Управление на мрежите

Христо Вълчанов
Технически Университет - Варна

Управление на мрежата

- Управление на мрежата (Network Management) - управление на мрежови ресурси:
  - Устройства - hubs, switches, routers
  - Връзки - по различна преносна среда
- Управление на мрежата (OAM&P):
  - Операции (Operations)
  - Администриране (Administration)
  - Поддръжка (Maintenance)
  - Обезпечаване (Provisioning)
- Управление на системата (System Management) - управление на системи и системни ресурси в мрежата

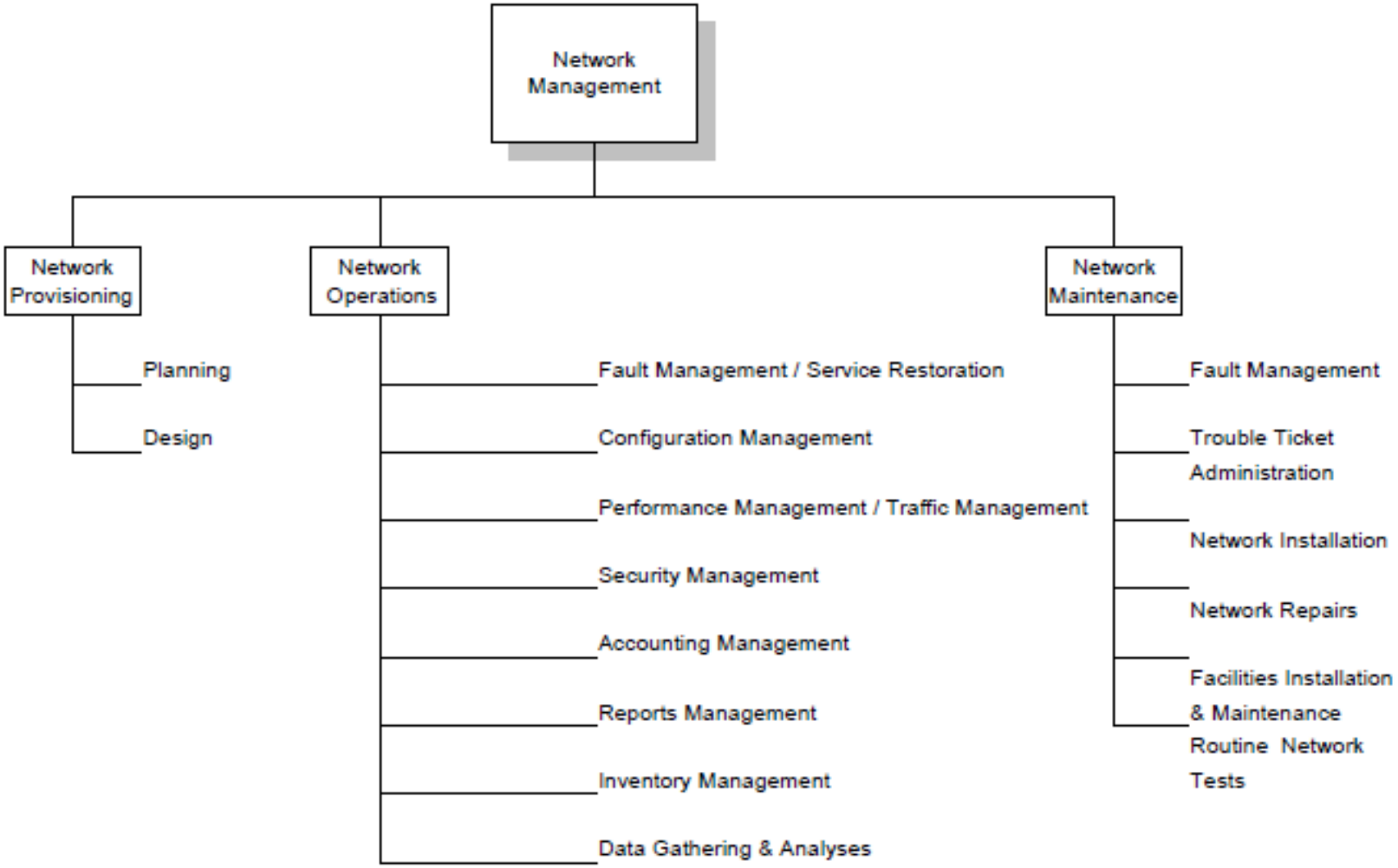
Възможни проблеми

- Загуба на свързаност
- Дублиране на IP адреси
- Временни проблеми
- Свързани с конфигуриране на мрежови настройки
- Влошаване на производителността

Стандарти

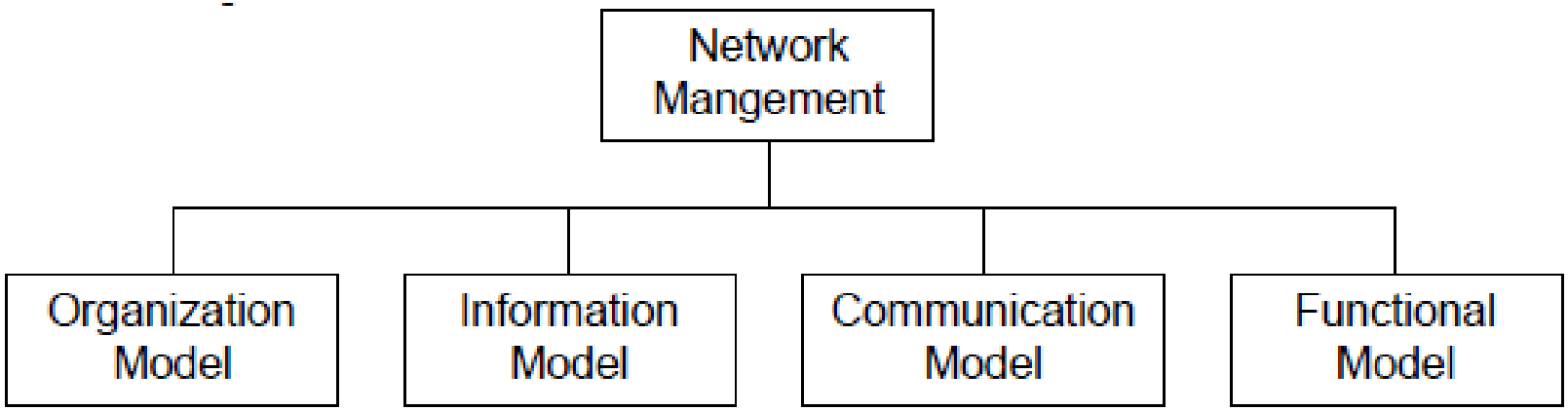
- OSI – Common Management Information Protocol (CMIP)
- IETF – Simple Network Management Protocol (SNMP) е най-често използван
- ITU-T – Telecommunications Management Network (TMN)
- IEEE standards
- Web-based Management

Функционални групи



Модел на мрежово управление

- OSI – Common Management Information Protocol (CMIP)



- SNMP
  - Не е дефиниран ясно
  - Първите 3 модела са подобни на OSI модела
  - Функционалният модел е свързан с операции, администриране и сигурност

Организационен модел

Описва компонентите на мрежата и тяхната взаимна връзка.

Дефинира 3 понятия:

- Менажер
- Агент
- Управляван обект

Организационен модел

Менажер

- Софтуер, чрез който се управляват обектите
- Изпраща заявки към обектите и получава информация за тях
- Наблюдават се аларми
- Поддържа приложения
- Предлага потребителски интерфейс

Организационен модел

Агент

- Събира информация от обектите
- Конфигурира параметрите от обектите
- Отговаря на заявки от менажера
- Генерира аларми и ги изпраща на менажера

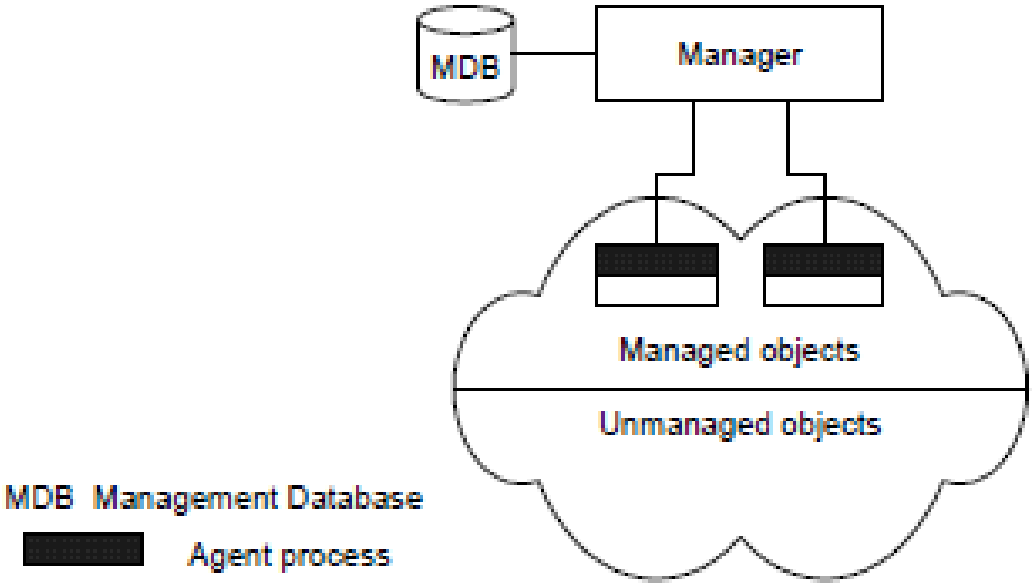
Организационен модел

Управляван обект

- Мрежов елемент, който се управлява
- Върху него се изпълнява агента
- Той е управляем/неуправляем

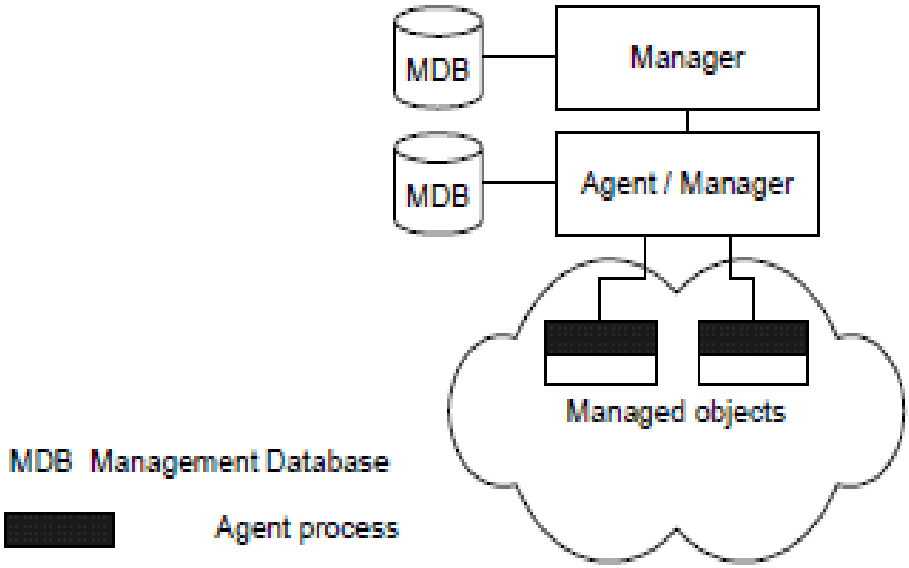
Дву-слоен модел

- **MDB** – физическа БД за управление
- **Agent** – във всеки обект (хъб, рутер)
- **Manager** – управлява елементите (комутатори)
- **Unmanaged** objects – мрежови елементи, които не се управляват – и физически (unmanaged hub) и логически (пасивни елементи)

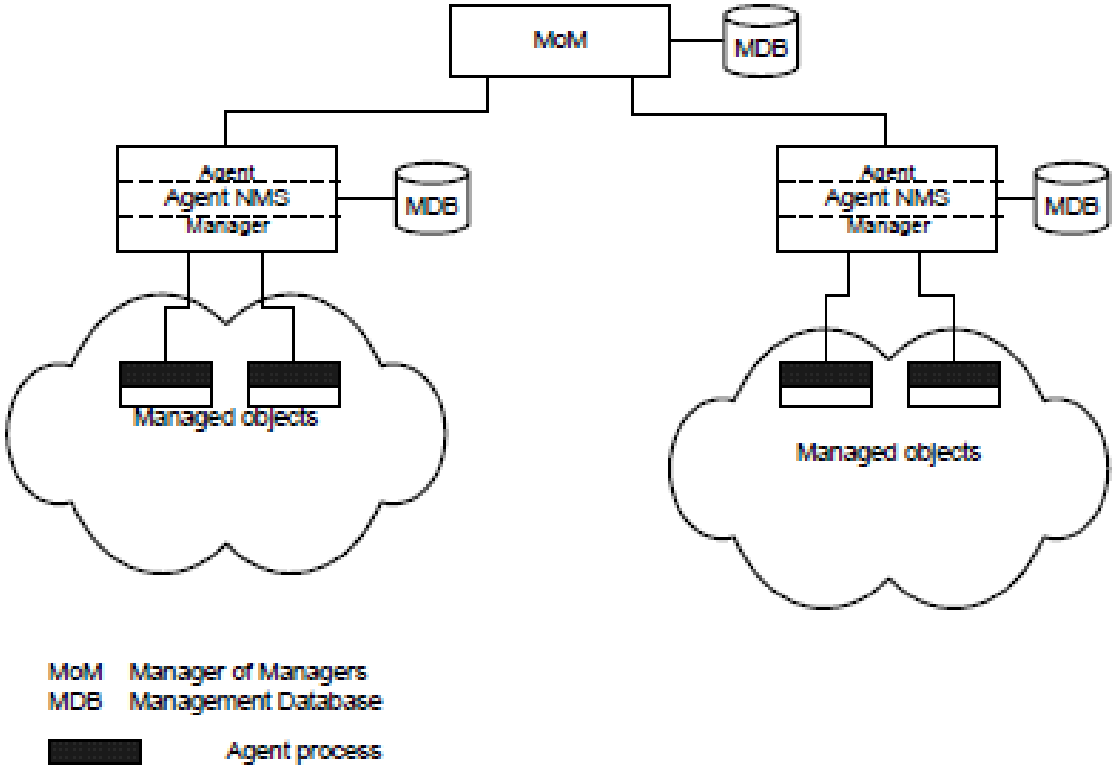


Три-слоен модел

- Междинният слой има двойна роля:
  - Agent за слой 1
  - Manager за слой 3
- Пример за междинен слой: Remote monitoring probe/agent (RMON)
- Поддръжка на статистика

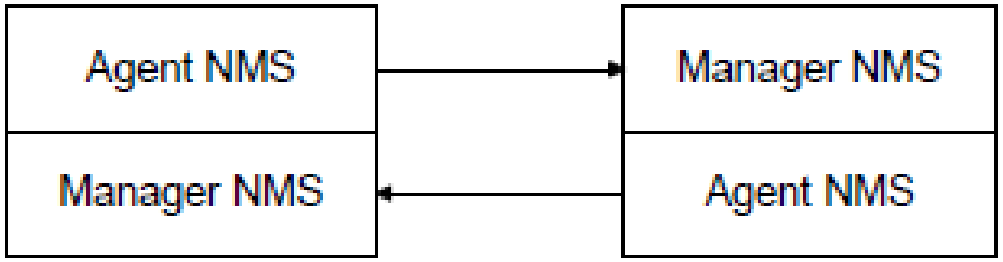


Модел Manager of Managers



- За големи по размер мрежи
- Дава възможност за разглеждане по домейни – географски, административни, производители и др.

Peer модел



- И двете системи работят равноправно (peers)
- Мениджърите и агентите се изпълняват като процеси
- Пример: обмен на информация за управление между два ISP

Информационен модел

- Занимава се с структурата и съхраняването на информация.
- Задава информационната база, за описания на управляваните обекти и техните взаимоотношения
- Структурата на управляваната информация (SMI) дефинира за управлявания обект:
  - Синтаксис
  - Семантика
  - Статус

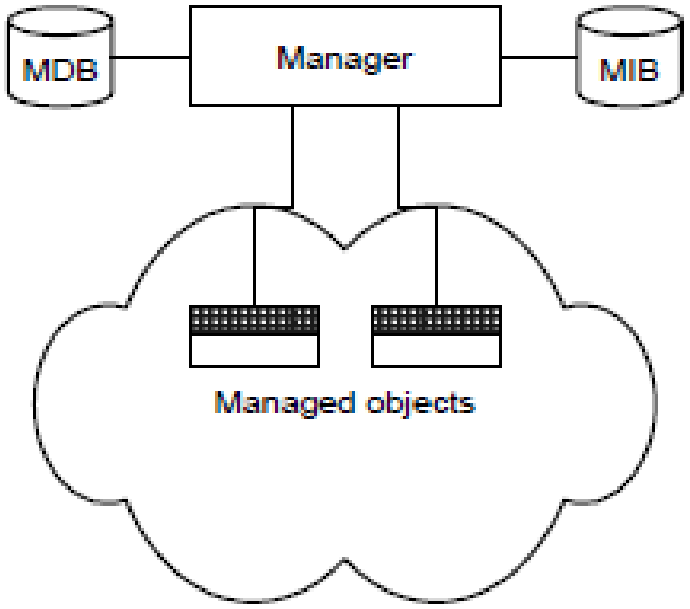
Информационен модел

- Пример за описание на обект:

```
sysDescr: { system 1 }
Syntax: OCTET STRING
Definition: "A textual description of the
entity."
Access: read-only
Status: mandatory
```

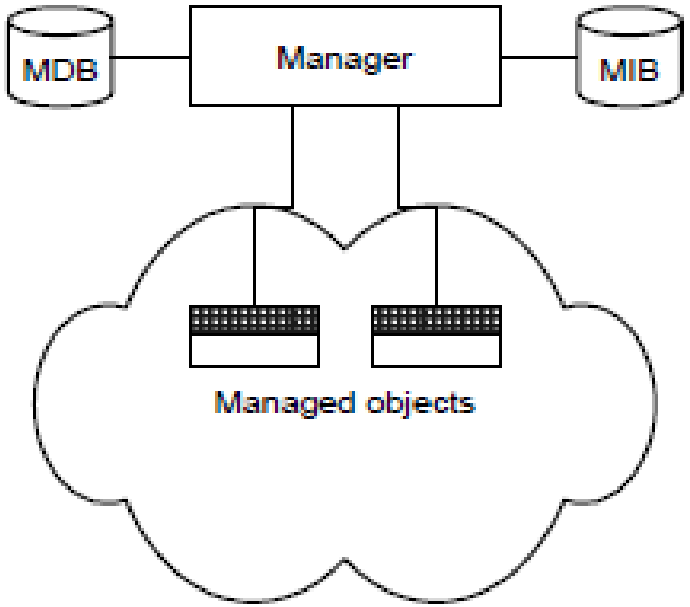
MIB

- Management Information Base (MIB)
  - Съдържа информация за обектите
  - Организирана е по групи от свързани обекти
  - Дефинира връзките между обектите
  - Не е физическа, а е виртуална и се компилира в управляващия софтуер
  - Системата за управление може да идентифицира новия обект (например хъб) само след като MIB е компилирана в управляващия софтуер

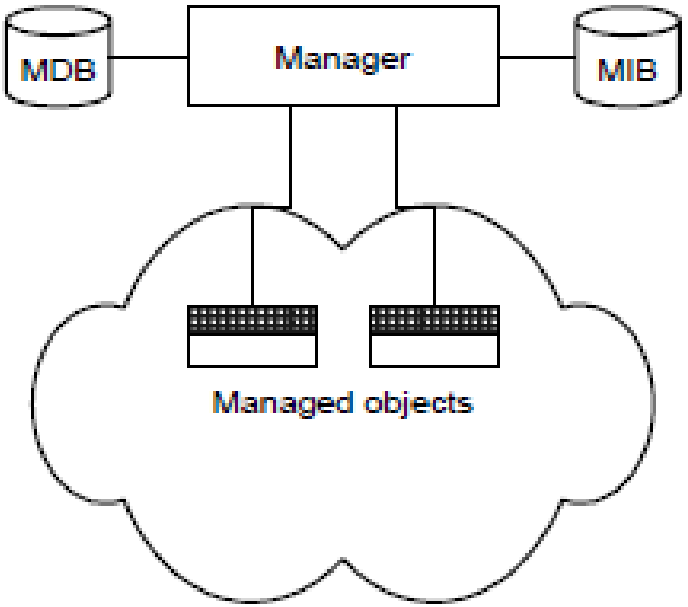


MIB view

- MIB view и достъп до обект:
  - Управлявания обект има много атрибути – информационната база
  - Върху обект могат да се извършат много операции
  - Менажерът може да види и изпълни определени операции чрез извикване на агент
  - Изгледът (view) на атрибутите е MIB view
  - Операциите, които могат да се извършат са MIB access



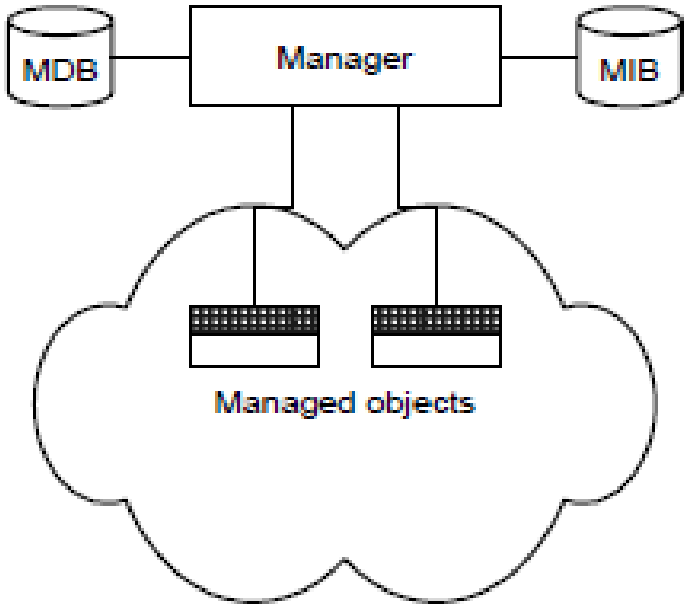
Management Database



- Management Database:
  - MDS е физическа БД (Oracle, Sybase)
  - MIB е виртуална, компилирана с софтуера за управление

Управлявани обекти в MIB

- Мрежови елементи – хъбове, рутери, комутатори
- Софтуер – програми, алгоритми
- Административна информация – лице за контакти, име на група от обекти (IP група)



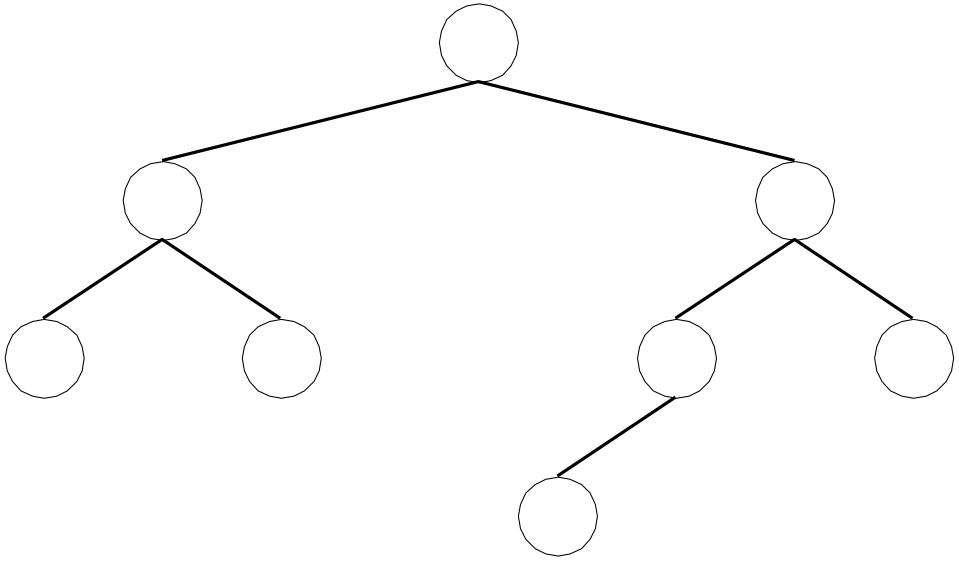
Management Information Tree

Root

Level 1

Level 2

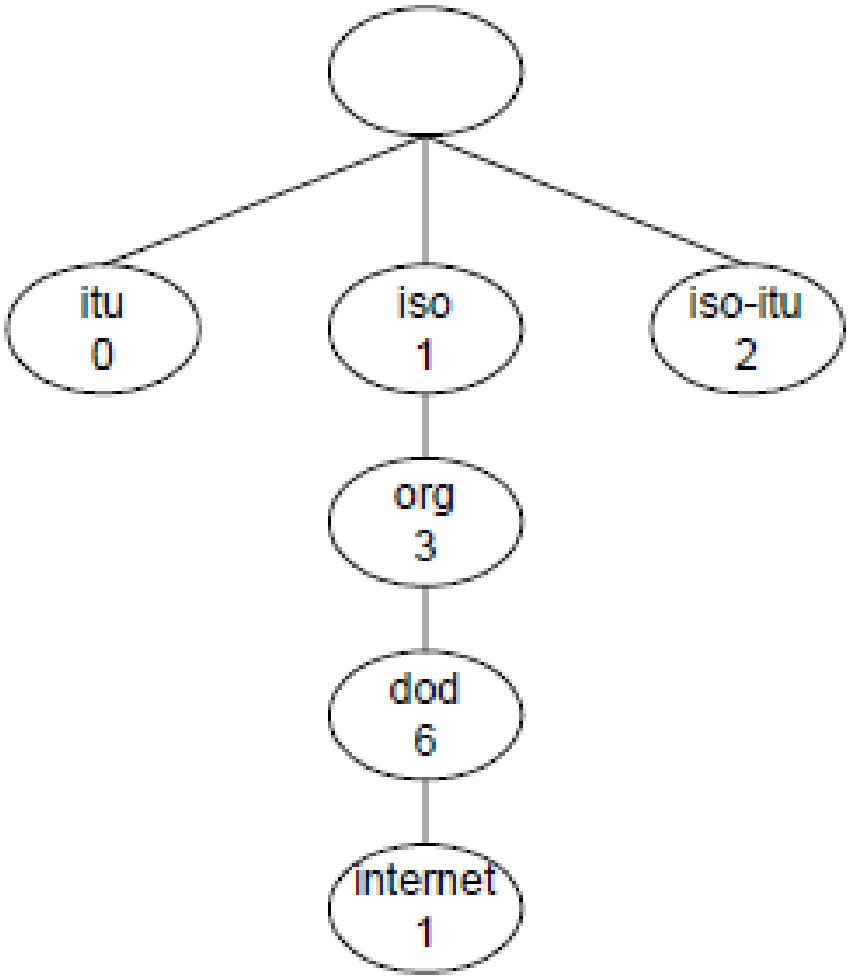
Level 3



- Управляваните обекти са еднозначно определени от дървовидна структура (MIT), дефинирана от OSI модела
- Всеки възел е управляван обект

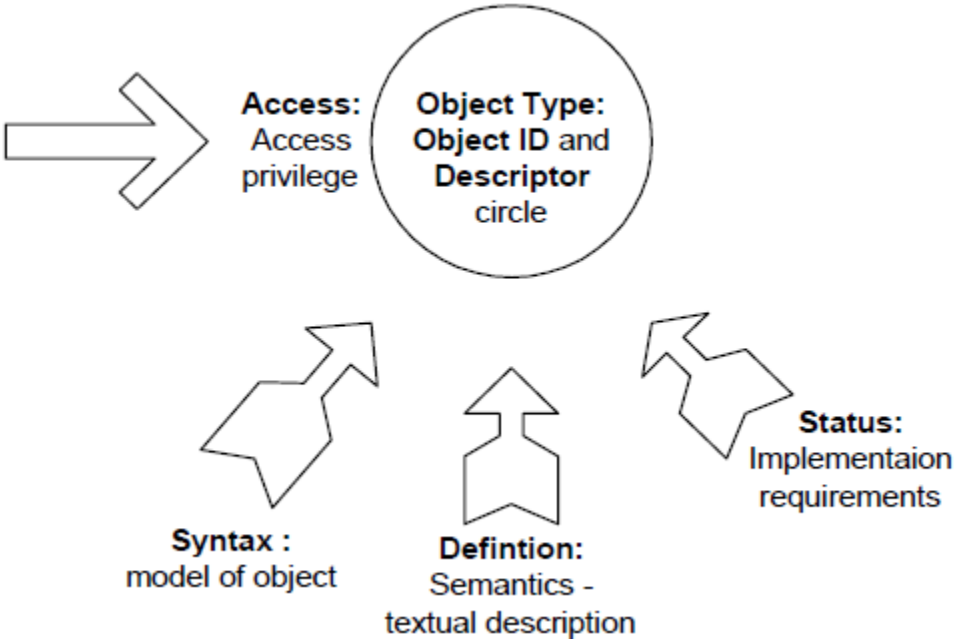
OSI Management Information Tree

- iso 1
- org 1.3
- dod 1.3.6
- internet 1.3.6.1



Обекти – Интернет перспектива

Характеристика	Значение
object ID	Уникален идентификатор
descriptor	Име на обект
syntax	Използва се за моделиране на обекта
access	Привилегии на достъп до обекта
status	Изисквания на реализацията
definition	Текстово описание на семантиката на обекта

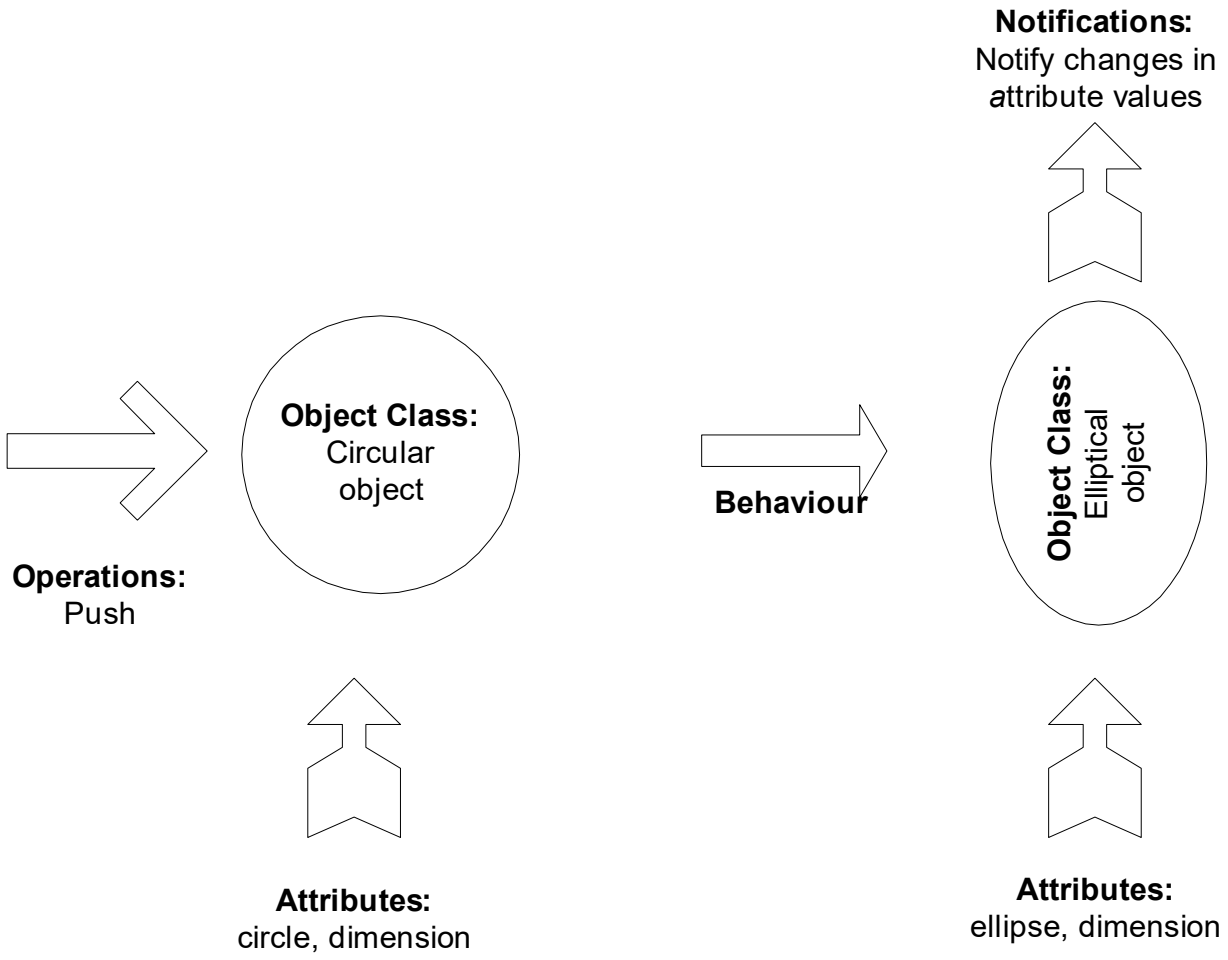


Обекти – Интернет перспектива

Интернет спецификация на обект „Packet Counter”:

Характеристика	Пример
Object type	PktCounter
Syntax	Counter
Access	Read-only
Status	Mandatory
Description	Counts number of packets

Обекти – OSI перспектива



Обекти – OSI перспектива

Характеристика	Значение
object class	Управлявания обект
attributes	Атрибути
operations	Действия, които могат да се прилагат върху обекта
behavior	Поведение на обекта в отговор на операцията
notifications	Съобщения, издадени от обекта

Обекти – OSI перспектива

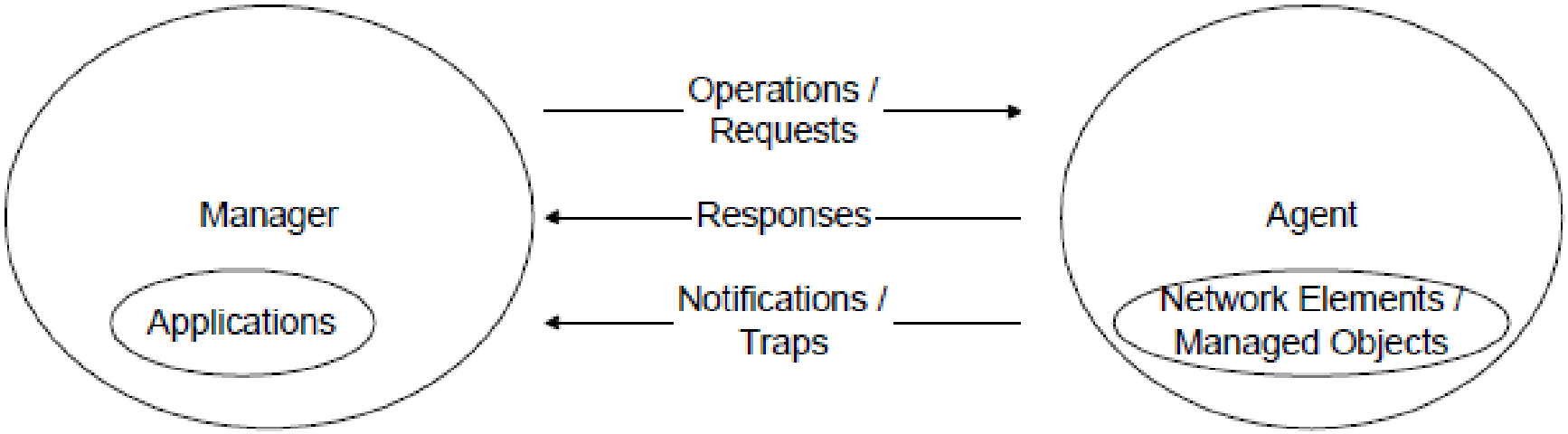
OSI спецификация на обект „Packet Counter”:

Характеристика	Пример
Object class	Packet Counter
Attributes	Single-valued
Operations	get, set
Behavior	Retrieves or resets values
Notifications	Generates notifications on new value

Интернет – OSI обекти

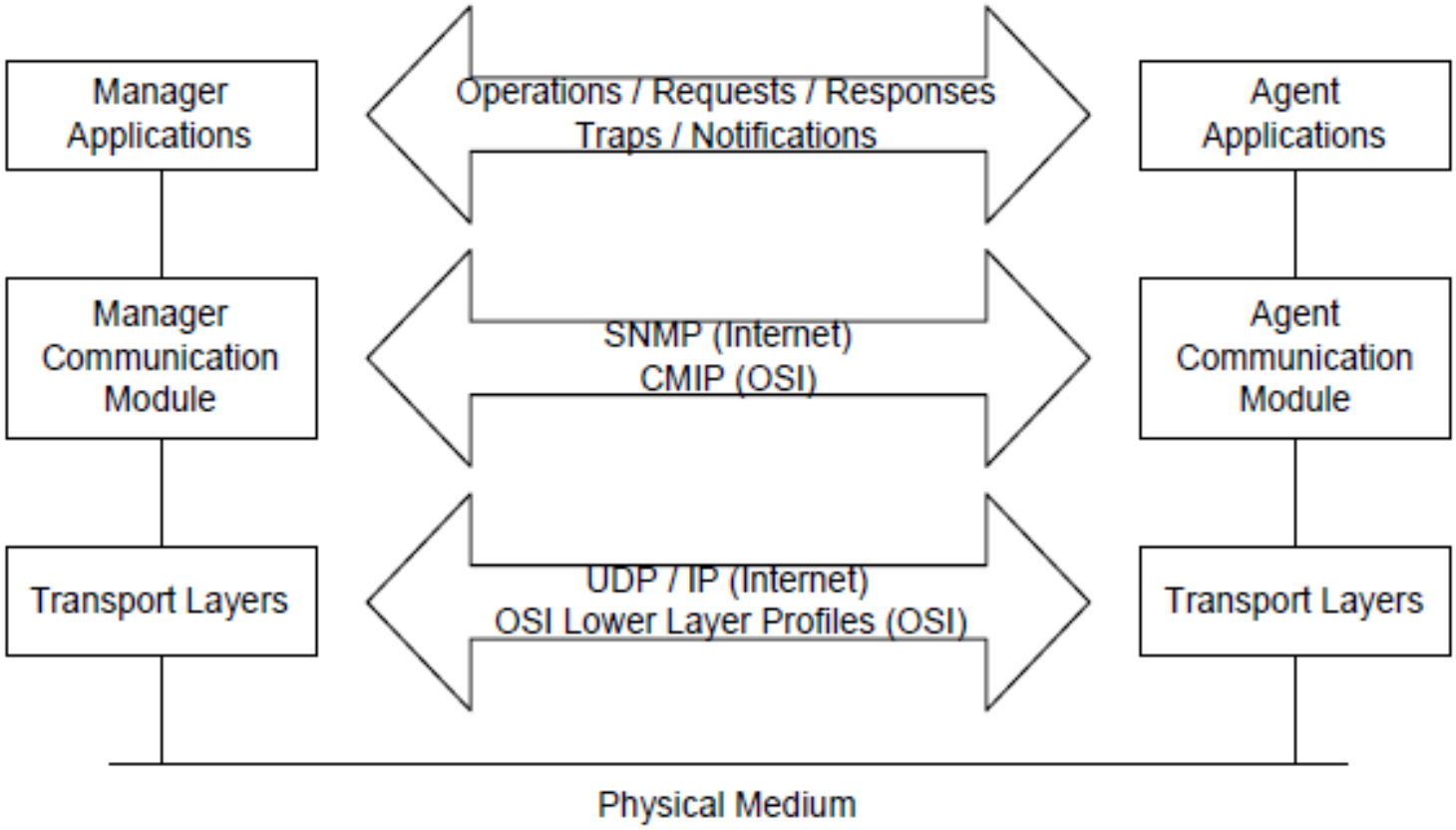
- Скаларни обекти (Интернет). Обектно-ориентирани (OSI)
- Операциите, поведението и съобщенията в OSI са част от комуникационния модел в Интернет
- Интернет ***syntax*** е включен като част от OSI атрибутите
- Интернет ***access*** е част от модела за сигурност на OSI
- Интернет ***status*** е част от OSI съответното приложение
- OSI позволява създаване и изтриване на обекти

Комуникационен модел

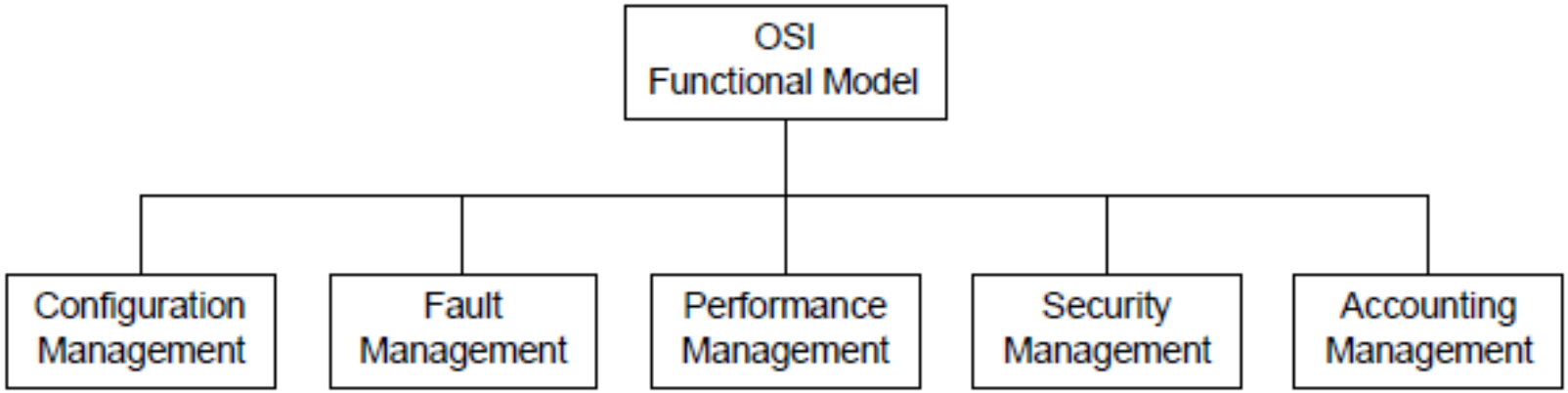


Описва начина по който информацията се обменя между системите

Комуникационен модел - протоколи



Функционален модел



Насочен е към потребителски приложения

Функционален модел – управление на конфигурирането

- Осигурява базова функционалност
  - Установява и променя мрежови конфигурации и параметри на компонентите на мрежата
  - Настройва прага за алармите
- Осигурява мрежови ресурси – проектиране, инсталиране, поддръжка
- Управление на инвентара от оборудване
- По отношение на мрежовата топология:
  - Автоматично откриване на устройства за управление чрез:
    - Broadcast *ping*
    - ARP таблици в устройствата
  - Views – физически и логически (VLAN)

Функционален модел – управление на отказите

- Откриване на отказа (генерира съобщение за проблема)
  - Запитване и връщане на статус
  - Trap съобщения - linkDown, egpNeighborLoss
- Локализиране на мястото на отказа
  - Откриване на всички дефектирали компоненти и проследяване по топологията на дървото до намиране на източника
  - Изолиране на дефектиралите устройства от мрежата чрез SNMP инструменти
  - Използване на изкуствен интелект / корелационни техники
- Възстановяване на услуга (има по-висок приоритет)
- Идентификация на причината за проблема
- Решение

Функционален модел – управление на производителността

- Наблюдаване на ефективността на мрежата с инструменти (анализатори на трафик)
- Следене на показатели за ефективност
  - Макро-ниво: пропускателна способност, време за реакция, достъпност, надеждност
  - Микро-ниво: широчина на честотната лента, използване, процент на грешки при пиково натоварване, средно натоварване
- Мониторинг на данните
  - Нормално поведение
  - Необичайно поведение (прекомерно много колизии, висока загуба на пакети)
  - Ръчно и автоматично изчистване на аларми
- Статистика за ефективността

Функционален модел – управление на сигурността

- Заплахи за сигурността
  - Модифициране на информация
  - Маскарадинг
  - Модифициране на даннови потоци
  - Прихващане на комуникация
- Сигурност на комуникацията
  - Защита на интегритета
  - Валидиране на автентикацията
- Политики и процедури
- Ресурси за предотвратяване на нарушения на сигурността
  - Защитни стени
  - Криптиране
  - Автентикация, цялостност на данните и произход на данни
  - Оторизация (за четене, четене и запис)

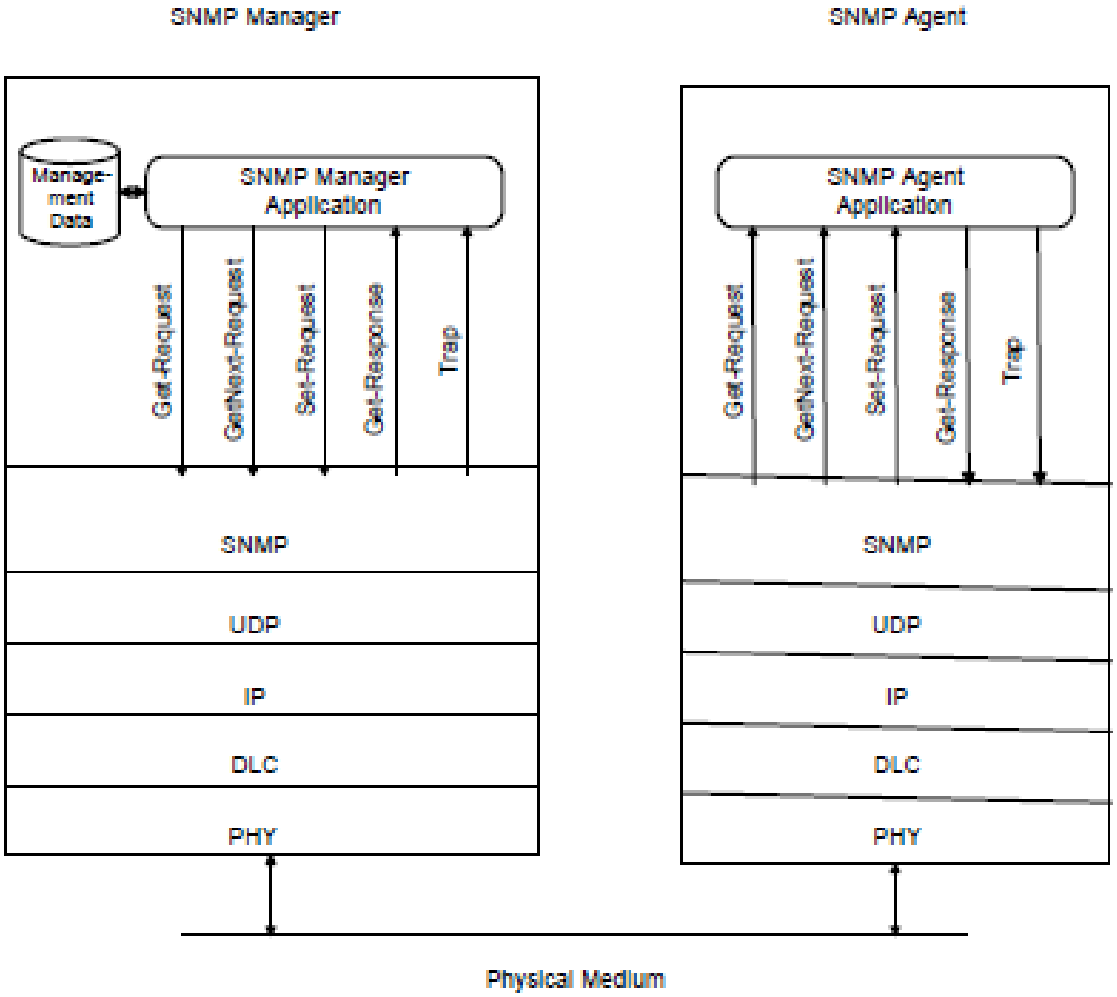
Функционален модел – управление на отчетността

- Функционално отчитане на използването на мрежата за планиране на бъдещо развитие
- Следи използването на ресурси
- Идентифицира скрити разходи за ИТ ползване

Simple Network Management Protocol

- SNMP е протокол от приложния слой
- Базиран на UDP, port 161
- Компонентите включват:
  - SNMP manager
  - SNMP agent
  - MIB - Management Information Base
- Версии на SNMP:
  - SNMPv1 – RFC 1157.
  - SNMPv2c – RFCs 1901 - 1908.
  - SNMPv3 – RFCs 2273 -2275 – сигурност, автентикация и криптиране на пакетите.

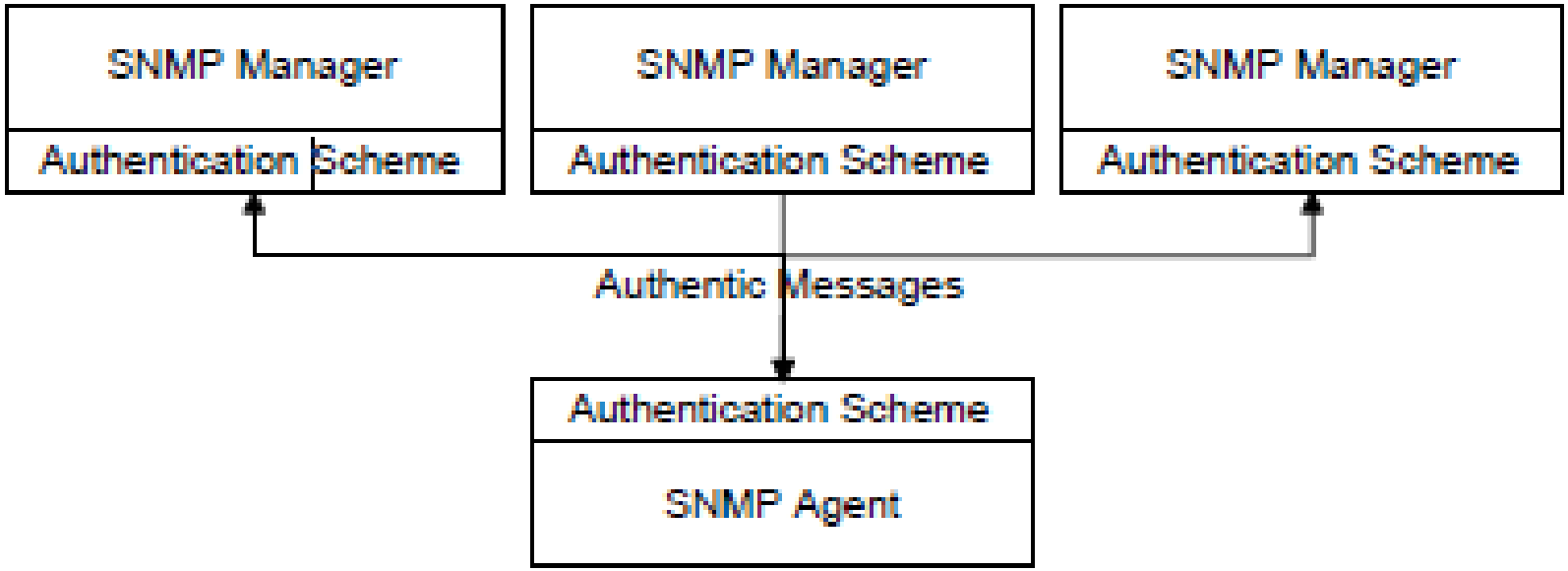
Архитектура на SNMP



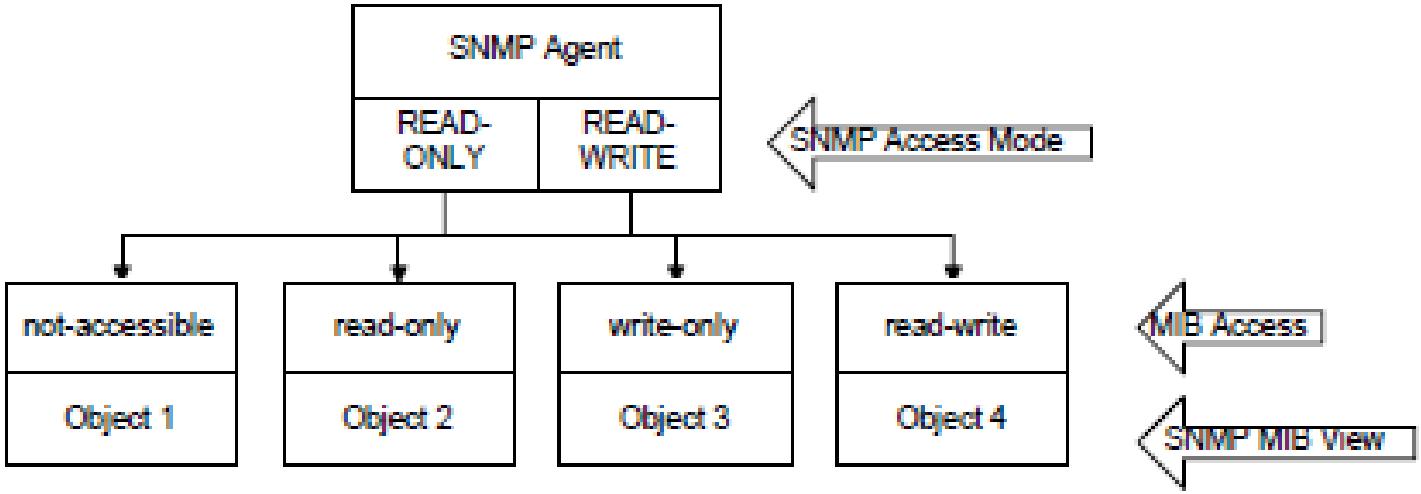
Административен модел на SNMPv1

- Базиран е на *community* профил и политика
- Схемата за автентикация е базирана на общото community име
- *Community*: Свързване на два приложни компонента
- *Community name* – низ от байтове.
- Две приложения в едно и също community могат да комуникират помежду си
- Комуникациите не са криптирани

SNMP community



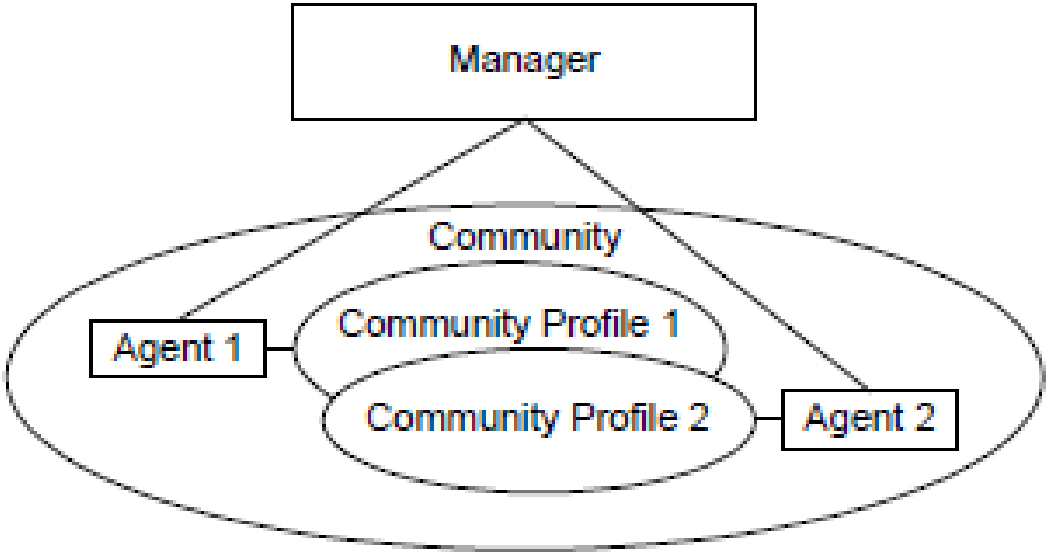
SNMP community профил



- SNMP MIB view – агентът вижда само подмножество от управлявани обекти
- SNMP access mode – всяко community има режим на достъп: read-only, read-write

Community profile: SNMP MIB view + SNMP access mode

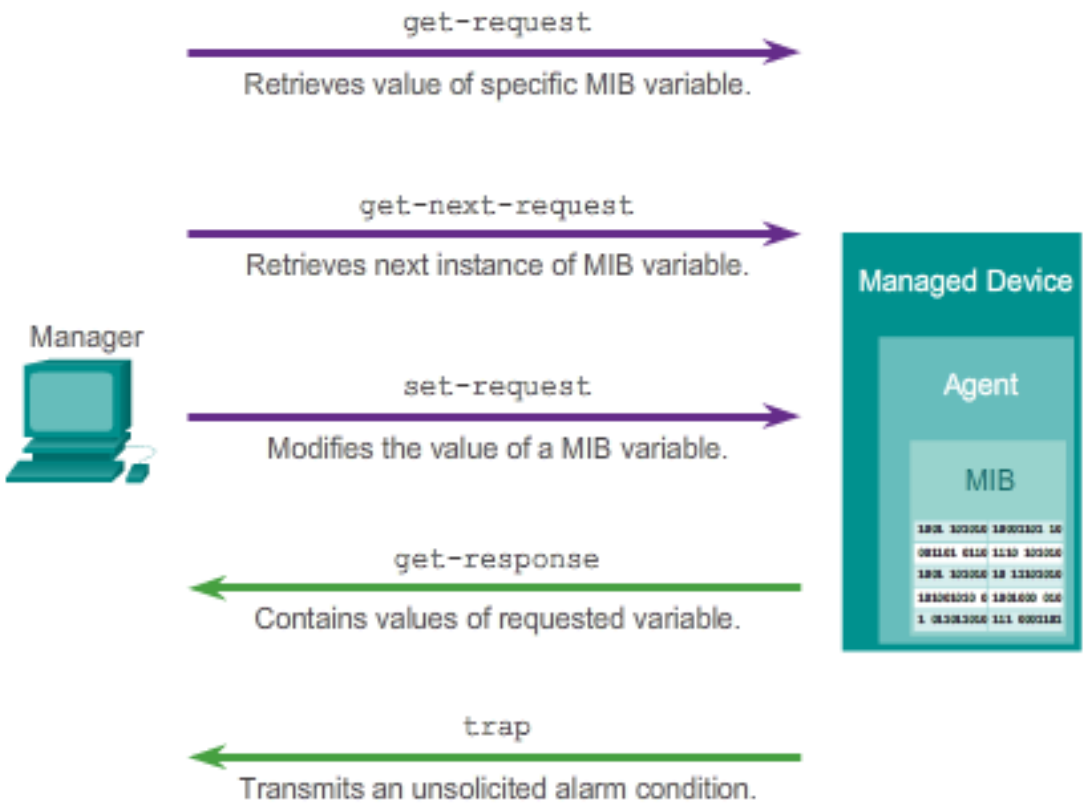
SNMP – политика на достъп



- Менажерът управлява Community и 2 мрежови компонента през Agent1 и Agent2
- Agent1 има view само на Community1 Profile (напр. Cisco у-ва)
- Agent2 има view само на Community2 Profile (напр. 3Com у-ва)
- Менажерът има тотално view и на двата типа компоненти

SNMP съобщения

- Get
- Set
- Trap - ненадеждно
- Trap (SNMPv3 с ACK) - надеждно



Get и Set съобщения

PDU Type	RequestID	Error Status	Error Index	VarBind name 1	VarBind value 1	...	VarBind n name	VarBind n value

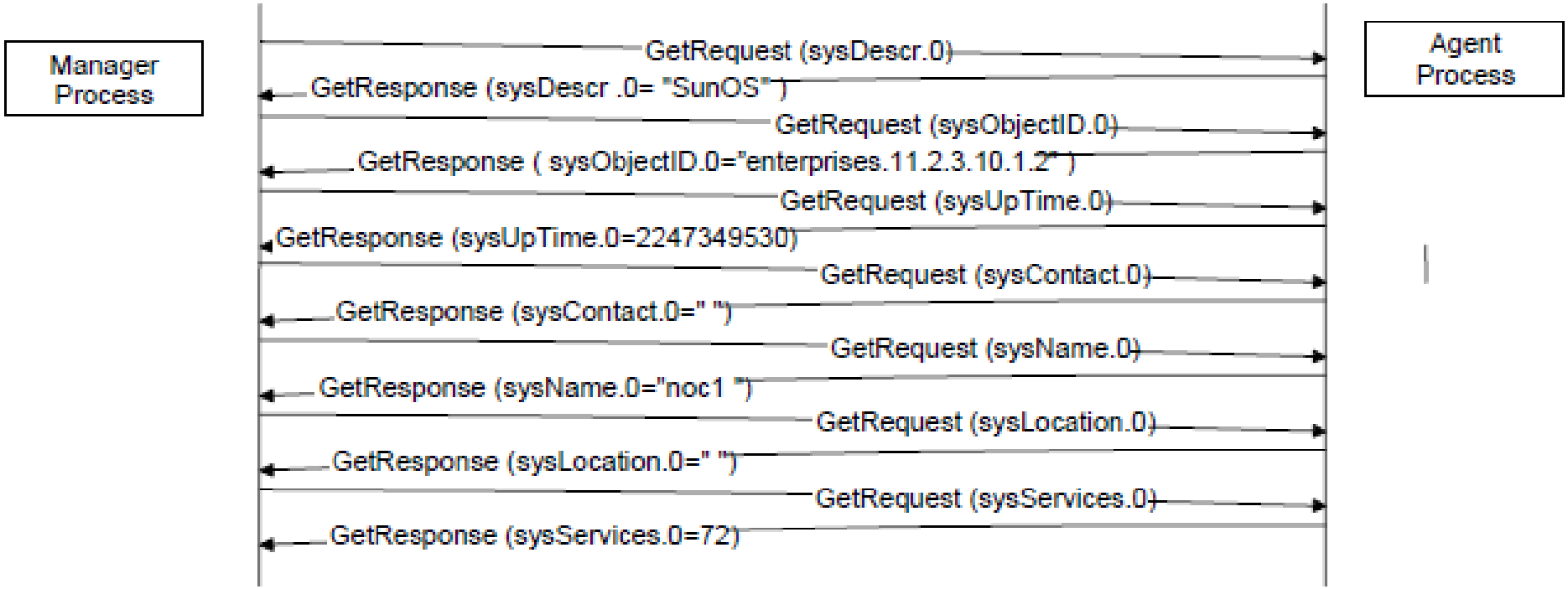
- get-request 0
- get-next-request 1
- get-response 2
- set-request 3

Trap съобщения

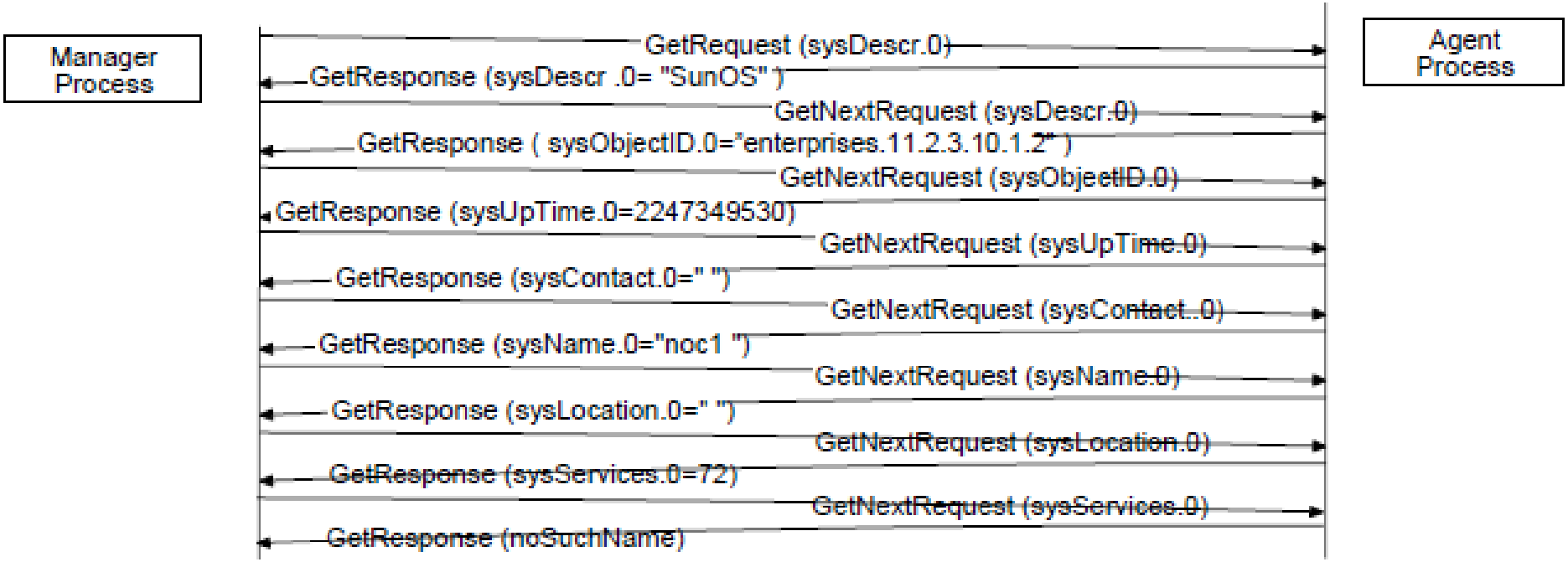
PDU Type	Enterprise	Agent Address	Generic Trap Type	Specific Trap Type	Timestamp	VarBind 1 name	VarBind 1 value	...	VarBind n name	VarBind n value

- Enterprise и Agent Address се отнасят за системата, генерирала trap
- Има 7 вида Generic trap съобщения
- Specific trap са дефинирани от съответната организация
- Ако Generic Trap = 6, Trap е Enterprise специфичен и е дефиниран в частна MIB

Get-request


Manager Process
Agent Process
GetRequest (sysDescr.0)
GetResponse (sysDescr .0= "SunOS")
GetRequest (sysObjectID.0)
GetResponse (sysObjectID.0="enterprises.11.2.3.10.1.2")
GetRequest (sysUpTime.0)
GetResponse (sysUpTime.0=2247349530)
GetRequest (sysContact.0)
GetResponse (sysContact.0=" ")
GetRequest (sysName.0)
GetResponse (sysName.0="noc1 ")
GetRequest (sysLocation.0)
GetResponse (sysLocation.0=" ")
GetRequest (sysServices.0)
GetResponse (sysServices.0=72)

Get-next-request



Версии на SNMP

- SNMPv1 – ниска сигурност; използва 32 битови броячи
- SNMPv2 – ниска сигурност; нова команда Inform; подобрена поддръжка на грешки
- SNMPv3 – подобрена сигурност (автентикация и криптиране)

Средства за мрежово администриране

- Наблюдение на статуса на мрежата:
  - ifconfig (Linux); ipconfig (Windows)
  - ping (Linux, Windows)
  - nslookup (Linux, windows)
- Наблюдение на трафика
  - ping (Linux, Windows)
  - tcpdump (Linux)
  - Wireshark (Linux, Windows)
- Наблюдение на маршрутизирането
  - arp (Linux, Windows)
  - traceroute (Linux); tracert (Windows)
  - netstat (Linux, Windows)

Въпроси?