An Introduction to Simple Network Management Protocol
Introduction

- Simple Network Management Protocol
  - What it is
  - Definition
  - Why it is needed
  - How it works
  - Alternatives
  - The Future
What is SNMP?

- **Simple Network Management Protocol**
- It’s designed to be **Simple**
  - Only five commands in version 1
- It’s concerned with **Network Management**
  - Manage network performance
  - Identify and diagnose issues
  - Baseline/Plan for network growth
- It’s a **Protocol**
  - defined by the IETF (Internet Engineering Task Force)
Definition

SNMP (Simple Network Management Protocol) is an industry standard communication protocol for managing and monitoring network devices. Its purpose is to provide a small, common and simple set of commands that allow network devices to be managed.
Why is SNMP needed?

- Distributed ad-hoc devices across the network including repeaters, routers, bridges, switches, hub, ups devices all need management.
- They all basically receive data in from the network, process it and put data back out onto the network.
- They can sometimes be cumbersome to manage.
- Inconsistent and differing interfaces require different resources.
Each line represents a connection, while each endpoint represents a node.

Asia Pacific - Red
Europe/Middle East/Central Asia/Africa - Green
North America - Blue
Latin American and Caribbean - Yellow
RFC1918 IP Addresses - Cyan
Unknown - White

Map of the Internet (Nov 2003)
What is SNMP technically?

- Part of the TCP/IP model
- Defined through IETF RFC’s
- Uses Protocol Data Units (PDU’s) which are special forms of packet
- Uses a community string as password
  - Read-only and read/write
- Made up of 3 primary elements:
  - SNMP Managers (NMS receive messages from Agents, reporting, execute programs).
  - SNMP Agents – (software module in a managed device and talks to Managers)
    - Translates local info to MIB info
  - MIBs (Collection of definitions of device management information) organised by OID (Object ID)
- Rootless MIB hierarchy
Standard Models

**OSI 7 Layer Model**
- Application Layer (e.g., SNMP)
- Presentation Layer (e.g., ASN.1)
- Session Layer (e.g., Winsock)
- Transport Layer (e.g., TCP)
- Network Layer (e.g., IP)
- Data Link Layer (e.g., Ethernet)
- Physical Layer (e.g., Cable)

**TCP/IP Model**
- Application (e.g., SNMP)
- Transport Layer (e.g., TCP)
- Inter-network Layer (e.g., IP)
- Link Layer

www.jasonslater.co.uk
Manager/Agent relationship

NMS (Network Management Station)

Management process

Management Database

Network

Commands

Responses

Notifications

Managed System

Agent process

Managed objects
(defined by MIB)

Management Database

NMS (Network Management Station)

Managed System

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network

Managed System

Network
The MIB Namespace

- root
  - itu-1 (0)
  - iso (1)
  - iso/itu-t (2)
    - standard (0)
    - registration authority (1)
    - member body (2)
    - Identified organization (e.g. .com .org) (3)
      - dod (Department of Defense) (6)
  - internet (1)
    - directory (1)
    - mgmt (2)
    - exp (3)
    - private (4)
    - security (5)
    - snmpv2 (6)
      - enterprises (1)
        - cisco (9)
        - nec (119)
Management Information Base

A MIB contains a list of characteristics of a managed device

```
nec OBJECT IDENTIFIER ::= { enterprises 119 }
nec-mib OBJECT IDENTIFIER ::= { nec 2 }
necProductDepend OBJECT IDENTIFIER ::= { nec-mib 3 }
atomis-mib OBJECT IDENTIFIER ::= { necProductDepend 14 }
m5core-mib OBJECT IDENTIFIER ::= { atomis-mib 3 }

-- MIB Groups
-- Node group
node OBJECT IDENTIFIER ::= { m5core-mib 1 }
-- Line interface group
linf OBJECT IDENTIFIER ::= { m5core-mib 2 }
-- Connection group
conn OBJECT IDENTIFIER ::= { m5core-mib 3 }
-- Performance group
perf OBJECT IDENTIFIER ::= { m5core-mib 4 }

nodeFanStatus OBJECT-TYPE
SYNTAX INTEGER {
    up(1),
    down(2)
}
ACCESS read-only
STATUS mandatory
DESCRIPTION "Operational FAN status"
 ::= { node 3 }

1.3.6.1.4.1.119.2.3.14.3.1.3
```
Example SNMP ‘GET’ operation

1. User makes request to NMS
2. NMS initiates formal request
3. Request traverses network
4. Agent processes request
5. Agent formulates reply
6. NMS receives reply
7. User informed of result
How is SNMP defined?

- Uses ASN.1
  - Abstract Syntax Notation One (ASN.1)
  - Standards based ‘descriptive’ language used to abstractly describe messages
    - Standardized in 1984 by CCITT and ISO in 1985
  - Uses predefined types
    - e.g. Integer and Boolean
  - Uses OID – Object IDentifier
  - Uses MIB hierarchy with a rootless tree

http://asn1.elibel.tm.fr/en/
Abstract Syntax Notation One (ASN.1) is a formal language for abstractly describing messages to be exchanged among an extensive range of applications involving the Internet, intelligent network, cellular phones, ground-to-air communications, electronic commerce, secure electronic services, interactive television, intelligent transportation systems, Voice Over IP and others.

Due to its streamlined encoding rules, ASN.1 is also reliable and ideal for wireless broadband and other resource-constrained environments. Its extensibility facilitates communications between newer and older versions of applications. In a world of change, ASN.1 is core technology, constantly adapting to new technologies.
SNMP v1

- Supports 5 operations (PDUs)
  - GetRequest
    - polls agents for information
  - GetNextRequest
    - requests the next item in a dataset
  - Set
    - requests a change to a value
  - GetResponse
    - sends a response to a Manager request
  - Trap
    - informs a Manager of an event
### SNMP Protocol Data Unit (PDU)

#### SNMPv1 message

<table>
<thead>
<tr>
<th>Version</th>
<th>Community</th>
<th>PDU</th>
</tr>
</thead>
</table>

**Command** | **Request ID** | **Error Status** | **Error Index** | **OID <value>** | **OID <value>** | **OID <value>** |
|-----------|--------------|----------------|----------------|----------------|----------------|----------------|

[… variable length …]
SNMP v2

- Never took off due to security concerns and disagreements
- v2 has several advantages over SNMPv1, including:
  - Expanded data types (e.g., 64 bit)
  - Added GetBulk Command
  - Added Inform Command (forwarding of TRAP info)
  - Better error handling (errors and exceptions)
- V2 addresses security issues missing from v1 including:
  - Authentication
  - Message integrity
  - Privacy
  - Authorization and access control
- Development of SNMP fragmented into different standards groups:
  - SNMPv2c
  - SNMPv2u
  - SNMPv2*
SNMP v3

- Security centric design
- V3 protocol was an attempt to consolidate the best features of the different versions of SNMP v2.
- V3 is gaining acceptance from big names in the industry (e.g. Cisco and HP)
Alternatives to SNMP

- **CMIP** Common Management Information Protocol (ISO)
  - Variables can perform tasks as well as store information
  - Built-in security for authorisation, access control, and logging.
  - Wider set of commands
  - Handles unusual network conditions better

- **DME** Distributed Management Environment (OSF)
  - Can integrate with SNMP (and CMIP)
  - Event Management
  - Print Servicing
  - Network licensing
  - Software Distribution

- **HNMS** Hierarchical Network Management System (NAS)
  - Low management traffic

- **HMMA** Hypermedia Management Architecture (WBEM)
  - Everything can be managed via a web browser
  - Lower costs – use of ‘already in place’ web technologies
Research

- Implementation of XML gateways to co-exist with ASN.1 specification
- Tighter security, possibly including IPSec
  - Currently only community names and general firewall exclusion rules
- Smart packets – small programs that can be embedded in packet data that run small programs to collect and process information
Summary

- SNMP is a network management protocol
  - Became popular because of its ‘simple’ nature
- 3 versions of SNMP exist
  - though v2 never really took off
  - V3 only recently started to gain favour
- Uses ASN.1 syntax with a rootless MIB tree hierarchy
- A number of alternatives are available
- Research is looking at:
  - ASN.1 and XML cross functionality
  - Better Security
  - Smart Packets
References

http://www.ietf.org/rfc.html
http://www.opte.org
http://asn1.elibel.tm.fr/en/
http://www.ietf.org/rfc/rfc2578.txt
IETF RFC

RFC 1065 - Structure and identification of management information for TCP/IP-based internets
RFC 1066 - Management Information Base for network management of TCP/IP-based internets
RFC 1067 - A Simple Network Management Protocol
RFC 1089 - SNMP over Ethernet
RFC 1140 - IAB Official Protocol Standards
RFC 1147 - Tools for Monitoring and Debugging TCP/IP Internets and Interconnected Devices
RFC 1155 - Structure and Identification of Management Information for TCP/IP based internets.
RFC 1156 - Management Information Base Network Management of TCP/IP based internets
RFC 1157 - A Simple Network Management Protocol
RFC 1158 - Management Information Base Network Management of TCP/IP based internets: MIB-II
RFC 1161 - SNMP over OSI
RFC 1187 - Bulk Table Retrieval with the SNMP
RFC 1212 - Concise MIB Definitions
RFC 1213 - Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RFC 1215 - A Convention for Defining Traps for use with the SNMP
RFC 1224 - Techniques for Managing Asynchronously-Generated Alerts
RFC 1270 - SNMP Communication Services
RFC 1303 - A Convention for Describing SNMP-based Agents
RFC 1470 - A Network Management Tool Catalog
RFC 1298 - SNMP over IPX (obsolete, see RFC 1420)
RFC 1418 - SNMP over OSI
RFC 1419 - SNMP over AppleTalk
RFC 1420 - SNMP over IPX (replaces RFC 1298)

http://www.ietf.org/rfc.html