OVERVIEW

• HISTORY OF INTERNET MANAGEMENT
  • SNMPv1
  • SNMPv2
  • SNMPv3

• DISTRIBUTED MANAGEMENT

• EXTENSIBLE AGENT TECHNOLOGY

• POLICY BASED MANAGEMENT

• IRTF NETWORK MANAGEMENT RESEARCH GROUP (NMRG)

• FURTHER INFORMATION
SNMP HISTORY

SNMPv1: 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
STRUCTURE

MANAGER

UDP

IP

LINK

SNMP PDUs

AGENT

MIB

UDP

IP

LINK

OVERVIEW OF PDUs

MANAGER

AGENT

MIB

GET

GET-NEXT

RESPONSE

RESPONSE

MANAGER

AGENT

MIB

SET

RESPONSE

MIB

TRAP

RESPONSE
**SNMPv1 RFCs**

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

---

**SNMPv2**

WORK STARTED IN 1993

IMPROVED INFORMATION MODEL (SMIv2)
• ADDITIONAL DATA TYPES
• TEXTUAL CONVENTIONS (E.G. ROW STATUS)
  • NOTIFICATIONS

IMPROVED COMMUNICATION MODEL
• TRAPS HAVE SAME FORMAT AS OTHER PDUS
• BETTER PERFORMANCE (GET-BULK PDU)
• ADDITIONAL ERROR CODES FOR SETS

INDEPENDENCE OF UNDERLYING TRANSPORT
• MIB-II SPLIT INTO MODULES

HIERARCHIES AND SECURITY: ...
HIERARCHIES: ORIGINAL IDEA

MANAGER TO MANAGER (M2M) MIB

- STANDARD MIB APPROACH
- LIMITED FUNCTIONALITY

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)
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 RFCs

INFORMATION MODEL:
• STANDARD
• RFC2578, RFC2579, RFC2580

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
SNMPv3

HAS A MODULAR ARCHITECTURE

ALLOWS SECURE COMMUNICATION

PROVIDES ACCESS CONTROL

HAS MANY IMPLEMENTATIONS

<table>
<thead>
<tr>
<th>SNMP ENTITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP APPLICATIONS</td>
</tr>
<tr>
<td>COMMAND GENERATOR</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SNMP ENGINE</th>
</tr>
</thead>
<tbody>
<tr>
<td>DISPATCHER</td>
</tr>
</tbody>
</table>
## Secure Communication

<table>
<thead>
<tr>
<th>Threat</th>
<th>Addressed?</th>
<th>Mechanism</th>
</tr>
</thead>
<tbody>
<tr>
<td>Masquerade</td>
<td>Yes</td>
<td>MD5 / SHA-1</td>
</tr>
<tr>
<td>Replay</td>
<td>Yes</td>
<td>Time Stamp</td>
</tr>
<tr>
<td>Disclosure</td>
<td>Yes</td>
<td>DES</td>
</tr>
<tr>
<td>Integrity</td>
<td>Yes</td>
<td>(MD5)</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Traffic Analysis</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

## Access Control Tables

<table>
<thead>
<tr>
<th>MIB View</th>
<th>Allowed Operations</th>
<th>Allowed Managers</th>
<th>Required Level of Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Table</td>
<td>SET</td>
<td>John</td>
<td>Authentication Encryption</td>
</tr>
<tr>
<td>Interface Table</td>
<td>GET / GETNEXT</td>
<td>John, Paul</td>
<td>Authentication</td>
</tr>
<tr>
<td>Systems Group</td>
<td>GET / GETNEXT</td>
<td>George</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td></td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td></td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td></td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td></td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>


IMPLEMENTATIONS

ACE*COMM
AdventNet
BMC Software
Cisco
Epilogue
Gambit communications
Halcyon
IBM
ISI
IWL
MG-SOFT
MultiPort Corporation
SimpleSoft
SNMP Research

SNMP++
TU of Braunschweig
UCD
University of Quebec

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

- 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

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 NECESSARY

• DIFFERENT SCRIPT LANGUAGES
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

EXTENSIBLE AGENTS

MASTER AGENT
• PROTOCOL OPERATIONS
• ENCODING

UDP
HISTORY

SMUX (RFC 1227)
SNMP MULTIPLEXING PROTOCOL

DPI (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 (RFC2257)

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

IRTF NMRG

EFFICIENT TRANSFER OF BULK MANAGEMENT DATA
• SNMP OVER TCP
• COMPRESSION
• GET-SUBTREE OPERATOR

SMI NEXT GENERATION
• INDEPENDENT FROM OTHER EXTERNAL STANDARDS
• BASED ON AUGMENTED BNF
• MORE DATA TYPES
• EASIER TO PARSE

ACTIVE MANAGEMENT
• ALLOW MANAGEMENT FUNCTIONS WITHIN MIBs
• CAN BE INTEGRATED WITH SMIV2
• CAN BE USED OVER SNMP OR COPS
  • POWERFUL NEW IDEA!
FURTHER INFO: 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/

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

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