SNMP

Simple Network Management Protocol

Chris Francois
CS 417d Fall 1998
cfrancois@acm.org

What is Network Management?

Basic tasks that fall under this category are:

- Configuration Management
  - Keeping track of device settings and how they function
- Fault Management
  - Dealing with problems and emergencies in the network (router stops routing, server loses power, etc.)
- Performance Management
  - How smoothly is the network running?
  - Can it handle the workload it currently has?

Network Management must be...

The management interface must be...

- Standardized
- Extendible
- Portable

The management mechanism must be...

- Inexpensive
- Implemented as software only

Functional Areas of Network Management

Configuration Management - inventory, configuration, provisioning

Fault Management - reactive and proactive network fault management

Performance Management - # of packets dropped, timeouts, collisions, CRC errors

Security Management - SNMP doesn t provide much here

Accounting Management - cost management and chargeback assessment

Asset Management - statistics of equipment, facility, and administration personnel

Planning Management - analysis of trends to help justify a network upgrade or bandwidth increase

SNMP & Network Management History

- ***1983*** - TCP/IP replaces ARPANET at U.S. Dept. of Defense, effective birth of Internet
- First model for net management - **HEMS** - High-Level Entity Management System (*RFCs 1021,1022,1024,1076*)
- ***1987*** - ISO OSI proposes **CMIP** - Common Management Information Protocol, and **CMOT** (CMIP over TCP) for the actual network management protocol for use on the internet
- ***Nov. 1987*** - **SGMP** - Simple Gateway Monitoring protocol (*RFC 1028*)
- ***1989*** - Marshall T. Rose heads up **SNMP** working group to create a common network management framework to be used by both **SGMP** and **CMOT** to allow for transition to **CMOT**
- ***Aug. 1989*** - "**Internet-standard Network Management Framework** "defined (*RFCs 1065, 1066, 1067*)
- ***Apr. 1989*** - **SNMP** promoted to ***recommended*** status as the de facto TCP/IP network management framework (*RFC 1098*)
- ***June 1989*** - IAB committee decides to let **SNMP** and **CMOT** develop separately
- ***May 1990*** - IAB promotes SNMP to a **standard protocol with a recommended status** (*RFC 1157*)
- ***Mar. 1991*** - format of MIBs and traps defined (*RFCs 1212, 1215*)
- TCP/IP MIB definition revised to create **SNMPv1** (RFC 1213)

Versions

- Two major versions SNMPv1, SNMPv2
- SNMPv1 is the recommended standard
- SNMPv2 has become split into:
  - SNMPv2u - SNMPv2 with user-based security
  - SNMPv2* - SNMPv2 with user-based security and additional features
  - SNMPv2c - SNMPv2 without security

What is SNMP?

- SNMP is a tool (protocol) that allows for remote and local management of items on the network including servers, workstations, routers, switches and other managed devices.
- Comprised of agents and managers
  - Agent - process running on each managed node collecting information about the device it is running on.
  - Manager - process running on a management workstation that requests information about devices on the network.

Advantages of using SNMP

- Standardized
- universally supported
- extendible
- portable
- allows distributed management access
- lightweight protocol

Client Pull & Server Push

- SNMP is a “client pull”model

  The management system (client) “pulls”data from the agent (server).

- SNMP is a “server push”model

  The agent (server) “pushes”out a trap message to a (client) management system

SNMP & The OSI Model

7	Application Layer	Management and Agent APIs
		SNMP
6	Presentation Layer	ASN.1 and BER
5	Session Layer	RPC and NetBIOS
4	Transport Layer	TCP and UDP
3	Network Layer	IP and IPX
2	Data Link Layer	Ethernet, Token Ring, FDDI
1	Physical Layer	

Ports & UDP

•SNMP uses User Datagram Protocol (UDP) as the transport mechanism for SNMP messages

•Like FTP, SNMP uses two well-known ports to operate:

- **UDP Port 161** - SNMP Messages
- **UDP Port 162** - SNMP Trap Messages

The Three Parts of SNMP

SNMP network management is based on three parts:

- **SNMP Protocol**
  - Defines format of messages exchanged by management systems and agents.
  - Specifies the Get, GetNext, Set, and Trap operations
- **Structure of Management Information (SMI)**
  - Rules specifying the format used to define objects managed on the network that the SNMP protocol accesses
- **Management Information Base (MIB)**
  - A map of the hierarchical order of all managed objects and how they are accessed

Nodes

Items in an SNMP Network are called nodes. There are different types of nodes.

- Managed nodes

  Typically runs an agent process that services requests from a management node

- Management nodes

  Typically a workstation running some network management & monitoring software

- Nodes that are not manageable by SNMP

  A node may not support SNMP, but may be manageable by SNMP through a proxy agent running on another machine

Nodes can be both managed nodes and a management node at the same time
(typically this is the case, since you want to be able to manage the workstation that your management application is running on.)

Community Names

Community names are used to define where an SNMP message is destined for.

They mirror the same concept as a Windows NT or Unix domain.

•Set up your agents to belong to certain communities.

•Set up your management applications to monitor and receive traps from certain community names.

SNMP Agents

Two basic designs of agents

- Extendible Agents
  - Open, modular design allows for adaptations to new management data and operational requirements
- Monolithic Agents
  - not extendible
  - optimized for specific hardware platform and OS
  - this optimization results in less overhead (memory and system resources) and quicker execution

Proxy & Gateway Agents

Proxy & Gateway Agents extend the capabilities of SNMP by allowing it to:

- Manage a device that cannot support an SNMP agent
- Manage a device that supports a non-SNMP management agent
- Allow a non-SNMP management system to access an SNMP agent
- Provide firewall-type security to other SNMP agents (UDP packet filtering)
- Translate between different formats of SNMP messages (v1 and v2)
- Consolidate multiple managed nodes into a single network address (also to provide a single trap destination)

Four Basic Operations

- **Get**

  Retrieves the value of a MIB variable stored on the agent machine

  (integer, string, or address of another MIB variable)

- **GetNext**

  Retrieves the next value of the next lexical MIB variable

- **Set**

  Changes the value of a MIB variable

- **Trap**

  An unsolicited notification sent by an agent to a management application (typically a notification of something unexpected, like an error)

Traps

- Traps are unrequested event reports that are sent to a management system by an SNMP agent process
- When a trappable event occurs, a trap message is generated by the agent and is sent to a trap destination (a specific, configured network address)
- Many events can be configured to signal a trap, like a network cable fault, failing NIC or Hard Drive, a "General Protection Fault", or a power supply failure
- Traps can also be throttled -- You can limit the number of traps sent per second from the agent
- Traps have a priority associated with them -- Critical, Major, Minor, Warning, Marginal, Informational, Normal, Unknown

Trap Receivers

- Traps are received by a management application.
- Management applications can handle the trap in a few ways:
  - Poll the agent that sent the trap for more information about the event, and the status of the rest of the machine.
  - Log the reception of the trap.
  - Completely ignore the trap.
- Management applications can be set up to send off an e-mail, call a voice mail and leave a message, or send an alpha-numeric page to the network administrator ś pager that says:

Your PDC just Blue-Screened at 03:46 AM. Have a nice day. :)

Languages of SNMP

- Structure of Management Information (SMI)

  specifies the format used for defining managed objects that are accessed via the SNMP protocol

- Abstract Syntax Notation One (ASN.1)

  used to define the format of SNMP messages and managed objects (MIB modules) using an unambiguous data description format

- Basic Encoding Rules (BER)

  used to encode the SNMP messages into a format suitable for transmission across a network

SMIv1

Structure of Management Information

SMIv1 is described in RFCs 1155, 1212, 1215

These RFCs describe:

- How MIB modules are defined with CCITT X.208 ASN.1 data description language
- The subset of the ASN.1 language that is used in MIBs
- The addition of the APPLICATION data type to ASN.1, specifically for use with SNMP MIBs
- All ASN.1 constructs are serialized using the CCITT X.209 BER for transmission across the wire
- definition of the high-level structure of the Internet branch (iso(1).org(3).dod(6).internet(1)) of the MIB naming tree
- the definition and description of an SNMP managed object

SMIv2

Structure of Management Information

SMIv2 is described in RFCs 1442, 1443, 1444

These RFCs describe:

- SMIv2 is a backward compatible update to SMIv1
- The only exception is the Counter64 type defined by SMIv2
- Counter64 cannot be created in SMIv2
- RFC 2089 defines how bilingual (SMIv1 & SMIv2) agents handle the Counter64 data type
- IETF requires that new and revised RFCs specify MIB modules using SMIv2

ASN.1

Abstract Syntax Notation One

ASN.1 is nothing more than a language definition. It is similar to C/C++ and other programming languages.

Syntax examples:

```
-- two dashes is a comment -- The C equivalent is written in the comment
MostSevereAlarm ::= INTEGER          -- typedef MostSevereAlarm int;
circuitAlarms MostSevereAlarm ::= 3    -- MostSevereAlarm circuitAlarms = 3;
MostSevereAlarm ::= INTEGER (1..5)  -- specify a valid range
ErrorCounts ::= SEQUENCE {
   circuitID                OCTET STRING,
   erroredSeconds       INTEGER,
   unavailableSeconds  INTEGER
}   -- data structures are defined using the SEQUENCE keyword
```

BER

Basic Encoding Rules

The relationship between ASN.1 and BER parallels that of source code and machine code.

CCITT X.209 specifies the Basic Encoding Rules

All SNMP messages are converted / serialized from ASN.1 notation into smaller, binary data (BER)

SNMP Data Types

- INTEGER -- signed 32-bit integer
- OCTET STRING
- OBJECT IDENTIFIER (OID)
- NULL -- not actually data type, but data value

Yellow items defined by ASN.1

Orange items defined by RFC 1155

- IpAddress -- OCTET STRING of size 4, in network byte order (B.E.)
- Counter -- unsigned 32-bit integer (rolls over)
- Gauge -- unsigned 32-bit integer (will top out and stay there)
- TimeTicks -- unsigned 32-bit integer (rolls over after 497 days)
- Opaque -- used to create new data types not in SNMPv1
- DateAndTime, DisplayString, MacAddress, PhysAddress, TimeInterval, TimeStamp, TruthValue, VariablePointer -- textual conventions used as types

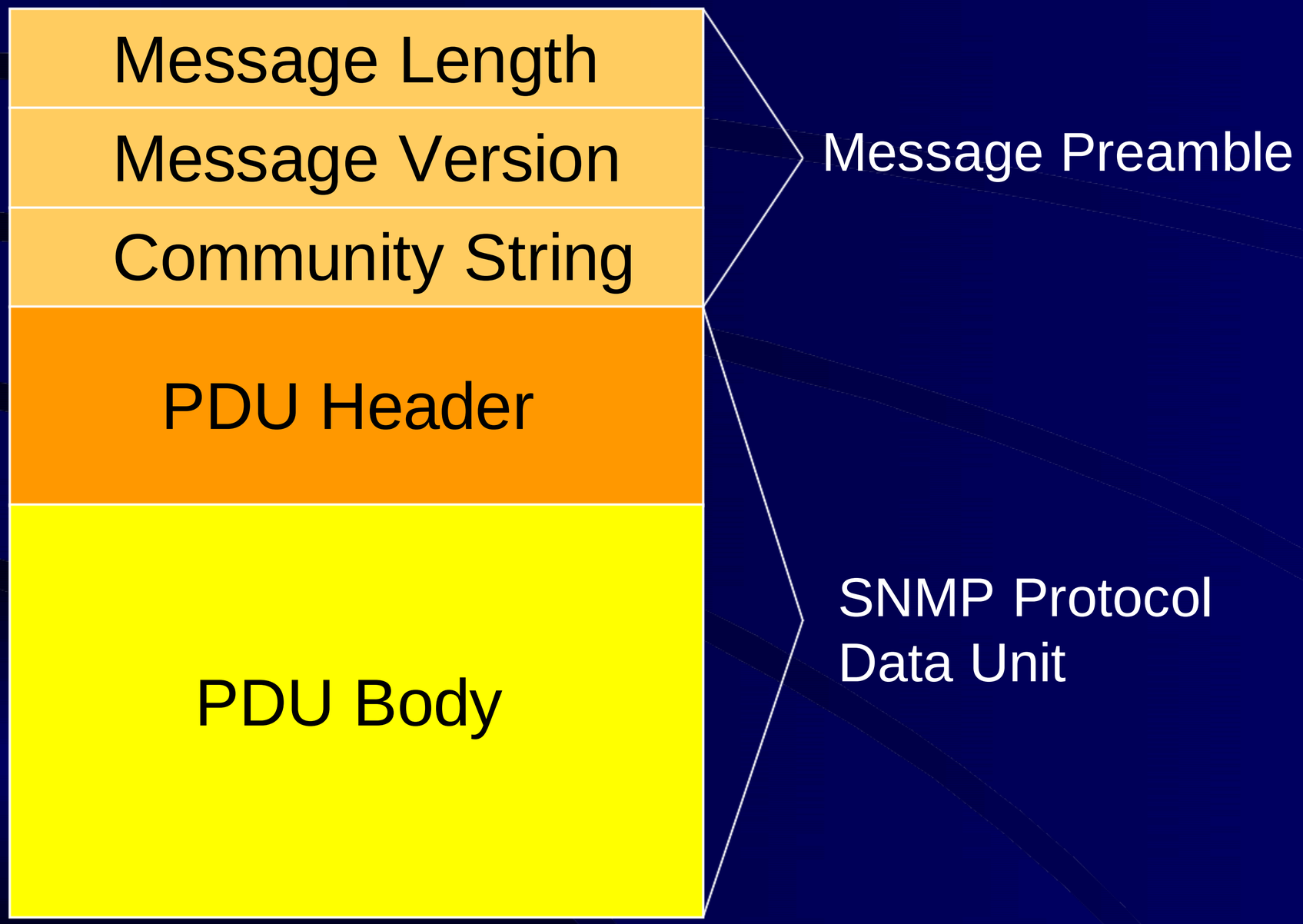
Managed “Objects ”& MIBs

Always defined and referenced within the context of a MIB

A typical MIB variable definition:

```
sysContact OBJECT-TYPE          -- OBJECT-TYPE is a macro
SYNTAX      DisplayString (SIZE (0..255))
ACCESS      read-write          -- or read-write, write-only, not-accessible
STATUS      mandatory           -- or optional, deprecated, obsolete
DESCRIPTION
        “Chris Francois
         cfrancois@acm.org
         (360)650-0000 ”
::= { system 4 }
```

Basic Message Format



SNMP Message Formats

SNMP Message Preamble

PDU Header

PDU Body

Message Length
Message Version
Community String
PDU Type
PDU Length
Request ID
Error Status
Error Index
Length of Variable Bindings
Length of First Binding
OID of First Binding
Type of First Binding
Value of First Binding
Length of Second Binding
OID of Second Binding
Type of Second Binding
Value of Second Binding
Additional Variable Bindings

Message Length
Message Version
Community String
PDU Type
PDU Length
Enterprises MIB OID
Agent IP Address
Standard Trap Type
Specific Trap Type
Time Stamp
Length of Variable Bindings
Length of First Binding
OID of First Binding
Type of First Binding
Value of First Binding
Length of Second Binding
OID of Second Binding
Type of Second Binding
Value of Second Binding
Additional Variable Bindings

Commercial SNMP Applications

Here are some of the various SNMP Management products available today:

•http://www.hp.com/go/openview/	HP OpenView
•http://www.tivoli.com/	IBM NetView
•http://www.novell.com/products/managewise/	Novell ManageWise
•http://www.sun.com/solstice/	Sun MicroSystems Solstice
•http://www.microsoft.com/smsmgmt/	Microsoft SMS Server
•http://www.compaq.com/products/servers/management/	Compaq Insight Manger
•http://www.redpt.com/	SnmpQL - ODBC Compliant
•http://www.empiretech.com/	Empire Technologies
•ftp://ftp.cinco.com/users/cinco/demo/	Cinco Networks NetXray
•http://www.netinst.com/html/snmp.html	SNMP Collector (Win9X/NT)
•http://www.netinst.com/html/Observer.html	Observer
•http://www.gordian.com/products_technologies/snmp.html	Gordian ȿs SNMP Agent
•http://www.castlerock.com/	Castle Rock Computing
•http://www.adventnet.com/	Advent Network Management
•http://www.smplsft.com/	SimpleAgent, SimpleTester

SNMP & Windows NT 5.0

Proposed features of the Windows NT5 SNMP Service

- Full bilingual support for SNMPv1 and SNMPv2c
- ability to map SNMPv2c requests to SNMPv1 for processing by extension agents
- better synchronization of MIB variables
- a new extension agent framework (backward compatible with original framework, but with MS add-ons)
- code-generator for creation of extension agents
- MIB-II, LAN Manager 2, IP Forwarding MIB (RFC 1354), and Host Resources MIB (RFC 1514) extension agents included
- All MIB modules included with SNMP install
- SMS 2.0 also has a Symantec PCAnywhere type of application integrated into it, allowing "remote-but-local" management as well

SNMP RFC ś

RFC	Description	Published	Current Status
1065	SMIv1	Aug-88	Obsoleted by 1155
1066	SNMPv1 MIB	Aug-88	Obsoleted by 1156
1067	SNMPv1	Aug-88	Obsoleted by 1098
1098	SNMPv1	Apr-89	Obsoleted by 1157
1155	SMIv1	May-90	Standard
1156	SNMPv1 MIB	May-90	Historic
1157	SNMPv1	May-90	Standard
1158	SNMPv1 MIB-II	May-90	Obsoleted by 1213
1212	SNMPv1 MIB definitions	Mar-91	Standard
1213	SNMPv1 MIB-II	Mar-91	Standard
1215	SNMPv1 traps	Mar-91	Informational
1351	Secure SNMP administrative model	Jul-92	Proposed Standard
1352	Secure SNMP managed objects	Jul-92	Proposed Standard
1353	Secure SNMP security protocols	Jul-92	Proposed Standard
1441	Introduction to SNMPv2	Apr-93	Proposed Standard
1442	SMIv2	Apr-93	Obsoleted by 1902
1443	Textual conventions for SNMPv2	Apr-93	Obsoleted by 1903
1444	Conformance statements for SNMPv2	Apr-93	Obsoleted by 1904
1445	SNMPv2 administrative model	Apr-93	Historic
1446	SNMPv2 security protocols	Apr-93	Historic
1447	SNMPv2 party MIB	Apr-93	Historic
1448	SNMPv2 protocol operations	Apr-93	Obsoleted by 1905
1449	SNMPv2 transport mapping	Apr-93	Obsoleted by 1906
1450	SNMPv2 MIB	Apr-93	Obsoleted by 1907
1451	Manger-to-manger MIB	Apr-93	Historic
1452	Coexistence of SNMPv1 and SNMPv2	Apr-93	Obsoleted by 1908
1901	Community-Based SNMPv2	Jan-96	Experimental
1902	SMIv2	Jan-96	Draft Standard
1903	Textual conventions for SNMPv2	Jan-96	Draft Standard
1904	Conformance statements for SNMPv2	Jan-96	Draft Standard
1905	Protocol operations for SNMPv2	Jan-96	Draft Standard
1906	Transport mapping for SNMPv2	Jan-96	Draft Standard
1907	SNMPv2 MIB	Jan-96	Draft Standard
1908	Coexistence of SNMPv1 and SNMPv2	Jan-96	Draft Standard
1909	Administrative infrastructure for SNMPv2	Feb-96	Experimental
1910	User-based security for SNMPv2	Feb-96	Experimental