A Brief Introduction to Internet Network Management and SNMP

Geoff Huston

NTW Track 4

What are we talking about?

- Network Management Tasks
  - fault management
  - configuration management
  - performance management
  - security management
  - inventory management
  - accounting management

Fault Management

- detection
- exception alarm generation
- investigation and analysis
- statistics for steady state behaviour characterisation

Configuration Management

- installation of new hardware/software
- tracking changes in control configuration
  - who, what and why!
- revert/undo changes
- change management
- configuration audit
  - does it do what was intended?

IP Route Management

- routing integrity
- consistency with customer requirements
- consistency with external peers
- conformance with imposed policy constraints

Security Management

- exception alarm generation
- detection
- uniform access controls to resources
- backup

Performance Management

- Availability and Reliability metrics
- Quality metrics
- real-time measurement
- historical analysis

Accounting Management

- identifying consumers and suppliers
  - of network resources
- mapping network resources to customer identity
- charge back
  - volumetric data
  - time data
  - date time of day

Problem Tracking

- reporting procedures
- fault management
- escalation and referral
- historical data for component reliability analysis

Inventory Control

- hardware
  - components
  - identity
  - location
- software
  - version control

Knowledge Based Management

- "expert" systems
- Modelling
  - simulation
  - routing
  - configuration changes

No single system will solve all your problems or meet all your requirements

Any Network Management package can only complement effective and efficient operational procedures

Need to identify what is important to you and your organization

SNMP

- Simple Network Management Protocol
- Doesn't SNMP solve all these problems ?
  - Don't be silly!

SNMP

- Where did it come from ?
  - Internet Engineering Task Force
    - » Network Management Area
  - SNMP V1
  - MIB definitions
  - SNMPV2

What is it ?

- more than just a protocol …

- It defines an architecture for extracting information from the network regarding the current operational state of the network, using a vendor-independent family of mechanisms

Structure of Management Information (SMI)

- identifies and defines structure of management information
  - RFC1155
- defines
  - commonly defined data item
  - syntax of the data type
  - semantics of the data object

Syntax

- uses ASN.1 (Abstract Syntax Notation)
  - binary encoding

    02 01 06is a 1 byte integer, value 6
- Primitive Types

  INTEGER, OCTECT STRING, OBJECT IDENTIFIER, NULL
- Constructor Types

  SEQUENCE <primitive-type> ... ie. a record

  SEQUENCE OF <primitive-type> ... ie. an array

Syntax

- Defined Data Types

IpAddress	what you expect
Counter	non-negative integer that wraps
Gauge	non-negative integer that latches
TimeTicks	time in hundredths of seconds

SNMP NAMES

SNMP Name Structure

SNMP

- Management Information Base (MIB)
  - "database"of network objects
  - Groups:
    - » System, Interfaces, Address Translation, IP, ICMP, TCP, UDP, EGP
  - "Access" and "Status" attributes
  - actual variables are "instances" of OIDs

1.3.6.1.2.1.1.1.0 sysDescr

1.3.6.1.2.1.2.1.1.10.3 ifInOctets for interface 3

1.3.6.1.2.1.4.21.1.7.130.56.0.0

ipRouteNextHop for network 130.56.0.0

SNMP

- The SNMP protocol itself
  - allows inspection and alteration of MIB variables
- UDP Based
  - not acknowledged transactions
- PUT, GET, GET-NEXT operators

SNMP

- SNMP Traps
  - unsolicited notification of events
  - can include variable list
  - ColdStart, WarmStart
  - LinkUp, LinkDown
  - Authentication Failure
  - EGP Neighbour Loss
  - Enterprise Specific

Network Management Software

- SNMP Agents
  - provided by all router vendors
  - many expanded (enterprise) MIBs
  - bridges, wiring concentrators, toasters

Network Management Software

- Public Domain
  - Application Programming Interfaces available from CMU and MIT
  - include variety of applications

Network Management Software

- Commercially
  - many offerings, UNIX and PC based
    - » HP OpenView
    - » SunNet Manager
    - » Cabletron Spectrum
    - » *MANY* others

Choosing a Management Platform

- Does it:
  a) Support your systems ?
  b) Run on your platforms ?
  c) Meet your requirements ?
  d) Match your resources ?

Choosing a Management Platform

- Maybe you can get away with something quick and dirty using existing tools
- Maybe a commercial management product will meet your operational requirements