Лабораторная работа. Сбор и анализ данных NetFlow

Топология

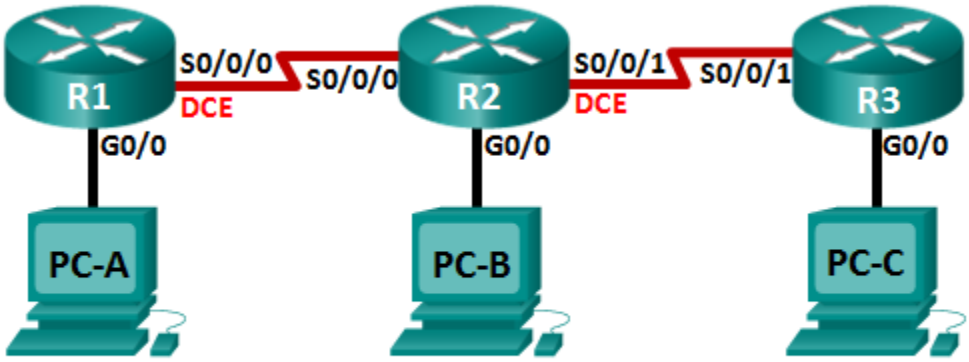

Таблица адресации

Устройство	Интерфейс	IP-адрес	Шлюз по умолчанию
R1	G0/0	192.168.1.1/24	Недоступно
	S0/0/0 (DCE)	192.168.12.1/30	Недоступно
R2	G0/0	192.168.2.1/24	Недоступно
	S0/0/0	192.168.12.2/30	Недоступно
	S0/0/1 (DCE)	192.168.23.1/30	Недоступно
R3	G0/0	192.168.3.1/24	Недоступно
	S0/0/1	192.168.23.2/30	Недоступно
PC-A	NIC	192.168.1.3	192.168.1.1
PC-B	NIC	192.168.2.3	192.168.2.1
PC-C	NIC	192.168.3.3	192.168.3.1

Задачи

Часть 1. Создание сети и настройка базовых параметров устройств

Часть 2. Настройка NetFlow на маршрутизаторе

Часть 3. Анализ NetFlow с помощью интерфейса командной строки

Часть 4. Изучение ПО сбора данных и анализатора NetFlow

Исходные данные/сценарий

NetFlow — это технология Cisco IOS, предоставляющая статистические данные о пакетах, проходящих через маршрутизатор или многоуровневый коммутатор Cisco. NetFlow обеспечивает контроль сети и безопасности, планирование сетевых ресурсов, анализ трафика и учёт IP. Важно не путать назначение и результаты NetFlow с назначением и результатами оборудования и программного обеспечения для сбора пакетов. Средства сбора пакетов записывают всю входящую и исходящую информацию сетевого устройства для последующего анализа, в то время как NetFlow собирает только определённую статистическую информацию.

Flexible NetFlow — это новейшая версия технологии NetFlow, которая расширяет возможности первоначального протокола NetFlow, позволяя настраивать параметры анализа трафика. Flexible NetFlow использует формат экспорта версии 9. Начиная с Cisco IOS версии 15.1, поддерживаются многие полезные команды Flexible NetFlow.

В этой лабораторной работе вам потребуется настроить NetFlow для сбора данных входящих и исходящих пакетов. С помощью команды **show** вы сможете проверить, что NetFlow находится в рабочем состоянии и осуществляет сбор статистических данных. Вы также рассмотрите доступные варианты ПО сборщика данных и анализатора NetFlow.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интеграцией сервисов Cisco 1941 (ISR) под управлением ОС Cisco IOS версии 15.2(4) M3 (образ universalk9). Возможно использование других маршрутизаторов и версий Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейсов указаны в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не содержат файла загрузочной конфигурации. Если вы не уверены в этом, обратитесь к инструктору.

Необходимые ресурсы:

- 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 3 компьютера (под управлением Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Построение сети и базовая настройка устройств

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

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Выполните запуск и перезагрузку маршрутизаторов.

Шаг 3: Произведите базовую настройку маршрутизаторов.

a. Отключите поиск DNS.

b. Настройте имена устройств в соответствии с топологией.

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

d. Назначьте cisco в качестве пароля консоли и виртуального терминала VTY и включите запрос пароля при подключении.

e. Зашифруйте пароли.

f. Настройте баннер MOTD (сообщение дня) для предупреждения пользователей о запрете несанкционированного доступа.

g. Настройте **logging synchronous** на линии консоли.

h. Настройте тактовую частоту на всех последовательных интерфейсах DCE на **128000**.

i. Настройте IP-адреса, как указано в таблице адресации.

j. Настройте OSPF с использованием идентификатора процесса 1 и объявите все сети. Интерфейсы Ethernet должны быть пассивными.

k. Создайте учётную запись в локальной базе данных на маршрутизаторе R3 с именем пользователя **admin** и паролем **cisco** и с уровнем привилегий **15**.

l. На маршрутизаторе R3 включите службу HTTP и настройте проверку подлинности пользователей HTTP с помощью локальной базы данных.

m. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

Шаг 4: Настройте узлы.

Шаг 5: Проверьте связь между конечными устройствами.

Все устройства должны иметь возможность отправлять эхо-запросы другим устройствам в топологии. При необходимости устраните неисправности, пока связь между конечными устройствами не будет установлена.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение брандмауэра на ПК.

Часть 2: Настройка NetFlow на маршрутизаторе

В части 2 вы должны будете настроить NetFlow на маршрутизаторе R2. NetFlow собирает весь входящий и исходящий трафик на последовательных интерфейсах R2 и экспортирует данные на сборщик данных NetFlow — ПК B. Для экспорта данных на сборщик NetFlow будет использоваться Flexible NetFlow версии 9.

Шаг 1: Настройте сбор данных NetFlow.

Настройте сбор данных NetFlow на обоих последовательных интерфейсах. Выполните сбор данных из входящих и исходящих пакетов.

```
R2(config)# interface s0/0/0
R2(config-if)# ip flow ingress
R2(config-if)# ip flow egress
R2(config-if)# interface s0/0/1
R2(config-if)# ip flow ingress
R2(config-if)# ip flow egress
```

Шаг 2: Настройте экспорт данных NetFlow.

С помощью команды **ip flow-export destination** определите IP-адрес и порт UDP сборщика данных NetFlow, на который маршрутизатор должен экспортировать данные NetFlow. Для данной настройки будет использоваться номер порта UDP 9996.

```
R2(config)# ip flow-export destination 192.168.2.3 9996
```

Шаг 3: Настройте версию экспорта NetFlow.

Маршрутизаторы Cisco под управлением IOS 15.1 поддерживают NetFlow версии 1, 5 и 9. Версия 9 — это наиболее универсальный формат экспорта данных, однако он не совместим с более ранними версиями. Для установки версии NetFlow используйте команду **ip flow-export version**.

```
R2(config)# ip flow-export version 9
```

Шаг 4: Выполните проверку конфигурации NetFlow.

a. Введите команду **show ip flow interface** для просмотра сведений об интерфейсе сбора данных NetFlow.

```
R2# show ip flow interface
Serial0/0/0
  ip flow ingress
  ip flow egress
Serial0/0/1
  ip flow ingress
  ip flow egress
```

b. Введите команду **show ip flow export** для просмотра сведений об экспорте данных NetFlow.

```
R2# show ip flow export
Flow export v9 is enabled for main cache
  Export source and destination details :
  VRF ID : Default
    Destination(1)  192.168.2.3 (9996)
  Version 9 flow records
  388 flows exported in 63 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
```

Часть 3: Анализ NetFlow с помощью интерфейса командной строки

В части 3 вы должны будете генерировать трафик данных между маршрутизаторами R1 и R3 для наблюдения за работой технологии NetFlow.

Шаг 1: Создайте трафик данных между маршрутизаторами R1 и R3.

a. Подключитесь по Telnet от маршрутизатора R1 к маршрутизатору R3 с использованием IP-адреса 192.168.3.1. Введите пароль **cisco** для перехода в пользовательский режим. Введите пароль **class** для включения глобального режима ввода. Введите команду **show run**, чтобы создать трафик Telnet. Не закрывайте текущий сеанс Telnet.

b. На маршрутизаторе R3 введите команду **ping 192.168.1.1 repeat 1000**, чтобы отправить эхо-запрос на интерфейс G0/0 маршрутизатора R1. Будет создан трафик ICMP через маршрутизатор R2.

c. На компьютере ПК A перейдите к маршрутизатору R3, используя IP-адрес 192.168.3.1. Войдите в систему с именем пользователя **admin** и паролем **cisco**. После входа в маршрутизатор R3 оставьте браузер открытым.

Примечание. Убедитесь, что в браузере отключено блокирование всплывающих окон.

Шаг 2: Выведите на экран сводную статистику NetFlow.

На маршрутизаторе R2 введите команду **show ip cache flow**, чтобы отобразить изменения в сводных данных NetFlow, включая распределение размеров пакета, информацию о потоках IP, записанные протоколы и активность интерфейса. Теперь протоколы отображают сводные данные.

```
R2# show ip cache flow
IP packet size distribution (5727 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .147 .018 .700 .000 .001 .001 .001 .001 .011 .009 .001 .002 .000 .001

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .001 .001 .097 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 114 added
  1546 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  0 active, 1024 inactive, 112 added, 112 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics 00:07:35
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet           4      0.0        27    43      0.2       5.0      15.7
TCP-WWW            104      0.2        14   275      3.4       2.1       1.5
ICMP                 4      0.0      1000   100      8.8      27.9      15.4

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Total:             112      0.2        50   146     12.5       3.1       2.5

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Se0/0/0       192.168.12.1    Null          224.0.0.5       59 0000 0000    43
Se0/0/1       192.168.23.2    Null          224.0.0.5       59 0000 0000    40
```

Шаг 3: Завершите сеансы Telnet и закройте браузер.

a. Введите команду **exit** на маршрутизаторе R1, чтобы отключить сеанс связи по Telnet с маршрутизатором R3.

b. Закройте сеанс браузера на компьютере ПК A.

Шаг 4: Удалите статистику NetFlow.

a. На маршрутизаторе R2 введите команду **clear ip flow stats**, чтобы удалить статистику NetFlow.

```
R2# clear ip flow stats
```

b. Повторно введите команду **show ip cache flow**, чтобы убедиться, что статистика NetFlow сброшена. Обратите внимание: даже несмотря на то, что вы больше не создаёте данные с помощью маршрутизатора R2, они по-прежнему принимаются NetFlow. В приведенном ниже примере адрес назначения для данного трафика — групповой адрес 224.0.0.5, это данные LSA OSPF.

```
R2# show ip cache flow
IP packet size distribution (124 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 1.00 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 2 added
  1172 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  2 active, 1022 inactive, 2 added, 2 added to flow
  0 alloc failures, 0 force free
  1 chunk, 0 chunks added
  last clearing of statistics 00:09:48
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
IP-other             2      0.0       193    79      0.6    1794.8       5.7
Total:               2      0.0       193    79      0.6    1794.8       5.7


SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Se0/0/0       192.168.12.1    Null          224.0.0.5       59 0000 0000    35

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Se0/0/1       192.168.23.2    Null          224.0.0.5       59 0000 0000    33
```

Часть 4: Изучение ПО сборщика данных и анализатора NetFlow

Программное обеспечение сборщика данных и анализатора NetFlow предоставляют многие производители. Некоторые программы распространяются бесплатно, другие — нет. По следующему URL-адресу размещена веб-страница с обзором некоторых бесплатных программ NetFlow: http://www.cisco.com/en/US/prod/iosswrel/ps6537/ps6555/ps6601/networking_solutions_products_genericcontent0900aecd805ff72b.html

Просмотрите эту веб-страницу, чтобы ознакомиться с некоторыми из доступных программных продуктов сборщика данных и анализатора NetFlow.

Вопросы на закрепление

1. В чём заключается назначение ПО сборщика данных NetFlow?

2. В чём заключается назначение программного анализатора NetFlow?

3. Перечислите семь основных полей, используемых первоначальным протоколом NetFlow для различения потоков данных.

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах 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 узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех сочетаний настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.