NETWORK MANAGEMENT

Myongji University
Sugwon Hong

Contents

- Network Management Overview
- Network Management Model
- SMI
- MIB
- SNMP
- SNMPv2, SNMPv3, RMON

What is network management?

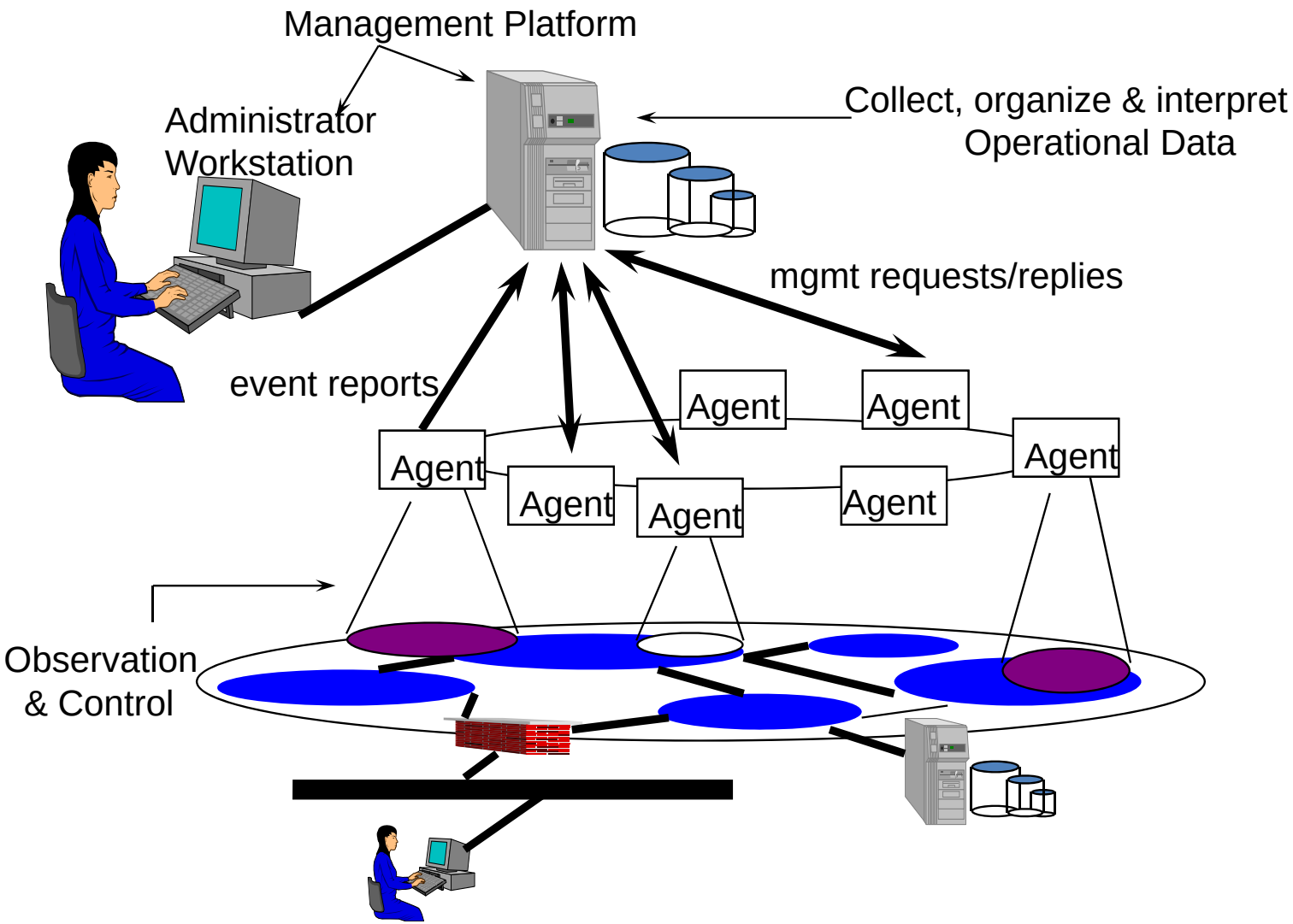
- Today's networks consist of 100s or 1000s of interacting hardware/software components. Even a single intranet is composed of more than 100s network devices (routers and switches).
- To guarantee proper operation, those complex systems require monitoring and control of all the components, which is called network management.
- The network management provides the following five functions.

Network Management Functions

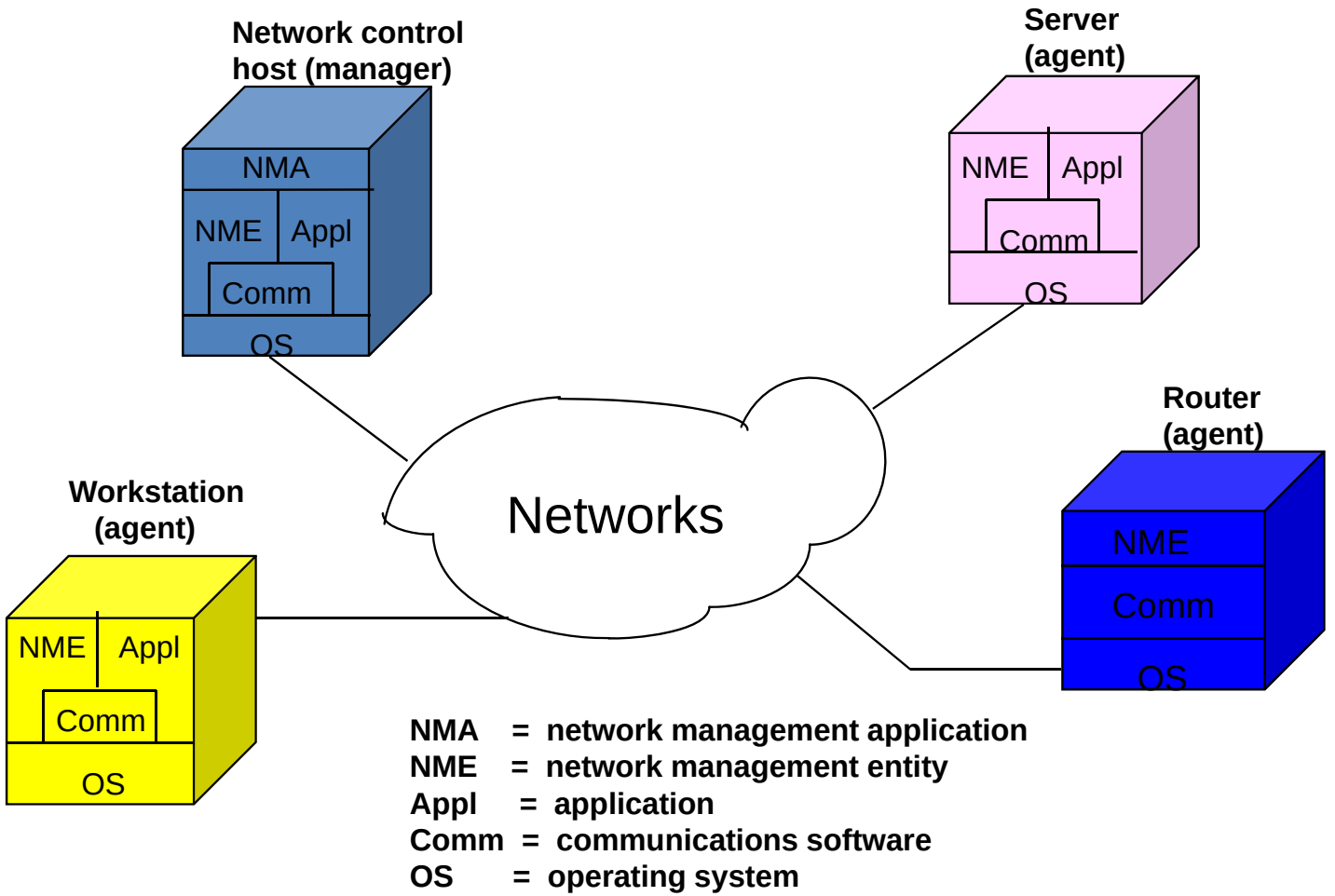
- Configuration management
- Fault management
- Security management
- Performance management
- Account management

Network Management System(NMS)

- NMS refers to the tools that can monitor and control the network.
- Based on manager-agent paradigm
  - A manager sends management requests to one or more agents.
  - Agents execute the requested operations and reply results.
  - When agents find any faults, notify the manager of them.
- NMS normally provides GUI for humans to facilitate the operations.
- commercial NMS
  - HP OpenView, IBM NetView, Sun Net Manager, etc.


Management Platform
Administrator
Workstation
Collect, organize & interpret
Operational Data
mgmt requests/replies
event reports
Agent
Agent
Agent
Agent
Agent
Agent
Agent
Observation
& Control

NMS components



NMA = network management application
NME = network management entity
Appl = application
Comm = communications software
OS = operating system

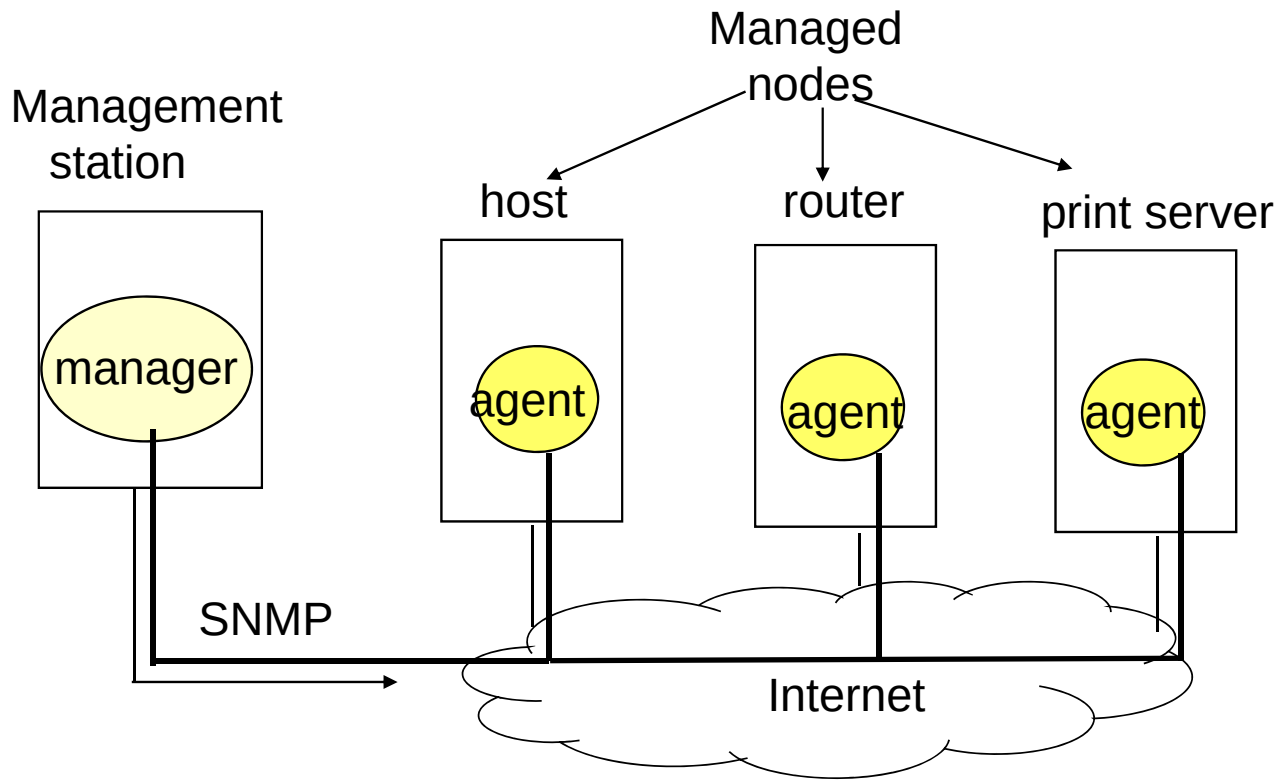
Standard Management Systems

- Internet Network Management Framework (IETF)
  - SNMPv1, SNMPv2, SNMPv3
- OSI Network Management Framework (ISO/ITU-T)
  - CMIP (X.700 Series)
- Telecommunication Management Network (ITU-T)
  - TMN (M.3000 Series)
- Distributed Management Task Force (DMTF)
  - DMI, CIM, WBEM

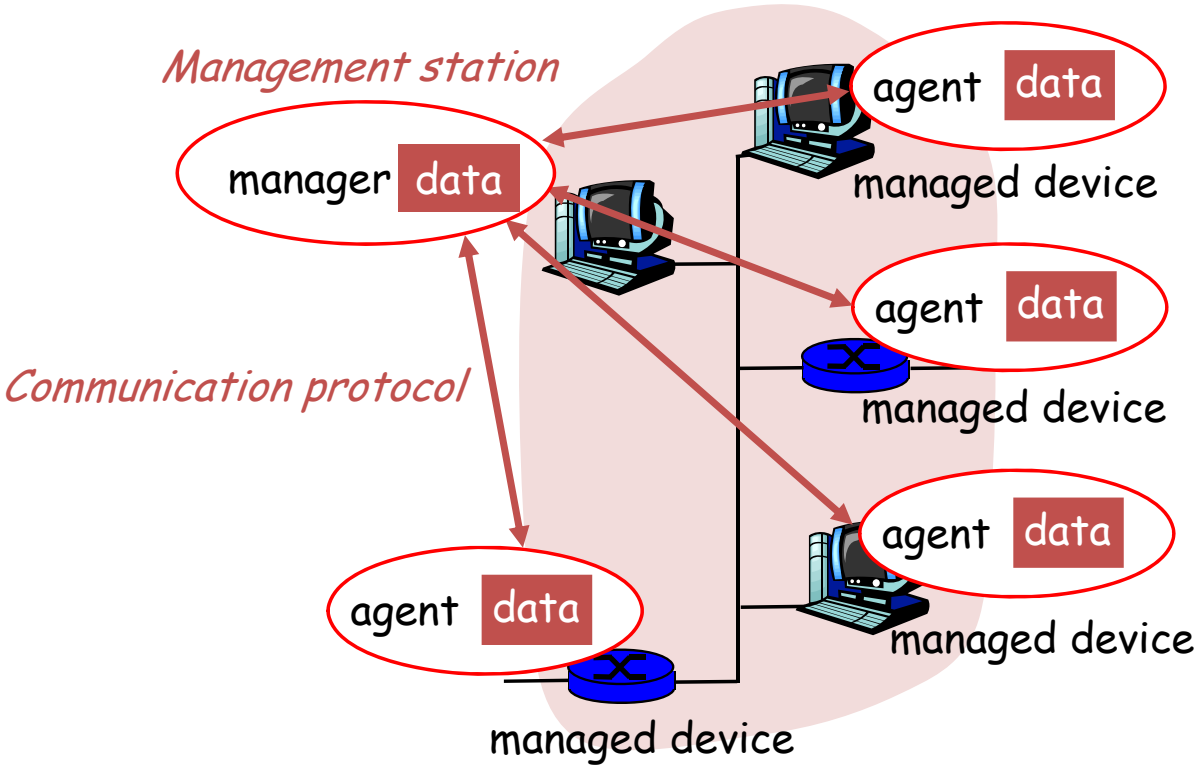
Contents

- Network Management Overview
- Network Management Model
- SMI
- MIB
- SNMP
- SNMPv2, SNMPv3, RMON

Network Management Model



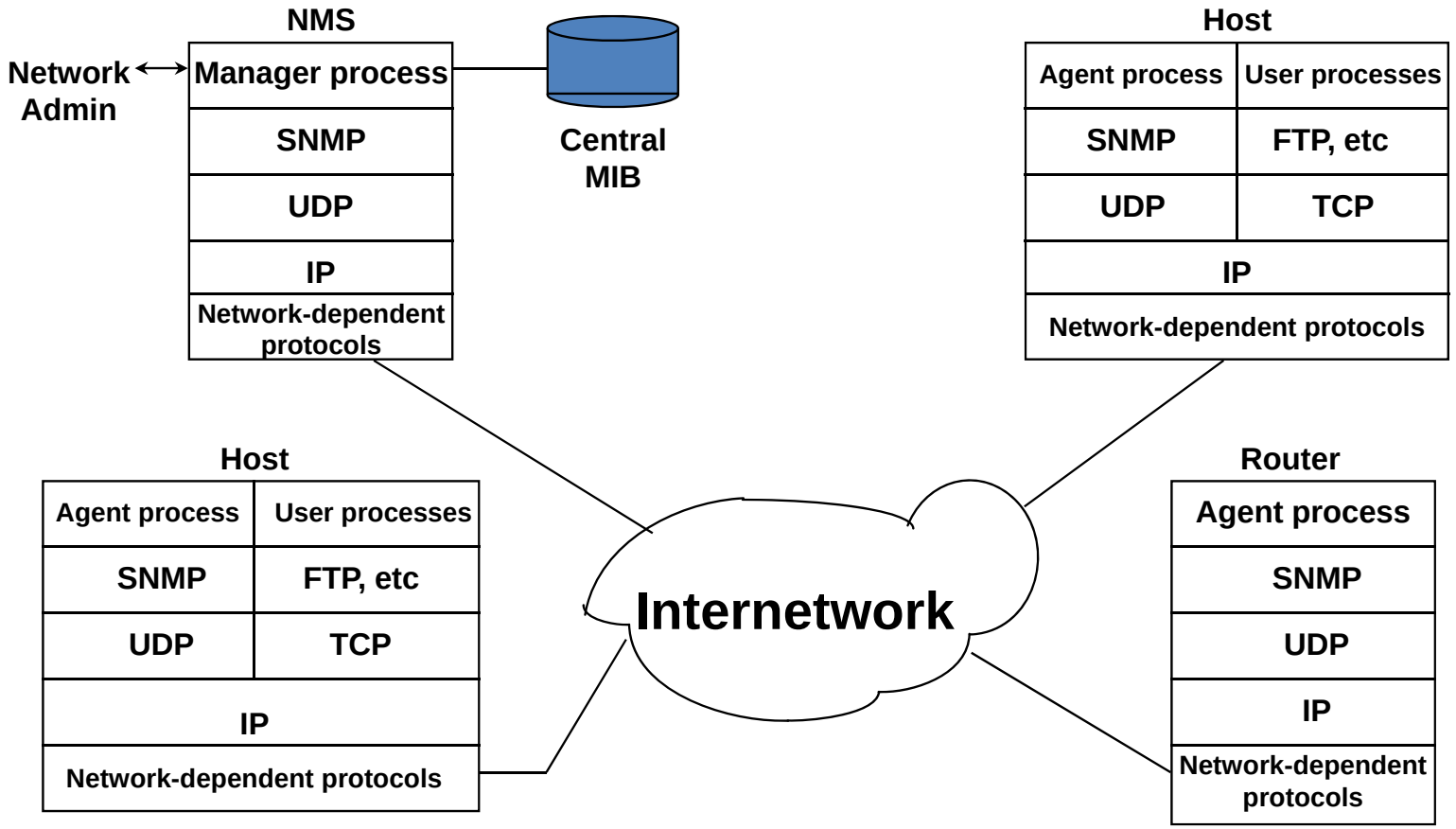
Network Management Model



NM Model

- Management station
  - Play a role of a client (also called manager)
  - Request services to agents
- Managed nodes
  - Play a role of a server (also called agent)
  - Collect managed data objects
  - Respond to requests of a server
- SNMP (Simple Network Management Protocol)
  - IETF standard communication protocol between a manager and agents

SNMP Protocol Architecture



Components of NM on Internet

- SMI (Structure of Management Information)
- MIB (Management Information Base)
- SNMP (Simple Network Management Protocol)

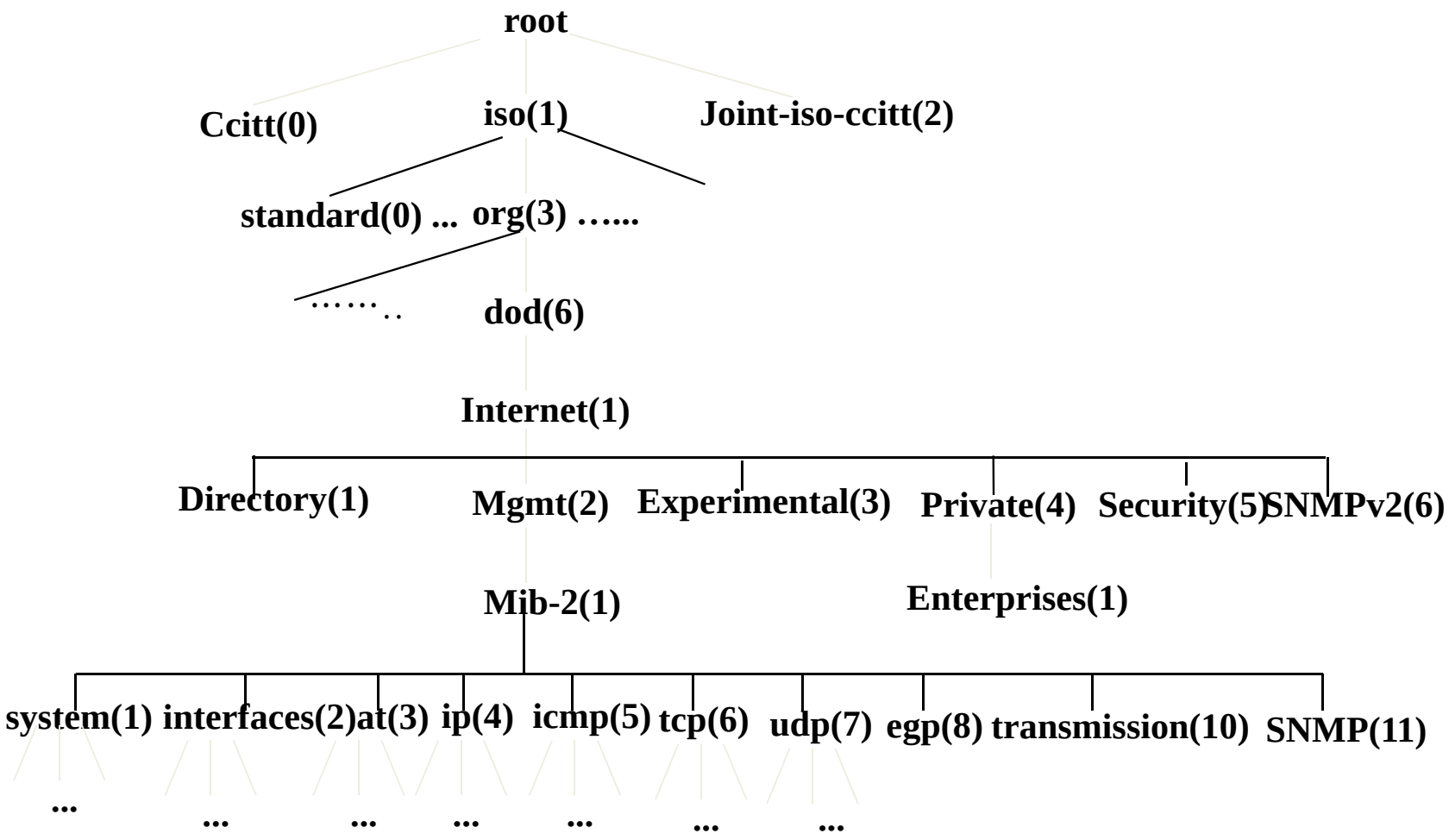
Contents

- Network Management Overview
- Network Management Model
- SMI
- MIB
- SNMP
- SNMPv2, SNMPv3, RMON

SMI

- SMI defines the naming structure (unique object identifier) and the format of managed objects (syntax and encoding).
- Object identifier
  - Objects are represented by object identifier types of the global naming tree.
- Object syntax
  - Define data types of objects
  - ASN.1
- Encoding
  - Describe the bit representation to convey object values.
  - Basic Encoding Rule (BER)

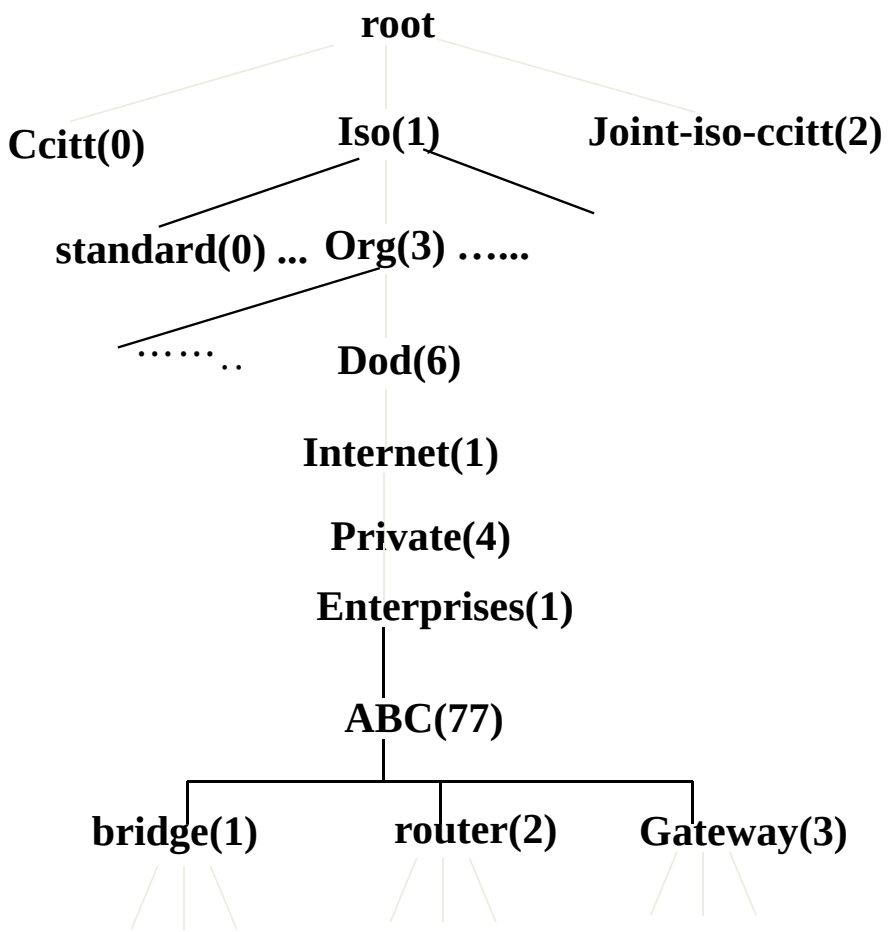
ISO/ITU-T Global Naming Tree



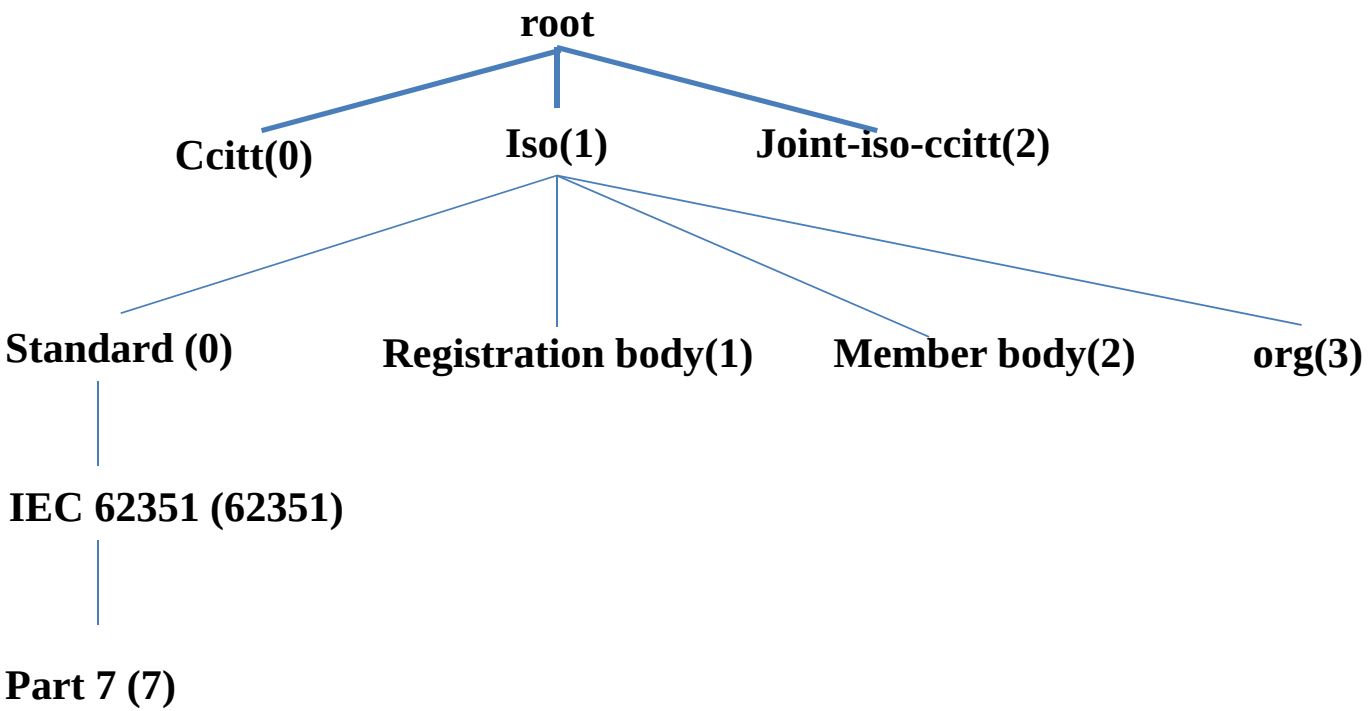
Internet subnode

- Directory
  - Reserved for future use with the OSI directory(X.500)
- Mgmt
  - Used for objects defined in IAM-approved documents
- Experimental
  - Used to identify objects in Internet experiments
- Private
  - Used to identify objects defined unilaterally

Vender subtree example



IEC 62351-7 object identifier structure



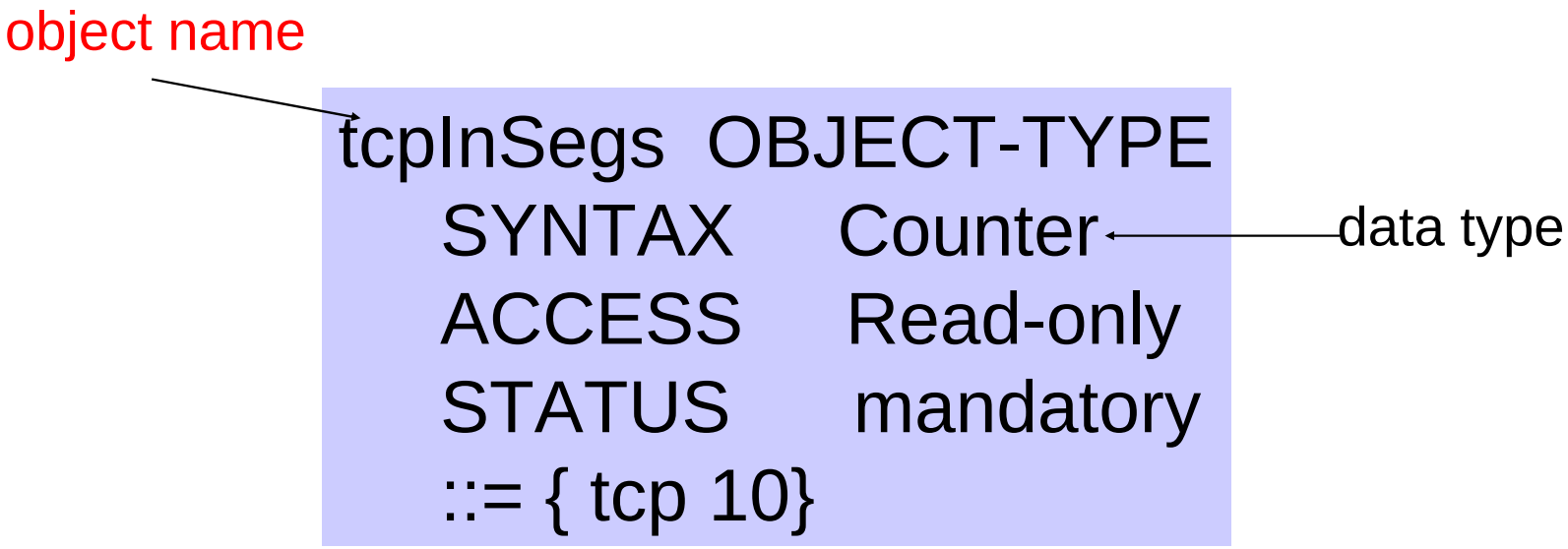
Object type macro(1)

- Define a set of related types used to describe managed objects.
- Syntax

```
object-name OBJECT-TYPE
      SYNTAX
      ACCESS
      STATUS
      DESCRIPTION
```

Object type macro(1)

- SYNTAX
  - Constructed using the universal and application-wide types
- ACCESS
  - Defines the way in which an instance of the object may be accessed, via SNMP protocol
  - *read-only, read-write, write-only, not accessible*
- STATUS
  - Indicates the implementation support required for this object
  - *mandatory, optional, deprecated, obsolute*
- INDEX


object name
tcpInSegs OBJECT-TYPE
SYNTAX Counter
ACCESS Read-only
STATUS mandatory
::= { tcp 10}
data type

Data types of managed object

- SMI only use the subset of ASN.1 data types.
- Universal types
  - INTEGER, OCTET STRING, OBJECT IDENTIFIER, NULL, SEQUENCE (SEQUENCE OF)
- application-wide types
  - NetworkAddress, IpAddresss, Counter, Gauge, TimeTicks, Opaque

Application-wide data types

- IpAddress
  - represents an IP address defined as 4 octets
- Counter
  - a non-negative integer that increases to a maximum value of 2^{32}-1 and then wraps around to 0
- Gauge
  - a counting value that can increase or decrease and has a maximum range of 0 to 2^{32}-1
- TimeTicks
  - non-negative integer used to record time
- Opaque
  - a special data type which enables the exchange of nonstandard information

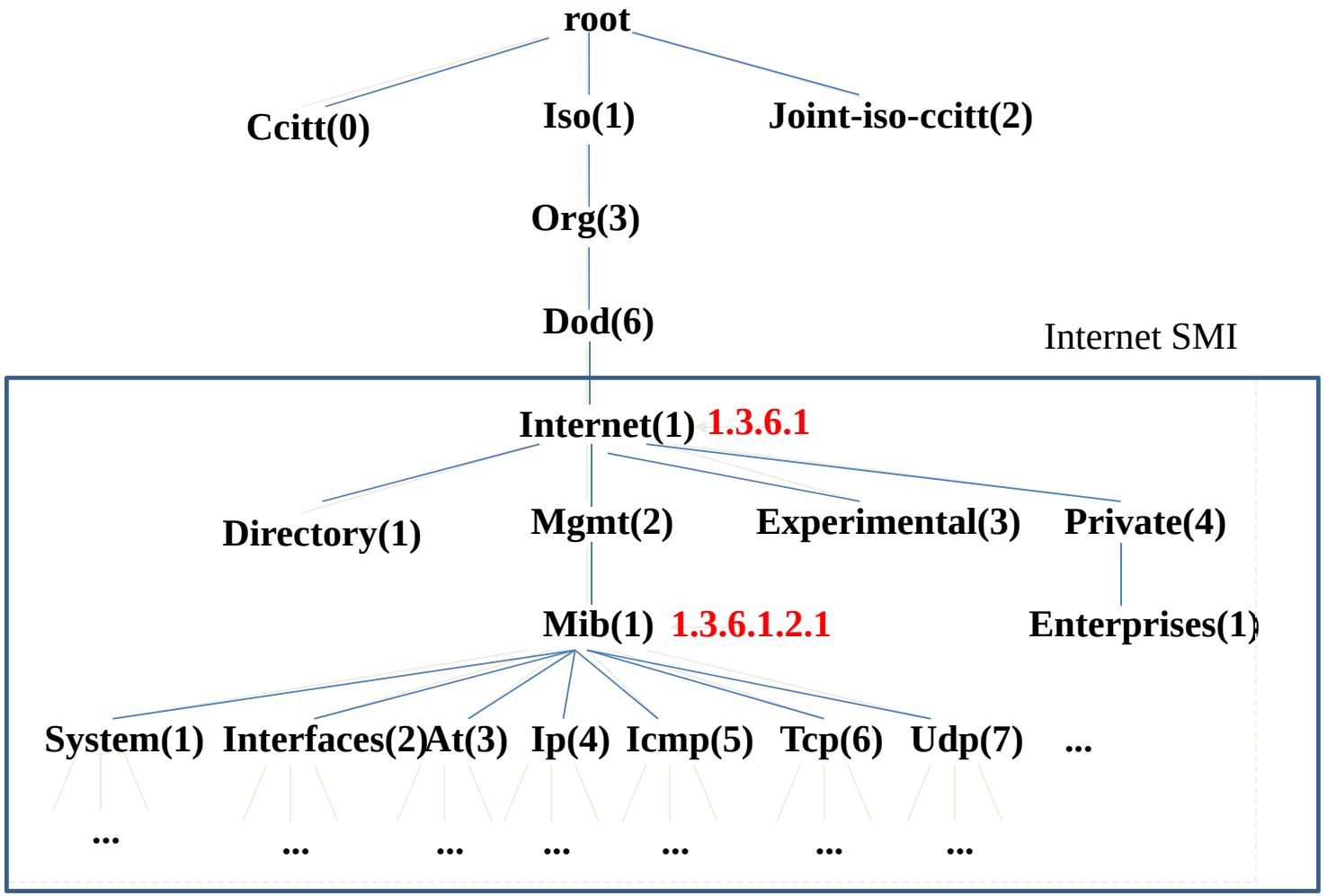
Object Identifier (1)

- Object Identifier
  - Begin with the root of the object identifier tree, and connect with the integers denoting each stage, and intersperse the period(.) between integers.
  - All variables of MIB-II begin with 1.3.6.1.2.1.
  - The textual name corresponding with each node
    - 1.3.6.1.2.1 = iso.org.dod.internet.mgmt.mib
    - 1.3.6.1.2.1.7.1 = iso.org.dod.internet.mgmt.mib.udp.udpInDatagrams
    - 1.3.6.1.2.1.4.3 = iso.org.dod.internet.mgmt.mib.ip.ipInReceive
  - The iso.org.dod.internet.private.enterprise(=1.3.6.1.4.1) has vendor-specific MIBs. Currently about 400 identifiers are defined in IETF RFCs.

Object Identifier (2)

- Name OBJECT IDENTIFIER ::= {path}
  - directory OBJECT IDENTIFIER ::= {1.3.6.1.1.}
  - directory OBJECT IDENTIFIER ::= {internet 1}
- management subtree
  - Currently only MIB-2 is defined.
  - path: 1.3.6.1.2.1

Object Identifier Name



Contents

- Network Management Overview
- Network Management Model
- SMI
- MIB
- SNMP
- SNMPv2, SNMPv3, RMON

Management Information Base(MIB)

- features
  - RFC 1213(MIB-II)
  - Managed nodes(agents) collect information relating to network interface status, transmited/received/discarded packets, error messages, etc.
  - All the information collected and maintained by agents are called MIB.
  - MIB is the target on which a manager and agents should install and query.
  - Thus, data objects of MIB should be defined and have unique names.
  - SMI specifies the rules of the MIB structure and MIB variables. (rfc1155).

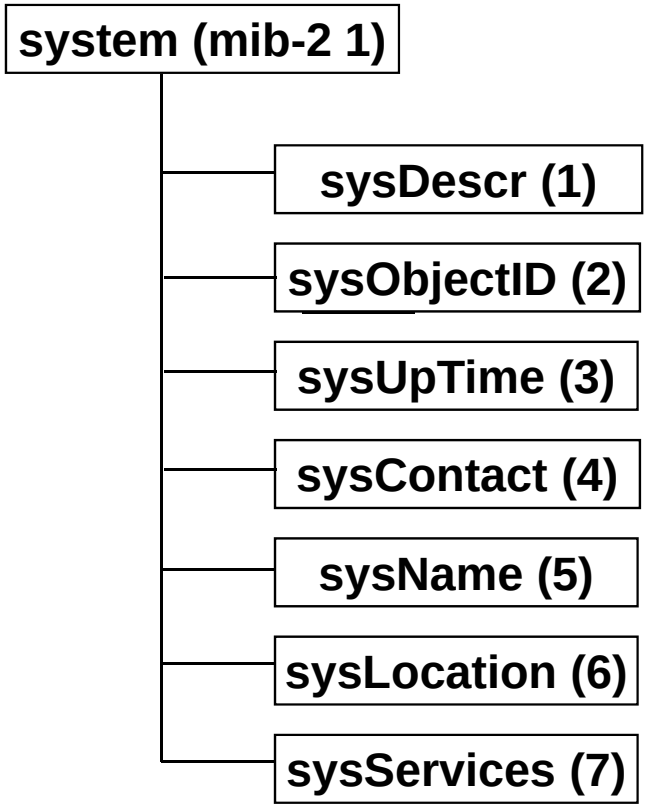
MIB-II

- RFC 1213
- The superset of MIB-I(RFC 1156)
- The most important MIB specification, including overall managed objects
- Define 10 groups of objects
- MIB-II objects should be implemented if they can be applied to devices.

MIB-II Groups

Group	Description
system	overall information about the system
interfaces	information about the interfaces from the system to a network
at	description of address translation table for internet-to-subnet address mapping
ip	information related to IP on this system
icmp	information related to ICMP on this system
tcp	information related to TCP on this system
udp	information related to UDP on this system
egp	information related to EGP on this system
dot3	information about the transmission schemes and access protocols at each system interface
snmp	information related to SNMP on this system

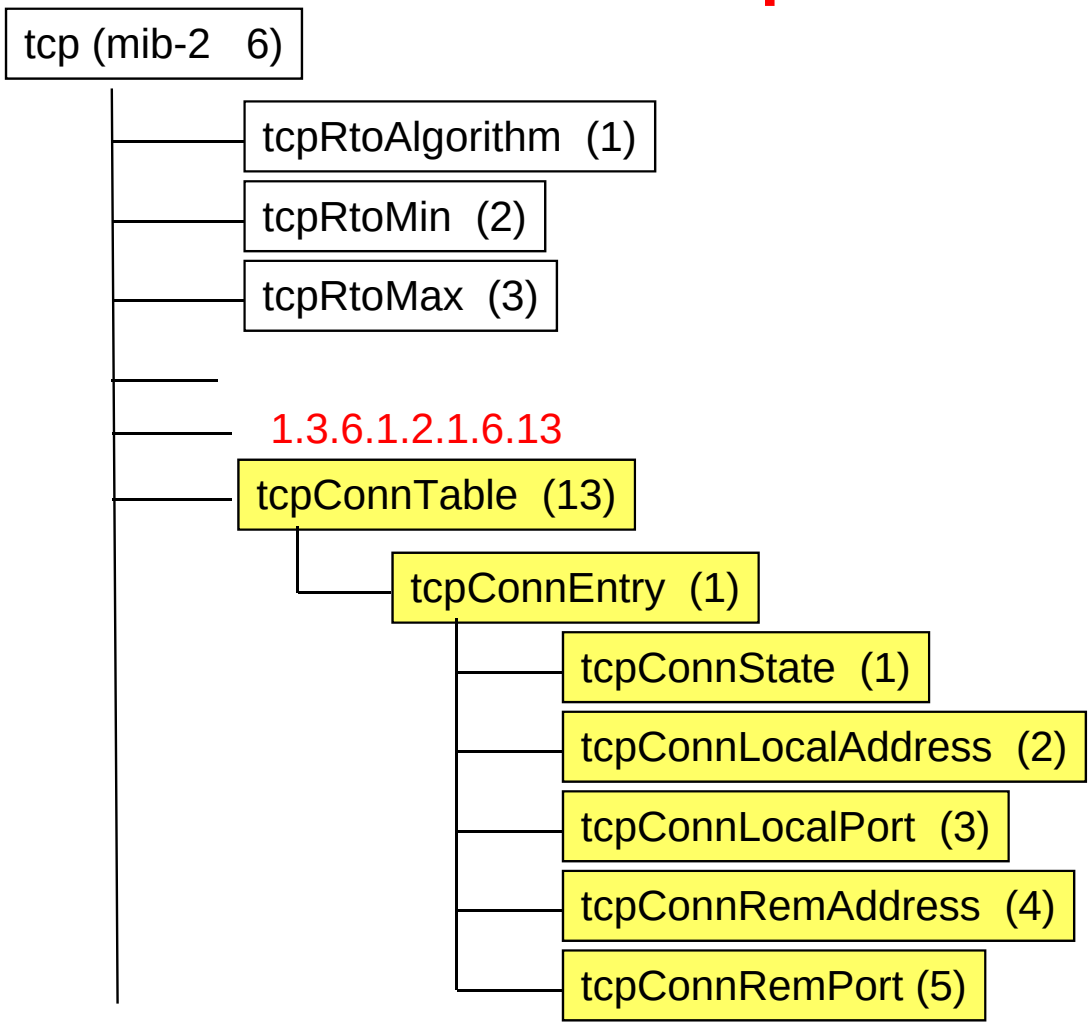
MIB-II System Group



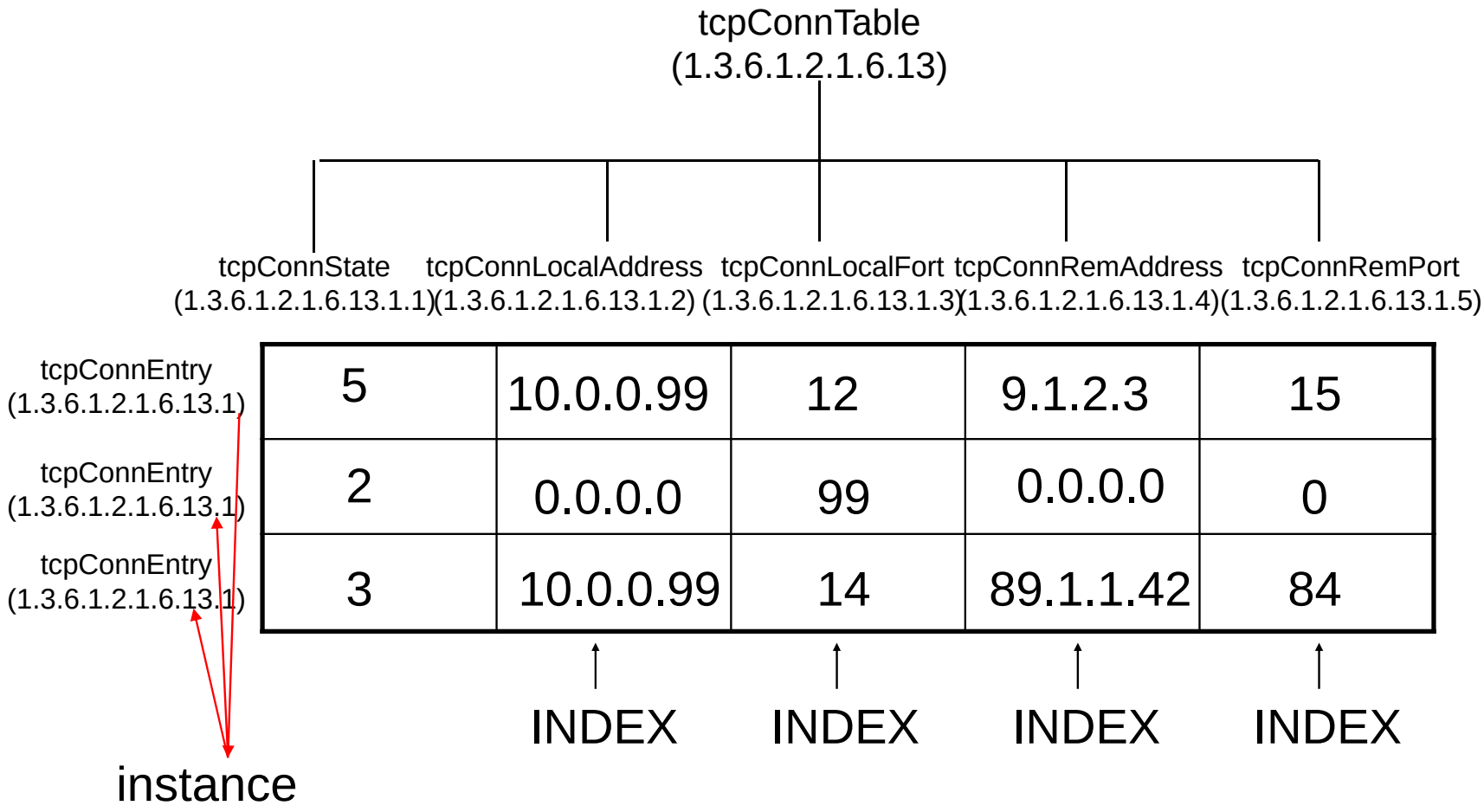
System Group Objects

Object	Syntax	Access	Description
sysDescr	DisplayString (SIZE (0 ... 255))	RO	A description of the entity, such as hardware, operating system, etc.
sysObjectID	OBJECT IDENTIFIER	RO	The vendor's authoritative identification of the network management subsystem contained in the entity.
sysUpTime	TimeTicks	RO	The time since the network management portion of the system was last reinitalized.
sysContact	DisplayString (SIZE (0 ... 255))	RW	The contact information of the contact person for this managed node.
sysName	DisplayString (SIZE (0 ... 255))	RW	An administratively assigned name for this managed node.
sysLocation	DisplayString (SIZE (0 ... 255))	RW	The physical location of this node
sysServices	INTEGER (0 ... 127)	RO	A value that indicates the set of services this entity primarily offers

Example


tcp (mib-2 6)
tcpRtoAlgorithm (1)
tcpRtoMin (2)
tcpRtoMax (3)
1.3.6.1.2.1.6.13
tcpConnTable (13)
tcpConnEntry (1)
tcpConnState (1)
tcpConnLocalAddress (2)
tcpConnLocalPort (3)
tcpConnRemAddress (4)
tcpConnRemPort (5)

Example


tcpConnTable
(1.3.6.1.2.1.6.13)
tcpConnState
(1.3.6.1.2.1.6.13.1.1)
tcpConnLocalAddress
(1.3.6.1.2.1.6.13.1.2)
tcpConnLocalFort
(1.3.6.1.2.1.6.13.1.3)
tcpConnRemAddress
(1.3.6.1.2.1.6.13.1.4)
tcpConnRemPort
(1.3.6.1.2.1.6.13.1.5)
tcpConnEntry
(1.3.6.1.2.1.6.13.1)
tcpConnEntry
(1.3.6.1.2.1.6.13.1)
tcpConnEntry
(1.3.6.1.2.1.6.13.1)
5
10.0.0.99
12
9.1.2.3
15
2
0.0.0.0
99
0.0.0.0
0
3
10.0.0.99
14
89.1.1.42
84
INDEX
INDEX
INDEX
INDEX
instance

Instance identification

- Identify by using INDEX
- Lexicographical ordering

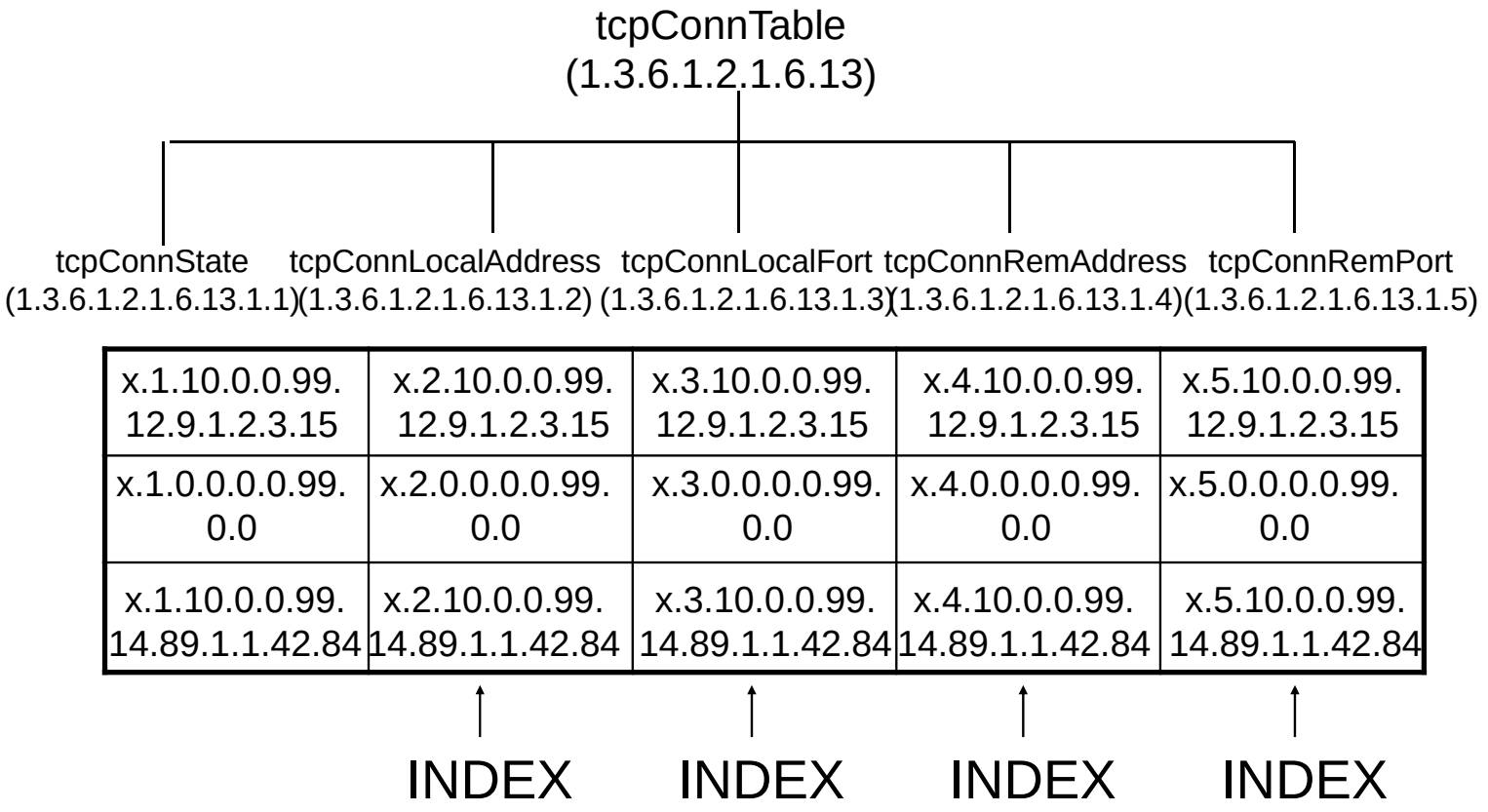
Example

- Using Index

x.i.(tcpConnLocalAddress).(tcpConnLocalPort).(tcpConnRemAddress).(tcpConnRemPort)

x: = 1.3.6.1.2.1.6.13.1 = object identifier of tcpConnEntry
i = the last sub-identifier
(name) = value of object name

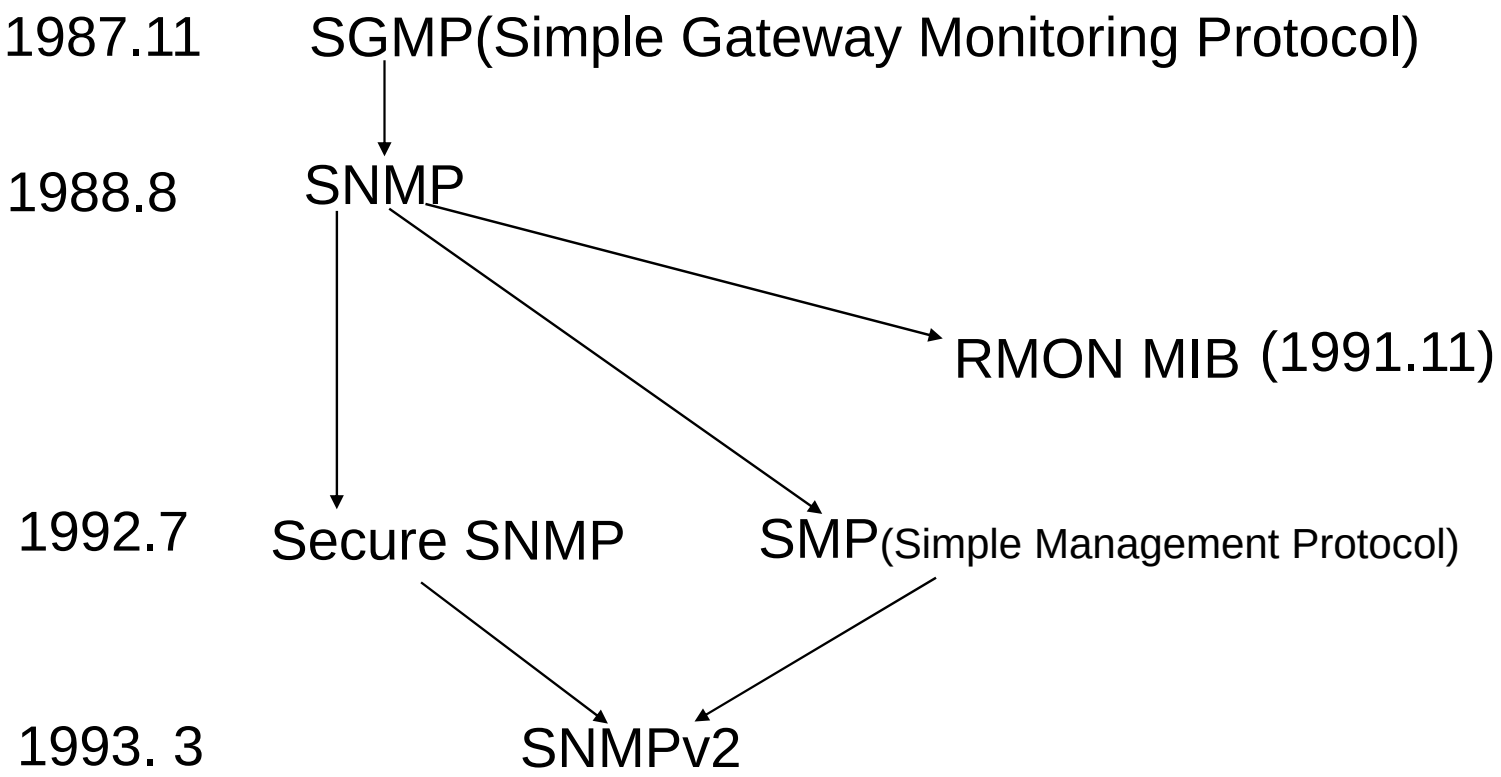
Example


tcpConnTable
(1.3.6.1.2.1.6.13)
tcpConnState
(1.3.6.1.2.1.6.13.1.1)
tcpConnLocalAddress
(1.3.6.1.2.1.6.13.1.2)
tcpConnLocalFort
(1.3.6.1.2.1.6.13.1.3)
tcpConnRemAddress
(1.3.6.1.2.1.6.13.1.4)
tcpConnRemPort
(1.3.6.1.2.1.6.13.1.5)
x.1.10.0.0.99.
12.9.1.2.3.15
x.2.10.0.0.99.
12.9.1.2.3.15
x.3.10.0.0.99.
12.9.1.2.3.15
x.4.10.0.0.99.
12.9.1.2.3.15
x.5.10.0.0.99.
12.9.1.2.3.15
x.1.0.0.0.0.99.
0.0
x.2.0.0.0.0.99.
0.0
x.3.0.0.0.0.99.
0.0
x.4.0.0.0.0.99.
0.0
x.5.0.0.0.0.99.
0.0
x.1.10.0.0.99.
14.89.1.1.42.84
x.2.10.0.0.99.
14.89.1.1.42.84
x.3.10.0.0.99.
14.89.1.1.42.84
x.4.10.0.0.99.
14.89.1.1.42.84
x.5.10.0.0.99.
14.89.1.1.42.84
INDEX
INDEX
INDEX
INDEX

Contents

- Network Management Overview
- Network Management Model
- SMI
- MIB
- SNMP
- SNMPv2, SNMPv3, RMON

SNMP History



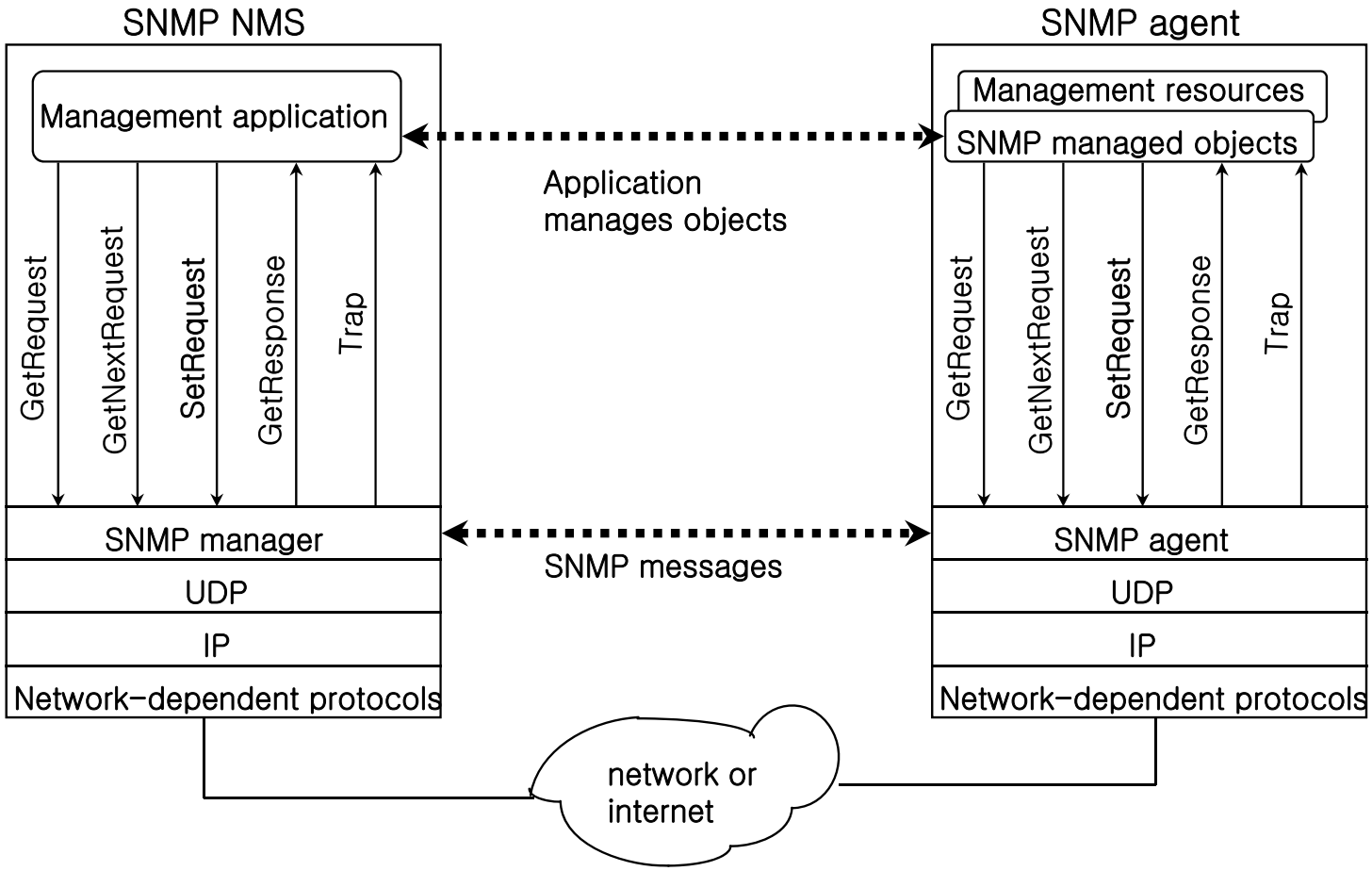
SNMP major features

- Query/response protocol to read or modify MIB variables
- Using UDP, so do not require ACKs.
- SNMP drawbacks
  - Send too many messages to the extent of degrading network performance,
  - Lack of security function
  - So, its roles are confined to network monitoring and fault surveillance.

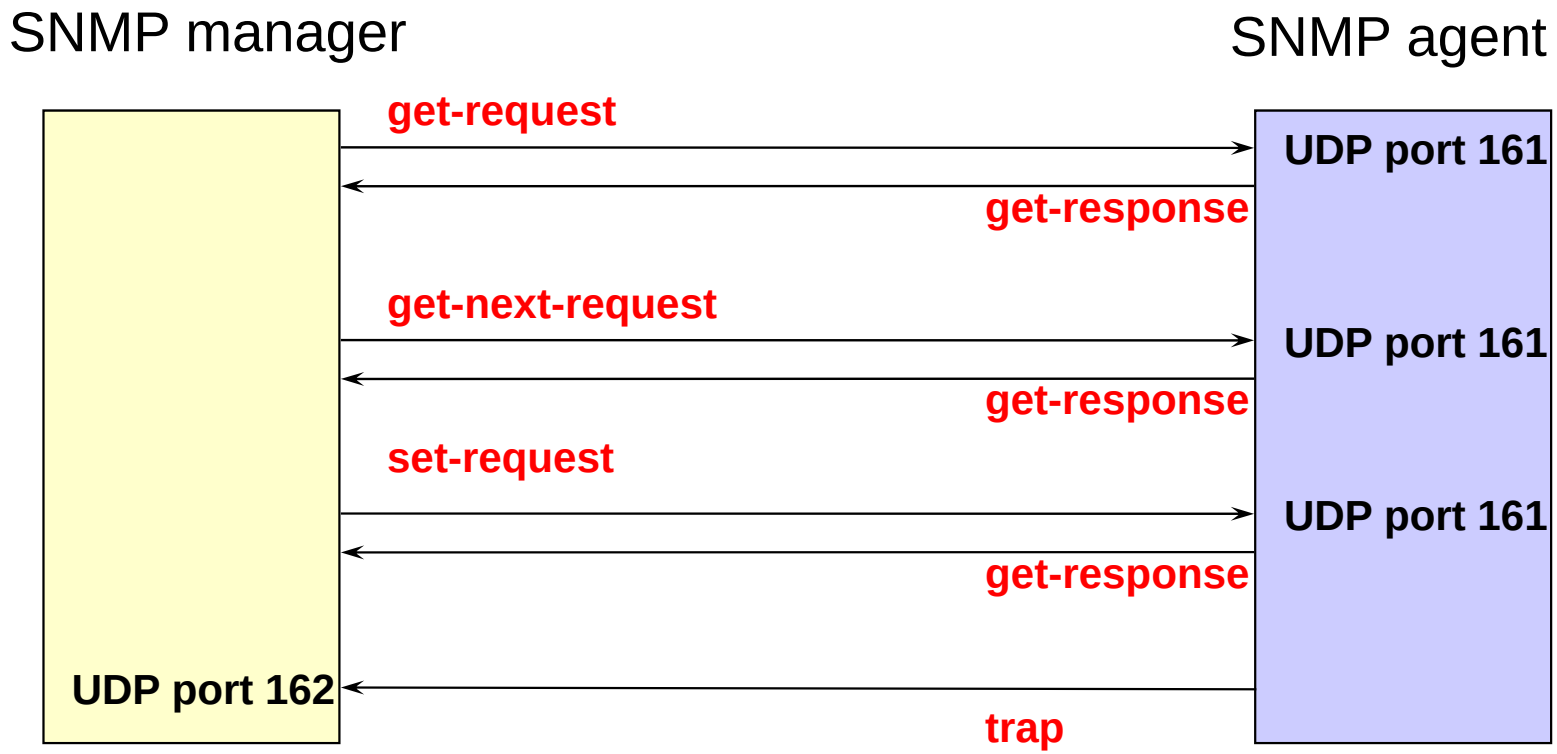
SNMP Upgrade

- IETF addressed the security issue of SNMP by issuing Secure SNMP in 1992.
- Secure SNMP added security functions such as authentication of users, data integrity, and data encryption
- Later, enforcing the security capability of Secure SNMP and improving performance, they published SNMPv3 in 1993.

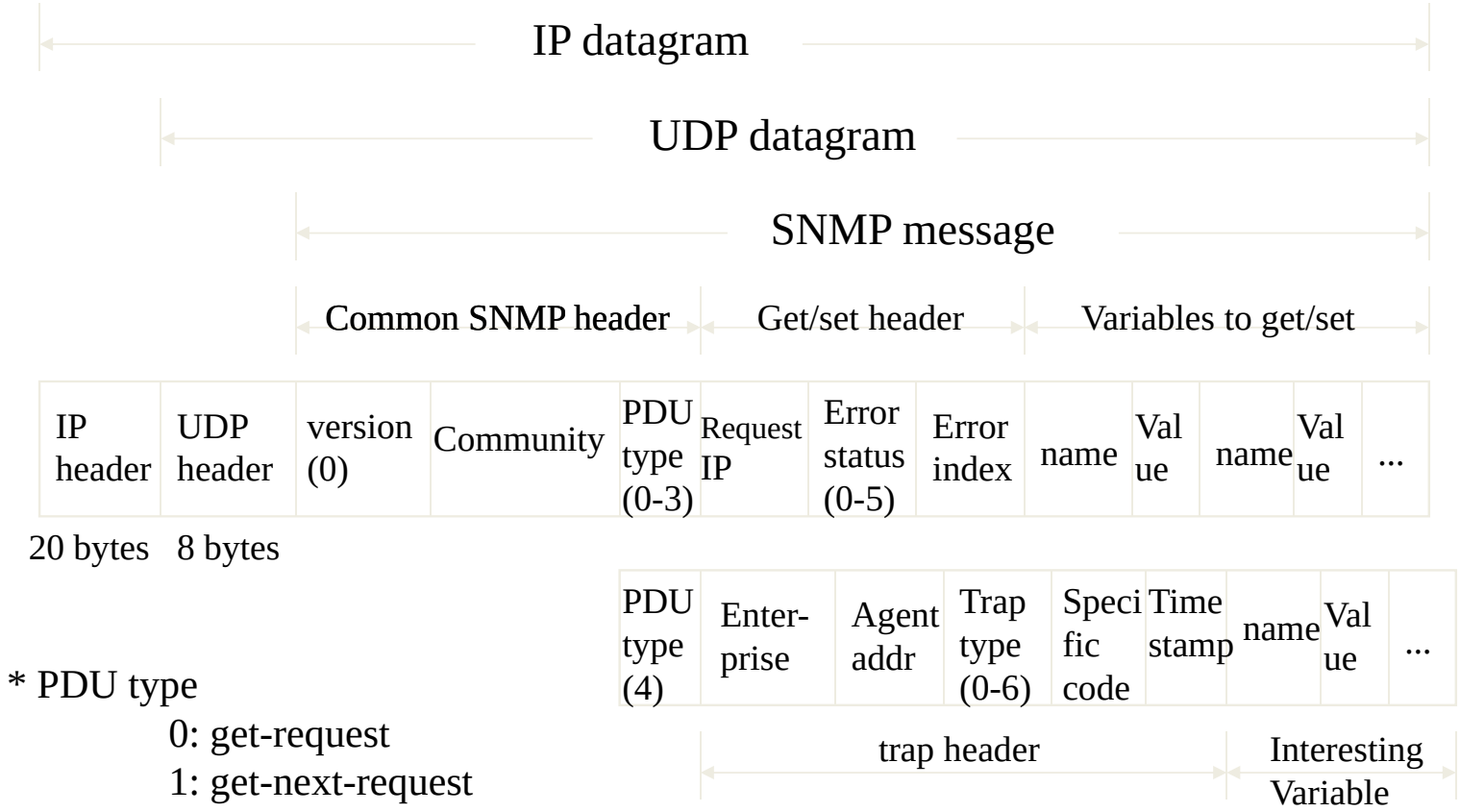
The role of SNMP



SNMP Protocol



SNMP message format (1)



* PDU type
  - 0: get-request
  - 1: get-next-request
  - 2: set-request
  - 3: get-response
  - 4: trap

SNMP message format (2)

GetRequest PDU, GetNextRequest PDU, SetRequest PDU

PDU type	request id	0	0	variables

GetResponse PDU

PDU type	request id	error status	error index	variables

Trap PDU

PDU type	enterprise	agent-addr	generic-trap	specific-trap	time stamp	variables

SNMP message format (3)

- PDU types
  - Get-request, Get-next-request
    - Used when a manager request MIB information to agents.
  - Set-request
    - Used when a manager set up information in agents.
  - Get-response
    - Used when agents reply to a manager
  - Trap
    - When agents notify a manger of emergency states without any request from a manager

Trap types

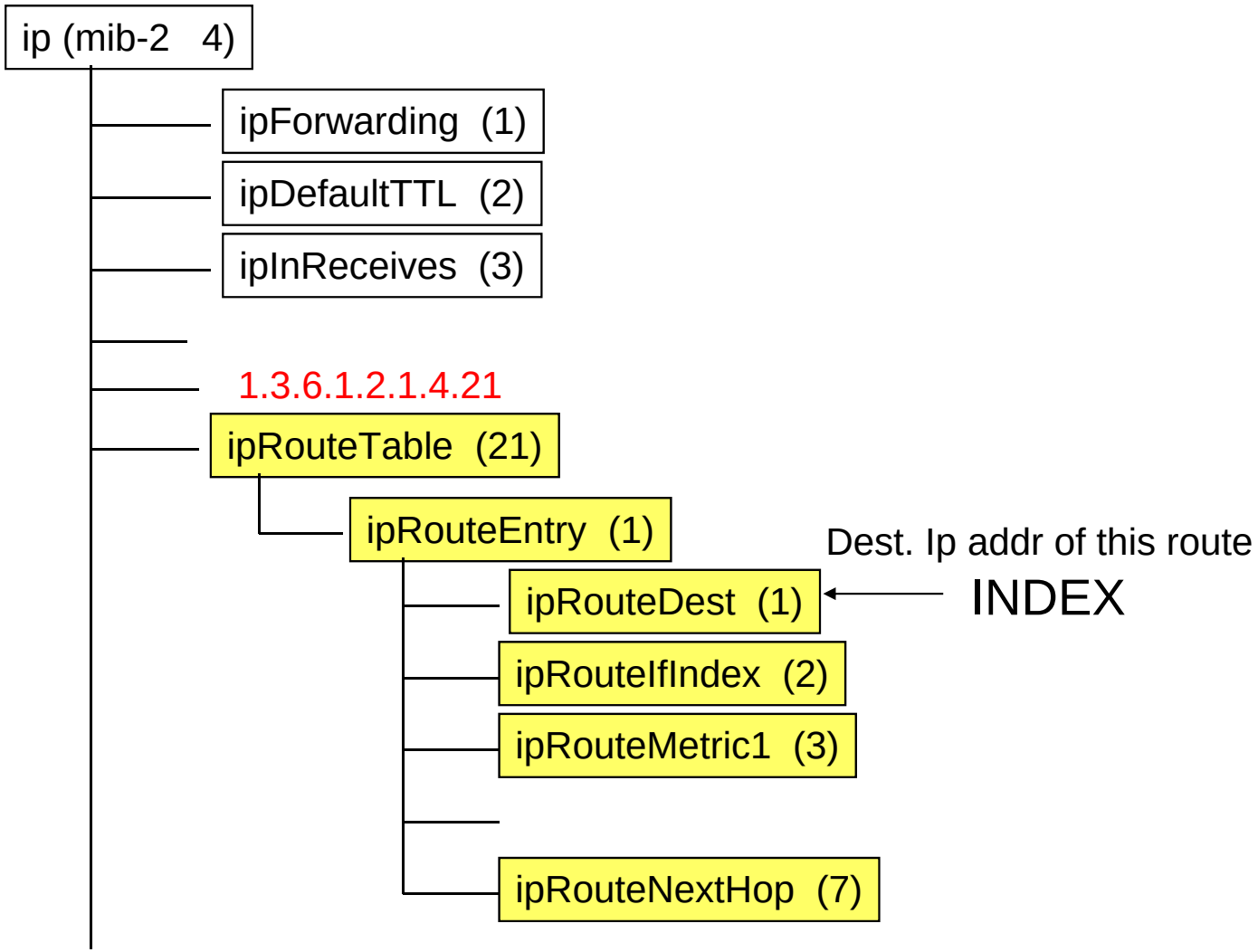
- Trap
  - Unlike other messages, trap message is sent for agents to inform of their states without any request from a manager.

Trap type	name	description
0	coldStart	Reinitializing itself, agent's configuration may be changed
1	warmStart	Reinitializing itself, agent's configuration not changed
2	linkDown	Signals a failure in one of the agent's communication link
3	linkUp	Signals one of the agent's communication link comes up
4	authenticationFailure	Signals authentication failed
5	egpNeighborLoss	Signals an EGP peer is down
6	enterpriseSpecific	Signals some enterprise-specific event has occured

Example: GetRequest

GetRequest (ipRouteDest.9.1.2.3,
ipRouteMetric1.9.1.2.3,
ipRouteNextHop.9.1.2.3)

ipRouteDest	ipRouteMetric1	ipRouteNextHop
9.1.2.3	3	99.0.0.3
10.0.0.51	5	89.1.1.42
10.0.0.99	5	89.1.1.42


ip (mib-2 4)
ipForwarding (1)
ipDefaultTTL (2)
ipInReceives (3)
1.3.6.1.2.1.4.21
ipRouteTable (21)
ipRouteEntry (1)
Dest. Ip addr of this route
ipRouteDest (1)
INDEX
ipRouteIfIndex (2)
ipRouteMetric1 (3)
ipRouteNextHop (7)

Example: GetNextRequest (1)

Suppose that a manager wants to retrieve all table information, but Has no information about the table size and contents.

GetNextRequest (ipRouteDest,
ipRouteMetric1,
ipRouteNextHop)

Then, an agent responds as follows:

GetResponse ((ipRouteDest.9.1.2.3=9.1.2.3),
(ipRouteMetric1.9.1.2.3=3),
(ipRouteNextHop.9.1.2.3=99.0.0.3))

Example: GetNextRequest (2)

Next, manager sends the following message.

GetNextRequest (ipRouteDest.9.1.2.3,
ipRouteMetric1.9.1.2.3,
ipRouteNextHop.9.1.2.3)

Then, agent responds as follows:

GetResponse ((ipRouteDest.10.0.0.51=10.0.0.51),
(ipRouteMetric1.10.0.0.51=5),
(ipRouteNextHop. 10.0.0.51=89.1.1.42))

Example: GetNextRequest (3)

Next, manager sends the following message.

GetNextRequest (ipRouteDest. 10.0.0.51,
ipRouteMetric1.10.0.0.51,
ipRouteNextHop.10.0.0.51)

Then, agent responds as follows:

GetResponse ((ipRouteDest.10.0.0.99=10.0.0.99),
(ipRouteMetric1.10.0.0.99=5),
(ipRouteNextHop.10.0.0.99=89.1.1.42))

Example: GetNextRequest (4)

Next, manager sends the following message.

GetNextRequest (ipRouteDest.10.0.0.99,
ipRouteMetric1.10.0.0.99,
ipRouteNextHop.10.0.0.99)

Then, agent responds as follows:

GetResponse ((ipRouteMetric1.9.1.2.3=3),
(ipRouteNextHop.9.1.2.3=99.0.0.3),
(ipNetToMediaIfIndex.1.3=1))

Ex: SetRequest (1)

Manager sends:

SetRequest (ipRouteMetric1.9.1.2.3=9)

Agent sends:

GetResponse (ipRouteMetric1.9.1.2.3=9)

Ex: SetRequest (3)

When deleting a row, manager sends:

SetRequest (ipRouteType.7.3.5.3=invalid)

Agent responds:

GetResponse (ipRouteType.7.3.5.3=invalid)

Ex: SetRequest (2)

When adding a new row, manager sends:

SetRequest ((ipRouteDest.11.3.3.12=11.3.3.12),
(ipRouteMetric1.11.3.3.12=9)
(ipRouteNextHop.11.3.3.12=91.0.0.5))

Contents

- Network Management Overview
- Network Management Model
- SMI
- MIB
- SNMP
- SNMPv2, SNMPv3, RMON

SNMPv2

- Supplement the drawbacks of SNMP
- Secure SNMP + SMP = SNMPv2 (1993.3)
- However, the proposal contained critical security errors, so was published excluding the security parts.
  - community-based SNMPv2 (1996.1)

Differences between SNMPv1 and SNMPv2

- Locking scheme
  - While a management system is modifying configuration of managed nodes, it can prevent from other management system interfering. It can lock a single node or a group of nodes.
- Exception condition
  - SNMP nodes ignore MIB requests which they can’t support, but, SNMPv2 can response selectively to MIB which it can support by setting “exception” flag.
- Add error codes

SNMPv3

- SNMPv1 and SNMPv2 lacks security capability.
- SNMPv3 supplement security capability.
  - Authentication: verifying that messages are from authenticated users
  - Encryption of messages

RMON (Remote Network Monitoring)

- RFC 2819
- Current management model should enforce every managed nodes to install agents.
- Too many nodes entail too much traffic, especially in the network consisting of many subnets.
- To cope with this problem, a single RMON agent is installed on each subnet. The RMON agent collects information on the subnet and sends this information to RMON manager.
- RMON agents capture, analyze, and store each subnet traffic, and later inform RMON manager of this information.

RMON

- Extend the SNMP functions
- Allowing remote network monitoring
- MAC layer monitoring
- Define ROMON MIB which supplements MIB II
  - In MIB-II, a manager collect information on each devices.
  - In ROMON MIB, a manager can collect information on LAN itself.
- Often called network monitor, analyzer, probe