System and Network Monitoring and Management With SNMP

John Sellens

GNAC Canada

jsellens@gnac.com

USENIX LISA-NT 99

July, 1999

Introduction and Goals

- An introduction to *practical* SNMP use
- Provide a simple overview or survey of what is possible
- “Industry acceptable practices”
- Some basic tool coverage
- Relatively independent of operating systems, etc.

What is SNMP?

- Simple Network Management Protocol
- Defined in Internet Standard 15, RFC 1157
- A method to query and control “devices” connected to a network
- Transaction based, uses UDP ports 161 and 162
- Implemented by virtually every device on an IP network now
- Used for almost all network management and monitoring now
- Less used for computer system management and monitoring, but also very useful in that area

SNMP Basics

- Two systems involved
  - Agent – the device on the network
  - Manager – sends queries to and receives responses from the agent
- Three goals
  - Easy and small to implement
  - Extensible to accomodate changing needs
  - System and architecture independent

Protocol Basics

- There are five types of SNMP messages
  - Get
  - GetNext
  - Set
  - Response
  - Trap e.g. coldStart, linkUp, linkDown, etc.
- Simple, short, easy to contruct, “unreliable” UDP datagrams

Some Simple Examples

```
% snmpget host1 pswd system.sysUpTime.0
system.sysUpTime.0 = Timeticks: (28946675) 3 days, 8:24:26

% snmpget localhost pswd system.sysContact.0
system.sysContact.0 = jsellens@uunet.ca

% snmpset localhost wrpswd \
      system.sysContact.0 s jsellens@gnac.com
system.sysContact.0 = jsellens@gnac.com

% snmpget localhost pswd system.sysContact.0
system.sysContact.0 = jsellens@gnac.com
```

Some More Simple Examples

```
% snmpget host1 pswd interfaces.ifTable.ifEntry.ifDescr.5 \
      interfaces.ifTable.ifEntry.ifPhysAddress.5 \
      interfaces.ifTable.ifEntry.ifOperStatus.5 \
      interfaces.ifTable.ifEntry.ifSpeed.5 \
      interfaces.ifTable.ifEntry.ifInOctets.5
interfaces.ifTable.ifEntry.ifDescr.5 = ed0
interfaces.ifTable.ifEntry.ifPhysAddress.5 = 0:60:97:93:4e:5b
interfaces.ifTable.ifEntry.ifOperStatus.5 = up(1)
interfaces.ifTable.ifEntry.ifSpeed.5 = Gauge: 10000000
interfaces.ifTable.ifEntry.ifInOctets.5 = 38675277
```

Even More Simple Examples

```
% env PREFIX=.iso.org.dod.internet.private.enterprises.ucdavis \
      snmpget localhost pswd disk.diskPath.3 \
      disk.diskUsed.3 disk.diskAvail.3 disk.diskTotal.3 \
      disk.diskPercent.3
enterprises.ucdavis.disk.diskPath.3 = /tmp
enterprises.ucdavis.disk.diskUsed.3 = 33
enterprises.ucdavis.disk.diskAvail.3 = 28863
enterprises.ucdavis.disk.diskTotal.3 = 31408
enterprises.ucdavis.disk.diskPercent.3 = 8

% snmpwalk localhost public
. . . lots of output . . .
```

SNMP Variables, MIBs, and OIDs

- Every object is a variable, with a hierarchical name

  e.g. iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0
- A "Management Information Base" is a textual description of a set of SNMP variables and the possible values
- An "Object Identifier" is the numeric equivalent

  e.g. 1.3.6.1.2.1.1.3.0
- You can typically query by either name (full or partial) or OID
- MIB-II (RFC 1213) is expected on every device
- The final number is (usually) an index into a table of values

  e.g. the interface or disk volume tables

SNMP Security

- In SNMP v1, interactions are governed by shared secrets knows as “community strings” - usually a “read” and a “write”
- This is not a “high-security” mechanism
  - Everything is clear text, and it’s all or nothing
  - No challenge response, no one time passwords
    - But this is a result of the typical intended use of the protocol i.e., automated, not commands initiated by humans at a keyboard
- v2 and v3 improve things, as does the “View-Based Access Control Model” (RFC2275), but are (currently) less used

Device and OS Specific Information

- Most vendor SNMP agents also implement private enterprise MIBs
  - Often have to resort to reading the raw MIBs to understand
- e.g. Cisco has an environmental MIB, NT has domain and DHCP MIBs, NetApp has disk-related MIBs
- Different vendors are better or worse, some information is hard to find and/or use
- But the vendor MIBs often have the most worthwhile variables

SNMP Applied: Monitoring

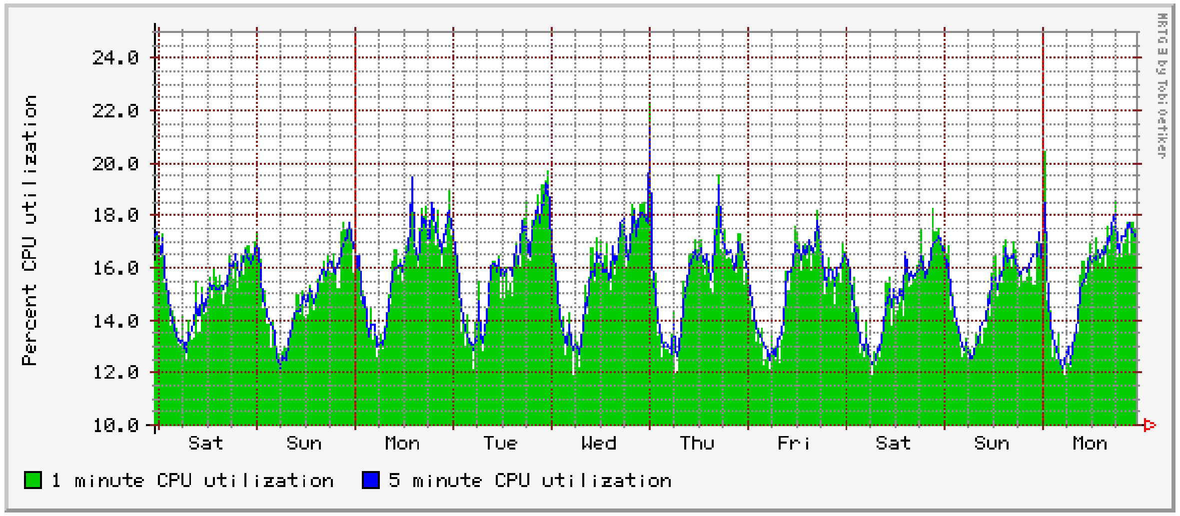
- Monitoring is for trends and exceptions
- Poll or Trap
- Collect history for analysis and execption identification
- Accounting or session data, traffic or activity levels
- Ripe for automation
- Have tools ready for investigation when needed
- Can do a lot with only the standard MIBs

Monitoring: How to Notice Problems?

- Catch traps
  - as long as the agent will trap what you want
  - and as long as you don't lose the trap packet
- Periodic poll
  - put the last polled value in a file, complain if changed
  - some variables are "last change time" which is convenient for noticing transient changes
  - Polling is a nice backup mechanism for traps
- Perl/VB/Tcl script or large commercial application
- Some sort of notification mechanism

Monitoring: How to Watch Trends?

- Some sort of historical database, and some sort of visualization
- MRTG (and its successor Cricket) is the way to go
- Very easy to track just about anything, and low overhead
- Favorite things to graph: memory, CPU, disk, network, uptime, users, mail waiting to be read, queue lengths, . . .



Monitoring: What?

- State changes e.g. network interface up/down
  - Or last change time, which is easier to notice when flapping
- Threshold limits e.g. disk more than 99.99% full
  - Queue sizes, traffic levels, users, web hits, . . .
  - Also watch for minimum thresholds
    - e.g. less than 3 users in the daytime might be a problem
- Directional changes e.g. uptime should always be increasing
- Security related stuff – # users in user database, failed authentications, etc.

SNMP Applied: Management

- Management is for manipulation and administration
- Remote configuration and manipulation
- Device configuration backups
- Kick unruly users off dialup ports
- More often triggered manually
- Some tasks are well automated e.g. config backups

Management: How?

- Depends largely on vendor-specific MIBs and implementation
- And often the vendor's applications or OpenView addons
- But you can accomplish a lot with a few simple SNMP gets and sets
  - Usually best if wrapped by a script for ease of use
- Change management and version control are problematic
  - Consider doing periodic config file backup and doing revision control on that

Management: What?

- Really depends on the agent's capabilities and the device type
- Networking devices:
  - Enable/disable/configure ports on routers or switches
  - Some routing tweaks e.g. weights, gateways
- Computers:
  - Typically fewer things that you can change on the OS
  - The NT MIBs imply a reasonable level of remote control
- Like any remote manipulation, don't shoot yourself in the foot
- Prediction: this will get better and be more effective soon

Basic SNMP Tools - 1

- A basic tool set for interactive or script use
- I'm not counting commercial applications as "basic" tools
- Primarily UNIX in origin, but also on NT (mostly)
- Not surprisingly, these tools happen to be freely available
- Current OS releases typically include an agent, and perhaps some tools

Basic SNMP Tools - 2

- UCD / CMU SNMP
  - Command line tools in C for manager and agent
  - Implements standard MIB-II, Host Resources MIB, plus the “ucdavis” MIB
  - Extensible - can monitor anything
  - libsnmp for writing applications
  - UCD agent not (yet) available for Windows
  - Better than “snmputil” from the NT reskit

Basic SNMP Tools - 3

- Scotty – Tcl Extensions
  - The Scotty package contains the Tnm Tcl extension, and the Tkined interactive network editor application
  - Tnm provides a very good library of SNMP-related functions, written in Tcl
  - scotty is a Tcl shell that includes Tnm
  - Very nice, well documented, worth learning Tcl for
  - version 3 beta works under Windows

Basic SNMP Tools - 4

- Perl
  - Simon Leinen's SNMP_Session.pm provides the basic SNMP functions in a native Perl module
  - Works, but is currently somewhat rudimentary
  - No support for MIBs, so everything is specified as an OID
  - Mike Mitchell's SNMP_util.pm provides convenient covers for some of the SNMP_Session.pm functions, and a labelling mechanism for SNMP variables
- Windows-specific tools - I'm not familiar enough to say

Basic SNMP Applications - 1

- There are many applications, commercial and non-commercial, that use SNMP
- These are typically for network monitoring and management, though they usually have some flexibility
- What follows is a quick overview of some “well known” applications

Basic SNMP Applications - 2

- MRTG – Multi Router Traffic Grapher
  - An AMAZINGLY useful tool by Tobias Oetiker – you need MRTG (or Cricket below)
  - Generates graphs of almost anything over time, using a simple config file, and makes them available through a web server
  - Typically used to monitor traffic counts on routers and other network devices, but can graph anything e.g., temperature, uptime, messages in mail queue, disk usage, etc.
  - Very widely used, lots of examples on the web site
  - Works on Windows NT and UNIX

Basic SNMP Applications - 2

- MRTG Successors
  - MRTG is not as fast as one would like it to be, and if you're monitoring lots of things, you can generate a non-trivial load
  - RRD Tool is Oetiker's next generation tool – Round Robin Database tool
    - major speed improvement over the MRTG engine
  - Cricket by Jeff Allen is a high performance replacement for MRTG that uses RRD Tool as it's engine
    - easy, tree-structured configuration, flexible
    - very fast
  - MRTG is more mature, but Cricket is getting there

Basic SNMP Applications - 2

- Other Freely Available SNMP Applications
  - NOCOL/NetConsole (Network Operation Center On-Line) is a system and network monitoring tool that uses SNMP for some of its polling
  - Big Brother has similar goals but approaches them differently
- Some Commercial SNMP Applications
  - Typically for mapping, monitoring and management, with lots of graphics
  - HP OpenView - very popular, with lots of plug-ins
  - Cabletron Spectrum – an OpenView alternative
  - Netcool from Micromuse
    - Similar to nocol, but far more sophsticated, fewer graphics

Summary

- If you're not using SNMP yet, start now
- The state of the art is advancing
- More and more SNMP tools, more and more SNMP applications
- Better security and control models
- Modest collection of SNMP pointers at:

  http://www.generalconcepts.com/resources/snmp/
- Questions?