Тема 9 Виртуальные локальные сети - VLAN

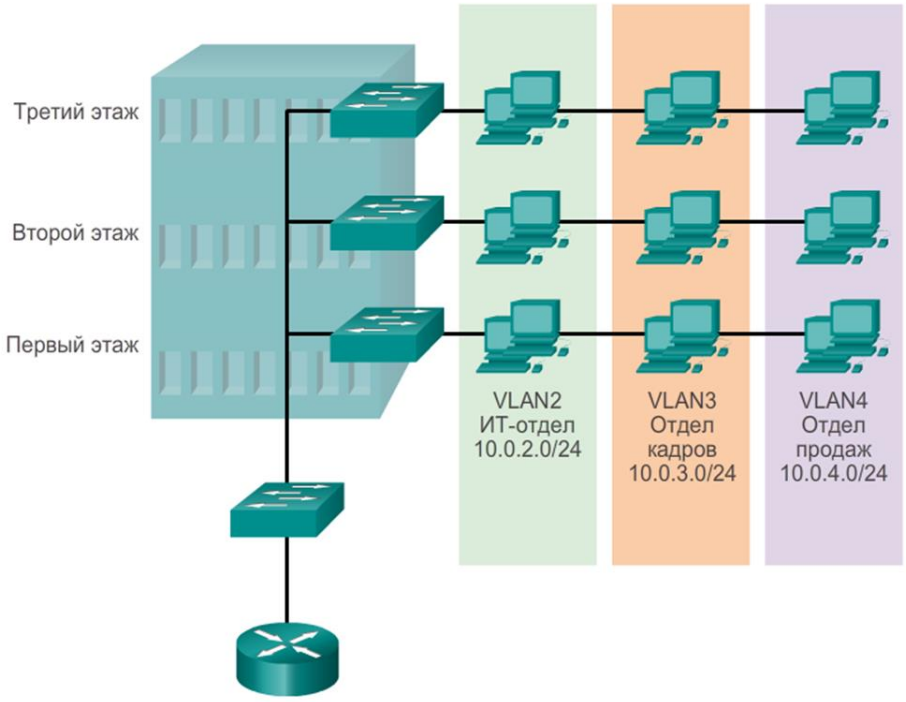
Производительность сети является важным фактором эффективности работы организации. Одной из технологий повышения производительности сети является разделение крупных широковещательных доменов на более мелкие. Маршрутизаторы устроены таким образом, что блокируют широковещательный трафик на интерфейсе. При этом маршрутизаторы обычно имеют ограниченное количество интерфейсов LAN. Основная роль маршрутизатора заключается в передаче информации между сетями, а не в предоставлении оконечные устройства доступа к сети.

Предоставление доступа в локальную сеть обычно обеспечивается коммутатором уровня доступа. Для уменьшения размера широковещательных доменов на коммутаторе 2-го уровня, как и на устройстве 3-го уровня, можно создать сеть VLAN. Сети VLAN обычно включаются в проекты сети, для того чтобы сеть облегчала процесс достижения целей организации. Несмотря на то, что сети VLAN в основном используются в коммутируемых локальных сетях, современные реализации VLAN способны функционировать также в муниципальных (MAN) и глобальных (WAN) сетях.

Общие сведения о виртуальных локальных сетях

В коммутируемых объединённых сетях сети VLAN обеспечивают гибкость сегментации и организации. Сети VLAN позволяют сгруппировать устройства внутри локальной сети. Группа устройств в пределах сети VLAN взаимодействует так, будто устройства подключены с помощью одного провода. Сети VLAN основываются не на физических, а на логических подключениях.

Сети VLAN позволяют администратору производить сегментацию по функциям, проектным группам или областям применения, вне зависимости от физического расположения пользователя или устройства. Устройства в пределах сети VLAN работают таким образом, будто находятся в собственной независимой сети, даже если делят одну общую инфраструктуру с другими VLAN. Любой порт коммутатора может принадлежать сети VLAN. Одноадресные, широковещательные и многоадресные пакеты пересылаются и рассылаются только к конечным станциям в пределах той сети VLAN, которая является источником этих пакетов. Каждая сеть VLAN считается отдельной логической сетью, и пакеты, адресованные станциям, не принадлежащим данной сети VLAN, должны пересылаться через устройство, поддерживающее маршрутизацию.



Сеть VLAN создаёт логический широковещательный домен, который может охватывать несколько физических сегментов LAN. Разделяя крупные широковещательные домены на более мелкие сети, VLAN повышают производительность сети. Если устройство в одной сети VLAN передаёт широковещательный кадр Ethernet, то этот кадр получают все устройства в рамках этой VLAN, устройства же в других сетях VLAN этот кадр не получают.

Сети VLAN позволяют реализовывать политику обеспечения доступа и безопасности, учитывая интересы различных групп пользователей. Каждый порт коммутатора может быть назначен только одной сети VLAN (за исключением порта, подключённого к IP-телефону или к другому коммутатору).

Преимущества VLAN

Производительность пользователей и адаптивность сети играют важную роль в процветании и успехе компании. Сети VLAN облегчают процесс проектирования сети, обеспечивающей помощь в выполнении целей организации. К основным преимуществам использования VLAN относятся:

- **Безопасность**: группы, обладающие уязвимыми данными, отделены от остальной части сети, благодаря чему снижается вероятность утечки конфиденциальной информации. Как показано на рисунке, компьютеры преподавателей находятся в сети VLAN 10 и полностью отделены от трафика данных учащихся и гостей.
- **Снижение расходов**: благодаря экономии на дорогих обновлениях сетевой инфраструктуры и более эффективному использованию имеющейся полосы пропускания и восходящих каналов происходит снижение расходов.
- **Повышение производительности**: разделение однородных сетей 2-го уровня на несколько логических рабочих групп (широковещательных

доменов) уменьшает количество лишнего сетевого трафика и повышает производительность.

- **Уменьшенные широковещательные домены**: разделение сети на сети VLAN уменьшает количество устройств в широковещательном домене. Сеть, показанная на рисунке, состоит из шести компьютеров и трёх широковещательных доменов: для преподавателей, для учащихся и гостевого домена.
- **Повышение производительности ИТ-отдела**: сети VLAN упрощают управление сетью, поскольку пользователи с аналогичными требованиями к сети используют одну и ту же сеть VLAN. При введении в эксплуатацию нового коммутатора на назначенных портах реализуются все правила и процедуры, уже применённые в этой конкретной VLAN. Также ИТ-специалистам легче определять функцию сети VLAN, назначая ей соответствующее имя. На данном рисунке для простой идентификации сеть VLAN 10 была названа «Для преподавателей», VLAN 20 — «Для учащихся» и VLAN 30 — «Гостевая».
- **Упрощённое управление проектами и приложениями**: сети VLAN объединяют пользователей и сетевые устройства для соответствия деловым или географическим требованиям сети. Управление проектом и работа на прикладном уровне упрощены благодаря использованию разделения функций. Пример такой прикладной задачи — платформа разработки приложений для электронного обучения преподавателей.

Каждая VLAN в коммутируемой сети относится к какой-либо IP-сети; таким образом, в проекте VLAN нужно учитывать реализацию иерархической системы сетевой адресации. Иерархическая адресация подразумевает упорядоченное назначение номеров IP-сети сегментам или сетям VLAN с учетом работы сети в целом. Как показано на рисунке, блоки смежных сетевых адресов резервируются и настраиваются на устройствах в определённой области сети.

Типы сетей VLAN

В современных сетях используется множество различных типов сетей VLAN. Некоторые типы VLAN определяются классами трафика. Другие типы VLAN обусловлены функциями, которые они выполняют.

Виртуальная локальная сеть для данных

Виртуальная локальная сеть для данных — это сеть VLAN, которая настроена специально для передачи трафика, генерируемого пользователем. Сеть VLAN, передающая голосовой трафик или трафик управления, не является сетью VLAN для передачи данных. Рекомендуется отделять голосовой и управляющий трафик от трафика данных. VLAN для передачи данных иногда называют пользовательской сетью VLAN. Сети VLAN для данных используются для разделения сети на группы пользователей или устройств.

Сеть VLAN по умолчанию

Все порты коммутатора становятся частью VLAN по умолчанию после первоначальной загрузки коммутатора. Порты коммутатора, находящиеся в сети VLAN по умолчанию, являются частью одного широковещательного домена. Благодаря этому любое устройство, подключённое к любому порту коммутатора,

может обмениваться данными с другими устройствами на других портах коммутатора. Сетью VLAN по умолчанию для коммутаторов Cisco установлена VLAN 1. На рисунке команда **show vlan brief** была выполнена на коммутаторе, настроенном по умолчанию. Обратите внимание, что на все порты по умолчанию назначены сети VLAN 1.

VLAN 1 поддерживает все функции любой сети VLAN, однако её нельзя переименовать или удалить. По умолчанию весь управляющий трафик 2-го уровня связан с сетью VLAN 1.

Native VLAN

Сеть native VLAN назначена транковому порту 802.1Q. Транковые порты — это каналы между коммутаторами, которые поддерживают передачу трафика, связанного с более чем одной сетью VLAN. Транковый порт 802.1Q поддерживает трафик, поступающий от нескольких VLAN (тегированный трафик), а также трафик, который поступает не от VLAN (нетегированный трафик). Тегированным называется трафик, для которого в исходный заголовок кадра Ethernet вставлен 4-байтовый тег, определяющий сеть VLAN, к которой относится этот кадр. Транковый порт 802.1Q размещает нетегированный трафик в сети native VLAN, которой по умолчанию является VLAN 1.

Сети native VLAN определены в спецификации IEEE 802.1Q для обеспечения обратной совместимости с нетегированным трафиком, характерным для устаревших сценариев локальных сетей. Сеть native VLAN служит общим идентификатором на противоположных концах транкового канала.

Рекомендуется настроить native VLAN как неиспользуемую VLAN, отличающуюся от сети VLAN 1 и других VLAN. Фактически принято выделять фиксированную VLAN для выполнения роли сети native VLAN для всех транковых портов в коммутируемом домене.

Управляющая VLAN

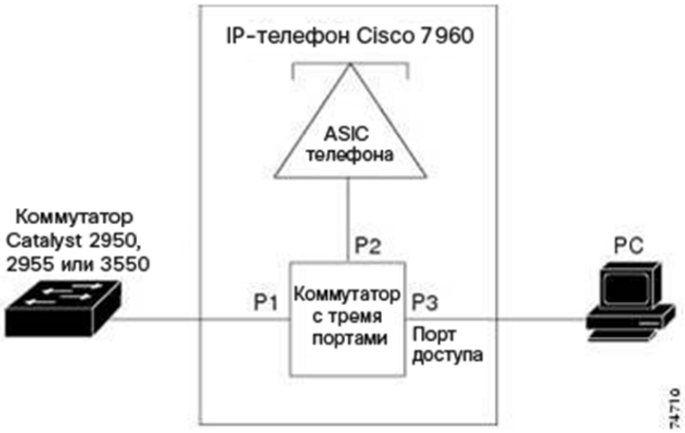
Управляющая VLAN — это любая сеть VLAN, настроенная для доступа к функциям управления коммутатора. Сеть VLAN 1 по умолчанию является управляющей VLAN. Для создания управляющей VLAN интерфейсу SVI коммутатора данной VLAN назначаются IP-адрес и маска подсети, благодаря чему коммутатором можно управлять через протоколы HTTP, Telnet, SSH или SNMP. Поскольку в исходной настройке коммутатора Cisco VLAN 1 является сетью VLAN по умолчанию, VLAN 1 не следует использовать в качестве управляющей VLAN.

Все порты назначены сети VLAN 1 по умолчанию. Ни одна native VLAN не назначена явно, и ни одна другая сеть VLAN не является активной. Таким образом, сети native VLAN и управляющая VLAN совпадают. Подобная настройка считается угрозой безопасности.

Для поддержки передачи голоса по IP (VoIP) требуется отдельная сеть VLAN. Для VoIP-трафика требуется:

- гарантированная полоса пропускания для обеспечения высокого качества голосовой передачи;
- приоритет передачи перед другими типами сетевого трафика;
- возможность маршрутизации в обход перегруженных участков;
- задержка менее 150 мс по всей сети.

Для того чтобы соответствовать этим требованиям, вся сеть должна быть специально спроектирована для поддержки VoIP.



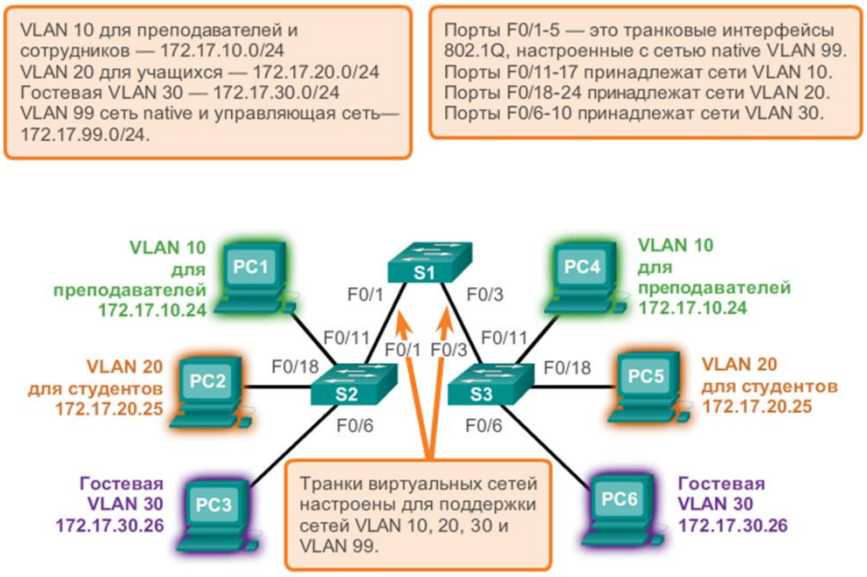
Виртуальные локальные сети в среде с множеством коммутаторов

Транк — это канал типа «точка-точка» между двумя сетевыми устройствами, который поддерживает более одной сети VLAN. Транк виртуальных сетей расширяет сети VLAN по всей сети. Cisco поддерживает стандарт IEEE 802.1Q для координации транков в интерфейсах Fast Ethernet, Gigabit Ethernet и 10-Gigabit Ethernet.

Использование сетей VLAN без транковых каналов существенно снижает полезные возможности VLAN. Транки виртуальных сетей обеспечивают распространение всего трафика VLAN между коммутаторами так, чтобы устройства, находящиеся в одной сети VLAN, но подключённые к разным коммутаторам, могли обмениваться данными без вмешательства маршрутизатора.

Транк виртуальных сетей не принадлежит какой-либо определённой сети VLAN, а, скорее, является «кабельным каналом» передачи многих VLAN между коммутаторами и маршрутизаторами. Транк может также использоваться между сетевым устройством и сервером или другим устройством, оснащённым соответствующим сетевым адаптером с поддержкой 802.1Q.

На рисунке каналы между коммутаторами S1 и S2, а также между S1 и S3 настроены для передачи трафика, отправляемого по всей сети от VLAN 10, 20, 30 и 99. Данная сеть не сможет работать без транковых каналов VLAN.



Сети без VLAN

При нормальной эксплуатации, когда коммутатор получает широковещательный кадр на одном из своих портов, он пересылает кадр из всех портов, кроме того, на котором он был получен. В анимации на рис. 1 вся сеть настроена в одной подсети (172.17.40.0/24), сети VLAN не настроены. В результате, когда компьютер преподавателя (PC1) отправляет широковещательный кадр, коммутатор S2 отправляет этот широковещательный кадр из всех своих портов. В конечном итоге вся сеть получает широковещательную рассылку, поскольку сеть является широковещательным доменом.

Сеть с VLAN

Сеть была разделена на сегменты с помощью двух VLAN. Устройства для преподавателей были назначены сети VLAN 10, а устройства учащихся — сети VLAN 20. Когда из компьютера преподавателя (PC1) отправляется широковещательный кадр на коммутатор S2, коммутатор пересылает кадр только на те порты коммутатора, которые настроены для поддержки VLAN 10.

Порты, обеспечивающие соединение между коммутаторами S1 и S2 (порт F0/1) и между коммутаторами S1 и S3 (порт F0/3), являются транковыми каналами и настроены для поддержки всех VLAN в сети.

Когда коммутатор S1 получает широковещательный кадр через порт F0/1, он пересылает широковещательный кадр из единственного другого порта, настроенного для поддержки сети VLAN 10, т.е. из порта F0/3. При получении коммутатором S3 широковещательного кадра через порт F0/3 он пересылает широковещательный кадр из другого порта, настроенного для поддержки сети VLAN 10, т.е. из порта F0/11. Широковещательный кадр прибывает на единственный другой компьютер в сети, настроенный для VLAN 10, т.е. на компьютер для преподавателей PC4.

В случае когда сети VLAN реализованы на коммутаторе, передача одноадресного, многоадресного и широковещательного трафика от узла в определённой VLAN ведется устройствами в пределах этой сети VLAN.