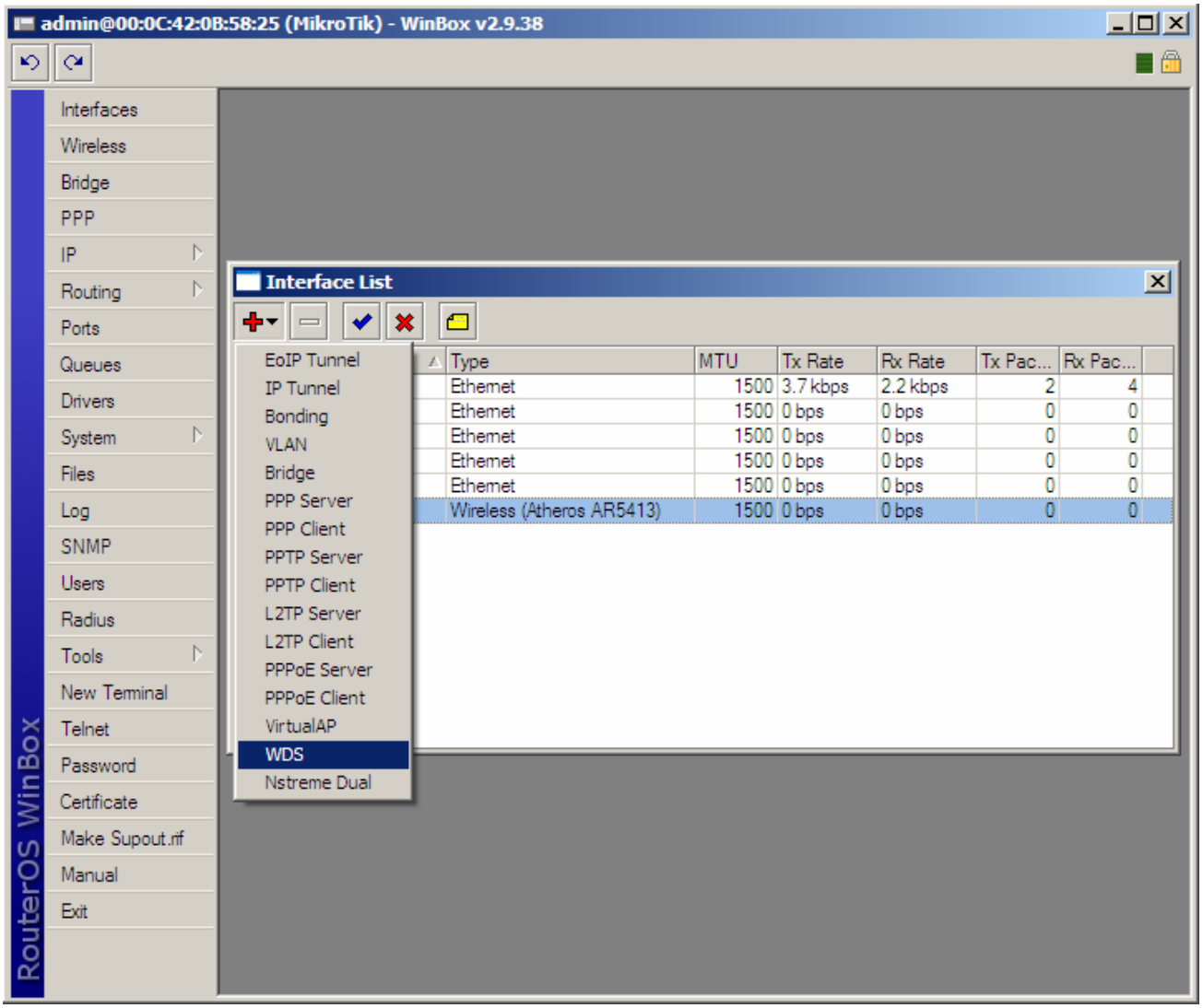
- Clique no botão OK

- Clique na guia WDS
- Em WDS Mode, escolha a opção static
- Ative a opção WDS Ignore SSID

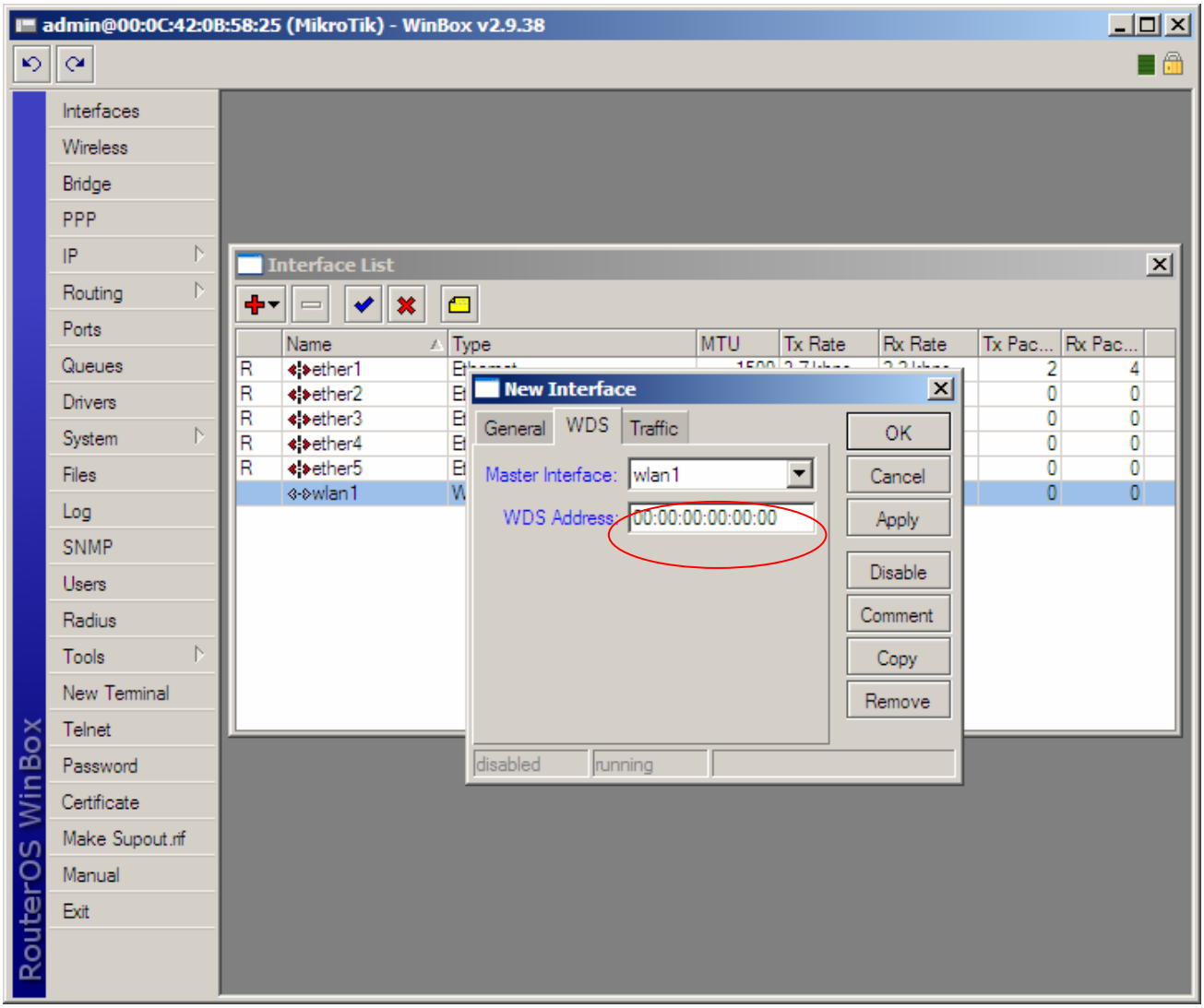


- Clique no botão OK

- Em Interface, clique em Adicionar
- Clique na opção WDS

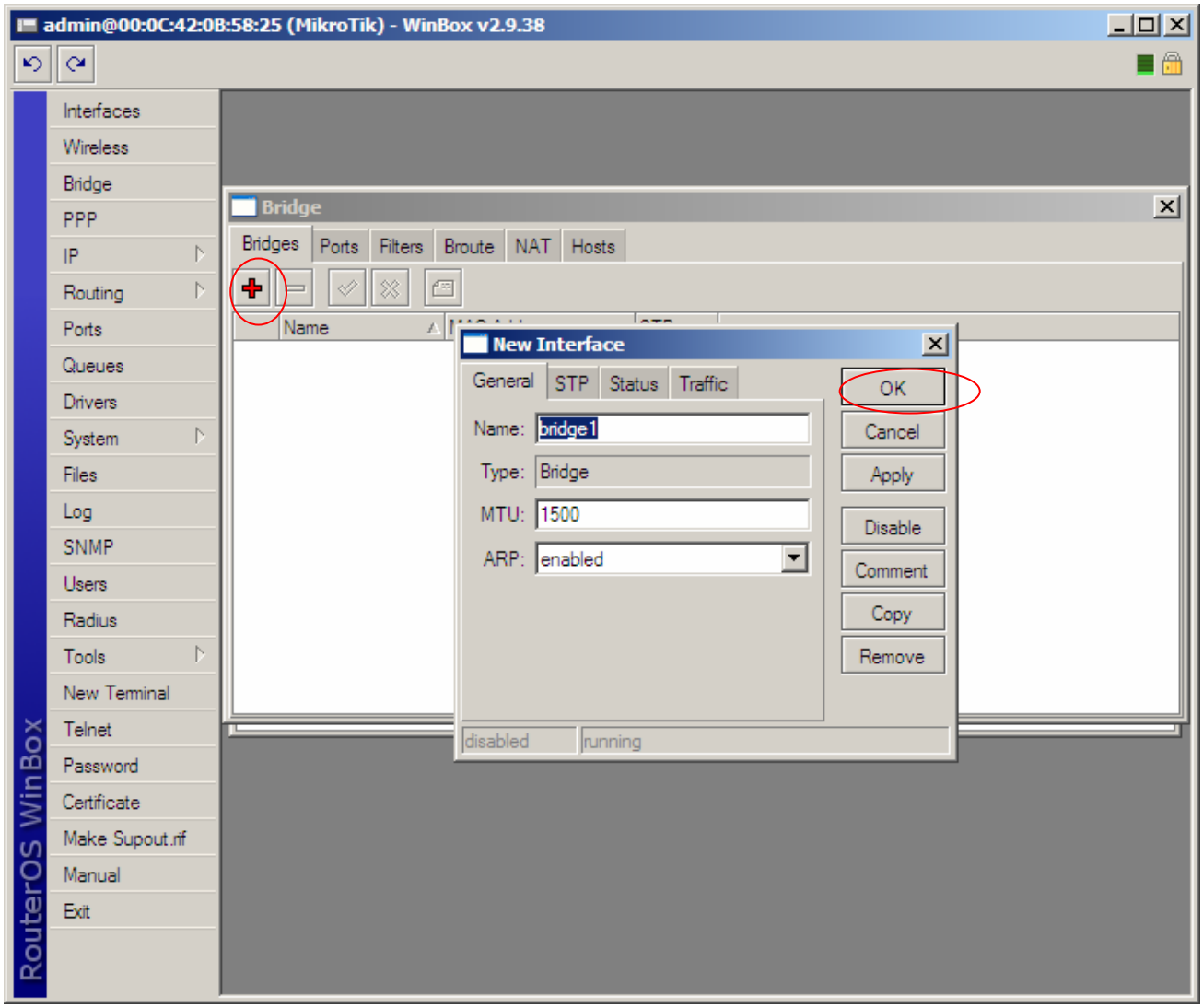


- Clique na guia WDS
- Em Master Interface, escolha a interface wlan1
- Em WDS Address, digite o MAC da interface wlan1 do Equipamento “Repetidora”



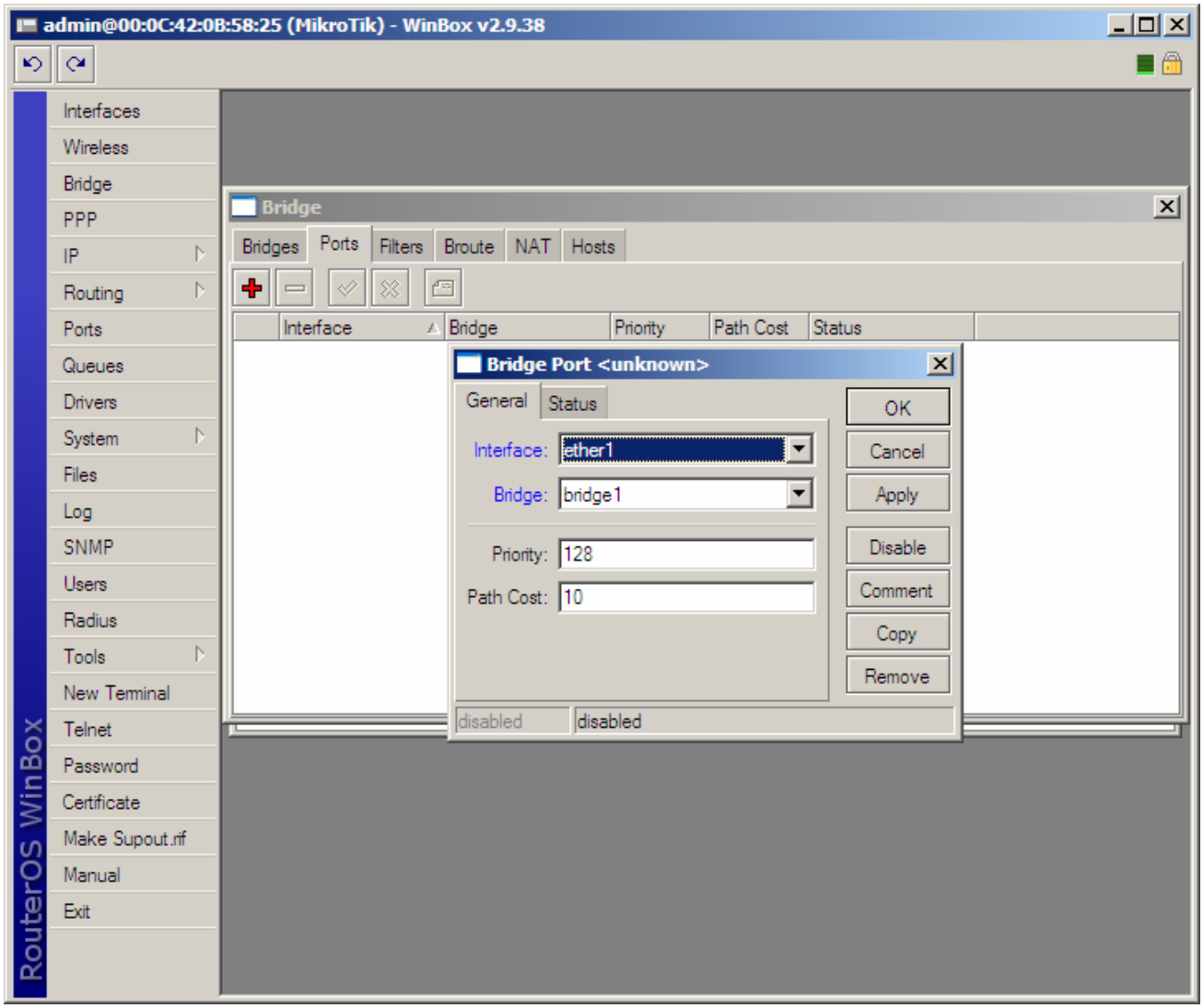
- Clique no botão OK

- Clique o Menu Bridge
- Clique em Adicionar



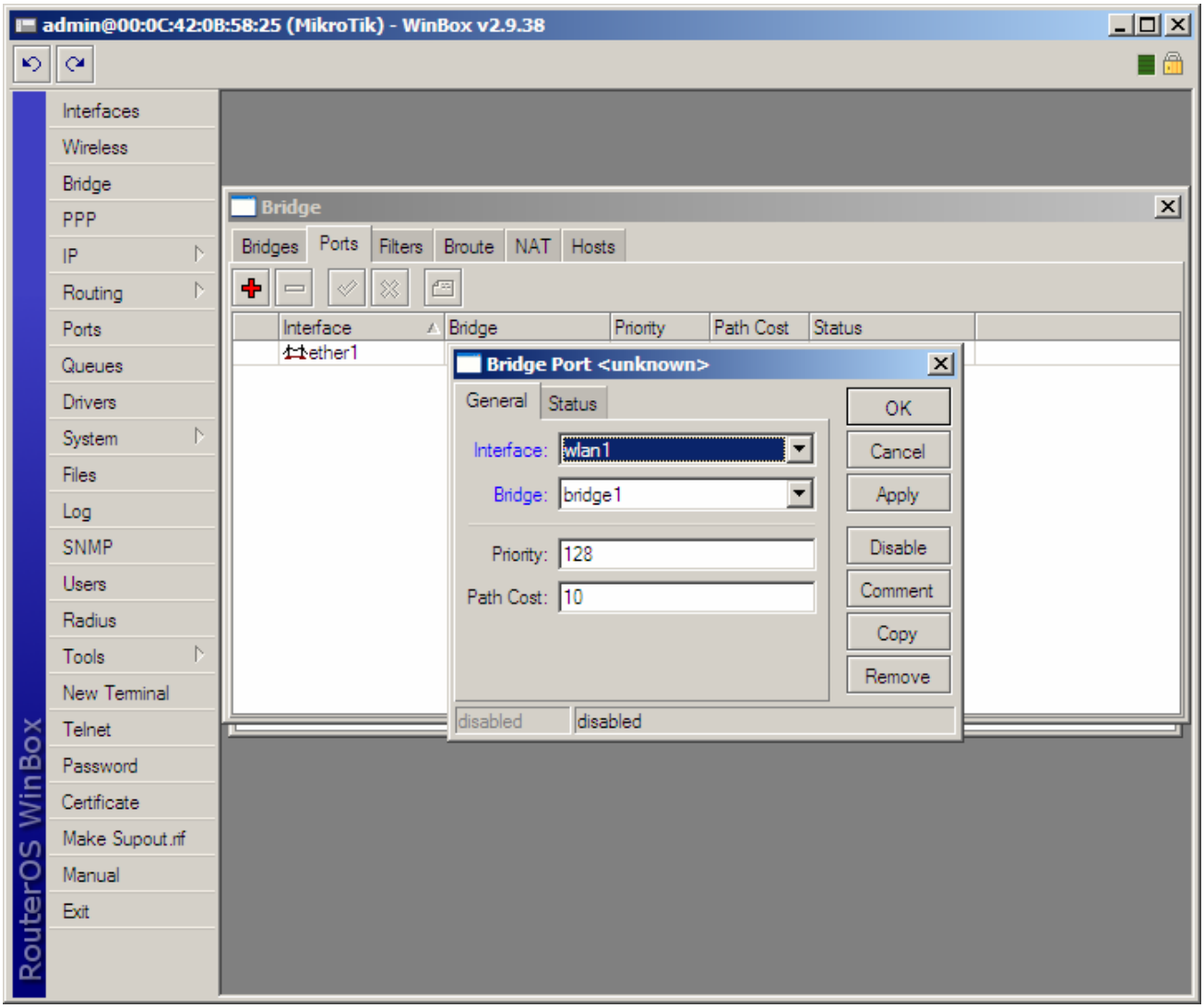
- Clique no botão OK

- Clique na guia Ports
- Clique em Adicionar
- Em Interface, escolha a opção ether1
- Em Bridge, escolha a opção bridge1



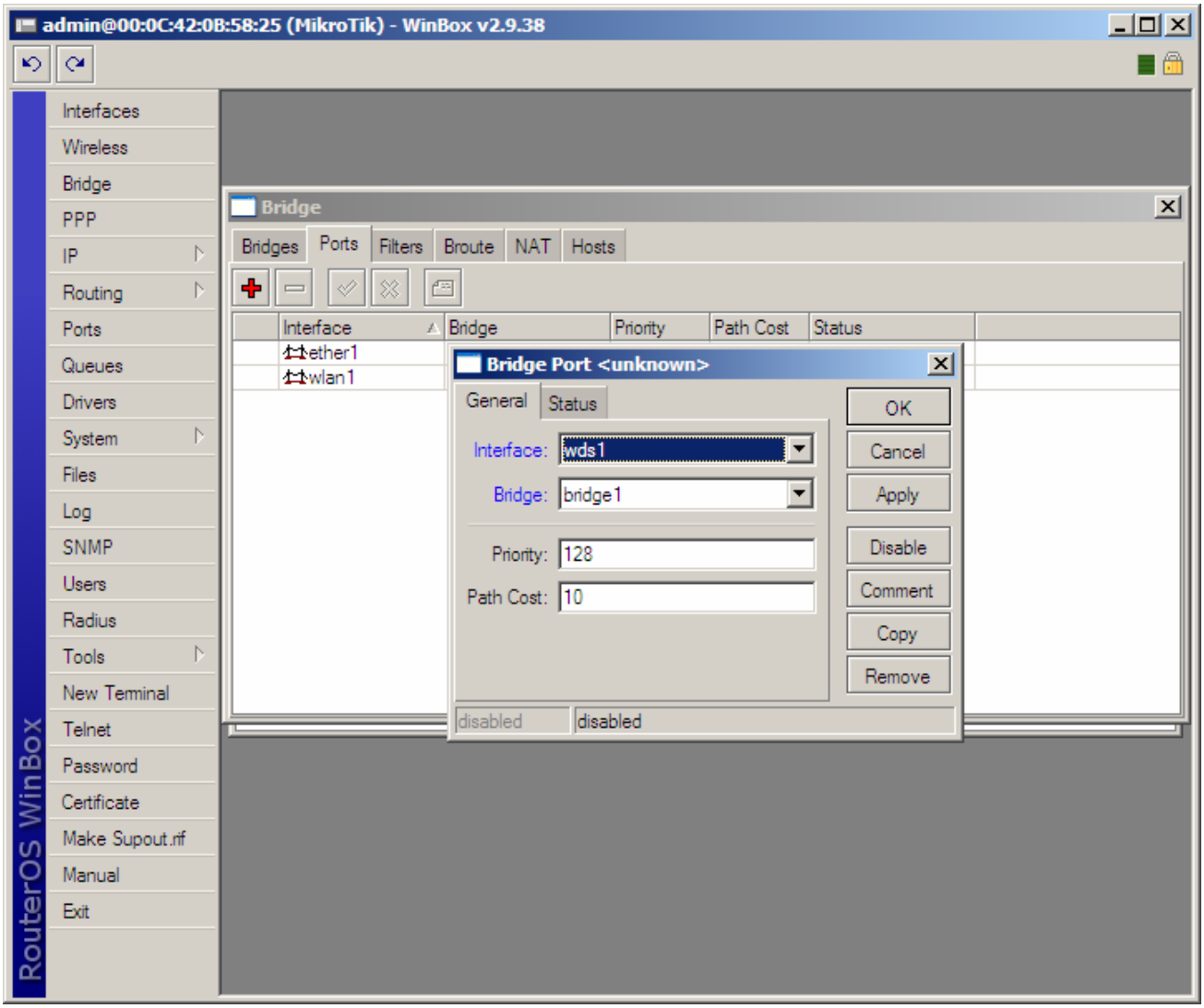
- Clique no botão OK

- Clique em Adicionar
- Em Interface, escolha a opção wlan1
- Em Bridge, escolha a opção bridge1



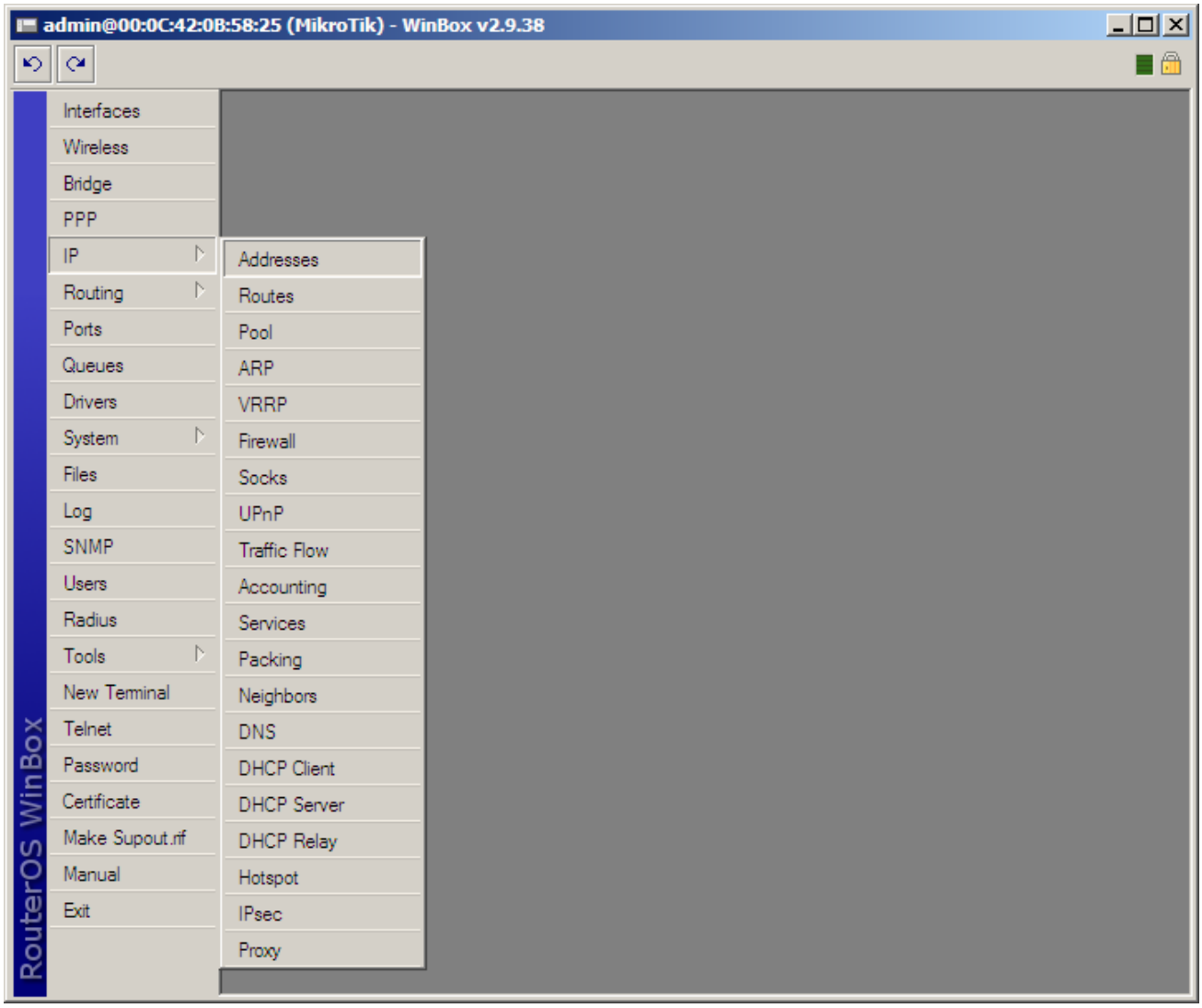
- Clique no botão OK

- Clique em Adicionar
- Em Interface, escolha a opção wds1
- Em Bridge, escolha a opção bridge1

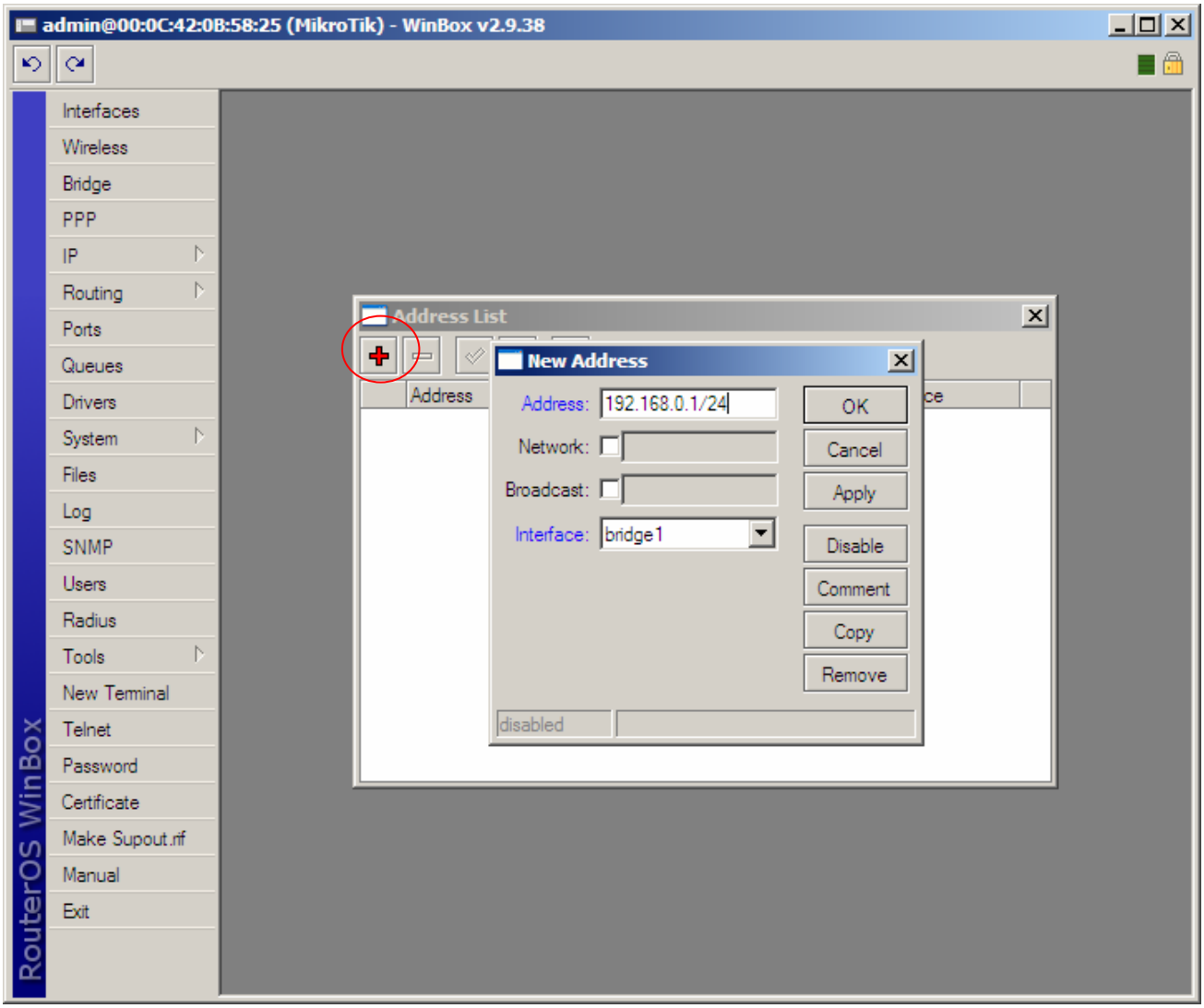


- Clique no botão OK

- Clique na guia IP, opção Address



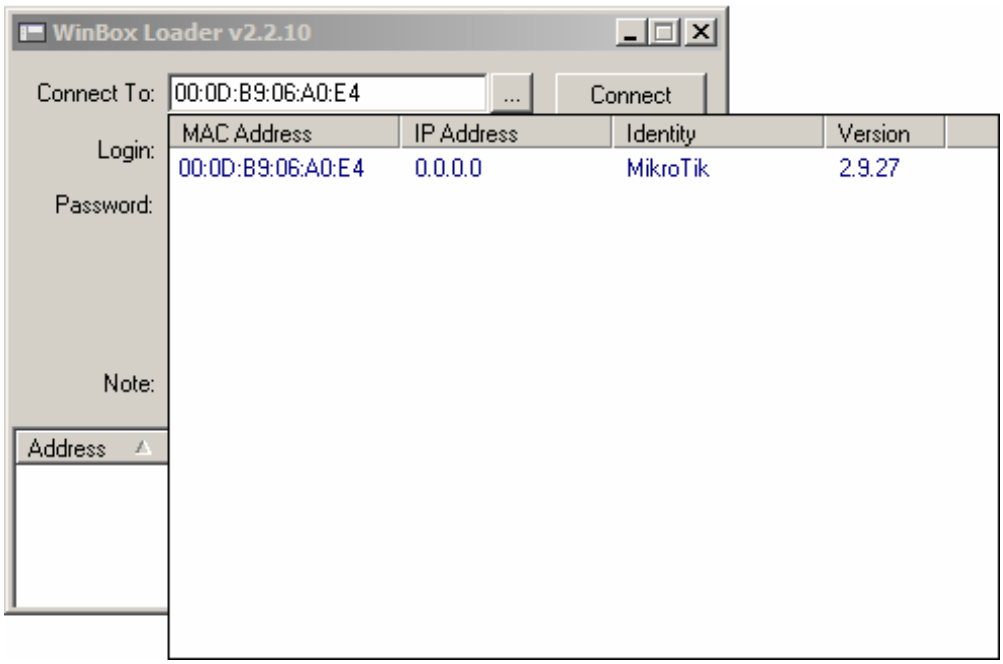
- Clique em Adicionar
- Em Address, digite um IP para o seu primeiro equipamento, em nosso caso: 192.168.0.1/24
- Em Interface, escolha a opção bridge1



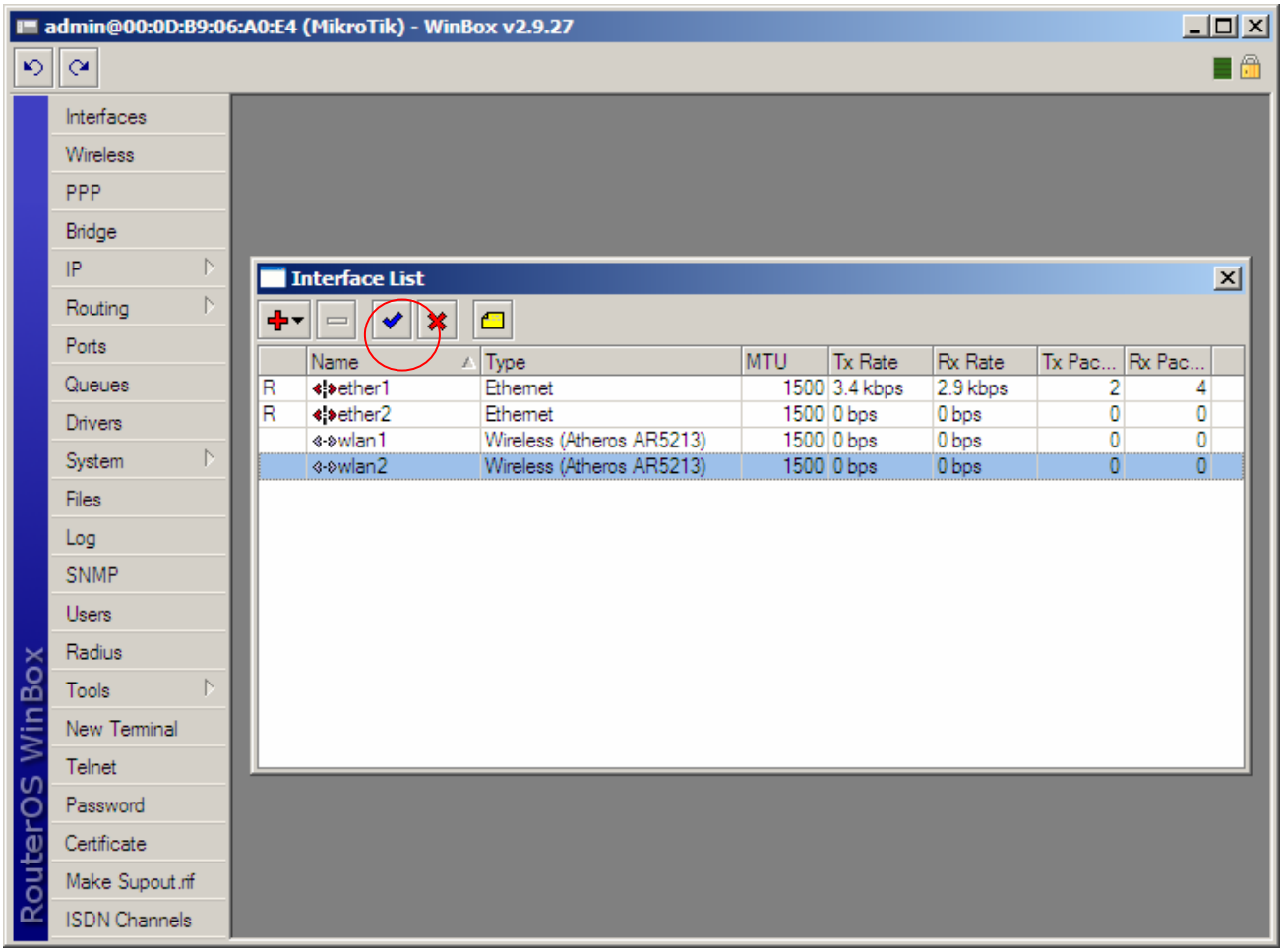
- Clique no botão OK

Configuração do Equipamento 2 - Repetidora

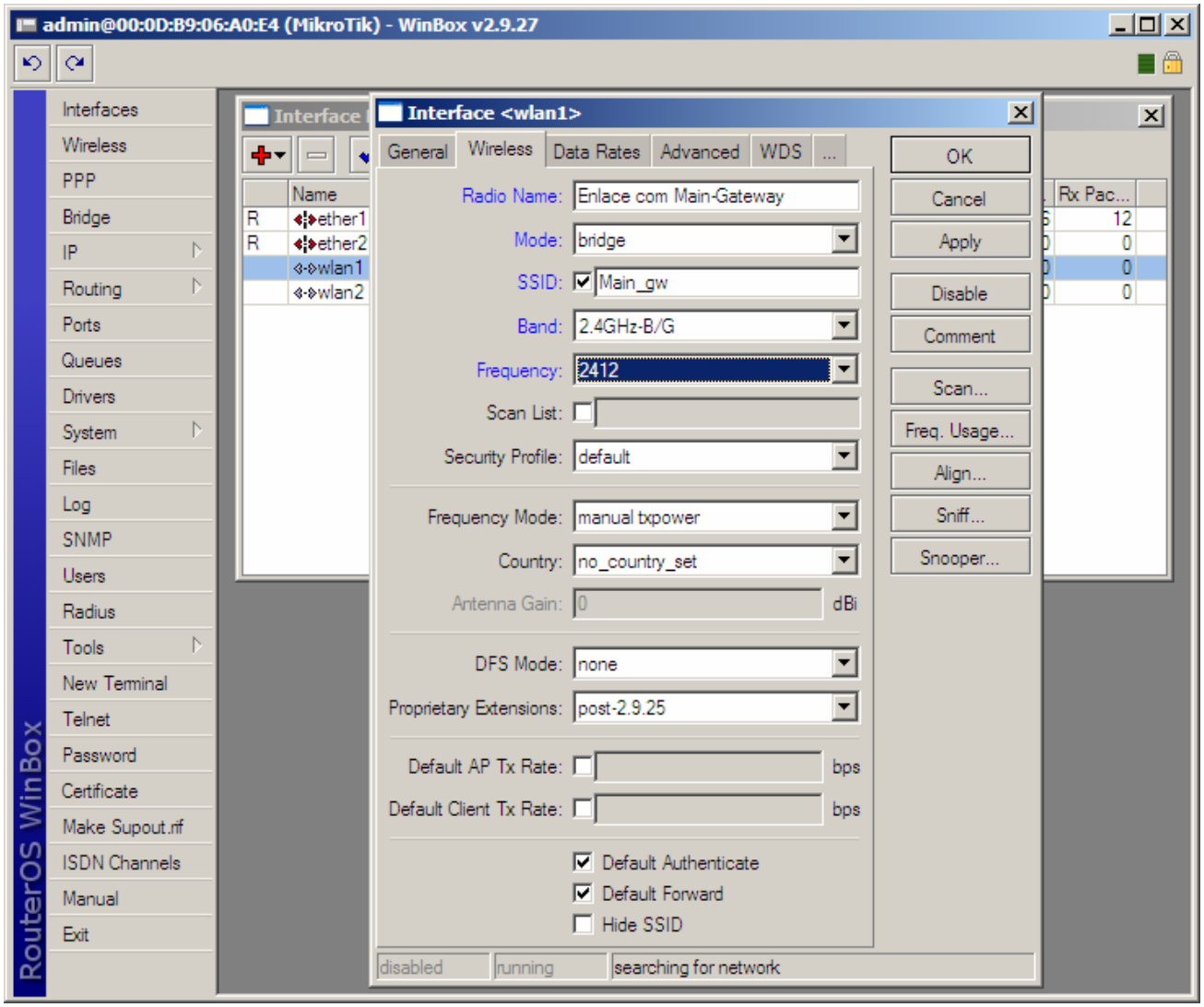
Acesse o RouterOS “Repetidora” através do Winbox



- Clique no menu Interface
- Habilite a interface wireless

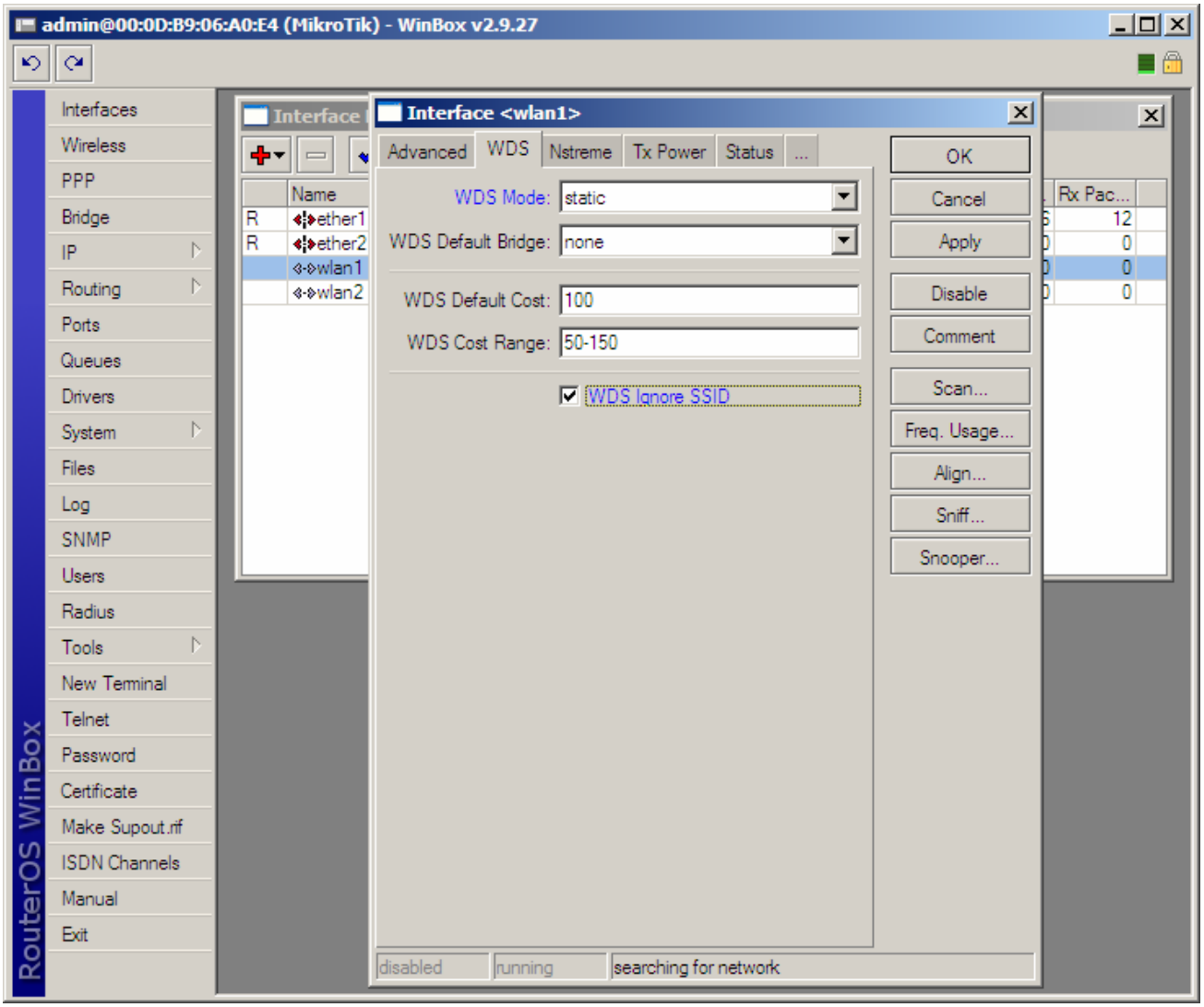


Configure a interface wireless wlan1, dando um clique duplo nela
- Clique na guia Wireless
- Em Radio Name, digite um nome para identificação da interface;
- Em Mode, escolha a opção bridge;
- Em SSID, digite um nome para identificação da interface na Rede;
- Em Band, escolha a banda desejada, em nosso caso: 2.4Ghz-B/G (a mesma banda escolhida na interface do Equipamento Main Gateway);
- Em Frequency, escolha o canal que melhor lhe convier (o mesmo canal escolhido na interface do Equipamento Main Gateway).



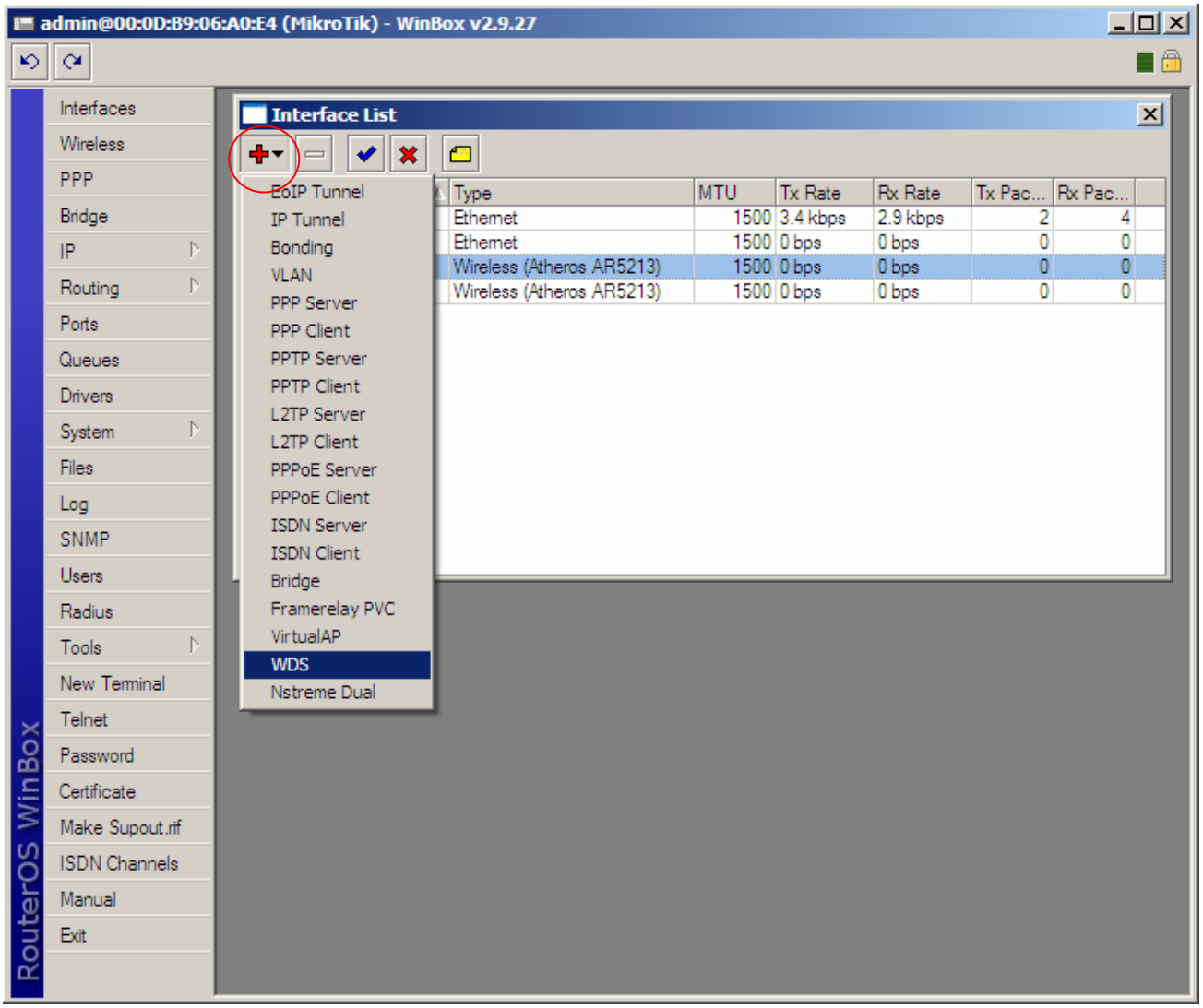
- Clique no botão OK

- Clique na guia WDS
- Em WDS Mode, escolha a opção static
- Ative a opção WDS Ignore SSID

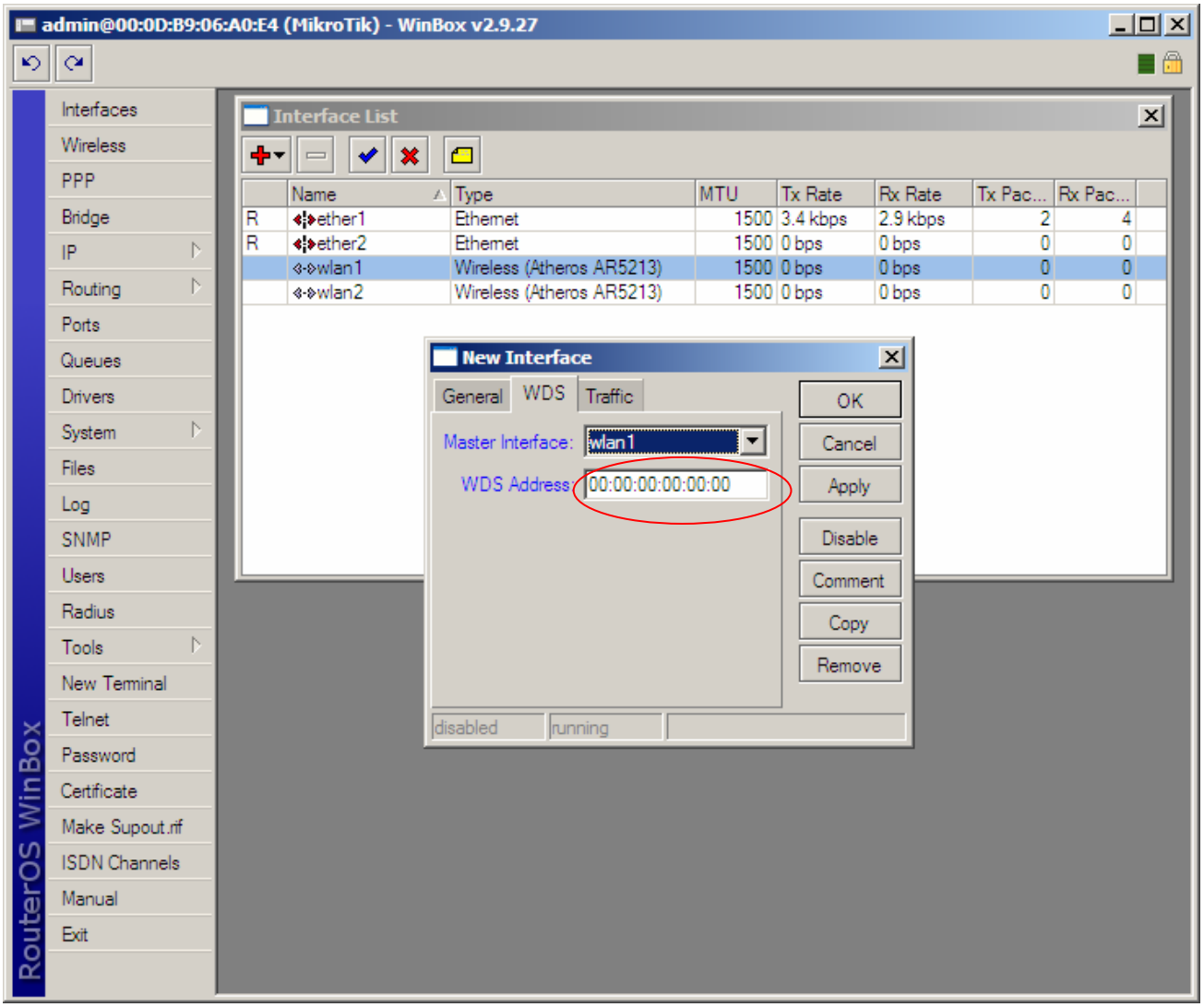


- Clique no botão OK

- Em Interface, clique em Adicionar
- Clique na opção WDS



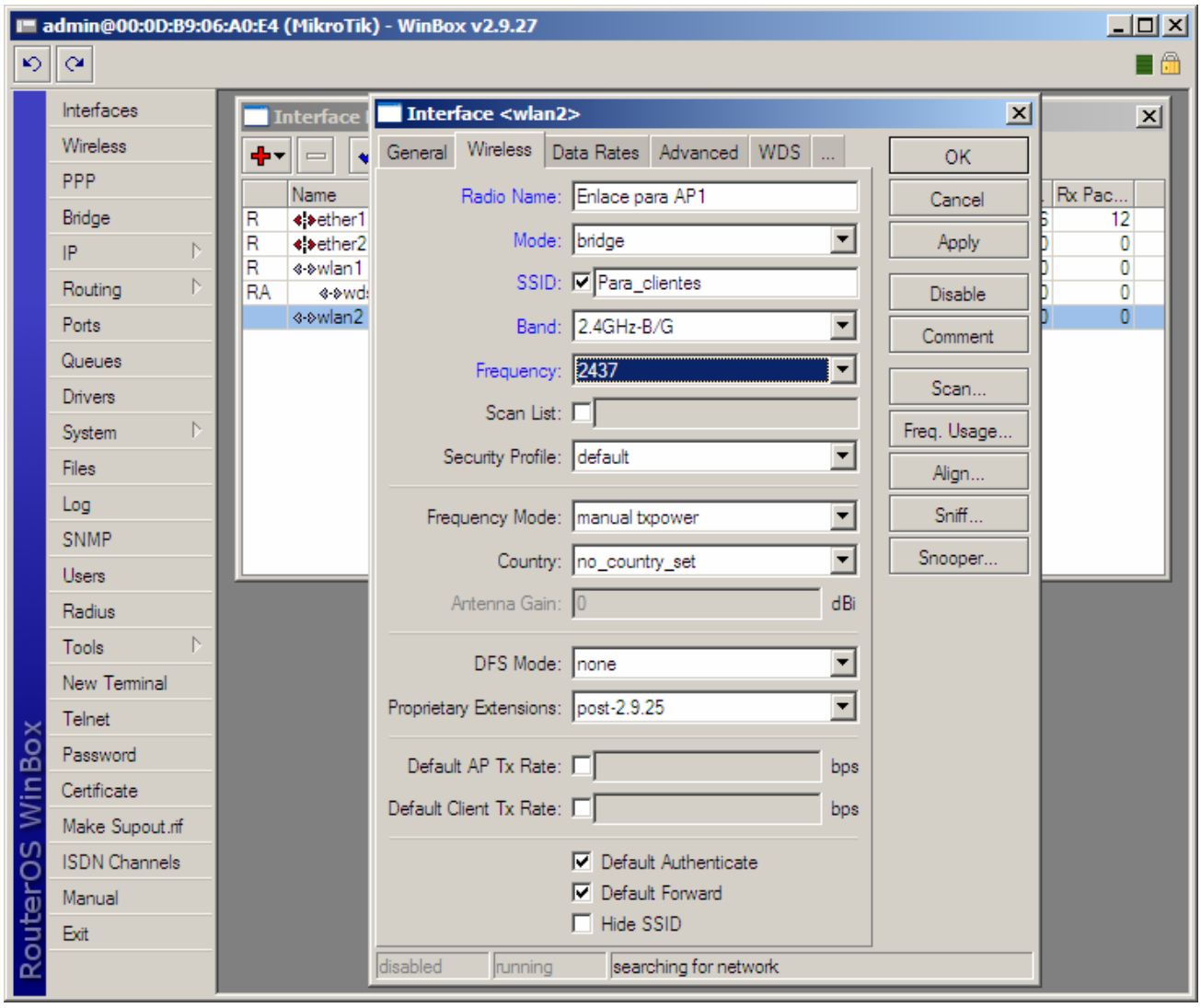
- Clique na guia WDS
- Em Master Interface, escolha a interface wlan1
- Em WDS Address, digite o MAC da interface wlan1 do Equipamento “Main Gateway”



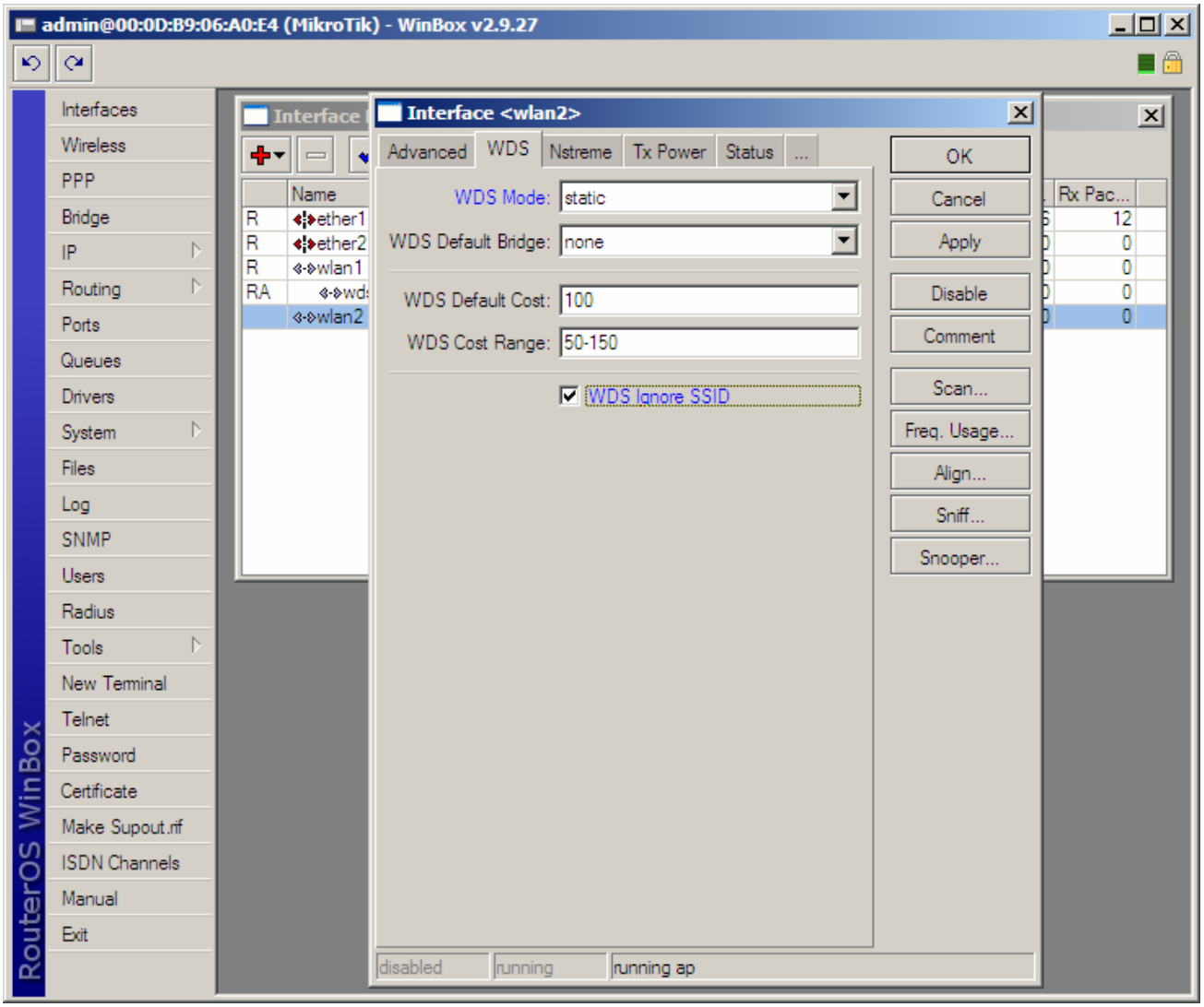
- Clique no botão OK

Configure a interface wireless wlan2, dando um clique duplo nela no menu Interface.
- Clique na guia Wireless
- Em Radio Name, digite um nome para identificação da interface;
- Em Mode, escolha a opção bridge;
- Em SSID, digite um nome para identificação da interface na Rede;
- Em Band, escolha a banda desejada, em nosso caso: 2.4Ghz-B/G (a mesma banda escolhida na interface do Equipamento AP1);
- Em Frequency, escolha o canal que melhor lhe convier (o mesmo canal escolhido na interface do Equipamento AP1).
- Clique no botão OK

Para permitir que usuários finais se conectem a esta interface (utilizando antena omni ou setorial, por exemplo, de acordo com o CASO 2 no início deste manual) em Mode, escolha a opção “ap-bridge”.

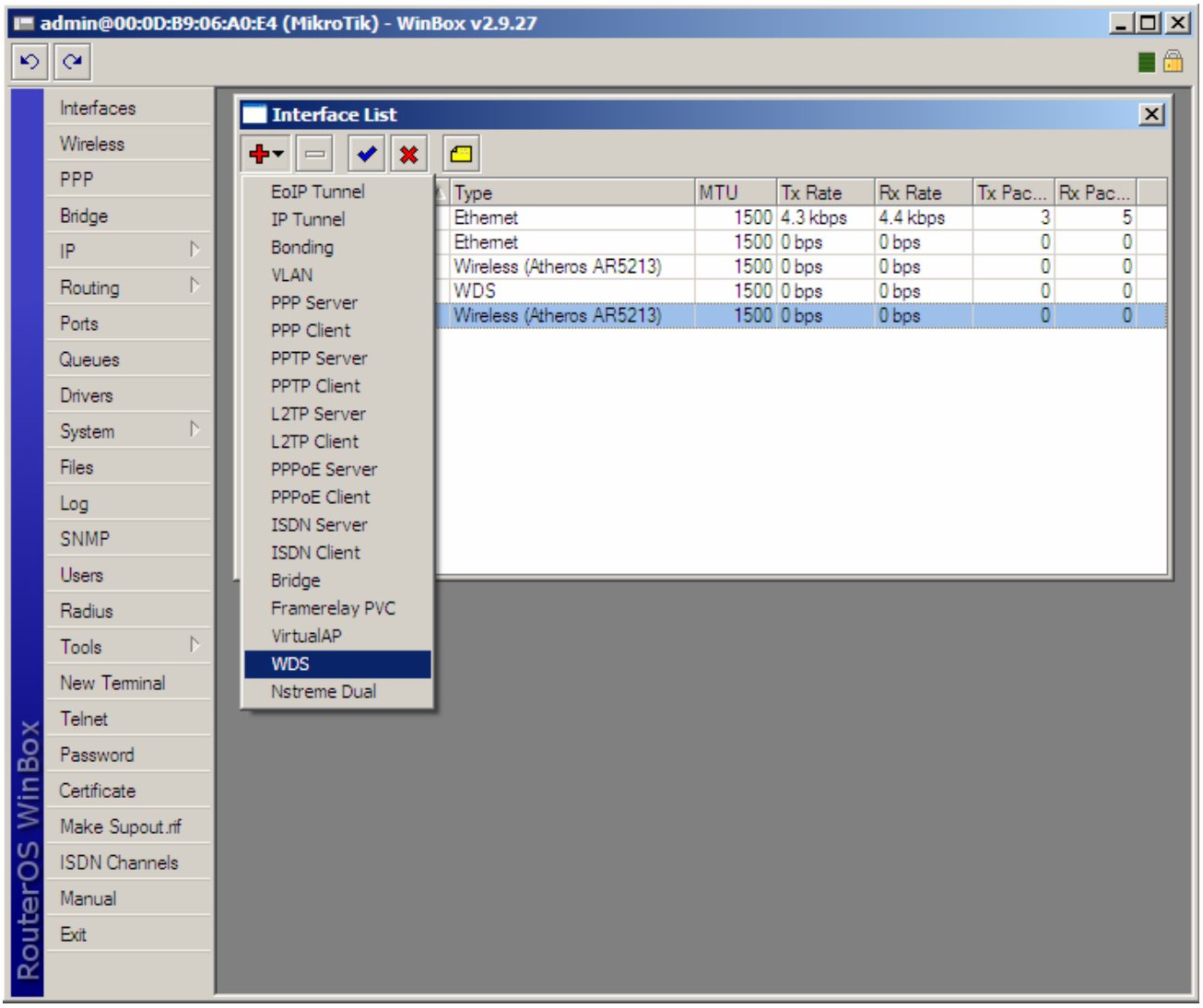


- Clique na guia WDS
- Em WDS Mode, escolha a opção static
- Ative a opção WDS Ignore SSID

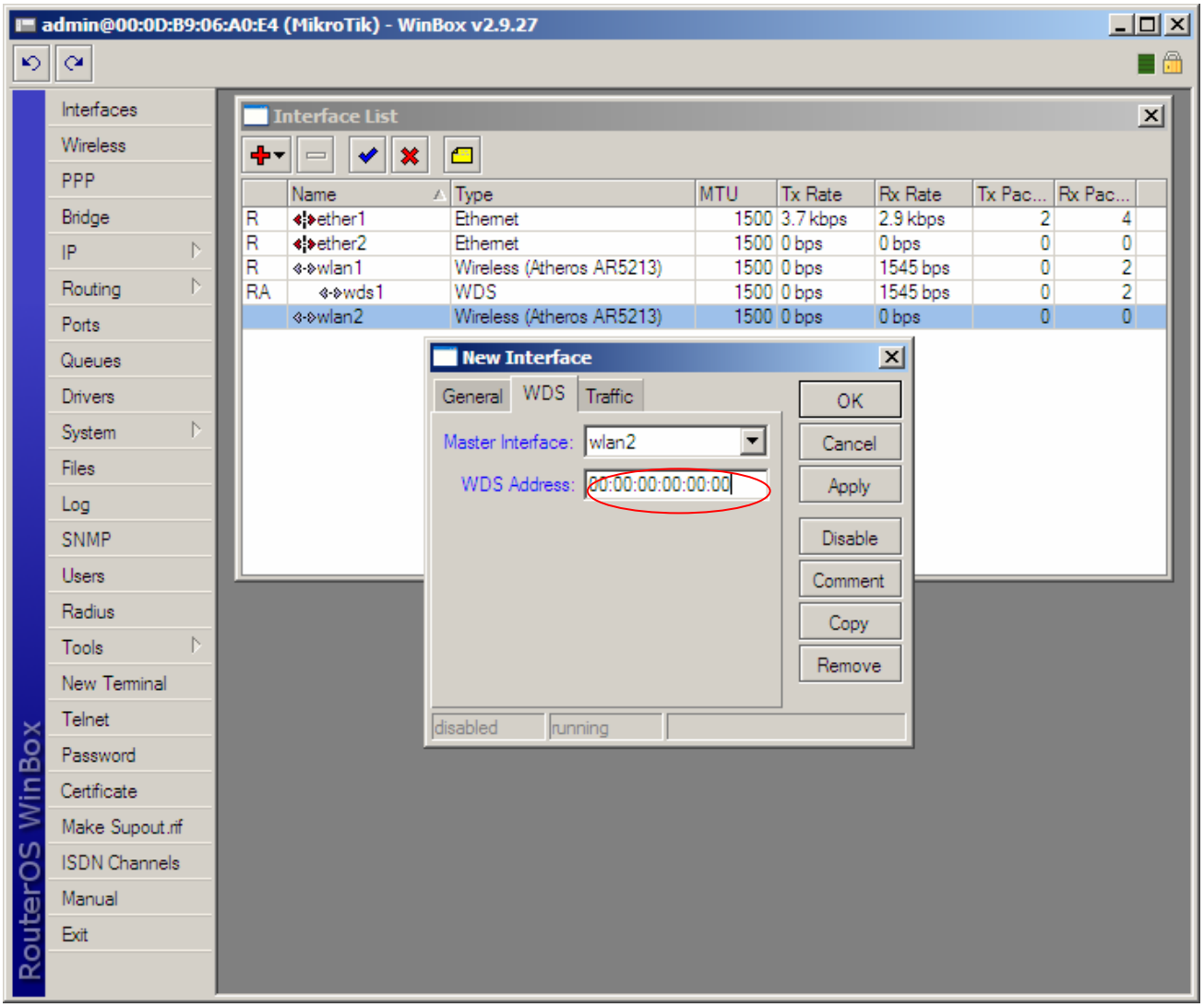


- Clique no botão OK

- Em Interface, clique em Adicionar
- Clique na opção WDS

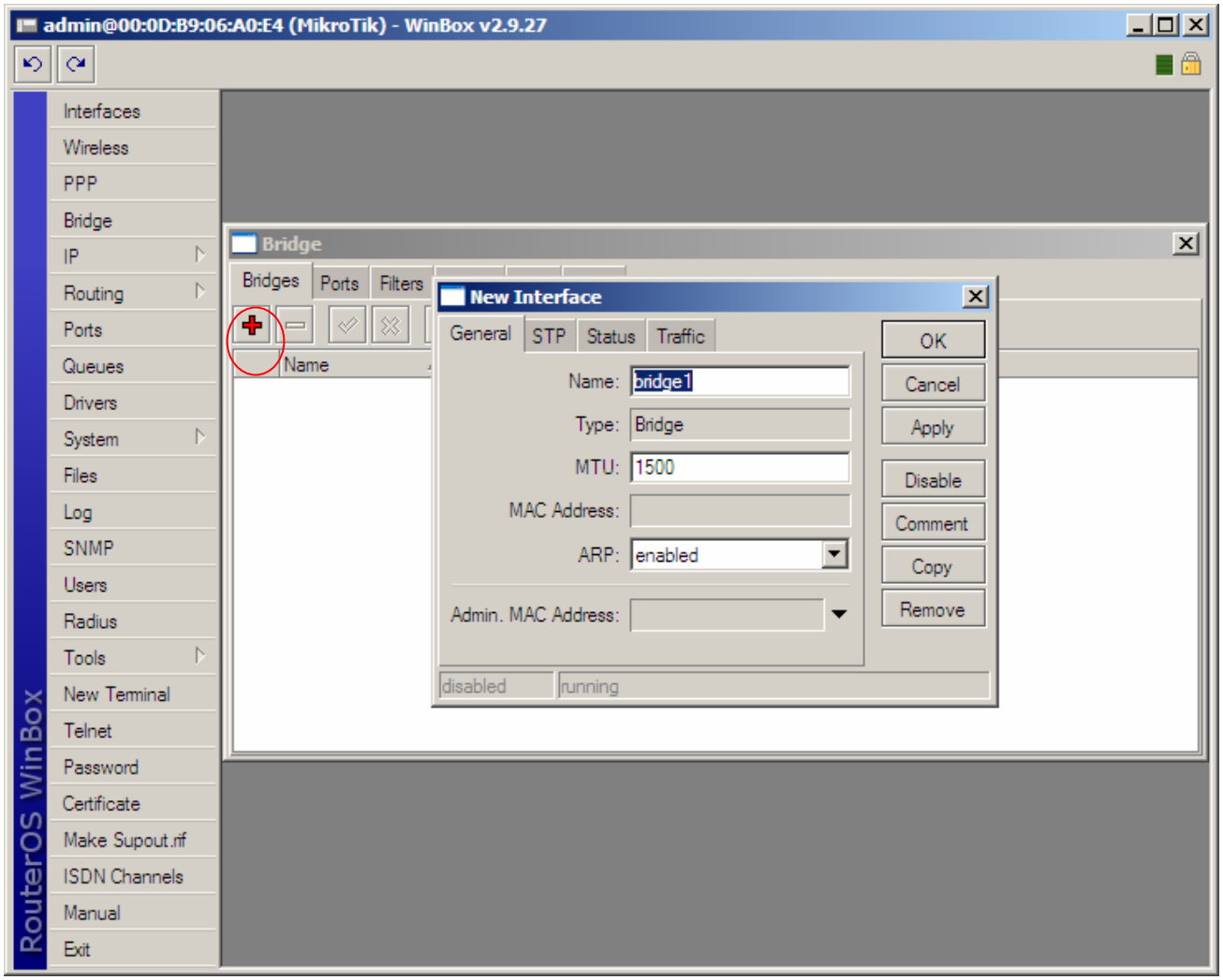


- Clique na guia WDS
- Em Master Interface, escolha a interface wlan1
- Em WDS Address, digite o MAC da interface wlan1 do Equipamento “AP1”



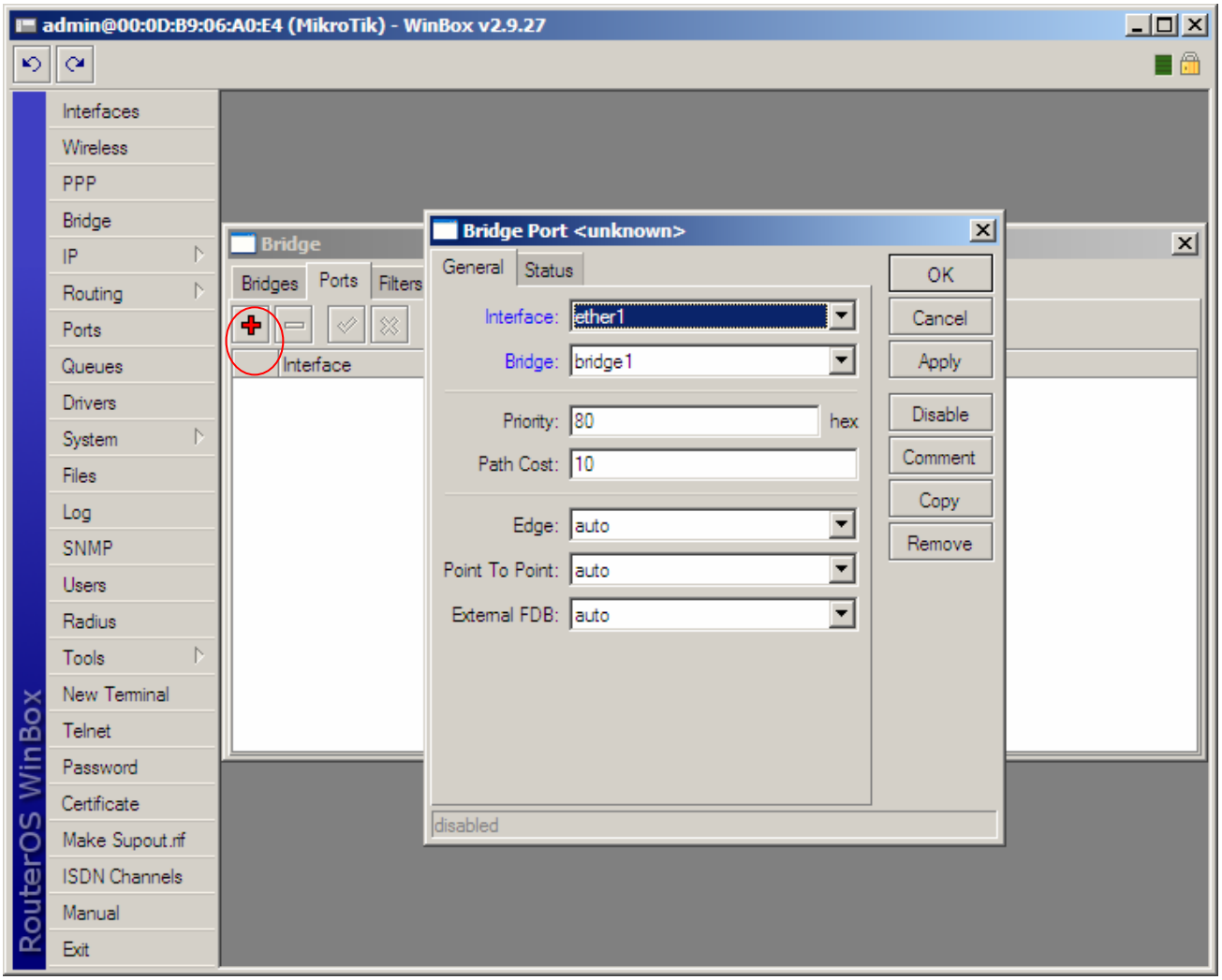
- Clique no botão OK

- Clique o Menu Bridge
- Clique em Adicionar



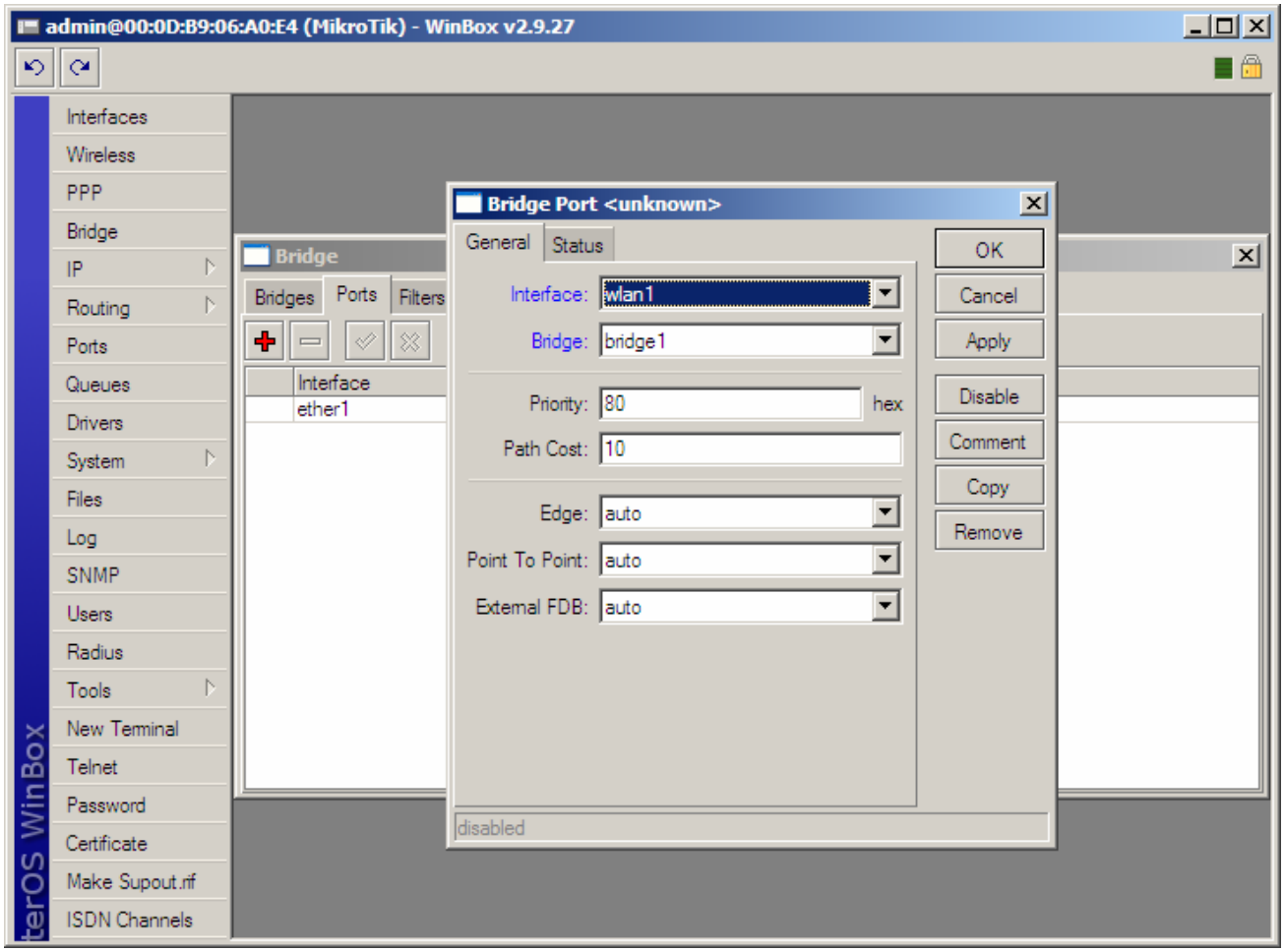
- Clique no botão OK

- Clique na guia Ports
- Clique em Adicionar
- Em Interface, escolha a opção ether1
- Em Bridge, escolha a opção bridge1



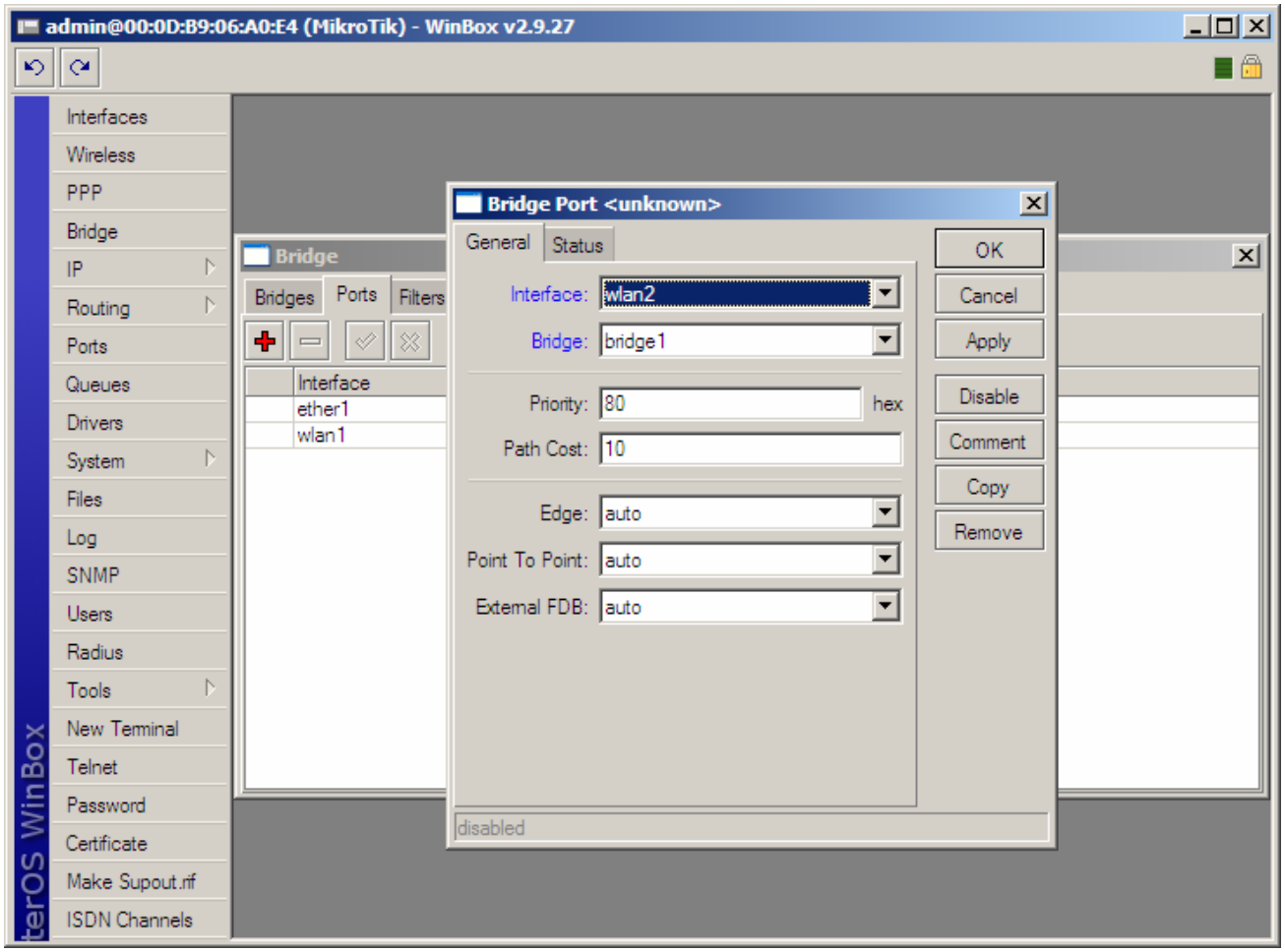
- Clique no botão OK

- Clique em Adicionar
- Em Interface, escolha a opção wlan1
- Em Bridge, escolha a opção bridge1



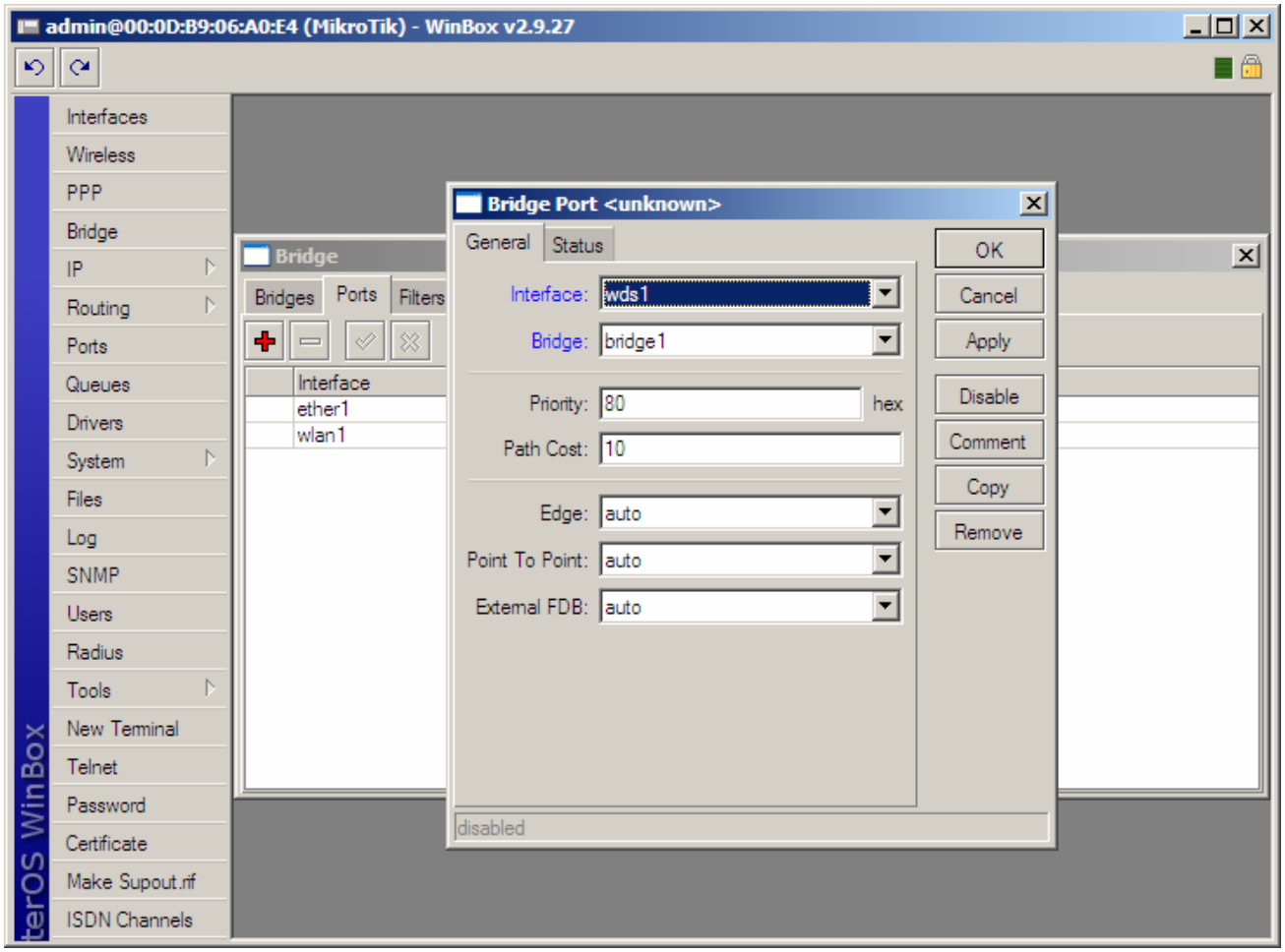
- Clique no botão OK

- Clique em Adicionar
- Em Interface, escolha a opção wlan2
- Em Bridge, escolha a opção bridge1



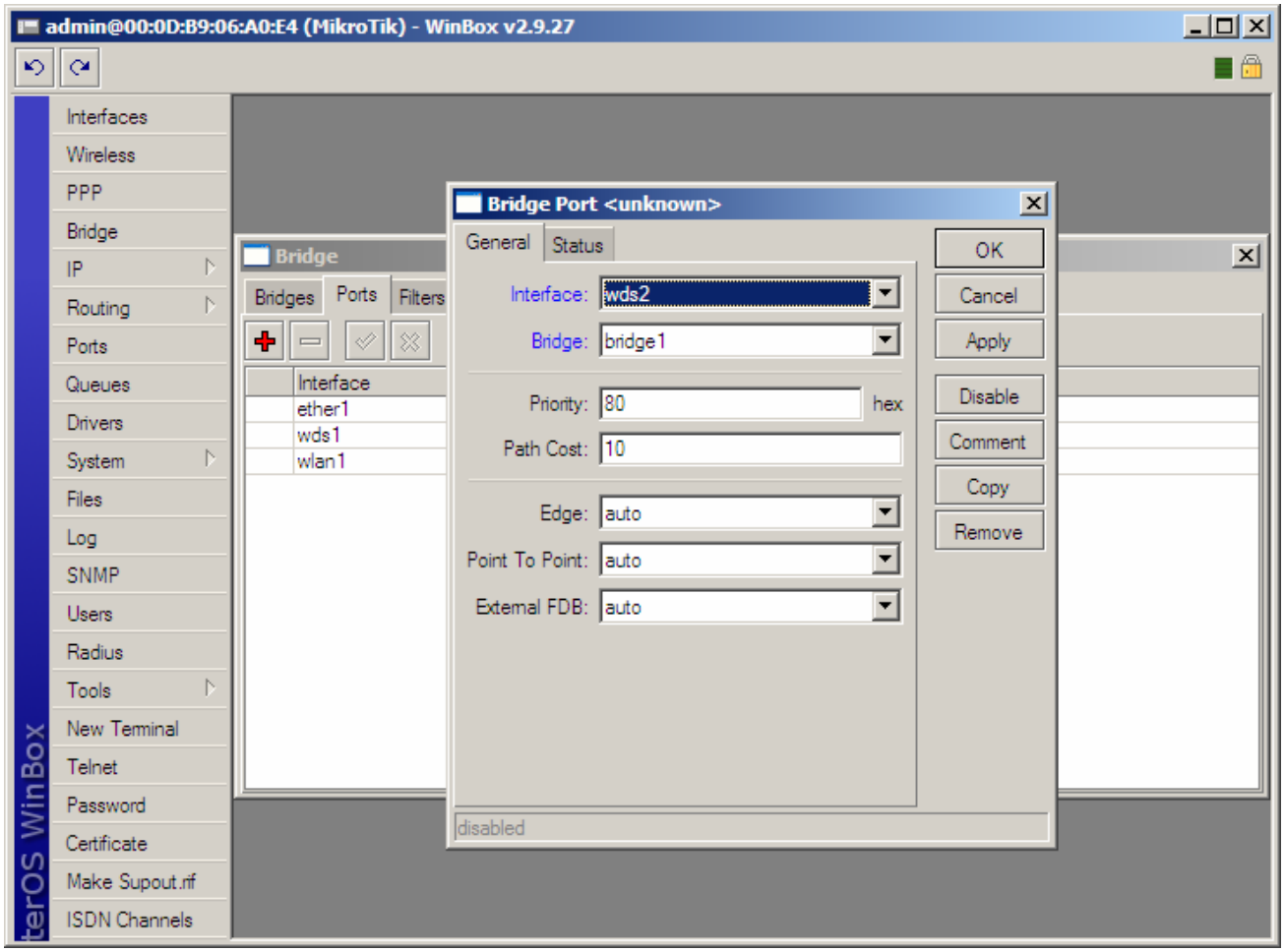
- Clique no botão OK

- Clique em Adicionar
- Em Interface, escolha a opção wds1
- Em Bridge, escolha a opção bridge1



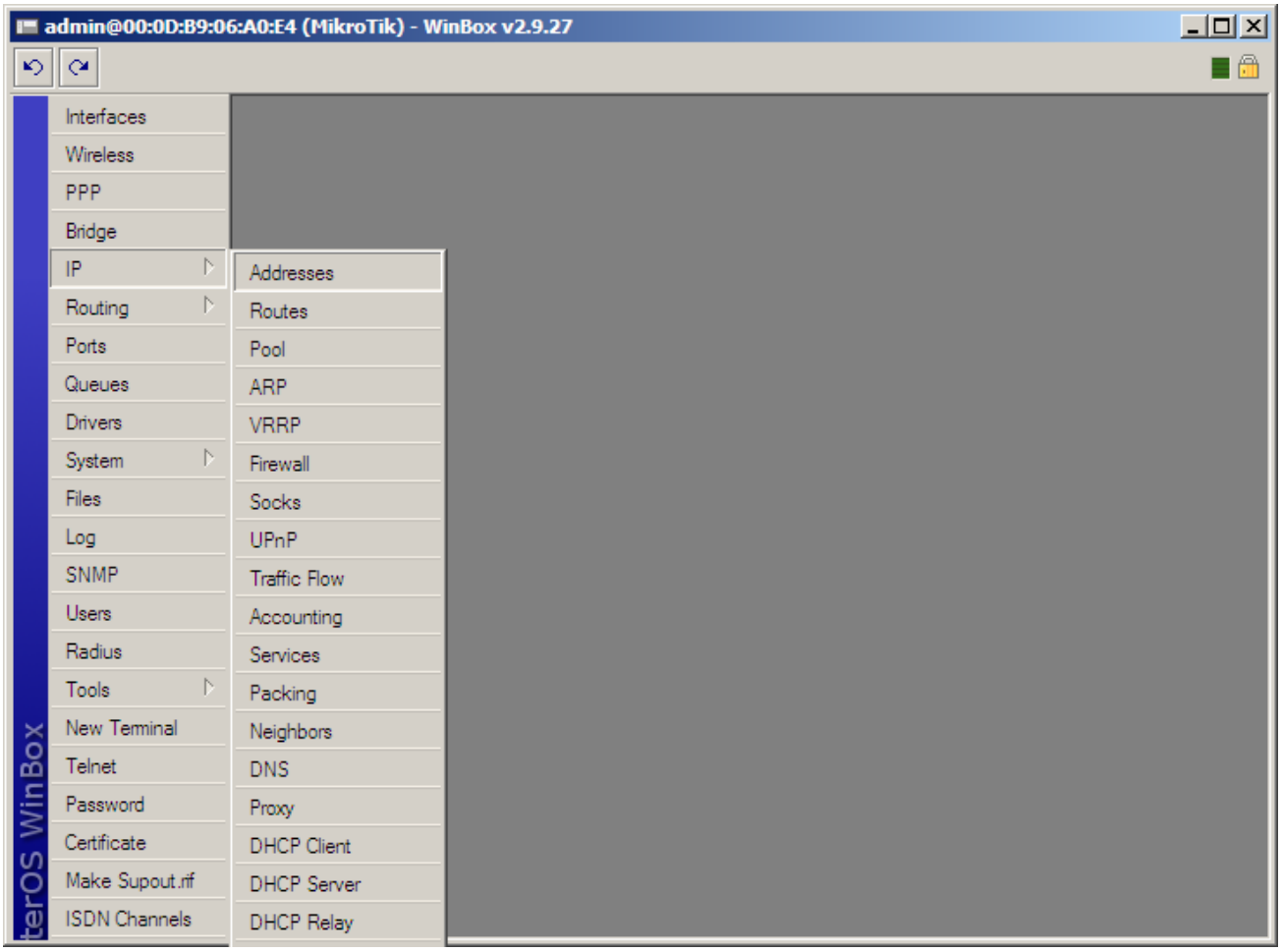
- Clique no botão OK

- Clique em Adicionar
- Em Interface, escolha a opção wds2
- Em Bridge, escolha a opção bridge1

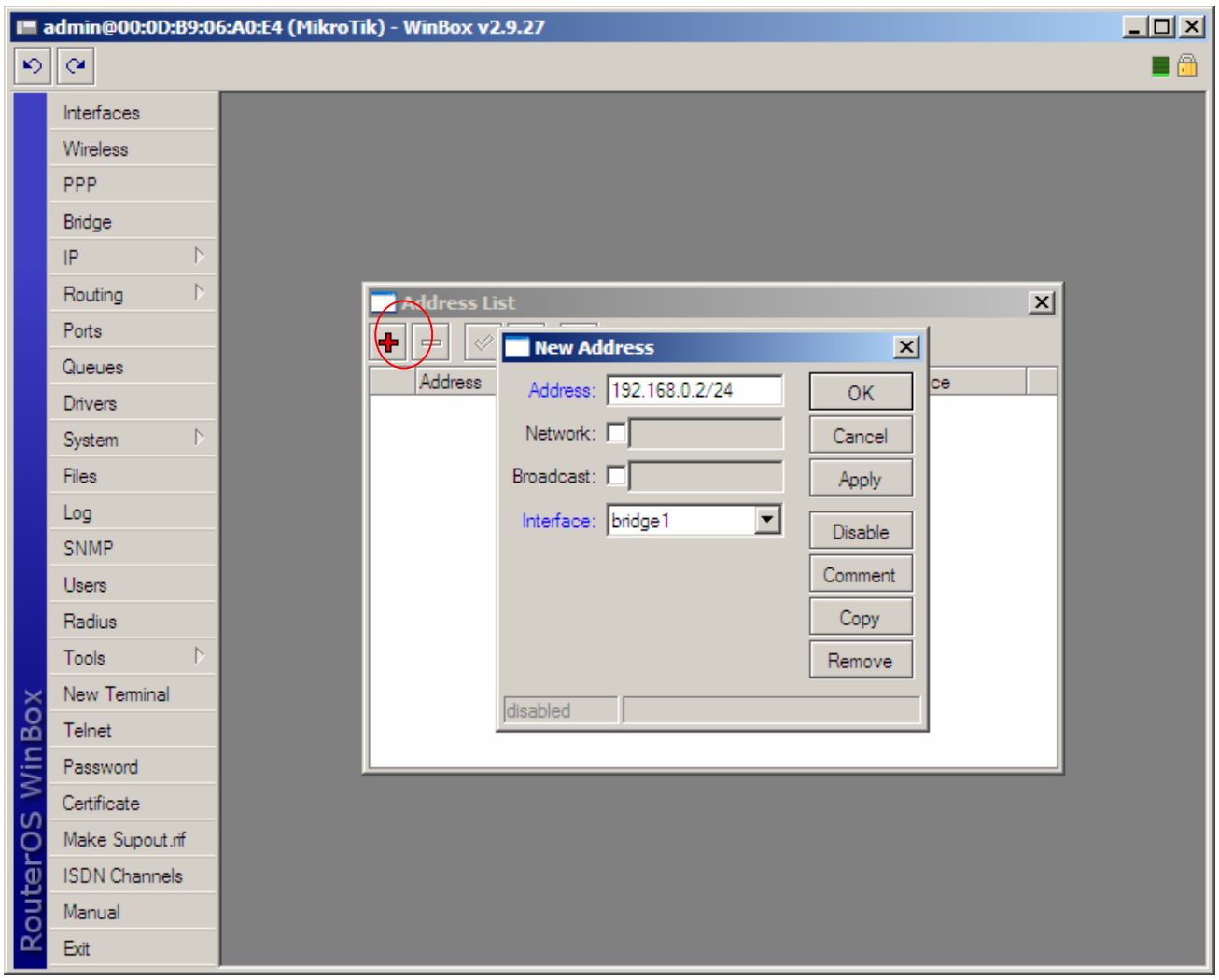


- Clique no botão OK

- Clique na guia IP, opção Address



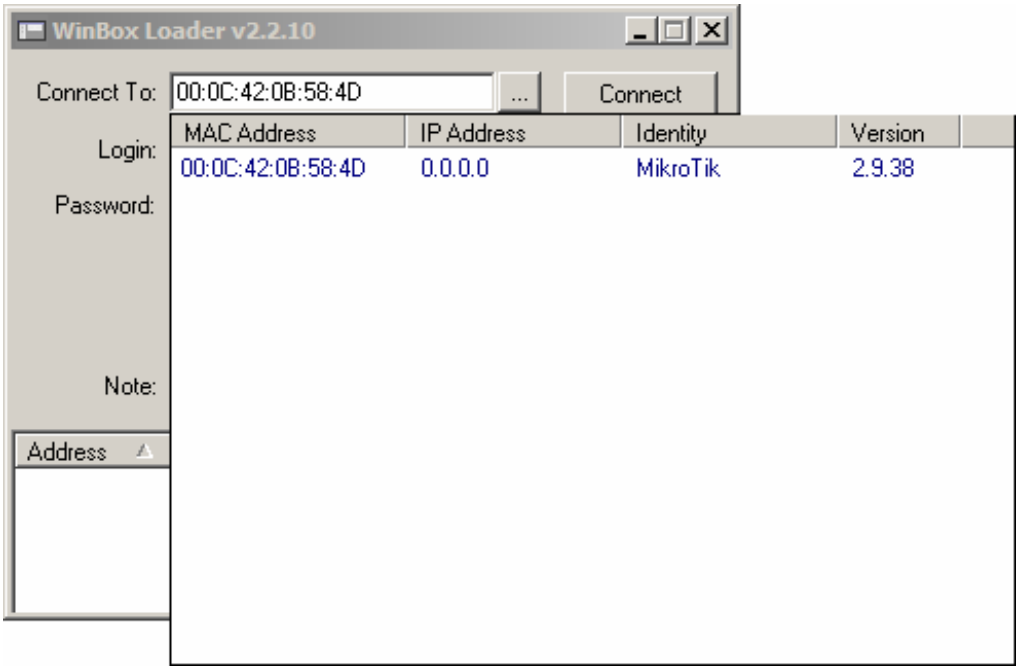
- Clique em Adicionar
- Em Address, digite um IP para o seu primeiro equipamento, em nosso caso: 192.168.0.2/24
- Em Interface, escolha a opção bridge1



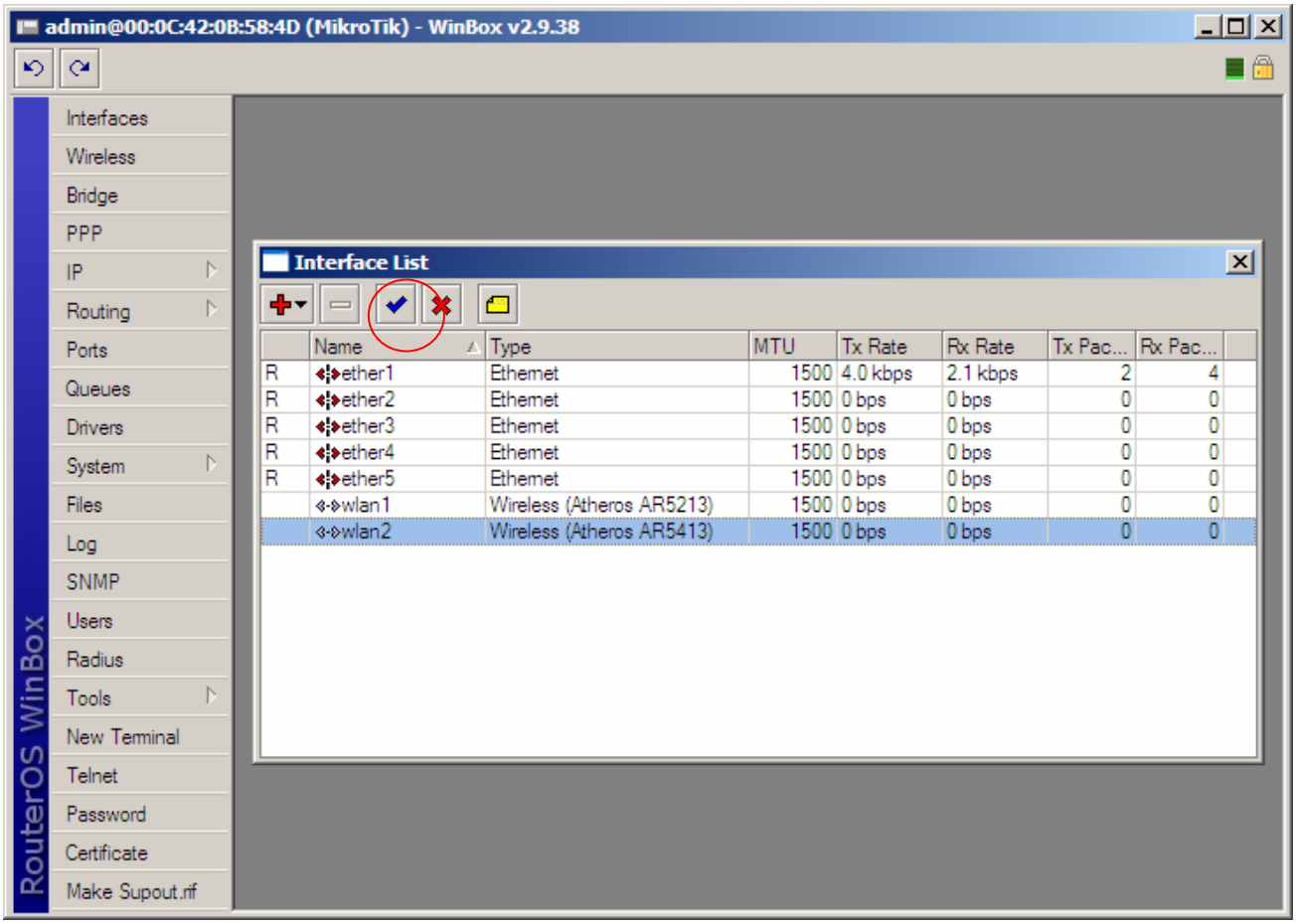
- Clique no botão OK

Configuração do Equipamento 1 – AP1

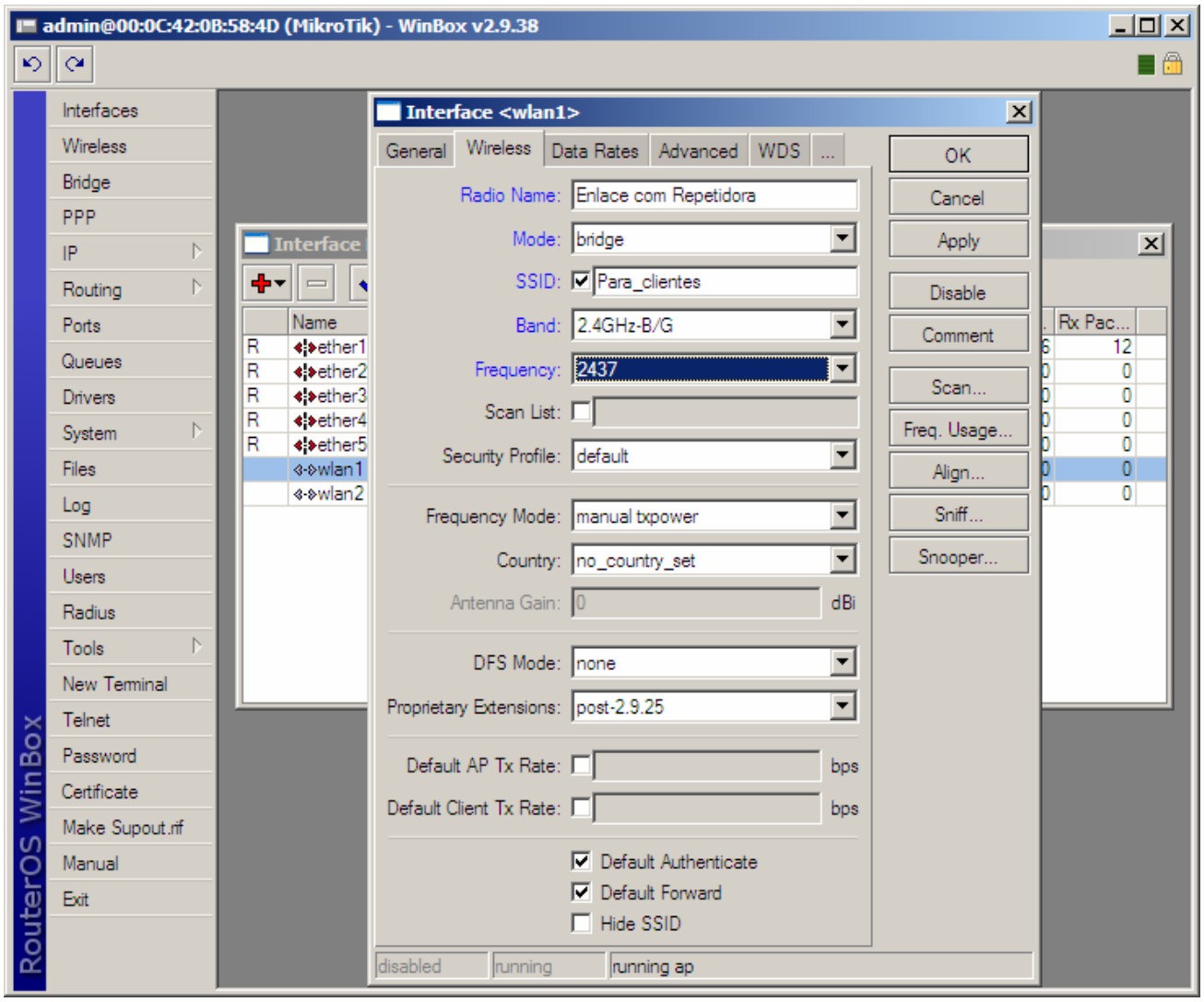
Acesse o RouterOS “Repetidora” através do Winbox



- Clique no menu Interface
- Habilite a interface wireless

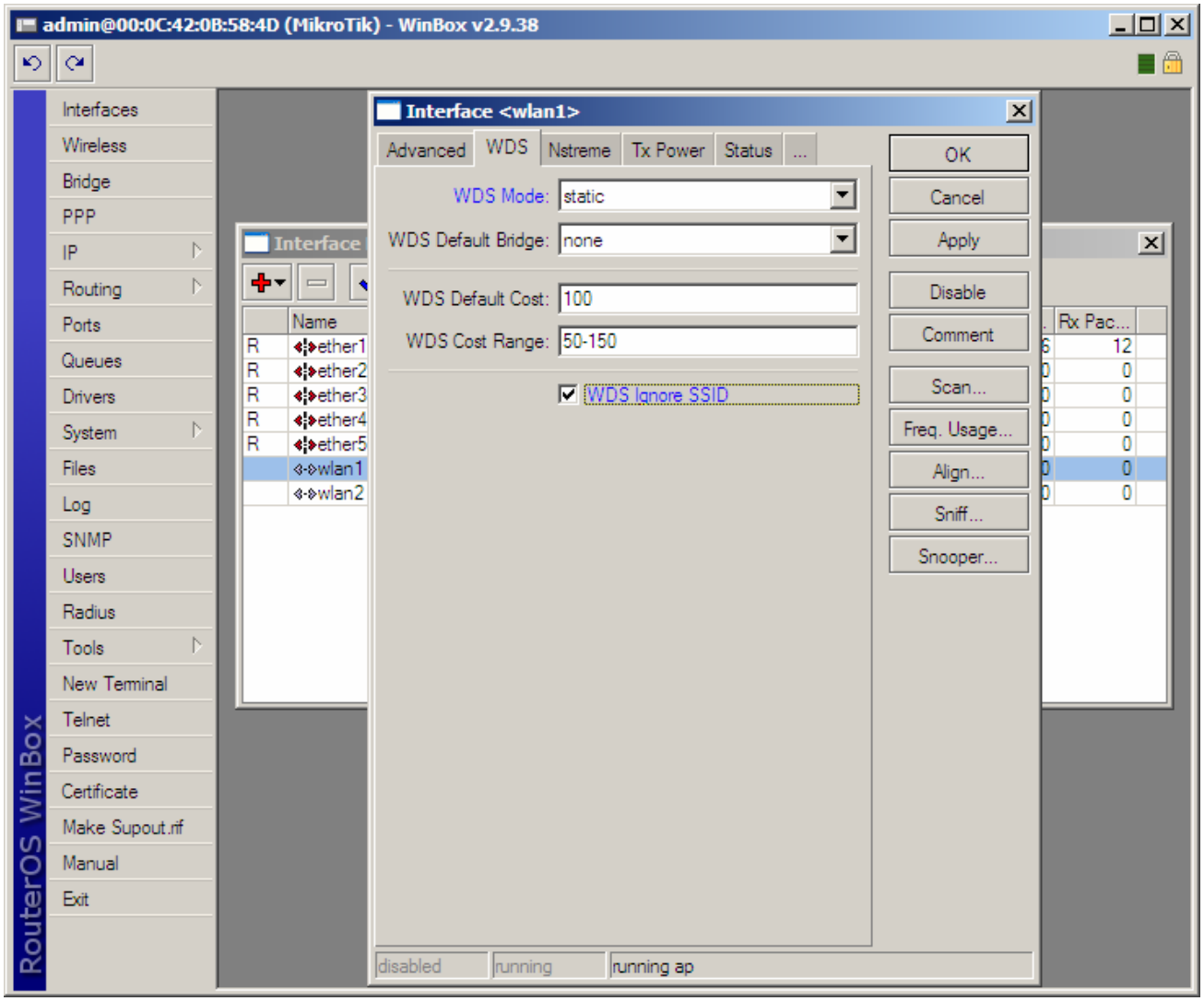


Configure a interface wireless wlan1, dando um clique duplo nela
- Clique na guia Wireless
- Em Radio Name, digite um nome para identificação da interface;
- Em Mode, escolha a opção bridge;
- Em SSID, digite um nome para identificação da interface na Rede;
- Em Band, escolha a banda desejada, em nosso caso: 2.4Ghz-B/G (a mesma banda escolhida na interface do Equipamento Repetidora);
- Em Frequency, escolha o canal que melhor lhe convier (o mesmo canal escolhido na interface do Equipamento Repetidora).

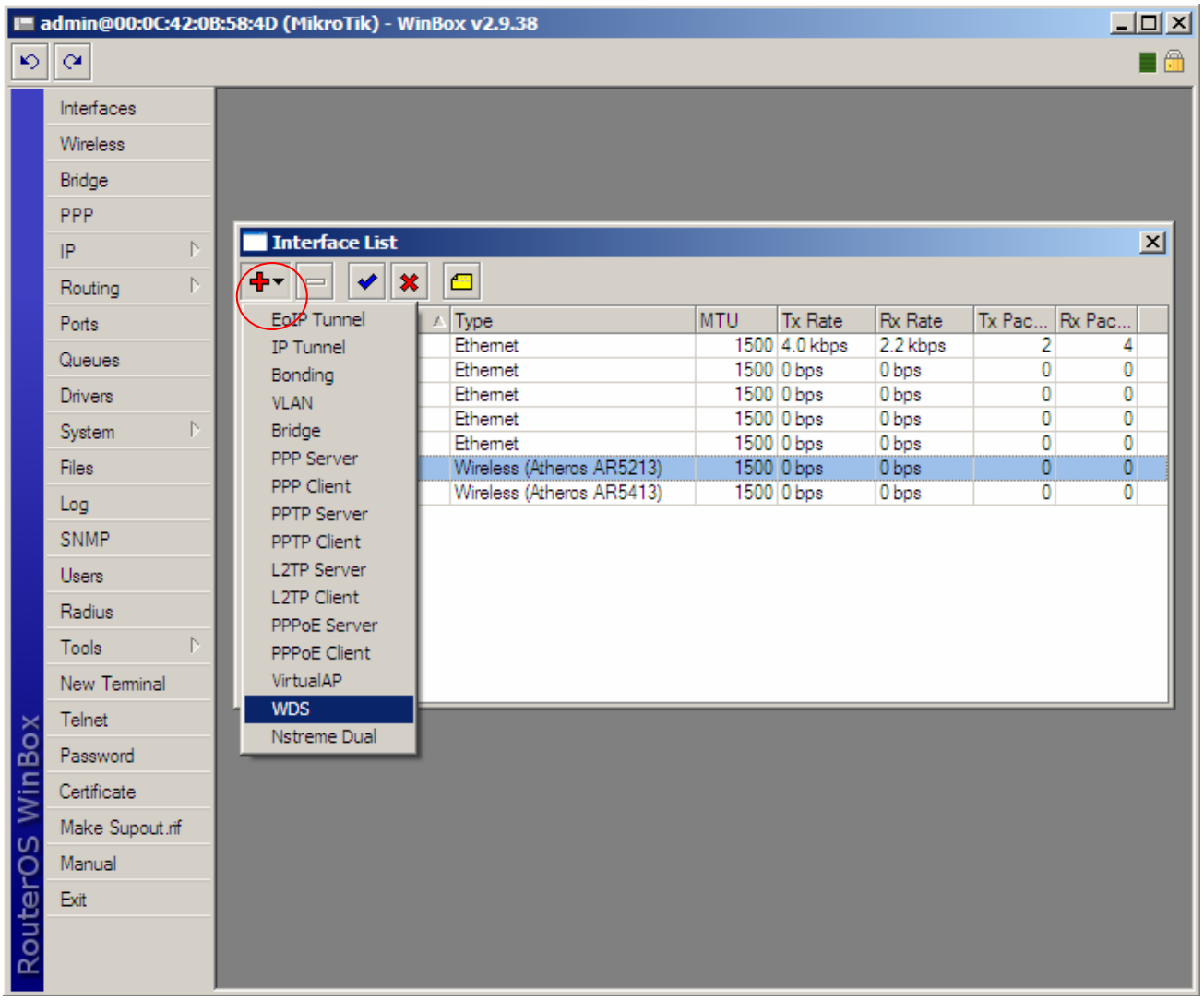


- Clique no botão OK

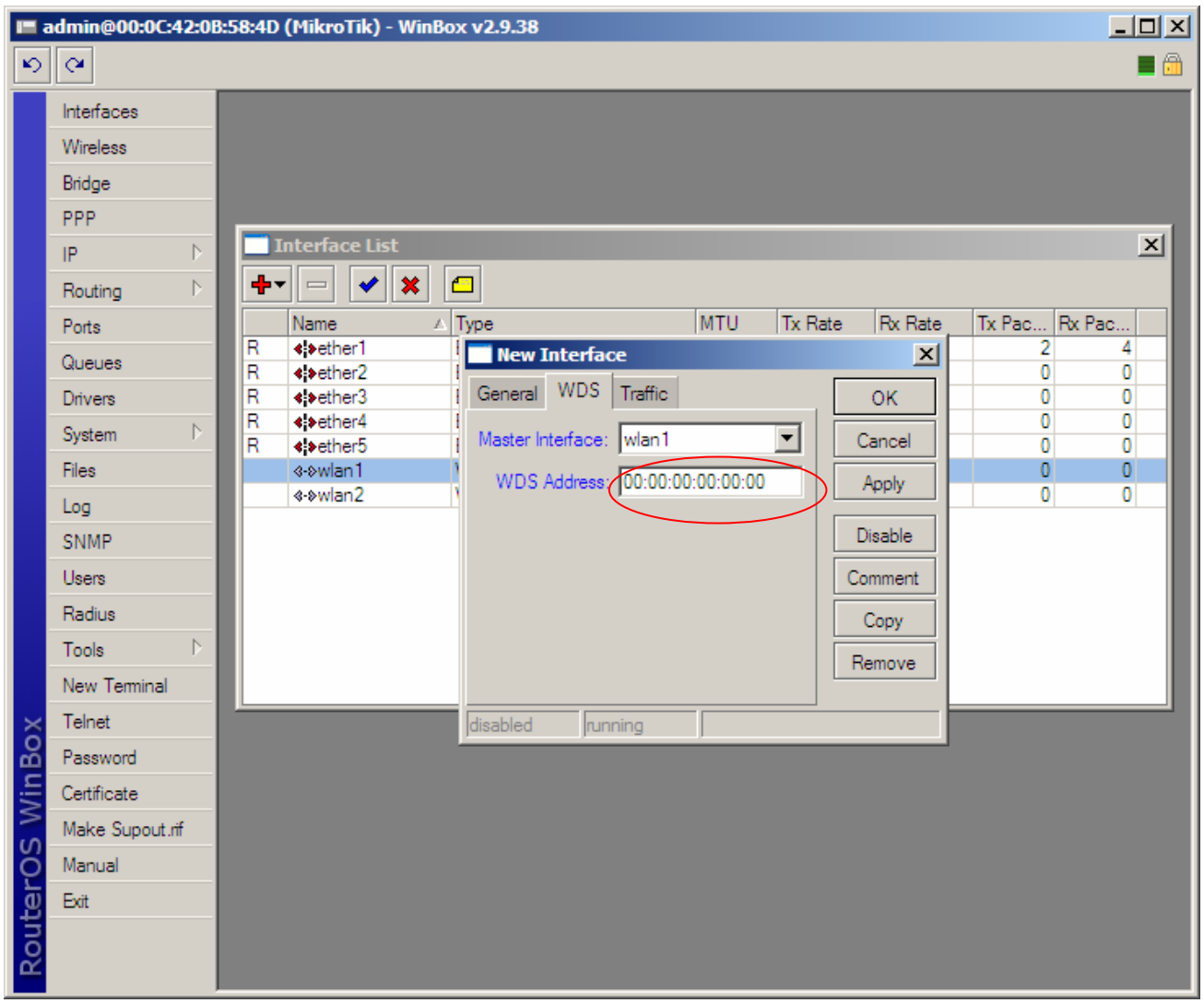
Clique na guia WDS
- Em WDS Mode, escolha a opção static
- Ative a opção WDS Ignore SSID
- Clique no botão OK



- Em Interface, clique em Adicionar
- Clique na opção WDS

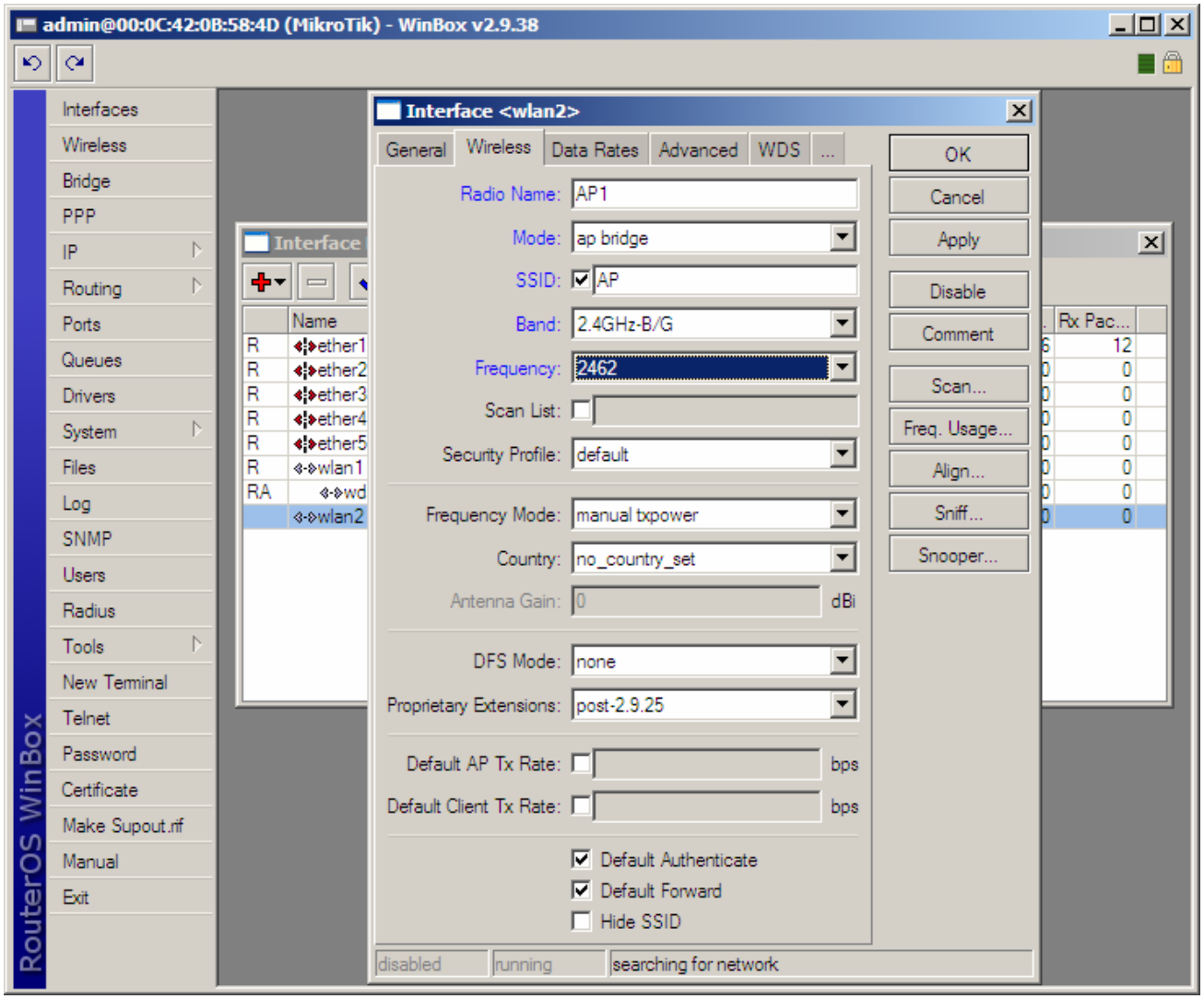


- Clique na guia WDS
- Em Master Interface, escolha a interface wlan1
- Em WDS Address, digite o MAC da interface wlan2 do Equipamento “Repetidora”



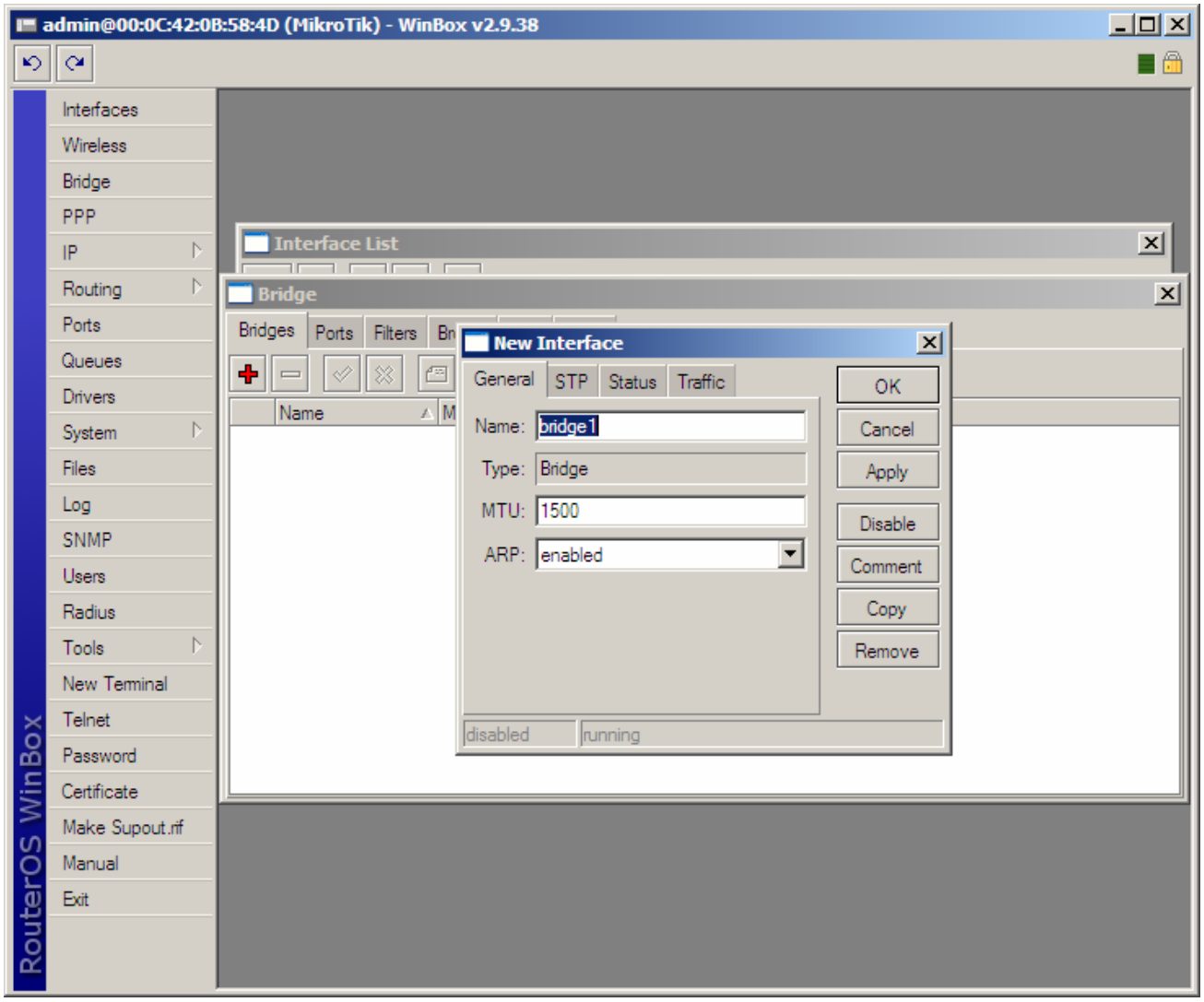
- Clique no botão OK

Configure a interface wireless wlan2, dando um clique duplo nela no menu Interface.
- Clique na guia Wireless
- Em Radio Name, digite um nome para identificação da interface;
- Em Mode, escolha a opção ap bridge;
- Em SSID, digite um nome para identificação da interface na Rede;
- Em Band, escolha a banda desejada, em nosso caso: 2.4Ghz-B/G;
- Em Frequency, escolha o canal que melhor lhe convier;



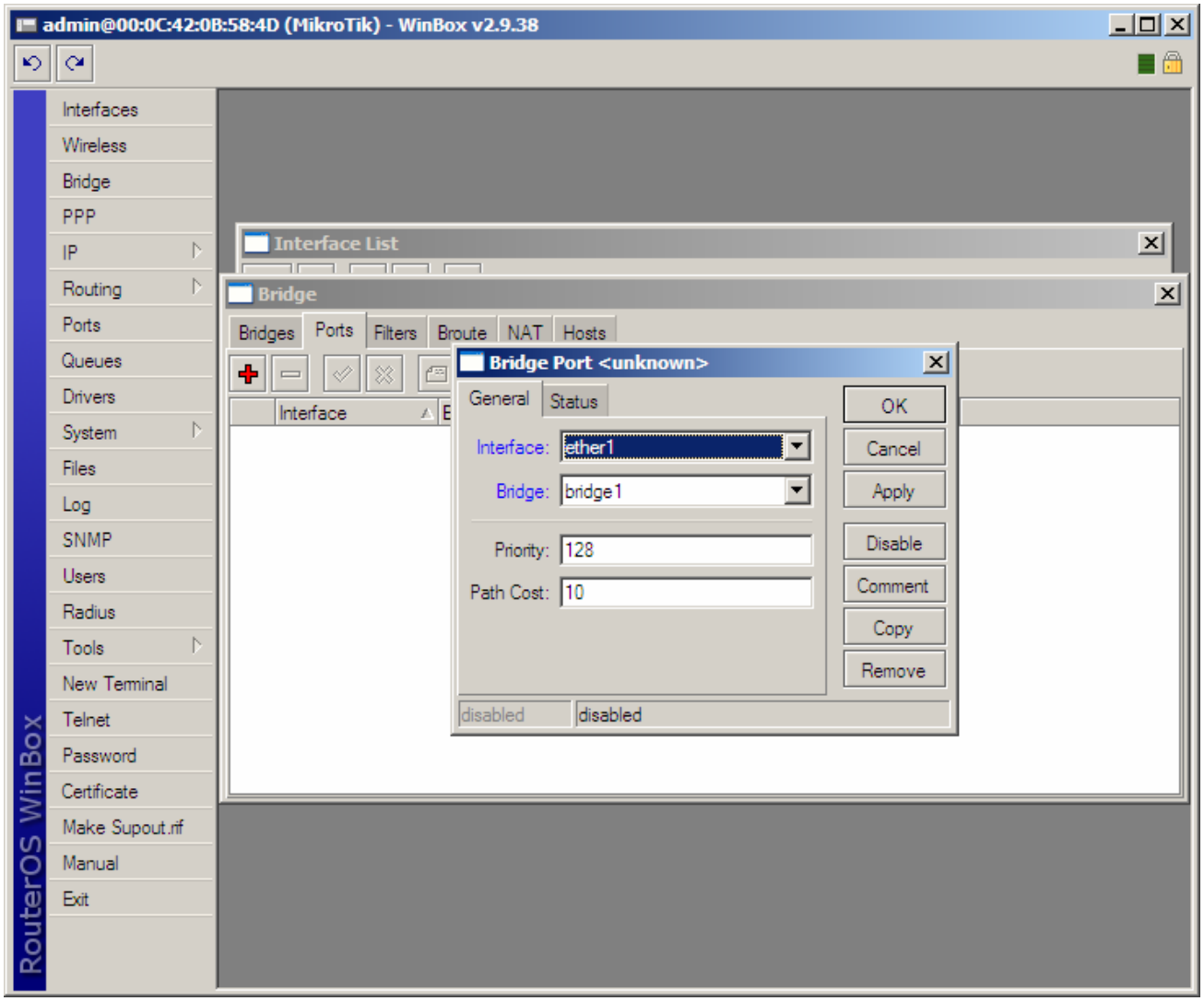
- Clique no botão OK.

- Clique o Menu Bridge
- Clique em Adicionar



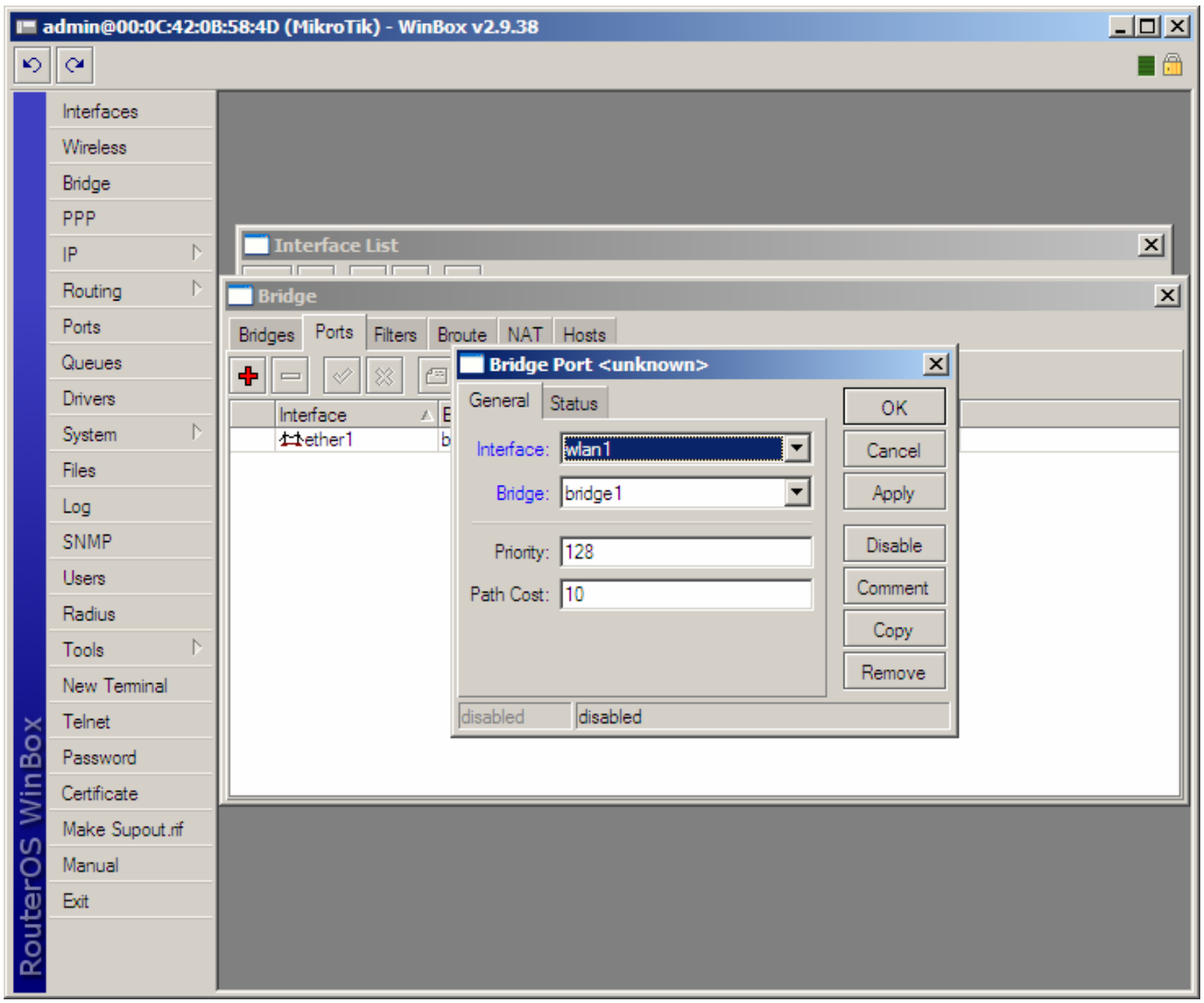
- Clique no botão OK

- Clique na guia Ports
- Clique em Adicionar
- Em Interface, escolha a opção ether1
- Em Bridge, escolha a opção bridge1



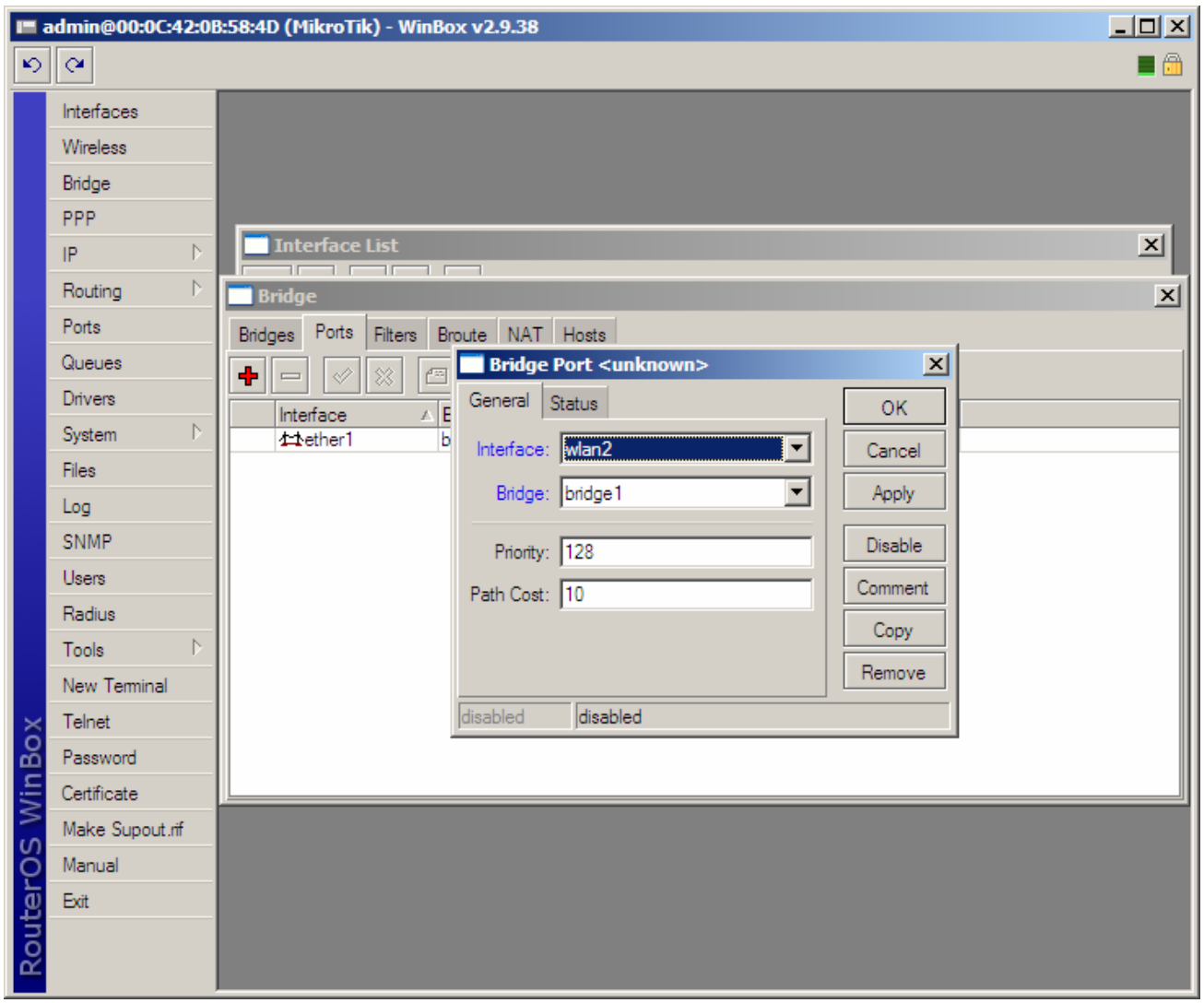
- Clique no botão OK

- Clique em Adicionar
- Em Interface, escolha a opção wlan1
- Em Bridge, escolha a opção bridge1



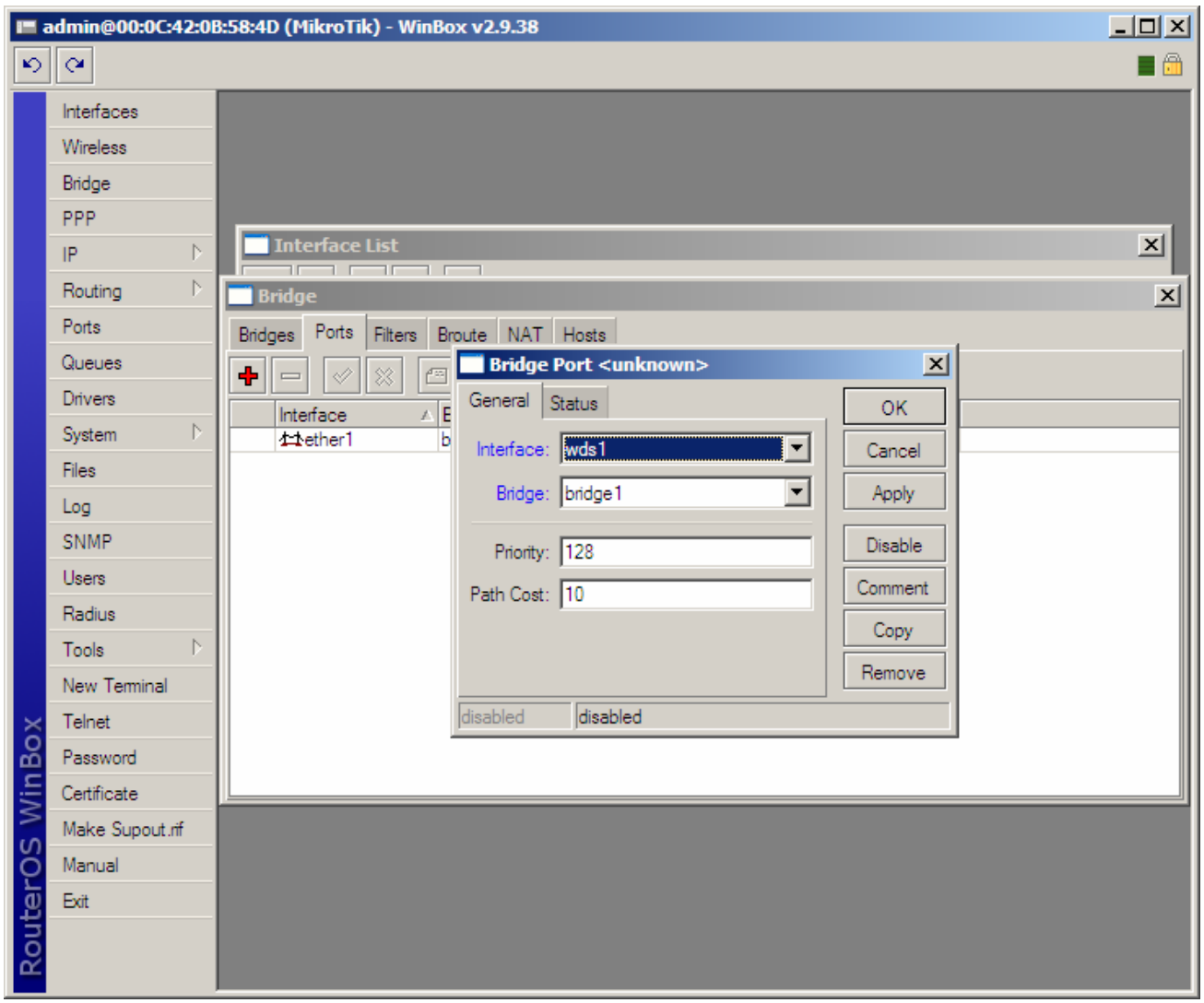
- Clique no botão OK

- Clique em Adicionar
- Em Interface, escolha a opção wlan2
- Em Bridge, escolha a opção bridge1



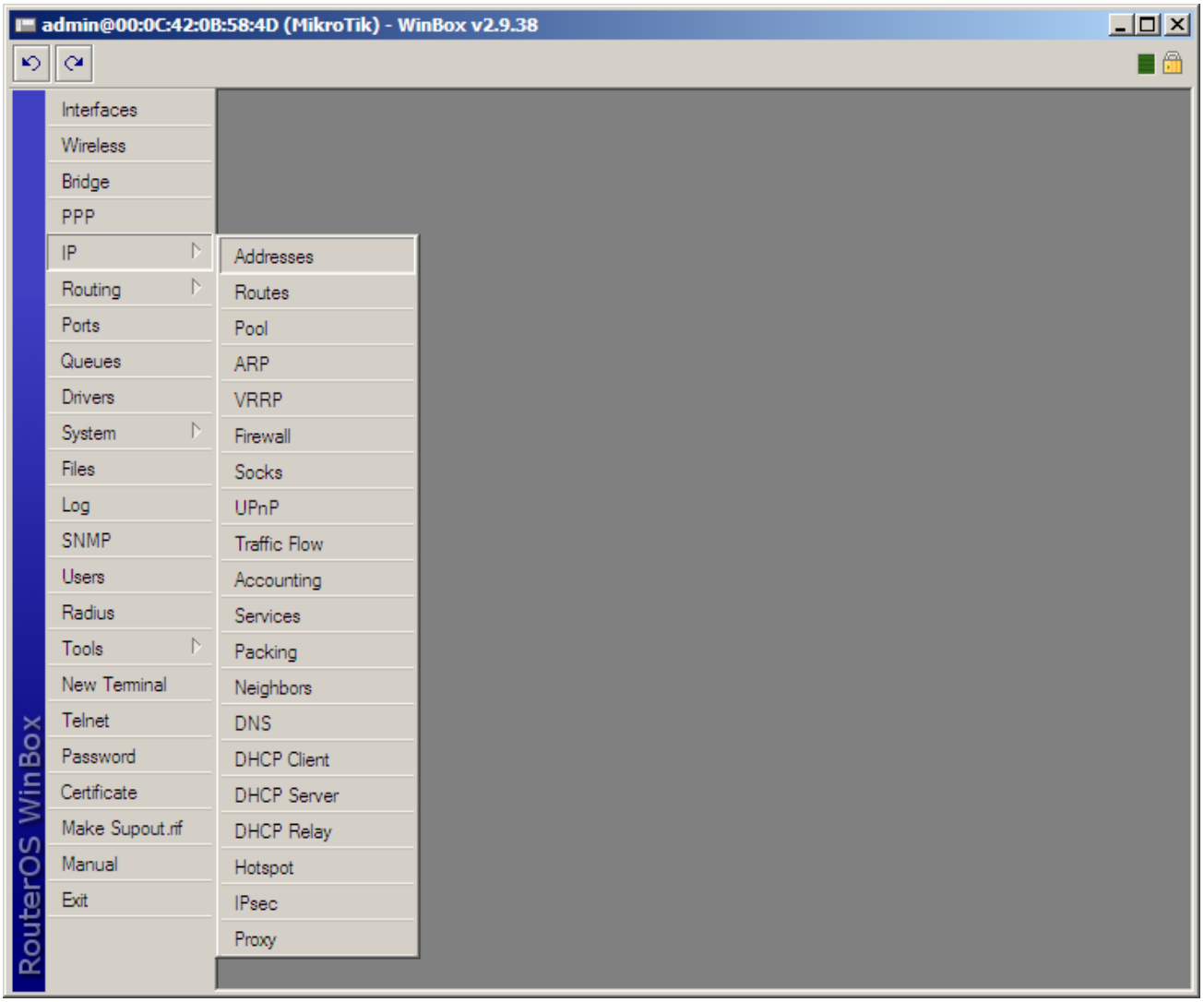
- Clique no botão OK

- Clique em Adicionar
- Em Interface, escolha a opção wds1
- Em Bridge, escolha a opção bridge1



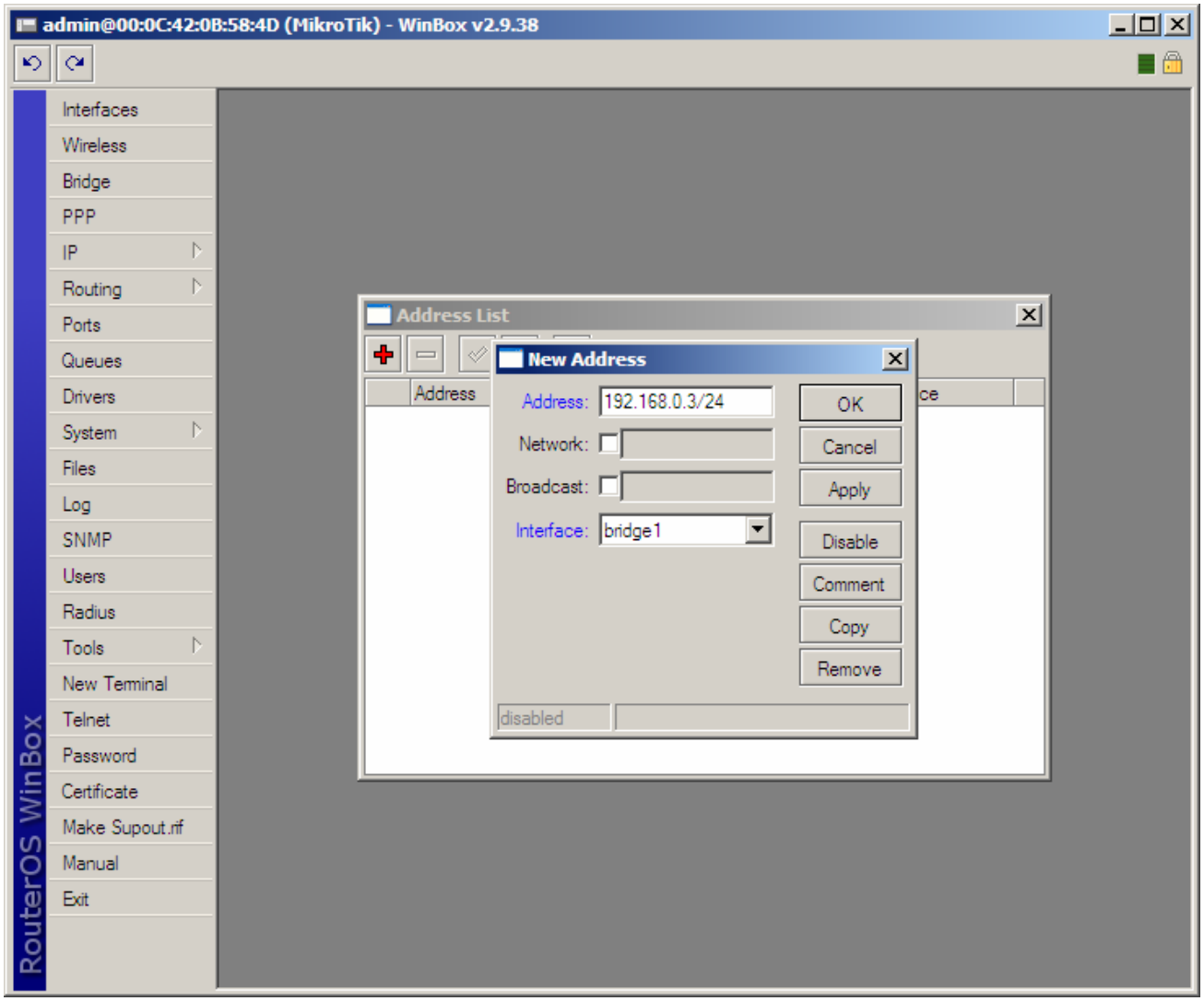
- Clique no botão OK

Clique na guia IP, opção Address



Clique em Adicionar

- Em Address, digite um IP para o seu primeiro equipamento, em nosso caso: 192.168.0.3/24
- Em Interface, escolha a opção bridge1



- Clique no botão OK

NAT

Em redes de computadores, NAT, **N**etwork **A**ddress **T**ranslation, também conhecido como masquerading é uma técnica que consiste em reescrever os endereços IP de origem de um pacote que passam sobre um roteador ou firewall de maneira que um computador de uma rede interna tenha acesso ao exterior (rede pública). Exemplo:

A estação com IP 192.168.1.13 faz uma requisição, por exemplo, para um endereço externo. O pacote sai com o IP da estação e corre em direção ao intermediador entre ambiente interno e externo, o gateway. O gateway, através do protocolo NAT mascara o IP da estação com seu IP (200.158.112.126 - que é válido na internet) assim fazendo com que o pacote seja entregue no destino solicitado pela estação. No retorno do pacote, ele parte do endereço externo, chega a nossa rede no servidor NAT (200.158.112.126) e lá é volta ater o IP da estação assim chegando à estação (192.168.1.13).

Esta foi uma medida de reação face à previsão da exaustão do espaço de endereçamento IP, e rapidamente adaptada para redes privadas também por questões econômicas (no início da Internet os endereços IP alugavam-se, quer individualmente quer por classes/grupos).

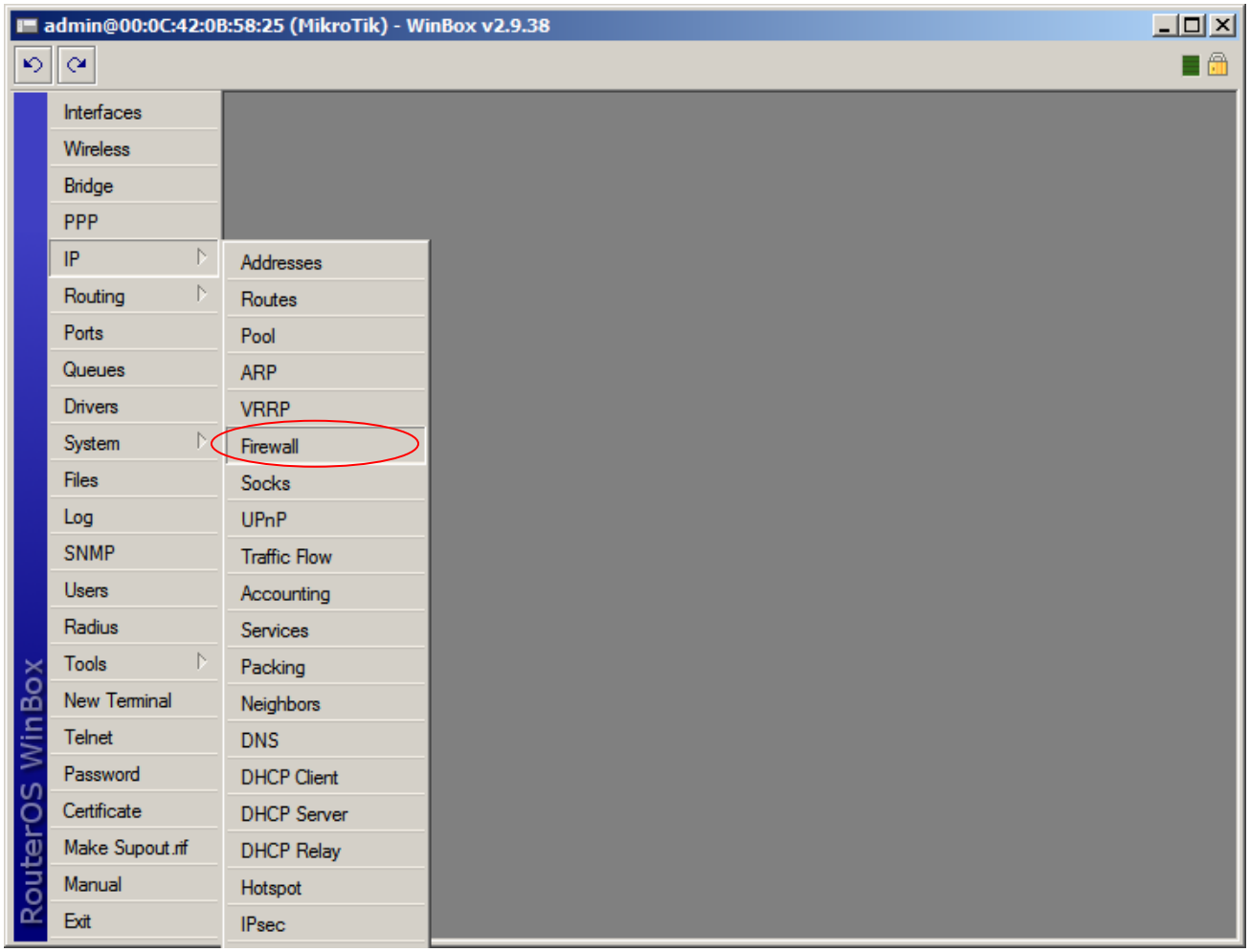
Um computador atrás de um roteador gateway NAT tem um endereço IP dentro de uma gama especial, própria para redes internas. Como tal, ao aceder ao exterior, o gateway seria capaz de encaminhar os seus pacotes para o destino, embora a resposta nunca chegasse, uma vez que os roteadores entre a comunicação não saberiam reencaminhar a resposta (imagine-se que um desses roteadores estava incluído em outra rede privada que, por ventura, usava o mesmo espaço de endereçamento). Duas situações poderiam ocorrer: ou o pacote seria indefinidamente [(1)] reencaminhado, ou seria encaminhado para uma rede errada e jogado fora.

[(1)] na verdade, existe um tempo de vida para os pacotes IP serem reencaminhados.

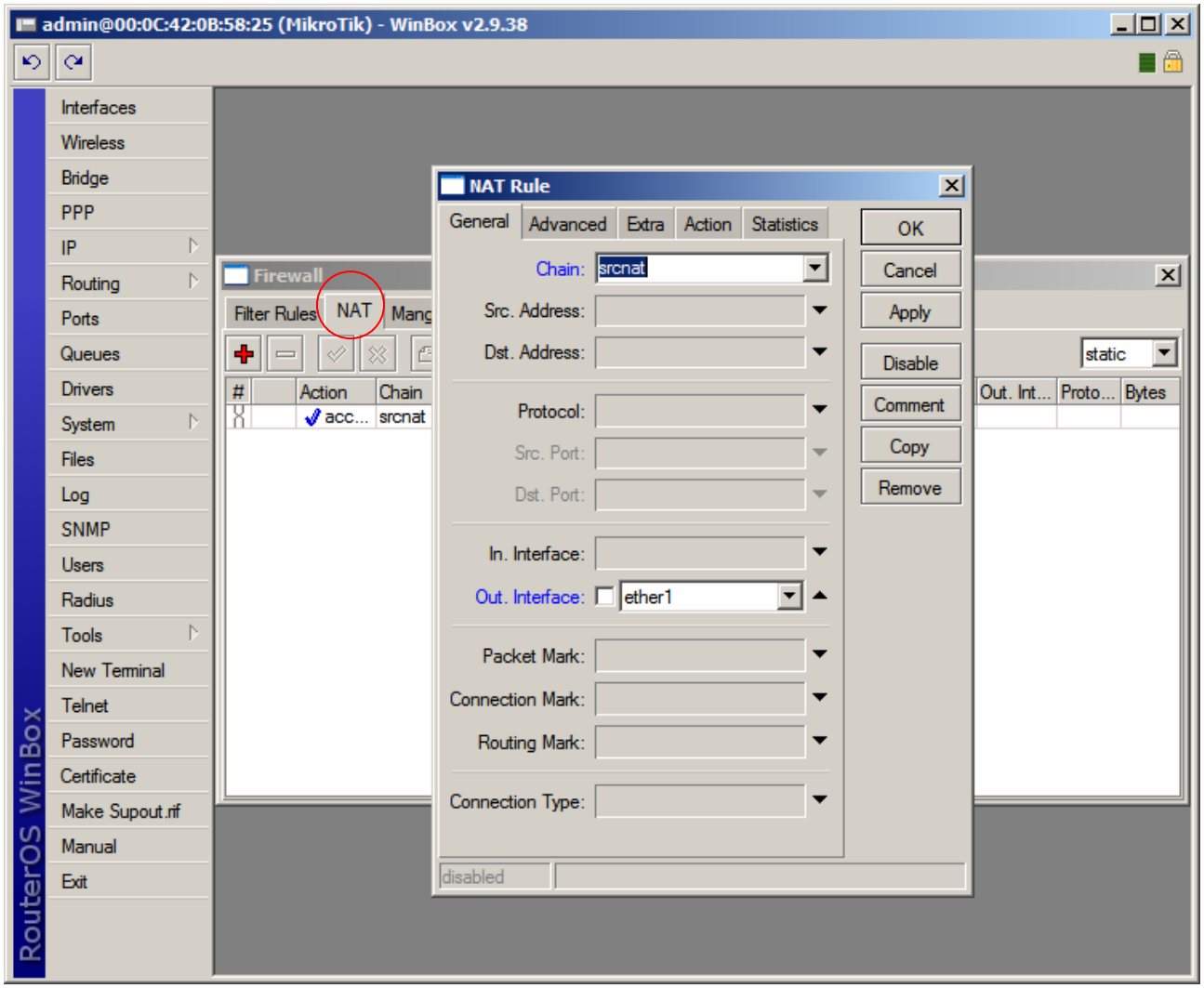
NAT-Network Address Translation, é a designação dada à técnica de conversão de endereços, quando se pretende que um pacote passe de uma rede privada para uma rede pública (internet)

Configurando o NAT no Mikrotik:

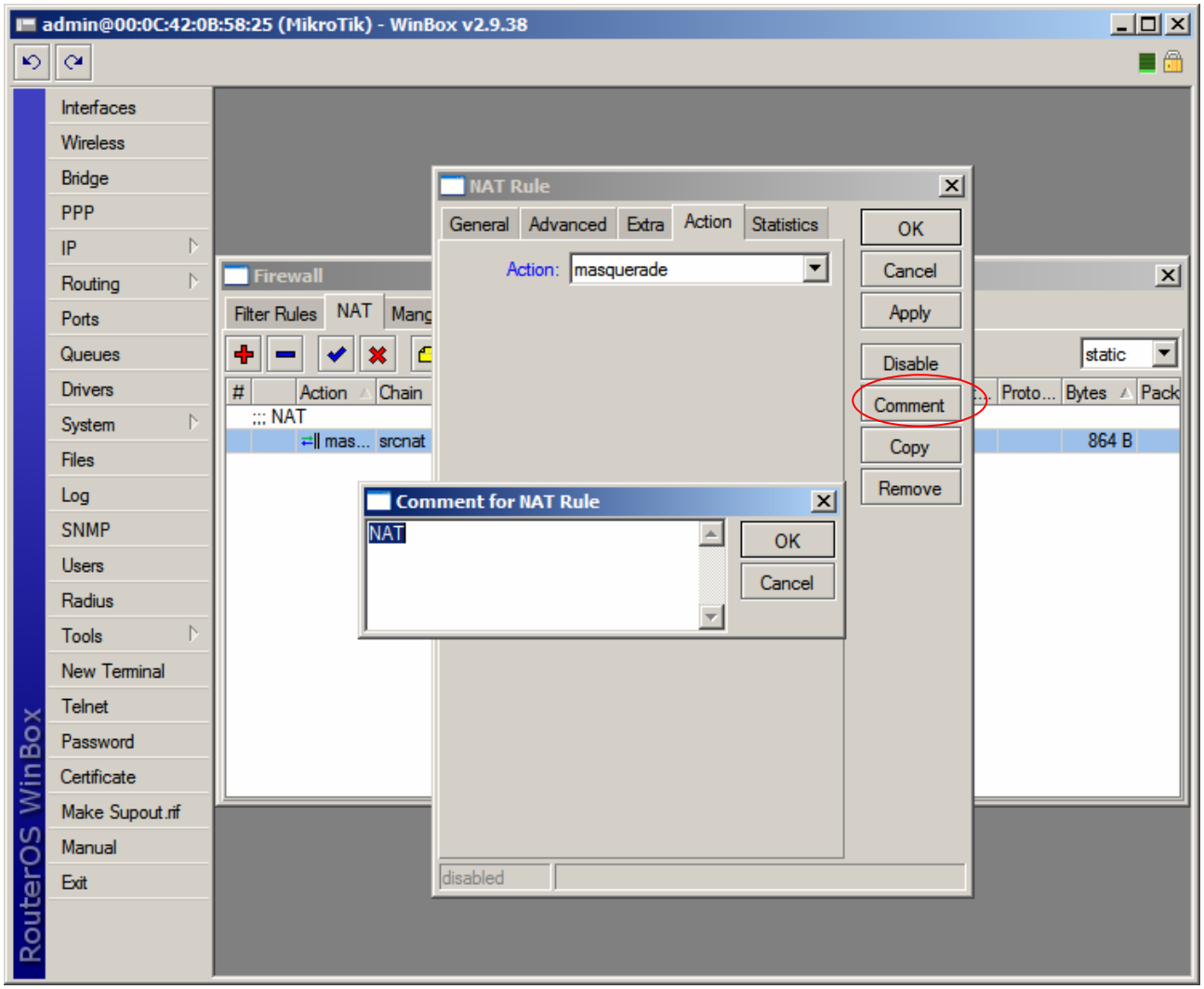
- Clique no menu “IP”
- Clique na opção “Firewall”



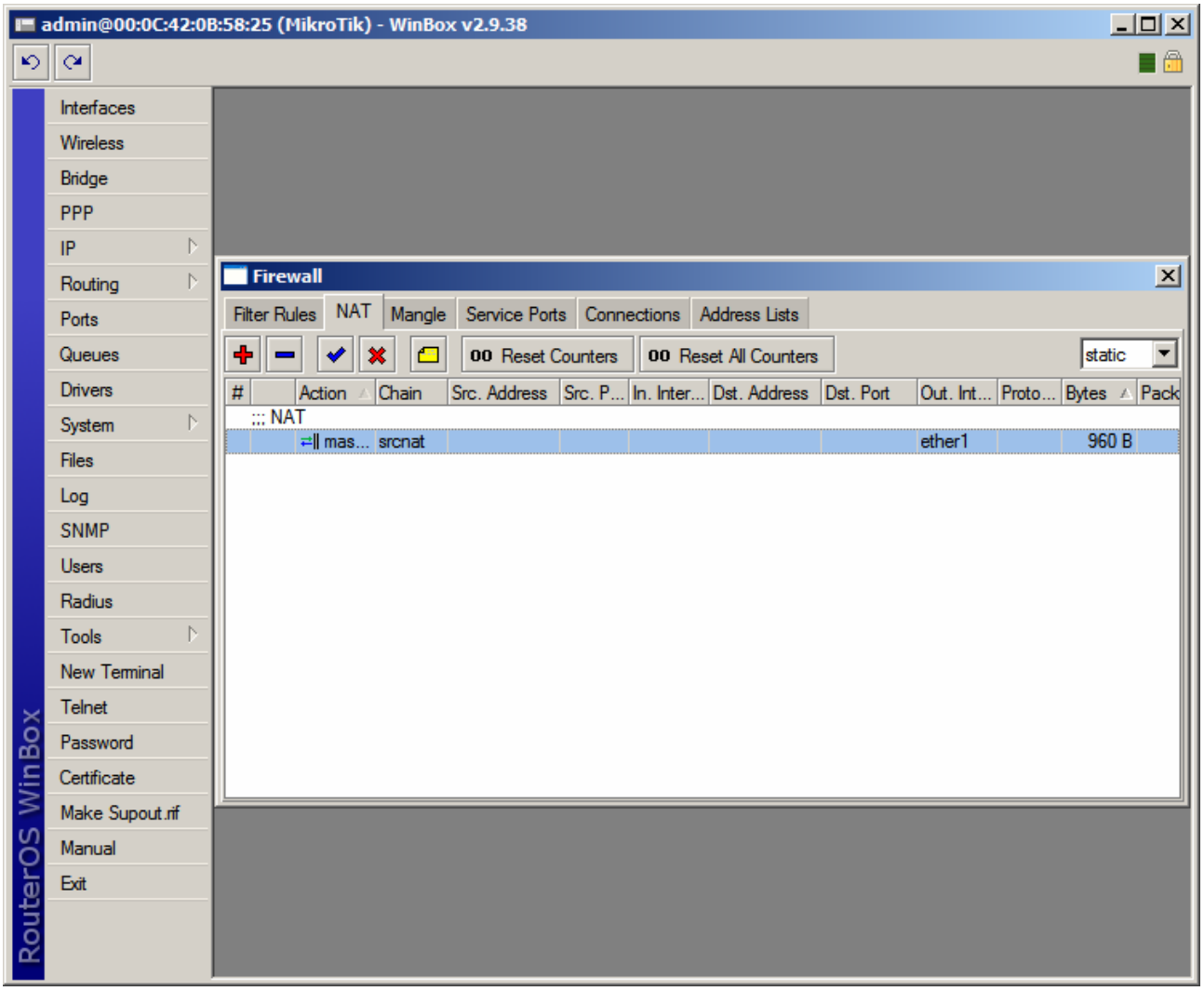
- Clique na guia “NAT”
- Na guia General, na opção Chain, escolha a opção “srcnat”
- Na opção Out. Interface (interface de saída), escolha a interface de saída para a internet. Em nosso caso, do exemplo: “ether1”
- Clique no botão “Apply”



- Clique na guia “Action”
- Na opção Action, escolha a opção “masquerade”
- Clique no botão “Comment”
- Digite um comentário para identificar a regra criada. Ex: NAT

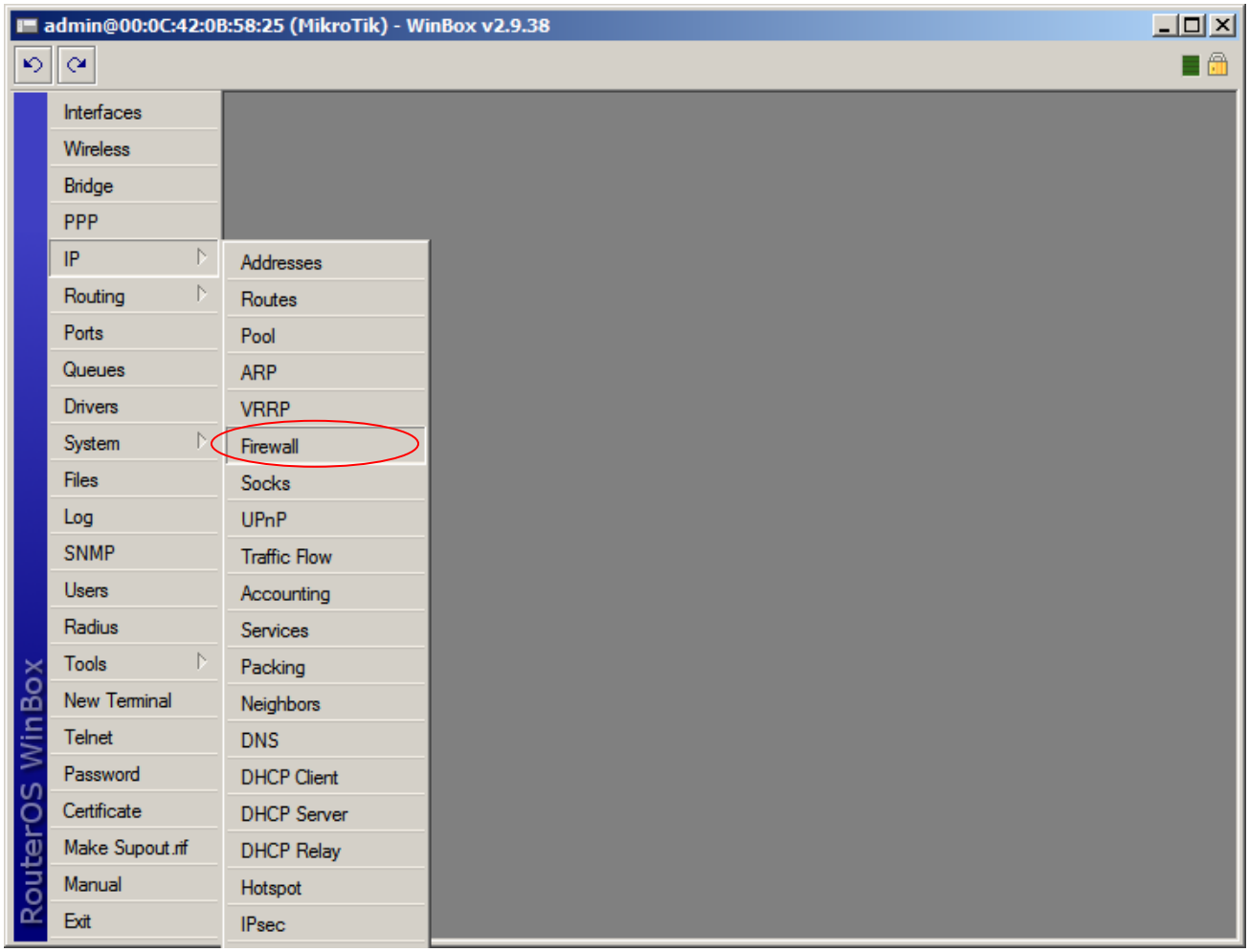


- Clique no botão OK
- Clique no botão OK

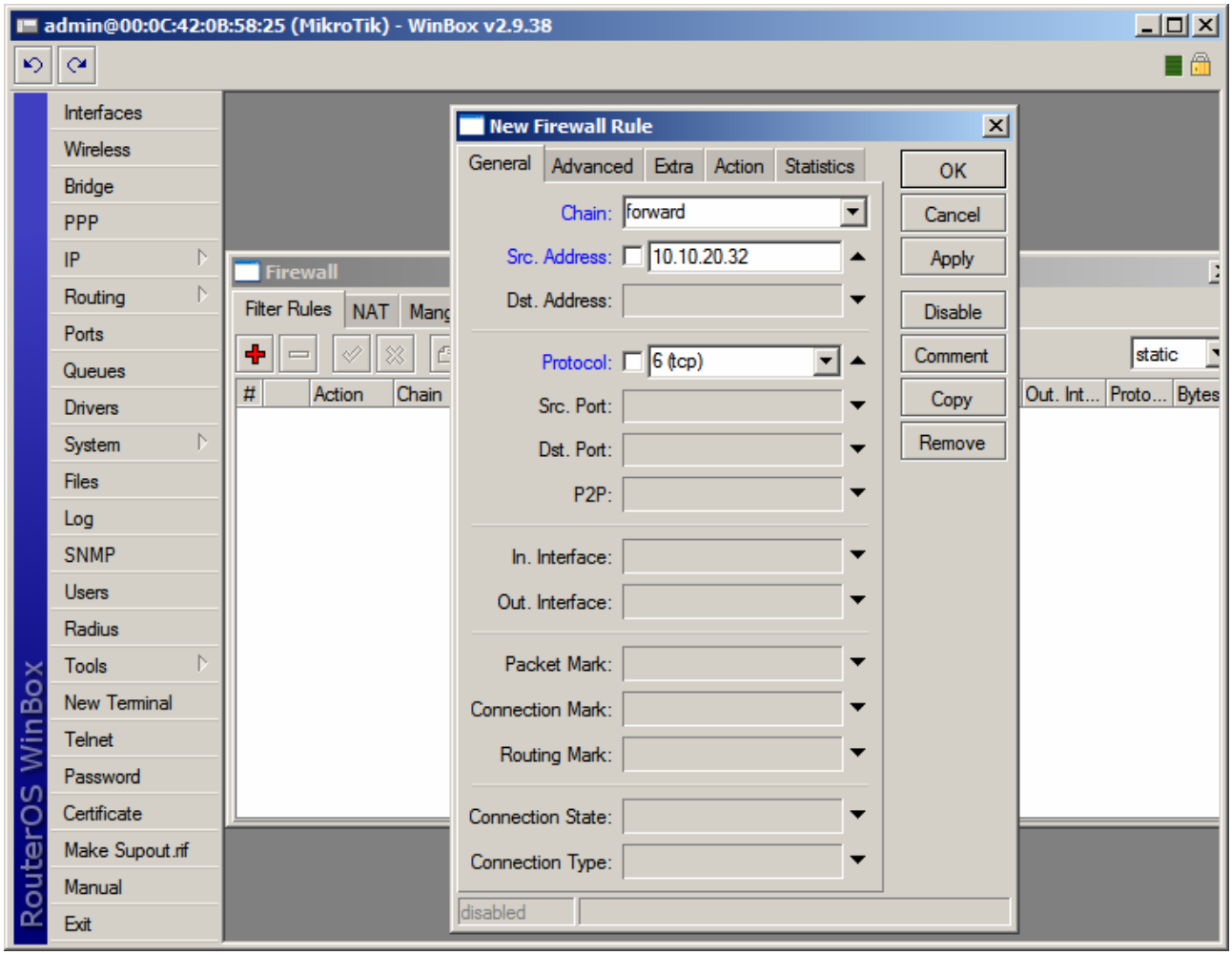


LIMITAR CONEXÕES POR IP

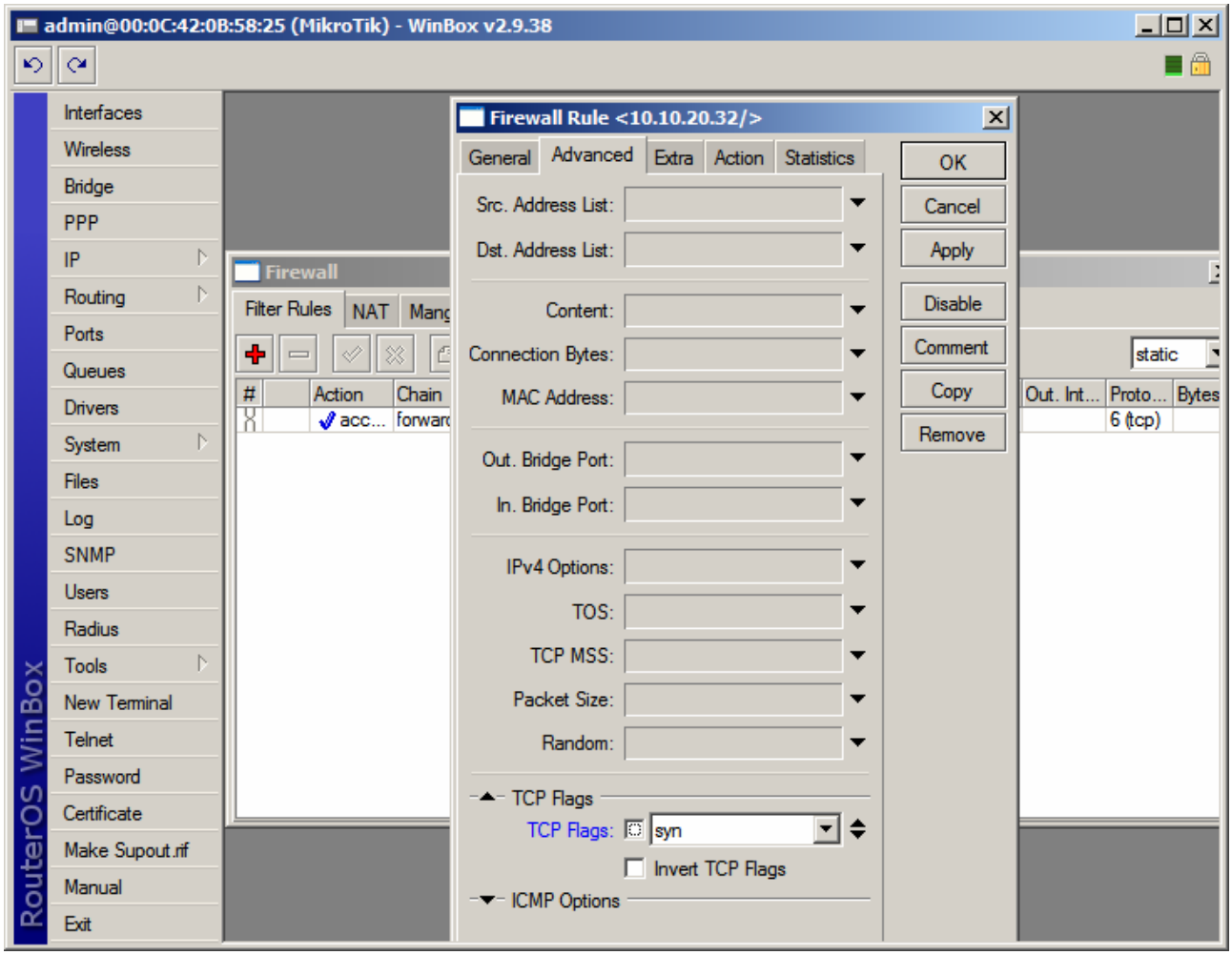
Esta opção é utilizada para limitar as conexões dos clientes conectados ao Mikrotik.



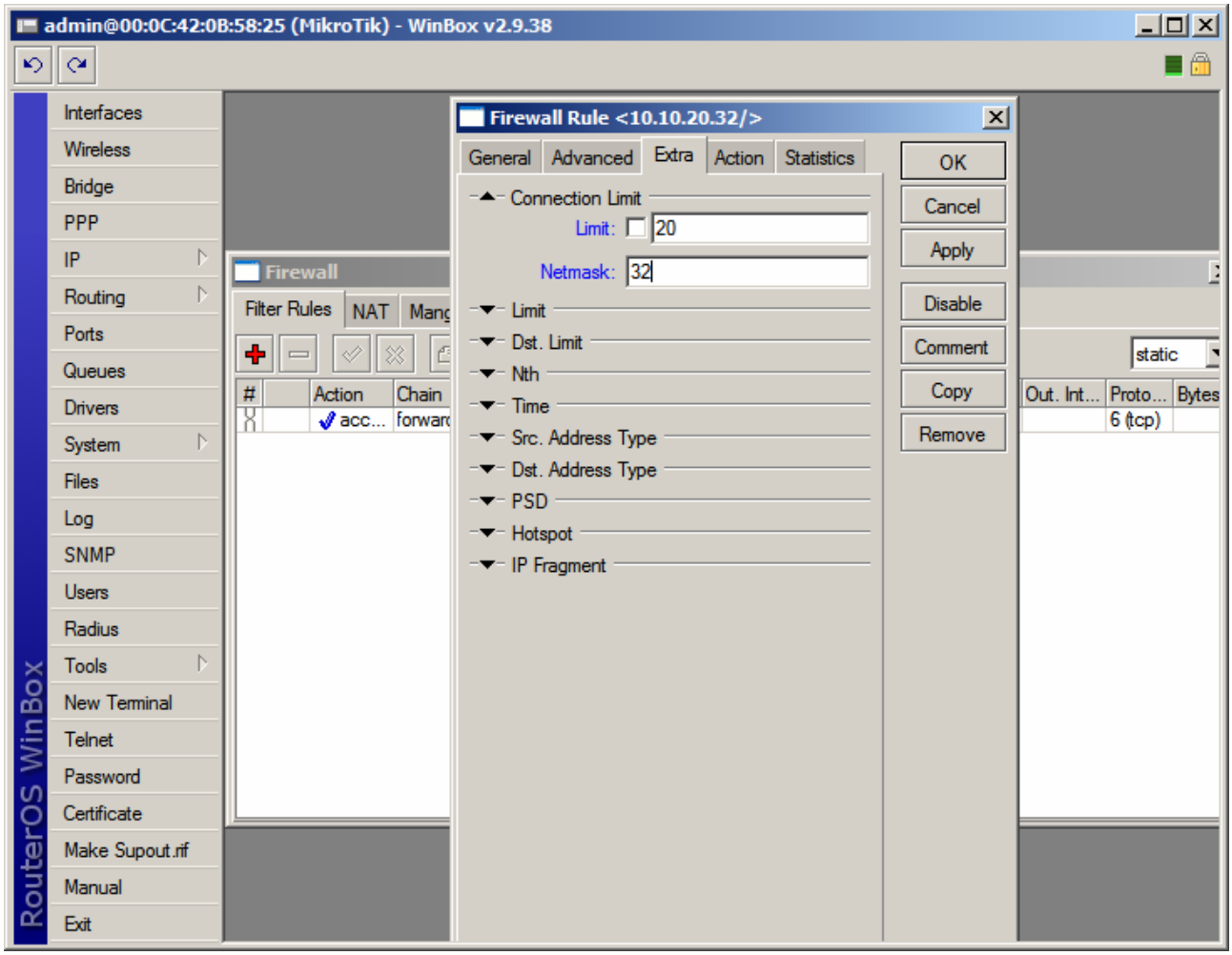
- Clique na guia “Filter Rules”.
- Na guia General, na opção “Chain”, escolha a opção “forward”.
- Na opção Src. Address, digite o IP do cliente a ser limitado.
- Na opção Protocol, escolha o protocolo “TCP”
- Clique no botão “Apply”



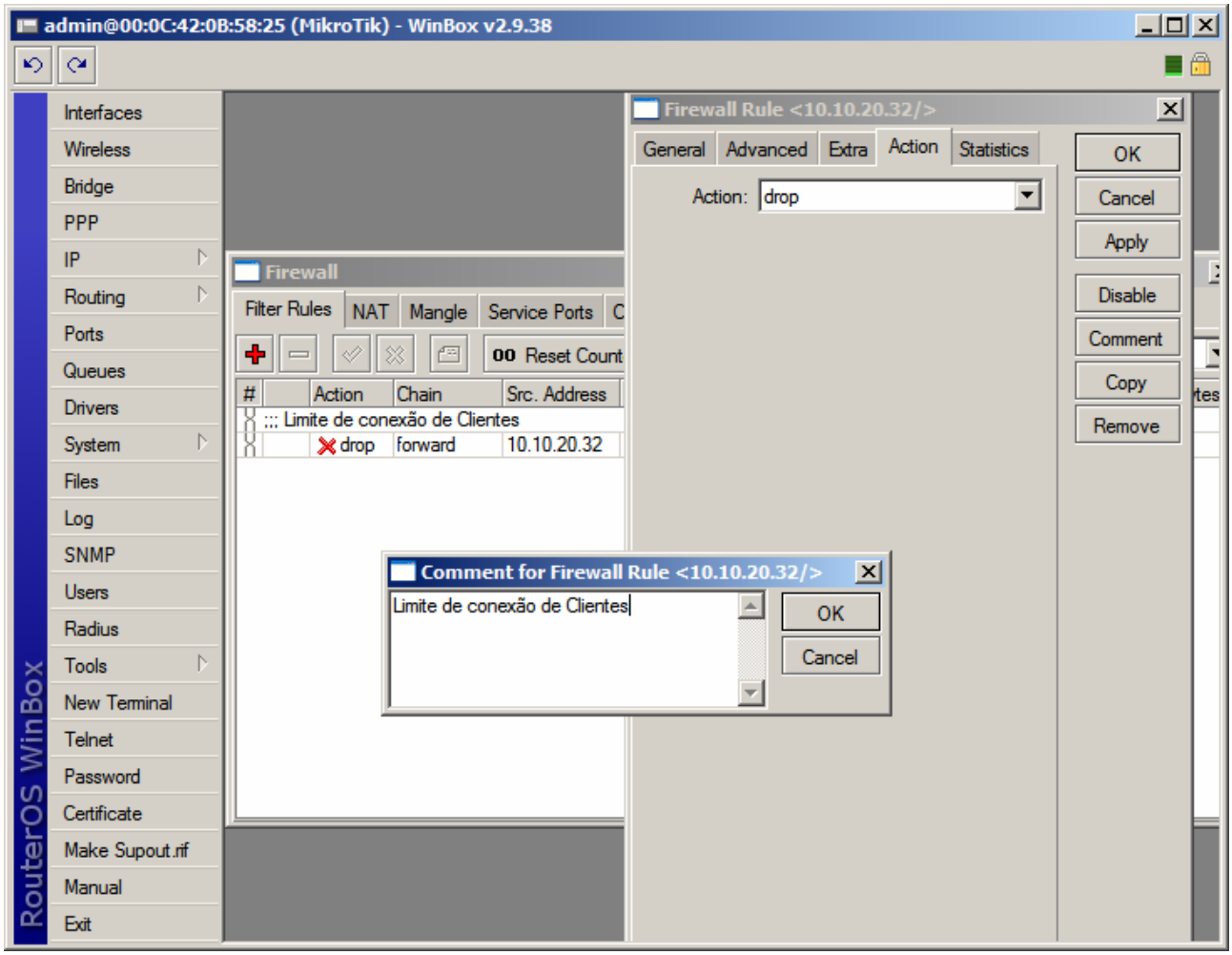
- Clique na guia “Advanced”
- Clique na opção “TCP Flags”
- Escolha a opção “syn”
- Clique no botão “Apply”



- Clique na guia “Extra”
- Clique na opção “Connection Limit”
- Na opção “Limit”, digite a quantidade de conexões que você quer permitir para o IP escolhido.
- Na opção “Netmask”, deixe a quantidade default (32)
- Clique no botão “Apply”



- Clique na guia “Action”
- Na opção “Action”, escolha a opção “drop”
- Clique no botão “Comment” e digite um comentário para a nova regra criada

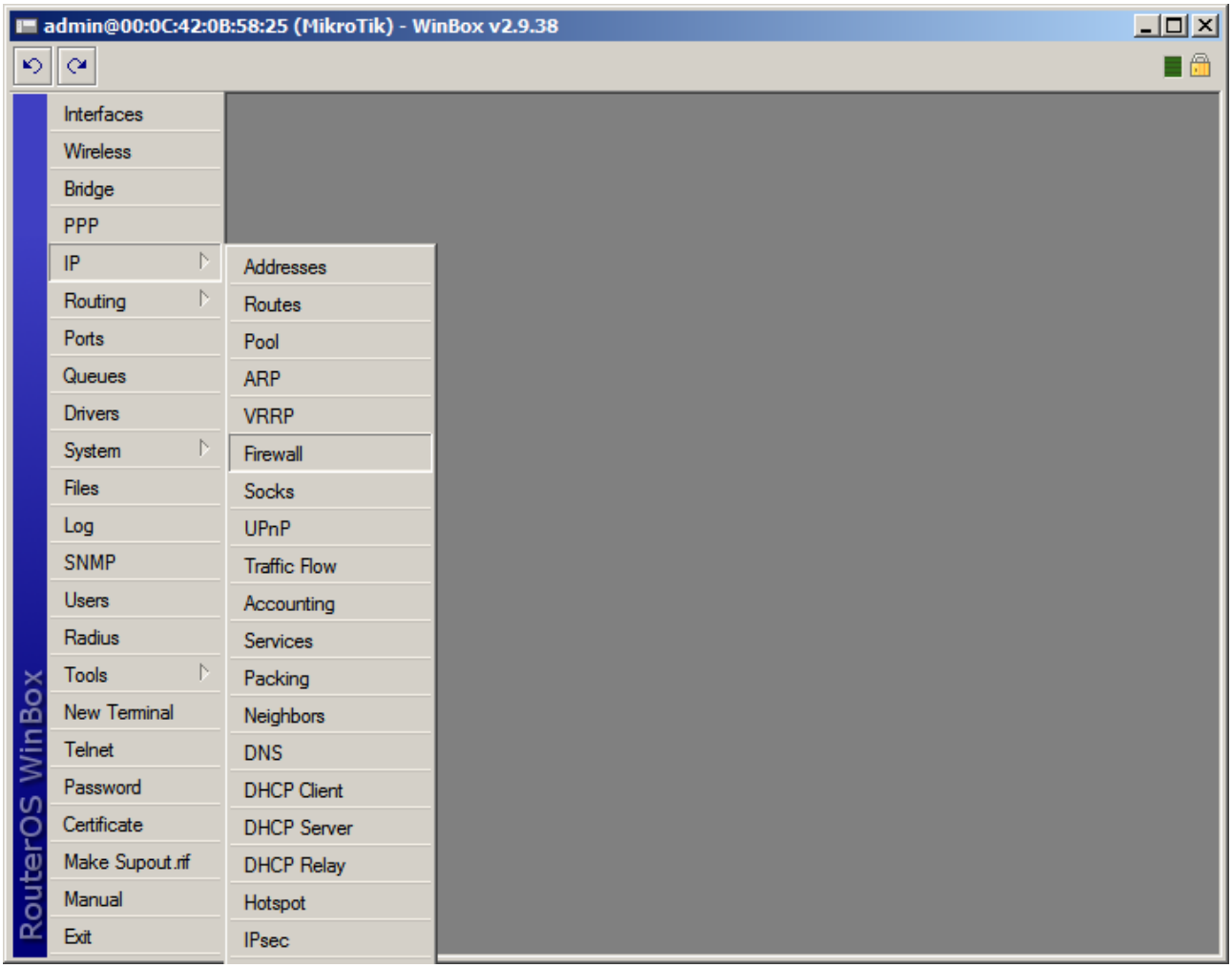


- Clique no botão “Ok”

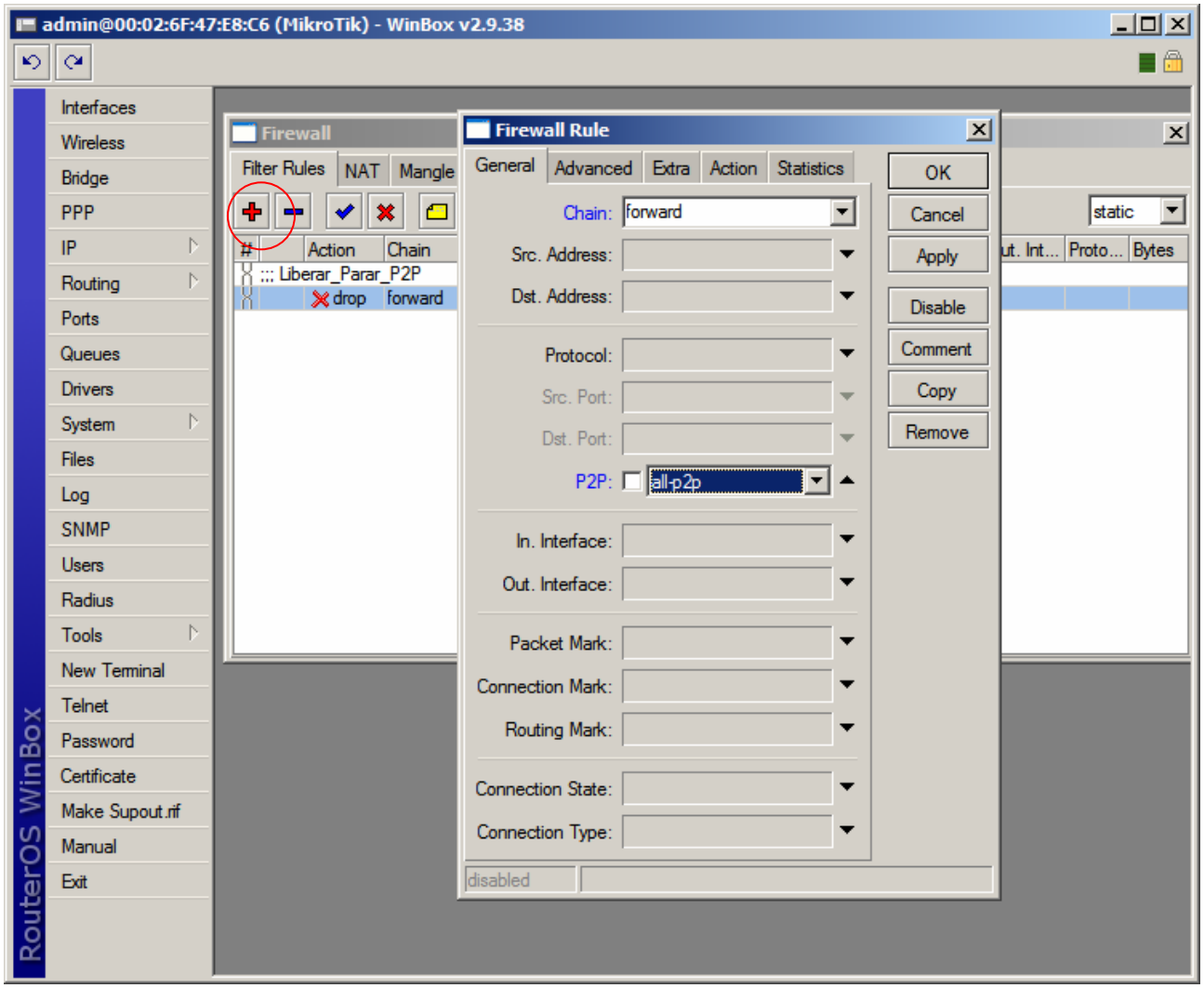
DESABILITAR E HABILITAR CONEXÕES P2P

Você pode criar uma regra do Firewall e usar Scripts para habilitar ou desabilitar essa regra com apenas um clique.

- Clique no menu “IP”
- Clique na opção “Firewall”

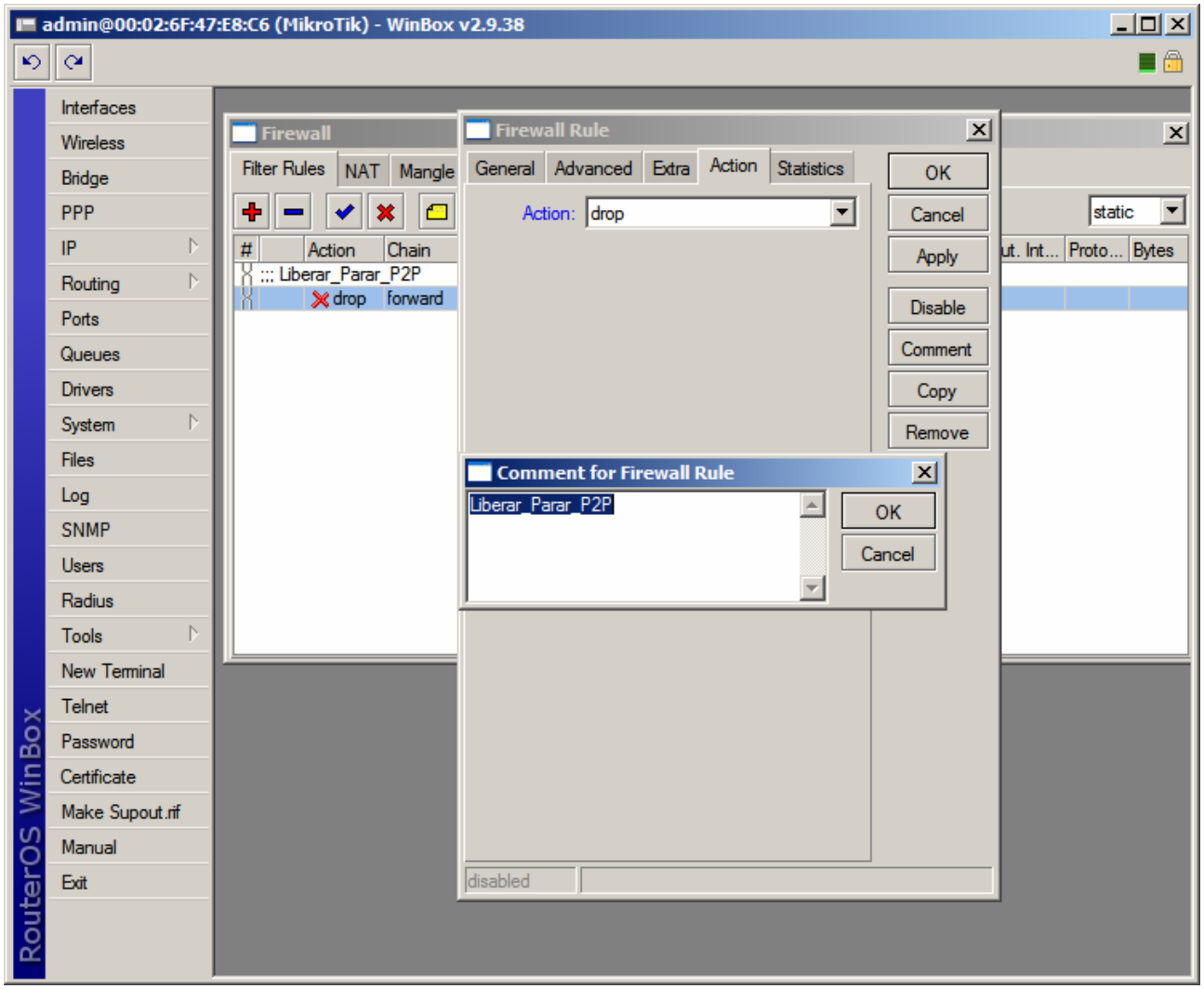


- Clique em “Adicionar”
- Na guia General, na opção “Chain”, escolha a opção “forward”
- Na opção P2P, escolha a opção “all-P2P”



- Clique no botão “Apply”

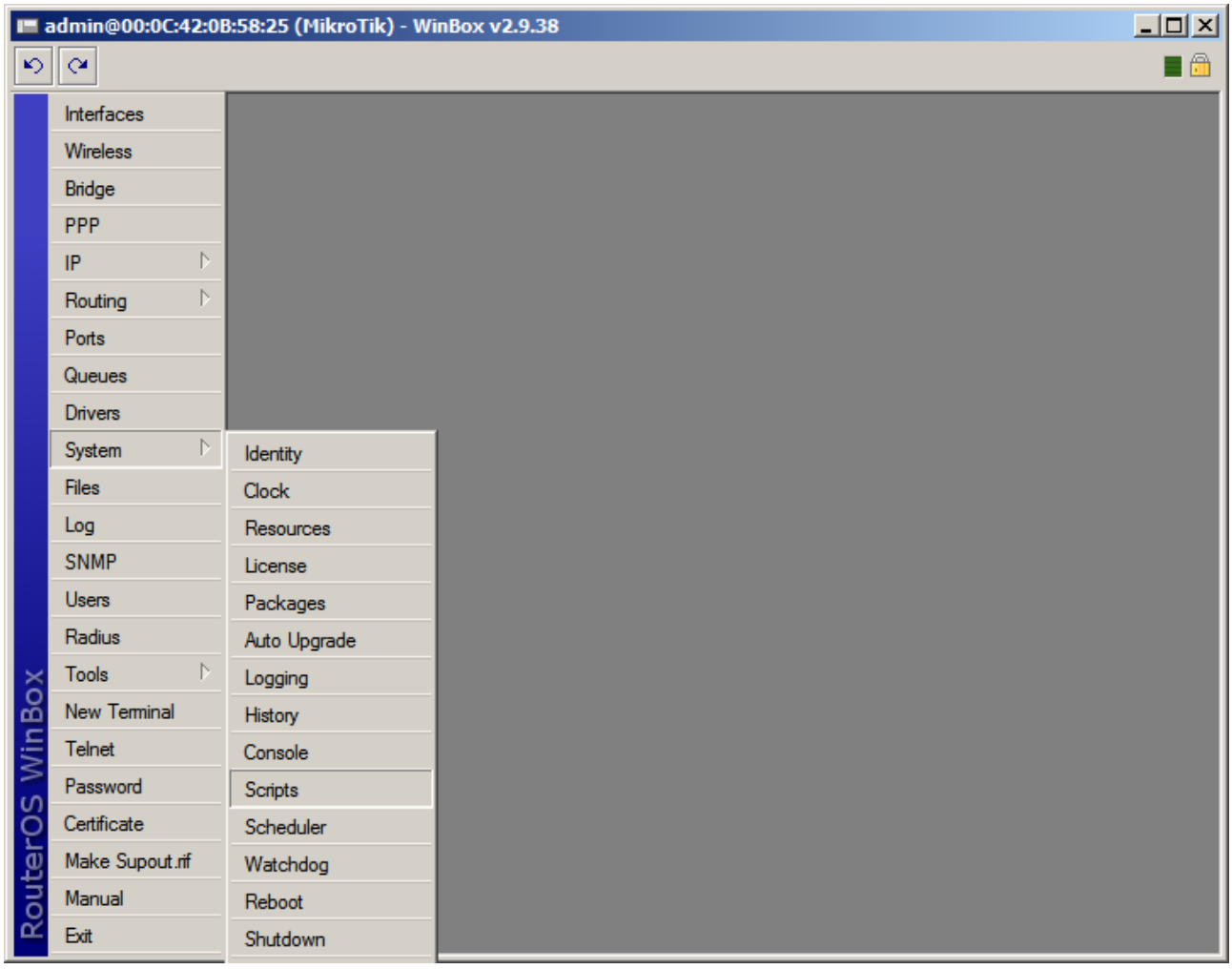
- Clique na guia “Action”
- Na opção “Action”, escolha a opção “drop”
- Clique no botão “Comment”
- Digite uma identificação para a nova regra que está sendo criada



- Clique no botão “OK”
- Clique no botão “OK”

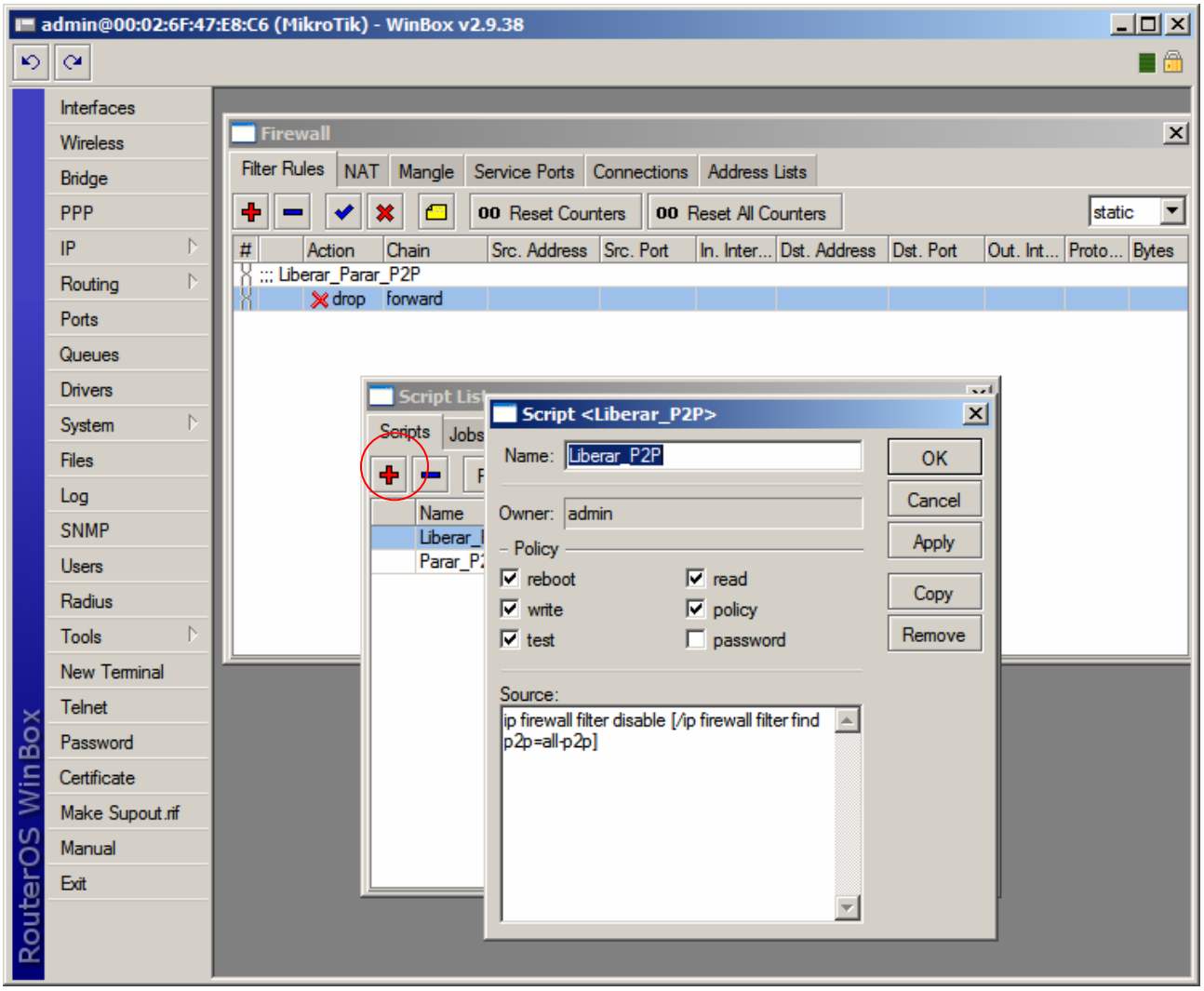
Criando Scripts

- Clique no menu “System”
- Clique na opção “Scripts”



- Clique em “Adicionar”
- No campo “Name”, digite: Liberar_P2P
- Na opção “Policy”, desative a opção “password”
- No campo Source, digite o seguinte script:

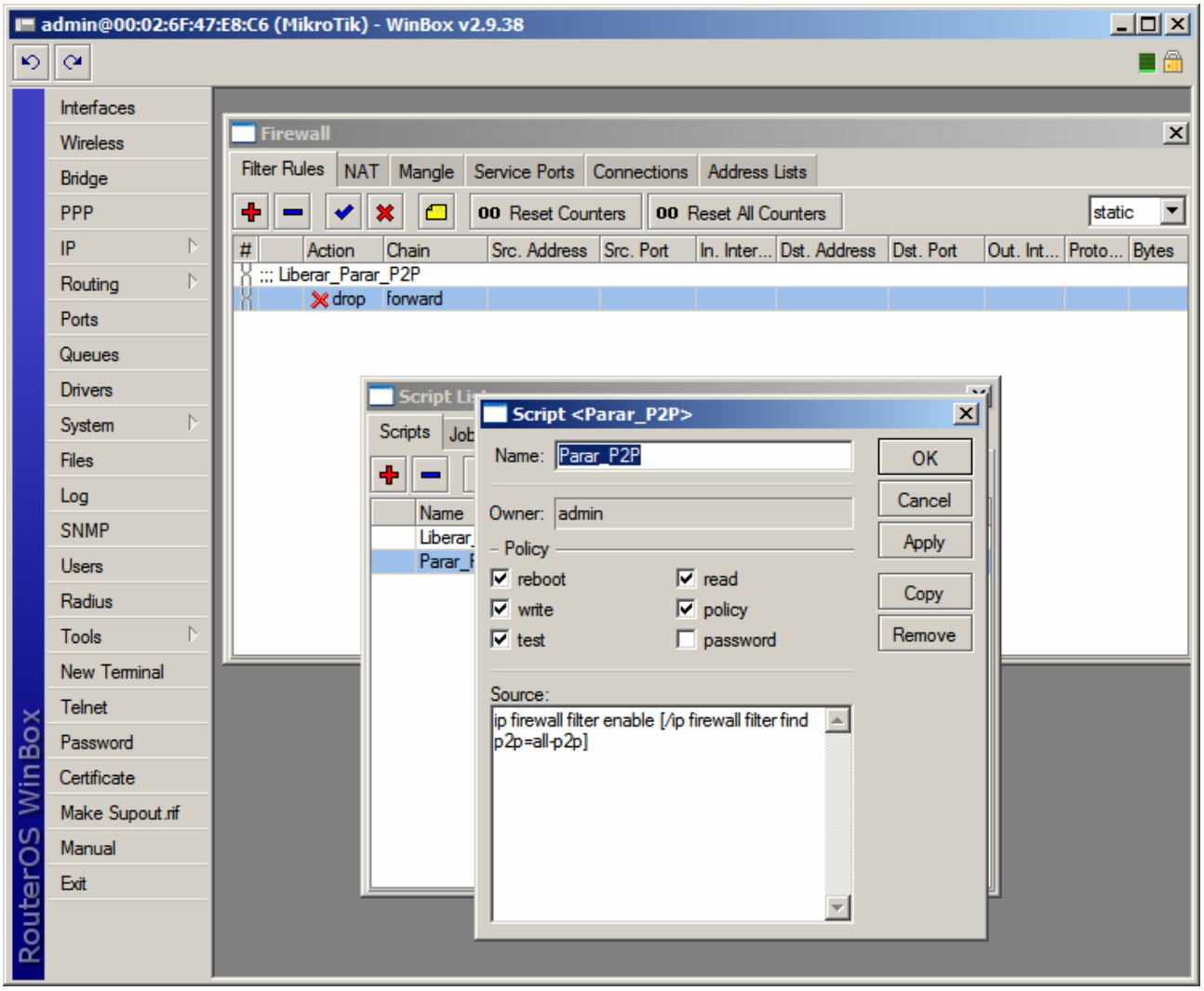
ip firewall filter disable [/ip firewall filter find p2p=all-p2p]



- Clique no botão “OK”

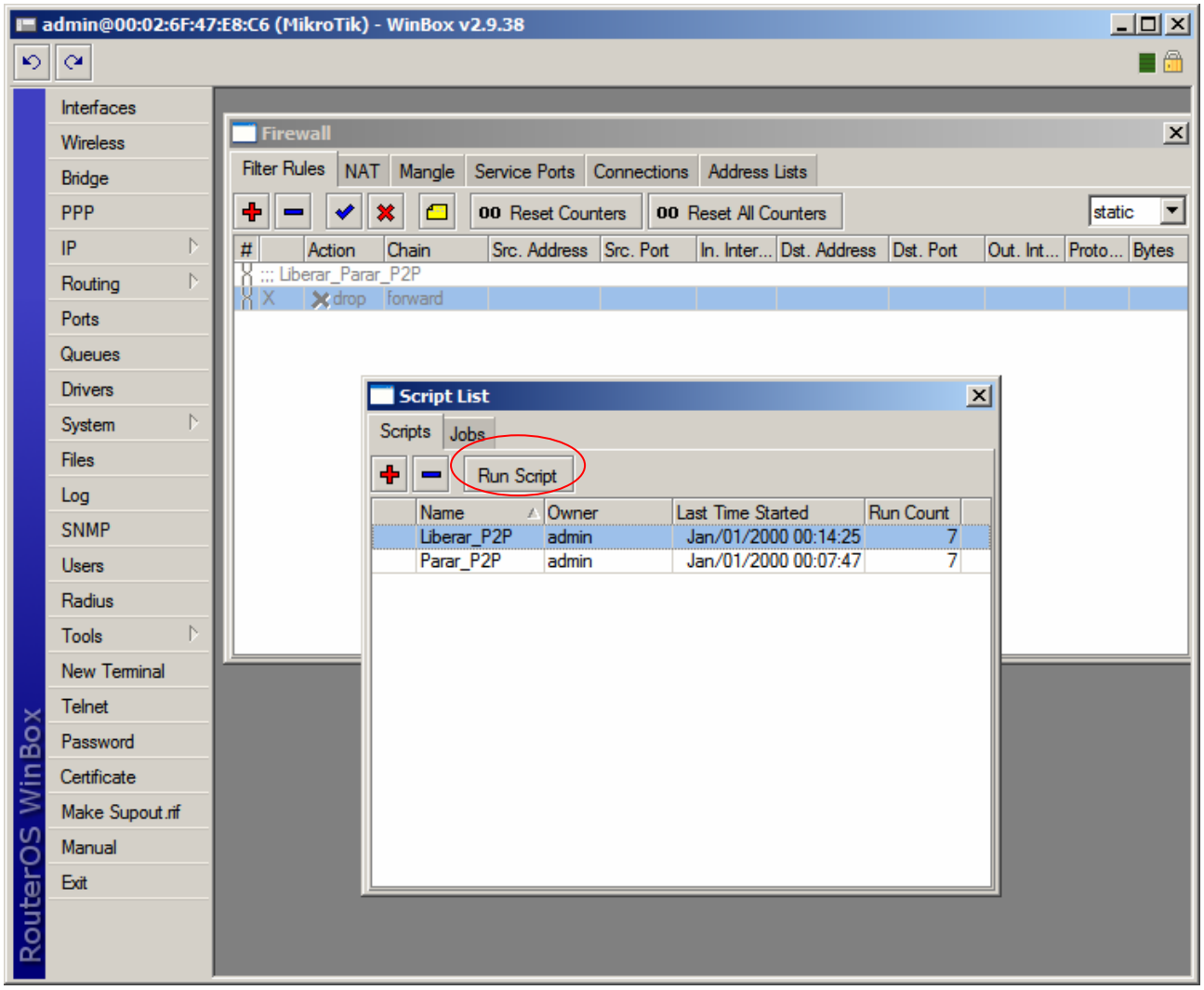
- Clique em “Adicionar”, novamente
- No campo “Name”, digite: Parar_P2P
- Na opção “Policy”, desative a opção “password”
- No campo Source, digite o seguinte script:

ip firewall filter enable [/ip firewall filter find p2p=all-p2p]

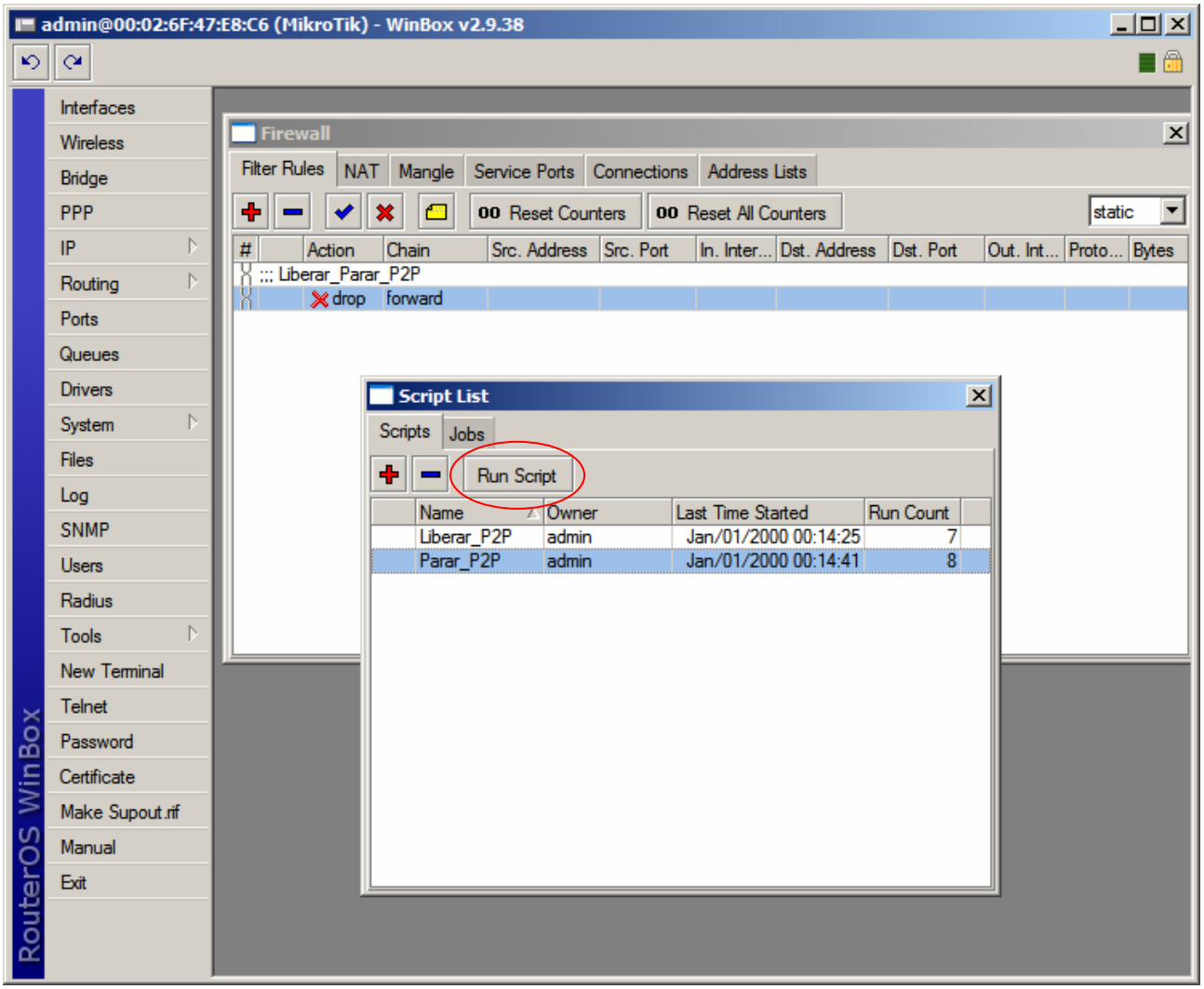


- Clique no botão “OK”

- Se você clicar no Script “Liberar_P2P” e clicar no botão “Run Script”, de acordo com o script, a regra do firewall ficará desabilitada.

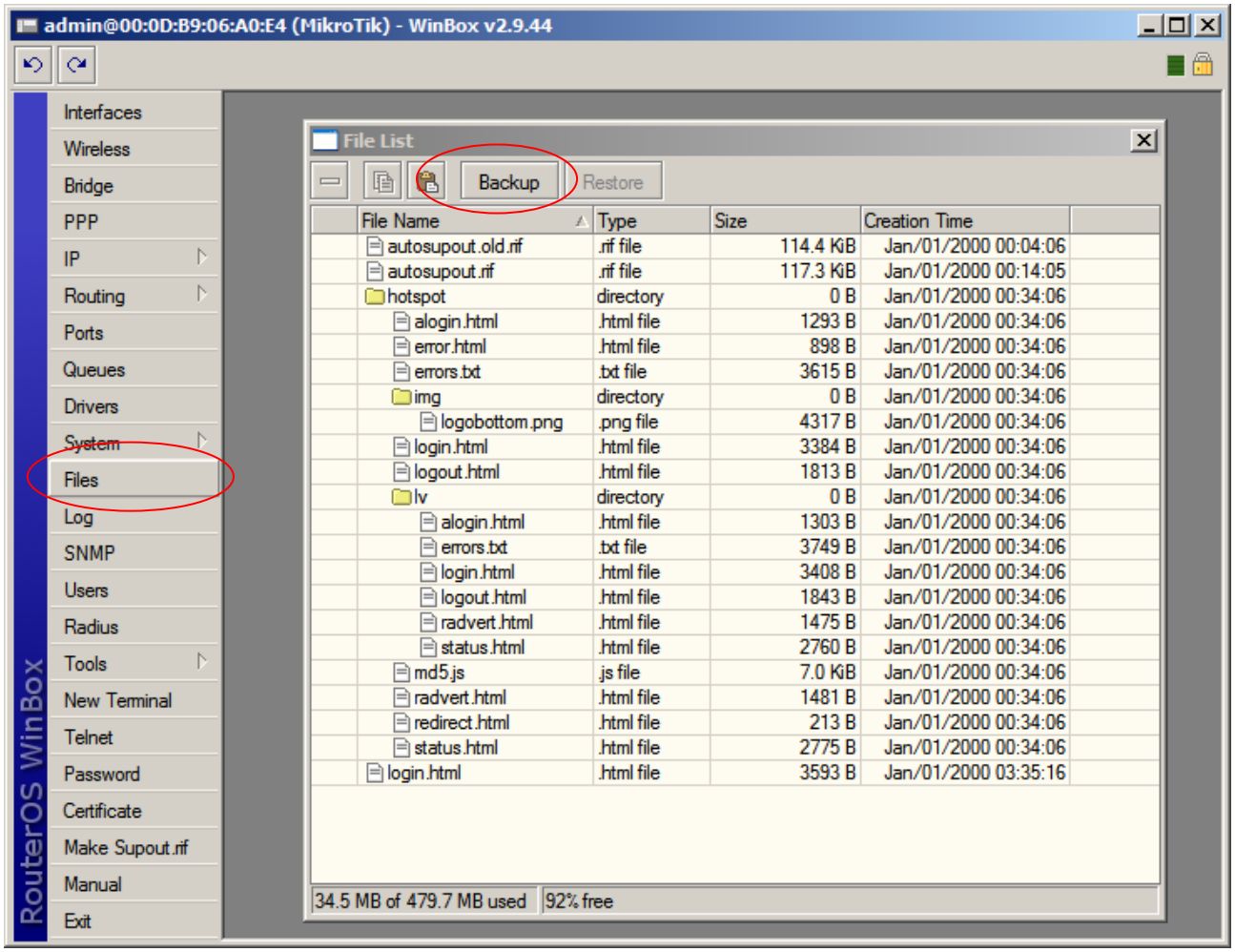


- Se você clicar no Script “Parar_P2P” e clicar no botão “Run Script”, de acordo com o script, a regra do firewall ficará habilitada.



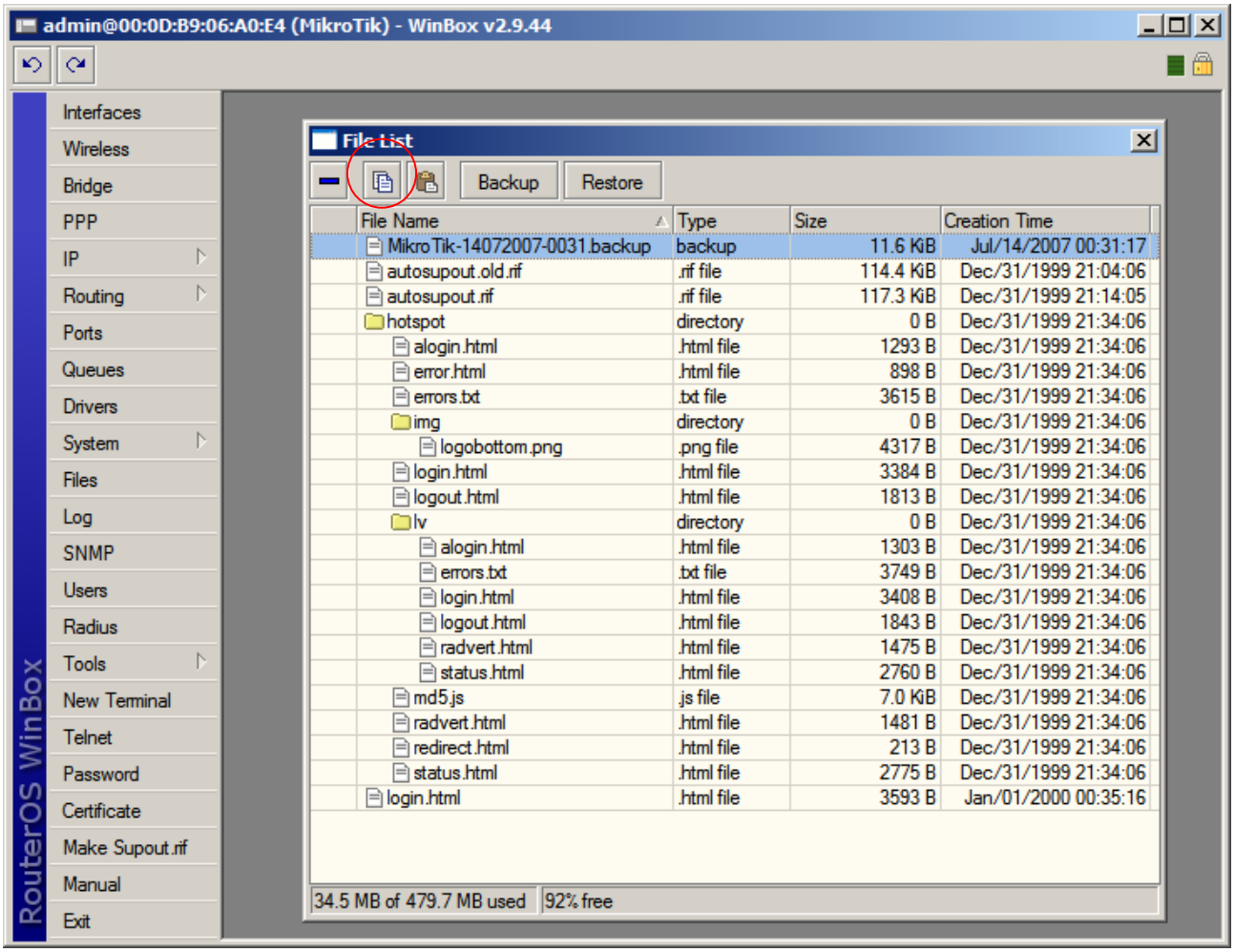
FAZENDO BACKUP E RESTAURANDO O BACKUP

BACKUP
- Clique no menu “Files”
- Para fazer o Backup, clique no botão backup



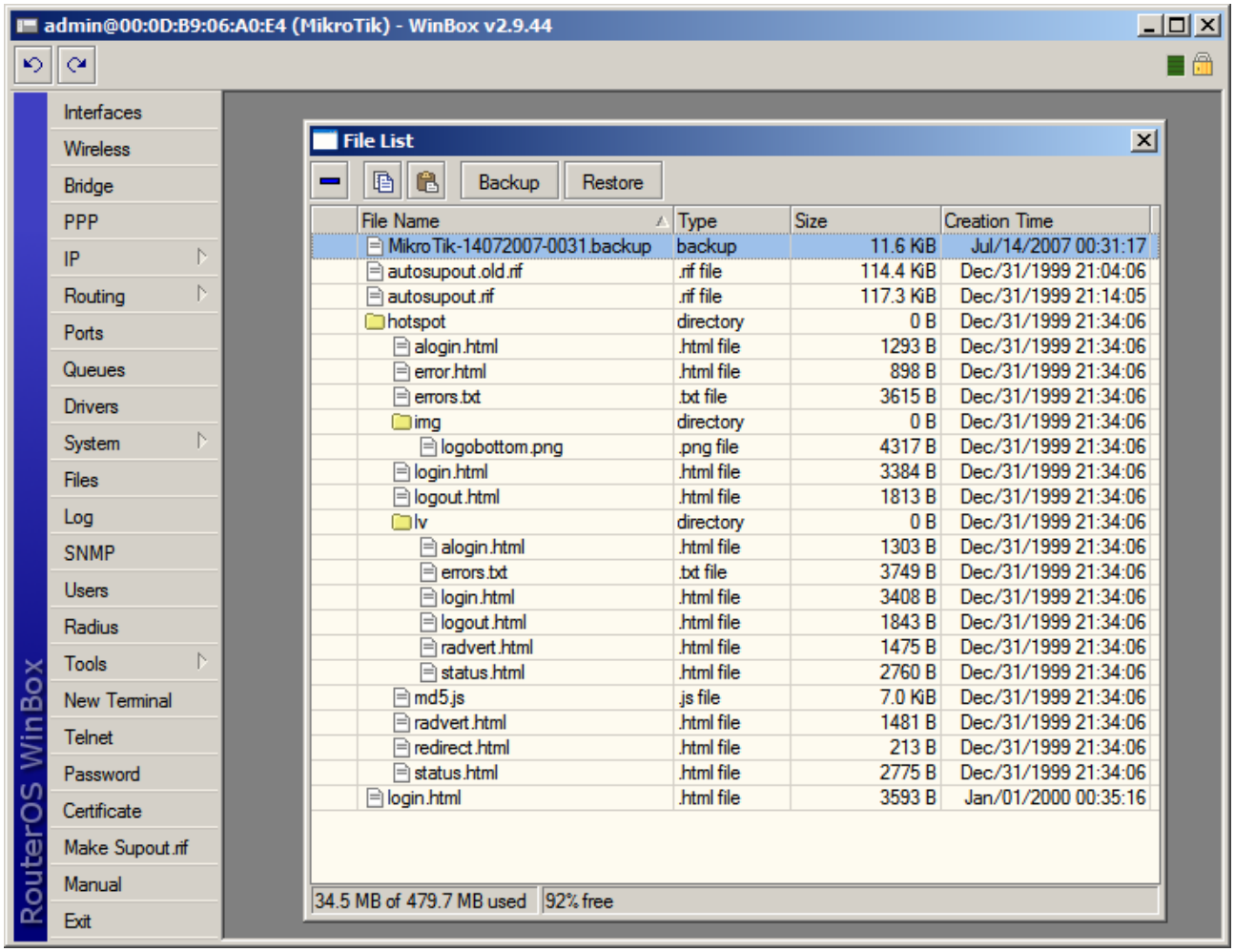
- O mikrotik irá gerar o backup dos arquivos em um arquivo com a extensão ".backup".

Observação: É recomendável que o arquivo seja copiado para algum lugar fora do Mikrotik. No caso do Windows, selecione o arquivo ".backup", clique no botão "copiar". No Windows Explorer, cole em sua pasta de preferência.

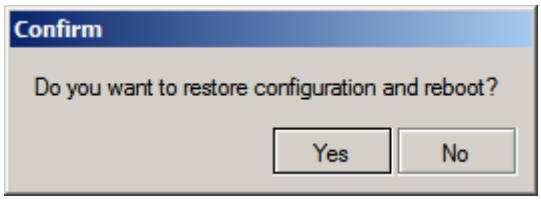


RESTAURANDO O BACKUP

- Selecione o arquivo com a extensão ".backup" e clique no botão "Restore"



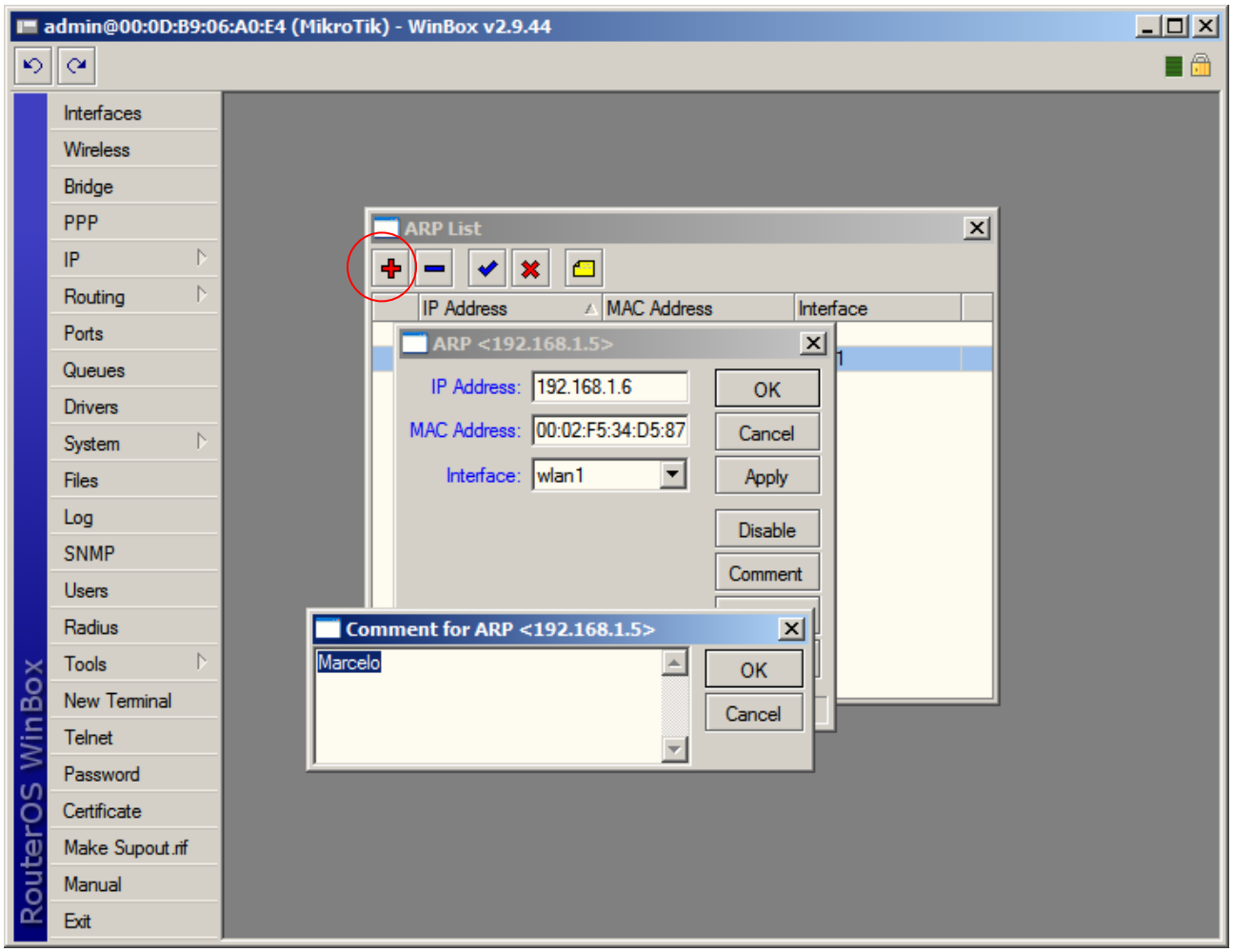
Na janela de confirmação, clique em "Yes". O Router será reiniciado.



ATRELANDO IP AO MAC

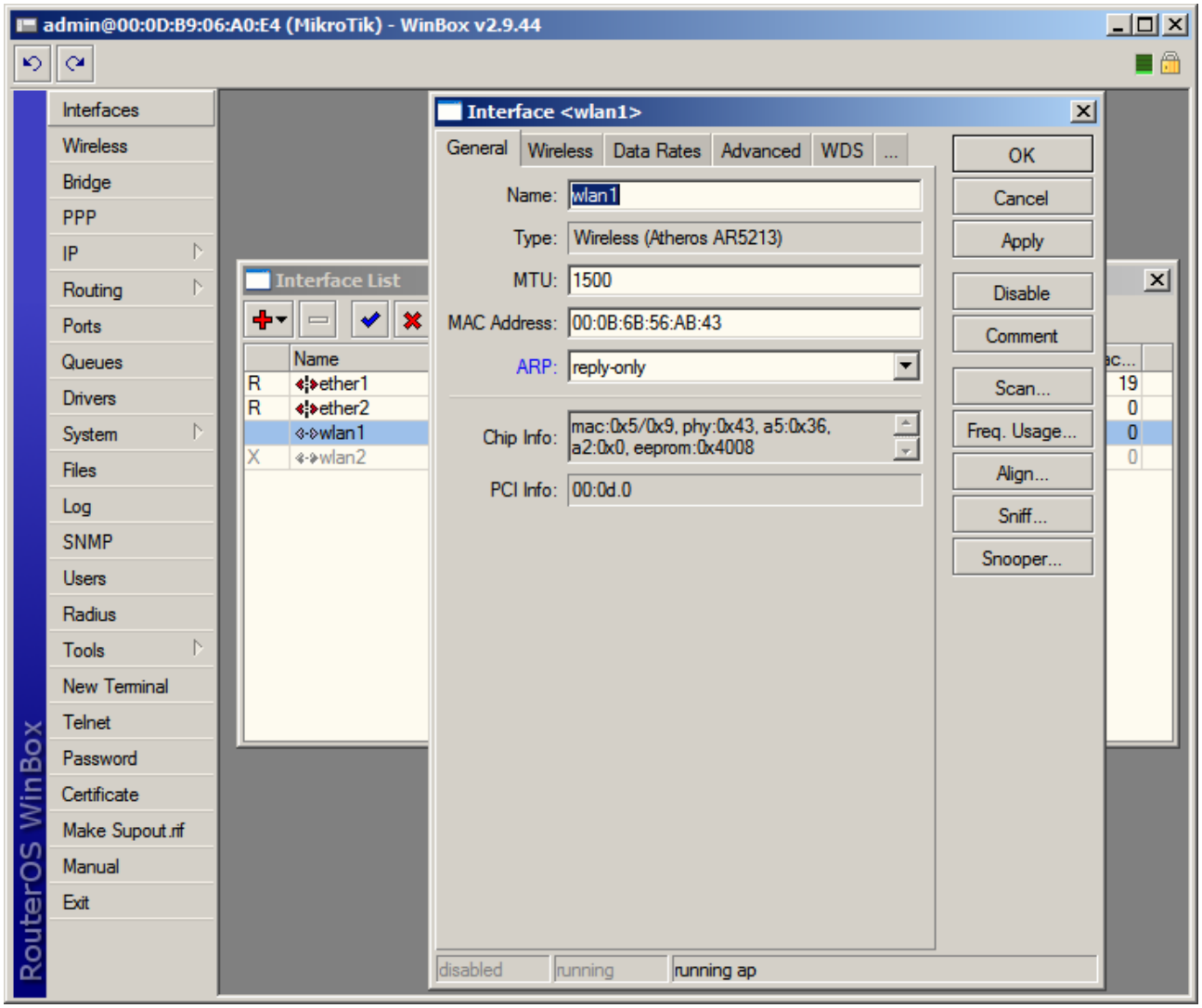
- Clique no menu “IP”
- Clique na opção “ARP”

- Clique em “Adicionar”
- Na opção “IP Address”, digite o IP do cliente
- Na opção “MAC Address”, digite o MAC do cliente
- Na opção “Interface”, escolha a interface na qual o cliente irá se conectar.
- Clique no botão “Comment” e digite algo para identificar a entrada (por exemplo: nome do cliente)
- Clique no botão “OK”
- Clique no botão “OK”



- Clique no menu “Interfaces”

- Dê um clique duplo na interface que estará recebendo os clientes com o atrelamento de IP ao MAC.
- Na guia “General”, na opção “ARP”, escolha a opção “reply-only”
- Clique no botão “OK”



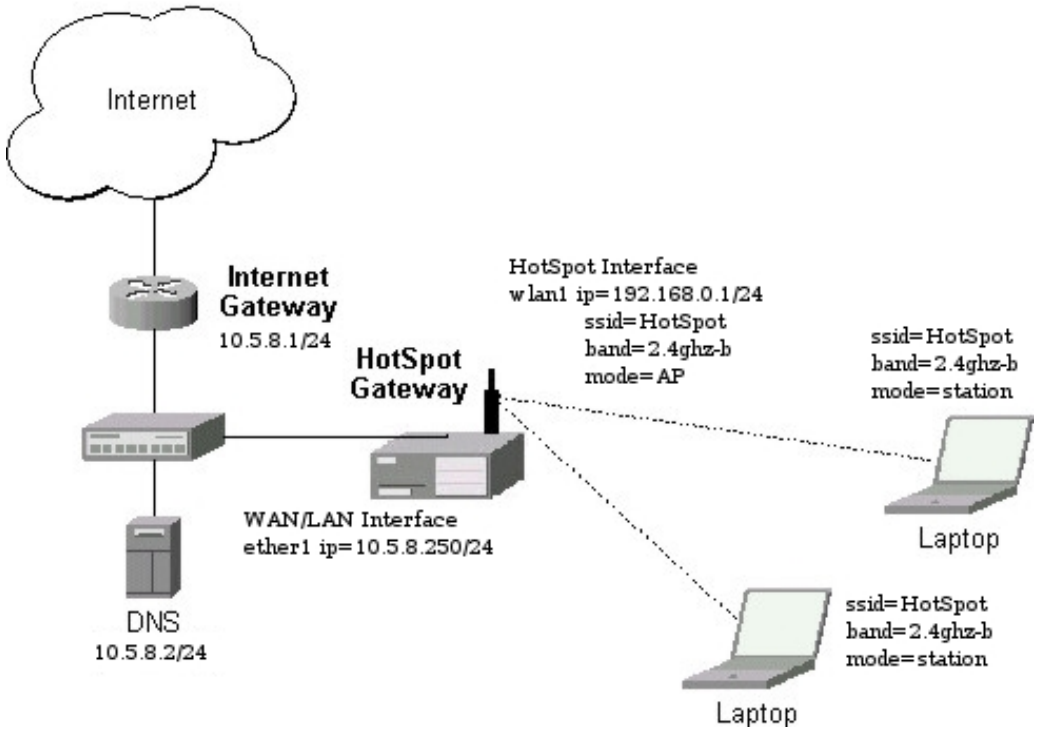
HOTSPOT

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

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

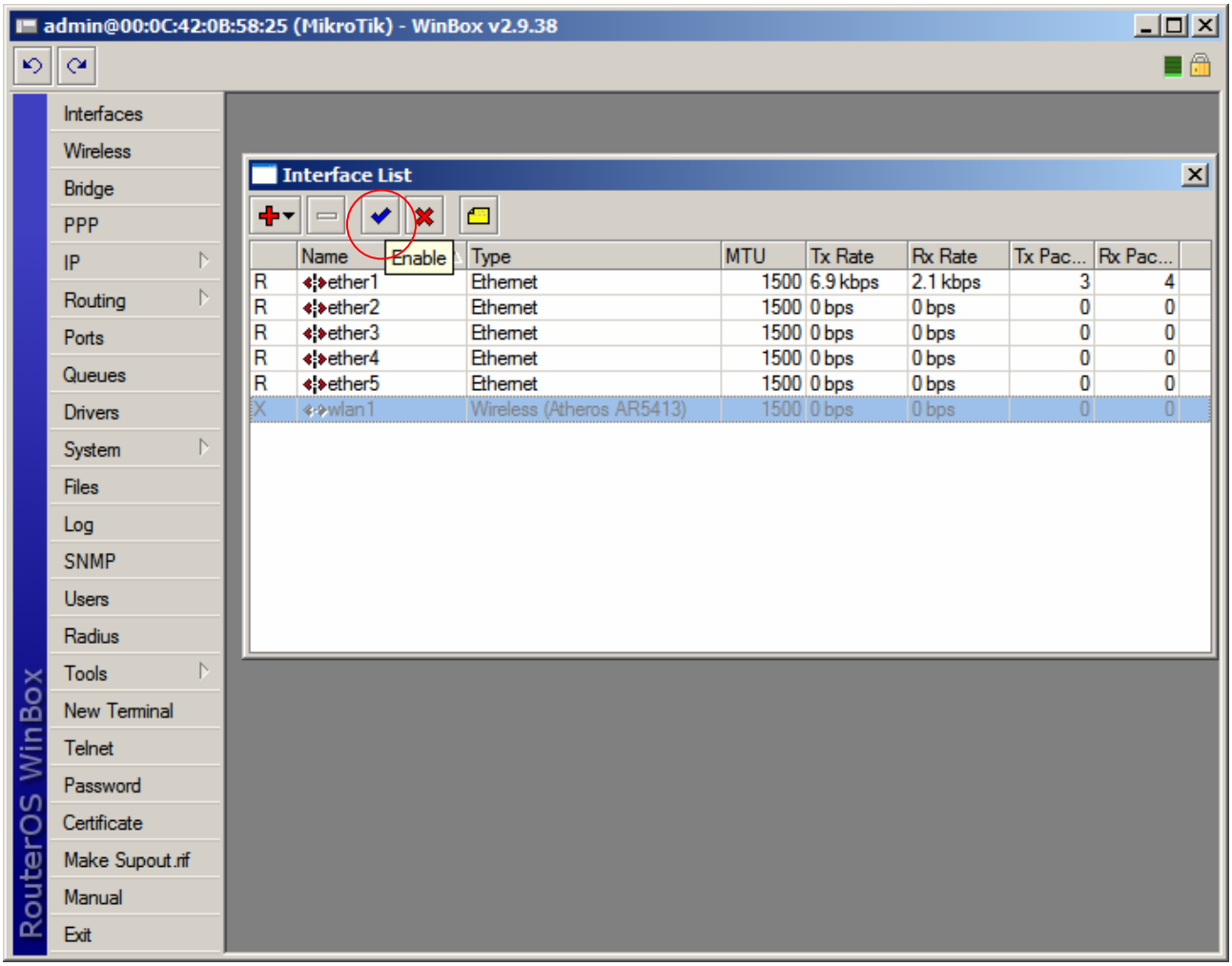
Quando em uma área coberta por um Hotspot, um usuário que possua um Laptop e tente navegar pela WEB é arremetido para uma página do Hotspot que pede suas credenciais, normalmente usuário e senha. Ao fornecê-las e sendo um cliente autorizado pelo Hotspot o usuário ganha acesso à internet, podendo sua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

Considerando a estrutura da imagem abaixo:

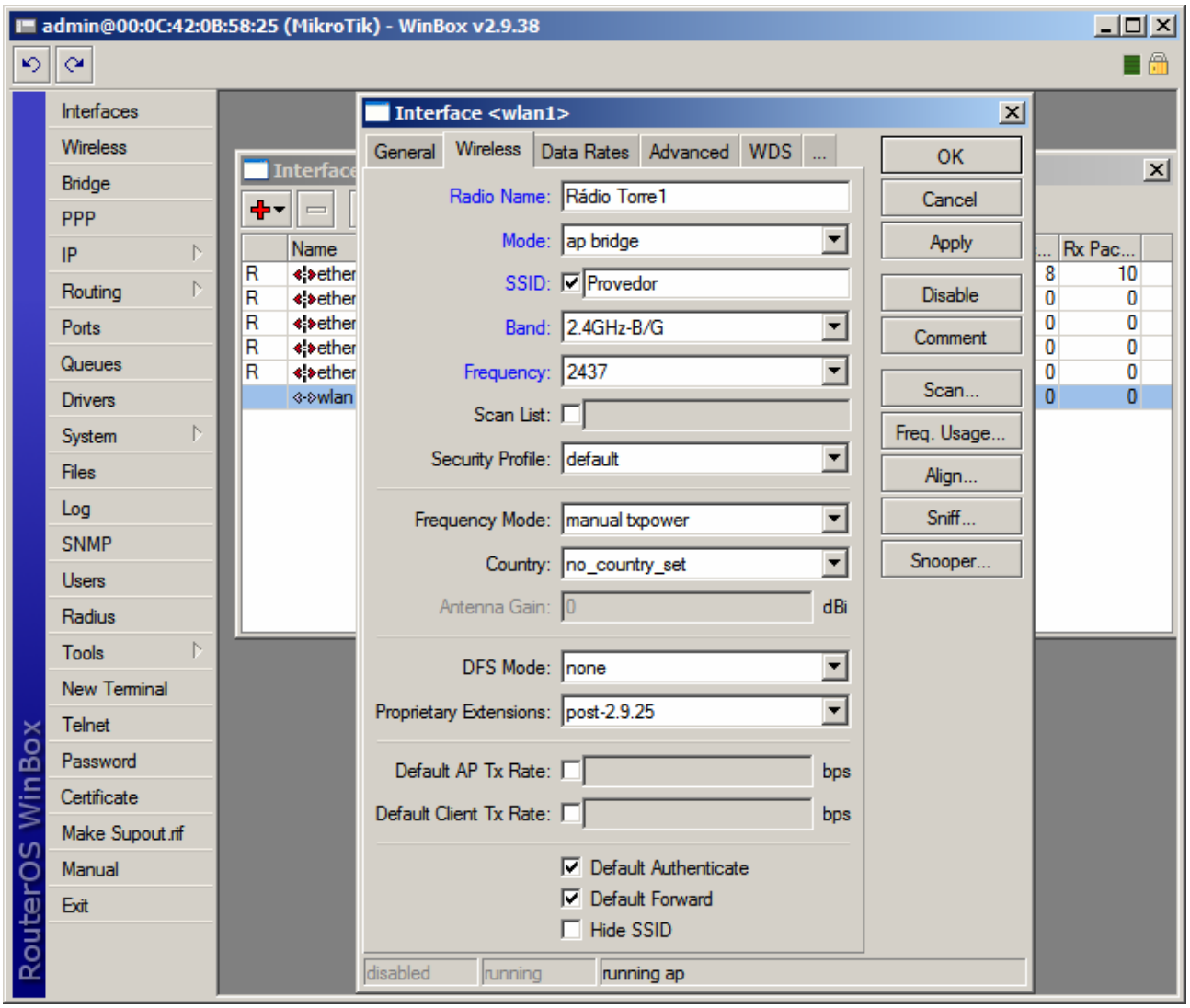


Primeiramente devemos habilitar as interfaces e configurar a interface que será o hotspot.

- Clique no menu Interfaces.
- Clique na interface Wlan desejada e clique no botão Habilitar



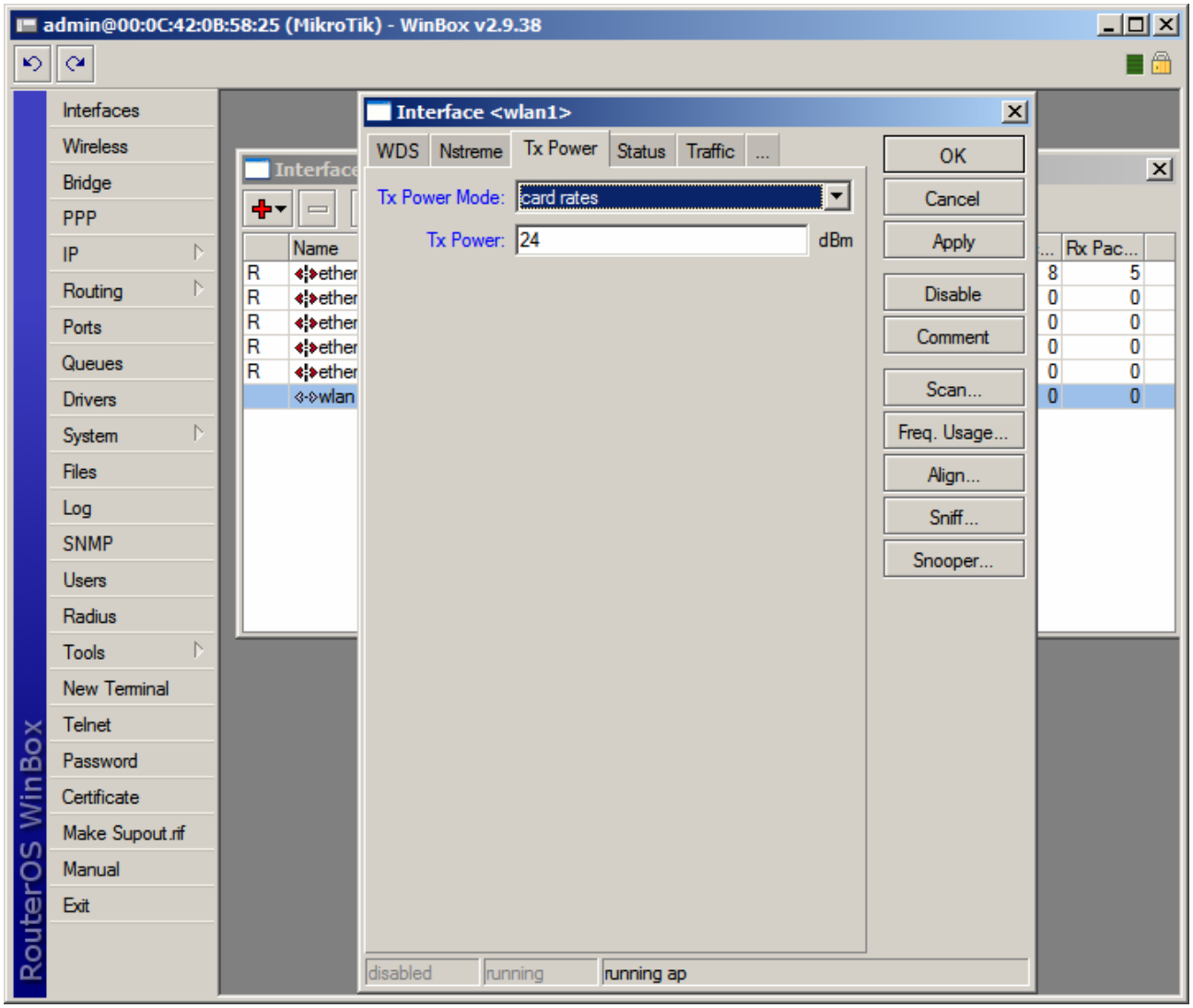
- Dê um clique duplo na interface habilitada
- Na guia Wireless, configure as opções:
- Opção “Radio Name”: Coloque nessa opção o nome que você deseja que o Rádio tenha na rede.
- Opção “Mode”: AP Bridge
- Opção “Band”: Escolha a Banda de Operação desejada
- Opção “Frequency”: Canal de operação do equipamento
- Clique no botão “OK”



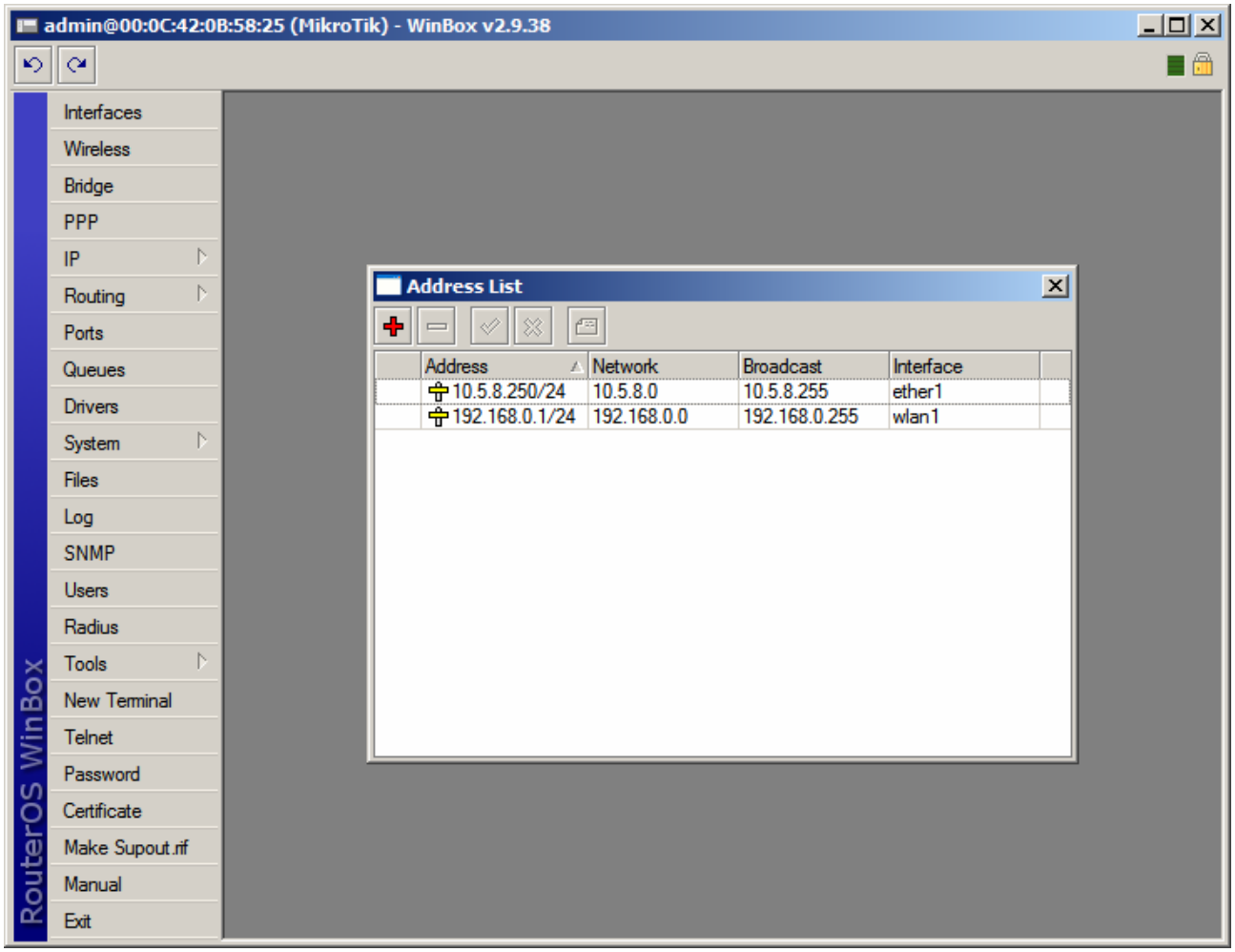
- Clique na guia “Tx Power” para escolher a potência do cartão, considerando:

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

Obs: Verifique a potência máxima permitida para o cartão utilizado antes de fazer a alteração.

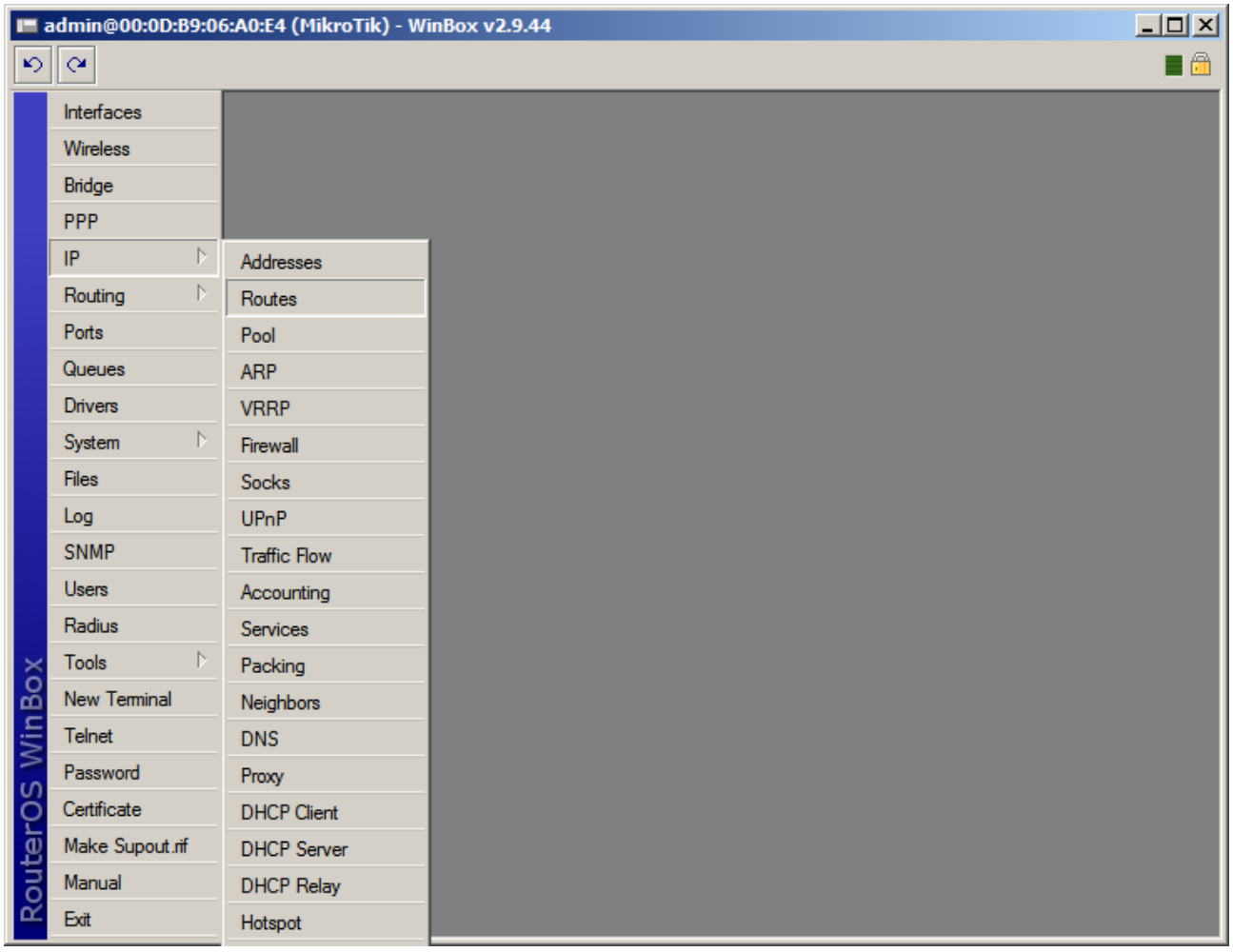


Devemos configurar os IPs para as suas respectivas interfaces:

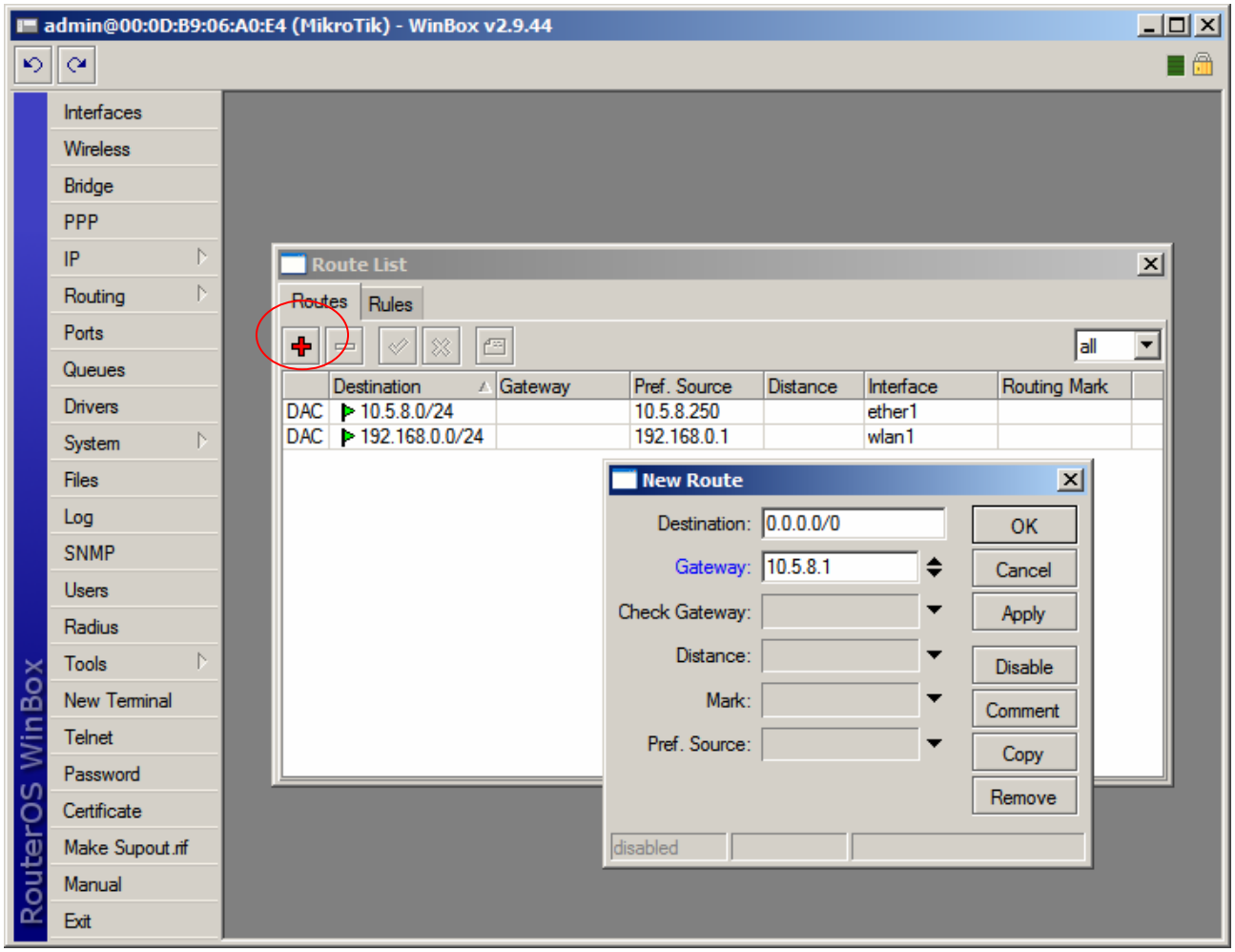


Devemos definir o Gateway de saída para a internet

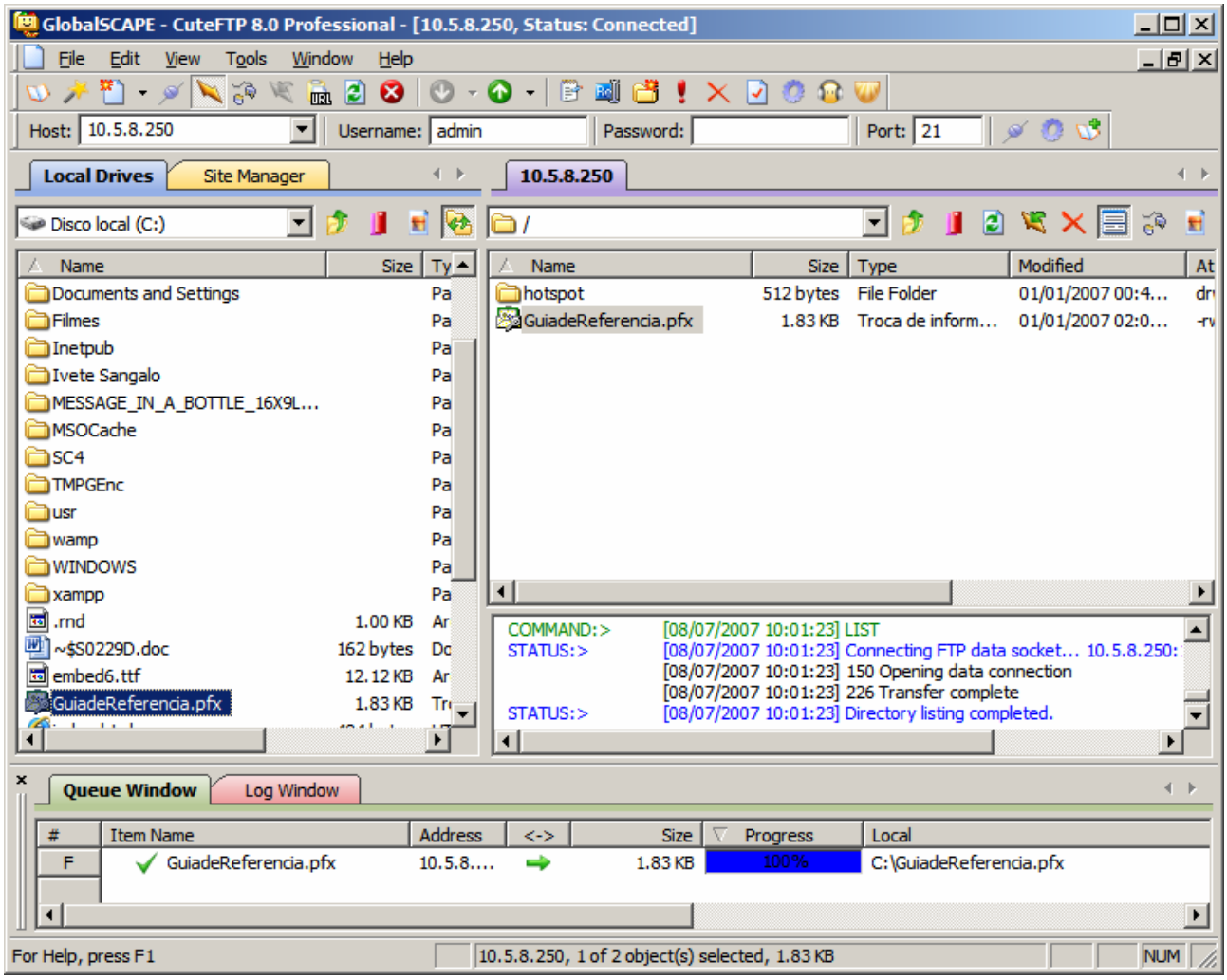
- Clique no menu “IP”
- Clique na opção “Routes”



- Clique em “Adicionar”
- No campo “Gateway”, digite o IP do servidor Gateway.
- Clique no botão “OK”



Se você possuir um Certificado de Segurança, faça a transferência dele para o Mikrotik através de FTP, utilizando qualquer cliente de FTP:

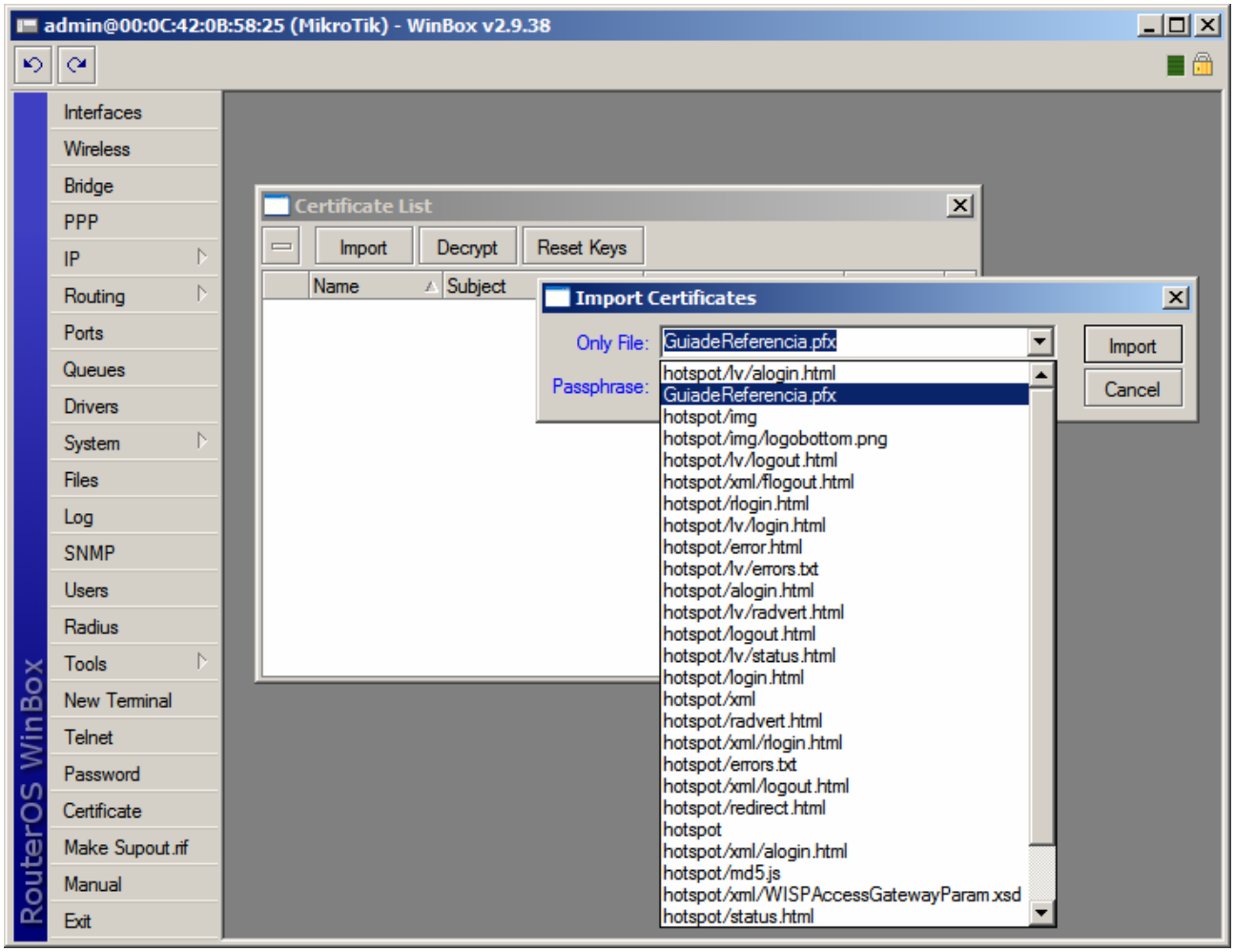


O QUE É SSL?
SSL (Secure Sockets Layer) é uma tecnologia de segurança que é comumente utilizada para codificar os dados trafegados entre o computador do usuário e o um website. O protocolo SSL, através de um processo de criptografia dos dados, previne que os dados trafegados possam ser capturados, ou mesmo alterados no seu curso entre o navegador (browser) do usuário e o site com o qual ele está se relacionando, garantindo desta forma informações sigilosas como login e senha, neste nosso caso.

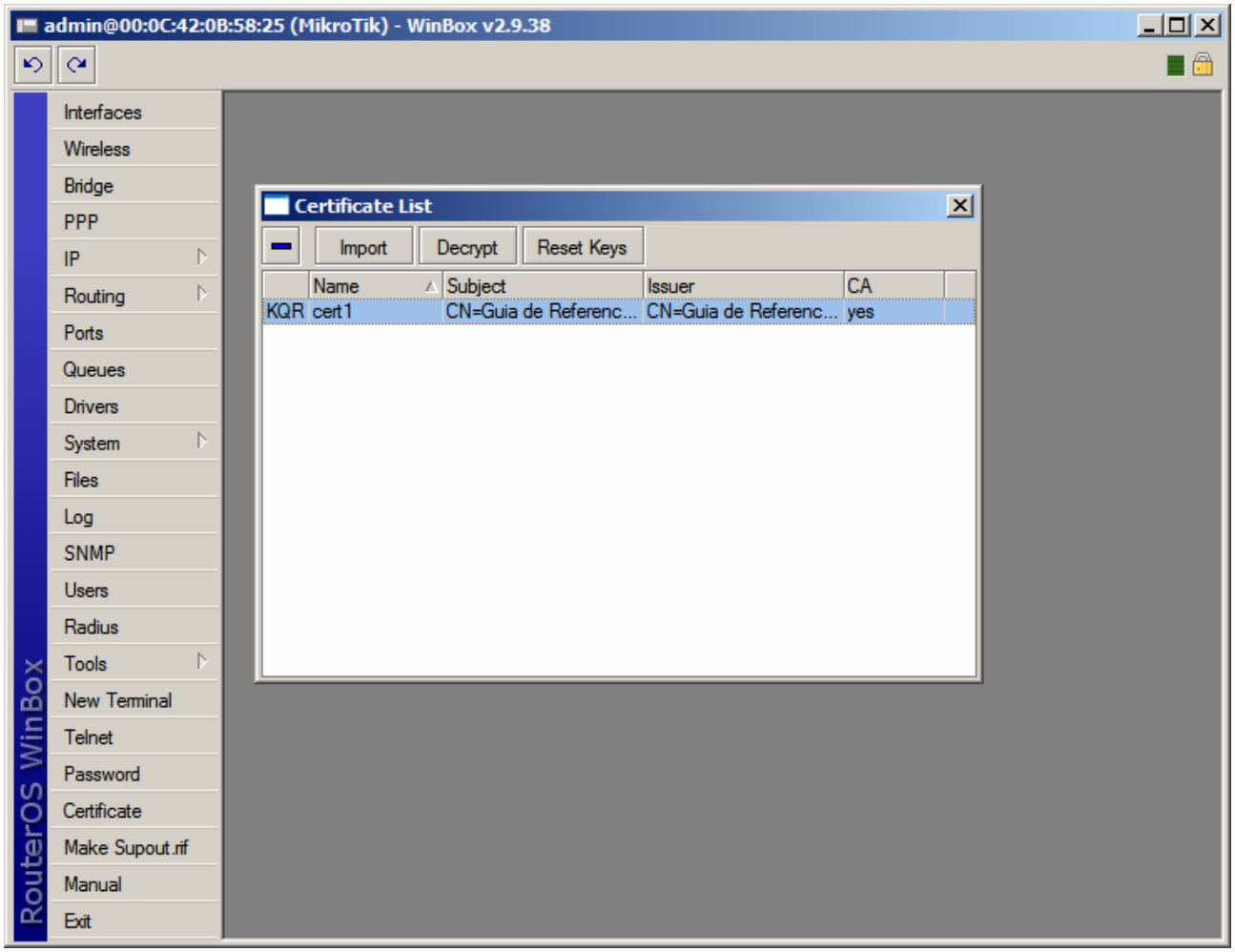
Uma sugestão: Pode-se contratar um Certificado de Segurança através do site:
http://www.laniway.com.br/br/corporativo/certificado.do;jsessionid=441CFD641B6F5981DE6594BF96E3D5FD

O próximo passo será fazer a importação do Certificado

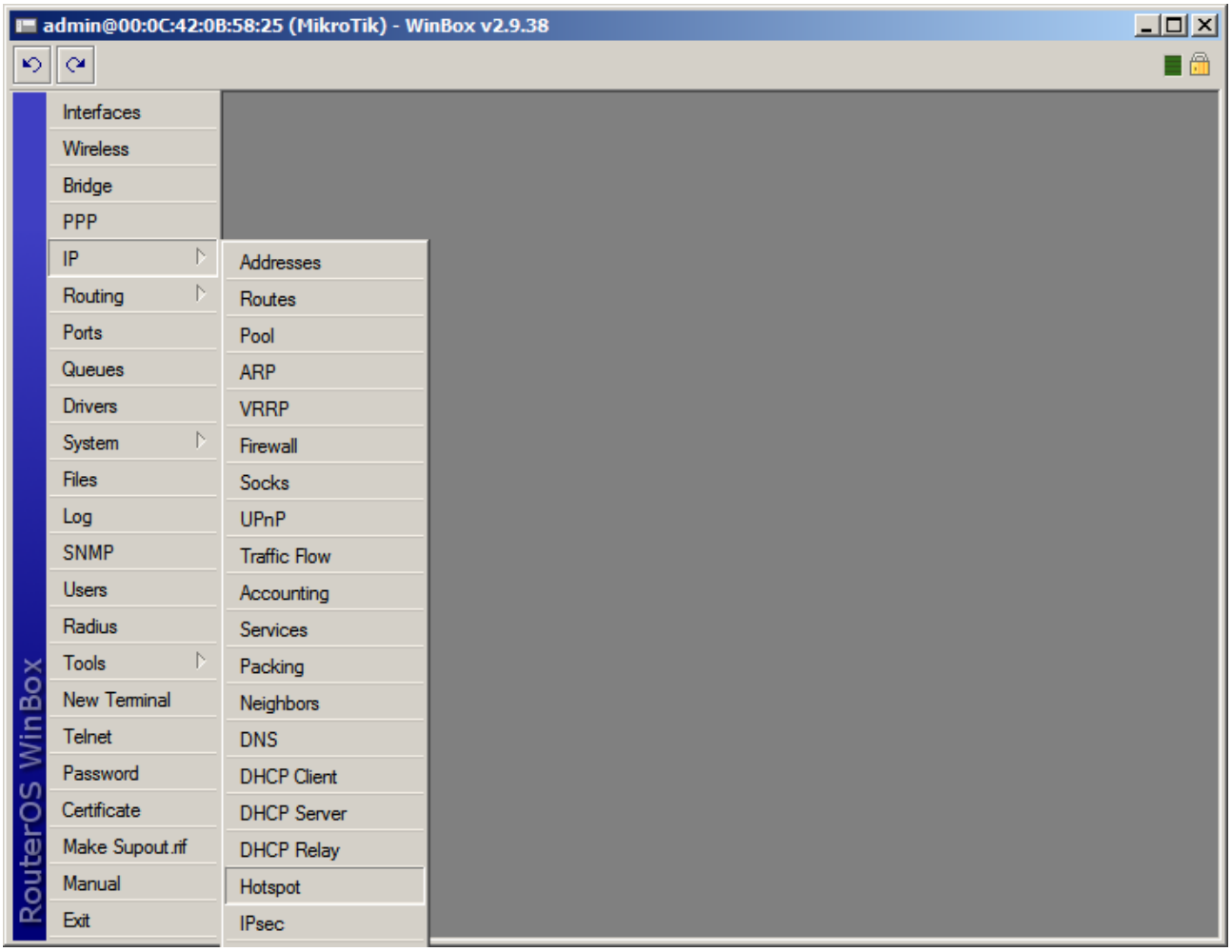
- Clique no menu “Certificate”
- Clique no botão “Import”
- Na opção “Only File”, escolha o Certificado que você transferiu anteriormente.
- Na opção “Passphrase”, digite a senha do seu Certificado
- Clique no botão “Import”



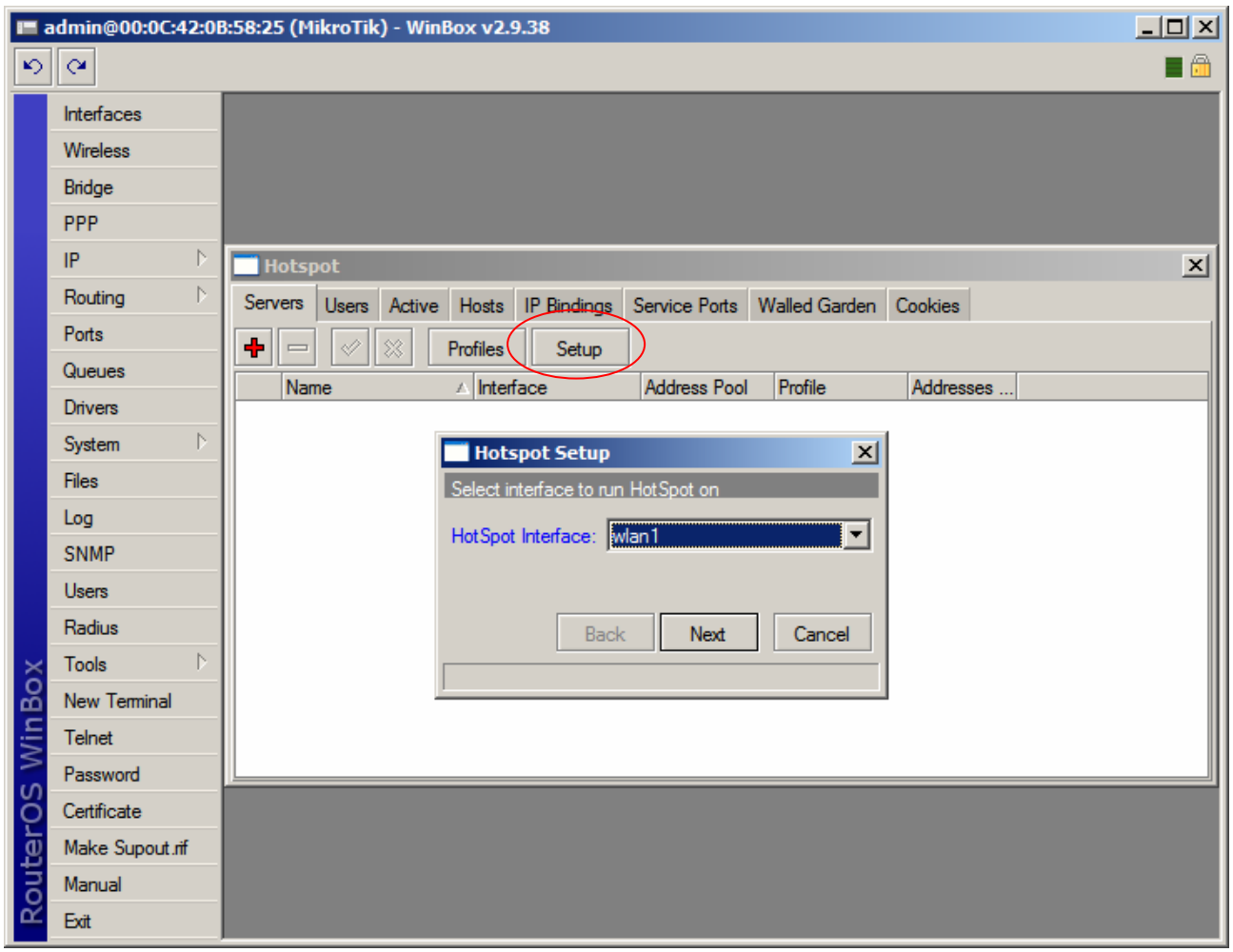
Seu Certificado estará importado



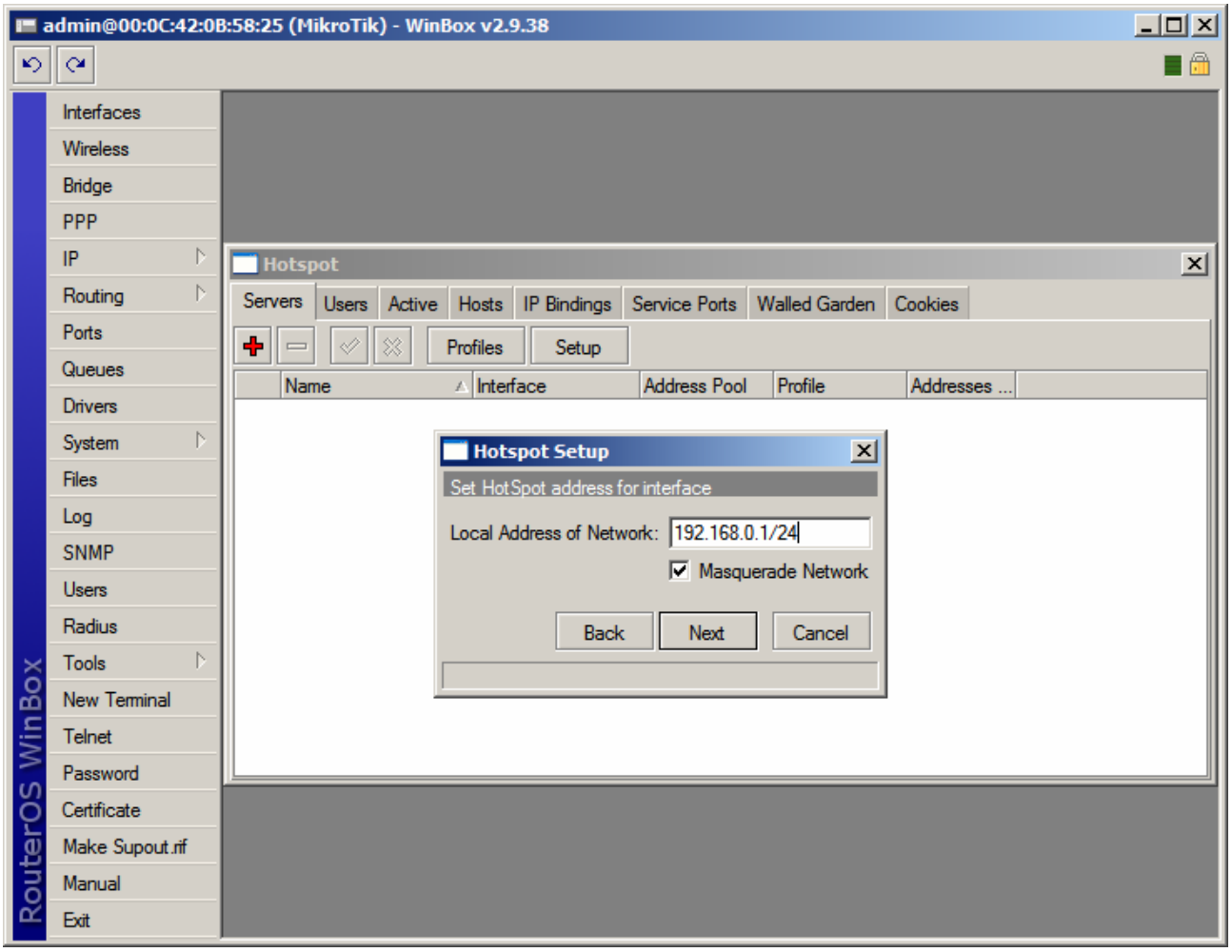
- Clique no menu “IP”
- Clique na opção “Hotspot”



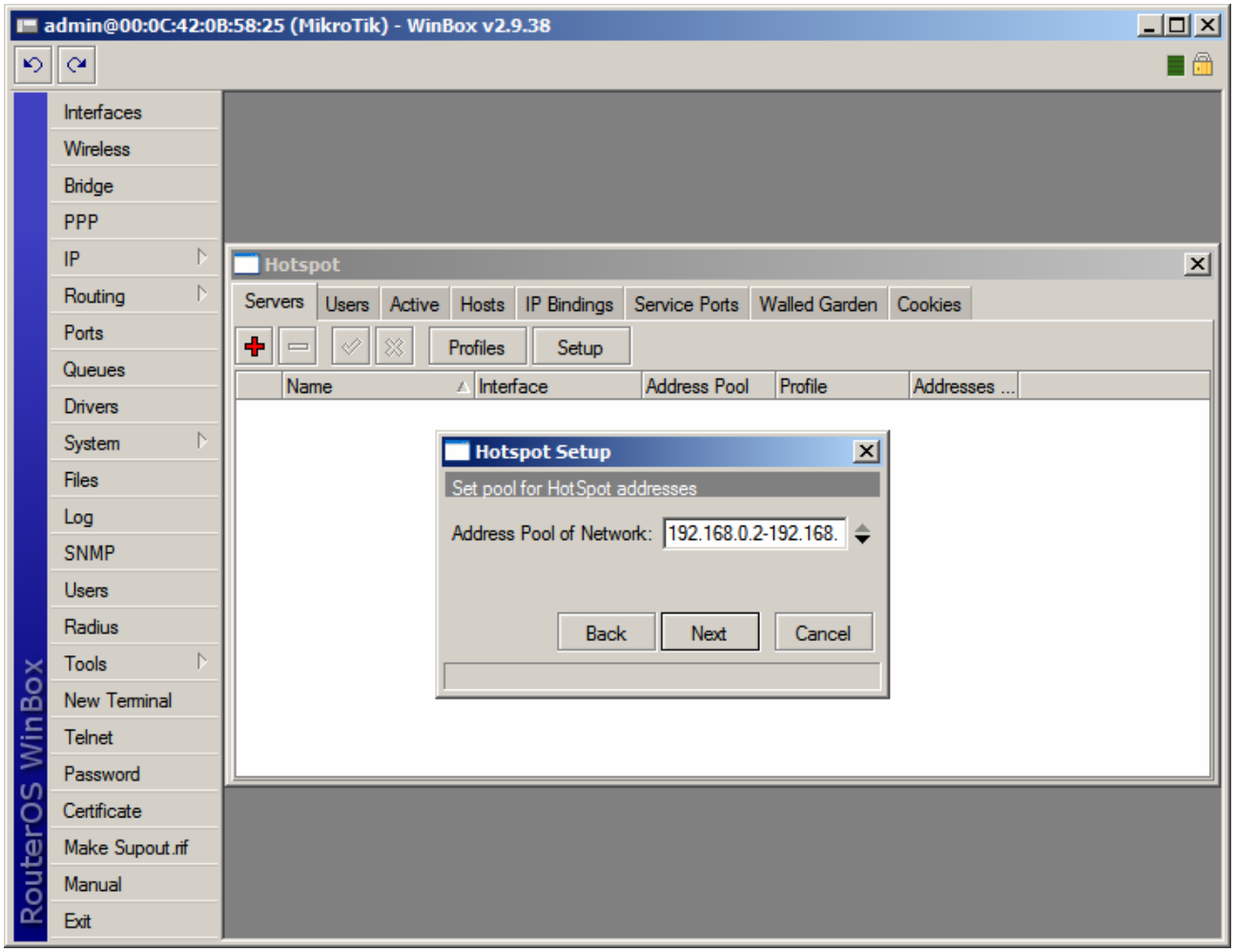
- Clique no botão “Setup”
- Selecione a interface onde os clientes se conectarão ao Hotspot.
- Clique no botão “Next”



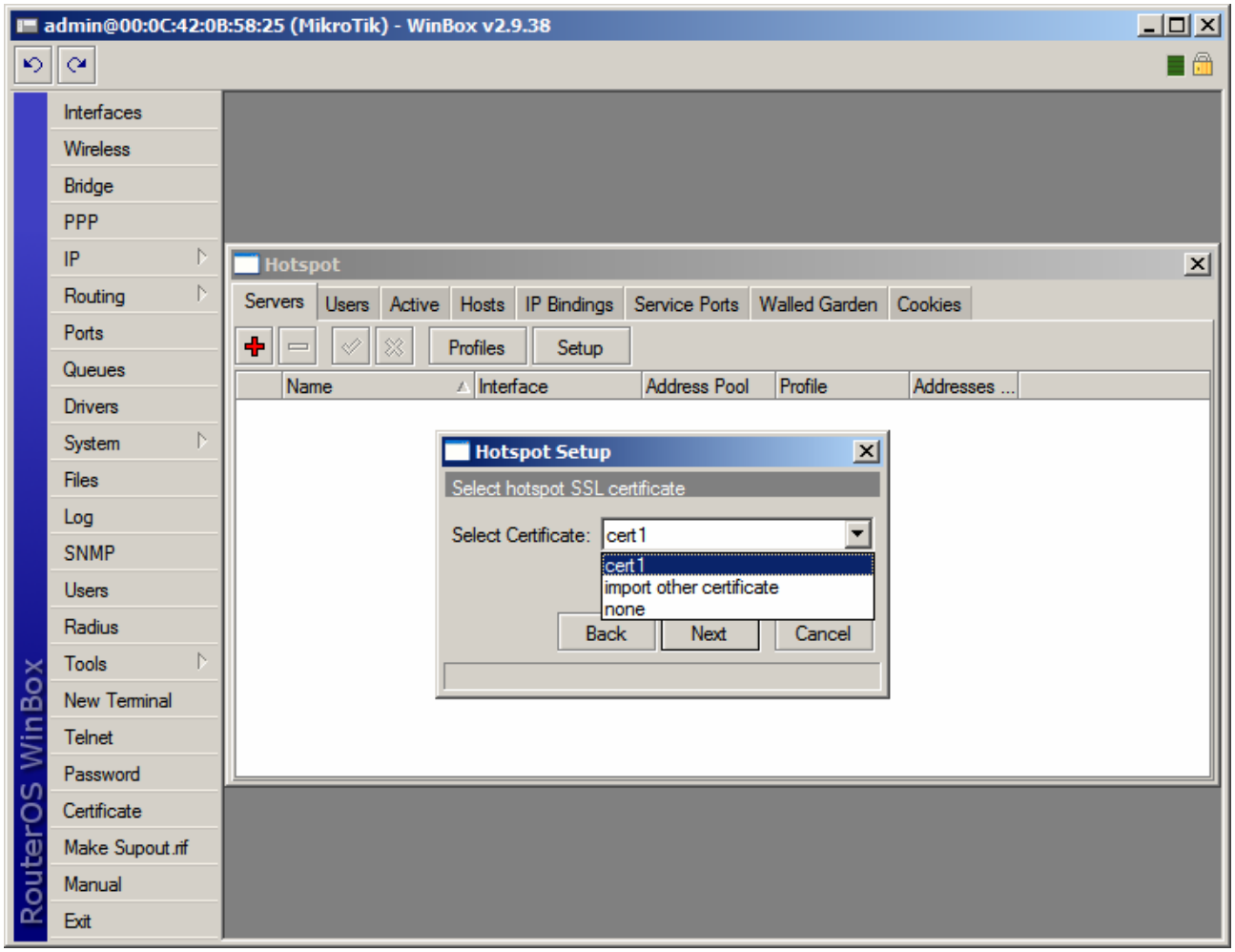
- No campo “Local Address of Network” aparecerá o IP da interface escolhida.
- Clique no botão “Next”



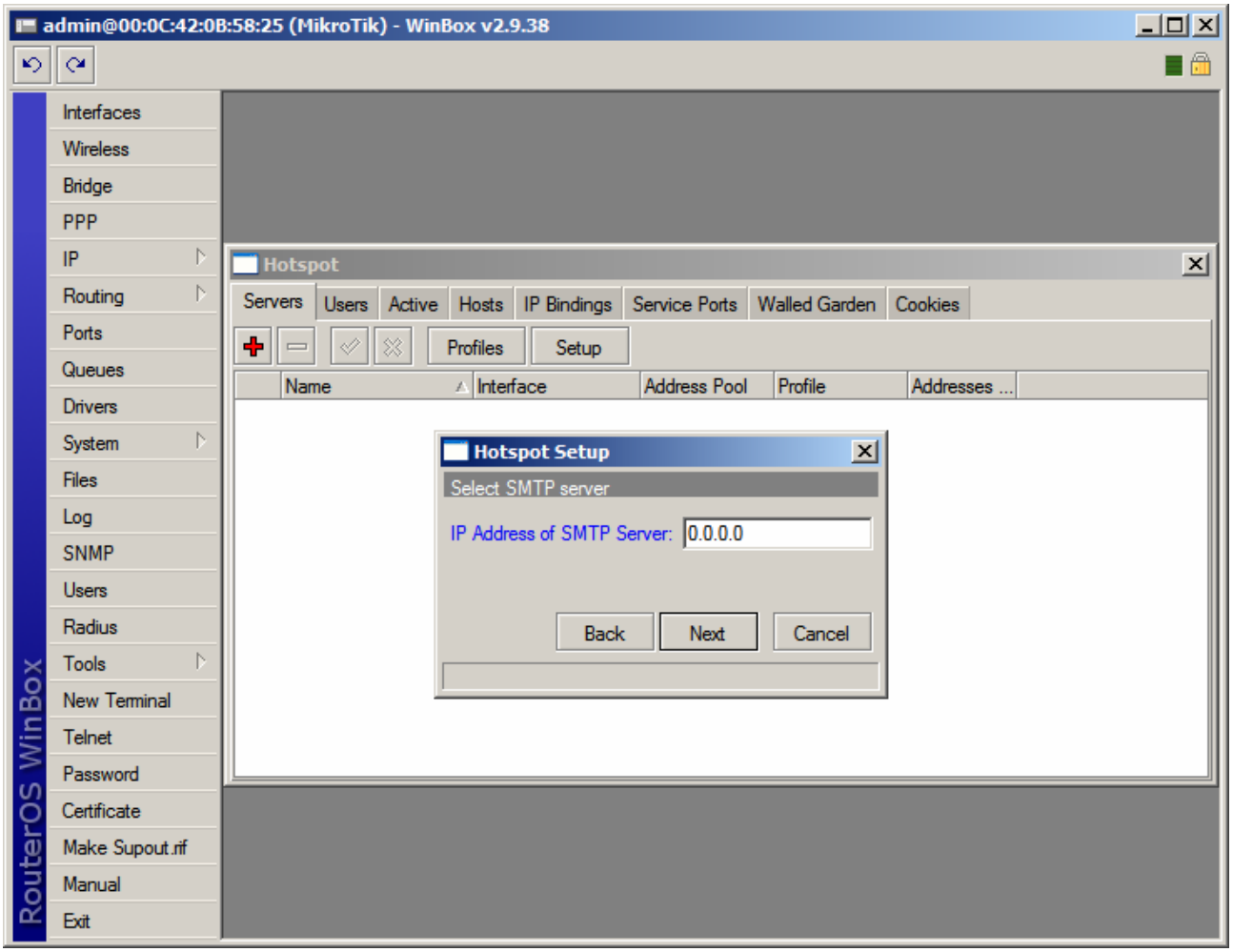
- No campo “Address Pool of Network” aparecerá o pool dos IPs que serão distribuídos aos clientes. Em nosso exemplo, é sugerido pelo Mikrotik o pool: 192.168.0.2-192.168.0.249
- Clique no botão “Next”



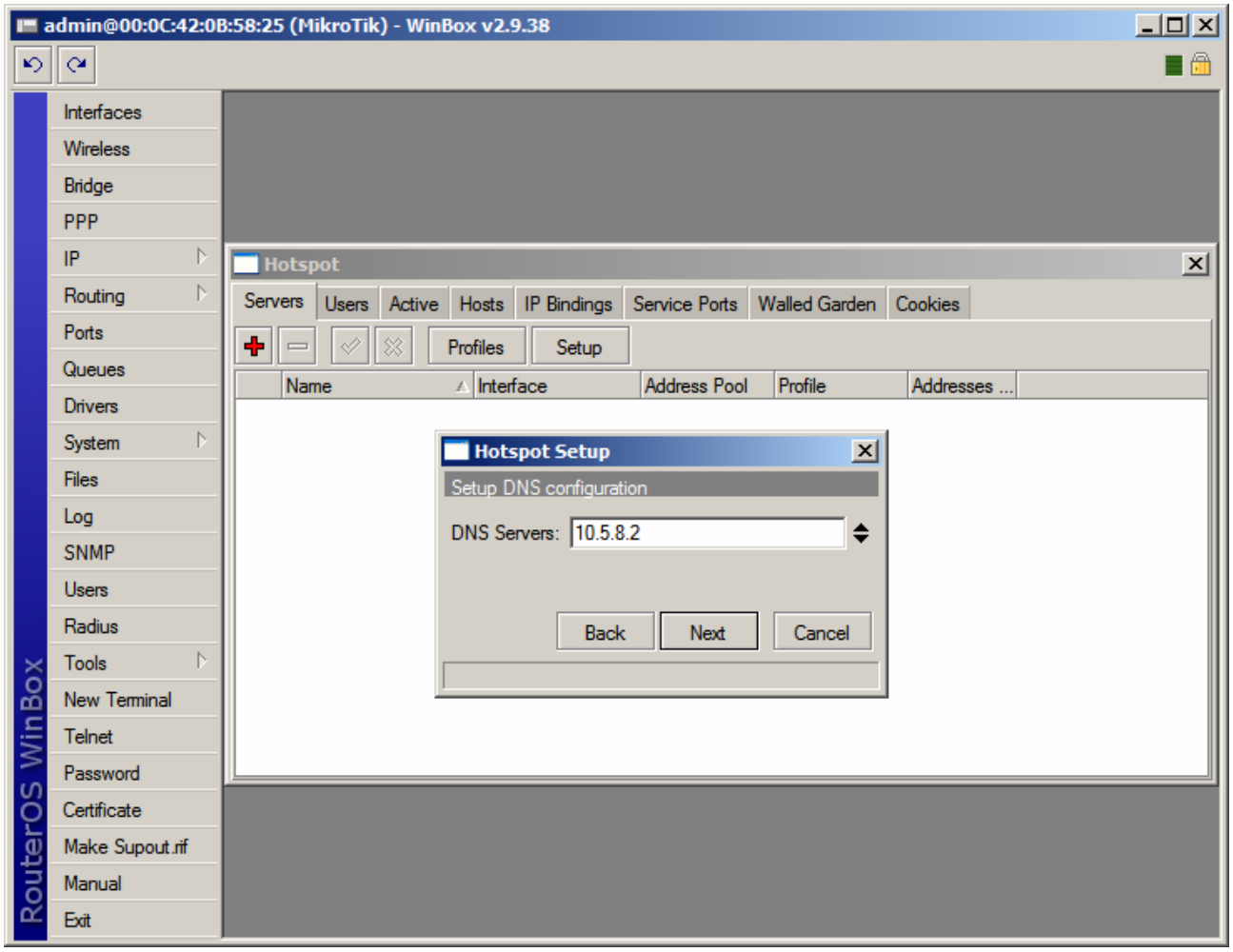
- Na opção “Select Certificate” escolha o certificado importado anteriormente. Caso você não tenha nenhum certificado, escolha a opção “none”.
- Clique no botão “Next”



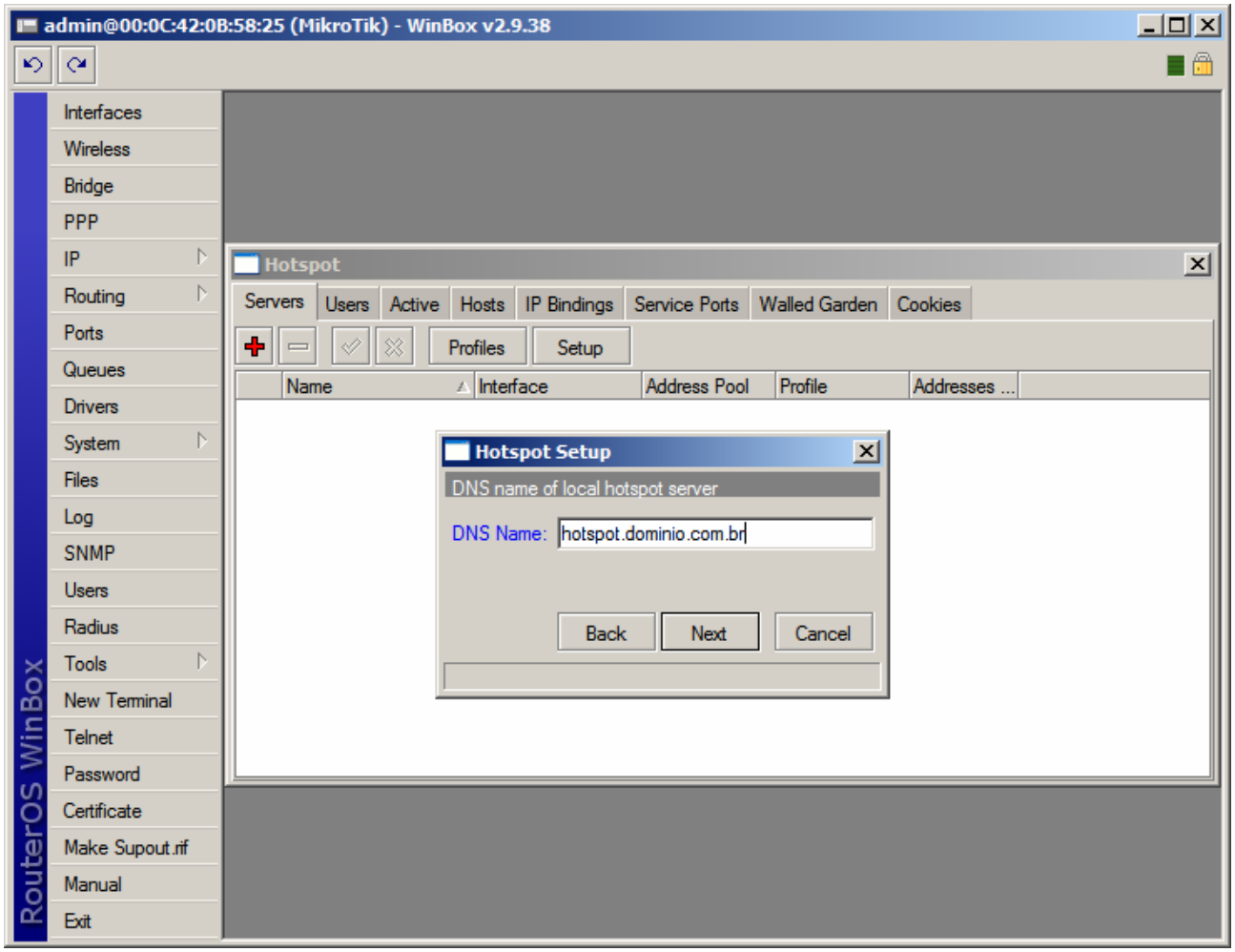
- Na opção “IP Address of SMTP Server”, digite o IP de seu Servidor SMTP, se desejar.
- Clique no botão “Next”



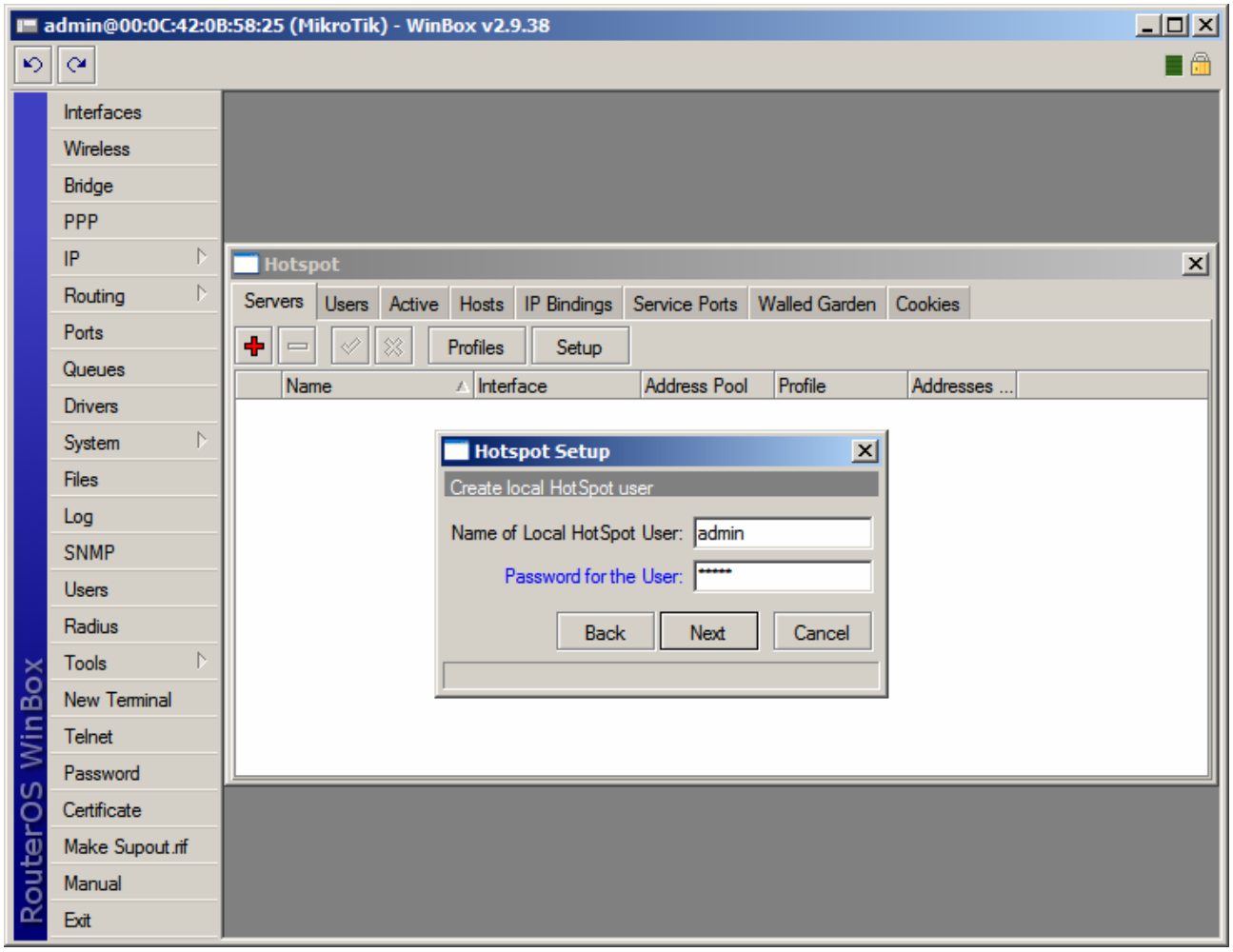
- Na opção “DNS Servers” digite o IP do seu servidor DNS.
- Clique no botão “Next”

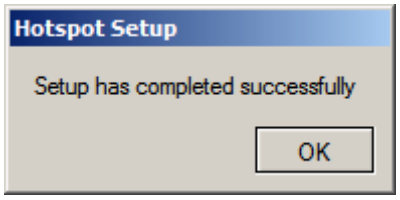


- Na opção “DNS Name”, Dê o nome do DNS (aparecerá no Browser dos clientes ao invés do IP).
- Clique no botão “Next”



- Na tela seguinte, por default, é cadastrado o usuário Administrador (admin).
- Após o cadastro, clique no botão “Next”

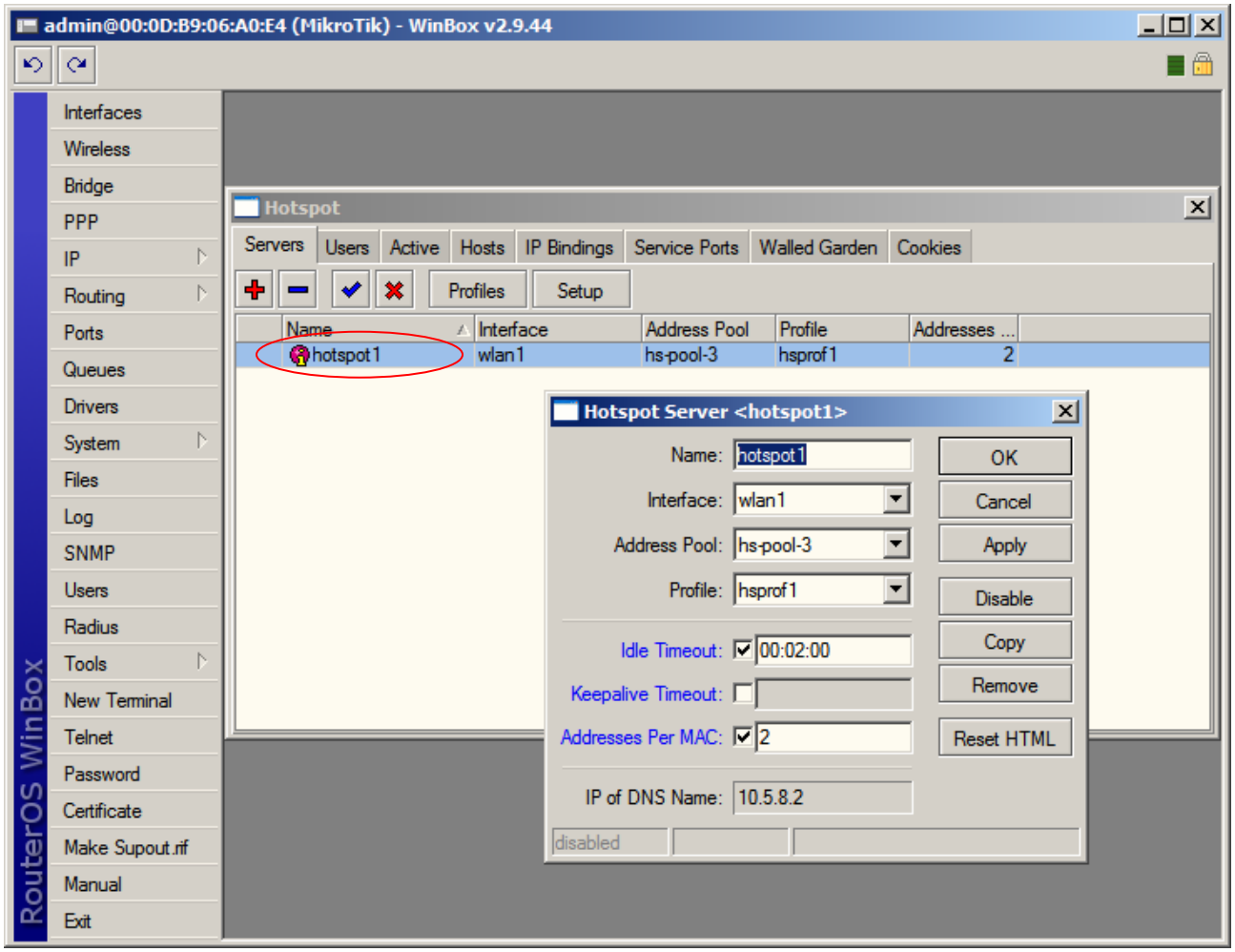




Seu Hotspot está configurado.

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

DETALHES DA CONFIGURAÇÃO

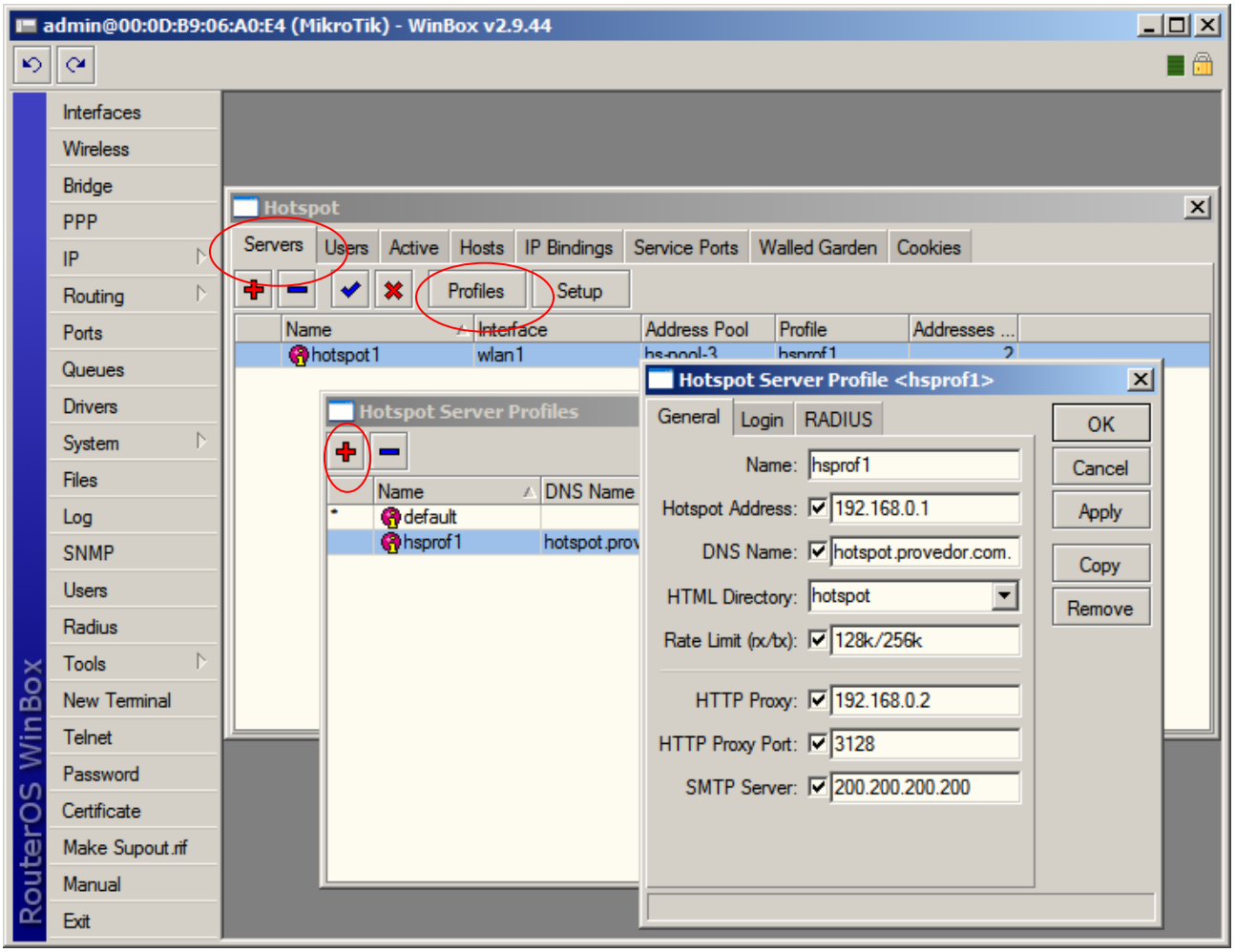


- idle Timeout (time | none; default: *none*)
Máximo período de inatividade para clientes autorizados. É utilizado para detectar quais clientes não estão usando redes externas (internet) e que não há tráfego do cliente através do roteador. Atingindo o timeout, o cliente é derrubado da lista dos hosts,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

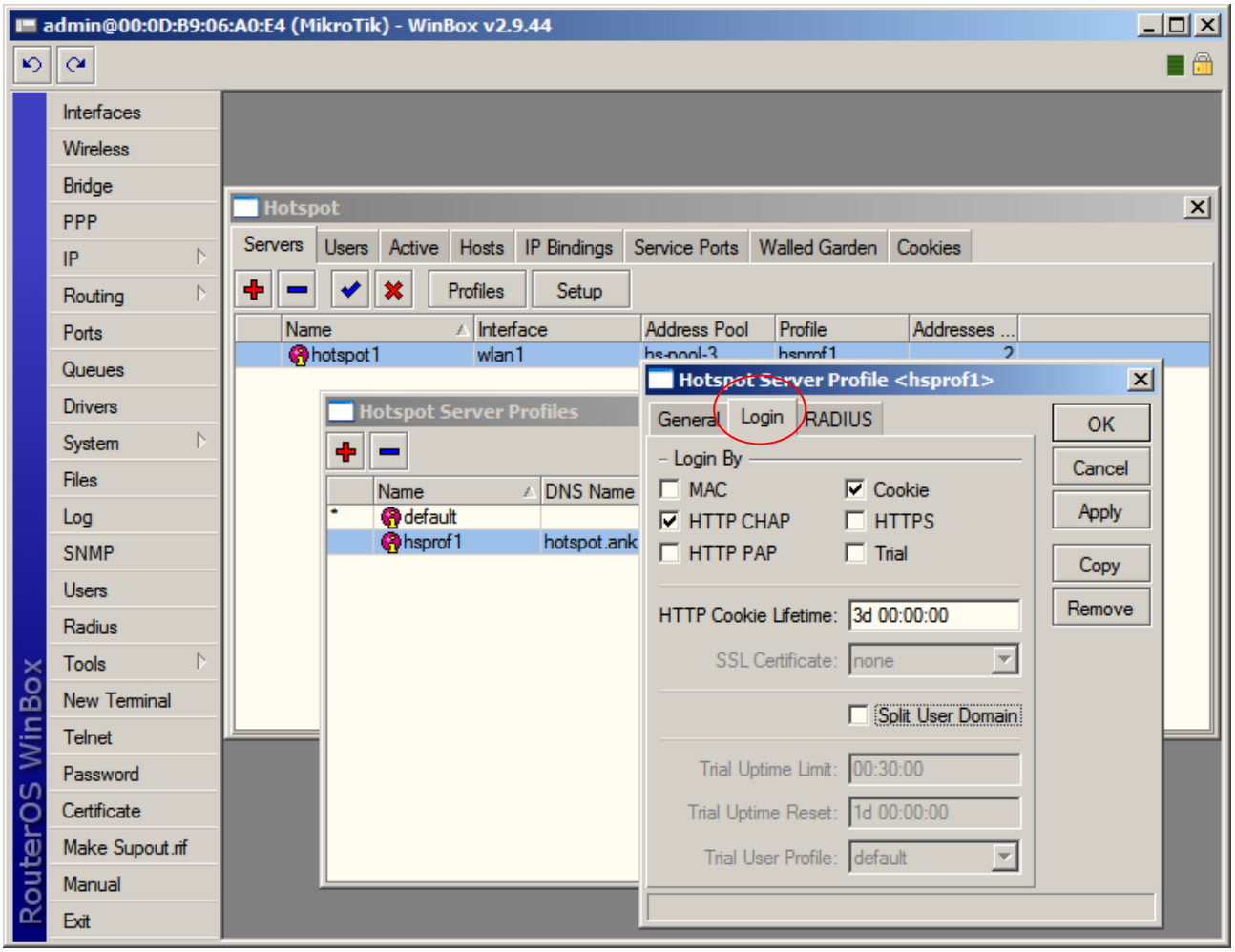
- Keepalive Timeout (time | none; default: *00:02:00*)
Utilizado para detector se o computador do cliente está ativo e encontrável. Caso nesse período de tempo o teste falhe, o usuário é tirado da tabela de hosts e o endereço IP que ele estava usando é liberado. O tempo é contabilizado levando em consideração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

- Address Per MAC (integer | unlimited; default 2)
Número de IPs permitidos para um particular MAC.

HOTSPOT SERVER PROFILES



- Rate Limit (rx/tx): (text; default: “”)
A limitação de velocidade tem a sintaxe:
rx-rate[/tx-rate][rx-burst-rate[/tx-burst-rate][rx-burst-threshold[/tx-burst-threshold][rx-burst-time[/tx-burst-time]]]]
onde:
- rx e o upload do cliente e tx é o download do cliente;
- as velocidades podem ser números com opcionais “k” (1.000s) e M para kiloo e Mega;
- se tx-rate não é especificado, tem o mesmo valor de rx-rate;
- o mesmo para tx-burst-rate, tx-burst-threshold e tx-burst-time;
- se ambos rx-burst-threshold e tx-burst-threshold não são especificados (mas burst-rate sim), rx-rate e tx-rate são usados como burst threshold;
- se ambos rx-burst-time e tx-burst-time não são especificados, 1s é usado como default.



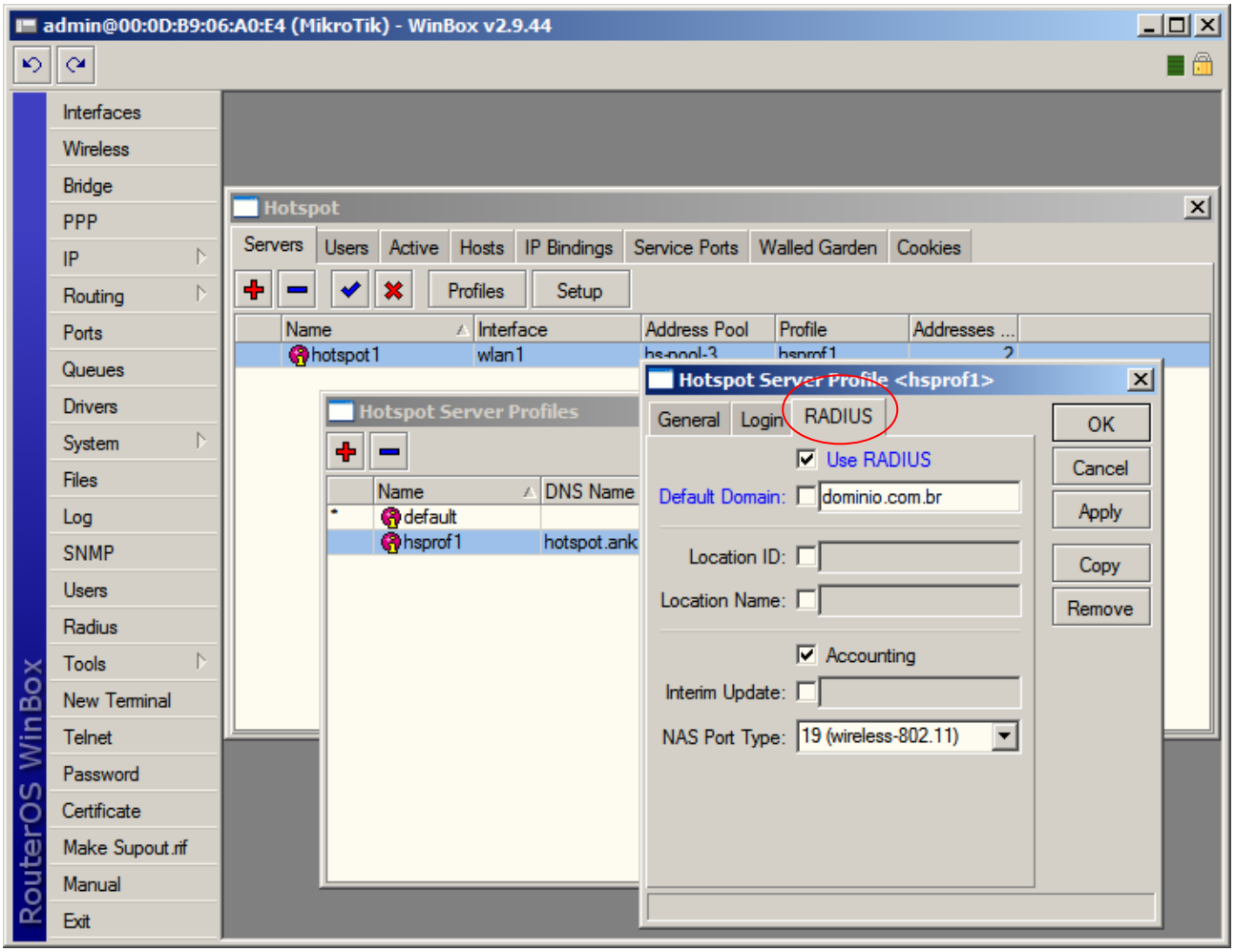
Login By

- ***MAC*** - Tenta usar o MAC dos clientes primeiro como nome de usuário. Se existir na tabela de usuários local ou em um Radius, o cliente é liberado sem login/senha;
- ***HTTP CHAP*** - Usa método CHAP – Método criptografado;
- ***HTTP PAP*** - Usa autenticação como texto plano – pode ser sniffado facilmente;
- ***Cookie*** - Usa http cookies para autenticar sem pedir as credenciais. Se o cliente ainda não tiver um cookie ou tiver expirado, usa outro método;
- ***HTTPS*** - Usa túnel SSL criptografado. Para isso funcionar, um certificado válido deve ser importado para o roteador.
- ***Trial*** - Não requer autenticação por um certo período de tempo.

HTTP Cookie Lifetime: tempo de vida dos Cookies

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

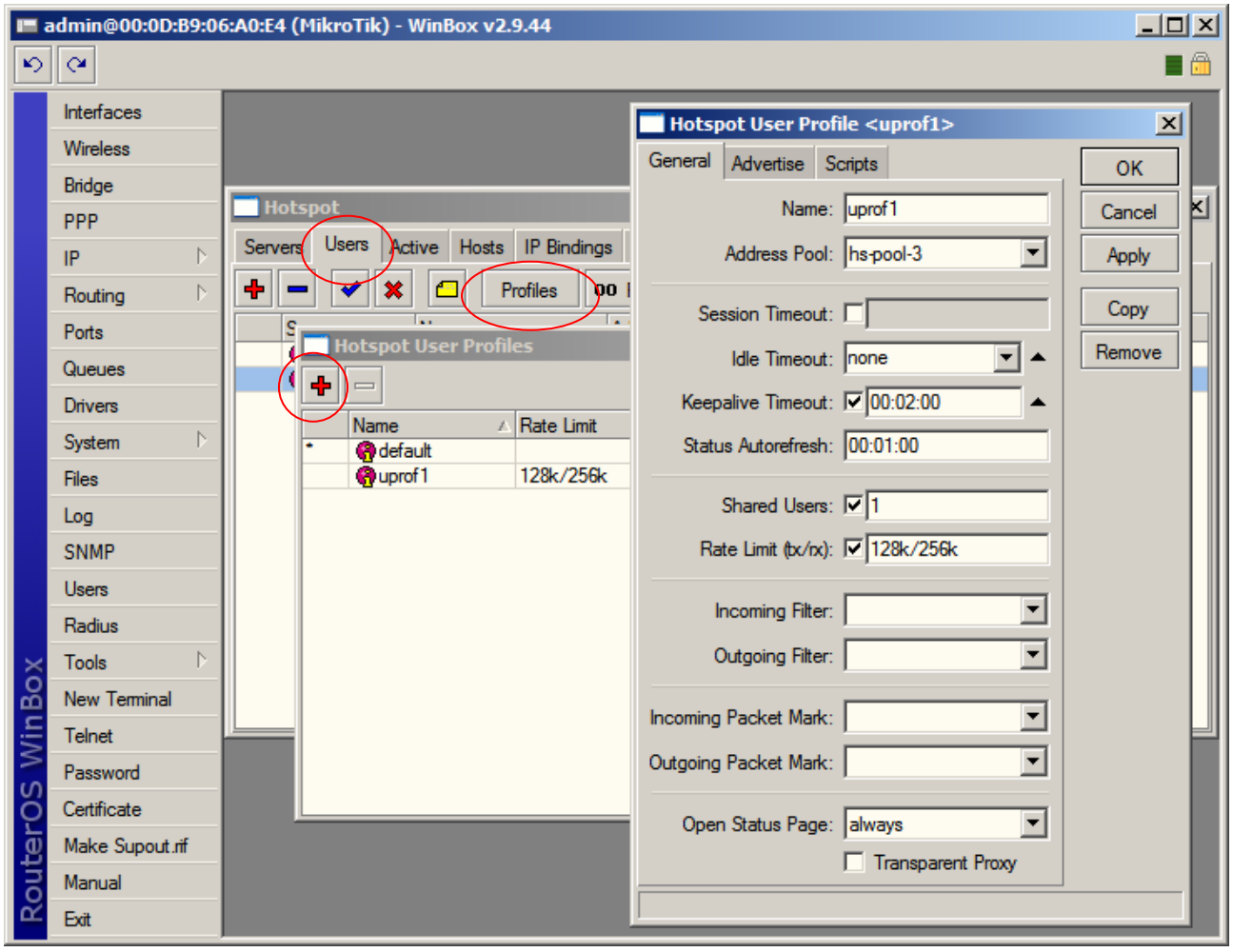
Utilização de Servidor Radius para autenticação do Hotspot



- Location ID
Pode ser atribuído aqui ou no servidor Radius – Normalmente deixar em branco
- Location Name
Pode ser atribuído aqui ou no servidor Radius – Normalmente deixar em branco
- Accounting
Se habilitado, faz a bilhetagem dos usuários, com histórico de logins, desconexões, etc.
- Interim Update
Freqüência de envio de informações de accounting (segundos)
0 – assim que ocorre o evento
(Gera tráfego – Interessante que coloque 30 ou 60s)
- NAS Port Type
Wireless, Ethernet ou Cabo

HOTSPOT USER PROFILES

O user profiles servem para dar tratamento diferenciado a grupos de usuários, como, por exemplo, usuários coorporativos, usuários residenciais, etc.



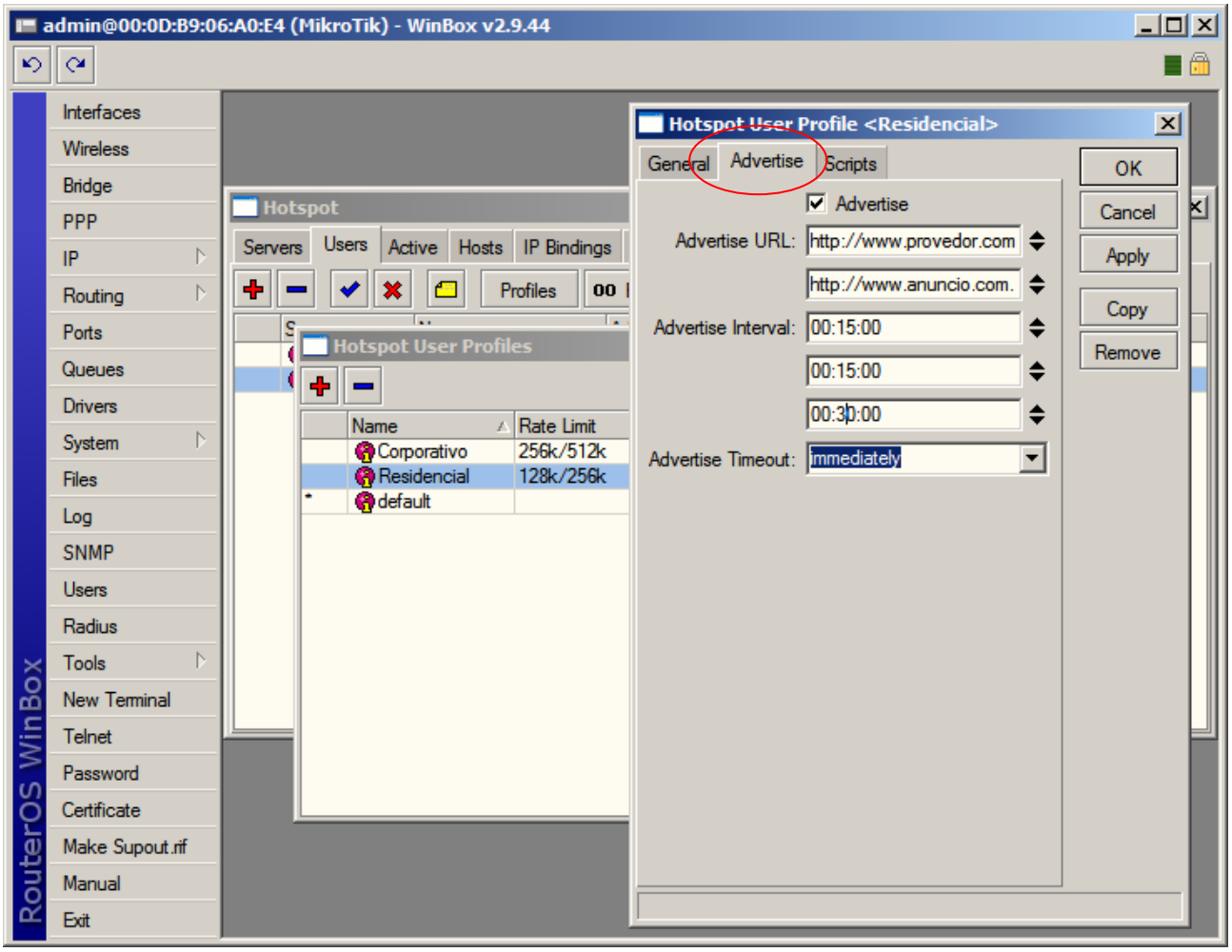
- **Session Timeout**: Tempo máximo permitido (depois disso o cliente é derrubado)
- **Idle timeout**: período de inatividade (acesso externo)
- **Keepalive Timeout**: se o computador está "vivo" e tem conectividade
- **Status Autorefresh**: tempo de refresh da página de Status do Hotspot
- **Shared Users:** número máximo permitido de clientes com o mesmo username
- **Rate Limit (tx/rx)**: A limitação de velocidade tem a sintaxe:

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

onde:

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

Com a opção Advertise é possível enviar, de tempos em tempos, pop-ups para os usuários do Hotspot



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

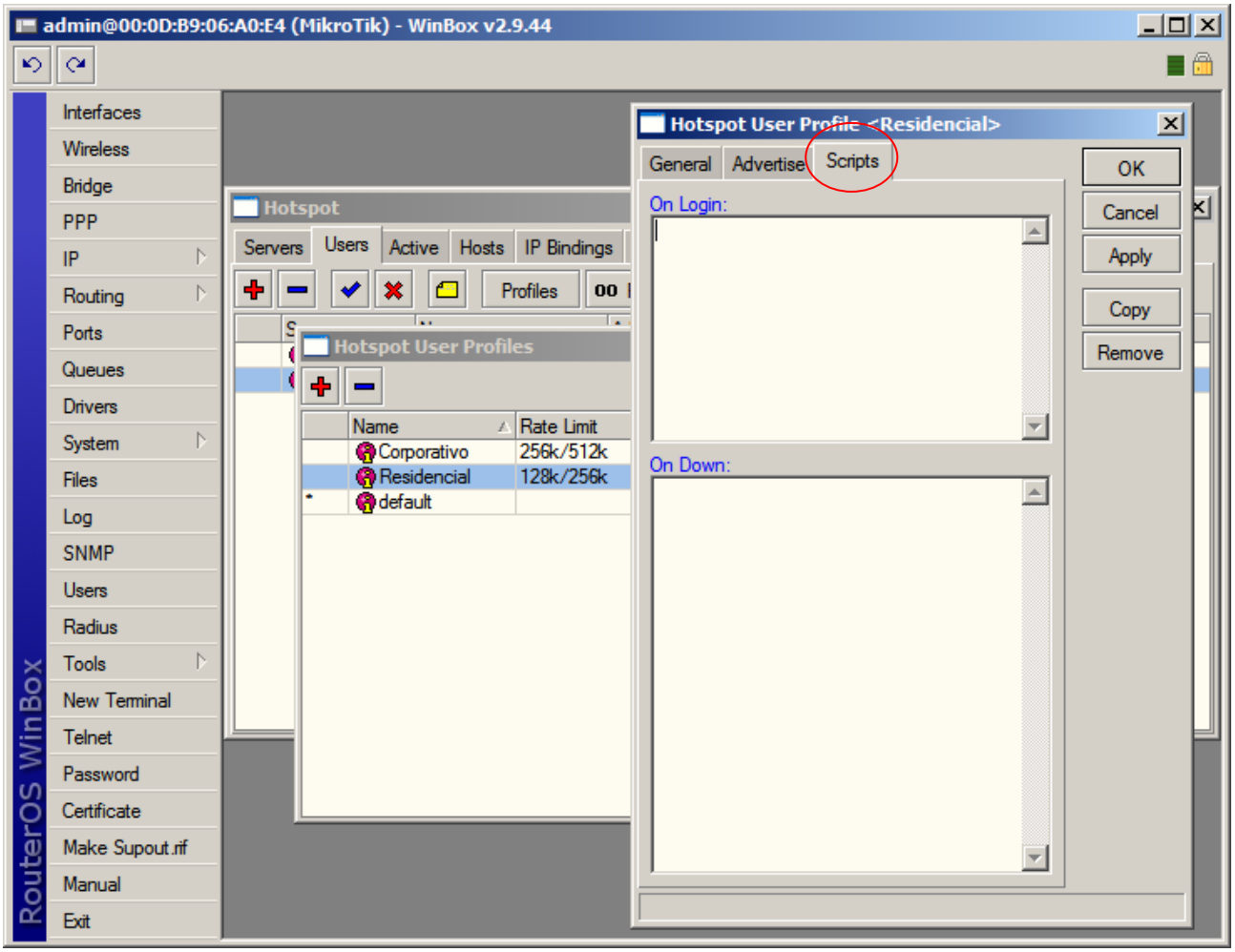
- Advertise Interval
Intervalos de exibição dos pop-ups. Depois da seqüência terminada, usa sempre o último intervalo. No exemplo, são mostradas a cada 15 minutos, 2 vezes e depois a cada 30 minutos

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

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

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

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

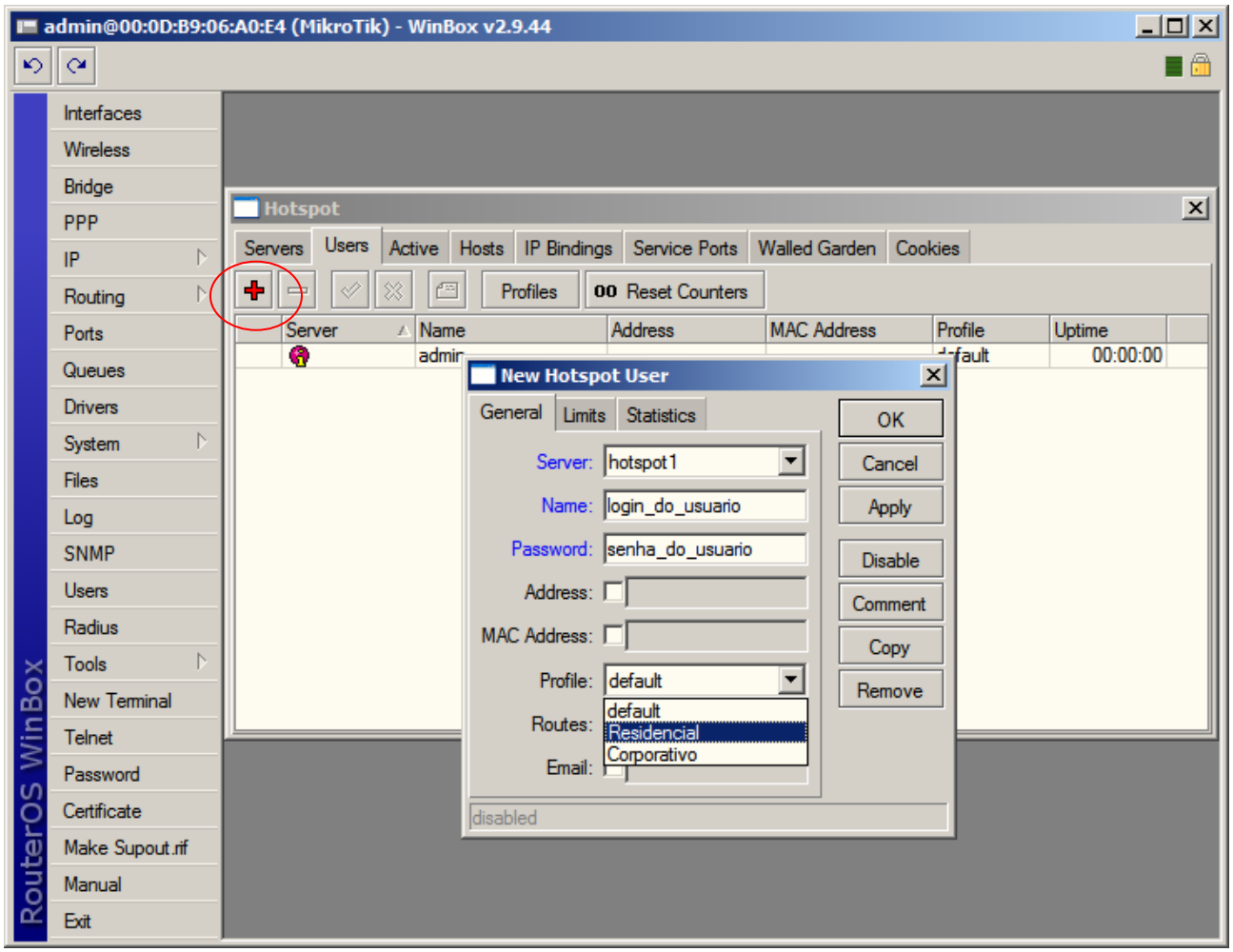


Os parâmetros que controlam essas execuções, são:
- on-login
- on-logout

Os Scripts são adicionados em Menu System / Scripts

Devemos, agora, cadastrar os usuários que terão permissão para se conectar ao Hotspot.

- Em Hotspot, clique na guia “Users”
- Clique em “Adicionar”
- Clique na guia General
    - Campo Server: “all” para todos os hotspots configurados ou para um específico.
    - Campo Name: Nome do usuário (login). No caso de autenticação por MAC, o MAC pode ser adicionado como username (sem senha)
    - Campo Password: para digitar a senha
    - Campo Address: Caso queira vincular esse usuário a um endereço fixo
    - Campo MAC Address: caso queira vincular esse usuário a um MAC determinado
    - Campo Profile: Perfil de onde esse usuário herda as propriedades
    - Campo Routes: Rota que será adicionada ao cliente quando esse se conectar. Sintaxe de destino gateway métrica. Várias rotas podem ser adicionadas separadas por vírgula.



- Clique na Guia “limits”

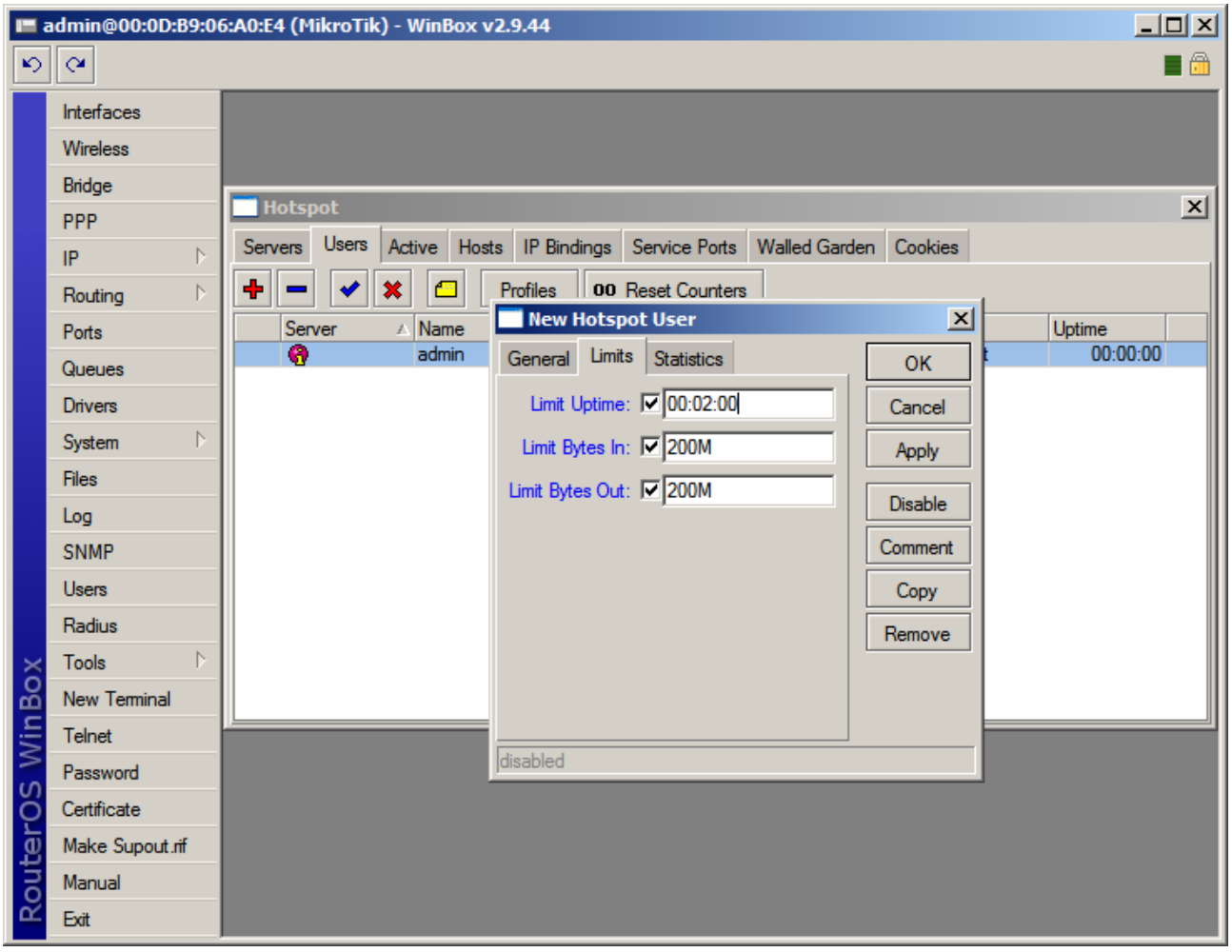
- Campo “Limit Uptime”: Total de tempo que o usuário pode usar o Hotspot. Útil para fazer acesso pré-pago.

Sintaxe: hh:mm:ss.

Default: 0s – Sem limite

- Campo “Limit Bytes In”: Total de bytes que o usuário pode **transmitir** (bytes que o roteador recebe para o usuário).

- Campo “Limit Bytes Out”: Total de bytes que o usuário pode **receber** (bytes que o roteador transmite para o usuário).



Se um usuário tem o endereço IP especificado, somente poderá haver 01 (um) logado. Caso outro entre com o mesmo usuário/senha, o primeiro será desconectado.

WALLED GARDEN (JARDIM MURADO)

Configurando um Walled Garden é possível oferecer ao usuário o acesso a determinados serviços sem necessidade de autenticação.
Exemplo: Em um aeroporto pode-se disponibilizar informações climáticas, horários de vôos, etc, se a necessidade de o usuário adquirir créditos para acesso externo.

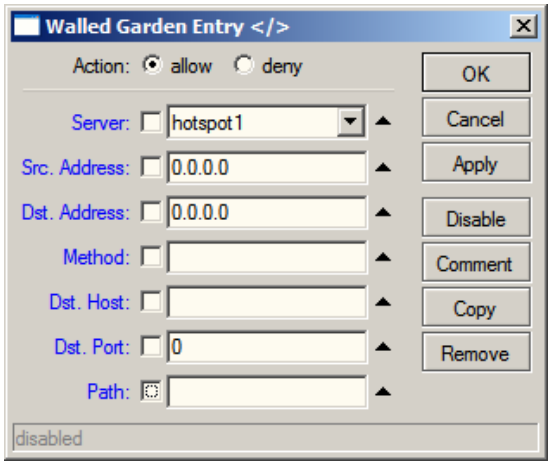
Quando um usuário não logado no Hotspot requisita um serviço do Walled Garden, o gateway não o intercepta e, no caso de http, redireciona a requisição para o destino ou para o Proxy.

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

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

É importante salientar que o Walled Garden não se destina somente a serviços WEB, mas qualquer serviço que queiramos configurar. Para tanto, existem 2 menus distintos que são apresentados abaixo, sendo que o primeiro destina-se somente para HTTP e HTTPS e o da segundo para os outros serviços e protocolos.

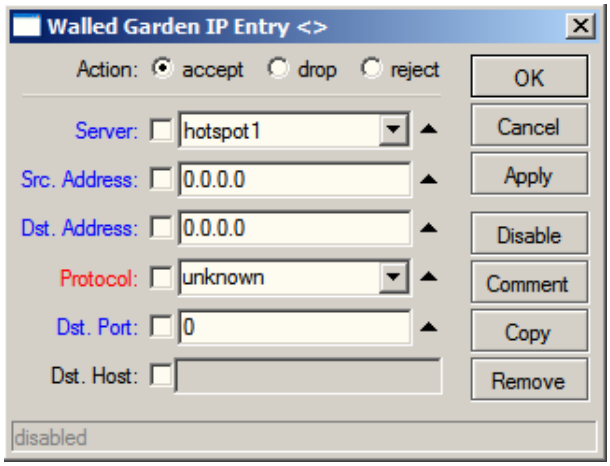
Walled Garden para http e HTTPS



Action: allow ou deny – permite ou nega
- Server: Hotspot ou Hotspots para o qual vale esse Walled Garden
- Src Address: endereço IP do usuário requisitante
- Dst Address: endereço IP do Web Server
- Method: método de http
- Dst Host: nome de domínio do servidor de destino
- Dst Port: porta de destino que o cliente manda a solicitação
- Path: caminho da requisição

Observação:
- nos nomes de domínio, é necessário o nome completo, podendo ser usado coringas
- aceita-se expressões regulares devendo ser iniciadas com dois pontos (:)

Walled Garden para outros protocolos



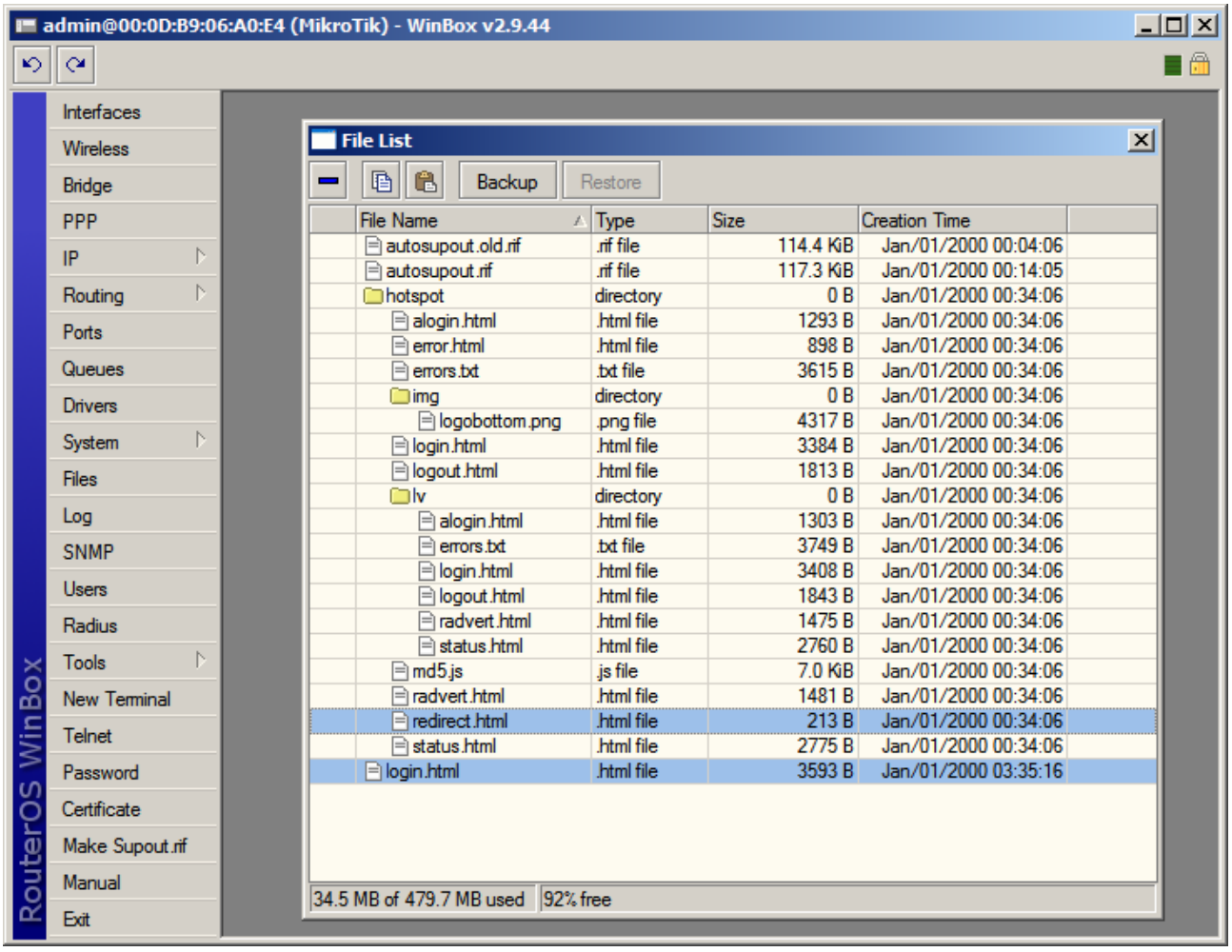
Action: aceita, descarta ou rejeita o pacote
- Server: Hotspot ou Hotspots para o qual vale esse Walled Garden
- Src Address: endereço IP de origem do usuário requisitante
- Protocol: Protocolo a ser escolhido da lista
- Dst Port: Porta TCP ou UDP que está sendo requisitado
- Dst Host: Nome de domínio do WEB Server

PERSONALIZANDO O HOTSPOT

As páginas do Hotspot são totalmente configuráveis e podem ser editadas em qualquer editor HTML, sendo posteriormente atualizadas no Mikrotik.

Além disso, é possível criar conjuntos totalmente diferentes das páginas do Hotspot para vários perfis de usuários especificando diferentes diretórios html raiz na opção html-directory em Hotspot Profile.

Essa possibilidade, associada a criação de Aps virtuais possibilita que, em uma mesma área pública o detentor de infra-estrutura possa, de forma transparente, servir a vários operadores, utilizando os mesmos equipamentos.

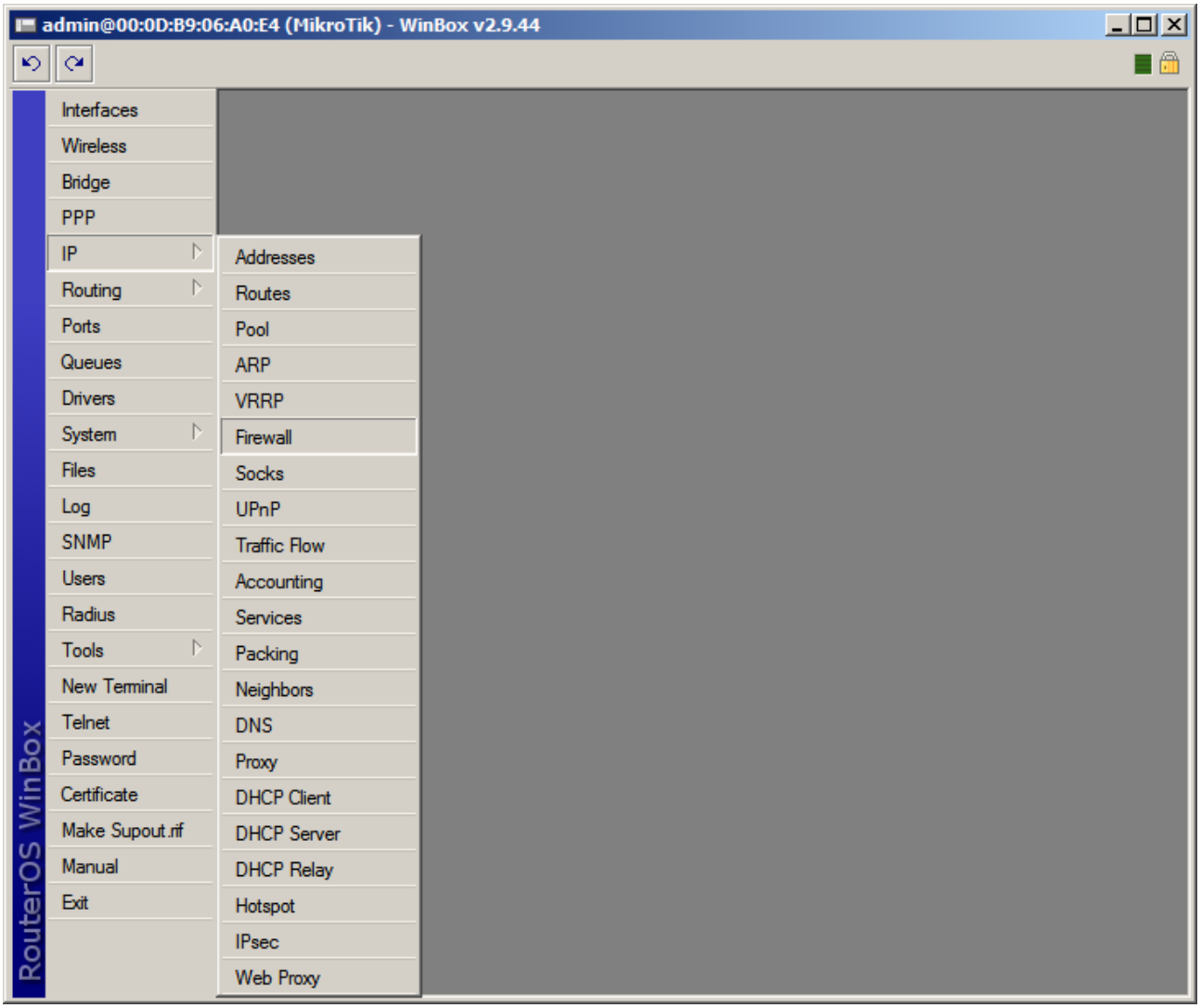


Principais páginas HTML que são mostradas aos usuários:
- redirect.html – redireciona o usuário para outra URL (exemplo: a página de login)
- login.html - Página de login mostrada a um usuário solicitando nome e senha. Esta página pode ter os seguintes parâmetros:
    - username – nome do usuários
    - password – senha
    - dst – URL original requisitada antes de cair na tela de login. O usuário será enviado a esta URL após um login bem-sucedido
    - pop-up – se deve ser aberta uma janela de pop-up após o login

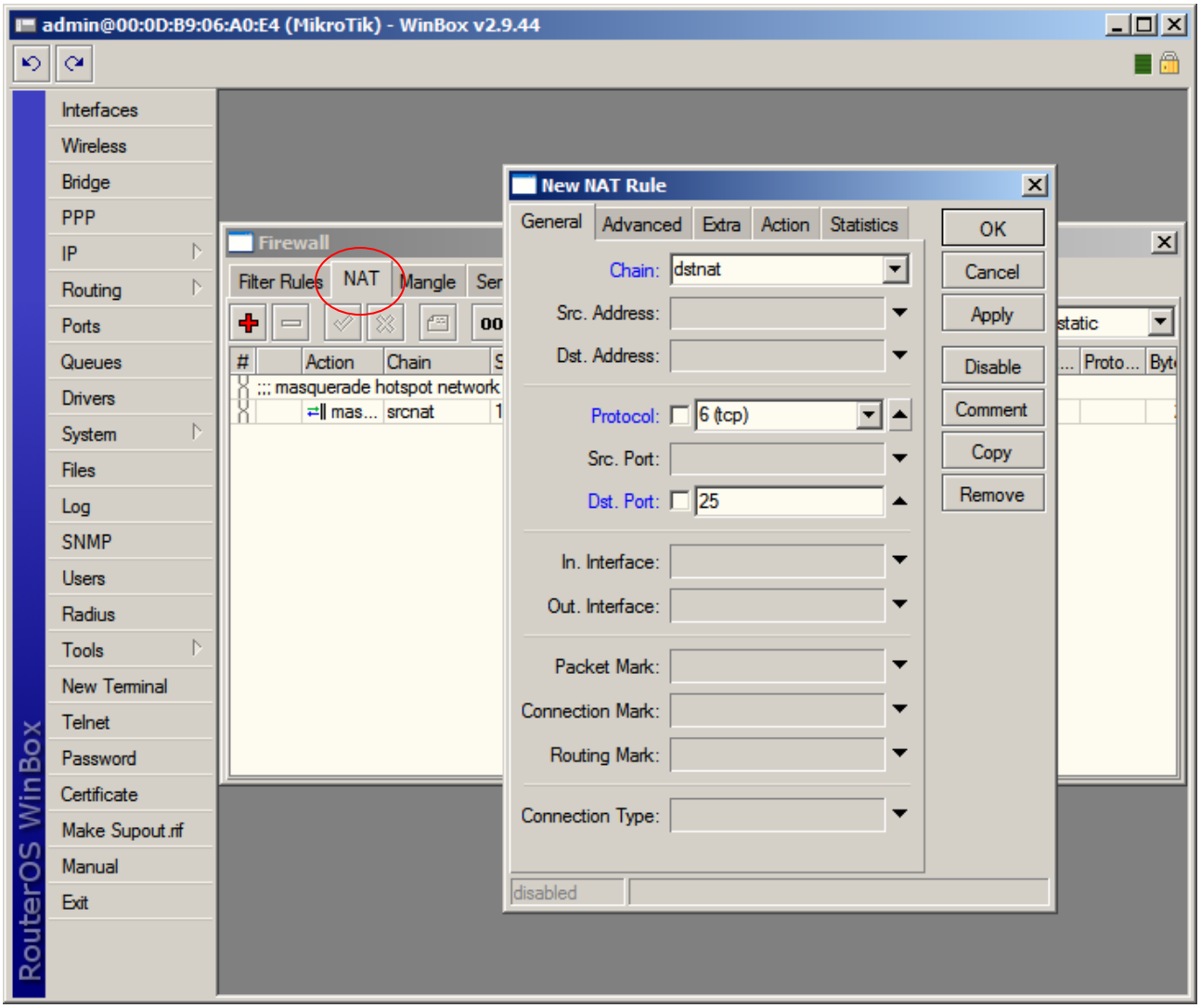
REDIRECIONANDO TRÁFEGO DE SMTP PARA SEU DEVIDO SERVIDOR

Você pode redirecionar todo o tráfego através de seu Router para o seu próprio Servidor de E-mail.

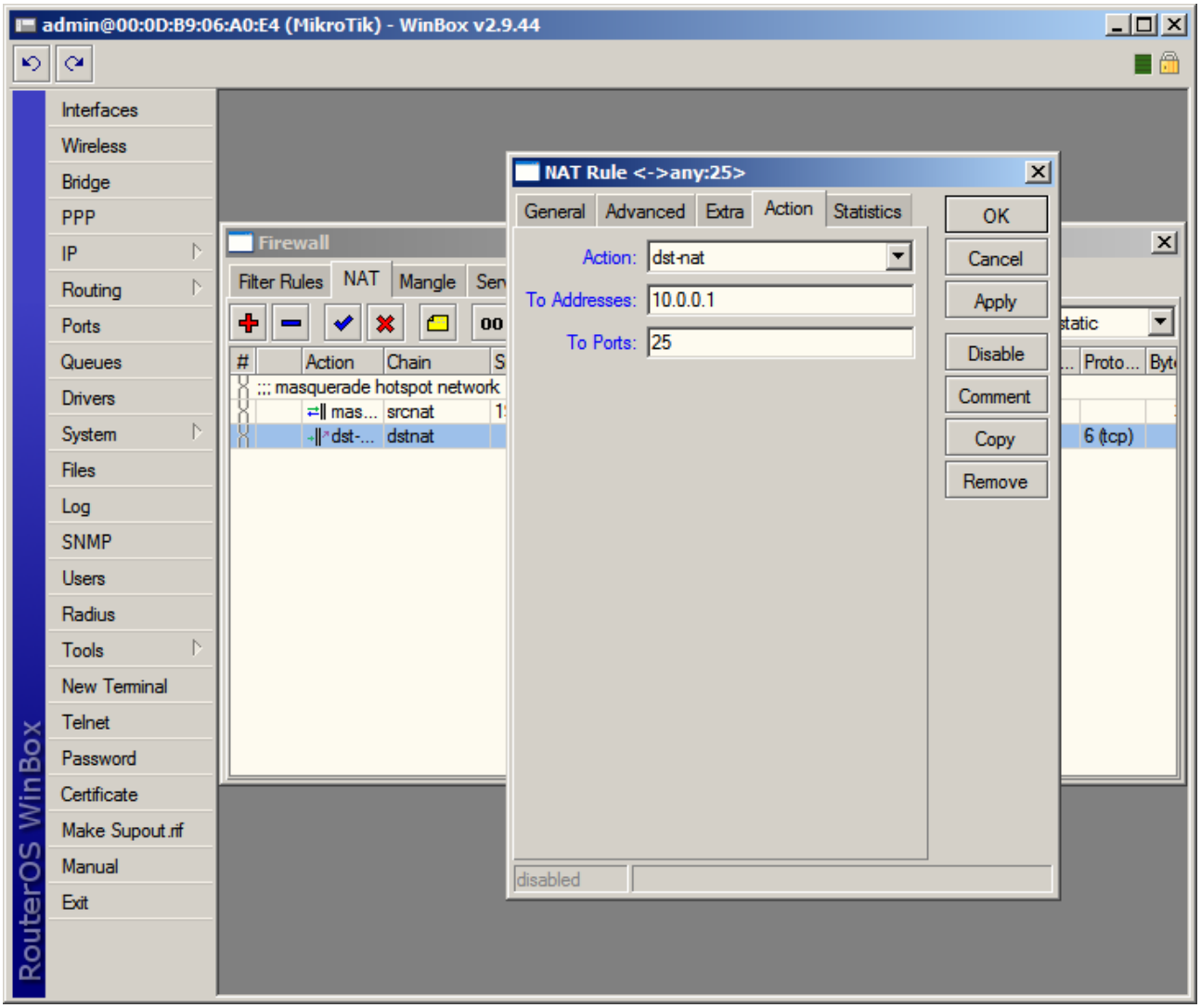
- Clique no Menu “IP”
- Clique na opção “Firewall”



- Clique na guia “NAT”
- Clique em “Adicionar”
- Na guia “General”, na opção “Chain”, escolha a opção “dstnat”
- Na opção “Protocol”, escolha “TCP”
- Na opção “Dst. Port.”, escolha a porta 25



- Clique na guia “Action”
- Na opção “Action”, escolha a opção “dst-nat”
- Na opção “To Addresses”, digite o IP do servidor de email
- Na opção “To Ports”, digite a porta SMTP, 25.
- Clique no botão “OK”



Referências:
- Mikrotik Wiki - http://wiki.mikrotik.com/wiki/
- Apostila Curso Router-OS Mikrotik – Wlan Brasil
- Certificado SSL - http://www.laniway.com.br

Marcelo Carvalho - MACNet (Ankaa W. S.)