SNMP:
“Simple” “Network” “Management” “Protocol”

Michael W Lucas

https://mwl.io

Who I Am?

- Author
- Unix since 198(mumble), sysadmin since 1995
- Founding member of SouthEast Michigan BSD User Group, semibug.org
- Blatant BSD demagogue
- Author of many tech books, including *SNMP Mastery*
- As Michael Warren Lucas, novels like *git commit murder*
- Martial arts, pet rats, married, blah blah blah

What is SNMP?

- Simple Network Management Protocol
- Created in 1980s as a replacement to SGMP, was intended as intermediate protocol until something more complex was created

- Manager = client, agent = server

- This talk uses net-snmp agent and manager

“Simple”

- GET
- GETBULK
- GETNEXT
- SET
- TRAP
- INFORM
- RESPONSE

“Network”

- Usable across the network
- 1980s networks != 1990s networks != Naughties != Teens !=20s

- usually UDP, usually port 161
- other transports: TCP, TLS, SSH

“Management”

- exchange “management information” with hosts
- What is management information?
  - Anything I say it is
  - Structured any way I think it should be

- Management Information Base
  - structured management information, described in a MIB file
  - implementation should always match description
  - some data defined by standard, some by vendor

“Protocol”

- SNMPv3 (2002)
  - current, extensible, efficient, encrypted, authenticated, flexible
- SNMPv2c (1996)
  - still here, extensible, efficient, unencrypted, unauthenticated, flexible
- SNMPv1 (1988)
  - zombie, extensible, inefficient, unencrypted, unauthenticated, flexible

- All three still being deployed in new products today!

Why SNMP?

- Network Duct Tape
- Produces data you can feed to anything

Why the Bad Rap?

- Human Beings are Trouble
  - misinterpretation
  - ignorance
  - sloppy code
  - indifference

The Management Information Base

- A hierarchical tree structure
- Objects have an address in the tree
- The object identifier (OID) is the address

- .1.3.6.1.2.1.1.1.0 = SNMPv2::sysDescr.0
- .1.3.6.1.4.1.2021 = net-snmp enterprise MIB
- .1.3.6.1.2.1.31.1.1 = ifXTable

Walking the Agent

$ **snmpbulkwalk gw**

SNMPv2-MIB::sysDescr.0 = STRING: RouterOS RB2011iL

SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.14988.1

DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (241494200) 27 days, 22:49:02.00

SNMPv2-MIB::sysContact.0 = STRING: support@mwl.io

SNMPv2-MIB::sysName.0 = STRING: 2019mainrouter

SNMPv2-MIB::sysLocation.0 = STRING: primary datacenter

SNMPv2-MIB::sysServices.0 = INTEGER: 78

IF-MIB::ifNumber.0 = INTEGER: 11

IF-MIB::ifIndex.1 = INTEGER: 1

IF-MIB::ifIndex.2 = INTEGER: 2

IF-MIB::ifIndex.3 = INTEGER: 3

IF-MIB::ifIndex.4 = INTEGER: 4

…

Walking Without Names

$ **snmpbulkwalk gw**

.1.3.6.1.2.1.1.1.0 = STRING: RouterOS RB2011iL

.1.3.6.1.2.1.1.2.0 = OID: .1.3.6.1.4.1.14988.1

.1.3.6.1.2.1.1.3.0 = Timeticks: (172674900) 19 days, 23:39:09.00

.1.3.6.1.2.1.1.4.0 = STRING: support@mwl.io

.1.3.6.1.2.1.1.5.0 = STRING: 2019mainrouter

.1.3.6.1.2.1.1.6.0 = STRING: primary datacenter

.1.3.6.1.2.1.1.7.0 = INTEGER: 78

.1.3.6.1.2.1.2.1.0 = INTEGER: 11

.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

…

SNMP Performance

- One query. One UDP packet. Easy.
- One interface. 22 characteristics.
- One server? 1000 servers?

SNMP Security

- “Security? Not My Problem!”
- SNMPv1/v2c Communities

Long-Term Survivability

- Protocols change
- Algorithms change
- vendors implement different algorithms at different times

SNMPv3, Privacy, and Authentication

- Three degrees of privacy
- noAuthNoPriv (noauth) – no encryption
- authNoPriv (auth) – hashed login & packet, plaintext data
- authpriv (priv) – encrypted login and data

SNMPv3 Users

- Traditional Sysadmin: Users are for access control
- SNMPv3: Users are a unique combination of access control, authentication algorithm, and privacy algorithm
- Suppose
  - manager speaks MD5, SHA, and SHA512 for auth and DES, 3DES, and AES128 for privacy
  - ShoggothCorp speaks MD5 and DES
  - Nightgaunt speaks SHA and AES128
- Users are stored on the agent

New User Checklist

- Username
- Privacy level (noauth, auth, priv)
- Authentication algorithm and passphrase
- Privacy algorithm and passphrase

Test User

$ **snmpstatus -v3 -l priv -u *username* -A *authPW* -a SHA-256 -X *privPW* -x AES128 localhost**

snmpd(8) Access Control – snmpd.conf

rwuser secureUser priv

rouser manager auth .1.3.6.1.4.1.2021

Querying Objects

```
$ snmpget gw DISMAN-EVENT-MIB::sysUpTimeInstance
DISMAN-EVENT-MIB::sysUpTimeInstance =
    Timeticks: (172632500) 19 days, 23:32:05.00
```

Grouping Objects

```
$ snmpwalk gw system
SNMPv2-MIB::sysDescr.0 = STRING: RouterOS RB2011iL
SNMPv2-MIB::sysObjectID.0 = OID: MIKROTIK-MIB::mikrotikExperimentalModule
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (172624200) 19 days, 23:30:42.00
SNMPv2-MIB::sysContact.0 = STRING: support@mwl.io
SNMPv2-MIB::sysName.0 = STRING: 2019mainrouter
SNMPv2-MIB::sysLocation.0 = STRING: primary datacenter
SNMPv2-MIB::sysServices.0 = INTEGER: 78
```

Tables

```
IF-MIB::ifName.1 = STRING: ether1-wow
IF-MIB::ifName.2 = STRING: ether2
…
IF-MIB::ifName.10 = STRING: ether10
IF-MIB::ifName.11 = STRING: bridge
IF-MIB::ifInMulticastPkts.1 = Counter32: 0
IF-MIB::ifInMulticastPkts.2 = Counter32: 0
…
IF-MIB::ifInMulticastPkts.10 = Counter32: 0
IF-MIB::ifInMulticastPkts.11 = Counter32: 0
IF-MIB::ifInBroadcastPkts.1 = Counter32: 0
IF-MIB::ifInBroadcastPkts.2 = Counter32: 0
…
```

Rendered Table

```
$ snmptable proxy3 ipNetToMediaTable
SNMP table: RFC1213-MIB::ipNetToMediaTable

ipNetToMediaIfIndex ipNetToMediaPhysAddress ipNetToMediaNetAddress ipNetToMediaType
                  1    "B8 69 F4 E8 39 0A "           203.0.113.1           other
                  1    "24 05 0F F6 AE 0D "          203.0.113.65           other
                  1    "08 00 27 B7 06 A6 "         203.0.113.207           other
…
```

Complete vs Empty Walks

- snmpwalk defaults to starting at “system” group & going down
- to see everything, start at .1

```
$ snmpbulkwalk switch666 .1
```

Walks vs Bulk Walks

- Walk = “give me the next object and its value”
- Bulk walk = give me the next 10 objects and their values” – SNMPv2+

Object Definitions

```
$ snmptranslate -Td SNMPv2-MIB::sysContact.0
SNMPv2-MIB::sysContact.0
sysContact OBJECT-TYPE
-- FROM       SNMPv2-MIB, RFC1213-MIB
-- TEXTUAL CONVENTION DisplayString
SYNTAX        OCTET STRING (0..255)
DISPLAY-HINT  "255a"
MAX-ACCESS    read-write
STATUS        current
DESCRIPTION   "The textual identification of the contact person for
this managed node, together with information on how
to contact this person.  If no contact information is
known, the value is the zero-length string."
::= { iso(1) org(3) dod(6) internet(1) mgmt(2) mib-2(1) system(1) sysContact(4) 0 }
```

The Good Stuff: Enterprise MIB

- an area of the SNMP tree where vendors and orgs can put their own MIBs.
- .1.3.6.1.4.1
- .iso.org.dod.internet.private.enterprises
- Orgs get numbers under this

Walk the Enterprise

```
$ snmpwalk gw enterprise
CISCO-SMI::ciscoMgmt.150.1.1.1.0 = Gauge32: 0
UCD-SNMP-MIB::ssCpuSystem.0 = INTEGER: 1
SQUID-MIB::cacheSysVMsize.0 = INTEGER: 50176
…
SQUID-MIB::cacheProtoStats.12.0 = INTEGER: 0
SQUID-MIB::cacheProtoStats.13.0 = INTEGER: 0
MIKROTIK-MIB::mtxrWlRtabEntryCount.0 = Gauge32: 0
MIKROTIK-MIB::mtxrWlCMRtabEntryCount.0 = Gauge32: 0
MIKROTIK-MIB::mtxrWlCMREntryCount.0 = Gauge32: 0
MIKROTIK-MIB::mtxrHlActiveFan.0 = STRING: n/a
MIKROTIK-MIB::mtxrHlProcessorFrequency.0 = INTEGER: 600
MIKROTIK-MIB::mtxrLicSoftwareId.0 = STRING: 1LJ9-HBY3
MIKROTIK-MIB::mtxrLicUpgrUntil.0 = STRING: 1970-1-1,0:1:7.0
…
```

snmpd(8): The net-snmp Agent

- common Unix agent
- configure with **snmpconf –g basic_setup**
- lets you set various alarms for disk, load, processes, etc

Issuing Commands with SET

- Use snmpset(1) to change agent's object values
- Effectiveness varies with agent, host, and MIB
- can only SET read-write and read-create objects

System Name Standards

```
$ snmptranslate -Td SNMPv2-MIB::sysName.0
SNMPv2-MIB::sysName.0
sysName OBJECT-TYPE
-- FROM       SNMPv2-MIB, RFC1213-MIB
-- TEXTUAL CONVENTION DisplayString
SYNTAX        OCTET STRING (0..255)
DISPLAY-HINT  "255a"
MAX-ACCESS    read-write
STATUS        current
DESCRIPTION   "An administratively-assigned name for this managed
node.  By convention, this is the node's fully-qualified
domain name.  If the name is unknown, the value is
the zero-length string."
::= { iso(1) org(3) dod(6) internet(1) mgmt(2) mib-2(1) system(1) sysName(5) 0 }
```

Check Hosts

```
$ snmpget -Ov freebsdtest SNMPv2-MIB::sysName.0
STRING: freebsdtest
$ snmpget -Ov centostest SNMPv2-MIB::sysName.0
STRING: centostest
$ snmpget -Ov debiantest SNMPv2-MIB::sysName.0
STRING: debiantest
$ snmpget -Ov gwtest SNMPv2-MIB::sysName.0
STRING: 2019testrouter.mwl.io
```

Using snmpset(1)

```
$ snmpset freebsdtest SNMPv2-MIB::sysName.0 s freebsdtest.mwl.io
SNMPv2-MIB::sysName.0 = STRING: freebsdtest.mwl.io
```

- command output comes from agent's response, confirming change
- I still don't trust it

```
$ snmpget -Ovq freebsdtest SNMPv2-MIB::sysName.0
freebsdtest.mwl.io
```

SNMP Proxies

- Send an OID through to another host or agent in snmpd.conf

proxy -v2c -c insecureRO localhost:1161 .1.3.6.1.4.1.12325

proxy –v2c –c insecureRO 127.0.0.2:161 .1.3.6.1.4.1.30155

AgentX

- Lets other programs register themselves as MIB providers
- MariaDB, Postgresql, Apache, NGINX, more
- can set AgentX socket permissions, listen to network, etc

Extending snmpd(8)

- Can run shell commands, scripts, external programs
- “extend” keyword is generic flexible MIB for simple commands

```
extend shoggoth /bin/echo "run away! run away!"
```

Running the Extension

```
$ snmpbulkwalk www1 nsExtendOutput1
NET-SNMP-EXTEND-MIB::nsExtendOutput1Line."shoggoth" =
     STRING: run away!
NET-SNMP-EXTEND-MIB::nsExtendOutputFull."shoggoth" =
     STRING: run away!
NET-SNMP-EXTEND-MIB::nsExtendOutNumLines."shoggoth" =
     INTEGER: 1
NET-SNMP-EXTEND-MIB::nsExtendResult."shoggoth" =
     INTEGER: 0
```

Real Work Extension

```
#extend shoggoth /bin/echo "run away! run away!"
extend files /bin/ls /tmp/files/
```

Real Extend: ls /tmp/files

```
$ snmpbulkwalk www1 nsExtendOutput1
NET-SNMP-EXTEND-MIB::nsExtendOutput1Line."files" =
     STRING: customer1
NET-SNMP-EXTEND-MIB::nsExtendOutputFull."files" =
     STRING: customer1
problem8
systemd.core
NET-SNMP-EXTEND-MIB::nsExtendOutNumLines."files" =
     INTEGER: 3
NET-SNMP-EXTEND-MIB::nsExtendResult."files" =
     INTEGER: 0
```

Other Queries

- net-snmp provides other information about the extension
- Don’t care what the files are, just how many?

```
$ snmpget -OvQ server1 NET-SNMP-EXTEND-MIB::nsExtendOutNumLines.\"files\"
105
```

Complex Extensions

- extend doesn’t have a shell, so call a script

```
extend files /usr/local/scripts/filecount.sh
```

```
#!/bin/sh
echo `/bin/ls /tmp/files | /usr/bin/wc -l`
```

Passthrough Scripts

- design your own MIB
- script must handle SET, GET, GETNEXT
- examples at net-snmp.org
- can do all sorts of things with scripts

- Most useless enterprise MIB of all: mine

```
http://http://www-old.michaelwlucas.com/TWP.mib
$ snmptable -v2c -c megadweeb snmp.mwl.io mwlbooks
```

View Agent Network

```
$ snmpnetstat www
Active Internet (tcp) Connections
Proto Local Address       Remote Address                    State   PID
tcp4  www.mwl.io.http     31.193.51.74.46125             TIMEWAIT     0
tcp4  www.mwl.io.http     broadband.actcorp..3073     ESTABLISHED     0
tcp4  www.mwl.io.https    broadband.actcorp..3081     ESTABLISHED     0
tcp4  www.mwl.io.https    ip-54-36-150-153.a.25228    ESTABLISHED     0
tcp6  www.mwl.io.https    broadband.bt.com.64597         FINWAIT2     0
…
```

- Can also view open sockets, routes, statistics, etc

Other SNMP Commands

- snmpdf(1) – disk usage
- fixproc(1) – command to fix error states
- snmpusm(1) – remotely manage users
- snmpdelta(1) – track changes

- And more, more, more!

Other SNMP things

- Access control – can restrict access to different parts of the MIB through View Based Access Control
- Traps – receive notifications via SNMP, send to programs or logs
- Monitoring Rule 1:
  - Whatever you choose to monitor, is the wrong thing

Questions and Answers?