ВЫЧИСЛИТЕЛЬНЫЕ СИСТЕМЫ И СЕТИ

УДК 004.732

ВНЕДРЕНИЕ ТЕХНОЛОГИИ VLAN ДЛЯ РАЗГРАНИЧЕНИЯ ДОСТУПА К РЕСУРСАМ ЛОКАЛЬНОЙ СЕТИ

М.В. Соснин

В статье рассматривается локальная сеть как базовая составляющая информационной системы. Рассмотрены варианты реализации разграничения доступа к ресурсам сети, приведена таблица для сравнения двух различных способов, рассмотрена технология VLAN и её ответвление – Asymmetric VLAN, которая позволяет наиболее эффективно в экономическом и временном плане организовывать независимые подсети в одной физической локальной сети.

Ключевые слова: *сервер, ресурсы, локальная сеть, управление, оптимизация.*

Key words: *server, resources, local area network, LAN, controlling, optimization.*

При развитии локальной сети очень часто возникает проблема разграничения доступа к её ресурсам пользователей различных категорий, а также объединения работников разных отделов в изолированные группы для решения определенных задач. При уже построенной и функционирующей сети становится довольно проблематичной организация новых точек подключения к компьютерам. В связи с этим рационально использовать технологию виртуальной локальной сети (Virtual Local Area Network – VLAN), разработанную Институтом инженеров электротехники и электроники (IEEE).

Внедрение технологии VLAN позволяет эффективно разделять трафик, лучше использовать полосу канала, гарантировать успешную совместную работу сетевого оборудования различных производителей и обеспечить высокую степень безопасности. При этом пакеты следуют между портами в пределах локальной сети. При внедрении технологии нет необходимости менять кабельную структуру сети и клиентские устройства доступа, следует заменить только активное оборудование, коммутирующее трафик.

VLAN обладают следующими преимуществами.

- Гибкость внедрения. **VLAN** являются эффективным способом группировки сетевых пользователей в виртуальные рабочие группы, несмотря на их физическое размещение в сети.
- **VLAN** обеспечивают возможность контроля широковещательных сообщений, что увеличивает полосу пропускания, доступную для пользователя.
- **VLAN** позволяют усилить безопасность сети, определив с помощью фильтров, настроенных на коммутаторе или маршрутизаторе, политику взаимодействия пользователей из разных виртуальных сетей.

В таблице представлено сравнение плюсов и минусов реализации раздельного доступа на физическом уровне и с помощью виртуальных локальных сетей VLAN.

Таблица

Сравнение реализации разделения ресурсов

Физическая		VLAN	
Плюсы	**Минусы**	**Плюсы**	**Минусы**
Надежность – при физическом отключении одного сегмента сети, остальные продолжают работать	Необходимость прокладки новых кабелей	Необходимо заменить только активное коммутирующее оборудование	Зависимость от физической среды передачи информации
	Необходимость закупки дополнительного оборудования	Возможность оперативно изменить топологию сети, не прибегая к затратам	
	Сложности при необходимости изменения топологии сети	Простота управления	
	Увеличение потребления физических ресурсов	Масштабируемость	
		Приоритезация	

Из таблицы можно сделать вывод, что применение виртуального разделения сети экономически целесообразно.

На рис. 1 представлена типовая схема реализации разделения пользователей с помощью технологии VLAN.

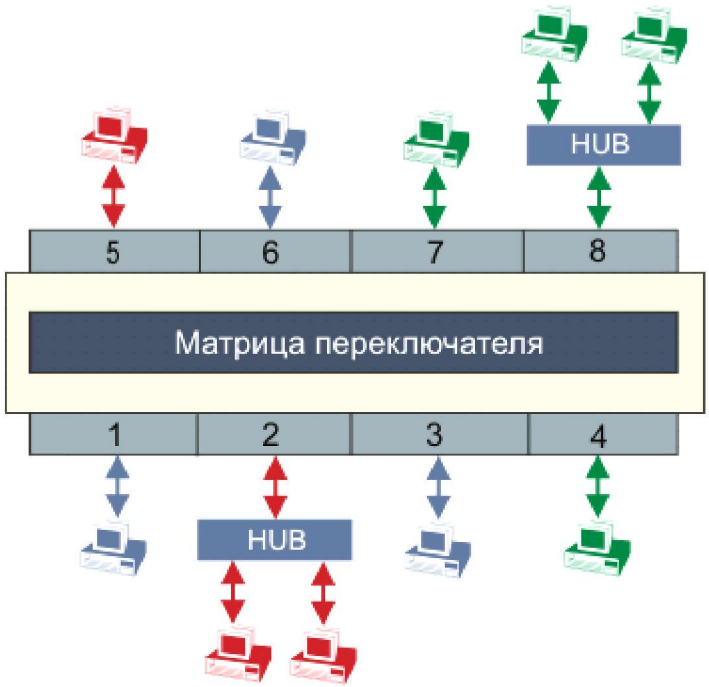

Рис. 1. Пример реализации VLAN на базе одного коммутатора

На коммутаторе запрограммирована возможность пересылки пакетов между портами 1, 3 и 6, 2 и 5, а также между портами 4, 7 и 8. Пакет из порта 1 никогда не попадет в порт 2, а из порта 8 в порт 6 и т.д. Таким образом, переключатель разделяется на три независимых виртуальных переключателя, принадлежащих различным виртуальным сетям. Управление

матрицей переключения возможно через подключаемый извне терминал или удаленным образом с использованием протокола SNMP или WEB.

Однако при этом возникает проблема доступа к одному какому-либо общему для всех пользователей физической сети ресурсу, например, шлюзу доступа в глобальную сеть интернет. Если следовать рассмотренной концепции, то для обеспечения работы во всех сегментах сети серверу необходимо иметь столько сетевых интерфейсов и задействовать столько портов коммутатора, сколько в сети запрограммировано виртуальных подсетей. Это нецелесообразно ни в экономическом, ни в ресурсном отношении при реализации системы.

Такая задача может быть решена с помощью асимметричных VLAN, построенных на основе меток в дополнительном поле пакета – стандарт IEEE 802.1q [1]. Для определения разрешения проходимости пакета в тот или иной VLAN коммутатор зарание составляет таблицу маршрутизации пакетов на основе ARP и IP.

На рис. 2 представлена схема реализации асимметричной виртуальной локальной сети, где VLAN1 – общие локальные ресурсы, VLAN2 – группа пользователей 1, VLAN3 – группа пользователей 2. VLAN2 и VLAN3 могут обмениваться данными с VLAN1, но не могут между собой. При этом пользователи и сервера с ресурсами находятся в одной подсети, но в разных широковещательных доменах.

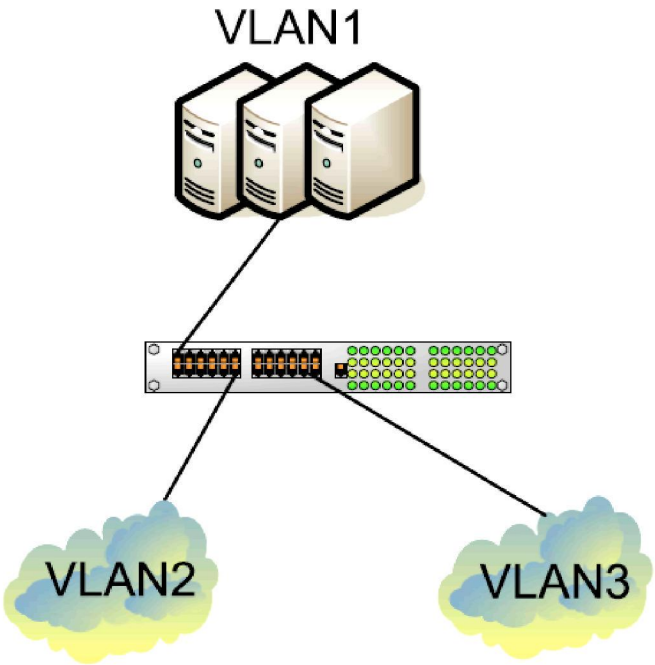

Рис. 2. Пример реализации Asymmetric VLAN в пределах одного коммутатора

На рис. 3 компьютеры от A до U не могут обмениваться друг с другом информацией и находятся в разных VLAN, а серверы принадлежат ко всем VLAN одновременно, при этом обмен между коммутаторами происходит через тегированные (tagged) порты.

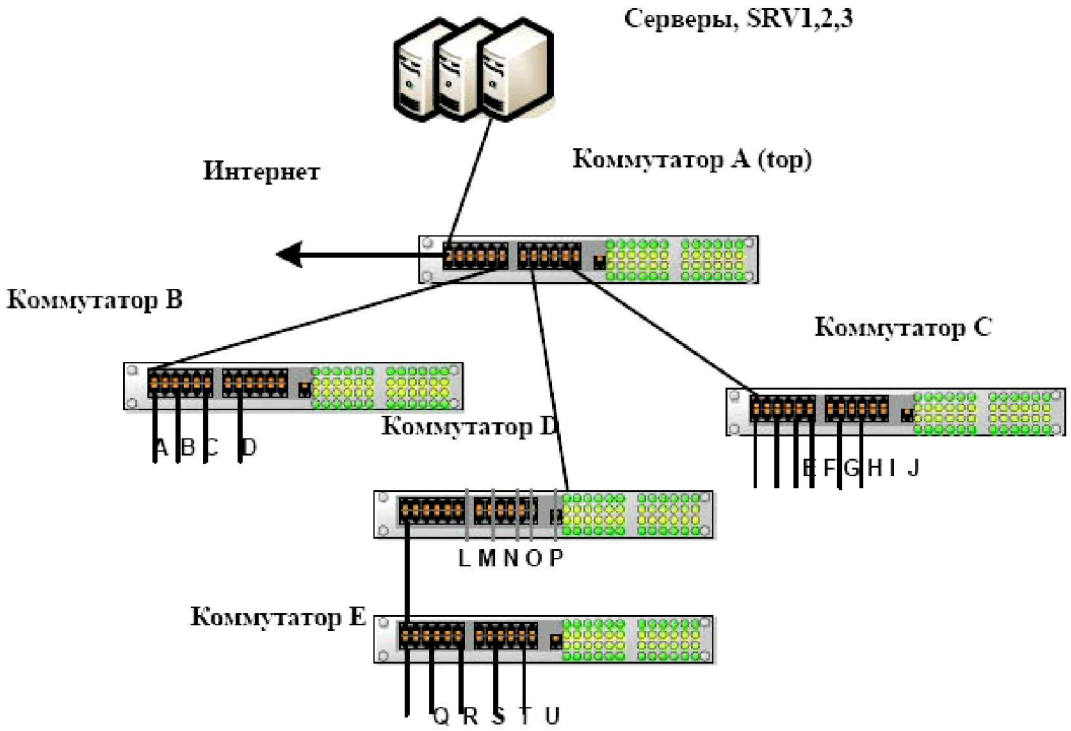

Рис. 3. Пример реализации Asymmetric VLAN в пределах небольшой локальной сети

Основное различие между базовым стандартом 802.1q VLAN или симметричными VLAN и асимметричными VLAN заключается в том, как выполняется отображение адресов. Симметричные VLAN используют отдельные адресные таблицы, т.е. не существует пересечения адресов между VLAN-ами. Асимметричные VLAN могут использовать одну, общую таблицу адресов. Однако использование одних и тех же адресов (пересечение по адресам) происходит только в одном направлении.

В примере, рассмотренном выше, VLAN1, созданная для порта, имела в своем распоряжении полную таблицу адресов, т.е. любой адрес мог быть отображен на ее порт (PVID).

Основными достоинствами рассмотренного варианта построения ЛВС являются следующие.

- Обеспечение высокой степени защищенности информации от несанкционированного доступа за счет создания для каждого подразделения предприятия (или отдельного пользователя) виртуальных локальных сетей (VLAN), ограничивающих трафик в пределах отдельной VLAN.
- Возможность размещения всех основных вычислительных ресурсов (серверов) в одной аппаратной (серверной) позволяет обеспечить требуемый уровень их защищенности от внешних воздействий и удобство обслуживания.
- Возможность предоставления доступа к любым из имеющихся сетевых ресурсов (серверов, систем хранения информации Internet и т.п.) на каждом коммутаторе уровня распределения без проведения работ по прокладке дополнительных кабельных линий.
- Структурная гибкость сети, позволяющая быстро менять строение сети, наращивая или подстраивая ее под изменяющуюся структуру предприятия без проведения работ по прокладке дополнительных кабельных линий.

- Масштабируемость сети, что дает возможность легко наращивать вычислительные ресурсы сети простым подключением дополнительных серверов и других сетевых элементов к стеку коммутаторов «ядра».
- Возможность подключения локальных средств архивизации в любой удобной точке сети, что позволяет расположить устройства архивизации как с учетом минимизации нагрузки на сеть, так и в месте, наиболее защищенном от пожара, затопления и т.п.
- Невысокая стоимость решения и оптимальное соотношение показателя цена/качество, позволяет при малом бюджете развертывать гибкую, высокозащищенную информационную инфраструктуру.

Дальнейшее развитие рассмотренной архитектуры и методологии должно предусматривать наращивание защищенности информационной инфраструктуры. Вполне очевидно, что для этого требуется наличие дублирующих маршрутов в сети, т.е. сеть рассматривается как граф, причем его связность не должна нарушаться при недоступности какого-либо ребра (при отказе информационного канала) или узла.

Библиографический список

1. ***Стандарт*** 802.1Q / Библиотека стандартов института IEEE. – Режим доступа: http://standards.ieee.org/getieee802/download/802.1Q-2005.pdf, свободный. – Заглавие с экрана. – Яз. англ.