Demystifying SNMP
Who is TruePath Technologies Inc?

US based, leading edge IT software and services company that specializes in in-house services for new or existing IT monitoring software. We offer software with an easy to use web based portal software that provides bandwidth and line quality monitoring and reporting.
Douglas Mauro is the Founder and Senior Engineer at TruePath Technologies Inc. with over 20 years of experience in enterprise data centers. He's an O'Reilly author of Amazon's #1 selling network management book "Essential SNMP" (now in it's second edition). His most recent endeavor has taken him to software publishing; TruePath's latest Telco Web Portal LMS.

His involvement in and outside the industry has guided TruePath to be one of America’s top monitoring software SaaS companies.

While computers and electronics are staples in his life, competitive bike racing, triathlons and, of course, family come first.

Email: dmauro@truepathtechnologies.com
LinkedIn: www.linkedin.com/in/douglasmauro

Phone: 585-672-5481
Cell: 716-474-1641
Agenda
Topics Of Discussion

• What is SNMP (what are MIBs)
• What are traps?
• Anyone use sets?
• What devices use SNMP?
• What’s an agent and NMS?
• What’s the BEST SNMP version?
• Flow of communication (how to use, commands, data flow view)
• Where can I get software for my OS?
• Does my XYZ device need software or agent?
• What does agentless mean?
• I have device X, does it support mib Z?
  • I’m polling mib XYZ, why doesn’t my ABC device respond?
• Exploring a sample MIB
• Doing the big walk! (why all numbers? What can I find that looks fun?)
• What about snmpget and bulk?
• Reverse eng a walk to mib (aka google it!)
• Poll –vs- trap? What’s better?

• Gimmie some popular software to try now!
• What’s all this rrd talk?
What Is SNMP?

“The core of SNMP is a simple set of operations”
HIGH LEVEL MONITORING ARCH

Traditional Single NMS

Switches

Servers

Applications

Network Management System

NMS

WEB

SNMP
HIGH LEVEL MON ARCH

Distributed NMS

LONDON
NMS

U.S.
NMS

WEB

VPN / Secure Network

SNMP

SNMP

SNMP
What’s a MIB?
Management Information Base

“The Structure of Management Information (SMI) provides a way to define managed objects and their behavior.”

ifOperStatus OBJECT-TYPE
SYNTAX INTEGER {
  up(1), -- ready to pass packets
down(2),
testing(3) -- in some test mode
}
ACCESS read-only
STATUS mandatory
DESCRIPTION "The current operational state of the interface. The testing(3) state indicates that no operational packets can be passed.”
 ::= { ifEntry 8 }

ifLastChange OBJECT-TYPE
SYNTAX TimeTicks
ACCESS read-only
STATUS mandatory
DESCRIPTION "The value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then this object contains a zero value.”
 ::= { ifEntry 9 }

ifInOctets OBJECT-TYPE
SYNTAX Counter
ACCESS read-only

RFC 1213 MIB-II March 1991
https://www.rfc-editor.org/rfc/rfc1213.txt
rfc1213.txt
Polling Versus Traps

**SNMP TRAP**

**ONE WAY**

**SNMP GET / NEXT / TABLE**

**TWO WAY**

Router -> NMS (One Way)

Router <-> NMS (Two Way)
What About Sets?

Not Very Common To Use

Router

SNMP SET

TWO WAY

NMS

```plaintext
sysLocation OBJECT-TYPE
SYNTAX   DisplayString (SIZE (0..255))
ACCESS   read-write
STATUS   mandatory
DESCRIPTION
    "The physical location of this node (e.g., 'telephone closet,
    3rd floor')."
 ::= { system 6 }
```
Do I Need An Agent?
What Does Agentless Mean?

Switches

Built In SNMP Agent

Operating Systems

Need to Install SNMP Agent

Scripts

Uses Free SNMP Libraries

NMS

SNMP

HW Device Dry Contacts

Generator

Uses Free SNMP Libraries

Switches

SNMP

SNMP

SNMP

SNMP
Where Can I Get SNMP Agent SW?
What Devices (os, ios, etc) Are You Using?

• For network type devices, the software will usually be installed (there) but might not be turned on or configured.

• Other devices like large UPS (battery) systems may require an additional card/software to use SNMP

• Windows has an agent that you can freely download and install
  •  You might want to look at WMI checks as the Win agent is very basic

• For Linux, the standard out there seems to be Net-SNMP
  •  http://www.net-snmp.org/download.html
What Version Is The Best?
SNMPv2 Is The Most Popular

• In a lot of ways you won’t have a choice. Your equipment will determine that.

• V2 and v3 can be thought of as the same with v3 including better security

• Should I push for v3? (Would you put a padlock on your car door?)
Why Doesn’t This MIB Work?
Agent Supports MIBs, NOT The Other Way Around
DATA COLLECTION

How Does The Information Flow?

Switches

INT STATS
PORT SPEED
DROPS

SNMP COMMANDS

Switches

VOIP

MOS
JITTER
LATENCY

WEB

SNMP COMMANDS

WEB

NMS

SNMP COMMANDS

DISK
MEMORY
CPU
APPLICATION
DB

......
.....

Applications
DATA COLLECTION
I WANT MORE!

- NMS receives a response from the agent for the *get-next* command
- It then issues another *get-next* command
- It keeps doing this until the agent returns an error, signifying that the end of the MIB has been reached and there are no more objects left to get.

agent sends back as much as it can in *one* response.
The Big Walk

Why All The Numbers?

[root@tpt-nms> /var/tpt/bin ]: snmpwalk -v2c -c public 11.0.44.171 .1.3.6.1.2.1.2.1.2.1.1.8.2 = INTEGER: up(1)
.1.3.6.1.2.1.2.1.9.1 = Timeticks: (97681) 0:16:16.81
.1.3.6.1.2.1.2.1.9.2 = Timeticks: (111822123) 12 days, 22:37:01.23
.1.3.6.1.2.1.2.1.10.1 = Counter32: 2457344102
.1.3.6.1.2.1.2.1.10.2 = Counter32: 2163677797
.1.3.6.1.2.1.2.1.11.1 = Counter32: 5331002
.1.3.6.1.2.1.2.1.11.2 = Counter32: 3581821
Mixing In Some Spice
Let's Add Some MIBs To Our Walk

[root@tpt-nms /var/tpt/bin ]: snmpwalk -v2c -c public 11.0.43.171 .1.3.6.1.2.1.2 -M /usr/share/snmp/mibs -m ALL

IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifDescr.1 = STRING: PORT-1
IF-MIB::ifType.1 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifMtu.1 = INTEGER: 2000
IF-MIB::ifSpeed.1 = Gauge32: 100000000
IF-MIB::ifPhysAddress.1 = STRING: 0:15:ad:1a:f8:49
IF-MIB::ifAdminStatus.1 = INTEGER: up(1)
IF-MIB::ifOperStatus.1 = INTEGER: up(1)
IF-MIB::ifLastChange.1 = Timeticks: (97681) 0:16:16.81
IF-MIB::ifInOctets.1 = Counter32: 2458205995
IF-MIB::ifInUcastPkts.1 = Counter32: 5340471
IF-MIB::ifInNUcastPkts.1 = Counter32: 1212759
IF-MIB::ifInDiscards.1 = Counter32: 0
IF-MIB::ifInErrors.1 = Counter32: 0
IF-MIB::ifInUnknownProtos.1 = Counter32: 0
IF-MIB::ifOutOctets.1 = Counter32: 2330564360
IF-MIB::ifOutUcastPkts.1 = Counter32: 5111373
IF-MIB::ifOutNUcastPkts.1 = Counter32: 91547
IF-MIB::ifOutDiscards.1 = Counter32: 0
IF-MIB::ifOutErrors.1 = Counter32: 0
Where’s My MIB?
Common Places To Find Vendor MIBs

• Ask The Vendor!
• Google the 1st OID to enterprise
  • Brocade would be: .1.3.6.1.4.1.1991

• Online Tools:
  • Cisco’s Object Nav: http://goo.gl/ZYFdRf
  • https://www.plixer.com/Support/mib-resources.html
  • http://www.oidview.com/mibs/detail.html
  • http://www.snmplink.org/OnLineMIB/Standards/
Just Gimmie The Software!
Quick Places To Grab Some Software And Start Playing

- Check_MK
- Op5
  - [http://www.op5.com/download-op5-monitor/](http://www.op5.com/download-op5-monitor/)
- Nagios
  - [https://www.nagios.org/downloads/](https://www.nagios.org/downloads/)
- Net-SNMP
  - [http://www.net-snmp.org/download.html](http://www.net-snmp.org/download.html)
- RRDtool
  - [http://oss.oetiker.ch/rrdtool/](http://oss.oetiker.ch/rrdtool/)
- Cacti
  - [http://www.cacti.net/download_cacti.php](http://www.cacti.net/download_cacti.php)
THANK YOU

http://truepathtechnologies.com
http://www.facebook.com/truepathtech
http://twitter.com/truepathtech