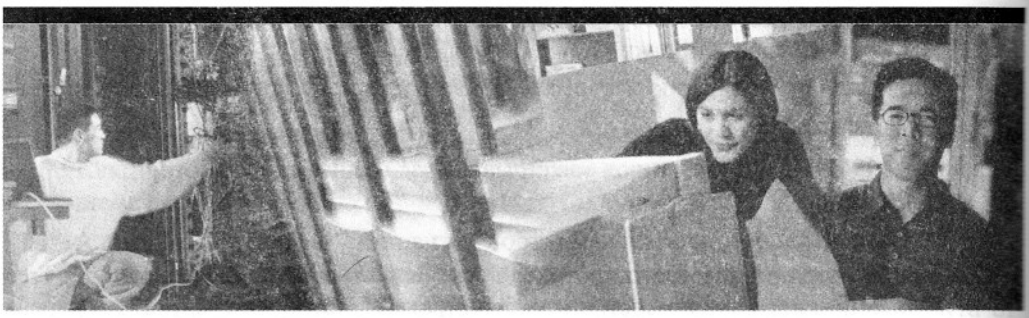

В этой главе...

- Дано определение виртуальной локальной сети
- Описаны причины создания сетей VLAN и описаны их преимущества
- Описаны способы реализации сетей VLAN
- Описано создание, тестирование и удаление конфигураций VLAN-сетей
- Описаны основные методы устранения ошибок в сетях VLAN

Глава 9

Виртуальные локальные сети

В настоящей главе приводятся начальные сведения о виртуальных локальных сетях (Virtual Local-Area Networks — VLAN) и описываются преимущества использования коммутируемой архитектуры VLAN. В ней также приведены основные понятия, используемые для описания работы VLAN-сетей и рассмотрены основные операции. Кроме того, в этой главе приведены инструкции по созданию, тестированию и удалению VLAN-сетей. В заключение описаны способы устранения шибок, которые можно использовать для их нахождения и разрешения проблем, возникающих при реализации сетей VLAN.

Рекомендуется также выполнить лабораторные работы (e-Lab Activities), ознакомиться с видеоклипами (Videos) и фотографиями (PhotoZooms), которые находятся на прилагаемом к книге компакт-диске. Эти приложения дополняют материал книги и помогают лучше усвоить используемые понятия и методы.

Начальные сведения о сетях VLAN

Одной из важных функций, реализуемых в технологии Ethernet, являются *виртуальные локальные сети VLAN*, в которых для объединения рабочих станций и серверов в логические группы используются коммутаторы. Связь устройств, принадлежащих к одной VLAN-сети, возможна только с устройствами этой же сети, поэтому сеть с коммутацией функционирует как несколько индивидуальных, не соединенных друг с другом локальных сетей LAN. Трудно дать общее строгое определение сетей VLAN, поскольку разные производители используют различные подходы к созданию таких сетей.

Компании часто используют сети VLAN в качестве способа логической группировки пользователей. Это можно сравнить с традиционной организацией рабочих мест, в которой несколько отделов обычно группировались в локальный департамент и локальная сеть естественным образом решала задачи связи для этого департамента. В настоящее время сотрудники часто не связаны с конкретным физическим рабочим местом, поэтому сети VLAN создают не физическую, а логическую группу пользователей. Например, сотрудники, работающие в отделе маркетинга, объединены VLAN-сетью маркетинга, а сотрудники инженерного подразделения — VLAN-сетью инженерных служб.

Сети VLAN решают задачи масштабирования сети, обеспечения безопасности и сетевого управления. В сетях с топологией VLAN маршрутизаторы обеспечивают фильтрацию широковещания, решают задачи защиты сети и управления потоками данных.

Сеть VLAN представляет собой группу сетевых устройств и служб, не ограниченную физическим сегментом или коммутатором. На рис. 9.1. показано логическое группирование рабочих станций в сети VLAN, в сравнении с физическим группированием рабочих станций в традиционной сети LAN.

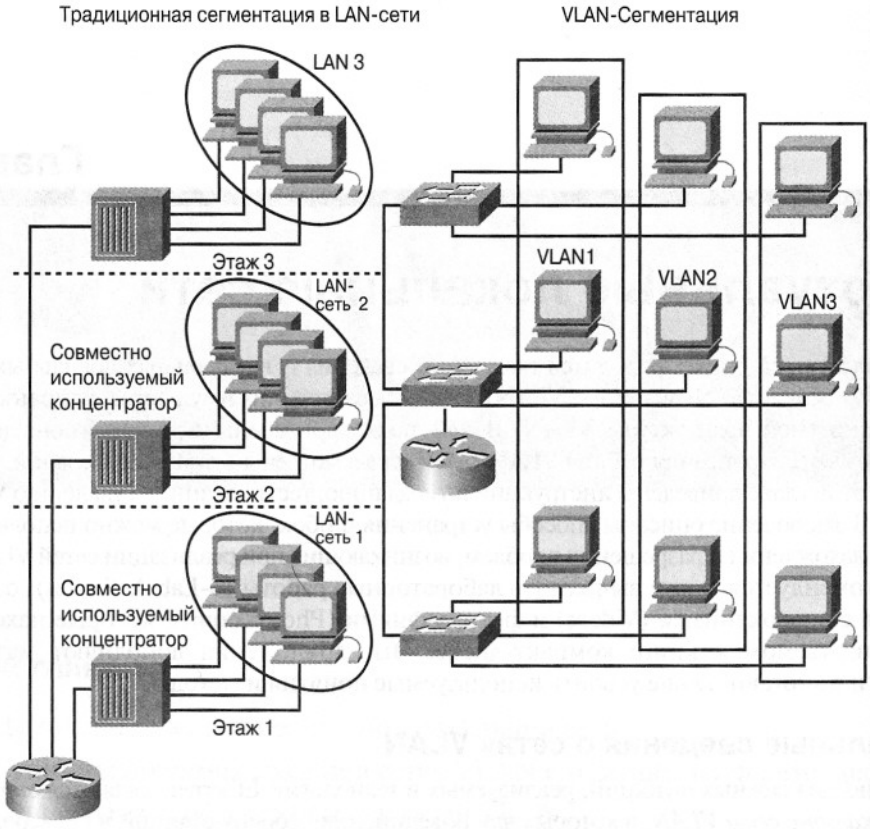

Рис. 9.1. Сети VLAN и физические границы

Сети VLAN логически сегментируют сети, использующие коммутацию, на основе их организационных функций, принадлежности к различным рабочим коллективам (группам) или используемым приложениям, а не на базе физического или географического расположения. Например, все рабочие станции и серверы, используемые некоторой рабочей группой, могут быть объединены в одну и ту же сеть VLAN, независимо от их физического подсоединения к сети или расположения на территории предприятия. На рис. 9.2 приведен пример проектирования сети VLAN в физической сети. В данном случае создаются три сети VLAN, в которых рабочие станции соединены друг с другом через коммутаторы, а сами коммутаторы соединены друг с другом через маршрутизатор. Реконфигурирование системы может быть выполнено программным способом, без физического перемещения устройств и изменения подключения кабелей.

На рис. 9.3 показано физическое проектирование сети VLAN, основанное на различных рабочих группах компании и их расположении на различных этажах офиса. В данном случае сеть VLAN создается для каждого отдела (инженерный отдел, отдел маркетинга и отдел учета), в каждом из которых имеется свой коммутатор.

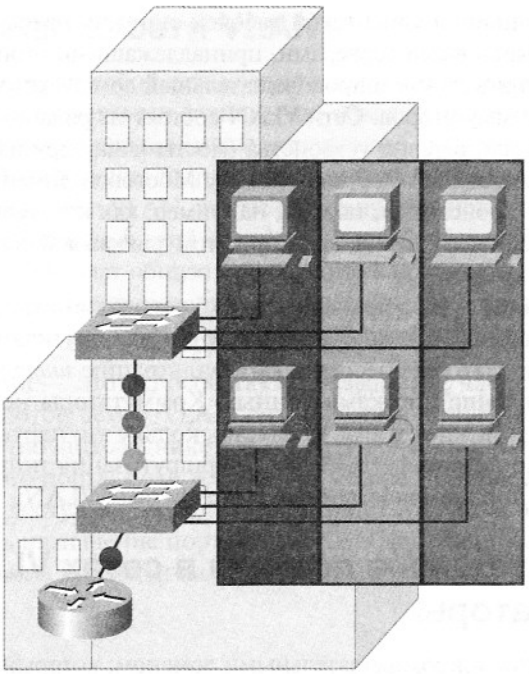

Рис. 9.2. Проектирование виртуальной локальной сети

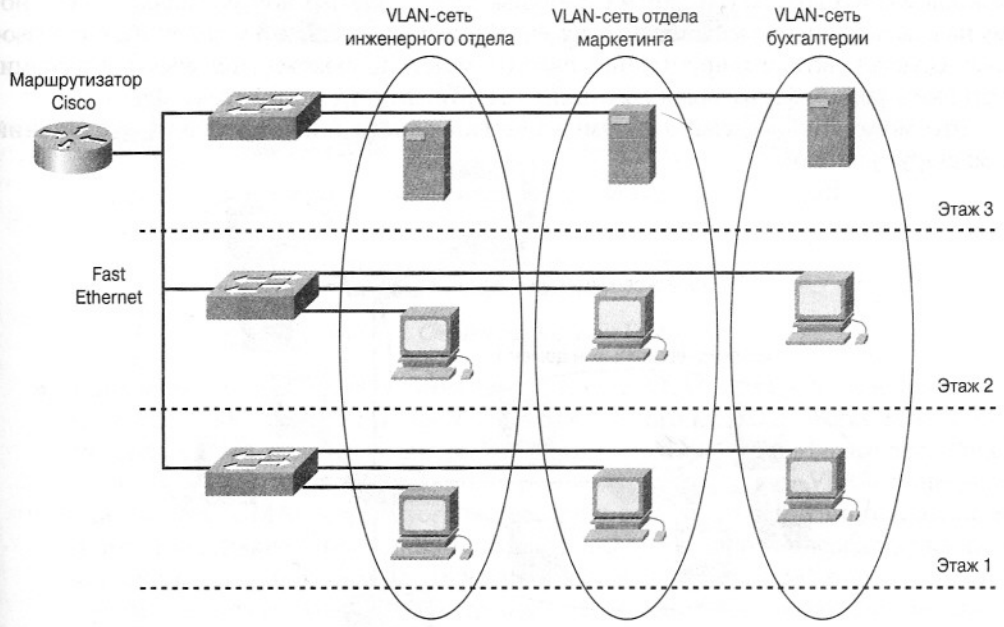

Рис. 9.3. Сети VLAN охватывают определенное физическое пространство

Как правило, соединения клиентской рабочей станции, находящейся в сети VLAN, ограничены только файловыми серверами, принадлежащими этой же сети VLAN. Сеть VLAN можно рассматривать как широковещательный домен, который существует в определенном наборе коммутаторов. Сети VLAN состоят из ряда конечных систем, таких как рабочие станции или сетевые устройства (мосты и маршрутизаторы), соединенных друг с другом через отдельный мостовой домен. Мостовой домен поддерживается различными сетевыми устройствами, такими, например, как коммутаторы сетей LAN, которые работают по мостовым протоколам; при этом для каждой сети VLAN имеется своя мостовая группа.

Сети VLAN создаются для реализации служб сегментации, которые в традиционных LAN-конфигурациях обычно обеспечиваются маршрутизаторами. В топологиях сетей VLAN маршрутизаторы обеспечивают фильтрацию *широковещания (broadcast)*, защиту сети и управление потоками данных. Коммутаторы не могут осуществлять мостовые соединения между сетями VLAN, поскольку это нарушило бы целостность широковещательного домена сети VLAN. Маршрутизация потоков данных должна происходить только при передаче данных между сетями VLAN.

Широковещательные домены в сетях VLAN и маршрутизаторы

Сеть VLAN является широковещательными доменом, который создается одним или более коммутаторами. В приводимом ниже сценарии при проектировании сети требуется создать два отдельных широковещательных домена. На рис. 9.4 два отдельных широковещательных домена создаются с помощью трех отдельных коммутаторов — по одному на каждый широковещательный домен. Следует отметить, что маршрутизатор позволяет осуществлять маршрутизацию пакетов между широковещательными доменами, которые в данном случае подобны отдельным группам устройств 3-го уровня.

Это может быть сделано путем установки одного или нескольких соединений с маршрутизатором.

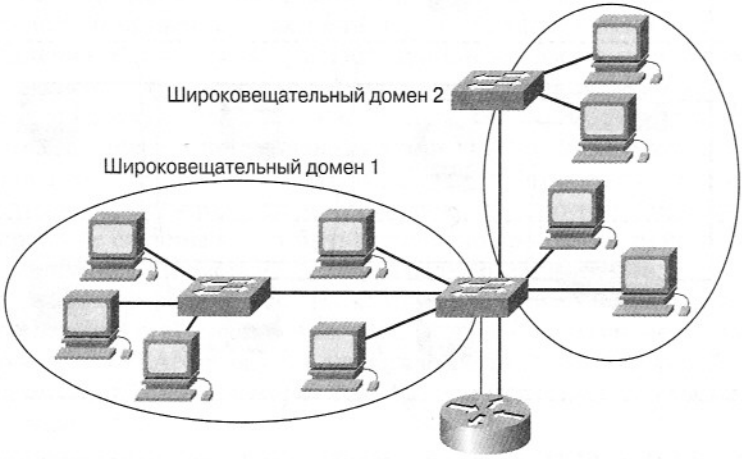

Рис. 9.4. Распределение широковещания в сети VLAN

Функционирование сети VLAN

Сеть VLAN представляет собой сеть коммутации, которая логически сегментируется в соответствии с выполняемыми функциями, объединением сотрудников в группы или согласно используемым приложениям, независимо от физического расположения пользователей. Сети VLAN может быть выделен любой порт коммутатора. Порты, выделенные одной и той же сети VLAN, имеют общее пространство широковещания.

Порты, не принадлежащие к этой сети VLAN, не получают эти широковещательные сообщения. Это повышает общую производительность сети, поскольку уменьшается количество ненужных широковещательных сообщений, которые потребляют полосу пропускания сети. Сети VLAN создаются двумя описанными ниже способами.

- **Статические сети** — этот способ также называется членством на базе порта. Назначение портов сетям VLAN создает статическое распределение VLAN. Когда устройство подсоединяется к порту, оно автоматически попадает во VLAN-сеть этого порта. Если устройство меняет порт своего подключения, но ему требуется доступ к той же самой сети VLAN, то сетевой администратор должен сделать назначение порта сети VLAN для нового соединения. Пример такого назначения приведен на рис. 9.5.

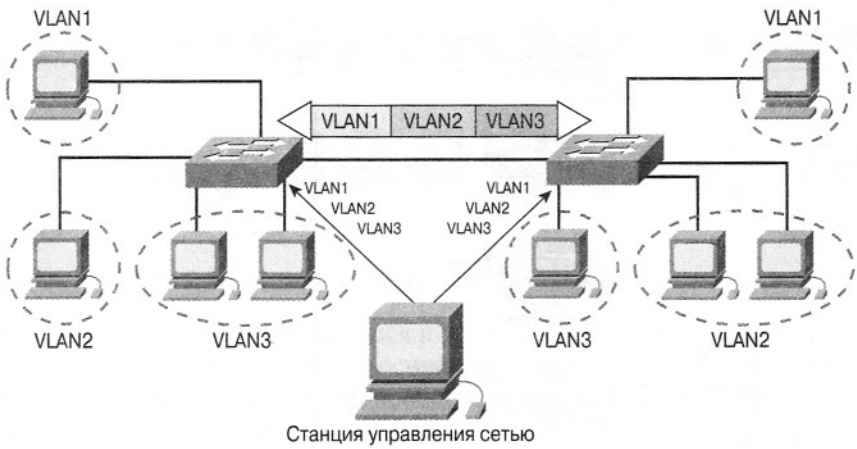

Рис. 9.5. Статические сети VLAN

- **Динамические сети VLAN** — динамические сети VLAN создаются с использованием пакетного программного обеспечения, такого как CiscoWorks 2000. С помощью сервера политик управления сетями VLAN (VLAN Management Policy Server — VMPS) можно назначать порты коммутатора сетям VLAN динамически, на основе MAC-адреса устройства-источника, подсоединенного к данному порту. В настоящее время динамические VLAN позволяют присоединять к себе устройства на основе MAC-адреса источника. Когда устройство присоединяется к сети, оно делает запрос в базу данных на сервере VMPS относительно своей принадлежности к данной сети VLAN. Этот процесс показан на рис. 9.6, где каждый коммутатор имеет свой уникальный MAC-адрес.

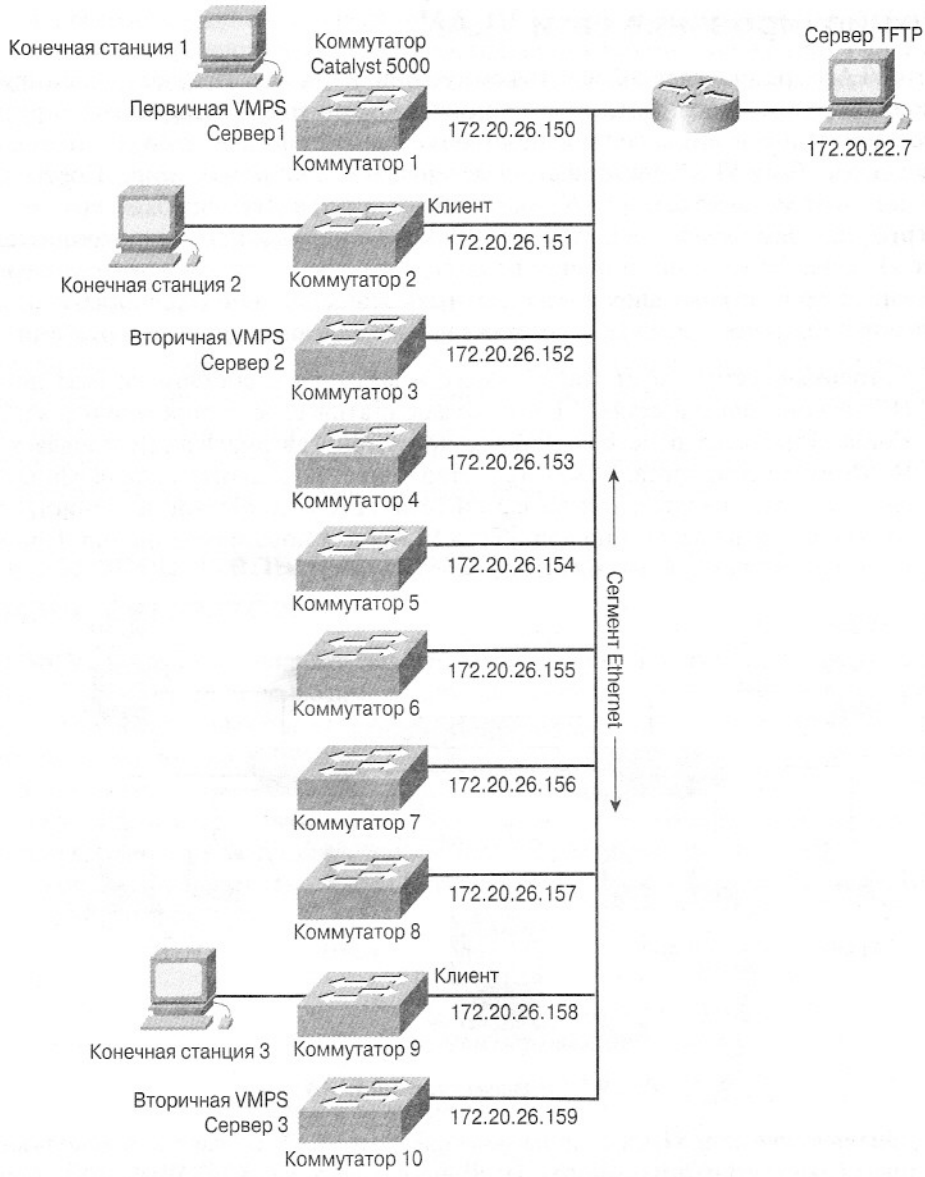

Рис. 9.6. Динамические сети VLAN

Принадлежность устройства к статической сети VLAN на основе портов проиллюстрировано на рис. 9.7. Конкретной сети VLAN назначается порт, который не зависит от пользователя или системы, подсоединенной к данному порту. Это означает, что все пользователи, подсоединенные к данному порту, должны быть членами одной и той же сети VLAN. Отдельная рабочая станция пользователя или концентратор, к которому подсоединены несколько рабочих станций, могут быть подсоединены к отдельному порту коммутатора. Назначение портов сетям VLAN обычно осуществляет сетевой администратор. Конфигурация порта в этом случае является статической и переключе-

ние порта на другую VLAN не может быть выполнено автоматически без реконфигурирования коммутатора. Следует обратить внимание на то, то каждая сеть VLAN находится в отдельной подсети, а маршрутизатор используется для связи между этими подсетями.

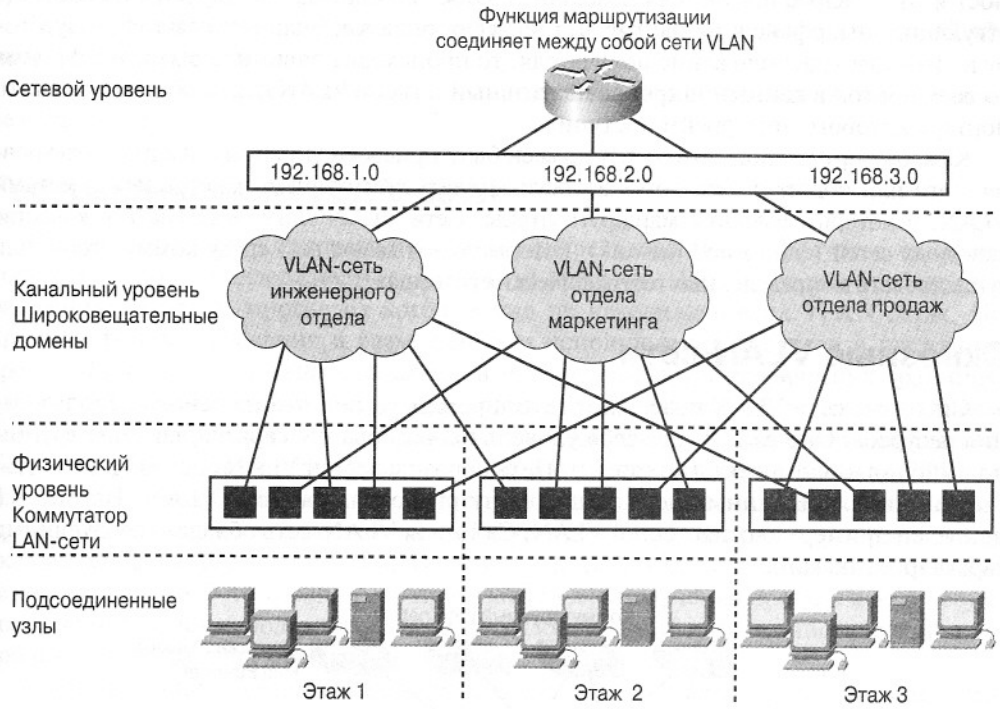

Рис. 9.7. Статические виртуальные сети на основе портов

Когда пользователи подсоединяются к этому совместно используемому сегменту, как это происходит в традиционных основанных на концентраторах сетях LAN, все они после этого используют общую полосу пропускания. На каждого дополнительного пользователя, который подсоединяется к совместно используемой среде передачи, приходится меньше доступной полосы пропускания, поскольку все пользователи находятся в одном и том же коллизионном домене. Если количество пользователей, использующих одну и ту же полосу пропускания становится слишком большим, то начинаются частые коллизии и работа приложения пользователя становится малопроизводительной. Коммутаторы уменьшают вероятность коллизий за счет обеспечения выделенной полосы пропускания между устройствами с помощью микросегментации; однако коммутаторы по-прежнему рассылают всем пользователям широковещательные сообщения, такие, как сообщения протокола ARP. Сети VLAN обеспечивают пользователям большую полосу пропускания в совместно используемой сети путем создания отдельных широковещательных доменов.

По умолчанию на каждом порте коммутатора имеется сеть VLAN1 или сеть VLAN управления. Сеть управления не может быть удалена, однако могут быть созданы дополнительные сети VLAN и этим альтернативным VLAN могут быть дополнительно назначены порты.

Следует помнить о том, что каждый интерфейс коммутатора ведет себя как порт моста и в целом коммутатор можно рассматривать как многопортовый мост. Мосты отфильтровывают потоки данных, которые не требуется направлять в иные сегменты, кроме того, из которого они поступили. Если фрейм необходимо переслать через мост и MAC-адрес получателя известен, то мост направляет этот фрейм на соответствующий интерфейс и не направляет на все остальные. Если мосту или коммутатору не известно расположение получателя, то происходит лавинная рассылка фрейма со всех портов в данный широковещательный домен (VLAN), за исключением того порта, с которого этот фрейм поступил.

Каждой виртуальной сети VLAN должен быть присвоен уникальный адрес 3-го уровня (сети или подсети). Это помогает осуществлять коммутацию пакетов между сетями VLAN, в которых имеются маршрутизаторы. Сети VLAN могут выступать в качестве сквозных сетей (end-to-end network), которые охватывают всю среду коммутатора, или существовать в определенных географических границах.

Сквозные VLAN-сети

Сквозные сети VLAN позволяют группировать устройства на основе использования ресурсов. Оно включает в себя уровень использования сервера, рабочие группы по выполняемым проектам и отделы. Цель сквозных сетей VLAN состоит в том, чтобы не менее 80% данных передавались внутри локальной сети VLAN. На рис. 9.8 приведен пример сквозных сетей VLAN. Сквозная VLAN-сеть обладает следующими характеристиками:

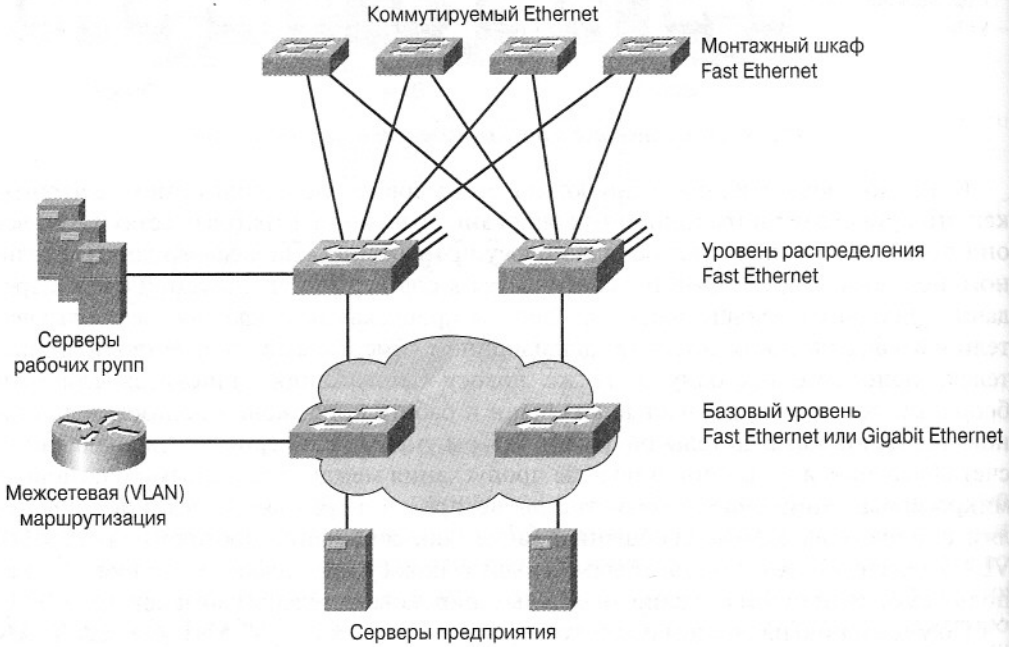

Рис. 9.8. Сквозные VLAN-сети

Пользователи группируются в сети VLAN независимо от их физического расположения, но в соответствии с исполняемыми ими рабочими функциями или с принадлежностью к разным рабочим группам.

У всех пользователей соотношение передачи данных внутри VLAN-сети и за ее пределы должно быть одним и тем же и составлять 80:20.

При перемещении пользователя в пределах сети кампуса его членство в сети VLAN не должно изменяться.

В каждой VLAN-сети для всех ее членов должны действовать общие правила безопасности

Географические VLAN-сети

По мере того, как корпоративные сети централизовали свои ресурсы, становилось все сложнее поддерживать сквозные VLAN-сети. Пользователям требовались различные ресурсы, многие из которых уже не находились в их VLAN-сетях. По причине такого изменения в размещении и использования ресурсов в настоящее время VLAN-сети все чаще создаются в определенных географических границах, а не в границах сообщества. Эти географические границы могут быть целым зданием или всего лишь одним коммутатором в монтажном шкафу. В такой географической VLAN-структуре типичным является случай соотношения обмена данными 20% для локального использования и 80% — для удаленных соединений. Это соотношение прямо противоположно тому, которое обычно устанавливается при проектировании сквозных VLAN. Хотя такая топология означает, что пользователю приходится пересекать устройство 3-го уровня (маршрутизатор) для получения доступа к 80% ресурсов, она позволяет использовать в сети последовательный детерминистический способ получения доступа к ресурсам.

Географическими сетями VLAN также значительно легче управлять и концептуализировать их, чем VLAN-сетями, устройства которых находятся в географически различных областях.

Преимущества сетей VLAN

Коммерческие компании постоянно реорганизуются. В среднем 20-40% рабочей силы физически меняют место проживания каждый год. Эти переезды, добавление новых пользователей, и другие изменения являются одними из главных головных болей сетевых менеджеров и составляют одну из самых больших статей расходов, связанных с управлением сетью. Многие перемещения пользователей требуют прокладки новых кабелей и почти все перемещения требуют новой адресации станций и реконфигурирования концентраторов и маршрутизаторов.

Изменения в системе управления сетью

Сети VLAN предоставляют эффективный механизм для управления изменениями в топологии сети и значительно снижают затраты, связанные с реконфигурированием концентраторов и маршрутизаторов. Пользователи сети VLAN могут использовать одно и то же сетевое адресное пространство (т.е. IP-подсеть), независимо от их физического расположения. Когда пользователи сети VLAN перемещаются из одного места в другое, до тех пор пока они остаются в одной и той же VLAN и подсоединены к од-

ному и тому же порту коммутатора, их сетевые адреса не изменяются. Изменение расположения пользователя требует лишь таких простых действий как включение штекера пользователя в соответствующий порт VLAN-коммутатора и конфигурирование порта коммутатора, к которому подсоединена данная VLAN. В динамических сетях VLAN при просматривании MAC-адреса сетевого адаптера переместившейся рабочей станции в VMPS, коммутатор автоматически конфигурирует порт таким образом, чтобы он оказался в требуемой сети VLAN.

VLAN-сети и безопасность

VLAN сети являются эффективным механизмом расширения сферы действия брандмауэра от маршрутизаторов к среде коммутатора и защиты сети от потенциально опасных проблем, связанных с широковещанием. Кроме того, сети VLAN сохраняют все преимущества высокопроизводительной коммутации.

Брандмауэры создаются путем назначения портов коммутатора или пользователей в конкретные группы VLAN как на одном коммутаторе, так и на нескольких соединенных друг с другом коммутаторах. Широковещательные потоки данных не передаются за пределы сети VLAN. На рис. 9.9 приведен пример широковещательных доменов. В свою очередь смежные порты не получают широковещательных данных, которые генерируются другими сетями VLAN. Такой тип конфигурации значительно уменьшает общий объем широковещательных данных, освобождает полосу пропускания для действительно полезных данных и снижает общий уровень уязвимости сети в отношении широковещательных штормов. На рис. 9.10 показано как маршрутизатор может выполнять функции брандмауэра между сетями VLAN.

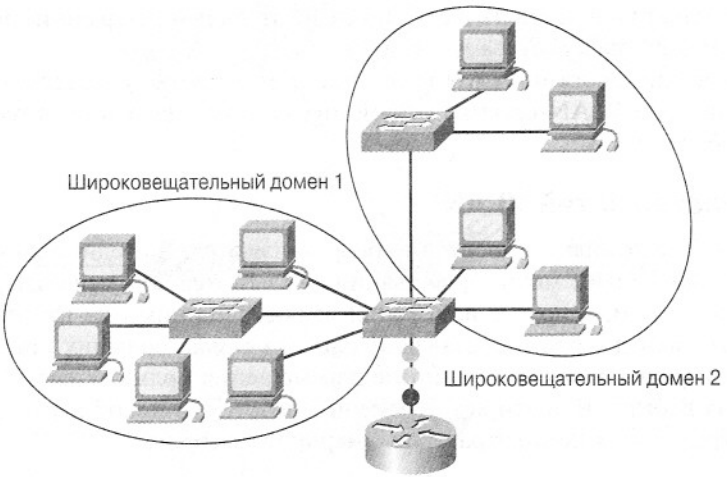

Рис. 9.9. Широковещательные домены

Одной из проблем совместно используемых сетей LAN является относительная легкость проникновения в них. Подключаясь к работающему порту несанкционированный пользователь получает доступ ко всем данным, передаваемым в сегменте. Чем больше группа пользователей, тем большие возможности создаются для потенциального несанкционированного доступа.

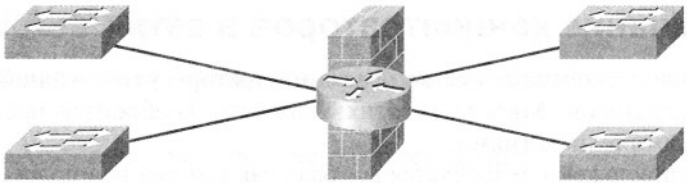

Рис. 9.10. Брандмауэр для широковещательных данных

Одним из экономически эффективных и легко административно реализуемых способов повышения уровня безопасности в сети является сегментация сети на несколько широковещательных групп. Это позволяет сетевому менеджеру решить следующие задачи:

- ограничить количество пользователей во VLAN-группе;
- предотвратить присоединение других полей без предварительного получения разрешения от приложения, управляющего сетью VLAN;
- сконфигурировать все неиспользуемые порты на принимаемую по умолчанию службу нижнего уровня VLAN.

Реализация такого типа сегментации относительно проста. Порты коммутатора объединяются в группы на основе типа приложения и привилегий при доступе. Ограниченные приложения и ресурсы обычно размещаются в защищенных VLAN-группах. В защищенных сетях VLAN коммутатор ограничивает доступ пользователей к группе. Ограничения могут основываться на адресах станций, типах приложений или типах протокола. Пример обеспечения безопасности в сети VLAN показан на рис. 9.11.

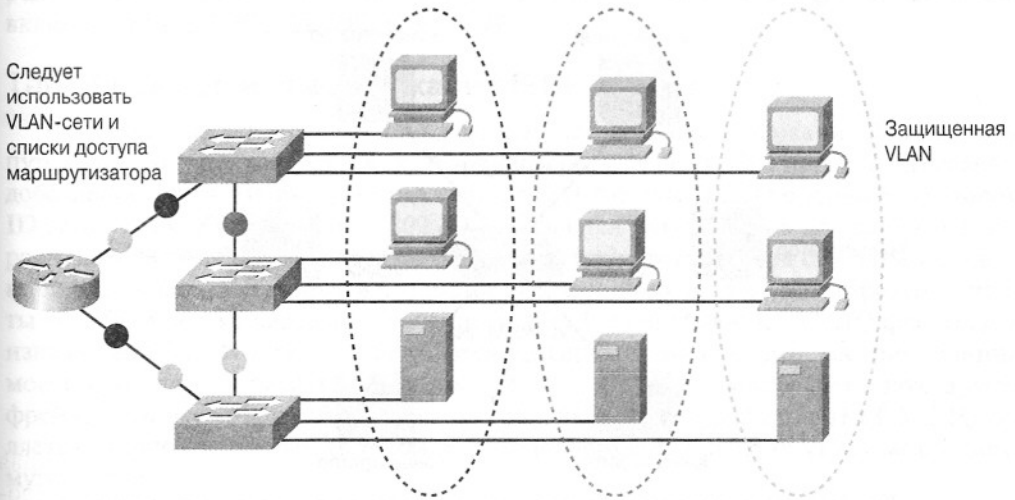

Рис. 9.11. Защищенная VLAN-сеть

Использование концентраторов в сетях VLAN

За последние несколько лет сетевые администраторы установили большое количество концентраторов. Многие из этих устройств заменяются настоящее время коммутирующими технологиями.

Поскольку приложениям требуется все большая выделенная полоса пропускания и производительность непосредственно на рабочем столе, эти концентраторы попрежнему выполняют полезные функции по многих уже существующих сетях. Сетевые менеджеры могут сэкономить средства. Подсоединив существующие концентраторы к коммутаторам. Пример такого использования концентраторов приведен на рис. 9.12. каждый сегмент концентратора, подсоединенный к порту коммутатора, может быть назначен только одной сети VLAN. Все станции, совместно использующие сегмент концентратора, становятся членами одной и той же группы VLAN. Коммутатор поддерживает несколько адресов доступа к среде передачи или MAC-адресов (Media Access Control — MAC), по одному на каждую станцию, которые логически связаны с портом, к которому подсоединен концентратор. Если требуется переназначить отдельную станцию в другую VLAN-сеть, то станцию необходимо подсоединить к соответствующему концентратору. Соединенные между собой коммутаторы обрабатывают передачу данных между портами коммутатора и автоматически определяют соответствующие принимающие сегменты. Чем больше мелких групп будет образовано на совместно используемом концентраторе, тем больше степень микросегментации и тем большая гибкость обеспечивается для назначения индивидуальных пользователей в группы VLAN. Путем подсоединения концентраторов к коммутаторам можно сконфигурировать концентраторы в качестве части архитектуры VLAN. Можно также обеспечить совместное использование передачи данных и сетевых ресурсов, непосредственно подсоединенных к коммутирующим портам с получателями VLAN.

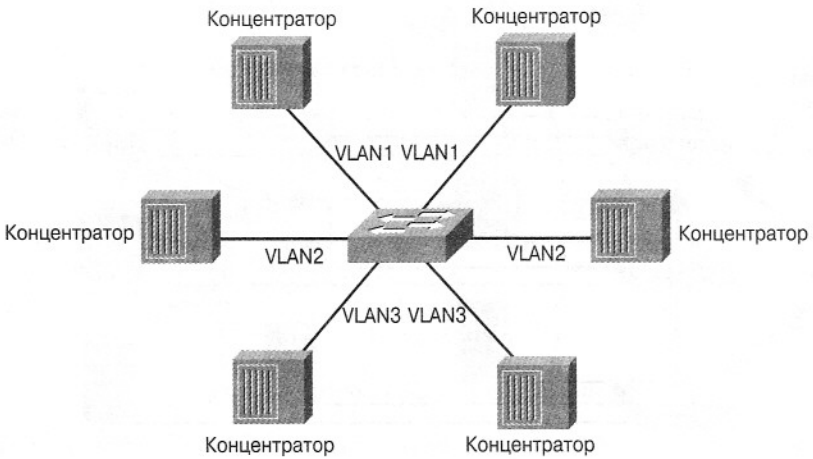

Рис. 9.12. Использование существующих концентраторов в среде коммутации сети VLAN

Типы VLAN-сетей

Три приведенных ниже базовых модели определяют назначение пакета сети VLAN и управляют его передачей.

- Сети VLAN, базирующиеся на портах (статические).
- VLAN-сети на основе MAC-адресов (динамические).
- Основанные на протоколах VLAN-сети.

Количество образованных на одном коммутаторе VLAN-сетей может изменяться в широких пределах, в зависимости от нескольких факторов. Среди этих факторов можно выделить типичный характер передачи данных, типы приложений, потребности сетевого управления и общей группы. Кроме того, важным фактором, определяющим количество VLAN-сетей на коммутаторе, является используемая схема IP-адресации. Например, предположим, что сеть использует 254-битовую маску для определения подсетей. В этом слу4чае в одной подсети можно использовать до 254 адресов для рабочих станций. Поскольку настоятельно рекомендуется устанавливать взаимно однозначное соответствие между сетями VLAN и IP-подсетями, в одной VLAN-сети может быть не более 254 устройств.

Идентификация фреймов в сетях VLAN

В сетях VLAN с несколькими коммутаторами заголовки фреймов инкапсулируются или модифицируются для указания идентификатора ID сети VLAN до того, как фрейм будет отправлен в канал между коммутаторами. Перед отправкой фрейма конечному устройству заголовок фрейма изменяется и приобретает первоначальный вид.

Идентификация VLAN логически идентифицирует принадлежность пакета к определенной группе VLAN. Существует несколько магистральных методологий, включая IEEE 802.1Q, ISL, 802.10 и LANE.

Теги фреймов в спецификации IEEE 802.1Q

Протокол 802.1Q является стандартным методом идентификации VLAN-сетей путем вставки идентификатора VLAN в заголовок фрейма. Это процесс называется добавлением тега. На рис. 9.13 показан формат фрейма 802.1Q с идентификатором ID сети VLAN. Каждому порту 802.1Q назначается магистраль, а все порты магистрали оказываются в одной изначальной сети VLAN. Все фреймы без тегов назначаются в LAN-сеть, указанную в параметре ID. Ассоциированные магистральные порты 802.1Q имеют изначальное значение VLAN. В спецификации 802.1Q фрейма для изначальной VLAN теги не добавляются. Следовательно обычные рабочие станции могут прочитать изначальные фреймы без тегов, но не могут прочитать другие фреймы, потому что они имеют теги. Добавление тегов к фреймам в IEEE 802.1Q является предпочтительным методом обмена информацией о сетях VLAN между коммутаторами.

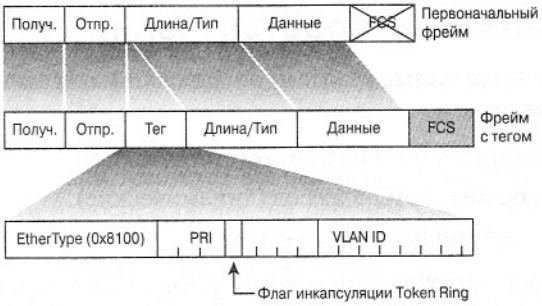

Рис. 9.13. Формат фрейма 802.1Q

Протокол межкоммутаторного канала

Протокол межкоммутаторного канала (Inter-Switch Link — ISL) представляет собой фирменный протокол инкапсуляции Cisco, используемый для связи между собой нескольких коммутаторов. На рис. 9.14 показан формат фрейма протокола ISL.

Для присвоения фреймов, которое используется коммутаторами серии Catalyst Cisco используется обладающий низкой задержкой механизм мультиплексирования потоков данных от нескольких сетей VLAN в один физический канал. Этот протокол был реализован для соединений между коммутаторами, маршрутизаторами и сетевыми адаптерами, используемыми на сетевых узлах, таких как серверы. Для поддержки функций протокола ISL на каждом подсоединенном устройстве должен быть сконфигурирован протокол ISL. Маршрутизатор, на котором сконфигурирован протокол ISL может быть использован для коммуникации между VLAN-сетями. Этот процесс описан более подробно в главе 10. Устройство, на котором не функционирует протокол ISL, при получении инкапсулированного ISL-фрейма Ethernet рассматривает его как ошибку протокола, если размер заголовка вместе с данными фрейма превосходит размер максимального модуля передачи (maximum transmission unit — MTU). Администраторы используют протокол ISL для поддержки избыточных каналов и перераспределения нагрузки между параллельными каналами с использованием протокола связующего дерева (Spanning Tree Protocol).

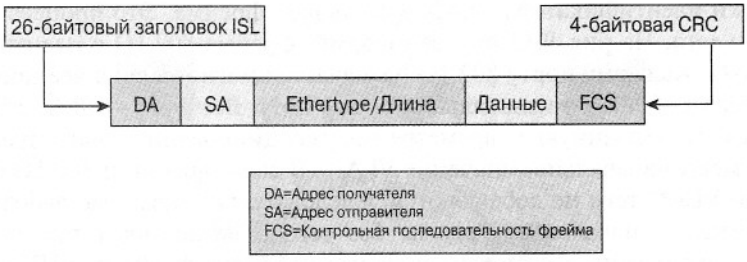

Рис. 9.14. Формат фрейма протокола ISL

Спецификация FDDI 802.10

Спецификация FDDI 802.10 является фирменным методом Cisco для передачи информации о VLAN-сетях во фрейме стандарта IEEE 802.10 (FDDI). Информация VLAN записывается в поле идентификатора ассоциации безопасности (security asso-

ciation identifier — SAID) фрейма 802.10. Этот метод, как правило, используется для передачи данных VLAN по магистрали распределенного оптоволоконного интерфейса данных (Fiber Distributed Data Interface — FDDI).

Эмуляция локальной сети

Эмуляция локальной сети (LAN Emulation — LANE) представляет собой стандарт, определенный форумом ATM и предоставляющий возможность двум станциям, подсоединенным через магистраль ATM те же возможности, которые они бы имели в обычных локальных сетях, таких как Ethernet или Token Ring. Как показывает само название, функцией протокола LANE является эмуляция LAN-сети в сети асинхронного режима передачи (Asynchronous Transfer Mode — ATM). В частности, протокол LANE определяет механизмы эмуляции по спецификации IEEE 802.3 Ethernet или 802.5 Token Ring LAN. Протокол LANE определяет интерфейс службы для протоколов более высокого уровня (т.е. для сетевого уровня), аналогично тому, как это происходит в существующих сетях LAN. Данные, пересылаемые по сети ATM, инкапсулируются в соответствующий MAC-формат LAN-сети. Иными словами, протоколы LANE принуждают ATM-сеть выглядеть и вести себя как LAN сеть Ethernet или Token Ring. Пример LANE-сети приведен на рис. 9.15.

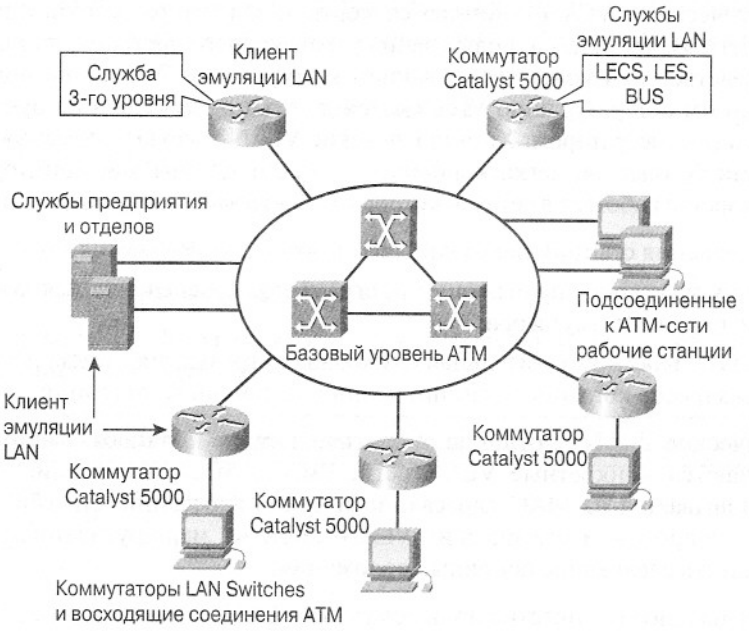

Рис. 9.15. Сеть LANE

В табл. 9.1 перечислены методы присвоения тегов и инкапсуляции.

Таблица 9.1. Методы присвоения тегов и инкапсуляции

Метод идентификации	Инкапсуляция	Присвоение тегов	Среда передачи
802.1Q	Нет	Да	Ethernet
ISL	Да	Нет	Ethernet
802.10	Нет	Нет	FDDI
LANE	Нет	Нет	ATM

Конфигурирование VLAN

Первоначально сетевые администраторы полагали, что сети VLAN упростят их работу и сделают ненужными маршрутизаторы. К сожалению для них, эти надежды не оправдались. Сети VLAN не устранили проблем, связанных с 3-м уровнем модели OSI. Сети VLAN позволяют легче решать задачи 3-го уровня, такие, например, как разработка более простых списков доступа, однако необходимость в маршрутизации на 3-м уровне не исчезла.

Конфигурирование статических VLAN-сетей

Под статическими VLAN понимаются порты коммутатора, которым вручную назначаются сети VLAN путем использования управляющего программного обеспечения или непосредственным конфигурированием коммутатора. Эти порты поддерживают назначенную им конфигурацию VLAN сетей до тех пор пока она не будет изменена системным администратором. Хотя статические VLAN требуют в несения изменений вручную, они безопасны, легко конфигурируются и удобны для мониторинга. Этот тип VLAN хорошо работает в сетях, в которых соблюдаются следующие условия:

- перемещения станций легко контролируются и управляются;
- имеется надежное управляющее программное обеспечение для конфигурирования портов коммутатора;
- нежелательная дополнительная служебная нагрузка, требуемая для поддержки MAC-адресов конечных станций и типовых таблиц фильтрации.

Динамические VLAN, в отличие от статических, не полагаются на порты, котором назначаются конкретные VLAN сети. Вместо этого назначение VLAN-сетей портам основывается на MAC-адресах, логической адресации или типе протокола. При конфигурировании статических VLAN-сетей на маршрутизаторах Cisco 29xx следует помнить следующие основные положения:

- максимальное количество подключаемых VLAN-сетей зависит от типа коммутатора и ограничивается количеством его портов;
- сеть VLAN1 является одной из VLAN-сетей, создаваемых по умолчанию производителем;
- по умолчанию VLAN1 является VLAN-сетью;
- по сети VLAN1 рассылаются анонсирования маршрутов протокола обнаружения устройств Cisco (*Cisco Discovery Protocol — CDP)* и магистрального протокола VLAN (*VLAN Trunking Protocol — VTP)*;

- на всех коммутаторных магистралях, принимающих участие в работе VLAN-сетей, должен быть сконфигурирован один и тот же протокол инкапсуляции, такой как 802.1Q или ISL;
- команды конфигурирования VLAN-сетей зависят от номера модели;
- IP-адреса для моделей Catalyst 29xx находятся в широковещательном домене VLAN;
- при создании , добавлении и удалении VLAN-сетей коммутатор должен находиться в режиме VTP-сервера.

Создание на коммутаторе статической VLAN-сети является несложной задачей. При использовании коммутатора, работающего с командами IOS Cisco, следует войти в режим конфигурирования VLAN с помощью команды привилегированного EXEC-режима **vlan database**. Для создания VLAN-сети следует выполнить приведенные ниже команды.

```
Switch#vlan database
Switch(vlan)vlan vlan_number [ vlan_name]
Switch(vlan)exit
```

При необходимости следует также сконфигурировать имя VLAN-сети.

После выхода из режима конфигурирования на коммутаторе создается VLAN-сеть. Следующим этапом является назначение данной VLAN одному или более интерфейсам.

```
Switch(config)#interface fastethernet 0/3
```

Коммутатор Catalyst 2900:

```
Switch(config-if)#switchport access vlan 2
```

Коммутатор Catalyst 1900:

```
(config-if)#vlan-membership static 2
```

Протестировать конфигурацию можно с помощью команды **show running-config**, как показано в примере 9.1.

Пример 9.1. `show running-configuration`

```
Switch#show running-config
Hostname Switch
!
ip subnet-zero
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
switchport access vlan 2
--- output omitted ---
```

Лабораторная работа: конфигурирование статической VLAN-сети

В этой лабораторной работе требуется сконфигурировать базовую конфигурацию коммутатора и протестировать ее. С консоли требуется определить версию встроенного программного обеспечения, создать две VLAN-сети, задать им имена и назначить им соответствующие порты.

Тестирование конфигурации VLAN-сети

Хорошей практикой является тестирование конфигурации VLAN-сети с помощью команд **show vlan** (как показано в примере 9.2), **show vlan brief** или **show vlan id** *id_number*

Пример 9.2. Команда `show vlan`

```
Switch#show vlan
Virtual LAN ID: 300 (IEEE 802.10 Encapsulation)
vLAN Trunk Interface: FDDI 1/1.10
Protocols Configured: Address: Received: Transmitted:
IP 31.108.1.1 642 645
Virtual LAN ID: 400 (ISL Encapsulation)
vLAN Trunk Interface: FastEthernet 2/1.20
Protocols Configured: Address: Received:Transmitted:
IP 171.69.2.2 123456 654321
Bridge Group 50 5190 8234
Virtual LAN ID:500 (ISL Encapsulation)
vLAN Trunk Interface: FastEthernet 2/1.30
Protocols Configured: Address: Received:Transmitted:
IPX 1000 987654 456789
Virtual LAN ID:600 (ISL Encapsulation)
vLAN Trunk Interface: FastEthernet 2/1.30
Protocols Configured: Address: Received:Transmitted:
IP 198.92.3.3 8114 4508
IPX 1001 2 3
Bridge Group 50 8234 5190
```

При работе с VLAN-сетями следует руководствоваться следующими положениями:

- созданная VLAN-сеть остается неиспользуемой до тех пор, пока она не будет логически связана с портами коммутатора;
- по умолчанию все порты Ethernet находятся в сети VLAN1.
- между номерами портов не следует вводить пробелы. В этом случае коммутатор реагирует сообщением об ошибке, поскольку пробел отделяет другой аргумент, который не является структурной частью команды.

Сохранение конфигурации VLAN

Полезно иметь копию конфигурации VLAN-сети в виде текстового файла в качестве резервной копии и для целей аудита. Для сохранения файла VLAN-конфигурации можно использовать дискету, с тем чтобы потом передать ее на другие рабочие станции. Если в файле конфигурации окажутся скопированными посторонние символы, то их следует удалить.

Ниже описаны действия, которые следует выполнить для копирования конфигурации VLAN-сети.

Этап 1. С консоли коммутатора перейти в привилегированный режим конфигурирования коммутатора.

Этап 2. В окне программы HyperTerminal выбрать опцию Transfer (Передача).

Этап 3. Выбрать опцию Capture Text.

Этап 4. Выбрать место сохранения файла конфигурации (такое, например, как "Рабочий стол").

Этап 5. Задать имя файла конфигурации VLAN-сети.

Этап 6. Выбрать опцию Start.

Этап 7. На коммутаторе выполнить команду **`show run`**.

Этап 8. После того, как будут выполнены команды файла конфигурации, (для окончания их выполнения следует нажать несколько раз клавишу пробела), вернуться к опции Transfer окна программы HyperTerminal, выбрать опцию Capture Text, а затем опцию Stop для сохранения и закрытия файла.

Этап 9. Удалить посторонние символы.

Лабораторная работа: тестирование конфигурации VLAN-сети

В этой лабораторной работе требуется создать базовую конфигурацию коммутатора и две виртуальных локальных сети VLAN. После этого VLAN-сетям следует присвоить имена и назначить им несколько портов. Протестировать функционирование сетей можно путем перемещения рабочей станции из одной сети в другую.

Удаление конфигурации VLAN-сети

Для удаления сети VLAN на коммутаторе, допускающем конфигурирование из командной строки, следует выполнить команду **`clear vlan`** *номер*, как показано в примере 9.3. В этом примере сеть VLAN 2 удаляется из домена с помощью команды **`clear vlan 2`**. Важно отметить, что эта команда должна быть выполнена на коммутаторе VTP-сервера. На коммутаторе клиента VTP удалить VLAN-сеть невозможно. Если коммутатор с конфигурирован в прозрачном режиме, то VLAN-сеть удалить можно, однако при этом VLAN-сеть будет удалена только на самом коммутаторе Catalyst, но не во всем домене управления. Все операции по добавлению и удалению VLAN-сетей на прозрачном коммутаторе имеют лишь локальное значение. Домены VTP описаны в главе 10.

ПРИМЕЧАНИЕ

При удалении сети VLAN все назначенные ей порты перестают быть активными. Эти порты остаются логически связанными с данной сетью VLAN до тех пор, пока они не будут назначены новой VLAN-сети.

Пример 9.3 Конфигурирование коммутатора

```
Console>(enable) clear vlan 2
This command will deactivate all ports on vlan2
In the entire management domain
Do you want to continue (y/n) [n]?y
Vlan 2 deleted
```

Удаление VLAN-сети с интерфейса командно-программируемого коммутатора Cisco аналогично удалению команды из конфигурации маршрутизатора. В предыдущем примере была создана сеть vlan 2 на порте FastEthernet 0/3 с помощью команды:

```
Switch(config-if)#switchport access vlan 2
```

Для удаления с интерфейса VLAN-сети используется форма этой команды с ключевым словом **no** для интерфейса Fa 0/3:

```
Switch(config-if)#no switchport access vlan 2
```

Лабораторная работа: удаление конфигурации VLAN-сети

В этой лабораторной работе требуется создать базовую конфигурацию коммутатора и две виртуальных локальных сети VLAN. После этого VLAN-сетям следует присвоить имена и назначить им несколько портов. После этого их следует удалить. Следует попытаться удалить сеть VLAN1 и убедиться, что это невозможно. Пояснить причины этого.

Устранение ошибок в конфигурации VLAN-сети

В сетях, основанных на коммутации, одной из типичных ошибок является неправильное конфигурирование сетей VLAN. В табл. 9.2 описаны типичные проблемы, связанные с конфигурированием VLAN-сетей, которые могут возникнуть на маршрутизаторе или коммутаторе.

Таблица 9.2. Возможные проблемы в сети VLAN

Проблема	Возможные причины и действия, которые следует предпринять
Сеть функционирует медленно и ненадежно	Сетевой адаптер устройства неисправен. Следует проверить исправность аппаратных устройств. Установка дуплексного (*Full-duplex)* или полудуплексного режима (*half-duplex)* Ethernet выполнена с ошибками. Есть проблемы с кабелями. Следует проверить подсоединенные LED. Следует также проверить правильность подсоединения кабеля и не превышает ли длина кабеля допустимого максимального значения.
Подсоединенный терминал или модем не может осуществлять связь с маршрутизатором или коммутатором.	Неправильно сконфигурирован терминальный или консольный порт. Следует проверить правильность задания скорости передачи (бод/с) и соответствие форматов символов. Также следует проверить, не требуется ли на маршрутизаторе стандартный маршрут для связи с коммутатором в другой IP-подсети.
Устройства локальной VLAN не могут осуществлять связь с удаленными устройствами VLAN сети вне маршрутизатора.	Имеется проблема несовместимости VLAN-сетей. Следует проверить соответствие VLAN-сетей на обеих сторонах магистрали. Есть проблема с ISL. Следует проверить магистраль, использовать сеть VLAN1 и убедиться, что не было действительного обновления информации VTP-сервера.

При наличии проблемы с низкой пропускной способностью сети следует выяснить тип ошибки. Возможно, что неисправен сетевой адаптер. Сочетание ошибки *в контрольной последовательности фрейма (frame check sequence — FCS)* с наличием фреймов-карликов, как правило, указывает на несоответствие дуплексного режима; обычно причиной является неправильное автосогласование или несоответствие установок на концах канала. Рассмотрим следующие вопросы.

- Где возникла проблема — на ближнем или на удаленном конце канала? Следует помнить о том, что в работе канала участвует минимальное количество портов.
- Какой путь избирает пакет? Избирает ли он в качестве маршрута к другим коммутаторам магистраль (или немагистральный канал)?

Если количество коллизий, указываемое в выводе по команде **`show interface`** быстро возрастает, то проблема может состоять в перегруженности канала. Существует ошибочное мнение, что в сетях Ethernet с коммутацией отсутствуют коллизии. На самом деле коммутаторы минимизируют количество коллизий, но если они работают в полудуплексном режиме, то коллизии все же могут происходить, поскольку два устройства, работающие в полудуплексном режиме могут попытаться начать передачу одновременно.

Примером может служить сервер новостей, имеющий много клиентов, пытающихся передавать данные в одно и то же время. Потоки данных проходят через маршрутизатор и коммутатор к непосредственно подсоединенному серверу. В то же самое время сервер пытается сам передавать данные этим клиентам. В то время как сервер отвечает одному клиенту, другой клиент посылает запрос и в результате становится потенциально возможной коллизия. Единственным способом полностью исключить возможность коллизии является использование дуплексного режима. На рис. 9.16 показан процесс поиска и устранения ошибок в сети VLAN.

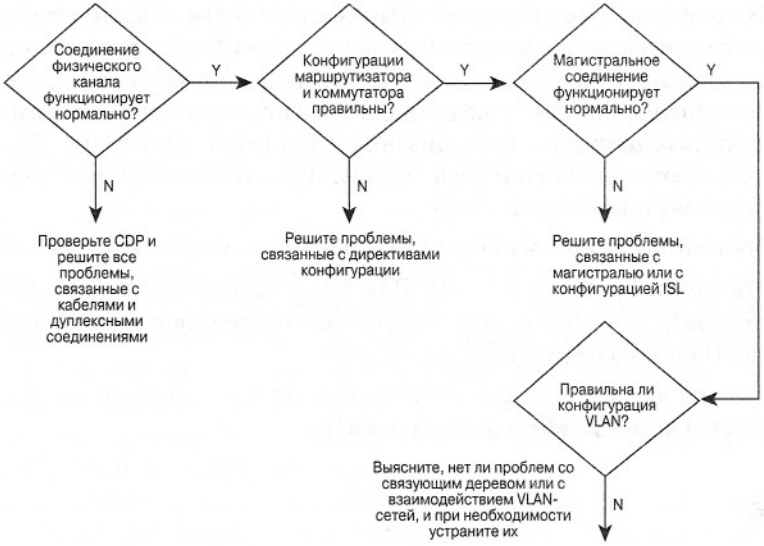

Рис. 9.16. Поиск и устранение ошибок в сети VLAN

В качестве примера рассмотрим ситуацию, когда одному устройству не удается установить связь с другим устройством. Ниже приводятся возможные способы решения этой проблемы.

- Сначала с помощью команды **show interface** следует проверить правильность задания IP-адресов, маски подсети и задание принадлежности к сети VLAN. Для предотвращения конфликтов следует проверить, что интерфейсы сконфигурированы с IP-адресами и масками подсетей в различных подсетях.
- Если узел находится в той же подсети где и интерфейс коммутатора, то следует убедиться, что интерфейс коммутатора и порт коммутатора, к которому подсоединен этот узел, назначены в одну и ту же виртуальную сеть. Для этого следует использовать команды **show interface** и **show port**.
- Если узел находится в другой подсети, то следует проверить, что стандартный шлюз (маршрут по умолчанию) на коммутаторе сконфигурирован с адресом маршрутизатора в той же самой подсети, где находится и интерфейс коммутатора. Для этого используется команда **show ip route**.
- Далее следует проверить состояние протокола связующего дерева на данном порте с помощью команды **show spantree** (для коммутатора Catalyst 1900) или **show spanning-tree vlan** (для коммутатора Catalyst 2950). Если порт находится в состоянии прослушивания или изучения топологии, то следует подождать его перехода в режим пересылки и попытаться вновь подсоединиться к узлу.
- Проверить правильность установок скорости и типа дуплексного режима на узле и соответствующем коммутаторе. Для этого следует использовать команду **show port**.
- Если подсоединенное устройство является конечной станцией, то следует выполнить следующие действия:
  - Включить на порте режим PortFast протокола связующего дерева. Для этого используется команда **set spantree portfast enable**. Следует помнить, что эти команды не поддерживаются на коммутаторах серии 2900. Применение PortFast немедленно переводит коммутатор в режим пересылки, пропуская режимы прослушивания и изучения топологии. (Не следует использовать эту функцию для соединения с устройствами, которые не являются конечными станциями)
  - Отключить на порте магистральный режим с помощью команды **set trunk**.
  - Отключить на порте каналы. Для этого используется команда **set port channel**. В этой команде следует указать действительный диапазон портов. Нельзя задавать только один порт.
- Следует проверить, что коммутатор изучает MAC-адрес узла. Для этого используется команда **show cam dynamic**.

Резюме

В данной главе было показано, что реализация VLAN-сетей предоставляет пользователю следующие преимущества:

- облегчается перемещение, добавление устройств и изменение их соединений друг с другом;

- достигается большая степень административного контроля вследствие наличия устройства, осуществляющего между сетями VLAN маршрутизацию на 3-м уровне;
- уменьшается потребление полосы пропускания по сравнению с ситуацией одного широковещательного домена;
- сокращается непроизводительное использование процессора CPU за счет сокращения пересылки широковещательных сообщений;
- для поиска и устранения ошибок в сетях VLAN были предложены приведенные ниже методы;
- конкретный подход к поиску и устранению ошибок в сетях VLAN;
- рассмотрены наиболее общие проблемы при конфигурировании VLAN-сетей и предложены методы поиска и устранения ошибок в них;
- предотвращение широковещательных штормов и предотвращение петель;
- описано применение команд поиска и устранения ошибок;

В дополнение к материалу, изложенному в настоящей главе, рекомендуется ознакомиться с лабораторными работами (e-Lab Activities), видеоклипами (Videos) и фотографиями (PhotoZooms), которые находятся на прилагаемом к книге компакт-диске.

Глоссарий

Виртуальная локальная сеть (virtual local-area network — VLAN). Группа устройств одной или более локальных сетей LAN, которые конфигурируются (с использованием управляющего программного обеспечения) таким образом, чтобы они могли осуществлять связь меду собой как если бы они находились в одном сегменте локальной сети, в то время как они фактически находятся в различных сегментах.

Дуплексная передача (full-duplex). Одновременная передача данных принимающим и передающим устройствами.

Контрольная последовательность фрейма (frame check sequence — FCS). Дополнительные символы, добавляемые к фрейму для контроля ошибок при передаче.

Магистральный протокол виртуальных локальных сетей(VLAN Trunking Protocol — VTP). Протокол VTP позволяет уменьшить объем административных работ в сети с коммутацией. При конфигурировании новой VLAN-сети на сервере VTP сеть VLAN распределяется по всем коммутаторам домена. Это избавляет от необходимости конфигурировать одну и ту же сеть VLAN во всех локальных сетях. Протокол VTP является фирменным протоколом Cisco, который имеется на большинстве коммутаторов Catalyst Cisco.

Полудуплексная передача (half-duplex). Передача данных между принимающей и передающей станциями только в одном направлении

Протокол обнаружения устройств Cisco (Cisco Discovery Protocol — CDP). Этот протокол содержит одну фирменную команду, позволяющую сетевому администратору получить доступ к набору конфигураций на других, непосредственно подсоединенных маршрутизаторах.

Широковещание (broadcast). Рассылка пакетов данных всем узлам сети. Широковещательные пакеты идентифицируются широковещательным адресом.

Контрольные вопросы

1. Для чего используются адреса VLAN?
   A. Для обеспечения масштабируемости сети
   B. Для обеспечения безопасности сети
   C. Для управления потоками данных
   D. Все вышеперечисленное
2. Что из перечисленного ниже характерно для сетей VLAN?
   A. Широковещательный домен
   B. Коллизионный домен
   C. Одновременно широковещательный и коллизионный домен
   D. Имя домена
3. Какова цель использования маршрутизаторов в топологиях сетей VLAN?
   A. Фильтрация широковещания
   B. Безопасность сети
   C. Управление потоками данных
   D. Все вышеперечисленное
4. Что означает фраза: "Микросегментация вместе с масштабируемостью"?
   A. Возможность увеличивать размер сети без создания коллизионных доменов
   B. Возможность подключения огромного количества станций к одному коммутатору
   C. Возможность широковещания одновременно на несколько узлов
   D. Все вышеперечисленное
5. Являясь базовым элементом VLAN-сетей, коммутаторы обладают интеллектуальными возможностями для выполнения следующих функций:
   A. Они группируют пользователей, порты и логические адреса в сети VLAN.
   B. Они выполняют фильтрацию и принимают решения о пересылке фреймов.
   C. Они осуществляют связь между коммутаторами и маршрутизаторами.
   D. Все вышеперечисленное.
6. Каждый сегмент _____, подсоединенный к порту _____ может быть причислен только к одной сети VLAN.
   A. Коммутатора; концентратора
   B. концентратора; маршрутизатора
   C. концентратора; коммутатора
   D. сети LAN; концентратора
7. Что из перечисленного ниже не является преимуществом статических VLAN-сетей?
   A. Они гарантируют безопасность.
   B. Их легко конфигурировать.

C. За ними легко осуществлять наблюдение (мониторинг).

D. Они автоматически конфигурируют порты при добавлении новых станций.

8. Что из перечисленного ниже не является критерием, на котором могут базироваться сети VLAN?

A. Идентификатор ID порта.

B. Протокол.

C. MAC-адрес.

D. Все вышеперечисленные элементы являются критериями на которых могут базироваться сети VLAN.

9. Что из перечисленного ниже является положительным результатом добавления сети VLAN? (Выбрать все правильные ответы).

A. Коммутаторы не требуют конфигурирования.

B. Возможно управление широковещанием.

C. Возможна защита конфиденциальных данных.

D. Могут быть удалены физические границы, препятствующие группировке пользователей.

10. Какие из приведенных ниже утверждений, относящиеся к виртуальным локальным сетям, не являются справедливыми?

A. Наиболее общими подходами к логической группировке пользователей в отдельные VLAN-сети являются фильтрация и идентификация фреймов.

B. Преимущества сетей VLAN включают в себя более надежную защиту сети и создание безопасных групп пользователей.

C. Мосты являются одним из базовых компонентов коммуникации в сетях VLAN.

D. VLAN-сети помогают осуществлять перераспределение нагрузки.

11. Какая функция коммутатора 3-го уровня позволяет легко управлять устройствами, расположенными в различных IP-подсетях?

A. Создание прозрачных мостовых соединений

B. Сегментация

C. Сокращение числа коллизионных доменов

D. Создание сетей VLAN

12. Какое из перечисленных ниже устройств требуется для передачи пакета из одной сети VLAN в другую?

A. Мост

B. Маршрутизатор

C. Коммутатор

D. Концентратор

13. На каком уровне эталонной модели OSI происходит добавление к фрейму тега?

A. На 1-м уровне

B. На 2-м уровне

C. На 3-м уровне

D. На 4-м уровне

14. _____ позволяет коммутаторам совместно использовать таблицы адресов, а _____ назначает определенные пользователем идентификаторы ID сетей VLAN каждому фрейму.

A. Присоединение тегов; пересылка фреймов

B. Идентификация фреймов; удаление фреймов

C. Фильтрация фреймов; присоединение тегов

D. Присоединение тегов; фильтрация фреймов

15. В чем состоит важность создания VLAN-сетей?

A. Становятся более простыми удаление, добавление устройств и другие перемены в сети.

B. Уменьшается объем передаваемых служебных данных.

C. Маршрутизатор быстрее осуществляет коммутацию.

D. A и B.