

Network Management

Jaakko Kotimäki

Aalto University

11.10.2011

Outline

Introduction

SNMP architecture

Management Information Base

SNMP protocol

Network management in practice

Niksula

Network Management

“When you have 100s of computers in a network or you are running a backbone, you are almost always interested about the state of the network nodes and want to know about the traffic flows.”

– Timo Kiravuo

Using the network to manage the network

- ▶ 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

Network management tasks

- ▶ ITU-T Telecommunications Management Network recommends FCAPS network management model
- ▶ A useful check list:
 - ▶ Fault Management
 - ▶ Configuration Management
 - ▶ Accounting
 - ▶ Performance Management
 - ▶ Security Management
- ▶ OSI CMIP (Common Management Information Protocol) implements this as a single protocol

Outline

Introduction

SNMP architecture

Management Information Base

SNMP protocol

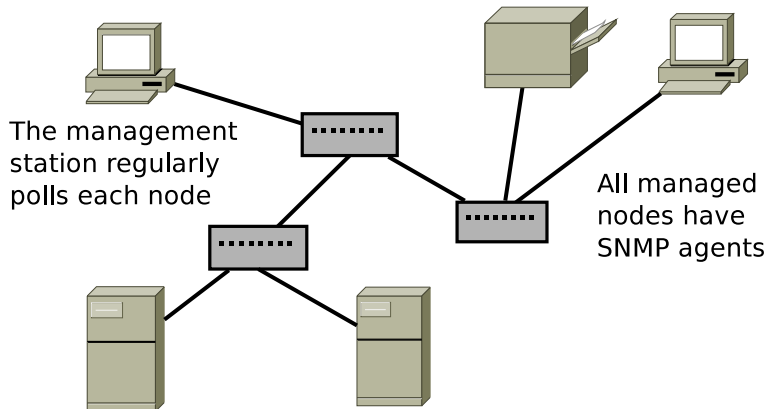
Network management in practice

Niksula

Network Management with SNMP

- ▶ Simple Network Management Protocol (SNMP)
- ▶ IETF's network management protocol and architecture
- ▶ Four defined components:
 - ▶ Network elements have a small server program called **agent**
 - ▶ **Management station** queries network elements for information
 - ▶ Simple Network Management **Protocol** for exchanging information between agents and management station
 - ▶ Management Information Base (**MIB**) defines the information given by SNMP agents

SNMP architecture



SNMP Agent

- ▶ The agent is a server on the managed device that collects information of the system
- ▶ Sources of information:
 - ▶ Operating system tables
 - ▶ Network interfaces
 - ▶ Software (servers)
- ▶ The agent replies to SNMP queries from the management station
- ▶ Commercial and freeware implementations
- ▶ Typically an agent comes with the operating system

Management station

- ▶ Typically commercial or free software running on a workstation
- ▶ The network management station software queries various agents in network elements for information
- ▶ The management station software reads the MIB descriptions
- ▶ The management software has addresses of the managed network elements
- ▶ The management software knows what particular information to fetch from the element

Outline

Introduction

SNMP architecture

Management Information Base

SNMP protocol

Network management in practice

Niksula

MIB descriptions

- ▶ The administrators read the MIB descriptions to understand the data
- ▶ The management software keeps the MIB descriptions in files for reference
- ▶ MIB description specifies the data on the managed equipment as variables
- ▶ Variables can be queried and set by the manager
- ▶ Variables are named using Object IDentifiers (OIDs), a hierarchical scheme, e.g. `iso.org.dod.internet.mgmt.mib-2`
- ▶ MIB descriptions are written using ASN.1 (Abstract Syntax Notation One)

MIB example

- ▶ The OID of the element is 1.3.6.1.2.1.1.3 – or
iso.org.dod.internet.mgmt.mib-2.system.sysUpTime

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 system was last re-initialized."

::= { system 3 }

MIB datatypes

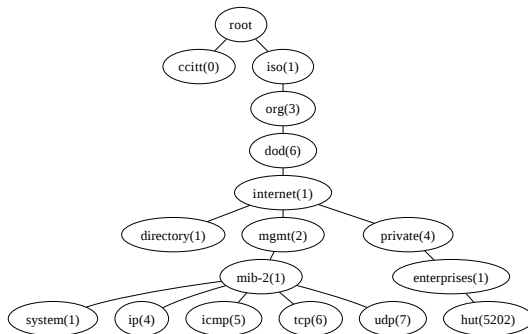
- ▶ Most common types
 - ▶ Integer, usually signed 32 bit
 - ▶ Octet String, a sequence of bytes
 - ▶ Gauge, can go up and down within a range
 - ▶ Counter, grows until it rolls to zero at max value (2^{32})
 - ▶ TimeTicks, time measure in hundredths of seconds
- ▶ Data can also be stored in tables
-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

Using MIB datatypes

- ▶ 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 and at the max value it rolls around
 - ▶ The counter should be read several times before it rolls around to obtain a correct reading
 - ▶ The management station is in charge of interpreting the counter and collecting statistics
 - ▶ The agent just keeps the current state of variables

MIB naming tree

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



Example: MIB-II

- ▶ The Internet MIB-II database (RFC-1213) defines commonly used MIB variables for Internet network elements
- ▶ Standard protocol MIBs start with 1.3.6.1.2.1 (iso.org.dod.internet.mgmt.mib-2)
 - ▶ The same management software can be used for monitoring network devices by different vendors
 - ▶ E.g. the IP address for the host is held in the mib-2.ip.ipAddrTable table (one host may have many addresses)
- ▶ Enterprise MIBs start with 1.3.6.1.4.1 (iso.org.dod.internet.private.enterprises)
 - ▶ Manufacturers (or anyone) can define their own MIB descriptions

Writing your own MIB

- ▶ Get your enterprise MIB address from IANA
- ▶ Understand the properties of the phenomenon to be monitored or controlled
 - ▶ webcam, vending machine, toaster...
- ▶ 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

Outline

Introduction

SNMP architecture

Management Information Base

SNMP protocol

Network management in practice

Niksula

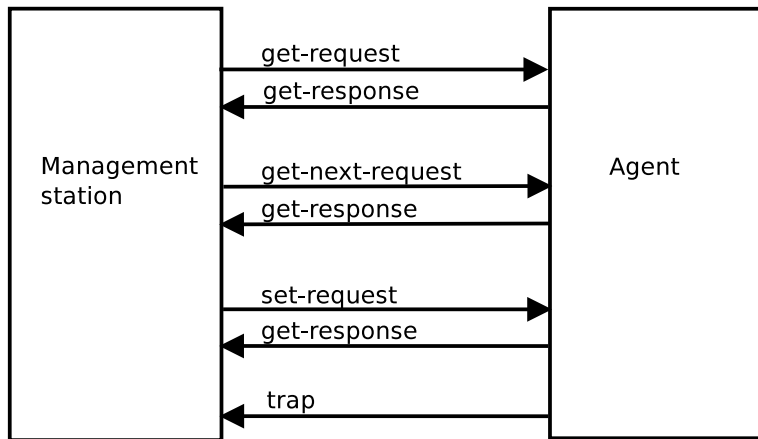
SNMP protocol

- ▶ Works on top of UDP
- ▶ Agent listens port 161
- ▶ Management station listens port 162 for trap messages
- ▶ Simple get/set protocol: device is managed by setting variables
- ▶ Messages are coded with ASN.1
- ▶ Three major versions

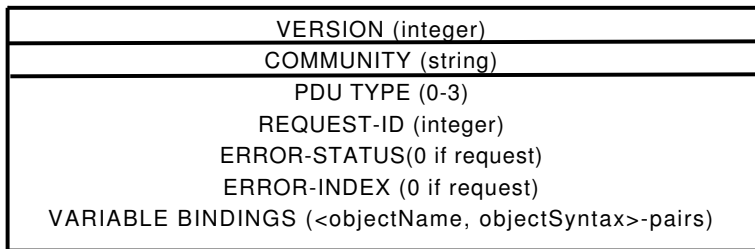
SNMPv1

- ▶ Defined in RFC-1157 (1990)
- ▶ 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

SNMPv1 messages



SNMP message format



SNMP message format

- ▶ Version is the version number of the protocol
- ▶ Community is the common name for managed are and it can be used as a clear-text password between the manager and agent
- ▶ PDU Type tells the message type
- ▶ Request ID is an identifier for separating the requests
- ▶ Error Status and Error Index are used in get-response to indicate problems e.g. noSuchName or readOnly.
- ▶ Variable Bindings is a list of object name-value pairs

SNMPv1 Traps

- ▶ A SNMP agent can send a trap to the SNMP manager when something happened in the agent that the manager wants to know about
- ▶ There is no reply, which means that traps are not reliable
- ▶ Traps should be considered an informational addition to the normal get -sequences of collecting the management information

SNMPv1 Traps

VERSION (integer)
COMMUNITY (string)
PDU TYPE (4=trap) ENTERPRISE AGENT ADDRESS TRAP TYPE (0-6) SPECIFIC CODE TIMESTAMP VARIABLE BINDINGS

SNMPv1 Traps

- ▶ PDU Type = 4 = trap
- ▶ Enterprise is the OID of the enterprise
- ▶ Agent Address is the address of the device
- ▶ Trap Type, six pre-defined traps, plus one vendor specific
 - ▶ ColdStart
 - ▶ WarmStart
 - ▶ linkDown
 - ▶ linkUp
 - ▶ authenticationFailure
 - ▶ egpNeighborLoss
 - ▶ enterpriseSpecific
- ▶ Specific Code some enterprise specific trap code
- ▶ Timestamp is the time since last initialization of the network

SNMPv2

- ▶ Extends the original SNMP version
- ▶ Multiple subversions: v2, v2c and v2u, several RFCs each
- ▶ New features:
 - ▶ GetBulkRequest – transfer potentially large amount of data, efficient for especially large tables
 - ▶ InformRequest – implements acknowledged trap
 - ▶ Trap – format changes
- ▶ Security enhancements in v2u, not widely used

SNMPv3

- ▶ RFC 3410-3418 (2002), an Internet standard STD0062 (2004)
- ▶ A new framework (architecture) for processing the messages
- ▶ Provides important security features:
 - ▶ Confidentiality, message integrity, authentication
- ▶ Not widely deployed yet

SNMP and security

- ▶ V1 has no security in the protocol
- ▶ V2 has some security features, not widely used
- ▶ V3 has cryptographic integrity and confidentiality protection for the protocol
 - ▶ User-based Security Model (USM) RFC-3414
- ▶ New:
 - ▶ RFC-5592 Secure Shell Transport Model for SNMP, 2009
 - ▶ RFC-5953 TLS Transport model for SNMP, 2010

SNMP and security in practice

- ▶ SNMP should not be used in untrusted networks
 - ▶ And blocked in the firewall
 - ▶ Better yet, in its own virtual LAN (VLAN) in a private network
- ▶ IPSec may be used directly to protect the SNMP traffic that uses UDP

Outline

Introduction

SNMP architecture

Management Information Base

SNMP protocol

Network management in practice

Niksula

SNMP freeware tools

- ▶ Several freeware packages are available that have both an agent and the command line tools for management
- ▶ The (command line) tools usually correspond to the SNMP protocol actions e.g. `snmpget`
 - ▶ Additionally often included the useful `snmpwalk` tool which traverses an OID branch of the MIB tree using the get-next-response
- ▶ DEMOS!

Network Management in action using SNMP

- ▶ When the management software finds something wrong, e.g. one of the power supplies of the switch fails, the management software sends an email alert
- ▶ Network manager may set variables in a network element, e.g. changing the network (VLAN) of a switch port to another
- ▶ A network element may send a trap, for example a printer may signal that it is out of paper

Practical network management

- ▶ Network management is about monitoring and tuning performance
 - ▶ How to locate performance bottlenecks
 - ▶ Planning for future needs
- ▶ Sometimes it is about disaster recovery
 - ▶ Devices break or an ignorant user causes problems for example by accidentally creating a loop to the network
 - ▶ Denial of Service attacks
 - ▶ Hunting down infected or misbehaving devices e.g. laptops or network flooding computers

Deploying SNMP to a network

- ▶ Activate agents at the nodes to be monitored
- ▶ Configure the management station
 - ▶ Decide which OIDs to monitor
 - ▶ For a router a table of interfaces
 - ▶ How often to poll
- ▶ Enjoy the show
 - ▶ Learn to interpret the data and behavior of the devices
 - ▶ Produce nice graphs and summaries for the management

Outline

Introduction

SNMP architecture

Management Information Base

SNMP protocol

Network management in practice

Niksula

CS-building network and Niksula

- ▶ One router and about 50 switches
- ▶ Hundreds of hosts
- ▶ Multiple subnets from HUT domain
- ▶ Devices managed via SNMP include printers, servers and network
- ▶ Other management tools: cfengine/puppet(configuration), firewall managed manually
- ▶ DEMO

Questions?