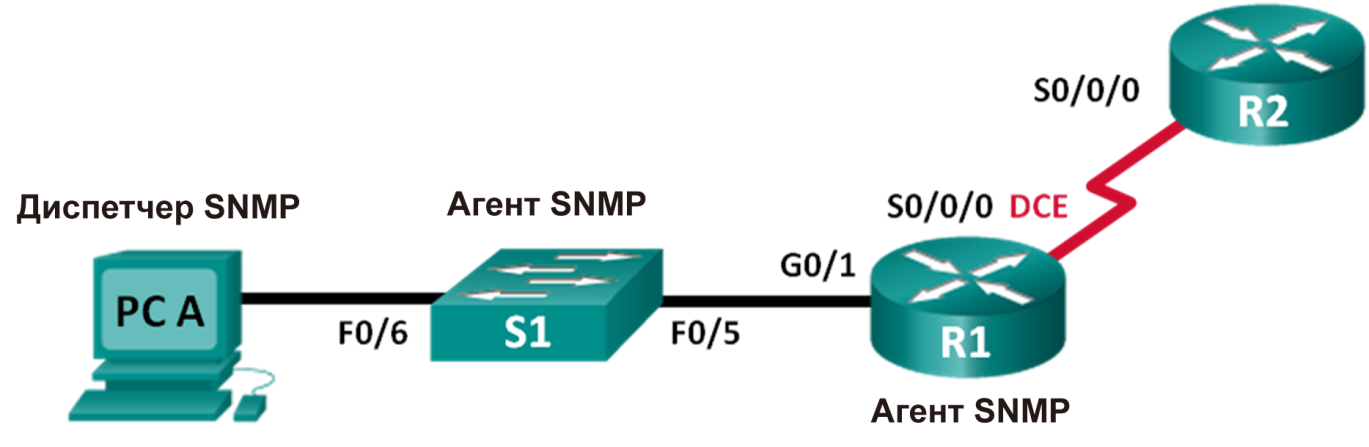
10 модуль Лабораторная работа. Настройка SNMP v2 и 3

1. Топология



1. Таблица адресации

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Устройство | Интерфейс | IP-адрес | Маска подсети | Шлюз по умолчанию |
| R1 | G0/1 | 192.168.1.1 | 255.255.255.0 | Н/Д (недоступно) |
| S0/0/0 | 192.168.2.1 | 255.255.255.252 | Н/Д (недоступно) |
| R2 | S0/0/0 | 192.168.2.2 | 255.255.255.252 | Н/Д (недоступно) |
| S1 | VLAN 1 | 192.168.1.2 | 255.255.255.0 | Н/Д (недоступно) |
| PC-A | NIC | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 |

Задачи

Часть 1. Создание сети и настройка базовых параметров устройства

Часть 2. Настройка диспетчера и агента SNMPv2

Часть 3. Настройка диспетчера и агента SNMPv3

1. Общие сведения/сценарий

Протокол SNMP (Simple Network Management Protocol — простой протокол управления сетями) — это протокол управления сетью и стандарт IETF, который может использоваться как для мониторинга сети, так и для контроля клиентов в ней. SNMP может использоваться для получения и настройки переменных, связанных с состоянием и настройкой сетевых машин, таких как маршрутизаторы и коммутаторы, а также клиентские компьютеры сети. Диспетчер SNMP может опрашивать агенты SNMP для получения данных, либо данные могут автоматически отправляться на диспетчер SNMP путем настройки ловушек на агентах SNMP.

В ходе этой лабораторной работы вы выполните загрузку, установку и настройку ПО для управления SNMP на компьютере PC-A. Также вы настроите маршрутизатор и коммутатор Cisco в качестве агентов SNMP. После получения сообщений с уведомлением SNMP от агента SNMP вы должны будете преобразовать коды MIB/ID объекта (OID), чтобы получить подробную информацию данных сообщений с помощью Cisco SNMP Object Navigator.

**Примечание**. В практических лабораторных работах CCNA используются маршрутизаторы с интегрированными сервисами (ISR) Cisco 1941 с операционной системой Cisco IOS версии 15.4(3) (образ universalk9). Также используются коммутаторы Cisco Catalyst 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, а также других версий операционной системы Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах. Правильные идентификаторы интерфейса см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

**Примечание**. Убедитесь, что у всех маршрутизаторов и коммутаторов была удалена загрузочная конфигурация. Если вы не уверены, обратитесь к инструктору.

**Примечание**. Выполнение команд **snmp-server** в этой лабораторной работе приведет к отправке коммутатором Cisco 2960 предупреждающего сообщения при сохранении файла конфигурации в NVRAM. Чтобы избежать этого сообщения с предупреждением, убедитесь, что коммутатор использует шаблон **lanbase-routing**. Шаблон IOS контролируется диспетчером базы данных коммутатора (SDM). При изменении предпочитаемого шаблона новый шаблон будет использоваться после перезагрузки, даже если конфигурация не сохраняется.

S1# **show sdm prefer**

Используйте следующие команды, чтобы назначить шаблон **lanbase-routing** в качестве шаблона SDM по умолчанию.

S1# **configure terminal**

S1(config)# **sdm prefer lanbase-routing**

S1(config)# **end**

S1# **reload**

1. Необходимые ресурсы

* 2 маршрутизатора (Cisco 1941 с операционной системой Cisco IOS 15.4(3) (универсальный образ) или аналогичная модель)
* 1 коммутатор (Cisco 2960 с ПО Cisco IOS 15.0(2) с образом lanbasek9 или аналогичная модель)
* 1 ПК (ОС Windows с программой эмуляции терминалов, например Tera Term, диспетчер SNMP, например браузер SNMP MIB от ManageEngine, и Wireshark)
* Консольные кабели для настройки устройств на базе Cisco IOS через консольные порты
* Кабели Ethernet и последовательные кабели согласно топологии
* ПО для управления SNMP (браузер SNMP MIB от ManageEngine)

1. Создание сети и настройка базовых параметров устройства

В части 1 вам предстоит настроить топологию сети и сделать базовую настройку устройств.

* 1. Создайте сеть согласно топологии.
  2. Настройте компьютер.
  3. Инициализируйте и перезагрузите коммутатор и маршрутизаторы при необходимости.
  4. Произведите настройку базовых параметров маршрутизаторов и коммутатора.
     1. Отключите DNS-поиск.
     2. Настройте имена устройств в соответствии с топологией.
     3. Настройте IP-адреса в соответствии с таблицей адресации. (На этом этапе не настраивайте и не включайте интерфейс VLAN 1 на коммутаторе S1.)
     4. Назначьте **cisco** в качестве пароля консоли и VTY и включите запрос пароля при входе в систему.
     5. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму EXEC.
     6. Настройте **logging synchronous**, чтобы сообщения от консоли не могли прерывать ввод команд.
     7. Убедитесь в наличии подключения между PC-A и R1 и между маршрутизаторами с помощью команды **ping**.
     8. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

1. Настройка диспетчера и агента SNMPv2

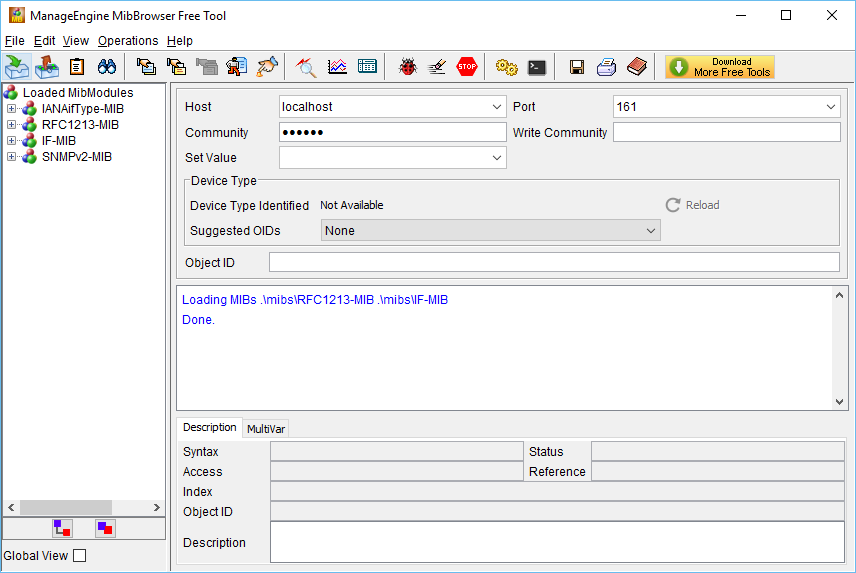
В части 2 вы должны будете установить ПО для управления SNMP и настроить его на PC-A, а также настроить R1 и S1 в качестве агентов SNMP.

* 1. Установите программу управления SNMP.
     1. Загрузите и установите браузер SNMP MIB от ManageEngine, который доступен по следующему URL-адресу: <https://www.manageengine.com/products/mibbrowser-free-tool/download.html>. Вам будет необходимо указать адрес электронной почты для загрузки ПО.
     2. Запустите программу ManageEngine MibBrowser.
        1. Если появится сообщение об ошибке, связанной со сбоем загрузки информационных баз управления, выполните следующие действия. Откройте папку MibBrowser Free Tool:

32-разрядная ОС: C:\Program Files (x86)\ManageEngine\MibBrowser Free Tool

64-разрядная ОС: C:\Program Files\ManageEngine\MibBrowser Free Tool

* + - 1. Правой кнопкой мыши нажмите папку **mibs** и выберите вкладку **Security**. Нажмите **Edit** (Изменить). Выберите **Users** (Пользователи). Нажмите **Full control** (Полный контроль). Нажмите **ОК**, чтобы изменить разрешение.
      2. Повторите предыдущее действие для папки **conf**.
      3. Повторно запустите программу ManageEngine MibBrowser.



* 1. Настройте агент SNMPv2.

В режиме глобальной настройки на коммутаторе S1 введите следующие команды для его настройки в качестве агента SNMP. В строке 1 ниже строка сообщества SNMP — **ciscolab** с правами только на чтение, а именованный список контроля доступа SNMP\_ACL определяет, каким хостам разрешено получать информацию SNMP от S1. В строках 2 и 3 команды расположения и контактной информации агента SNMP предоставляют описательную контактную информацию. В строке 4 указаны IP-адрес хоста, который будет получать уведомления SNMP, версия SNMP и строка сообщества. В строке 5 включаются все SNMP-ловушки по умолчанию, а строки 6 и 7 создают именованный список контроля доступа, который определяет, каким хостам разрешено получать информацию SNMP от коммутатора.

S1(config)# **snmp-server community ciscolab ro SNMP\_ACL**

S1(config)# **snmp-server location Company\_HQ**

S1(config)# **snmp-server contact admin@company.com**

S1(config)# **snmp-server host 192.168.1.3 version 2c ciscolab**

S1(config)# **snmp-server enable traps**

S1(config)# **ip access-list standard SNMP\_ACL**

S1(config-std-nacl)# **permit 192.168.1.3**

* 1. Проверьте параметры SNMPv2.

Для проверки параметров SNMPv2 используйте команды **show**.

S1# **show snmp**

Chassis: FCQ1628Y5MG

Contact: admin@company.com

Location: Company\_HQ

0 SNMP packets input

0 Bad SNMP version errors

0 Unknown community name

0 Illegal operation for community name supplied

0 Encoding errors

0 Number of requested variables

0 Number of altered variables

0 Get-request PDUs

0 Get-next PDUs

0 Set-request PDUs

0 Input queue packet drops (Maximum queue size 1000)

0 SNMP packets output

0 Too big errors (Maximum packet size 1500)

0 No such name errors

0 Bad values errors

0 General errors

0 Response PDUs

0 Trap PDUs

SNMP global trap: enabled

SNMP logging: enabled

Logging to 192.168.1.3.162, 0/10, 0 sent, 0 dropped.

SNMP agent enabled

S1# **show snmp community**

Community name: ciscolab

Community Index: ciscolab

Community SecurityName: ciscolab

storage-type: nonvolatile active access-list: SNMP\_ACL

<Данные опущены>

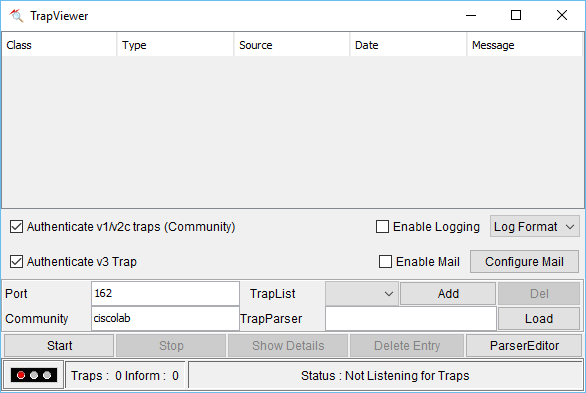
Какое сообщество SNMP настроено?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Включите SNMP-ловушку.

На этом этапе вы активируете SNMP-ловушку и проследите за сообщениями во время настройки и включения SVI на интерфейсе VLAN 1 маршрутизатора S1.

* + 1. В MibBrowser нажмите **Изменить** > **Параметры**. Убедитесь, что выбрана версия SNMP **v2c**. Для продолжения нажмите **OК.**
    2. Нажмите **Интерфейс пользователя средства просмотра ловушки**().
    3. Убедитесь, что задан номер порта **162**, и настройте **ciscolab** в качестве сообщества.



* + 1. После проверки параметров нажмите **Начать**. В поле TrapList показано **162: ciscolab**.
    2. Для создания сообщений SNMP настройте и включите SVI на коммутаторе S1. Используйте IP-адрес **192.168.1.2 /24** для VLAN 1 и отключите и включите интерфейс.
    3. Введите команду **show snmp**, чтобы убедиться в отправке сообщений SNMP.

S1# **show snmp**

Chassis: FCQ1628Y5MG

Contact: admin@company.com

Location: Company\_HQ

0 SNMP packets input

0 Bad SNMP version errors

0 Unknown community name

0 Illegal operation for community name supplied

0 Encoding errors

0 Number of requested variables

0 Number of altered variables

0 Get-request PDUs

0 Get-next PDUs

0 Set-request PDUs

0 Input queue packet drops (Maximum queue size 1000)

2 SNMP packets output

0 Too big errors (Maximum packet size 1500)

0 No such name errors

0 Bad values errors

0 General errors

0 Response PDUs

2 Trap PDUs

SNMP global trap: enabled

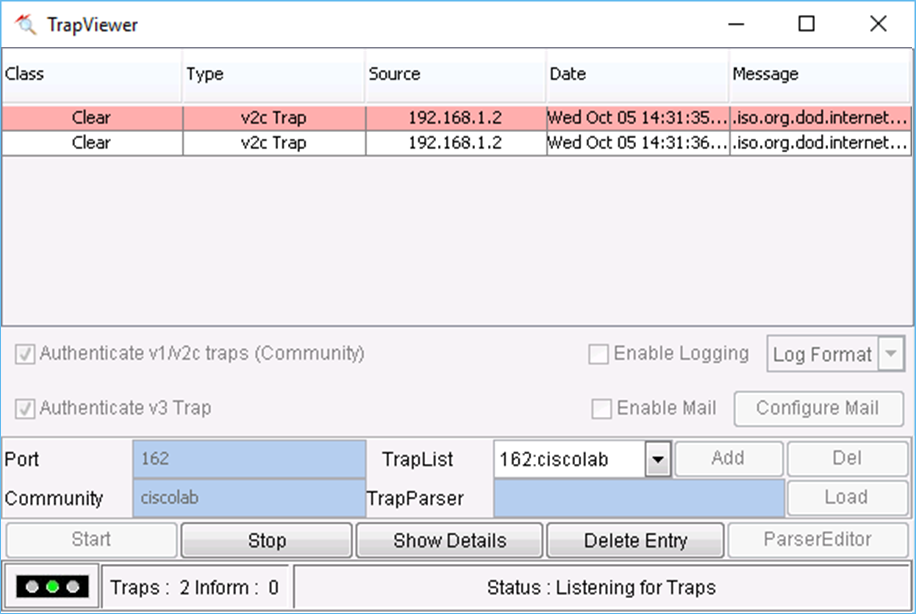
SNMP logging: enabled

Logging to 192.168.1.3.162, 0/10, 2 sent, 0 dropped.

SNMP agent enabled

SNMP agent enabled

* + 1. Перейдите к TrapViewer. Просмотрите сообщения, перехваченные MibBrowser. Для просмотра сведений о каждом сообщении нажмите **Показать сведения**.



1. Настройка диспетчера и агента SNMPv3
   1. Настройте агент SNMPv3 на маршрутизаторе R1.

В режиме глобальной настройки на маршрутизаторе R1 введите следующие команды для его настройки в качестве агента SNMP. В строках 1–3 ниже стандартный список контроля доступа с именем PERMIT-ADMIN разрешает доступ к агенту SNMP на маршрутизаторе R1 только хостам из сети 192.168.1.0 /24. Строка 4 настраивает представление SNMP (SNMP-RO) и включает дерево ISO из MIB. В строке 5 настраивается группа SNMP с именем ADMIN для агента SNMPv3 с необходимой аутентификацией и шифрованием и разрешает доступ только хостам, разрешенным в списке контроля доступа PERMIT-ADMIN. Строка 5 определяет пользователя USER1 в группе ADMIN. Необходимо использовать аутентификацию SHA с паролем cisco12345 и шифрование по алгоритму AES 128 с настроенным паролем cisco54321.

R1(config)# **ip access-list standard PERMIT-ADMIN**

R1(config-std-nacl)# **permit 192.168.1.0 0.0.0.255**

R1(config-std-nacl)# **exit**

R1(config)# **snmp-server view SNMP-RO iso included**

R1(config)# **snmp-server group ADMIN v3 priv read SNMP-RO access PERMIT-ADMIN**

R1(config)# **snmp-server user USER1 ADMIN v3 auth sha cisco12345 pri aes 128 cisco54321**

R1(config)#

\* Aug 5 02:52:50.715: Configuring snmpv3 USM user, persisting snmpEngineBoots. Please Wait...

* 1. Проверьте конфигурацию агента SNMPv3 на маршрутизаторе R1.

Для проверки параметров SNMPv3 используйте команды **show**.

R1# **show run | include snmp**

snmp-server group ADMIN v3 priv read SNMP-RO access PERMIT-ADMIN

snmp-server view SNMP-RO iso included

R1# **show snmp user**

User name: USER1

Engine ID: 800000090300D48CB5CEA0C0

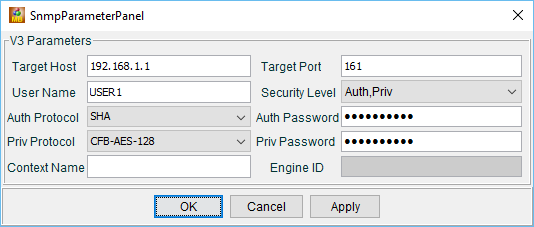
storage-type: nonvolatile active

Authentication Protocol: SHA

Privacy Protocol: AES128

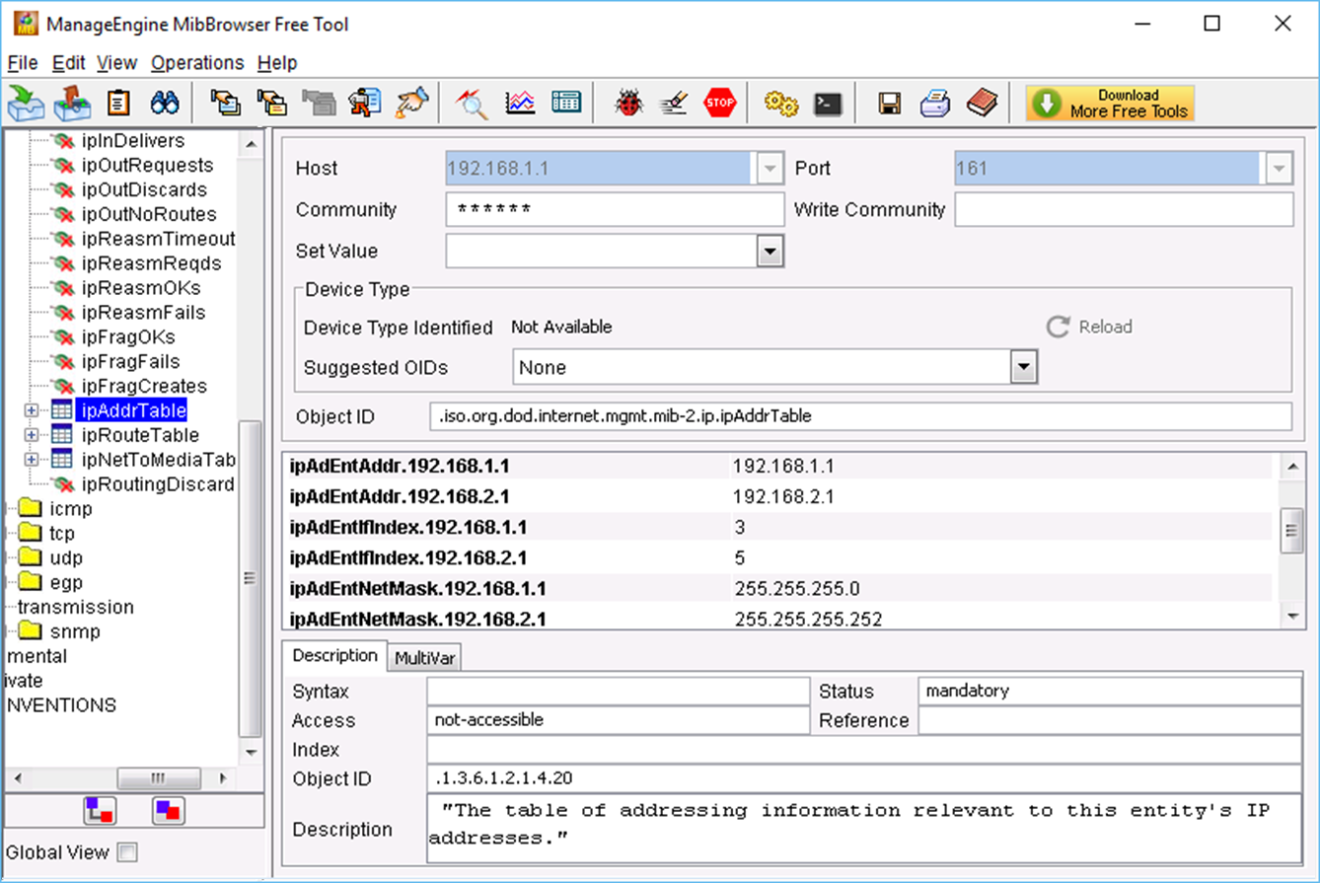
Group-name: ADMIN

* 1. Настройте доступ диспетчера SNMP к агенту SNMPv3.
     1. Перейдите к PC-A Open **Wireshark**. Начните перехват в режиме реального времени на соответствующем интерфейсе.
     2. Введите **snmp** в поле «Фильтр».
     3. В MibBrowser нажмите **Изменить** > **Параметры**. Выберите **v3** для версии SNMP. Нажмите **Добавить**.
     4. Введите параметры SNMPv3, настроенные на маршрутизаторе R1. Для продолжения нажмите **OК**.

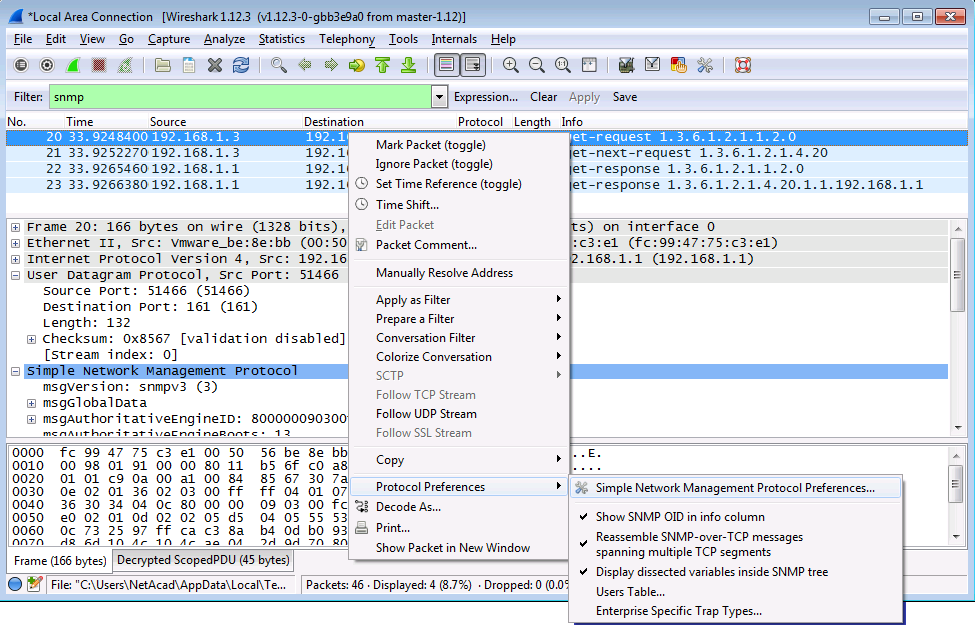


|  |  |
| --- | --- |
| Параметры SNMPv3 | Настройки |
| Целевой хост | 192.168.1.1 |
| Имя пользователя | USER1 |
| Протокол аутентификации | SHA |
| Протокол привилегированного режима | CFB-AES-128 |
| Целевой порт | 161 |
| Уровень безопасности | Auth, Priv |
| Пароль для аутентификации | cisco12345 |
| Пароль привилегированного режима | cisco54321 |

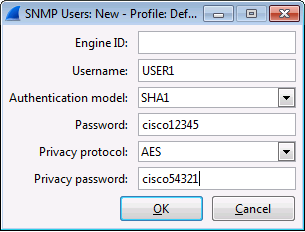
* + 1. Нажмите **Редактировать** > **Найти узел**. Введите **ipAddrTable** в поле «Что искать» и нажмите **Закрыть**. В левой панели должно быть выбрано **ipAddrTable**, а в поле ObjectID указано **.iso.org.dod.internet.mgmt.mib-2.ip.ipAddrTable**.
    2. Нажмите **Операция** > **Получить**, чтобы получить все объекты в выбранном управляемом объекте MIB (в данном случае **ipAddrTable**).



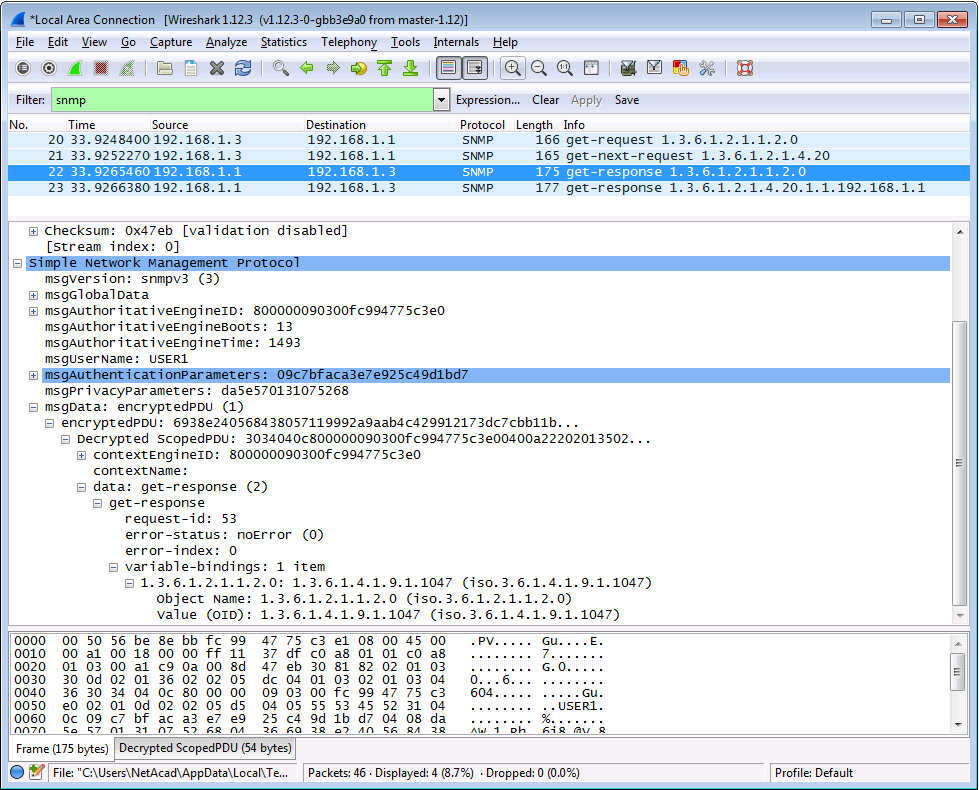
* + 1. Вернитесь к экрану Wireshark. Остановите перехват в режиме реального времени.
    2. На панели «Результаты» щелкните правой кнопкой мыши на результатах. Выберите **Настройки протокола > Настройки SNMP**.



* + 1. Нажмите **Изменить**  для «Таблица пользователей». Нажмите **Создать** и введите информацию о пользователе на шаге 1. Нажмите **ОК**.



* + 1. Нажмите **OК** для подтверждения информации о пользователе. Нажмите **OК** еще раз, чтобы закрыть окно «Настройки Wireshark».
    2. Выберите одну из строк. Разверните результат SNMP и просмотрите расшифрованные сообщения.



* 1. Проанализируйте полученные результаты.

Какие IP-адреса, настроенные на маршрутизаторе R1, включены в результаты SNMPv3?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Сравните расшифрованные Wireshark пакеты SNMP и результаты MIB Browser. Запишите свои наблюдения.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Вопросы для повторения
   1. Перечислите несколько потенциальных преимуществ мониторинга за сетью с помощью протокола SNMP.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Почему при работе с SNMPv2 предпочтительно использовать исключительно доступ с правами только для чтения?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Каковы преимущества использования SNMPv3 по сравнению с SNMPv2?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Сводная таблица по интерфейсам маршрутизаторов

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Сводка по интерфейсам маршрутизаторов | | | | |
| Модель маршрутизатора | Ethernet-интерфейс № 1 | Ethernet-интерфейс № 2 | Последовательный интерфейс № 1 | Последовательный интерфейс № 2 |
| 1800 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 1900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2801 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 2811 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| **Примечание**. Чтобы определить конфигурацию маршрутизатора, можно посмотреть на интерфейсы и установить тип маршрутизатора и количество его интерфейсов. Перечислить все комбинации конфигураций для каждого класса маршрутизаторов невозможно. Эта таблица содержит идентификаторы для возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов на устройстве. Другие типы интерфейсов в таблице не представлены, хотя они могут присутствовать в данном конкретном маршрутизаторе. В качестве примера можно привести интерфейс основного доступа ISDN. Строка в скобках — это официальная аббревиатура, которое можно использовать в командах Cisco IOS для обозначения интерфейса. | | | | |