SNMP Basics

BUPT/QMUL

2021-05-27

北京邮电大学
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

Electronic Engineering

Agenda

- Brief introduction to Network Management
- Brief introduction to SNMP
- SNMP Network Management Framework
- RMON
- New trends of network management
- Summary

Brief Introduction To Network Management

Brief Introduction To Network Management

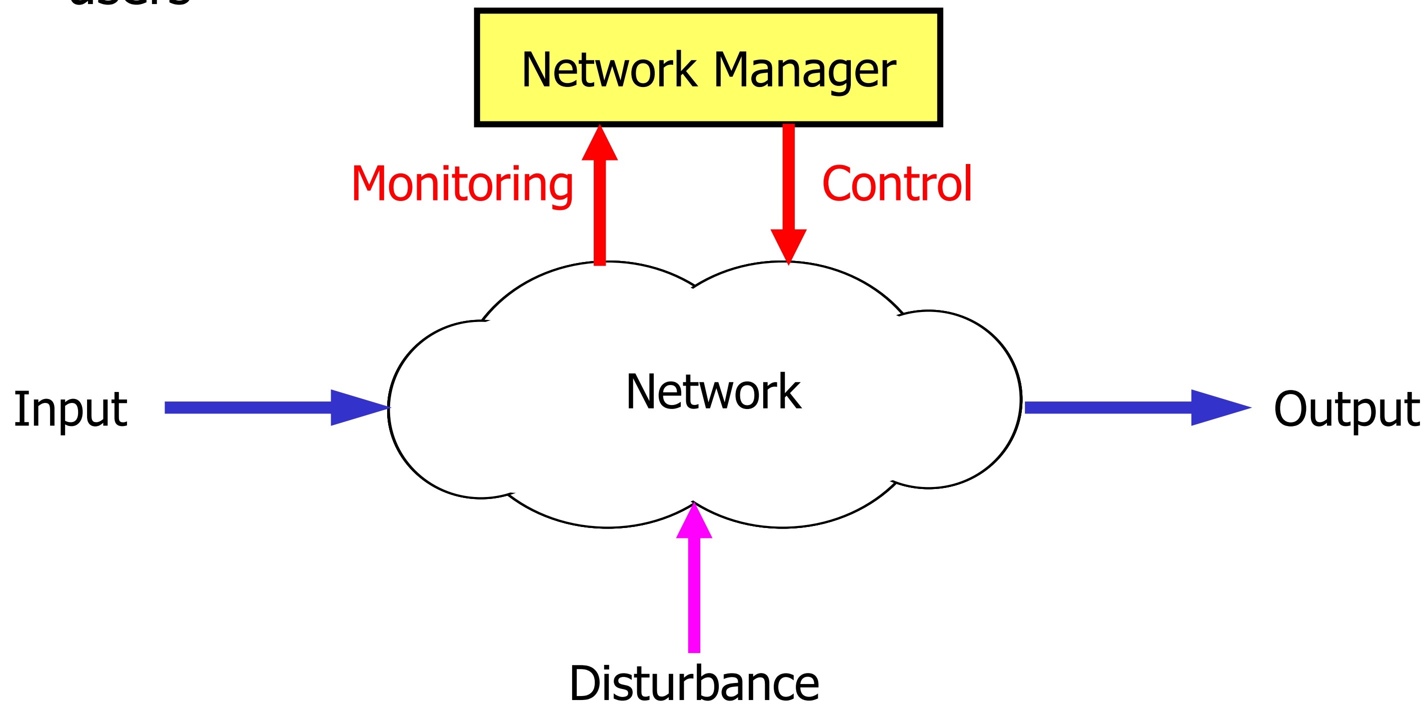
- What is network management?
- The goal of network management
- Functional areas defined by ISO
- Network management architectures
- Network management protocols

What is Network Management?

- Different things to different people, e.g.,
  - Monitoring network activity with protocol analyzer
  - Based on a distributed database, autopolling of network devices, generating real-time graphical views of network topology changes and traffic etc.
- Definition
  - Network management is a service that employs a variety of tools, applications, and devices to assist human network managers in monitoring and maintaining networks

The Goal Of Network Management

- The overall goal of network management is to help with the complexity of a data network and to ensure that data can go across it with maximum efficiency and transparency to the users



Functional Areas Defined By ISO

- Defined by ISO Network Management Forum
- FCAPS
  - Fault Management
  - Configuration Management
  - Accounting Management
  - Performance Management
  - Security Management

FCAPS (1)

- Fault management
  - Is the process of locating problems, or faults, on the data network
  - It involves the following steps:
    - Discover the problem
    - Isolate the problem
    - Fix the problem (if possible)
- Configuration management
  - The configuration of certain network devices controls the behaviour of the data network
  - Configuration management is the process of finding and setting up (configuring) these critical devices

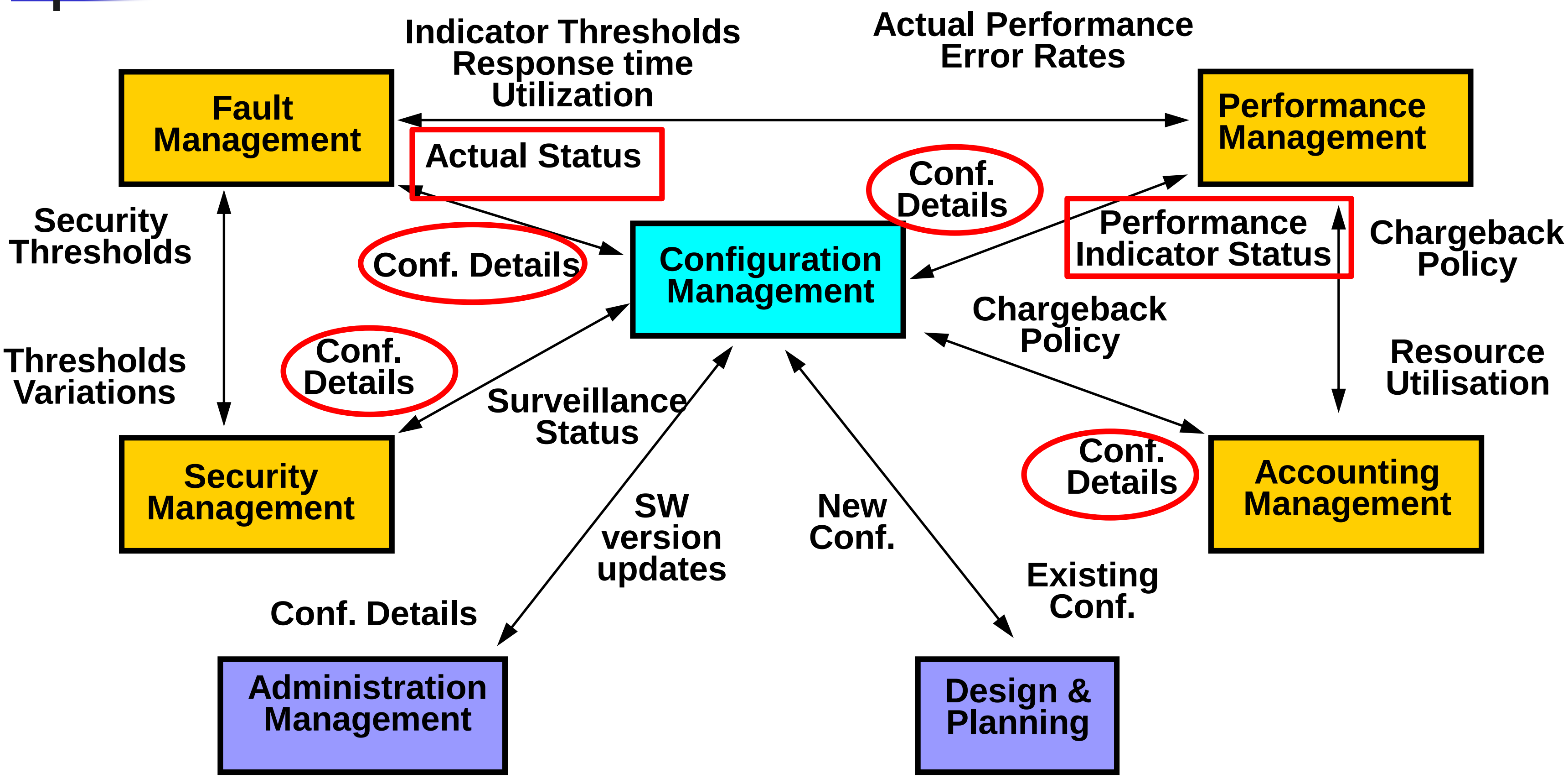
FCAPS (2)

- Accounting management
  - Involves tracking individual's utilization and grouping of network resources to ensure that users have sufficient resources
  - Involves granting or removing permission for access to the network
- Performance management
  - Involves measuring the performance of the network hardware, software, and media
  - Examples of measured activities are:
    - Overall throughput
    - Percentage utilization
    - Error rates
    - Response time

FCAPS (3)

- Security management
  - Is the process of controlling access to information on the data network
  - Provides a way to monitor access points and records information on a periodic basis
  - Provides audit trails and sounds alarms for security breaches

Relationship among Functional Areas

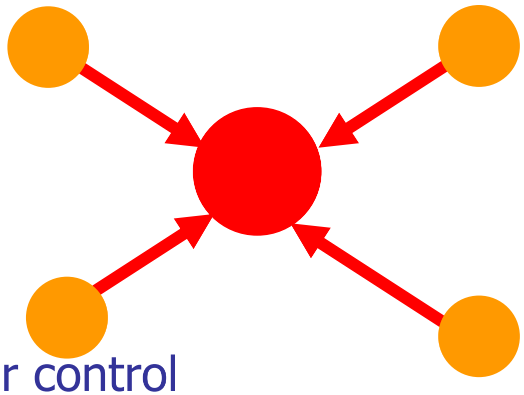


Network Management Architectures

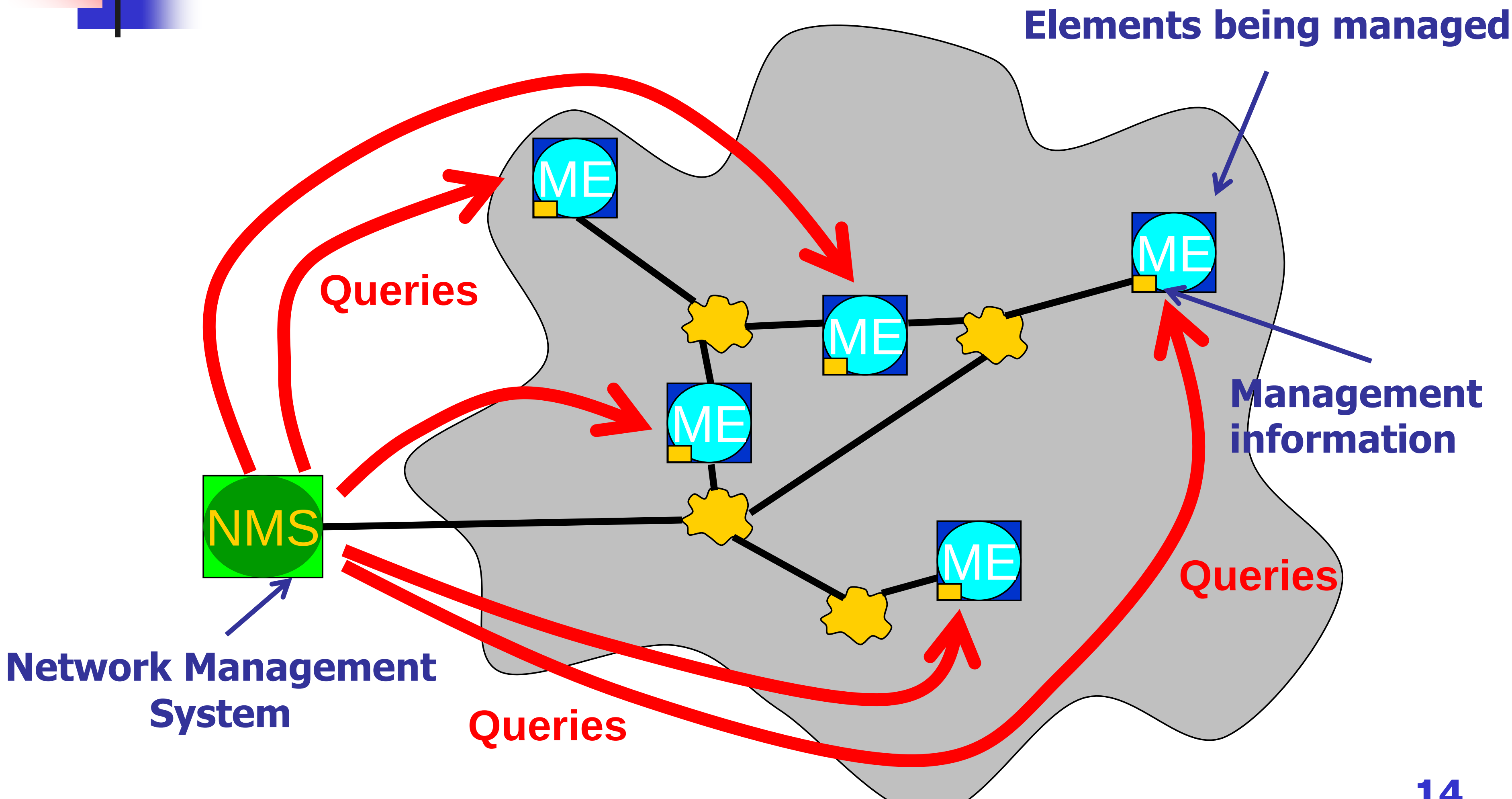
- The Network Management Platform can use various architectures to provide functionality
- The 3 most common are:
  - Centralized
  - Hierarchical
  - Distributed

Network Management Architectures
– Centralized Architecture

- The Network Management Platform resides on a single computer system
- Used for:
  - All network alerts & events
  - All network information
  - Access all management applications
- Pros:
  - Single location to view events & alerts - easier control
  - Easier maintenance
  - Security is easier to maintain
- Cons:
  - Single system is not redundant or fault tolerant (For full redundancy, the computer system is backed up by another system)
  - As network elements are added, may be difficult or expensive to scale system to handle load
  - Having to query all devices from a single location
- Examples: IBM NetView

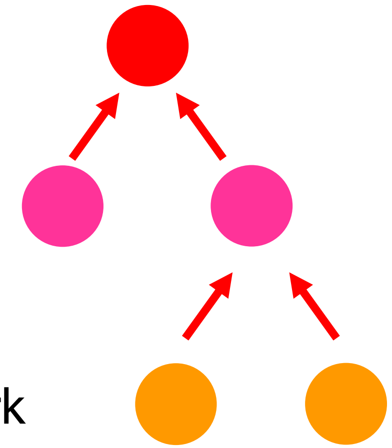


Centralized Architecture

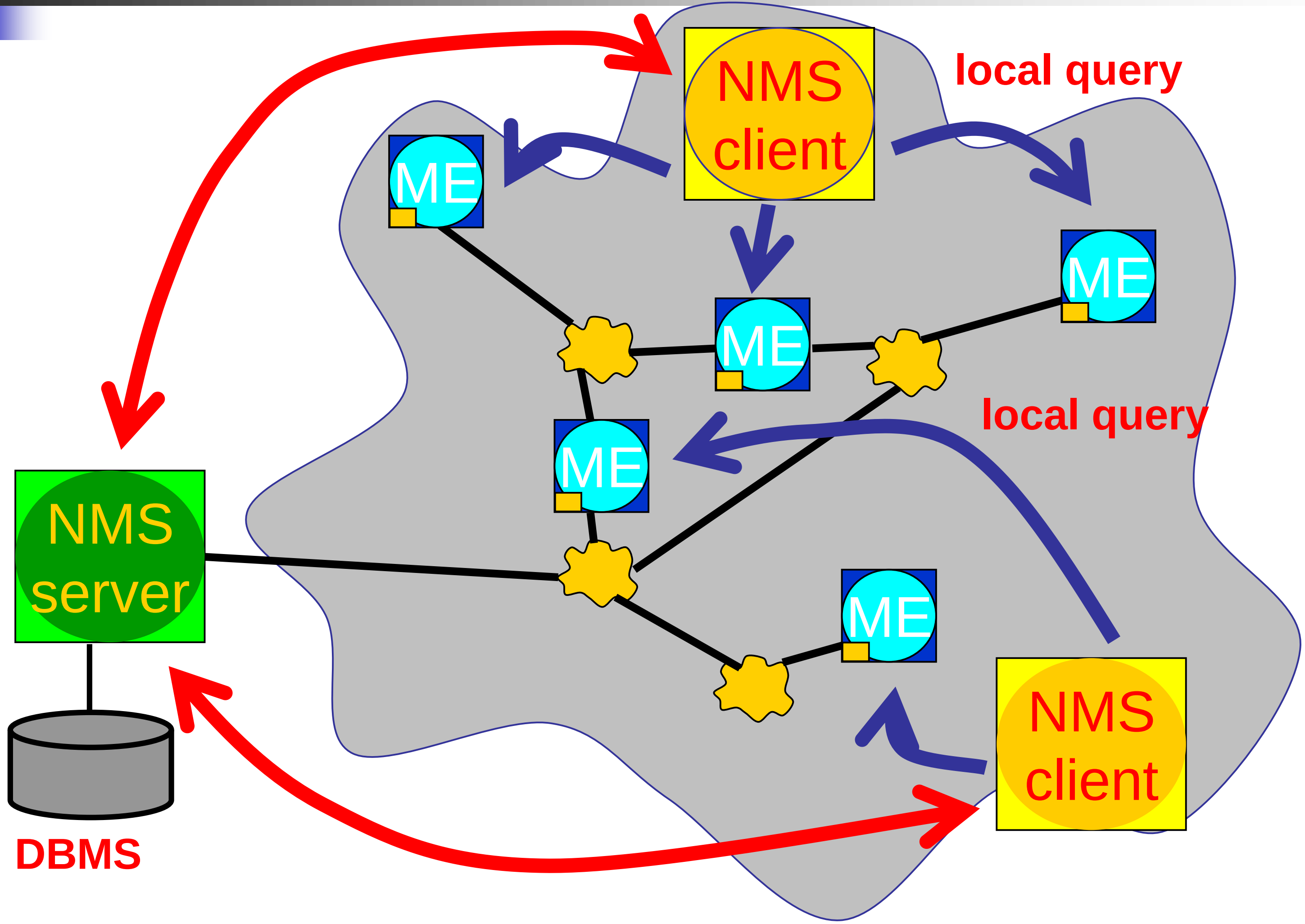


Network Management Architectures – Hierarchical Architecture

- Uses multiple computer systems
  - One system acting as the central server
  - Other systems working as clients
- Central server requires backups for redundancy
- Key features:
  - Not dependent on a single system
  - Network management tasks distributed
  - Network monitoring distributed throughout network
  - Centralized information storage
- Pros:
  - Multiple systems to manage the network – more robust and scalable
- Cons:
  - Information gathering is more difficult and time consuming
  - The list of managed devices managed by each client needs to be predetermined and manually configured - more administration
- Examples: HP Openview

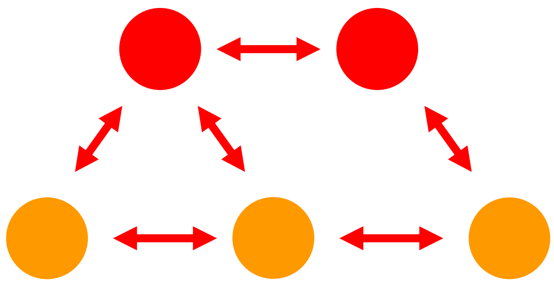


Hierarchical Architecture



Network Management Architectures
– Distributed Architecture

- Uses multiple peer network management systems
- Contains advantages from central & hierarchical architectures
  - Selected location(s) for all network information, alerts & events
  - Selected location(s) to access all management applications
  - Not dependent on a single system
  - Distribution of network management tasks
  - Distribution of network monitoring throughout the network



Network Management Protocols

- SNMP (Simple Network Management Protocol)
- SNMPv2 (SNMP version 2)
- SNMPv3 (SNMP version 3)
- CMIS/CMIP (Common Management Information Services/Common Management Information Protocol)

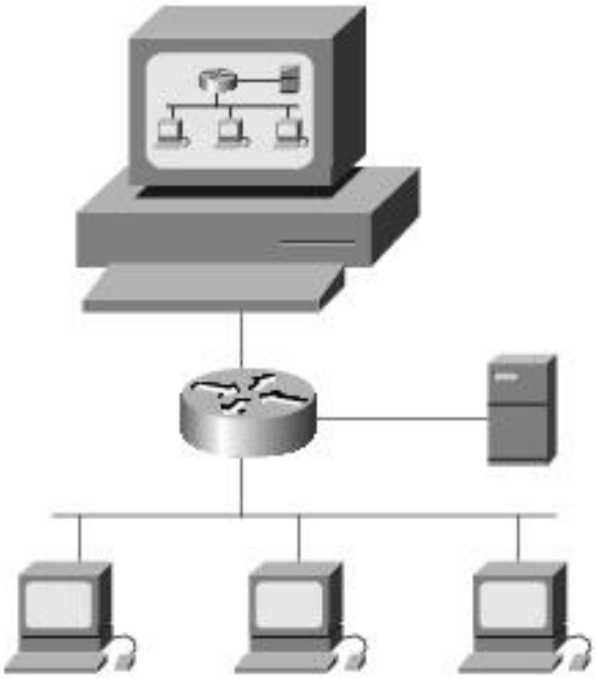
Brief Introduction to SNMP

Brief Introduction To SNMP

- What is SNMP?
- SNMP history
- SNMP model

What Is SNMP?

- Simple Network Management Protocol
- An application layer protocol that provides a way of monitoring and managing a heterogeneous computer network
- A part of TCP/IP protocol suite
- Based on client/server model
- Based on UDP
- Well-known ports
  - UDP Port 161: SNMP Get/Set Messages
  - UDP Port 162: SNMP Trap Messages

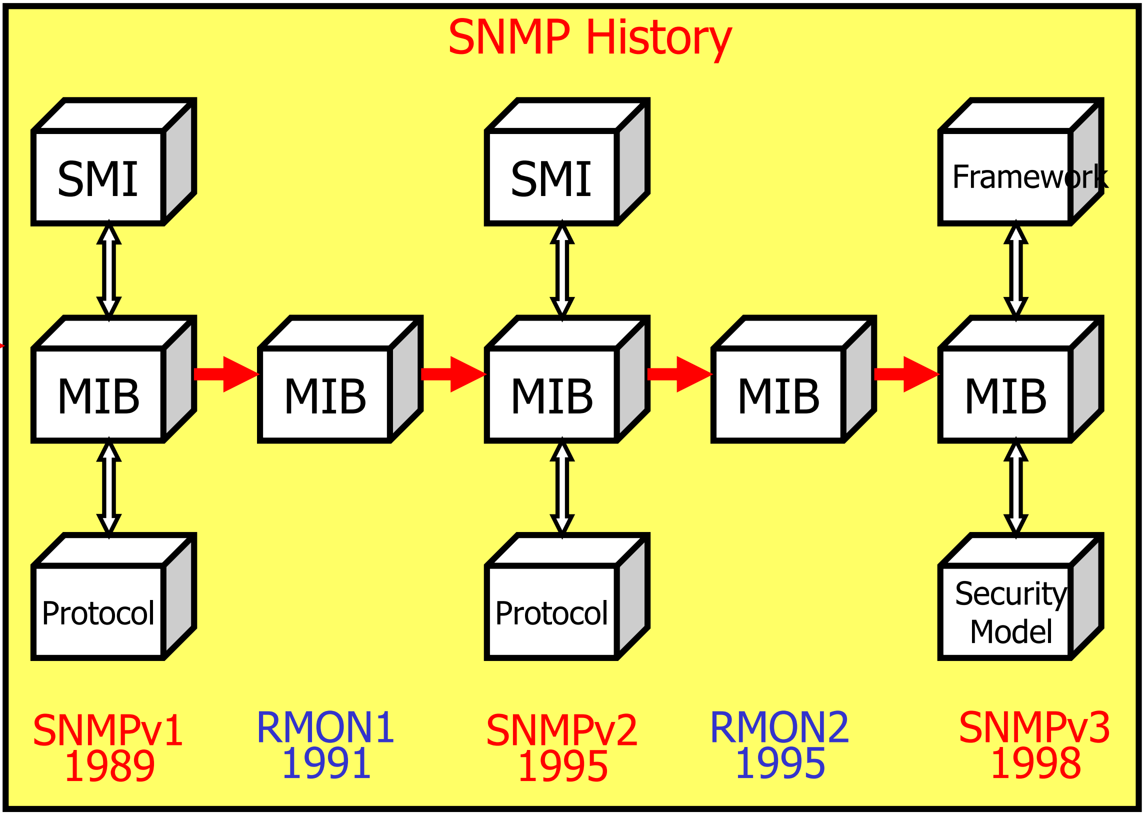


SNMP vs. Network Management

- SNMP realizes the F-C-P functions of network management
- SNMP does not cover all the function areas of network management
- Network management is a systematic work, in which SNMP is an important tool and protocol

SNMP History (1)

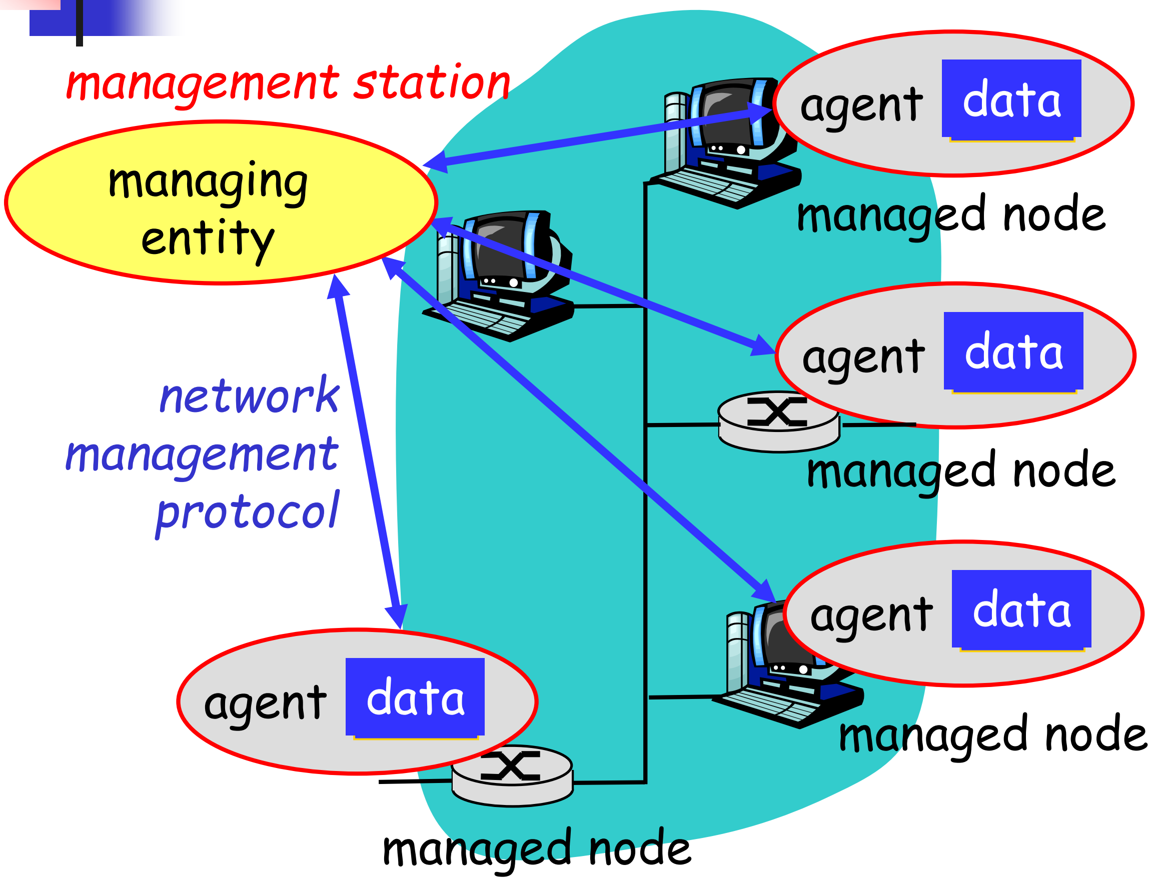
Network Management is based on ICMP and PING → SGMP →



SNMP History (2)

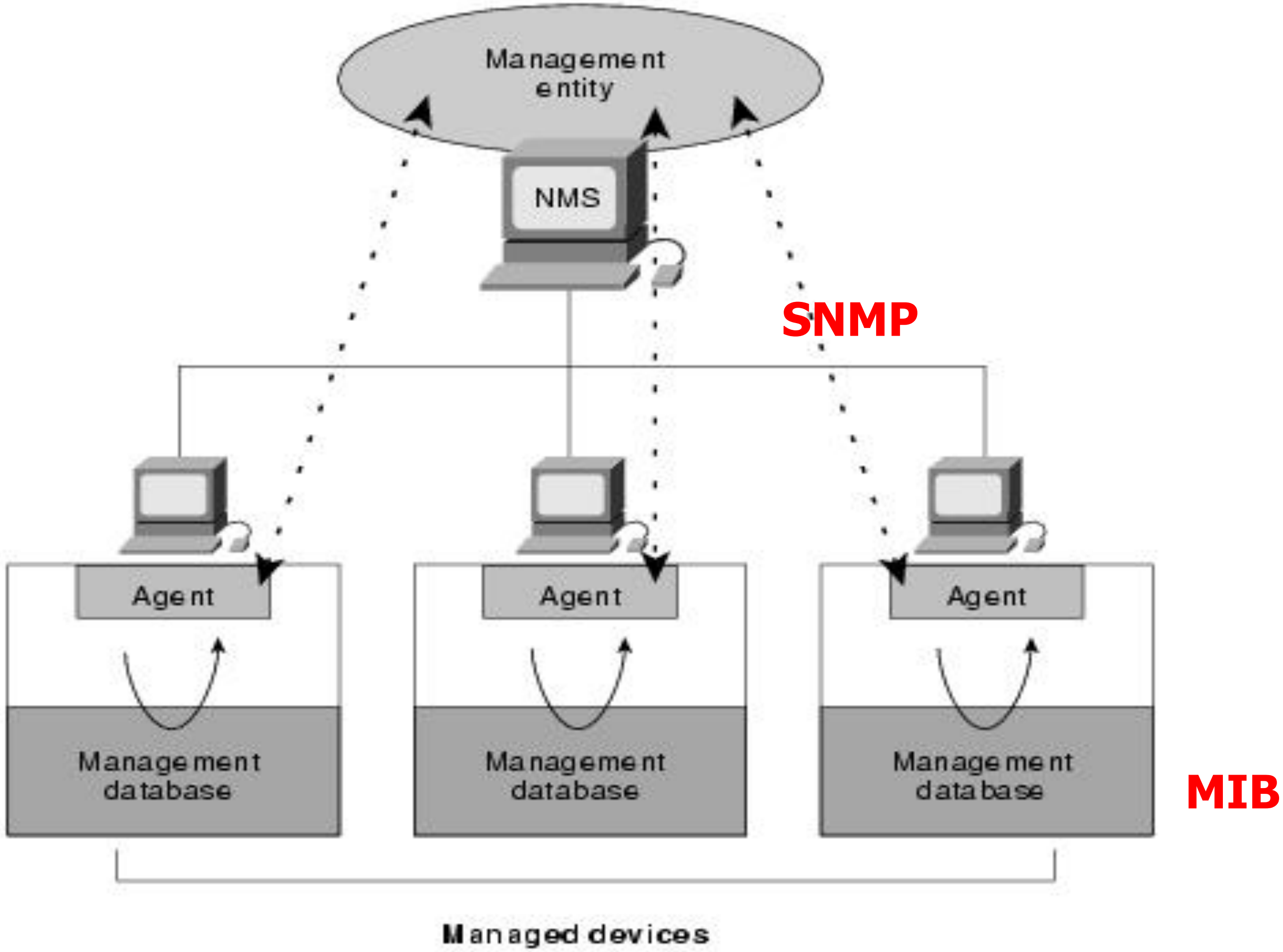
- SNMPv1
  - *Basic function of read/write MIB*
- SNMPv2
  - *improve performance, security, confidentiality, and manager-to-manager communications*
- SNMPv3
  - *Security enhancement*
- RMON1
  - *Providing monitoring capability at data link layer in OSI model*
- RMON2
  - *Providing monitoring capability above data link layer in OSI model*

SNMP Model (1)

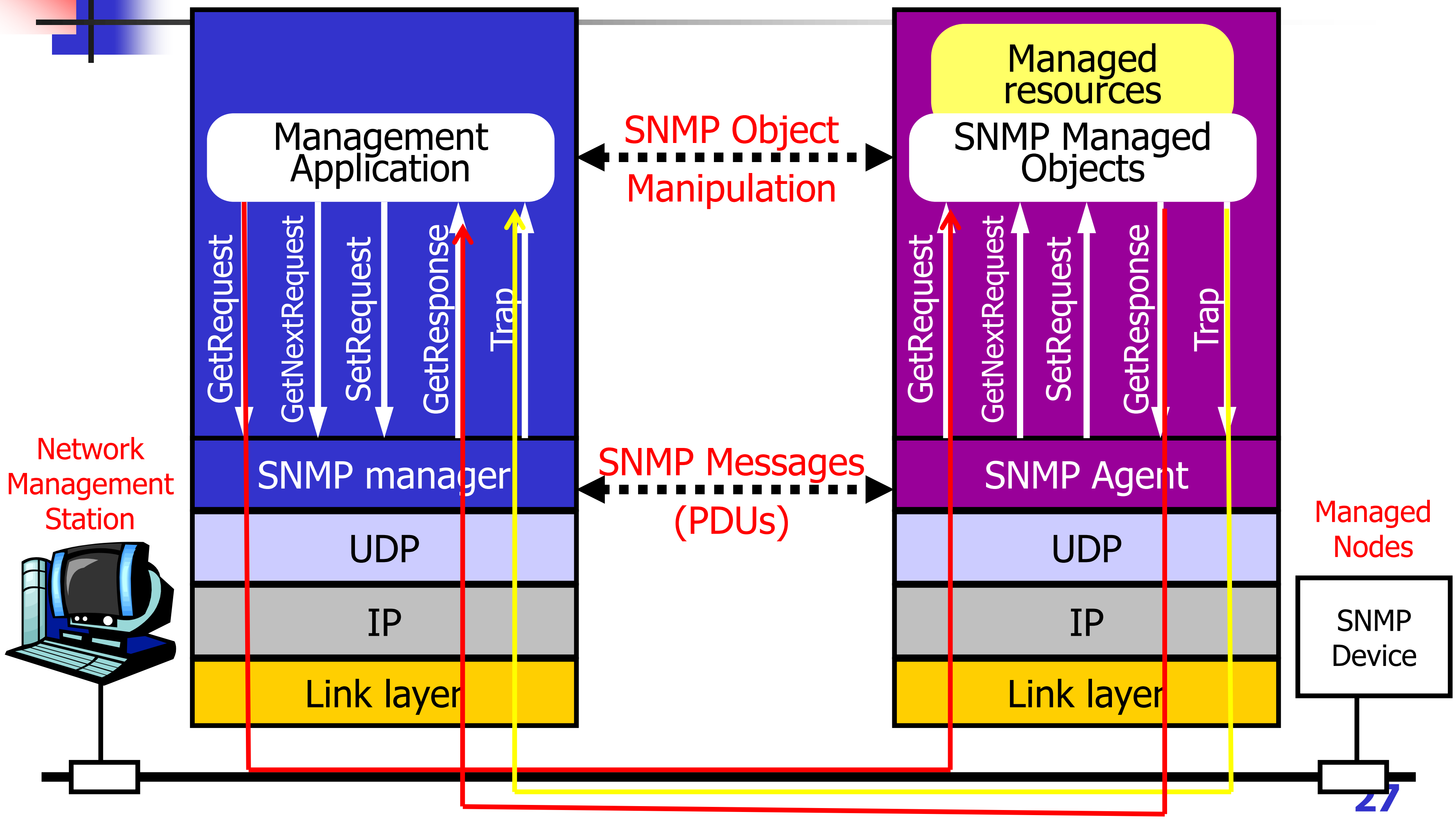


- The SNMP model of a managed network consists of four components:
  - Managed Nodes (Agent)
  - Management Stations (NMS)
  - Management Information (MIB)
  - A Management Protocol (SNMP)

SNMP Model (2)
– more abstract description



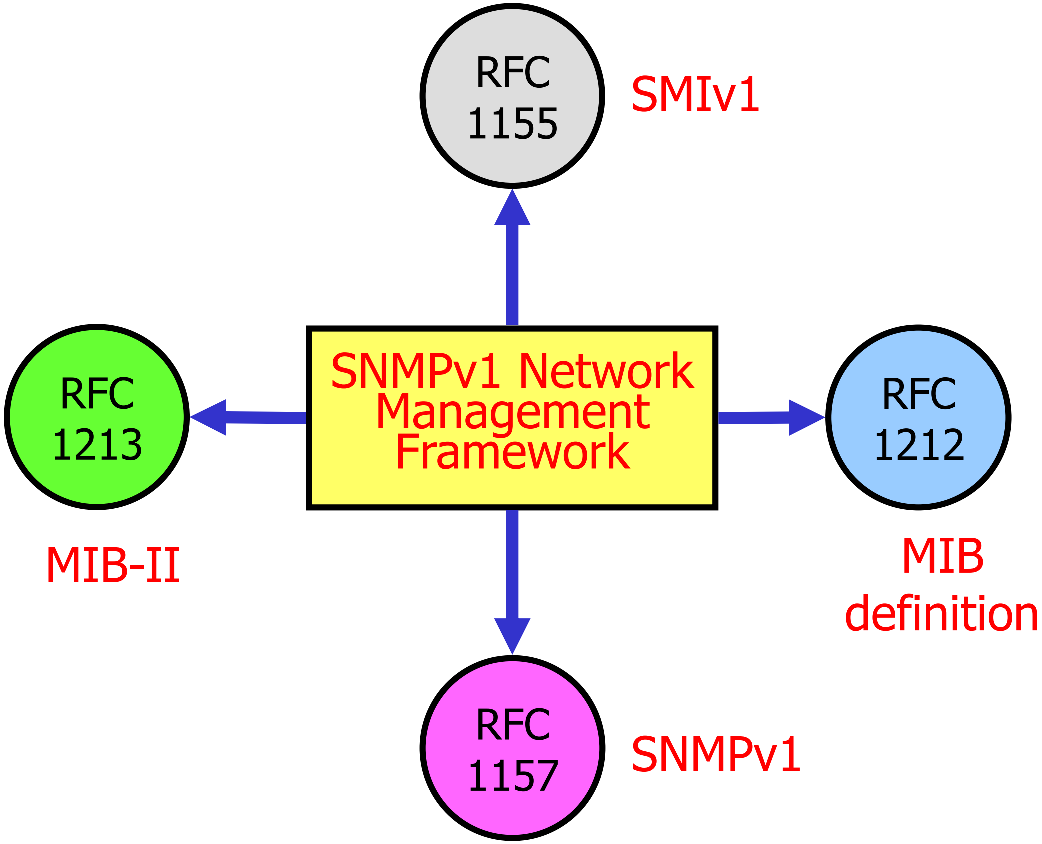
SNMP Architecture



SNMP Network Management Framework

SNMP Network Management Framework

- 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 information, commands between manager<->managed object



SMI: Structure of Management Information

- The *SMI* defines the rules for describing management information
- Syntax, semantics of management data, well-defined, unambiguous
- using ASN.1 (Abstract Syntax Notation One) for an unambiguous description without inconsistencies
- only a subset of ASN.1

SMI – What Is ASN.1?

- An international standard defining the data structure used and how these are transferred between systems (BER, Basic Encoding Rules)
- Widely used in many standards
  - X.400/X.500
  - H.323
  - SNMP
- Simple ASN.1 example

```
Age::=INTEGER (0..120)
User::=SEQUENCE {
       name    IA5String(SIZE(1..128)),
       age     Age DEFAULT 18.
       address IA5String OPTIONAL
       }
```

SMI – SMI Syntax

- General ASN.1 data type
  - INTEGER
  - OCTET STRING
  - OBJECT IDENTIFIER
  - NULL
  - SEQUENCE
- SMI-specific data type
  - IPAddress: data type used to describe 32-bit IP address
  - Counter: data type used to define a cycle counter
  - TimeTicks: data type related to a timer
  - PhysAddress: data type used to define the MAC address
  - ...
- MIBs are written using the ASN.1 specification language and must adhere to the grammar specified in the SMI specifications

MIB: Management Information Base

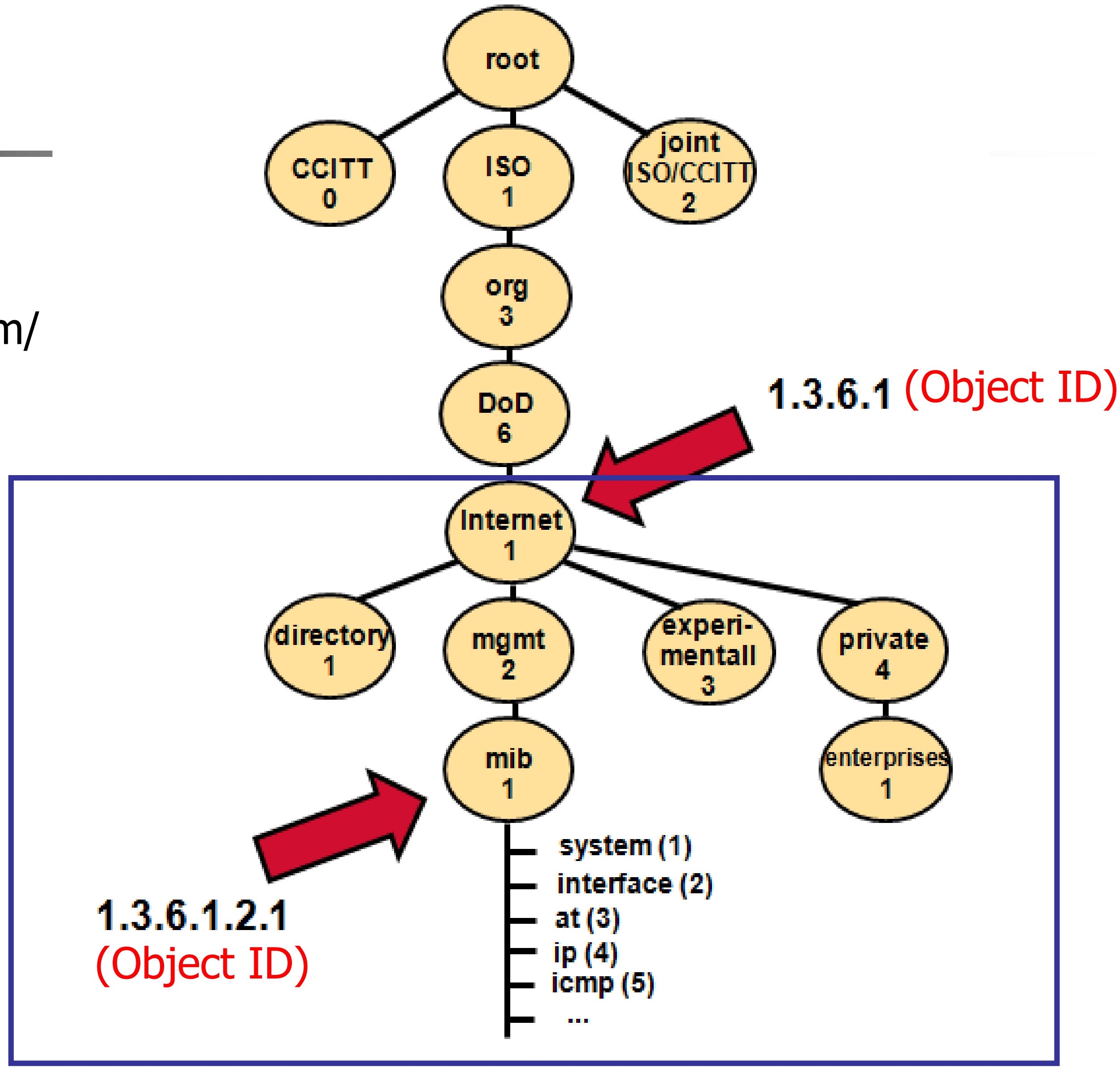
- A *MIB* is a collection of information that is organized *hierarchically*
  - MIBs are comprised of managed objects and are identified by *OIDs* (object identifiers)
- Two types of managed objects exist
  - *Scalar objects* define a single object instance
    - E.g., tcpInSegs, icmpInMsgs
  - *Tabular objects* define multiple related object instances that are grouped in MIB tables
    - E.g., udpTable, tcpConnTable, ipRouteTable
- *SMI* is the data definition language for MIB objects

MIB – ISO Object Identifier Tree

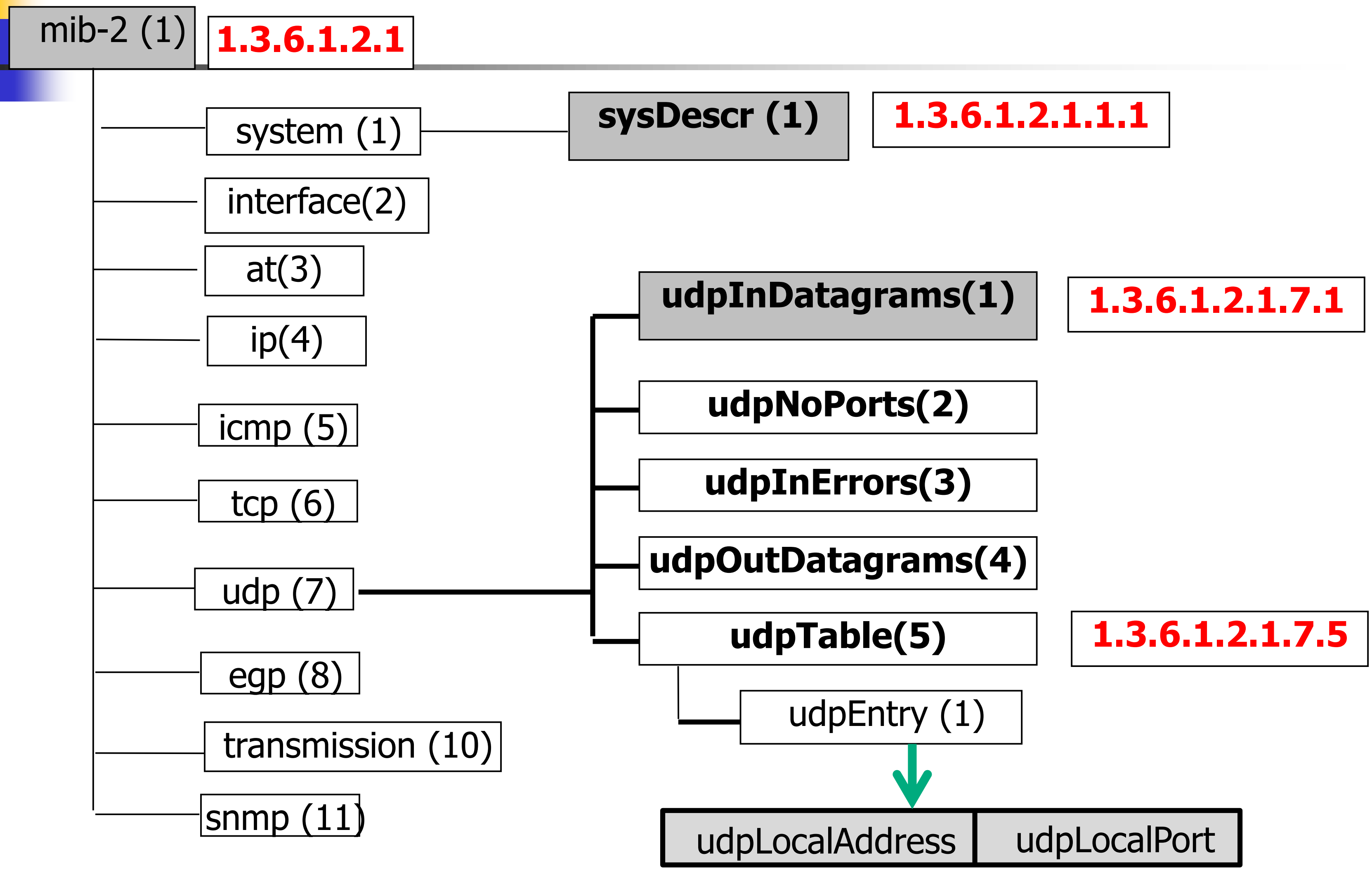
Check out:

http://www.oid-info.com/

Subtree of Internet object IDs

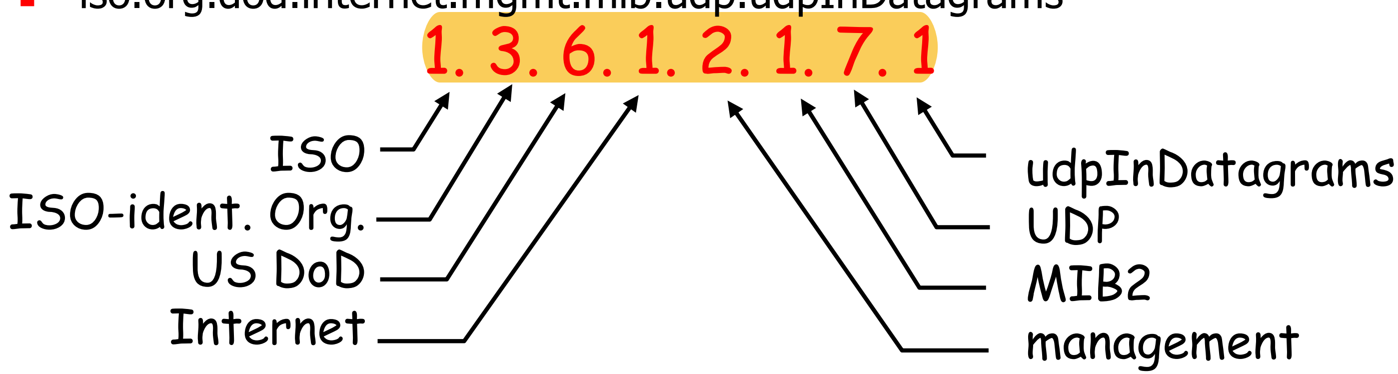


SMI MIB


mib-2 (1)
1.3.6.1.2.1
system (1)
sysDescr (1)
1.3.6.1.2.1.1.1
interface(2)
at(3)
ip(4)
icmp (5)
tcp (6)
udp (7)
egp (8)
transmission (10)
snmp (11)
udpInDatagrams(1)
1.3.6.1.2.1.7.1
udpNoPorts(2)
udpInErrors(3)
udpOutDatagrams(4)
udpTable(5)
1.3.6.1.2.1.7.5
udpEntry (1)
udpLocalAddress
udpLocalPort

MIB – Naming

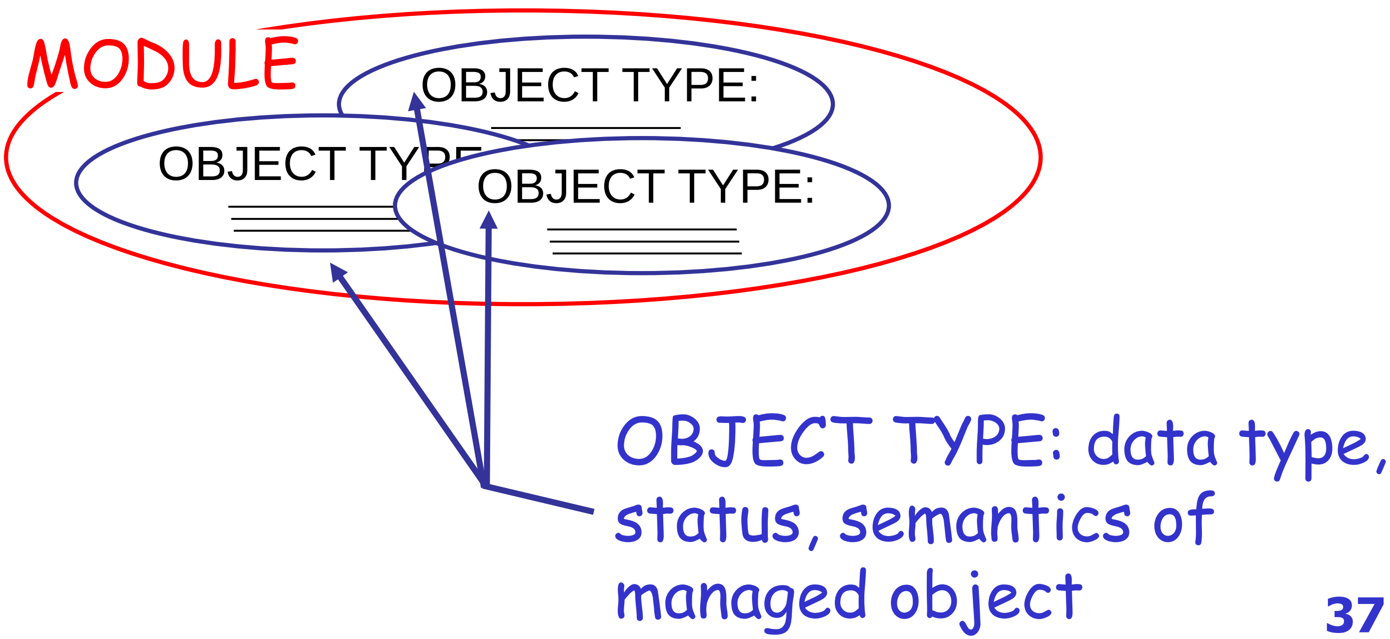
- Each object has a unique OID consisting of numbers separated by decimal points, and a more readable name. E.g.,
  - 1.3.6.1.2.1.7.1
  - iso.org.dod.internet.mgmt.mib.udp.udpInDatagrams



- When an SNMP manager wants to know the value of an object, it will assemble a GetRequest packet that includes the OID for that object.
- The agent receives the request and looks up the OID in its MIB. If the OID is found, a response packet is assembled and sent with the current value of the object. If the OID is not found, a special error response is sent

MIB – Definition

- "A MIB definition consists of two parts: a textual part, in which objects are placed into groups, and a MIB module, in which objects are described solely in terms of the ASN.1 macro OBJECT-TYPE, which is defined by the SMI." --- From RFC1212



MIB – Definition Example

```
-- the UDP group

udpInDatagrams OBJECT-TYPE
...
::= { udp 1 }

udpNoPorts OBJECT-TYPE
...
::= { udp 2 }

udpInErrors OBJECT-TYPE
...
::= { udp 3 }

udpOutDatagrams OBJECT-TYPE
...
::= { udp 4 }

udpTable OBJECT-TYPE
...
::= { udp 5 }
...
```

```
udpInDatagrams OBJECT-TYPE
    SYNTAX Counter
    ACCESS read-only
    STATUS mandatory
    DESCRIPTION
            "The total number of UDP
            datagrams delivered to
            UDP users."
    ::= { udp 1 }
```

See RFC 1213 for more detailed examples

Module

MIB example: UDP module

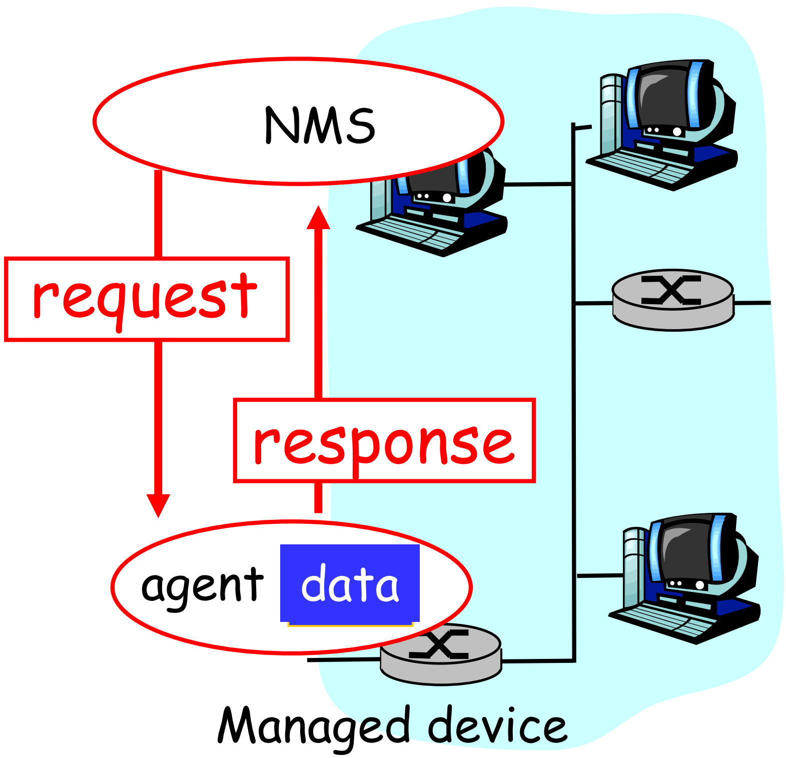
Object ID	Name	Type	Comments
1.3.6.1.2.1.7.1	UDPInDatagrams	Counter	total # datagrams delivered at this node
1.3.6.1.2.1.7.2	UDPNoPorts	Counter	# underliverable datagrams as no app at port
1.3.6.1.2.1.7.3	UDPInErrors	Counter	# undeliverable datagrams all other reasons
1.3.6.1.2.1.7.4	UDPOutDatagrams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

SNMP Protocol

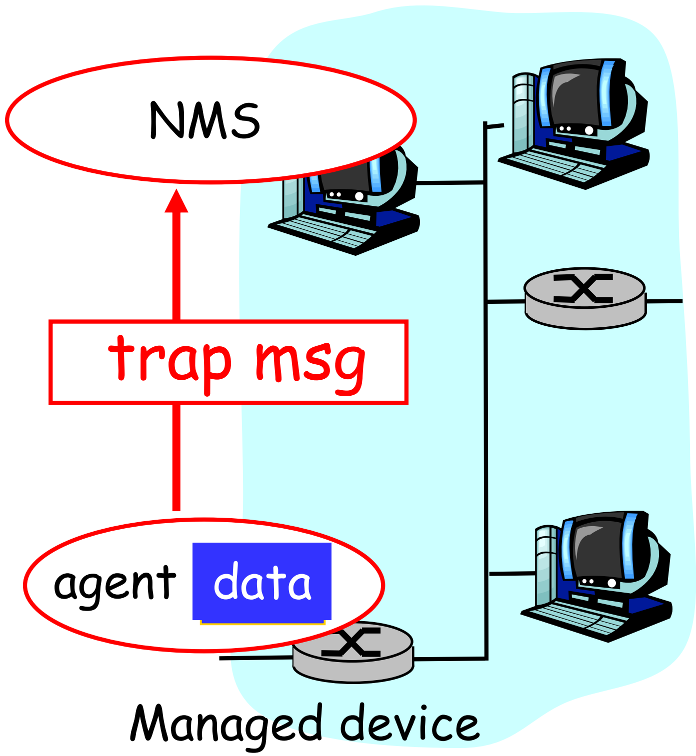
- SNMP traps / polling
- SNMP commands
- SNMP message format

SNMP Traps / Polling (1)

- Two ways to deliver MIB information, commands



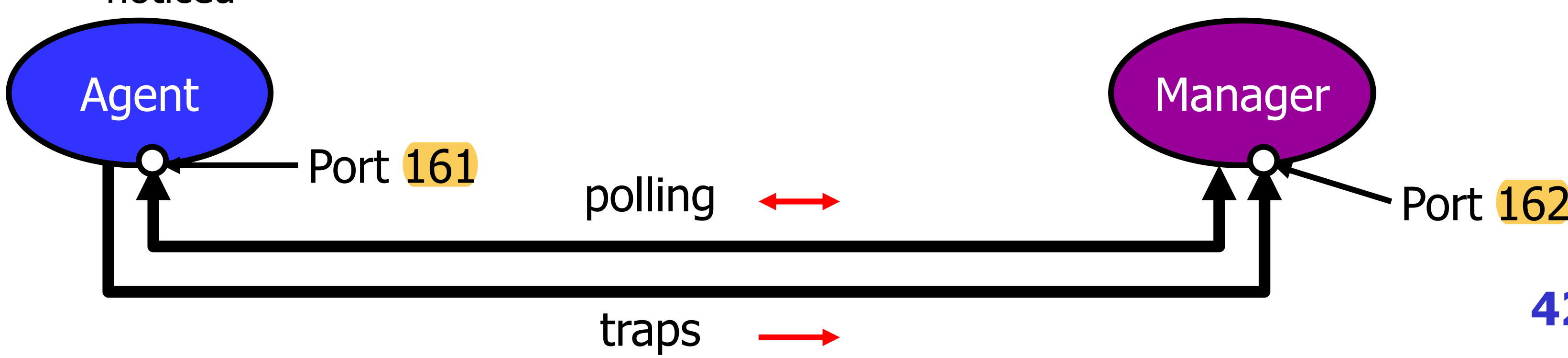
Polling mode



trap mode

SNMP Traps / Polling (2)

- **Traps**
  - When abnormal event occurs, an agent sends a trap message to nominated NMS(s)
    - Trap indicates broad class of error [type], network device name and which object(s) should be queried for more information and time of event.
    - Hence keeps the message short and simple
  - NMS may then query the agent for more information on the named objects
  - NMS must be listening for TRAP messages
- **Polling**
  - The NMS periodically queries the network devices for information
  - The advantage is NMS is in control and knows the “big picture”
  - The disadvantage is the amount of delay from when an event occurs to when it’s noticed

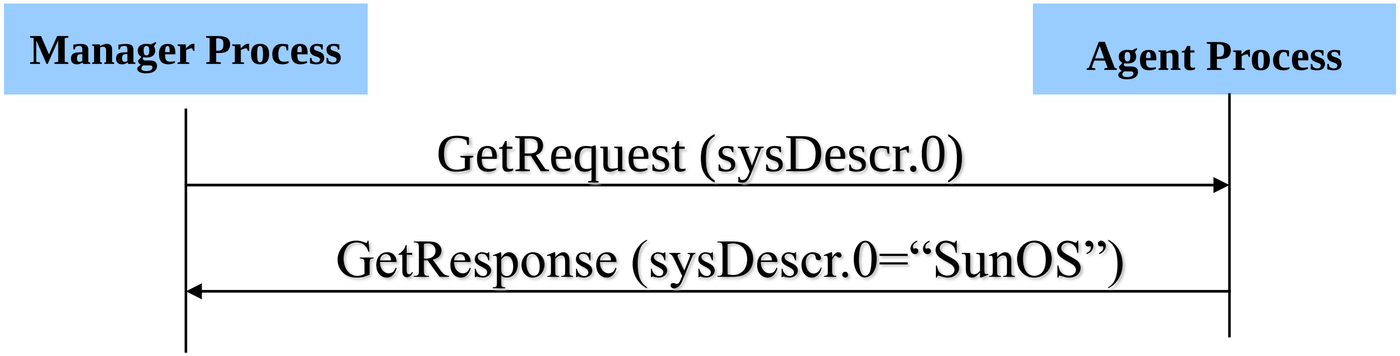


SNMP Commands

Command	Description	Version
GetRequest	NMS-to-Agent: get data (instance)	SNMPv1
GetNextRequest	NMS-to-Agent: get data (next in list)	SNMPv1
GetBulkRequest	NMS-to-Agent: get data (block)	SNMPv2
InformRequest	NMS-to-NMS: MIB information exchange	SNMPv2
SetRequest	NMS-to-Agent: set MIB value	SNMPv1
GetResponse	Agent-to-NMS: value, response to request	SNMPv1
Trap	Agent-to-NMS: report exceptional event to NMS	SNMPv1

GetRequest [Get]

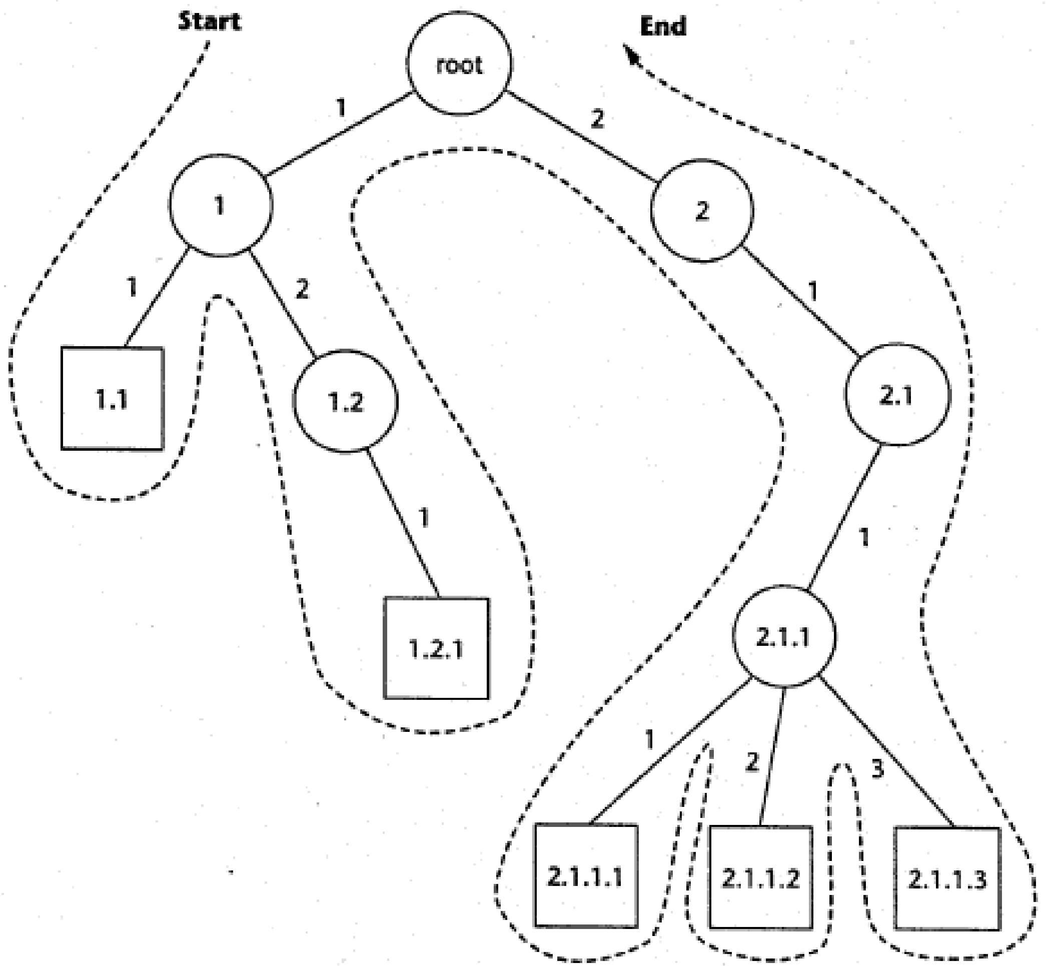
- Most common PDU(Packet Data Unit).
- Used to ask SNMP agent for value of a particular MIB agent.
- NMS sends out 1 Get PDU for each instance, which is a unique OID string.



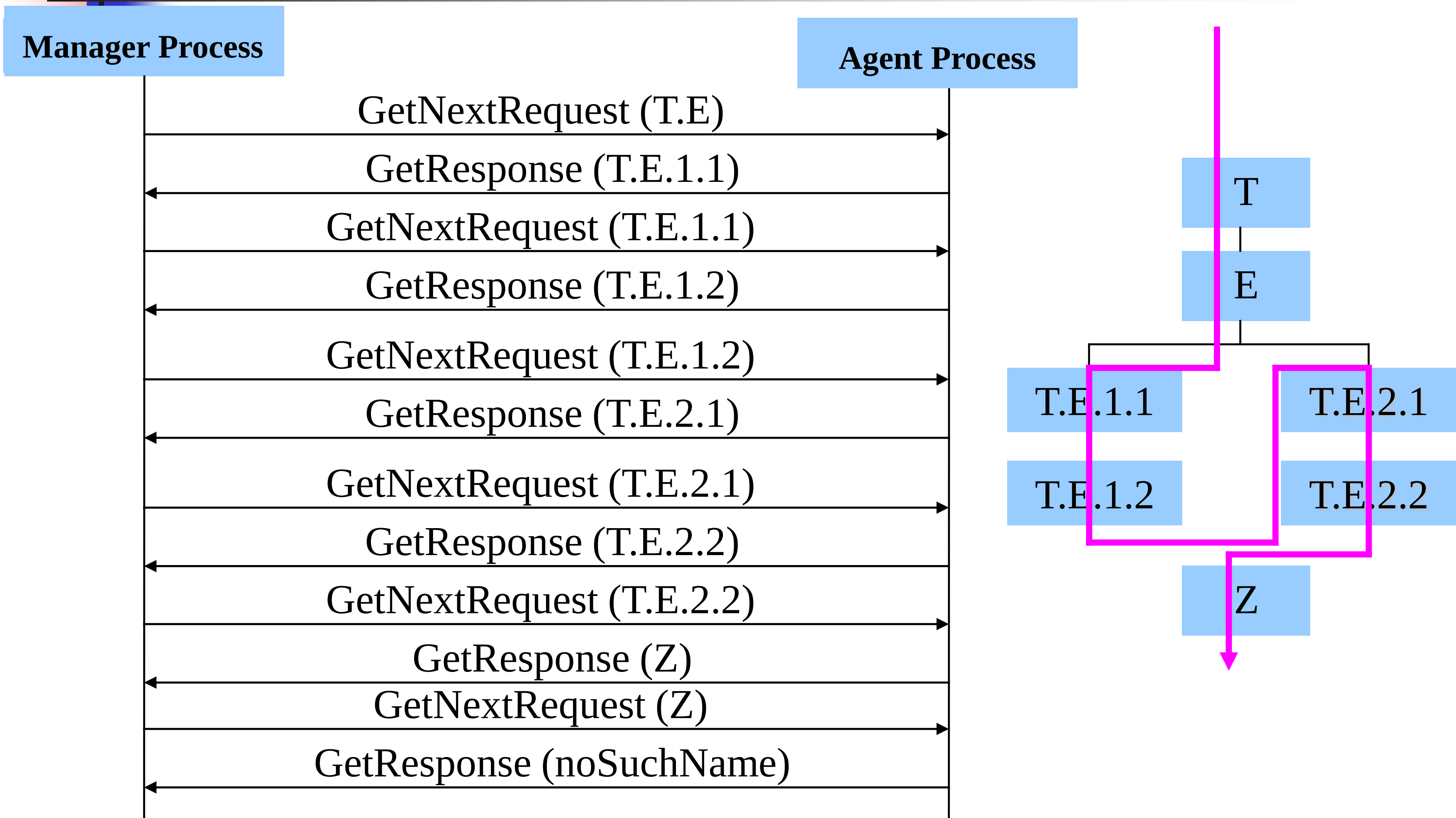
GetNextRequest

- Retrieves the NEXT variable instance existing on the agent in the tree of objects
- It either returns the next existing object, or error if none
- Can be used to traverse any part or all of the objects present on an agent
- Starting from the known mandatory **sysDescr** object, a NMS can find all others
- Simple, powerful mechanism
  - easy to implement on an agent, but
  - makes NMS do more work to discover necessary information

Lexicographic Ordering



SNMP Commands [GetNext]



Example of GetNextRequest

snmpwalk: an SNMP application using SNMP *GetNextRequest* to query a network entity for a tree of information

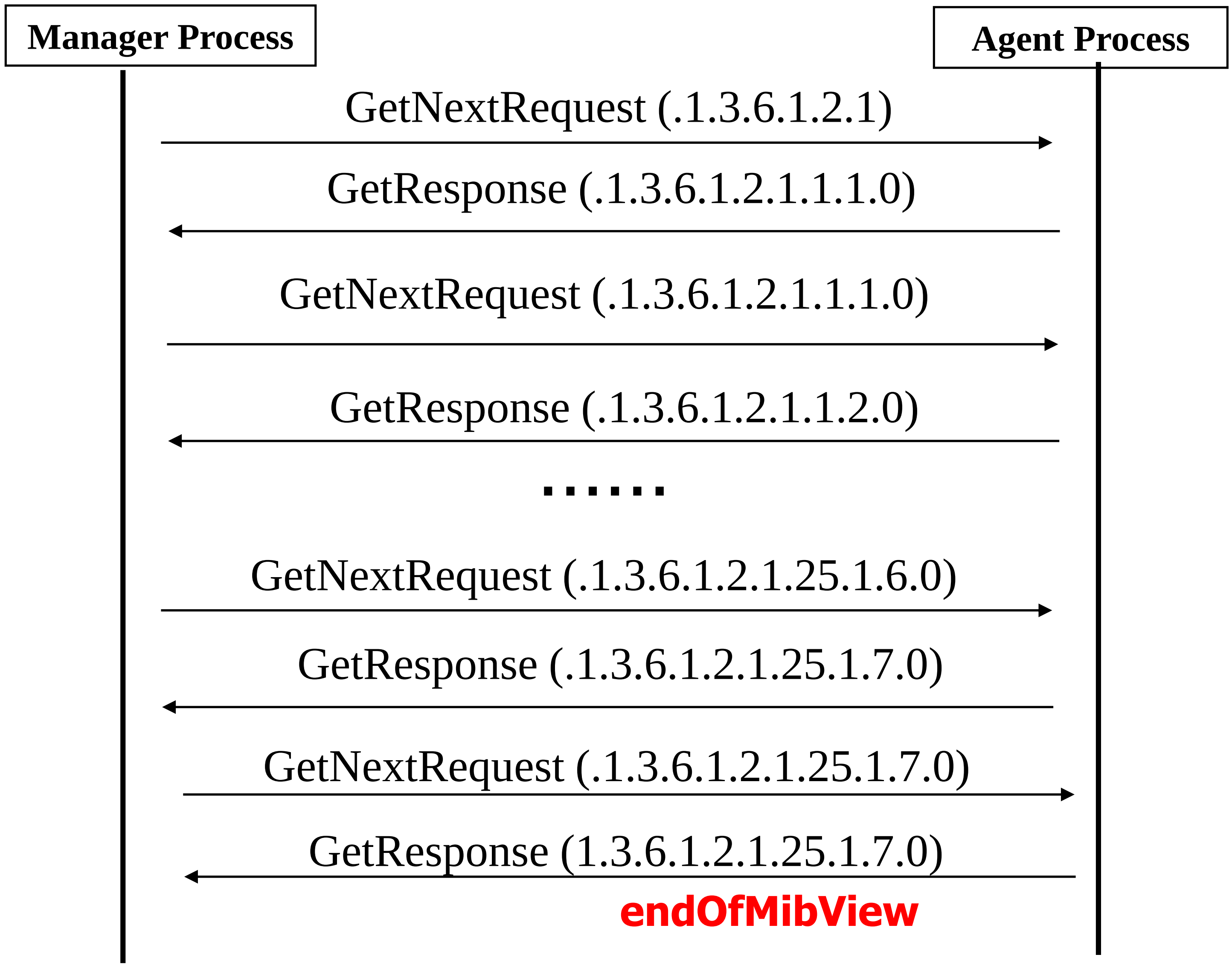
```
student@BUPTIA:~/lab$ sudo snmpwalk -v 2c -c public 127.0.0.1 .1.3.6.1.2.1
iso.3.6.1.2.1.1.1.0 = STRING: "Linux BUPTIA 4.4.0-31-generic #50~14.04.1-Ubu
 Wed Jul 13 01:06:37 UTC 2016 i686"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (397933) 1:06:19.33
iso.3.6.1.2.1.1.4.0 = STRING: "Me <me@example.org>"
iso.3.6.1.2.1.1.5.0 = STRING: "BUPTIA"
iso.3.6.1.2.1.1.6.0 = STRING: "Sitting on the Dock of the Bay"
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.1.8.0 = Timeticks: (2) 0:00:00.02
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.10.3.1.1
```

Object ID of ***MIB***

Refer to RFC3418 for SNMPv2-MIB

```
iso.3.6.1.2.1.1.9.1.4.9 = Timeticks: (2) 0:00:00.02
iso.3.6.1.2.1.1.9.1.4.10 = Timeticks: (2) 0:00:00.02
iso.3.6.1.2.1.25.1.1.0 = Timeticks: (400409) 1:06:44.09
iso.3.6.1.2.1.25.1.2.0 = Hex-STRING: 07 E2 05 0D 10 39 33 00 2B
iso.3.6.1.2.1.25.1.3.0 = INTEGER: 393216
iso.3.6.1.2.1.25.1.4.0 = STRING: "BOOT_IMAGE=/vmlinuz-4.4.0-31-ge
pper/BUPTIA--vg-root ro
"
iso.3.6.1.2.1.25.1.5.0 = Gauge32: 2
iso.3.6.1.2.1.25.1.6.0 = Gauge32: 27
iso.3.6.1.2.1.25.1.7.0 = INTEGER: 0
iso.3.6.1.2.1.25.1.7.0 = No more variables left in this MIB View
```

Corresponding SNMP commands



As captured by wireshark(1)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	127.0.0.1	127.0.0.1	SNMP	82	get-next-request 1.3.6.1.2.1
2	0.000931000	127.0.0.1	127.0.0.1	SNMP	171	get-response 1.3.6.1.2.1.1.1.0
3	0.011073000	127.0.0.1	127.0.0.1	SNMP	85	get-next-request 1.3.6.1.2.1.1.1.0
4	0.011934000	127.0.0.1	127.0.0.1	SNMP	95	get-response 1.3.6.1.2.1.1.2.0
5	0.016460000	127.0.0.1	127.0.0.1	SNMP	85	get-next-request 1.3.6.1.2.1.1.2.0
6	0.017460000	127.0.0.1	127.0.0.1	SNMP	88	get-response 1.3.6.1.2.1.1.3.0
7	0.021872000	127.0.0.1	127.0.0.1	SNMP	85	get-next-request 1.3.6.1.2.1.1.3.0
8	0.022643000	127.0.0.1	127.0.0.1	SNMP	104	get-response 1.3.6.1.2.1.1.4.0
9	0.027523000	127.0.0.1	127.0.0.1	SNMP	85	get-next-request 1.3.6.1.2.1.1.4.0

```
Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
User Datagram Protocol, Src Port: 41935 (41935), Dst Port: snmp (161)
Simple Network Management Protocol
    version: v2c (1)
    community: public
  data: get-next-request (1)
    get-next-request
        request-id: 221841049
        error-status: noError (0)
        error-index: 0
      variable-bindings: 1 item
        1.3.6.1.2.1: Value (Null)
```

As captured by wireshark(2)

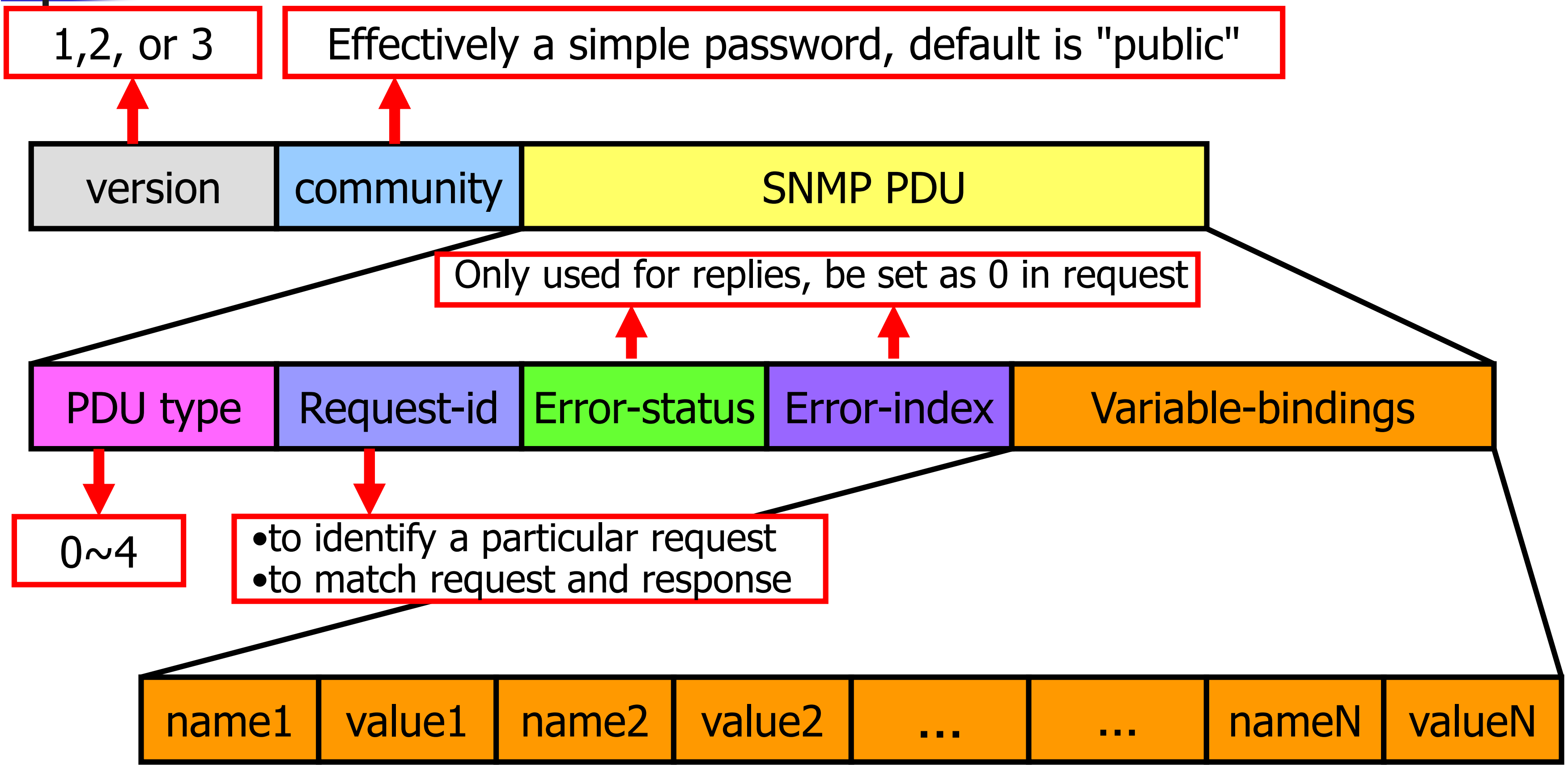
No.	Time	Source	Destination	Protocol	Length	Info
84	0.220940000	127.0.0.1	127.0.0.1	SNMP	159	get-response 1.3.6.1.2.1.25.1.4.0
85	0.230965000	127.0.0.1	127.0.0.1	SNMP	86	get-next-request 1.3.6.1.2.1.25.1.4.0
86	0.232617000	127.0.0.1	127.0.0.1	SNMP	87	get-response 1.3.6.1.2.1.25.1.5.0
87	0.236899000	127.0.0.1	127.0.0.1	SNMP	86	get-next-request 1.3.6.1.2.1.25.1.5.0
88	0.254236000	127.0.0.1	127.0.0.1	SNMP	87	get-response 1.3.6.1.2.1.25.1.6.0
89	0.258494000	127.0.0.1	127.0.0.1	SNMP	86	get-next-request 1.3.6.1.2.1.25.1.6.0
90	0.259883000	127.0.0.1	127.0.0.1	SNMP	87	get-response 1.3.6.1.2.1.25.1.7.0
91	0.263929000	127.0.0.1	127.0.0.1	SNMP	86	get-next-request 1.3.6.1.2.1.25.1.7.0
92	0.264971000	127.0.0.1	127.0.0.1	SNMP	86	get-response 1.3.6.1.2.1.25.1.7.0

```
Frame 92: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
User Datagram Protocol, Src Port: snmp (161), Dst Port: 41935 (41935)
Simple Network Management Protocol
    version: v2c (1)
    community: public
    data: get-response (2)
        get-response
            request-id: 221841094
            error-status: noError (0)
            error-index: 0
            variable-bindings: 1 item
                1.3.6.1.2.1.25.1.7.0: endOfMibView
```

SNMPv3: security and administration

- Encryption
- Authentication
- Protection against playback
- Access control

SNMP Message Format



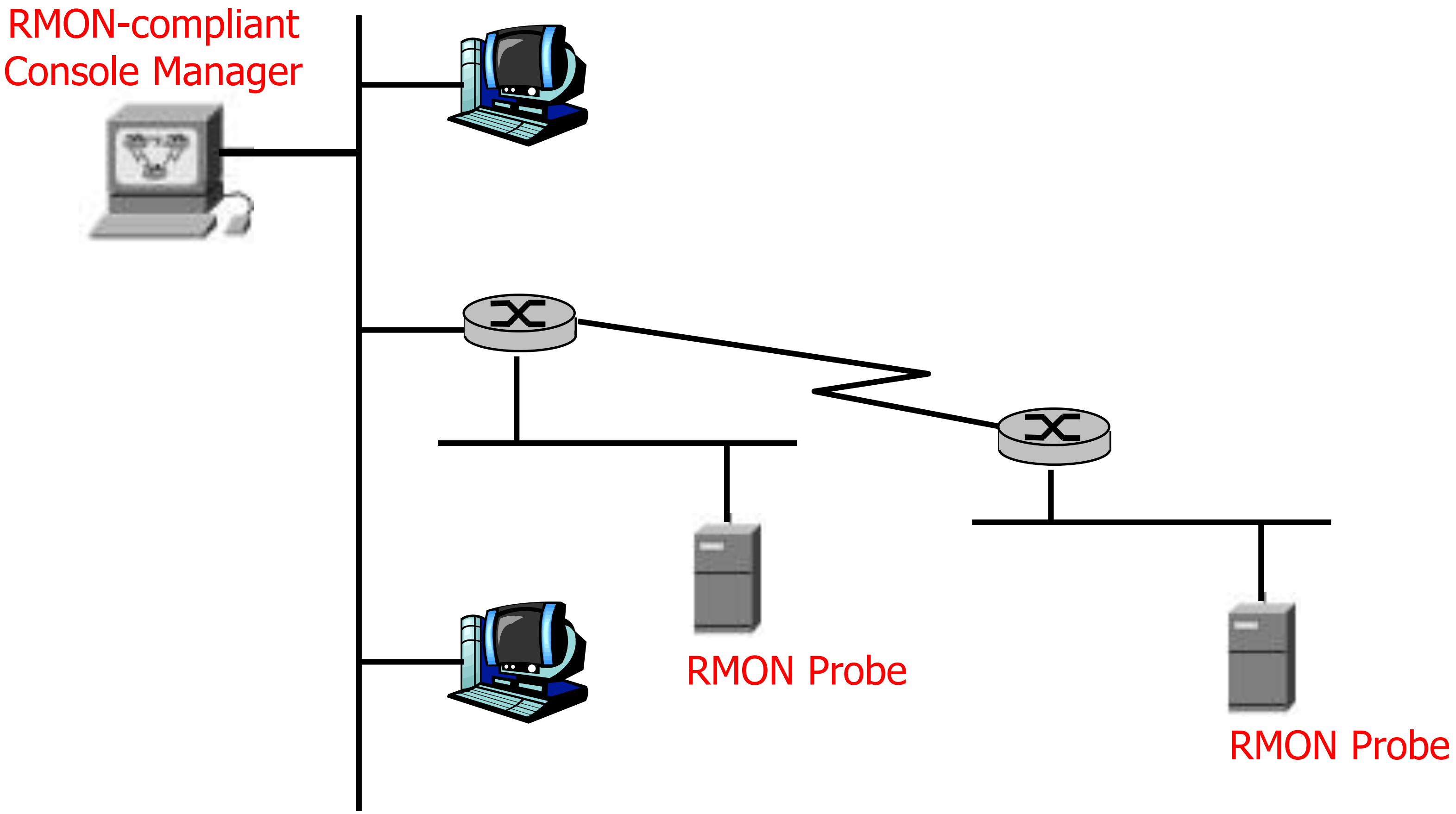
- Trap PDU has different format, see RFCs for more details

RMON (Remote Monitoring)

RMON

- RMON= Remote MONitoring
- Extensions to SNMP provide comprehensive network monitoring capabilities
- RMON uses remote network monitoring devices known as probes. A probe has the same function as a SNMP agent. A probe has RMON capabilities; an agent does not
- The RMON specification defines a set of statistics and functions that can be exchanged between RMON-compliant console managers and probes
- RMON provides standard information to monitor, analyze, and troubleshoot a group of distributed LANs and interconnecting T-1/E-1 and T-2/E-3 lines from a central site.
- RMON specifically defines the information that any network monitoring system will be able to provide as part of the MIB

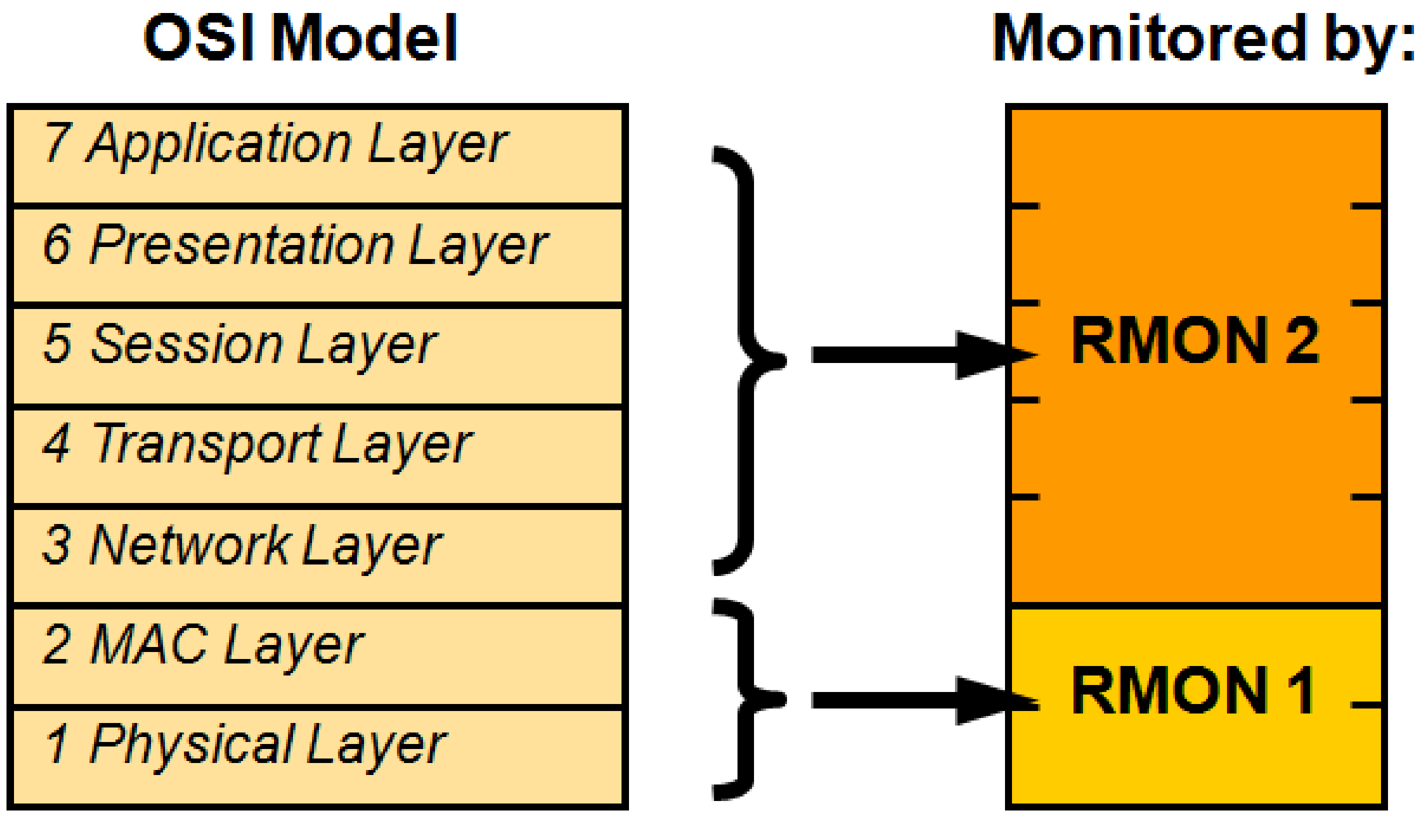
RMON Configuration



RMON – collected information

- RMON collects 9 kinds (groups) of information and alarms can be set in order to be aware of impending problems.
- The 9 groups of RMON are:
  - Statistics, History, Alarm, Host, HostTopN, Matrix, Filter, Packet Capture, Event
- Standardized to only operate on Ethernet segments

Scope of RMON Standards



New Trends Of Network Management

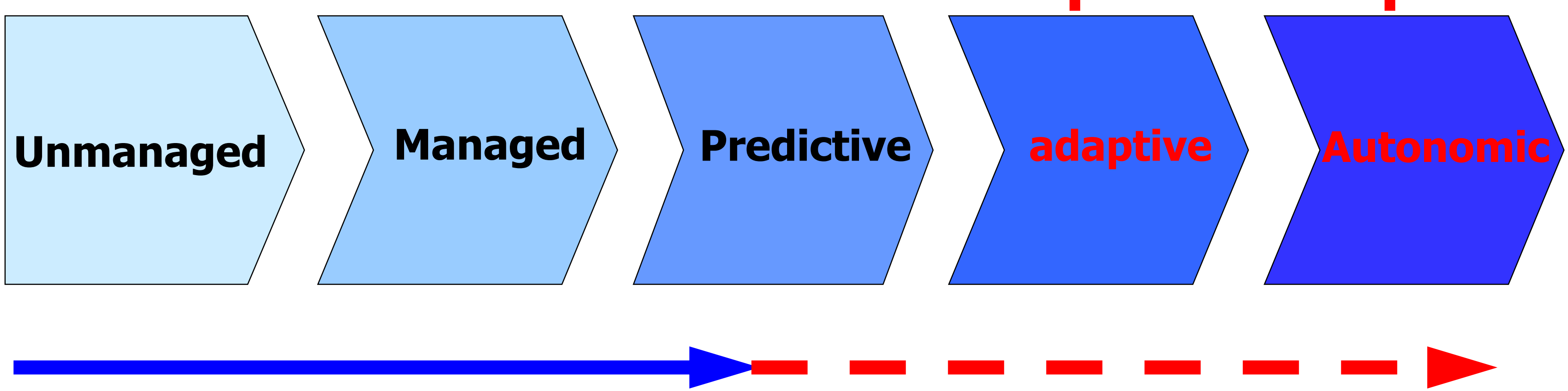
New Trends Of Network Management

- Focus shifting from network management to service management
- Distributed management
- Web-based management
- Policy-based management
- Use of intelligent agents for alarm filtering, alarm correlation, and performance reporting
- Customer-based network/service/SLA management
- Priority-based traffic classification

Key Word: Autonomic

Networks **organize themselves** without much human involvement and explicit management

Networks **adapt** themselves **to changes** in the environment



Summary

Summary

- Terminologies
  - SNMP
  - MIB
  - SMI
  - RMON
- Network management
  - FACPS functional areas defined by ISO
  - Architectures
- SNMP
  - History
  - Features
  - SNMP model and components
- SNMP framework
  - SMI and ASN.1
  - MIB hierarchy naming, definition
  - SNMP protocol: traps/polling, SNMP commands, SNMP message format
- RMON
  - Purpose
  - RMON configuration

Sample Questions

- Define what is meant by Network Management and describe the pros and cons of using a distributed architecture for network management?
- According to the International Standards Organisation (ISO) Network Management Forum, what are the five functional components of network management? For each type, provide a brief description of the activities associated with that function.
- What are the key components and structure of an Simple Network Management Protocol (SNMP) architecture?
- What are the five basic commands of SNMP and what is their function?
- Explain the two approaches by which information can be obtained from monitored network devices. What are the pros and cons of each approach?
- Briefly explain the purpose of the Remote Network Monitoring (RMON) protocol.

Useful URLs

- RFCs
  - http://www.ietf.org/
- Basic introduction to network management and SNMP
  - http://www.dpstele.com/snmp/tutorial-what-is.php
- OID assignments
  - http://www.alvestrand.no//objectid/top.html
- RMON
  - https://tools.ietf.org/html/rfc3577

Abbreviations

ASN.1	Abstract Syntax Notation One
ME	Managed Entity
MIB	Management Information Base
NMS	Network Management System
OID	Object IDentifier
PDU	Packet Data Unit
RMON	Remote MONitoring
SMI	Structure of Management Information
SNMP	Simple Network Management Protocol