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

A note on the use of these ppt slides:
We're making these slides freely available to all (faculty, students, readers). They're in PowerPoint form so you can add, modify, and delete slides (including this one) and slide contents to suit your needs. They obviously represent a lot of work on our part. In return for use, we only ask the following:
- If you use these slides (e.g., in a class) in substantially unaltered form, that you mention their source (after all, we'd like people to use our book!)
- If you post any slides in substantially unaltered form on a www site, that you note that they are adapted from (or perhaps identical to) our slides, and note our copyright of this material.

All material copyright 1996-2004 J.F. Kurose and K.W. Ross. All Rights Reserved.

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."

Network Management standards
- OSI CMIP
  - Common Management Information Protocol
  - designed 1980's: the unifying network 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 |
|-----------------------------|-----------------------------|
| Basic Data Types            |
| INTEGER                     |
| Integer32                   |
| Unsigned32                  |
| OCTET STRING                |
| OBJECT IDENTIFIED           |
| IP address                  |
| Counter32                   |
| Counter64                   |
| Gauge32                     |
| Time ticks                  |
| Opaque                      |

SMI: Object, module examples

OBJECT-TYPE: ipInDelivers

ipInDelivers OBJECT-TYPE Syntax Counter32 MAX-ACCESS read-only STATUS current
DESCRIPTION "The total number of input datagrams successfully delivered to IP user-protocols (including ICMP)"
::= { ip 9}

MODULE-IDENTITY: ipMIB

%MIB MODULE-IDENTITY
LAST-UPDATED "941101000Z"
ORGANIZATION "IETF SNPv2 Working Group"
CONTACT-INFO "Keith McCloghrie"
DESCRIPTION "The MIB module for managing IP and ICMP implementations, but excluding their management of IP routes."
REVISION "019331000Z"
::= {mib-2 48}

SNMP MIB

MIB module specified via SMI

MODULE-IDENTITY
(100 standardized MIBs, more vendor-specific)

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>UDPPDlDatagrams</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>UDPPNoPorts</td>
<td>Counter32</td>
<td># undeliverable datagrams no app at port!</td>
</tr>
<tr>
<td>1.3.6.1.2.1.7.3</td>
<td>UDPEErrors</td>
<td>Counter32</td>
<td># undeliverable datagrams 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</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
  - Object Identifier
  - Org.
  - 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

SNMP protocol: message types

<table>
<thead>
<tr>
<th>Message type</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>GetRequest</td>
<td>Mgr-to-agent: &quot;get me data&quot;</td>
</tr>
<tr>
<td>GetNextRequest</td>
<td>(instance, next in list, block)</td>
</tr>
<tr>
<td>GetBulkRequest</td>
<td></td>
</tr>
<tr>
<td>InformRequest</td>
<td>Mgr-to-Mgr: here's MIB value</td>
</tr>
<tr>
<td>SetRequest</td>
<td>Mgr-to-agent: set MIB value</td>
</tr>
<tr>
<td>Response</td>
<td>Agent-to-mgr: value, response to Request</td>
</tr>
<tr>
<td>Trap</td>
<td>Agent-to-mgr: inform manager of exceptional event</td>
</tr>
</tbody>
</table>

SNMP protocol: message formats

<table>
<thead>
<tr>
<th>PDUs</th>
<th>Variables to get/set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request</td>
<td>Error Status</td>
</tr>
<tr>
<td>Next</td>
<td>(32)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PDUs</th>
<th>Specific code</th>
<th>Time stamp</th>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>(16)</td>
<td>(32)</td>
<td>(64)</td>
<td>(64)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Trap header</th>
<th>Trap information</th>
</tr>
</thead>
</table>

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!

```c
struct {
    char code;
    int x;
} test;
```

- test.x = 256;
- test.code = 'a'

**problem:** different data format, storage conventions

A real-life presentation problem:

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

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?