TUTORIAL

SNMP:
STATUS AND APPLICATION
FOR
LAN/MAN MANAGEMENT

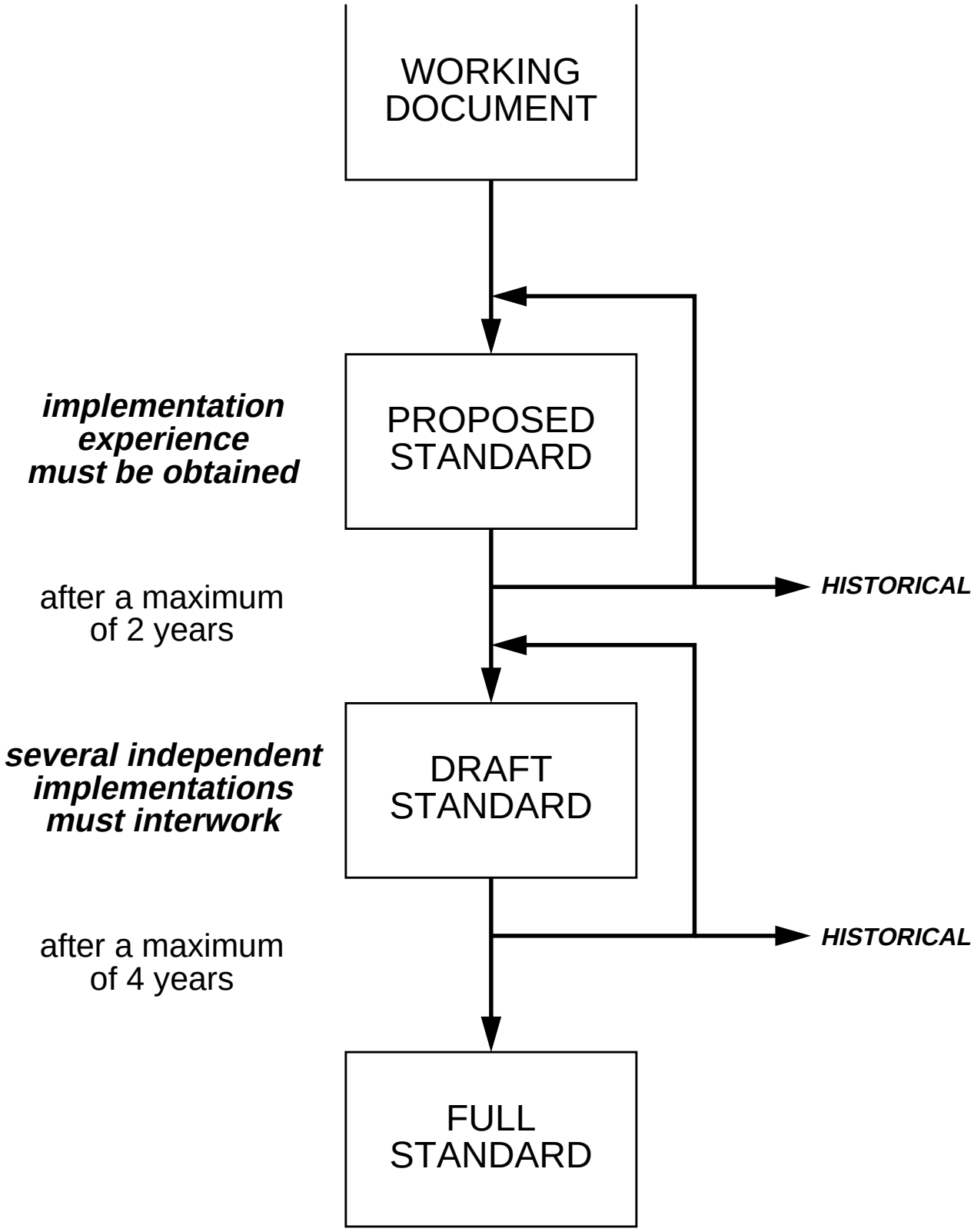
9 July 1996

Aiko Pras
pras@cs.utwente.nl

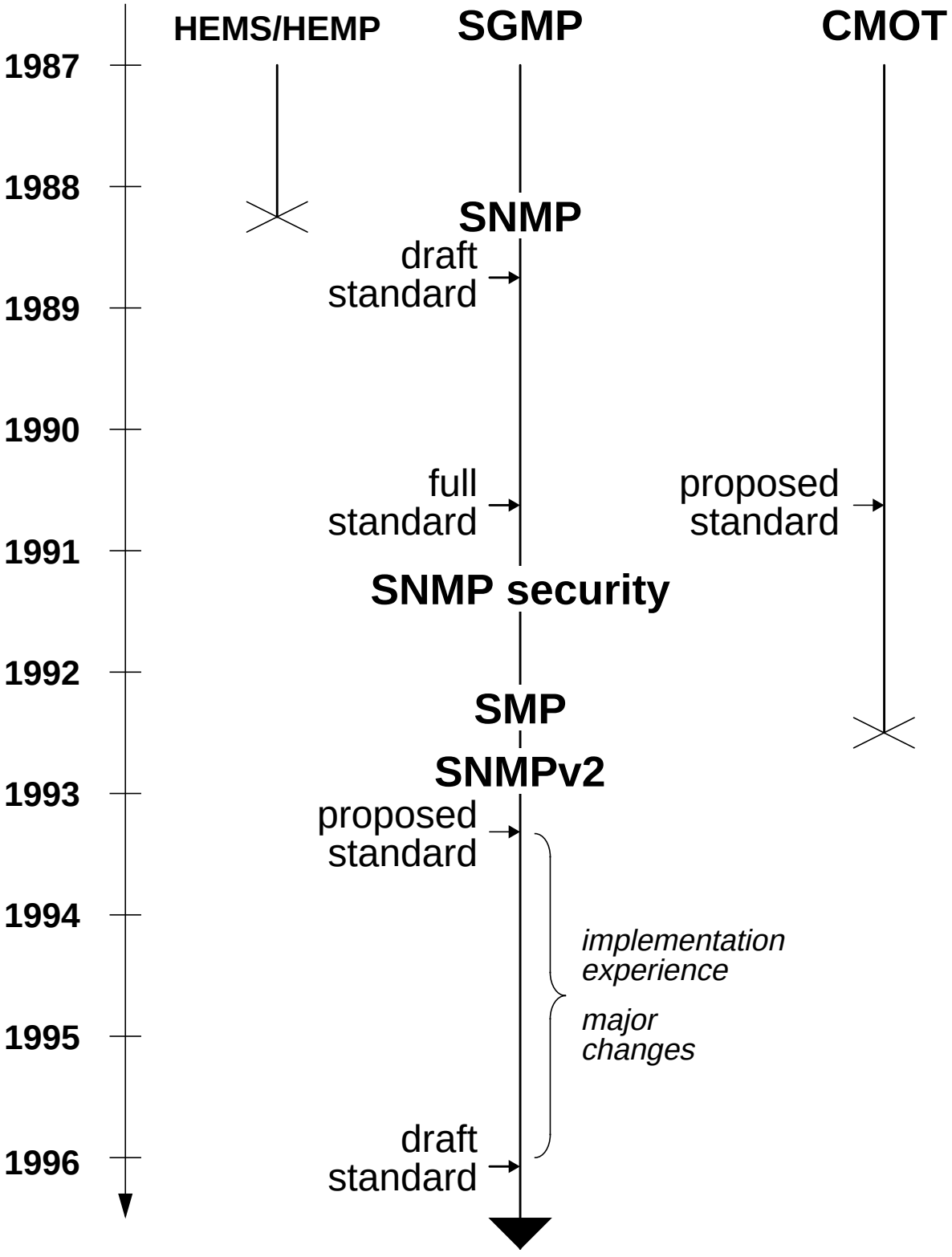
http://wwwtios.cs.utwente.nl/~pras
http://wwwtios.cs.utwente.nl/
http://wwwsnmp.cs.utwente.nl/

CONTENTS

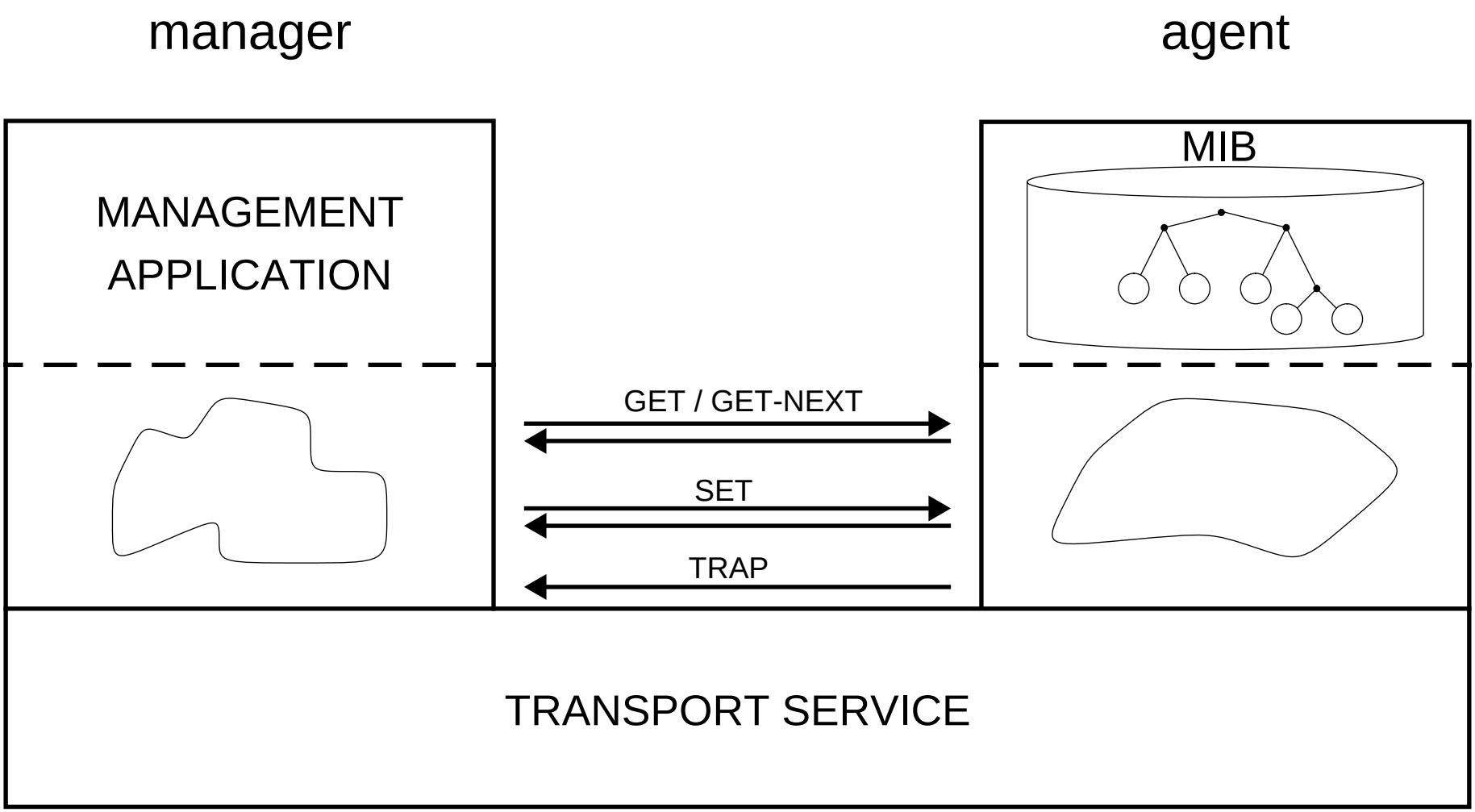
IETF STANDARDIZATION



HISTORY IETF



SNMPv1 STRUCTURE



SNMPv1 MESSAGE & PDU STRUCTURE

variable bindings:

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

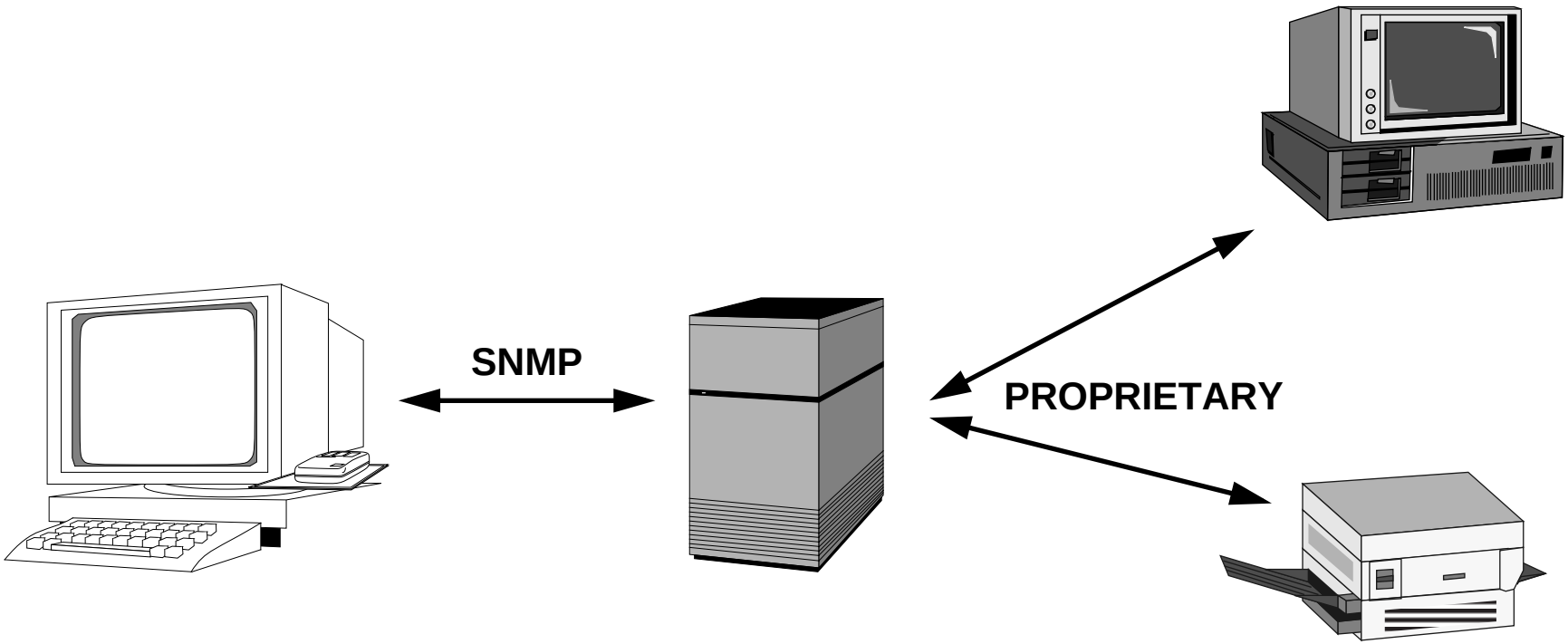
SNMP PDU:

PDU TYPE*	REQUEST ID	ERROR STATUS	ERROR INDEX	VARIABLE BINDINGS

SNMP message:

VERSION	COMMUNITY	SNMP PDU

PROXY MANAGEMENT



MANAGER PROXY AGENT NON-SNMP AGENT

SNMPv2

APRIL 1993:

- PROPOSED STANDARD
- RFC 1441 - RFC1452
- PARTY BASED SECURITY MODEL

JUNE 1995:

- PARTY BASED MODEL REJECTED
- NEW PROPOSALS APPEARED

JANUARY 1996:

- SNMPv2**C** BECAME DRAFT STANDARD
- RFC 1901 - RFC 1908
- COMMUNITY BASED SECURITY MODEL

SECURITY:

- SNMPv2 USER SECURITY MODEL (USEC)
- SNMPv2*

MANAGEMENT HIERARCHY:

- DISMAN WORKING GROUP

SNMPv2 GOALS

IMPROVED PERFORMANCE

- GET-BULK PDU

SECURITY

- AUTHENTICATION
- ENCRYPTION
- ACCESS CONTROL

MANAGEMENT HIERARCHY

- MANAGER TO MANAGER COMMUNICATION

OTHER IMPROVEMENTS

OTHER IMPROVEMENTS

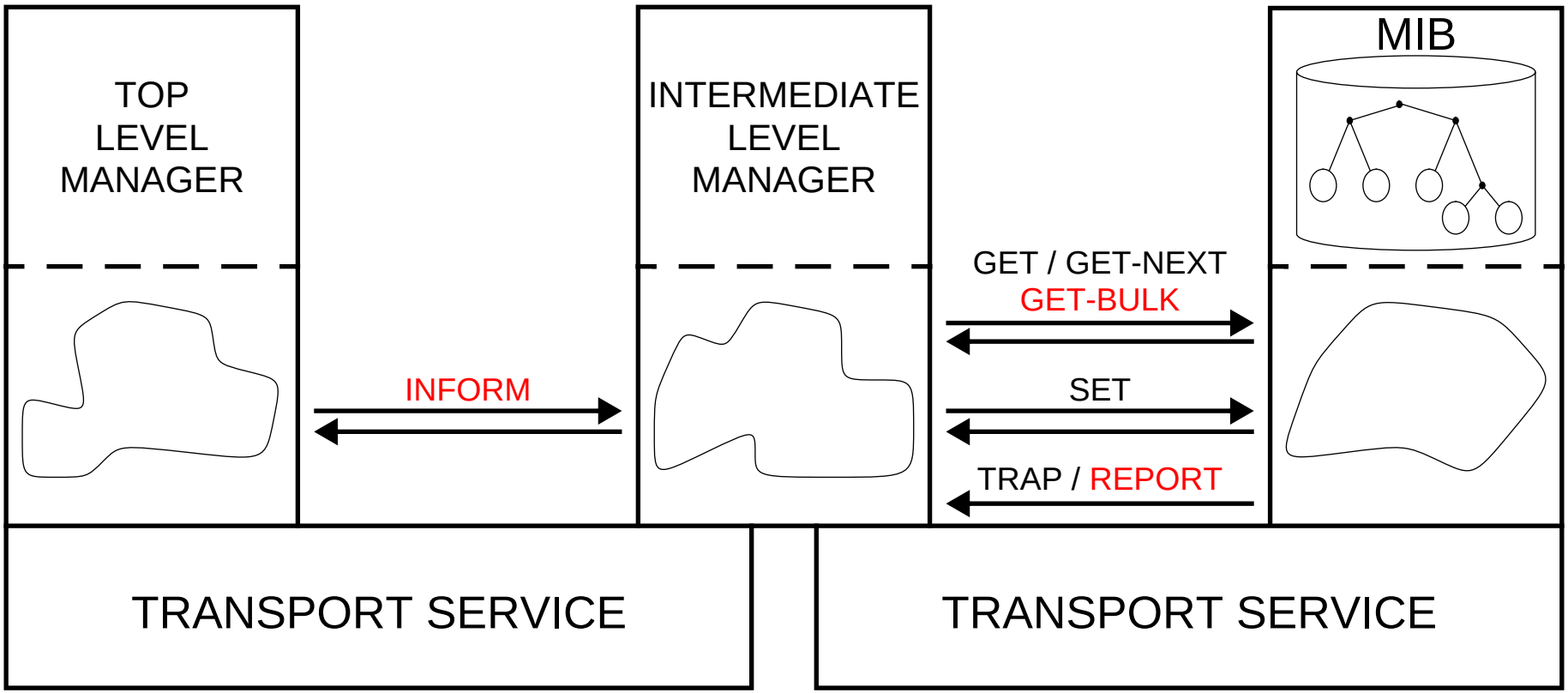
• DEFINITION OF ADDITIONAL DATA TYPES
AND FORMALISMS
BASED ON IMPLEMENTATION EXPERIENCE

• TRANSPORT SERVICE INDEPENDENCE:
MAPPINGS FOR SNMPV2
OVER SEVERAL TRANSPORTS ARE DEFINED

• RECORDING THE UNWRITTEN RULES OF SNMP
- ROW STATUS PLUS OTHER TEXTUAL CONVENTIONS

• REDEFINED TRAP PDU
- HAS SAME PDU FORMAT AS OTHER PDUs
- MAY BE SEND TO ZERO, ONE OR MORE MANAGERS

SNMPv2 PDUs


TOP
LEVEL
MANAGER
INTERMEDIATE
LEVEL
MANAGER
MIB
GET / GET-NEXT
GET-BULK
INFORM
SET
TRAP / REPORT
TRANSPORT SERVICE
TRANSPORT SERVICE

USEC:
SECURE TRANSFER OF MANAGEMENT PDUs (1)

GOALS

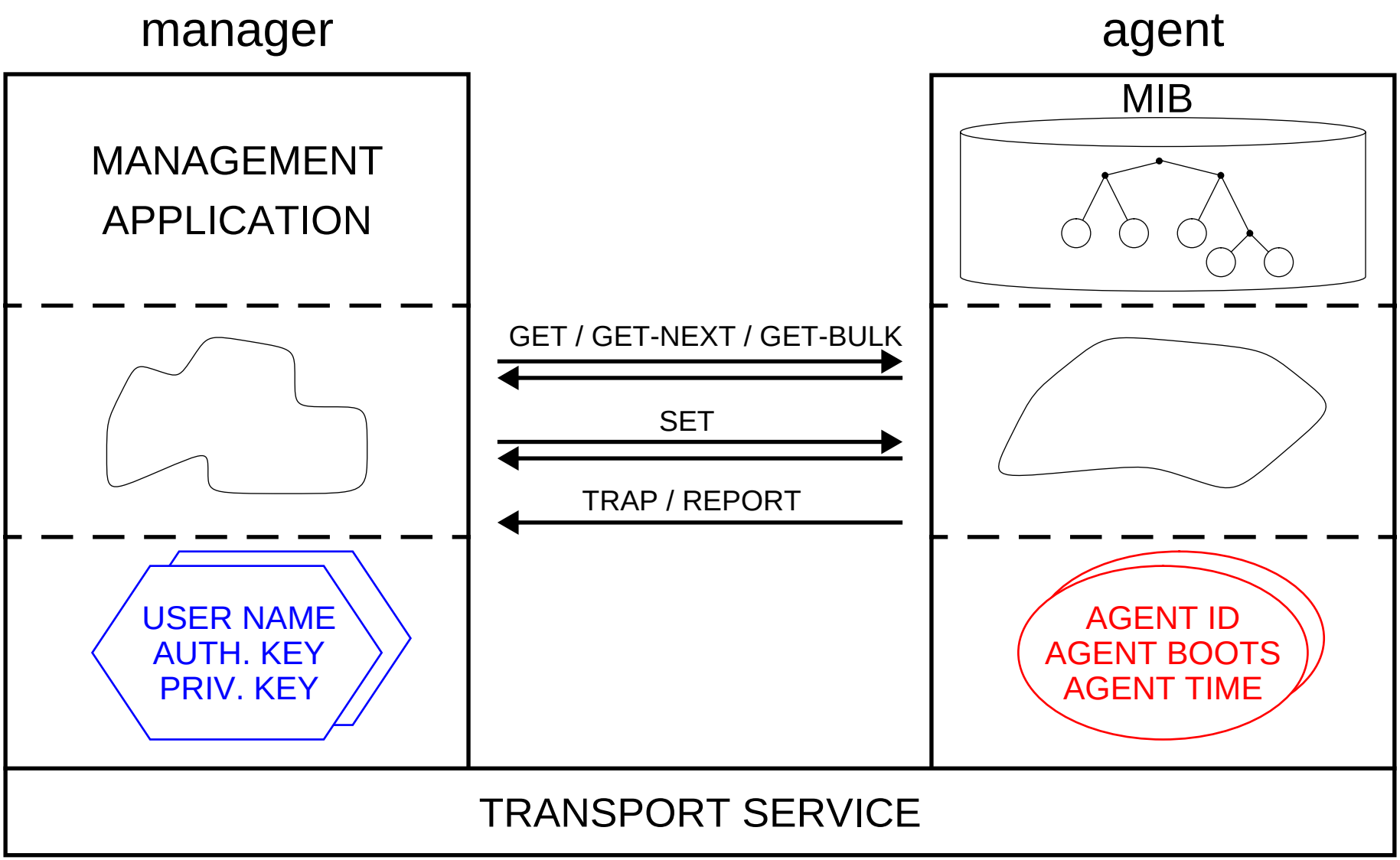
PROTECTION AGAINST:

- MODIFICATION OF INFORMATION
- MASQUERADE
- MESSAGE STREAM MODIFICATION
  (REORDERING, DELAY, REPLAY)
- DISCLOSURE

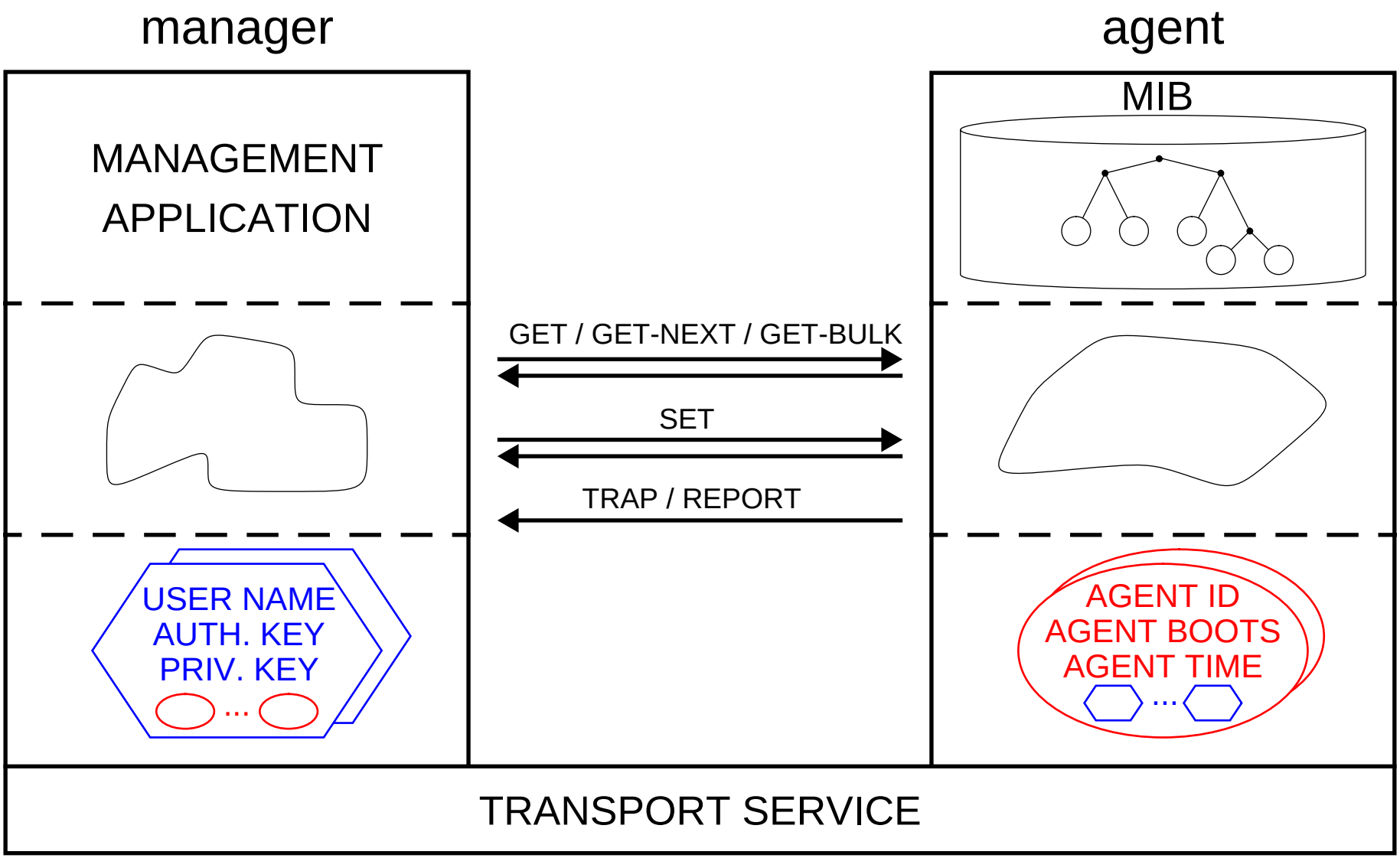
NO PROTECTION AGAINST:

- DENIAL OF SERVICE ATTACKS
- TRAFFIC ANALYSIS ATTACKS

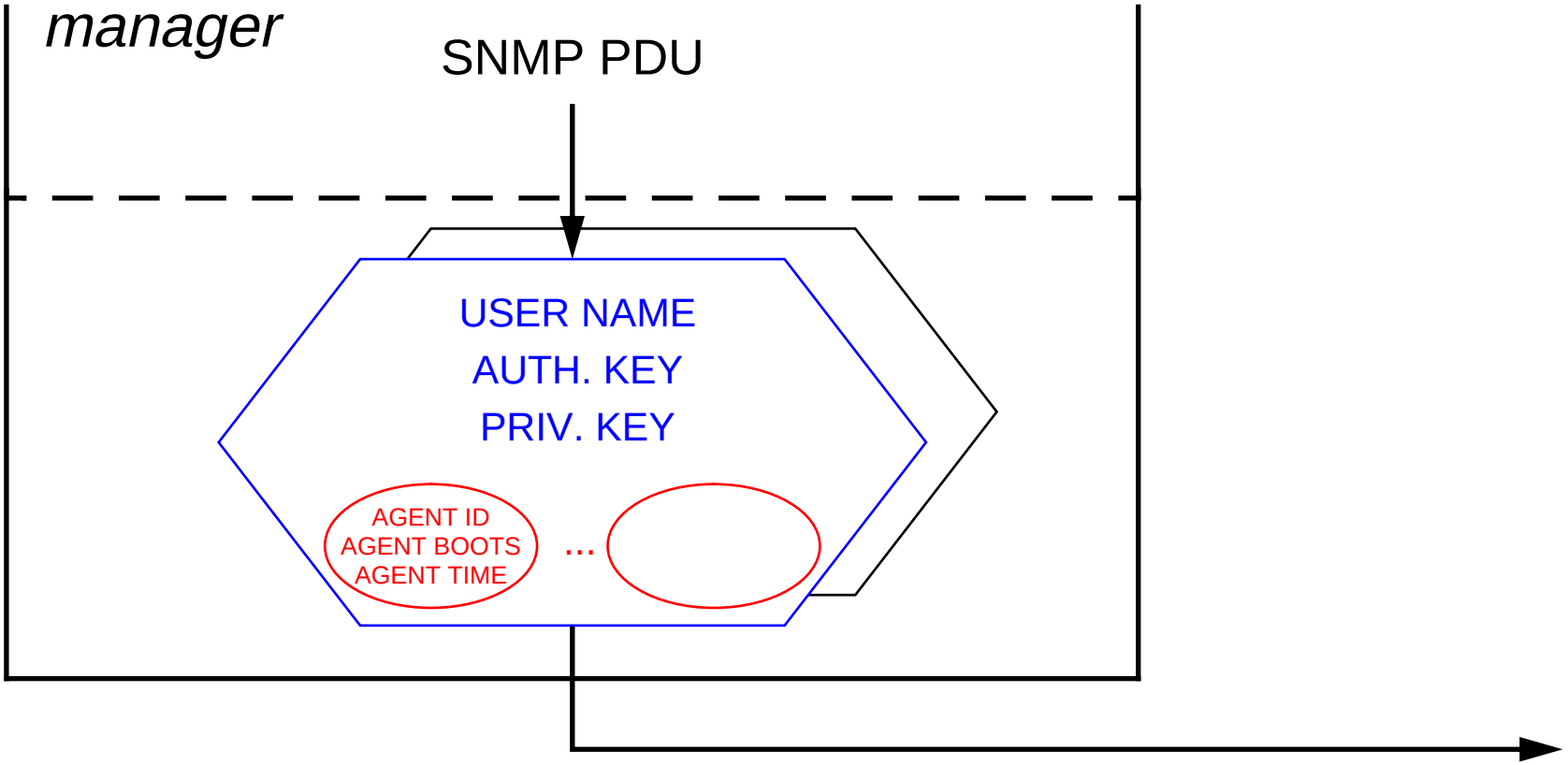
USEC: SECURE TRANSFER OF MANAGEMENT PDUs (2)



USEC: SECURE TRANSFER OF MANAGEMENT PDUs (3)



USEC: SECURE TRANSFER OF MANAGEMENT PDUs (4)



ENCRYPTED SNMP PDU	DIGEST	USER NAME	AGENT TIME	AGENT BOOTS	AGENT ID	QoS	SECURITY MODEL	SNMP VERSION

USEC:
SECURE TRANSFER OF MANAGEMENT PDUs (5)

MECHANISMS

MODIFICATION OF INFORMATION
- DIGEST
- MD5

MASQUERADE
- USER NAME

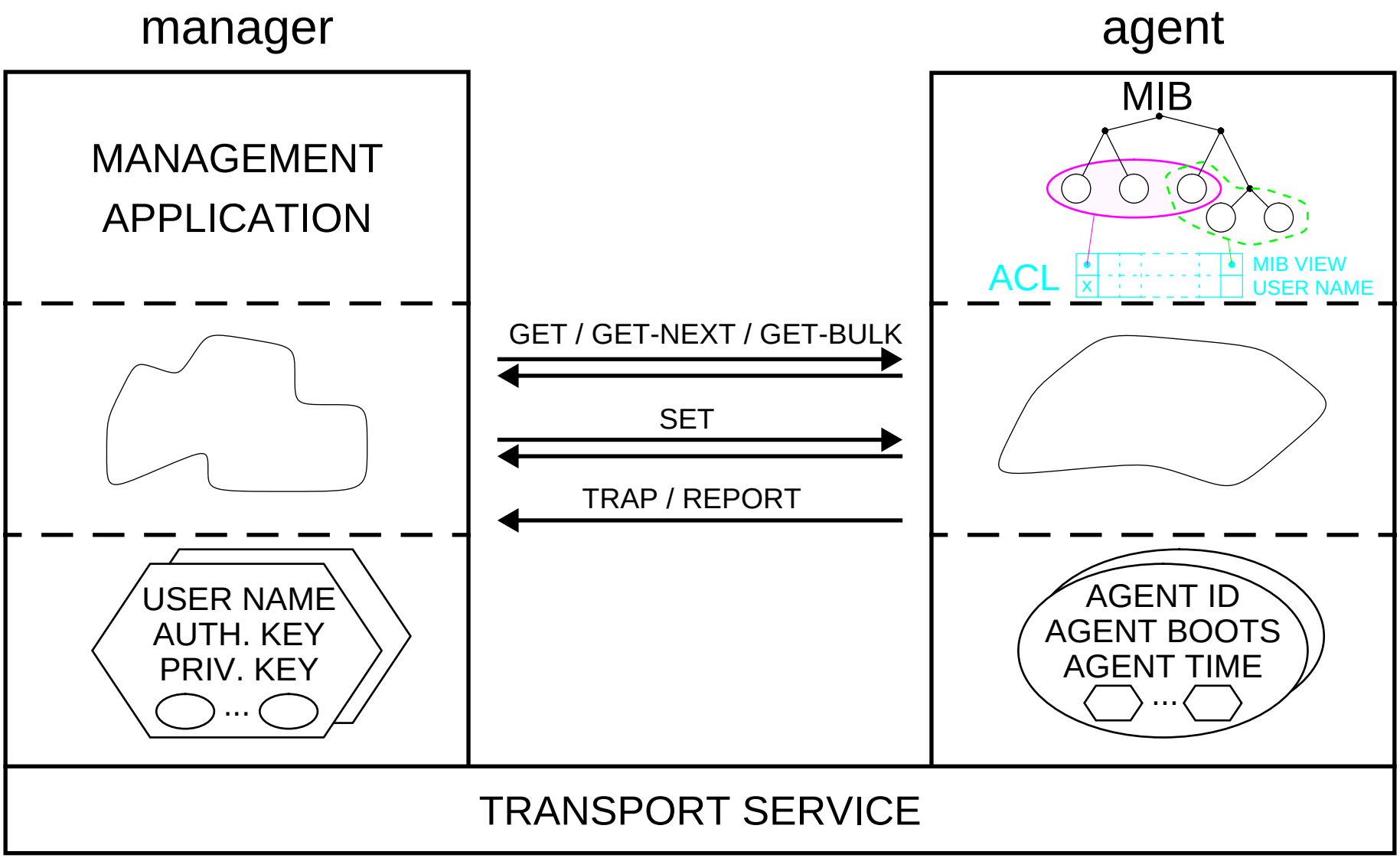
(DIGEST)

MESSAGE STREAM MODIFICATION
- AGENT BOOTS, AGENT TIME

(DIGEST)

DISCLOSURE
- SNMP PDU ENCRYPTION
- DES

USEC: ACCESS CONTROL



CMIP versus SNMP - 1

	CMIP	SNMP
model	event based	polling based
information approach	object oriented	variable oriented
complexity	agent is complex	agent is simple
state information	kept by agent	kept by manager
underlying service	CO - reliable	CL - unreliable
efficiency	good	acceptable
implementation	difficult	simple *(V2 is more difficult)*

CMIP versus SNMP - 2

	CMIP	SNMP
retrieves	objects	scalars
many items	multiple replies	error: tooBIG
object selection	scoping & filtering	-
synchronization	atomic & best effort	atomic
events / traps	confirmed & unconfirmed	unconfirmed
actions	possible	via ‘trick’

CMIP versus SNMP - 3

	CMIP	SNMP
security	via underlying services	- *authentication / encryption / ACL-lists*
management functions	many	none
approach	object oriented	variable oriented
ASN.1	full support	subset
naming structure	flexible	simple

CMOL versus SNMP

CMOL IS COMPARIBLE TO CMIP

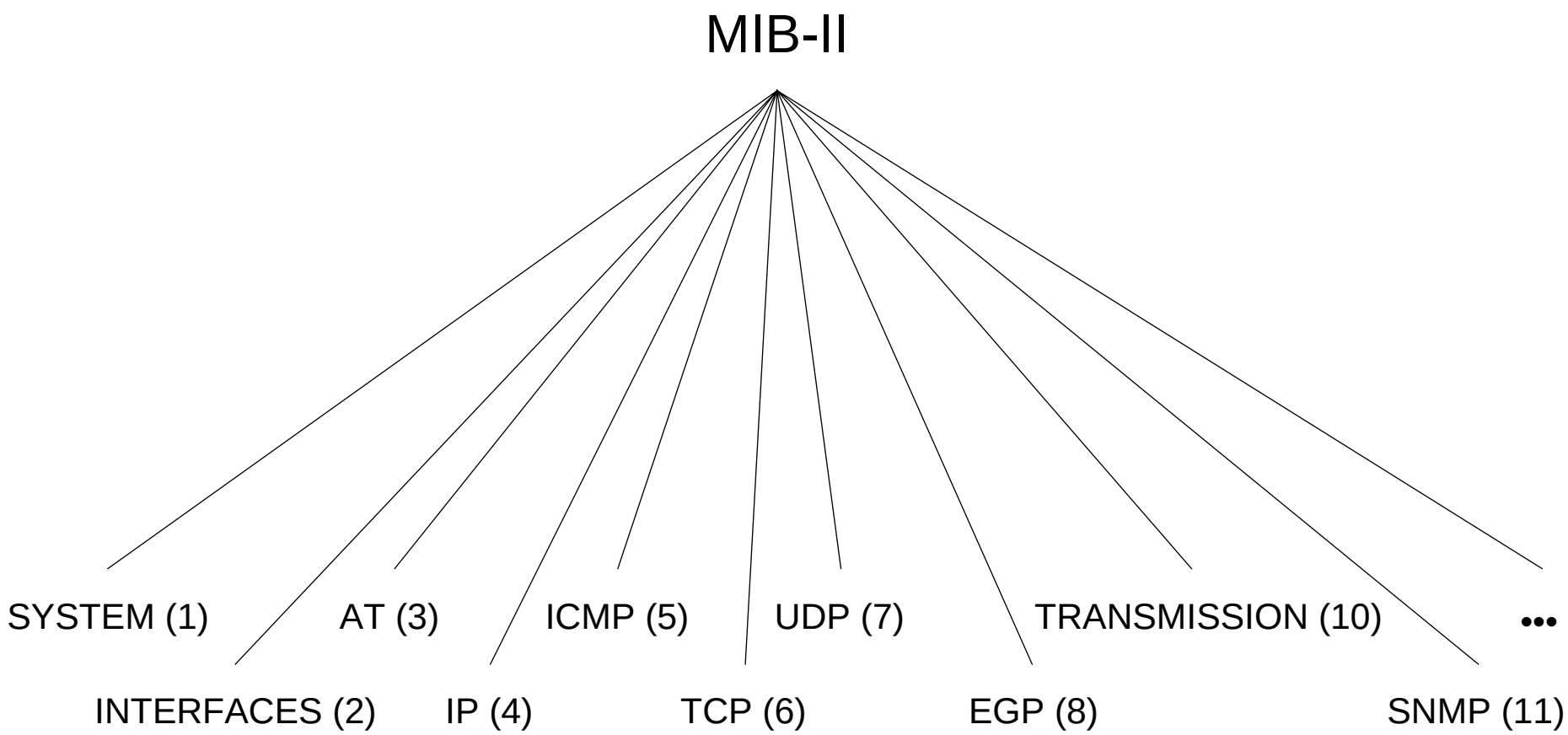
CMOL OPERATES OVER LLC

CMOL CAN NOT OPERATE OVER ROUTERS

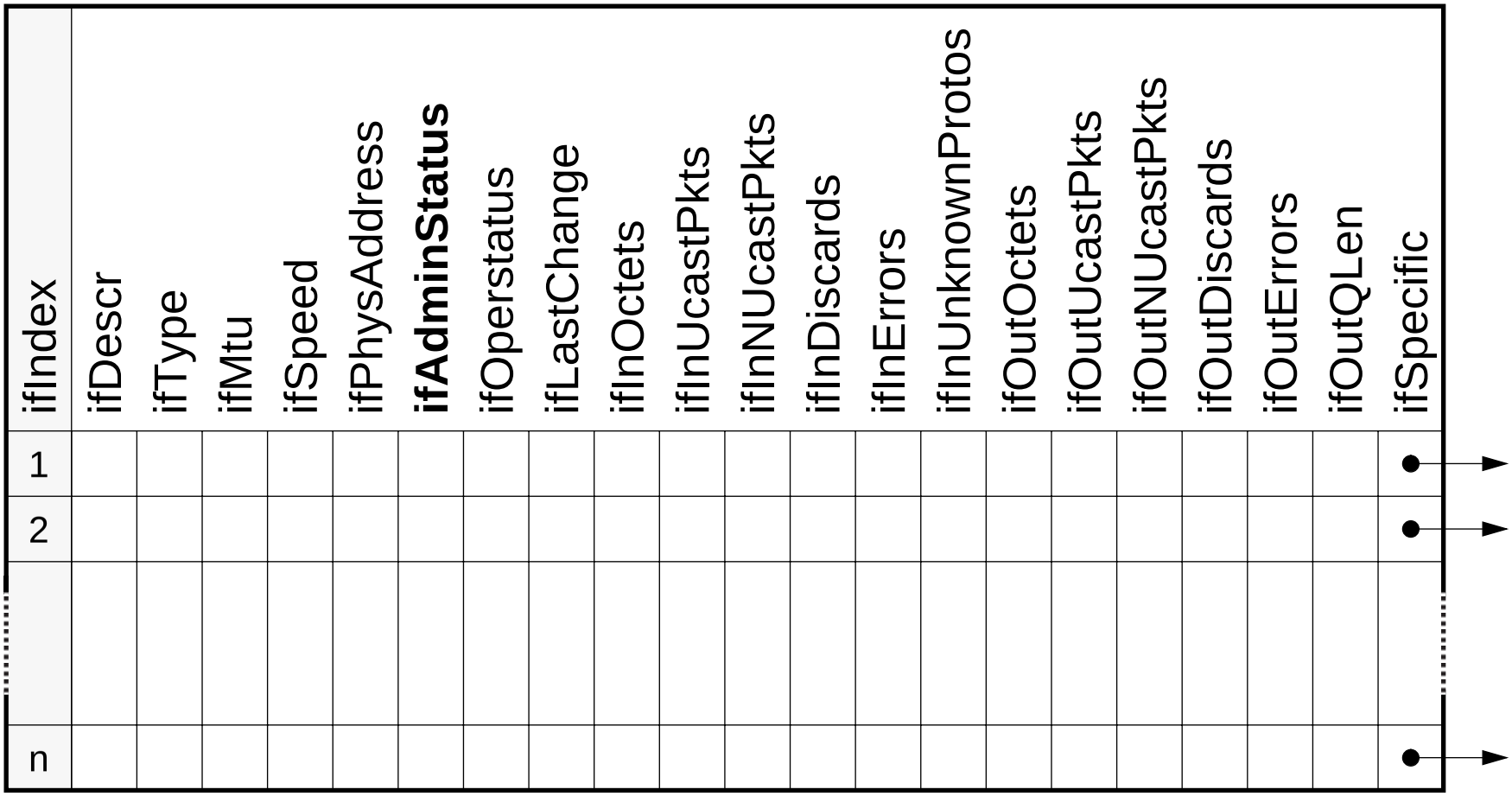
CMOL: FEW IMPLEMENTATIONS

-

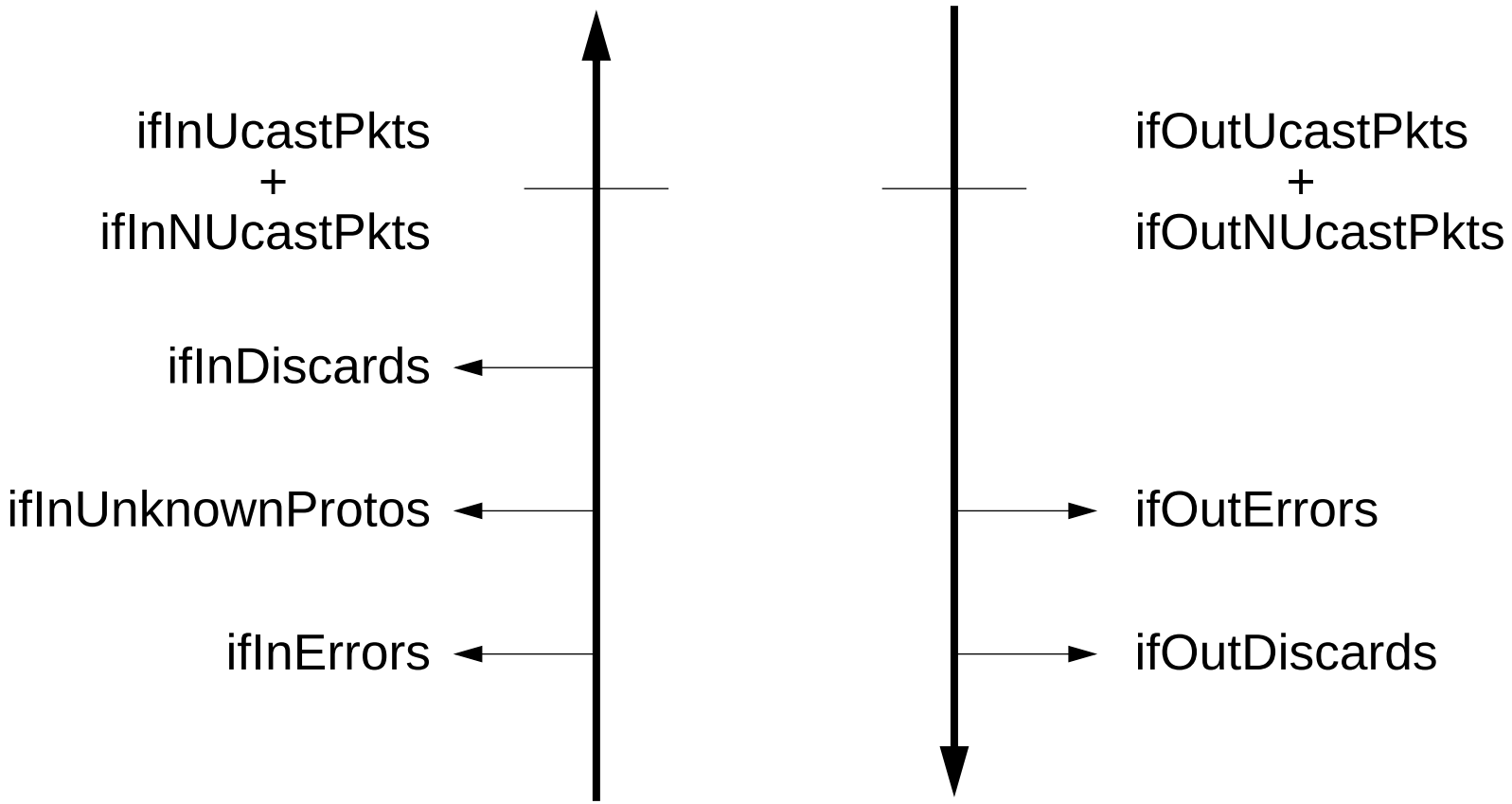
MIBs


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

MIB-II ifTable



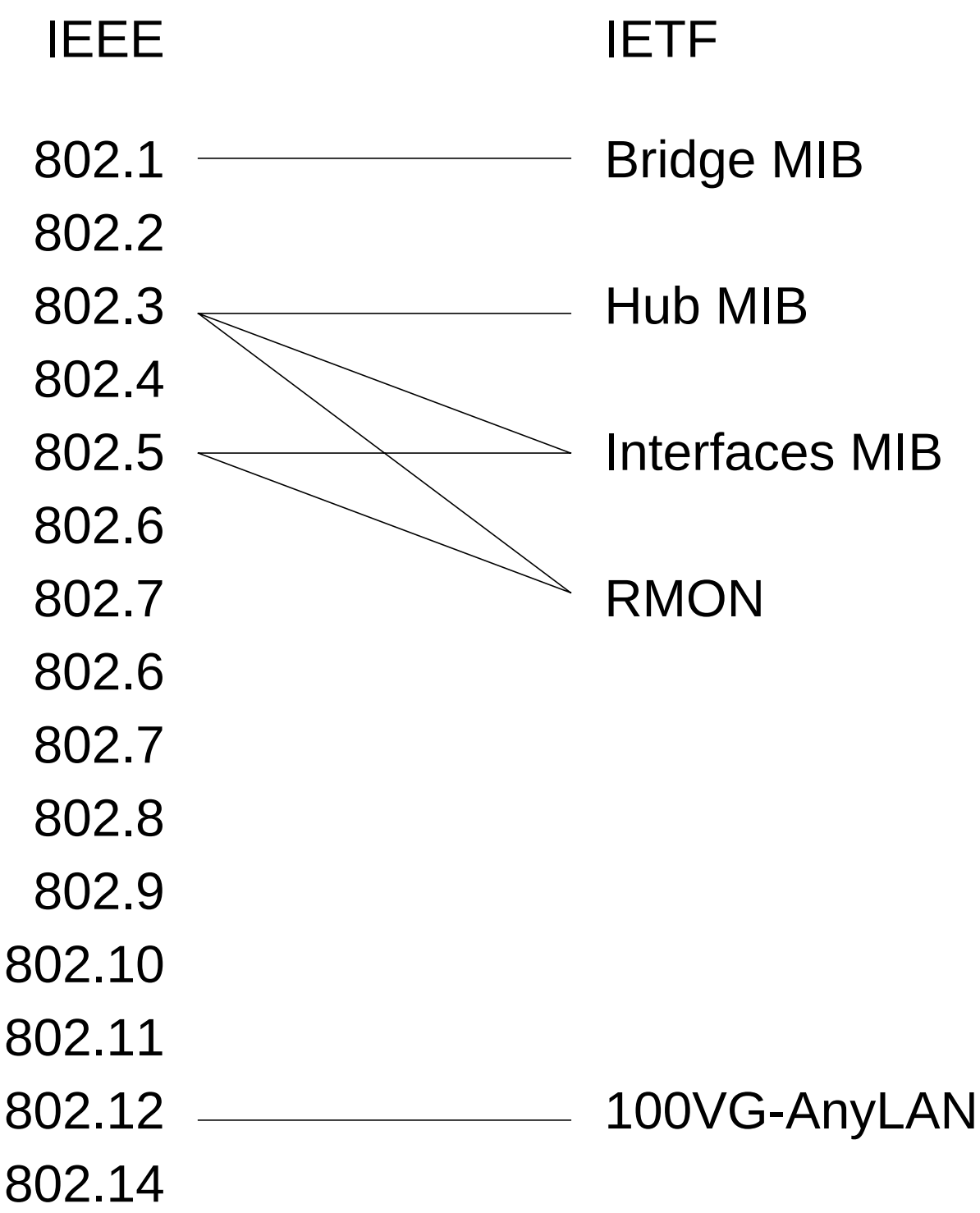
MIB-II IF PACKET COUNT



OVERVIEW LAN SPECIFIC MIBs

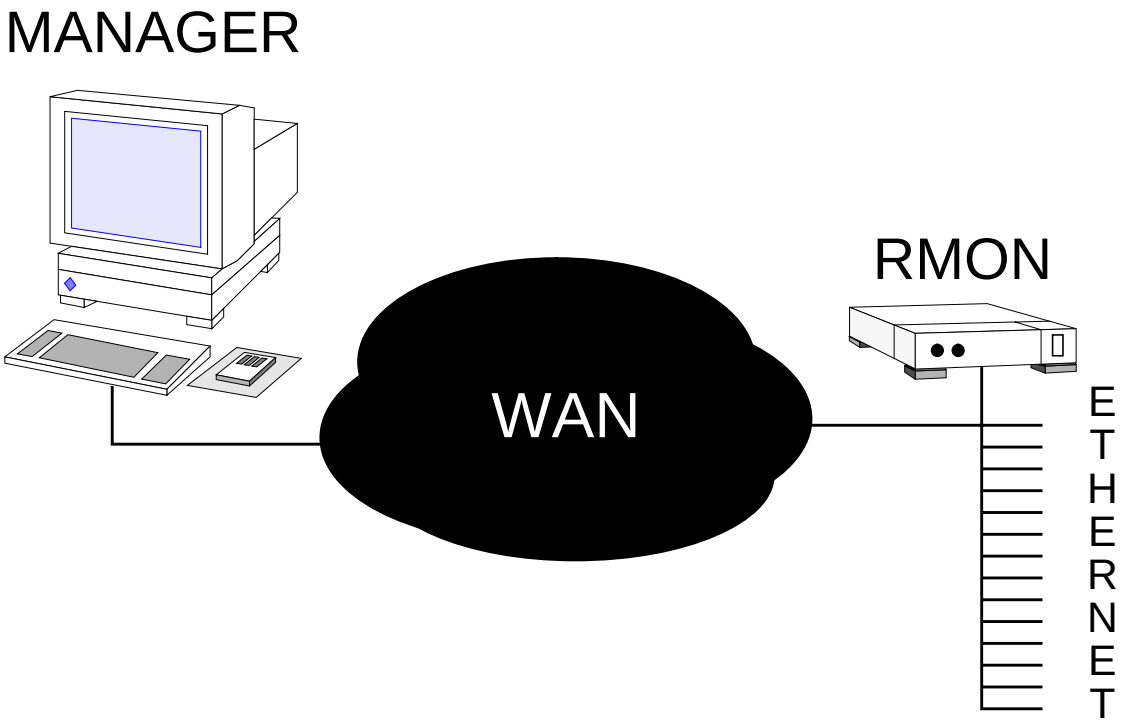
NAME	SMI	RFC	STATUS	WORKING GROUP
ETHERNET-LIKE INTERFACES	v1 v2	1643 1650	STANDARD PROPOSED	INTERFACE
802.3 MAU	v1	1515	PROPOSED	HUB
802.3 REPEATER DEVICES	v1	1516	DRAFT	HUB
802.4 TOKEN BUS	v1	1230	HISTORIC	-
802.5	v2	1748	DRAFT	INTERFACE
802.5 STATION SOURCE ROUTING	v2	1749	PROPOSED	INTERFACE
802.12	v2	-	WORKING DOC.	100VG-AnyLAN
802.12 REATER DEVICES	v2	-	WORKING DOC.	100VG-AnyLAN
REMOTE NETWORK MONITORING (RMON)	v1 v2	1757 -	DRAFT WORKING DOC.	RMON
TOKEN RING EXTENSIONS TO RMON	v1	1513	PROPOSED	RMON
BRIDGES	v1 v2	1493 -	DRAFT WORKING DOC.	BRIDGE
SOURCE ROUTING BRIDGES	v1 v2	1525 -	PROPOSED WORKING DOC.	BRIDGE

IEEE - IETF WORKING GROUPS



REMOTE NETWORK MONITORING

RMON



RFC 1757

RMON GROUPS

NINE GROUPS:

- STATISTICS
- HISTORY
- HOST TABLE
- HOST TOP N
- TRAFFIC MATRIX
- ALARMS
- FILTERS
- PACKET CAPTURE
- EVENTS

STATISTICS GROUP

KEEPS STATISTICS PER ETHERNET SEGMENT

SHOWS:

- PACKETS
- OCTETS
- BROADCASTS
- MULTICASTS
- COLLISIONS
- ERRORS

	< 64 Bytes	**64 to 1518**	**>1518 bytes**
WELL-FORMED PACKETS	undersize	GOOD!	oversize
BAD FCS ERRORS	fragments	CRC or alignment errors	jabber

KEEPS TRACK OF PACKET SIZE DISTRIBUTION:

- 65 - 127 OCTETS
- 128 - 255 OCTETS
- 256 - 511 OCTETS
- 512 - 1023 OCTETS
- 1024 - 1518 OCTETS

HISTORY GROUP

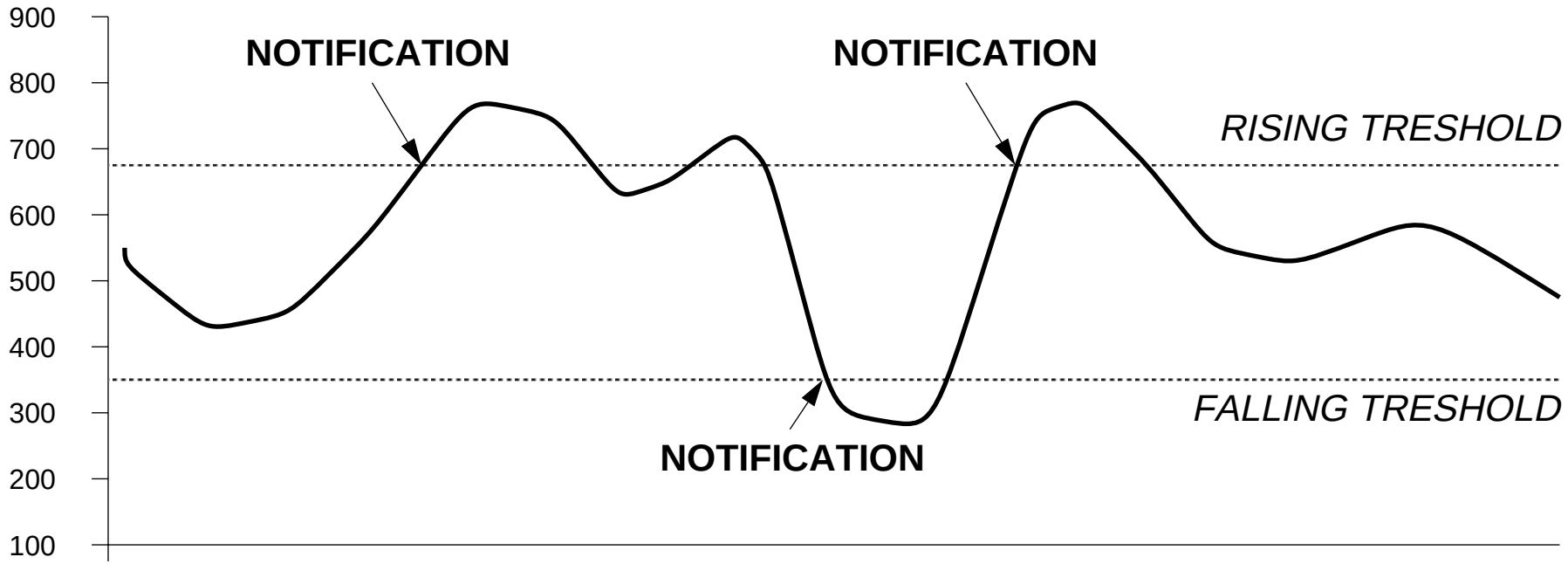
STORES INFORMATION OF STATISTICS GROUP
EXCEPT PACKET SIZE DISTRIBUTION

USES A CIRCULAR BUFFER

- BUCKETS
- SIZE MAY BE SET BY MANAGER

SAMPLING INTERVAL
MAY BE SET BY MANAGER

ALARM GROUP



ABSOLUTE OR DELTA VALUES

HOST INFORMATION

- HOST GROUP
- HOST TOP N

IN / OUT:
PACKETS / OCTETS

OUT:
BROADCASTS
MULTICASTS
ERRORS

INFORMATION INDEXED BY:

- INTERFACE AND MAC ADDRESS
hostTable

- CREATION TIME
hostTimetable

- SORTED ON SOME VARIABLE VALUE
hostTopN

OTHER GROUPS

- TRAFFIC MATRIX

FOR EACH SOURCE & DESTINATION

- PACKETS
- OCTETS
- ERRORS

- FILTER GROUP

TO COUNT PACKETS
THAT CARRY A SPECIFIC BIT-PATTERN

- PACKET CAPTURE GROUP

TO STORE SPECIFIC PACKETS

- EVENT GROUP

TO DEFINE THE VARIOUS EVENTS
DETERMINE TRANSMISSION OF TRAPS

NEW DEVELOPMENTS

WEB BASED MANAGEMENT!

EMBEDDED MANAGEMENT APPLICATIONS:

• MANAGER IS A STANDARD WWW BROWSER

• DEVICE VENDORS CAN SELL MANAGEMENT CAPABILITIES

• AGENT BECOMES MORE COMPLEX

• USE OF JAVA

HTTP AS MANAGEMENT PROTOCOL:

• CONNECTION ORIENTED TRANSPORT

• USE OF HTTP SECURITY

APPLICATIONS:

• DEVICE MANAGEMENT

• CUSTOMER NETWORK MANAGEMENT

FURTHER INFORMATION

- http://wwwtios.cs.utwente.nl/~pras

SHEETS OF THIS PRESENTATION

- http://wwwsnmp.cs.utwente.nl/

'THE SIMPLEWEB'
WWW SERVER FOR NETWORK MANAGEMENT
(STANDARDS, SOFTWARE, ARTICLES, ...)

- WILLIAM STALLINGS

SNMP, SNMPv2 AND RMON
ADDISON WESLEY
ISBN: 0-201-63479-1
JUNE 1996

- MARSHALL ROSE

THE SIMPLE BOOK
PRENTICE HALL
ISBN: 0-13-451659-1
APRIL 1996