Simple Network Management Protocol (SNMP)

Past — Present — Future ?

Jürgen Schönwälder

Institut für Betriebssysteme und Rechnerverbund
TU Braunschweig

Bültenweg 74/75
D-38106 Braunschweig, Germany

E-mail: schoenw@ibr.cs.tu-bs.de

The SNMP History:

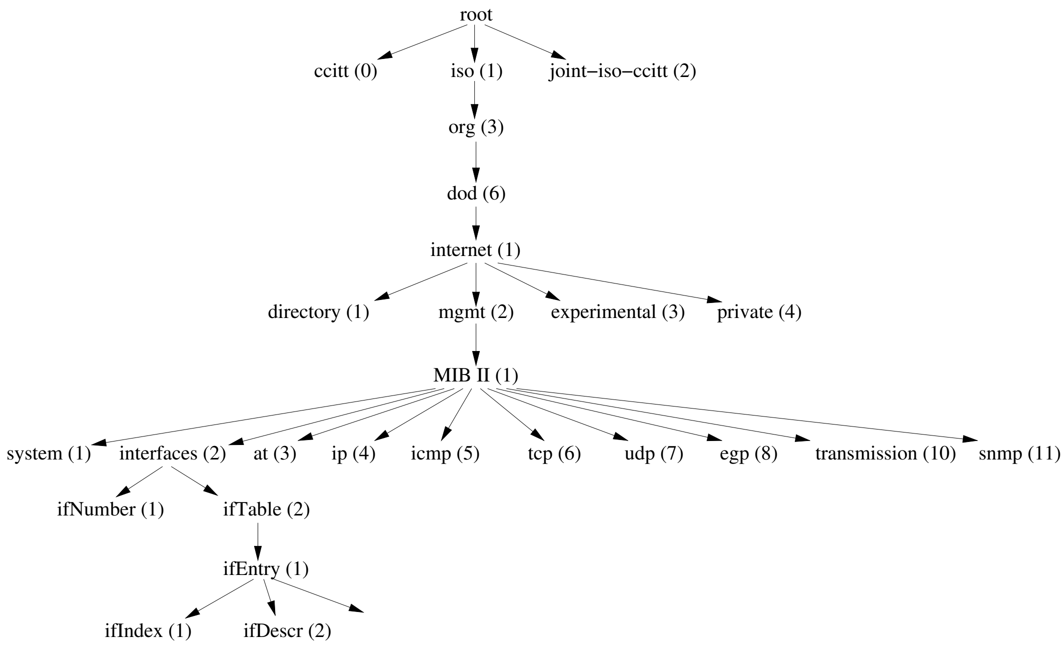
Date	Milestone	State	RFCs
October '87	High-level Entity Management System		1023
November '87	Simple Gateway Monitoring Protocol		1028
February '88	IAB SNMP Working Group		1052
August '88	First SNMP Specification		1065-1067
May '90	SNMP Version 1 (Community)	STD 15, 16	1155, 1157
March '91	Management Information Base II	STD 17	1213
April '93	SNMP Version 2 (P/P/C)	Historic	1441-1452
January '96	SNMP Version 2 (Community)	Draft*	1901-1908

Draft* = 1 Experimental (RFC 1901) + 7 Draft (RFC 1902-1908) Standards

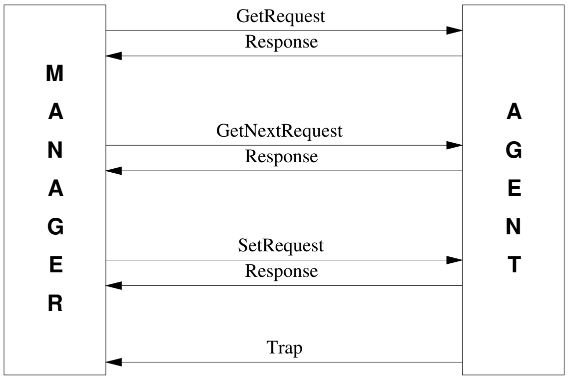
Outline of this talk:

- SNMP version 1 (SNMPv1) (full Internet standard)
- SNMP version 2 (SNMPv2) (draft Internet standard)
- Approaches to SNMP security (no standard yet)
- Agent extensibility (work in progress)
- Interesting MIB developments: (work in progress)
  - Entity MIB
  - RMON / RMON-2
  - ATM MIBs
  - Network information server MIB (HTTP, NNTP, FTP, ...)

SNMP Management Information Base (RFC 1213)



SNMPv1 operational model (RFC 1157)



- Minimize the number and complexity of management functions realized by the management agent itself.
- Trap-directed polling (agent sends traps and manager starts polling).
- Trivial authentication using plaintext community strings.

SNMPv1 message formats (RFC 1157)

SNMPv1 message

version	community	SNMP PDU

GetRequest, GetNextRequest, SetRequest PDU

PDU type	request−id	0	0	variable−bindings

GetResponse PDU

PDU type	request−id	error−status	error−index	variable−bindings

Trap PDU

PDU type	enterprise	agent−address	generic−trap	specific−trap	time−stamp	variable−bindings

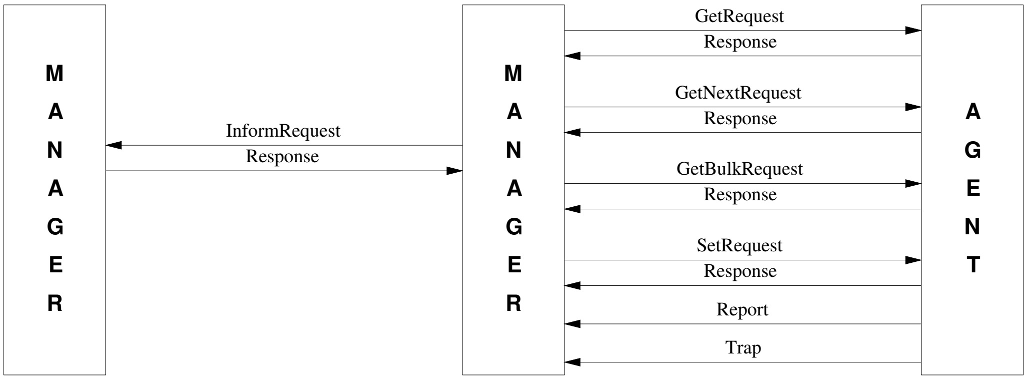
variable−bindings

name1	value1	name2	value2		name n	value n

Problems with SNMPv1 (RFC 1155, 1157)

- Lack of security makes SNMPv1 a simple network monitoring protocol.
- Poor performance when retrieving large tables.
- No support for communication between management applications.
- No standard way to create and delete rows in conceptual tables.
- No support to describe the conformance of agent implementations.

SNMPv2 operational model (RFC 1901-1908)



- InformRequest PDU to support manager ⟷ manager communication.
- GetBulk PDU to speed up MIB walks and table retrieval.
- Report PDU to be used internally by future security protocols.
- VarBind exceptions to handle non existing instances efficiently.

SNMPv2 message formats (RFC 1901-1908)

SNMPv2 message

version	community	SNMP PDU

GetRequest, GetNextRequest, SetRequest, Trap, InformRequest, Report PDU

PDU type	request−id	0	0	variable−bindings

Response PDU

PDU type	request−id	error−status	error−index	variable−bindings

GetBulkRequest PDU

PDU type	request−id	non−repeaters	max−repetitions	variable−bindings

variable−bindings

name1	value1	name2	value2		name n	value n

SNMPv2 SMI enhancements (RFC 1901-1908)

- Textual conventions allow application specific data types.
- Capability statements can be used to describe limitations of SNMP agents.
- MIB modules keep track of the revision history, contact information etc. and compliance macros define implementation requirements.
- Notification macro to describe the syntax and the semantics of a trap.
- Support for MIB table augmentation.
- 32 bit and 64 bit base data types (Counter64) for high-speed networks.
- RowStatus textual convention to create/delete rows.

Problems with SNMPv2 (RFC 1901-1908)

- Still no standard for secure SNMP operations.
- No clear definition how the InformRequest should be used.
- Some performance problems remain with large conceptual tables.
- No remote configuration MIB to configure SNMP agents via SNMP.
- No standard event filtering and forwarding MIB.

Goals of SNMP security:

Protection against the following security threads:

- modification of information
- masquerade
- message stream modification
- disclosure

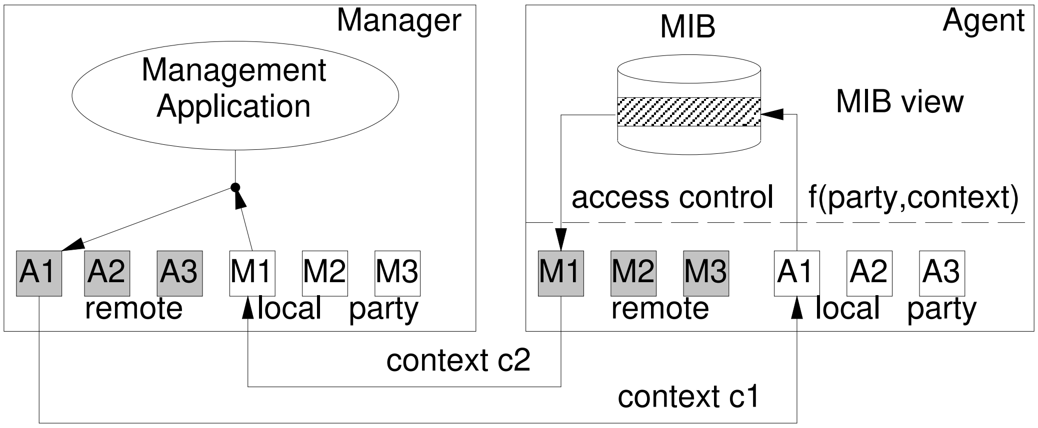
No protection against:

- denial of service attacks
- traffic analysis attacks

Mechanisms:

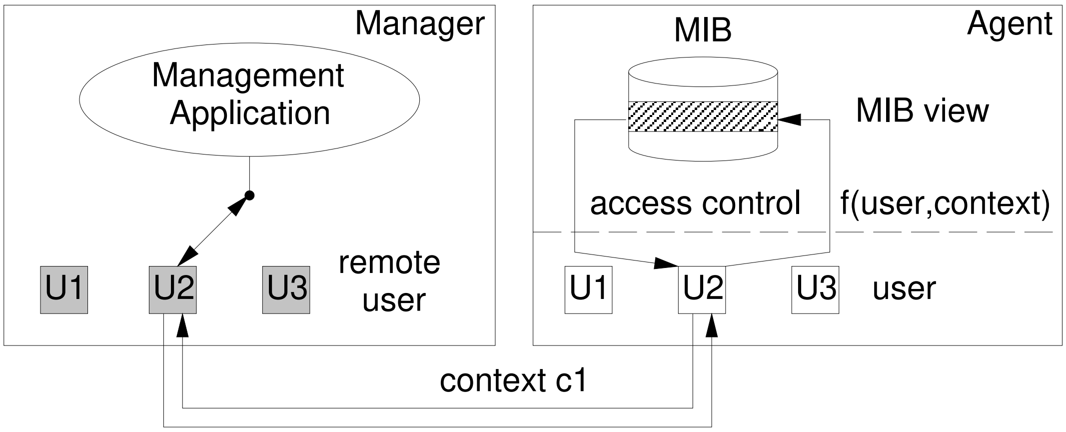
- digest authentication protocol (MD 5)
- symmetric encryption protocol (optional) (DES in CBC mode)

Party-based security (P/P/C) for SNMPv2 (historic)



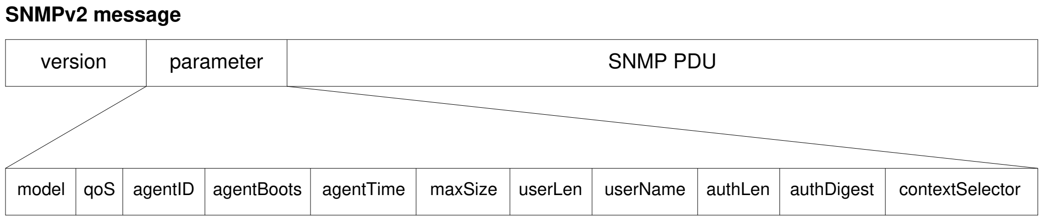
- Complex configuration (party information may not be shared).
- Slow and complex clock synchronization procedure.

User-based security (USEC) for SNMPv2 (draft)



- Efficient time synchronization and error handling using Report PDUs.
- Simple administration using well-known concepts: users and passwords.
- No changes to the SNMP message format.

SNMPv2 USEC message format (RFC 1910)



- The model parameter defines the security model and the qoS parameter the quality of service (authentication, privacy) required by a message.
- The agentBoots and agentTime provide an indication of time at the agent.
- The maximum message size (maxSize) accepted by the sender of a message.
- The length and value of the user name (userLen, userName).
- The length and value of the MD5 digest (authLen, authDigest).
- The contextSelector in combination with the agentID identifies the SNMPv2 context.

Comparison of the SNMP versions:

- SNMPv1 (RFC 1155, 1157):
  - Successful Internet standard and in widespread use today.
  - Modeling and performance problems, insecure.
- SNMPv2 (RFC 1901-1908):
  - Many good enhancements to SNMPv1, likely to get delivered by vendors.
  - Compatibility to SNMPv1 but still insecure.
- SNMPv2 USEC (RFC 1901-1910):
  - USEC on top of SNMPv2 solves most security problems at very low cost.
  - Remote configuration MIB still under development.
- SNMPv2 P/P/C (RFC 1441-1452):
  - Complex administrative model which is too complex to understand and use.
  - This is now a historic standard. ⇒ DO NOT USE !!!

Extensible agents (active working group)

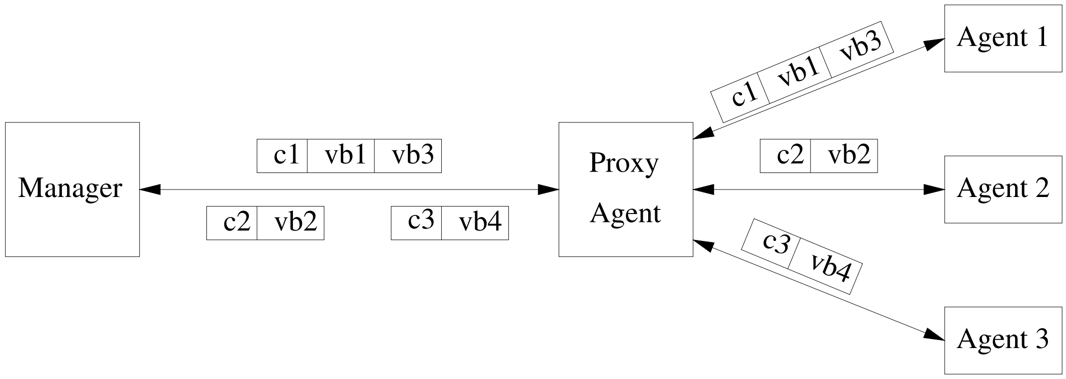
"The goal of this working group is to define standards-track technology for SNMP agent extensibility. The resulting technology specification will allow independently developed sub-agents to communicate with a master-agent running on an Internet device."

Agents need to be extensible for various reasons. Two examples:

- Hubs can be extended with new modules each providing its own SNMP interface.

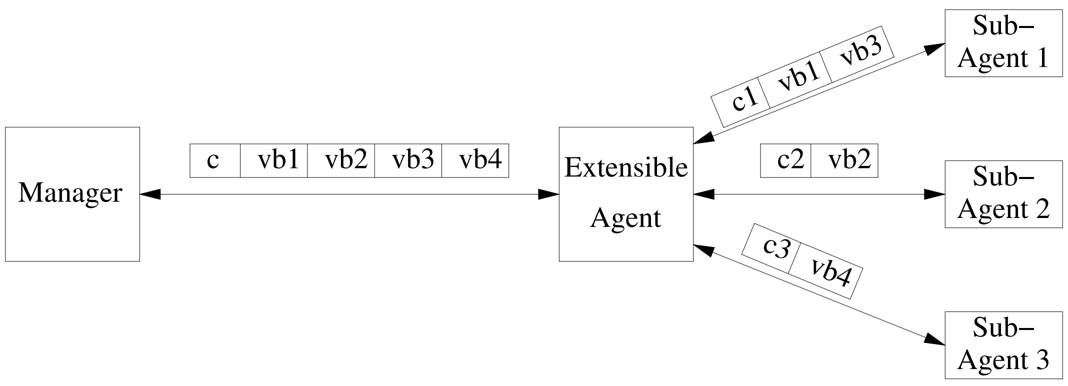
- Applications will provide their own management agents (e.g. SAP R3).

PDU multiplexing (proxy agent):



- PDU multiplexing based on community strings or context identifier.
- The contents of a PDU (varbind list) is never changed.
- Management application must be aware of proxy relationships.
- "As if simultaneous" semantics are easy to maintain, no discontinuity problems.

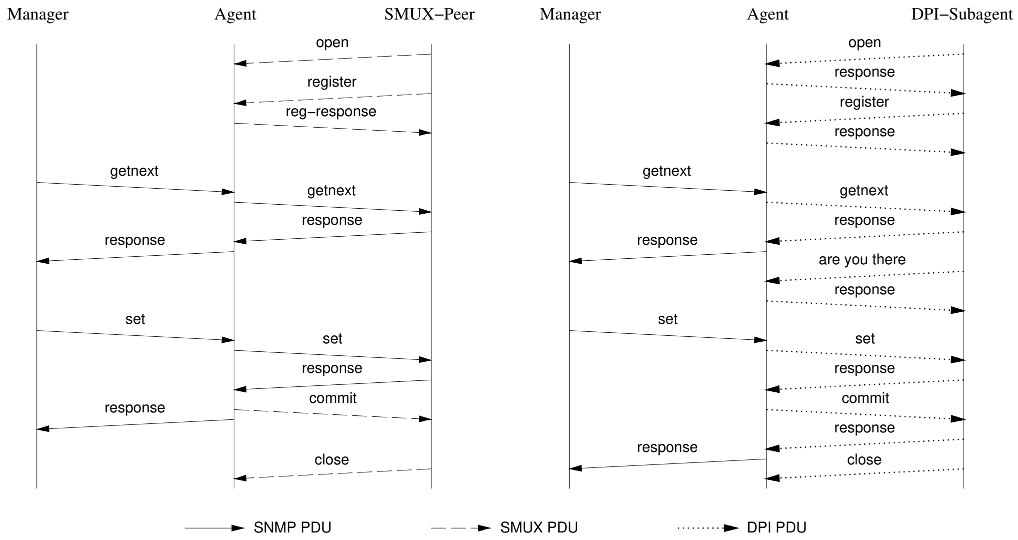
Varbind multiplexing (extensible agent):



- Sub-agents register MIB subtrees or single instances.
- Extensible agent protocol ensures "as if simultaneous" semantics.
- Counter discontinuities possible whenever an agent registers/unregisters.
- Management application talks to a single SNMP agent (transparency).

Existing extensible agent protocols:

SMUX (RFC 1227) DPI (RFC 1592)



Agent extensibility – some open issues:

- Should the intra-agent protocol use the SNMP message format?
- Instance registration versus subtree registration.
- How to support tables spread across many agents (efficiently)?
- How to solve indexing conflicts between multiple sub-agents?
- How many and which phases are needed to process SNMP set requests?
- How to resolve registration conflicts?

Entity MIB

The goal is to define a set of managed objects representing logical and physical entities and the relationships between them.

- Physical entities represent identifiable physical resources.
- Logical entities represent logical objects that allow management access.
- Each logical entity has an associated naming scope to access MIB objects (community string, transport address).
- The containment relationships between physical entities are expressed in a strict hierarchy (e.g. a Hub with 2 backplanes, various slots and network interfaces).
- Each logical/physical entity pair can have associated alias bindings (pointer to associated MIB instances).

Remote network monitoring (RMON / RMON-2)

RMON (RFC 1757)	Token Ring RMON (RFC 1513)	RMON-2 (working draft)
Ethernet Statistics	Token Ring Statistics	Protocol Directory
History Control	Token Ring History	Protocol Distribution
Ethernet History	Token Ring Ring Station	Address Mapping
Alarm	Token Ring Ring Station Order	Network Layer Host
Host	Token Ring Ring Station Config	Network Layer Matrix
HostTopN	Token Ring Source Routing	Application Layer Host
Matrix		Application Layer Matrix
Filter		User History
Packet Capture		Probe Configuration
Event		

RMON-2 TimeFilter tables:

Goal:

Reduce the number of SNMP transactions needed to monitor large tables.

Mechanism:

- Every row has an internal timestamp indicating the value of sysUpTime when the row was last updated.
- A manager passes a TimeFilter value as part of the index into the table.
- A row is in the MIB view if the associated timestamp is greater than the Time-Filter value contained in the request.

Effect:

A manager can restrict the MIB view to include only those rows that changed in the interval given by the TimeFilter value.

ATM management information base (AToMMIB)

ATM Supplemental MIB

- Provides ATM management information (e.g. for management of SVCs).

ATM Textual Convention and Object Identity MIB

- Provides textual conventions and object identities for ATM management.

ATM Testing MIB

- Provides ATM testing information.

ATM Accounting MIB

- New MIB that provides accounting information.

Network Information Server MIB

Network information server (e.g. HTTP, FTP) are typically monitored through vendor specific access and error log files. A standard network information server MIB should provide access to performance, error and access statistics in a uniform way.

- Basic request/response and error statistics.
- HTTP information server are the primary target.
- Information server with similar request/response protocols are taken into account.
- Access statistics to individual documents.

What is the future of SNMP management?

Scenario 1:

- The SNMPv2 protocol plus a standard security model plus some standard high-level MIBs are implemented in every Internet device and standard management applications allow cost-effective control.

Scenario 2:

- The “wars” on the security front continue and further attempts to define high-level MIBs fail because SNMP and its limited information model does not allow enough abstraction.

Scenario 3:

- SNMPv2 plus a standard security model make SNMP a successful element management protocol. Additional protocols will be used to implement high-level management facilities on top of it.