

Network Management

An introduction

Marcin Cieślak

System Business Consulting

Exit

Contents

- Overview of Network Management
 - Network management functions
 - Internet management model
 - SNMP framework

Definition of Network Management

Network Collection of computers and other devices that are able to communicate with each other over some transmission medium.

Management Management involves the planning, organizing, monitoring, accounting and controlling of activities and resources.

Network management overview

Network management can be viewed from several perspectives:

- managed objects
 - functions performed
 - human resources
 - financial resources
 - administrative boundaries
 - policies

Network management process

- Planning and design
 - Implementation (deployment)
 - Operation and maintenance

Design phase

- Capacity planning
 - Trend analysis
 - Build history
 - Topology map
 - Procurement
 - Initial documentation

Implementation phase

- Installation and configuration
 - Addressing
 - Security
 - Accounting
 - Documentation

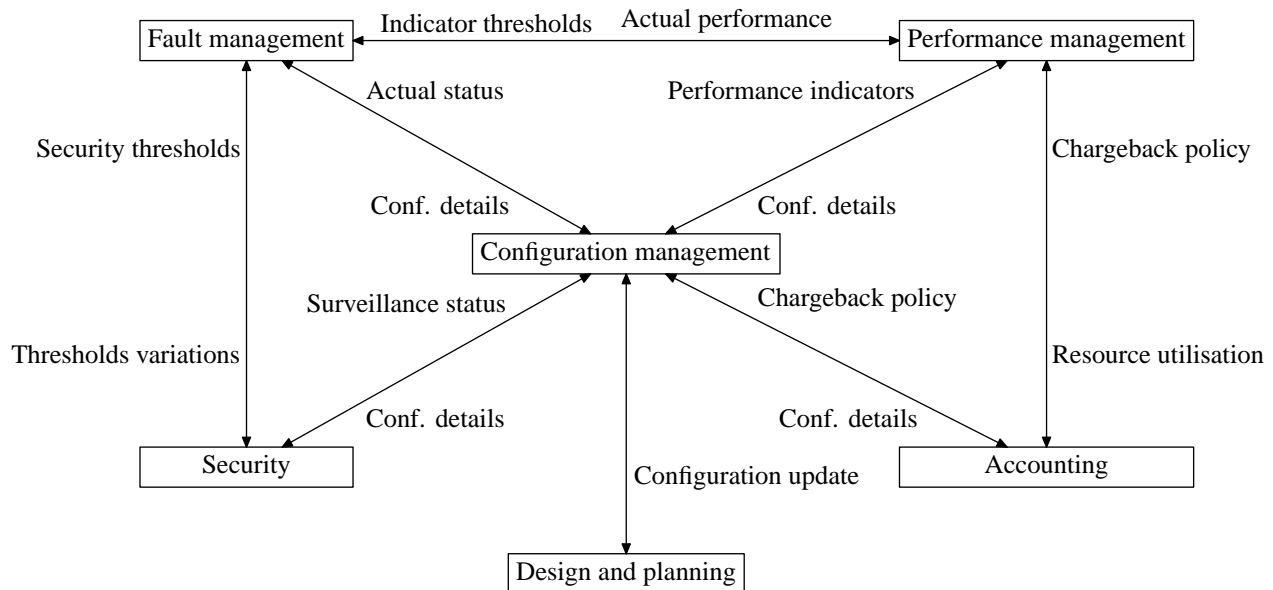
Operational phase

- Notification
 - Proactive monitoring
 - Troubleshooting
 - Reporting

Areas of network management (1)

- Configuration management
 - Fault management and recovery
 - Security management
 - Performance management
 - Accounting

Areas of network management (2)



Configuration management (1)

The necessary data should be obtained from the design/deployment phase documentation.

- Configuration planning
 - Distributing
 - Installing
 - Testing
 - Revision tracking
 - Backup and recovery

Configuration management (2)

Network manager tools:

- Command line configuration
 - Graphical and Web-based interface configuration
 - SNMP
 - Revision control (RCS, SCCS, CVS)

Configuration management (3)

Typical device access:

- Local out-of-band management via serial port
 - In-band network management
 - Hardware methods (DIP switches, etc)
 - Useful protocols: BOOTP, TFTP.

Fault management (1)

- Problem discovery
 - Problem isolation - fix one thing at once!
 - Bypass and recovery
 - Problem resolution (fix)
 - Tracking and reporting

Fault management (2)

- Simple tools (ping, traceroute)
 - Extensive logging and timestamping
 - Configuration backup ("last known good")
 - Emergency access (serial console)
 - Firmware management and upgrades
 - Vendor contact and bug reporting
 - Support contract management

Security management (1)

Process of controlling access to information on the data network. Start with a security policy:

- identify sensitive information (what to protect)
 - locale access points (where to protect)
 - secure access points
 - monitor and log

Security management (2)

Network security management should not be confused with application security, operating system security, or physical security, but cannot fulfill its tasks without them.

The policy should be approved and fully endorsed by the top management.

Security management (3)

Security management tools:

- Simple TCP/IP tools (netcat, sock)
 - Host scanning utilities (nmap)
 - Extensive logging (even hardcopy)
 - Intrusion detection systems (IDS)
 - Firewalls
 - Specialized network scanning software

Performance management

Involves measuring of performance of network hardware, software and media.
Performance management involves data collection and analysis.

Typical parameters to collect and analyse:

- Throughput
 - Utilization
 - Error rates
 - Response times

Accounting

Accounting involves tracking individual and group usage of network resources. It implies:

- user and group identification
 - resource-to-user identity mapping
 - billing

Accounting is also useful as a security problem analysis tool.

Internet management model (1)

The Internet management model includes:

- managed elements
 - management stations
 - management protocols (e.g. SNMP)
 - management information (e.g. MIB)

Managed element – the agent

Managed element runs a software called the **management agent**, collecting data directly from the source (hardware, operating system kernel etc.)

Management station

- runs management application(s)
 - monitors and controls managed elements
 - collects event reports from the elements

Management information

- Management Information Base (MIB)
 - Structure of Management Information (SMI)
 - Simple Network Management Protocol (SNMP)
 - Remote MONitoring (RMON)

Management Information Base

MIB is the data base of variables the network elements maintain

Structure of Management Information

SMI	SMI describes the syntax and type of information available in the MIB and defines rules for naming types of information (with the help of ASN.1)
------------	--

Evolution of network management

- 1988: IAB sets general requirements (RFC1052)
- 1988: SMI (RFC1065), MIB (RFC1066) and SNMP (RFC1067) published.
- 1991: Internet standards: SMI – RFC1155, RFC1212; MIB-II – RFC1213; SNMP – RFC1157.
 - 1991: RMON (RFC1271)
 - 1993: SNMPv2 (RFC2222)
 - 1997: RMON2 (RFC2021, RFC2074)
 - 1998: SNMPv3 (RFC2271-2275)

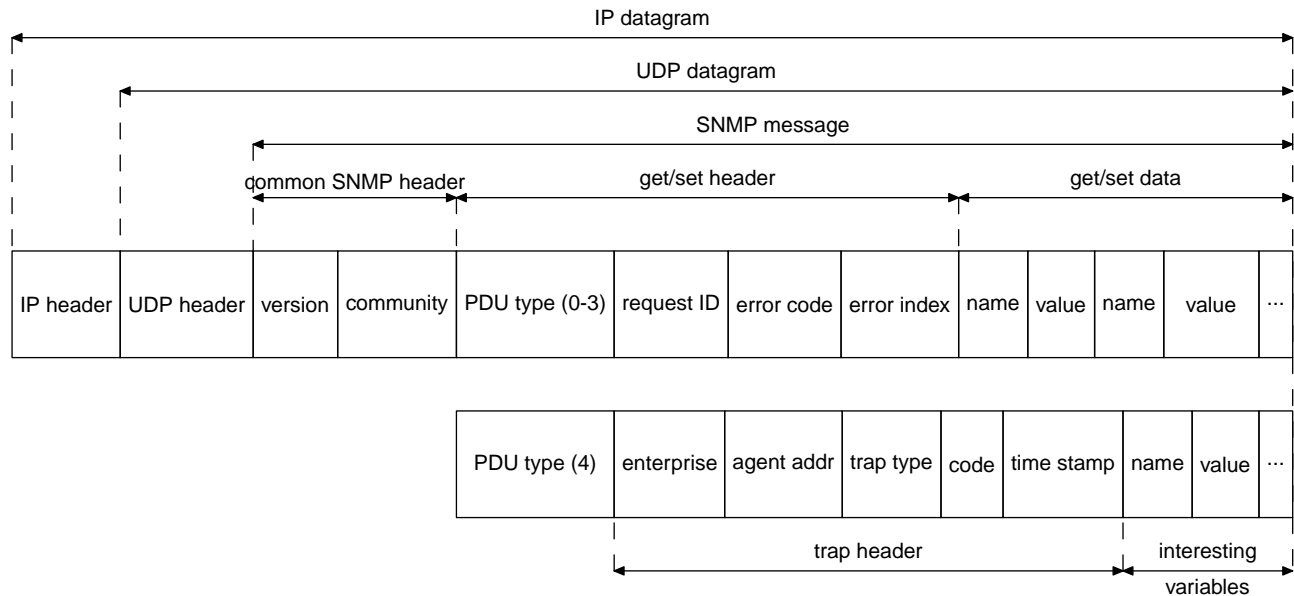
SNMP request types

The protocol defines the following request types:

- get-request
 - get-response
 - get-next-response
 - set-request
 - trap
 - get-bulk-request (SNMPv2)
 - inform-request (SNMPv2)

SNMP uses UDP protocol for transport, with ports 161 for requests and 162 for traps.

SNMP packet format



Data types defined by SMI (1)

INTEGER

Integer numer with or without restrictions in range

OCTET STRING

A string of 0 or more 8-bit bytes. Each byte has a value of 0-255.

DisplayString

A string of 0 or more 8-bit bytes. Each byte must be a character from 7bit set of NVT ASCII.

OBJECT IDENTIFIER

Object identifier from a MIB tree.

Data types defined by SMI (2)

NULL

Corresponding variable has no value.

IpAddress

An OCTET STRING of length 4, with 1 byte for each byte of IP address.

PhysAddress

An OCTET STRING specifying physical address.

Data types defined by SMI (3)

Counter

A non-negative integer value increases from 0 to $2^{32} - 1$ and then wraps to 0.

Gauge

A non-negative integer between from 0 to $2^{32} - 1$, whose value increases or decreases but latches at the max value.

TimerTicks

A counter that counts time in 1/100 sec.

Data types defined by SMI (4)

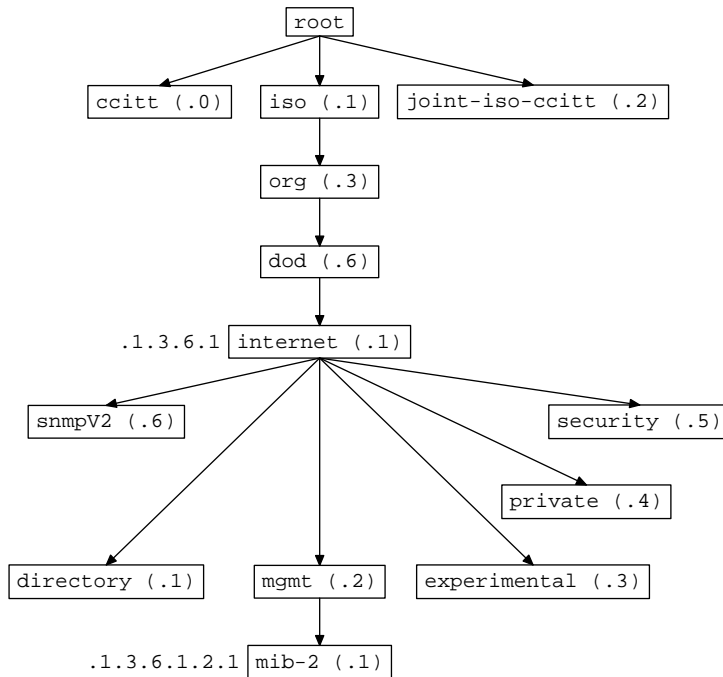
SEQUENCE

A structure of variables of different types.

SEQUENCE OF

A vector with all elements having the same data structure.

Structure of MIB objects



SNMP security

In order to authenticate communicating parties SNMP employs following methods:

- SNMPv1: plaintext community name ("public" etc.)
 - SNMPv2: one-way hashed password
 - SNMPv3: user-based security model (USM), view-based access control model (VSAM) with optional DES encryption and secure hashing

Networking equipment comes very often with a predefined access with a public community name. This may give an unauthorized access to crucial data on your network.

RMON Overview

- Remote MONitoring
 - Distributed monitoring of network data
 - Statistics gathered from every frame coming to the probe
 - SNMP used for transport
 - RMON 1 used for layers 1 and 2
 - RMON 2 used for layers 3 and above

RMON Groups (1)

- Statistics group (1)
 - History group (2)
 - Alarms group (3)
 - Hosts group (4)
 - Hosts TopN group (5)
 - Traffic matrix (6)

RMON Groups (2)

- Filter group (7)
 - Packet capture group (8)
 - Event group (9)