Описание основ работы VLAN, принципы построения сетей с использованием VLAN

Опубликовано muff в Ср, 2010-06-30 16:03

Введение

В начале истории Ethernet, локальные сети ограничивались одним доменном коллизий. При появлении мостов с двумя и более портами, стало возможным сегментировать большую сеть на меньшие домены коллизий, значительно улучшив производительность сети. Однако это не уменьшало перегрузок сети, вызванных внезапным широковещательным штормом. Широковещательный трафик свободно перемещался через Ethernet-мосты.

С появлением Ethernet-маршрутизаторов, пользователей сети стали группировать в рабочие группы с общим доменном коллизий. Это не только улучшило эффективность сети внутри каждой группы, но и уменьшило перегрузки общей сети, вызванное внезапным широковещательным штормом. Однако разделение общей сети маршрутизаторами на рабочие группы вызвало другие проблемы. Связь между рабочими группами стала возможно только через маршрутизаторы уровня 3. Это замедлило доступ к глобальным серверам компании.

С появлением технологии коммутируемого VLAN Ethernet стало возможно логического сегментирования сети на множество широковещательных доменов, улучшающее производительность сети и уменьшающее широковещательный трафик, без замедления доступа к глобальным серверам компании.

Коммутируеммый VLAN Ethernet

С появление коммутируемого Ethernet потребность его на рынке все возрастала и возрастала. На протяжении нескольких лет число коммутируемых портов в корпоративных сетях постоянно возрастало. При этом каждый коммутируемый порт был разделен все меньшим и меньшим числом пользователе сети, и даже достиг одиночного подключения каждого пользователя сети к коммутируемым портам. Этот тип сетевой инфраструктуры лучше всего пригоден для развертывания Виртуальных Локальных Сетей (VLAN).

Виртуальные сети могут быть определенны как группы пользователей отнесенные к определенным отделам или выполняющие общие функции, без ограничения физическим местонахождением пользователей и даже без ограничения использования разных сетевых устройств (коммутаторов), к которым они подключены физически.

Вышенаписанное предложение как бы определяет границы Виртуальной локальной сети (VLAN). Чаще Виртуальную локальную сеть воспринимают как общий домен широковещания. Технология VLAN делит большой домен широковещания на меньшие домены широковещания, ограничивая широковещательный трафик в пределах одной группы пользователей.

Порт ориентированная ВЛС

Этот тип виртуальных локальных сетей (ВЛС) определяет членство каждой ВЛС на основе номера подключенного порта. Смотрите следующий пример порт ориентированной ВЛС.

Пример 1. Порты 3,6,8 и 9 принадлежат к VLAN1 а порты 1,2,4,5 и 7 принадлежат к VLAN2

Таблица 1. Членство в каждой ВЛС определяется номером порта

PORT	**1**	**2**	**3**
VLAN 1			x

VLAN 2	x	x	

На рисунке 1 покзан пример реализации порт ориентированной ВЛС (на основе коммутатора SXP1224WM и двухскоростного концентратора DX2216 фирмы Compex).

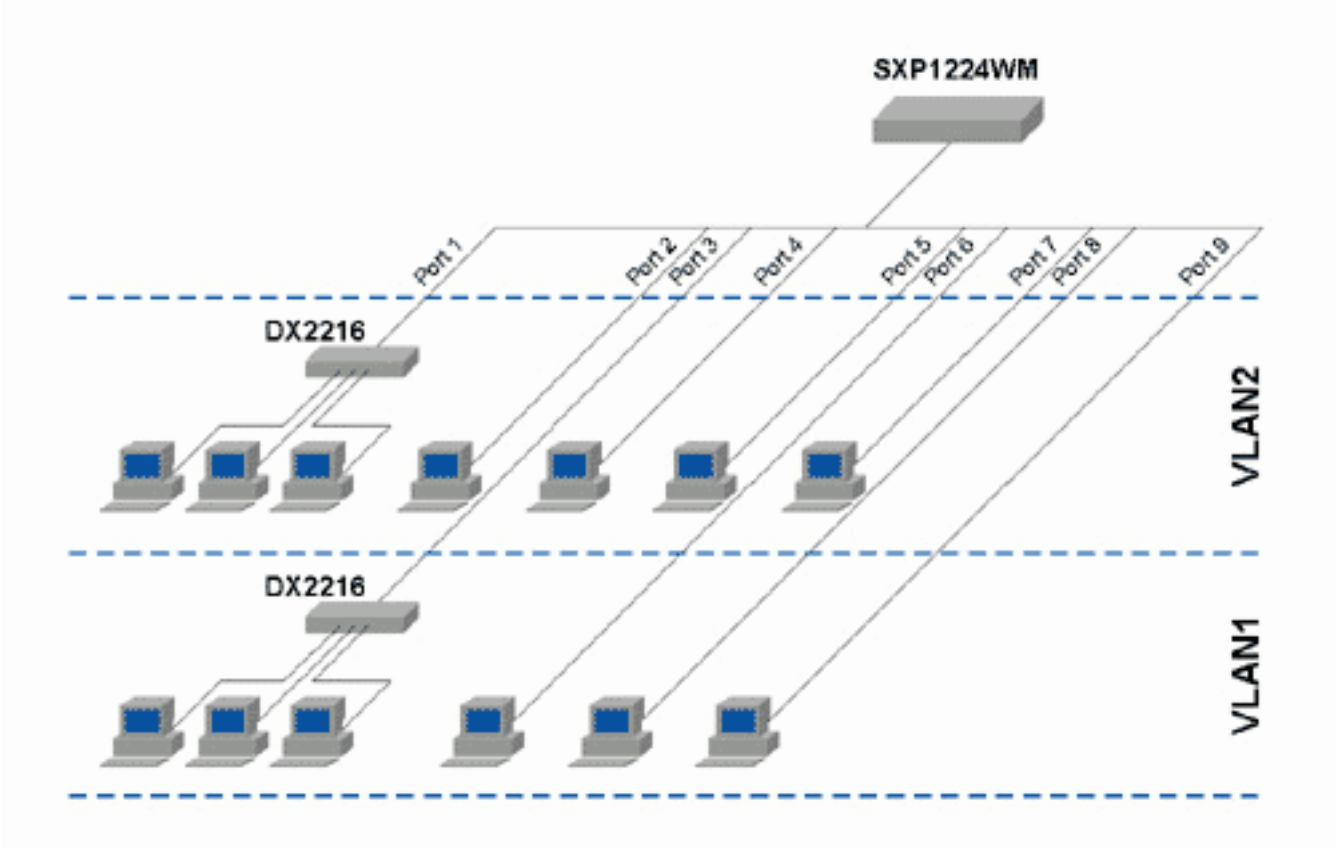

Рис. 1. Пример порт ориентированной ВЛС

В этом примере два концентратора DX2216 подключены к отдельным портам коммутатора SXP1224WM. Так как порт ориентированная ВЛС определяет членство VLAN на основе номера порта, то все рабочие станции подключенные к портам концентратора (DX2216) принадлежат к одной VLAN. В нашем случае, рабочие станции подключенные через концентратор DX2216 к 1 порту коммутатора принадлежат VLAN2, а рабочие станции подключенные через концентратор DX2216 к 3 порту коммутатора принадлежат к VLAN1. Так как эти автоматизированные рабочие места связаны через концентратор DX2216, они должны быть физически размещены не далеко друг от друга. С другой стороны, есть 7 рабочих мест станций, подключенных непосредственно к портам коммутатора (Private Port Switching). Рабочие места подключены к портам 6,8 и 9 коммутатора SXP1224WM физически отдалены от других станций (подключенных через концетратор), тем не менее, все они принадлежат VLAN2.

Для одного коммутатора SXP1224WM максимальное число пользователей с непосредственным (не разделяемым) подключением к коммутируемому порту - 24, по числу портов у этого коммутатора. Как же VLAN может быть реализована, если использован больше чем один коммутатор типа SXP1224WM и пользователи одной VLAN подключены к разным коммутаторам?
На рисунке 2 показан пример подключения пользователей VLAN через несколько коммутаторов.

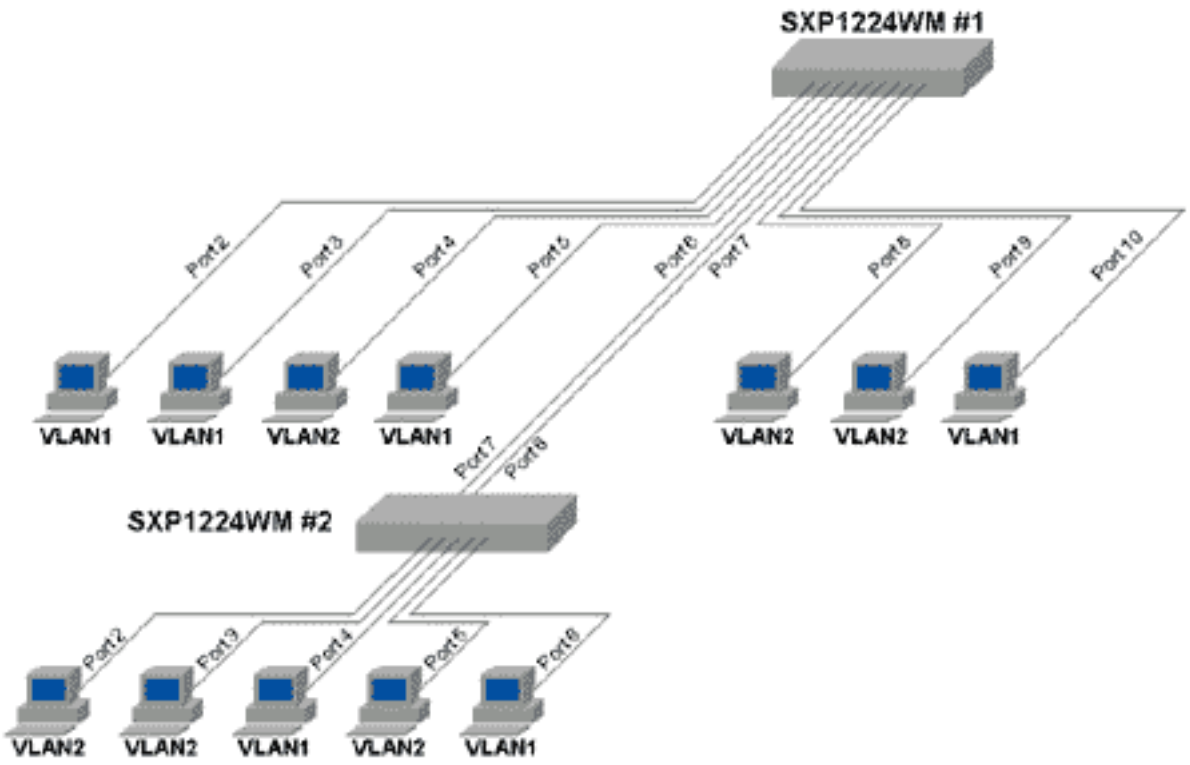

Рис.2. Сеть VLAN с использованием нескольких коммутаторов

VLAN членство для этого примера показываются в таблице 2 и 3.

Таблица 2. VLAN членство SXP1224WM *1

PORT	**2**	**3**	**4**	**5**	**6**	**7**
VLAN	x	x		x	x	
VLAN			x			x

Таблица 3. VLAN членство SXP1224WM *2

PORT	**2**	**3**	**4**	**5**	**6**	**7**	**8**
VLAN			x		x	x	
VLAN	x	x		x			x

В этом примере на обоих коммутаторах определенны две общие виртуальные подсети (VLAN). VLAN1 в коммутаторе #1 и VLAN1 в коммутаторе #2 есть та же самая общая VLAN, для которой должен быть определен общий порт. В этом случае, порт 6 на коммутаторе #1 и порт 7 на коммутаторе #2 члены VLAN1 и эти порты (порт 6 коммутатора #1 и порт 7 коммутатора #2) связаны вместе. Принимая во внимание, что порт 7 коммутатора #1 и порт 8 коммутатора #2 члены VLAN2, они связаны тоже вместе.

ВЛС с маркированными кадрами (IEEE 802.1Q)

Данный тип VLAN использует второй уровень сетевой модели. В каждый кадр вставляется тег ID идентифицирующий их членство в определенной VLAN. Эту технологию используют что бы создать виртуальные сети (VLAN) охватывающие множество коммутаторов. На рисунке 3 показан пример такой ВЛС.

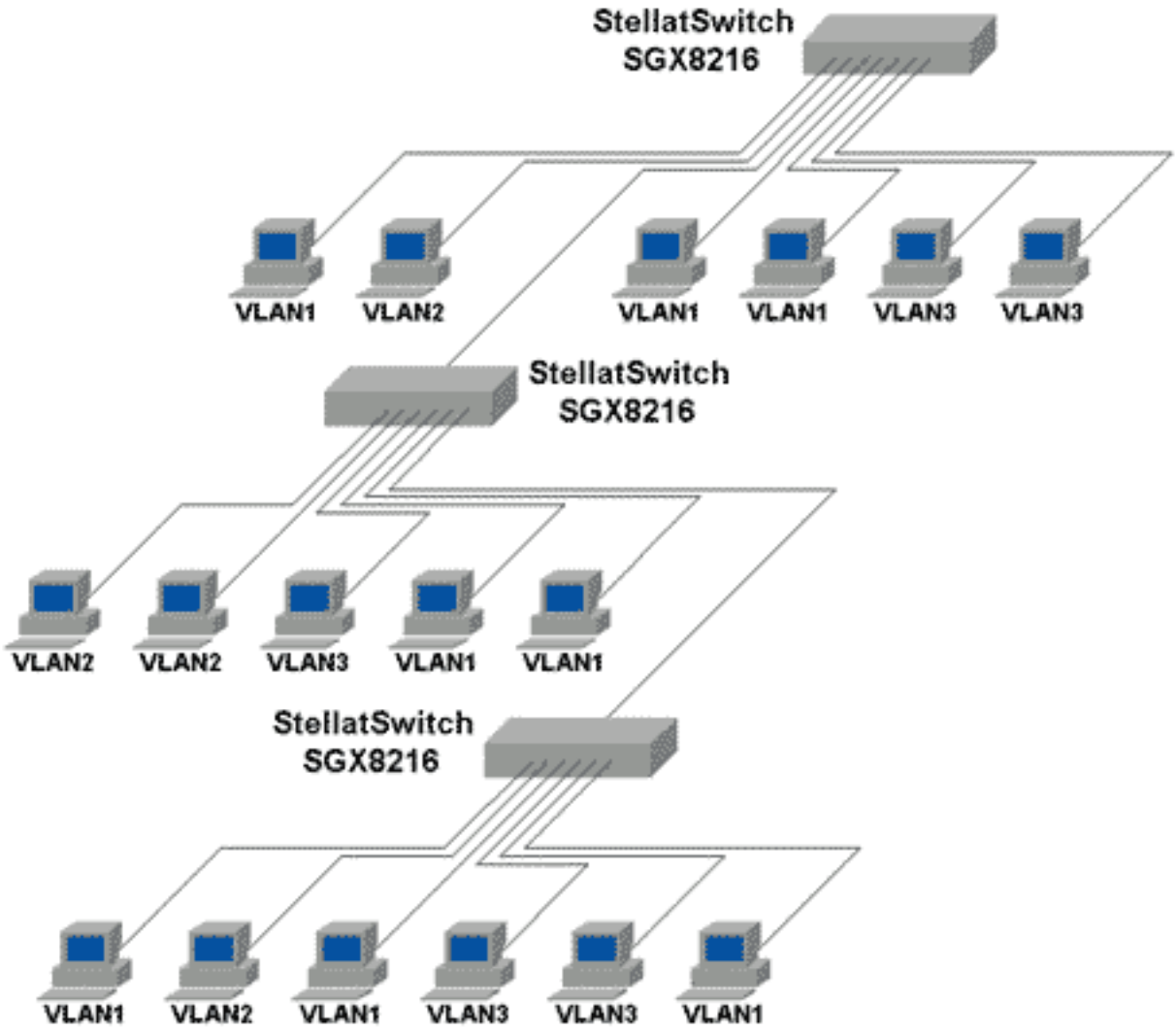

Рис. 3. Теговый VLAN, охватывающий три коммутатора

Теги ID в такой ВЛС могут быть добавлены явно или неявно. Если в сети есть сетевые карты с поддержкой IEEE 802.1Q, и на этих картах включены соответствующие опции, то исходящие кадры Ethernet от этих карт будут содержать теги VLAN идентификации. Данные теги идентификации VLAN добавлены явно. Коммутаторы поддерживающие IEEE 802.1Q идентифицируют членство в VLAN проверяя теги ID в кадрах Ethernet.

Если сетевые адаптеры (подключенные к этой сети) не поддерживают протокол IEEE 802.1Q, то добавление тегов VLAN может быть все же выполнено на основе группировки по портам. Предположим, что порты 1-3 сгруппированы в некоторую VLAN. Коммутатотор с поддержкой IEEE 802.1Q будет добавлять тег ID к входящим на этот порт кадрам Ethernet с соответствующим ID VLAN. Но эти теги будут удаленны коммутатором из исходящих кадров.

Если идентификация VLAN тегами протокола 802.1Q была осуществленна обоими спосабами - явно и неявно, входящие кадры к портам коммутатора могут состоять из обоих (с тегами и без) типов кадров. В этой ситуации к неотмеченным входящим кадрам будут добавляться теги ID VLAN описанные методом группировки по портам. В то время как маркированные кадры уже поддерживают членство VLAN определенное явно. Например, если порт 5 был сгруппирован неявно под VLAN1, входящик к порту 5 кадры с отметками ID сети VLAN2

сохроняют их членство в VLAN2 даже при том что порт 5 был сгруппирован под VLAN1.

ВЛС на основе протоколов высокого уровня

Протокол-основанные VLAN реализованы на 3 уровне сетевой модели, группируя рабочие станции с определенным транспортным протоколом под определенную VLAN. Например, если сеть состоит из компьютеров Apple и рабочих станций Unix, соответственно используя протоколы AppleTalk и TCP/IP, компьютеры Apple могут сгруппированы в одну VLAN в то время как станции Unix в другую. Протокол-основанный VLAN проверяет в пакетах информацию протоколов 3 уровня и позволяет пакетам с определенным транспортным протоколом (AppleTalk или TCP/IP) участвовать в соответствующем домене широковещания. На рисунке 4 показан пример реализации такой ВЛС.

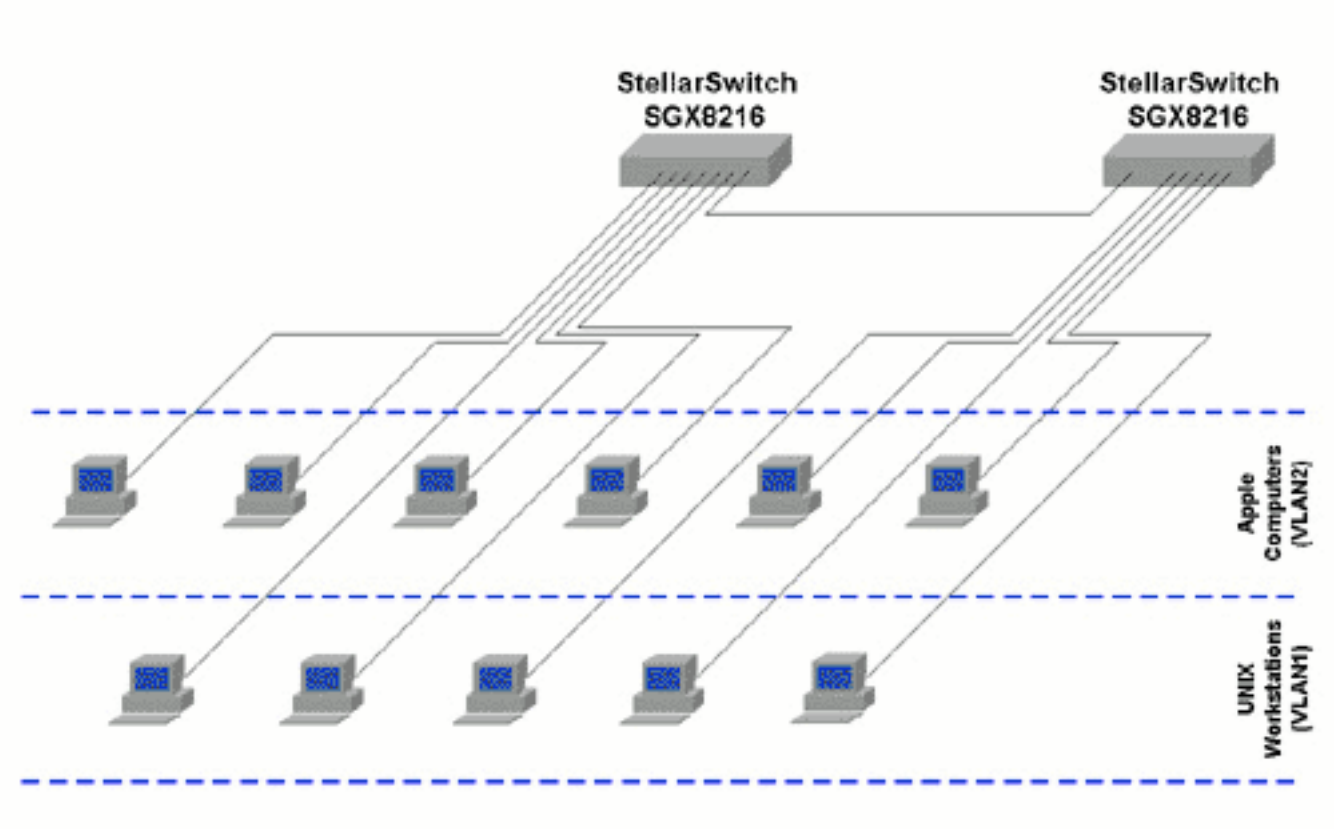

Рис. 4. Protocol-based VLAN

Преимущества VLAN

Виртуальные Рабочие группы

Главная функция виртуальных сетей это создание виртуальных рабочих групп, основанных на общих функциях пользователей и общих ресурсах, в доступе к которым они нуждаются. Например, предприятие состоит из множества департаментов - учета, снабжения, маркетинга, продаж и т.д.. Пользователям каждого департамента необходим доступ к определенным своим ресурсам. При помощи реализации VLAN пользователи каждого департамента могут быть логически описаны и сгруппированы в различные рабочие группы с различными доступными ресурсами сети.

Повышение производительности сети

Поскольку мы договорились, что ВЛС подобна домену широковещания, и что виртуальные локальные сети соответствуют реальным доменнам широковещания в сетях с несколькими VLAN. Предположим имеется сеть с 1000 автоматизированных рабочих мест расположенных в

одном домене широковещания. Каждая рабочая станция в этой сети принимает широковещательный трафик, генерируемый другими рабочими станциями. При использовании VLAN технологии эта большая сеть с большим широковещательным трафиком сегментируется на множество широковещательных доменов с несколькими рабочими станциями на один широковешательный домен. Следовательно частота (плотность) широковещания будет уменьшена. Производительность каждой подсети возрастает, потому что все сетевые устройства сети меньше отвлекается от передачи реальных данных при приеме широковещательного трафика.

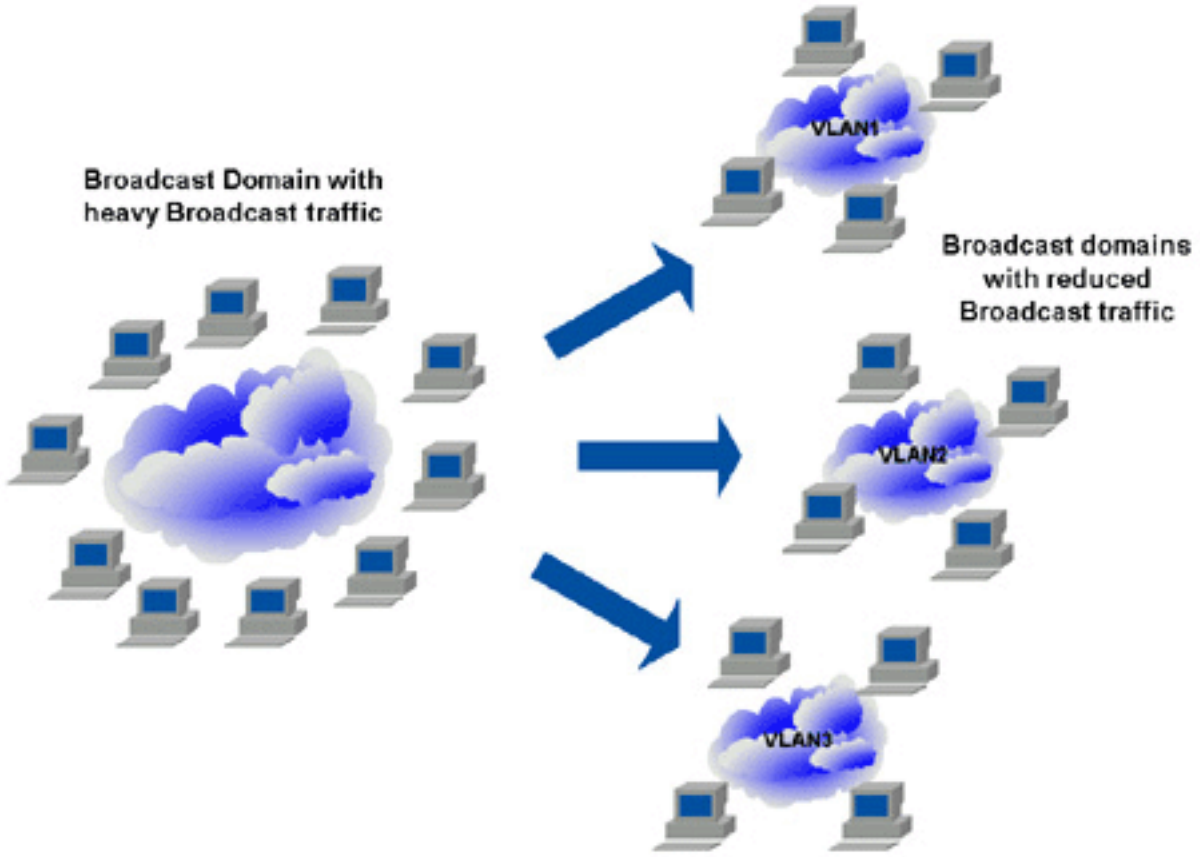

Рис. 5. Большая сеть, сегментированнаяная на множество виртуальных сетей (VLAN)

Разрушение традиционных концепций границ сети

В прошлом, рабочиее станции в той же самой рабочей группе или отделе обычно физически располагались в одном и том же месте. При использовании технологии VLAN, пользователи сети одной рабочей группы или отдела меньше ограничены их физическим местонахождением. Эта свобода зависит от возможностей применяемых Ethernet коммутаторов. В случае применения VLAN, пользователи сети одной рабочей группы или отдела могут находится на разных этажах и даже в разных зданиях и при этом относиться к одной виртуальной сети, как это показано на рисунке 6.

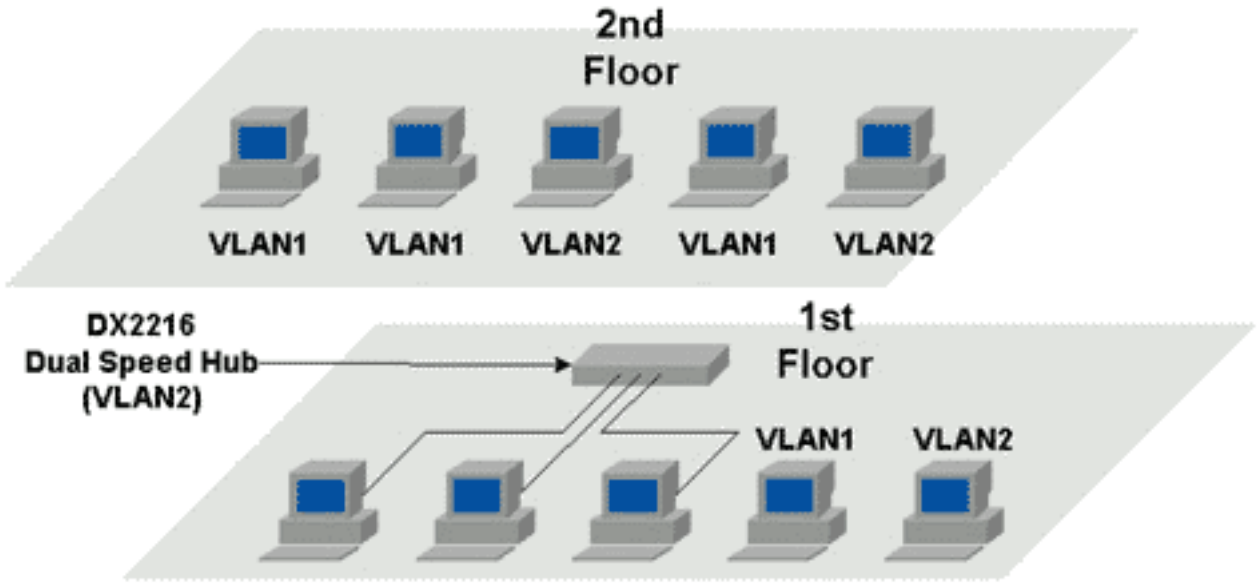

Рис. 6. Концепция свободных границ

На рисунке 6 показана сеть расположенная на двух различных этажах здания. На втором этаже все 5 рабочих мест подключены напрямую к Ethernet-коммутатору (private port switching). Заметьте, что 3 рабочих места на 1 этаже подключены к двухскоростному концентратору DX2216, а два других рабочих места подключены напрямую к потртам коммутатора, также как на 2 этаже. Коммутируемй потрт, через который каскадируется концетратор DX2216 определен к VLAN2, следовательно все три компьютера подключенные к DS2216 относятся к VLAN2. Рабочие станции подключенные к двухскоростному концетратору DX2216 должны физически близко располагаться друг к другу и принадлежать одной рабочей группе или отделу. С другой стороны, рабочие места подключенные к одному и тому же коммутатору с поддержкой VLAN не обязательно должны принадлежать одной рабочей группе или отделу. А рабочие станции подключенные к различным коммутаторам, не связанные физическим расположением могут принадлежать одной рабочей группе или департаменту и учавствовать в одном домене широковещания.

Безопасность и разделение доступа к сетевым ресурсам

Многие управляемые коммутаторы (например SXP1216/24WM и SGX3224/PLUS фирмы Compex) позволяют одному коммутируемому порту иметь членство в нескольких VLAN. Например, Порт 5 коммутатора может одновременно принадлежать VLAN1, VLAN2 и VLAN3, и участвовать в широковещании всех трех виртуальных сетей. Благодаря этой возможности сервер подключенный к порту 5 может предоставлять доступ рабочим станциям во всех трех сетях. С другой стороны, доступ к серверам одного отдела, подключенных к портам с членством в одной VLAN возможен только в пределах соответствующей VLAN.

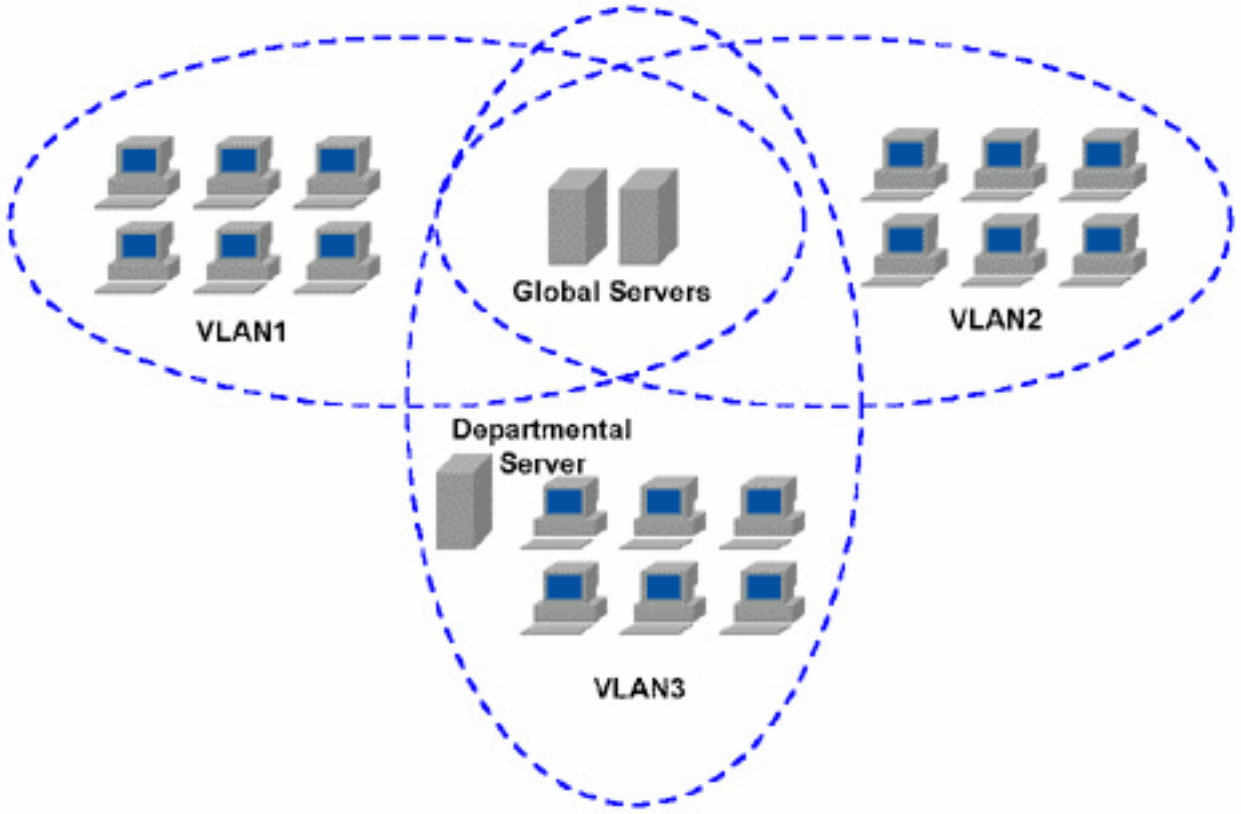

Рис. 7. Применение ВЛС для доступа к общему (глобальному) серверу предприятия

Уменьшение затрат при перемещения персонала

Положим есть потребность перемещения рабочих мест персонала из различных отделов в пределах компании, или изменения физического местоположения конкретного отдела. При применении тегового VLAN (IEEE 802.1Q) с прямым подключением к коммутируемым портам, стоимость перемещения включает только физическое перемещение рабочих мест персонала, потому что индентификоторы ID членства VLAN будут перенесены вместе с рабочими станциями сети. Нет никакой потребности в реконструкции соединений на существующих коммутаторах Ethernet.

Заключение

Даже при том, что для организации виртуальных локальных сетей существуют утвержденные стандарты, тем не менее способы построения ВЛС и способы назначения членства в ВЛС зависит от характеристик оборудования предоставляемого различными вендорами. Например, ВЛС могут создаваться путем группирования членства по номерам портов коммутаторов. А при обработке содержимого кадров Ethernet возможно группировать членство на основе таблицы MAC адресов или по содержимому специального тега ID кадра Ethernet.

Источник (получено *2025-12-07 11:16*):
http://muff.kiev.ua/content/opisanie-osnov-raboty-vlan-printsipy-postroeniya-setei-s-ispolzovaniem-vlan