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/

Copyright © 1996 by Aiko Pras, Hengelo, The Netherlands
All rights reserved.
No part of these sheets may be used, reproduced, stored in a retrieval system or transmitted,
in any form or by any means, without obtaining written permission of the author.
CONTENTS

• IETF / SNMP INTRO

• SNMP version 2

• COMPARISON TO CMIP / CMOL
  • MIBs
  • RMON

• NEW DEVELOPMENTS

• FURTHER INFORMATION
IETF STANDARDIZATION

WORKING DOCUMENT

PROPOSED STANDARD

*implementation experience must be obtained*

after a maximum of 2 years

DRAFT STANDARD

*several independent implementations must interwork*

after a maximum of 4 years

FULL STANDARD

HISTORICAL
SNMPv1 STRUCTURE

MANAGEMENT
APPLICATION

TRANSPORT SERVICE

manager

to

agent

GET / GET-NEXT

SET

TRAP

MIB
### SNMPv1 MESSAGE & PDU STRUCTURE

**variable bindings:**

<table>
<thead>
<tr>
<th>NAME 1</th>
<th>VALUE 1</th>
<th>NAME 2</th>
<th>VALUE 2</th>
<th>...</th>
<th>...</th>
<th>NAME n</th>
<th>VALUE n</th>
</tr>
</thead>
</table>

**SNMP PDU:**

<table>
<thead>
<tr>
<th>PDU TYPE*</th>
<th>REQUEST ID</th>
<th>ERROR STATUS</th>
<th>ERROR INDEX</th>
<th>VARIABLE BINDINGS</th>
</tr>
</thead>
</table>

**SNMP message:**

<table>
<thead>
<tr>
<th>VERSION</th>
<th>COMMUNITY</th>
<th>SNMP PDU</th>
</tr>
</thead>
</table>

* PDU TYPE: Request or Response
PROXY MANAGEMENT

MANAGER  PROXY AGENT  NON-SNMP AGENT
SNMPv2

APRIL 1993:
• PROPOSED STANDARD
• RFC 1441 - RFC 1452
• PARTY BASED SECURITY MODEL

JUNE 1995:
• PARTY BASED MODEL REJECTED
• NEW PROPOSALS APPEARED

JANUARY 1996:
• SNMPv2c 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

- GET / GET-NEXT
- TRAP / REPORT
- GET-BULK
- SET
- INFORM

TOP LEVEL MANAGER

INTERMEDIATE LEVEL MANAGER

MIB

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)

Manager

Management Application

Get / Get-Next / Get-Bulk

Set

Trap / Report

Transport Service

Agent

MIB

Agent ID

Agent Boots

Agent Time

User Name

Auth. Key

Priv. Key
USEC: SECURE TRANSFER OF MANAGEMENT PDUs (3)

Manager

**Management Application**

- User name
- Auth. Key
- Priv. Key

**Transport Service**

Agent

**MIB**

- Agent ID
- Agent boots
- Agent time

Actions:

- GET / GET-NEXT / GET-BULK
- SET
- TRAP / REPORT
USEC: SECURE TRANSFER OF MANAGEMENT PDUs (4)

manager

SNMP PDU

USER NAME
AUTH. KEY
PRIV. KEY

AGENT ID
AGENT BOOTS
AGENT TIME

DIGEST
USER NAME
AGENT TIME
AGENT BOOTS
AGENT ID
QoS
SECURITY
VERSION

ENCRIPTED SNMP PDU
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
<table>
<thead>
<tr>
<th></th>
<th>CMIP</th>
<th>SNMP</th>
</tr>
</thead>
<tbody>
<tr>
<td>model</td>
<td>event based</td>
<td>polling based</td>
</tr>
<tr>
<td>information approach</td>
<td>object oriented</td>
<td>variable oriented</td>
</tr>
<tr>
<td>complexity</td>
<td>agent is complex</td>
<td>agent is simple</td>
</tr>
<tr>
<td>state information</td>
<td>kept by agent</td>
<td>kept by manager</td>
</tr>
<tr>
<td>underlying service</td>
<td>CO - reliable</td>
<td>CL - unreliable</td>
</tr>
<tr>
<td>efficiency</td>
<td>good</td>
<td>acceptable</td>
</tr>
<tr>
<td>implementation</td>
<td>difficult</td>
<td>simple</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(V2 is more difficult)</td>
</tr>
</tbody>
</table>
## CMIP versus SNMP - 2

<table>
<thead>
<tr>
<th></th>
<th>CMIP</th>
<th>SNMP</th>
</tr>
</thead>
<tbody>
<tr>
<td>retrieves</td>
<td>objects</td>
<td>scalars</td>
</tr>
<tr>
<td>many items</td>
<td>multiple replies</td>
<td>error: tooBIG</td>
</tr>
<tr>
<td>object selection</td>
<td>scoping &amp; filtering</td>
<td>-</td>
</tr>
<tr>
<td>synchronization</td>
<td>atomic &amp; best effort</td>
<td>atomic</td>
</tr>
<tr>
<td>events / traps</td>
<td>confirmed &amp; unconfirmed</td>
<td>unconfirmed</td>
</tr>
<tr>
<td>actions</td>
<td>possible</td>
<td>via ‘trick’</td>
</tr>
<tr>
<td></td>
<td><strong>CMIP</strong></td>
<td><strong>SNMP</strong></td>
</tr>
<tr>
<td>----------------</td>
<td>-------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>security</td>
<td>via underlying services</td>
<td>- authentication / encryption / ACL-lists</td>
</tr>
<tr>
<td>management functions</td>
<td>many</td>
<td>none</td>
</tr>
<tr>
<td>approach</td>
<td>object oriented</td>
<td>variable oriented</td>
</tr>
<tr>
<td>ASN.1</td>
<td>full support</td>
<td>subset</td>
</tr>
<tr>
<td>naming structure</td>
<td>flexible</td>
<td>simple</td>
</tr>
</tbody>
</table>
CMOL versus SNMP

CMOL IS COMPARIBLE TO CMIP

CMOL OPERATES OVER LLC

CMOL CAN NOT OPERATE OVER ROUTERS

CMOL: FEW IMPLEMENTATIONS
<table>
<thead>
<tr>
<th>n</th>
<th>2</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>ifIndex</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ifDescr</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ifType</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ifMtu</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ifSpeed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ifPhysAddress</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>ifAdminStatus</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ifOperStatus</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ifLastChange</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ifInOctets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ifInUcastPkts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ifInNUcastPkts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ifInDiscards</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ifInErrors</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ifInUnknownProtos</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ifOutOctets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ifOutUcastPkts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ifOutNUcastPkts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ifOutDiscards</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ifOutErrors</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ifOutQLen</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>ifSpecific</strong></td>
</tr>
</tbody>
</table>
MIB-II IF PACKET COUNT

IfInUcastPkts + IfInNUcastPkts

IfInDiscards

IfInUnknownProtos

IfInErrors

IfOutUcastPkts + IfOutNUcastPkts

IfOutErrors

IfOutDiscards
# OVERVIEW LAN SPECIFIC MIBs

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

IEEE

802.1
802.2
802.3
802.4
802.5
802.6
802.7
802.8
802.9
802.10
802.11
802.12
802.14

IETF

Bridge MIB
Hub MIB
Interfaces MIB
RMON
100VG-AnyLAN
REMOTE NETWORK MONITORING

RMON

MANAGER

WAN

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

<table>
<thead>
<tr>
<th>WELL-FORMED PACKETS</th>
<th>64 to 1518</th>
<th>&gt;1518 bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>undersize</td>
<td>GOOD!</td>
<td>oversize</td>
</tr>
<tr>
<td>fragments</td>
<td>CRC or alignment errors</td>
<td>jabber</td>
</tr>
</tbody>
</table>

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

NOTIFICATION

RISING TRESHOLD

FALLING TRESHOLD

NOTIFICATION

NOTIFICATION
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://wwttios.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