Chapter 8

Network Management Security

Outline

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

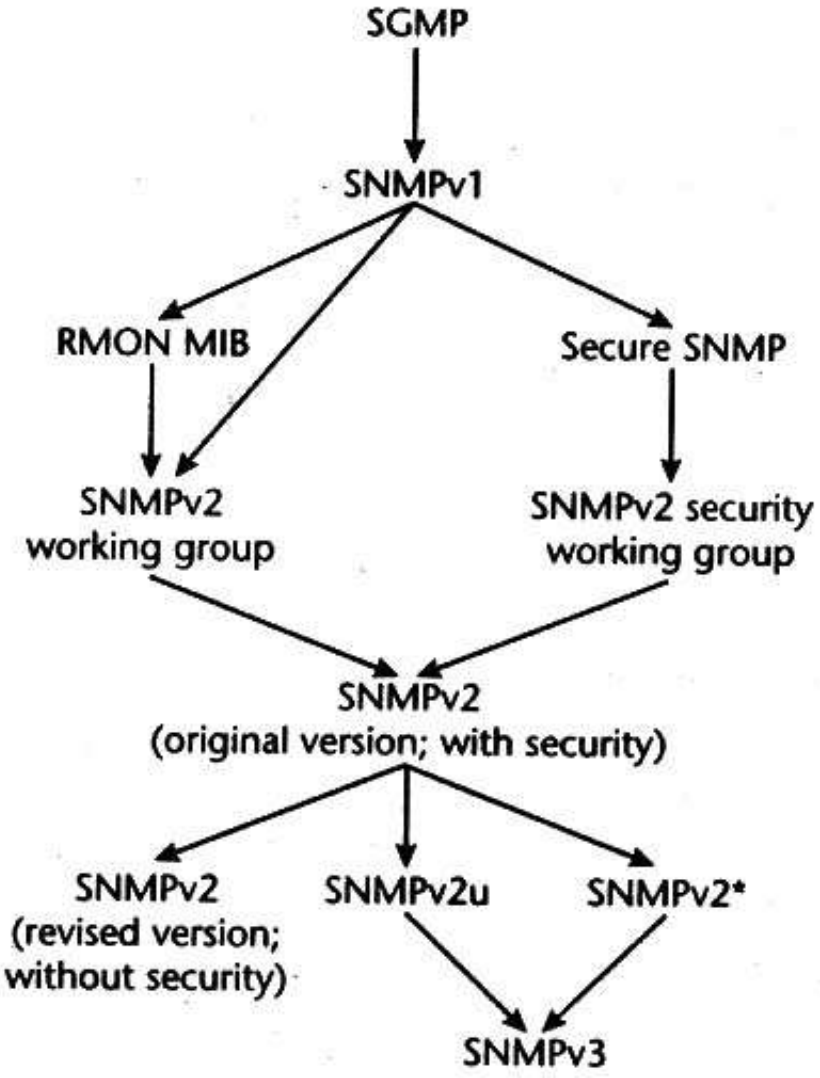
Introduction

- ICMP (Internet Control Message Protocol) for transferring control message from routers and other hosts to a host : the late 1970s
  - useful features : echo/echo-reply message pair, time stamp and time stamp reply message pair
  - a management tool : PING (Packet Internet Groper)
    - verifying the operation of a server on a host
    - observing variations in round-trip times and in datagram loss rates
- Internet growing in the late 1980s
  - SGMP (Simple Monitoring Protocol) in Nov. 1987 ----> SNMP
  - HEMS (High-level Entity Management System) : generalization of Host Monitoring Protocol (HMP)
  - CMIP over TCP/IP (CMOT)
- In 1988, IAB approved further development of SNMP as short-term solution and CMOT as the long-term solution

Evolution of SNMP

- Development of a remote monitoring capability for SNMP
- RMON (Remote Monitoring) MIB and addition to SNMP MIB for monitoring
- Vendor-independent SNMP MIB and Vendor-specific SNMP MIB
- SNMP v2 : dealing with security aspects
- SNMP v3 : specifying use of cryptographic algorithms

Evolution of SNMP(2)



SNMP-Related Standards by IETF

- Foundation specifications
  - Structure and Identification for Information for TCP/IP-based networks (RFC 1155)
  - Management Information Base for Network Management of TCP/IP-based Internet: MIB-II (RFC 1213)
  - Simple Network Management Protocol (RFC 1157)

Network Management Architecture and its key elements for TCP/IP Network

- Management station having: a set of management application for data analysis and fault recovery
  - an interface for the network manager to monitor and control the network
  - a database of information extracted from the MIBs of all the managed entities in the network
  - the capability of translating the network manager's requirements into the actual monitoring and control of remote elements in the network
- Management agent
  - managed from a management station
  - providing the management station with important but unsolicited information

Network Management Architecture and its key elements for TCP/IP Network

- MIB (Management Information Base)
  - representing resources as objects
  - data variables representing one aspect of the managed agent
  - management station performs the monitoring function by retrieving the value of MIB objects
- Network management protocol
  - linking management station and agents
  - key capabilities of SNMP
    - *get* : retrieving the value of objects at the agent
    - *set* : setting the value of objects at the agent
    - *trap* : notifying the management station of significant events

Basic Concepts of SNMP

An integrated collection of tools for network monitoring and control.

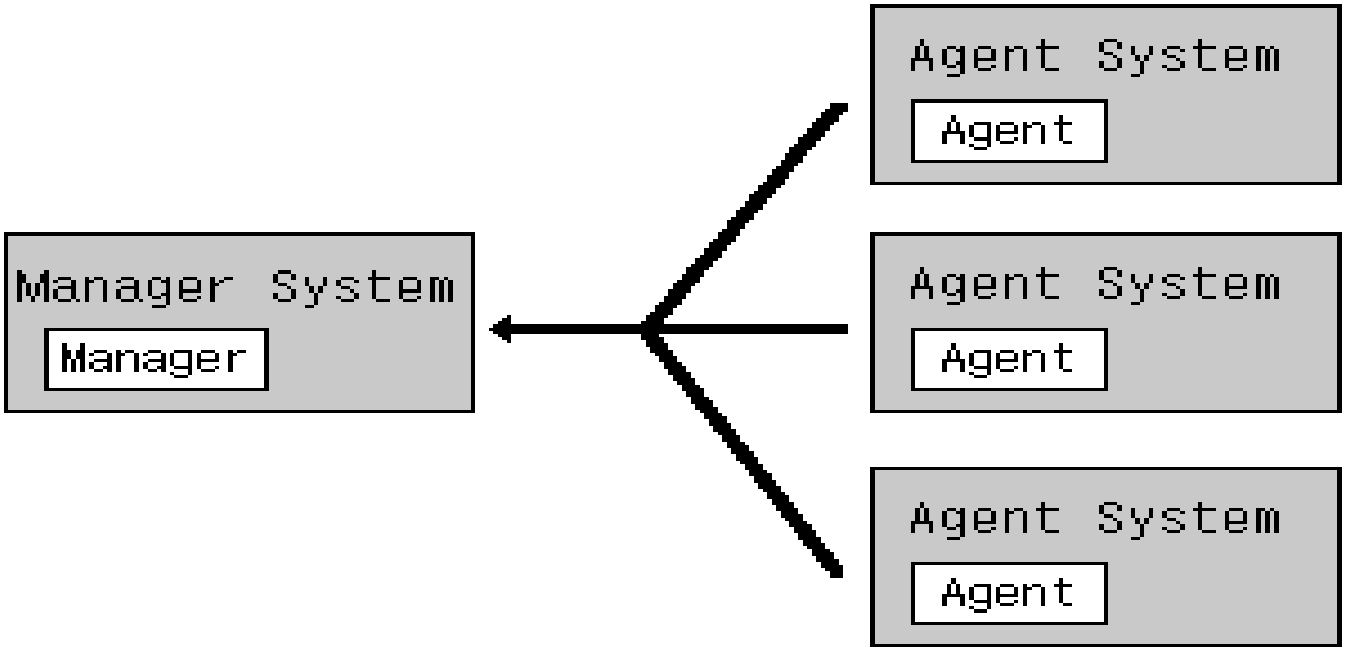
- Single operator interface
- Minimal amount of separate equipment. Software and network communications capability built into the existing equipment

- SNMP key elements:
  - Management station
  - Managament agent
  - Management information base
  - Network Management protocol
    - Get, Set and Notify (Trap)

Basic Functions of SNMP

- Network Configuration Management : Draw a map of how hosts are connected
- Performance Management
  - Throughput on a network segment
  - Errors
  - Speed
  - Response time
- Equipment Management : Monitor System Information
  - CPU, Memory, Disk Usage
- Security Management : Information control and Protection on SNMPv3

Basic Functions of SNMP



Basic Functions of SNMP

- **The other active element in the NMS**
- **Placed in the nodes managed from a management station**
- **Responds to requests :**
  - **for information from a management station (Get and GetNext)**
  - **for actions from the management station (Set)**
- **Provides the management station with important but unsolicited information (Trap)**

- **SNMP message format**

Version	Community name	SNMP PDU

SNMP PDU

- Protocol Data Unit

Version	Community	SNMP PDU

(a) SNMP message

PDU type	Request-id	0	0	Variablebindings

(b) GetRequest PDU, GetNextRequest PDU, and SetRequest PDU

PDU type	Request-id	Error status	Error index	Variablebindings

(c) Get Response PDU

PDU type	enterprise	Agent addr	Generic-trap	Specific-trap	Time stamp	Variablebindings

(d) Trap PDU

name1	value 1	name2	value2	- - -	namen	valuen

(e) variablebindings

Generic trap :

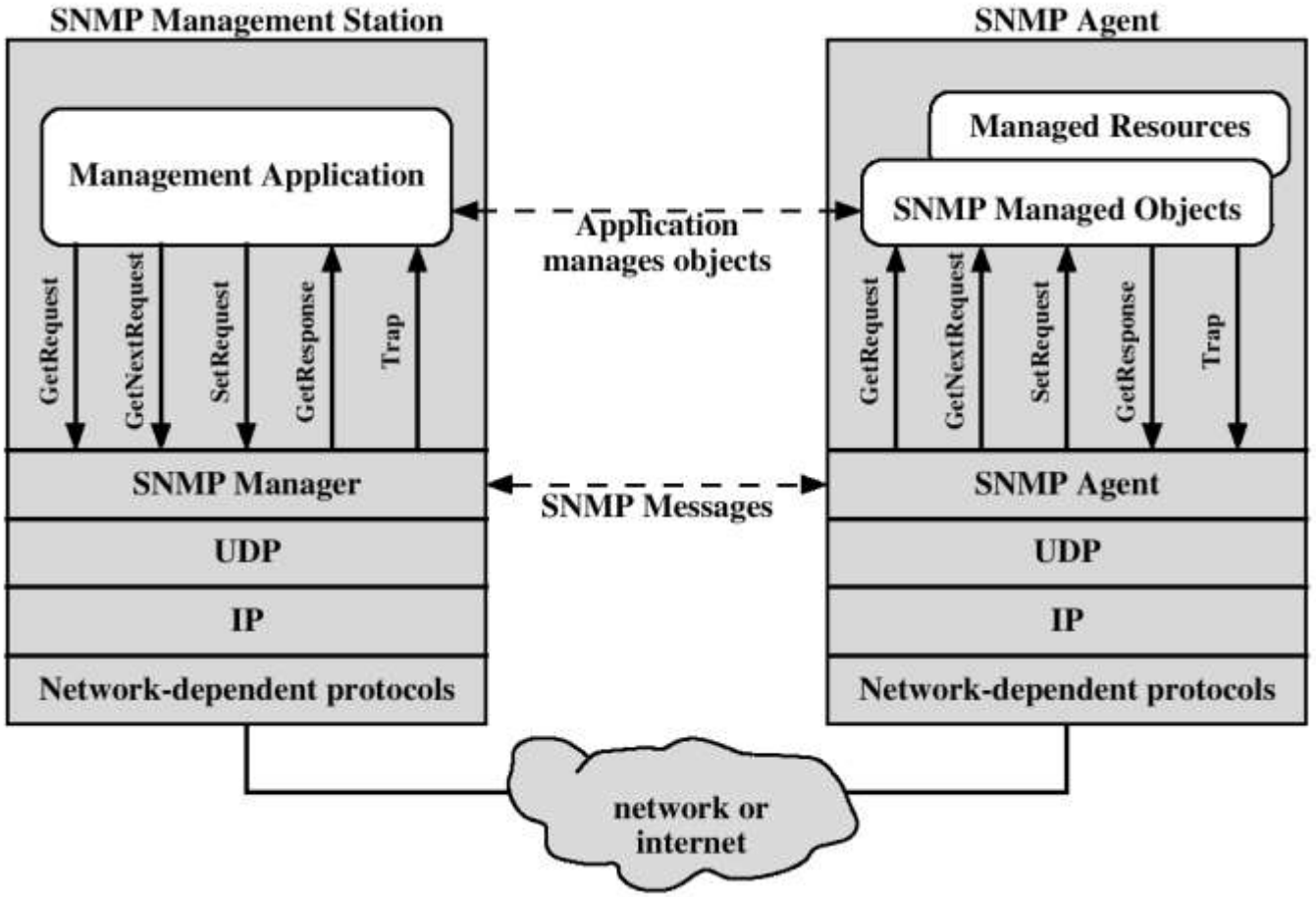
- A warmStart trap signifies that the sending protocol entity is reinitializing itself such that neither the agent configuration nor the protocol entity implementation is altered.

- A coldStart trap signifies that the sending protocol entity is reinitializing itself such that the agent's configuration or the protocol entity implementation may be altered

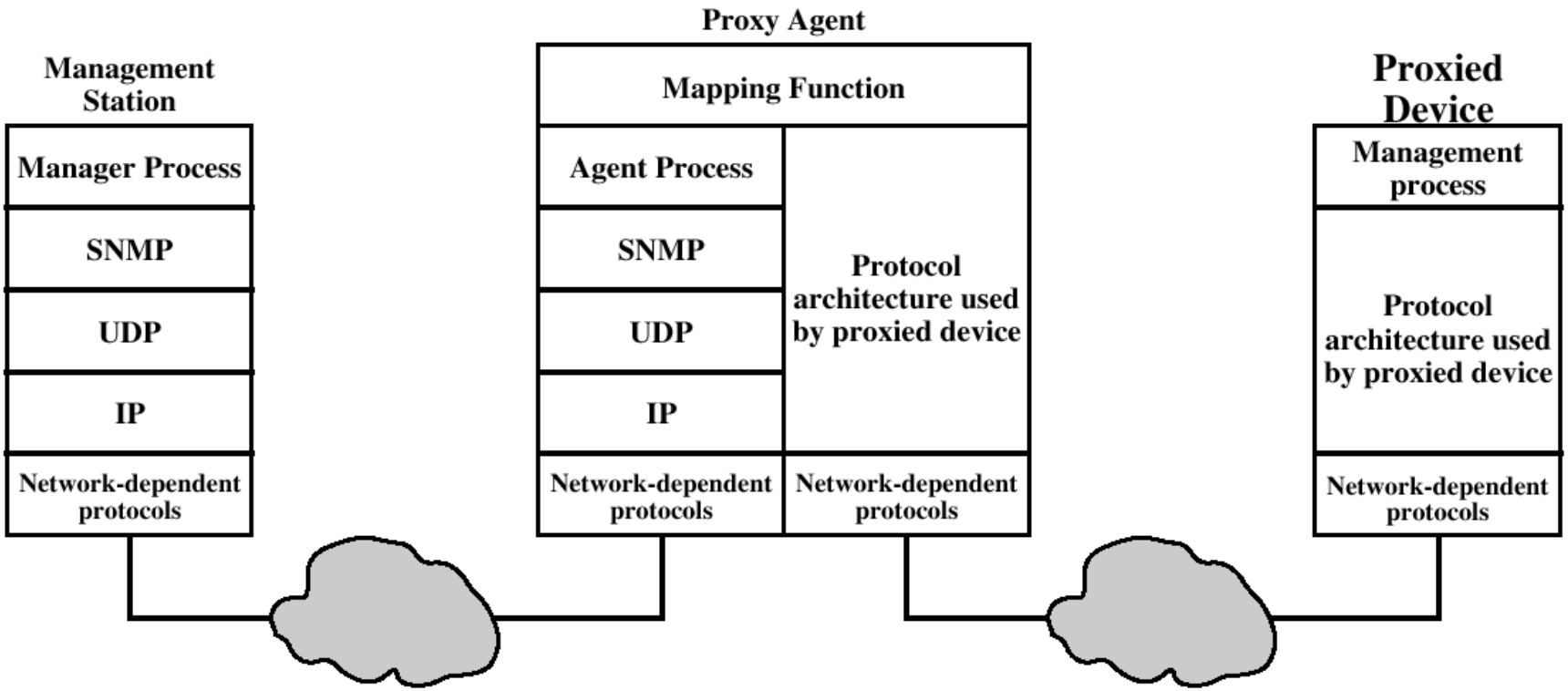
Error Status: noError(0), tooBig(1), noSuchName (2), badValue(3), readOnly(4), genErr(5)

Enterprise : Type of object generating trap; based on sysObjectID

Protocol context of SNMP

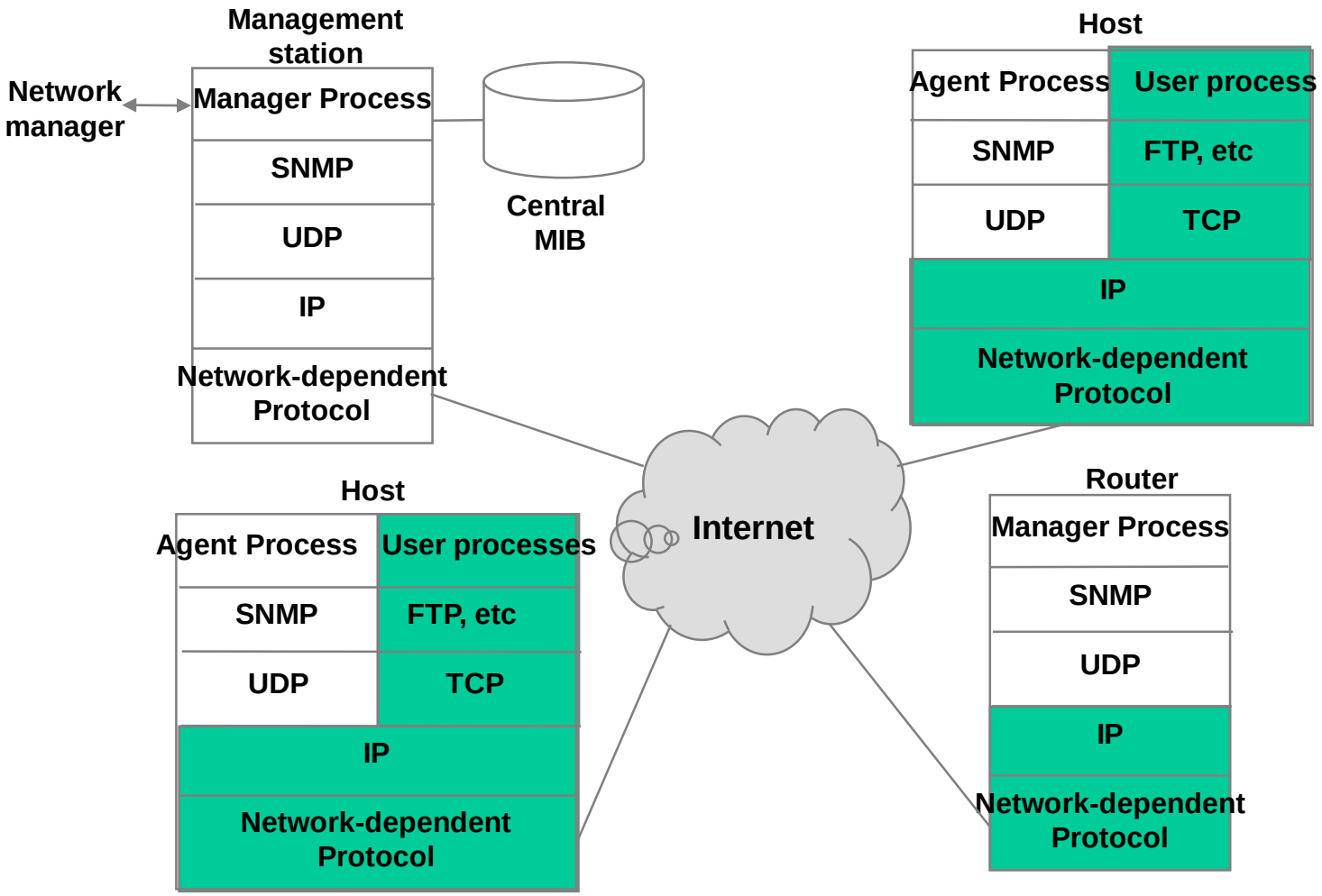


Proxy Configuration



Network Management Protocol Architecture

- SNMP implemented on the top of UDP (or TCP), IP and relevant network-dependent protocol (ex, Ethernet, FDDI, X.25, ATM,…)



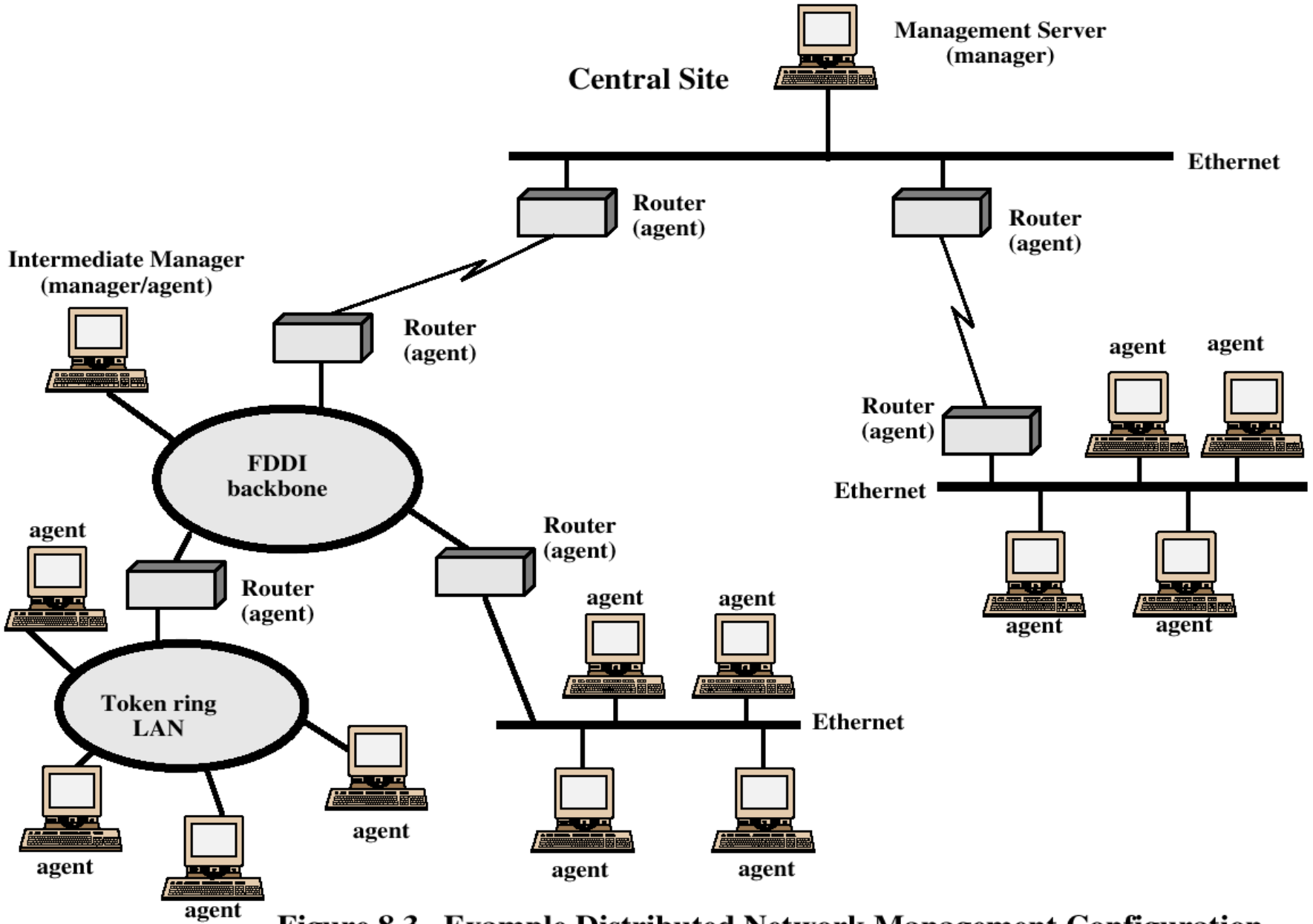
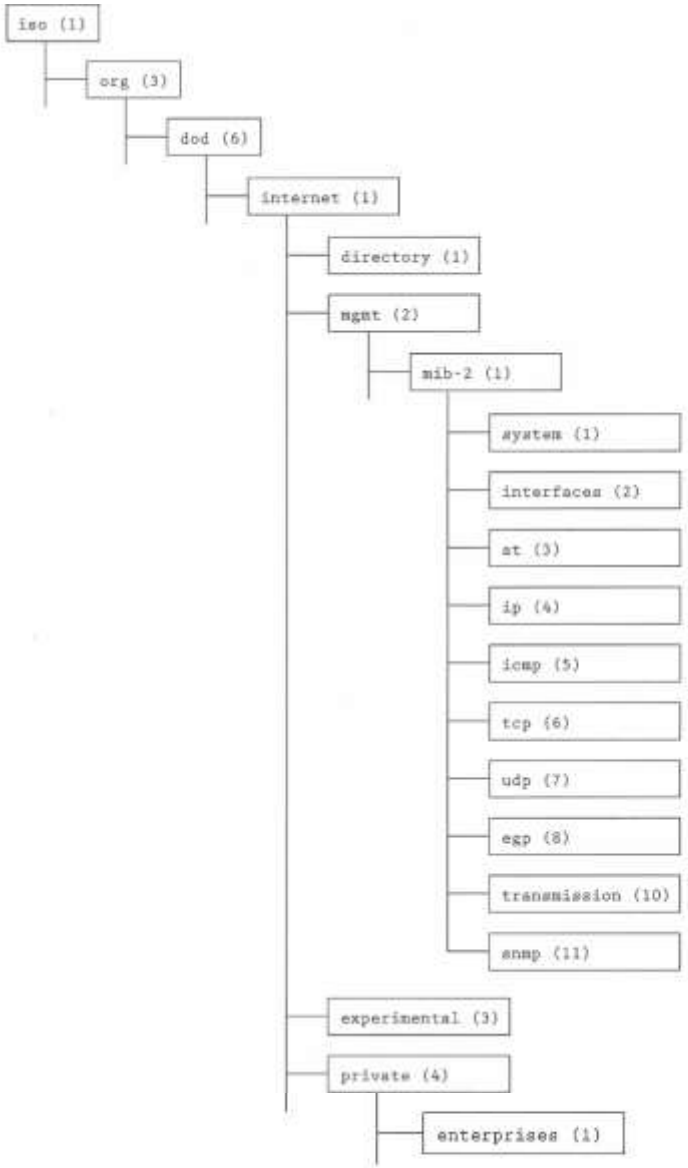


Figure 8.3 Example Distributed Network Management Configuration

MIB Structure

- Leaf objects of the tree to be actual managed objects to represent some resource, activity, or related information
- Object identifier : a unique identifier for particular object type
  - Serving as name the object
  - internet OBJECT IDENTIFIER :: = { iso (1) org(3) dod (6) 1}
  - therefore, internet node's object ID : 1.3.6.1
  - four nodes under the internet node
    - directory
    - mgmt ----> mib-1, mib-2
    - experimental
    - private

MIB Tree


iso (1)
org (3)
dod (6)
internet (1)
directory (1)
mgmt (2)
mib-2 (1)
system (1)
interfaces (2)
at (3)
ip (4)
icmp (5)
tcp (6)
udp (7)
egp (8)
transmission (10)
snmp (11)
experimental (3)
private (4)
enterprises (1)

MIB Tree (2)

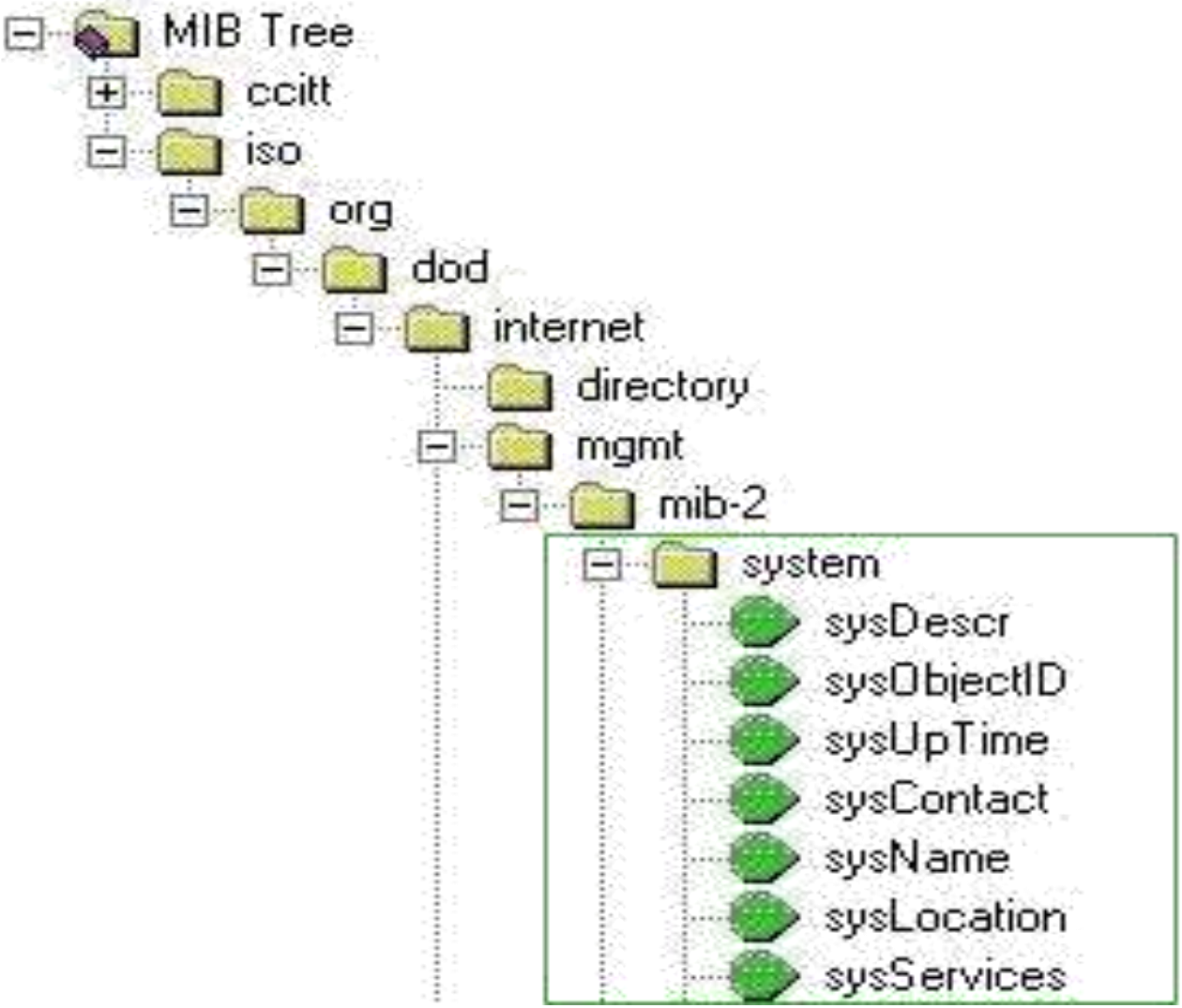
Object ID consisting of sequence of integers

- **for example : object ID for *tcpConnTable* : 1.3.6.1.2.1.6.13**

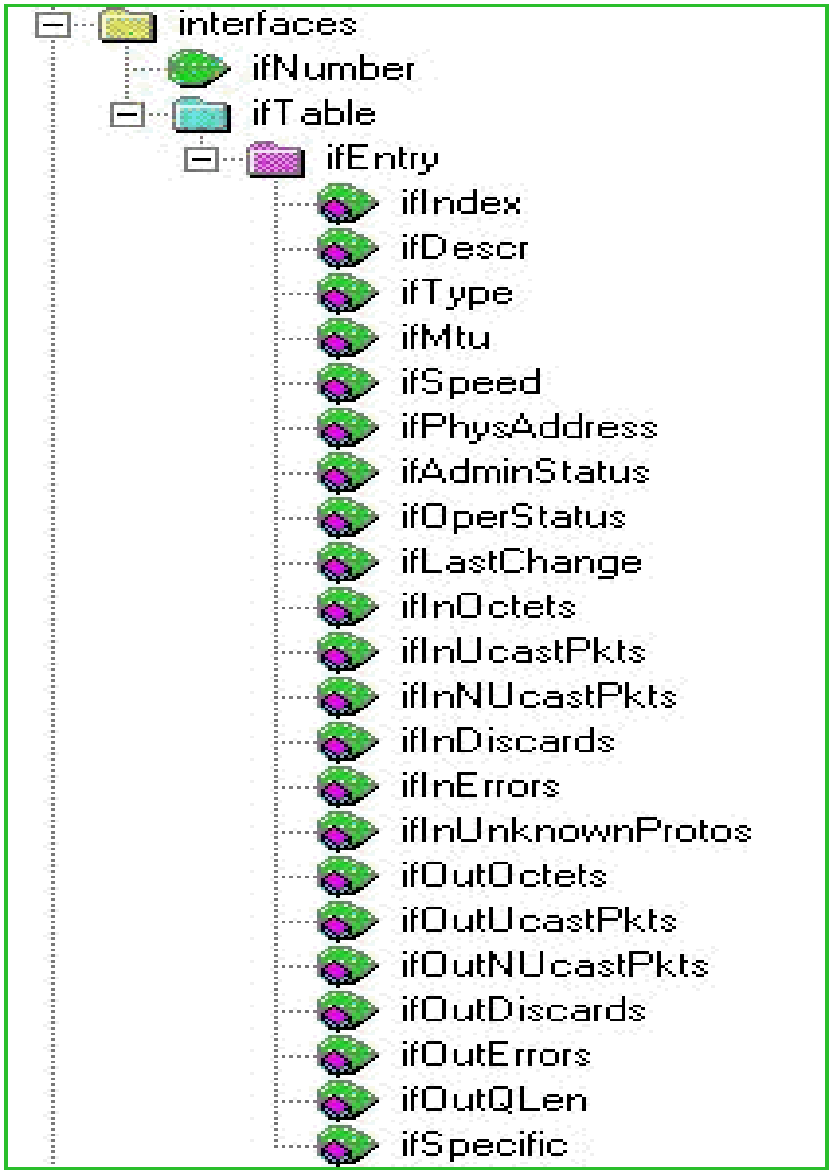
iso org dod internet mgmt mib-2 tcp tcpConnTable

1 3 6 1 2 1 6 13

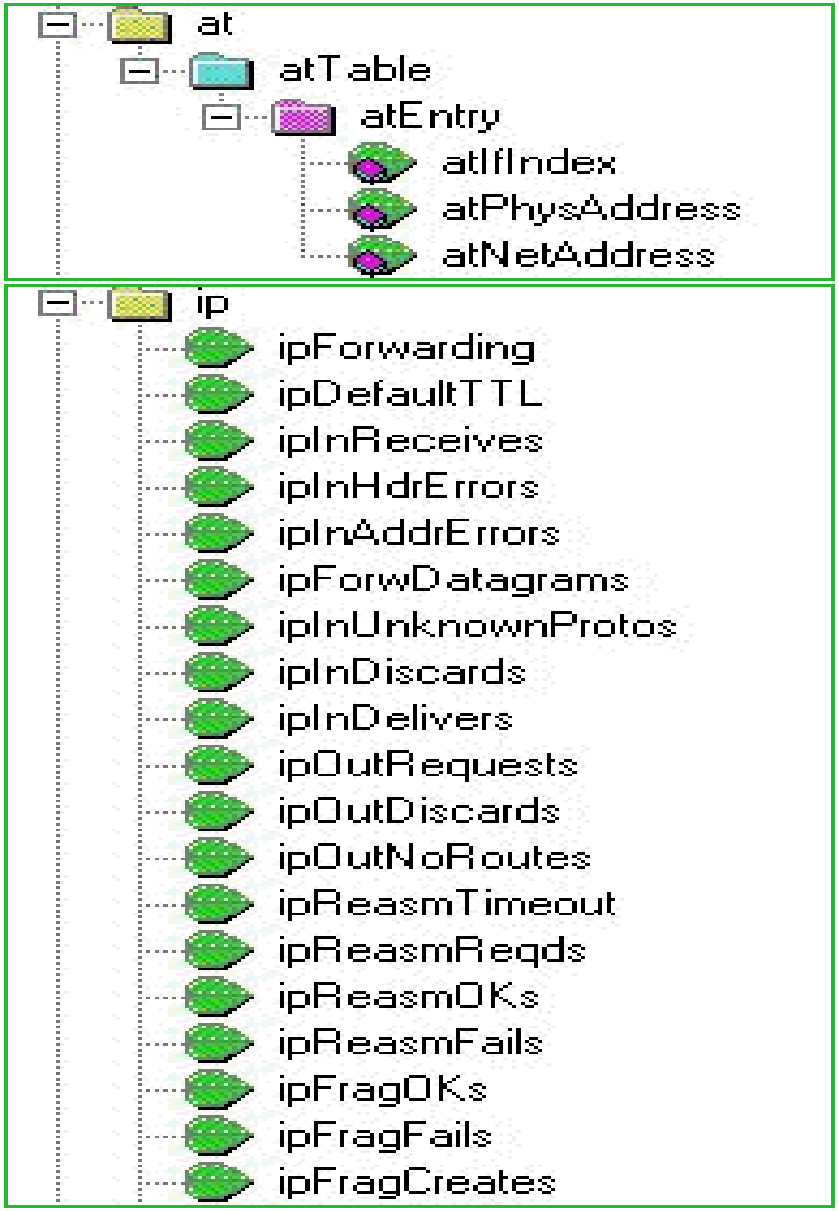
MIB II


MIB Tree
ccitt
iso
org
dod
internet
directory
mgmt
mib-2
system
sysDescr
sysObjectID
sysUpTime
sysContact
sysName
sysLocation
sysServices

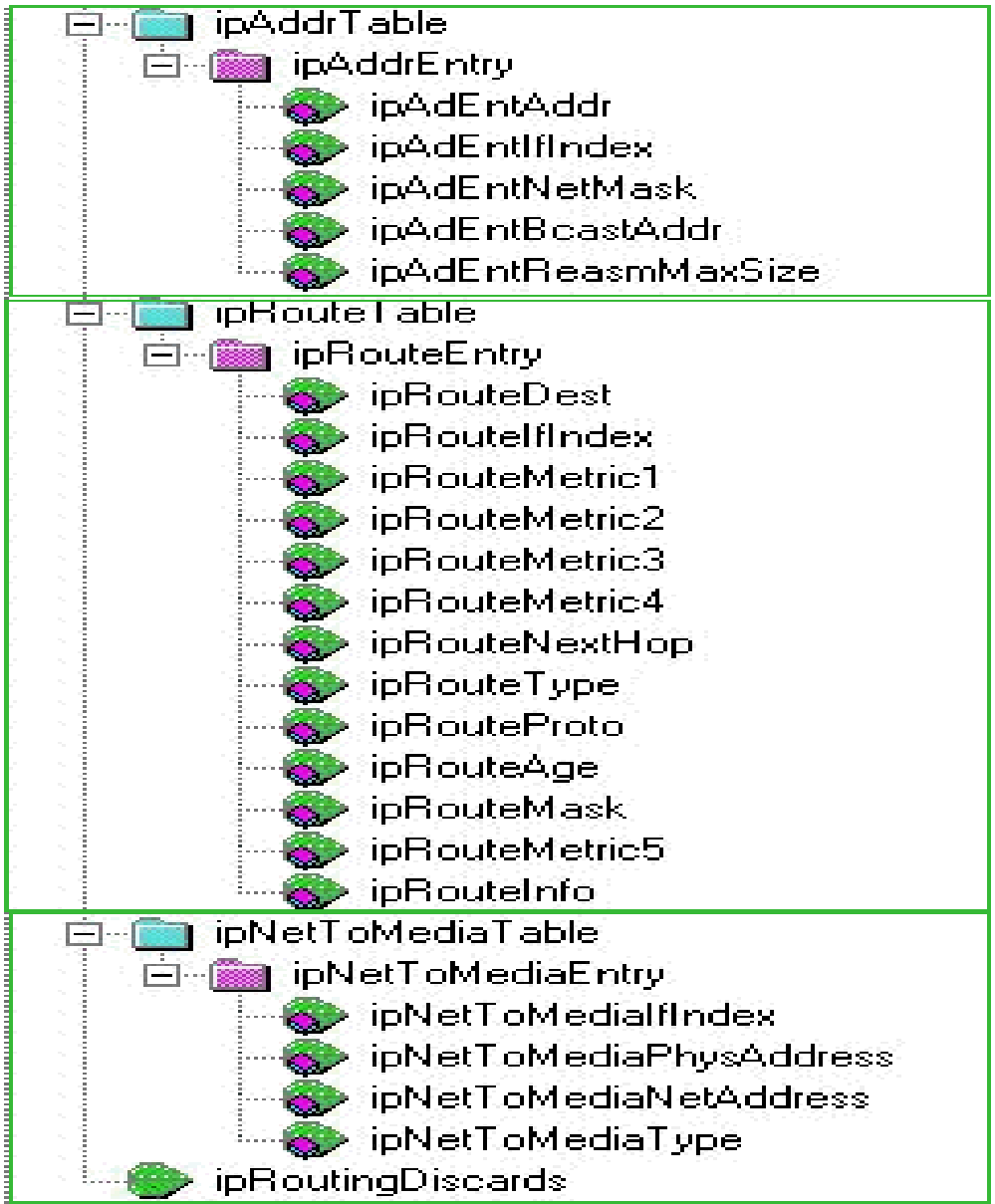
MIB II


interfaces
ifNumber
ifTable
ifEntry
ifIndex
ifDescr
ifType
ifMtu
ifSpeed
ifPhysAddress
ifAdminStatus
ifOperStatus
ifLastChange
ifInOctets
ifInUcastPkts
ifInNUcastPkts
ifInDiscards
ifInErrors
ifInUnknownProtos
ifOutOctets
ifOutUcastPkts
ifOutNUcastPkts
ifOutDiscards
ifOutErrors
ifOutQLen
ifSpecific

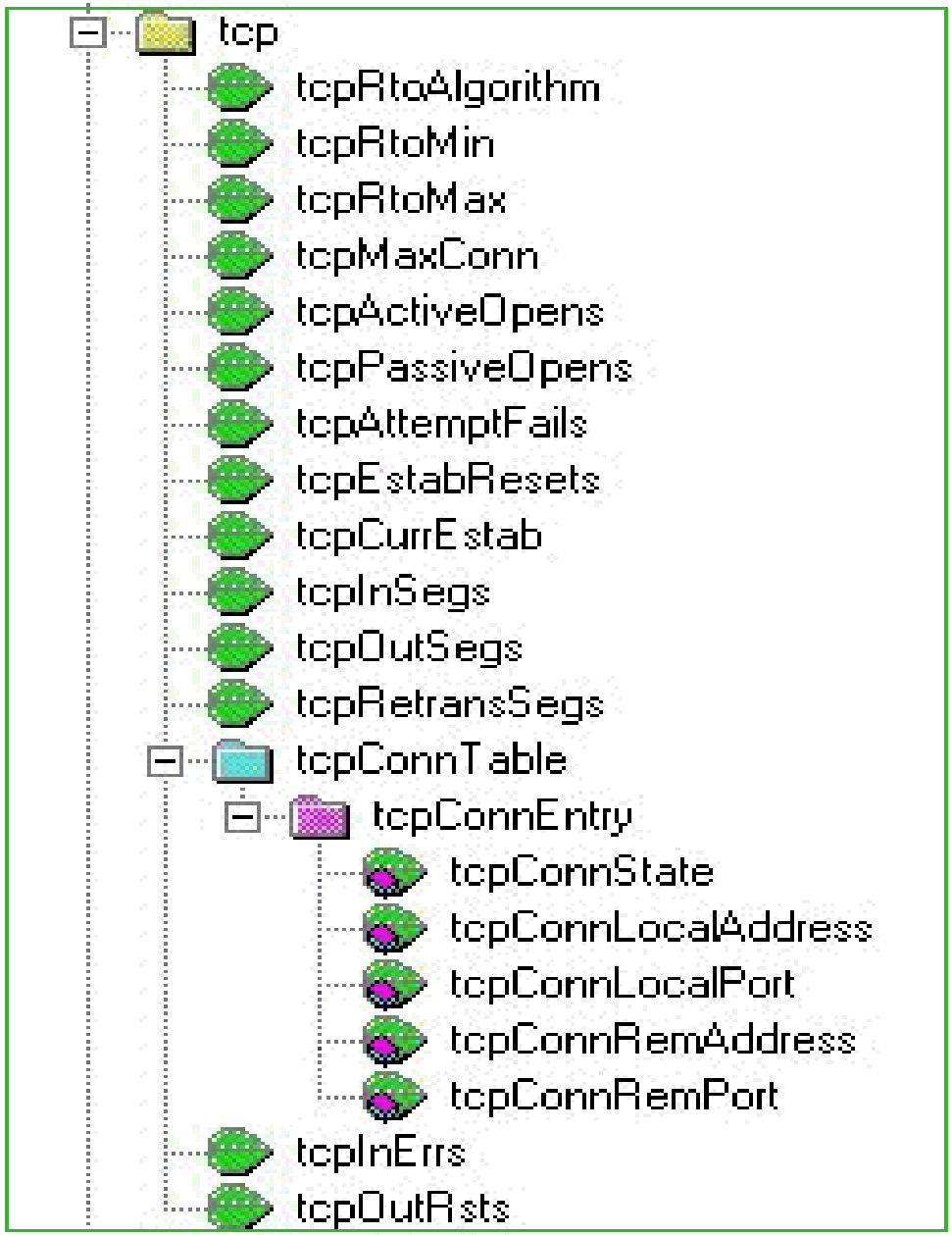
MIB II


at
atTable
atEntry
atIfIndex
atPhysAddress
atNetAddress
ip
ipForwarding
ipDefaultTTL
ipInReceives
ipInHdrErrors
ipInAddrErrors
ipForwDatagrams
ipInUnknownProtos
ipInDiscards
ipInDelivers
ipOutRequests
ipOutDiscards
ipOutNoRoutes
ipReasmTimeout
ipReasmReqds
ipReasmOKs
ipReasmFails
ipFragOKs
ipFragFails
ipFragCreates

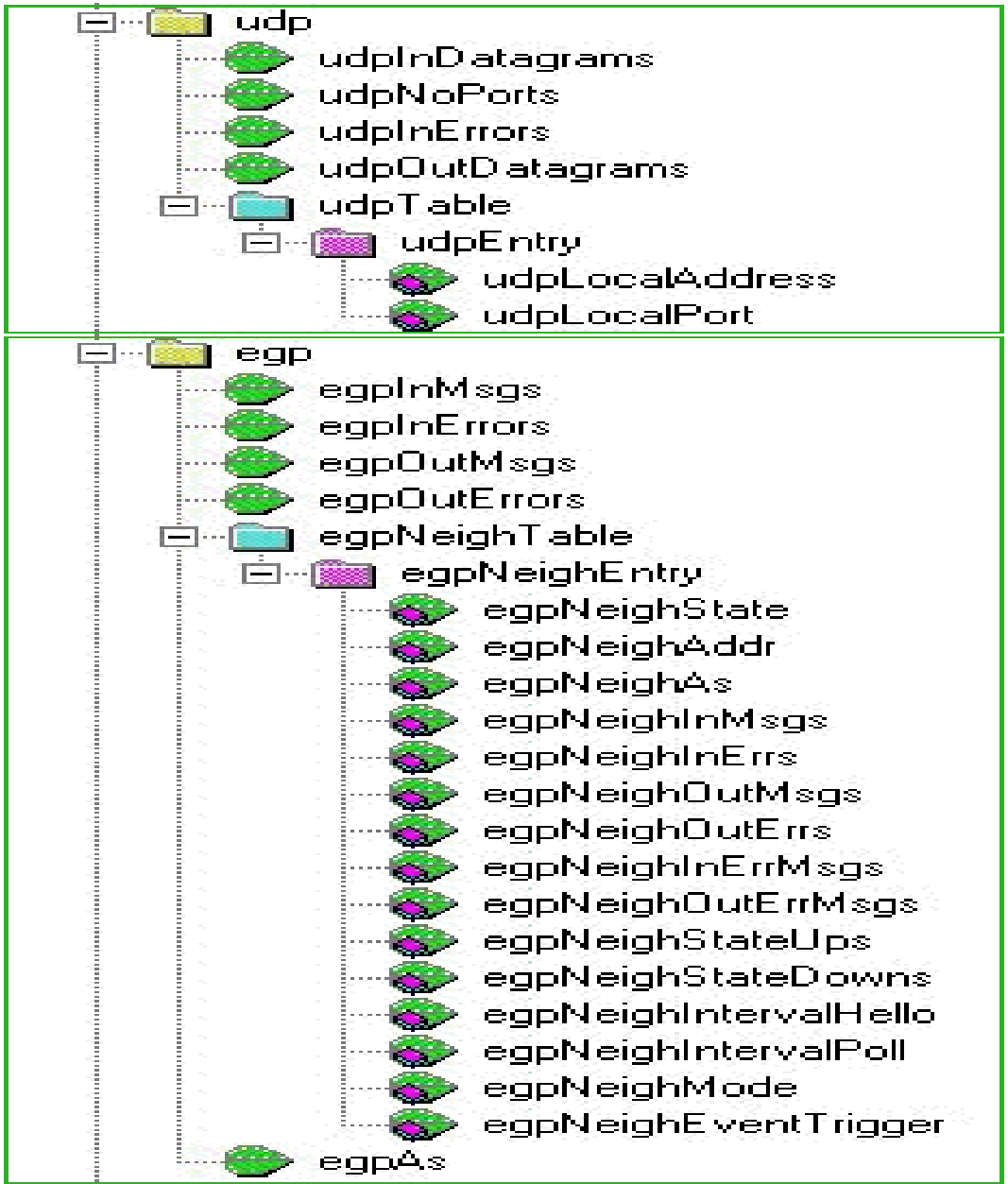
MIB II


ipAddrTable
ipAddrEntry
ipAdEntAddr
ipAdEntIfIndex
ipAdEntNetMask
ipAdEntBcastAddr
ipAdEntReasmMaxSize
ipRouteTable
ipRouteEntry
ipRouteDest
ipRouteIfIndex
ipRouteMetric1
ipRouteMetric2
ipRouteMetric3
ipRouteMetric4
ipRouteNextHop
ipRouteType
ipRouteProto
ipRouteAge
ipRouteMask
ipRouteMetric5
ipRouteInfo
ipNetToMediaTable
ipNetToMediaEntry
ipNetToMediaIfIndex
ipNetToMediaPhysAddress
ipNetToMediaNetAddress
ipNetToMediaType
ipRoutingDiscards

MIB II


tcp
tcpRtoAlgorithm
tcpRtoMin
tcpRtoMax
tcpMaxConn
tcpActiveOpens
tcpPassiveOpens
tcpAttemptFails
tcpEstabResets
tcpCurrEstab
tcpInSegs
tcpOutSegs
tcpRetransSegs
tcpConnTable
tcpConnEntry
tcpConnState
tcpConnLocalAddress
tcpConnLocalPort
tcpConnRemAddress
tcpConnRemPort
tcpInErrs
tcpOutRsts

MIB II


udp
udpInDatagrams
udpNoPorts
udpInErrors
udpOutDatagrams
udpTable
udpEntry
udpLocalAddress
udpLocalPort
egp
egpInMsgs
egpInErrors
egpOutMsgs
egpOutErrors
egpNeighTable
egpNeighEntry
egpNeighState
egpNeighAddr
egpNeighAs
egpNeighInMsgs
egpNeighInErrs
egpNeighOutMsgs
egpNeighOutErrs
egpNeighInErrMsgs
egpNeighOutErrMsgs
egpNeighStateUps
egpNeighStateDowns
egpNeighIntervalHello
egpNeighIntervalPoll
egpNeighMode
egpNeighEventTrigger
egpAs

SNMP v1 and v2

- 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.
- GetBulkRequest /InformRequest

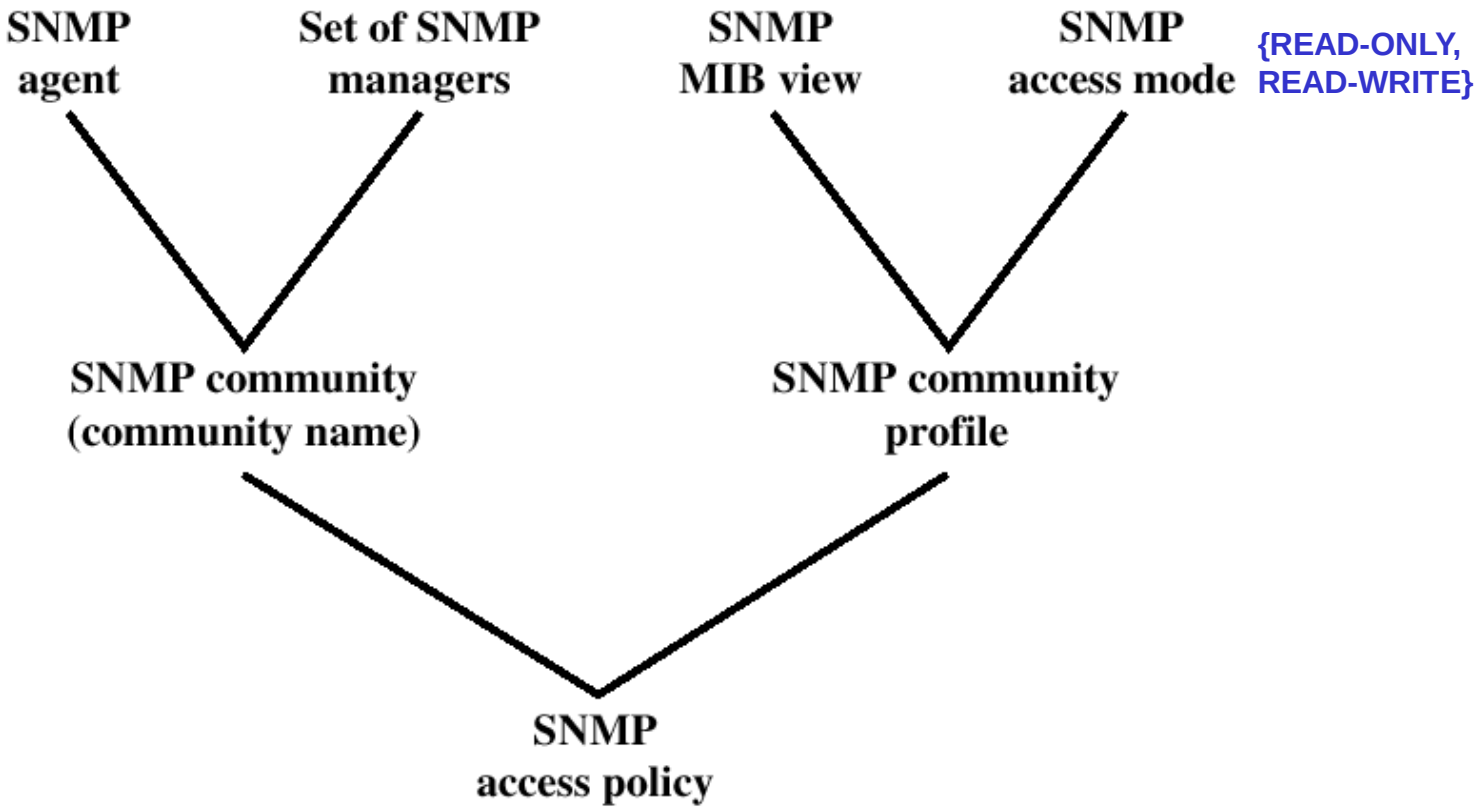
Comparison of SNMPv1 and SNMPv2

SNMPv1 PDU	SNMPv2 PDU	Direction	Description
GetRequest	GetRequest	Manager to agent	Request value for each listed object
GetNextRequest	GetNextRequest	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

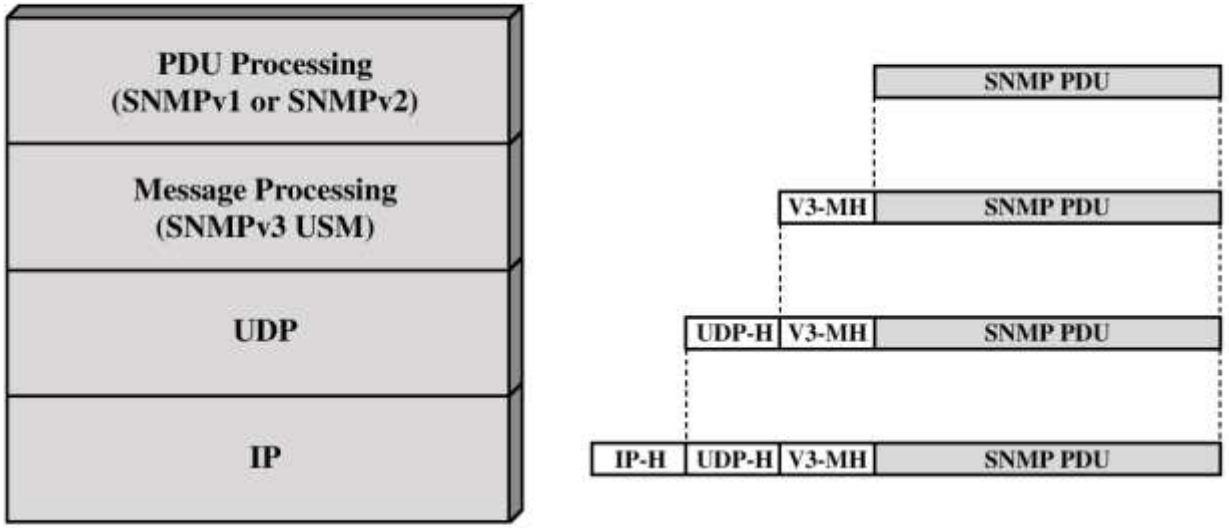
- SNMP Community – Relationship between an SNMP agent and SNMP managers.
- Three aspect of agent control:
  - Authentication service
  - Access policy
  - Proxy service

SNMPv1 Administrative Concepts



SNMPv3

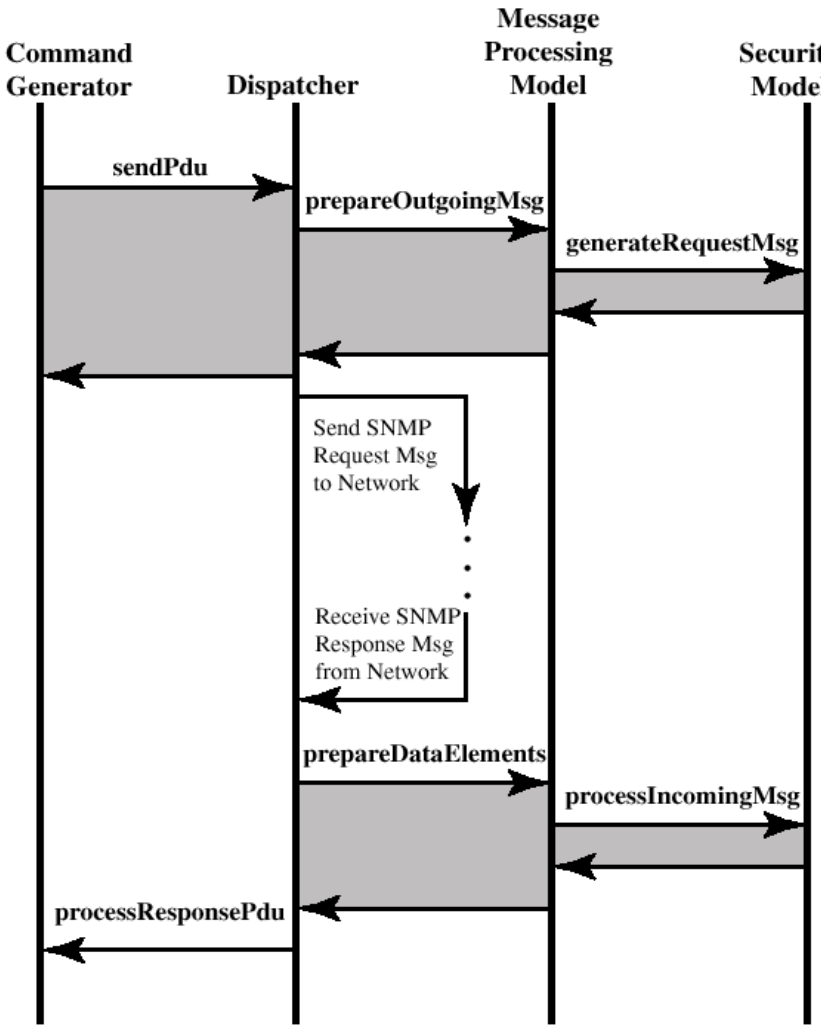
- SNMPv3 defines a security capability to be used in conjunction with SNMPv1 or v2



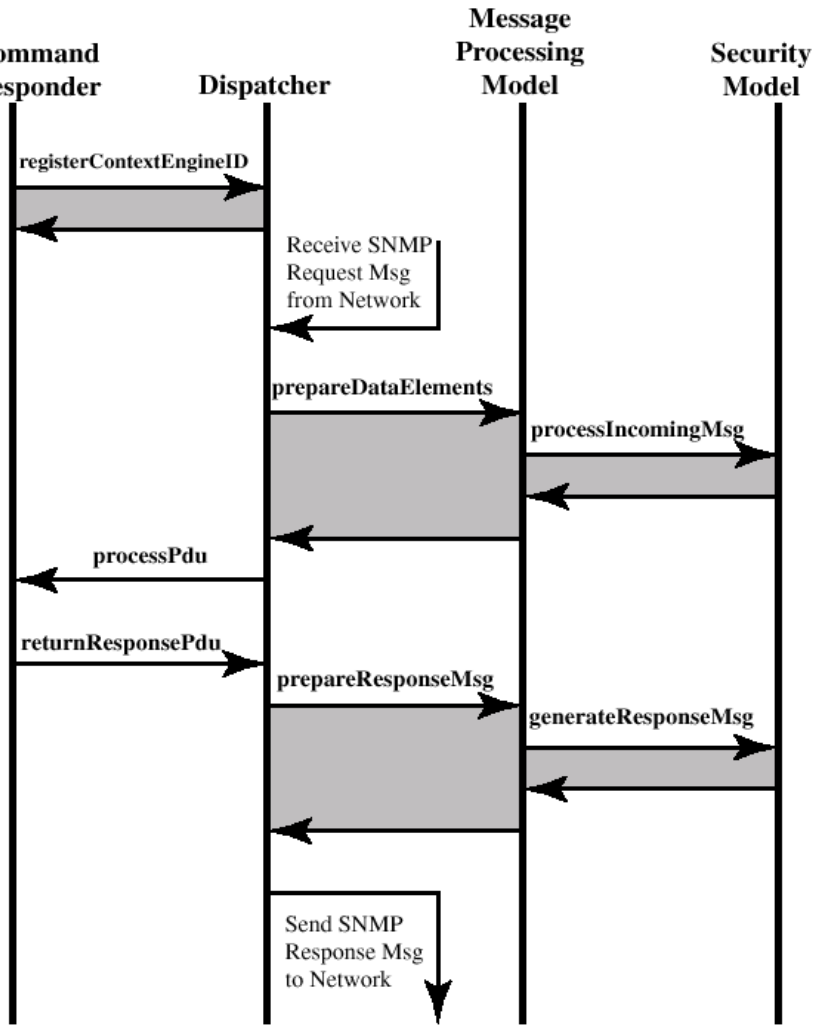
IP-H = IP header
UDP-H = UDP header
V3-MH = SNMPv3 message header
PDU = Protocol data unit

USM : User Security Model

SNMPv3 Flow

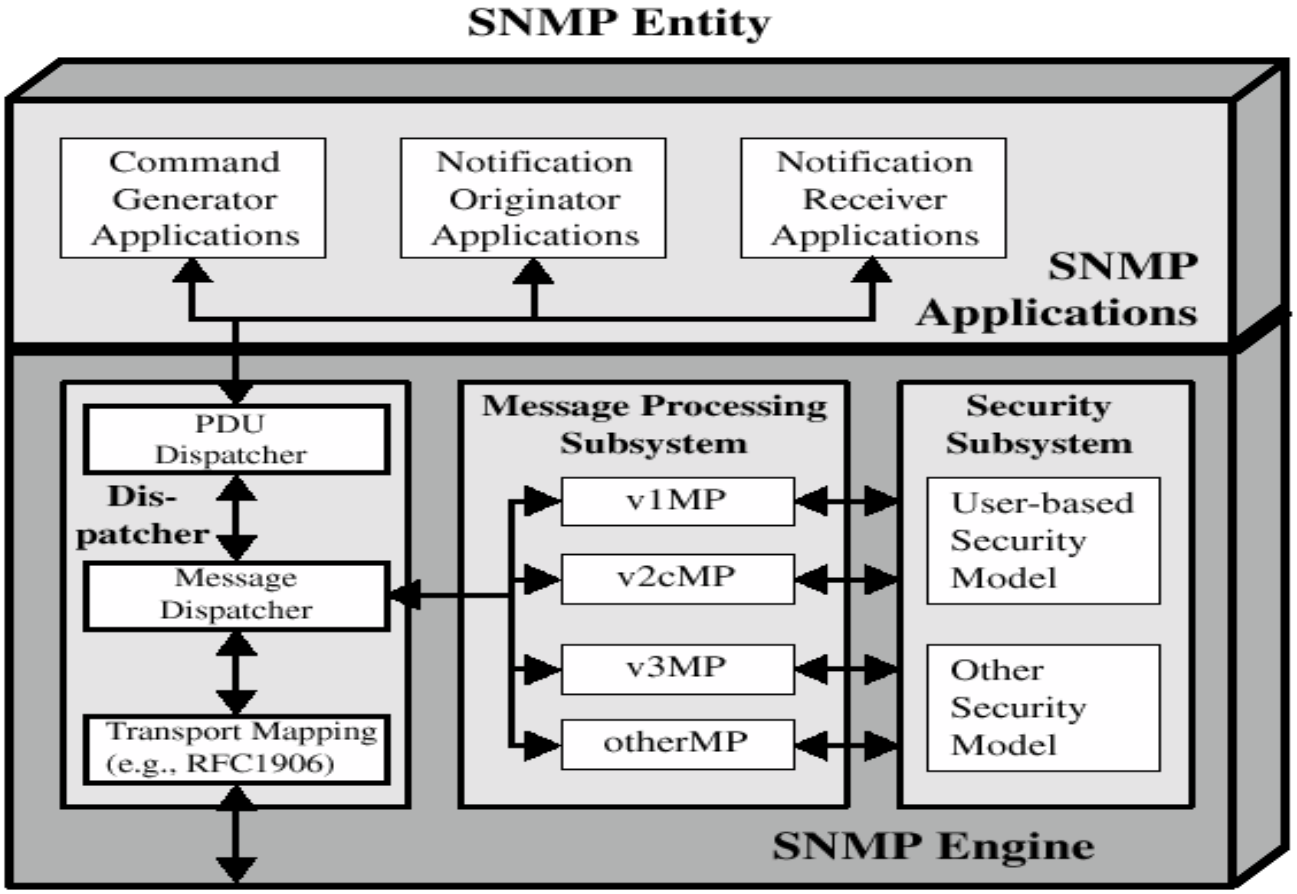


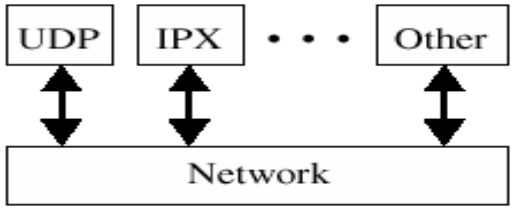
(a) Command Generator or Notification Originator



(b) Command Responder

Traditional SNMP Manager





- SNMP Engine
  - send/recv
  - authentication/Encryption/Decryption
  - access control

Traditional SNMP Agent

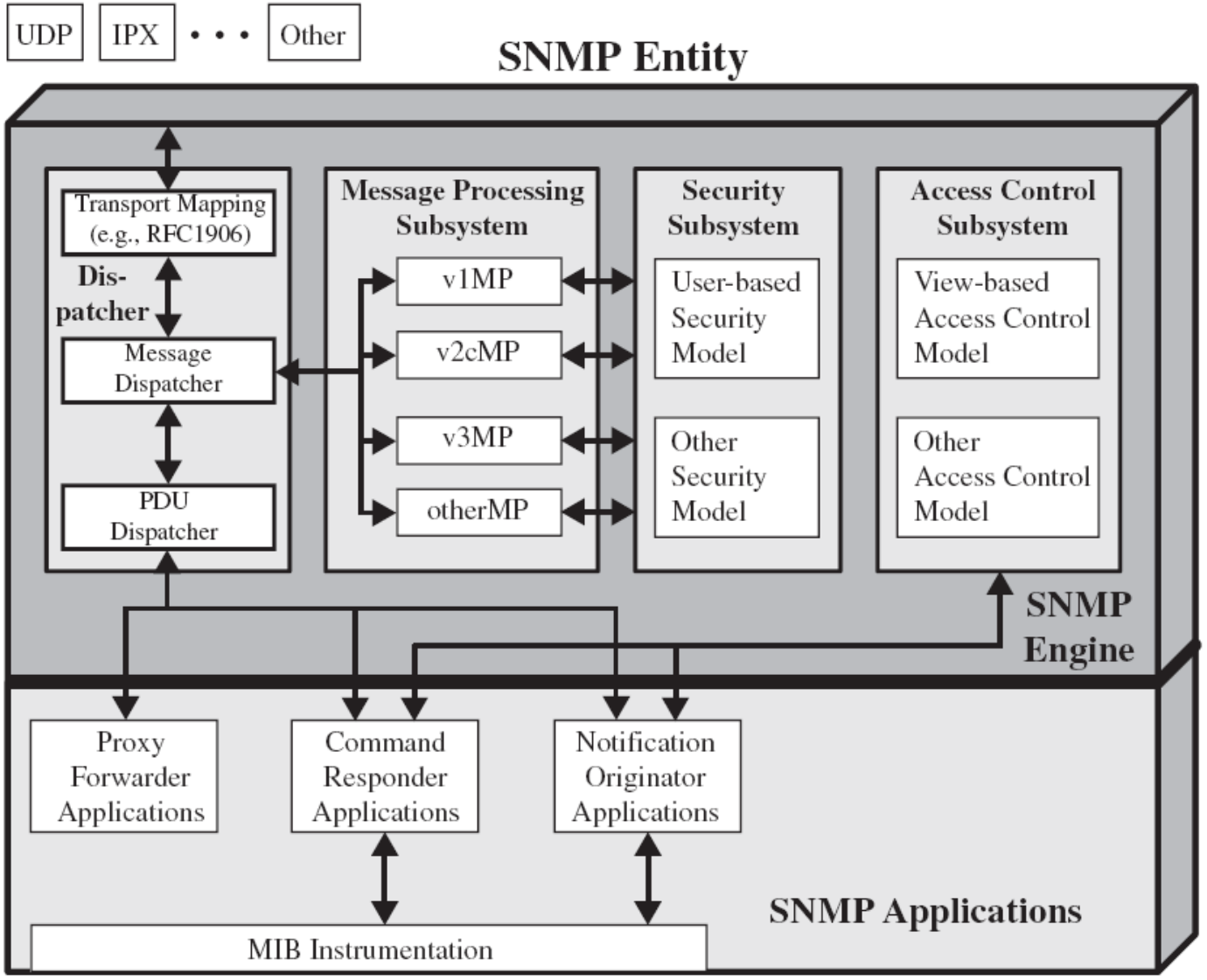
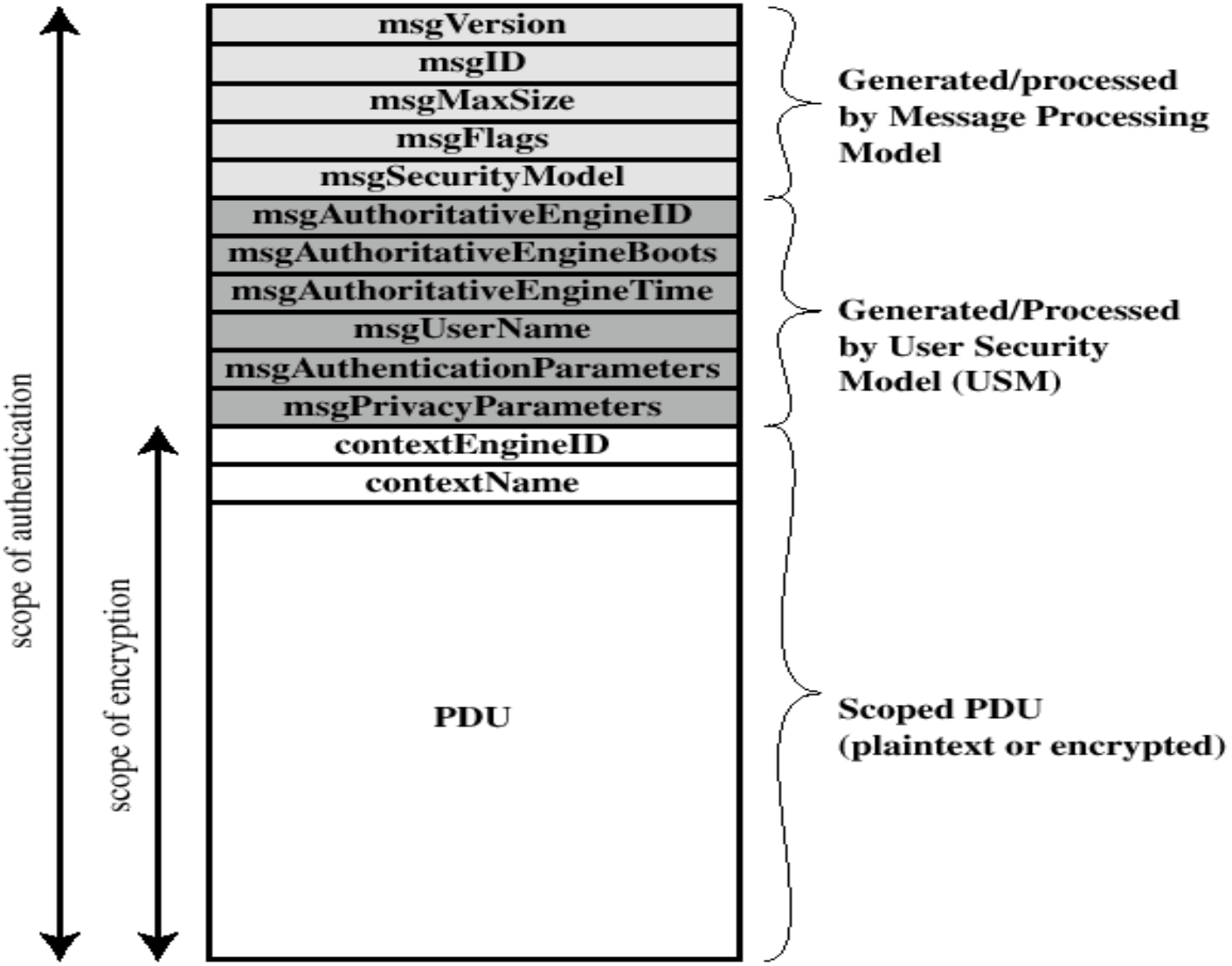


Figure 8.7 Traditional SNMP Agent

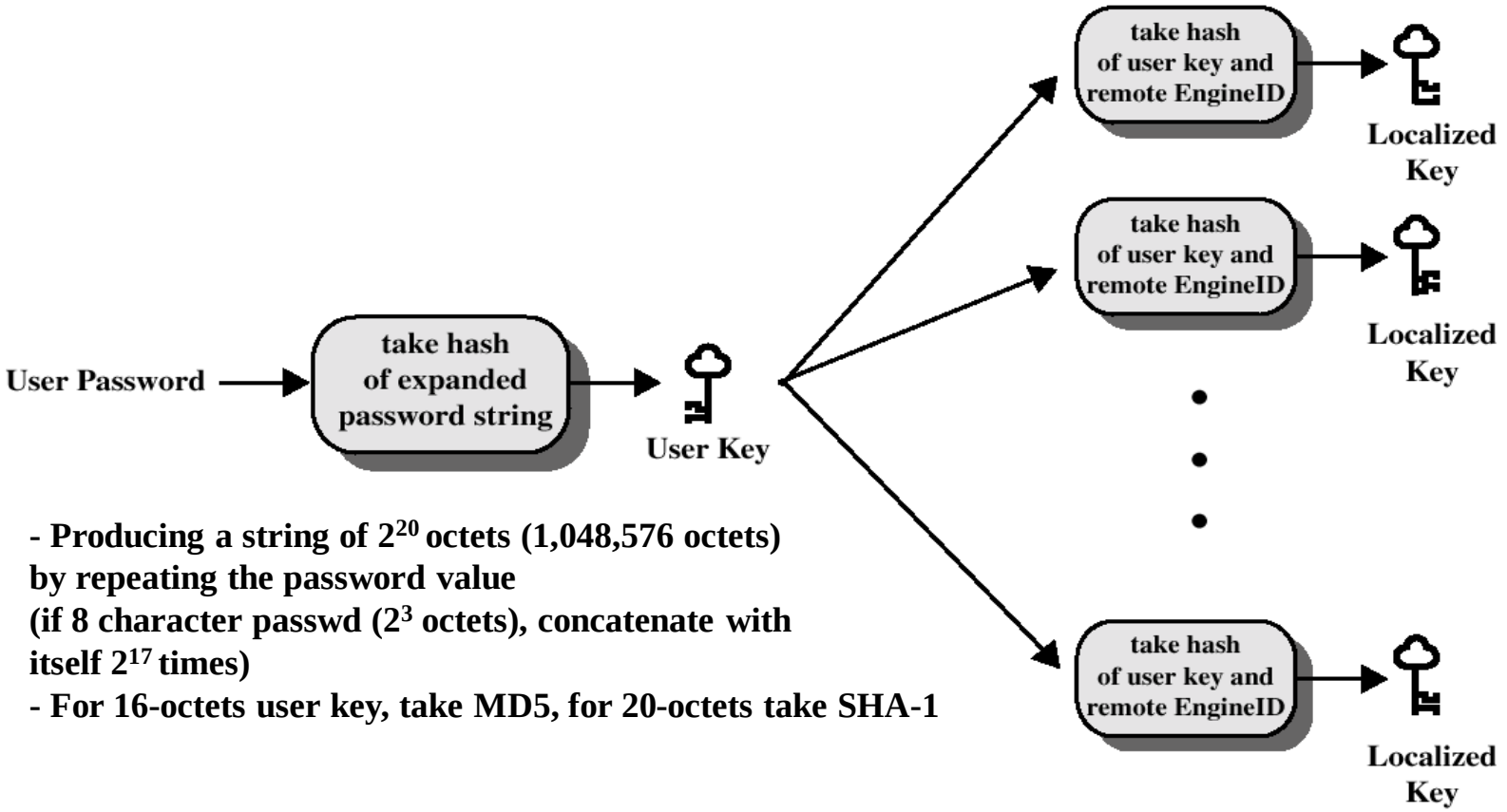
SNMP3 Message Format with USM



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

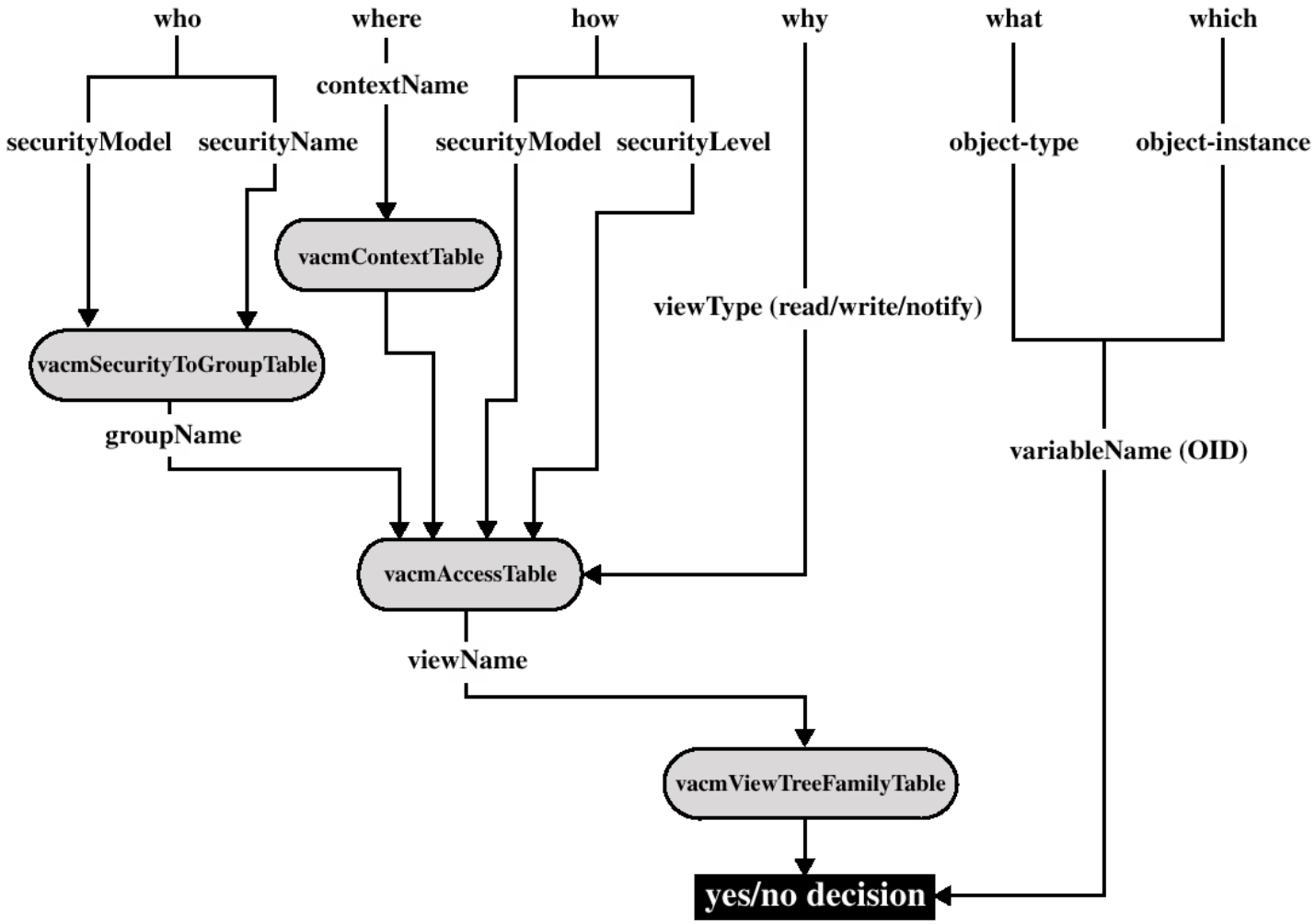


- Producing a string of 2^{20} octets (1,048,576 octets) by repeating the password value (if 8 character passwd (2^3 octets), concatenate with itself 2^{17} times)
- For 16-octets user key, take MD5, for 20-octets take SHA-1

View-Based Access Control Model (VACM)

- VACM has two characteristics:
  - Determines whether 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



Summary

- For managing the coplexed network systems, we need the use of automated network magement tools
- SNMP is most popular mangement protocol stadardized by IETF
- Security enhancements were accomplished in SNMPv3
- SNMP includes key elements such as mangement station, management agent, management information base and network management protocol