ICND1

Interconnecting Cisco Networking Devices Part 1

Версия 1.0

Руководство по лабораторным работам

Номер текста по каталогу: 97-2569-0–

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Содержание

ICND1

Руководство по лабораторным работам

Обзор

В этом руководстве представлены инструкции и другие сведения об упражнениях, которые необходимо выполнить во время данного курса. Решения можно найти в разделе «Ответы к лабораторным работам».

Общие сведения

Это руководство охватывает следующие упражнения:

- Лабораторная работа 1-1: Использование приложений Windows в качестве сетевых инструментов.
- Лабораторная работа 1-2: Обзор трехстороннего квитирования TCP.
- Лабораторная работа 1-3: Анализ расширенных данных сети ПК.
- Лабораторная работа 2-1: Подключение к удаленному лабораторному оборудованию.
- Лабораторная работа 2-2: Запуск коммутатора и его начальная настройка.
- Лабораторная работа 2-3: Повышение безопасности начальной конфигурации коммутатора.
- Лабораторная работа 2-4: Эксплуатация и настройка устройства Cisco IOS.
- Лабораторная работа 4-1: Преобразование десятичных чисел в двоичные и двоичных в десятичные.
- Лабораторная работа 4-2: Классификация способов сетевой адресации.
- Лабораторная работа 4-3: Расчет доступных подсетей и хостов.
- Лабораторная работа 4-4: Вычисление масок подсети
- Лабораторная работа 4-5: Начальный запуск маршрутизатора.
- Лабораторная работа 4-6: Начальная настройка маршрутизатора.
- Лабораторная работа 4-7: Повышение безопасности начальной конфигурации маршрутизатора

- Лабораторная работа 4-8: Использование Cisco SDM для настройки функций DHCP-сервера.
- Лабораторная работа 4-9: Управление сеансами удаленного доступа.
- Лабораторная работа 5-1: Подключение к сети Интернет.
- Лабораторная работа 5-2: Подключение к главному офису.
- Лабораторная работа 5-3: Обеспечение динамической маршрутизации к главному офису.
- Лабораторная работа 6-1: Использование протокола обнаружения Cisco.
- Лабораторная работа 6-2: Управление параметрами запуска маршрутизатора.
- Лабораторная работа 6-3: Управление устройствами Cisco.
- Лабораторная работа 6-4: Подтверждение реконфигурации сети филиала.
- Ответы.

Лабораторная работа 1-1: Использование приложений Windows в качестве сетевых инструментов.

Выполните упражнение этой лабораторной работы, чтобы применить на практике знания, полученные в соответствующем модуле.

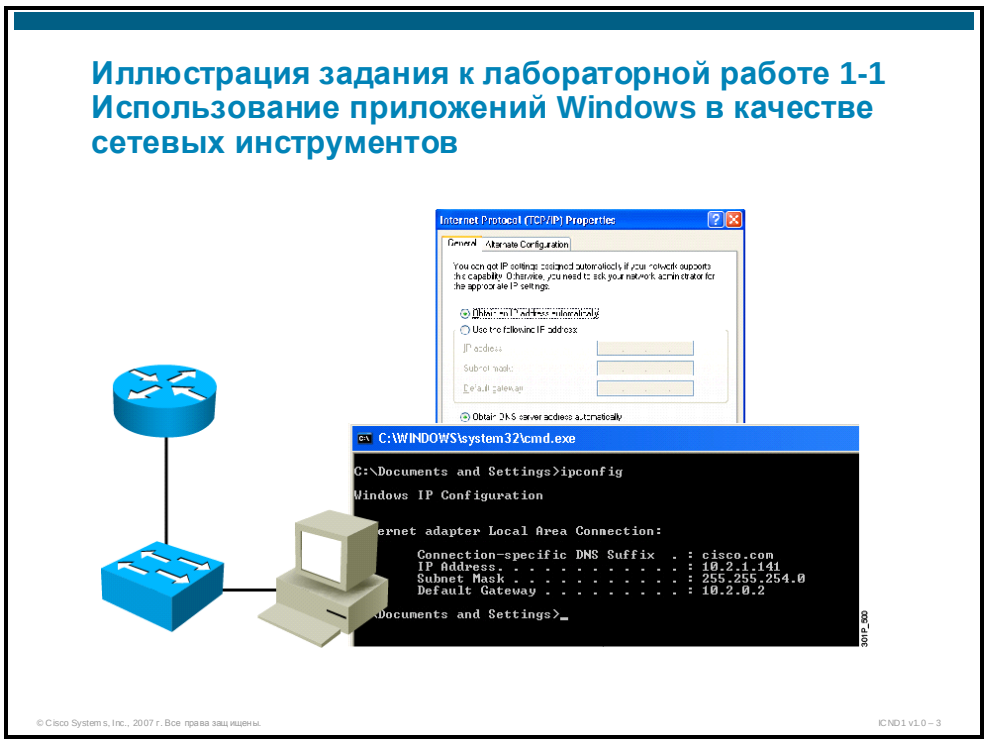
Задачи упражнения

В этом упражнении будут использоваться команды и приложения Windows для анализа IP-конфигурации ПК и локальной сети. После выполнения этого упражнения вы будете способны сделать следующее:

- получить сведения о текущих сетевых адресах ПК с помощью команды **ipconfig** ОС Windows;
- проверить подключение к маршрутизатору, который используется в качестве шлюза по умолчанию, с помощью команды **ping** ОС Windows;
- вывести таблицу ARP локальных ПК и определять связь между IP-адресом и MAC-адресом шлюза по умолчанию.

Иллюстрация задания

На рисунке ниже показано, что вы должны сделать во время данного упражнения.



Необходимые ресурсы

Ниже перечислены ресурсы и устройства, необходимые для выполнения упражнения.

- ПК, подключенный к исправной сети с доступом в Интернет.

Список команд

В таблице приводится описание команд, используемых в упражнении.

Команды Windows

Команда	Описание
arp -a	С помощью этой команды с параметром **–a** можно вывести таблицу ARP. Необходимо помнить, что записи таблицы ARP удаляются после 5 минут бездействия.
ipconfig	С помощью этой команды можно получить текущий IP-адрес, маску сети и IP-адрес шлюза по умолчанию.
ping	**ping (-t)**

Подсказки

Для этого упражнения доступны следующие подсказки.

- Для этой лабораторной работы нет подсказок.

Задача 1: Получение сведений о текущем IP-адресе

Чтобы получить сведения о текущем IP-адресе, используйте команду **ipconfig** ОС Windows. Чтобы получить доступ к командам Windows, откройте окно командной строки.

Процедура упражнения

Выполните следующие действия:

Действие 1 На рабочем столе Windows нажмите кнопку **Пуск**.

Действие 2 Выберите **Выполнить** и введите **cmd** в диалоговом окне «Выполнить». Для продолжения нажмите кнопку **OK**.

Действие 3 В командной строке введите **ipconfig.** При вводе этой команды используйте строчные буквы.

Действие 4 Вывод должен совпадать с одним из четырех приведенных ниже примеров.

Пример неудачного завершения 1. Вывод ниже указывает на отсутствие соединения – возможно, не подключен кабель Ethernet.

```
C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Media State . . . . . . . . . . . : Media disconnected
```

Пример неудачного завершения 2. Вывод ниже указывает, что ПК ожидает автоматического получения информации об IP-адресе. Этот вывод является промежуточным, ПК либо получит адрес, либо будет периодически повторять команду **ipconfig** до тех пор, пока ее вывод не будут соответствовать одному из оставшихся примеров.


```
C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    IP Address. . . . . . . . . . . . : 0.0.0.0
    Subnet Mask . . . . . . . . . . . : 0.0.0.0
    Default Gateway . . . . . . . . . :
```

Пример неудачного завершения 3. Вывод ниже указывает, что сетевому адаптеру ПК не удалось получить IP-адрес автоматически, поэтому ПК будет использовать сгенерированный локальный адрес. Получение адреса может казаться успешным, однако на самом деле соединение с сервером IP-адреса отсутствует. Этот адрес не может использоваться для сетевых подключений. Если отображаемый IP-адрес начинается с 169.254.*x.x*, ПК не имеет допустимого адреса.

```
C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    Autoconfiguration IP Address. . . : 169.254.249.221
    Subnet Mask . . . . . . . . . . . : 255.255.0.0
    Default Gateway . . . . . . . . . :
```

Пример успешного завершения 1. Вывод ниже указывает, что у ПК есть предварительно настроенный или автоматически полученный IP-адрес. Ваш IP-адрес, маска подсети и шлюз по умолчанию скорее всего будут отличаться от приведенных ниже.

```
C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : cisco.com
    IP Address. . . . . . . . . . . . : 192.168.1.105
    Subnet Mask . . . . . . . . . . . : 255.255.255.0
    Default Gateway . . . . . . . . . : 192.168.1.1
```

Действие 1 При возникновении проблем обращайтесь за помощью к инструктору. Продолжайте работу только при наличии допустимого IP-адреса.

Действие 2 Запишите полученные в результате выполнения команды **ipconfig** значения в строки ниже, они будут использоваться в следующих задачах.

IP-адрес ПК_____

IP-адрес шлюза по умолчанию_____

Проверка упражнения

Задание считается выполненным, если достигнут следующий результат:

- при выполнении команды **ipconfig** получены сведения о допустимом IP-адресе.

Задача 2: Просмотр сетевых параметров Ethernet-адаптера персонального компьютера

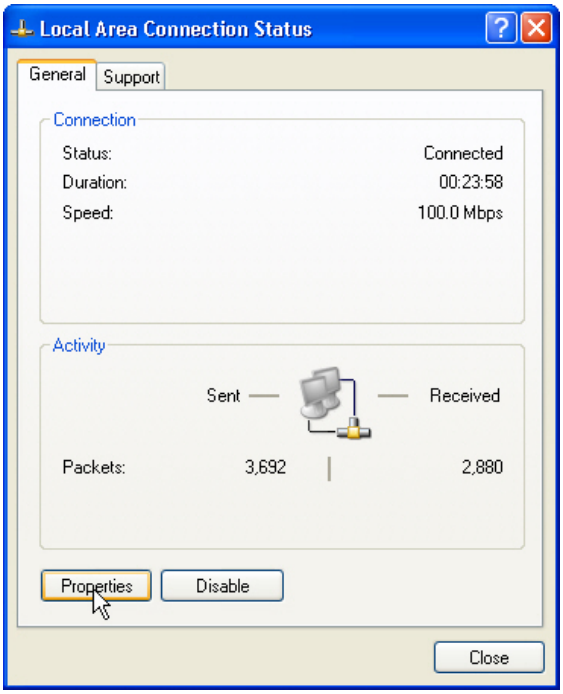
Используйте диалоговое окно свойств сети ОС Windows. В этой задаче вы будете только просматривать конфигурацию, однако, для изменения или ввода новых значений IP-адресов сети используется тот же процесс.

Процедура упражнения

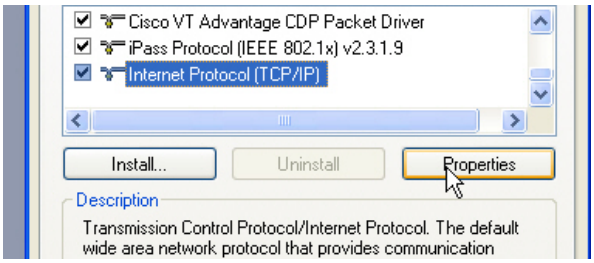
Выполните следующие действия:

Действие 1 На рабочем столе Windows щелкните ярлык **Подключение по локальной сети**.

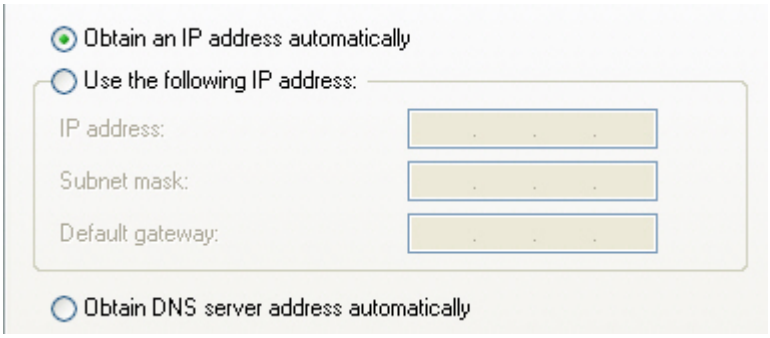
Действие 2 В окне состояния подключения по локальной сети нажмите кнопку **Свойства**.



Действие 3 С помощью прокрутки перейдите в нижнюю часть окна свойств подключения локальной сети и щелкните левой кнопкой мыши пункт **Протокол Интернета (TCP/IP)**, чтобы выделить его. Затем нажмите кнопку **Свойства**.

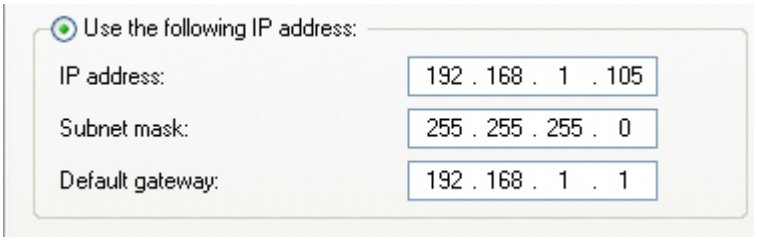


Действие 4 В окне свойств протокола Интернета (TCP/IP) может быть уже установлен переключатель «Получить IP-адрес автоматически», все поля будут пустыми.



Действие 5 Кроме того, вы можете увидеть переключатель «Использовать следующий IP-адрес», в этом случае в полях будут указаны IP-адреса, соответствующие выводу команды **ipconfig**, которую вы ввели ранее.

Примечание. Следующие данные приведены только для примера. *Не* изменяйте настройки.



Действие 6 Закройте все диалоговые окна и вернитесь на рабочий стол Windows.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- вы использовали окно свойств TCP/IP в ОС Windows для просмотра текущей конфигурации подключения по локальной сети;
- значения в свойств TCP/IP соответствуют выводу команды **ipconfig**.

Задача 3: Проверка соединения с маршрутизатором, используемым в качестве шлюза по умолчанию

Вы должны проверить соединение с сетью с помощью команды **ping** ОС Windows. В выводе этой команды указывается, был ли эхо-запрос обработан успешно, и приводится время прохождения сигнала в прямом и обратном направлении.

Процедура упражнения

Выполните следующие действия:

Действие 1 В командной строке введите команду **ping** с адресом шлюза по умолчанию, полученным во время задачи 1.

Действие 2 В первом примере показан неудачного вывода команды **ping**. При получении такого вывода следует обратиться за помощью к инструктору.

Пример неудачного завершения. Вывод ниже указывает, что от целевого IP-адреса не был получен ответ.

```
C:\Documents and Settings>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Пример успешного завершения. Вывод ниже указывает на успешное получение ответов от целевого IP-адреса.

```
C:\Documents and Settings>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Действие 3 Обратите внимание, что по умолчанию эта команда Windows отправляет четыре пакета эхо-запросов (эхо-запросов ICMP).

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- вы использовали команду **ping** ОС Windows для проверки подключения к маршрутизатору, который используется в качестве шлюза по умолчанию;
- время прохождения сигнала в прямом и обратном направлении было малым.

Задача 4: Просмотр привязок IP-адресов к MAC-адресам по протоколу ARP

Команда **arp –a** ОС Windows позволяет вывести привязку логического IP-адреса к физическому MAC-адресу.

Процедура упражнения

Выполните следующие действия:

Действие 1 В командной строке введите команду **arp –a**. Для вывода таблицы ARP необходимо использовать параметр **–a**.

```
C:\Documents and Settings>arp -a

Interface: 192.168.1.125 --- 0x2
   Internet Address   Physical Address    Type
   192.168.1.1        00-00-0c-07-ac-04   dynamic
```

Действие 2 Вывод должен совпадать с выводом, полученным во время действия 1. Если значения не отображаются, возможно, превышено время ожидания записи таблицы ARP и необходимо повторить действие 1 предыдущей задачи.

Действие 3 Введите в командной строке команду **exit**, чтобы закрыть окно командной строки.

Проверка упражнения

Задание считается выполненным, если достигнут следующий результат:

- вам удалось вывести сведения о привязке IP-адреса к MAC-адресу.

Лабораторная работа 1-2: Обзор трехстороннего квитирования TCP

Выполните упражнение этой лабораторной работы, чтобы применить на практике знания, полученные в соответствующем модуле.

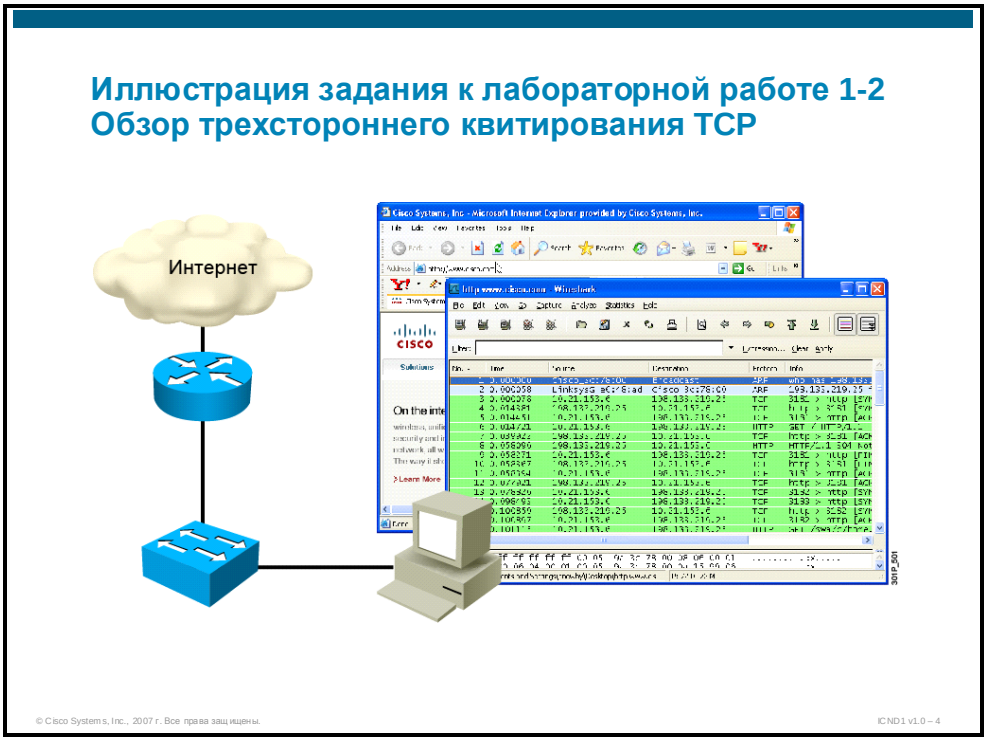
Задачи упражнения

В этом упражнении вы воспользуетесь ПО анализатор пакетов для просмотра сведений о начальном трехстороннем квитировании TCP. После выполнения этого упражнения вы будете способны сделать следующее:

- запустить ПО анализатора пакетов для журналирования потока пакетов на нужном Ethernet-интерфейсе.
- создать TCP-подключение с помощью обозревателя.
- отследить исходные пакеты потока TCP, в частности пакеты SYN, SYN ACK и пакет ACK.

Иллюстрация задания

На рисунке ниже показано, что вы должны сделать во время данного упражнения.



Необходимые ресурсы

Ниже перечислены ресурсы и устройства, необходимые для выполнения упражнения.

- ПК с доступом в Интернет.
- ПО анализа пакетов Wireshark для Windows.
- Руководство для студентов к занятию 1 модуля 1.

Список команд

В таблице приводится описание приложений, используемых в упражнении.

Приложения ПК

Приложение Windows	Описание
`Internet Explorer`	Обозреватель, предоставляющий доступ к медиаконтенту.
`Wireshark`	ПО анализатор пакетов.

Примечание. Установка и использование ПО анализатора пакетов может рассматриваться как нарушение политики безопасности организации, приводящее к серьезным юридическим и финансовым последствиям. Перед загрузкой, установкой и выполнением такого ПО рекомендуется получить соответствующее разрешение.

Подсказки

Для этого упражнения доступны следующие подсказки.

- Для этой лабораторной работы нет подсказок.

Задача 1: Подготовка ПО анализа пакетов к перехвату потока TCP

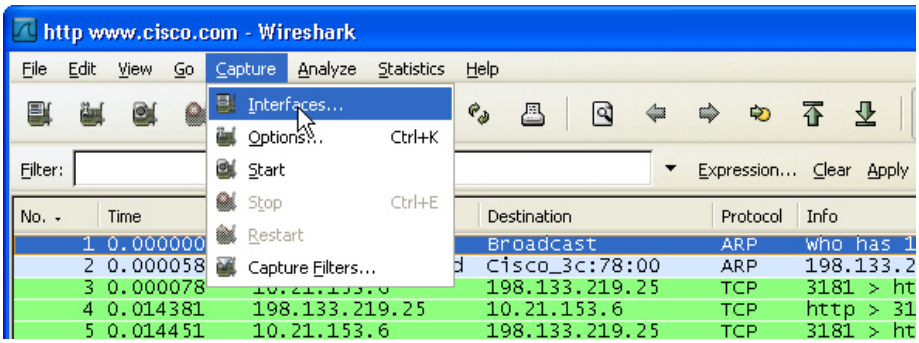
В этой задаче вам следует открыть приложение Wireshark и применить перехват пакетов к активному интерфейсу Ethernet.

Процедура упражнения

Выполните следующие действия:

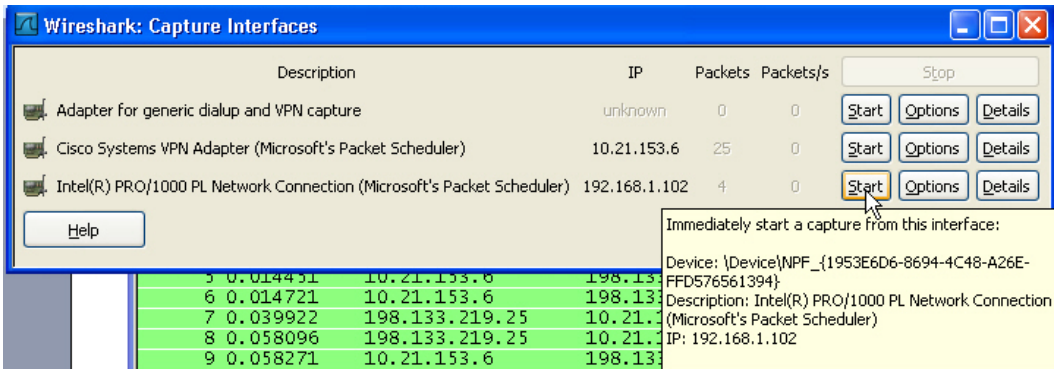
Действие 1 Откройте приложение Wireshark, дважды щелкнув его значок на рабочем столе.

Действие 2 Выберите **Capture (Перехват)**, затем выберите **Interfaces (Интерфейсы)** в раскрывающемся меню.

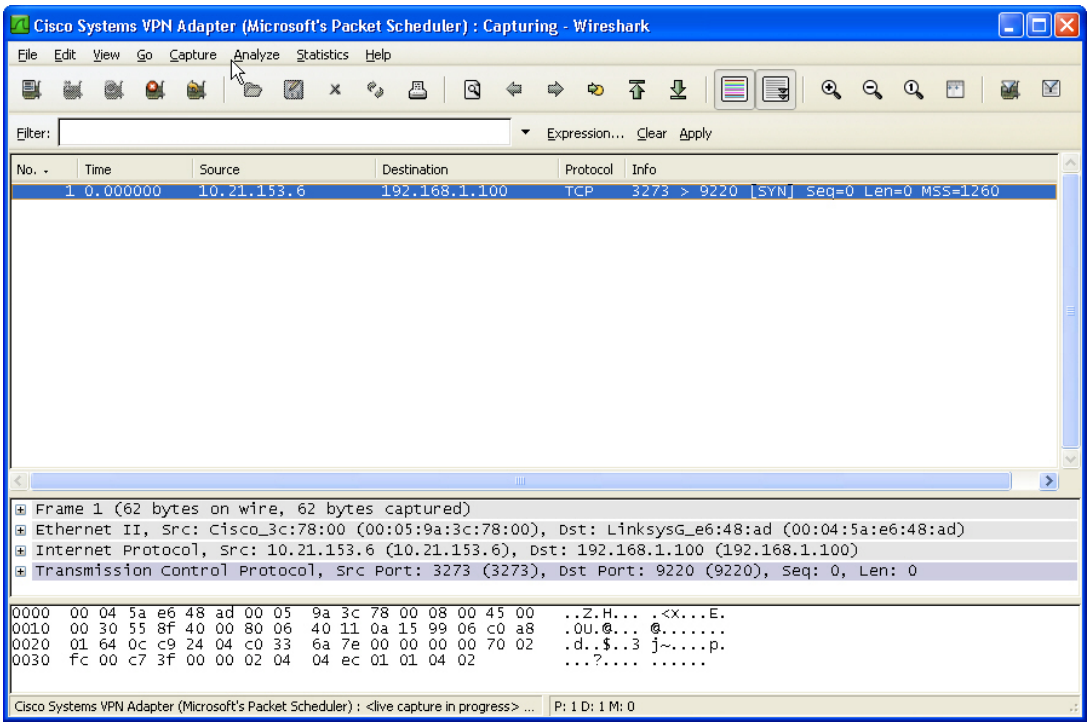


Действие 3 Выберите локальный сетевой адаптер Ethernet. Если вам что-то неясно, обратитесь за помощью к инструктору. Нажмите кнопку «Start» (Пуск) рядом с выбранным интерфейсом. Запишите IP-адрес выбранного Ethernet-адаптера. Это будет IP-адрес источника, который необходимо будет найти при анализе перехваченных пакетов.

Запишите этот IP-адрес здесь: _____



Действие 4 Теперь окна перехвата активны.



Действие 5 После перехвата пакета TCP необходимо подробно проанализировать окна перехвата.

Действие 6 В верхнем окне могут отображаться пакеты. Это зависит от уровня фоновых операций в сети, к которой подключен компьютер.

Проверка упражнения

Задание считается выполненным, если достигнут следующий результат:

- вы открыли окно перехвата пакетов для Ethernet-интерфейса, подключенного к маршрутизатору по умолчанию.

Задача 2: Формирование потока TCP для перехвата

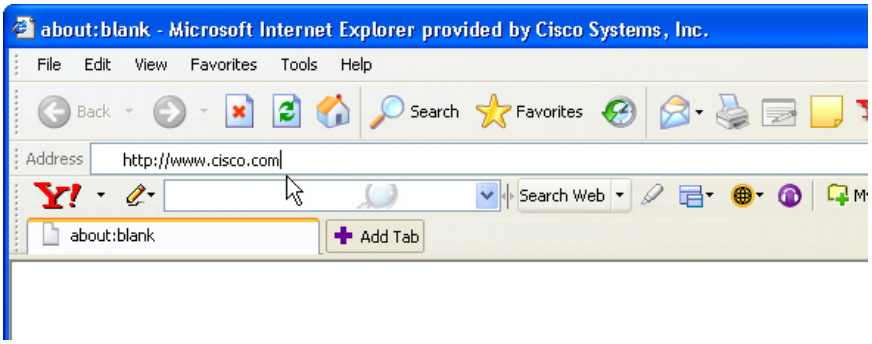
Для подключения к веб-серверу будет использоваться обозреватель (Internet Explorer). На самом деле не важно, какой веб-сервер вы выберете. Для надежности для HTTP-данных, которые применяются для переноса текста и графики веб-страницы, используется транспорт TCP. В качестве альтернативного протокола с негарантированной доставкой можно упомянуть UDP. В данный момент вам следует сосредоточиться на начальном обмене, который выполняется протоколом TCP при установлении соединения.

Процедура упражнения

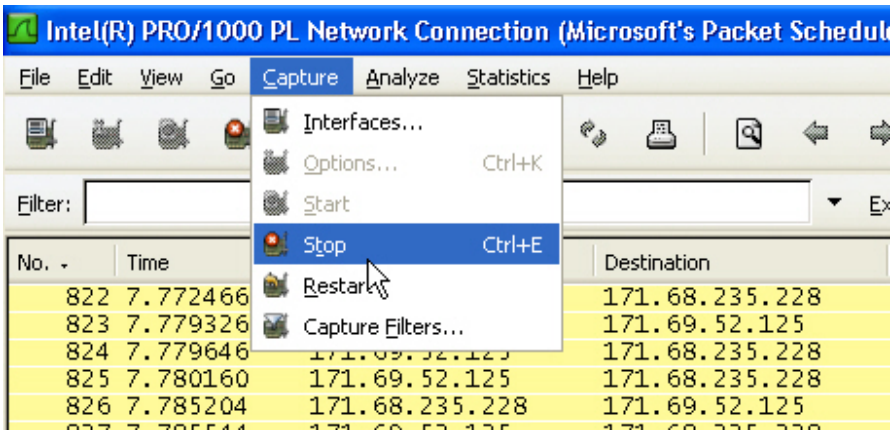
Выполните следующие действия:

Действие 1 На рабочем столе дважды щелкните значок **Internet Explorer** для запуска обозревателя.

Действие 2 Введите имя или адрес получателя. Инструктор может предоставить имя или адрес, отличный от www.cisco.com. В этом случае введите эти данные в соответствующей строке. _____



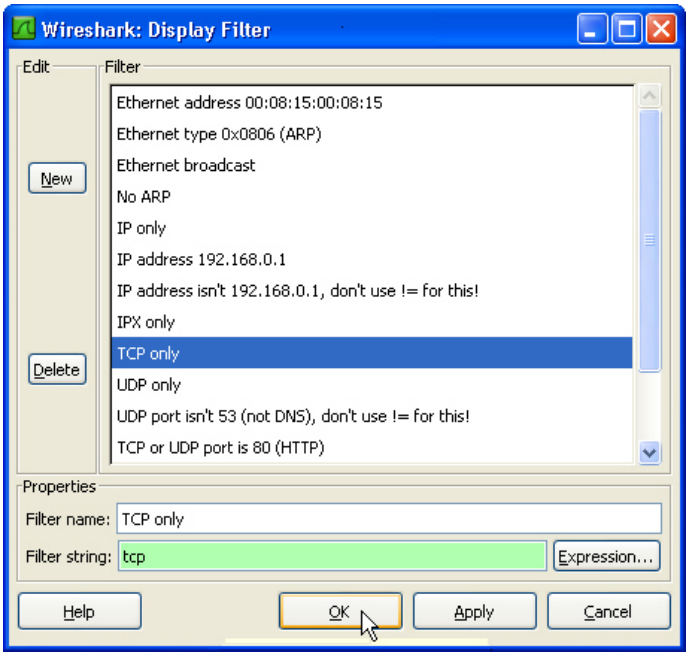
Действие 3 Вернитесь в уже открытое приложение Wireshark и выберите **Capture** > **Stop** в раскрывающемся меню.



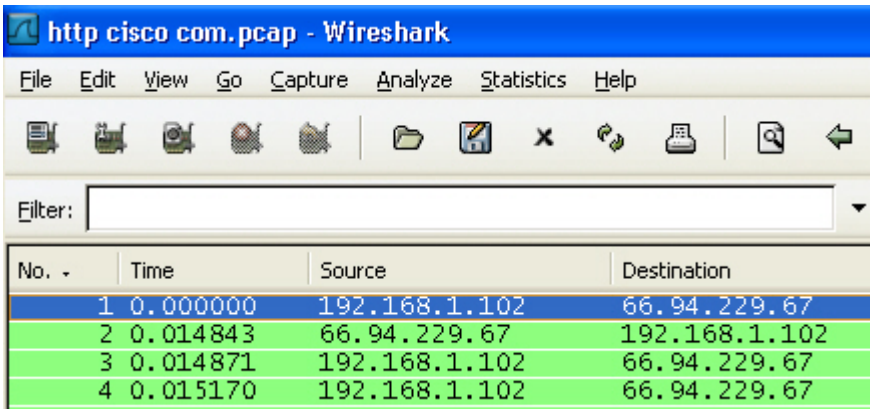
Действие 4 При появлении большого числа TCP-пакетов, не связанных с вашим TCP-соединением, используйте средства фильтрации Wireshark.

Действие 5 Чтобы использовать предварительно настроенный фильтр, перейдите на вкладку **Analyze (Анализ)**. Выберите **Display Filters (Фильтры вывода)**.

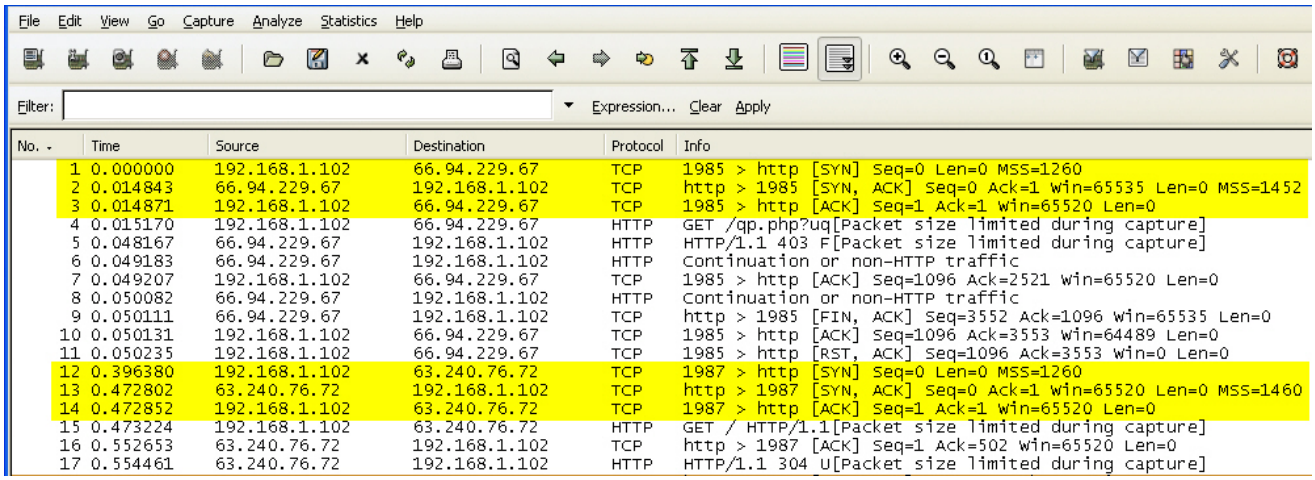
Действие 6 В окне **Wireshark:Display Filter (Фильтр вывода)** выберите **TCP only (Только TCP)** и нажмите кнопку **OK**.



Действие 7 В верхнем окне приложения Wireshark перейдите к первому перехваченному TCP-пакету в первой строке окна с помощью полосы прокрутки. Это должен быть первый пакет в потоке.



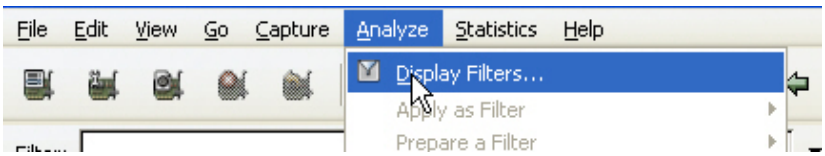
Действие 8 Просмотрите столбец Info для перехваченных пакетов в верхнем окне и найдите три пакета, аналогичные показанным ниже. В качестве примера выделены две группы из трех пакетов.



Действие 9 Запишите номер первого пакета в последовательности, обнаруженной в *вашем* окне перехвата. Достаточно найти одну последовательность пакетов. В приведенном выше примере и пакет 1, и пакет 12 являются начальными пакетами последовательности. В следующей задаче будет подробно рассматриваться содержимое этих пакетов.

Запишите номер последовательности первого пакета TCP в строке ниже:

_____



Действие 10 При необходимости вернитесь к действию 4 этой задачи.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- вы определили, что перехвачена последовательность пакетов, описанная в действии 8;
- вы записали первый пакет в последовательности, который вы будете подробно анализировать позднее.

Задача 3: Изучение последовательности инициализации TCP

Для просмотра параметров TCP, обмен которыми выполняется в процессе начальной загрузки и часто называется «трехсторонним квитированием», будет использоваться окно «Packet Details» (Свойства пакета) приложения Wireshark.

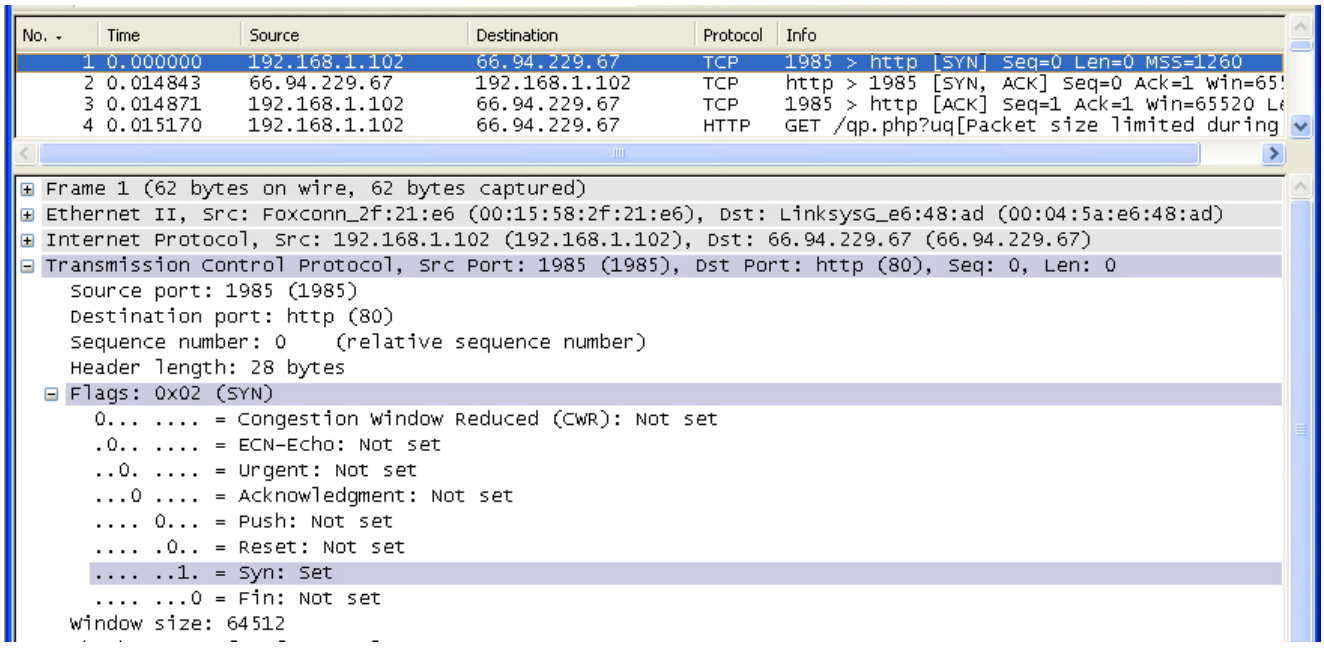
Процедура упражнения

Выполните следующие действия:

Действие 1 В верхнем окне приложения Wireshark щелкните (в любом месте) строку первого пакета, идентифицированного во время предыдущей задачи. Строка будет выделена, и в двух окнах ниже появится декодированная информация пакета.

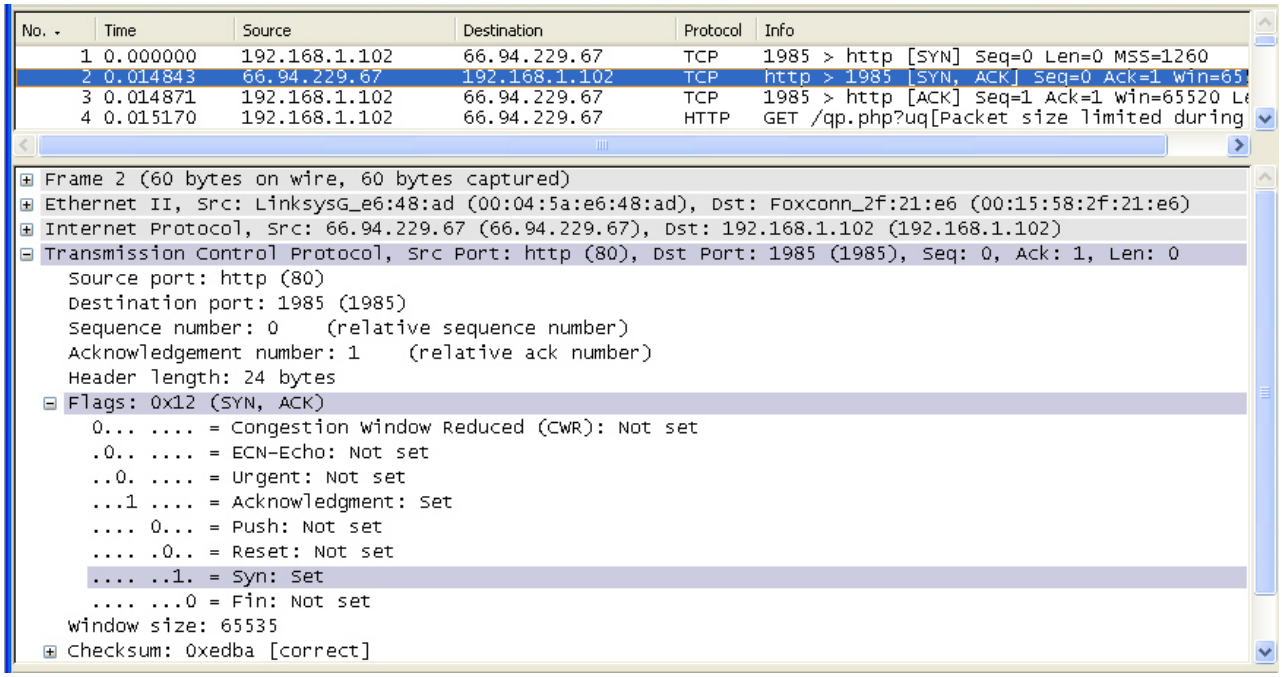
Действие 2 В этом примере размер окон Wireshark был скорректирован для компактного представления информации. Среднее окно содержит подробную расшифровку пакета.

Действие 3 Щелкните значок «+» в левой части окна, чтобы развернуть окно сведений TCP. С помощью значка «–» это представление можно свернуть.



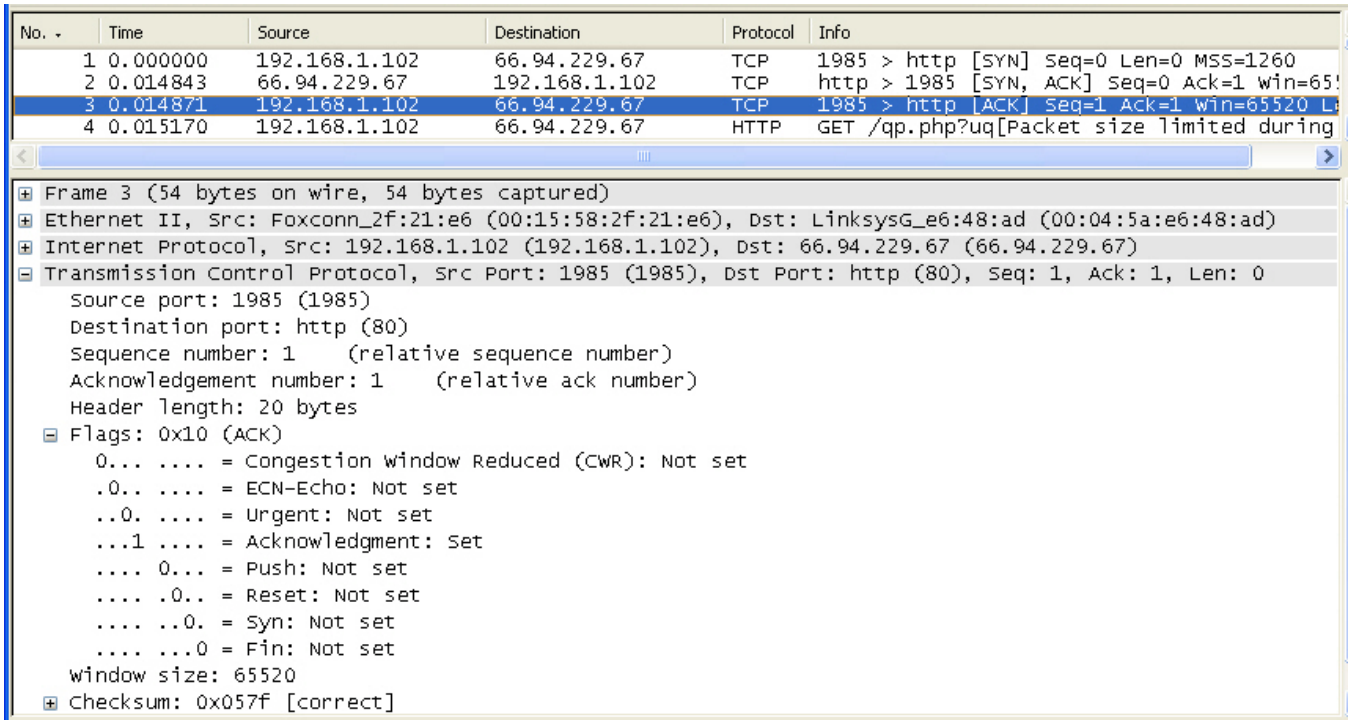
Действие 4 Обратите внимание, что в этом примере номер последовательности (прямой) установлен на 0, а в поле «Flags» (Флаги) для бита SYN задано значение 1 (установлен).

Действие 5 Щелкните следующий пакет в последовательности (верхнее окно). После этого подробная информация изменится в соответствии с новыми значениями.



Действие 6 Обратите внимание, что номер последовательности пакета ответа (обратный) установлен в 0 и появился номер подтверждения, для которого установлено значение 1. Кроме того, в поле «Flags» для бита подтверждения (acknowledgment) и бита SYN задано значение 1 (установлен).

Действие 7 Щелкните следующий пакет в последовательности (верхнее окно). После этого подробная информация изменится в соответствии с новыми значениями.



Действие 8 Обратите внимание, что в третьем и последнем пакете обмена для (прямого) номера последовательности установлено значение 1, для номера подтверждения – значение 1, и в поле Flags только бит подтверждения имеет значение 1 (установлен). В этот момент соединение TCP считается «установленным», так как на обеих сторонах синхронизированы номера последовательности, номера подтверждений и другие параметры, которые не рассматриваются в этом курсе.

Действие 9 Закройте приложение Wireshark и все другие открытые окна.

Проверка упражнения

Задание считается выполненным, если достигнут следующий результат:

- вы выбрали и декодировали три перехваченных пакета, их параметры соответствуют параметрам, которые рассматриваются в примерах для этой задачи.

Лабораторная работа 1-3: Анализ расширенных данных сети ПК

Выполните упражнение этой лабораторной работы, чтобы применить на практике знания, полученные в соответствующем модуле.

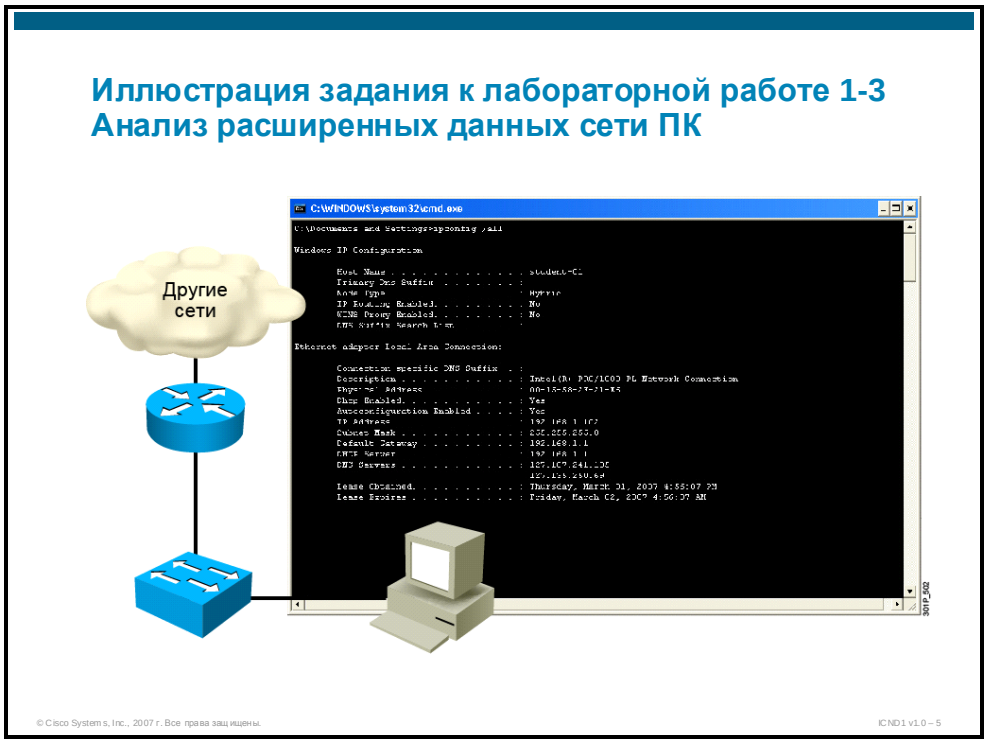
Задачи упражнения

В этом упражнении для сбора информации о сети будут использоваться инструментальные средства ПК. После выполнения этого упражнения вы будете способны сделать следующее:

- определить IP-адреса DNS-серверов, доступных вашему ПК, с помощью команды **ipconfig /all** ОС Windows;
- проверить соединение с DNS-серверами с помощью команды **ping** ОС Windows для IP-адреса одного из DNS-серверов, определенных во время задачи 1;
- получить IP-адреса промежуточных маршрутизаторов на пути к DNS-серверу, проверенному во время задачи 2, с помощью команды **tracert /d** ОС Windows.

Иллюстрация задания

На рисунке ниже показано, что вы должны сделать во время данного упражнения.



Необходимые ресурсы

Ниже перечислены ресурсы и устройства, необходимые для выполнения упражнения.

- ПК, подключенный к исправной сети с доступом в Интернет.

Список команд

В таблице приводится описание команд, используемых в упражнении.

Команды Windows

Команда	Описание
ipconfig /all	Эта команда выводит все текущие сведения об IP-сети.
ping	ping (-t)
tracert /d <ip-адрес>	Отображает IP-адрес маршрутизатора на каждом переходе, через который проходит пакет на пути к IP-адресу назначения.

Подсказки

Для этого упражнения доступны следующие подсказки.

- Для этой лабораторной работы нет подсказок.

Задача 1: Получение полной информации о текущем IP-адресе

Чтобы получить полную информацию о текущем IP-адресе вашего ПК, используйте команду **ipconfig /all** ОС Windows. Чтобы получить доступ к командам Windows, откройте окно командной строки.

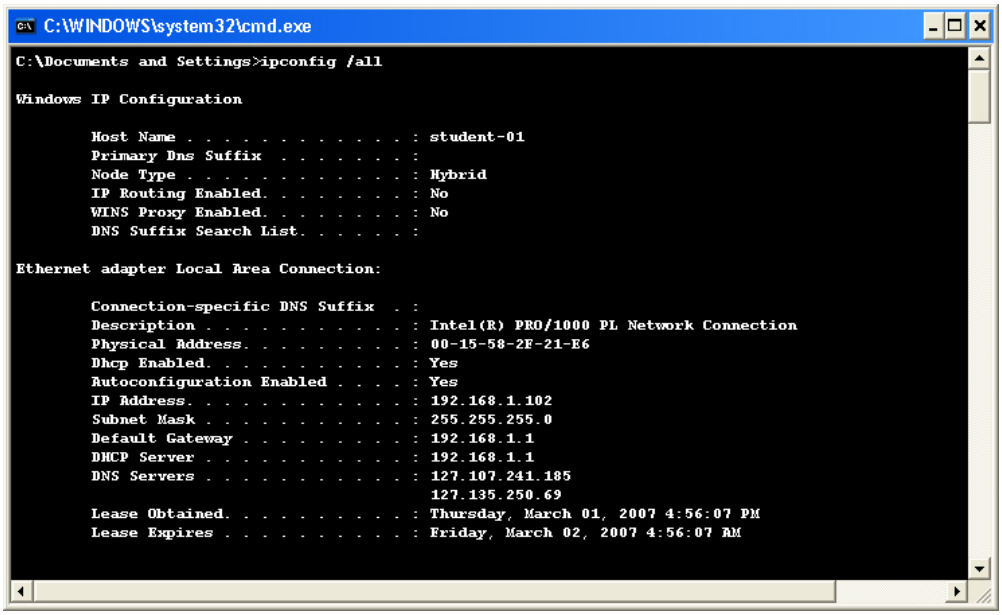
Процедура упражнения

Выполните следующие действия:

Действие 1 На рабочем столе Windows нажмите кнопку **Пуск**.

Действие 2 Выберите **Выполнить** и введите **cmd** в диалоговом окне «Выполнить». Нажмите OK для продолжения.

Действие 3 В командной строке введите **ipconfig /all.** При необходимости добавьте параметр **/all**, чтобы получить полный вывод.



Действие 4 В выводе появится дополнительная полезная информация.

Действие 5 Запишите IP-адрес первого DNS-сервера в выводе команды, полученном во время предыдущего действия, в строке ниже.

_____

Проверка упражнения

Задание считается выполненным, если достигнут следующий результат:

- Из выходных данных команды **ipconfig /all,** выполненной на ПК, получен IP–адрес DNS-сервера.

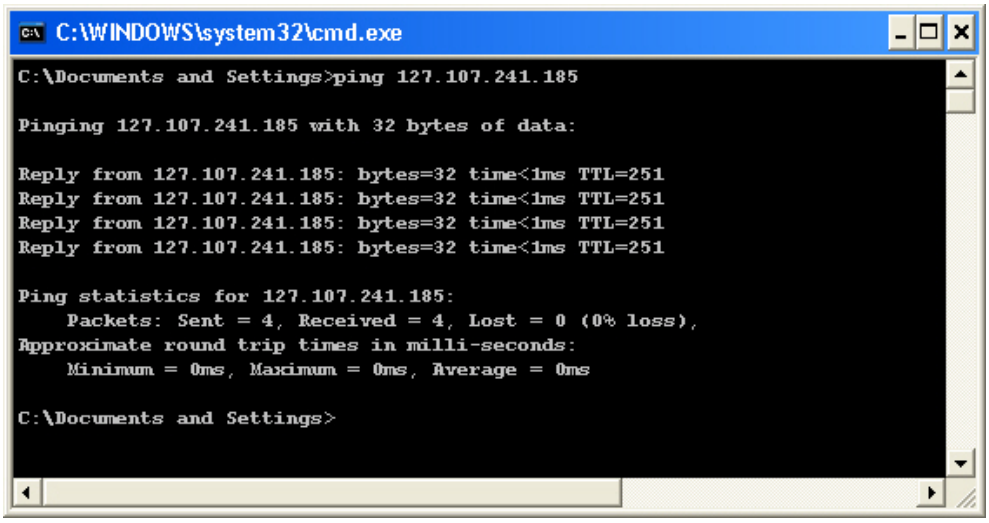
Задача 2: Проверка соединения с DNS-сервером

В этой задаче для проверки соединения с DNS-сервером, записанным во время предыдущей задачи, будет использоваться команда **ping**.

Процедура упражнения

Выполните следующие действия:

Действие 1 В окне командной строки введите **ping** *<IP-адрес DNS-сервера>*. Вывод команды должен выглядеть следующим образом (в этом примере используется вымышленный IP-адрес).



Действие 2 Успешная обработка эхо-запроса означает, что пакеты запроса получены на удаленном сервере, и пакеты ответа успешно доставлены на ПК.

Действие 3 При неудачной обработке эхо-запроса необходим анализ проблемы. Если эхо-запрос обработан неудачно, следующим шагом будет поиск проблемы в сети.

Проверка упражнения

Задание считается выполненным, если достигнут следующий результат:

- вам удалось проверить соединение с IP-адресом DNS-сервера, записанным во время задачи 1, помощью команды **ping** ОС Windows.

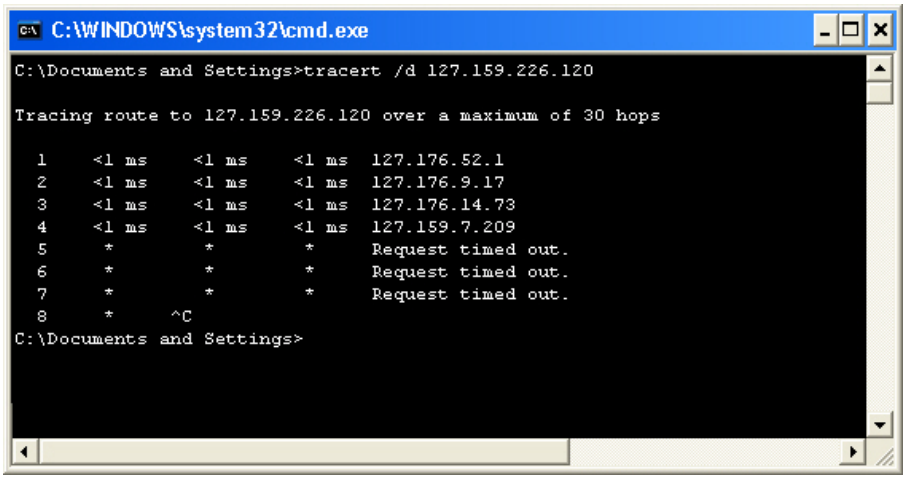
Задача 3: Трассировка соединения с DNS-сервером

В этой задаче для трассировки маршрута к DNS-серверу, записанному во время предыдущей задачи, будет использоваться команда **tracert /d**. Параметр **/d** позволяет предотвратить запросы dns-имен промежуточных маршрутизаторов пути по IP-адресам и отображение этих имен в результатах. В этом сценарии служба DNS не работает, поэтому такие запросы будут пустой тратой времени. Используйте команду **tracert** без параметра **/d**, если необходимо узнать, как будет выглядеть вывод, если служба DNS может разрешить некоторые или все IP-адреса.

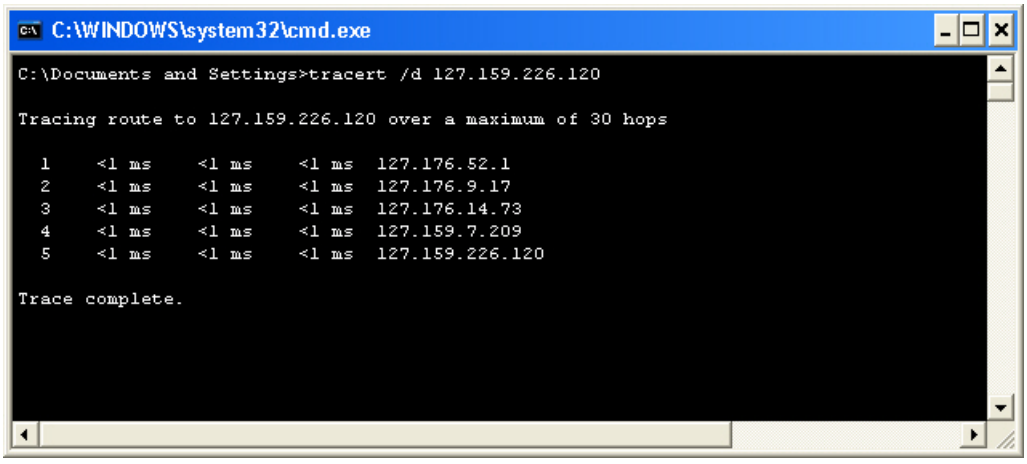
Процедура упражнения

Выполните следующие действия:

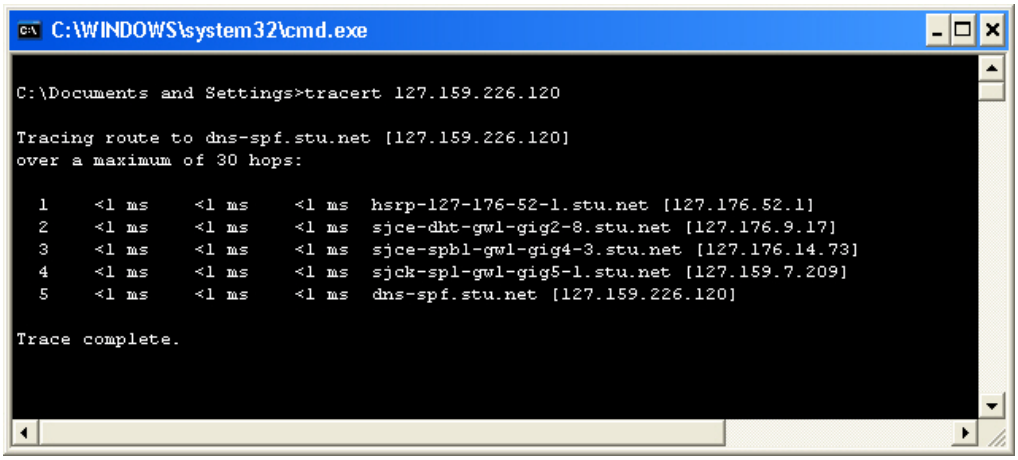
Действие 1 Ниже приводится пример неудачной трассировки маршрута к DNS-серверу. Эта последовательность может продолжаться, пока не будут проверены 30 переходов. В следующем примере вывода показано, что для прекращения команды до достижения числа переходов по умолчанию (30) был использован управляющий символ ^C <ctrl-C>.



Действие 2 В окне командной строки введите **tracert /d** *<IP-адрес DNS-сервера>*. Вывод команды должен выглядеть следующим образом (в этом примере используется вымышленный IP-адрес).



Действие 3 После успешного завершения проверки маршрута к DNS-серверу используйте эту команду без параметра **/d**, чтобы увидеть вывод команды, с символьными именами. Вывод команды должен выглядеть следующим образом (в этом примере используется вымышленный IP-адрес).



Действие 4 Закройте окно командной строки, нажав кнопку **X** в верхнем правом углу.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- вы запретили поиск DNS-сервера при трассировке пути к адресу назначения с помощью команды **tracert /d**, выполненной на ПК;
- с помощью команды **tracert** без параметра **/d**, выполненной на ПК, были выведены символьные имена, связанные с конкретными IP-адресами обнаруженных устройств на пути к адресу назначения.

Лабораторная работа 2-1: Подключение к удаленному лабораторному оборудованию

Выполните это упражнение, чтобы проверить соединение к вашему комплекту оборудования (pod) и применить на практике методы подключения к терминальному серверу и подключения с помощью VPN-клиента.

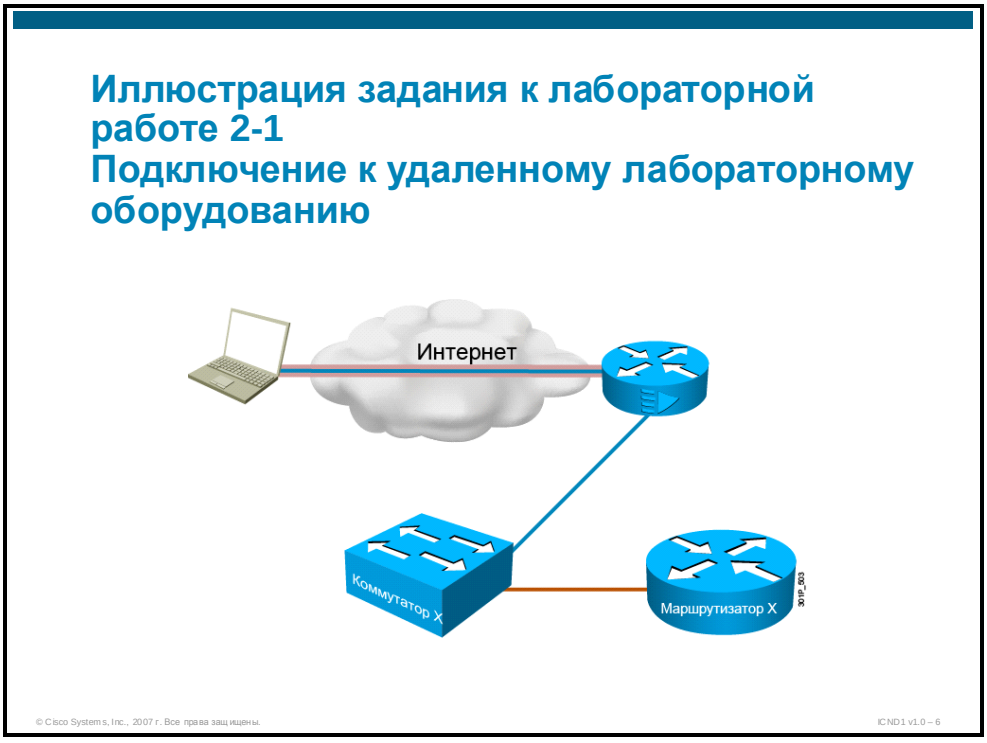
Задачи упражнения

В этом упражнении вы начнете подготовку к следующим лабораторным работам – протестируете подключение к оборудованию вашей рабочей группы, которое будет использоваться в упражнениях остальных лабораторных работ этого курса. Кроме того, вы попрактикуетесь в работе с этим подключением. После выполнения этого упражнения вы будете способны сделать следующее:

- подключиться к оборудованию назначенной вам рабочей группы, используя терминальный сервер для настройки маршрутизаторов и коммутаторов по консольным портам;
- подключиться к оборудованию назначенной рабочей группы, используя программный VPN-клиент, чтобы подключить ПК к интерфейсу коммутатора рабочей группы; это позволит настроить маршрутизатор рабочей группы с помощью ПО Cisco Router и Security Device Manager (SDM).

Иллюстрация задания

На рисунках ниже показано, что вы должны сделать во время данного упражнения.



Лабораторное оборудование находится на удаленной площадке. Для получения доступа к этому оборудованию будут использоваться два различных метода.

Первый метод основан на SSH-подключении. Оно обеспечивает доступ к тевминальному серверу (называемому также сервером консолей). Терминальный сервер имеет последовательные подключение к консольным портам маршрутизаторов и коммутаторов Cisco, используемых в лабораторных работах. В первом методе пакеты отправляются через Интернет. В этих пакетах данные отдельно защищены шифрованием.

Во втором методе используется VPN-подключение. Оно обеспечивает доступ через VPN-маршрутизатор в сеть, к которой подключен коммутатор рабочей группы. Во этом методе пакеты отправляются через Интернет с помощью зашифрованного туннеля.

Необходимые ресурсы

Ниже перечислены ресурсы и устройства, необходимые для выполнения упражнения.

- Лабораторная топология, настроенная для этого курса.
- Комплект оборудования студента, состоящий из одного коммутатора Cisco Catalyst 2960 и одного маршрутизатора Cisco 2811 (или эквивалентных по функциональности устройств Cisco).

В аудитории доступны следующие справочные материалы:

- руководство по лабораторным работам;
- ПК студента или рабочая станция с доступом к устройствам рабочего комплекта оборудования.

Список команд

В таблице приводится описание команды и приложений, используемых в упражнении.

Приложение ПК

Приложения Windows	Описание
`Putty SSH Client`	Приложение эмуляции терминала, поддерживающее протокол SSH
`Cisco VPN Client`	Программный VPN-клиент
Команда Windows	
`ipconfig /all`	Эта команда выводит все текущие сведения об IP-сети

Подсказки

Для упражнений этой лабораторной работы доступны следующие подсказки.

- Заполните эту таблицу данными о подключении и сети класса (предоставляются инструктором).

Таблица 1. Сведения о сети и подключении

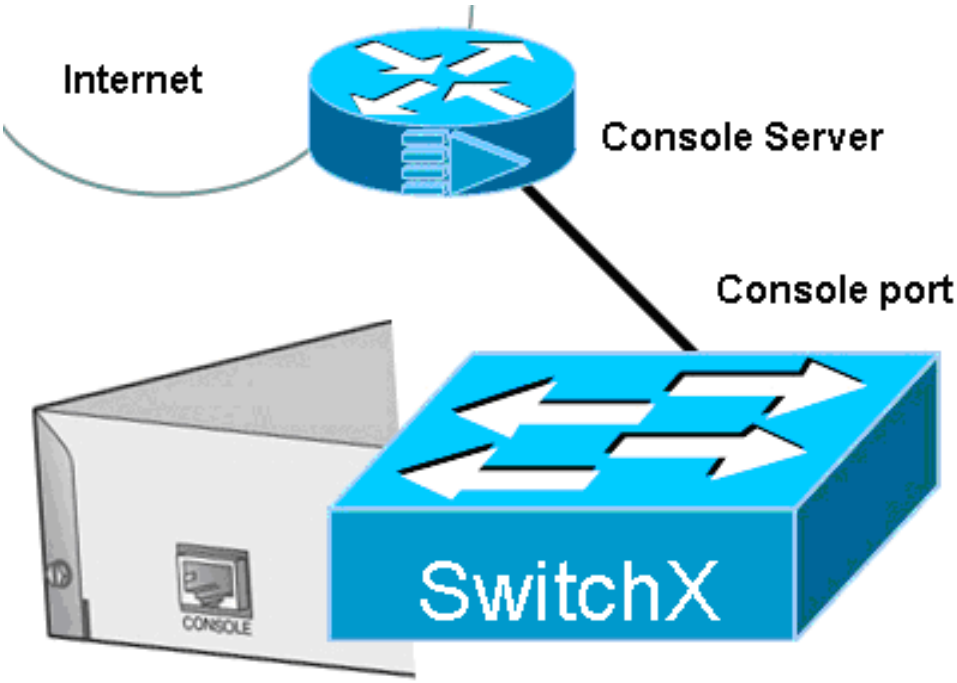
Сведения	Значение, назначенное инструктором
Назначенная рабочая группа (буква)	
IP-адрес *терминального сервера*	
Имя пользователя и пароль для SSH	
IP-адрес *VPN-RTR (если он отличается от адреса выше)*	
Имя записи подключения VPN-клиента	
Имя пользователя и пароль для VPN (если отличаются от SSH)	
Приложение эмуляции терминала SSH	

Таблица 2. Данные IP-адреса TFTP-сервера

Рабочая группа	IP-адрес TFTP-сервера	Рабочая группа	IP-адрес TFTP-сервера
A	**10.2.2.1**	**E**	**10.6.6.1**
B	**10.3.3.1**	**F**	**10.7.7.1**
C	**10.4.4.1**	**G**	**10.8.8.1**
D	**10.5.5.1**	**H**	**10.9.9.1**

Задача 1: Подключение к удаленному серверу консоли

В этой задаче вам следует использовать приложение эмуляции терминала с поддержкой протокола SSH. Этот эмулятор терминала позволяет настраивать и контролировать удаленные сетевые устройства Cisco при подключении к терминальному серверу через «консольный» порт.

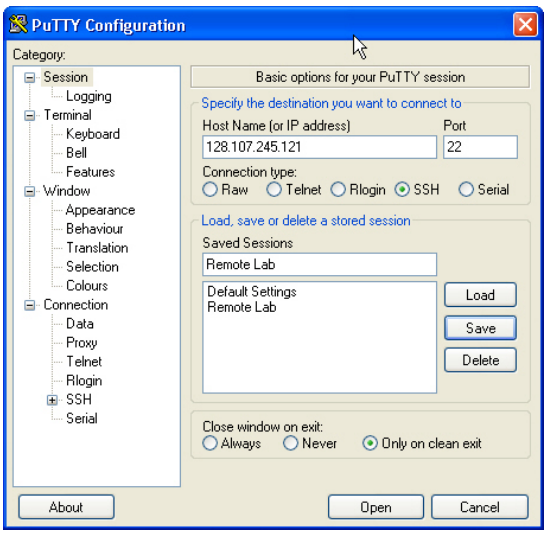


Процедура упражнения

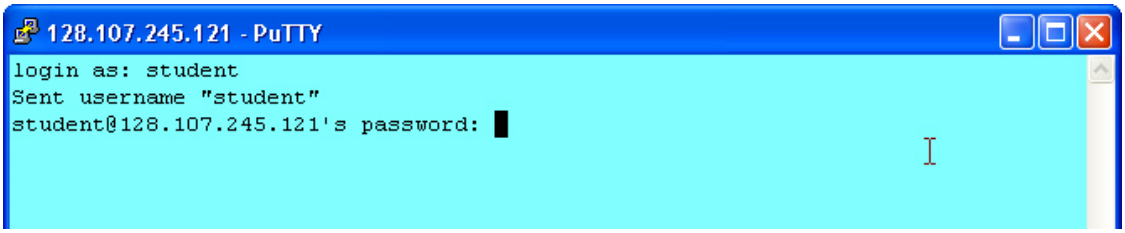
Выполните следующие действия:

Действие 1 На рабочем столе дважды щелкните значок **эмулятора терминала**. В этом примере используется ПО PuTTY.

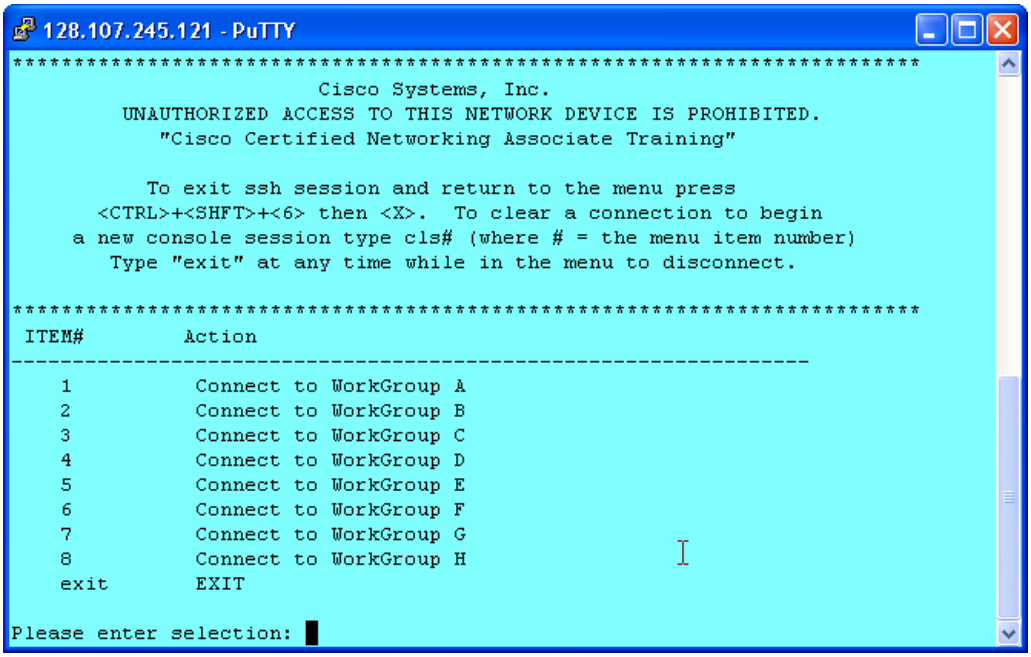
Действие 2 Убедитесь, что установлен переключатель **SSH**. Введите IP-адрес терминального сервера в поле **Host Name (Имя хоста)** и нажмите кнопку **Open (Открыть)**.



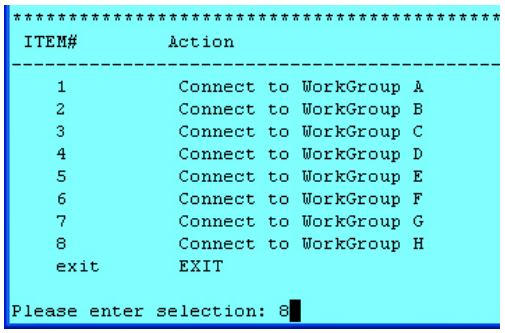
Действие 3 Введите имя пользователя и пароль для сеанса SSH в соответствующие строки запросов, используя значения из таблицы 1. При отсутствии ключа хоста в кэше может отображаться предупреждение безопасности PuTTY. Для продолжения выберите **Yes (Да)**.



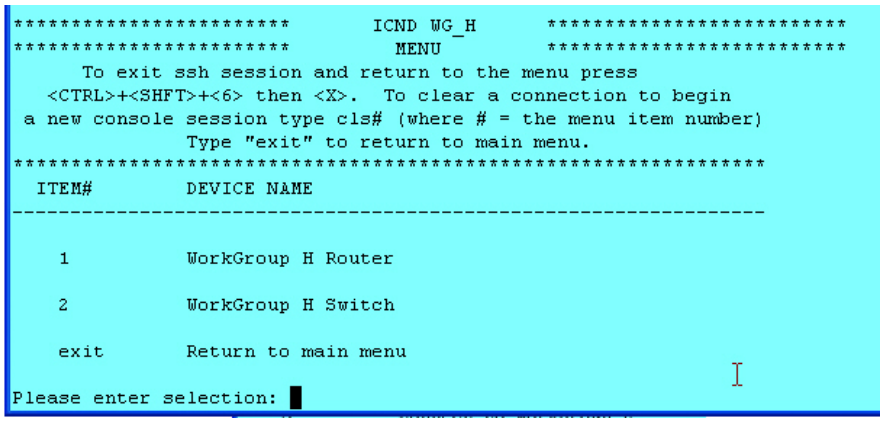
Действие 4 Появится баннерное сообщение и таблица с номерами элементов, используемых для подключения к рабочим группам. Ознакомьтесь с информацией последовательности действий, используемой для возвращения в меню из режима подключения к маршрутизатору или коммутатору. Для этого нажмите одновременно следующие клавиши: **Ctrl-Shift-6**. Затем отпустите их и нажмите **x** (в нижнем регистре).



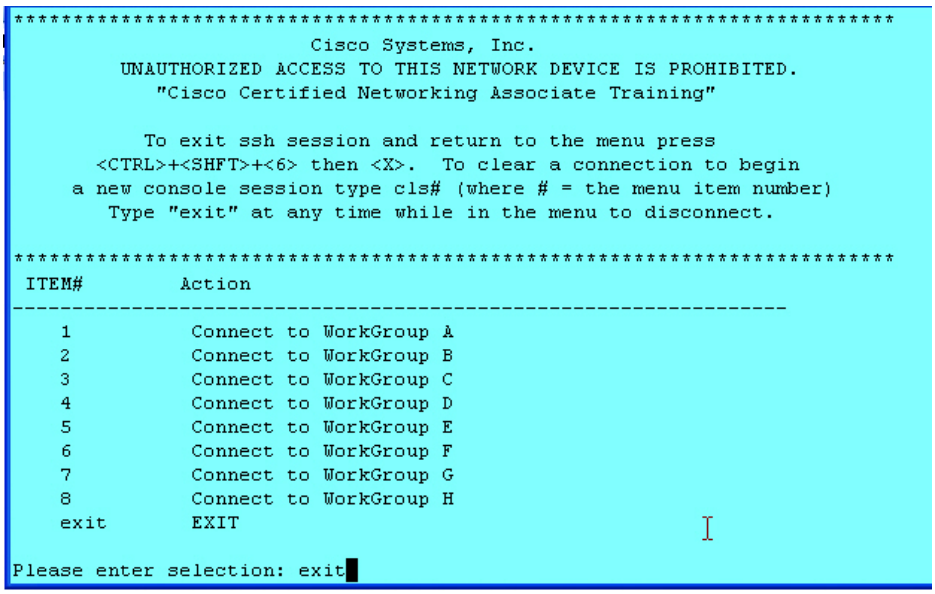
Действие 5 Выберите рабочую группу, указав соответствующий номер элемента.



Действие 6 Вы перешли в меню рабочей группы Можно выбрать вариант **1** для подключения к маршрутизатору, **2** для подключения к коммутатору или **exit** для возвращения к предыдущему меню. Введите **exit** для возвращения к предыдущему меню. Введите **exit**, затем нажмите клавишу **Enter**.



Действие 7 Теперь введите **exit** и нажмите клавишу **Enter** для завершения сеанса SSH.



Действие 8 В зависимости от используемого эмулятора терминала это окно может закрываться, очищаться или оставаться в неизменном виде. Однако сеанс завершен и все нажатия клавиш будут игнорироваться.

Действие 9 Закройте приложение эмуляции терминала, если оно не закрылось автоматически.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- вы получили доступ к удаленному терминальному серверу, используя данные из таблицы 1;
- вы получили доступ в меню рабочей группы назначенного комплекта оборудования;
- вы вернулись в главное меню, завершили сеанс терминала и закрыли приложение.

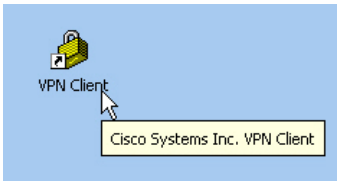
Задача 2: Подключение к удаленному VPN-маршрутизатору

В этой задаче вы должны использовать клиентское приложение Cisco VPN Client для доступа к удаленной лаборатории. Подключившись, вы сможете наблюдать изменения локальных IP-адресов ПК и обсуждать изменения в режиме пересылки пакетов.

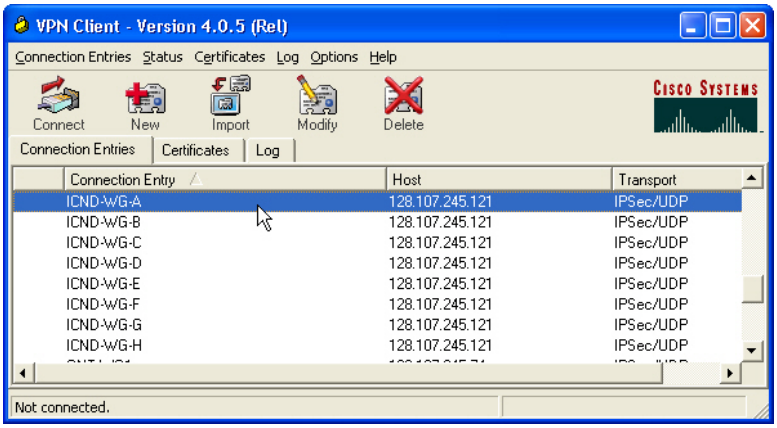
Процедура упражнения

Выполните следующие действия:

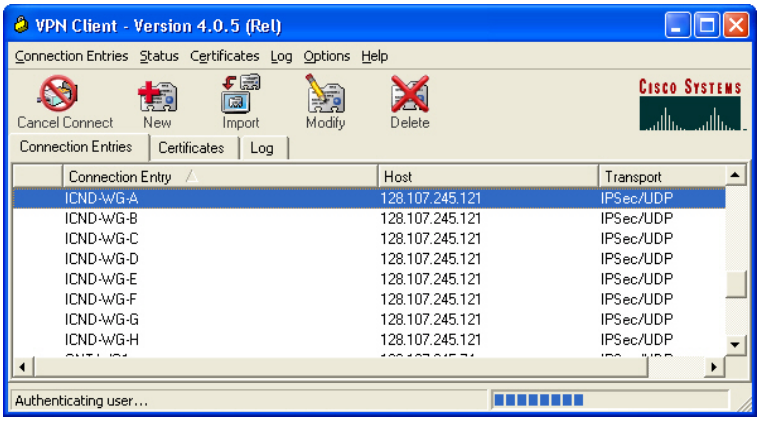
Действие 1 На рабочем столе откройте ПО Cisco VPN Client, щелкнув значок **VPN Client**.



Действие 2 Выберите запись подключения назначенной рабочей группы.



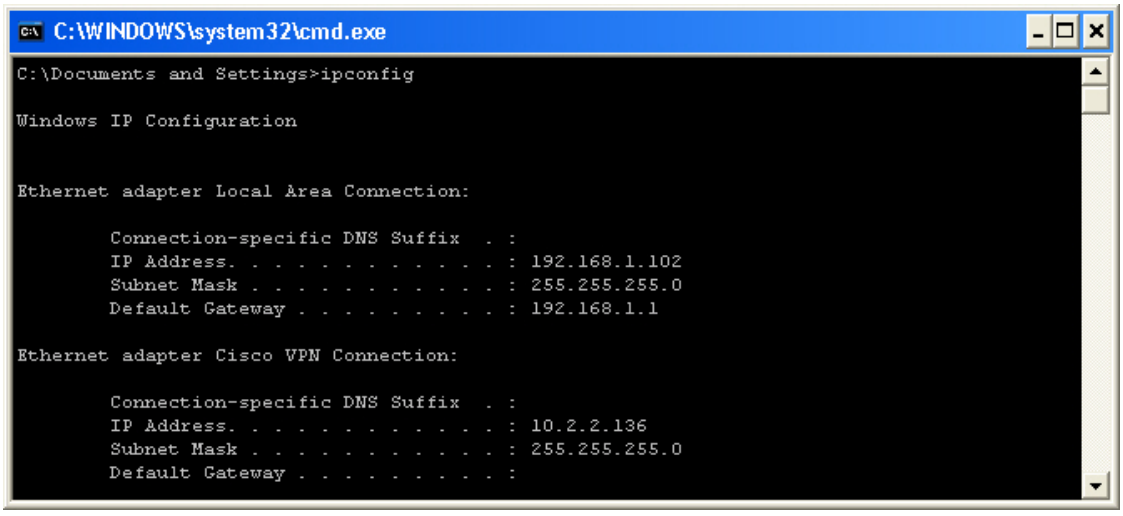
Действие 3 Щелкните значок **Connect (Подключение)** в верхнем левом углу окна приложения.



Действие 4 Значок «Connect» изменится, и откроется окно аутентификации пользователя.

Действие 5 Введите имя пользователя и пароль VPN, записанные в таблице 1, затем нажмите клавишу **Enter**. После короткой паузы окна VPN закроются. Небольшой значок открытого замка на панели задач в правом нижнем углу экрана изменится на закрытый замок. Если это окно НЕ закроется, сверните его вручную.

Действие 6 Чтобы просмотреть изменения IP-адресов ПК, необходимо открыть окно командной строки и ввести команду **IPCONFIG**.



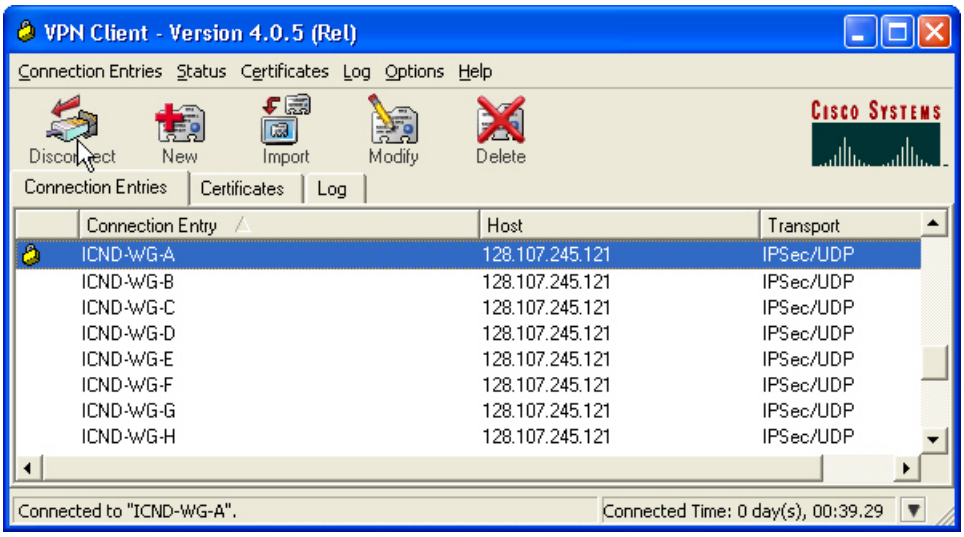
Действие 7 В выводе команды появится IP-адрес и маска второго адаптера Ethernet. Ваш вывод может отличаться, однако этот адрес и маска зависят от адресации рабочих групп, используемой в будущих лабораторных работах. Для адаптера VPN НЕ задается шлюз по умолчанию, поскольку режим пересылки пакетов был изменен на использование туннеля для сетей, настроенных на VPN-маршрутизаторе. Это будет происходить автоматически, и в случае несоответствия данные будут отправляться на настроенный шлюз по умолчанию, связанный с другим Ethernet-адаптером.

Действие 8 Эхо-запросы, отправленные по адресу 10.*x*.*x*.1, где *x* = 2 для рабочей группы A, *x* =3 для рабочей группы B и т. д. (*x* = 9 для рабочей группы H), должны быть обработаны успешно. Если эхо-запросы не обрабатываются, обратитесь за помощью к инструктору. Вывод должен быть аналогичен примеру ниже.

```
C:\Documents and Settings>ping 10.10.10.1

Pinging 10.10.10.1 with 32 bytes of data:

Reply from 10.10.10.1: bytes=32 time=9ms TTL=127
Reply from 10.10.10.1: bytes=32 time=8ms TTL=127
Reply from 10.10.10.1: bytes=32 time=9ms TTL=127
Reply from 10.10.10.1: bytes=32 time=8ms TTL=127

Ping statistics for 10.10.10.1:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 8ms, Maximum = 9ms, Average = 8ms
```

Действие 9 В следующих лабораторных работах для подключения обозревателя к маршрутизатору рабочей группы будет использоваться туннель VPN.

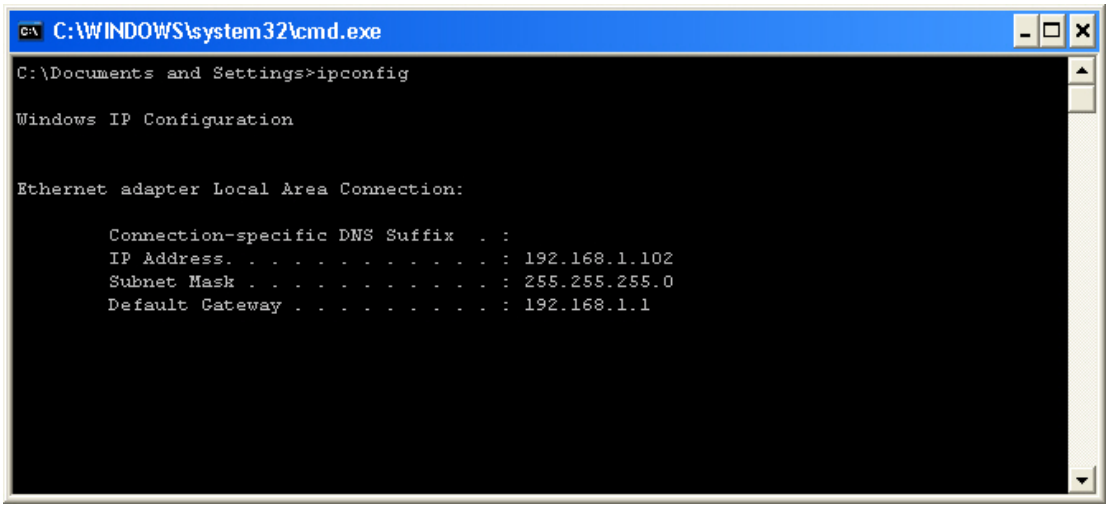
Действие 10 Чтобы завершить VPN-подключение, дважды щелкните значок **замка** на панели задач, чтобы открыть окно приложения VPN. Кроме того, можно щелкнуть правой кнопкой мыши значок замка и выбрать **Disconnect (Отключение)**.



Действие 11 Щелкните значок **Disconnect** в правом верхнем углу окна приложения VPN. В результате туннельное соединение будет закрыто и изменения IP-адресов ПК будут отменены.

Действие 12 Закройте окно приложения VPN.

Действие 13 Введите команду **IPCONFIG** в окне командной строки, чтобы убедиться, что ПК вернулся к исходному сетевому IP-адресу.



Действие 14 После проверки удаления данных подключения закройте все оставшиеся приложения Windows.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- вы получили доступ к сети удаленной лаборатории с помощью VPN-клиента и данных из таблицы 1;
- вы успешно проверили доступ к оборудованию с помощью команды **ping** и обозревателя.

Лабораторная работа 2-2: Запуск коммутатора и его начальная настройка

Выполните упражнение этой лабораторной работы, чтобы применить на практике знания, полученные в соответствующем модуле.

Задачи упражнения

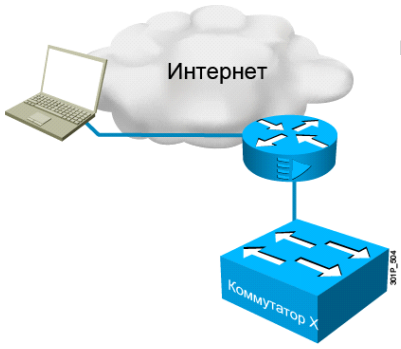
В этом упражнении вам необходимо подключиться к коммутатору рабочей группы и выполнить начальную настройку устройства. После выполнения этого упражнения вы будете способны сделать следующее:

- перезапустить коммутатор и проверить сообщения начального запуска;
- выполнить начальную настройку коммутатора Cisco Catalyst.

Иллюстрация задания

На рисунке ниже показано, что вы должны сделать во время данного упражнения.

Иллюстрация к лабораторной работе 2-2
Запуск коммутатора и его начальная настройка



Имя хоста рабочей группы	IP-адрес коммутатора	Маска подсети
SwitchA	10.2.2.11	255.255.255.0
SwitchB	10.3.3.11	255.255.255.0
SwitchC	10.4.4.11	255.255.255.0
SwitchD	10.5.5.11	255.255.255.0
SwitchE	10.6.6.11	255.255.255.0
SwitchF	10.7.7.11	255.255.255.0
SwitchG	10.8.8.11	255.255.255.0
SwitchH	10.9.9.11	255.255.255.0

Необходимые ресурсы

Ниже перечислены ресурсы и устройства, необходимые для выполнения упражнения.

- ПК, подключенный к удаленной лаборатории.
- Приложение для эмуляции терминала с поддержкой SSH.
- Информация о назначенном комплекте оборудования, полученная в лабораторной работе 2-1.

Список команд

В таблице приводится описание команд, используемых в упражнении.

Команды коммутатора Cisco IOS

Команда	Описание
configure terminal	Активирует режим конфигурации с терминала.
copy running-config *место назначения*	Копирует файл текущей конфигурации коммутатора в другое место назначения. Обычно это загрузочная конфигурация.
enable	Активирует привилегированный режим EXEC. В привилегированном режиме EXEC доступно большее количество команд. Эта команда требует ввода пароля разрешения доступа (enable password), если он настроен.
enable password *пароль*	Enable password используется для защиты доступа к привилегированному режиму (enable). Однако этот пароль хранится в виде нешифрованного текста в конфигурации.
enable secret *секретный_пароль*	Зашифрованный пароль используется для защиты доступа к привилегированному режиму (enable). Команда enable secret переопределяет незашифрованный пароль, заданный с помощью команды enable password, если заданы оба пароля.
end	Эта команда завершает режим конфигурации.
erase startup-config	Стирает загрузочную конфигурацию, сохраненную в энергонезависимой памяти.
hostname *имя_хоста*	Задает имя системы, являющееся частью приглашения.
interface vlan 1	Активирует режим конфигурации интерфейса VLAN 1, в котором задается IP-адрес для управления коммутатором.
ip address *ip-адрес маска*	Задает IP-адрес и маску интерфейса.
ip default-gateway *ip-адрес*	Задает шлюз по умолчанию для коммутатора. Шлюз по умолчанию – это маршрутизатор, который будет пересылать IP-пакеты, не предназначенные для локальной сети.
line vty 0 15	Активирует режим конфигурации линии виртуального терминала. Линии виртуального терминала (VTY) позволяют получать доступ к коммутатору для удаленного управления сетью. Доступное количество линий VTY зависит от версии ПО Cisco IOS. Обычно используются значения 0-4 и 0-15 (включительно).
login	Эта команда активирует процесс входа в систему, запрашивающий ввод имени пользователя и пароля для доступа в систему.
password *пароль линии*	Назначает пароль портам VTY или консольным портам.
reload	Перезапускает коммутатор и перезагружает операционную систему Cisco IOS и конфигурацию.
show interface vlan 1	Отображает информацию об IP-адресе коммутатора (Cisco Catalyst 2950).
[**no**] **shutdown**	Используйте команду конфигурации интерфейса **shutdown** для отключения интерфейса. Используйте форму **no** этой команды для перезапуска отключенного интерфейса.

Подсказки

Для этого упражнения доступны следующие подсказки. Таблица ниже содержит данные, которые необходимо ввести во время начальной настройки коммутатора.

Таблица 1. Сведения о пароле

Параметр конфигурации	Значение
Enable password	cisco
Enable secret password	sanfran
Hostname	См. таблицу 2
IP address and subnet mask	См. таблицу 2
IP default gateway	10.*x.x*.3 (где *x.x* второй и третий октет адреса рабочей группы)
Пароль линии VTY	sanjose

Таблица 2. Сведения об IP-адресах коммутаторов

Рабочая группа	Имя хоста	IP-адрес коммутатора	Маска
A	**SwitchA**	**10.2.2.11**	**255.255.255.0**
B	**SwitchB**	**10.3.3.11**	**255.255.255.0**
C	**SwitchC**	**10.4.4.11**	**255.255.255.0**
D	**SwitchD**	**10.5.5.11**	**255.255.255.0**
E	**SwitchE**	**10.6.6.11**	**255.255.255.0**
F	**SwitchF**	**10.7.7.11**	**255.255.255.0**
G	**SwitchG**	**10.8.8.11**	**255.255.255.0**
H	**SwitchH**	**10.9.9.11**	**255.255.255.0**

Задача 1: Подключение к коммутатору назначенной рабочей группы

В этой задаче вам необходимо подключиться к назначенной рабочей группе, используя сведения и процедуру из лабораторной работы 2-1.

Процедура упражнения

Выполните следующие действия:

Действие 1 Подключитесь к коммутатору рабочей группы через SSH, используя сведения из лабораторной работы 2-1.

Действие 2 В первом меню введите номер элемента, соответствующий назначенной рабочей группе. Этот номер –число из диапазона от 1 до 8.

Действие 3 В меню рабочей группы введите **cls2**. При запросе подтверждения нажмите клавишу **Enter**. При этом будут сброшены все соединения, открытые ранее. Эта операция может потребоваться в следующих лабораторных работах в случае неожиданного завершения соединения. Вывод должен быть аналогичен примеру ниже.


```
************************    ICND WG_Z   ***************************
************************      MENU      ***************************
   To exit ssh session and return to the menu press
  <CTRL>+<SHFT>+<6> then <X>. To clear a connection to begin
 a new console session type cls# (where # = the menu item number)
        Type "exit" to return to main menu.
*****************************************************************
 ITEM#    DEVICE NAME
-----------------------------------------------------------------


  1       WorkGroup Z Router

  2       WorkGroup Z Switch

  exit    Return to main menu

Please enter selection: cls2
[confirm]<ENTER>
 [OK]
```

Действие 4 Подключитесь к коммутатору рабочей группы, выбрав вариант **2** в меню, затем нажмите клавишу **Enter**. Вывод на экран должен быть аналогичен примеру ниже.

```
************************    ICND WG_Z   ***************************
************************      MENU      ***************************
   To exit ssh session and return to the menu press
  <CTRL>+<SHFT>+<6> then <X>. To clear a connection to begin
 a new console session type cls# (where # = the menu item number)
        Type "exit" to return to main menu.
*****************************************************************
 ITEM#    DEVICE NAME
-----------------------------------------------------------------


  1       WorkGroup Z Router

  2       WorkGroup Z Switch

  exit    Return to main menu

Please enter selection: 2
Trying swa (10.10.10.12, 2067)... Open
```

Проверка упражнения

Задание считается выполненным, если достигнут следующий результат:

- вы получили доступ к коммутатору назначенной рабочей группы в удаленной сети лаборатории с помощью SSH-клиента и сведений из таблицы 2 лабораторной работы 2-1.

Задача 2: Подтверждение отсутствия конфигурации коммутатора и перезагрузка

В этой задаче вам необходимо использовать команду **erase startup-config**, чтобы убедиться в отсутствии сохраненной конфигурации коммутатора в файле startup-config в NVRAM (энергонезависимой памяти). Затем следует перезагрузить ПО коммутатора и изучить вывод, созданный при перезагрузке.

Процедура упражнения

Выполните следующие действия:

Действие 1 Чтобы открыть приглашение нажмите клавишу **Enter** несколько раз. Если появилось приглашение «Switch>», перейдите к действию 3. В противном случае перейдите к действию 2.

Действие 2 Если вывод аналогичен примеру ниже, выберите **Yes** в качестве ответа на вопрос. Дважды нажмите клавишу **Enter**.

```
Would you like to terminate autoinstall? [yes]: yes


     --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no

Switch>
Switch>
```

Действие 3 В данный момент система работает в пользовательском режиме. Чтобы просмотреть результат ввода команды привилегированного режима в пользовательском режиме, введите команду **erase startup-config.** Вывод должен быть аналогичен примеру ниже.

```
Switch>erase startup-config
    ^
% Invalid input detected at '^' marker.
```

Действие 4 Эти данные появляются после ввода привилегированной команды EXEC в пользовательском режиме. Введите команду **enable**. На экране должна появиться следующая информация.

```
Switch>enable
Switch#
```

Действие 5 Обратите внимание, что приглашение коммутатора изменилось с Switch> на Switch#. Оно указывает, что используется привилегированный режим (enable EXEC). Если теперь ввести команду **erase startup-config**, она будет принята. Нажмите клавишу **Enter** для подтверждения и снова нажмите **Enter**, чтобы получить приглашение маршрутизатора. На экране должна появиться следующая информация.

```
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]<ENTER>
[OK]
Erase of nvram: complete
00:18:46: %SYS-7-NV_BLOCK_INIT: Initalized the geometry of nvram <ENTER>
Switch#
```

Действие 6 Введите команду **reload**. Появится запрос подтверждения. Подтвердите перезагрузку. Затем появится большой массив данных о состоянии коммутатора в процессе перезагрузки. Вывод должен быть аналогичен примеру ниже. Некоторые повторяющиеся фрагменты пропущены для сокращения объема вывода.

```
Switch#reload
Proceed with reload? [confirm]<ENTER>

00:21:00: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.
```



```
Base ethernet MAC Address: 00:1a:6d:44:6c:80
Xmodem file system is available.
The password-recovery mechanism is enabled.
Initializing Flash...
flashfs[0]: 597 files, 19 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 32514048
flashfs[0]: Bytes used: 8208384
flashfs[0]: Bytes available: 24305664
flashfs[0]: flashfs fsck took 9 seconds.
...done Initializing Flash.
Boot Sector Filesystem (bs) installed, fsid: 3
done.
Loading "flash:c2960-lanbasek9-mz.122-25.SEE2/c2960-lanbasek9-mz.122-
25.SEE2.bin"...@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
..
.. text omitted
..
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
File "flash:c2960-lanbasek9-mz.122-25.SEE2/c2960-lanbasek9-mz.122-25.SEE2.bin"
uncompressed and installed, entry point: 0x3000
executing...

       Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

      cisco Systems, Inc.
      170 West Tasman Drive
      San Jose, California 95134-1706



Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(25)SEE2, RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 28-Jul-06 11:57 by yenanh
Image text-base: 0x00003000, data-base: 0x00BB7944

Initializing flashfs...

flashfs[1]: 597 files, 19 directories
flashfs[1]: 0 orphaned files, 0 orphaned directories
flashfs[1]: Total bytes: 32514048
flashfs[1]: Bytes used: 8208384
flashfs[1]: Bytes available: 24305664
flashfs[1]: flashfs fsck took 1 seconds.
flashfs[1]: Initialization complete....done Initializing flashfs.

POST: CPU MIC register Tests : Begin
POST: CPU MIC register Tests : End, Status Passed

POST: PortASIC Memory Tests : Begin
POST: PortASIC Memory Tests : End, Status Passed

POST: CPU MIC PortASIC interface Loopback Tests : Begin
POST: CPU MIC PortASIC interface Loopback Tests : End, Status Passed

POST: PortASIC RingLoopback Tests : Begin
```

```
POST: PortASIC RingLoopback Tests  : End, Status Passed

POST: PortASIC CAM Subsystem Tests : Begin
POST: PortASIC CAM Subsystem Tests : End, Status Passed

POST: PortASIC Port Loopback Tests : Begin
POST: PortASIC Port Loopback Tests : End, Status Passed

Waiting for Port download...Complete


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco WS-C2960-24TT-L (PowerPC405) processor (revision B0) with 61440K/4088K bytes of
memory.
Processor board ID FOC1048ZE27
Last reset from power-on
1 Virtual Ethernet interface
24 FastEthernet interfaces
2 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.

64K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:1A:6D:44:6C:80
Motherboard assembly number    : 73-10390-03
Power supply part number       : 341-0097-02
Motherboard serial number      : FOC10483A1C
Power supply part number       : DCA104382KM
Model revision number          : B0
Motherboard serial number      : C0
Model number                   : WS-C2960-24TT-L
System serial number           : FOC1048ZE27
Top Assembly Part Number       : 800-27221-02
Top Assembly Revision Number   : C0
Version ID                     : V02
CLEI Code Number               : COM3L00BRA
Hardware Board Revision Number : 0x01


Switch  Ports   Model             SW Version        SW Image
------  -----   -----             ----------        ----------
*    1  26      WS-C2960-24TT-L   12.2(25)SEE2      C2960-LANBASEK9-M



Press RETURN to get started!


00:00:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:40: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for type vlan
00:01:01: %SYS-5-RESTART: System restarted --
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(25)SEE2, RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2006 by Cisco Systems, Inc.
```



```
Compiled Fri 28-Jul-06 11:57 by yenanh
00:01:03: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
00:01:03: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to up
00:01:03: %LINK-3-UPDOWN: Interface FastEthernet0/11, changed state to up
00:01:03: %LINK-3-UPDOWN: Interface FastEthernet0/12, changed state to up
00:01:04: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state
to up
00:01:04: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state
to up
00:01:04: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed state
to up
00:01:04: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/12, changed state
to up
00:01:33: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
```

Действие 7 Чтобы запретить автоматическую установку, при отображении соответствующего запроса нажмите клавишу **Enter**, чтобы принять значение по умолчанию «yes» (запретить автоматическую установку).

```
Would you like to terminate autoinstall? [yes]:<ENTER>
```

Действие 8 Далее система предложит войти в диалог начальной конфигурации. Задача выполнена**.** *Обратите внимание, что ответ на этот вопрос необходимо будет ввести в действии 1 следующей задачи.*

```
     --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:
```

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- существующая конфигурация успешно удалена;
- получен вывод, аналогичный выводу в действия с 6 по 8.

Задача 3: Использование диалога конфигурации системы для создания начальной конфигурации

Продолжая процесс, начатый в предыдущей задаче, выберите диалог начальной конфигурации, чтобы вызвать диалог System Configuration (Конфигурация системы). После этого следует ввести базовые параметры коммутатора. Этот режим настройки также называется «setup» по названию инструкции командной строки, которая его активирует.

Процедура упражнения

Выполните следующие действия:

Действие 1 Вы готовы к начальной настройке. В ответ на запрос (*из последнего шага предыдущей задачи, см. ниже*), введите **yes** и нажмите клавишу **Enter**, чтобы продолжить настройку коммутатора. Значения, которые необходимо ввести во время настройки, выделены жирным шрифтом.

```
     --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:yes
```

Действие 2 Откажитесь от ввода базовых параметров управления, выбрав **no**.

```
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: no
```

Действие 3 Откажитесь от проверки интерфейсов, указав **no** в качестве ответа на вопрос.

```
First, would you like to see the current interface summary? [yes]: no
```

Действие 4 Введите имя хоста назначенного коммутатора (например, SwitchJ).

```
Configuring global parameters:

 Enter host name [Switch]: SwitchX
```

Действие 5 Введите все пароли, используя данные из таблицы 1 лабораторной работы 2-2.

Пароль «enable secret» используется для защиты доступа к привилегированному режиму EXEC и режимам конфигурации. После ввода в конфигурацию этот пароль шифруется.

```
 Enter enable secret: sanfran
```

Действие 6 Пароль «enable password» используется в некоторых старых версиях программного обеспечения и загрузочных образах, если не указан пароль enable secret.

```
 Enter enable password: cisco
```

Действие 7 Пароль виртуального терминала используется для защиты доступа к маршрутизатору через сетевой интерфейс.

```
 Enter virtual terminal password: sanjose
```

Действие 8 Введите **no** в качестве ответа на приглашение Configure SNMP Network Management.

```
 Configure SNMP Network Management? [no]: no
```

Действие 9 Введите **yes** в качестве ответа на приглашение «Do You Want to Configure Vlan1 Interface?». Данные об IP-адресе можно найти в таблице 2.

```
Configuring interface parameters:

Do you want to configure Vlan1 interface? [no]: yes
 Configure IP on this interface? [no]: yes
  IP address for this interface: 10.x.x.11
  Subnet mask for this interface [255.0.0.0] : 255.255.255.0
  Class A network is 10.0.0.0, 24 subnet bits; mask is /24
```

Действие 10 Введите **no** в качестве ответа на все остальные приглашения конфигурации интерфейса.

```
Do you want to configure FastEthernet0/1 interface? [yes]: no
```



```
Do you want to configure FastEthernet0/2 interface? [yes]: no
Do you want to configure FastEthernet0/3 interface? [yes]: no
Do you want to configure FastEthernet0/4 interface? [yes]: no
Do you want to configure FastEthernet0/5 interface? [yes]: no
Do you want to configure FastEthernet0/6 interface? [yes]: no
Do you want to configure FastEthernet0/7 interface? [yes]: no
Do you want to configure FastEthernet0/8 interface? [yes]: no
Do you want to configure FastEthernet0/9 interface? [yes]: no
Do you want to configure FastEthernet0/10 interface? [yes]: no
Do you want to configure FastEthernet0/11 interface? [yes]: no
Do you want to configure FastEthernet0/12 interface? [yes]: no
Do you want to configure FastEthernet0/13 interface? [yes]: no
Do you want to configure FastEthernet0/14 interface? [yes]: no
Do you want to configure FastEthernet0/15 interface? [yes]: no
Do you want to configure FastEthernet0/16 interface? [yes]: no
Do you want to configure FastEthernet0/17 interface? [yes]: no
Do you want to configure FastEthernet0/18 interface? [yes]: no
Do you want to configure FastEthernet0/19 interface? [yes]: no
Do you want to configure FastEthernet0/20 interface? [yes]: no
Do you want to configure FastEthernet0/21 interface? [yes]: no
Do you want to configure FastEthernet0/22 interface? [yes]: no
Do you want to configure FastEthernet0/23 interface? [yes]: no
Do you want to configure FastEthernet0/24 interface? [yes]: no
Do you want to configure GigabitEthernet0/1 interface? [yes]: no
Do you want to configure GigabitEthernet0/2 interface? [yes]: no
```

Действие 11 Введите **no** в качестве ответа на приглашение Enable as a Cluster Command Switch.

```
Would you like to enable as a cluster command switch? [yes/no]: no
```

Действие 12 Процесс конфигурации отобразит команды Cisco IOS, правильность которых вы должны проверить. Нажимайте клавишу **ПРОБЕЛ** для получения дополнительных данных при запросе вывода дополнительных данных (приглашение --More--).

```
The following configuration command script was created:

hostname SwitchX
enable secret 5 $1$3PTL$CG2pEpzgAJO3pkB7If4P9.
enable password cisco
line vty 0 15
password sanjose
no snmp-server
!
!
interface Vlan1
no shutdown
ip address 10.10.10.11 255.255.255.0
```

```
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
end
```

Действие 13 Если отображается правильная начальная конфигурация, введите **2** для сохранения этой конфигурации в загрузочном файле конфигурации в NVRAM и выйдите из режима конфигурации.

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.
```


Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- вывод начальной конфигурации совпал со значениями, заданными для коммутатора рабочей группы;
- вы выбрали вариант 2, чтобы сохранить конфигурацию в NVRAM и выйти из режима настройки.

Задача 4: Добавление шлюза по умолчанию в начальную конфигурацию

После настройки коммутатора в режиме «setup» необходимо добавить IP-адрес маршрутизатора по умолчанию. Шлюз по умолчанию будет использоваться при пересылке пакетов через интерфейс управления Vlan 1 в сеть без прямого подключения. Настройка маршрутизатора будет выполняться в следующей лабораторной работе.

Процедура упражнения

Выполните следующие действия:

Действие 1 Перейдите из пользовательского режима EXEC в привилегированный режим с помощью команды **enable**. Введите пароль, когда система попросит сделать это.

Примечание. Вспомните, что во время предыдущей задачи для «enable password» задано значение «sanfran».

Действие 2 В привилегированном режиме введите команду **configure terminal**. Эта команда часто сокращается до **conf t**. Вывод должен выглядеть следующим образом.

```
SwitchX#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchX(config)#
```

Действие 3 Введите команду **ip default-gateway 10.*x*.*x*.3**, где *x.x* – это второй и третий октеты адреса, назначенного интерфейсу VLAN 1 коммутатора. Вывод на экран должен выглядеть следующим образом.

```
SwitchX(config)#ip default-gateway 10.10.10.3
SwitchX(config)#
```

Действие 4 Выйдите из режима конфигурации с помощью команды **end**. Вывод на экран должен выглядеть следующим образом.

```
SwitchX(config)#end
SwitchX#
1d00h: %SYS-5-CONFIG_I: Configured from console by console
```

Действие 5 Введите команду **copy running-config startup-config** для сохранения текущей конфигурации в NVRAM. Вам будет предложено подтвердить имя файла. Для подтверждения нажмите клавишу **Enter**. Вывод на экран должен выглядеть следующим образом.

```
SwitchX#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SwitchX#
```

Примечание. Общепринятое сокращение команды **copy running-config startup-config** – **copy run start.**

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- в текущую конфигурацию добавлен IP-адрес шлюза по умолчанию;
- текущая конфигурация сохранена в файле startup-config.

Лабораторная работа 2-3: Повышение безопасности начальной конфигурации коммутатора

Выполните упражнение этой лабораторной работы, чтобы применить на практике знания, полученные в соответствующем модуле.

Задачи упражнения

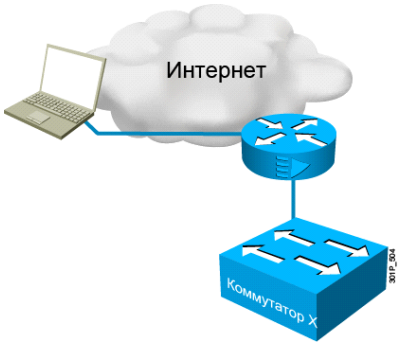
В этом упражнении вам необходимо повысить безопасность начальной конфигурации коммутатора. После выполнения этого упражнения вы будете способны сделать следующее:

- настроить безопасность консоли и линий VTY на базе пароля;
- зашифровать все пароли с помощью команды Cisco IOS;
- добавить баннерное сообщение для процесса входа в систему;
- повысить безопасность удаленного управления коммутатором, добавив протокол SSH к линиям VTY;
- повысить безопасность физических интерфейсов путем настройки различных методов безопасности на базе MAC-адреса;
- отключить неиспользуемые интерфейсы.

Иллюстрация задания

На рисунке ниже показано, что вы должны сделать во время данного упражнения.

Иллюстрация задания к лабораторной работе 2-3 Повышение безопасности начальной конфигурации коммутатора



Имя хоста рабочей группы	IP-адрес коммутатора	Маска подсети
SwitchA	10.2.2.11	255.255.255.0
SwitchB	10.3.3.11	255.255.255.0
SwitchC	10.4.4.11	255.255.255.0
SwitchD	10.5.5.11	255.255.255.0
SwitchE	10.6.6.11	255.255.255.0
SwitchF	10.7.7.11	255.255.255.0
SwitchG	10.8.8.11	255.255.255.0
SwitchH	10.9.9.11	255.255.255.0

Необходимые ресурсы

Ниже перечислены ресурсы и устройства, необходимые для выполнения упражнения.

- ПК, подключенный к удаленной лаборатории.
- Приложение для эмуляции терминала с поддержкой SSH.
- Информация о назначенном комплекте оборудования, полученная в лабораторной работе 2-1.
- Успешное выполнение лабораторной работы 2-2.

Список команд

В таблице приводится описание команд, используемых в упражнении.

Команды коммутатора Cisco IOS

Команда	Описание
? или **help**	В пользовательском режиме EXEC ПО Cisco IOS выводит подмножество команд, доступных на данном уровне привилегий.
banner login	Позволяет настроить сообщение, которое будет отображаться во время входа в систему.
clear mac-address-table dynamic interface *int-id*	Очищает динамически полученные MAC-адреса, связанные с указанным интерфейсом.
clear port-security sticky interface *int-id* **access**	Очищает безопасные MAC-адреса, связанные с указанным интерфейсом. При использовании параметра access команда не действует на транковые порты.
configure terminal	Активирует режим конфигурации с терминала.
copy running-config *место назначения*	Копирует файл текущей конфигурации коммутатора в другое место назначения. Обычно это загрузочная конфигурация.
copy running-config startup-config	Копирует файл текущей конфигурации в файл загрузочной конфигурации, который хранится в локальной памяти NVRAM.
crypto key generate rsa	Генерирует используемые пары ключей RSA.
enable	Активирует привилегированный режим EXEC. В привилегированном режиме EXEC доступно большее количество команд. Эта команда требует ввода пароля разрешения доступа (enable password), если он настроен.
end	Эта команда завершает режим конфигурации.
interface *int-id*	Активирует режим конфигурации интерфейса.
interface range *int-id* **–** *последний номер порта*	Активирует режим конфигурации группы интерфейсов. Это позволит применять следующие команды конфигурации ко всем указанным интерфейсам одновременно.
ip domain-name *имя*	Задает имя домена IP, которое необходимо для процесса генерации криптографического ключа.
ip ssh version [1 | 2]	Указывает версию протокола SSH, которую необходимо запустить. Чтобы отключить настроенную версию SSH и вернуться в режим совместимости, используйте версию **no** данной команды.
line console 0	Активирует режим конфигурации консольной линии 0.

line vty 0 15	Вход в режим конфигурации линий виртуального терминала. Линии виртуального терминала (VTY) позволяют получать доступ к коммутатору для удаленного управления сетью. Доступное количество линий VTY зависит от версии ПО Cisco IOS. Обычно используются значения от 0 до 4 и от 0 до15 (включительно).
login	Активирует процесс входа на консоли или линиях VTY.
login local	Активирует процесс входа на консоли или линиях VTY, требующий использования локальной базы данных аутентификации.
logout	Выход из режима EXEC, после которого потребуется повторная аутентификация (если она включена).
password	Назначает пароль линиям VTY или консоли.
ping *ip-адрес*	Общепринятое средство выявления проблем доступа к устройствам. Использует эхо-запросы и эхо-ответы ICMP, чтобы определить, активен ли удаленный хост. Команда **ping** также определяет количество времени, затрачиваемое на получение эхо-ответа.
reload	Перезапускает коммутатор и перезагружает операционную систему Cisco IOS.
service password-encryption	Включает службу, которая будет шифровать все пароли в текущей конфигурации.
show ip arp	Отображает таблицу разрешения IP-адресов, в которой хранятся привязки между IP-адресами и соответствующими MAC-адресами.
show ip ssh	Показывает текущие параметры протокола SSH.
show mac-address-table dynamic	Выводит только динамически полученные MAC-адреса таблицы.
show mac-address-table interface *int-id*	Выводит только MAC-адреса таблицы, связанные с указанным интерфейсом.
show port-security *интерфейс int-id*	Выводит все административные и рабочие состояния всех безопасных портов коммутатора. Также может выводить параметры безопасности определенного интерфейса и все безопасные MAC-адреса.
show running-config	Выводит активную конфигурацию.
show running-config interface *int-id*	Выводит текущую конфигурацию интерфейса, указанного в команде.
shutdown **no shutdown**	Отключает или включает интерфейс.
switchport mode access	Устанавливает режим доступа для порта. Используйте версию **no** этой команды, чтобы вернуться к значением по умолчанию.
switchport port-security	Включает защиту портов интерфейса. Вводится без ключевых слов.
switchport port-security mac-address sticky	Задает безопасные MAC-адреса, связанные с интерфейсом, которые должны быть получены динамически.
switchport port-security maximum *[число]*	Задает максимальное число безопасных MAC-адресов для интерфейса. Используйте версию **no** этой команды, чтобы отменить ее.
switchport port-security violation *режим нарушения*	Определяет действие, предпринимаемое портом при нарушении безопасности. Три допустимых режима: protect (защита), restrict (ограничение) и shutdown (отключение).
transport input telnet ssh	Определяет, какие протоколы используются для подключения к определенной линии коммутатора.
username *имя_пользователя* **password** *пароль*	Создает пару имени пользователя и пароля, которая затем может использоваться как локальная база данных аутентификации.

Подсказки

Для этого упражнения доступны следующие подсказки.

- См. сведения о подключении в лабораторной работе 2-1.

Таблица 1. Текущие пароли

Вход в консоль коммутатора	нет
Пароль «enable password» коммутатора	cisco
Пароль «enable secret» коммутатора	sanfran
Пароль для входа в систему коммутатора через линию VTY	sanjose

Задача 1: Добавление защиты на основе пароля к консольному порту и линиям VTY

В начальной конфигурации коммутатора, в которой заданы пароли для линий VTY, существуют две потенциальные бреши системы безопасности. Во-первых, нарушение безопасности возможно в том случае, если для линий VTY отключен процесс входа и используется слишком простой пароль. Во-вторых, безопасность может быть нарушена, если порт консоли не защищен паролем.

Процедура упражнения

Выполните следующие действия:

Действие 1 Подключитесь к удаленному коммутатору рабочей группы через терминальный сервер и введите необходимые команды и пароли, чтобы перейти к приглашению привилегированного режима.

Действие 2 В приглашении пользовательского режима EXEC введите команду **enable** и пароль коммутатора, заданный в параметре «enable password».

Действие 3 В приглашении привилегированного режима EXEC (которое иногда называется «приглашением enable») назначенного коммутатора введите команду **config t**.

Действие 4 Перейдите к конфигурации консольного порта с помощью команды **line console 0**.

Действие 5 В режиме конфигурации консольной линии используйте пароль «sanjose» для консольной линии. Введите команду **password sanjose**.

Действие 6 Введите команду **login**, чтобы в будущем для доступа к коммутатору через консоль запрашивался ввод пароля.

Действие 7 Введите команду **line vty 0 15**.

Действие 8 Введите команду **login**, которая будет применяться ко всем 16 линиям (с 0 по 15).

Действие 9 Введите команду **end**, чтобы вернуться к приглашению привилегированного режима EXEC.

Действие 10 Введите команду **show running-config** и изучите вывод, чтобы убедиться в правильности конфигурации порта консоли (0) и линий vty (с 0 по 15). Он должен соответствовать выводу в примере ниже, конфигурация линий выделена жирным шрифтом. Обратите внимание, что пароли для консольного порта и линий виртуального терминала сохраняются в виде незашифрованного текста.

```
SwitchX#show running-config
..
..Text omitted
..
!
line con 0
 password sanjose
 login
line vty 0 4
 password sanjose
 login
line vty 5 15
 password sanjose
 login
!
end
```

Действие 11 Теперь следует проверить настройку пароля. Для этого выйдите из системы коммутатора и войдите в нее снова через консоль.

Действие 12 Введите команду **logout**.

Действие 13 Нажмите клавишу **Enter**, чтобы получить приглашение к вводу пароля.

Действие 14 Введите только что заданный пароль, чтобы получить приглашение пользовательского режима (user EXEC).

Действие 15 Введите команду и пароль для получения доступа к приглашению привилегированного режима (enable EXEC).

Действие 16 Ниже приводится пример данных, которые должны выводиться на экран при выполнении действий с 12 по 15.

```
SwitchX#logout

..
..empty lines omitted
..

SwitchX con0 is now available


Press RETURN to get started.

..
..empty lines omitted
..

User Access Verification

Password:
SwitchX>enable
Password:
SwitchX#
```

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- вы настроили запрос пароля для консоли и линий VTY;
- при проверке конфигурации вы выяснили, что пароли для линий сохранены в виде незашифрованного текста;
- вы успешно проверили процесс входа в систему и доступ к консоли с использованием пароля;
- вывод соответствовал примеру, приведенному в действии 14.

Задача 2: Активация службы шифрования паролей

В предыдущей задаче мы отметили, что некоторые пароли хранятся в незашифрованном виде. При передаче и сохранении данной конфигурации на удаленных файловых системах могут возникать проблемы безопасности. В этой задаче необходимо настроить службу шифрования паролей для защиты всех незашифрованных паролей.

Процедура упражнения

Выполните следующие действия:

Действие 1 Используя приглашение привилегированного режима (enable EXEC), введите команду для перехода в режим глобальной конфигурации.

Действие 2 Введите команду **service password-encryption**.

Действие 3 Введите команду для возвращения к приглашению привилегированного режима.

Действие 4 Введите команду для просмотра текущей конфигурации. Обратите внимание на первые и последние строки конфигурации, команда **service password-encryption** активна и действует на пароли для линий. Вывод должен соответствовать примеру ниже. Жирным шрифтом выделены данные, на которые следует обратить внимание.

```
SwitchX#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchX(config)#service password-encryption
SwitchX(config)#end
SwitchX#
00:38:45: %SYS-5-CONFIG_I: Configured from console by console
SwitchX#show running-config
Building configuration...

Current configuration : 1453 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
..
..Text omitted
..

!
!
```



```
line con 0
 password 7 14041305060B392E
 login
line vty 0 4
 password 7 14041305060B392E
 login
line vty 5 15
 password 7 120A041918041F01
 login
!
end
```

Действие 5 Введите команду для сохранения текущей конфигурации в файле startup-config.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- включена служба шифрования паролей;
- вам удалось вывести текущую конфигурацию и найти зашифрованные пароли линий;
- вы сохранили текущую конфигурацию.

Задача 3: Применение баннера входа

В рамках любой политики безопасности необходимо явно указать, что доступ к сетевым ресурсам случайным посетителем запрещен. В прошлом хакеры успешно использовали факт наличия приглашения «welcome» (добро пожаловать) при входе в качестве юридического оправдания несанкционированного проникновения в сеть. Когда пользователь пытается получить доступ к сетевому устройству (коммутатору, маршрутизатору и т. д.), должно появляться сообщение, явно указывающее на ограничение доступа. Его можно создать с помощью команды **banner** Cisco IOS.

Процедура упражнения

Выполните следующие действия:

Действие 1 Введите команду для доступа к приглашению глобальной конфигурации.

Действие 2 Введите команду **banner login %** и нажмите клавишу **Enter**. Знак процента (%) является начальным символом-разделителем текста сообщения.

Действие 3 Введите текст сообщения после знака **%**.

Примечание. *Не* используйте знаки процента в тексте сообщения в заголовке, поскольку они будут рассматриваться как конечные символы-разделители сообщения.

Действие 4 Ниже приведен пример вывода конфигурации баннерного сообщения.

```
SwitchX#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchX(config)#banner login %
Enter TEXT message. End with the character '%'.
********** Warning  *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.

************************************************************%
SwitchX(config)#
```

Действие 5 Введите команду для возвращения в режим EXEC.

Действие 6 Введите команду для просмотра текущей конфигурации. Ниже приведен фрагмент вывода, который относится к конфигурации баннера. Обратите внимание, что текстовый символ-разделитель заменен нетекстовым управляющим символом ^C.

```
!
banner login ^C
**********  Warning  *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.

************************************************************^C
!
```

Действие 7 Используйте команду **logout** для завершения сеанса консоли. Затем снова выполните вход, чтобы получить доступ к приглашению привилегированного режима. Обратите внимание, что перед вводом пароля отображается баннерное сообщение. Ниже приведен фрагмент информации, которая должна появиться на экране. Для экономии места вывод приведен не полностью.

```
SwitchX#logout


SwitchX con0 is now available


Press RETURN to get started.



*********  Предупреждение  *************
Доступ к этому устройству разрешен только санкционированным пользователям!
Несанкционированный доступ запрещен. Злоумышленники будут преследоваться
по закону.

************************************************************

User Access Verification

Password:
SwitchX>en
Password:
SwitchX#
```

Действие 8 Введите команду для сохранения текущей конфигурации в файле startup-config.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- настроено баннерное сообщение для входа, явно указывающее, на то, что доступ к коммутатору ограничен;
- сообщения при входе в систему проверено, перед запросом пароля отображается предупреждение;
- конфигурация сохранена.

Задача 4: Включение протокола SSH для удаленного управления

В предыдущей задаче пароли были защищены с помощью шифрования. Однако если процесс удаленного управления основан на протоколе Telnet, который отправляет все символы, включая пароли, в незашифрованном виде, существует потенциальная опасность перехвата пакета и неправомерного использования информации. В этой задаче вам необходимо настроить протокол SSH, который является альтернативой протоколу Telnet. Если среда позволяет, мы рекомендуем *заменить* Telnet на SSH. Для работы SSH требуются следующие данные:

- имя пользователя и пароль;
- определенное имя хоста;
- определенный домен IP;
- ключ шифрования RSA.

Процедура упражнения

Выполните следующие действия:

Действие 1 В приглашении привилегированного режима (enable EXEC) введите команду для доступа к приглашению глобальной конфигурации.

Действие 2 Протокол SSH требует использования имени пользователя и пароля. Если они еще не заданы, настройте их сейчас. Введите команду **username** *имя_пользователя* **password** *пароль*. В этом примере в качестве имени пользователя и пароля будет использоваться слово «netadmin». Безусловно, в реальной среде необходимо использовать более сложное имя пользователя и пароль.

Действие 3 Для генерации криптографического ключа SSH необходимо, чтобы в конфигурации были заданы и имя хоста, и имя домена. Имя хоста уже задано, поэтому необходимо указать имя домена. Обычно используется имя домена организации, но в этой лабораторной работе будет использоваться «cisco.com».

Действие 4 Введите команду **ip domain-name** *имя домена*.

Действие 5 Введите команду **crypto key generate rsa**. Появится запрос размера ключа; по умолчанию используется значение 512, но для создания более безопасного ключа необходимо ввести **1024**. Вывод должен соответствовать примеру ниже. В этот пример включены только строки, которые относятся к данной задаче.

```
SwitchX(config)#username netadmin password netadmin
SwitchX(config)#ip domain-name cisco.com
SwitchX(config)#crypto key generate rsa
The name for the keys will be: SwitchX.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
 General Purpose Keys. Choosing a key modulus greater than 512 may take
 a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys ...[OK]

01:26:52: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Действие 6 Введите команду **ip ssh version 2**, чтобы включить нужную версию SSH.

Действие 7 Введите команду **line vty 0 15**.

Действие 8 Введите команду **login local**. Она позволяет перевести процесс входа на использование локально заданных пар имени пользователя и пароля.

Действие 9 Введите команду **transport input telnet ssh**. Она настроит 16 линий VTY для поддержки обоих протоколов: Telnet и SSH. Вывод должен быть аналогичен примеру ниже.

```
SwitchX(config)#line vty 0 15
SwitchX(config-line)#login local
SwitchX(config-line)#transport input telnet ssh
```

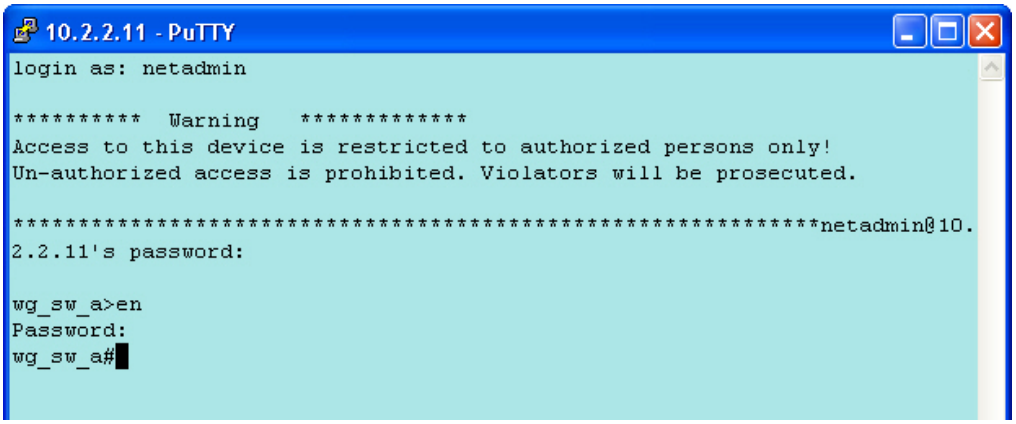
Действие 10 Введите команду для возвращения к приглашению привилегированного режима.

Действие 11 Введите команду **show ip ssh**.

```
SwitchX#sh ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
```

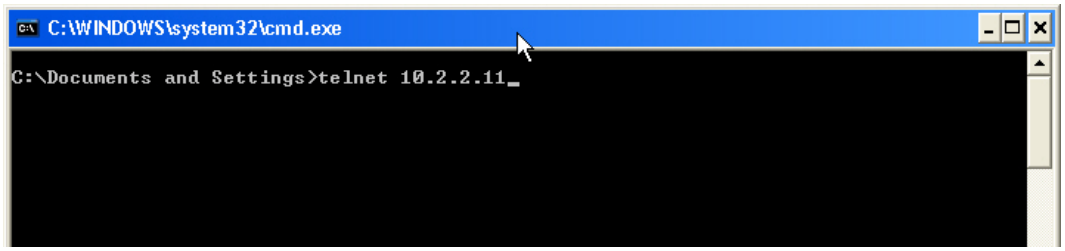
Действие 12 Для проверки конфигурации необходимо создать подключение туннеля VPN к удаленной лаборатории, используя метод из задачи 2 лабораторной работы 2-1. На ПК откройте клиентское приложение терминала SSH. Используйте IP-адрес коммутатора рабочей группы и пару имени пользователя и пароля, заданную во время действия 2 этой задачи.

Действие 13 Ниже приводится пример успешного подключения через протокол SSH с помощью приложения PuTTY.



Действие 14 Введите команду **logout**, чтобы выйти из окна подключения PuTTY.

Действие 15 Откройте окно командной строки Windows и введите команду **telnet 10.*x.x*.11** (IP-адрес коммутатора рабочей группы). Вывод должен быть аналогичен примеру ниже.



Действие 16 Введите имя пользователя и пароль в новом окне командной строки Telnet, которое откроется автоматически. Включив сеансы Telnet и SSH одновременно, введите **logout** в приглашении пользовательского режима (user EXEC) и закройте окно командной строки, введя **exit** в приглашении. Вывод должен быть аналогичен примеру ниже.

Действие 17 Введите команду для сохранения конфигурации в файле startup-config.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- на линиях VTY настроена поддержка протокола SSH 2;
- создано прямое подключение к коммутатору рабочей группы с использованием протоколов SSH и Telnet, чтобы проверить поддержку их одновременной работы;
- конфигурация сохранена.

Задача 5: Настройка безопасности порта на коммутаторе

В этой задаче вам необходимо разрешить использование ограниченного числа MAC-адресов на первом порту доступа коммутатора, а также выбрать действие, которое коммутатор должен выполнить при превышении максимально допустимого числа. Сначала вы должны определить, сколько адресов получается динамически, затем изменить интерфейс, разрешив меньшее на единицу количество, чтобы создать нарушение правила для MAC-адресов. Для просмотра состояния и режима работы коммутатора перед окончательной настройкой безопасного количества адресов (возврата к приемлемому значению, не вызывающему ошибок) следует использовать команду **show**.

Процедура упражнения

Обратитесь к порту консоли коммутатора SwitchX, где *x* – это ваш комплект оборудования. Выполните следующие действия для настройки безопасности порта на коммутаторе рабочей группы:

Примечание. В конце предыдущей лабораторной работы вы должны были сохранить текущую активную конфигурацию. Если вы сомневаетесь, что это было сделано, сохраните текущую конфигурацию в файле startup-config перед перезагрузкой.

Действие 1 Введите команды для перезагрузки коммутатора.

Действие 2 Введите команду для перехода к приглашению привилегированного режима (enable EXEC).

Действие 3 Введите команду ping для проверки связи с IP-адресом, указанным в следующей таблице. **Эта таблица будет заполняться во время действий 4 и 5.**

Таблица MAC-адресов

IP-адрес устройства	MAC-адрес
10.*x.x*.100	
Неуправляемое устройство	

Действие 4 Введите команду **show ip arp**. Будут выведены привязки между IP-адресом и MAC-адресом. **Введите соответствующий MAC-адрес в приведенную выше таблицу.** Вывод должен быть аналогичен примеру ниже.

```
SwitchX#show ip arp
Protocol Address     Age (min) Hardware Addr   Type   Interface
Internet 10.x.x.11           -  001a.6d44.6cc0  ARPA   Vlan1
Internet 10.x.x.100          0  001a.2fe7.3089  ARPA   Vlan1
```

Действие 5 Введите команду **show mac-address-table int fa0/1**. Должен появиться один MAC-адрес, не связанный с IP-адресом, на который вы отправили эхо-запрос. Это MAC-адрес неуправляемого устройства. Используйте его для заполнения таблицы действия 3. Вывод на экран должен выглядеть следующим образом.

```
SwitchX#show mac-address-table int fa0/1
     Mac Address Table
-------------------------------------------

Vlan  Mac Address     Type      Ports
----  -----------     --------  -----
   1  0017.5a78.be01  DYNAMIC   Fa0/1
   1  0017.5a78.be01  DYNAMIC   Fa0/1
Total Mac Addresses for this criterion: 2
```

Действие 6 Перед настройкой безопасности порта необходимо очистить записи динамически полученных MAC-адресов. Введите команду **clear mac-address-table dynamic int fa0/1**.

Действие 7 Подождите хотя бы 10 секунд перед вводом команды **show mac-address-table int fa0/1**, чтобы увидеть результат выполнения этой команды. Убедитесь, что MAC-адрес неуправляемого устройства все еще присутствует в таблице MAC-адресов. Это связано с тем, что это устройство периодически отправляет кадры 2-го уровня. Для других интерфейсов Ethernet можно настроить периодическую отправку кадров «keep-alive». Однако должны отображаться *только* MAC-адреса, полученные в данный момент. Вывод на экран должен выглядеть следующим образом.

```
SwitchX#show mac-address-table int fa0/1
     Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0017.5a78.be01    DYNAMIC     Fa0/1
Total Mac Addresses for this criterion: 1
```


Действие 8 Введите команду **configure t**.

Действие 9 Введите команду **interface fa0/1**.

Действие 10 Отключите интерфейс с помощью команды **shutdown**.

Действие 11 Перед применением функций безопасности порта к порту коммутатора на нем необходимо отключить режим автосогласования. Введите команду **switchport mode access**.

Действие 12 Перед активацией функции безопасности порта необходимо задать максимальное число MAC-адресов, если их больше 1 (значение по умолчанию). Но поскольку в данной задаче необходимо инициировать нарушение ограничения MAC-адресов, и во время действия 5 было определено, что с этим интерфейсом связано два MAC-адреса, никаких действий не требуется.

Действие 13 Кроме того, перед активацией безопасности порта необходимо настроить действие, которое должно выполняться при попытке использования интерфейсом большего количества MAC-адресов, чем задано в конфигурации. Оно называется действием, выполняемым в случае нарушения. По умолчанию используется действие **shutdown** (административного отключение в результате ошибки). Первоначально вы будете использовать значение по умолчанию, чтобы попрактиковаться во включении отключенного интерфейса.

Действие 14 Введите команду **switchport port-security mac-address sticky**. Полученные MAC-адреса будут сохранены в текущей конфигурации. Если вы сохраните эту конфигурацию в startup-config, они не будут потеряны при перезапуске.

Действие 15 Введите команду **switchport port-security**. При вводе этой команды без параметров активируется защита порта. Если этого не сделать, функция безопасности порта остается отключенной.

Действие 16 Введите команду **no shutdown**, чтобы включить порт коммутатора.

Действие 17 Введите команду **end** для выхода из режима конфигурации и возврата к приглашению привилегированного режима (enable EXEC).

Действие 18 Подождите 20 секунд перед вводом команды **show running-config int fa0/1** для вывода фрагмента текущей конфигурации интерфейса fa0/1. Ниже приведен пример вывода, наиболее важные фрагменты выделены жирным шрифтом.

```
SwitchX#show running-config int fa0/1
Building configuration...

Current configuration : 128 bytes
!
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0017.5a78.be0f
end
```

Действие 19 Введите команду **show port-security int fa0/1** для вывода текущих параметров безопасности порта.

```
SwitchX#show port-security int fa0/1
Port Security        : Enabled
Port Status          : Secure-up
Violation Mode       : Shutdown
Aging Time           : 0 mins
```

```
Aging Type           : Absolute
SecureStatic Address Aging  : Disabled
Maximum MAC Addresses       : 1
Total MAC Addresses         : 1
Configured MAC Addresses    : 0
Sticky MAC Addresses        : 1
Last Source Address:Vlan    : 0017.5a78.be01:1
Security Violation Count    : 0
```

Действие 20 Введите команду **show mac-address dynamic int fa0/1**, чтобы вывести только динамические записи таблицы MAC-адресов интерфейса fa0/1. Команда не должна вернуть записи, поскольку они преобразованы в статические (закрепленные) записи. Вывод на экран должен выглядеть следующим образом.

```
SwitchX#show mac-address dynamic int fa0/1
     Mac Address Table
-------------------------------------------
Vlan  Mac Address     Type      Ports
----  -----------     --------  -----
```

Действие 21 Используйте команду **ping**, чтобы спровоцировать нарушение безопасности, **ping 10.*x*.*x*.100**. Вывод на экран должен выглядеть следующим образом.

```
23:07:41: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/1,
putting Fa0/1 in err-disable state
23:07:41: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred,
caused by MAC address 001a.2fe7.3089 on port FastEthernet0/1.
23:07:42: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down.
23:07:43: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down....
Success rate is 0 percent (0/5)
SwitchX#
```

Действие 22 Введите команду **show port-security interface fa0/1** для отображения текущих параметров безопасности порта.

```
SwitchX#show port-security int fa0/1
Port Security               : Enabled
Port Status                 : Secure-shutdown
Violation Mode              : Shutdown
Aging Time                  : 0 mins
Aging Type                  : Absolute
SecureStatic Address Aging  : Disabled
Maximum MAC Addresses       : 1
Total MAC Addresses         : 1
Configured MAC Addresses    : 0
Sticky MAC Addresses        : 1
Last Source Address:Vlan    : 001a.2fe7.3089:1
Security Violation Count    : 1
```

Действие 23 Теперь необходимо изменить максимальное число допустимых MAC-адресов на 2. Также следует изменить действие, предпринимаемое в случае нарушения, на «restrict» (ограничить), а затем изменить для состояние интерфейса с «error disable» на «error disable».

Действие 24 Перед изменением параметров безопасности порта рекомендуется очистить записи таблицы MAC-адресов.

Действие 25 Введите команду **clear port-security sticky int fa0/1 access**. Примечание. Ограничив действие команды «clear» текущим портом, можно избежать риска случайного влияния на другие интерфейсы.

Действие 26 Введите команду **configure t**.

Действие 27 Введите команду **int fa0/1**.

Действие 28 Введите команду **switchport port-security maximum 2**.

Действие 29 Введите команду **switchport port-security violation restrict**. Если в случае нарушения применяется действие «restrict», вместо отключения интерфейса система блокирует кадры, создает локальное сообщение и увеличивает счетчик нарушений безопасности на 1. Это действие предназначено для сред с низким уровнем безопасности.

Действие 30 Чтобы перевести интерфейс из состояния «error disable» в «administratively up», необходимо сначала ввести команду **shutdown**, а затем команду **no shutdown**.

Действие 31 Введите команду **end** для выхода из режима конфигурации и возврата к приглашению привилегированного режима (enable EXEC).

Действие 32 Подождите 20 секунд и проверьте конфигурацию с помощью команды **ping** для 10.*x.x.*100.

Действие 33 Ниже приведен пример вывода команды **show running-config int fa0/1**. Ваши вывод должен быть аналогичен.

```
SwitchX#show running-config int fa0/1
Building configuration...

Current configuration : 329 bytes
!
interface FastEthernet0/1
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0017.5a78.be01
 switchport port-security mac-address sticky 001a.2fe7.3089
end
```

Действие 34 Ниже приводится пример вывода команды **show port-security int fa0/1**.

```
SwitchX#show port-security int fa0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 2
Last Source Address:Vlan   : 001a.2fe7.3089:1
Security Violation Count   : 0
```

Действие 35 Сравните выделенный жирным шрифтом текст с выводом действия 22, чтобы убедиться, что порт включен и в случае нарушения вместо режима Shutdown используется режим Restrict.

Действие 36 Сохраните текущую конфигурацию в файле startup-config.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- для коммутатора настроено разрешение одного динамически полученного MAC-адреса на первом порте доступа (fa0/1);
- инициировано нарушение безопасности порта, которое привело к переводу порта в состояние «error disabled»;
- конфигурация изменена для поддержки двух динамически полученных адресов, действие при нарушении изменено с «shutdown» на «restrict» для ограничения доступа вместо отключения порта;
- состояние порта «error disable» изменено на «administratively up»;
- порт был повторно проверен на отсутствие нарушения безопасности;
- текущая конфигурация сохранена в файле startup-config.

Задача 6: Отключение неиспользуемых портов и перевод всех портов в режим доступа

В этой задаче вам необходимо отключить все неиспользуемые порты. Кроме того, следует перевести все порты коммутатора из режима автосогласования в режим доступа. Это действие позволяет повысить устойчивость коммутатора к атакам с устройств с прямым подключением к коммутатору. В этой задаче предполагается, что не используются следующие порты: с Fa0/3 по Fa0/10, с Fa0/13 по fa0/24 и с Gi0/1 по Gi0/2.

Процедура упражнения

Выполните следующие действия:

Действие 1 В приглашении привилегированного режима (enable EXEC) введите команду для доступа к приглашению глобальной конфигурации.

Действие 2 Введите команду **interface range fa0/3 – 10.** Все следующие команды будут применяться к указанным портам.

Действие 3 Введите команду **shutdown**.

Действие 4 Введите команду **interface range fa0/13 – 24**, чтобы заменить предыдущий диапазон.

Действие 5 Введите команду **shutdown**.

Действие 6 Введите команду **interface range gi0/1 – 2**, чтобы заменить предыдущий диапазон.

Действие 7 Введите команду **shutdown**.

Действие 8 Вернитесь к приглашению привилегированного режима (enable EXEC).

Действие 9 Введите команду для вывода текущей конфигурации, чтобы убедиться, что отключены только указанные интерфейсы.

Действие 10 Введите команду для доступа к приглашению глобальной конфигурации.

Действие 11 Введите команду **interface range fa0/1 – 24, gi0/1 – 2**, чтобы включить в диапазон все порты. Обратите внимание, что в этом примере диапазоны интерфейсов группируются в одной команде с помощью разделителя (запятая).

Действие 12 Введите команду **switchport mode access**.

Действие 13 Вернитесь к приглашению привилегированного режима (enable EXEC).

Действие 14 Введите команду для вывода текущей конфигурации, чтобы убедиться, что все интерфейсы переведены в режим доступа.

Действие 15 После того, как вы убедитесь, что для всех портов используется режим доступа и все порты, за исключением fa0/1, fa0/2, fa0/11 и fa0/12 отключены, сохраните текущую конфигурацию в файле startup-config.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- настроен заданный диапазон неиспользуемых портов для отключения;
- всех порты в конфигурации переведены в режим доступа;
- текущая конфигурация сохранена в файле startup-config.

Лабораторная работа 2-4: Эксплуатация и настройка устройства Cisco IOS

Выполните упражнение этой лабораторной работы, чтобы применить на практике знания, полученные в соответствующем модуле.

Задачи упражнения

В этом упражнении вы ознакомитесь с функциями интерфейса командной строки коммутатора рабочей группы и попрактикуетесь в их использовании. После выполнения этого упражнения вы будете способны сделать следующее:

- использовать контекстную справку;
- исправить неправильно введенные команды интерфейса командной строки на коммутаторе;
- определить состояние коммутатора с помощью команд **show**.

Иллюстрация задания

На рисунке ниже показано, что вы должны сделать во время данного упражнения.

Необходимые ресурсы

Ниже перечислены ресурсы и устройства, необходимые для выполнения упражнения.

- ПК, подключенный к удаленной лаборатории.
- Приложение для эмуляции терминала с поддержкой SSH.
- Информация о назначенном комплекте оборудования, полученная в лабораторной работы 2-1.

Список команд

В таблице приводится описание команд, используемых в упражнении.

Команды коммутатора Cisco IOS

Команда	Описание
? или **help**	Выводит список доступных команд в пользовательском режиме Cisco IOS. После ввода команды **enable** и пароля «enable password» для входа в привилегированный режим список доступных команд значительно увеличивается.
clock set	Управляет системными часами.
configure terminal	Активирует режим конфигурации с терминала.
enable	Активирует привилегированный режим. В привилегированном режиме доступно большее количество команд. Эта команда требует ввода пароля доступа (enable password), если он настроен. Если пароль «enable secret» также настроен, он переопределяет пароль enable password.
exec time-out	Задает допустимое время бездействия перед автоматическим завершением сеанса.
history size	Задает количество строк, сохраняемых в буфере журнала для повторного вызова. Используется два отдельных буфера – один для команд режима EXEC и другой для команд режима конфигурации.
[**no**] **ip domain-lookup**	По умолчанию интерпретатор командной строки пытается обработать команду, которую не удается распознать, как символьное имя IP-адреса. Форма **no** этой команды отключает это действие по умолчанию и позволяет таким образом ускорить интерпретацию ошибочных записей.
line console 0	Активирует режим конфигурации консольной линии 0.
line vty 0 15	Активирует режим конфигурации линий виртуального терминала. Линии виртуального терминала (VTY) позволяют получать доступ к коммутатору для удаленного управления сетью. Доступное количество линий VTY зависит от версии ПО Cisco IOS. Обычно используются значения 0-4 и 0-15 (включительно).
logging synchronous	Синхронизирует вывод незапрошенных сообщений и команды отладки привилегированного режима EXEC с запрошенным выводом устройства и приглашениями конкретной линии консольного порта или линии VTY.
show clock	Выводит системные часы.
show history	Выводит недавно введенные команды.

Команда	Описание
show interfaces	Выводит информацию обо всех интерфейсах маршрутизатора.
show running-config	Выводит активную конфигурацию.
show terminal	Выводит текущие параметры для терминала.
show version	Выводит конфигурацию аппаратного обеспечения маршрутизатора и различных версий программного обеспечения.
terminal history size	Задает размер буфера истории команд.

Подсказки

Для этого упражнения доступны следующие подсказки.

Текущие пароли

Вход в консоль коммутатора	sanjose
Пароль «enable password» коммутатора	cisco
Пароль «enable secret» коммутатора	sanfran
Идентификатор пользователя для входа в систему коммутатора через линию VTY	netadmin
Пароль для входа в коммутатор через линию VTY	netadmin

Задача 1: Использование контекстной справки

В этой задаче вы должны использовать контекстную справку в пользовательском и привилегированном режимах EXEC для поиска команд и завершения синтаксиса команд.

Процедура упражнения

Выполните следующие действия:

Действие 1 Подключитесь к коммутатору рабочей группы, используя сведения из лабораторной работы 2-1.

Действие 2 Введите команду help (**?**). В приглашении пользовательского режима EXEC - должен отобразиться список доступных команд. Вывод должен выглядеть следующим образом.

```
Exec commands:
 access-enable  Create a temporary Access-List entry
 clear          Reset functions
 connect        Open a terminal connection
..
..Text omitted
..
 set            Set system parameter (not config)
 show           Show running system information
 ssh            Open a secure shell client connection
 systat         Display information about terminal lines
 telnet         Open a telnet connection
 --More--
```

Действие 3 Нажмите клавишу **ПРОБЕЛ** для завершения или продолжения списка.

Действие 4 Войдите в привилегированный режим EXEC.

Действие 5 Обратите внимание, что приглашение изменилось – вместо пользовательского режима коммутатора «>» теперь используется привилегированный режим «#».

Действие 6 Введите команду help (**?**) в приглашении привилегированного режима EXEC. Используйте справку для поиска команды, управляющей системными часами, по ключевому слову.

Действие 7 На консоли должно отображаться приглашение «--More--». Это значит, что она ожидает нажатия клавиши перед отображением дополнительных выходных данных. Введите **q**, чтобы отказаться от продолжения вывода данных.

Действие 8 Введите команду **clock ?**. Должна появиться контекстная справка. Вывод должен выглядеть следующим образом.

```
SwitchX#clock ?
 set Set the time and date
```

Действие 9 Задайте текущее время и дату для системных часов. Используйте контекстную справку для получения инструкций для этого процесса.

Действие 10 В приглашении switch# введите **sh?**. Должен появиться другой пример контекстной справки. Вывод будет выглядеть следующим образом.

```
SwitchX#sh?
show
```

Действие 11 Нажмите клавишу **Tab**. Функция автоматического завершения ввода команды должна вступить в действие. Когда введено достаточное количество букв команды или ключевое слово, после нажатия клавиши Tab автоматически вводится оставшаяся часть слова и ставится пробел, что позволяет ввести дополнительные данные.

Действие 12 Введите команду **show clock**. В выходных данных должны отразиться изменения, сделанные с помощью команды **clock set** во время действия 9. Вывод должен выглядеть следующим образом.

```
SwitchX#show clock
10:45:25.073 UTC Tue Jul 10 2007
```

Проверка упражнения

Задание считается выполненным, если достигнут следующий результат:

- вы использовали контекстную справку системы и модуль автоматического завершения ввода команд.

Задача 2: Изменение неправильно введенной команды

В этой задаче вы должны использовать расширенные функции редактирования ПО Cisco IOS для исправления ошибок в командной строке.

Процедура упражнения

Выполните следующие действия:

Действие 1 Введите в приглашении следующую строку комментария: **«This command changes the clock speed for the router»**. Текст следует вводить без кавычек (").

```
SwitchX#This command changes the clock speed for the router.
         ^
% Invalid input detected at '^' marker.
```

Действие 2 Введите следующую строку комментария после восклицательного знака (!): **!ths comand changuw the clck sped for the swch,**. Восклицательный знак (!) перед строкой текста указывает на ввод комментария.

```
SwitchX#!ths comand changuw the clck sped for the swch,
```

Действие 3 Введите **Ctrl-P** или нажмите **Стрелку вверх** для просмотра предыдущей строки.

Действие 4 Используйте команды редактора **Ctrl-A**, **Ctrl-F**, **Ctrl-E** и **Ctrl-B** для перемещения по строке и клавишу **Backspace** для удаления ненужных символов.

Действие 5 Используя команды редактирования, измените строку комментария на **!This command changes the clock speed for the switch**.

Проверка упражнения

Задание считается выполненным, если достигнут следующий результат:

- вы использовали встроенный редактор и соответствующие клавиши для перемещения курсора.

Задача 3: Оптимизация использования CLI

В этой задаче вам следует ввести команды для оптимизации использования интерфейса командной строки (CLI). Необходимо увеличить число строк в буфере журнала, увеличить значение таймера бездействия порта консоли и запретить разрешение имен при неверном вводе команд.

Процедура упражнения

Выполните следующие действия:

Действие 1 Введите команду **show terminal**. Вывод должен выглядеть следующим образом. В этом примере некоторые ненужные строки были удалены.

```
SwitchX#sh terminal
Line 0, Location: "", Type: ""
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 9600/9600, no parity, 2 stopbits, 8 databits
..
..Text omitted
..
Editing is enabled.
History is enabled, history size is 10.
DNS resolution in show commands is enabled
Full user help is disabled
```



```
Allowed input transports are none.
Allowed output transports are telnet ssh.
Preferred transport is telnet.
No output characters are padded
No special data dispatching characters
```

Действие 2 Размер буфера журнала равен 10. Это значение можно изменить с помощью команды **terminal history size 100**. Однако его необходимо вводить после каждого выхода и повторного входа в систему коммутатора. Размер журнала можно задать в конфигурации консоли и линий VTY.

Действие 3 Введите команду **config t**, чтобы перейти к приглашению глобальной конфигурации.

Действие 4 Введите команду **line console 0**.

Действие 5 Введите команду **history size 100**.

Действие 6 В режиме консольной линии рекомендуется увеличить значение таймаута EXEC с 15 до 60 минут. Введите команду **exec-timeout 60**.

Действие 7 Введите команду **logging synchronous** для синхронизации вывода незапрошенных сообщений и вывода команды отладки привилегированного режима EXEC с вводом из CLI.

Действие 8 Введите команду **line vty 0 15** для настройки линий VTY.

Действие 9 Введите команды для установки значения 100 для буфера журнала и включения синхронизации сообщений.

Действие 10 Введите команду **exit** для возврата в режим глобальной конфигурации.

Действие 11 Введите команду **no ip domain-lookup**, чтобы отключить разрешение символьных имен.

Действие 12 Вернитесь к приглашению привилегированного режима (enable EXEC).

Действие 13 Используйте повторный вызов журнала для ввода команды **show terminal**. Вывод должен выглядеть следующим образом. В этом примере некоторые ненужные строки были удалены.

```
SwitchX#sh term
Line 0, Location: "", Type: ""
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 9600/9600, no parity, 2 stopbits, 8 databits
..
..Text omitted
..
Editing is enabled.
History is enabled, history size is 100.
DNS resolution in show commands is enabled
Full user help is disabled
Allowed input transports are none.
Allowed output transports are telnet ssh.
Preferred transport is telnet.
No output characters are padded
No special data dispatching characters
```

Действие 14 Введите команду **show running-config**, чтобы убедиться в правильности изменений конфигурации.

Действие 15 Убедитесь, что в текущей конфигурации отражены изменения, и сохраните ее в файле startup-config.

Действие 16 Закройте соединения с коммутатором рабочей группы.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- для таймаута бездействия порта консоли задано значение 60 минут;
- вы подтвердили, что для размер буфера журнала имеет значение 100 строк для линий VTY и консоли;
- вы подтвердили, что для линий VTY и консоли настроена функция logging synchronous;
- конфигурация сохранена в файле startup-config;
- все открытые соединения с коммутатором рабочей группы закрыты.

Лабораторная работа 4-1: Преобразование десятичных чисел в двоичные и двоичных в десятичные.

Выполните упражнение этой лабораторной работы, чтобы применить на практике знания, полученные в соответствующем модуле.

Задачи упражнения

В этом упражнении вы займетесь преобразованием десятичных и двоичных чисел. После выполнения этого упражнения вы будете способны сделать следующее:

- преобразовать десятичные числа в двоичные;
- преобразовать двоичные числа в десятичные.

Иллюстрация задания

На рисунке ниже показано, что вы должны сделать во время данного упражнения.

Необходимые ресурсы

Для этого упражнения лабораторной работы не требуется никаких ресурсов.

Список команд

В этом упражнении команды не используются.

Подсказки

Для этой лабораторной работы нет подсказок.

Подготовка к выполнению упражнения

Для этого упражнения подготовки не требуется.

Задача 1: Преобразование десятичных чисел в двоичный формат

Процедура упражнения

Заполните следующую таблицу, чтобы попрактиковаться в преобразовании десятичных чисел в двоичные.

Основание 2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Десятичное число	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Двоичное число**
48	0	0	1	1	0	0	0	0	48 = 32 + 16 = 00110000
146	1	0	0	1					
222									
119									
135									
60									

Задача 2: Преобразование двоичных чисел в десятичный формат

Процедура упражнения

Заполните следующую таблицу, чтобы попрактиковаться в преобразовании двоичные чисел в десятичные.

Основание 2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Двоичное число	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Десятичное число**
11001100	1	1	0	0	1	1	0	0	128 + 64 + 8 + 4 = 204
10101010	1	0	1	0					
11100011									
10110011									
00110101									
10010111									

Проверка упражнения

Лабораторная работа считается выполненной, если достигнуты следующие результаты:

- числа в десятичном формате правильно преобразованы в двоичное представление;
- числа в двоичном формате правильно преобразованы в десятичное представление.

Лабораторная работа 4-2: Классификация способов сетевой адресации

Выполните упражнение этой лабораторной работы, чтобы применить на практике знания, полученные в соответствующем модуле.

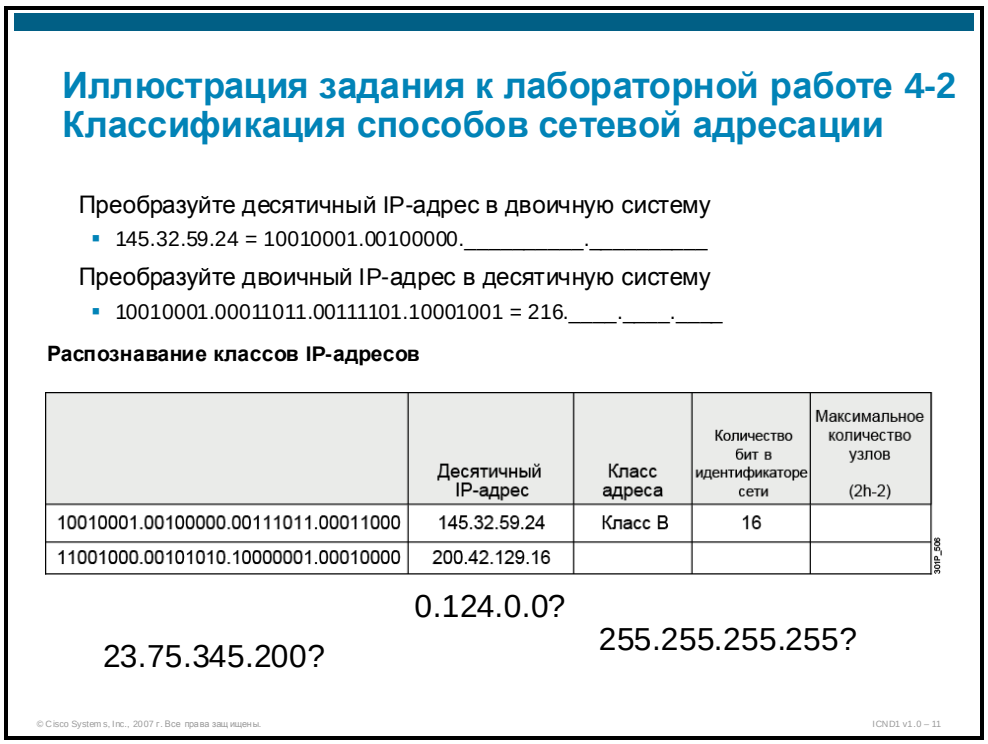
Задачи упражнения

В этом упражнении классифицировать сетевые адреса IPv4. После выполнения этого упражнения вы будете способны сделать следующее:

- преобразовывать десятичные IP-адреса в двоичные числа;
- преобразовывать двоичные числа в IP-адреса;
- определять классы IP-адресов;
- распознавать допустимые и недопустимые IP-адреса хостов.

Иллюстрация задания

На рисунке ниже показано, что вы должны сделать во время данного упражнения.



Необходимые ресурсы

Для этого упражнения лабораторной работы не требуется никаких ресурсов.

Список команд

В этом упражнении команды не используются.

Подсказки

Для этой лабораторной работы нет подсказок.

Подготовка к выполнению упражнения

Для этого упражнения подготовки не требуется.

Задача 1: Преобразование IP-адреса в десятичном формате в двоичный формат

Процедура упражнения

Выполните следующие действия.

Действие 1 Заполните следующую таблицу, чтобы представить адрес 145.32.59.24 в двоичном формате.

Основание 2	**2^7**	**2^6**	**2^5**	**2^4**	**2^3**	**2^2**	**2^1**	**2^0**	
Десятичное число	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Двоичное число**
145	1	0	0	1	0	0	0	1	10010001
32	0	0	1	0	0	0	0	0	00100000
59									
24									

IP-адрес в двоичном формате	10010001. 00100000. _____ . _____

Действие 2 Заполните следующую таблицу, чтобы представить адрес 200.42.129.16 в двоичном формате.

Основание 2	**2^7**	**2^6**	**2^5**	**2^4**	**2^3**	**2^2**	**2^1**	**2^0**	
Десятичное число	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Двоичное число**
200									
42									
129									
16									

IP-адрес в двоичном формате	

Действие 3 Заполните следующую таблицу, чтобы представить адрес 14.82.19.54 в двоичном формате.

Основание 2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Десятичное число	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Двоичное число**
14									
82									
19									
54									
IP-адрес в двоичном формате									

Задача 2: Преобразование IP-адреса в двоичном формате в десятичный формат

Процедура упражнения

Выполните следующие действия:

Действие 1 Заполните следующую таблицу, чтобы представить IP-адрес 11011000.00011011.00111101.10001001 в десятичном формате.

Основание 2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Двоичное число	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Десятичное число**
11011000	1	1	0	1	1	0	0	0	216
00011011									
00111101									
10001001									
IP-адрес в десятичном формате									216. _____ . _____ . _____

Действие 2 Заполните следующую таблицу, чтобы представить IP-адрес 11000110.00110101.10010011.00101101 в десятичном формате.

Основание 2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Двоичное число	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Десятичное число**
11000110									
00110101									
10010011									
00101101									
IP-адрес в десятичном формате									

Действие 3 Заполните следующую таблицу, чтобы представить IP-адрес 01111011.00101101.01000011.01011001 в десятичном формате.

Основание 2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Двоичное число	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Десятичное число**
01111011									
00101101									
01000011									
01011001									
IP-адрес в десятичном формате									

Задача 3: Распознавание классов IP-адресов

Процедура упражнения

Заполните эту таблицу, чтобы указать класс адреса, число бит в идентификаторе сети и максимальное число хостов.

Двоичный IP-адрес	Десятичный IP-адрес	Класс адреса	Число бит в идентификаторе сети	Максимальное число хостов ($2^h - 2$)
10010001.00100000.00111011.00011000	145.32.59.24	Класс B	16	
11001000.00101010.10000001.00010000	200.42.129.16			
00001110.01010010.00010011.00110110	14.82.19.54			
11011000.00011011.00111101.10001001	216.27.61.137			
10110011.00101101.01000011.01011001	179.45.67.89			
11000110.00110101.10010011.00101101	198.53.147.45			

Задача 4: Распознавание допустимых и недопустимых IP-адресов хостов

Процедура упражнения

В таблице ниже укажите, какие IP-адреса хостов являются допустимыми, а какие недопустимыми.

Десятичный IP-адрес	Допустимый или недопустимый	Если адрес недопустимый, укажите причину
23.75.345.200		
216.27.61.134		
102.54.94		
255.255.255.255		
142.179.148.200		
200.42.129.16		
0.124.0.0		

Проверка упражнения

Лабораторная работа считается выполненной, если достигнуты следующие результаты:

- IP-адреса в десятичном формате правильно преобразованы в двоичный формат;
- IP-адреса в двоичном формате правильно преобразованы в десятичный формат;
- правильно распознан класс указанного IP-адреса;
- правильно распознаны допустимые и недопустимые IP-адреса.

Лабораторная работа 4-3: Расчет доступных подсетей и хостов

Выполните упражнение этой лабораторной работы, чтобы применить на практике знания, полученные в соответствующем модуле.

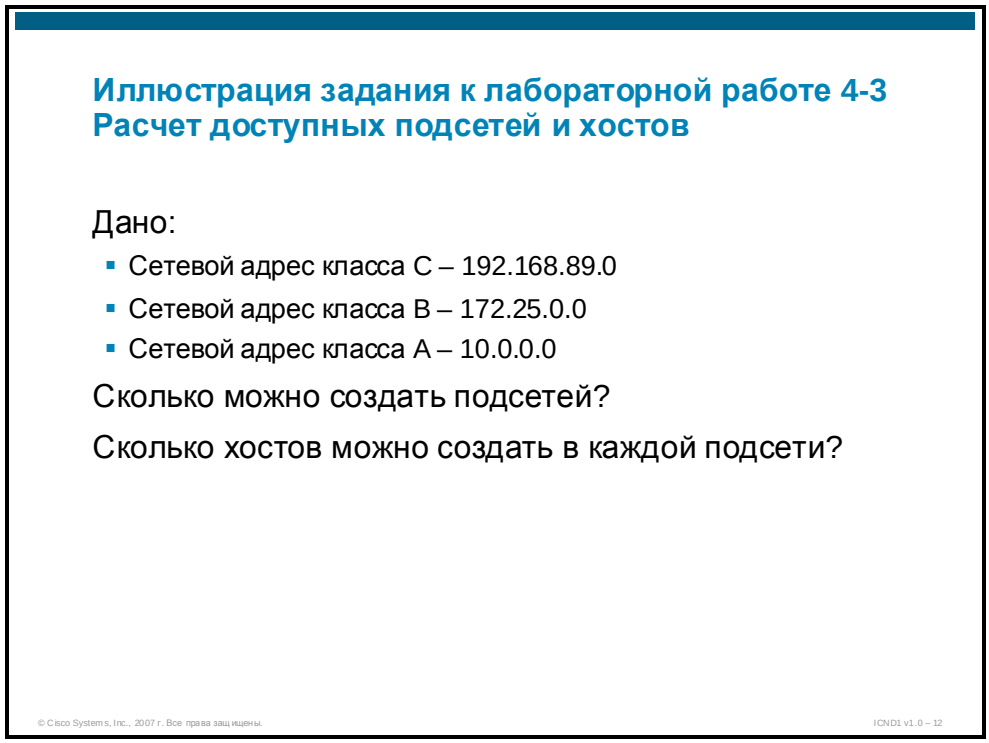
Задачи упражнения

В этом упражнении вам необходимо определить число бит, которое должно заимствоваться из идентификатора хоста для создания необходимого числа подсетей для данного IP-адреса. После выполнения этого упражнения вы будете способны сделать следующее:

- определить количество бит, которое необходимо для создания различных подсетей;
- определить максимальное количество адресов хостов, доступных в данной подсети.

Иллюстрация задания

На рисунке ниже показано, что вы должны сделать во время данного упражнения.



Необходимые ресурсы

Для этого упражнения лабораторной работы не требуется никаких ресурсов.

Список команд

В этом упражнении команды не используются.

Подсказки

Для этой лабораторной работы нет подсказок.

Подготовка к выполнению упражнения

Для этого упражнения подготовки не требуется.

Задача 1: Определение количества бит, необходимых для создания подсетей сети класса C

Процедура упражнения

Используя адрес сети класса C 192.168.89.0, заполните таблицу, чтобы определить количество бит, которые необходимы для создания указанного числа подсетей для данной сети, а затем определите количество хостов для каждой подсети.

Количество подсетей	Количество заимствованных бит	Количество хостов для подсети ($2^h - 2$)
2		
5		
12		
24		
40		

Задача 2: Определение количества бит, необходимых для создания подсетей сети класса B

Процедура упражнения

Используя адрес сети класса B 172.25.0.0, заполните таблицу, чтобы определить количество бит, которые необходимы для создания указанного числа подсетей для данной сети, а затем определите количество хостов для каждой подсети.

Количество подсетей	Количество заимствованных бит	Количество хостов для подсети ($2^h - 2$)
5		
8		
14		
20		
35		

Задача 3: Определение количества бит, необходимых для создания подсетей сети класса A

Процедура упражнения

Используя адрес сети класса A 10.0.0.0, заполните таблицу, чтобы определить количество бит, которые необходимы для создания указанного числа подсетей для данной сети, а затем определите количество хостов для каждой подсети.

Количество подсетей	Количество заимствованных бит	Количество хостов для подсети ($2^h - 2$)
10		
14		
20		
40		
80		

Проверка упражнения

Лабораторная работа считается выполненной, если получены следующие результаты:

- для сети класса A, B или C определено количество бит, необходимых для создания заданного числа подсетей;
- для сети класса A, B или C определено количество хостов в сети, исходя из известного количества подсетей и количества заимствованных битов.

Лабораторная работа 4-4: Вычисление масок подсети

Выполните упражнение этой лабораторной работы, чтобы применить на практике знания, полученные в соответствующем модуле.

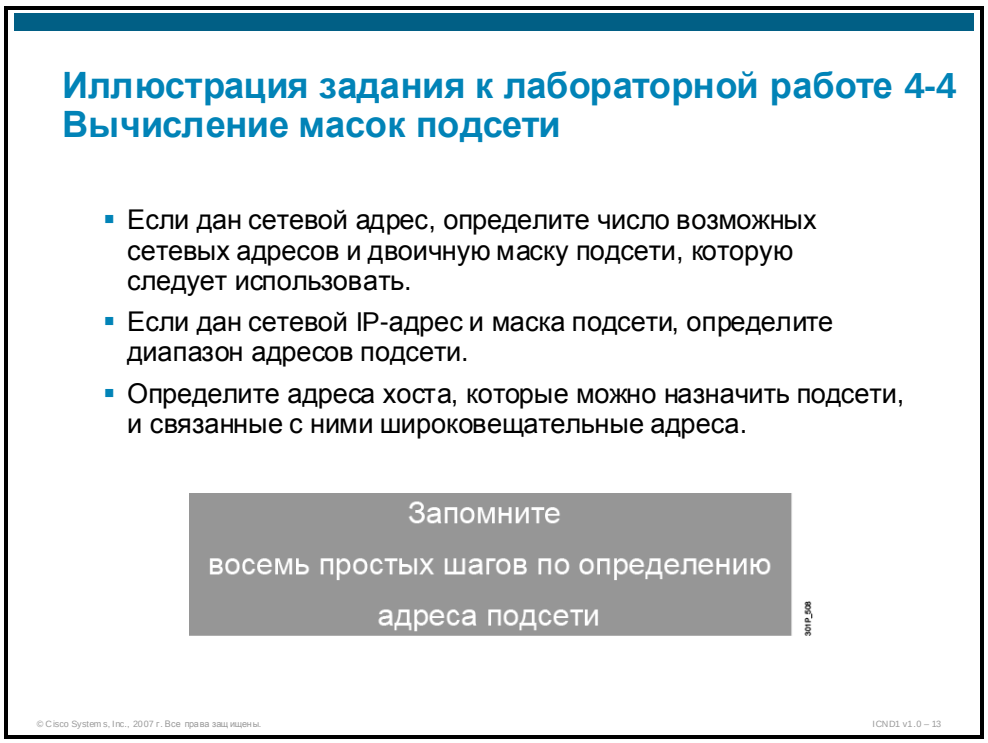
Задачи упражнения

В этом упражнении вы займетесь вычислением масок подсети. После выполнения этого упражнения вы будете способны сделать следующее:

- зная сетевой адрес, определять количество возможных сетевых адресов и двоичную маску подсети, которую следует использовать;
- зная сетевой IP-адрес и маску подсети, определять диапазон адресов подсети;
- определять адреса хостов, которые можно назначить подсети, и связанные с ними широковещательные адреса.

Иллюстрация задания

На рисунке ниже показано, что вы должны сделать во время данного упражнения.



Необходимые ресурсы

Для этого упражнения лабораторной работы не требуется никаких ресурсов.

Список команд

В этом упражнении команды не используются.

Подсказки

Для этой лабораторной работы нет подсказок.

Подготовка к выполнению упражнения

Для этого упражнения подготовки не требуется.

Задача 1: Определение количества доступных сетевых адресов

Процедура упражнения

Для сети класса A на основе указанного числа бит сети заполните следующую таблицу, чтобы определить маску подсети и количество возможных адресов хостов для каждой маски.

Классовый адрес	Десятичная маска подсети	Двоичная маска подсети	Количество хостов для подсети ($2^h - 2$)
/20			
/21			
/22			
/23			
/24			
/25			
/26			
/27			
/28			
/29			
/30			

Задача 2: Определение подсетей для сетевого адреса

Процедура упражнения

Предположим, что вам выделена сеть 172.25.0.0 /16. Необходимо создать двенадцать подсетей. Ответьте на следующие вопросы.

1. Сколько бит потребуется позаимствовать для задания 12 подсетей?

   _____

2. Укажите классовый адрес и маску подсети в двоичном и десятичном формате, которые позволят создать 12 подсетей.

   _____

3. Используйте метод, включающий восемь действий, чтобы задать 12 подсетей.

Действие	Описание	Пример
1.	Укажите разделяемый октет в двоичном формате.	
2.	Укажите маску или длину классового префикса в двоичном формате.	
3.	Отделите линией значимые биты в назначенном IP-адресе. Разделите линией маску, чтобы выделить значимые биты IP-адреса.	
4.	Скопируйте значимые биты четыре раза.	
5.	В первой строке укажите сетевой адрес, поставив 0 в оставшиеся биты хоста.	
6.	В последней строке укажите широковещательный адрес, поставив 1 в битах хоста.	
7.	В средних строках укажите идентификатор первого и последнего хостов подсети.	
8.	Чтобы определить следующий адрес подсети, увеличивайте биты подсети на единицу. Повторите шаги с 4 по 8 для всех подсетей.	

4. Заполните следующую таблицу, чтобы задать каждую из подсетей.

Номер подсети	Адрес подсети	Диапазон адресов хостов	Широковещательный адрес
0			
1			
2			
3			
4			
5			
6			
7			
. . .			

Задача 3: Определение подсетей на основе другого сетевого адреса

Процедура упражнения

Предположим, что вам выделена сеть 192.168.1.0 /24.

1. Сколько бит потребуется позаимствовать для задания 6 подсетей?

_____

2. Укажите классовый адрес и маску подсети в двоичном и десятичном формате, которые позволят создать 6 подсетей.

_____

3. Используйте метод, включающий восемь действий, чтобы задать 6 подсетей.

Действие	Описание	Пример
1.	Укажите разделяемый октет в двоичном формате.	
2.	Укажите маску или длину классового префикса в двоичном формате.	
3.	Отделите линией значимые биты в назначенном IP-адресе. Разделите линией маску, чтобы выделить значимые биты IP-адреса.	
4.	Скопируйте значимые биты четыре раза.	
5.	В первой строке укажите сетевой адрес, поставив 0 в оставшиеся биты хоста.	
6.	В последней строке укажите широковещательный адрес, поставив 1 в битах хоста.	
7.	В средних строках укажите идентификатор первого и последнего хостов подсети.	
8.	Чтобы определить следующий адрес подсети, увеличивайте биты подсети на единицу. Повторите шаги с 4 по 8 для всех подсетей.	

4. Заполните следующую таблицу, чтобы задать каждую из подсетей.

Номер подсети	Адрес подсети	Диапазон адресов хостов	Широковещательный адрес
0			
1			
2			
3			
4			
5			
6			
7			

Задача 4: Определение подсетей на основе заданного сетевого адреса и классового адреса

Процедура упражнения

Предположим, что вам выделен адрес 192.168.111.129 в сетевом блоке /28.

1. Укажите маску подсети в двоичном и десятичном формате.

_____

2. Сколько подсетей можно задать для указанной маски?

_____

3. Сколько хостов будет в каждой подсети?

_____

4. Используйте метод, включающий восемь действий, чтобы задать подсет.

Действие	Описание	Пример
1.	Укажите разделяемый октет в двоичном формате.	
2.	Укажите маску или длину классового префикса в двоичном формате.	
3.	Отделите линией значимые биты в назначенном IP-адресе. Разделите линией маску, чтобы выделить значимые биты IP-адреса.	
4.	Скопируйте значимые биты четыре раза.	
5.	В первой строке укажите сетевой адрес, поставив 0 в оставшиеся биты хоста.	
6.	В последней строке укажите широковещательный адрес, поставив 1 в битах хоста.	
7.	В средних строках укажите идентификатор первого и последнего хостов подсети.	
8.	Чтобы определить следующий адрес подсети, увеличивайте биты подсети на единицу. Повторите шаги с 4 по 8 для всех подсетей.	

5. Заполните следующую таблицу, чтобы задать каждую из подсетей.

Номер подсети	Адрес подсети	Диапазон адресов хостов	Широковещательный адрес
0			
1			
2			
3			
4			
5			
6			
7			

Задача 5: Определение подсетей на основе заданного сетевого блока и классового адреса

Процедура упражнения

Предположим, что вам выделен адрес 172.25.112.0 в сетевом блоке /23.

1. Укажите маску подсети в двоичном и десятичном формате.

_____

2. Сколько подсетей можно создать для указанной маски?

_____

3. Сколько хостов будет в каждой подсети?

_____

4. Используйте метод, включающий восемь действий, чтобы создать подсеть.

Действие	Описание	Пример
1.	Укажите разделяемый октет в двоичном формате.	
2.	Укажите маску или длину классового префикса в двоичном формате.	
3.	Отделите линией значимые биты в назначенном IP-адресе. Разделите линией маску, чтобы выделить значимые биты IP-адреса.	
4.	Скопируйте значимые биты четыре раза.	
5.	В первой строке укажите сетевой адрес, поставив 0 в оставшиеся биты хоста.	
6.	В последней строке укажите широковещательный адрес, поставив 1 в битах хоста.	
7.	В средних строках укажите идентификатор первого и последнего хостов подсети.	
8.	Чтобы определить следующий адрес подсети, увеличивайте биты подсети на единицу. Повторите шаги с 4 по 8 для всех подсетей.	

5. Заполните следующую таблицу, чтобы задать каждую из подсетей.

Номер подсети	Адрес подсети	Диапазон адресов хостов	Широковещательный адрес
0			
1			
2			
3			
4			
5			
6			
7			

Задача 6: Определение подсетей на основе заданного сетевого блока и классового адреса

Процедура упражнения

Предположим, что вам выделен адрес 172.20.0.129 в сетевом блоке /25.

1. Укажите маску подсети в двоичном и десятичном формате.

_____

2. Сколько подсетей можно определить с указанной маской?

_____

3. Сколько хостов будет в каждой подсети?

_____

4. Используйте метод, включающий восемь действий, чтобы задать подсет.

Действие	Описание	Пример
1.	Укажите разделяемый октет в двоичном формате.	
2.	Укажите маску или длину классового префикса в двоичном формате.	
3.	Отделите линией значимые биты в назначенном IP-адресе. Разделите линией маску, чтобы выделить значимые биты IP-адреса.	
4.	Скопируйте значимые биты четыре раза.	
5.	В первой строке укажите сетевой адрес, поставив 0 в оставшиеся биты хоста.	
6.	В последней строке укажите широковещательный адрес, поставив 1 в битах хоста.	
7.	В средних строках укажите идентификатор первого и последнего хостов подсети.	
8.	Чтобы определить следующий адрес подсети, увеличивайте биты подсети на единицу. Повторите шаги с 4 по 8 для всех подсетей.	

5. Заполните следующую таблицу, чтобы создать подсети.

Номер подсети	Адрес подсети	Диапазон адресов хостов	Широковещательный адрес
0			
1			
2			
3			
4			
5			
6			
7			

Проверка упражнения

Лабораторная работа считается выполненной, если получены следующие результаты:

- на основе указанного сетевого адреса правильно определено количество доступных сетевых адресов и двоичная маска подсети, которую следует использовать;
- на основе сетевого IP-адреса и маски подсети правильно определен диапазон адресов подсети.

Вы можете применить маски подсети для определения адресов хостов, которые можно назначить подсети, и связанных с ними широковещательных адресов.

Лабораторная работа 4-5: Начальный запуск маршрутизатора

Выполните упражнение этой лабораторной работы, чтобы применить на практике знания, полученные в соответствующем модуле.

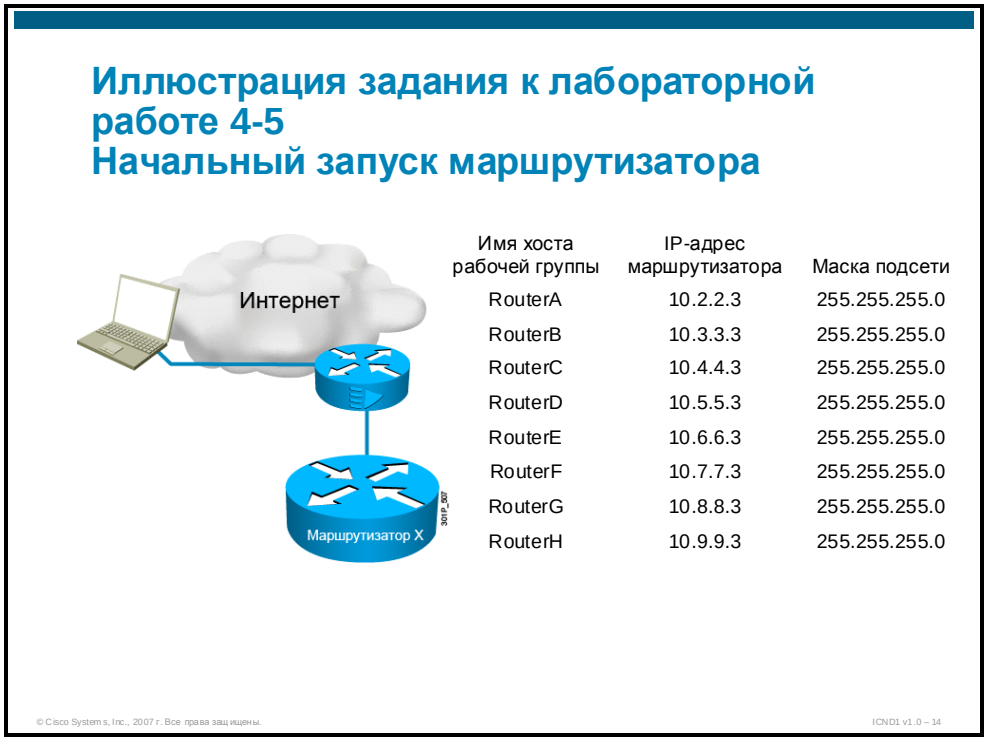
Задачи упражнения

В этом упражнении вам необходимо подключиться к удаленному маршрутизатору рабочей группы, убедиться в отсутствии конфигурации и проверить процесс запуска. После выполнения этого упражнения вы будете способны сделать следующее:

- удалить существующую конфигурацию маршрутизатора;
- перезапустить маршрутизатор и изучить данные вывода;
- отклонить запрос диалогового окна начальной конфигурации по окончании процесса перезапуска.

Иллюстрация задания

На рисунке ниже показано, что вы должны сделать во время данного упражнения.



Необходимые ресурсы

Ниже перечислены ресурсы и устройства, необходимые для выполнения упражнения.

- ПК, подключенный к удаленной лаборатории.
- Приложение для эмуляции терминала с поддержкой SSH.
- Информация о доступе к назначенному комплекту оборудования, полученная в лабораторной работе 2-1.

Список команд

В таблице приводится описание команд, используемых в упражнении.

Команды маршрутизатора Cisco IOS

Команда	Описание
enable	Вход в интерпретатор команд привилегированного режима EXEC.
erase startup-config	Удаление загрузочной конфигурации из памяти.
Reload	Перезагрузка маршрутизатора для применения изменений конфигурации.

Подсказки

Для этого упражнения доступны следующие подсказки.

Текущие пароли

Вход в консоль маршрутизатора	Нет
Пароль «enable password» маршрутизатора	Нет
Пароль «enable secret» маршрутизатора	Нет
Идентификатор пользователя для входа в систему маршрутизатора через линию VTY	Нет
Пароль для входа в систему маршрутизатора через линию VTY	Нет
Вход в консоль коммутатора	sanjose
Пароль «enable password» коммутатора	cisco
Пароль «enable secret» коммутатора	sanfran
Идентификатор пользователя для входа в систему коммутатора через линию VTY	netadmin
Пароль для входа в систему коммутатора через линию VTY	netadmin

Задача 1: Удаление существующей конфигурации маршрутизатора

В этой задаче вам необходимо запустить маршрутизатор рабочей группы и проверить, правильно ли он загружается. У маршрутизатора может быть конфигурация по умолчанию, которая поддерживает начальную настройку с помощью Cisco SDM (Router and Security Device Manager) и требует ввода имени пользователя **cisco** и пароля **cisco** для получения доступа к приглашению привилегированного режима (enable).

Процедура упражнения

Выполните следующие действия:

Действие 1 Подключитесь к маршрутизатору рабочей группы, используя сведения о доступе из лабораторной работы 2-1. См. также информацию об IP-адресе в иллюстрации задания.

Действие 2 При запросе имени пользователя и пароля введите **cisco** в обоих случаях. Если этого не происходит, перейдите к следующему действию.

Действие 3 Если после выполнения предыдущего действия вы не получили приглашение привилегированного режима, введите команду для получения доступа к нему.

Действие 4 Введите команду **erase startup-config** и подтвердите продолжение. Должны появиться следующие выходные данные.

```
Username: cisco
Password:
yourname#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
yourname#
*Apr 24 00:16:130.683: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
yourname#
```

Проверка упражнения

Задание считается выполненным, если достигнут следующий результат:

- удалена загрузочная конфигурация.

Задача 2: Перезагрузка маршрутизатора и анализ данных, отображаемых при запуске

В этой задаче вам следует проанализировать вывод маршрутизатора. Он должен быть аналогичен выводу, полученному при перезагрузке коммутатора рабочей группы.

Процедура упражнения

Выполните следующие действия:

Действие 1 Введите команду **reload**. Подтвердите запрос на продолжение перезагрузки, нажав клавишу ENTER. Вывод должен выглядеть следующим образом.

```
yourname#reload
Proceed with reload? [confirm]
.
```

Действие 2 Проанализируйте данные, отображаемые при перезагрузке. Вывод всех данных займет несколько минут, после чего появится финальное приглашение. Вывод должен выглядеть следующим образом. В этом примере некоторые строки были отредактированы для уменьшения объема данных.

```
*Apr 24 00:18:02.043: %SYS-5-RELOAD: Reload requested by cisco on console.
Reload Reason: Reload Command.

System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2006 by cisco Systems, Inc.
```

```
Initializing memory for ECC
.
c2811 platform with 262144 Kbytes of main memory
Main memory is configured to 64 bit mode with ECC enabled


Upgrade ROMMON initialized
program load complete, entry point: 0x8000f000, size: 0xcb80
program load complete, entry point: 0x8000f000, size: 0xcb80

program load complete, entry point: 0x8000f000, size: 0x228d9f8
Self decompressing the image :
################################################################################
########################################## [OK]

Smart Init is enabled
smart init is sizing iomem
 ID        MEMORY_REQ            TYPE
0003E7     0X003DA000 C2811 Mainboard
           0X00263F50 Onboard VPN
           0X000021B8 Onboard USB
           0X002C29F0 public buffer pools
           0X00211000 public particle pools
TOTAL:     0X00B13AF8

If any of the above Memory Requirements are
"UNKNOWN", you may be using an unsupported
configuration or there is a software problem and
system operation may be compromised.
Rounded IOMEM up to: 12Mb.
Using 4 percent iomem. [12Mb/256Mb]

       Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

      cisco Systems, Inc.
      170 West Tasman Drive
      San Jose, California 95134-1706


Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M),
Version 12.4(12), RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 17-Nov-06 12:02 by prod_rel_team
Image text-base: 0x40093160, data-base: 0x42B00000


This product contains cryptographic features and is subject to
United States and local country laws governing import, export, transfer
and use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
```



```
Cisco 2811 (revision 49.46) with 249856K/12288K bytes of memory.
Processor board ID FTX1108A3G8
2 FastEthernet interfaces
2 Low-speed serial(sync/async) interfaces
1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bits wide with parity enabled.
239K bytes of non-volatile configuration memory.
62720K bytes of ATA CompactFlash (Read/Write)


     --- System Configuration Dialog ---
```

Действие 3 Введите **no** в ответ на вопрос «Would you like to enter the initial configuration dialog». Дождитесь завершения вывода данных, затем нажмите клавишу **Enter**, чтобы получить приглашение.

```
Would you like to enter the initial configuration dialog? [yes/no]: no

Press RETURN to get started!

sslinit fn

*Apr 24 00:19:270,795: %VPN_HW-6-INFO_LOC: Crypto engine: onboard 0 State
changed to: Initialized
*Apr 24 00:19:270,799: %VPN_HW-6-INFO_LOC: Crypto engine: onboard 0 State
changed to: Enabled
*Apr 24 00:19:29.059: %LINEPROTO-5-UPDOWN: Line protocol on Interface VoIP-
Null0, changed state to up
*Apr 24 00:19:29.059: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state
to up
*Apr 24 00:19:29.063: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state
to up
*Apr 24 00:19:29.063: %LINK-3-UPDOWN: Interface Serial0/0/0, changed state to
down
*Apr 24 00:19:29.063: %LINK-3-UPDOWN: Interface Serial0/0/1, changed state to
down
*Apr 24 00:19:30.483: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to down
*Apr 24 00:19:30.483: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down
*Apr 24 00:19:30.483: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to down
*Apr 24 00:19:30.483: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to down
*Apr 24 00:19:32.295: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
*Apr 24 00:19:32.323: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
*Apr 24 00:29:25.479: %IP-5-WEBINST_KILL: Terminating DNS process
*Apr 24 00:29:26.659: %LINK-5-CHANGED: Interface FastEthernet0/0, changed
state to administratively down
*Apr 24 00:29:26.659: %LINK-5-CHANGED: Interface FastEthernet0/1, changed
state to administratively down
*Apr 24 00:29:26.659: %LINK-5-CHANGED: Interface Serial0/0/0, changed state
to administratively down
*Apr 24 00:29:26.659: %LINK-5-CHANGED: Interface Serial0/0/1, changed state
to administratively down
*Apr 24 00:29:26.991: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M),
Version 12.4(12), RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 17-Nov-06 12:02 by prod_rel_team
```

```
*Apr 24 00:29:26.995: %SNMP-5-COLDSTART: SNMP agent on host Router is
undergoing a cold start
*Apr 24 00:29:27.203: %SYS-6-BOOTTIME: Time taken to reboot after reload =
684 seconds
*Apr 24 00:29:27.383: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
*Apr 24 00:29:27.659: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to down
*Apr 24 00:29:27.659: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down
<ENTER>
Router>
```

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- выполнена перезагрузка маршрутизатора рабочей группы;
- отклонено диалоговое окно начальной конфигурации.

Лабораторная работа 4-6: Начальная настройка маршрутизатора

Выполните упражнение этой лабораторной работы, чтобы применить на практике знания, полученные в соответствующем модуле.

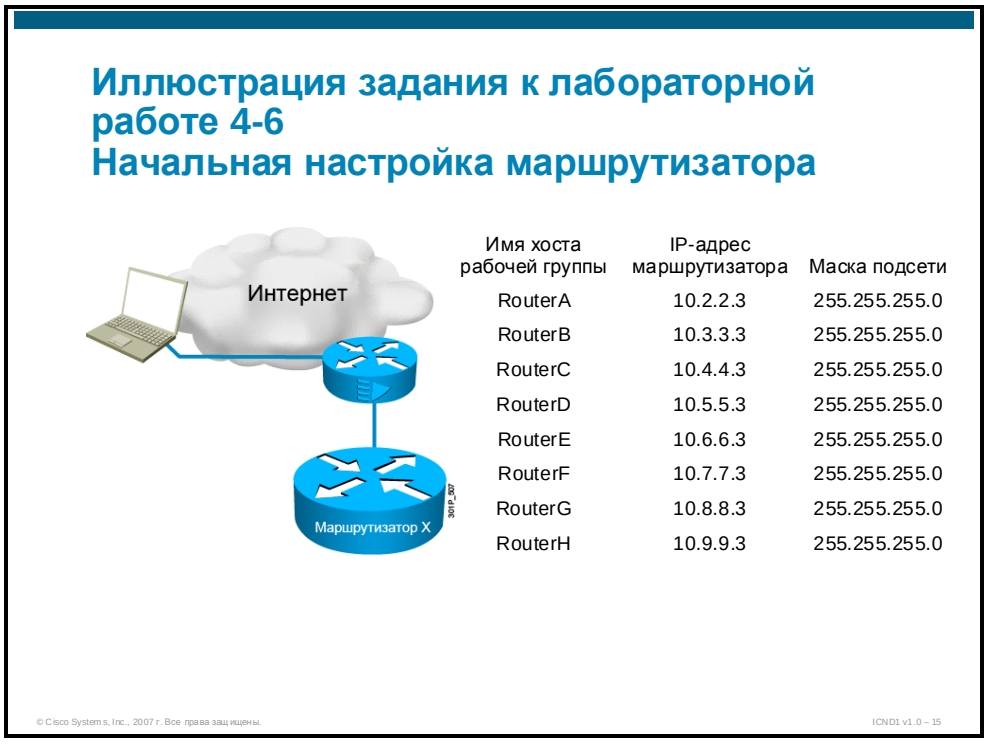
Задачи упражнения

В этом упражнении вам необходимо выполнить начальную минимальную настройку. После выполнения этого упражнения вы будете способны сделать следующее:

- использовать команду **setup**, чтобы активировать процесс настройки минимальной конфигурации для работы маршрутизатора;
- использовать команды **show** для проверки конфигурации.

Иллюстрация задания

На рисунке ниже показано, что вы должны сделать во время данного упражнения.



Необходимые ресурсы

Ниже перечислены ресурсы и устройства, необходимые для выполнения упражнения.

- ПК, подключенный к удаленной лаборатории.
- Приложение для эмуляции терминала с поддержкой SSH.
- Информация о доступе к назначенному комплекту оборудования, полученная в лабораторной работы 2-1.
- Успешное выполнение лабораторной работы 2-4.

Список команд

В таблице приводится описание команд, используемых в упражнении.

Команды маршрутизатора Cisco IOS

Команда	Описание
configure terminal	Активирует режим конфигурации с терминала.
setup	Активирует режим диалога начальной конфигурации.
show running-config	Выводит текущие параметры конфигурации маршрутизатора.
show startup-config	Отображает параметры загрузочной конфигурации, сохраненной в NVRAM.

Подсказки

Для этого упражнения доступны следующие подсказки.

Текущие пароли

Вход в консоль маршрутизатора	нет
Пароль «enable password» маршрутизатора	нет
Пароль «enable secret» маршрутизатора	нет
Идентификатор пользователя для входа в систему маршрутизатора через линию VTY	нет
Пароль для входа в систему маршрутизатора через линию VTY	нет
Вход в консоль коммутатора	sanjose
Пароль «enable password» коммутатора	cisco
Пароль «enable secret» коммутатора	sanfran
Идентификатор пользователя для входа в систему коммутатора через линию VTY	netadmin
Пароль для входа в систему коммутатора через линию VTY	netadmin

Задача 1: Ввод начальной конфигурации с помощью команды setup

В этой задаче вам необходимо использовать диалог начальной конфигурации для ввода базовой конфигурации маршрутизатора.

Процедура упражнения

Выполните следующие действия:

Действие 1 Если эта работа не является продолжением лабораторной работы 4-5, подключитесь к маршрутизатору рабочей группы, используя информацию о доступе из лабораторной работы 2-1 и сведения об IP-адресе и маске подсети из иллюстрации задания.

Действие 2 Введите команду **enable** для перехода в привилегированный режим EXEC.

Действие 3 В приглашении привилегированного режима введите команду **setup**. Эта команда запускает диалоговое окно начальной настройки.

Действие 4 Введите **yes** в качестве ответа на вопрос «Continue with configuration dialog?».

```
Continue with configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
```

Действие 5 Введите **no** в качестве ответа на вопрос «Would you like to enter basic management setup?».

```
Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: no
```

Действие 6 Введите **yes** в качестве ответа на вопрос «First, would you like to see the current interface summary?». Вывод на экран должен выглядеть следующим образом:

```
First, would you like to see the current interface summary? [yes]: yes

Interface            IP-Address   OK? Method Status                Protocol
FastEthernet0/0      unassigned   YES unset  administratively down down
FastEthernet0/1      unassigned   YES unset  administratively down down
FastEthernet0/0      unassigned   YES unset  administratively down down
FastEthernet0/0      unassigned   YES unset  administratively down down

Configuring global parameters:
```

Действие 7 Введите имя хоста маршрутизатора назначенной рабочей группы в приглашении «Enter host name», в приведенном ниже примере *x* соответствует букве рабочей группы (A, B, C, D, E, F, G или H).

```
Enter host name [Switch]: RouterX
```

Действие 8 Введите пароль «enable secret» в приглашении «Enter enable secret».

Пароль «enable secret» используется для защиты доступа к привилегированному режиму EXEC и режимам конфигурации. После ввода в конфигурацию этот пароль шифруется.

```
Enter enable secret: sanfran
```

Действие 9 Введите пароль «enable password» в приглашении «Enter enable password».

Пароль «enable password» используется в некоторых старых версиях программного обеспечения и загрузочных образах загрузки, если не указан пароль «enable secret».

```
Enter enable password: cisco
```

Действие 10 Введите пароль линии VTY в приглашении «Enter virtual terminal password».

Пароль виртуального терминала используется для защиты доступа к маршрутизатору через сетевой интерфейс.

```
Enter virtual terminal password: sanjose
```

Действие 11 Введите **no** в качестве ответа на вопрос «Configure SNMP Network Management?».

```
Configure SNMP Network Management? [no]:no
```

Действие 12 Введите **yes** в качестве ответа на вопрос «Configure IP?».

```
Configure IP? [yes]:yes
```

Действие 13 Введите **no** в качестве ответа на вопрос «Configure RIP routing?».

```
Configure RIP routing? [yes]: no
```

Действие 14 Введите **no** в качестве ответа на вопрос «Configure CLNS?».

```
Configure CLNS? [no]:no
```

Действие 15 Введите **no** в качестве ответа на запрос «Configure bridging?».

```
Configure bridging? [no]:no
```

Действие 16 Введите **yes** в качестве ответа на запрос «Do you want to configure FastEthernet0/0 interface?».

```
Configuring interface parameters:

Do you want to configure FastEthernet0/0 interface? [no]: yes
```

Действие 17 Введите **no** в качестве ответа на запрос «Use the 100 Base-TX (RJ-45) connector?».

```
Use the 100 Base-TX (RJ-45) connector? [yes]:no
```

Действие 18 Введите **no** в качестве ответа на вопрос «Operate in full-duplex mode?».

```
Operate in full-duplex mode? [no]:no
```

Действие 19 Введите **yes** в качестве ответа на вопрос «Configure IP on this interface?».

```
Configure IP on this interface? [no]: yes
```

Действие 20 Введите IP-адрес маршрутизатора, назначенного рабочей группе. (См. иллюстрацию задания для этой лабораторной работы.)

```
IP address for this interface: 10.x.x.3
```

Действие 21 Введите маску подсети для маршрутизатора, назначенного рабочей группе. Обратите внимание, что ПО Cisco IOS может определять класс IP-адреса.

```
Subnet mask for this interface [255.0.0.0] : 255.255.255.0
Class A network is 10.0.0.0, 24 subnet bits; mask is /24
```

Действие 22 Введите **no** в качестве ответа на вопрос «Do you want to configure FastEthernet0/1 interface?».

```
Do you want to configure FastEthernet0/1 interface? [no]:no
```

Действие 23 Введите **no** в качестве ответа на вопрос «Do you want to configure Serial0/0/0 interface?».

```
Do you want to configure Serial0/0/0 interface? [no]:no
```

Действие 24 Введите **no** в качестве ответа на вопрос «Do you want to configure Serial0/0/1 interface».

```
Do you want to configure Serial0/0/1 interface? [no]:no
```


Действие 25 Введите **no** в качестве ответа на вопрос «Would you like to go through AutoSecure configuration?».

```
Would you like to go through AutoSecure configuration? [yes]: no
AutoSecure dialog can be started later using «auto secure» CLI
```

Действие 26 Процесс настройки выводит сценарий конфигурации, который будет применяться в зависимости от ответа на соответствующий вопрос. Обратите внимание, что по умолчанию для маршрутизатора настраивается только пять (с 0 по 4) линий VTY. Коммутатор имеет 16 линий (от 0 до 15). Нажимайте клавишу **ПРОБЕЛ** для получения дополнительных данных при запросе вывода дополнительных данных (приглашение --More--).

```
The following configuration command script was created:

hostname RouterX
enable secret 5 $1$.dET$BDxkofHF3aAsRthe/c0.c.
enable password cisco
line vty 0 4
password sanjose
no snmp-server
!
ip routing
no clns routing
no bridge 1
!
interface FastEthernet0/0
no shutdown
half-duplex
ip address 10.x.x.3 255.255.255.0
no mop enabled
!
interface FastEthernet0/1
shutdown
no ip address
!
interface Serial0/0/0
shutdown
no ip address
!
interface Serial0/0/1
shutdown
no ip address
dialer-list 1 protocol ip permit
!
end


[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]:2
```

Действие 27 Введите **2**, чтобы сохранить эту конфигурацию в NVRAM и выйти из диалогового окна.

Действие 28 Проанализируйте вывод. Текущая версия Cisco IOS объявляет о том, что указанное имя хоста не соответствует последней конфигурации интерфейса командной строки (CLI), однако это имя принимается.

```
Building configuration...
[OK]
*Apr 24 00:37:02.203: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state
to up
Use the enabled mode 'configure' command to modify this configuration.
```

```
RouterX#
*Apr 24 00:37:04.867: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
```

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- с помощью команды **setup** введены параметры конфигурации маршрутизатора рабочей группы;
- выбрано сохранение конфигурации и выход из диалогового окна конфигурации.

Задача 2: Проверка конфигурации маршрутизатора

Используйте команды **show**, чтобы проверить соответствие конфигурации маршрутизатора вашим требованиям и убедиться, что она сохранена в файле загрузочной конфигурации startup-config.

Процедура упражнения

Выполните следующие действия:

Действие 1 Введите команду **show running-config**. Проанализируйте вывод, проверьте установку и соответствие паролей значениям, указанным в таблице 1. Убедитесь, что для интерфейса FastEthernet 0/0 указан IP-адрес, назначенный маршрутизатору данной вашей группы, и к этому интерфейсу не применяется команда **shutdown**. Ниже приводится пример вывода на экран, ваши данные должны выглядеть также.

```
..Text omitted!
..
!
interface FastEthernet0/0
 ip address 10.x.x.3 255.255.255.0
 duplex half
 speed auto
 no mop enabled
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
..Text omitted!
```

Действие 2 Введите команду **show startup-config**. Проанализируйте вывод и проверьте его соответствие информации, проверенной во время действия 1. Соответствие указывает, что команда **setup** сохранила конфигурацию в текущей и загрузочной конфигурациях.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- вывод команды **show running-config** соответствует данным, введенным во время задачи 1;
- загрузочная конфигурация совпадает с текущей конфигурацией.

Лабораторная работа 4-7: Повышение безопасности начальной конфигурации маршрутизатора

Выполните упражнение этой лабораторной работы, чтобы применить на практике знания, полученные в соответствующем модуле.

Задачи упражнения

В этом упражнении вам необходимо повысить безопасность маршрутизатора после его начальной конфигурации. После выполнения этого упражнения вы будете способны сделать следующее:

- добавить защиту на основе пароля для порта консоли;
- зашифровать все пароли с помощью команды Cisco IOS;
- добавить баннерное сообщение для процесса входа в систему;
- повысить безопасность удаленного управления маршрутизатором, добавив протокол SSH для к линиям VTY.

Иллюстрация задания

На рисунке ниже показано, что вы должны сделать во время данного упражнения.

Иллюстрация задания к лабораторной работе 4-7 Повышение безопасности начальной конфигурации маршрутизатора

Имя хоста рабочей группы	IP-адрес маршрутизатора	Маска подсети
RouterA	10.2.2.3	255.255.255.0
RouterB	10.3.3.3	255.255.255.0
RouterC	10.4.4.3	255.255.255.0
RouterD	10.5.5.3	255.255.255.0
RouterE	10.6.6.3	255.255.255.0
RouterF	10.7.7.3	255.255.255.0
RouterG	10.8.8.3	255.255.255.0
RouterH	10.9.9.3	255.255.255.0

ICND1 v1.0 – 16

Необходимые ресурсы

Ниже перечислены ресурсы и устройства, необходимые для выполнения упражнения.

- ПК, подключенный к удаленной лаборатории.
- Приложение для эмуляции терминала с поддержкой SSH.
- Информация о доступе к назначенному комплекту оборудования, полученная в лабораторной работы 4.1.
- Успешное выполнение лабораторной работы 4-6.

Список команд

В таблице приводится описание команд, используемых в упражнении.

Команда	Описание
banner login	Позволяет настроить сообщение, которое будет отображаться во время входа в систему.
configure terminal	Переводит устройство в режим глобальной конфигурации из привилегированного режима EXEC.
copy running-config startup-config	Копирует файл текущей конфигурации в файл загрузочной конфигурации, который хранится в памяти NVRAM.
crypto key generate rsa	Генерирует используемые пары ключей RSA.
enable	Активирует привилегированный режим EXEC. В привилегированном режиме EXEC доступно большее количество команд. Эта команда требует ввода пароля разрешения доступа (enable password), если он настроен.
end	Эта команда завершает режим конфигурации.
exit	Выход из текущего режима конфигурации.
ip domain-name *имя*	Задает имя домена IP, которое необходим для процесса генерации криптографического ключа.
ip ssh version [**1** | **2**]	Указывает версию протокола SSH, которую необходимо запустить. Чтобы отключить настроенную версию SSH и вернуться в режим совместимости, используйте версию **no** данной команды.
line console 0	Задает линию консоли и позволяет перейти в режим конфигурации линии.
line vty 0 4	Вход в режим конфигурации линий виртуального терминала. Линии виртуального терминала (VTY) позволяют получать доступ к коммутатору для удаленного управления сетью. Доступное количество линий VTY зависит от версии ПО Cisco IOS. Обычно используются значения от 0 до 4 и от 0 до15 (включительно).
login	Активирует процесс ввода пароля при входе на консоли или линиях VTY.
login local	Активирует процесс ввода пароля при входе на консоли или линиях VTY, требующий использования локальной базы данных аутентификации.
logout	Выход из режима EXEC, после которого потребуется повторная аутентификация (если она включена).
password	Назначает пароль линиям VTY или консоли.
service password-encryption	Включает службу, которая будет шифровать все пароли в текущей конфигурации.

Команда	Описание
show ip ssh	Показывает текущие параметры протокола SSH.
show running-config	Выводит текущие параметры конфигурации маршрутизатора.
transport input telnet ssh	Определяет, какие протоколы используются для подключения к определенной линии маршрутизатора.
username *имя_пользователя* **password** *пароль*	Создает пару имени пользователя и пароля, которая затем может использоваться как локальная база данных аутентификации.

Подсказки

Для этого упражнения доступны следующие подсказки.

Текущие пароли

Вход в консоль маршрутизатора	нет
Пароль «enable password» маршрутизатора	cisco
Пароль «enable secret» маршрутизатора	sanfran
Идентификатор пользователя для входа в систему маршрутизатора через линию VTY	нет
Пароль для входа в систему маршрутизатора через линию VTY	sanjose
Вход в консоль коммутатора	sanjose
Пароль «enable password» коммутатора	cisco
Пароль «enable secret» коммутатора	sanfran
Идентификатор пользователя для входа в систему коммутатора через линию VTY	netadmin
Пароль для входа в систему коммутатора через линию VTY	netadmin

Задача 1: Добавление безопасности консольного порта на базе пароля

После начальной настройки маршрутизатора, во время которой заданы пароли для линий VTY, в системе безопасности остается потенциальная брешь, поскольку консольный порт не защищен паролем. Используйте пароль **sanjose** для линии консоли, если инструктор не предоставил вам другой пароль, который следует указать ниже.

Процедура упражнения

Выполните следующие действия:

Действие 1 Подключитесь к удаленному маршрутизатору рабочей группы через терминальный сервер. Для входа в пользовательский режим EXEC необходимо использовать настроенный ранее пароль VTY.

Действие 2 Введите команду enable и пароль для доступа к приглашению привилегированного режима EXEC.

Действие 3 В приглашении привилегированного режима назначенного маршрутизатора введите команду **config t**.

Действие 4 Введите команду **line console 0**.

Действие 5 В режиме конфигурации консоли линии введите команду **password** *пароль*. Используйте пароль, заданный для линий VTY.

Действие 6 Введите команду **login**, чтобы в будущем для доступа к маршрутизатору через консоль запрашивался пароль.

Действие 7 Введите команду **end** для выхода из режима конфигурации.

Действие 8 Введите команду **show running-config** и проанализируйте вывод, чтобы убедиться в правильности конфигурации порта консоли (0) и линий VTY (с 0 по 4). Вывод должен соответствовать выводу в примере ниже, конфигурация линий выделена жирным шрифтом. Обратите внимание, что пароли для консольного порта и линий VTY сохраняются в виде незашифрованного текста.

```
RouterX#show running-config
..
..Text omitted
..
!
line con 0
 password sanjose
 login
line aux 0
line vty 0 4
 password sanjose
 login
!
end
```

Действие 9 Выйдите из системы маршрутизатора и войдя в нее снова через консоль, чтобы проверить настроенный пароль.

Действие 10 Введите команду **logout**.

Действие 11 Нажмите клавишу **Enter**, чтобы открыть приглашение к вводу пароля.

Действие 12 Введите только что заданный пароль, чтобы получить доступ к приглашению пользовательского режима EXEC.

Действие 13 Введите команду и пароль для получения доступа к приглашению привилегированного режима (enable EXEC).

Действие 14 Ниже приводится пример данных, которые должны выводиться на экран при выполнении действий с 10 по 13.

```
RouterX#logout

..
..empty lines omitted
..

RouterX con0 is now available


Press RETURN to get started.

..
..empty lines omitted
..

User Access Verification

Password:
RouterX>enable
Password:
RouterX#
```


Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- для консоли линии настроен запрос пароля;
- в результате проверки конфигурации вы обнаружили, что пароли линий сохранены в виде незашифрованного текста;
- вы успешно проверили процесс входа в систему и доступ к консоли с использованием пароля;
- вывод соответствовал примеру, приведенному в действии 14.

Задача 2: Активация службы шифрования паролей

В предыдущей задаче мы отметили, что некоторые пароли хранятся в незашифрованном виде. При передаче и сохранении данной конфигурации в удаленных файловых системах могут возникать проблемы безопасности. В этой задаче вам необходимо настроить службу шифрования паролей для защиты незашифрованных паролей.

Процедура упражнения

Выполните следующие действия:

Действие 1 Используя приглашение привилегированного режима EXEC, введите команду для перехода в режим глобальной конфигурации.

Действие 2 Введите команду **service password-encryption**.

Действие 3 Введите команду для возвращения к приглашению привилегированного режима.

Действие 4 Введите команду для просмотра текущей конфигурации. Обратите внимание на первые и последние строки конфигурации, команда активна и действует на пароли для линий. Вывод должен соответствовать примеру ниже. Жирным шрифтом выделены данные, на которые следует обратить внимание.

```
RouterX#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RouterX(config)#service password-encryption
RouterX(config)#end
RouterX#
*Mar 16 20:19:40.509: %SYS-5-CONFIG_I: Configured from console by console
RouterX#show running-config
Building configuration...

Current configuration : 940 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
..
..Text omitted
..

!
!
line con 0
 password 7 051807012B435D0C
 login
line aux 0
```

```
line vty 0 4
 password 7 051807012B435D0C
 login
!
scheduler allocate 20000 1000
!
end
```

Действие 5 Введите команду для сохранения текущей конфигурации в файле startup-config.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- включена служба шифрования паролей;
- вам удалось вывести текущую конфигурацию и найти зашифрованные пароли линий;
- вы сохранили текущую конфигурацию.

Задача 3: Настройка баннера входа

В рамках любой политики безопасности необходимо явно указать, что доступ к сетевым ресурсам случайным посетителем запрещен. В прошлом хакеры успешно использовали факт наличия приглашения «welcome (добро пожаловать)» при входе в качестве юридического оправдания несанкционированного проникновения в сеть. Когда пользователь пытается получить доступ к сетевому устройству (коммутатору, маршрутизатору и т. д.), должно появляться сообщение, явно указывающее на ограничение доступа. Его можно создать с помощью команды настройки **banner** в Cisco IOS.

Процедура упражнения

Выполните следующие действия:

Действие 1 Введите команду для доступа к приглашению глобальной конфигурации.

Действие 2 Введите команду **banner login %**. Знак процента является начальным ограничителем текста сообщения.

Действие 3 Введите текст сообщения после знака **%**. НЕ включайте знак процента в текст, поскольку он будет рассматриваться как конечный ограничитель сообщения. Ниже приведен пример вывода конфигурации баннерного сообщения.

```
RouterX#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RouterX(config)#banner login %
Enter TEXT message. End with the character '%'.
********** Warning  *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.

************************************************************%

RouterX(config)#end
```

Действие 4 Введите команду для просмотра текущей конфигурации. Ниже приведен фрагмент вывода на экран, который относится к конфигурации баннера. Обратите внимание, что ограничитель текста заменен нетекстовым управляющим символом ^C.

```
!
```



```
banner login ^C
********** Warning  *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.
************************************************************^C
!
```

Действие 5 Используйте команду **logout** для завершения сеанса консоли. Затем снова выполните вход, чтобы получить доступ к приглашению привилегированного режима. Обратите внимание, что перед вводом пароля отображается баннерное сообщение. Ниже приведен фрагмент информации, которая должна появиться на экране. Для экономии места вывод приведен не полностью.

```
RouterX#logout


RouterX con0 is now available


Press RETURN to get started.



********* Warning  *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.
************************************************************

User Access Verification

Password:
RouterX>en
Password:
RouterX#
```

Действие 6 Введите команду для сохранения текущей конфигурации в NVRAM.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- вы настроили баннерное сообщения для входа в систему, в котором явно указано, что доступ к маршрутизатору ограничен;
- сообщения при входе в систему проверено, перед запросом пароля отображается предупреждение;
- конфигурация сохранена.

Задача 4: Включение протокола SSH для удаленного управления

В предыдущей задаче вы защитили пароли с помощью шифрования. Однако если процесс удаленного управления основан на протоколе Telnet, который отправляет все символы, включая пароли, в незашифрованном виде, существует потенциальная опасность перехвата пакета и неправомерного использования информации. В этой задаче вам необходимо настроить протокол SSH, который является альтернативой протоколу Telnet. Если среда позволяет, мы рекомендуем *заменять* Telnet на SSH.

Процедура упражнения

Выполните следующие действия:

Действие 1 В приглашении привилегированного режима (enable EXEC) введите команду для доступа к приглашению глобальной конфигурации.

Действие 2 Протокол SSH требует использования имени пользователя и пароля. Эти параметры еще не заданы в конфигурации, это необходимо сделать сейчас. Введите команду **username netadmin password netadmin**. В этом примере используется простое имя пользователя, но в реальной среде *необходимо* использовать более сложные значения.

Действие 3 Введите команду **ip domain-name** *имя-домена*. Для генерации криптографического ключа SSH необходимо, чтобы в конфигурации были заданы и имя хоста, и имя домена. Имя хоста уже задано, поэтому необходимо указать имя домена. Обычно используется имя домена организации, но в этой лабораторной работе будет использоваться «cisco.com».

Действие 4 Введите команду **crypto key generate rsa**. Появится запрос на выбор размера ключа; по умолчанию используется значение 512, но вам необходимо ввести **1024**. Ниже приведен фрагмент вывод, в который включены только строки, которые относятся к данной задаче.

```
RouterX(config)#username netadmin password netadmin
SwitchX(config)#ip domain-name cisco.com
SwitchX(config)#crypto key generate rsa
The name for the keys will be: RouterX.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
 General Purpose Keys. Choosing a key modulus greater than 512 may take
 a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

RouterX(config)#
*Mar 16 20:32:15.613: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Действие 5 Введите команду **ip ssh version 2**, чтобы включить нужную версию SSH.

Действие 6 Введите команду **line vty 0 4**.

Действие 7 Введите команду **login local**. Она позволяет перевести процесс входа на использование локально заданных пар имени пользователя и пароля.

Действие 8 Введите команду **transport input telnet ssh**. Она настроит 5 линий VTY для поддержки обоих протоколов: Telnet и SSH. Вывод должен быть аналогичен примеру ниже.

```
RouterX(config)#line vty 0 4
RouterX(config-line)#login local
SwitchX(config-line)#transport input telnet ssh
```

Действие 9 Введите команду для возвращения к приглашению привилегированного режима.

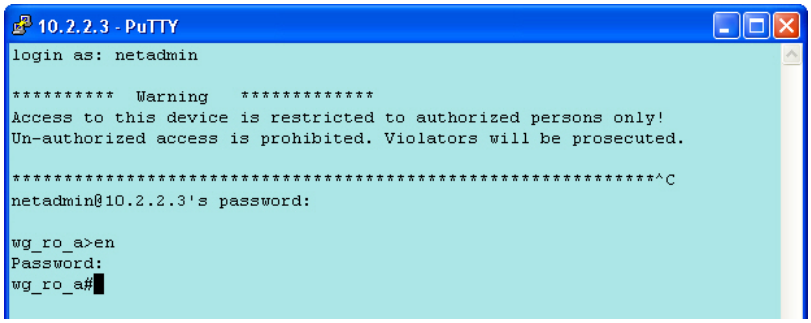
Действие 10 Введите команду **show ip ssh**.

```
RouterX#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
```

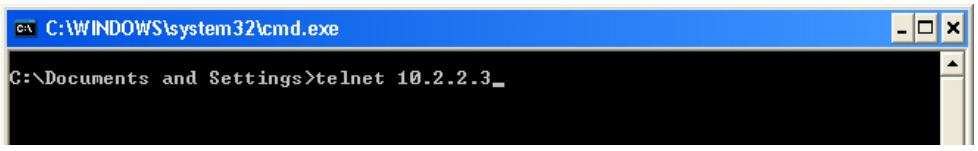

Действие 11 Для проверки конфигурации необходимо выполнить подключение туннеля VPN к удаленной лаборатории, используя метод, описанный в лабораторной работе 2-1. Может появиться предупреждение безопасности, относящееся к криптографическому ключу. Нажмите кнопку **Yes** во всплывающем окне, чтобы принять этот ключ.

Действие 12 Откройте на ПК клиентское приложение терминала SSH. Используйте IP-адрес маршрутизатора рабочей группы (**10.*x*.*x*.3**) и пару имени пользователя и пароля, заданную во время действия 2 этой задачи.

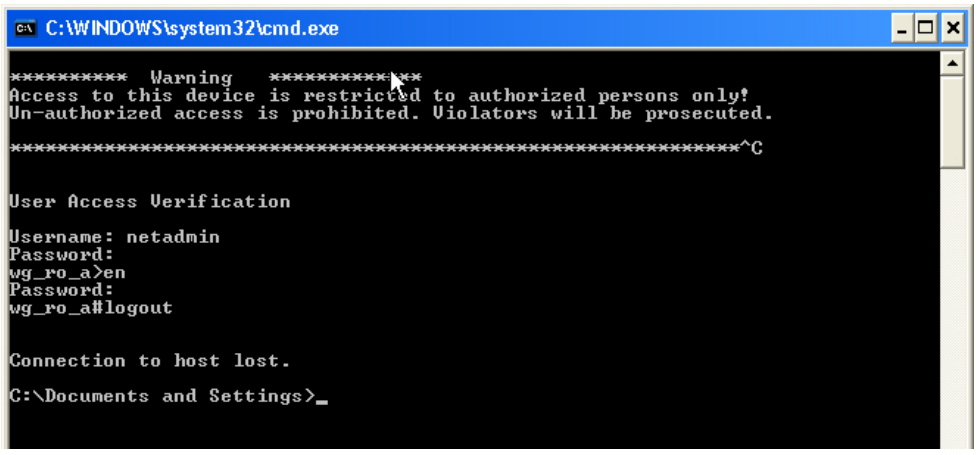
Действие 13 Ниже приводится пример успешного подключения через протокол SSH с помощью приложения PuTTY.



Действие 14 Откройте окно командной строки Windows и введите команду **telnet 10.*x*.*x*.3** (IP-адрес *вашего* маршрутизатора рабочей группы). Вывод на экран должен выглядеть следующим образом.



Действие 15 Введите имя пользователя и пароль в новом окне командной строки Telnet, которое откроется автоматически. Включив сеансы Telnet и SSH одновременно, введите **logout** в приглашении пользовательского режима (user EXEC) и закройте окно командной строки, введя **exit** в приглашении командной строки. Вывод на экран должен выглядеть следующим образом.



Действие 16 Введите команду для сохранения конфигурации в файле startup-config.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- на линиях VTY настроена поддержка протокола SSH 2;
- создано прямое подключение к маршрутизатору рабочей группы с использованием протоколов SSH и Telnet, чтобы проверить поддержку их одновременной работы;
- конфигурация сохранена.

Лабораторная работа 4-8: Использование Cisco SDM для настройки функций DHCP-сервера

Выполните упражнение этой лабораторной работы, чтобы применить на практике знания, полученные в соответствующем модуле.

Задачи упражнения

В этом упражнении вам необходимо использовать систему Cisco SDM для настройки функций DHCP-сервера на маршрутизаторе рабочей группы. После выполнения этого упражнения вы будете способны сделать следующее:

- использовать ПО Cisco SDM для настройки пула адресов DHCP;
- использовать Cisco SDM, чтобы проверить получение адреса из только что созданного пула хотя бы одним клиентом DHCP;
- использовать команды Cisco IOS для определения порта коммутатора, через который DHCP-клиент подключен к коммутатору рабочей группы.

Иллюстрация задания

На рисунке ниже показано, что вы должны сделать во время данного упражнения.

Иллюстрация задания к лабораторной работе 4-8 Использование Cisco SDM для настройки функций DHCP-сервера

Комплект оборудования	IP-адрес маршрутизатора	IP-адрес коммутатора
A	10.2.2.3 /24	10.2.2.11 /24
B	10.3.3.3 /24	10.3.3.11 /24
C	10.4.4.3 /24	10.4.4.11 /24
D	10.5.5.3 /24	10.5.5.11 /24
E	10.6.6.3 /24	10.6.6.11 /24
F	10.7.7.3 /24	10.7.7.11 /24
G	10.8.8.3 /24	10.8.8.11 /24
H	10.9.9.3 /24	10.9.9.11 /24

ICND1 v1.0 – 17

Необходимые ресурсы

Ниже перечислены ресурсы и устройства, необходимые для выполнения упражнения.

- ПК, подключенный к удаленной лаборатории.
- Приложение для эмуляции терминала с поддержкой SSH.
- Информация о доступе к назначенному комплекту оборудования, полученная в лабораторной работы 4.1.
- Успешное выполнение лабораторной работы 4-7.

Список команд

В таблице приводится описание команд, используемых в упражнении.

Команды Cisco IOS для маршрутизатора и коммутатора

Команда	Описание
ping	**Используется для диагностики основного сетевого подключения.**
show mac-address-table *dynamic*	**Отображает только динамические записи таблицы MAC-адресов, используется в привилегированном режиме EXEC.**
show ip arp	**Используется для вывода кэша ARP.**

Подсказки

Для упражнений этой лабораторной работы доступны следующие подсказки.

Таблица 1. Информация о пуле DHCP-сервера

Рабочая группа	Имя пула DHCP	Сеть/маска пула DHCP	Начальный IP-адрес	Конечный IP-адрес	Маршрутизатор по умолчанию	Время аренды (дни:часы:минуты)
A	wgA_clients	10.2.2.0/24	10.2.2.150	10.2.2.199	10.2.2.3	0:0:5
B	wgB_clients	10.3.3.0/24	10.3.3.150	10.3.3.199	10.3.3.3	0:0:5
C	wgC_clients	10.4.4.0/24	10.4.4.150	10.4.4.199	10.4.4.3	0:0:5
D	wgD_clients	10.5.5.0/24	10.5.5.150	10.5.5.199	10.5.5.3	0:0:5
E	wgE_clients	10.6.6.0/24	10.6.6.150	10.6.6.199	10.6.6.3	0:0:5
F	wgF_clients	10.7.7.0/24	10.7.7.150	10.7.7.199	10.7.7.3	0:0:5
G	wgG_clients	10.8.8.0/24	10.8.8.150	10.8.8.199	10.8.8.3	0:0:5
H	wgH_clients	10.9.9.0/24	10.9.9.150	10.9.9.199	10.9.9.3	0:0:5

Текущие пароли

Вход в консоль маршрутизатора	sanjose
Пароль «enable password» маршрутизатора	cisco
Пароль «enable secret» маршрутизатора	sanfran
Идентификатор пользователя для входа в систему маршрутизатора через линию VTY	netadmin
Пароль для входа в систему маршрутизатора через линию VTY	netadmin
Вход в консоль коммутатора	sanjose
Пароль «enable password» коммутатора	cisco
Пароль «enable secret» коммутатора	sanfran
Идентификатор пользователя для входа в систему коммутатора через линию VTY	netadmin
Пароль для входа в систему коммутатора через линию VTY	netadmin

Задача 1: Настройка маршрутизатора для поддержки веб-приложений, пользователя с уровнем привилегий 15, а также протоколов Telnet и SSH

В этой задаче вам необходимо включить Cisco SDM на маршрутизаторе, который настроен с помощью последовательности загрузки Cisco IOS или интерфейса командной строки. Если заводская загрузочная конфигурация стерта для использования последовательности загрузки Cisco IOS, вы все еще можете работать с Cisco SDM. Для этого необходимо настроить маршрутизатор для поддержки веб-приложений, использования учетной записи пользователя с уровнем привилегий 15, а затем настроить поддержку протоколов Telnet и SSH. Эти изменения можно сделать с помощью сеанса Telnet или консольного подключения.

Процедура упражнения

Выполните следующие действия:

Действие 1 Подключитесь к удаленному маршрутизатору рабочей группы через терминальный сервер и введите необходимые команды и пароли, чтобы получить доступ к приглашению привилегированного режима EXEC.

Действие 2 В текущих конфигурациях служба HTTP уже включена. Однако рекомендуется использовать безопасную версию протокола HTTP (HTTPS). Чтобы включить сервер HTTP/HTTPS на маршрутизаторе рабочей группы, введите команду **ip http secure-server**.

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

Примечание. Поддержка защищенного сервера зависит от версии Cisco IOS, запущенной на маршрутизаторе. Если протокол HTTPS не поддерживается, вы все еще можете включить сервер HTTP.

Действие 3 Кроме того, необходимо настроить метод аутентификации для служб HTTPS. Чтобы включить метод аутентификации сервера HTTP/HTTPS маршрутизатора рабочей группы, введите команду **ip http authentication local** в режиме глобальной конфигурации.

```
Router(config)# ip http authentication local
```

Действие 4 Чтобы присвоить учетной записи пользователя netadmin уровень привилегий 15 (привилегии полного доступа), введите команду **username netadmin privilege 15** в режиме глобальной конфигурации.

```
Router(config)# username netadmin privilege 15
```

Задача 2: Использование Cisco SDM для настройки пула DHCP

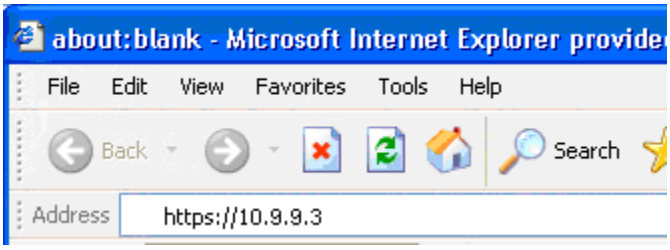
В этой задаче вам необходимо использовать ПО Cisco SDM для настройки пула DHCP на маршрутизаторе рабочей группы.

Процедура упражнения

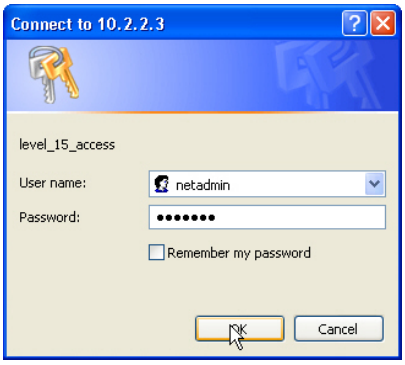
Выполните следующие действия:

Действие 1 Откройте VPN-подключение к удаленной рабочей группе.

Действие 2 Откройте окно Windows Internet Explorer и введите IP-адрес маршрутизатора рабочей группы в адресной строке в виде URL-адреса, например **https://10.*x*.*x*.3**.

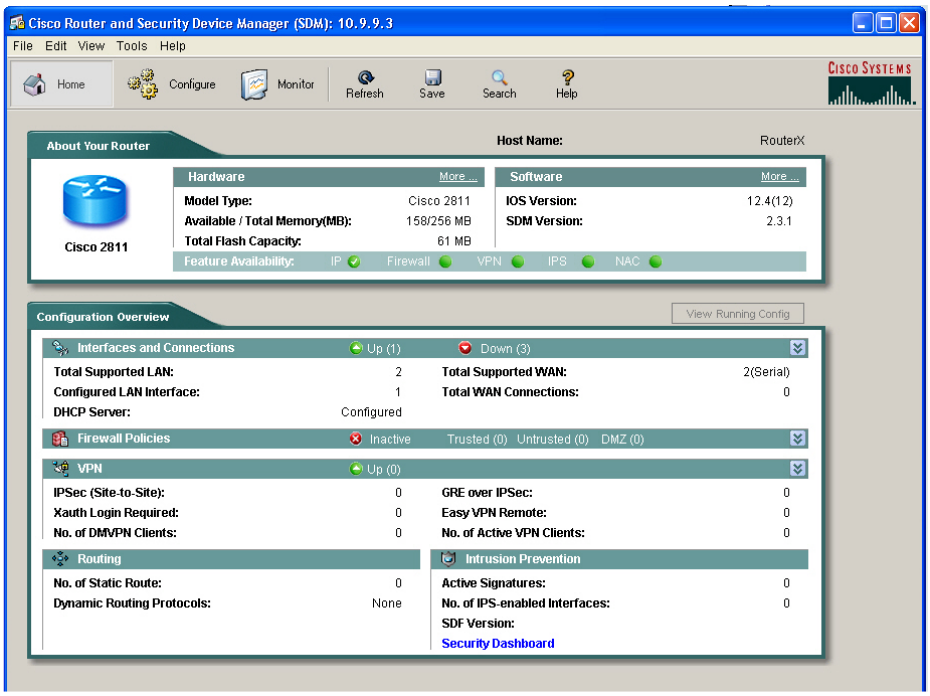


Действие 3 В открывшемся окне введите имя пользователя и пароль (netadmin).

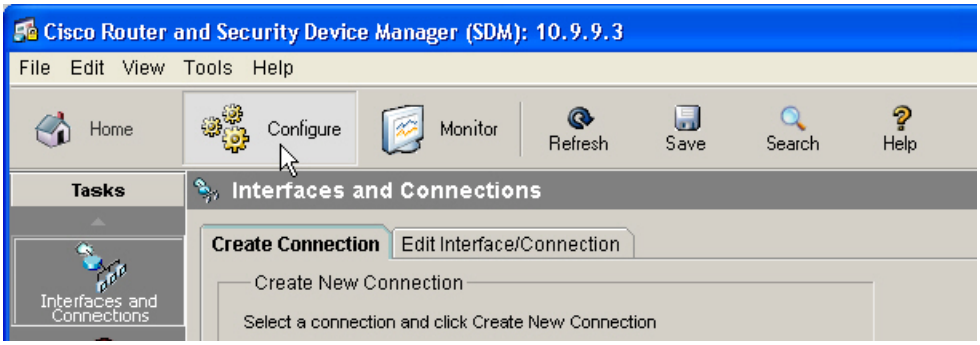


Действие 4 Может появиться следующее сообщение. Нажмите кнопку **Yes** в этом и *всех* следующих предупреждениях системы безопасности.

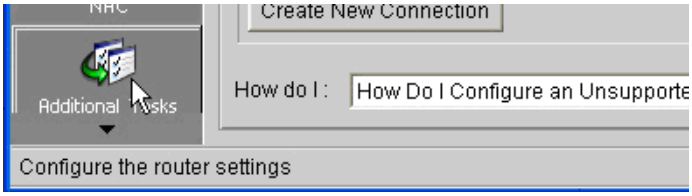
Действие 5 В конечном итоге должен появиться следующий экран.



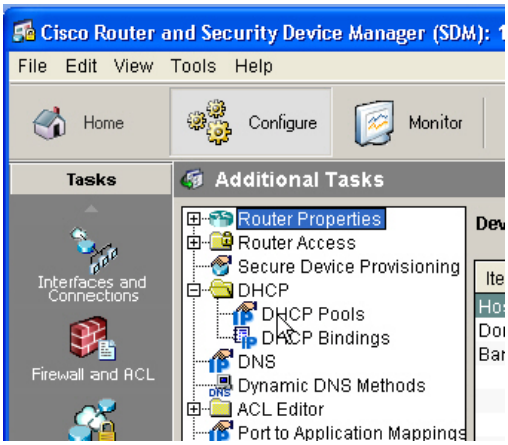
Действие 6 Перейдите на вкладку **Configure (Настройка)**.



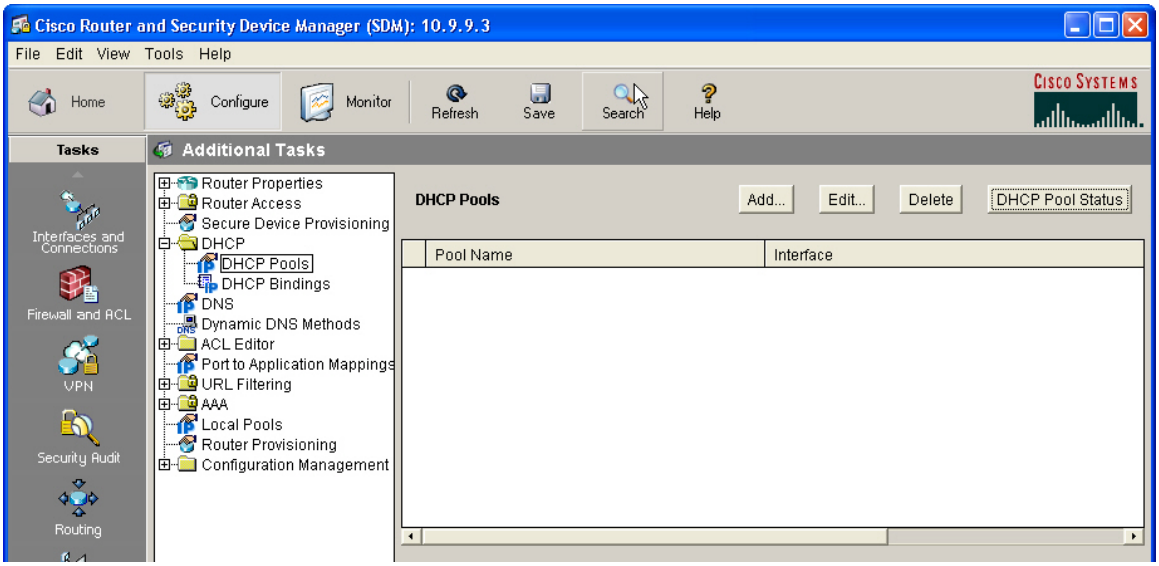
Действие 7 В левой части окна появятся новые элементы. Выберите **Additional Tasks (Дополнительные задачи)** (самый нижний элемент).



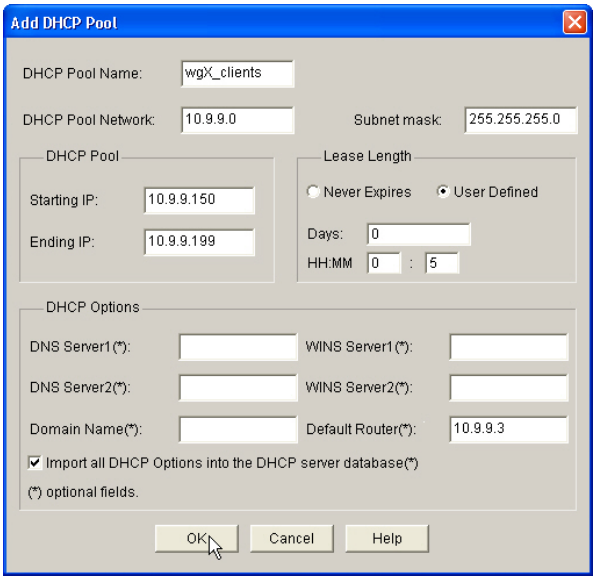
Действие 8 На панели «Additional Tasks» откройте вкладку **DHCP** и выберите **DHCP Pools (Пулы DHCP)**.



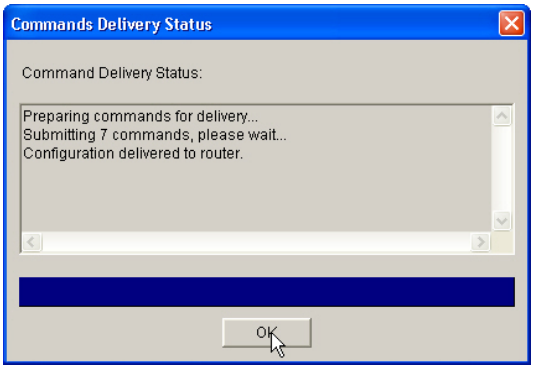
Действие 9 На панели «DHCP Pools» нажмите кнопку **Add (Добавить)**.



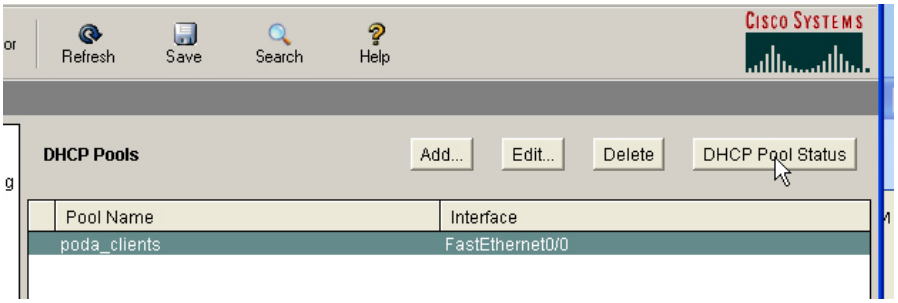
Действие 10 В окне «Add DHCP Pool» добавьте данные из таблицы 1 для своей рабочей группы. Завершив ввод, нажмите кнопку **OK**.



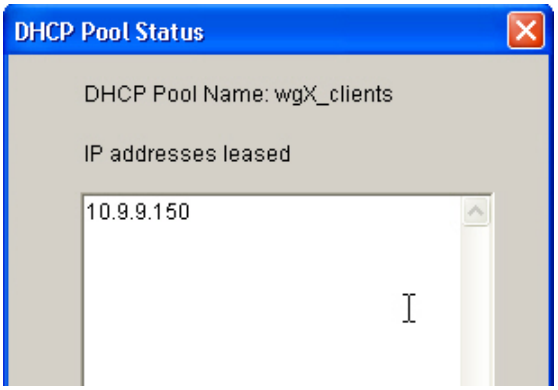
Действие 11 Откроется окно «Commands Delivery» с данными о состоянии передачи команд конфигурации маршрутизатору рабочей группы. Когда появится сообщение «Configuration delivered to router», нажмите кнопку **OK**.



Действие 12 Подождите несколько минут, пока клиенты в вашей получают адрес. Затем нажмите кнопку **DHCP Pool Status (Состояние пула DHCP)**.



Действие 13 В окне «DHCP Pool Status» (Состояние пула DHCP) должны отображаться следующие данные. Это значит, что адрес клиента относится к диапазону пула. Для обновления экрана можно нажать кнопку «Refresh» в главном окне.



Действие 14 Запишите IP-адрес DHCP-клиента в следующей строке.

_____

Действие 15 Нажмите кнопку **OK**, чтобы закрыть окно состояния пула DHCP.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- создано подключение к маршрутизатору рабочей группы и открыто окно Cisco SDM;
- выполнена настройка маршрутизатора для поддержки пула DHCP;
- с помощью ПО Cisco SDM подтверждено получение клиентом адреса из заданного пула;
- вы записали фактический адрес клиента DHCP.

Задача 3: Использование инструментальных средств для сопоставления данных о сети

При внедрении сетей необходимо проверять правильность конфигурации. Кроме того, для обеспечения безопасности и выполнения технического обслуживания вы должны уметь находить и использовать информацию о сети для определенных целей. В этом упражнении вы должны использовать собранную информацию об адресах для определения точки подключения конечной системы к сети. Кроме того, эта информация необходима для отслеживания источников дублированных адресов и пути пакетов через сеть при поиске и устранении неполадок.

Процедура упражнения

Выполните следующие действия:

Действие 1 Откройте SSH-подключение к маршрутизатору рабочей группы.

Действие 2 В приглашении привилегированного режима маршрутизатора рабочей группы введите команду **ping** *IP_адрес_dhcp-клиента*. Вывод на экран должен выглядеть следующим образом.


```
RouterX#ping 10.10.10.150

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.150, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Действие 3 Введите команду **show ip arp** *IP_адрес_dhcp-клиента*, чтобы получить аппаратный адрес (MAC-адрес), связанный с IP-адресом, по которому вы отправили эхо-запрос . Вывод на экран должен выглядеть следующим образом.

```
RouterX#show ip arp 10.10.10.150
Protocol Address      Age (min) Hardware Addr  Type  Interface
Internet 10.10.10.150       63  001a.6ca1.eea9 ARPA  FastEthernet0/0
```

Действие 4 Запишите аппаратный адрес (MAC-адрес) *вашего* DHCP-клиента в строке ниже.

Действие 5 Откройте консольное подключение к коммутатору рабочей группы.

Действие 6 В приглашении привилегированного режима коммутатора рабочей группы введите команду **show mac-address-table dynamic**, чтобы отобразить только динамически полученные элементы. Вывод на экран должен выглядеть следующим образом.

```
SwitchX#show mac-address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan   Mac Address      Type      Ports
----   -----------      --------  -----
  1    001a.6ca1.eea9   DYNAMIC   Fa0/11
  1    001a.6ca1.eed8   DYNAMIC   Fa0/2
  1    001a.6dd7.1981   DYNAMIC   Fa0/11
  1    001a.6dfb.c401   DYNAMIC   Fa0/12
Total Mac Addresses for this criterion: 4
```

Действие 7 Используя MAC-адрес из предыдущего действия, определите порт коммутатора, через который DHCP-клиент подключен к сети, и запишите его в строке ниже.

Действие 8 Вы определили порт коммутатора, через который DHCP-клиент подключен к сети. Этот процесс можно использовать в сети с любым количеством коммутаторов или маршрутизаторов для отслеживания физического местоположения любого устройства на основе его IP-адреса и MAC-адреса (аппаратного адреса).

Действие 9 Закройте все открытые подключения и туннель VPN.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- команда **ping** выполнена для IP-адреса DHCP-клиента, определенного в задаче 1;
- используя информацию в выводе команды **ping**, вы определили MAC-адрес DHCP-клиента;
- с помощью команды **workgroup switch mac-address-table** вы определили порт, через который DHCP-клиент получает доступ в сеть.

Лабораторная работа 4-9: Управление сеансами удаленного доступа.

Выполните упражнение этой лабораторной работы, чтобы применить на практике знания, полученные в соответствующем модуле.

Задачи упражнения

В этом упражнении вы должны использовать подключения по протоколам Telnet и SSH для доступа к маршрутизаторам и коммутаторам Cisco. После выполнения этого упражнения вы будете способны сделать следующее:

- инициировать, приостанавливать, возобновлять и закрывать сеансы Telnet на маршрутизаторе или коммутаторе Cisco;
- инициировать, приостанавливать, возобновлять и закрывать сеансы SSH на маршрутизаторе или коммутаторе Cisco.

Иллюстрация задания

На рисунке ниже показано, что вы должны сделать во время данного упражнения.

Необходимые ресурсы

Ниже перечислены ресурсы и устройства, необходимые для выполнения упражнения.

- ПК, подключенный к удаленной лаборатории.
- Приложение для эмуляции терминала с поддержкой SSH.

- Информация о доступе к назначенному комплекту оборудования, полученная в лабораторной работы 2-1.
- Успешное выполнение лабораторной работы 4-8.

Список команд

В таблице приводится описание команд, используемых в упражнении.

Команды маршрутизатора и коммутатора Cisco IOS

Команда	Описание
Ctrl-Shift-6 x	Последовательность выхода для сеансов Telnet или SSH.
disconnect [*сеанс*]	Отключение существующего сетевого подключения. При необходимости можно ввести номер сеанса.
exec-timeout *мин* [*сек*]	Задает время бездействия, по истечении которого подключение закрывается автоматически.
exit	Команда exit в режиме EXEC позволяет завершить активный сеанс (выйти из системы).
history size *число*	Задает количество строк, сохраняемых в буфере журнала для повторного вызова. Используется два отдельных буфера – один для команд режима EXEC и другой для команд режима конфигурации.
ip domain-lookup	Включает разрешение символьных имен с помощью DNS сервера.
line console 0	Вход в режим конфигурации консольной линии 0.
logging synchronous	Синхронизирует вывод незапрошенных сообщений и команды отладки привилегированного режима EXEC с запрошенным выводом устройства и приглашениями конкретной линии консольного порта или линии VTY.
logout	Выход из режима EXEC, после которого потребуется повторная аутентификация или переподключение.
resume	Переключение на другое открытое подключение по протоколу Telnet или SSH.
show sessions	Выводит информацию об открытых подключениях по протоколу Telnet или SSH.
show users	Выводит информацию об активных линиях.
ssh *ip_адрес*	Создает шифрованный сеанс с удаленным сетевым устройством, используя идентификатор текущего пользователя. IP-адрес идентифицирует устройство назначения.
telnet *ip_адрес*	Создает сетевое подключение протоколу Telnet. IP-адрес идентифицирует устройство назначения.

Подсказки

- Для этой лабораторной работы нет подсказок.

Задача 1: Оптимизация использования CLI маршрутизатора

В этой задаче вам следует ввести команды для оптимизации использования интерфейса командной строки (CLI), которые уже использовались для коммутатора рабочей группы. Необходимо увеличить число строк в буфере журнала, увеличить значение таймера бездействия порта консоли и запретить разрешение имен при неверном вводе команд.

Процедура упражнения

Выполните следующие действия:

Действие 1 Подключитесь к удаленному маршрутизатору рабочей группы через терминальный сервер и введите необходимые команды и пароли, чтобы войти в привилегированный режим.

Действие 2 Размер буфера журнала равен 20. Это значение можно изменить с помощью команды **terminal history size 100**. Однако его необходимо вводить после каждого выхода и повторного входа в систему коммутатора. Размер журнала можно задать в конфигурации консоли и линий VTY.

Действие 3 Введите команду **config t**, чтобы перейти к приглашению глобальной конфигурации.

Действие 4 Введите команду **line console 0**.

Действие 5 Введите команду **history size 100** для изменения размера буфера журнала.

Действие 6 Введите команду **exec-timeout 60** для увеличения значения таймаута бездействия.

Действие 7 Введите команду **logging synchronous** для синхронизации вывода незапрошенных сообщений и вывода команды отладки привилегированного режима EXEC с вводом из CLI.

Действие 8 Введите команду **line vty 0 4** для настройки линий VTY.

Действие 9 Введите команды для установки значения 100 для буфера журнала и включения синхронизации сообщений.

Действие 10 Введите команду **exit** для возврата в режим глобальной конфигурации.

Действие 11 Введите команду **no ip domain-lookup**, чтобы отключить разрешение символьных имен.

Действие 12 Введите команду **end** для возвращения к приглашению привилегированного режима EXEC.

Действие 13 Введите команду **show terminal**. Вывод должен выглядеть следующим образом. В этом примере некоторые ненужные строки были удалены.

```
RouterX#show terminal
Line 0, Location: "", Type: ""
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 9600/9600, no parity, 2 stopbits, 8 databits
..
..Text omitted
..
Editing is enabled.
History is enabled, history size is 100.
DNS resolution in show commands is enabled
Full user help is disabled
Allowed input transports are none.
Allowed output transports are pad telnet rlogin lapb-ta mop v120 ssh.
Preferred transport is telnet.
No output characters are padded
No special data dispatching characters
```


Действие 14 Введите команду **show running-config** для просмотра текущей конфигурации и убедитесь, что сделанные изменения верны.

Действие 15 Убедитесь, что в текущей конфигурации отражены изменения, и сохраните ее в файле startup-config.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- для таймаута бездействия порта консоли задано значение 60 минут;
- вы подтвердили, что для размер буфера журнала имеет значение 100 строк для линий VTY и консоли;
- вы подтвердили, что для линий VTY и консоли настроена функция logging synchronous;
- вы подтвердили отключение запроса доменных имен IP;
- текущая конфигурация сохранена в файле startup-config.

Задача 2: Подключение к удаленной рабочей группе через тоннель VPN

В этой задаче вам необходимо открыть VPN-подключение к удаленной рабочей группе, затем выполнить вход в систему маршрутизатора своей рабочей группы, используя приложение эмуляции терминала. Используйте имя пользователя и пароль **netadmin**. Затем вам следует увеличить автоматический таймаут бездействия для линий виртуального терминала маршрутизатора рабочей группы до 30 минут на время выполнения этой лабораторной работы.

Процедура упражнения

Выполните следующие действия:

Действие 1 На ПК установите VPN-подключение с назначенной рабочей группой.

Действие 2 На ПК используйте ПО PuTTY для подключения к IP-адресу маршрутизатора рабочей группы и перехода к приглашению привилегированного режима. Для этого упражнения используйте имя пользователя и пароль **netadmin**.

Действие 3 В приглашении привилегированного режима введите команду **show sessions**. Вывод команды должен выглядеть следующим образом:

```
login as: netadmin

********** Warning  *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.
************************************************************^C
netadmin@10.10.10.3's password:

RouterX#show sessions
% No connections open
RouterX#
```

Действие 4 Введите команду **show users**, чтобы вывести список текущих пользователей, подключенных к маршрутизатору рабочей группы. Вывод команды должен выглядеть следующим образом:

```
RouterX#sh users
   Line      User      Host(s)       Idle       Location
*322 vty 0   netadmin  idle          00:00:00 10.10.10.134
 Interface   User           Mode     Idle     Peer Address
```

Действие 5 Пользователь «netadmin» связан с адресом вашего ПК, поскольку вы создали VPN-подключение во время действия 2 данной задачи.

Действие 6 Введите команду **conf t**, чтобы перейти к приглашению глобальной конфигурации.

Действие 7 Введите команду **line vty 0 4** для перехода в режим конфигурации линии VTY.

Действие 8 Введите команду **exec-timeout 30**, чтобы увеличить период таймера бездействия до 30 минут.

Действие 9 С помощью команды **end** верните приглашение режима EXEC. Вывод команды должен выглядеть следующим образом:

```
RouterX#conf t
Enter configuration commands, one per line. End with CNTL/Z.
RouterX(config)#line vty 0 4
RouterX(config-line)#exec-timeout 30
RouterX(config-line)#end
RouterX#
```

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- создано подключение ПК к маршрутизатору удаленной рабочей группы с помощью приложения PuTTY через туннель VPN;
- таймаут бездействия для линий VTY маршрутизатора увеличен до 30 минут;
- с помощью команды **show sessions** вы подтвердили отсутствие открытых сеансов маршрутизатора;
- с помощью команды **show users** вы определили, что являетесь единственным пользователем, подключенным к маршрутизатору.

Задача 3: Использование команд CLI Cisco IOS для управления сеансами Telnet и SSH

В этой задаче вы попрактикуетесь в запуске, приостановке и возобновлении сеансов Telnet и SSH. Для этого упражнения используйте имя пользователя и пароль **netadmin**. Кроме того, вам следует увеличить автоматический таймаут бездействия для линий виртуального терминала маршрутизатора рабочей группы до 30 минут на время выполнения этой лабораторной работы.

Процедура упражнения

Выполните следующие действия:

Действие 1 На маршрутизаторе рабочей группы откройте сеанс Telnet для коммутатора рабочей группы с помощью команды **telnet** *ip_адрес*.

Действие 2 Введите команду для перехода к приглашению привилегированного режима EXEC. Вывод команды должен выглядеть следующим образом:

```
RouterX#telnet 10.10.10.11
Trying 10.10.10.11 ... Open

**********  Предупреждение  *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.
************************************************************

User Access Verification

Username: netadmin
Password:
SwitchX>enable
Password:
SwitchX#
```

Действие 3 Введите команду **conf t**, чтобы перейти к приглашению глобальной конфигурации.

Действие 4 Введите команду **line vty 0 15** для перехода в режим конфигурации линии VTY.

Действие 5 Введите команду **exec-timeout 30**, чтобы увеличить период таймера бездействия до 30 минут.

Действие 6 С помощью команды **end** верните приглашение режима EXEC. Вывод команды должен выглядеть следующим образом:

```
SwitchX#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SwitchX(config)#line vty 0 15
SwitchX(config-line)#exec-timeout 30
SwitchX(config-line)#end
SwitchX#
```

Действие 7 Введите последовательность выхода **Ctrl-Shift-6**, **x** для приостановки сеанса и перехода к приглашению RouterX#.

Действие 8 Введите команду **show sessions** для отображения активных сеансов. Вывод на экран должен выглядеть следующим образом, но последовательность выхода не должна быть выделена жирным шрифтом.

```
SwitchX#<cntrl+shift+6,x>
RouterX#show sessions
Conn Host            Address         Byte  Idle Conn Name
* 1 10.10.10.11      10.10.10.11        0     0 10.10.10.11

RouterX#
```

Действие 9 Введите команду **ssh** *ip_адрес*, чтобы открыть второе подключение к коммутатору рабочей группы по протоколу SSH.

Примечание. Необходимо ввести пароль, связанный с именем пользователя «netadmin».

Вывод команды должен выглядеть следующим образом:

```
RouterX#ssh 10.10.10.11

********** Warning  *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.
************************************************************
Password:

SwitchX>
```

Действие 10 Введите последовательность выхода **Ctrl-Shift-6**, **x** для приостановки сеанса и перехода к приглашению RouterX#.

Действие 11 Введите команду **show sessions** для отображения активных сеансов. Вывод на экран должен выглядеть следующим образом, последовательность выхода не должна быть выделена жирным шрифтом.

```
SwitchX><ctrl+shift+6,x>
RouterX#show sessions
Conn Host         Address        Byte Idle Conn Name
  1 10.10.10.11      10.10.10.11       0   4 10.10.10.11
* 2 10.10.10.11      10.10.10.11       0   0

RouterX#
```

Действие 12 Введите команду **resume 1** для возобновления первого подключения к коммутатору рабочей группы. Обратите внимание, что в этом сеансе доступно приглашение привилегированного режима.

```
<ENTER>
RouterX#resume 1
[Resuming connection 1 to 10.10.10.11 ... ]
<ENTER>
SwitchX#show users
  Line    User    Host(s)       Idle    Location
* 1 vty 0   netadmin  idle         00:00:00 10.10.10.3
  2 vty 1   netadmin  idle         00:00:22 10.10.10.3

 Interface   User    Mode           Idle   Peer Address

SwitchX#
```

Действие 13 На коммутаторе создайте подключение к маршрутизатору рабочей группы по протоколу Telnet, не добавляя префикс «Telnet» перед адресом. Обратите внимание, что доступ к привилегированному режиму маршрутизатора предоставлен автоматически. Вывод команды должен выглядеть следующим образом:

```
SwitchX#10.10.10.3
Trying 10.10.10.3 ... Open

**********  Предупреждение  *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.
************************************************************^C

User Access Verification

Username: netadmin
Password:
RouterX#
```

Действие 14 Введите команду **show sessions**, чтобы вывести данные о сеансах, связанных с этим подключением. Вывод команды должен выглядеть следующим образом:

```
RouterX#show sessions
% No connections open
RouterX#
```


Примечание. К этому моменту вы создали Telnet-подключения маршрутизатора к коммутатору и коммутатора к маршрутизатору. Кроме того, создано SSH-подключение маршрутизатора к коммутатору.

Действие 15 Текущее представление – пользовательский режим EXEC маршрутизатора, доступ к которому получен через Telnet-подключение к коммутатору. Если вы введете одну последовательность выхода, появится приглашение Router# (сеанс 1). Однако если использовать *две* последовательности выхода, а затем нажать **x**, появится приглашение коммутатора.

Действие 16 Введите последовательность **Ctrl-Shift-6**, **Ctrl-Shift-6**, **x**. Обратите внимание, что **x** используется только один раз в конце. Появится приглашение коммутатора. Вывод команды должен выглядеть следующим образом:

```
RouterX#<ctrl-shift-6, ctrl-shift-6, x>
SwitchX#sh sessions
Conn Host           Address         Byte  Idle Conn Name
* 1 10.10.10.3      10.10.10.3         0     0 10.10.10.3

SwitchX#
```

Действие 17 Введите последовательность выхода **Ctrl-Shift-6**, **x** для приостановки исходного сеанса, инициированного на маршрутизаторе, и перехода к приглашению RouterX#. Вывод команды должен выглядеть следующим образом:

```
SwitchX#<ctrl-shift-6, x>
RouterX#sh sessions
Conn Host          Address         Byte Idle Conn Name
* 1 10.10.10.11      10.10.10.11        0   0 10.10.10.11
  2 10.10.10.11      10.10.10.11        0   7
```

Действие 18 Просмотрите выходные данные. Звездочкой (*) помечен номер 1. Это значит, что сеанс активен. Если вы нажмете клавишу **Enter** без добавления другого текста, сеанс будет автоматически возобновлен.

Действие 19 Нажмите клавишу **Enter** дважды. Первое нажатие возобновляет подключение к коммутатору, а второе интерпретируется на коммутаторе для возобновления сеанса коммутатора к маршрутизатору. Чтобы вернуться к приглашению маршрутизатора, необходимо нажать клавишу **Enter** третий раз. Вывод команды должен выглядеть следующим образом:

```
RouterX#<ENTER>
[Resuming connection 1 to 10.10.10.11 ... ]
<ENTER>
[Resuming connection 1 to 10.10.10.3 ... ]
<ENTER>
RouterX#
```

Действие 20 Введите последовательность **Ctrl-Shift-6**, **Ctrl-Shift-6**, **x** для возвращения к коммутатору. Вывод команды должен выглядеть следующим образом:

```
RouterX#<ctrl-shift-6, ctrl-shift-6, x>
SwitchX#
```

Действие 21 Закройте подключение к маршрутизатору с помощью команды **disconnect**. Ввод этой команды без численного значения интерпретируется как закрытие последнего созданного соединения. Необходимо подтвердить запрошенное действие. Вывод команды должен выглядеть следующим образом:

```
SwitchX#disconnect
Closing connection to 10.10.10.3 [confirm]
SwitchX#
```

Действие 22 Отмените изменение значения таймаута режима EXEC, вернув значение по умолчанию 10 минут. Вывод команды должен выглядеть следующим образом:

```
SwitchX#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SwitchX(config)#line vty 0 15
SwitchX(config-line)#exec-timeout 10
SwitchX(config-line)#end
SwitchX#
```

Действие 23 Используйте последовательность **Ctrl-Shift-6**, **x** для возвращения к маршрутизатору, затем введите команду **show sessions**. Вывод на экран должен выглядеть следующим образом:

```
SwitchX#<ctrl-shift-6, x>
RouterX#show sessions
Conn Host         Address        Byte Idle Conn Name
* 1 10.10.10.11      10.10.10.11       0   1 10.10.10.11
  2 10.10.10.11      10.10.10.11       0  39
```

Действие 24 Используйте команду **disconnect**, чтобы закрыть оба подключения к коммутатору. Вывод на экран должен выглядеть следующим образом:

```
RouterX#disconnect 1
Closing connection to 10.10.10.11 [confirm]
RouterX#disconnect 2
Closing connection to 10.10.10.11 [confirm]
RouterX#
```

Действие 25 Отмените изменение значения таймаута режима EXEC, вернув значение по умолчанию 10 минут. Вывод на экран должен выглядеть следующим образом:

```
RouterX#conf t
Enter configuration commands, one per line. End with CNTL/Z.
RouterX(config)#line vty 0 4
RouterX(config-line)#exec-timeout 10
RouterX(config-line)#end
RouterX#
```

Действие 26 Закройте SSH-подключение к маршрутизатору рабочей группы с помощью команды **logout**. Затем закройте VPN-подключение.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- инициированы Telnet-подключения между коммутатором и маршрутизатором рабочей группы;
- инициировано SSH-подключение между коммутатором и маршрутизатором рабочей группы;
- с помощью команды **show sessions** определены текущие подключения и их параметры, включая активные сеансы и номера сеансов;
- с помощью команды **show users** определены пользователи, подключенные в к коммутатору и маршрутизатору рабочей группы;
- с помощью последовательности выхода приостановлено используемое (активное) соединение (сеанс);
- с помощью команды **resume** выбрано открытое подключение (сеанс) для использования;
- с помощью команды **exec-timeout** возвращено исходное значение таймера на маршрутизаторе и коммутаторе рабочей группы (10 минут);
- все подключения закрыты с помощью команд **disconnect** и **logout**;
- завершена работа туннеля VPN от ПК к удаленной рабочей группе.

Лабораторная работа 5-1: Подключение к сети Интернет

Выполните упражнение этой лабораторной работы, чтобы применить на практике знания, полученные в соответствующем модуле.

Задачи упражнения

В этом упражнении вам следует настроить использование IP-адреса, полученного от DHCP-сервера, на Ethernet-интерфейсе PBC и включить PAT (преобразование адресов и портов). После выполнения этого упражнения вы будете способны сделать следующее:

- с помощью Cisco SDM настроить использование IP-адреса, полученного от DHCP-сервера, на Ethernet-интерфейсе PBC;
- с помощью Cisco SDM настроить на маршрутизаторе поддержку преобразования PAT для внутреннего Ethernet-интерфейса через Ethernet-интерфейс PBC;
- с помощью Cisco SDM проверить соответствие конфигурации требованиям лабораторной работы;
- с помощью интерфейса командной строки проверить работу преобразования PAT на Ethernet-интерфейсе PBC.

Иллюстрация задания

На рисунке ниже показано, что вы должны сделать во время данного упражнения.

Необходимые ресурсы

Ниже перечислены ресурсы и устройства, необходимые для выполнения упражнения.

- ПК, подключенный к удаленной лаборатории.
- Приложение для эмуляции терминала с поддержкой SSH.
- Информация о доступе к назначенному комплекту оборудования, полученная в лабораторной работе 2-1.
- Успешное выполнение лабораторной работы 4-9.

Список команд

В таблице приводится описание команд, используемых в упражнении.

Команды маршрутизатора Cisco IOS

Команда	Описание
clear ip nat translation *	Удаляет динамические преобразования NAT из таблицы преобразования.
ping *ip_адрес*	Общепринятое средство выявления проблем доступа к устройствам. Использует эхо-запросы и эхо-ответы пути ICMP, чтобы определить, активен ли удаленный хост. Команда **ping** также определяет количество времени, затрачиваемого на получение эхо-ответа.
show dhcp lease	Отображает адреса DHCP, арендуемые у сервера.
show ip nat translations	Отображает активные процессы преобразования NAT.

Подсказки

Для этой лабораторной работы нет подсказок.

Задача 1: Использование Cisco SDM для настройки подключения к Интернету через Ethernet

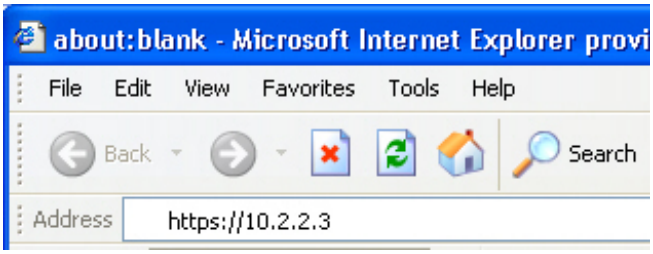
В этой задаче вам необходимо использовать ПО Cisco SDM, чтобы настроить Ethernet-подключение к РВС на использование DHCP-сервера для получения IP-адреса. Этот интерфейс также будет использоваться в режиме преобразования адресов портов NAT.

Процедура упражнения

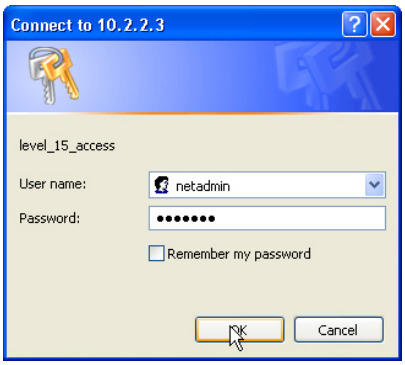
Выполните следующие действия:

Действие 1 Откройте VPN-подключение к удаленной рабочей группе.

Действие 2 Откройте окно Windows Internet Explorer и введите IP-адрес маршрутизатора рабочей группы в адресной строке в виде URL-адреса, например **https://10.*x*.*x*.3**.

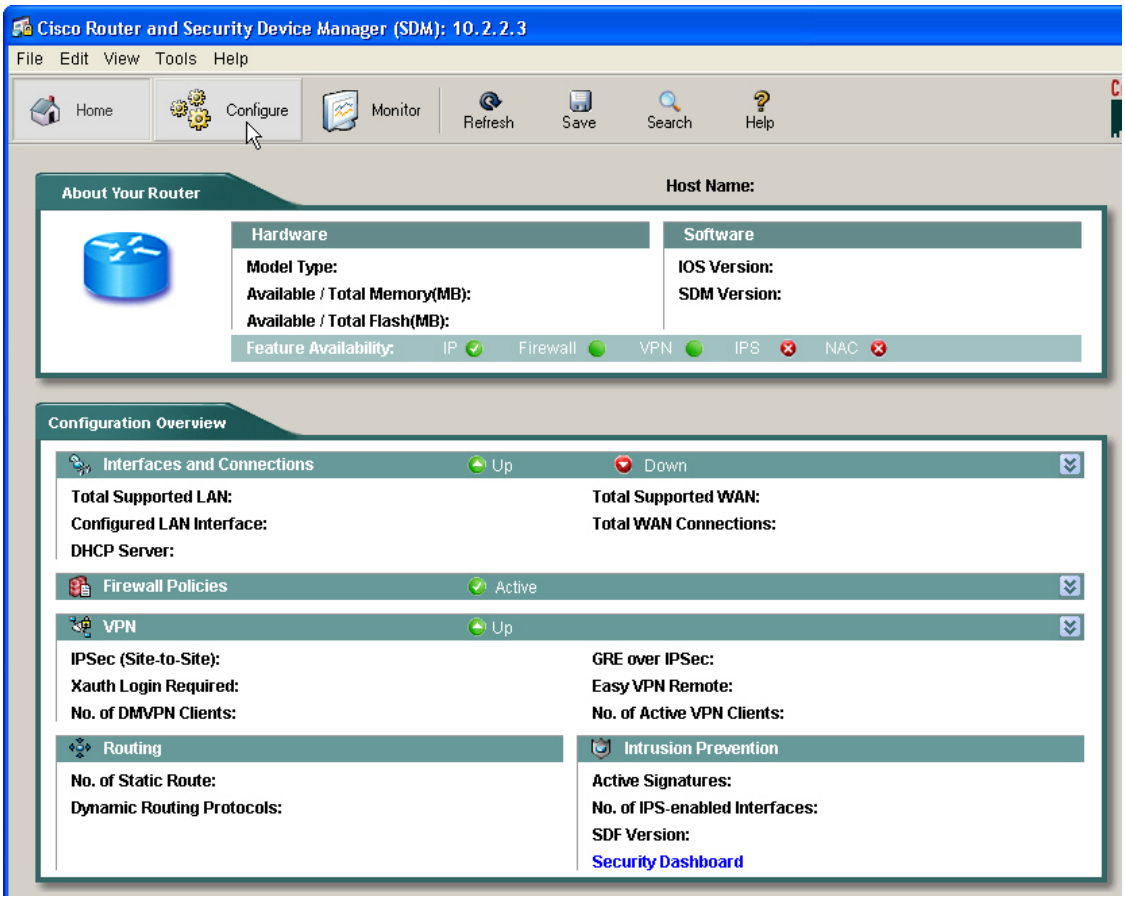


Действие 3 В открывшемся новом окне введите имя пользователя **netadmin** и пароль **netadmin**.

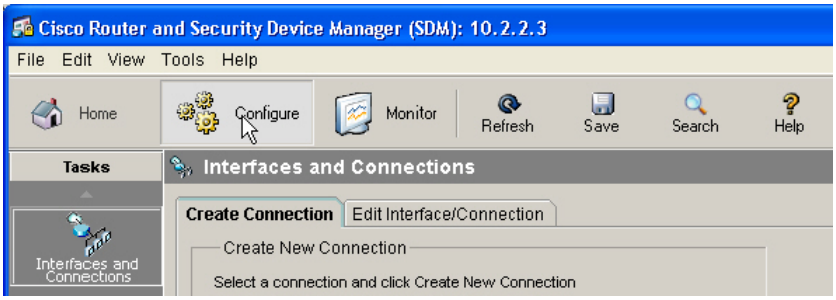


Действие 4 Может появиться следующее окно. В этом случае нажимайте кнопку **Yes** в этом и *всех* следующих окнах предупреждения системы безопасности.

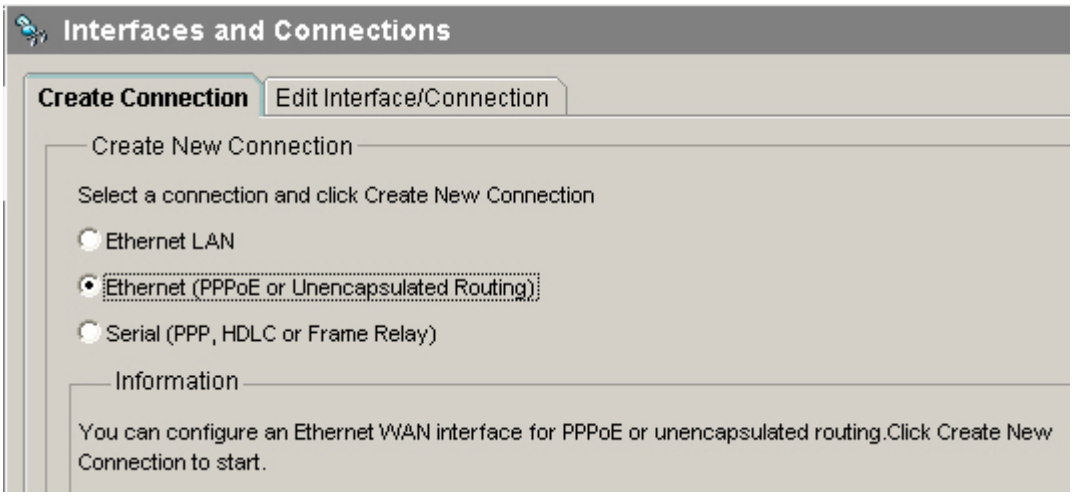
Действие 5 В конечном итоге должен появиться следующий экран.



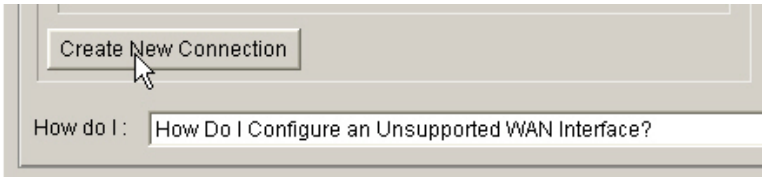
Действие 6 Перейдите на вкладку **Configure (Настройка)**.



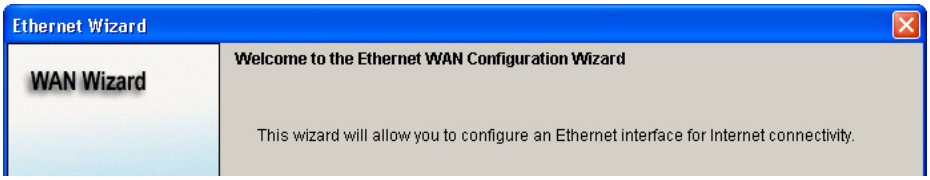
Действие 7 Перейдите на вкладку **Create Connection (Создать подключение)** и установите переключатель **Ethernet PPPoE or Unencapsulated Routing (Ethernet PPPoE или маршрутизация без инкапсуляции)**.



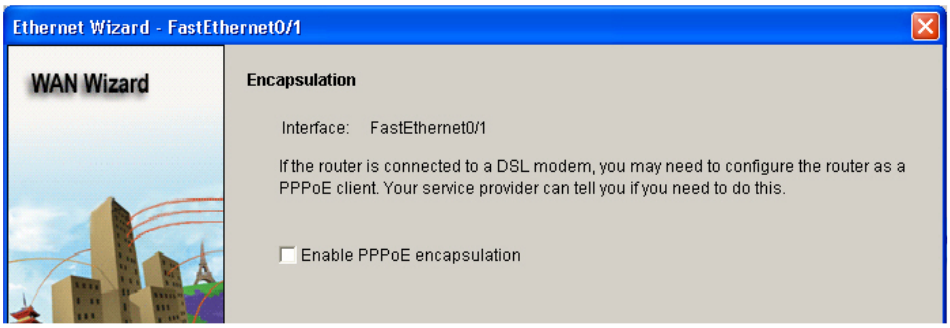
Действие 8 Нажмите кнопку **Create New Connection (Создать подключение)** в нижней части этой вкладки.



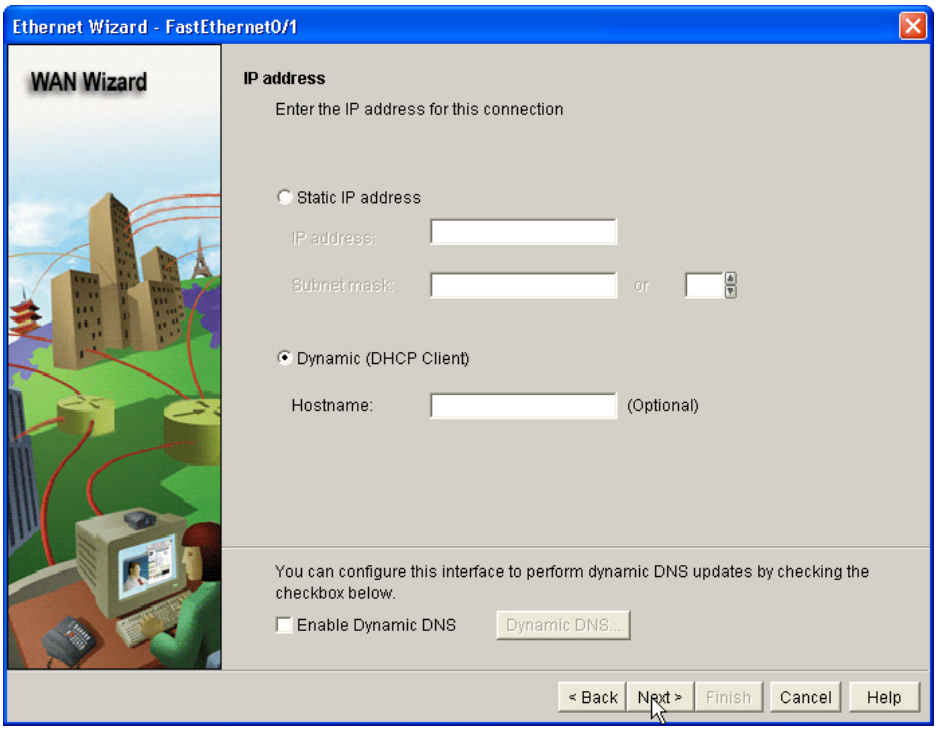
Действие 9 В окне «Welcome to the Ethernet WAN Configuration Wizard» нажмите кнопку **Next (Далее)** в нижней части области.



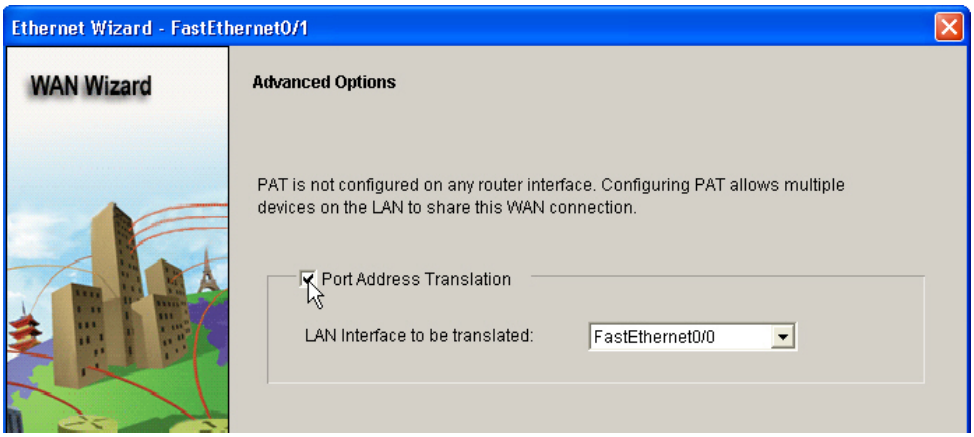
Действие 10 В окне «Encapsulation» (Инкапсуляция) не устанавливайте никаких флажков. Для продолжения нажмите кнопку **Next (Далее)** в нижней части панели.



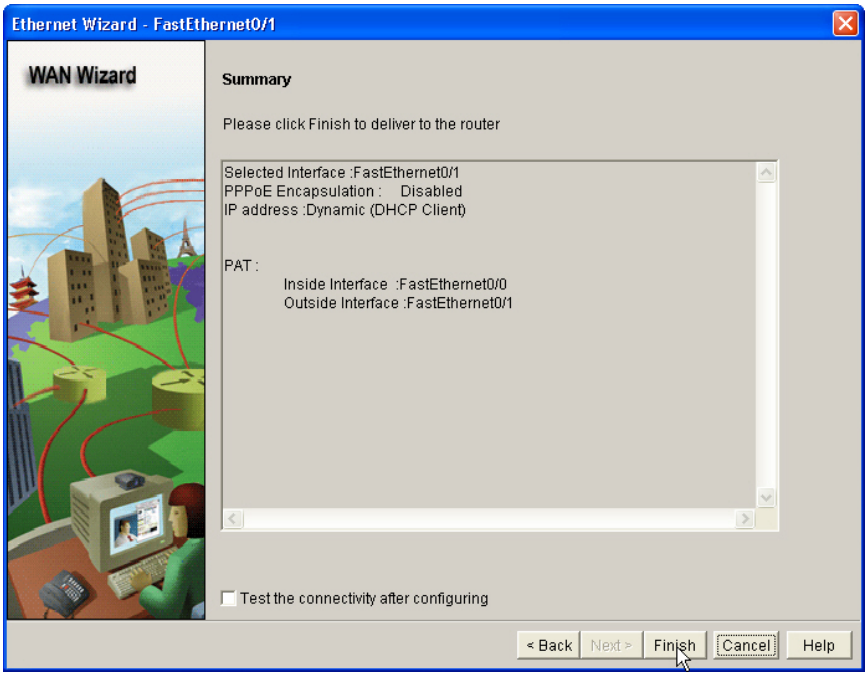
Действие 11 В окне «IP address» (IP-адрес) не устанавливайте никаких флажков. Должен быть установлен только переключатель **Dynamic (DHCP Client) (Динамическое (DHCP-клиент))**. Для продолжения нажмите кнопку **Next (Далее)**.



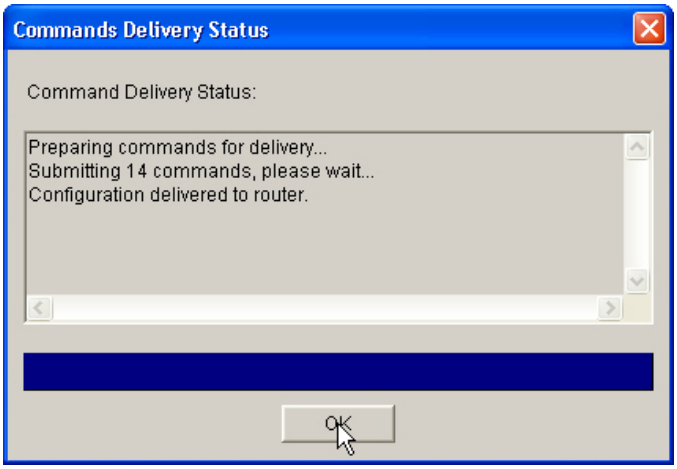
Действие 12 В окне «Advanced Options» (Дополнительные параметры) установите флажок **Port Address Translation (Преобразование адресов и портов)**. В поле **LAN Interface to Be Translated (Интерфейс ЛВС для преобразования)** автоматически добавится значение «FastEthernet0/0». Для продолжения нажмите кнопку **Next (Далее)** в нижней части панели.



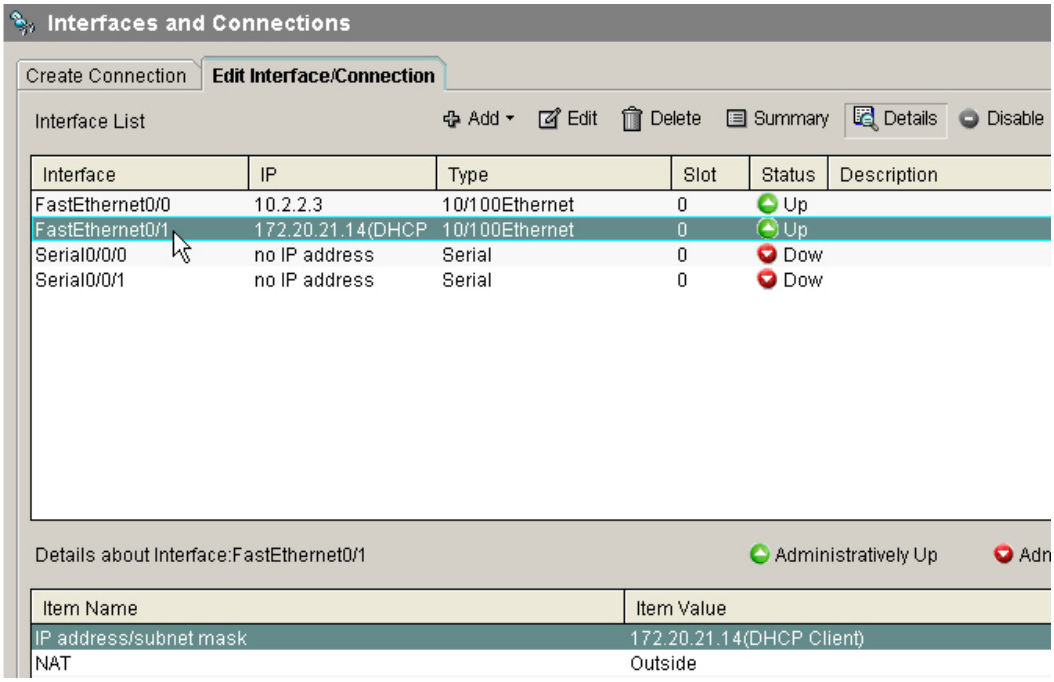
Действие 13 Ознакомьтесь с информацией в окне «Summary» (Сводка). Для завершения работы мастера нажмите кнопку **Finish (Готово)**.



Действие 14 Команды конфигурации переданы. Нажмите кнопку **OK**, чтобы закрыть окно «Commands Delivery Status» (Состояние доставки команд).



Действие 15 На вкладке «Edit Interface/Connection» (Изменить интерфейс/подключение), которая открылась после выполнения предыдущего действия, выберите **FastEthernet0/1**.



Действие 16 Убедитесь, что задан IP-адрес и после него отображается значение (DHCP). Также обратите внимание, что в нижней панели для NAT задано значение «Outside» (Внешнее).

Примечание. Для принудительно обновления этого экрана можно нажать кнопку «Refresh».

Действие 17 Закройте сеанс Cisco SDM и VPN-подключение.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- при проверке установлено, что интерфейс FastEthernet0/1 имеет адрес, полученный с помощью DHCP;
- во время действия 15 вы убедились, что интерфейс FastEthernet0/0 определен как *внутренний* интерфейс в конфигурации PAT;
- во время действия 15 вы убедились, что интерфейс FastEthernet0/1 определен как *внешний* интерфейс в конфигурации PAT.

Задача 2: Использование интерфейса командной строки для проверки работы PAT на маршрутизаторе рабочей группы

В этой задаче вам необходимо создать SSH-подключение к рабочей группе. Для отправки эхо-запроса по IP-адресу шлюза по умолчанию, предоставленного DHCP-сервером, необходимо использовать команды интерфейса командной строки. Затем с помощью команд **clear** и **show ip nat translations** выведите информацию о преобразовании PAT, сохраненную маршрутизатором рабочей группы.

Процедура упражнения

Выполните следующие действия:

Действие 1 С помощью приложения эмуляции терминала с поддержкой SSH подключитесь к маршрутизатору назначенной рабочей группы.

Действие 2 В приглашении привилегированного режима введите команду **show dhcp lease**. Вывод на экран должен выглядеть аналогично примеру ниже. Конкретные данные будут отличаться для каждого комплекта оборудования.

```
RouterX#show dhcp lease
Temp IP addr: 172.20.21.5 for peer on Interface: FastEthernet0/1
Temp sub net mask: 255.255.255.0
  DHCP Lease server: 172.20.21.254, state: 3 Bound
  DHCP transaction id: 1F7E
  Lease: 86400 secs, Renewal: 43200 secs, Rebind: 75600 secs
Temp default-gateway addr: 172.20.21.254
  Next timer fires after: 11:53:31
  Retry count: 0  Client-ID: 001a.6ca1.eed9
  Client-ID hex dump: 001A6CA1EED9
  Hostname: RouterX
RouterX#
```

Действие 3 Используйте команду **clear ip nat translation** * для очистки оставшихся данных NAT перед переходом к следующему действию.

Действие 4 Используйте команду **show ip nat translations**, чтобы убедиться в отсутствии данных.

```
RouterX#clear ip nat translation *
RouterX#show ip nat translations

RouterX#
```

Действие 5 Используйте команду **ping** для проверки связи с IP-адресом маршрутизатора по умолчанию, полученным из вывода.

Действие 6 Используйте команду **show ip nat translations**, чтобы проверить, выполнялось ли преобразование. Вывод на экран должен выглядеть следующим образом:

```
RouterX#show ip nat translations

RouterX#
```

Примечание. Вас может удивить отсутствие записей для успешно обработанного эхо-запроса. Причина в специфике процесса обработки эхо-запроса, который использует IP-адрес исходящего интерфейса в качестве IP-адреса источника. В проверке, которую вы только что выполнили, исходящий интерфейс (FastEthernet0/1) имеет IP-адрес 172.20.x.254, который *не* подлежит преобразованию. Чтобы это проверить, необходимо *перейти к коммутатору рабочей группы и повторить команду ping*, затем *вернуться к маршрутизатору* для просмотра записи преобразования.

Действие 7 В приглашении пользовательского режима EXEC коммутатора рабочей группы введите команду **ping** для IP-адреса маршрутизатора по умолчанию, который был использован в действии 5. Вывод на экран должен выглядеть следующим образом:

```
SwitchX>ping 172.20.21.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.20.21.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms
SwitchX>
```


Действие 8 Вернитесь к маршрутизатору рабочей группы и введите команду **show ip nat translations**.

```
RouterX#show ip nat translations
Pro Inside global   Inside local     Outside local   Outside global
icmp 172.20.21.5:33  10.10.10.11:33    172.20.21.254:33  172.20.21.254:33
```

Действие 9 Обратите внимание, что в выводе команды внутренний локальный IP-адрес относился к коммутатору рабочей группы, а внутренний глобальный IP-адрес относился к интерфейсу FastEthernet0/1.

Действие 10 Сохраните текущую конфигурацию в файле startup-config.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- IP-адрес шлюза по умолчанию успешно получен от DHCP-сервера;
- работоспособность PAT проверена с помощью эхо-запроса, сформированного локально на маршрутизаторе рабочей группы; в выводе команды **show ip nat translation** не отображались записи преобразования, это связано со свойствами пакетов эхо-запросов (с использованием IP-адресов источника);
- на коммутаторе рабочей группы вы повторно выполнили команда *ping*, а затем ввели команду **show ip nat translation**, эта последовательность пакетов инициировала преобразование;
- текущая конфигурация сохранена в файле startup-config.

Лабораторная работа 5-2: Подключение к главному офису

Выполните упражнение этой лабораторной работы, чтобы применить на практике знания, полученные в соответствующем модуле.

Задачи упражнения

В этом упражнении вы должны настроить последовательное подключение и статический маршрут. После выполнения этого упражнения вы будете способны сделать следующее:

- настроить последовательный интерфейс на использование PPP;
- настроить статический маршрут к заданной IP-сети, доступ к которой можно получить через последовательный интерфейс.

Иллюстрация задания

На рисунке ниже показано, что вы должны сделать во время данного упражнения.

Необходимые ресурсы

Ниже перечислены ресурсы и устройства, необходимые для выполнения упражнения.

- ПК, подключенный к удаленной лаборатории.
- Приложение для эмуляции терминала с поддержкой SSH.
- Информация о доступе к назначенному комплекту оборудования, полученная в лабораторной работе 2-1.
- Успешное выполнение лабораторной работы 5-1.

Список команд

В таблице приводится описание команд, используемых в упражнении.

Команды маршрутизатора Cisco IOS

Команда	Описание
description *описание*	Позволяет настроить для интерфейса текст описания.
interface serial 0/0/0	Активирует режим конфигурации указанного интерфейса.
encapsulation ppp	Задает протокол PPP в качестве метода инкапсуляции последовательного интерфейса.
ip address *ip_адрес маска*	Задает IP-адрес и маску интерфейса.
ip route *префикс_сети маска_префикса ip_адрес_следующего_перехода*	Устанавливает статический маршрут к месту назначения.
shutdown **no shutdown**	Отключает или включает интерфейс.
ping *ip_адрес*	Использует эхо-запросы и эхо-ответы ICMP, чтобы определить, активен ли удаленный хост.
show ip route	Отображает текущее состояние таблицы маршрутизации.
traceroute *ip_адрес*	Обнаруживает фактические IP-маршруты, по которым проходят пакеты к месту назначения.

Подсказки

Для упражнений этой лабораторной работы доступны следующие подсказки.

Таблица 1. Сведения о последовательном интерфейсе PBC

Рабочая группа	IP-адрес интерфейса PBC s0/0/0, маска 255.255.255.0	IP-адрес удаленного интерфейса PBC (маршрутизатор следующего перехода)	Удаленная сеть, доступная через s0/0/0	Удаленный хост, доступный через s0/0/0
A	**10.140.1.2**	**10.140.1.1**	**192.168.21.0**	**192.168.21.200**
B	**10.140.2.2**	**10.140.2.1**	**192.168.22.0**	**192.168.22.200**
C	**10.140.3.2**	**10.140.3.1**	**192.168.23.0**	**192.168.23.200**
D	**10.140.4.2**	**10.140.4.1**	**192.168.24.0**	**192.168.24.200**
E	**10.140.5.2**	**10.140.5.1**	**192.168.25.0**	**192.168.25.200**
F	**10.140.6.2**	**10.140.6.1**	**192.168.26.0**	**192.168.26.200**
G	**10.140.7.2**	**10.140.7.1**	**192.168.27.0**	**192.168.27.200**
H	**10.140.8.2**	**10.140.8.1**	**192.168.28.0**	**192.168.28.200**

Текущие пароли

Вход в консоль маршрутизатора	sanjose
Пароль «enable password» маршрутизатора	cisco
Пароль «enable secret» маршрутизатора	sanfran
Идентификатор пользователя для входа в систему маршрутизатора через линию VTY	netadmin
Пароль для входа в систему маршрутизатора через линию VTY	netadmin
Вход в консоль коммутатора	sanjose
Пароль «enable password» коммутатора	cisco
Пароль «enable secret» коммутатора	sanfran
Идентификатор пользователя для входа в систему коммутатора через линию VTY	netadmin
Пароль для входа в систему коммутатора через линию VTY	netadmin

Задача 1: Настройка последовательного интерфейса 0/0/0 маршрутизатора рабочей группы

В этой задаче вы должны назначить первому последовательному интерфейсу IP-адрес. Кроме того, для этого интерфейса необходимо настроить поддержку инкапсуляции PPP.

Процедура упражнения

Выполните следующие действия:

Действие 1 Подключитесь к консольному порту маршрутизатора назначенной рабочей группы и перейдите к приглашению привилегированного режима EXEC.

Действие 2 Введите команду **config terminal**, чтобы перейти к приглашению глобальной конфигурации.

Действие 3 Введите команду **interface s0/0/0** для перехода в режим конфигурации первого последовательного интерфейса.

Действие 4 Введите команду **encapsulation ppp**, чтобы включить инкапсуляцию PPP вместо используемой по умолчанию инкапсуляции HDLC.

Действие 5 Введите команду **ip address** *ip_адрес* **255.255.255.0**, указав IP-адрес PBC из таблицы 1 в начале этой лабораторной работы.

Действие 6 Введите команду **description Link to Main Office**, чтобы связать текст с интерфейсом.

Действие 7 Введите команду **no shutdown**, чтобы снова включить интерфейс.

Действие 8 Подождите несколько секунд для завершения вывода сообщений о статусе. Затем введите команду **end**, чтобы вернуться к приглашению режима EXEC.

Действие 9 При выполнении действий с 3 по 8 вывод на экран должен выглядеть следующим образом:

```
RouterX(config)#int s0/0/0
RouterX(config-if)#encapsulation ppp
RouterX(config-if)#ip address 10.140.10.2 255.255.255.0
RouterX(config-if)#description Link to Main Office
RouterX(config-if)#no shutdown
*Mar 26 21:10:35.451: %SYS-5-CONFIG_I: Configured from console by console
RouterX#
*Mar 26 21:10:35.983: %LINK-3-UPDOWN: Interface Serial0/0/0, changed state to up
RouterX#
*Mar 26 21:10:37.015: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up
RouterX(config-if)#end
```

Действие 10 Введите команду **show interface s0/0/0** для вывода текущего состояния последовательного интерфейса.

Действие 11 Обратите внимание на выделенные жирным шрифтом строки в приведенном ниже примере. Строки в вашем выводе должны быть такими же.

```
RouterX#show interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Description: Link to Main Office
  Internet address is 10.140.10.2/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, loopback not set
  Keepalive set (10 sec)
  ..
  Text omitted
```

Действие 12 Если канальный протокол последовательного интерфейса НЕ включен, убедитесь в правильном вводе информации.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- для протокола PPP корректно настроена пара имени пользователя и пароля;
- интерфейсу назначен IP-адрес из таблицы 1 этой лабораторной работы;
- с помощью команды **show interface** вы определили, что последовательный интерфейс *включен* и канальный протокол *включен*.

Задача 2: Проверка подключения к назначенной удаленной сети

Проверка подключения к удаленной сети с помощью команды **ping**, которая доступна только через только что настроенный последовательный интерфейс, будет неудачной. Затем вы должны использовать различные команды Cisco IOS для выяснения причины недоступности сети.

Процедура упражнения

Выполните следующие действия:

Действие 1 Введите команду **ping** *удаленный_хост*, используя назначенный IP-адрес удаленного хоста из таблицы 1 выше. Вывод на экран должен выглядеть следующим образом:

```
RouterX#ping 192.168.21.200

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.200, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
```

Действие 2 Введите команду **traceroute** *удаленный_хост*, используя IP-адрес из предыдущего действия. Вывод на экран должен выглядеть следующим образом:

```
RouterX#traceroute 192.168.21.200

Type escape sequence to abort.
Tracing the route to 192.168.21.200

 1 172.20.21.254 0 msec 4 msec 0 msec
 2 172.20.21.254 !H * !H
```

Действие 3 Вывод должен указывать, что пакеты отправлены на IP-адрес «Internet» через интерфейс FastEthernet 0/1.

Действие 4 Введите команду **show ip route** для просмотра текущей информации, сохраненной в таблице маршрутов. Вывод на экран должен выглядеть следующим образом:

```
RouterX#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
    D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
    N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
    E1 - OSPF external type 1, E2 - OSPF external type 2
    i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
    ia - IS-IS inter area, * - candidate default, U - per-user static route
    o - ODR, P - periodic downloaded static route

Gateway of last resort is 172.20.21.254 to network 0.0.0.0

   172.20.0.0/24 is subnetted, 1 subnets
C    172.20.21.0 is directly connected, FastEthernet0/1
   10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C    10.10.10.0/24 is directly connected, FastEthernet0/0
C    10.140.10.1/32 is directly connected, Serial0/0/0
C    10.140.10.0/24 is directly connected, Serial0/0/0
S*  0.0.0.0/0 [254/0] via 172.20.21.254
```

Действие 5 Обратите внимание на две строки примера, выделенные жирным шрифтом. Они указывают, что единственное место, в которое маршрутизатор может отправить пакеты с адресами назначения, не найденными в сетях с прямым подключением, – это маршрутизатор по умолчанию. Маршрутизатор по умолчанию определен с помощью адреса 0.0.0.0.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- с помощью команды **traceroute** вы определили, куда отправлены пакеты;
- с помощью команды **show ip route commands** вы определили, что в таблице маршрутизации нет записей, соответствующих сети, к которой вы пытались получить доступ; кроме того, в таблице маршрутизации присутствует запись для пересылки пакетов с «неизвестным» местом назначения, которая называется шлюзом last resort (шлюзом последней надежды).

Задача 3: Добавление записи статического маршрута для удаленной сети

Вы определили, что причина проблемы доступа к удаленной сети заключается в отсутствии записи в таблице маршрутизации для этой сети. В данной задаче вы должны устранить эту проблему, добавив запись статического маршрута в конфигурацию. Затем вы должны убедиться в том, что в результате этого действия проблема устранена. Обратите внимание, что для решения этой проблемы с помощью статического маршрута на удаленном маршрутизаторе должна быть соответствующая статическая запись, определяющая обратный маршрут к рабочей группе. Вы можете предполагать, что она уже создана администратором этого маршрутизатора.

Процедура упражнения

Выполните следующие действия:

Действие 1 В приглашении привилегированного режима введите команду **conf t** для перехода в режим глобальной конфигурации.

Действие 2 Введите команду **ip route** *удаленная_сеть маска_удаленной_сети IP_адрес_маршрутизатора_следующего_перехода*. Параметры этой команды можно найти в таблице 1. Вывод на экран должен выглядеть следующим образом:

```
RouterX(config)#ip route 192.168.2x.0 255.255.255.0 10.140.x.1
```

Действие 3 Введите команду **end** для выхода из режима конфигурации и возврата к приглашению режима EXEC.

Действие 4 Введите команду **show ip route** для просмотра текущей информации, сохраненной в таблице маршрутов. Вывод на экран должен выглядеть следующим образом:

```
RouterX#show ip route
..
..Текст пропущен
..
Gateway of last resort is 172.20.21.254 to network 0.0.0.0

   172.20.0.0/24 is subnetted, 1 subnets
C    172.20.21.0 is directly connected, FastEthernet0/1
S  192.168.21.0/24 [1/0] via 10.140.10.1
   10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C    10.10.10.0/24 is directly connected, FastEthernet0/0
C    10.140.10.1/32 is directly connected, Serial0/0/0
C    10.140.10.0/24 is directly connected, Serial0/0/0
S*  0.0.0.0/0 [254/0] via 172.20.21.254
RouterX#
```

Действие 5 Введите команду **ping** *удаленный_хост_сети* для проверки доступности удаленной сети. Вывод на экран должен выглядеть следующим образом:

```
RouterX#ping 192.168.21.200

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.200, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms
RouterX#
```

Действие 6 Введите команду **traceroute** *удаленный_хост_сети* для отображения пути пакетов к удаленной сети. Вывод на экран должен выглядеть следующим образом:

```
RouterX#traceroute 192.168.21.200

Type escape sequence to abort.
Tracing the route to 192.168.21.200

 1 10.140.10.1 12 msec * 12 msec
```

Действие 7 Обратите внимание, что в выводе трассировки маршрута присутствует только одна строка, так как расстояние до удаленной сети составляет один переход.

Действие 8 Сохраните текущую конфигурацию в файле startup-config.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- настроена запись статического маршрута, определяющая IP-адрес маршрутизатора следующего перехода для последовательного интерфейса 0/0/0 в конфигурации маршрутизатора рабочей группы;
- с помощью команды **show ip route** подтверждено наличие записи удаленной сети;
- с помощью команды **ping** успешно проверена доступность сети;
- с помощью команды **traceroute** вы убедились, что путь проходит через IP-подсеть, используемую на последовательном интерфейсе 0/0/0;
- текущая конфигурация сохранена в файле startup-config.

Лабораторная работа 5-3: Динамическая маршрутизация к главному офису

Выполните упражнение этой лабораторной работы, чтобы применить на практике знания, полученные в соответствующем модуле.

Задачи упражнения

В этом упражнении вам необходимо включить протокол динамической маршрутизации RIP. После выполнения этого упражнения вы будете способны сделать следующее:

- настроить протокол RIP на маршрутизаторе рабочей группы;
- проверить работу RIP;
- удалить ненужные статические маршруты к соседней сети.

Иллюстрация задания

На рисунке ниже показано, что вы должны сделать во время данного упражнения.

Необходимые ресурсы

Ниже перечислены ресурсы и устройства, необходимые для выполнения упражнения.

- ПК, подключенный к удаленной лаборатории.
- Приложение для эмуляции терминала с поддержкой SSH.
- Информация о доступе к назначенному комплекту оборудования, полученная в лабораторной работе 2-1.
- Успешное выполнение лабораторной работы 5-2.

Список команд

В таблице приводится описание команд, используемых в упражнении.

Команды

Команда	Описание
configure terminal	Активирует режим конфигурации с терминала.
end	Завершает режим конфигурации.
[**no**] **ip route**	Удаляет статический маршрут, настроенный ранее.
network *префикс_сети*	Задает список сетей для процесса маршрутизации RIP. Процесс RIP будет отправлять и отслеживать обновления маршрутов на интерфейсах, IP-адреса которых соответствуют указанной сети.
router rip	Активирует процесс маршрутизации RIP.
show ip protocol	Отображает текущие значения для различных свойств активных протоколов маршрутизации.
show ip route	Отображает текущее состояние таблицы маршрутизации.
traceroute *ip_адрес*	Обнаруживает фактические IP-маршруты, по которым проходят пакеты при перемещении к месту назначения.
version {**1** | **2**}	Указывает версию RIP, глобально применяемую на маршрутизаторе.

Подсказки

Таблица 1. Сведения об удаленном хосте

Рабочая группа	IP-адрес удаленного хоста в сетях, доступных через s0/0/0		
A	**192.168.21.200**	**192.168.121.200**	**192.168.221.200**
B	**192.168.22.200**	**192.168.122.200**	**192.168.222.200**
C	**192.168.23.200**	**192.168.123.200**	**192.168.223.200**
D	**192.168.24.200**	**192.168.124.200**	**192.168.224.200**
E	**192.168.25.200**	**192.168.125.200**	**192.168.225.200**
F	**192.168.26.200**	**192.168.126.200**	**192.168.226.200**
G	**192.168.27.200**	**192.168.127.200**	**192.168.227.200**
H	**192.168.28.200**	**192.168.128.200**	**192.168.228.200**

Эти адреса могут использоваться как адреса назначения в командах **ping** или traceroute. Они допустимы только для указанной рабочей группы.

Задача 1: Настройка протокола маршрутизации RIP на маршрутизаторе рабочей группы

В этой задаче вам необходимо настроить работу протокола маршрутизации RIP на маршрутизаторе рабочей группы. Затем необходимо использовать команды Cisco IOS для проверки работоспособности протокола.

Процедура упражнения

Выполните следующие действия:

Действие 1 В приглашении EXEC введите команду **show ip route** для отображения текущих записей таблицы маршрутизации. Вывод на экран должен выглядеть следующим образом:

```
RouterX#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
    D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
    N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
    E1 - OSPF external type 1, E2 - OSPF external type 2
    i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
    ia - IS-IS inter area, * - candidate default, U - per-user static route
    o - ODR, P - periodic downloaded static route

Gateway of last resort is 172.20.21.254 to network 0.0.0.0

   172.20.0.0/24 is subnetted, 1 subnets
C    172.20.21.0 is directly connected, FastEthernet0/1
S  192.168.21.0/24 [1/0] via 10.140.10.1
   10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C    10.10.10.0/24 is directly connected, FastEthernet0/0
C    10.140.10.1/32 is directly connected, Serial0/0/0
C    10.140.10.0/24 is directly connected, Serial0/0/0
S*  0.0.0.0/0 [254/0] via 172.20.21.254
```

Действие 2 Введите команду **configure terminal**, чтобы перейти к приглашению глобальной конфигурации.

Действие 3 Введите команду **router rip** для настройки протокола маршрутизации RIP.

Действие 4 Введите команду **network 10.0.0.0**, чтобы включить протокол RIP на интерфейсах, IP-адреса которых соответствуют адресу сети (в данном случае сети 10.0.0.0).

Действие 5 Введите команду **end** для выхода из режима конфигурации. Вывод на экран должен выглядеть следующим образом:

```
RouterX#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
RouterX(config)#router rip
RouterX(config-router)#network 10.0.0.0
RouterX(config-router)#end
```

Действие 6 Введите команду **show ip protocol** для отображения информации о протоколах маршрутизации IP, настроенных на маршрутизаторе. Вывод на экран должен выглядеть следующим образом:

```
RouterX#show ip protocol
Routing Protocol is "rip"
 Outgoing update filter list for all interfaces is not set
 Incoming update filter list for all interfaces is not set
 Sending updates every 30 seconds, next due in 0 seconds
 Invalid after 180 seconds, hold down 180, flushed after 240
 Redistributing: rip
 Default version control: send version 1, receive any version
  Interface       Send Recv Triggered RIP Key-chain
  FastEthernet0/0    1   1 2
  Serial0/0/0      1   1 2
 Automatic network summarization is in effect
 Maximum path: 4
 Routing for Networks:
  10.0.0.0
 Routing Information Sources:
  Gateway     Distance   Last Update
 Distance: (default is 120)
```

Действие 7 Обратите внимание, что в соответствии с выводом маршрутизатор будет отправлять обновления версии 1, но будет распознавать и использовать обновления версий 1 и 2.

Действие 8 Введите команды, необходимые для настройки RIP на использование версии 2. Вывод на экран должен выглядеть следующим образом:

```
RouterX#conf t
Enter configuration commands, one per line. End with CNTL/Z.
RouterX(config)#router rip
RouterX(config-router)#version 2
RouterX(config-router)#end
```

Действие 9 Введите команду **show ip protocol** для отображения информации о протоколах маршрутизации IP, настроенных на маршрутизаторе. Вывод на экран должен выглядеть следующим образом:

```
RouterX#show ip protocol
Routing Protocol is "rip"
 Outgoing update filter list for all interfaces is not set
 Incoming update filter list for all interfaces is not set
 Sending updates every 30 seconds, next due in 28 seconds
 Invalid after 180 seconds, hold down 180, flushed after 240
 Redistributing: rip
 Default version control: send version 2, receive version 2
  Interface       Send Recv Triggered RIP Key-chain
  FastEthernet0/0    2   2
  Serial0/0/0      2   2
 Automatic network summarization is in effect
 Maximum path: 4
 Routing for Networks:
  10.0.0.0
 Routing Information Sources:
  Gateway     Distance   Last Update
  10.140.10.1      120   00:00:01
 Distance: (default is 120)
```

Действие 10 Обратите внимание, что теперь RIP может отправлять и получать *только* обновления версии 2.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- вы включили протокол маршрутизации RIP;
- вы использовали команду **show ip protocol** для проверки работоспособности протокола;
- конфигурация была изменена для использования только обновлений RIP версии 2;
- для проверки этого изменения использована команда **show ip protocol**.

Задача 2: Замена существующего статического маршрута и проверка соединения

В этой задаче вам необходимо удалить статический маршрут, настроенный в предыдущей лабораторной работе. Кроме того, вы должны проверить соединение с удаленной сетью, полученной от протокола маршрутизации RIP.

Процедура упражнения

Выполните следующие действия:

Действие 1 Введите команду **show ip route** для вывода текущих записей таблицы маршрутизации. Вывод на экран должен выглядеть следующим образом:

```
RouterX#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
    D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
..
..Text omitted
..

Gateway of last resort is 172.20.21.254 to network 0.0.0.0

R  192.168.121.0/24 [120/1] via 10.140.10.1, 00:00:12, Serial0/0/0
   172.20.0.0/24 is subnetted, 1 subnets
C    172.20.21.0 is directly connected, FastEthernet0/1
R  192.168.131.0/24 [120/1] via 10.140.10.1, 00:00:12, Serial0/0/0
S  192.168.21.0/24 [1/0] via 10.140.10.1
   10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C    10.10.10.0/24 is directly connected, FastEthernet0/0
C    10.140.10.1/32 is directly connected, Serial0/0/0
C    10.140.10.0/24 is directly connected, Serial0/0/0
R  192.168.221.0/24 [120/2] via 10.140.10.1, 00:00:13, Serial0/0/0
S*  0.0.0.0/0 [254/0] via 172.20.21.254
```

Действие 2 Обратите внимание, что несколько сетевых записей получены с помощью обновлений RIP. В выводе они обозначены буквой «R». Однако статический маршрут по-прежнему используется для записи маршрута к сети 192.168.2*x*.0 (где *x* – номер комплекта оборудования). Эта запись обозначена буквой «S». Такой маршрут не использует преимущества динамических обновлений протокола RIP. Вспомните, для выбора маршрута, который добавляется в таблицу, используется административное расстояние. Значение для RIP равно 120, для статического маршрута – 1.

Действие 3 Введите команду **conf terminal**, чтобы войти в режим глобальной конфигурации.

Действие 4 Введите команду **no ip route 192.168.2x.0 255.255.255.0 10.140.10.1** для удаления записи статического маршрута из конфигурации.

Действие 5 Введите команду **end** для выхода из режима конфигурации.

Действие 6 Введите команду **show ip route 192.168.2*x*.0** , чтобы отобразить данные только для указанного маршрута. Вывод на экран должен выглядеть следующим образом:

```
RouterX#sh ip route 192.168.21.0
Routing entry for 192.168.21.0/24
 Known via "rip", distance 120, metric 1
 Redistributing via rip
 Last update from 10.140.10.1 on Serial0/0/0, 00:00:13 ago
 Routing Descriptor Blocks:
 * 10.140.10.1, from 10.140.10.1, 00:00:13 ago, via Serial0/0/0
   Route metric is 1, traffic share count is 1
```

Действие 7 Введите команду **traceroute 192.168.22*x*.200**, чтобы использовать протокол ICMP для отслеживания пути к хосту в сети. Вывод на экран должен выглядеть следующим образом:

```
RouterX#traceroute 192.168.221.200

Type escape sequence to abort.
Tracing the route to 192.168.221.200

 1 10.140.10.1 16 msec 12 msec 12 msec
 2 192.168.131.253 16 msec * 12 msec
```

Действие 8 Введите команду для сохранения конфигурации в файле startup-config.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- удален статический маршрут, настроенный в предыдущей лабораторной работе;
- удаление подтверждено с помощью команды **show ip route**;
- с помощью команды **traceroute** проверена доступность сети;
- текущая конфигурация сохранена в файле startup-config.

Лабораторная работа 6-1: Использование протокола обнаружения Cisco

Выполните упражнение этой лабораторной работы, чтобы применить на практике знания, полученные в соответствующем модуле.

Задачи упражнения

В этом упражнении вы будете использовать протокол обнаружения Cisco (Cisco Discovery Protocol, CDP) для получения информации о напрямую подключенных устройствах Cisco. Кроме того, вам следует отключить протокол CDP на некоторых интерфейсах. После выполнения этого упражнения вы будете способны сделать следующее:

- проверить выполнение протокола CDP на маршрутизаторе и коммутаторе рабочей группы;
- вывести информацию о соседних устройствах Cisco;
- в целях безопасности ограничить число интерфейсов под управлением протокола CDP;
- подтвердить изменения.

Иллюстрация задания

На рисунке ниже показано, что вы должны сделать во время данного упражнения.

Необходимые ресурсы

Ниже перечислены ресурсы и устройства, необходимые для выполнения упражнения.

- ПК, подключенный к удаленной лаборатории.
- Приложение для эмуляции терминала с поддержкой SSH.
- Информация о доступе к назначенному комплекту оборудования, полученная в лабораторной работе 2-1.
- Успешное выполнение лабораторной работы 5-3.

Список команд

В таблице приводится описание команд, используемых в упражнении.

Команды маршрутизатора Cisco IOS

Команда	Описание
[**no**] **cdp enable**	Включает протокол CDP на интерфейсе. Версия «no» этой команды отключает протокол CDP на интерфейсе.
[**no**] **cdp run**	Глобально включает протокол CDP на маршрутизаторе или коммутаторе. Версия «no» этой команды глобально отключает протокол CDP.
interface range interface *номеринтерфейса - номеринтерфейса*	Переводит в режим конфигурации группы интерфейсов. Это позволит применять следующие команды конфигурации ко всем указанным интерфейсам одновременно.
show cdp	Выводит глобальную данные по протоколу CDP, включая данные таймера и времени сохранения информации.
show cdp entry *	Выводит информацию об определенном соседнем устройстве, обнаруженном с помощью протокола CDP, символ * обозначает любые текущие записи.
show cdp interfaces	Выводит информацию об интерфейсах, на которых включен протокол CDP.
show cdp neighbors [**detail**]	Выводит подробную информацию о соседних устройствах, обнаруженных с помощью протокола CDP.
show cdp traffic	Выводит информацию о трафике между устройствами, собранную с помощью протокола CDP.

Подсказки

Для этого упражнения нет подсказок.

Задача 1: Использование протокола обнаружения Cisco на маршрутизаторе рабочей группы и управление им

В этой задаче вам необходимо использовать протокол CDP для получения информации о напрямую подключенных устройствах Cisco. Кроме того, вы должны проконтролировать, какие интерфейсы работают под управлением протокола CDP, так как информация, предоставляемая этим протоколом, может использоваться хакерами для получения данных, необходимых для использования уязвимости систем безопасности.

Процедура упражнения

Выполните следующие действия:

Действие 1 Подключитесь к удаленному маршрутизатору рабочей группы через терминальный сервер и введите необходимые команды и пароли, чтобы получить доступ к приглашению привилегированного режима EXEC.

Действие 2 Введите команду **show cdp**, чтобы убедиться, что протокол CDP включен и вывести глобальную информацию.

```
RouterX#show cdp
Global CDP information:
    Sending CDP packets every 60 seconds
    Sending a holdtime value of 180 seconds
    Sending CDPv2 advertisements is enabled
```

Действие 3 Введите команду **show cdp interface**, чтобы вывести список интерфейсов под управлением протокола CDP. Вывод на экран должен выглядеть следующим образом:

```
RouterX#show cdp interface
FastEthernet0/0 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
FastEthernet0/1 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
Serial0/0/0 is up, line protocol is up
  Encapsulation PPP
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
Serial0/0/1 is administratively down, line protocol is down
  Encapsulation HDLC
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
```

Действие 4 Введите команду **show cdp neighbors** для отображения всех известных устройств Cisco. Вывод на экран должен выглядеть следующим образом:

```
RouterX#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID    Local Intrfce   Holdtme  Capability Platform Port ID
MainRouter     Ser 0/0/0     167    R S I   2811   Ser 1/0
SwitchX.cisco.com
             Fas 0/0      137     S I    WS-C2960- Fas 0/2
```

Действие 5 Используя информацию, собранную во время предыдущего действия, введите команду **show cdp entry** для вывода подробных данных протокола CDP для маршрутизатора Cisco, полученных через последовательный интерфейс. Вывод на экран должен выглядеть следующим образом:

```
RouterX#show cdp entry MainRouter
-------------------------
Device ID: MainRouter
Entry address(es):
 IP address: 10.140.10.1
Platform: Cisco 2811, Capabilities: Router Switch IGMP
Interface: Serial0/0/0, Port ID (outgoing port): Serial1/0
Holdtime : 150 sec

Version :
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M),
Version 12.4(12), RELEASE SOFTWARE (fc1)
```

```
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 17-Nov-06 12:02 by prod_rel_team

advertisement version: 2
VTP Management Domain: ''
```

Действие 6 В выводе команды найдите IP-адрес удаленного устройства, сведения о программном обеспечении и платформе маршрутизатора.

Действие 7 Используя IP-адрес из вывода, полученный во время действия 5, вы можете попытаться войти в систему маршрутизатора MainRouter, однако эта попытка завершится неудачей, так как у MainRouter есть список контроля доступа (ACL) для защиты от несанкционированного доступа.

Действие 8 Введите команду **show cdp neighbors detail**, чтобы отобразить данные, аналогичные выводу команды **show cdp entry**. Однако команда **neighbors detail** выводит список всех известных соседних устройств без дополнительных параметров. Вывод на экран должен выглядеть следующим образом:

```
RouterX#show cdp neighbors detail
-------------------------
Device ID: MainRouter
Entry address(es):
 IP address: 10.140.10.1
Platform: Cisco 2811, Capabilities: Router Switch IGMP
Interface: Serial0/0/0, Port ID (outgoing port): Serial1/0
Holdtime : 167 sec

Version :
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version
12.4(12), RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 17-Nov-06 12:02 by prod_rel_team

advertisement version: 2
VTP Management Domain: ''

-------------------------
Device ID: SwitchX.cisco.com
Entry address(es):
 IP address: 10.10.10.11
Platform: cisco WS-C2960-24TT-L, Capabilities: Switch IGMP
Interface: FastEthernet0/0, Port ID (outgoing port): FastEthernet0/2
Holdtime : 135 sec

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(25)SEE2,
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 28-Jul-06 11:57 by yenanh

advertisement version: 2
Protocol Hello: OUI=0x00000C, Protocol ID=0x0112; payload len=27,
value=00000000FFFFFFFF010221FF000000000000001A6D446C80FF0000
VTP Management Domain: ''
Native VLAN: 1
Duplex: half
```

Действие 9 Исходя из вывода команд **cdp** и информации о топологии можно определить, какие интерфейсы подключены к сетевой инфраструктуре. На всех интерфейсах, которые не подключены к инфраструктуре, протокол CDP должен быть отключен, так как он позволяет хакерам получить сведения о сети. С точки зрения маршрутизаторов рабочей группы на интерфейсе fa0/1 и Serial 0/0/1 протокол CDP должен быть отключен.

Действие 10 В режиме глобальной конфигурации введите команду **interface fa0/1**, а затем команду **no cdp enable** для отключения протокола CDP только на этом интерфейсе.

Действие 11 Введите ту же последовательность команд для отключения протокола CDP на Serial 0/0/1, затем вернитесь к приглашению привилегированного режима.

Действие 12 Введите команду **show cdp interface** чтобы убедиться, что протокол CDP работает только на интерфейсах Fa0/0 и s0/0/0. Вывод на экран должен выглядеть следующим образом:

```
RouterX#show cdp interface
FastEthernet0/0 is up, line protocol is up
 Encapsulation ARPA
 Sending CDP packets every 60 seconds
 Holdtime is 180 seconds
Serial0/0/0 is up, line protocol is up
 Encapsulation PPP
 Sending CDP packets every 60 seconds
 Holdtime is 180 seconds
```

Действие 13 После подтверждения изменений конфигурации сохраните ее в файле startup-config.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- вы проанализировали вывод протокола CDP о соседних, напрямую подключенных устройствах Cisco;
- вы отключили протокол CDP на интерфейсах, которые не подключены к инфраструктуре сети;
- конфигурация маршрутизатора рабочей группы сохранена в файле startup-config.

Задача 2: Использование протокола обнаружения Cisco на коммутаторе рабочей группы и управление им

В этой задаче вам необходимо использовать протокол CDP для получения информации о напрямую подключенных к коммутатору рабочей группы устройствах Cisco. Для обеспечения безопасности вам необходимо проконтролировать, какие интерфейсы работают под управлением протокола CDP. Скорее всего коммутатор будет первым сетевым устройством на пути потенциального хакера.

Процедура упражнения

Выполните следующие действия:

Действие 1 Подключитесь к удаленному коммутатору рабочей группы через терминальный сервер и введите необходимые команды и пароли, чтобы получить доступ к приглашению привилегированного режима EXEC.

Действие 2 Введите команду **show cdp**, чтобы убедиться, что протокол CDP включен и вывести глобальную информацию. Вывод на экран должен выглядеть следующим образом, часть текста опущена для экономии пространства.

```
SwitchX#show cdp interface
FastEthernet0/1 is up, line protocol is up
 Encapsulation ARPA
 Sending CDP packets every 60 seconds
 Holdtime is 180 seconds
FastEthernet0/2 is up, line protocol is up
 Encapsulation ARPA
 Sending CDP packets every 60 seconds
 Holdtime is 180 seconds
FastEthernet0/3 is administratively down, line protocol is down
 Encapsulation ARPA
 Sending CDP packets every 60 seconds
 Holdtime is 180 seconds
FastEthernet0/4 is administratively down, line protocol is down
 Encapsulation ARPA
..
..Text omitted
..
GigabitEthernet0/2 is administratively down, line protocol is down
 Encapsulation ARPA
 Sending CDP packets every 60 seconds
 Holdtime is 180 seconds
```

Действие 3 Введите команду **show cdp neighbors** для отображения устройств Cisco, подключенных напрямую. Вывод на экран должен выглядеть следующим образом:

```
SwitchX#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID      Local Intrfce     Holdtme  Capability  Platform  Port ID
RouterX.cisco.com
               Fas 0/2           150      R S I       2811      Fas 0/0
```

Действие 4 Обратите внимание, что обнаружено только одно соседнее устройство – маршрутизатор рабочей группы. Эти данные соответствуют схеме сети, так как протокол CDP должен выполняться только на интерфейсе Fa0/2.

Действие 5 Введите необходимые команды, чтобы протокол CDP был активен только на интерфейсе fa0/2. Вывод на экран должен выглядеть следующим образом:

```
SwitchX#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SwitchX(config)#interface range fa0/1 - 24, gi0/1 - 2
SwitchX(config-if-range)#no cdp enable
SwitchX(config-if-range)#interface fa0/2
% Command exited out of interface range and its sub-modes.
 Not executing the command for second and later interfaces
SwitchX(config-if)#cdp enable
SwitchX(config-if)#end
```

Действие 6 Введите команду **show cdp interface**, чтобы убедиться в том, что изменения применены. Вывод на экран должен выглядеть следующим образом:

```
SwitchX#sh cdp interface
FastEthernet0/2 is up, line protocol is up
 Encapsulation ARPA
 Sending CDP packets every 60 seconds
 Holdtime is 180 seconds
```


Действие 7 Введите команду **show cdp traffic** для просмотра информации о типе отправляемых и получаемых обновлений CDP. Эта информация может быть полезна, если вы подозреваете, что в процессе CDP возникли проблемы. Вывод на экран должен выглядеть следующим образом:

```
SwitchX#sh cdp traffic
CDP counters :
    Total packets output: 645, Input: 164
    Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
    No memory: 0, Invalid packet: 0, Fragmented: 0
    CDP version 1 advertisements output: 0, Input: 0
    CDP version 2 advertisements output: 645, Input: 164
```

Действие 8 После проверки работоспособности и изменений конфигурации сохраните конфигурацию в файле startup-config.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- вы ознакомились со списком непосредственно подключенных соседних устройств Cisco в выводе команды cdp коммутатора рабочей группы;
- протокол CDP отключен на интерфейсах, которые не подключены к инфраструктуре сети;
- вы подтвердили отсутствие ошибок в процессе обновления CDP с помощью команды **show cdp traffic**;
- текущая конфигурация сохранена в файле startup-config.

Лабораторная работа 6-2: Управление параметрами запуска маршрутизатора

Выполните упражнение этой лабораторной работы, чтобы применить на практике знания, полученные в соответствующем модуле.

Задачи упражнения

В этом упражнении вам необходимо внести изменения для управления режимом запуска маршрутизатора. После выполнения этого упражнения вы будете способны сделать следующее:

- вывести конфигурационный регистр, заменить его указанным значением и вернуть исходное значение;
- исходя из вывода определить, какая конфигурация отображается – текущая активная конфигурация или загрузочная конфигурация, сохраненная в файле startup-config;
- изменить последовательность загружаемых файлов Cisco IOS при запуске, используя последовательный список команд boot system;
- пранализировать перезагрузку и проверить, какая из инструкций загрузки обрабатывалась для получения работающего двоичного файла Cisco IOS.

Иллюстрация задания

На рисунке ниже показано, что вы должны сделать во время данного упражнения.

Необходимые ресурсы

Ниже перечислены ресурсы и устройства, необходимые для выполнения упражнения.

- ПК, подключенный к удаленной лаборатории.
- Приложение для эмуляции терминала с поддержкой SSH.
- Информация о доступе к назначенному комплекту оборудования, полученная в лабораторной работе 2-1.
- Успешное выполнение лабораторной работы 6-1.

Список команд

В таблице приводится описание команд, используемых в упражнении.

Команды маршрутизатора Cisco IOS

Команда	Описание
boot system flash [*имя_файла*]	Указывает имя файла с образом системы, который загружается из флэш-памяти при запуске маршрутизатора.
boot system tftp *имя_файла ip-адрес_сервера*	Указывает имя файла и IP-адрес (параметр *ip-адрес_сервера)* образа системы, который загружается с TFTP-сервера при запуске маршрутизатора.
config-register *значение*	Изменяет параметры конфигурационного регистра, *значение* – это шестнадцатеричное число.
show flash	Отображает формат и содержимое файловой системы флэш-памяти.
show running-config	Отображает текущую активную конфигурацию.
show startup-config	Отображает содержимое конфигурации, которая хранится в NVRAM и будет использоваться при следующей перезагрузке маршрутизатора.
show version	Отображает информацию о загруженной версии ПО, а также информацию об устройстве и аппаратном обеспечении.

Подсказки

Для упражнений этой лабораторной работы доступны следующие подсказки.

Таблица 1. IP-адреса TFTP-сервера

Рабочая группа	IP-адрес TFTP-сервера	Рабочая группа	IP-адрес TFTP-сервера
A	**10.2.2.1**	**E**	**10.6.6.1**
B	**10.3.3.1**	**F**	**10.7.7.1**
C	**10.4.4.1**	**G**	**10.8.8.1**
D	**10.5.5.1**	**H**	**10.9.9.1**

Задача 1: Изменение конфигурационного регистра

В этой задаче вам необходимо изменить значение конфигурационного регистра и проверить его установку. Затем вы должны восстановить исходное значение конфигурационного регистра, которое использовалось в начале этой задачи.

Процедура упражнения

Выполните следующие действия:

Действие 1 Подключитесь к удаленному маршрутизатору рабочей группы через терминальный сервер и введите необходимые команды и пароли, чтобы получить доступ к приглашению привилегированного режима EXEC.

Действие 2 Введите команду **show version** и нажмите кнопку **ПРОБЕЛ** для отображения вывода. Вывод на экран должен выглядеть следующим образом:

```
RouterX#show version
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M),
Version 12.4(12), RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 17-Nov-06 12:02 by prod_rel_team

ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)

RouterX uptime is 2 minutes
System returned to ROM by reload at 23:05:39 UTC Fri Mar 30 2007
System image file is "flash:c2800nm-advipservicesk9-mz.124-12.bin"

This product contains cryptographic features and is subject to United
..
..Text omitted
..
Cisco 2811 (revision 53,50) with 249856K/12288K bytes of memory.
Processor board ID FTX1050A3Q6
2 FastEthernet interfaces
2 Serial(sync/async) interfaces
1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bits wide with parity enabled.
239K bytes of non-volatile configuration memory.
62720K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102
```

Действие 3 Запишите значение конфигурационного регистра (в том виде, в котором оно появилось) в следующей строке.

_____

Действие 4 В режиме глобальной конфигурации введите команду **config-register 0x2104** для изменения параметра конфигурации.

```
RouterX#conf t
Enter configuration commands, one per line. End with CNTL/Z.
RouterX(config)#config-register 0x2104
```


Действие 5 Выйдите из режима глобальной конфигурации и введите команду **show version** для отображения нового значения. Вывод на экран должен выглядеть следующим образом:

```
RouterX(config)#^Z
RouterX#
RouterX#show version
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version
12.4(12), RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 17-Nov-06 12:02 by prod_rel_team

ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)

RouterX uptime is 8 minutes
System returned to ROM by reload at 23:05:39 UTC Fri Mar 30 2007
..
..Text omitted
..
239K bytes of non-volatile configuration memory.
62720K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102 (will be 0x2104 at next reload)

RouterX#
```

Действие 6 Вы увидите, что новое значение не будет активно до следующей перезагрузки.

Действие 7 При необходимости можно ввести команду **show running-config** для поиска параметра config-register, однако он не будет отображаться, если НЕ является частью текущей конфигурации.

Действие 8 Введите команды, необходимые для восстановления значения конфигурационного регистра по умолчанию, записанного во время действия 3. После этого введите команду **show version** и убедитесь, что исходное значение конфигурационного регистра восстановлено.

Действие 9 Иногда студентам будет трудно отличить, к какой конфигурации относится вывод – к текущей или к загрузочной.

Действие 10 Введите команду **show running-config** и используйте команду **q**, чтобы завершить вывод данных после отображения первого экрана. Вывод на экран должен выглядеть следующим образом:

```
RouterX#show running-config
Building configuration...

Current configuration : 2170 bytes
!
version 12.4
..
..Text omitted
..
 --More--q
```

Действие 11 Обратите внимание, что этот вывод начинается со слов «Building configuration». Эта особенность объясняется тем, что текущая конфигурация НЕ является файлом. Это значения параметров, сохраненные в исполняемой программе Cisco IOS.

Действие 12 Введите команду **show startup-config** и используйте команду **q**, чтобы завершить вывод данных после отображения первого экрана. Вывод на экран должен выглядеть следующим образом:

```
RouterX#sh startup-config
Using 2170 out of 245752 bytes
!
version 12.4
..
..Text omitted
..
 --More--q
```

Действие 13 Обратите внимание, что вывод в данном примере включают слова «Using 2170 out of 245 752 bytes». Это значит, что для хранения файла конфигурации используется определенный объем NVRAM.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- вы проверили и записали текущее значение конфигурационного регистра;
- вы изменили значение регистра конфигурации, вывели результат команды **show version** и определили, что значение изменено, но это изменение вступит в силу только после перезапуска маршрутизатора;
- вы вернули исходное значение конфигурационного регистра;
- вы отобразили и определили различия между текущей и загрузочной конфигурациями в выводе команд **show**.

Задача 2: Обзор файловой системы флэш-памяти и добавление команд системы загрузки

В этой задаче вы должны определить, какой файл ПО Cisco IOS используется. Затем вам необходимо добавить три команды boot system, изменяющие режим по умолчанию для процесса выбора файла при запуске. При изменении процесса загрузки необходимо проявлять крайнюю осторожность, поскольку в случае ошибки маршрутизатор стать недоступным. Обычно этот процесс выполняет только старший сетевой администратор.

Процедура упражнения

Выполните следующие действия:

Действие 1 Введите команду **show flash:** для вывода списка файлов, хранятся во флэш-памяти. Вывод на экран должен выглядеть следующим образом:

```
RouterX#show flash:
-#- --length-- -----date/time------ path
1   36232088 Mar 28 2007 17:27:46 +00:00 c2800nm-advipservicesk9-mz.124-12.bin
2       1823 Dec 14 2006 08:25:40 +00:00 sdmconfig-2811.cfg
3    4734464 Dec 14 2006 08:26:10 +00:00 sdm.tar
4     833024 Dec 14 2006 08:26:26 +00:00 es.tar
5    1052160 Dec 14 2006 08:26:46 +00:00 common.tar
6       1038 Dec 14 2006 08:27:02 +00:00 home.shtml
7     102400 Dec 14 2006 08:27:24 +00:00 home.tar
8     491213 Dec 14 2006 08:27:48 +00:00 128MB.sdf

20557824 bytes available (43458560 bytes used)
```


Действие 2 Обратите внимание, что двоичный файл Cisco IOS имеет расширение BIN. Другие файлы (в примере выше) относятся к программе настройки Cisco SDM. Во флэш-памяти может быть несколько образов Cisco IOS. Запишите имя файла Cisco IOS в следующей строке (в данном примере c2800nm-advipservicesk9-mz.124-12.bin).

Действие 3 Первый обнаруженный во флэш-памяти двоичный файл определяет образ Cisco IOS, загружаемый при запуске. С помощью команд конфигурации **boot system flash** *filename.bin* можно изменить этот порядок.

Примечание. Использование команд boot system требуется крайней осторожности, поскольку в случае ошибки запуск маршрутизатора будет невозможен, и для восстановления процесса загрузки потребуется много времени. Поэтому изменение файлов Cisco IOS во флэш-памяти и последовательности загрузки, как правило, выполняется старшими системными администраторами.

Действие 4 В приглашении глобальной конфигурации введите команду **boot system tftp** *имя_файла адрес_tftp*, где *имя_файла* – это имя, записанное во время действия 2, а *адрес_tftp* – IP-адрес TFTP-сервера рабочей группы, который можно найти в таблице 1. Если введена эта команда, маршрутизатор при перезагрузке пытается найти и загрузить файл Cisco IOS с указанного TFTP-сервера. Вывод на экран должен выглядеть следующим образом:

```
RouterX(config)#boot system tftp c2800nm-advipservicesk9-mz.124-12.bin 10.x.x.1
```

Действие 5 Введите **boot system flash** *имя_файла*, где *имя_файла* – это имя, скопированное во время действия 2. При обработке этой команды маршрутизатор попытается загрузить файл Cisco IOS из флэш-памяти, используя указанное имя файла. Вывод на экран должен выглядеть следующим образом:

```
RouterX(config)#boot system flash c2800nm-advipservicesk9-mz.124-12.bin
```

Действие 6 Введите **boot system flash**. Имя файла вводить не нужно. При обработке этой команды маршрутизатор будет загружаться с использованием первого обнаруженного во флэш-памяти файла Cisco IOS. Вывод на экран должен выглядеть следующим образом:

```
RouterX(config)#boot system flash
```

Действие 7 Введите команду для выхода из режима конфигурации.

Действие 8 Введите команду **show run** и проанализируйте вывод, чтобы убедиться в правильности ввода команд системы загрузки. Ваш вывод должен быть аналогичен примеру ниже, но имена файлов и хоста должны соответствовать вашей рабочей группе:

```
..
..Text omitted
..
hostname RouterX
!
boot-start-marker
boot system tftp c2800nm-advipservicesk9-mz.124-12.bin 10.x.x.1
boot system flash c2800nm-advipservicesk9-mz.124-12.bin
boot system flash
boot-end-marker
!
```

Действие 9 Внесите все необходимые изменения перед переходом к следующему действию.

Действие 10 Введите команду **copy run start** для сохранения текущей конфигурации в NVRAM.

Примечание. Длительность перезагрузки может быть разной (минимум 5 – 10 минут) в зависимости от аппаратного обеспечения маршрутизатора и производительности TFTP-сервера. Перезагрузка из флэш-памяти занимает 2 – 3 минуты для того же аппаратного обеспечения маршрутизатора.

Действие 11 Введите и подтвердите команду **reload**. Проанализируйте вывод, который отображается при перезагрузке. В следующей строке укажите, где по-вашему мнению, находится файл Cisco IOS для загрузки.

Действие 12 Вывод на экран должен выглядеть следующим образом:

```
RouterX#reload
Proceed with reload? [confirm]<ENTER>

*Apr 6 18:17:24.619: %SYS-5-RELOAD: Reload requested by console. Reload
Reason: Reload Command.

System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)

..
..Text omitted
..
<ENTER><ENTER>
*Apr 6 18:22:16.311: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
********** Warning  *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.

************************************************************^


User Access Verification

Password:
```

Действие 13 После завершения перезагрузки маршрутизатора дважды нажмите клавишу **Enter**, чтобы перейти к приглашению входа в систему. Введите данные для перехода в привилегированный режим EXEC.

Действие 14 Введите команду **show version** и проанализируйте выходные данные, чтобы подтвердить расположение файла Cisco IOS. Вывод на экран должен выглядеть следующим образом:

```
RouterX#sh version
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version
12.4(12), RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 17-Nov-06 12:02 by prod_rel_team

ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)

RouterX uptime is 1 minute
```



```
System returned to ROM by reload at 18:17:24 UTC Fri Apr 6 2007
System image file is "tftp://10.x.x.1/c2800nm-advipservicesk9-mz.124-12.bin"

..
..Текст пропущен
..
 --More--q
```

Действие 15 Если при загрузке с TFTP-сервера возникли проблемы, в выводе **show version** появится следующая строка:

```
System image file is "flash:c2800nm-advipservicesk9-mz.124-12.bin"
```

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- вы определили и записали текущий двоичный файл Cisco IOS, сохраненный во флэш-памяти;
- вы добавили три команды boot system для применения следующей последовательности поиска файла для загрузки при перезапуске маршрутизатора:
  - сначала указанный файл Cisco IOS ищется на TFTP-сервере;
  - в случае неудачи осуществляется поиск указанного файла Cisco IOS во флэш-памяти;
  - в последнюю очередь используется первый файл Cisco IOS, обнаруженный во флэш-памяти.
- вы перезагрузили маршрутизатор и с помощью вывода определили, какая из команд boot system обнаружила системный файл для запуска;
- с помощью вывода команды **show version** вы определили, какой метод используется.

Лабораторная работа 6-3: Управление устройствами Cisco

Выполните упражнение этой лабораторной работы, чтобы применить на практике знания, полученные в соответствующем модуле.

Задачи упражнения

В этом упражнении вы воспользуетесь командами **copy** и **debug** ПО Cisco IOS. После выполнения этого упражнения вы будете способны сделать следующее:

- сохранить текущую конфигурацию на удаленном TFTP-сервере;
- загружать и отправлять файлы конфигурации;
- копировать и удалять файлы в локальной флэш-памяти;
- перед использованием команд отладки убедиться, что нагрузка на маршрутизатор незначительна;
- включить и отключить отладку.

Иллюстрация задания

На рисунке ниже показано, что вы должны сделать во время данного упражнения.

Необходимые ресурсы

Ниже перечислены ресурсы и устройства, необходимые для выполнения упражнения.

- ПК, подключенный к удаленной лаборатории.
- Приложение для эмуляции терминала с поддержкой SSH.
- Информация о доступе к назначенному комплекту оборудования, полученная в лабораторной работе 2-1.
- Успешное выполнение лабораторной работы 6-2.

Список команд

В таблице приводится описание команд, используемых в упражнении.

Команды маршрутизатора Cisco IOS

Команда	Описание
copy running-config tftp	Многострочная команда, которая копирует файл текущей конфигурации на TFTP-сервер.
copy tftp flash	Многострочная команда, которая копирует файл конфигурации с TFTP-сервера во флэш-память.
copy tftp running-config	Многострочная команда, которая копирует файл конфигурации с TFTP-сервера в текущую конфигурацию.
copy tftp startup-config	Многострочная команда, которая копирует файл конфигурации с TFTP-сервера в файл startup-config, также известный как NVRAM.
debug ip icmp	Выводит данные отладки транзакций ICMP.
debug ip rip	Выводит данные отладки транзакций протокола маршрутизации RIP.
no debug all	Отключает *все* операции отладки.
delete flash:*имя_файла*	Удаляет указанный файл из флэш-памяти.
more flash:*имя_файла*	Отображает содержимое файла во флэш-памяти в виде текста.
ping *ip_адрес*	Общепринятое средство выявления проблем доступа к устройствам. Использует эхо-запросы и эхо-ответы ICMP, чтобы определить, активен ли удаленный хост. Команда **ping** также определяет количество времени, затрачиваемого на получение эхо-ответа.
show debugging	Выводит информацию о типах отладки, которые активны на маршрутизаторе.
show flash	Отображает формат и содержимое файловой системы флэш-памяти.
show processes	Выводит информацию об активных процессах, включая загрузку ЦП.
show running-config interface *идентификатор_интерфейса*	Выводит только текущую конфигурацию указанного интерфейса.
show startup-config	Выводит параметры конфигурации файла загрузочной конфигурации в NVRAM.

Подсказки

Для упражнений этой лабораторной работы доступны следующие подсказки.

Таблица 1. IP-адреса TFTP-сервера

Рабочая группа	IP-адрес TFTP-сервера	Рабочая группа	IP-адрес TFTP-сервера
A	10.2.2.1	E	10.6.6.1
B	10.3.3.1	F	10.7.7.1
C	10.4.4.1	G	10.8.8.1
D	10.5.5.1	H	10.9.9.1

Задача 1: Копирование файлов конфигурации

Для сохранения и изменения конфигурации путем загрузки файлов конфигурации на сервер TFTP или с TFTP-сервера будут использоваться команды Cisco IOS.

Процедура упражнения

Выполните следующие действия:

Действие 1 Подключитесь к удаленному маршрутизатору рабочей группы через терминальный сервер и введите необходимые команды и пароли, чтобы получить доступ к приглашению пользовательского режима EXEC.

Действие 2 Введите команду для перехода к приглашению привилегированного режима EXEC.

Действие 3 Перед сохранением или копированием конфигурации с TFTP-сервера рекомендуется проверить доступность сервера. Введите команду для отправки эхо-запросов на TFTP-сервер рабочей группы, используя адрес из таблицы 1. Вывод на экран должен выглядеть следующим образом:

```
RouterX#ping 10.10.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

Действие 4 Введите команду **copy running tftp**.

Действие 5 В приглашении введите назначенный IP-адрес TFTP-сервера рабочей группы из таблицы 1.

Действие 6 В приглашении примите имя по умолчанию, которое основывается имени хоста маршрутизатора, нажав клавишу **Enter**.

Действие 7 Вывод на экран во время этих действий должен выглядеть следующим образом:

```
RouterX#copy running tftp
Address or name of remote host []? 10.x.x.100
Destination filename [RouterX-confg]?
.!!
2140 bytes copied in 4.760 secs (450 bytes/sec)
```


Действие 8 Введите команду **show run int s0/0/0** для вывода только конфигурации последовательного интерфейса. Вывод на экран должен выглядеть следующим образом:

```
RouterX#show interface s0/0/0
Building configuration...

Current configuration : 125 bytes
!
interface Serial0/0/0
 description Link to Main Office
 ip address 10.140.10.2 255.255.255.0
 encapsulation ppp
 no fair-queue
end
```

Действие 9 Введите команду **copy tftp run** для копирования файла с TFTP-сервера в текущую конфигурацию.

Действие 10 При запросе адреса укажите IP-адрес TFTP-сервера рабочей группы.

Действие 11 При запросе имени исходного файла укажите имя файла «descript-confg».

Действие 12 Примите имя файла назначения по умолчанию.

Действие 13 Вывод на экран во время этих действий должен выглядеть следующим образом:

```
RouterX#copy tftp run
Address or name of remote host []? 10.10.10.1
Source filename []? descript-confg
Destination filename [running-config]?
Accessing tftp://10.10.10.1/descript-confg...
Loading descript-confg from 10.10.10.1 (via FastEthernet0/0): !
[OK - 289 bytes]

289 bytes copied in 2.024 secs (143 bytes/sec)
```

Действие 14 Введите команду **show run int s0/0/0** для вывода только конфигурации последовательного интерфейса. Вывод на экран должен выглядеть следующим образом:

```
RouterX#show run int s0/0/0
Building configuration...

Current configuration : 164 bytes
!
interface Serial0/0/0
 description Connection to Main Office
 ip address 10.140.10.2 255.255.255.0
 encapsulation ppp
 no fair-queue
end
```

Действие 15 В выводе должно быть указано, что прежнее описание последовательного интерфейса перезаписано инструкцией description.

Действие 16 Введите команду **copy tftp flash** для копирования файла с TFTP-сервера в локальную флэш-память.

Действие 17 При запросе адреса укажите IP-адрес TFTP-сервера рабочей группы.

Действие 18 При запросе имени исходного файла укажите имя файла «descript-confg».

Действие 19 Примите имя файла назначения по умолчанию.

Действие 20 Вывод на экран во время этих действий должен выглядеть следующим образом:

```
RouterX#copy tftp flash:
Address or name of remote host [10.x.x.1]?
Source filename [descript-confg]?
Destination filename [descript-confg]?
Accessing tftp://10.x.x.1/descript-confg...
Loading descript-confg from 10.x.x.1 (via FastEthernet0/0): !
[OK - 289 bytes]

289 bytes copied in 2.228 secs (130 bytes/sec)
```

Действие 21 Введите команду **show flash** для вывода файлов, сохраненных во флэш-памяти.

Действие 22 В выводе должно присутствовать имя только что загруженного файла.

Действие 23 Введите команду **more flash:descript-confg** для вывода содержимого файла в виде текста.

Действие 24 Вывод на экран во время этих действий должен выглядеть следующим образом:

```
RouterX#more flash:descript-confg
! This file demonstrates the way the IOS removes remarks
! from configuration files
! and allows parts of a configuration to be updated
!*********************[
interface serial 0/0/0
 description Connection to Main Office
interface serial 0/0/1
 description Unused Interface
end
```

Действие 25 Обратите внимание, что этот файл содержит незначительное количество команд конфигурации, которые были добавлены в текущую активную конфигурацию или объединены с ней. Также обратите внимание, что файл содержит комментарии. Эти комментарии игнорируются и не сохраняются в текущей конфигурации.

Действие 26 Введите команду **delete flash:descript-confg** для удаления файла, только что загруженного из флэш-памяти. Вывод на экран должен выглядеть следующим образом:

```
RouterX#delete flash:descript-confg
Delete filename [descript-confg]?
Delete flash:descript-confg? [confirm]
```

Действие 27 Введите команду и последующие параметры для копирования файла descript-confg в startup-config. Вывод на экран должен выглядеть следующим образом:

```
RouterX#copy tftp start
RouterX#copy tftp startup-config
Address or name of remote host [10.x.x.1]?10.x.x.1
Source filename [descript-confg]?descript-confg
Destination filename [startup-config]?
Accessing tftp://10.x.x.1/descript-confg...
Loading descript-confg from 10.x.x.1 (via FastEthernet0/0): !
[OK - 289 bytes]
[OK]
289 bytes copied in 3.348 secs (86 bytes/sec)
```


Действие 28 Введите команду **show startup** для отображения содержимого файла startup-config. Вывод на экран должен выглядеть следующим образом:

```
RouterX#show startup
Using 289 out of 245752 bytes! This file demonstrates the way the IOS removes
remarks
! from configuration files
! and allows parts of a configuration to be updated
!********************[
interface serial 0/0/0
 description Connection to Main Office
interface serial 0/0/1
 description Unused Interface
end
```

Действие 29 Обратите внимание, что загрузочная конфигурация полностью заменена небольшим новым файлом конфигурации. Это доказывает, что при копировании в файл загрузочной конфигурации выполняется замена (или перезапись) этого файла. Если перезагрузить маршрутизатор в этот момент, у него не будет действующих интерфейсов!

Действие 30 Введите команду для сохранения текущей конфигурации в файле startup-config.

Действие 31 С помощью команды **show startup** убедитесь, что фрагмент конфигурации в файле startup-config заменен полной текущей конфигурацией.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- выполнено сохранение текущей конфигурации на назначенном TFTP-сервере;
- файл с небольшим фрагментом конфигурации загружен в текущую конфигурацию;
- файл конфигурации загружен во флэш-память, с помощью команды **more** выведен текст файла;
- загруженный файл удален из флэш-памяти;
- файл конфигурации загружен в файл startup-config, подтверждено, что этот файл перезаписал все предыдущие записи конфигурации;
- текущая конфигурация скопирована в startup-config, что привело к замене фрагмента конфигурации полной текущей конфигурацией.

Задача 2: Использование команд отладки

В этой задаче вы должны использовать команды **show** and **debug** для выборочного вывода данных об определенных динамических событиях, а также для предотвращения возникновения проблем производительности.

Процедура упражнения

Выполните следующие действия:

Действие 1 В реальной производственной среде перед использованием команды **debug** необходимо проверить степень загрузки ЦП, так как от этого зависит производительность маршрутизатора. Командам **debug** присваивается самый высокий приоритет. Они могут привести к перезапуску маршрутизатора. Это может происходить из-за отсутствия обслуживания программных таймеров, что приводит к неустранимой ошибке.

Действие 2 Введите команду **show processes** для вывода информации о загрузке ЦП. Закройте экран после вывода первой страницы. Вывод на экран должен выглядеть следующим образом:

```
RouterX#show processes
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
 PID QTy    PC Runtime (ms)  Invoked  uSecs  Stacks TTY Process
  1 Cwe 400A7A2C      0     4      0  5456/6000  0 Chunk Manager
  2 Csp 4008C430      4    1614    2  2528/3000  0 Load Meter
  3 M*     0       7832   379196   20 7200/12000 0 Exec
..
..Текст пропущен
..
```

Действие 3 Обратите внимание на первую строку вывода, в которой приводится информация об загрузке ЦП в течение трех временных периодов. В примере выше эти данные выделены жирным шрифтом. В вашем выводе значение также должно быть мало.

Действие 4 Введите команду **show debugging**, чтобы убедиться в отсутствии других активных команд **debug**. В выводе не должно быть активных процессов отладки.

Действие 5 Введите команду **debug ip icmp**, чтобы включить отладку сообщений ICMP. Вывод на экран должен выглядеть следующим образом:

```
RouterX#debug ip icmp
ICMP packet debugging is on
```

Действие 6 Повторите действие 4, на экране должны появиться следующие данные:

```
RouterX#sh debugging
Generic IP:
 ICMP packet debugging is on
```

Действие 7 Введите команду **ping 10.*x.x*.1** для отправки пакетов эхо-запроса ICMP на IP-адрес назначенного TFTP-сервера. Вывод на экран должен выглядеть следующим образом:

```
RouterX#ping 10.10.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
RouterX#
*Apr 3 19:44:43.699: ICMP: echo reply rcvd, src 10.10.10.1, dst 10.10.10.3
*Apr 3 19:44:43.703: ICMP: echo reply rcvd, src 10.10.10.1, dst 10.10.10.3
*Apr 3 19:44:43.703: ICMP: echo reply rcvd, src 10.10.10.1, dst 10.10.10.3
*Apr 3 19:44:43.703: ICMP: echo reply rcvd, src 10.10.10.1, dst 10.10.10.3
*Apr 3 19:44:43.707: ICMP: echo reply rcvd, src 10.10.10.1, dst 10.10.10.3
```

Действие 8 Введите команду **debug ip rip**, чтобы включить отладку пакетов маршрутизации RIP.

Действие 9 Подождите несколько минут и пронаблюдайте отправку и получение обновлений протокола маршрутизации RIP. Вывод на экран должен выглядеть следующим образом:

```
RouterX#
*Apr 3 20:12:01.355: RIP: sending v2 update to 224.0.0.9 via FastEthernet0/0 (10.10.10.3)
*Apr 3 20:12:01.355: RIP: build update entries
*Apr 3 20:12:01.355:  10.140.10.0/24 via 0.0.0.0, metric 1, tag 0
*Apr 3 20:12:01.355:  10.140.10.1/32 via 0.0.0.0, metric 1, tag 0
*Apr 3 20:12:01.355:  192.168.21.0/24 via 0.0.0.0, metric 1, tag 0
*Apr 3 20:12:01.355:  192.168.121.0/24 via 0.0.0.0, metric 1, tag 0
*Apr 3 20:12:01.355:  192.168.131.0/24 via 0.0.0.0, metric 1, tag 0
*Apr 3 20:12:01.355:  192.168.221.0/24 via 0.0.0.0, metric 3, tag 0
RouterX#
*Apr 3 20:12:06.083: RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (10.140.10.2)
*Apr 3 20:12:06.083: RIP: build update entries
*Apr 3 20:12:06.083:  10.10.10.0/24 via 0.0.0.0, metric 1, tag 0
RouterX#
*Apr 3 20:12:27.295: RIP: received v2 update from 10.140.10.1 on Serial0/0/0
*Apr 3 20:12:27.295:   192.168.21.0/24 via 0.0.0.0 in 1 hops
*Apr 3 20:12:27.295:   192.168.121.0/24 via 0.0.0.0 in 1 hops
*Apr 3 20:12:27.295:   192.168.131.0/24 via 0.0.0.0 in 1 hops
*Apr 3 20:12:27.295:   192.168.221.0/24 via 0.0.0.0 in 2 hops
RouterX#
```

Действие 10 Введите команду для просмотра количества активных команд **debug**. Должны появиться следующие выходные данные:

```
RouterX#show debugging
Generic IP:
 ICMP packet debugging is on
IP routing:
 RIP protocol debugging is on
```

Действие 11 Хотя каждую из команд **debug** можно отключить отдельно, быстрее и надежнее отключить все операции отладки с помощью одной команды. Введите команду **no debug all** для удаления всех активных процессов отладки на маршрутизаторе.

```
RouterX#no debug all
All possible debugging has been turned off
```

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- с помощью команды **show processes** было определено, что маршрутизатор потребляет крайне мало ресурсов ЦП;
- для просмотра выходных данных для пакетов ICMP и обновлений протокола маршрутизации RIP использовались команды **debug**;
- для обнаружения активных команд **debug** на маршрутизаторе использовалась команда **show debug**;
- все операции отладки были отключены с помощью одной команды.

Лабораторная работа 6-4: Подтверждение реконфигурации сети филиала

Выполните упражнение этой лабораторной работы, чтобы применить на практике знания, полученные в соответствующем модуле.

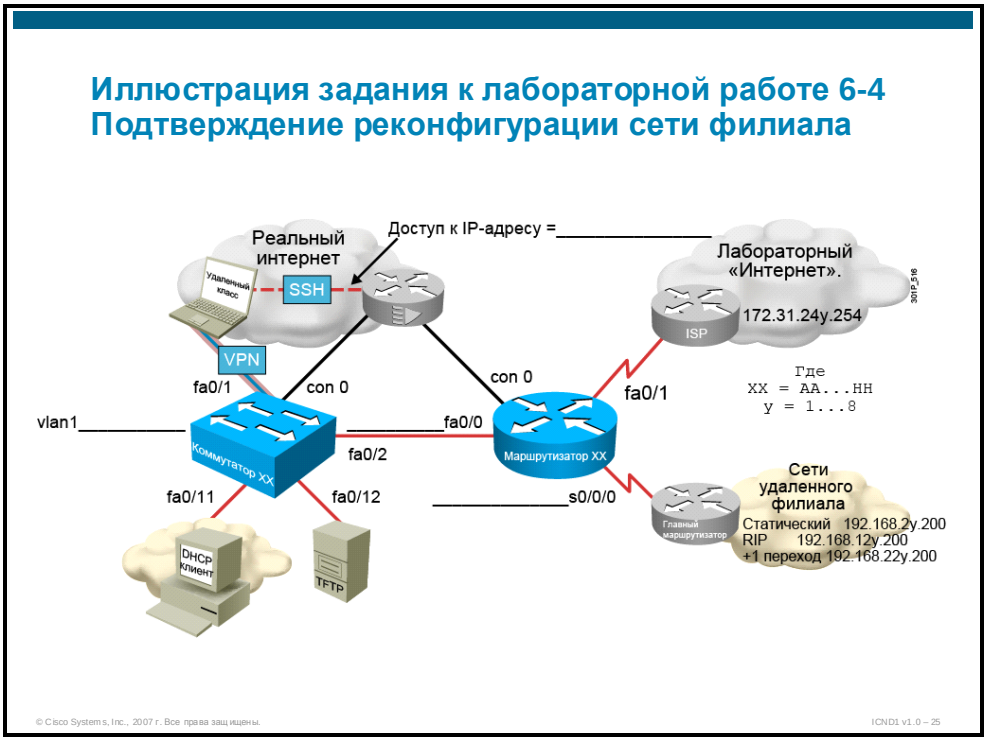
Задачи упражнения

В этом упражнении вы будете вносить изменения в конфигурацию сети филиала, которая не полностью настроена администратором. При реконфигурации, внесении исправлений и проверке будут использоваться практические навыки и знания, полученные во время предыдущих лабораторных работ. После выполнения этого упражнения вы будете способны сделать следующее:

- настроить коммутатор рабочей группы, используя информацию из контрольной таблицы ниже;
- настроить маршрутизатор рабочей группы, используя информацию из контрольной таблицы ниже;
- после включения динамической маршрутизации на маршрутизаторе рабочей группы найти маршрутизаторы, указанные в иллюстрации задания;
- выполнить проверку соответствия окончательной конфигурации новым данным о топологии.

Иллюстрация задания

На рисунке ниже показано, что вы должны сделать во время данного упражнения.



Необходимые ресурсы

Ниже перечислены ресурсы и устройства, необходимые для выполнения упражнения.

- ПК, подключенный к удаленной лаборатории.
- Приложение для эмуляции терминала с поддержкой SSH.
- Новые данные о доступе к назначенному комплекту оборудования для этой лабораторной работы, приведенные в разделе «Подсказки».

Списки команд

См. списки команд, связанные с предыдущей лабораторной работой, которая соответствует выполняемой задаче.

Подсказки

Для этого упражнения доступны следующие подсказки.

- Иллюстрации задания для этой лабораторной работы.
- Таблица задач коммутатора.
- Таблица задач маршрутизатора.
- Таблица с данными об адресах для каждой рабочей группы.

Таблица 1. Информация об адресах рабочих групп

Рабочая группа	Имя хоста коммутатора	Маска IP-адреса VLAN 1 /24	Имя хоста маршрутизатора	Маска IP-адреса Fa0/0 /24
AA	SwitchAA	10.22.22.11	RouterAA	10.22.22.3
BB	SwitchBB	10.33.33.11	RouterBB	10.33.33.3
CC	SwitchCC	10.44.44.11	RouterCC	10.44.44.3
DD	SwitchDD	10.55.55.11	RouterDD	10.55.55.3
EE	SwitchEE	10.66.66.11	RouterEE	10.66.66.3
FF	SwitchFF	10.77.77.11	RouterFF	10.77.77.3
GG	SwitchGG	10.88.88.11	RouterGG	10.88.88.3
HH	SwitchHH	10.99.99.11	RouterHH	10.99.99.3

Таблица 2. Информация об адресе интерфейса s0/0/0 маршрутизатора

Рабочая группа	Маска IP-адреса /24 интерфейса s0/0/0	Рабочая группа	Маска IP-адреса /24 интерфейса s0/0/0
AA	10.140.11.2	EE	10.140.55.2
BB	10.140.22.2	FF	10.140.66.2
CC	10.140.33.2	GG	10.140.77.2
DD	10.140.44.2	HH	10.140.88.2

Таблица задач коммутатора

Выполнена	Таблица задач коммутатора	Рабочая группа:
✓	**Задача и свойство (лабораторная работа)**	**Подсказки по конфигурации и информация**
	1) Базовая конфигурация (лабораторные работы 2-2, 2-3)	
	Имя хоста (рабочая группа с AA по HH)	**hostname SwitchXX**
	Интерфейс	**vlan 1**
	IP-адрес и маска подсети	**ip address** *ip_адрес маска*
	IP-адрес шлюза по умолчанию	**ip default-gateway** *ip_адрес*
	Enable password	**cisco**
	Enable secret	**sanfran**
	Применение шифрования пароля	**service password-encryption**
	Имя пользователя и пароль для консоли и линий VTY. Netadmin имеет 15-й уровень привилегий	**username netadmin privilege 15 password netadmin**
	Линии VTY	**line vty 0 15**
	Вход с использованием локального имени пользователя и паролей	**login local**
	Линия консоли	**line console 0**
	Вход с запросом пароля	**login**
	Пароль консоли	**sanjose**
	Баннер входа с соответствующим сообщением системы безопасности	**banner login %** *сообщение* **%**
	Проверка	
	2) Настройка для использования ТОЛЬКО протокола SSH (лабораторная работа 2-3, задача 4)	
	Имя пользователя и пароль	**netadmin** **netadmin**
	Имя домена IP	**cisco.com**
	Генерация криптографического ключа	**RSA – 1 024 bit**
	Версия SSH	**2**
	Линии VTY	**line vty 0 15**
	Ограничение поддерживаемых протоколов	**transport input ssh**
	Проверка	**show run**
	3) Настройка безопасности порта (лабораторная работа 2-3, задача 5)	
	Интерфейс	**fa0/1**
	Режим порта коммутатора	**switchport mode access**
	Максимальное число адресов	**switchport port-security max 2**
	Действие «restrict» при нарушении	**switchport port-security violation restrict**
	Получение MAC-адреса = sticky	**switchport port-security mac-address sticky**

Выполнена	Таблица задач маршрутизатора	Рабочая группа:
✓	**Задача и свойство (лабораторная работа)**	**Подсказки по конфигурации и информация**
	Включение безопасности порта	**switchport port-security**
	Проверка	**show port-security interface**
	4) Защищенный коммутатор (лабораторная работа 2-3, задача 6, лабораторная работа 6-1, задача 2)	
	Отключение неиспользуемых портов	**fa0/3-10, fa0/13-24, gi0/1-2**
	Ограничение использования протокола CDP интерфейсом, подключенным к маршрутизатору	**no cdp enable**
	Проверка	

Таблица задач маршрутизатора

Выполнена	Таблица задач маршрутизатора	Рабочая группа:
✓	**Задача и свойство (лабораторная работа)**	**Подсказки по конфигурации и информация**
	1) Базовая конфигурация (лабораторная работа 4-6)	
	Имя хоста (рабочая группа с AA по HH)	**hostname Router*XX***
	Интерфейс	**interface fa0/0**
	IP-адрес и маска подсети	**ip address** *ip_адрес маска*
	Enable password	**enable password cisco**
	Enable secret	**enable secret sanfran**
	Проверка	
	2) Модифицированная конфигурация (лабораторная работа 4-7, лабораторная работа 6-1, задача 1)	
	Применение шифрования пароля	**service password-encryption**
	Имя пользователя и пароль для консоли и линий VTY Пользователь имеет 15-й уровень привилегий	**username netadmin privilege** *уровень* **password netadmin**
	Линии VTY	**line vty 0 4**
	Вход с использованием локального имени пользователя и паролей	**login local**
	Порт консоли	**line console 0**
	Вход с использованием пароля	**login**
	Пароль консоли	**password sanjose**
	Баннер входа с соответствующим сообщением системы безопасности	**banner login %** *сообщение* **%**
	Ограничение использования протокола CDP интерфейсом, подключенным к маршрутизатору	**no cdp enable**
	Проверка	
	3) Настройка для использования ТОЛЬКО протокола SSH (лабораторная работа 4-7, задача 4)	
	Имя домена IP	**cisco.com**
	Генерация криптографического ключа	**RSA – 1 024 bit**

Выполнена	Таблица задач маршрутизатора	Рабочая группа:
✓	**Задача и свойство (лабораторная работа)**	**Подсказки по конфигурации и информация**
	Использование версии SSH v2	**ip ssh version 2**
	Линии VTY	**line vty 0 4**
	Ограничение поддерживаемых протоколов	**transport input ssh**
	Проверка	

Выполнена	Таблица задач маршрутизатора	Рабочая группа:
✓	**Задача и свойство (лабораторная работа)**	**Подсказки по конфигурации и информация**
	4) Настройка поддержки Cisco SDM (лабораторная работа 4-8, задача 1)	
	Подключение через HTTP	**ip http server**
	Разрешение подключения через HTTPS	**ip http secure-server**
	Аутентификация с использованием локального имени пользователя и паролей	**ip http authentication local**
	5) Настройка DHCP-сервера (лабораторная работа 4-8, задача 2) *Поддержка клиентов на интерфейсе Fa0/0*	
	Имя пула	**Branch*xx*-clients**
	Начальный IP-адрес .150	**150**
	Конечный IP-адрес .199	**199**
	Время аренды: 5 минут	**0 0 5**
	Маршрутизатор по умолчанию: этот маршрутизатор	**10.*xx.xx*.3**
	Проверка	
	6) Настройка доступа к Интернету (лабораторная работа 5-1)	
	Интерфейс	**fa0/1**
	IP-адрес использует DHCP	**Динамический (клиент DHCP)**
	Внешний интерфейс PAT	**fa0/1**
	Внутренний интерфейс PAT Проверка	**fa0/0**
	7) Настройка подключения к главному офису (лабораторная работа 5-2)	
	Интерфейс	**s0/0/0**
	IP-адрес последовательного интерфейса 0/0/0 – см. таблицу 2	**ip address** *ip-адрес маска*
	Инкапсуляция	**encapsulation ppp**
	Проверка	
	8) Настройка маршрутизации RIPv2 (лабораторная работа 5-3)	
	Протокол маршрутизации	**router rip**
	RIP версии 2	**version 2**

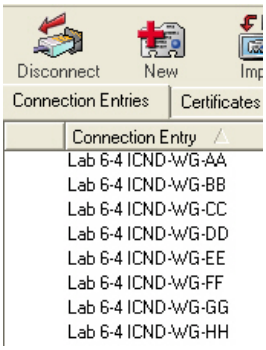
Выполнена	Таблица задач маршрутизатора	Рабочая группа:
✓	**Задача и свойство (лабораторная работа)**	**Подсказки по конфигурации и информация**
	Протокол, работающий на интерфейсах	**network 10.0.0.0**
	Проверка	
	9) Настройка загрузки устройства (лабораторная работа 6-2)	
	Адрес TFTP-сервера – хост .1 в локальной сети.	**10.*nn.nn*.1**
	Должна быть задана следующая последовательность загрузки: Файл Cisco IOS во флэш-памяти; файл Cisco IOS с TFTP-сервера; первый обнаруженный во флэш-памяти файл Cisco IOS	**boot system flash** *имя_файла* **boot system tftp** *адрес имя_файла* **boot system flash**
	Проверка	

Задача 1: Подключение к удаленной лаборатории

Процедура упражнения

Для подключения к новой назначенной рабочей группе будут использоваться меню, которые уже использовались в предыдущих лабораторных работах. Новая рабочая группа обозначена двумя буквами. Например, если в данной лабораторной работе вам назначена рабочая группа AA, используйте меню A, если назначена рабочая группа BB – используйте меню B, и т. д.

Чтобы подключиться через туннель VPN и использовать Cisco SDM для настройки маршрутизатора рабочей группы, необходимо использовать другой профиль конфигурации VPN-клиента. Этот профиль позволит подключиться к нужной подсети, соответствующей новому адресу подсети рабочей группы.



Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- с помощью меню, используемых в предыдущих лабораторных работах, создано подключение к удаленной лаборатории и устройствами рабочей группы;
- с помощью нового профиля VPN-клиента выполнено подключение к удаленной лаборатории, чтобы обеспечить поддержку использования Cisco SDM для настройки маршрутизатора рабочей группы.

Задача 2: Подготовка к проверке конфигурации

Процедура упражнения

Чтобы проверить, правильность настройки сети филиала, убедитесь, что дискретные параметры настроены в соответствии со значениями, заданными для коммутатора и маршрутизатора. Чтобы убедиться в том, что конфигурация филиала а целом работает верно, используйте команды Cisco IOS. Предполагается, что этот процесс состоит из трех этапов, которые могут повторяться для создания окончательной рабочей конфигурации.

Во время этапа 1 вам необходимо собрать всю необходимую информацию о коммутаторе и маршрутизаторе назначенной рабочей группы.

Во время этапа 2 вы должны проверить соответствие конфигурации коммутатора и маршрутизатора значениям, полученным во время этапа 1. Может потребоваться изменение конфигурации, включая добавление отсутствующих или замену неправильных значений. На этом этапе необходимо использовать Cisco SDM или интерфейс командной строки. Правильный синтаксис и процедуры настройки можно найти в предыдущих лабораторных работах.

Во время этапа 3 вам необходимо использовать команды Cisco IOS, чтобы проверить совместную работу коммутатора и маршрутизатора для поддержки конфигурации в целом. Это могут быть команды **ping** *или* команды **show**, показывающие, например, что клиент DHCP получил адрес. Для решения проблем, возникающих на этом этапе, необходимо выявить их источник. Вы должны исходить из того, что окружающая сеть настроена верно, и она будет работать если ваши настройки будут соответствовать значениям, приведенным в подсказках и таблицах. Если решить проблемы не удается, обращайтесь за помощью к инструктору.

Используйте данные из таблиц 1 и 2 и перенесите их в иллюстрацию задания, чтобы подготовить IP-адреса для задач из таблицы задач коммутатора и маршрутизатора.

Проверка упражнения

Задание считается выполненным, если достигнут следующий результат:

- вы изучили инструкции и подготовили сведения, необходимые для выполнения следующей задачи.

Задача 3: Проверка конфигурации

Процедура упражнения

Используйте данные из таблиц 1 и 2 и перенесите их в иллюстрацию задания, чтобы подготовить IP-адреса для задач из таблицы задач коммутатора и маршрутизатора.

Устанавливайте флажки по мере выполнения задач из таблицы. Дополнительные сведения о настройке и проверке конфигурации см. в предыдущих лабораторных работах.

Подробные инструкции не приводятся, поскольку вся необходимая информация доступна в этой или предыдущих лабораторных работах. Если вам потребуются дополнительные указания, обратитесь к инструктору.

Проверка упражнения

Задание считается выполненным, если в сети филиала достигнуты следующие результаты:

- Базовая настройка коммутатора соответствуют свойствам, назначенным рабочей группе;
- для коммутатора создано баннерное сообщение с соответствующим предупреждением;
- Конфигурация SSH на коммутаторе соответствуют свойствам, назначенным рабочей группе;
- Конфигурация безопасности порта соответствуют свойствам, назначенным рабочей группе;
- безопасность коммутатора обеспечена в соответствии со свойствами, назначенными рабочей группе;
- Базовая конфигурация маршрутизатора соответствуют свойствам, назначенным рабочей группе;
- для коммутатора создано баннерное сообщение с соответствующим предупреждением;

- Конфигурация пароля маршрутизатора соответствуют свойствам, назначенным рабочей группе;
- Конфигурация протокола SSH на маршрутизаторе соответствуют свойствам, назначенным рабочей группе;
- Конфигурация DHCP-сервера маршрутизатора соответствуют свойствам, назначенным рабочей группе;
- Конфигурация доступа в Интернет маршрутизатора соответствуют свойствам, назначенным рабочей группе;
- Конфигурация подключения к главному офису соответствуют свойствам, назначенным рабочей группе;
- Конфигурация динамической маршрутизации на маршрутизаторе соответствуют свойствам, назначенным рабочей группе;
- Конфигурация системы загрузки маршрутизатора соответствуют свойствам, назначенным рабочей группе;
- в сети филиала успешно проверена работа служб DHCP-сервера, маршрутизации и подключений.

Ответы к лабораторным работам

Ниже приводятся правильные ответы и ожидаемые решения для упражнений, описанных в этом руководстве.

Ответы для лабораторных работ 1-1, 1-2, 1-3 и 2-1 доступны в самих работах. В ходе этих работ конфигурация не изменяется.

Ответы к лабораторной работе 2-2: Запуск коммутатора и его начальная настройка

После выполнения этого упражнения конфигурация коммутатора рабочей группы будет выглядеть следующим образом (отличия зависят от рабочей группы):

```
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname SwitchX
!
enable secret 5 $1$A11O$0z83HwmswM/vk5.RSZpVr.
enable password cisco
!
no aaa new-model
ip subnet-zero
!
!
!
!
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
```

```
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 10.10.10.11 255.255.255.0
 no ip route-cache
!
ip default-gateway 10.10.10.3
ip http server
ip http secure-server
!
control-plane
!
!
line con 0
line vty 0 4
 password sanjose
 no login
line vty 5 15
 password sanjose
 no login
!
end
```


Ответы к лабораторной работе 2-3: Повышение безопасности начальной конфигурации коммутатора

После выполнения этого упражнения конфигурация коммутатора рабочей группы будет выглядеть следующим образом (отличия зависят от рабочей группы):

```
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname SwitchX
!
enable secret 5 $1$A11O$0z83HwmswM/vk5.RSZpVr.
enable password 7 05080F1C2243
!
username netadmin password 7 030A5E1F070B2C4540
no aaa new-model
ip subnet-zero
!
ip domain-name cisco.com
ip ssh version 2
!
!
crypto pki trustpoint TP-self-signed-1833200768
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1833200768
 revocation-check none
 rsakeypair TP-self-signed-1833200768
!
!
crypto ca certificate chain TP-self-signed-1833200768
 certificate self-signed 01
 3082028D 308201F6 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
 53312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
 69666963 6174652D 31383333 32303037 36383120 301E0609 2A864886 F70D0109
 02161177 675F7377 5F612E63 6973636F 2E636F6D 301E170D 39333033 30313030
 30313033 5A170D32 30303130 31303030 3030305A 3053312F 302D0603 55040313
 26494F53 2D53656C 662D5369 676E6564 2D436572 74696669 63617465 2D313833
 33323030 37363831 20301E06 092A8648 86F70D01 09021611 77675F73 775F612E
 63697363 6F2E636F 6D30819F 300D0609 2A864886 F70D0101 01050003 818D0030
 81890281 8100B444 4F07E979 88953526 E0B8480C 52DBC1E7 E5FF660A 41932329
 8FB4A8EE 142FAEC4 744CB8BE 021BDAE5 BF005CA6 99D0BDC7 68C4A873 25A2F06C
 E460FAE5 1435B900 43505E02 3F0F5E4B D61D6787 59B6AE32 13558C75 561A6BB0
 42C15C96 D078A449 669E4B58 CD5857D0 1B570F43 008B811F 45CD05B0 50D144BA
 F83865F5 8BFD0203 010001A3 71306F30 0F060355 1D130101 FF040530 030101FF
 301C0603 551D1104 15301382 1177675F 73775F61 2E636973 636F2E63 6F6D301F
 0603551D 23041830 16801414 679B7C0E C82E65FB 8953EC84 1FC9DD49 E672A630
 1D060355 1D0E0416 04141467 9B7C0EC8 2E65FB89 53EC841F C9DD49E6 72A6300D
 06092A86 4886F70D 01010405 00038181 006C7E92 A7F96199 D1D81ADA FA16C868
 0660013D 4A91A319 6D6DBD61 B5147AAA FF0FCF26 3DF20CA7 9694B3B8 24ABBEAC
 F8942F5F E53466BB 04E12200 25432AFE A09DDFCF A07A5A4A 145BE58D 4040040A
 5B085A4E 895C45BC 4DF264BC BFE32124 F4AA3BDB B9CF2CC2 35F3B42A B16BFD69
 44531337 B03B7055 48A0B320 0A6C3173 C0
 quit
!
```

```
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0017.5a78.be01
 switchport port-security mac-address sticky 001a.2fe7.3089
!
interface FastEthernet0/2
 switchport mode access
!
interface FastEthernet0/3
 switchport mode access
 shutdown
!
interface FastEthernet0/4
 switchport mode access
 shutdown
!
interface FastEthernet0/5
 switchport mode access
 shutdown
!
interface FastEthernet0/6
 switchport mode access
 shutdown
!
interface FastEthernet0/7
 switchport mode access
 shutdown
!
interface FastEthernet0/8
 switchport mode access
 shutdown
!
interface FastEthernet0/9
 switchport mode access
 shutdown
!
interface FastEthernet0/10
 switchport mode access
 shutdown
!
interface FastEthernet0/11
 switchport mode access
!
interface FastEthernet0/12
 switchport mode access
!
interface FastEthernet0/13
 switchport mode access
 shutdown
!
```



```
interface FastEthernet0/14
 switchport mode access
 shutdown
!
interface FastEthernet0/15
 switchport mode access
 shutdown
!
interface FastEthernet0/16
 switchport mode access
 shutdown
!
interface FastEthernet0/17
 switchport mode access
 shutdown
!
interface FastEthernet0/18
 switchport mode access
 shutdown
!
interface FastEthernet0/19
 switchport mode access
 shutdown
!
interface FastEthernet0/20
 switchport mode access
 shutdown
!
interface FastEthernet0/21
 switchport mode access
 shutdown
!
interface FastEthernet0/22
 switchport mode access
 shutdown
!
interface FastEthernet0/23
 switchport mode access
 shutdown
!
interface FastEthernet0/24
 switchport mode access
 shutdown
!
interface GigabitEthernet0/1
 switchport mode access
 shutdown
!
interface GigabitEthernet0/2
 switchport mode access
 shutdown
!
interface Vlan1
 ip address 10.10.10.11 255.255.255.0
 no ip route-cache
!
ip default-gateway 10.10.10.3
ip http server
ip http secure-server
!
control-plane
!
```

```
banner login ^C
********** Warning  *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.

************************************************************^C
!
line con 0
 password 7 111A180B1D1D1809
 login
line vty 0 4
 password 7 111A180B1D1D1809
 login local
line vty 5 15
 password 7 111A180B1D1D1809
 login local
!
end
```


Ответы к лабораторной работе 2-4: Эксплуатация и настройка устройства Cisco IOS

После выполнения этого упражнения конфигурация коммутатора рабочей группы будет выглядеть следующим образом (отличия зависят от рабочей группы):

```
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname SwitchX
!
enable secret 5 $1$A11O$0z83HwmswM/vk5.RSZpVr.
enable password 7 05080F1C2243
!
username netadmin password 7 030A5E1F070B2C4540
no aaa new-model
ip subnet-zero
!
ip domain-name cisco.com
ip ssh version 2
!
!
crypto pki trustpoint TP-self-signed-1833200768
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1833200768
 revocation-check none
 rsakeypair TP-self-signed-1833200768
!
!
crypto ca certificate chain TP-self-signed-1833200768
 certificate self-signed 01
 3082028D 308201F6 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
 53312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
 69666963 6174652D 31383333 32303037 36383120 301E0609 2A864886 F70D0109
 02161177 675F7377 5F612E63 6973636F 2E636F6D 301E170D 39333033 30313030
 30313033 5A170D32 30303130 31303030 3030305A 3053312F 302D0603 55040313
 26494F53 2D53656C 662D5369 676E6564 2D436572 74696669 63617465 2D313833
 33323030 37363831 20301E06 092A8648 86F70D01 09021611 77675F73 775F612E
 63697363 6F2E636F 6D30819F 300D0609 2A864886 F70D0101 01050003 818D0030
 81890281 8100B444 4F07E979 88953526 E0B8480C 52DBC1E7 E5FF660A 41932329
 8FB4A8EE 142FAEC4 744CB8BE 021BDAE5 BF005CA6 99D0BDC7 68C4A873 25A2F06C
 E460FAE5 1435B900 43505E02 3F0F5E4B D61D6787 59B6AE32 13558C75 561A6BB0
 42C15C96 D078A449 669E4B58 CD5857D0 1B570F43 008B811F 45CD05B0 50D144BA
 F83865F5 8BFD0203 010001A3 71306F30 0F060355 1D130101 FF040530 030101FF
 301C0603 551D1104 15301382 1177675F 73775F61 2E636973 636F2E63 6F6D301F
 0603551D 23041830 16801414 679B7C0E C82E65FB 8953EC84 1FC9DD49 E672A630
 1D060355 1D0E0416 04141467 9B7C0EC8 2E65FB89 53EC841F C9DD49E6 72A6300D
 06092A86 4886F70D 01010405 00038181 006C7E92 A7F96199 D1D81ADA FA16C868
 0660013D 4A91A319 6D6DBD61 B5147AAA FF0FCF26 3DF20CA7 9694B3B8 24ABBEAC
 F8942F5F E53466BB 04E12200 25432AFE A09DDFCF A07A5A4A 145BE58D 4040040A
 5B085A4E 895C45BC 4DF264BC BFE32124 F4AA3BDB B9CF2CC2 35F3B42A B16BFD69
 44531337 B03B7055 48A0B320 0A6C3173 C0
 quit
!
!
```

```
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0017.5a78.be01
 switchport port-security mac-address sticky 001a.2fe7.3089
!
interface FastEthernet0/2
 switchport mode access
!
interface FastEthernet0/3
 switchport mode access
 shutdown
!
interface FastEthernet0/4
 switchport mode access
 shutdown
!
interface FastEthernet0/5
 switchport mode access
 shutdown
!
interface FastEthernet0/6
 switchport mode access
 shutdown
!
interface FastEthernet0/7
 switchport mode access
 shutdown
!
interface FastEthernet0/8
 switchport mode access
 shutdown
!
interface FastEthernet0/9
 switchport mode access
 shutdown
!
interface FastEthernet0/10
 switchport mode access
 shutdown
!
interface FastEthernet0/11
 switchport mode access
!
interface FastEthernet0/12
 switchport mode access
!
interface FastEthernet0/13
 switchport mode access
 shutdown
!
interface FastEthernet0/14
```



```
 switchport mode access
 shutdown
!
interface FastEthernet0/15
 switchport mode access
 shutdown
!
interface FastEthernet0/16
 switchport mode access
 shutdown
!
interface FastEthernet0/17
 switchport mode access
 shutdown
!
interface FastEthernet0/18
 switchport mode access
 shutdown
!
interface FastEthernet0/19
 switchport mode access
 shutdown
!
interface FastEthernet0/20
 switchport mode access
 shutdown
!
interface FastEthernet0/21
 switchport mode access
 shutdown
!
interface FastEthernet0/22
 switchport mode access
 shutdown
!
interface FastEthernet0/23
 switchport mode access
 shutdown
!
interface FastEthernet0/24
 switchport mode access
 shutdown
!
interface GigabitEthernet0/1
 switchport mode access
 shutdown
!
interface GigabitEthernet0/2
 switchport mode access
 shutdown
!
interface Vlan1
 ip address 10.10.10.11 255.255.255.0
 no ip route-cache
!
ip default-gateway 10.10.10.3
ip http server
ip http secure-server
!
control-plane
!
```

```
banner login ^C
********** Warning  *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.

************************************************************^C
!
line con 0
 password 7 111A180B1D1D1809
 login
line vty 0 4
 password 7 111A180B1D1D1809
 login local
line vty 5 15
 password 7 111A180B1D1D1809
 login local
!
end
```


Ответы к лабораторной работе 4-1: Преобразование десятичных чисел в двоичные и двоичных в десятичные

В ходе этого упражнения вы должны получить следующие результаты.

Задача 1: Преобразование десятичных чисел в двоичный формат

Основание-2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Десятичное число	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Двоичное число**
48	0	0	1	1	0	0	0	0	48 = 32 + 16 = 00110000
146	1	0	0	1	0	0	1	0	146 = 128 + 16 + 2 = 10010010
222	1	1	0	1	1	1	1	0	222 = 128 + 64 + 16 + 8 + 4 + 2 = 1101110
119	0	1	1	1	0	1	1	1	119 = 64 + 32 + 16 + 4 + 2 + 1 = 01110111
135	1	0	0	0	0	1	1	1	135 = 128 + 4 + 2 + 1 = 10000111
60	0	0	1	1	1	1	0	0	60 = 32 + 16 + 8 + 4 = 00111100

Задача 2: Преобразование двоичных чисел в десятичный формат

Основание-2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Двоичное число	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Десятичное число**
11001100	1	1	0	0	1	1	0	0	128 + 64 + 8 + 4 = 204
10101010	1	0	1	0	1	0	1	0	128 + 32 + 8 + 2 = 170
11100011	1	1	1	0	0	0	1	1	128 + 64 + 32 + 2 + 1 = 227
10110011	1	0	1	1	0	0	1	1	128+ 32 + 16 + 2 + 1 = 179
00110101	0	0	1	1	0	1	0	1	32 + 16 + 4 + 1 = 53
10010111	1	0	0	1	0	1	1	1	128 + 16 + 4 + 2 + 1 = 151

Ответы к лабораторной работе 4-2: Классификация способов сетевой адресации

В ходе этого упражнения вы должны получить следующие результаты.

Задача 1: Преобразование IP-адреса в десятичном формате в двоичный формат

В следующей таблице показано преобразование адреса 145.32.59.24 в двоичный формат.

Основание-2	**2^7**	**2^6**	**2^5**	**2^4**	**2^3**	**2^2**	**2^1**	**2^0**	
Десятичное число	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Двоичное число**
145	1	0	0	1	0	0	0	1	10010001
32	0	0	1	0	0	0	0	0	00100000
59	0	0	1	1	1	0	1	1	00111011
24	0	0	0	1	1	0	0	0	00011000
IP-адрес в двоичном формате						10010001.00100000.00111011.00011000			

Действие 1 В следующей таблице показано преобразование адреса 200.42.129.16 в двоичный формат.

Основание-2	**2^7**	**2^6**	**2^5**	**2^4**	**2^3**	**2^2**	**2^1**	**2^0**	
Десятичное число	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Двоичное число**
200	1	1	0	0	1	0	0	0	11001000
42	0	0	1	0	1	0	1	0	00101010
129	1	0	0	0	0	0	0	1	10000001
16	0	0	0	1	0	0	0	0	00010000
IP-адрес в двоичном формате						11001000.00101010.10000001.00010000			

Действие 2 В следующей таблице показано преобразование адреса 14.82.19.54 в двоичный формат.

Основание-2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Десятичное число	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Двоичное число**
14	0	0	0	0	1	1	1	0	00001110
82	0	1	0	1	0	0	1	0	01010010
19	0	0	0	1	0	0	1	1	00010011
54	0	0	1	1	0	1	1	0	00110110
IP-адрес в двоичном формате						00001110.01010010.00010011.00110110			

Задача 2: Преобразование IP-адреса в двоичном формате в десятичный формат

Действие 1 В следующей таблице показано преобразование IP-адреса в двоичном формате 11011000.00011011.00111101.10001001 в десятичный формат.

Основание-2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Двоичное число	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Десятичное число**
11011000	1	1	0	1	1	0	0	0	216
00011011	0	0	0	1	1	0	1	1	27
00111101	0	0	1	1	1	1	0	1	61
10001001	1	0	0	0	1	0	0	1	137
IP-адрес в десятичном формате						216.27.61.137			

Действие 2 В следующей таблице показано преобразование IP-адреса в двоичном формате 11000110.00110101.10010011.00101101 в десятичный формат.

Основание-2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Двоичное число	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Десятичное число**
11000110	1	1	0	0	0	1	1	0	198
00110101	0	0	1	1	0	1	0	1	53
10010011	1	0	0	1	0	0	1	1	147
00101101	0	0	1	0	1	1	0	1	45
IP-адрес в десятичном формате						198.53.147.45			

Действие 3 В следующей таблице показано преобразование IP-адреса в двоичном формате 01111011.00101101.01000011.01011001 в десятичный формат.

Основание-2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Двоичное число	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Десятичное число**
01111011	0	1	1	1	1	0	1	1	123
00101101	0	0	1	0	1	1	0	1	45
01000011	0	1	0	0	0	0	1	1	67
01011001	0	1	0	1	1	0	0	1	89
IP-адрес в десятичном формате						123.45.67.89			

Задача 3: Распознавание классов IP-адресов

Двоичный IP-адрес	Десятичный IP-адрес	Класс адреса	Число битов в коде сети	Максимальное число хостов (2^h –2)
10010001.00100000.00111011.00011000	145.32.59.24	Класс B	16	2^{16}-2 = 65 534
11001000.00101010.10000001.00010000	200.42.129.16	Класс C	24	2^8-2 = 254
00001110.01010010.00010011.00110110	14.82.19.54	Класс A	8	2^{24}-2 = 16 777 214
11011000.00011011.00111101.10001001	216.27.61.137	Класс C	24	2^8-2 = 254
10110011.00101101.01000011.01011001	179.45.67.89	Класс B	16	2^{16}-2 = 65 534
11000110.00110101.10010011.00101101	198.53.147.45	Класс C	24	2^8-2 = 254

Задача 4: Распознавание допустимых и недопустимых IP-адресов хостов

Десятичный IP-адрес	Допустимый или недопустимый	Если адрес недопустимый, укажите причину
23.75.345.200	Недопустимый	Значение 345 не является восьмибитовым (максимум = 255)
216.27.61.134	Допустимый	
102.54.94	Недопустимый	Отсутствует один октет
255.255.255.255	Недопустимый	Значение допустимое, однако оно является административным (зарезервированным) значением, которое нельзя назначать хосту
142.179.148.200	Допустимый	
200.42.129.16	Допустимый	
0.124.0.0	Недопустимый	В адресе класса A нельзя использовать 0 в качестве первого октета

Ответы к лабораторной работе 4-3: Расчет доступных подсетей и хостов

При выполнении данного упражнения вы должны получить следующие результаты.

Задача 1: Определение количества битов, необходимого для подсети сети класса C

В следующей таблице приведены значения, которые должны быть получены для сетевого адреса 192.168.89.0 (класс C).

Количество подсетей	Количество заимствованных битов	Количество хостов для подсети ($2^h - 2$)
2	1	$2^7 - 2 = 126$
5	3	$2^5 - 2 = 30$
12	4	$2^4 - 2 = 14$
24	5	$2^3 - 2 = 6$
40	6	$2^2 - 2 = 2$

Задача 2: Определение количества битов, необходимого для подсети сети класса B

В следующей таблице приведены значения, которые должны быть получены для сетевого адреса 172.25.0.0 (класс B).

Количество подсетей	Количество заимствованных битов	Количество хостов для подсети ($2^h - 2$)
5	3	$2^{13} - 2 = 8\ 190$
8	3	$2^{13} - 2 = 8\ 190$
14	4	$2^{12} - 2 = 4\ 094$
20	5	$2^{11} - 2 = 2\ 046$
35	6	$2^{10} - 2 = 1\ 022$

Задача 3: Определение количества битов, необходимого для подсети сети класса A

В следующей таблице приведены значения, которые должны быть получены для сетевого адреса 10.0.0.0 (класс A).

Количество подсетей	Количество заимствованных битов	Количество хостов для подсети ($2^h - 2$)
10	4	$2^{20} - 2 = 1\ 048\ 574$
14	4	$2^{20} - 2 = 1\ 048\ 574$
20	5	$2^{19} - 2 = 524\ 286$
40	6	$2^{18} - 2 = 262\ 142$
80	7	$2^{17} - 2 = 131\ 070$

Ответы к лабораторной работе 4-4

При выполнении данного упражнения вы должны получить следующие результаты.

Задача 1: Определение количества доступных сетевых адресов

Классовый адрес	Десятичная маска подсети	Двоичная маска подсети	Количество хостов для подсети ($2^h - 2$)
/20	255.255.240.0	11111111.11111111.11110000.00000000	4 094
/21	255.255.248.0	11111111.11111111.11111000.00000000	2 046
/22	255.255.252.0	11111111.11111111.11111100.00000000	1 022
/23	255.255.254.0	11111111.11111111.11111110.00000000	510
/24	255.255.255.0	11111111.11111111.11111111.00000000	254
/25	255.255.255.128	11111111.11111111.11111111.10000000	126
/26	255.255.255.192	11111111.11111111.11111111.11000000	62
/27	255.255.255.224	11111111.11111111.11111111.11100000	30
/28	255.255.255.240	11111111.11111111.11111111.11110000	14
/29	255.255.255.248	11111111.11111111.11111111.11111000	6
/30	255.255.255.252	11111111.11111111.11111111.11111100	2

Задача 2: Определение подсетей для сетевого блока

Предположим, что вам назначен сетевой блок 172.25.0.0 /16. Необходимо создать восемь подсетей. Ответьте на следующие вопросы.

1. Сколько битов потребуется позаимствовать для задания 12 подсетей? 4

2. Укажите классовый адрес и маску подсети в двоичном и десятичном формате, которые позволят создать 12 подсетей.
   Классовый адрес: /20
   Маска подсети (двоичная): 11111111.11111111.11110000.00000000
   Маска подсети (десятичная): 255.255.240.0

3. Используйте метод, включающий восемь действий, чтобы задать 12 подсетей.

Действие	Описание	Пример
1.	Укажите разделяемый октет в двоичном формате.	00000000
2.	Укажите маску или длину классового префикса в двоичном формате.	11110000
3.	Отделите линией значимые биты в назначенном IP-адресе. Разделите линией маску, чтобы выделить значимые биты IP-адреса.	0000 | 0000 1111 | 0000

Действие	Описание	Пример
4.	Скопируйте значимые биты четыре раза.	0000 0000 (первая подсеть) 0000 0001 (адрес первого хоста) 0000 1110 (адрес последнего хоста) 0000 1111 (широковещательный адрес)
5.	В первой строке укажите сетевой адрес, поставив 0 в оставшиеся биты хоста.	
6.	В последней строке укажите широковещательный адрес, поставив 1 в битах хоста.	
7.	В средних строках укажите идентификатор первого и последнего хостов подсети.	
8.	Чтобы определить следующий адрес подсети, увеличивайте биты подсети на единицу. Повторите шаги с 4 по 8 для всех подсетей.	0001 0000 (следующая подсеть)

4. Заполните следующую таблицу, чтобы задать каждую из подсетей.

Номер подсети	Адрес подсети	Диапазон адресов хостов	Широковещательный адрес
0	172.25.0.0	с 172.25.0.1 по 172.25.15.254	172.25.15.255
1	172.25.16.0	с 172.25.16.1 по 172.25.31.254	172.25.31.255
2	172.25.32.0	с 172.25.32.1 по 172.25.47.254	172.25.47.255
3	172.25.48.0	с 172.25.48.1 по 172.25.63.254	172.25.63.255
4	172.25.64.0	с 172.25.64.1 по 172.25.79.254	172.25.79.255
5	172.25.80.0	с 172.25.80.1 по 172.25.93.254	172.25.93.255
6	172.25.94.0	с 172.25.94.1 по 172.25.109.254	172.25.109.255
7	172.25.110.0	с 172.25.110.1 по 172.25.123.254	172.25.123.255

Задача 3: Определение подсетей на основе другого сетевого блока

Предположим, что вам выделен сетевой блок 192.168.1.0 /24.

1. Сколько битов потребуется позаимствовать для задания 6 подсетей? 3

2. Укажите классовый адрес и маску подсети в двоичном и десятичном формате, которые позволят создать 6 подсетей.
   Классовый адрес: /27
   Маска подсети (двоичная): 11111111.11111111.11111111.11100000
   Маска подсети (десятичная): 255.255.255.224

3. Используйте метод, включающий восемь действий, чтобы задать 6 подсетей.

Действие	Описание	Пример
1.	Укажите разделяемый октет в двоичном формате.	00000000
2.	Укажите маску или длину классового префикса в двоичном формате.	11100000
3.	Отделите линией значимые биты в назначенном IP-адресе. Разделите линией маску, чтобы выделить значимые биты IP-адреса.	000 | 00000 111 | 00000
4.	Скопируйте значимые биты четыре раза.	000 00000 (первая подсеть) 000 00001 (адрес первого хоста) 000 11110 (адрес последнего хоста) 000 11111 (широковещательный адрес)
5.	В первой строке укажите сетевой адрес, поставив 0 в оставшиеся биты хоста.	
6.	В последней строке укажите широковещательный адрес, поставив 1 в битах хоста.	
7.	В средних строках укажите идентификатор первого и последнего хостов подсети.	
8.	Чтобы определить следующий адрес подсети, увеличивайте биты подсети на единицу. Повторите шаги с 4 по 8 для всех подсетей.	001 0000 (следующая подсеть)

4. Заполните следующую таблицу, чтобы задать каждую из подсетей.

Номер подсети	Адрес подсети	Диапазон адресов хостов	Широковещательный адрес
0	192.168.1.0	с 192.168.1.1 по 192.168.1.30	192.168.1.31
1	192.168.1.32	с 192.168.1.33 по 192.168.1.62	192.168.1.63
2	192.168.1.64	с 192.168.1.65 по 192.168.1.94	192.168.1.95
3	192.168.1.96	с 192.168.1.97 по 192.168.1.126	192.168.1.127
4	192.168.1.128	с 192.168.1.129 по 192.168.1.158	192.168.1.159
5	192.168.1.160	с 192.168.1.161 по 192.168.1.190	192.168.1.191

Задача 4: Определение подсетей на основе заданного сетевого блока и классового адреса

Предположим, что вам выделен сетевой блок 192.168.111.0 /28.

1. Укажите маску подсети в двоичном и десятичном формате.
   Маска подсети (двоичная): 11111111.11111111.11111111.11110000
   Маска подсети (десятичная): 255.255.255.240

2. Сколько подсетей можно задать для указанной маски? 16

3. Сколько хостов будет в каждой подсети? 14

4. Используйте метод, включающий восемь действий, чтобы задать подсет.

Действие	Описание	Пример
1.	Укажите разделяемый октет в двоичном формате.	10000001
2.	Укажите маску или длину классового префикса в двоичном формате.	11110000
3.	Отделите линией значимые биты в назначенном IP-адресе. Разделите линией маску, чтобы выделить значимые биты IP-адреса.	1000 | 0001 1111 | 0000
4.	Скопируйте значимые биты четыре раза.	1000 0000 (первая подсеть) 1000 0001 (адрес первого хоста) 1000 1110 (адрес последнего хоста) 1000 1111 (широковещательный адрес)
5.	В первой строке укажите сетевой адрес, поставив 0 в оставшиеся биты хоста.	
6.	В последней строке укажите широковещательный адрес, поставив 1 в битах хоста.	
7.	В средних строках укажите идентификатор первого и последнего хостов подсети.	
8.	Чтобы определить следующий адрес подсети, увеличивайте биты подсети на единицу. Повторите шаги с 4 по 8 для всех подсетей.	1001 0000 (следующая подсеть)

5. Заполните следующую таблицу, чтобы задать каждую из подсетей.

Номер подсети	Адрес подсети	Диапазон адресов хостов	Широковещательный адрес
0	192.168.111.0	с 192.168.111.1 по 192.168.111.14	192.168.111.15
1	192.168.111.16	с 192.168.111.17 по 192.168.111.30	192.168.111.31
2	192.168.111.32	с 192.168.111.33 по 192.168.111.46	192.168.111.47
3	192.168.111.48	с 192.168.111.49 по 192.168.111.64	192.168.111.65
4	192.168.111.64	с 192.168.111.65 по 192.168.111.78	192.168.111.79
5	192.168.111.80	с 192.168.111.81 по 192.168.111.94	192.168.111.95
6	192.168.111.96	с 192.168.111.97 по 192.168.111.110	192.168.111.111

Задача 5: Определение подсетей на основе заданного сетевого блока и классового адреса

Предположим, что вам назначен сетевой блок 172.25.0.0 /23.

1. Укажите маску подсети в двоичном и десятичном формате.
   Маска подсети (двоичная): 11111111.11111111.11111110.00000000
   Маска подсети (десятичная): 255.255.254.0

2. Сколько подсетей можно определить с указанной маской?
   126

3. Сколько хостов будет в каждой подсети?
   510

4. Используйте метод, включающий восемь действий, чтобы задать подсет.

Действие	Описание	Пример
1.	Укажите разделяемый октет в двоичном формате.	01110000.00000000
2.	Укажите маску или длину классового префикса в двоичном формате.	11111110.00000000
3.	Отделите линией значимые биты в назначенном IP-адресе. Разделите линией маску, чтобы выделить значимые биты IP-адреса.	0111000 0|00000000 1111111 0|00000000
4.	Скопируйте значимые биты четыре раза.	0111000 0.00000000 (первая подсеть)
5.	В первой строке укажите сетевой адрес, поставив 0 в оставшиеся биты хоста.	0111000 0.00000001 (адрес первого хоста)
6.	В последней строке укажите широковещательный адрес, поставив 1 в битах хоста.	0111000 1.11111110 (адрес последнего хоста)
7.	В средних строках укажите идентификатор первого и последнего хостов подсети.	0111000 1.11111111 (широковещательный адрес)
8.	Чтобы определить следующий адрес подсети, увеличивайте биты подсети на единицу. Повторите шаги с 4 по 8 для всех подсетей.	0111001 0.00000000 (следующая подсеть)

5. Заполните следующую таблицу, чтобы задать каждую из подсетей.

Номер подсети	Адрес подсети	Диапазон адресов хостов	Широковещательный адрес
0	172.25.0.0	с 172.25.0.1 по 172.25.1.254	172.25.1.255
1	172.25.2.0	с 172.25.2.1 по 172.25.3.254	172.25.3.255
2	172.25.4.0	с 172.25.4.1 по 172.25.5.254	172.25.5.255
3	172.25.6.0	с 172.25.6.1 по 172.25.7.254	172.25.7.255
4	172.25.8.0	с 172.25.8.1 по 172.25.9.254	172.25.9.255
. . .			

Задача 6: Определение подсетей на основе заданного сетевого блока и классового адреса

Предположим, что вам назначен сетевой блок 172.20.0.0 /25.

1. Укажите маску подсети в двоичном и десятичном формате.
   Маска подсети (двоичная): 11111111.11111111.11111111.10000000
   Маска подсети (десятичная): 255.255.255.128

2. Сколько подсетей можно определить с указанной маской?
   510

3. Сколько хостов будет в каждой подсети?
   126

4. Используйте метод, включающий восемь действий, чтобы задать подсет.

Действие	Описание	Пример
1.	Укажите разделяемый октет в двоичном формате.	00000000.00000001
2.	Укажите маску или длину классового префикса в двоичном формате.	11111111.10000000
3.	Отделите линией значимые биты в назначенном IP-адресе. Разделите линией маску, чтобы выделить значимые биты IP-адреса.	00000000.0|0000000 11111111.1|0000000
4.	Скопируйте значимые биты четыре раза.	00000000.10000000 (первая подсеть)
5.	В первой строке укажите сетевой адрес, поставив 0 в оставшиеся биты хоста.	00000000.10000001 (адрес первого хоста)
6.	В последней строке укажите широковещательный адрес, поставив 1 в битах хоста.	00000000.11111110 (адрес последнего хоста)
7.	В средних строках укажите идентификатор первого и последнего хостов подсети.	00000000.11111111 (широковещательный адрес)
8.	Чтобы определить следующий адрес подсети, увеличивайте биты подсети на единицу. Повторите шаги с 4 по 8 для всех подсетей.	00000001.10000000 (следующая подсеть)

5. Заполните следующую таблицу, чтобы задать каждую из подсетей.

Номер подсети	Адрес подсети	Диапазон адресов хостов	Широковещательный адрес
0	172.20.0.0	с 172.20.0.1 по 172.20.0.126	172.20.0.127
1	172.20.0.128	с 172.20.0.129 по 172.20.0.254	172.20.0.255
2	172.20.1.0	с 172.20.1.1 по 172.20.1.126	172.20.1.127
3	172.20.1.128	с 172.20.1.129 по 172.20.1.254	172.20.1.255
4	172.20.2.0	с 172.20.2.1 по 172.20.2.126	172.20.2.127
5	172.20.2.128	с 172.20.2.129 по 172.20.2.254	172.20.2.255
. . .			

Ответы к лабораторной работе 4-5: Начальный запуск маршрутизатора

После выполнения этого упражнения у коммутатора рабочей группы будет отсутствовать конфигурация. Ниже приведены выходные данные команды **erase startup-config**. Имя пользователя «cisco» и пароль «cisco» используются в конфигурации Cisco SDM по умолчанию. Вывод на экран должен выглядеть следующим образом:

```
Username: cisco
Password:
yourname#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
yourname#
*Mar 13 17:28:00.003: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
yourname#reload
Proceed with reload? [confirm]

*Mar 13 17:28:07.939: %SYS-5-RELOAD: Reload requested by console. Reload Reason:
Reload Command.

System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2006 by cisco Systems, Inc.

Initializing memory for ECC
.
c2811 platform with 262144 Kbytes of main memory
Main memory is configured to 64 bit mode with ECC enabled


Upgrade ROMMON initialized
program load complete, entry point: 0x8000f000, size: 0xcb80
program load complete, entry point: 0x8000f000, size: 0xcb80

program load complete, entry point: 0x8000f000, size: 0x228d9f8
Self decompressing the image :
################################################################################
################################################################################
######################################## [OK]

Smart Init is enabled
smart init is sizing iomem
 ID      MEMORY_REQ         TYPE
0003E7     0X003DA000 C2811 Mainboard
        0X00263F50 Onboard VPN
        0X000021B8 Onboard USB
        0X002C29F0 public buffer pools
        0X00211000 public particle pools
TOTAL:     0X00B13AF8

If any of the above Memory Requirements are
"UNKNOWN", you may be using an unsupported
configuration or there is a software problem and
system operation may be compromised.
Rounded IOMEM up to: 12Mb.
```

```
Using 4 percent iomem. [12Mb/256Mb]

       Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

      cisco Systems, Inc.
      170 West Tasman Drive
      San Jose, California 95134-1706



Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(12),
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 17-Nov-06 12:02 by prod_rel_team
Image text-base: 0x40093160, data-base: 0x42B00000


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco 2811 (revision 49.46) with 249856K/12288K bytes of memory.
Processor board ID FTX1050A3Q6
2 FastEthernet interfaces
2 Serial(sync/async) interfaces
1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bits wide with parity enabled.
239K bytes of non-volatile configuration memory.
62720K bytes of ATA CompactFlash (Read/Write)


     --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no


Press RETURN to get started!

sslinit fn

*Mar 13 17:29:36.819: %VPN_HW-6-INFO_LOC: Crypto engine: onboard 0 State changed
to: Initialized
```



```
*Mar 13 17:29:36.819: %VPN_HW-6-INFO_LOC: Crypto engine: onboard 0 State changed
to: Enabled
*Mar 13 17:29:38.087: %LINEPROTO-5-UPDOWN: Line protocol on Interface VoIP-
Null0, changed state to up
*Mar 13 17:29:38.087: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state
to up
*Mar 13 17:29:38.087: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state
to up
*Mar 13 17:29:38.087: %LINK-3-UPDOWN: Interface Serial0/0/0, changed state to up
*Mar 13 17:29:38.087: %LINK-3-UPDOWN: Interface Serial0/0/1, changed state to
down
*Mar 13 17:29:390,491: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to down
*Mar 13 17:29:39.495: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down
*Mar 13 17:29:39.495: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to up
*Mar 13 17:29:39.495: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to down
*Mar 13 17:29:41.311: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
*Mar 13 17:29:410,371: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
*Mar 13 17:30:04.463: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to down
*Mar 13 17:30:07.223: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to up
*Mar 13 17:31:02.663: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to down
*Mar 13 17:31:44.471: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state
to administratively down
*Mar 13 17:31:44.471: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state
to administratively down
*Mar 13 17:31:44.471: %LINK-5-CHANGED: Interface Serial0/0/0, changed state to
administratively down
*Mar 13 17:31:44.475: %LINK-5-CHANGED: Interface Serial0/0/1, changed state to
administratively down
*Mar 13 17:31:44.491: %IP-5-WEBINST_KILL: Terminating DNS process
*Mar 13 17:31:45.471: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to down
*Mar 13 17:31:45.471: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down
*Mar 13 17:31:46.007: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(12),
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 17-Nov-06 12:02 by prod_rel_team
*Mar 13 17:31:46.011: %SNMP-5-COLDSTART: SNMP agent on host Router is undergoing
a cold start
*Mar 13 17:31:46.219: %SYS-6-BOOTTIME: Time taken to reboot after reload =
216 seconds
*Mar 13 17:31:46.399: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
```

Ответы к лабораторной работе 4-6: Начальная настройка маршрутизатора

После выполнения этого упражнения конфигурация маршрутизатора рабочей группы будет выглядеть следующим образом (отличия зависят от рабочей группы):

```
!
version 12.4
!
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RouterX
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$.dET$BDxkofHF3aAsRthe/c0.c.
enable password cisco
!
no aaa new-model
!
!
ip cef
!
!
!
!
voice-card 0
 no dspfarm
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 10.10.10.3 255.255.255.0
 duplex half
 speed auto
 no mop enabled
!
interface FastEthernet0/1
 no ip address
```



```
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
!
!
ip http server
no ip http secure-server
!
dialer-list 1 protocol ip permit
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
!
line con 0
line aux 0
line vty 0 4
 password sanjose
 login
!
scheduler allocate 20000 1000
!
end
```

Ответы к лабораторной работе 4-7: Повышение безопасности начальной конфигурации маршрутизатора

После выполнения этого упражнения конфигурация маршрутизатора рабочей группы будет выглядеть следующим образом (отличия зависят от рабочей группы):

```
!
!
version 12.4
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname RouterX
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$.dET$BDxkofHF3aAsRthe/c0.c.
enable password 7 14141B180F0B
!
no aaa new-model
!
!
ip cef
!
!
no ip domain lookup
ip domain name cisco.com
ip ssh version 2
!
!
voice-card 0
 no dspfarm
!
!
!
!
!
!
!
!
!
!
!
!
!
!
username netadmin password 7 082F495A081D081E1C
!
!
!
!
!
!
interface FastEthernet0/0
```



```
 ip address 10.10.10.3 255.255.255.0
 duplex half
 speed auto
 no mop enabled
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
!
!
ip http server
no ip http secure-server
!
dialer-list 1 protocol ip permit
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
banner login ^C
********** Warning  *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.

************************************************************^C
!
line con 0
 password 7 14041305060B392E
 login
line aux 0
line vty 0 4
 password 7 071C204244060A00
 login local
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
end
```

Ответы к лабораторной работе 4-8: Использование Cisco SDM для настройки функций DHCP-сервера

После выполнения этого упражнения конфигурация маршрутизатора рабочей группы будет выглядеть следующим образом (отличия зависят от рабочей группы):

```
!
!
version 12.4
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname RouterX
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$.dET$BDxkofHF3aAsRthe/c0.c.
enable password 7 14141B180F0B
!
no aaa new-model
!
!
ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 10.10.10.1 10.10.10.149
ip dhcp excluded-address 10.10.10.200 10.10.10.254
!
ip dhcp pool wgA_clients
  import all
  network 10.10.10.0 255.255.255.0
  lease 0 0 5
!
!
no ip domain lookup
ip domain name cisco.com
ip ssh version 2
!
!
voice-card 0
 no dspfarm
!
!
!
!
!
!
!
!
!
!
!
!
!
!
crypto pki trustpoint TP-self-signed-3715519608
```



```
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3715519608
 revocation-check none
 rsakeypair TP-self-signed-3715519608
!
!
crypto pki certificate chain TP-self-signed-3715519608
 certificate self-signed 01
 30820249 308201B2 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
 31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
 69666963 6174652D 33373135 35313936 3038301E 170D3037 30343035 32333135
 30305A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
 4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 37313535
 31393630 3830819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
 8100D0D2 4D67CC33 F0966C60 96BD12D2 675EB867 42087A6F 4310110E 1E852852
 E965291B A9E21580 7F77960A B83618A5 65A718BE 4E81DB21 669B48D1 172E1FF3
 73575C54 6B25A849 6E886C49 3EA0D03C CC5E7AFA 186AE594 22F612D6 8CA089EC
 355AFCF5 9FBA492A EEEB13C8 27A6F2BE EEC51E85 18B52144 10DDA46C C0831824
 D0450203 010001A3 71306F30 0F060355 1D130101 FF040530 030101FF 301C0603
 551D1104 15301382 1177675F 726F5F61 2E636973 636F2E63 6F6D301F 0603551D
 23041830 168014B7 CBDB7C0C C2AEB57B B2CA8F85 6C9567DA ACA8F430 1D060355
 1D0E0416 0414B7CB DB7C0CC2 AEB57BB2 CA8F856C 9567DAAC A8F4300D 06092A86
 4886F70D 01010405 00038181 0061FD2F C903A4A2 0E241513 68AD17EA 16856A52
 46C655CA 7AD9C703 DE996CD7 7F009ED1 19829639 6D57B06C 5225DEF4 5F3325D1
 1567E90F 60858412 AB1E106A 3110FD46 9439D60A 7FFB783D D740FDAC EC00C4B5
 388FFD58 436F2B2A A305F71B 00E91CAD 90B5F317 D705450E DC511A46 E777ACAC
 1C07F960 64CCE156 F65330FE 02
 quit
username netadmin privilege 15 password 7 082F495A081D081E1C
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 10.10.10.3 255.255.255.0
 duplex half
 speed auto
 no mop enabled
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
!
!
ip http server
ip http authentication local
```

```
ip http secure-server
!
dialer-list 1 protocol ip permit
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
banner login ^C
********** Warning  *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.

************************************************************^C
!
line con 0
 password 7 14041305060B392E
 login
line aux 0
line vty 0 4
 password 7 071C204244060A00
 login local
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
end
```


Ответы к лабораторной работе 4-9. Управление сеансами удаленного доступа

После выполнения этого упражнения конфигурация маршрутизатора рабочей группы будет выглядеть следующим образом (отличия зависят от рабочей группы):

```
!
!
version 12.4
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname RouterX
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$.dET$BDxkofHF3aAsRthe/c0.c.
enable password 7 14141B180F0B
!
no aaa new-model
!
!
ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 10.10.10.1 10.10.10.149
ip dhcp excluded-address 10.10.10.200 10.10.10.254
!
ip dhcp pool wgA_clients
  import all
  network 10.10.10.0 255.255.255.0
  lease 0 0 5
!
!
no ip domain lookup
ip domain name cisco.com
ip ssh version 2
!
!
voice-card 0
 no dspfarm
!
!
!
!
!
!
!
!
!
!
!
!
!
!
crypto pki trustpoint TP-self-signed-3715519608
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3715519608
```

```
 revocation-check none
 rsakeypair TP-self-signed-3715519608
!
!
crypto pki certificate chain TP-self-signed-3715519608
 certificate self-signed 01
 30820249 308201B2 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
 31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
 69666963 6174652D 33373135 35313936 3038301E 170D3037 30343035 32333135
 30305A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
 4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 37313535
 31393630 3830819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
 8100D0D2 4D67CC33 F0966C60 96BD12D2 675EB867 42087A6F 4310110E 1E852852
 E965291B A9E21580 7F77960A B83618A5 65A718BE 4E81DB21 669B48D1 172E1FF3
 73575C54 6B25A849 6E886C49 3EA0D03C CC5E7AFA 186AE594 22F612D6 8CA089EC
 355AFCF5 9FBA492A EEEB13C8 27A6F2BE EEC51E85 18B52144 10DDA46C C0831824
 D0450203 010001A3 71306F30 0F060355 1D130101 FF040530 030101FF 301C0603
 551D1104 15301382 1177675F 726F5F61 2E636973 636F2E63 6F6D301F 0603551D
 23041830 168014B7 CBDB7C0C C2AEB57B B2CA8F85 6C9567DA ACA8F430 1D060355
 1D0E0416 0414B7CB DB7C0CC2 AEB57BB2 CA8F856C 9567DAAC A8F4300D 06092A86
 4886F70D 01010405 00038181 0061FD2F C903A4A2 0E241513 68AD17EA 16856A52
 46C655CA 7AD9C703 DE996CD7 7F009ED1 19829639 6D57B06C 5225DEF4 5F3325D1
 1567E90F 60858412 AB1E106A 3110FD46 9439D60A 7FFB783D D740FDAC EC00C4B5
 388FFD58 436F2B2A A305F71B 00E91CAD 90B5F317 D705450E DC511A46 E777ACAC
 1C07F960 64CCE156 F65330FE 02
 quit
username netadmin privilege 15 password 7 082F495A081D081E1C
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 10.10.10.3 255.255.255.0
 duplex half
 speed auto
 no mop enabled
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
!
!
ip http server
ip http authentication local
ip http secure-server
!
```



```
dialer-list 1 protocol ip permit
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
banner login ^C
********** Warning  *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.

************************************************************^C
!
line con 0
 exec-timeout 60 0
 password 7 14041305060B392E
 logging synchronous
 login
 history size 100
line aux 0
line vty 0 4
 password 7 071C204244060A00
 logging synchronous
 login local
 history size 100
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
end
```

Ответы к лабораторной работе 5-1: Подключение к сети Интернет

После выполнения этого упражнения конфигурация маршрутизатора рабочей группы будет выглядеть следующим образом (отличия зависят от рабочей группы):

```
!
!
version 12.4
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname RouterX
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$.dET$BDxkofHF3aAsRthe/c0.c.
enable password 7 14141B180F0B
!
no aaa new-model
!
!
ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 10.10.10.1 10.10.10.149
ip dhcp excluded-address 10.10.10.200 10.10.10.254
!
ip dhcp pool wgA_clients
  import all
  network 10.10.10.0 255.255.255.0
  lease 0 0 5
!
!
no ip domain lookup
ip domain name cisco.com
ip ssh version 2
!
!
voice-card 0
 no dspfarm
!
!
!
!
!
!
!
!
!
!
!
!
!
!
crypto pki trustpoint TP-self-signed-3715519608
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3715519608
```



```
 revocation-check none
 rsakeypair TP-self-signed-3715519608
!
!
crypto pki certificate chain TP-self-signed-3715519608
 certificate self-signed 01
 30820249 308201B2 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
 31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
 69666963 6174652D 33373135 35313936 3038301E 170D3037 30343035 32333135
 30305A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
 4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 37313535
 31393630 3830819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
 8100D0D2 4D67CC33 F0966C60 96BD12D2 675EB867 42087A6F 4310110E 1E852852
 E965291B A9E21580 7F77960A B83618A5 65A718BE 4E81DB21 669B48D1 172E1FF3
 73575C54 6B25A849 6E886C49 3EA0D03C CC5E7AFA 186AE594 22F612D6 8CA089EC
 355AFCF5 9FBA492A EEEB13C8 27A6F2BE EEC51E85 18B52144 10DDA46C C0831824
 D0450203 010001A3 71306F30 0F060355 1D130101 FF040530 030101FF 301C0603
 551D1104 15301382 1177675F 726F5F61 2E636973 636F2E63 6F6D301F 0603551D
 23041830 168014B7 CBDB7C0C C2AEB57B B2CA8F85 6C9567DA ACA8F430 1D060355
 1D0E0416 0414B7CB DB7C0CC2 AEB57BB2 CA8F856C 9567DAAC A8F4300D 06092A86
 4886F70D 01010405 00038181 0061FD2F C903A4A2 0E241513 68AD17EA 16856A52
 46C655CA 7AD9C703 DE996CD7 7F009ED1 19829639 6D57B06C 5225DEF4 5F3325D1
 1567E90F 60858412 AB1E106A 3110FD46 9439D60A 7FFB783D D740FDAC EC00C4B5
 388FFD58 436F2B2A A305F71B 00E91CAD 90B5F317 D705450E DC511A46 E777ACAC
 1C07F960 64CCE156 F65330FE 02
 quit
username netadmin privilege 15 password 7 082F495A081D081E1C
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 10.10.10.3 255.255.255.0
 duplex half
 speed auto
 no mop enabled
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
!
!
ip http server
ip http authentication local
ip http secure-server
!
```

```
dialer-list 1 protocol ip permit
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
banner login ^C
**********  Предупреждение  *************
Доступ к этому устройству разрешен только санкционированным пользователям!
Несанкционированный доступ запрещен. Злоумышленники будут преследоваться
по закону.

**************************************************************^C
!
line con 0
 exec-timeout 60 0
 password 7 14041305060B392E
 logging synchronous
 login
 history size 100
line aux 0
line vty 0 4
 password 7 071C204244060A00
 logging synchronous
 login local
 history size 100
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
end
```


Ответы к лабораторной работе 5-2: Подключение к главному офису

После выполнения этого упражнения конфигурация маршрутизатора рабочей группы будет выглядеть следующим образом (отличия зависят от рабочей группы):

```
!
!
version 12.4
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname RouterX
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$.dET$BDxkofHF3aAsRthe/c0.c.
enable password 7 14141B180F0B
!
no aaa new-model
!
!
ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 10.10.10.1 10.10.10.149
ip dhcp excluded-address 10.10.10.200 10.10.10.254
!
ip dhcp pool wgA_clients
  import all
  network 10.10.10.0 255.255.255.0
  lease 0 0 5
!
!
no ip domain lookup
ip domain name cisco.com
ip ssh version 2
!
!
voice-card 0
 no dspfarm
!
!
!
!
!
!
!
!
!
!
!
!
!
!
crypto pki trustpoint TP-self-signed-3715519608
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3715519608
```

```
 revocation-check none
 rsakeypair TP-self-signed-3715519608
!
!
crypto pki certificate chain TP-self-signed-3715519608
 certificate self-signed 01
 30820249 308201B2 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
 31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
 69666963 6174652D 33373135 35313936 3038301E 170D3037 30343035 32333135
 30305A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
 4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 37313535
 31393630 3830819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
 8100D0D2 4D67CC33 F0966C60 96BD12D2 675EB867 42087A6F 4310110E 1E852852
 E965291B A9E21580 7F77960A B83618A5 65A718BE 4E81DB21 669B48D1 172E1FF3
 73575C54 6B25A849 6E886C49 3EA0D03C CC5E7AFA 186AE594 22F612D6 8CA089EC
 355AFCF5 9FBA492A EEEB13C8 27A6F2BE EEC51E85 18B52144 10DDA46C C0831824
 D0450203 010001A3 71306F30 0F060355 1D130101 FF040530 030101FF 301C0603
 551D1104 15301382 1177675F 726F5F61 2E636973 636F2E63 6F6D301F 0603551D
 23041830 168014B7 CBDB7C0C C2AEB57B B2CA8F85 6C9567DA ACA8F430 1D060355
 1D0E0416 0414B7CB DB7C0CC2 AEB57BB2 CA8F856C 9567DAAC A8F4300D 06092A86
 4886F70D 01010405 00038181 0061FD2F C903A4A2 0E241513 68AD17EA 16856A52
 46C655CA 7AD9C703 DE996CD7 7F009ED1 19829639 6D57B06C 5225DEF4 5F3325D1
 1567E90F 60858412 AB1E106A 3110FD46 9439D60A 7FFB783D D740FDAC EC00C4B5
 388FFD58 436F2B2A A305F71B 00E91CAD 90B5F317 D705450E DC511A46 E777ACAC
 1C07F960 64CCE156 F65330FE 02
 quit
username netadmin privilege 15 password 7 082F495A081D081E1C
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 10.10.10.3 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex half
 speed auto
 no mop enabled
!
interface FastEthernet0/1
 description $ETH-WAN$
 ip address dhcp client-id FastEthernet0/1
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface Serial0/0/0
 description Link to Main Office
 ip address 10.140.10.2 255.255.255.0
 encapsulation ppp
 no fair-queue
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
ip route 192.168.21.0 255.255.255.0 10.140.10.1
```



```
!
!
ip http server
ip http authentication local
ip http secure-server
ip nat inside source list 1 interface FastEthernet0/1 overload
!
access-list 1 remark INSIDE_IF=FastEthernet0/0
access-list 1 remark SDM_ACL Category=2
access-list 1 permit 10.10.10.0 0.0.0.255
dialer-list 1 protocol ip permit
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
banner login ^C
********** Warning  *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.

************************************************************^C
!
line con 0
 exec-timeout 60 0
 password 7 14041305060B392E
 logging synchronous
 login
 history size 100
line aux 0
line vty 0 4
 password 7 071C204244060A00
 logging synchronous
 login local
 history size 100
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
end
```

Ответы к лабораторной работе 5-3: Обеспечение динамической маршрутизации к главному офису

После выполнения этого упражнения конфигурация маршрутизатора рабочей группы будет выглядеть следующим образом (отличия зависят от рабочей группы):

```
!
!
version 12.4
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname RouterX
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$.dET$BDxkofHF3aAsRthe/c0.c.
enable password 7 14141B180F0B
!
no aaa new-model
!
!
ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 10.10.10.1 10.10.10.149
ip dhcp excluded-address 10.10.10.200 10.10.10.254
!
ip dhcp pool wgA_clients
  import all
  network 10.10.10.0 255.255.255.0
  lease 0 0 5
!
!
no ip domain lookup
ip domain name cisco.com
ip ssh version 2
!
!
voice-card 0
 no dspfarm
!
!
!
!
!
!
!
!
!
!
!
!
!
```



```
crypto pki trustpoint TP-self-signed-3715519608
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3715519608
 revocation-check none
 rsakeypair TP-self-signed-3715519608
!
!
crypto pki certificate chain TP-self-signed-3715519608
 certificate self-signed 01
 30820249 308201B2 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
 31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
 69666963 6174652D 33373135 35313936 3038301E 170D3037 30343035 32333135
 30305A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
 4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 37313535
 31393630 3830819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
 8100D0D2 4D67CC33 F0966C60 96BD12D2 675EB867 42087A6F 4310110E 1E852852
 E965291B A9E21580 7F77960A B83618A5 65A718BE 4E81DB21 669B48D1 172E1FF3
 73575C54 6B25A849 6E886C49 3EA0D03C CC5E7AFA 186AE594 22F612D6 8CA089EC
 355AFCF5 9FBA492A EEEB13C8 27A6F2BE EEC51E85 18B52144 10DDA46C C0831824
 D0450203 010001A3 71306F30 0F060355 1D130101 FF040530 030101FF 301C0603
 551D1104 15301382 1177675F 726F5F61 2E636973 636F2E63 6F6D301F 0603551D
 23041830 168014B7 CBDB7C0C C2AEB57B B2CA8F85 6C9567DA ACA8F430 1D060355
 1D0E0416 0414B7CB DB7C0CC2 AEB57BB2 CA8F856C 9567DAAC A8F4300D 06092A86
 4886F70D 01010405 00038181 0061FD2F C903A4A2 0E241513 68AD17EA 16856A52
 46C655CA 7AD9C703 DE996CD7 7F009ED1 19829639 6D57B06C 5225DEF4 5F3325D1
 1567E90F 60858412 AB1E106A 3110FD46 9439D60A 7FFB783D D740FDAC EC00C4B5
 388FFD58 436F2B2A A305F71B 00E91CAD 90B5F317 D705450E DC511A46 E777ACAC
 1C07F960 64CCE156 F65330FE 02
 quit
username netadmin privilege 15 password 7 082F495A081D081E1C
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 10.10.10.3 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex half
 speed auto
 no mop enabled
!
interface FastEthernet0/1
 description $ETH-WAN$
 ip address dhcp client-id FastEthernet0/1
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface Serial0/0/0
 description Link to Main Office
 ip address 10.140.10.2 255.255.255.0
 encapsulation ppp
 no fair-queue
!
interface Serial0/0/1
 no ip address
 shutdown
```

```
 clock rate 2000000
!
router rip
 version 2
 network 10.0.0.0
!
!
!
ip http server
ip http authentication local
ip http secure-server
ip nat inside source list 1 interface FastEthernet0/1 overload
!
access-list 1 remark INSIDE_IF=FastEthernet0/0
access-list 1 remark SDM_ACL Category=2
access-list 1 permit 10.10.10.0 0.0.0.255
dialer-list 1 protocol ip permit
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
banner login ^C
********** Warning  *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.

************************************************************^C
!
line con 0
 exec-timeout 60 0
 password 7 14041305060B392E
 logging synchronous
 login
 history size 100
line aux 0
line vty 0 4
 password 7 071C204244060A00
 logging synchronous
 login local
 history size 100
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
end
```


Ответы к лабораторной работе 6-1: Использование протокола обнаружения Cisco

После выполнения этого упражнения конфигурация маршрутизатора рабочей группы будет выглядеть следующим образом (отличия зависят от рабочей группы):

```
!
version 12.4
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname RouterX
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$.dET$BDxkofHF3aAsRthe/c0.c.
enable password 7 14141B180F0B
!
no aaa new-model
!
!
ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 10.10.10.1 10.10.10.149
ip dhcp excluded-address 10.10.10.200 10.10.10.254
!
ip dhcp pool wgA_clients
  import all
  network 10.10.10.0 255.255.255.0
  lease 0 0 5
!
!
no ip domain lookup
ip domain name cisco.com
ip ssh version 2
!
!
voice-card 0
 no dspfarm
!
!
!
!
!
!
!
!
!
!
!
!
!
!
crypto pki trustpoint TP-self-signed-3715519608
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3715519608
 revocation-check none
```

```
 rsakeypair TP-self-signed-3715519608
!
!
crypto pki certificate chain TP-self-signed-3715519608
 certificate self-signed 01
 30820249 308201B2 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
 31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
 69666963 6174652D 33373135 35313936 3038301E 170D3037 30343035 32333135
 30305A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
 4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 37313535
 31393630 3830819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
 8100D0D2 4D67CC33 F0966C60 96BD12D2 675EB867 42087A6F 4310110E 1E852852
 E965291B A9E21580 7F77960A B83618A5 65A718BE 4E81DB21 669B48D1 172E1FF3
 73575C54 6B25A849 6E886C49 3EA0D03C CC5E7AFA 186AE594 22F612D6 8CA089EC
 355AFCF5 9FBA492A EEEB13C8 27A6F2BE EEC51E85 18B52144 10DDA46C C0831824
 D0450203 010001A3 71306F30 0F060355 1D130101 FF040530 030101FF 301C0603
 551D1104 15301382 1177675F 726F5F61 2E636973 636F2E63 6F6D301F 0603551D
 23041830 168014B7 CBDB7C0C C2AEB57B B2CA8F85 6C9567DA ACA8F430 1D060355
 1D0E0416 0414B7CB DB7C0CC2 AEB57BB2 CA8F856C 9567DAAC A8F4300D 06092A86
 4886F70D 01010405 00038181 0061FD2F C903A4A2 0E241513 68AD17EA 16856A52
 46C655CA 7AD9C703 DE996CD7 7F009ED1 19829639 6D57B06C 5225DEF4 5F3325D1
 1567E90F 60858412 AB1E106A 3110FD46 9439D60A 7FFB783D D740FDAC EC00C4B5
 388FFD58 436F2B2A A305F71B 00E91CAD 90B5F317 D705450E DC511A46 E777ACAC
 1C07F960 64CCE156 F65330FE 02
 quit
username netadmin privilege 15 password 7 082F495A081D081E1C
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 10.10.10.3 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex half
 speed auto
 no mop enabled
!
interface FastEthernet0/1
 description $ETH-WAN$
 ip address dhcp client-id FastEthernet0/1
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
 no cdp enable
!
interface Serial0/0/0
 description Link to Main Office
 ip address 10.140.10.2 255.255.255.0
 encapsulation ppp
 no fair-queue
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
router rip
```



```
 version 2
 network 10.0.0.0
!
!
!
ip http server
ip http authentication local
ip http secure-server
ip nat inside source list 1 interface FastEthernet0/1 overload
!
access-list 1 remark INSIDE_IF=FastEthernet0/0
access-list 1 remark SDM_ACL Category=2
access-list 1 permit 10.10.10.0 0.0.0.255
dialer-list 1 protocol ip permit
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
banner login ^C
********** Warning  *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.

************************************************************^C
!
line con 0
 exec-timeout 60 0
 password 7 14041305060B392E
 logging synchronous
 login
 history size 100
line aux 0
line vty 0 4
 password 7 071C204244060A00
 logging synchronous
 login local
 history size 100
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
end

!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname SwitchX
```

```
!
enable secret 5 $1$A11O$0z83HwmswM/vk5.RSZpVr.
enable password 7 05080F1C2243
!
username netadmin password 7 030A5E1F070B2C4540
no aaa new-model
ip subnet-zero
!
no ip domain-lookup
ip domain-name cisco.com
ip ssh version 2
!
!
crypto pki trustpoint TP-self-signed-1833200768
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1833200768
 revocation-check none
 rsakeypair TP-self-signed-1833200768
!
!
crypto ca certificate chain TP-self-signed-1833200768
 certificate self-signed 01
 3082028D 308201F6 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
 53312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
 69666963 6174652D 31383333 32303037 36383120 301E0609 2A864886 F70D0109
 02161177 675F7377 5F612E63 6973636F 2E636F6D 301E170D 39333033 30313030
 30313033 5A170D32 30303130 31303030 3030305A 3053312F 302D0603 55040313
 26494F53 2D53656C 662D5369 676E6564 2D436572 74696669 63617465 2D313833
 33323030 37363831 20301E06 092A8648 86F70D01 09021611 77675F73 775F612E
 63697363 6F2E636F 6D30819F 300D0609 2A864886 F70D0101 01050003 818D0030
 81890281 8100B444 4F07E979 88953526 E0B8480C 52DBC1E7 E5FF660A 41932329
 8FB4A8EE 142FAEC4 744CB8BE 021BDAE5 BF005CA6 99D0BDC7 68C4A873 25A2F06C
 E460FAE5 1435B900 43505E02 3F0F5E4B D61D6787 59B6AE32 13558C75 561A6BB0
 42C15C96 D078A449 669E4B58 CD5857D0 1B570F43 008B811F 45CD05B0 50D144BA
 F83865F5 8BFD0203 010001A3 71306F30 0F060355 1D130101 FF040530 030101FF
 301C0603 551D1104 15301382 1177675F 73775F61 2E636973 636F2E63 6F6D301F
 0603551D 23041830 16801414 679B7C0E C82E65FB 8953EC84 1FC9DD49 E672A630
 1D060355 1D0E0416 04141467 9B7C0EC8 2E65FB89 53EC841F C9DD49E6 72A6300D
 06092A86 4886F70D 01010405 00038181 006C7E92 A7F96199 D1D81ADA FA16C868
 0660013D 4A91A319 6D6DBD61 B5147AAA FF0FCF26 3DF20CA7 9694B3B8 24ABBEAC
 F8942F5F E53466BB 04E12200 25432AFE A09DDFCF A07A5A4A 145BE58D 4040040A
 5B085A4E 895C45BC 4DF264BC BFE32124 F4AA3BDB B9CF2CC2 35F3B42A B16BFD69
 44531337 B03B7055 48A0B320 0A6C3173 C0
 quit
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0017.5a78.be01
 switchport port-security mac-address sticky 001a.2fe7.3089
!
```



```
interface FastEthernet0/2
 switchport mode access
!
interface FastEthernet0/3
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/4
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/5
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/6
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/7
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/8
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/9
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/10
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/11
 switchport mode access
 no cdp enable
!
interface FastEthernet0/12
 switchport mode access
 no cdp enable
!
interface FastEthernet0/13
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/14
 switchport mode access
 shutdown
 no cdp enable
!
```

```
interface FastEthernet0/15
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/16
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/17
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/18
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/19
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/20
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/21
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/22
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/23
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/24
 switchport mode access
 shutdown
 no cdp enable
!
interface GigabitEthernet0/1
 switchport mode access
 shutdown
 no cdp enable
!
interface GigabitEthernet0/2
 switchport mode access
 shutdown
 no cdp enable
!
interface Vlan1
```



```
 ip address 10.10.10.11 255.255.255.0
 no ip route-cache
!
ip default-gateway 10.10.10.3
ip http server
ip http secure-server
!
control-plane
!
banner login ^C
********** Warning  *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.

************************************************************^C
!
line con 0
 exec-timeout 60 0
 password 7 111A180B1D1D1809
 logging synchronous
 login
 history size 100
line vty 0 4
 password 7 111A180B1D1D1809
 logging synchronous
 login local
 history size 100
line vty 5 15
 password 7 111A180B1D1D1809
 logging synchronous
 login local
 history size 100
!
end
```

Ответы к лабораторной работе 6-2: Управление параметрами запуска маршрутизатора

После выполнения этого упражнения конфигурация маршрутизатора рабочей группы будет выглядеть следующим образом (отличия зависят от рабочей группы):

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname RouterX
!
boot-start-marker
boot system tftp c2800nm-advipservicesk9-mz.124-12.bin 10.10.10.1
boot system flash c2800nm-advipservicesk9-mz.124-12.bin
boot system flash
boot-end-marker
!
no logging buffered
enable secret 5 $1$X.GH$OkseupwTuqqjGp4oP4Fdg0
enable password 7 121A0C041104
!
no aaa new-model
!
!
ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 10.10.10.1 10.10.10.149
ip dhcp excluded-address 10.10.10.200 10.10.10.254
!
ip dhcp pool wgA_clients
  import all
  network 10.10.10.0 255.255.255.0
  default-router 10.10.10.3
  lease 0 0 5
!
!
no ip domain lookup
ip domain name cisco.com
ip ssh version 2
!
!
voice-card 0
 no dspfarm
!
!
!
!
!
!
!
!
!
!
!
```



```
!
!
crypto pki trustpoint TP-self-signed-3715519608
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3715519608
 revocation-check none
 rsakeypair TP-self-signed-3715519608
!
!
crypto pki certificate chain TP-self-signed-3715519608
 certificate self-signed 01
 30820249 308201B2 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
 31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
 69666963 6174652D 33373135 35313936 3038301E 170D3037 30343035 32333135
 30305A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
 4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 37313535
 31393630 3830819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
 8100D0D2 4D67CC33 F0966C60 96BD12D2 675EB867 42087A6F 4310110E 1E852852
 E965291B A9E21580 7F77960A B83618A5 65A718BE 4E81DB21 669B48D1 172E1FF3
 73575C54 6B25A849 6E886C49 3EA0D03C CC5E7AFA 186AE594 22F612D6 8CA089EC
 355AFCF5 9FBA492A EEEB13C8 27A6F2BE EEC51E85 18B52144 10DDA46C C0831824
 D0450203 010001A3 71306F30 0F060355 1D130101 FF040530 030101FF 301C0603
 551D1104 15301382 1177675F 726F5F61 2E636973 636F2E63 6F6D301F 0603551D
 23041830 168014B7 CBDB7C0C C2AEB57B B2CA8F85 6C9567DA ACA8F430 1D060355
 1D0E0416 0414B7CB DB7C0CC2 AEB57BB2 CA8F856C 9567DAAC A8F4300D 06092A86
 4886F70D 01010405 00038181 0061FD2F C903A4A2 0E241513 68AD17EA 16856A52
 46C655CA 7AD9C703 DE996CD7 7F009ED1 19829639 6D57B06C 5225DEF4 5F3325D1
 1567E90F 60858412 AB1E106A 3110FD46 9439D60A 7FFB783D D740FDAC EC00C4B5
 388FFD58 436F2B2A A305F71B 00E91CAD 90B5F317 D705450E DC511A46 E777ACAC
 1C07F960 64CCE156 F65330FE 02
 quit
username netadmin privilege 15 password 7 0208014F0A02022842
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 10.10.10.3 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex half
 speed auto
 no mop enabled
!
interface FastEthernet0/1
 description $ETH-WAN$
 ip address dhcp client-id FastEthernet0/1
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
 no cdp enable
!
interface Serial0/0/0
 description Link to Main Office
 ip address 10.140.10.2 255.255.255.0
 encapsulation ppp
 no fair-queue
!
```

```
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
router rip
 version 2
 network 10.0.0.0
!
!
!
ip http server
ip http authentication local
no ip http secure-server
ip nat inside source list 1 interface FastEthernet0/1 overload
!
access-list 1 remark INSIDE_IF=FastEthernet0/0
access-list 1 remark SDM_ACL Category=2
access-list 1 permit 10.10.10.0 0.0.0.255
dialer-list 1 protocol ip permit
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
banner login ^C
********** Warning  *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.

************************************************************^C
!
line con 0
 exec-timeout 60 0
 password 7 051807012B435D0C
 logging synchronous
 login
 history size 100
line aux 0
line vty 0 4
 password 7 051807012B435D0C
 logging synchronous
 login local
 history size 100
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
end
```


Ответы к лабораторной работе 6-3: Управление устройствами Cisco

После выполнения этого упражнения конфигурация маршрутизатора рабочей группы будет выглядеть следующим образом (отличия зависят от рабочей группы):

```
There were no overall changes to the configuration.!
```

Ответы к лабораторной работе 6-4: Подтверждение реконфигурации сети филиала

После выполнения этого упражнения конфигурация маршрутизатора рабочей группы будет выглядеть следующим образом (отличия зависят от рабочей группы):

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname RouterXX
!
boot-start-marker
boot system flash c2800nm-advipservicesk9-mz.124-12.bin
boot system tftp c2800nm-advipservicesk9-mz.124-12.bin 10.10.10.1
boot system flash
boot-end-marker
!
enable secret 5 $1$t7tb$L8Par/.s/MaoshaZH1cLq0
enable password 7 0822455D0A16
!
no aaa new-model
!
!
ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 10.10.10.1 10.10.10.149
ip dhcp excluded-address 10.10.10.200 10.10.10.254
!
ip dhcp pool branchXX-clients
  import all
  network 10.10.10.0 255.255.255.0
  default-router 10.10.10.3
  lease 0 0 5
!
!
ip domain name cisco.com
ip ssh version 2
!
!
voice-card 0
 no dspfarm
!
!
!
!
!
!
!
!
!
!
!
!
!
```



```
crypto pki trustpoint TP-self-signed-3575601183
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3575601183
 revocation-check none
 rsakeypair TP-self-signed-3575601183
!
!
crypto pki certificate chain TP-self-signed-3575601183
 certificate self-signed 01
 3082023F 308201A8 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
 31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
 69666963 6174652D 33353735 36303131 3833301E 170D3037 30353034 32313439
 31315A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
 4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 35373536
 30313138 3330819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
 8100E3CA 6B4F5C16 545F1796 C3600BE9 433F7C87 CB676A33 D42BF42A A6433BAF
 25582787 6028AE73 F3EAFD24 EA37AFEE CF6F101D 14EF2CCF 8EF4085C 2ED0E54B
 E1758915 13A5499E 378275C7 3BBE4F32 009DB10E 5039EB40 2C43D4EA 1407B634
 A0EFEB26 23E4045E EAFE99BE 88C4DA01 357684AC 65572494 ABDC6A99 AA85D645
 D8530203 010001A3 67306530 0F060355 1D130101 FF040530 030101FF 30120603
 551D1104 0B300982 07526F75 74657258 301F0603 551D2304 18301680 14E0035D
 916FE499 69EDA5C0 C15FDB83 17F62591 45301D06 03551D0E 04160414 E0035D91
 6FE49969 EDA5C0C1 5FDB8317 F6259145 300D0609 2A864886 F70D0101 04050003
 81810070 7B5F8CB1 BB014CBA 3E317573 C2303187 3534E5C7 71FDDDE5 EC4D6331
 A0498B71 49FE6A9A 5A5F6703 091EBDDC B828F955 4851F005 B214B407 4A0E67C0
 87AC8E94 52F130E9 73E28BD9 EC4A028B 6424BCF2 EF0A993C 1BA75BED E3E0D217
 E1129982 E1A40C9C 98F43F91 363474F2 97E3BBFF E60A7AA5 01327A27 EA69FCE6 0C4D36
 quit
username netadmin privilege 15 password 7 0505031B2048430017
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 10.10.10.3 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description $ETH-WAN$
 ip address dhcp client-id FastEthernet0/1
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
 no cdp enable
!
interface Serial0/0/0
 ip address 10.140.100.2 255.255.255.0
 encapsulation ppp
 no cdp enable
!
interface Serial0/0/1
 no ip address
 shutdown
 no cdp enable
!
```

```
router rip
 version 2
 network 10.0.0.0
!
!
!
ip http server
ip http authentication local
ip http secure-server
ip nat inside source list 1 interface FastEthernet0/1 overload
!
access-list 1 remark INSIDE_IF=FastEthernet0/0
access-list 1 remark SDM_ACL Category=2
access-list 1 permit 10.10.10.0 0.0.0.255
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
banner login _
********** Warning  *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.

**********************************************************^C
!
line con 0
 exec-timeout 60 0
 password 7 08324D4003161612
 logging synchronous
 login
 history size 100
line aux 0
line vty 0 4
 logging synchronous
 login local
 history size 100
 transport input ssh
!
scheduler allocate 20000 1000
!
end

!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname SwitchXX
!
```



```
enable secret 5 $1$LLvt$3gBuRQzm6eAcGfQjsgHC01
enable password 7 01100F175804
!
username netadmin privilege 15 password 7 1419171F0D0027222A
no aaa new-model
ip subnet-zero
!
no ip domain-lookup
ip domain-name cisco.com
ip ssh version 2
!
!
crypto pki trustpoint TP-self-signed-809024768
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-809024768
 revocation-check none
 rsakeypair TP-self-signed-809024768
!
!
crypto ca certificate chain TP-self-signed-809024768
 certificate self-signed 01
 3082028B 308201F4 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
 52312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
 69666963 6174652D 38303930 32343736 38312030 1E06092A 864886F7 0D010902
 16115377 69746368 582E6369 73636F2E 636F6D30 1E170D39 33303330 31303030
 3130305A 170D3230 30313031 30303030 30305A30 52312E30 2C060355 04031325
 494F532D 53656C66 2D536967 6E65642D 43657274 69666963 6174652D 38303930
 32343736 38312030 1E06092A 864886F7 0D010902 16115377 69746368 582E6369
 73636F2E 636F6D30 819F300D 06092A86 4886F70D 01010105 0003818D 00308189
 02818100 D2D79D92 1395A6CB 46CAAD3C 6873B3D3 75B1B226 1E4EC5BC 87906C24
 DAC40D83 6380CE06 C04AE1DE B6DBD7A4 5941D5E5 C2FA7464 DC6135A6 EFED87E4
 966DC533 6BB18EDF 213503E7 B5B0E919 99C666B9 89AB8988 553288C0 400D6821
 912B2908 B076FE8D 4645B79C 1FDEEBEF 83DBB7AF 3C92B363 52F68131 E2BEEDC3
 4E0CC8FB 02030100 01A37130 6F300F06 03551D13 0101FF04 05300301 01FF301C
 0603551D 11041530 13821153 77697463 68582E63 6973636F 2E636F6D 301F0603
 551D2304 18301680 14B5A18A 31CE43E7 9D9704B4 815246B1 3D601AB8 A7301D06
 03551D0E 04160414 B5A18A31 CE43E79D 9704B481 5246B13D 601AB8A7 300D0609
 2A864886 F70D0101 04050003 81810007 16DD332F F2711854 434842FA 026C6F29
 82718220 8249778B 4CDFFE66 1B52B55E AA6BC328 CF0CD466 E9DE6464 CF1836A3
 F62723B8 14D8A873 535C205E BDC26BAC E73C448D 0E0B8194 402C6A67 CD6EFA78
 CDD0A83A 0335EB3E 9ADCA41E 768FA332 572AE050 1121207E D4E79437 894E3588
 65E3D60A 57150B63 9206A35B C71BB9
 quit
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0017.5a78.be0f
 switchport port-security mac-address sticky 001a.2fe7.3089
 no cdp enable
!
```

```
interface FastEthernet0/2
 switchport mode access
!
interface FastEthernet0/3
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/4
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/5
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/6
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/7
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/8
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/9
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/10
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/11
 switchport mode access
 no cdp enable
!
interface FastEthernet0/12
 switchport mode access
 no cdp enable
!
interface FastEthernet0/13
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/14
 switchport mode access
 shutdown
 no cdp enable
!
```



```
interface FastEthernet0/15
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/16
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/17
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/18
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/19
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/20
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/21
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/22
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/23
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/24
 switchport mode access
 shutdown
 no cdp enable
!
interface GigabitEthernet0/1
 switchport mode access
 shutdown
 no cdp enable
!
interface GigabitEthernet0/2
 switchport mode access
 shutdown
 no cdp enable
!
interface Vlan1
```

```
 ip address 10.10.10.11 255.255.255.0
 no ip route-cache
!
ip default-gateway 10.10.10.3
ip http server
ip http secure-server
!
control-plane
!
banner login _
********** Warning  *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.

**************************************************************^C
!
line con 0
 exec-timeout 60 0
 password 7 04480A08052E5F4B
 logging synchronous
 login
 history size 100
line vty 0 4
 password 7 03175A01091C24
 logging synchronous
 login local
 history size 100
 transport input ssh
line vty 5 15
 password 7 001712080E541803
 logging synchronous
 login local
 history size 100
 transport input ssh
!
end
```

