Network Management (SNMP)

Raj Jain

Raj Jain is now at
Washington University in Saint Louis
Jain@cse.wustl.edu
http://www.cse.wustl.edu/~jain/
Overview

- Network Management
- SNMP
- Management information base (MIB)
- ASN.1 Notation
Network Management

- Management = Initialization, Monitoring, Control
- Manager, Agents, and Management Information Base (MIB)
SNMP

- Based on Simple Gateway Management Protocol (SGMP)
- SNMP = Simply Not My Problem [Rose]
- Simple Network Management Protocol
- Only Five commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>get-request</td>
<td>Fetch a value</td>
</tr>
<tr>
<td>get-next-request</td>
<td>Fetch the next value (in a tree)</td>
</tr>
<tr>
<td>get-response</td>
<td>Reply to a fetch operation</td>
</tr>
<tr>
<td>set-request</td>
<td>Store a value</td>
</tr>
<tr>
<td>trap</td>
<td>An event</td>
</tr>
</tbody>
</table>
Management Information Base

- MIBs follow a fixed naming and structuring convention
  ⇒ Structure of Management Information (SMI)
- All names are unique
- All nodes of the name tree are assigned numeric values by standards authorities
  iso.org.dod.internet.mgmt.mib.ip.ipInReceives
  1.3.6.1.2.1.4.3
- Tables rows are referenced by appending the index
MIB (Cont)

- All names are specified using a subset of Abstract Syntax Notation (ASN.1)
- ASN.1 specifies notation (that humans can read) and encoding (representation and ranges)
- Only INTEGER, OCTET STRING, OBJECT IDENTIFIER, NULL types
- Only SEQUENCE, SEQUENCE OF, CHOICE constructors
Global Naming Hierarchy

ccitt(0)  iso (1)  joint-iso-ccitt (2)

standard (0)  org (3)

iso9314 (9314)  dod (6)

fddiMIB (1)

internet (1)

directory (1)  mgmt(2)  experimental (3) private (4)

mib (1)

system (1)  interfaces (2)  •  •  •  transmission(10) fddimib (73)

fddi (15)
<table>
<thead>
<tr>
<th>Variable</th>
<th>Category</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>sysUpTime</td>
<td>system</td>
<td>Time since last reboot</td>
</tr>
<tr>
<td>ifNumber</td>
<td>interfaces</td>
<td># of Interfaces</td>
</tr>
<tr>
<td>ifMTU</td>
<td>interfaces</td>
<td>MTU</td>
</tr>
<tr>
<td>ipDefaultTTL</td>
<td>ip</td>
<td>Default TTL</td>
</tr>
<tr>
<td>ipInReceives</td>
<td>ip</td>
<td># of datagrams received</td>
</tr>
<tr>
<td>ipForwDatagrams</td>
<td>ip</td>
<td># of datagrams forwarded</td>
</tr>
<tr>
<td>icmpInEchos</td>
<td>icmp</td>
<td># of Echo requests received</td>
</tr>
<tr>
<td>tcpRtoMin</td>
<td>tcp</td>
<td>Min retrans time</td>
</tr>
<tr>
<td>tcpMaxConn</td>
<td>tcp</td>
<td>Max connections allowed</td>
</tr>
</tbody>
</table>
MIB Definition: Example

ipAddrTable ::= SEQUENCE of ipAddrEntry
ipAddrEntry ::= SEQUENCE {
ipAdEntAddr ipAddress,
ipAdEntIfIndex INTEGER,
ipAdEntNetMask ipAddress,
ipAdEntBcastAddr ipAddress,
ipAdEntReasmMaxSize INTEGER (0..65535)
}
ipAddrEntry { ipAddrTable 1}
ipAdEntNetMask {ipAddrTable 3}
SNMP Message Format

- In ASN.1 Notation:

```
SNMP-Message ::= SEQUENCE {
    version INTEGER {version-1 (0)},
    community OCTET STRING,
    data ANY
}
```
SNMP Message Types

SNMP-PDUs ::= CHOICE{
get-request GetRequest-PDU,
get-next-request GetNextRequest-PDU,
get-response GetResponse-PDU,
set-request SetRequest-PDU,
trap Trap-PDU
}

Message Types (Cont)

GetRequestPDU ::= [0]
IMPLICIT SEQUENCE{
request-id RequestID,
error-status ErrorStatus,
error-index ErrorIndex,
variable-bindings VarBindList
}
SNMPv2

- Improved security: authentication and integrity using Data Encryption Standard (DES)
- inform request $\Rightarrow$ Multiple manager coordination
  Locking mechanisms prevent multiple managers from writing at the same time
- get bulk $\Rightarrow$ Better table handling
- Confirmation option for Traps
  $\Rightarrow$ Agents can ensure that trap was received correctly.
- New Error codes: noSuchName, badValue, readOnly
- Reference: RFC 1441
OSI Net Management Standards

- Common Management Information Protocol (CMIP)
- Common Management Information Service (CMIS)
- CMIP is the management (application layer) protocol
- CMIS is the service interface to CMIP
- M-GET (read attribute), M-SET (write attribute), M-EVENT-REPORT (report an event), M-ACTION (perform an action), M-CREATE (create an instance), M-DELETE (delete an instance)
Remote Network Monitoring

- RMON Allows network managers to monitor the traffic on the network
- Network monitors/analyzers promiscuously monitor the LAN traffic
- RMON allows a central network management station to communicate with monitors throughout the network.
- RMON = Monitor MIB
- Allows remote control of monitors
- Allows multiple managers
A Sample RMON Configuration

Management Console

PC with RMON Agent

PC with RMON Agent

Local Management Console with RMON

Router

Router

Router with RMON Agent
Summary

- Management = Initialization, Monitoring, and Control
- SNMP = Only 5 commands
- Standard MIBs defined for each object
- Uses ASN.1 encoding