Лабораторная работа. Реализация локального анализатора коммутируемых портов

Топология

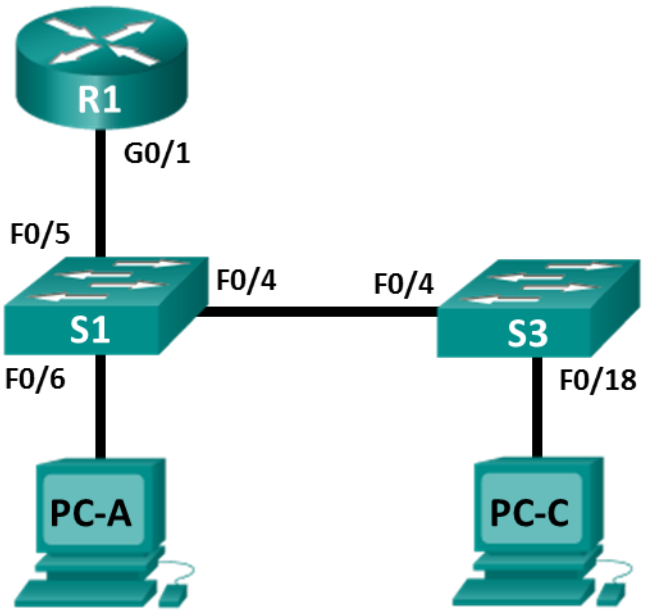


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	—
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.1.3	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.254	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Задачи

Часть 1. Построение сети и проверка соединения

Часть 2. Настройка локального анализатора коммутируемых портов и сбор копируемого трафика с помощью ПО Wireshark

Общие сведения/сценарий

Как сетевой администратор, вы хотите анализировать входящий и исходящий трафик локальной сети. Для этого вы настроите зеркалирование портов на коммутационном порте, подключенном к маршрутизатору, и зеркально скопируете весь трафик на другой коммутационный порт. Цель состоит в отправке зеркалированного трафика в систему обнаружения вторжений (IDS) для анализа. В этой первоначальной реализации вы будете отправлять весь зеркалированный трафик на ПК, который

будет перехватывать трафик для анализа, используя программу прослушивания портов. Для настройки зеркалирования портов будет использоваться функция анализатора коммутируемых портов (SPAN) на коммутаторе Cisco. Анализатор коммутируемых портов — это тип зеркалирования портов, в котором копии кадров, поступающих на порт, отправляются на другой порт того же коммутатора. Очень часто можно найти устройство, на котором работает анализатор трафика пакетов или система обнаружения вторжений (IDS), подключенные к зеркалированному порту.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интегрированными сетевыми 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 версии 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. Точные идентификаторы интерфейсов см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

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

Необходимые ресурсы

- 1 маршрутизатор (Cisco 1941 с операционной системой Cisco IOS 15.4(3) (универсальный образ) или аналогичная модель)
- 2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель)
- 2 ПК (Windows и программа эмуляции терминала, такая как Tera Term)
- Консольные кабели для настройки устройств Cisco IOS через консольные порты
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Построение сети и проверка связи

В первой части вам предстоит настроить топологию сети и выполнить базовую настройку, например, IP-адреса интерфейсов, статическую маршрутизацию, доступ к устройствам и пароли.

Шаг 1: Создайте сеть согласно топологии.

Подключите устройства, как показано в топологии, и подсоедините необходимые кабели.

Шаг 2: Настройте узлы ПК.

Шаг 3: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Шаг 4: Настройте базовые параметры этого маршрутизатора.

a. Отключите DNS-поиск.

b. Присвойте имена устройствам в соответствии с топологией.

c. Настройте IP-адрес для маршрутизатора, указанный в таблице адресации.

d. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму EXEC.

e. Назначьте **cisco** в качестве пароля консоли и VTY и включите запрос пароля при подключении.

f. Установите режим **transport input telnet** для линий VTY.

g. Настройте **logging synchronous**, чтобы сообщения от консоли не могли прерывать ввод команд.

h. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

Шаг 5: Настройте базовые параметры каждого коммутатора.

a. Отключите DNS-поиск.

b. Присвойте имена устройствам в соответствии с топологией.

c. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму EXEC.

d. Настройте IP-адреса для коммутаторов, указанных в таблице адресации.

e. На каждом коммутаторе настройте шлюз по умолчанию.

f. Назначьте **cisco** в качестве пароля консоли и VTY и включите запрос пароля при подключении.

g. Настройте **logging synchronous**, чтобы сообщения от консоли не могли прерывать ввод команд.

h. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

Шаг 6: Проверьте подключение.

a. Необходимо получать ответ на ping-запросы с компьютера PC-A от каждого интерфейса маршрутизаторов R1, S1 и S3, а также от компьютера PC-C. Удалось ли получить все ответы?

_____

Если команды ping завершились неудачно и связь установить не удалось, исправьте ошибки в основных настройках устройства.

b. Необходимо получать ответ на ping-запросы с компьютера PC-C от каждого интерфейса маршрутизаторов R1, S1 и S3, а также от компьютера PC-A. Удалось ли получить все ответы?

_____

Если команды ping завершились неудачно и связь установить не удалось, исправьте ошибки в основных настройках устройства.

Часть 2: Настройка локального анализатора коммутируемых портов и сбор копируемого трафика с помощью ПО Wireshark

Для настройки локального анализатора коммутируемых портов необходимо настроить один или несколько исходных зеркалированных портов и один зеркалированный порт назначения для копирования или зеркалирования трафика. Исходные порты анализатора коммутируемых портов можно настроить для мониторинга трафика на входе, на выходе или в обоих направлениях (по умолчанию).

Исходный порт анализатора коммутируемых портов необходимо настроить на порту, который подключается к маршрутизатору через порт F0/5 коммутатора S1. Таким образом будет контролироваться весь входящий и исходящий трафик локальной сети. Порт назначения анализатора коммутируемых портов будет настроен на порту F0/6 коммутатора S1, подключенном к узлу PC-A, на котором работает Wireshark.

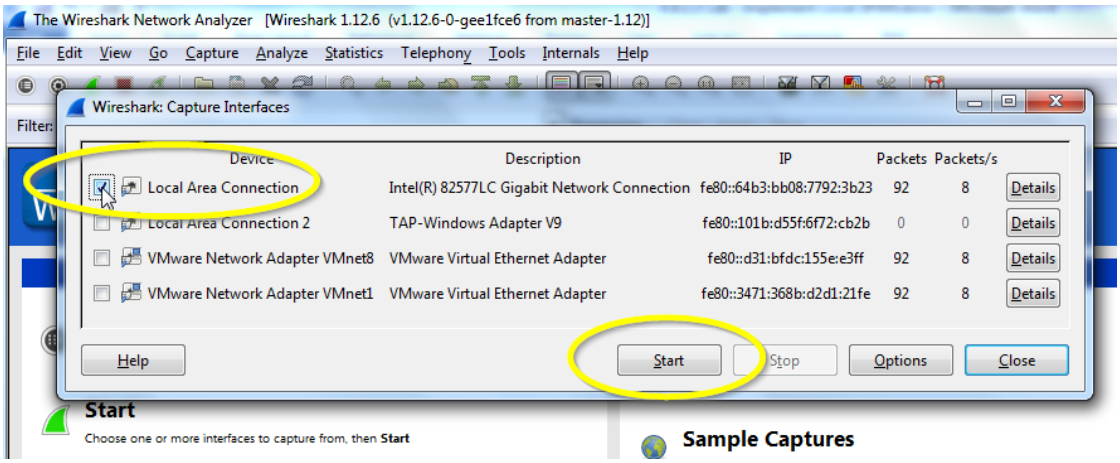
Шаг 1: Настройте анализатор коммутируемых портов на коммутаторе S1.

a. Подключитесь с консоли к S1 и настройте исходный и целевой порты мониторинга на коммутаторе S1. Теперь весь входящий и исходящий трафик на порту F0/5 будет копироваться и перенаправляться на порт F0/6.

```
S1(config)# monitor session 1 source interface f0/5
S1(config)# monitor session 1 destination interface f0/6
```

Шаг 2: Запустите сбор трафика с помощью ПО Wireshark на компьютере PC-A.

a. Откройте ПО Wireshark на компьютере PC-A, настройте для интерфейса сбора трафика подключение по локальной сети и щелкните **Start** (Начать).



Шаг 3: Подключитесь к маршрутизатору R1 по Telnet и создайте трафик ICMP в локальной сети.

a. Установите подключение по Telnet от S1 к R1.

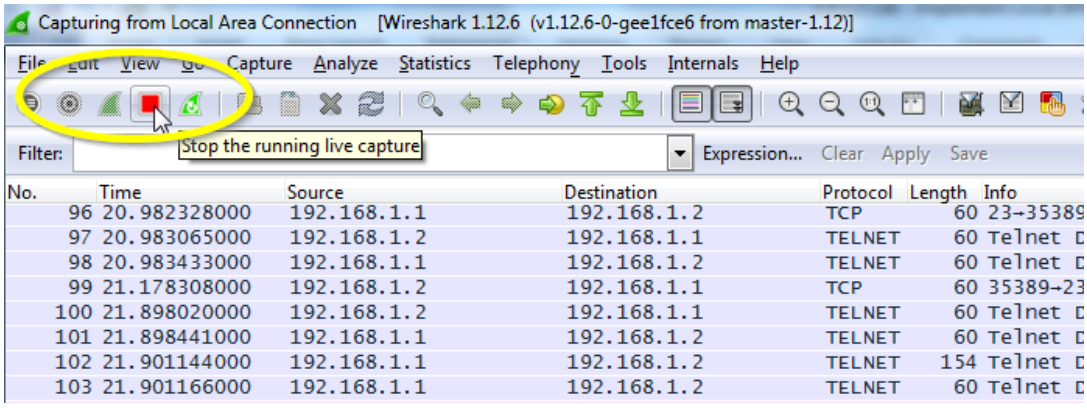
```
S1# Telnet 192.168.1.1
Trying 192.168.1.1. . . Open

User Access Verification

Password:
R1>
```

b. В привилегированном режиме отправьте эхо-запросы к PC-C, S1 и S3.

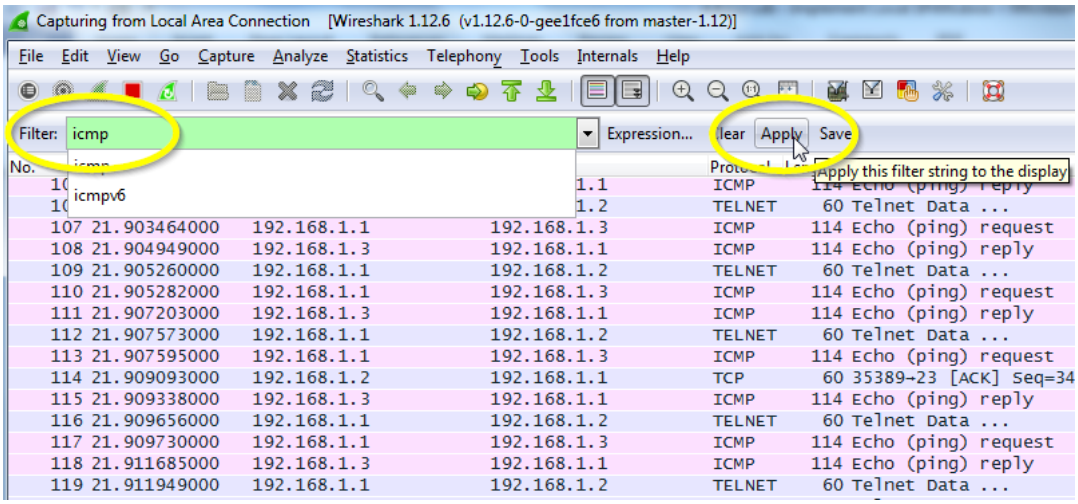
```
R1> enable
Password:
R1# ping 192.168.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R1# ping 192.168.1.2
<Выходные данные опущены>
R1# ping 192.168.1.3
<Выходные данные опущены>
```

Шаг 4: Остановите сбор трафика с помощью Wireshark на PC-A и выполните фильтрацию трафика ICMP.

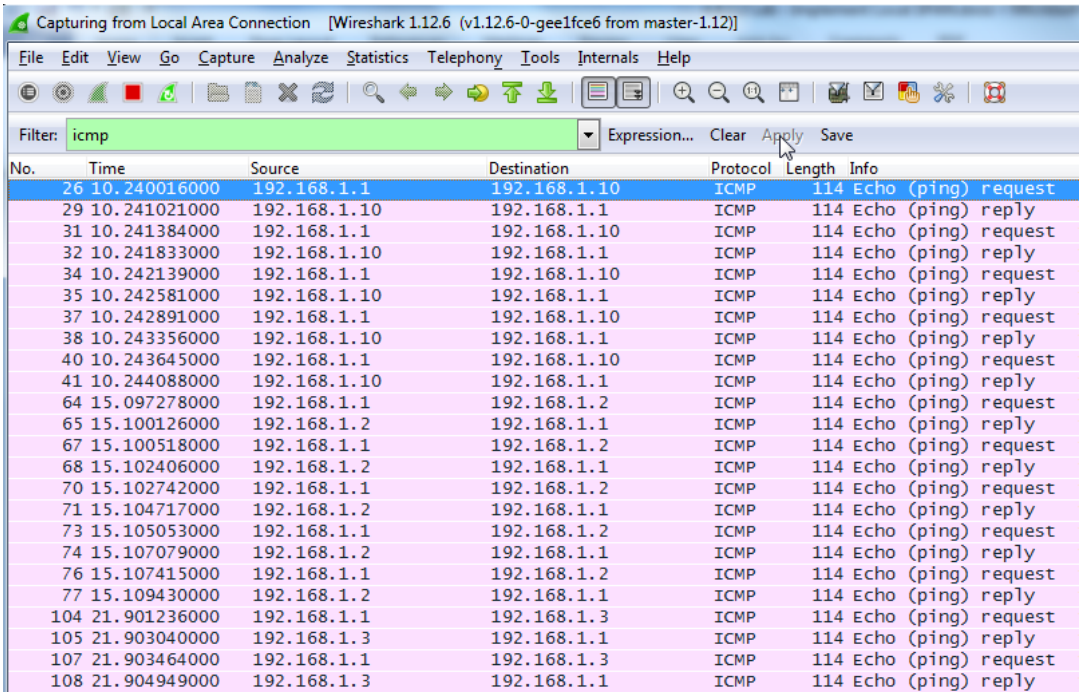
a. Вернитесь на компьютер PC-A и остановите захват трафика программой Wireshark.



b. Отфильтруйте ICMP-пакеты в трафике, собранном Wireshark.



c. Изучите отфильтрованные ICMP-пакеты в трафике, собранном Wireshark.



No.	Time	Source	Destination	Protocol	Length	Info
26	10.240016000	192.168.1.1	192.168.1.10	ICMP	114	Echo (ping) request
29	10.241021000	192.168.1.10	192.168.1.1	ICMP	114	Echo (ping) reply
31	10.241384000	192.168.1.1	192.168.1.10	ICMP	114	Echo (ping) request
32	10.241833000	192.168.1.10	192.168.1.1	ICMP	114	Echo (ping) reply
34	10.242139000	192.168.1.1	192.168.1.10	ICMP	114	Echo (ping) request
35	10.242581000	192.168.1.10	192.168.1.1	ICMP	114	Echo (ping) reply
37	10.242891000	192.168.1.1	192.168.1.10	ICMP	114	Echo (ping) request
38	10.243356000	192.168.1.10	192.168.1.1	ICMP	114	Echo (ping) reply
40	10.243645000	192.168.1.1	192.168.1.10	ICMP	114	Echo (ping) request
41	10.244088000	192.168.1.10	192.168.1.1	ICMP	114	Echo (ping) reply
64	15.097278000	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request
65	15.100126000	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply
67	15.100518000	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request
68	15.102406000	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply
70	15.102742000	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request
71	15.104717000	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply
73	15.105053000	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request
74	15.107079000	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply
76	15.107415000	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request
77	15.109430000	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply
104	21.901236000	192.168.1.1	192.168.1.3	ICMP	114	Echo (ping) request
105	21.903040000	192.168.1.3	192.168.1.1	ICMP	114	Echo (ping) reply
107	21.903464000	192.168.1.1	192.168.1.3	ICMP	114	Echo (ping) request
108	21.904949000	192.168.1.3	192.168.1.1	ICMP	114	Echo (ping) reply

d. Были ли ping-запросы от R1 к PC-C, S1 и S3 успешно скопированы и перенаправлены с порта F0/6 на PC-A?

_____

e. Выполнялся ли мониторинг и копирование трафика в обоих направлениях? _____

Вопросы для повторения

В данном сценарии не лучше ли было использовать систему обнаружения (IDS) или предотвращения (IPS) вторжений вместо PC-A и анализатора трафика пакетов?

_____

_____

Сводная таблица по интерфейсам маршрутизаторов

Сводка по интерфейсам маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet № 1**	**Интерфейс Ethernet № 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 ISDN BRI. Строка в скобках — это официальное сокращение, которое можно использовать в командах Cisco IOS для обозначения интерфейса.