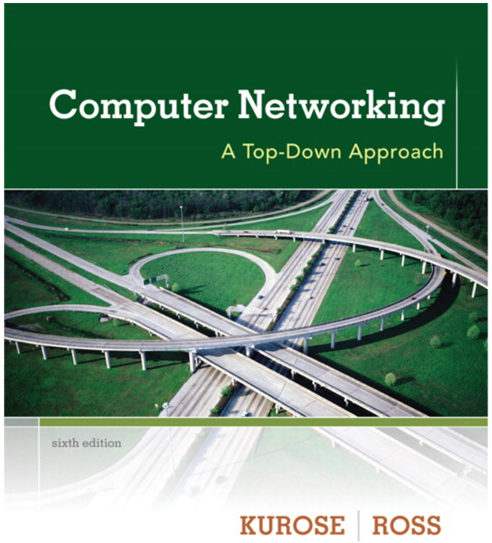
Chapter 9
Network Management



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 see the animations; and can add, modify, and delete slides (including this one) and slide content 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) that you mention their source (after all, we'd like people to use our book!)
- If you post any slides 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.

Thanks and enjoy! JFK/KWR

Computer Networking: A Top Down Approach
6th edition
Jim Kurose, Keith Ross
Addison-Wesley
March 2012

Chapter 9: Network Management

Chapter goals:

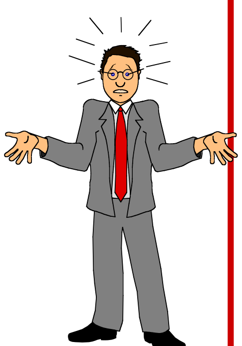
- introduction to network management
  - motivation
  - major components
- Internet network management framework
  - MIB: management information base
  - SMI: data definition language
  - SNMP: protocol for network management
  - security and administration
- presentation services: ASN.1

Chapter 9 outline

- 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?

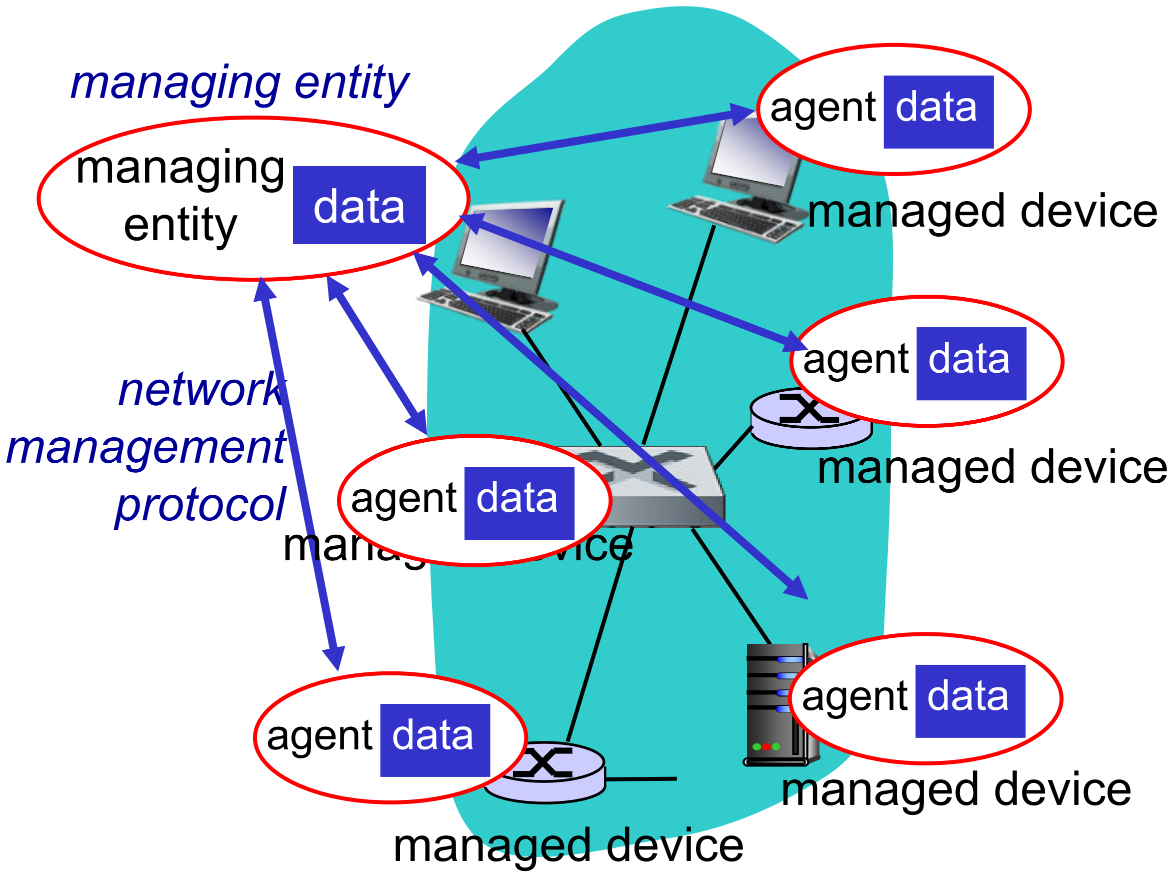
- autonomous systems (aka "network"): 1000s of interacting hardware/software components
- other complex systems requiring monitoring, control:
  - jet airplane
  - nuclear power plant
  - others?



"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

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

- 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

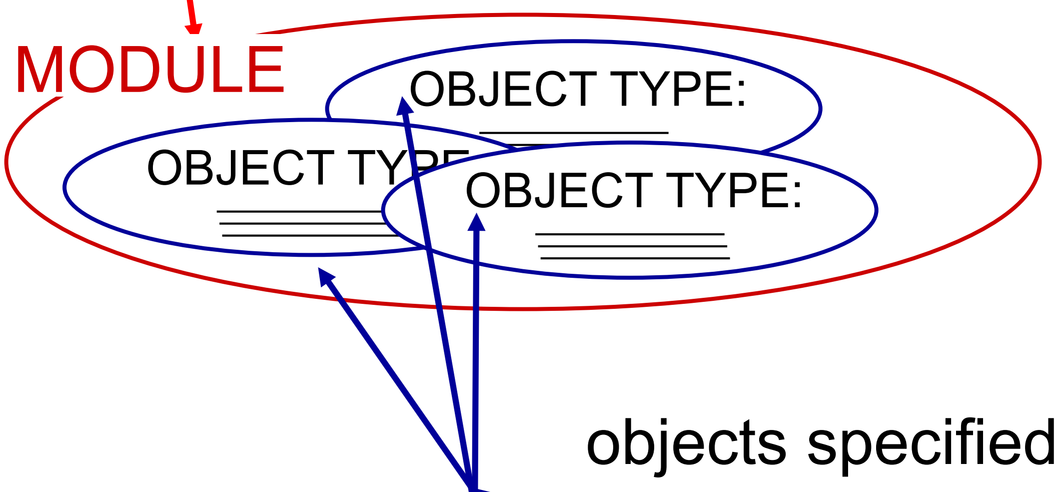
- base data types:
  - straightforward, boring
- OBJECT-TYPE
  - data type, status, semantics of managed object
- MODULE-IDENTITY
  - groups related objects into MIB module

Basic Data Types

INTEGER
Integer32
Unsigned32
OCTET STRING
OBJECT IDENTIFIED
IPaddress
Counter32
Counter64
Guage32
Time Ticks
Opaque

SNMP MIB

MIB module specified via SMI
MODULE-IDENTITY
(100 standardized MIBs, more vendor-specific)



objects specified via SMI
OBJECT-TYPE construct

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}
```

MIB example: UDP module

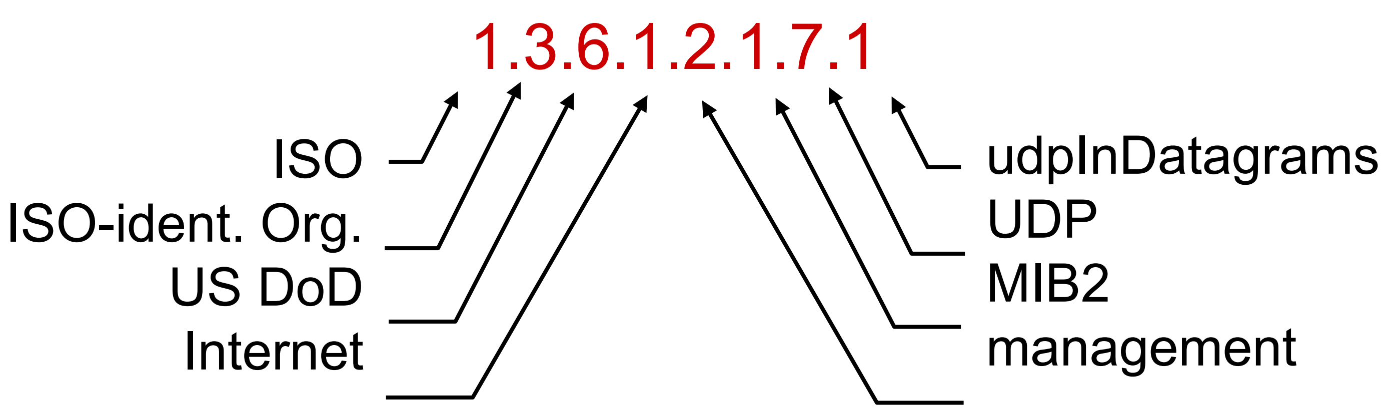
Object ID	Name	Type	Comments
1.3.6.1.2.1.7.1	UDPInDatagrams	Counter32	total # datagrams delivered at this node
1.3.6.1.2.1.7.2	UDPNoPorts	Counter32	# underliverable datagrams: no application at port
1.3.6.1.2.1.7.3	UDInErrors	Counter32	# undeliverable datagrams: all other reasons
1.3.6.1.2.1.7.4	UDPOutDatagrams	Counter32	# datagrams sent
1.3.6.1.2.1.7.5	udpTable	SEQUENCE	one entry for each port in use by app, gives port # and IP address

SNMP naming

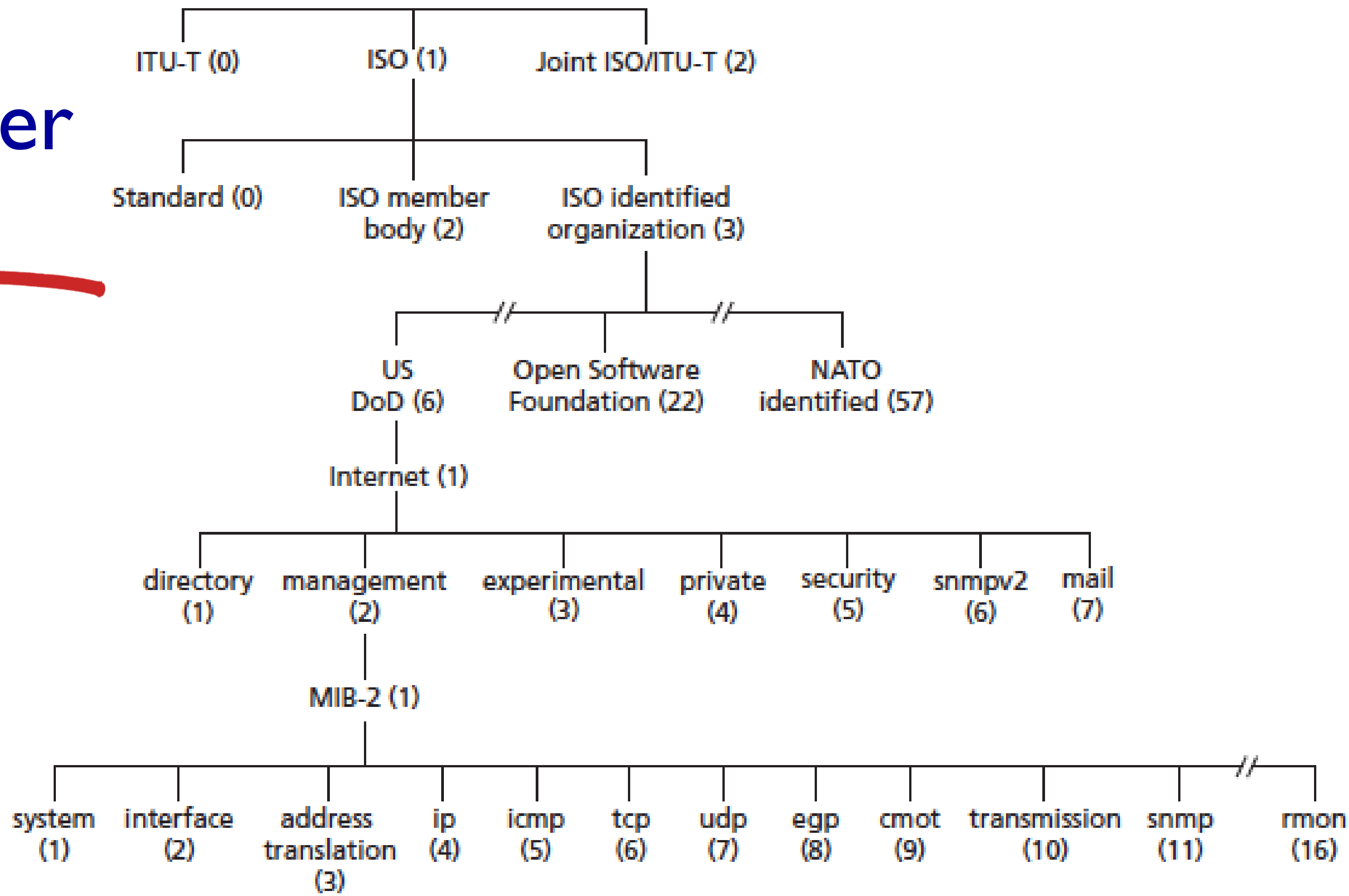
question: how to name every possible standard object (protocol, data, more..) in every possible network standard??

answer: ISO Object Identifier tree:

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

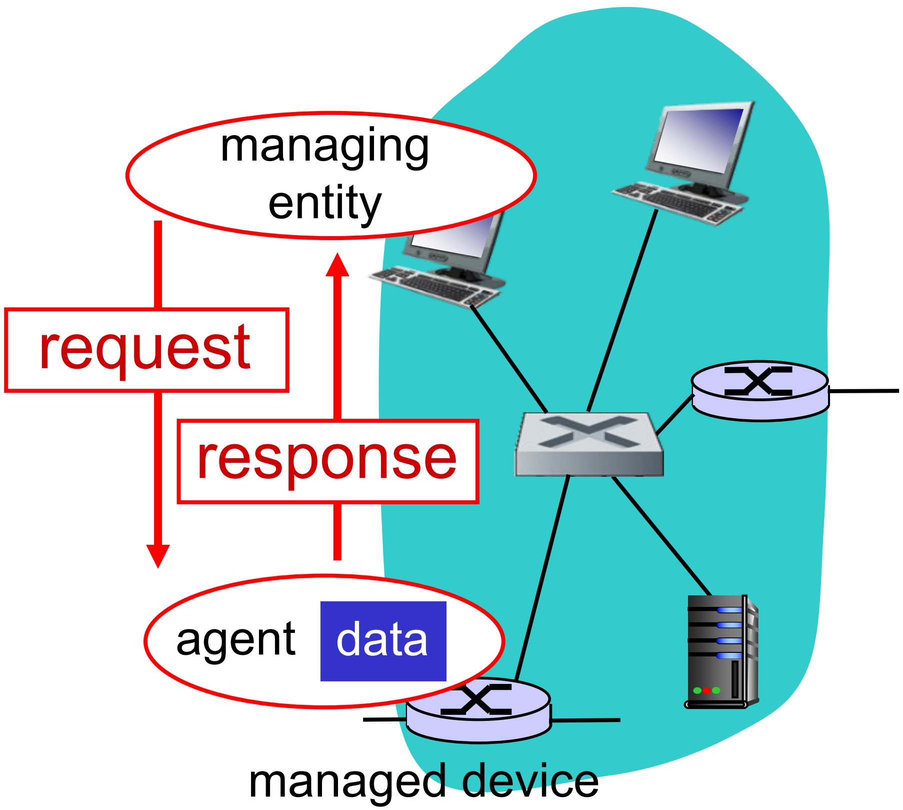


OSI Object Identifier Tree

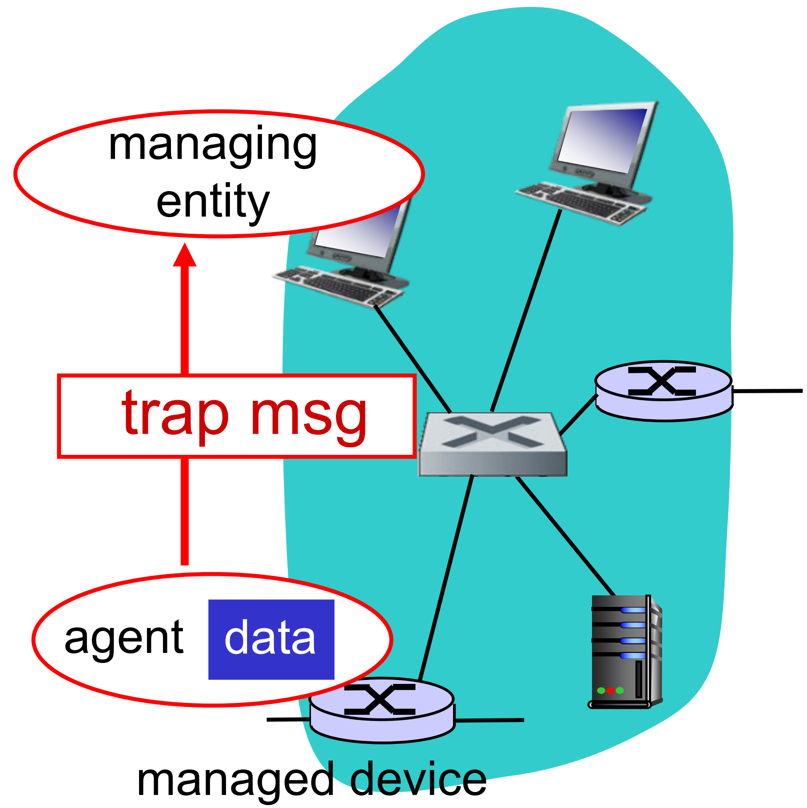


SNMP protocol

Two ways to convey MIB info, commands:



request/response mode

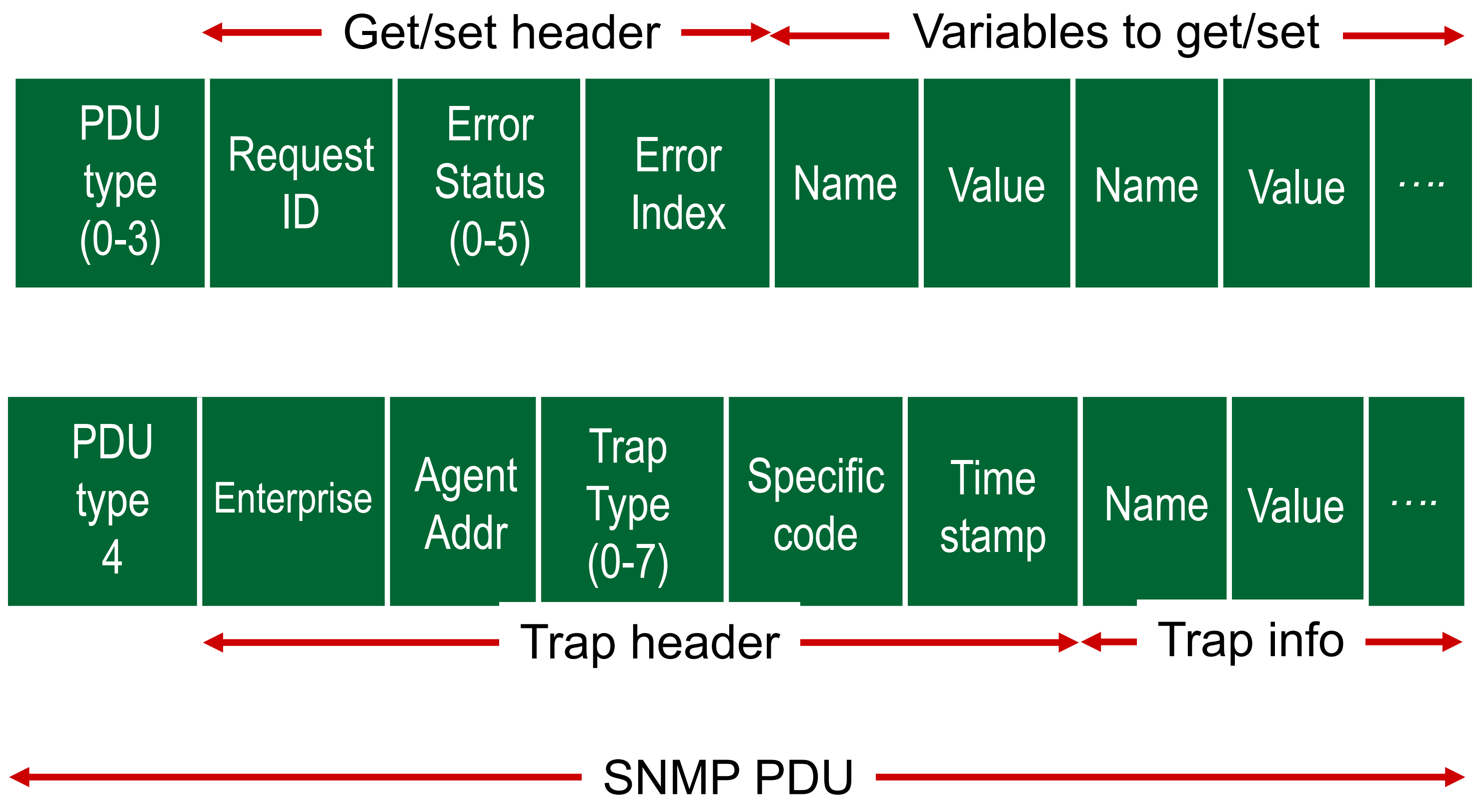


trap mode

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 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

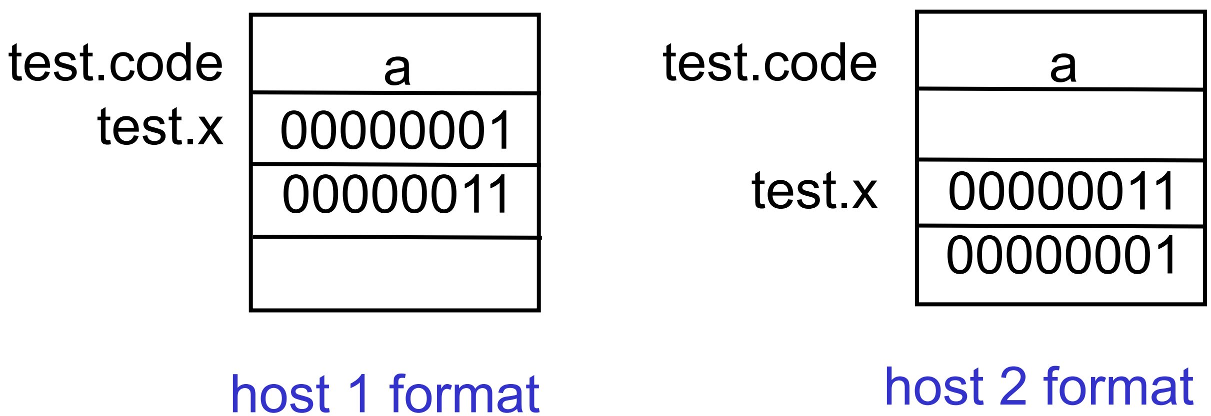
- What is network management?
- Internet-standard management framework
  - Structure of Management Information: SMI
  - Management Information Base: MIB
  - SNMP Protocol Operations and Transport Mappings
  - Security and Administration
- The presentation problem: ASN.1

The presentation problem

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

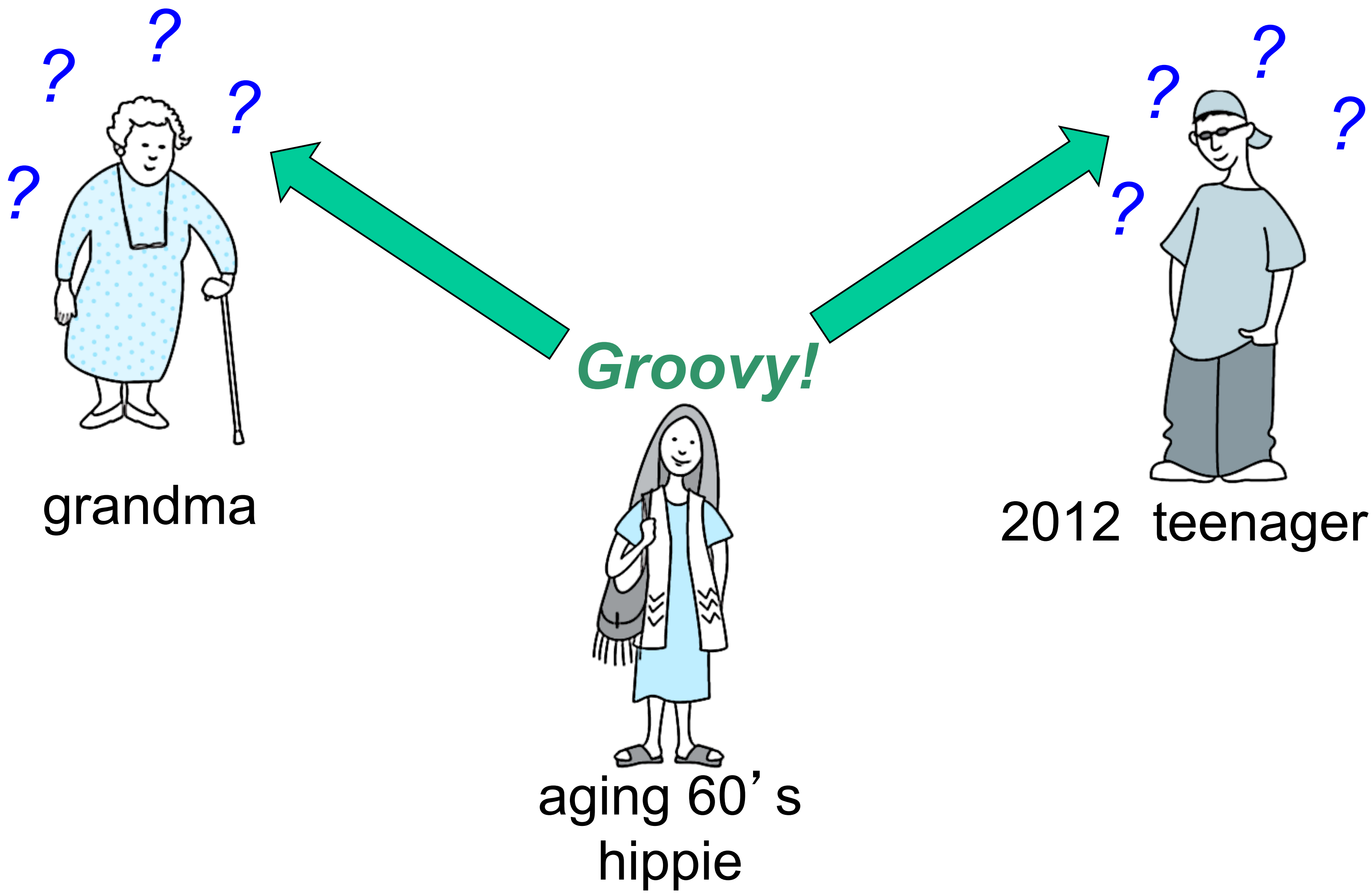
A: not always!

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



problem: different data format, storage conventions

A real-life presentation problem:

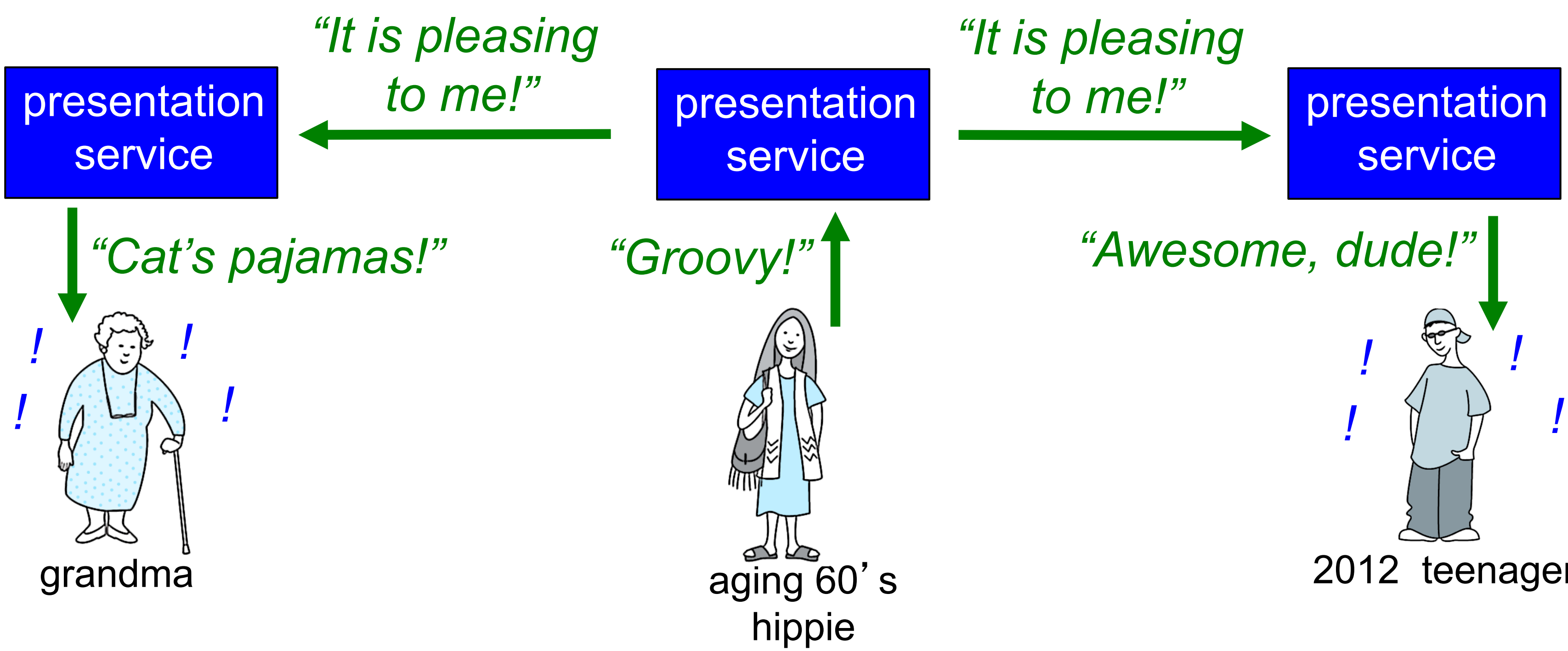


Presentation problem: potential solutions

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

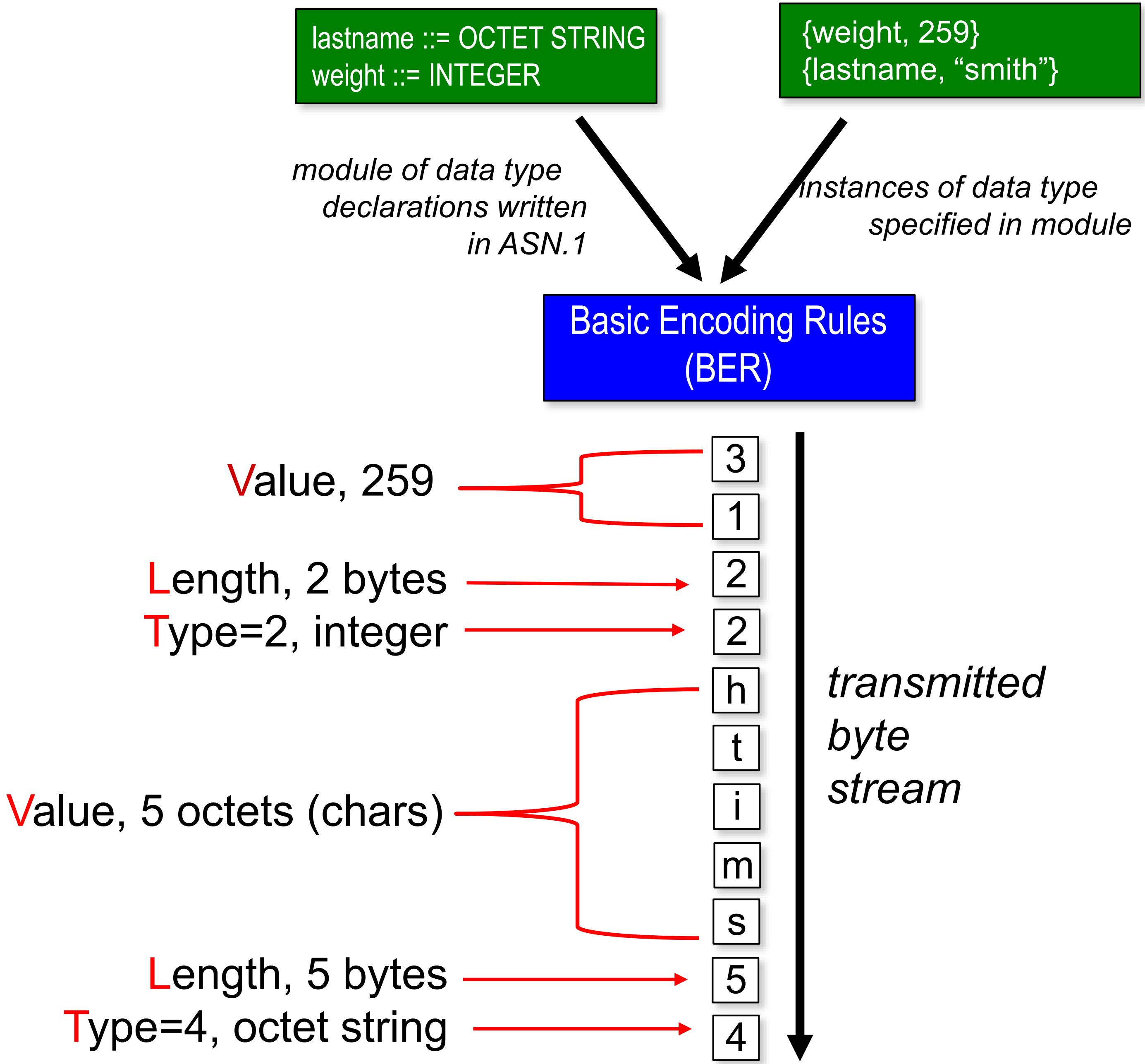
TLV Encoding

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?