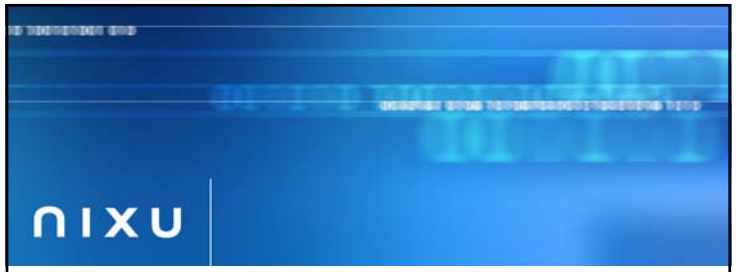


SNMP and Network Management

Nixu Ltd

nixu

Contents

- Network Management
- MIB naming tree, MIB-II
- SNMP protocol
- SNMP traps
- SNMP versions

nixu

Network management

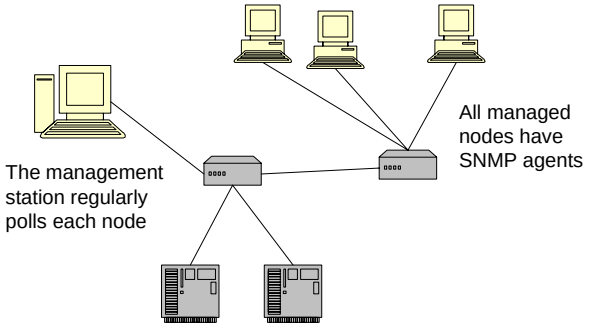
- When you have 100s of computers in a network or are running a backbone, you are almost always interested about the state of the network nodes and want to know about the traffic flows
- You might also want to change the parameters that control the nodes
- Network management requires a protocol which should:
  - Not generate too much load on the network and nodes
  - Be affected as little as possible by congestion, packet loss, outages etc.
  - Report meaningful information about the network and its nodes
  - Not block the management or managed nodes

nixu

Network Management with SNMP

- There are four defined components:
  - Network elements (routers, hosts, printers etc) have a small server program called **agent**
  - **Management** station queries network elements for information
  - Simple Network Management **Protocol** is defined in RFC-1157
    - Transports the data
  - Management Information Base (MIB) **defines** the information served by SNMP agents
    - The data types are independent of the protocol

…Network Management with SNMP



5

The Agent

- The agent is a UDP server that receives SNMP queries from the management station and retrieves information from the system for the reply
- Sources of information
  - Operating system tables
  - Network interfaces
  - Software (servers)
- The agent implements the description in the MIB
- Commercial and freeware implementations
- Typically an agent comes with the operating system and implements the standard MIB-II, additional MIBs can be implemented by adding modules

6

The Management Station

- The network management station has software that is configured to query various agents in network elements for information
  - Received information is usually stored in a database for long term analysis
  - The network is often displayed graphically
- The management software is configured with the addresses of the network elements to be managed and what particular information to fetch from that element
  - Reading everything is usually not efficient
- Typically commercial of free software running on a workstation, often has several modules for separate tasks
- The management station software reads the MIB descriptions

7

The Management Software Modules (typical)

- Data collection module
  - Collect data in real time
  - Thin out old data so that needed information is kept with acceptable loss of accuracy
- Data analysis module
  - Display network as a picture
  - Generate alarms
  - Show graphs
  - Enable the operator to look at different aspects of the data, change resolution, time, combine information etc.

8

MIB Descriptions (files)

- Specifies the data to be excanged
- Variables can be queried and set by the manager
- Variables are named using Object IDentifiers (OIDs), a hierarchical scheme that is unlimited in expansion, e.g. iso.org.dod.internet.mgmt.mib-2.
- There is a branch in the naming tree for private enterprises (usually manufacturers of network hardware) to locate their own MIBs.
- The management software uses the MIB files to read descriptions to the data
- The administrators read the MIB descriptions to understand the data

MIB example

- Here is a definition for a single data element in ASN.1 (Abstract Syntax Notation One) macro language

```
sysUpTime OBJECT-TYPE
    SYNTAX      TimeTicks
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The time (in hundredths of a second) since
             the network management portion of the sys-
             tem was last re-initialized."
    ::= { system 3 }
```

- This element's OID is iso.org.dod.internet.mgmt.mib-2.system.sysUpTime
  – or 1.3.6.1.2.1.1.3

MIB Data Types

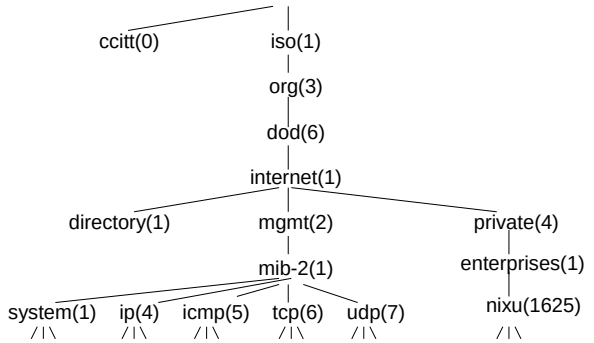
- Most common types
  – Integer, usually signed 32 bit
  – Octet String, a sequence of bytes
  – Gauge, can go up and down within a range
  – Counter, grows until it rolls to zero at max value (2^32)
  – TimeTicks, time measure in hundredths of seconds
- More complex data types can be constructed using sequence and union
- Data can also be stored in tables
  – "getnext" is a very powerful tool for reading tables

Reading data

- Integers and octet strings are useful for relatively static data
- Gauge can be for example the CPU load as percents
- Counter is especially useful for collecting traffic statistics
  – It grows only up, never down
  – At the max value it rolls around
  – To obtain a correct reading the counter should be read several times before it rolls around
    – Be aware of the maximum volume
  – The management station is in charge of reading the counter
  – The agent does not have to collect statistics, just keep one variable up to state

MIB naming tree

- Every SNMP variable has a place in the global MIB tree



13

Example: MIB-II

- The Internet MIB-II database (RFC-1213) defines a MIB which contains most information needed to manage an Internet network element
- iso.org.dod.internet.mgmt.mib or 1.3.6.1.2.1 is the name of the MIB
  - For example iso.org.dod.internet.mgmt.mib-2.udp.udpInDatagrams is a counter of the number of datagrams the network interface has delivered to the user programs in that network element.
  - iso.org.dod.internet.mgmt.mib-2.system.sysName is a string for domain name for the network element, while the IP address for the host is held in the iso.org.dod.internet.mgmt.mib-2.ip.ipAddrTable table (one host may have many addresses).
- The MIB-II database has also variables for IP, TCP, ICMP etc. statistics.

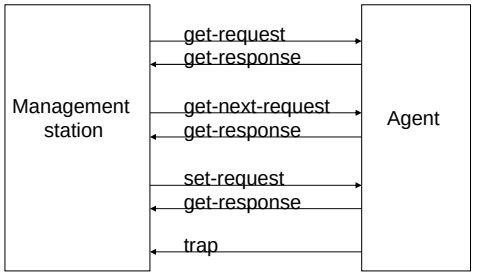
14

SNMPv1 protocol

- UDP-based protocol, defined in RFC-1098
- Agent listens to UDP port 161, management station to port 162 for traps
- Five message types
  - get-request – fetching the value of some variables
  - get-next-request – fetch the value of next OID (useful)
  - set-request – set the value of some variables
  - get-response – return message from queries above
  - trap – notify the manager
- Data is encoded in BER (Basic Encoding Rules) format that is derived from ASN.1 description

15

SNMP messages



16

Traps

- A SNMP agent can send a trap to the SNMP manager
  - Trap is sent when something happened in the agent that the manager may want to know about
  - There is no replay, which means that traps are not reliable
  - Traps should be considered an informational addition to the normal get -sequences of collecting the management information
- Six pre-defined traps, plus one vendor specific
  - ColdStart
  - WarmStart
  - linkDown
  - linkUp
  - authenticationFailure
  - egpNeighborLoss
  - enterpriseSpecific

SNMPv1 Message Format

version	community	PDU type (0-3)	request ID	error status (0-5)	error index	name	value	name	value	...

PDU type (4)	enter-prise	agent addr	trap type (0-6)	specific code	time stamp	name	value	...

- Message is encapsulated in a UDP/IP datagram
- Community is a character string (a cleartext password between the manager and agent)
- PDU and ID fields identify the message

…SNMPv1 Message Format

- Name is the OID identifier
- Value is actually:

tag	length	value

  - The tags are part of the BER encoding and derived from the ASN.1 definitions
  - Note that this encoding allows encoding any bit pattern of any length
- The value can be a sequence of values

SNMP freeware tools

- Several freeware packages are available that have both an agent and command line tools
- The agent can be usually easily modified to attach additional functionality for own MIBs
- The (command line) tools usually correspond to the SNMP protocol actions
  - Additionally often included the useful “snmpwalk” tool which transverses an OID branch of the MIB tree
- Some user interface issues
  - Password usually required (usually “private” works)
  - “get” might want that the OID ends in .0
  - The initial 1.3.6.1 can sometimes be dropped from the OID

SNMP and security

- V1 has no real security in the protocol
  - Clear text password that is usually “public” for reading and “private” for writing
- V2 has some security features
- V3 has cryptographic integrity and confidentiality protection for the protocol
  - User-based Security Model (USM)
- Weaknesses have been found in the SNMP software implementations like in all other commonly used server software
- In practice:
  - SNMP should not be used in untrusted networks
    - And blocked in the firewall
  - Agent passwords should be changed, especially the set password
  - IPSec may be used to protect the traffic
    - TSL and SSH are TCP only, SNMP uses UDP, thus IPSec

21

SNMPv2

- Extended version of the original SNMP
- Specification in 1993
  - RFC1901-1908
- Enhanced the protocol with new features
  - GETBULK especially useful
- Security enhancements
  - Can provide authentication and privacy between managers and agents
- Many products have some support for some SNMPv2 functionalities
  - Usualy the Community based SNMPv2

22

SNMPv3

- RFC 3410-3418
- An Internet Standard
- A new framework (architecture) for processing the messages
- Also finally provides the lacking security features
  - Confidentiality, message integrity, authentication
  - A possibility to manage fine-grained access to agents
- Not widely deployed yet

23

CMIP

- Common Management Information Protocol
- The OSI protocol comparable to SNMP
- Addresses many of the shortcomings of SNMP, is also more complicated and requires more resources.
- In many cases agents might be too heavy for practical use as compared to SNMP.
- Currently should be considered only if network management is of serious importance.
  - E.g. the telecommunications industry uses CMIP

24

Network Management in action

- Network manager software is configured with the network layout and the MIBs of different network elements.
- Network manager regularly queries the network elements and displays the information to human supervisor.
- When the management software finds something wrong, for example a router does not reply to queries for a while, the software alerts the human supervisor.
- Network manager may set variables in a network element, e.g. the address of a DNS server.
- A network element may send a trap, for example a printer may signal that it is out of paper.

25

Practical network management

- SNMP and technology are part of the story
- In real life it is important to remember that the measurement is not the reality
  - I.e. always suspect the tool
- Monitoring a network requires experience and understanding
  - What is the difference between monitoring the number of packets or traffic volume
  - How to find the bottlenecks inside a router
- Generally the job should be boring
  - Mostly monitoring and tuning the performance
- Too many panic events mean that something is seriously flawed

26

The FCAPS Model

- Fault Management
- Configuration Management
- Accounting
- Performance Management
- Security Management

- Part of Telecommunications Management Network (TMN) standard from ITU
- An useful check list

27

Deploying SNMP to an existing Network

- Activate agents at the nodes to be monitored
  - Install software if needed, set passwords
  - Usually routers and switches
- Configure the management station
  - Decide which OIDs to monitor
    - For a router a table of interfaces
    - How often to poll (1-30 s)
    - Install additional vendor MIBs
- Enjoy the show
  - Learn to interpret the data and behavior of the devices
  - Produce nice graphs and summaries for the management

28

Writing your own MIB

- Get your enterprise MIB address from IANA
- Understand the properties of the phenomenon to be monitored or controlled
  – Router, webcam, soda vending machine...
- Describe the data to be transferred in terms of single variables and tables
- Write the MIB definition in ASN.1 language
- Select a module from an existing SNMP agent and rewrite it to implement the MIB
- Feed your MIB file to a management software and test it

29

Summary

- MIB definition file describes the data that can be monitored
- An agent implements the MIB in software
  – Usually the standard MIB-II and other MIBs
- The management station queries the agent and summarizes the data for the user

30