**Packet Tracer. Исследование реализации NetFlow**

**Задачи**

**Часть 1. Наблюдение за записью потоков NetFlow (одно направление)**

**Часть 2. Наблюдение за записью потоков NetFlow для сеанса, который входит в коллектор и выходит из него**

**Общие сведения**

В этом задании будет использоваться Packet Tracer для создания сетевого трафика и наблюдения за соответствующими записями потоков NetFlow в коллекторе NetFlow . Packet Tracer обеспечивает базовое моделирование функциональных возможностей NetFlow. Он не является заменой обучения технологии NetFlow на физическом оборудовании. Могут существовать некоторые различия между записями потоков NetFlow, созданными Packet Tracer , и записями, созданными полнофункциональным сетевым оборудованием.

**Часть 1.** **Наблюдение за записями потоков NetFlow в одну сторону**

**Шаг 1.** **Откройте коллектор NetFlow.**

a. В коллекторе NetFlow нажмите вкладку «Рабочий стол». Нажмите пиктограмму коллектора Netflow .

b. Нажмите переключатель “On” (Вкл.) для активации коллектора при необходимости. Задайте положение и размер окна таким образом, чтобы его было видно из окна топологии Packet Tracer .

**Шаг 2.** **Выполните ping-запрос на шлюз по умолчанию с ПК-1.**

a. Нажмите **РС-1**.

b. Откройте вкладку «Рабочий стол» и нажмите значок командной строки.

c. Введите команду **ping-запроса** для проверки связи со шлюзом по умолчанию на 10.0.0.1.

C:\> **ping 10.0.0.1**

d. После небольшой задержки на экране коллектора NetFlow отобразится круговая диаграмма.

**Примечание.** Первый набор ping-запросов не отправляется на коллектор NetFlow, поскольку ARP-процесс сначала должен распознать IP-адрес и MAC- адрес. Если через 30 секунд не отображается круговая диаграмма, то повторно отправьте ping-запрос на шлюз по умолчанию .

e. Нажмите по круговой диаграмме или записи условных обозначений для отображения сведений записи потока.

f. В записи потока буду записи, аналогичные тем, которые представлены в таблице ниже. У вас метки времени будут другими.

|  |  |  |
| --- | --- | --- |
| **Начальный уровень** | **Значение** | **Описание** |
| Распределение трафика | 100 % (1/1) | Это доля всего трафика, представленного данным потоком. |
| АДРЕС ИСТОЧНИКА IPV4 | 10.0.0.10 | Это IP-адрес источника пакетов потока. |
| АДРЕС НАЗНАЧЕНИЯ IPV4 | 10.0.0.1 | Это IP-адрес назначения пакетов потока. |
| ПОРТ ИСТОЧНИКА TRNS | 0 | Это порт источника транспортного уровня. Значение равняется 0 , поскольку это поток ICMP. |
| ПОРТ НАЗНАЧЕНИЯ TRNS | 0 | Это порт назначения транспортного уровня. Значение равняется 0, поскольку это поток ICMP. |
| ПРОТОКОЛ IP | 1 | Он определяет службу 4-го уровня, обычно 1 для ICMP, 6 для TCP и 17 для UDP. |
| первая метка времени | 00:47:49.593 | Это метка времени для начала потока. |
| последняя метка времени | 00:47:52.598 | Это метка времени для последнего пакета в потоке. |
| флаги tcp | 0x00 | Это значение флага TCP. В этом случае не участвовал сеанс TCP , поскольку протоколом являлся ICMP. |
| счетчик байтов | 512 | Это количество байтов в потоке. |
| счетчик пакетов | 4 | Это количество пакетов в потоке. |
| входной интерфейс | Gig0/0 | Это интерфейс экспортера потока, который собрал поток во входном направлении (вход в интерфейс устройства мониторинга). |
| выходной интерфейс | Null | Это интерфейс экспортера потока, который собрал поток в выходном направлении (выход из интерфейса устройства мониторинга). Значение Null, поскольку это был ping-запрос на входной интерфейс. |

В этом случае поток представляет ping-запрос ICMP с хоста 10.0.0.10 для 10.0.0.1. В потоке было четыре ping-пакета. Пакеты вошли в интерфейс Gig0/0 экспортера.

**Примечание.** В этом задании граничный маршрутизатор был настроен в качестве экспортера потока NetFlow. Интерфейс локальной сети настроен на мониторинг потоков, которые вошли из локальной сети. Последовательный интерфейс был настроен на сбор потоков, которые вошли из Интернета. Это было сделано для упрощения выполнения этого задания.

Для просмотра трафика, который соответствует полноценному двунаправленному сеансу, экспортер NetFlow нужно настроить на сбор потоков, которые входят в сеть и покидают ее.

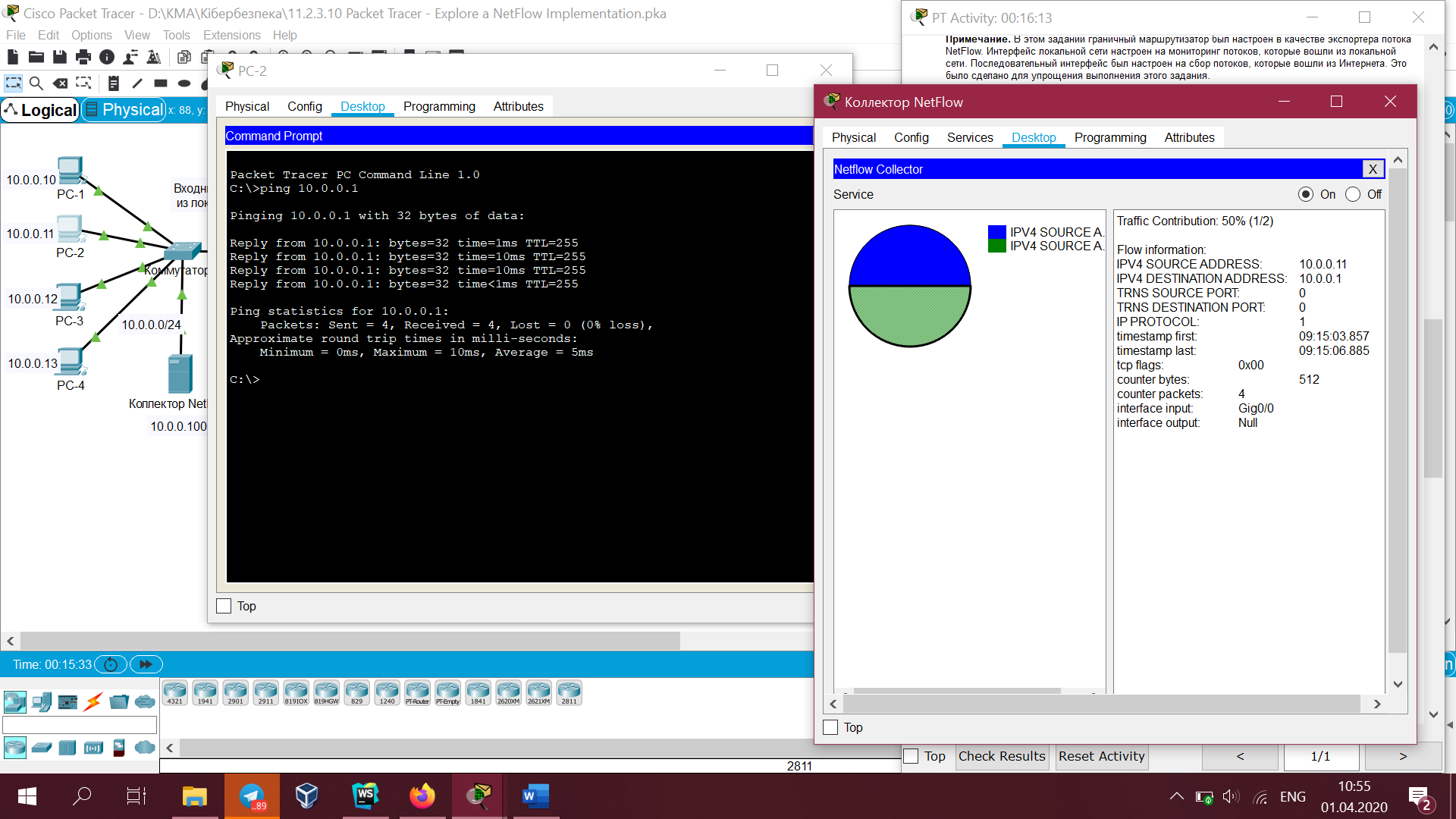
**Шаг 3.** **Создание дополнительного трафика.**

a. Нажмите **ПК-2 > Рабочий стол**.

b. Откройте командную строку и выполните **ping-запрос** на шлюз по умолчанию 10.0.0.1.

Что вы ожидаете увидеть в записях коллектора потоков NetFlow ? Изменится статистика для существующей записи потоков или в круговой диаграмме появится новый поток?

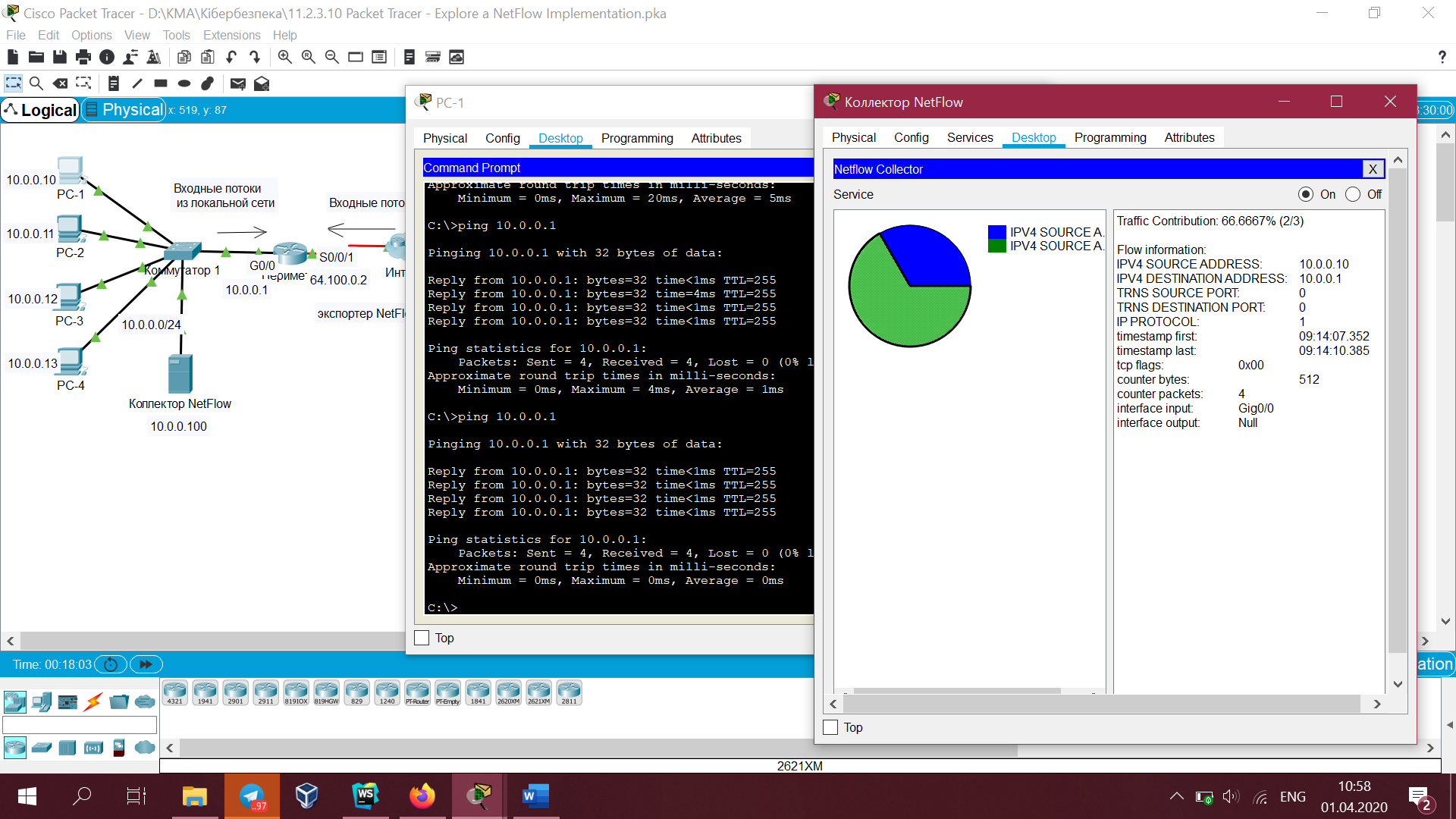
В колекторі з’явився новий потік. В даних змінився тільки ipv4 source address



c. Вернитесь к РС-1 и повторите ping-запрос на шлюз.

Как будет представлен этот трафик? В виде нового сегмента на круговой диаграмме или он изменит значения в существующей записи потока?

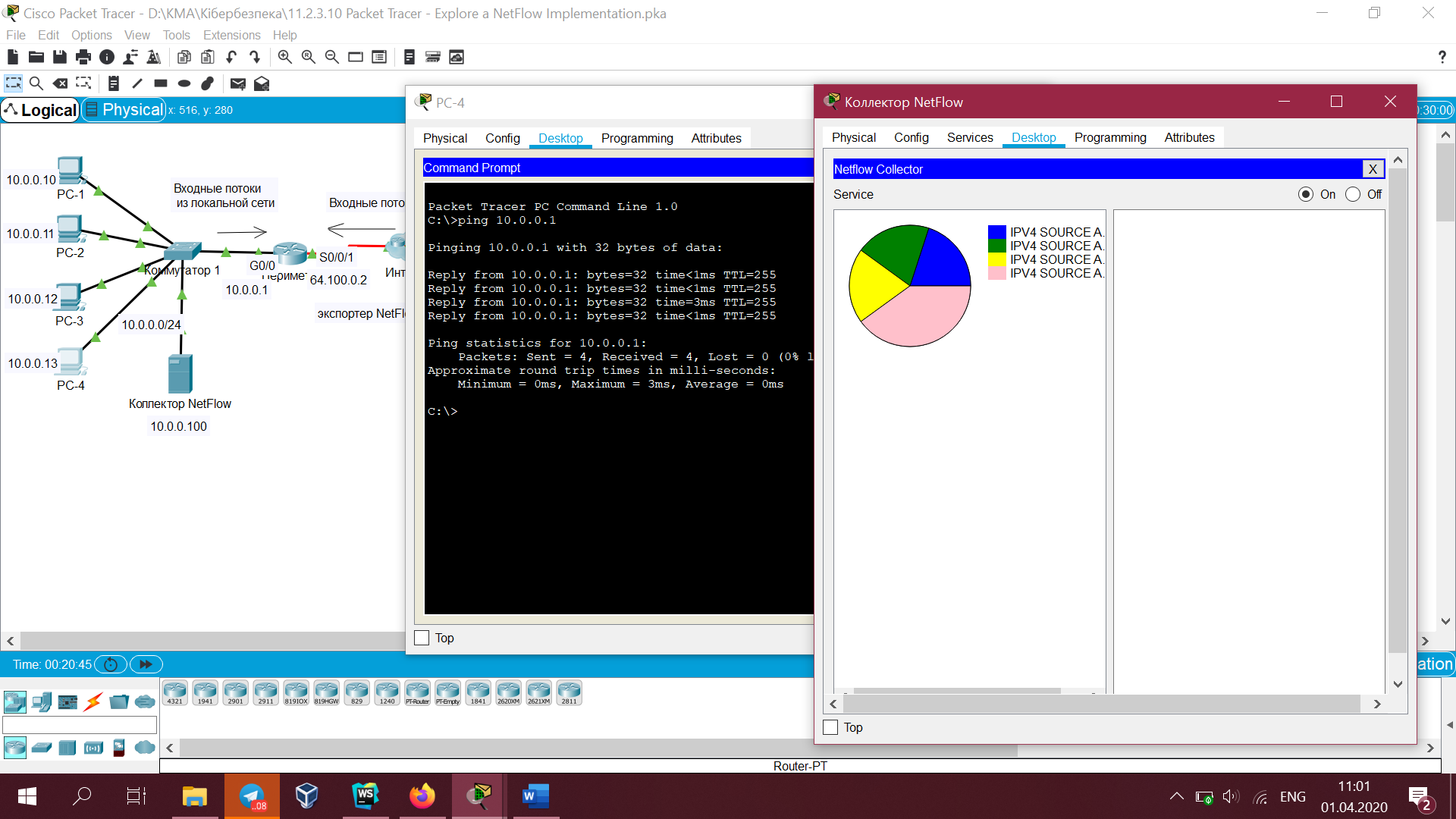
Змінився сам вигляд діаграми, але новий окремий сегмент не додався, просто попередній став в 2 рази більшим.



d. Отправьте ping-запросы с РС-3 и РС-4 на адрес шлюза по умолчанию.

Что произойдет с дисплеем в коллекторе потоков?

Додались два нові сегменти



**Часть 2.** **Наблюдайте записи NetFlow для сеанса, который поступает в коллектор и выходит из него**

Экспортер NetFlow был настроен для сбора данных о потоках , которые выходят из локальной сети и входят в маршрутизатор из Интернета.

**Шаг 1.** **Доступ к веб-серверу по IP-адресу.**

Прежде чем продолжить, запустите цикл коллектора NetFlow для очистки потоков.

a. Нажмите **Коллектор NetFlow > Физические параметры**.

b. Нажмите красную кнопку питания для отключения сервера. Повторно нажмите кнопку для включения сервера.

c. В коллекторе NetFlow нажмите вкладку «Рабочий стол».

d. Нажмите пиктограмму коллектора Netflow. Нажмите селективную кнопку On (Вкл.), чтобы активировать коллектор. Закройте окно средства сбора данных NetFlow Collector.

e. Прежде чем получить доступ к веб-серверу на РС-1, необходимо спрогнозировать количество потоков, которые будут присутствовать на круговой диаграмме? Дайте пояснение.

4потоки, два in два out

Опираясь на свои знания сетевых протоколов и NetFlow, спрогнозируйте значения для запросов веб-страницы, которые выходят из локальной сети.

|  |  |  |
| --- | --- | --- |
| **Поле записи** | **Значение** | **Рекомендации** |
| IP-адрес источника | 10.0.0.10 |  |
| IP-адрес назначения | 192.0.2.100 |  |
| Порт источника | 1025–5000 (MS Windows по умолчанию, которая аналогична используемой в PT). | Это динамически созданное приблизительное значение. |
| Порт назначения | 80 |  |
| Входной интерфейс | Gig0/0 |  |
| Выходной интерфейс | Se0/0/1 |  |

Прогнозирование значений для веб-страницы ответа, входящей в маршрутизатор экспортера NetFlow из Интернета.

|  |  |  |
| --- | --- | --- |
| **Поле записи** | **Значение** | **Рекомендации** |
| IP-адрес источника | 192.0.2.100 |  |
| IP-адрес назначения | 10.0.0.10 |  |
| Порт источника | 80 |  |
| Порт назначения | 1025–5000 | Это любое значение, случайно назначаемое из диапазона временных портов. |
| Входной интерфейс | Se0/0/1 |  |
| Выходной интерфейс | Gig0/0 |  |

f. Нажмите **ПК-1 > Рабочий стол**. Закройте окно командной строки при необходимости. Щелкните пиктограмму Web Browser (Веб-обозреватель).

g. В веб-обозревателе для ПК-1 введите 192.0.2.100 и нажмите **Go** (Перейти). Будет отображаться пример веб-страницы веб-сайта.

h. После короткой задержки в коллекторе NetFlow появится новая круговая диаграмма. Вы увидите по крайней мере два сегмента для запроса и ответа круговой HTTP. Возможно, вы также увидите третий сегмент, если истекло время ожидания PC-1 для кеша ARP.

i. Нажмите по каждому сегменту круговой HTTP для отображения записи и проверки прогнозов.

j. Выберите ссылку на страницу авторского права.

Что произошло? Дайте пояснение. (Подсказка. Сравните номер порта на хосте для потоков.)

Сравните потоки. Помимо таких очевидных характеристик, как метка времени, IP-адрес источника и пункта назначения, порты и интерфейсы, какие еще существуют различия между потоками запроса и ответа?

Кількість байтів та пакетів,що передаються

**Шаг 2.** **Доступ к веб-серверу по URL-адресу.**

a. Запустите цикл коллектора NetFlow для очистки потоков.

b. Включите службу коллектора Netflow.

c. До получения доступа к веб-серверу по этому URL. Что вы ожидаете увидеть на дисплее коллектора NetFlow?

діаграму розділену на 4 сегменти, 2 in 2 out

d. На РС-1 введите **www.example.com** в поле URL и нажмите **Go** (Перейти).

e. После отображения потоков изучите каждую запись потока.

Какие значения вы видите в поле протокола IP в записи потока? Что они обозначают?

ip protocol 17 for source 192.0.2.254( in) and ip protocol 6 for source 10.0.0.10 (out)