Information Technology Engineering

Mohammad Hossein Manshaei

manshaei@gmail.com

1393

MIB, SMI, SNMP, and ASN.1

NETWORK MANAGEMENT

Slides derived from those available on the Web site of the book "Computer Networking", by Kurose and Ross, PEARSON

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

Chapter 9 outline

9.1 What is network management?

9.2 The Infrastructure for Network Management

9.3 Internet-standard management framework

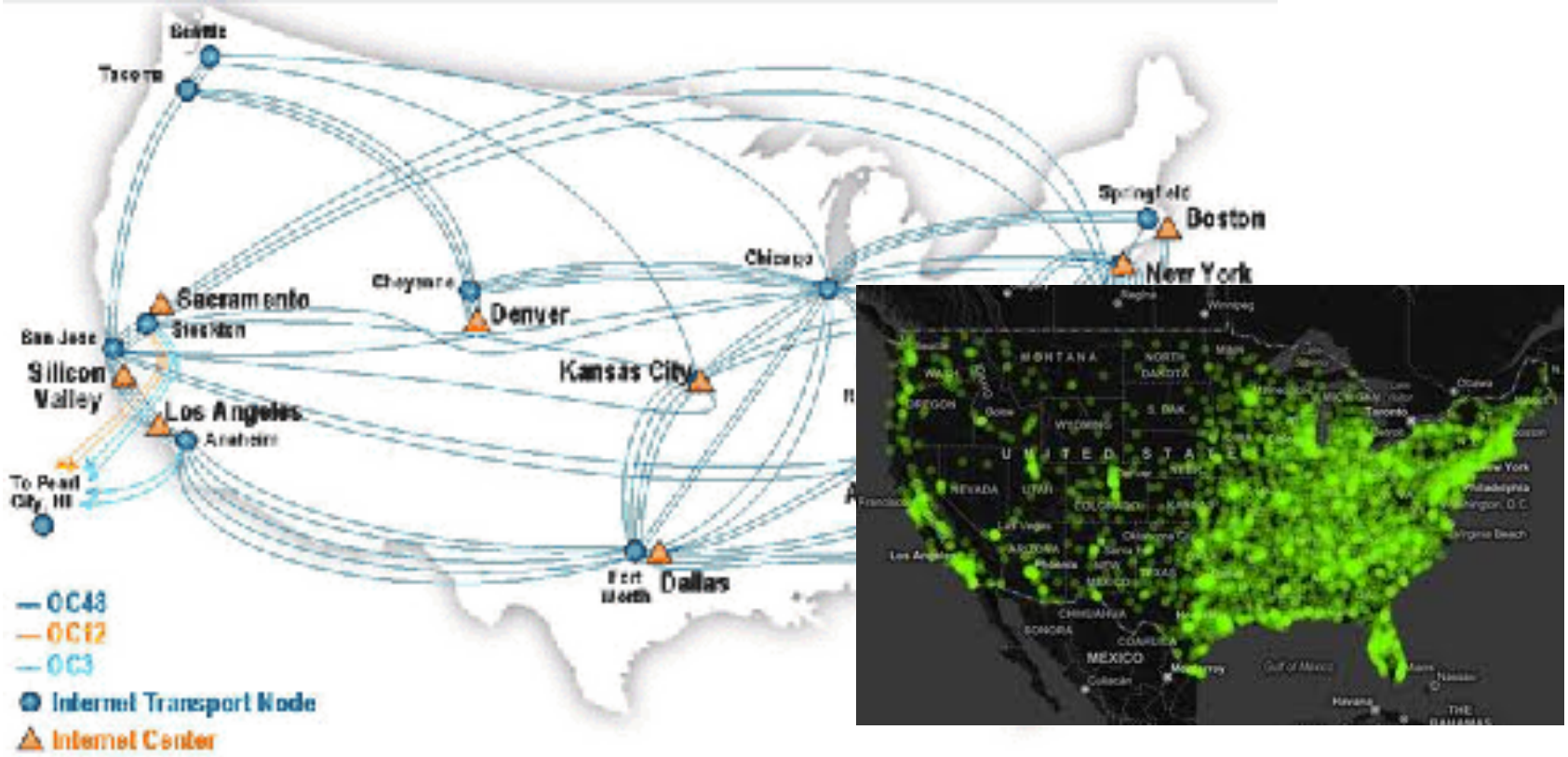
- Structure of Management Information: SMI
- Management Information Base: MIB
- SNMP Protocol Operations and Transport Mappings
- Security and Administration

9.4 The Presentation Problem: ASN.1

What is network management?

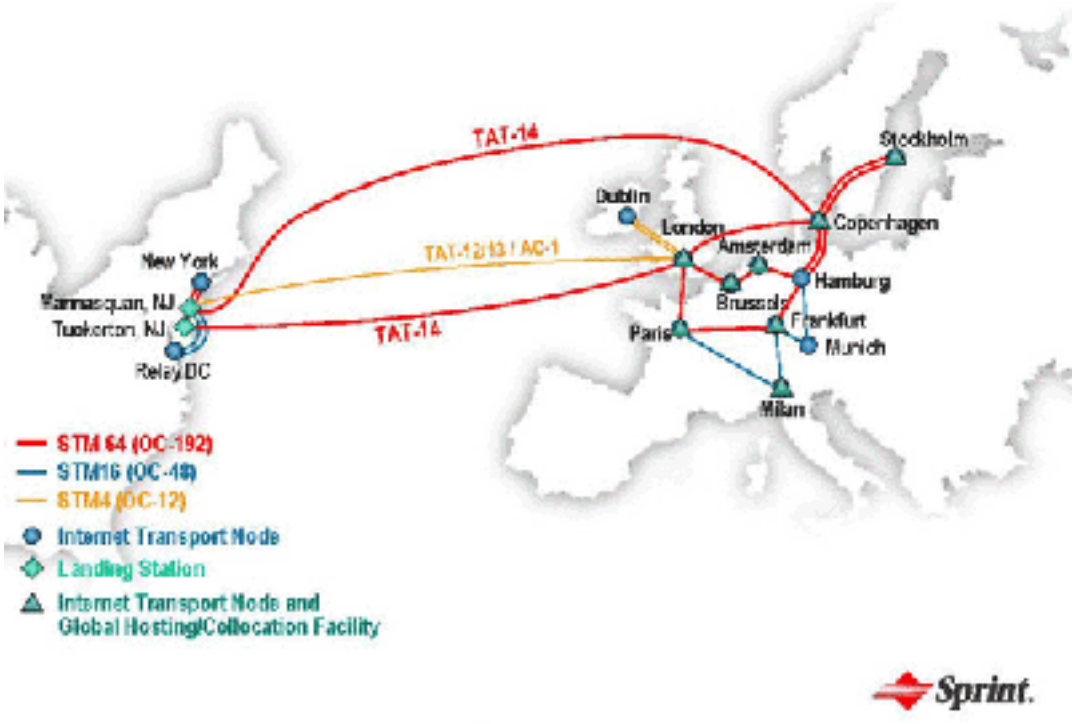
- autonomous systems (aka "network"): 1000s of interacting hardware/software components
- other complex systems requiring monitoring, control:
  - jet airplane
  - nuclear power plant
  - others?

Sprintlink's Network Operations Center: A Case Study

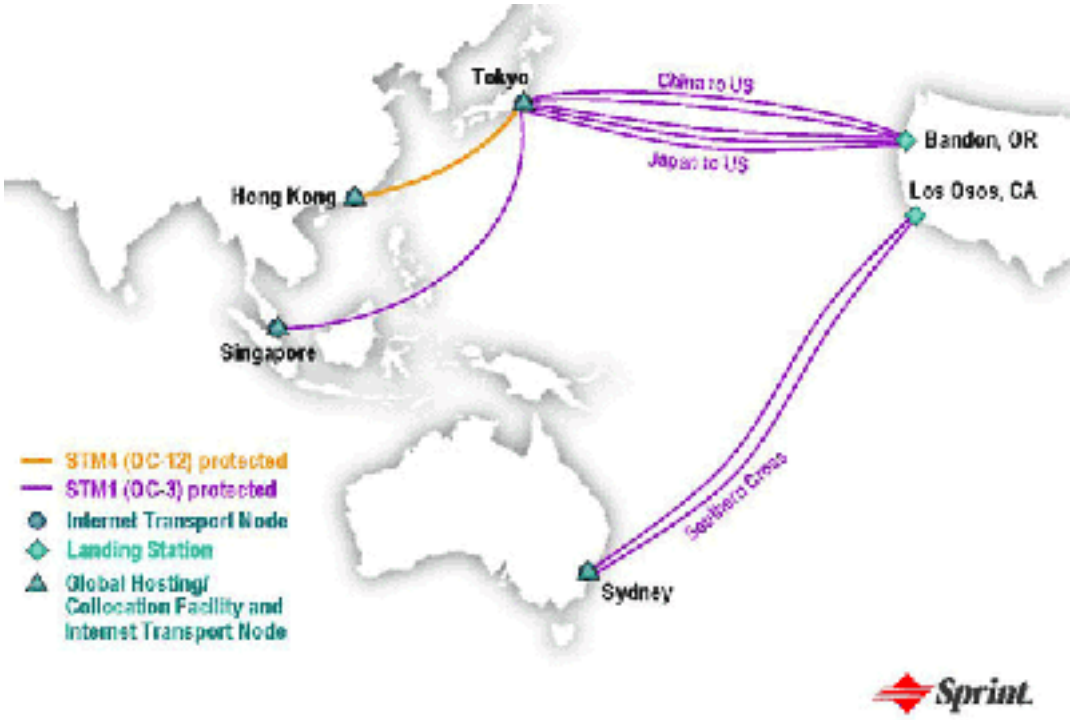


1. 70 points of presence
2. 800 routers
3. Primary NOC (network operations center) located in Reston, VA
4. At any time, a team of 4 network operation centers is monitoring and managing
5. Another team is standing by to handle customer trouble reports
6. National Technical Assistance Center (NTAC) if the problem cannot be solved in 15min

Sprintlink's Network Operations Center: A Case Study



Sprintlink's Network Operations Center: A Case Study



Sprintlink's Network Operations Center: A Case Study

Network Management Model [ISO]

1. Performance Management
   - ✧ Traffic Monitoring
2. Fault Management
   - ✧ Detect Failure of an interface card
3. Configuration Management
   - ✧ Host monitoring
4. Accounting Management
   - ✧ Service Level Agreements
5. Security Management
   - ✧ Intrusion Detection

Definition

"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."

Chapter 9 outline

9.1 What is network management?

9.2 The Infrastructure for Network Management

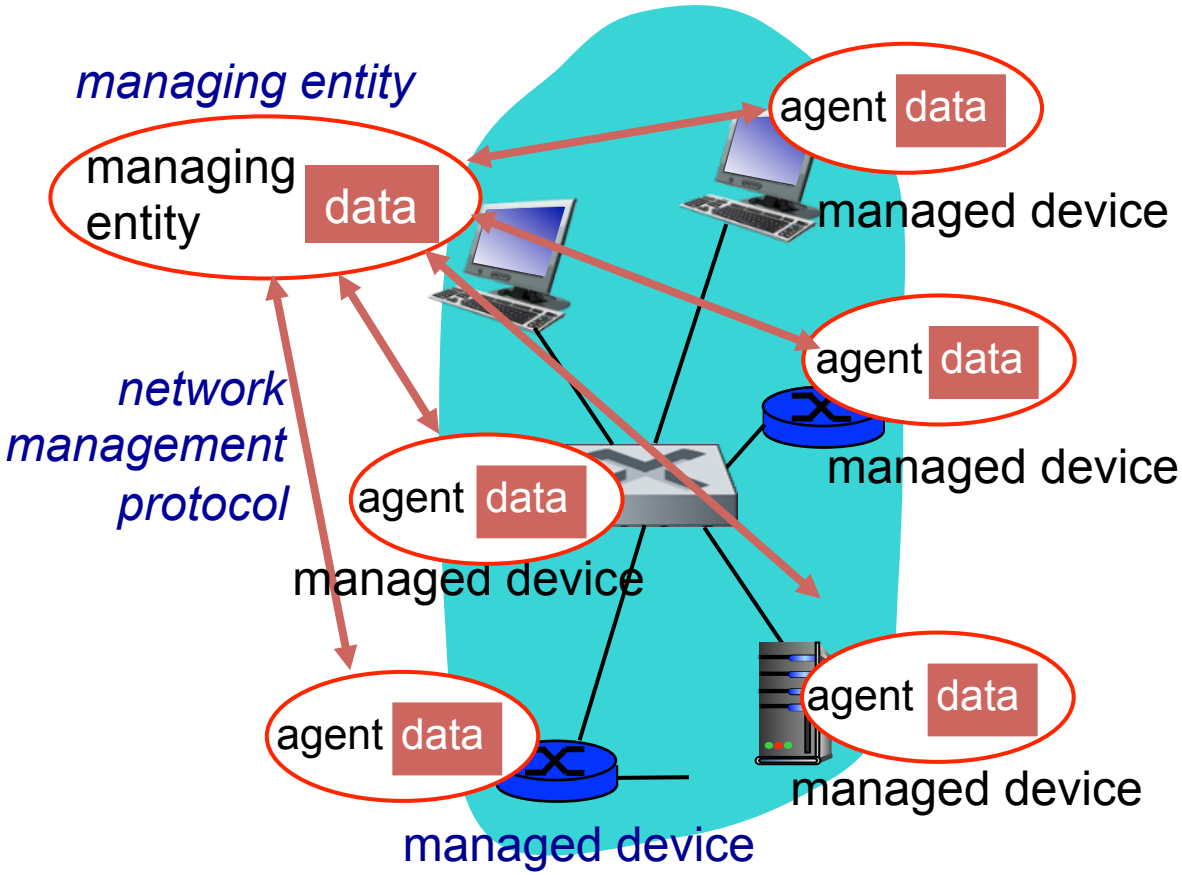
9.3 Internet-standard management framework

- Structure of Management Information: SMI
- Management Information Base: MIB
- SNMP Protocol Operations and Transport Mappings
- Security and Administration

9.4 The Presentation Problem: ASN.1

Infrastructure for network management

definitions:



managed devices contain *managed objects* whose data is gathered into a *Management Information Base (MIB)*

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

9.1 What is network management?

9.2 The Infrastructure for Network Management

9.3 Internet-standard management framework

- Structure of Management Information: SMI
- Management Information Base: MIB
- SNMP Protocol Operations and Transport Mappings
- Security and Administration

9.4 The Presentation Problem: ASN.1

SNMP: History

1. Simple Gateway Monitoring Protocol (SGMP) [RFC 1028]
2. SNMP v1 and SNMP v2
3. SNMP v3 [RFC 3410], released in April 1999 and updated in December 2002

3 Main Questions

1. What is being monitored? What form of controls can be exercised?
2. What is the specific form of the information?
3. What is the communication protocol?

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 construct
  - data type, status, semantics of managed object
- MODULE-IDENTITY construct
  - groups related objects into MIB module

Basic Data Types

1. INTEGER
2. Integer32
3. Unsigned32
4. OCTET STRING
5. OBJECT IDENTIFIED
6. IPaddress
7. Counter32
8. Counter64
9. Guage32
10. Time Ticks
11. Opaque

Basic Data Types of the SMI

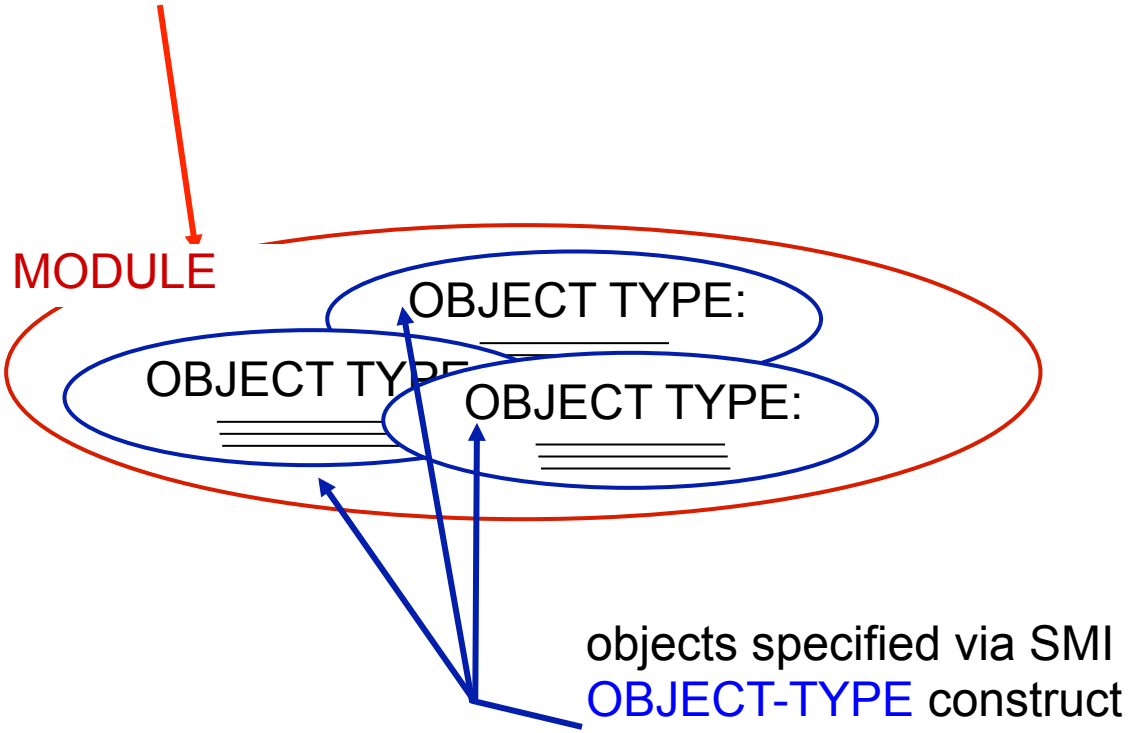
Data Type	Description
INTEGER	32-bit integer, as defined in ASN.1, with a value between -2^{31} and $2^{31} - 1$ inclusive, or a value from a list of possible named constant values.
Integer32	32-bit integer with a value between -2^{31} and $2^{31} - 1$ inclusive.
Unsigned32	Unsigned 32-bit integer in the range 0 to $2^{32} - 1$ inclusive.
OCTET STRING	ASN.1-format byte string representing arbitrary binary or textual data, up to 65,535 bytes long.
OBJECT IDENTIFIER	ASN.1-format administratively assigned (structured name); see Section 9.3.2.
IPaddress	32-bit Internet address, in network-byte order.
Counter32	32-bit counter that increases from 0 to $2^{32} - 1$ and then wraps around to 0.
Counter64	64-bit counter.
Gauge32	32-bit integer that will not count above $2^{32} - 1$ nor decrease beyond 0 when increased or decreased.
TimeTicks	Time, measured in 1/100ths of a second since some event.
Opaque	Uninterpreted ASN.1 string, needed for backward compatibility.

SNMP MIB

MIB module specified via SMI

MODULE-IDENTITY

(100 standardized MIBs, more vendor-specific)



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

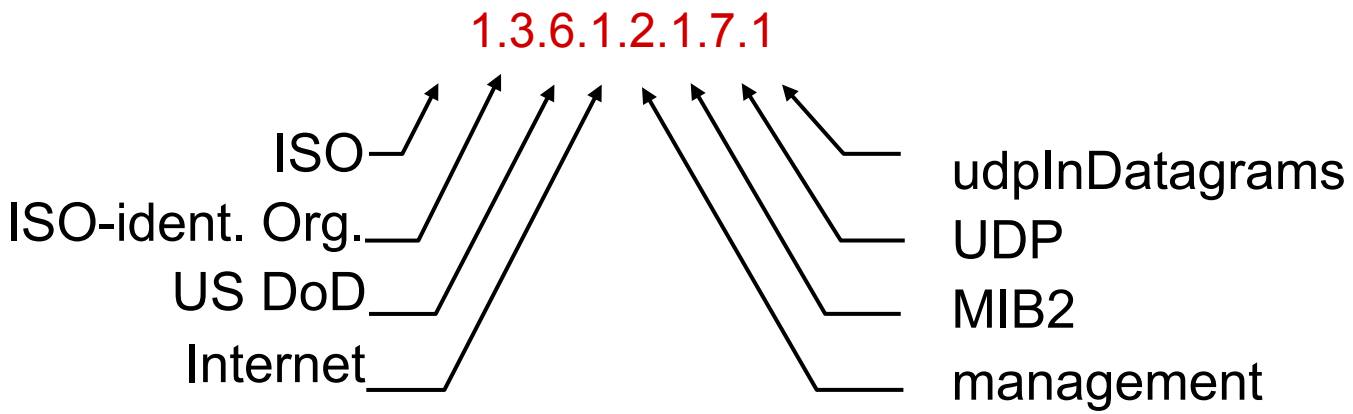
```
ipMIB MODULE-IDENTITY
  LAST-UPDATED "941101000Z"
  ORGANZATION "IETF SNPv2
          Working Group"
  CONTACT-INFO
    " Keith McCloghrie
          "
    ……
  DESCRIPTION
    "The MIB module for managing IP
    and ICMP implementations, but
    excluding their management of
    IP routes."
  REVISION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

SNMP naming

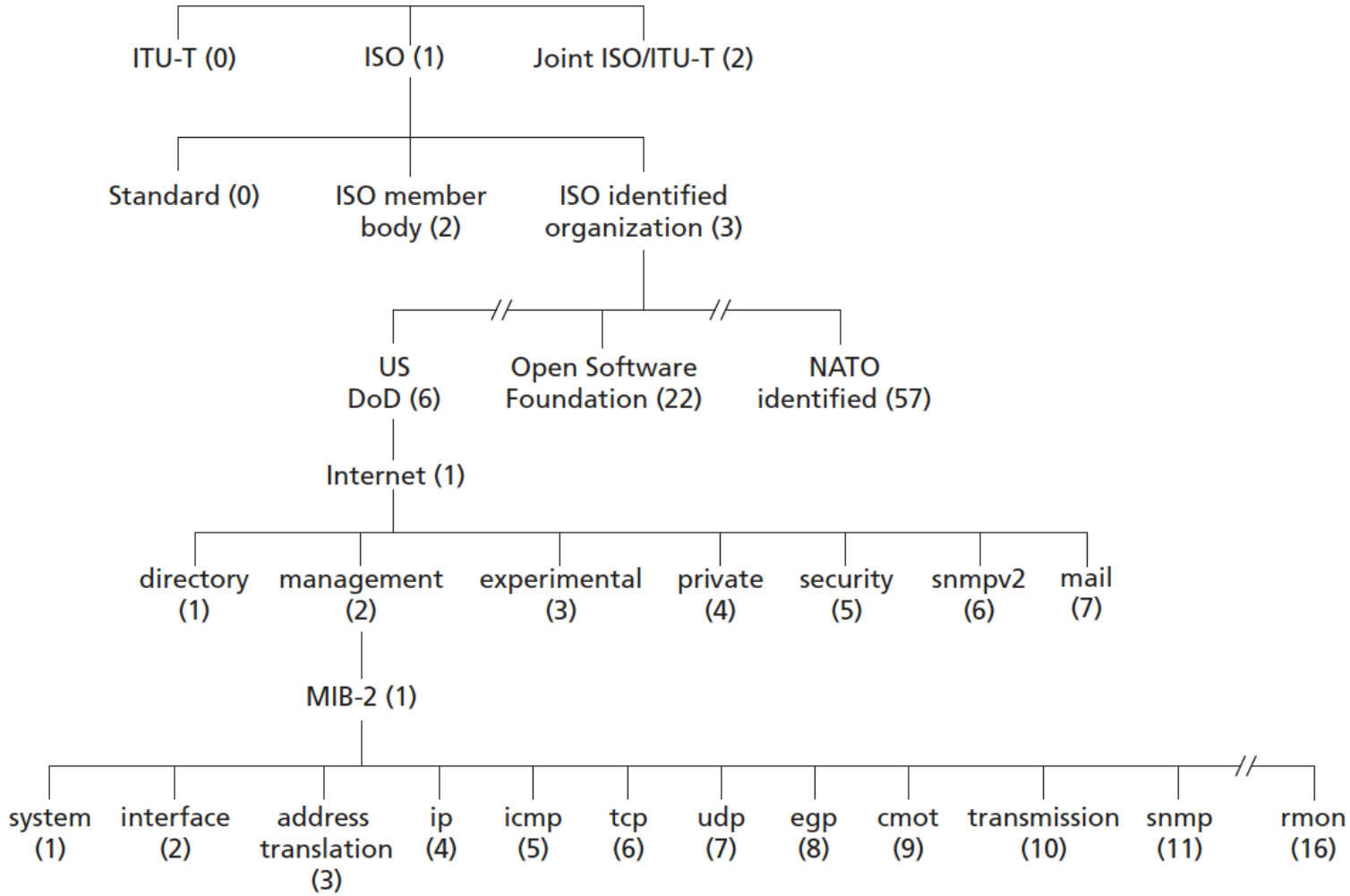
Question: how to name every possible standard object (protocol, data, more..) in every possible network standard??

Answer: *ISO Object Identifier tree:*

- hierarchical naming of all objects
- each branchpoint has name, number



ISO Object Identifier Tree



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

MIB-2 example: UDP module

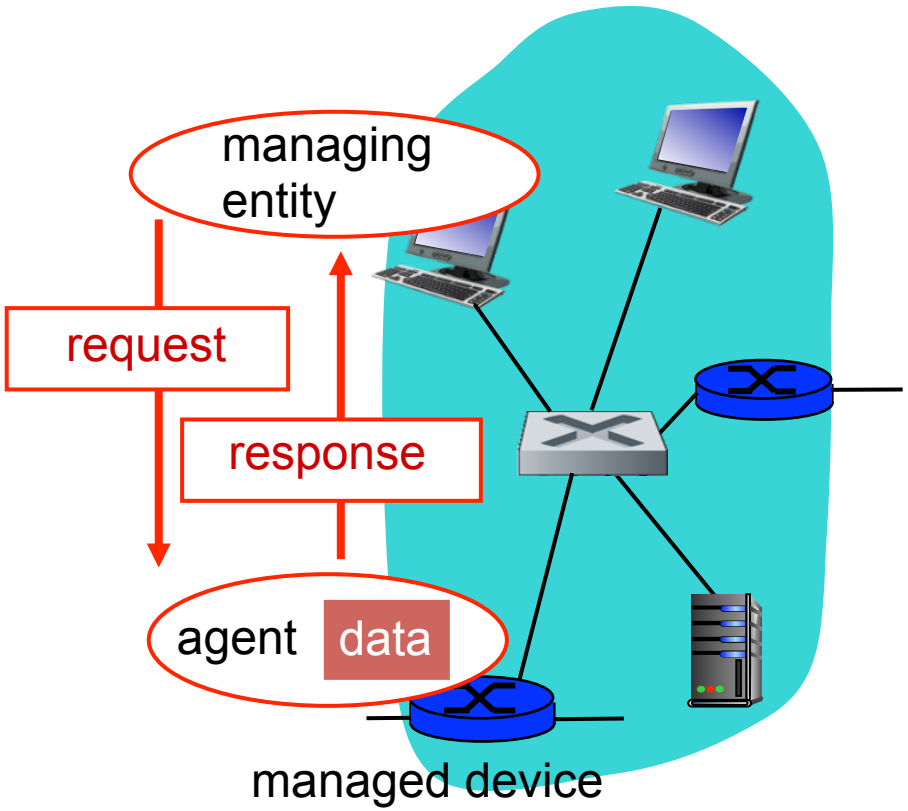
Object Identifier	Name	Type	Description (from RFC 4113)
1.3.6.1.2.1.7.1	`udpInDatagrams`	Counter32	"total number of UDP datagrams delivered to UDP users"
1.3.6.1.2.1.7.2	`udpNoPorts`	Counter32	"total number of received UDP datagrams for which there was no application at the destination port"
1.3.6.1.2.1.7.3	`udpInErrors`	Counter32	"number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port"
1.3.6.1.2.1.7.4	`udpOutDatagrams`	Counter32	"total number of UDP datagrams sent from this entity"

Managed Objects in the MIB-2 System Group

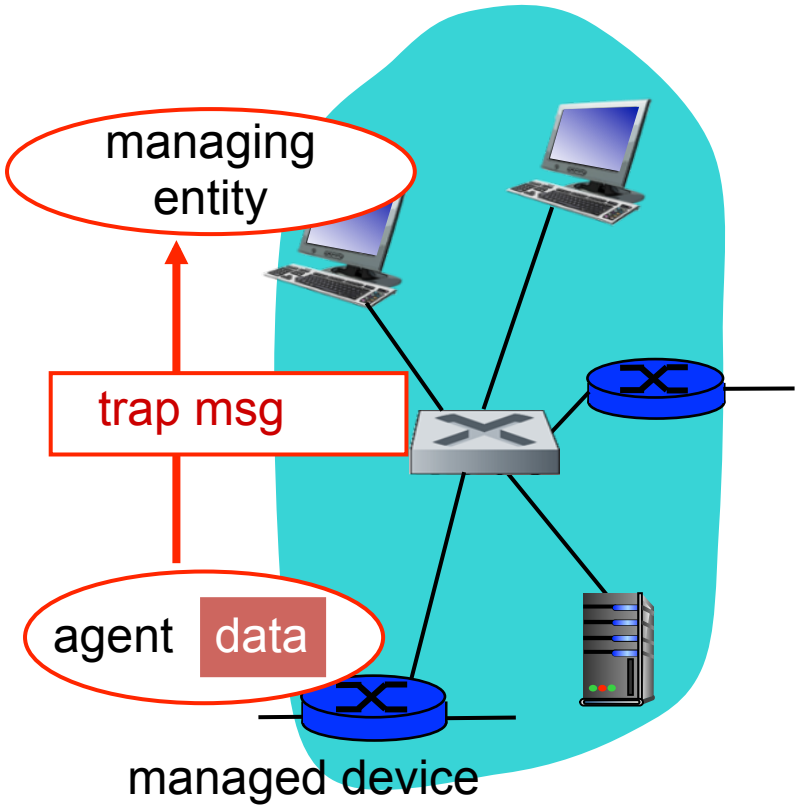
Object Identifier	Name	Type	Description (from RFC 1213)
1.3.6.1.2.1.1.1	`sysDescr`	OCTET STRING	"Full name and version identification of the system's hardware type, software operating-system, and networking software."
1.3.6.1.2.1.1.2	`sysObjectID`	OBJECT IDENTIFIER	Vendor-assigned object ID that "provides an easy and unambiguous means for determining 'what kind of box' is being managed."
1.3.6.1.2.1.1.3	`sysUpTime`	TimeTicks	"The time (in hundredths of a second) since the network management portion of the system was last re-initialized."
1.3.6.1.2.1.1.4	`sysContact`	OCTET STRING	"The contact person for this managed node, together with information on how to contact this person."
1.3.6.1.2.1.1.5	`sysName`	OCTET STRING	"An administratively assigned name for this managed node. By convention, this is the node's fully qualified domain name."
1.3.6.1.2.1.1.6	`sysLocation`	OCTET STRING	"The physical location of this node."
1.3.6.1.2.1.1.7	`sysServices`	Integer32	A coded value that indicates the set of services available at this node: physical (for example, a repeater), data link/subnet (for example, bridge), Internet (for example, IP gateway), end-to-end (for example, host), applications.

SNMP protocol

Two ways to convey MIB info, commands:



request/response mode

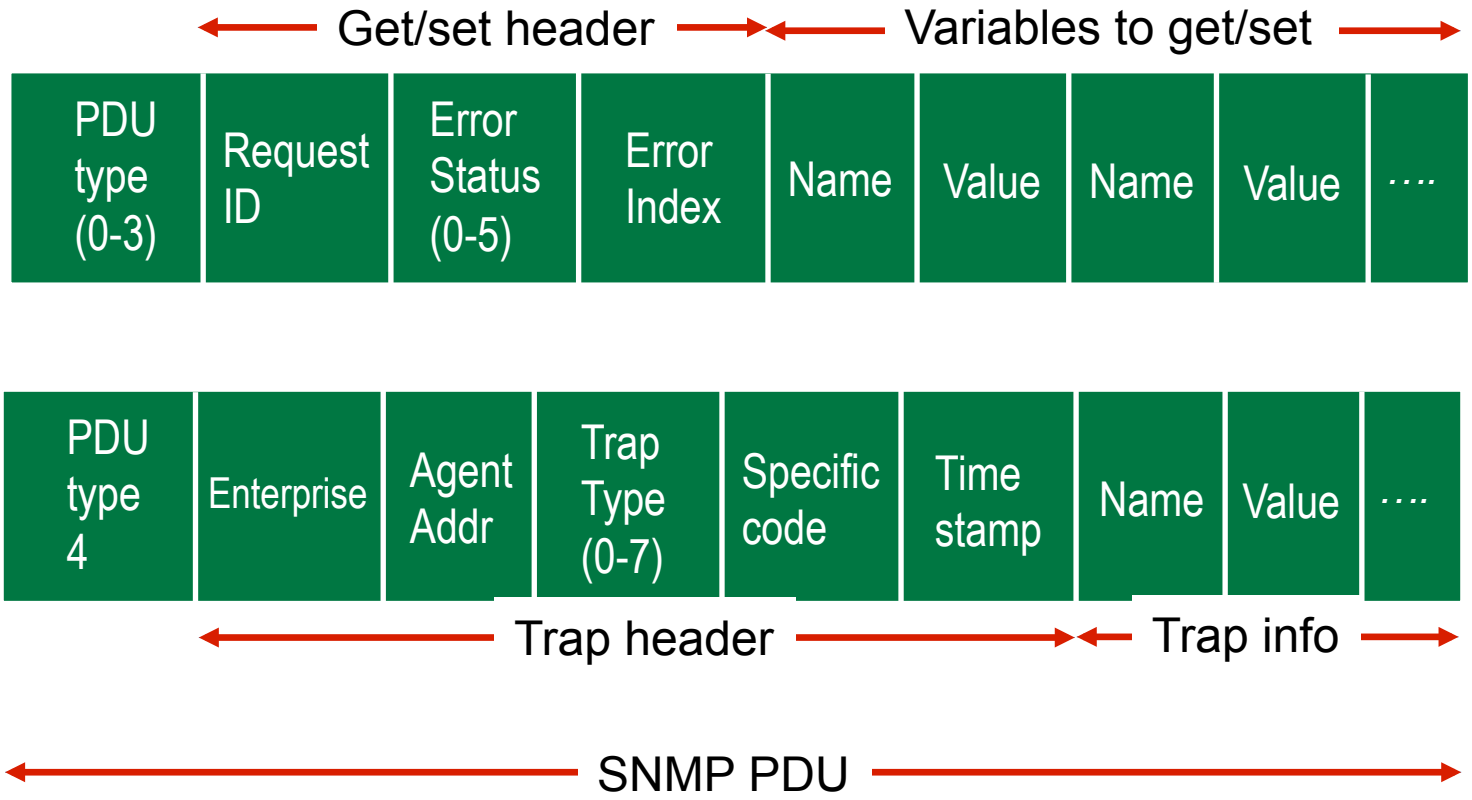


trap mode

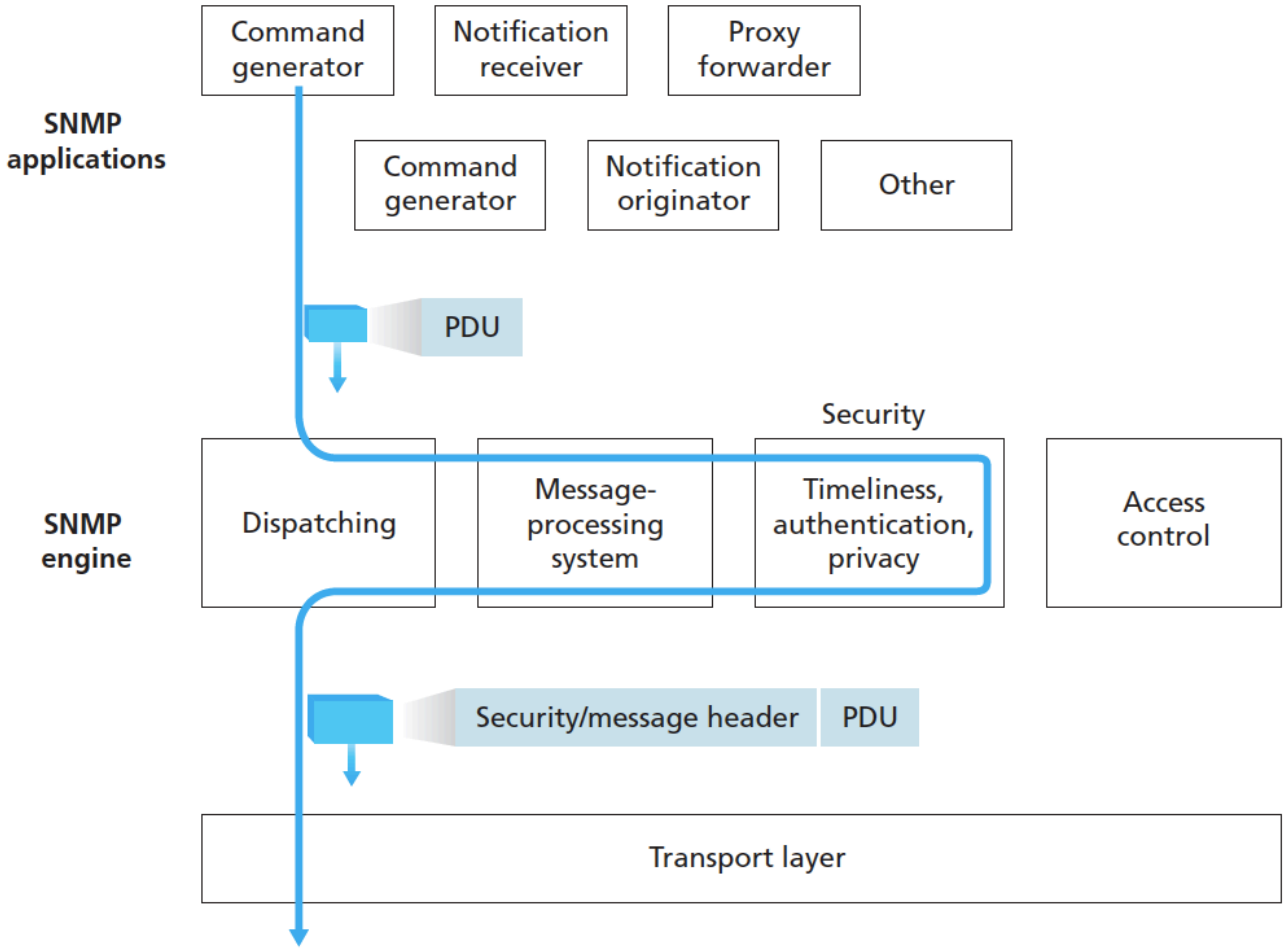
SNMP Protocol: Message Types

Message type	Function
GetRequest GetNextRequest GetBulkRequest	Mgr-to-agent: "get me data" (instance,next in list, block)
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



SNMP Engine and Application



SNMP security and administration

- Encryption: DES-encrypt SNMP message
- Authentication: compute, send MAC(m,k): compute hash (MAC) 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
  - Local Configuration Datastore (LCD)
  - database itself accessible as managed object!

Chapter 9 outline

9.1 What is network management?

9.2 The Infrastructure for Network Management

9.3 Internet-standard management framework

- Structure of Management Information: SMI
- Management Information Base: MIB
- SNMP Protocol Operations and Transport Mappings
- Security and Administration

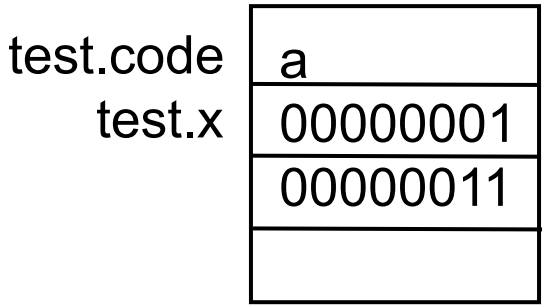
9.4 The Presentation Problem: ASN.1

The presentation problem

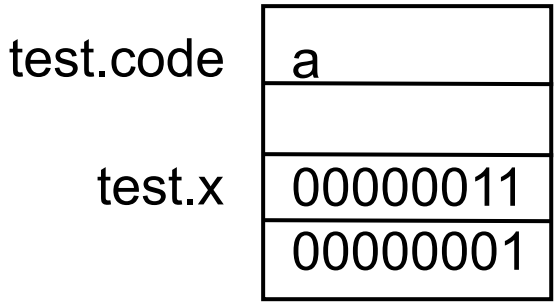
Q: does perfect memory-to-memory copy solve "the communication problem"?

A: not always!

```
struct {
   char code;
    int x;
    } test;
test.x = 256;
test.code= 'a'
```



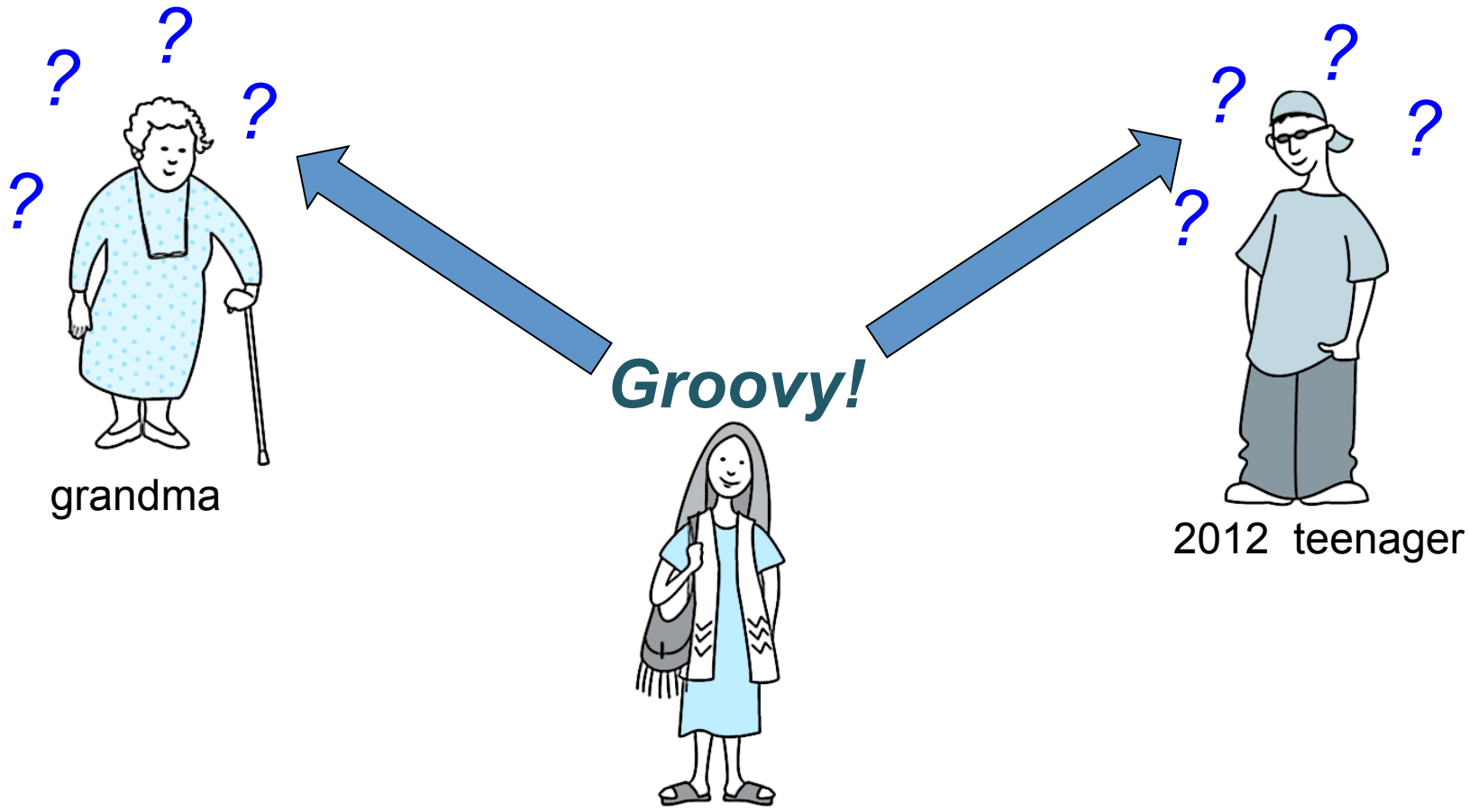
host 1 format



host 2 format

problem: different data format, storage conventions

A real-life presentation problem:

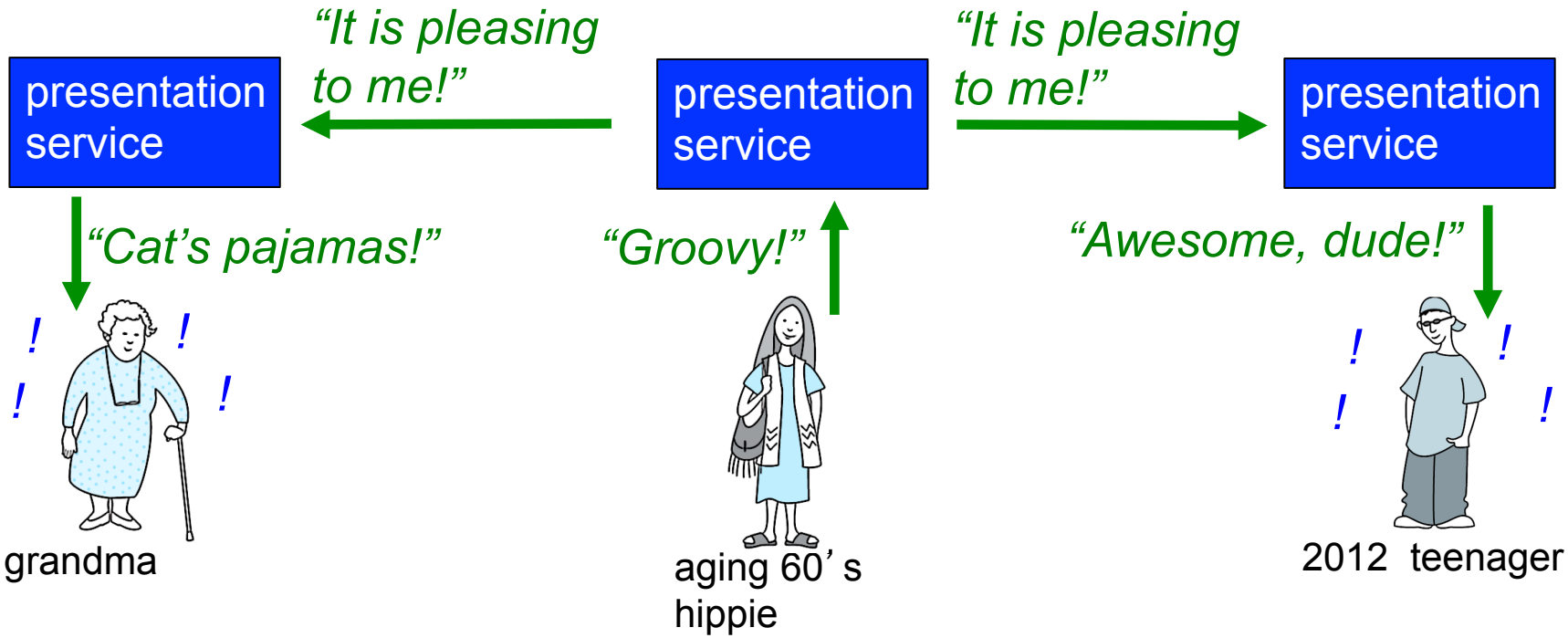


Presentation problem: potential solutions

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 translate into receiver-local format
   - real-world-analogy
   - pros and cons?
3. Sender translates host-independent format. Sends. Receiver translates to receiver-local format.
   - 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

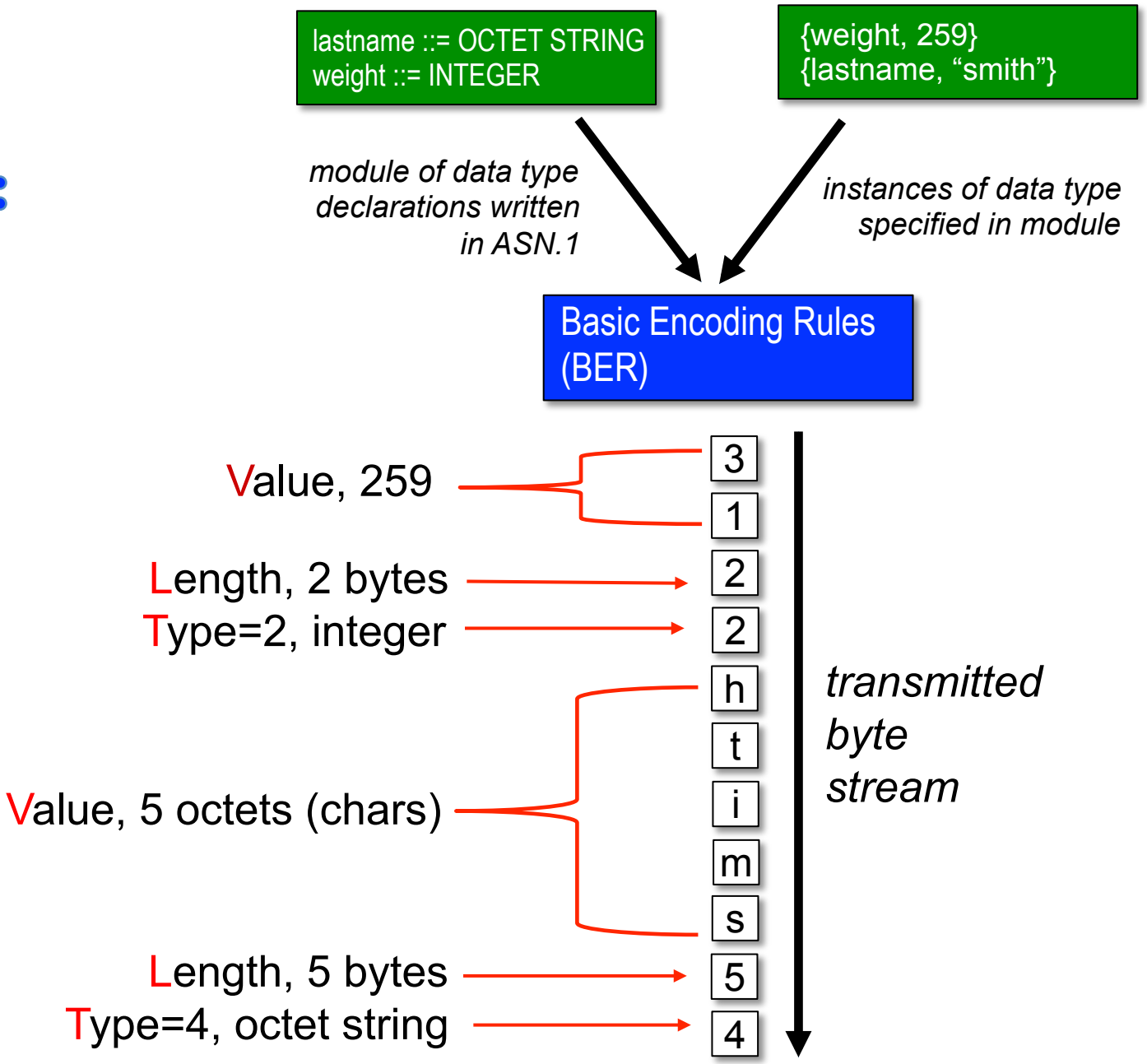
TLV Encoding

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

Tag Value	Type
1	Boolean
2	Integer
3	Bitstring
4	Octet string
5	Null
6	Object Identifier
9	Real

TLV encoding: example



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?