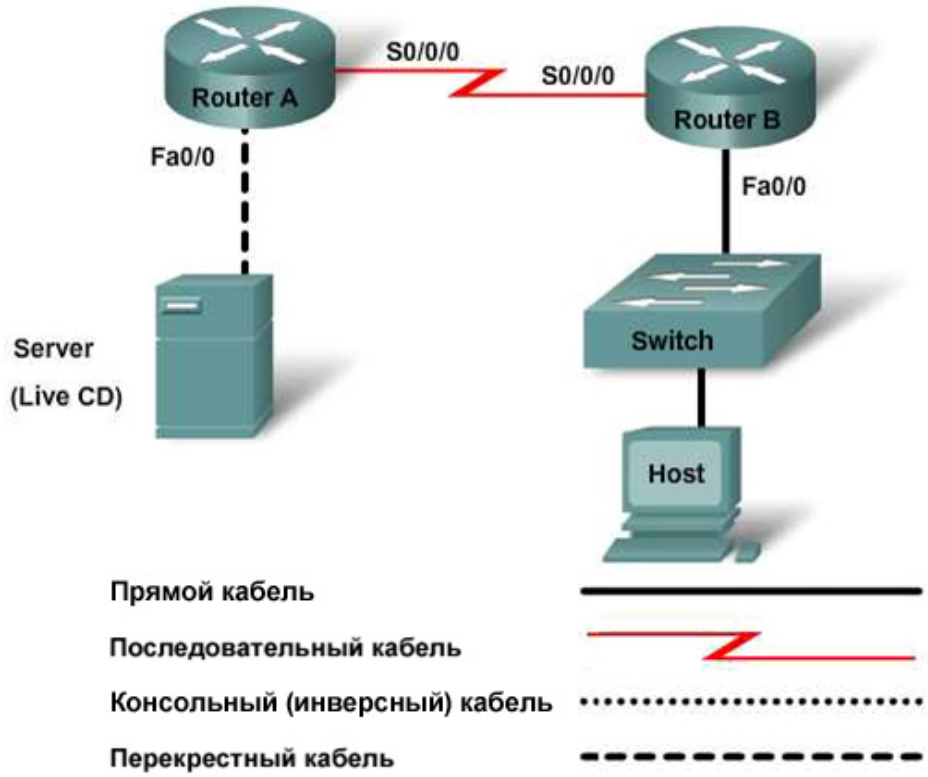
Лабораторная работа 1.2.2. Захват и анализ сетевого трафика



Имя узла	IP-адрес интерфейса Fa0/0	Маска подсети	IP-адрес интерфейса S0/0/0	Маска подсети	Шлюз по умолчанию
RouterA	172.17.0.1	255.255.0.0	192.168.1.1 (**DCE**)	255.255.255.0	Нет
RouterB	192.168.3.1	255.255.255.0	192.168.1.2	255.255.255.0	Нет
Server	172.17.1.1	255.255.0.0			172.17.0.1
Switch					
Host	192.168.3.2	255.255.255.0			192.168.3.1

Задачи

- С помощью анализатора Wireshark осуществить захват пакетов данных протоколов в процессе их передвижения по сетям.
- С помощью Wireshark произвести анализ захваченных пакетов данных.

Исходные данные/подготовка

В данной лабораторной работе рассматривается основная конфигурация маршрутизаторов Cisco 1841 или их аналогов с помощью команд программы Cisco IOS. Информация, содержащаяся в этой лабораторной работе, распространяется и на другие маршрутизаторы, однако синтаксис командного языка может отличаться. Настройка коммутатора Cisco Catalyst 2960 выполняется на заводе-изготовителе. Перед подключением к сети необходимо задать только основную информацию о безопасности.

Необходимо использовать следующие ресурсы:

- коммутатор Cisco 2960 или аналог;
- два маршрутизатора Cisco 1841 или аналога с одним или большим количеством последовательных интерфейсов и одним интерфейсом Fast Ethernet;
- два ПК с ОС Windows, один ПК с программой эмуляции терминала (один ПК используется в качестве узла, другой – в качестве сервера);
- консольный кабель с разъемами RJ-45 и DB-9 для настройки маршрутизаторов;
- два прямых кабеля Ethernet;
- один перекрестный кабель Ethernet;
- доступ к командной строке ПК;
- доступ к сетевой конфигурации TCP/IP ПК.

ПРИМЕЧАНИЕ. Убедитесь в том, что файлы начальной конфигурации всех маршрутизаторов и коммутатора удалены. Инструкции см. в конце лабораторной работы. Инструкции составлены и для коммутатора, и для маршрутизатора.

ПРИМЕЧАНИЕ. Маршрутизаторы SDM. Если для маршрутизатора SDM удалена начальная конфигурация, при перезагрузке маршрутизатора SDM он перестает отображаться по умолчанию. Необходимо создать основную конфигурацию маршрутизатора с использованием команд IOS. По вопросам обращайтесь к преподавателю.

Шаг 1. Подсоединение маршрутизаторов и настройка конфигурации

а. Подсоедините два маршрутизатора с помощью последовательного кабеля. Маршрутизатор подаст синхронизирующий (тактовый) сигнал для согласования времени работы двух маршрутизаторов. Соедините маршрутизаторы между собой посредством интерфейсов S0/0/0.

б. При настройке обоих маршрутизаторов используйте протокол RIP. Объявите соответствующие сети на каждом маршрутизаторе.

в. Подсоедините Fa0/0 на маршрутизаторе A с помощью перекрестного кабеля к серверу, на котором запущен установочный компакт-диск сервера "Discovery Server Live".

г. Подсоедините маршрутизатор B с помощью прямого кабеля, идущего от Fa0/0, к коммутатору через Fa0/1. Выполните настройку маршрутизаторов согласно схеме топологии (см. выше).

Шаг 2. Подсоединение узла к коммутатору и настройка конфигурации

Подключите узел к порту коммутатора Fa0/2. Выполните настройку коммутатора согласно схеме топологии (см. выше).

Шаг 3. Проверка связи с помощью команды ping

а. Для проверки связи выполните тестирование с использованием эхо-запросов с узла на сервер.

б. Если эхо-запрос выполнить не удалось, проверьте подсоединения и конфигурацию еще раз. Убедитесь в том, что все кабели подключены правильно и надежно. Проверьте правильность конфигурации узла, сервера и маршрутизатора.

в. Эхо-запрос обработан успешно? _____

Шаг 4. Запуск Wireshark

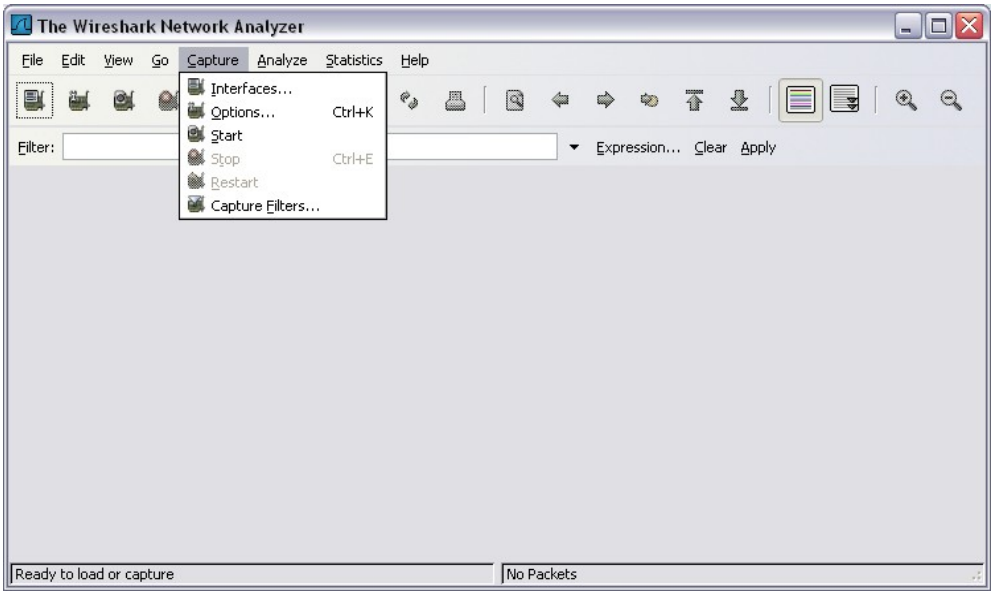
ПРИМЕЧАНИЕ. Wireshark можно загрузить по ссылке www.wireshark.org и установить на каждом локальном узле. Если такой возможности нет, Wireshark можно запустить с сервера Discovery, запускаемого с диска "Discovery Server Live". Проконсультируйтесь по этому поводу с преподавателем.

а. При запуске Wireshark с локального узла дважды щелкните по пиктограмме запуска приложения и выполните все шаги вплоть до шага г. В случае запуска Wireshark с сервера Discovery, выполните все шаги вплоть до шага б.

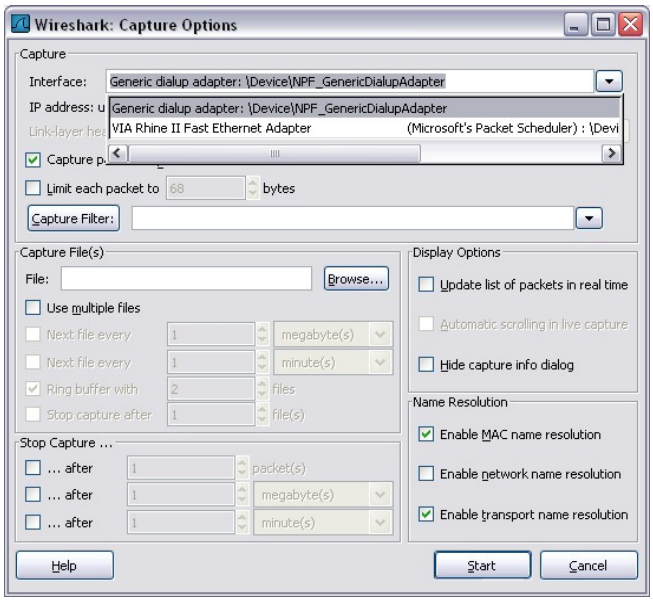
б. В меню **Start** (пуск) на рабочем столе сервера выберите **Internet> Wireshark Network Analyzer** (интернет> анализатор сетевых протоколов Wireshark).

в. Если программа Wireshark не открыта, запустите ее. По запросу введите пароль "**discoverit**".

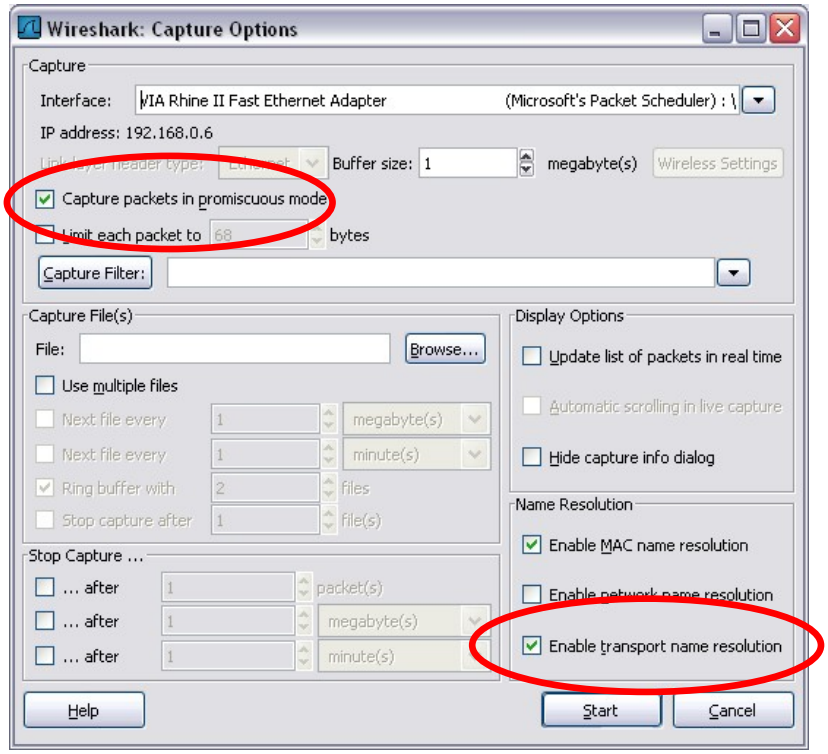
г. Чтобы начать процесс захвата данных, перейдите в меню **Capture** (захват) и нажмите **Options** (параметры). В диалоговом окне **Options** (параметры) представлены различные настройки и фильтры для определения степени захвата трафика.



д. Убедитесь в том, что Wireshark настроен на мониторинг нужного интерфейса. В раскрывающемся списке **Interface** (интерфейс) выберите используемый сетевой адаптер. Для большинства компьютеров таким адаптером является подключенный адаптер Ethernet.



е. После этого можно настроить другие параметры. Следующие параметры, обведенные красным, требуют повышенного внимания: **Capture packets in promiscuous mode** (режим "неразборчивого" захвата) и **Enable transport name resolution** (активация трансляции сетевых имен).



- **Перевод Wireshark в режим "неразборчивого" захвата**

  Если этот флажок *не* установлен, будет выполняться захват пакетов, предназначенных только для этого компьютера.

  Если этот флажок установлен, будет выполняться захват всех пакетов, предназначенных только для этого компьютера, а также всех пакетов, обнаруженных сетевой платой компьютера в том же сегменте сети (т.е. тех, которые "проходят" через сетевую плату, но не адресованы на этот компьютер).

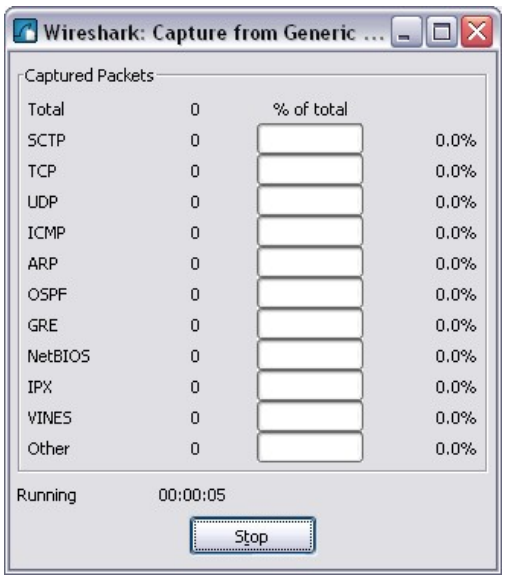
  ПРИМЕЧАНИЕ. Поскольку для подсоединения оконечных сетевых устройств вы используете различные промежуточные устройства (концентраторы, коммутаторы, маршрутизаторы), Wireshark выдаст различные результаты.

- **Перевод Wireshark в режим трансляции сетевых имен**

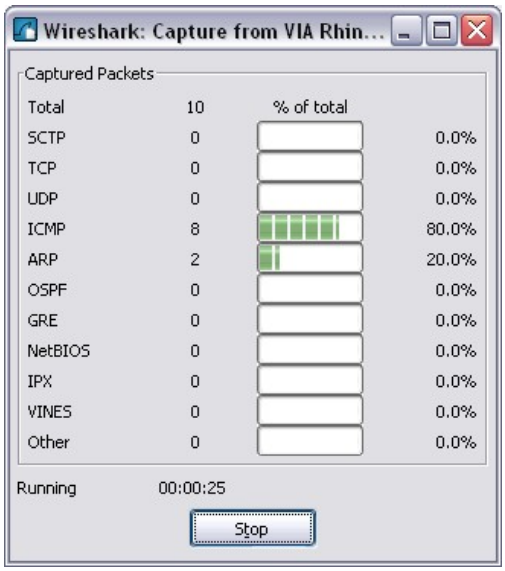
  Данный параметр позволяет установить/отменить режим трансляции сетевых адресов, обнаруженных в пакетах PDU, в имена. Несмотря на полезность данной функции, процесс трансляции имен может добавить лишние пакеты к захваченным данным, что может исказить результаты анализа.

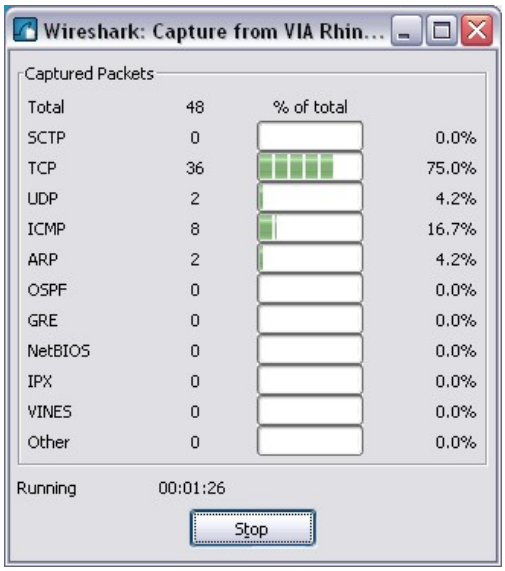
В этом диалоговом окне также имеется ряд фильтров и другие параметры процесса захвата пакетов.

- Нажатие кнопки **Start** (пуск) запускает процесс захвата данных. Ход выполнения процесса отображается в отдельном окне.
- Для захвата пакетов инициируйте трафик. Введите команды **`ping`** и **`tracert`** с узла и наблюдайте за обновлениями маршрута.

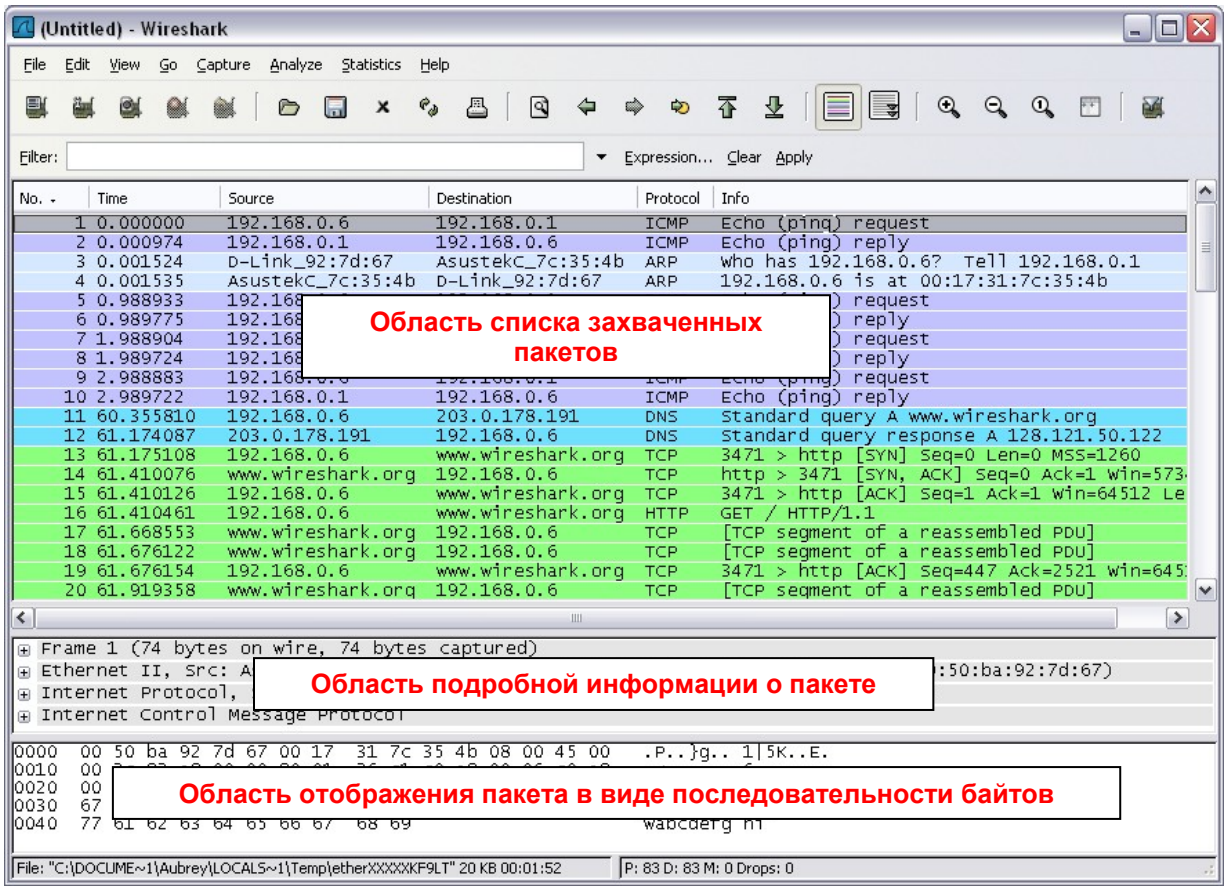


В процессе захвата пакетов в отдельном окне отображаются их типы и количество. Примеры иллюстрируют захват процесса обмена эхо-запросами и получение доступа к веб-странице.





- Нажатие кнопки **Stop** (стоп) останавливает процесс захвата данных. Появится основной экран. Экран анализатора Wireshark имеет 3 области.



- В верхней области отображается список захваченных пакетов и их основные данные. Щелчки на пакетах в этой области влияют на содержимое двух остальных областей.
- Средняя область отображает более подробные сведения о пакете, выделенном в верхней области.
- Нижняя область отображает тот же пакет в виде последовательности байтов (в шестнадцатеричном формате), причем выделяются байты, соответствующие полю данных, выбранному в верхней области, и выделенные в полях в средней области подробной информации о пакете.

Область списка захваченных пакетов

Каждая строка в этой области соответствует одному пакету захваченных данных. При выделении строки в данной области автоматически выделяются дополнительные сведения в области подробной информации о пакете и в области отображения пакетов в виде последовательности байтов. Пример показывает захваченные пакеты при выполнении эхо-запроса и установлении связи с сайтом http://www.Wireshark.org. В данной области выделен пакет №1.

Область подробной информации о пакете

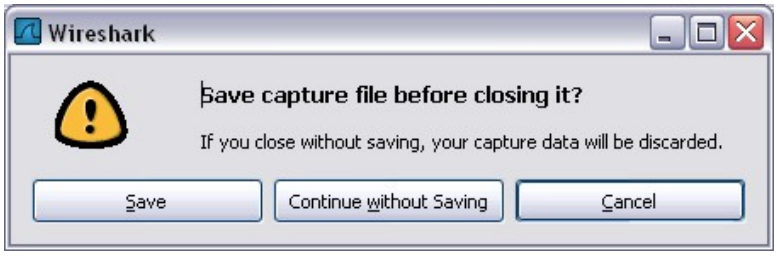
Данная область содержит подробные сведения о текущем пакете, который выделен в верхней области. В этой области отображаются типы протоколов и структура полей выбранного пакета. Средняя область показывает древовидную структуру (вложенность) полей пакета, которую можно сворачивать или разворачивать.

Область отображения пакета в виде последовательности байтов

Данная область дает шестнадцатеричное представление (в виде последовательности байтов) текущего пакета, который выделен в верхней области. В данной лабораторной работе эта область подробно рассматриваться не будет. Информация данной области полезна при необходимости более подробного анализа захваченных данных, а именно, бинарных значений и содержимого пакета.

Захваченную информацию пакета можно сохранить в файл. Этот файл можно впоследствии снова открыть в Wireshark для анализа, не прибегая к повторной процедуре захвата пакетов. Информация данного файла аналогична изначально захваченным данным.

При закрытии экрана захвата данных или завершении работы с Wireshark система попросит вас сохранить захваченные пакеты.



Нажатие кнопки **Continue without Saving** (продолжить без сохранения) закрывает файл или завершает работу Wireshark без сохранения отображенных захваченных данных.

Шаг 5. Эхо-запрос захвата пакетов PDU

а. Запустите Wireshark.

б. Задайте параметры захвата, как описано в шаге 4, и инициируйте процесс захвата пакетов.

в. Из командной строки узла выполните эхо-запрос IP-адреса сервера на другом конце лабораторной топологии. В данном случае выполните проверку связи с сервером Discovery Server Live CD с помощью команды **`ping 172.17.1.1`**.

г. После получения ответа об успешном установлении связи в окне ввода команды ping остановите процесс захвата.

Шаг 6. Изучение области списка захваченных пакетов

а. Область списка захваченных пакетов в Wireshark должна выглядеть примерно так:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	Cisco_79:f3:80	CDP/VTP/DTP/PAgP/UDLD	CDP	Device ID: ROUTER_A Port ID: FastEthernet0/0
2	4.959859	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
3	5.555085	192.168.3.2	172.17.1.1	ICMP	Echo (ping) request
4	5.555108	172.17.1.1	192.168.3.2	ICMP	Echo (ping) reply
5	6.557116	192.168.3.2	172.17.1.1	ICMP	Echo (ping) request
6	6.557137	172.17.1.1	192.168.3.2	ICMP	Echo (ping) reply
7	7.557337	192.168.3.2	172.17.1.1	ICMP	Echo (ping) request
8	7.557359	172.17.1.1	192.168.3.2	ICMP	Echo (ping) reply
9	8.557088	192.168.3.2	172.17.1.1	ICMP	Echo (ping) request
10	8.557111	172.17.1.1	192.168.3.2	ICMP	Echo (ping) reply
11	10.557548	Intel_56:98:68	Cisco_79:f3:80	ARP	Who has 172.17.0.1? Tell 172.17.1.1
12	10.558224	Cisco_79:f3:80	Intel_56:98:68	ARP	172.17.0.1 is at 00:0d:28:79:f3:80

б. Посмотрите на перечисленные пакеты; нас интересуют пакеты № 3 - № 10.

в. Найдите эквивалентные пакеты в списке пакетов на своем компьютере. Возможно, нумерация пакетов будет отличаться.

г. Исходя из данных списка захваченных пакетов в Wireshark, ответьте на следующие вопросы:

1) Какой протокол используется при эхо-тестировании связи?
_____

2) Укажите полное название протокола. _____

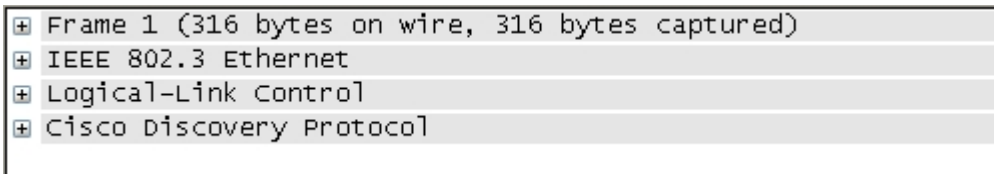
3) Как называются два сообщения ping? _____ и
_____

4) Соответствуют ли IP-адреса источника и назначения вашим ожиданиям? _____

5) Почему?
_____

Шаг 7. Изучение области подробной информации о пакете

а. Выделите мышью первый пакет эхо-запроса в списке. Область подробной информации о пакете должна иметь примерно следующий вид:



б. Щелкните каждый из символов "**+**", чтобы отобразить скрытую информацию. Область подробной информации о пакете будет иметь примерно следующий вид:

```
⊟ Frame 1 (316 bytes on wire, 316 bytes captured)
    Arrival Time: Aug 12, 2007 16:26:56.565057000
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 316 bytes
    Capture Length: 316 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:llc:cdp:data]
    [Coloring Rule Name: Routing]
    [Coloring Rule String: hsrp || eigrp || ospf || bgp || cdp || vrrp || gvrp || igmp || ismp]
⊟ IEEE 802.3 Ethernet
  ⊞ Destination: CDP/VTP/DTP/PAgP/UDLD (01:00:0c:cc:cc:cc)
  ⊞ Source: Cisco_79:f3:80 (00:0d:28:79:f3:80)
    Length: 302
⊟ Logical-Link Control
    DSAP: SNAP (0xaa)
    IG Bit: Individual
    SSAP: SNAP (0xaa)
    CR Bit: Command
  ⊞ Control field: U, func=UI (0x03)
    Organization Code: Cisco (0x00000c)
    PID: CDP (0x2000)
⊟ Cisco Discovery Protocol
    Version: 2
```

Как вы видите, имеется возможность развернуть элементы дерева полей и отобразить дополнительные сведения о протоколах.

в. Изучите эти элементы, пользуясь для просмотра полосой прокрутки. На данном этапе обучения вы, возможно, не совсем понимаете всю отображенную информацию. Запишите информацию, которая вам непонятна.

г. Найдите два разных типа отправителя и получателя.

Назовите их:

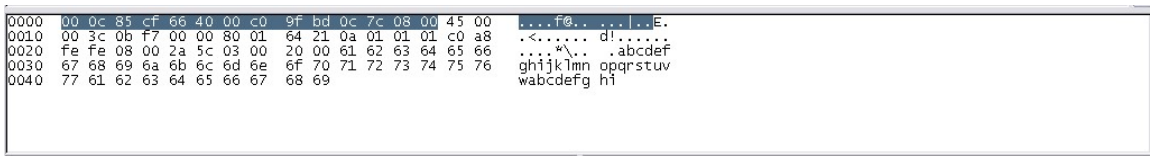
_____

Какие протоколы присутствуют в кадре Ethernet?

_____

д. Выделите строку в области подробной информации о пакете (средняя область). Обратите внимание на то, что вся или часть информации в области отображения пакета в виде последовательности байтов (байтовое представление) также становится выделенной.

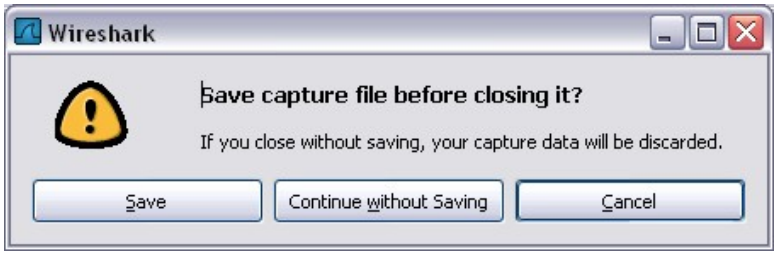
Например, если в области подробной информации о пакете выделена вторая строка (+ Ethernet II), то и в области байтового представления также будут выделены соответствующие значения.



Пример иллюстрирует определенные бинарные значения, представляющие эту информацию в пакете. На данном этапе обучения совсем необязательно скрупулезно разбираться в этой информации.

е. Перейдите в меню **File** (файл) и выберите команду **Close** (закрыть).

ж. При появлении следующего сообщения нажмите кнопку **Continue without Saving** (продолжить без сохранения).



Шаг 8. Захват FTP-пакетов

а. Допустим, что Wireshark продолжает работать после выполнения предыдущих шагов. В этом случае нажмите в меню **Capture** (захват) пункт **Start** (пуск).

б. В командной строке своего узла введите **ftp 172.17.1.1**. Как только соединение установлено, введите имя пользователя "**anonymous**".

в. После успешного входа в систему введите **get /pub/Discovery_1/document_1** и нажмите клавишу **ВВОД**. Обратите внимание на то, что после **get** нужен пробел. В результате данной команды начнется загрузка файла с FTP-сервера. Выходные данные должны выглядеть примерно так:

```
C:\> ftp 172.17.1.1
Connected to 172.17.1.1
220 Welcome to The CCNA-Discovery FTP service.
ftp> get /pub/Discovery_1/document_1
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for pub/Discovery_1/document_1
<73 bytes>.
226 File send OK.
ftp: 73 bytes received in 0.03Seconds 2.35Kbytes/sec.
```

г. После завершения загрузки файла введите команду **quit**.

```
ftp> quit
221 Goodbye.

C:\>
```

д. Остановите процесс захвата пакетов в Wireshark.

Шаг 9. Изучение области списка захваченных пакетов

а. Увеличьте размеры области списка захваченных пакетов и просмотрите все указанные пакеты.

б. Найдите и пометьте те пакеты, которые имеют отношение к процессу загрузки файла. Это будут пакеты протокола TCP (4-ый уровень) и FTP (7-ой уровень).

в. Определите три группы пакетов, связанных с процессом передачи файла. Первая группа пакетов связана с этапом установления соединения и входом в систему на сервере. Приведите примеры сообщений, обмен которыми произошел на данном этапе.

г. Найдите и приведите примеры сообщений, обмен которыми произошел на втором этапе непосредственного запроса загрузки и передачи данных.

д. Третья группа пакетов относится к выходу из системы и разрыву соединения. Приведите примеры сообщений, обмен которыми произошел на данном этапе.

е. Найдите пакеты протокола TCP, обмен которыми повторяется в процессе FTP. Какое свойство TCP это подчеркивает?

Шаг 10. Изучение области подробной информации о пакете и области байтового представления пакета

а. Выделите мышью первый пакет в списке, связанный с первым этапом процесса передачи данных по протоколу FTP. Просмотрите подробные сведения о пакете в соответствующей области.

б. Какие три протокола инкапсулированы в кадре?

_____

в. Выделите пакеты, содержащие имя пользователя и пароль. Изучите выделенные элементы в области байтового представления. Что эта информация сообщает о безопасности входа в систему по протоколу FTP?

_____

г. Выделите пакет, связанный со вторым этапом. Найдите пакет, содержащий имя файла, в любом из окон. Назовите имя загруженного файла.

_____

д. По завершении закройте рабочее окно Wireshark и продолжите, не сохраняя данные.

Шаг 11. Захват HTTP-пакетов

а. Инициируйте процесс захвата пакетов. Допустим, что Wireshark продолжает работать после выполнения предыдущих шагов, в этом случае нажмите в меню **Capture** (захват) пункт **Start** (пуск).

ПРИМЕЧАНИЕ. Если вы продолжаете последовательно выполнять шаги данной лабораторной работы, выполнять настройку параметров режима захвата не нужно.

б. Запустите веб-обозреватель на компьютере, на котором запущена программа Wireshark.

в. Введите IP-адрес сервера Discovery Server 172.17.1.1 в поле адреса. После того как веб-страница будет полностью загружена, остановите процесс захвата пакетов в Wireshark.

Шаг 12. Изучение области списка захваченных пакетов

а. Увеличьте размеры области списка захваченных пакетов и просмотрите все указанные пакеты.

б. Найдите пакеты протокола TCP и HTTP, имеющие отношение к процессу загрузки веб-страницы.

в. Обратите внимание на сходство сообщений, обмениваемых в данном процессе и в процессе передачи данных по протоколу FTP.

Шаг 13. Изучение области подробной информации о пакете и области байтового представления пакета

а. В области списка захваченных пакетов выделите HTTP-пакет с определением **(text/html)** в столбце **Info** (информация).

б. В области подробной информации щелкните значок "**+**" рядом с полем **Line-based text data: html** (строковые данные:html). Какие элементы отображаются при разворачивании дерева этого поля?

_____

в. Изучите выделенные элементы в области байтового представления. Эта часть окна отображает HTML-код, содержащийся в пакете.

г. По завершении закройте рабочее окно Wireshark и продолжите, не сохраняя данные.

Шаг 14. Анализ захваченных данных

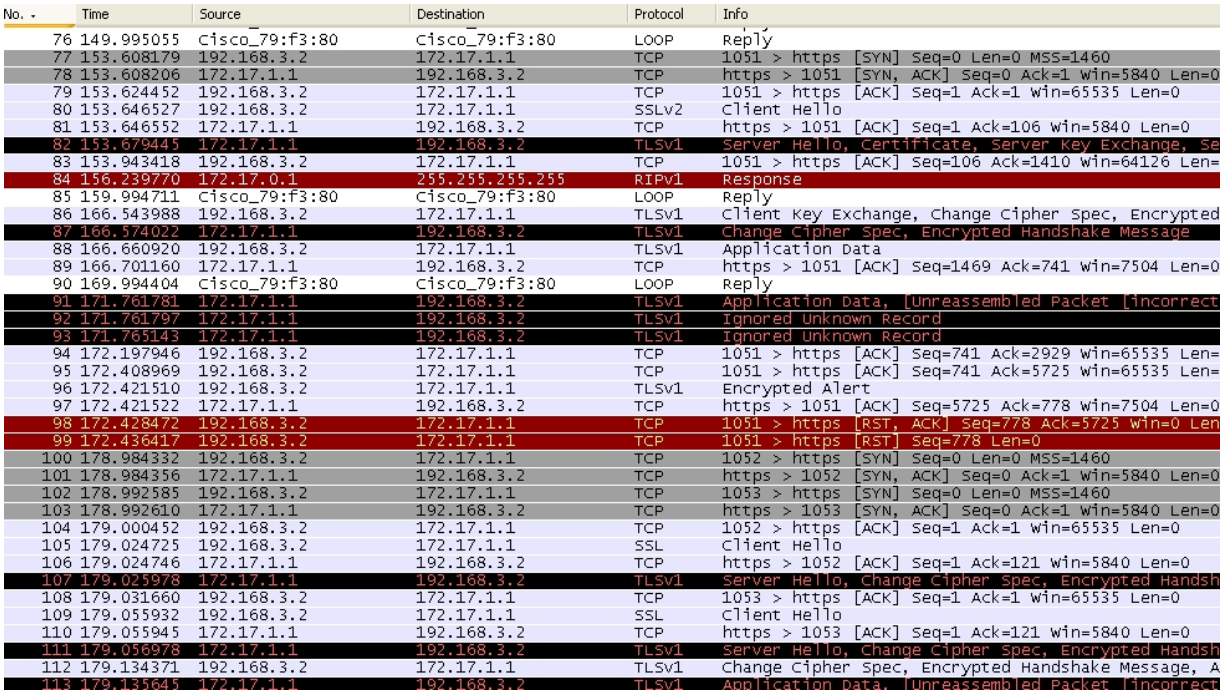
а. Посмотрите на захваченные данные примера (внизу) и изучите функции различных протоколов, использованных в данной сети.

No.	Time	Source	Destination	Protocol	Info
39	75.037581	Cisco_79:f3:80	CDP/VTP/DTP/PAgP/UDLD	CDP	Device ID: ROUTER_A Port ID: FastEthernet0/0
40	79.997380	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
41	82.124081	192.168.3.2	172.17.1.1	FTP	Request: QUIT
42	82.124211	172.17.1.1	192.168.3.2	FTP	Response: 221 Goodbye.
43	82.131646	172.17.1.1	192.168.3.2	TCP	ftp > 1042 [FIN, ACK] Seq=275 Ack=97 Win=5840 Le
44	82.141466	192.168.3.2	172.17.1.1	TCP	1042 > ftp [FIN, ACK] Seq=97 Ack=275 Win=65261 L
45	82.141482	172.17.1.1	192.168.3.2	TCP	ftp > 1042 [ACK] Seq=276 Ack=98 Win=5840 Len=0
46	82.148391	192.168.3.2	172.17.1.1	TCP	1042 > ftp [ACK] Seq=98 Ack=276 Win=65261 Len=0
47	89.997017	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
48	99.885642	172.17.0.1	255.255.255.255	RIPv1	Response
49	99.996682	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
50	109.996337	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
51	115.806501	192.168.3.2	172.17.1.1	TCP	1047 > http [SYN] Seq=0 Len=0 MSS=1460
52	115.806540	172.17.1.1	192.168.3.2	TCP	http > 1047 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=
53	115.822708	192.168.3.2	172.17.1.1	TCP	1047 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
54	115.886954	192.168.3.2	172.17.1.1	HTTP	GET / HTTP/1.1
55	115.886977	172.17.1.1	192.168.3.2	TCP	http > 1047 [ACK] Seq=1 Ack=403 Win=6432 Len=0
56	115.888244	172.17.1.1	192.168.3.2	HTTP	HTTP/1.1 200 OK (text/html)
57	115.888334	172.17.1.1	192.168.3.2	TCP	http > 1047 [FIN, ACK] Seq=1114 Ack=403 Win=643
58	116.068416	192.168.3.2	172.17.1.1	TCP	1047 > http [FIN, ACK] Seq=403 Ack=1114 Win=644
59	116.068430	172.17.1.1	192.168.3.2	TCP	http > 1047 [ACK] Seq=1115 Ack=404 Win=6432 Len=
60	116.075768	192.168.3.2	172.17.1.1	TCP	1047 > http [ACK] Seq=404 Ack=1115 Win=64422 Len
61	116.189037	192.168.3.2	172.17.1.1	TCP	1048 > http [SYN] Seq=0 Len=0 MSS=1460
62	116.189048	172.17.1.1	192.168.3.2	TCP	http > 1048 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=
63	116.205143	192.168.3.2	172.17.1.1	TCP	1048 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
64	116.259606	192.168.3.2	172.17.1.1	HTTP	GET /favicon.ico HTTP/1.1
65	116.259618	172.17.1.1	192.168.3.2	TCP	http > 1048 [ACK] Seq=1 Ack=334 Win=6432 Len=0
66	116.260609	172.17.1.1	192.168.3.2	HTTP	HTTP/1.1 404 Not Found (text/html)
67	116.260672	172.17.1.1	192.168.3.2	TCP	http > 1048 [FIN, ACK] Seq=464 Ack=334 Win=6432
68	116.348047	192.168.3.2	172.17.1.1	TCP	1048 > http [FIN, ACK] Seq=334 Ack=464 Win=6507
69	116.348059	172.17.1.1	192.168.3.2	TCP	http > 1048 [ACK] Seq=465 Ack=335 Win=6432 Len=(
70	116.355070	192.168.3.2	172.17.1.1	TCP	1048 > http [ACK] Seq=335 Ack=465 Win=65072 Len=
71	119.995999	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
72	128.964548	172.17.0.1	255.255.255.255	RIPv1	Response
73	129.995382	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
74	135.035662	Cisco_79:f3:80	CDP/VTP/DTP/PAgP/UDLD	CDP	Device ID: ROUTER_A Port ID: FastEthernet0/0
75	139.995357	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
76	149.995055	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply

б. Перечислите протоколы, использованные в сети на рисунке вверху.

_____

в. Изучите захваченные данные в примере внизу.



No.	Time	Source	Destination	Protocol	Info
76	149.995055	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
77	153.608179	192.168.3.2	172.17.1.1	TCP	1051 > https [SYN] Seq=0 Len=0 MSS=1460
78	153.608206	172.17.1.1	192.168.3.2	TCP	https > 1051 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
79	153.624452	192.168.3.2	172.17.1.1	TCP	1051 > https [ACK] Seq=1 Ack=1 Win=65535 Len=0
80	153.646527	192.168.3.2	172.17.1.1	SSLv2	Client Hello
81	153.646552	172.17.1.1	192.168.3.2	TCP	https > 1051 [ACK] Seq=1 Ack=106 Win=5840 Len=0
82	153.679445	172.17.1.1	192.168.3.2	TLSv1	Server Hello, Certificate, Server Key Exchange, Se
83	153.943418	192.168.3.2	172.17.1.1	TCP	1051 > https [ACK] Seq=106 Ack=1410 Win=64126 Len=
84	156.239770	172.17.0.1	255.255.255.255	RIPv1	Response
85	159.994711	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
86	166.543988	192.168.3.2	172.17.1.1	TLSv1	Client Key Exchange, Change Cipher Spec, Encrypted
87	166.574022	172.17.1.1	192.168.3.2	TLSv1	Change Cipher Spec, Encrypted Handshake Message
88	166.660920	192.168.3.2	172.17.1.1	TLSv1	Application Data
89	166.701160	172.17.1.1	192.168.3.2	TCP	https > 1051 [ACK] Seq=1469 Ack=741 Win=7504 Len=0
90	169.994404	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
91	171.761781	172.17.1.1	192.168.3.2	TLSv1	Application Data, [Unreassembled Packet [incorrect
92	171.761797	172.17.1.1	192.168.3.2	TLSv1	Ignored Unknown Record
93	171.765143	172.17.1.1	192.168.3.2	TLSv1	Ignored Unknown Record
94	172.197946	192.168.3.2	172.17.1.1	TCP	1051 > https [ACK] Seq=741 Ack=2929 Win=65535 Len=
95	172.408969	192.168.3.2	172.17.1.1	TCP	1051 > https [ACK] Seq=741 Ack=5725 Win=65535 Len=
96	172.421510	192.168.3.2	172.17.1.1	TLSv1	Encrypted Alert
97	172.421522	172.17.1.1	192.168.3.2	TCP	https > 1051 [ACK] Seq=5725 Ack=778 Win=7504 Len=0
98	172.428472	192.168.3.2	172.17.1.1	TCP	1051 > https [RST, ACK] Seq=778 Ack=5725 Win=0 Len
99	172.436417	192.168.3.2	172.17.1.1	TCP	1051 > https [RST] Seq=778 Len=0
100	178.984332	192.168.3.2	172.17.1.1	TCP	1052 > https [SYN] Seq=0 Len=0 MSS=1460
101	178.984356	172.17.1.1	192.168.3.2	TCP	https > 1052 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
102	178.992585	192.168.3.2	172.17.1.1	TCP	1053 > https [SYN] Seq=0 Len=0 MSS=1460
103	178.992610	172.17.1.1	192.168.3.2	TCP	https > 1053 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
104	179.000452	192.168.3.2	172.17.1.1	TCP	1052 > https [ACK] Seq=1 Ack=1 Win=65535 Len=0
105	179.024725	192.168.3.2	172.17.1.1	SSL	Client Hello
106	179.024746	172.17.1.1	192.168.3.2	TCP	https > 1052 [ACK] Seq=1 Ack=121 Win=5840 Len=0
107	179.025978	172.17.1.1	192.168.3.2	TLSv1	Server Hello, Change Cipher Spec, Encrypted Handsh
108	179.031660	192.168.3.2	172.17.1.1	TCP	1053 > https [ACK] Seq=1 Ack=1 Win=65535 Len=0
109	179.055932	192.168.3.2	172.17.1.1	SSL	Client Hello
110	179.055945	172.17.1.1	192.168.3.2	TCP	https > 1053 [ACK] Seq=1 Ack=121 Win=5840 Len=0
111	179.056978	172.17.1.1	192.168.3.2	TLSv1	Server Hello, Change Cipher Spec, Encrypted Handsh
112	179.134371	192.168.3.2	172.17.1.1	TLSv1	Change Cipher Spec, Encrypted Handshake Message, A
113	179.135645	172.17.1.1	192.168.3.2	TLSv1	Application Data, [Unreassembled Packet [incorrect

г. Какие два протокола присутствуют в этих данных, но отсутствуют в ранее захваченных данных из предыдущего примера?

_____

д. Сравните результаты захвата в примере в шаге 14 с результатами второго захвата. В чем состоит ощутимая разница между протоколом HTTP и HTTPS?

_____

_____

Шаг 15. Вопросы для обсуждения

Как уровни моделей OSI и TCP/IP отражаются в сетевом трафике, захваченном с помощью анализатора Wireshark?

_____

_____

_____

Удаление начальной конфигурации и перезагрузка коммутатора

При выполнении большинства лабораторных работ в рамках курса CCNA Discovery необходимо использовать ненастроенный коммутатор. Использование коммутатора с существующей конфигурацией может привести к непредсказуемым результатам. Выполните следующие инструкции для подготовки коммутатора до выполнения лабораторной работы, чтобы предыдущие параметры конфигурации не влияли на процесс ее выполнения. Инструкции составлены для коммутаторов серии 2900 и 2950.

а. Перейдите в привилегированный режим EXEC, введя команду **enable**. Если система затребует пароль, введите **class** (если он не подходит, спросите пароль у преподавателя).

```
Switch>enable
```


б. Удалите информационный файл базы данных виртуальной локальной сети.

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]? [Enter]
Delete flash:vlan.dat? [confirm] [Enter]
%Error deleting flash:vlan.dat (No such file or directory)
```

в. Удалите файл начальной конфигурации коммутатора из NVRAM.

```
Switch#erase startup-config
Erasing the nvram filesystem will remove all files! Continue? [confirm]
Erase of nvram: complete
```

г. Убедитесь, что сведения о виртуальной локальной сети удалены.

д. Перезагрузите программное обеспечение, введя команду **reload**.

1) В привилегированном режиме EXEC введите команду **reload**:

```
Switch# reload
System configuration has been modified. Save? [yes/no]:
```

2) Введите **n**, а затем нажмите **ВВОД**.

```
Proceed with reload? [confirm] [Enter]
Reload requested by console.
Would you like to enter the initial configuration dialog? [yes/no]:
```

3) Введите **n**, а затем нажмите **ВВОД**.

```
Press RETURN to get started! [Enter]
```

Удаление начальной конфигурации и перезагрузка маршрутизатора

а. Перейдите в привилегированный режим EXEC, введя команду **enable**.

```
Router>enable
```

б. В привилегированном режиме EXEC введите команду **erase startup-config**.

```
Router#erase startup-config
Erasing the nvram filesystem will remove all files! Continue?
[confirm]
```

в. Для подтверждения нажмите **ВВОД**.

```
Erase of nvram: complete
```

г. В привилегированном режиме EXEC введите команду **reload**.

```
Router# reload
System configuration has been modified. Save? [yes/no]:
```

д. Введите **n**, а затем нажмите **ВВОД**.

```
Proceed with reload? [confirm]
```

е. Для подтверждения нажмите **ВВОД**.

```
Reload requested by console.
Would you like to enter the initial configuration dialog? [yes/no]:
```

ж. Введите **n**, а затем нажмите **ВВОД**.

```
Press RETURN to get started!
```

з. Нажмите **ВВОД**.

Основная IOS-конфигурация маршрутизатора SDM для загрузки SDM

Если из маршрутизатора SDM была удалена начальная конфигурация, SDM больше не сможет поддерживать настройки по умолчанию после перезапуска маршрутизатора. Необходимо создать основную конфигурацию следующим образом. Дополнительные сведения о настройке и использовании SDM можно получить в кратком руководстве пользователя по SDM:

http://www.cisco.com/en/US/docs/routers/access/cisco_router_and_security_device_manager/software/quick/guide/SDMq7.html

а. Задайте IP-адрес интерфейса Fa0/0 маршрутизатора.

```
Router(config)#interface Fa0/0
Router(config-if)#ip address 10.10.10.1 255.255.255.248
Router(config-if)#no shutdown
```

б. Включите сервер HTTP/HTTPS маршрутизатора, используя следующие команды Cisco IOS:

```
Router(config)#ip http server
Router(config)#ip http secure-server
Router(config)#ip http authentication local
```

в. Создайте учетную запись пользователя с уровнем привилегий 15 (привилегии полного доступа).

```
Router(config)#username <имя пользователя> privilege 15 password 0
<пароль>
```

г. Настройте протоколы SSH и Telnet для локального входа и уровня привилегий 15.

```
Router(config)#line vty 0 4
Router(config-line)#privilege level 15
Router(config-line)#login local
Router(config-line)#transport input telnet
Router(config-line)#transport input telnet ssh
Router(config-line)#exit
```