SYSTEMS MANAGEMENT ’98

Ontwikkelingen in SNMP-netwerkbeheer vooruitblik op SNMPv3

29 oktober 1998

Aiko Pras

Centre for Telematics and Information Technology
Universiteit Twente
Postbus 217
7500 AE Enschede

http://wwwctit.utwente.nl/
http://www.ctit.utwente.nl/~pras

PRESENTATION OVERVIEW

STATUS SNMPv1

- LIMITATIONS

SNMPv2

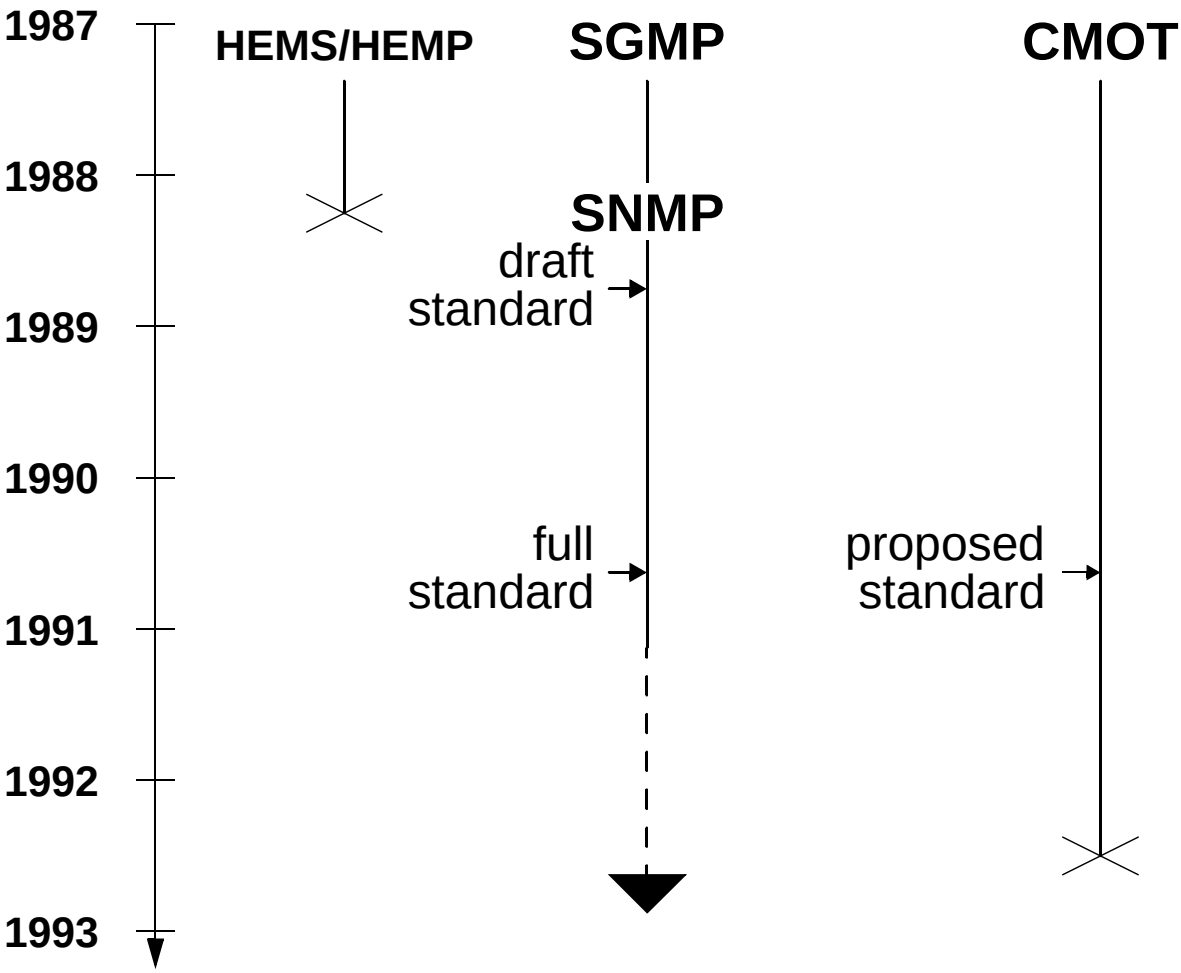
- UNDOCUMENTED RULES
- ERROR CODES
- DATA TYPES
- TRAPS
- PERFORMANCE
- TRANSPORT DEPENDENCE
- HIERARCHIES
- SECURITY

SNMPv3

- ARCHITECTURE
- SECURE COMMUNICATION
- ACCESS CONTROL

CONCLUSIONS

SNMPv1: STATUS



DEFACTO STANDARD

HUNDREDS OF MIBs

MANY IMPLEMENTATIONS

SNMPv1: PROBLEMS

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

1993: WORK STARTED ON SNMPv2

UNDOCUMENTED RULES

• DEFINE TEXTUAL CONVENTIONS
TO REFINE SEMANTICS OF EXISTING TYPES

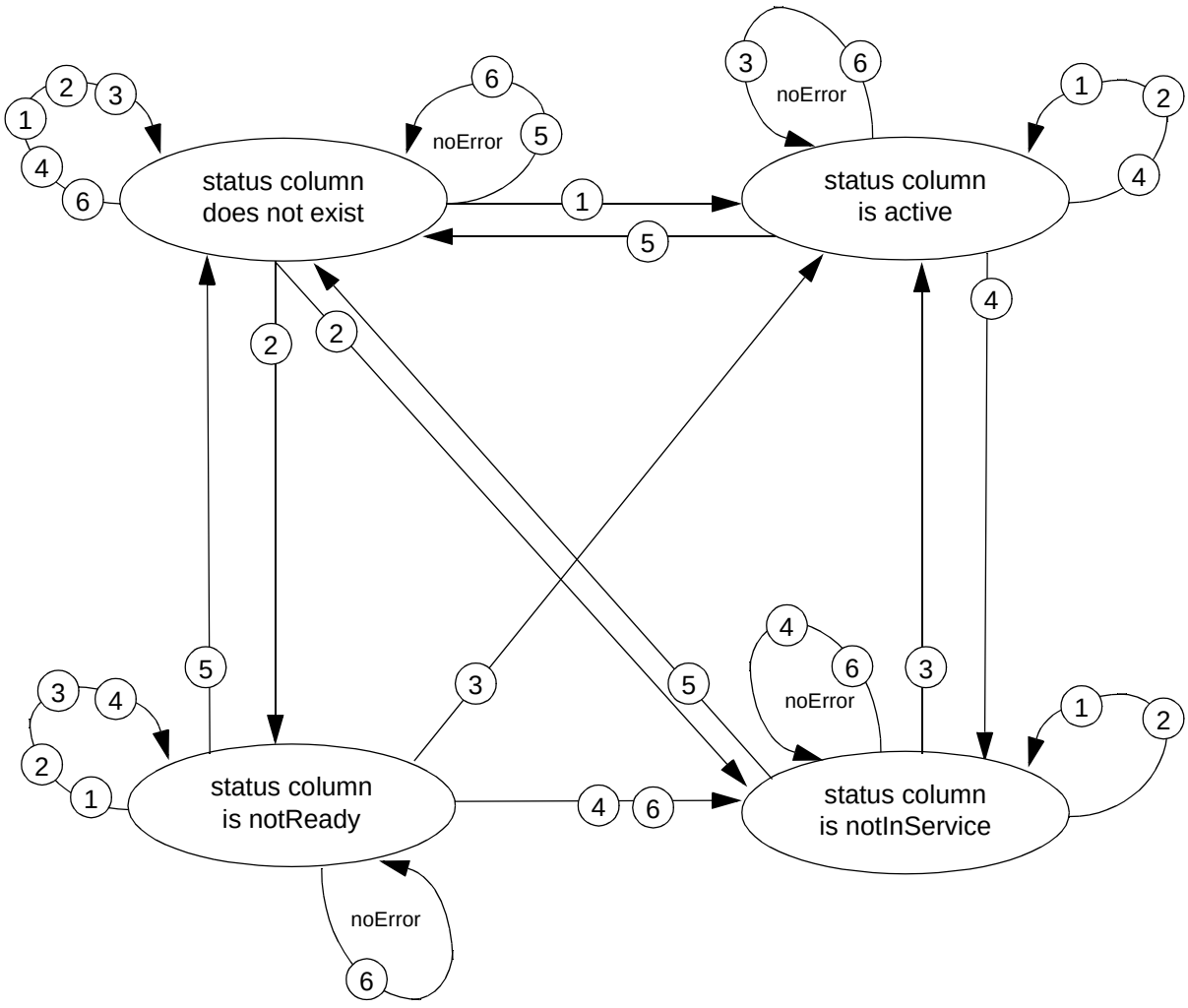
EXAMPLE:

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

• DEFINE USE OF ROW STATUS
FOR CHANGES TO TABLE ROWS

TO:	VIA:	STATUS:
130.89.16.4	130.89.1.1	ACTIVE
130.89.17.6	130.89.1.1	NOT READY
130.89.18.2	130.89.1.4	ACTIVE
130.89.18.7	130.89.1.4	ACTIVE

ROW STATUS STATE DIAGRAM



1	set status column to createAndGo	4 6	4 or 6
2	set status column to createAndWait		
3	set status column to active		
4	set status column to notInService		
5	set status column to destroy		
6	set any other column to some value		

ADDITIONAL ERROR CODES FOR SETS

SNMPv1	SNMPv2
badValue	wrongValue
badValue	wrongEncoding
badValue	wrongType
badValue	wrongLength
badValue	inconsistentValue
noSuchName	noAccess
noSuchName	notWritable
noSuchName	noCreation
noSuchName	inconsistentName
genErr	resourceUnavailable
genErr	CommitFailed
genErr	undoFailed
...	...

ADDITIONAL DATA TYPES

SMIv1	SMIv2
INTEGER	INTEGER
OCTET STRING	OCTET STRING
OBJECT IDENTIFIER	OBJECT IDENTIFIER
INTEGER	INTEGER32
-	UNSIGNED32
GAUGE	GAUGE32
COUNTER	COUNTER32
-	COUNTER64
TIMETICKS	TIMETICKS
IPADDRESS	IPADDRESS
OPAQUE	OPAQUE
-	BITS
NETWORKADDRESS	-

NOTIFICATIONS

SNMPv1:

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

SNMPv2:

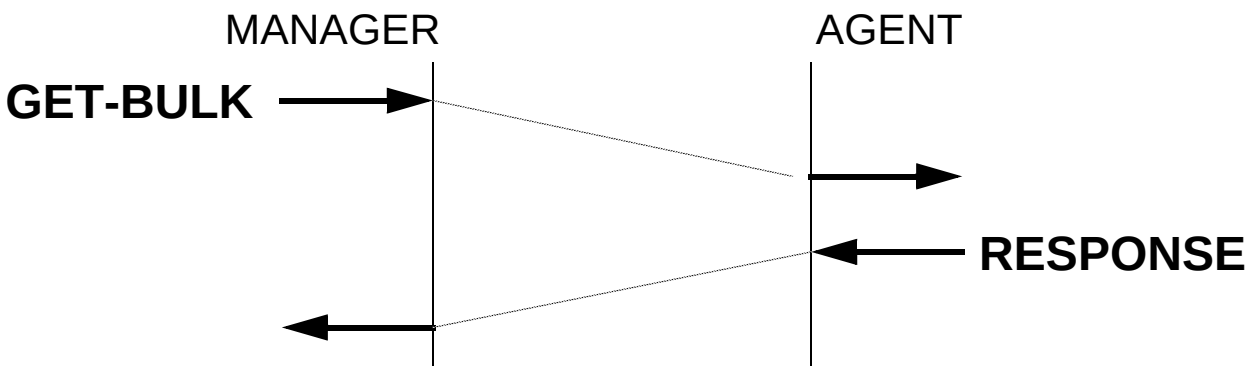
- MIBs MAY NOW INCLUDE NOTIFICATION TYPE MACROS

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}
```

PERFORMANCE

NEW GET-BULK PDU



EXAMPLE:

GET-BULK(max-repetitions = 4; 1.1)

RESPONSE(
1.1.0 => *130.89.16.2*
1.2.1.0 => *printer-1*
1.2.2.0 => *123456*
1.3.1.1.1 => *1*
)

GET-BULK PDU

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

N-TIMES

RESPONSE(
VariableBinding-1; ... ; VariableBinding-N; VariableBinding-(N+1); ... ; VariableBinding-(N+R)

1st LEXICOGRAPHICAL SUCCESSOR

VariableBinding-(N+1); ... ; VariableBinding-(N+R)

2nd LEXICOGRAPHICAL SUCCESSOR

VariableBinding-(N+1); ... ; VariableBinding-(N+R)

3th LEXICOGRAPHICAL SUCCESSOR

...

VariableBinding-(N+1); ... ; VariableBinding-(N+R)

M-TIMES

)

Mth LEXICOGRAPHICAL SUCCESSOR

TRANSPORT DEPENDANCE

SNMPv1:

- UDP

SNMPv2:

- UDP
- CLNS (OSI)
- DDP (APPLETALK)
- IPX

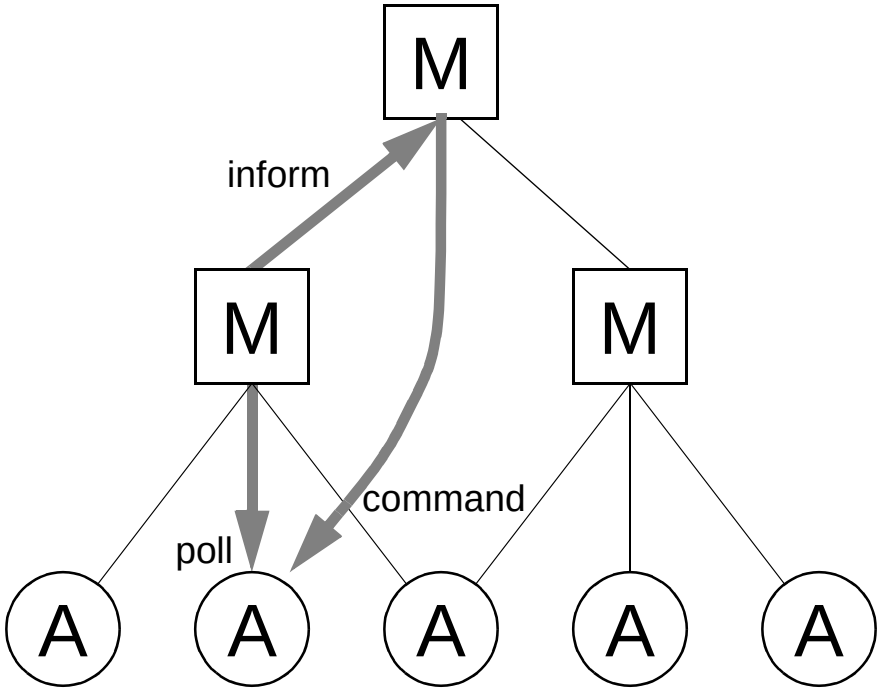
HIERARCHIES

• ORIGINAL IDEA:
MANAGER TO MANAGER (M2M) MIB

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

• TWO APPROACHES
ARE STANDARDIZED:
• MIB BASED
• SCRIPT BASED

DISMAN: MIB APPROACH



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

MIBs:

- EVENT MIB
- EXPRESSION MIB
- NOTIFICATION LOG MIB

DISMAN: SCRIPT APPROACH

• 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

SNMPv2 SECURITY: WHAT HAPPENED?

APRIL 1993:
PROPOSED STANDARD
SECURITY BASED ON *PARTIES*
FOUR EDITORS

SOON AFTERWARDS:
FIRST PROTOTYPES

SPRING 1995:
MANAGEMENT HIERARCHIES REMOVED
SPECIAL WORKING GROUP FORMED
(DISMAN)

JUNE 1995:
PROPOSED STANDARD REJECTED
BY TWO OF THE ORIGINAL EDITORS!

AUGUST 1995:
GENERAL AGREEMENT THAT
PARTY BASED SECURITY MODEL WAS
TOO COMPLEX!
MANY NEW PROPOSALS APPEARED

SNMPv3

NEW GROUP OF PEOPLE

MODULAR APPROACH

REACHED AGREEMENT ON SECURITY

- SECURE COMMUNICATION
- ACCESS CONTROL

SEVERAL VENDOR IMPLEMENTATIONS

MODULAR SNMPv3 ARCHITECTURE

SNMP ENTITY

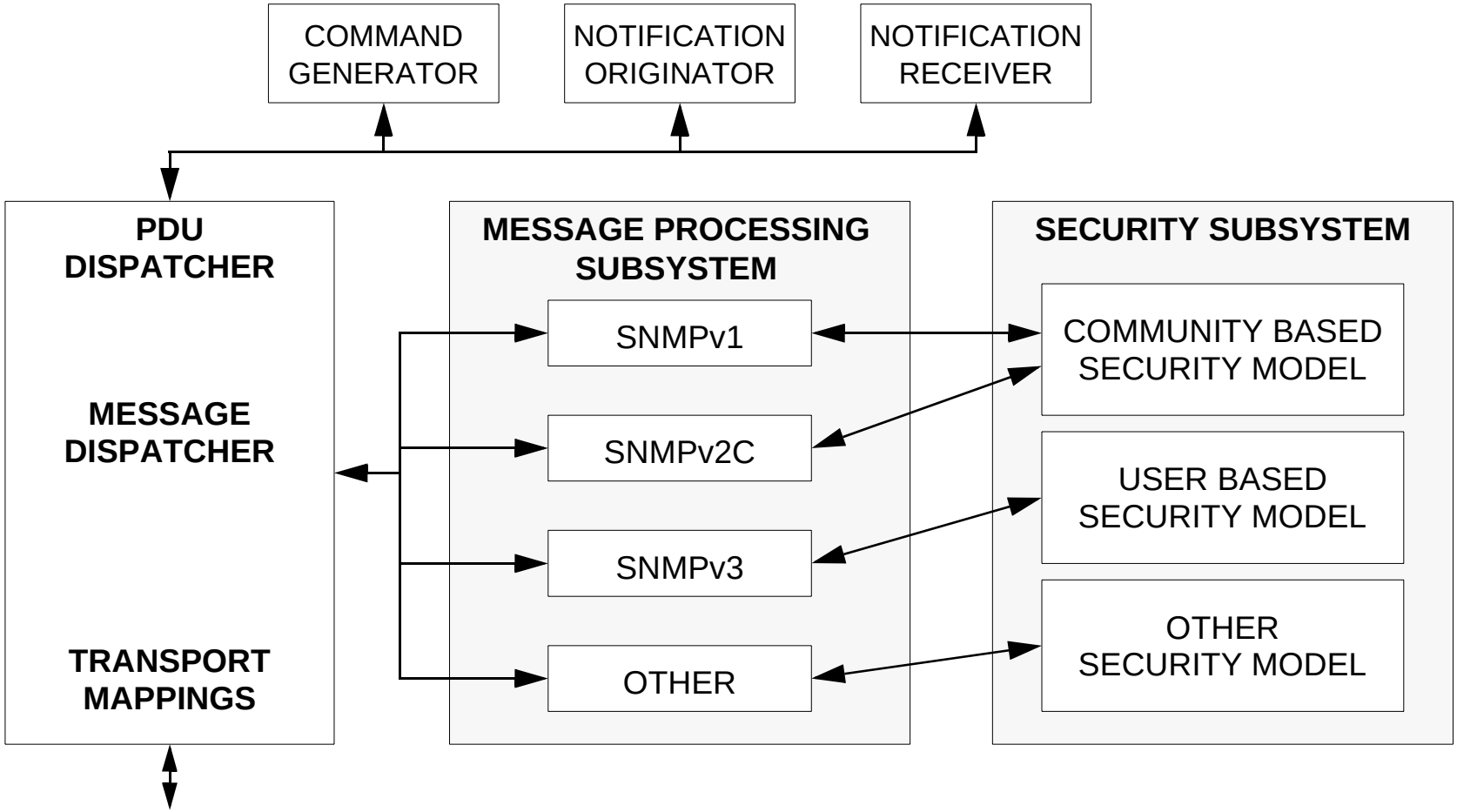
SNMP APPLICATIONS

- COMMAND GENERATOR
- COMMAND RESPONDER
- NOTIFICATION ORIGINATOR
- NOTIFICATION RECEIVER
- PROXY FORWARDER
- OTHER SNMP ENGINE

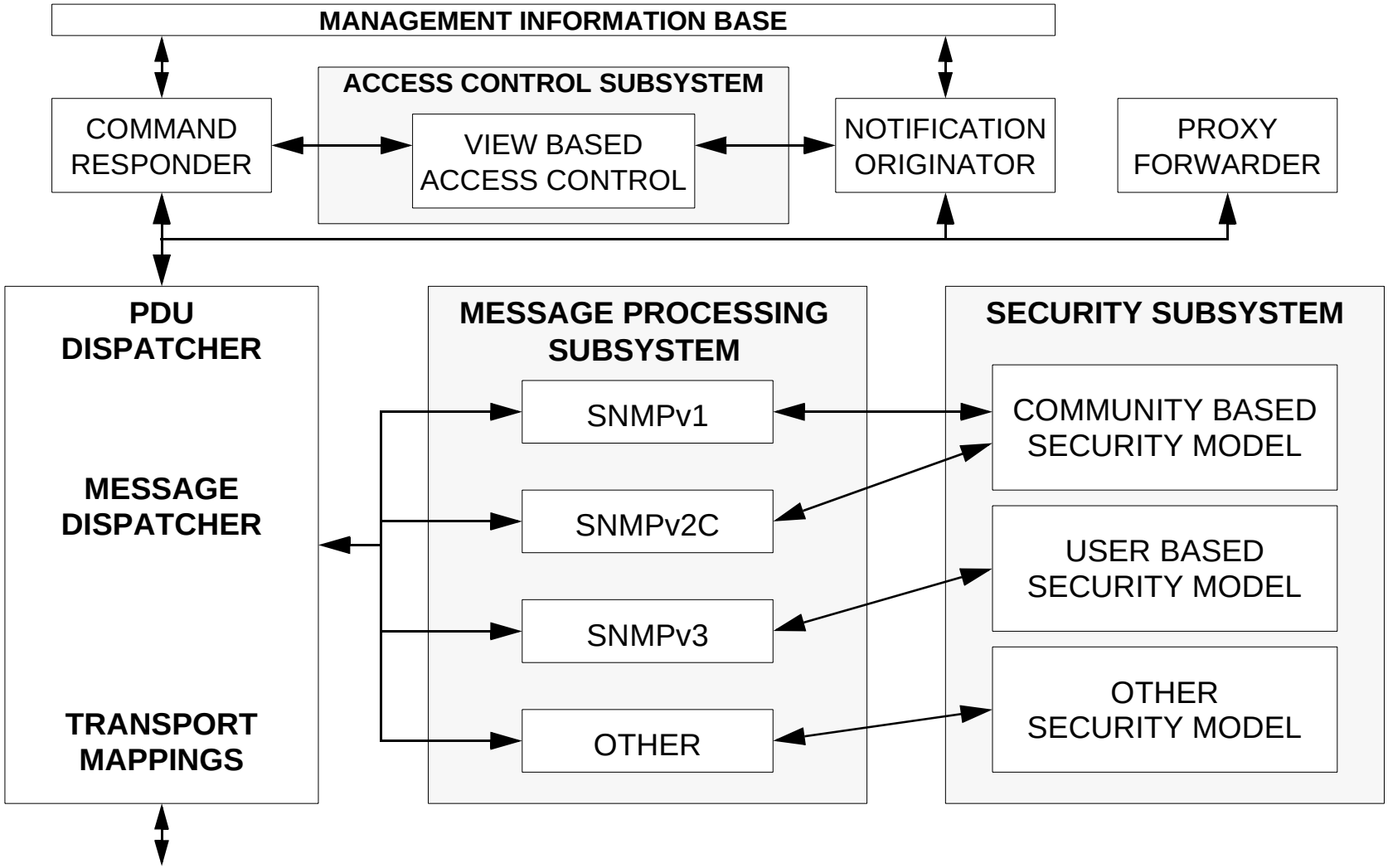
SNMP ENGINE

- DISPATCHER
- MESSAGE PROCESSING SUBSYSTEM
- SECURITY SUBSYSTEM
- ACCESS CONTROL SUBSYSTEM

MODULAR SNMPv3 ARCHITECTURE: MANAGER



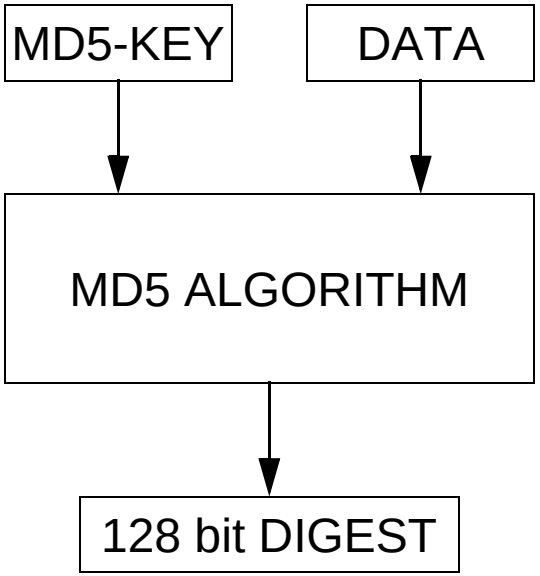
MODULAR SNMPv3 ARCHITECTURE: AGENT



SECURITY THREATS

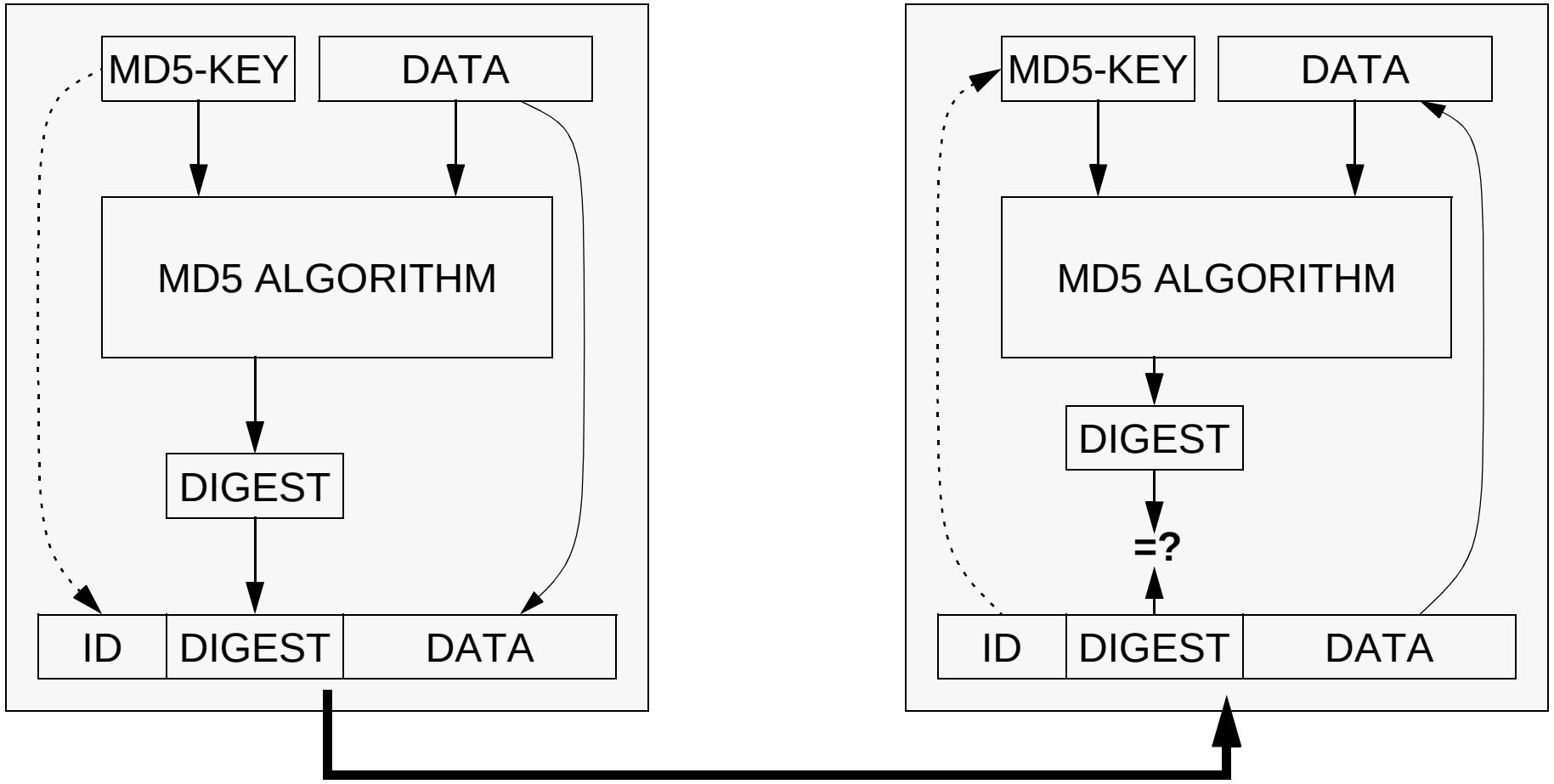
THREAT	ADDRESSED?	MECHANISM
MASQUERADE	YES	MD5 / SHA-1
REPLAY	YES	TIME STAMP
DISCLOSURE	YES	DES
INTEGRITY	YES	(MD5)
DENIAL OF SERVICE	NO	
TRAFFIC ANALYSIS	NO	

IDEA BEHIND MESSAGE DIGEST ALGORITHM (MD5)

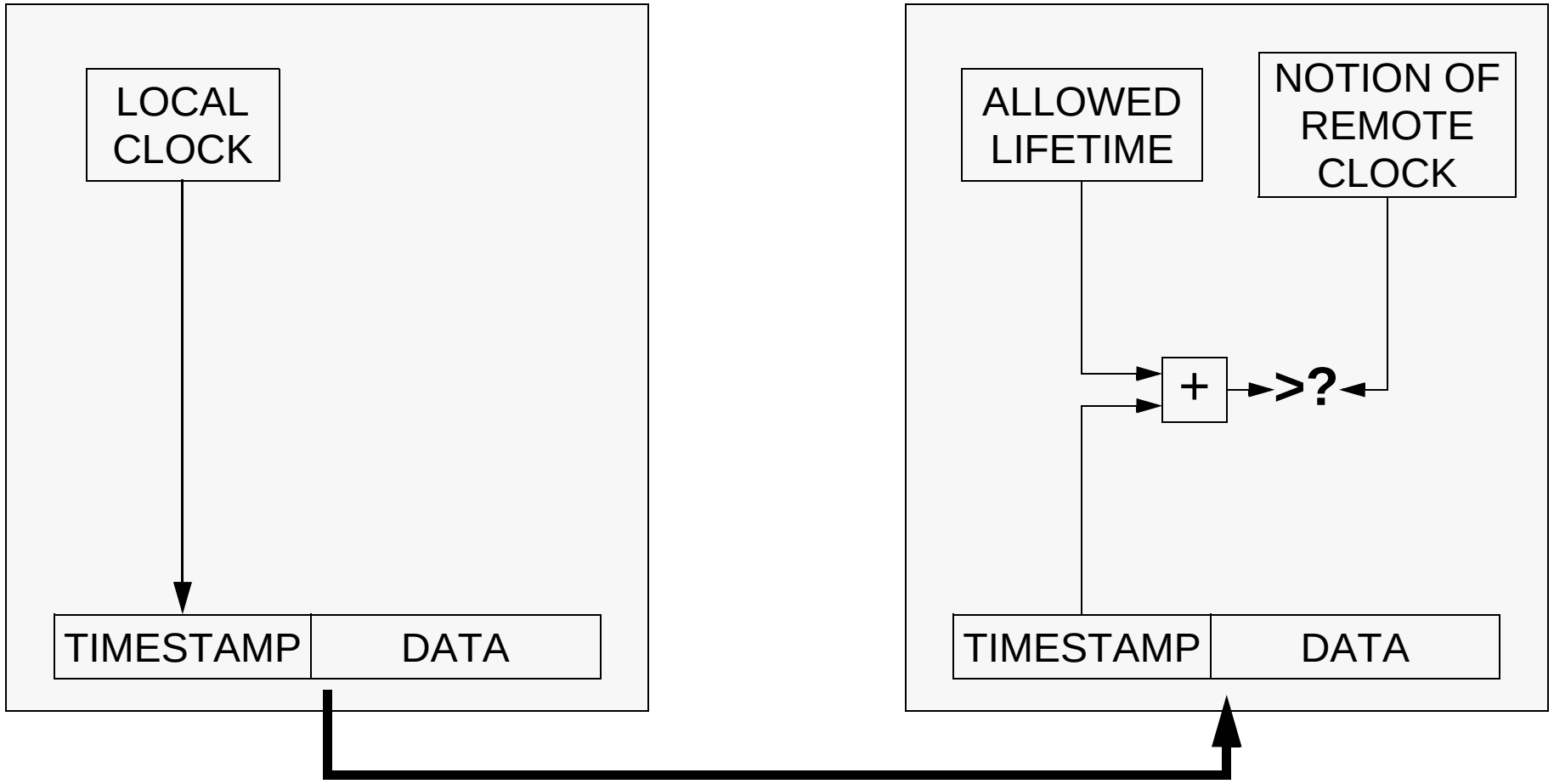


ADD THE DIGEST TO THE DATA
AND SEND THE RESULT

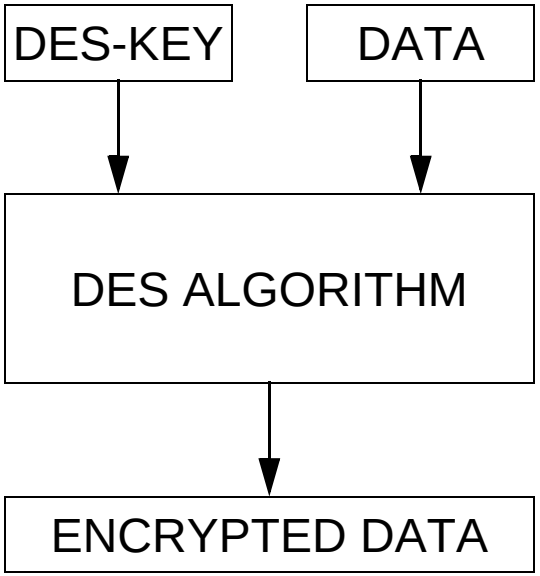
IDEA BEHIND AUTHENTICATION



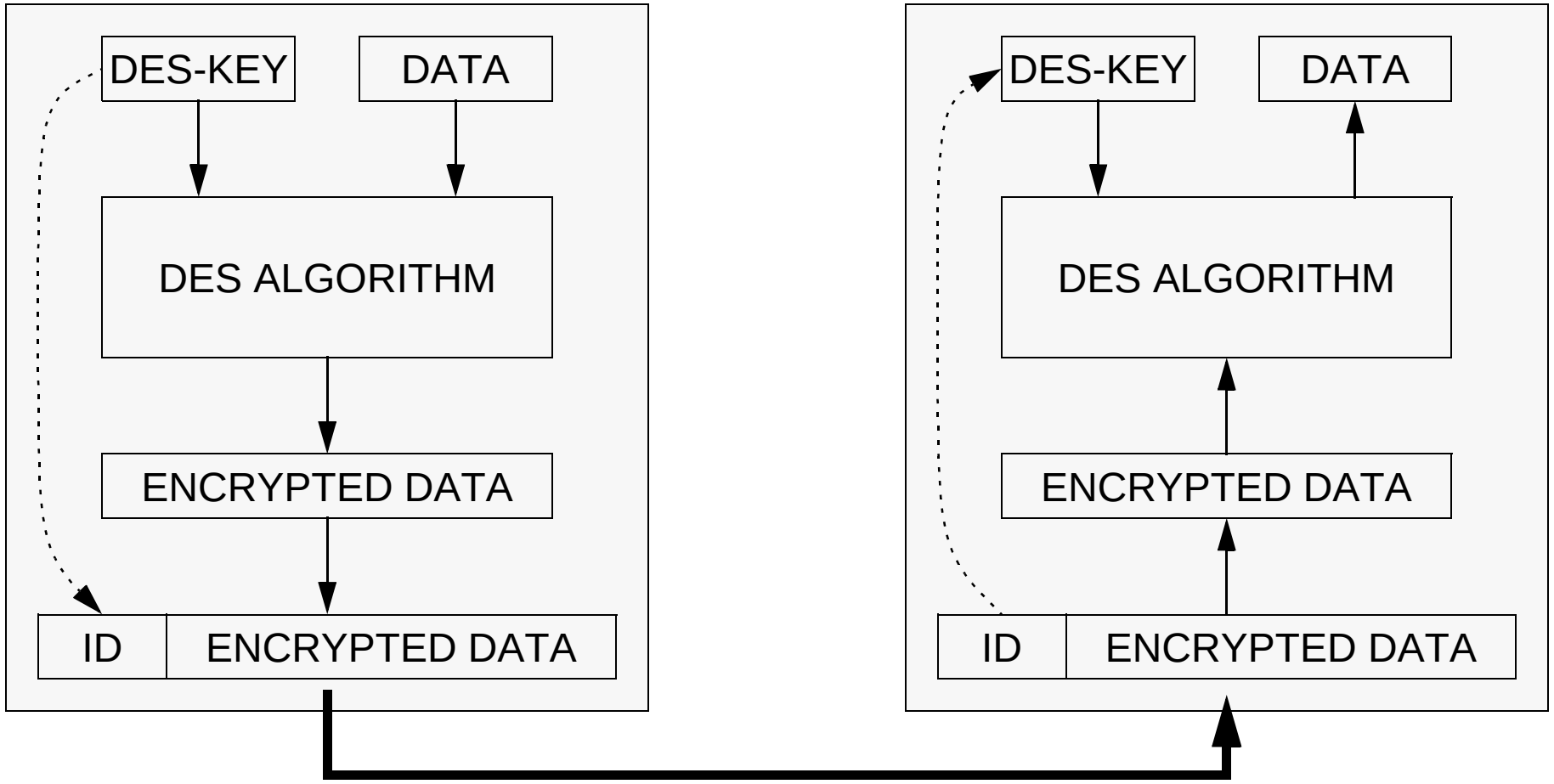
IDEA BEHIND REPLAY PROTECTION



IDEA BEHIND THE DATA ENCRYPTION STANDARD (DES)



IDEA BEHIND ENCRYPTION



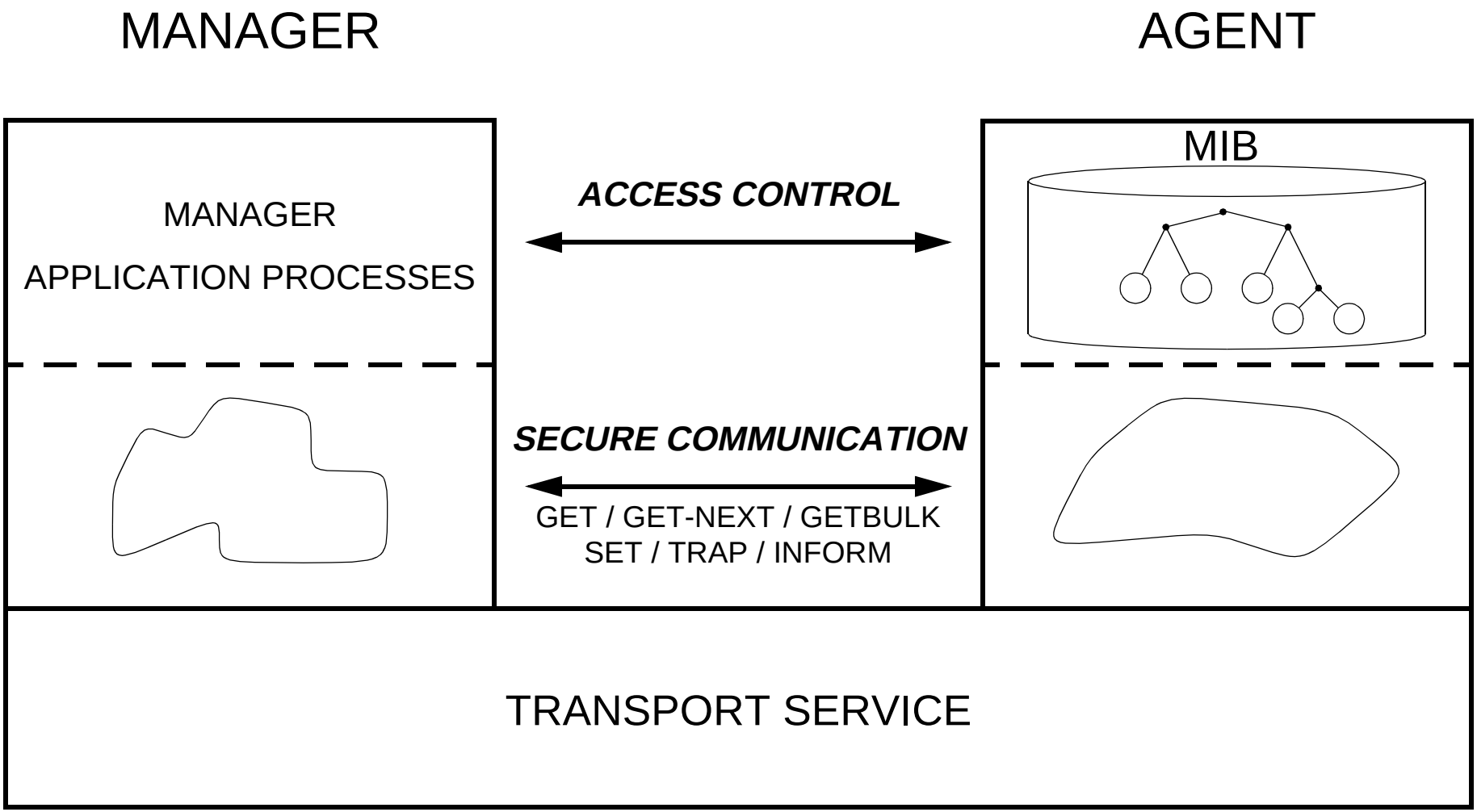
OTHER SECURITY ASPECTS

ACCESS CONTROL

MIB VIEWS

CONTEXTS

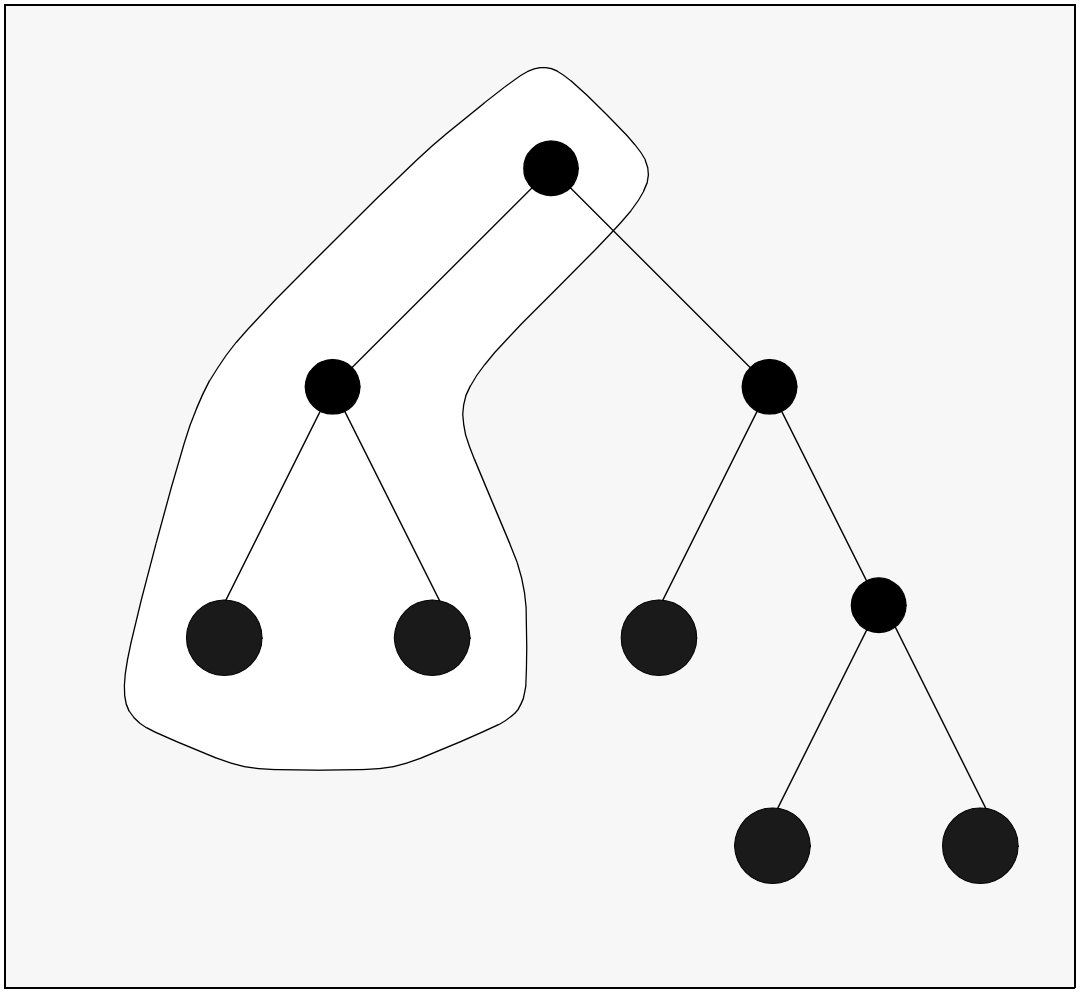
SECURE COMMUNICATION VERSUS ACCESS CONTROL



ACCESS CONTROL TABLES

MIB VIEW	ALLOWED OPERATIONS	ALLOWED MANAGERS	REQUIRED LEVEL OF SECURITY
•••	•••	•••	•••

MIB VIEWS



SNMPv3 IMPLEMENTATIONS

ACE*COMM

BMC Software

Epilogue

IBM

ISI

IWL

SNMP RESEARCH

TU of Braunschweig

University of Quebec

NEW INTEROPERABILITY TEST
AT INTEROP (OCTOBER 1998)

CONCLUSIONS