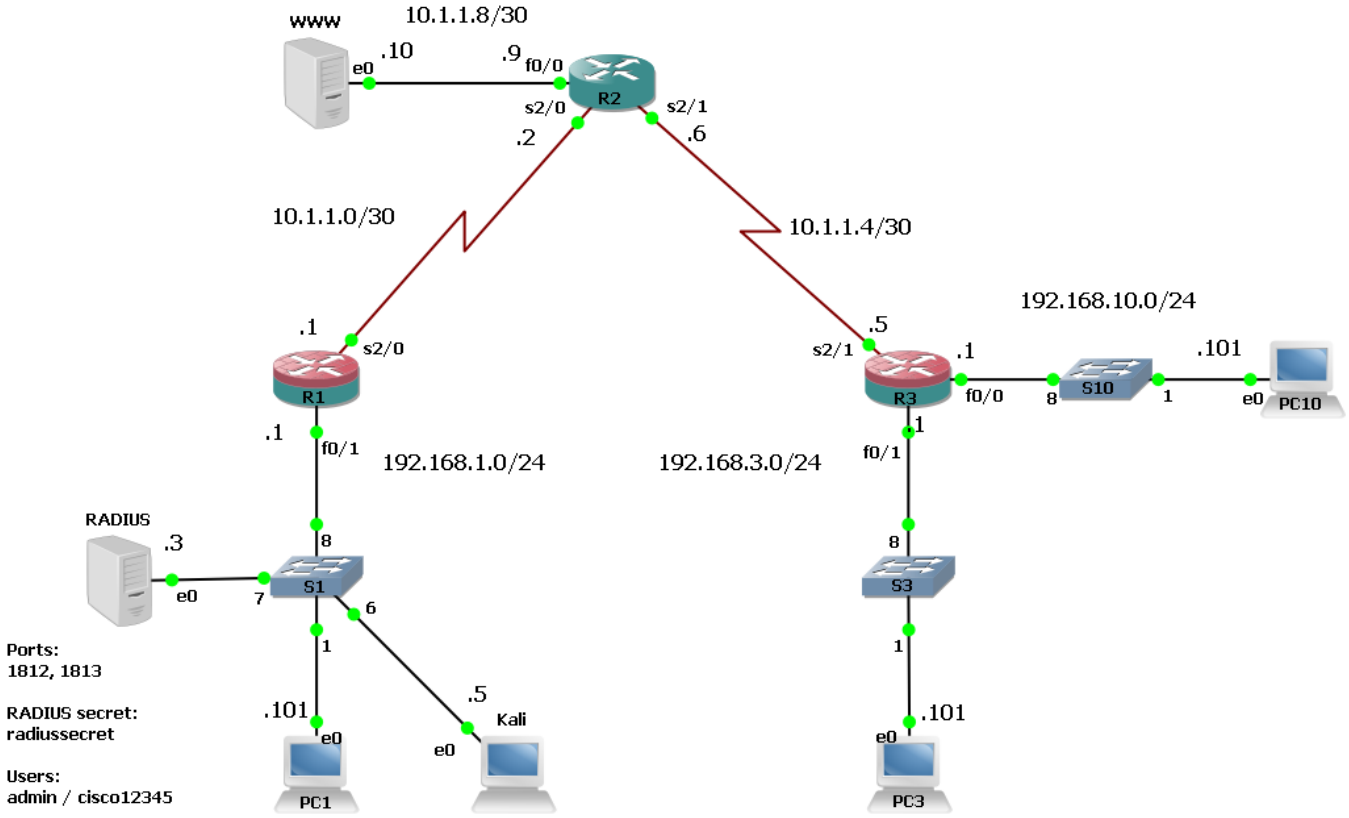
CCNA Security

Лабораторная работа 7

Изучение протокола Syslog

Топология



Описание

В этой лабораторной работе вы настроите пересылку лог-сообщений на Syslog-сервер. В качестве Syslog-сервера будет выступать узел PC1 с установленным ПО tftpd32/tftpd64.

Более подробная информация о tftpd32/tftpd64 есть на сайте проекта https://tftpd32.jounin.net/

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

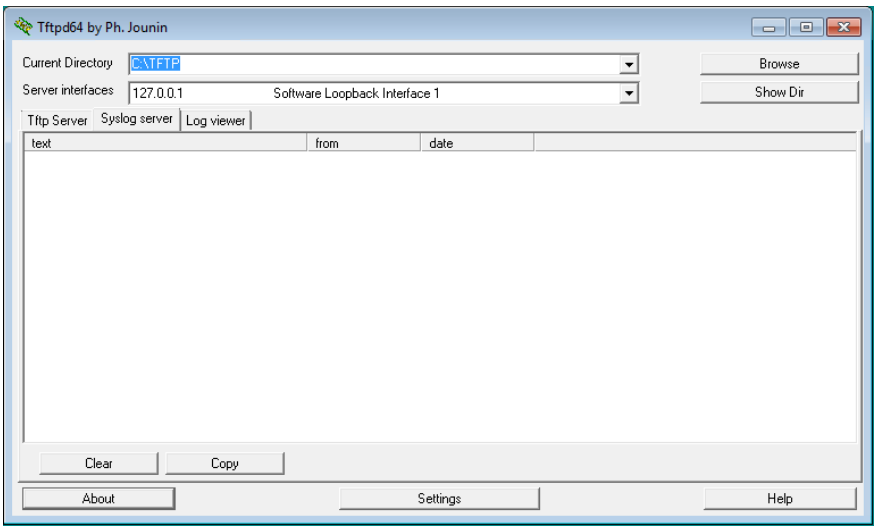
Часть 1: Изучение протокола Syslog и настройка протоколирования на маршрутизаторе R1

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 **OK**. Дождитесь открытия Wireshark.

2. Войдите в виртуальную машину PC1.

3. Запустите Tftpd64.

4. Перейдите на вкладку **Syslog server**.



5. Подключитесь к консоли маршрутизатора R1.

6. Войдите в режим конфигурирования.
```
R1# conf t
```

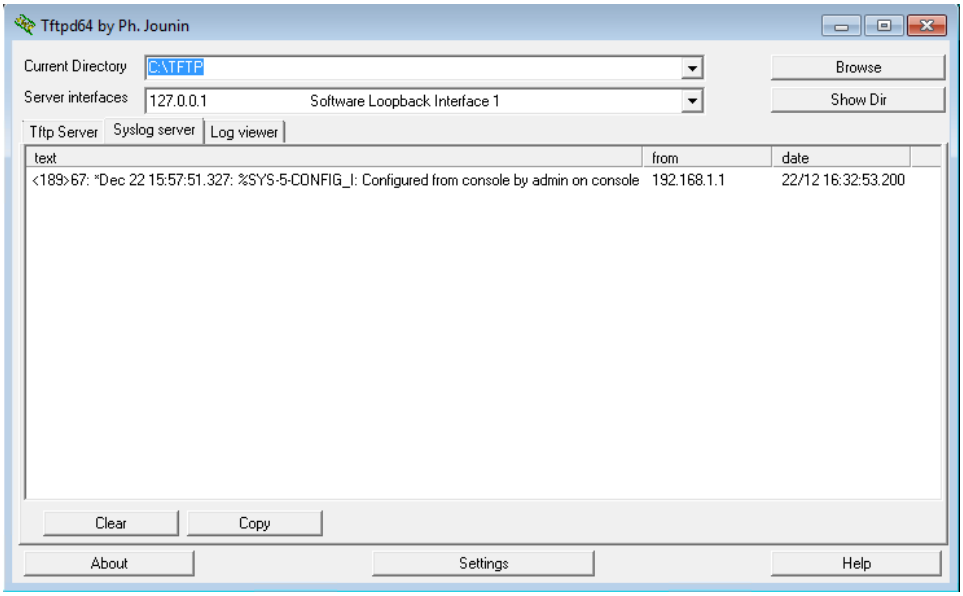
7. Настройте пересылку лог-сообщений на PC1. В качестве адреса отправителя используйте адрес с интерфейса fa0/1.
```
R1(config)# logging host 192.168.1.101
R1(config)# logging source-interface fa0/1
R1(config)# logging on
R1(config)# exit
```

8. Проверьте настройки протоколирования.

```
R1# show logging

< Вывод опущен >

    Trap logging: level informational, 67 message lines logged

        Logging to 192.168.1.101  (udp port 514, audit disabled,

              link up),

              4 message lines logged,

              0 message lines rate-limited,
```

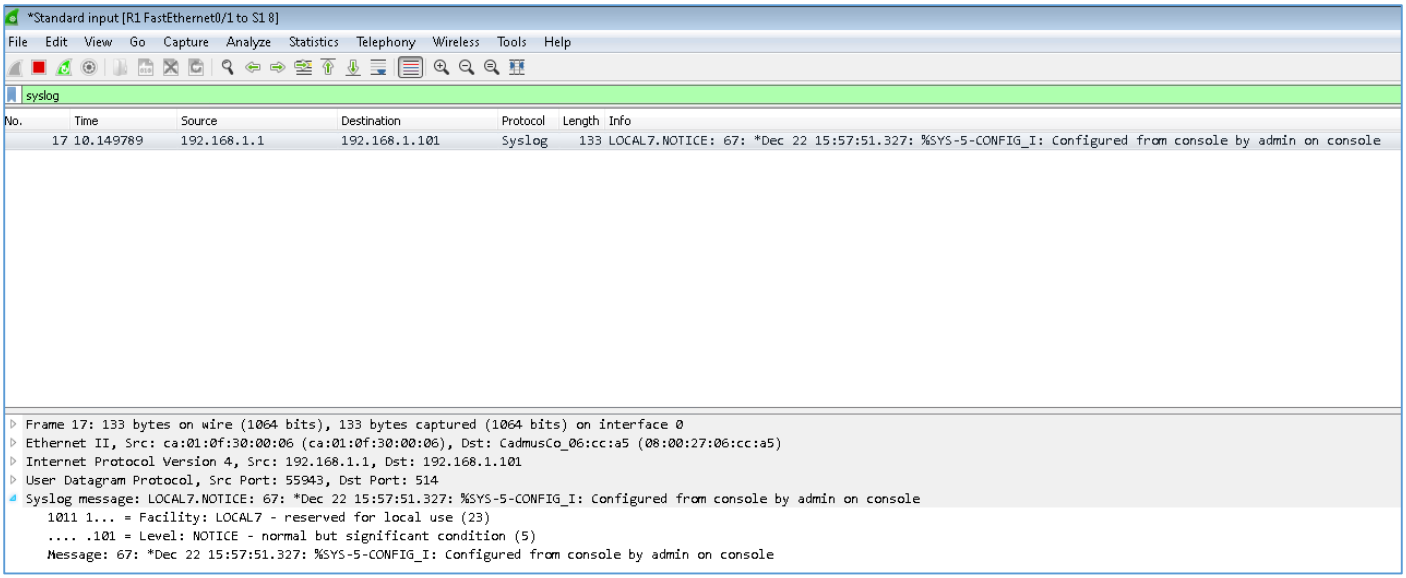
```
        0 message lines dropped-by-MD,
        xml disabled, sequence number disabled
        filtering disabled
    Logging Source-Interface:       VRF Name:
    FastEthernet0/1
< Вывод опущен >
```

9. Войдите в виртуальную машину PC1. Посмотрите лог-сообщения, собранные tftpd64.



10. Вернитесь в Wireshark на основной машине.

11. Введите в поле Display Filter слово **syslog** и нажмите Enter. Выделите любой пакет и изучите его содержимое. Протокол Syslog передаёт всё в открытом виде, при этом использует транспортный протокол UDP на стандартный порт 514. Также протокол Syslog не имеет встроенных средств обеспечения надёжной доставки, все сообщения передаются ненадёжно.



12. Закройте основное окно Wireshark.

Часть 2: Настройка протоколирования на маршрутизаторе R3

1. Проделайте шаги 5-9 из части 1, но в этот раз на маршрутизаторе R3.