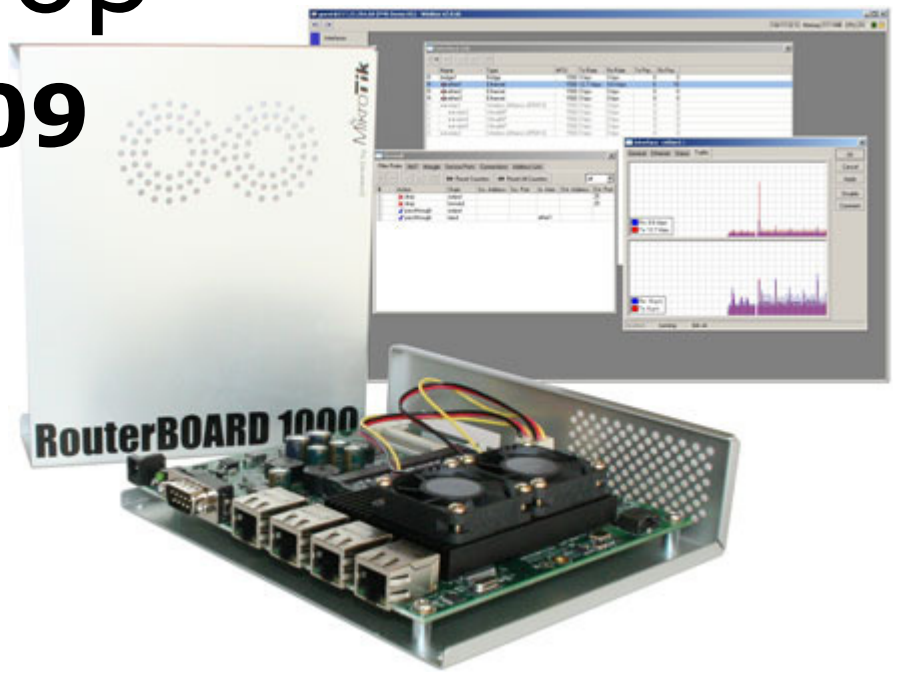
Dude Workshop

MUM Prague 2009

by Patrik Schaub



FMS Internetservice, www.fmsweb.de
info@fmsweb.de, Phone: +49 761 2926500

copyright FMS 2009

Contents

1. About FMS
2. Dude intro
3. Dude and secure SNMP
4. Charts and datastores

About FMS

- Founded in 1999

- Distribution, http://shop.fmsweb.de
- Consulting, http://www.fmsweb.de
- Training, http://www.mikrotik-training.de
- Support contracts

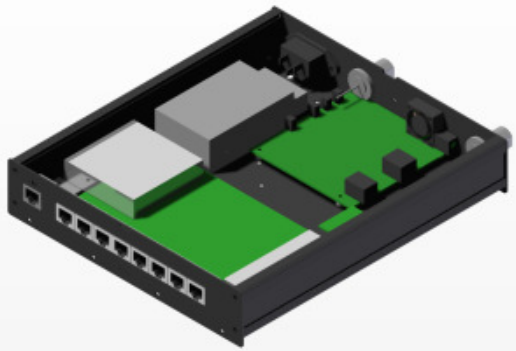
- Running a smal datacenter

New: mikroCase enclosures

- For RouterBOARD, ALIX and ITX
- Integrated power supply
- Integrated DSL modem possible
- Up to two mainboards and two DSL modems in 1U

New: mikroCase enclosures

- Distributor and reseller inquiries welcome
- Custom designs possible

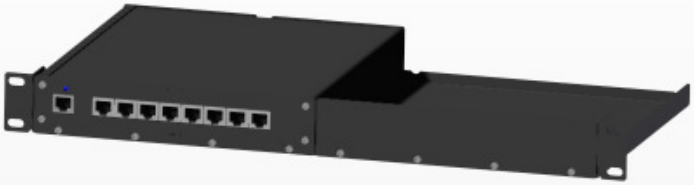


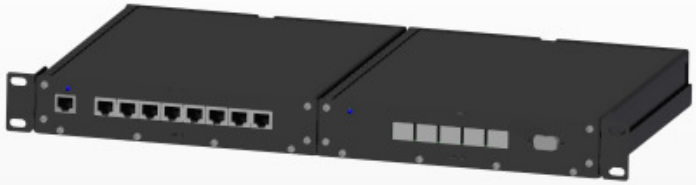
DSL Modem

RB493 + DSL Modem

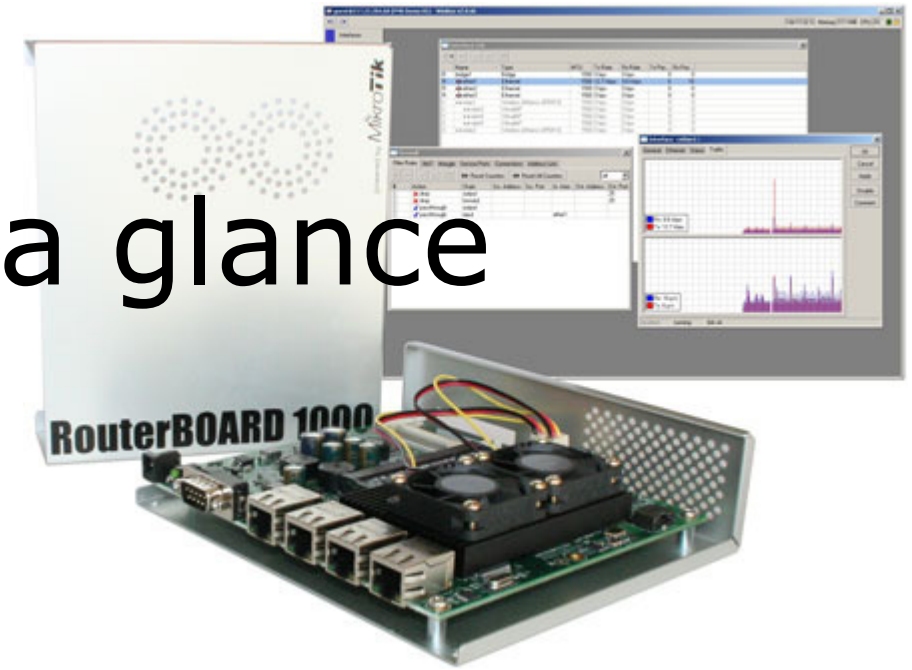
mikroCase distributors

- www.wirelessconnect.eu (Ireland, UK)
- www.mdbrasil.com (Brasil)



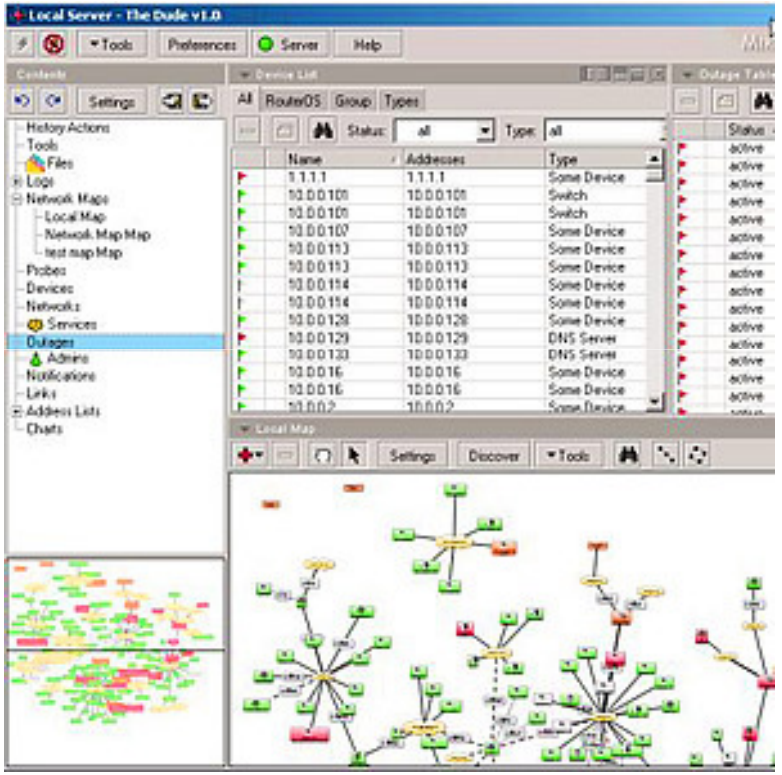


The Dude at a glance



A powerfull network monitoring system

- Graphical representation
- Monitoring
- Notifications
- Statistics
- Central admnistration



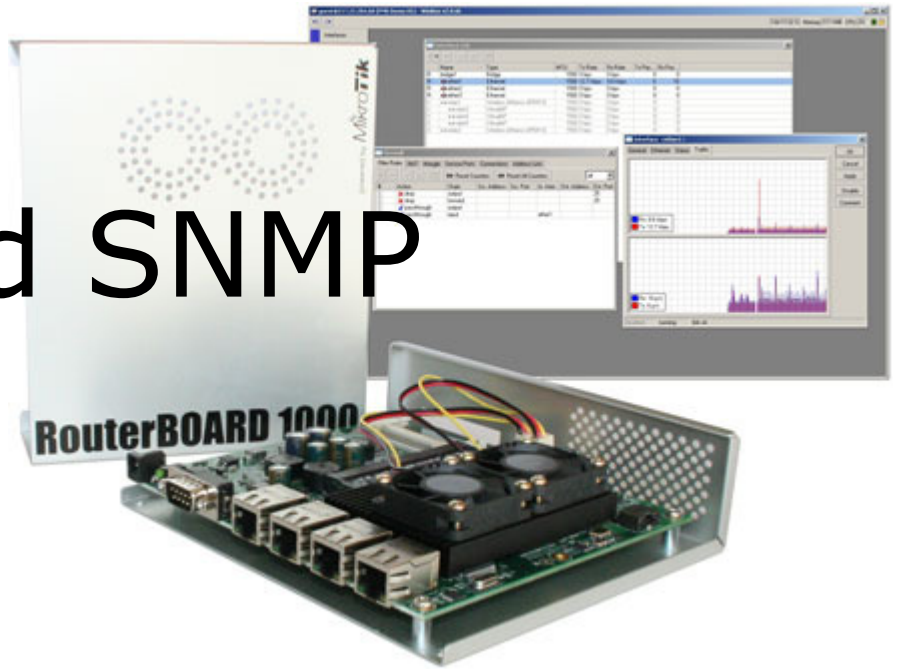
The Dude‘s architecture

- Client / Server modle
- Multilple clients can connect to one server
- Server on Windows, Linux, MAC and RouterOS
- Client on Windows, Linux, MAC and Webclient

Quick start for first time users

- Create a device manually
- or use auto discovery

The Dude and SNMP



SNMP Basics

- Simple Network Management Protocol

- Vendor independent management
- Read and write device statistics and configuration
- Major versions 1, 2c, 3
- Supported by many network devices, Linux, BSD, Windows …

SNMP & security

- „Security is Not My Problem“
- Little security in v1 and v2c
  (2p and 2u are rarely used)
  - Clear text community string („username“)
  - Limiting access by IP adress
- Major security changes in v3
  - Authorisation (User + Pass) with MD5/SHA1
  - Encryption with DES

Public read access critical?

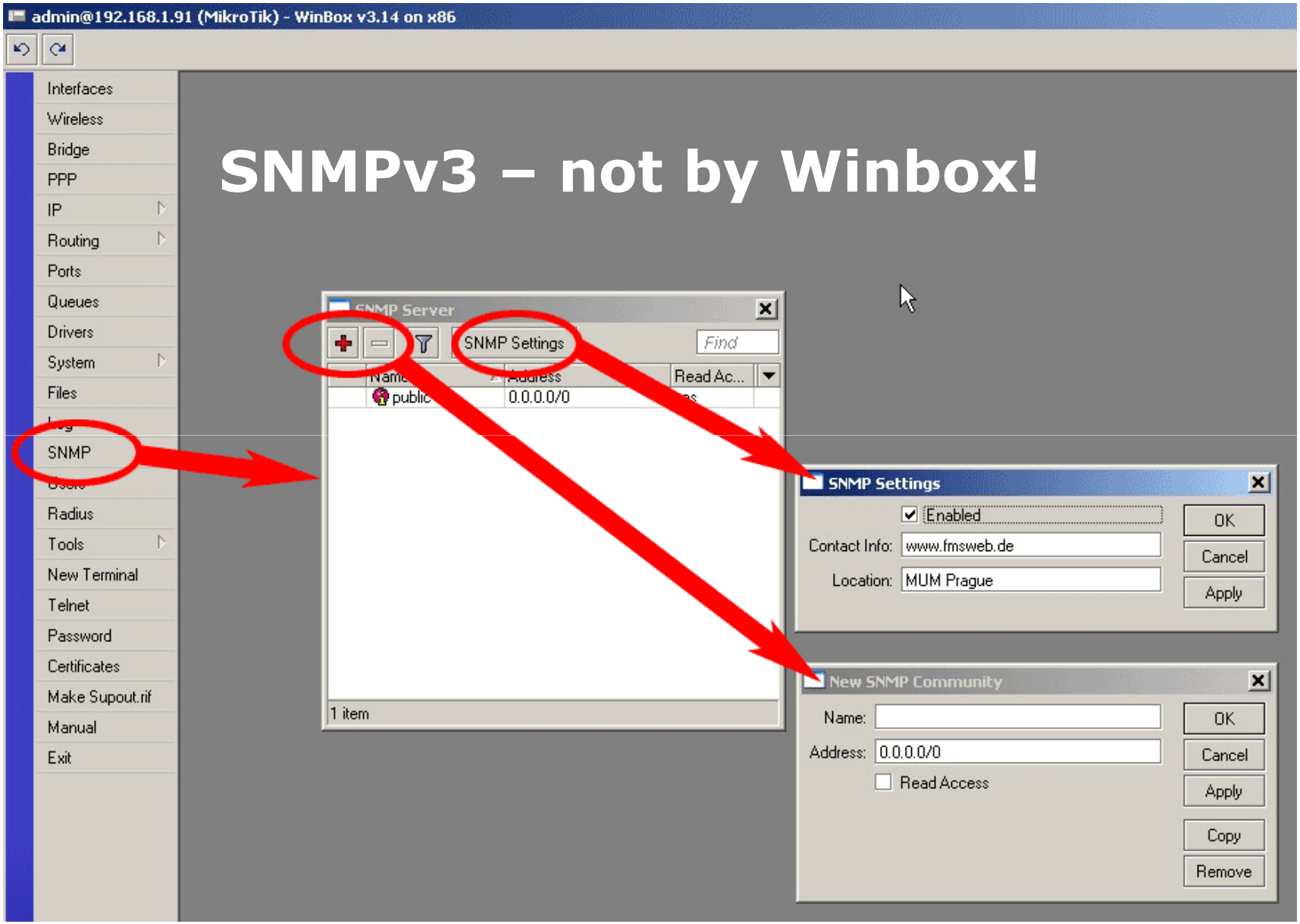
- YES, e.g. monitoring
  - CPU load during DOS attack
  - HDD space of /var to find out when no more logs can be written
  - Get details about internal network structure

TIP: NEVER USE STANDARD COMMUNITY „PUBLIC“ or „PRIVATE“

Who supports SNNMP v3?

- The Dude does
- net-snmp does
- Many network devices do

- And what about RouterOS… ?


admin@192.168.1.91 (MikroTik) - WinBox v3.14 on x86
Interfaces
Wireless
Bridge
PPP
IP
Routing
Ports
Queues
Drivers
System
Files
SNMP
Radius
Tools
New Terminal
Telnet
Password
Certificates
Make Supout.rif
Manual
Exit
SNMPv3 – not by Winbox!
SNMP Server
SNMP Settings
Find
Name
Address
Read Ac...
public
0.0.0.0/0
1 item
SNMP Settings
Enabled
Contact Info: www.fmsweb.de
Location: MUM Prague
OK
Cancel
Apply
New SNMP Community
Name:
Address: 0.0.0.0/0
Read Access
OK
Cancel
Apply
Copy
Remove

SNMP Settings

v 2.9.51

Terminal

```
  MMM      MMM       KKK                          TTT
  MMMM    MMMM       KKK                          TTT
  MMM MMMM MMM  III  KKK  KKK  RRRRRR     000000
  MMM  MM  MMM  III  KKKKK     RRR  RRR  000  000
  MMM      MMM  III  KKK KKK   RRRRRR    000  000
  MMM      MMM  III  KKK  KKK  RRR  RRR   000000

  MikroTik RouterOS 2.9.51 (c) 1999-2008       http:/

Terminal vtl02 detected, using multiline input mode
[admin@MikroTik] > /snmp print
   enabled: yes
   contact: "www.fmsweb.de"
  location: "MUM Prague"
```

v 3.0

```
[admin@MikroTik] > /snmp print
          enabled: yes
          contact: "www.fmsweb.de"
         location: "MUM Prague"
        engine-id: ""
     engine-boots: 2
      time-window: 0
        trap-sink: 0.0.0.0
   trap-community: (unknown)
    trap-version: 1
[admin@MikroTik] >
```

v 3.14

Terminal

```
[admin@MikroTik] > /snmp print
          enabled: yes
          contact: "www.fmsweb.de"
         location: "MUM Prague"
        engine-id: ""
     engine-boots: 3
      time-window: 0
        trap-sink: 0.0.0.0
   trap-community: (unknown)
    trap-version: 1
[admin@MikroTik] >
```

SNMP Community Settings

v 2.9.51

```
  MMM      MMM       KKK
  MMMM    MMMM       KKK
  MMM MMMM MMM  III  KKK  KKK  RRRRRR     000000
  MMM  MM  MMM  III  KKKKK     RRR  RRR  000  000
  MMM      MMM  III  KKK KKK   RRRRRR    000  000
  MMM      MMM  III  KKK  KKK  RRR  RRR   000000

  MikroTik RouterOS 2.9.51 (c) 1999-2008       http:/

Terminal vtl02 detected, using multiline input mode
[admin@MikroTik] > /snmp community print value-list
         name: "public"
      address: 0.0.0.0/0
  read-access: yes

[admin@MikroTik] >
```

v 3.0

```
[admin@MikroTik] > /snmp community print value-list
                    name: "public"
                 address: 0.0.0.0/0
                security: none
             read-access: yes
  authentication-password: ""
      encryption-password: ""
  authentication-protocol: MD5
      encryption-protocol: DES
[admin@MikroTik] >
```

Terminal

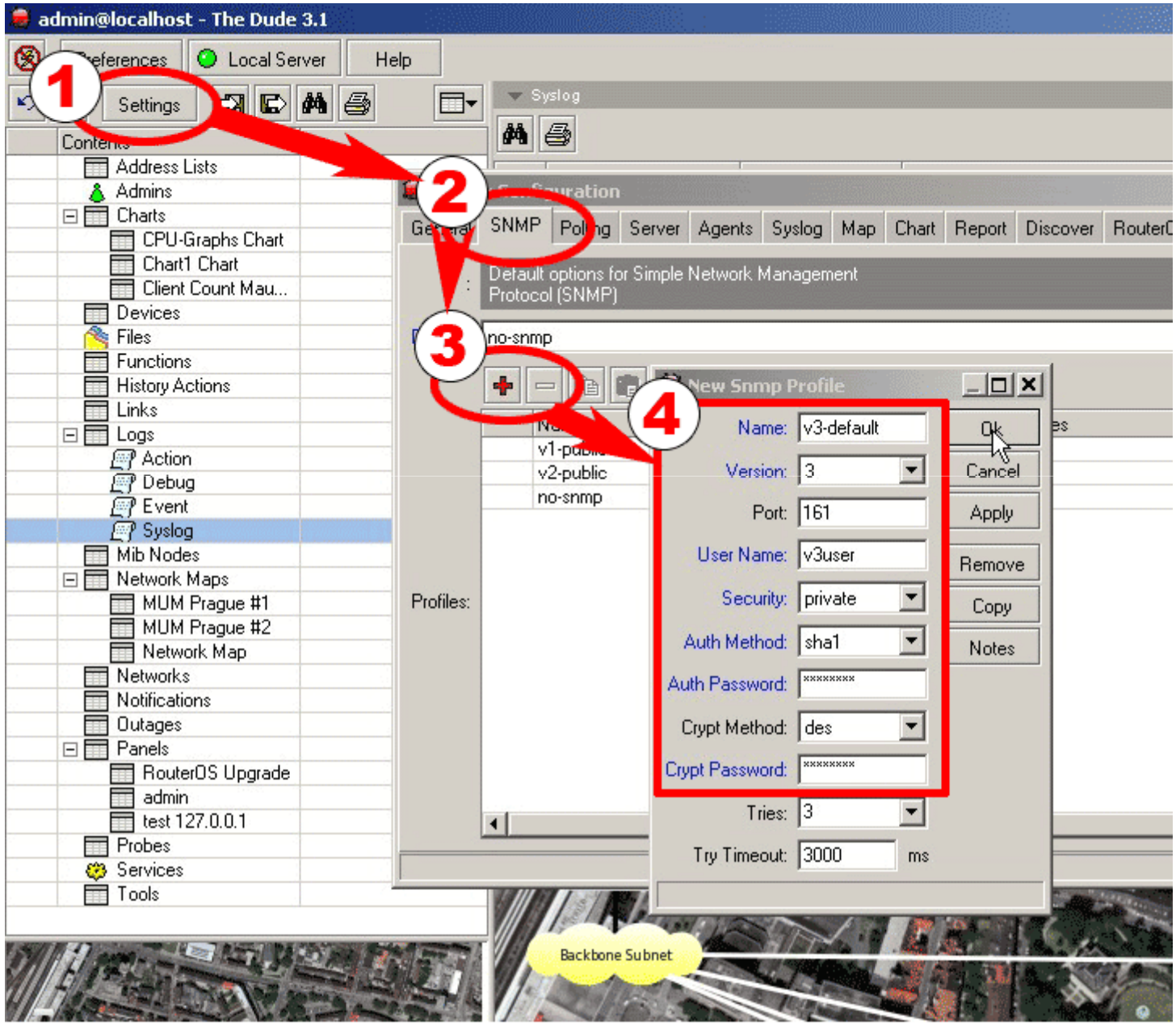
v 3.14

```
[admin@MikroTik] > /snmp community print value-list
                    name: "public"
                 address: 0.0.0.0/0
                security: none
             read-access: yes
            write-access: no
  authentication-password: ""
      encryption-password: ""
  authentication-protocol: MD5
      encryption-protocol: DES
[admin@MikroTik] >
```

SNMPv3 Workshop

- Create SNMPv3 profile on the Dude
- Create SNMPv3 user on RouterOS
- Create SNMPv3 user on Linux net-snmp
- SNMP walk the devices with the v3 profile

Dude SNMPv3 Profile



SNMP – Basic configuration

```
[admin@fmsweb.de] > /snmp set enabled="yes"
contact="info@fmsweb.de" location="Prague“
```

SNMP – User with authentication and encryption

```
[admin@fmsweb.de] > /snmp community add
name=v3user security=private authentication-
protocol=SHA authentication-password=12345678
encryption-protocol=DES encryption-
password=87654321 read-access=yes
```

Overview

1. Create SNMPv3 user with read/write access as template
2. Create SNMPv3 user with read access from template
3. Change passphrases for new user
4. Delete or disable SNMPv3 template user

net-snmp v3 User

	TEMPLATE USER	RO USER
Name:	fmsinit	v3user
Type:	read/write	read only
Auth protocol:	SHA	SHA
Enc protocol:	DES	DES
Auth pass:	b2345678	12345678
Enc pass:	b7654321	87654321

Examples done on Debian Etch:

Config file:	/etc/snmp/snmpd.conf
Persistent data file:	/var/lib/snmp/snmpd.conf

Step 1/4: Create template user:

1.Shut down snmpd:
/etc/init.d/snmpd stop

2.Configure as rw user
add line to /etc/snmp/snmpd.conf**:**
rwuser fmsinit priv

3.Create user
add line to /var/lib/snmpd.conf:
createUser fmsinit SHA b2345678 DES b7654321

Start service and test the user

Step 2/4: Clone user from template user:

1.Configure as rw user

add line to /etc/snmp/snmpd.conf:
rouser v3user priv

2.Clone user on command line

snmpusm -v3 -u fmsinit -n "" -l authPriv -a SHA –A b2345678 -x DES –X b7654321 localhost create v3user fmsinit

Restart service and test the user

Step 3/4: Change passphrases for new user:

1. **Change authentication passphrase:**
   # snmpusm -v 3 -u fmsinit -n "" -l authPriv -a SHA –A b2345678 -x DES –X b7654321 localhost -Ca passwd b2345678 12345678 v3user

2. **Change encryption passphrase:**
   # snmpusm -v 3 -u fmsinit -n "" -l authPriv -a SHA –A b2345678 -x DES –X b7654321 localhost -Cx passwd b7654321 87654321 v3user

Return value: SNMPv3 Key(s) successfully changed.

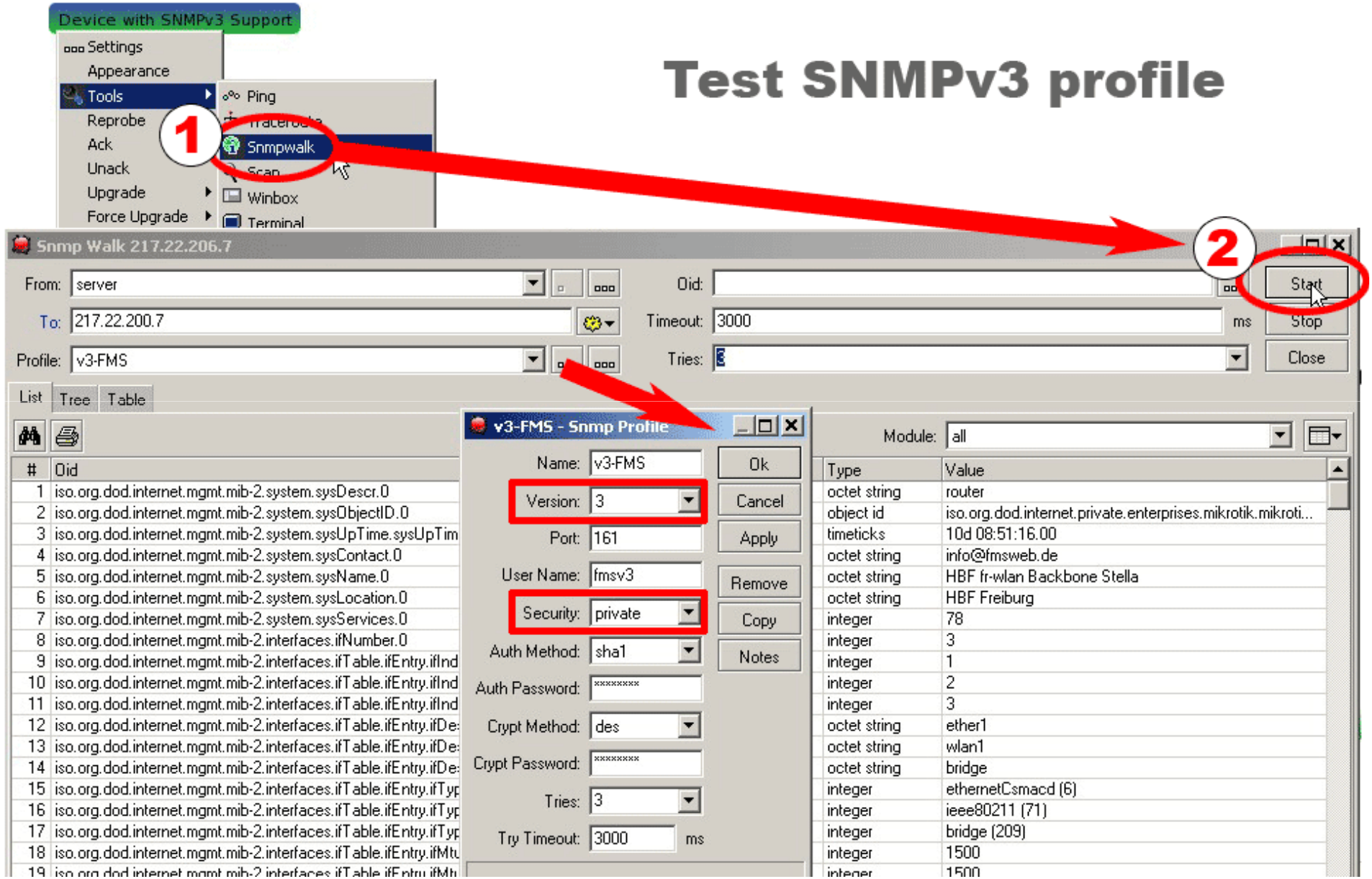
Test the user with new passphrases

Step 4/4: Disable rw template user:

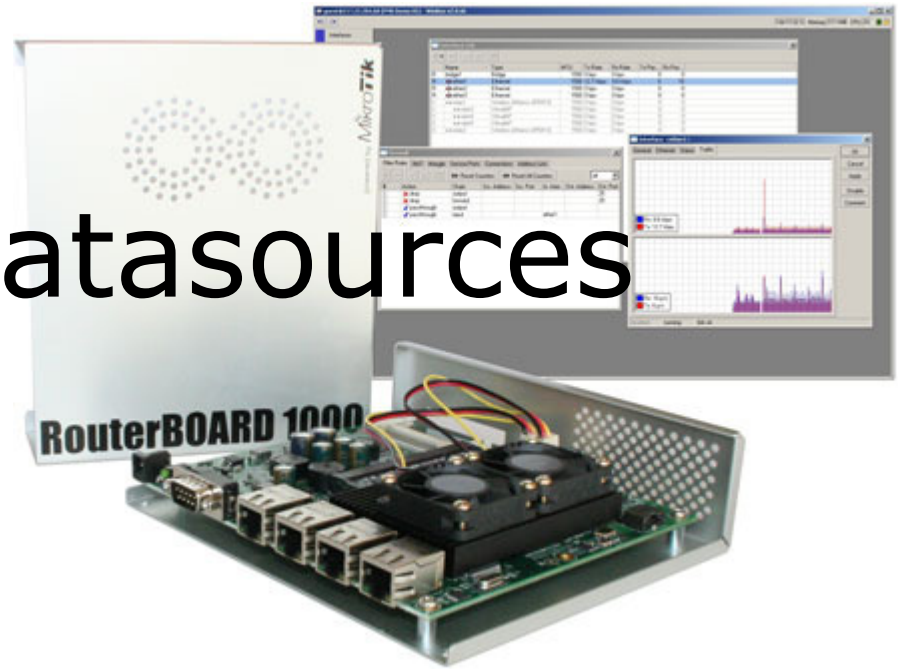
1.Disable rw template user
remove line at /etc/snmp/snmpd.conf:
rwuser fmsinit priv

(or disable with comment “#”)

Test SNMPv3


Device with SNMPv3 Support
Settings
Appearance
Tools
Reprobe
Ack
Unack
Upgrade
Force Upgrade
Ping
Snmpwalk
Winbox
Terminal
1
Test SNMPv3 profile
Snmp Walk 217.22.206.7
From: server
To: 217.22.200.7
Profile: v3-FMS
Oid:
Timeout: 3000
ms
Tries: 3
Start
Stop
Close
2
List
Tree
Table
v3-FMS - Snmp Profile
Name: v3-FMS
Version: 3
Port: 161
User Name: fmsv3
Security: private
Auth Method: sha1
Auth Password: ********
Crypt Method: des
Crypt Password: ********
Tries: 3
Try Timeout: 3000 ms
Ok
Cancel
Apply
Remove
Copy
Notes
Module: all
Oid
1 iso.org.dod.internet.mgmt.mib-2.system.sysDescr.0
2 iso.org.dod.internet.mgmt.mib-2.system.sysObjectID.0
3 iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.sysUpTim
4 iso.org.dod.internet.mgmt.mib-2.system.sysContact.0
5 iso.org.dod.internet.mgmt.mib-2.system.sysName.0
6 iso.org.dod.internet.mgmt.mib-2.system.sysLocation.0
7 iso.org.dod.internet.mgmt.mib-2.system.sysServices.0
8 iso.org.dod.internet.mgmt.mib-2.interfaces.ifNumber.0
9 iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInd
10 iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInd
11 iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInd
12 iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifDe
13 iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifDe
14 iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifDe
15 iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifTyp
16 iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifTyp
17 iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifTyp
18 iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifMtu
Type Value
octet string router
object id iso.org.dod.internet.private.enterprises.mikrotik.mikroti...
timeticks 10d 08:51:16.00
octet string info@fmsweb.de
octet string HBF fr-wlan Backbone Stella
octet string HBF Freiburg
integer 78
integer 3
integer 1
integer 2
integer 3
octet string ether1
octet string wlan1
octet string bridge
integer ethernetCsmacd (6)
integer ieee80211 (71)
integer bridge (209)
integer 1500
integer 1500

Charts and Datasources

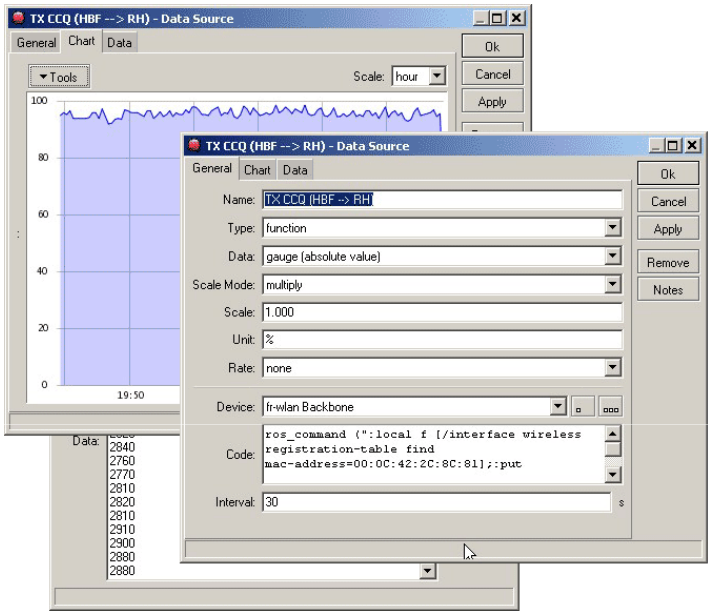


Basics / Charts

- Charts:
  - are named plots
  - one or multiple data sources
  - hold configuration options for the apperance

Basics / Datasources

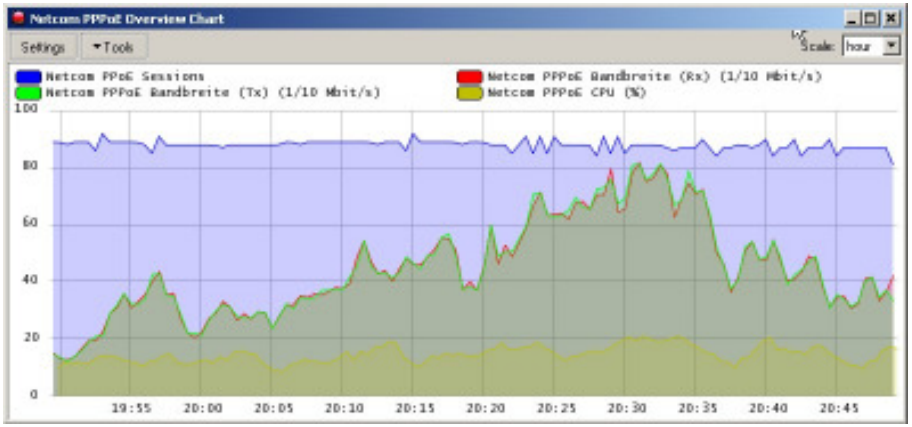
- Data sources:
  - are named sources of data
  - fetch data by snmp or build in functions
  - hold information about interpretation of data
  - default datasources for services and links



Workshop: PPPoE Server Chart

Target:

- Create a single overview chart for a pppoe server



- Include:
  - Total number of active users
  - Bandwidth Rx, Tx
  - CPU usage

Workshop: PPPoE Server Chart

- Create 4 Datasources:
  - active PPPoE Sessions
  - CPU usage
  - Tx Bitrate
  - Rx Bitrate
- Create chart with 4 sources

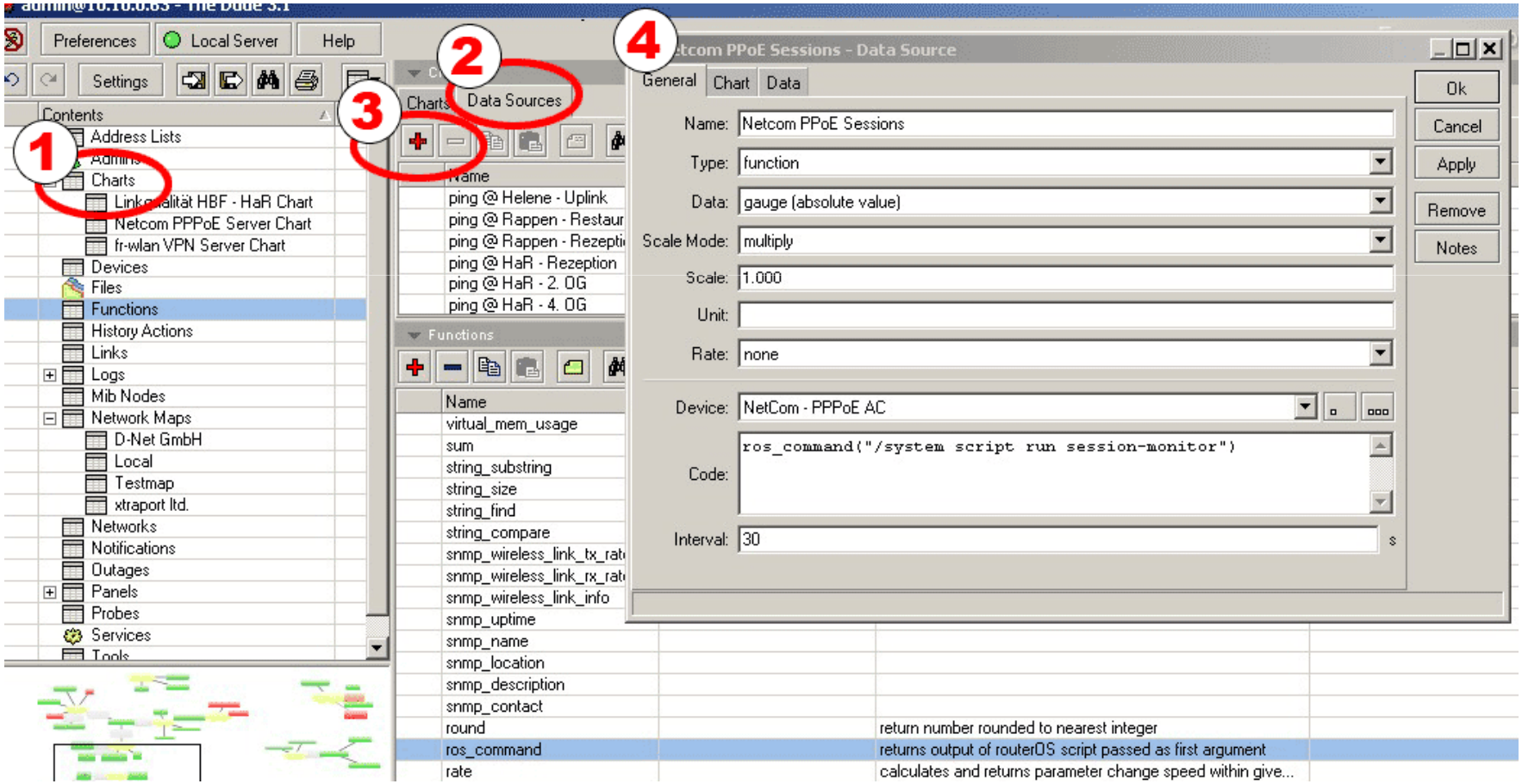
Workshop: PPPoE Server Chart

1. Data Source - active PPPoE connections:

   - not available by SNMP
   - build in functions will be used

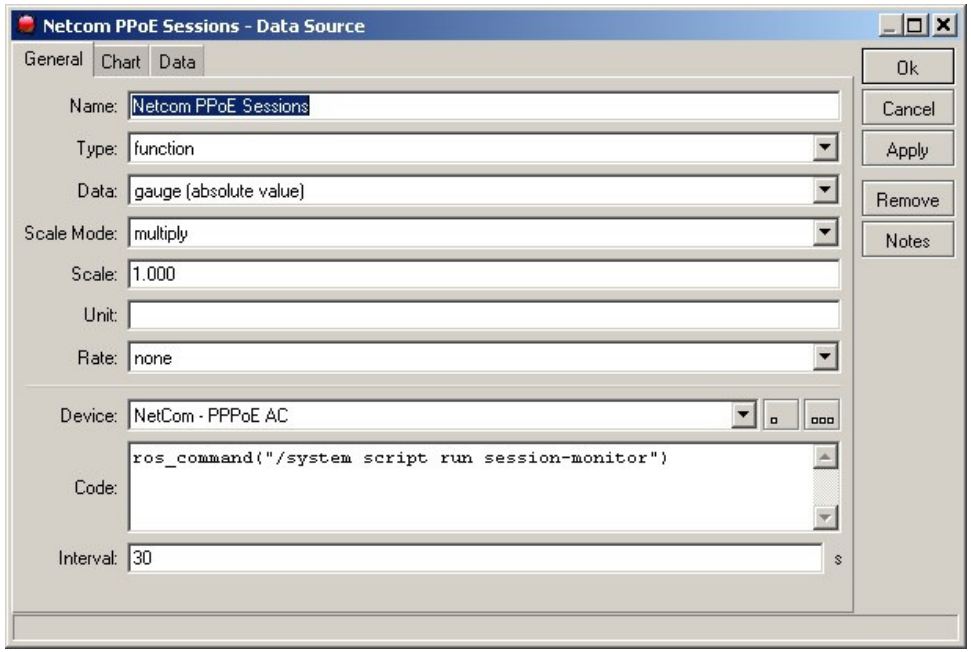
   - function „ros_command()“ executes script on device
   - script returns number of active PPPoE connectsion

New Data Source



New Data Source

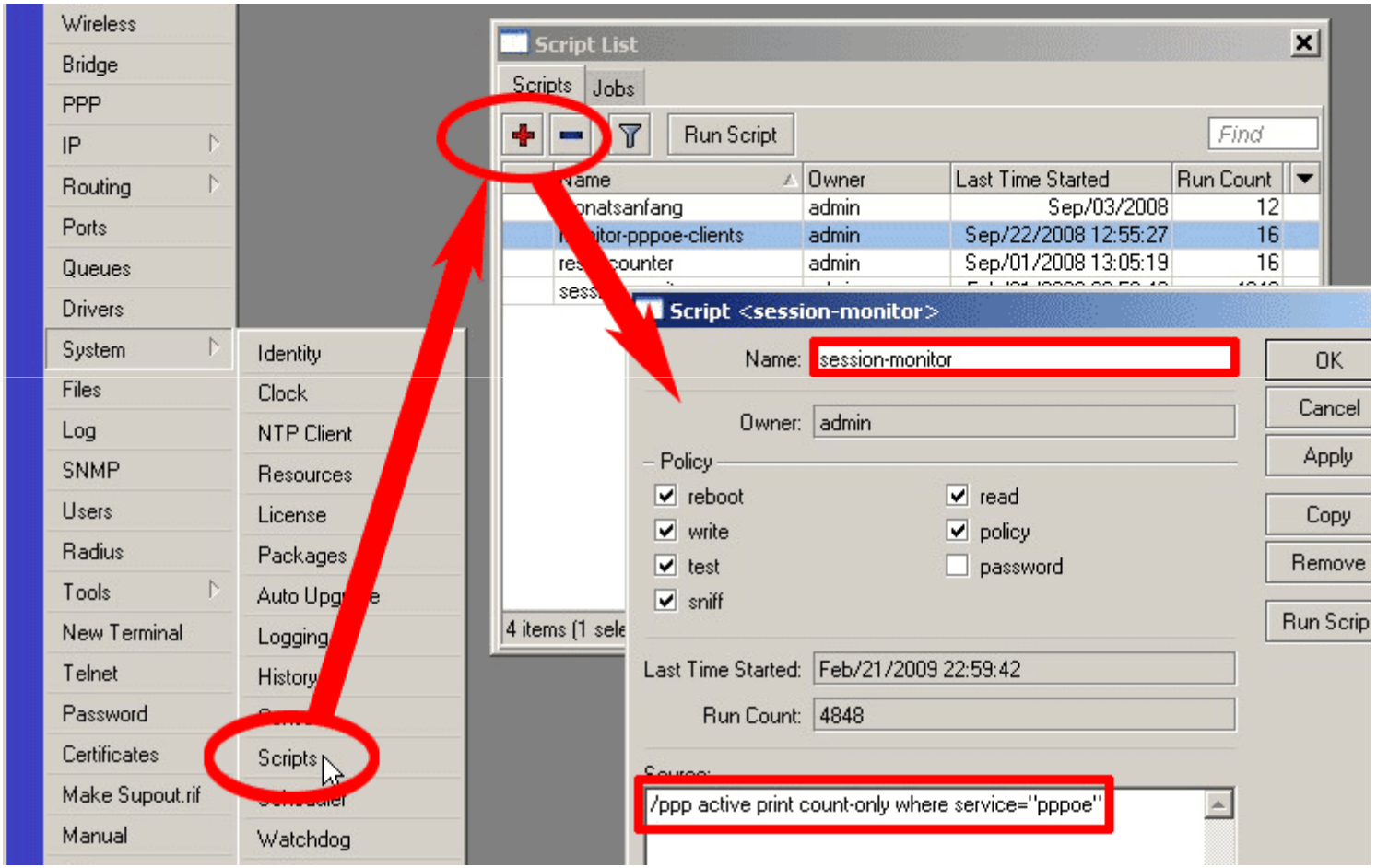
Type: function
Data: absolute
Device: [choose]



Code:

ros_command("/system script run session-monitor")

Create RouterOS Script



Source: /ppp active print count-only where service="pppoe"

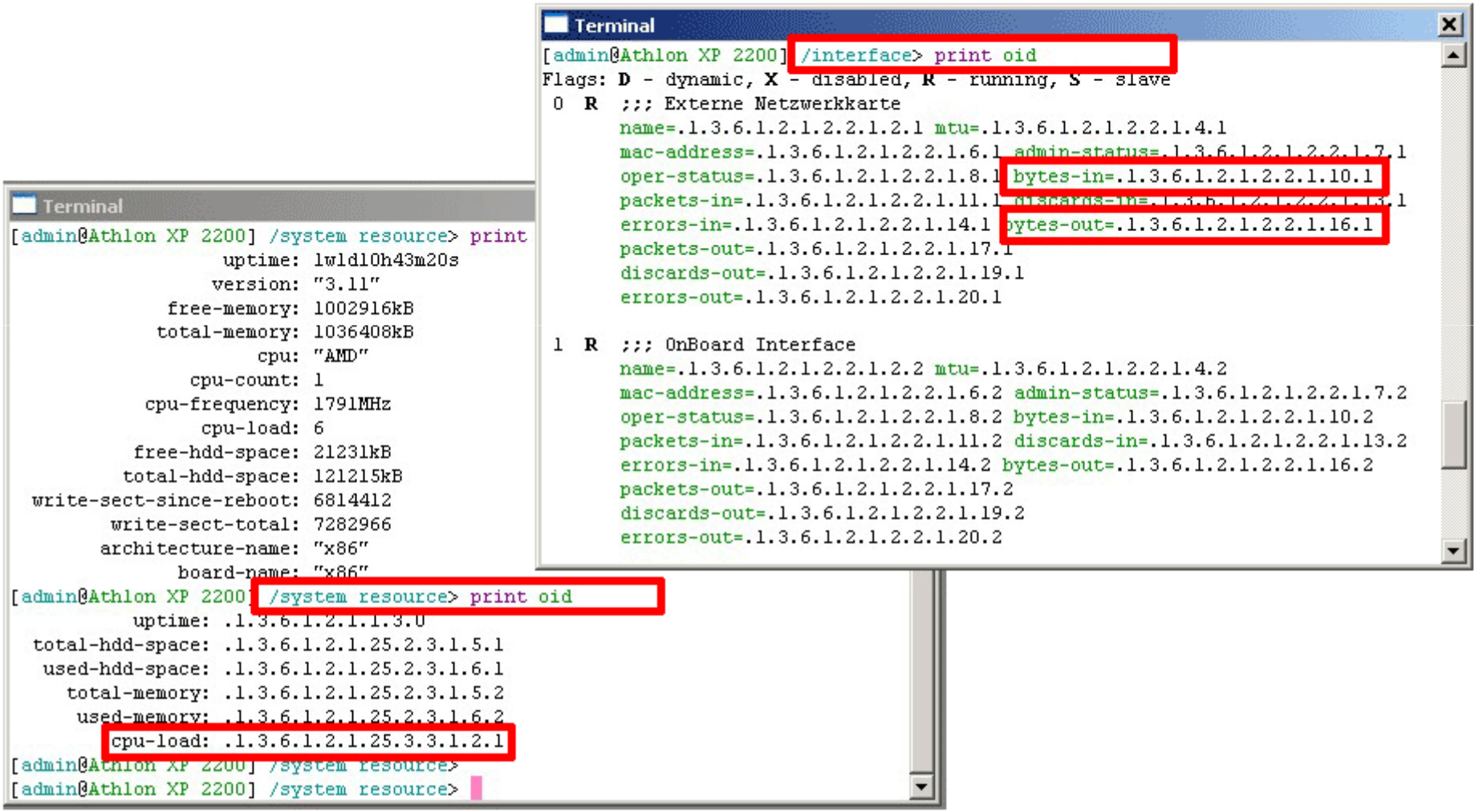
Workshop: PPPoE Server Chart

2. Data Source – CPU Usage

- available by SNMP
- OID can be easily found with:

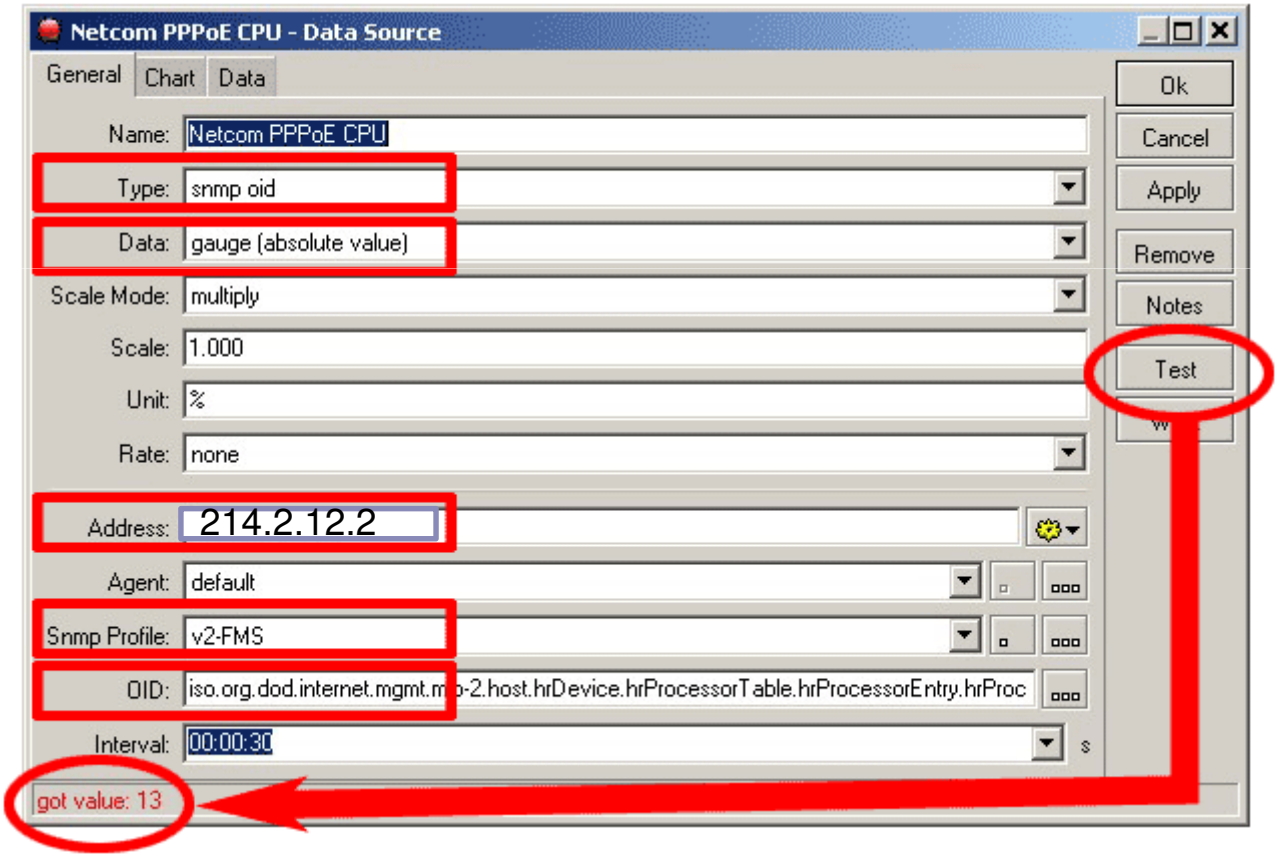
  print oid

Find OIDs with „print oid“



New Data Source (SNMP)

CPU Usage by SNMP



Workshop: PPPoE Server Chart

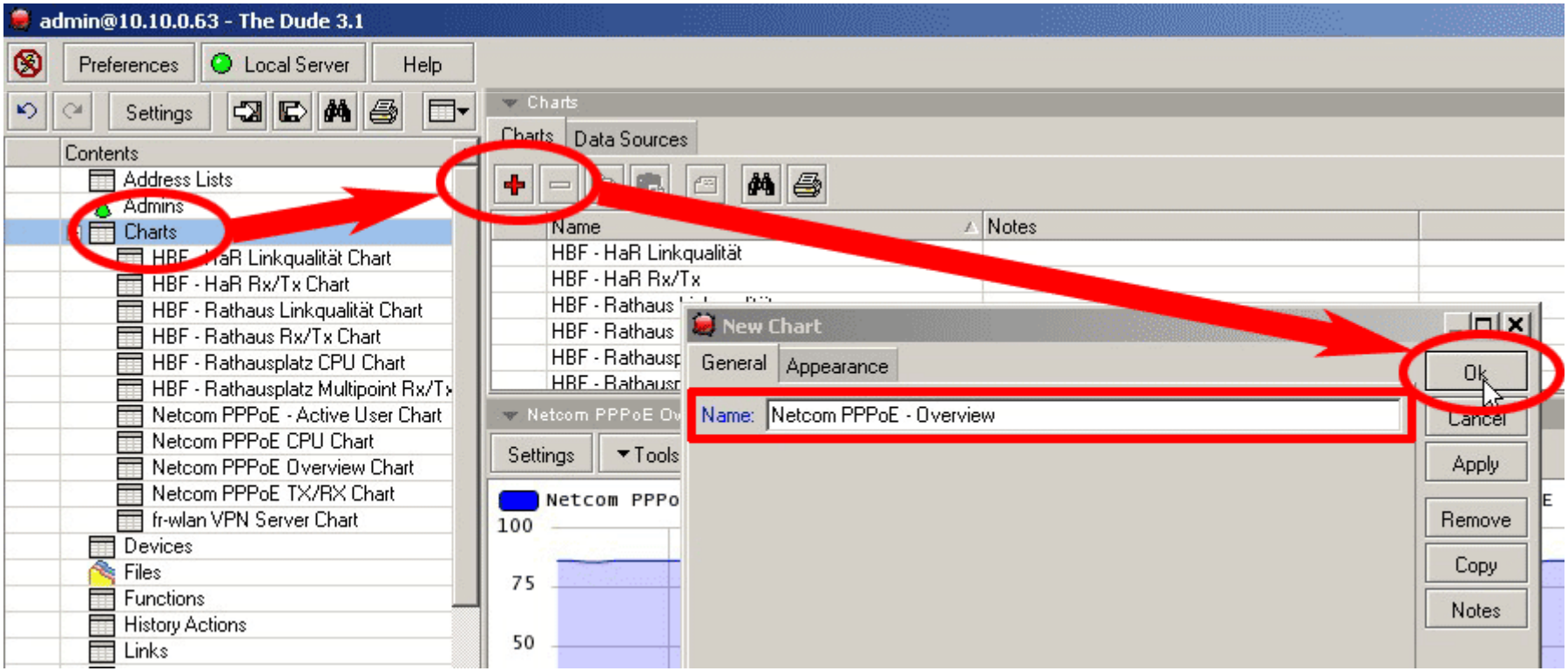
3. and 4. Data Source – Tx Bytes and Rx Bytes
   - available by SNMP

Differences:

   - Delta value, use „Data:Delta“
   - set Rate to „second“
   - scale with „Scalemode:Divide“ and Scale:“12500“ (*8 *10/10^6)

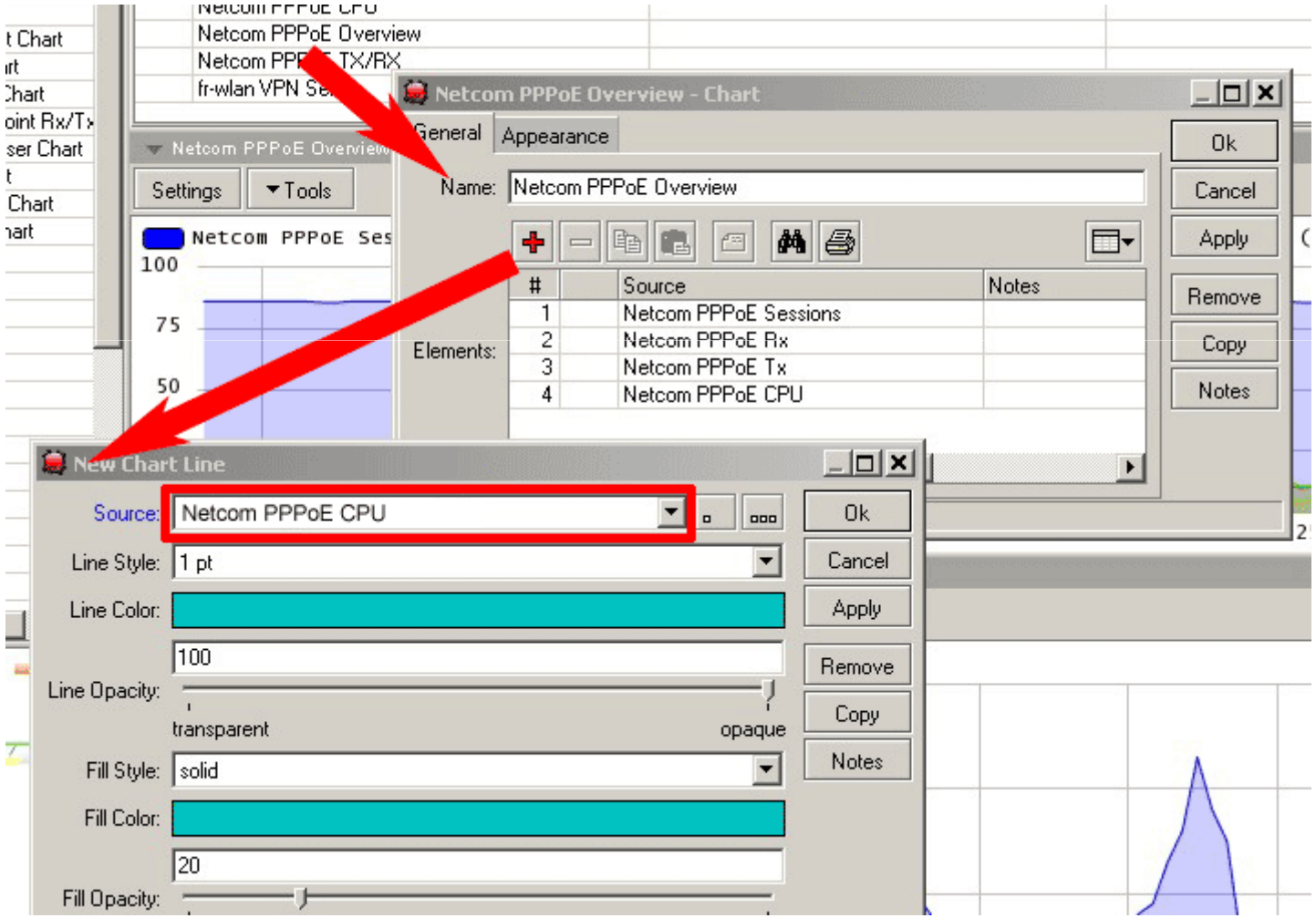
Workshop: PPPoE Server Chart

New Chart



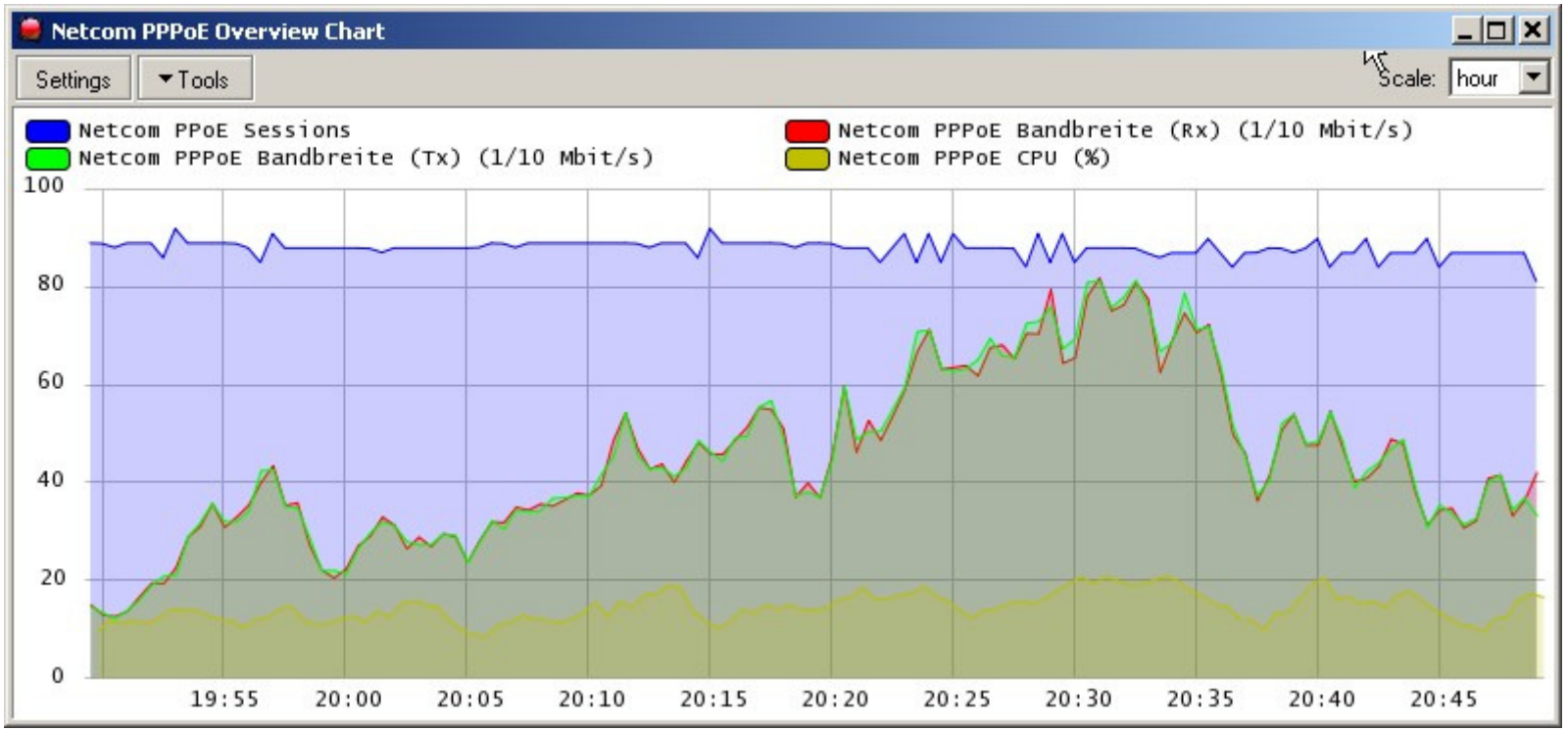
Workshop: PPPoE Server Chart

Add data stores to chart



Workshop: PPPoE Server Chart

Result:



Remark: On this server Rx = Tx

Charts and Datasources – further hints

Charts for CCQ values and links details

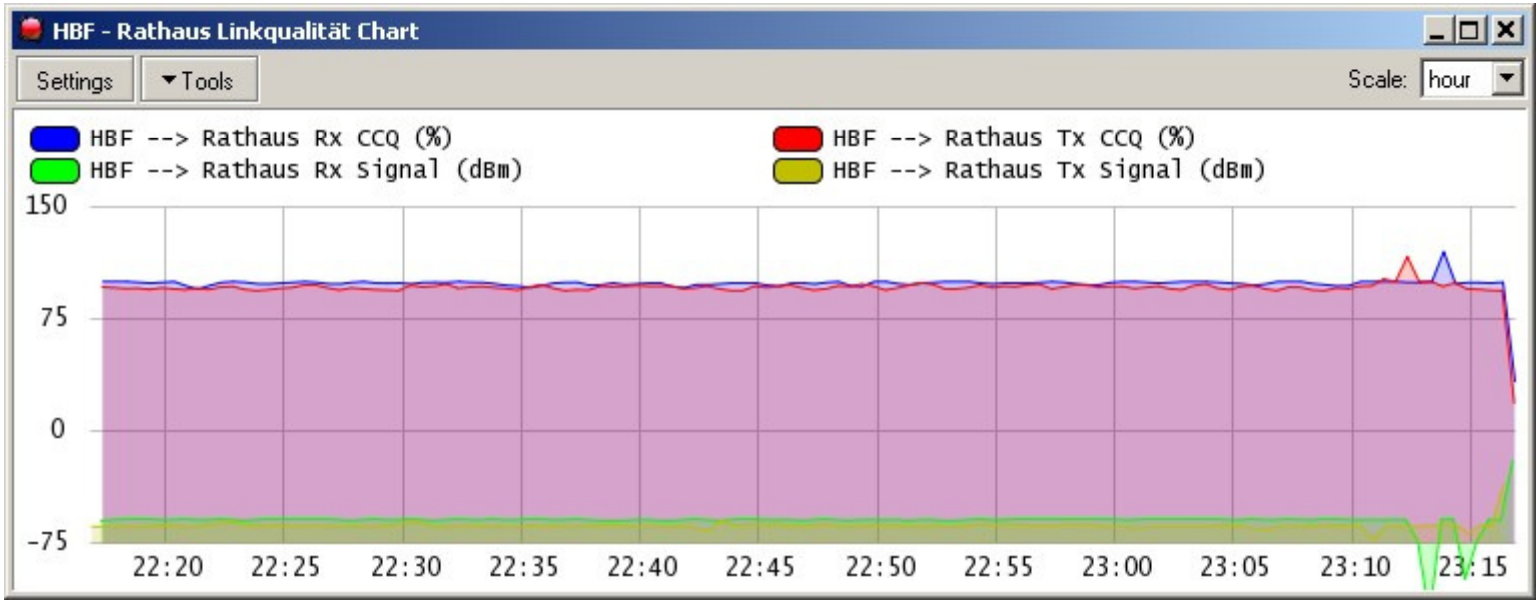
ros_command (":local f [/interface wireless registration-table find mac-address =00:0C:42:3A:26:26];:put [/interface wireless registration-table get $f rx-ccq];")

See all possible values: print stats where mac-address="00:0C:42:3A:26:26“

tx-signal-strength, signal-strength, signal-to-noise

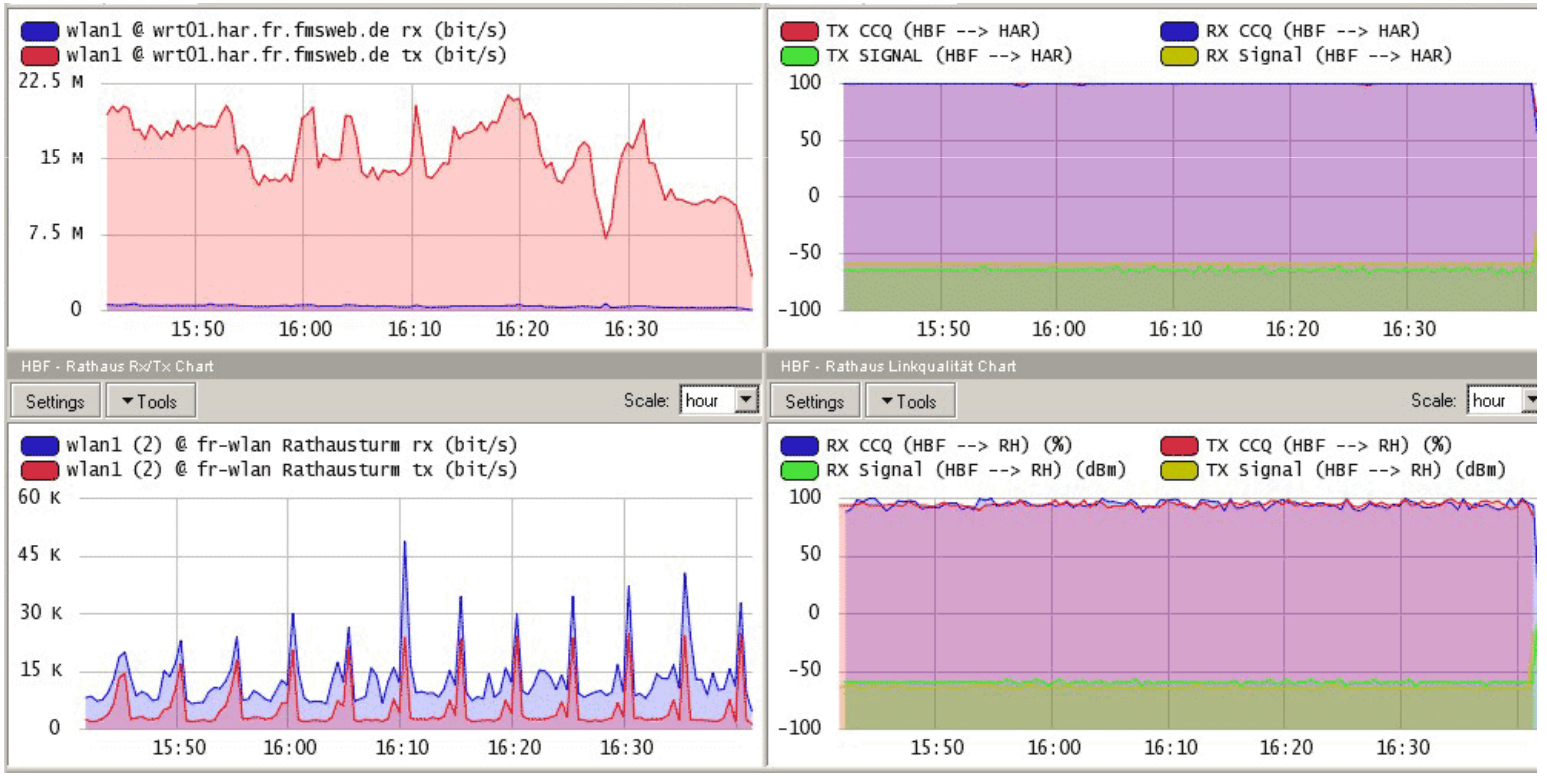
Charts and Datasources – further hints

WLAN Example 1

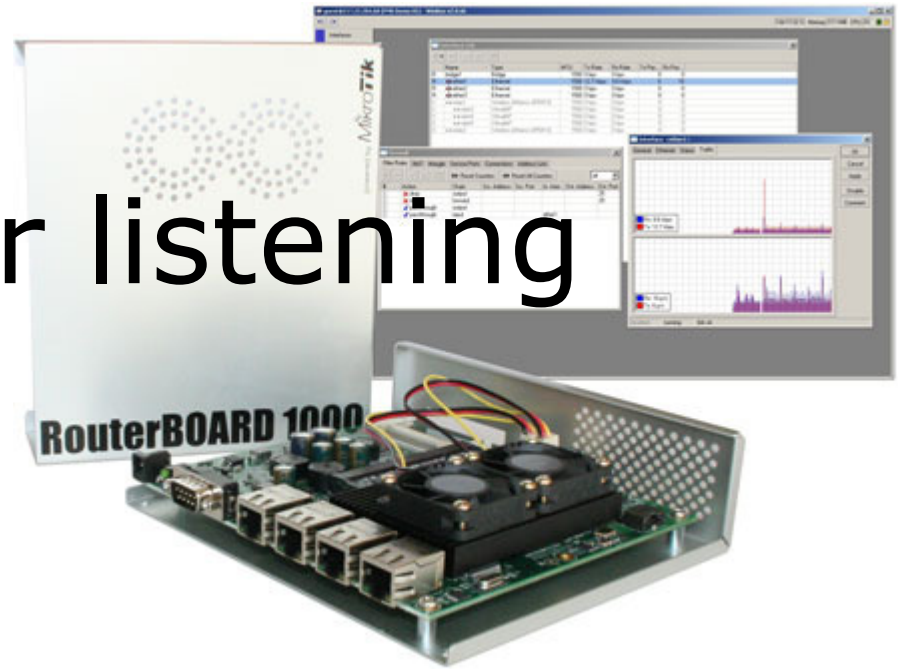


Charts and Datasources – further hints

WLAN Example 2



Thank you for listening



FMS Internetservice, www.fmsweb.de
info@fmsweb.de, Phone: +49 761 2926500

copyright FMS 2009