Сетевое управление и мониторинг

Введение в SNMP

Содержание

- Что такое SNMP?
- Запросы и опрашивание
- OIDы и MIBы
- Ловушки
- SNMP версии 3 (опционально)

Что такое SNMP?

SNMP – ”простой протокол сетевого управления”

- Стандарт, сотни инструментов использующих протокол
- Поддерживается многими сетевыми устройствами

Основан на запросах/откликах: **GET / SET**

- Для мониторинго обычно используется GET

Идентификаторы объектов (OIDы)

- “Ключи” для идентификации каждой порции данных

Концепция MIB (база управляющей информации)

- Определяет набор взаимосвязаных OIDов

Что такое SNMP?

Типичные запросы

- Входящий/исходящий трафик на интерфейсе, ошибки
- Загрузка процессора
- Время работы
- Температура и другие OIDы, поддерживаемые производителем оборудования

Для машин (серверов или рабочих станций)

- Свободное место на диске
- Установленное программное обеспечение
- Список активных процессов
- ...

Windows и UNIX предоставляют агенты SNMP

Что такое SNMP?

Протокол UDP, порт 161

Различные версии

- V1 (1988) – RFC1155, RFC1156, RFC1157
  - Первая спецификация
- v2 – RFC1901 ... RFC1908 + RFC2578
  - Развивает v1, новые типы данных, лучшие методы получения информации (GETBULK)
  - Используется v2c (простая модель безопасности)
- v3 – RFC3411 ... RFC3418 (расширенная безопасность)

Обычно мы пользуемся SNMPv2 (v2c)

SNMP роли

Терминология:

- Менеджер (осуществляет мониторинг)
- Агент (выполняется на сетевом оборудовании/ на сервере)

Как это работает?

Основные команды

- GET (менеджер -> агент)
  - Запрос значения
- GET-NEXT (менеджер -> агент)
  - Запрос следующего значения (например для получения списка значений из таблицы)
- GET-RESPONSE (агент -> менеджер)
  - Ответ на GET/SET, или ошибка
- SET (менеджер -> агент)
  - Установка значение либо выполнение действия
- TRAP (агент -> менеджер)
  - Асинхронное сообщение от оборудования (потеря связи, температура выше порогового значения, ...)

OIDы и MIBы

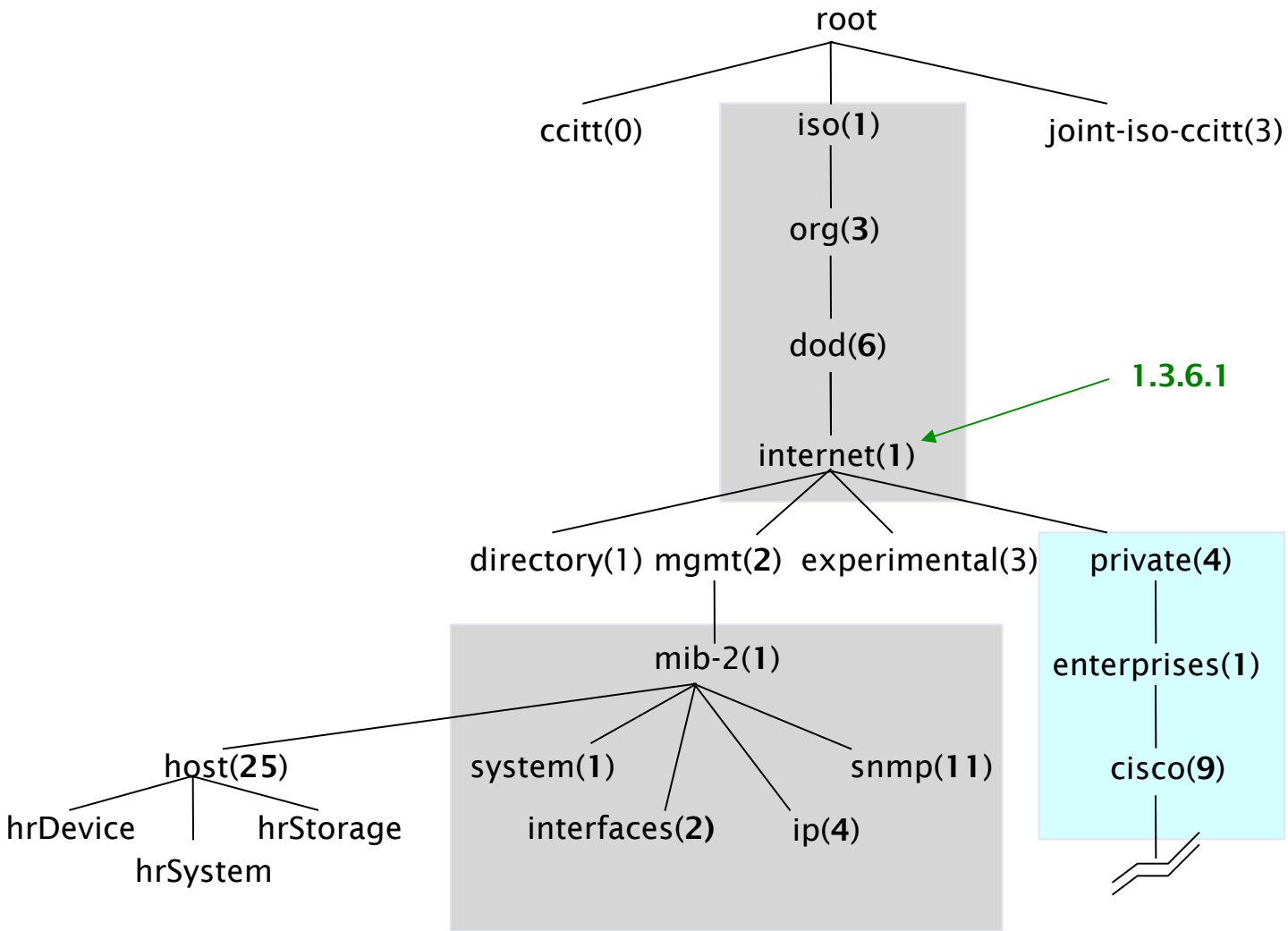
OID: Идентификатор объекта

- Уникальный ключ для идентификации порции данных в устройстве
- Одна и та же информация всегда определяется одним и тем же OID. Просто, не правда ли?
- OID – цепочка чисел переменной длины, разделяемая точками, например 1.3.6.1.2.1.1.3
- Организуется в рамках иерархической древовидной структуры для обеспечения уникальности (чем-то похоже на DNS)

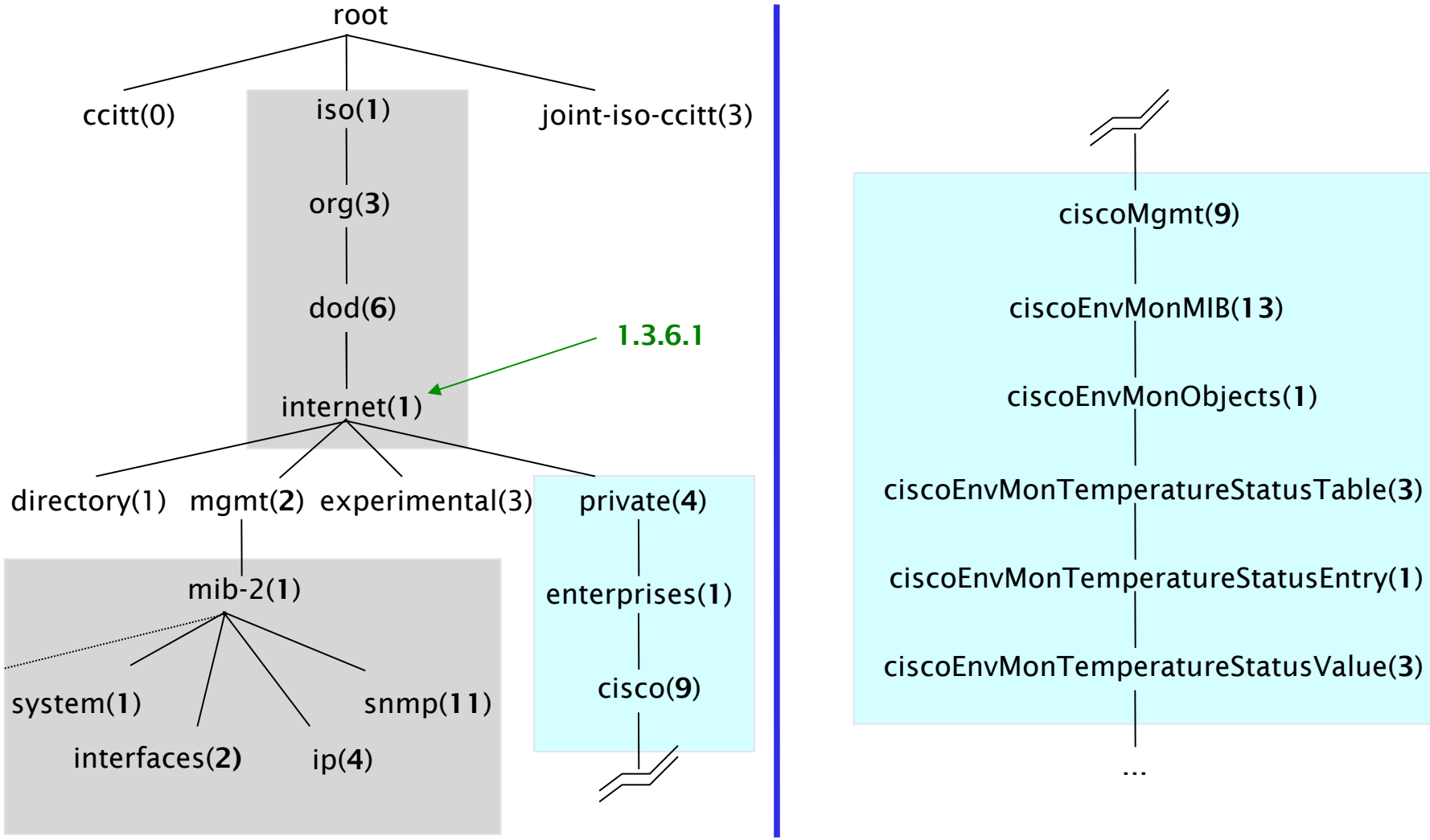
MIB: База управляющей информации

- Набор взаимосвязанных OIDов
- Соответствие числовых OIDов именам, удобным для человека

Дерево MIB


root
ccitt(0)
iso(1)
joint-iso-ccitt(3)
org(3)
dod(6)
1.3.6.1
internet(1)
directory(1)
mgmt(2)
experimental(3)
private(4)
mib-2(1)
enterprises(1)
host(25)
system(1)
snmp(11)
cisco(9)
hrDevice
hrStorage
hrSystem
interfaces(2)
ip(4)

Дерево MIB


root
ccitt(0)
iso(1)
joint-iso-ccitt(3)
org(3)
dod(6)
1.3.6.1
internet(1)
directory(1)
mgmt(2)
experimental(3)
private(4)
mib-2(1)
enterprises(1)
system(1)
snmp(11)
cisco(9)
interfaces(2)
ip(4)
ciscoMgmt(9)
ciscoEnvMonMIB(13)
ciscoEnvMonObjects(1)
ciscoEnvMonTemperatureStatusTable(3)
ciscoEnvMonTemperatureStatusEntry(1)
ciscoEnvMonTemperatureStatusValue(3)
...

Если бы адреса Email были OIDами

user@nsrc.org

стало бы чем то вроде:

user@nsrc.enterprises.private.internet.dod.org.iso

user@99999.1.4.1.6.3.1

за тем исключением, что запись “от корня” идет слева направо:

1.3.6.1.4.1.99999.117.115.101.114

Не беспокойтесь о количестве “ветвей” в дереве. Важно то, что OIDы уникальны.

Так обеспечивается то, что OIDы от разных производителей не пересекаются друг с другом

Численные OIDы – это то, чем реально оперирует протокол

The Internet MIB

- **directory**(1) Каталог OSI
- **mgmt**(2) Стандартные объекты RFC*
- **experimental**(3) Экспериментальные
- **private**(4) Зависящие от производителя*
- **security**(5) Безопасность
- **snmpV2**(6) Используемые самим SNMP

* На самом деле интересны только две ветви:

1.3.6.1.2.1 = Стандартные MIBы

1.3.6.1.4.1 = MIBы специфичные для производителей

OIDы и MIBы

Читаются слева направо

Компоненты OIDa разделяются точкой '.'

- `1.3.6.1.4.1.9. ...`

Каждому OIDy соответствует имя

- `.1.3.6.1.2.1.1.5 => sysName`

Полный путь в дереве:

- `.iso.org.dod.internet.mgmt.mib-2.system.sysName`

Как мы переводим OIDы в имена (и наоборот)?

- Используйте файлы MIBов!

Файлы MIBов

- Файлы MIBов определяют объекты, для которых можно сформировать запрос, и включают в себя
  - Имя объекта
  - Описание объекта
  - Тип данных (целое число, текст, список)
- Файлы MIBов представляют собой структурированный текст в формате ASN.1
- Примеры стандартных MIBов:
  - MIB-II – (RFC1213) – коллекция под-MIBов
  - HOST-RESOURCES-MIB (RFC2790)

MIBы - ПРИМЕР

```
sysUpTime OBJECT-TYPE
              SYNTAX  TimeTicks
              ACCESS  read-only
              STATUS  mandatory
              DESCRIPTION
                      "The time (in hundredths of a second) since the
                      network management portion of the system was last
                      re-initialized."
              ::= { system 3 }
```

sysUpTime OBJECT-TYPE

Определяет объект под названием `sysUpTime`.

SYNTAX TimeTicks

Этот объект имеет тип `TimeTicks`. Типы объектов определены в SMI, о котором мы только что упоминали.

ACCESS read-only

Этот объект можно читать (т.е., `get-request`), но не писать (т.е., `set-request`) с помощью SNMP

STATUS mandatory

Этот объект должен поддерживаться любым SNMP-агентом.

DESCRIPTION

Описание объекта

::= { system 3 }

Объект `sysUpTime` находится на третьей ветке от дерева объектов `system`.

Файлы MIBов - 2

Файлы MIBов также дают возможность интерпретировать значения, возвращаемые агентами

- Например, статус вентилятора может быть числом 1,2,3,4,5,6 – но что эти числа означают ?

MIBы - ПРИМЕР

```
CiscoEnvMonState ::= TEXTUAL-CONVENTION
        STATUS  current
        DESCRIPTION
                "Represents the state of a device being monitored.
                 Valid values are:

                 normal(1):          the environment is good, such as low
                                     temperature.

                 warning(2):         the environment is bad, such as temperature
                                     above normal operation range but not too
                                     high.

                 critical(3):        the environment is very bad, such as
                                     temperature much higher than normal
                                     operation limit.

                 shutdown(4):        the environment is the worst, the system
                                     should be shutdown immediately.

                 notPresent(5):      the environmental monitor is not present,
                                     such as temperature sensors do not exist.

                 notFunctioning(6): the environmental monitor does not
                                     function properly, such as a temperature
                                     sensor generates a abnormal data like
                                     1000 C.
```

Запросы к SNMP-агенту

Типичные команды запросов:

- `snmpget`
- `snmpwalk`
- `snmpstatus`
- `snmptable`

Синтаксис:

```
snmpXXX -c community -v1 host [oid]
snmpXXX -c community -v2c host [oid]
```

Запросы к SNMP-агенту

Рассмотрим примеры:

- `snmpstatus -c NetManage -v2c 10.10.0.254`
- `snmpget -c NetManage -v2c 10.10.0.254 ifNumber.0`
- `snmpwalk -c NetManage -v2c 10.10.0.254 ifDescr`

Запросы к SNMP-агенту

Community:

- Пароль, определяющий уровень доступа менеджера, осуществляющего запрос (только чтение либо чтение/запись)
- Это простейший способ аутентификации в SNMP

OID

- OID объекта, например, .1.3.6.1.2.1.1.5.0
- или эквивалентное имя объекта: sysName.0

Давайте запросим имя системы (используя OID выше)

- Зачем там .0? Что вы заметили?

Отказ SNMP: нет ответа?

Устройство может быть выключено либо недоступно

SNMP-агент на устройстве может не быть запущен

Устройство может быть настроено с другим паролем

Устройство может быть настроено не отвечать на запросы SNMP с вашего IP адреса

Во всех этих случаях вы не получите ответа

Переходя к упражнениям...

- Использование snmpwalk, snmpget
  - Файл конфигурации: `/etc/snmp/`**`snmp.`**`conf`
- Запуск SNMP-агента *(демона) под* Linux
  - Файл конфигурации: `/etc/snmp/`**`snmpd.`**`conf`
- Загрузка MIBов
- Настройка SNMPv3 (не обязательно)

Ссылки

- *Essential SNMP* (O'Reilly Books) Douglas Mauro, Kevin Schmi
- *Основы SNMP на сайте Cisco*
  http://www.cisco.com/warp/public/535/3.html
  http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm
- Википедия:
  http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol
- IP Monitor броузер MIB
  http://support.ipmonitor.com/mibs_byoidtree.aspx
  Броузер Cisco MIB: http://tools.cisco.com/Support/SNMP/do/BrowseOID.do
- Броузер MIB на Java (открытые исходные тексты)
  http://www.kill-9.org/mbrowse
  http://www.dwipal.com/mibbrowser.htm (Java)
- SNMP Link – подборка ресурсов о SNMP
  http://www.snmplink.org/
- Net-SNMP – инструменты работы с SNMP с открытыми исходниками
  http://net-snmp.sourceforge.net/
- Интеграция с Nagios http://www.cisl.ucar.edu/nets/tools/nagios/SNMP-traps.html

Необязательный материал

SNMP версии 3

SNMP и защита

- SNMP версий 1 и 2c не защищены
- SNMP версии 3 создан, чтобы это исправить

- Компоненты
  - Диспетчер
  - Подсистема обработки сообщений
  - Подсистема защиты
  - Подсистема контроля доступа

SNMP версии 3 (SNMPv3)

The most common module is based in user, or a “User-based Security Model”

- **Authenticity and integrity:** Keys are used for users and messages have digital signatures generated with a hash function (MD5 or SHA)
- **Privacy:** Messages can be encrypted with secret-key (private) algorithms (DES)
- **Temporary validity:** Utilizes a synchronized clock with a 150 second window with sequence checking.

Security Levels

noAuthPriv

- No authentication, no privacy

authNoPriv

- Authentication with no privacy

authPriv

- Authentication with privacy

Cisco SNMPv3 configuration

```
snmp-server view  vista-ro   internet  included
snmp-server group ReadGroup  v3 auth read vista-ro
snmp-server user  admin ReadGroup v3 auth md5  xk122r56
```

Or alternatively:

```
snmp-server user  admin  ReadGroup v3 auth md5 xk122r56
    priv des56 D4sd#rr56
```

Net-SNMP SNMPv3 configuration

```
# apt-get install snmp snmpd
# net-snmp-config --create-snmpv3-user -a "xk122r56" admin
  /usr/sbin/snmpd
# snmpwalk -v3 -u admin -l authNoPriv -a MD5 -A "xk122r56"
    127.0.0.1
```