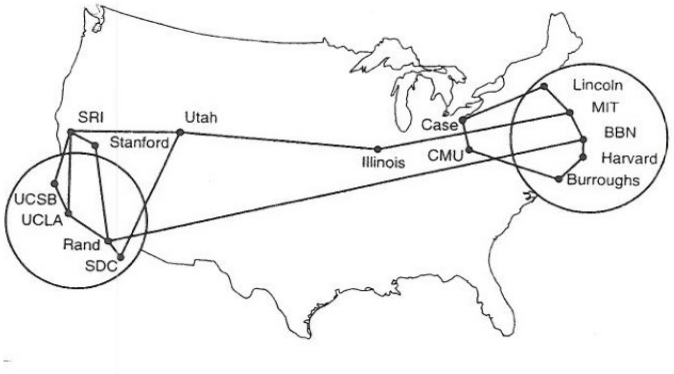


Network Management

Reading: Section 9.1

Goals:

- Understand Network Management Problem
- Understand SNMP Approach
- Understand SNMP Protocol

Network Management

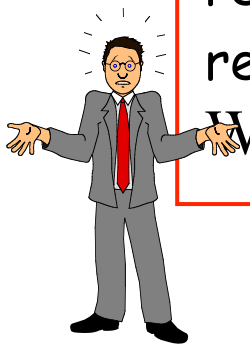
Outline:

- 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

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?

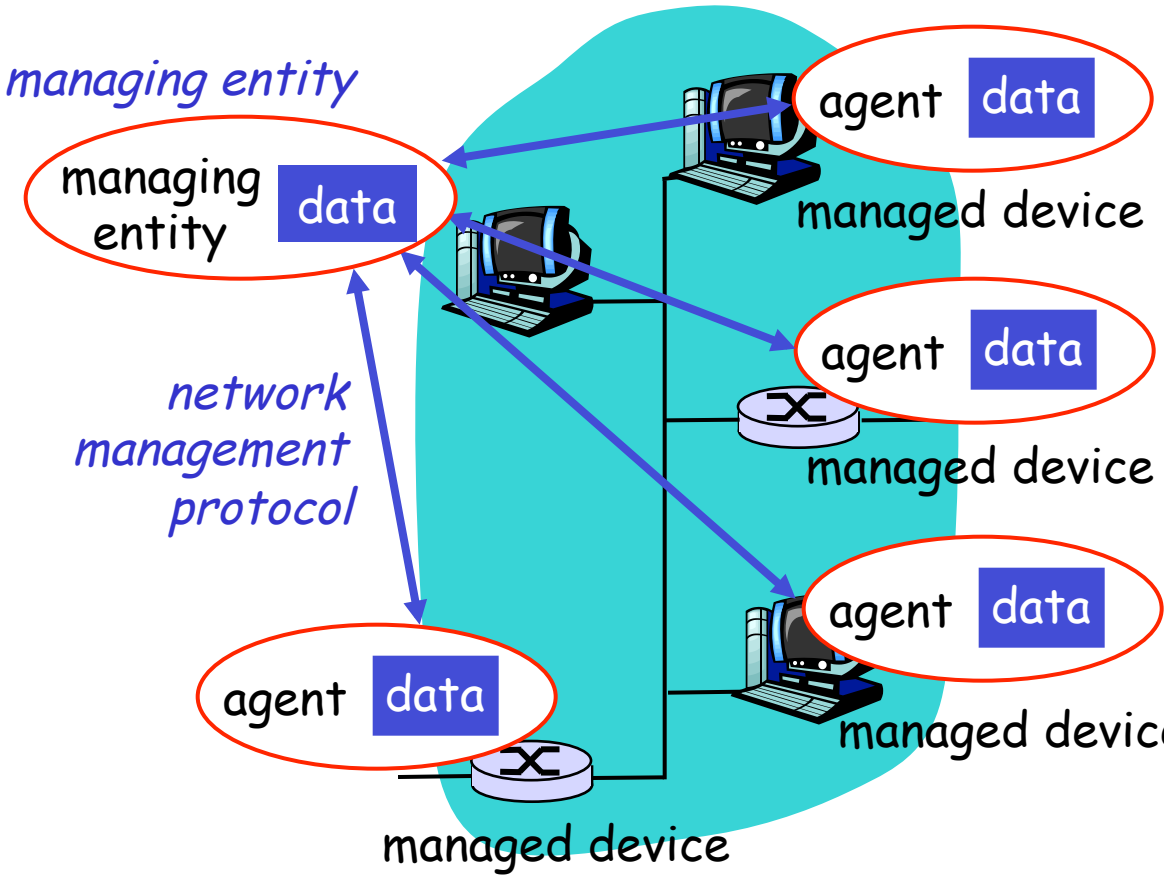
"Network management includes the deployment, integration and coordination of the hardware, software, and human elements to monitor, test, poll, configure, analyze, evaluate, and control the network and element resources to meet the real-time, operational performance, and Quality of Service requirements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



No standard Link Protocol

Architecture for network management
Standard Paradigm, Protocols. Different Tools

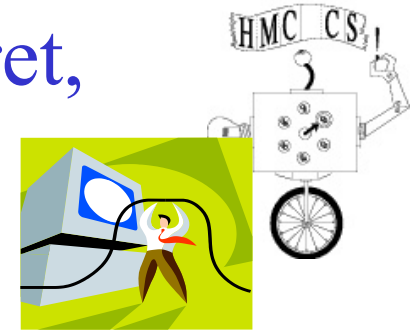
definitions:

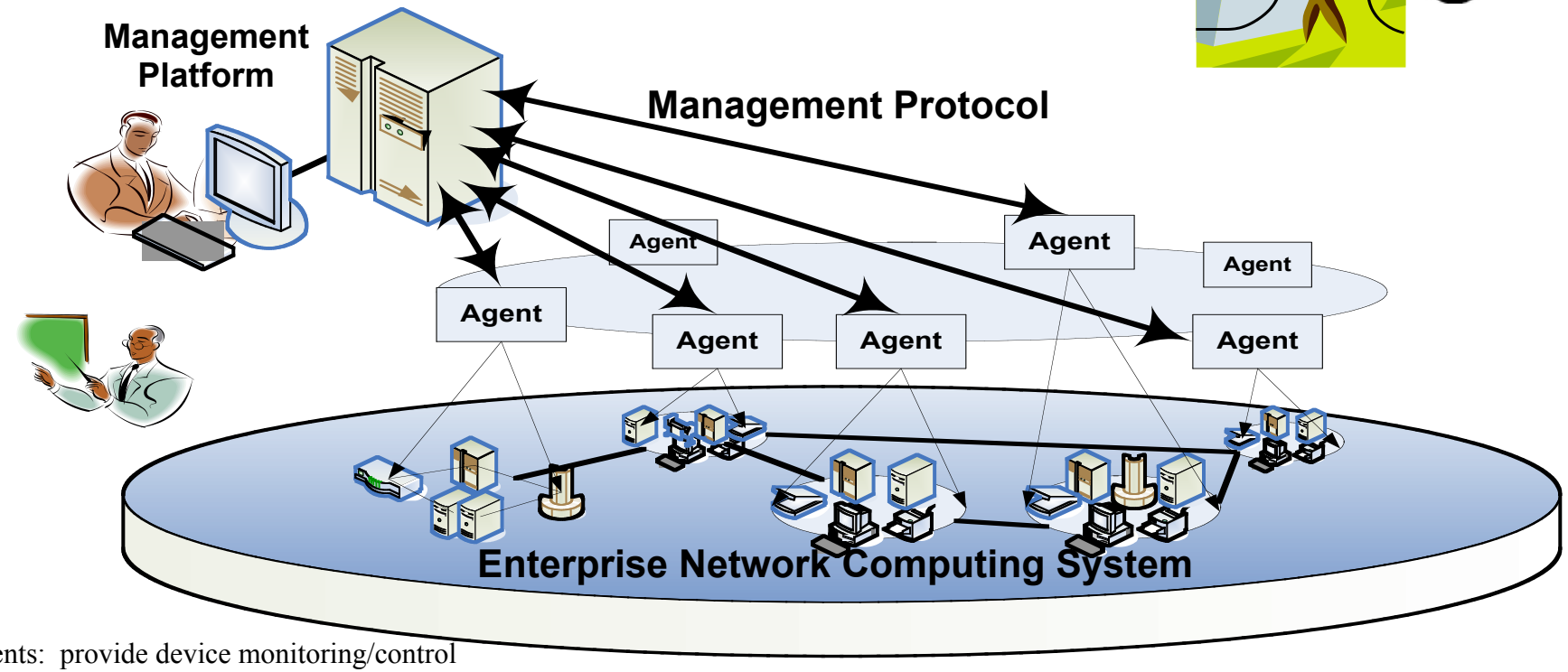


managed devices contain *managed objects* whose data is gathered into a *Management Information Base (MIB)*

Develop Local Policies

Management Model = Monitor, Interpret, Control





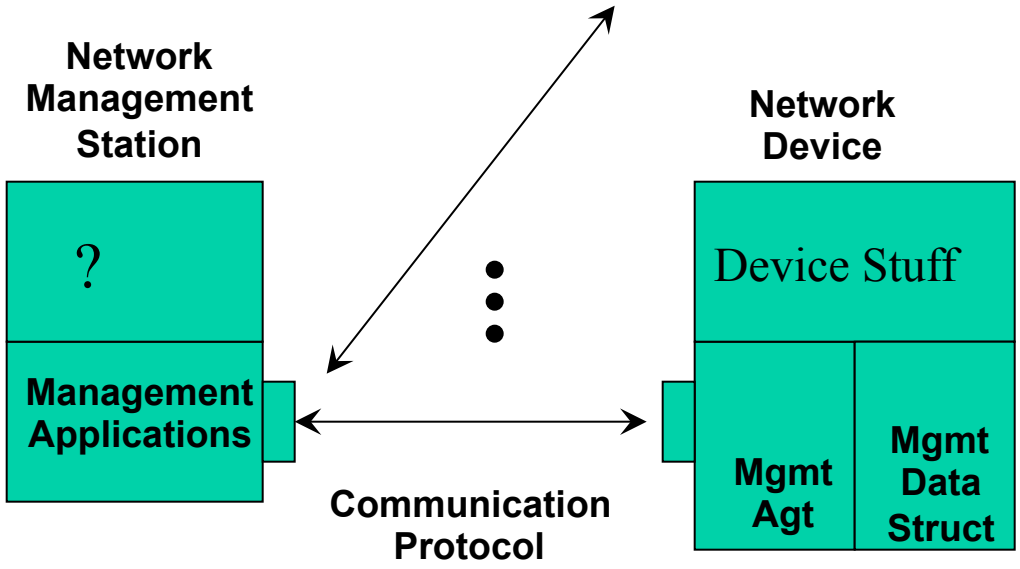
- Agents: provide device monitoring/control
- Platform: interpretation of NM data & control
- Management protocol: queries of device data
- Management Information Bases (MIB): standardize management data representation & access
- Picture shows that NetMgt is in another network 'plane'

Network Management Issues

Operation costs dominate network management

- Cost of equipment: commodity market
- Complexity of network operations is driven up by
  - Growth in scale and heterogeneity
    - 2 LANs vs 100 LANs
  - Shift to distributed computing requires distributed management
- Operations depend on costly expert staff
  - "Lights out" is a myth
- Operational and Management Planes are combined in the network – fear that NM could take over the network.

Network Management: The Model



Network Management Paradigm
Add NM onto a Nodes Functionality

The Model: Network Management System

Network Management Station

- Execute management applications
- Monitor and control network elements
- May be fancy or useful or both; may be character, window, or script oriented
- NM application peers with SNMP application entities in the Agents of managed network devices/elements
- Examples: HP OpenView, Spectrum, MRTG
- Can provide WEB based views

The Model: Device – Any Network Node

Network Devices/Elements

- Anything and everything connected to network
- Have a primary task, e.g., router
- Have management agents (Agents) that respond to Network Management Station queries and commands
- Have instrumentation to keep track of network management variables
- Support inter-layer communications mechanisms

Agents

- Agents usually include 2 components:
  - Protocol engine – got to talk on network
  - Management profiles – must agree what to talk about

Network Management standards

OSI CMIP

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

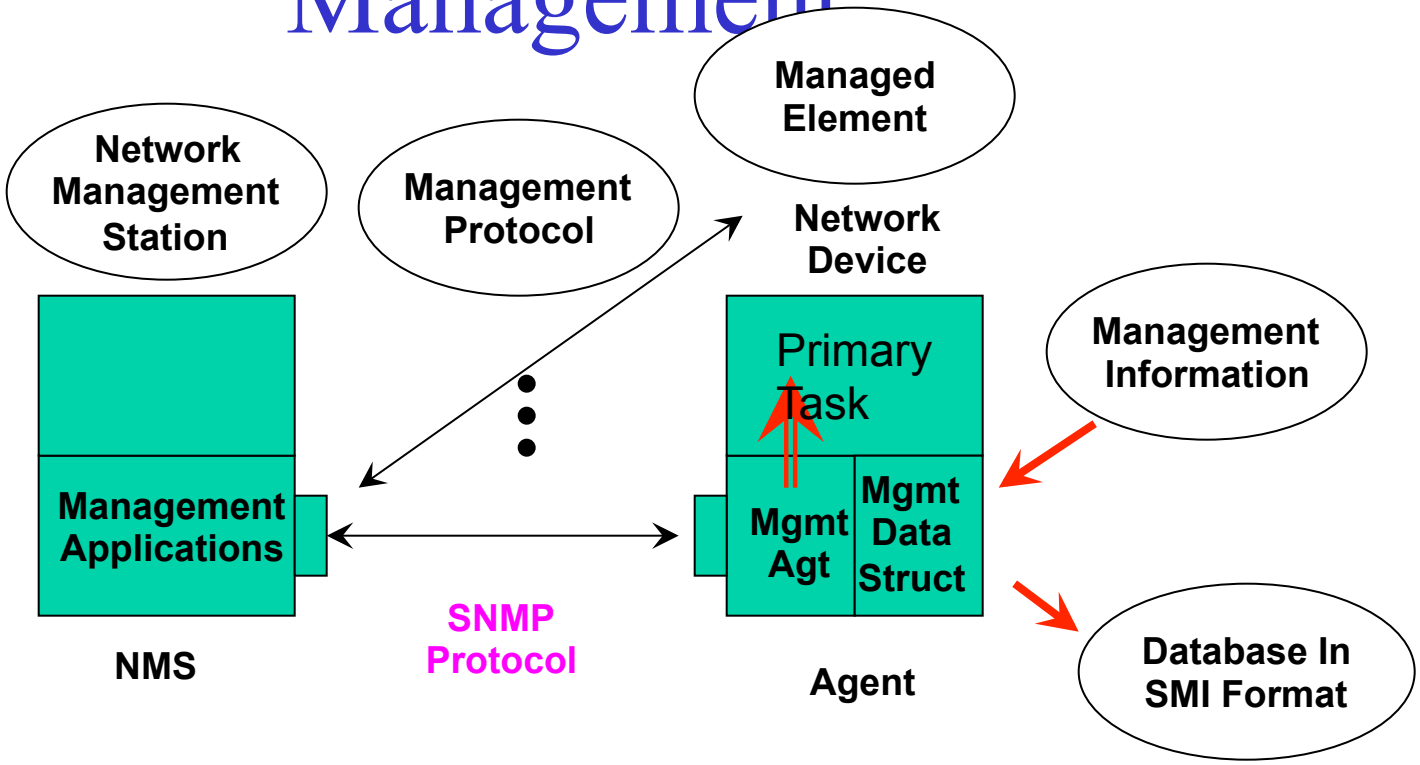
SNMP: Simple Network Management Protocol

- Internet roots (SGMP)
- started simple Why??
- deployed, adopted rapidly
- growth: size, complexity
- currently: SNMP V3
- *de facto* network management standard

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
  - SNMPv1 still dominates (telnet like) Why??

SNMP Based Network Management



Details: SMI
Structure of Management Information

SMI - Structure of Management Information

- Defines how information is structured
- Uses an object information model
- Defines a set of generic types
  - INTEGER, COUNTER, GAUGE, etc.
- Defines rules for MIB documents
- Defines rules for revising MIB documents
- Guarantees consistency of data "Templates"
- "Neither specifies the objects which are managed, nor the protocols used to manage these objects"

Details: Structure of Management Information

SMI

1. Places restrictions on the types of variables allowed in MIB – Integer, Octets, Strings – NO FLOATS
2. Specifies rules for naming these variables
3. Creates rules for defining new types, for example:
   IP address – 4 octet strings
   Counter – Integer 0 to $2^{\wedge 22} - 1$
4. Form of specification:
   Abstract Syntax Notation 1 (ASN.1)
   - Notation used for documents
   - Compact encoded representation of same info for communication
   - Guarantees interoperability unlike two compilers for "Pascal"

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

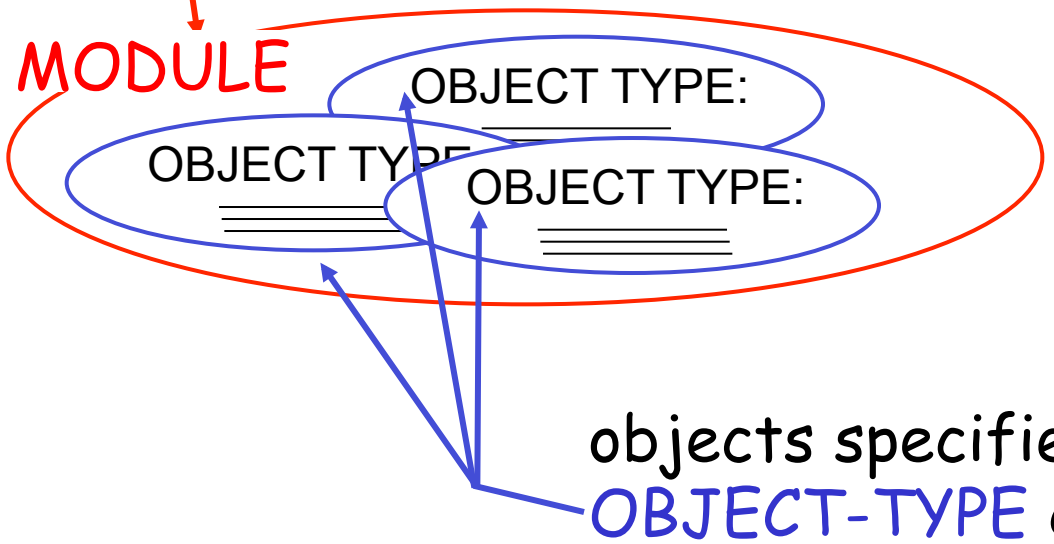
Network Management System Details
Management Information Base
MIB

SNMP MIB

MIB module specified via SMI

MODULE-IDENTITY

(100 standardized MIBs, more vendor-specific)



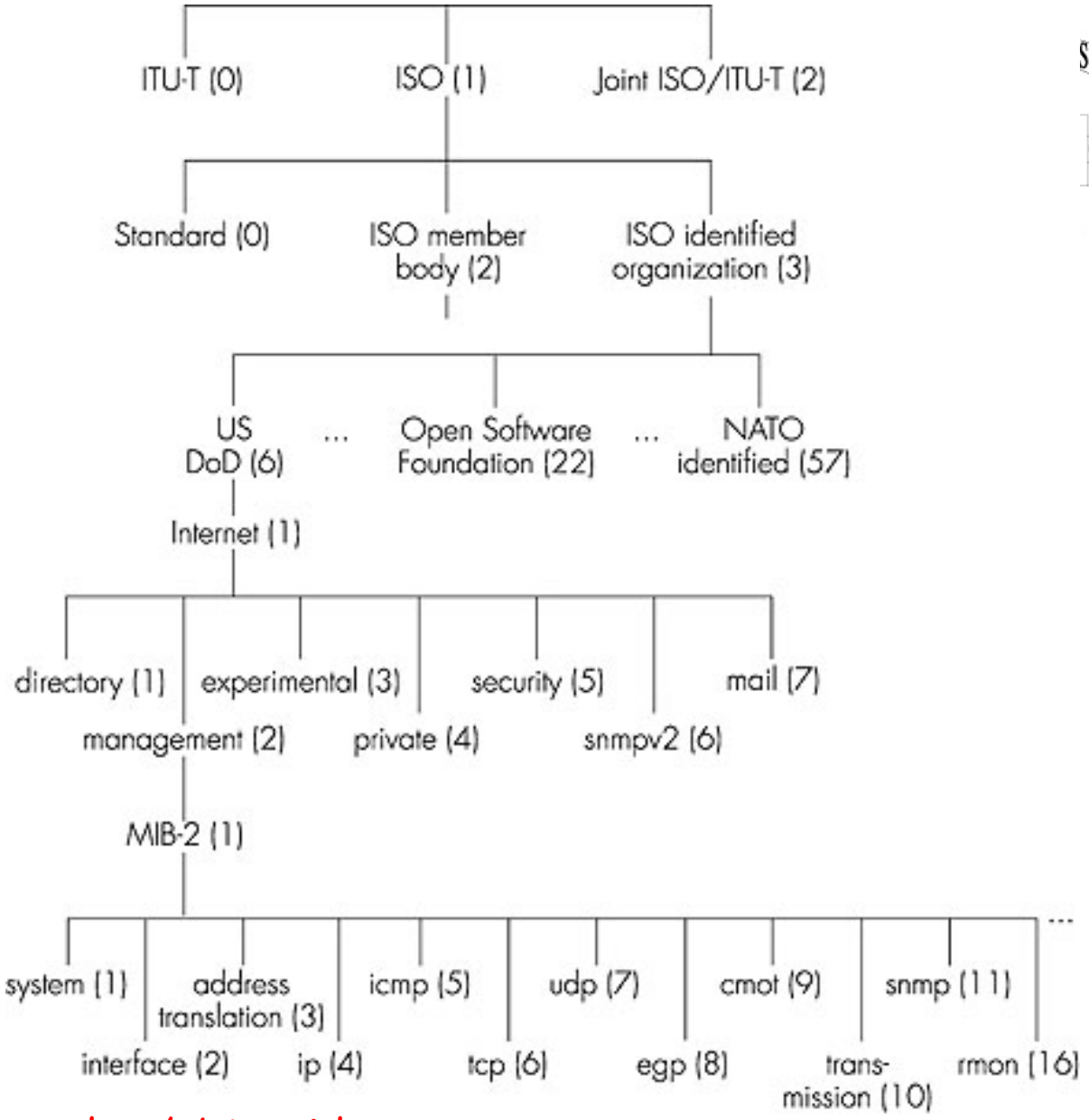
objects specified via SMI

OBJECT-TYPE construct

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 app at portl
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

OSI Object Identifier Tree



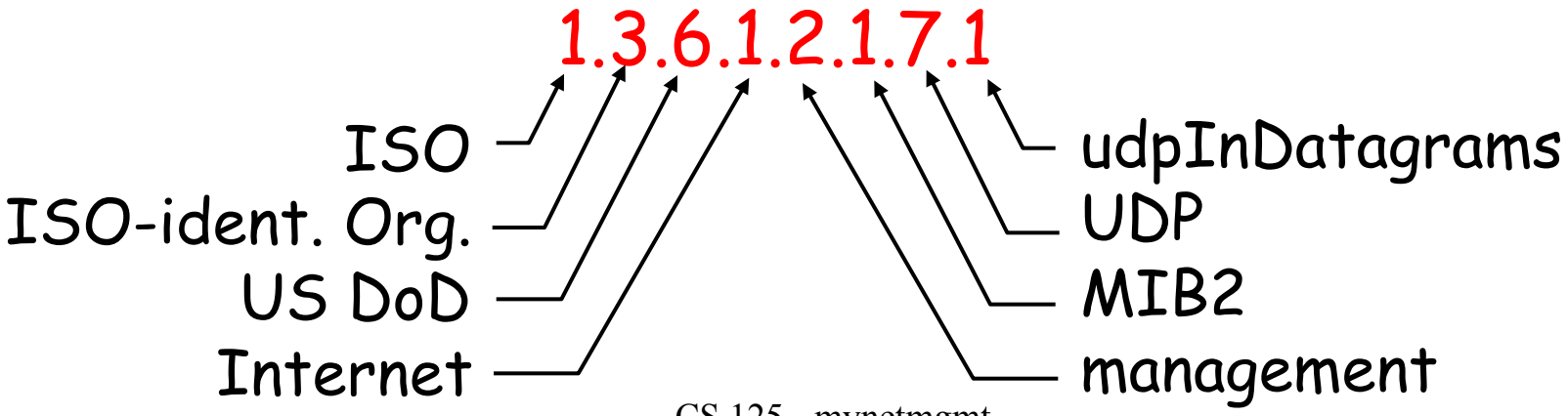
Check out www.alvestrand.no/objectid

SNMP Naming

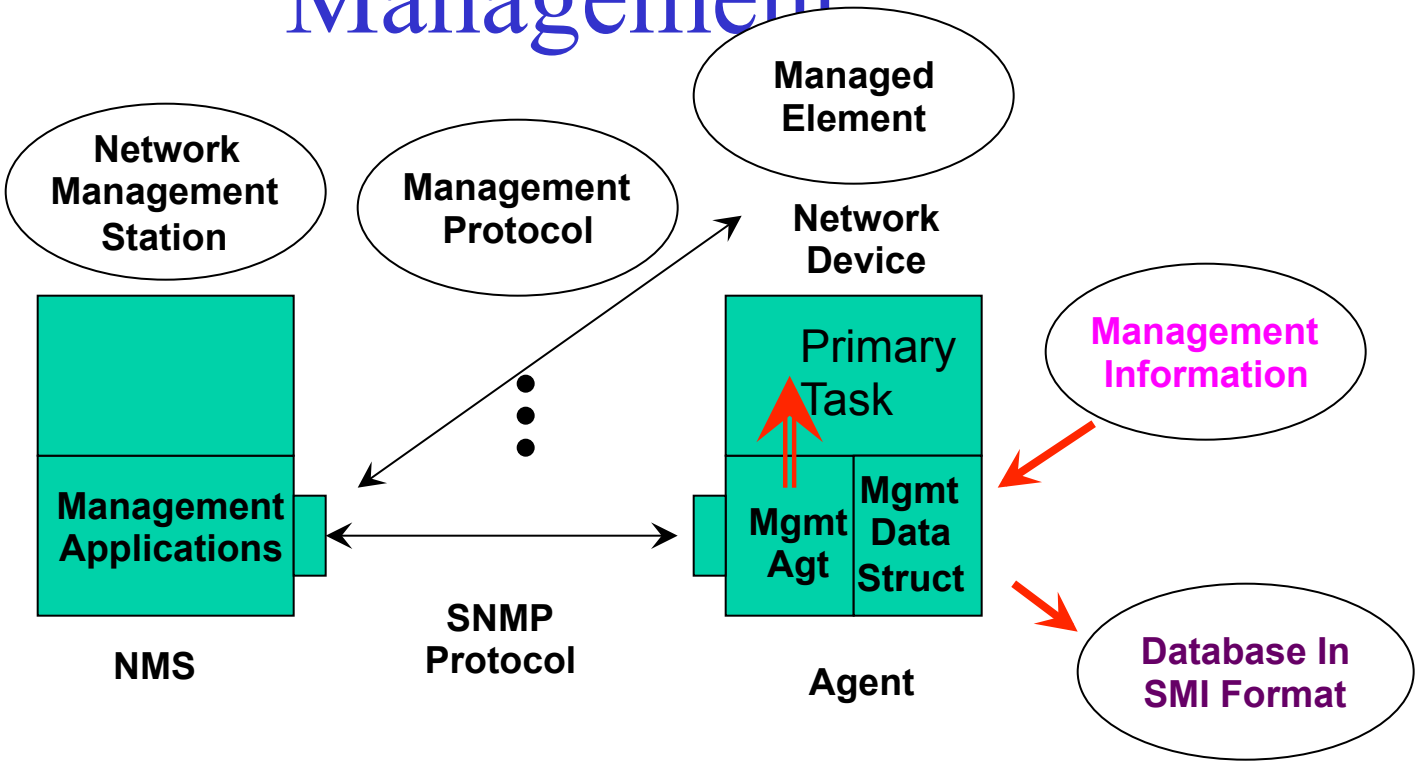
question: how to name every possible standard object (protocol, data, more..) in every possible network standard??

answer: ISO Object Identifier tree:

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



SNMP Based Network Management



Management Information Base

MIB – Management Information Base

- Describes what information is managed
- Defines objects anywhere: protocols, network, nodes, application
- Places information in the tree (Virtual Information Store) defined by the SMI
- Also used to cause action

Management Information Base

Variable Naming

- A variable is named using an OBJECT IDENTIFIER (OID), an administrative assigned unique name
- i.e., 1.3.6.1.2.1.1.1.0
- Symbolic representation of variable names
  - OBJECT DESCRIPTOR synonym for OID used by humans – sysDescr

Management Information Base

Variable Names – Management

- Managed objects accessed via virtual information store – MIB
- MIB Objects defined using Abstract Syntax Notation One (ASN.1)
- MIB conceptually organized as a tree with named edges
- Objects are leaves of the tree (SMI Tree structure)
- Path from root through tree to the object uniquely identifies that object
- Different parts of the tree controlled by different administrative naming authorities – delegated

Example – RFC 1213 MIB-II

Network Working Group
Request for Comments: 1213
Obsoletes: RFC 1158

Perfor

Management Information Base for Ne
of TCP/IP-based intern
MIB-II

Status of this Memo

This memo defines the second version of th
Base (MIB-II) for use with network managem
based internets. This RFC specifies an IA
for the Internet community, and requests d
for improvements. Please refer to the cur
Official Protocol Standards" for the stand
of this protocol. Distribution of this memo is unlimited.

The objects defined in MIB-II ha

mib-2 OBJECT IDENTIFIER

which is identical to the prefix

3.1. Deprecated Objects

In order to better prepare imple
MIB, a new term "deprecated" may
A deprecated object in the MIB i
one which will most likely be re
MIB (e.g., MIB-III).

MIB-II marks one object as being

atTable

Network Working Group **K. McCloghrie**
Request for Comments: 1213 **Hughes LAN Systems, Inc.**
Obsoletes: RFC 1158 **M. Rose**
Performance Systems International
Editors
March 1991

Management Information Base for Network Management of TCP/IP-based internets: MIB-II

Status of this Memo

This memo defines the second version of the Management Information

The objects defined in MIB-II have the OBJECT IDENTIFIER prefix:

mib-2 OBJECT IDENTIFIER ::= { mgmt 1 }

which is identical to the prefix used in MIB-I.

3.1. Deprecated Objects

In order to better prepare implementors for future changes in the MIB, a new term "deprecated" may be used when describing an object. A deprecated object in the MIB is one which must be supported, but one which will most likely be removed from the next version of the MIB (e.g., MIB-III).

MIB-II marks one object as being deprecated:

atTable

Example – RFC 1213 MIB-II cont'd


```
3.2.  Display Strings

      ...

3.3.  Physical Addresses

      ...

-----------------------------------------

3.4.  The System Group

   Four new objects are added to this gro

      sysContact
      sysName
      sysLocation
      sysServices

   These provide contact, administrative,
   information regarding the managed node.

-----------------------------------------

3.7.  The IP Group

   The access attribute of the variable i
   from read-only to read-write.

      ...

-----------------------------------------

Groups

      - System
      - Interfaces
      - Address Translation (deprecated)
      - IP
      - ICMP
      - TCP
      - UDP
      - EGP
      - Transmission
      - SNMP

-----------------------------------------
```

3.4. The System Group

Four new objects are added to this group:

- **sysContact**
- **sysName**
- **sysLocation**
- **sysServices**

These provide contact, administrative, location, and service information regarding the managed node.

3.7. The IP Group

The access attribute of the variable ipForwarding has been changed from read-only to read-write.

...

Groups

- **System**
- **Interfaces**
- **Address Translation (deprecated)**
- **IP**
- **ICMP**
- **TCP**
- **UDP**
- **EGP**
- **Transmission**
- **SNMP**

Example – RFC 1271 RMON MIB

Network Working Group
Request for Comments: 1271 Carnegie Me

Remote Network Monitoring Management Information

⋮

Table of Contents

⋮

4.3. Structure of MIB

The objects are arranged into the following gr

- statistics
- history
- alarm
- host
- hostTopN
- matrix
- filter
- packet capture
- event

⋮

4.3.1. The Statistics Group

The statistics group contains statistics measu
each monitored interface on this device. This
consists of the etherStatsTable but in the fut
for other media types including Token Ring and

Network Working Group **S. Waldbusser**
Request for Comments: 1271 **Carnegie Mellon University**
November 1991

Remote Network Monitoring Management Information Base

4.3. Structure of MIB

The objects are arranged into the following groups:

- **statistics**
- **history**
- **alarm**
- **host**
- **hostTopN**
- **matrix**
- **filter**
- **packet capture**
- **event**

⋮

What does
Each group do
In Ethernet ??

4.3.1. The Statistics Group

The statistics group contains statistics measured by the probe for each monitored interface on this device. This group currently consists of the etherStatsTable but in the future will contain tables for other media types including Token Ring and FDDI.

Example – RFC 1271 RMON MIB cont'd


```
   A problem can arise when multiple management stations attempt to set
   configuration information simultaneously using SNMP.  When this
   involves the addition of a new conceptual row in the same control
   table, the managers may collide, attempting to create the same entry.
   To guard against these collisions, each
   status object with special semantics th
   managers.  If an attempt is made with
   create such a status object and that
   is returned.  When more than one mana
   create the same conceptual row, only
   others will receive an error.

---------------------------------------

6.  Definitions

          RFC1271-MIB DEFINITIONS ::= BE

              IMPORTS
                  Counter
                  DisplayString
                  mib-2
                  OBJECT-TYPE


              rmon    OBJECT IDENTIFIER

             ...

              EntryStatus ::= INTEGER
                          { valid(1),
                            createRequest
                            underCreation
                            invalid(4)
                          }
             -- The status of a table en

---------------------------------------

             ...
```

6. Definitions

RFC1271-MIB DEFINITIONS ::= BEGIN

IMPORTS
Counter FROM RFC1155-SMI
DisplayString FROM RFC1158-MIB
mib-2 FROM RFC1213-MIB
OBJECT-TYPE FROM RFC-1212;
rmon OBJECT IDENTIFIER ::= { mib-2 16 }

...

EntryStatus ::= INTEGER
{ valid(1),
createRequest(2),
underCreation(3),
invalid(4)
}
-- The status of a table entry.

The Model: Management Protocol

- Carries network management information
- Communications method between NMS and Agents
- Allows management information to be inspected (read) or altered (written)
- Self-contained unit of information
- Message format changes with SNMP versions, but PDU (Protocol Data Unit) is (almost) unchanged

SNMP Based NetMgt: The SNMP Protocol

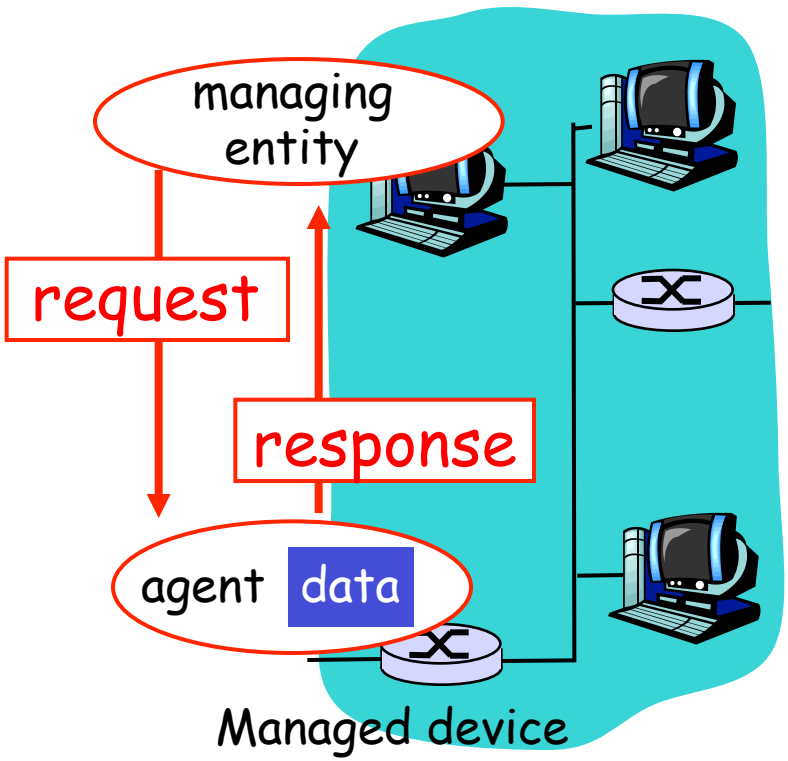
SNMP Protocol Exchange

Communication of management information among management entities is realized in SNMP through exchange of SNMP protocol messages.

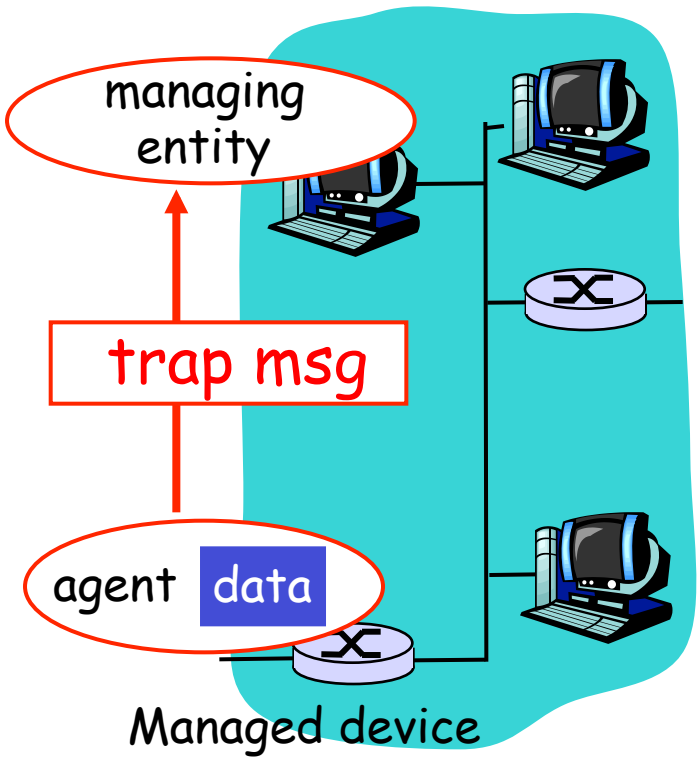
The exchange of SNMP messages requires only an unreliable datagram service, every message is entirely and independently represented by a single transport datagram, typically UDP – no TCP.

SNMP protocol

Two ways to convey MIB info, commands:



request/response mode

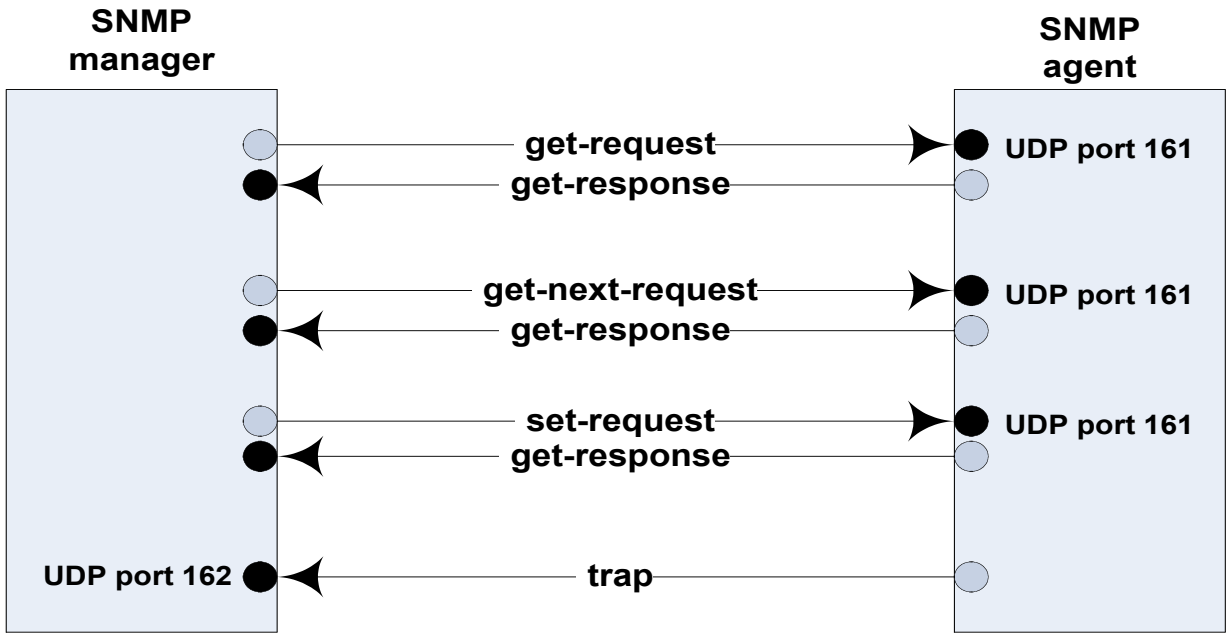


trap mode

Details: The Protocol

- SNMP – Simple Network Management Protocol
  - Does NOT define a list of commands
    - E.g., boot, clear, etc.
  - Rather classes all operations in a fetch-store paradigm:
    - E.g., set "boot" to 1 causes Agent to reboot
  - Simple, flexible, adaptable, etc.
- Hence, very simple set of operations available via The Protocol:
  - Get-request – fetch a value from a specific variable
  - Get-next-request – fetch next value after this one
  - Get-response – response to Get or Set
  - Set request – store a value in a specific variable
  - Trap – reply triggered by an event

Details: Summary of five SNMP Operations



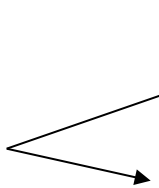
Notice the port numbers

Details: SNMP Message Format

- Version – 0
- Community – authority
- PDU Type
  - 0 – get-request
  - 1 – get-next
  - 2 – set-request
  - 3 – get –response
  - 4 – trap
- Request ID – NMS message management
- Error Status
  - 0 – no error
  - 1 – too big
  - 2 – no such name
  - 3 – bad value
- Error Index – which variable screwed up
- VARBIN's name/value pairs

Details: SNMP Message Format


```
SNMP-message::=
        Sequence{
                version INTEGER{
                        Version-1(0)
                        },
                community
                        OCTET STRING,
                Data
                        ANY
                }
```

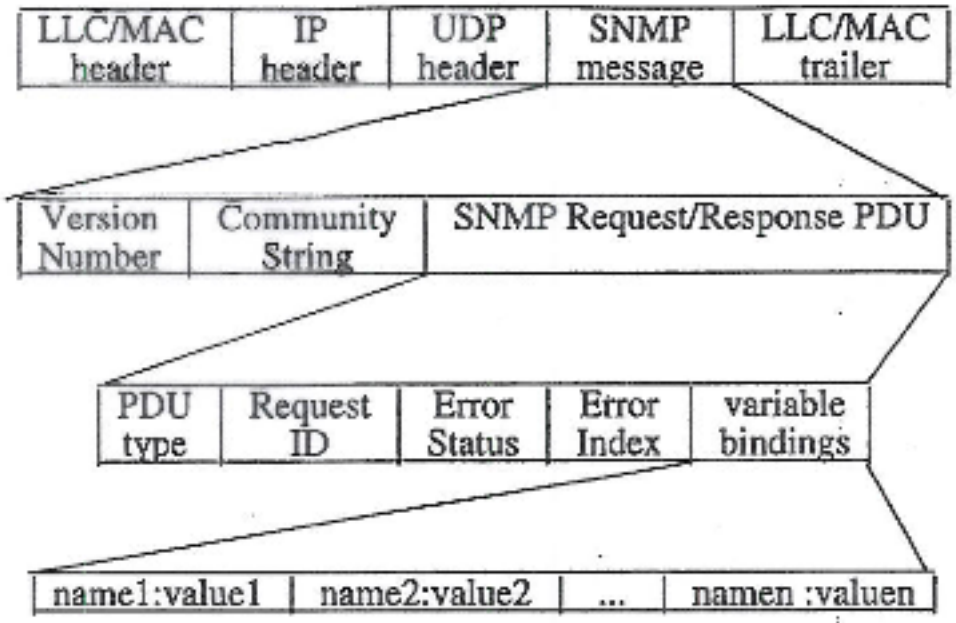


```
SNMP-PDUs::=
                get-request
                        GetRequest-PDU,
                get-next-request
                        GetNext Request-PUD,
                set-request
                        SetRequest-PDU,
                trap
                        Trap-PDU,
                }
```

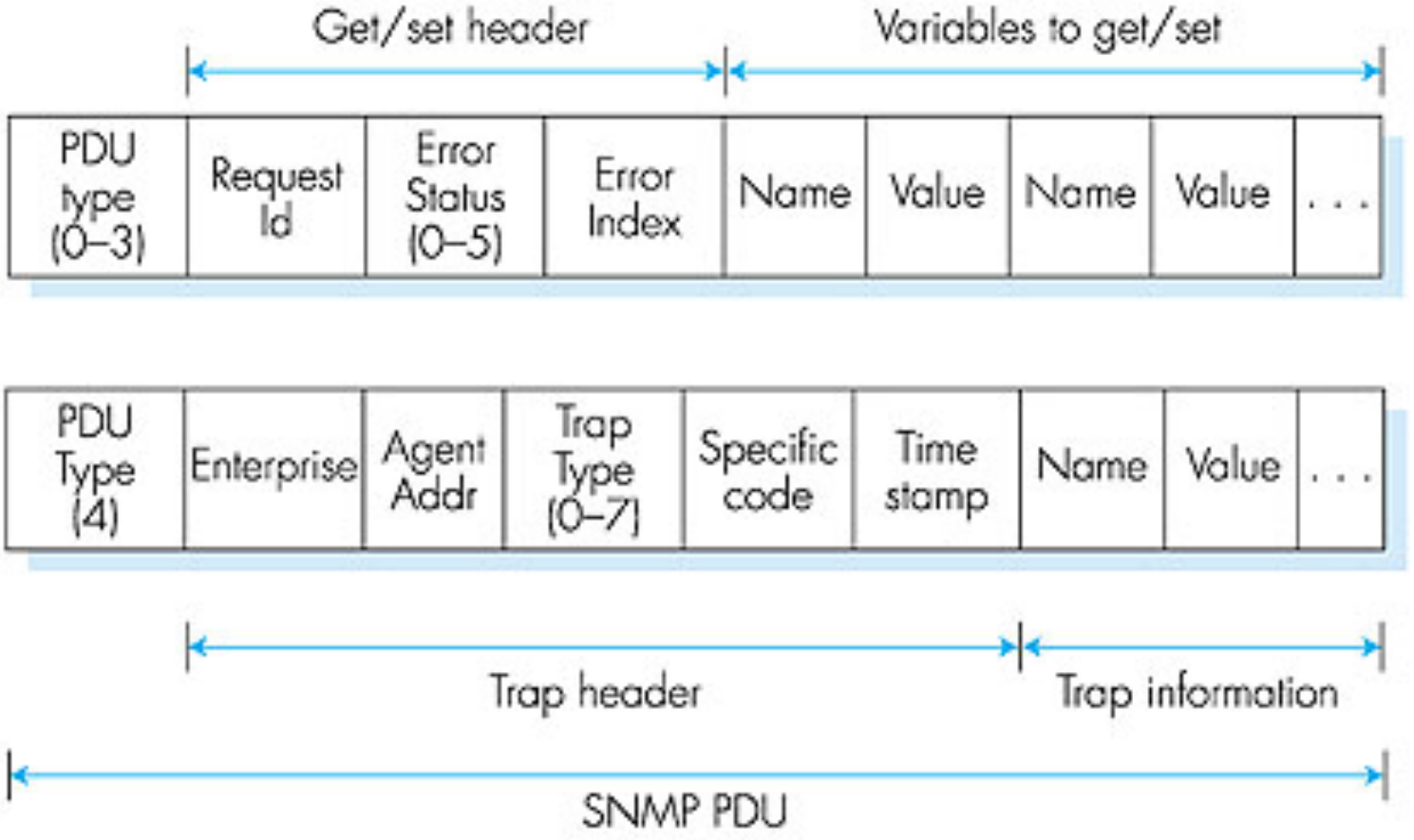
Details: SNMP Message Format


```
GetRequest-PDU::=[0]
        IMPLICIT SEQUENCE {
                request-id
                        RequestID,
                error-status
                        ErrorStatus,
                error-index
                        Error-Index,
                Variable-bindings
                        VarBindList – list of OIDS
                }

                OID A value

                SNMPtest OID, 0
```

SNMP Message Encoding



SNMP protocol: message formats



26.11 Example Encoded SNMP Message

The encoded form of ASN.1 uses variable-length fields to represent items. In general, each field begins with a header that specifies the type of object and its length in bytes. For example, Figure 26.10 shows the string of encoded octets in a *get-request* message for data item *sysDescr* (numeric object identifier *1.3.6.1.2.1.1.1*).

```
 30      29      02      01      00
SEQUENCE len=41 INTEGER len=1   vers=0

 04      06      70      75      62      6C      69      63
string   len=6    p       u       b       l       i       c

 A0      1C      02      04      05      AE      56      02
getreq.  len=28 INTEGER len=4   -------- request ID --------

 02      01      00      02      01      00
INTEGER  len=1   status INTEGER len=1 error index

 30      0E      30      0C      06      08
SEQUENCE len=14 SEQUENCE len=12 objectid len=8

 2B      06      01      02      01      01      01      00
1.3   .  6   .  1   .  2   .  1   .  1   .  1   .  0

 05      00
null     len=0
```

Figure 26.10 The encoded form of a *get-request* for data item *sysDescr* with octets shown in hexadecimal and their meanings below. Related octets have been grouped onto lines; they are contiguous in the message.

As Figure 26.10 shows, the message starts with a code for *SEQUENCE* which has a length of 41 octets. The first item in the sequence is a 1-octet integer that specifies the protocol *version*. The *community* field is stored in a character string, which in the example, is a 6-octet string that contains the word *public*.

SNMP security and administration

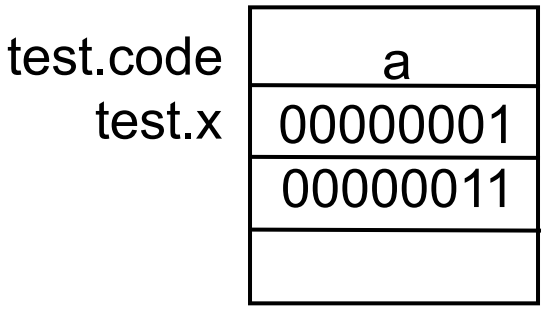
- encryption: DES-encrypt SNMP message
- authentication: compute, send MIC(m,k): compute hash (MIC) over message (m), secret shared key (k)
- protection against playback: use nonce
- view-based access control
  - SNMP entity maintains database of access rights, policies for various users
  - database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

ASN.1 - The presentation problem

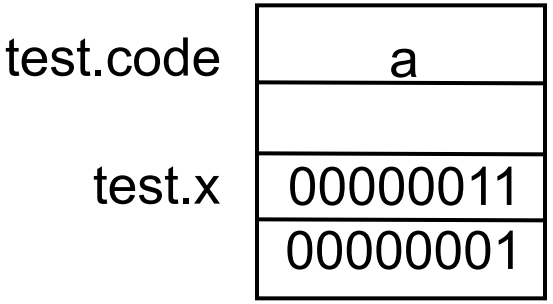
Q: does perfect memory-to-memory copy solve "the communication problem"?

A: not always!

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



host 1 format



host 2 format

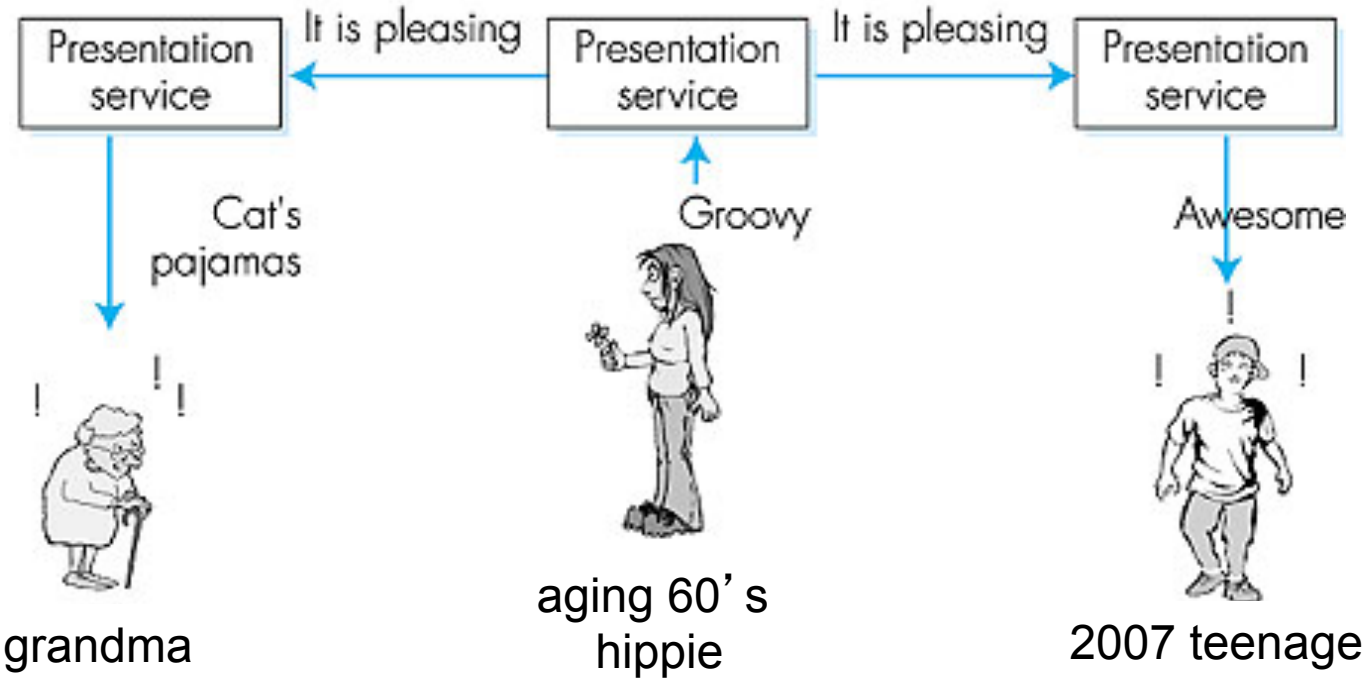
problem: different data format, storage conventions

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

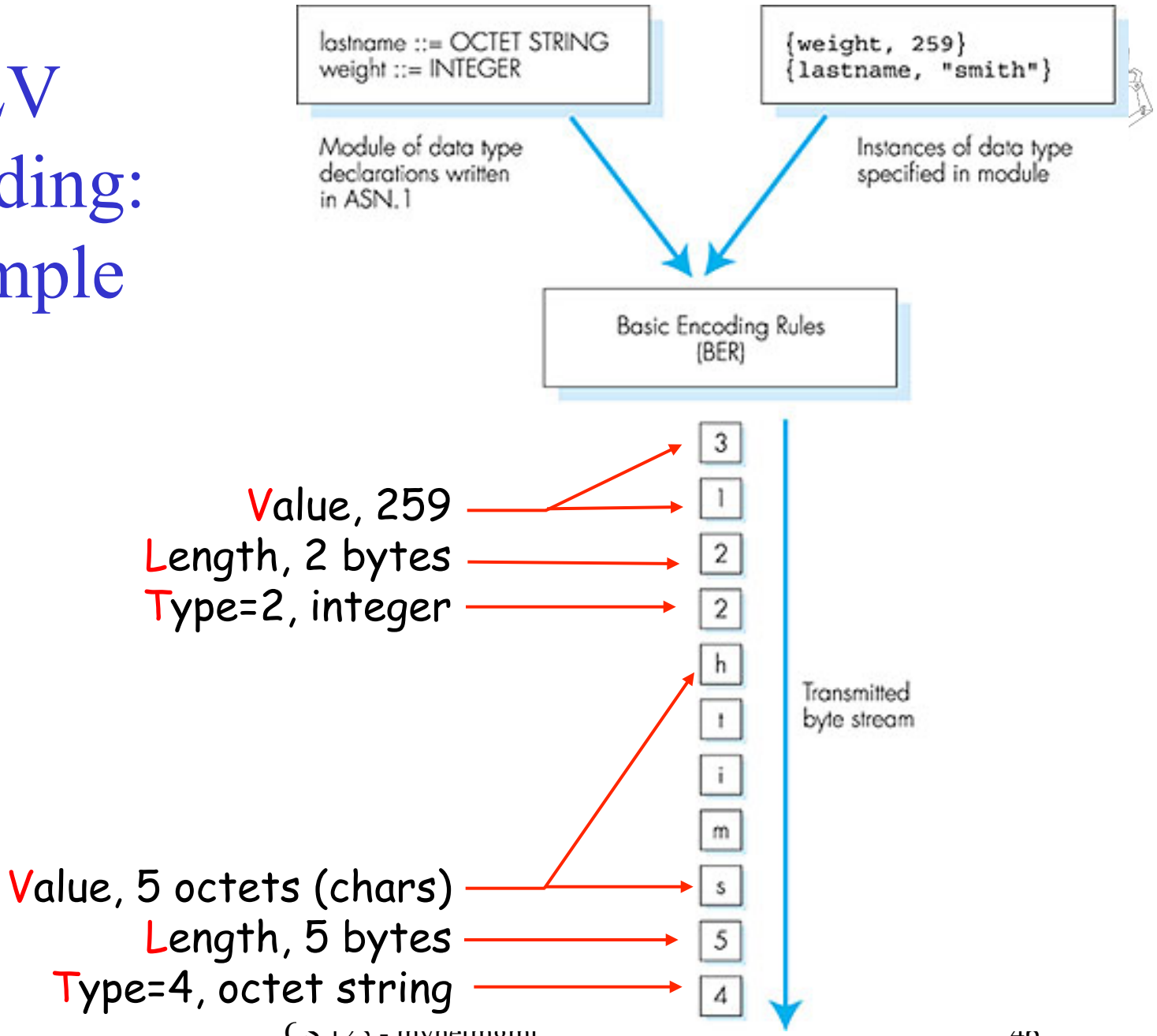
TLV Encoding

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: continued cost of network
  - 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?

Fundamental Axioms

Simple Stupid Devices

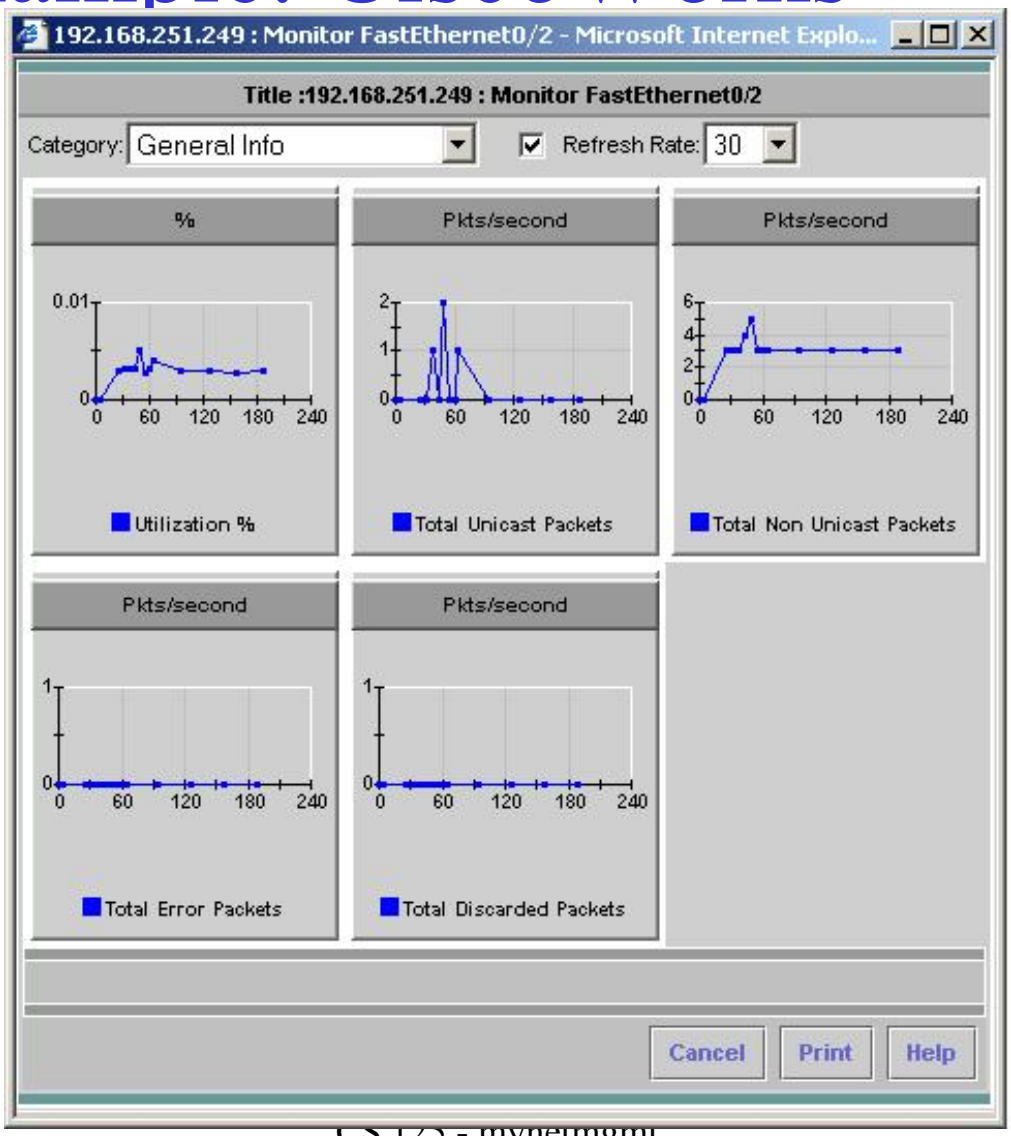
- *The impact of adding network management to managed nodes must be minimal, reflecting a lowest common denominator.*
- *If network management is viewed as an essential aspect of an internet, then it must be universally deployed on the largest possible collection of devices in the network.*

UDP

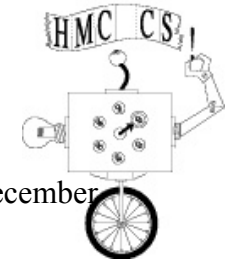
- *When all else fails, network management must continue to function, if at all possible.*

Example: CiscoWorks – Device View

Example: CiscoWorks -



References



RFC 3418 Management Information Base (MIB) for the Simple Network Management Protocol (SNMP), Presuhn R, December 2002.

RFC 3417 Transport Mappings for the Simple Network Management Protocol (SNMP), Presuhn R, December 2002.

RFC 3416 Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP), Presuhn R, December 2002.

RFC 3415 View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP), McCloghrie K, Presuhn R, Wijnen B, December 2002.

RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), Blumenthal U, Wijnen B, December 2002.

RFC 3413 Simple Network Management Protocol (SNMP) Applications, Levi D, Meyer P, Stewart B, December 2002.

RFC 3412 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP), Case J, Harrington D, Presuhn R, Wijnen B, December 2002.

RFC 3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks, Harrington D, Presuhn R, Wijnen B, December 2002.

RFC 3410 Introduction and Applicability Statements for Internet-Standard Management Framework, Case J, Mundy R, Partain D, Stewart B, December 2002.