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

<table>
<thead>
<tr>
<th>TO:</th>
<th>VIA:</th>
<th>STATUS:</th>
</tr>
</thead>
<tbody>
<tr>
<td>130.89.16.4</td>
<td>130.89.1.1</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>130.89.17.6</td>
<td>130.89.1.1</td>
<td>NOT READY</td>
</tr>
<tr>
<td>130.89.18.2</td>
<td>130.89.1.4</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>130.89.18.7</td>
<td>130.89.1.4</td>
<td>ACTIVE</td>
</tr>
</tbody>
</table>
**ROW STATUS STATE DIAGRAM**

- **status column does not exist**: 
  - 1. set status column to createAndGo
  - 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

- **status column is active**: 
  - 1. noError
  - 2.
  - 3.
  - 4.
  - 5.
  - 6.

- **status column is notReady**: 
  - 1.
  - 2.
  - 3.
  - 4.
  - 5.
  - 6.

- **status column is notInService**: 
  - 1.
  - 2.
  - 3.
  - 4.
  - 5.
  - 6.
## ADDITIONAL ERROR CODES FOR SETS

<table>
<thead>
<tr>
<th>SNMPv1</th>
<th>SNMPv2</th>
</tr>
</thead>
<tbody>
<tr>
<td>badValue</td>
<td>wrongValue</td>
</tr>
<tr>
<td>badValue</td>
<td>wrongEncoding</td>
</tr>
<tr>
<td>badValue</td>
<td>wrongType</td>
</tr>
<tr>
<td>badValue</td>
<td>wrongLength</td>
</tr>
<tr>
<td>badValue</td>
<td>inconsistentValue</td>
</tr>
<tr>
<td>noSuchName</td>
<td>noAccess</td>
</tr>
<tr>
<td>noSuchName</td>
<td>notWritable</td>
</tr>
<tr>
<td>noSuchName</td>
<td>noCreation</td>
</tr>
<tr>
<td>noSuchName</td>
<td>inconsistentName</td>
</tr>
<tr>
<td>genErr</td>
<td>resourceUnavailable</td>
</tr>
<tr>
<td>genErr</td>
<td>CommitFailed</td>
</tr>
<tr>
<td>genErr</td>
<td>undoFailed</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
## ADDITIONAL DATA TYPES

### SMIPv1

- INTEGER
- OCTET STRING
- OBJECT IDENTIFIER
- INTEGER
- GAUGE
- COUNTER
- TIMETICKS
- IPADDRESS
- OPAQUE
- NETWORKADDRESS

### SMIPv2

- INTEGER
- OCTET STRING
- OBJECT IDENTIFIER
- INTEGER32
- UNSIGNED32
- GAUGE32
- COUNTER32
- COUNTER64
- TIMETICKS
- IPADDRESS
- OPAQUE
- BITS
- NETWORKADDRESS
NOTIFICATIONS

SNMPv1:
- COLD START
- WARM START
- LINK DOWN
- LINK UP
- AUTHENTICATION 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**

![Diagram of manager-agent communication]

**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
)

**MANAGER**

**AGENT**

**RESPONSE**
GET-BULK PDU

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

RESPONSE (N-TIMES
  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)

  3rd LEXICOGRAPHICAL SUCCESSOR
  VariableBinding-(N+1); ... ; VariableBinding-(N+R)

  ...)

  Mth LEXICOGRAPHICAL SUCCESSOR

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

  ...)

  Mth LEXICOGRAPHICAL SUCCESSOR

M-TIMES
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 NECESSARY

• 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

- **PDU DISPATCHER**
  - COMMAND GENERATOR
  - NOTIFICATION ORIGINATOR
  - NOTIFICATION RECEIVER

- **MESSAGE DISPATCHER**
  - MESSAGE PROCESSING SUBSYSTEM
    - SNMPv1
    - SNMPv2C
    - SNMPv3
    - OTHER

- **SECURITY SUBSYSTEM**
  - COMMUNITY BASED SECURITY MODEL
  - USER BASED SECURITY MODEL
  - OTHER SECURITY MODEL
MODULAR SNMPv3 ARCHITECTURE: AGENT
## SECURITY THREATS

<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>
IDEA BEHIND MESSAGE DIGEST ALGORITHM (MD5)

1. MD5-KEY
2. DATA

MD5 ALGORITHM

128 bit DIGEST

ADD THE DIGEST TO THE DATA AND SEND THE RESULT
IDEA BEHIND AUTHENTICATION

MD5-KEY  DATA

MD5 ALGORITHM

DIGEST

ID  DIGEST  DATA

MD5-KEY  DATA

MD5 ALGORITHM

DIGEST

ID  DIGEST  DATA

ID  DIGEST  DATA

=?
IDEA BEHIND REPLAY PROTECTION

- LOCAL CLOCK
- ALLOWED LIFETIME
- NOTION OF REMOTE CLOCK
- TIMESTAMP
- DATA
- +
- >?

TIMESTAMP + DATA
IDEA BEHIND THE DATA ENCRYPTION STANDARD (DES)

DES-KEY

DATA

DES ALGORITHM

ENCRYPTED DATA
IDEA BEHIND ENCRYPTION

DES-KEY \rightarrow DATA \rightarrow DES ALGORITHM \rightarrow ENCRYPTED DATA \rightarrow ID \rightarrow ENCRYPTED DATA

DES-KEY \rightarrow DATA \rightarrow DES ALGORITHM \rightarrow ENCRYPTED DATA \rightarrow ID \rightarrow ENCRYPTED DATA
OTHER SECURITY ASPECTS

ACCESS CONTROL

MIB VIEWS

CONTEXTS
SECURE COMMUNICATION VERSUS ACCESS CONTROL

MANAGER

APPLICATION PROCESSES

AGENT

MIB

TRANSPORT SERVICE

SECURE COMMUNICATION

GET / GET-NEXT / GETBULK
SET / TRAP / INFORM

ACCESS CONTROL

SNMPv3
## 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></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>

...
MIB VIEWS

SNMPv3
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)