INTERNET MANAGEMENT PROTOCOLS

TUTORIAL T5 - PRESENTED AT IM'2001
SEATTLE, USA
14 MAY 2001

AIKO PRAS
UNIVERSITY OF TWENTE
THE NETHERLANDS

pras@ctit.utwente.nl
http://wwwhome.ctit.utwente.nl/~pras

http://www.simpleweb.org/bibliography/tutorials.html

OVERVIEW

BACKGROUND
- HISTORY, GOALS & STANDARDS

- STRUCTURE OF MANAGEMENT INFORMATION
  - SCALARS
  - TABLES

- MANAGEMENT INFORMATION BASES
  - OVERVIEW
  - MIB-II
  - SNMPv2, IF & IP MIB

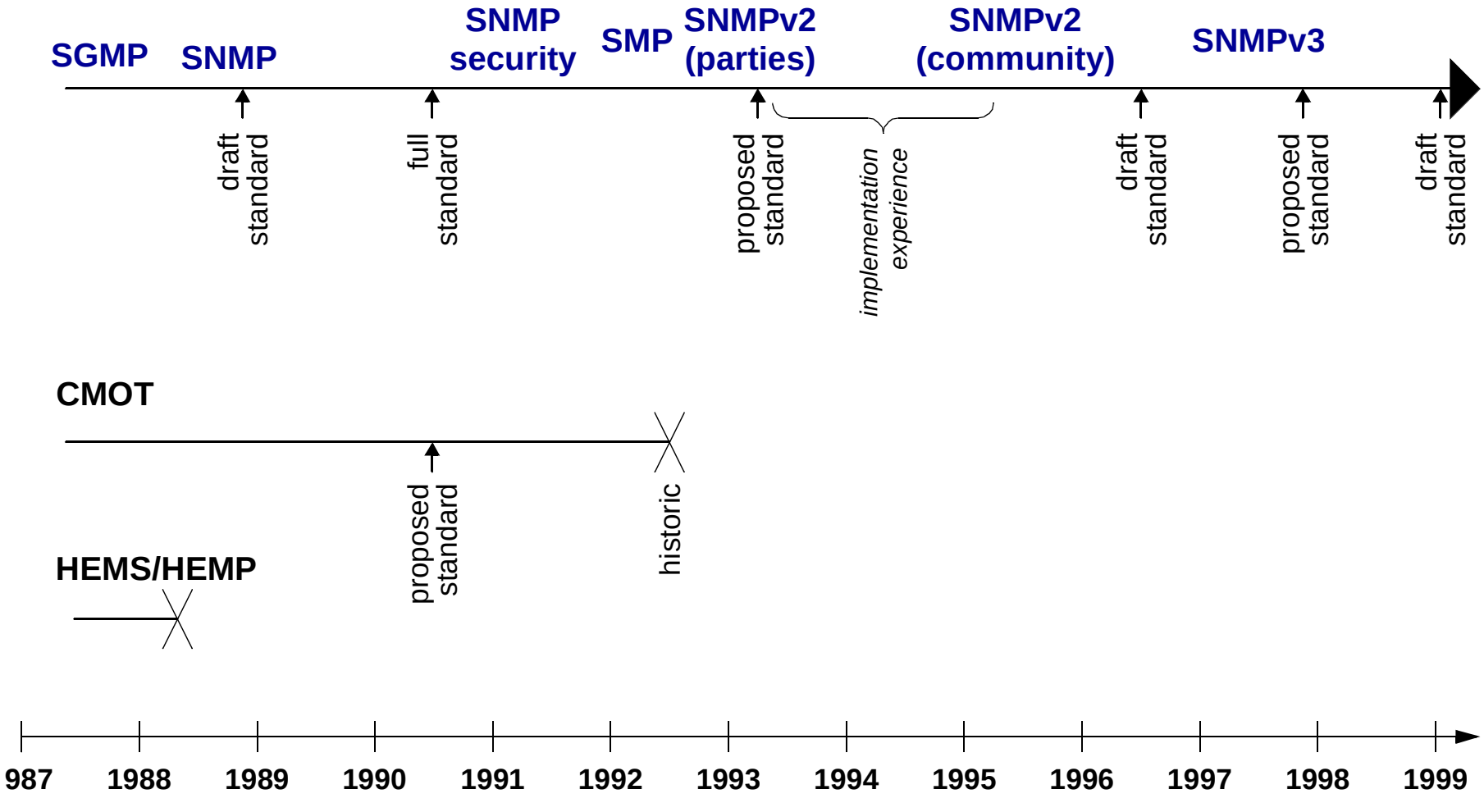
- SIMPLE NETWORK MANAGEMENT PROTOCOL
  - VERSION 1
  - VERSION 2
  - VERSION 3

AGENTX

DISMAN

FURTHER INFORMATION

SNMP HISTORY



SNMP GOALS

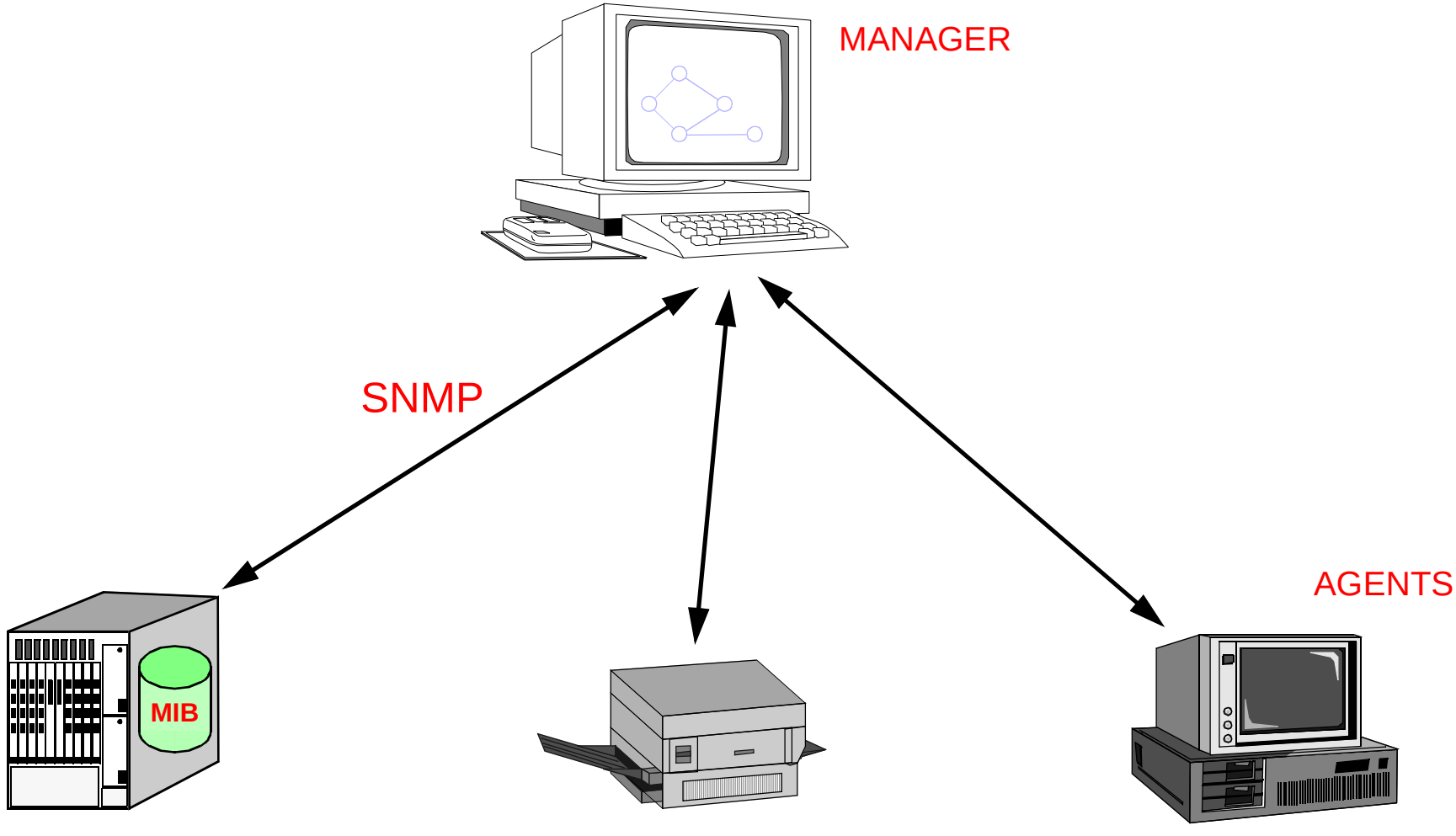
UBIQUITY
- PCs AND CRAYs

INCLUSION OF MANAGEMENT SHOULD BE INEXPENSIVE
- SMALL CODE
- LIMITED FUNCTIONALITY

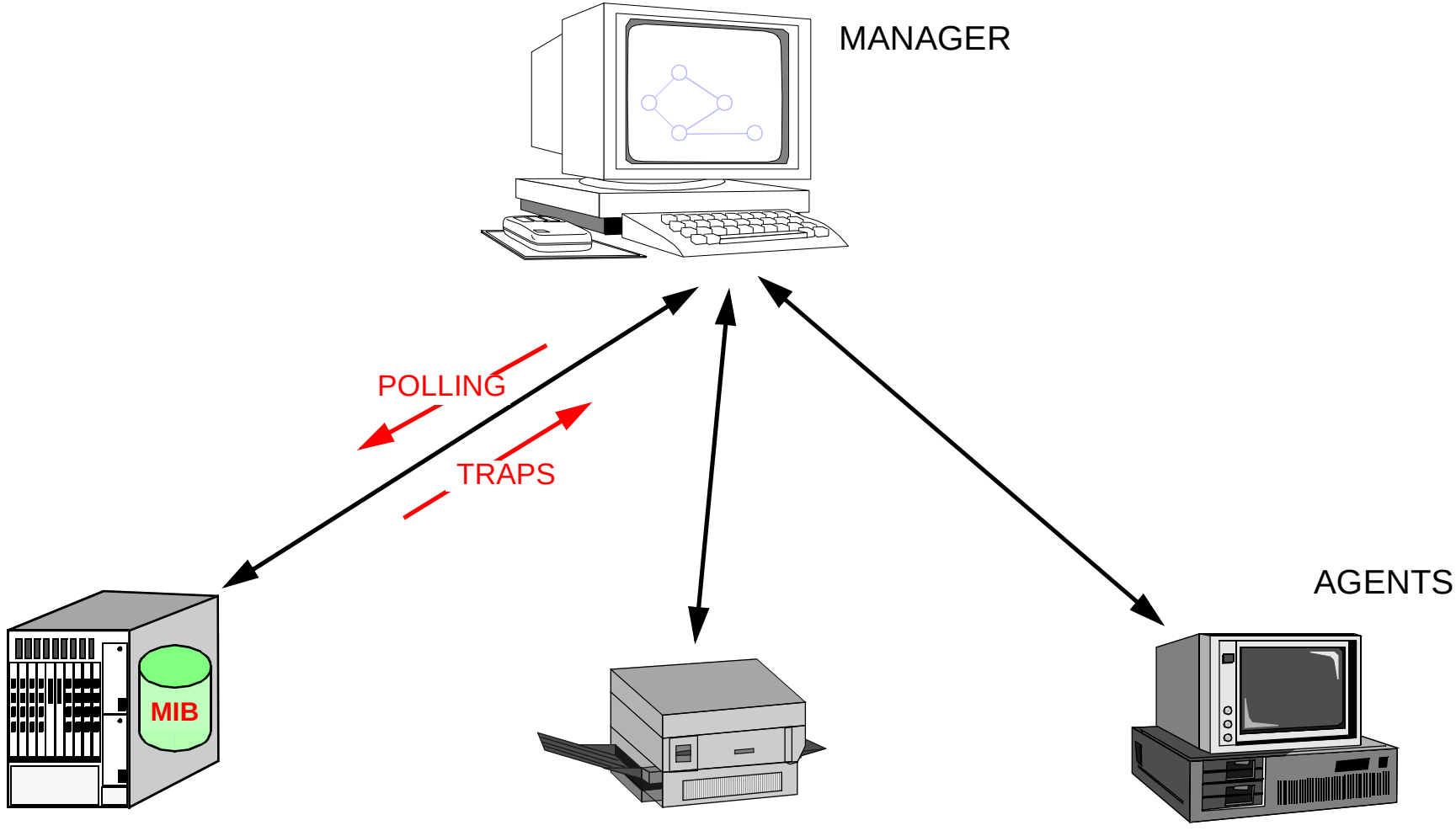
MANAGEMENT EXTENSIONS SHOULD BE POSSIBLE
- NEW MIBs

MANAGEMENT SHOULD BE ROBUST
- CONNECTIONLESS TRANSPORT

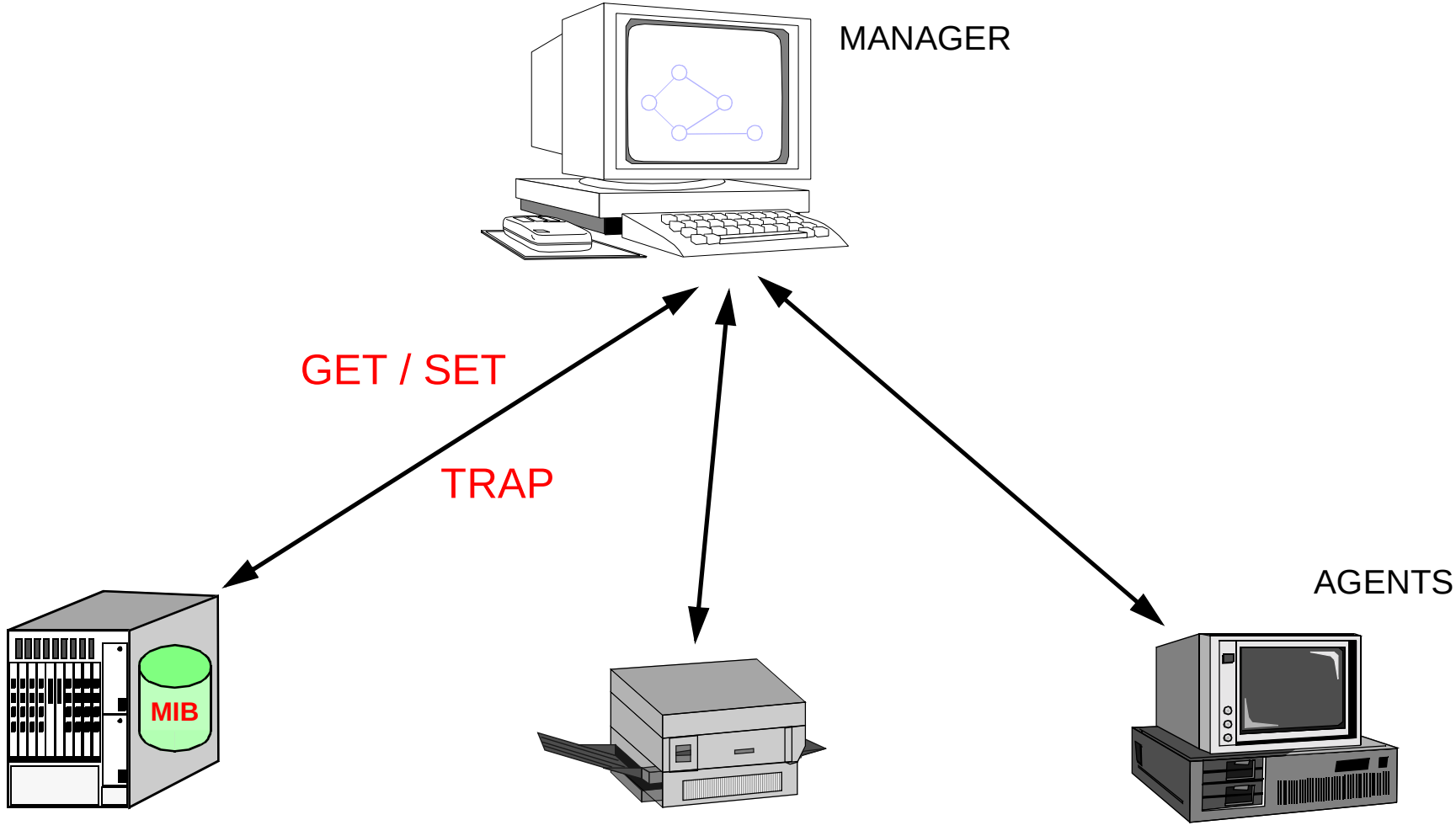
PRINCIPLE OPERATION



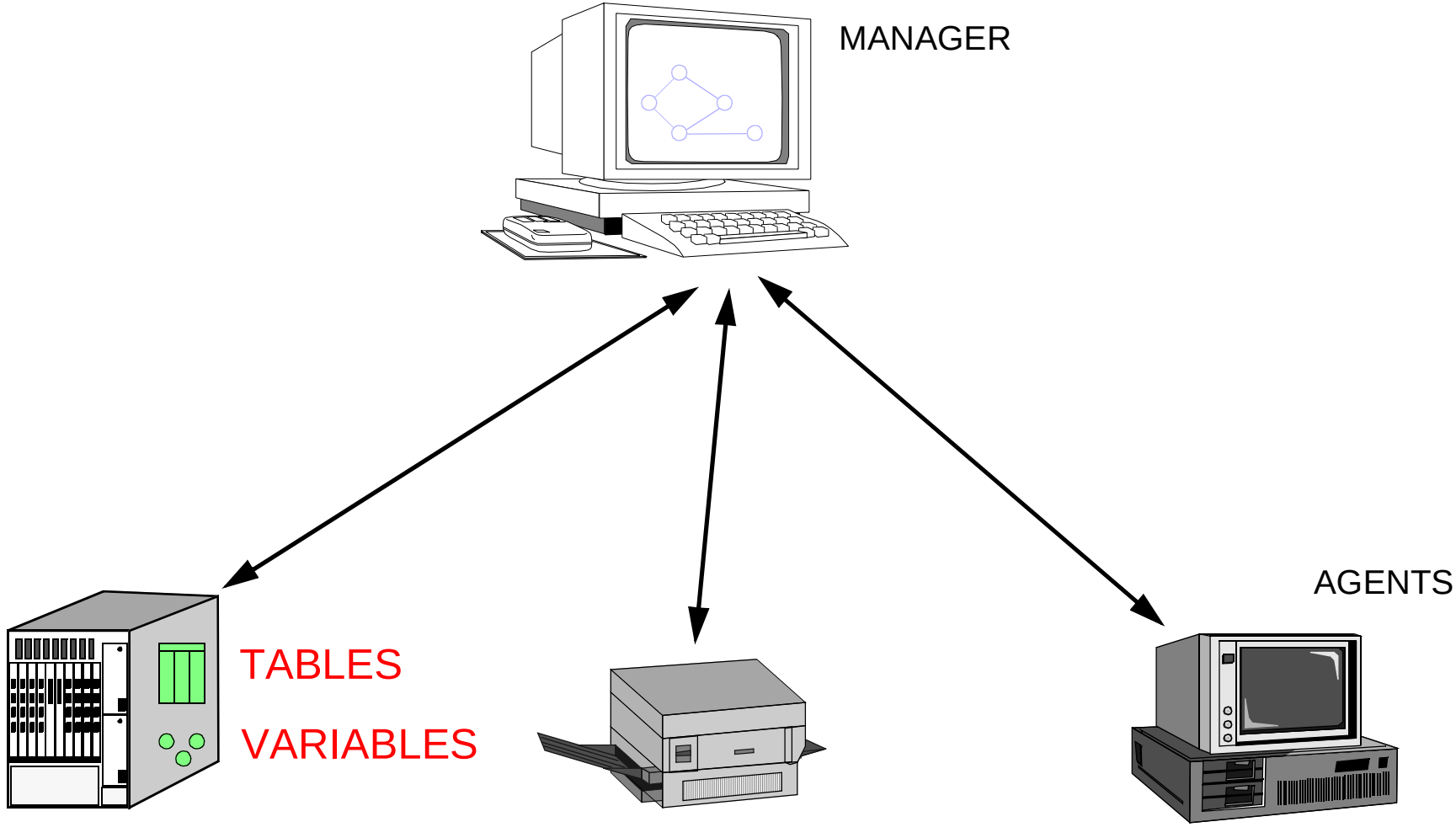
PRINCIPLE OPERATION



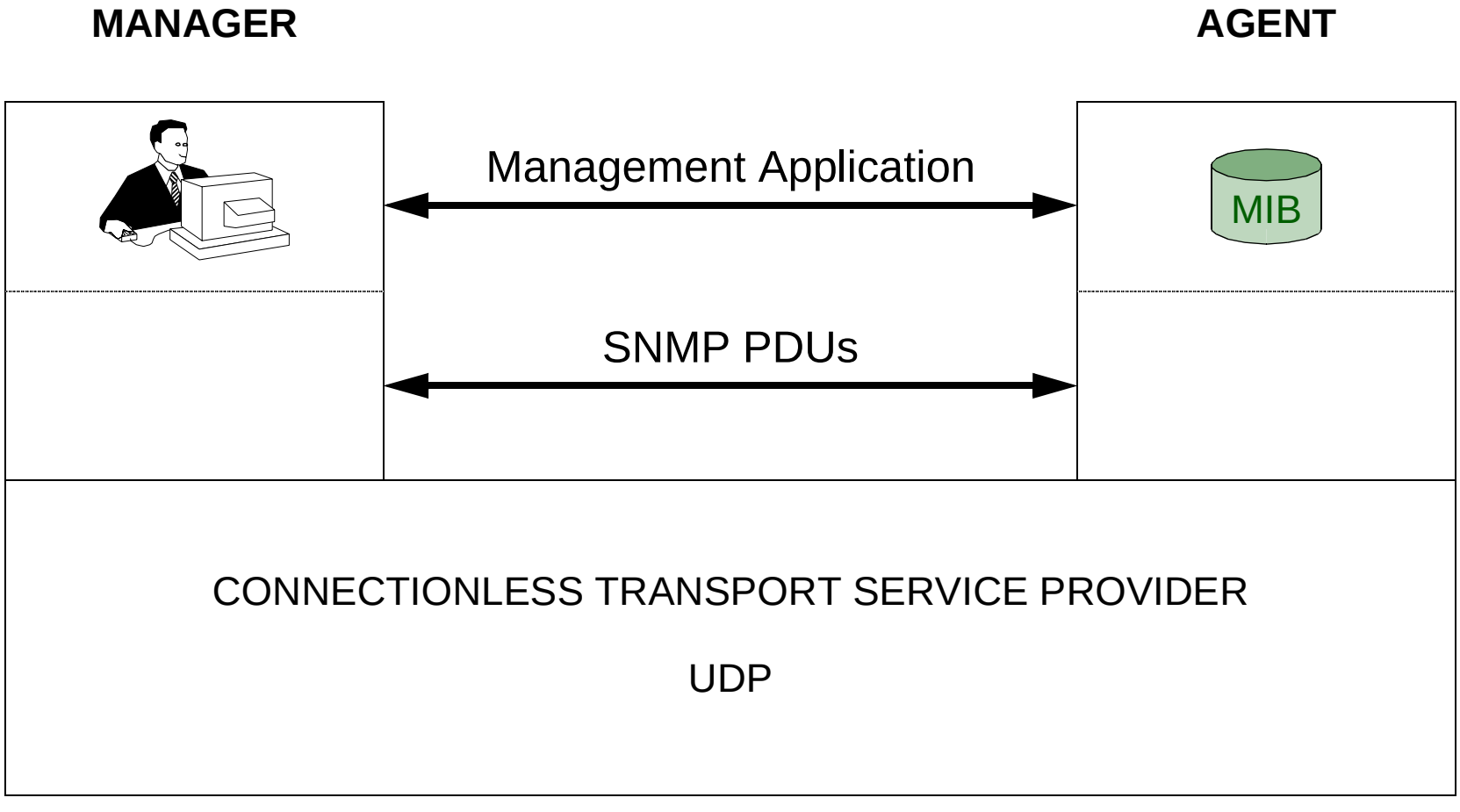
PRINCIPLE OPERATION



PRINCIPLE OPERATION



SNMP STRUCTURE



STANDARDS

SMI

- STRUCTURE OF MANAGEMENT INFORMATION
- RFC 1155

MIB-II

- MANAGEMENT INFORMATION BASE
- RFC 1213
- A LARGE NUMBER OF ADDITIONAL MIBs EXIST

SNMP

- SIMPLE NETWORK MANAGEMENT PROTOCOL
- RFC 1157
- NAME IS USED IN A MORE GENERAL SENSE

NEWER VERSIONS: SNMPv2 & SNMPv3

SMI

STRUCTURE OF MANAGEMENT INFORMATION

RFC 1155: SMIv1

RFC 1212: CONCISE MIB DEFINITIONS

RFC 2578: SMIv2

RFC 2579: TEXTUAL CONVENTIONS

MAKES THE DEFINITION OF (NEW) MIBs EASIER

SMI

MANAGEMENT INFORMATION WITHIN MANAGED SYSTEMS
MUST BE REPRESENTED AS:

- SCALARS
- TABLES

(= TWO DIMENSIONAL ARRAYS OF SCALARS)

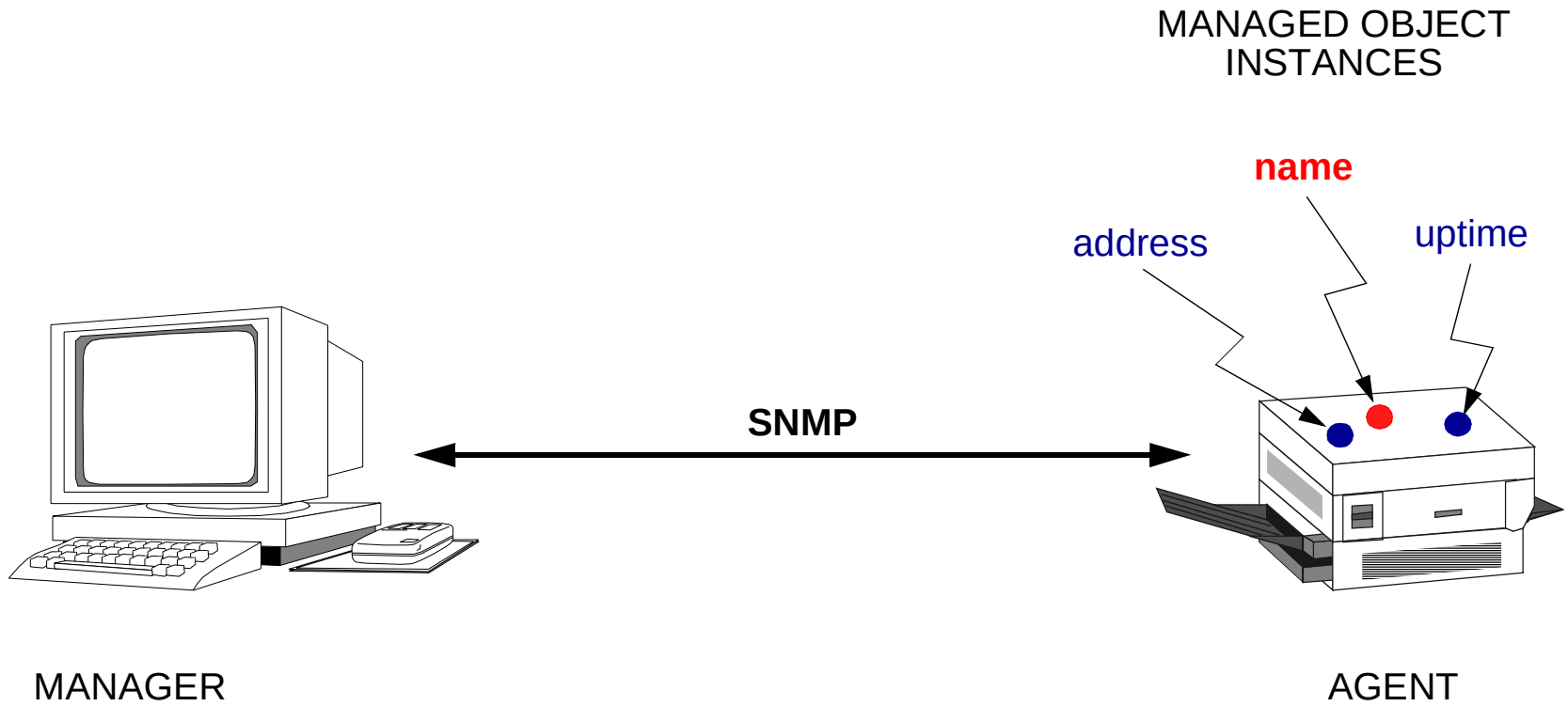
THE SNMP PROTOCOL CAN ONLY EXCHANGE
(A LIST OF) SCALARS

DEFINED IN TERMS OF ASN.1 CONSTRUCTS

SMI: DATA TYPES FOR SCALARS

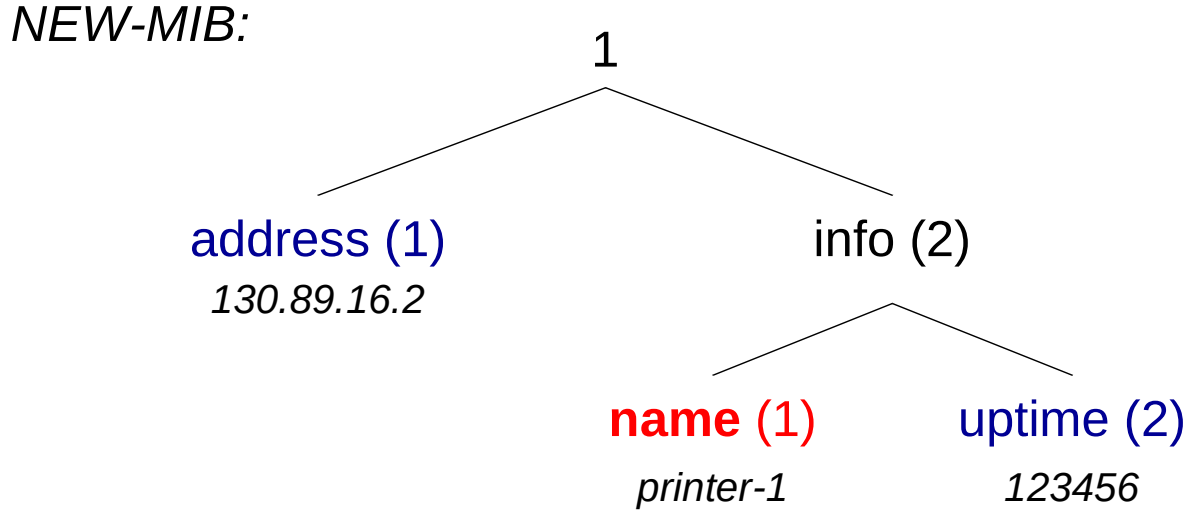
	SMIv1	SMIv2
SIMPLE TYPES:	INTEGER	INTEGER
	OCTET STRING	OCTET STRING
	OBJECT IDENTIFIER	OBJECT IDENTIFIER
	-	Integer32
APPLICATION-WIDE TYPES:	-	Unsigned32
	Gauge	Gauge32
	Counter	Counter32
	-	Counter64
	TimeTicks	TimeTicks
	IpAddress	IpAddress
	Opaque	Opaque
	NetworkAddress	-
PSEUDO TYPES:	-	BITS

EXAMPLE OF SCALAR OBJECTS



OBJECT NAMING

INTRODUCE NAMING TREE



THE LEAVES OF THE TREE REPRESENT THE MANAGED OBJECTS

NODES ARE INTRODUCED FOR NAMING PURPOSES

OBJECT NAMING

• address
Object ID = 1.1
Object Instance = 1.1.0
Value of Instance = *130.89.16.2*

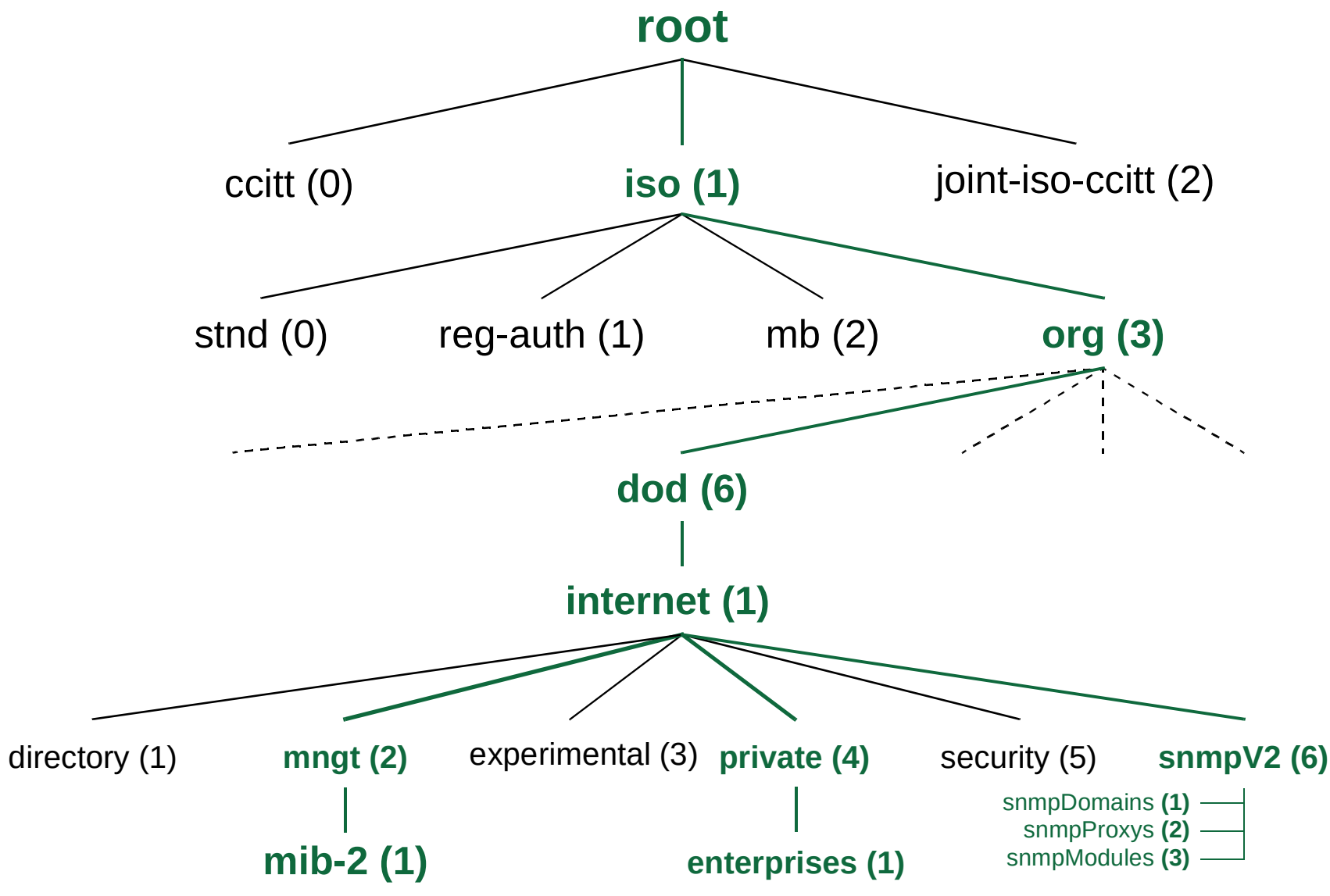
• info
Object ID = 1.2

• name
Object ID = 1.2.1
Object Instance = 1.2.1.0
Value of Instance = *printer-1*

• uptime
Object ID = 1.2.2
Object Instance = 1.2.2.0
Value of Instance = *123456*

ALTERNATIVE:
Object ID = NEW-MIB info uptime

OBJECT NAMING: MIBs



OBJECT TYPE DEFINITION

OBJECT-TYPE:

SYNTAX
- INTEGER
- OCTET STRING
- OBJECT IDENTIFIER
- BITS
- IpAddress
- Integer32
- Counter32
- Counter64
- Gauge32
- TimeTicks
- Opaque
- New Type

MAX-ACCESS
- read-only
- read-write
- read-create
- accessible-for-notify
- not-accessible

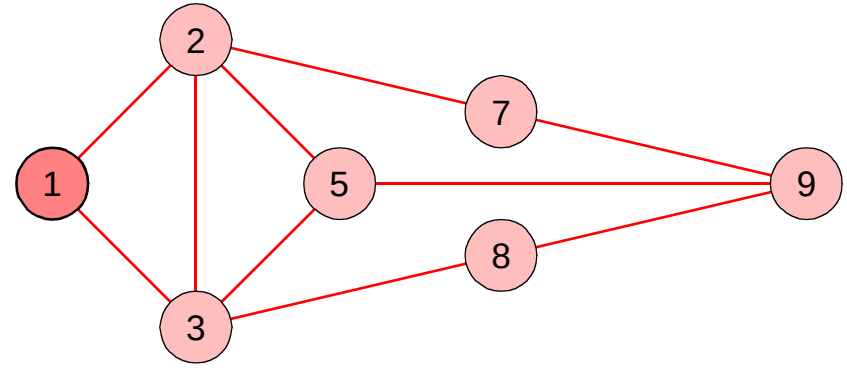
STATUS
- current
- deprecated
- obsolete

DESCRIPTION ""

TABLES

EXAMPLE: ROUTING TABLE

destination	next
2	2
3	3
5	2
7	2
8	3
9	3



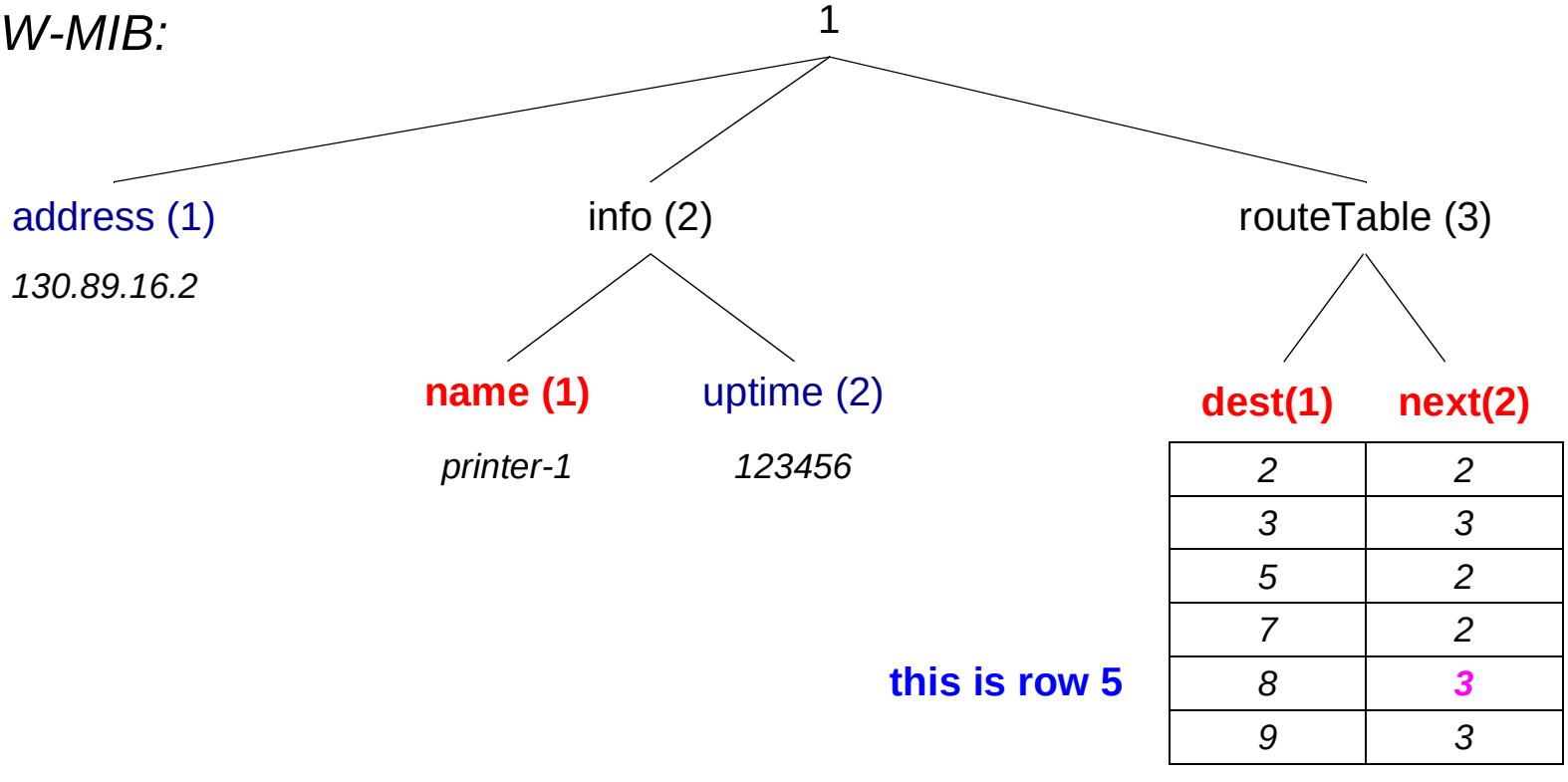
TO RETRIEVE INDIVIDUAL TABLE ENTRIES

EACH ENTRY SHOULD GET A NAME

NAMING OF TABLE ENTRIES - I

POSSIBILITY 1 (NOT BEING USED BY SNMP): USE ROW NUMBERS

NEW-MIB:

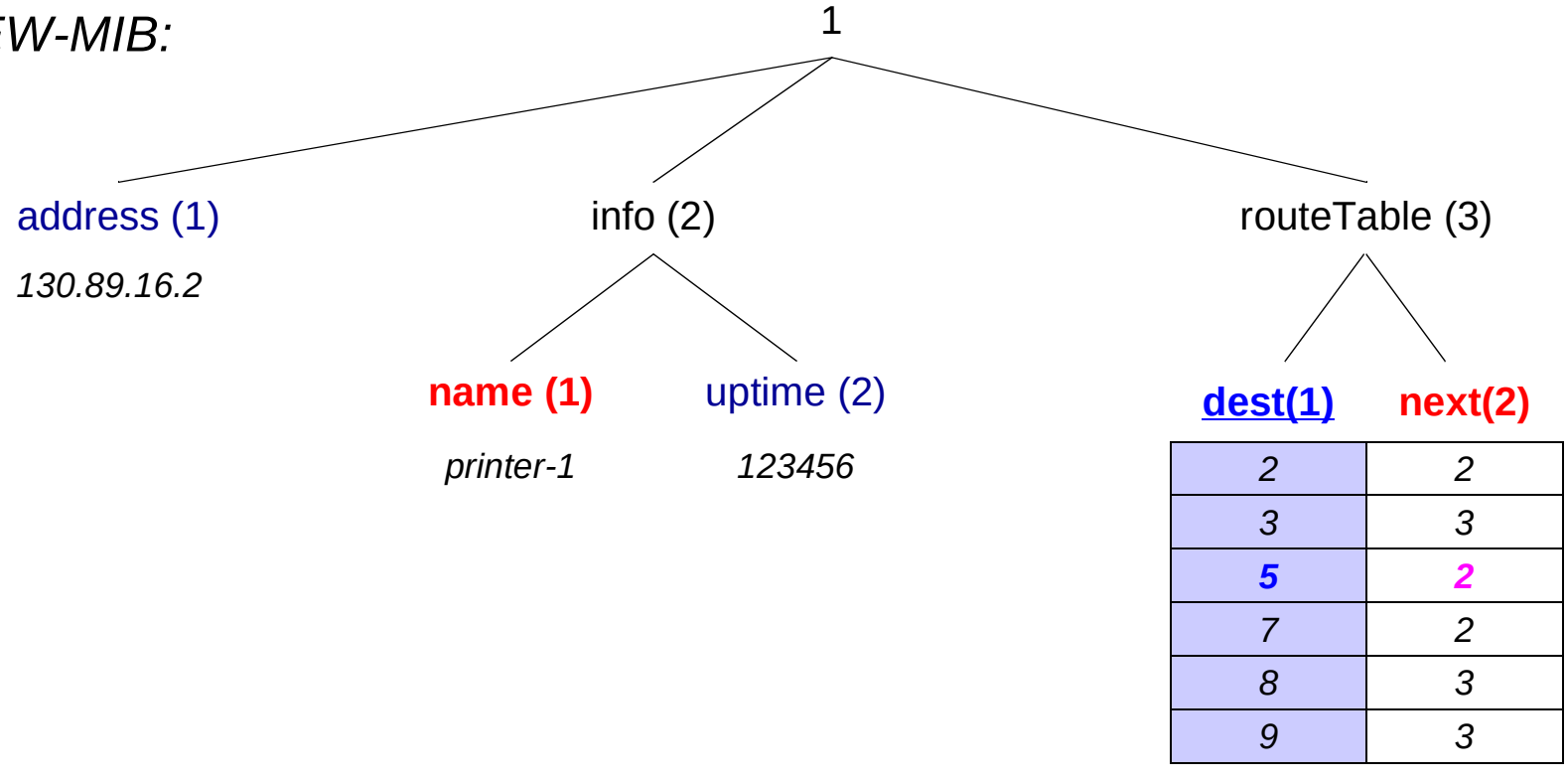


EXAMPLE: THE VALUE OF *NEW-MIB routeTable next 5* IS *3*

NAMING OF TABLE ENTRIES - II

POSSIBILITY 2 (USED BY SNMP): INTRODUCE AN INDEX COLUMN

NEW-MIB:



EXAMPLE: THE VALUE OF *NEW-MIB routeTable next 5* IS *2*

TABLE INDEXING

GENERAL SCHEME

X.C.I

OID of Table Column number Index value

EXAMPLES:

OID of Table = 1.3

1.3.1.5 => *5*
1.3.2.5 => *2*
1.3.1.9 => *9*
1.3.2.9 => *3*
1.3.2.7 => *2*
1.3.1.1 => *entry does not exist*
1.3.2.1 => *entry does not exist*

TABLE INDEXING - NON-INTEGER INDEX

AN INDEX NEED NOT BE AN INTEGER

routeTable (3)

dest (1)	next (2)
130.89.16.1	*130.89.16.1*
130.89.16.4	*130.89.16.4*
130.89.16.23	*130.89.16.1*
130.89.19.121	*130.89.16.1*
192.1.23.24	*130.89.16.4*
193.22.11.97	*130.89.16.4*

EXAMPLES:

OID of Table = 1.3

1.3.1.130.89.16.23 => *130.89.16.23*

1.3.2.130.89.16.23 => *130.89.16.1*

1.3.1.193.22.11.97 => *193.22.11.97*

1.3.2.193.22.11.97 => *130.89.16.4*

1.3.2.130.89.19.121 => *130.89.16.1*

TABLE INDEXING - MULTIPLE INDEX FIELDS

USE OF MULTIPLE INDEX FIELDS

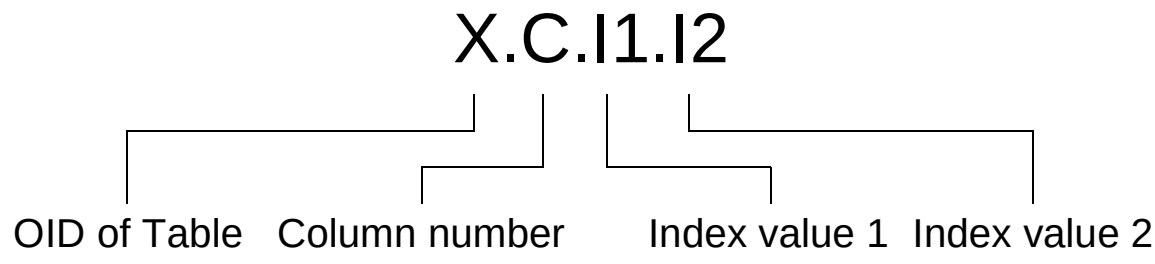


TABLE INDEXING - MULTIPLE INDEX FIELDS: EXAMPLE

EXAMPLE:

1 = low costs
2 = high reliability

routeTable (3)

dest (1)	**policy (2)**	**next (3)**
130.89.16.23	*1*	*130.89.16.23*
130.89.16.23	*2*	*130.89.16.23*
130.89.19.121	*1*	*130.89.16.1*
192.1.23.24	*1*	*130.89.16.1*
192.1.23.24	*2*	*130.89.16.4*
193.22.11.97	*1*	*130.89.16.1*

1.3.3.192.1.23.24.1 => *130.89.16.1*

1.3.3.192.1.23.24.2 => *130.89.16.4*

DEFINITION OF NEW TYPES

TEXTUAL CONVENTIONS

TO REFINE SEMANTICS OF EXISTING TYPES

EXAMPLE:

```
RunState ::= TEXTUAL CONVENTION
   STATUS current
   DESCRIPTION "..."
   SYNTAX INTEGER{
      running(1)
      runable(2)
      waiting(3)
      exiting(4)}
```

TEXTUAL CONVENTIONS

- PhysAddress
- MacAddress
- TruthValue
- AutonomousType
- InstancePointer
- VariablePointer
- RowPointer
- RowStatus
- TimeStamp
- TimeInterval
- DateAndTime
- StorageType
- TDomain
- TAddress

- Inet-Address...

NOTIFICATION TYPES

SMIv2:

- MIBs MAY NOW INCLUDE NOTIFICATION TYPE MACROS

EXAMPLE:

```
linkUp NOTIFICATION-TYPE
   OBJECTS   {ifIndex}
   STATUS    current
   DESCRIPTION
      "A linkUp trap signifies that the
      entity has detected that the
      ifOperStatus object has changed to Up"
::= {snmpTraps 4}
```

SMIng

PROBLEMS WITH SMIvx

- SMIv2 RELIED ON 1988 VERSION OF ASN.1
- TOOLS FOR SMIv2 RELATIVELY COMPLEX
- CERTAIN DATA TYPES WERE MISSING IN SMIv2
  64 bit integers, …
- LIMITED FACILITIES TO REUSE DEFINITIONS
- SMIv2 DID NOT ALLOW FOR EXTENSIONS
- NEW, POSSIBLY INCOMPATIBLE VARIANTS APPEARED
  SPPI, ...

SMIng

TO RESOLVE THESE PROBLEMS
A NEW SMI IS BEING DEFINED

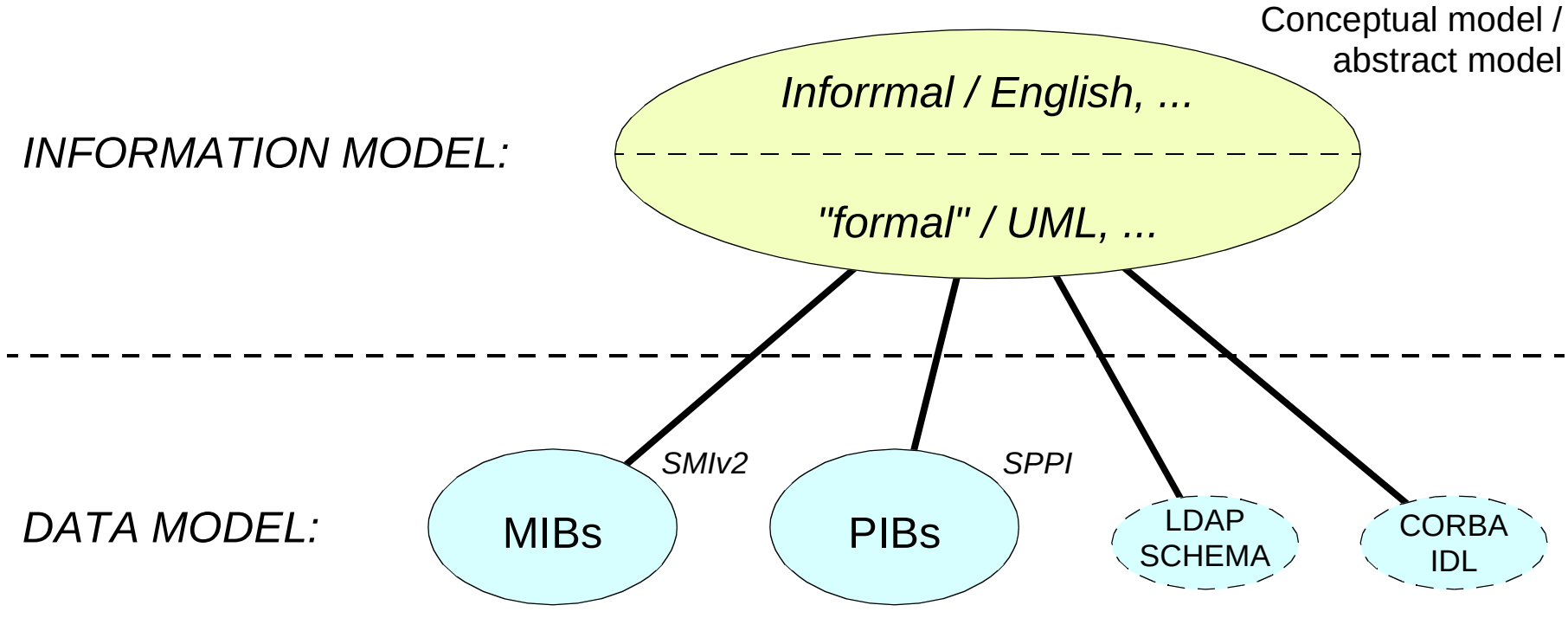
SMI next generation (ng)

STARTED AS IRTF NMRG ACTIVITY

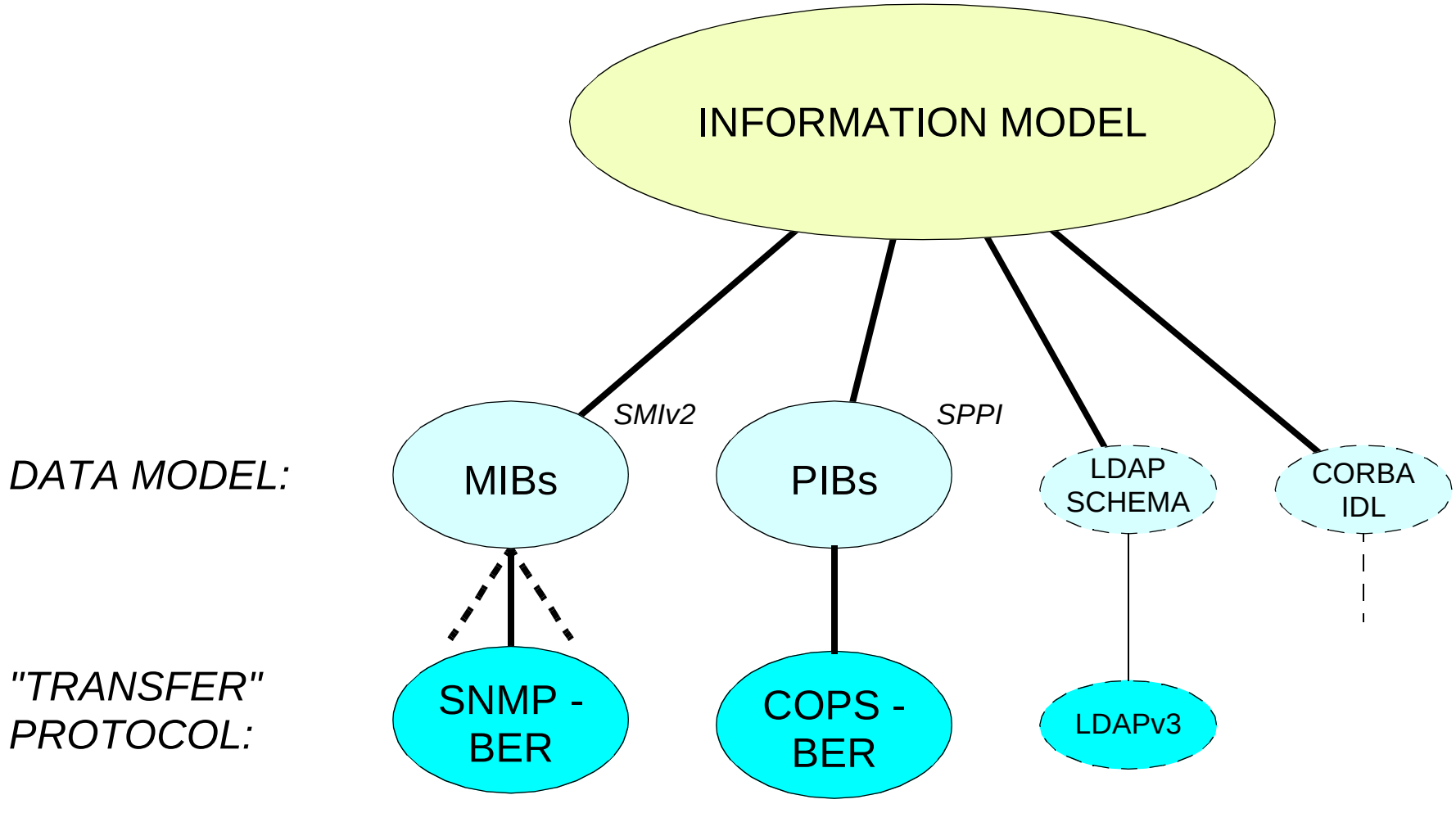
IS NOW IETF WG

THE CHALLANGE:
CREATE A COMMON DATA DEFINITION LANGUAGE,
INDEPENDENT OF SPECIFIC PROTOCOLS

DATA VERSUS INFORMATION MODEL

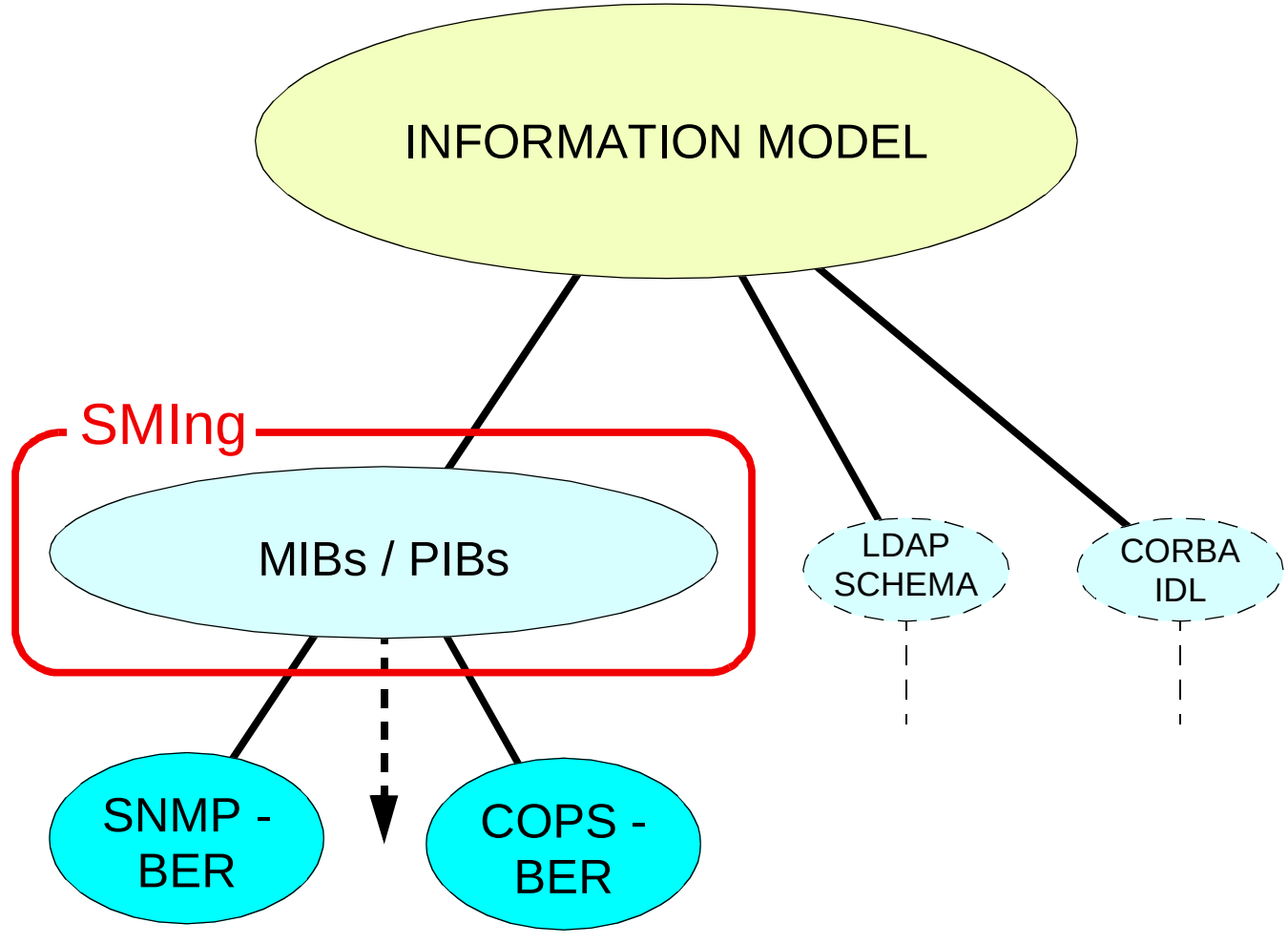


DATA MODEL & "TRANSFER" PROTOCOL



ROLE OF SMIng

DATA MODEL:



MIBs

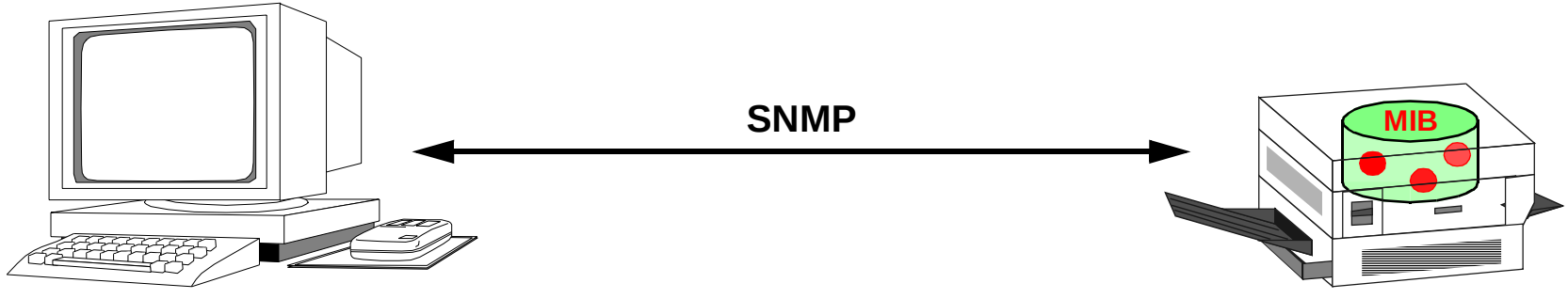
MANAGEMENT INFORMATION BASES

CONTAIN THE MANAGED OBJECTS (VARIABLES)

THAT REPRESENT THE RESOURCES OF A SYSTEM

AND WHICH MAY BE MONITORED AND MODIFIED BY A (REMOTE) MANAGER

TO CONTROL THE BEHAVIOUR OF THAT SYSTEM



MIB DEFINITION AND MIB INSTANCE

MIB DEFINITIONS SHOULD BE KNOWN BY:

- THE IMPLEMENTORS OF THE MANAGED SYSTEM
- THE MANAGER

THE MIB IS INSTANTIATED WITHIN THE MANAGED SYSTEM

MODULARITY

THE MANAGED OBJECTS OF A SYSTEM
ARE USUALLY DEFINED IN MULTIPLE MIB DEFINITIONS

MODULES

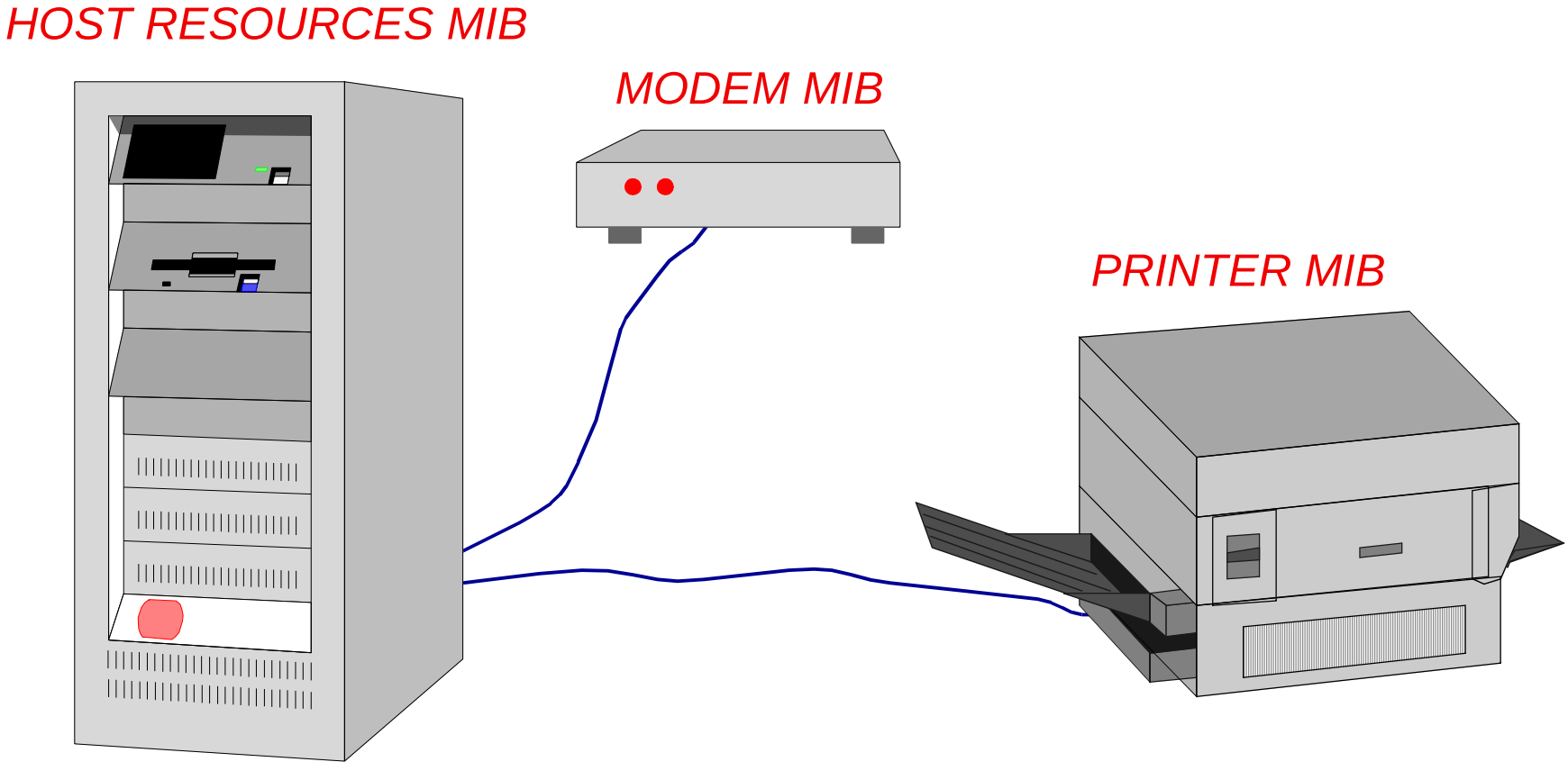
- DIFFERENT MODULES CAN BE DEFINED BY DIFFERENT TEAMS

- MANAGEMENT FUNCTIONALITY CAN GRADUALLY BE EXTENDED

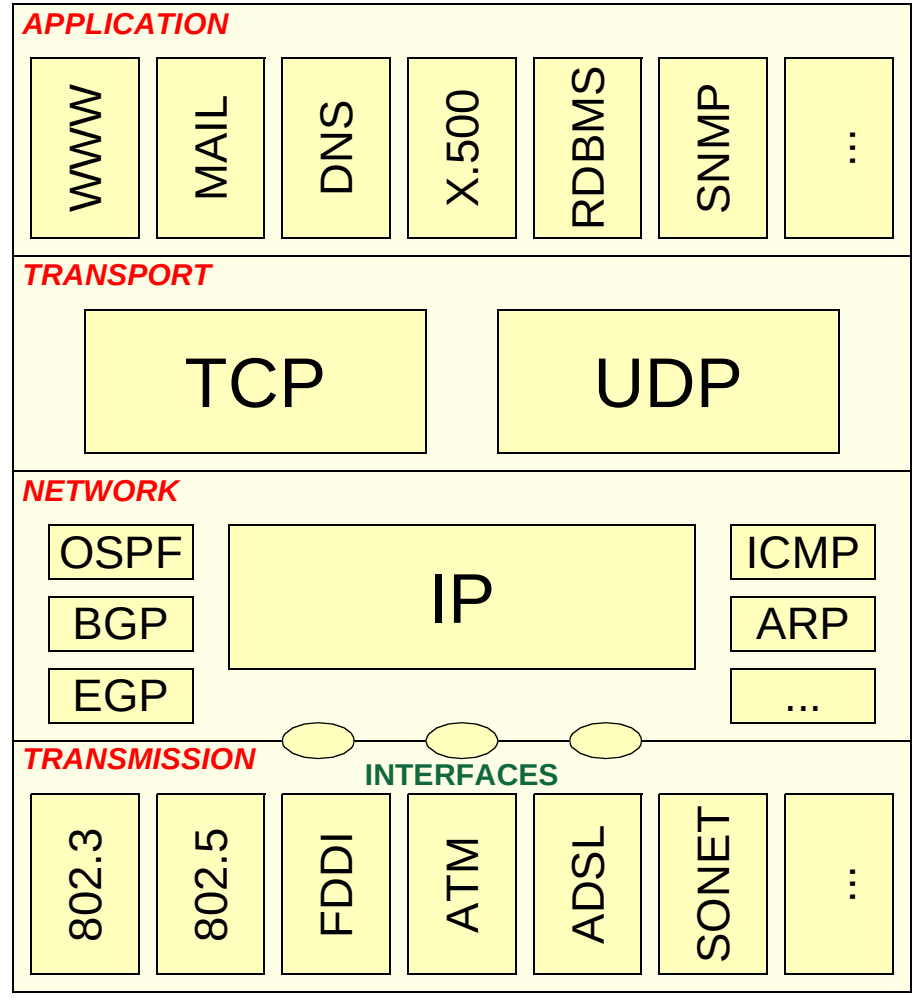
- DIFFERENT TYPES OF SYSTEMS
CAN SUPPORT DIFFERENT MIB MODULES

- VENDORS CAN EXTEND THE MANAGEMENT FUNCTIONALITY
VIA PROPRIETARY MIBS

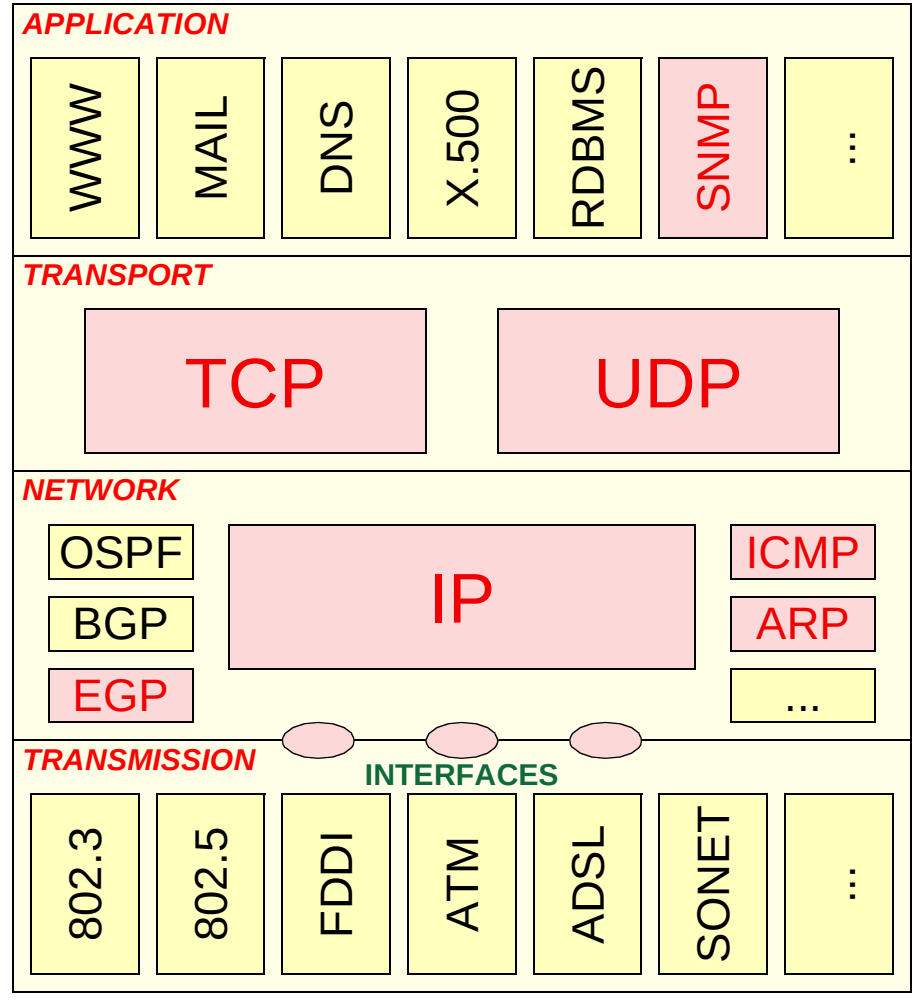
HARDWARE MIBS



PROTOCOL MIBS



PROTOCOL MIBS - EXAMPLE: MIB-II



HARDWARE SPECIFIC MIBs

Title	RFC	STATUS
Host Resources MIB	2790	D
Entity MIB	2737	P
Job Monitoring MIB	2707	I
Printer	1759	P
Modem	1696	P
Parallel printer-like Hardware	1660	D
RS-232-like Hardware	1659	D
Character Stream Devices	1658	D
UPS	1628	P

TRANSMISSION MIBs

Title	RFC	STATUS
UNI/NNI Multilink Frame Relay function	3020	P
Frame Relay/ATM PVC Service Interworking Function	2955	P
Frame Relay Service	2954	P
Inverted Stack Table Extension to the Interfaces Group	2864	P
Interfaces Group	2863	D
Fabric Element in Fibre Channel Standard	2837	P
NBMA Next Hop Resolution Protocol (NHRP)	2677	P
Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions	2674	P
Radio Frequency MIB for MCNS/DOCSIS compliant RF interfaces	2670	P
Cable Device MIB for DOCSIS compliant Cable Modems and Cable Modem Termination Systems	2669	P
IEEE 802.3 Medium Attachment Units (MAUs)	2668	P
Object Identifiers for Identifying Ethernet Chip Sets	2666	I

Title	RFC	STATUS
Ethernet-like Interface Types	2665	P
ADSL Lines	2662	P
SONET/SDH Interface Type	2558	P
ATM Management	2515	P
Textual Conventions and OBJECT-IDENTITIES for ATM Management	2514	P
DS3/E3 Interface Type	2496	P
DS1, E1, DS2 and E2 Interface Types	2495	P
DS0 and DS0 Bundle Interface Type	2494	P
Classical IP and ARP Over ATM (IPOA)	2320	P
IEEE 802.12 Repeater Devices	2266	P
Dial Control	2128	P
ISDN	2127	P
Frame Relay DTEs	2115	D
IEEE 802.3 Repeater Devices	2108	P
Data Link Switching	2024	P
IEEE 802.12 Interfaces	2020	P
IEEE 802.5 Station Source Routing	1749	P

Title	RFC	STATUS
IEEE 802.5	1748	D
SMDS	1694	D
Source Routing Bridges	1525	P
FDDI	1512	P
Bridges	1493	D
Bridge Network Control Protocol of PPP	1474	P
IP Network Control Protocol of PPP	1473	P
Security Protocols of PPP	1472	P
Link Control Protocol of PPP	1471	P
Multiprotocol Interconnect over X.25	1461	P
X.25 Packet Layer	1382	P
X.25 LAPB	1381	P

NETWORK LAYER MIBs

Title	RFC	STATUS
IPv6 MIB for The Multicast Listener Discovery Protocol	3019	P
Protocol Independent Multicast MIB for IPv4	2934	E
Internet Group Management Protocol MIB	2933	P
IPv4 Multicast Routing MIB	2932	P
Textual Conventions for Internet Network Addresses	2851	P
Definitions of MO for the Virtual Router Redundancy Protocol	2787	P
IP Tunnel MIB	2667	P
MIB for IPv6: ICMPv6 Group	2466	P
MIB for IPv6: Textual Conventions and General Group	2465	P
Definitions of MO for Multicast over UNI 3.0/3.1 based ATM Networks	2417	P
Integrated Services - Guaranteed Service Ext.	2214	P
Integrated Services	2213	P
RSVP	2206	P
IP Forwarding Table	2096	P

Title	RFC	STATUS
IP MIB	2011	P
IP Mobility Support	2006	P
OSPF Version 2	1850	D
RIP Version 2 MIB Extension	1724	D
BGP Version 4	1657	D
Identification MIB	1414	P
BGP Version 3	1269	P
MIB-II	1213	S

TRANSPORT LAYER MIBs

Title	RFC	STATUS
Real-Time Transport Protocol	2959	P
IP Version 6 MIB for the User Datagram Protocol	2454	P
IP Version 6 MIB for the Transmission Control Protocol	2452	P
User Datagram Protocol (UDP)	2013	P
Transmission Control Protocol (TCP)	2012	P

APPLICATION LAYER MIBs

Title	RFC	STATUS
MIB for the PINT Services Architecture	3055	P
Mail Monitoring MIB	2789	P
Network Services Monitoring	2788	P
RADIUS Accounting Server MIB	2621	I
RADIUS Accounting Client MIB	2620	I
RADIUS Authentication Server MIB	2619	P
RADIUS Authentication Client MIB	2618	P
Directory Server Monitoring MIB	2605	P
Definitions of Managed Objects for WWW Services	2594	P
Application Management MIB	2564	P
Definitions of System-Level Managed Objects for Applications	2287	P
SNMPv2 MIB	1907	P
RDBMS MIB	1697	P
DNS Resolver MIB Extensions	1612	P
DNS Server MIB Extensions	1611	P

REMOTE MONITORING AND MEASUREMENT

Title	RFC	STATUS
Remote Network Monitoring (RMON) MIB	2819	S
Traffic Flow Measurement: Meter MIB	2720	P
RMON MIB Extensions for Switched Networks Version 1.0	2613	P
RMON Version 2	2021	P
Token Ring extensions to RMON	1513	P

DISTRIBUTED MANAGEMENT

Title	RFC	STATUS
Notification Log MIB	3014	P
Expression MIB	2982	P
Event MIB	2981	P
Remote Ping, Traceroute, and Lookup Operations	2925	P
Delegation of Management Scripts	2592	P
Scheduling Management Operations	2591	P

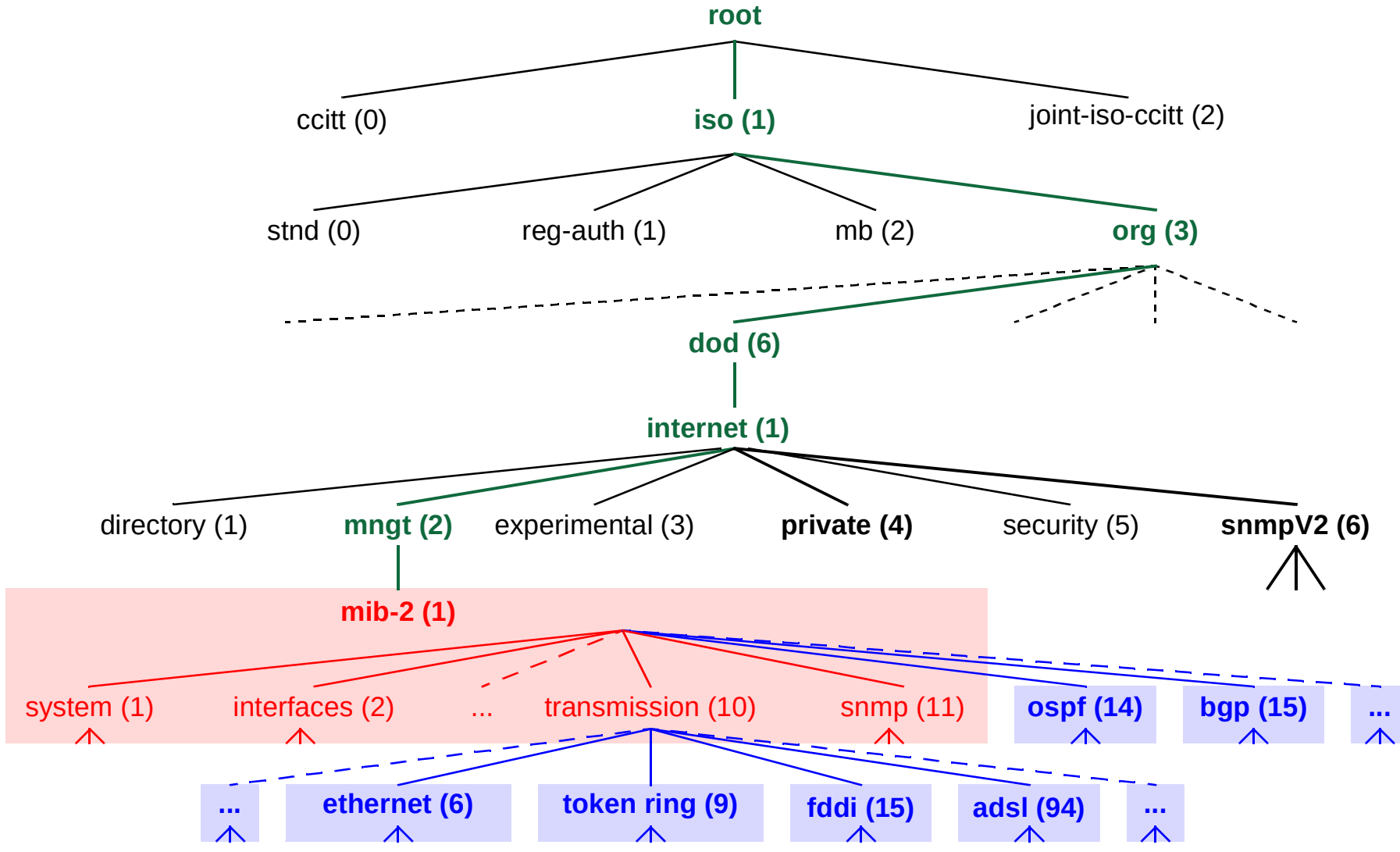
VENDOR SPECIFIC MIBs

Title	RFC	STATUS
APPN/HPR in IP Networks	2584	P
TN3270E Response Time Collection	2562	P
TN3270E	2561	P
Extended Border Node	2457	P
APPN TRAPS	2456	P
APPN	2455	P
HPN	2238	P
DLUR	2232	P
APPC	2051	P
TCP/IPX Connection	1792	E
SNA Data Link Control (SDLC)	1747	P
Appletalk	1742	P
SNA NAUs	1666	P
DECNET Phase IV	1559	D

MISCELLANY

Title	RFC	STATUS
Common Open Policy Service (COPS) Protocol Clients	2940	P
Physical Topology	2922	I
Service Level Agreements Performance Monitoring	2758	E
Definitions of Managed Objects for Extensible SNMP Agents	2742	P
Collection and Storage of Accounting Information for CO Networks	2513	P
Accounting Information for ATM Networks	2512	P
Textual Conventions for MIB Modules Using Performance History Based on 15 Minute Intervals	2493	P
Techniques for managing asynchronously generated alerts	1224	E

NAMING OF MIBs



MIB-II

DEFINES THE VARIABLES TO MANAGE THE TCP/IP PROTOCOL STACK

170 VARIABLES

RFC 1213
SMIv1

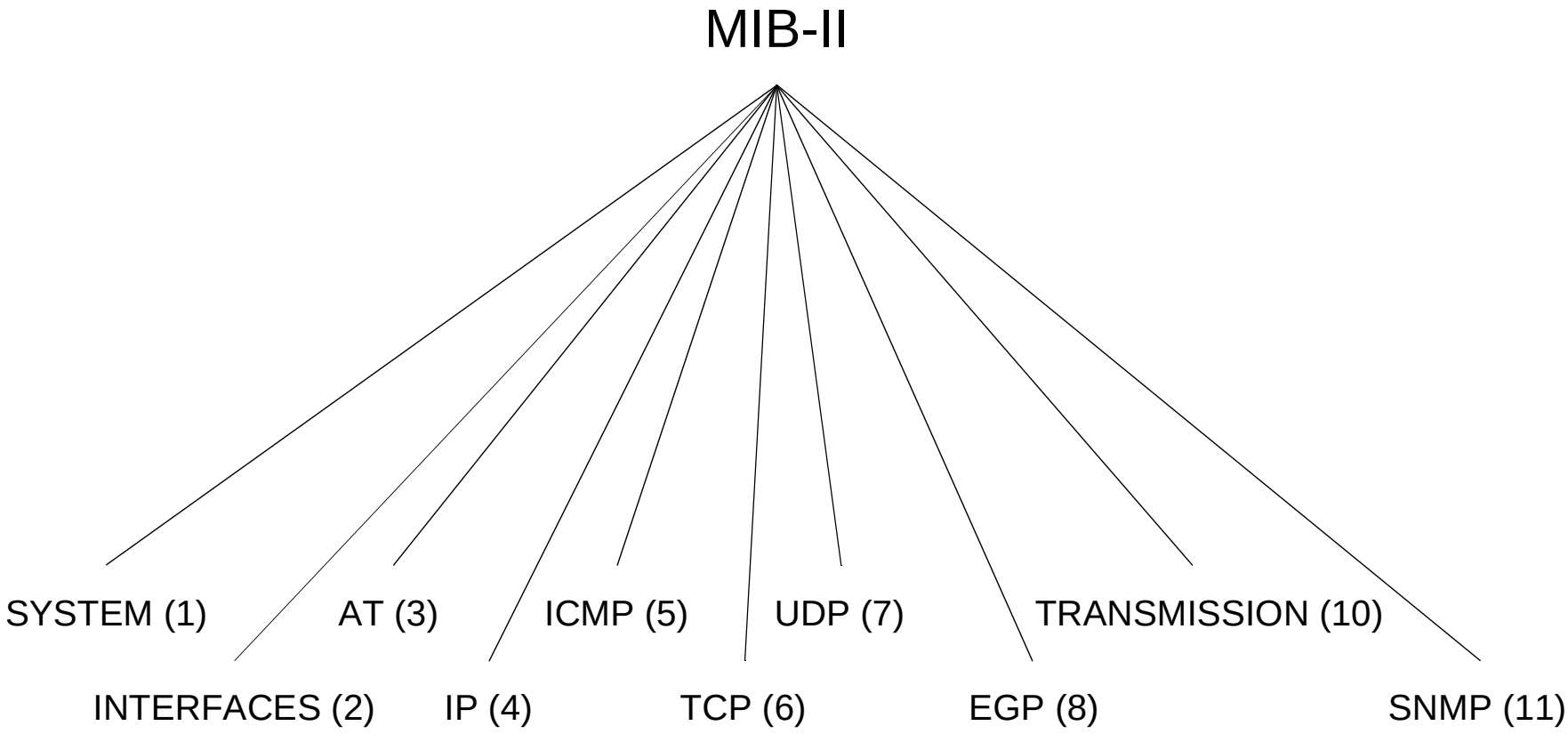
ENHANCEMENT OF MIB-I

RFC 1156

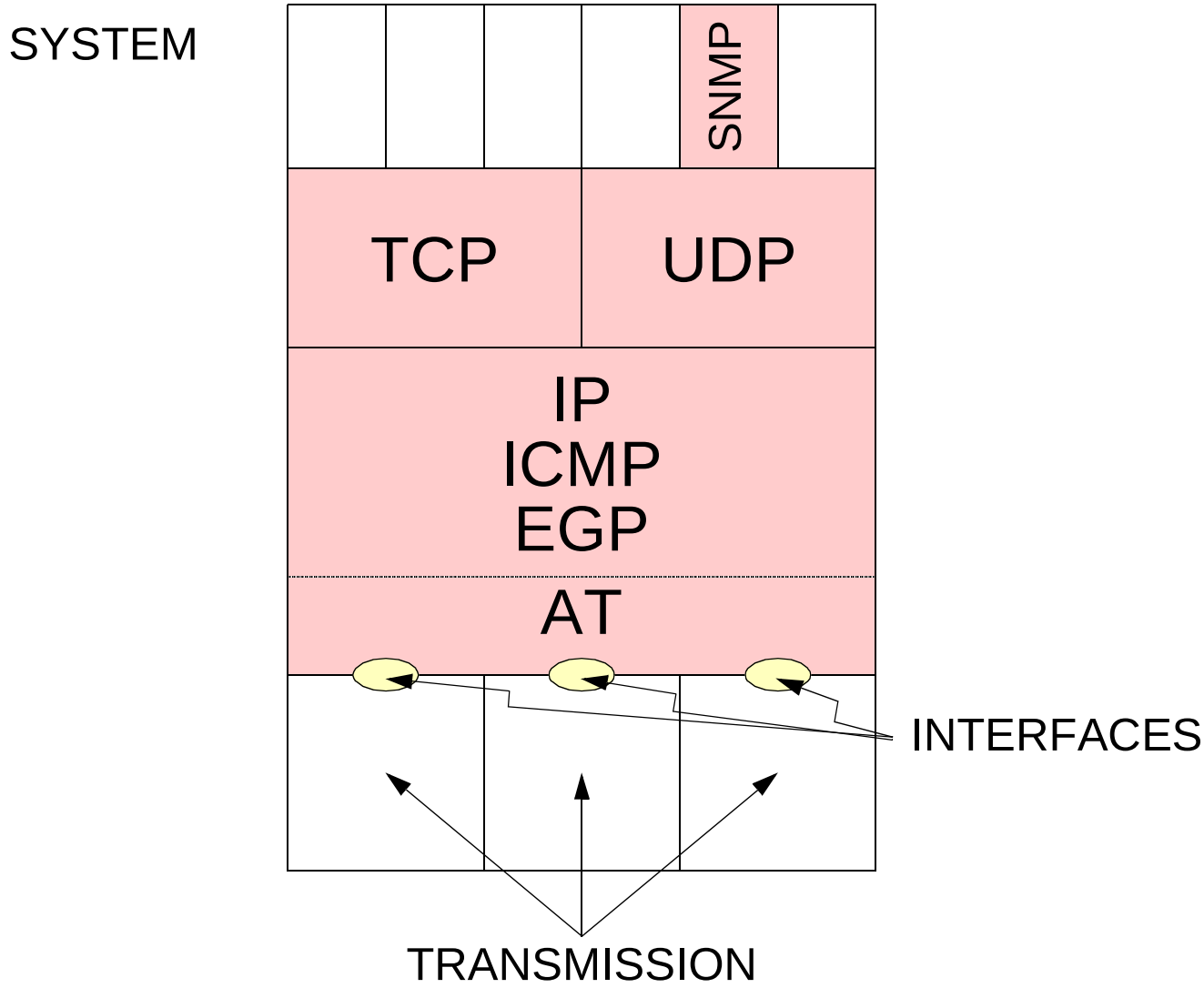
DESIGN CRITERIA

- ESSENTIAL FOR FAULT OR CONFIGURATION MANAGEMENT
- ONLY WEAK CONTROL OBJECTS
- SMALL NUMBER OF OBJECTS
- AVOID REDUNDANCY
- EVIDENCE OF UTILITY
- DO NOT DISTURB NORMAL OPERATION
- NO IMPLEMENTATION SPECIFIC ISSUES

STRUCTURE


MIB-II
SYSTEM (1)
INTERFACES (2)
AT (3)
IP (4)
ICMP (5)
TCP (6)
UDP (7)
EGP (8)
TRANSMISSION (10)
SNMP (11)

MIB-II GROUPS IN A PROTOCOL STACK



NEW VERSIONS

SYSTEM GROUP ⇨ SNMPv2 MIB (RFC 1907)

INTERFACES (IF) GROUP ⇨ IF-MIB (RFC 2863)

ADDRESS TRANSLATION (AT) GROUP ⇨ DEPRECATED

IP & ICMP GROUPS ⇨ IP-MIB (RFC 2011)

TCP GROUP ⇨ TCP-MIB (RFC 2012)

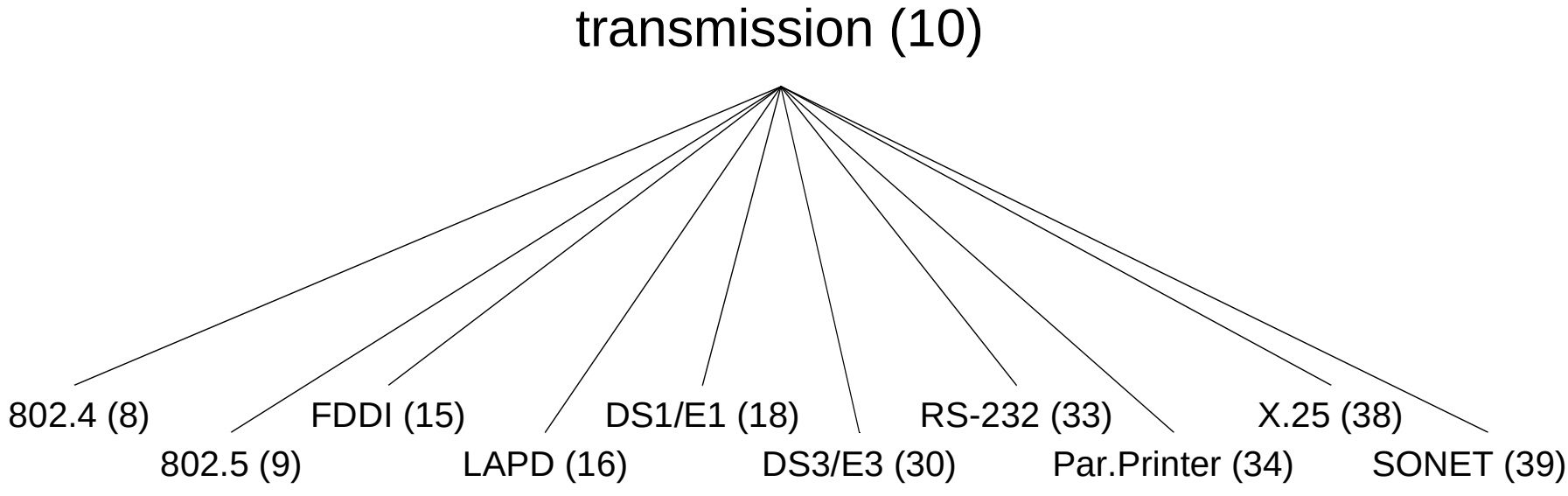
UDP GROUP ⇨ UDP-MIB (RFC 2013)

EGP GROUP ⇨ OUTDATED (BGP)

TRANSMISSION GROUP ⇨ IS PLACEHOLDER

SNMP GROUP ⇨ SNMPv2 MIB (RFC 1907)

TRANSMISSION GROUP

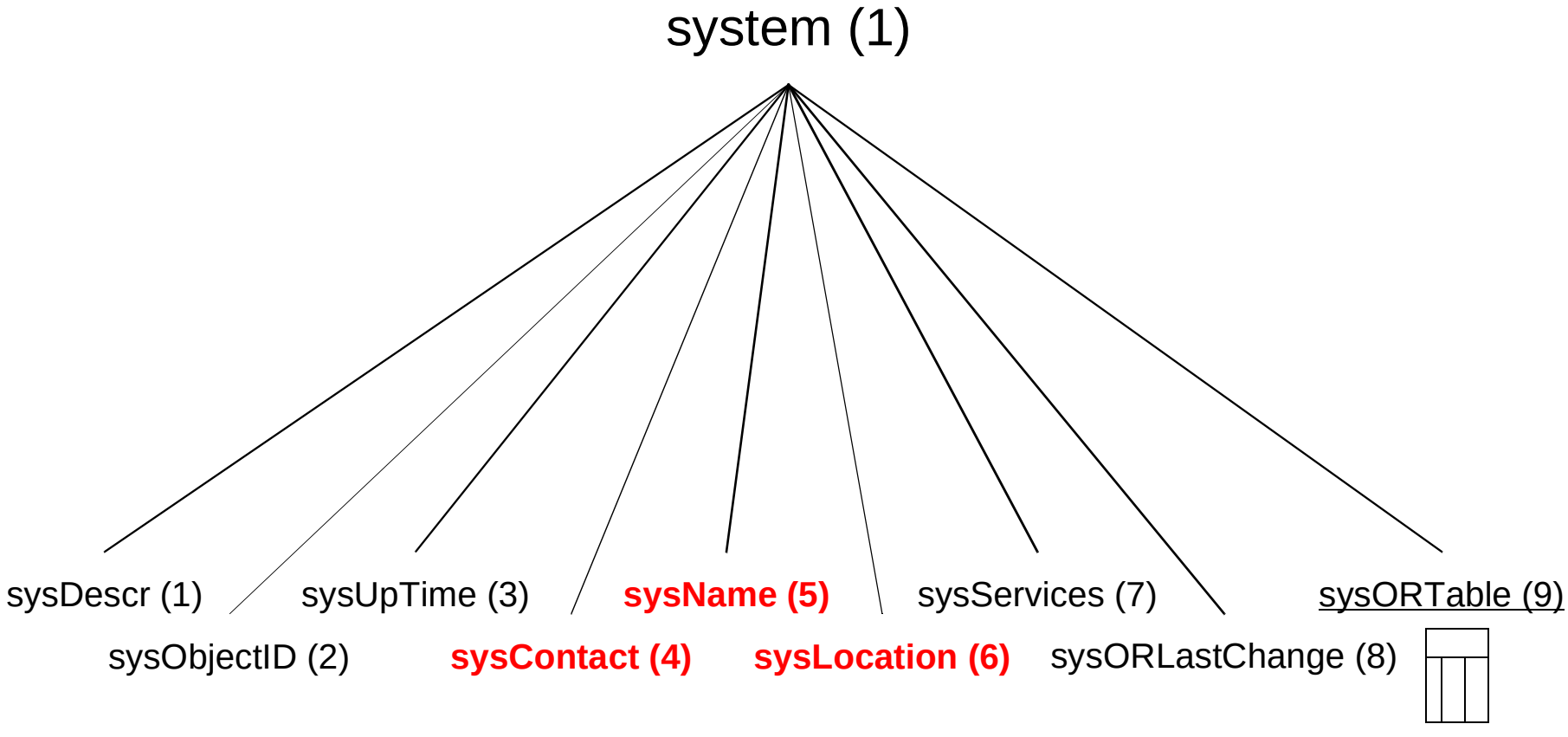


SNMPv2 MIB

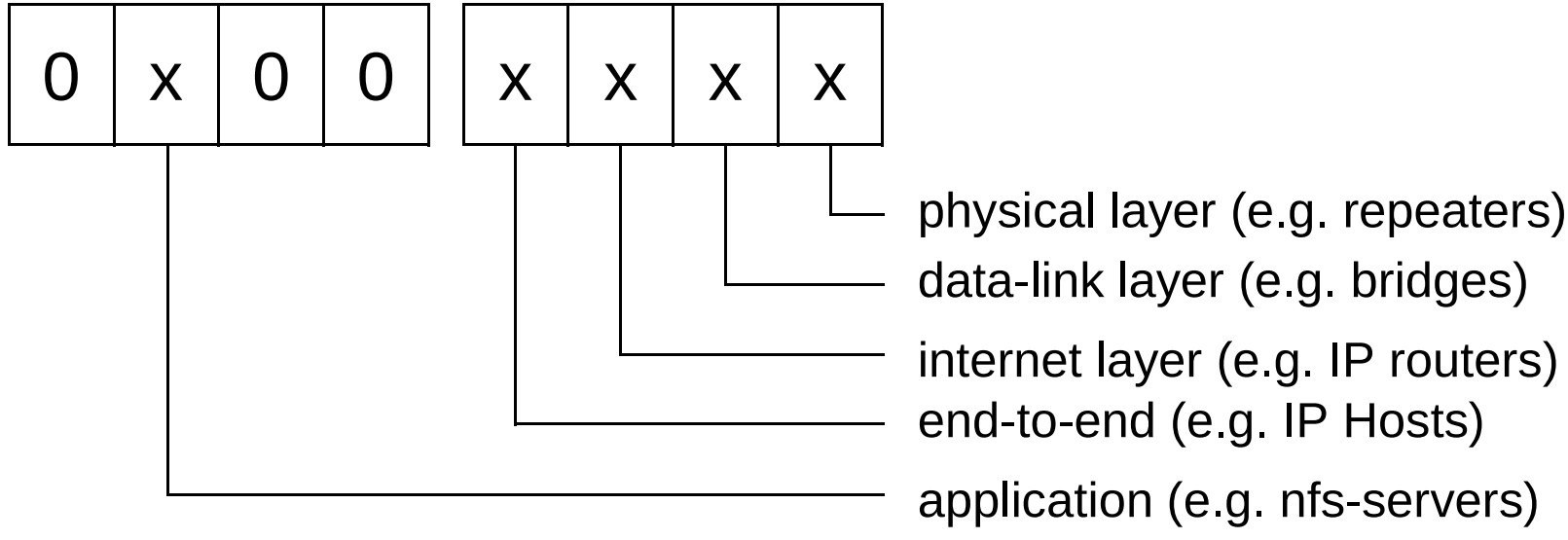
RFC 1907
PROPOSED STANDARD

- SYSTEM GROUP
- SNMP GROUP
- SNMP MIBObjects GROUP
  snmpTrap
  snmpTraps
  snmpSet (snmpSetSerialNo)

SYSTEM GROUP



sysServices



EXAMPLE

sysDescr:	"**Cisco Gateway**"
sysObjectID:	**1.3.6.1.4.1.9.1.1**
sysUpTime:	**37153422** *(4 days, 7 h, 12 min, 14.22 s)*
sysContact:	"**helpdesk@cs.utwente.nl**"
sysName:	"**utic01.cs.utwente.nl**"
sysLocation:	"**near logica meeting room**"
sysServices:	**6** *(bridge and router functions)*

sysORTable - EXAMPLE

sysORIndex	sysORID	sysORDescr	sysORUpTime
1	IF-MIB!ifMIB	The MIB module to describe generic objects for network interface sub-layers	82
2	SNMPv2-MIB!snmpMIB	The MIB module for SNMPv2 entities	82
3	TCP-MIB!tcpMIB	The MIB module for managing TCP implementations	82
4	IP-MIB!ip	The MIB module for managing IP and ICMP implementations	85
5	UDP-MIB!udpMIB	The MIB module for managing UDP implementations	85

IF MIB

RFC 2863

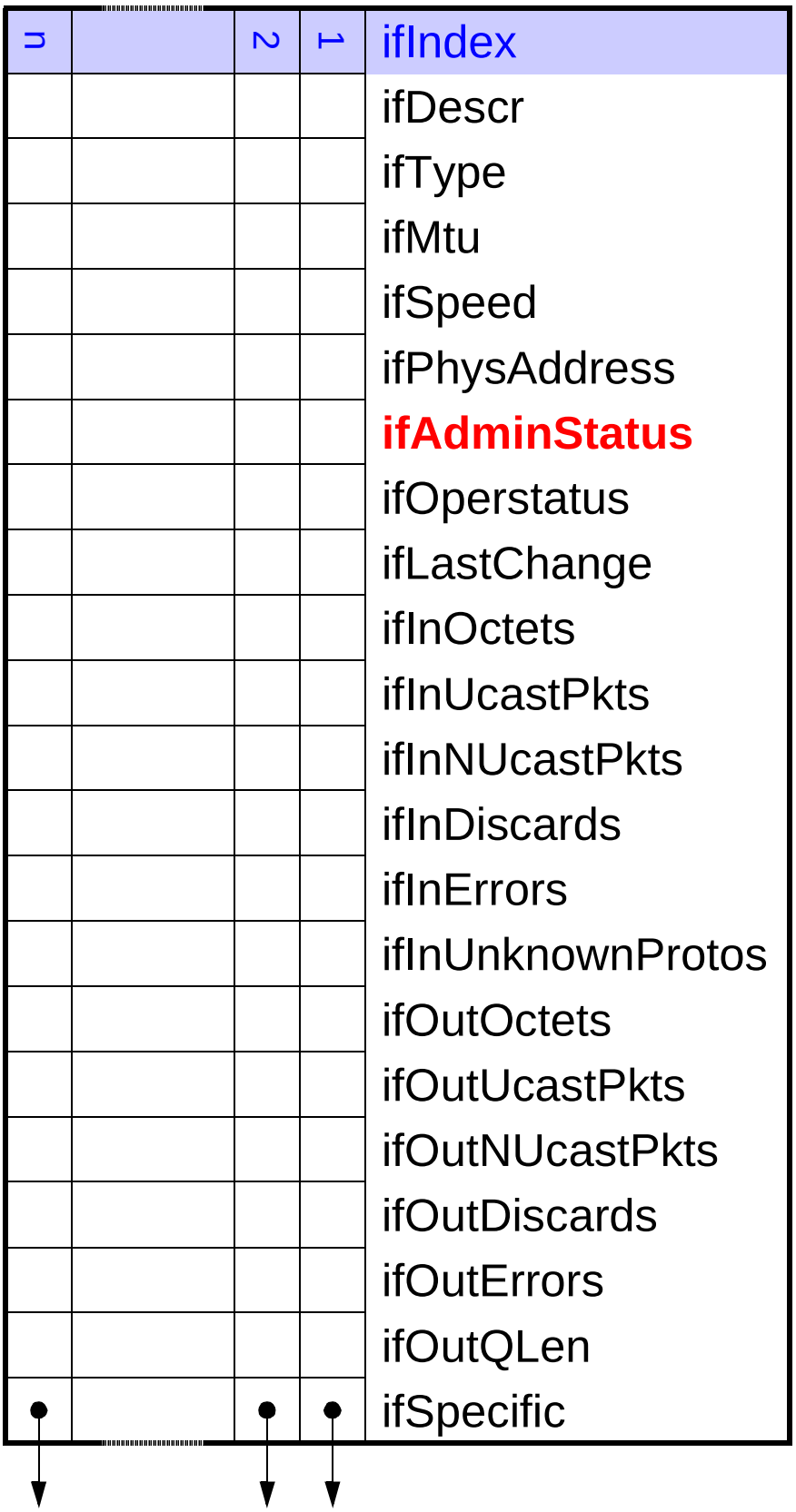
DRAFT STANDARD

REPLACES IF GROUP OF MIB-II

- RFC 1213
- RFC1229 (EXTENSIONS TO THE IF GROUP)

DEFINES THE FOLLOWING MAIN TABLES:

- ifStackTable
- ifTable
- ifXTable


n
2
1
ifIndex
ifDescr
ifType
ifMtu
ifSpeed
ifPhysAddress
ifAdminStatus
ifOperstatus
ifLastChange
ifInOctets
ifInUcastPkts
ifInNUcastPkts
ifInDiscards
ifInErrors
ifInUnknownProtos
ifOutOctets
ifOutUcastPkts
ifOutNUcastPkts
ifOutDiscards
ifOutErrors
ifOutQLen
ifSpecific

ifTable

ifType and ifStatus

- ifType

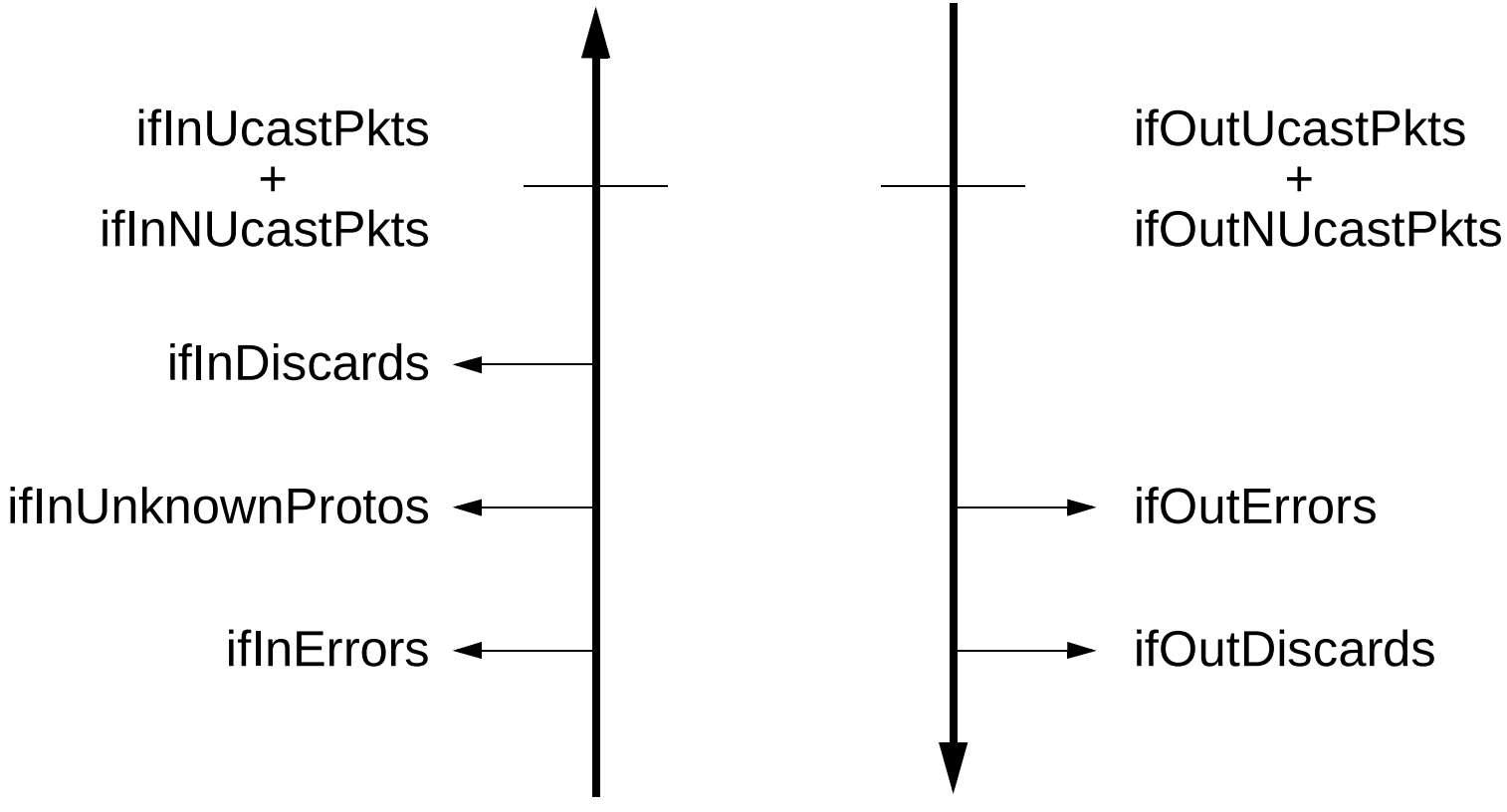
EXAMPLES:

1	Undefined	16	LAPB
6	Ethernet	20	ISDN Basic
7	IEEE 802.3	21	ISDN Primary
8	IEEE 802.4	23	PPP
9	IEEE 802.5	24	Loopback
10	IEEE 802.6	28	SLIP
15	FDDI	32	Frame Relay

- ifAdminStatus / ifOperStatus

1 = up
2 = down
3 = testing

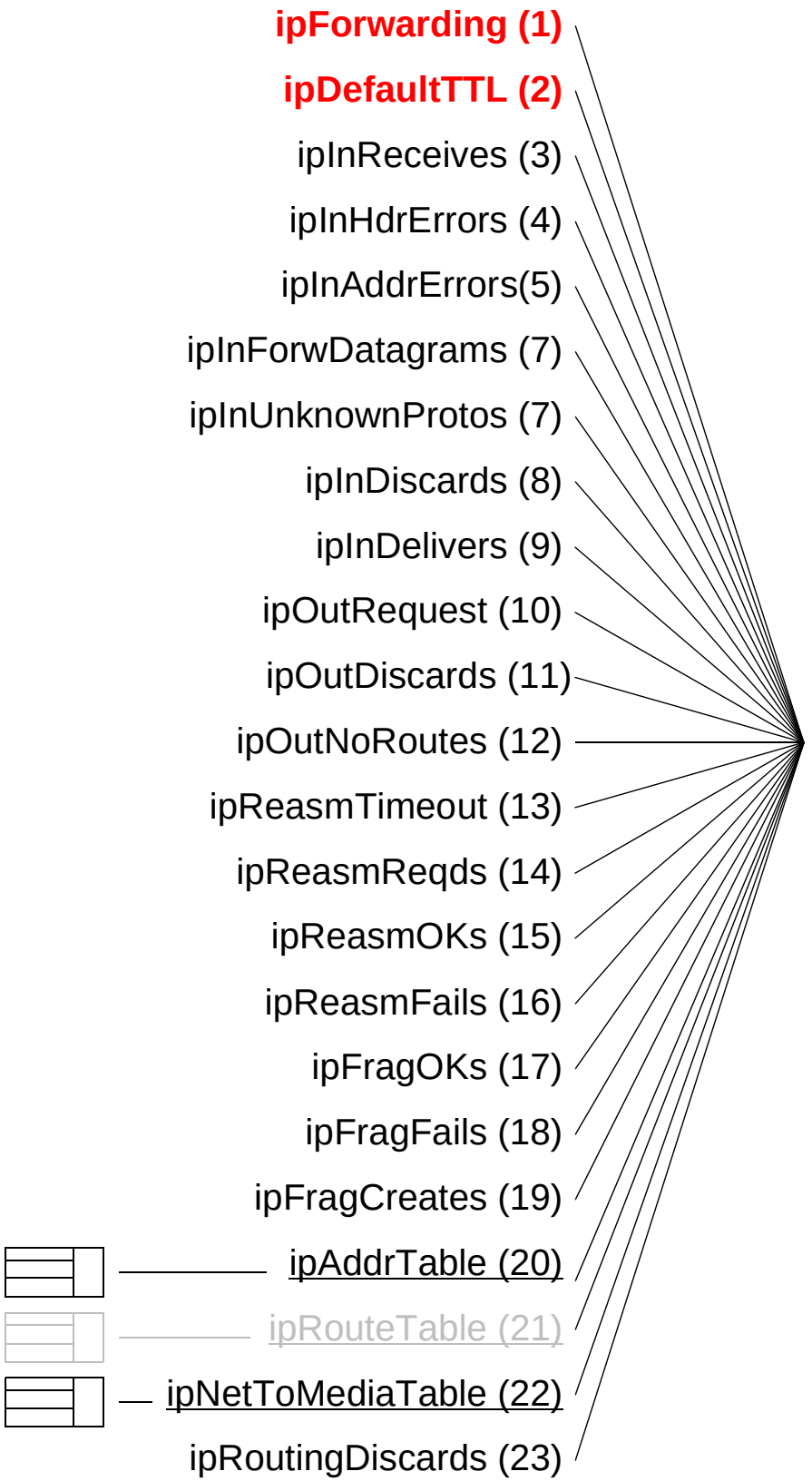
IF PACKET COUNT



IP MIB

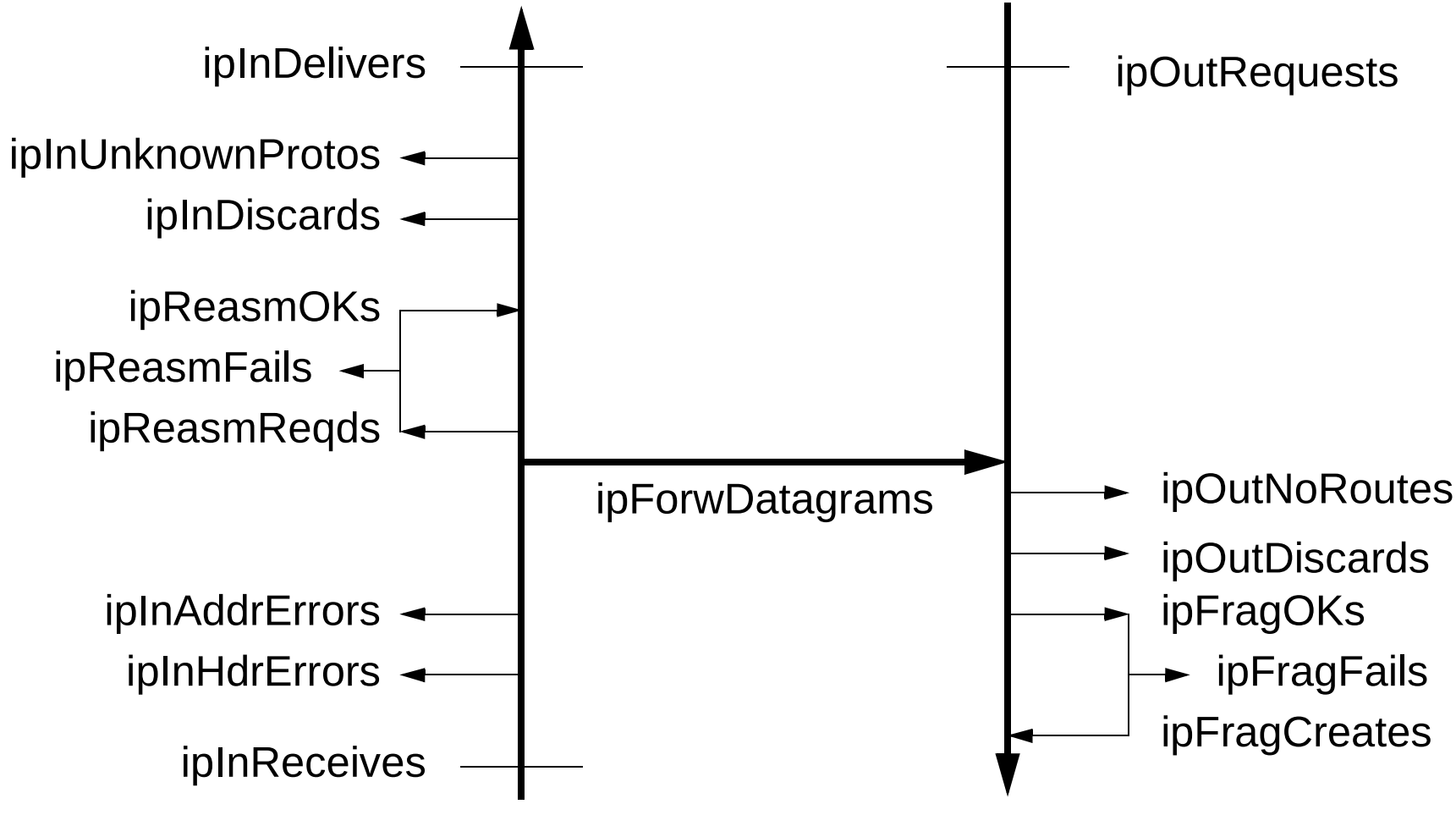
RFC 2011

- IP GROUP
- ICMP GROUP
- IP MIB Conformance

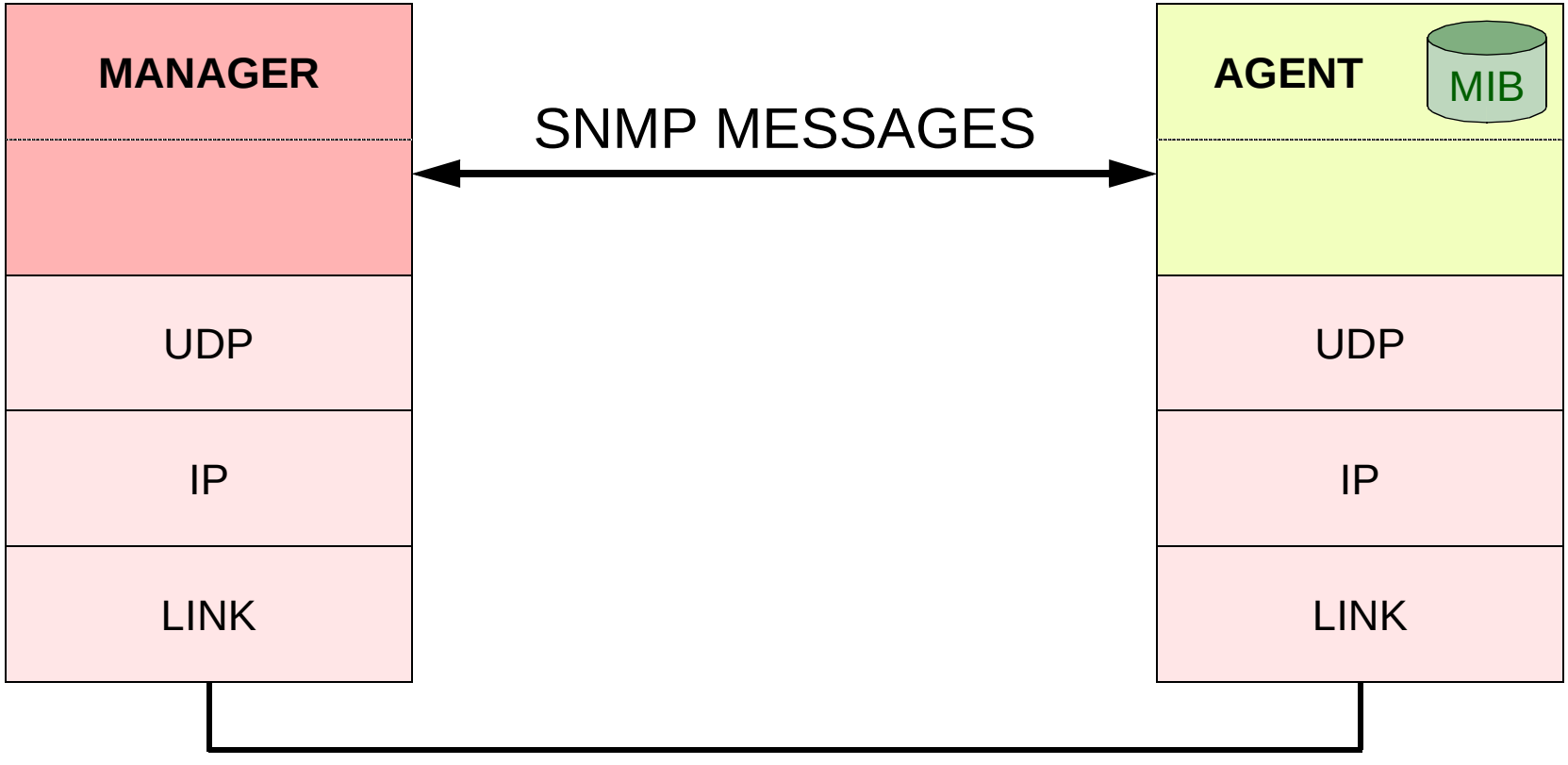

ipForwarding (1)
ipDefaultTTL (2)
ipInReceives (3)
ipInHdrErrors (4)
ipInAddrErrors(5)
ipInForwDatagrams (7)
ipInUnknownProtos (7)
ipInDiscards (8)
ipInDelivers (9)
ipOutRequest (10)
ipOutDiscards (11)
ipOutNoRoutes (12)
ipReasmTimeout (13)
ipReasmReqds (14)
ipReasmOKs (15)
ipReasmFails (16)
ipFragOKs (17)
ipFragFails (18)
ipFragCreates (19)
ipAddrTable (20)
ipRouteTable (21)
ipNetToMediaTable (22)
ipRoutingDiscards (23)
IP (4)

IP GROUP

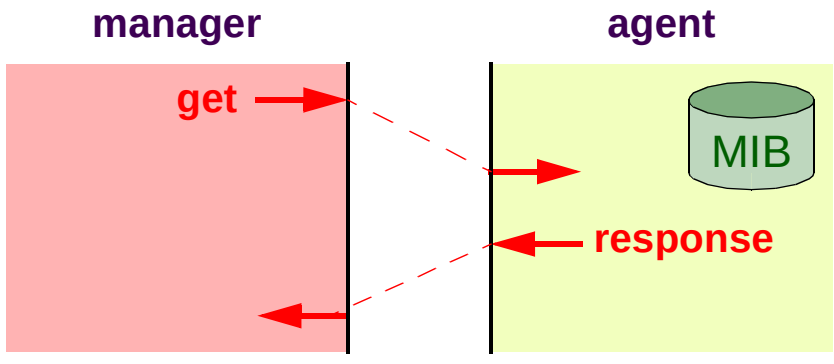
IP PACKET COUNT

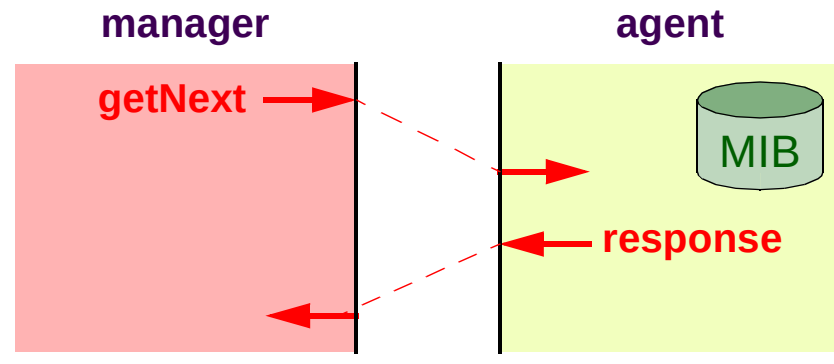


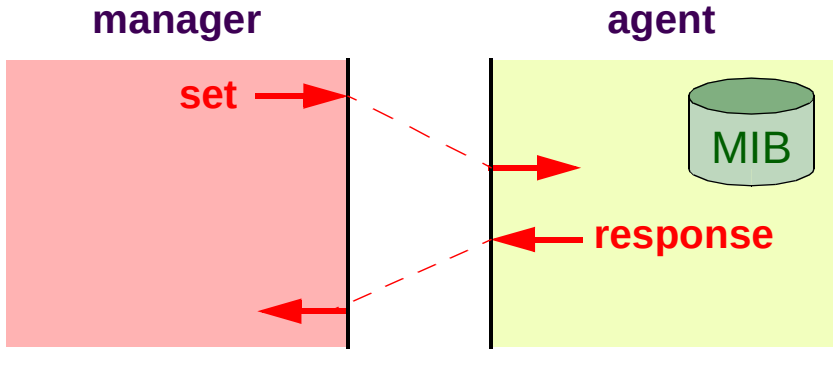
SNMP PROTOCOL

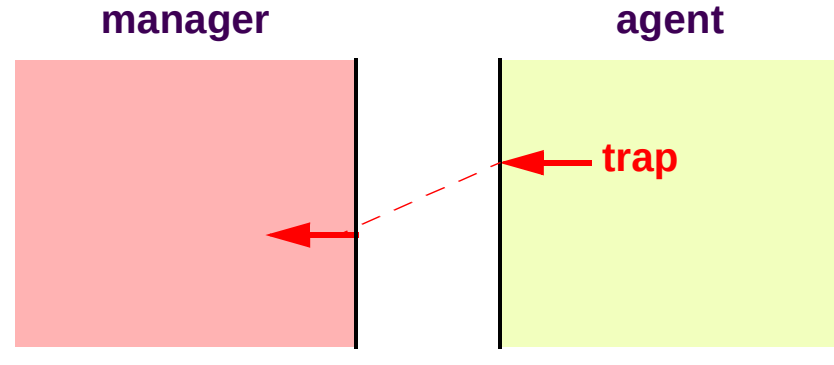


OVERVIEW OF PDUs









MESSAGE & PDU STRUCTURE

variable bindings:

NAME *1*	VALUE *1*	NAME *2*	VALUE *2*	•••	•••	NAME *n*	VALUE *n*

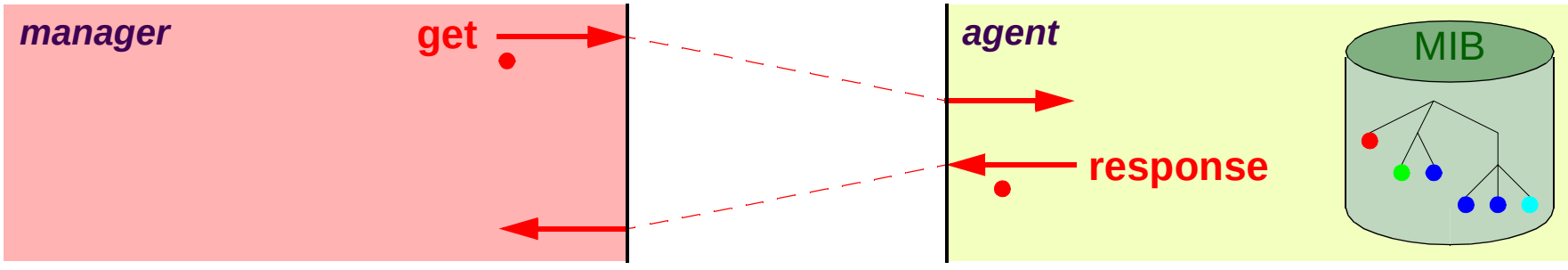
SNMP PDU:

PDU TYPE*	REQUEST ID	ERROR STATUS	ERROR INDEX	VARIABLE BINDINGS

SNMP message:

VERSION	COMMUNITY	SNMP PDU

GET

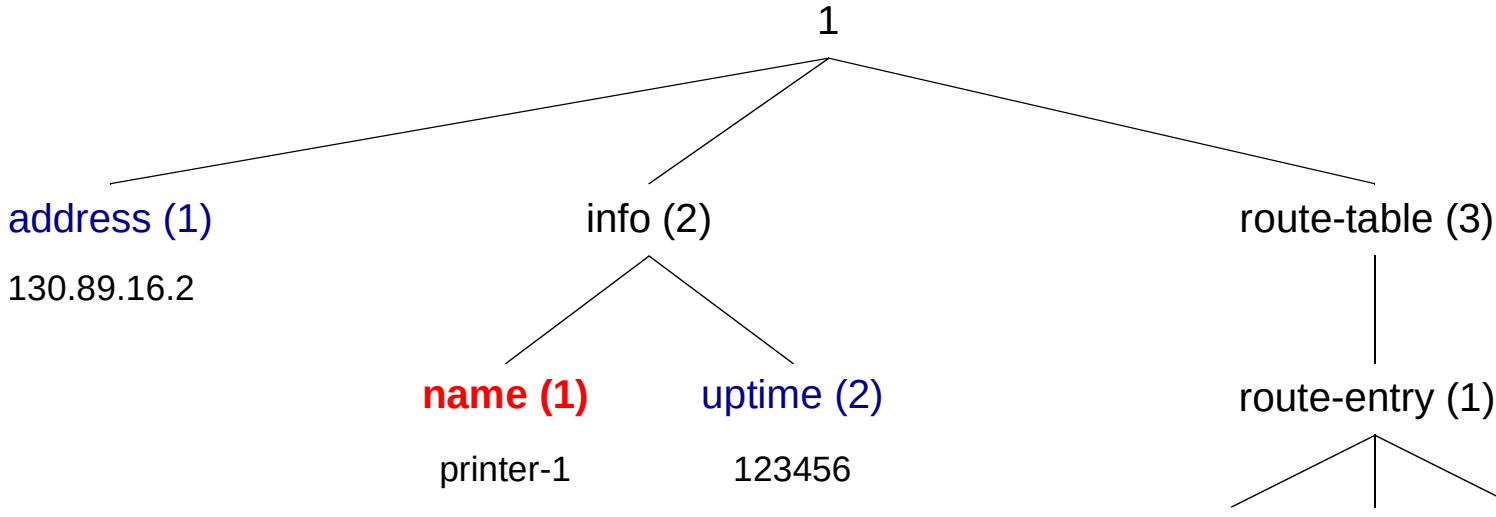


TO REQUEST THE VALUE OF 1 OR MORE VARIABLES

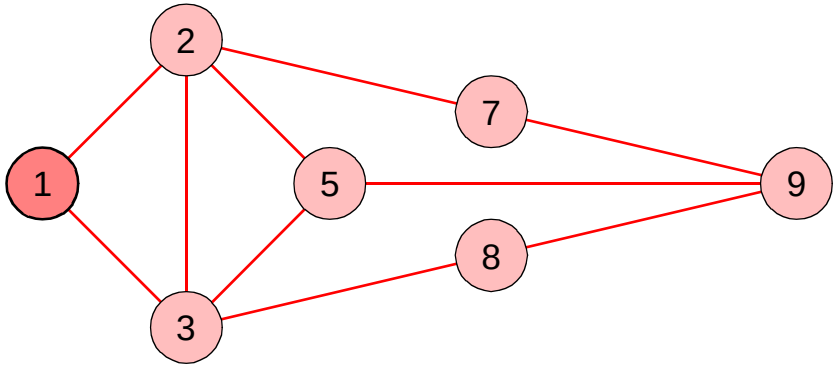
POSSIBLE ERRORS:

- noSuchName ⇨ Object does not exist / Object is not a leaf
- tooBig ⇨ Result does not fit in response PDU
- genErr ⇨ All other causes

EXAMPLE MIB



dest(1)	policy(2)	next(3)
2	1	2
3	1	3
5	1	2
5	2	3
7	1	2
8	1	3
9	1	2



GET EXAMPLES

get(1.1.0)
response(1.1.0 => *130.89.16.2*)

get(1.2.0)
response(error-status = noSuchName)

get(1.1)
response(error-status = noSuchName)

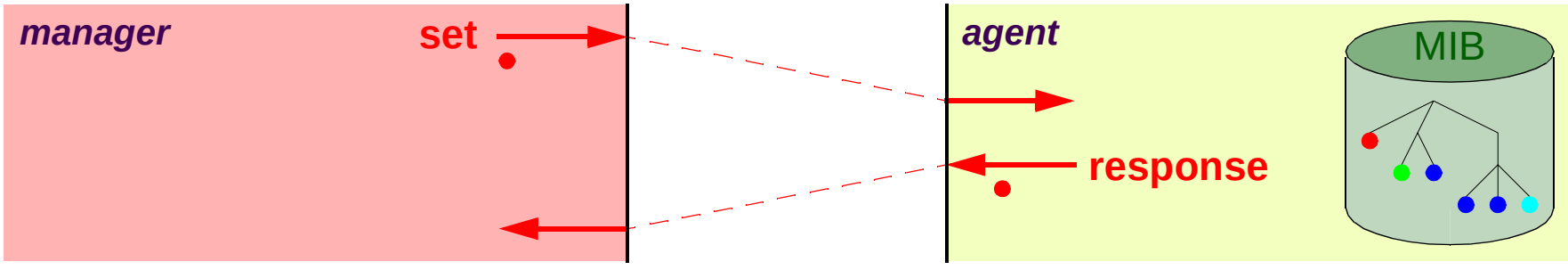
get(1.1.0; 1.2.2.0)
response(1.1.0 => *130.89.16.2*; 1.2.2.0 => *123456*)

get(1.3.1.3.5.1)
response(1.3.1.3.5.1 => *2*)

get(1.3.1.1.5.1)
response(1.3.1.1.5.1 => *5*)

get(1.3.1.1.5.1, 1.3.1.2.5.1, 1.3.1.3.5.1)
response(1.3.1.1.5.1 => *5*, 1.3.1.2.5.1 => *1*, 1.3.1.3.5.1 => *2*)

SET



TO ASSIGN A VALUE TO AN EXISTING OBJECT INSTANCE

TO CREATE NEW INSTANCES
- TABLE ROWS

THE SET REQUEST IS ATOMIC

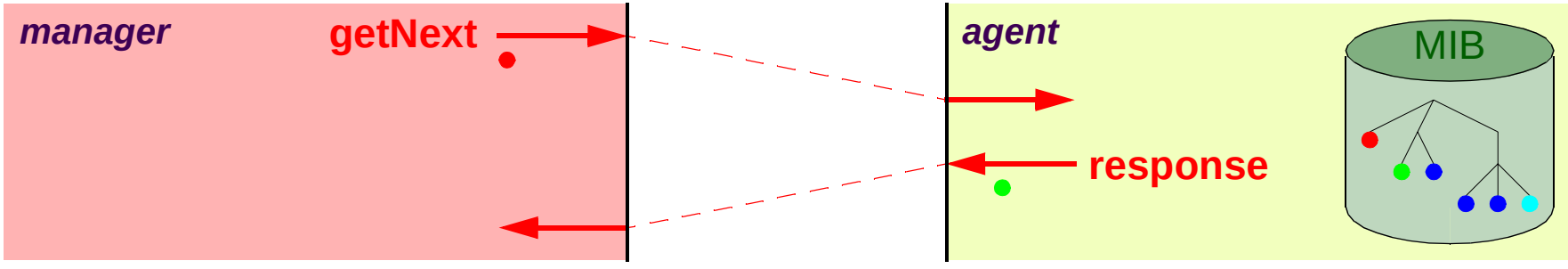
POSSIBLE ERRORS:
- noSuchName
- badValue
- tooBig
- genErr

SET EXAMPLES

set(1.2.1.0 => *my-printer*)
response(noError; 1.2.1.0 => *my-printer*)

set(1.2.1.0 => *my-printer*, 1.2.2.0 => *0*)
response(error-status = noSuchName; error-index = 2)

GET-NEXT



RETRIEVES THE INSTANCE NAME AND VALUE OF THE **NEXT** MIB ELEMENT

TO DISCOVER MIB STRUCTURES

TO RETRIEVE TABLE ROWS

POSSIBLE ERRORS:

- noSuchName (= END OF MIB)
- tooBig
- genErr

GET-NEXT EXAMPLES

getNext(1.1.0)
response(1.2.1.0 => *printer-1*)

getNext(1.2.1.0)
response(1.2.2.0 => *123456*)

getNext(1)
response(1.1.0 => *130.89.16.2*)

getNext(1.3.1.3.5.1)
response(1.3.1.3.5.2 => *3*)

getNext(1.3.1.1; 1.3.1.2; 1.3.1.3)
response(1.3.1.1.2.1 => *2*; 1.3.1.2.2.1 => *1*; 1.3.1.3.2.1 => *2*)

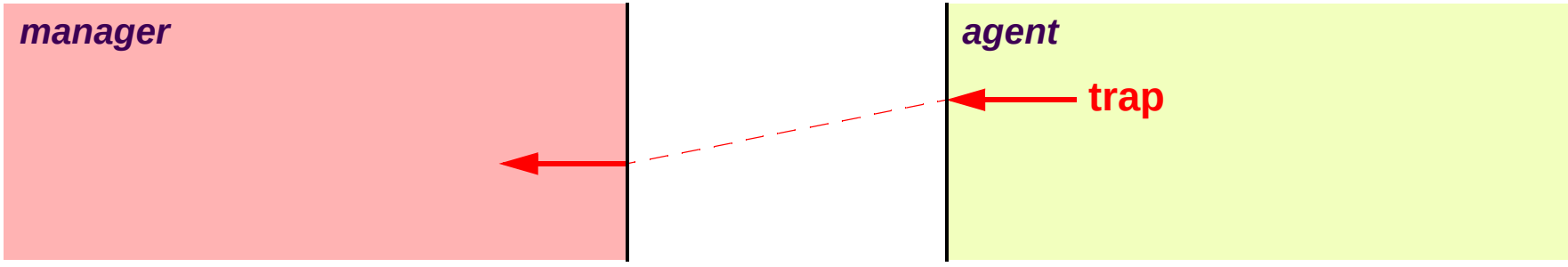
getNext(1.3.1.1.2.1; 1.3.1.2.2.1; 1.3.1.3.2.1)
response(1.3.1.1.3.1 => *3*; 1.3.1.2.3.1 => *1*; 1.3.1.3.3.1 => *3*)

LEXICOGRAPHICAL ORDERING

THE MIB CAN BE CONSIDERED AS AN ORDERED LIST

INSTANCE ID	INSTANCE VALUE
1.1.0	130.89.16.2
1.2.1.0	printer-1
1.2.2.0	123456
1.3.1.1.2.1	2
1.3.1.1.3.1	3
1.3.1.1.5.1	5
•••	•••
1.3.1.1.9.1	9
1.3.1.2.2.1	1
1.3.1.2.3.1	1
•••	•••
1.3.1.2.9.1	1
1.3.1.3.2.1	2
1.3.1.3.3.1	3
1.3.1.3.5.1	2
1.3.1.3.5.2	3
1.3.1.3.7.1	2
•••	•••

TRAP



TO SIGNAL AN EVENT

TRAP RECEPTION IS NOT CONFIRMED
(THUS UNRELIABLE)

POLLING REMAINS NECESSARY

AGENTS MAY BE CONFIGURED SUCH THAT:
- NO TRAPS WILL BE TRANSMITTED
- TRAPS WILL BE TRANSMITTED TO CERTAIN MANAGERS

SNMPv2

OVERVIEW:

RFCs

LIMITATIONS OF SNMPv1

HISTORY OF SNMPv2
- HIERARCHIES
- SECURITY

SNMPv2 PROTOCOL OPERATIONS

SNMPv2 RFCs

COMMUNICATION MODEL

• DRAFT STANDARD

• RFC 1905, RFC1906

SECURITY MODEL - SNMPv2C:

• COMMUNITY BASED SNMP

• SAME 'SECURITY MECHANISMS' AS SNMPv1

• EXPERIMENTAL STATUS

• RFC 1901

SECURITY MODEL - SNMPv2U:

• USER BASED SECURITY (AUTHENTICATION / ENCRYPTION / ACCESS CONTROL)

• EXPERIMENTAL STATUS

• RFC 1909, RFC1910

INFORMATION MODEL:

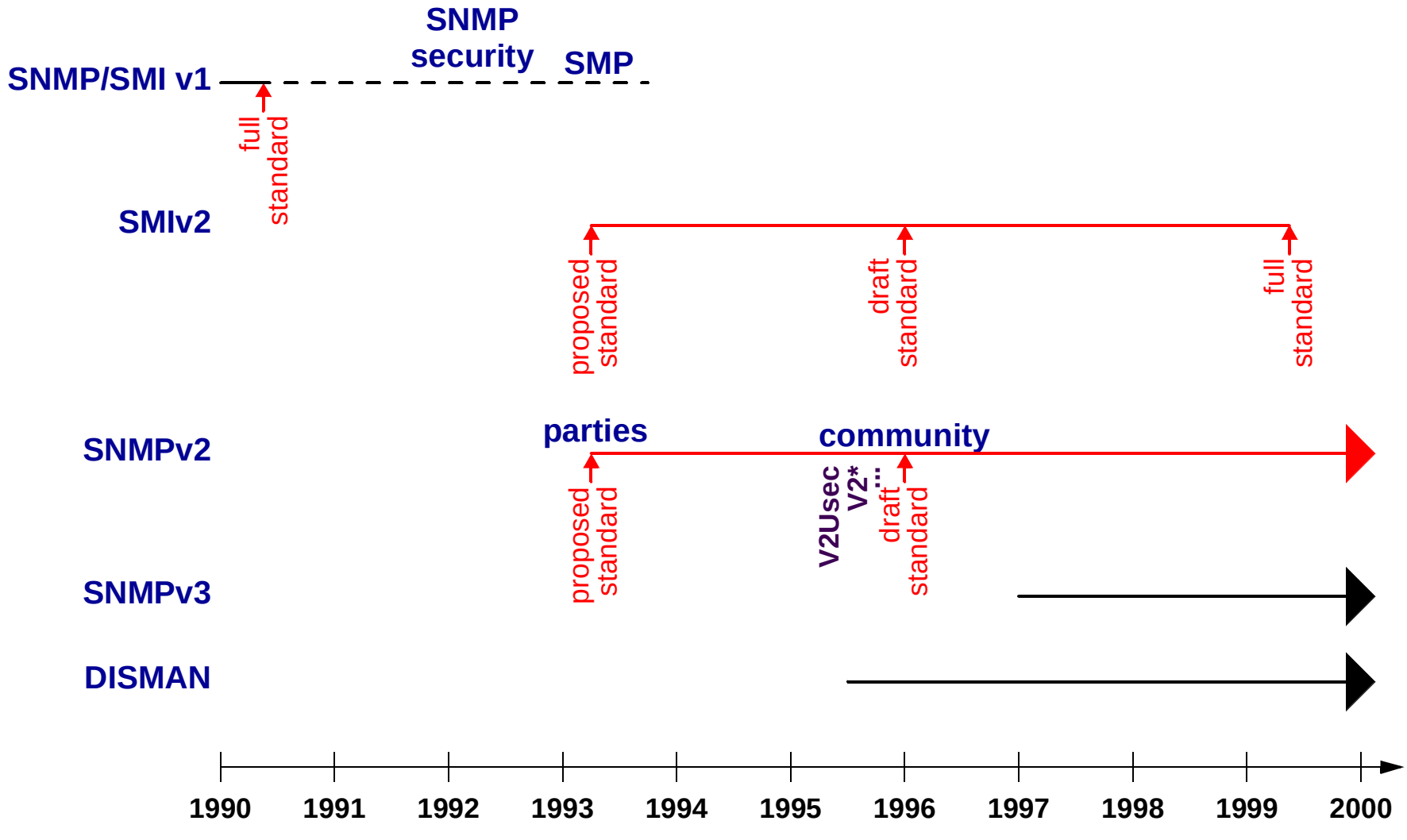
• STANDARD

• RFC2578, RFC2579, RFC2580

LIMITATIONS OF SNMPv1

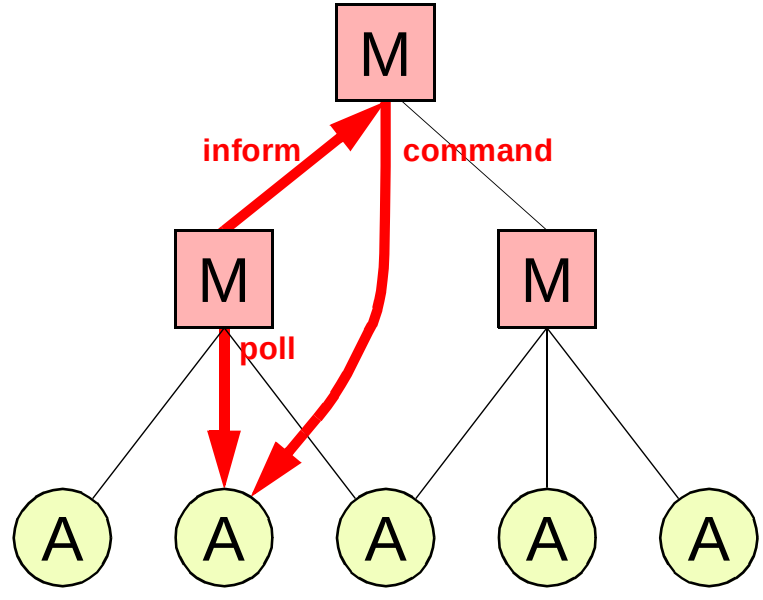
- UNDOCUMENTED RULES
- LIMITED ERROR CODES
- LIMITED DATA TYPES
- LIMITED NOTIFICATIONS
- LIMITED PERFORMANCE
- TRANSPORT DEPENDENCE
- LACK OF HIERARCHIES
- LACK OF SECURITY

HISTORY OF SNMPv2



HIERARCHIES: ORIGINAL IDEA

MANAGER TO MANAGER (M2M) MIB



- STANDARD MIB APPROACH
- LIMITED FUNCTIONALITY
- RUN-TIME BEHAVIOUR MUST BE DEFINED AT IMPLEMENTATION TIME

HIERARCHIES: STATUS

WORK HAS MOVED TO A SEPARATE
DISTRIBUTED MANAGEMENT GROUP
(DISMAN)

THREE APPROACHES ARE STANDARDIZED:

- MIB BASED (EXPRESSION, EVENT AND NOTIFICATION LOG MIB)
- SCRIPT BASED (SCRIPT AND SCHEDULE MIB)
- REMOTE OPERATIONS BASED (REMOPS MIB)

SNMPv2 SECURITY: WHAT HAPPENED?

APRIL 1993:

PROPOSED STANDARD
FOUR EDITORS
SECURITY BASED ON *PARTIES*
FIRST PROTOTYPES APPEARED SOON

JUNE 1995:

PROPOSED STANDARD REJECTED BY TWO OF THE ORIGINAL EDITORS!

AUGUST 1995:

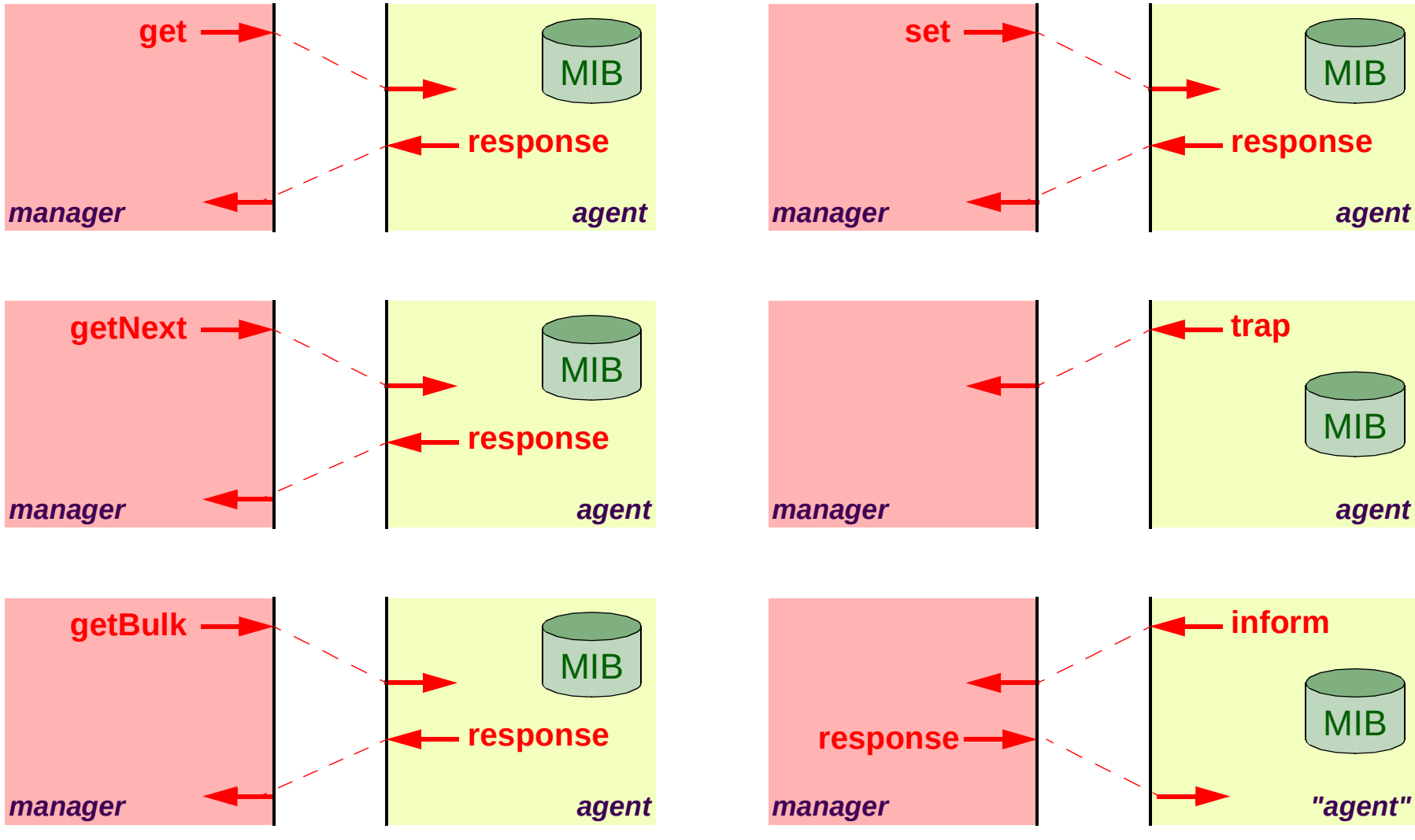
GENERAL AGREEMENT THAT PARTY BASED MODEL WAS TOO COMPLEX!
MANY NEW PROPOSALS APPEARED:

- SNMPv2C: COMMUNITY BASED
- SNMPv2U: USER BASED
- ...

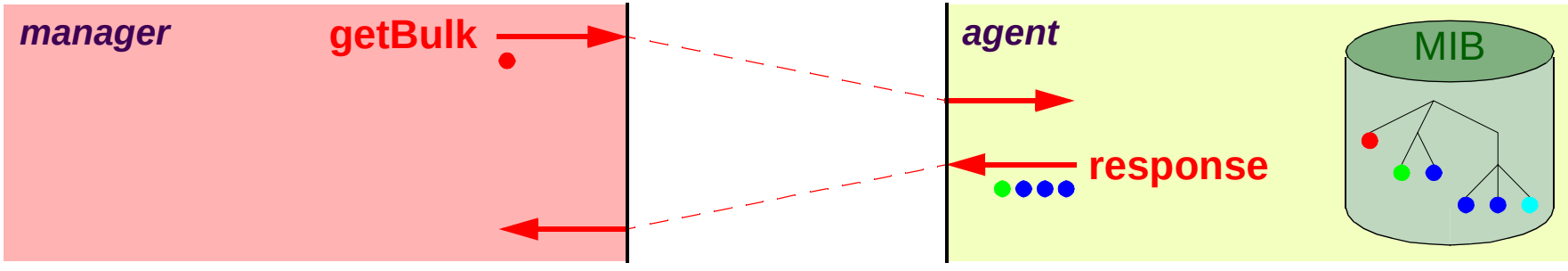
1997:

NEW SNMPv3 WORKING GROUP WAS FORMED
WITH NEW EDITORS

SNMPv2 PROTOCOL OPERATIONS



GET-BULK



NEW IN SNMPv2

TO RETRIEVE A LARGE NUMBER OF VARBINDS

IMPROVES PERFORMANCE!

GET-BULK

getBulk REQUEST HAS TWO ADDITIONAL PARAMETERS:

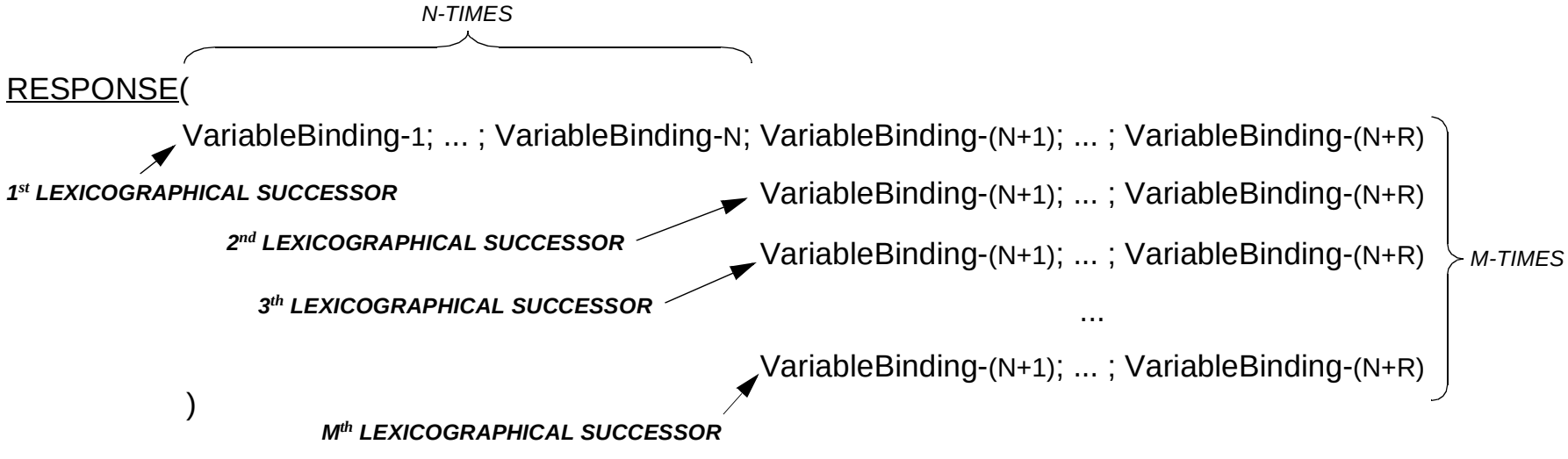
- non-repeators
- max-repetitions

- THE FIRST N ELEMENTS (non-repeators) OF THE VARBIND LIST ARE TREATED AS IF THE OPERATION WAS A NORMAL getnext OPERATION

- THE NEXT ELEMENTS OF THE VARBIND LIST ARE TREATED AS IF THE OPERATION CONSISTED OF A NUMBER (max-repetitions) OF REPEATED getnext OPERATIONS

GET-BULK

REQUEST(non-repeaters = N; max-repetitions = M;
VariableBinding-1; ... ; VariableBinding-N; VariableBinding-(N+1); ... ; VariableBinding-(N+R)
)



GET-BULK EXAMPLE

getBulk(max-repetitions = 4; 1.1)

response(
1.1.0 => *130.89.16.2*
1.2.1.0 => *printer-1*
1.2.2.0 => *123456*
1.3.1.1.2.1 => *2*)

getBulk(max-repetitions = 3; 1.3.1.1; 1.3.1.2; 1.3.1.3)

response(

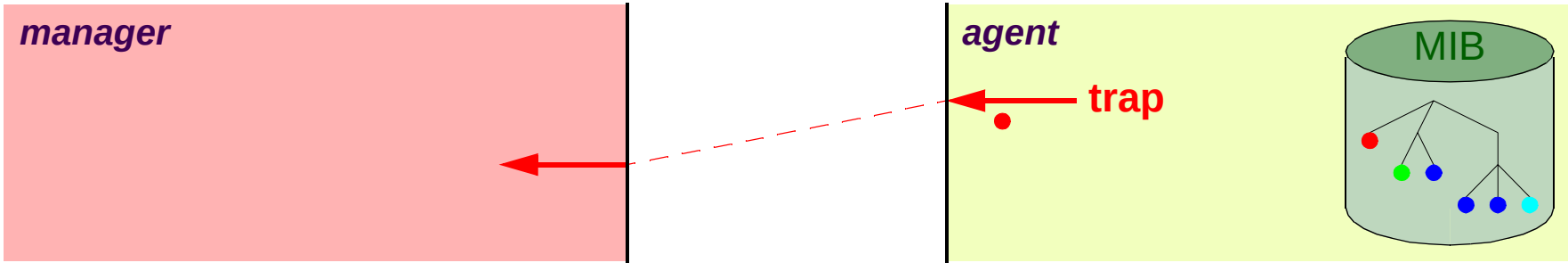
1.3.1.1.2.1 => *2*;	1.3.1.2.2.1 => *1*;	1.3.1.3.2.1 => *2*
1.3.1.1.3.1 => *3*;	1.3.1.2.3.1 => *1*;	1.3.1.3.3.1 => *3*
1.3.1.1.5.1 => *5*;	1.3.1.2.5.1 => *1*;	1.3.1.3.5.1 => *2*

)

SET: NEW ERROR CODES

	SNMPv1	SNMPv2
PHASE 1:	badValue	wrongValue
	badValue	wrongEncoding
	badValue	wrongType
	badValue	wrongLength
	badValue	inconsistentValue
	noSuchName	noAccess
	noSuchName	notWritable
	noSuchName	noCreation
	noSuchName	inconsistentName
	genErr	resourceUnavailable
	genErr	genErr
PHASE 2:	genErr	CommitFailed
	genErr	undoFailed

TRAP



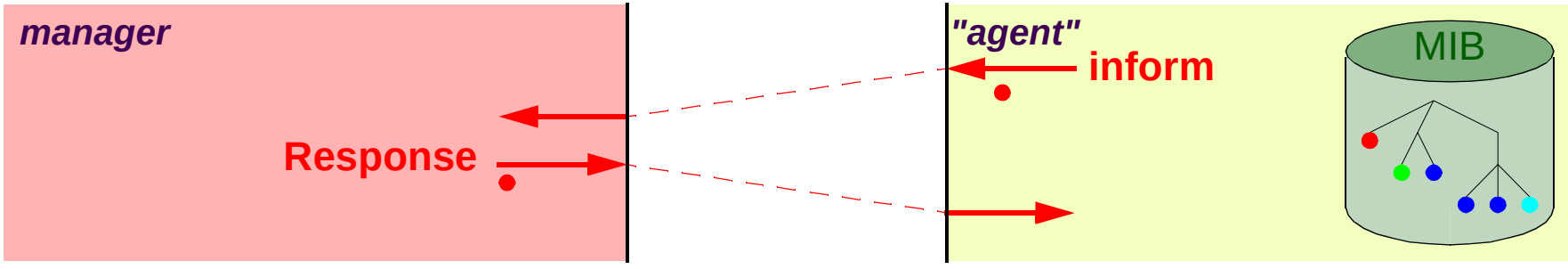
SNMPv1:

- COLD START
- WARM START
- LINK DOWN
- LINK UP
- AUTHETICATION FAILURE
- EGP NEIGHBOR LOSS

SNMPv2:

- MIBs MAY NOW INCLUDE NOTIFICATION TYPE MACROS
- FIRST TWO VARBINDS: sysUptime AND snmpTrapOID
- USES SAME FORMAT AS OTHER PDUs

INFORM



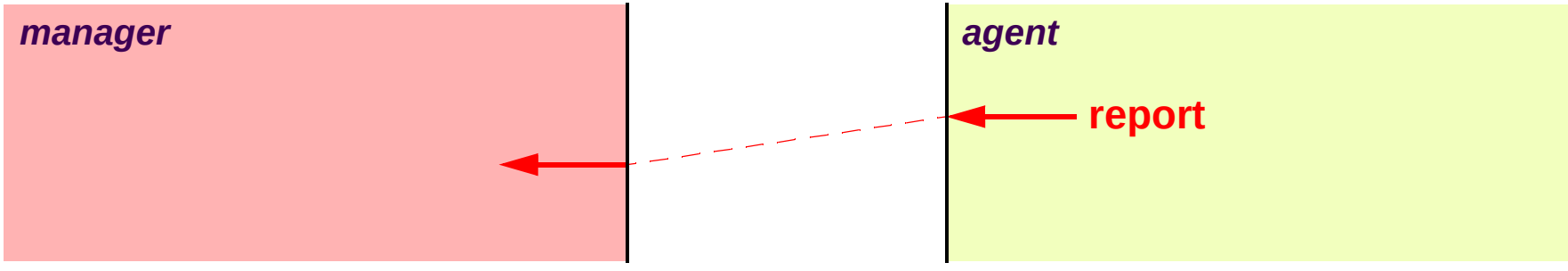
CONFIRMED TRAP

ORIGINALLY TO INFORM A HIGHER LEVEL MANAGER

SAME FORMAT AS TRAP PDU

POSSIBLE ERROR: tooBig

REPORT



NEW PDU TO SIGNAL PROTOCOL EXCEPTIONS / ERRORS

NO SEMANTICS DEFINED IN SNMPv2

SNMPv3

OVERVIEW:

DESIGN DECISIONS

ARCHITECTURE

SNMP MESSAGE STRUCTURE

SECURE COMMUNICATION
- USER SECURITY MODEL (USM)

ACCESS CONTROL
- VIEW BASED ACCESS CONTROL MODEL (VACM)

RFCs

DESIGN DECISIONS

ADDRESS THE NEED FOR SECURY SET SUPPORT

DEFINE AN ARCHITECTURE THAT ALLOWS FOR LONGEVITY OF SNMP

ALLOW THAT DIFFERENT PORTIONS OF THE ARCHITECTURE
MOVE AT DIFFERENT SPEEDS TOWARDS STANDARD STATUS

ALLOW FOR FUTURE EXTENSIONS

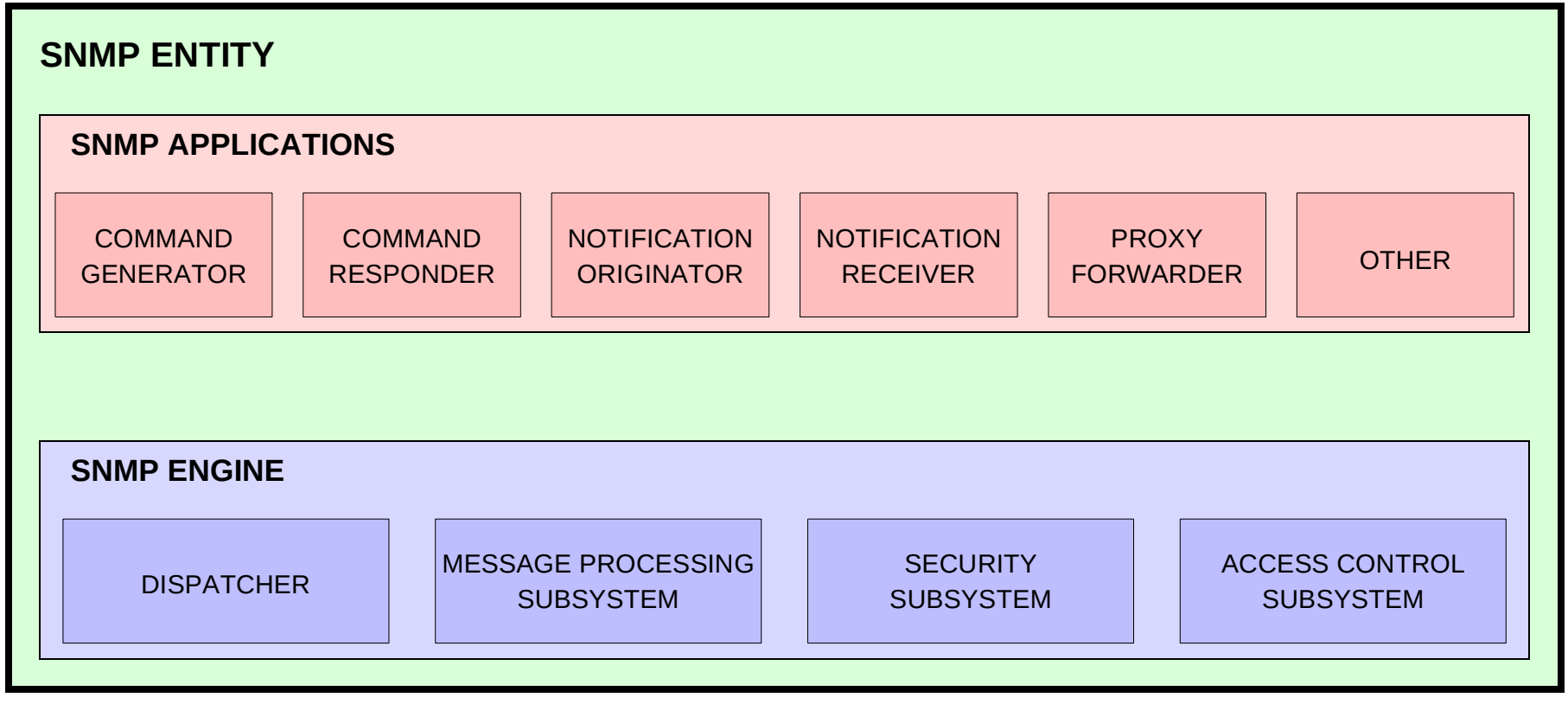
KEEP SNMP AS SIMPLE AS POSSIBLE

ALLOW FOR MINIMAL IMPLEMENTATIONS

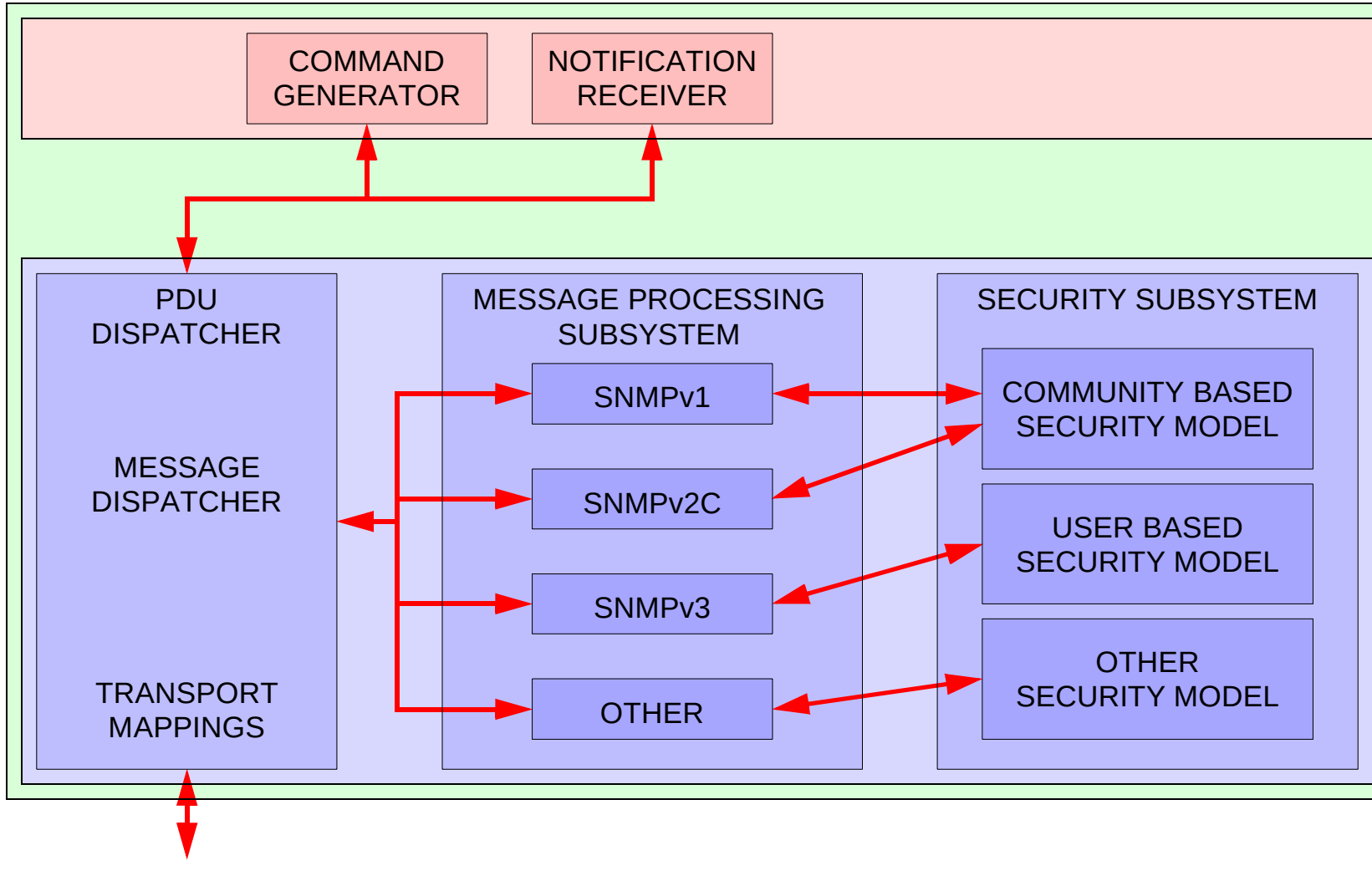
SUPPORT ALSO THE MORE COMPLEX FEATURES,
WHICH ARE REQUIRED IN LARGE NETWORKS

RE-USE EXISTING SPECIFICATIONS, WHENEVER POSSIBLE

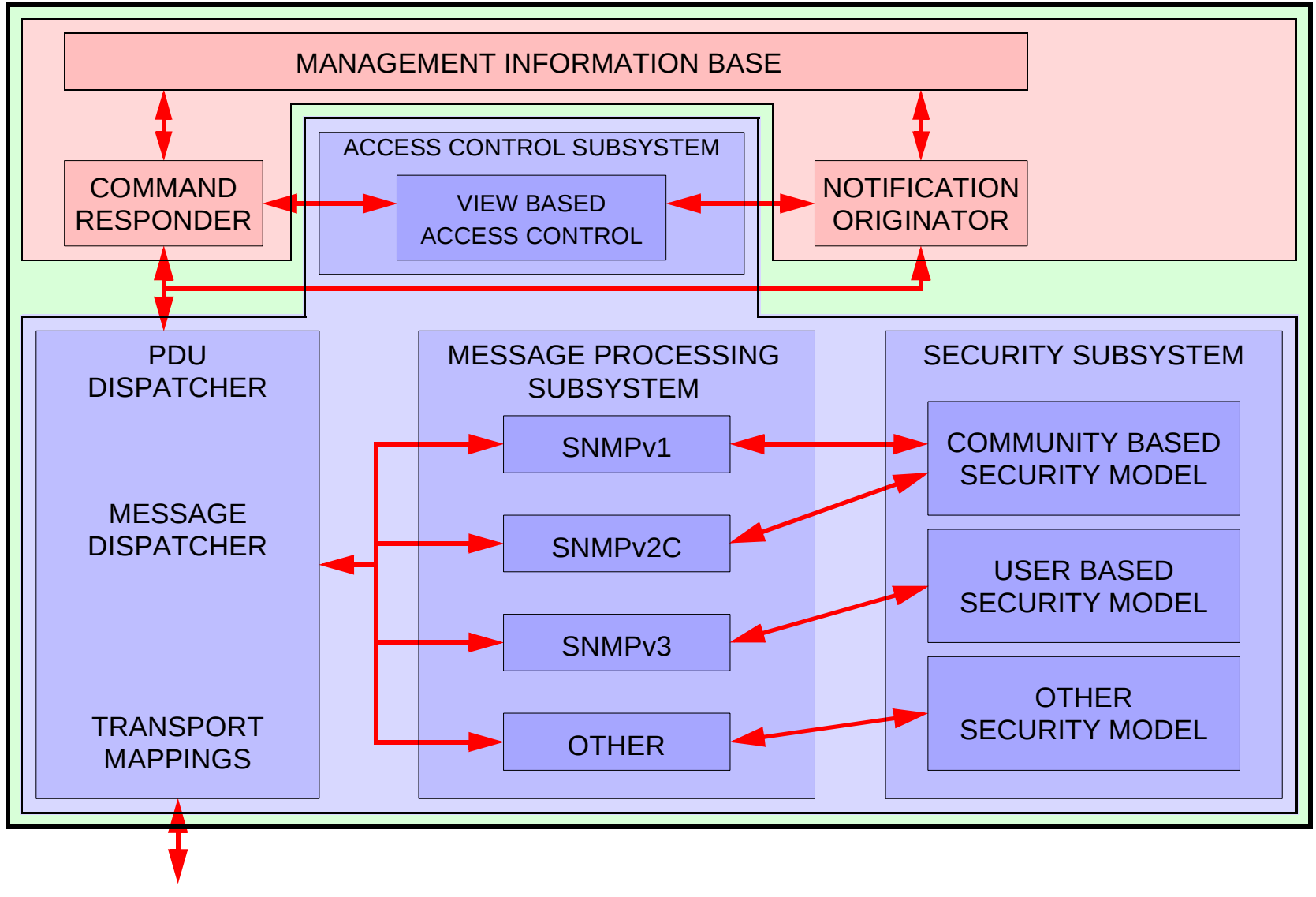
SNMPv3 ARCHITECTURE



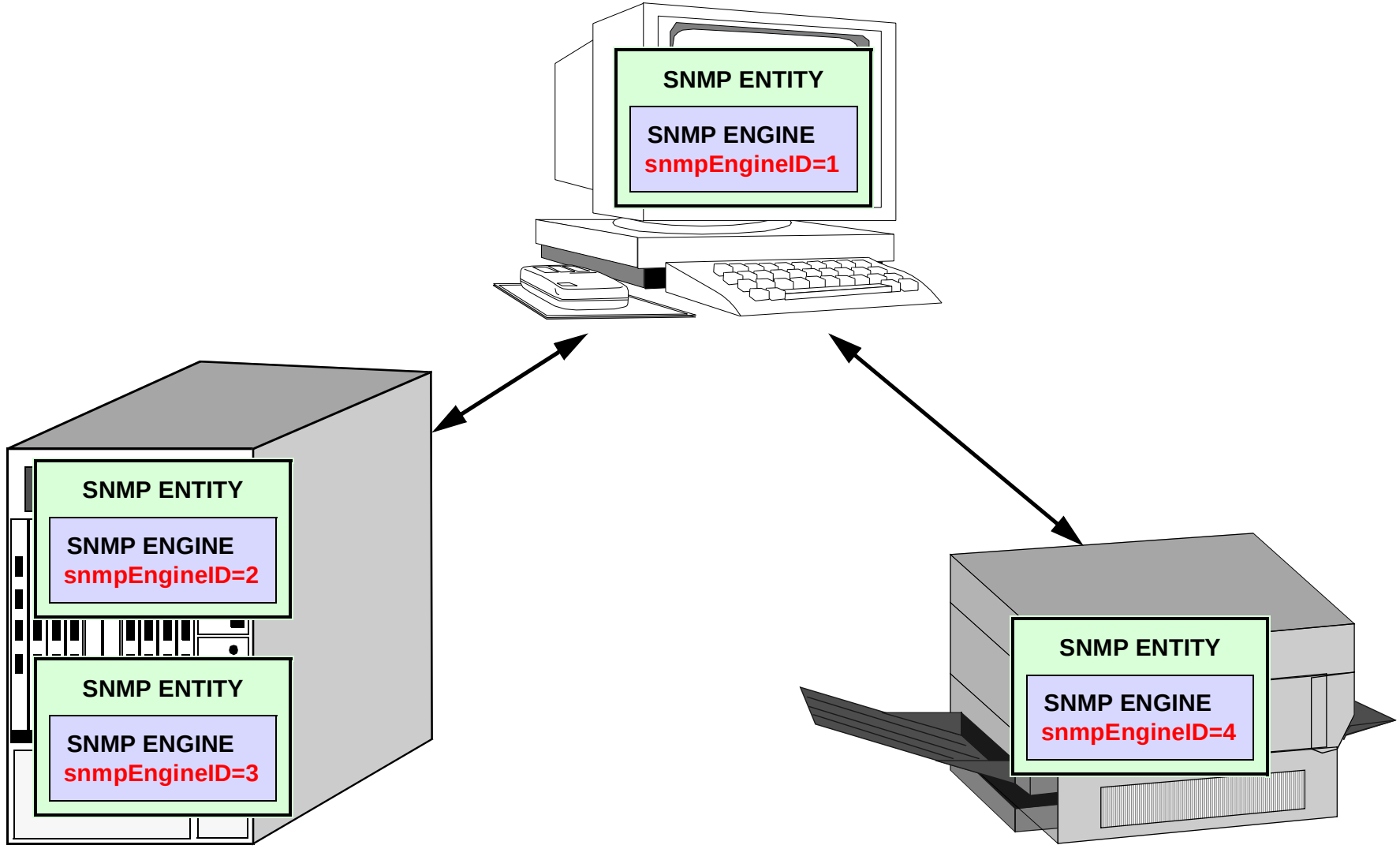
SNMPv3 ARCHITECTURE: MANAGER



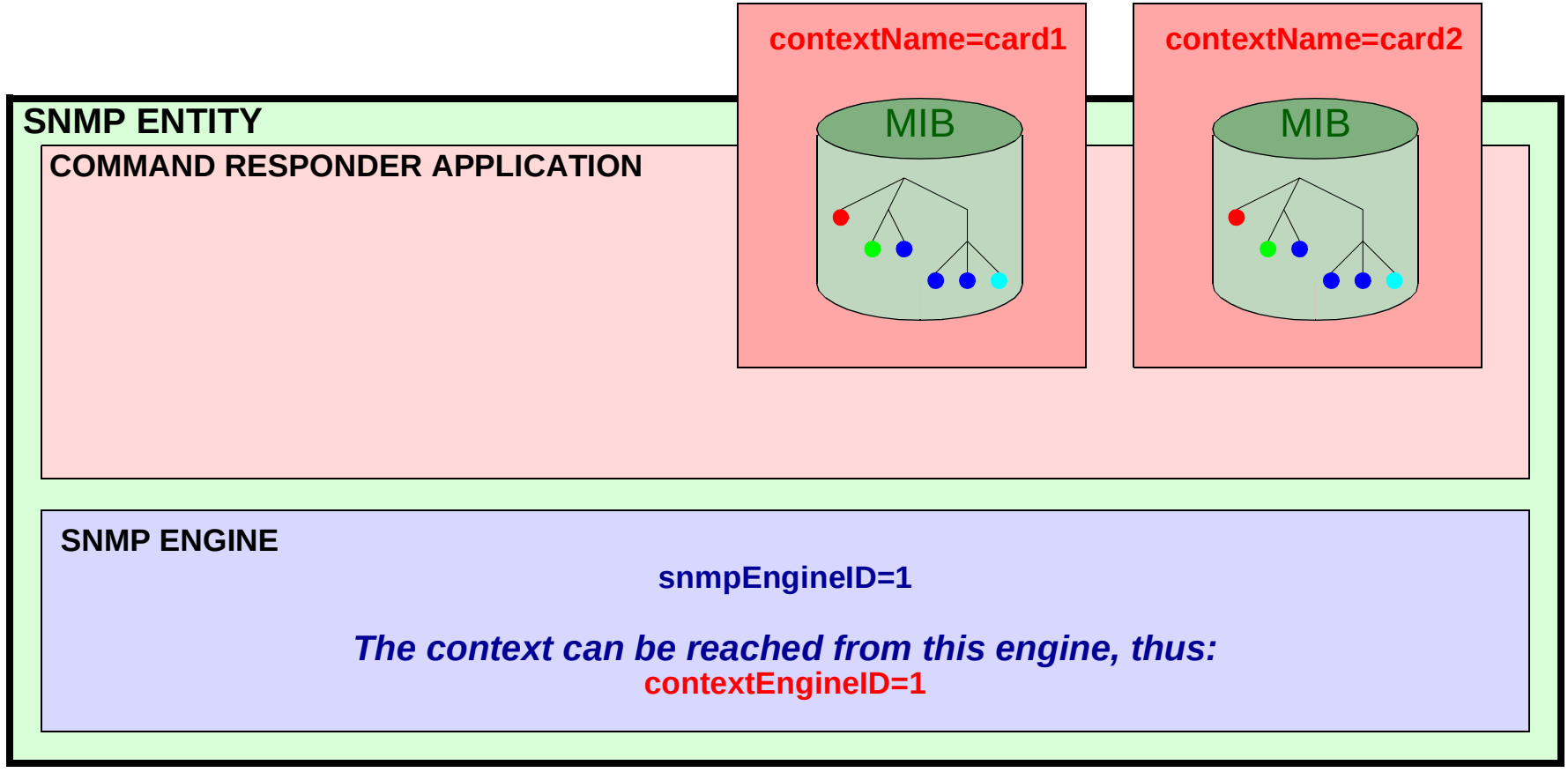
SNMPv3 ARCHITECTURE: AGENT



CONCEPTS: snmpEngineID



CONCEPTS: Context



MODULES OF THE SNMPv3 ARCHITECTURE

DISPATCHER AND MESSAGE PROCESSING MODULE

- SNMPv3 MESSAGE STRUCTURE
- snmpMPDMIB
- RFC 2572

APPLICATIONS

- snmpTargetMIB
- snmpNotificationMIB
- snmpProxyMIB
- RFC 2573

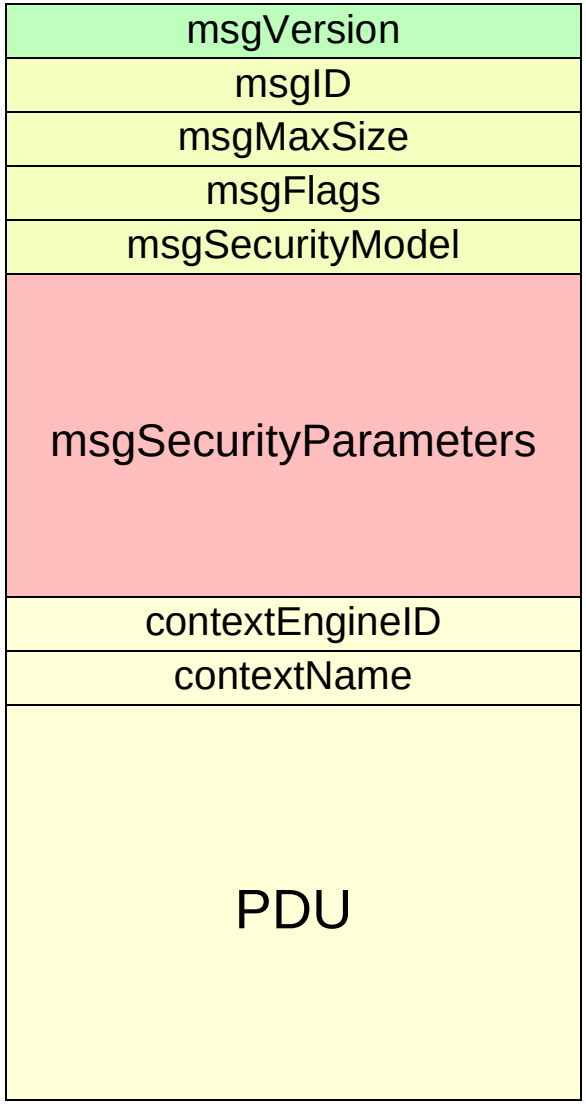
SECURITY SUBSYSTEM

- USER BASED SECURITY MODEL
- snmpUsmMIB
- RFC 2574

ACCESS CONTROL SUBSYSTEM

- VIEW BASED ACCESS CONTROL MODEL
- snmpVacmMIB
- RFC 2574

SNMPv3 MESSAGE STRUCTURE



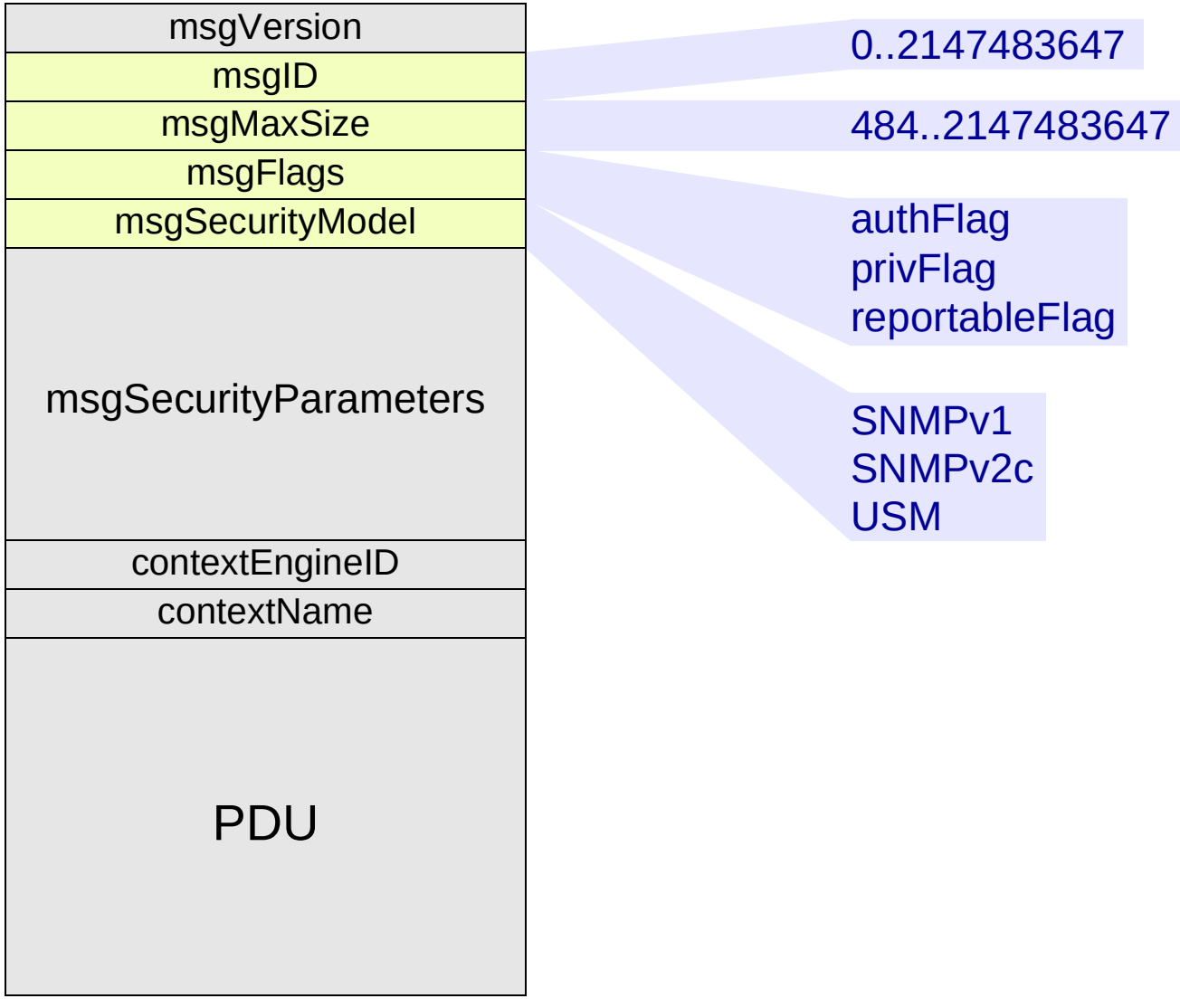
USED BY MESSAGE PROCESSING SUBSYSTEM

USED BY SNMPv3 PROCESSING MODULE

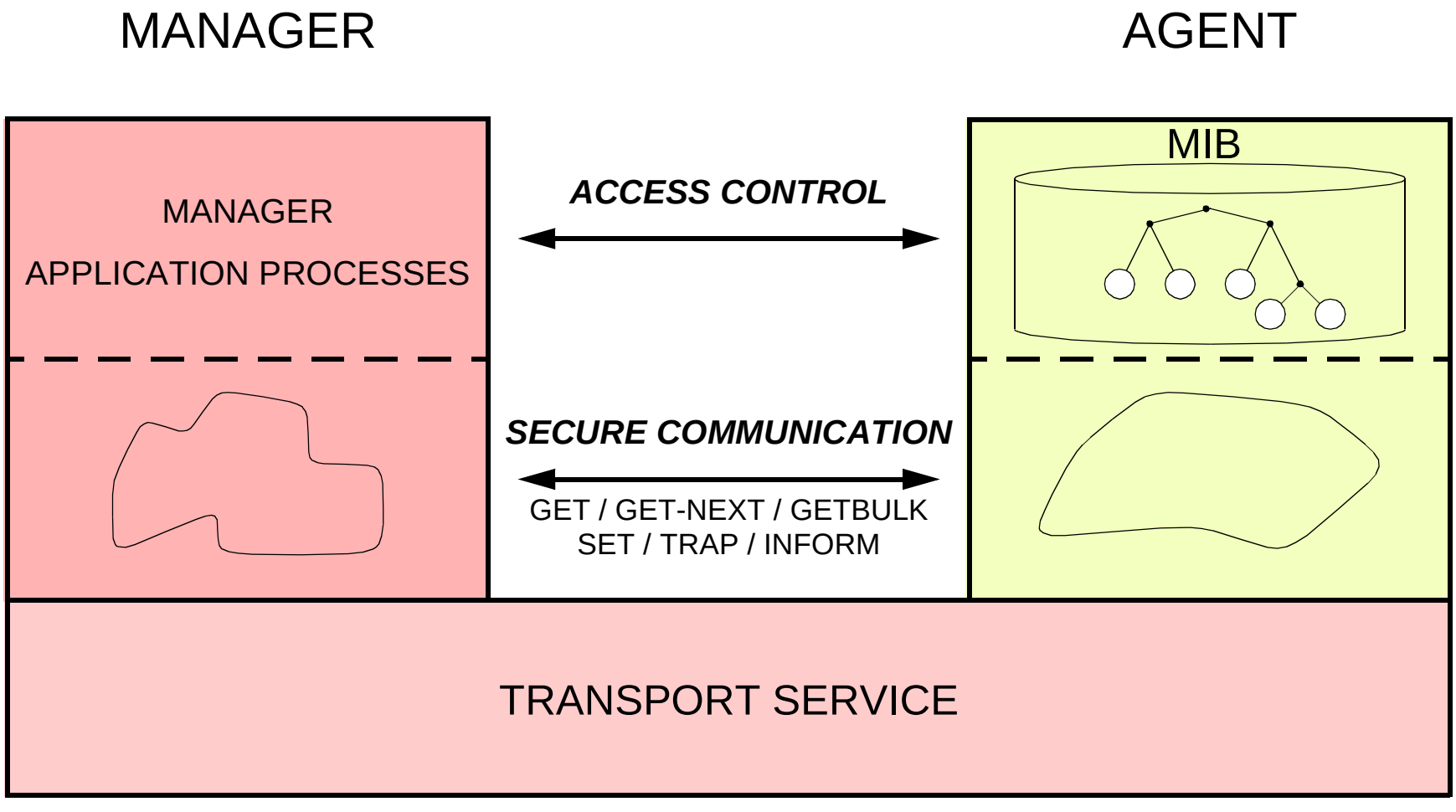
USED BY SECURITY SUBSYSTEM

USED BY ACCESS CONTROL SUBSYSTEM AND APPLICATIONS

SNMPv3 PROCESSING MODULE PARAMETERS



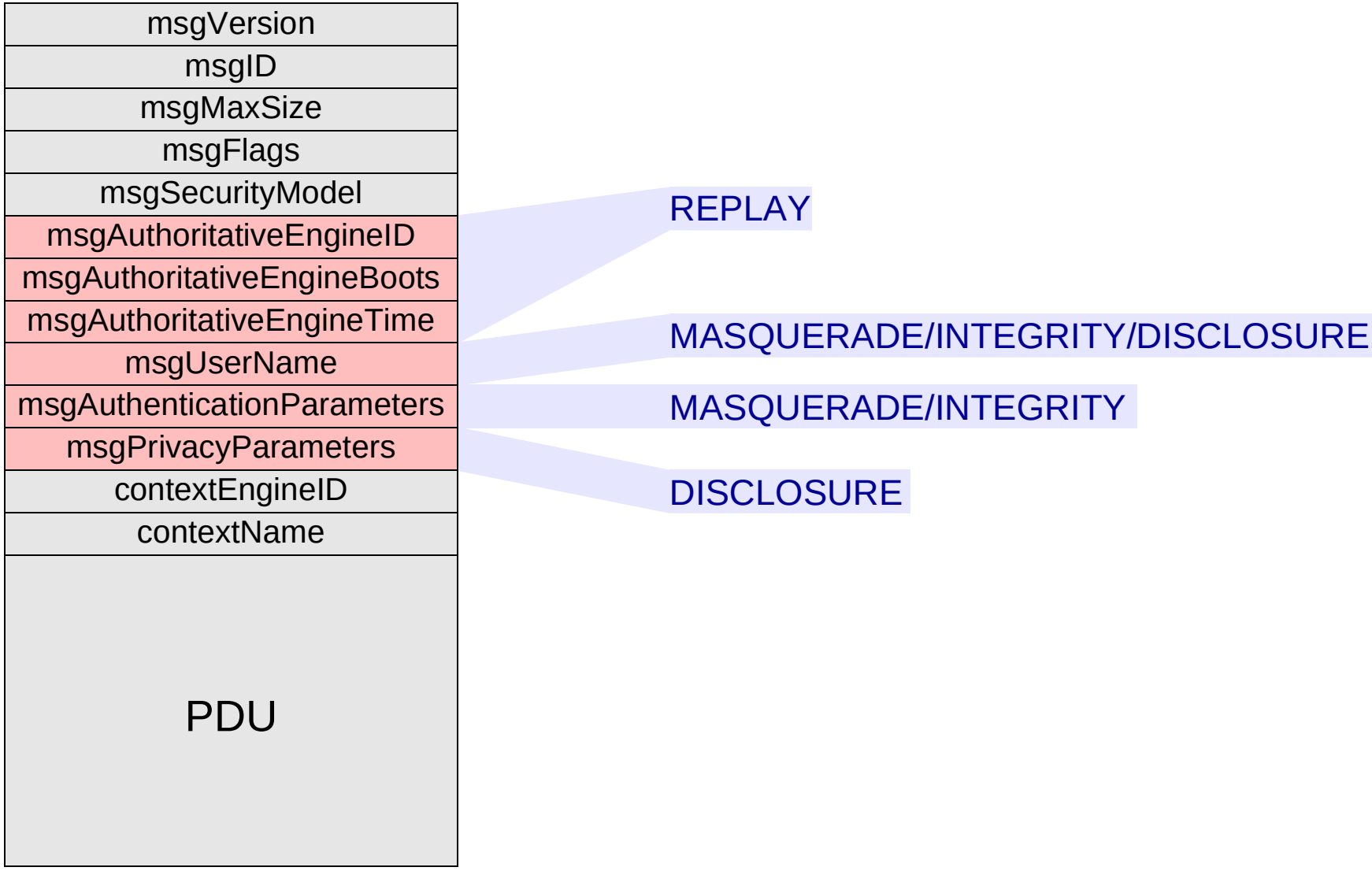
SECURE COMMUNICATION VERSUS ACCESS CONTROL



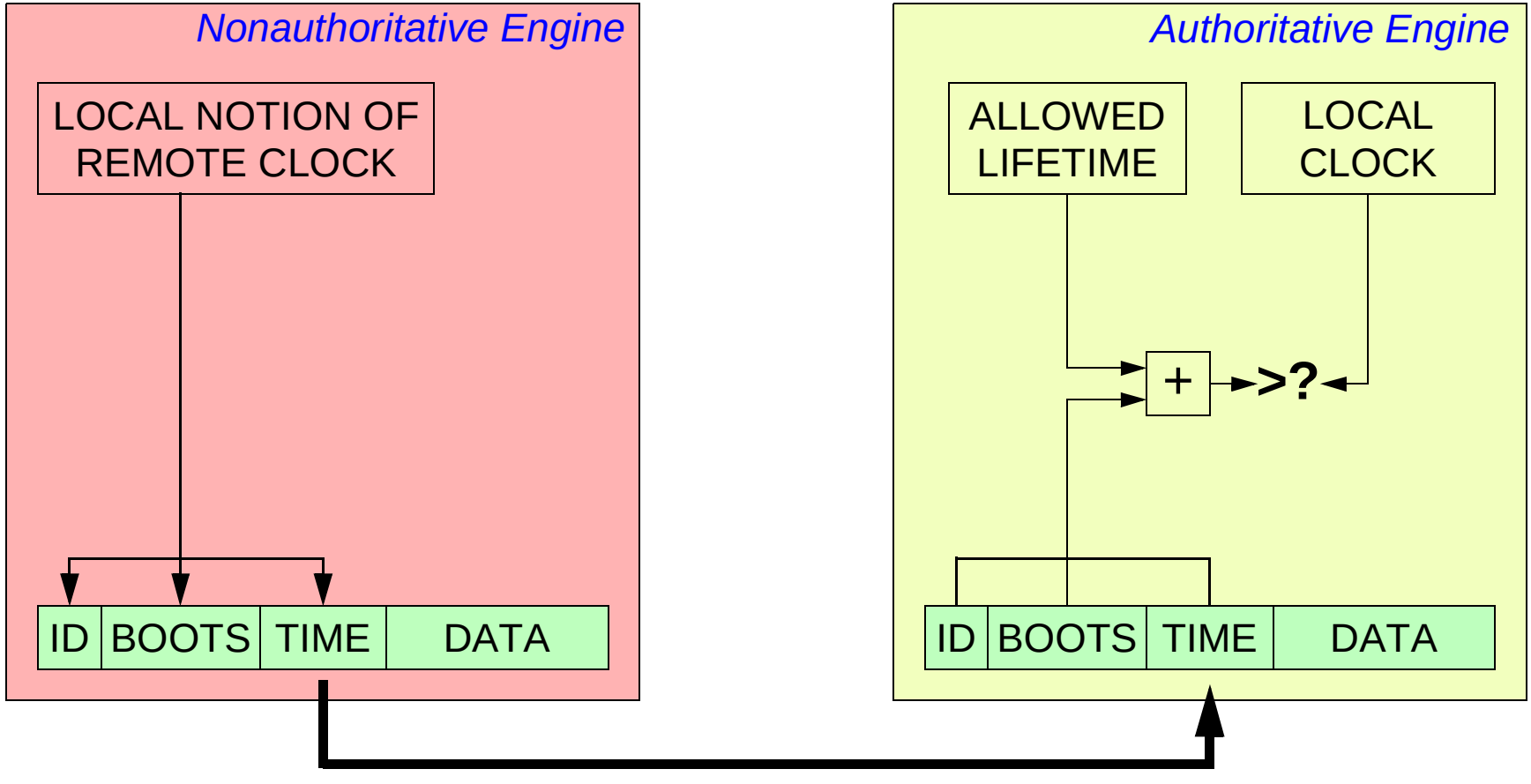
USM: SECURITY THREATS

THREAT	ADDRESSED?	MECHANISM
REPLAY	YES	TIME STAMP
MASQUERADE	YES	MD5 / SHA-1
INTEGRITY	YES	(MD5 / SHA-1)
DISCLOSURE	YES	DES
DENIAL OF SERVICE	NO	
TRAFFIC ANALYSIS	NO	

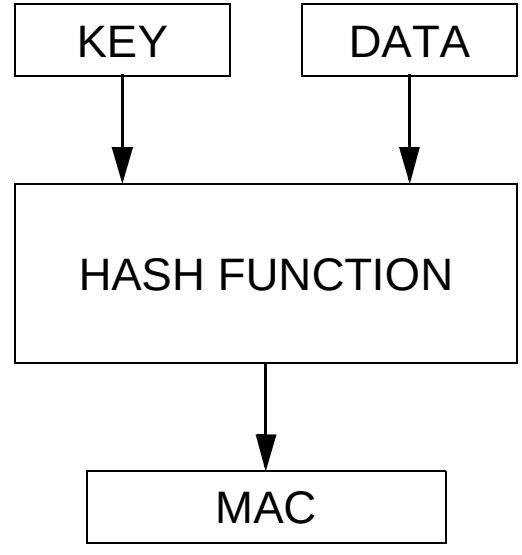
USM MESSAGE STRUCTURE



IDEA BEHIND REPLAY PROTECTION

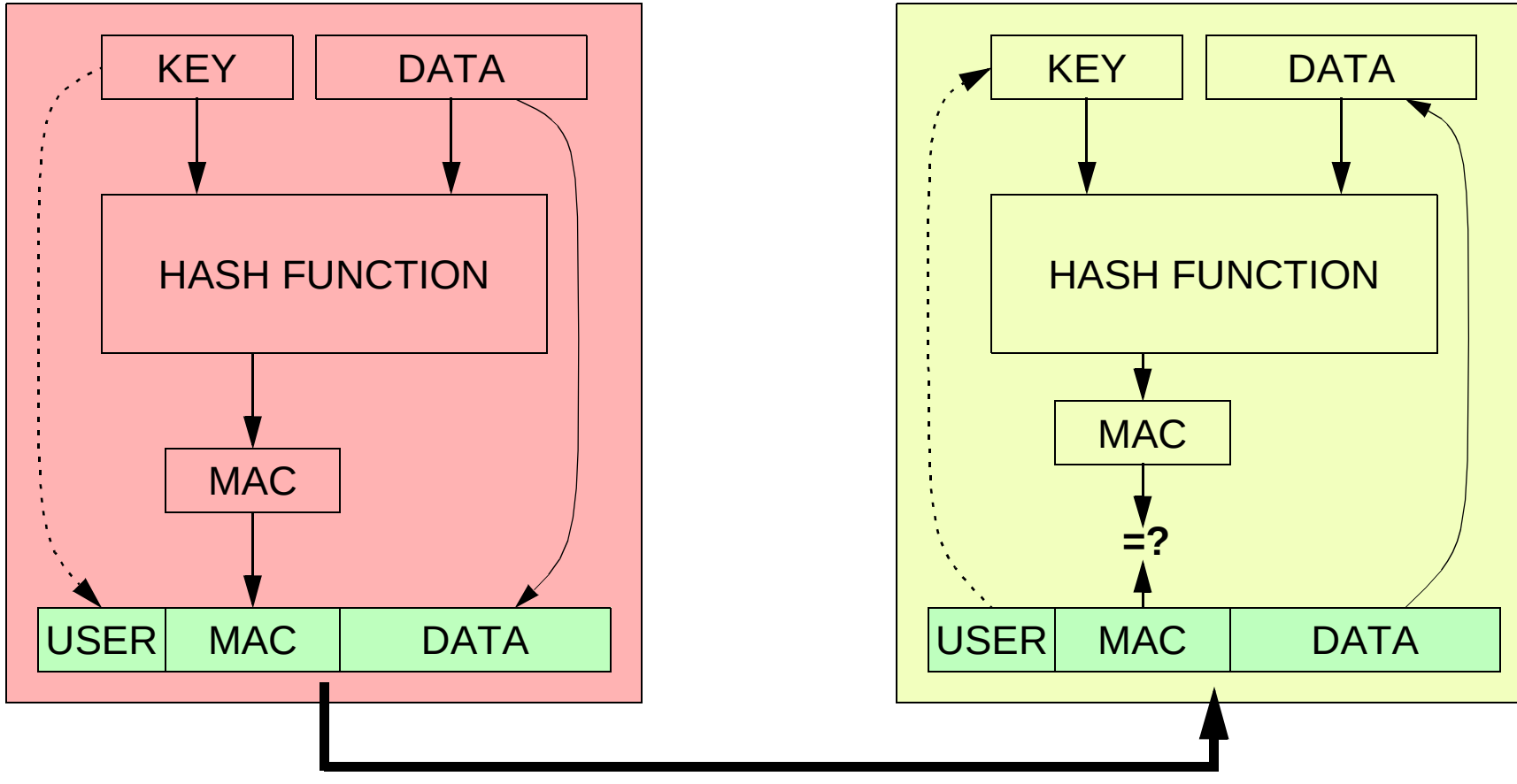


IDEA BEHIND DATA INTEGRITY AND AUTHENTICATION

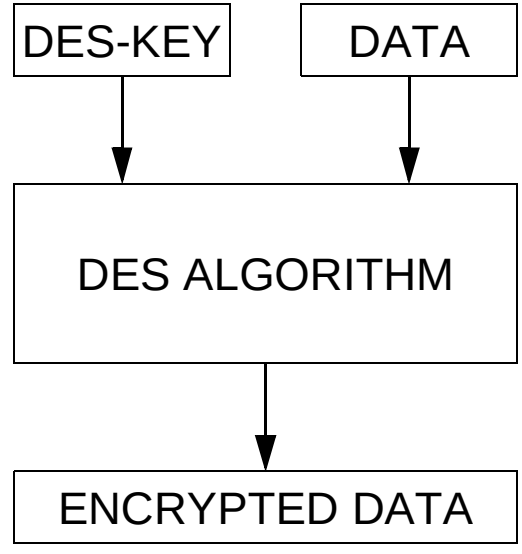


ADD THE MESSAGE AUTHENTICATION CODE (MAC) TO THE DATA
AND SEND THE RESULT

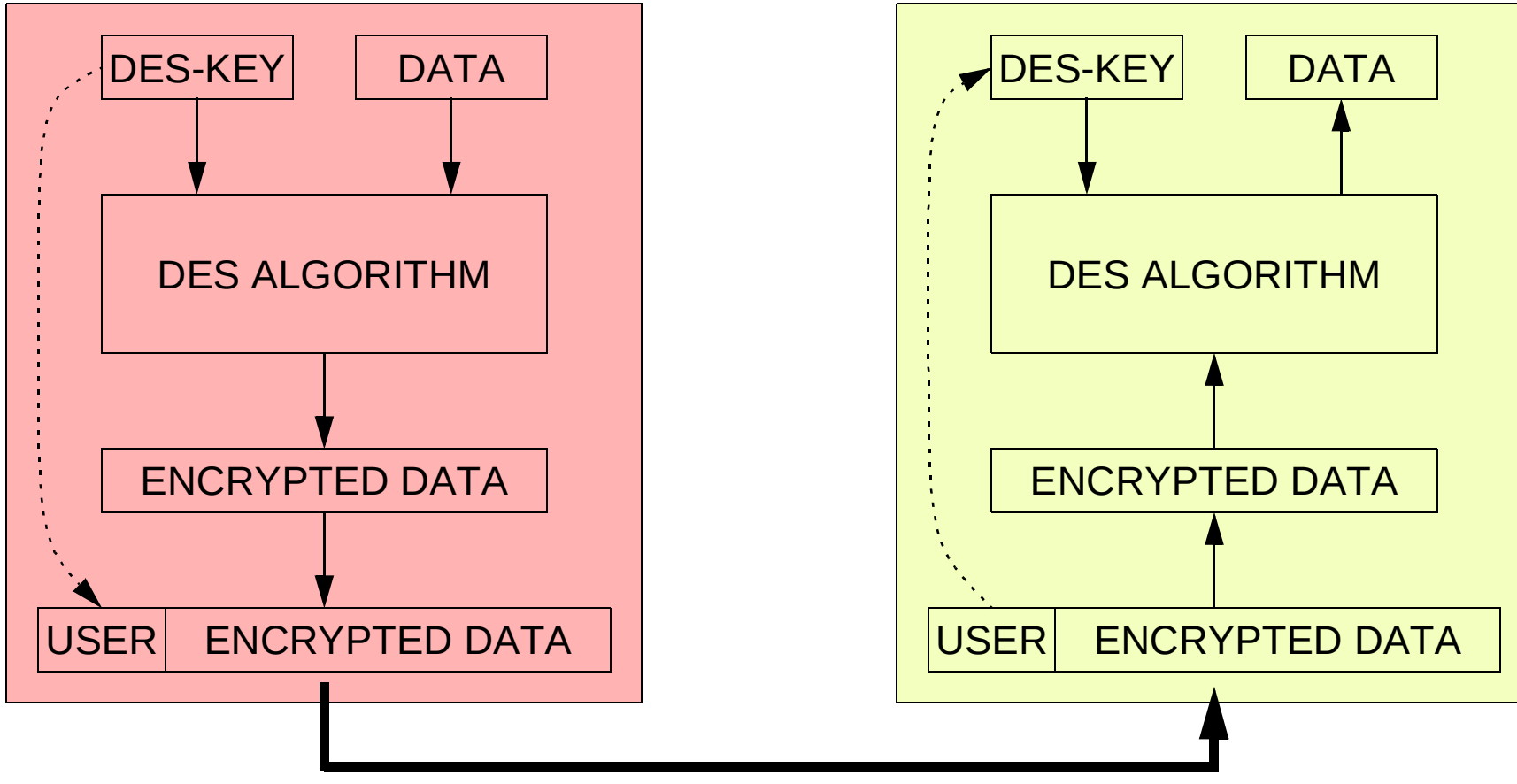
IDEA BEHIND AUTHENTICATION



IDEA BEHIND THE DATA CONFIDENTIALITY (DES)



IDEA BEHIND ENCRYPTION



VIEW BASED ACCESS CONTROL MODEL

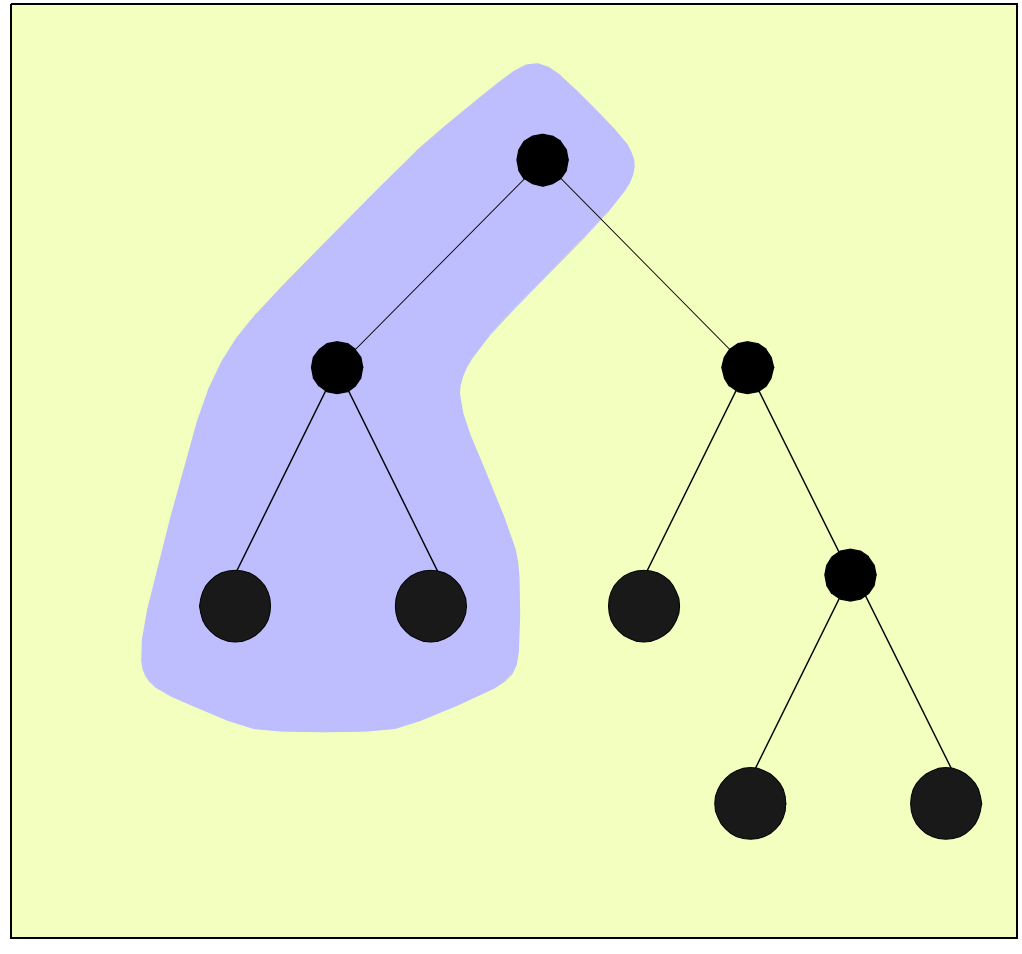
ACCESS CONTROL TABLE

MIB VIEWS

ACCESS CONTROL TABLES

MIB VIEW	ALLOWED OPERATIONS	ALLOWED MANAGERS	REQUIRED LEVEL OF SECURITY
Interface Table	SET	John	Authentication Encryption
Interface Table	GET / GETNEXT	John, Paul	Authentication
Systems Group	GET / GETNEXT	George	None
•••	•••	•••	•••
•••	•••	•••	•••
•••	•••	•••	•••
•••	•••	•••	•••

MIB VIEWS



SNMPv3 RFCs

SNMP ENTITY — **RFC 2571**

SNMP APPLICATIONS — **RFC 2573**

SNMP ENGINE

RFC 2572	RFC 2572	USM: RFC 2574	VACM: RFC 2575
DISPATCHER	MESSAGE PROCESSING SUBSYSTEM	SECURITY SUBSYSTEM	ACCESS CONTROL SUBSYSTEM

EXTENSIBLE AGENTS

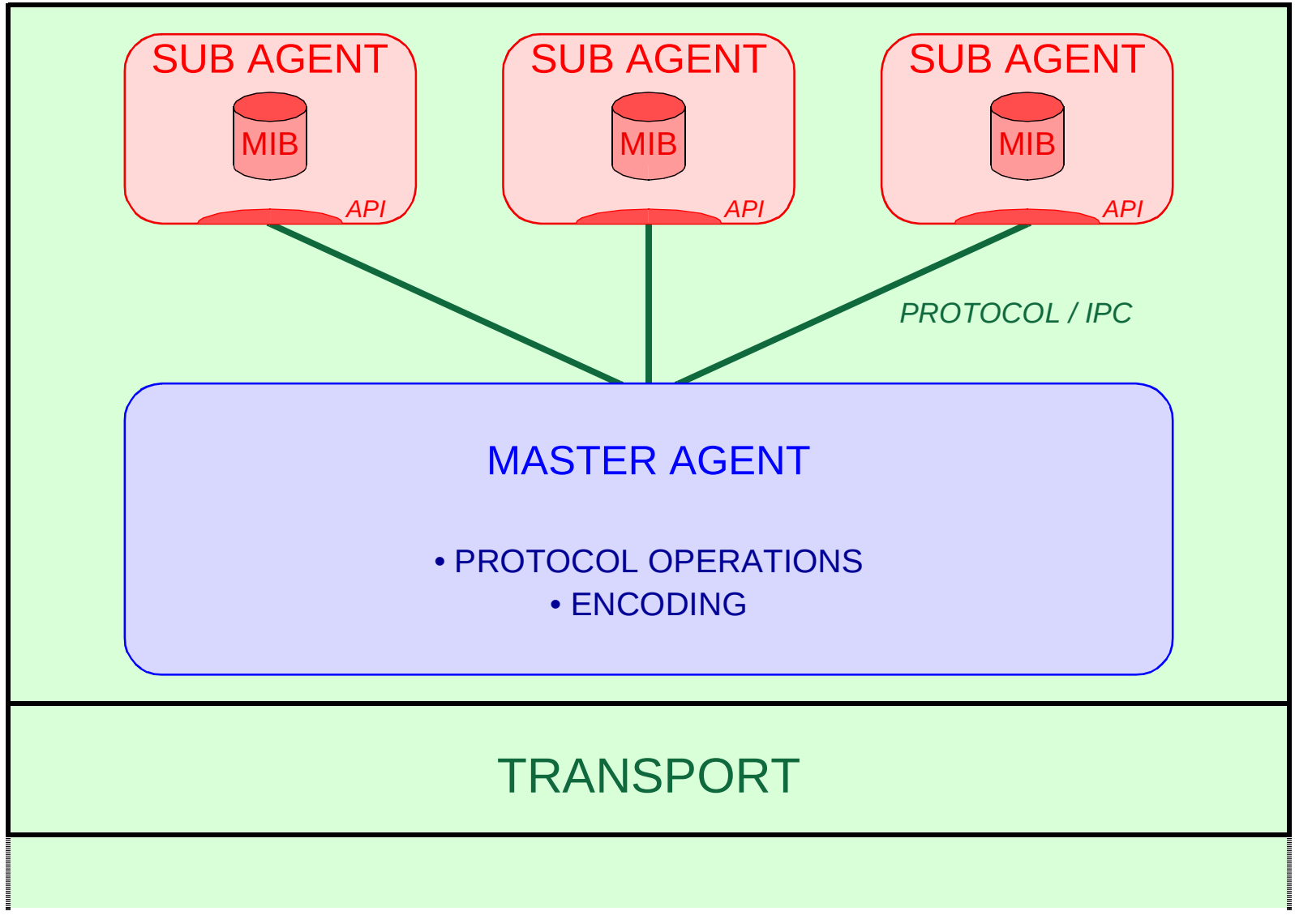
FACILITATE THE EXTENSION OF SNMP AGENTS
WITH NEW MIB MODULES

- SEPARATE SNMP PROTOCOL ENGINE
FROM MIB INSTRUMENTATION

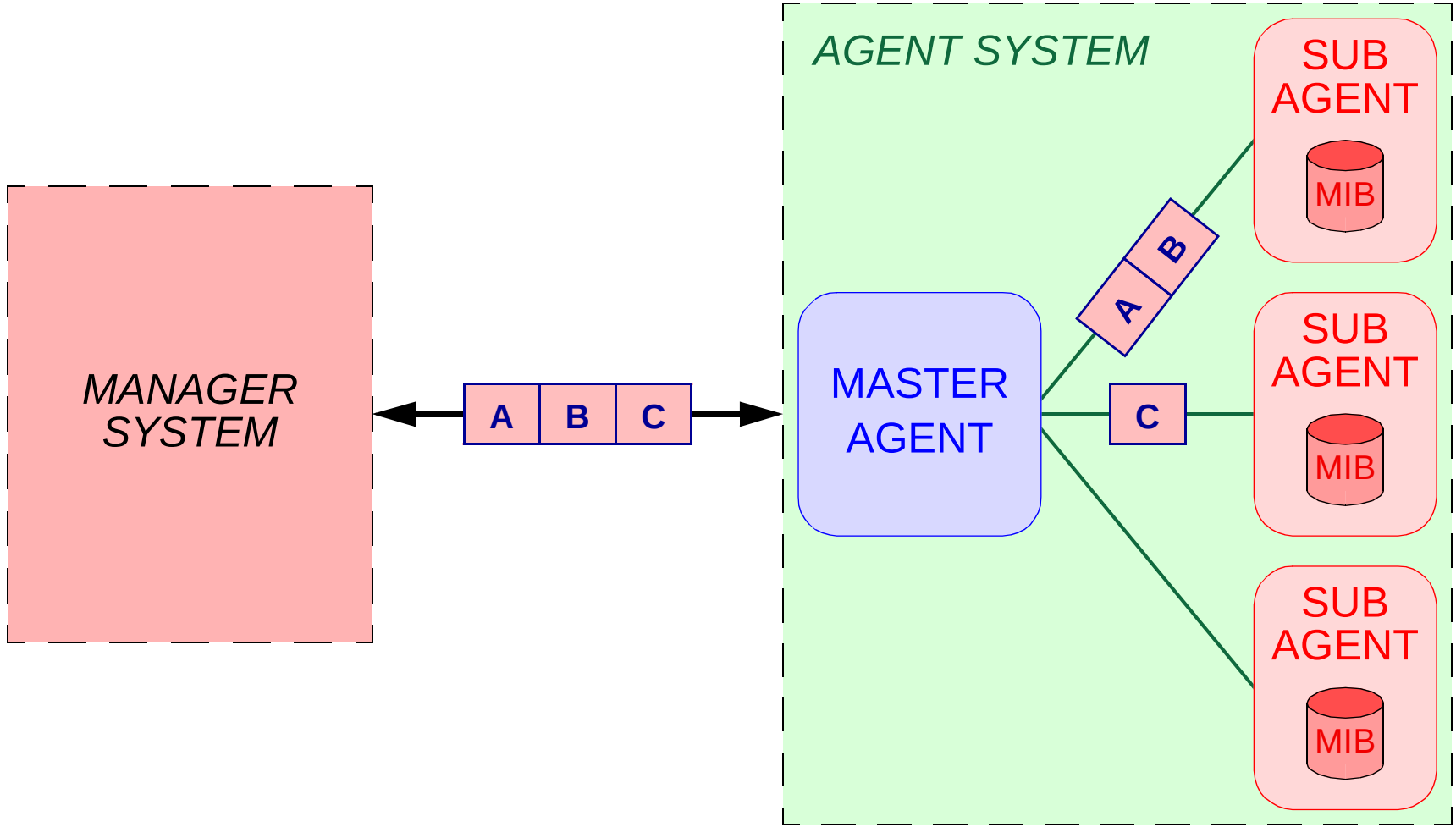
- ALLOW DYNAMIC ADDITION
OF NEW MIB MODULE IMPLEMENTATIONS

- EXTENSIBLE AGENTS SHOULD BE TRANSPARENT

BASIC STRUCTURE



SPLITTING OF VARBIND LIST



CHARACTERISTICS

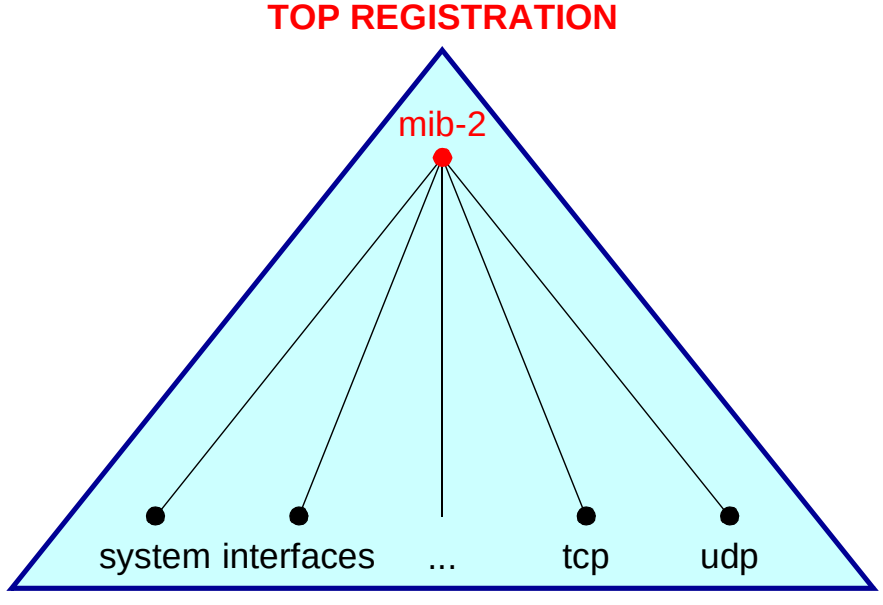
REQUIRES OID REGISTRATION:

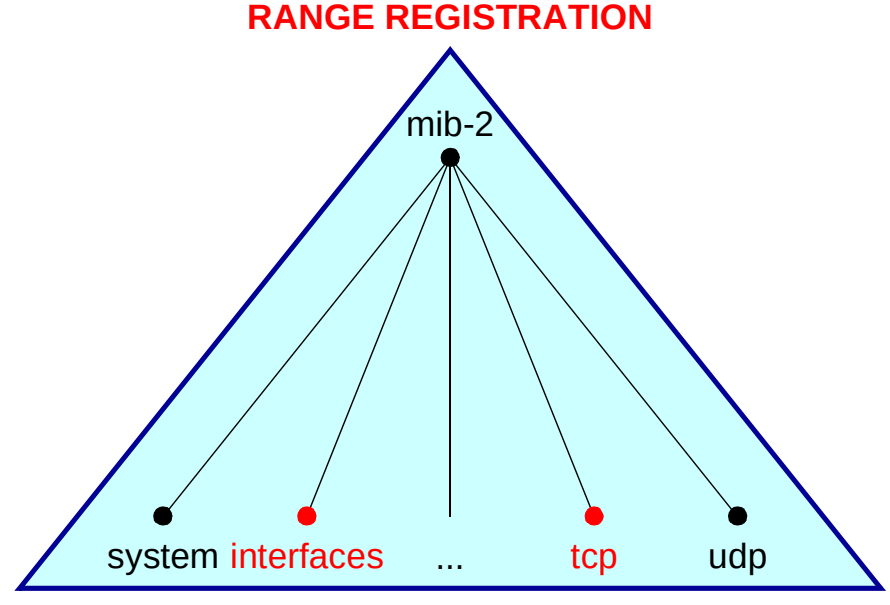
- TOP REGISTRATION

EXAMPLE: REGISTER(mib-2)

- RANGE REGISTRATION

EXAMPLE REGISTER(interfaces -> tcp)





POTENTIAL PROBLEMS

- TABLE ENTRIES MAY BE CREATED AND DELETED AT RUN-TIME

- ENTRIES OF A SINGLE TABLE MAY BE LOCATED IN DIFFERENT SUBAGENTS

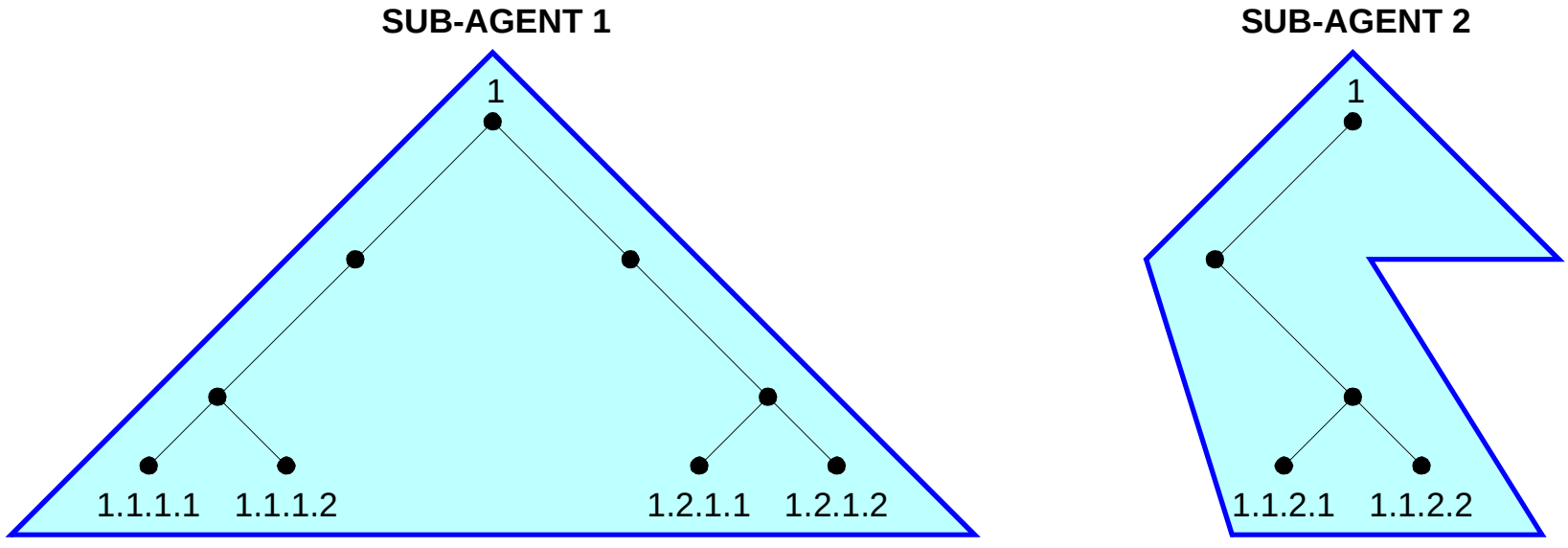
- DUPLICATED OIDs

- GAPS

- SETS

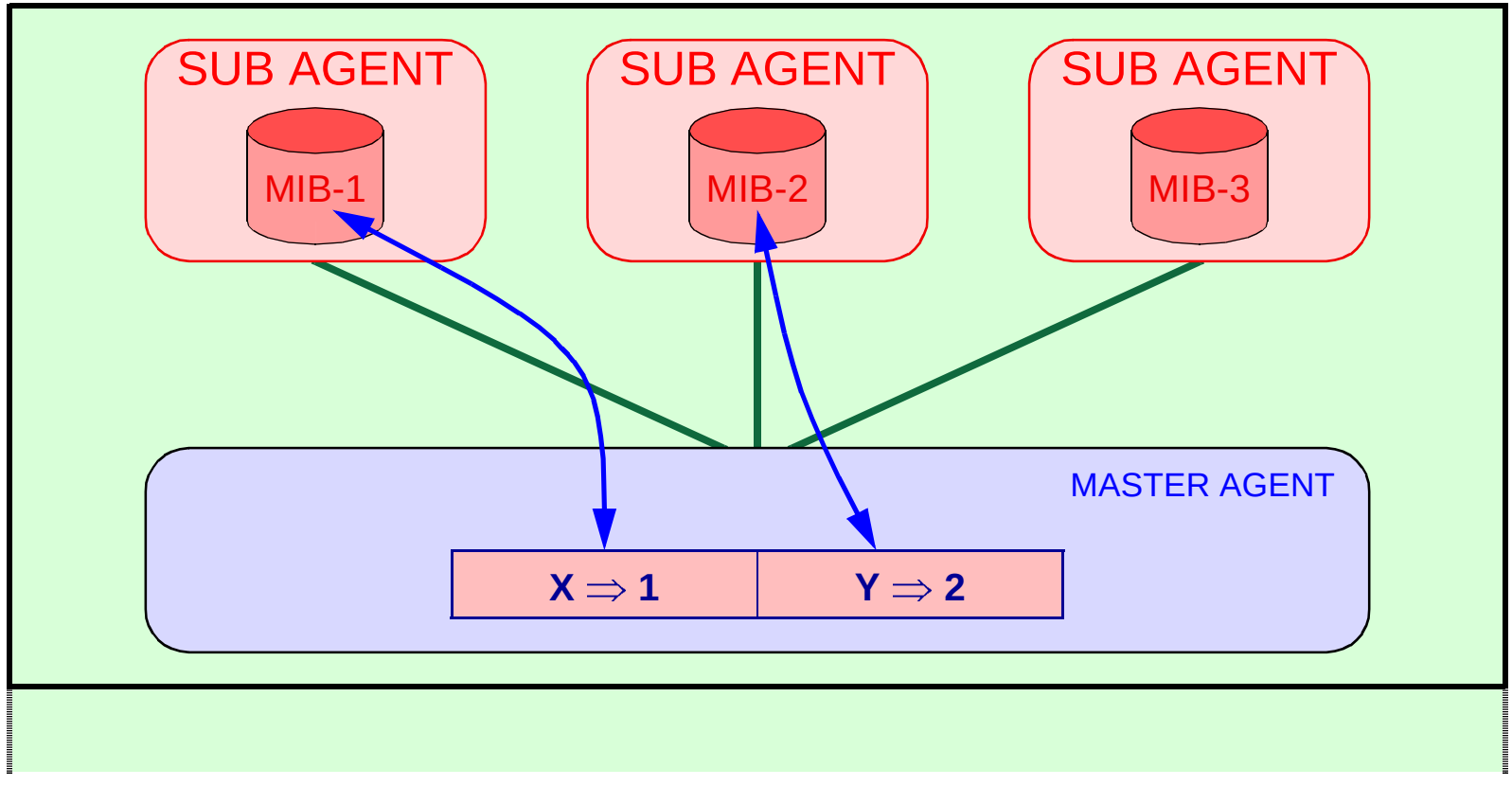
- sysUpTime

EXAMPLE: GAPS



GET-NEXT ...

SETS AND ATOMICITY



TRANSACTION-LIKE APPROACH

- TEST
- COMMIT
- UNDO / CLEAN

HISTORY

SMUX (1991: RFC 1227)
SNMP MULTIPLEXING PROTOCOL

DPI (1991-1994: RFC 1228 & RFC 1592)
DISTRIBUTED PROTOCOL INTERFACE

RESEARCH PROTOTYPES
FOR EXAMPLE: UNIVERSITY OF TWENTE - UT-SNMPv2

COMMERCIAL PRODUCTS
FOR EXAMPLE: SNMP RESEARCH - EMANATE
(ENHANCED MANAGEMENT AGENT THROUGH EXTENSIONS)

AGENTX (1998-2000: RFC2741 & RFC2742)

AGENTX

PROPOSED IETF STANDARD

- RFC 2741 & RFC 2742
- http:www.scguild.com/agentx/

HAS EFFICIENT MESSAGE FORMAT AND CODING

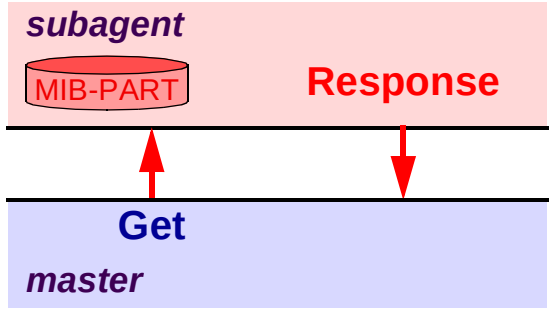
SUPPORTS

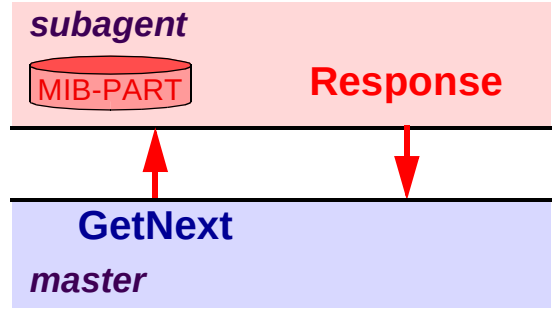
- SUBAGENTS IMPLEMENTING SEPARATE MIB MODULES
- SUBAGENTS IMPLEMENTING ROWS IN "SIMPLE TABLES"
- SUBAGENTS SHARING TABLES ALONG NON-ROW BORDERS

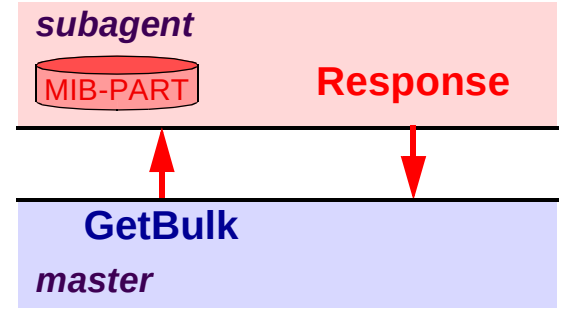
NON-GOALS

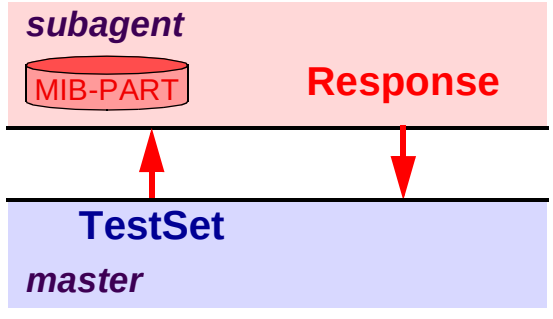
- SUBAGENTS SHARING "COMPLEX TABLES"
- SUBAGENT TO SUBAGENT COMMUNICATION

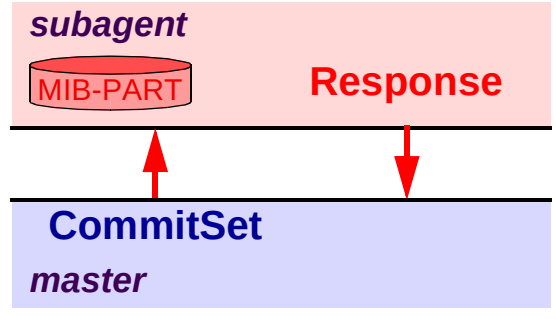
AGENTX - NORMAL PDUS

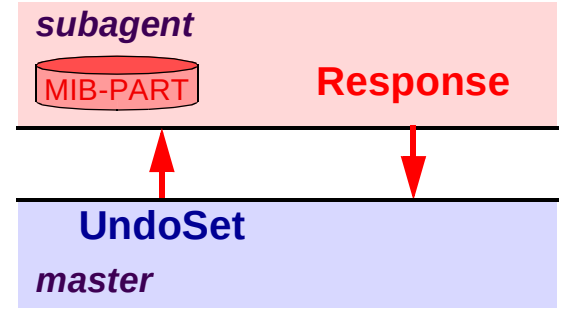


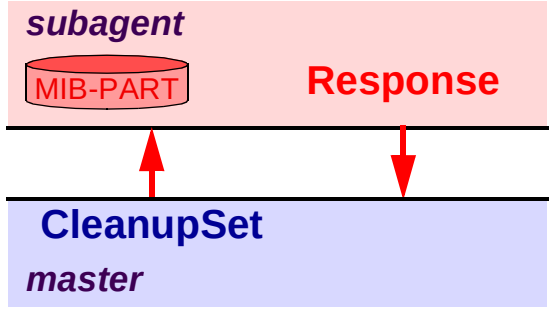


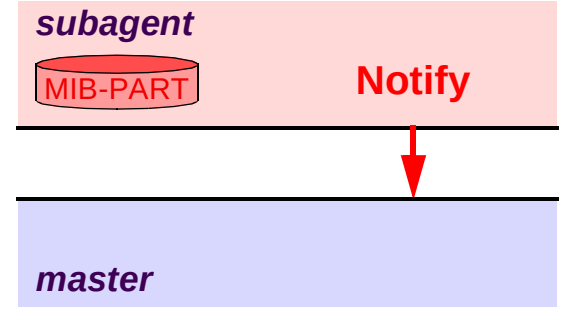




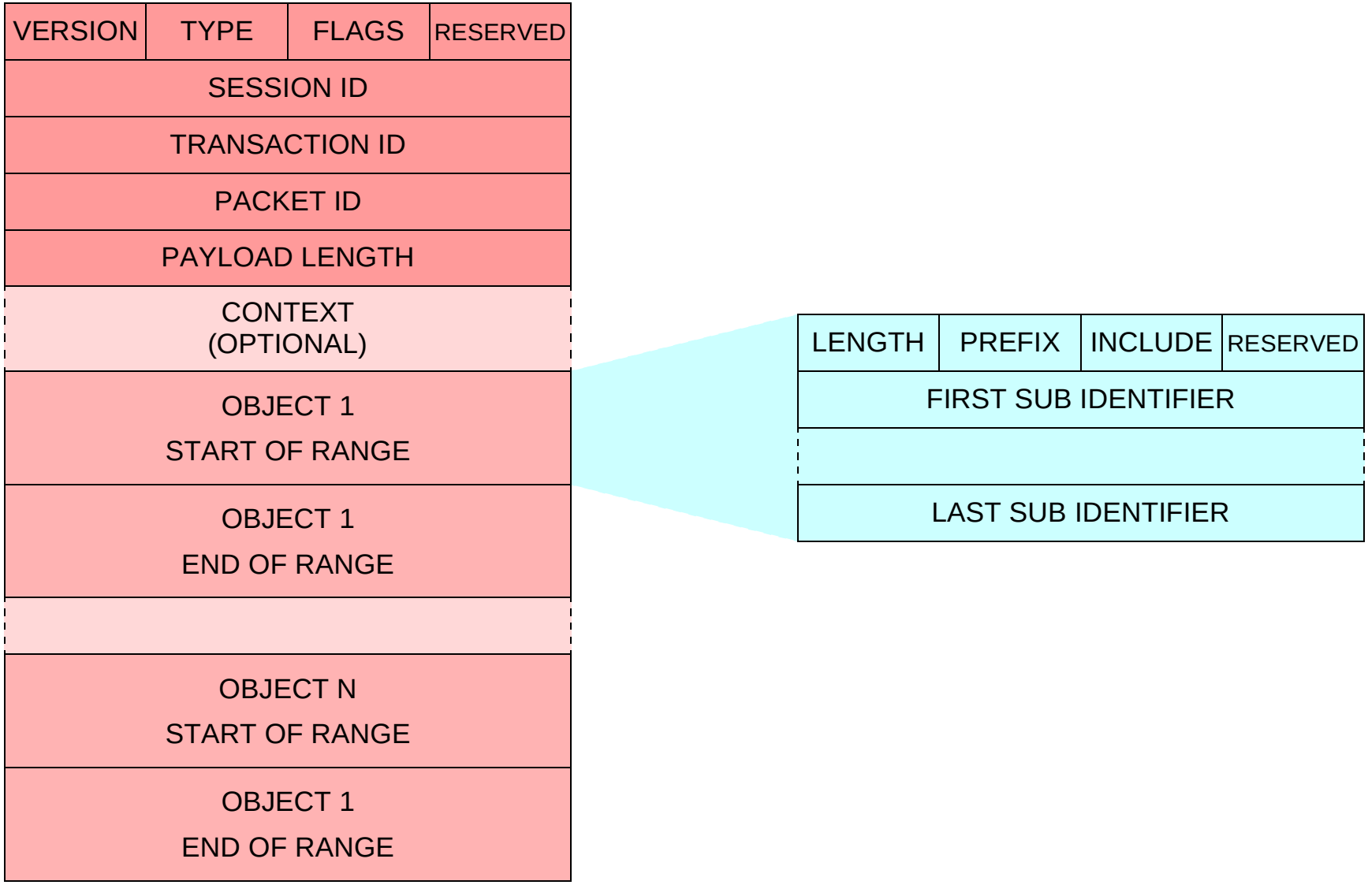








EXAMPLE: PDU FORMAT OF GetNext



AGENTX - ADMINISTRATIVE PDUS

Open
Close

AddAgentCaps
RemoveAgentCaps

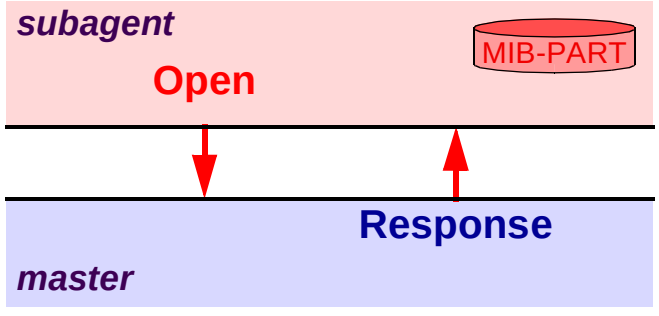
Register
Unregister

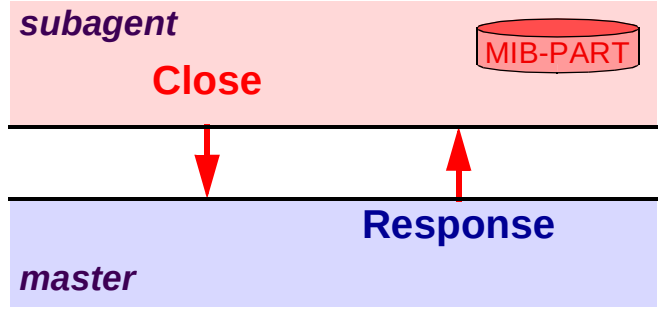
IndexAllocate
IndexDeallocate

Ping

Response

OPEN & CLOSE





TO ESTABLISH A SESSION

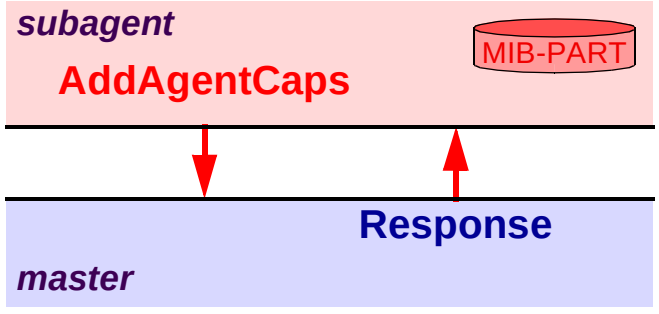
A UNIQUE sessionID IS ASSIGNED

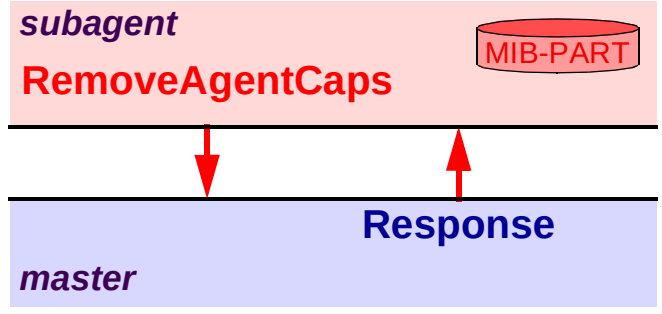
SUBAGENT SPECIFIES DEFAULT TIME-OUT

RESPONSES FROM MASTER ALWAYS INCLUDE sysUpTime

SESSION CAN BE CLOSED BY MASTER OR SUBAGENT

AGENT CAPABILITIES



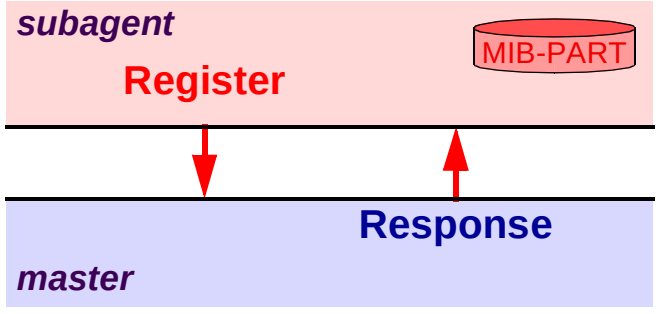


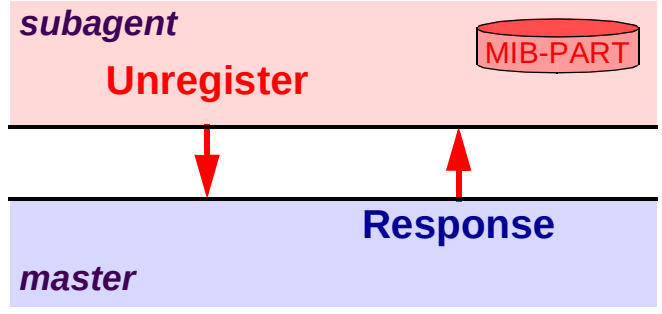
TO INFORM THE MASTER OF THE AGENT'S CAPABILITIES

CAPABILITIES ARE DEFINED AS:
- AN OBJECT ID
- A HUMAN READABLE STRING

THE CAPABILITIES ARE STORED IN THE sysORTable

REGISTRATION



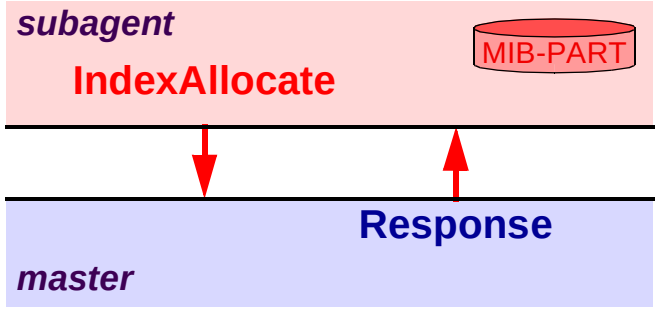


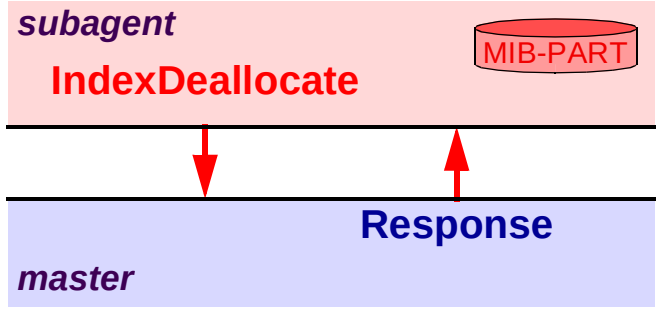
CHOICE BETWEEN:
- TOP REGISTRATION
- RANGE REGISTRATION

PRIORITY CAN BE SPECIFIED
- TO DETERMINE THE AUTHORITATIVE SUBAGENT

TIME-OUT CAN BE SPECIFIED

INDEXALLOCATION





TO ALLOCATE ONE OR MORE TABLE ROWS

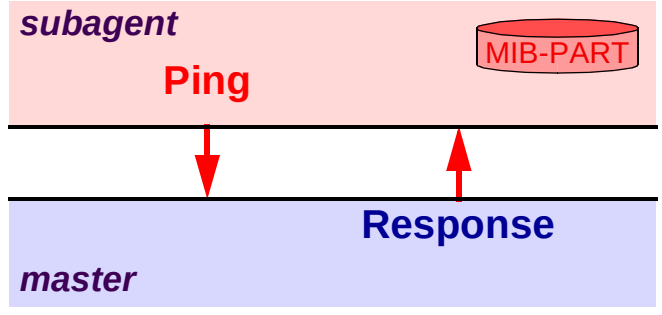
SUBAGENT REQUESTS ALLOCATION OF:

- A SPECIFIC INDEX VALUE
- AN INDEX VALUE THAT IS NOT CURRENTLY ALLOCATED
- AN INDEX VALUE THAT HAS NEVER BEEN ALLOCATED

MASTER AGENT MAINTAINS DATABASE

AFTER ALLOCATION REGISTRATION IS STILL NEEDED

PING



TO MONITOR IF THE MASTER AGENT IS STILL ABLE TO RECEIVE AND SEND AGENTX PDUs

DISTRIBUTED MANAGEMENT

THREE APPROACHES ARE BEING DEFINED

MIB BASED
- EXPRESSION MIB
- EVENT MIB
- NOTIFICATION LOG MIB

SCRIPT BASED
- SCRIPT MIB
- SCHEDULE MIB

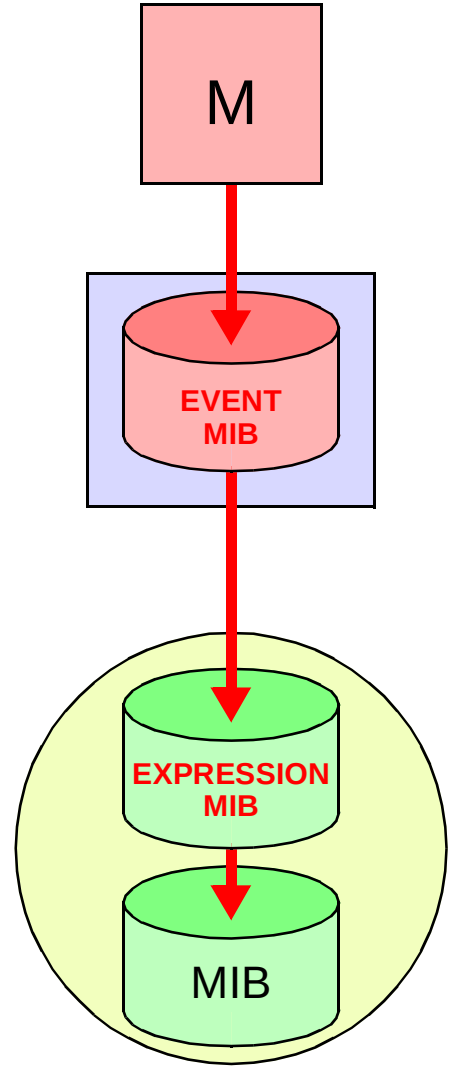
REMOTE OPERATIONS BASED
- REMOTE OPERATIONS MIB

EXPRESSION AND EVENT MIB

TOP LEVEL MANAGER

INTERMEDIATE LEVEL MANAGER

AGENT



EXPRESSION AND EVENT MIB: CHARACTERISTICS

• STANDARD MIB APPROACH

• RESEMBLES THE OLD SNMPv2 M2M MIB

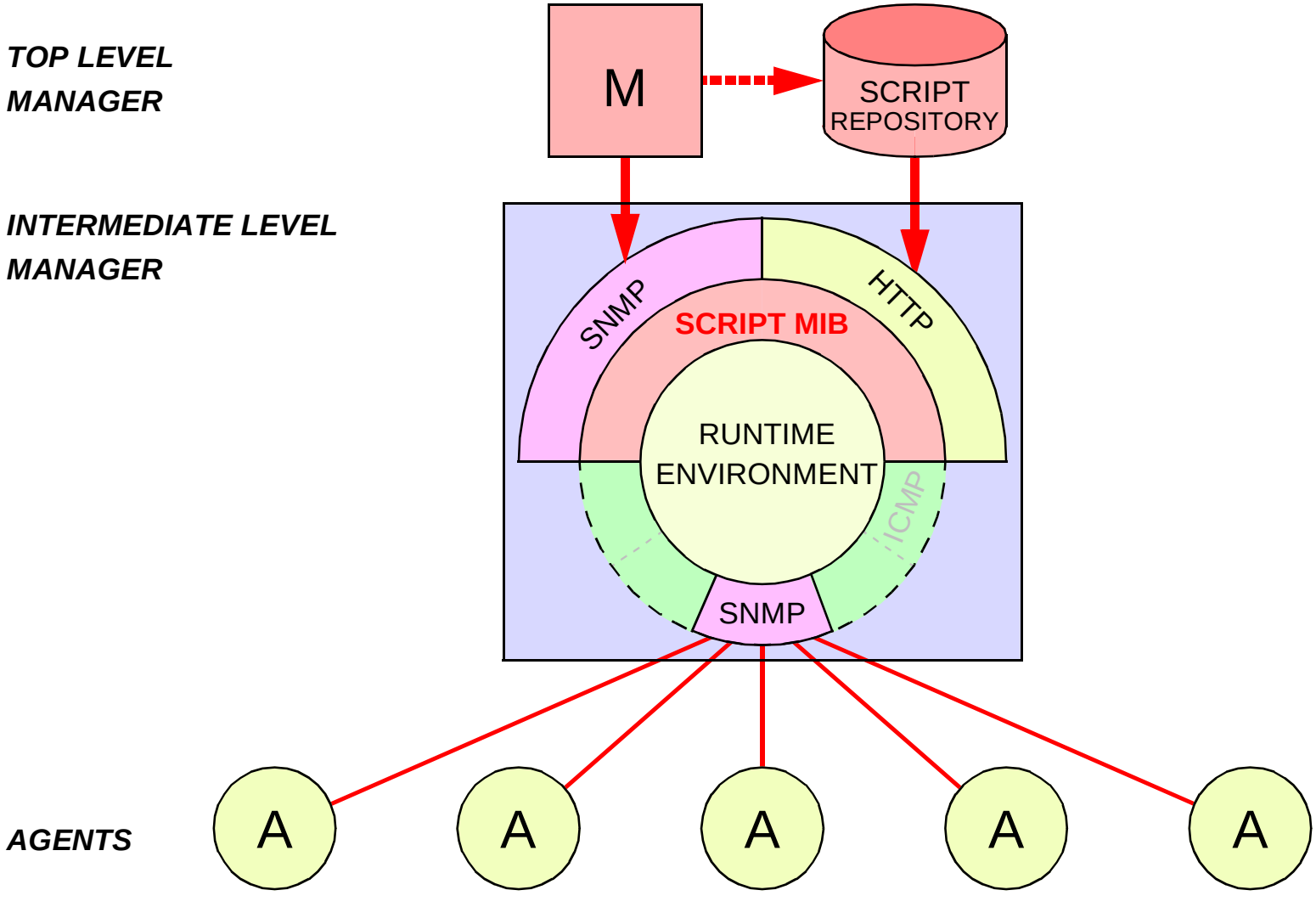
EXPRESSION MIB:

• INPUT ARE (WILDCARDED) VARIABLES OF A (LOCAL) MIB
• OPERATES ON ABSOLUTE AS WELL AS DELTA VALUES
• RICH SET OF EXPRESSIONS
• THE OUTPUT IS STORED IN THE *VALUE TABLE*
• THIS TABLE MAY SERVE AS INPUT FOR OTHER EXPRESSIONS

EVENT MIB:

• INPUT ARE VARIABLES OF A (REMOTE) MIB
• TRIGGERS ON CHANGES, OR TRESHOLD CROSSING
• GENERATES A NOTIFICATION OR SET OPERATION

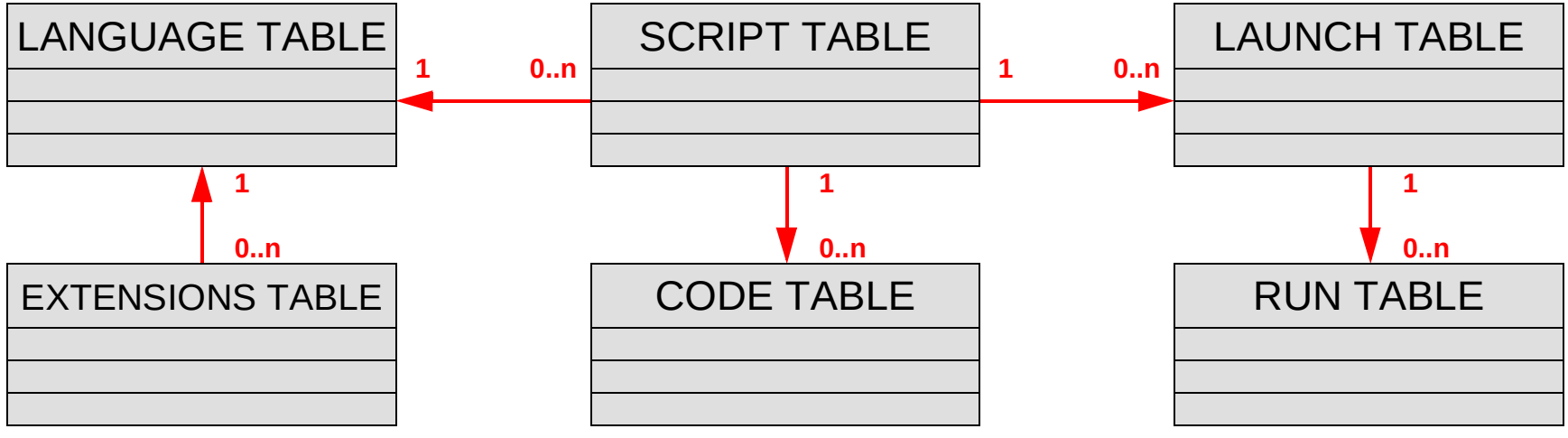
SCRIPT MIB


TOP LEVEL MANAGER
INTERMEDIATE LEVEL MANAGER
AGENTS
M
SCRIPT REPOSITORY
SNMP
SCRIPT MIB
HTTP
RUNTIME ENVIRONMENT
ICMP
SNMP
A
A
A
A
A

SCRIPT MIB: CHARACTERISTICS

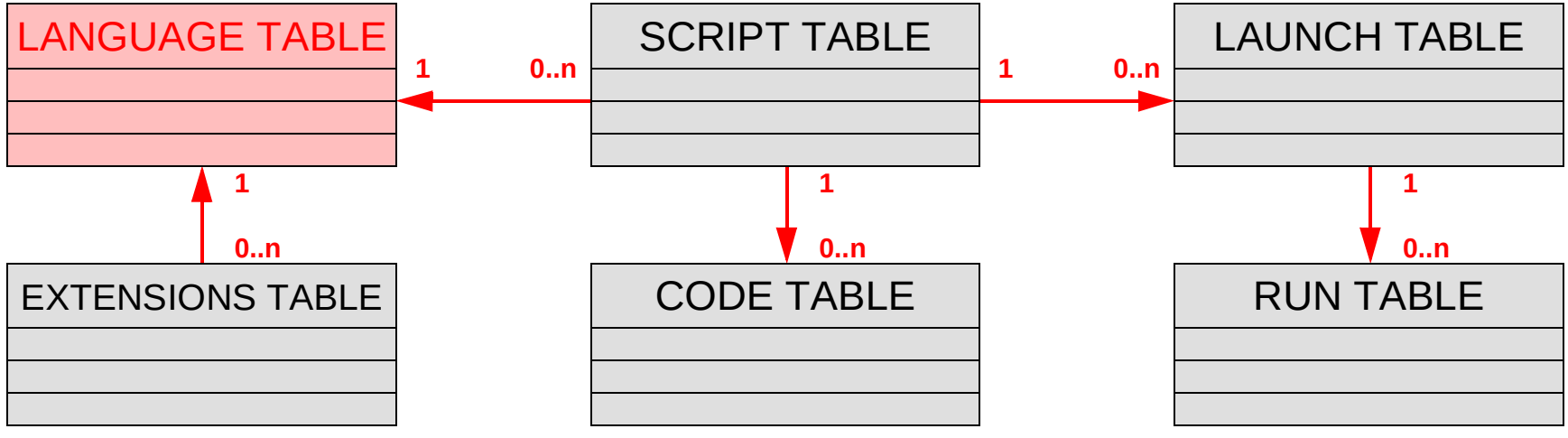
- FUNCTIONALITY CAN BE DEFINED AT RUN-TIME
- POWERFUL AUTONOMOUS ACTIONS
- MAY BE EASIER TO OPERATE FOR THE TOP-LEVEL MANAGER
- PROTECTION MECHANISMS NECESSARRY
- DIFFERENT SCRIPT LANGUAGES

SCRIPT MIB: STRUCTURE



CONSISTS OF 6 TABLES

SCRIPT MIB: LANGUAGE TABLE

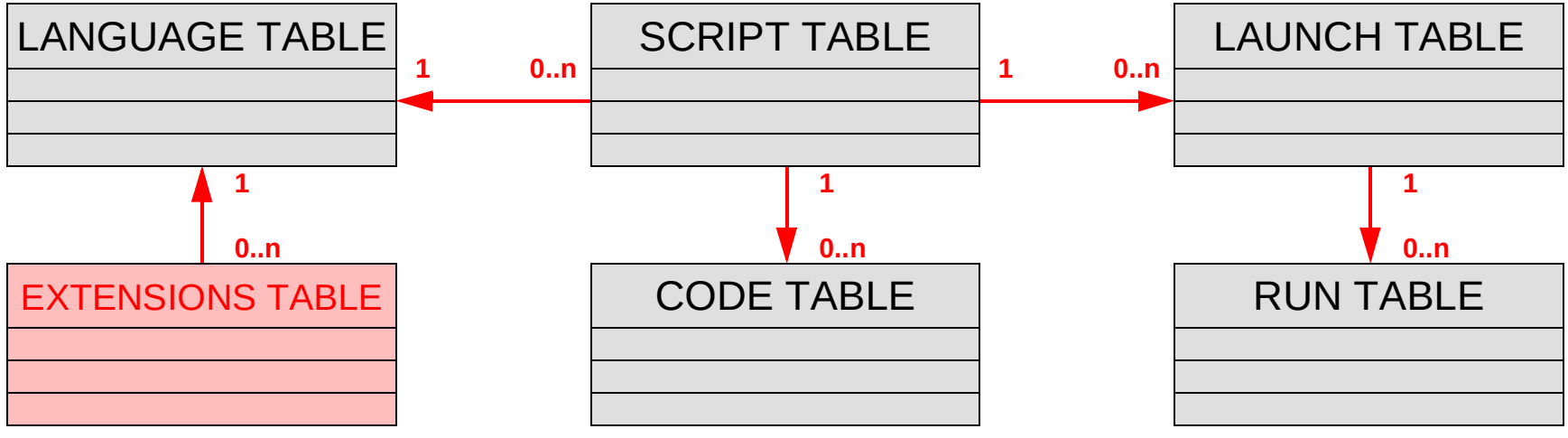


DEFINES THE LANGUAGES THIS SYSTEM SUPPORTS

- AN OID TO INDICATE THE LANGUAGE
- THE VERSION
- AN OID TO INDICATE THE VENDOR
- THE REVISION
- A DESCRIPTION

TABLE IS READ ONLY

SCRIPT MIB: EXTENSIONS TABLE

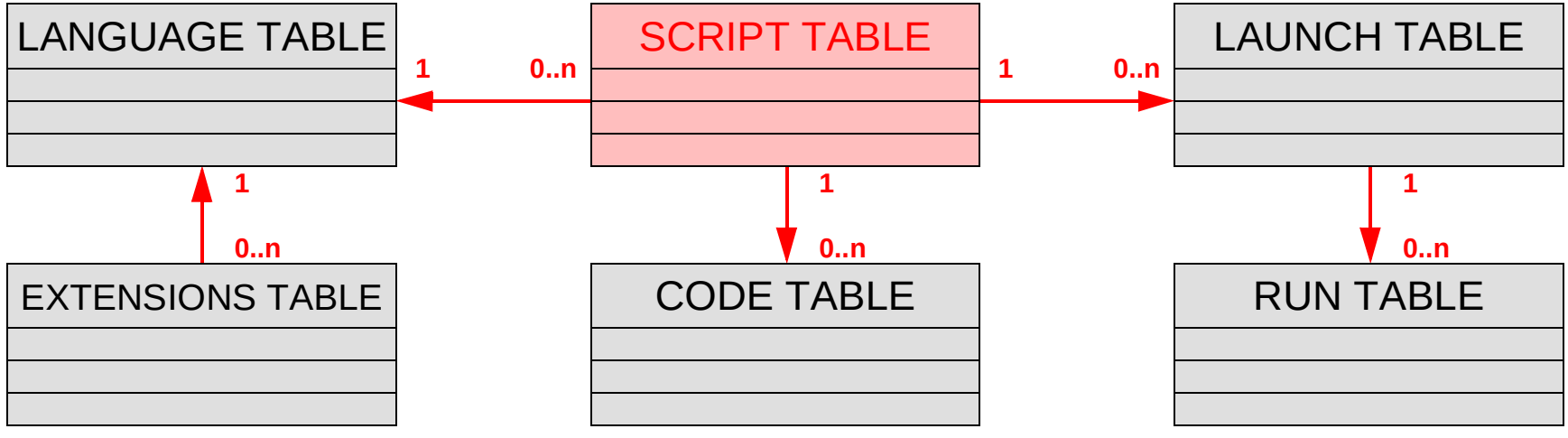


DEFINES THE EXTENSIONS FOR EACH LANGUAGE

- AN OID TO INDICATE THE EXTENSION
- THE VERSION
- AN OID TO INDICATE THE VENDOR
- THE REVISION
- A DESCRIPTION

TABLE IS READ ONLY

SCRIPT MIB: SCRIPT TABLE

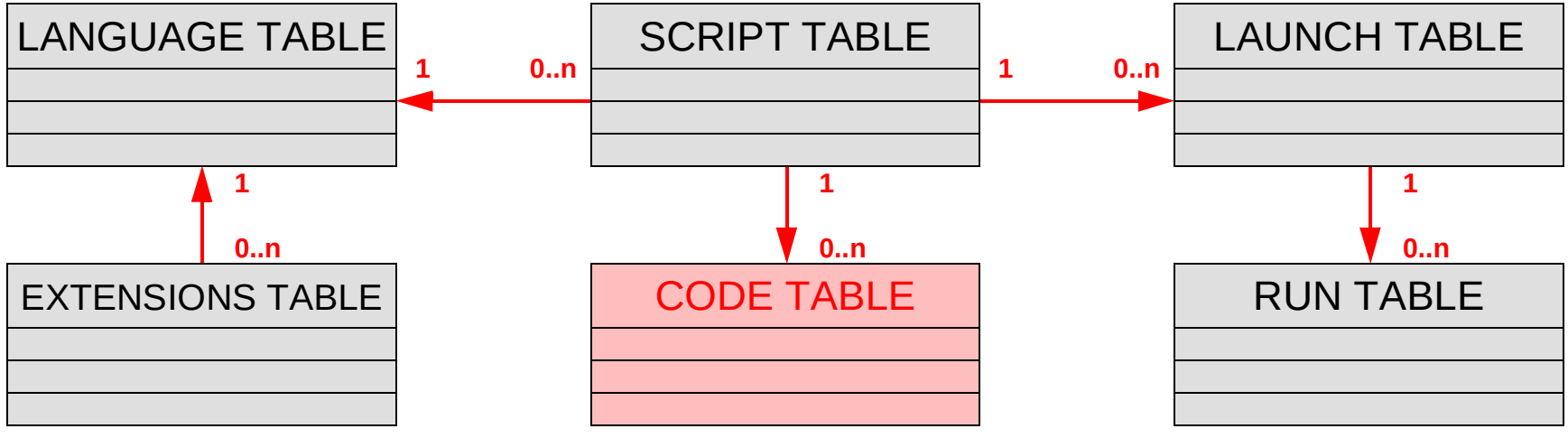


LISTS ALL SCRIPTS KNOWN TO THE SYSTEM

ALLOWS TO:

- DOWNLOAD SCRIPTS FROM A URL (PULL MODEL)
- READ SCRIPTS FROM LOCAL NON-VOLATILE STORAGE
- STORE SCRIPTS IN LOCAL NON-VOLATILE STORAGE
- DELETE SCRIPTS FROM LOCAL NON-VOLATILE STORAGE
- LIST PERMANENT SCRIPTS (THAT CAN NOT BE CHANGED OR REMOVED)
- READ AND MODIFY THE SCRIPT STATUS (ENABLED, DISABLED, EDITING)

SCRIPT MIB: CODE TABLE



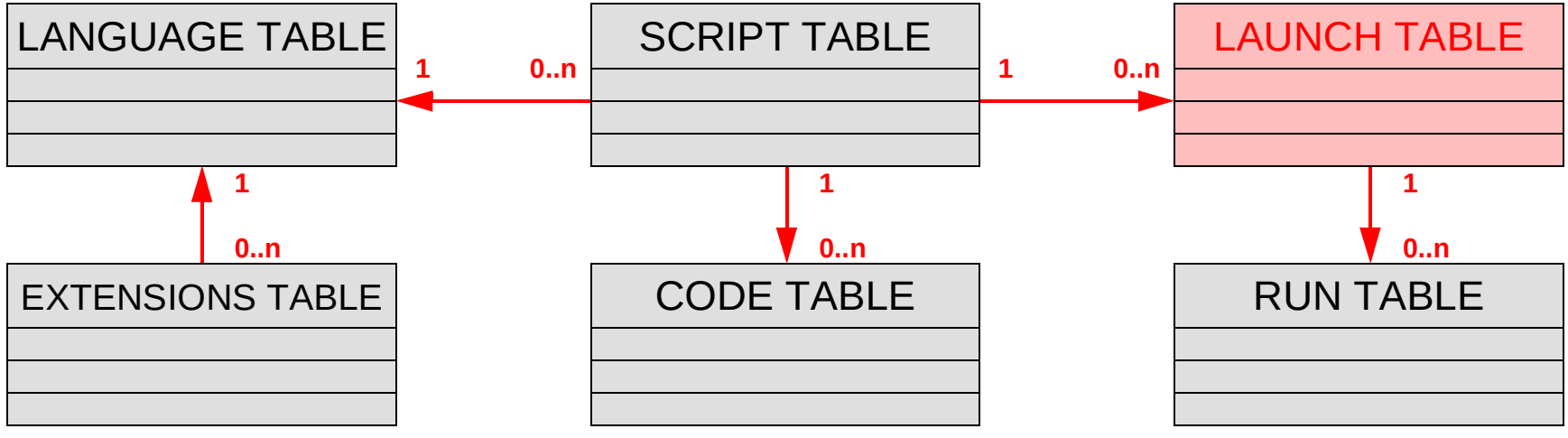
LISTS THE CODE OF A SCRIPT

ALLOWS TO:

- DOWNLOAD SCRIPTS VIA SNMP (PUSH MODEL)
- MODIFY SCRIPTS VIA SNMP (EDITING)

IMPLEMENTATION IS OPTIONAL

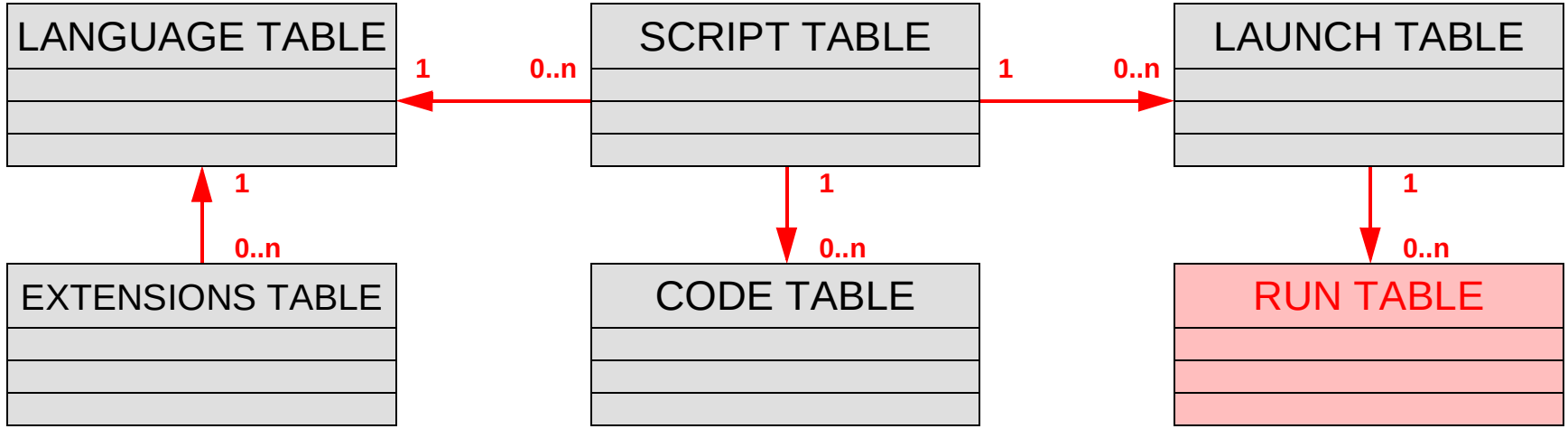
SCRIPT MIB: LAUNCH TABLE



ALLOWS TO:

- ASSOCIATE A SCRIPT WITH A 'PERSON' WHO INVOKES EXECUTION
- PROVIDE ARGUMENTS AND PARAMETERS FOR SCRIPT INVOCATION
- INVOKE SCRIPTS WITH A SINGLE SET OPERATION
- CONTROL THE NUMBER OF ACTIVE INVOCATIONS
- CONTROL THE TOTAL NUMBER OF INVOCATIONS

SCRIPT MIB: RUN TABLE



ALLOWS TO:

- RETRIEVE STATUS INFORMATION FROM RUNNING SCRIPTS
- CONTROL RUNNING SCRIPTS (SUSPEND, RESUME, ABORT)
- RETRIEVE RESULTS FROM RECENTLY TERMINATED SCRIPTS
- CONTROL THE REMAINING MAXIMUM LIFETIME OF A RUNNING SCRIPT
- CONTROL HOW LONG SCRIPT RESULTS ARE ACCESSIBLE

SCHEDULE MIB

PERFORMS SET OPERATIONS

FOR EXAMPLE ON THE SCRIPT MIB

- TARGET MUST BE Integer32

ON A PERIODIC OR CALENDER DRIVEN BASE

REMOTE OPERATIONS MIB

PING MIB

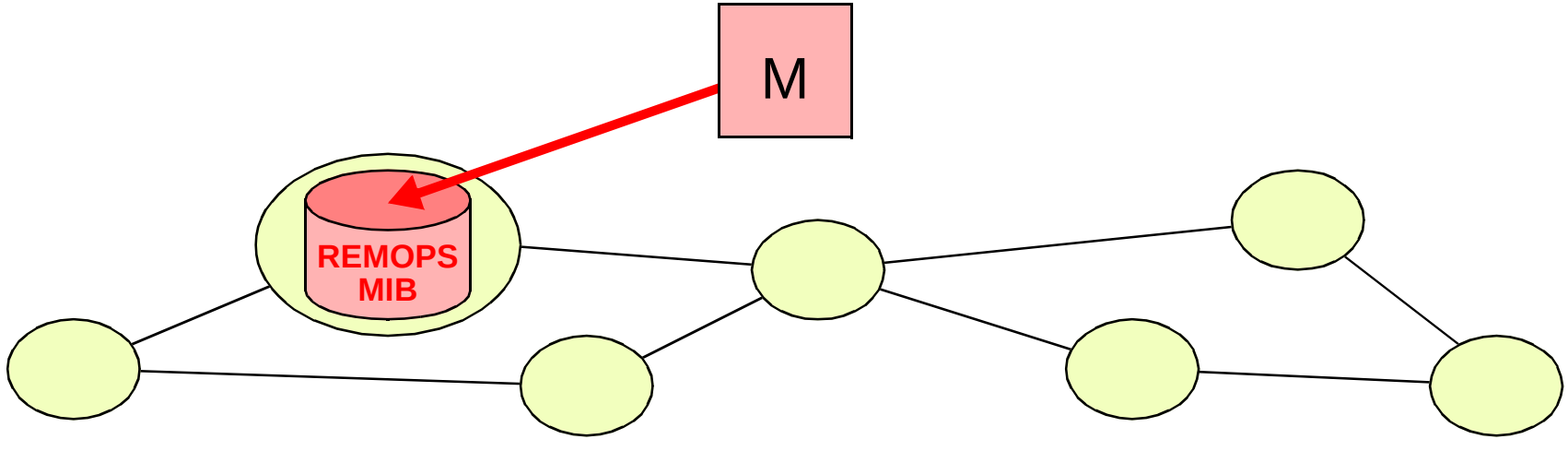
• TO PERFORM PING FROM A REMOTE HOST

TRACEROUTE MIB

• TO PERFORM TRACEROUTE FROM A REMOTE HOST

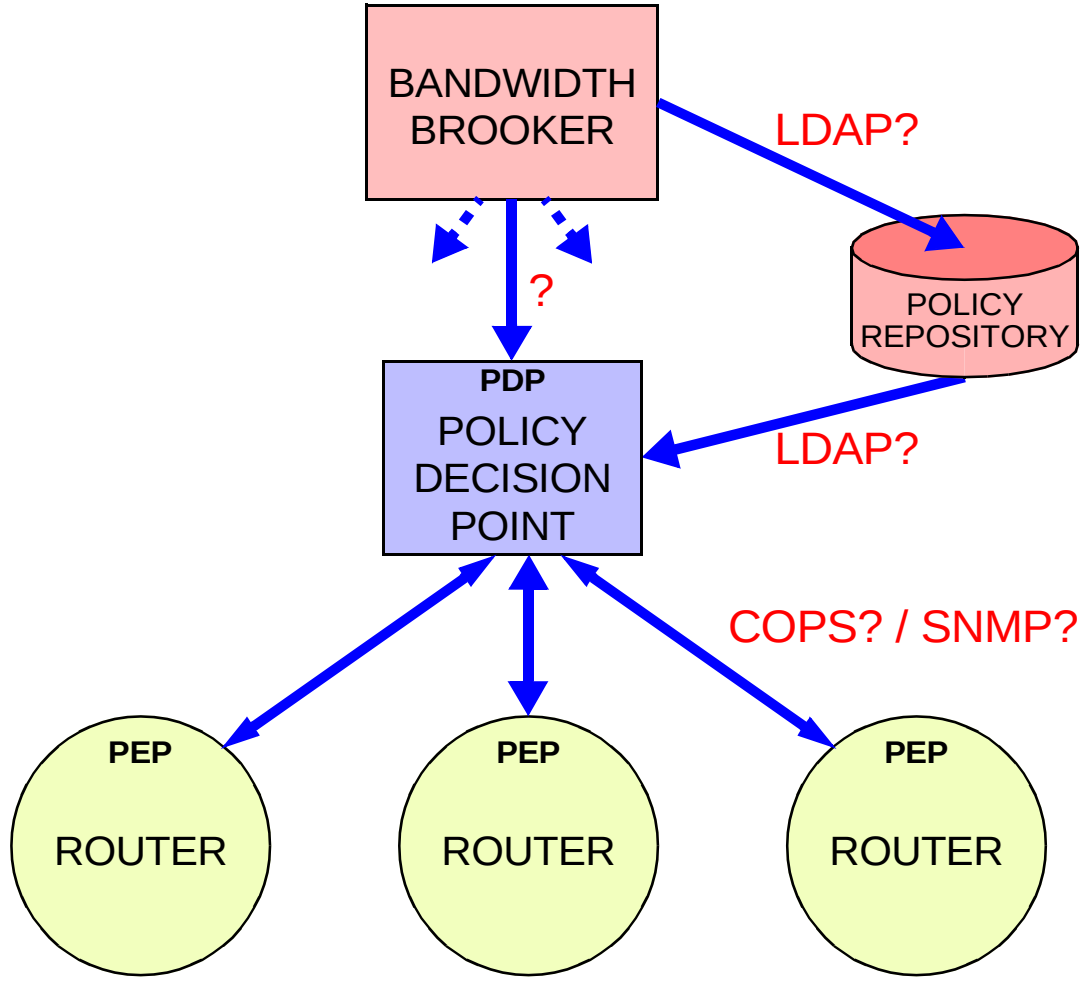
NAME LOOKUP MIB

• TO PERFORM NAME LOOKUP FROM A REMOTE HOST



NEW DEVELOPMENTS

POLICY BASED MANAGEMENT



COPS VERSUS SNMP

COPS:

- SPECIAL CASE OF CONFIGURATION MANAGEMENT
- HIGHER LEVEL OBJECTS THAN USUAL WITH SNMP
- POLICY INFORMATION BASE (PIB)
- SINGLE OPERATION TO ADD OR DELETE TABLE ROWS
- RELIABLE COMMUNICATION BETWEEN PDP AND PEP (BECAUSE OF TCP)
- EACH PEP IS CONNECTED TO SINGLE PDP

SNMP:

- INTEGRATED APPROACH TO MANAGEMENT
- POLICIES CAN BE DEFINED WITHIN MIBs
- EACH PEP MAY BE CONNECTED TO MULTIPLE PDPs

WWW SERVERS

- IETF
  http://www.ietf.org/

- The SimpleWeb
  http://www.simpleweb.org/

- The Simple Times
  http://www.simple-times.org/

- The Smurfland NM Web Server
  http://netman.cit.buffalo.edu/

BOOKS

• W. Stallings
SNMP, SNMPv2, SNMPv3 and RMON1 and 2
Third edition, Addison-Wesley, 1999
ISBN: 0-201-48534-6

• D. Zeltserman
A Practical Guide to SNMPv3 and Network Management
Prentice Hall, 1999
ISBN: 0-13-021453-1

• D. Perkins, E. McGinnis
Understanding SNMP MIBs
Prentice Hall, 1996
ISBN: 0-13-437708-7

ARTICLES

The Simple Times: *Special issue on Agent Extensibility*
Issue 4-2, April 1996

The Simple Times: *Special issue on SNMPv3*
Issue 5-1, December 1997

The Simple Times: *An overview of the AgentX Protocol*
Issue 6-1, March 1998

The Simple Times: *Special issue on SNMPv3*
Issue 7-2, November 1999

William Stallings,
Security Comes to SNMP: The New SNMPv3 Proposed Internet Standards
The Protocol Journal, December 1998

William Stallings,
SNMPv3: A Security Enhancement for SNMP,
IEEE Communications Survey, Q4, 1998