Лекция 11 Виртуальные ЛВС

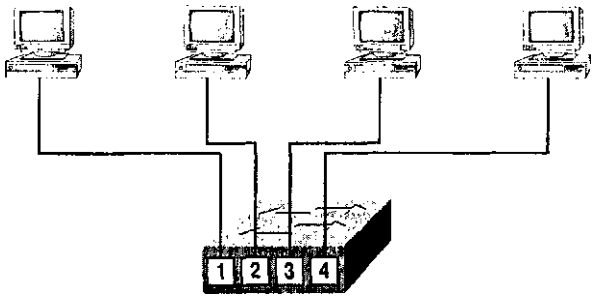
Виртуальная локальная сеть (Virtual Local Area Network, VLAN) — это логическая группировка пользователей сети и ресурсов, подключенных к административно определенным портам на коммутаторе уровня 2. Виртуальные ЛВС позволяют создавать в пределах коммутатора меньшие широковещательные домены через назначение разных портов коммутатора разным подсетям. Виртуальная ЛВС становится как бы отдельной подсетью или широковещательным доменом, и при широковещательной рассылке фреймов они коммутируются только между портами одной и той же виртуальной ЛВС.

Применение виртуальных ЛВС избавляет от необходимости формировать рабочие группы в зависимости от физического расположения устройств и пользователей. Виртуальные ЛВС можно организовать по признаку физического расположения устройств, по выполняемым функциям, отделу организации и даже по используемому приложению или протоколу, вне зависимости от местонахождения ресурсов или пользователей.

Преимущества виртуальных ЛВС

Коммутаторы уровня 2 сегментируют коллизионные домены, но только маршрутизаторы могут сегментировать широковещательные домены. Однако виртуальные ЛВС вполне способны сегментировать широковещательные домены в коммутируемых сетях уровня 2. При этом на уровне 2 коммутируемой объединенной сети возникает потребность в маршрутизаторах для связи между разными виртуальными ЛВС.

Создание виртуальных ЛВС в объединенной сети имеет много преимуществ. В коммутируемой сети уровня 2 сеть является *плоской,* как показано на рис. 11.1. Каждый пакет широковещательной рассылки воспринимается всеми устройствами сети независимо от того, нужны устройству эти данные или нет.



Каждый участок имеет свой коллизионный домен.
Все участки находятся в одном широковещательном домене.

Рис. 11.1. Плоская структура сети

В плоской сети меры безопасности ограничиваются паролями, и каждому пользователю доступны любые устройства. Невозможно запретить устройствам производить рассылку, а пользователям пытаться отвечать на нее. Безопасность осуществляется паролями на серверах и других устройствах.

Создание виртуальных ЛВС помогает решить много проблем коммутации уровня 2.

Контроль широковещательной рассылки

Широковещание может осуществляться в любом протоколе, но его частота зависит от протокола, от работающих в объединенной сети приложений и от того, как все эти возможности используются. Виртуальные ЛВС способны выделять меньшие широковещательные домены, т.е. позволяют запретить рассылку приложения на те участки, которые его не будут использовать.

Хотя более старые приложения создавались с таким расчетом, чтобы уменьшить занимаемую ими полосу пропускания, новое поколение приложений использует максимально широкую полосу пропускания. Это мультимедийные приложения, интенсивно использующие широковещательные и многоадресные рассылки. Ненадежное оборудование, недостаточная сегментация и плохо организованные брандмауэры могут усугубить проблему с приложениями, активно использующими рассылку.

Приложения, требующие широкой полосы пропускания, добавляют в проектирование сети новый фактор, потому что рассылки могут транслироваться через коммутируемую сеть. Маршрутизаторы по умолчанию передают вещание только в пределах исходной сети, а коммутаторы уровня 2 направляют рассылку всем участкам. Такая сеть называется плоской, потому что составляет один домен рассылки.

Обязанность администратора — обеспечить правильную сегментацию сети, чтобы проблемы на одном сетевом участке не распространялись по всей объединенной сети. Самым эффективным средством для этого являются коммутация и маршрутизация. В связи с тем, что коммутаторы стали более приемлемыми по цене, многие компании меняют плоские сети, состоявшие из концентратора и маршрутизатора, на чисто коммутируемую сеть и виртуальные ЛВС. Самое большое достоинство коммутаторов с заданными виртуальными ЛВС заключается в том, что все устройства виртуальной ЛВС входят в один широковещательный домен и получают все рассылки. По умолчанию фильтруются рассылки всех портов, находящихся на коммутаторе и не принадлежащих одной и той же виртуальной ЛВС.

Для того чтобы рассылка не передавалась по всей объединенной сети, нужен маршрутизатор, коммутаторы уровня 3 или модули переключения маршрутов (Route Switch Modules, RSM) с коммутаторами для обеспечения связи между сетями (виртуальными ЛВС).

Безопасность

В плоской объединенной сети безопасность реализуется подключением концентраторов и коммутаторов к маршрутизаторам. Далее безопасность обеспечивается маршрутизатором, но в этом кроются три серьезные проблемы:

- Всякий пользователь, подключающийся к физической сети, имеет доступ к сетевым ресурсам этой физической ЛВС.
- Пользователь может подключиться к анализатору сети через концентратор и наблюдать за всеми передачами данных в сети
- Пользователи могут присоединиться к рабочей группе, просто включив свою рабочую станцию в имеющийся концентратор

Благодаря использованию виртуальных ЛВС и созданию нескольких групп рассылки администраторы могут контролировать каждый порт и каждого пользователя. Пользователи уже не могут просто подключить свою рабочую станцию к концентратору и получить доступ к сетевым ресурсам. Администратор контролирует каждый порт и доступные ему ресурсы.

Поскольку существует возможность создания групп в соответствии с необходимыми пользователю ресурсами сети, то можно настроить коммутаторы так, чтобы они сообщали терминалу управления сети о каждом несанкционированном доступе к сетевым ресурсам. Если необходимо иметь связь между виртуальными ЛВС, можно добавить ограничения и на маршрутизаторе. Также можно использовать ограничения и на аппаратных адресах, протоколах и приложениях.

Гибкость и масштабируемость

Виртуальные ЛВС обеспечивают большую гибкость сети, позволяя ограничивать доступ или добавлять пользователей в домен рассылки независимо от их физического расположения. Коммутаторы уровня 2 считывают фреймы только с целью фильтрации, они не обращают внимания на протокол сетевого уровня. Это позволяет коммутатору пересылать все рассылки. Но при создании виртуальных ЛВС, в сущности, создаются отдельные широковещательные домены. Широковещательные рассылки из узла одной виртуальной ЛВС не пересылаются на порты, сконфигурированные в другой виртуальной ЛВС. При назначении коммутируемых портов или пользователей группам виртуальных ЛВС или группе объединенных коммутаторов (иначе называемой ***структурой коммутаторов)*** их можно добавлять в домен рассылки независимо от физического расположения. Это позволяет предотвратить рассылочные штормы, вызываемые несоответствующей сетевой платой или приложением при трансляции на всю объединенную сеть.

Когда виртуальная ЛВС становится чрезмерно велика, можно создать еще несколько виртуальных ЛВС для того, чтобы рассылка не потребляла слишком много пропускной способности. Чем меньше пользователей в виртуальной ЛВС, тем меньше чувствуется влияние рассылок.

Свернутая магистраль и виртуальная ЛВС

Для понимания того, как виртуальная ЛВС воспринимает коммутатор, следует сначала рассмотреть обычную свернутую опорную сеть. На рис. 11.2 показана свернутая опорная сеть, состоящая из подключенных к маршрутизатору физических ЛВС.

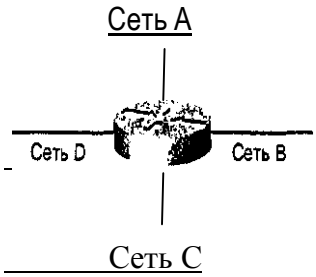


Рис. 11.2. Подключенные к маршрутизатору физические ЛВС

Каждая сеть подключена к маршрутизатору и имеет свой логический сетевой номер. Каждый узел, подключенный к какой-либо физической сети, должен иметь такой же сетевой код, чтобы поддерживать связь по объединенной сети. Теперь посмотрим, какие функции выполняет коммутатор. На рис. 11.3 показано, как коммутаторы устраняют физическую границу.

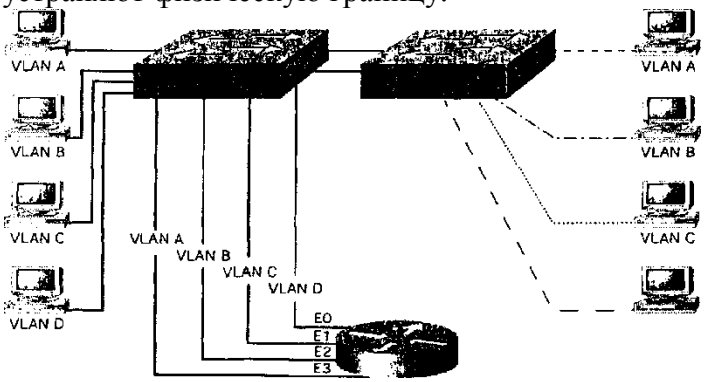


Рис. 11.3. Устранение физической границы коммутаторами

Коммутаторы обеспечивают большую гибкость и масштабируемость, чем та, которой сами по себе обладают маршрутизаторы, потому что коммутаторы определяют виртуальные ЛВС сети и назначения портов виртуальных ЛВС. Можно объединять пользователей в группы но интересам, которые называются группами виртуальных ЛВС.

Значит ли это, что маршрутизаторы больше не. нужны? Нет. Обратите внимание, что на рис. 11.3 показаны четыре виртуальные ЛВС, или домена рассылки. Узлы в пределах каждой виртуальной ЛВС могут связываться между собой, но не с другой виртуальной сегыо или ее узлом. Находясь в виртуальной ЛВС, узлы как бы находятся в свернутой опорной сети, что изображено на рис. 11.2. Что нужно сделать узлам, изображенным на рисунке, чтобы связаться с узлом другой сети? Им нужно пройти через маршрутизатор или другое устройство уровня 3, как и при их организации для связи в виртуальной ЛВС, что изображено на рис. 11.3. Связь между виртуальными ЛВС, как и в физических сетях, должна проходить по устройству уровня 3.

Масштабирование блока коммутаторов

Описанные блоки коммутаторов представляют собой коммутатор или группу коммутаторов, обеспечивающих доступ пользователей. Затем коммутаторы соединяются с коммутаторами уровня распределения, которые, в свою очередь, организуют маршрутизацию и распределение в виртуальной ЛВС.

Для определения количества виртуальных ЛВС, которое можно создать в блоке коммутаторов, следует знать следующие параметры:

- Структура трафика
- Используемые приложения

- Сетевое управление
- Общность группы
- Схема IP-адресации

Рекомендуется использовать соотношение между виртуальными ЛВС и подсетями один к одному. Если, например, в здании 2000 пользователей, то для создания виртуальных ЛВС Нужно знать, как пользователи подразделяются по подсетям. Если бы в каждой подсети было 1000 пользователей, что абсурдно, то нужно было бы создать лишь две виртуальные ЛВС. Если бы в каждой подсети было только 100 пользователей, то организуется около 20 или больше виртуальных ЛВС.

На практике лучше сперва сформировать группы доменов рассылки (т.е. виртуальные ЛВС), а потом создать маску подсети, соответствующую потребностям. Но это не всегда возможно, и чаще всего приходится создавать виртуальные ЛВС в уже сконфигурированной сети.

Определение границ виртуальных ЛВС

При создании блока коммутаторов следует знать два основных типа виртуальных ЛВС:

- Сквозные виртуальные ЛВС
- Локальные виртуальные ЛВС

Сквозные виртуальные ЛВС

Сквозные виртуальные ЛВС соединяют между собой все устройства коммутаторов; все коммутаторы в сквозных ЛВС знают о всех сконфигурированных виртуальных сетях. Эта конфигурация позволяет создавать группы на основе функций, проектов, отделов и т.п.

Самое большое достоинство сквозных ЛВС заключается в том, что пользователей можно отнести к определенной виртуальной ЛВС вне зависимости от их физического расположения. Администратор определяет порт, к которому подключен пользователь как участник виртуальной ЛВС. Если пользователь перемещается, администратор определяет ему новый порт как участнику той же самой виртуальной сети. Согласно правилу 80/20, задача администратора при создании сквозных виртуальных ЛВС — обеспечить, чтобы 80% сетевого трафика оставалось локальным, т.е. в пределах виртуальной ЛВС. Лишь 20% или меньше могут выходить за пределы виртуальной ЛВС.

Локальные виртуальные ЛВС

Локальные виртуальные ЛВС конфигурируются в соответствии с физическим расположением, а не на основе функций, проектов, отделов и т.п., как сквозные виртуальные ЛВС. Локальные виртуальные ЛВС используются в организациях, имеющих централизованные блоки серверов и больших ЭВМ, потому что в этом случае трудно обслуживать сквозные виртуальные ЛВС. Другими словами, когда правило 80/20 сменяется правилом 20/80, сквозные виртуальные ЛВС поддерживать труднее, чем локальные виртуальные сети.

В отличие от сквозных виртуальных ЛВС локальные сети конфигурируются в соответствии с пространственным расположением; единицей расположения может быть здание или только кабинет в здании, в зависимости от размера коммутаторов. Пространственно организованные виртуальные ЛВС проектируются, когда организация использует централизованные ресурсы, например ферму серверов. Пользователи проводят большую часть своего времени в диалоге с этими централизованными ресурсами, и 20% (или меньше) времени находятся в локальной сети. Отсюда следует вывод, что 80% трафика пересекает устройство уровня 3. На первый взгляд это кажется неэффективным.

В связи с тем, что устройства уровня 3 становятся все быстрее, локальная виртуальная сеть имеет возможность использовать наиболее высокоскоростные устройства уровня 3, справляющиеся с большим объемом трафика. Преимущество такой структуры в том, что пользователям предлагается заранее определенный, последовательный способ получения ресурсов. Но с менее мощным устройством уровня 3 такую конфигурацию создать невозможно, поэтому она требует вложения больших средств.

Группы виртуальных ЛВС

Создав виртуальные ЛВС, следует назначить им порты коммутации. Есть два типа конфигураций портов виртуальных ЛВС: статическая и динамическая. Статическая виртуальная ЛВС требует меньше труда при создании, но труднее для обслуживания. Динамическая виртуальная ЛВС, наоборот, требует больше работы при своей организации, но более проста в обслуживании.

Статические виртуальные ЛВС

В *статической виртуальной ЛВС* администратор назначает ей коммутационные порты, и это сопоставление остается постоянным, пока администратор не изменит назначение порта. Это обычный и самый безопасный способ создания виртуальных ЛВС. Такую конфигурацию проще организовать и контролировать, перемещение же пользователей контролируется, в сущности, тем, что просто запираются двери сетевых центров. Для удобства можно воспользоваться программным обеспечением управления сетью, но это необязательно.

Динамические виртуальные ЛВС

Если администратор согласен немного больше потрудиться в самом начале и определить в базе данных аппаратные адреса всех устройств, то можно обеспечить динамическое назначение виртуальной ЛВС в объединенной сети. Хорошее программное обеспечение управления позволяет разрешать аппаратные (MAC) адреса, протоколы или даже приложения для создания ***динамических виртуальных ЛВС.***

Предположим, что в централизованное приложение управления виртуальной ЛВС введены MAC-адреса. Если после этого к неназначенному порту коммутации подключается узел, база данных управления виртуальной сети находит аппаратный адрес и назначает и настраивает порт коммутации для соответствующей виртуальной ЛВС. Это упрощает администратору управление и настройку. Если пользователь перемещается, коммутатор автоматически определит его в нужную виртуальную ЛВС. Но для установки базы данных требуется большая работа администратора на начальном этапе.

Администраторы Cisco могут использовать службу сервера политик управления виртуальными ЛВС (VLAN Management Policy Server, VMPS) для создания базы данных MAC-адресов, которые могут быть задействованы для динамической адресации виртуальных сетей. VMPS — это база данных, сопоставляющая MAC-адреса с виртуальными ЛВС.

Настройка статических виртуальных ЛВС

Для конфигурации виртуальных ЛВС на коммутаторе служит команда vlan [vlan#] name [vlan-name]:

```
>en
# config t
Enter configuration commands, one per line, End with CNTL/Z
(config)#hostname 1900EN
Switch (config)#vlan 2 name sales
Switch (config)#vlan 3 name marketing
Switch (config)#vlan 4 name mie
Switch (config)#exit
```

Создав нужные виртуальные ЛВС, с помощью команды show vlan можно просмотреть их конфигурации. В выходных данных ниже видно, что по умолчанию все порты на коммутаторе расположены в виртуальной ЛВС 1.