PA160: Net-Centric Computing II.

Network Management

Luděk Matyska

Slides by: Tomáš Rebok

Faculty of Informatics Masaryk University

Spring 2016

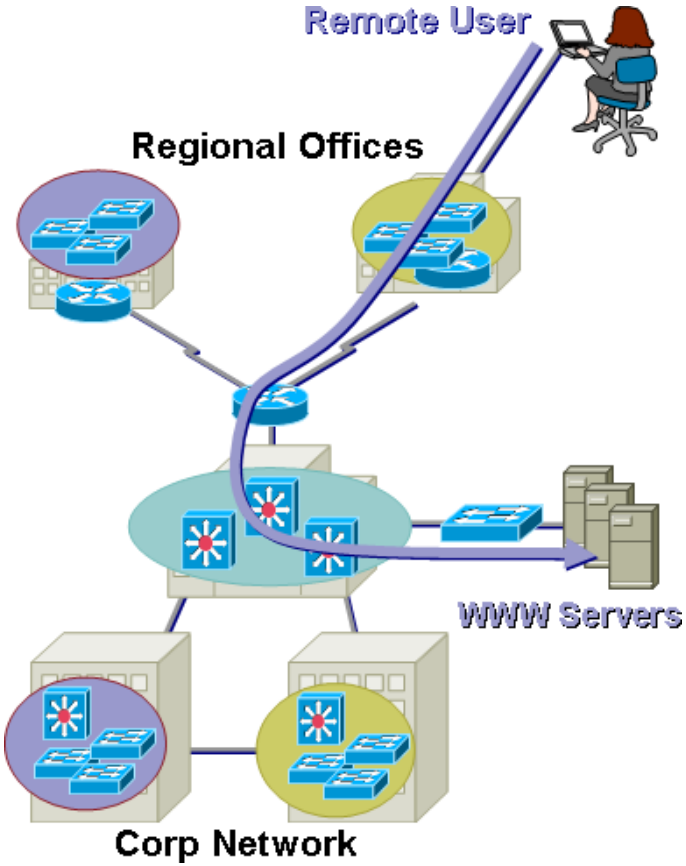
Lecture overview

1. Motivation
2. Network Management
   - Network Management by ISO
3. Basic Network Management Components
   - Network Elements
   - Management Systems
   - Management Network
   - Management Support Organization
   - Basic Components Refined
4. Simple Network Management Protocol (SNMP)
   - Structure of Management Information
   - Management Information Base (MIB)
   - Simple Network Management Protocol (SNMP)
5. Conclusion

Lecture overview

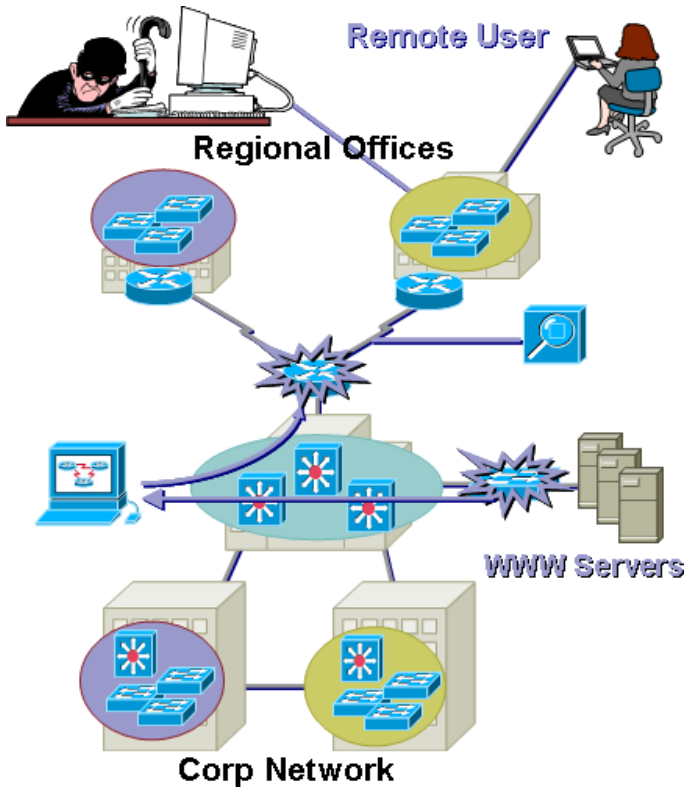
The Case for Management I.

- typical problem
  - remote user arrives at regional office and experiences slow or no response from corporate web server
- *Where should we begin?*
  - Where is the problem?
  - What is the problem?
  - What is the solution?
- without proper network management, these questions are difficult to answer



The Case for Management II.

- with proper management procedures and tools, one may "easily" get the answer
- consider some possibilities:
  - What configuration changes were made overnight?
  - Have you received a device fault notification indicating the issue?
  - Have you detected a security breach?
  - Has your performance baseline predicted this behavior on an increasingly congested network link?



The Case for Management III.

A bit of history

- during the old days, a network could be managed using human efforts only
  - in a small system, running few *"pings"* may help locating the problem
- **27. 10. 1980**: first real (ARPANET) network crash
  - described in RFC 789
  - including the steps performed for the recovery
- further experiences obtained on similar cases
  - e.g., a "worm" in 1988
- as the Internet becomes a large global infrastructure, *automated network management and monitoring tools are essential*
  - standardized tools that can be used across a broad spectrum of product types are also needed (heterogenous equipment)
  - $\Rightarrow$ *Network Management* $\Rightarrow$ *Network Management System (NMS)*

The Case for Management III.

What should be monitored?

What should be monitored?

- *basic network elements*
  - network interfaces – e.g., an increase in checksum errors in frames sent out by the interface
  - network components – servers, routers, end-hosts, etc.
  - physical links
- *traffic monitoring* – by link utilization monitoring, system bottlenecks may be determined (and solved)
- *routing information* – e.g., rapid changes in routing tables
- *a compliance with SLAs (Service Level Agreements)*
- *suspicious behavior* – security attacks, patterns indicating suspicious traffic, etc.
- etc.

Lecture overview

Network Management

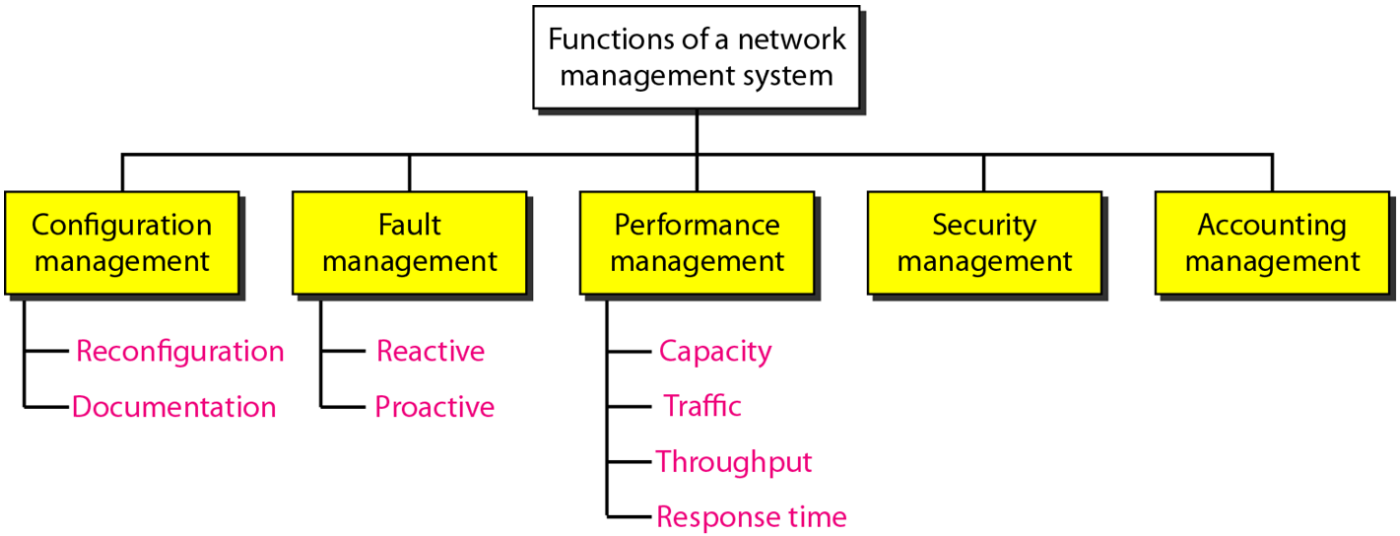
- the process of controlling a complex data network
  - controlling = monitoring, testing, configuring, and troubleshooting
- the overall goal is to help with the complexity of the network and to ensure that data can go across it with *maximum efficiency and transparency* to the users

Network Management

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 by ISO

- ISO (International Organization for Standardization) has created a network management model (often referred as *FCAPS model*):
  - *Fault management*
  - *Configuration management*
  - *Accounting management*
  - *Performance management*
  - *Security management*
- this classification has gained broad acceptance by vendors of both standardized and proprietary NMSs
  - the model does not define the actual implementation of a NMS



Network Management by ISO

Fault Management

- *a fault* = an abnormal condition that requires management attention (or action) to repair

Fault management:

- the facilities that enable the *detection, isolation, and correction* of abnormal operation of the network
  - deals with both HW & SW failures
  - includes logging the detected information
- two variants:
  - *Reactive Fault Management* – reacts to incurred errors; involves the following steps:
    - discovering the problem
    - isolating the problem
    - fixing the problem (if possible)
    - and *documenting the problem*
  - *Proactive Fault Management* – tries to prevent faults from occurring
- provides *alarms* – unsolicited messages indicating that some unexpected event has occurred in the network (link down, intrusion detected, etc.)

Network Management by ISO

Configuration management

Configuration management:

- includes functionality to perform operations that will deliver and modify configuration settings to equipment in the network
  - includes the initial configuration of a device to bring it up as well as ongoing configuration changes
  - includes both HW & SW configurations
  - includes (HW & SW) *documentation* as well
- *functions:*
  - configuring Managed Resources
  - auditing the network and discovery what's in it
  - synchronization management information in the network
  - backing up network configuration and restoring
  - managing software images running on network equipment
- steps:
  1. gather information about current network, maintain an up-to-date inventory of all network components
  2. (if necessary) use that data to modify the configuration of the network devices (= reconfiguration)

Network Management by ISO

Accounting Management

Accounting management:

- concerned with tracking network utilization information, such that individual users, departments, or business units can be appropriately billed or charged for accounting purposes
- but does not serve for charging purposes only – tracking network utilization information can be also used for:
  - detecting users that are abusing their access privileges and burdening the network at the expense of other users
  - detecting users making inefficient use of the network (network managers can assist in changing procedures to improve performance)
  - network managers to plan the network growth (easier when end user activity is known in sufficient detail)

Network Management by ISO

Performance Management

Performance management:

- involves measuring the performance of the network hardware, software, and media
  - e.g., overall throughput, percentage utilization, error rates, response time, etc.
  - measures both individual and complex components (e.g., an end-to-end path)
- tries to monitor and control the network to ensure that it is running as efficiently as possible
  - closely related to fault management (but considers long-term behavior)
- functional categories:
  - *Monitoring* – ability to monitor and track activities on the network
  - *Controlling* – ability to make adjustments to improve network performance
- performance statistics can help managers to:
  - plan, manage and maintain large networks
  - recognize potential bottlenecks in advance

Network Management by ISO

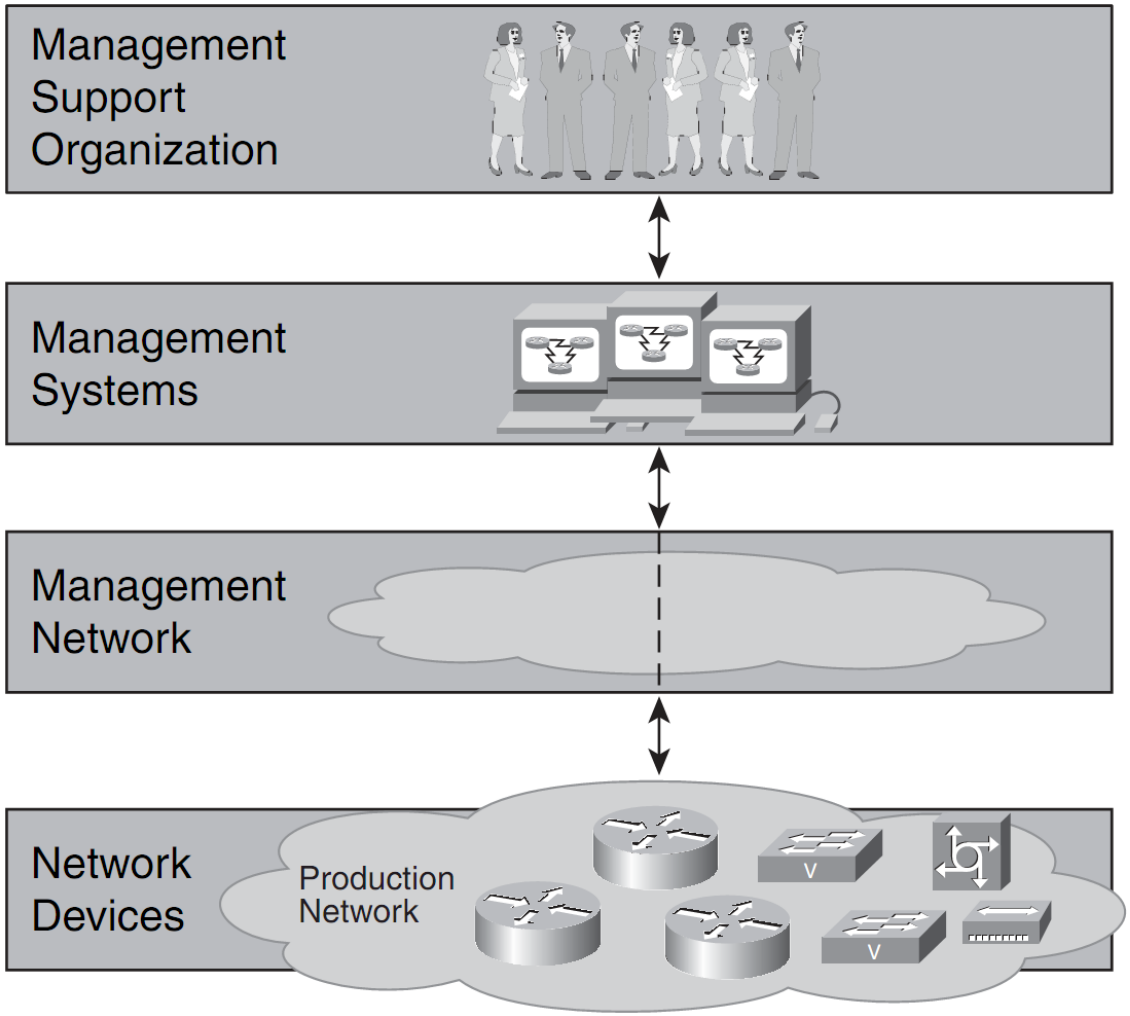
Security Management

Security management:

- responsible for controlling access to the network based on a predefined policy
- requires identifying the sensitive information (e.g., network management information), which should be protected
- provides audit trails and sounds alarms for security breaches
- not only concerned with ensuring that a network environment is secure, but also that gathered security-related information is analyzed regularly
- includes network authentication, authorization, and auditing
  - together with firewalls and IDSs

Lecture overview

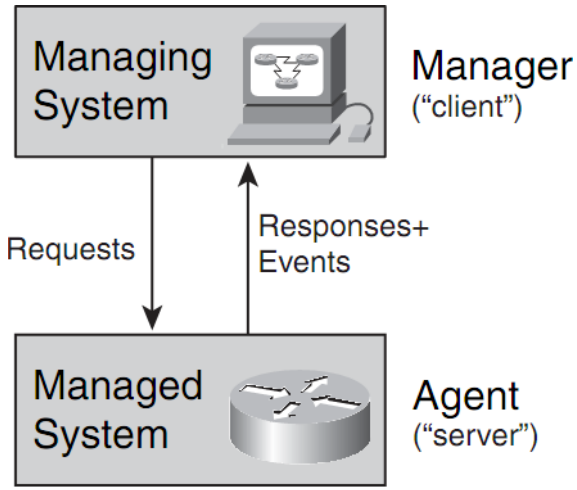
Basic Components of Network Management Systems



Network Elements (NEs) I.

Network Devices $\rightarrow$ **Network Elements (NEs)**

- to be managed, every NE must offer a management interface through which a managing system can communicate with it
  - receives requests and responses to them
  - sends *unsolicited information*, when an unexpected event has occurred (e.g., failure of a fan or a buffer overflow)
- a managing application = **manager**, the network element = **agent**



Network Elements (NEs) II.

Management Agents I.

NEs have to provide a piece of software that implements the management interface

- = **Management Agent**
  - *"agent"* becomes overloaded
    - agent = the role that a network element plays in network management
    - agent = software component that allows the network element to play that role (provides the management interface)
- management agent's functionality:
  - collects statistics (stores them locally)
  - responds to manager's commands, e.g.:
    - sends the collected statistics
    - provides/changes the node's parameters
    - provides status information
    - sends unsolicited messages for significant changes in local conditions
    - etc.

Network Elements (NEs) II.

Management Agents II.

- the *(Management) Agent* consists of three main parts:
  - **management interface** – handles management communication
    - supports a *management protocol* that defines the "rules of conversation"
  - **Management Information Base (MIB)** – a conceptual data store that contains a management view of the device being managed
    - a way to view the device itself, not a database in which information about the device is stored
    - constitutes the *management information* (provides an abstraction of real-world aspects (= *managed objects*) for management purposes)
  - **core agent logic** – translates between the operation of the management interface, the MIB, and the actual device
    - e.g., translates the request "retrieve a counter" (referred to in the MIB) into an internal operation that reads out a device hardware register containing the desired information

Network Elements (NEs) II.

Management Agents III.

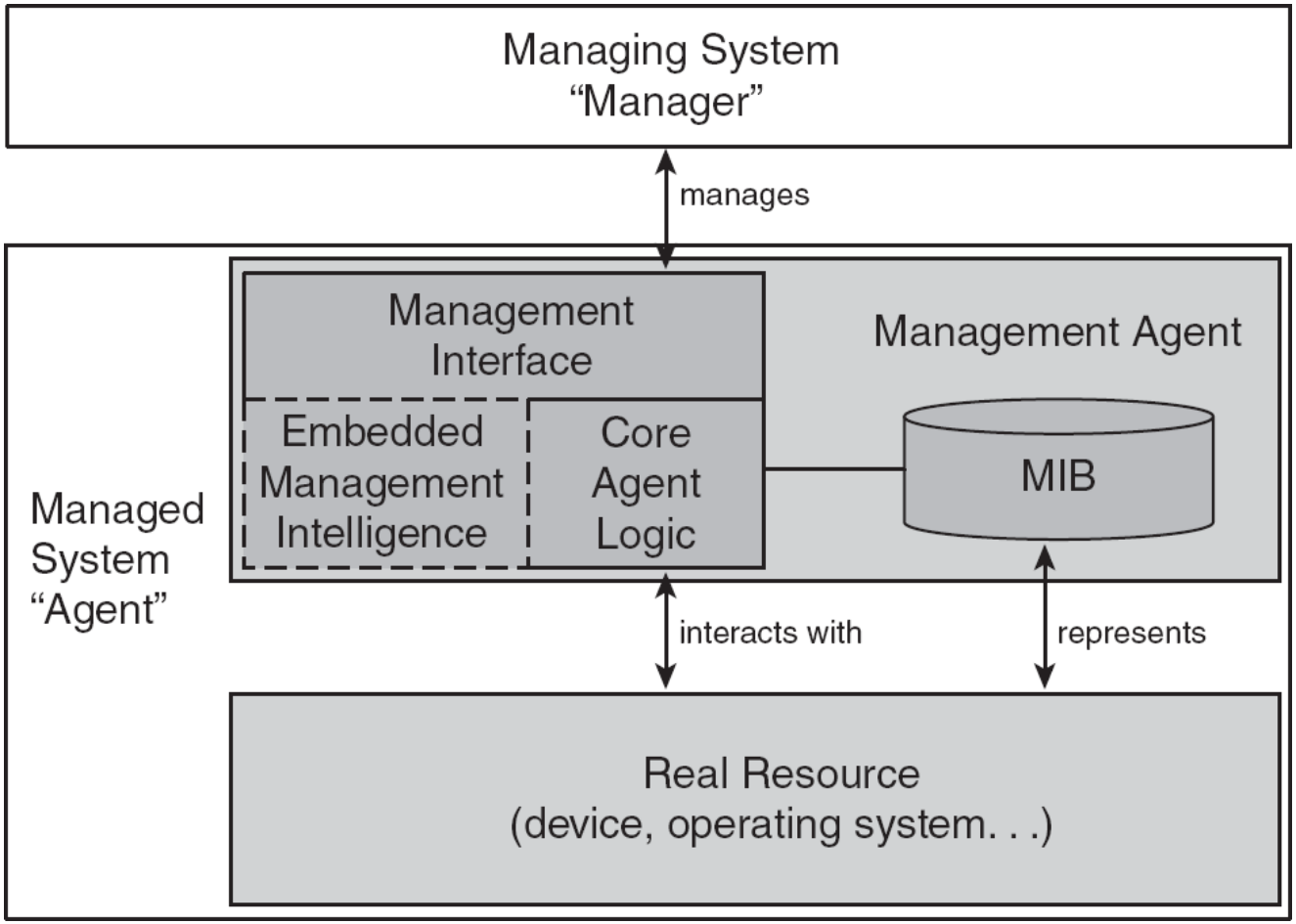


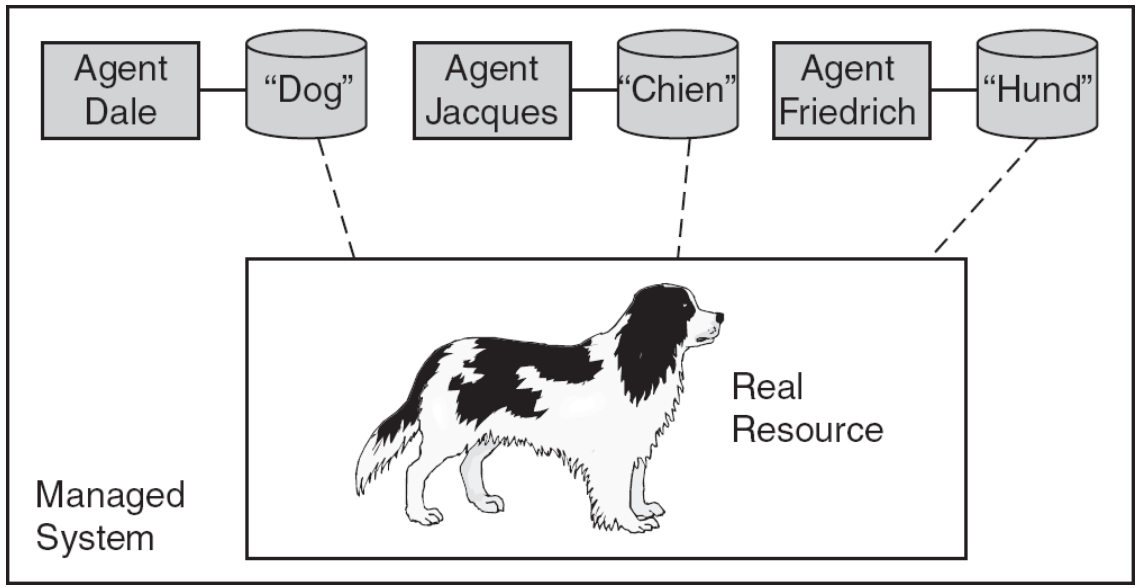
Figure : Anatomy of a Management Agent.

Network Elements (NEs) II.

Management Agents IV.

Management Agents cont'd.

- a single network element can contain several management agents managing the same objects
  - each of which with its own management interface
  - *reasons:* e.g., to give management applications a choice of management interfaces or different management agents might each serve different functions



(Network) Management System (NMS) I.

Network Management System (NMS)

- a collection of tools for network monitoring and control
  - designed to view the entire network as a unified architecture
  - providing an interface with a powerful but user-friendly set of commands
- the network active elements provide regular feedback of status information to the network control center(s)
  - one or more network control centers can be used
  - *centralized* vs. *hierarchical* vs. *distributed* layout

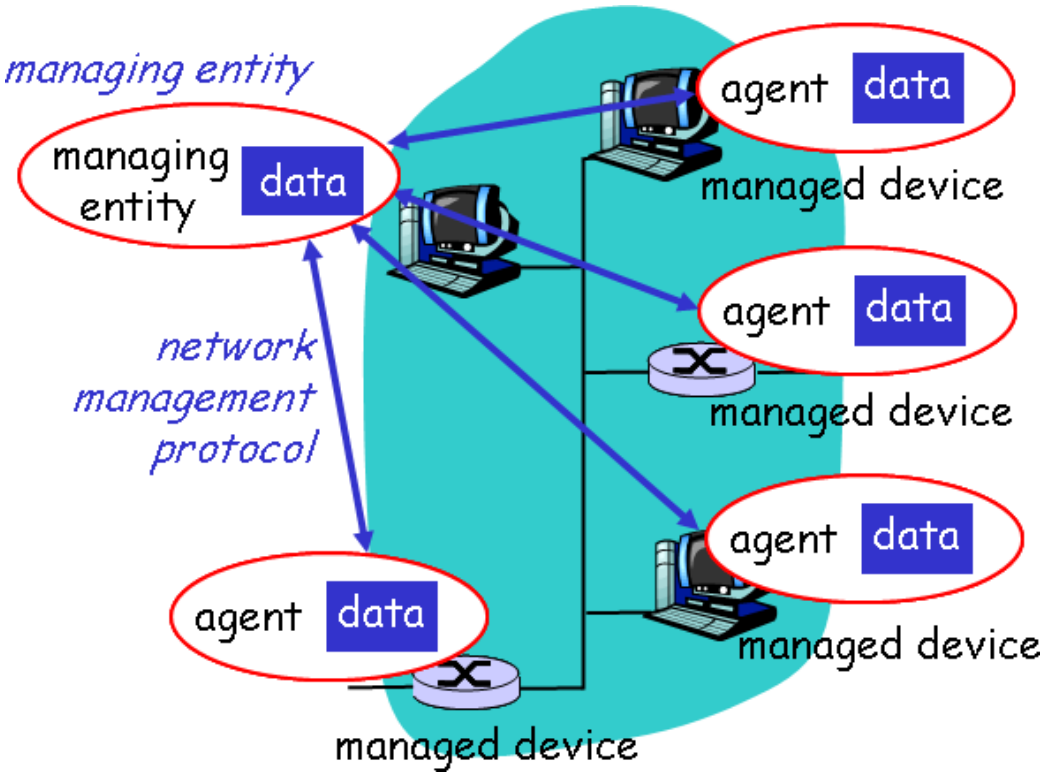
Paradoxical situation:

- to work properly, a NMS needs a network that works properly so that management applications and managed network can talk to each other
  - without this, it would be impossible to exchange management commands and management information
- of course, for the network to work properly, a proper NMS needs to be employed

(Network) Management System (NMS) II.

Centralized Layout

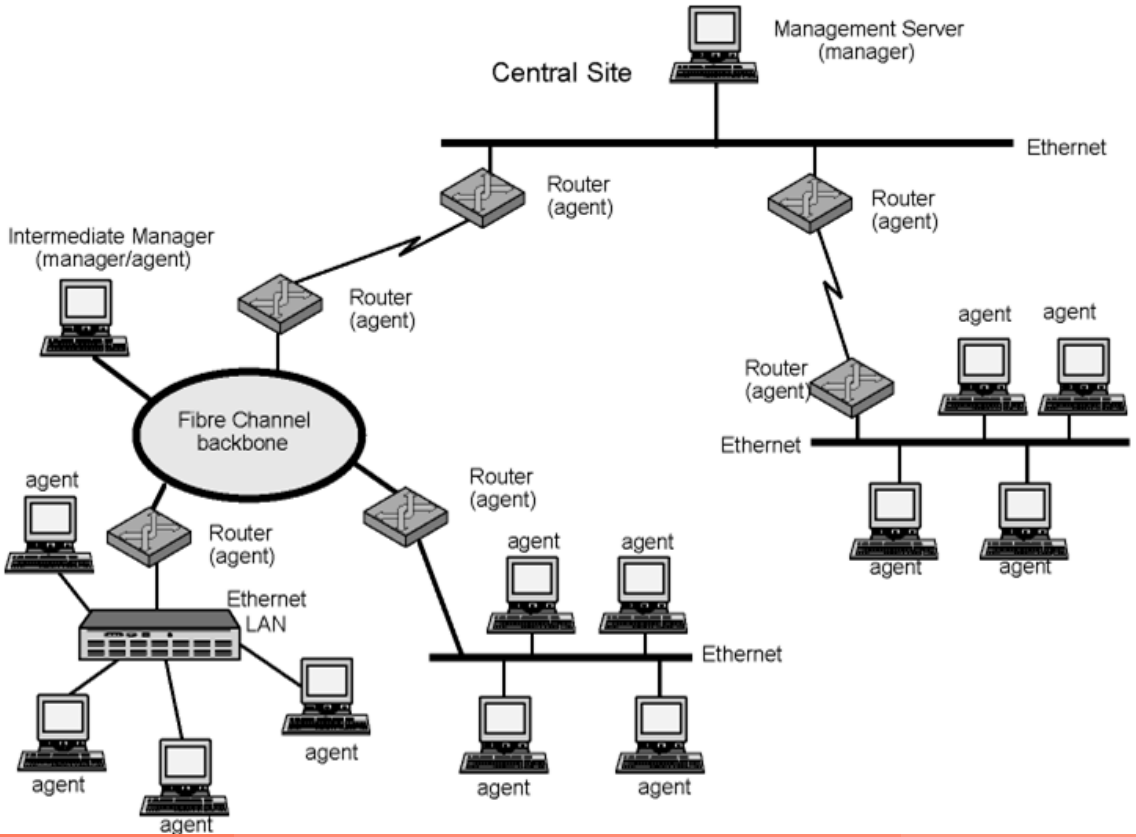
- the NMS resides on a single computer system
  - may be backed up by another system for High Availability purposes
- but may reside on multiple computer systems as well
  - e.g., to distribute the load – one center is idle or collecting statistics, while the other is used for control



(Network) Management System (NMS) II.

Hierarchical Layout I.

- the NMS resides on multiple management servers
  - one system acts as the central server
  - other systems working as clients = *intermediate managers (management proxies)*

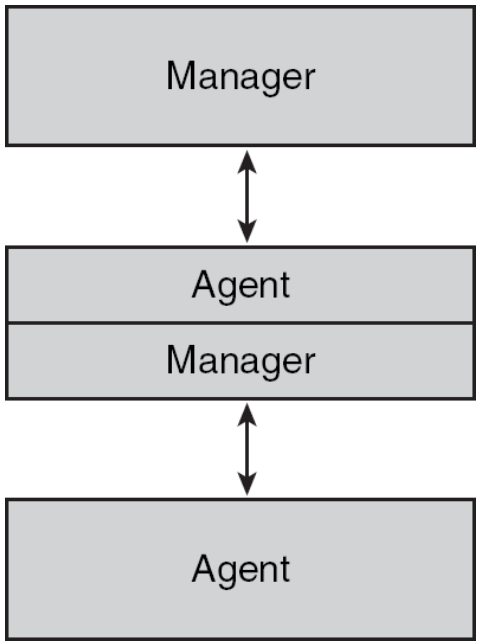


(Network) Management System (NMS) II.

Hierarchical Layout II. – Management Proxies

Management Proxies

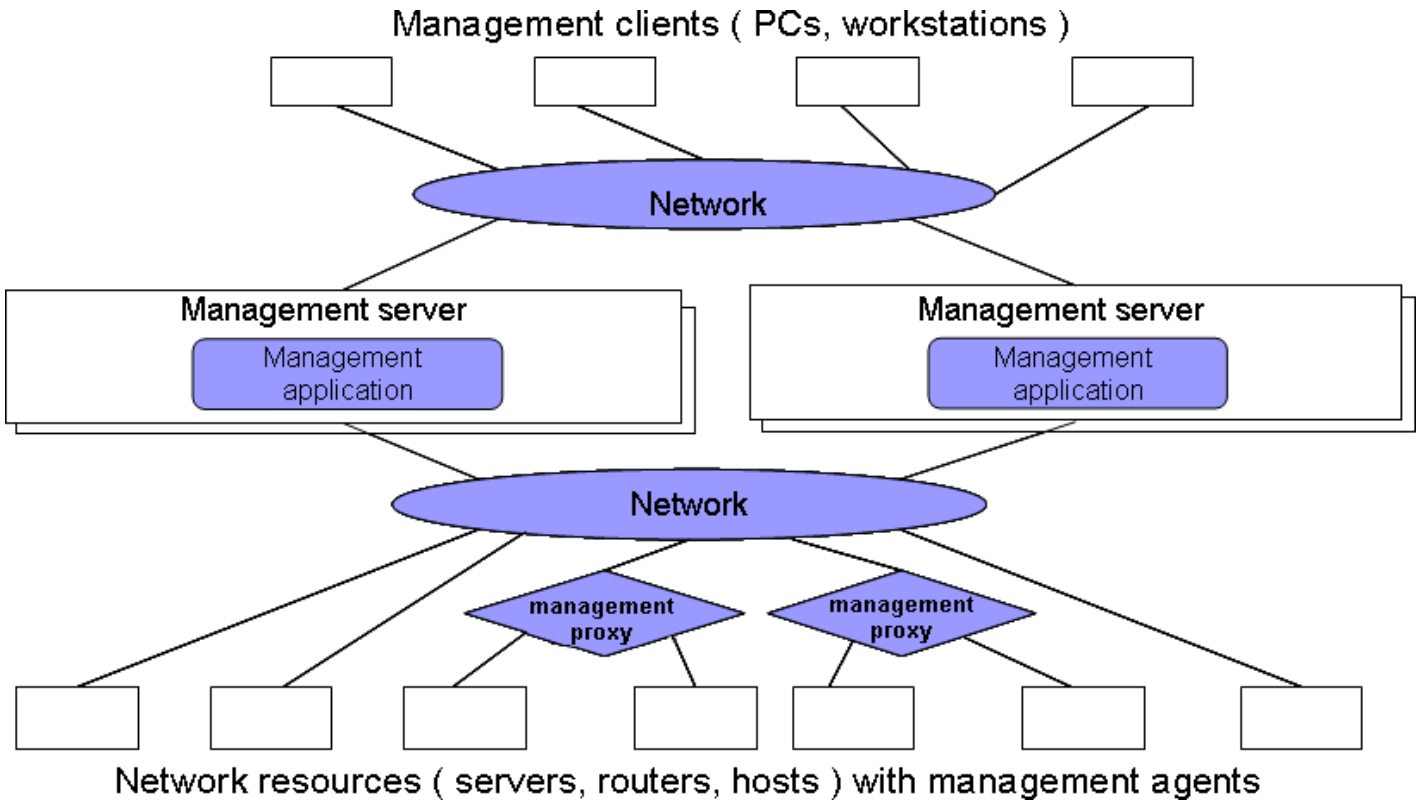
- the systems that play both agent and manager roles simultaneously
  - the system plays the agent role in interacting with the NMS, but it plays the manager role in interacting with the other network element(s)
  - multiple levels of hierarchy are possible



(Network) Management System (NMS) II.

Distributed Layout

- combines the centralized and hierarchical architectures
- the NMS uses multiple peer network management systems
  - each peer controls/monitors a part of the network

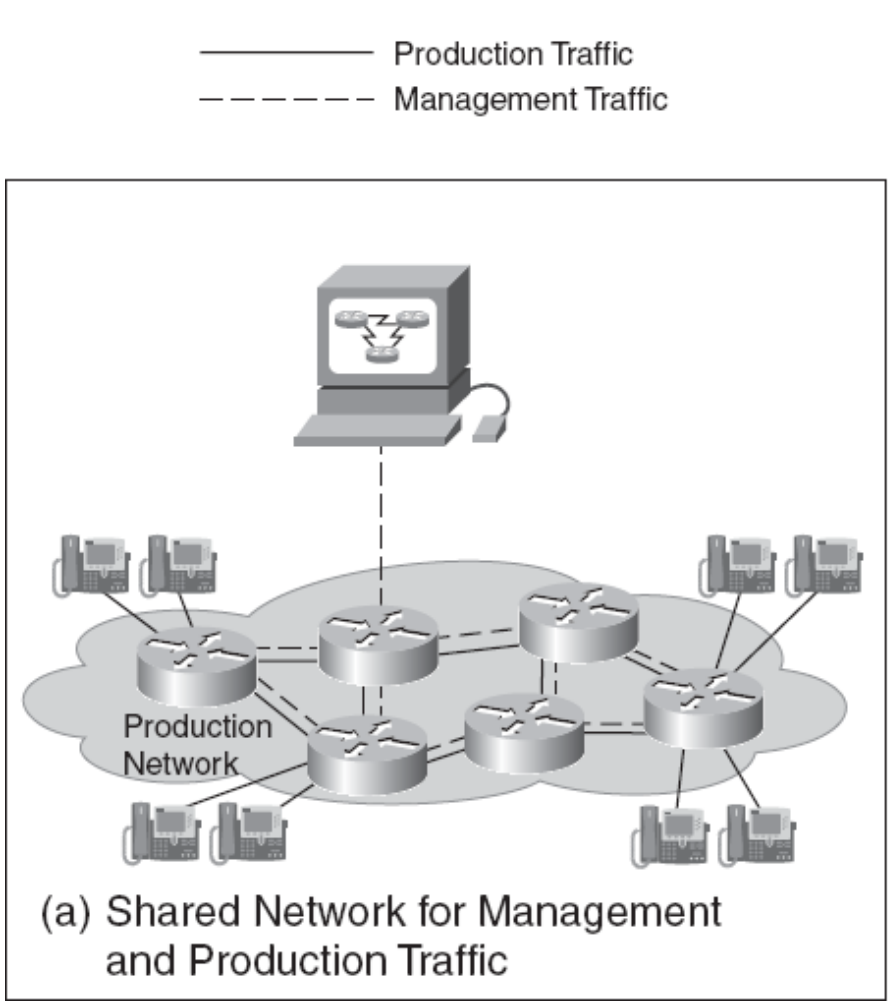


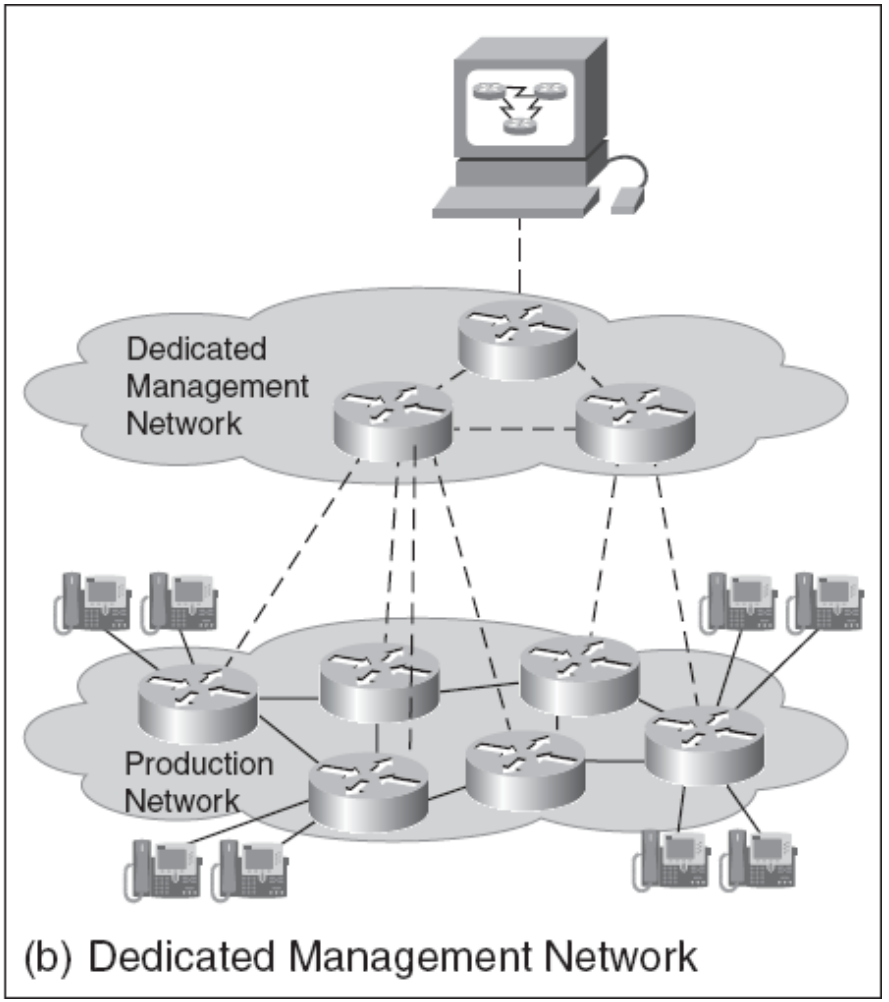
Management Network

- managing systems and managed systems need to be interconnected
  - $\Rightarrow$ **Management Network**
- a management network and a production network can:
  - be physically separate (dedicated) networks
    - serial interface (direct or through terminal servers)
    - network interface (Ethernet or any other dedicated network)
  - share the same physical network

Management Network

Dedicated vs. Shared management and production networks I.





Management Network

Dedicated vs. Shared management and production networks II.

Advantages of dedicated management network:

- *Reliability* – since the management traffic is carried independently of the production traffic, the management becomes significantly more reliable
  - e.g., network congestion/failure will not make a certain segment out of reach
- *Interference avoidance* – the management traffic does not compete with other networking (production) traffic
  - important when high QoS requirements have to be satisfied in the production network
    - although management traffic is not very high in volume, it may be bursty and still of non-negligible volume
    - (it might involve downloading large files with new configurations or software images to network elements, etc.)
  - interference between management and production network traffic can also make certain problems harder to diagnose
- *Security* – a dedicated mgmt network is harder to attack and easier to secure
  - $\Rightarrow$ less prone to hackers and less vulnerable to, e.g., DoS attacks on the production network
- *Ease of network planning* – (production) network planning becomes easier if there is no need to consider management traffic

Management Network

Dedicated vs. Shared management and production networks III.

Disadvantages of dedicated management network:

- *Cost and overhead* – a dedicated management network requires a separate network to be built
  - the dedicated network requires additional devices, additional space, and additional cabling
  - $\Rightarrow$ significant additional cost
- *No reasonable alternative* – sometimes, a shared network might realistically be the only option
  - e.g., the equipment deployed at the customer side might be reachable only through one network (DSL lines, etc.)

Question: *What about a management of the dedicated management network?*

- i.e., to have a "management management network"

Management Support Organization I.

Organizational (non-technical) aspects of network management, e.g.:

- **Establishment of process and operational policies, documentation of operational procedures**
  - helps to make the management consistent and efficient
    - especially in cases of emergencies
  - may include:
    - *well-defined workflows* to make sure that things that are supposed to happen do not fall through cracks
    - *well-defined escalation procedures* to ensure responsiveness
    - etc.
- **Collection of audit trails**
  - automatic logging the activities of management support staff
    - who initiated what action, and at what time
  - makes it easier to reproduce what happened and how to recover from situations in which human error or omission led to operational failures

Management Support Organization II.

Organizational (non-technical) aspects of network management cont'd.:

- **Network documentation**
  - the network itself should be documented (and *up-to-date*!)
  - important for network planning
    - e.g., planning the SW updates
    - also enables to identify discrepancies between what is supposed to be in the network and what actually has been deployed
- **Reliable backup and restore procedures**
  - allows to bring the network back up in case of disasters or emergencies
    - e.g., restoring the last configuration that was known to work properly
- **Security emphasis**
  - the most significant threats to the network might be lead from disgruntled employees on the inside
    - employees have physical access to the network equipment
- etc.

Basic Components of Network Management Refined

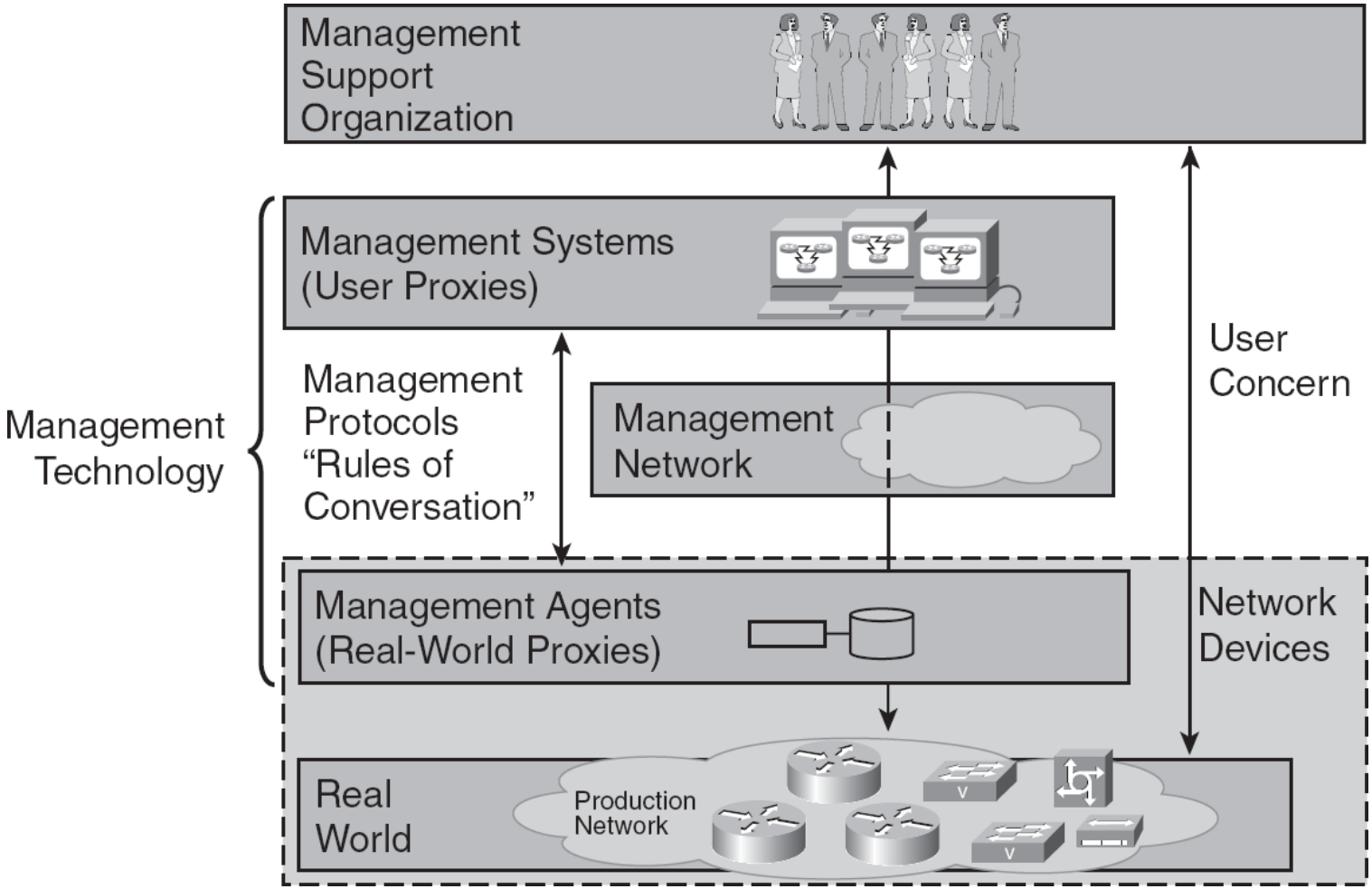


Figure : Basic Parts of the Network Management – Refined.

Lecture overview

Network Management Protocol

Two competing standards:

- *OSI CMISE/CMIP (Common Management Service Element/Common Management Information Protocol)*
  - *de jure* standards derived from the OSI framework
  - implementation issues have limited its use
- *SNMP (Simple Network Management Protocol)*
  - *de facto* standards based on TCP/IP

- both standards define, how multiple devices in a network can exchange messages for the purpose of network management
  - including what information can be passed between the devices for this purpose
- at the present time, the SNMP is winning the battle

Simple Network Management Protocol (SNMP) I.

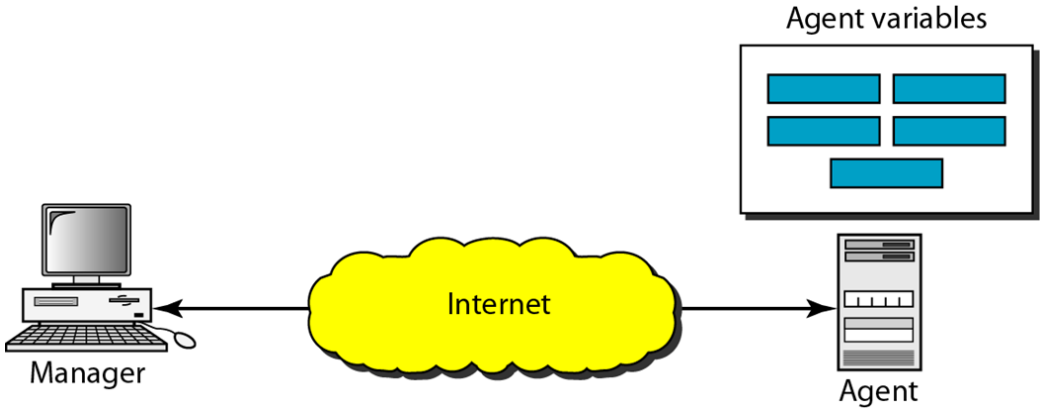
Simple Network Management Protocol (SNMP)

- a tool (protocol) that allows for remote and local management of items on the network including servers, workstations, routers, switches, and other managed devices
  - application-level "protocol"
    - more than a protocol → it's a framework consisting of a number of architectural components that define how management information is structured, stored, and how it is exchanged using the SNMP protocol itself
- SNMP history:
  - SNMP derived from its predecessor *SGMP (Simple Gateway Monitoring Protocol)* (RFC 1028)
  - SNMPv1 (1988) – poor security (authentication only by a "community string", transmitted in cleartext)
  - SNMPv2 (1993) – improvements in the areas of performance, security, confidentiality, and manager-to-manager communications
    - several variants – SNMPv2c (community-based security), SNMPv2u (user-based security), and SNMPv2 (party-based security)
  - currently – SNMPv3 (1999)
    - makes no changes to the protocol aside from the addition of cryptographic security – encryption, message integrity, and authentication

Simple Network Management Protocol (SNMP) II.

Simple Network Management Protocol (SNMP) cont'd.

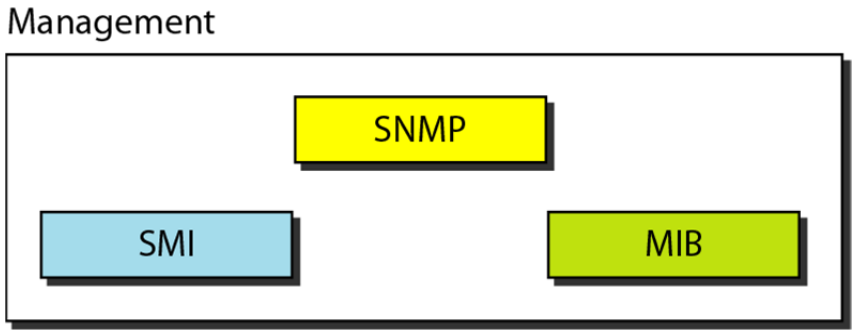
- uses the *Manager* - *Agent* approach
  - proxy managers are also supported (from SNMPv2)



- *main SNMP advantages:*
  - standardized
  - universally supported
  - extendible
  - portable
  - allows distributed management access
  - lightweight
    - both simple framework architecture & simple agent implementations on NEs

Simple Network Management Protocol (SNMP)

Components



- *role of SNMP:*
  - defines the format of messages (packets) exchanged by management systems and agents
- *role of SMI (Structure of Management Information):*
  - rules specifying the format used to define objects managed on the network that the SNMP protocol accesses
    - defines general rules for naming objects, defining object types (including range and length), and showing how to encode objects and values
- *role of MIBs (Management Information Bases):*
  - collections of named objects, their types, and their relationships to each other in an entity to be managed

Simple Network Management Protocol (SNMP)

Components – A Computer Program Analogy

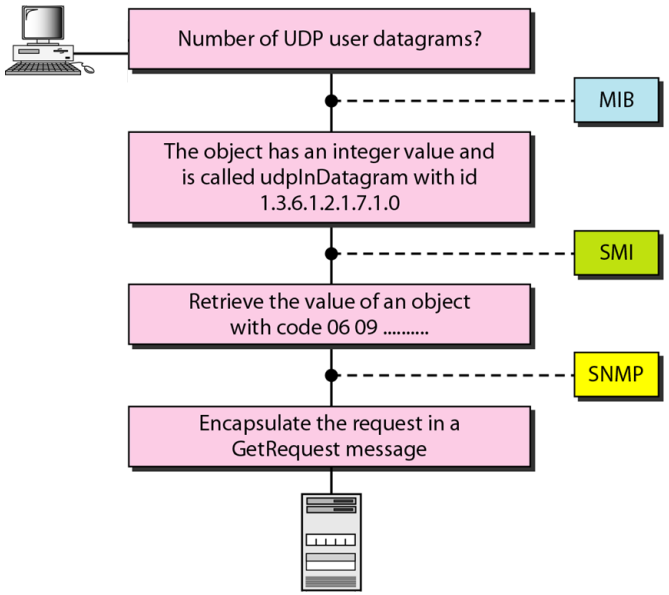
The task of network management may be compared to the task of writing a computer program:

- before one writes a program, **the syntax** of the language (such as C or Java) must be predefined
  - including the structure of variables (simple, structured, pointer, etc.) and how the variables must be named
  - *in network management, these rules are defined by SMI*
- most computer languages require **variables to be declared** in a program
  - the declaration names each variable and defines the predefined type
  - *in network management, this is defined by MIB*
    - MIB names each object and defines the type of the objects
    - the type is a type defined by SMI
- once variables are declared, the program needs to write **statements to store values** in the variables and change them if needed
  - *in network management, this task is done by SNMP*
    - it stores, changes, and interprets the values of objects already declared by MIB according to the rules defined by SMI

Simple Network Management Protocol (SNMP)

Overview

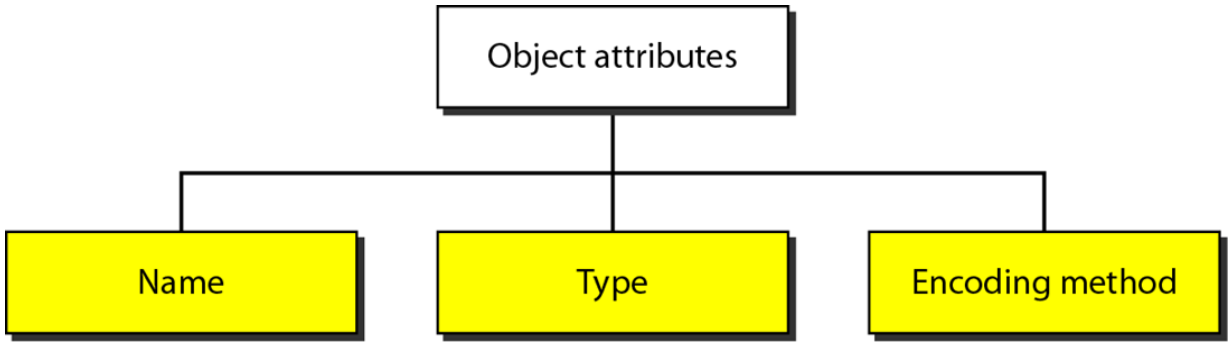
- when a manager wants to send a message to an agent station to find the number of UDP user datagrams received:
  - **MIB** is responsible for finding the object that holds the number of the UDP user datagrams received
  - **SMI**, with the help of another embedded protocol, is responsible for encoding the name of the object
  - **SNMP** is responsible for creating a message, called *GetRequest*, and encapsulating the encoded message



Structure of Management Information (SMI)

Structure of Management Information (SMI)

- currently version 2 (SMIv2)
- functions:
  - to name objects
  - to define the type of data that can be stored in an object
  - to show how to encode data for transmissions over the network

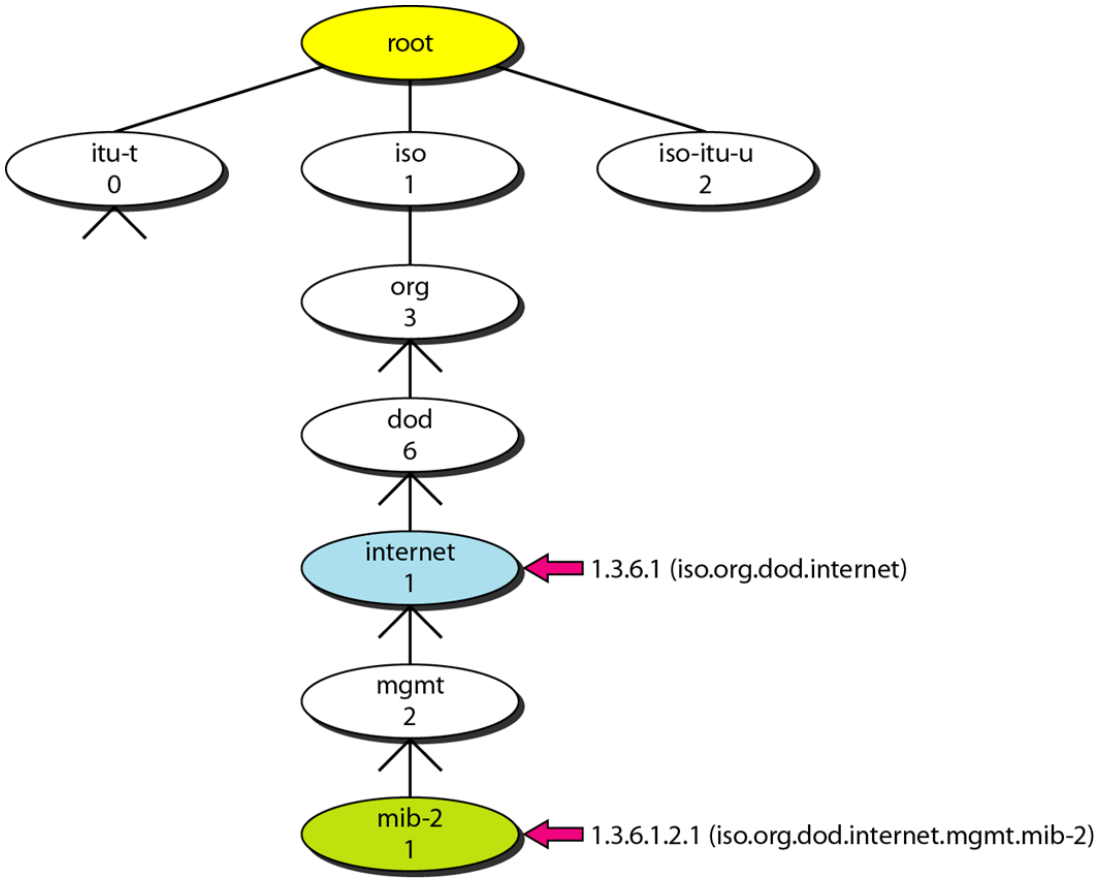


Structure of Management Information (SMIv2)

Naming objects I.

Object Name

- to name objects globally, SMI uses an object identifier, which is a *hierarchical identifier based on a tree structure*



Structure of Management Information (SMIv2)

Naming objects II.

- = **OIDs (Object IDentifiers)**
- each object can be defined using a sequence of integers separated by dots
  - e.g., *1.3.6.1.2.1*
  - this representation is used by SNMP
- or using a sequence of textual names separated by dots
  - e.g., *iso.org.dod.internet.mgmt.mib-2*
  - this representation is used by people

Structure of Management Information (SMIv2)

Object type

Object Type

- the type of data stored in the object
- to define the data type, SMI makes use of *Abstract Syntax Notation 1 (ASN.1)* definitions
  - and adds some new definitions
  - **ASN.1** – a standard and flexible notation that describes data structures for representing, encoding, transmitting, and decoding data
- two categories of object types: *simple* and *structured*
  - structured data types created by: *sequence* and *sequence of* operators
    - *sequence* – a list of (arbitrary) data fields ($\approx$ a record/structure in computer programming)
    - *sequence of* – an array of data fields or records (sequences)
  - by a combination of simple and structured data types, new structured data types can be created

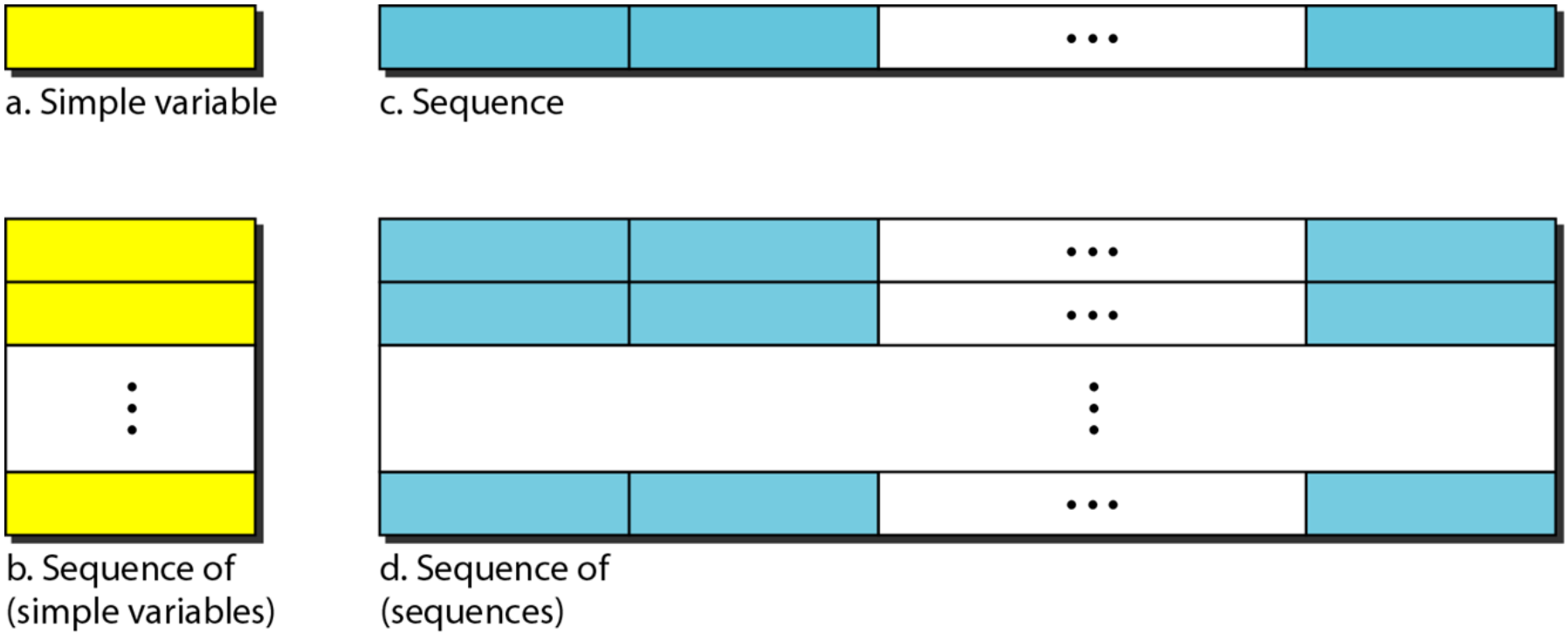
Structure of Management Information (SMIv2)

Object type – Simple data types

Type	*Size*	*Description*
INTEGER	4 bytes	An integer with a value between -2^{31} and $2^{31} - 1$
Integer32	4 bytes	Same as INTEGER
Unsigned32	4 bytes	Unsigned with a value between 0 and $2^{32} - 1$
OCTET STRING	Variable	Byte string up to 65,535 bytes long
OBJECT IDENTIFIER	Variable	An object identifier
IPAddress	4 bytes	An IP address made of four integers
Counter32	4 bytes	An integer whose value can be incremented from 0 to 2^{32}; when it reaches its maximum value, it wraps back to 0.
Counter64	8 bytes	64-bit counter
Gauge32	4 bytes	Same as Counter32, but when it reaches its maximum value, it does not wrap; it remains there until it is reset
TimeTicks	4 bytes	A counting value that records time in $\frac{1}{100}$ s
BITS		A string of bits
Opaque	Variable	Uninterpreted string

Structure of Management Information (SMIv2)

Object type – Structured data types

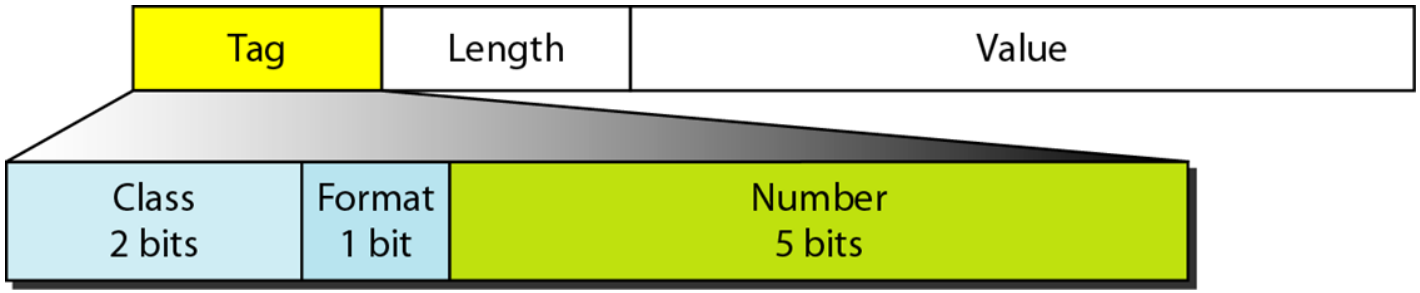


Structure of Management Information (SMIv2)

Encoding method

Encoding method

- the *Basic Encoding Rules (BER)* standard is used to encode data to be transmitted over the network
  - in order to be understood by both communicating parties uniformly
- BER specifies that each piece of data can be encoded in triplet format: *tag*, *length*, and *value*



Structure of Management Information (SMIv2)

Encoding method – Tag I.

Encoding method – Tag

- 1-byte field that defines the type of data
- composed of three subfields:
  - *class* – universal (00), applicationwide (01), context-specific (10), or private (11)
    - universal – data types taken from ASN.1
    - applicationwide – data types added by SMI
    - context-specific – data types having the meanings that may change from one protocol to another
    - private – data types that are vendor-specific
  - *format* – simple (0) or structured (1)
  - *number* – further divides simple or structured data into subgroups

Structure of Management Information (SMIv2)

Encoding method – Tag II.

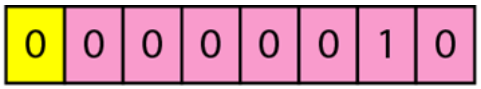
Data Type	*Class*	*Format*	*Number*	*Tag (Binary)*	*Tag (Hex)*
INTEGER	00	0	00010	**00000010**	**02**
OCTET STRING	00	0	00100	**00000100**	**04**
OBJECT IDENTIFIER	00	0	00110	**00000110**	**06**
NULL	00	0	00101	**00000101**	**05**
Sequence, sequence of	00	1	10000	**00110000**	**30**
IPAddress	01	0	00000	**01000000**	**40**
Counter	01	0	00001	**01000001**	**41**
Gauge	01	0	00010	**01000010**	**42**
TimeTicks	01	0	00011	**01000011**	**43**
Opaque	01	0	00100	**01000100**	**44**

Structure of Management Information (SMIv2)

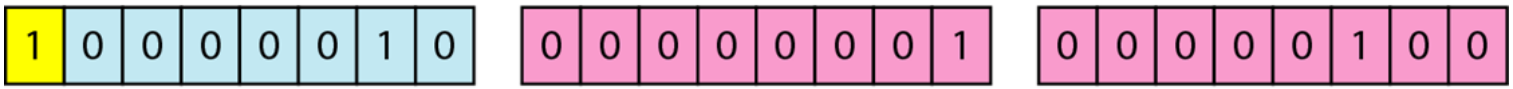
Encoding method – Length

Encoding method – Length

- 1 or more bytes field
  - 1-byte ⇒ the most significant bit must be 0
    - the other 7 bits define the length of the data
  - more-bytes ⇒ the most significant bit of the first byte must be 1
    - the other 7 bits of the first byte define the number of bytes needed to define the length



a. The colored part defines the length (2).

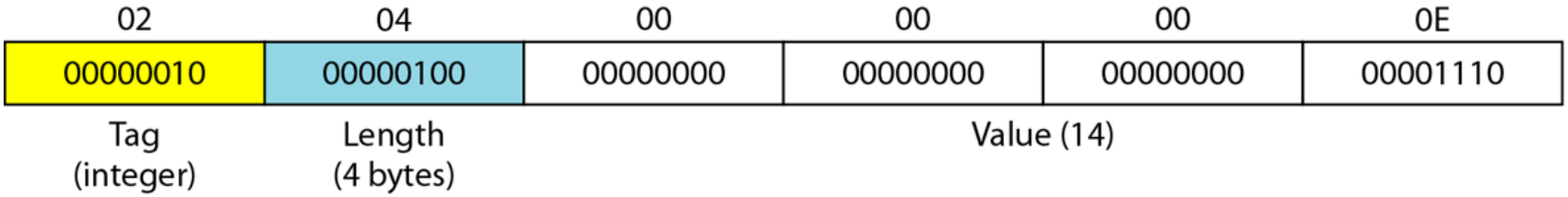


b. The shaded part defines the length of the length (2 bytes);
the colored bytes define the length (260 bytes).

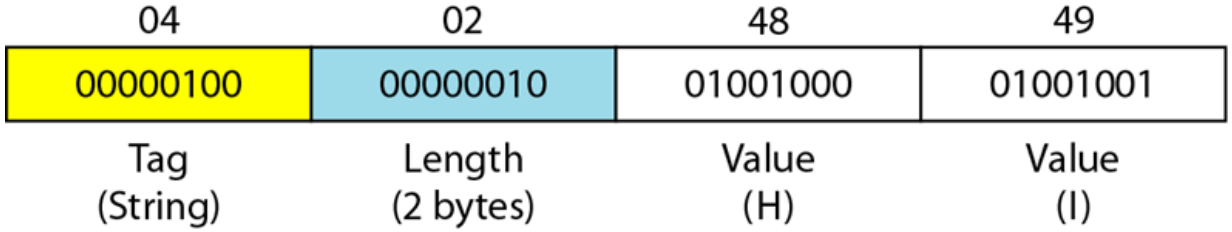
Structure of Management Information (SMIv2)

Encoding method – Examples I.

- INTEGER with a value 14



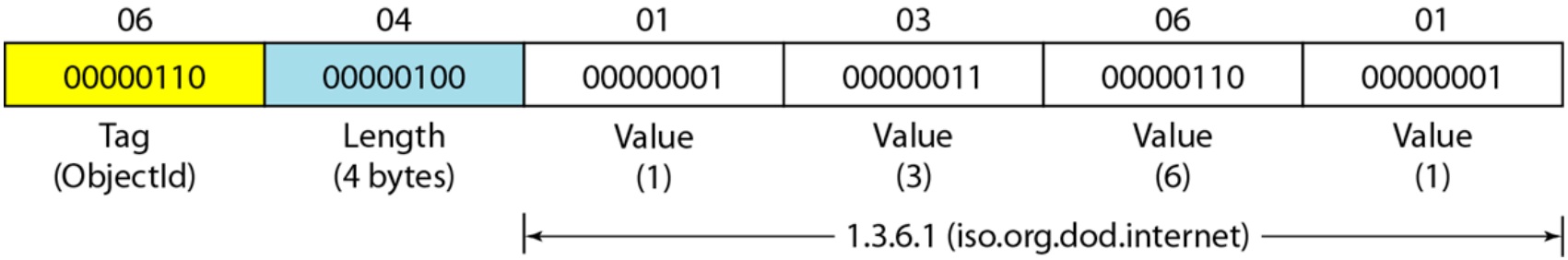
- OCTET STRING with a value "HI"



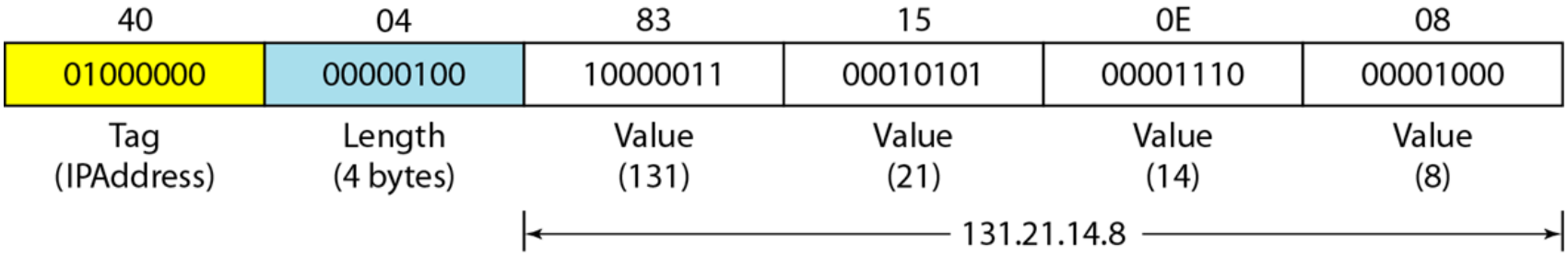
Structure of Management Information (SMIv2)

Encoding method – Examples II.

- ObjectIdentifier with a value *1.3.6.1*



- IPAddress with a value *131.21.14.8*



Structure of Management Information (SMIv2)

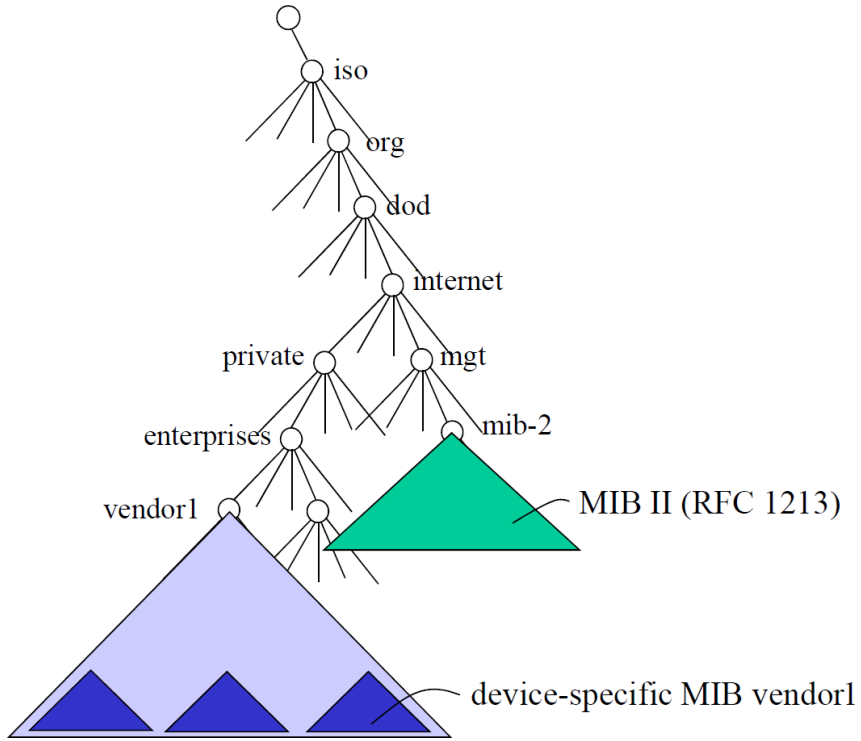
Object example:

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

Management Information Base (MIB)

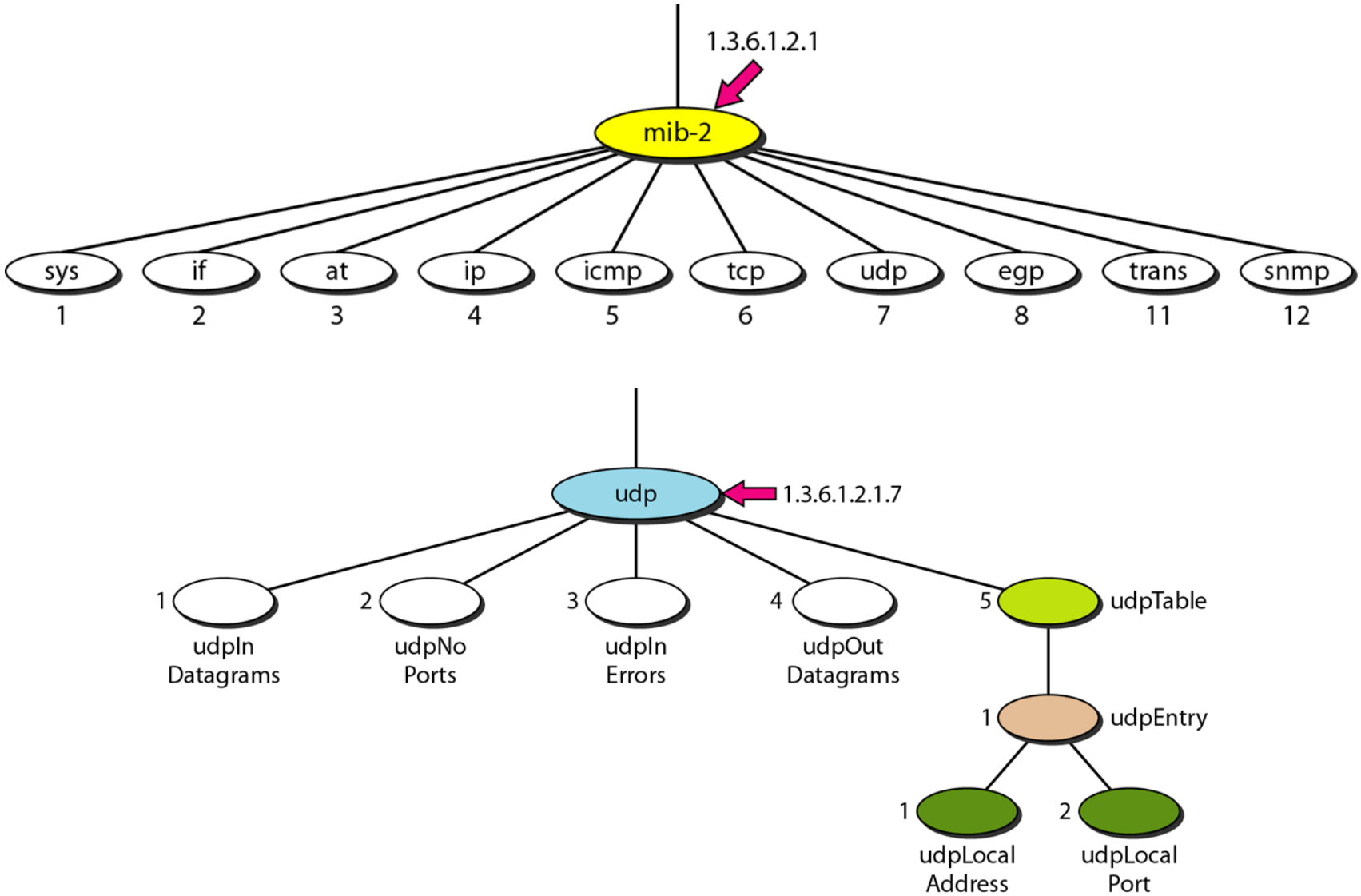
Management Information Base (MIB)

- a virtual database used for managing the entities in a communications network
  - organized in a *global MIB tree*
  - each *MIB (module)* represents a sub tree of this global MIB tree
- defines the properties of managed objects within a device to be managed (a router, switch, etc.)
  - each managed device keeps a database of values for each of the definitions written in the MIB it supports
- every device that supports SNMP must also support a generic *MIB-2 module*
  - device manufacturers are allowed to define their own device-specific MIBs
- *remember:* the standard describing how to create a MIB $\Rightarrow$ SMI(v2)



Management Information Base (MIB)

MIB-2 Module and UDP group example



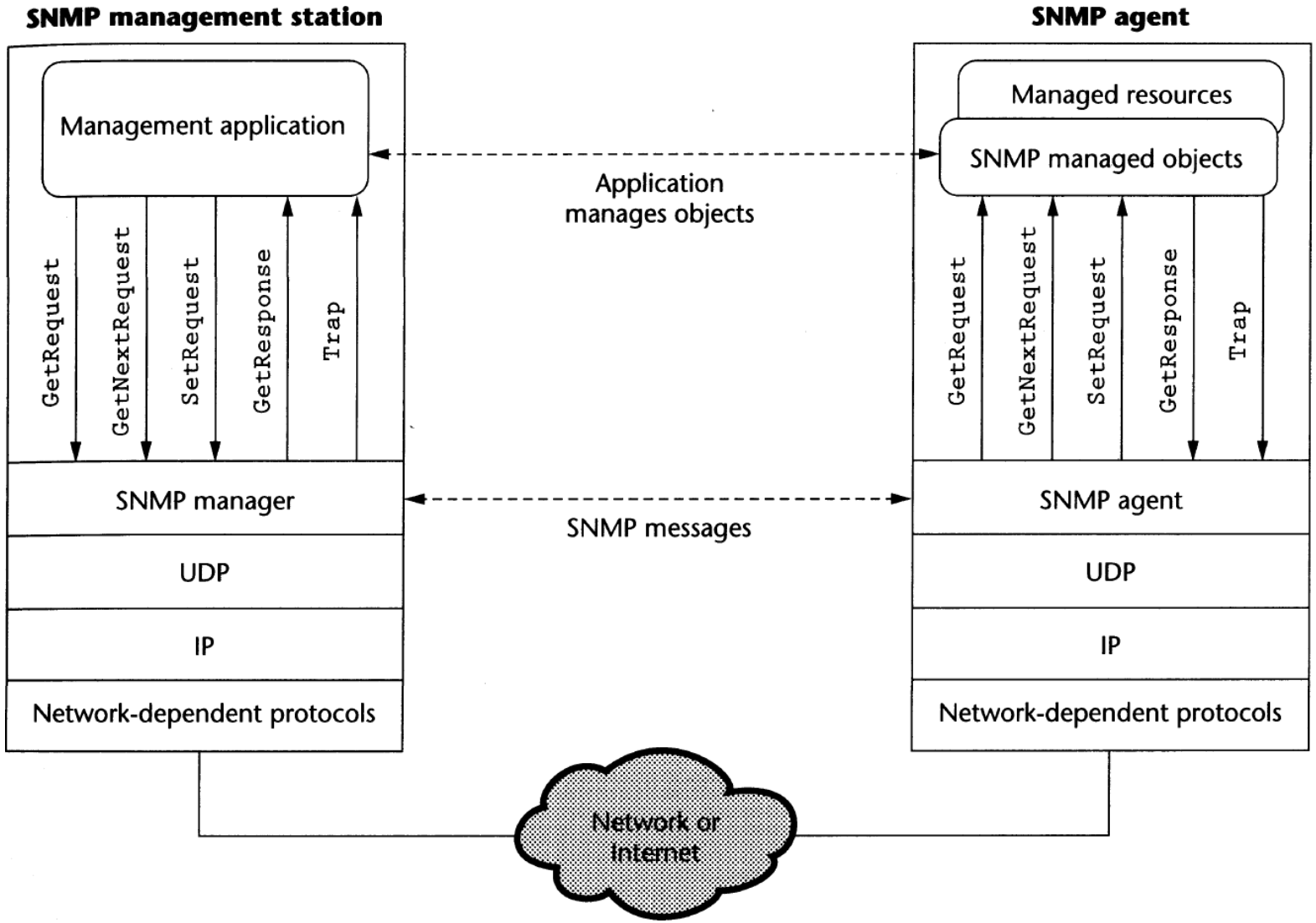
Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP)

- uses both SMI and MIB to allow the network management
- it allows:
  - a manager to retrieve the value of an object defined in an agent
    - the agent responses with the value
  - a manager to store a value in an object defined in an agent
    - the agent informs about the success/failure or responses with the newly set value
  - an agent to send an alarm message about an abnormal situation to the manager
- SNMPv3 defines eight types of packets (PDUs):
  - *GetRequest*, *GetNextRequest*, *GetBulkRequest*, *SetRequest*, *Response*, *Trap*, *InformRequest*, and *Report*

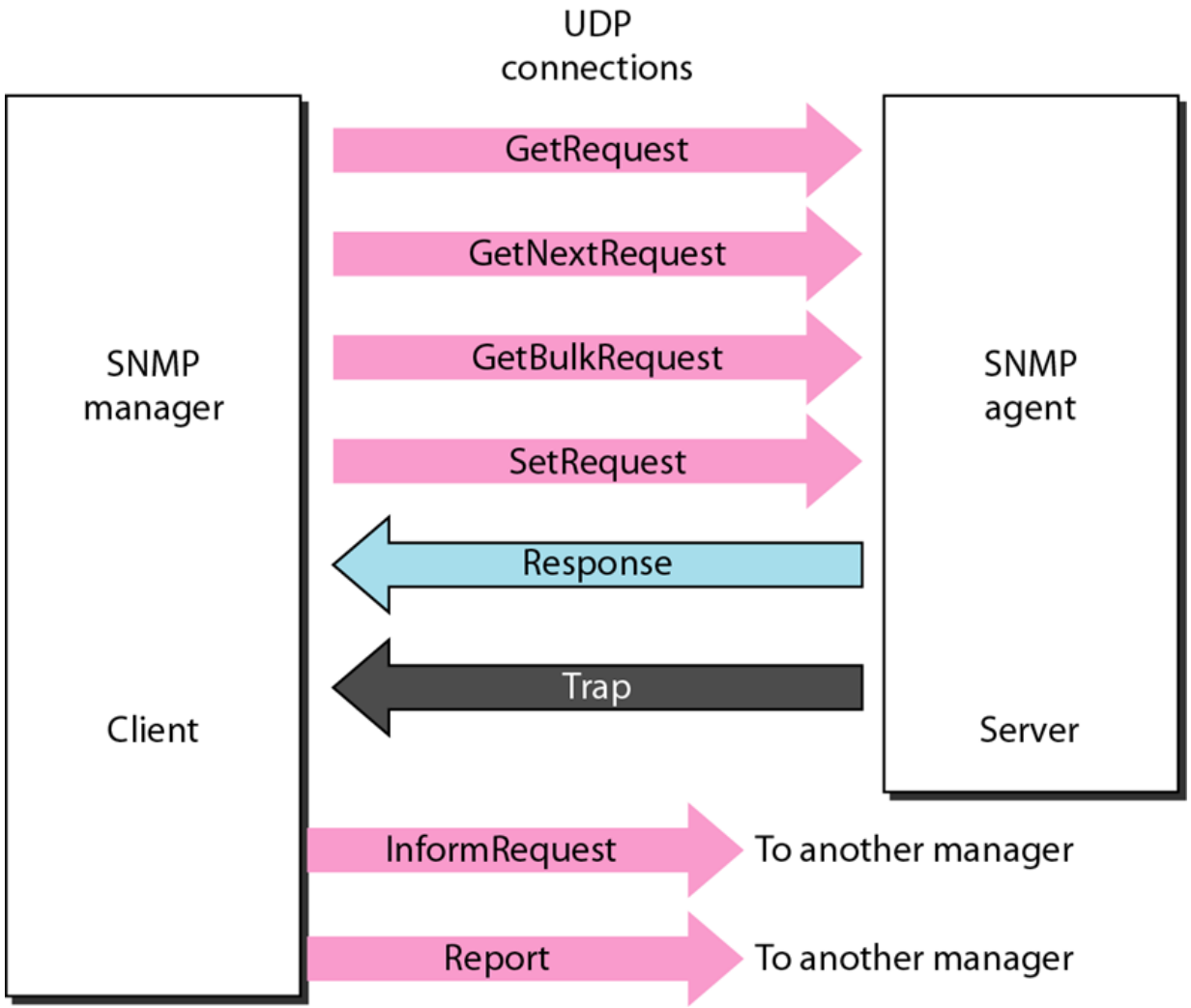
Simple Network Management Protocol (SNMP)

Communication Architecture Scheme



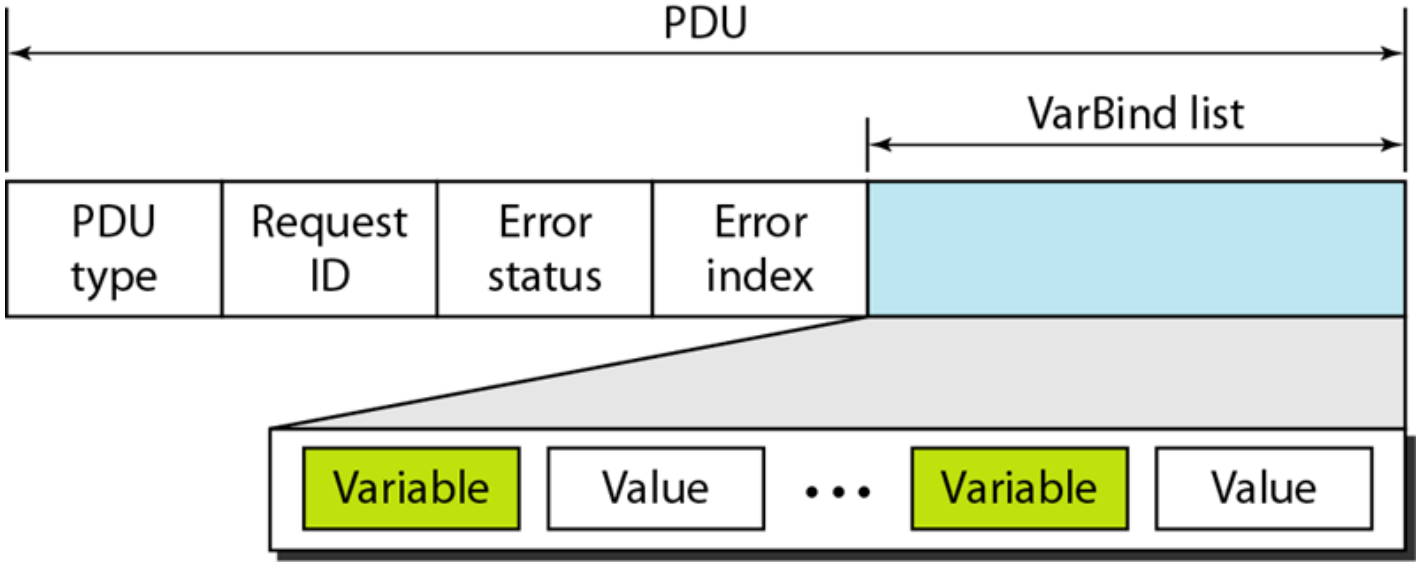
Simple Network Management Protocol (SNMP)

Protocol Data Units (PDUs) ⇒ Types of Packets



Simple Network Management Protocol (SNMP)

Protocol Data Units' (PDUs') Format



- *Request ID* – a sequence number used by the manager in a request and repeated by the agent in a response
  - allows to match a request and a corresponding response
- *Error Status* – an integer used only in response PDUs to indicate an error reported by an agent

Simple Network Management Protocol (SNMP)

Protocol Data Units' (PDUs') Format – Codes for PDU Type field

Data	*Class*	*Format*	*Number*	*Whole Tag (Binary)*	*Whole Tag (Hex)*
GetRequest	10	1	00000	**10100000**	**A0**
GetNextRequest	10	1	00001	**10100001**	**A1**
Response	10	1	00010	**10100010**	**A2**
SetRequest	10	1	00011	**10100011**	**A3**
GetBulkRequest	10	1	00101	**10100101**	**A5**
InformRequest	10	1	00110	**10100110**	**A6**
Trap (SNMPv2)	10	1	00111	**10100111**	**A7**
Report	10	1	01000	**10101000**	**A8**

Lecture overview

Network Management – Recapitulation

- Network Management by ISO – *FCAPS model*
  - Fault management, Configuration management, Accounting management, Performance management, Security management
- basic network management components
  - *Network Elements* – contain management interfaces (provided by agents)
  - *Management Network* – dedicated vs. shared network
  - *Network Management System* – centralized, distributed, or hierarchical layout
  - *Management Support Organization* – non-technical aspects of network management
- *Simple Network Management Protocol (SNMP)*
  - manager–agent approach
  - $\approx$ a framework – involves SMI, MIB, and other components
  - objects identified by identifiers (OIDs), each object has a type (defined by SMI)

Network Management – Further Information

- **FI courses:**
  - PV090: UNIX – Seminar of System Management (dr. Kasprzak)
  - PV065: UNIX – Programming and System Management I. (dr. Kasprzak)
  - PV077: UNIX – Programming and System Management II. (dr. Kasprzak)
  - PV175: MS Windows Systems Management I. (Bc. Dušek et al.)
  - PV176: MS Windows Systems Management II. (Mgr. Bukač et al.)
  - etc.
- **(Used) Literature:**
  - A. Farrel: *Network Management: Know It All.* Morgan Kaufmann, 2009.
  - A. Clemm: *Network Management Fundamentals.* Cisco Press, 2006.
  - B. Forouzan: *Data Communications and Networking,* 4^{th} *edition.* McGraw-Hill, 2007.
  - M. Subramanian: *Network management: principles and practice.* Addison-Wesley, 2000.
  - J. R. Burke: *Network Management: Concepts And Practice, A Hands-On Approach.* Pearson Education, 2008.
  - etc.