**Лабораторная работа №26 Тема:** Управление сетями на основе протокола SNMP.

**Цель:** Изучить процесс управлениями сетями на основе протокола SNMP, изучить протокол SNMP.

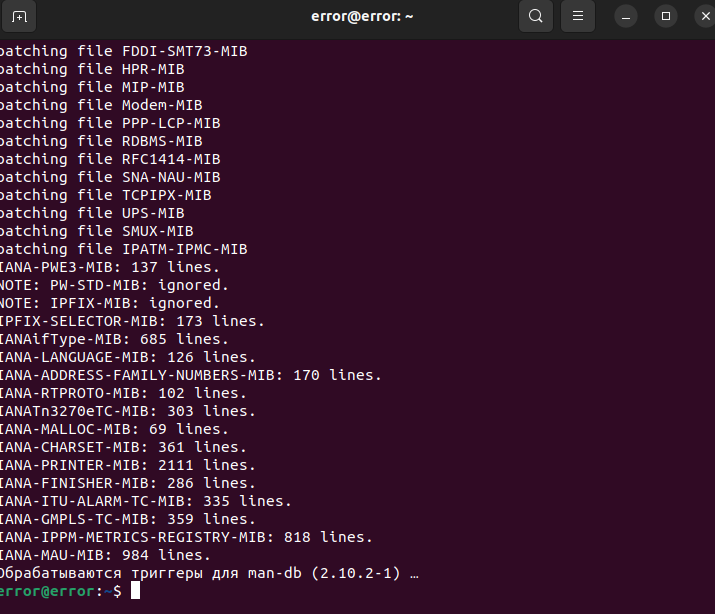
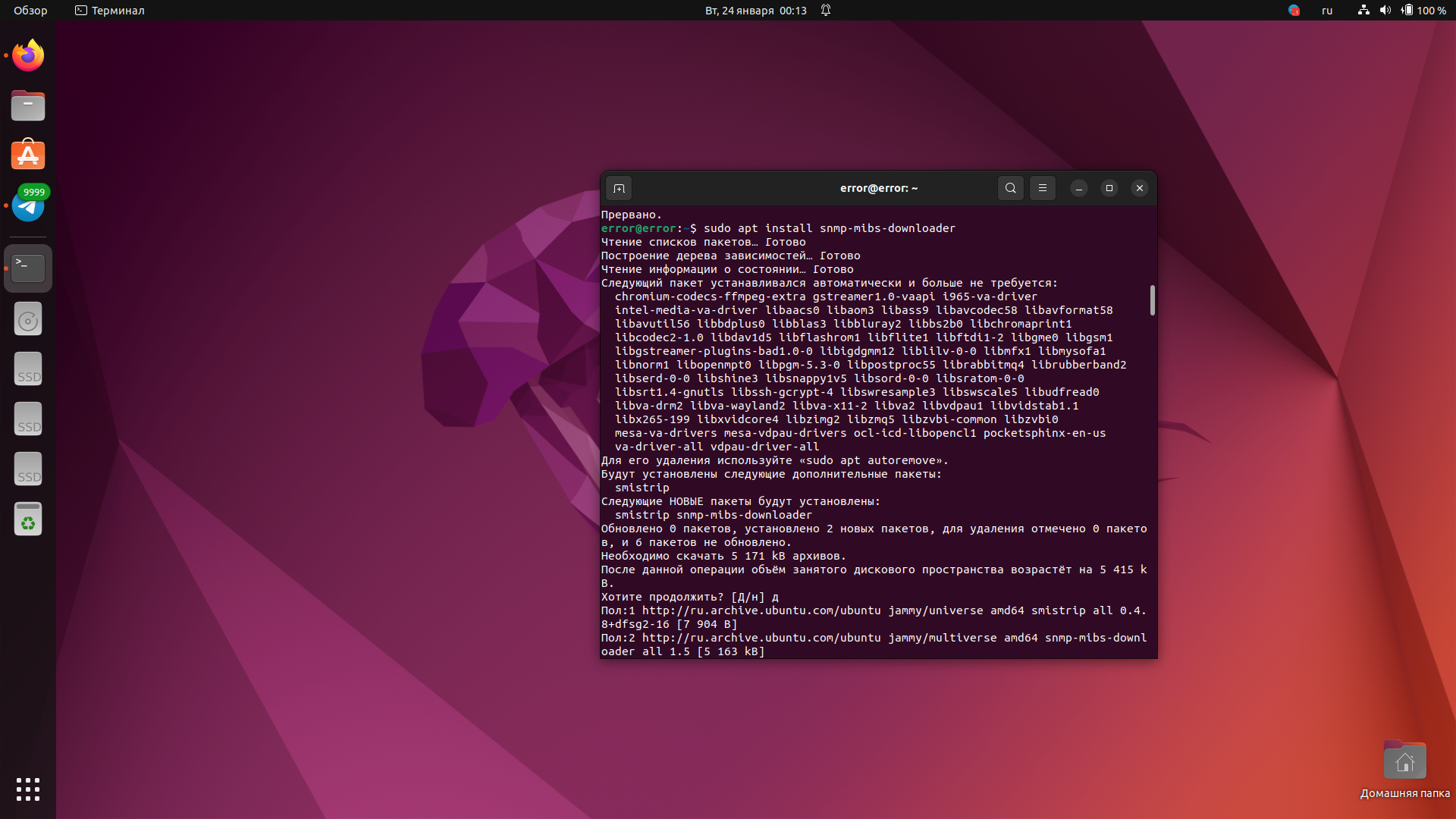
# Ход работы:

**Часть 1. Изучение теоретического материала.**

1. Ознакомиться с теоретическим материалом.

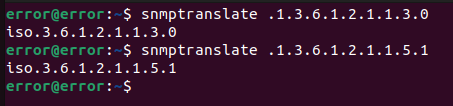
# Часть 2. Установка и настройка программных средств

1. Установить в VirtualBox (на рабочих столах) - ОС Ubuntu. (Дистрибутив в файлообменнике \\10.7.3.3\Shared\soft)
2. Запустить Ubuntu.
3. Установить snmp пакет, выполнив в gnome-terminal: *sudo apt-get install snmp*



# Часть 3. Изучение утилит snmp (Описание утилит приведено в теоретических материалах).

1. Изучить работу утилит snmp:
2. Выполнить: snmptranslate .1.3.6.1.2.1.1.3.0
3. Выполнить: snmptranslate 1.3.6.1.2.1.5.1



1. Выполнить: snmpget -c demopublic -v 2c test.net-snmp.org system.sysUpTime.0



10.4.9.102

Выполнить: snmpgetnext -v 2c -c demopublic test.net-snmp.

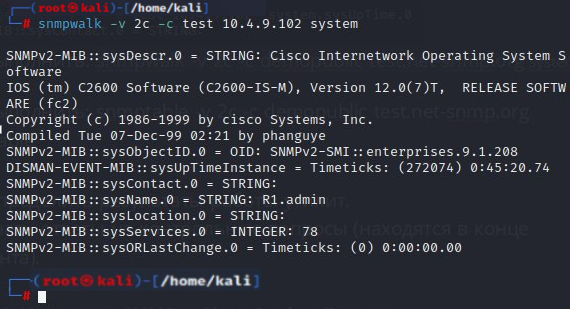
1. org system.sysUpTime.0



Выполнить snmpwal

k -v 2c -c test

1. 10.4.9.102 system

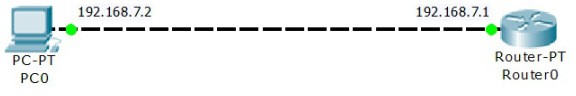


Выполнить: snmptable -v 2c -c demopublic test.net-snmp.org sysORTable



1. Определить результаты работы утилит.
2. Знать ответы на контрольные вопросы (находятся в конце документа).

# Часть 4. Изучение SNMP в Cisco Packet Tracer

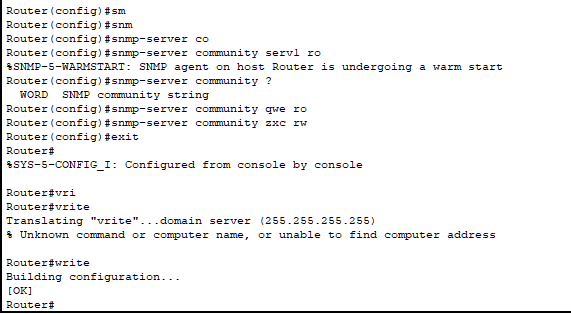


* 1. Добавить роутер (Router-PT) и ПК.
  2. Настроить интерфейсы:
  3. Настроить роутер:

*Router# configure terminal*

*Router(config)# snmp­server community [name1] ro Router(config)# snmp­server community [name2] rw Router(config)# ctrl+z*

*Router# write*



*Тут я немного по клавишам не попадал*

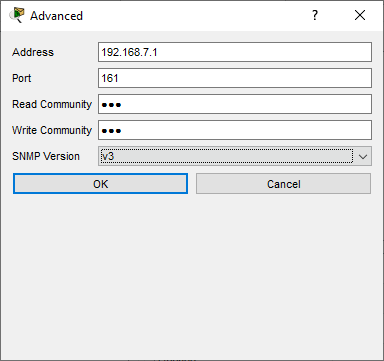
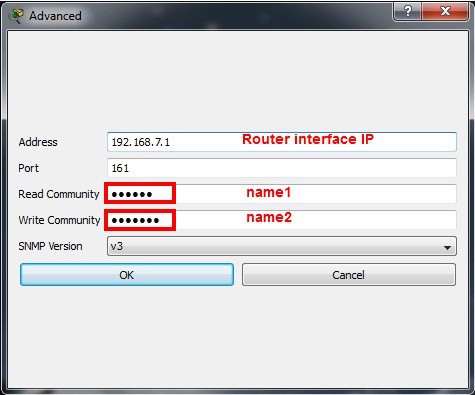
* 1. Настроить ПК:

Выделите ПК, откройте MIB-browser, во вкладке введите следующие значения:

*Address [IP address of router’s connected interface]*

*Port 161*

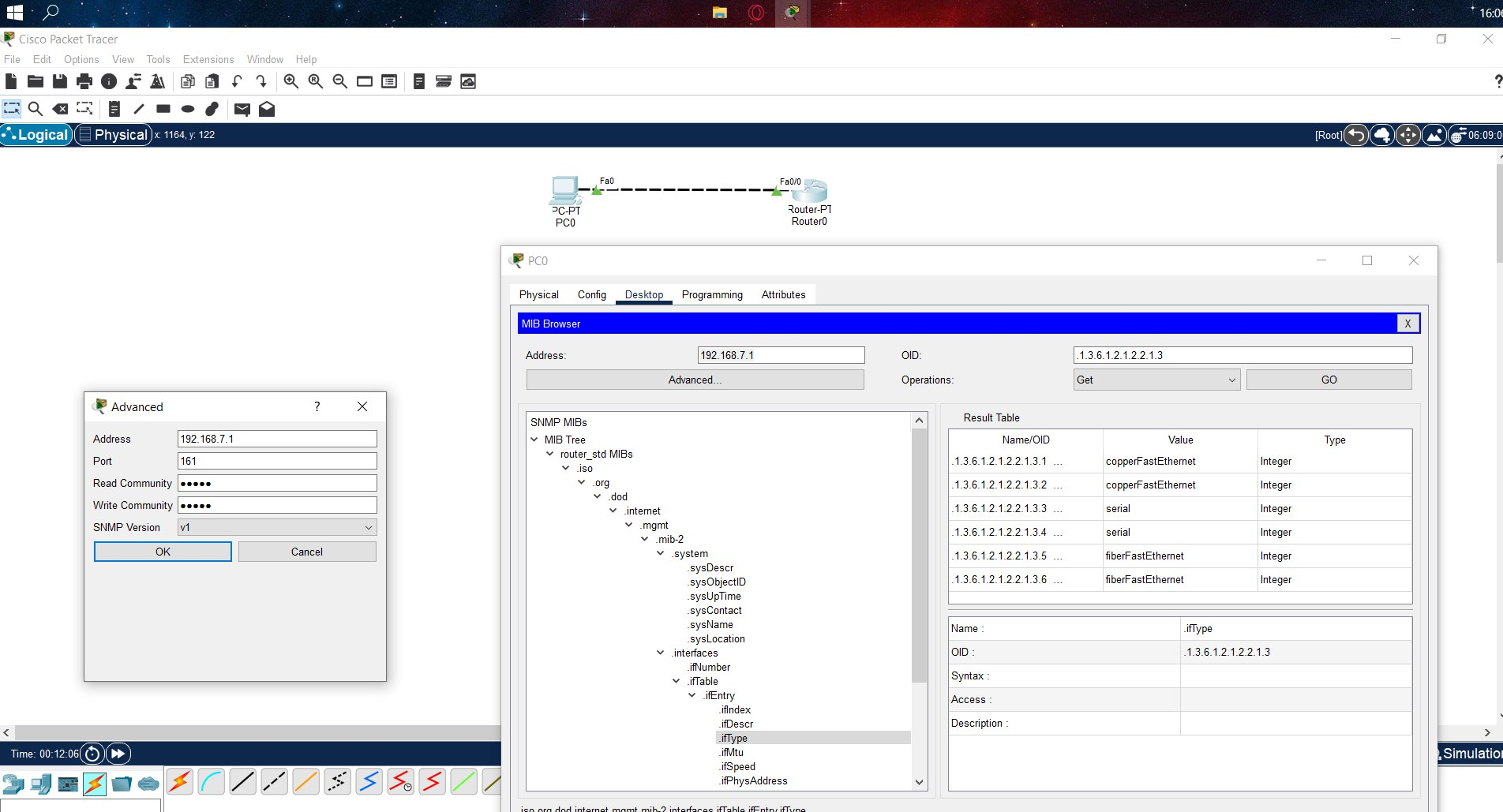
*Read Community [name1] Write community [name2] SNMP Version v3*



* 1. В MIB-Browser в ПК для роутера:
* изменить имя роутера: MyRouter



* получить список интерфейсов роутера
* включить интерфейс FastEthernet1/0



# Теоретический материал SNMP

SNMP (англ. Simple Network Management Protocol — простой протокол управления сетями) — это протокол управления сетями связи на основе архитектуры UDP. Устройства, которые обычно поддерживают SNMP это маршрутизаторы, коммутаторы, серверы, рабочие станции, принтеры, модемы и т.д. SNMP является компонентом стека протоколов TCP/IP, как это определено Инженерным советом Интернет (Internet Engineering Task Force, IETF). Он состоит из набора стандартов сетевого управления, включая протокол передачи данных прикладного уровня, схему базы данных и набора объектов.

Обычно при использовании SNMP присутствуют управляемые и

управляющие системы. В состав управляемой системы входит компонент, называемый агентом, который отправляет отчёты управляющей системе. По существу SNMP агенты передают управленческую информацию на управляющие системы как переменные (такие как «свободная память», «имя системы»,

«количество работающих процессов»).

Управляющая система может получить информацию через операции протокола GET, GETNEXT и GETBULK. Агент может самостоятельно без запроса отправить данные, используя операцию протокола TRAP или INFORM. Управляющие системы могут также отправлять конфигурационные обновления или контролирующие запросы, используя операцию SET для непосредственного управления системой. Операции конфигурирования и управления используются только тогда, когда нужны изменения в сетевой инфраструктуре. Операции мониторинга обычно выполняются на регулярной основе.

Переменные, доступные через SNMP, организованы в иерархии. Эти иерархии и другие метаданные (такие, как тип и описание переменной) описываются Базами Управляющей Информации.

# Команды SNMP

|  |  |  |
| --- | --- | --- |
| Команда SNMP | Тип PDU | Назначение |
| GET-request | 0 | Получить значение указанной переменной или информацию о состоянии сетевого элемента; |
| GET\_next\_request | 1 | Получить значение переменной, не зная точного ее имени |

|  |  |  |
| --- | --- | --- |
|  |  | (следующий логический идентификатор на дереве MIB); |
| SET-request | 2 | Присвоить переменной соответствующее значение. Используется для описания действия, которое должно быть выполнено; |
| GET response | 3 | Отклик на GET-request, GET\_next\_request и SET-request. Содержит также информацию о состоянии (коды ошибок и другие данные); |
| TRAP | 4 | Отклик сетевого объекта на событие или на изменение состояния. |
| GetBulkRequest | 5 | Запрос пересылки больших объемов данных, например, таблиц. |
| InformRequest | 6 | Менеджер обращает внимание партнера на определенную информацию в MIB. |
| SNMPv3-Trap | 7 | Отклик на событие (расширение по отношению v1 и v2). |
| Report | 8 | Отчет (функция пока не задана). |

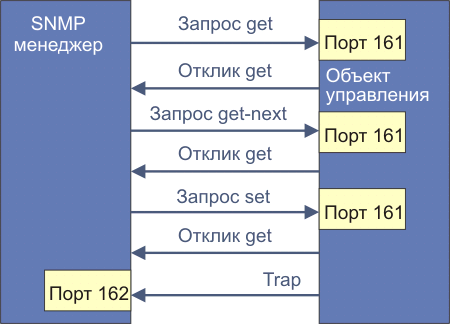
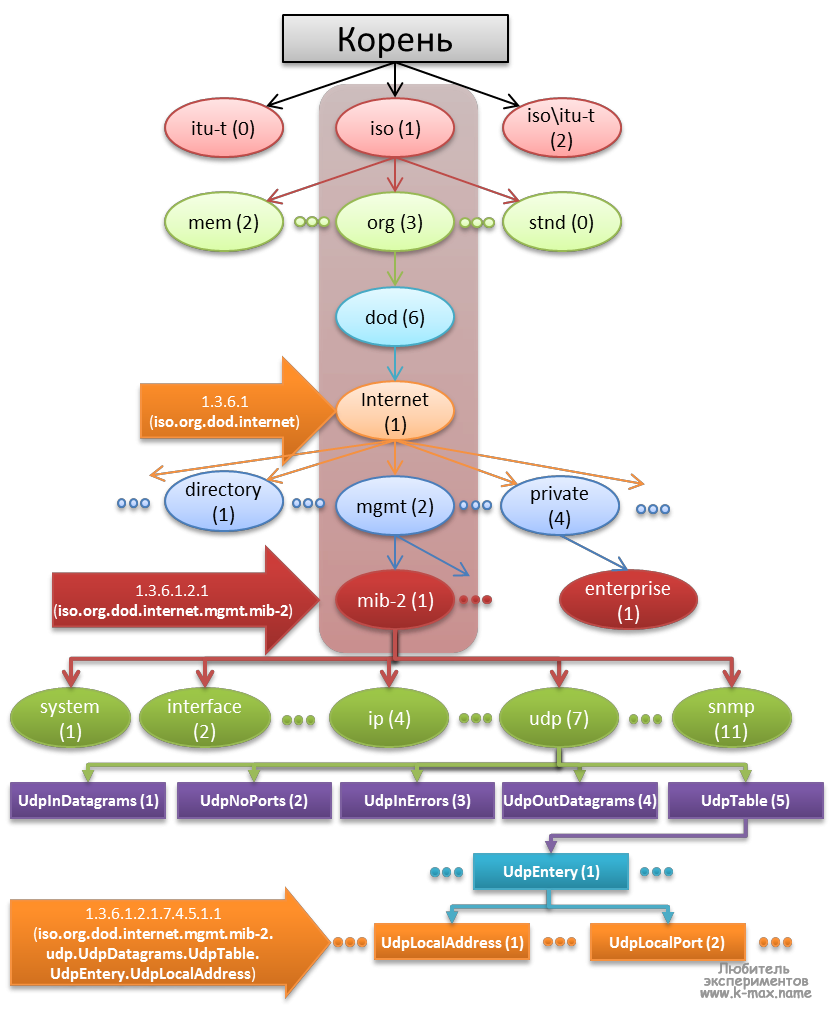


Рис. Схема запросов/откликов SNMP

# Management Information Bases (MIBs)



SNMP не определяет, какую информацию (какие переменные) управляемая система должна предоставлять. Наоборот, SNMP

использует расширяемую модель, в которой доступная информация определяется Базами Управляющей Информации (MIB — Management Information Base). Базы Управляющей Информации описывают структуру управляющей информации устройств. Они используют иерархическое пространство имён, содержащее уникальный идентификатор объекта (англ. object identifier (OID)). Грубо говоря, каждый уникальный идентификатор объекта идентифицирует переменную, которая может быть прочитана или установлена через SNMP.

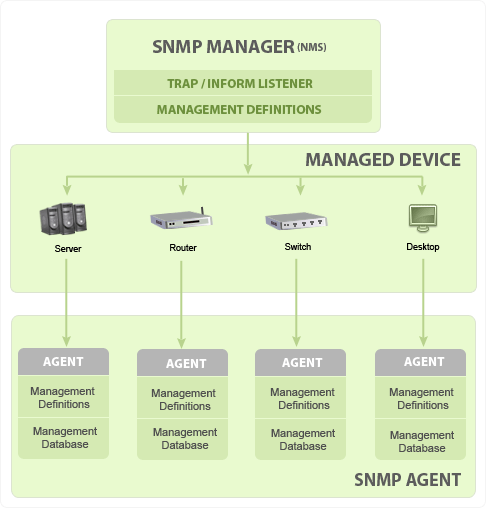
Иерархия MIB может быть изображена как дерево с безымянным корнем, уровни которого присвоены разными организациями. На самом высоком уровне MIB OIDы принадлежат различным организациям, занимающимся стандартизацией, в то время как на более низком уровне OIDы выделяются ассоциированными организациями. Эта модель обеспечивает управление на всех слоях сетевой модели OSI, так как MIBы могут быть определены для любых типов данных и операций.

**Управляемый объект** — это одна из любого числа характеристик, специфических для управляемого устройства. Управляемый объект включает в себя один или более экземпляров объекта (идентифицируемых по OID), которые на самом деле переменные.

Существует два типа управляемых объектов:

Скалярные объекты определяют единственный экземпляр объекта.

Табличные объекты определяют множественные, связанные экземпляры объектов, которые группируются в таблицах MIB. Идентификатор объекта (OID) уникально идентифицирует управляемый объект в иерархии MIB.



# SNMP в Linux

В большинстве [дистрибутивов Linux](http://www.google.com/url?q=http%3A%2F%2Fwww.k-max.name%2Fcategory%2Flinux%2F&sa=D&sntz=1&usg=AFQjCNFAAn6239zUDc51OdbxszS8xF4pHQ) для работы с SNMP используется пакет net-snmp (RedHat) и snmp + snmpd (в Debian в snmp лежит клиентская часть, а в snmpd – серверная часть),

который позволяет использовать протокол SNMP посредством отправки и получения PDU. После [установки пакета(ов) в linux](http://www.google.com/url?q=http%3A%2F%2Fwww.k-max.name%2Flinux%2Fupravlenie-programmnym-obespecheniem-v-linux%2F&sa=D&sntz=1&usg=AFQjCNFf1dvGdGnGr1fKSb2u3fck_8F9Dw) появятся следующие инструменты (перечислены не все):

* snmptranslate - Перевод MIB OID имён между цифровой и текстовой представлениями.
* snmpget - Взаимодействует с агентом, используя PDU GetRequest запросы.
* snmpgetnext - Взаимодействует с агентом, используя PDU GetNextRequest запросы.
* snmpbulkget - Взаимодействует с агентом, используя PDU GetBulkRequest запросы.
* snmpwalk - Получает поддерево объектов OID из MIB базы агента с помощью PDU GetNextRequest запросов. Если OID не задан, то команда получает дерево, начиная от MIB-2 (iso.org.dod.internet.mgmt.mib-2 (1.3.6.1.2.1))
* snmpbulkwalk - Получает поддерево объектов OID из MIB базы агента с помощью PDU GetBulkRequest запросов.
* snmpset - Взаимодействует с агентом, используя PDU SetRequest запросы.
* snmptrap - Посылает SNMP Trap или информационные сообщения.
* snmptest - Взаимодействует с сетью, используя SNMP запросы.

Основной и часто используемой из всех указанных команд, является snmpwalk. При указании данной команды, без OID она попытается получить все объекты из ветки iso.org.dod.internet.mgmt.mib-2.

# Категории объектов MIB

MIB-категория включает в себя информацию о (префикс=1.3.6.1.2.1)

|  |  |  |
| --- | --- | --- |
| MIB-категория | Описание | Код |
| system | Операционная система ЭВМ или маршрутизатора. | 1 |
| Interfaces | Сетевой интерфейс. | 2 |
| addr.trans | Преобразование адреса (напр., с помощью ARP). | 3 |
| IP | Программная поддержка протоколов Интернет. | 4 |
| ICMP | Программное обеспечение ICMP-протокола. | 5 |
| TCP | Программное обеспечение TCP-протокола. | 6 |
| UDP | Программное обеспечение UDP-протокола. | 7 |
| EGP | Программное обеспечение EGP-протокола. | 8 |
| cmot | (группа в настоящее время не используется). | 9 |
| Trans | Transmission | 10 |

|  |  |  |
| --- | --- | --- |
| SNMP | Программное обеспечение SNMP-протокола. | 11 |

# Системные переменные

Системные переменные MIB (префикс=1.3.6.1.2.1.1)

|  |  |  |
| --- | --- | --- |
| Системная переменная | Описание | Код |
| Sysdescr | Текстовое описание объекта; | 1 |
| Sysobjectid | Идентификатор производителя в рамках дерева 1.3.6.1.4.1 | 2 |
| Sysuptime | Время с момента последней загрузки системы (timeticks); | 3 |
| Syscontact | Имя системного менеджера и способы связи с ним; | 4 |
| Sysname | Полное имя домена; | 5 |
| Syslocation | Физическое местоположение системы; | 6 |
| Sysservice | Величина, которая характеризует услуги, предоставляемые узлом (сумма номеров уровней модели OSI); | 7 |

# Переменные интерфейсов

Переменные **IFtable** (интерфейсы; префикс=1.3.6.1.2.1.2)

|  |  |  |  |
| --- | --- | --- | --- |
| Переменная описания интерфейсов (iftable) | Тип данных | Описание | ifEntry |
| IFindex | integer | Список интерфейсов от 1 до ifnumber. | 1 |
| IfDescr | displaystring | Текстовое описание интерфейса. | 2 |
| IfType | integer | Тип интерфейса, например, 6  - ethernet; 9 - 802.5 маркерное кольцо; 23 - PPP; 28 - SLIP. | 3 |
| IfNumber | integer | Число сетевых интерфейсов. |  |
| IfMTU | integer | mtu для конкретного интерфейса; | 4 |
| IfSpeed | gauge | Скорость в бит/с. | 5 |
| IfPhysaddress | physaddress | Физический адрес или строка нулевой длины для интерфейсов без физического адреса (напр. последовательный). | 6 |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| IfAdminStatus | [1...3] | Требуемое состояние интерфейса: 1 - включен; 2 - выключен; 3 - тестируется. | 7 |
| IfOperStatus | [1...3] | Текущее состояние интерфейса: 1 - включен; 2 - выключен; 3 - тестируется. | 8 |
| IfLastchange | timeticks | Sysuptime, когда интерфейс оказался в данном состоянии. | 9 |
| IfInOctets | counter | Полное число полученных байтов. | 10 |
| IfInUcastpkts | counter | Число пакетов, доставленных на верхний системный уровень (unicast). | 11 |
| IfInNUcastpkts | counter | Число пакетов, доставленных на верхний системный уровень (unicast). | 12 |
| IfInDiscads | counter | Число полученных но отвергнутых пакетов. | 13 |
| IfInErrors | counter | Число пакетов, полученных с ошибкой; | 14 |
| IfInUnknownProtos | counter | Число пакетов, полученных с ошибочным кодом протокола; | 15 |

|  |  |  |  |
| --- | --- | --- | --- |
| IfOutOctets | counter | Число отправленных байтов; | 16 |
| IfOutUcastPkts | counter | Число unicast- пакетов, полученных с верхнего системного уровня; | 17 |
| IfOutNucastPkts | counter | Число мультикастинг- и широковещательных пакетов, полученных с верхнего системного уровня; | 18 |
| IfOutDiscads | counter | Количество отвергнутых пакетов из числа отправленных; | 19 |
| IfOutErrors | counter | Число отправленных пакетов, содержащих ошибки; | 20 |
| IfOutQlen | gauge | Число пакетов в очереди на отправку; | 21 |

Каждый протокол (например IP) имеет свою таблицу преобразования адресов. Для IP это ipnettomediatable. Способ пропечатать эту таблицу с помощью программы SNMPI описан ниже.

Стандарт на структуру управляющей информации (SMI) требует, чтобы все MIB-переменные были описаны и имели имена в соответствии с ASN.1 (abstract syntax notation 1, формализованный синтаксис). ASN.1 является формальным языком, который обладает двумя основными чертами: используемая в документах нотация легко читаема и понимаема,

а в компактном кодовом представлении информация может использоваться коммуникационными протоколами. В SMI не используется полный набор типов объектов, предусмотренный в ASN.1, разрешены только следующие типы примитивов: integer, octet string, object identifier и null. Практически в протоколе SNMP фигурируют следующие виды данных:

**integer**. Некоторые переменные объявляются целыми (integer) с указанием начального значения или с заданным допустимым диапазоном значений (в качестве примера можно привести номера UDP- или TCP-портов).

**octet string** (последовательность байтов). В соответствии с требованиями BER (basic encoding rules, ASN.1) последовательность октетов должна начинаться с числа байт в этой последовательности (от 0 до n).

**object identifier** (идентификатор объекта). Имя объекта, представляющее собой последовательность целых чисел, разделенных точками. Например, 192.148.167.129 или 1.3.6.1.2.1.5.

**null.** Указывает, что соответствующая переменная не имеет значения.

**displaystring**. Строка из 0 или более байт (но не более 255), которые представляют собой ASCII-символы. Представляет собой частный случай octet string.

**physaddress**. Последовательность октетов, характеризующая физический адрес объекта (6 байт для Ethernet). Частный случай object identifier.

**Сетевой адрес**. Допускается выбор семейства сетевых протоколов. В рамках ASN.1 этот тип описан как choice, он позволяет выбрать протокол из семейства протоколов. В настоящее время идентифицировано только семейство протоколов Интернет.

**IP-адрес**. Этот адрес используется для определения 32-разрядного Интернет-адреса. В нотации ASN.1 - это octet string.

**time ticks** (такты часов). Положительное целое число, которое используется для записи, например, времени последнего изменения параметров управляемого объекта, или времени последней актуализации базы данных. Время измеряется в сотых долях секунды.

**gauge** (масштаб). Положительное целое число в диапазоне 0 - (232-1), которое может увеличиваться или уменьшаться. Если эта переменная достигнет величины 232-1, она будет оставаться неизменной до тех пор пока не будет обнулена командой сброс. Примером такой переменной может служить tcpcurresta, которая характеризует число TCP соединений, находящихся в состоянии established или close\_wait.

**counter** (счетчик). Положительное целое число в диапазоне 0 - (232-1), которое может только увеличиваться, допуская переполнение.

**sequence**. Этот объект аналогичен структуре в языке Си. Например, MIB определяет sequence с именем udpentry, содержащую информацию об активных UDP-узлах. В этой структуре содержится две записи:

1. UDPlocaladdress типа ipaddress, содержит местные IP-адреса.
2. UDPlocalport типа integer, содержит номера местных портов. **SEQUENCE OF**. Описание вектора, все элементы которого имеют один и тот же тип. Элементы могут представлять собой простые объекты, например, типа целое. В этом случае мы имеем одномерный список. Но элементами вектора могут быть объекты типа SEQUENCE, тогда этот вектор описывает двумерный массив. В Интернет MIB каждый объект должен иметь имя (object identifier), синтаксис и метод кодировки.

Стандарт ASN.1 определяет форму представления информации и имен. Имена переменных MIB соответствуют в свою очередь стандартам ISO и CCITT. Структура имен носит иерархический характер, отображенный на рис. 4.4.13.1.1.

Рис. Структура идентификаторов переменных в MIB

В приведенной ниже таблице охарактеризованы четыре простые переменные, идентификаторы которых помещены в нижней части рис. 4.4.13.1.1. Все эти переменные допускают только чтение.

# Контрольные вопросы:

# Контрольные вопросы:

1. Для чего используется SNMP?

*SNMP (Simple Network Management Protocol) представляет собой стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP, который позволяет отслеживать управляемые сетевые устройства, включая маршрутизаторы, сетевые коммутаторы, серверы, принтеры и другие устройства, которые включены через IP через единую систему управления/программное обеспечение.*

1. Что такое MIB?

*Management Information Base (MIB, база управляющей информации) - виртуальная база данных, используемая для управления объектами в сети связи. Наиболее часто это понятие связывают с Simple Network Management Protocol (SNMP), но также оно используется в более широком смысле - в контексте модели управления сети OSI/ISO.*

1. Назначение утилиты snmptranslate?

*Перевод MIB OID имён между цифровой и текстовой представлениями.*

1. Назначение утилиты snmpget?

*Взаимодействует с агентом, используя PDU GetRequest запросы.*