ИПМ им.М.В.Келдыша РАН • Электронная библиотека

Препринты ИПМ • Препринт № 25 за 2007 г.


ISSN 2071-2898 (Print)
ISSN 2071-2901 (Online)

**В.П. Андреев, В.В. Врублевский**

# Особенности построения структурированной локальной вычислительной сети на Ethernet коммутаторах D-Link на основе использования асимметричных VLAN



***Рекомендуемая форма библиографической ссылки:*** Андреев В.П., Врублевский В.В. Особенности построения структурированной локальной вычислительной сети на Ethernet коммутаторах D-Link на основе использования асимметричных VLAN // Препринты ИПМ им. М.В.Келдыша. 2007. № 25. 12 с.
https://library.keldysh.ru/preprint.asp?id=2007-25

**РОССИЙСКАЯ АКАДЕМИЯ НАУК**
**Ордена Ленина**
**ИНСТИТУТ ПРИКЛАДНОЙ МАТЕМАТИКИ**
**им. М.В.Келдыша**

В.П. Андреев, В.В. Врублевский

# ОСОБЕННОСТИ ПОСТРОЕНИЯ СТРУКТУРИРОВАННОЙ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ НА **ETHERNET** КОММУТАТОРАХ **D-LINK** НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ АСИММЕТРИЧНЫХ **VLAN**

Москва – 2007

## Аннотация

Описан один из вариантов построения архитектуры локальной вычислительной сети (ЛВС), позволяющий разделять ее ресурсы между изолированными группами пользователей. Постановка задачи включает в качестве одного из основных требований формирование методики построения высокозащищенной ЛВС, обеспечивающей гарантированную конфиденциальность трафика отдельных групп пользователей. Ключевым аспектом рассматриваемой архитектуры ЛВС является ее организация в виде регулярной структуры и применение типовых элементов (Ethernet коммутаторов) для построения узлов. Детальные методики двух вариантов построения асимметричных VLAN в рамках рассматриваемой архитектуры ЛВС показывают практические способы их реализации, которые могут применяться виде типовых, тиражируемых решений и выбираться в зависимости от того, какие особенности функционирования системы и организации доступа к ресурсам сети необходимо получить. В заключении даны рекомендации по выбору способов организации VLAN, анализ ограничений и достоинств описанных методик.

**V.P. Andreev, V.V.Vrublevsky. Design of structured local area network using D-Link Ethernet switches based on asymmetric VLAN technology.** The paper is suggesting a variant of the local area network (LAN) architecture, allowing to share resources of the isolated users. The main task was to find a LAN construction method with high protection and confidence for any traffic generated by some users groups. The key aspect of the LAN architecture is the operation with regular structures and typical elements (Ethernet switches) for all designed nodes. We consider in details two suggested methods of design of asymmetric VLAN with such architecture. This consideration shows the practical way of LAN designing to be used for standardized and reproducible solutions, depending on required system functionality and required access to resources. One can find recommendations on how to choose the way of building a LAN, restrictions and advantages of the method.

**1. Введение.** Целью создания структурированной ***локальной вычислительной сети*** (ЛВС) предприятия является обеспечение более высокой степени защищенности информации от несанкционированного доступа по сравнению с традиционными (распределенными) сетями, повышение производительности сети и организация более эффективного управления компонентами сети и информационными потоками.

Создание такой ЛВС стало возможным благодаря использованию во всех коммутационных узлах интеллектуальных Ethernet коммутаторов, работающих на канальном (2-м) уровне модели OSI. Кроме того, они должны поддерживать передачу маркированных (tegging) пакетов (стандарт IEEE 802.1q [1]), а также ассиметричные виртуальные локальные сети (например, коммутаторы DES-3226S и DES-3526 компании D-Link). ***Виртуальная локальная сеть*** (VLAN) это сегмент общей сети, который представляет собой объединение портов различных коммутаторов в логическую группу, образующую безопасный автономный широковещательный домен. Основной целью разбиения сети на несколько VLAN является ограничение распространения широковещательных пакетов, поскольку их передача между различными VLAN невозможна. Поэтому исключается развитие широковещательных штормов, которые существенно снижают производительность сети. Наряду с этим использование VLAN дает целый ряд дополнительных преимуществ, которые будут рассмотрены ниже.

В рамках рассматриваемой концепции построения ЛВС не предусматривается применение маршрутизации/коммутации пакетов на сетевом (3-м) уровне. Такой подход обусловлен изначальным ключевым требованием обеспечения максимальной защищенности информационных каналов. Поэтому используются имеющиеся технические возможности по изолированию трафика групп пользователей, начиная с возможного низкого уровня, то есть со 2- уровня модели OSI. Кроме того, концепция организации сети описанная ниже, единственно возможная в тех случаях, когда выполнятся

передача информации посредством пакетов, не обладающих способностью к маршрутизации (например, NetBIOS или протоколы специального назначения), но требуется высокая степень защищенность сети и изолированности информационных потоков пользователей.

Тем ни менее, данная методика построения сети не исключает применение маршрутизации, которая может рассматриваться как следующий уровень управления трафиком.

В качестве практического примера рассмотрим схему структурированной ЛВС некоторого предприятия, представленную на рис.1. В ее основу положена древовидная топология [1].

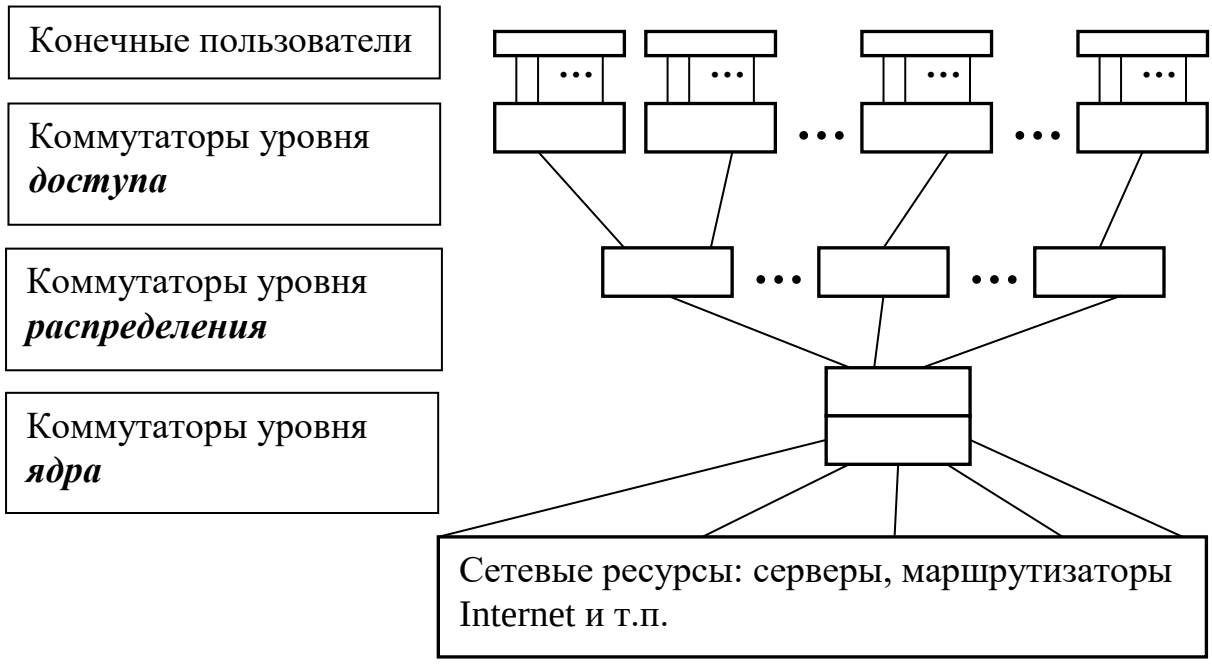


Рис.1. Функциональная схема структурированной ЛВС

***Коммутаторы уровня ядра*** устанавливаются в аппаратной (серверной), где также, как правило, располагаются все сетевые ресурсы: серверы (файл-серверы, серверы приложений, почтовые серверы и т.п.), маршрутизатор доступа в Internet и т.п. Эти коммутаторы формируют единую производительную информационную магистраль предприятия.

***Коммутаторы уровня распределения*** обычно располагаются в коммутационных помещениях и/или шкафах, установленных на разных этажах

или в разных секциях здания. Там же, как правило, располагаются и ***коммутаторы уровня доступа***, к которым подходят линии от персональных компьютеров (ПК) пользователей, сетевых принтеров и иных конечных устройств. Коммутаторы уровня доступа обычно служат для увеличения количества портов, требуемых для подключения ПК пользователей.

Коммутаторы «ядра» удобно объединить в *стек*. Стек коммутаторов ядра соединяется с коммутаторами уровня распределения, причем обычно в этом случае используется агрегирование каналов или, иначе, объединение портов в транк, состоящий из нескольких (2 – 8) кабельных линий. Это позволяет с одной стороны расширить полосу пропускания соединения, а с другой стороны обеспечивает повышенную надежность соединения за счет дублирования каналов.

Задача состоит в том, чтобы иметь возможность обеспечить доступ к различным комбинациям сетевых ресурсов пользователям в зависимости от их прав доступа, организационной принадлежности и политик безопасности без прокладки дополнительных кабельных линий. При этом должна быть исключена возможность трафика между компьютерами различных подразделений предприятия. Такая задача может быть решена с помощью ***асимметричных VLAN***, построенных на основе меток в дополнительном поле пакета – стандарт IEEE 802.1q [1].

**2. Экспериментальное исследование вариантов использования асимметричных VLAN.** Рассмотрим решение данной задачи на примере простейшей сети, изображенной на рис.2.

Имеются три сервера S1, S2 и S3. Эти сетевые ресурсы подключены к коммутатору «ядра» SW1 (DES-3226S или DES-3526), который в свою очередь соединен с коммутатором уровня распределения SW2 (DES-3226S или DES-3326S). Для каждого сервера на базе портов 1, 2 и 3 коммутатора SW1 создается отдельный VLAN – соответственно VS1 (включает порт 1), VS2 (включает порт 2) и VS3 (включает порт 3). Создаем еще 2 VLAN - VS12

(включает порт 4) и VS23 (включает порт 5), и с помощью настроек асимметричных VLAN формируем пути для трафика, показанные на рисунке стрелками (сплошные линии). В этом случае ПК PC12, который подключен к порту 4 коммутатора SW1, входящему в VLAN VS12, будут доступны данные на серверах S1 и S2, а ПК PC23, который подключен к порту 5 коммутатора SW1, входящему в VLAN VS23, будут доступны данные на серверах S2 и S3. В то же время трафик между VS12 и VS23 будет запрещен (перечеркнутая стрелка); следовательно, информация на S3 и PC23 будет недоступна для PC12, и информация на S1 и PC12 будет недоступна для PC23, а ресурсы сервера S3 будут доступны как PC12, так и PC23.

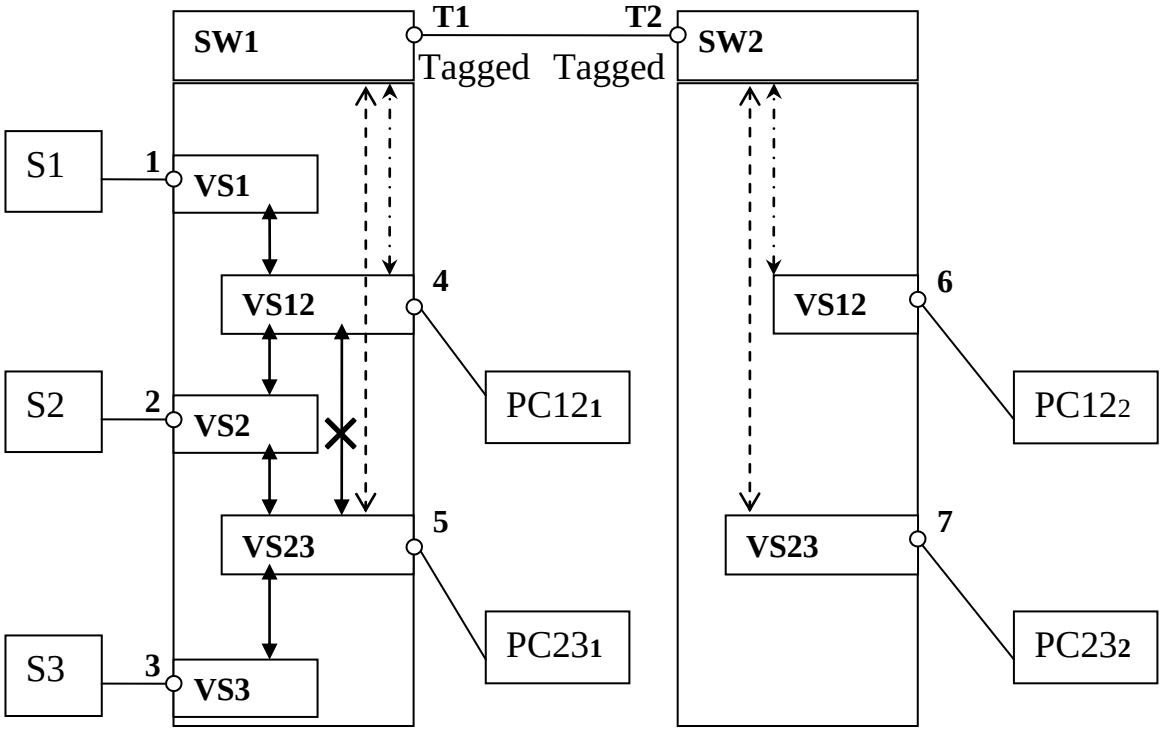


Рис.2. Использование асимметричных VLAN
для создания разделенных ресурсов

Поскольку коммутатор SW1 является коммутатором «ядра», то компьютеры пользователей PC12 и PC23 желательно подключать к другому коммутатору – коммутатору уровня распределения, например SW2, или коммутатору уровня доступа (на рисунке не показан). В этом случае

необходимо распространить действие VS12 и VS23 на коммутатор SW2. Для этого воспользуемся таким свойством коммутаторов, как поддержка VLAN на основе меток в дополнительном поле пакета – стандарт IEEE 802.1q.

Казалось бы, можно решить эту задачу следующим образом. На коммутаторе SW2 создаем 2 аналогичных VLAN - VS12 и VS23 и соединяем эти коммутаторы, например, портами T1 и T2. Отмечаем эти порты как Tagged (маркирующие) и включаем их в состав VS12 и VS23 на обоих коммутаторах. Предполагаемый трафик обозначен на рисунке стрелками из пунктирных линий. Однако такое решение оказывается неверным, поскольку поддержка асимметричных VLAN ограничена автономными коммутаторами, а мы пытаемся распространить действие асимметричных VLAN на 2 коммутатора. Верное решение приведено на рис.3.

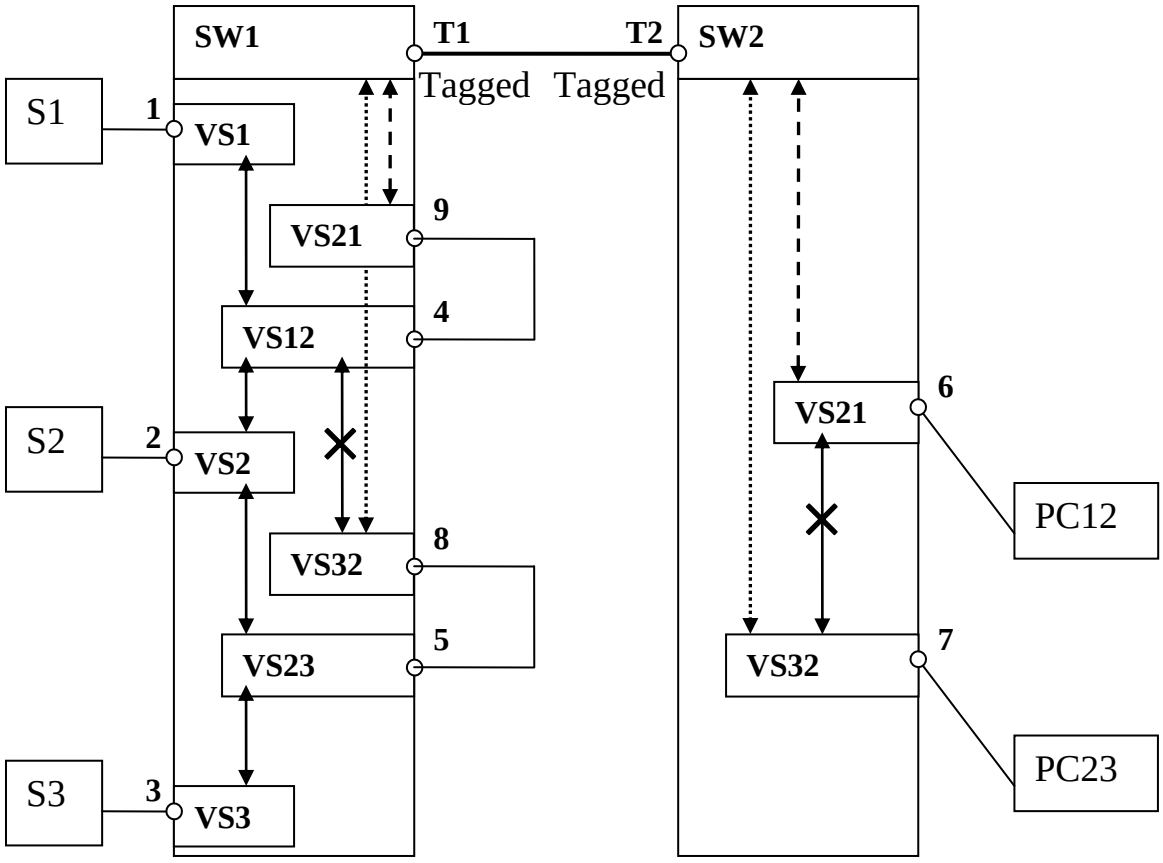


Рис.3. Организация передачи сетевых ресурсов
на уровень распределения – вариант I.

На коммутаторах SW1 и SW2 создаем по 2 дополнительных VLAN – VS21 на портах 6 и 9 и VS32 на портах 7 и 8 соответствующих коммутаторов.

Соединяем эти коммутаторы посредством маркирующих (Tagged) портов T1 и T2. Порты 5 и 8, а также 4 и 9 коммутатора SW1 соединяем перемычками. В результате организуется связь между портами различных коммутаторов, принадлежащих одноименным VLAN. Такую организацию виртуальных сетей будем в дальнейшем называть ***распределенной (мостовой)*** VLAN. В этом случае трафик будет осуществляться так, как показано на рисунке стрелками. Тогда ПК PC12 будет иметь доступ к ресурсам серверов S1 и S2, а ПК PC23 будет иметь доступ к ресурсам серверов S2 и S3; в то же время трафик между PC12 и PC23 оказывается невозможен (перечеркнутая стрелка).

Для увеличения полосы пропускания соединения коммутаторов SW1 и SW2 следует применить агрегирование портов. Коммутатор уровня распределения, например SW2, желательно использовать для создания «распределенных» VLAN, имеющих на этом коммутаторе всего один порт, а для увеличения числа портов, предназначенных для включения в эти VLAN конечных пользователей, следует использовать коммутаторы уровня доступа, подключаемые, например, к портам 6 и 7 коммутатора SW2. Для увеличения полосы пропускания соединения коммутаторов уровня распределения и коммутаторов уровня доступа можно также использовать агрегирование портов.

В ряде случаев возникает необходимость передавать каждый сетевой ресурс на уровень распределения и уже там организовать доступ к этому ресурсу, исключая трафик между его потребителями. Например, необходимо предоставить доступ к Internet ПК подразделений П1 и П2 предприятия, исключив возможность трафика между компьютерами этих подразделений. На рис.4 приведен простейший вариант такой сети.

Создаем «распределенную» VLAN VS1 на обоих коммутаторах описанным выше способом. На коммутаторе SW2 создаем две пользовательских VLAN подразделений – VS11 и VS12 на портах соответственно 6 и 7. Как было отмечено выше, поддержка асимметричных

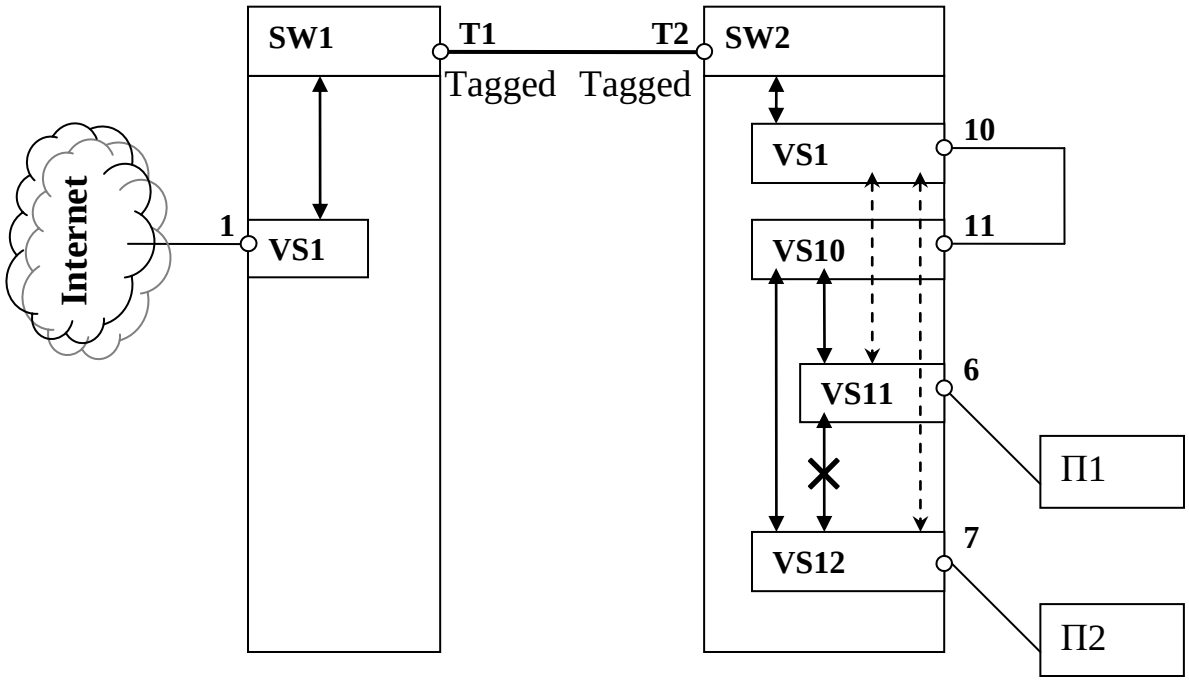


Рис.4. Организация передачи сетевого ресурса
на уровень распределения – вариант II.

VLAN ограничена автономными коммутаторами. Поэтому, если непосредственно включить порты 6 и 7 в состав VS1 в качестве асимметричных VLAN, то трафик, обозначенный стрелками из пунктирных линий, не будет выполняться, поскольку в этом случае асимметричный VS1 будет располагаться на нескольких коммутаторах. Для реализации поставленной задачи на коммутаторе SW2 создаем дополнительный VLAN VS10, в состав которого включаем порты 6 и 7, одновременно принадлежащие виртуальным сетям VS11 и VS12, а в состав VS11 и VS12 включаем порт 11, принадлежащий VS10; иными словами, создаем асимметричный VLAN. Порты 10 и 11 коммутатора SW2 соединяем перемычкой. В результате будет соблюдаться требование, ограничивающее действие асимметричного VLAN одним коммутатором, и в то же время будет организован совместный доступ компьютеров подразделений П1 и П2 к Internet при запрете трафика между ПК подразделений (перечеркнутая стрелка).

**3. Рекомендации.** Оба рассмотренных способа организации передачи сетевых ресурсов с уровня ядра на уровень распределения имеют свои

достоинства и недостатки. Первый способ позволяет создавать необходимые комбинации сетевых ресурсов в одном месте и передавать их только на те коммутаторы уровня распределения, где они требуются. В этом случае существенно сокращается трафик между коммутаторами ядра и коммутаторами уровня распределения. Кроме того, данный способ не требует установки на уровне распределения коммутаторов, поддерживающих асимметричные VLAN; достаточно коммутатора, поддерживающего обычный стандарт IEEE 802.1q. К недостаткам такого способа следует отнести необходимость установки на уровне ядра коммутаторов с большим количеством портов или создания стека коммутаторов ядра. Также изменение конфигурации коммутаторов ядра в процессе эксплуатации, что обычно требуется при изменении топологии сети, может повлиять на работу всех пользователей.

Второй способ удобен тем, что на всех коммутаторах уровня распределения можно иметь сразу все сетевые ресурсы, изначально подключенные к коммутаторам ядра, и по мере необходимости создавать из них требуемые комбинации лишь для групп пользователей, подключенных к конкретному коммутатору уровня распределения. В этом случае переконфигурирование коммутатора может затронуть лишь подключенных к нему пользователей. К недостаткам такого способа следует отнести повышенный трафик между коммутаторами ядра и коммутаторами уровня распределения, поскольку доступ к сетевым ресурсам распространяется сразу на все коммутаторы уровня распределения. Кроме того, все коммутаторы уровня распределения должны поддерживать асимметричные VLAN. Но основной недостаток второго способа заключается в том, что он не позволяет простым образом обеспечивать связь между ПК, подключенными к различным коммутаторам уровня распределения, например, в случае, когда ПК одного подразделения предприятия располагаются на разных этажах и физически подключены к различным коммутаторам уровня распределения.

Опыт построения большой распределенной ЛВС показывает, что при проектировании такой сети следует предусмотреть возможность использования сразу обоих способов организации передачи сетевых ресурсов на уровень распределения, т.е. на уровне ядра следует создавать стек из коммутаторов, поддерживающих асимметричные VLAN, и на уровне распределения использовать также коммутаторы, поддерживающие асимметричные VLAN. Кроме того, для обеспечения повышенной защищенности системы управления настройками коммутаторов ЛВС от несанкционированного доступа следует создать на всех коммутаторах сети отдельную распределенную VLAN и настроить коммутаторы так, чтобы управлять настройками всех коммутаторов сети было возможно лишь со станции управления сетью, подключенной только в эту VLAN.

Предложенный вариант построения локальной вычислительной сети обладает следующими свойствами: структурность, универсальность и избыточность [2, с.25].

**4. Заключение.** Основными достоинствами рассмотренного варианта построения ЛВС являются:

- 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.

## Литература


1. Коммутаторы локальных сетей D-Link. Учебное пособие. – Первое изд. – М.: D-Link, 2004.
2. Семенов А.Б., Стрижаков С.К., Сунчелей И.Р. Структурированные кабельные системы.- 5-е изд. – М.: Компания Ай Ти; ДМК Пресс, 2004. – 640+16с.: ил.