**SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)**

David Sánchez Rodríguez  
Department of Ingeniería Telemática  
University of Las Palmas de Gran Canaria  
Canary Islands, Spain  
dsanchez@dit.ulpgc.es

---

**Objectives**

- What is Network Management ?
- Network management protocols
- SNMP
  - Architecture
  - Operations
  - Versions

---

**Summary**

1. Introduction
   - Usually they are larger and many devices are used
   - Many users and many applications use them

2. Structure of Management Information (SMI)
3. MIB-II
4. SNMP v1
5. SNMP v2
6. SNMP v3
7. References

---

**1. Introduction**

- Networks are growing very fast:
  - Usually they are larger and many devices are used
  - Many users and many applications use them

- Management complex:
  - Heterogeneous network devices → Different configurations
  - It is necessary to learn configuration method of each network device
  - Network larger → Difficulties and problems increase

- It is necessary to use network management protocols for managing complex networks such that they provide services with high quality
1. Introduction

- ISO (International Organization for Standardization) defines five functional areas of network management:
  - Fault management
    - Detection, isolation and correction of abnormal operations
  - Accounting management
    - Supervise activities of users
  - Configuration management
    - Configure of network devices
  - Performance management
    - Monitor and control network performance
  - Security management
    - Access control to network resources

1. Introduction

- Network Management Protocols
  - Common Management Information Protocol (CMIP) (OSI Model)
    - Most complete but most complex and consumes large resources
  - Telecommunications Management Network (TMN)
    - Based on OSI network and for managing telecommunication networks
  - Web-Based Management
    - No standards exist. However two technologies are in vogue:
      - Web-Based Enterprise Management (WBEM)
      - Java Management Extensions (JMX)
  - Simple Network Management Protocol (SNMP) (Internet Model)
    - Easy to implement and most widely used

1. Introduction

- Why SNMP?
  - Simple protocol (based on polling and asynchronous messages)
  - Rapid development of standards (versions)
  - Devices management for IP networks (Internet)
  - Many and free distributions
  - Low overhead
  - Easy to configure
  - Easy to extend the capabilities for managing specific resources
  - Most of manufacturers embed a SNMP agent on their products

1. Introduction

- The evolution of SNMP
  - '87: Simple Gateway Monitoring Protocol (SGMP)
  - '90: SNMP (enhanced version of SGMP)
  - '92: S-SNMP and SMP (security and advanced operations)
  - '93: SNMPv2 (security)
  - '95: IETF orders a revision of SNMPv2 (Complicated security model)
  - '96: SNMPv2C (no security, trivial authentication)
  - '99: SNMPv3 (security based on users, encryption)
1. Introduction

**Basic Concepts**

- Management station
  - It is typically stand-alone device (may be replicated)
  - Application/s for data analysis, remote control, fault recovery,....
  - Normally named “Manager”
  - Interface between human network manager and managed systems
  - Usually it has a database with information extracted from MIB of managed devices

**RFCs:**
- RFC 1155: Structure of Management Information
- RFC 1213: Management Information Base II (MIB II)
- RFC 1157: SNMPv1
- RFC 1901 and 1905-07: SNMPv2
- RFC 2570-75: SNMPv3

**The model of network management for TCP/IP includes four elements:**
- Management station (runs a manager)
- Managed devices (runs an agent)
- Management Information Base (MIB)
- Network Management Protocol
1. Introduction

**Basic Concepts**

- Management Information Base (MIB)
  - Each aspect to manage is represented as an object (IP address, TCP connections, number of received TCP packets,...)
  - An object is a variable which stores a value
  - The collection of objects is referred as MIB
  - Objects are standardized for each device (a set of objects is used to manage routers, another for hubs,...)
  - Each agent manages and updates one MIB

By default, Gets and Sets are sent to UDP:161 and Traps via UDP:162

SNMP is an application-level protocol
- It operates over User Datagram Protocol (UDP)
- By default, Gets and Sets are sent to UDP:161 and Traps via UDP:162

Summary

1. Introduction
2. Structure of Management Information (SMI)
3. MIB-II
4. SNMP v1
5. SNMP v2
6. SNMP v3
7. References
2. Structure of Management Information

- RFC 1155 specifies the SMI
- Defines how MIBs have to be built
  - Language used (ASN.1 Abstract Syntax Notation One)
  - Structure (a tree for SNMP)
  - Object definition
- SMI does not support complex data structures
- MIBs only store simple data types: scalars and two-dimensional arrays of scalars
- MIB requisites:
  - Number of objects used to represent a particular aspect must be the same at each system
  - Same object must be defined equally in each system

MIB Structure

- All objects are arranged in a hierarchical or tree structure
- The leaves of tree represent the managed aspects (objects)

## MIB Structure

- Associated to each object there is a OBJECT IDENTIFIER (OID)
- OID names the object and it is a sequence of integers (from top of tree to object)
- There is an unique OID for each object

  - Internet OID: 1.3.6.1
  - mib-2 OID: 1.3.6.1.2.1

RFC 1155 defines the MIB basic structure for internet management

- Four nodes:
  - directory: reserved for use with OSI directory (X.500)
  - mgmt: used for objects defined by IAB (Internet Architecture Board)
  - experimental: used for experiments
  - private: used for objects defined by vendors. IANA (Internet Assigned Numbers Authority) assigns numbers to enterprises
Simple Network Management Protocol – April 06

2. Structure of Management Information

MIB Definition

new-mib  DEFINITIONS ::= BEGIN

import statements
module identity definition (SMIV2)
definition of all nodes and leaf objects
definition of notifications (traps)
END

IMPORTS

MODULE-IDENTITY, OBJECT-TYPE,
IpAddress, enterprises, ...
FROM SNMPv2-SMI

nodes, types, ...
FROM RFCs or MIBS
DisplayString
FROM SNMPv2-TC;

....

MIB Definition

Module identity definition

new-mib_module MODULE-IDENTITY
LAST-UPDATED "04042006"
ORGANIZATION "Grupo de Arquitectura y Concurrencia"
CONTACT-INFO
"David Sanchez
Phone: +34 928 458047
Fax: +34 928 451380
E-Mail: dsanchez@dit.ulpgc.es"

DESCRIPTION
"module example"
::= { previous_node number }

Managed Object Definition

It is defined with four parameters

OBJECT-TYPE:

INT32
OBJECT-IDENTIFIER
BIT
IpAddress
Counter32
Counter64
 Gauge32
Gauge64
Timeticks
Opaque

SYNTAX

read-only
read-write
read-write-for-notification
not-accessible

MAX-ACCESS

STATUS

deprecated
obsolete

DESCRIPTION

....
Simple Network Management Protocol – April 06

### 2. Structure of Management Information

**MIB Definition**

```plaintext
atTable OBJECT-TYPE
SYNTAX SEQUENCE OF atEntry
ACCESS not-accessible
STATUS deprecated
DESCRIPTION "The Address The Address Translation tables contain the NetworkAddress to 'physical' address equivalences."
 ::= { atEntry 3 }
```

**Table Definition (1)**

```plaintext
atTable
  atEntry
    atIfIndex  INTEGER, atPhysAddress  PhysAddress, atNetAddress  NetworkAddress
```

**Example:**

```
1
00:00:e2...
193.145.1...
```

**MIB Definition**

```plaintext
atEntry OBJECT-TYPE
SYNTAX AtnEntry
ACCESS not-accessible
STATUS deprecated
DESCRIPTION "Each entry contains one NetworkAddress to 'physical' address equivalence."
INDEX { atIfIndex, atNetAddress }
 ::= { atTable 1 }
```

**Table Definition (2)**

```plaintext
atEntry
  atIfIndex  INTEGER, atPhysAddress  PhysAddress, atNetAddress  NetworkAddress
```

**MIB Definition**

```plaintext
atPhyAddress OBJECT-TYPE
SYNTAX PhysAddress
ACCESS read-write
STATUS deprecated
DESCRIPTION "The ...
 ::= { atEntry 2 }
```

**Table Definition (3)**

```plaintext
atPhyAddress
  atIfIndex  INTEGER, atPhysAddress  PhysAddress, atNetAddress  NetworkAddress
```

**Example:**

```
... ... 193.145.1...
```
### 2. Structure of Management Information

#### MIB Definition

**Definition of non-leaf object (nodes)**

- name OBJECT IDENTIFIER ::= { previous_node number }

**Example:**

- mgmt OBJECT IDENTIFIER ::= { internet 2 }

**Definition of a notification (trap)**

- name_Notification NOTIFICATION-TYPE
  - STATUS current
  - OBJECTS { lbBatteryLevel, lbBatteryTime }
  - DESCRIPTION "A notification is sent when .."

### Summary

1. Introduction
2. Structure of Management Information (SMI)
3. MIB-II
4. SNMP v1
5. SNMP v2
6. SNMP v3
7. References
3. MIB-II

- It is a standard MIB
- Defined in RFC 1213
- Defines variables to manage TCP/IP protocol
- Under mgmt node
- Formed by ten nodes

3. MIB-II

- Information about each network interface

3. MIB-II

- Information about IP on the system
3. MIB-II

- Information about TCP on the system
  - tcp node
    - tcpRtoMax (3)
    - tcpPassiveOpens (6)
    - tcpAttemptFails (7)
    - tcpResets (15)
    - tcpRetransSegs (12)

- Information about UDP on the system
  - udp node
    - udpTable
      - udpOutDatagrams
        - udpLocAddress
        - udpLocalPort
      - udpInDatagrams
      - udpNoPorts
      - udpInErrors

Summary

1. Introduction
2. Structure of Management Information (SMI)
3. MIB-II
   4. SNMP v1
5. SNMP v2
6. SNMP v3
7. References

4. SNMP v1

- SNMP v1 is specified in RFC 1157
- Specifies:
  - Access control to MIB
  - Protocol specification
  - Other aspects (no outstanding)
Each agent controls its own MIB

Two aspects related to this control:
- Authentication service (To limit access to managers)
- Access policy (Different access privileges to different managers)

SNMP provides a simple and limited capability for access control (based on the concept of community)

SNMP community is a relationship between an Agent and set of Managers

Community is defined locally at the agent (it is a name)

Different agents can use the same community

Multiple communities can be defined in an agent

Each community establishes a combination of authentication and access control

Authentication service aspect:

Trivial scheme (not encryption)
- Every message from manager to agent includes a community name
- This name acts as password
- The message is assumed to be authentic if this name is equal to the community name fixed by agent

Access policy aspect:

For each community name, agent defines two aspects:
- MIB view: a subset of the managed objects within a MIB. Different MIB views may be defined for each community
- Access mode to MIB views: [READ-ONLY or READ-WRITE]
4. SNMP v1

Protocol specification

- Limited set of operations
- Manager:
  - GetRequest
  - GetNextRequest
  - SetRequest
- Agent:
  - Response
  - Trap

- We can query or set several objects invoking one operation
- Field Name has to specify an Instance
- Instance example:
  - Instance = OID + 
  - "column number" + "index value" for tables

- List of pairs of Name/value to query or set
- We can query or set several objects invoking one operation
- Field Name has to specify an Instance
- Instance = OID + 
  - ".0" for scalar
  - ".column number" + ".index value" for tables
- Instance example:
  - //sysContact OID: 1.3.6.1.2.1.4
  - //sysContact Instance: 1.3.6.1.2.1.4.0
4. SNMP v1

**Protocol specification**

- **GetRequest**
  - Request the value of 1 or more managed objects
  - Possible errors:
    - noSuchName → Object does not exist / Object is not a leaf
    - tooBig → Result does not fit in Response PDU
    - genErr → Other causes
  - No information is returned if some error occurs (atomic)
  - Examples:
    - `get (1.3.6.1.2.1.1.4.0) //sysContact` → Response ("David Sanchez")
    - `get (1.3.6.1.2.1.1.4.0, 1.3.5)` → Response (error-status=noSuchName; error-index = 2)

**SetRequest**

- Assign a value to an existing MIB object
- It is atomic (all values of variables bindings has to be set)
- Possible errors:
  - noSuchName → Object does not exist / Object is not a leaf
  - tooBig → Result does not fit in Response PDU
  - badValue → Inconsistency among OID and value
  - genErr → Other causes
- Examples:
  - `Set (1.3.6.1.2.1.1.4.0, "administrator") //sysContact`
  - `Response (1.3.6.1.2.1.1.4.0, "administrator")`

**Trap**

- Used to signal an event (asynchronously)
- Trap reception is not conformed
- Agent can be configured such that traps will be send to certain managers
- PDU Format:
4. **SNMP v1**

Protocol specification

- enterprises: identifies the system that generated the trap
- Agent-addr: IP address
- Generic-trap: one of seven predefined traps
- Specific-trap: code of specific trap (of a vendor device)
- Time-stamp: time
- Variable bindings: list of pairs OID/value enclosed to trap (additional information)

**Limitations of SNMPv1**

- Limited error codes
- Limited data types
- Large queries for retrieving large volumes of data
- Traps are unacknowledged
- No security, only trivial authentication
- No supports manager to manager communications

---

**Summary**

1. Introduction
2. Structure of Management Information (SMI)
3. MIB-II
4. **SNMP v1**
5. **SNMP v2**
6. **SNMP v3**
7. References

---

5. **SNMP v2**

- SNMPv2 is an extension of SNMPv1
- It is also based on community name (SNMP v1 access control)
- New types of PDUs operations
- Provides three types of access to management information:
  - Manager-agent: To query or modify values
  - Agent-manager: To send unsolicited message
  - Manager-manager: Communication among managers or between manager and agent acting in a manager role
5. SNMP v2

Protocol specification

- Manager:
  - GetRequest
  - GetNextRequest
  - GetBulkRequest
  - SetRequest
  - InformRequest
- Agent:
  - Response
  - SNMPv2 Trap

Protocol specification

- Message structure (include Trap)

<table>
<thead>
<tr>
<th>NAME</th>
<th>VALUE</th>
<th>NAME</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SNMP PDU:

- PDU Type
- Request ID
- Error Status
- Error Index
- Variable Bindings

SNMP message:

- Version
- Community
- SNMP PDU

- It is identical in format and semantics to SNMPv1 GetRequest
- Variable-bindings list is prepared even if values cannot be supplied
- Handles two exceptions:
  - NoSuchObject (OID does not match)
  - NoSuchInstance (Instance does not match)
- Exceptions are encoded within the variable bindings

get (1.3.6.1.2.1.4.0) → Response (error-status, "noError", 1.3.6.1.2.1.4.0, "David Sanchez")

get (1.4.0) → Response (error-status, "noError", 1.4.0, "noSuchObject")
5. SNMP v2

- Protocol specification
- GetNextRequest

- It is identical in format and semantics to SNMPv1 GetRequest
- Variable-bindings list is prepared even if values cannot be supplied
- Handles one exception:
  - endOfMibview
- Exceptions is encoded within the variable bindings

\( \text{get (1.4.0) \rightarrow Response (error-status, "noError", 1.4.0, "endOfMibView")} \)

5. SNMP v2

- Protocol specification
- GetBulkRequest

- New in SNMPv2
- Minimizes the number exchanges to query a large amount of data
- Improves the performance
- Has two additional parameters:
  - Non-repeaters
  - Max-repetitions
- PDU format:

<table>
<thead>
<tr>
<th>PDU type</th>
<th>Request id</th>
<th>Non-repeaters (n)</th>
<th>Max-repetitions (m)</th>
<th>Variable bindings</th>
</tr>
</thead>
</table>

- Operation:

  - The first \( N \) elements (non-repeaters) of the variable bindings are treated as GetNextRequest operation

  - The next elements of the variable bindings are treated as if the operation consisted of a number (\( M \) max-repetitions) of repeated GetNextRequest operations
5. SNMP v2

Protocol specification

GetBulkRequest

GetBulk (non-repeaters=1, max-repetitions=2, 1.3.6.1.2.1.1.2.0, 1.3.6.1.2.1.1.4.0, 1.3.6.1.2.1.1.10)

Response (1.3.6.1.2.1.1.3.0 \(\rightarrow\) 0:10:25, 1.3.6.1.2.1.1.5.0 \(\rightarrow\) DEBIAN, 1.3.6.1.2.1.1.6.0 \(\rightarrow\) Laboratorio, 1.3.6.1.2.1.1.2.0 \(\rightarrow\) its value, 1.3.6.1.2.1.1.3.0 \(\rightarrow\) its value)

---

Protocol specification

SetRequest

- It is identical in format and semantics to SNMPv1 SetRequest
- Two phases
  - Checks/Validates each pair name/value
  - If all validated, performs SET operation
- Atomic (all sets must be done for returning information)
- Many new error codes

---

Protocol specification

SNMPv1

SetRequest

SNMPv2

PHASE 1:
- badValue
- badValue
- badValue
- badValue
- badValue
- notObject
- notObject
- notObject
- genErr
- genErr

PHASE 2:
- genErr
- genErr

SNMPv2 Trap

- Different format to SNMPv1 Trap
- Same format to other SNMPv2 operations
- No response from manager
- Two specific name/value are added to two first pairs of variable bindings
  - sysUptime (time from agent starts to now)
  - snmpTrapOID (OID of notification)
- Rest of list can be completed by other name/value
5. SNMP v2

- New in SNMPv2
- Same format as SNMPv2 Trap
- There is response from manager (confirmed trap)
- Possible error: tooBig

6. SNMP v3

- Two Main Key features:
  - Architecture
    - Integrates SNMPv1 and SNMPv2 specifications
    - Design for future extensions
    - Same architecture in all systems (managed and management stations)
    - Divided in two components:
      - SNMP engine (equal for all devices)
      - SNMP applications (Depending on functionality has specific modules)
  - Security
    - Security model based on users
    - Encryption/Decryption
6. SNMP v3

**Security and Access Control**

- Based on secret keys shared by users (login/password)
- Uses MD5 and SHA algorithms (hash functions) for authentication
- Uses DES (Data Encryption Standard) algorithm for encryption/decryption
- Access Control based on Views
  - Access Control Table
  - For each MIB view is specified
    - allowed users
    - allowed operations
    - Required security level (authentication, encryption)
## Summary

1. Introduction
2. Structure of Management Information (SMI)
3. MIB-II
4. SNMP v1
5. SNMP v2
6. SNMP v3
7. References

## References

- Books:
  - “Network Management: Principles and Practice”, Mani Subramanian, Addison-Wesley, 2000
  - “SNMP, SNMPv2 and RMON”, William Stallings, Addison-Wesley, 1997
- Useful Links:
  - [http://www.net-snmp.org](http://www.net-snmp.org) (Most used distribution)
  - [http://www.mg-soft.com](http://www.mg-soft.com) (Applications, APIs for windows)
  - [http://www.snmplink.org/](http://www.snmplink.org/)

---

**Thank you for your attention**