



Виртуальные ЛВС

В каких ситуациях полезны виртуальные ЛВС?

Виртуальная ЛВС (VLAN или ВЛВС) представляет собой область широковещания (broadcast domain), заданную программными средствами. Коммутаторы пересылают широковещательные пакеты (а также пакеты с групповыми и неизвестными адресами) внутри виртуальной ЛВС, но не между виртуальными сетями.

VLAN являются фундаментом при построении иерархических (многоуровневых) сетей. В сетях на базе концентраторов и маршрутизаторов иерархия организуется автоматически – каждый сегмент Ethernet или кольцо token ring представляют собой область широковещания, ограниченную портом маршрутизатора. В сетях TCP/IP областями широковещания являются также подсети IP.

В сетях, построенных полностью на базе коммутаторов, каждое устройство имеет собственный сегмент Ethernet или token ring.

- ♦ Должно ли каждое устройство иметь собственную подсеть IP и использовать маршрутизацию для каждого кадра? Поскольку маршрутизация более сложна, нежели коммутация ЛВС, задержки при маршрутизации превышают задержки при коммутации. Использование маршрутизации для всего трафика (даже в случаях применения высокопроизводительных коммутаторов сетевого уровня) ведет к снижению производительности сети.
- ♦ Может быть достаточно организации большой «плоской» сети без использования маршрутизации? В этом случае каждое устройство сети будет получать все широковещательные пакеты, а также все пакеты с групповыми и неизвестными адресами. В больших сетях столь вольная рассылка широковещательных и групповых пакетов приведет к значительному расходу полосы и интенсивной нагрузке на все сетевые станции из-за необходимости обработки всех широковещательных и групповых пакетов.

Использование VLAN позволяет найти компромисс между этими полюсами. В сетях с ВЛВС коммутация используется внутри каждой области широковещания, а для связи между этими доменами служит маршрутизация.

Организация VLAN не требуется для каждой коммутируемой сети. Множество сетей достаточно невелики для того, чтобы обеспечивать высокую производительность при использовании одной области широковещания (домена). В других случаях маршрутизация используется только для связи между коммутаторами, каждый из которых образует область широковещания.

Общие вопросы, касающиеся ВЛВС

По мере распространения коммутации ЛВС варианты организации VLAN начали расти как грибы после дождя. При этом реализации разных фирм зачастую весьма сильно различаются и просто несовместимы между со-

бой¹. Существует несколько причин возникновения такой ситуации:

- ♦ существуют стандарты VLAN, но они достаточно ограничены. Поэтому производители коммутаторов предлагают фирменные реализации VLAN, что ведет к значительному разбросу возможностей.
- ♦ механизмы VLAN должны быстро проверять заголовки кадров и принимать достаточно сложные решения на основе такого анализа, внося минимальную задержку в передачу кадров. Производители оборудования, разработав контроллеры коммутации и многопортовые коммутаторы на базе этих контроллеров, уже не хотят вносить фундаментальные изменения в свои разработки, поскольку такие изменения замедляют продвижение продукции на рынок.

VLAN на базе множества коммутаторов

Некоторые из механизмов VLAN реализуются только в масштабах одного коммутатора. Этого зачастую бывает достаточно при использовании коммутаторов для связи между разделяемыми сегментами на базе традиционных концентраторов. Но в сетях, полностью построенных на базе коммутаторов, такой подход менее эффективен, поскольку все устройства, подключенные к одному коммутатору, могут находиться в одной области широковещания практически для любых конфигураций сети.

Во многих организациях все (или большая часть) серверов собраны вместе, а большинство пользователей размещается в одном или нескольких зданиях. Очевидно, что в таких случаях серверы и пользователи скорее всего будут подключены к портам разных коммутаторов. Передача данных между такими пользователями и сервером может осуществляться двумя способами:

- ♦ сервер и пользователь находятся в разных ВЛВС и связь между ними осуществляется с использованием маршрутизатора;
- ♦ сервер и пользователь включены в одну виртуальную ЛВС, существующую на базе нескольких коммутаторов.

С этим тесно связана задача обеспечения мобильности пользователей. Некоторые фирмы преподносят свои VLAN как решения, обеспечивающие полную поддержку мобильности пользователей, – при организации VLAN вы можете добавлять или переносить пользовательские станции без повторной настройки адресов сетевого уровня. Это правильно, но более фунда-

¹ Более того, зачастую даже у одной фирмы появляется несколько несовместимых между собой реализаций VLAN.

ментальным преимуществом VLAN является изоляция широковещательного трафика. Во многих сетях серверы DHCP автоматически выделяют пользователям IP-адреса, однако, использование DHCP возможно только в рамках одной IP-сети, а для других протоколов вопрос сохранения сетевых адресов остается прерогативой VLAN. Естественно, что при этом требуется сохранение принадлежности пользователя к VLAN даже после подключения к порту другого коммутатора.

Теоретически VLAN может содержать множество коммутаторов за счет выделения специального транка для каждой виртуальной ЛВС. Такое решение может оказаться дорогим и неповоротливым. Альтернативой этому являются теговые протоколы (*tagging protocol*), обеспечивающие специальные идентификаторы (теги) для каждого кадра, передаваемого по сети. Теги позволяют коммутатору на другой стороне соединения передавать кадры в соответствующие VLAN. Некоторые из теговых протоколов связаны с решениями определенных фирм, другие же основываются исключительно на стандартах общего пользования.

Пропускная способность и задержки VLAN

Как и все коммуникационные технологии, разные реализации VLAN отличаются параметрами производительности. Хорошим способом проверки данных о производительности различных коммутаторов являются отчеты об анализе производительности, публикуемые ведущими сетевыми журналами. Обращая внимание на методику тестирования и способы представления результатов, можно много узнать о возможностях оборудования различных фирм. Не следует только забывать, что достаточно часто публикуются результаты «тестов», спроектированных специально для того или иного оборудования, с целью показать его превосходство.

VLAN с поддержкой разных технологий и преобразования скоростей.

Реализации VLAN на базе множества коммутаторов должны поддерживать различные типы MAC-адресов в рамках одной VLAN, поскольку транки между коммутаторами почти всегда используют скоростные технологии типа Fast Ethernet, ATM, Gigabit Ethernet или FDDI, тогда как для подключения станций используются более медленные традиционные технологии Ethernet, Fast Ethernet или token ring. То же самое относится и к подключению серверов. Некоторые реализации VLAN обеспечивают также трансляцию кадров token ring в кадры Ethernet, Fast Ethernet или Gigabit Ethernet (и наоборот). Это означает, что станции token ring в одной части здания могут работать с серверами Fast Ethernet в другой части здания через магистраль Gigabit Ethernet. Пользователи token ring, планирующие переход на Ethernet, но не имеющие сделать это в масштабе всей сети сразу, могут решать эту задачу постепенно за счет поддержки VLAN с трансляцией кадров.

Возможность включения устройства во множество VLAN

Рабочие станции в сети используют одновременно несколько стеков сетевых протоколов. Типичной комбинацией является использование TCP/IP для доступа в

Internet, работы с внутренними Web-серверами и корпоративными серверами приложений, IPX для доступа к файловым серверам NetWare и т.п. Желательно в любом случае чтобы каждая станция входила хотя бы в одну IP VLAN и IPX VLAN.

VLAN также обеспечивают гибкое решение для контроля доступа к сетевым ресурсам на уровне рабочих станций и даже пользователей, которые могут быть допущены в одни VLAN, и не иметь прав доступа для других виртуальных ЛВС.

Как определяются VLAN

Прямая настройка и управление на основе правил

Существует два основных способа настройки VLAN:

- ♦ Для каждого порта можно прямо задать принадлежность к VLAN (обычно одной). Такое решение может оказаться весьма неэффективным для больших сетей, поскольку ручная настройка потребует много сил и времени, а конфигурацию придется менять при каждом добавлении или переносе станций.
- ♦ Более гибкое решение обеспечивает включение станций в VLAN на основе заданных администратором правил принадлежности к виртуальным ЛВС.

VLAN как группа коммутируемых портов

VLAN может быть просто набором физических портов коммутатора и реализации некоторых фирм предоставляют только такой способ организации виртуальных ЛВС. Как было отмечено выше, такой способ требует весьма трудоемкой настройки и при переносе станций операции по настройке приходится повторять. Кроме того, при переносе станции в другое помещение зачастую просто не удастся сохранить принадлежность этой станции к VLAN на базе портов.



Рисунок 1. VLAN как группа коммутируемых портов

VLAN как набор MAC-адресов

VLAN может объединять станции по списку MAC-адресов. В некоторых случаях такие списки создаются для отдельного коммутатора, в других администратор не связывает MAC-адреса с конкретными коммутаторами и список адресов копируется во все коммутато-

ры, а последние автоматически связывают соответствующие порты с VLAN.

MAC адрес – вещь неудобная в работе и при создании списков принадлежности к виртуальным ЛВС легко допустить ошибку. При смене сетевого адаптера в рабочей станции принадлежность – этой станции к VLAN теряется и требуется новая настройка сети.

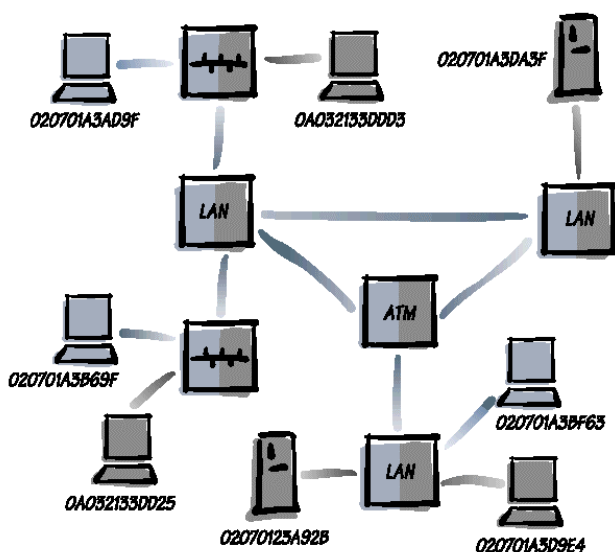


Рисунок 2 VLAN на основе MAC-адресов

VLAN на основе протокола

Во многих случаях очень удобно группировать рабочие станции по используемым ими протоколам, объединяя станции с VLAN на базе одного из протоколов. Например, при наличии в сети станций, использующих протокол DECNet или AppleTalk, будет целесообразно выделить эти станции в отдельные VLAN. Такое решение позволит изолировать широковещательные пакеты для каждого из протоколов в своей виртуальной ЛВС.

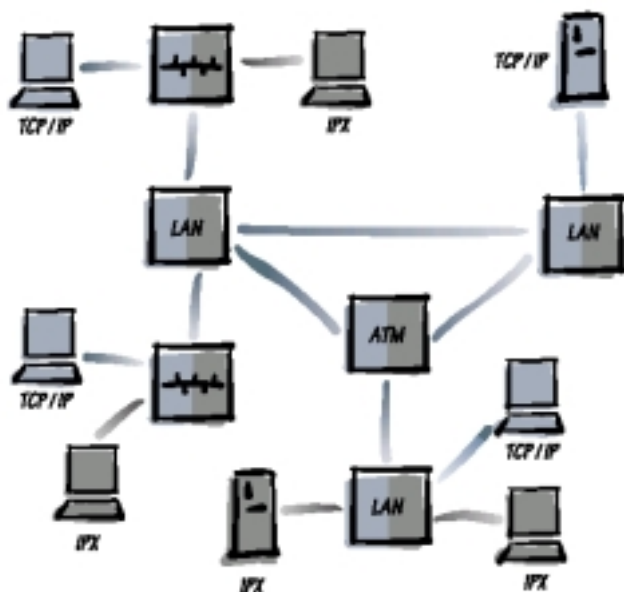


Рисунок 3 VLAN на основе протокола

VLAN как подсеть

В маршрутизируемых сетях TCP/IP базовым элементом является подсеть IP, представляющая собой область широковещания с общей сетевой частью IP-адреса для всех

членов подсети. Очевидно, что организация VLAN на основе подсетей IP для таких случаев будет эффективным решением и обеспечит простой способ управления большим числом рабочих станций IP.

Отметим, что в общем случае такой способ организации сети может конфликтовать с системами распределения IP-адресов на базе протокола DHCP. Очевидно, что использование автоматически выделяемых IP-адресов и организация виртуальных ЛВС на основе таких адресов приведет к случайному распределению рабочих станций между VLAN. Однако существует возможность объединить эти два процесса, предоставив серверам DHCP возможность автоматически выделять диапазон адресов для предопределенного набора устройств.

Некоторые производители коммутаторов также поддерживают VLAN на основе сетевых номеров IPX и зон AppleTalk.

VLAN как multicast-группа

В некоторых реализациях VLAN могут определяться как группы рабочих станций, использующие общий multicast-адрес.

Стандарты VLAN

В последние годы существенно выросла роль сетевых стандартов общего пользования. Было бы хорошо, если бы все реализации VLAN соответствовали единому стандарту. К несчастью, реализация VLAN тесно связана с аппаратными решениями, что существенно затрудняет создание стандарта для виртуальных ЛВС с широким набором функций, поскольку многие производители оборудования в этом случае не смогут обеспечить соответствие своих решений такому стандарту без внесения существенных изменений в свое оборудование. Очевидно, что принятие такого стандарта многие производители оборудования встречают в штыки.

Существует, однако, ряд частных стандартов VLAN, играющих достаточно серьезную роль.

ATM LANE

Эмуляция ЛВС (LAN Emulation) обеспечивает возможность подключения оборудования ЛВС к сетям ATM с сохранением стандартного сервиса, принятого в локальных сетях. Эмуляция ЛВС позволяет соединять локальные сети через ATM. Необходимость использования такой эмуляции обусловлена существенными различиями в технологиях ЛВС и ATM. Одним из таких различий является роль широковещательного трафика. Каждый протокол MAC-уровня использует широковещание как базовый инструмент, тогда как ATM является технологией, основанной на соединениях «точка-точка» и широковещательный трафик в сетях ATM приходится эмулировать.

LANE позволяет обеспечить такую эмуляцию в сетях ATM. Эмулируемая ЛВС в сети ATM представляет собой определенную на программном уровне область широковещания. Иными словами – это ATM VLAN. Как и в обычных VLAN, широковещательные и групповые пакеты, а также пакеты с неизвестными адресами коммутируются внутри эмулируемой ЛВС, а маршрутизация служит для передачи трафика между эмулируемыми сетями. Поддержка транков позволяет передавать трафик, относящийся к разным эмулируемым ЛВС, через один физический канал.

Но, как и в обычных VLAN, здесь также наблюдаются очень существенные различия между реализациями разных фирм. Например, некоторые компании поддерживают для своих решений включение портов в эмулируемые ЛВС только вручную отдельно для каждого порта, а другие поддерживают наборы правил для автоматического включения портов в эмулируемые ЛВС.

Модифицированный стандарт 802.10

Была предпринята попытка использования существующего стандарта IEEE 802.10 (протокол обеспечения безопасности в сетях городского масштаба) в качестве транкового протокола VLAN. Идея заключалась в использовании двух зарезервированных полей заголовка. Однако подкомиссия IEEE не согласилась с этим предложением, хотя некоторые производители успели его реализовать. Таким образом, эти реализации остаются в состоянии фирменных стандартов.

802.1Q и 802.1p

Одновременно в комитете IEEE 802 началась подготовка стандартов для виртуальных ЛВС, которая оказалась на этот раз успешной. Принятый стандарт 802.1Q уже реализуется в оборудовании различных фирм. Стандарт 802.1Q тесно связан со стандартом 802.1p.

802.1Q определяет:

- ♦ Стандартизованную форму виртуальных ЛВС на основе портов (отметим, что это очень ограниченный вариант VLAN без поддержки правил, требуемой для множества приложений).
- ♦ Измененный формат кадров Ethernet с тремя битами, позволяющими задать до 8 уровней приоритета; 12 битами, обеспечивающими возможность определения до 4096 различных VLAN и одним битом, зарезерви-

рованным для кадров, отличных от Ethernet, которые будут коммутироваться через сеть Ethernet.

- ♦ Механизм организации транков VLAN.
- ♦ Протокол распространения информации о VLAN между коммутаторами.

Протокол 802.1p используется в основном для приоритизации кадров и позволяет задать до 8 уровней приоритета.

Этот протокол определяет:

- ♦ Обобщенный протокол GARP (Generic Attributes Registration Protocol) для передачи сигналов между рабочими станциями и сетью.
- ♦ Вариант протокола GARP (GARP Multicast Registration Protocol), позволяющий устройствам запрашивать включение в указанные multicast-группы.
- ♦ Вариант протокола GARP (GARP VLAN Registration Protocol), позволяющий устройствам запрашивать включение в указанные VLAN.

Будущее виртуальных ЛВС

- ♦ VLAN на основе портов коммутатора слишком сложны в управлении и будут постепенно заменяться виртуальными ЛВС на базе правил.
- ♦ По мере распространения коммутации на сетевом уровне многие приложения, в которых виртуальные ЛВС играют важную роль, будут реализовываться с использованием новых возможностей коммутации. Однако эти две технологии (коммутация на сетевом уровне и VLAN) не исключают, а дополняют друг друга и могут использоваться совместно.
- ♦ VLAN будут продолжать играть роль полезной структуры для многих типов сервиса, включая аутентификацию и приоритизацию.