SNMP
Management and monitoring of small networks

Marcus Wilhelmsson
marcus.wilhelmsson@lnu.se

Contents

- Introduction to SNMP
- Versions of SNMP
- Configuration
  - Communities
  - SMI, MIBs, OID
  - Polling
  - Traps
- SNMP agents
- Network equipment
- Servers

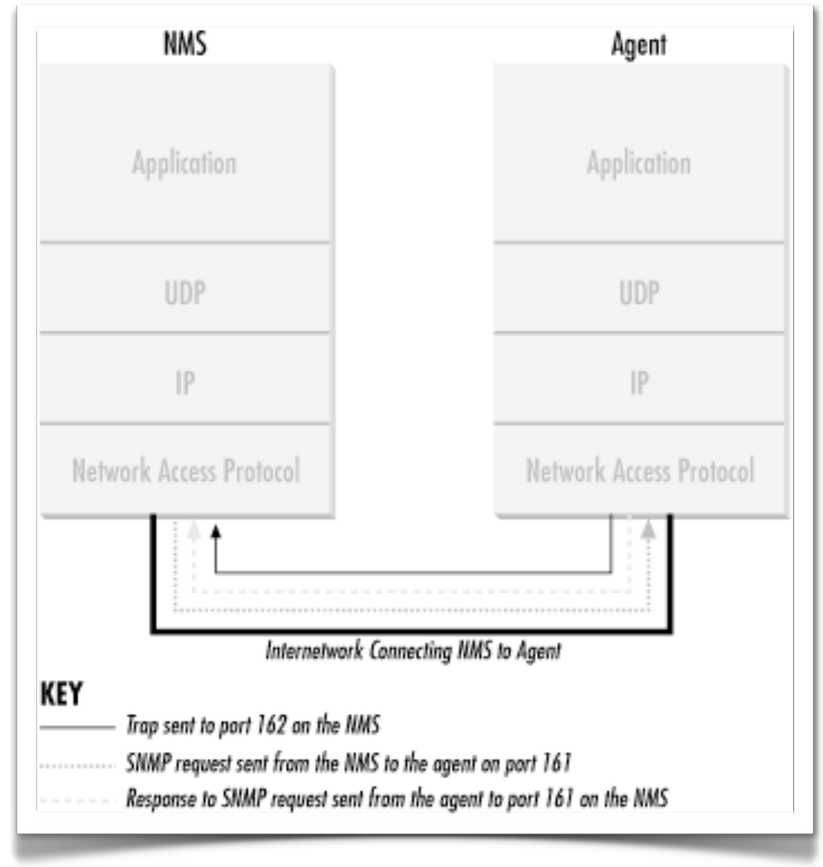
Introduction to SNMP

- A collection of simple operations for communicating with SNMP capable equipment and units
- Turn an interface on a router on and off
- Monitoring the traffic on an interface
- Monitoring temperatures
- Send a warning if the temperature exceeds a threshold

- Often associated with network equipment such as routers and switches, but can be used for almost any network capable equipment

Communication

- Connunication via UDP
- Works well for collecting information
- Traps, which are only sent once, are less suited for UDP



- UDP gives you and advantage since it's overhead is very low
- TCP in an already congested network is a bad idea

- Uses UDP port 161 for polled information and TCP port 162 for traps

SNMPv1

- First version released, defined through RFC1157 (not considered obsolete)
- The security is based on communities
- There are three standard communities: read-only, read-write and trap
- Since this version of SNMP is obsolete it's not used, although it can be present on older equipment
- Can be used over other protocols than UDP, for example CLNS, DDP and IPX

SNMPv2c

- Works a lot like SNMPv1
- If a poll is sent to a monitored unit, but the poll contains fault, this will be handled correctly
- Improved security
- Everything except the destination in the packet is encrypted

SNMPv3

- Above else improved security
- Message integrity
- Authentication
- Encryption
- Greater possibilities to use SNMPv3 for remote configuration of units

SNMP communities

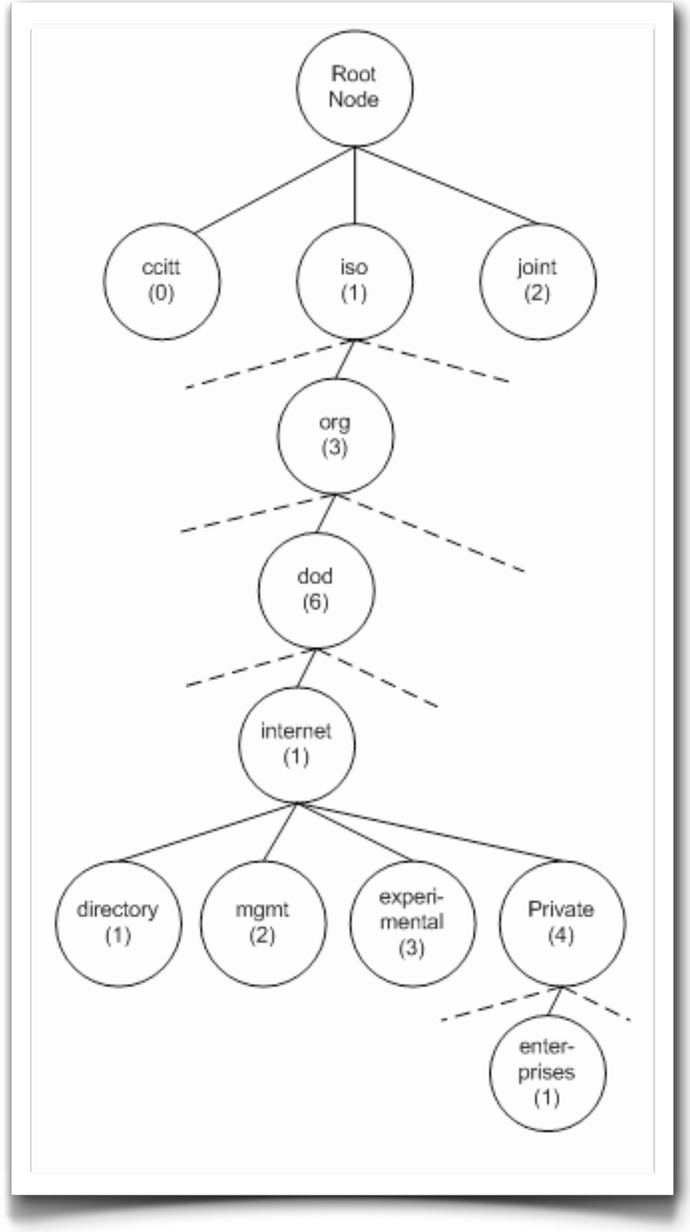
- A relation between the manager and the SNMP agent
- There are three communities handling different activites
  - Read-only - Used to read values from polling
  - Read-write - Used to read values from polling and to modify values
  - Trap - Receive traps from agents
- Change the standard community names for improved security
- To get secure authentication and transfer you should use SNMPv3
- The community name should be treated with the same precautions as a password

SMI - Structure of Management Information

- Name
  - Called OID (Object IDentifier)
  - Numerical and readable
- Type and attribute
  - Machine/OS independent
- Coding
  - Contains information about how the information is coded for sending over for example Ethernet

OID

- Objects that can be called via SNMP are organized in a tree
  - In this case 1.3.6.1.4.1 if you follow the “branches” on the tree
- Anyone can register numbers under “enterprise” for their own units
- Cisco has 1.3.6.1.4.1.9 or iso.org.dod.internet.private.enterprise.cisco
- This widens the possibilities for corporations and manufacturers since they can add their own custom SNMP OIDs



MIB-2

- MIB-2 contains standard objects that most SNMP capable units have support for
- Contents (you can read the full description in RFC1213)
  - system (1.3.6.1.2.1.1)
  - interfaces (1.3.6.1.2.1.2)
  - at (1.3.6.1.2.1.3)
  - ip (1.3.6.1.2.1.4)
  - icmp (1.3.6.1.2.1.5)
  - tcp (1.3.6.1.2.1.6)
  - udp (1.3.6.1.2.1.7)
  - egp (1.3.6.1.2.1.8)
  - transmission (1.3.6.1.2.1.10)
  - snmp (1.3.6.1.2.1.11)

SNMP commands

- PDU (Protocol Data Unit)
  - get
  - getnext
  - getbulk
  - set
  - getresponse
  - trap
  - notification
  - inform
  - report

get

- Initiated by the NMS (Network Monitoring System)
- The agent responds with get response
- Query: OID 1.3.6.1.2.1.1.6.0
- Answer: system.sysLocation.0 = “Building 18, cabinet 2”

getnext

- Queries the agent about a group of values in a MIB
- get ang getresponse are generated for each separate value in the group
- This can be seen as a type of search in a MIB
- For example, you can send a query containing “system”. Then you’ll get an answer for all the values in “system”.
  - system.sysDescr.0 = “Cisco IOS Software...”
  - system.sysObjectID.0 = OID: enterprises.9.1.19
  - system.sysUpTime.0 = TimeTicks: (27210723) 3 days, 3:35:07.23
  - system.sysContact.0 = “”
  - system.sysName.0 = “cisco.hik.se”
  - system.sysLocation.0 = “Building 18, cabinet 2”
  - system.sysServices.0 = 6

getbult

- get can be used to try to fetch information about more than one MIB object at a time, although the size of the answer is limited
- getbulk does the same thing, except it allows answers that aren't complete

set

- The NMS sends “set” and tries to change sysLocation to “Kalmar”
- The agent receives the set command and determines of the NMS has permissions to change sysLocation
- When all checks have been done the agent sends either a “getresponse” with an error code if the request was denied or if everything went OK it sets sysLocation and responds with “noError”

SNMP traps

- Sent from the agent to the NMS
- Sent when something happens evaluated by certain rules on the agent
- No confirmation of the trap actually reaching the NMS
- The meaning of a trap is identified by a number within the trap message
- The following trap numbers exist
  - coldStart(0) - The agent has been restarted, all variables reset
  - warmStart(1) - Reinitialization of the agent, all variables are still set
  - linkDown(2) - A network interface on the unit is down
  - linkUp(3) - A network interface on the unit is up
  - authenticationFailure(4) - Someone has tried to connect and send a commands to the unit with a faulty community string
  - egpNeighborLoss(5) - One of the units EGP neighbors is down
  - enterpriseSpecific(6) - Indicates that the trap is enterprise specific, i.e. a trap defined by the manufacturer and located under private-enterprise in the SMI object tree

Enterprise specific traps

- Example of an enterprise specific trap

```
rbmsOutOfSpace TRAP-TYPE
    ENTERPRISE    rdbmsTraps
    VARIABLES     {rdbmsSrvInfoDiskOutOfSpaces }
    DESCRIPTION
        "An rdbmsOutOfSpace trap signifies that one of the database
        servers managed by this agent has been unable to allocate
        space for one of the databases managed by this agent. Care
        should be taken to avoid flooding the network with these traps."
    ::=2
```

- Oracle, for example, sends their databases with an SNMP agent

SNMP agents

- Must be present on all SNMP capable devices
- Consists of software on the unit being monitored
- Specially written software on routers, switches, etc.
- Specially written of general software on servers and other computers

SNMP agents

- Common parameters
  - sysLocation - Where the unit is located
  - sysContact - Mail or other contact info
  - sysName - Name of the unit (FQDN)
  - Community strings for read-write, read-only and (usually) trap
    - Default is private, public and trap
  - Trap destination - NMS to send the traps to

Net-SNMP

- Program suite for SNMP on computer
- Has more features than the built in SNMP support in Windows
- Support for Windows, Linux, Mac OS X, etc.
- Open Source under BSD license

MIBs

- Bytesphere
- http://www.oidview.com/mibs/detail.html

- MIB Search
- http://www.mibsearch.com/

- Usually provided by the unit manufacturer

Demo