



GUIA EXCLUSIVO DE REFERÊNCIA



INTRODUÇÃO AO MIKROTIK



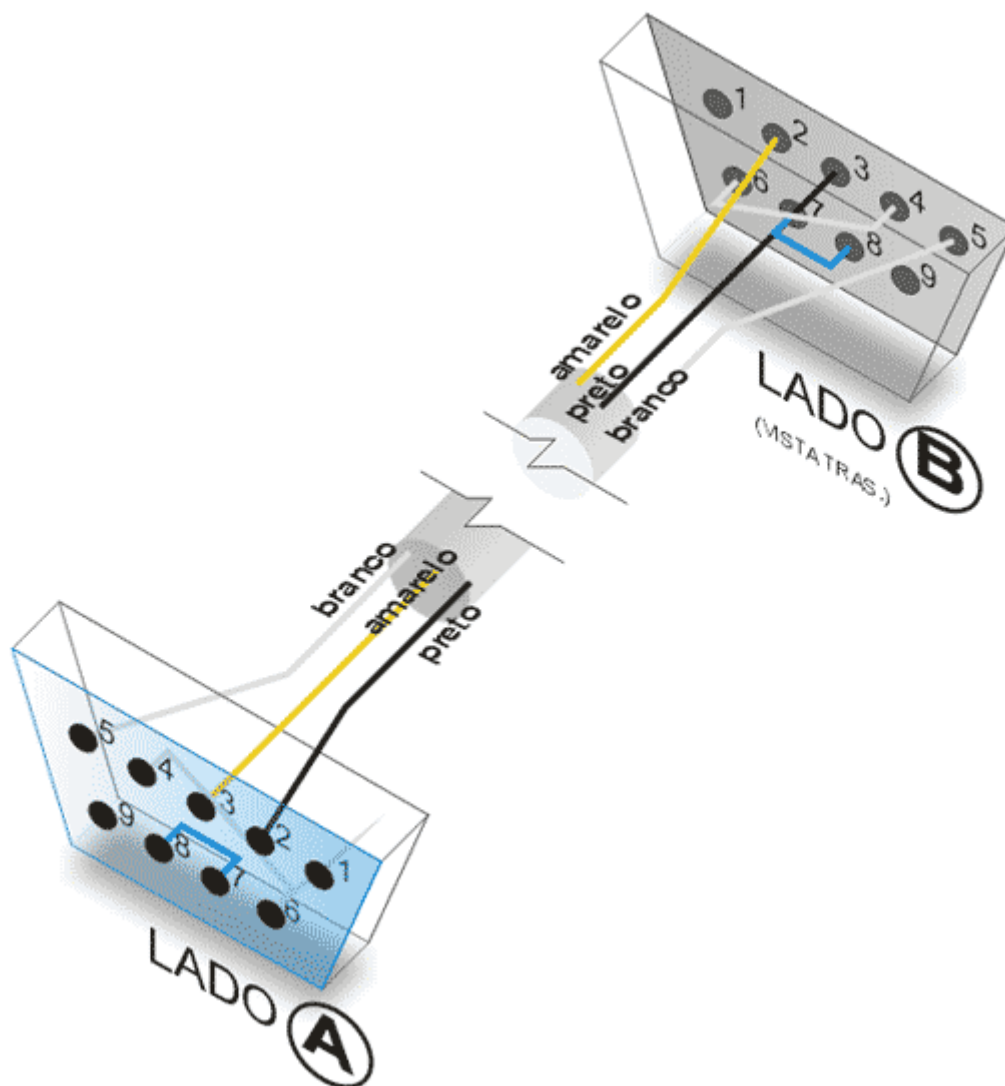
COMO ACESSAR O ROUTEROS MIKROTIK

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>

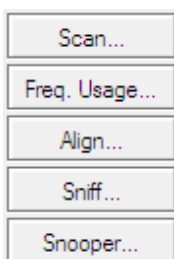
MAC Address	IP Address	Identity	Version
00:0C:42:0B:58:25	0.0.0.0	RealsatRS5800	2.9.38
00:0C:42:0B:58:4D	10.0.43.1	MikroTik	2.9.38



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

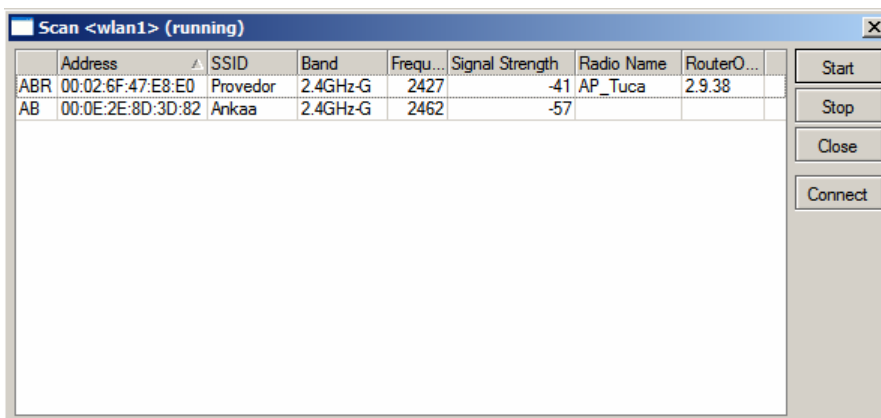
INTERFACE WIRELESS



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 frequências em todo o espectro, para site survey

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

Frequency Usage <wlan1> (running)			
Frequency	Usage		
2412MHz	0.0		Start
2417MHz	1.0		Stop
2422MHz	1.0		Close
2427MHz	1.0		
2432MHz	1.0		
2437MHz	0.5		
2442MHz	0.0		
2447MHz	0.0		
2452MHz	0.0		
2457MHz	0.0		
2462MHz	1.8		

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

Alignment <wlan1> (running)									
Address	SSID	Rx Qu...	Avg. Rx ...	Last Rx	Tx Qu...	Last Tx	Correct		
00:02:6F:47:E...		-54	0	2.34	0	0.00	0%		Start
									Stop
									Close
									Settings...

Wireless Alignment Settings	
Frame Size:	300
☒ Active Mode	OK
☒ Receive All	Cancel
Filter MAC Address: 00:02:6F:47:E8:C6	Apply
☒ SSID All	
Frames per Second:	25
Audio Monitor: 00:02:6F:47:E8:C6	
Audio Min:	-100
Audio Max:	-20



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

Processed Packets:	130	Start
Memory Size:	9.9 KB	Stop
Memory Saved Packets:	61	Close
Memory Over Limit Packets:	69	Save...
File Size:	0 B	Settings...
File Saved Packets:	0	Packets...
File Overlimit Packets:	0	
Stream Dropped Packets:	0	
Stream Sent Packets:	0	
File Limit:	10KB	
Memory Limit:	10KB	

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 frequências definidas em scan-list da interface.

Frequency	Band	Address	SSID	Of Freq (%)	Of Traf. (%)	Bandwidth
2412MHz	2.4GHz...			0.0		0 bps
2417MHz	2.4GHz...			0.5		4.4 kbps
2422MHz	2.4GHz...			0.5		4.4 kbps
2427MHz	2.4GHz...			1.0		8.8 kbps
2427...	2.4GHz...	00:02:6F:47:E8:E0	Provedor	1.0	100.0	8.8 kbps
2432MHz	2.4GHz...			1.0		8.8 kbps
2437MHz	2.4GHz...			0.5		4.4 kbps
2442MHz	2.4GHz...			0.0		0 bps
2447MHz	2.4GHz...			0.0		0 bps
2452MHz	2.4GHz...			0.0		0 bps
2457MHz	2.4GHz...			0.3		2.7 kbps
2462MHz	2.4GHz...			1.2		5.5 kbps
2462...	2.4GHz...	00:0E:2E:8D:3D:82	Ankaa	0.7	58.0	5.5 kbps



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:** 802.11b 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 “clocking”, utiliza canal de 10Mhz;
- **2.Ghz-5Mhz:** Modo “clocking”, utiliza canal de 5Mhz;
- **5.Ghz-10Mhz:** Modo “clocking”, utiliza canal de 10Mhz;
- **5.Ghz-5Mhz:** Modo “clocking”, utiliza canal de 5Mhz.

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

Scan List: lista de frequências a serem escaneadas.

- Quando a interface está configurada como cliente, serão “procuradas” APs que estiverem nessa lista;
- Por default, serão buscadas as frequências do domínio regulatório;
- Pode-se forçar o escaneamento de frequências específicas, 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 frequências 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 frequência.

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



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

Interface <wlan1>

Data Rates Advanced WDS Nstreme Tx Power ...

Area:

Max Station Count: 2007

Ack Timeout: dynamic us

Noise Floor Threshold:

Periodic Calibration: default

Calibration Interval: 00:01:00

Burst Time: us

Antenna Mode: antenna a

Preamble Mode: ☐ long ☐ short ☒ both

Disconnect Timeout: 00:00:03

On Fail Retry Time: 100 ms

Update Stats Interval: s

disabled running running ap

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 habilite-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

The screenshot shows the 'Interface <wlan1>' configuration window in WinBox. The 'WDS' tab is selected. The settings are as follows:

- WDS Mode: disabled (dropdown menu)
- WDS Default Bridge: none (dropdown menu)
- WDS Default Cost: 100 (text field)
- WDS Cost Range: 50-150 (text field)
- WDS Ignore SSID: ☐ (checkbox)

On the right side of the window, there are several buttons: OK, Cancel, Apply, Disable, Comment, Scan..., Freq. Usage..., Align..., Sniff..., and Snooper... At the bottom of the window, there are three status indicators: 'disabled', 'running', and 'running ap'.



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.

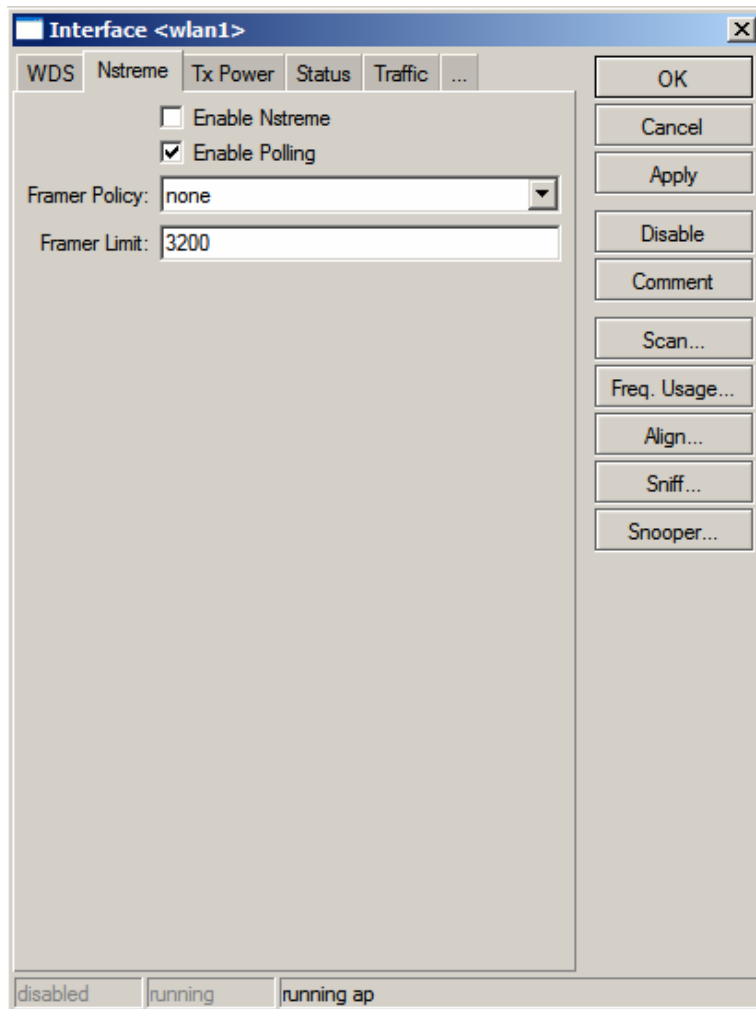
WDS Cost Range: Indicação da faixa de custos que serão empregados na rede Mesh.

WDS Ignore SSID: Uma vez habilitada essa opção, os APs irão criar links com qualquer outro AP que esteja configurado na mesma frequência, 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 método CSMA/CA comum das redes Wi-fi.

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

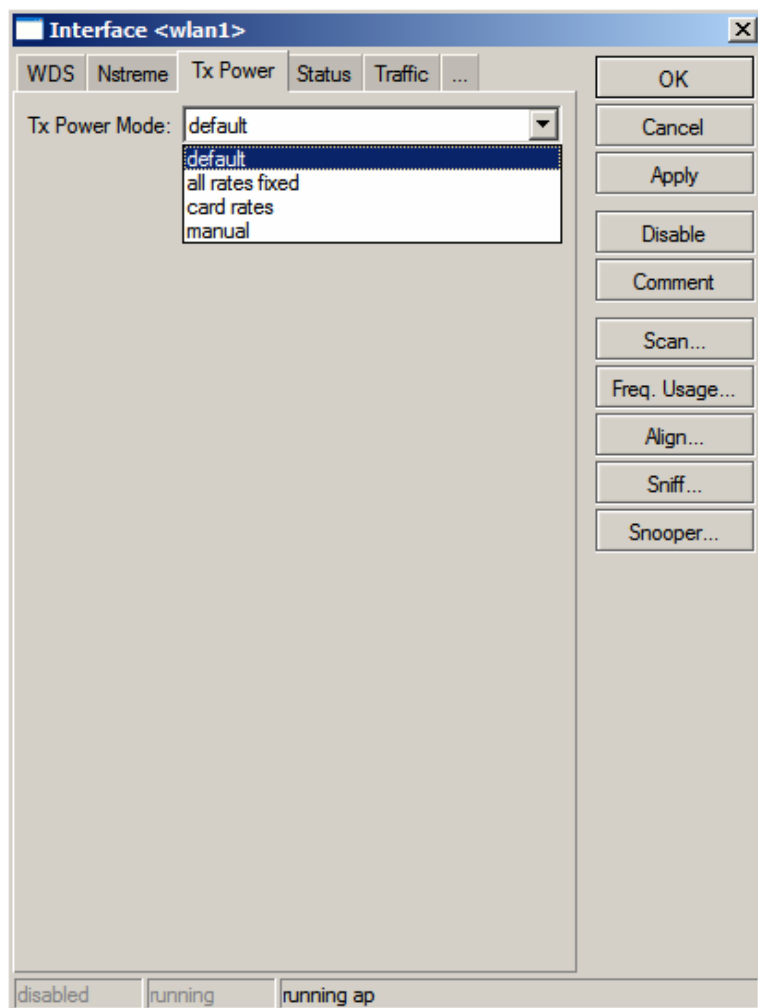
- none: não combina os pacotes
- best-fit: coloca o maior número de pacotes possíveis em um frame, até que o limite estabelecido em framer-limit seja atingido. Não fragmenta pacotes.
- exact-size: põe quantos pacotes for possível em um quadro, até que o limite estabelecido em framer-limit seja atingido,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

Framer Limit: Tamanho máximo do quadro.



Default = 3200 bytes

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 aumentá-la



Guia – Status

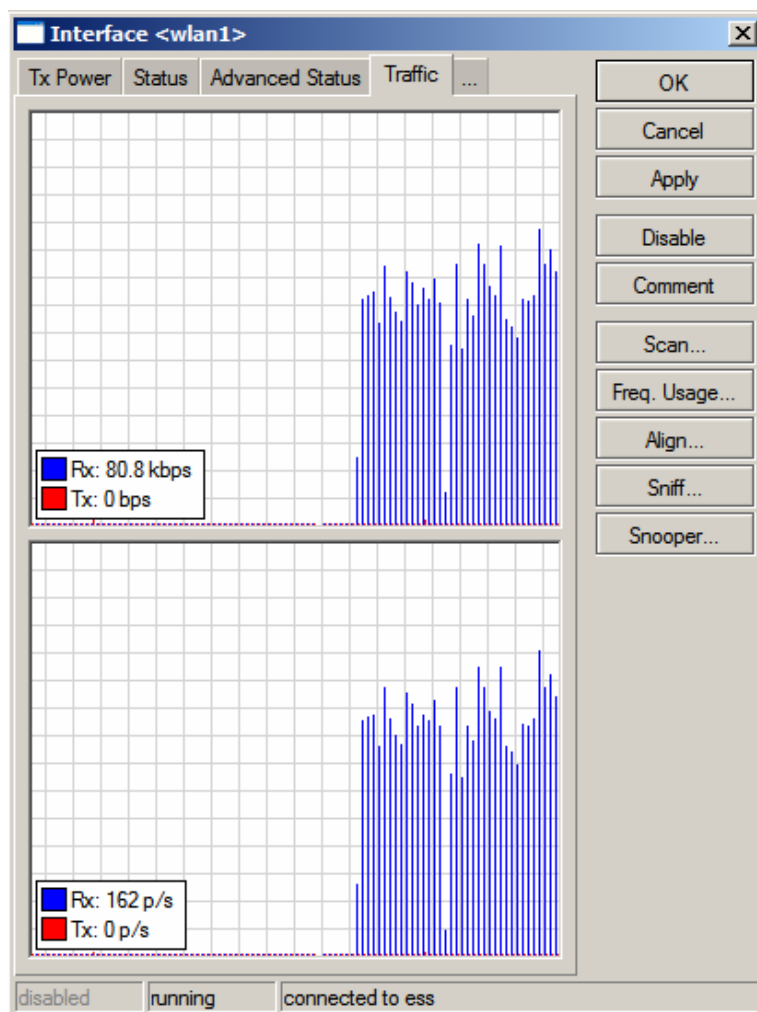
WDS	Nstreme	Tx Power	Status	Traffic	...
Band: 2.4GHz-G Frequency: 2427 MHz Registered Clients: 0 Authenticated Clients: 0 Overall Tx CCQ: 32 % Ack. Timeout: 53 us Noise Floor: -94 dBm					
OK Cancel Apply Disable Comment Scan... Freq. Usage... Align... Sniff... Snooper...					
disabled running running ap					

Mostra informações sobre o status do AP

- **Band:** Frequência e modo de operação
- **Frequência:** Canal utilizado
- **Registered Clients:** Clientes registrados
- **Authenticated Clients:** Clientes autenticados
- **Overall 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.

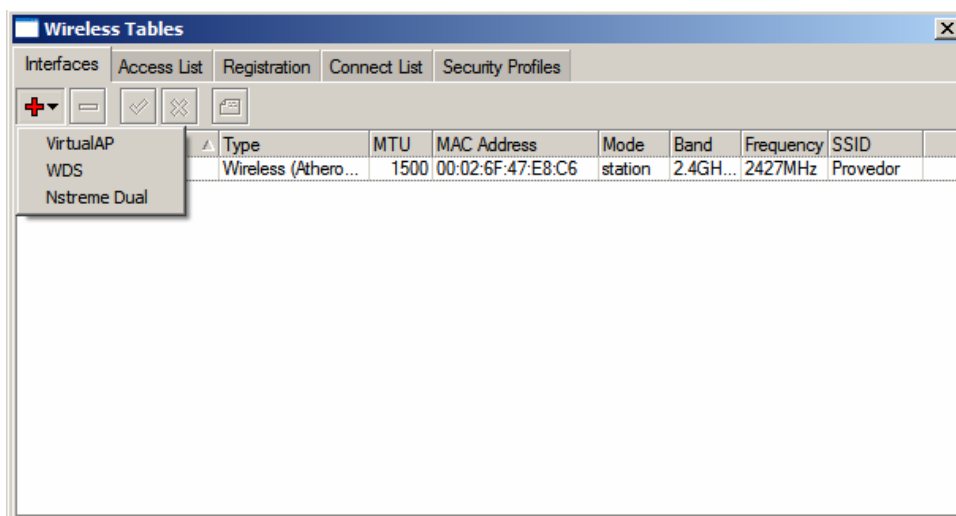


Guia – Traffic





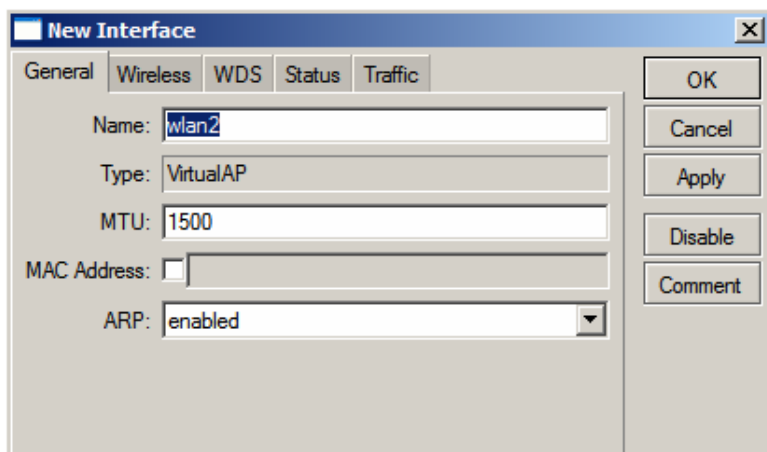
Menu Wireless – Interfaces



Ao clicar em adicionar interfaces, são dadas as opções:

- **VirtualAP**: Cria interfaces virtuais (APs com nomes diferentes) na mesma interface física. Os parâmetros de frequência, 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)).

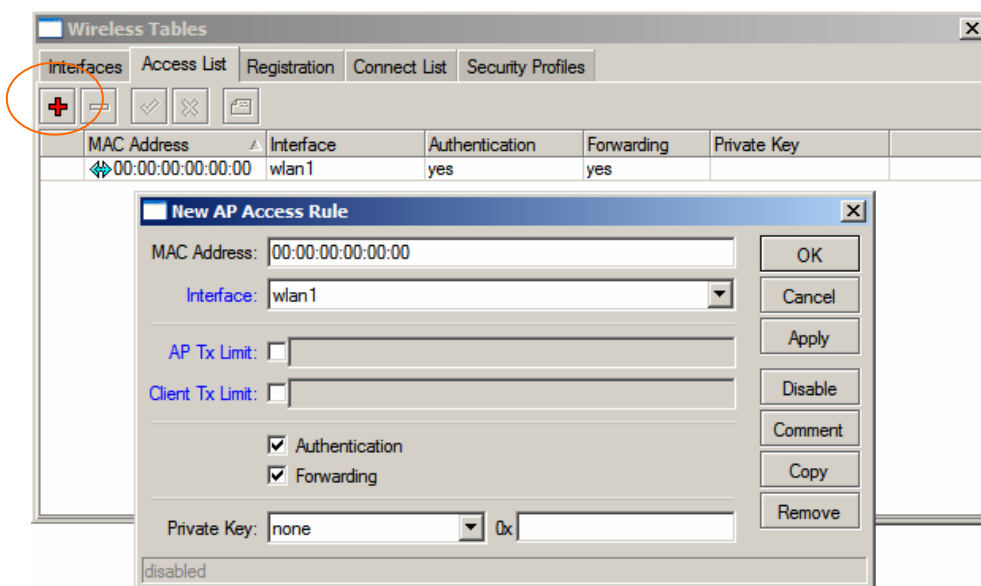
- Tx Rádio: especifica-se as interfaces de Tx.
- Rx Rádio: especifica-se as interfaces de Rx.
- Tx/Rx Band e Frequency: Especifica-se a Banda de Tx e Rx que podem inclusive ser de frequências diferentes (2.4Ghz para Tx e 5.8Ghz para Rx)
- Framers Policy:
 - Best-fit: pacotes são agrupados em frames, 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



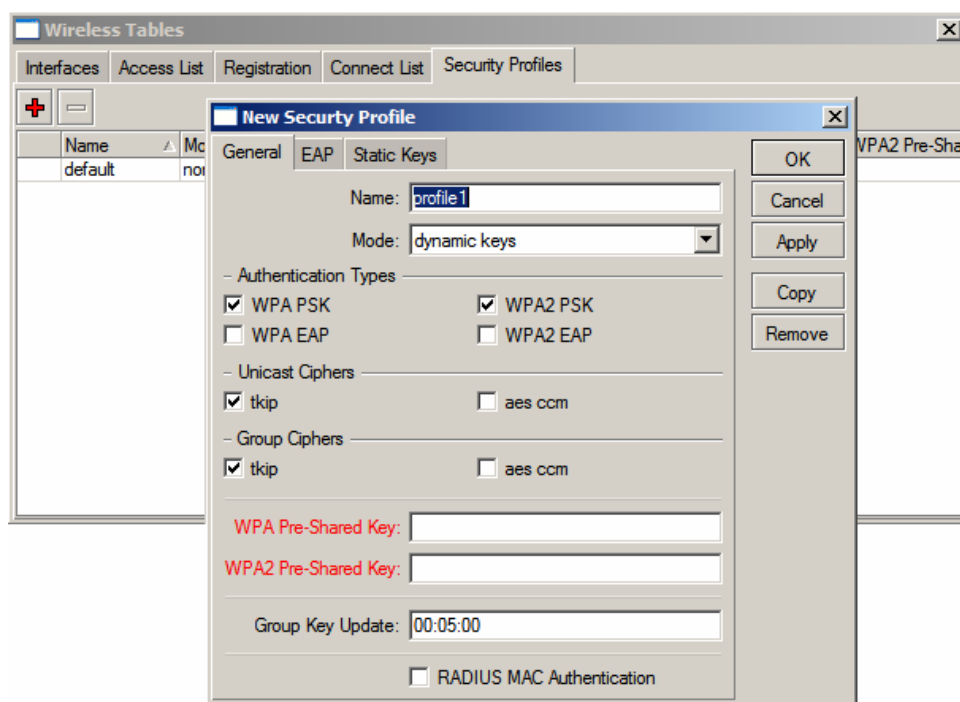
O Access List é utilizado pelo Access Point para restringir associações de clientes. Esta lista contém os endereços MAC de clientes e determina qual a ação deve ser tomada quando um cliente tenta conectar. A comunicação entre clientes da mesma interface, virtual ou real, também é controlada nos Access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

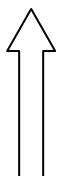


Na tabela Security Profiles são definidos os perfis de segurança da parte Wireless que poder ser utilizados no RouterOS.

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



*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

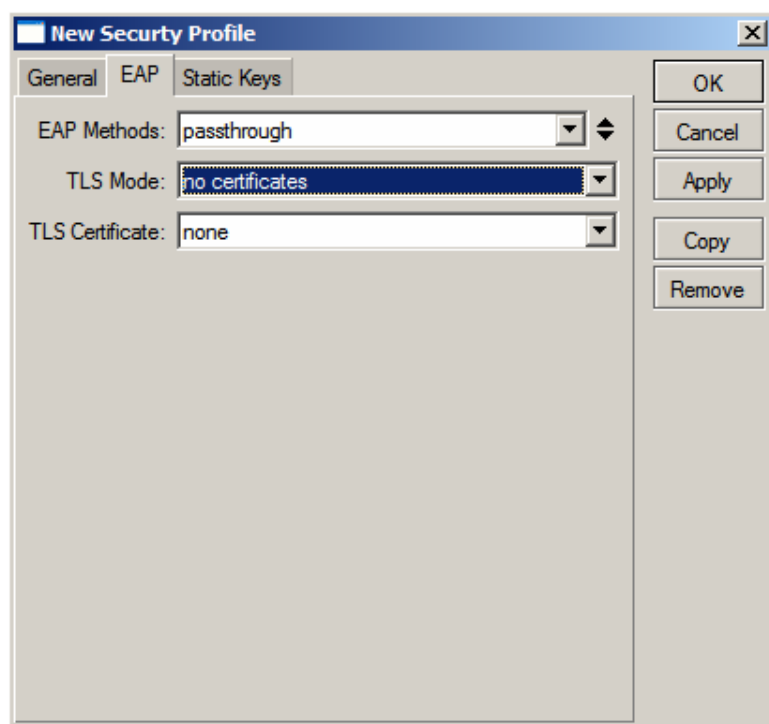
- TKIP: Protocolo de integridade de chave Temporal. Método utilizado durante algum tempo para contornar problemas da WEP (Proxim implementa como WEP Plus).
- AES CCM: Método de criptografia WPA mais seguro, que utiliza algoritmo AES.
- PSK (Pré Shared Key): chave compartilhada entre dois dispositivos.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



- Passthrough: 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 Diffie-Hellman.
 - 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

A screenshot of the 'New Security Profile' dialog box in a software application. The dialog has a title bar with a close button. It contains three tabs: 'General', 'EAP', and 'Static Keys'. The 'Static Keys' tab is selected. It features four rows for keys, each with a dropdown menu set to 'none' and a text field preceded by '0x'. Below these is a 'Transmit Key:' dropdown set to 'key 0'. At the bottom is a 'St. Private Key:' dropdown set to 'none' and a text field preceded by '0x'. On the right side, there are five buttons: 'OK', 'Cancel', 'Apply', 'Copy', and 'Remove'.



Referências:

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

Cópia autorizada: Marcelo Carvalho - MACNet (AWS)