ГЛАВА 9

Реализация виртуальных локальных сетей

Коммутаторы Ethernet получают фреймы Ethernet, принимают решение, а затем перенаправляют (коммутируют) полученные фреймы. Эта базовая логика основана на MAC-адресах интерфейсов, на которые поступают фреймы и на которые коммутатор перенаправляет их. На решение коммутатора о перенаправлении фреймов оказывают влияние многие факторы, но из всех рассматриваемых в данной книге наибольшее влияние оказывают *виртуальные локальные сети* (VLAN).

Эта глава посвящена концепции VLAN и их настройке. В первом разделе обсуждаются основные концепции, включая влияние сетей VLAN на отдельный коммутатор, использование магистрального соединения для создания сетей VLAN, охватывающих несколько коммутаторов, и перенаправление трафика между сетями VLAN с использованием маршрутизатора. Во втором разделе демонстрируется настройка сетей VLAN и их магистральных каналов, включая статическое присвоение интерфейсов.

В этой главе рассматриваются следующие экзаменационные темы

Работа сетей передачи данных IP

Передача данных между двумя хостами по сети.

Технологии коммутации сетей LAN

Базовые концепции коммутации и работа коммутаторов Cisco.

- Широковещательные домены.
- Таблица CAM.

Создание логических сегментов сети VLAN и необходимость маршрутизации между ними.

Принцип сегментации сети и базовые концепции управления трафиком.

Настройка и проверка сети VLAN.

Настройка и проверка магистрального соединения на коммутаторах Cisco.

- Протокол DTP.

Поиск и устранение неисправностей

Поиск неисправностей и решение проблем сетей VLAN.

- Идентификация настроенных сетей VLAN.
- Исправление принадлежности порта.
- Настройка IP-адреса.

Поиск неисправностей и решение проблем магистрального соединения на коммутаторах Cisco.

- Исправление состояния магистрального канала.
- Исправление конфигурации инкапсуляции.
- Исправление разрешенных VLAN.

Основные темы

Концепции виртуальных локальных сетей

Прежде чем приступить к изучению VLAN, сначала имеет смысл выяснить, что это такое. С одной стороны, локальная сеть включает все пользовательские устройства, серверы, коммутаторы, маршрутизаторы, кабели и беспроводные точки доступа в одной области. Но для концепции виртуальной сети LAN больше подходит другое определение локальной сети:

Локальная сеть (LAN) объединяет все устройства в том же широковещательном домене.

Широковещательный домен объединяет все устройства, подключенные к сети LAN, таким образом, что когда любое из устройств посылает широковещательный фрейм, все остальные устройства получают его копию. Таким образом, с другой стороны, локальная сеть и широковещательный домен — это одно и то же.

Без виртуальных сетей коммутатор полагает, что все его интерфейсы находятся в том же широковещательном домене. Таким образом, когда на один порт коммутатора поступает широковещательный фрейм, он перенаправляет его на все остальные порты. Согласно этой логике, чтобы создать два разных широковещательных домена (или LAN), необходимо купить два разных коммутатора Ethernet (рис. 9.1).

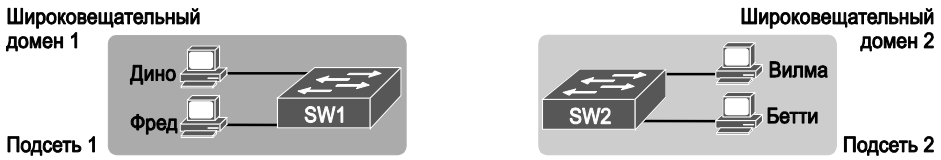

Рис. 9.1. Создание двух широковещательных доменов с двумя физическими коммутаторами и без сетей VLAN

При поддержке VLAN тех же целей (создание двух широковещательных доменов) может достичь один коммутатор, как показано на рис. 9.1. Коммутатор VLAN может настроить часть интерфейсов на один широковещательный домен, а часть на другой, создав в результате два широковещательных домена. Эти созданные коммутатором индивидуальные широковещательные домены и являются *виртуальными локальными сетями* (virtual LAN — VLAN).

На рис. 9.2 представлен один коммутатор, создающий две сети VLAN, его порты для каждой из них являются полностью независимыми. Коммутатор никогда не перенаправит фрейм, посланный компьютером Дино (VLAN 1), через порты на компьютер Вилмы или Бетти (VLAN 2).

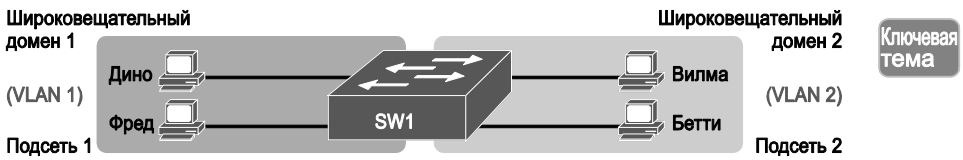

Рис. 9.2. Создание двух широковещательных доменов с использованием одного коммутатора и сети VLAN

Проект территориальной локальной сети, в котором больше сетей VLAN с меньшим количеством устройств в каждой, зачастую имеет больше преимуществ. Например, широковещательное сообщение, посланное одним хостом VLAN, будет получено и обработано всеми другими хостами данной VLAN, но не хостами в других VLAN. Ограничение количества хостов, получающих каждый широковещательный фрейм, снижает количество хостов, впустую тратящих ресурсы на обработку ненужных им широковещательных сообщений. Это снижает также риск нарушения безопасности, поскольку фреймы, посланные любым хостом, поступают на меньшее количество хостов. И это лишь некоторые из причин разделения хостов на отдельные сети VLAN. Ниже приведен список наиболее распространенных причин создания меньших широковещательных доменов (сетей VLAN):

Ключевая тема **Причины применения сетей VLAN**

- Сокращение дополнительных затрат процессоров всех устройств за счет сокращения количества устройств, получающих каждый широковещательный фрейм.
- Улучшение защиты за счет сокращения количества хостов, получающих копии фреймов при их лавинной рассылке коммутатором (широковещание, групповая передача и одноадресатные фреймы с неизвестным получателем).
- Улучшение защиты хостов, пересылающих важные данные, за счет их помещения в отдельную сеть VLAN.
- Возможность более гибкого объединения пользователей в группы (например, по отделам) вместо физического разделения по местоположению.
- Упрощение поиска проблемы в сети, поскольку большинство проблем локализуется в области набора устройств, формирующих широковещательный домен.
- Сокращение дополнительных затрат на работу протокола распределенного связующего дерева (STP) за счет ограничения VLAN одним коммутатором доступа.

Причины применения сетей VLAN подробно не рассматриваются в этой главе, достаточно лишь знать, что они используются в большинстве корпоративных сетей. В оставшейся части данной главы рассматривается механика работы сетей VLAN на нескольких коммутаторах Cisco, включая необходимую настройку. Для этого в следующем разделе исследуется магистральное соединение VLAN — обязательное средство при установке сети VLAN, содержащей несколько коммутаторов LAN.

Создание сети VLAN при нескольких коммутаторах и магистральном соединении

Настройка сети VLAN с одним коммутатором требует немного усилий: достаточно настроить каждый порт так, чтобы указать ему номер VLAN, к которой он принадлежит. При наличии нескольких коммутаторов следует учитывать дополнительные концепции перенаправления трафика между ними.

Когда сети VLAN используются в сетях с несколькими соединенными между собой коммутаторами, на каналах связи между ними применяется *магистральное со-*

единение VLAN (VLAN trunking). Магистральное соединение VLAN подразумевает использование коммутаторами процесса *назначения тегов VLAN* (VLAN tagging), когда передающий коммутатор добавляет к фрейму другой заголовок перед его передачей по магистральному каналу. Этот дополнительный заголовок включает поле *идентификатора VLAN* (VLAN ID), позволяющего передающему коммутатору ассоциировать фрейм с конкретной сетью VLAN, а получающему коммутатору узнать, к какой именно VLAN принадлежит данный фрейм.

На рис. 9.3 приведен пример двух сетей VLAN с несколькими коммутаторами, но без магистрального соединения. Здесь используются две сети VLAN: VLAN 10 и VLAN 20. Каждой сети VLAN присвоено по два порта на каждом коммутаторе, поэтому каждая сеть VLAN существует в обоих коммутаторах. Для перенаправления трафика сети VLAN 10 между двумя коммутаторами проект подразумевает наличие канала связи между ними, который полностью находится в сети VLAN 10. Аналогично для обеспечения трафика сети VLAN 20 между коммутаторами расположен второй канал связи, уже полностью расположенный в сети VLAN 20.

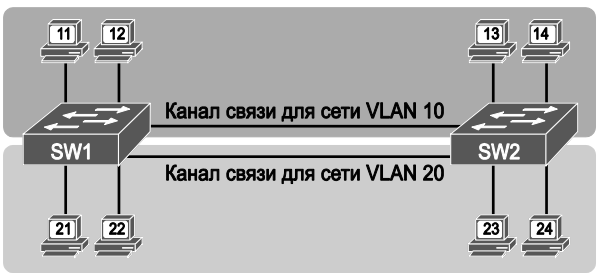

Рис. 9.3. Сети VLAN при наличии нескольких коммутаторов, но без магистрального соединения

Проект, показанный на рис. 9.3, работает прекрасно. Компьютер PC11 (в сети VLAN 10) вполне может послать фрейм компьютеру PC14. Фрейм попадет на коммутатор SW1, а затем по каналу связи (для VLAN 10) на коммутатор SW2. Но хотя этот проект работает, его масштабирование не так просто. Для поддержки каждой сети VLAN требуется отдельный физический канал связи между коммутаторами. Если бы понадобилось 10 или 20 сетей VLAN, то между коммутаторами пришлось бы проложить 10 или 20 каналов связи и использовать для них 10 или 20 портов на каждом коммутаторе.

Концепции назначения тегов VLAN

Магистральное соединение VLAN создает между коммутаторами один канал связи, способный поддерживать столько сетей VLAN, сколько необходимо. Коммутаторы рассматривают магистральный канал как часть всех VLAN. Тем не менее трафик в магистральном канале VLAN остается раздельным, и фреймы VLAN 10 никоим образом не попадут на устройства VLAN 20 (и наоборот), поскольку, пересекая магистральный канал, каждый фрейм идентифицирован номером VLAN. На рис. 9.4 приведена концепция сети с одним физическим каналом связи между двумя коммутаторами.

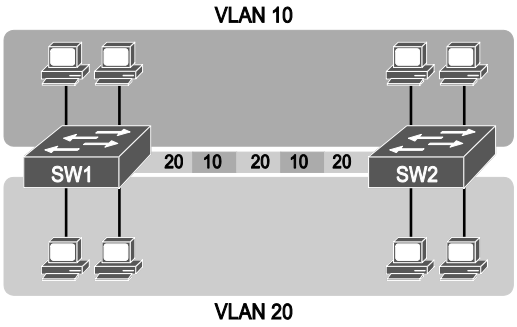

Рис. 9.4. Сети VLAN с несколькими коммутаторами и магистральным соединением

Магистральное соединение позволяет коммутаторам передавать фреймы нескольких сетей VLAN по одному физическому каналу за счет добавления небольшого заголовка к фрейму Ethernet. Пример на рис. 9.5 демонстрирует передачу компьютером PC11 широковещательного фрейма на интерфейсе Fa0/1 (этап 1). Для лавинной рассылки коммутатор SW1 должен перенаправить широковещательный фрейм на коммутатор SW2. Но коммутатор SW1 должен как-то дать знать коммутатору SW2, что фрейм принадлежит сети VLAN 10, чтобы после его получения осуществить лавинную рассылку только в сети VLAN 10, а не VLAN 20. Как показано на этапе 2, перед передачей фрейма коммутатор SW1 добавил к исходному фрейму Ethernet заголовок VLAN, в котором указан идентификатор VLAN (в данном случае VLAN 10).

Ключевая тема

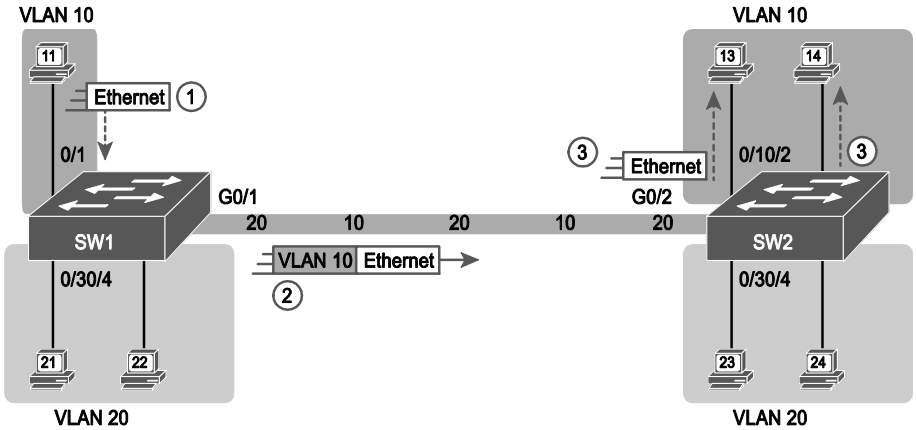

Рис. 9.5. Магистральное соединение VLAN между двумя коммутаторами

Когда коммутатор SW2 получает фрейм, он понимает, что фрейм принадлежит сети VLAN 10. Затем коммутатор SW2 удаляет заголовок VLAN и перенаправляет первоначальный фрейм по интерфейсу к VLAN 10 (этап 3).

Для другого примера рассмотрим случай, когда компьютер PC21 (в сети VLAN 20) посылает широковещательный фрейм. Коммутатор SW1 посылает его через порт Fa0/4 (поскольку этот порт находится в сети VLAN 20) и порт Gi0/1 (поскольку это магистральный канал, а значит, он поддерживает несколько разных сетей VLAN).

Коммутатор SW1 добавляет к фрейму заголовок магистрали, содержащий идентификатор VLAN 20. Выяснив, что фрейм принадлежит сети VLAN 20, коммутатор SW2 удалит магистральный заголовок и перенаправит его только на порты Fa0/3 и Fa0/4, поскольку они находятся в сети VLAN 20, но не на порты Fa0/1 и Fa0/2, так как они находятся в сети VLAN 10.

Протоколы магистралей VLAN 802.1Q и ISL

В последние годы компания Cisco использует два протокола магистральных соединений: *протокол межкоммутаторных соединений* (Inter-Switch Link — ISL) и протокол 802.1Q стандарта IEEE. Компания Cisco использовала протокол ISL задолго до появления протокола 802.1Q частично потому, что IEEE еще не определил стандарт для магистралей VLAN. Несколько лет назад IEEE закончил работу над стандартом 802.1Q, определяющим иной способ создания магистральных соединений. Сейчас протокол 802.1Q стал наиболее популярным протоколом магистральных соединений, и компания Cisco больше не поддерживает стандарт ISL на некоторых более новых моделях коммутаторов LAN, включая 2960, который используется в примерах этой книги.

Хотя оба протокола отмечают каждый фрейм идентификатором VLAN, детали процесса у них разные. Протокол 802.1Q использует дополнительное 4-байтовое поле — заголовок 802.1Q в заголовке Ethernet первоначального фрейма, как показано на рис. 9.6, *сверху*. Что касается полей в заголовке 802.1Q, то поле идентификатора VLAN занимает только 12 битов, но для тем данной книги это не имеет значения. Теоретически это 12-битовое поле способно идентифицировать максимум 2^{12} (4096) сетей VLAN, хотя на практике доступно максимум 4094 значения. (Согласно стандартам 802.1Q и ISL, поле идентификатора VLAN имеет два зарезервированных значения — 0 и 4095.)

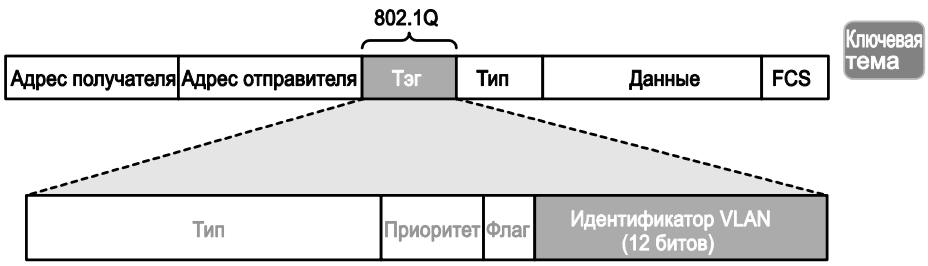

Рис. 9.6. Заголовок магистрального соединения по стандарту 802.1Q

Коммутаторы Cisco разделяют диапазон идентификаторов VLAN (1-4094) на два диапазона: нормальный и расширенный. Все коммутаторы могут использовать нормальный диапазон идентификаторов VLAN со значениями 1–1005, и только некоторые могут использовать расширенный диапазон от 1005 до 4094. Правила использования коммутаторами расширенного диапазона идентификаторов VLAN зависят от конфигурации *протокола создания магистралей VLAN* (VLAN Trunking Protocol — VTP), кратко обсуждаемого ниже.

Для каждого магистрального канала стандарт 802.1Q определяет также один специальный идентификатор VLAN, обозначающий *собственную сеть VLAN* (native

VLAN) (стандартно это VLAN 1). По определению протокол 802.1Q не добавляет заголовок 802.1Q к фреймам в собственной сети VLAN. Когда коммутатор с другой стороны магистрального канала получает фрейм без заголовка 802.1Q, он понимает, что фрейм принадлежит собственной сети VLAN. Из-за этого оба коммутатора должны "договориться", какую сеть VLAN считать собственной.

Согласно стандарту 802.1Q, собственная сеть VLAN обладает некими уникальными функциями: она, например, способна обеспечивать соединения с устройствами, которые не поддерживают магистральное соединение. Например, коммутатор Cisco может быть подключен к коммутатору, который не поддерживает магистральные соединения 802.1Q. Коммутатор Cisco мог бы послать фреймы со значением собственной сети VLAN, т.е. без магистрального заголовка, и другой коммутатор будет понимать их. Концепция собственной сети VLAN позволяет коммутаторам передавать трафик как минимум одной сети VLAN (собственной VLAN), поддерживая некоторые базовые функции, такие как доступность коммутатора по Telnet.

Перенаправление данных между сетями VLAN

При создании территориальной локальной сети, содержащей много сетей VLAN, требуется обеспечить всем устройствам возможность передавать данные на все остальные устройства. Давайте обсудим некоторые из концепций перенаправления данных между сетями VLAN.

В первую очередь это поможет усвоить терминологию коммутаторов LAN. Все функции и логика коммутаторов Ethernet, описанные до сих пор, соответствовали протоколам уровня 2 модели OSI. Например, в главе 6 упоминалось о том, что коммутаторы LAN получают фреймы Ethernet (концепция уровня 2), распознают MAC-адрес получателя (адрес уровня 2) и перенаправляют фрейм Ethernet на другой интерфейс. В этой главе уже упоминалась концепция сетей VLAN как широковещательных доменов, что тоже является концепцией уровня 2.

Хотя некоторые коммутаторы LAN работают так, как описывалось до сих пор, другие коммутаторы LAN обладают куда бо́льшими возможностями. Коммутаторы LAN, передающие данные на основании логики уровня 2, зачастую называют *коммутаторами уровня 2* (Layer 2 switch). Но есть коммутаторы, способные выполнять некоторые функции маршрутизатора, — они используют дополнительную логику, определенную протоколами уровня 3. Эти коммутаторы называют *многоуровневыми коммутаторами* (multilayer switch), или *коммутаторами уровня 3* (Layer 3 switch). Этот раздел начинается с обсуждения перенаправления данных между сетями VLAN коммутаторами уровня 2, а завершается обсуждением применения для этого коммутаторов уровня 3.

Маршрутизация пакетов между сетями VLAN с использованием маршрутизатора

При включении виртуальной локальной сети (VLAN) в проект территориальной локальной сети все устройства сети VLAN должны быть в той же подсети. Согласно той же логике, устройства в разных сетях VLAN должны принадлежать разным подсетям. Например, два компьютера, показанные на рис. 9.7, *слева*, находятся в сети VLAN 10 и в подсети 10. Два компьютера, показанные справа, находятся в другой сети VLAN (20) и в другой подсети (20).

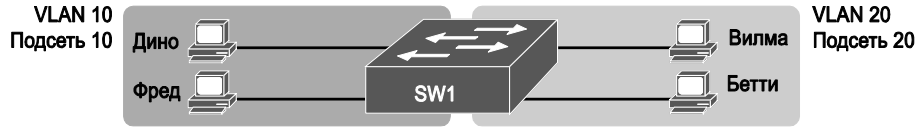

Рис. 9.7. Маршрутизация на коммутаторах между двумя физически отделенными сетями VLAN

ВНИМАНИЕ!

Подсети на рисунке обозначены несколько абстрактно, как “подсеть 10”, чтобы не отвлекаться на номера подсетей. Обратите также внимание на то, что номера подсетей не должны совпадать с номерами сетей VLAN.

Коммутаторы уровня 2 не будут перенаправлять данные между двумя сетями VLAN. Фактически одна из задач сетей VLAN заключается в том, чтобы отделить трафик одной виртуальной сети от другой и предотвратить попадание фреймов из одной сети VLAN в другую. Например, если компьютер Дино (VLAN 10) пошлет любой фрейм Ethernet на коммутатор SW1 уровня 2, то коммутатор не станет перенаправлять его на компьютеры справа, находящиеся в сети VLAN 20.

Сеть в целом должна обеспечивать передачу трафика, входящего и исходящего из каждой сети VLAN, даже при том, что коммутатор уровня 2 не перенаправляет фреймы за пределы виртуальной сети. Задачу перенаправления данных между сетями VLAN выполняет маршрутизатор. Вместо коммутации фреймов Ethernet уровня 2 между двумя сетями VLAN сеть должна перенаправлять между этими двумя подсетями пакеты уровня 3.

Поскольку в предыдущем абзаце встретилась довольно специфическая формулировка, связанная с уровнями 2 и 3, уделим минуту этой теме. Логика уровня 2 не позволяет коммутатору уровня 2 перенаправлять фреймы Ethernet уровня 2 (L2PDU) между сетями VLAN. Однако маршрутизаторы могут перенаправить пакеты уровня 3 (L3PDU) между подсетями, как и положено.

На рис. 9.8, например, представлен маршрутизатор, способный перенаправлять пакеты между подсетями 10 и 20. На рисунке демонстрируется тот же коммутатор уровня 2, что и на рис. 9.7, с теми же компьютерами и теми же сетями VLAN и подсетями. Но теперь коммутатор подключен к маршрутизатору R1 одним физическим интерфейсом, принадлежащим сети VLAN 10, и вторым, принадлежащим сети VLAN 20. При соединении с каждой подсетью коммутатор уровня 2 вполне может продолжить перенаправлять фреймы в каждой сети VLAN, в то время как маршрутизатор будет решать задачу о направлении пакетов IP между подсетями.

На рис. 9.8 показан пакет IP, передаваемый компьютером Фреда из одной сети VLAN (подсети) на компьютер Бетти, находящийся в другой сети VLAN (подсети). Коммутатор уровня 2 передает два разных фрейма Ethernet уровня 2: один в сети VLAN 10, от компьютера Фреда на интерфейс F0/0 маршрутизатора R1, и другой, в сети VLAN 20, от интерфейса F0/1 маршрутизатора R1 на компьютер Бетти. С точки зрения уровня 3 компьютер Фреда посылает пакет IP на свой стандартный маршрутизатор (R1), он перенаправляет пакет на другой интерфейс (F0/1) в другую подсеть, где располагается компьютер Бетти.

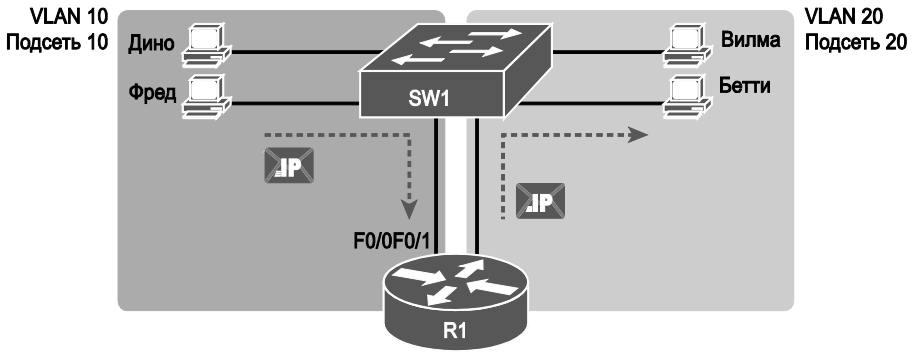

Рис. 9.8. Маршрутизация между двумя сетями VLAN на двух физических интерфейсах

Хотя проект на рис. 9.8 вполне работоспособен, он использует слишком много физических интерфейсов, по одному на каждую VLAN. Намного менее расточительное (и более предпочтительное) решение подразумевает использование магистрального канала VLAN между коммутатором и маршрутизатором. Так, для поддержки всех сетей VLAN достаточно только одного физического канала связи между маршрутизатором и коммутатором. Магистральное соединение возможно между любыми двумя устройствами, способными поддерживать его: между двумя коммутаторами, между маршрутизатором и коммутатором и даже между аппаратными средствами сервера и коммутатором.

На рис. 9.9 представлен концептуально тот же проект, что и на рис. 9.8, с тем же пакетом, следующим от компьютера Фреда к компьютеру Бетти, но теперь маршрутизатор R1 использует магистральное соединение VLAN вместо отдельного канала связи для каждой сети VLAN.

Ключевая тема

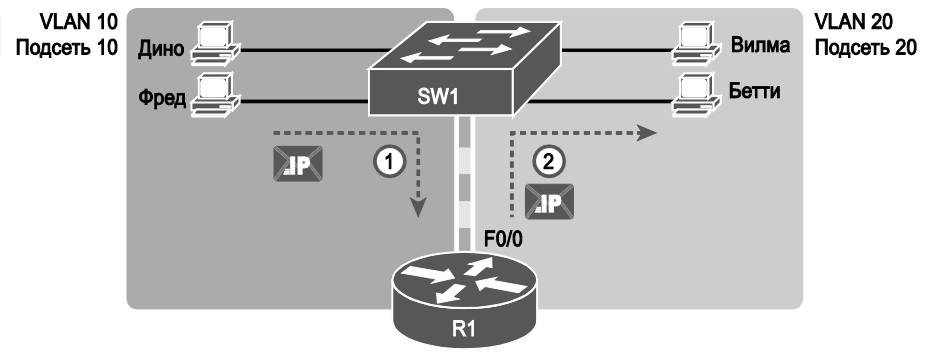

Рис. 9.9. Маршрутизация между двумя сетями VLAN с использованием магистрального канала на маршрутизаторе

ВНИМАНИЕ!

Поскольку у маршрутизатора один физический канал связи, подключенный к коммутатору LAN, такой проект сети иногда вызывают “маршрутизатор на палочке” (router-on-a-stick).

Еще немного терминологии: концепцию на рис. 9.8 и 9.9 иногда упоминают как “маршрутизацию пакетов между сетями VLAN” (routing packets between VLAN). Эту

фразу вполне можно использовать, люди поймут, что имеется в виду. Но для подготовки к экзамену буквально эта фраза неверна, поскольку объединяет маршрутизацию пакетов (концепция уровня 3) и VLAN (концепция уровня 2). Просто "маршрутизация между сетями VLAN" короче, хотя буквально правильно "маршрутизация пакетов уровня 3 между подсетями уровня 3, при сопоставлении каждой из подсетей с различными сетями VLAN уровня 2".

Маршрутизация пакетов коммутаторами уровня 3

У маршрутизации пакетов с использованием физического маршрутизатора (даже при магистральном канале VLAN, как на рис. 9.9) все еще остается одна серьезная проблема: производительность. Физический канал связи налагает ограничение на количество передаваемых битов, а недорогие маршрутизаторы обычно не отличаются высокой мощностью и не могут перенаправлять достаточно много *пакетов за секунду* (packets per second — pps), чтобы поддерживать необходимый объем трафика.

Окончательное решение подразумевает передачу функций маршрутизации аппаратным средствам коммутатора LAN. Производители уже довольно давно начали объединять аппаратные и программные средства коммутаторов уровня 2 с маршрутизаторами уровня 3, выпуская *коммутаторы уровня 3* (они же *многоуровневые коммутаторы*). Коммутаторы уровня 3 могут быть настроены так, чтобы действовать или как только коммутаторы уровня 2, или как коммутаторы уровня 2 с маршрутизаторами уровня 3.

В настоящее время многие средние и крупные корпоративные территориальные локальные сети используют для перенаправления пакетов между подсетями (VLAN) коммутаторы уровня 3.

Концептуально коммутатор уровня 3 работает подобно первоначальным двум устройствам, на базе которых он создан: коммутатора LAN уровня 2 и маршрутизатора уровня 3. Фактически, если понятны концепции перенаправления пакетов на рис. 9.8, при отдельном коммутаторе уровня 2 и маршрутизаторе уровня 3, вы имеете общее представление о работе коммутатора уровня 3, объединяющем все эти функции в одном устройстве. Эта концепция представлена на рис. 9.10, она повторяет многие подробности рис. 9.8, но с дополнительным прямоугольником, демонстрирующим, что один коммутатор уровня 3 выполняет функции коммутатора уровня 2 и маршрутизатора уровня 3.

Эта глава знакомит с основами маршрутизации пакетов IP между сетями VLAN (точнее, между подсетями в сетях VLAN). Конфигурация сетей, использующих внешний маршрутизатор, рассматривается в главе 16, а пока рассмотрим конфигурацию и проверку сетей VLAN и магистральных каналов VLAN.

Конфигурация сетей и магистралей VLAN

Для работы коммутаторам Cisco никакой настройки не требуется. Вполне можно купить коммутатор Cisco, подключить его к соответствующим кабелям, включить, и он заработает. Вам никогда не придется настраивать коммутатор, и он будет прекрасно работать (даже если придется соединять коммутаторы), пока не понадобится несколько сетей VLAN. Но если необходимо использовать несколько сетей VLAN (как в большинстве корпоративных сетей), то некоторая настройка понадобится.

Ключевая тема

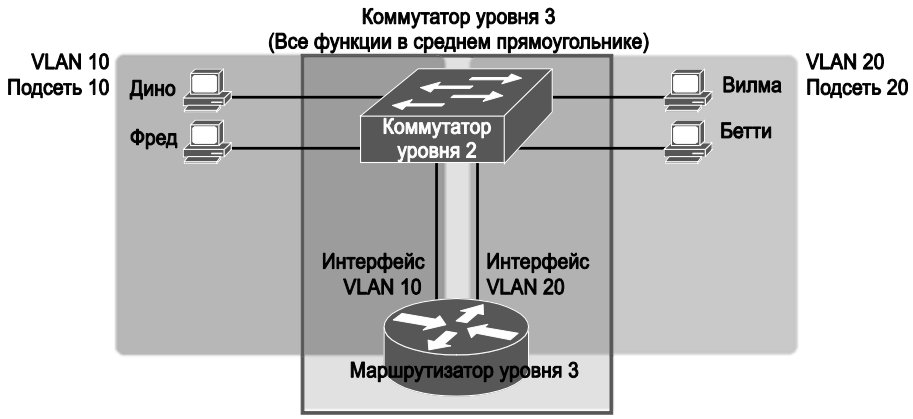

Рис. 9.10. Маршрутизация между сетями VLAN с использованием коммутатора уровня 3

Подробнее конфигурация VLAN рассматривается в двух разделах этой главы. В первом описана настройка интерфейсов доступа, т.е. интерфейсов коммутатора, не используемых для магистральных соединений VLAN. Настройка интерфейсов, используемых для магистральных соединений VLAN, рассматриваются во втором разделе.

Создание сетей VLAN и назначение интерфейсов доступа

В этом разделе показано, как создать сеть VLAN, присвоить ей имя и добавить в нее интерфейсы. Чтобы можно было сосредоточиться на рассмотрении этой темы, в примерах настоящего раздела используется один коммутатор, который не нуждаются в магистрали VLAN.

Чтобы коммутатор Cisco начал перенаправлять фреймы в определенную сеть VLAN, его нужно настроить, указав на существование еще одной сети VLAN. Кроме того, у коммутатора должны быть немагистральные интерфейсы (*интерфейсы доступа* (access interface)), принадлежащие этой сети VLAN, и (или) магистральные каналы, поддерживающие эту VLAN. Этапы настройки интерфейсов доступа приведены ниже, настройка магистрального канала — в соответствующем разделе далее.

Ключевая тема

Последовательность настройки конфигурации VLAN и назначения интерфейсов

Этап 1 Чтобы настроить конфигурацию новой сети VLAN, выполните следующие действия:

A. В режиме настройки конфигурации введите глобальную команду конфигурации `vlan` *`идентификатор_vlan`* для создания сети VLAN и перейдите в режим настройки конфигурации сети VLAN.

B. (Необязательно.) Чтобы присвоить сети VLAN имя, введите подкоманду VLAN `name` *`имя`*. Если этого не сделать, именем VLAN будет `VLAN`*`ZZZZ`*, где *`ZZZZ`* — десятичный идентификатор из четырех цифр

Этап 2 Для каждого интерфейса доступа (интерфейса, принадлежащего не магистральному каналу, а отдельной сети VLAN) выполните следующие действия:

A. Используя команду `interface`, перейдите в режим конфигурации каждого настраиваемого интерфейса.

B. Используя подкоманду интерфейса `switchport access vlan` *`идентификатор_vlan`*, укажите номер сети VLAN, связанной с данным интерфейсом.

C. (Необязательно). Чтобы отключить магистральное соединение на том же интерфейсе и запретить переговоры о создании магистрального канала, используйте подкоманду интерфейса `switchport mode access`.

Хоть этот список и выглядит устрашающе, на самом деле процесс настройки одиночного коммутатора довольно прост. Например, если порты коммутатора следует распределить по трем сетям VLAN (11, 12 и 13), достаточно ввести три команды: `vlan 11`, `vlan 12` и `vlan 13`. Затем для каждого интерфейса введите команду `switchport access vlan 11` (или `12`, или `13`), чтобы присвоить соответствующий интерфейс надлежащей сети VLAN.

Первый пример: полная настройка сети VLAN

В примере 9.1 показан процесс настройки, сводящийся к добавлению новой сети VLAN и назначению интерфейсов доступа к ней. На рис. 9.11 представлена сеть, рассматриваемая в данном примере, с одним коммутатором LAN (SW1) и тремя сетями VLAN (1, 2 и 3), в каждой из которых имеются по два хоста. В этом примере приведены подробные сведения о выполнении двухэтапного процесса настройки сети VLAN 2 и назначения ей интерфейсов; настройка конфигурации сети VLAN 3 рассматривается в следующем примере.

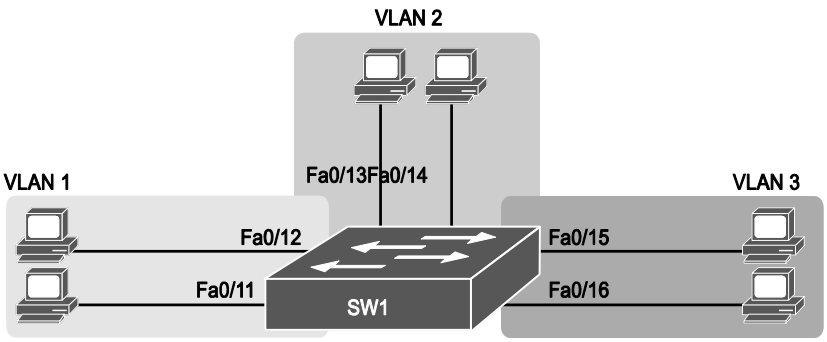

Рис. 9.11. Сеть с одним коммутатором и тремя сетями VLAN

Пример 9.1. Настройка сетей VLAN и назначение им интерфейсов

```
SW1# show vlan brief
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, Fa0/11, 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
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
```

```
1005 trnet-default       act/unsup
! Выше, сети VLAN 2 и 3 еще не существуют. Ниже добавляется сеть VLAN 2,
! командой name Freds-vlan, с присвоением ей двух интерфейсов.

SW1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# vlan 2
SW1(config-vlan)# name Freds-vlan
SW1(config-vlan)# exit
SW1(config)# interface range fastethernet 0/13 - 14
SW1(config-if)# switchport access vlan 2
SW1(config-if)# end

! Ниже подкоманда интерфейса show running-config выводит списки команд
! на интерфейсах Fa0/13 и Fa0/14.
SW1# show running-config
! Часть строк опущена для краткости
vlan 2
name Freds-vlan
!
! еще часть строк опущена для краткости
interface FastEthernet0/13
  switchport access vlan 2
  switchport mode access
!
interface FastEthernet0/14
  switchport access vlan 2
  switchport mode access
!

SW1# show vlan brief

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, Fa0/11, Fa0/12
                                     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 Freds-vlan              active     Fa0/13, Fa0/14
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup

SW1# show vlan id 2
VLAN Name                 Status     Ports
---- -------------------- ---------- -------------------------------------
2    Freds-vlan           active     Fa0/13, Fa0/14

VLAN Type  SAID   MTU  Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ----- ------ ---- ------ ------ -------- --- -------- ------ -------
2    enet  100010 1500 -      -      -        -   -        0      0

Remote SPAN VLAN
----------------
Disabled
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------
```

Этот пример начинается с выполнения команды `show vlan brief`, позволяющей убедиться в том, что пять не удаляемых сетей VLAN имеют стандартные параметры, а все интерфейсы назначены сети VLAN 1. (Сеть VLAN 1 не может быть удалена, но может использоваться. На настоящий момент сети VLAN 1002–1005 не могут быть удалены и не могут использоваться для доступа.) Следует отметить, что рассматриваемый коммутатор 2960 имеет 24 порта Fast Ethernet (Fa0/1–Fa0/24) и два порта Gigabit Ethernet (Gi0/1 и Gi0/2), в выводе первой команды все они принадлежали сети VLAN 1.

Далее показан процесс создания сети VLAN 2 и назначение ей интерфейсов Fa0/13 и Fa0/14. Обратите внимание, что в данном примере используется команда `interface range`, применяющая подкоманды интерфейса `switchport access vlan 2` к обоим интерфейсам в диапазоне, что подтверждается выводом команды `show running-config` в конце примера.

После добавления данной конфигурации для получения информации о новой сети VLAN в этом примере повторно выполняется команда `show vlan brief`. В ее выводе указаны сеть VLAN 2, имя `Freds-vlan` и присвоенные ей интерфейсы Fa0/13 и Fa0/14.

Сеть в примере на рис. 9.11 использует в качестве портов доступа шесть интерфейсов коммутатора. Такие порты не должны использовать магистральное соединение, они должны быть присвоены конкретной сети VLAN командой `switchport access vlan` *`идентификатор_vlan`*. Однако, согласно конфигурации в примере 9.1, эти интерфейсы могли вести переговоры, чтобы стать портами магистрального канала (стандартное состояние коммутатора). Это позволяет порту договориться о магистральном соединении и решить, действовать ли как интерфейс доступа или как магистральный интерфейс.

Для портов, которые всегда должны быть портами доступа, имеет смысл ввести необязательную подкоманду интерфейса `switchport mode access`. Она указывает коммутатору, что порту позволено быть только интерфейсом доступа. Более подробная информация о командах, позволяющих порту вести переговоры об использовании магистральных соединений, приведена в следующем разделе.

Второй пример: сокращенная настройка сети VLAN

Пример 9.1 демонстрирует несколько необязательных команд конфигурации, побочным эффектом которых является немного более продолжительная настройка. Альтернативная конфигурация в примере 9.2 намного короче, в нем добавляется сеть VLAN 3 (как показано на рис. 9.11), ее следует считать продолжением примера 9.1. Обратите также внимание, что до начала этого примера на коммутаторе SW1 отсутствуют данные о сети VLAN 3.

Пример 9.2. Более короткий пример настройки сети VLAN (сети VLAN 3)

```
SW1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# interface range Fastethernet 0/15 - 16
SW1(config-if-range)# switchport access vlan 3
% Access VLAN does not exist. Creating vlan 3
SW1(config-if-range)# ^Z
```

```
SW1# show vlan brief

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, Fa0/11, Fa0/12
                                       Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                       Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                       Gi0/1, Gi0/2
2    Freds-vlan             active     Fa0/13, Fa0/14
3    VLAN0003               active     Fa0/15, Fa0/16
1002 fddi-default           act/unsup
1003 token-ring-default     act/unsup
1004 fddinet-default        act/unsup
1005 trnet-default          act/unsup
```

Пример 9.2 демонстрирует, как коммутатор может динамически создать сеть VLAN (эквивалент глобальной команды конфигурации `vlan` *`идентификатор_vlan`*), когда подкоманда интерфейса `switchport access vlan` применяется к ненастроенной в настоящий момент сети VLAN. В начале этого примера на коммутаторе SW1 отсутствует информация о сети VLAN 3, а когда используется подкоманда интерфейса `switchport access vlan 3`, коммутатор понимает, что такой сети не существует и, как упомянуто в затененном сообщении этого примера, создает сеть VLAN 3, используя стандартное имя (VLAN0003). Никаких других действий по созданию этой сети VLAN не требуются. В конце рассматриваемого процесса обнаруживается, что на коммутаторе существует сеть VLAN 3, а в сети VLAN 3 находятся интерфейсы Fa0/15 и Fa0/16, о чем свидетельствует затененная часть вывода команды `show vlan brief`.

Протокол создания магистралей VLAN (VTP)

Прежде чем перейти к следующим примерам конфигурации, следует узнать о прежнем протоколе Cisco — *протоколе создания магистралей VLAN* (VLAN Trunking Protocol — VTP). Это собственный протокол компании Cisco, выполняющийся на ее коммутаторах. Он анонсирует каждую сеть VLAN, настроенную на одном коммутаторе командой `vlan` *`номер`*, чтобы о ней узнали все остальные коммутаторы в территориальной локальной сети. Однако по разным причинам в большинстве корпоративный сетей протокол VTP не используют.

Эта книга не пропагандирует протокол VTP. Но он оказывает некоторое влияние на работу коммутаторов Cisco Catalyst, даже если и не используется. В этом кратком разделе протокол VTP обсуждается достаточно подробно, чтобы можно было заметить небольшие отличия в его работе.

Каждый коммутатор может работать в одном из трех режимов VTP: серверном, клиентском или прозрачном. Коммутаторы используют серверный и клиентский режимы, когда протокол VTP применяется по прямому назначению: для динамического анонсирования информации о конфигурации сетей VLAN. Однако при множестве коммутаторов Cisco и версий операционной системы IOS протокол VTP не может быть отключен на коммутаторе Cisco полностью; вместо этого коммутатор переводит его в прозрачный режим.

В данной книге мы пытаемся, по возможности, игнорировать протокол VTP. Для этого во всех приведенных примерах коммутаторы используются в прозрачном режиме протокола VTP (глобальная команда `vtp mode transparent`) или при его отключении (глобальная команда `vtp mode off`). Обе позволяют администратору задать как стандартный, так и расширенный диапазон сетей VLAN, а коммутатор перечисляет команды `vlan` в файле конфигурации `running-config`.

И наконец, встретив в практическом применении (выполняя упражнения лабораторных работ с реальными коммутаторами или их эмуляторами) необычное поведение сетей VLAN, проверьте состояние протокола VTP командой `show vtp status`. Если коммутатор будет использовать серверный или клиентский режим VTP, то обнаружится следующее:

- серверные коммутаторы могут настраивать сети VLAN только в стандартном диапазоне (1–1005);
- клиентские коммутаторы не могут настраивать сети VLAN;
- команда `show running-config` не отображает команды `vlan`.

Выполняя практические задания экзаменов CCENT и CCNA по настройке коммутатора, по возможности переведите коммутатор в прозрачный режим или вообще отключите протокол VTP.

ВНИМАНИЕ!

Экспериментируя с параметрами VTP на реальном коммутаторе, будьте очень осторожны. Если этот коммутатор подключен к другим коммутаторам, которые в свою очередь подключены к коммутаторам, используемым в рабочей сети LAN, вполне можно вызвать проблемы, переписав конфигурации VLAN других коммутаторов. Будьте внимательны и никогда не экспериментируйте с параметрами VTP на коммутаторе, если к нему подключены другие коммутаторы, особенно если есть физические каналы связи с рабочими сетями LAN.

Конфигурация магистрального соединения VLAN

Настройка магистрального соединения между двумя коммутаторами Cisco может быть очень простой, если она осуществляется только статически. Например, если два коммутатора Cisco 2960 соединены друг с другом, они поддерживают только протокол 802.1Q, но не ISL. Достаточно добавить буквально одну подкоманду интерфейса для порта коммутатора на каждой стороне канала связи (`switchport mode trunk`), и будет получен магистральный канал VLAN, поддерживаемый всеми сетями VLAN, известными каждому коммутатору.

Однако конфигурация магистрали на коммутаторах Cisco имеет еще много возможностей, включая несколько вариантов для динамических переговоров о разных параметрах магистрали. Они могут быть либо заданы предварительно, либо коммутаторы могут сами договориться о них следующим образом.

- *Тип магистрального соединения*: протокол IEEE, протокол 802.1Q или переговоры о применяемом протоколе.
- *Административный режим*: всегда магистральный канал, никогда магистральный канал или переговоры.

Сначала рассмотрим тип магистрального соединения. Коммутаторы Cisco, поддерживающие протоколы ISL и 802.1Q, способны вести переговоры об используемом типе при помощи *протокола динамического согласования магистральных каналов* (Dynamic Trunk Protocol — DTP). Если оба коммутатора поддерживают оба протокола, они используют протокол ISL; в противном случае они используют общий протокол. Современные коммутаторы Cisco не поддерживают устаревший протокол ISL. Коммутаторы, поддерживающие оба типа магистрального соединения, используют подкоманду интерфейса `switchport trunk encapsulation {dot1q | isl | negotiate}` для того, чтобы задать тип или позволить протоколу DTP договариваться о типе.

Протокол DTP позволяет также согласовать административный режим локальных портов коммутаторов. Под *административным режимом* (administrative mode) подразумевается настройка конфигурации, определяющая, должно ли использоваться магистральное соединение в интерфейсе. У каждого интерфейса также есть *рабочий режим* (operational mode), когда интерфейс выполняет присущие ему действия, возможно, выбранные протоколом DTP в ходе переговоров с другим устройством. Для определения административного режима магистрали коммутаторы Cisco используют подкоманду интерфейса `switchport mode` с параметрами, перечисленными в табл. 9.1.

Ключевая тема

Таблица 9.1. Параметры команды `switchport mode`, определяющие административный режим магистрали

Параметр	Описание
`access`	Всегда быть портом доступа (а не магистрального канала)
`trunk`	Всегда быть портом магистрального канала
`dynamic desirable`	Передавать и отвечать на сообщения переговоров, чтобы динамически решить, использовать ли магистральное соединение
`dynamic auto`	Пассивно ожидать получения сообщений переговоров. При получении таковых вести переговоры об использовании магистрального соединения

В качестве примера рассмотрим два коммутатора на рис. 9.12. Это сеть, показанная на рис. 9.11, дополненная магистральным каналом к новому коммутатору SW2, часть портов которого подключена к сетям VLAN 1 и VLAN 3. Для магистрального соединения оба коммутатора используют канал связи Gigabit Ethernet. В данном случае магистральное соединение не создается динамически, поскольку у обоих коммутаторов (2960) стандартно задан административный режим `dynamic auto`, а это значит, что ни один из них не инициализирует процесс согласования магистрального соединения. После изменения конфигурации одного коммутатора для использования режима `dynamic desirable`, предназначенного для инициализации переговоров, на коммутаторах проводится согласование магистрального соединения, а именно — соединения по протоколу 802.1Q, поскольку коммутаторы 2960 поддерживают только протокол 802.1Q.

Пример 9.3 начинается с отображения стандартной конфигурации двух коммутаторов на рис. 9.12 и позволяет убедиться в отсутствии магистрального соединения между ними.

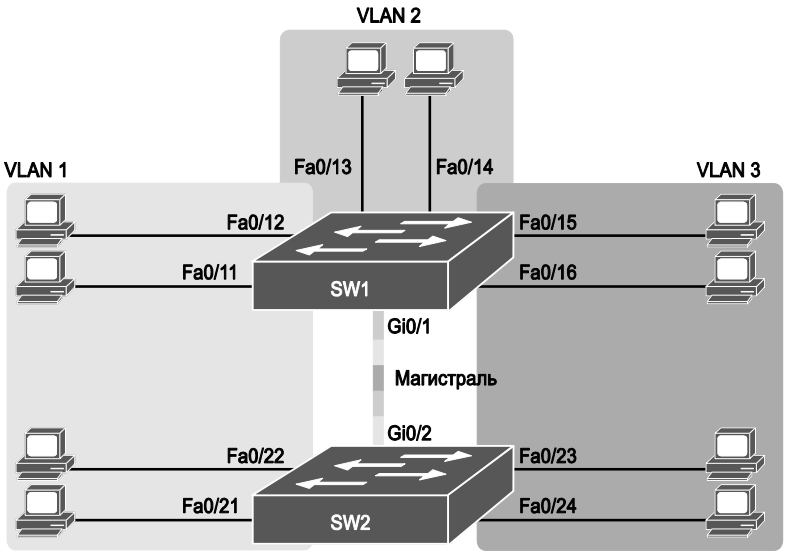

Рис. 9.12. Сеть с двумя коммутаторами и тремя сетями VLAN

Пример 9.3. Изначальное (стандартное) состояние: между коммутаторами SW1 и SW2 нет магистрального соединения

```
SW1# show interfaces gigabit 0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
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

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
```

```
Appliance trust: none

! Обратите внимание, выполнение следующей команды приводит к
! появлению одной пустой строки вывода.
SW1# show interfaces trunk

SW1#
```

Прежде всего рассмотрим важные сведения, содержащиеся в выводе команды `show interfaces switchport` в начале примера 9.3. Вывод демонстрирует применение стандартного значения административного режима `dynamic auto`. В коммутаторе SW2 также применяется значение `dynamic auto`, поэтому в выводе команды состояния коммутатора SW1 показано как `access`, а это значит, что магистральное соединение отсутствует. В третьей затененной строке показан единственный поддерживаемый тип магистрального соединения (802.1Q) в коммутаторе 2960. (На коммутаторе, поддерживающем оба протокола, ISL и 802.1Q, это было бы значение `negotiate`, означающее переговоры о типе или инкапсуляции магистрального соединения.) Наконец, фактически применяемый тип магистрального соединения указан как `native`, а значит, используется собственная сеть VLAN в соответствии с протоколом 802.1Q.

Пример завершается командой `show interfaces trunk`, но без вывода. Эта команда выводит информацию обо всех интерфейсах магистральных каналов, работающих в настоящий момент, т.е. она перечисляет интерфейсы, которые в настоящее время используют магистральное соединение VLAN. Не перечисляя интерфейсы, эта команда также подтверждает, что канал связи между коммутаторами не является магистральным соединением.

Теперь рассмотрим пример 9.4, демонстрирующий новую конфигурацию, где магистральное соединение разрешено. В данном случае коммутатор SW1 настроен командой `switchport mode dynamic desirable`, требующей от коммутатора начать процесс переговоров, а не ждать их от другого устройства. Как только команда будет введена, появятся регистрационные сообщения, свидетельствующие об отключении, а затем о включении интерфейса, как обычно происходит при переходе интерфейса из режима доступа в режим магистрального канала.

Пример 9.4. Изменение режима коммутатора SW1 с `dynamic auto` на `dynamic desirable`

```
SW1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# interface gigabit 0/1
SW1(config-if)# switchport mode dynamic desirable
SW1(config-if)# ^Z
SW1#
01:43:46: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed
state to down
01:43:49: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed
state to up
SW1# show interfaces gigabit 0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: dynamic desirable
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)
! строки опущены для краткости

! Следующая команда раньше выводила одну пустую строку, а теперь ее вывод
! содержит информацию об одной действующей магистрали.

SW1# show interfaces trunk

Port   Mode      Encapsulation   Status   Native vlan
Gi0/1  desirable 802.1q          trunking 1

Port   Vlans allowed on trunk
Gi0/1  1-4094

Port   Vlans allowed and active in management domain
Gi0/1  1-3

Port   Vlans in spanning tree forwarding state and not pruned
Gi0/1  1-3

SW1# show vlan id 2
VLAN Name                   Status     Ports
---- -------------------- ---------- -------------------------------------
2    Freds-vlan           active     Fa0/13, Fa0/14, G0/1

VLAN Type  SAID   MTU  Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ----- ------ ---- ------ ------ -------- --- -------- ------ -------
2    enet  100010 1500 -      -      -        -   -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------
```

Для проверки того, что магистральное соединение теперь работает, в середине примера 9.4 введена команда `show interfaces switchport`. Обратите внимание: в ее выводе по-прежнему отображаются административные параметры, демонстрирующие введенные в конфигурацию значения, но наряду с ними отображаются рабочие настройки, благодаря чему можно узнать, какие действия в настоящее время выполняются коммутатором. В данном случае коммутатор SW1 находится в рабочем режиме магистрального канала с применением инкапсуляции `dot1Q`.

В конце примера приведен вывод команды `show interfaces trunk`, который отображает интерфейс G0/1, подтверждая, что теперь он работает как магистраль. Смысл вывода этой команды обсуждается в следующем разделе.

Для подготовки к экзаменам следует быть готовым интерпретировать вывод команды `show interfaces switchport`, разбираться в том, как по ее выводу определять заданный административный режим, и знать, должно ли в канале быть создано магистральное соединение, если применяются указанные настройки. В табл. 9.2 перечислены сочетания административных режимов магистрального соединения и ожидаемые режимы работы (магистральный или доступа), устанавливаемые в результате

применения заданных параметров. В левой части таблицы указаны административные режимы, используемые коммутатором на одном конце канала, а в верхней части — административные режимы, заданные для коммутатора на другом конце канала.

Ключевая тема **Таблица 9.2. Ожидаемый рабочий режим магистрали на основании параметров административных режимов**

Административный режим	access	dynamic auto	trunk	dynamic desirable
access	access	access	Не используется *	access
dynamic auto	access	access	trunk	trunk
trunk	Не используется *	trunk	trunk	trunk
dynamic desirable	access	trunk	trunk	trunk

* Когда коммутатор на одном конце находится в режиме `access`, а на другом конце в режиме `trunk`, возникают проблемы. Избегайте такой комбинации.

Компания Cisco рекомендует отключать переговоры магистральных каналов на большинстве портов для повышения их защиты. Большинство портов на большинстве коммутаторов используется для подключения пользователей. Не забывайте, переговоры DTP можно отключить в целом с помощью подкоманды интерфейса `switchport nonegotiate`.

Контроль сетей VLAN, поддерживаемых на магистральном канале

Список разрешенных сетей VLAN (allowed VLAN list) — это механизм, позволяющий сетевым инженерам административно отключать сети VLAN от магистрального канала. Стандартно коммутаторы включают в список разрешенных сетей VLAN каждой магистрали все возможные сети VLAN (от VLAN 1 до VLAN 4094). Однако впоследствии инженер может сократить количество сетей VLAN, которым разрешено использовать магистральный канал. Для этого используется следующая подкоманда интерфейса:

`switchport trunk allowed vlan {add | all | except | remove}` *`список_vlan`*

Эта команда предоставляет удобный способ добавления и удаления сетей VLAN из списка разрешенных. В частности, параметр `add` позволяет коммутатору добавлять сети VLAN к существующему списку разрешенных сетей VLAN, а с помощью параметра `remove` можно удалить сети VLAN из существующего списка коммутатора. Под параметром `all` подразумеваются все сети VLAN, поэтому он может применяться для переустановки коммутатора в стандартную конфигурацию (разрешающую применение магистрали для сетей VLAN от 1 до 4094). С другой стороны, параметр `except` является довольно сложным; он позволяет добавить к списку все сети VLAN, не указанные в команде. Например, выполнение подкоманды интерфейса `switchport trunk allowed vlan except 100-200` добавит к существующему списку разрешенных сетей сети VLAN 1–VLAN 99 и сети VLAN 201–VLAN 4094.

Кроме списка разрешенных сетей VLAN, коммутатор может руководствоваться другими причинами для запрета передачи через определенную магистраль трафика конкретной сети VLAN. Все пять причин запрета прохождения трафика перечислены ниже.

Причины невозможности передачи трафика сети VLAN по магистральному каналу

Ключевая тема

- Сеть VLAN удалена из списка *разрешенных сетей VLAN* для магистрального канала.
- Сеть VLAN отсутствует в конфигурации коммутатора (как свидетельствует вывод команды `show vlan`).
- Сеть VLAN существует, но административно отключена (командой `shutdown`).
- Сеть VLAN автоматически отсечена протоколом VTP.
- Экземпляр STP сети VLAN перевел магистральный интерфейс в состояние блокировки.

ВНИМАНИЕ!

Последние две причины не рассматриваются в этой книге, но упоминаются здесь для порядка.

Первая причина (список разрешенных сетей VLAN) уже упоминалась в этом разделе, а теперь обсудим две следующие. Если у коммутатора нет информации о существовании какой-то сети VLAN (т.е. команды `vlan` *`идентификатор_vlan`* в конфигурации коммутатора нет, что подтверждает вывод команды `show vla`), то он не будет перенаправлять фреймы этой сети VLAN ни по какому интерфейсу. Кроме того, сеть VLAN может существовать в конфигурации коммутатора, но быть административно отключенной либо глобальной командой конфигурации `shutdown vlan` *`идентификатор_vlan`*, либо командой `shutdown` в режиме конфигурации VLAN. Когда сеть VLAN отключена, коммутатор больше не будет перенаправлять ее фреймы даже по магистральным каналам. В результате коммутаторы не перенаправляют фреймы несуществующих или отключенных сетей VLAN ни по одному из магистральных каналов.

В этой книге есть смысл перечислить причины невозможности передачи трафика сети VLAN по магистральному каналу: команда `show_interfaces_trunk` выводит список идентификаторов VLAN в том же порядке, на основании тех же причин. Вывод указанной команды содержит продолжение в виде трех списков сетей VLAN, поддерживаемых магистральным каналом.

- Сети VLAN, разрешенные на магистральном канале (стандартно 1–4094).
- Сети VLAN из первой группы, настроенные и активные (не отключенные).
- Сети VLAN из второй группы, не отсеченные протоколом VTP и не блокированные протоколом STP.

Чтобы получить представление об этих трех списках в выводе команды `show interfaces trunk`, рассмотрим пример 9.5, демонстрирующий варианты запрета передачи трафика сетей VLAN через магистральный канал по разным причинам. Вывод указанной команды получен на коммутаторе SW1 (см. рис. 9.12) после настройки конфигурации в соответствии с предыдущими примерами этой главы. Другими словами, сети VLAN 1–3 существуют в конфигурации коммутатора SW1 и не отключены. Магистральное соединение между коммутаторами SW1 и SW2 находится в рабочем состоянии. Затем в ходе выполнения данного примера на коммутаторе SW1 настраиваются следующие параметры конфигурации.

Этап 1 Настройка сети VLAN 4

Этап 2 Отключение сети VLAN 2

Этап 3 Удаление сети VLAN 3 из списка разрешенных сетей VLAN магистрального канала

Пример 9.5. Списки разрешенных и активных сетей VLAN

```
! Три списка сетей VLAN в выводе следующей команды показывают разрешенные
! сети VLAN (1-4094), разрешенные и активные сети VLAN (1-3) и
! разрешенные, активные, неотсеченные и перенаправляемые STP
! сети VLAN (1-3).
SW1# show interfaces trunk

Port   Mode      Encapsulation   Status   Native vlan
Gi0/1  desirable 802.1q          trunking 1

Port   Vlans allowed on trunk
Gi0/1  1-4094

Port   Vlans allowed and active in management domain
Gi0/1  1-3

Port   Vlans in spanning tree forwarding state and not pruned
Gi0/1  1-3

! После этого в конфигурации коммутатора выполняется настройка новой сети
! VLAN 4, сеть VLAN 2 отключается, а сеть VLAN 3 удаляется из списка
! разрешенных сетей VLAN для этой магистрали.
SW1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# vlan 4
SW1(config-vlan)# vlan 2
SW1(config-vlan)# shutdown
SW1(config-vlan)# interface gi0/1
SW1(config-if)# switchport trunk allowed vlan remove 3
SW1(config-if)# ^Z

! Три списка сетей VLAN в выводе следующей команды показывают разрешенные
! сети VLAN (1, 2 и 4-4094), разрешенные и активные сети VLAN (1 и 4) и
! разрешенные, активные, неотсеченные и перенаправляемые протоколом STP
! сети VLAN (1 и 4).

SW1# show interfaces trunk
Port   Mode      Encapsulation   Status   Native vlan
Gi0/1  desirable 802.1q          trunking 1

! Далее сеть VLAN 3 исключается, поскольку она была удалена из списка
! разрешенных сетей VLAN.
Port   Vlans allowed on trunk
Gi0/1  1-2,4-4094

! Сеть VLAN 2 исключается, поскольку она отключена. Сети VLAN 5-4094
! исключаются, поскольку на коммутаторе SW1 они не настроены.
Port   Vlans allowed and active in management domain
Gi0/1  1,4

Port   Vlans in spanning tree forwarding state and not pruned
Gi0/1  1,4
```

Обзор

Резюме

- Локальная сеть (LAN) объединяет все устройства в том же широковещательном домене.
- Без виртуальных сетей коммутатор полагает, что все его интерфейсы находятся в том же широковещательном домене.
- Коммутатор VLAN может настроить часть интерфейсов на один широковещательный домен, а часть на другой, создав в результате два широковещательных домена. Эти созданные коммутатором индивидуальные широковещательные домены и являются виртуальными локальными сетями (VLAN).
- Ниже приведен список наиболее распространенных причин создания меньших широковещательных доменов (сетей VLAN).
  - Сокращение дополнительных затрат процессоров всех устройств за счет сокращения количества устройств, получающих каждый широковещательный фрейм.
  - Улучшение защиты за счет сокращения количества хостов, получающих копии фреймов при их лавинной рассылке коммутатором (широковещание, групповая передача и одноадресатные фреймы с неизвестным получателем).
  - Улучшение защиты хостов, пересылающих важные данные, за счет их помещения в отдельную сеть VLAN.
  - Возможность более гибкого объединения пользователей в группы (например, по отделам) вместо физического разделения по местоположению.
  - Упрощение поиска проблемы в сети, поскольку большинство проблем локализуется в области набора устройств, формирующих широковещательный домен.
  - Сокращение дополнительных затрат на работу протокола распределенного связующего дерева (STP) за счет ограничения VLAN одним коммутатором доступа.
- Настройка сети VLAN с одним коммутатором требует немного усилий: достаточно настроить каждый порт так, чтобы указать ему номер VLAN, к которой он принадлежит.
- Когда сети VLAN используются в сетях с несколькими соединенными между собой коммутаторами, на каналах связи между ними применяется магистральное соединение VLAN.
- Магистральное соединение VLAN подразумевает использование коммутаторами процесса назначения тегов VLAN, когда передающий коммутатор добавляет к фрейму другой заголовок перед его передачей по магистральному каналу. Этот дополнительный заголовок включает поле идентификатора VLAN (VLAN ID), позволяющего передающему коммутатору ассоциировать фрейм с конкретной сетью VLAN, а получающему коммутатору узнать, к какой именно VLAN принадлежит данный фрейм.

- В последние годы компания Cisco использует два разных протокола магистральных соединений: протокол межкоммутаторных соединений (ISL) и протокол 802.1Q стандарта IEEE.
- Для каждого магистрального канала стандарт 802.1Q определяет также один специальный идентификатор VLAN, обозначающий собственную сеть VLAN (стандартно это VLAN 1).
- При создании территориальной локальной сети, содержащей много сетей VLAN, требуется обеспечить всем устройствам возможность передавать данные на все остальные устройства.
- Окончательное решение подразумевает передачу функций маршрутизации аппаратным средствам коммутатора LAN. Производители уже довольно давно начали объединять аппаратные и программные средства коммутаторов уровня 2 с маршрутизаторами уровня 3, выпуская коммутаторы уровня 3 (они же многоуровневые коммутаторы). Коммутаторы уровня 3 могут быть настроены так, чтобы действовать только как коммутаторы уровня 2 или коммутаторы уровня 2 с маршрутизаторами уровня 3.
- Последовательность настройки конфигурации VLAN и назначения интерфейсов.

  Этап 1 Чтобы настроить конфигурацию новой сети VLAN, выполните следующие действия:

  A. В режиме настройки конфигурации введите глобальную команду конфигурации `vlan` *`идентификатор_vlan`* для создания сети VLAN и перейдите в режим настройки конфигурации сети VLAN.

  B. (Необязательно.) Чтобы присвоить сети VLAN имя, введите подкоманду VLAN `name` *`имя`*. Если этого не сделать, именем VLAN будет `VLAN`*`ZZZZ`*, где *`ZZZZ`* — десятичный идентификатор из четырех цифр

  Этап 2 Для каждого интерфейса доступа (интерфейса, принадлежащего не магистральному каналу, а отдельной сети VLAN) выполните следующие действия:

  A. Используя команду `interface`, перейдите в режим конфигурации каждого настраиваемого интерфейса.

  B. Используя подкоманду интерфейса `switchport access vlan` *`идентификатор_vlan`*, укажите номер VLAN, связанной с данным интерфейсом.

  C. (Необязательно). Чтобы отключить магистральное соединение на том же интерфейсе и запретить переговоры о создании магистрального канала, используйте подкоманду интерфейса `switchport mode access`

- Протокол создания магистралей VLAN — это собственный протокол компании Cisco, выполняющийся на ее коммутаторах. Он анонсирует каждую сеть VLAN, настроенную на одном коммутаторе командой `vlan` *`номер`*, чтобы о ней узнали все остальные коммутаторы в территориальной локальной сети.

Контрольные вопросы

Ответьте на эти вопросы. Ответы можно найти на последней странице главы. Полное объяснение ответов приведено в приложении B на веб-сайте.

1. Какой из следующих терминов, применяемых в локальной сети, наиболее соответствует термину *сеть VLAN*?

   А) Домен коллизий.

   Б) Широковещательный домен.

   В) Домен подсети.

   Г) Отдельный коммутатор.

   Д) Магистраль.

2. Предположим, имеется коммутатор с тремя сетями VLAN. Сколько требуется подсетей IP при условии, что на всех хостах во всех сетях VLAN должны применяться протоколы TCP/IP?

   А) 0.

   Б) 1.

   В) 2.

   Г) 3.

   Д) Об этом нельзя судить на основании лишь предоставленной информации.

3. Коммутатор SW1 посылает фрейм коммутатору SW2 по магистрали, использующей протокол 802.1Q. Какой из ответов описывает процесс изменения или добавления коммутатором SW1 заголовка фрейма Ethernet перед его перенаправлением на коммутатор SW2?

   А) Добавляет 4-байтовый заголовок и изменяет MAC-адрес.

   Б) Добавляет 4-байтовый заголовок и не изменяет MAC-адрес

   В) Инкапсулирует первоначальный фрейм в совершенно новый заголовок Ethernet

   Г) Все ответы неверные.

4. Между двумя коммутаторами Ethernet существует магистральный канал 802.1Q. Какой из ответов наиболее точно определяет фреймы, в которые не включается заголовок 802.1Q?

   А) Фреймы в собственной сети VLAN (только один).

   Б) Фреймы сетей VLAN расширенного диапазона.

   В) Фреймы сети VLAN 1 (не настраиваемой)

   Г) Фреймы всех собственных сетей VLAN (когда разрешено несколько).

5. Предположим, получено такое указание, что коммутатор 1 настроен с параметром `dynamic auto` для создания магистрали на интерфейсе Fa0/5, который подключен к коммутатору 2. Необходимо настроить конфигурацию коммутатора 2. Какая из следующих настроек для магистрального соединения может обеспечить работу магистрали? (Выберите два ответа.)

   А) Перевод магистрали в режим `on`.

   Б) Параметр `dynamic auto`.

   В) Параметр `dynamic desirable`.

   Г) Параметр `access`.

   Д) Все ответы неверные.

6. Коммутатор только что получен от корпорации Cisco. Еще не проводилось никаких настроек сетей VLAN, протокола VTP или любой другой конфигурации. Инженер переходит в режим настройки конфигурации и вводит команду `vlan 22`, за которой следует команда `name Hannahs-VLAN`. Какое из следующих утверждений является истинным?

   А) В выводе команды `show vlan brief` отображается сеть VLAN 22.

   Б) В выводе команды `show running-config` отображается сеть VLAN 22.

   В) Сеть VLAN 22 не создается в этом процессе.

   Г) Сеть VLAN 22 не существует в этом коммутаторе до тех пор, пока в нее не добавлено ни одного интерфейса.

7. Какая из следующих команд позволяет получить информацию о состоянии интерфейсов коммутатора, т.е. работают ли они в настоящий момент как магистральные каналы VLAN? (Выберите два ответа).

   А) `show interfaces`

   Б) `show interfaces switchport`

   В) `show interfaces trunk`

   Г) `show trunks`

Ключевые темы

Повторите все ключевые темы данной главы, отмеченные пиктограммой "Ключевая тема". Ключевые темы и соответствующие им страницы перечислены в табл. 9.3.

Таблица 9.3. Ключевые темы главы 9

Элемент	Описание	Страница
Рис. 9.2	Создание двух широковещательных доменов с использованием одного коммутатора и сети VLAN	285
Список	Причины применения сетей VLAN	286
Рис. 9.5	Магистральное соединение VLAN между двумя коммутаторами	288
Рис. 9.6	Заголовок магистрального соединения по стандарту 802.1Q	289
Рис. 9.9	Маршрутизация между двумя сетями VLAN с использованием магистрального канала на маршрутизаторе	292
Рис. 9.10	Маршрутизация между сетями VLAN с использованием коммутатора уровня 3	294
Список	Последовательность настройки конфигурации VLAN и назначения интерфейсов	294
Табл. 9.1	Параметры команды switchport mode, определяющие административный режим магистрали	300
Табл. 9.2	Ожидаемый рабочий режим магистрали на основании параметров административных режимов	304
Список	Причины невозможности передачи трафика сети VLAN по магистральному каналу	305

Заполните таблицы и списки по памяти

Распечатайте приложение H (Appendix M) с веб-сайта или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении O (Appendix N) приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

После первого прочтения главы попытайтесь дать определения следующим ключевым терминам. Но не расстраивайтесь, если не все получится сразу, в главе 30 описано, как использовать эти термины на завершающем этапе подготовки к экзамену.

802.1Q, магистральный канал (trunk), административный режим магистрали (trunking administrative mode), рабочий режим магистрали (trunking operational mode), VLAN, VTP, прозрачный режим VTP (VTP transparent mode), коммутатор третьего уровня (Layer 3 switch), интерфейс доступа (access interface), магистральный интерфейс (trunk interface)

Таблицы команд

Хоть и не обязательно заучивать информацию из таблиц данного раздела, в табл. 9.4 приведен список команд конфигурации, а в табл. 9.5 пользовательские команды главы. Фактически команды стоит запомнить, чтобы лучше понять содержимое главы и выполнить задания по подготовке к экзамену. Чтобы проверить, насколько хорошо вы запомнили команды, закройте левую сторону таблицы листом бумаги, читайте описания с правой стороны и пытайтесь вспомнить команду.

Таблица 9.4. Команды конфигурации главы 9

Команда	Описание
`vlan` *`идентификатор_vlan`*	Глобальная команда конфигурации, позволяющая создать сеть VLAN и перевести интерфейс командной строки в режим настройки конфигурации сети VLAN
`Name` *`имя_vlan`*	Подкоманда сети VLAN, позволяющая присвоить имя сети VLAN
`[no] shutdown`	Подкоманда режима VLAN, позволяющая включить (`no shutdown`) или отключить (`shutdown`) сеть VLAN
`[no] shutdown vlan` *`идентификатор_vlan`*	Глобальная команда конфигурации, аналогичная подкоманде режима VLAN `[no] shutdown`
`vtp mode {server | client | transparent | off}`	Глобальная команда конфигурации, определяющая режим VTP
`switchport mode {access | dynamic {auto | desirable} | trunk}`	Подкоманда интерфейса, задающая административный режим магистрального соединения на интерфейсе
`switchport trunk allowed vlan {add | all | except | remove}` *`список_vlan`*	Подкоманда интерфейса, определяющая список разрешенных сетей VLAN

Окончание табл. 9.4

Команда	Описание
`switchport access vlan` *`идентификатор_vlan`*	Подкоманда интерфейса, применяемая для статической настройки интерфейса при подключении к одной указанной сети VLAN
`switchport trunk encapsulation {dot1q | isl | negotiate}`	Подкоманда интерфейса, определяющая тип используемого магистрального соединения с учетом того, задано ли магистральное соединение в конфигурации или согласовано
`switchport trunk native vlan` *`идентификатор_vlan`*	Подкоманда интерфейса, определяющая собственную сеть VLAN для порта магистрального канала
`switchport nonegotiate`	Подкоманда интерфейса, запрещающая согласование при создании магистрали VLAN

Таблица 9.5 Пользовательские команды главы 9

Команда	Описание
`show interfaces` *`идентификатор_интерфейса`* `switchport`	Выводит информацию о любом интерфейсе, относящуюся к административным настройкам и рабочему состоянию
`show interfaces` *`идентификатор_интерфейса`* `trunk`	Выводит информацию обо всех действующих магистралях (но не о других интерфейсах), включая список сетей VLAN, трафик которых может быть перенаправлен по данной магистрали
`show vlan [brief | id` *`идентификатор_vlan`* `| name` *`имя_vlan`* `| summary]`	Выводит информацию о сети VLAN
`show vlan [`*`vlan`*`]`	Отображает информацию о сети VLAN
`show vtp status`	Выводит информацию о конфигурации протокола VTP и о состоянии

Ответы на контрольные вопросы:

1 Б. **2** Г. **3** Б. **4** А. **5** А и В. **6** А и Б. **7** Б и В.