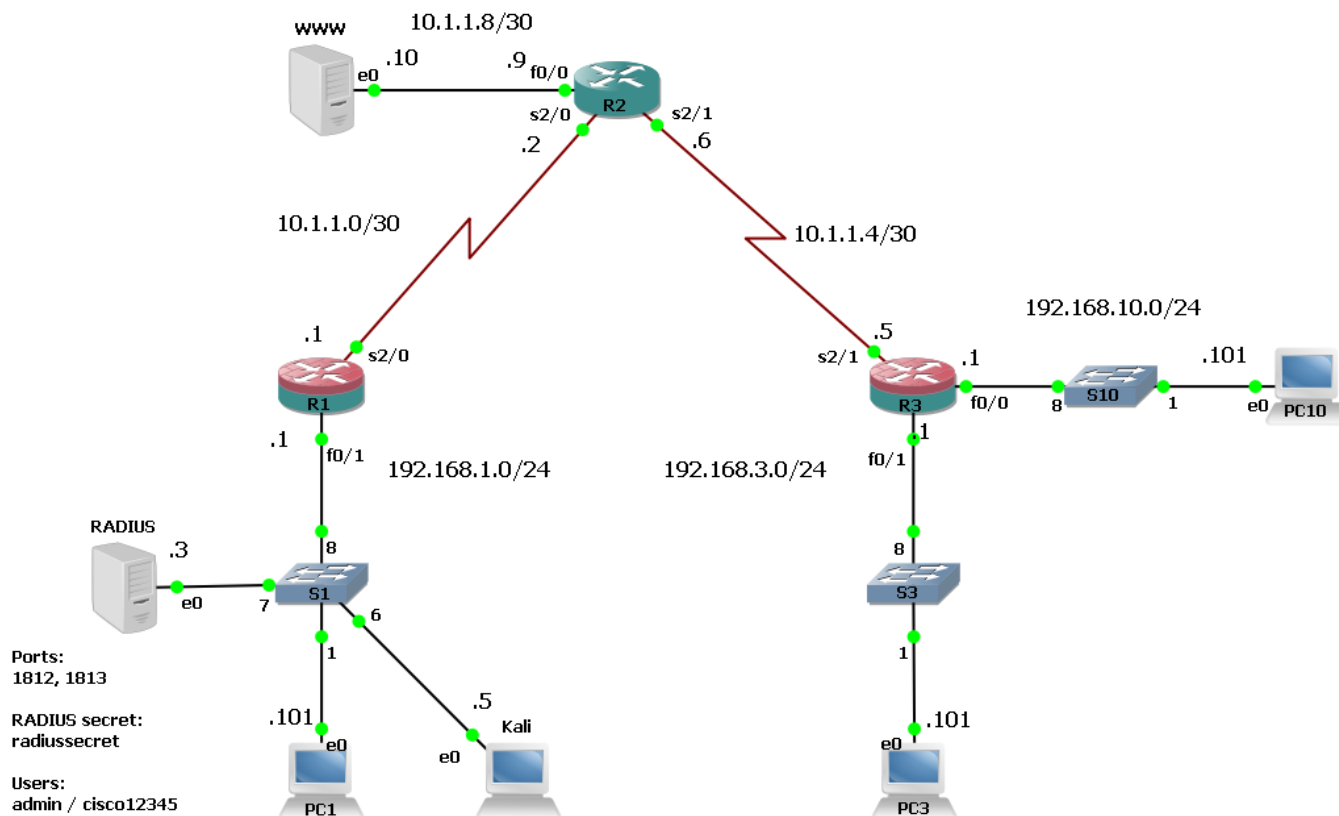


Изучение протокола SNMP

Топология



Описание

В этой лабораторной работе вы настроите на маршрутизаторах функционал SNMP-агента. Вначале вы включите протокол SNMP версии 2с, потом – версии 3. В качестве SNMP-менеджера будет выступать узел PC1. Для работы с SNMP на PC1 установлен набор утилит net-snmp и PowerSNMP FreeManager.

Более подробная информация о net-snmp есть на сайте проекта <http://www.net-snmp.org/>

Более подробная информация о PowerSNMP FreeManager есть на сайте проекта <https://www.dart.com/pages/powersnmp-free-manager>

Таблица адресации

Устройство	Интерфейс	IPv4-адрес/Маска подсети	Шлюз по умолчанию	Описание
R1	Fa0/1	192.168.1.1/24	-	LAN interface
	Se2/0	10.1.1.1/30	-	WAN interface (To R2)
R2	Se2/0	10.1.1.2/30	-	To R1
	Se2/1	10.1.1.6/30	-	To R3
	Fa0/0	10.1.1.9/30	-	To WWW server
R3	Fa0/1	192.168.3.1/24	-	LAN interface
	Fa0/0	192.168.10.1/24	-	Conference Room
	Se2/1	10.1.1.5/30	-	WAN interface (To R2)
PC1	NIC	192.168.1.101/24	192.168.1.1	-
PC2	NIC	192.168.3.101/24	192.168.3.1	-
PC10	NIC	192.168.10.101/24	192.168.10.1	-
Kali	NIC	192.168.1.5/24	192.168.1.1	-
RADIUS	NIC	192.168.1.3/24	192.168.1.1	-
WWW	NIC	10.1.1.10/24	10.1.1.9	-

Имена пользователей и пароли

	Console		VTY		Enable
Устройство	Имя пользователя	Пароль	Имя пользователя	Пароль	Пароль
R1	admin	cisco12345	admin	cisco12345	cisco12345
R2	-	-	-	-	-
R3	admin	cisco12345	admin	cisco12345	cisco12345

Устройство	Имя пользователя	Пароль
PC1	Student1	1
PC2	Student1	1
PC10	Student1	1
Kali	root	toor

Часть 1: Изучение протокола SNMPv2c

1. Запустите захват на линке между R1 и S1. Для этого в окне GNS3 щёлкните правой кнопкой мыши по линку между R1 и S1, в контекстном меню выберите **Start Capture**. В открывшемся окне просто нажмите **ОК**. Дождитесь открытия Wireshark.

2. Подключитесь к консоли маршрутизатора R1.

3. Войдите в режим конфигурирования.

```
R1# conf t
```

4. Настройте переменную contact, переменную location, включите функционал SNMP-сервера (SNMP-агента), разрешите доступ ко всему дереву объектов в режиме «только чтение» со строкой сообщества (community) testpassword1.

```
R1(config)# snmp-server contact help@acad.local
```

```
R1(config)# snmp-server location Main Office
```

```
R1(config)# snmp-server community testpassword1 ro
```

```
R1(config)# exit
```

5. Протокол SNMP использует для своей работы транспортный протокол UDP и стандартные порты 161 (для работы с пакетами get и set) и 162 (для работы с пакетами trap). Проверьте, что на R1 прослушивается порт 161.

```
R1# show control-plane host open-ports
```

Active internet connections (servers and established)

Prot	Local Address	Foreign Address	Service	State
tcp	*:22	*:0	SSH-Server	LISTEN
tcp	*:23	*:0	Telnet	LISTEN
udp	*:61148	192.168.1.101:514	Syslog	ESTABLIS
udp	*:161	*:0	IP SNMP	LISTEN
udp	*:162	*:0	IP SNMP	LISTEN
udp	*:60419	*:0	IP SNMP	LISTEN

6. Войдите в виртуальную машину PC1.

7. Получите информацию (имя устройства) с маршрутизатора R1 с помощью протокола SNMP. Для этого откройте командную строку и введите команду ниже. Результат будет успешен, мы увидим имя устройства. Краткое описание команды и параметров:

- snmpget – программа, позволяющая отправить пакет get протокола SNMP;
- -v 2c – использовать версию 2c;
- -c testpassword1 – использовать строку сообщества testpassword1;
- 192.168.1.1 – адрес устройства;
- sysName.0 – строковое обозначение переменной.

```
C:\Users\Student1> snmpget -v 2c -c testpassword1 192.168.1.1 sysName.0
```

```
SNMPv2-MIB::sysName.0 = STRING: R1.acad.local
```

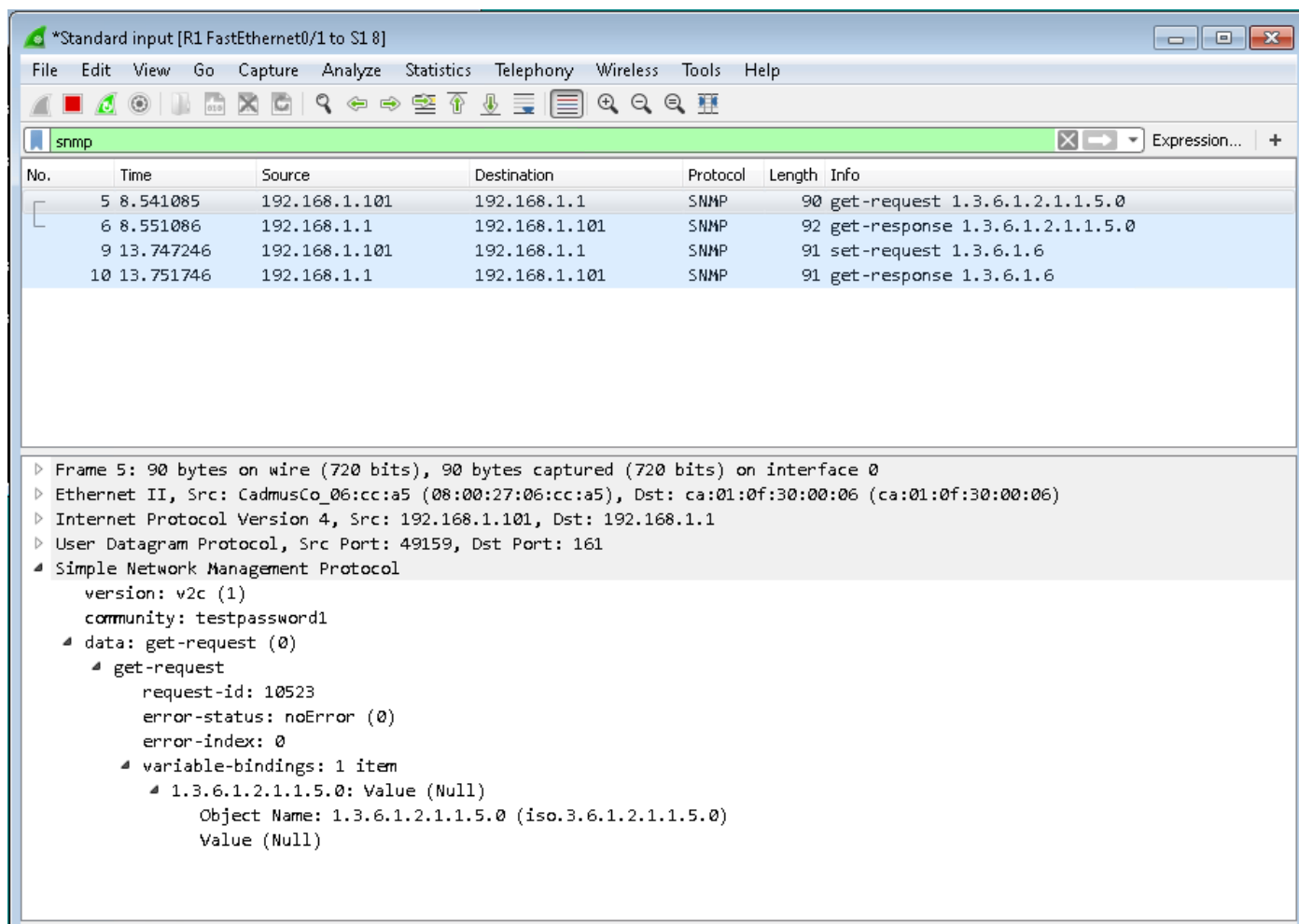
8. Попробуйте изменить информацию (имя устройства) на маршрутизаторе R1 с помощью протокола SNMP. Для этого откройте командную строку и введите команду ниже. Результат будет неуспешен, т.к. с этой строкой сообщества есть доступ «только чтение». Краткое описание команды и параметров:

- snmpset - программа, позволяющая отправить пакет set протокола SNMP;
- s – тип переменной, в данном случае строковая (string);
- R1new – новое значение переменной.

```
C:\Users\Student1>snmpset -v 2c -c testpassword1 192.168.1.1 s sysName.0 R1new
Error in packet.
Reason: noAccess
Failed object: SNMPv2-SMI::snmpV2
```

9. Вернитесь в Wireshark на основной машине.

10. Введите в поле Display Filter слово **snmp** и нажмите Enter. Вы должны увидеть 4 пакета: Get-Request, Get-Response, Set-Request, Set-Response. Изучите содержимое пакетов. Видно ли строку сообщества (community)?



11. В SNMP версии 2 строка сообщества передаётся в открытом виде. Можно задать две строки сообщества: для доступа в режиме «только чтение» (что мы сделали раньше) и в режиме «чтение и запись» (что совершенно небезопасно). Также хорошо бы разрешить доступ по протоколу SNMP только с определённых узлов. Войдите в виртуальную машину PC3.

12. Получите информацию (имя устройства) с маршрутизатора R1 с помощью протокола SNMP. Для этого откройте командную строку и введите команду ниже. Результат будет успешен, мы увидим имя устройства.

```
C:\Users\Student1> snmpget -v 2c -c testpassword1 192.168.1.1 sysName.0
SNMPv2-MIB::sysName.0 = STRING: R1.acad.local
```

Автор - Монахов Павел Сергеевич, monakhovps.ru, 2015 – 2021
Использование без разрешения автора запрещено

13.Вернитесь в консоль маршрутизатора R1. Составьте ACL и прикрепите его к команде snmp-server.

```
R1(config)# ip access-list standard ACL-SNMP
R1(config-std-nacl)# permit host 192.168.1.101
R1(config-std-nacl)# exit
R1(config)# snmp-server community testpassword1 ro ACL-SNMP
R1(config)# exit
```

14.Проверьте настройки протокола SNMP.

```
R1# show snmp
Chassis: 4279256517
Contact: help@acad.local
Location: Main Office
< Вывод опущен >
```

```
R1# show snmp community
< Вывод опущен >
Community name: testpassword1
Community Index: cisco2
Community SecurityName: testpassword1
storage-type: nonvolatile          active access-list: ACL-SNMP
```

```
R1# show snmp group
< Вывод опущен >
groupname: testpassword1          security model:v1
contextname: <no context specified> storage-type: permanent
readview : vldefault              writeview: <no writeview specified>
notifyview: <no notifyview specified>
row status: active               access-list: ACL-SNMP
```

```
groupname: testpassword1          security model:v2c
contextname: <no context specified> storage-type: permanent
readview : vldefault              writeview: <no writeview specified>
notifyview: <no notifyview specified>
row status: active               access-list: ACL-SNMP
```

```
R1# show snmp view
< Вывод опущен >
vldefault iso - included permanent active
vldefault internet.6.3.15 - excluded permanent active
vldefault internet.6.3.16 - excluded permanent active
vldefault internet.6.3.18 - excluded permanent active
vldefault ciscoMgmt.394 - excluded permanent active
vldefault ciscoMgmt.395 - excluded permanent active
vldefault ciscoMgmt.399 - excluded permanent active
vldefault ciscoMgmt.400 - excluded permanent active
```

15.Войдите в виртуальную машину PC3 и снова попробуйте получить информацию с маршрутизатора R1.

```
C:\Users\Student1> snmpget -v 2c -c testpassword1 192.168.1.1 sysName.0
Timeout: No Response from 192.168.1.1
```


Часть 2: Изучение протокола SNMPv3

Протокол SNMPv3 гораздо более гибкий и безопасный, нежели предыдущая версия.

1. Вернитесь в консоль маршрутизатора R1. Удалите конфигурацию SNMPv2.

```
R1(config)# no snmp-server community testpassword1 ro ACL-SNMP
```

2. Создайте представление с названием SNMP-RO. Представление будет содержать всё дерево объектов (ветку iso и все её подветки).

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

3. Создайте группу SNMP-G1. Пользователи этой группы будут проходить при подключении аутентификацию по имени пользователя и паролю, а сами пакеты будут шифроваться и проходить проверку целостности. Также предоставьте права к представлению SNMP-RO в режиме «только чтение». Разрешите подключение только с узла PC1.

```
R1(config)# snmp-server group SNMP-G1 v3 priv read SNMP-RO access ACL-SNMP
```

4. Создайте пользователя SNMP-Admin. Занесите пользователя в группу SNMP-G1. Задайте параметры аутентификации и шифрования.

```
R1(config)# snmp-server user SNMP-Admin SNMP-G1 v3 auth sha Authpass  
priv aes 128 Encrypass
```

```
R1(config)# end
```

5. Проверьте настройки.

```
R1# show snmp user
```

```
User name: SNMP-Admin
```

```
Engine ID: 800000090300CA010F300008
```

```
storage-type: nonvolatile active
```

```
Authentication Protocol: SHA
```

```
Privacy Protocol: AES128
```

```
Group-name: SNMP-G1
```

```
R1# show snmp group
```

```
< Вывод опущен >
```

```
groupname: SNMP-G1
```

```
security model:v3 priv
```

```
contextname: <no context specified>
```

```
storage-type: nonvolatile
```

```
readview : SNMP-RO
```

```
writeview: <no writeview specified>
```

```
notifyview: <no notifyview specified>
```

```
row status: active
```

```
access-list: ACL-SNMP
```

```
R1# show snmp view
```

```
< Вывод опущен >
```

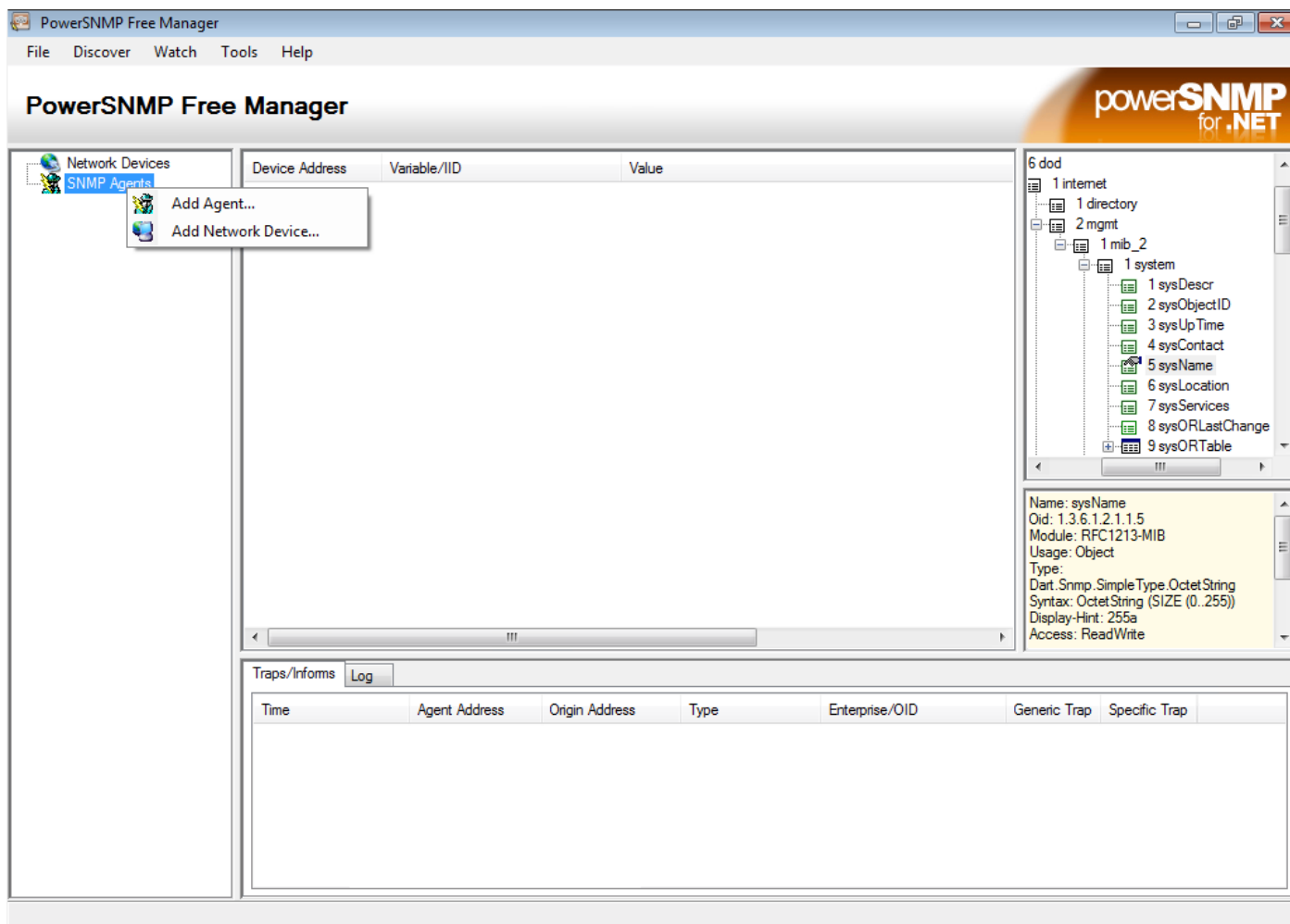
```
SNMP-RO iso - included nonvolatile active
```

```
< Вывод опущен >
```



6. Войдите в виртуальную машину PC1.

7. Запустите PowerSNMP FreeManager.

8. В левой части окна щёлкните правой кнопкой мыши на пункте **SNMP Agents**. В контекстном меню выберите **Add agent...**



9. В открывшемся окне нажмите в левом нижнем углу ссылку **Add Agent...**

 Add SNMP Agents 

Discover Agents

Address:

Community: Timeout (ms):

Address	Name	Description
---------	------	-------------

[Add Agent...](#)

10. В открывшемся окне заполните поля ниже, а потом нажмите **OK**.

Address: **192.168.1.1**

Version: **3**

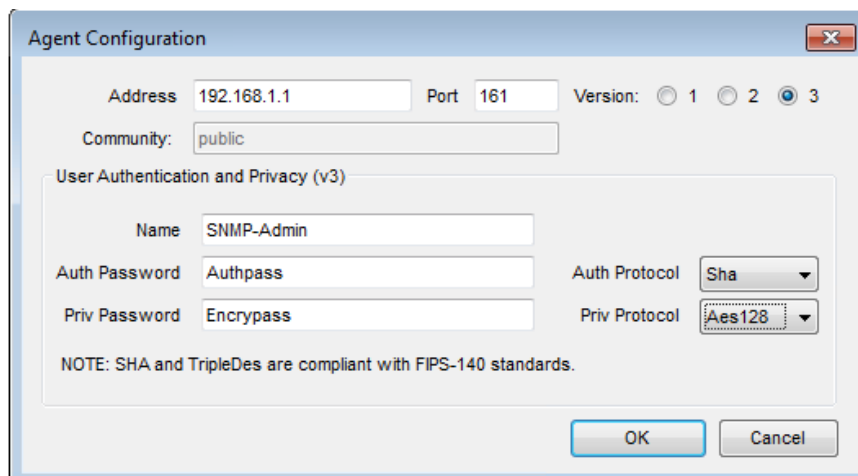
Name: **SNMP-Admin**

Auth Password: **Authpass**

Auth Protocol: **Sha**

Priv Password: **Encrypass**

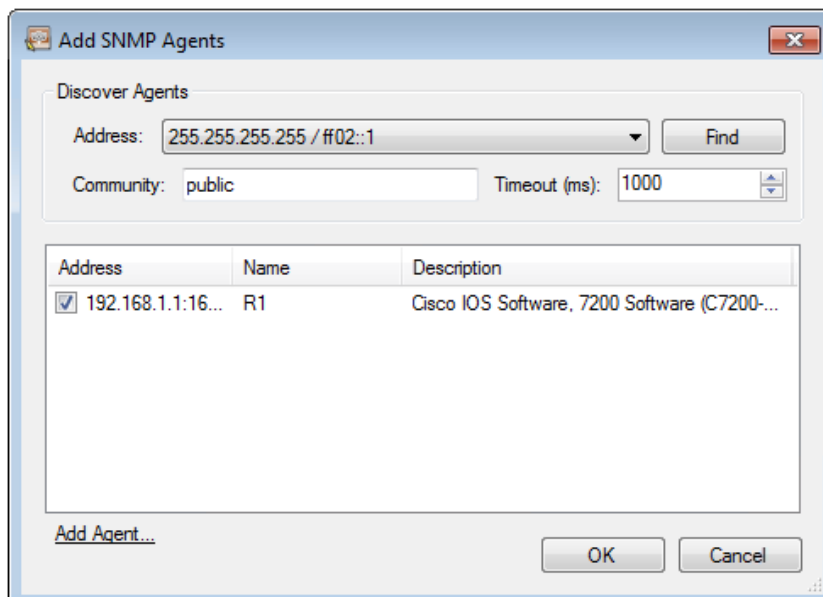
Priv Protocol: **Aes128**



The 'Agent Configuration' dialog box contains the following fields and settings:

- Address: 192.168.1.1
- Port: 161
- Version: 3 (selected)
- Community: public
- User Authentication and Privacy (v3) section:
 - Name: SNMP-Admin
 - Auth Password: Authpass
 - Auth Protocol: Sha
 - Priv Password: Encrypass
 - Priv Protocol: Aes128
- NOTE: SHA and TripleDes are compliant with FIPS-140 standards.
- Buttons: OK, Cancel

11. Снова нажмите **OK**.



The 'Add SNMP Agents' dialog box contains the following fields and settings:

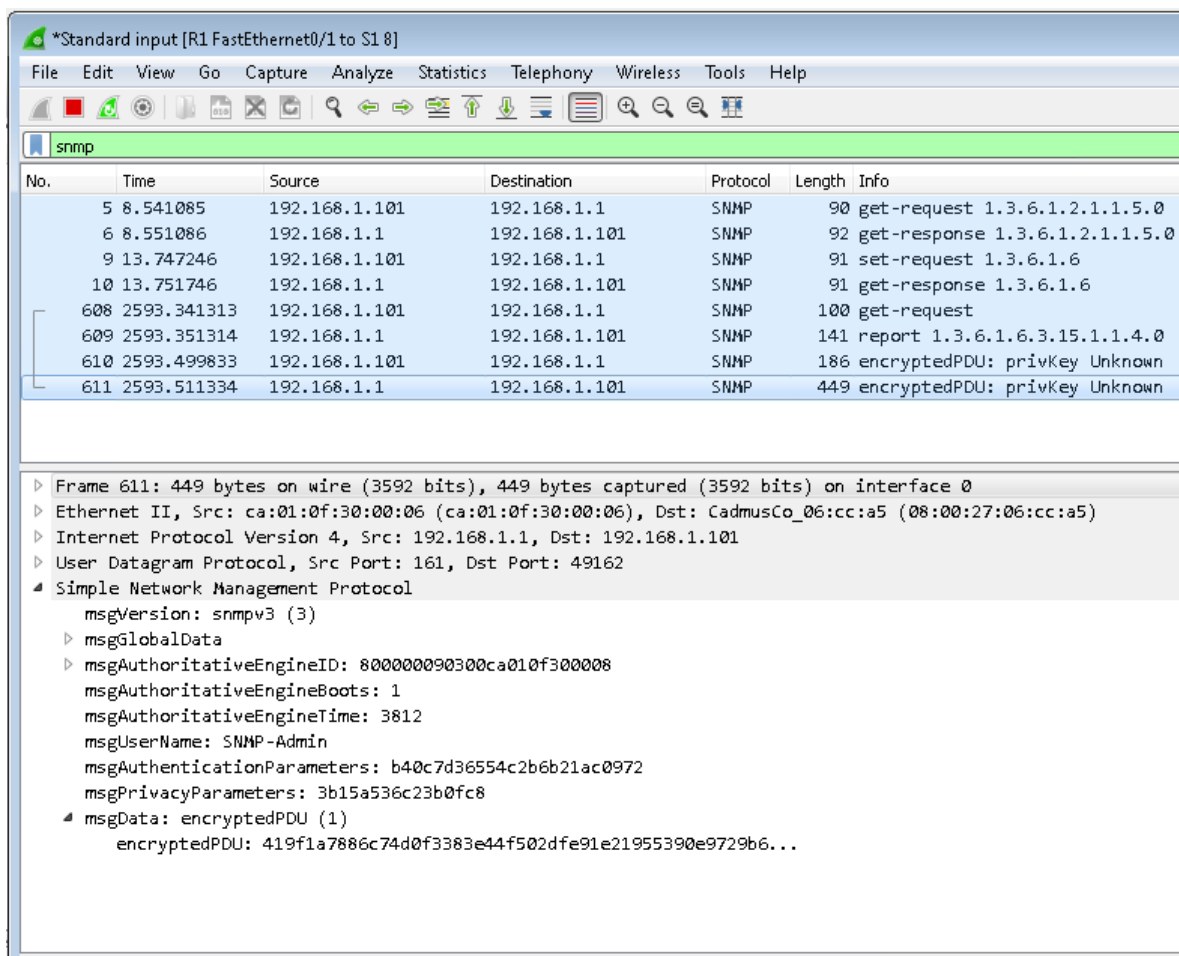
- Discover Agents section:
 - Address: 255.255.255.255 / ff02::1
 - Find button
 - Community: public
 - Timeout (ms): 1000
- Table of discovered agents:

Address	Name	Description
<input checked="" type="checkbox"/> 192.168.1.1:16...	R1	Cisco IOS Software, 7200 Software (C7200-...

Buttons: Add Agent..., OK, Cancel

12. Вы вернулись в главное окно PowerSNMP Free Manager. Когда вы добавляли агента, PowerSNMP Free Manager уже попробовал получить информацию с устройства (имя и описание).

13. Вернитесь в Wireshark на основной машине. Выберите последний пакет SNMP, попробуйте что-нибудь в нём разобрать.



14. Закройте основное окно Wireshark.

Часть 3: Настройка маршрутизатора R3

1. Подключитесь к консоли маршрутизатора R3.

2. Войдите в режим конфигурирования.

```
R3# conf t
```

3. Настройте переменную contact и переменную location.

```
R3(config)# snmp-server contact help@acad.local
```

```
R3(config)# snmp-server location Branch Office
```

4. Составьте ACL. Доступ всё также будет разрешён только с PC1.

```
R3(config)# ip access-list standard ACL-SNMP
```

```
R3(config-std-nacl)# permit host 192.168.1.101
```

```
R3(config-std-nacl)# exit
```

5. Создайте представление с названием SNMP-RO. Представление будет содержать всё дерево объектов (ветку iso и все её подветки).

```
R3(config)# snmp-server view SNMP-RO iso included
```

6. Создайте группу SNMP-G1. Пользователи этой группы будут проходить при подключении аутентификацию по имени пользователя и паролю, а сами пакеты будут шифроваться и проходить проверку целостности. Также предоставьте права к представлению SNMP-RO в режиме «только чтение». Разрешите подключение только с узла PC1.

```
R3(config)# snmp-server group SNMP-G1 v3 priv read SNMP-RO access ACL-SNMP
```

7. Создайте пользователя SNMP-Admin. Занесите пользователя в группу SNMP-G1. Задайте параметры аутентификации и шифрования.

```
R3(config)# snmp-server user SNMP-Admin SNMP-G1 v3 auth sha Authpass priv aes 128 Encrypass
```

```
R3(config)# end
```

8. Проверьте настройки.

```
R3# show snmp user
```

```
User name: SNMP-Admin
```

```
Engine ID: 800000090300CA010F300008
```

```
storage-type: nonvolatile active
```

```
Authentication Protocol: SHA
```

```
Privacy Protocol: AES128
```

```
Group-name: SNMP-G1
```

```
R3# show snmp group
```

```
< Вывод опущен >
```

```
groupname: SNMP-G1
```

```
security model: v3 priv
```

```
contextname: <no context specified>
```

```
storage-type: nonvolatile
```

```
readview : SNMP-RO
```

```
writeview: <no writeview specified>
```

```
notifyview: <no notifyview specified>
```

```
row status: active
```

```
access-list: ACL-SNMP
```

```
R3# show snmp view
```

```
< Вывод опущен >  
SNMP-RO iso - included nonvolatile active  
< Вывод опущен >
```