Управление и наблюдение на работата на компютърна мрежа

проф. д-р инж. Венета Алексиева,
проф. д-р инж. Христо Вълчанов

Основни моменти

- Управление на мрежата
- Управление на системата
- Видове
- Проблеми
- Стандарти за управление на мрежата
- Модели за управление на мрежата
- SNMP
- Syslog
- NTP

Възможни проблеми в мрежа

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

Управление на мрежата

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

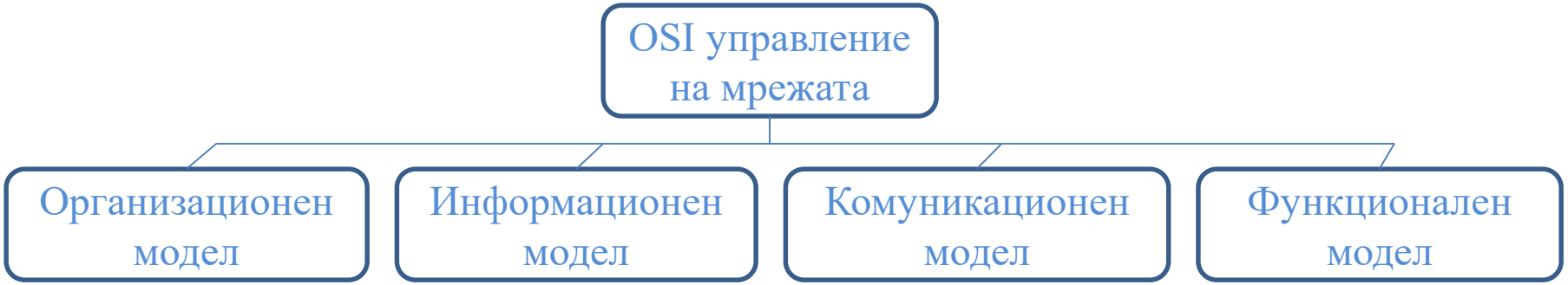
Видове управление на мрежата

- Обезпечаване на мрежата
  - Планиране
  - Проектиране
- Работа на мрежата
  - Възстановяване на услуги при проблем
  - Конфигуриране на мрежови устройства
  - Управление на трафика
  - Управление на сигурността
  - Отчетност за използване на ресурси/услуги
  - Лог-файлове
  - Събиране на статистически данни и анализът им
- Поддръжка на мрежата
  - Проблеми
  - Повреди
  - Възстановяване на мрежата
  - Инсталиране на устройства
  - Рутинни тестове

Стандарти за управление на мрежата

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

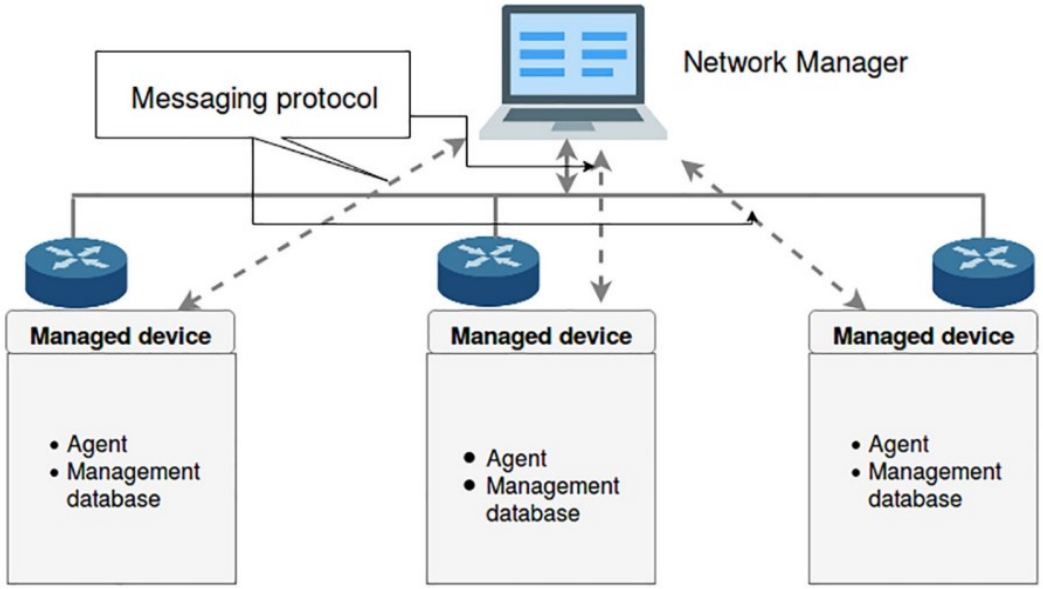
OSI модел за управление на мрежата



SNMP модел

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

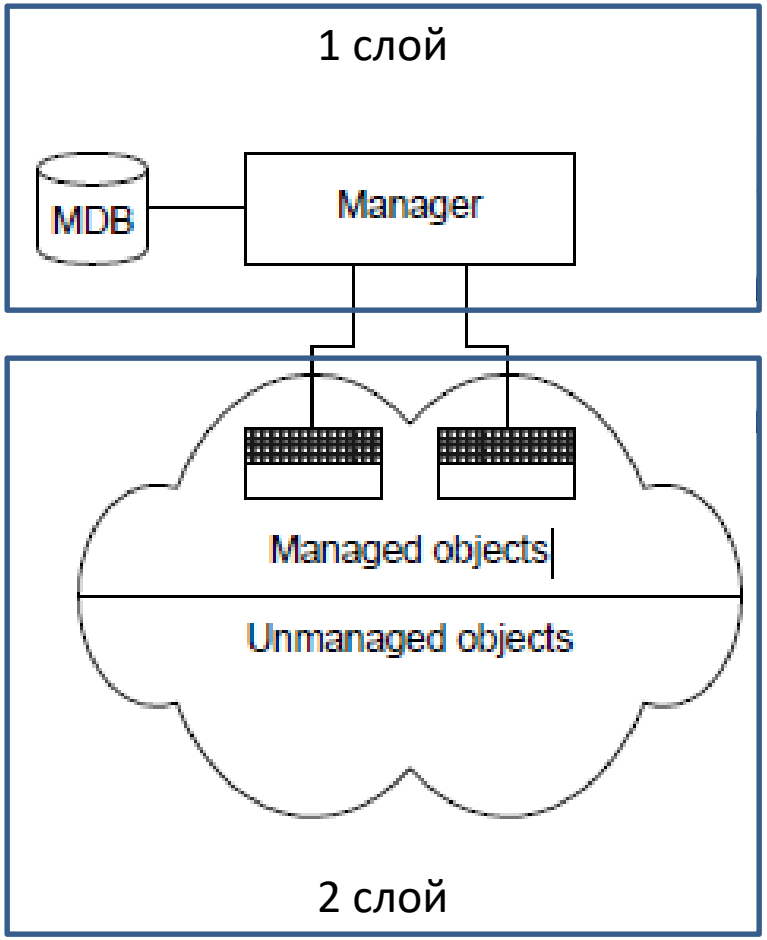
Организационен модел



Описва компонентите на мрежата и тяхната взаимна връзка.

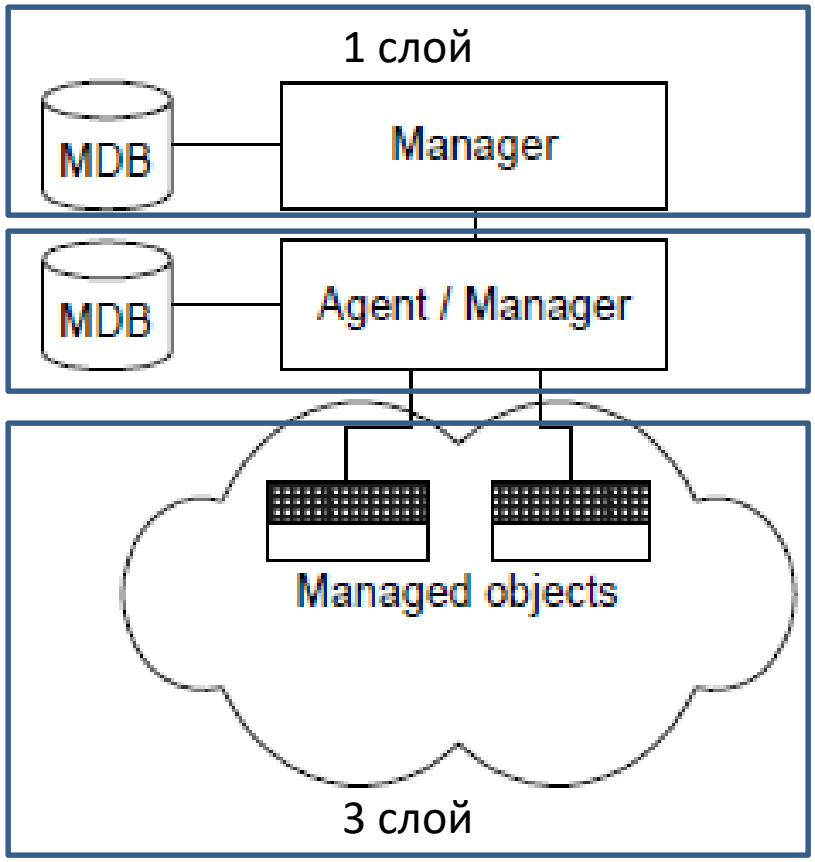
- **Manager** – софтуер, чрез който се управляват обектите. Изпращат заявки към обектите и се получава информация за тях,. Наблюдават се аларми. Предлага се потребителски интерфейс.
- **Agent -** Събира информация от обектите. Конфигурира параметрите от обектите. Отговаря на заявки от manager. Генерира аларми и ги изпраща на manager
- **Object -** Мрежов елемент, който се управлява. Върху него се изпълнява агента. Бива управляем/неуправляем.

Двуслоен модел



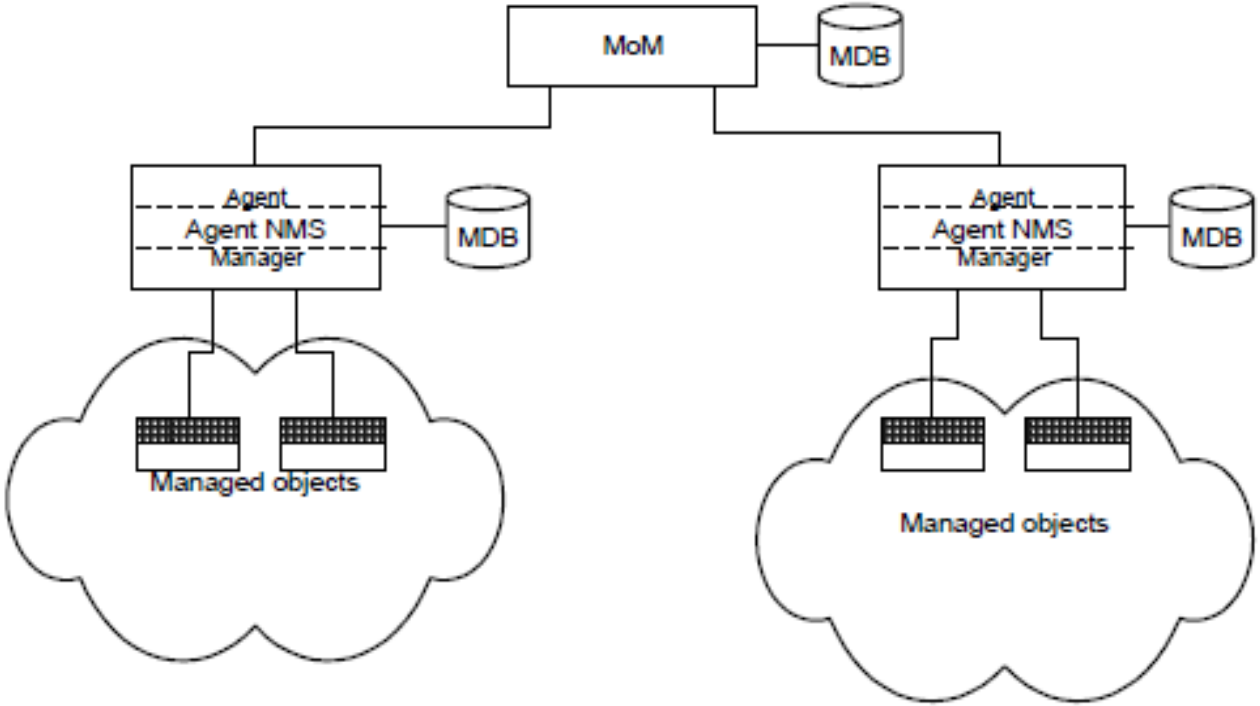
- **MDB** – БД за мениджмънт
- **Агенти** – във всеки обект (хъб, рутер)
- **Manager** –управлява елементите (суич, ATM суич)
- **Unmanaged objects**- мрежови елементи, които не се управляват – физически (unmanaged hub) и логически (пасивни елементи)

Трислоен модел



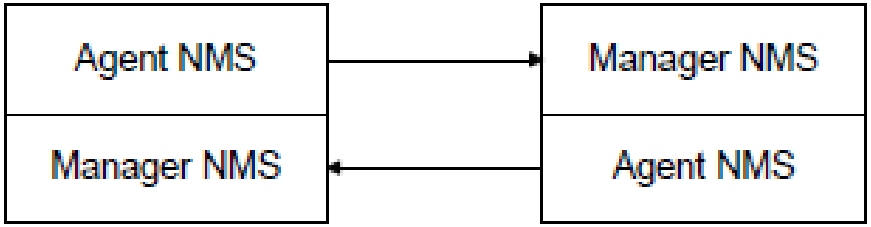
- Междинният слой има двойна роля:
  - Agent за слой 1
  - Manager за слой 3
- Пример за междинен слой:
  - Remote monitoring probe/agent (RMON)

Manager of Managers (MoM) модел



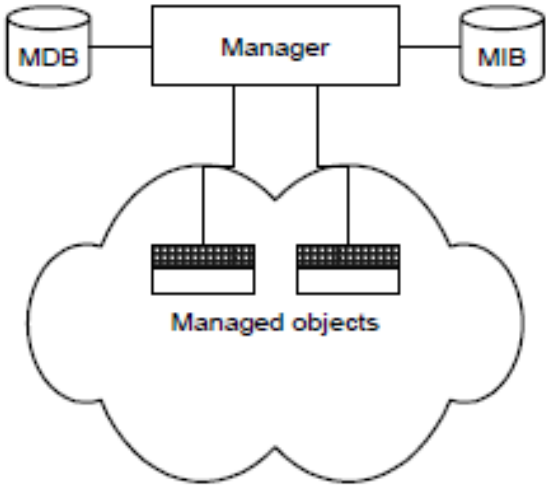
- За големи по размер мрежи
- Дава възможност за разглеждане по домейни – географски, административни…

Peer-to-peer модел



- И двете системи работят като пиъри.
- Те са стартирали едновременно процеси мениджър и агент.

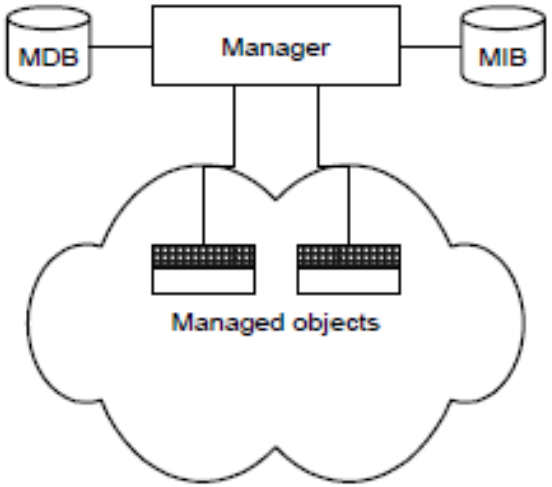
Информационен модел



- Занимава се с структурата и съхраняването на информация.
- Задава информационната база, за да опише управляваните обекти и техните взаимоотношения.
- Структурата на управляваната информация (SMI) дефинира за управлявания обект **синтаксис, семантика и статус:**

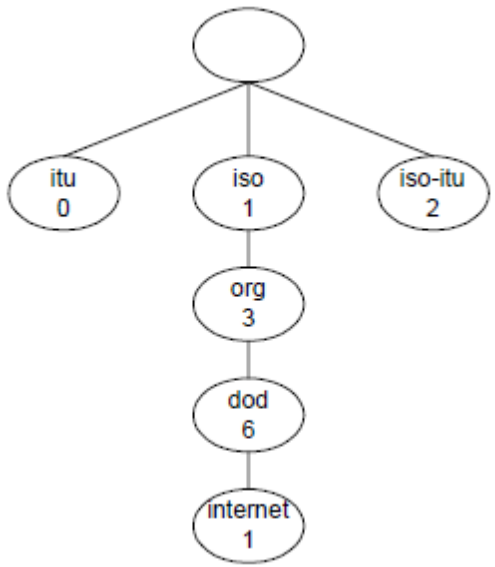
```
sysDescr: { system 1 }
Syntax: OCTET STRING
Definition: "A textual description of the entity."
Access: read-only
Status: mandatory
```

Информационен модел



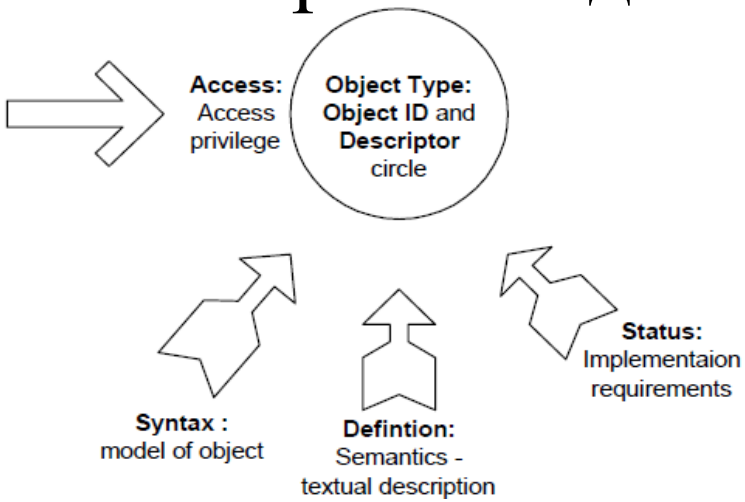
- **Managed Objects**
  - Мрежови елементи - hubs, bridges, routers, transmission facilities
  - Софтуер – програми, алгоритми
  - Административна информация – лице за контакти, име на група от обекти…
- **Management Information Base (MIB)**
  - съдържа информация за обектите
  - Организирана е по групи 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
- **Management Data Base / Information Base**
  - MDB е физическа база данни - Oracle, Sybase

Management Information Tree (MIT)



- Управляваните обекти са еднозначно определени от дървовидна структура, определена от OSI модела.
- Всеки възел е управляван обект

От Интернет гледна точка

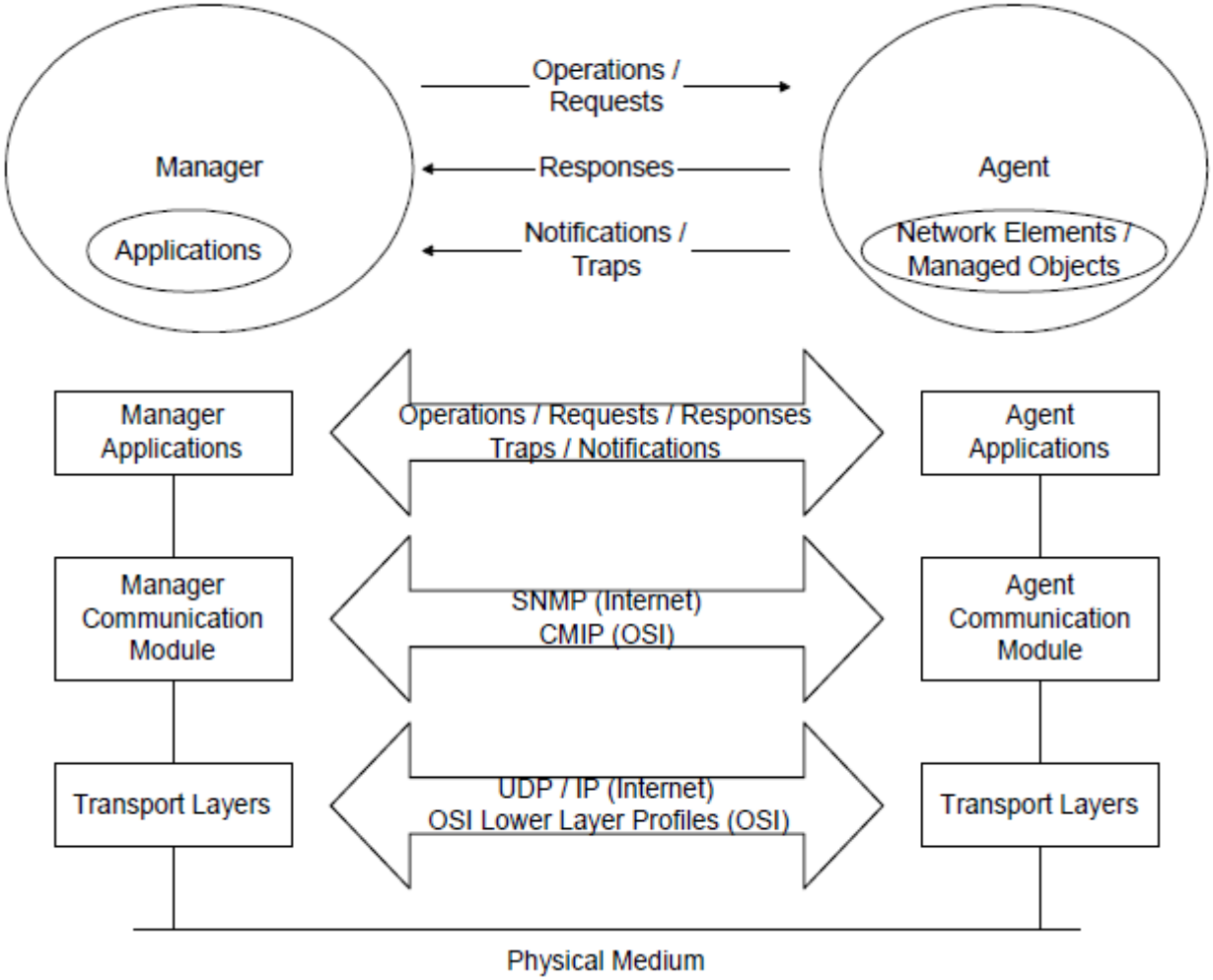


Спецификация

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

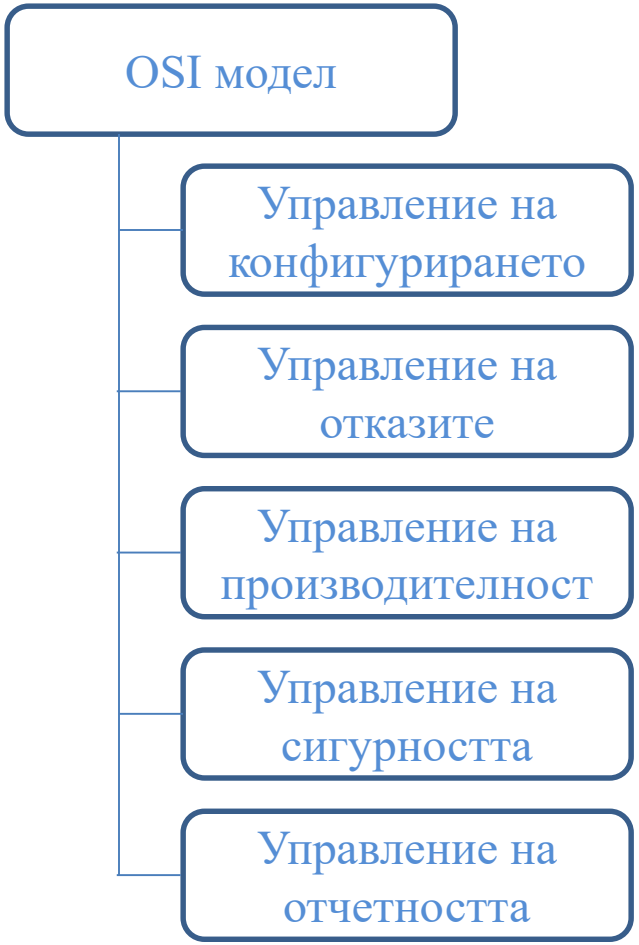
Комуникационен модел

- Описва начина, по който информацията се обменя между системите



Функционален модел

- Насочен е към потребителски приложения



Управление на конфигурирането

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

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

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, оползотворяване, процент на грешки при пиково натоварване, средно натоварване
- Мониторинг на данните
  - Нормално поведение
  - Необичайно поведение (прекомерно много колизии, висока загуба на пакети и т.н.)
- Ръчно и автоматично изчистване на аларми
- Статистика за ефективността
  - За трафика
  - За грешки
  - Проследяване на QoS
  - Проследяване на споразуменията за ниво на услугите
  - Анализ на трендовете
  - Механизъм за планиране на поддръжката на обарудване
  - Акаунтинг

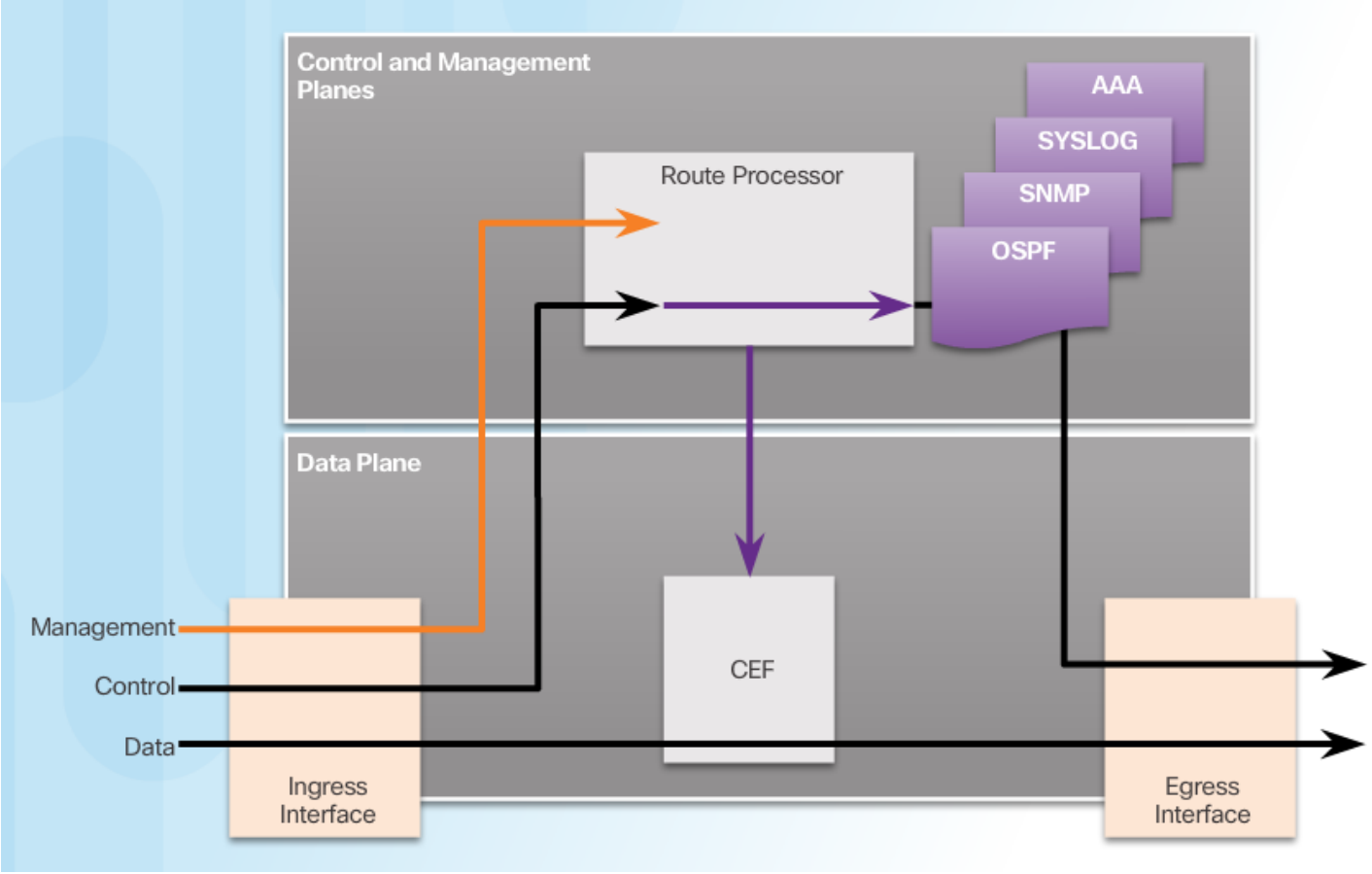
Управление на сигурността

- Проблеми със сигурността
  - Модифициране на информация
  - Маскарадинг
  - Модифициране на даннови потоци
  - Прихващане на комуникация
  - Защита на интегритета
  - Валидиране на автентикацията
  - Политики и процедурию
  - ресурси за предотвратяване на нарушения на сигурността
  - защитни стени
  - Криптиране
  - Автентикация , цялостност на данните и произход на данни
  - Оторизация (за четене, четене и запис, не-достъп)

Управление на отчетността

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

Мрежовите устройства работят на 3 равнини– данни, контрол и управление



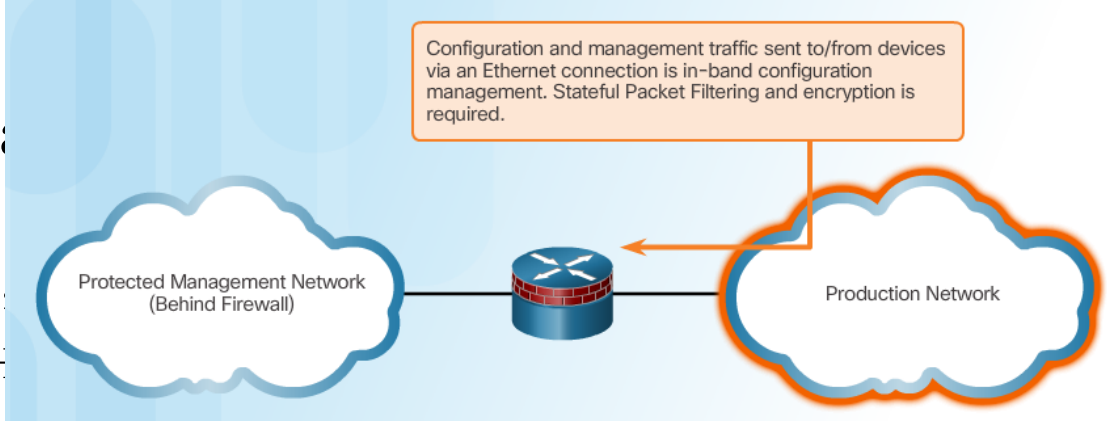
Информационни потоци

- In-band – регулярните потоци в мрежата
- Out-of-band – отделни потоци за управление

Определяне на типа на достъпа за управление

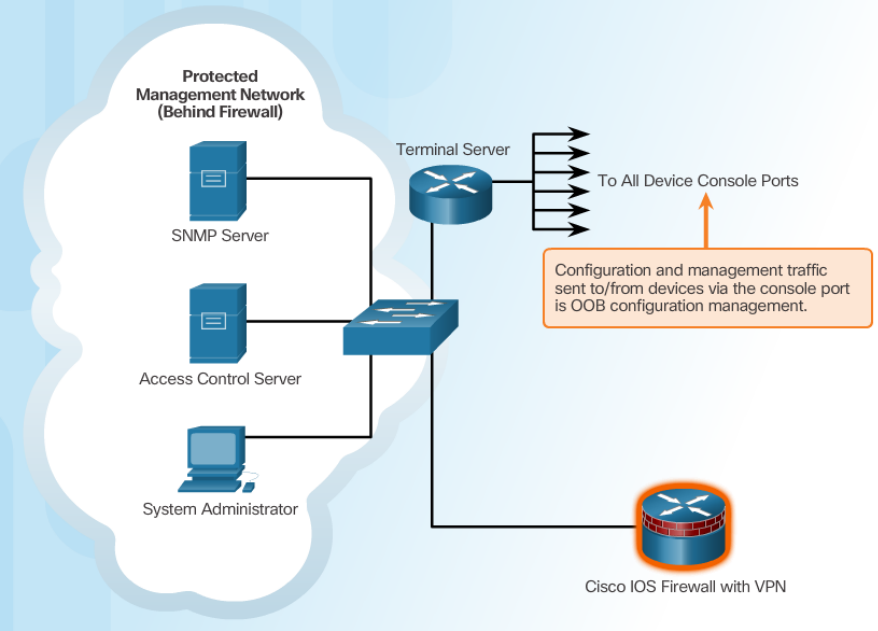
In-Band Management:

- Прилага се само за устройства, които трябва бъдат управлявани
- Използват се IPsec, SSH,
- Дали канала за управлен трябва да бъде отворен постоянно?



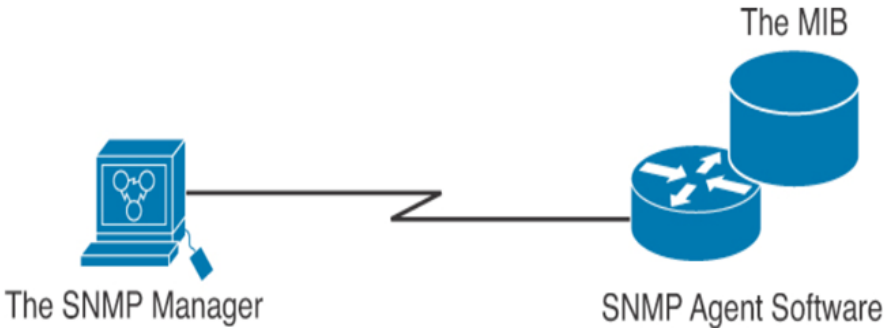
Out-of-Band Management:

- Осигуряване на най-високо ниво на сигурност
- Смекчаване на риска от предаване на протоколи за управление през използваната мрежа



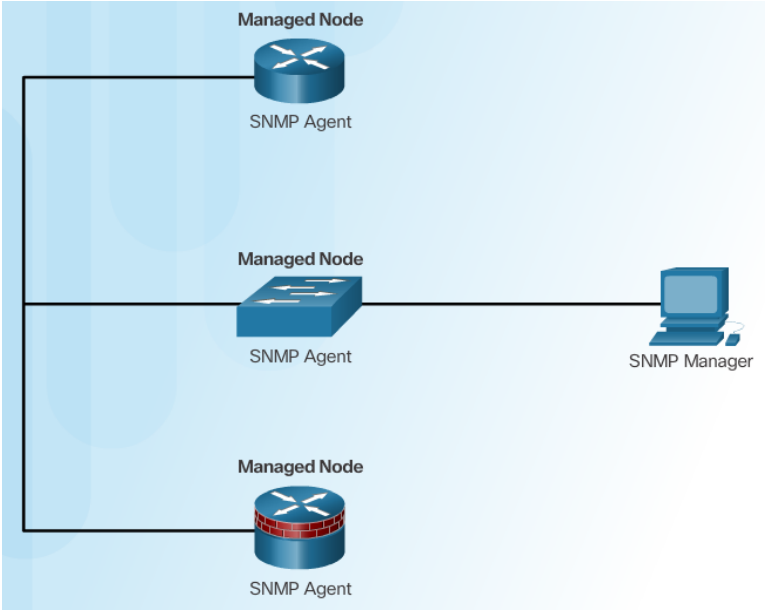
SNMP

- SNMP е най-широко използвания протокол за управление на мрежа и мрежови устройства.
- SNMP е протокол от приложния слой.
- Базиран на UDP.
- Версии на SNMP:
  - **SNMPv1** – в RFC 1157.
  - **SNMPv2c** – в RFCs 1901-1908.
  - **SNMPv3** – в RFCs 2273-2275 – сигурност, автентикация и криптиране на пакетите.

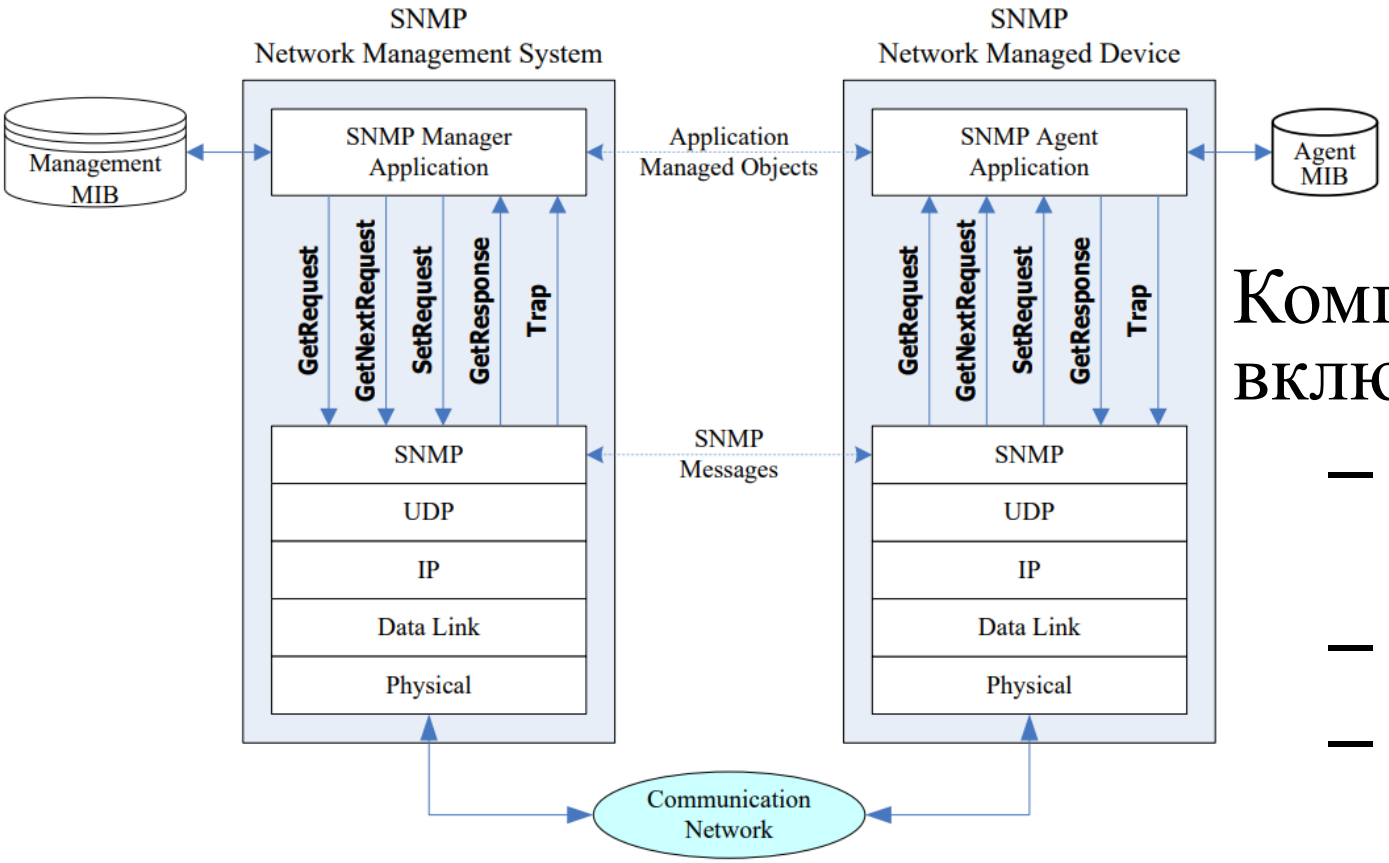


SNMP

- SNMP agents е по UDP port 161
- SNMP managers е по UDP port 162



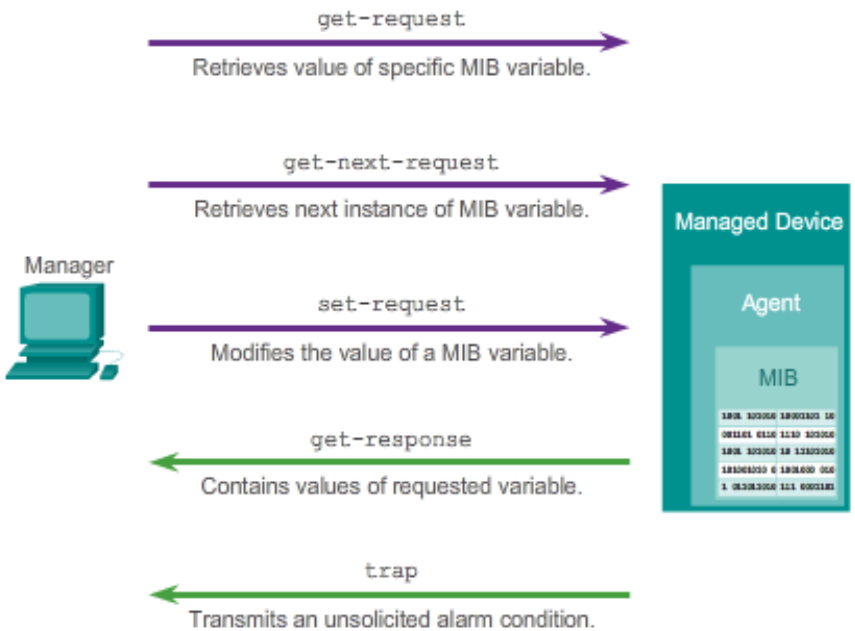
Архитектура на SNMP



Компонентите включват:

- SNMP manager
- SNMP agent
- MIB - Management Information Base

SNMP Съобщения



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

Version	Community Name	SNMP PDU

(a) SNMP message

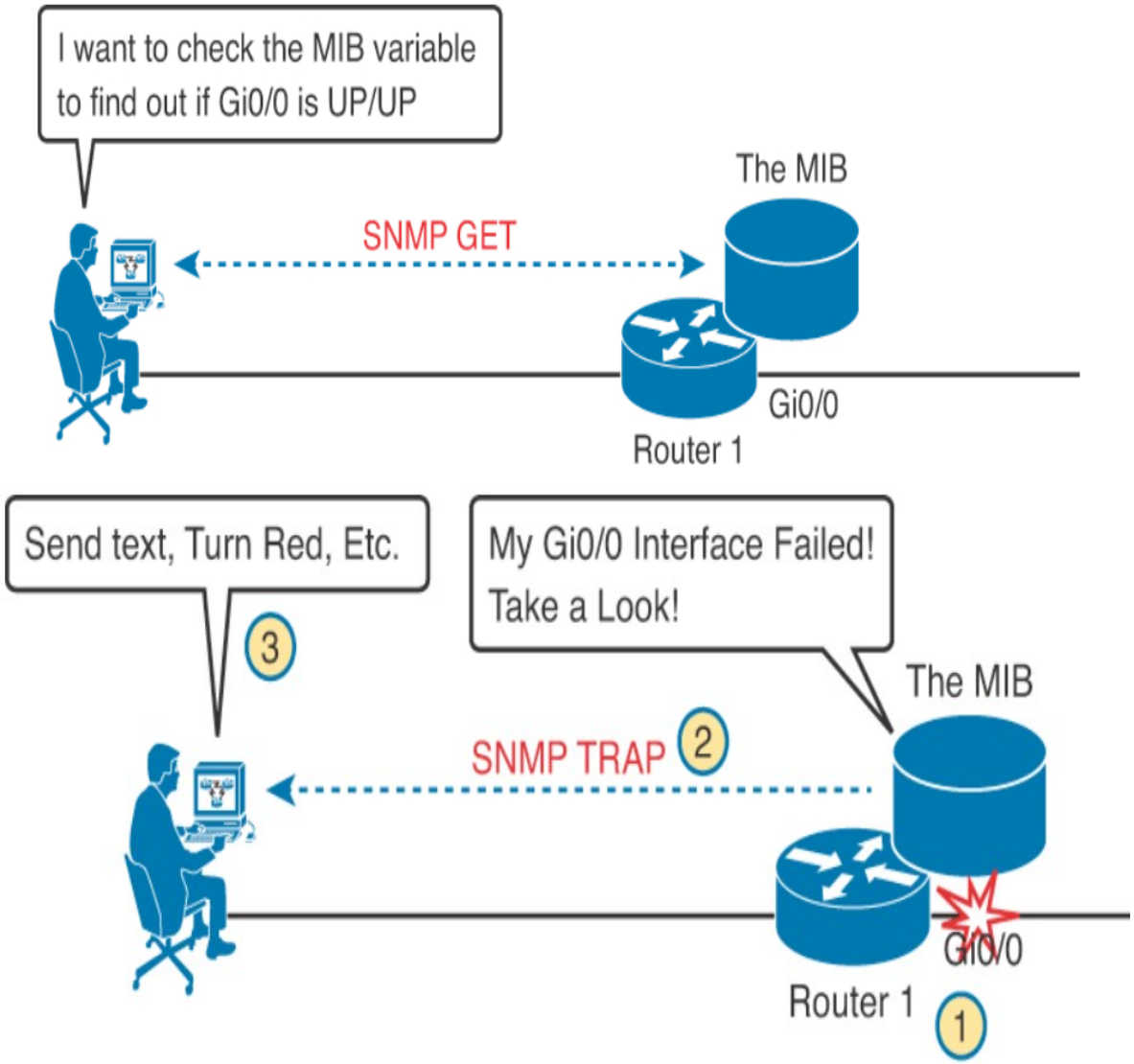
PDU Type	RequestID	ErrorStatus	ErrorIndex	VariableBindings				
				Name 1	Value 1	...	Name N	Value N

(b) Get/Set Type of PDUs

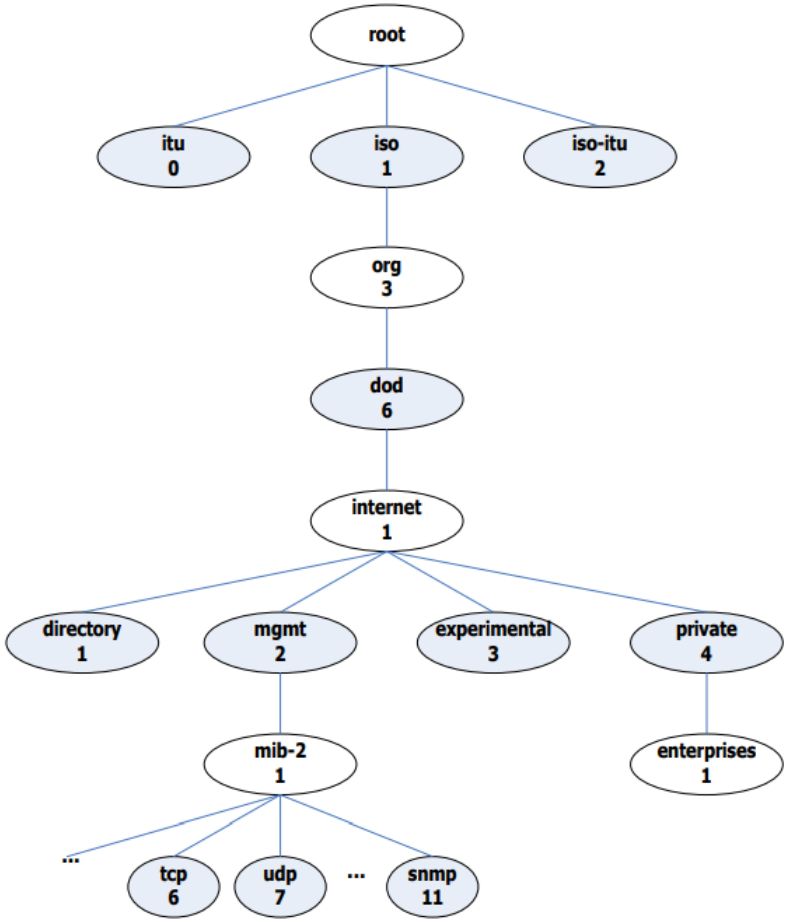
PDU Type	Enterprise	Agent-Address	Generic-Trap	Specific-Trap	Timestamp	VariableBindings				
						Name 1	Value 1	...	Name N	Value N

(c) Trap PDUs

SNMP наблюдение



Management Information Tree (MIT)



- MIB определя всяка променлива като ID обект (OID)
- Организира в дървовидна йерархия OIDs
- MIB за всяко устройство включва:
  - клонове на дървото с променливи, **общи** за много мрежови устройства
  - клонове с променливи, **специфични** за това устройство.
- Мрежови доставчици на оборудване могат да определят свои собствени частни клонове на дървото.

Събиране на данни за MIB с snmpget

```
[13:22][cisco@NMS~ ]$ snmpget -v2c -c community 10.250.250.14
1.3.6.1.4.1.9.2.1.58.0
SNMPv2-SMI::enterprises.9.2.1.58.0 = INTEGER: 11
```

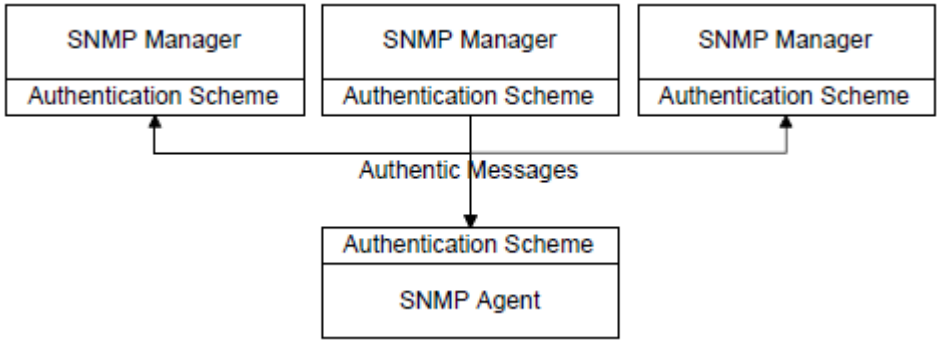
-v2c Показва версията на SNMP

-c community SNMP паролата, наречена community string

10.250.250.14 е IP адреса на наблюдаваното устройство

1.3.6.1.4.1.9.2.1.58.0 е числовия идентификатор OID за MIB променливата

SNMPv1



- Сигурността в SNMPv1 е чрез името на общността, съдържащо се в SNMP съобщението
- Автентикационната схема е модул в manager и agent (общо име на общността)
- Комуникацията в SNMPv1 не е криптирана
- Много реализации на SNMPv1 са избрали да не изпълнява командата Set, което намалява тяхната полезност само до наблюдение.

SNMPv2

- Архитектурата на SNMPv2 е същата като тази на SNMPv1.
- Ключовото подобрение в SNMPv2 може да се обобщи, както следва:
- **Възможност за групово прехвърляне на данни**: Най-забележимата промяна в SNMPv2 е включването на два нови PDU. Първият PDU е GetBulkRequest, който позволява на мениджъра да извлича ефективно големи блокове от данни и следователно ускорява процеса GetNextRequest.
- **Възможност от мениджър към мениджър**: Вторият PDU е InformRequest, който позволява на един мениджър да изпраща trap информация на друг и по този начин прави системите за управление на мрежи интероперативни.
- **Структура на информацията за управление**: SMI, дефиниран в SNMP, е пренаписан.

SNMPv2 съобщения

- В SNMPv2 е стандартизирана до общ формат за всички съобщения

PDU Type	RequestID	ErrorStatus	ErrorIndex	VariableBindings				
				Name 1	Value 1	...	Name N	Value N

(a) All but Bulk Type of PDUs

PDU Type	RequestID	NonRepeaters	MaxRepetitions	VariableBindings				
				Name 1	Value 1	...	Name N	Value N

(b) `GetBulkRequest` PDU

Пароли при SNMP v2c

- **Read-only (RO):** Осигурява достъп до променливите в MIB, но не позволява промени, а само четене. Тъй като сигурността е толкова слаба във Version 2c, много организации използват SNMP само в този режим само за четене.
- **Read-write (RW):** Осигурява достъп за четене и запис до всички обекти в MIB.

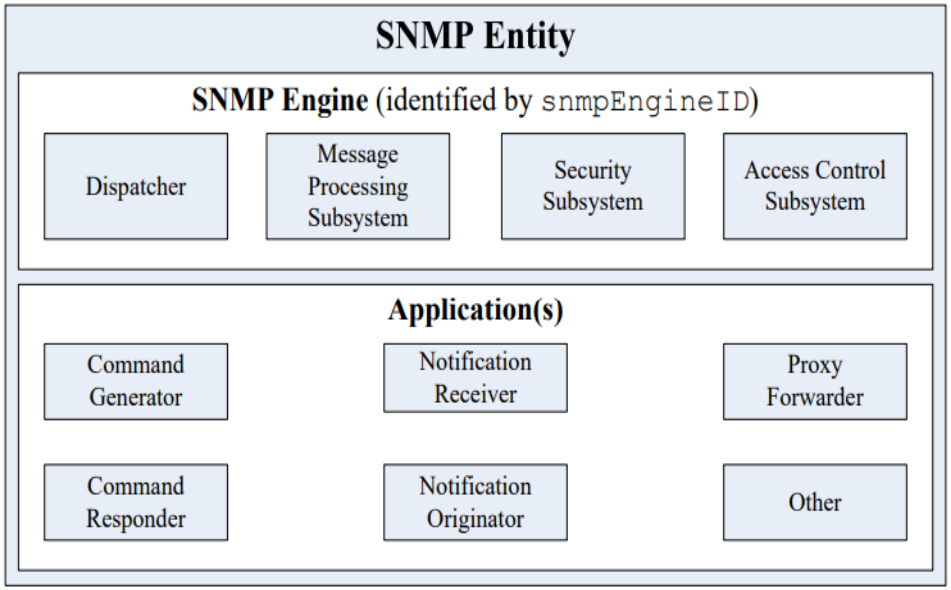
SNMPv2 - MIB

SNMPv2 MIB дефинира обекти, които описват поведението на SNMPv2 обект. Състои се от три групи:

- **Системна група**: разширение на оригиналната MIB-2 системна група. Включва колекция на обекти, които позволяват на SNMPv2 обект да действа в роля на агент, за да опише своята динамика конфигурируеми обектни ресурси.
- **SNMP група**: усъвършенстване на оригиналната MIB-2 snmp група. Състои се от обекти, които осигуряват основните инструменти на протоколната дейност.
- **MIB Обектна група**: колекция от обекти, които се занимават с SNMPv2 Trap PDU и които позволяват на няколко сътрудничещи SNMPv2 единици, всеки от които действа в роля на мениджър, да координират своите SNMPv2 set операции.

SNMPv3 архитектура

Мрежата за управление на SNMPv3 се състои от разпределена взаимодействаща колекция от SNMP единици.



Диспечер: изпраща и получава SNMP съобщения от мрежата; определя версията на съобщението и взаимодейства със съответния модел за обработка на съобщения; предоставя абстрактен интерфейс към SNMP приложения за доставяне на входящ PDU към локалното приложение и за изпращане на PDU от локалното приложение към отдалечена единица.

Подсистема за обработка на съобщения: подготвя съобщенията за изпращане и извлича данни от получените съобщения.

Подсистема за сигурност: Предоставя удостоверяване и поверителност на съобщенията.

Подсистема за контрол на достъпа: Предоставя оторизация чрез един или повече Модели за контрол на достъпа.

SNMPv3

Поддържа:

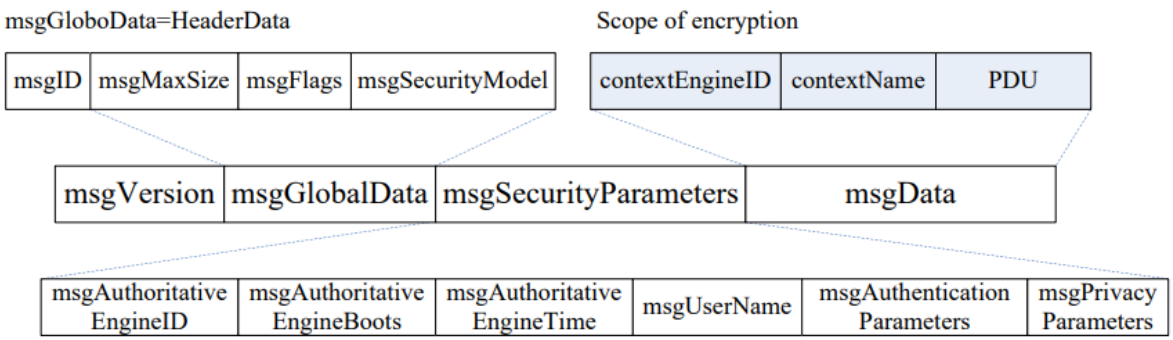
- Интегритет на съобщенията
  - гарантира, че един пакет не е бил отварян при транзит.
- Автентикация
  - гарантира, че пакетът идва от познат и надежден източник.
- Криптиране
  - гарантира, че информацията не може да се чете, ако данните са прихванати при преминаване през мрежата

Автентикация	Метод за автентикация	Криптиране
noAuthNoPriv	username	без
authNoPriv	MD5 , SHA	без
authPriv	MD5 , SHA	DES, DES-56

SNMPv3 приложения

- **Генератор на команди** - използва sendPdu и processResponsePdu примитивите, за да генерира GetRequest, GetNextRequest, GetBulk и SetRequest съобщения. Той също така обработва отговора на изпратената команда.
- **Команда за отговор -** използва четири примитиви на диспечера (registerContextEngineID, unregisterContextEngineID, processPdu и returnResponsePdu) и един примитив на подсистемата за контрол на достъпа (isAccessAllowed) за получаване и обработка SNMP get и set заявки. Също така изпраща съобщения за отговор.
- **Генератор на известия** – подобно генериране на команди, генерира trap или Inform съобщение.
- **Получател на известия** – подобно приложението за отговор на команди за получаване на SNMP съобщение за уведомление.
- **Proxy forwarder -** обработва четирите типа съобщения.

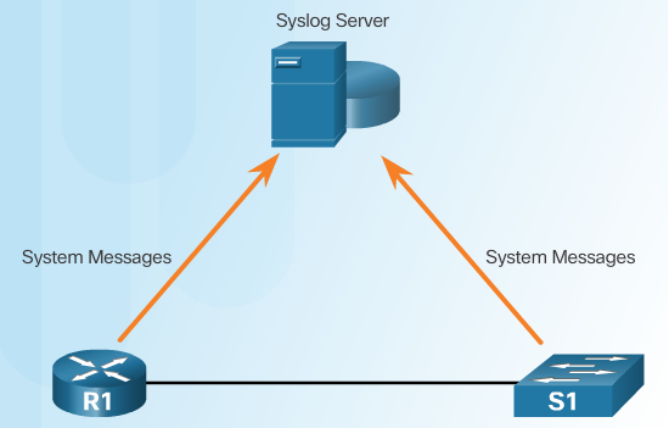
Формат на SMNPv3 съобщение

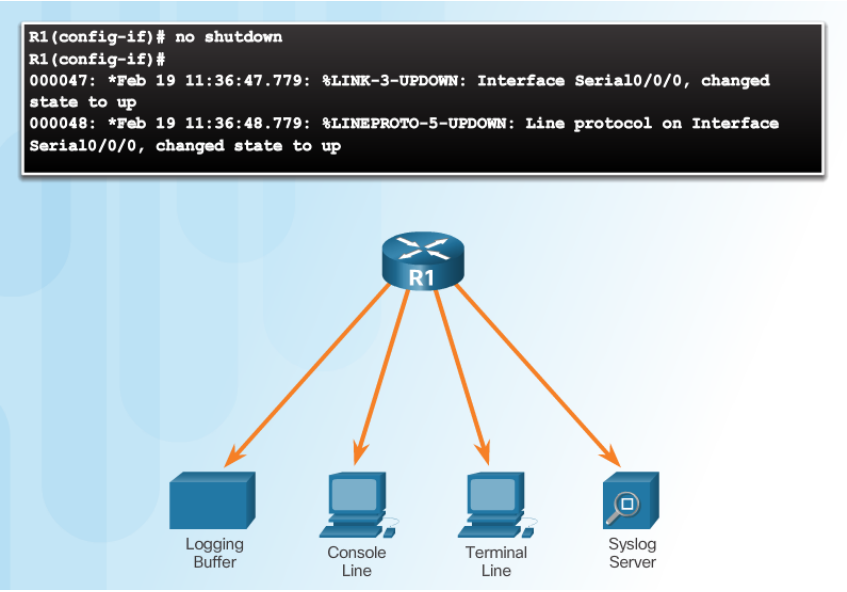


- SNMPv3 е предназначен да адресира четири вида заплахи за сигурността:
  - промяна на информация,
  - маскарад,
  - разкриване
  - промяна на потока от съобщения.

Syslog

- Събира системни и debug съобщения:
  - в текстов файл локално
  - в текстов файл на сървър
  - Текст на конзолата
  - Текст на отдалечен терминал





Syslog съобщения според ниво на сигурност

	Level	Keyword	Description	Definition
Highest Level	0	emergencies	System is unusable	LOG_EMERG
	1	alerts	Immediate action is needed	LOG_ALERT
	2	critical	Critical conditions exist	LOG_CRIT
	3	errors	Error conditions exist	LOG_ERR
	4	warnings	Warning conditions exist	LOG_WARNING
	5	notifications	Normal but significant condition	LOG_NOTICE
	6	informational	Informational messages only	LOG_INFO
Lowest Level	7	debugging	Debugging messages	LOG_DEBUG

- Например:

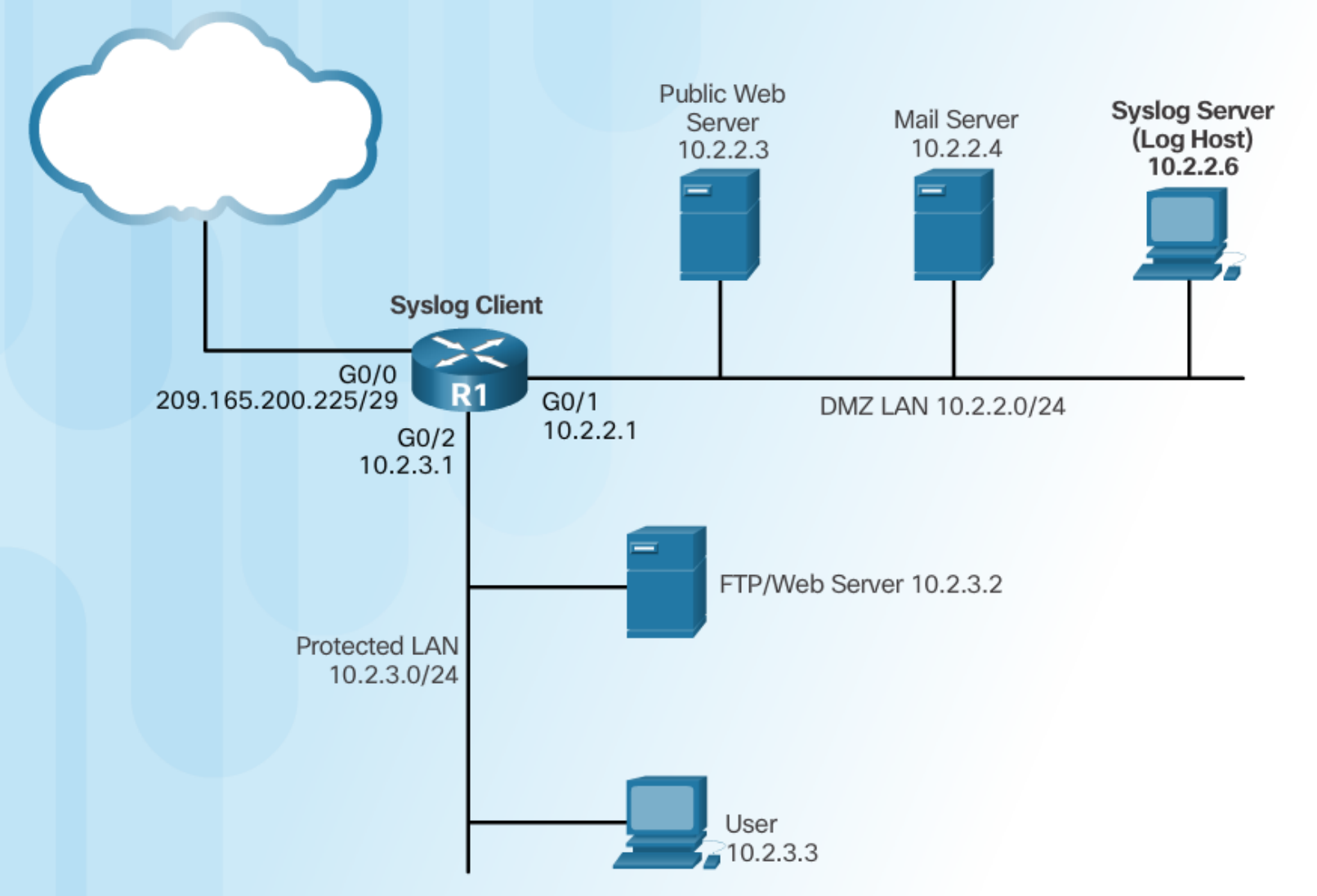
Syslog Level and Name	Definition	Example
0 LOG_EMERG	A panic condition normally broadcast to all users	Cisco IOS software could not load
1 LOG_ALERT	A condition that should be corrected immediately, such as a corrupted system database	Temperature too high
2 LOG_CRIT	Critical conditions; for example, device errors	Unable to allocate memory
3 LOG_ERR	Errors	Invalid memory size
4 LOG_WARNING	Warning messages	Crypto operation failed
5 LOG_NOTICE	Non-error conditions that may require special handling	Interface changed state, up or down
6 LOG_INFO	Informational messages	Packet denied by ACL
7 LOG_DEBUG	Messages that contain information that is normally used only when debugging a program	Packet type invalid

Syslog съобщения- синтаксис

```
000048: *Feb 19 11:36:48.779: %LINEPROTO-5-UPDOWN:
Line protocol on Interface Serial0/0/0, changed state to up
```

	Column 1	Column 2
1	seq no	Stamps log messages with a sequence number if service sequence-numbers is configured.
2	timestamp	displays if service timestamps log is configured
3	facility	denotes the source or the cause of the system message
4	severity	levels 0 – 7
5	MNEMONIC	text string that uniquely describes the message
6	description	text string containing detailed information about the event being reported

Syslog сървъри и Syslog клиенти



NTP(Network Time Protocol)

- Обикновено, настройките на датата и часа на рутера може да се настроят :
  - чрез ръчно редактиране на датата и часа
  - чрез конфигуриране на NTP- избира се между:
    - Частен таймер за синхронизация
    - Публичен таймер
- Преценяват се рисковете и в двата случая.

```
R1# clock set 10:28:00 DEC 16 2008
R1#
*Dec 16 10:28:00.000: %SYS-6-CLOCKUPDATE: System clock
has been updated from 16:07:17 UTC Tue Dec 16 2008 to
10:28:00 UTC Tue Dec 16 2008, configured from console
by console.
R1#
```

NTP сървър и NTP клиент

- Може да се добави автентикация за по-голяма сигурност

```
R1# conf t
R1(config)# ntp master 1
R1(config)# ^Z
R1#
R1# show clock
13:01:15.735 UTC Tue Dec 16 2008
R1#
```

```
R2# conf t
R2(config)# ntp server 10.10.10.1
R2(config)# ^Z
R2# show clock
13:01:41.986 UTC Tue Dec 16 2008
R2# show ntp status
Clock is synchronized, stratum 2, reference is 10.10.10.1
nominal freq is 250.0000 Hz, actual freq is 249.9992 Hz, precision is 2**18
reference time is CCF2253E.5DC2A53B (13:01:50.366 UTC Tue Dec 16 2008) clock
offset is 0.3072 msec, root delay is 23.41 msec
root dispersion is 0.38 msec, peer dispersion is 0.05 msec
R2#
```

Инструменти за наблюдение на сигурността

- Cisco Discovery Protocol (CDP) – на производител
- Link Layer Discovery Protocol (LLDP) - отворен стандарт

```
R1(config)# lldp run
R1(config)# end
R1# show cdp neighbors detail
-------------------------
Device ID: S1
Entry address(es):
  IP address: 192.168.1.254
Platform: cisco WS-C2960-24TT-L,  Capabilities: Switch IGMP
Interface: GigabitEthernet0/1,  Port ID (outgoing port): FastEthernet0/5
Holdtime : 164 sec

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE7,
RELEASE SOFTWARE (fc1)
<output omitted>
```

```
R1# show lldp neighbors detail
------------------------------------------------
Local Intf: Gi0/1
Chassis id: 0022.9121.0380
Port id: Fa0/5
Port Description: FastEthernet0/5
System Name: S1

System Description:
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE7,
RELEASE SOFTWARE (fc1)
<output omitted>
```

Препоръки за сигурност

- Изключване на ненужните услуги и интерфейси.
- Изключване и ограничаване на често конфигурирани услуги за управление.
- Забраняване на сонди и сканиране.
- Обезпечаване на сигурността на достъп през терминал.
- Забрана на proxy ARPs
- Забрана на IP-бродкасти.

Въпроси ?

Благодаря за вниманието !