Network management

Chapter 9: Network Management

Chapter goals:
- introduction to network management
- motivation
- major components
- Internet network management framework
  - MIB: management information base
  - SMI: data definition language
  - SNMP: protocol for network management
  - security and administration
- presentation services: ASN.1

Acknowledgement: Some slides taken from Kurose/Ross and Katz/Stoica

Chapter 9 outline

- What is network management?
- Internet-standard management framework
  - Structure of Management Information: SMI
  - Management Information Base: MIB
  - SNMP Protocol Operations and Transport Mappings
  - Security and Administration
- ASN.1

What is network management?

- autonomous systems (aka "network"): 100s or 1000s of interacting hardware/software components
- other complex systems requiring monitoring, control:
  - jet airplane
  - nuclear power plant
  - others?

Network management includes the deployment, integration, and coordination of the hardware, software, and human elements to monitor, test, poll, configure, analyze, evaluate, and control the network and element resources to meet the real-time, operational performance, and Quality of Service requirements at a reasonable cost.

Infrastructure for network management

Network Management standards

OSI CMIP
- Common Management Information Protocol
- designed 1980's: the unifying net management standard
- too slowly standardized

SNMP: Simple Network Management Protocol
- Internet roots (SGMP)
- started simple
- deployed, adopted rapidly
- growth: size, complexity
- currently: SNMP V3
- de facto network management standard
Chapter 9 outline

- What is network management?
- Internet-standard management framework
  - Structure of Management Information (SMI)
  - Management Information Base (MIB)
  - SNMP Protocol Operations and Transport Mappings
  - Security and Administration
- ASN.1

SNMP overview: 4 key parts

- Management information base (MIB):
  - distributed information store of network management data
- Structure of Management Information (SMI):
  - data definition language for MIB objects
- SNMP protocol:
  - convey manager<>managed object info, commands
  - security, administration capabilities
  - major addition in SNMPv3

SMI: data definition language

**Purpose:** syntax, semantics of management data well-defined, unambiguous
- base data types:
  - straightforward, boring
- **OBJECT-TYPE**
  - data type, status, semantics of managed object
- **MODULE-IDENTITY**
  - groups related objects into MIB module

Basic Data Types

- INTEGER
- Unsigned32
- OCTET STRING
- OBJECT IDENTIFIED
- IP address
- Counter32
- Counter64
- Gauge32
- Time Ticks
- Opaque

SMI: Object, module examples

**OBJECT-TYPE:** ipInDelivers

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipInDelivers</td>
<td>Counter32</td>
<td>The total number of input datagrams successfully delivered to IP user-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>protocols (including ICMP)</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>::= {ip 9}</code></td>
</tr>
</tbody>
</table>

**MODULE-IDENTITY:** ipMIB

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipMIB</td>
<td>OBJECT-TYPE</td>
<td>The MIB module for managing IP and ICMP implementations, but excluding</td>
</tr>
<tr>
<td></td>
<td></td>
<td>their management of IP routes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>::= {mib-2 48}</code></td>
</tr>
</tbody>
</table>

SNMP MIB

**MIB module specified via SMI**

- (100 standardized MIBs, more vendor-specific)

<table>
<thead>
<tr>
<th>Module Identity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipMIB</td>
<td>The MIB module for managing IP and ICMP implementations, but excluding their</td>
</tr>
<tr>
<td></td>
<td>management of IP routes.</td>
</tr>
</tbody>
</table>

MIB example: UDP module

<table>
<thead>
<tr>
<th>Object ID</th>
<th>Name</th>
<th>Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.2.1.7.1</td>
<td>UDPInDatagrams</td>
<td>Counter32</td>
<td>Total # datagrams delivered at this node</td>
</tr>
<tr>
<td>1.3.6.1.2.1.7.2</td>
<td>UDPNoPorts</td>
<td>Counter32</td>
<td># underdeliverable datagrams</td>
</tr>
<tr>
<td>1.3.6.1.2.1.7.3</td>
<td>UDDErrors</td>
<td>Counter32</td>
<td># undeliverable datagrams due to all other reasons</td>
</tr>
<tr>
<td>1.3.6.1.2.1.7.4</td>
<td>UDPOutDatagrams</td>
<td>Counter32</td>
<td># datagrams sent</td>
</tr>
<tr>
<td>1.3.6.1.2.1.7.5</td>
<td>udpTable</td>
<td>SEQUENCE</td>
<td>One entry for each port used by app, gives port # and IP address</td>
</tr>
</tbody>
</table>
SNMP Naming

question: how to name every possible standard object (protocol, data, more..) in every possible network standard??

answer: ISO Object Identifier tree:
- hierarchical naming of all objects
- each branchpoint has name, number

ISO
US DoD
Internet

1.3.6.1.2.1.7.1
udpInDatagrams
UDP
MIB2
management

Check out www.alvestrand.no/harald/objectid/top.html

SNMP protocol

Two ways to convey MIB info, commands:

request/response mode
trap mode

request
response

SNMP protocol: message types

Message type
Function
GetRequest
Mgr-to-agent: “get me data”
GetInstance
Mgr-to-agent: get instance
next in list, block

GetNextRequest
Mgr-to-agnt: “get next item”

GetBulkRequest
Mgr-to-agnt: “get in bulk”

InformRequest
Mgr-to-Mgr: here’s MIB value

SetRequest
Mgr-to-agent: set MIB value

Response
Agent-to-mgr: value, response to Request

Trap
Agent-to-mgr: inform manager of exceptional event

SNMP protocol: message formats

Get/set handle
Variable to get/set

POX
POX
POX
POX
POX
POX

POX
POX
POX
POX
POX

POX
POX
POX
POX
POX

SNMP security and administration

- encryption: DES-encrypt SNMP message
- authentication: compute, send MIC(m,k);
compute hash (MIC) over message (m), secret
shared key (k)
- protection against playback: use nonce
- view-based access control
  - SNMP entity maintains database of access rights,
policies for various users
  - database itself accessible as managed object!
Chapter 9 outline

- What is network management?
- Internet-standard management framework
  - Structure of Management Information: SMI
  - Management Information Base: MIB
  - SNMP Protocol Operations and Transport Mappings
  - Security and Administration
- The presentation problem: ASN.1

The presentation problem

Q: does perfect memory-to-memory copy solve “the communication problem”?

A: not always!

<table>
<thead>
<tr>
<th>host 1 format</th>
<th>host 2 format</th>
</tr>
</thead>
<tbody>
<tr>
<td>test.code</td>
<td>test.code</td>
</tr>
<tr>
<td>00000001</td>
<td>00000011</td>
</tr>
<tr>
<td>test.x</td>
<td>test.x</td>
</tr>
<tr>
<td>00000011</td>
<td>00000001</td>
</tr>
</tbody>
</table>

problem: different data format, storage conventions

A real-life presentation problem:

- grandma
- aging 60’s hippie
- 2004 teenager
- groovy

Presentation problem: potential solutions

1. Sender learns receiver’s format. Sender translates into receiver’s format. Sender sends.
   - real-world analogy?
   - pros and cons?

2. Sender sends. Receiver learns sender’s format. Receiver translates into receiver-local format.
   - real-world analogy?
   - pros and cons?

   - real-world analogy?
   - pros and cons?

Solving the presentation problem

1. Translate local-host format to host-independent format
2. Transmit data in host-independent format
3. Translate host-independent format to remote-host format

ASN.1: Abstract Syntax Notation 1

- ISO standard X.680
  - used extensively in Internet
  - like eating vegetables, knowing this “good for you”!
- defined data types, object constructors
  - like SMI
- BER: Basic Encoding Rules
  - specify how ASN.1-defined data objects to be transmitted
  - each transmitted object has Type, Length, Value (TLV) encoding
TLV Encoding

Idea: transmitted data is self-identifying
- T: data type, one of ASN.1-defined types
- L: length of data in bytes
- V: value of data, encoded according to ASN.1 standard

<table>
<thead>
<tr>
<th>Tag Value</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Boolean</td>
</tr>
<tr>
<td>2</td>
<td>Integer</td>
</tr>
<tr>
<td>3</td>
<td>Bitstring</td>
</tr>
<tr>
<td>4</td>
<td>Octet string</td>
</tr>
<tr>
<td>5</td>
<td>Null</td>
</tr>
<tr>
<td>6</td>
<td>Object Identifier</td>
</tr>
<tr>
<td>9</td>
<td>Real</td>
</tr>
</tbody>
</table>

Network Management: summary

- network management
  - extremely important: 80% of network "cost"
  - ASN.1 for data description
  - SNMP protocol as a tool for conveying information
- Network management: more art than science
  - what to measure/monitor
  - how to respond to failures?
  - alarm correlation/filtering?