INTRODUCTION TO SNMP & INTERNET MANAGEMENT

TUTURIAL PRESENTED AT IM'99
BOSTON, USA
24 MAY 1999

AIKO PRAS
UNIVERSITY OF TWENTE
THE NETHERLANDS

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

OVERVIEW

BACKGROUND
- HISTORY
- GOALS
- STRUCTURE OF INTERNET MANAGEMENT
- STANDARDS

- STRUCTURE OF MANAGEMENT INFORMATION
  - SCALARS
  - TABLES

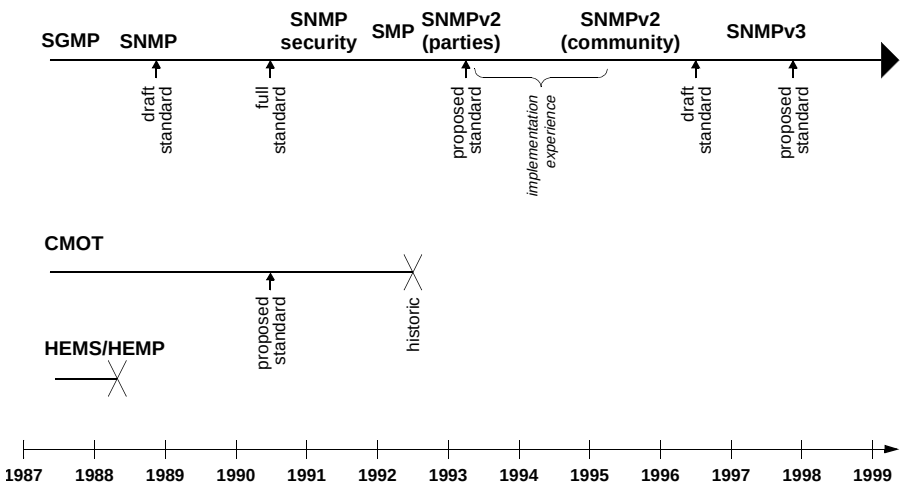
- MANAGEMENT INFORMATION BASE - II

- SIMPLE NETWORK MANAGEMENT PROTOCOL

OTHER MIBs
- REMOTE MONITORING

FURTHER INFORMATION

SNMP HISTORY



SNMP GOALS

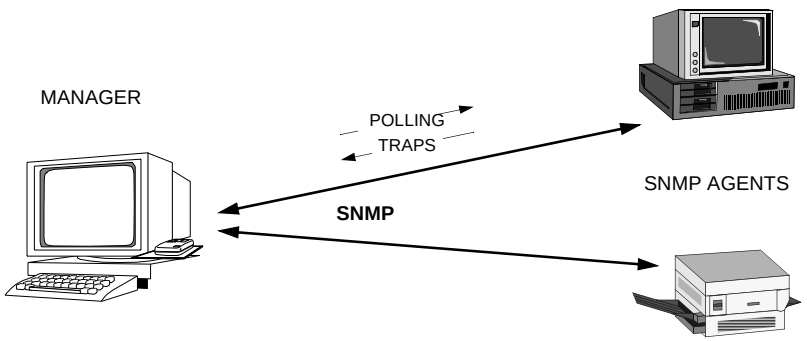
UBIQUITY
- PCs AND CRAYs

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

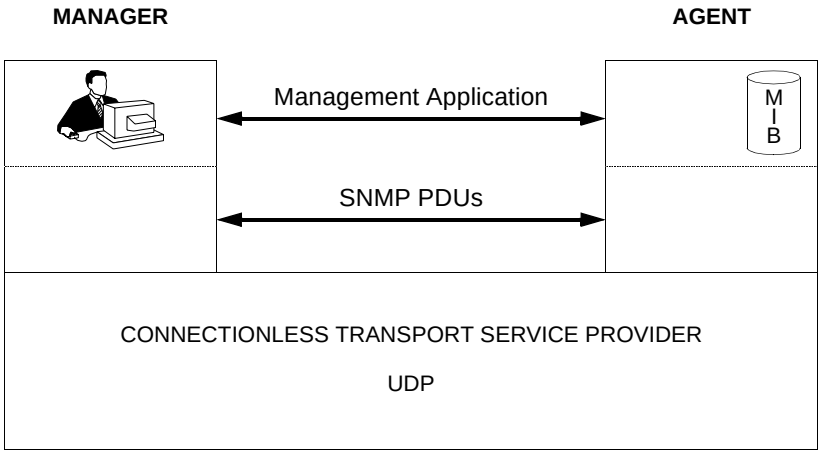
MANAGEMENT EXTENSIONS SHOULD BE POSSIBLE
- NEW MIBs

MANAGEMENT SHOULD BE ROBUST
- CONNECTIONLESS TRANSPORT

SNMP STRUCTURE



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

NEW VERSIONS: SNMPv2 & SNMPv3

SMI

STRUCTURE OF
MANAGEMENT INFORMATION
=
RFC 1155

CONCISE MIB DEFINITIONS
=
RFC 1212

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

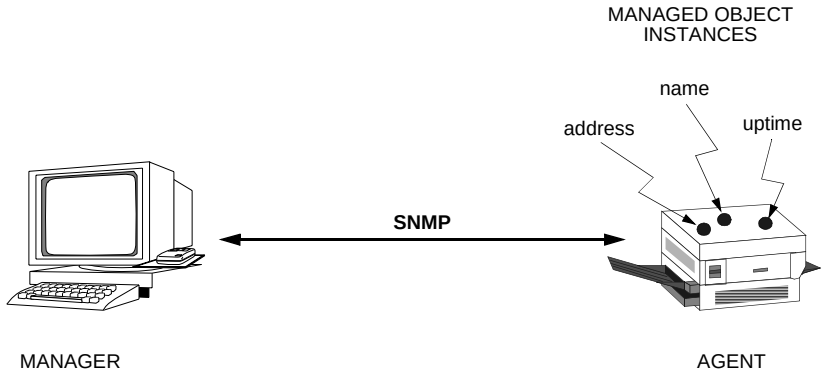
DEFINED IN TERMS OF
ASN.1
CONSTRUCTS

SMI: DATA TYPES FOR SCALARS

SIMPLE TYPES
- INTEGER
- OCTET STRING
- OBJECT IDENTIFIER
- NULL

APPLICATION-WIDE TYPES
- IpAddress
- NetworkAddress
- Counter
- Gauge
- TimeTicks
- Opaque

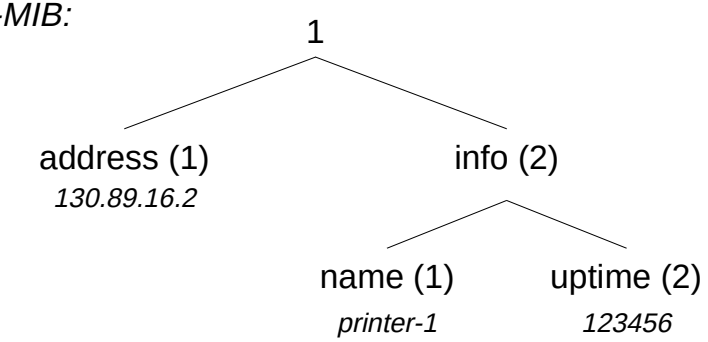
EXAMPLE OF SCALAR OBJECTS



OBJECT NAMING

INTRODUCE NAMING TREE

new-MIB:



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*

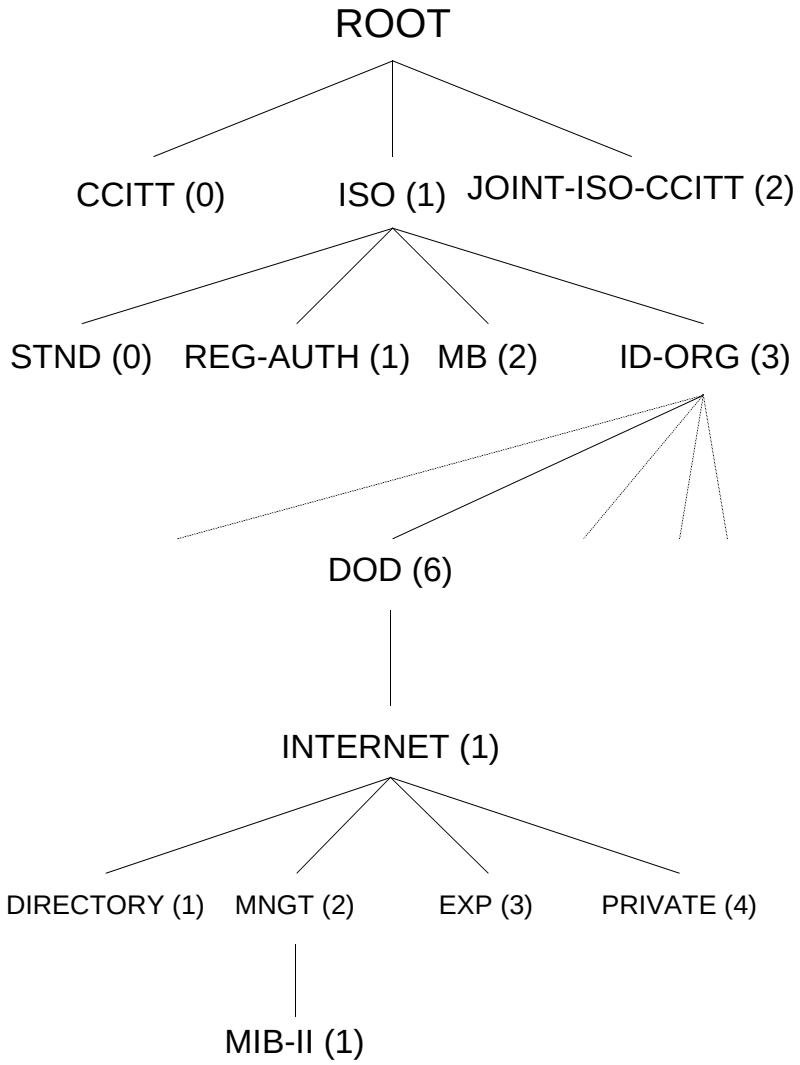
• info
Object ID = 1.2

• 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
  - NULL
  - IpAddress
  - NetworkAddress
  - Counter
  - Gauge
  - TimeTicks
  - Opaque
  - New Type
- ACCESS
  - read-only
  - read-write
  - write-only
  - not-accessible
- STATUS
  - mandatory
  - optional
  - obsolete
  - deprecated
- DESCRIPTION ""

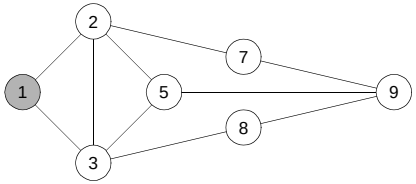
-- Definition of address

```
address     OBJECT-TYPE
    SYNTAX      IpAddress
    ACCESS      read-write
    STATUS      mandatory
    DESCRIPTION "The Internet address of this system"
    ::= {new-MIB  1}
```

TABLES

EXAMPLE: ROUTING TABLE

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



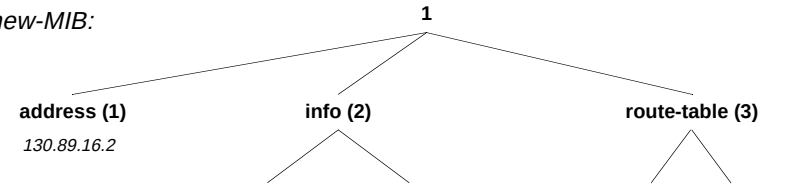
TO RETRIEVE INDIVIDUAL TABLE ENTRIES

EACH ENTRY SHOULD GET A NAME

NAMING OF TABLE ENTRIES - I

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

new-MIB:



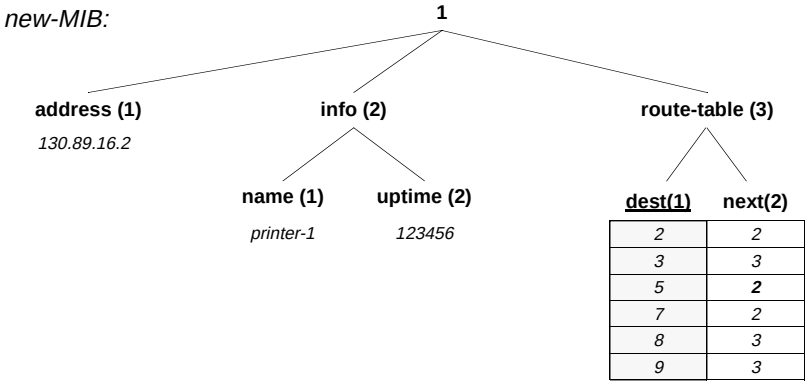
dest(1)	next(2)
2	*2*
3	*3*
5	*2*
7	*2*
8	***3***
9	*3*

EXAMPLE: THE VALUE OF *new-MIB route-table next 5* IS *3*

NAMING OF TABLE ENTRIES - II

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

new-MIB:



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

EXAMPLE: THE VALUE OF *new-MIB route-table next 5* IS *2*

TABLE INDEX - I

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 INDEX - II

AN INDEX NEED NOT BE AN INTEGER

route-table (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 INDEX - III

USE OF MULTIPLE INDEX FIELDS

X.C.I1.I2

OID of Table | Column number | Index value 1 | Index value 2

EXAMPLE:

1 = low costs
2 = high reliability

route-table (3)

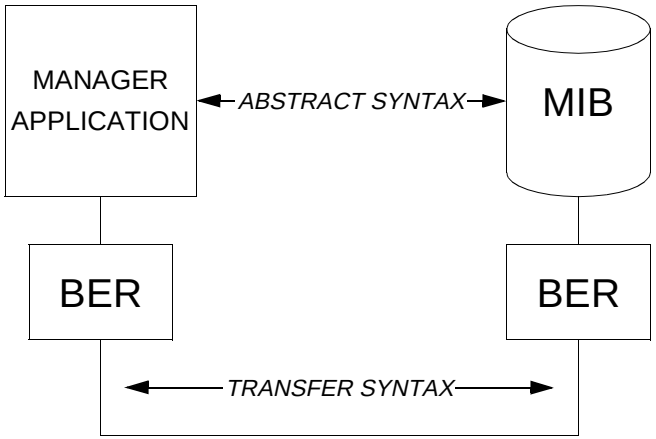
dest (1)	**policy (2)**	**next (3)**
130.89.16.23	*1*	*130.89.16.23*
130.89.16.23	*2*	*130.89.16.23*
130.89.19.121	*1*	*130.89.16.1*
192.1.23.24	*1*	*130.89.16.1*
192.1.23.24	*2*	*130.89.16.4*
193.22.11.97	*1*	*130.89.16.1*

1.3.3.192.1.23.24.1 => *130.89.16.1*

1.3.3.192.1.23.24.2 => *130.89.16.4*

ASN.1 & BER

MIB DEFINITIONS
ARE DESCRIBED IN TERMS OF
THE ASN.1 LANGUAGE



THE MAPPING FROM THIS
ABSTRACT SYNTAX
UPON A
TRANSFER SYNTAX
IS DEFINED BY THE
BASIC ENCODING RULES

BER

MIB-II

DEFINES THE VARIABLES
TO MANAGE THE
TCP/IP PROTOCOL STACK

170 VARIABLES

RFC 1213

ENHANCEMENT OF MIB-I

RFC 1156

MIB-II

• ESSENTIAL FOR
FAULT OR CONFIGURATION MANAGEMENT

• ONLY WEAK CONTROL OBJECTS

• SMALL NUMBER OF OBJECTS

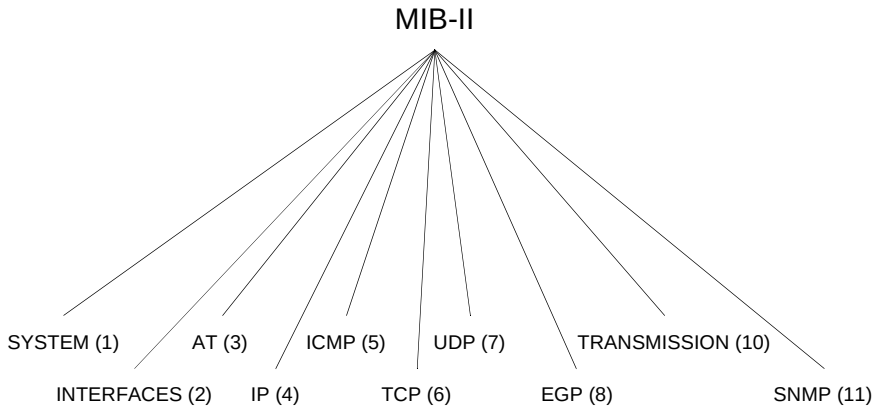
• AVOID REDUNDANCY

• EVIDENCE OF UTILITY

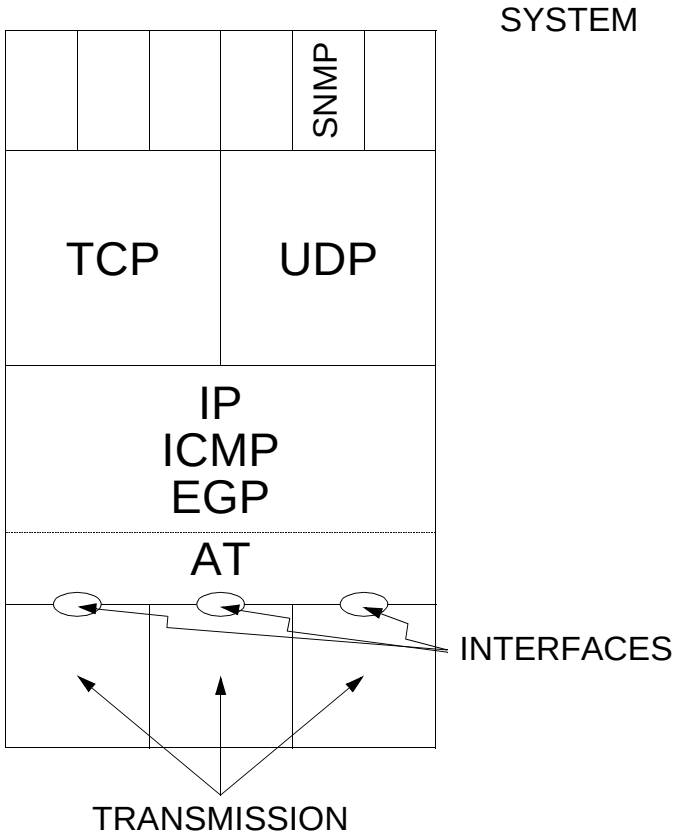
• DO NOT DISTURB NORMAL OPERATION

• NO IMPLEMENTATION SPECIFIC ISSUES

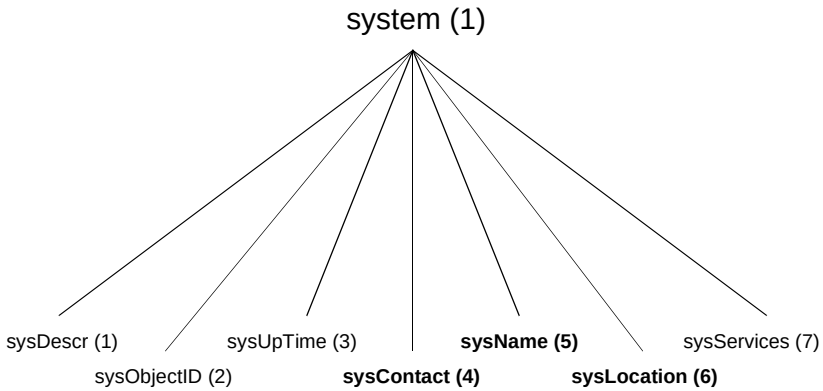
MIB-II



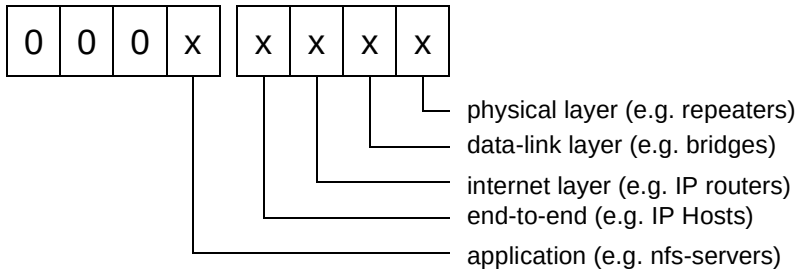
MIB-II GROUPS



SYSTEM GROUP



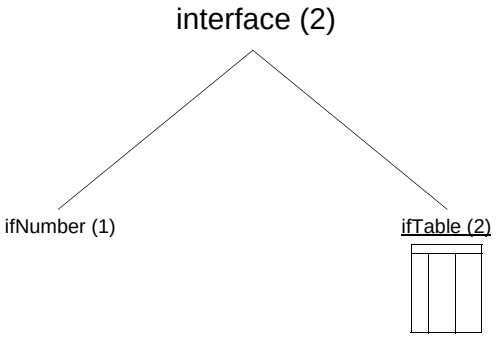
sysServices



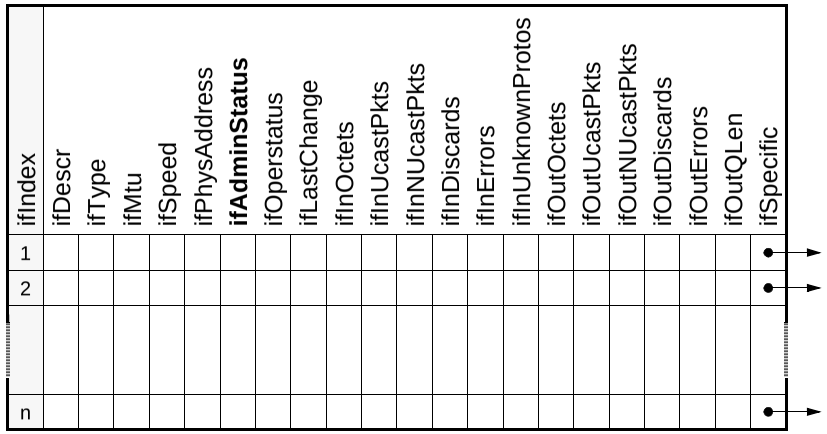
EXAMPLE

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)*

INTERFACES GROUP



ifTable



ifTable

- ifAdminStatus / ifOperStatus

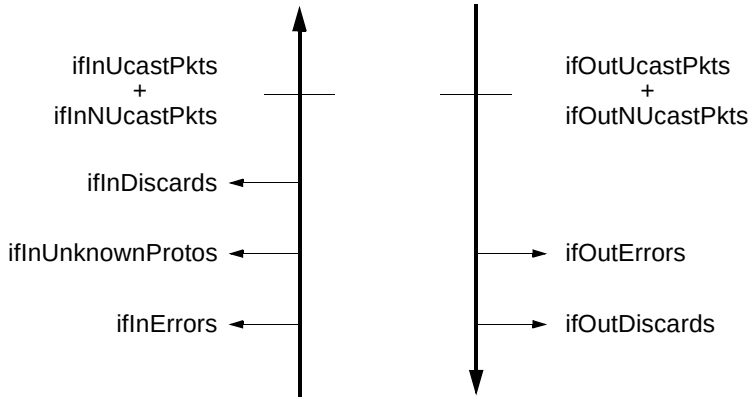
1 = up
2 = down
3 = testing

- ifType

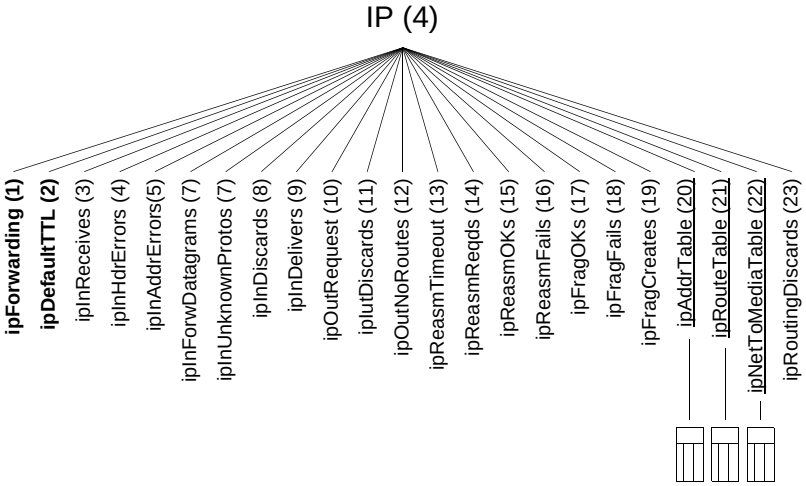
EXAMPLES:

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

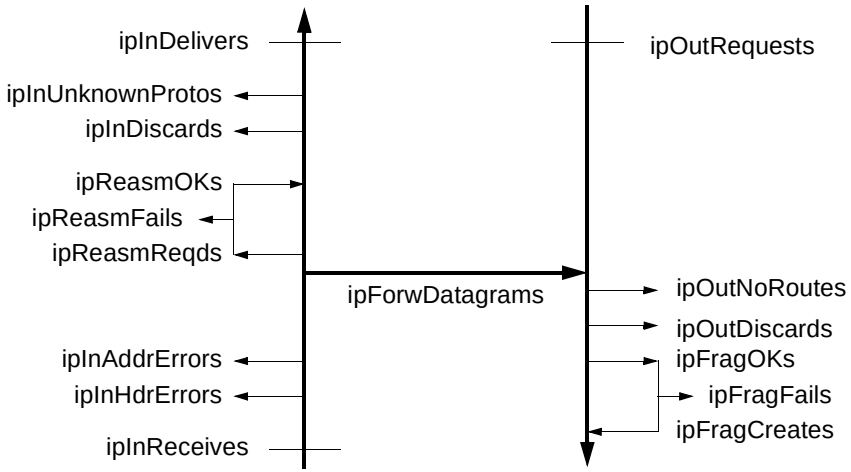
IF PACKET COUNT



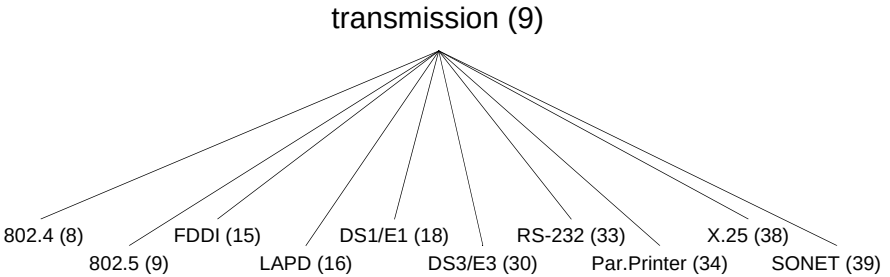
IP GROUP



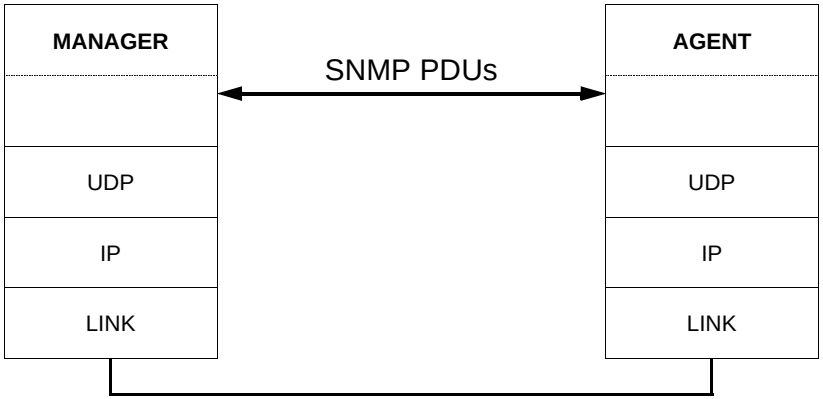
IP PACKET COUNT



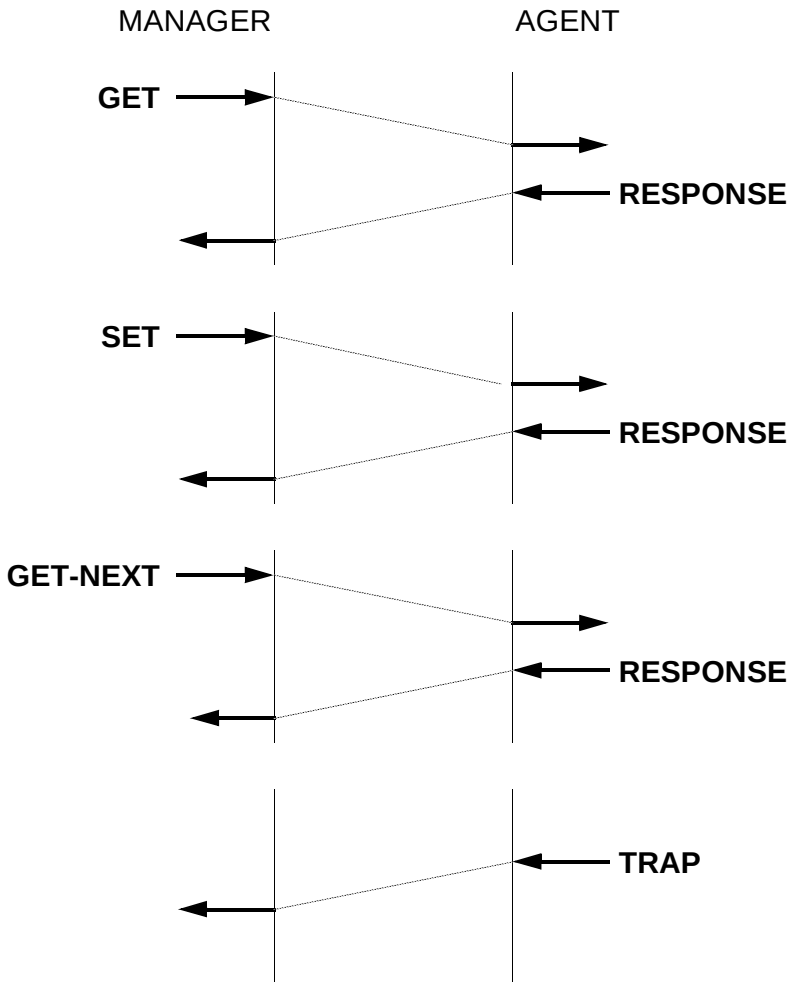
TRANSMISSION GROUP



SNMP PROTOCOL



OVERVIEW OF PDUs



MESSAGE & PDU STRUCTURE

variable bindings:

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

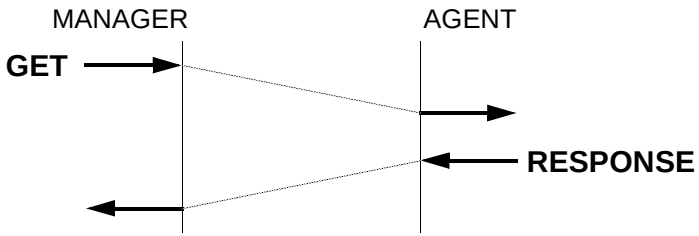
SNMP PDU:

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

⇩

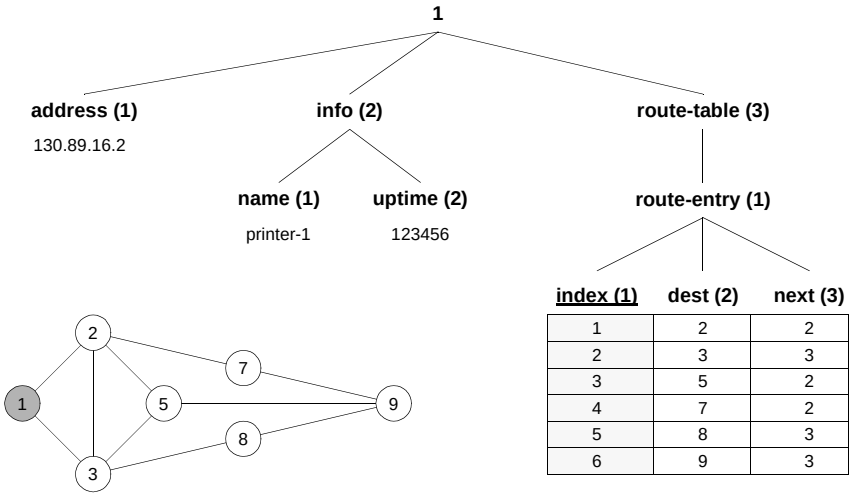
Result does not fit in Response PDU

• genErr

⇩

All other causes

EXAMPLE MIB



index (1)	dest (2)	next (3)
1	2	2
2	3	3
3	5	2
4	7	2
5	8	3
6	9	3

GET EXAMPLES

GET(1.1.0)
RESPONSE(1.1.0 => *130.89.16.2*)

GET(1.2.0)
RESPONSE(ErrorStatus = NoSuchName)

GET(1.1)
RESPONSE(ErrorStatus = NoSuchName)

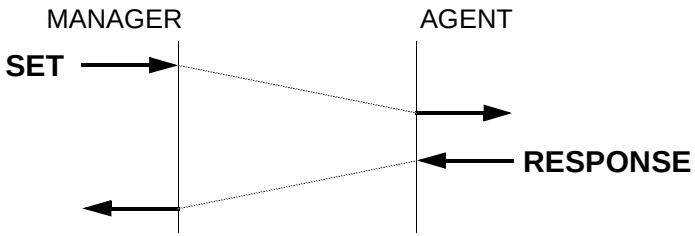
GET(1.1.0; 1.2.2.0)
RESPONSE(1.1.0 => *130.89.16.2*; 1.2.2.0 => *123456*)

GET(1.3.1.1.4)
RESPONSE(1.3.1.1.4 => *4*)

GET(1.3.1.3.4)
RESPONSE(1.3.1.3.4 => *2*)

GET(1.3.1.2.4, 1.3.1.3.4)
RESPONSE(1.3.1.2.4 => *7*, 1.3.1.3.4 => *2*)

SET



SET(1.2.1.0 => *my-printer*)
RESPONSE(noError; 1.2.1.0 => *my-printer*)

POSSIBLE ERRORS:

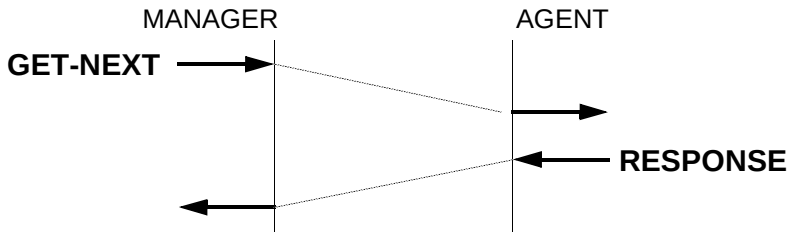
- noSuchName
- badValue
- genErr
- tooBig

SET

THE SET REQUEST IS
ATOMIC

SET(1.2.1.0 => *my-printer*, 1.2.2.0 => *0*)
RESPONSE(ErrorStatus = noSuchName; ErrorIndex = 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)
- genErr
- tooBig

GET-NEXT EXAMPLES

GET-NEXT(1.1.0)
RESPONSE(1.2.1.0 => *printer-1*)

GET-NEXT(1.2.1.0)
RESPONSE(1.2.2.0 => *123456*)

GET-NEXT(1.1)
RESPONSE(1.1.0 => *130.89.16.2*)

GET-NEXT(1.3.1.1.1)
RESPONSE(1.3.1.1.2 => *2*)

GET-NEXT(1.3.1.1.6)
RESPONSE(1.3.1.2.1 => *2*)

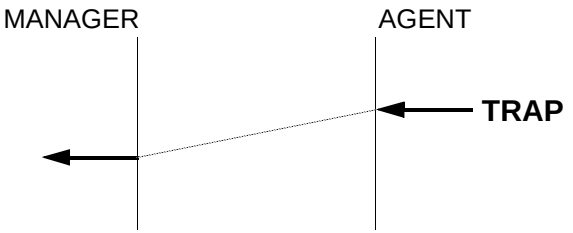
GET-NEXT(1.3.1.1.1; 1.3.1.2.1; 1.3.1.3.1)
RESPONSE(1.3.1.1.2 => *2*; 1.3.1.2.2 => *3*; 1.3.1.3.2 => *3*)

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*
1.3.1.1.1	*1*
1.3.1.1.2	*2*
1.3.1.1.3	*3*
1.3.1.1.4	*4*
1.3.1.1.5	*5*
1.3.1.1.6	*6*
1.3.1.2.1	*2*
1.3.1.2.2	*3*
1.3.1.2.3	*5*
1.3.1.2.4	*7*
1.3.1.2.5	*8*
1.3.1.2.6	*9*
1.3.1.3.1	*2*
1.3.1.3.2	*3*
•••	•••

TRAP



TRAP RECEPTION
IS NOT CONFIRMED
(THUS UNRELIABLE)

POLLING REMAINS NECESSARY

AGENTS MAY BE CONFIGURED
TO DISCARD TRAPS

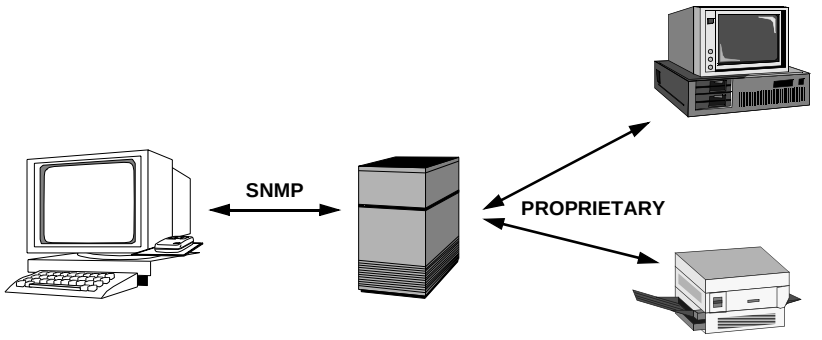
DEFINED TRAPS

- COLDSTART
- WARMSTART
- LINKDOWN
- LINKUP
- AUTHENTICATION FAILURE
- EGPNEIGHBOURLOSS
- ENTERPRISESPECIFICTRAP

TRAP - PDU FORMAT

ENTERPRISE
AGENT-ADDRESS
GENERIC-TRAP
SPECIFIC-TRAP
TIME-STAMP
VARIABLE-BINDINGS

PROXY MANAGEMENT



TRANSMISSION MIBs

Title	RFC	STATUS
Classical IP and ARP over ATM (IPOA)	2320	P
IEEE 802.12 Repeater Devices	2266	P
IEEE 802.3 Medium Attachment Units	2239	P
Interfaces Group MIB	2233	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
IEEE 802.5	1748	D
ATM	2515	P
SMDS	1694	D
Ethernet	2358	P
Frame Relay	1604	P
SONET / SDH	1595	P
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
DS3 / E3	2496	P
DS1 / E1	2495	P
X.25 Packet Layer	1382	P
X.25 LAPB	1381	P

NETWORK LAYER MIBs

Title	RFC	STATUS
IPv6	2465	P
Integrated Services - Guaranteed Service Ext.	2214	P
Integrated Services	2213	P
RSVP	2206	P
IP Forwarding Table	2096	P
RMON Version 2	2021	P
SNMPv2	2011	P
IP Mobility Support	2006	P
OSPF Version 2	1850	D
RMON	1757	D
RIP	1724	D
BGP Version 4	1657	D
Token Ring extensions to RMON	1513	P
Identification MIB	1414	P
BGP Version 3	1269	P
MIB-II	1213	S

TRANSPORT LAYER MIBs

Title	RFC	STATUS
UDP for IPv6	2454	P
TCP for IPv6	2452	P
User Datagram Protocol (UDP)	2013	P
Transmission Control Protocol (TCP)	2012	P

APPLICATION LAYER MIBs

Title	RFC	STATUS
System-Level M.O. for Applications	2287	P
Mail Monitoring	2249	P
Network Service Monitoring	2248	P
RDBMS	1697	P
DNS Resolver	1612	P
DNS Server	1611	P
X.500 Directory	1567	P
Host Resources	1514	P

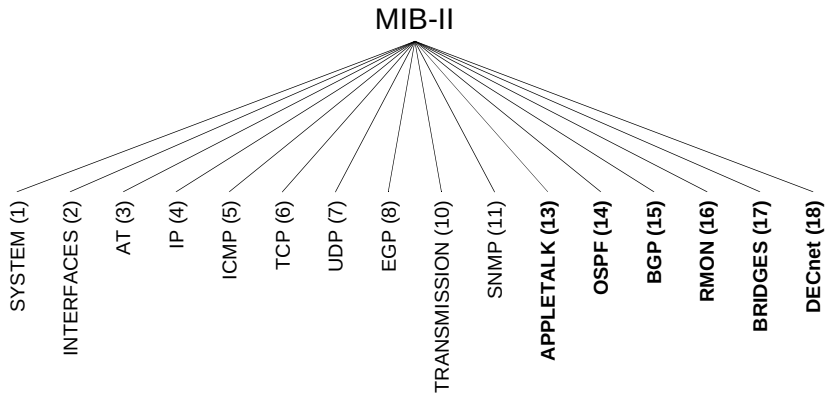
HARDWARE SPECIFIC MIBs

Title	RFC	STATUS
Entity	2037	P
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

VENDOR SPECIFIC MIBs

Title	RFC	STATUS
HPN	2238	P
DLUR	2232	P
APPN	2455	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
SNMP over IPX	1420	P
SNMP over Appletalk	1419	P

OTHER MIBs



RELATION BETWEEN MIBs - 1

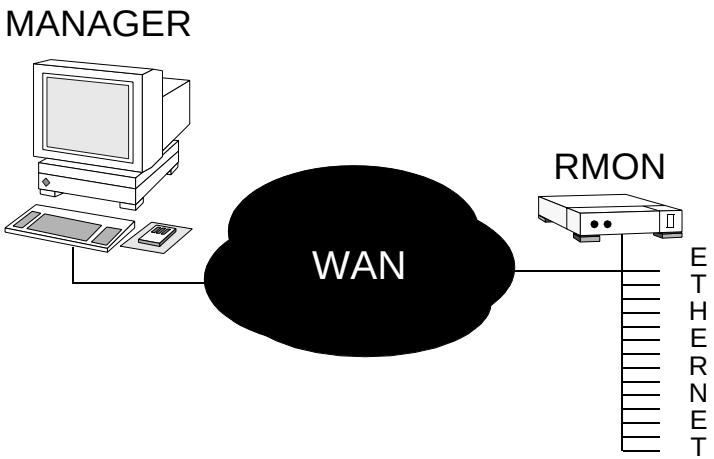
	MIB-II	HOST	REPEATER	BRIDGE	RMON
INTERFACE STATISTICS	✓				
IP, TCP & UDP STATISTICS	✓				
SNMP STATISTICS	✓				
HOST JOB COUNTS		✓			
HOST FILE SYSTEM INFORMATION		✓			
LINK TESTING			✓	✓	
NETWORK TRAFFIC STATISTICS			✓	✓	✓
TABLE WITH ALL MAC ADDRESSES			✓		✓
STATISTICS PER HOST			✓		✓

RELATION BETWEEN MIBs - 2

	MIB-II	HOST	REPEATER	BRIDGE	RMON
HISTORICAL STATISTICS					✓
SPANNING TREE PERFORMANCE				✓	
WIDE AREA LINK PERFORMANCE				✓	
TRESHOLDS FOR ANY VARIABLE					✓
CONFIGURABLE STATISTICS					✓
TRAFFIC MATRIX WITH ALL NODES					✓
'HOST TOP N' INFORMATION					✓
PACKET / PROTOCOL ANALYSIS					✓
DISTRIBUTED LOGGING					✓

REMOTE 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

HISTORY GROUP

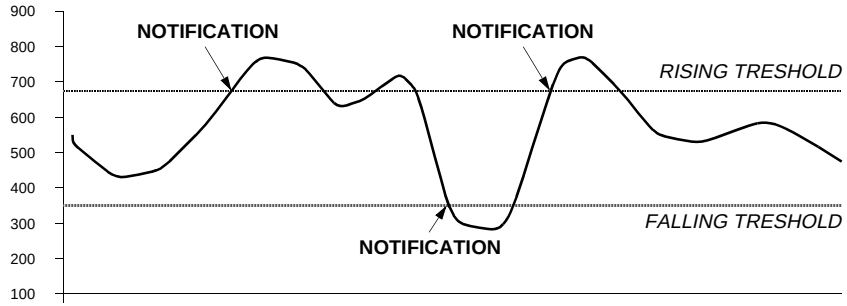
STORES INFORMATION OF STATISTICS GROUP
EXCEPT PACKET SIZE DISTRIBUTION

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

SNMP version 2

SMI version 2

SNMP version 3

AGENTX

DISTRIBUTED MANAGEMENT

IRTF SERVICE MANAGEMENT

IRTF NETWORK MANAGEMENT

COMMERCIAL SNMP SOFTWARE

BULL OPENMASTER
http://www.openmaster.com/ism

HP OPENVIEW
http://www.openview.hp.com/

SNMP RESEARCH
http://www.snmp.com/

CABLETRON SPECTRUM
http://www.cabletron.com/spectrum/

SUN SOLSTICE
http://www.sun.com/solstice/

TIVOLI
http://www.tivoli.com/

FREE SNMP SOFTWARE

CMU
http://www.net.cmu.edu/projects/snmp/

Scotty
http://wwwhome.cs.utwente.nl/~schoenw/scotty/

JMAPI
http://java.sun.com/products/JavaManagement/

Advent
http://www.adventnet.com/

ModularSnmp
http://www.teleinfo.uqam.ca/snmp/

FURTHER INFORMATION

WWW SERVERS

- IETF
http://www.ietf.org

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

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

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

FURTHER INFORMATION

BOOKS

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

• M.T. Rose
The Simple Book
2nd edition, Prentice Hall, 1994
ISBN: 0-131-77254-6

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