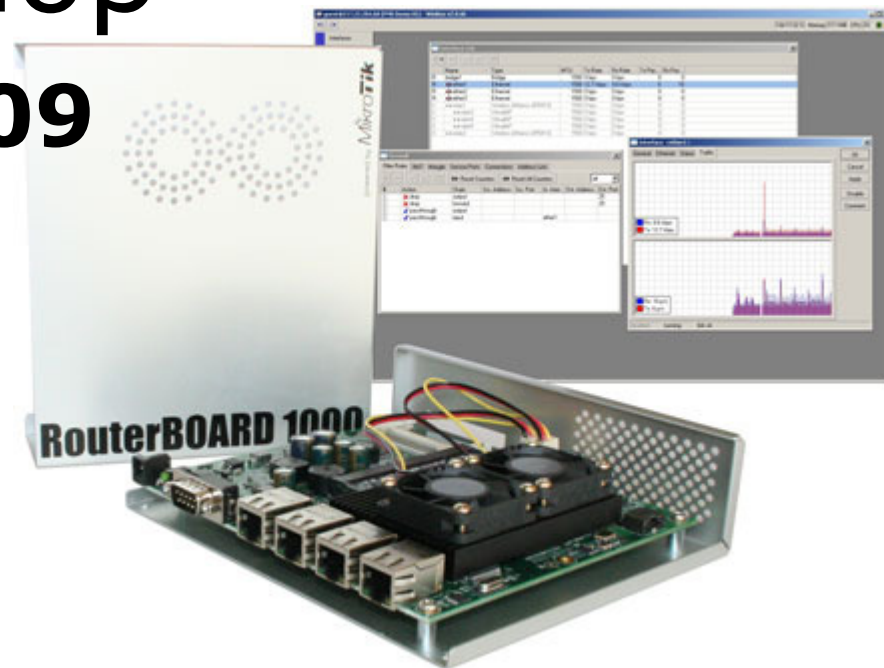


Dude Workshop

MUM Prague 2009

by Patrik Schaub





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 small datacenter

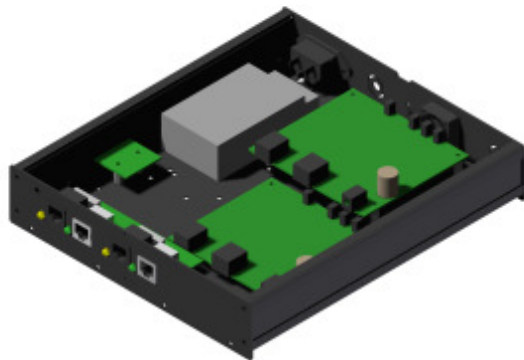
New: mikroCase enclosures

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

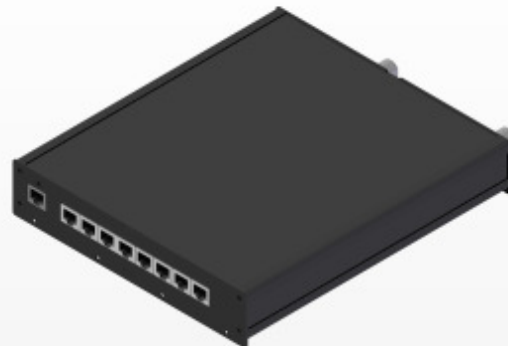


New: mikroCase enclosures

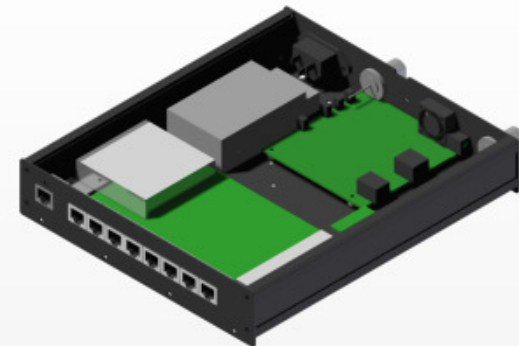
- Distributor and reseller inquiries welcome
- Custom designs possible



DSL Modem



RB493 + DSL Modem

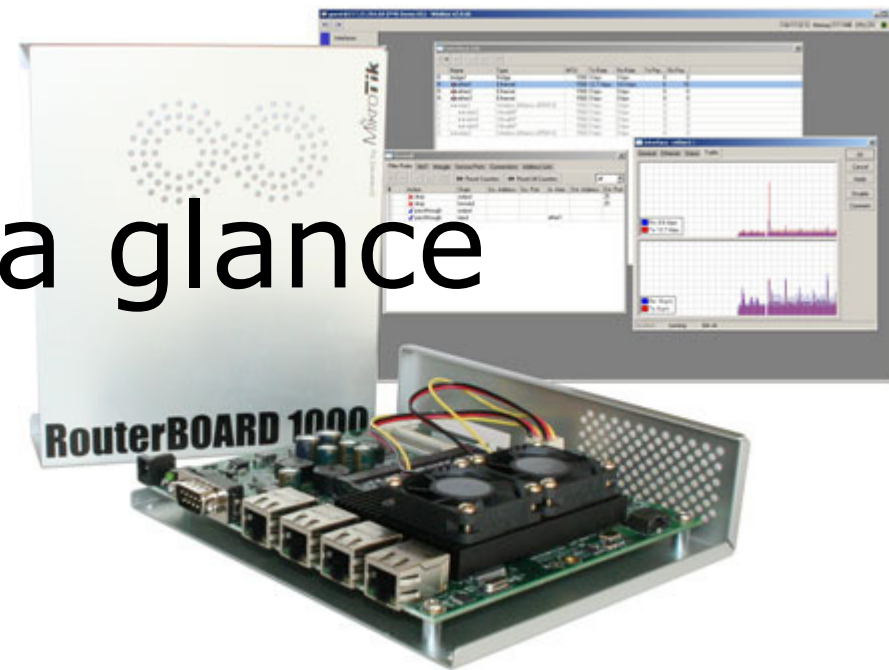


mikroCase distributors

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

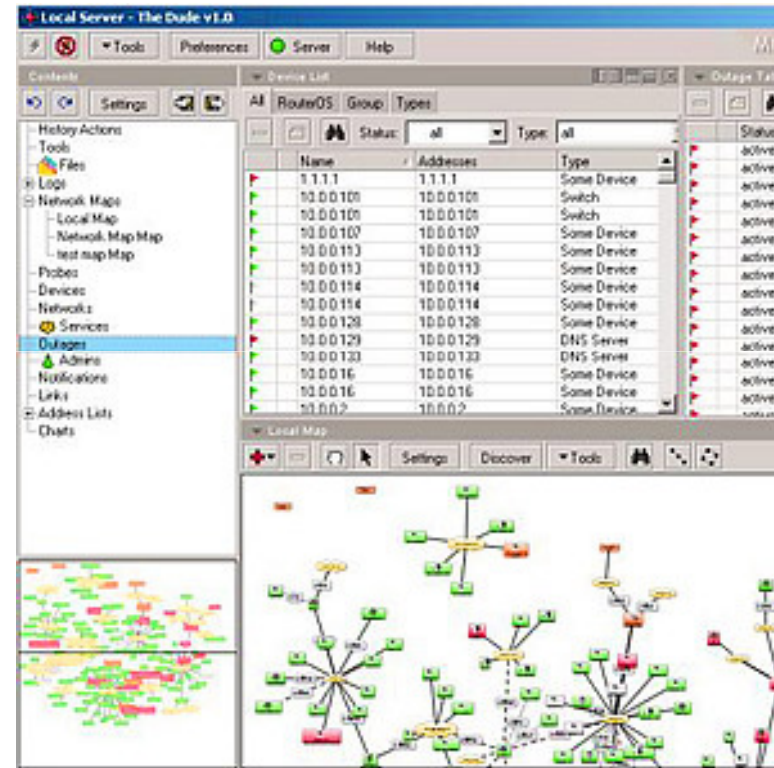


The Dude at a glance



A powerful network monitoring system

- Graphical representation
- Monitoring
- Notifications
- Statistics
- Central administration





The Dude's architecture

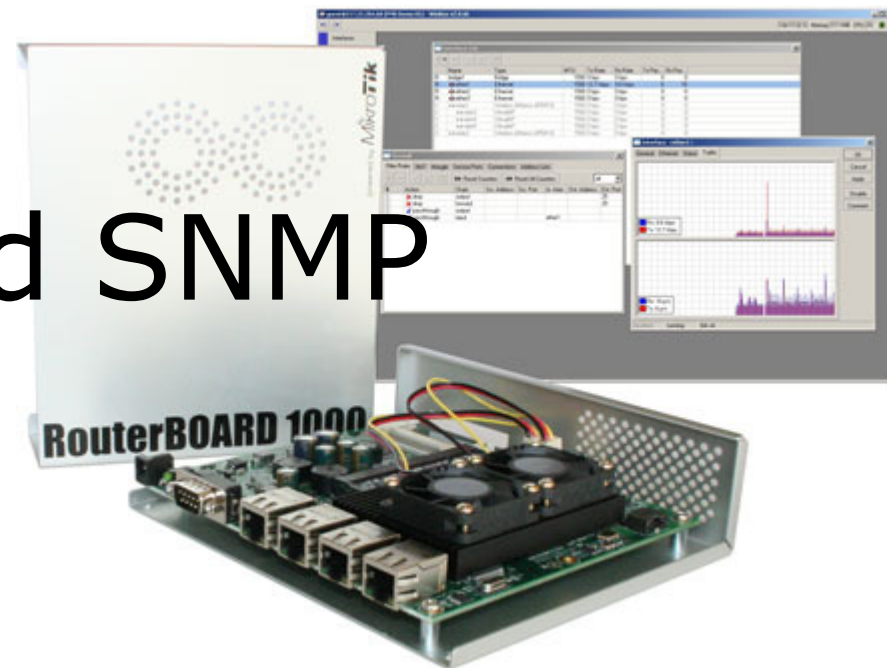
- Client / Server modle
- Multilple clients can connect to one server
- Server on Windows, Linux, MAC and RouterOS
- Client on Windows, Linux, MAC and Webclient



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 address
- 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

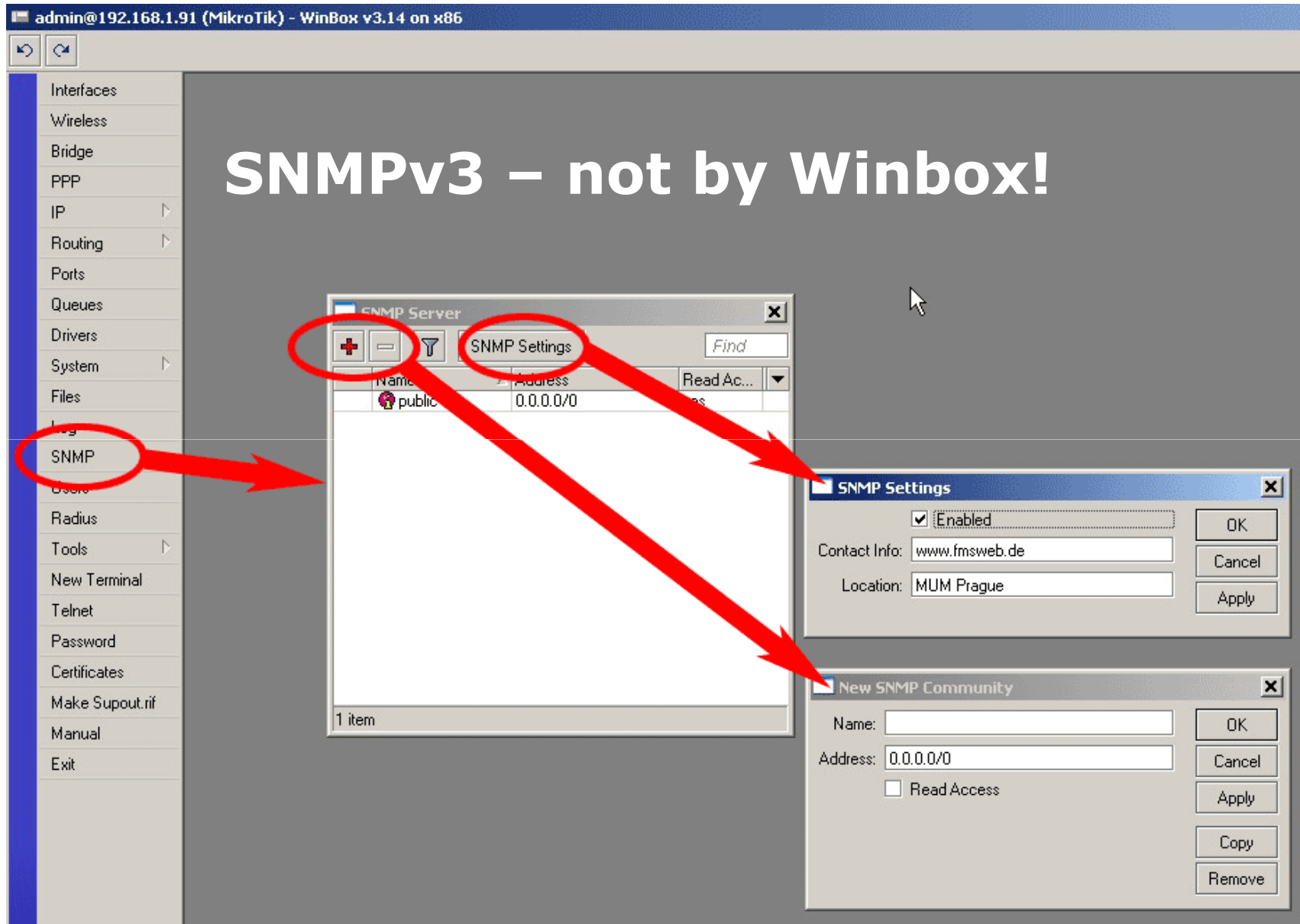
**TIP: NEVER USE STANDARD COMMUNITY
„PUBLIC“ or „PRIVATE“**

Who supports SNNMP v3?

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

- And what about RouterOS... ?

SNMPv3 – not by Winbox!



The screenshot shows the Mikrotik WinBox interface. The left sidebar contains a menu with the following items: Interfaces, Wireless, Bridge, PPP, IP, Routing, Ports, Queues, Drivers, System, Files, Log, **SNMP**, Users, Radius, Tools, New Terminal, Telnet, Password, Certificates, Make Supout.rif, Manual, and Exit. The 'SNMP' menu item is circled in red. A red arrow points from this menu item to the 'SNMP Settings' dialog box. The 'SNMP Settings' dialog box has a 'SNMP Settings' tab selected, and a red circle highlights this tab. A red arrow points from this tab to the 'New SNMP Community' dialog box. Another red arrow points from the 'SNMP Settings' dialog box to the 'SNMP Server' table. The 'SNMP Server' table has a red circle around the '+' icon in the top-left corner. The table contains one item:

Name	Address	Read Access
public	0.0.0.0/0	Yes

The 'SNMP Settings' dialog box contains the following fields:

- Enabled
- Contact Info:
- Location:

The 'New SNMP Community' dialog box contains the following fields:

- Name:
- Address:
- Read Access

SNMP Settings

v 2.9.51

Terminal

```
MMM      MMM      KKK      TTTT
MMMM     MMMM     KKK      TTTT
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 vt102 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] >
```

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 vt102 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] >
  
```

SNMP Community Settings

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] >
  
```

v 3.14

```

Terminal
[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

The screenshot shows the 'The Dude 3.1' interface. On the left is a tree view with categories like Address Lists, Admins, Charts, Devices, Files, Functions, History Actions, Links, Logs, Mib Nodes, Network Maps, Networks, Notifications, Outages, Panels, Probes, Services, and Tools. The 'Syslog' category is selected. The main window shows the 'Configuration' tab for 'SNMP'. A 'New Snmp Profile' dialog box is open, with the following fields:

- Name: v3-default
- Version: 3
- Port: 161
- User Name: v3user
- Security: private
- Auth Method: sha1
- Auth Password: [masked]
- Crypt Method: des
- Crypt Password: [masked]
- Tries: 3
- Try Timeout: 3000 ms

Red annotations indicate the steps: 1. Clicking 'Settings' in the top menu; 2. Clicking 'SNMP' in the configuration tabs; 3. Clicking the '+' icon to add a new profile; 4. Filling out the 'New Snmp Profile' dialog box.

Backbone Subnet



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



	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 profile

1 Snmpwalk

2 Start

From: server To: 217.22.200.7 Profile: v3-FMS

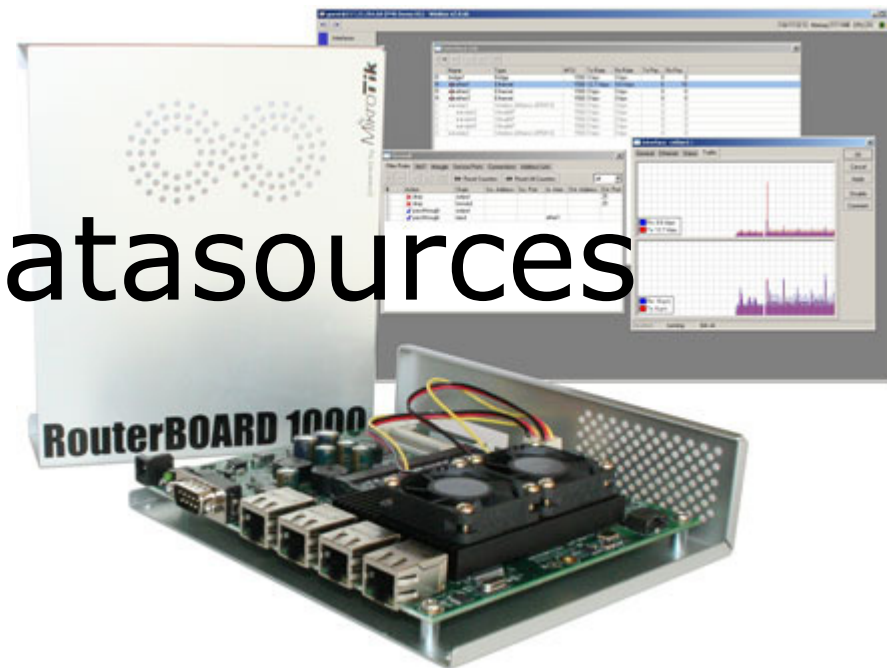
Timeout: 3000 ms Tries: 3

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

Type	Value
object id	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



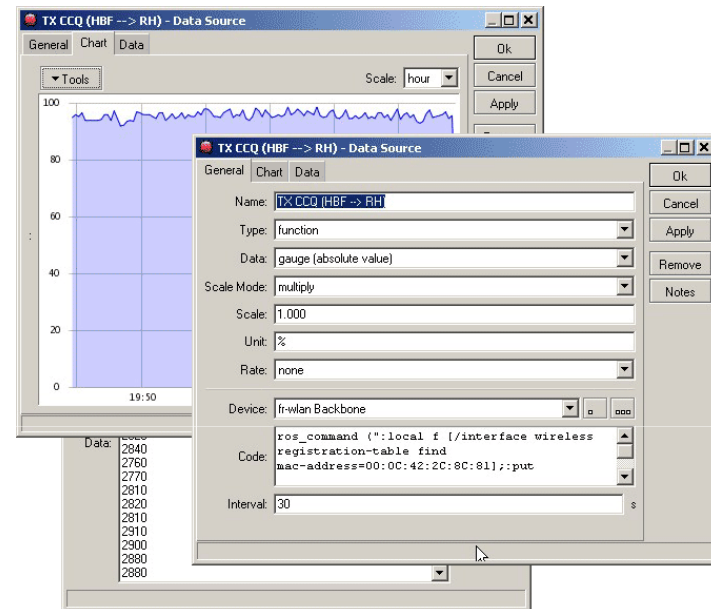
Basics / Charts

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



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

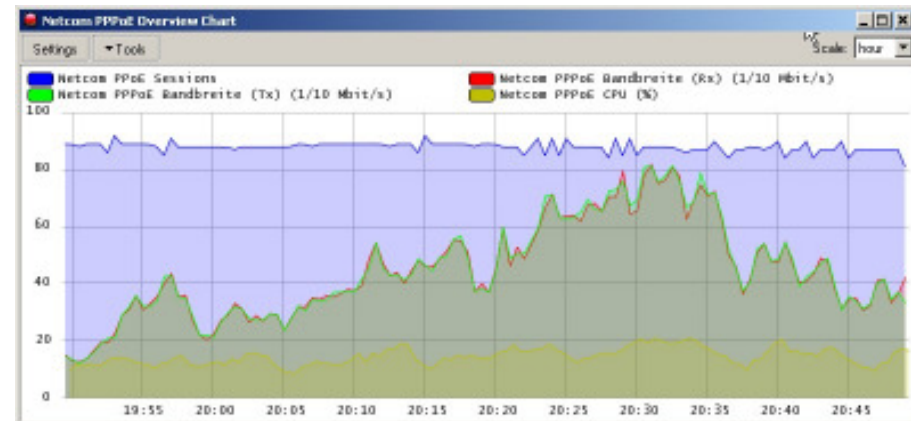


Workshop: PPPoE Server Chart

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 connections

New Data Source

The screenshot shows the FMS interface with the 'New Data Source' dialog box open. The dialog is titled 'Netcom PPoE Sessions - Data Source' and has four numbered callouts: 1 points to the 'Functions' folder in the left sidebar; 2 points to the '+' icon in the 'Data Sources' list; 3 points to the '+' icon in the 'Functions' list; 4 points to the 'General' tab of the dialog. The dialog fields include Name, Type, Data, Scale Mode, Scale, Unit, Rate, Device, Code, and Interval. The 'Code' field contains 'ros_command(\"/system script run session-monitor\")'.

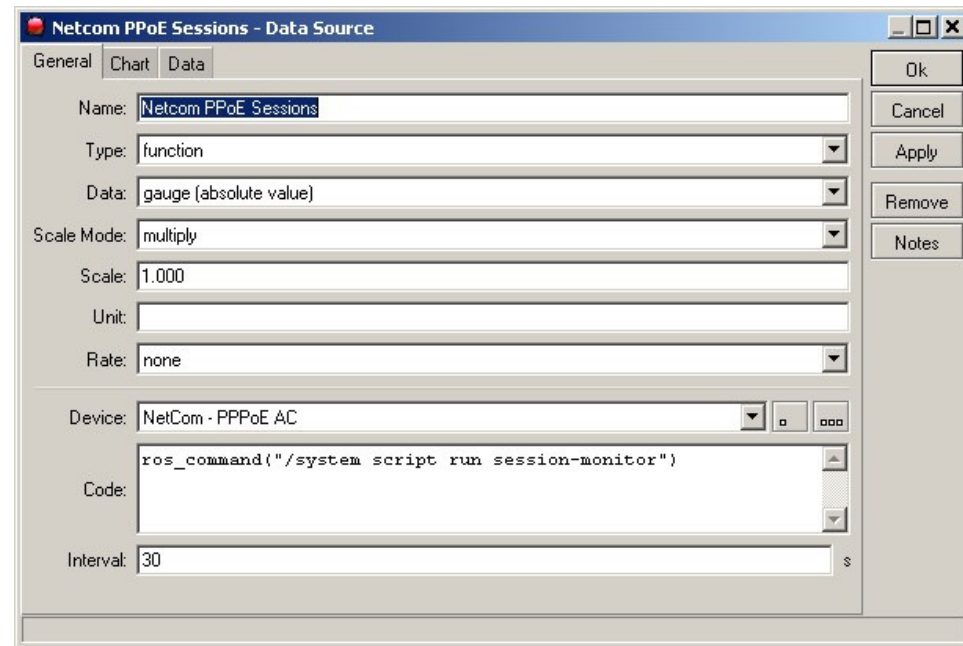
Name	Description
virtual_mem_usage	
sum	
string_substring	
string_size	
string_find	
string_compare	
snmp_wireless_link_tx_rate	
snmp_wireless_link_rx_rate	
snmp_wireless_link_info	
snmp_uptime	
snmp_name	
snmp_location	
snmp_description	
snmp_contact	
round	return number rounded to nearest integer
ros_command	returns output of routerOS script passed as first argument
rate	calculates and returns parameter change speed within give...

New Data Source

Type: function
Data: absolute
Device: [choose]

Code:

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



Netcom PPoE Sessions - Data Source

General Chart Data

Name: Netcom PPoE Sessions

Type: function

Data: gauge (absolute value)

Scale Mode: multiply

Scale: 1.000

Unit:

Rate: none

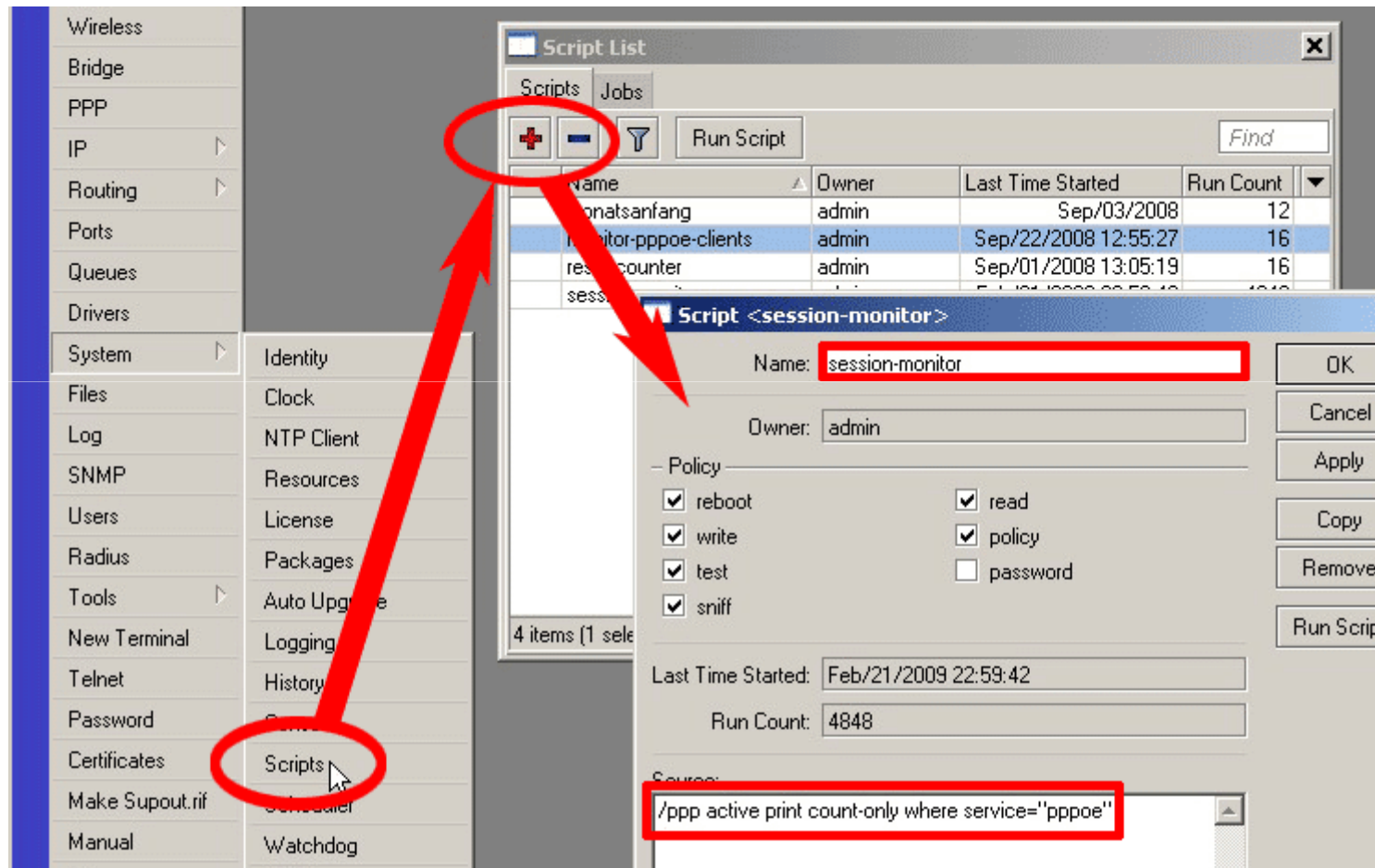
Device: NetCom - PPPoE AC

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

Interval: 30 s

Ok
Cancel
Apply
Remove
Notes

Create RouterOS Script



The screenshot shows the Mikrotik WinBox interface. On the left, the 'Scripts' menu is highlighted. In the center, the 'Script List' window displays a table of scripts:

Name	Owner	Last Time Started	Run Count
monatsanfang	admin	Sep/03/2008	12
monitor-pppoe-clients	admin	Sep/22/2008 12:55:27	16
res_counter	admin	Sep/01/2008 13:05:19	16
session-monitor	admin	Feb/21/2009 22:59:42	4848

The configuration window for the 'session-monitor' script is shown below, with the following details:

- Name: session-monitor
- Owner: admin
- Policy:
 - reboot
 - write
 - test
 - sniff
 - read
 - policy
 - password
- Last Time Started: Feb/21/2009 22:59:42
- Run Count: 4848
- Source: /ppp active print count-only where service="pppoe"

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

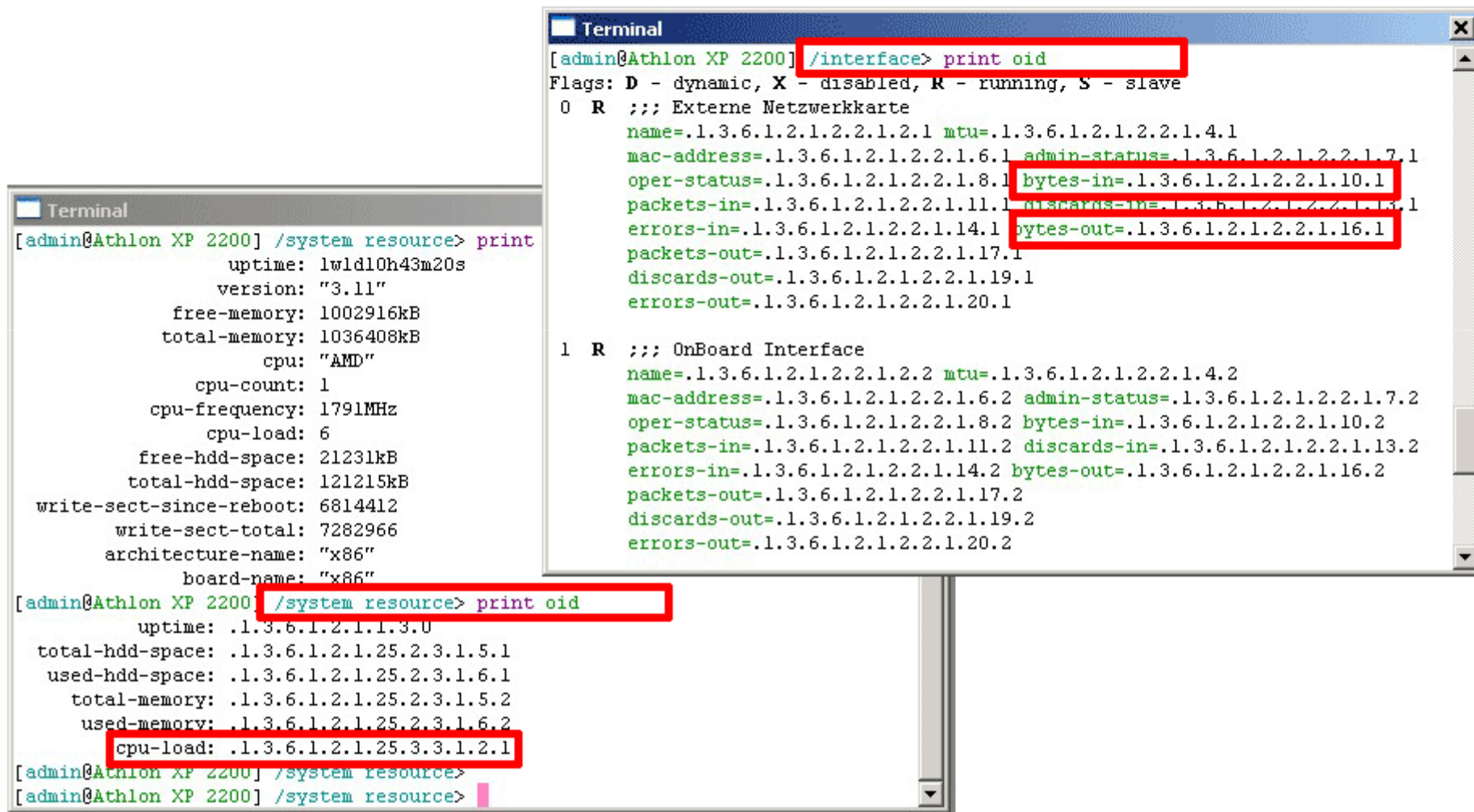
Workshop: PPPoE Server Chart

2. Data Source – CPU Usage

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

print oid

Find OIDs with „print oid“



The image shows two terminal windows. The left window displays system resource information, and the right window displays network interface configuration details. Red boxes highlight specific commands and values in both windows.

```
[admin@Athlon XP 2200] /system resource> print
    uptime: 1w1d10h43m20s
    version: "3.11"
    free-memory: 1002916kB
    total-memory: 1036408kB
    cpu: "AMD"
    cpu-count: 1
    cpu-frequency: 1791MHz
    cpu-load: 6
    free-hdd-space: 21231kB
    total-hdd-space: 121215kB
    write-sect-since-reboot: 6814412
    write-sect-total: 7282966
    architecture-name: "x86"
    board-name: "x86"

[admin@Athlon XP 2200] /system resource> print oid
    uptime: .1.3.6.1.2.1.1.3.0
    total-hdd-space: .1.3.6.1.2.1.25.2.3.1.5.1
    used-hdd-space: .1.3.6.1.2.1.25.2.3.1.6.1
    total-memory: .1.3.6.1.2.1.25.2.3.1.5.2
    used-memory: .1.3.6.1.2.1.25.2.3.1.6.2
    cpu-load: .1.3.6.1.2.1.25.3.3.1.2.1

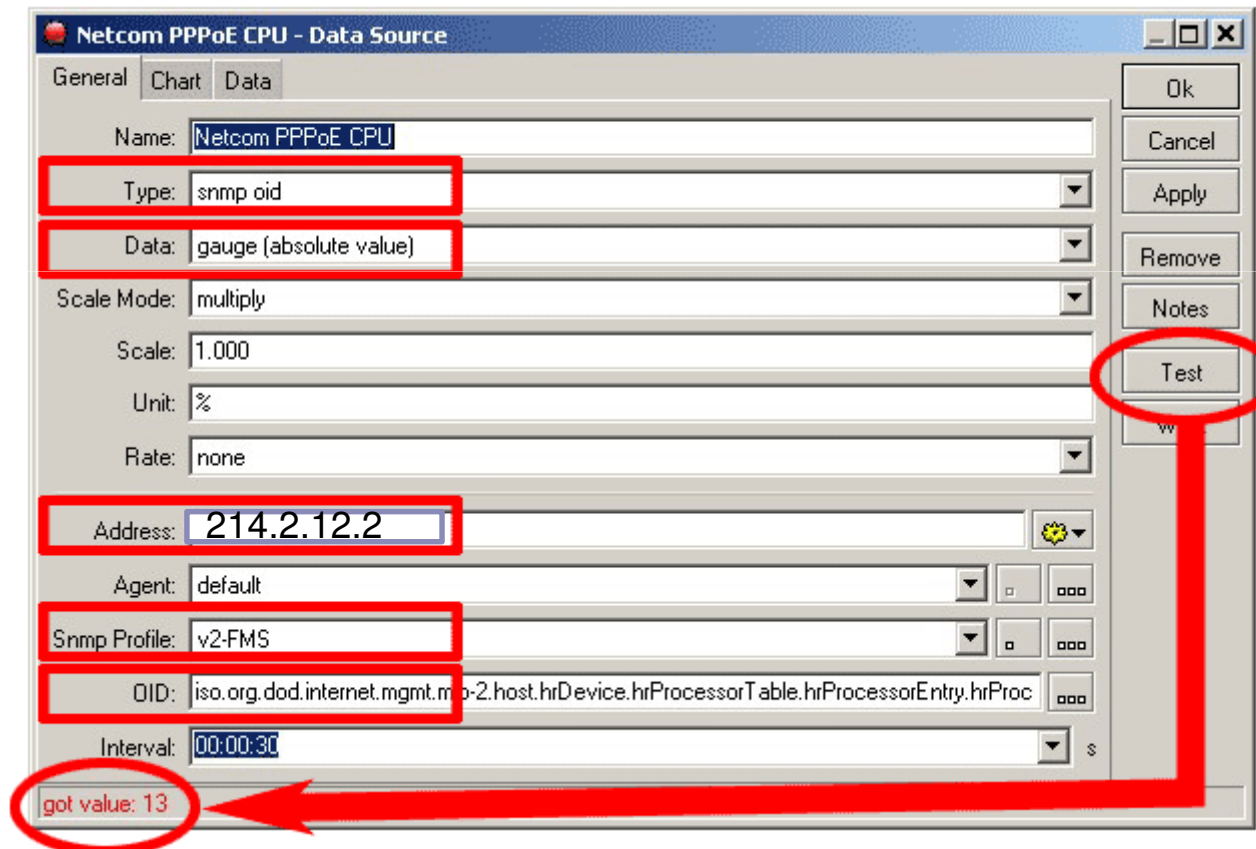
[admin@Athlon XP 2200] /system resource>
[admin@Athlon XP 2200] /system resource>
```

```
Terminal
[admin@Athlon XP 2200] /interface> print oid
Flags: D - dynamic, X - disabled, R - running, S - slave
0 R   ;;; Externe Netzwerkkarte
    name=.1.3.6.1.2.1.2.2.1.2.1 mtu=.1.3.6.1.2.1.2.2.1.4.1
    mac-address=.1.3.6.1.2.1.2.2.1.6.1 admin-status=.1.3.6.1.2.1.2.2.1.7.1
    oper-status=.1.3.6.1.2.1.2.2.1.8.1 bytes-in=.1.3.6.1.2.1.2.2.1.10.1
    packets-in=.1.3.6.1.2.1.2.2.1.11.1 discards-in=.1.3.6.1.2.1.2.2.1.13.1
    errors-in=.1.3.6.1.2.1.2.2.1.14.1 bytes-out=.1.3.6.1.2.1.2.2.1.16.1
    packets-out=.1.3.6.1.2.1.2.2.1.17.1
    discards-out=.1.3.6.1.2.1.2.2.1.19.1
    errors-out=.1.3.6.1.2.1.2.2.1.20.1

1 R   ;;; OnBoard Interface
    name=.1.3.6.1.2.1.2.2.1.2.2 mtu=.1.3.6.1.2.1.2.2.1.4.2
    mac-address=.1.3.6.1.2.1.2.2.1.6.2 admin-status=.1.3.6.1.2.1.2.2.1.7.2
    oper-status=.1.3.6.1.2.1.2.2.1.8.2 bytes-in=.1.3.6.1.2.1.2.2.1.10.2
    packets-in=.1.3.6.1.2.1.2.2.1.11.2 discards-in=.1.3.6.1.2.1.2.2.1.13.2
    errors-in=.1.3.6.1.2.1.2.2.1.14.2 bytes-out=.1.3.6.1.2.1.2.2.1.16.2
    packets-out=.1.3.6.1.2.1.2.2.1.17.2
    discards-out=.1.3.6.1.2.1.2.2.1.19.2
    errors-out=.1.3.6.1.2.1.2.2.1.20.2
```

New Data Source (SNMP)

CPU Usage by SNMP



Netcom PPPoE CPU - Data Source

General Chart Data

Name: Netcom PPPoE CPU

Type: snmp oid

Data: gauge (absolute value)

Scale Mode: multiply

Scale: 1.000

Unit: %

Rate: none

Address: 214.2.12.2

Agent: default

Snmp Profile: v2-FMS

OID: iso.org.dod.internet.mgmt.mib-2.host.hrDevice.hrProcessorTable.hrProcessorEntry.hrProc

Interval: 00:00:30 s

got value: 13

Ok
Cancel
Apply
Remove
Notes
Test

Workshop: PPPoE Server Chart

3. and 4. Data Source – Tx Bytes and Rx Bytes

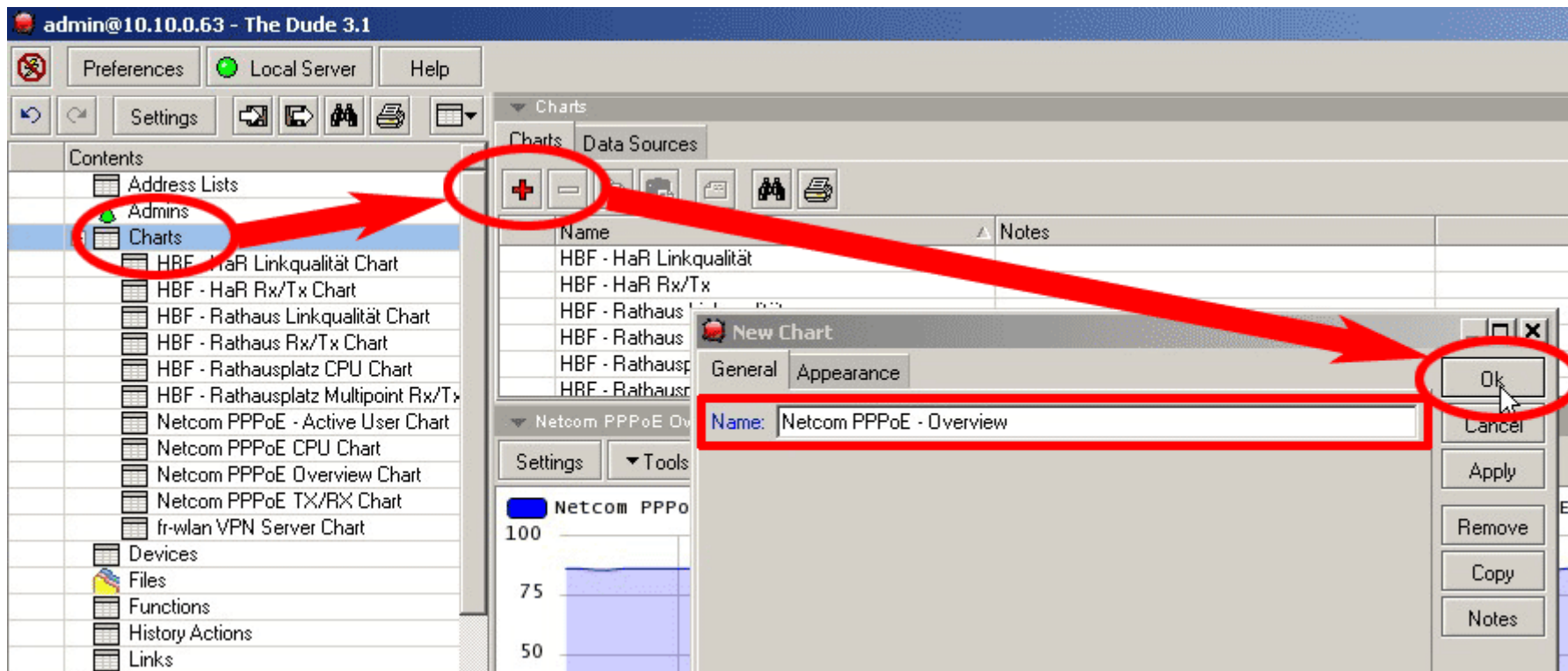
- available by SNMP

Differences:

- Delta value, use „Data:Delta“
- set Rate to „second“
- scale with „Scalemode:Divide“ and Scale:“12500“ (*8 *10/10⁶)

Workshop: PPPoE Server Chart

New Chart



The screenshot shows the 'admin@10.10.0.63 - The Dude 3.1' interface. The 'Contents' pane on the left has the 'Charts' folder selected. The 'Charts' toolbar has a '+' button circled in red. A red arrow points from this '+' button to the 'New Chart' dialog box. The dialog box has the 'Name' field set to 'Netcom PPPoE - Overview' and the 'Ok' button circled in red. A red arrow also points from the 'Charts' folder in the Contents pane to the 'New Chart' dialog box.

Name	Notes
HBF - HaR Linkqualität Chart	
HBF - HaR Rx/Tx	
HBF - Rathaus	
HBF - Rathaus	
HBF - Rathaus	
HBF - Rathaus	
HBF - Rathaus	
HBF - Rathaus	
Netcom PPPoE - Active User Chart	
Netcom PPPoE CPU Chart	
Netcom PPPoE Overview Chart	
Netcom PPPoE TX/RX Chart	
fr-wlan VPN Server Chart	

Netcom PPPoE Overview Chart

100
75
50

Workshop: PPPoE Server Chart

Add
data
stores
to
chart

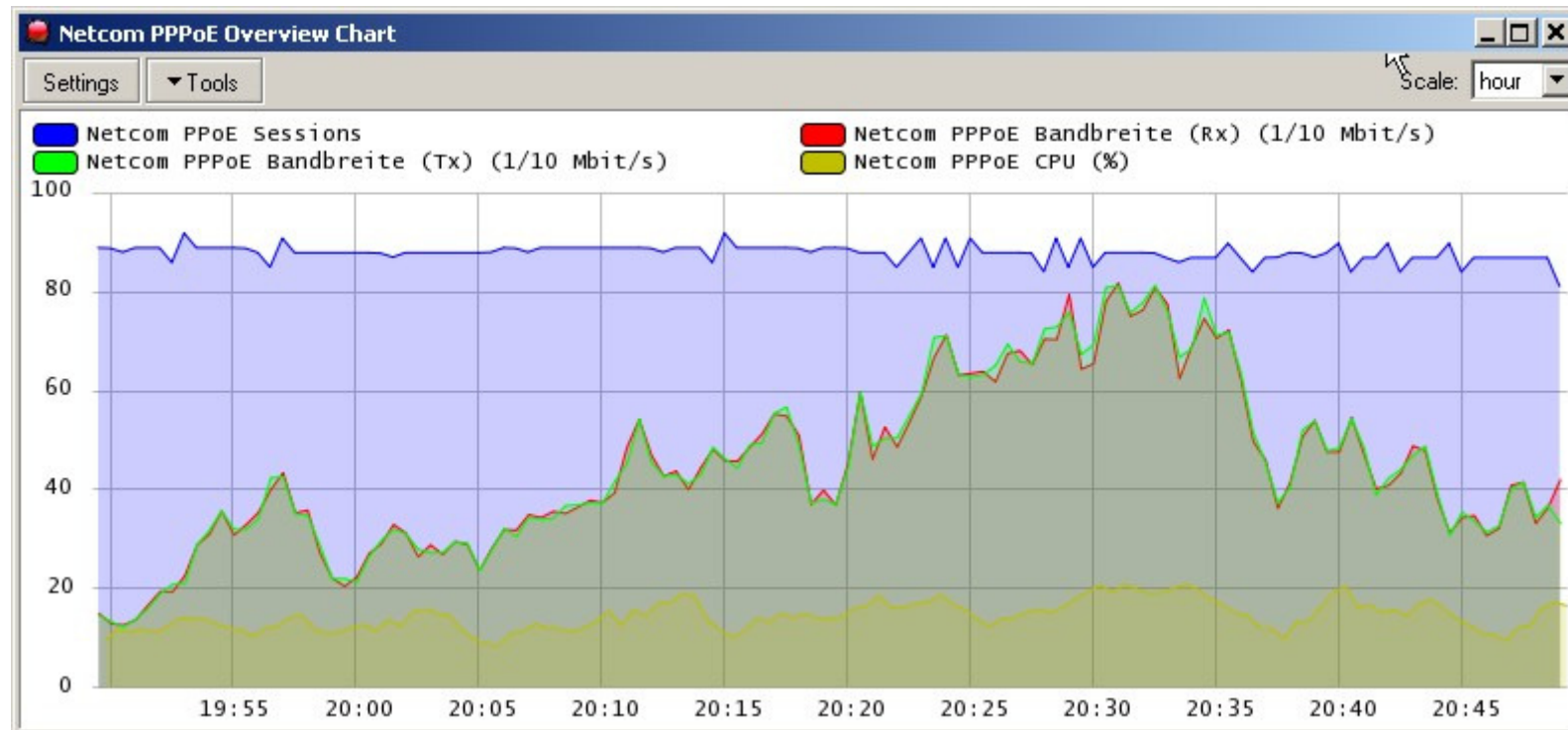
The screenshot shows the 'Netcom PPPoE Overview - Chart' configuration dialog. The 'Elements' table lists the data sources available for the chart:

#	Source	Notes
1	Netcom PPPoE Sessions	
2	Netcom PPPoE Rx	
3	Netcom PPPoE Tx	
4	Netcom PPPoE CPU	

The 'New Chart Line' dialog is open, with the 'Source' dropdown menu set to 'Netcom PPPoE CPU', which is highlighted with a red box. A red arrow points from the 'Netcom PPPoE CPU' entry in the 'Elements' table to the 'Source' dropdown in the 'New Chart Line' dialog.

Workshop: PPPoE Server Chart

Result:



Remark: On this server Rx = Tx

Charts and Datasources – further hints

Charts for CCQ values and links details

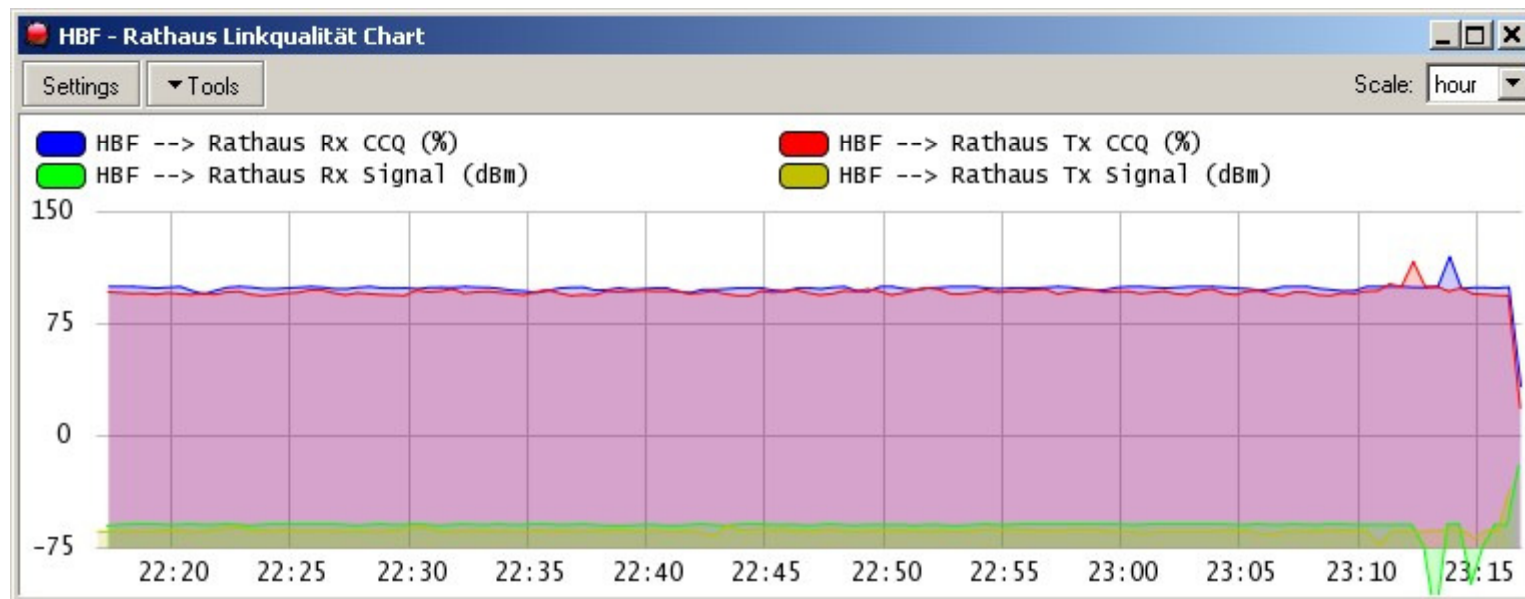
```
ros_command (":local f [/interface wireless  
registration-table find mac-address  
=00:0C:42:3A:26:26];:put [/interface wireless  
registration-table get $f rx-ccq];")
```

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

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

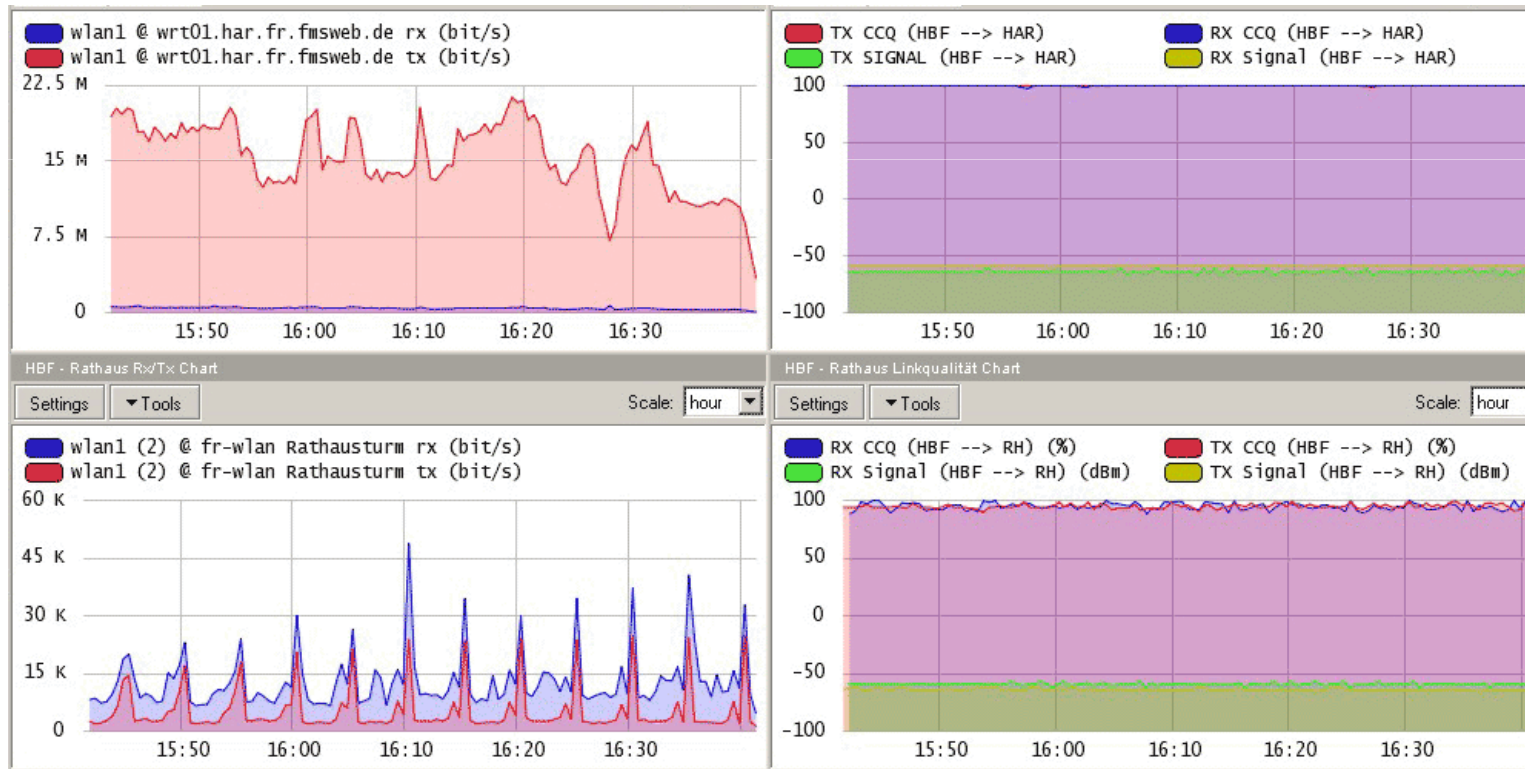
Charts and Datasources – further hints

WLAN Example 1



Charts and Datasources – further hints

WLAN Example 2



Thank you for listening

