Chapter 8

Network Management Security

Henric Johnson

Blekinge Institute of Technology, Sweden

http://www.its.bth.se/staff/hjo/

henric.johnson@bth.se

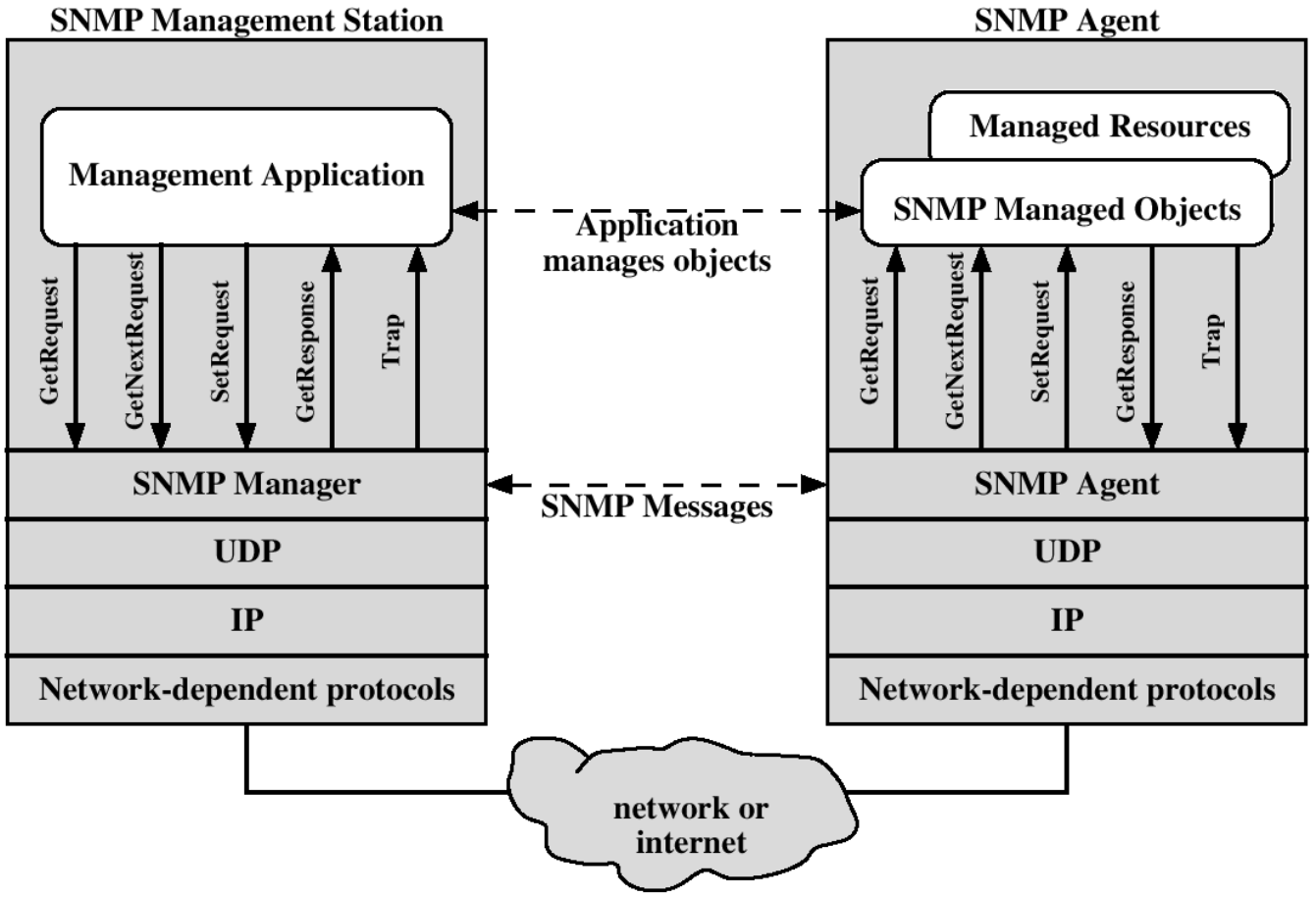
Outline

- Basic Concepts of SNMP
- SNMPv1 Community Facility
- SNMPv3
- Recommended Reading and WEB Sites

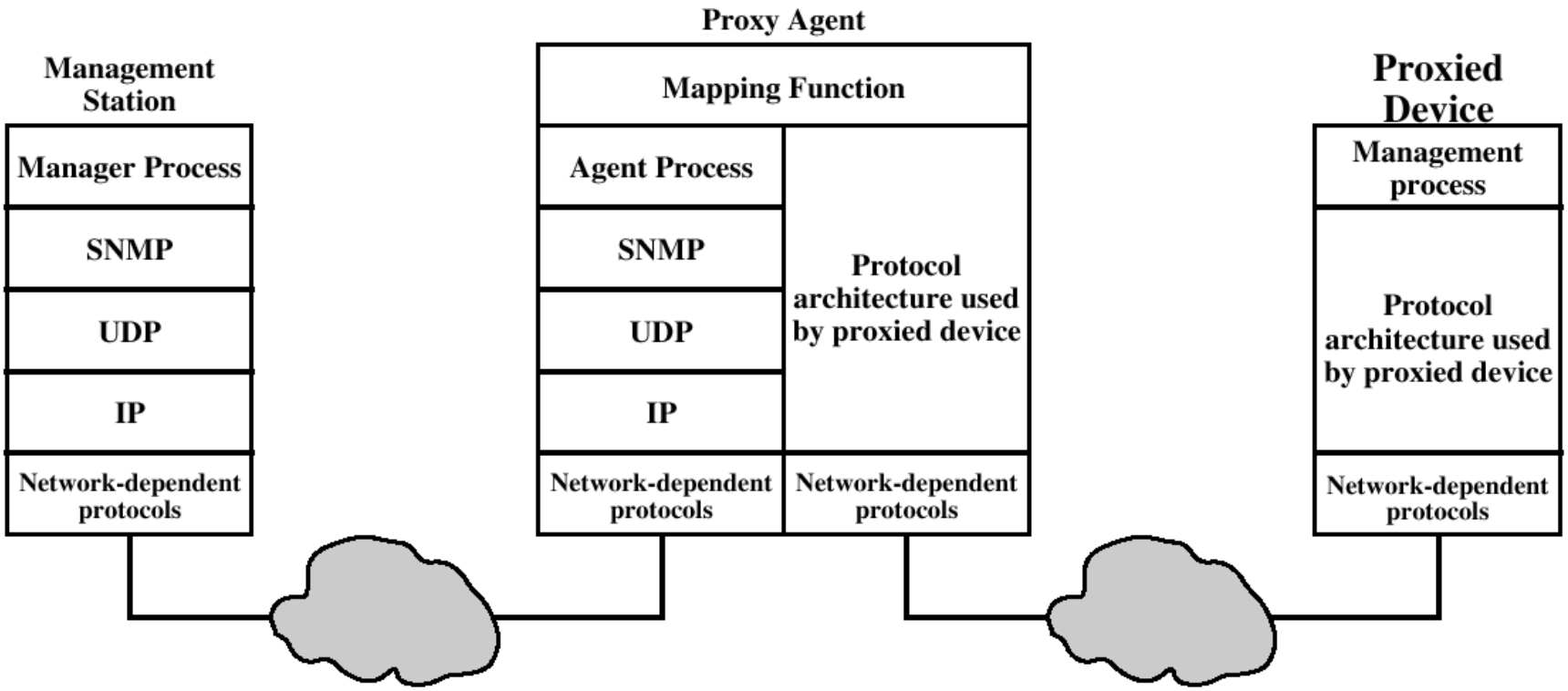
Basic Concepts of SNMP

- An integrated collection of tools for network monitoring and control.
  - Single operator interface
  - Minimal amount of separate equipment. Software and network communications capability built into the existing equipment
- SNMP key elements:
  - Management station
  - Managament agent
  - Management information base
  - Network Management protocol
    - Get, Set and Notify

Protocol context of SNMP



Proxy Configuration



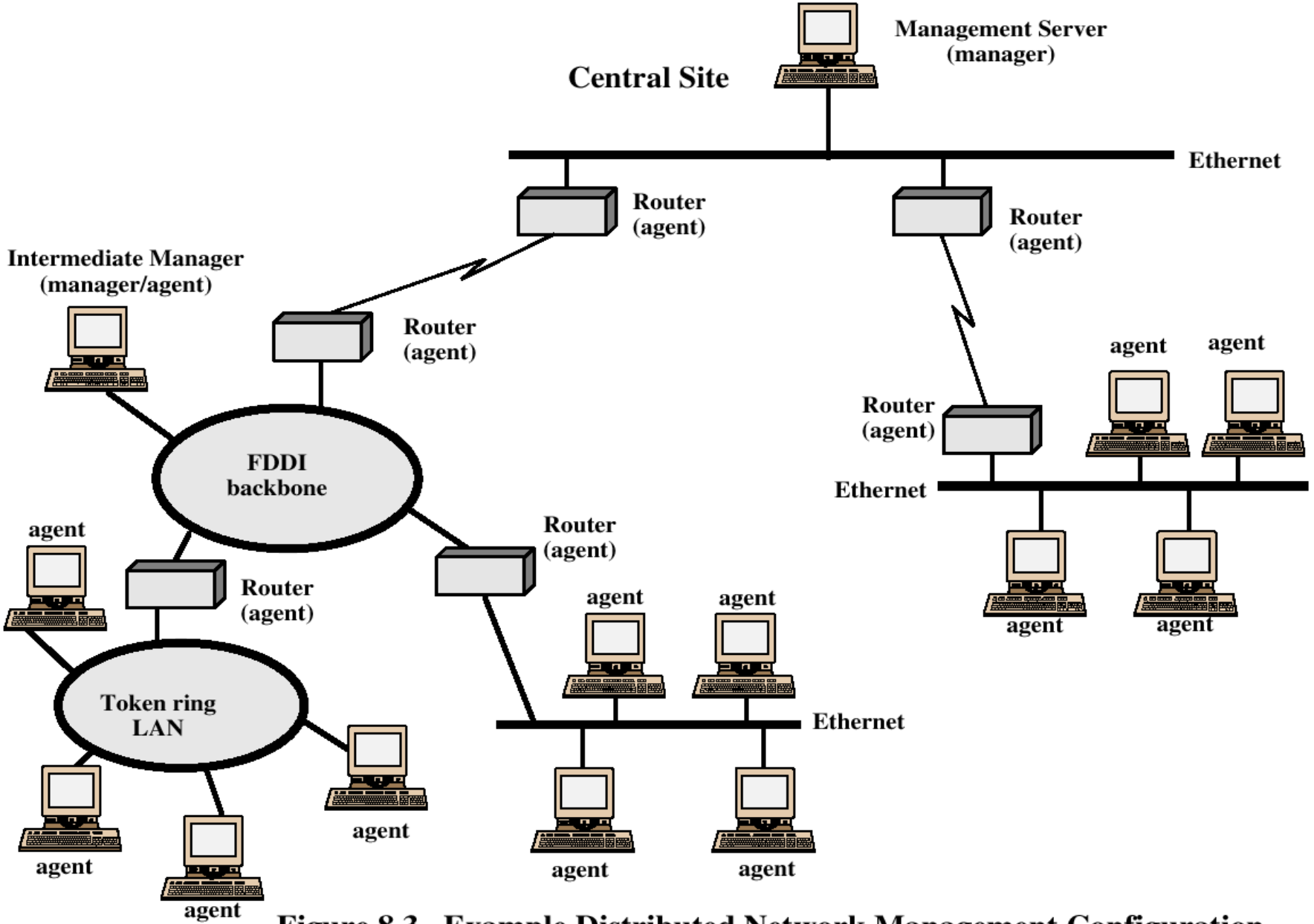


Figure 8.3 Example Distributed Network Management Configuration

SNMP v1 and v2

- Trap – an unsolicited message (reporting an alarm condition)
- SNMPv1 is "connectionless" since it utilizes UDP (rather than TCP) as the transport layer protocol.
- SNMPv2 allows the use of TCP for "reliable, connection-oriented" service.

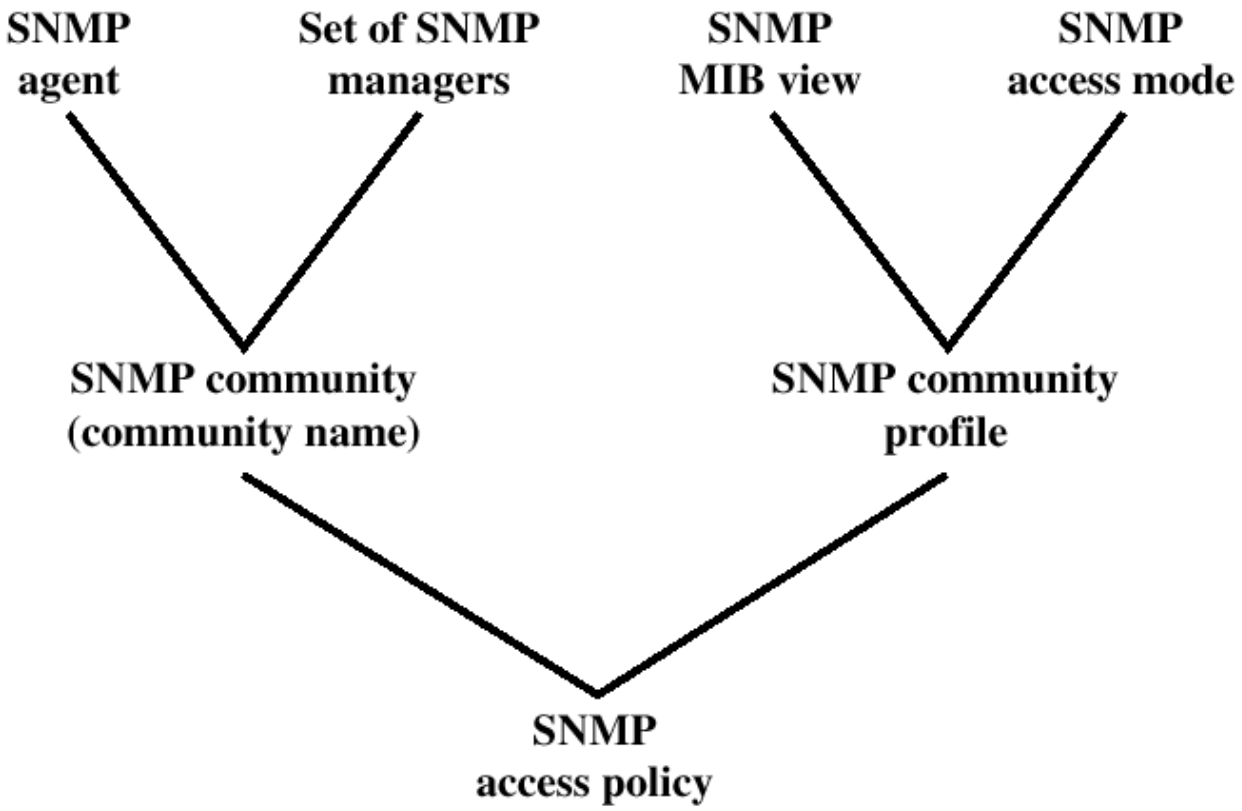
Comparison of SNMPv1 and SNMPv2

SNMPv1 PDU	SNMPv2 PDU	Direction	Description
GetRequest	GetRequest	Manager to agent	Request value for each listed object
GetRequest	GetRequest	Manager to agent	Request next value for each listed object
------	GetBulkRequest	Manager to agent	Request multiple values
SetRequest	SetRequest	Manager to agent	Set value for each listed object
------	InformRequest	Manager to manager	Transmit unsolicited information
GetResponse	Response	Agent to manager or Manage to manager(SNMPv2)	Respond to manager request
Trap	SNMPv2-Trap	Agent to manager	Transmit unsolicited information

SNMPv1 Community Facility

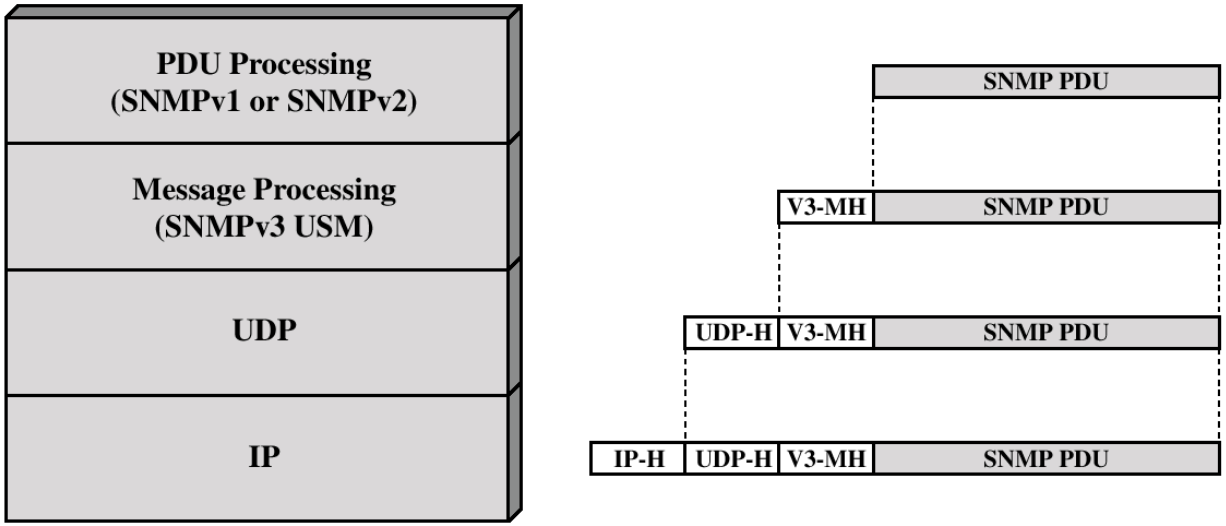
- SNMP Community – Relationship between an SNMP agent and SNMP managers.
- Three aspect of agent control:
  - Authentication service
  - Access policy
  - Proxy service

SNMPv1 Administrative Concepts



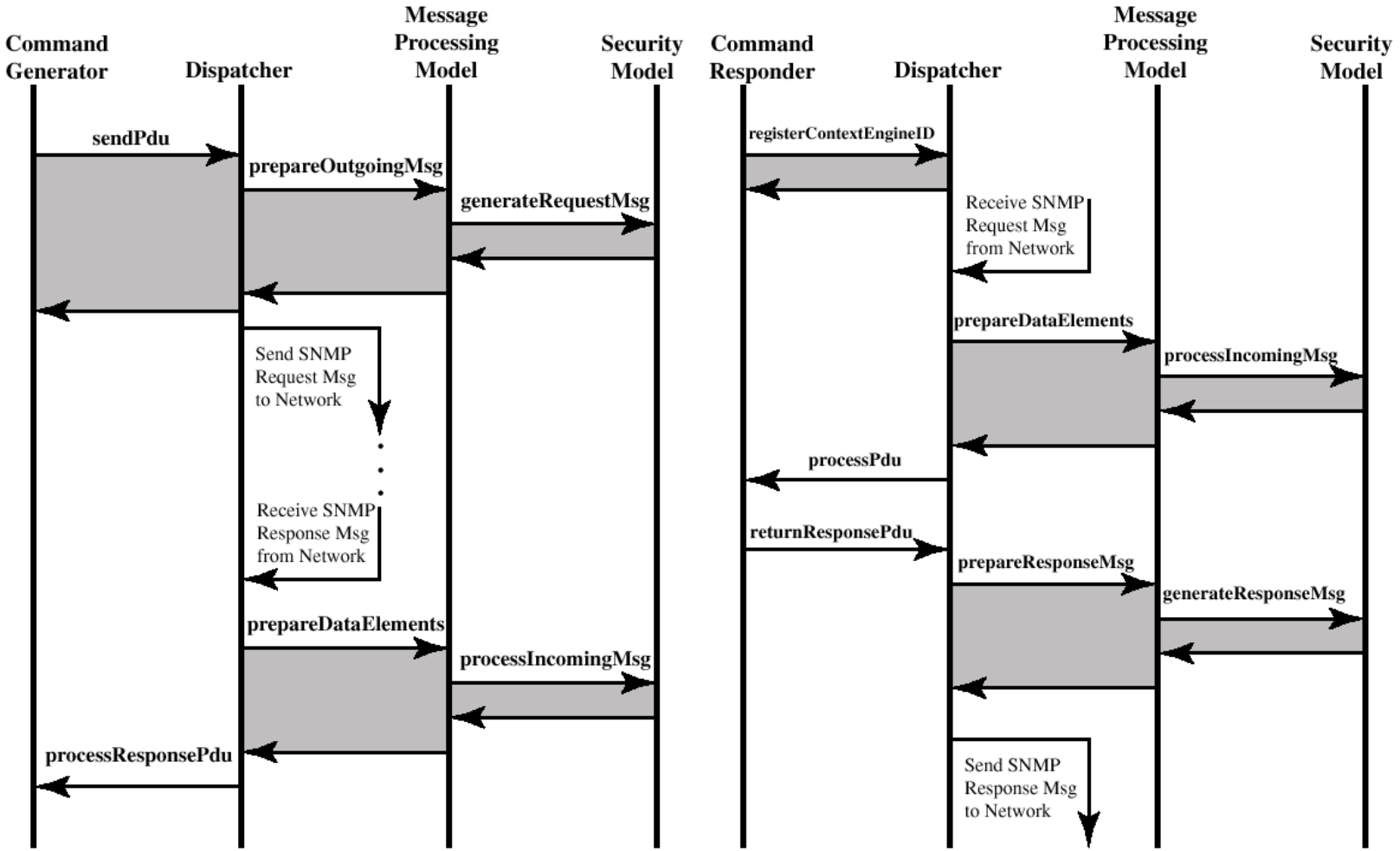
SNMPv3

- SNMPv3 defines a security capability to be used in conjunction with SNMPv1 or v2



IP-H = IP header
UDP-H = UDP header
V3-MH = SNMPv3 message header
PDU = Protocol data unit

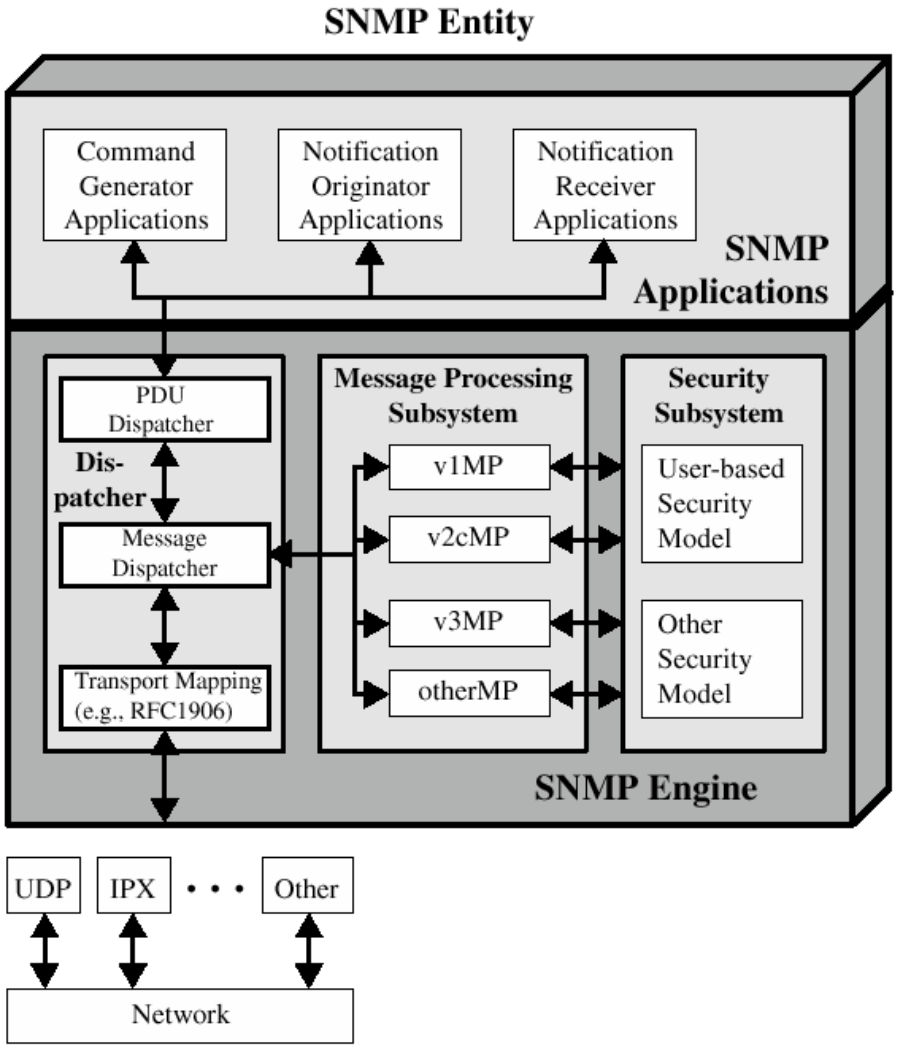
SNMPv3 Flow



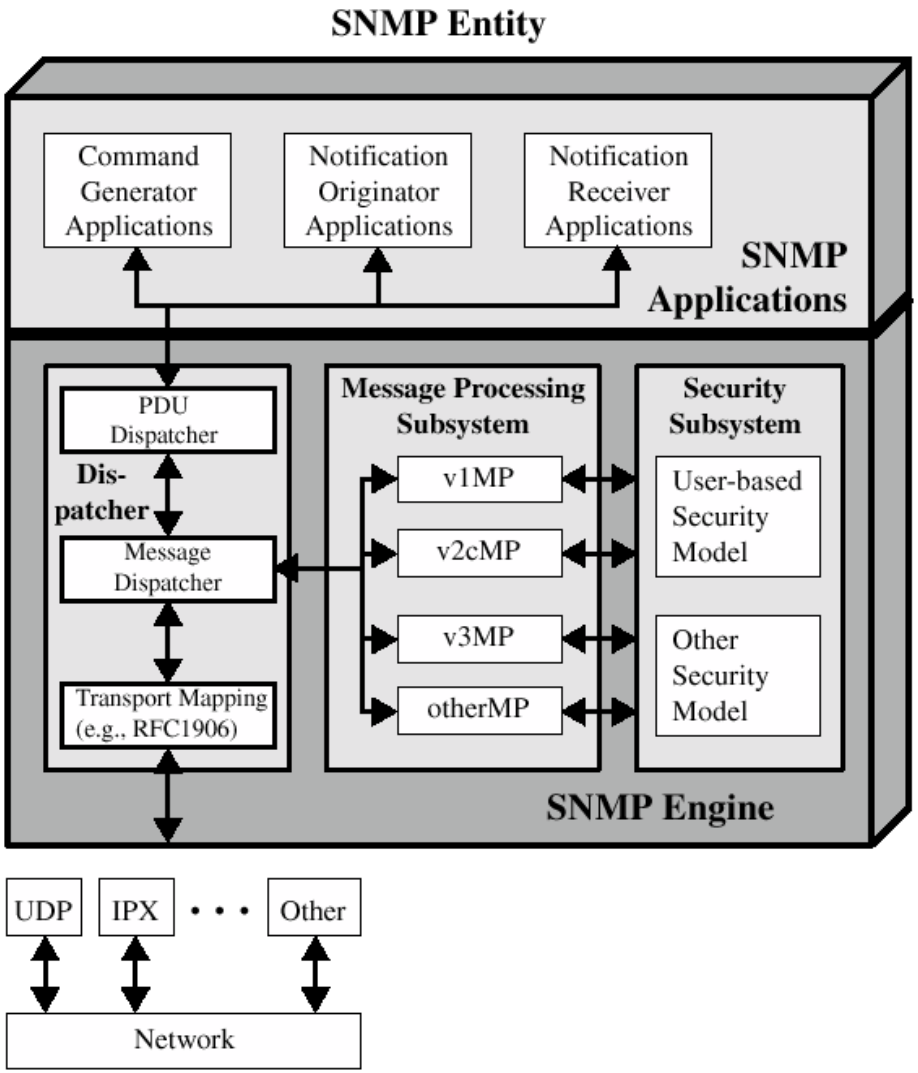
(a) Command Generator or Notification Originator

(b) Command Responder

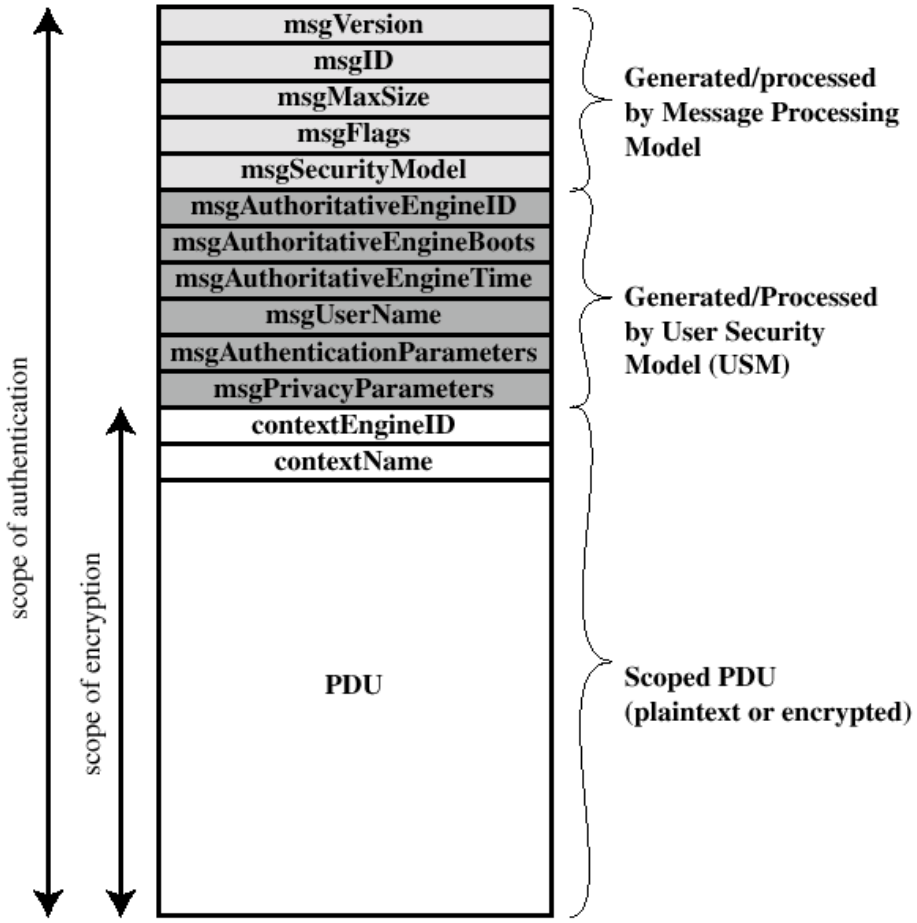
Traditional SNMP Manager



Traditional SNMP Agent



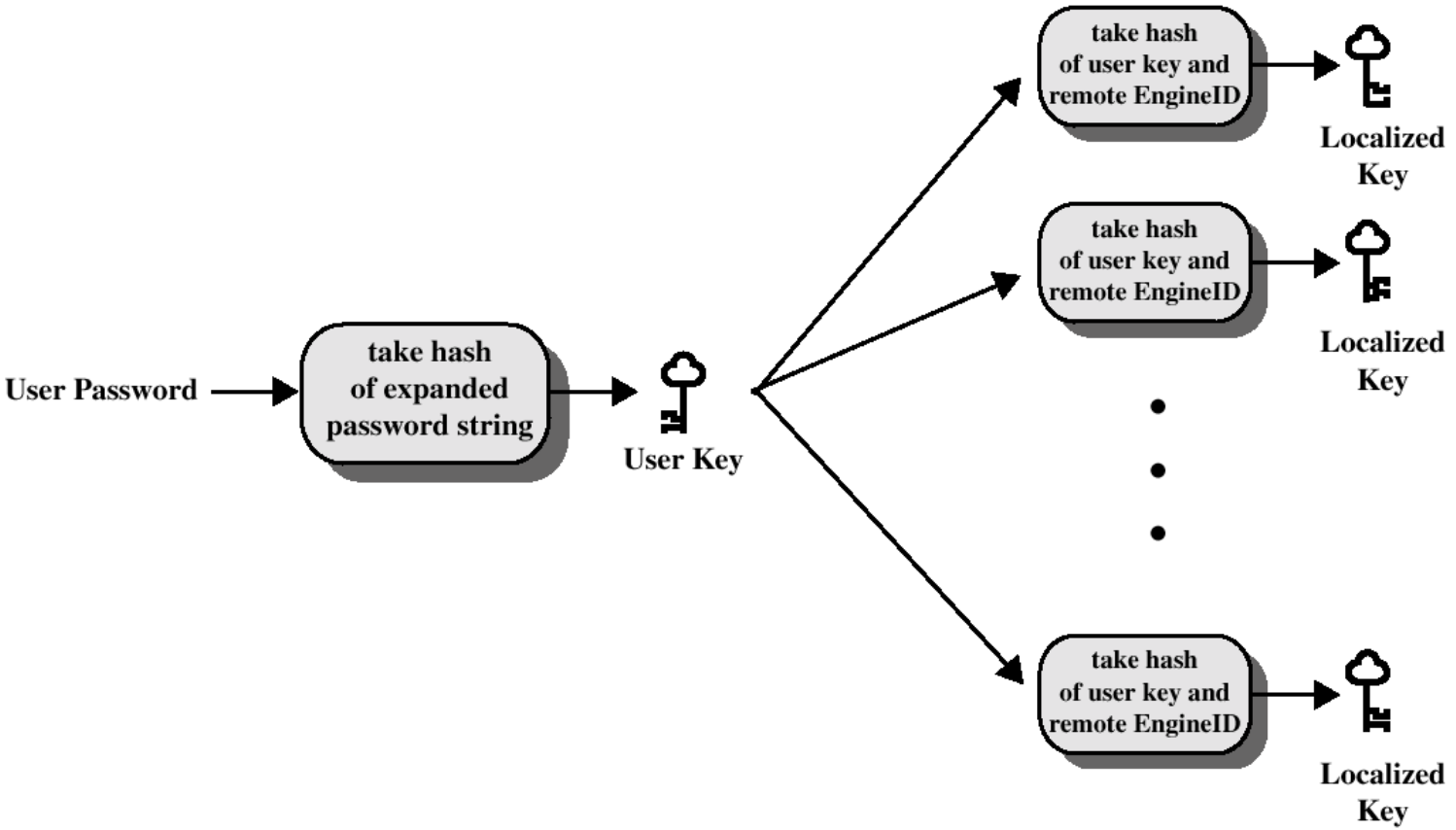
SNMP3 Message Format with USM



User Security Model (USM)

- Designed to secure against:
  - Modification of information
  - Masquerade
  - Message stream modification
  - Disclosure
- Not intended to secure against:
  - Denial of Service (DoS attack)
  - Traffic analysis

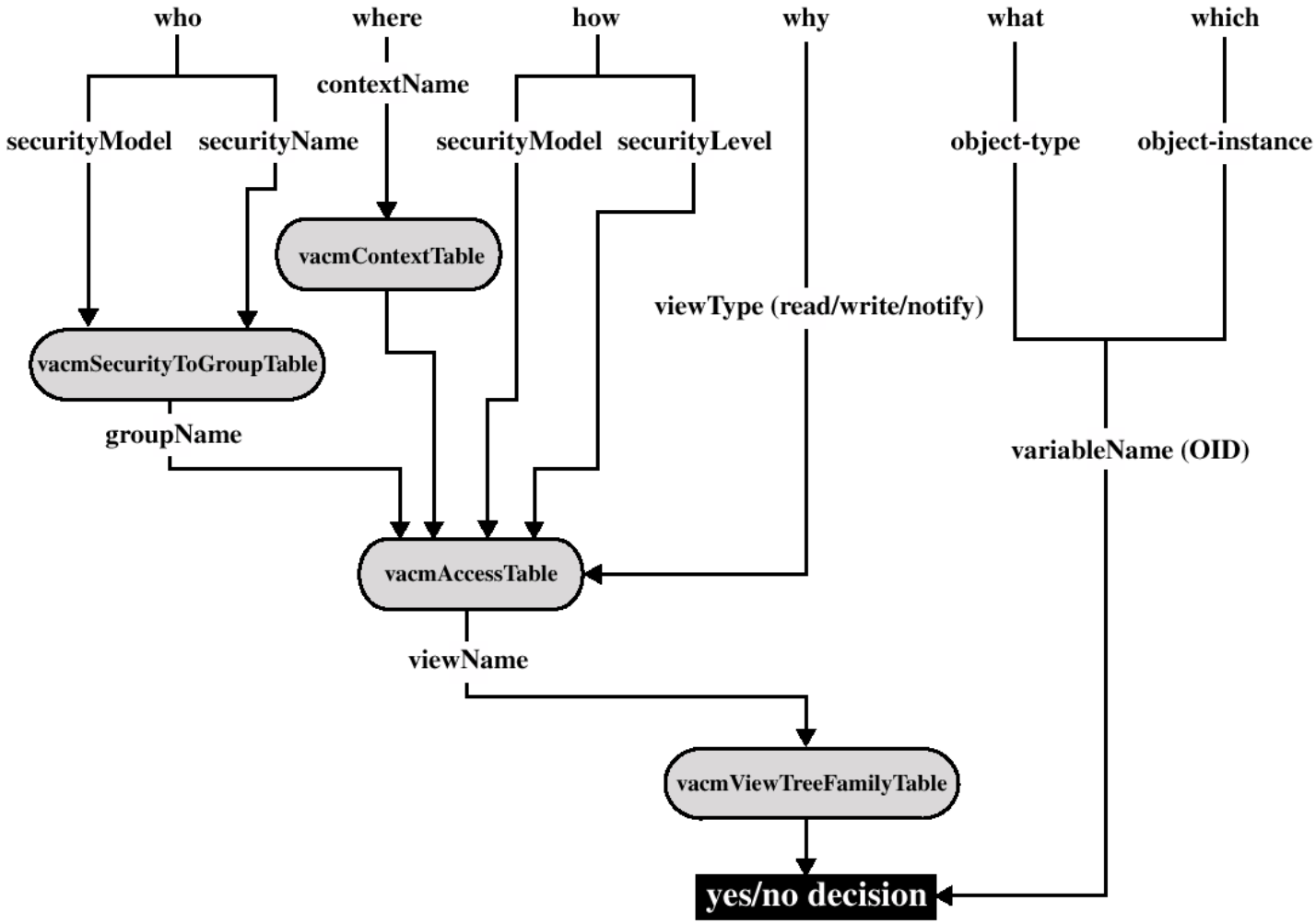
Key Localization Process



View-Based Access Control Model (VACM)

- VACM has two characteristics:
  - Determines wheter access to a managed object should be allowed.
  - Make use of an MIB that:
    - Defines the access control policy for this agent.
    - Makes it possible for remote configuration to be used.

Access control decision



Recommended Reading and WEB Sites

- Subramanian, Mani. *Network Management*. Addison-Wesley, 2000
- Stallings, W. *SNMP, SNMPv1, SNMPv3 and RMON 1 and 2*. Addison-Wesley, 1999
- IETF SNMPv3 working group (Web sites)
- SNMPv3 Web sites