

# Network Management

Stuart Johnston

[stuart.johnston@inmon.com](mailto:stuart.johnston@inmon.com)

13 October 2011

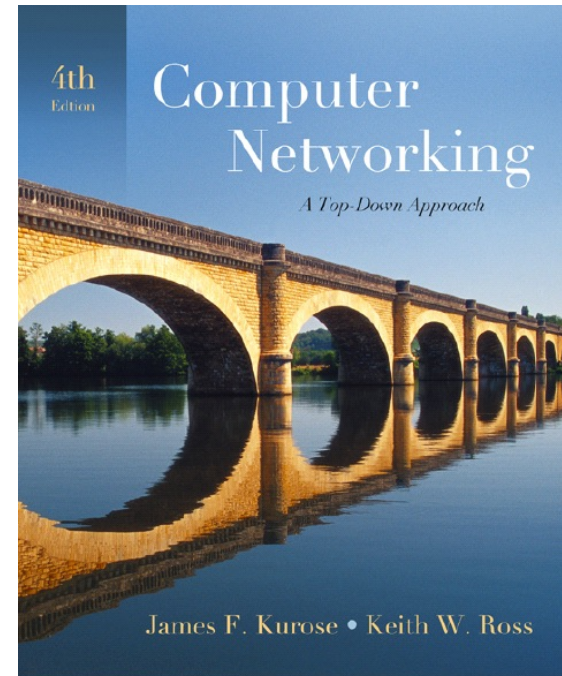
Slides from: Computer Networking: A Top Down Approach, 4th edition.

Jim Kurose, Keith Ross

Addison-Wesley, July 2007

All material copyright 1996-2007

J.F Kurose and K.W. Ross, All Rights Reserved



# Network Management: objectives

- ❑ 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
- ❑ Traffic management

# Lecture 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
- ❑ Traffic management

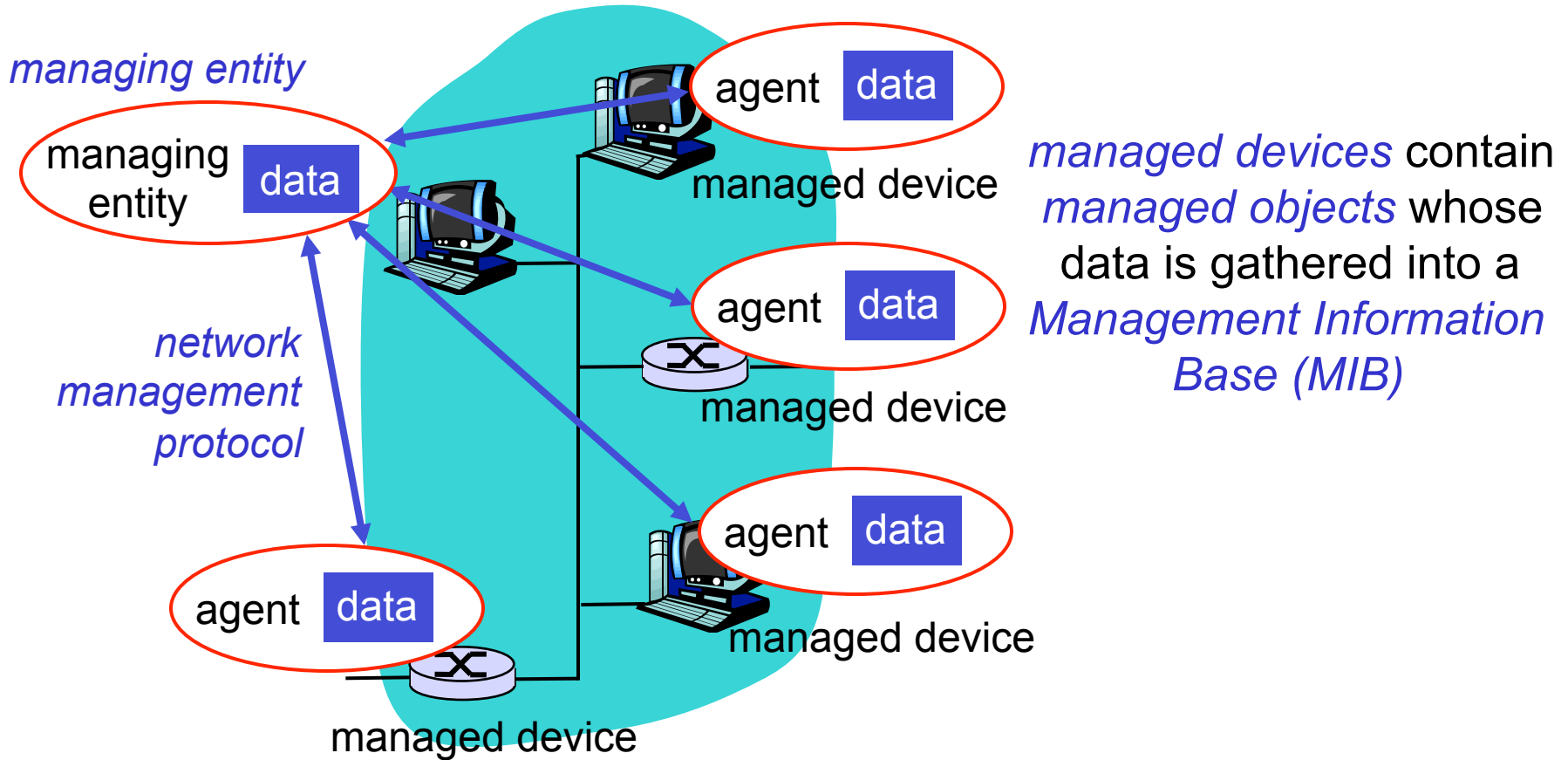
# What is network management?

- ❑ **network:** autonomous system of 100s, 1000s or 10000s interacting hardware/software components
- ❑ **management:** accomplishing goals and objectives, efficiently and effectively
- ❑ **network management:**
  - configuration of the network
  - monitoring equipment performance
  - monitoring network traffic
  - meeting business goals: eg partitioning of users, billing
  - dealing with issues – equipment failure, overload, malicious attacks, ...
  - change management

# Why bother?

- ❑ Mission critical networks: most businesses, governments depend on the network
- ❑ Safety-critical networks: running power plants, hospitals, etc
- ❑ Internet outages have global impact
- ❑ Networks are too large and complex to function without sophisticated management
- ❖ Management represents a substantial proportion of cost of network ownership: must be effective
- ❑ In this lecture we focus on device management

# Infrastructure for network management: definitions



# Network Management standards

## OSI CMIP

- ❑ Common Management Information Protocol
- ❑ designed in 1980s: *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 protocol

# Lecture 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
- ❑ Traffic management

# 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

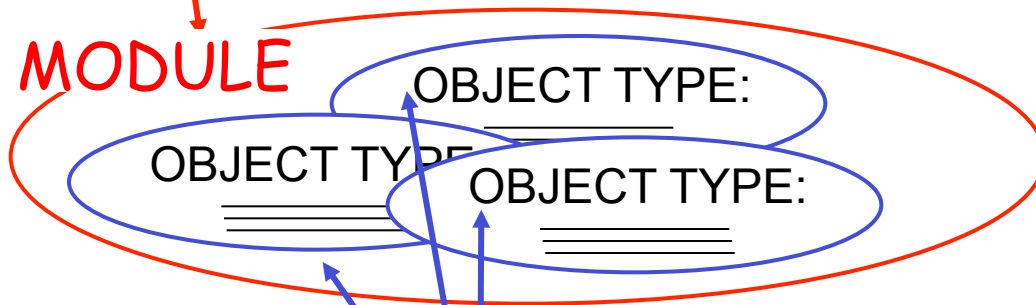
INTEGER  
Integer32  
Unsigned32  
OCTET STRING  
OBJECT IDENTIFIER  
IPAddress  
Counter32  
Counter64  
Gauge32  
Time Ticks  
Opaque

# SNMP MIB

MIB module specified via SMI

**MODULE-IDENTITY**

(100 standardized MIBs, more vendor-specific)



objects specified via SMI  
**OBJECT-TYPE** construct

# SMI: Module and Object examples

## MODULE-IDENTITY: ipMIB

```
ipMIB MODULE-IDENTITY
  LAST-UPDATED "941101000Z"
  ORGANIZATION "IETF SNMPv2
    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 4}

## 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}
```

# MIB example: UDP module

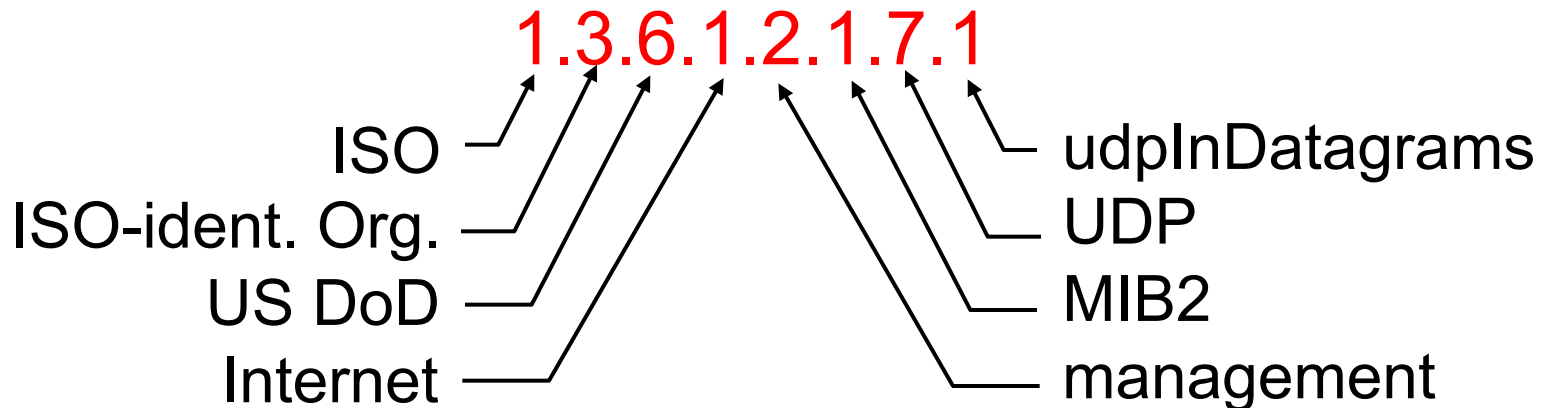
<u>Object ID</u>	<u>Name</u>	<u>Type</u>	<u>Comments</u>
1.3.6.1.2.1.7.1	UDPInDatagrams	Counter32	total # datagrams delivered at this node
1.3.6.1.2.1.7.2	UDPNoPorts	Counter32	# undeliverable datagrams no app at port
1.3.6.1.2.1.7.3	UDInErrors	Counter32	# undeliverable datagrams all other reasons
1.3.6.1.2.1.7.4	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

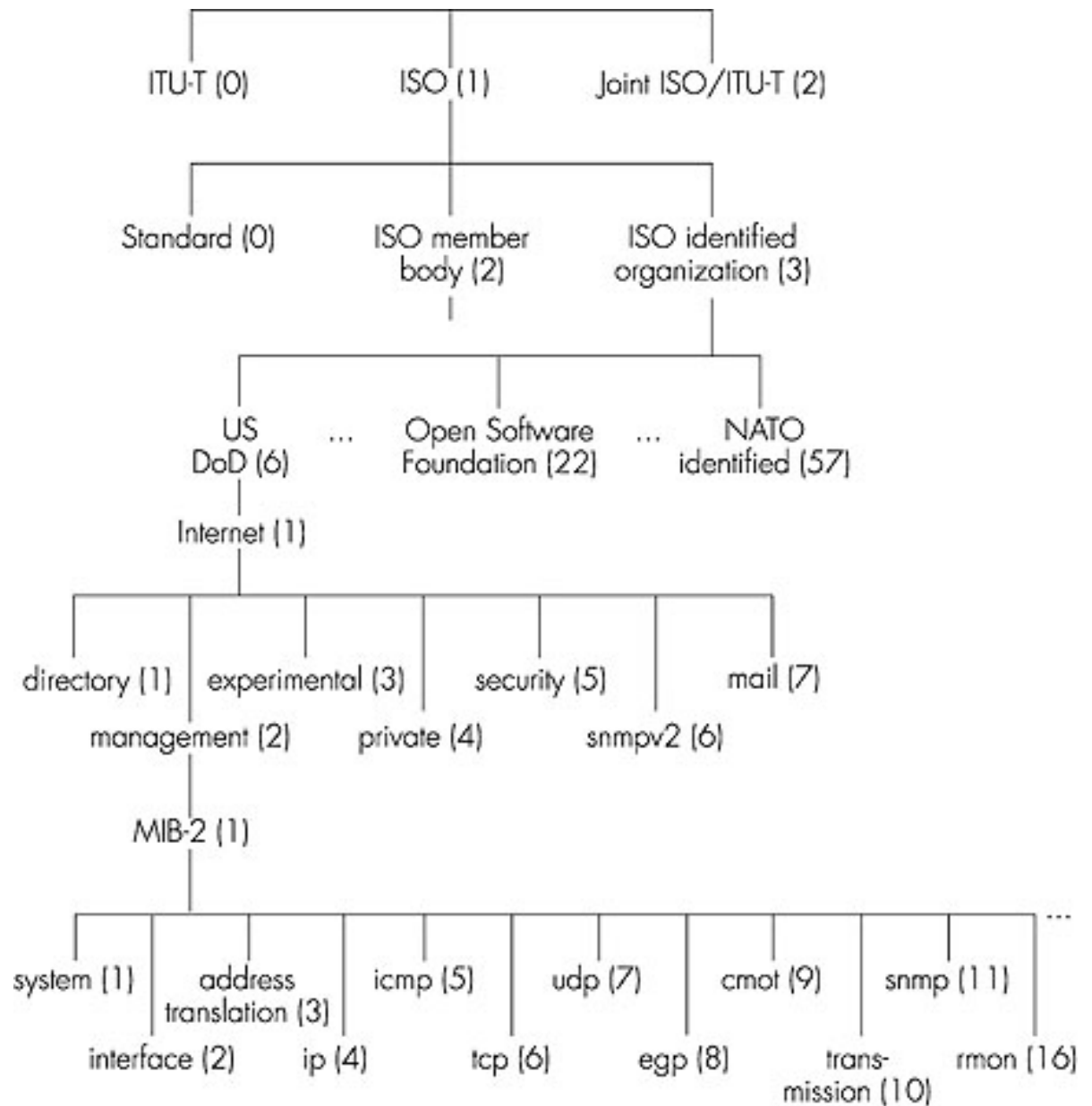
question: how to name every possible standard object (protocol, data, more..) in every possible network standard?

answer: *ISO Object Identifier tree:*

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



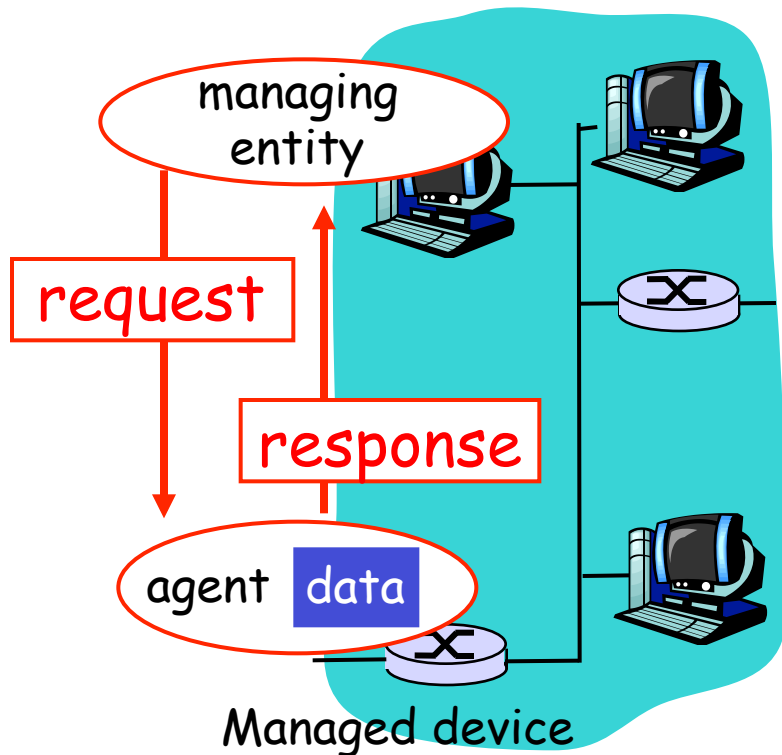
# OSI Object Identifier Tree



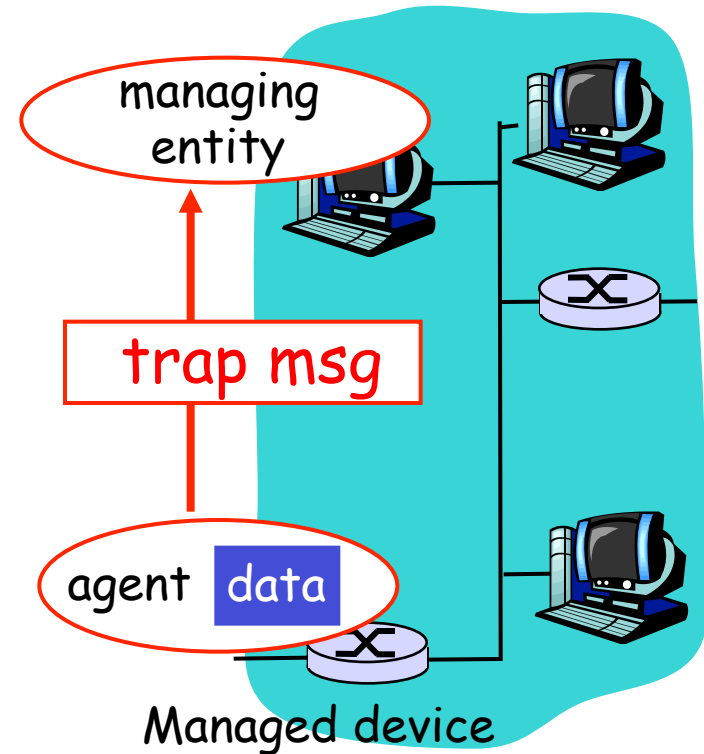
Check out [www.alvestrand.no/objectid/top.html](http://www.alvestrand.no/objectid/top.html)

# SNMP protocol

Two ways to convey MIB info, commands:



request/response mode

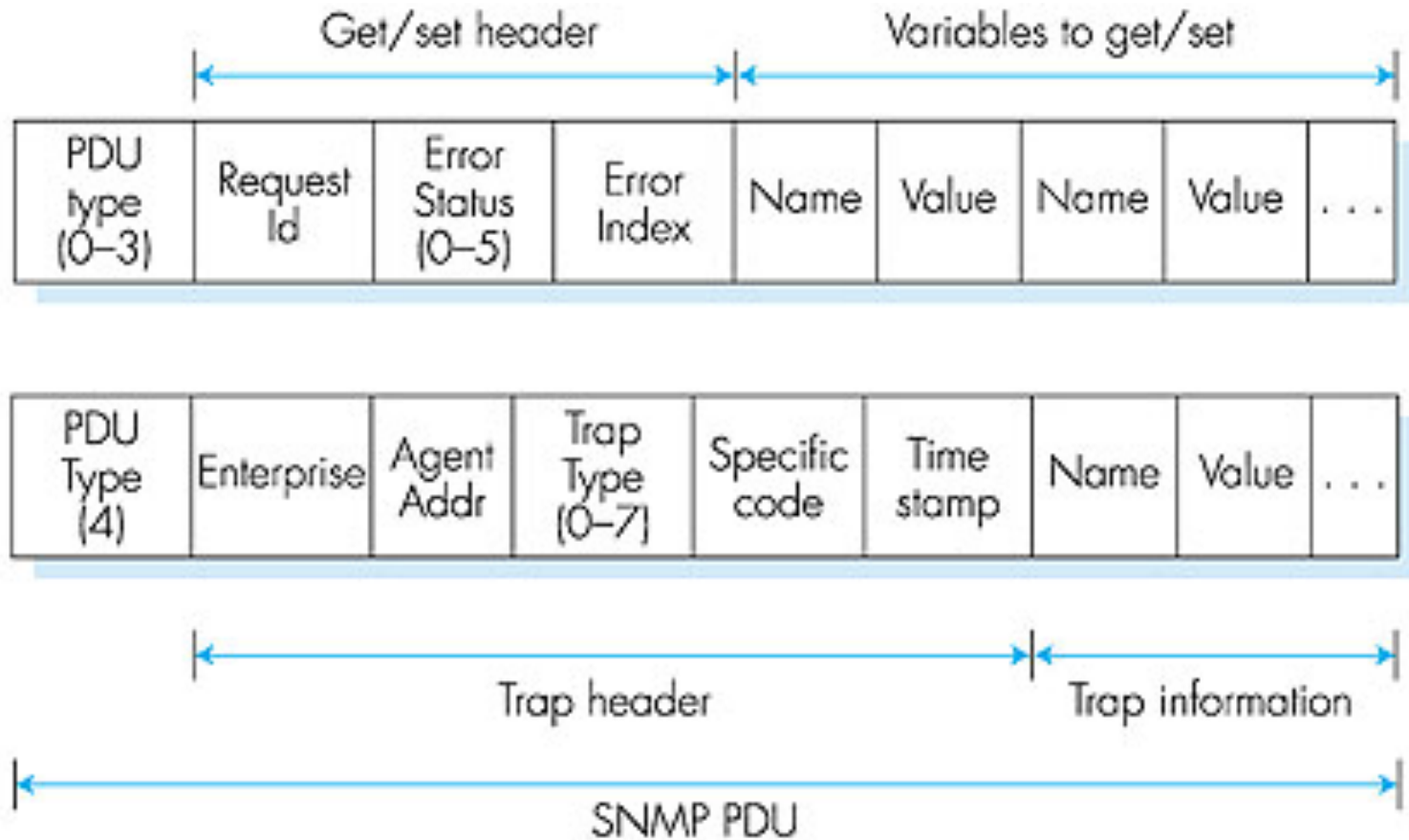


trap mode

# SNMP protocol: message types

<u>Message type</u>	<u>Function</u>
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

- ❑ SNMP v2c provides minimal security
  - Simple password (“*community string*”), transmitted in clear, for read and write access
  - Switches often provide a management VLAN to segregate SNMP traffic
  - Many networks do not allow SNMP writes
- ❑ SNMP v3 addresses security
  - Adds authentication, encryption, role-based permission

# SNMP v3 security features

- ❑ **encryption:** DES-encrypt SNMP message
- ❑ **authentication:** compute, send  $\text{MIC}(m,k)$ :  
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!

# Lecture outline

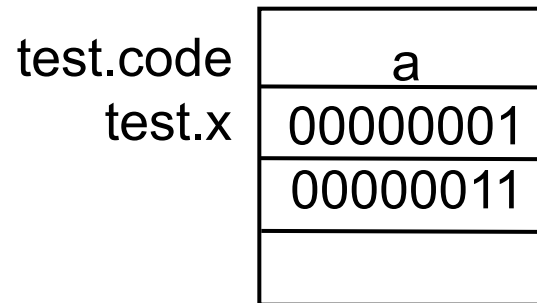
- ❑ What is network management?
- ❑ Internet-standard management framework
  - Structure of Management Information: SMI
  - Management Information Base: MIB
  - SNMP Protocol Operations and Transport Mappings
  - Security and Administration
- ❑ **The presentation problem: ASN.1**
- ❑ Traffic management

# The presentation problem

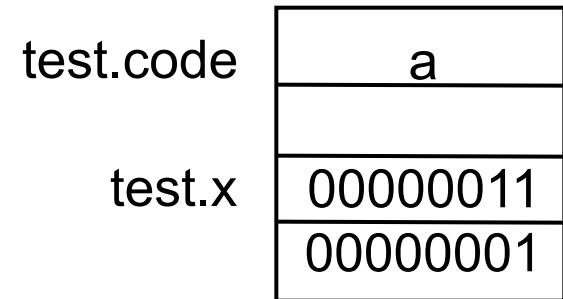
Q: does perfect memory-to-memory copy solve “the communication problem”?

A: not always!

```
struct {  
    char code;  
    int x;  
} test;  
test.x = 259;  
test.code = 'a'
```



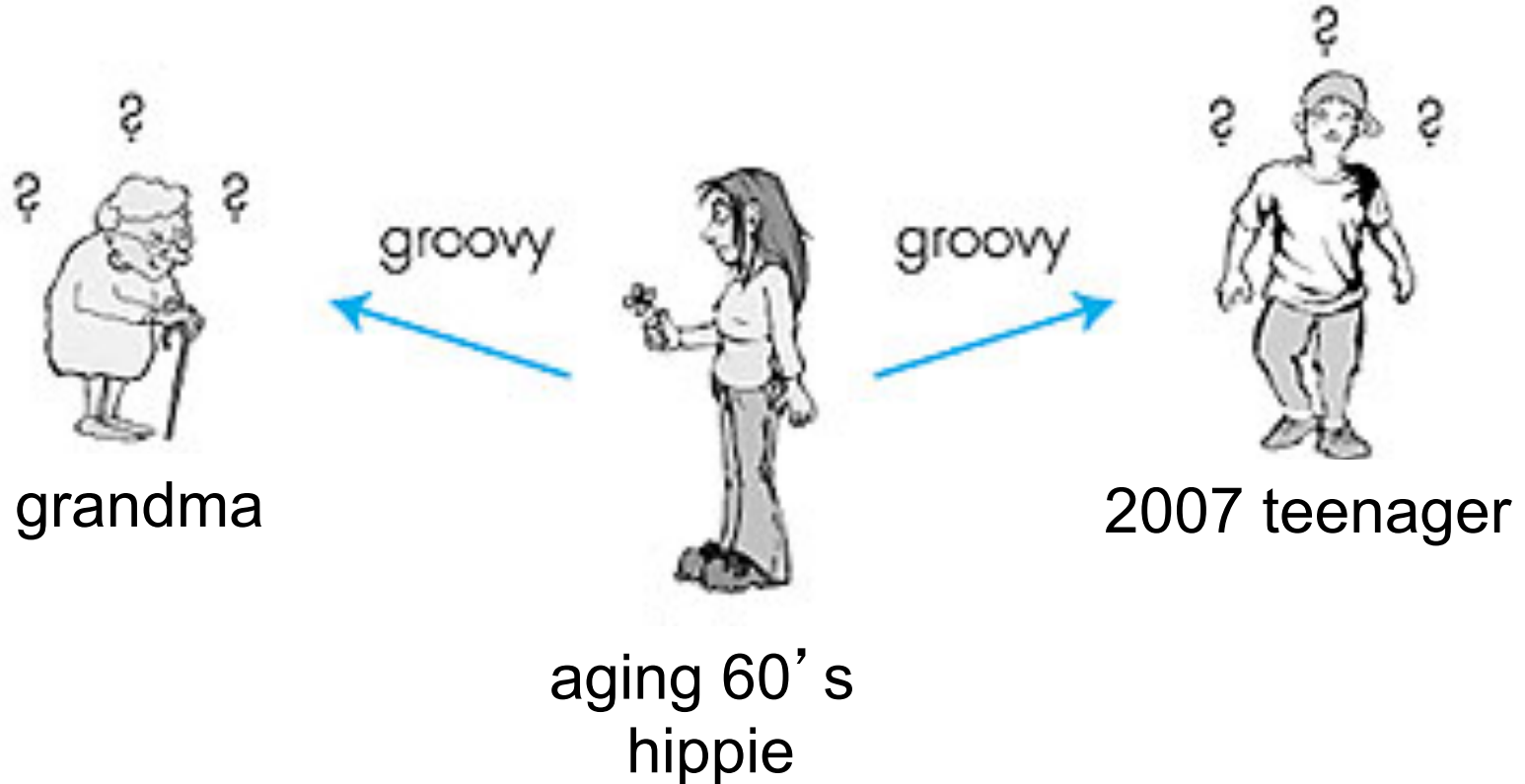
host 1 format



host 2 format

problem: different data format, storage conventions

# A real-life presentation problem:

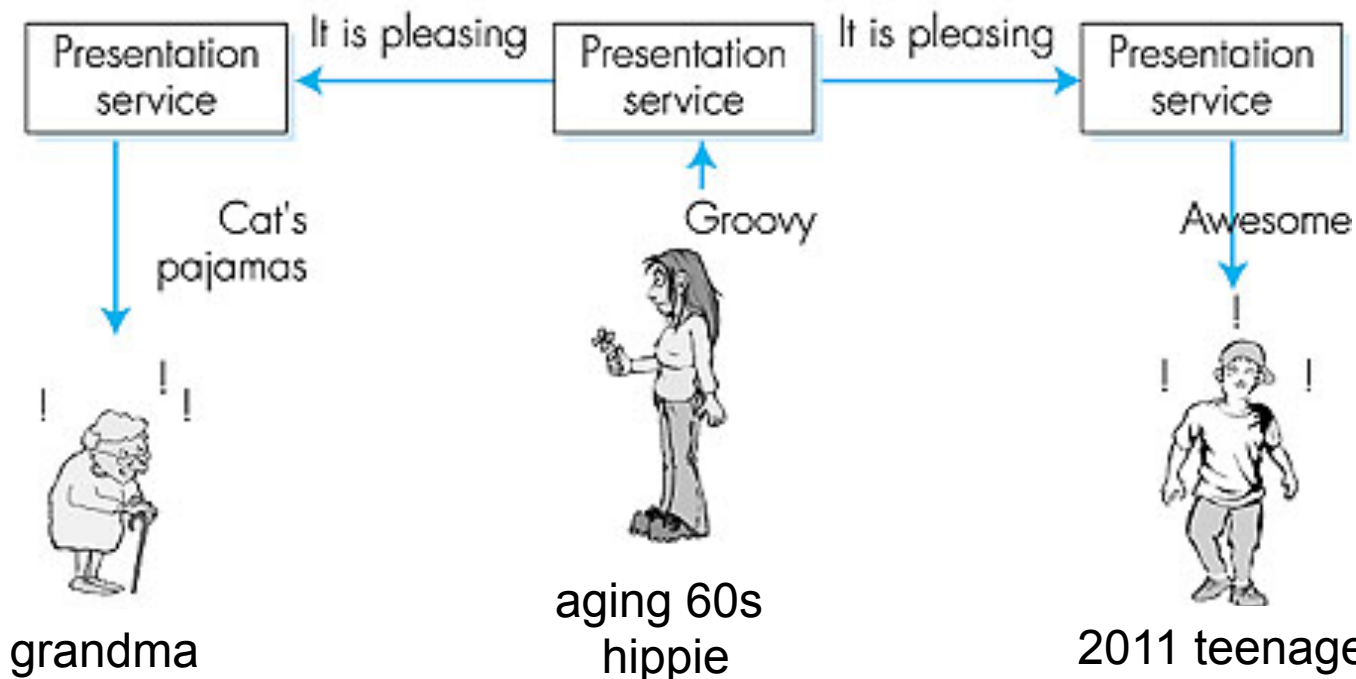


# Presentation problem: potential solutions

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 to 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

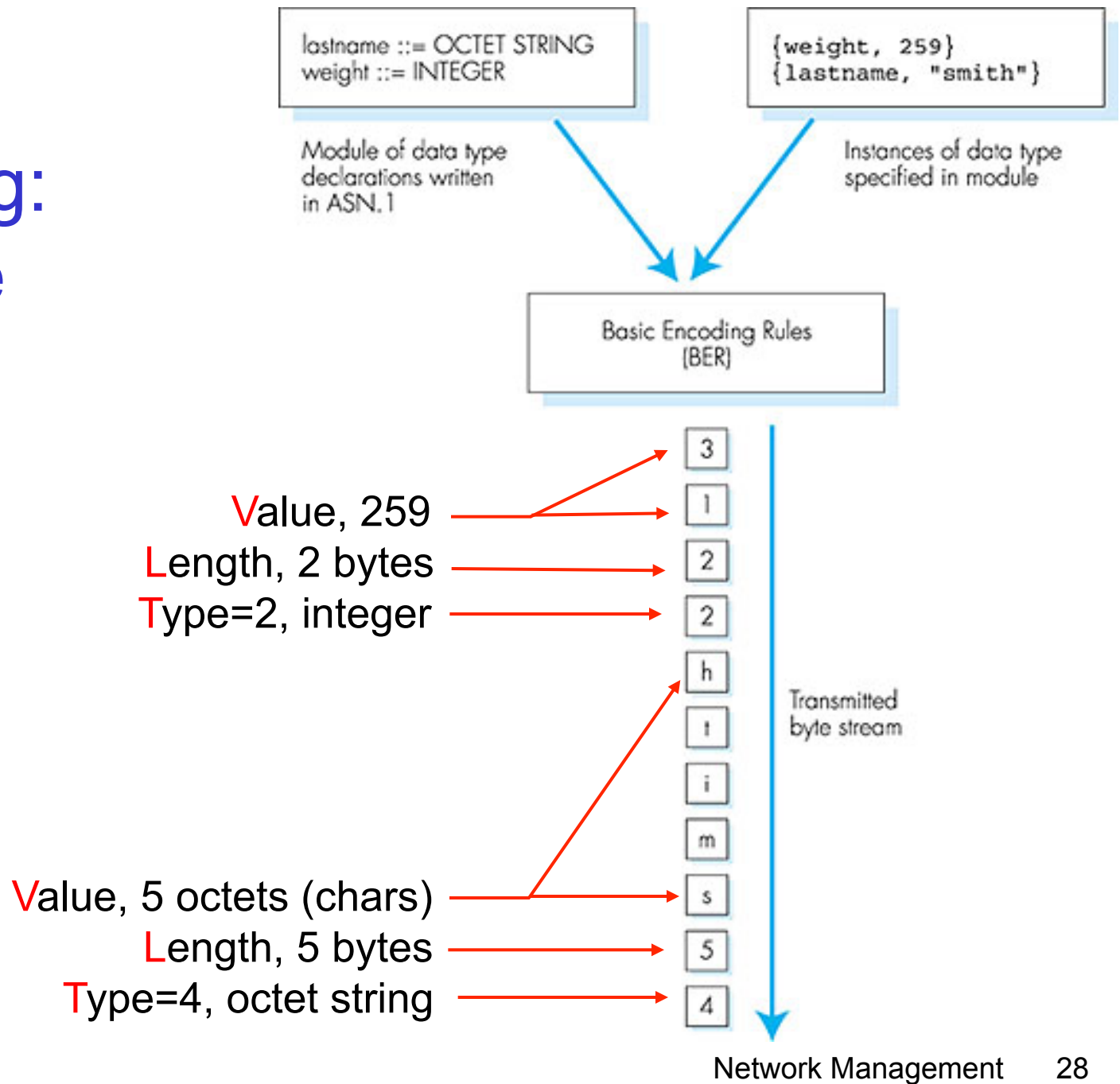
# TLV Encoding

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

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

# TLV encoding: example



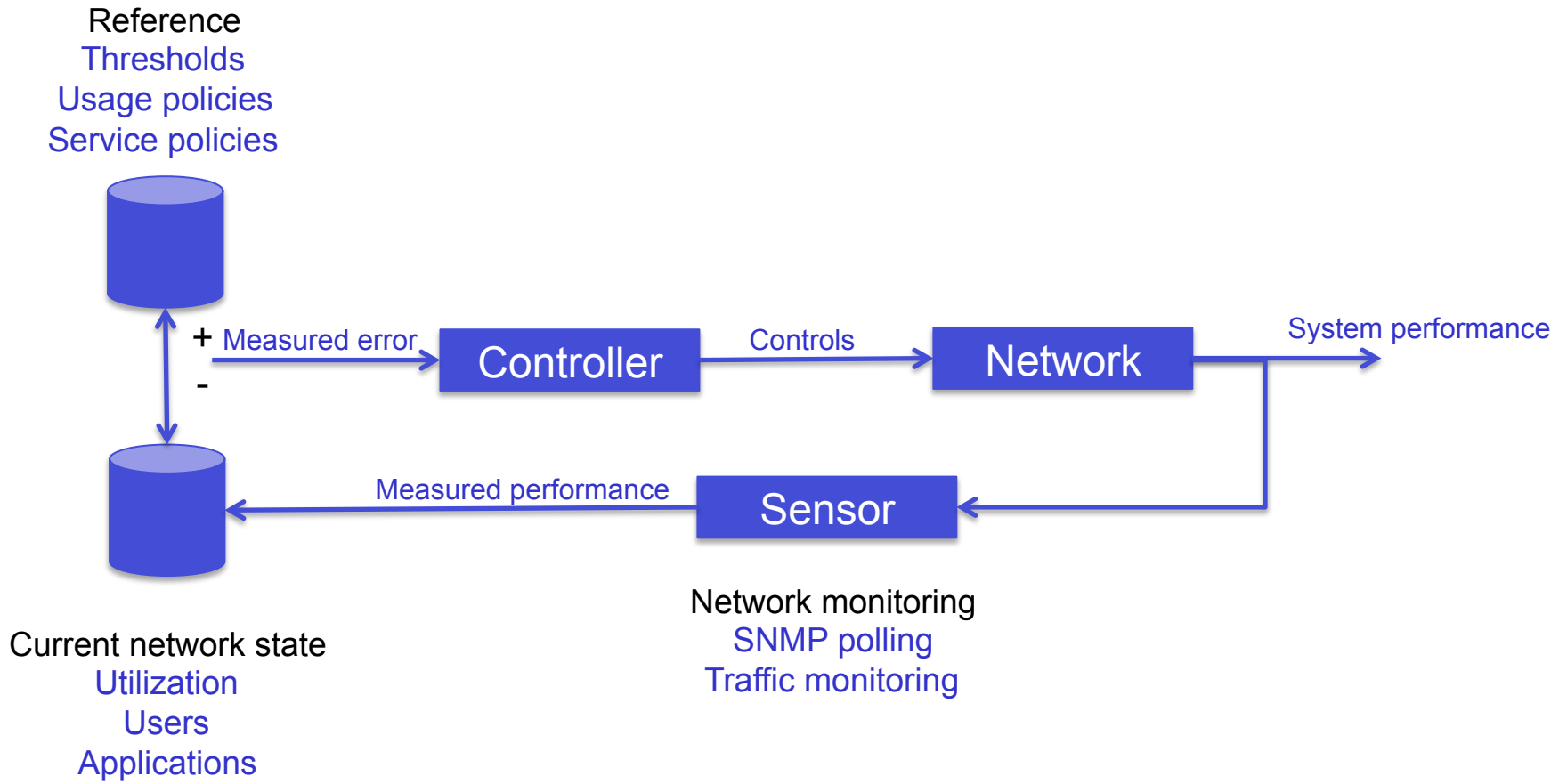
# Lecture outline

- ❑ 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
- ❑ **Traffic management**

# What is network traffic management?

- ❑ Understanding the use of the network
- ❑ Understanding the requirements of users
- ❑ Measuring how well user requirements are met
- ❑ Making changes to improve the quality of service experienced by users
- ❑ Monitoring the effectiveness of the changes
- ❑ Monitoring network traffic is an effective way to measure demand and usage

# Control theory applied to network management



# Traffic management applications

- ❑ Detecting and resolving congestion
- ❑ Identifying and correcting performance problems
- ❑ Identifying and mitigating security breaches
- ❑ Planning for future growth and new applications
- ❑ Billing for usage

# Network management in practice

## ❑ Network configuration

- Understanding the network
- Configuring each network device to interoperate and meet business objectives

## ❑ Network monitoring

- Alerts from network components prior to failure – proactive
- Troubleshooting problems – reactive
- Understanding *what* the network is used for – traffic management

## ❑ Network control

- Responding to alerts and resolving issues
- Managing changes to configuration, and software updates
- Planning future upgrades

# Network management: summary

- ❑ Critical for modern complex networks
- ❑ Device management
  - SNMP used for conveying information
  - ASN.1 for data description
- ❑ Network management: more art than science
  - what to measure/monitor
  - how to respond to failures?
  - alarm correlation/filtering?