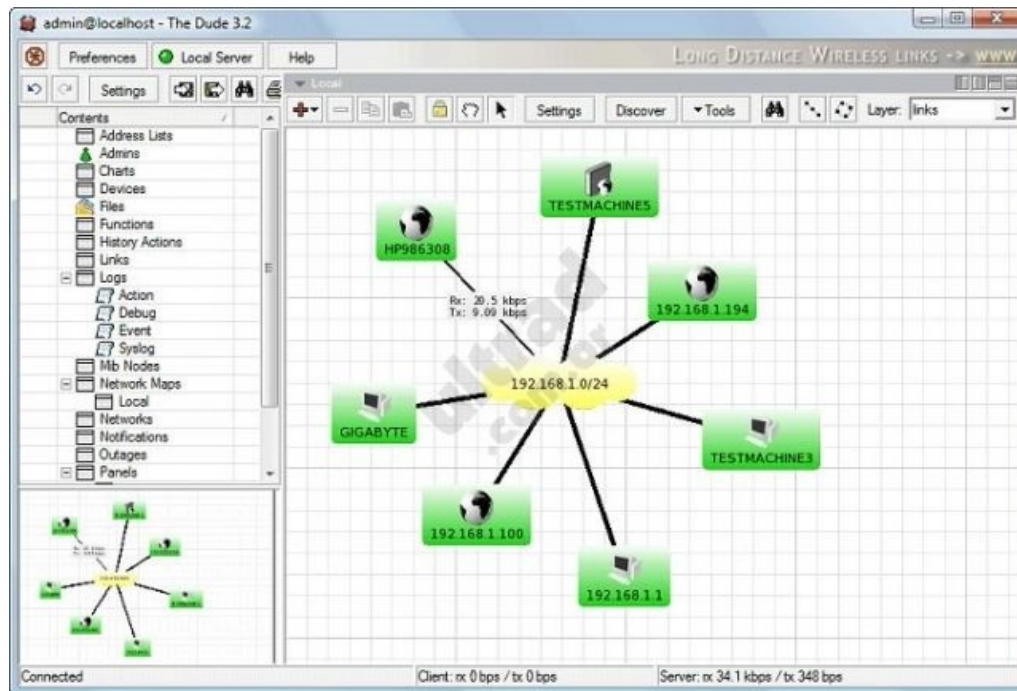


The Dude “O Cara”

Mini Curso



MUM – Brasil – Novembro de 2009
Eng. Wardner Maia

Nome: Wardner Maia

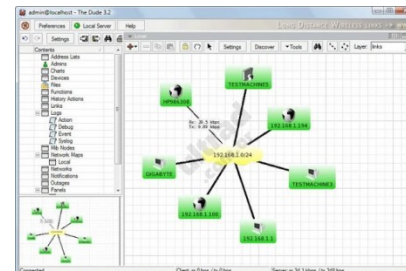
- Engenheiro Eletricista modalidade Eletrotécnica/Eletrônica/Telecomunicações
- Provedor de Internet desde 1995, utilizando rádio frequência para provimento de acesso desde 2000
- Ministra treinamentos em rádio frequência desde 2002 e em Mikrotik desde 2006
- Certificações Mikrotik:
 - Trainer (2007) – Riga, Latvia
 - MTCWE, MTCRE (2008) – Krakow, Poland
 - MTCUME, MTCTE (2009) – Praga, Czech Republik

MD Brasil – TI & Telecom

- Operadora de Serviços de Comunicação Multimídia e Serviços de Valor Adicionado
- Distribuidora oficial de Hardware e Software Mikrotik
- Integradora e fabricante de equipamentos com produtos homologados na Anatel.
- Parceira da Mikrotik em treinamentos

www.mdbrasil.com.br / www.mikrotikbrasil.com.br

Motivação e Objetivos



O Dude é um potente sistema de monitoramento de Redes, Dispositivos e Serviços, mantido pela Mikrotik que, mesmo sendo livre de custos de licença, tem um uso modesto entre operadores brasileiros.

O objetivo dessa apresentação, que tem o nome de “mini Curso” é fornecer uma receita básica para a implantação do DUDE de uma forma organizada e segura em redes de operadores pequenos e médios que ainda não o utilizem.

Espera-se ao final dessa pequena apresentação que os participantes que ainda não instalaram e utilizaram o DUDE tenham um guia prático de como começar essa tarefa, incentivando assim a sua disseminação.

AGENDA

Introdução

- O que é
- Porque utilizar

Instalação

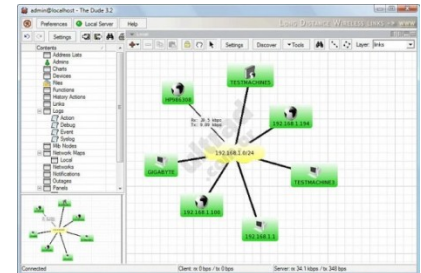
- Windows
- Linux
- RouterOS

Conceitos Gerais

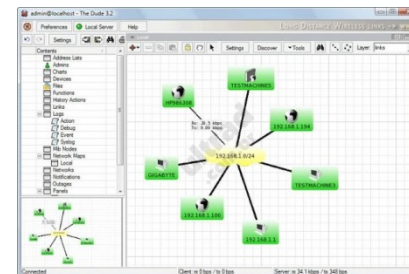
- Server/Client/Agent
- Charts/Dependencias

Utilizando o Dude:

- Criando o desenho da rede, dispositivos, alertas, notificações
- Trabalhando com SNMP



O que é o DUDE



Como ferramenta de Monitoramento:

→ Fornece informações acerca de quedas e restabelecimentos de redes, serviços, assim como uso de recursos de equipamentos.

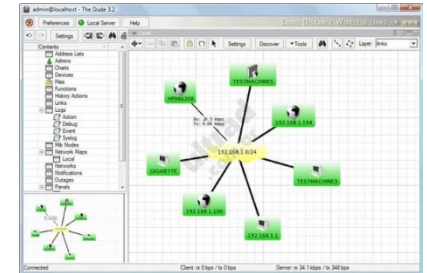
→ Permite o mapeamento da rede com gráficos da topologia da rede e relacionamentos lógicos entre os dispositivos

→ Notificações via audio/vídeo/email acerca de eventos

→ Gráfico de serviços mostrando, latencia, tempos de resposta de DNS, utilização de banda, informações físicas de links, etc.

→ Monitoramento de dispositivos não RouterOS com SNMP..

O que é o DUDE



Como ferramenta de Gerenciamento:

- Possibilidade de utilizar ferramentas para acesso direto a dispositivos da rede a partir do diagrama da mesma.
 - Acesso direto a dispositivos Mikrotik RouterOS através do Winbox
 - Armazenamento de histórico de eventos (logs) de toda a rede, com momentos de queda, restabelecimentos, etc.
 - Possibilidade de utilizar SNMP também para a tomada a tomada de decisões (SNMP set)
- (V. MUM Czech Republic 2009 – Andrea Coppini)

Instalando o DUDE

Instalando no Windows:

The Dude for Windows



Optional RouterOS package

- For X86 (RB200, PC)
- For MIPS-LE (RB100, RB500)
- For MIPS-BE (RB400)
- For PPC (RB300, RB600, RB1000)

→ Fazer o download, clicar no executável e responder sim para todas perguntas 😊

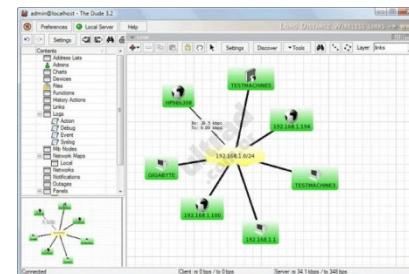
Instalando no Linux:

→ Instalar o Wine e a partir daí proceder como no Windows.

Instalando em uma Routerboard ou PC com Mikrotik

→ Baixar o pacote referente a arquitetura específica, enviar para o equipamento via ftp ou Winbox e bootar o mesmo

Instalação em Routerboards

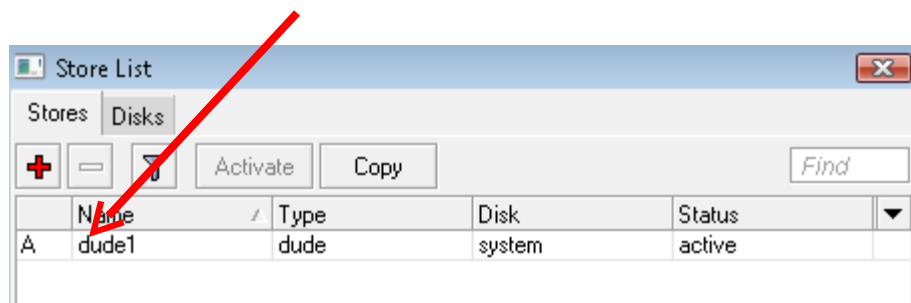
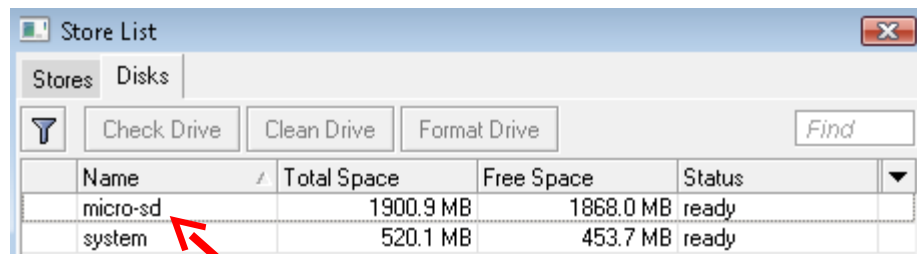
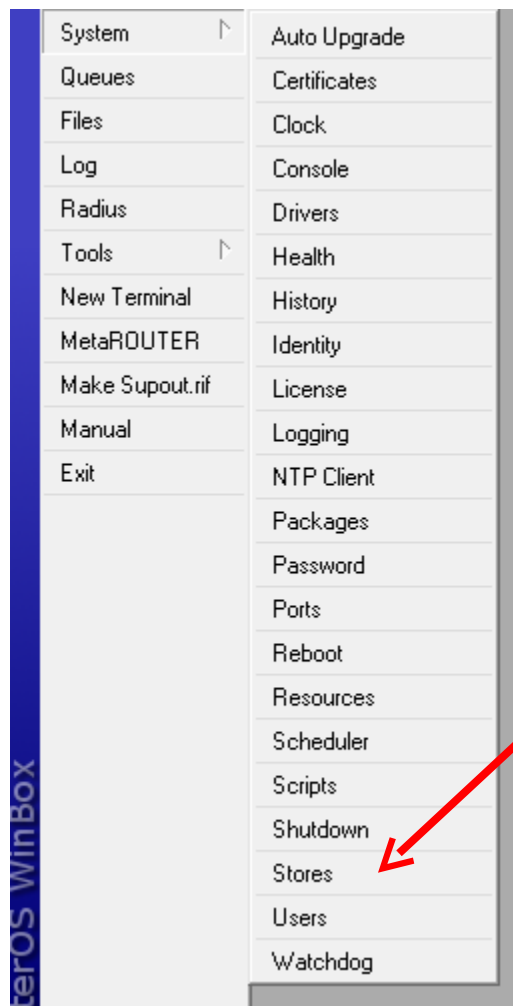


O espaço em disco consumido pelo DUDE é considerável devido, entre outras coisas, aos gráficos e logs a serem armazenados. Assim, no caso de instalação em Routerboards é aconselhável o uso daquelas que possuam possibilidade de armazenamento adicional, como

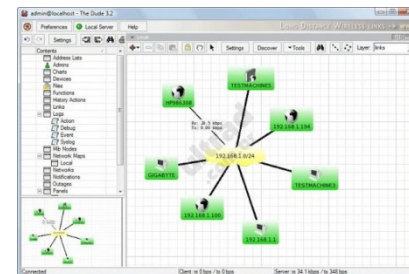
- RB 433UAH – aceita HD externo via USB
- RB 450G – aceita micro SD
- RB 600A – aceita micro SD
- RB 1000 – aceita flash card

OBS: É possível instalar em equipamentos sem as capacidades acima, porém poderão ocorrer problemas de perda de dados e impossibilidade de efetuar backup.

Instalação em Routerboards

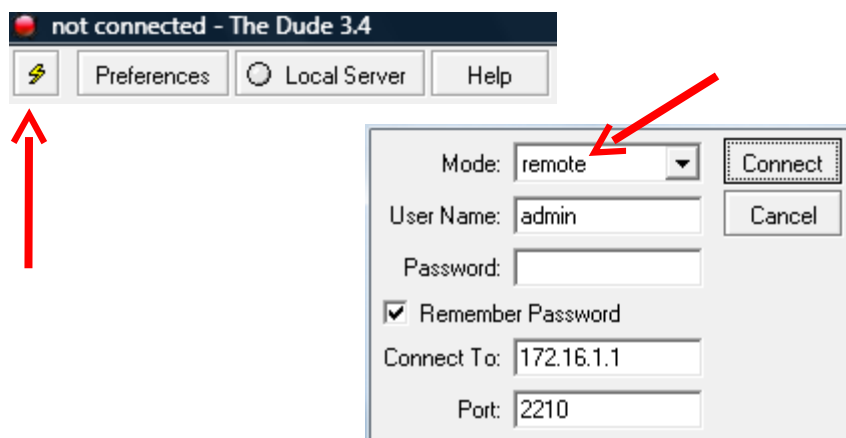


Começando usar o DUDE

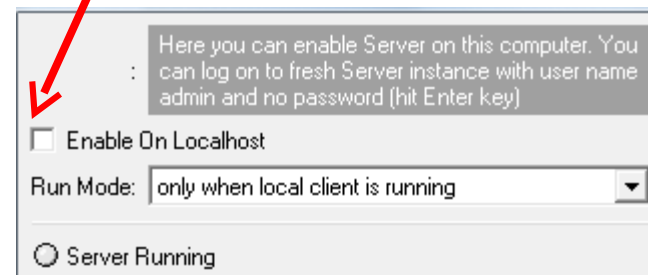


A instalação do DUDE em Windows ou Linux sempre instala o Cliente e o Servidor e no primeiro uso ele sempre irá tentar usar o Servidor Local (localhost).

Caso queira se conectar em outro DUDE (por exemplo instalado em outra Routerboard) clique em



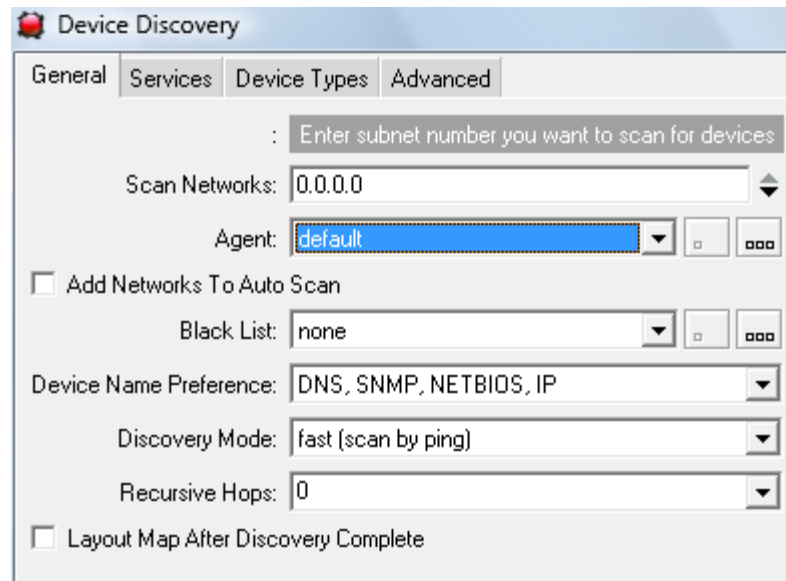
Para desabilitar o Servidor Local:



Começando usar o DUDE Auto Discovery

O auto discovery permite que o Servidor DUDE localize os dispositivos de seu segmento de rede, através de provas de ping, arp, snmp, etc e por serviços.

Outros segmentos de redes que tenham Mikrotiks podem também ser mapeados por seus vizinhos (neighbours)



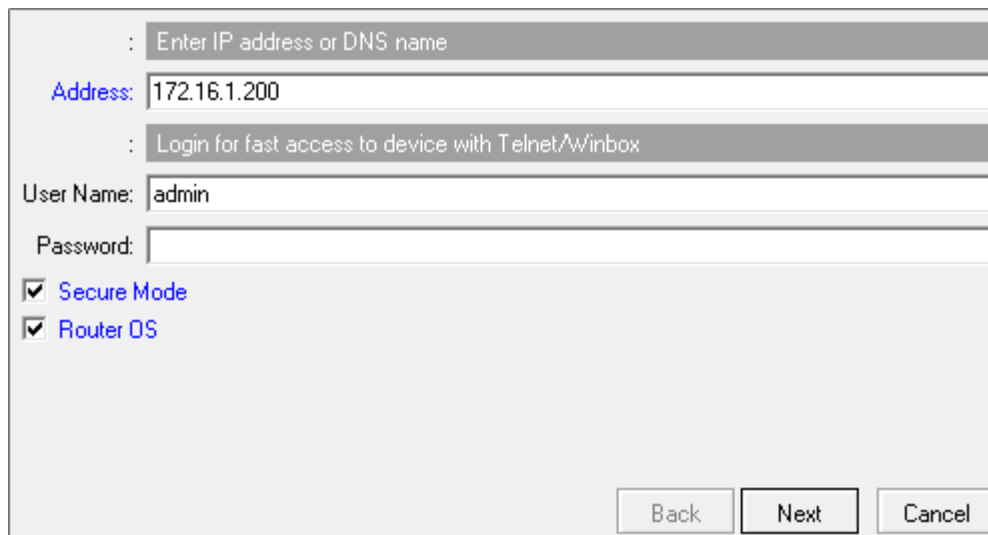
The screenshot shows the 'Device Discovery' window with the 'General' tab selected. The interface includes the following fields and options:

- Scan Networks:** A text field containing '0.0.0.0' with a dropdown arrow on the right.
- Agent:** A dropdown menu showing 'default'.
- Add Networks To Auto Scan:** An unchecked checkbox.
- Black List:** A dropdown menu showing 'none'.
- Device Name Preference:** A dropdown menu showing 'DNS, SNMP, NETBIOS, IP'.
- Discovery Mode:** A dropdown menu showing 'fast (scan by ping)'.
- Recursive Hops:** A dropdown menu showing '0'.
- Layout Map After Discovery Complete:** An unchecked checkbox.

Conselho amigo: Se vai usar o DUDE para fazer um bom controle de sua rede esqueça o auto discovery !

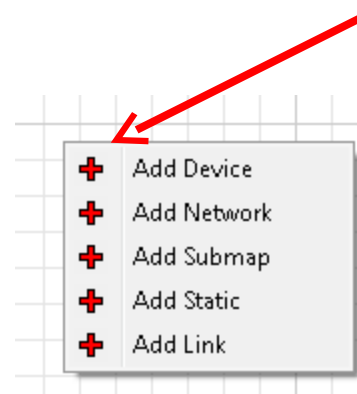
Começando o desenho da Rede Adicionando dispositivos

O Mikrotik tem um Wizard para a criação de dispositivos. Informe o IP e, se for Mikrotik clique em RouterOS



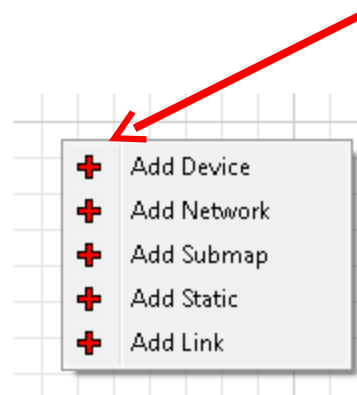
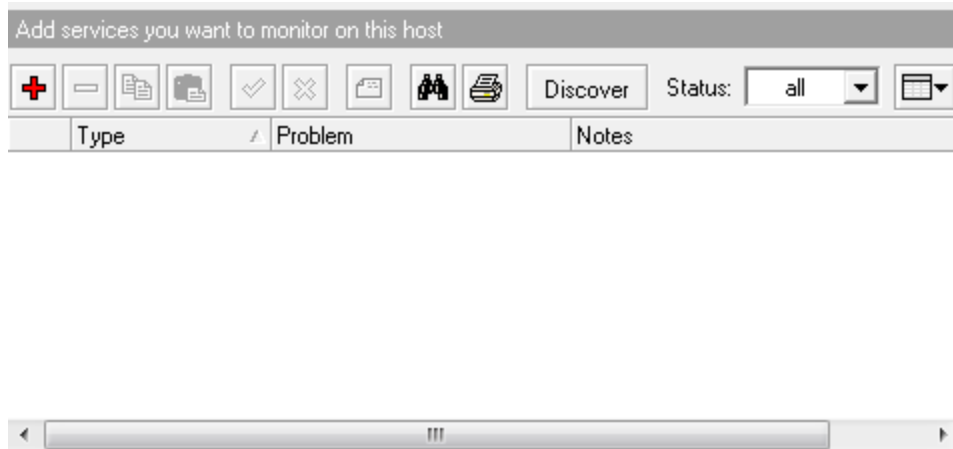
The screenshot shows a 'Wizard' dialog box for adding a device. It has a title bar and a main area with the following fields and options:

- A label 'Enter IP address or DNS name' above a text input field containing '172.16.1.200'.
- A label 'Login for fast access to device with Telnet/Winbox' above a 'User Name' field containing 'admin' and a 'Password' field.
- Two checked checkboxes: 'Secure Mode' and 'Router OS'.
- At the bottom, three buttons: 'Back', 'Next', and 'Cancel'.



Começando o desenho da Rede Adicionando dispositivos

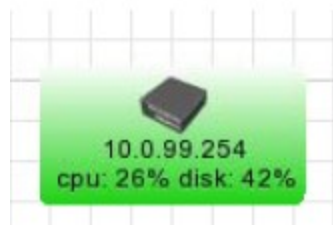
Em seguida descubra os serviços que estão rodando nesse equipamento.



Aproveite esse momento para refletir quanta coisa inútil e insegura pode estar rodando em sua rede ☺ Desabilite tudo que for desnecessário.

Começando o desenho da Rede Adicionando dispositivos

O dispositivo está criado.



Clique no dispositivo criado para ajustar vários parâmetros, mas principalmente:

- Nome para exibição
- Tipo do dispositivo

General Polling Services Outages Snmp RouterOS History

Name: MKBR-4

Addresses: 172.16.1.4

DNS Names:

DNS Lookup: address to name

DNS Lookup Interval: 60 min

MAC Addresses: 00:0C:42:04:04:04

MAC Lookup: ip to mac

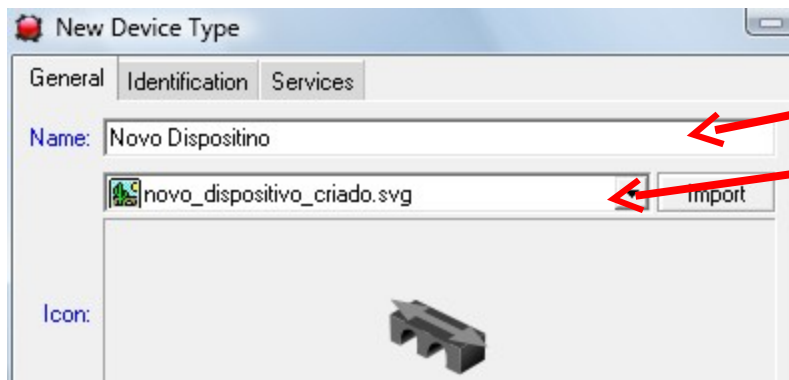
Type: Router

Começando o desenho da Rede Adicionando dispositivos não pré definidos

O DUDE possui vários dispositivos pré definidos mas pode-se criar novos dispositivos customizados para que o desenho realmente reflita a realidade prática.

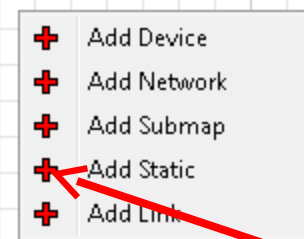
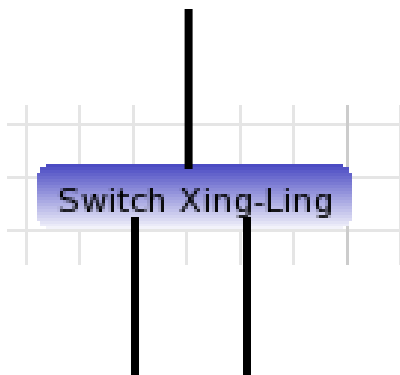
Por razões de produtividade é aconselhável que todos os dispositivos existentes na rede sejam criados com suas propriedades específicas antes do desenho da rede, mas nada impede que isso seja feito depois.

▼ Devices		
List	Tree	RouterOS Types Mac Mappings
#	Name	Notes
1	MikroTik Device	
2	Bridge	
3	Router	
4	Switch	
5	Dude Server	
6	Windows Computer	
7	HP Jet Direct	
8	FTP Server	
9	Mail Server	
10	Web Server	
11	DNS Server	
12	POP3 Server	
13	IMAP4 Server	
14	News Server	
15	Time Server	
16	Printer	
17	Some Device	



Começando o desenho da Rede Adicionando dispositivos estáticos

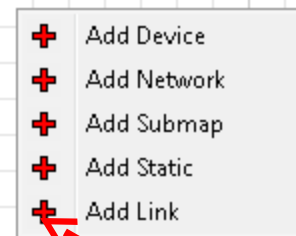
Quando a rede possui elementos não configuráveis por IP (switches L2 não gerenciáveis por exemplo), é necessário criar dispositivos estáticos para fazer as ligações.



Com isso pode-se completar o diagrama de rede de forma mais realista e parecida com a rede real.

Começando o desenho da Rede Criando os Links entre dispositivos

No mapa, clicar com o botão direito, selecionar Add Link e ligar os dispositivos linkados, informando:



Mastering Type:

→ RouterOS: Se o dispositivo for Mikrotik, habilita a escolha da Interface para mostrar velocidades e estado do link.

→ SNMP: para outros dispositivos que tenham suporte a snmp.

→ Simple: somente traça a linha mas não mostra informações.

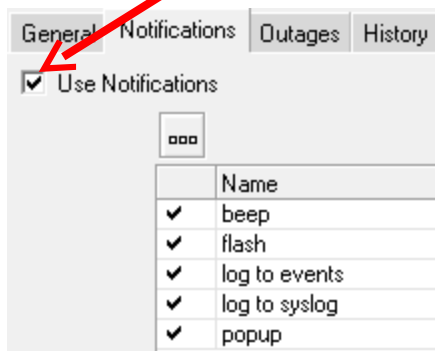
A screenshot of a configuration form for adding a link. It has several fields: 'Device' with a dropdown menu showing 'MKBR-4'; 'Mastering Type' with a dropdown menu showing 'routeros'; 'Interface' with a dropdown menu showing '(unknown)'; 'Speed' with a checked checkbox and a text input field containing '100000'; and 'Type' with a dropdown menu showing 'fast ethernet'. Four red arrows point to the 'Device', 'Mastering Type', 'Speed', and 'Type' fields.

Informando a velocidade máxima do link, ativa a sinalização do estado do mesmo.

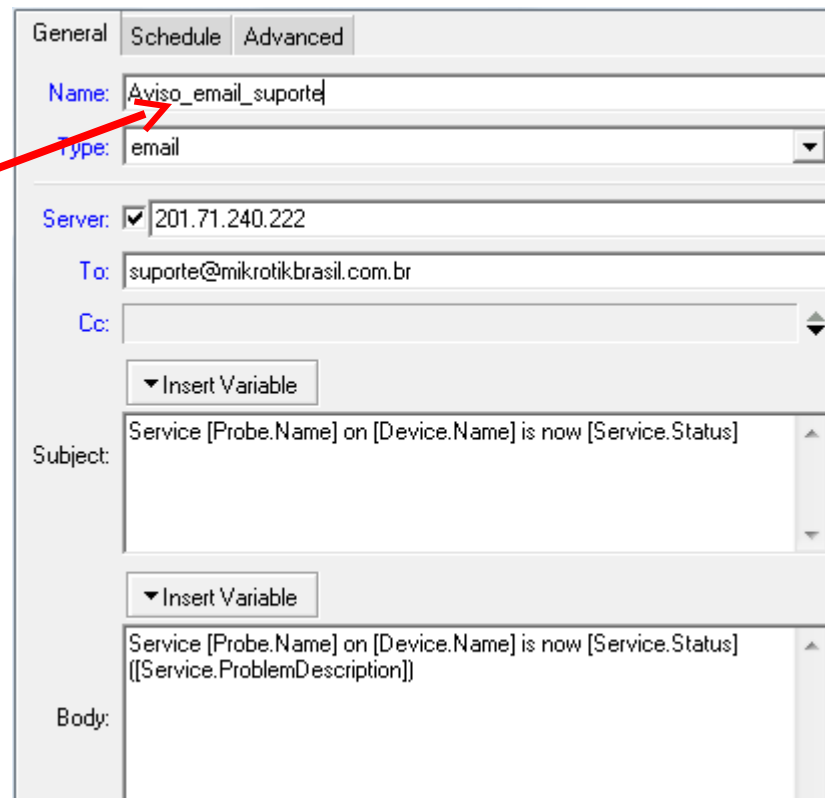
Notificações

Criando novos tipos de notificação

Duplo clique no dispositivo / clique no serviço e na guia notificação informar o tipo de notificação.



	Name
<input checked="" type="checkbox"/>	beep
<input checked="" type="checkbox"/>	flash
<input checked="" type="checkbox"/>	log to events
<input checked="" type="checkbox"/>	log to syslog
<input checked="" type="checkbox"/>	popup



General Schedule Advanced

Name: Aviso_email_suporte

Type: email

Server: ☒ 201.71.240.222

To: suporte@mikrotikbrasil.com.br

Cc:

▼ Insert Variable

Subject: Service [Probe.Name] on [Device.Name] is now [Service.Status]

▼ Insert Variable

Body: Service [Probe.Name] on [Device.Name] is now [Service.Status] ([Service.ProblemDescription])

Notificações“ao contrario”

Úteis quando se quer monitorar serviços que não devem estar ativos

General Schedule Advanced

Name:

Type:

Server: ☐

To:

Cc:

▼ Insert Variable

Subject:

▼ Insert Variable

Body:

General Schedule Advanced

Delay:

Repeat Interval:

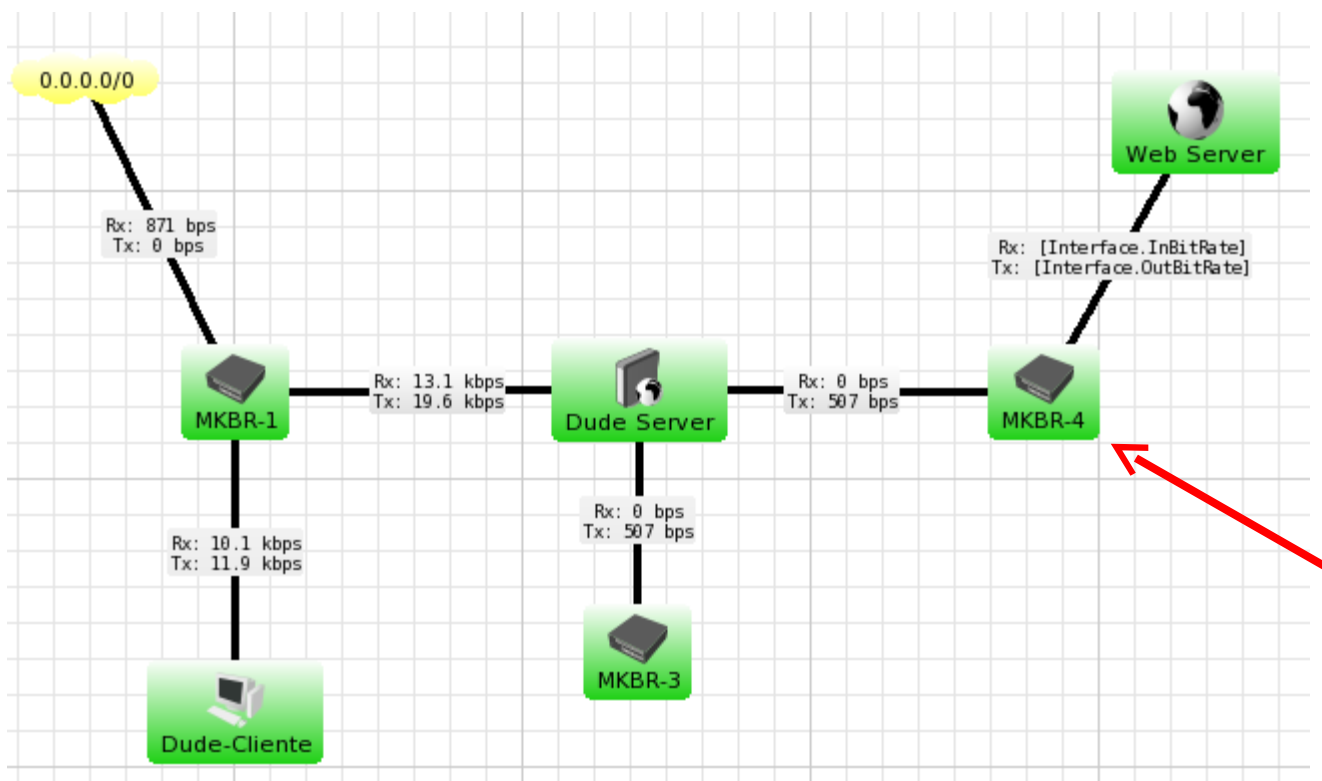
Repeat Count:

On Status:

	Name
	acked -> down
	acked -> unstable
	acked -> up
	down -> acked
	down -> unknown
✓	down -> up
	unknown -> down
	unknown -> unstable
	unknown -> up
	unstable -> acked
	unstable -> down
	unstable -> unknown
	unstable -> up
	up -> down
	up -> unknown
	up -> unstable

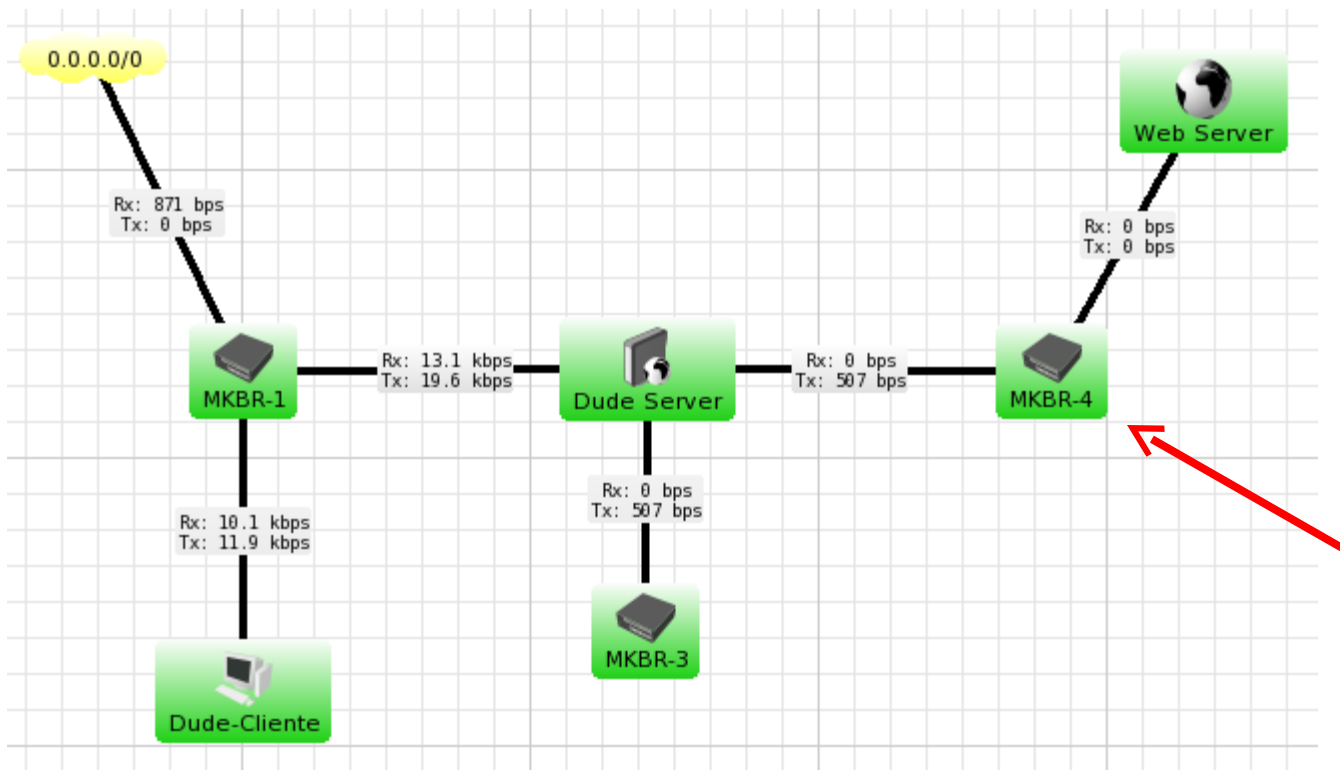
Eliminando notificações desnecessárias dependencias

Caso MKBR-4 caia, será gerada uma notificação desnecessária
referente ao Web Server



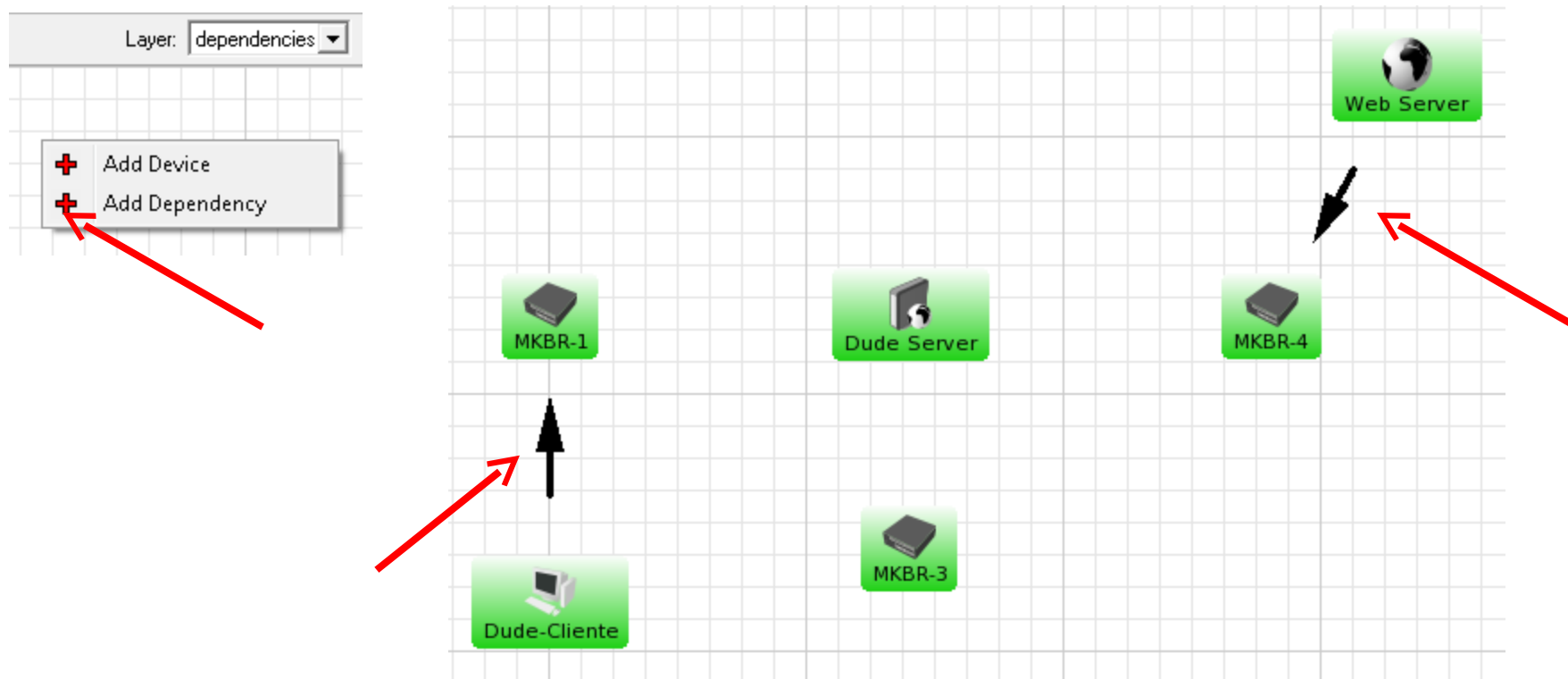
Eliminando notificações desnecessárias dependencias

Caso MKBR-4 caia, será gerada uma notificação desnecessária
referente ao Web Server

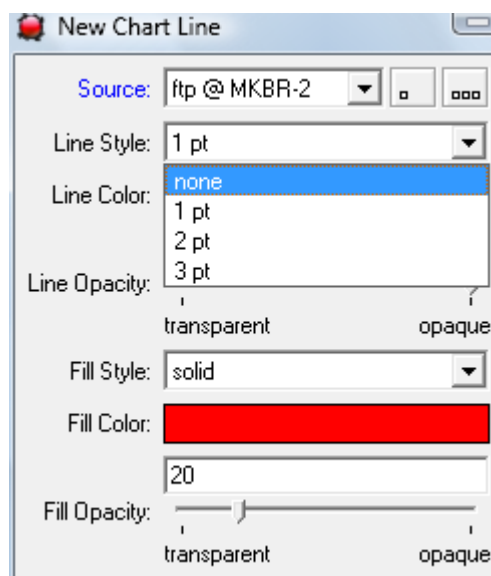
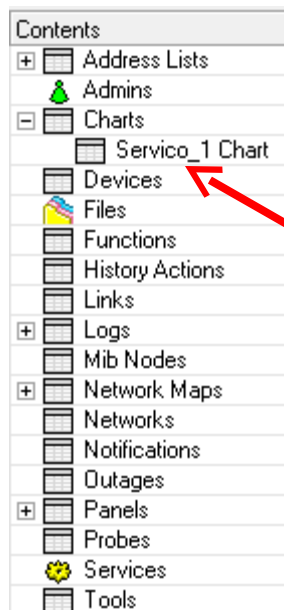


Eliminando notificações desnecessárias criando as dependencias

Mudando o layer para dependencias e informando todas,
notificações desnecessárias serão evitadas

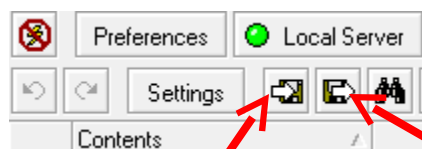


Gráficos de uso / performance, etc



Salvando as configurações

As configurações são salvas automaticamente na medida em que são feitas. Para ter um backup externo, use o export que será gerado um XML com todas as configurações que por sua vez podem ser importadas em outro DUDE.



Export

Import



RouterOS & DUDE & SNMP

SNMP

SNMP significa:

Simple Network Management Protocol

ou seja:

Protocolo Simples de Gerenciamento de Redes

- Protocolo suportado por vários fabricantes
- SNMP get – obtém diversas informações de dispositivos
- SNMP set – envia e interage com os dispositivos
- Versões do SNMP 1, 2 e 3.

SNMP e Mikrotik RouterOS

Simple Network Management Protocol

às vezes pode ser traduzido por::

Segurança Não é Meu Problema !

- Pequena segurança no SNMP-V1 e SNMP-V2,
 - String “community” trafega em texto plano.
 - É possível apenas restringir os IP's
- Segurança melhorada com SNMP-V3
 - Autorização com usuário e senha (MD5 + SHA1)
 - Criptografia com DES

SNMP e Segurança

Suporte ao SNMP V3 no Mikrotik RouterOS e

V 2.9x → não suporta

Anteriores a V3.14 → suporta, porem somente get

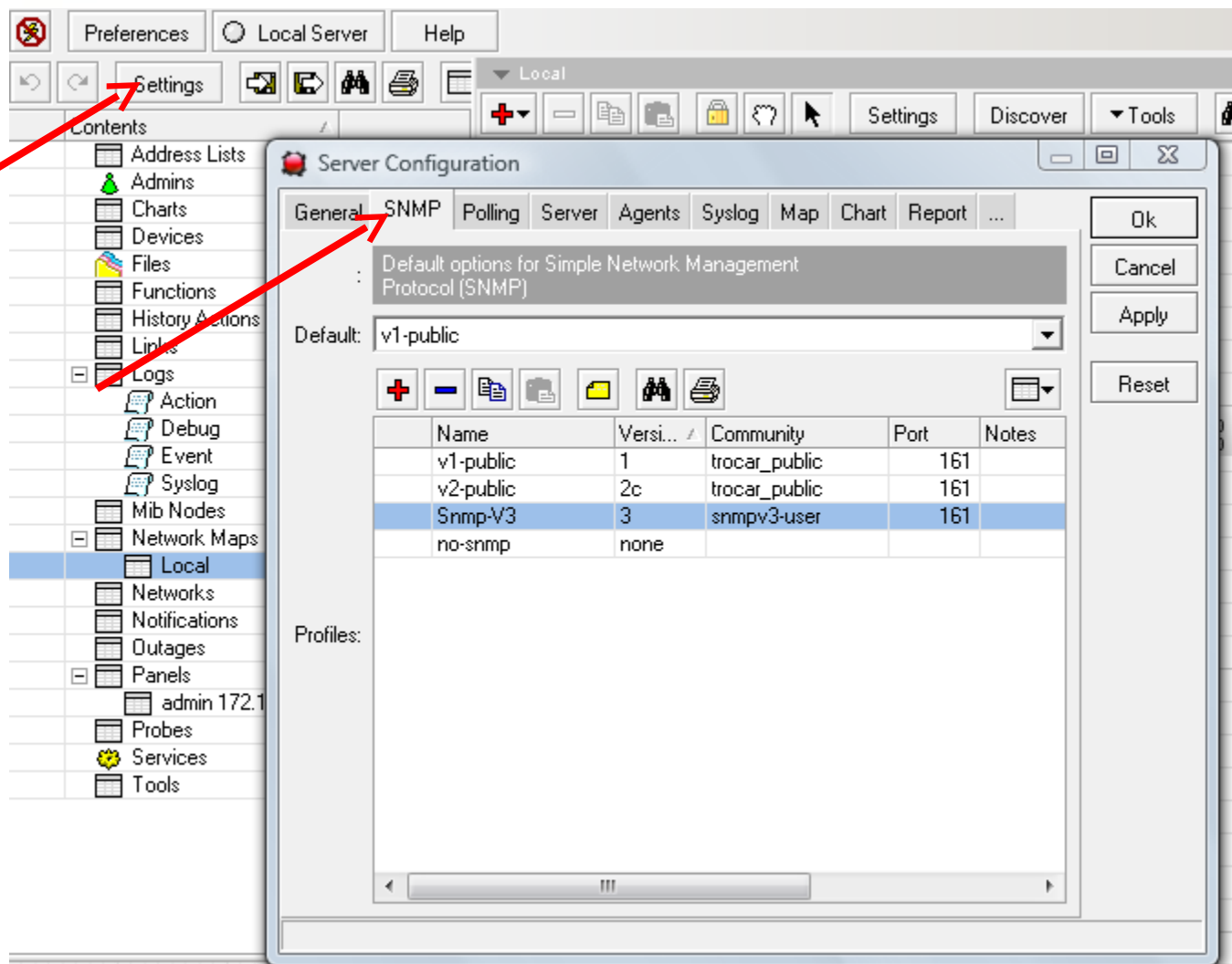
A partir da V3.14 e V4.x→ suportam get e set

SNMP e Segurança

Porque mesmo o acesso SNMP somente read é crítico

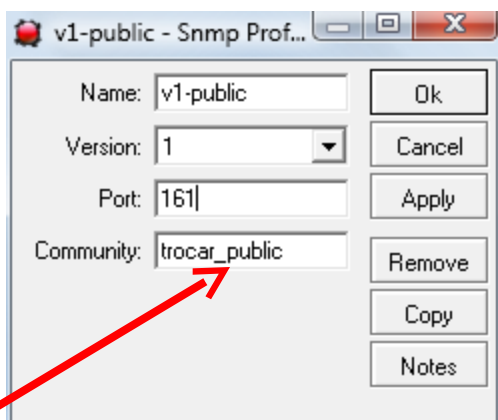
- Revela detalhes da estrutura interna da rede
- Monitora uso de CPU para medir ataque de DoS
- Espaço de HD e partição /var podem ser monitoradas para verificar quando não mais existe espaço para logs !

Atenção – Nunca deixe o SNMP habilitado com as strings “public” ou “private”



Criando os perfis de SNMP no DUDE

V1

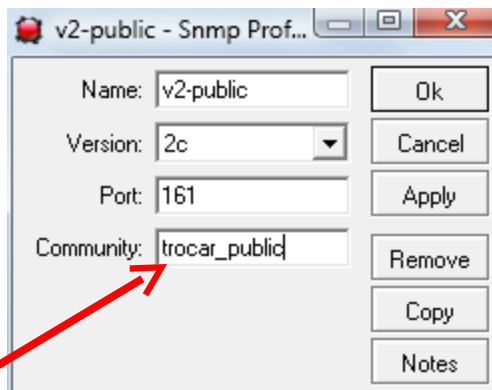


Dialog box titled "v1-public - Snmp Prof...". It contains the following fields and buttons:

- Name: v1-public
- Version: 1 (dropdown)
- Port: 161
- Community: trocar_public
- Buttons: Ok, Cancel, Apply, Remove, Copy, Notes

A red arrow points to the "Community" field.

V2

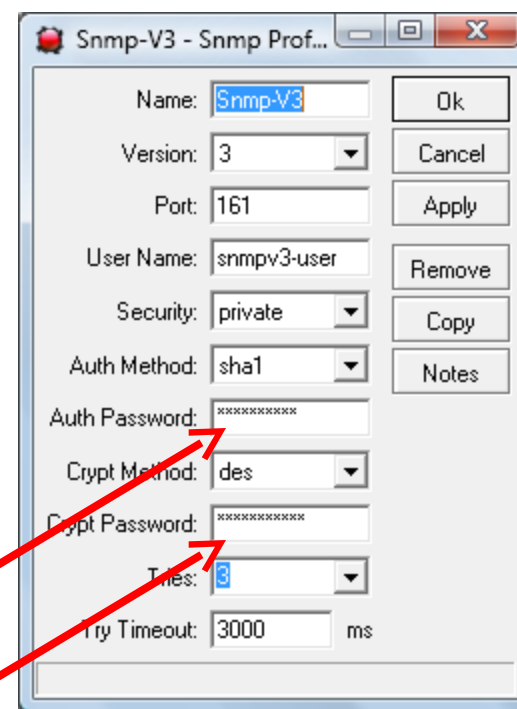


Dialog box titled "v2-public - Snmp Prof...". It contains the following fields and buttons:

- Name: v2-public
- Version: 2c (dropdown)
- Port: 161
- Community: trocar_public
- Buttons: Ok, Cancel, Apply, Remove, Copy, Notes

A red arrow points to the "Community" field.

V3

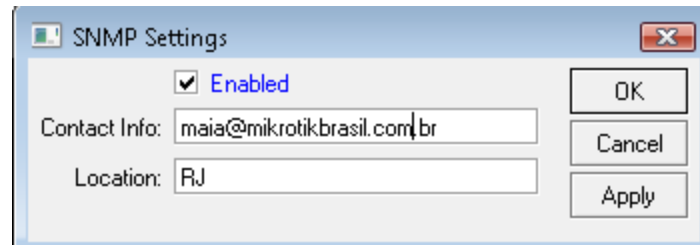
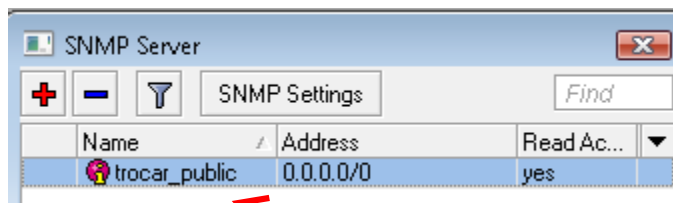
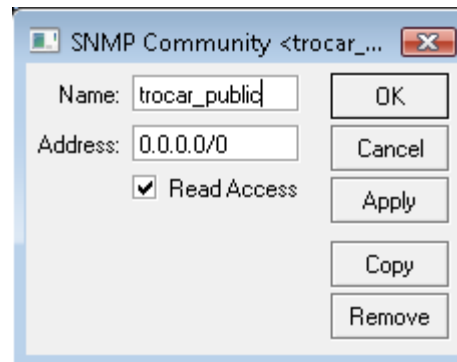
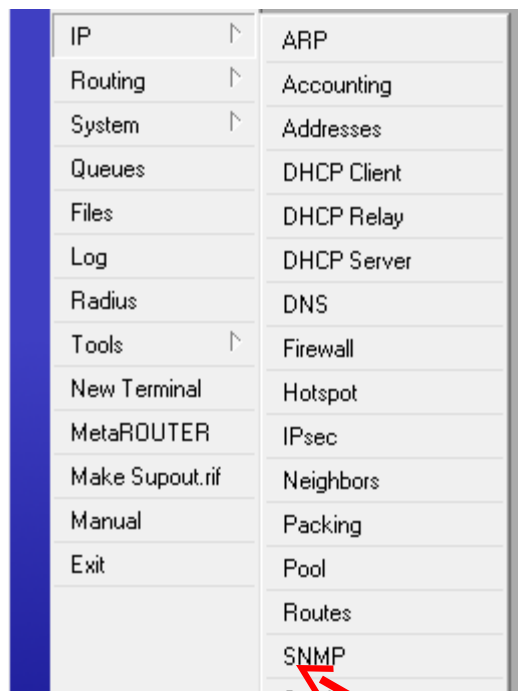


Dialog box titled "Snmp-V3 - Snmp Prof...". It contains the following fields and buttons:

- Name: Snmp-V3
- Version: 3 (dropdown)
- Port: 161
- User Name: snmpv3-user
- Security: private (dropdown)
- Auth Method: sha1 (dropdown)
- Auth Password: (masked with asterisks)
- Crypt Method: des (dropdown)
- Crypt Password: (masked with asterisks)
- Tries: 3 (dropdown)
- Try Timeout: 3000 ms
- Buttons: Ok, Cancel, Apply, Remove, Copy, Notes

Two red arrows point to the "Auth Password" and "Crypt Password" fields.

Configurações do SNMP v1 no Mikrotik RouterOS



Configurações de SNMP V3 no Mikrotik

Somente pela linha de comando

```
wmaia@MKBR-4] > snmp community add name=Snmp-V3 security=private  
authentication-protocol=SHA authentication-password=senha_auth encryption-  
protocol=DES encryption-password=senha_crypt read-access=yes
```

```
[admin@MKBR-4] > snmp community pr
```

#	NAME	ADDRESS	SECURITY	READ-ACCESS
0	trocar_public	0.0.0.0/0	none	yes
1	Snmp-V3	0.0.0.0/0	private	yes

```
[admin@MKBR-4] > 
```

Configurações do net-snmp para Linux e FreeBSD

1. Parar o snmpd:

```
/etc/init.d/snmpd stop
```

2. Configurar um usuário read-write

adicionar a linha a /etc/snmp/snmpd.conf:

```
rwuser usuario1 priv
```

3. Configurar o usuário read-write

adicionar linha a /var/lib/snmp/snmpd.conf:

```
createUser usuario1 SHA senha1 DES senha2
```

4. Reiniciar o serviço

```
/etc/init.d/snmpd start
```

Configurações do net-snmp para Linux e FreeBSD

1. Configurar um usuário read-only
adicionar linha a /etc/snmp/snmpd.conf:
rouser usuario_ro priv

2. Clonar usuário como o utilitário snmpusm

```
snmpusm -v3 -u usuario1 -n "" -l authPriv -a SHA -A  
senha1 -x DES -X senha2 localhost create usuario2  
usuario1
```

3. Restartar o serviço
/etc/init.d/snmpd start

Configurações do net-snmp para Linux e FreeBSD

1. Mudar senha de autenticação:

```
snmpusm -v 3 -u usuario1 -n "" -l authPriv -a SHA -A  
senha1 -x DES -X senha2 localhost -Ca passwd  
senha1 novassenha1 usuario2
```

2. Mudar senha de Criptografia:

```
snmpusm -v 3 -u usuario1 -n "" -l authPriv -a SHA -A  
senha1 -x DES -X senha2 localhost -Cx passwd  
senha2 novassenha2 usuario2
```

Mensagem de retorno: SNMPv3 Key(s) successfully changed.

Referências:

- Trabalho de Patrik Schaub – MUM 2009 República Checa
- Trabalho de Andrea Coppini – MUM 2009 República Checa
- Trabalho de Mike Delp – MUM 2009 Estados Unidos
- WIKI da Mikrotik



Obrigado !

Wardner Maia – maia@mikrotikbrasil.com.br



Localização do Restaurante

Restaurante Temperarte

Hotel South American

