Monitoring and visualizing your MikroTik networks

A monitoring deep-dive

Presenter information

Tomas Kirnak

Network design and security
Ethernet and wireless
Servers & Virtualization
Network management & monitoring

MikroTik Certified Trainer
MikroTik Certified Consultant

RF elements s.r.o.

Wireless equipment manufacturer
Enclosures
Antennas
Shields

RF ELEMENTS®

Agenda

- SNMP primer
- Syslog primer

- How to configure SNMP and syslog on MikroTik
- Most useful OIDs on MikroTik

- A look at monitoring software (The Dude and NetXMS)

- Gotchas and things that don’t work

First a little poll

A monitoring poll - essential

- How many of you do **NOT** have any monitoring in your network?
- How many of you **DO** have monitoring?

A monitoring poll - level 1

- Keep your hands up if you:
  - monitor CPU, RAM, HDD usage
  - monitor traffic (bps and pps) of interfaces on your board
  - monitor temperature, voltage and watt usage of your boards
  - have proper thresholds on all of these monitored values and generate alarms on threshold violation

  - have mail alerting on alarms
  - have sms alerting on alarms

A monitoring poll - level 2

- Keep your hands up if:
  - collect snmp traps
  - alert based on snmp traps
  - you collect syslog
  - alert based on syslog

A monitoring poll - level “maps”

- Another test, how many of you have:
  - maps of your network
  - those maps are still completely accurate
  - separate L2 map?
  - separate L3 map?

  - have dynamic L2 and L3 maps?

Why all these questions?

- Monitoring is amongst the most important things in networking and IT in general.

- A difference between "I think everything is OK" and "I know everything is OK for a fact" is huge.

Why all these questions? v2

- These questions were aimed at a few things…
- A monitoring system that doesn’t monitor necessary things is not very useful.
- A proper monitoring system needs to be independent.
  - You should not have to look at it to see if there is a problem - the system should **tell you** when there is a problem

Why all these questions? v3

- Regarding Network maps…

- Network maps are a very useful **addition** to your documentation
  - Visualizing your network helps identify break points
  - Helps new employees to understand your network faster
  - Helps consultants help you faster

What are we doing here?

- Hopeful outcome of this presentation…
- Hopefully, by the end of this presentation, all of you will know enough basics to have all of these nice things.

RF ELEMENTS®

SNMP primer

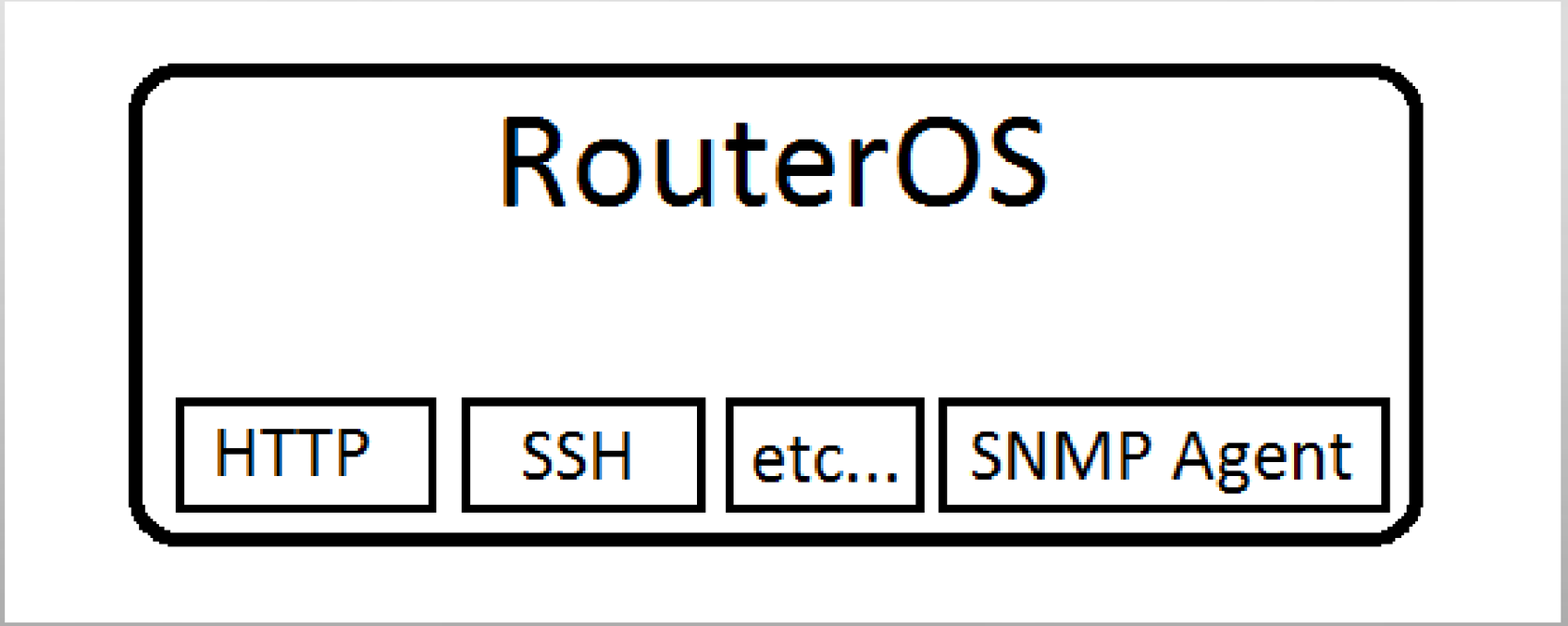
SNMP (Simple Network Management Protocol) basics

- SNMP is an L7 protocol used for management of network devices.
- It is used to get management information from devices and set configuration on the device.

- For this presentation - we use it to collect data (CPU usage, interface statistics, etc.) from our MikroTik devices.

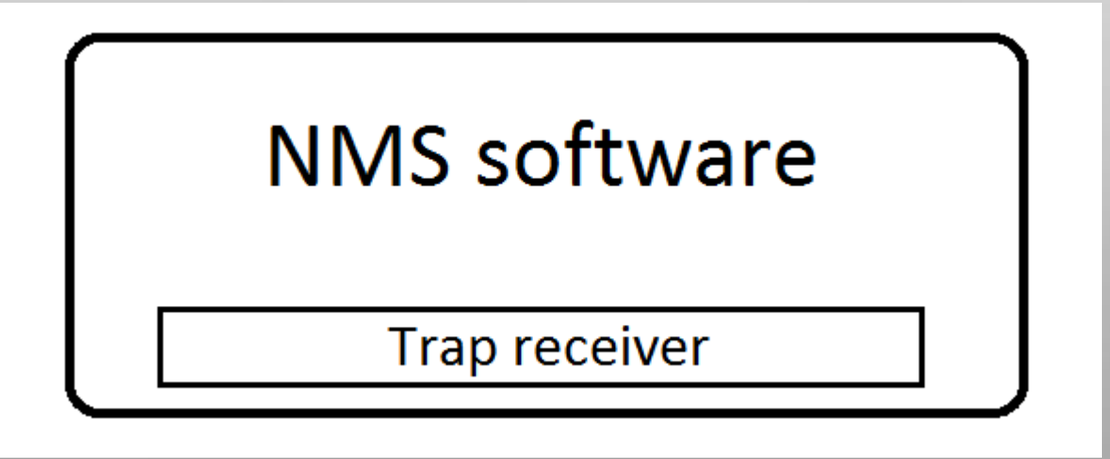
How SNMP works – components 1

- Device runs an SNMP agent.
  - This is a piece of software providing SNMP service.
  - You could call it a SNMP “server”, but please don’t – that is wrong.



How SNMP works – components 2

- We have a NMS (Network Monitoring System)
  - also called a SNMP manager
  - retrieves information from the device
- We have an SNMP trap collector
  - this is a receiver service running in the NMS
  - receives SNMP traps from the device

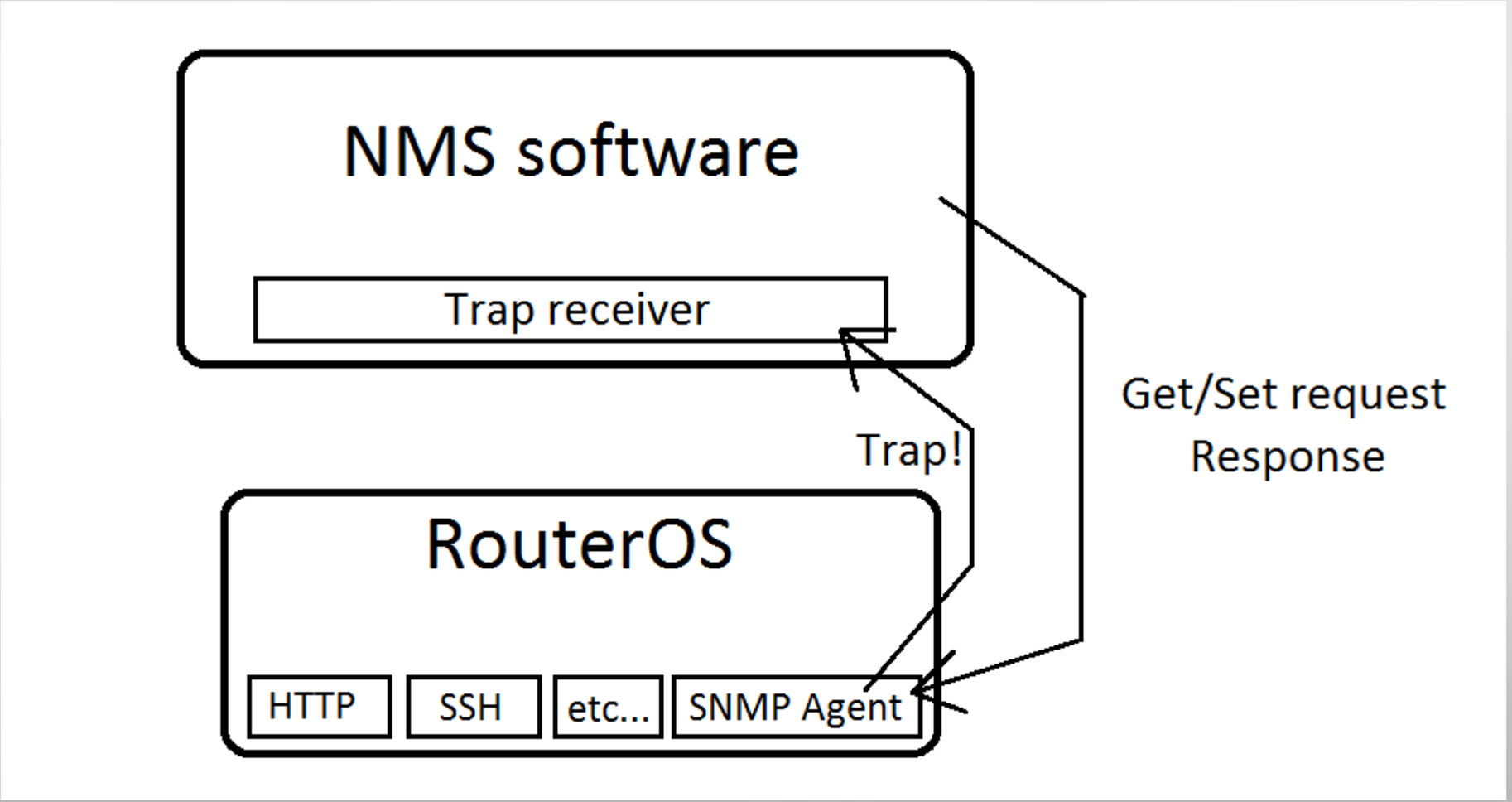


SNMP Get/Set

- SNMP can be used to GET information from a device
  - most common usage of SNMP

- SNMP can also be used to SET some device configuration
  - this includes turning interfaces on/off
  - managing the SNMP Agent itself
  - rebooting device
  - MANY other things

Completely technically accurate graph



Just a note: responses are not traps.

SNMP versions

- SNMP has 3 version
  - v1, v2c, v3

- Lets take a closer look.

SNMP v1 - 1988

- First standardized SNMP version
  - Authentication using a community string (basically a PSK)
  - Separate community for GET and SET

- It was a great start, but it had issues...
- Mainly - 32 bit counters
  - max 32 but unsigned integer - 4GiB
  - using a 1GBit interface, counter will overflow in 4 sec

SNMP v2c

- SNMP getting better:
  - performance improvements
  - support for 64bit counters!
- Still using a community string for authentication

SNMP v3

- All the good things from v2c but with new security model.
  - Supports username/password authentication
  - Supports integrity message integrity verification using md5/sha1
  - Supports message encryption using des/aes128

- 3 security modes
  - NoAuthNoPriv (no integrity check, no encryption)
  - AuthNoPriv (integrity check, no encryption)
  - AuthPriv (integrity check and encryption - CPU heavy)

SNMP best practice

- What to do with all of these versions?
  - Do NOT use v1 under any circumstance...
  - Use v2c only if you have to.
  - Use v3 - best to use AuthNoPriv... (use over VPN, not public internet)

MIBs (Management information bases)

- MIBs describe data (and its organization) inside of the SNMP structures.

- Why do they exist?
  - SNMP structure is made to be easily expandable
  - each vendor may need to expose different thing over SNMP
  - makes the system actually quite user-friendly

So what is a MIB??

- It is a file you give your NMS
- It will use it to make the information you get from SNMP more useful

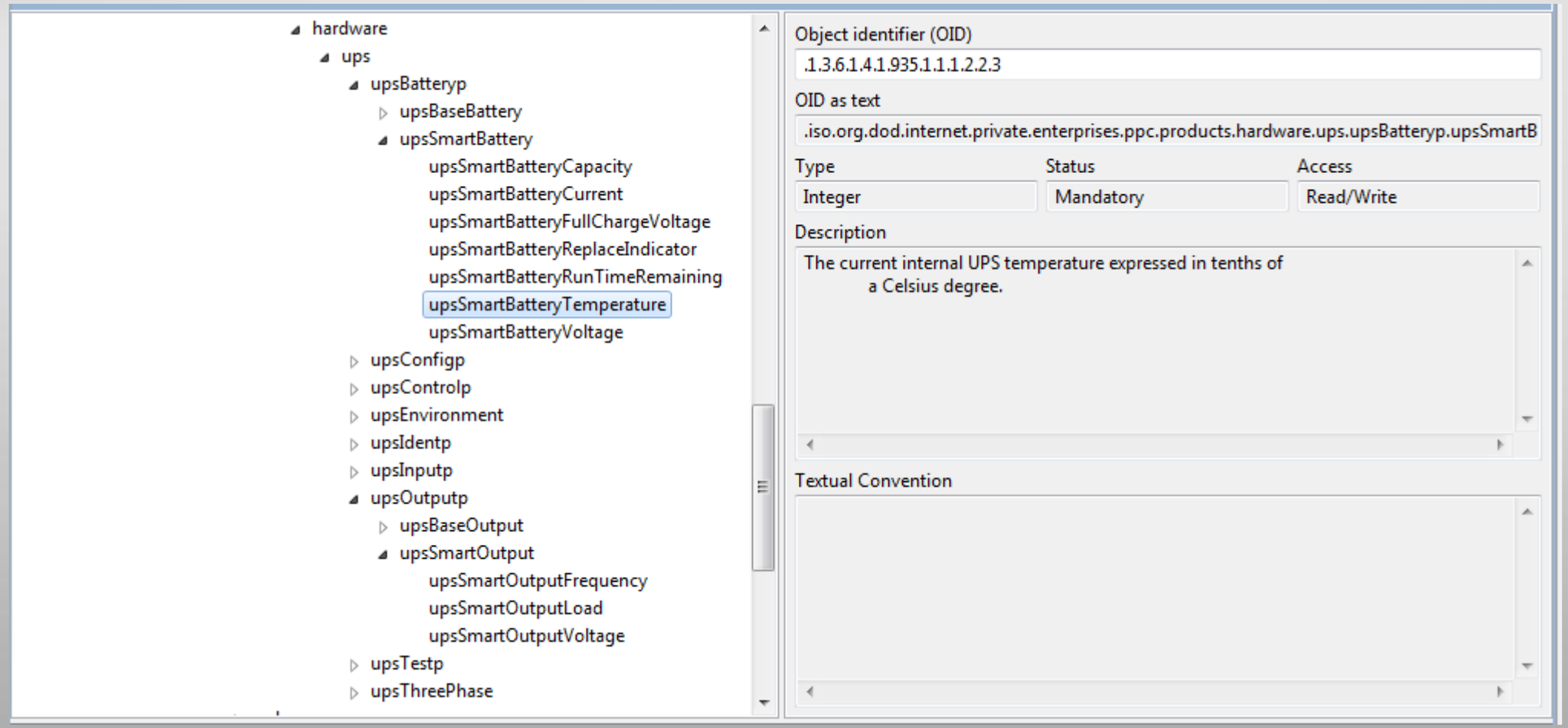
With and without MIBs - 1

- Difference of having MIBs and **NOT having** MIBs

OID	Type	Value
.1.3.6.1.4.1.935.1.1.1.1.1.1.0	STRING	Intelligent
.1.3.6.1.4.1.935.1.1.1.1.1.2.0	STRING	
.1.3.6.1.4.1.935.1.1.1.1.2.1.0	STRING	R1.1.1
.1.3.6.1.4.1.935.1.1.1.1.2.2.0	STRING	
.1.3.6.1.4.1.935.1.1.1.1.2.3.0	STRING	
.1.3.6.1.4.1.935.1.1.1.1.2.4.0	STRING	2.47.CT504.WEST
.1.3.6.1.4.1.935.1.1.1.2.1.1.0	INTEGER	2
.1.3.6.1.4.1.935.1.1.1.2.1.2.0	INTEGER	0
.1.3.6.1.4.1.935.1.1.1.2.1.3.0	STRING	2013/01/15
.1.3.6.1.4.1.935.1.1.1.2.2.1.0	INTEGER	95
.1.3.6.1.4.1.935.1.1.1.2.2.2.0	INTEGER	22
.1.3.6.1.4.1.935.1.1.1.2.2.3.0	INTEGER	290
.1.3.6.1.4.1.935.1.1.1.2.2.4.0	INTEGER	0
.1.3.6.1.4.1.935.1.1.1.2.2.6.0	INTEGER	720
.1.3.6.1.4.1.935.1.1.1.2.2.7.0	INTEGER	0
.1.3.6.1.4.1.935.1.1.1.3.1.1.0	INTEGER	1
.1.3.6.1.4.1.935.1.1.1.3.2.1.0	INTEGER	2303
.1.3.6.1.4.1.935.1.1.1.3.2.2.0	INTEGER	2322
.1.3.6.1.4.1.935.1.1.1.3.2.3.0	INTEGER	2299
.1.3.6.1.4.1.935.1.1.1.3.2.4.0	INTEGER	500
.1.3.6.1.4.1.935.1.1.1.3.2.5.0	INTEGER	1
.1.3.6.1.4.1.935.1.1.1.4.1.1.0	INTEGER	2

With and without MIBs - 2

- Difference of **having** MIBs and NOT having MIBs



How data is structured in SNMP

- Data (information) in SNMP is structured as a tree.

- As you work with SNMP, you will learn what is located where in the tree.

- Example:
  - .1.3.6.1.2.1.1 – basic system information
  - .1.3.6.1.2.1.2.2.1 – basic interface table
  - .1.3.6.1.2.1.31.1.1 – advanced interface table

OIDs (Object Identifiers)

- These “paths” are called OIDs
  - .1.3.6.1.2.1.1 – basic system information
  - .1.3.6.1.2.1.2.2.1 – basic interface table
  - .1.3.6.1.2.1.31.1.1 – advanced interface table

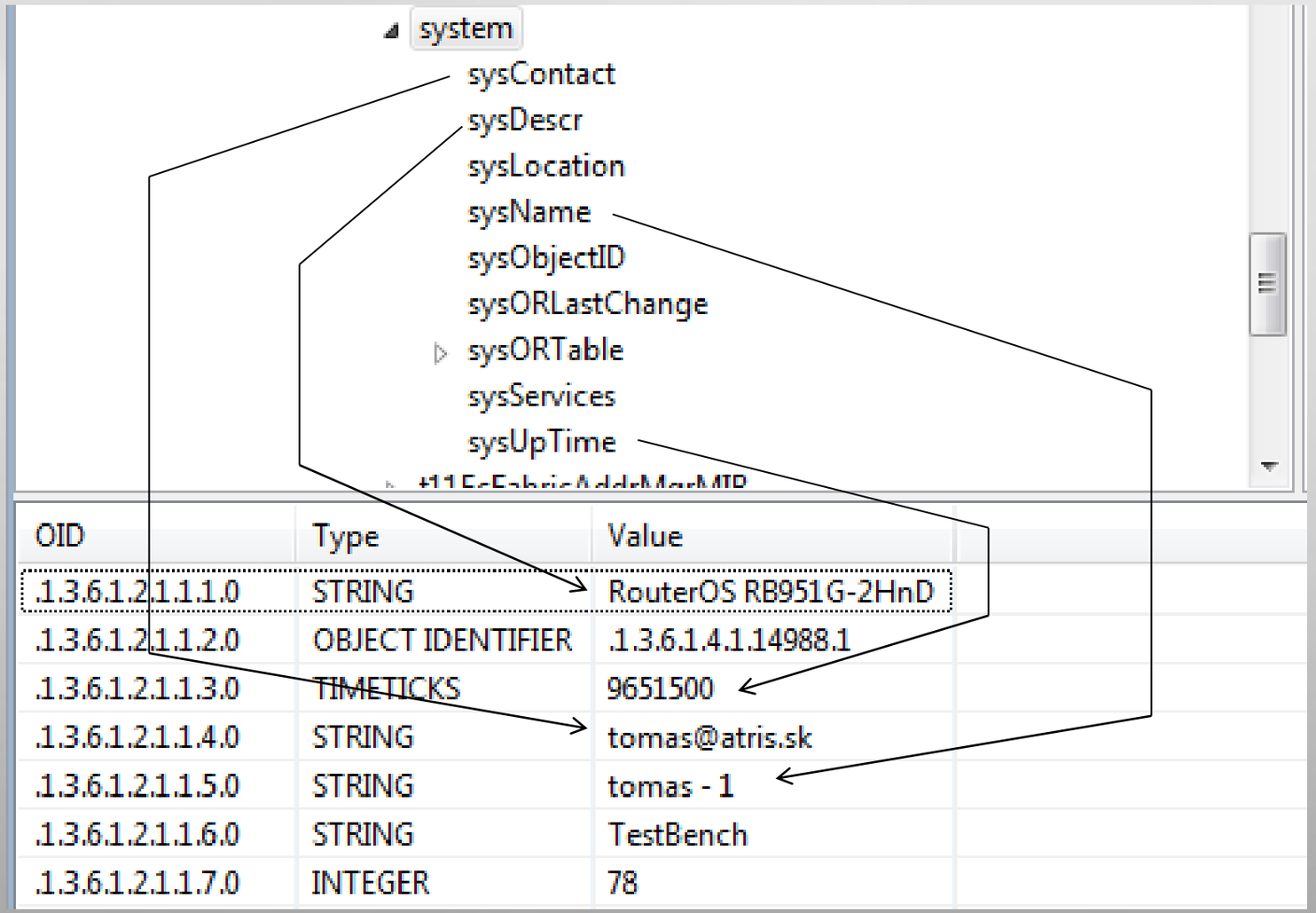
- There are many OIDs for many things…
- We will look at some useful ones soon

SNMP “walking”

- SNMP walking refers to getting all the data in the tree under a certain OID.
- For example, walking .1.3.6.1.2.1.1 would give me basic information about the device
- Walking .1 would dump all info available over SNMP
  - Don’t do it, it will take ages and possibly kill the CPU in your device

Actual SNMP walk

- Actual walk of .1.3.6.1.2.1.1



OID	Type	Value
.1.3.6.1.2.1.1.1.0	STRING	RouterOS RB951G-2HnD
.1.3.6.1.2.1.1.2.0	OBJECT IDENTIFIER	.1.3.6.1.4.1.14988.1
.1.3.6.1.2.1.1.3.0	TIMETICKS	9651500
.1.3.6.1.2.1.1.4.0	STRING	tomas@atris.sk
.1.3.6.1.2.1.1.5.0	STRING	tomas - 1
.1.3.6.1.2.1.1.6.0	STRING	TestBench
.1.3.6.1.2.1.1.7.0	INTEGER	78

SNMP Tables

- Data in SNMP is organized in tables
- Here is an example:

Index	Name	Alias/Comment	MTU	Type	MAC address	Connector present
1	ether1	oobm.local	1500	6	??m??	
2	ether2		1500	6	??m??	
3	ether3		1500	6	??m??	
4	ether4		1500	6	??m??	
5	ether5		1500	6	??m??	
6	ether5.vlan3003	tomas.local	1500	135	??m??	
7	lo1		1500	209	??????	
8	ether5.vlan1000	backbone.local	1500	135	??m??	
9	ether5.vlan1002	b1.wlan1.local	1500	135	??m??	

How SNMP tables work

- There is usually a main TableIndex OID
- Example - .1.3.6.1.2.1.2.2.1.1 – ifIndex table

OID	Type	Value
.1.3.6.1.2.1.2.2.1.1.1	INTEGER	1
.1.3.6.1.2.1.2.2.1.1.2	INTEGER	2
.1.3.6.1.2.1.2.2.1.1.3	INTEGER	3
.1.3.6.1.2.1.2.2.1.1.4	INTEGER	4
.1.3.6.1.2.1.2.2.1.1.5	INTEGER	5
.1.3.6.1.2.1.2.2.1.1.6	INTEGER	6
.1.3.6.1.2.1.2.2.1.1.7	INTEGER	7

- We have 7 interfaces on this router

Working with the SNMP tables

- We can then walk different OIDs for data about each interface
- Index ensures we know which data belongs to which interface

walk .1.3.6.1.2.1.2.2.1.1
ifIndex

OID	Type	Value
.1.3.6.1.2.1.2.2.1.1.1	INTEGER	1
.1.3.6.1.2.1.2.2.1.1.2	INTEGER	2
.1.3.6.1.2.1.2.2.1.1.3	INTEGER	3
.1.3.6.1.2.1.2.2.1.1.4	INTEGER	4
.1.3.6.1.2.1.2.2.1.1.5	INTEGER	5
.1.3.6.1.2.1.2.2.1.1.6	INTEGER	6
.1.3.6.1.2.1.2.2.1.1.7	INTEGER	7

walk .1.3.6.1.2.1.2.2.1.2
ifDescr

OID	Type	Value
.1.3.6.1.2.1.2.2.1.2.1	STRING	ether1
.1.3.6.1.2.1.2.2.1.2.2	STRING	ether2
.1.3.6.1.2.1.2.2.1.2.3	STRING	ether3
.1.3.6.1.2.1.2.2.1.2.4	STRING	ether4
.1.3.6.1.2.1.2.2.1.2.5	STRING	ether5
.1.3.6.1.2.1.2.2.1.2.6	STRING	wlan1
.1.3.6.1.2.1.2.2.1.2.7	STRING	bridge1

walk .1.3.6.1.2.1.2.2.1.4
ifMTU

OID	Type	Value
.1.3.6.1.2.1.2.2.1.4.1	INTEGER	1500
.1.3.6.1.2.1.2.2.1.4.2	INTEGER	1500
.1.3.6.1.2.1.2.2.1.4.3	INTEGER	1500
.1.3.6.1.2.1.2.2.1.4.4	INTEGER	1500
.1.3.6.1.2.1.2.2.1.4.5	INTEGER	1500
.1.3.6.1.2.1.2.2.1.4.6	INTEGER	1500
.1.3.6.1.2.1.2.2.1.4.7	INTEGER	1500

Too complicated - TMI

- Don’t worry, most of this is handled internally by the NMS
- You just have to know certain data is available at a certain OID
- You can use [insert your favorite search engine here] to find the OID of the data you are looking for

RF ELEMENTS®

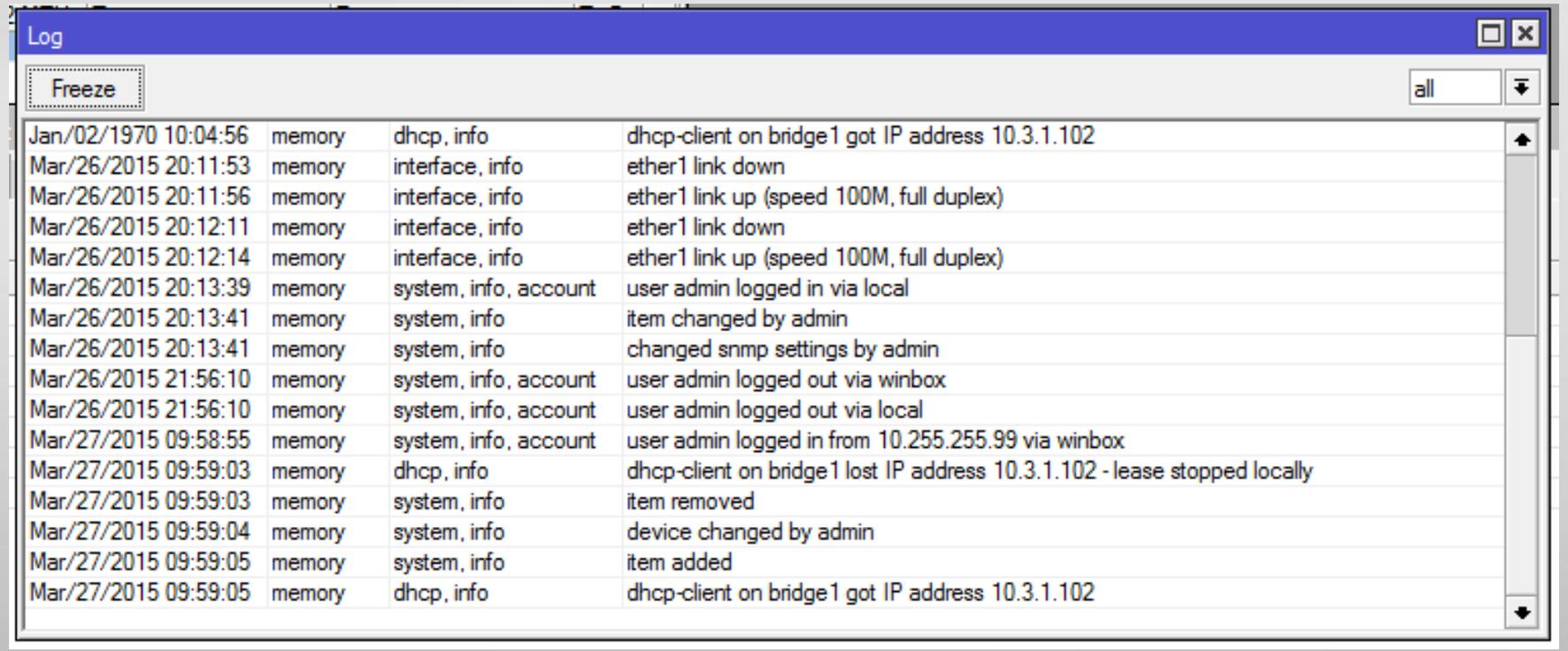
Syslog primer

Syslog is easy

- On a basic level - Syslog is just a standard to transfer logs over the network
- Using syslog, you can dump all the logs your device generates to a NMS
- This is very useful, and you should do it!

Why syslog?

- You have logs locally in your device



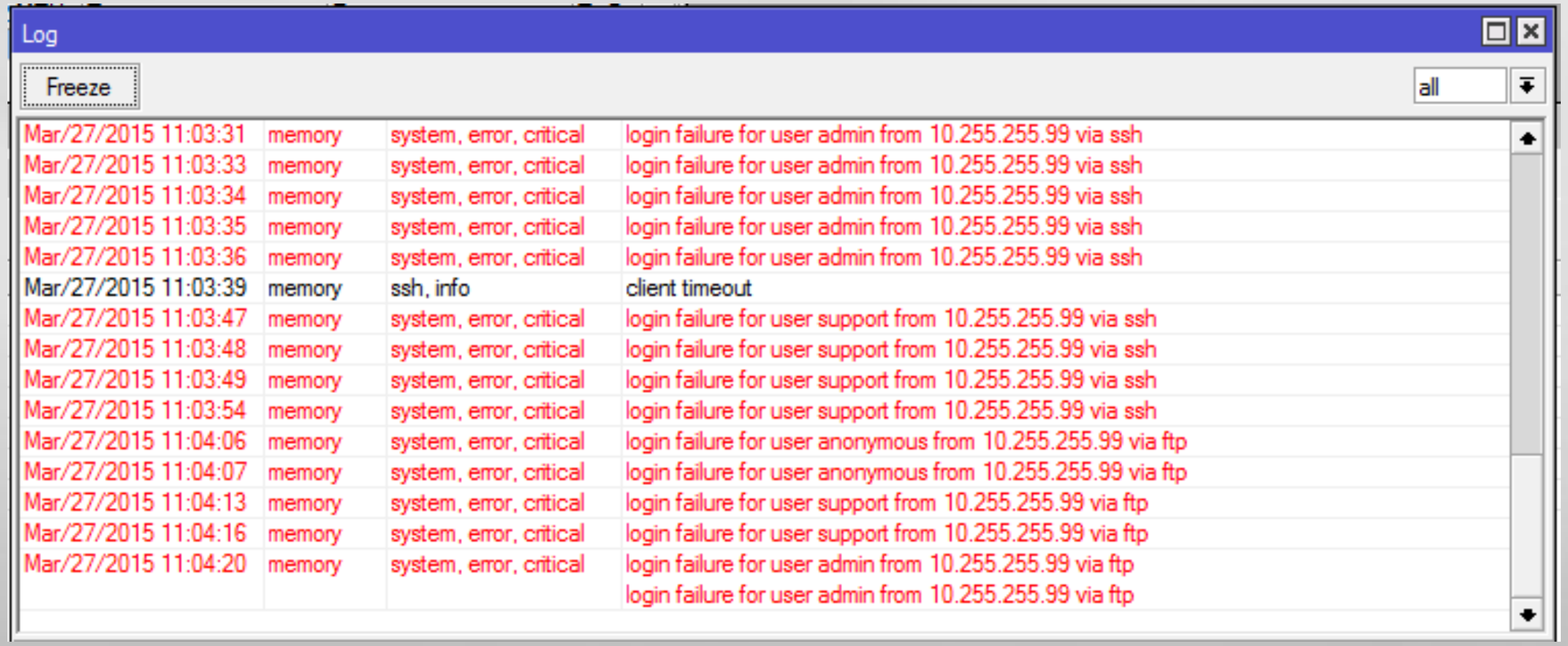
- These are lost at reboot

What is Syslog useful for?

- If a device goes down, its useful to look at logs, to see why.
- A NMS can keep a long history of logs, device has limited memory
- With a right NMS, you can do really nice searching a filtering of logs.

- You can generate alerts and alarms based on logs!
  - If an invalid login happens more then 3x in 5 minutes, send me an email!

Actual Syslog usage.



- This is bad, and you should know about it!

RF ELEMENTS®

Configuring SNMP on MikroTik

CLI to get SNMP

- SNMP v3 made easy:

/snmp community

set [find default=yes] authentication-password="my-password" authentication-protocol=SHA1 name="my-username" security=authorized

/snmp

set enabled=yes contact="kirnak@rfelements.com" location="TestBench" trap-target="NMS-IP-address" trap-generators=interfaces,start-trap trap-interfaces=all trap-version=3

RF ELEMENTS®

Configuring Syslog on MikroTik

CLI to get Syslog

- Syslog made east:

/system logging action

set 3 remote= “NMS-IP-address”

/system logging

add action=remote topics=critical

add action=remote topics=error

add action=remote topics=info

add action=remote topics=warning

RF ELEMENTS®

Useful OIDs on MikroTik

Useful general OIDs

- Cpu usage of each core
  - .1.3.6.1.2.1.25.3.3.1.2
- RouterOS version
  - .1.3.6.1.4.1.14988.1.1.4.4.0
- Health table (temperatures, voltage, etc…)
  - .1.3.6.1.4.1.14988.1.1.3
- Storage table (disk and RAM usage)
  - .1.3.6.1.2.1.25.2.3
- IfXTable (interface data – including bps and pps)
  - .1.3.6.1.2.1.31.1.1.1

Useful wireless OIDs

- Wireless card frequency
  - .1.3.6.1.4.1.14988.1.1.1.3.1.7
- Total wireless clients
  - .1.3.6.1.4.1.14988.1.1.1.4
- In AP mode – per client data (signal strength, speed, etc…)
  - .1.3.6.1.4.1.14988.1.1.1.2.1.1
- Number of PPP clients
  - .1.3.6.1.4.1.9.9.150.1.1.1

What you should aim for

Our aim – level 1

- To have monitoring!

- To collect:
  - CPU, RAM, HDD usage
  - traffic (bps and pps) of interfaces on your devices
  - monitor temperature, voltage and watt usage of your boards
  - have proper thresholds on all of these monitored values and generate alarms on threshold violation

  - have mail alerting on alarms
  - have sms alerting on alarms with high severity

Our aim – level 2

- To have more nice things!
  - collect snmp traps
  - alert based on snmp traps
  - collect syslog
  - alert based on syslog

  - dynamic L2 and L3 maps

What I'm trying to say

Monitor everything!

Why all of this?

- Have “peace-of-mind” and know for a fact your network is fine, not just assume.

- Have an independent system that will let you know when something is wrong, rather then you having to look at it.

A look at some NMSs

The Dude

- MikroTik NMS
- Free
- Very easy to pick up and learn
- Very fast to get started

Dude demo…

Please watch presentation video

The Dude - faults

- Its no longer maintained
  - Last release about 4 years ago

- No templates
- Tedious setup for many things
- 64bit counters break a lot…
- 2GB DB limit on-disk SQLite
- Windows only
- Web interface … simplistic
- Etc, etc…

NetXMS

- Enterprise-grade NMS
- Free and open source
- Extremely powerful
- Extremely versatile

NetXMS best features

- Linux / Windows / Solaris / Mac OS X
- MySQL, PostgreSQL, MSSQL, Oracle DB….
- Unified web / dedicated client
- Templates, thresholds, lots of alerting options
- Topology aware
- Summary tables
- IP/MAC search
- Syslog
- Dashboards
- I could go on…

NetXMS demo…

Please watch presentation video

A few gotchas

- There has been a lot of SNMP bugs in RouterOS
  - Bulk walk doesn’t work v6.20 - v6.23
  - v3 timing problems make v3 not work at all v6.8 - v6.16
  - Storage was missing completely in SNMP v6.20 - v6.23
  - Etc…

- What I’m trying to say, always use newest RouterOS version - also make sure to use latest RouterBOOT version
  - Some SNMP bugs were fixed with RouterBOOT upgrade before

A few gotchas - more bugs

- You are not safe even right now!
  - There is currently a bug in 6.27 that causes the routing table not being reported over SNMP in certain cases.
- This will be fixed in v6.29 (not v6.28!)
- Make sure to upgrade to 6.29 when it comes out.

A few gotchas - storage…

- In older versions (older then ~v6.15) storage was reported differently on x86 and RouterBoards
- This basically meant you needed separate monitoring templates for x86 and RouterBoards.
- This has since been fixed, but watch for this if you use older RouterOS.

What can still be improved

- There are still things that could be improved.

- MikroTik currently does **not** support
  - LLDP
  - STP MIB
  - BGP MIB

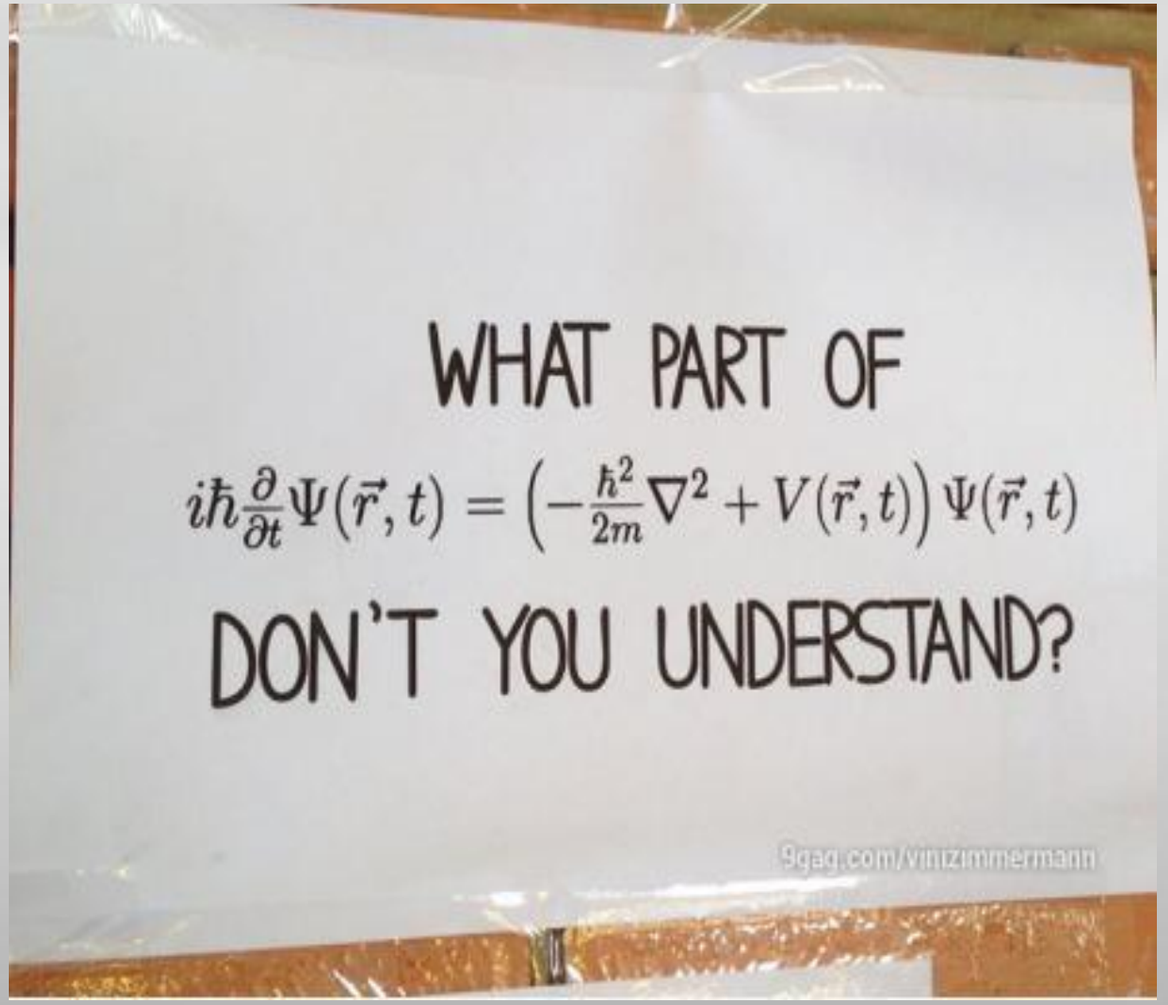
- Supporting these would **REALLY** help.

That's it!

- If you liked this presentation, more material from me:
  - **Bandwidth-based load-balancing without MPLS TE**
  - **Scalable IPSec (IPSec basics + L2TP /IPSec)**
  - **MPLS for ISPs (MPLS basics + PPPoE over VPLS)**
  - **OSPF to the customer**
  - **Using DSCP for traffic separation, routing and load-balancing**

- Find the presentations on www.tiktube.com

  Search for "Kirnak"



If you have any questions, please ask now, or find me after the presentation.

Thanks for listening

Tomas Kirnak

kirnak@rfelements.com