
# Simple Network Management Protocol

SNMP

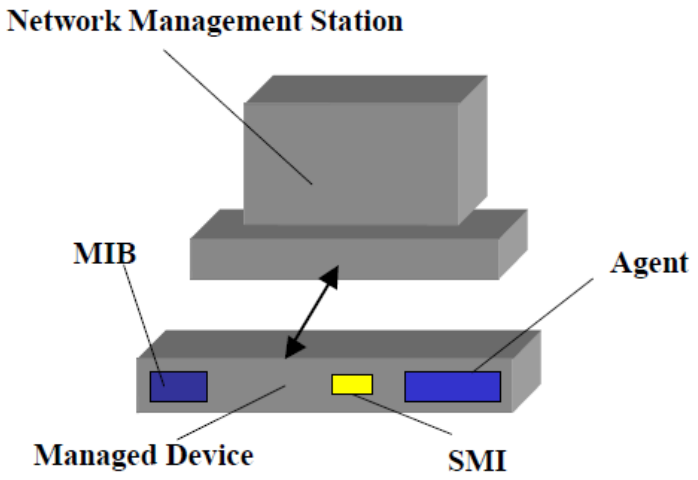
# Introduction

- The Simple Network Management Protocol (SNMP) Internet-standard protocol (application layer protocol)
- Used for managing devices on IP networks.
- Prior to SNMP, administrators would have to be physically attached to network devices in order to access configuration and troubleshooting data.
- Using SNMP provides standardization to reduce the complexity of network management..
- Devices that typically support SNMP include
  - routers
  - switches
  - servers
  - workstations
  - printers
  - modem racks, and more

# SNMP Components

- The SNMP has three basic components:

1. the Structure of Management Information (SMI),
2. the Management Information Base (MIB)
3. and the SNMP agents



# the Structure of Management Information (SMI)

- The SMI defines the data types that are allowed in the MIB.
- It sets aside a unique naming structure for each managed object.
- Typically MIB objects have six attributes.

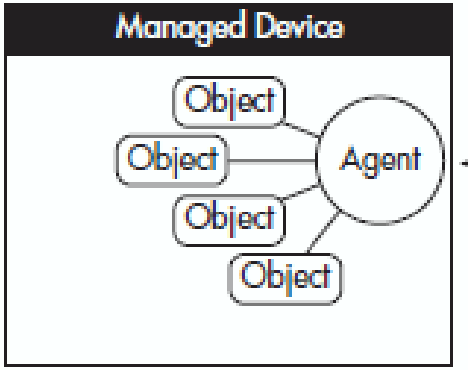
1. a name
2. an object identifier
3. an access field (The access mode of an object: read only – read-write ..)
4. and a text description

# Management Information Base (MIB)

- The MIB is a collection of network information.
- This information is stored in a database of managed objects that can be accessed using SNMP.
- The MIB is organized into a tree-like hierarchy
- A managed object represents a characteristic of a certain managed device.
- Ex of objects associated to a router in the network:
  1. Object 1 store a value of number of inbound packets to the corresponding device.
  2. Object2 store a value of clock ticks in the corresponding device .

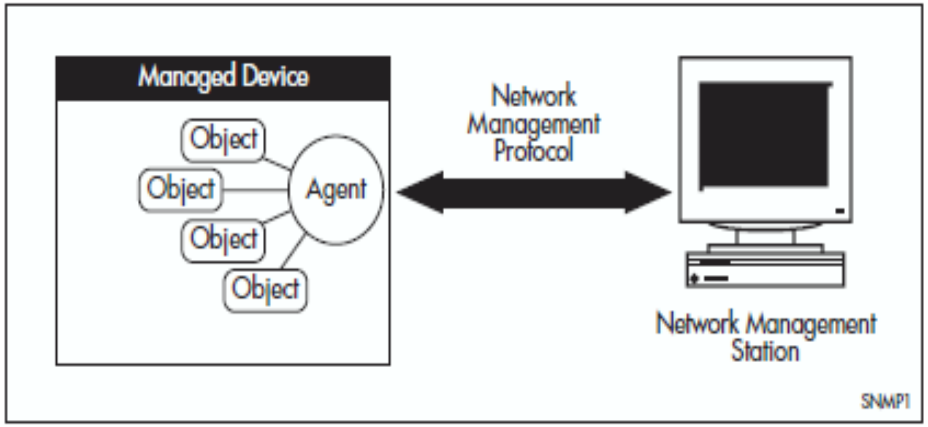
# SNMP Agent

- All network devices that are to be SNMP managed need to be fitted with an agent that executes all the MIB objects that are relevant.
- The agent provides the information contained in the MIB to management applications when asked



# SNMP

- The SNMP protocol provides a mechanism for management entities, or stations, to extract information from MIB of a managed device.
- SNMP access information in a MIB through Network Management Station (NMS) to send commands to the managed device .



# Implementation

- Architecture

An SNMP-managed network includes

1. management stations
2. network devices.

- The management stations execute SNMP which monitor network performance.
- Network agents are responsible for maintaining network statistics for management stations.
- When asked, each managed network device is expected to communicate such information for processing.

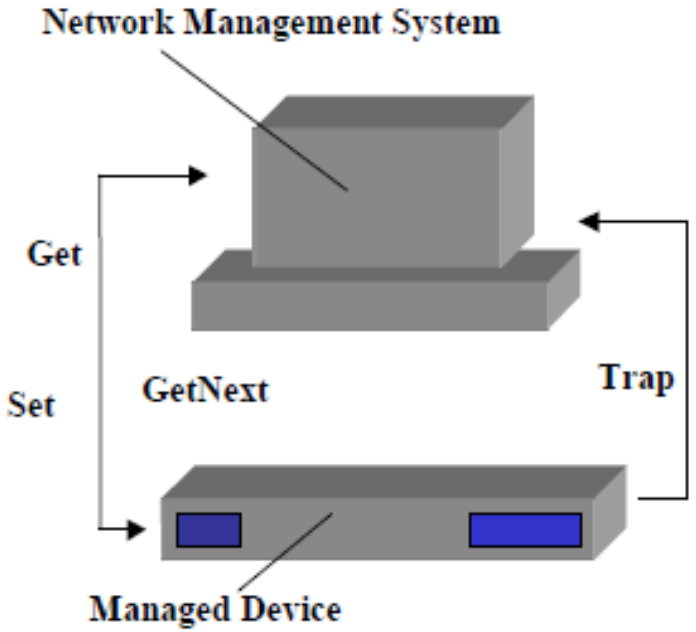
# Implementation

- Architecture
- SMI enables a vendor to write an SMI-compatible management object.
- This object is run through a MIB compiler to create an executable code.
- The code is installed in network devices and management consoles that in turn generate network reports.

# Initial network SNMPv1 Protocol Operations

- The most basic operations include: **Get, GetNext, Set,** and **Trap**
- **Get** is used by the SMI to retrieve the value of an object instance from an agent.
- **GetNext** is used by the SMI to retrieve the value of the next object instance from a table within an agent.
- The **Set** function is used to write a value to an object instance within an agent.
- **Traps** are used by agents to send information to the network management system.

# Initial network SNMPv1 Protocol Operations



# SNMP Versions

- Versions : SNMP version 1 (SNMPv1), SNMP version 2c (SNMPv2c) and SNMP Version 3 (SNMPv3).
- The three versions operate similarly.
- Security has been a big concern with SNMPv1 and SNMPv2. an unauthorized user could execute network management functions. This had led many operations to have read-only capability.
- SNMPv3 provides significant enhancements to address the security weaknesses existing in the earlier versions.
- This is achieved by implementing two new major features:
  - Authentication - by using password hashing and time stamping.
  - confidentiality - by using message encryption

# SNMP (1-2) message format

- Version :
  - 0 → SNMPv1
  - 1→ SMNPv2
- Community :The name of an SNMP community, for authentication purposes.
- SNMP PDU :An SNMP Protocol Data Unit (PDU). i.e. operation : get, set..

# SNMP Communities (Version v1 and v2c)

- A community is a relationship between an NMS and an agent. The community name is used like a password for a trivial authentication scheme.
- Both SNMPv1 and SNMPv2c provide security based on the community name only.
- The concept of communities does not exist for SNMPv3, which instead provides for a far more secure communications method using *entities*, *users* and *groups*.

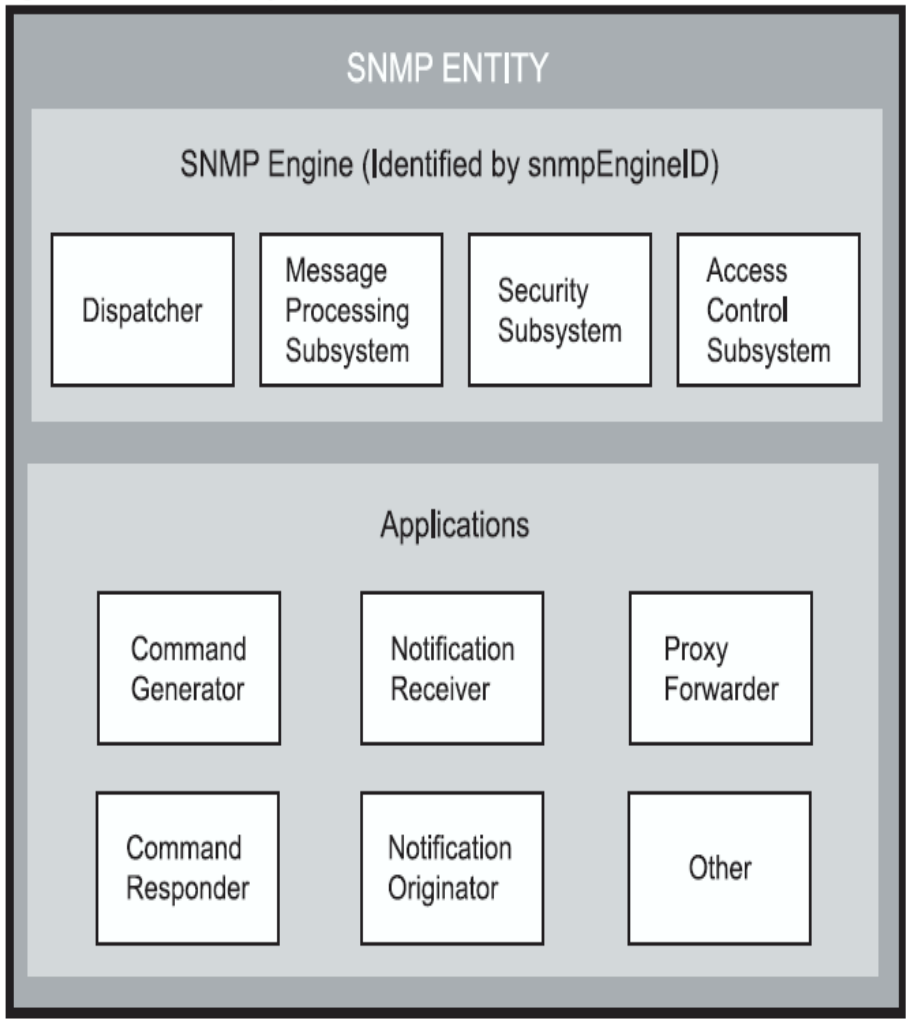
# SNMPv3 Entities

- Entities comprise one of the basic components of the SNMPv3 enhanced architecture.
- They define the functionality and internal structure of the SNMP managers and agents.
- SNMPv3 defines two entity types

1. a *manager* and
2. an *agent*.

- Both entity types contain two basic components:

1. an *SNMP engine*
2. and a set of *applications*.

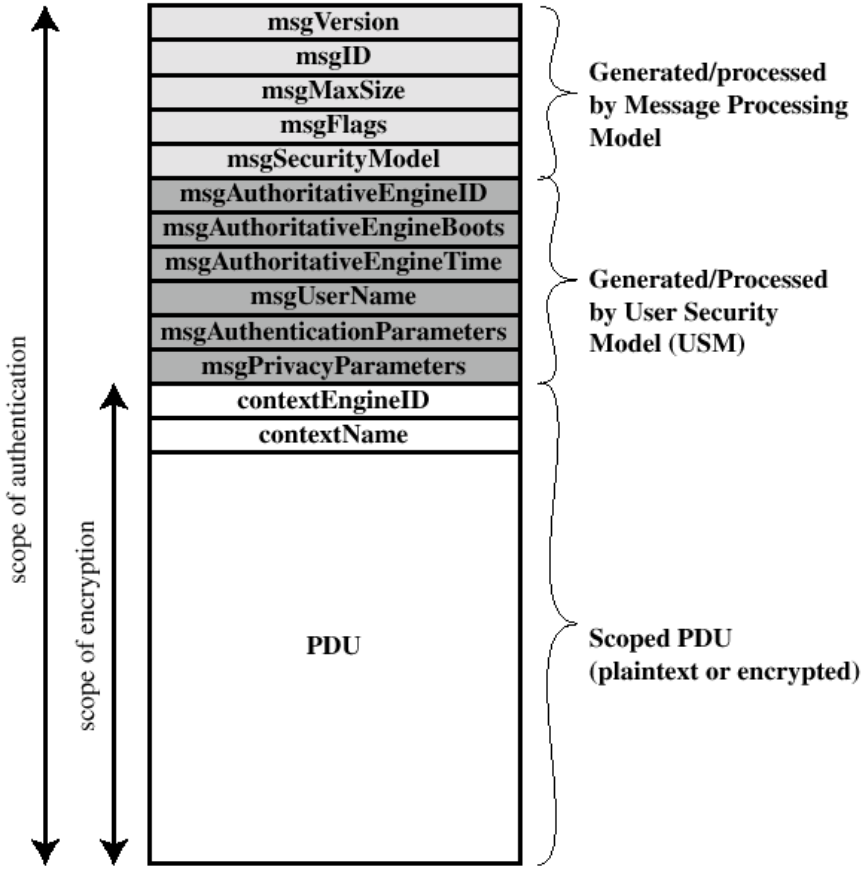


# SNMP Engine

- The engine provides the basic services to support the agents component applications such as

1. Message transmission and reception,
2. authentication and encryption
3. and access control to its (MIB).

# SNMP v3 message format




| | |
|---|---|
| msgAuthoritativeEngineID | The ID of the authoritative engine that relates to a particular message, i.e. the source engine ID for Traps, Responses and Reports, and the destination engine for Gets, GetNexts, Sets, and Informs. |
| msgAuthoritativeEngineBoots | A value that represents the number of times the authoritative engine has rebooted since its installation. Its value has the range 1 to $2^{31}$-1. |
| msgAuthoritativeEngineTime | The number of seconds since the authoritative engine snmpEngineBoots counter was last incremented. |
| msgUserName | The name of the user (principal) on whose behalf the message is being exchanged. |
| msgAuthenticationParameters | If the message has been authenticated, this field contains a serialized OCTET STRING representing the first 12 octets of the HMAC-MD5-96 output done over the whole message. |
| msgPrivacyParameters | For encrypted data, this field contains the "salt" used to create the DES encryption Initialisation Vector (IV). |
| ContextEngineID | Within a particular administrative domain, this field uniquely identifies an SNMP entity that may realize an instance of a context with a particular contextName. |
| ContextName | A unique name given to a context within a particular SNMP entity. |

# References

- Book “**AR400 Series Router Software Reference” chapter “AR400 Series Router Software Reference”.**
- **White paper from Asante.com**