



UNIVERSITY OF M'SILA
FACULTY OF MATHEMATICS AND COMPUTER SCIENCE
Computer Science Department

Network Administration and Security

Prepared by:

- **Ms. SAOUDI Lalia**

Master 2 RTIC: 2025/2026

Course Outline

Introduction to network administration: Areas of activity, Architectures and administration models , Network administration tools

2 Network administration protocols (SNMP, CMIP)

3 Introduction to cyber security

4 Vulnerability audit (vulnerability scanner)

5 Penetration test

6 different network attacks

7 firewalls

8 Intrusion detection systems

9 Security protocols

10 Virtual Private Networks VPN)

Introduction

What is network administration?

Network administration involves controlling, coordinating, and monitoring the various resources implemented to provide operational services to users. these resources include equipment, network, services offered by various servers, applications, Internet, etc...

Example:

- access to shared data and computing resources (databases, directories, software, etc.)
- browsing websites;
- A shared printer

Introduction

- Areas of activity (according to OSI): In 1988, the organisation published the ISO7498/4 standard defining the main functions that supervision and administration systems must implement.

Fault management

Accounting management

Configuration management

Performance Audit

Security management

Areas of activity

1. Performance Management

- Performance management continuously analyses the network's performance to maintain it in an acceptable state of performance. This management occurs in three stages:
 1. variables containing meaningful information regarding network performance are collected. (response time, traffic, etc.).
 2. Once these variables are obtained, they are analysed.
 3. If they exceed a previously set performance threshold, an alarm is immediately sent to the network administrator to resolve the issue as quickly as possible

Areas of activity

2. Configuration Management

- Configuration management monitors the various configurations of the elements present on the network. It stores in a database the versions of operating systems and software installed on each machine in the network environment
 - Resource Identification
 - Installation, initialisation,
 - configuration,
 - reconfiguration.
 - Collection of useful information and saving of a history

Areas of activity

3 Accounting management

- The purpose of accounting management is to measure resource usage in order to regulate access and establish a degree of fairness among network users.
- Thus, usage quotas may be set, either temporarily or permanently, on each of the network resources.
- Furthermore, accounting management allows for the implementation of billing systems based on usage for each user.

Areas of activity

4. Fault management:

- Fault management detects network problems (software or hardware). It automatically resolves the anomaly. If not, it alerts the individuals concerned with the type of problem to seek their intervention.
- Detection,
- localisation,
- isolation,
- repair

Areas of activity

5. Security management:

Goal: to protect network resources and the administration system.

How: To ensure security services(authentication, confidentiality, integrity, availability, and non-repudiation).

Means:

- cryptography.
- supervision software.
- audit
- firewall.
- monitoring of event logs.
 - Security log
 - System log
 - Application log

Administration models

Administration can be viewed through 4 models (according to ISO):

Organizational model

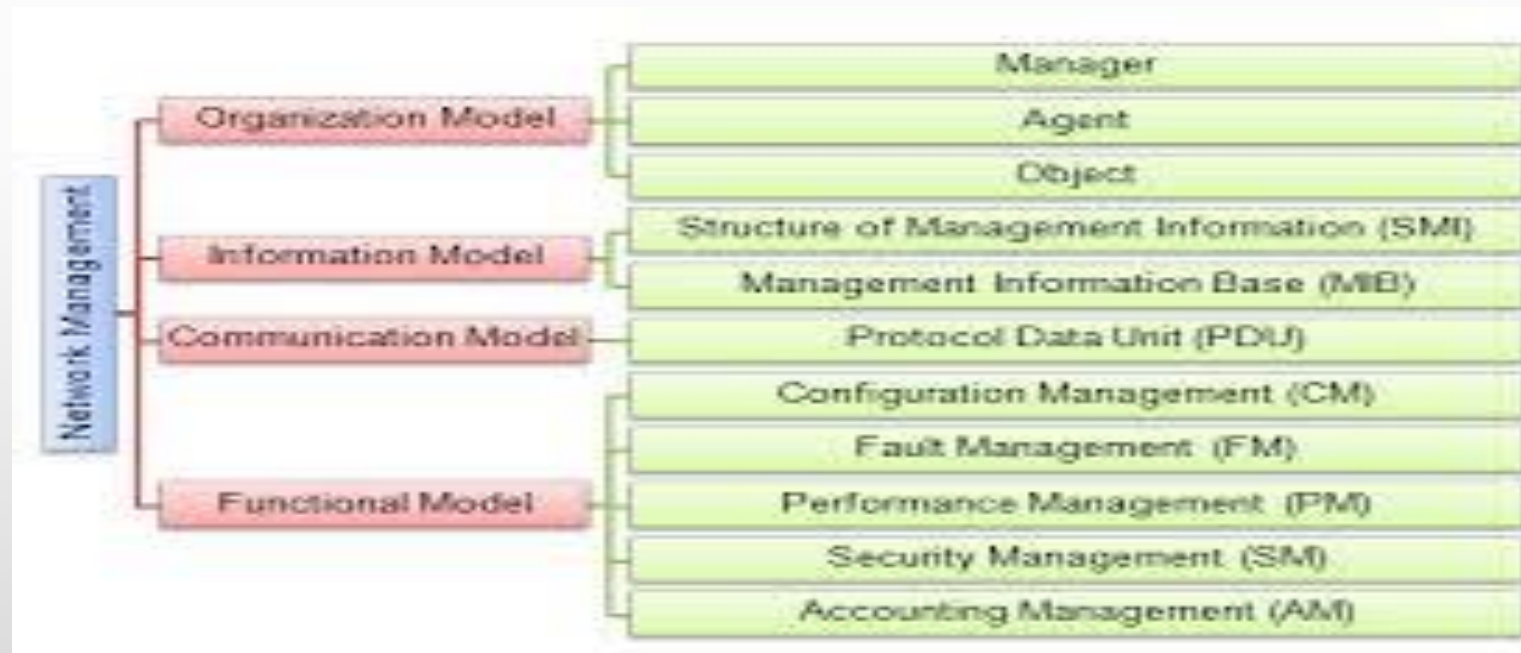
Functional model

Information model

Communication model

Administration models

Administration can be viewed through 4 models (according to ISO):



Administration models

1. Organisational model:

The organisational model describes the components of a network management system, their functions, and their infrastructure. The organisational model defines the terms object, agent, and manager, and their relationships.

- A domain can comprise several agents/managers.
- An agent/manager can be shared among several domains.

Cooperative and distributed management system.

Why an administration domain?

- scalability,
- security,
- administrative autonomy

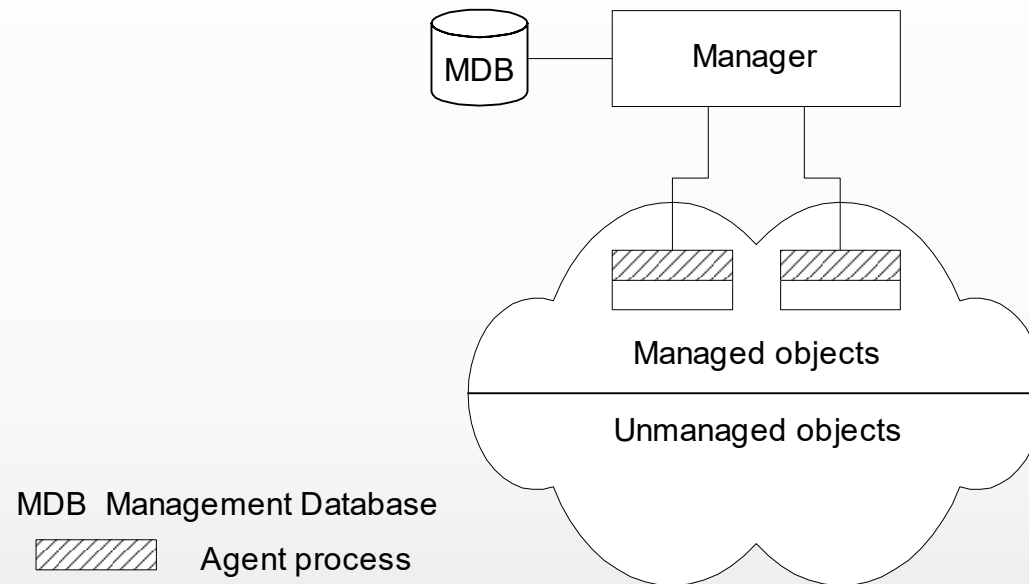
Management models

1. Organisational model:

- Manager
 - Sends requests to agents
 - Monitors alarms
 - Houses applications
 - Provides user interface
- Agent
 - Gathers information from objects
 - Configures parameters of objects
 - Responds to managers' requests
 - Generates alarms and sends them to managers
- Managed object
 - Network element that is managed
 - Houses management agent

Management models

1. Organisational model: Two-level model

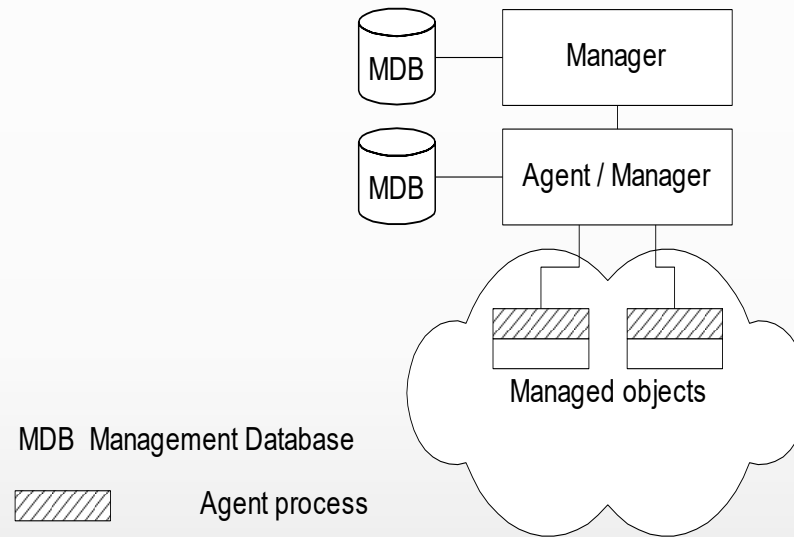


- Agent built into network element Example: Managed
- An agent can manage multiple elements Example: Sw
- MDB is a physical database
- Unmanaged objects are network elements that are no

Figure 3.2 Two-Tier Network Management Organization Model

Management models

1. Organisational model: Three-level model

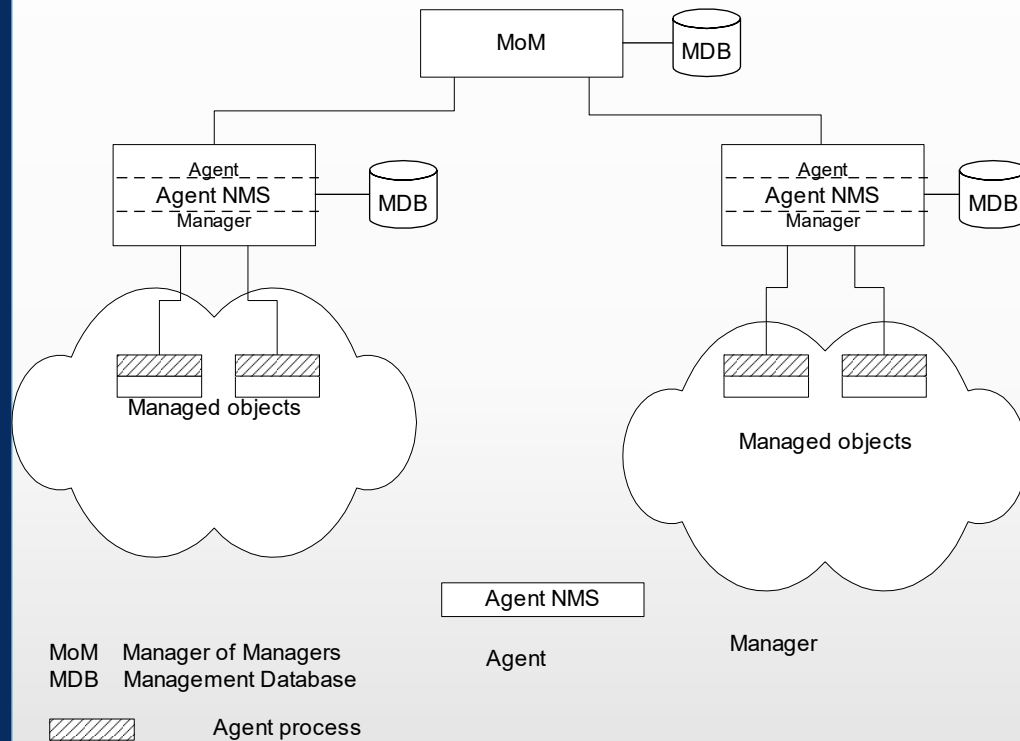


- Middle layer plays the dual role
 - Agent to the top-level manager
 - Manager to the managed objects
- Example of middle level: Remote monitoring agent

Figure 3.3 Three-Tier Network Management Organization Model

Management models

1. Organisational model: Manager of managers



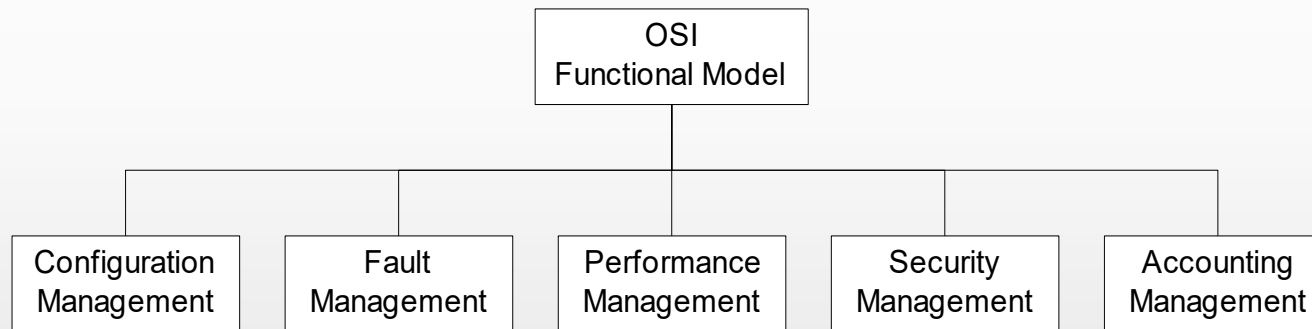
- Agent NMS manages the domain
- MoM presents integrated view of domains
- Domain may be geographical, administrative, vendor

Figure 3.4 Network Management Organization Model with MoM

Management models

2. Functional model (SMFA 'Specific Management Functional Areas')

concerning network management applications that reside on the network management station (NMS). The OSI management model consists of five domains:



This network management model has been widely adopted by manufacturers as a useful method for describing the needs of any network management system.

Management Models

3. SMI Model 'Structure of Management Information'

This model relates to the structure and storage of network management information.

This information is stored in a database called the Management Information Base (MIB).

ISO established the structure of management information (SMI) to define the syntax and semantics of the management information stored in the MIB. MIBs and SMIs are studied in detail later.

Management Models

3. SMI Model 'Structure of Management Information'

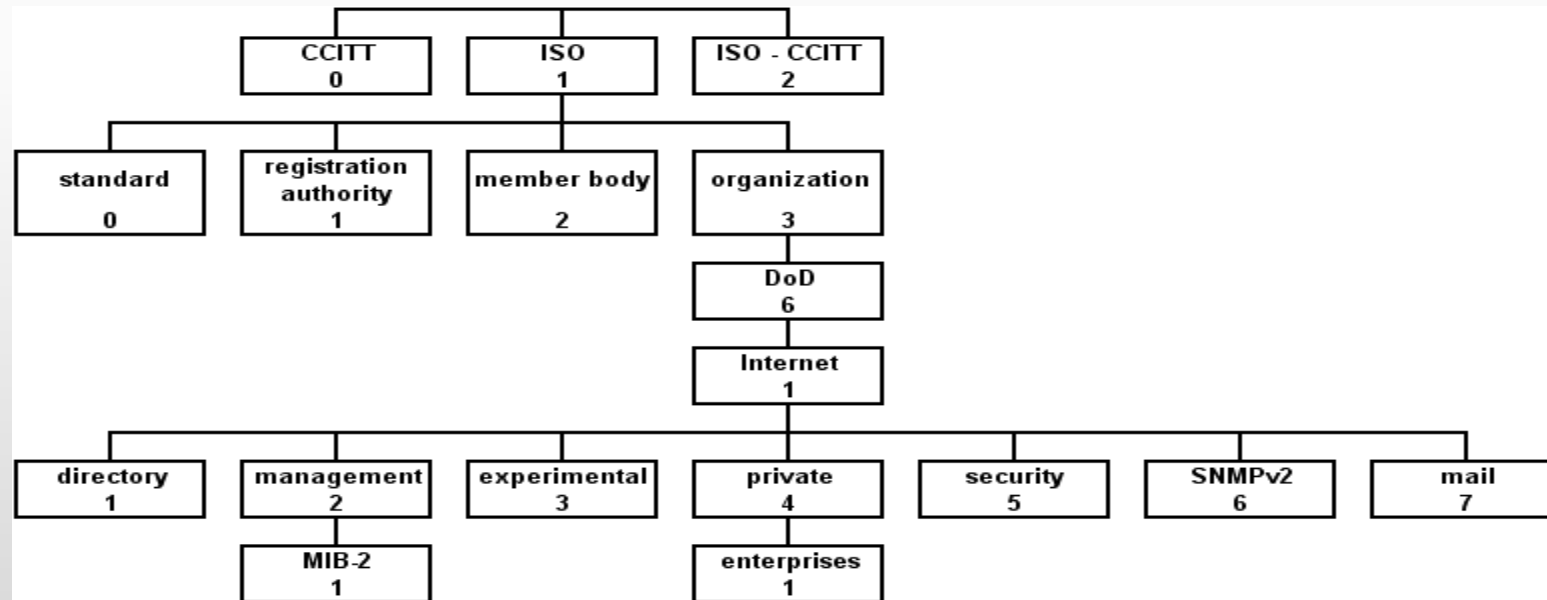
MIB: A MIB (Management Information Base) is a structured set of information about a network entity, such as a router, switch, or server. This information can be retrieved, or sometimes modified, using the SNMP protocol. The structure of the MIB is hierarchical: the information is grouped in a tree. Each piece of information has an object identifier, a sequence of numbers separated by dots, which uniquely identifies it and a name, specified in the document that describes the MIB.

Management Models

3. SMI Model 'Structure of Management Information'

Example: For instance, 1.3.6.1.2.1.2.2.1.2 is the object identifier

Nominal: iso.org.dod.internet.mgmt.mib-2.ip.ipInReceives *Numeric:* 1.3.6.1.2.1.4.3



Management Models

Managed objects:

- Managed objects can be
 - Network elements (hardware, system)
 - switch, routers, transmission facilities
 - Software (non-physical)
 - programs, algorithms
 - Administrative information
 - contact person, name of group of objects (IP group)

Administration models

4. Communication model:

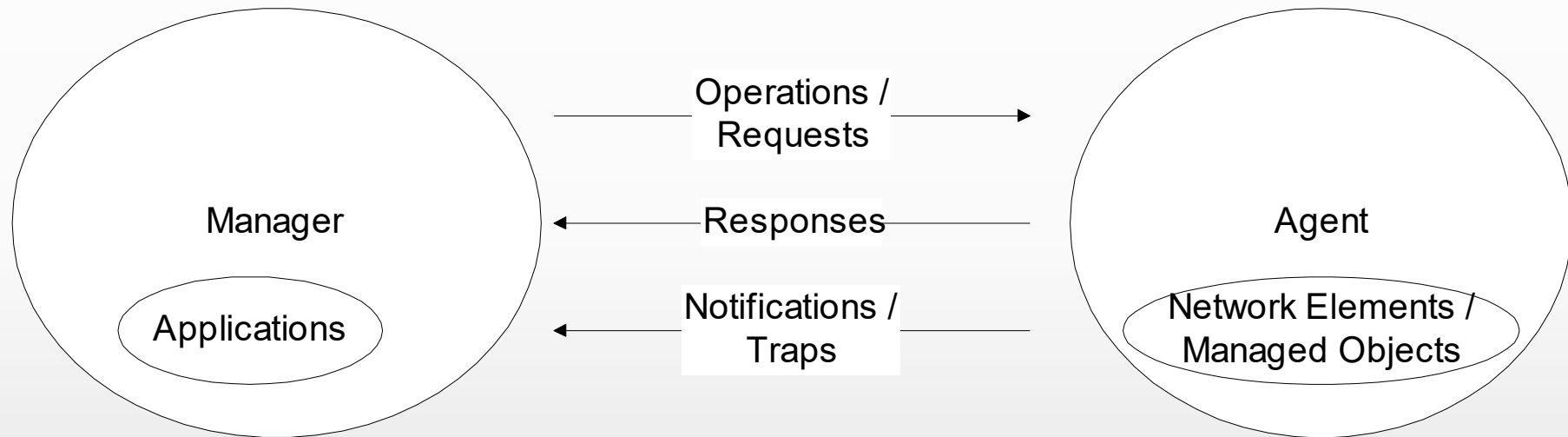


Figure 3.11 Management Message Communication Model

Administration models

4. Communication model (transfer protocol):

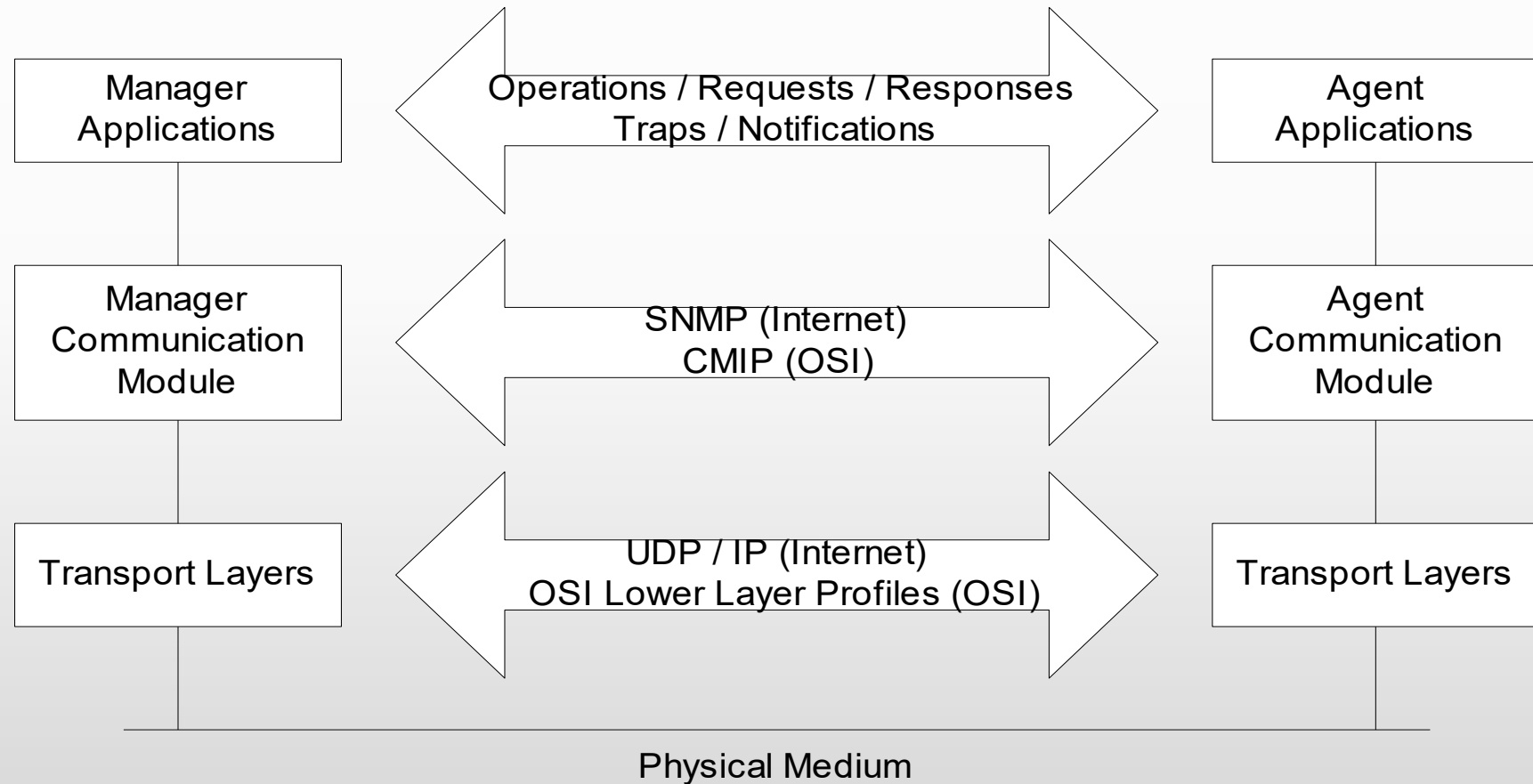


Figure 3.12 Management Communication Transfer Protocols

Standards

Why standards?

To use them across a wide range of products (terminals, bridges, routers, etc.) and in a multi-vendor environment.

- Families of standards
- Internet Network Management Framework (IETF)
 - SNMPv1, SNMPv2, SNMPv3
- OSI Network Management Framework (ISO/ITU-T)
 - CMISE/CMIP: Common Management Information Service Element / CMI Protocol
- Telecommunication Management Network (ITU-T)
 - TMN (M.3000 Series)
- Distributed Management Task Force (DMTF)
 - DMI, CIM, WBEM

Standards

Table 3.1 Network Management Standards

Standard	Salient Points
OSI / CMIP	■ International standard (ISO / OSI) ■ Management of data communications network - LAN and WAN ■ Deals with all 7 layers ■ Most complete ■ Object oriented ■ Well structured and layered ■ Consumes large resource in implementation
SNMP / Internet	■ Industry standard (IETF) ■ Originally intended for management of Internet components, currently adopted for WAN and telecommunication systems ■ Easy to implement ■ Most widely implemented
TMN	■ International standard (ITU-T) ■ Management of telecommunications network ■ Based on OSI network management framework ■ Addresses both network and administrative aspects of management
IEEE	■ IEEE standards adopted internationally ■ Addresses LAN and MAN management ■ Adopts OSI standards significantly ■ Deals with first two layers of OSI RM
Web-based Management	■ Web-Based Enterprise Management (WBEM) ■ Java Management Application Program Interface (JMAPI)

Network monitoring software

A network management system is a collection of tools to

- observe and track the status of network resources
- control the network by modifying its operating parameters
- A process running continuously in the background.
- Dynamic consideration of
 - The emergence of new nodes.
 - The disappearance of certain others

Network monitoring software

Several management software options available:

Commercial:

- HP openView
- IBM NetView/6000
- SunSoft Solstice
- Bull ISM

OpenSource

- NetXMS
- Pandora FMS
- Cacti
- Zabbix
- Nagios
- OpenNMS

Nagios

The best way to describe Nagios is as the grandfather of network monitoring as it has been around for so long. In fact, the company behind Nagios refers to it as the 'Industry Standard in IT Infrastructure Monitoring.'

Nagios

Some features of Nagios

- Monitoring network services such as: SMTP, HTTP, FTP, SSH, etc.
- Monitoring machine resources such as: CPU load, Disk space usage, Memory usage, etc.
- Automatic log file rotation
- Optional Web interface for viewing the current status of the network, log file notifications
- Design of simple plugins allowing users to develop their own service checks;
- Notification by email or SMS when an issue occurs with a service or machine;
- Proactive problem resolution;
- Etc...

Pandora FMS

Pandora FMS (Flexible Monitoring System) is monitoring software for general purposes

Pandora FMS allows measuring the state of:

- ✓ Systems/Servers.
- ✓ WEB Applications.
- ✓ Communications
- ✓ Applications (Unix/Windows).
- ✓ Power consumption, temperature...
- ✓ Business applications

Course questions1

- *Q1: why perform network administration?
- *Q2: What are the main functions that administration systems must implement?
- *Q3: Name the 4 models (according to ISO) of network administration,
- *Q4: What is the administration model that includes the 5 activity domains,
- *Q5: What is the role of the agent and the manager,
- *Q6: What is a MIB base
- *Q7: What are the objects to be managed
- *Q8: Why use standard administration protocols