ICND2

Interconnecting Cisco Networking Devices Part 2

Версия 1.0

Руководство по лабораторным работам

Номер текста по каталогу: 97-2512-01

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.**

ПРАКТИКИ ЗАКЛЮЧЕНИЯ СДЕЛОК, ИСПОЛЬЗОВАНИЕ ИЛИ ТОРГОВЛИ. Этот обучающий продукт может включать содержимое из ранних версий и, хотя компания Cisco считает его точным, такое содержимое подчиняется вышеизложенным условиям отказа от гарантий.

Содержание

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 «Ключ к лабораторным работам».

План

Это руководство охватывает следующие упражнения:

- Лабораторная работа 1-1: внедрение малой сети (лабораторная работа для повторения пройденного).
- Лабораторная работа 2-1: настройка расширенных коммутируемых сетей.
- Лабораторная работа 2-2: устранение неполадок в коммутируемых сетях.
- Лабораторная работа 4-1: внедрение OSPF.
- Лабораторная работа 4-2: устранение неполадок OSPF.
- Лабораторная работа 5-1: внедрение EIGRP.
- Лабораторная работа 5-2: устранение неполадок EIGRP.
- Лабораторная работа 6-1: внедрение и устранение неполадок списков контроля доступа (ACL)
- Лабораторная работа 7-1: настройка NAT (преобразование сетевых адресов) и PAT (преобразование адресов портов).
- Лабораторная работа 7-2: внедрение IPv6.
- Лабораторная работа 8-1: создание глобальной сети на базе Frame Relay.
- Лабораторная работа 8-2: устранение неполадок в глобальных сетях на базе Frame Relay.
- Ключ.

Лабораторная работа 1-1: внедрение малой сети (лабораторная работа для повторения пройденного)

Выполните упражнения данной лабораторной работы, чтобы применить на практике сведения, которые вы повторили в соответствующем модуле.

Задачи упражнения

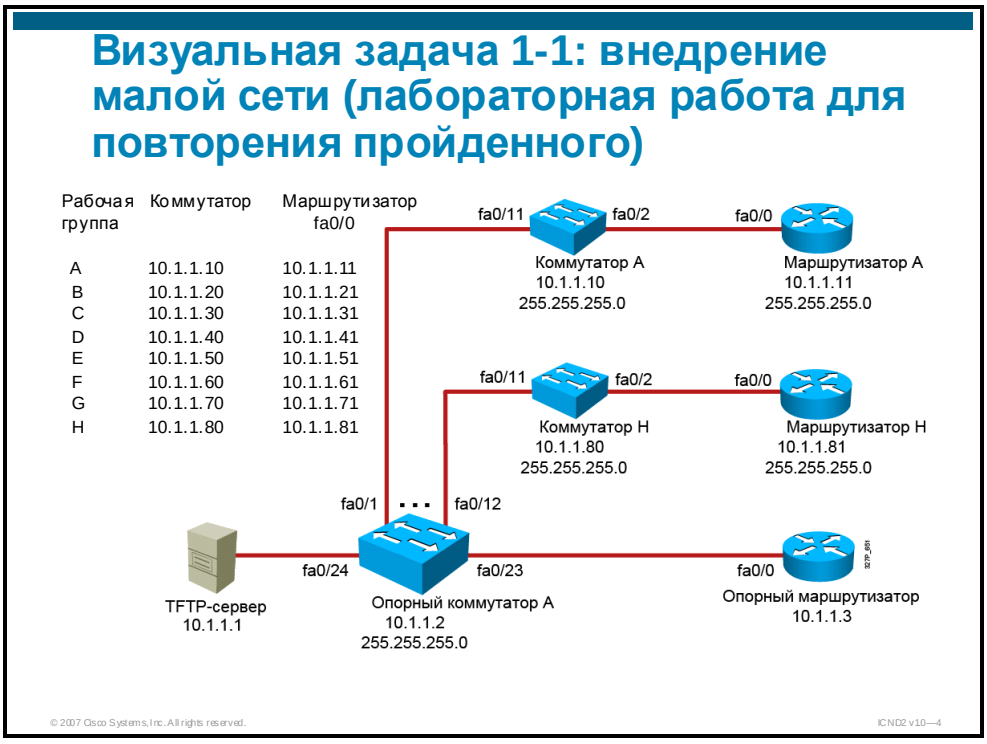
В этом упражнении вы должны воспользоваться навыками и знаниями, полученными до этого курса, чтобы развернуть малую сеть. Используйте команды, которые вы повторили в соответствующем модуле, чтобы создать базовую конфигурацию коммутатора и маршрутизатора рабочей группы для IP-подключений.

После выполнения этого упражнения вы должны быть готовы к следующим задачам:

- возвращение коммутатора и маршрутизатора рабочей группы к конфигурациям по умолчанию;
- настройка коммутатора и маршрутизатора рабочей группы с верными удостоверениями и IP-адресацией;
- обеспечение безопасности сети на базовом уровне с помощью паролей и средств защиты портов.

Визуальная задача

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 локальной лаборатории или ПК с Интернет-подключением и доступом к удаленной лаборатории.
- Терминальный сервер, подключенный к консольному порту всех лабораторных устройств (при использовании удаленной лаборатории).
- Рабочая группа ICND, назначенная инструктором.

Инструктор предоставит сведения о конфигурации, которая понабится для выполнения этого и всех последующих упражнениях. Кроме того, инструктор назначит вас в группу с буквенным идентификатором (от A до H). Заполните форму ниже в соответствии с информацией, предоставленной инструктором.

Значение	**Информация, предоставленная инструктором**
Рабочая группа	
IP-адрес терминала	
Маска подсети	
IP-адрес шлюза по умолчанию	
IP-адрес терминального сервера	
Имя пользователя для доступа к терминальному серверу	
Пароль для доступа к терминальному серверу	
IP-адрес TFTP-сервера	

Список команд

В таблице приводится описание команд, используемых в упражнении. Команды перечислены в алфавитном порядке, что позволит легко найти нужные сведения. Если во время упражнения вам потребуется помощь по командам конфигурации, воспользуйтесь этим списком.

Обзор команд

Команда	Описание
banner motd	Настраивает баннер "Сообщение дня".
configure terminal	Активирует режим глобальной конфигурации.
copy running-config startup-config	Сохраняет работающую конфигурацию в энергонезависимую память (NVRAM) в качестве загрузочной конфигурации.
description	Добавляет описательный комментарий в конфигурацию интерфейса. Эта функция может быть полезна в сложных конфигурациях.
duplex full	Включает полнодуплексный режим интерфейса.
enable	Открывает интерпретатор команд в привилегированном режиме EXEC.
enable secret *пароль*	Устанавливает и активирует пароль для входа в привилегированный режим EXEC.
erase startup-configuration	Удаляет загрузочную конфигурацию из NVRAM.
hostname *имя*	Присваивает устройству имя узла.
interface *интерфейс*	Указывает интерфейс и активирует режим конфигурации для этого интерфейса.
ip address *маска адреса*	Устанавливает IP-адрес и маску устройства.
ip default-gateway *адрес*	Устанавливает шлюз по умолчанию для коммутатора.
line console 0	Указывает канал консоли и активирует режим конфигурации для этого канала.
line vty 0 4	Указывает канал VTY и активирует режим конфигурации для этого канала.
login	Активирует запрос пароля при входе в систему.
logging synchronous	Включает синхронное ведение журнала сообщений.
password *пароль*	Устанавливает пароль в канале.
ping *ip-адрес*	Использует эхо-запросы и эхо-ответы ICMP, чтобы определить, доступен ли удаленный узел.
reload	Перезагружает устройство, чтобы применить изменения конфигурации.
show cdp neighbors	Отображает обновления протокола CDP (протокола обнаружения Cisco), полученные на всех локальных интерфейсах устройства.
show interfaces	Отображает сведения обо всех интерфейсах устройства.
show port-security [interface *идентификатор интерфейса*] [address]	Отображает административные и операционные состояния всех защищенных портов коммутатора. Также может отображать параметры безопасности определенного интерфейса или все защищенные MAC-адреса.
show running-configuration	Отображает активную конфигурацию.
show startup-configuration	Отображает параметры загрузочной конфигурации, сохраненной в NVRAM.

Команда	Описание
shutdown/no shutdown	Отключает или включает интерфейс.
speed *скорость*	Устанавливает скорость передачи данных порта.
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 *mac-адрес*	Назначает порту безопасный MAC-адрес. Используйте версию "**no**" этой команды, чтобы удалить MAC-адрес.
switchport port-security maximum *значение*	Устанавливает максимальное количество безопасных MAC-адресов для интерфейса.

Подсказки

Для этого упражнения доступны следующие подсказки.

Рабочая группа (WG)	Имя маршрути-затора	Интерфейс Fa0/0 маршрутизатора (Router*X*)	Имя комму-татора	Сеть VLAN 1 интерфейса коммутатора (Switch*X*)	Порт Switch*X* (к центральным устройствам)	Порт центрального коммутатора A (к рабочей группе)
A	RouterA	10.1.1.11/24	SwitchA	10.1.1.10/24	Fa0/11	Fa0/1
B	RouterB	10.1.1.21/24	SwitchB	10.1.1.20/24	Fa0/11	Fa0/2
C	RouterC	10.1.1.31/24	SwitchC	10.1.1.30/24	Fa0/11	Fa0/3
D	RouterD	10.1.1.41/24	SwitchD	10.1.1.40/24	Fa0/11	Fa0/4
E	RouterE	10.1.1.51/24	SwitchE	10.1.1.50/24	Fa0/11	Fa0/5
F	RouterF	10.1.1.61/24	SwitchF	10.1.1.60/24	Fa0/11	Fa0/6
G	RouterG	10.1.1.71/24	SwitchG	10.1.1.70/24	Fa0/11	Fa0/7
H	RouterH	10.1.1.81/24	Switch H	10.1.1.80/24	Fa0/11	Fa0/8

Задача 1: настройка коммутатора рабочей группы.

Используйте команды, которые вы повторили в соответствующем модуле, чтобы создать базовую конфигурацию маршрутизатора рабочей группы для IP-подключений.

Процедура упражнения

Выполните следующие действия.

Действие 1 Со своего ПК создайте подключение к лабораторному оборудованию.

Действие 2 Выберите свою рабочую группу в главном меню.

Действие 3 Выберите маршрутизатор рабочей группы в меню "Модуль". Если система попросит ввести пароль, попробуйте пароль **cisco** (или спросите пароль у инструктора).

Действие 4 Войдите в привилегированный режим EXEC. Если система предложит ввести пароль для перехода в привилегированный режим EXEC, попробуйте пароль **sanfran**. Если пароль **sanfran** не работает, обратитесь к инструктору.

Действие 5 Удалите загрузочную конфигурацию маршрутизатора рабочей группы.

Действие 6 Перезагрузите маршрутизатор рабочей группы. Когда система предложит сохранить изменения, выберите **N**. когда система предложит подтвердить перезагрузку, выберите **Y**.

Действие 7 После перезагрузки маршрутизатора рабочей группы система предложит войти в диалоговое окно конфигурации (Configuration Dialog) Выберите **N**. Если система предложит завершить работу службы AutoInstall, выберите **Y**.

Действие 8 Задайте имя узла для маршрутизатора рабочей группы. Используйте имя, указанное в таблице подсказок для этого упражнения.

Действие 9 Настройте и активируйте пароль **sanfran**, он будет использоваться для доступа к привилегированному режиму EXEC.

Действие 10 Назначьте IP-адрес первому Ethernet-интерфейсу (Fa0/0) маршрутизатора рабочей группы. См. нужный IP-адрес в подсказках для этого упражнения.

Действие 11 Включите первый Ethernet-интерфейс (Fa0/0) маршрутизатора рабочей группы

Действие 12 Введите описание конфигурации интерфейса с описанием подключенного пункта назначения.

Действие 13 Задайте баннерное сообщение с предупреждением, запрещающим вход для неавторизованных пользователей.

Действие 14 Включите запрос пароля при доступе к маршрутизатору с консольного порта. Задайте пароль **cisco**.

Действие 15 Включите запрос пароля при доступе к маршрутизатору с первых пяти каналов VTY (0–4). Задайте пароль **sanjose**.

Действие 16 Введите команду **logging synchronous** для консольного порта.

Действие 17 Сохраните работающую конфигурацию в NVRAM.

Действие 18 Воспользуйтесь следующими командами, чтобы проверить параметры конфигурации:

- **show interfaces**

  Каков MAC-адрес первого Ethernet-интерфейс маршрутизатора (Fa0/0), подключенного к коммутатору рабочей группы? (Эта информация потребуется для следующей задачи.)

  _____

- **show running-configuration**
- **show startup-configuration**

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- маршрутизатор рабочей группы имеет верное удостоверение и IP-адрес;
- на маршрутизаторе рабочей группы настроены базовые средства безопасности с паролями.

Задача 2: настройка коммутатора рабочей группы.

Используйте команды, которые вы повторили в соответствующем модуле, чтобы создать базовую конфигурацию коммутатора рабочей группы для IP-подключений.

Процедура упражнения

Выполните следующие действия.

Действие 1 Со своего ПК создайте подключение к лабораторному оборудованию.

Действие 2 Выберите свою рабочую группу в главном меню.

Действие 3 Выберите коммутатор рабочей группы в меню "Модуль". Если система запросит пароль для доступа в консоль, введите пароль **cisco** (или спросите пароль у инструктора).

Действие 4 Войдите в привилегированный режим EXEC. Если система запросит пароль для перехода в привилегированный режим EXEC, введите пароль **sanfran** или обратитесь к инструктору, если этот пароль не работает.

Действие 5 Удалите загрузочную конфигурацию коммутатора рабочей группы.

Действие 6 Удалите базу данных VLAN коммутатора рабочей группы с помощью следующей команды: **delete flash:vlan.dat**.

Примечание. При появлении сообщения "**Delete filename [vlan.dat]?**" нажмите клавишу ВВОД.

При появлении сообщения "**Delete flash:vlan.dat? [confirm]**" нажмите клавишу ВВОД.

Действие 7 Перезагрузите коммутатор. Когда система предложит сохранить изменения, выберите **N**. Когда система предложит подтвердить перезагрузку, выберите **Y**.

Действие 8 После перезагрузки коммутатора, система предложит войти в диалоговое окно конфигурации (Configuration Dialog) Выберите **N**.

Действие 9 Настройте имя узла для коммутатора. Используйте имя, указанное в таблице подсказок для этого упражнения.

Действие 10 Настройте и активируйте пароль **sanfran**, он будет использоваться для доступа к привилегированному режиму EXEC.

Действие 11 Назначьте IP-адрес управляющему интерфейсу VLAN коммутатора рабочей группы. Используйте IP-адрес, указанный в таблице подсказок для этого упражнения.

Действие 12 Включите управляющий интерфейс VLAN коммутатора рабочей группы.

Действие 13 Назначьте шлюз по умолчанию для коммутатора рабочей группы. Используйте адрес центрального маршрутизатора (10.1.1.3).

Действие 14 Задайте баннерное сообщение с предупреждением, запрещающим неавторизованным пользователей вход в систему.

Действие 15 Задайте скорость 100 Мбит/с для порта Fa0/11 коммутатора рабочей группы.

Действие 16 Задайте полнодуплексный режим порта Fa0/11 коммутатора рабочей группы.

Действие 17 Введите описание конфигурации интерфейса Fa0/11, характеризующее подключенный пункт назначения.

Действие 18 Настройте защиту порта коммутатора Fa0/2, доступ к порту должен иметь только маршрутизатор рабочей группы.

- Убедитесь, что порт является портом доступа.
- Разрешите использование порта только одним устройством (может быть значением по умолчанию).
- Укажите MAC-адрес маршрутизатора (см. задачу 1) в качестве единственного разрешенного устройства.
- Включите защиту порта.

Действие 19 Введите описание конфигурации интерфейса Fa0/2, характеризующее подключенный пункт назначения.

Действие 20 Включите запрос пароля при доступе к коммутатору с консольного порта. Задайте пароль **cisco**.

Действие 21 Введите команду **logging synchronous** для консольного порта.

Действие 22 Включите запрос пароля при доступе к коммутатору с первых пяти каналов VTY (0–4). Задайте пароль **sanjose**.

Действие 23 Сохраните работающую конфигурацию в NVRAM.

Действие 24 Воспользуйтесь следующими командами, чтобы проверить параметры конфигурации:

- **show interfaces**
- **show port-security**
- **show running-configuration**
- **show startup-configuration**

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- коммутатор рабочей группы имеет верное удостоверение и IP-адрес;
- на коммутаторе рабочей группы настроены базовые средства безопасности с паролями.

Задача 3: проверка подключений рабочей группы.

Используйте команды, которые вы повторили в соответствующем модуле, чтобы проверить подключения коммутатора и маршрутизатора рабочей группы.

Процедура упражнения

Выполните следующие действия в коммутаторе рабочей группы.

Действие 1 С помощью протокола CDP (протокола обнаружения Cisco) идентифицируйте маршрутизатор рабочей группы и центральный коммутатор A как соседние узлы.

Действие 2 Отправьте эхо-запрос на первый Ethernet-интерфейс (Fa0/0) маршрутизатора рабочей группы.

Действие 3 Отправьте эхо-запрос на TFTP-сервер (10.1.1.1).

Выполните следующие действия в маршрутизаторе рабочей группы.

Действие 4 С помощью протокола CDP (протокола обнаружения Cisco) идентифицируйте коммутатор рабочей группы как соседний узел.

Действие 5 Отправьте эхо-запрос в управляющий интерфейс VLAN коммутатора рабочей группы.

Действие 6 Отправьте эхо-запрос на TFTP-сервер (10.1.1.1).

Действие 7 Сообщите инструктору, что вы выполнили упражнение.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- устройства с прямым подключением отображаются как соседи CDP на коммутаторе и маршрутизаторе;
- все эхо-запросы, отправленные с маршрутизатора и коммутатора рабочей группы, обрабатываются успешно.

Лабораторная работа 2-1: настройка расширенных коммутируемых сетей.

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

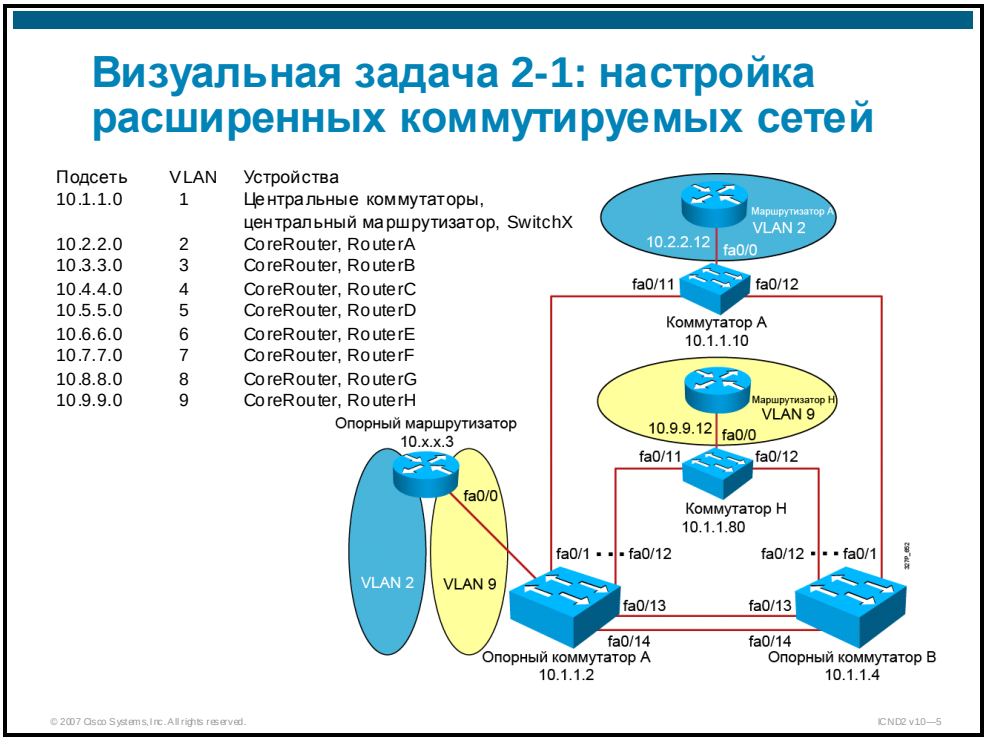
Задачи упражнения

В этом упражнении вам необходимо настроить коммутатор в соответствии с требованиями определенной сети VLAN. После выполнения этого упражнения вы должны быть готовы к следующим задачам:

- настройка коммутатора в качестве участника домена VTP и перевод коммутатора в прозрачный режим;
- настройка транкинга на транковом порте для обеспечения доступа к маршрутизатору в сети;
- настройка отдельных сетей VLAN для отдельных логических сетей;
- включение протокола RSTP и настройка корневого коммутатора и резервного корневого коммутатора.

Визуальная задача

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 локальной лаборатории или ПК с Интернет-подключением и доступом к удаленной лаборатории.
- Терминальный сервер, подключенный к консольному порту всех лабораторных устройств (при использовании удаленной лаборатории).
- Рабочая группа ICND, назначенная инструктором.

Список команд

В таблице приводится описание команд, используемых в упражнении. Команды перечислены в алфавитном порядке, что позволит легко найти нужные сведения. Если во время упражнения вам потребуется помощь по командам конфигурации, воспользуйтесь этим списком.

Команды

Команда	Описание
ping <cr>	Выполняет расширенную команду **ping**. Количество эхо-запросов и другие параметры настраиваются вручную. (Эта команда используется в привилегированном режиме EXEC.)
switchport mode trunk	Режим конфигурации интерфейса для перевода порта Fast Ethernet или Gigabit Ethernet в режим транкинга.
switchport access vlan ***номер vlan***	Режим конфигурации интерфейса для назначения порта сети VLAN.
ping ***ip-адрес***	Стандартный инструмент, используемый для проверки доступности устройств. Использует эхо-запросы и эхо-ответы ICMP, чтобы определить, активен ли удаленный узел. Кроме того, команда **ping** измеряет время до прихода эхо-ответа.
show interface ***интерфейс***	Отображает параметры транкинга.
show spanning-tree vlan ***номер VLAN***	Отображает данные связующего дерева указанной сети VLAN.
show interfaces ***интерфейс*** **switchport**	Отображает сведения о VLAN и транкинге.
show vlan	Отображает сведения обо всех настроенных сетях VLAN.
show vtp status	Отображает состояние VTP.
shutdown/no shutdown	Отключает или включает интерфейс.
vlan ***идентификатор vlan***	Глобальный режим конфигурации для добавления сети VLAN и активации режима субконфигурации ***config-vlan***. Используйте версию "**no**" этой команды, чтобы удалить сеть VLAN.
name ***имя vlan***	Задает имя сети VLAN в режиме субконфигурации ***config-vlan***.

Команда	Описание
spanning-tree mode rapid-pvst	Глобальный режим конфигурации для включения протокола Rapid-PVST.
spanning-tree portfast	Включает функцию PortFast в интерфейсе.
spanning-tree vlan *идентификатор VLAN* root primary	Глобальный режим конфигурации для назначения коммутатора основным корневым коммутатором указанной сети VLAN.
spanning-tree vlan *идентификатор VLAN* root secondary	Глобальный режим конфигурации для назначения коммутатора вспомогательным корневым коммутатором указанной сети VLAN.
vtp mode {server | client | transparent}	Устанавливает режим VTP; используйте версию "**no**" этой команды, чтобы вернуться к значениям по умолчанию.
vtp domain *домен*	Устанавливает административный домен VTP.

Подсказки

Для упражнений этой лабораторной работы доступны следующие подсказки. Действия по подготовке к этому упражнению:

- убедитесь, что между коммутатором рабочей группы и центральным коммутатором A существует только одно подключение с помощью команды **show cdp neighbors**; убедитесь, что отображается только один соседний узел в центральной части сети — коммутатор A.
- инструктор должен загрузить новые конфигурации на центральные коммутаторы; узнайте у инструктора, были ли загружены новые конфигурации.

В этой таблице приведены подключения Fast Ethernet, которые необходимы для выполнения этого упражнения.

Рабочая группа	Порт	Порт центрального коммутатора A	Порт	Порт центрального коммутатора B
A	Fa0/11	Fa0/1	Fa0/12	Fa0/1
B	Fa0/11	Fa0/2	Fa0/12	Fa0/2
C	Fa0/11	Fa0/3	Fa0/12	Fa0/3
D	Fa0/11	Fa0/4	Fa0/12	Fa0/4
E	Fa0/11	Fa0/5	Fa0/12	Fa0/5
F	Fa0/11	Fa0/6	Fa0/12	Fa0/6
G	Fa0/11	Fa0/7	Fa0/12	Fa0/7
H	Fa0/11	Fa0/8	Fa0/12	Fa0/8

Задача 1: настройка VTP и доменов VTP.

В этом упражнении вам необходимо настроить коммутатор рабочей группы для участия в домене VTP в прозрачном режиме. Это предотвратит распространение изменений конфигурации VLAN, сделанных в коммутаторе рабочей группы, на другие коммутаторы в лаборатории.

Процедура упражнения

Выполните следующие действия на коммутаторе рабочей группы.

Действие 1 Со своего ПК создайте подключение к лабораторному оборудованию.

Действие 2 Выберите свою рабочую группу в главном меню.

Действие 3 Выберите коммутатор рабочей группы в меню "Модуль".

Действие 4 Введите команду **enable**, чтобы войти в привилегированный режим EXEC.

Действие 5 Отключите интерфейс Fa0/12 на коммутаторе рабочей группы.

Действие 6 Задайте имя домена VTP **(ICND)**.

Действие 7 Установите прозрачный режим VTP.

Какая последовательность команд используется для задания имени домена и режима VTP на коммутаторе рабочей группы?

Действие 8 Проверьте конфигурацию VTP с помощью команды **show vtp status**. Выходные данные команды должны выглядеть следующим образом:

```
SwitchA# sh vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 6
VTP Operating Mode              : Transparent
VTP Domain Name                 : ICND
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x68 0x9E 0x44 0xAC 0xFE
0xA4 0xFF 0xD6
Configuration last modified by 10.1.1.10 at 0-0-00 00:00:00
```

Имя домена совпадает с именем, которое вы ввели? Находится ли коммутатор в прозрачном режиме?

Действие 9 Переходите к задаче 2.

Проверка упражнения

Задание считается выполненным, если достигнут следующий результат:

- коммутатор рабочей группы настроен для участия в домене VTP в прозрачном режиме, что позволит предотвратить распространение изменений конфигурации VLAN, сделанных в коммутаторе рабочей группы, на другие коммутаторы в лаборатории.

Задача 2: назначение порта коммутатора для транкинга

Инструктор настроил центральные коммутаторы на транкинг коммутаторов рабочей группы, которые не использую транкинг. В этой конфигурации прохождение кадров между центральными коммутаторами и коммутаторами рабочей группы блокируется. Кроме того, у вас не будет доступа к центральным устройствам. Вы должны настроить транкинг на одном из транковых портов, что позволит восстановить доступ к центральному маршрутизатору.

Процедура упражнения

Выполните следующие действия для настройки режима транкинга на коммутаторе рабочей группы.

Действие 1 Включите транковый режим на порте Fa0/11 коммутатора рабочей группы.

Какая команда используется для перевода порта в транковый режим?

Действие 2 Проверьте конфигурацию транкинга.

Какая команда используется для отображения конфигурации транкинга?

Выходные данные команды должны выглядеть следующим образом:

```
SwitchA#show interface FastEthernet 0/11 switchport
Name: Fa0/11
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
```

Действие 3 Чтобы проверить конфигурацию транкинга, отправьте эхо-запрос в центральный коммутатор по адресу 10.1.1.3 с коммутатора рабочей группы. (Если эхо-запрос не будет обработан, убедитесь, что интерфейс Fa0/12 отключен.)

Действие 4 Переходите к задаче 3.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- транкинг настроен на одном транковом порте;
- в центральный коммутатор отправлен эхо-запрос для проверки транкинга и подключения.

Задача 3: настройка отдельных сетей VLAN на коммутаторе

В этой задаче вам необходимо настроить сеть VLAN для порта коммутатора, подключенного к маршрутизатору рабочей группы, и изменить IP-адрес первого Ethernet-интерфейса маршрутизатора рабочей группы. Новый адрес принадлежит сети VLAN, которая назначена вашей рабочей группе и может обращаться только к другим устройствам в рабочей группе (в другой сети VLAN) через центральный маршрутизатор. Инструктор настроил центральный маршрутизатор на поддержку маршрутизации между сетями VLAN.

В таблице назначений VLAN ниже представлены сведения, необходимые для выполнения этой задачи.

Рабочая группа	Номер VLAN	Имя VLAN	Центральный маршрутизатор	Router*X* Fa0/0 (где *x* — буква рабочей группы)
A	2	VLAN0002	10.2.2.3	10.2.2.12
B	3	VLAN0003	10.3.3.3	10.3.3.12
C	4	VLAN0004	10.4.4.3	10.4.4.12
D	5	VLAN0005	10.5.5.3	10.5.5.12
E	6	VLAN0006	10.6.6.3	10.6.6.12
F	7	VLAN0007	10.7.7.3	10.7.7.12
G	8	VLAN0008	10.8.8.3	10.8.8.12
H	9	VLAN0009	10.9.9.3	10.9.9.12

Процедура упражнения

Выполните следующие действия для настройки отдельных сетей VLAN на коммутаторе рабочей группы.

Действие 1 С помощью таблицы назначений VLAN создайте сеть VLAN только для своей рабочей группы.

Какая команда используется для создания сети VLAN на коммутаторе?

Действие 2 С помощью команды **show vlan** режима EXEC убедитесь, что добавлена верная сеть VLAN.

Выходные данные команды должны выглядеть следующим образом:

```
SwitchA# sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gi0/1
```



```
                                                  Gi0/2
2    VLAN0002                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Действие 3 Задайте порт коммутатора рабочей группы (порт Fa0/2), подключенный к маршрутизатору рабочей группы, для назначенного номера назначенной сети VLAN.

Какую команду необходимо использовать, чтобы задать порт для номера назначенной сети VLAN?

_____

Действие 4 Настройте команду **spanning-tree portfast** на порте коммутатора, подключенном к маршрутизатору рабочей группы (порт Fa0/2).

Действие 5 Введите соответствующую команду **show**, чтобы убедиться, что порт Fa0/2 находится в верной сети VLAN.

Выходные данные команды должны выглядеть следующим образом:

```
SwitchA# sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
-
1    default                          active    Fa0/1, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gi0/1, Gi0/2
2    VLAN0002                         active    Fa0/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Действие 6 Обратитесь к порту консоли маршрутизатора рабочей группы (маршрутизатора *X*, где *X* — буква рабочей группы, назначенная вам для этого упражнения).

Действие 7 В маршрутизаторе рабочей группы активируйте режим конфигурации интерфейса для первого Ethernet-интерфейса (Fa0/0).

Действие 8 Измените основной Ethernet-интерфейс в маршрутизаторе рабочей группы на 10.*x*.*x*.12 (где *x* — номер назначенной сети VLAN) и назначьте маску подсети 255.255.255.0.

Действие 9 Отправьте эхо-запрос в центральный маршрутизатор по адресу 10.*x*.*x*.3 (где *x* — номер назначенной сети VLAN) с маршрутизатора рабочей группы.

Эхо-запрос должен быть обработан успешно. Почему?

Действие 10 Отправьте эхо-запрос в коммутатор рабочей с маршрутизатора рабочей группы.

Эхо-запрос *не* должен быть обработан успешно. Почему?

Действие 11 Создайте связь между сетями VLAN, настроив маршрут по умолчанию на маршрутизаторе рабочей группы, указывающий на центральный маршрутизатор, с помощью команды **ip route 0.0.0.0 0.0.0.0 10.***x***.***x***.3**, где *x* — номер назначенной сети VLAN**.** Теперь отправьте эхо-запрос в коммутатор рабочей группы.

Эхо-запрос должен быть обработан успешно? Почему?

Примечание. Обратите внимание, что шлюз по умолчанию для коммутатора рабочей группы настроен с адресом 10.1.1.3, что позволяет коммутатору рабочей группы отправлять эхо-запросы в другие сети VLAN через центральный маршрутизатор. Если шлюз по умолчанию отсутствует в конфигурации, добавьте его с помощью команды **ip default-gateway 10.1.1.3** в режиме глобальной конфигурации.

Действие 12 Переходите к задаче 4.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- сеть настроена VLAN и назначена порту коммутатора, который подключен к маршрутизатору рабочей группы;
- IP-адрес первого Ethernet-интерфейса маршрутизатора рабочей группы изменен;
- маршрутизатору рабочей группы назначен маршрут по умолчанию;
- в другие сети VLAN отправлены эхо-запросы для проверки подключения.

Задача 4: настройка протокола Rapid-PVST

В этой задаче вам необходимо настроить протокол Rapid-PVST, настроить второй транковый порт коммутатора рабочей группы для транкового подключения к центральному коммутатору B и пронаблюдать конвергенцию Rapid-PVST при создании петли.

Процедура упражнения

Выполните следующие действия, чтобы настроить протокол Rapid-PVST на коммутаторе рабочей группы.

Действие 1 Попросите инструктора подтвердить, что интерфейс центрального коммутатора B, подключенный к коммутатору рабочей группы, настроен для транкинга. (Возможно, инструктору придется ввести команду **no shutdown** на этом интерфейсе.) Убедитесь, что интерфейс Fa0/12 коммутатора рабочей группы отключен.

Действие 2 Включите протокол Rapid-PVST на коммутаторе рабочей группы.

Действие 3 Задайте скорость 100 Мбит/с для порта Fa0/12 коммутатора рабочей группы.

Действие 4 Задайте полнодуплексный режим порта Fa0/12 коммутатора рабочей группы.

Действие 5 Включите транковый режим для порта Fa0/12 коммутатора рабочей группы.

Какая команда используется для перевода порта в транковый режим?

Какая команда используется для отображения конфигурации транкинга?

Выходные данные команды должны выглядеть следующим образом:

```
SwitchA# show interfaces Fa0/12 switchport
Name: Fa0/12
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

Действие 6 Введите команду **no shutdown** на интерфейсе Fa0/12 коммутатора рабочей группы.

Действие 7 Введите команду, чтобы определить состояние связующего дерева сети VLAN, созданной ранее.

Какие интерфейсы находятся в режиме пересылки для созданной сети VLAN?

Примечание. Порты Fa0/2 и Fa0/11 коммутатора рабочей группы должны работать в режиме пересылки.

Действие 8 Не закрывая текущий сеанс консоли для коммутатора рабочей группы, откройте второй сеанс консоли для маршрутизатора рабочей группы. (Для этого действия необходимо два открытых сеанса связи с лабораторным оборудованием.)

Действие 9 С маршрутизатора рабочей группы подключитесь центральным коммутаторам по протоколу Telnet и повторите действие 6 с центральных коммутаторов A и B.

Примечание. IP-адрес центрального коммутатора A — 10.1.1.2, IP-адрес центрального коммутатора B — 10.1.1.4.
В качестве пароля VTY центральных коммутаторов используется слово "cisco".
Включать привилегированный режим на центральных коммутаторах не нужно.

Действие 10 Основываясь на выходных данных команды **show spanning-tree vlan** *x*, выполненной на центральных коммутаторах и коммутаторе рабочей группы во время предыдущих действий, ответьте на вопросы ниже.

Каков MAC-адрес корневого моста сети VLAN, которую вы создали ранее?

Какой коммутатор является корневым мостом?

Каков приоритет корневого моста?

Какой порт находится в блокирующем режиме?

Выходные данные команды должны выглядеть следующим образом:

```
CoreSwitchA> show spanning-tree vlan 2

VLAN0002
  Spanning tree enabled protocol rstp
  Root ID    Priority    24578
             Address     001a.6dd7.1880
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24578  (priority 24576 sys-id-ext 2)
             Address     001a.6dd7.1880
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/5            Desg FWD 19        128.5    P2p
Fa0/6            Desg FWD 19        128.6    P2p
Fa0/23           Desg FWD 19        128.23   P2p
Po1              Desg FWD 12        128.72   P2p Peer(STP)

CoreSwitchB> sh spanning-tree vlan 2

VLAN0002
  Spanning tree enabled protocol ieee
  Root ID    Priority    24578
             Address     001a.6dd7.1880
             Cost        12
             Port        72 (Port-channel1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    28674  (priority 28672 sys-id-ext 2)
             Address     001a.6de6.d800
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/5            Desg FWD 19        128.5    P2p
Fa0/6            Desg FWD 19        128.6    P2p
Po1              Root FWD 12        128.72   P2p
```

Действие 11 Не закрывая текущие сеансы консоли (один для коммутатора, второй для маршрутизатора), отправьте расширенный эхо-запрос в центральный коммутатор с маршрутизатора рабочей группы (10.*x*.*x*.3, где *x* — номер назначенной сети VLAN), задав количество запросов 45000.

Эхо-запрос обработан успешно?

Выходные данные команды должны выглядеть следующим образом:

```
RouterA# ping
```

```
Protocol [ip]:
Target IP address: 10.1.1.3
Repeat count [5]: 45000
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sending 45000, 100-byte ICMP Echos to 10.1.1.3, timeout is 2
seconds:
```

Примечание. Центральный коммутатор должен вернуть непрерывную последовательность успешных эхо-ответов. Текущий маршрут с коммутатора в центральный маршрутизатор лежит через порт FastEthernet0/11. Если это не так, не переходите к следующему действию, пока не найдете и не устраните проблему. Или попросите помощи у инструктора.

Действие 12 На коммутаторе рабочей группы отключите интерфейс Fa0/11.

Что произошло при отправке расширенного эхо-запроса в центральный маршрутизатор?

Был ли эхо-запрос обработан успешно через несколько секунд?

Действие 13 Включите интерфейс Fa0/11 на коммутаторе рабочей группы.

Что произошло при отправке расширенного эхо-запроса в центральный маршрутизатор?

Был ли эхо-запрос обработан успешно через несколько секунд?

Действие 14 Остановите отправку расширенного эхо-запроса в центральный маршрутизатор рабочей группы, нажав сочетание клавиш **Ctrl-Shift-6** два раза.

Действие 15 Сохраните конфигурацию в NVRAM с помощью команды **copy run start**.

Действие 16 Сообщите инструктору, что вы выполнили упражнение.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- на коммутаторе рабочей группы настроен второй транковый порт для транкового подключение к центральному маршрутизатору B;
- вы ознакомились с результатами отправки расширенного эхо-запроса в центральный маршрутизатор и отключили пересылающий транковый порт, чтобы пронаблюдать прерывание обработки эхо-запросов.

Задача 5: настройка основного и вспомогательного корневого моста (необязательно)

Для выполнения этой задачи вы будете работать со студентом из другой рабочей группы. Необходимо создать две или более сетей VLAN (основную и вспомогательные). Ваш коммутатор рабочей группы станет корневым мостом для вашей основной сети VLAN и вспомогательным корневым мостом для сети VLAN вашего напарника.

Назначение групп: A-B, C-D, E-F, G-H.

Назначение основной и вспомогательной сетей VLAN

Рабочая группа	Номер основной сети VLAN	Номер вспомогательной сети VLAN
A	20	30
B	30	20
C	40	50
D	50	40
E	60	70
F	70	60
G	80	90
H	90	80

Процедура упражнения

Выполните следующие действия, чтобы настроить основной и вспомогательный корневой мост на коммутаторе рабочей группы.

Действие 1 С помощью таблицы назначений основной и вспомогательной сетей VLAN создайте основную сеть VLAN для своей рабочей группы.

Действие 2 С помощью таблицы назначений основной и вспомогательной сетей VLAN создайте вспомогательную сеть VLAN для своей рабочей группы.

Какая команда используется для создания сети VLAN на коммутаторе?

Действие 3 С помощью команды **show vlan** режима EXEC убедитесь, что добавлена верная сеть VLAN.

Действие 4 Настройте коммутатор рабочей группы в качестве корневого моста вашей основной сети VLAN.

Какая команда используется для настройки коммутатора в качестве корневого моста выбранной сети VLAN?

Действие 5 Настройте коммутатор рабочей группы в качестве вспомогательного корневого моста основной сети VLAN вашего напарника.

Какая команда используется для настройки коммутатора в качестве вспомогательного корневого моста?

Действие 6 Введите команду, чтобы определить состояние связующего дерева сети VLAN, созданной во время этой задачи.

Какие интерфейсы находятся в режиме пересылки для созданной сети VLAN?

Действие 7 Не закрывая текущий сеанс консоли для коммутатора рабочей группы, откройте второй сеанс консоли для маршрутизатора рабочей группы. (Для этого действия необходимо два открытых сеанса связи с лабораторным оборудованием.)

Действие 8 В маршрутизаторе рабочй группы откройте сеанс связи Telnet с центральными коммутаторами и введите команду, чтобы определить состояние связующего дерева основной и вспомогательной сетей VLAN на центральных коммутаторах A и B.

Примечание. IP-адрес центрального коммутатора A — 10.1.1.2, IP-адрес центрального коммутатора B — 10.1.1.4. В качестве пароля VTY центральных коммутаторов используется слов **cisco**. Включение привилегированного режима на центральных коммутаторах не требуется.

Действие 9 Основываясь на выходных данных команды **show spanning-tree vlan** *x*, выполненной на центральных коммутаторах и коммутаторе рабочей группы во время предыдущих действий, ответьте на вопросы ниже.

Каков MAC-адрес корневого моста основной сети VLAN, которую вы создали ранее? Каков MAC-адрес вспомогательной сеть VLAN?

Какой коммутатор служит корневым мостом основной сети VLAN? Какой коммутатор служит корневым мостом вспомогательной сети VLAN?

Каков приоритет корневого моста основной сети VLAN? Каков приоритет вспомогательной сети VLAN?

Какой порт находится в блокирующем режиме для основной сети VLAN? Какой порт находится в блокирующем режиме для вспомогательной сети VLAN?

Выходные данные команды должны выглядеть следующим образом:

```
SwitchA# sh spanning-tree vlan 20

VLAN0020
  Spanning tree enabled protocol rstp
  Root ID    Priority    24596
             Address     0017.596d.2a00
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24596  (priority 24576 sys-id-ext 20)
             Address     0017.596d.2a00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/11           Desg FWD 19        128.11   P2p
Fa0/12           Desg FWD 19        128.12   P2p Peer(STP)

SwitchA# sh spanning-tree vlan 30

VLAN0030
  Spanning tree enabled protocol rstp
  Root ID    Priority    24606
             Address     0017.596d.1580
             Cost        38
             Port        11 (FastEthernet0/11)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    28702  (priority 28672 sys-id-ext 30)
             Address     0017.596d.2a00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/11           Root FWD 19        128.11   P2p
Fa0/12           Altn BLK 19        128.12   P2p Peer(STP)


CoreSwitchA> sh spanning-tree vlan 20

VLAN0020
  Spanning tree enabled protocol rstp
  Root ID    Priority    24596
             Address     0017.596d.2a00
             Cost        19
             Port        1 (FastEthernet0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
             Address     001a.6dd7.1880
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/5            Desg FWD 19        128.5    P2p
Fa0/6            Desg FWD 19        128.6    P2p
Fa0/23           Desg FWD 19        128.23   P2p
```

```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------

Po1              Desg FWD 12        128.72   P2p Peer(STP)
```

```
CoreSwitchB> show spanning-tree vlan 30

VLAN0030
  Spanning tree enabled protocol ieee
  Root ID    Priority    24606
             Address     0017.596d.1580
             Cost        19
             Port        2 (FastEthernet0/2)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32798  (priority 32768 sys-id-ext 30)
             Address     001a.6de6.d800
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- ------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Root FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/5            Desg FWD 19        128.5    P2p
Fa0/6            Desg FWD 19        128.6    P2p
Po1              Altn BLK 12        128.72   P2p
```

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- основная и вспомогательная сети VLAN настроены и проверены;
- основной и вспомогательный корневой мосты для основной и вспомогательной сетей VLAN настроены и проверены.

Лабораторная работа 2-2: устранение неполадок в коммутируемых сетях

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

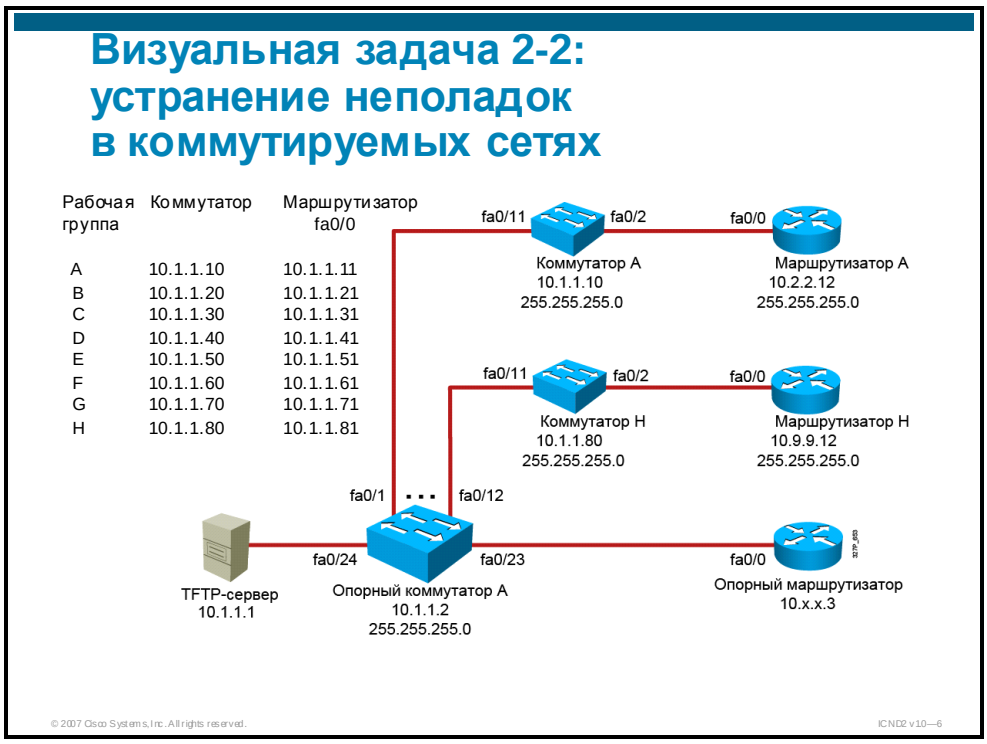
Задачи упражнения

В этом упражнении вам необходимо воспользоваться инструкциями по устранению неполадок, рассмотренными в соответствующем модуле, чтобы собрать сведения о симптомах, а затем изолировать и устранить проблемы, часто встречающиеся в коммутируемых сетях. После выполнения этого упражнения вы должны быть готовы к следующим задачам:

- обнаружение проблем подключений в коммутируемых сетях, выявление проблем подключений коммутируемой сети в соответствии с инструкциями по устранению неполадок, восстановление подключений в коммутируемой сети.

Визуальная задача

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 локальной лаборатории или ПК с Интернет-подключением и доступом к удаленной лаборатории.
- Терминальный сервер, подключенный к консольному порту всех лабораторных устройств (при использовании удаленной лаборатории).
- Рабочая группа ICND, назначенная инструктором.

Список команд

В таблице приводится описание команд, используемых в упражнении. Команды перечислены в алфавитном порядке, что позволит легко найти нужные сведения. Если во время упражнения вам потребуется помощь по командам конфигурации, воспользуйтесь этим списком.

Команды

Команда	Описание
copy tftp running-configuration	Объединяет файл на TFTP-севере с работающей конфигурацией.
ping 10.1.1.1	Тестирует подключения третьего уровня.
show interface	Отображает состояние и статистику интерфейса.
show interface switchport	Отображает статистику интерфейса, связанную с коммутацией.
show interface trunk	Отображает интерфейсы, настроенные в качестве транковых портов.
show port-security	Отображает интерфейсы, настроенные с функциями защиты порта.
show port-security address	Отображает MAC-адреса, обнаруженные на защищенном порте.
show spanning-tree vlan #	Отображает состояние связующего дерева.
show vlan	Отображает базу данных VLAN коммутатора.
show vtp status	Отображает параметры VTP.

Подсказки

Для этого упражнения доступны следующие подсказки. Используйте эту таблицу для документирования процесса устранения неполадок.

Действия по устранению неполадок

Команды для сбора данных о симптомах	Изоляция проблемы	Команда для устранения проблемы
Пример:		
ping 172.16.2.2	отказ	-----
show ip interface brief	интерфейс Fa0/1 отключен администратором	**no shutdown**
ping 172.16.2.2	повторный отказ	-----
show interface Fa0/1	неверный ip-адрес	**ip address** 192.168.1.2
ping 172.16.2.2	успешно	

Задача 1: обновление конфигураций рабочей группы.

В этой задаче вам необходимо загрузить новые дополнительные конфигурации на маршрутизатор и коммутатор рабочей группы с TFTP-сервера. Эти дополнительные конфигурации могут содержать проблемы, которые помешают выполнению задачи. В этом случае вам необходимо изолировать и устранить проблему.

Процедура упражнения

Выполните следующие действия.

Действие 1 Отключите порт Fa0/12 коммутатора рабочей группы.

Действие 2 Отправьте эхо-запрос на TFTP-сервер (10.1.1.1) с маршрутизатора рабочей группы.

Действие 3 Проверьте соединение с TFTP-сервером. Отправьте эхо-запрос на TFTP-сервер (10.1.1.1) с коммутатора рабочей группы.

Примечание. Если любой из эхо-запросов не получает ответ, обратитесь к инструктору.

Действие 4 На **коммутаторе** рабочей группы загрузите дополнительную конфигурацию с TFTP-сервера в работающую конфигурацию коммутатора рабочей группы. Имя файла, который необходимо загрузить: i2-wg_**sw**-config-lab2-2.txt.

Действие 5 Введите команду **exit** в привилегированном приглашении EXEC и убедитесь, что баннер коммутатора выглядит следующим образом:

********** wg_sw-config-lab2-2 **********

Действие 6 На **маршрутизаторе** рабочей группы загрузите дополнительную конфигурацию с TFTP-сервера в работающую конфигурацию маршрутизатора рабочей группы. Имя файла, который необходимо загрузить: i2-wg_**ro**-config-lab2-2.txt.

Загрузка выполнена успешно?

Возвращает ли TFTP-сервер эхо-ответ при отправке эхо-запроса с маршрутизатора рабочей группы?

Действие 7 Не используя команду **show run**, соберите сведения о симптомах, а затем изолируйте и устраните проблему с помощью инструкций по устранению неполадок и команд, рассмотренных в соответствующем модуле. Во время устранения неполадок вы можете воспользоваться таблицей подсказок на предыдущей странице.

Действие 8 После того, как подключение будет восстановлено, загрузите дополнительную конфигурацию с TFTP-сервера в работающую конфигурацию маршрутизатора рабочей группы. Имя файла, который необходимо загрузить: i2-wg_**ro**-config-lab2-2.txt.

Действие 9 Введите команду **exit** в привилегированном приглашении EXEC и убедитесь, что баннер коммутатора выглядит следующим образом:

****** Congratulations! You have successfully completed the lab. ******

Действие 10 Сохраните работающую конфигурацию в NVRAM.

Действие 11 Сообщите инструктору, что вы выполнили упражнение.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- TFTP-сервер возвращает эхо-ответы при отправке эхо-запросов с коммутатора и маршрутизатора рабочей группы;
- в работающие конфигурации коммутатора и маршрутизатора рабочей группы загружены конфигурации lab2-2.

Лабораторная работа 4-1: внедрение OSPF

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

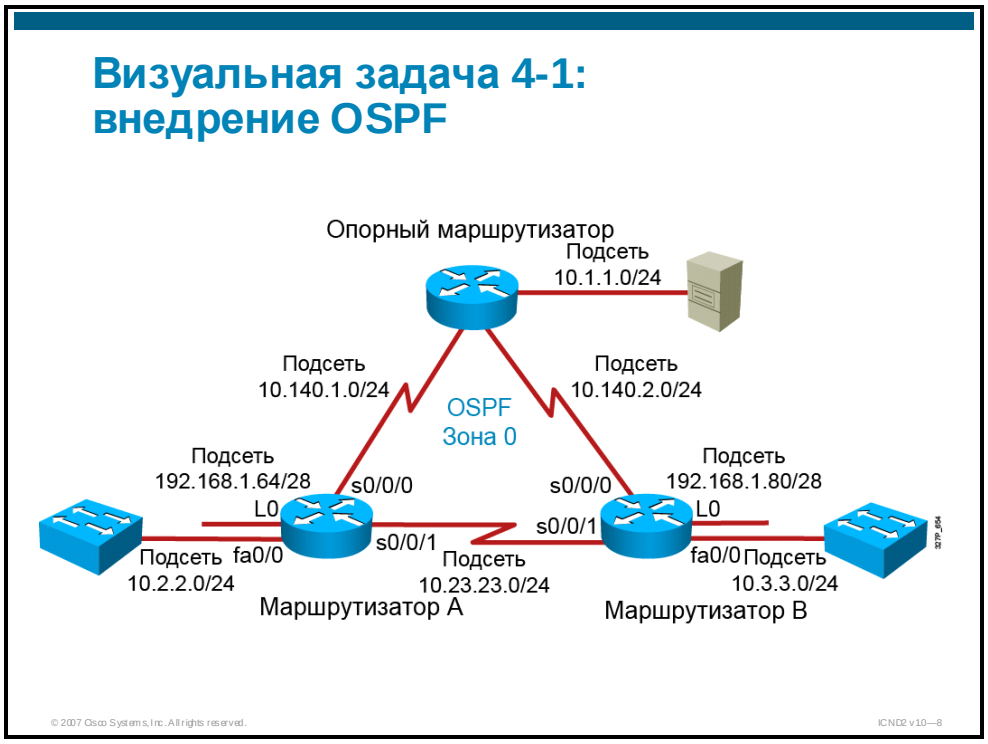
Задачи упражнения

В этом упражнении вам необходимо определить IP-маршруты с помощью протокола маршрутизации OSPF. После выполнения этого упражнения вы должны быть готовы к следующим задачам:

- блокировка соединений с центральными устройствами через локальную сети;
- включение последовательных соединений на маршрутизаторе рабочей группы;
- настройка OSPF на маршрутизаторе рабочей группы;
- настройка аутентификации на базе простого текста для OSPF;
- проверка работы и конфигурации маршрутизации OSPF аутентификации OSPF на базе простого текста.

Визуальная задача

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 локальной лаборатории или ПК с Интернет-подключением и доступом к удаленной лаборатории.
- Терминальный сервер, подключенный к консольному порту всех лабораторных устройств (при использовании удаленной лаборатории).
- Рабочая группа ICND, назначенная инструктором.

Список команд

В таблице приводится описание команд, используемых в упражнении. Команды перечислены в алфавитном порядке, что позволит легко найти нужные сведения. Если во время упражнения вам потребуется помощь по командам конфигурации, воспользуйтесь этим списком.

Команды коммутаторов Cisco Catalyst

Команда	Описание
interface vlan1 **ip address** ***ip-адрес маска***	Задает IP-адрес и маску подсети для коммутатора Cisco Catalyst.
ip default-gateway ***ip-адрес***	Задает шлюз по умолчанию для коммутатора Cisco Catalyst.
ping ***ip-адрес***	Стандартный инструмент, используемый для проверки доступности устройств. Использует эхо-запросы и эхо-ответы ICMP, чтобы определить, активен ли удаленный узел. Кроме того, команда **ping** измеряет время до прихода эхо-ответа.
show interfaces vlan 1	Отображает конфигурацию IP коммутатора Cisco Catalyst.
show vlan	Отображает данные по сетям VLAN коммутатора Cisco Catalyst.
switchport access vlan 1	Задает членство интерфейса в сети VLAN.

Команды маршрутизатора Cisco

Команда	Описание
bandwidth	Настраивает полосу пропускания на последовательных интерфейсах.
clock rate	Настраивает тактовую частоту на последовательных интерфейсах.
debug ip ospf events	Отображает сводные сведения о транзакциях OSPF.
interface loopback	Использует команду глобальной конфигурации интерфейсов для настройки типа интерфейса и активирует режим конфигурации интерфейса.
ip ospf authentication-key ***пароль***	Задает пароль для аутентификации OSPF.
ip ospf authentication	Включает аутентификацию OSPF на базе простого текста.
network ***номер сети шаблонная маска*** **area** ***идентификатор области***	Запускает протокол маршрутизации на всех интерфейсах маршрутизатора в указанной сети. Задает количество битов, значимое для данной сети, и область OSPF, к которой привязана эта сеть.
ping ***ip-адрес***	Стандартный инструмент, используемый для проверки доступности устройств. Использует эхо-запросы и эхо-ответы ICMP, чтобы определить, активен ли удаленный узел. Кроме того, команда **ping** измеряет время до прихода эхо-ответа.
router ospf ***router-идентификатор процесса***	Включает протокол маршрутизации OSPF.
show controllers ***тип***	Отображает состояние контроллера в зависимости от его аппаратного обеспечения.
show interfaces ***тип***	Отображает статистику интерфейсов, настроенных на маршрутизаторе.

Команда	Описание
show ip ospf neighbor	Определяет состояние соседнего узла OSPF.
show ip protocols	Отображает параметры протоколов маршрутизации и данные таймера протокола маршрутизации, связанного с маршрутизатором.
show ip route	Отображает таблицу маршрутизации IP.
shutdown/no shutdown	Отключает или включает интерфейс.
undebug all	Отключает все экраны отладки.

Подсказки

Для данного упражнения доступны следующие подсказки.

В этом упражнении вам необходимо использовать инкапсуляцию последовательного канала по умолчанию (HDLC) для распространения трафика протокола маршрутизации вашей рабочей группы в центральном сегменте. Для этого вы должны закрыть все восходящие каналы к центральным коммутаторам на коммутаторе рабочей группы и назначить IP-адрес первому последовательному интерфейсу маршрутизатора.

Кроме того, вы должны настроить протокол маршрутизации OSPF и применить аутентификацию OSPF на базе простого текста для гарантии подлинности обновлений маршрутизации. Затем вы должны проверить конфигурацию и работу протокола OSPF.

В таблице ниже перечислены IP-адреса, которые необходимы для этого упражнения. Для масок подсети указано количество сетевых битов (/биты).

IP-адреса

Рабочая группа	Сеть VLAN 1 интерфейса коммутатора (Switch*X*)	Интерфейс Fa0/0 маршрутизатора (Router*X*)	Интерфейс Loopback 0 маршрути-затора (Router*X*)	Интерфейс S0/0/0 маршрути-затора (Router*X*)	Интерфейс S0/0/1 маршрути-затора (Router*X*)	Последова-тельный интерфейс центрального маршрутизатора (Центральный маршрутизатор)
A	10.2.2.11/24	10.2.2.3/24	192.168.1.65/28	10.140.1.2/24	10.23.23.1/24	10.140.1.1/24
B	10.3.3.11/24	10.3.3.3/24	192.168.1.81/28	10.140.2.2/24	10.23.23.2/24	10.140.2.1/24
C	10.4.4.11/24	10.4.4.3/24	192.168.2.65/28	10.140.3.2/24	10.45.45.1/24	10.140.3.1/24
D	10.5.5.11/24	10.5.5.3/24	192.168.2.81/28	10.140.4.2/24	10.45.45.2/24	10.140.4.1/24
E	10.6.6.11/24	10.6.6.3/24	192.168.3.65/28	10.140.5.2/24	10.67.67.1/24	10.140.5.1/24
F	10.7.7.11/24	10.7.7.3/24	192.168.3.81/28	10.140.6.2/24	10.67.67.2/24	10.140.6.1/24
G	10.8.8.11/24	10.8.8.3/24	192.168.4.65/28	10.140.7.2/24	10.89.89.1/24	10.140.7.1/24
H	10.9.9.11/24	10.9.9.3/24	192.168.4.81/28	10.140.8.2/24	10.89.89.2/24	10.140.8.1/24

Задача 1: отключение соединения с центральными устройствами через локальную сеть

В этой задаче необходимо отключить соединение между рабочей группой и центральными устройствами через локальную сеть. Кроме того, вы должны изменить IP-адрес коммутатора рабочей группы и первого Ethernet-интерфейса маршрутизатора.

Процедура упражнения

Выполните следующие действия, чтобы отключить соединения между рабочей группой и центральными устройствами через локальную сеть.

Действие 1 Со своего ПК создайте подключение к лабораторному оборудованию.

Действие 2 Выберите свою рабочую группу в главном меню.

Действие 3 Выберите коммутатор рабочей группы в меню "Модуль".

Действие 4 Отключите порты (Fa0/11 и Fa0/12), подключенные к центральным коммутаторам A и B.

Действие 5 Измените IP-адрес интерфейса VLAN 1 коммутатора рабочей группы на адрес, указанный в таблице подсказок этого упражнения.

Действие 6 Измените шлюз по умолчанию коммутатора на первый Ethernet-интерфейс маршрутизатора рабочей группы. Используйте адрес, указанный в таблице подсказок для этого упражнения. Например, для рабочей группы A шлюз по умолчанию для коммутатора рабочей группы будет 10.2.2.3.

Действие 7 Измените порт коммутатора рабочей группы, подключенный к маршрутизатору рабочей группы (Fa0/2) на VLAN 1. Для этого войдите в режим конфигурации интерфейса и выполните соответствующую команду.

Действие 8 Выйдите из режима глобальной конфигурации.

Действие 9 Введите команду **show interface vlan 1**, чтобы убедиться в правильной настройке IP-адреса.

Выходные данные команды должны выглядеть следующим образом:

```
SwitchA# sh interface vlan 1
Vlan1 is up, line protocol is up
  Hardware is EtherSVI, address is 0017.596d.2a40 (bia
0017.596d.2a40)
  Internet address is 10.2.2.11/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:11:45, output 00:11:45, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops:
0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     280 packets input, 28716 bytes, 0 no buffer
```



```
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     142 packets output, 15568 bytes, 0 underruns
     0 output errors, 1 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Действие 10 Отобразите работающую конфигурацию, чтобы убедиться в правильности настройки шлюза по умолчанию.

Действие 11 Введите соответствующую команду **show vlan**, чтобы убедиться, что порт маршрутизатора рабочей группы находится в сети VLAN 1.

Выходные данные команды должны выглядеть следующим образом:

```
SwitchA# sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------
-----
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                Gi0/2
2    VLAN0002                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Действие 12 Перейдите к консольному подключению маршрутизатора рабочей группы. Измените адрес первого Ethernet-интерфейса маршрутизатора рабочей группы на адрес, указанный в таблице подсказок для этого упражнения.

Действие 13 Проверьте первый Ethernet-интерфейс маршрутизатора рабочей группы. Выходные данные команды должны выглядеть следующим образом:

```
RouterA# sh ip int fa0/0
FastEthernet0/0 is up, line protocol is up
  Internet address is 10.2.2.3/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
```

Действие 14 С маршрутизатора рабочей группы отправьте эхо-запрос в коммутатор рабочей группы, чтобы проверить подключение. Эхо-запрос должен быть обработан успешно.

Действие 15 Переходите к задаче 2.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- отключено соединение между рабочей группой и центральными устройствами через локальную сеть;
- изменен IP-адрес коммутатора рабочей группы и первого Ethernet-интерфейса маршрутизатора.

Задача 2: активация последовательных соединений на маршрутизаторе рабочей группы

В этой задаче вам необходимо удалить маршрут по умолчанию, настроенный на маршрутизаторе, назначить IP-адрес последовательным интерфейсам и убедиться, что у вас есть связь только с устройствами, подключенными напрямую. Кроме того, вы должны убедиться, что IP-адрес центрального маршрутизатора (10.1.1.3) недоступен. Подключения будут созданы во время следующей задачи.

Процедура упражнения

Выполните следующие действия на маршрутизаторе рабочей группы, чтобы активировать последовательное подключение.

Действие 1 Войдите в режим глобальной конфигурации.

Действие 2 Удалите маршрут по умолчанию, настроенный в одной из предыдущих работ, с помощью команды **no ip route 0.0.0.0 0.0.0.0 10.*x*.*x*.3**.

Действие 3 Убедитесь, что два первых последовательных интерфейса (S0/0/0 и S0/0/1) настроены на использование HDLC. Для этого введите команду **show interfaces serial *интерфейс***. Тип инкапсуляции указывается в четвертой строке выходных данных.

Действие 4 Измените адрес первого последовательного интерфейса (S0/0/0) маршрутизатора рабочей группы на адрес, указанный в таблице подсказок для этого упражнения. Например, для рабочей группы A необходимо задать адрес 10.140.1.2.

Действие 5 Введите команду **no shutdown** на первом последовательном интерфейсе (S0/0/0).

Действие 6 Отправьте эхо-запрос в последовательный интерфейс центрального маршрутизатора, который напрямую подключен к маршрутизатору рабочей группы. Верный IP-адрес можно посмотреть в таблице подсказок для этого упражнения. Например, для рабочей группы A необходимо указать адрес 10.140.1.1.

Эхо-запрос должен быть обработан успешно. Почему?

_____

Действие 7 Отправьте эхо-запрос в центральный маршрутизатор по адресу 10.1.1.3.

Эхо-запрос обработан неудачно. Почему?

Действие 8 Откройте таблицу маршрутизации IP, чтобы увидеть все пути, которые в ней указаны. Какую команду необходимо ввести, чтобы открыть таблицу маршрутизации IP? Выходные данные команды должны выглядеть следующим образом:

```
RouterA# 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
       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 not set

     10.0.0.0/24 is subnetted, 2 subnets
C       10.2.2.0 is directly connected, FastEthernet0/0
C       10.140.1.0 is directly connected, Serial0/0/0
```

Действие 9 Проверьте, какой кабель — DCE или DTE — подключен ко второму последовательному интерфейсу (S0/0/1) с помощью команды **show controllers serial** *интерфейс*. (Обратите внимание, что между словом **serial** и параметром (*интерфейс*) необходимо поставить пробел.)

Действие 10 Если в качестве второго последовательного интерфейса (S0/0/1) используется DCE, задайте тактовую частоту 64000.

Примечание. Интерфейсы DTE не требуют настройки тактовой частоты.

Действие 11 На втором последовательном интерфейсе (S0/0/1) задайте IP-адрес, указанный в подсказках для этого упражнения.

Действие 12 Введите команду **no shutdown** на втором последовательном интерфейсе.

Отправьте эхо-запрос на второй последовательный интерфейс (S0/0/1) маршрутизатора вашего напарника, подключенный напрямую к вашему маршрутизатору рабочей группы. Верный IP-адрес можно посмотреть в таблице подсказок для этого упражнения.

Эхо-запрос должен быть обработан успешно. Почему?

Примечание. Для успешной обработки эхо-запроса необходимо, чтобы интерфейс S0/0/1 маршрутизатора вашего напарника был настроен верно.

Действие 13 Переходите к задаче 3.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- маршрут по умолчанию, ранее настроенный на маршрутизаторе, удален;
- последовательным интерфейсам назначен IP-адрес;
- соединение с подключенным напрямую последовательным интерфейсом соседнего маршрутизатора проверено;
- вы убедились, что центральный маршрутизатор с IP-адресом 10.1.1.3 недоступен, не получив ответа на эхо-запрос.

Задача 3: активация маршрутизации по протоколу OSPF.

Цель этой задачи — настроить протокол OSPF на маршрутизаторе. Для этого необходимо назначить идентификатор процессу маршрутизации и определить сети, которые будут участвовать в процессе OSPF.

Процедура упражнения

Выполните следующие действия на маршрутизаторе рабочей группы.

Действие 1 Настройте интерфейс loopback 0 с адресом, указанным в таблице подсказок для этого упражнения.

Действие 2 Включите протокол маршрутизации OSPF. Укажите число 100 в качестве идентификатора процесса OSPF.

Действие 3 Включите протокол OSPF на интерфейсах loopback 0, Fa0/0 и двух последовательных интерфейсах S0/0/0 и S0/0/1. Используйте таблицу подсказок для этого упражнения. Все интерфейсы должны находиться в области 0. Используйте четыре сетевых оператора с шаблонной маской 0.0.0.0. Пример:

```
RouterA(config)#router ospf 100
RouterA(config-router)#network 192.168.1.65 0.0.0.0 area 0
RouterA(config-router)#network 10.2.2.3 0.0.0.0 area 0
RouterA(config-router)#network 10.140.1.2 0.0.0.0 area 0
RouterA(config-router)#network 10.23.23.1 0.0.0.0 area 0
```

Действие 4 Настройте полосу пропускания 64 Кбит/с на обоих последовательных интерфейсах (S0/0/0 и S0/0/1)**.**

Действие 5 Переходите к задаче 4.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- процессу маршрутизации назначен идентификатор;
- определены сети, которые будут участвовать в процессе маршрутизации OSPF.

Задача 4: включение аутентификации OSPF на базе обычного текста

Цель этой задачи — настроить аутентификацию OSPF на маршрутизаторе. Протокол OSPF не будет объявлять маршруты между соседними узлами, если они не идентифицировали себя должным образом.

Процедура упражнения

Выполните следующие действия на маршрутизаторе рабочей группы.

Действие 1 Задайте пароль, который будет использоваться для всех соседних маршрутизаторов с активной аутентификация OSPF (центральный маршрутизатор и маршрутизатор напарника). В качестве пароля используйте слово **san-fran**.

Действие 2 Настройте маршрутизатор рабочей группы на использование аутентификации OSPF на базе простого текста со всеми соседними маршрутизаторами OSPF.

Действие 3 Переходите к задаче 5.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- задан пароль аутентификации;
- включена аутентификация.

Задача 5: проверка маршрутизации OSPF и аутентификации на базе простого текста

В этой задаче вы должны проверить работу и конфигурацию протокола маршрутизации OSPF и аутентификации на базе простого текста. Для этого необходимо использовать несколько команд **show**.

Процедура упражнения

Выполните следующие действия на маршрутизаторе рабочей группы.

Действие 1 С помощью команды **show ip route** проверьте маршруты, полученные от протокола маршрутизации OSPF. Выходные данные команды должны выглядеть следующим образом:

```
RouterA# 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
       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 not set
```

```
     10.0.0.0/24 is subnetted, 5 subnets
C       10.23.23.0 is directly connected, Serial0/0/1
C       10.2.2.0 is directly connected, FastEthernet0/0
O       10.1.1.0 [110/1563] via 10.140.1.1, 00:03:15, Serial0/0/0
O       10.140.2.0 [110/3124] via 10.140.1.1, 00:03:15, Serial0/0/0
                   [110/3124] via 10.23.23.2, 00:03:15, Serial0/0/1
C       10.140.1.0 is directly connected, Serial0/0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.64/28 is directly connected, Loopback0
O       192.168.1.81/32 [110/1563] via 10.23.23.2, 00:03:17, Serial0/0/1
```

Действие 2 С помощью команды **show ip protocols** убедитесь, что протокол маршрутизации OSPF включен и идентификатор процесса маршрутизации, назначенный во время задачи 1, распознается процессом OSPF (идентификатор маршрутизатора должен совпадать с IP-адресом интерфейса возвратной петли маршрутизатора рабочей группы). Выходные данные команды должны выглядеть следующим образом:

```
RouterA# sh ip protocol
Routing Protocol is "ospf 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.1.65
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.2.2.3 0.0.0.0 area 0
    10.23.23.1 0.0.0.0 area 0
    10.140.1.2 0.0.0.0 area 0
    192.168.1.65 0.0.0.0 area 0
 Reference bandwidth unit is 100 mbps
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.1.81         110      00:04:52
    172.16.31.100        110      00:04:52
  Distance: (default is 110)
```

Действие 3 С помощью команды **show ip ospf neighbor** выведите данные о состоянии соседства. Выходные данные команды должны выглядеть следующим образом:

```
RouterA# sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.31.100     0   FULL/  -        00:00:31    10.140.1.1      Serial0/0/0
192.168.1.81      0   FULL/  -        00:00:31    10.23.23.2      Serial0/0/1
```

Каково состояние соседства по отношению к центральному маршрутизатору и смежному маршрутизатору рабочей группы?

Какие идентификаторы соседства используют эти маршрутизаторы?

Примечание. Соседние узлы не будут отображаться, пока на них не будут выполнены предыдущие задачи этого упражнения.

Действие 4 Отправьте эхо-запрос на TFTP-сервер по адресу 10.1.1.1. Отправьте эхо-запрос в Ethernet-интерфейс маршрутизатора другой рабочей группы. Адрес, по которому необходимо отправить эхо-запрос, можно найти в таблице подсказок для этого упражнения. Если другая рабочая группа также настроила протокол OSPF, эхо-запросы должны быть обработаны успешно.

Действие 5 С помощью команды **debug ip ospf events** выведите приветственные сообщения OSPF, отправленные маршрутизатору. Выходные данные команды должны выглядеть следующим образом:

```
RouterA# debug ip ospf events
OSPF events debugging is on
RouterA#
*Feb 28 18:48:54.039: OSPF: Send hello to 224.0.0.5 area 0 on
Serial0/0/0 from 10.140.1.2
*Feb 28 18:48:54.039: OSPF: Send hello to 224.0.0.5 area 0 on
FastEthernet0/0 from 10.2.2.3
*Feb 28 18:48:54.039: OSPF: Send hello to 224.0.0.5 area 0 on
Serial0/0/1 from 10.23.23.1
*Feb 28 18:48:56.979: OSPF: Rcv hello from 192.168.1.81 area 0
from Serial0/0/1 10.23.23.2
*Feb 28 18:48:56.979: OSPF: End of hello processing
*Feb 28 18:48:57.187: OSPF: Rcv hello from 172.16.31.100 area
0 from Serial0/0/0 10.140.1.1
*Feb 28 18:48:57.191: OSPF: End of hello processing
*Feb 28 18:49:04.039: OSPF: Send hello to 224.0.0.5 area 0 on
Serial0/0/0 from 10.140.1.2
*Feb 28 18:49:04.039: OSPF: Send hello to 224.0.0.5 area 0 on
FastEthernet0/0 from 10.2.2.3
*Feb 28 18:49:04.039: OSPF: Send hello to 224.0.0.5 area 0 on
Serial0/0/1 from 10.23.23.1u a
*Feb 28 18:49:06.979: OSPF: Rcv hello from 192.168.1.81 area 0
from Serial0/0/1 10.23.23.2
*Feb 28 18:49:06.979: OSPF: End of hello processing
```

Действие 6 Отключите отладку. Выходные данные команды должны выглядеть следующим образом:

```
RouterA# undebug all
All possible debugging has been turned off
```

Действие 7 Сохраните работающую конфигурацию в NVRAM.

Действие 8 Сообщите инструктору, что вы выполнили упражнение.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- конфигурация и работа протокола OSPF проверены с помощью команд **show** и **debug**;
- соединения проверены путем отправки эхо-запроса по удаленным адресам, не имеющим прямого подключения к маршрутизатору рабочей группы.

Лабораторная работа 4-2: устранение неполадок OSPF

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

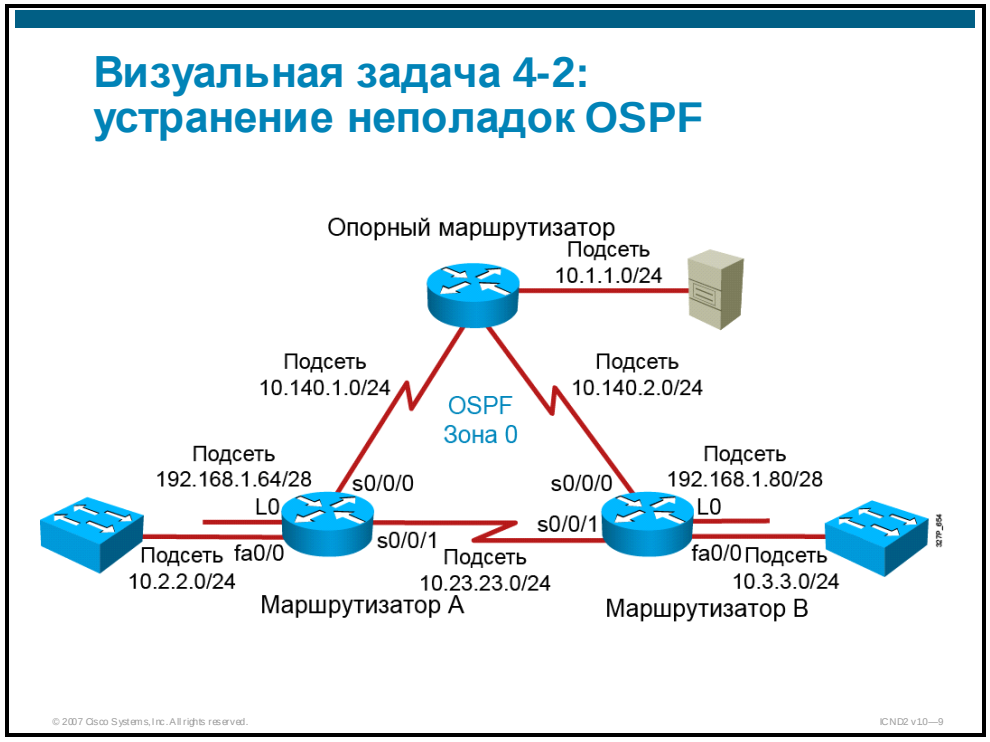
Задачи упражнения

В этом упражнении вам необходимо воспользоваться инструкциями по устранению неполадок, рассмотренными в соответствующем модуле, чтобы собрать сведения о симптомах, а затем изолировать и устранить проблемы, часто встречающиеся в сетях OSPF. После выполнения этого упражнения вы должны быть готовы к следующим задачам:

- обнаружение проблем подключения в сетях OSPF, изоляция и устранение проблем подключения OSPF в соответствии с инструкциями по устранению неполадок.

Визуальная задача

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



Необходимые ресурсы

Ниже перечислены ресурсы и устройства, необходимые для выполнения этого упражнения.

- ПК, подключенный к локальной лаборатории или ПК с Интернет-подключением и доступом к удаленной лаборатории.
- Терминальный сервер, подключенный к консольному порту всех лабораторных устройств (при использовании удаленной лаборатории).
- Рабочая группа ICND, назначенная инструктором.

Список команд

В таблице приводится описание команд, используемых в упражнении. Команды перечислены в алфавитном порядке, что позволит легко найти нужные сведения. Если во время упражнения вам потребуется помощь по командам конфигурации, воспользуйтесь этим списком.

Команды для устранения неполадок OSPF

Команда	Описание
copy tftp running-configuration	Объединяет файл на TFTP-севере с конфигурацией, запущенной на устройстве.
debug ip ospf adj	Отображает процесс установления соседства OSPF.
debug ip ospf events	Отображает сводные сведения о транзакциях OSPF.
ping 10.1.1.1	Проверяет подключения третьего уровня.
show interfaces *тип*	Отображает статистику интерфейсов, настроенных на маршрутизаторе.
show ip ospf interface	Отображает статистику интерфейсов, на которых включен протокол OSPF.
show ip ospf neighbor	Определяет состояние соседнего узла OSPF.
show ip protocols	Отображает параметры протоколов маршрутизации и данные таймера протокола маршрутизации, связанного с маршрутизатором.
show ip route	Отображает таблицу маршрутизации.

Подсказки

Для этого упражнения доступны следующие подсказки.

Рабочая группа	Сеть VLAN 1 интерфейса коммутатора (Switch*X*)	Интерфейс Fa0/0 маршрути-затора (Router*X*)	Интерфейс Loopback 0 маршрути-затора (Router*X*)	Интерфейс S0/0/0 маршрути-затора (Router*X*)	Интерфейс S0/0/1 маршрути-затора (Router*X*)	Последовательный интерфейс центрального маршрутизатора (Центральный маршрутизатор)
A	10.2.2.11/24	10.2.2.3/24	192.168.1.65/28	10.140.1.2/24	10.23.23.1/24	10.140.1.1/24
B	10.3.3.11/24	10.3.3.3/24	192.168.1.81/28	10.140.2.2/24	10.23.23.2/24	10.140.2.1/24
C	10.4.4.11/24	10.4.4.3/24	192.168.2.65/28	10.140.3.2/24	10.45.45.1/24	10.140.3.1/24
D	10.5.5.11/24	10.5.5.3/24	192.168.2.81/28	10.140.4.2/24	10.45.45.2/24	10.140.4.1/24
E	10.6.6.11/24	10.6.6.3/24	192.168.3.65/28	10.140.5.2/24	10.67.67.1/24	10.140.5.1/24
F	10.7.7.11/24	10.7.7.3/24	192.168.3.81/28	10.140.6.2/24	10.67.67.2/24	10.140.6.1/24
G	10.8.8.11/24	10.8.8.3/24	192.168.4.65/28	10.140.7.2/24	10.89.89.1/24	10.140.7.1/24
H	10.9.9.11/24	10.9.9.3/24	192.168.4.81/28	10.140.8.2/24	10.89.89.2/24	10.140.8.1/24

Используйте эту таблицу для документирования процесса устранения неполадок.

Действия по устранению неполадок

Команды для сбора данных о симптомах	Изоляция проблемы	Команда для устранения проблемы
Пример:		
ping 172.16.2.2	отказ	-----
show ip interface brief	интерфейс Fa0/1 отключен администратором	**no shutdown**
ping 172.16.2.2	повторный отказ	-----
show interface Fa0/1	неверный ip-адрес	**ip address** 192.168.1.2
ping 172.16.2.2	успешно	

Задача 1: обновление конфигураций рабочей группы

В этой задаче вам необходимо загрузить новую дополнительную конфигурацию на маршрутизатор рабочей группы с TFTP-сервера. Однако дополнительная конфигурация, которую вы загрузите, содержит ошибки, которые могут вызвать потерю соединения с остальной частью сети. Вам необходимо изолировать и устранить проблему или проблемы, которые вызваны дополнительным файлом.

Процедура упражнения

Выполните следующие действия.

Действие 1 Проверьте соединение с TFTP-сервером. Отправьте эхо-запрос на TFTP-сервер (10.1.1.1) с маршрутизатора рабочей группы.

Примечание. Если эхо-запрос обрабатывается неудачно, обратитесь к инструктору.

Действие 2 Загрузите дополнительную конфигурацию с TFTP-сервера в работающую конфигурацию маршрутизатора рабочей группы. Имя файла, который необходимо загрузить: i2-wg_**ro**-config-lab4-2.txt.

Действие 3 Введите команду **exit** в привилегированном приглашении EXEC и убедитесь, что баннер маршрутизатора выглядит следующим образом:

********** wg_ro-config-lab4-2 **********

Действие 4 Отправьте эхо-запрос на TFTP-сервер с маршрутизатора рабочей группы. Был ли эхо-запрос обработан успешно?

Действие 5 Проверьте таблицу маршрутизации маршрутизатора рабочей группы. Проверьте отношения соседства OSPF. Что вы обнаружили?

Действие 6 Воспользуйтесь командой **debug ip ospf events**. Что вы обнаружили?

Действие 7 Не используя команду **show run**, соберите сведения о симптомах, а затем изолируйте и устраните проблему с помощью инструкций по устранению неполадок и команд, рассмотренных в соответствующем модуле. Воспользуйтесь таблицей подсказок, чтобы задокументировать процесс устранения неполадок.

Действие 8 Устранив проблему, сохранит работающую конфигурацию в NVRAM.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- отношения соседства OSPF с маршрутизаторами, подключенными напрямую, восстановлены;
- таблица маршрутизации маршрутизатора рабочей группы заполнена маршрутами, полученными от центрального маршрутизатора через протокол OSPF;
- сетевое подключение к TFTP-серверу восстановлено. Эхо-запрос, отправленный на этот сервер, обрабатывается успешно.

Лабораторная работа 5-1: внедрение EIGRP

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

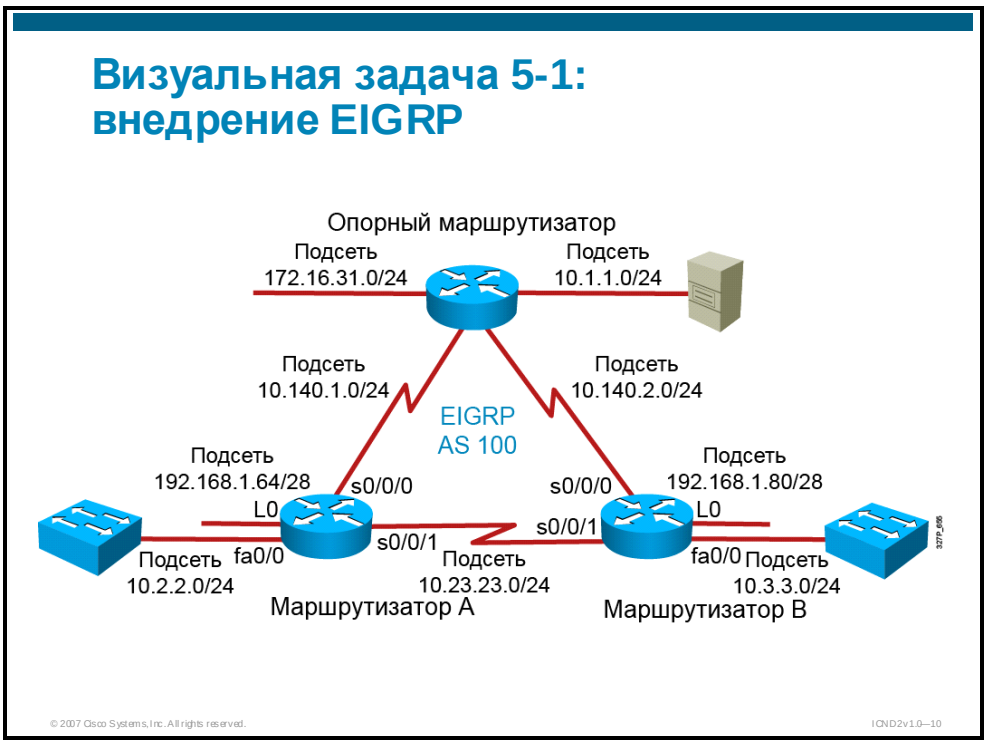
Задачи упражнения

В этом упражнении вам необходимо определить маршруты от рабочей группы к центральному сегменту с помощью протокола EIGRP. После выполнения этого упражнения вы должны быть готовы к следующим задачам:

- настройка протокола EIGRP на маршрутизаторе;
- настройка аутентификации MD5 для EIGRP;
- проверка работы и конфигурации маршрутизации EIGRP с помощью команд **show**, а также проверка работы и конфигурации аутентификации EIGRP MD5;
- устранение неполадок процессов установления соседства EIGRP.

Визуальная задача

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 локальной лаборатории или ПК с Интернет-подключением и доступом к удаленной лаборатории.
- Терминальный сервер, подключенный к консольному порту всех лабораторных устройств (при использовании удаленной лаборатории).
- Рабочая группа ICND, назначенная инструктором.

Список команд

В таблице приводится описание команд, используемых в упражнении. Команды перечислены в алфавитном порядке, что позволит легко найти нужные сведения. Если во время упражнения вам потребуется помощь по командам конфигурации, воспользуйтесь этим списком.

Команды

Команда	Описание
debug eigrp neighbors	Отображает соседние узлы EIGRP, обнаруженные протоколом EIGRP.
ip authentication mode eigrp ***автономная система*** **md5**	Задает аутентификацию MD5 для пакетов EIGRP.
ip authentication key-chain eigrp ***автономная система*** ***имя цепи***	Включает аутентификацию пакетов EIGRP с использованием ключа в цепи ключей.
key chain ***имя цепи***	Активирует режим конфигурации цепи ключей.
key ***идентификатор ключа***	Определяет ключ и активирует режим конфигурации идентификатора ключа.
key-string ***текст***	Определяет строку ключа (пароль)
network ***номер сети***	Включает протокол маршрутизации на интерфейсах указанной сети.
no debug all	Отключает все экраны отладки.
ping ***ip-адрес***	Тестирует подключения третьего уровня.
router eigrp ***автономная система***	Включает EIGRP.
show interfaces	Отображает статистику интерфейсов, настроенных на маршрутизаторе.
show ip eigrp neighbors	Определяет состояние соседнего узла EIGRP.
show ip protocols	Отображает параметры протоколов маршрутизации и данные таймера протокола маршрутизации, связанного с маршрутизатором.
show ip route	Отображает таблицу маршрутизации IP.

Подсказки

Для этого упражнения доступны следующие подсказки.

В этом упражнении вам необходимо использовать инкапсуляцию последовательного канала по умолчанию (HDLC) для распространения трафика протокола маршрутизации вашей рабочей группы в центральном сегменте. Кроме того, вам следует настроить протокол маршрутизации EIGRP и применить аутентификацию EIGRP MD5 для гарантии подлинности обновлений маршрутизации. Затем вы должны проверить конфигурацию и работу протокола EIGRP.

В таблице ниже перечислены IP-адреса, которые необходимы для этого упражнения. Для масок подсети указано количество сетевых битов (/биты).

Рабочая группа	Сеть VLAN 1 интерфейса коммутатора (Switch*X*)	Интерфейс Fa0/0 маршрутизатора (Router*X*)	Интерфейс Loopback 0 маршрутизатора (Router*X*)	Интерфейс S0/0/0 маршрутизатора (Router*X*)	Интерфейс S0/0/1 маршрутизатора (Router*X*)	Последовательный интерфейс центрального маршрутизатора (Центральный маршрутизатор)
A	10.2.2.11/24	10.2.2.3/24	192.168.1.65/28	10.140.1.2/24	10.23.23.1/24	10.140.1.1/24
B	10.3.3.11/24	10.3.3.3/24	192.168.1.81/28	10.140.2.2/24	10.23.23.2/24	10.140.2.1/24
C	10.4.4.11/24	10.4.4.3/24	192.168.2.65/28	10.140.3.2/24	10.45.45.1/24	10.140.3.1/24
D	10.5.5.11/24	10.5.5.3/24	192.168.2.81/28	10.140.4.2/24	10.45.45.2/24	10.140.4.1/24
E	10.6.6.11/24	10.6.6.3/24	192.168.3.65/28	10.140.5.2/24	10.67.67.1/24	10.140.5.1/24
F	10.7.7.11/24	10.7.7.3/24	192.168.3.81/28	10.140.6.2/24	10.67.67.2/24	10.140.6.1/24
G	10.8.8.11/24	10.8.8.3/24	192.168.4.65/28	10.140.7.2/24	10.89.89.1/24	10.140.7.1/24
H	10.9.9.11/24	10.9.9.3/24	192.168.4.81/28	10.140.8.2/24	10.89.89.2/24	10.140.8.1/24

Задача 1: активация маршрутизации по протоколу EIGRP

Цель этой задачи — настроить протокол EIGRP на маршрутизаторе. Для этого необходимо назначить автономную систему маршрутизации и определить сети, которые будут участвовать в процессе EIGRP.

Процедура упражнения

Выполните следующие действия на маршрутизаторе рабочей группы.

Действие 1 Со своего ПК создайте подключение к лабораторному оборудованию.

Действие 2 Выберите свою рабочую группу в главном меню.

Действие 3 Выберите маршрутизатор рабочей группы в меню "Модуль".

Действие 4 Убедитесь, что два первых последовательных интерфейса (S0/0/0 и S0/0/1) настроены на использование HDLC. Для этого введите команду **show interfaces serial**. Тип инкапсуляции указывается в четвертой строке выходных данных.

Действие 5 Проверьте, какой кабель — DCE или DTE — подключен ко второму последовательному интерфейсу (S0/0/1) с помощью команды **show controllers serial** *интерфейс*. Если ко второму последовательному интерфейсу (S0/0/1) подключена сторона DCE, убедитесь, что задана тактовая частота 64000. (Вы должны были сделать это во время предыдущей лабораторной работы.)

Примечание. Интерфейсы DTE не требуют настройки тактовой частоты.

Действие 6 Включите процесс маршрутизации EIGRP. Используйте число 100 в качестве номера автономной системы EIGRP.

Действие 7 Включите протокол EIGRP на интерфейсах loopback 0 и Fa0/0, а также на двух последовательных интерфейсах (S0/0/0 и S0/0/1). Используйте два сетевых оператора.

Настройте полосу пропускания 64 Кбит/с на обоих последовательных интерфейсах (S0/0/0 и S0/0/1)**.**

Действие 8 Переходите к задаче 2.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- протокол EIGRP включен и ему назначен номер автономной системы;
- определены сети, которые будут участвовать в процессе маршрутизации EIGRP.

Задача 2: включение аутентификации EIGRP MD5

Цель этой задачи — настроить аутентификацию EIGRP на маршрутизаторе. Протокол EIGRP не будет объявлять маршруты между соседними узлами, если они не идентифицировали себя должным образом.

Процедура упражнения

Выполните следующие действия на маршрутизаторе рабочей группы.

Действие 1 Создайте цепь ключей с именем **icndchain.**

Действие 2 Настройте ключ 1 со строкой **san-fran**.

Действие 3 Настройте маршрутизатор рабочей группы на использование аутентификации EIGRP MD5 со всеми соседними узлами EIGRP с цепью ключей **icndchain**.

Действие 4 Переходите к задаче 3.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- создана и применена цепь ключей EIGRP;
- активирована аутентификация EIGRP MD5.

Задача 3: проверка маршрутизации EIGRP и аутентификации MD5

В этой задаче вы должны проверить работу и конфигурацию протокола маршрутизации EIGRP. Для этого необходимо использовать несколько команд **show**.

Процедура упражнения

Выполните следующие действия на маршрутизаторе рабочей группы.

Действие 1 С помощью команды **show ip route** убедитесь, что маршруты от протокола EIGRP получены. Выходные данные команды должны выглядеть следующим образом:

```
RouterA# 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
       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 not set

     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
D       172.16.31.0/24 [90/40640000] via 10.140.1.1, 00:01:09, Serial0/0/0
     10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
C       10.23.23.0/24 is directly connected, Serial0/0/1
D       10.3.3.0/24 [90/40514560] via 10.23.23.2, 00:01:09, Serial0/0/1
C       10.2.2.0/24 is directly connected, FastEthernet0/0
D       10.1.1.0/24 [90/40514560] via 10.140.1.1, 00:01:10, Serial0/0/0
D       10.0.0.0/8 is a summary, 00:27:11, Null0
D       10.140.2.0/24 [90/41024000] via 10.140.1.1, 00:01:12, Serial0/0/0
                      [90/41024000] via 10.23.23.2, 00:01:12, Serial0/0/1
C       10.140.1.0/24 is directly connected, Serial0/0/0
     192.168.1.0/24 is variably subnetted, 3 subnets, 3 masks
C       192.168.1.64/28 is directly connected, Loopback0
O       192.168.1.81/32 [110/1563] via 10.23.23.2, 00:26:58, Serial0/0/1
D       192.168.1.0/24 is a summary, 00:01:09, Null0
```

Отображается комбинация протоколов OSPF и EIGRP? Почему или почему не не отображается?

_____

Примечание. Настройку EIGRP могли закончить не все рабочие группы в классе.

Действие 2 С помощью команды **show ip protocols** убедитесь, что протокол EIGRP включен и распознает автономную систему. Выходные данные команды должны выглядеть следующим образом:

```
RouterA# show ip protocols
Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 100
```



```
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is in effect
  Automatic address summarization:
    192.168.1.0/24 for FastEthernet0/0, Serial0/0/0,
Serial0/0/1
      Summarizing with metric 128256
    10.0.0.0/8 for Loopback0
      Summarizing with metric 28160
  Maximum path: 4
  Routing for Networks:
    10.0.0.0
    192.168.1.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    (this router)         90      00:01:08
    10.140.1.1            90      00:01:08
  Distance: internal 90 external 170
```

Действие 3 С помощью команды **show ip eigrp neighbor** выведите состояние соседнего узла. Выходные данные команды должны выглядеть следующим образом:

```
RouterA# sh ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
1   10.23.23.2              Se0/0/1           13 00:02:26   29  2280  0  15
0   10.140.1.1              Se0/0/0           10 00:28:26   24  2280  0  25
```

Примечание. Соседние узлы не будут отображаться, пока на них не будут выполнены предыдущие задачи этого упражнения.

Действие 4 Отправьте эхо-запрос в интерфейс возвратной петли (172.16.31.100) центрального маршрутизатора. Как только другая рабочая группа закончит настройку EIGRP, отправьте эхо-запрос в Ethernet-интерфейс локальной сети, указанный в таблице подсказок для этого упражнения. Эхо-запросы должны быть обработаны успешно.

Действие 5 Переходите к задаче 4.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- конфигурация и функционирование протокола маршрутизации EIGRP проверены с помощью команд **show**;
- соединения проверены путем отправки эхо-запроса по удаленным адресам, не имеющим прямого подключения к вашему маршрутизатору рабочей группы.

Задача 4: отладка маршрутизации по протоколу EIGRP

В этой задаче вам необходимо выполнить отладку EIGRP. В результате вы будете знать, какие симптомы следует искать для устранения проблем EIGRP.

Процедура упражнения

Выполните следующие действия на маршрутизаторе рабочей группы.

Действие 1 Выведите данные о событиях соседних узлов EIGRP с помощью команды **debug eigrp neighbors**.

Действие 2 Войдите в режим конфигурации интерфейса и введите команду **shutdown** на втором последовательном интерфейсе.

Действие 3 Подождите 10 секунд и введите команду **no shutdown** на последовательном интерфейсе. Выходные данные команды должны выглядеть следующим образом:

```
RouterA#debug eigrp neighbors
*Feb 28 22:05:51.651: %OSPF-5-ADJCHG: Process 100, Nbr 192.168.1.81 on
Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached
*Feb 28 22:05:51.659: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 10.23.23.2
(Serial0/0/1) is down: interface downn
*Feb 28 22:05:51.659: Going down: Peer 10.23.23.2 total=1 stub 0 template=1,
iidb-stub=0 iid-all=0
*Feb 28 22:05:51.659: EIGRP: Neighbor 10.23.23.2 went down on Serial0/0/1
*Feb 28 22:05:52.559: EIGRP: Packet from ourselves ignoredo
*Feb 28 22:05:53.651: %LINK-5-CHANGED: Interface Serial0/0/1, changed state to
administratively down
*Feb 28 22:05:54.651: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to do
*Feb 28 22:05:57.391: EIGRP: Packet from ourselves ignoredn
*Feb 28 22:06:02.271: EIGRP: Packet from ourselves ignoredo shut
RouterA(config-if)#
*Feb 28 22:06:06.955: EIGRP: Packet from ourselves ignored
*Feb 28 22:06:07.355: %LINK-3-UPDOWN: Interface Serial0/0/1, changed state to
up
*Feb 28 22:06:07.515: %OSPF-5-ADJCHG: Process 100, Nbr 192.168.1.81 on
Serial0/0/1 from LOADING to FULL, Loading Done
*Feb 28 22:06:08.355: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
*Feb 28 22:06:10.715: EIGRP: New peer 10.23.23.2 total=2 stub 0 template=1
idbstub=0 iidball=1
*Feb 28 22:06:10.715: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 10.23.23.2
(Serial0/0/1) is up: new adjacency
```

Действие 4 Отключите отладку.

Действие 5 Сохраните работающую конфигурацию в NVRAM.

Действие 6 Сообщите инструктору, что вы выполнили упражнение.

Проверка упражнения

Задание считается выполненным, если достигнут следующий результат:

- выполнена отладка EIGRP с помощью команды **debug eigrp neighbor**.

Лабораторная работа 5-2: устранение неполадок EIGRP

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

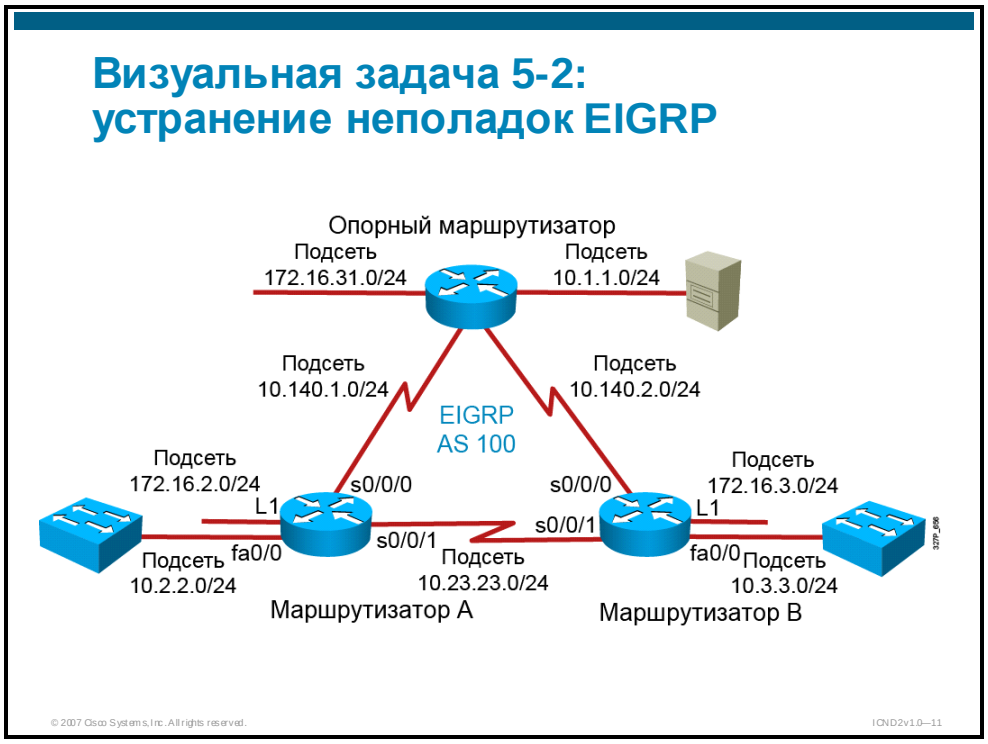
Задачи упражнения

В этом упражнении вам необходимо воспользоваться инструкциями по устранению неполадок, рассмотренными в соответствующем модуле, чтобы собрать сведения о симптомах, а затем изолировать и устранить проблемы, часто встречающиеся в сетях EIGRP. После выполнения этого упражнения вы должны быть готовы к следующим задачам:

- обнаружение проблем подключения в сетях EIGRP, изоляция и устранение проблем подключения EIGRP в соответствии с инструкциями по устранению неполадок.
- тестирование сетевых подключений EIGRP.

Визуальная задача

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



Необходимые ресурсы

Ниже перечислены ресурсы и устройства, необходимые для выполнения этого упражнения.

- ПК, подключенный к локальной лаборатории или ПК с Интернет-подключением и доступом к удаленной лаборатории.
- Терминальный сервер, подключенный к консольному порту всех лабораторных устройств (при использовании удаленной лаборатории).
- Рабочая группа ICND, назначенная инструктором.

Список команд

В таблице приводится описание команд, используемых в упражнении. Команды перечислены в алфавитном порядке, что позволит легко найти нужные сведения. Если во время упражнения вам потребуется помощь по командам конфигурации, воспользуйтесь этим списком.

Команды для устранения неполадок EIGRP

Команда	Описание
debug ip eigrp	Отображает сводные сведения о транзакциях EIGRP.
interface loopback 1	Создает интерфейс возвратной петли.
network 172.16.0.0	Включает протокол маршрутизации на интерфейсах указанной сети.
ping <cr>	Расширенный эхо-запрос для проверки подключений 3-го уровня с возможностью добавления параметров.
show interfaces ***тип***	Отображает статистику интерфейсов, настроенных на маршрутизаторе.
show ip eigrp neighbor	Определяет состояние соседнего узла EIGRP.
show ip protocols	Отображает параметры протоколов маршрутизации и данные таймера протокола маршрутизации, связанного с маршрутизатором.
show ip route	Отображает таблицу маршрутизации.

Подсказки

В этом упражнении интерфейсы возвратной петли на маршрутизаторе рабочей группы и центральном маршрутизаторе будут представлять локальные сети, которые соединяются с помощью протокола маршрутизации EIGRP. Вы должны создать новый интерфейс возвратной петли на маршрутизаторе рабочей группы, который будет представлять локальную сеть, и проверить подключение к интерфейсу возвратной петли центрального маршрутизатора. Если подключение неисправно, вам следует изолировать и устранить проблему.

Для этого упражнения доступны следующие подсказки.

Рабочая группа	Интерфейс Fa0/0 маршрутизатора (Router*X*)	Интерфейс Loopback 0 маршрутизатора (Router*X*)	Интерфейс Loopback 1 маршрутизатора (Router*X*)	Интерфейс S0/0/0 маршрутизатора (Router*X*)	Интерфейс S0/0/1 маршрутизатора (Router*X*)	Последовательный интерфейс центрального маршрутизатора (Центральный маршрутизатор)
A	10.2.2.3/24	192.168.1.65/28	172.16.2.1/24	10.140.1.2/24	10.23.23.1/24	10.140.1.1/24
B	10.3.3.3/24	192.168.1.81/28	172.16.3.1/24	10.140.2.2/24	10.23.23.2/24	10.140.2.1/24
C	10.4.4.3/24	192.168.2.65/28	172.16.4.1/24	10.140.3.2/24	10.45.45.1/24	10.140.3.1/24
D	10.5.5.3/24	192.168.2.81/28	172.16.5.1/24	10.140.4.2/24	10.45.45.2/24	10.140.4.1/24
E	10.6.6.3/24	192.168.3.65/28	172.16.6.1/24	10.140.5.2/24	10.67.67.1/24	10.140.5.1/24
F	10.7.7.3/24	192.168.3.81/28	172.16.7.1/24	10.140.6.2/24	10.67.67.2/24	10.140.6.1/24
G	10.8.8.3/24	192.168.4.65/28	172.16.8.1/24	10.140.7.2/24	10.89.89.1/24	10.140.7.1/24
H	10.9.9.3/24	192.168.4.81/28	172.16.9.1/24	10.140.8.2/24	10.89.89.2/24	10.140.8.1/24

Используйте эту таблицу для документирования процесса устранения неполадок.

Действия по устранению неполадок

Команды для сбора данных о симптомах	Изоляция проблемы	Команда для устранения проблемы
Пример:		
ping 172.16.2.2	отказ	-----
show ip interface brief	интерфейс Fa0/1 отключен администратором	no shutdown
ping 172.16.2.2	повторный отказ	-----
show interface Fa0/1	неверный ip-адрес	ip address 192.168.1.2
ping 172.16.2.2	успешно	

Задача 1: создание и объявление локальной сети.

В этой задаче вам необходимо создать интерфейс возвратной петли на маршрутизаторе рабочей группы. Этот интерфейс будет представлять локальную сеть и объявлять ее в других компонентах сети.

Процедура упражнения

Выполните следующие действия.

Действие 1 Проверьте подключение к интерфейсу возвратной петли центрального маршрутизатора. Отправьте эхо-запрос в интерфейс возвратной петли центрального маршрутизатора (172.16.31.100) с маршрутизатора рабочей группы.

Примечание. Если эхо-запрос обрабатывается неудачно, обратитесь к инструктору.

Действие 2 Создайте интерфейс loopback 1 на маршрутизаторе рабочей группы и назначьте ему адрес, указанный в таблице подсказок для этого упражнения.

Действие 3 Настройте протокол EIGRP в маршрутизаторе рабочей группы на объявление сети loopback 1 (172.16.0.0).

Действие 4 Проверьте интерфейс и его адрес с помощью команды **show interface loopback 1**. Выходные данные команды должны выглядеть следующим образом:

```
RouterA# sh int lo1
Loopback1 is up, line protocol is up
  Hardware is Loopback
  Internet address is 172.16.2.1/24
  MTU 1514 bytes, BW 8000000 Kbit, DLY 5000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation LOOPBACK, loopback not set
  Last input 00:00:03, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     202106 packets output, 12126360 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Действие 5 С помощью команды **show ip protocols**, убедитесь, объявляется сеть, представленная интерфейсом loopback 1. Выходные данные команды должны выглядеть следующим образом:

```
RouterA# show ip protocols
Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 100
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is in effect
  Automatic address summarization:
    172.16.0.0/16 for FastEthernet0/0, Serial0/0/0, Serial0/0/1
      Summarizing with metric 128256
    10.0.0.0/8 for Loopback1
      Summarizing with metric 28160
  Maximum path: 4
  Routing for Networks:
    10.0.0.0
    172.16.0.0
    192.168.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    (this router)         90      00:17:20
    10.23.23.2            90      00:02:16
    10.140.1.1            90      00:02:16
  Distance: internal 90 external 170
```

Действие 6 Переходите к задаче 2.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- создан интерфейс loopback 1 и ему назначен адрес;
- сеть loopback 1 объявлена с помощью протокола EIGRP.

Задача 2: проверка подключения.

В этой задаче вам необходимо проверить подключение локальной сети (интерфейса loopback 1) к локальной сети центрального маршрутизатора (интерфейсу возвратной петли центрального маршрутизатора). Если подключение недосупно, вам следует изолировать и устранить проблему.

Процедура упражнения

Выполните следующие действия.

Действие 1 Помимо увеличения числа пакетов, отправляемых в эхо-запросе, расширенный эхо-запрос позволяет изменить адрес источника эхо-запроса. На маршрутизаторе рабочей группы создайте расширенный эхо-запрос, используя интерфейс loopback 1 в качестве источника и интерфейс возвратной петли центрального маршрутизатора (172.16.31.100) в качестве адресата. Выходные данные команды должны выглядеть следующим образом:

```
RouterA# ping
Protocol [ip]:
Target IP address: 172.16.31.100
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: loopback 1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.31.100, timeout is 2
seconds:
Packet sent with a source address of 172.16.2.1
```

Примечание. Кроме того, вы можете изменить адрес источника эхо-запросе маршрутизатора с помощью команды **ping** [*адрес_назначения*] **source** [*адрес_источника*|*возвратная петля*]

Эхо-запрос обработан успешно?

Действие 2 Проверьте таблицу маршрутизации маршрутизатора рабочей группы. Что вы обнаружили?

Выходные данные команды должны выглядеть следующим образом:

```
RouterA# 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
       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 not set

     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.2.0 is directly connected, Loopback1
     10.0.0.0/24 is subnetted, 6 subnets
C       10.23.23.0 is directly connected, Serial0/0/1
D       10.3.3.0 [90/40514560] via 10.23.23.2, 01:11:41, Serial0/0/1
C       10.2.2.0 is directly connected, FastEthernet0/0
D       10.1.1.0 [90/40514560] via 10.140.1.1, 01:11:39, Serial0/0/0
D       10.140.2.0 [90/41024000] via 10.140.1.1, 01:11:40, Serial0/0/0
                   [90/41024000] via 10.23.23.2, 01:11:40, Serial0/0/1
C       10.140.1.0 is directly connected, Serial0/0/0
     192.168.1.0/24 is variably subnetted, 3 subnets, 3 masks
C       192.168.1.64/28 is directly connected, Loopback0
O       192.168.1.81/32 [110/1563] via 10.23.23.2, 00:09:27, Serial0/0/1
D       192.168.1.0/24 [90/40640000] via 10.23.23.2, 00:07:25, Serial0/0/1
```

Действие 3 Создайте сеанс связи с центральным маршрутизатором (10.1.1.3) по протоколу Telnet и проверьте его таблицу маршрутизации. Что вы обнаружили?

Выходные данные команды должны выглядеть следующим образом:

```
CoreRouter> 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
       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 not set
```



```
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.31.0/24 is directly connected, Loopback0
D       172.16.0.0/16 is a summary, 00:10:39, Null0
     10.0.0.0/24 is subnetted, 6 subnets
D       10.23.23.0 [90/41024000] via 10.140.1.2, 01:15:07, Serial1/0
D       10.3.3.0 [90/41026560] via 10.140.1.2, 01:15:07, Serial1/0
D       10.2.2.0 [90/40514560] via 10.140.1.2, 01:15:07, Serial1/0
C       10.1.1.0 is directly connected, FastEthernet0/0.1
C       10.140.2.0 is directly connected, Serial1/1
C       10.140.1.0 is directly connected, Serial1/0
     192.168.1.0/24 is variably subnetted, 4 subnets, 3 masks
O       192.168.1.65/32 [110/1563] via 10.140.1.2, 00:12:41, Serial1/0
D       192.168.1.64/28 [90/40640000] via 10.140.1.2, 00:10:42, Serial1/0
O       192.168.1.81/32 [110/1563] via 10.140.2.2, 00:12:44, Serial1/1
D       192.168.1.0/24 [90/41152000] via 10.140.1.2, 00:10:42, Serial1/0
```

Действие 4 На маршрутизаторе рабочей группы введите команду **debug ip eigrp**.

Действие 5 Введите команду **shutdown**, а затем команду **no shutdown**, чтобы сбросить интерфейс loopback 1 маршрутизатора рабочей группы. Проанализируйте выходные данные отладки, которые будут выведены в результате этого действия. Что вы обнаружили при анализе выходных данных отладки?

Выходные данные команды должны выглядеть следующим образом:

```
*Mar  2 05:09:47.151: IP-EIGRP(Default-IP-Routing-Table:100):
route installed for 172.16.0.0  (Summary)
*Mar  2 05:09:47.167: IP-EIGRP(Default-IP-Routing-Table:100):
172.16.2.0/24 - don't advertise out Serial0/0/0
*Mar  2 05:09:47.167: IP-EIGRP(Default-IP-Routing-Table:100):
172.16.0.0/16 - do advertise out Serial0/0/0
*Mar  2 05:09:47.167: IP-EIGRP(Default-IP-Routing-Table:100): Int
172.16.0.0/16 metric 128256 - 256 128000
*Mar  2 05:09:47.167: IP-EIGRP(Default-IP-Routing-Table:100):
172.16.2.0/24 - don't advertise out Serial0/0/1
*Mar  2 05:09:47.167: IP-EIGRP(Default-IP-Routing-Table:100):
172.16.0.0/16 - do advertise out Serial0/0/1
*Mar  2 05:09:47.167: IP-EIGRP(Default-IP-Routing-Table:100): Int
172.16.0.0/16 metric 128256 - 256 128000
```

Действие 6 Не используя команду **show run**, соберите сведения о симптомах, а затем изолируйте и устраните проблему с помощью инструкций по устранению неполадок и команд, рассмотренных в соответствующем модуле. Воспользуйтесь таблицей подсказок в начале этого упражнения, чтобы задокументировать процесс устранения неполадок.

Действие 7 Сохраните работающую конфигурацию в NVRAM.

Проверка упражнения

Задание считается выполненным, если достигнут следующий результат:

- сетевое подключение восстановлено, эхо-запрос, отправленный с интерфейса loopback 1 маршрутизатора рабочей группы в интерфейс возвратной петли центрального маршрутизатора обрабатывается успешно.

Лабораторная работа 6-1: внедрение и устранение неполадок списков контроля доступа (ACL)

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

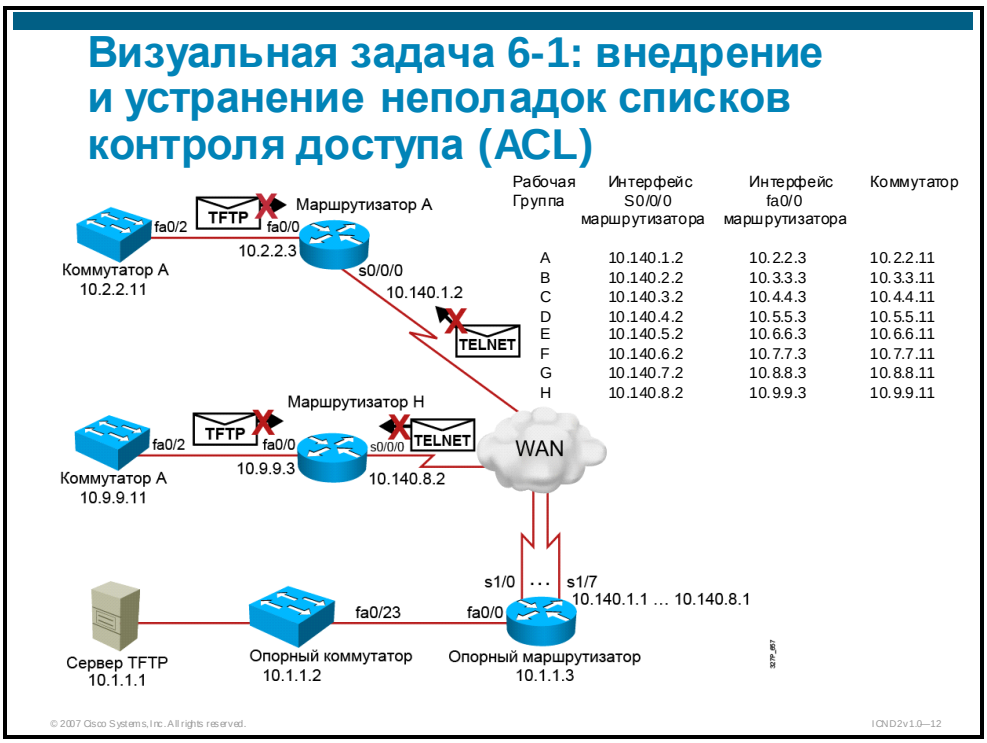
Задачи упражнения

В этом упражнении вам необходимо настроить список контроля доступа для протокола IP (IP ACL). После выполнения этого упражнения вы должны быть готовы к следующим задачам:

- создание расширенного списка доступа по протоколу IP для блокировки трафика Telnet, применение списка доступа к интерфейсу и проверка его работы.
- создание расширенного списка контроля доступа по протоколу IP для блокировки запросов TFTP от рабочей группы;
- изоляция и устранение проблемы списка контроля доступа.

Визуальная задача

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 локальной лаборатории или ПК с Интернет-подключением и доступом к удаленной лаборатории.
- Терминальный сервер, подключенный к консольному порту всех лабораторных устройств (при использовании удаленной лаборатории).
- Рабочая группа ICND, назначенная инструктором.

Список команд

В таблице приводится описание команд, используемых в упражнении. Команды перечислены в алфавитном порядке, что позволит легко найти нужные сведения. Если во время упражнения вам потребуется помощь по командам конфигурации, воспользуйтесь этим списком.

Команды

Команда	Описание
access-list ***номер списка доступа*** **{permit | deny} {test conditions}**	Создает расширенный список доступа по протоколу IP.
copy tftp://10.1.1.1/ ***имя файла*** **running-config**	Копирует конфигурацию с TFTP-сервера в оперативную память коммутатора Cisco Catalyst.
ip access-group ***номер списка доступа*** **{in | out}**	Включает список доступа по протоколу IP на интерфейсе.
ping ***ip-адрес***	Стандартный инструмент, используемый для проверки доступности устройств.
show ip access-list	Отображает содержимое всех списков доступа по протоколу IP.
show ip interface ***тип интерфейса номер интерфейса***	Отображает данные об интерфейсе, связанные с протоколом IP, включая списки контроля доступа, настроенные для этого интерфейса.
telnet ***ip-адрес***	Запускает программу эмуляции терминала на ПК, маршрутизаторе или коммутаторе, которая обеспечивает удаленный доступ к сетевым устройствам через сеть.

Подсказки

Для упражнений этой лабораторной работы доступны следующие подсказки.

Рабочая группа	Подсети 10.x.x.0/24	Сеть VLAN 1 интерфейса коммутатора (Switch*X*)	Интерфейс Fa0/0 маршрути-затора (Router*X*)	Интерфейс Loopback 0 маршрути-затора (Router*X*)	Интерфейс S0/0/0 маршрути-затора (Router*X*)	Последователь ный интерфейс центрального маршрути-затора (Центральный маршрути-затор)
A	10.2.2.0/24	10.2.2.11/24	10.2.2.3/24	192.168.1.65/28	10.140.1.2/24	10.140.1.1/24
B	10.3.3.0/24	10.3.3.11/24	10.3.3.3/24	192.168.1.81/28	10.140.2.2/24	10.140.2.1/24
C	10.4.4.0/24	10.4.4.11/24	10.4.4.3/24	192.168.2.65/28	10.140.3.2/24	10.140.3.1/24
D	10.5.5.0/24	10.5.5.11/24	10.5.5.3/24	192.168.2.81/28	10.140.4.2/24	10.140.4.1/24
E	10.6.6.0/24	10.6.6.11/24	10.6.6.3/24	192.168.3.65/28	10.140.5.2/24	10.140.5.1/24
F	10.7.7.0/24	10.7.7.11/24	10.7.7.3/24	192.168.3.81/28	10.140.6.2/24	10.140.6.1/24
G	10.8.8.0/24	10.8.8.11/24	10.8.8.3/24	192.168.4.65/28	10.140.7.2/24	10.140.7.1/24
H	10.9.9.0/24	10.9.9.11/24	10.9.9.3/24	192.168.4.81/28	10.140.8.2/24	10.140.8.1/24

Задача 1: создание расширенного списка контроля доступа для блокировки трафика Telnet, направленного в вашу рабочую группу

В ходе выполнения этой задачи вы будете работать со студентом из другой рабочей группы. Вам необходимо настроить расширенный список контроля доступа по протоколу IP для блокировки входящего трафика Telnet, отправленного извне вашей рабочей группы. Вы должны настроить список контроля доступа, применить его к интерфейсу и проверить конфигурацию, попросив напарника создать сеанс Telnet с вашим коммутатором рабочей группы. Если список контроля доступа настроен верно, запрос Telnet не будет выполнен. Затем попытайтесь отправить эхо-запрос на то же устройство. Этот эхо-запрос должен быть обработан успешно.

Назначения рабочих групп: A-B, C-D, E-F, G-H.

Процедура упражнения

Выполните следующие действия на маршрутизаторе рабочей группы.

Действие 1 Со своего ПК создайте подключение к лабораторному оборудованию.

Действие 2 Выберите свою рабочую группу в главном меню.

Действие 3 Выберите маршрутизатор рабочей группы в меню "Модуль".

Действие 4 Отключите второй последовательный интерфейс маршрутизатора рабочей группы (S0/0/1) с помощью команды **shutdown**.

Действие 5 Создайте расширенный список доступа по протоколу IP, запрещающий отправку трафика Telnet в вашу рабочую группу.

Действие 6 Примените расширенный список доступа по протоколу IP к первому последовательному интерфейсу.

Список контроля доступа должен быть применен как входящий или как исходящий?

Действие 7 Введите команду **show ip access-list**, чтобы вывести содержимое списка контроля доступа по протоколу IP.

Действие 8 На последовательном интерфейсе введите команду **show ip interface**, чтобы убедиться, что список контроля доступа применен к первому последовательному интерфейсу.

Действие 9 Попросите напарника создать сеанс Telnet с вашим коммутатором рабочей группы (10.x.x.11) со своего маршрутизатора рабочей группы.

Примечание. Все попытки использования протокола Telnet на вашем коммутаторе рабочей группы должны завершиться неудачей.

Действие 10 Попросите напарника отправить эхо-запрос в коммутатор рабочей группы (10.x.x.11) со своего маршрутизатора рабочей группы.

Примечание. Весь трафик, за исключением трафика Telnet, должен успешно обрабатываться в устройствах вашей рабочей группы.

Действие 11 Переходите к задаче 2.

Проверка упражнения

Задание считается выполненным, если достигнут следующий результат:

- создан расширенный список доступа по протоколу IP, который блокирует входящий трафик Telnet, но разрешает весь прочий трафик, направленный в вашу рабочую группу из внешней сети.

Задача 2: изменение расширенного списка доступа по протоколу IP для блокировки запросов TFTP из вашей рабочей группы

Для этой задачи вам необходимо загрузить новую дополнительную конфигурацию на маршрутизатор рабочей группы с TFTP-сервера. Дополнительная конфигурация подразумевает применение списка контроля доступа, который блокирует все TFTP-запросы из подсети вашей рабочей группы.

Однако дополнительная конфигурация, которую вам следует загрузить, содержит ошибки, которые приведут к потере подключения с другими сегментами сети. Вы должны проверить конфигурацию, чтобы изолировать и устранить проблему путем изменения расширенного списка доступа по протоколу IP.

Процедура упражнения

Действие 1 Проверьте соединение с TFTP-сервером. Отправьте эхо-запрос на TFTP-сервер (10.1.1.1) с коммутатора рабочей группы.

Действие 2 Отправьте эхо-запрос на TFTP-сервер (10.1.1.1) с маршрутизатора рабочей группы.

Примечание. Если любой из эхо-запросов не получает ответ, обратитесь к инструктору.

Действие 3 Загрузите дополнительную конфигурацию с TFTP-сервера в работающую конфигурацию маршрутизатора рабочей группы. Имя файла, который необходимо загрузить: i2-wg_**ro**-config-lab6-1.txt.

Действие 4 Введите команду **exit** в привилегированном приглашении EXEC и убедитесь, что баннер маршрутизатора выглядит следующим образом:

********** wg_ro-config-lab6-1 **********

Примечание. Если вам не удалось загрузить конфигурацию, обратитесь к инструктору.

Введите команду **show ip access-list**, чтобы вывести содержимое расширенного списка контроля доступа по протоколу IP, который вы загрузили (access-list 175). Выходные данные команды должны выглядеть следующим образом:

```
RouterA# sh ip access-lists
Extended IP access list 101
    10 deny tcp 10.140.2.0 0.0.0.255 any eq telnet (12 matches)
    20 permit ip any any (353 matches)
Extended IP access list 175
    10 deny udp any any eq tftp
    20 permit udp any any
```


Действие 5 Введите команду **show ip interface serial** *интерфейс*, чтобы убедиться, что загруженный список контроля доступа (access-list 175) применен к интерфейсу. Выходные данные команды должны выглядеть следующим образом:

```
RouterA# sh ip int s0/0/0
Serial0/0/0 is up, line protocol is up
  Internet address is 10.140.1.2/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10 224.0.0.5
  Outgoing access list is 175
  Inbound  access list is 101
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is enabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF Feature Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF

  -----Output omitted--------
```

Действие 6 Возвращает ли TFTP-сервер эхо-ответ при отправке эхо-запроса с коммутатора рабочей группы?

Действие 7 На маршрутизаторе рабочей группы введите команду **show ip route**, чтобы проверить маршрут к подсети TFTP-сервера (10.1.1.0).

Что вы обнаружили?

Действие 8 Измените список контроля доступа access-list 175 так, чтобы он отклонял только запросы TFTP из вашей рабочей группы и разрешал весь прочий трафик.

Действие 9 Изменив список контроля доступа, проверьте его эффективность. В коммутаторе рабочей группы попробуйте скопировать файл конфигурации i2-wg_sw-config-lab6-1.txt с TFTP-сервера (10.1.1.1) в загрузочную конфигурацию коммутатора.

Примечание. После установки расширенного списка контроля доступа по протоколу IP все запросы TFTP должны отклоняться. Возможно вам придется подождать отклонения запроса TFTP. Коммутатор повторит запрос TFTP несколько раз, прежде чем появится сообщение об ошибке.

Действие 10 С коммутатора рабочей группы отправьте эхо-запрос на TFTP-сервер и интерфейс возвратной петли центрального маршрутизатора (172.16.31.100).

Примечание. Все трафик, за исключением TFTP, должен обрабатываться успешно.

Действие 11 Переходите к задаче 3.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- конфигурация маршрутизатора рабочей группы скопирована с TFTP-сервера и вы убедились том, что соединение между коммутатором рабочей группы и TFTP-сервером потеряно;
- в результате изменения расширенный список контроля доступа по протоколу IP блокирует все запросы TFTP из вашей рабочей группы, но разрешает весь прочий трафик.

Задача 3: удаление списков контроля доступа с последовательного интерфейса

В этой задаче вам необходимо очистить конфигурацию, чтобы изменения, сделанные во время этого упражнения, не помешали выполнению следующей лабораторной работы. Очень важно выполнить эту задачу.

Процедура упражнения

Выполните следующие действия на маршрутизаторе рабочей группы.

Действие 1 Войдите в режим конфигурации для последовательного интерфейса.

Действие 2 Удалите все группы доступа с последовательного интерфейса.

Действие 3 Войдите в режим глобальной конфигурации.

Действие 4 Удалите оба списка контроля доступа.

Действие 5 Сохраните работающую конфигурацию в NVRAM.

Действие 6 Сообщите инструктору, что вы выполнили упражнение.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- с последовательного интерфейса удалены все группы доступа;
- оба списка контроля доступа удалены в режиме глобальной конфигурации.

Лабораторная работа 7-1: настройка NAT (преобразование сетевых адресов) и PAT (преобразование адресов портов)

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

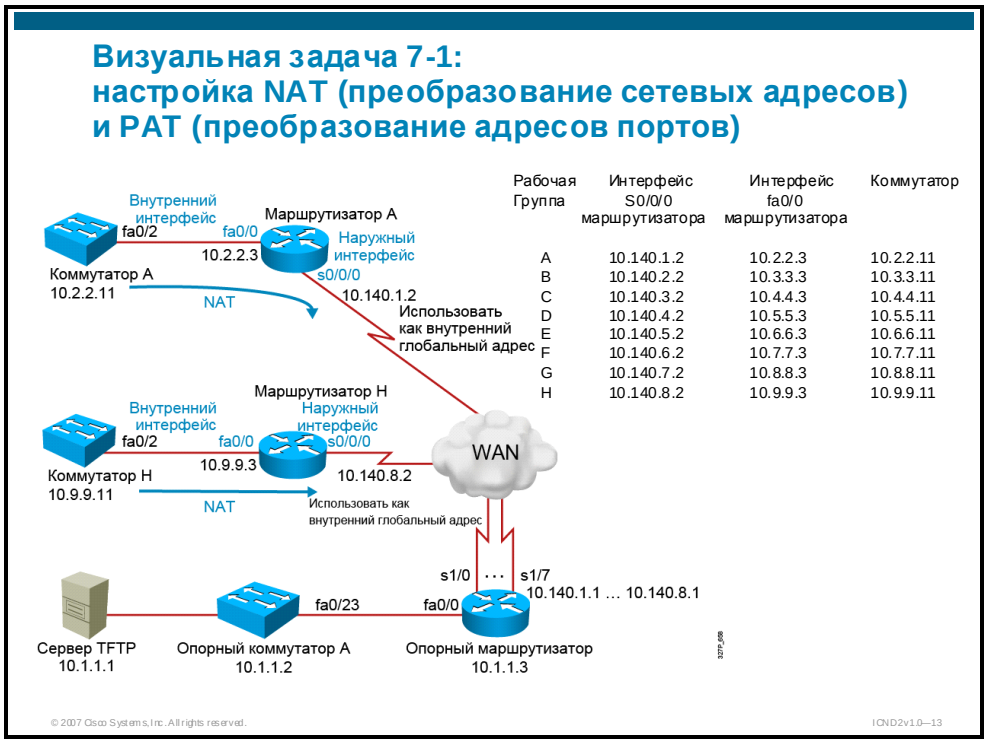
Задачи упражнения

В этом упражнении вы должны настроить маршрутизатор рабочей группы на использование PAT. После выполнения этого упражнения вы должны быть готовы к следующим задачам:

- настройка внутренних и внешних интерфейсов NAT, а также изменение списков контроля доступа по протоколу IP, чтобы дать узлам разрешение на использование PAT;
- использование команд **show** для проверки конфигурации NAT.

Визуальная задача

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 локальной лаборатории или ПК с Интернет-подключением и доступом к удаленной лаборатории.
- Терминальный сервер, подключенный к консольному порту всех лабораторных устройств (при использовании удаленной лаборатории).
- Рабочая группа ICND, назначенная инструктором.

Список команд

В таблице приводится описание команд, используемых в упражнении. Команды перечислены в алфавитном порядке, что позволит легко найти нужные сведения. Если во время упражнения вам потребуется помощь по командам конфигурации, воспользуйтесь этим списком.

Команды

Команда	Описание
debug ip nat	Выполняет отладку процесса преобразования NAT.
ip nat inside	Отмечает интерфейс, как подключенный к внутренней сети.
ip nat inside source list ***номер списка доступа*** **interface** ***интерфейс*** **overload**	Активирует динамическое преобразование источника с учетом списка доступа.
ip nat outside	Отмечает интерфейс, как подключенный к внутренней сети.
show ip nat statistics	Отображает статистику преобразования.
show ip nat translations	Отображает активные процессы преобразования.

Подсказки

Для упражнений этой лабораторной работы доступны следующие подсказки.

Рабочая группа	Подсети FastEthernet рабочей группы 10.x.x.0/24	Сеть VLAN 1 интерфейса коммутатора (Switch*X*)	Интерфейс Fa0/0 маршрутизатора (Router*X*)	Интерфейс Loopback 0 маршрутизатора (Router*X*)	Интерфейс S0/0/0 маршрутизатора (Router*X*)	Последовательный интерфейс центрального маршрутизатора (Центральный маршрутизатор)
A	10.2.2.0/24	10.2.2.11/24	10.2.2.3/24	192.168.1.65/28	10.140.1.2/24	10.140.1.1/24
B	10.3.3.0/24	10.3.3.11/24	10.3.3.3/24	192.168.1.81/28	10.140.2.2/24	10.140.2.1/24
C	10.4.4.0/24	10.4.4.11/24	10.4.4.3/24	192.168.2.65/28	10.140.3.2/24	10.140.3.1/24
D	10.5.5.0/24	10.5.5.11/24	10.5.5.3/24	192.168.2.81/28	10.140.4.2/24	10.140.4.1/24
E	10.6.6.0/24	10.6.6.11/24	10.6.6.3/24	192.168.3.65/28	10.140.5.2/24	10.140.5.1/24
F	10.7.7.0/24	10.7.7.11/24	10.7.7.3/24	192.168.3.81/28	10.140.6.2/24	10.140.6.1/24
G	10.8.8.0/24	10.8.8.11/24	10.8.8.3/24	192.168.4.65/28	10.140.7.2/24	10.140.7.1/24
H	10.9.9.0/24	10.9.9.11/24	10.9.9.3/24	192.168.4.81/28	10.140.8.2/24	10.140.8.1/24

Задача 1: настройка PAT

В этой задаче вам необходимо настроить маршрутизатор на предоставление одного внешнего адреса для всех адресов рабочей группы, запрашивающих в доступ к сети общего пользования. Во-первых вы должны проверить соединение между маршрутизатором рабочей группы и центральным маршрутизатором. Затем необходимо настроить внутренние и внешние интерфейсы NAT. И наконец нужно изменить расширенный список доступа по протоколу IP, чтобы дать определенным узлам разрешение на использование PAT.

Процедура упражнения

Выполните следующие действия, чтобы настроить преобразование адресов портов (PAT).

Действие 1 Со своего ПК создайте подключение к лабораторному оборудованию.

Действие 2 Выберите свою рабочую группу в главном меню.

Действие 3 Выберите свою рабочую группу в меню "Модуль".

Действие 4 Убедитесь, что эхо-запрос, отправленный с коммутатора рабочей группы в центральный маршрутизатор (10.1.1.3), обрабатывается успешно.

Примечание. Если на эхо-запрос не приходит ответа, обратитесь к инструктору.

Действие 5 Чтобы начать конфигурацию NAT, настройте первый Ethernet-интерфейс маршрутизатора рабочей группы в качестве внутреннего интерфейса.

Действие 6 Затем настройте первый последовательный интерфейс маршрутизатора рабочей группы в качестве внешнего интерфейса.

Действие 7 Измените стандартный список доступа по протоколу IP, чтобы разрешить всем узлам в подсети FastEthernet рабочей группы (10.*x*.*x*.0/24) использовать преобразование PAT. См. адреса подсетей в таблице подсказок для этого упражнения.

Действие 8 Настройте процесс PAT с IP-адресом первого последовательного интерфейса в качестве глобального внутреннего IP-адреса.

Действие 9 Включите отладку NAT.

Действие 10 Переходите к задаче 2.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- проверено соединение между маршрутизатором рабочей группы и центральным маршрутизатором;
- настроены внешние и внутренние интерфейсы NAT;
- список контроля доступа по протоколу IP изменен, чтобы дать определенным узлам право на использованием PAT.

Задача 2: проверка PAT с помощью команд show и debug

В этой задаче вам необходимо проверить правильность настройки PAT.

Процедура упражнения

Выполните следующие действия, чтобы проверить преобразование адресов портов.

Действие 1 С коммутатора рабочей группы отправьте эхо-запрос в центральный маршрутизатор (10.1.1.3) и убедитесь, что он запускает процесс PAT на маршрутизаторе рабочей группы.

Действие 2 Вы должны увидеть выходные данные отладки NAT.

Действие 3 На маршрутизаторе рабочей группы введите команду **show ip nat translations**. Выходные данные команды должны выглядеть следующим образом:

```
RouterA# show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 10.140.1.2:13     10.2.2.11:13       10.1.1.3:13        10.1.1.3:13
```

Действие 4 Введите команду **show ip nat statistics**. Выходные данные команды должны выглядеть следующим образом:

```
RouterA# show ip nat statistics
Total active translations: 1 (0 static, 1 dynamic; 1 extended)
Outside interfaces:
  Serial0/0/0
Inside interfaces:
  FastEthernet0/0
Hits: 9  Misses: 1
CEF Translated packets: 10, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 2] access-list 1 interface Serial0/0/0 refcount 1
Queued Packets: 0
```

Действие 5 Отключите все конфигурации PAT на маршрутизаторе рабочей группы.

Действие 6 Отправьте эхо-запрос в центральный маршрутизатор (10.1.1.3) с коммутатора рабочей группы, чтобы убедиться в работоспособности конфигурации.

Действие 7 Сохраните работающую конфигурацию в NVRAM.

Действие 8 Сообщите инструктору, что вы выполнили упражнение.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- правильность настройки PAT проверена путем отправки эхо-запроса в центральный маршрутизатор (10.1.1.3);
- на маршрутизаторе рабочей группы отключены все конфигурации PAT.

Лабораторная работа 7-2: внедрение IPv6

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

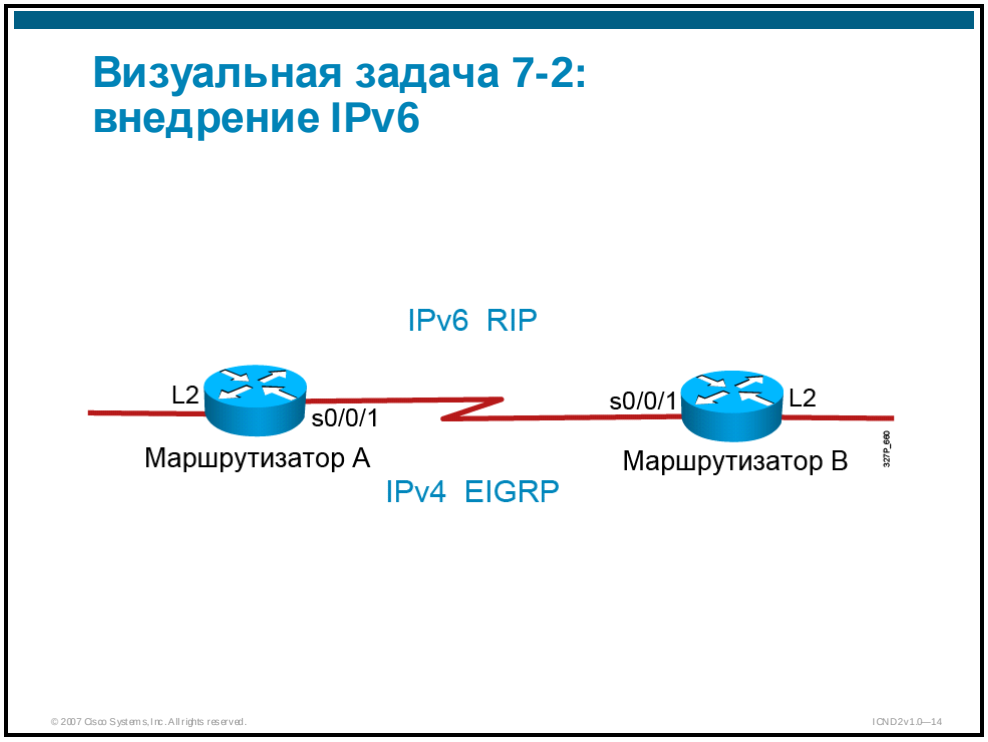
Задачи упражнения

В этом упражнении вам необходимо выделить и настроить адреса IPv6 на маршрутизаторах рабочей группы. После выполнения этого упражнения вы должны быть готовы к следующим задачам:

- определение способа выделения адресов IPv6 для заданных маршрутизаторов с учетом системы нумерации и префикса IPv6;
- настройка интерфейсов маршрутизатора для IPv6 и назначение адресов;
- настройка протокола RIP для поддержки протокола IPv6 и адресов;
- Configure and verify a dual-stack router configurationсоздание и проверка двухстековой конфигурации маршрутизатора.

Визуальная задача

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 локальной лаборатории или ПК с Интернет-подключением и доступом к удаленной лаборатории.
- Терминальный сервер, подключенный к консольному порту всех лабораторных устройств (при использовании удаленной лаборатории).
- Рабочая группа ICND, назначенная инструктором.

Список команд

В таблице приводится описание команд, используемых в упражнении. Команды перечислены в алфавитном порядке, что позволит легко найти нужные сведения. Если во время упражнения вам потребуется помощь по командам конфигурации, воспользуйтесь этим списком.

Команды

Команда	Описание
ipv6 address длина *префикса и адреса* **eui-64**	Включает адрес IPv6 на интерфейсе и заставляет маршрутизатор заполнить младшие 64 бита этого адреса с использованием MAC-адреса.
ipv6 address *длина адреса и префикса ipv6*	Статически назначает адрес IPv6 и длину префикса туннельному интерфейсу.
ipv6 rip *имя* **enable**	Включает выбранный процесс IPv6 RIP на интерфейсе.
ipv6 router rip *имя*	Настраивает процесс маршрутизации IPv6 RIP и активирует режим конфигурации для процесса маршрутизации IPv6 RIP.
ipv6 unicast-routing	Включает пересылку трафика IPv6.
show ipv6 interface	Отображает данные IPv6 для интерфейса.
show ipv6 rip	Отображает сведения о текущих процессах IPv6 RIP.
show ipv6 route	Отображает таблицу маршрутизации IPv6.

Подсказки

Для упражнений этой лабораторной работы доступны следующие подсказки.

Рабочая группа	Номер группы	Номер маршрутизатора	Адрес интерфейса IPv4 Loopback 2 (Router X)
A	1	1	10.123.123.1/24
B	1	2	10.132.132.1/24
C	2	3	10.145.145.1/24
D	2	4	10.154.154.1/24
E	3	5	10.167.167.1/24
F	3	6	10.176.176.1/24
G	4	7	10.189.189.1/24
H	4	8	10.198.198.1/24

Задача 1: подготовка IPv6

Цель задачи 1 — планирование адресации. Настройка начнется в задаче 2. Вы будете работать со студентом из другой рабочей группы.

Назначение групп: A-B, C-D, E-F, G-H.

Процедура упражнения

Выполните следующие действия.

Действие 1 Воспользуйтесь информацией ниже, чтобы заполнить таблицу для всех маршрутизаторов в группе.

	Номер группы (X)	**Номер маршрутизатора (Y)**	**Адрес IPv6 интерфейса S0/0/1**	**Адрес IPv6 интерфейса Loopback 2**
Ваш маршрутизатор:				
Маршрутизатор напарника:				

В этом упражнении для второго последовательного интерфейса (S0/0/1) будет использоваться следующий формат адреса IPv6:

2001:0410:000*x*:10::/64 eui-64

Где *x* = номер вашей группы, указанный в подсказках для этого упражнения.

Например, адрес IPv6 второго последовательного интерфейса (S0/0/1) маршрутизатора A будет 2001:0410:0001:10::/64 eui-64.

Примечание. В адресе IPv6 :10 обозначает подсеть. Для этой лабораторной работы важно, чтобы интерфейсы S0/0/1 одной группы имели одинаковый адрес подсети.

Параметр eui-64 заставляет маршрутизатор принудительно заполнять младшие 64 бита адреса (соответствующие узлу) с использованием MAC-адреса.

Вы создадите интерфейс loopback 2 на маршрутизаторе рабочей группы во время задачи 2. Интерфейсы loopback 2 для всех маршрутизаторов рабочей группы будут иметь следующий формат адреса IPv6:

2001:0410:000*x*:*y*::/64 eui-64

где *x* = номер вашей группы, указанный в таблице подсказок для этого упражнения и *y* = номер вашего маршрутизатора, указанный в той же таблице.

Например, адрес IPv6 интерфейса loopback 2 маршрутизатора A будет 2001:0410:0001:1::/64 eui-64.

Примечание. В адресе IPv6 подсеть обозначается параметром :*y*. Для этой лабораторной работы важно, чтобы интерфейсы loopback 2 маршрутизаторов находились в одной подсети.

Проверка упражнения

Задание считается выполненным, если достигнут следующий результат:

- вы определили адреса IPv6, которые будут назначены всем интерфейсам.

Задача 2: настройка адресов IPv6

Вам необходимо глобально активировать IPv6 на маршрутизаторе и настроить адреса IPv6 на интерфейсах S0/0/1 и Lo2.

Процедура упражнения

Выполните следующие действия.

Действие 1 Отключите первый последовательный интерфейс (S0/0/0) маршрутизатора рабочей группы, подключенный к центральному сегменту, с помощью команды **shutdown**.

Действие 2 Отключите второй последовательный интерфейс (S0/0/1) маршрутизатора рабочей группы с помощью команды **shutdown**.

Действие 3 Включите протокол IPv6 на маршрутизаторе рабочей группы.

Действие 4 Назначьте адрес IPv6, определенный во время задачи 1, второму последовательному интерфейсу (S0/0/1).

Действие 5 Создайте интерфейс loopback 2 и назначьте ему адрес IPv6, определенный во время задачи 1.

Действие 6 Выведите сведения об интерфейсах IPv6 на экран, чтобы убедиться, что всем интерфейсам маршрутизатора рабочей группы назначены верные адреса IPv6.

Выходные данные команды должны выглядеть следующим образом:

```
RouterA# show ipv6 int
Serial0/0/1 is down, line protocol is down
  IPv6 is enabled, link-local address is FE80::21A:6CFF:FE59:D60
[TEN]
  Global unicast address(es):
    2001:410:1:10:21A:6CFF:FE59:D60, subnet is 2001:410:1:10::/64
[EUI/TEN]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF59:D60
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  Hosts use stateless autoconfig for addresses.

Loopback2 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::21A:6CFF:FE59:D60
  Global unicast address(es):
```



```
    2001:410:1:1:21A:6CFF:FE59:D60, subnet is 2001:410:1:1::/64
[EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF59:D60
  MTU is 1514 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is not supported
  ND reachable time is 30000 milliseconds
  Hosts use stateless autoconfig for addresses.
```

Примечание. Состояние интерфейса Pv6 S0/0/1 зависит от того, выполнили ли вы и ваш напарник задачу 2.

Для интерфейсов IPv6 отображаются адреса IPv6, которые вы не настраивали? Если да, какие адреса?

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- протокол IPv6 включен глобально, интерфейсам S0/0/1 и Lo2 назначены адреса IPv6;
- на маршрутизаторе рабочей группы отключен первый последовательный интерфейс и включен второй последовательный интерфейс.

Задача 3: включение протокола RIP для сети IPv6

В этой задаче вы должны включить протокол RIP для сети IPv6 на маршрутизаторе рабочей группы.

Процедура упражнения

Действие 1 На маршрутизаторе рабочей группы глобально включите протокол IPv6 RIP. Используйте имя процесса **cisco**.

Действие 2 Включите процесс IPv6 RIP на втором последовательном интерфейсе (S0/0/1) и интерфейсе loopback 2.

Действие 3 Выведите сведения о процессе IPv6 RIP, чтобы убедиться, что он включен на маршрутизаторах.

Выходные данные, полученные от маршрутизаторов, должны выглядеть следующим образом:

```
RouterA# show ipv6 rip
RIP process "cisco", port 521, multicast-group FF02::9, pid 230
     Administrative distance is 120. Maximum paths is 16
```

```
    Updates every 30 seconds, expire after 180
    Holddown lasts 0 seconds, garbage collect after 120
    Split horizon is on; poison reverse is off
    Default routes are not generated
    Periodic updates 6, trigger updates 1
  Interfaces:
    Loopback2
    Serial0/0/1
  Redistribution:
    None
```

Действие 4 Выведите таблицу маршрутизации IPv6 маршрутизатора. Выходные данные должны выглядеть следующим образом:

```
RouterA# show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS
summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 -
OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   2001:410:1:1::/64 [0/0]
     via ::, Loopback2
L   2001:410:1:1:21A:6CFF:FE59:D60/128 [0/0]
     via ::, Loopback2
R   2001:410:1:2::/64 [120/2]
     via FE80::217:5AFF:FE2E:F570, Serial0/0/1
C   2001:410:1:10::/64 [0/0]
     via ::, Serial0/0/1
L   2001:410:1:10:21A:6CFF:FE59:D60/128 [0/0]
     via ::, Serial0/0/1
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
```

Примечание. Таблица маршрутизации IPv6 должна включать маршрут к сети интерфейса loopback 2 вашего напарника.

Проверка упражнения

Задание считается выполненным, если достигнут следующий результат:

- вы получили данные о сети IPv6 интерфейса loopback 2 маршрутизатора вашего напарника.

Задача 4: настройка и проверка двухстекового маршрутизатора

В этой задаче вам необходимо создать соединение IPv4 между сетями, настроенными на использование IPv6 в маршрутизаторе рабочей группы.

Процедура упражнения

Действие 1 На маршрутизаторе рабочей группы настройте интерфейс loopback 2 с адресом IPv4, указанным в таблице подсказок для этого упражнения.

Действие 2 С помощью команды **show ip route** убедитесь, что процесс EIGRP получил данные о сети интерфейса loopback 2 вашего напарника.

Примечание. Сетевой оператор EIGRP, настроенный во время предыдущей лабораторной работы (**network 10.0.0.0**), должен объявлять сеть IPv4, назначенную интерфейсу loopback 2.

Действие 3 Отправьте эхо-запрос по всем адресам IPv4 маршрутизатора рабочей группы вашего напарника, включая интерфейс loopback 2.

Действие 4 Отправьте эхо-запрос по всем адресам IPv6 маршрутизатора рабочей группы вашего напарника, включая интерфейс loopback 2.

Примечание. Чтобы упростить отправку эхо-запросов по адресам IPv6 в оставшейся части этого упражнения, скопируйте все адреса IPv6 рабочей группы в документ Notepad. Вы можете использовать команду **show cdp neighbor detail**, чтобы отобразить адрес IPv6 подключенного напрямую интерфейса маршрутизатора вашего напарника. Кроме того, вы можете установить сеанс Telnet с маршрутизатором вашего напарника и ввести команду **show ipv6 interface brief**, чтобы вывести адреса IPv6 других интерфейсов маршрутизатора вашего напарника. Задокументировав адреса IPv6 вы сможете просто копировать нужный адрес из документа Notepad и вставлять его в команду ping при отправке эхо-запроса в интерфейс IPv6 одного из соседних маршрутизаторов.

Действие 5 Выходные данные команды должны выглядеть следующим образом:

```
RouterA# ping 2001:410:1:2:216:9DFF:FEB0:EA48


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to
2001:410:1:2:216:9DFF:FEB0:EA48, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms
```

Проверка упражнения

Задание считается выполненным, если достигнут следующий результат:

- между маршрутизаторами группы созданы соединения IPv4 и IPv6.

Лабораторная работа 8-1: создание глобальной сети на базе Frame Relay

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

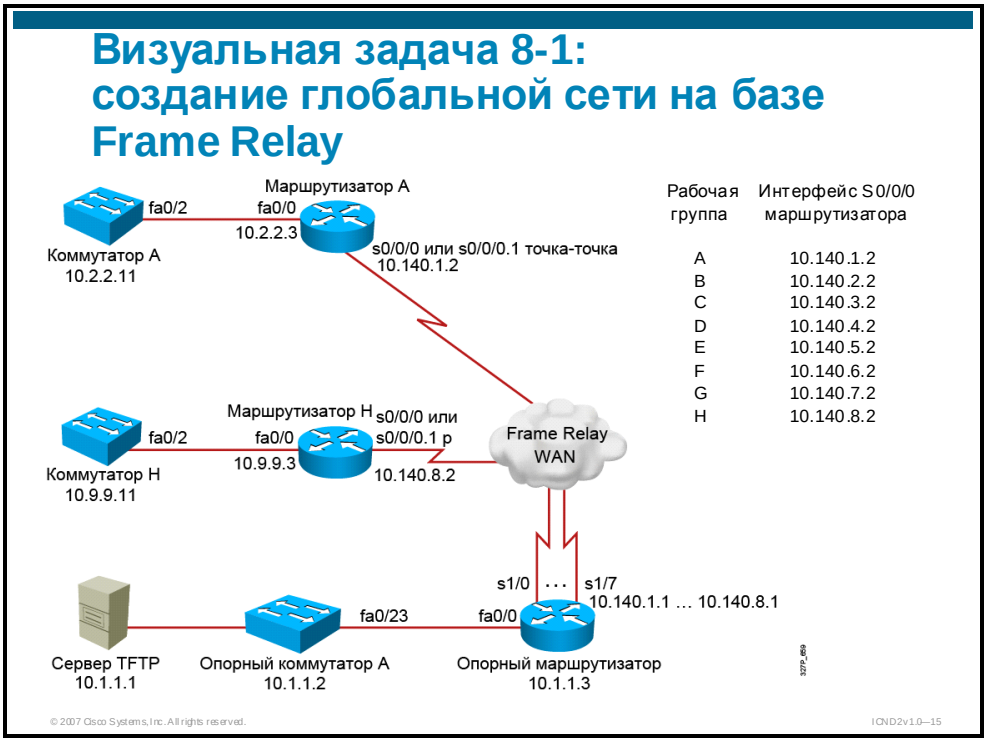
Задачи упражнения

В этом упражнении вам необходимо настроить последовательный интерфейс маршрутизатора рабочей группы на использование инкапсуляции Frame Relay, чтобы создать подключение с пакетной коммутацией к центральным устройствам. После выполнения этого упражнения вы должны быть готовы к следующим задачам:

- настройка последовательного интерфейса на использование инкапсуляции Frame Relay;
- проверка подключения Frame Relay с помощью команд **show** и **ping**;
- настройка команды **debug frame-relay lmi** и интерпретация выходных данных;
- настройка субинтерфейса маршрутизатора и привязка этого субинтерфейса с заданным идентификатором DLCI.

Визуальная задача

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 локальной лаборатории или ПК с Интернет-подключением и доступом к удаленной лаборатории.
- Терминальный сервер, подключенный к консольному порту всех лабораторных устройств (при использовании удаленной лаборатории).
- Рабочая группа ICND, назначенная инструктором.

Список команд

В таблице приводится описание команд, используемых в упражнении. Команды перечислены в алфавитном порядке, что позволит легко найти нужные сведения. Если во время упражнения вам потребуется помощь по командам конфигурации, воспользуйтесь этим списком.

Команда

Команда	Описание
debug frame relay lmi	Отображает данные отладки для сигнализации Frame Relay LMI.
encapsulation frame-relay	Включает инкапсуляцию Frame Relay на интерфейсе.
frame-relay interface-dlci ***номер dlci***	Задает идентификатор DLCI для субинтерфейса типа "точка-точка".
interface serial ***номер.номер субинтерфейса*** **{multipoint | point-to-point}**	Активирует режим конфигурации субинтерфейса и задает тип подключения — "точка-точка" или многоточечное.
ping ***ip-адрес***	Стандартный инструмент, используемый для проверки доступности устройств. Использует эхо-запросы и эхо-ответы ICMP, чтобы определить, активен ли удаленный узел. Кроме того, команда **ping** измеряет время до прихода эхо-ответа.
show frame-relay lmi	Отображает данные LMI.
show frame-relay map	Отображает данные маршрутов Frame Relay.
show frame-relay pvc	Отображает статистику трафика PVC.
show interfaces	Отображает данные по интерфейсу.
show running-config	Отображает активную конфигурацию.
show running-config interface ***тип слот/порт***	Отображает работающую конфигурацию интерфейса.

Подсказки

Для упражнений этой лабораторной работы доступны следующие подсказки. В таблице перечислены IP-адреса для последовательного подключения.

Рабочая группа	Сеть VLAN 1 интерфейса коммутатора (Switch*X*)	Интерфейс Fa0/0 маршрути-затора (Router*X*)	Интерфейс S0/0/0 маршрутиз-атора (Router*X*)	Локальный идентификатор DLCI, определяющий канал PVC к центральным устройствам	Последовательный интерфейс центрального маршрути-затора (Центральный маршрути-затор)
A	10.2.2.11/24	10.2.2.3/24	10.140.1.2/24	100	10.140.1.1/24
B	10.3.3.11/24	10.3.3.3/24	10.140.2.2/24	110	10.140.2.1/24
C	10.4.4.11/24	10.4.4.3/24	10.140.3.2/24	120	10.140.3.1/24
D	10.5.5.11/24	10.5.5.3/24	10.140.4.2/24	130	10.140.4.1/24
E	10.6.6.11/24	10.6.6.3/24	10.140.5.2/24	140	10.140.5.1/24
F	10.7.7.11/24	10.7.7.3/24	10.140.6.2/24	150	10.140.6.1/24
G	10.8.8.11/24	10.8.8.3/24	10.140.7.2/24	160	10.140.7.1/24
H	10.9.9.11/24	10.9.9.3/24	10.140.8.2/24	170	10.140.8.1/24

Задача 1: активация подключения Frame Relay

В этой задаче вам необходимо настроить первый последовательный интерфейс на использование инкапсуляции Frame Relay.

Процедура упражнения

Действие 1 Со своего ПК создайте подключение к лабораторному оборудованию.

Действие 2 Выберите свою рабочую группу в главном меню.

Действие 3 Выберите маршрутизатор рабочей группы в меню "Модуль".

Действие 4 Войдите в режим конфигурации первого последовательного интерфейса маршрутизатора рабочей группы (S0/0/0) и отключите его с помощью команды **shutdown.**

Действие 5 Включите Frame Relay на первом последовательном интерфейсе (S0/0/0) маршрутизатора.

Примечание. Тип LMI будет задан с использованием функции автоопределения. Протокол ARP с инверсией будет использован для привязки IP-адресов идентификаторам DLCI.

Действие 6 Включите первый последовательный интерфейс (S0/0/0) с помощью команды **no shutdown**.

Действие 7 Введите команду **show running-config** для интерфейса S0/0/0. Выходные данные команды должны выглядеть следующим образом:

```
interface Serial 0/0/0
 ip address 10.140.1.2 255.255.255.0
 encapsulation frame-relay
 no ip mroute-cache
 no fair-queue
```

Действие 8 Переходите к задаче 2.

Проверка упражнения

Задание считается выполненным, если достигнут следующий результат:

- последовательный интерфейс настроен на использование инкапсуляции Frame Relay.

Задача 2: проверка подключения Frame Relay

В этой задаче вам необходимо проверить конфигурацию с помощью команды **show** и отправки эхо-запроса в центральный маршрутизатор.

Процедура упражнения

Выполните следующие действия на маршрутизаторе рабочей группы, чтобы проверить подключение Frame Relay.

Действие 1 Убедитесь, что первый последовательный интерфейс находится в состоянии "up/up" с помощью команды **show interfaces serial**. Выходные данные команды должны выглядеть следующим образом:

```
RouterA#show interfaces s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 10.140.1.2/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255,
load 1/255
  Encapsulation FRAME-RELAY, loopback not set, keepalive set (10
sec)
  LMI enq sent  19, LMI stat recvd 20, LMI upd recvd 0, DTE LMI
up
  LMI enq recvd 0, LMI stat sent  0, LMI upd sent  0
  LMI DLCI 1023  LMI type is CISCO  frame relay DTE
  FR SVC disabled, LAPF state down
  Broadcast queue 0/64, broadcasts sent/dropped 8/0, interface
broadcasts 5
  Last input 00:00:02, output 00:00:02, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     38756 packets input, 5695381 bytes, 0 no buffer
     Received 24172 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0
abort
     38777 packets output, 2164927 bytes, 0 underruns
     0 output errors, 0 collisions, 6069 interface resets
     0 output buffer failures, 0 output buffers swapped out
     510 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Действие 2 Проверьте тип сигнализации LMI с помощью команды **show frame-relay lmi**. Выходные данные команды должны выглядеть следующим образом:

```
RouterA#show frame-relay lmi
LMI Statistics for interface Serial0/0/0 (Frame Relay DTE) LMI
TYPE = CISCO
  Invalid Unnumbered info 0             Invalid Prot Disc 0
  Invalid dummy Call Ref 0              Invalid Msg Type 0
  Invalid Status Message 0              Invalid Lock Shift 0
  Invalid Information ID 0              Invalid Report IE Len 0
  Invalid Report Request 0              Invalid Keep IE Len 0
  Num Status Enq. Sent 18               Num Status msgs Rcvd 19
  Num Update Status Rcvd 0              Num Status Timeouts 0
```

Действие 3 Проверьте состояние PVC с помощью команды **show frame-relay lmi**. Выходные данные команды должны выглядеть следующим образом:

```
RouterA#show frame-relay pvc
PVC Statistics for interface Serial0/0/0 (Frame Relay DTE)

DLCI = 100, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE
= Serial0/0/0

  input pkts 28            output pkts 10           in bytes
8398
  out bytes 1198           dropped pkts 0           in FECN
pkts 0
  in BECN pkts 0           out FECN pkts 0          out BECN
pkts 0
  in DE pkts 0             out DE pkts 0
  out bcast pkts 10        out bcast bytes 1198
  pvc create time 00:03:46, last time pvc status changed
00:03:47
```

Действие 4 Убедитесь, что таблица привязок Frame Relay содержит путь к центральному маршрутизатору с помощью команды **show frame-relay map**. Выходные данные команды должны выглядеть следующим образом:

```
RouterA#show frame-relay map
Serial0/0/0 (up): ip 10.140.1.1 dlci 100(0x64,0x1840),
dynamic,
              broadcast, status defined, active
```

Действие 5 Отправьте эхо-запрос в последовательный интерфейс центрального маршрутизатора, который напрямую подключен к маршрутизатору рабочей группы. Используйте адрес, указанный в таблице подсказок для этого упражнения.

Действие 6 Отправьте эхо-запрос на TFTP-сервер по адресу 10.1.1.1.

Примечание. Все эхо-запросы должны быть обработаны успешно.

Действие 7 Переходите к задаче 3.

Проверка упражнения

Задание считается выполненным, если достигнут следующий результат:

- вы ввели команды **show** и отправили эхо-запрос в центральный маршрутизатор (и успешно получили эхо-ответ), чтобы проверить конфигурацию Frame Relay на маршрутизаторе рабочей группы.

Задача 3: использование команды debug frame-relay lmi для просмотра операций обмена LMI

Протокол LMI используется для передачи информации между периферийными устройствами Frame Relay, такими как маршрутизаторы и коммутаторы Frame Relay. При устранении неполадок может быть полезно узнать, переданы ли обновления LMI между коммутатором и маршрутизатором. В этой задаче вам необходимо настроить команду **debug frame-relay lmi** и интерпретировать ее выходные данные.

Процедура упражнения

Выполните следующие действия на маршрутизаторе рабочей группы, чтобы вывести сведения об операциях обмена LMI.

Действие 1 Выведите сведения об обмене кадрами состояния LMI, включая данные протокола Inverse ARP, с помощью команды **debug frame-relay lmi**. Выходные данные команды должны выглядеть следующим образом:

```
RouterA#debug frame lmi
Frame Relay LMI debugging is on
Displaying all Frame Relay LMI data
RouterA#
1w2d: Serial0/0/0(out): StEnq, myseq 140, yourseen 139, DTE up
1w2d: datagramstart = 0xE008EC, datagramsize = 13
1w2d: FR encap = 0xFCF10309
1w2d: 00 75 01 01 01 03 02 8C 8B
1w2d:
1w2d: Serial0/0/0(in): Status, myseq 140
1w2d: RT IE 1, length 1, type 1
1w2d: KA IE 3, length 2, yourseq 140, myseq 140
1w2d: Serial0/0/0(out): StEnq, myseq 141, yourseen 140, DTE up
1w2d: datagramstart = 0xE008EC, datagramsize = 13
1w2d: FR encap = 0xFCF10309
1w2d: 00 75 01 01 01 03 02 8D 8C
1w2d:
1w2d: Serial0/0/0(in): Status, myseq 141
1w2d: RT IE 1, length 1, type 1
1w2d: KA IE 3, length 2, yourseq 141, myseq 141
1w2d: Serial0/0/0(out): StEnq, myseq 142, yourseen 141, DTE up
1w2d: datagramstart = 0xE008EC, datagramsize = 13
1w2d: FR encap = 0xFCF10309
1w2d: 00 75 01 01 00 03 02 8E 8D
1w2d:
1w2d: Serial0/0/0(in): Status, myseq 142
1w2d: RT IE 1, length 1, type 0
1w2d: KA IE 3, length 2, yourseq 142, myseq 142
1w2d: PVC IE 0x7 , length 0x6 , dlci 100, status 0x2 , bw 0
1w2d: Serial0/0/0(out): StEnq, myseq 143, yourseen 142, DTE up
1w2d: datagramstart = 0xE008EC, datagramsize = 13
1w2d: FR encap = 0xFCF10309
1w2d: 00 75 01 01 01 03 02 8F 8E
```

Действие 2 Отключите отладку.

Действие 3 Переходите к задаче 4.

Проверка упражнения

Задание считается выполненным, если достигнут следующий результат:

- вы вывели выходные данные команды **debug frame-relay lmi**.

Задача 4: настройка и проверка субинтерфейсов Frame Relay

Часто для решения проблем горизонта разделения возникает необходимость в использовании протоколов маршрутизации. Один из способов решения проблем горизонта разделения — внедрение нескольких логических интерфейсов на одном физическом интерфейсе. Эти логические интерфейсы также называются субинтерфейсами. В этой задаче вам необходимо настроить субинтерфейс, связанный с заданным идентификатором DLCI (методика адресации Frame Relay уровня 2).

Процедура упражнения

Действие 1 Войдите в режим конфигурации первого последовательного интерфейса маршрутизатора рабочей группы (S0/0/0) и отключите его с помощью команды **shutdown.**

Действие 2 Удалите IP-адрес первого последовательного интерфейса.

Действие 3 Введите команду **show run interface s0/0/0**. Какие команды были удалены из интерфейса при удалении IP-адреса?

Действие 4 Активируйте режим конфигурации для первого последовательного интерфейса. Субинтерфейс должен иметь тип "точка-точка", тип LMI будет задан с помощью функции автоопределения.

Действие 5 Назначьте субинтерфейсу IP-адрес, который был задан для первого физического интерфейса (S0/0/0). Используйте адрес, указанный в таблице подсказок для этого упражнения.

Действие 6 На субинтерфейсе назначьте локальный идентификатор DLCI, определяющий подключение PVC к центральному маршрутизатору. Номера DLCI указаны в таблице подсказок для этого упражнения.

Действие 7 На субинтерфейсе настройте аутентификацию EIGRP с использование цепи ключей **icndchain**.

Действие 8 Включите первый физический последовательный интерфейс (S0/0/0) с помощью команды **no shutdown**.

Действие 9 Проверьте конфигурацию с помощью команд **show running-config interface s0/0/0** и **show running-config interface s0/0/0.1**. Выходные данные команды должны выглядеть следующим образом:

```
RouterA#show running-config interface s0/0/0
Building configuration...

Current configuration:
!
interface Serial0/0/0
 no ip address
 no ip directed-broadcast
 encapsulation frame-relay
 no ip mroute-cache
 no fair-queue
end

RouterA#show running-config interface s0/0/0.1
Building configuration...

Current configuration:
!
interface Serial0/0/0.1 point-to-point
 ip address 10.140.12.2 255.255.255.0
 no ip directed-broadcast
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 icndchain
 frame-relay interface-dlci 230
end
```

Действие 10 Отправьте эхо-запрос на TFTP-сервер, чтобы проверить подключение.

Действие 11 Сохраните конфигурацию в NVRAM;

Действие 12 Сообщите инструктору, что вы выполнили упражнение.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- вы настроили Frame Relay на последовательном субинтерфейсе;
- эхо-запрос, отправленный в центральный коммутатор через подключение Frame Relay для проверки подключения, обработан успешно.

Лабораторная работа 8-2: устранение неполадок в глобальных сетях на базе Frame Relay

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

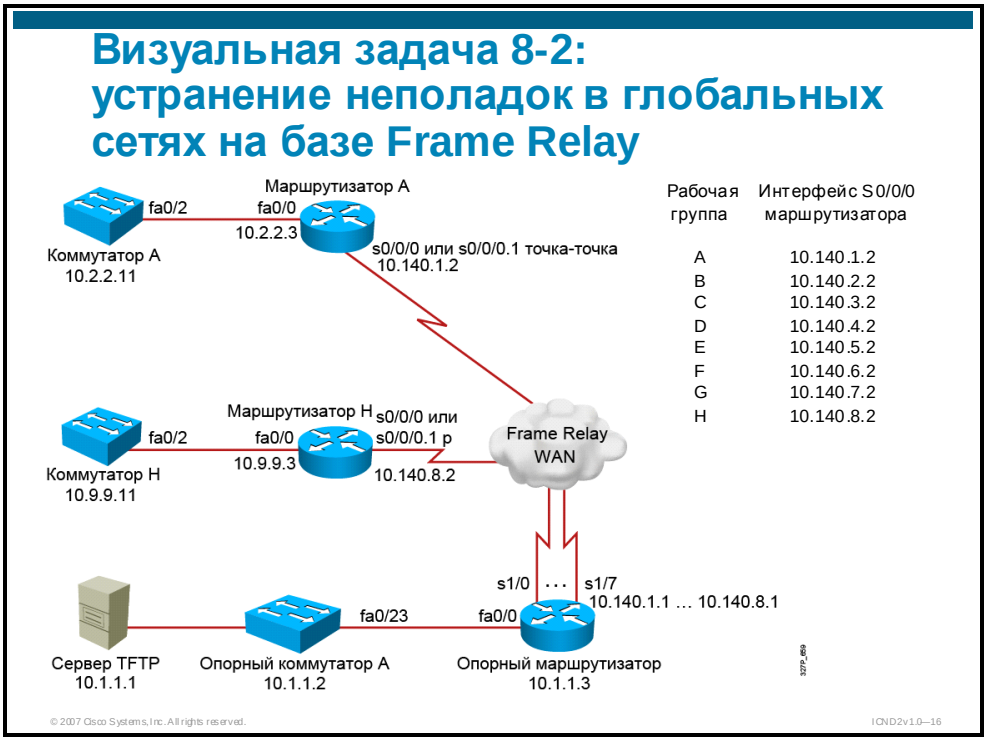
Задачи упражнения

В этом упражнении вам необходимо воспользоваться инструкциями по устранению неполадок, рассмотренными в соответствующем модуле, чтобы собрать сведения о симптомах, а затем изолировать и устранить проблемы, которые часто встречаются в сетях Frame Relay. После выполнения этого упражнения вы должны быть готовы к следующим задачам:

- обнаружение проблем подключения Frame Relay, определение и устранение проблем сетевых подключений в соответствии с инструкциями по устранению неполадок.

Визуальная задача

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 локальной лаборатории или ПК с Интернет-подключением и доступом к удаленной лаборатории.
- Терминальный сервер, подключенный к консольному порту всех лабораторных устройств (при использовании удаленной лаборатории).
- Рабочая группа ICND, назначенная инструктором.

Список команд

В таблице приводится описание команд, используемых в упражнении. Команды перечислены в алфавитном порядке, что позволит легко найти нужные сведения. Если во время упражнения вам потребуется помощь по командам конфигурации, воспользуйтесь этим списком.

Команды Frame Relay

Команда	Описание
debug frame relay lmi	Отображает данные отладки для сигнализации Frame Relay LMI.
show frame-relay lmi	Отображает данные LMI.
show frame-relay map	Отображает данные маршрутов Frame Relay.
show frame-relay pvc	Отображает статистику трафика PVC.
show interfaces	Отображает данные по интерфейсу.

Подсказки

Для упражнений этой лабораторной работы доступны следующие подсказки. В таблице перечислены IP-адреса, используемые в этой лабораторной работе.

Рабочая группа	Сеть VLAN 1 интерфейса коммутатора (Switch*X*)	Интерфей с Fa0/0 маршрути-затора (Router*X*)	Интерфейс S0/0/0 маршрути-затора (Router*X*)	Локальный идентификатор DLCI, определяющий канал PVC к центральным устройствам	Последователь ный интерфейс центрального маршрути-затора (Центральный маршрути-затор)
A	10.2.2.11/24	10.2.2.3/24	10.140.1.2/24	100	10.140.1.1/24
B	10.3.3.11/24	10.3.3.3/24	10.140.2.2/24	110	10.140.2.1/24
C	10.4.4.11/24	10.4.4.3/24	10.140.3.2/24	120	10.140.3.1/24
D	10.5.5.11/24	10.5.5.3/24	10.140.4.2/24	130	10.140.4.1/24
E	10.6.6.11/24	10.6.6.3/24	10.140.5.2/24	140	10.140.5.1/24
F	10.7.7.11/24	10.7.7.3/24	10.140.6.2/24	150	10.140.6.1/24
G	10.8.8.11/24	10.8.8.3/24	10.140.7.2/24	160	10.140.7.1/24
H	10.9.9.11/24	10.9.9.3/24	10.140.8.2/24	170	10.140.8.1/24

Используйте эту таблицу для документирования процесса устранения неполадок.

Действия по устранению неполадок

Команды для сбора данных о симптомах	Изоляция проблемы	Команда для устранения проблемы
Пример:		
ping 172.16.2.2	отказ	-----
show ip interface brief	интерфейс Fa0/1 отключен администратором	**no shutdown**
ping 172.16.2.2	повторный отказ	-----
show interface Fa0/1	неверный ip-адрес	**ip address** 192.168.1.2
ping 172.16.2.2	успешно	

Задача 1: обновление конфигураций рабочей группы.

В этой задаче вам необходимо загрузить новую дополнительную конфигурацию на маршрутизатор рабочей группы с TFTP-сервера. Однако дополнительная конфигурация, которую вам следует загрузить, содержит ошибки, которые приведут к потере подключения с другими сегментами сети. Вам необходимо изолировать и устранить проблему.

Процедура упражнения

Выполните следующие действия.

Действие 1 Проверьте соединение с TFTP-сервером. Отправьте эхо-запрос на TFTP-сервер (10.1.1.1) с маршрутизатора рабочей группы.

Примечание. Если эхо-запрос обрабатывается неудачно, обратитесь к инструктору.

Действие 2 Загрузите дополнительную конфигурацию с TFTP-сервера в работающую конфигурацию маршрутизатора рабочей группы. Имя файла, который необходимо загрузить: i2-wg_**ro**-config-lab8-2.txt.

Действие 3 Введите команду **exit** в привилегированном приглашении EXEC и убедитесь, что баннер маршрутизатора выглядит следующим образом:

********** wg_ro-config-lab8-2 **********

Действие 4 Отправьте эхо-запрос на TFTP-сервер с маршрутизатора рабочей группы. Был ли эхо-запрос обработан успешно?

Действие 5 Проверьте таблицу маршрутизации маршрутизатора рабочей группы. Проверьте отношения соседства EIGRP. Что вы обнаружили?

Действие 6 Проверьте состояние последовательного интерфейса Frame Relay. Что вы обнаружили?

Действие 7 Не используя команду **show run**, соберите сведения о симптомах, а затем изолируйте и устраните проблему с помощью инструкций по устранению неполадок и команд, рассмотренных в соответствующем модуле. Во время устранения неполадок вы можете воспользоваться таблицей подсказок на предыдущей странице.

Действие 8 Отправьте эхо-запрос в TFTP-сервер (10.1.1.1) с маршрутизатора рабочей группы, чтобы подтвердить устранение проблемы.

Действие 9 Сохраните работающую конфигурацию в NVRAM.

Проверка упражнения

Задание считается выполненным, если достигнуты следующие результаты:

- восстановлено подключение Frame Relay к маршрутизатором, подключенным напрямую;
- таблица маршрутизации маршрутизатора рабочей группы заполнена маршрутами, полученными от центрального маршрутизатора через протокол EIGRP;
- сетевое подключение к TFTP-серверу восстановлено, эхо-запрос, отправленный на этот сервер, обрабатывается успешно.

Ключ к лабораторным работам

Ключ к упражнению 1-1: внедрение малой сети (лабораторная работа для повторения пройденного)

Конфигурация коммутатора рабочей группы

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 $1$DbHt$Zq1t4P2kmfMGUeZSRRy0g0
!
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
 description To RouterX Fa0/0
 switchport mode access
 switchport port-security
 switchport port-security mac-address xxxx.xxxx.xxxx
!
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
 description Connected to CoreSwitchA
 speed 100
 duplex full
!
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 10.1.1.X 255.255.255.0
 no ip route-cache
!
ip default-gateway 10.1.1.3
ip http server
ip http secure-server
!
control-plane
!
banner motd ^C
Authorized access only.  Unauthorized users disconnect.^C
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password sanjose
 login
line vty 5 15
 no login
!
end
```

Конфигурация маршрутизатора рабочей группы

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 $1$HNdR$hOG1GhzoNoHMEgZQU21mo1
!
no aaa new-model
!
!
ip cef
!
!
!
!
voice-card 0
 no dspfarm
!
interface FastEthernet0/0
 description To SwitchX Fa0/2
 ip address 10.1.1.X 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
!
interface Serial0/0/1
 no ip address
 shutdown
!
!
!
ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
banner motd ^C
Authorized access only.  Unauthorized users disconnect.^C
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password sanjose
 login
!
scheduler allocate 20000 1000
!
end
```


Ключ к упражнению 2-1: настройка расширенных коммутируемых сетей

Конфигурация коммутатора рабочей группы

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 $1$.9i2$TbVkDQfzCgf/CeFNEKMm9/
!
no aaa new-model
vtp domain ICND
vtp mode transparent
ip subnet-zero
!
no file verify auto
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan X0 priority 24576
spanning-tree vlan X0 priority 28672
!
vlan internal allocation policy ascending
!
vlan X,X0,X0
!
interface FastEthernet0/1
!
interface FastEthernet0/2
 description To RouterX Fa0/0
 spanning-tree portfast
 switchport access vlan X
 switchport mode access
 switchport port-security
 switchport port-security mac-address xxxx.xxxx.xxxx
!
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
 description port connected to CoreSwitchA
 switchport mode trunk
 speed 100
 duplex full
!
```

```
interface FastEthernet0/12
 description port connected to CoreSwitchB
 switchport mode trunk
 speed 100
 duplex full
!
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
 description Management VLAN interface
 ip address 10.1.1.X 255.255.255.0
 no ip route-cache
!
ip default-gateway 10.1.1.3
ip http server
ip http secure-server
!
control-plane
!
banner motd ^C
Authorized Access Only!
^C
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password sanjose
 login
line vty 5 15
 no login
!
end
```

Конфигурация маршрутизатора рабочей группы

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 $1$HNdR$hOG1GhzoNoHMEgZQU21mo1
!
no aaa new-model
!
!
ip cef
!
!
!
!
voice-card 0
 no dspfarm
!
interface FastEthernet0/0
 description To SwitchX Fa0/2
 ip address 10.X.X.12 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
!
interface Serial0/0/1
 no ip address
 shutdown
!
ip route 0.0.0.0 0.0.0.0 10.X.X.3
!
!
ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
banner motd ^C
Authorized access only.  Unauthorized users disconnect.^C
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password sanjose
 login
!
scheduler allocate 20000 1000
```

```
!
```

Ключ к упражнению 2-2: устранение неполадок в коммутируемых сетях

Конфигурация коммутатора рабочей группы

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 $1$.9i2$TbVkDQfzCgf/CeFNEKMm9/
!
no aaa new-model
vtp domain ICND
vtp mode transparent
ip subnet-zero
!
no file verify auto
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan X0 priority 24576
spanning-tree vlan X0 priority 28672
!
vlan internal allocation policy ascending
!
vlan X,X0,X0
!
interface FastEthernet0/1
!
interface FastEthernet0/2
 description To RouterX Fa0/0
 spanning-tree portfast
 switchport access vlan X
 switchport mode access
 switchport port-security
 switchport port-security mac-address xxxx.xxxx.xxxx
!
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
 description port connected to CoreSwitchA
 switchport mode trunk
 speed 100
 duplex full
```



```
!
interface FastEthernet0/12
 description port connected to CoreSwitchB
 switchport mode trunk
 shutdown
 speed 100
 duplex full
!
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
 description Management VLAN interface
 ip address 10.1.1.X 255.255.255.0
 no ip route-cache
!
ip default-gateway 10.1.1.3
ip http server
ip http secure-server
!
control-plane
!
banner motd ^C


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


                  wg_sw-config-lab2-2

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



^C
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password sanjose
```

```
 login
line vty 5 15
 no login
!
end
```

Конфигурация маршрутизатора рабочей группы

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$8qBT$p6X.Rp20jVs3qobVevWSj/
!
no aaa new-model
!
resource policy
!
ip cef
!
voice-card 0
 no dspfarm
!
interface FastEthernet0/0
 description To SwitchX F0/2
 ip address 10.X.X.12 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
!
interface Serial0/0/1
 no ip address
 shutdown
!
ip route 0.0.0.0 0.0.0.0 10.X.X.3
!
!
ip http server
no ip http secure-server
!
control-plane
!
banner motd ^C



**********************************************************************
```



```
**************************************************************************


^C
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password sanjose
 logging synchronous
 login
!
scheduler allocate 20000 1000
!
end
```

Ключ к упражнению 4-1: внедрение OSPF

Конфигурация коммутатора рабочей группы

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 $1$.9i2$TbVkDQfzCgf/CeFNEKMm9/
!
no aaa new-model
vtp domain ICND
vtp mode transparent
ip subnet-zero
!
no file verify auto
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan X0 priority 24576
spanning-tree vlan X0 priority 28672
!
vlan internal allocation policy ascending
!
vlan X,X0,X0
!
interface FastEthernet0/1
!
interface FastEthernet0/2
 description To RouterX Fa0/0
 spanning-tree portfast
 switchport mode access
 switchport port-security
 switchport port-security mac-address xxxx.xxxx.xxxx
!
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
 description port connected to CoreSwitchA
 switchport mode trunk
 shutdown
 speed 100
 duplex full
!
interface FastEthernet0/12
 description port connected to CoreSwitchB
 switchport mode trunk
 shutdown
 speed 100
 duplex full
!
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
 description Management VLAN interface
 ip address 10.X.X.11 255.255.255.0
 no ip route-cache
!
ip default-gateway 10.X.X.3
ip http server
ip http secure-server
!
control-plane
!
```



```
banner motd ^C


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


                    wg_sw-config-lab2-2

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



^C
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password sanjose
 login
line vty 5 15
 no login
!
end
```

Конфигурация маршрутизатора рабочей группы

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$8qBT$p6X.Rp20jVs3qobVevWSj/
!
no aaa new-model
!
resource policy
!
ip cef
!
voice-card 0
 no dspfarm
!
interface Loopback0
 ip address 192.168.X.X 255.255.255.240
!
interface FastEthernet0/0
 description To SwitchX F0/2
 ip address 10.X.X.3 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
```

```
 speed auto
!
interface Serial0/0/0
 bandwidth 64
 ip address 10.140.X.2 255.255.255.0
 ip ospf authentication
 ip ospf authentication-key san-fran
!
interface Serial0/0/1
 bandwidth 64
 ip address 10.XX.XX.X 255.255.255.0
 ip ospf authentication
 ip ospf authentication-key san-fran
!
router ospf 100
 log-adjacency-changes
 network 10.X.X.3 0.0.0.0 area 0
 network 10.XX.XX.X 0.0.0.0 area 0
 network 10.140.X.2 0.0.0.0 area 0
 network 192.168.X.X 0.0.0.0 area 0
!
ip http server
no ip http secure-server
!
control-plane
!
banner motd ^C



**********************************************************************
                           wg_ro-config-lab2-2
**********************************************************************



^C
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password sanjose
 logging synchronous
 login
!
scheduler allocate 20000 1000
!
end
```

Ключ к упражнению 4-2: устранение неполадок OSPF

Конфигурация маршрутизатора рабочей группы

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$8qBT$p6X.Rp20jVs3qobVevWSj/
!
no aaa new-model
!
resource policy
!
ip cef
!
voice-card 0
 no dspfarm
!
interface Loopback0
 ip address 192.168.X.X 255.255.255.240
!
interface FastEthernet0/0
 description To SwitchX F0/2
 ip address 10.X.X.3 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 bandwidth 64
 ip address 10.140.X.2 255.255.255.0
 ip ospf authentication
 ip ospf authentication-key san-fran
!
interface Serial0/0/1
 bandwidth 64
 ip address 10.XX.XX.X 255.255.255.0
 ip ospf authentication
 ip ospf authentication-key san-fran
!
router ospf 100
 log-adjacency-changes
 network 10.X.X.3 0.0.0.0 area 0
 network 10.XX.XX.X 0.0.0.0 area 0
 network 10.140.X.2 0.0.0.0 area 0
 network 192.168.X.X 0.0.0.0 area 0
!
ip http server
no ip http secure-server
!
control-plane
!
banner motd ^C



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

                           wg_ro-config-lab4-2

**********************************************************************
```

```
^C
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password sanjose
 logging synchronous
 login
!
scheduler allocate 20000 1000
!
end
```

Ключ к упражнению 5-1: внедрение EIGRP

Конфигурация маршрутизатора рабочей группы

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$8qBT$p6X.Rp20jVs3qobVevWSj/
!
no aaa new-model
!
resource policy
!
ip cef
!
voice-card 0
 no dspfarm
!
!
key chain icndchain
 key 1
  key-string san-fran
!
interface Loopback0
 ip address 192.168.X.X 255.255.255.240
!
interface FastEthernet0/0
 description To SwitchX F0/2
 ip address 10.X.X.3 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
```



```
interface Serial0/0/0
 bandwidth 64
 ip address 10.140.X.2 255.255.255.0
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 icndchain
 ip ospf authentication
 ip ospf authentication-key san-fran
!
interface Serial0/0/1
 bandwidth 64
 ip address 10.XX.XX.X 255.255.255.0
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 icndchain
 ip ospf authentication
 ip ospf authentication-key san-fran
!
router eigrp 100
 network 10.0.0.0
 network 192.168.X.0
 auto-summary
!
router ospf 100
 log-adjacency-changes
 network 10.X.X.3 0.0.0.0 area 0
 network 10.XX.XX.X 0.0.0.0 area 0
 network 10.140.X.2 0.0.0.0 area 0
 network 192.168.X.X 0.0.0.0 area 0
!
ip http server
no ip http secure-server
!
control-plane
!
banner motd ^C



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

                      wg_ro-config-lab4-2

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



^C
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password sanjose
 logging synchronous
 login
!
scheduler allocate 20000 1000
!
end
```

Ключ к упражнению 5-2: устранение неполадок EIGRP

Конфигурация маршрутизатора рабочей группы

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$8qBT$p6X.Rp20jVs3qobVevWSj/
!
no aaa new-model
!
resource policy
!
ip cef
!
voice-card 0
 no dspfarm
!
!
key chain icndchain
 key 1
  key-string san-fran
!
interface Loopback0
 ip address 192.168.X.X 255.255.255.240
!
interface Loopback1
 ip address 172.16.X.1 255.255.255.0
!
interface FastEthernet0/0
 description To SwitchX F0/2
 ip address 10.X.X.3 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 bandwidth 64
 ip address 10.140.X.2 255.255.255.0
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 icndchain
 ip ospf authentication
 ip ospf authentication-key san-fran
!
interface Serial0/0/1
 bandwidth 64
 ip address 10.XX.XX.X 255.255.255.0
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 icndchain
 ip ospf authentication
 ip ospf authentication-key san-fran
```



```
!
router eigrp 100
 network 10.0.0.0
 network 172.16.0.0
 network 192.168.X.0
 no auto-summary
!
router ospf 100
 log-adjacency-changes
 network 10.X.X.3 0.0.0.0 area 0
 network 10.XX.XX.X 0.0.0.0 area 0
 network 10.140.X.2 0.0.0.0 area 0
 network 192.168.X.X 0.0.0.0 area 0
!
ip http server
no ip http secure-server
!
control-plane
!
banner motd ^C



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

                      wg_ro-config-lab4-2

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



^C
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password sanjose
 logging synchronous
 login
!
scheduler allocate 20000 1000
!
end
```

Ключ к упражнению 6-1: внедрение и устранение неполадок списков контроля доступа (ACL)

Конфигурация маршрутизатора рабочей группы

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$8qBT$p6X.Rp20jVs3qobVevWSj/
!
no aaa new-model
!
resource policy
!
ip cef
!
voice-card 0
 no dspfarm
!
!
key chain icndchain
 key 1
  key-string san-fran
!
interface Loopback0
 ip address 192.168.X.X 255.255.255.240
!
interface Loopback1
 ip address 172.16.X.1 255.255.255.0
!
interface FastEthernet0/0
 description To SwitchX F0/2
 ip address 10.X.X.3 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 bandwidth 64
 ip address 10.140.X.2 255.255.255.0
 ip access-group 101 in
 ip access-group 175 out
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 icndchain
 ip ospf authentication
 ip ospf authentication-key san-fran
!
interface Serial0/0/1
 bandwidth 64
 ip address 10.XX.XX.X 255.255.255.0
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 icndchain
 ip ospf authentication
 ip ospf authentication-key san-fran
 shutdown
!
router eigrp 100
 network 10.0.0.0
 network 172.16.0.0
 network 192.168.X.0
 auto-summary
!
router ospf 100
 log-adjacency-changes
 network 10.X.X.3 0.0.0.0 area 0
 network 10.XX.XX.X 0.0.0.0 area 0
 network 10.140.X.2 0.0.0.0 area 0
 network 192.168.X.X 0.0.0.0 area 0
!
```



```
!
!
ip http server
no ip http secure-server
!
access-list 101 deny   tcp any any eq telnet
access-list 101 permit ip any any
access-list 175 deny   udp any any eq tftp
access-list 175 permit ip any any
!
control-plane
!
banner motd ^C


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

                    wg_ro-config-lab6-1

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



^C
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password sanjose
 logging synchronous
 login
!
scheduler allocate 20000 1000
!
end
```

```
================
```

ИЛИ

```
===============

!
interface Serial0/0/0
 bandwidth 64
 ip address 10.140.X.2 255.255.255.0
 ip access-group KILLTELNET in
 ip access-group 175 out
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 icndchain
 ip ospf authentication
 ip ospf authentication-key san-fran
!
!
ip access-list extended KILLTELNET
 deny   tcp any any eq telnet
 permit ip any any
!
```

Ключ к упражнению 7-1: настройка NAT (преобразование сетевых адресов) и PAT (преобразование адресов портов)

Конфигурация маршрутизатора рабочей группы

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$8qBT$p6X.Rp20jVs3qobVevWSj/
!
no aaa new-model
!
resource policy
!
ip cef
!
voice-card 0
 no dspfarm
!
!
key chain icndchain
 key 1
  key-string san-fran
!
interface Loopback0
 ip address 192.168.X.X 255.255.255.240
!
interface Loopback1
 ip address 172.16.X.1 255.255.255.0
!
interface FastEthernet0/0
 description To SwitchX F0/2
 ip address 10.X.X.3 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 bandwidth 64
 ip address 10.140.X.2 255.255.255.0
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 icndchain
 ip nat outside
 ip virtual-reassembly
 ip ospf authentication
 ip ospf authentication-key san-fran
!
interface Serial0/0/1
```



```
 bandwidth 64
 ip address 10.XX.XX.X 255.255.255.0
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 icndchain
 ip ospf authentication
 ip ospf authentication-key san-fran
 shutdown
!
router eigrp 100
 network 10.0.0.0
 network 172.16.0.0
 network 192.168.X.0
 auto-summary
!
router ospf 100
 log-adjacency-changes
 network 10.X.X.3 0.0.0.0 area 0
 network 10.XX.XX.X 0.0.0.0 area 0
 network 10.140.X.2 0.0.0.0 area 0
 network 192.168.X.X 0.0.0.0 area 0
!
ip http server
no ip http secure-server
ip nat inside source list 1 interface Serial0/0/0 overload
!
access-list 1 permit 10.X.X.0 0.0.0.255
!
control-plane
!
banner motd ^C



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

                        wg_ro-config-lab6-1

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



^C
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password sanjose
 logging synchronous
 login
!
scheduler allocate 20000 1000
!
end
```

Ключ к упражнению 7-2: внедрение IPv6

Конфигурация маршрутизатора рабочей группы

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 $1$HNdR$hOG1GhzoNoHMEgZQU21mo1
!
no aaa new-model
!
!
ip cef
!
!
!
ipv6 unicast-routing
!
voice-card 0
 no dspfarm
!
!
key chain icndchain
 key 1
  key-string san-fran
!
interface Loopback0
 ip address 192.168.X.X 255.255.255.252
!
interface Loopback1
 ip address 172.16.X.1 255.255.255.0
!
interface Loopback2
 ip address 10.XXX.XXX.1 255.255.255.0
 ipv6 address 2001:410:4:8::/64 eui-64
 ipv6 rip cisco enable
!
interface FastEthernet0/0
 description To SwtichX Fa0/2
 ip address 10.X.X.3 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 bandwidth 64
 ip address 10.140.X.2 255.255.255.0
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 icndchain
 ip ospf authentication
 ip ospf authentication-key san-fran
 shutdown
!
interface Serial0/0/1
 bandwidth 64
 ip address 10.XX.XX.X 255.255.255.0
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 icndchain
 ip ospf authentication
 ip ospf authentication-key san-fran
```



```
 ipv6 address 2001:410:4:10::/65 eui-64
 ipv6 rip cisco enable
!
router eigrp 100
 network 10.0.0.0
 network 192.168.X.0
 auto-summary
!
router ospf 100
 log-adjacency-changes
 network 10.X.X.3 0.0.0.0 area 0
 network 10.XX.XX.X 0.0.0.0 area 0
 network 10.140.X.2 0.0.0.0 area 0
 network 192.168.X.XX 0.0.0.0 area 0
!
!
!
ip http server
no ip http secure-server
!
ipv6 router rip cisco
!
control-plane
!
banner motd ^C



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

                        wg_ro-config-lab6-1

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



^C
!
banner motd ^C
Authorized access only.  Unauthorized users disconnect.^C
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password sanjose
 login
!
scheduler allocate 20000 1000
!
end
```

Ключ к упражнению 8-1: создание глобальной сети на базе Frame Relay

Конфигурация маршрутизатора рабочей группы

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$8qBT$p6X.Rp20jVs3qobVevWSj/
!
no aaa new-model
!
resource policy
!
ip cef
!
voice-card 0
 no dspfarm
!
!
key chain icndchain
 key 1
  key-string san-fran
!
interface Loopback0
 ip address 192.168.X.X 255.255.255.240
!
interface Loopback1
 ip address 172.16.X.1 255.255.255.0
!
interface Loopback2
 ip address 10.XXX.XXX.1 255.255.255.0
 ipv6 address 2001:410:4:8::/64 eui-64
 ipv6 rip cisco enable
!
interface FastEthernet0/0
 description To SwitchX F0/2
 ip address 10.X.X.3 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 bandwidth 64
 no ip address
 encapsulation frame-relay
 ip ospf authentication
 ip ospf authentication-key san-fran
!
interface Serial0/0/0.1 point-to-point
 ip address 10.140.X.2 255.255.255.0
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 icndchain
 frame-relay interface-dlci 120
!
interface Serial0/0/1
 bandwidth 64
 ip address 10.XX.XX.X 255.255.255.0
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 icndchain
 ip ospf authentication
 ip ospf authentication-key san-fran
 shutdown
```



```
!
router eigrp 100
 network 10.0.0.0
 network 172.16.0.0
 network 192.168.X.0
 no auto-summary
!
router ospf 100
 log-adjacency-changes
 network 10.X.X.3 0.0.0.0 area 0
 network 10.XX.XX.X 0.0.0.0 area 0
 network 10.140.X.2 0.0.0.0 area 0
 network 192.168.X.X 0.0.0.0 area 0
!

ip http server
no ip http secure-server
!
access-list 1 permit 10.X.X.0 0.0.0.255
!
control-plane
!
banner motd ^C



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

                      wg_ro-config-lab6-1

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



^C
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password sanjose
 logging synchronous
 login
!
scheduler allocate 20000 1000
!
end
```

Ключ к упражнению 8-2: устранение неполадок в глобальных сетях на базе Frame Relay

Конфигурация маршрутизатора рабочей группы

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$8qBT$p6X.Rp20jVs3qobVevWSj/
!
no aaa new-model
!
resource policy
!
ip cef
!
voice-card 0
 no dspfarm
!
!
key chain icndchain
 key 1
  key-string san-fran
!
interface Loopback0
 ip address 192.168.X.X 255.255.255.240
!
interface Loopback1
 ip address 172.16.X.1 255.255.255.0
!
interface Loopback2
 ip address 10.XXX.XXX.1 255.255.255.0
 ipv6 address 2001:410:4:8::/64 eui-64
 ipv6 rip cisco enable
!
interface FastEthernet0/0
 description To SwitchX F0/2
 ip address 10.X.X.3 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 bandwidth 64
 no ip address
 encapsulation frame-relay IETF
 ip ospf authentication
 ip ospf authentication-key san-fran
!
interface Serial0/0/0.1 point-to-point
 ip address 10.140.X.2 255.255.255.0
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 icndchain
 frame-relay interface-dlci 120
!
interface Serial0/0/1
 bandwidth 64
 ip address 10.XX.XX.X 255.255.255.0
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 icndchain
 ip ospf authentication
 ip ospf authentication-key san-fran
 shutdown
!
router eigrp 100
 network 10.0.0.0
```



```
 network 172.16.0.0
 network 192.168.X.0
 no auto-summary
!
router ospf 100
 log-adjacency-changes
 network 10.X.X.3 0.0.0.0 area 0
 network 10.XX.XX.X 0.0.0.0 area 0
 network 10.140.X.2 0.0.0.0 area 0
 network 192.168.X.X 0.0.0.0 area 0
!

ip http server
no ip http secure-server
!
access-list 1 permit 20.4.4.0 0.0.0.255
!
control-plane
!
banner motd ^C



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

                        wg_ro-config-lab8-2

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



^C
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password sanjose
 logging synchronous
 login
!
scheduler allocate 20000 1000
!
end
```

