Виртуальные сети

Дисциплина – Компьютерные сети

Преподаватель – Литвинова М.А.

введение

Виртуальной локальной сетью называется логическая *группа* узлов сети, трафик которой, в том числе и широковещательный, на канальном уровне полностью изолирован от других узлов сети.

Это означает, что передача кадров между разными виртуальными сетями на основании MAC-адреса невозможна независимо от типа адреса — уникального, группового или широковещательного. В то же время внутри виртуальной сети кадры передаются *по* технологии коммутации, то есть только на тот *порт*, который связан с адресом назначения кадра. Таким образом с помощью виртуальных сетей решается проблема распространения широковещательных кадров и вызываемых ими следствий, которые могут развиться в широковещательные штормы и существенно снизить *производительность* сети.

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 повысить безопасность сети, определив с помощью фильтров, настроенных на коммутаторе или маршрутизаторе, политику взаимодействия пользователей из разных виртуальных сетей.

Задание

- Краткий конспект сделать в тетрадь по сл.слайдам: 2;4-5; 28-41.
- Рисунки со слайдов 30-35
- Срок сдачи – в начале сл недели, т.е. до 03 октября.

- **VLAN — ЭТО ТЕХНОЛОГИЯ, КОТОРАЯ ПОЗВОЛЯЕТ СТРОИТЬ ВИРТУАЛЬНЫЕ СЕТИ С НЕЗАВИСИМОЙ ОТ ФИЗИЧЕСКИХ УСТРОЙСТВ ТОПОЛОГИЕЙ.**

например,

- **можно объединить в одну сеть отдел компании, сотрудники которого работают в разных зданиях и подключены к разным коммутаторам.**

или наоборот,

- **создать отдельные сети для устройств, подключённых к одному коммутатору, если этого требует политика безопасности.**

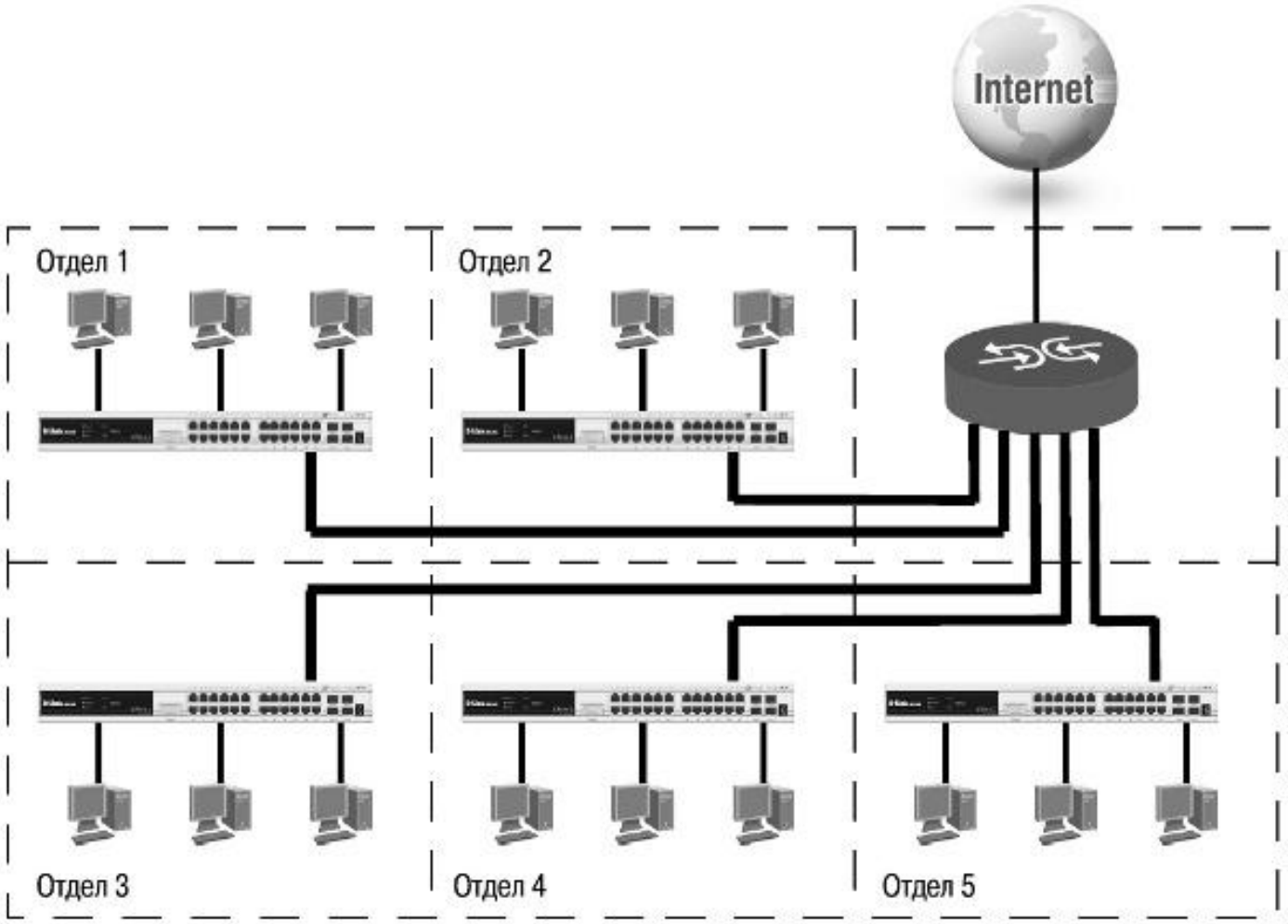
Преимущества VLAN

- Сокращение числа широковещательных запросов, которые снижают пропускную способность сети.
- Повышение безопасности каждой виртуальной сети. Работники одного отдела офиса не смогут отслеживать трафик отделов, не входящих в их VLAN, и не получат доступ к их ресурсам.
- Возможность разделять или объединять отделы или пользователей, территориально удаленных друг от друга. Это позволяет привлекать к рабочему процессу специалистов, не находящихся в здании офиса.
- Создать новую виртуальную сеть можно без прокладки кабеля и покупки коммутатора.
- Позволяет объединить в одну сеть компьютеры, подключенные к разным коммутаторам.
- Упрощение сетевого администрирования. При переезде пользователя VLAN в другое помещение или здание сетевому администратору нет необходимости перекоммутировать кабели, достаточно со своего рабочего места перенастроить сетевое оборудование. А в случае использования динамических VLAN регистрация пользователя в «своём» VLAN на новом месте выполнится автоматически.

Рассмотрим пример, показывающий эффективность использования логической сегментации сетей с помощью технологии *VLAN* при решении типовой задачи организации доступа в *Интернет* сотрудникам офиса. При этом трафик каждого отдела должен быть изолирован.

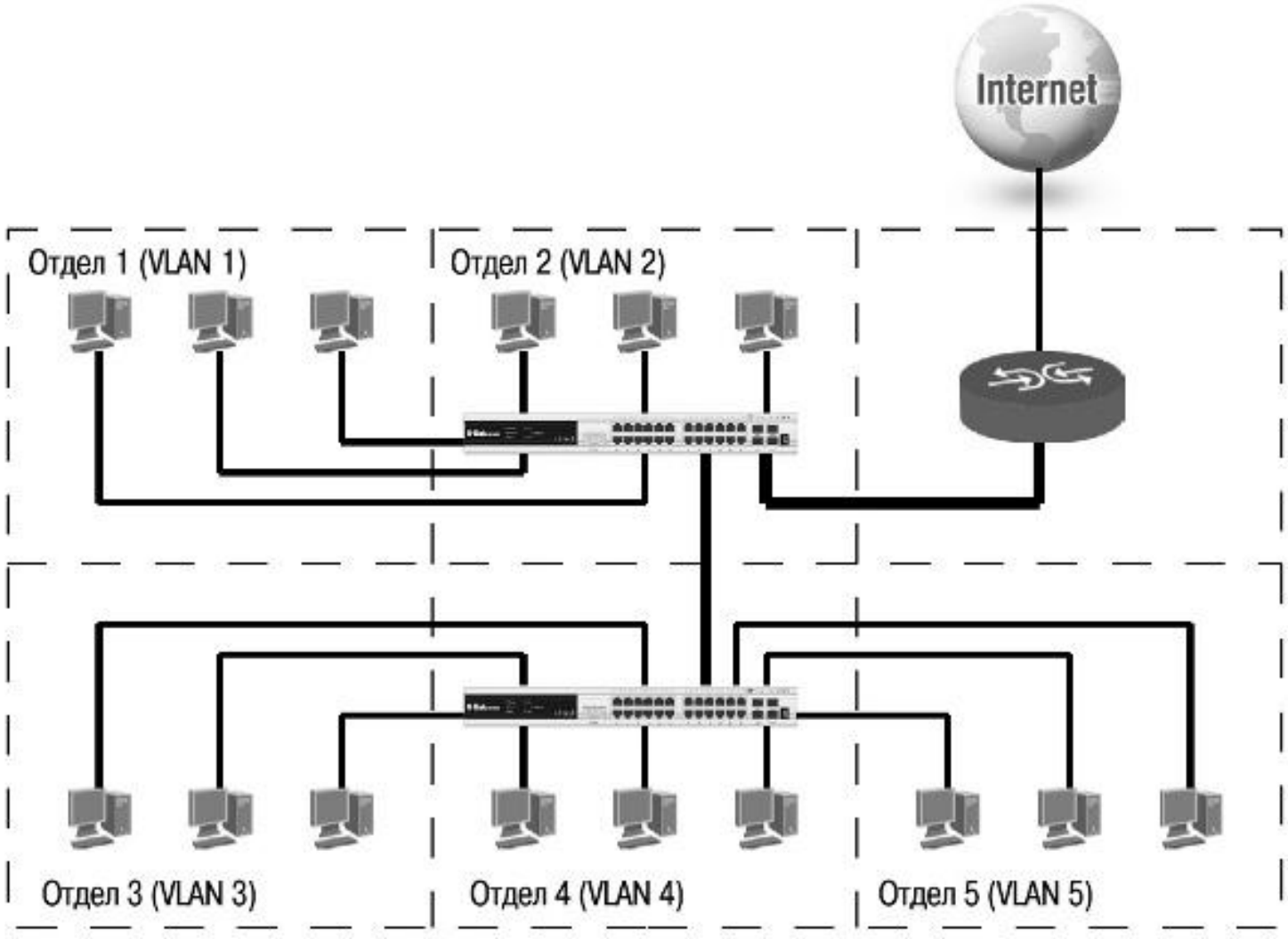
- Предположим, что в офисе имеется несколько комнат, в каждой из которых располагается небольшое количество сотрудников. Каждая комната представляет собой отдельную рабочую группу.
- При стандартном подходе к решению задачи с помощью физической сегментации трафика каждого отдела потребовалось бы в каждую комнату устанавливать отдельный *коммутатор*, который бы подключался к маршрутизатору, предоставляющему *доступ* в *Интернет*. При этом *маршрутизатор* должен обладать достаточным количеством портов, обеспечивающим возможность подключения всех *физических сегментов* (комнат) сети. Данное решение плохо масштабируемо и является дорогостоящим, т.к. при увеличении количества отделов увеличивается количество необходимых коммутаторов, интерфейсов маршрутизатора и магистральных кабелей.

Физическая сегментация сети



- При использовании *виртуальных локальных сетей* уже не требуется подключать пользователей одного отдела к отдельному коммутатору, что позволяет сократить количество используемых устройств и магистральных кабелей. *Коммутатор*, *программное обеспечение* которого поддерживает функцию *виртуальных локальных сетей*, позволяет выполнять логическую сегментацию сети путем соответствующей программной настройки. Это дает возможность подключать пользователей, находящихся в разных сегментах, к одному коммутатору, а также сокращает количество необходимых физических интерфейсов на маршрутизаторе.

Логическая группировка сетевых пользователей в VLAN



Типы VLAN

В коммутаторах могут быть реализованы следующие типы *VLAN*:

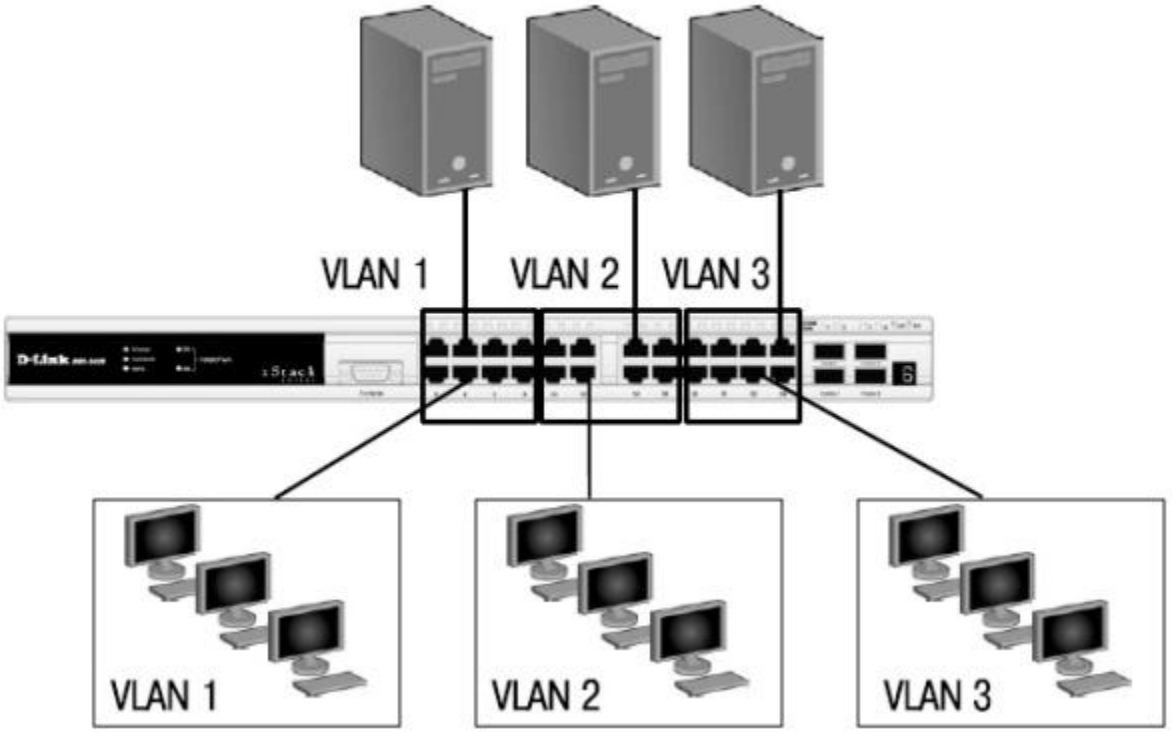
- на основе портов;
- на основе стандарта *IEEE 802.1Q*;
- на основе стандарта IEEE 802.1ad (Q-in-Q *VLAN*);
- на основе портов и протоколов IEEE 802.1v;
- на основе MAC-адресов;
- асимметричные.

VLAN на основе портов

- При использовании *VLAN* на основе портов (Port-based *VLAN*) каждый *порт* назначается в определенную *VLAN*, независимо от того, какой *пользователь* или *компьютер* подключен к этому порту.

- Это означает, что все пользователи, подключенные к этому порту, будут членами одной *VLAN*. *Конфигурация* портов статическая и может быть изменена только вручную.

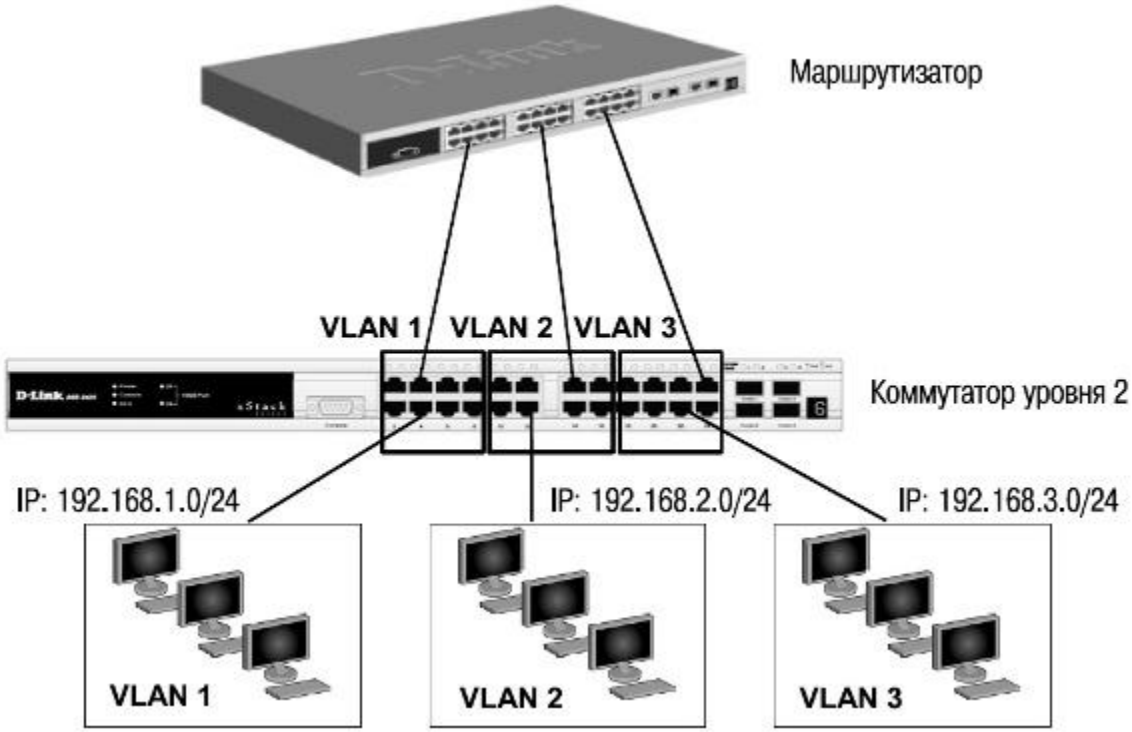
VLAN на основе портов



Основные характеристики *VLAN* на основе портов:

- применяются в пределах одного коммутатора. Если необходимо организовать несколько рабочих групп в пределах небольшой сети на основе одного коммутатора, например, необходимо разнести технический отдел и отдел продаж, то решение *VLAN* на базе портов оптимально подходит для данной задачи;
- простота настройки. Создание виртуальных сетей на основе группирования портов не требует от администратора большого объема ручной работы — достаточно всем портам, помещаемым в одну *VLAN*, присвоить одинаковый идентификатор *VLAN* (*VLAN* ID);
- возможность изменения логической топологии сети без физического перемещения станций. Достаточно всего лишь изменить настройки порта с одной *VLAN* (например, *VLAN* технического отдела) на другую (*VLAN* отдела продаж), и рабочая станция сразу же получает возможность совместно использовать ресурсы с членами новой *VLAN*. Таким образом, *VLAN* обеспечивают гибкость при перемещениях, изменениях и наращивании сети;
- каждый порт может входить только в одну *VLAN*. Для объединения виртуальных подсетей как внутри одного коммутатора, так и между двумя коммутаторами, нужно использовать сетевой уровень OSI-модели. Один из портов каждой *VLAN* подключается к интерфейсу маршрутизатора, который создает таблицу маршрутизации для пересылки кадров из одной подсети (*VLAN*) в другую (IP-адреса подсетей должны быть разными).

Объединение VLAN с помощью маршрутизирующего устройства

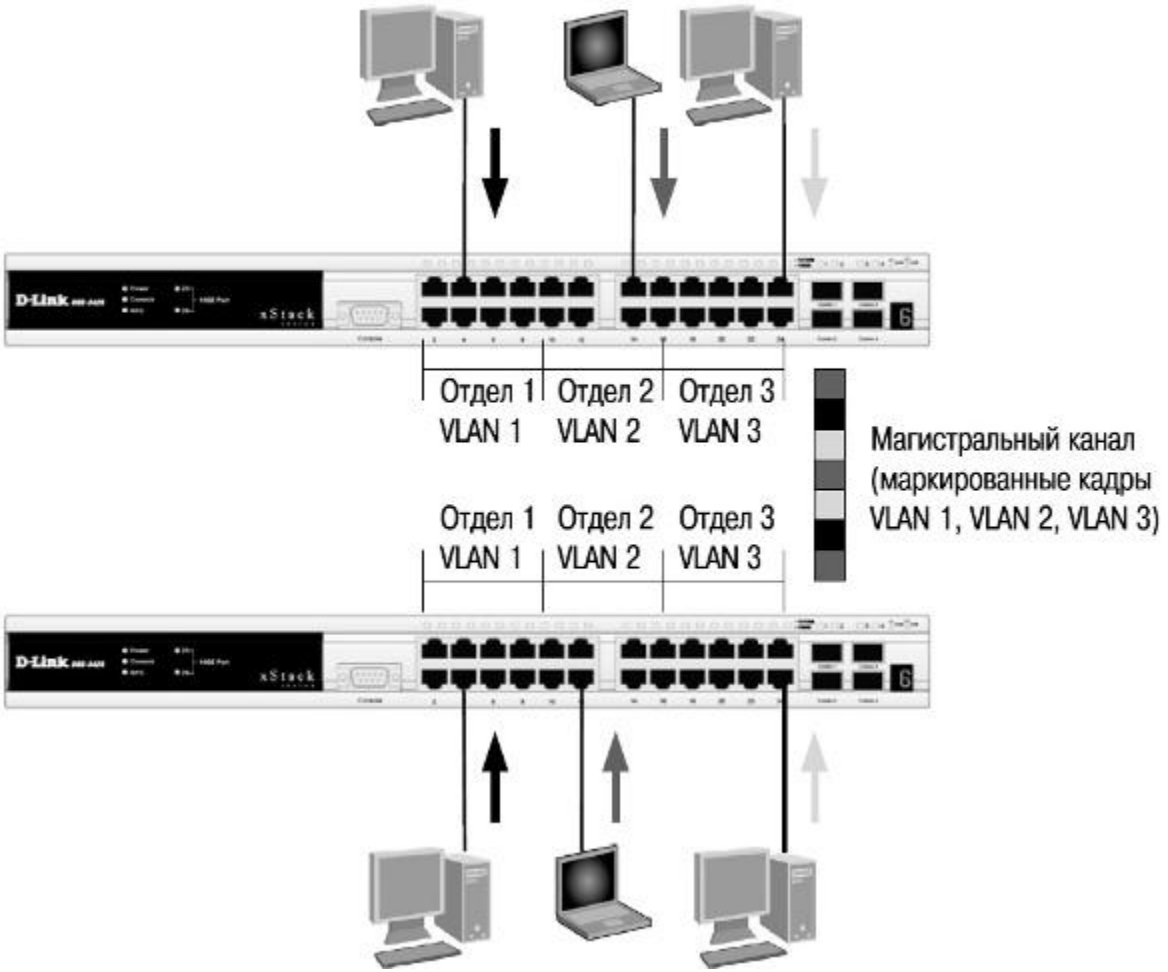


- Недостатком такого решения является то, что один *порт* каждой *VLAN* необходимо подключать к маршрутизатору. Это приводит к *дополнительным расходам* на покупку кабелей и маршрутизаторов, а также порты коммутатора используются очень расточительно. Решить данную проблему можно двумя способами: использовать коммутаторы, которые на основе фирменного решения позволяют включать *порт* в несколько *VLAN*, или использовать коммутаторы уровня 3.

VLAN на основе стандарта IEEE 802.1Q

- Построение *VLAN* на основе портов основано только на добавлении дополнительной информации к адресным таблицам коммутатора и не использует возможности *встраивания* информации о принадлежности к виртуальной сети в передаваемый *кадр*. *Виртуальные локальные сети*, построенные на основе стандарта *IEEE 802.1Q*, используют дополнительные поля кадра для хранения информации о принадлежности к *VLAN* при его перемещении *по* сети. С точки зрения удобства и гибкости настроек, *VLAN* стандарта *IEEE 802.1Q* является лучшим решением *по* сравнению с *VLAN* на основе портов. **Его основные преимущества:**
- гибкость и удобство в настройке и изменении — можно создавать необходимые комбинации *VLAN* как в пределах одного коммутатора, так и во всей сети, построенной на коммутаторах с поддержкой стандарта *IEEE 802.1Q*. Способность добавления тегов позволяет информации о *VLAN* распространяться через множество 802.1Q-совместимых коммутаторов по одному физическому соединению (*магистральному каналу, Trunk Link*);
- позволяет активизировать алгоритм связующего дерева (*Spanning Tree*) на всех портах и работать в обычном режиме. Протокол *Spanning Tree* оказывается весьма полезным для применения в крупных сетях, построенных на нескольких коммутаторах, и позволяет коммутаторам автоматически определять древовидную конфигурацию связей в сети при произвольном соединении портов между собой. Для нормальной работы коммутатора требуется отсутствие *замкнутых маршрутов* в сети. Эти маршруты могут создаваться администратором специально для образования резервных связей или же возникать случайным образом, что вполне возможно, если сеть имеет многочисленные связи, а кабельная система плохо структурирована или документирована. С помощью протокола *Spanning Tree* коммутаторы после построения схемы сети блокируют избыточные маршруты. Таким образом, автоматически предотвращается возникновение петель в сети;
- способность *VLAN IEEE 802.1Q* добавлять и извлекать теги из заголовков кадров позволяет использовать в сети коммутаторы и сетевые устройства, которые не поддерживают стандарт *IEEE 802.1Q*;
- устройства разных производителей, поддерживающие стандарт, могут работать вместе, независимо от какого-либо фирменного решения;
- чтобы связать подсети на сетевом уровне, необходим маршрутизатор или коммутатор L3. Однако для более простых случаев, например, для организации доступа к серверу из различных *VLAN*, маршрутизатор не потребуется. Нужно включить порт коммутатора, к которому подключен сервер, во все подсети, а сетевой адаптер сервера должен поддерживать стандарт *IEEE 802.1Q*.

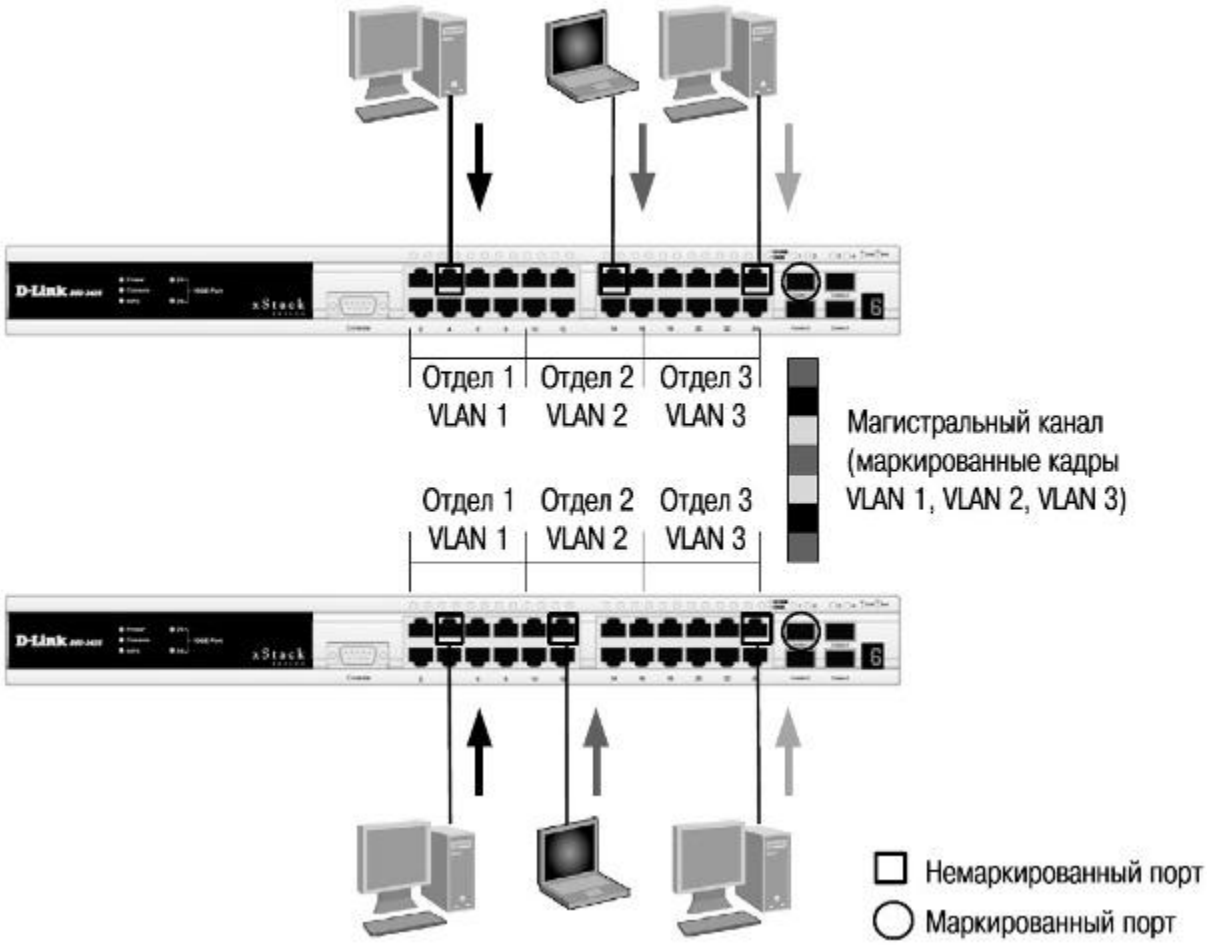
Передача кадров разных VLAN по магистральному каналу связи



Некоторые определения IEEE 802.1Q

- **Tagging ("Маркировка кадра")** — процесс добавления информации о принадлежности к 802.1Q *VLAN* в заголовок кадра.
- **Untagging ("Извлечение тега из кадра")** — процесс извлечения информации о принадлежности к 802.1Q *VLAN* из заголовка кадра.
- **VLAN ID (VID)** — идентификатор *VLAN*.
- **Port VLAN ID (PVID)** — идентификатор порта *VLAN*.
- **Ingress port ("Входной порт")** — порт коммутатора, на который поступают кадры, и при этом принимается решение о принадлежности к *VLAN*.
- **Egress port ("Выходной порт")** — порт коммутатора, с которого кадры передаются на другие сетевые устройства, коммутаторы или рабочие станции, и, соответственно, на нем должно приниматься решение о маркировке.
- Любой порт коммутатора может быть настроен как *tagged* (маркированный) или как *untagged* (немаркированный). Функция *untagging* позволяет работать с теми сетевыми устройствами виртуальной сети, которые не понимают тегов в заголовке кадра Ethernet. Функция *tagging* позволяет настраивать *VLAN* между несколькими коммутаторами, поддерживающими стандарт *IEEE 802.1Q*.

Маркированные и немаркированные порты VLAN



Статические и динамические VLAN

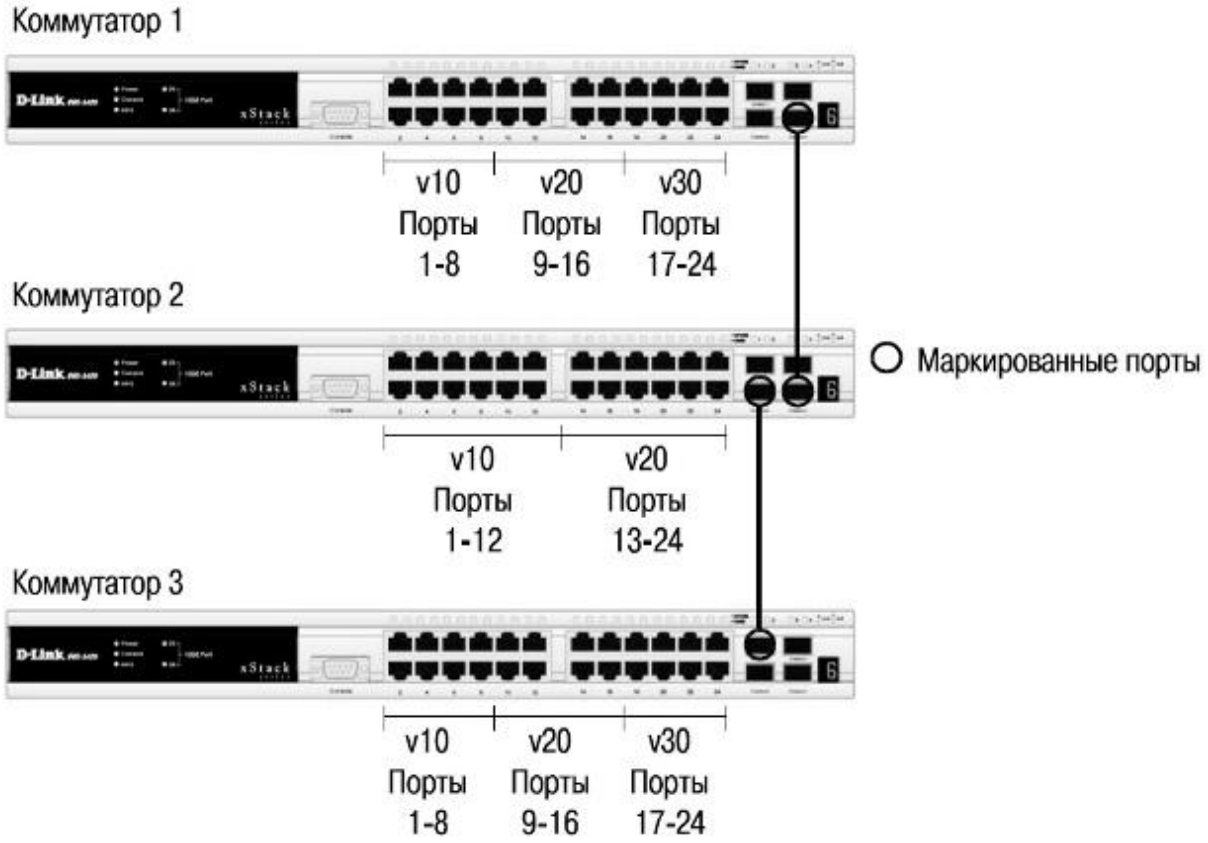
- Для корректной работы *виртуальной локальной сети* требуется, чтобы в базе данных фильтрации (*Filtering Database*) содержалась *информация* о членстве в *VLAN*. Эта *информация* необходима для принятия правильного решения (переслать или отбросить) при передаче кадров между портами коммутатора.
- Существуют два основных способа, позволяющие устанавливать членство в *VLAN*:
- статические *VLAN*;
- динамические *VLAN*.
- В статических *VLAN* установление членства осуществляется вручную администратором сети. При изменении топологии сети или перемещении пользователя на другое рабочее *место* администратору требуется вручную выполнять привязку *порт-VLAN* для каждого нового соединения.
- Членство в динамических *VLAN* может устанавливаться динамически на магистральных интерфейсах коммутаторов на основе протокола GVRP (GARP *VLAN Registration Protocol*). Протокол GARP (*Generic Attribute Registration Protocol*) используется для регистрации и отмены регистрации атрибутов, таких как *VID*.
- Статические записи о регистрации в *VLAN* (*Static VLAN Registration Entries*) используются для представления информации о статических *VLAN* в базе данных фильтрации. Эти записи позволяют задавать точные настройки для каждого порта *VLAN*: *идентификатор VLAN*, тип порта (маркированный или немаркированный), один из управляющих элементов протокола GVRP:
- Fixed (порт всегда является членом данной *VLAN*);
- Forbidden (порту запрещено регистрироваться как члену данной *VLAN*);
- Normal (обычная регистрация с помощью протокола GVRP).
- *Управляющие* элементы GVRP используются для активизации работы протокола на портах коммутатора, а также для указания того, может ли данная *VLAN* быть зарегистрирована на порте.
- Динамические записи о регистрации в *VLAN* (*Dynamic VLAN Registration Entries*) используются для представления в базе данных фильтрации информации о портах, членство в *VLAN* которых установлено динамически. Эти записи создаются, обновляются и удаляются в процессе работы протокола GVRP.

Протокол GVRP

- Протокол GVRP определяет способ, посредством которого коммутаторы обмениваются информацией о сети *VLAN*, чтобы автоматически зарегистрировать членов *VLAN* на портах во всей сети. Он позволяет динамически создавать и удалять *VLAN* стандарта *IEEE 802.1Q* на магистральных портах, автоматически регистрировать и исключать атрибуты *VLAN* (под регистрацией *VLAN* подразумевается включение порта в *VLAN*, под исключением — удаление порта из *VLAN*).
- Протокол GVRP использует сообщения GVRP BPDU (GVRP *Bridge Protocol Data Units*), рассылаемые на многоадресный MAC-*адрес* 01-80-C2-00-00-21 для оповещения устройств-подписчиков о различных событиях. Оповещения (*advertisement*) могут содержать информацию о выполнении следующих действий:
- **Join message** — регистрация порта в *VLAN*.JoinEmpty: VLAN на локальном подписчике не настроена; JoinIn: VLAN на локальном подписчике зарегистрирована;
- **Leave message** — удаление *VLAN* с конкретного порта.LeaveEmpty: VLAN на локальном подписчике не настроена; LeaveIn: VLAN на локальном подписчике удалена;
- **Leave message** — удаление всех, зарегистрированных на порте *VLAN*. Это сообщение отправляется после того, как истечет время, заданное таймером LeaveAll Timer;
- **Empty message** — требование повторного динамического оповещения и статической настройки *VLAN*.

Пример настройки протокола GVRP

- В примере, показанном на рис., требуется настроить возможность динамического распространения по сети информации о *VLAN* v30 с использованием протокола GVRP. Ниже приведены настройки коммутаторов.



Настройка коммутаторов 1, 3

- Удалить соответствующие порты из *VLAN* по умолчанию (default *VLAN*) и создать новые *VLAN*.

```
config vlan default delete 1-24
create vlan v10 tag 10
create vlan v20 tag 20
create vlan v30 tag 30
```

- В созданные *VLAN* добавить порты, для которых необходимо указать, какие из них являются маркированными и немаркированными.

```
config vlan v10 add untagged 1-8
config vlan v20 add untagged 9-16
config vlan v30 add untagged 17-24
config vlan v10 add tag 25-26
config vlan v20 add tag 25-26
```

- Активизировать протокол GVRP и функцию оповещения о соответствующей *VLAN* (в данном примере *VLAN* v30) по сети.

```
config vlan v30 advertisement enable enable gvrp
config port_vlan 25-26 gvrp_state enable
```

Настройка коммутатора 2

```
config vlan default delete 1-24
create vlan v10 tag 10
create vlan v20 tag 20
config vlan v10 add untagged 1-12
config vlan v20 add untagged 13-24
config vlan v10 add tagged 25-26
config vlan v20 add tagged 25-26
enable gvrp
config port_vlan 25-26 gvrp_state enable
```

Асимметричные VLAN

- Для обеспечения возможности использования разделяемых ресурсов (серверов, *Интернет*-шлюзов и т.д.) пользователями из разных сетей *VLAN* в программном обеспечении коммутаторов **2-го уровня** D-Link реализована *поддержка* функции *Asymmetric VLAN* (ассиметричные *VLAN*). Эта *функция* позволяет клиентам из разных *VLAN* взаимодействовать с разделяемыми устройствами (например, серверами), *не поддерживающими тегирование 802.1Q*, через один *физический канал* связи с коммутатором, не требуя использования внешнего маршрутизатора. Активизация функции *Asymmetric VLAN* на коммутаторе 2-го уровня позволяет сделать его *немаркированные* порты *членами нескольких виртуальных локальных сетей*. При этом рабочие станции остаются полностью изолированными друг от друга. Например, асимметричные *VLAN* могут быть настроены так, чтобы обеспечить *доступ* к почтовому серверу всем почтовым клиентам. Клиенты смогут отправлять и получать данные через *порт* коммутатора, подключенный к почтовому серверу, но прием и *передача данных* через остальные порты будет для них запрещена.
- При активизации асимметричных *VLAN* каждому порту коммутатора назначается уникальный PVID в соответствии с идентификатором *VLAN*, членом которой он является. При этом каждый *порт* может получать кадры от *VLAN по* умолчанию.
- **Внимание**: функция *Asymmetric VLAN* не поддерживается коммутаторами 3-го уровня. Организация обмена данными между устройствами различных *VLAN*, не поддерживающих *тегирование*, реализуется в таких коммутаторах с помощью маршрутизации и *списков управления доступом* (ACL), ограничивающих доступ устройств к сети.
- Основное различие между базовым стандартом 802.1Q *VLAN* (или симметричными *VLAN*) и асимметричными *VLAN* заключается в том, как выполняется *отображение* MAC-адресов. Симметричные *VLAN* используют отдельные адресные таблицы, и, таким образом, не происходит пересечения MAC-адресов между *виртуальными локальными сетями*. Асимметричные *VLAN* используют одну общую таблицу MAC-адресов.
- При использовании асимметричных *VLAN* существует следующее ограничение: не функционирует механизм *IGMP Snooping*.
- *По* умолчанию асимметричные *VLAN* на коммутаторах D-Link отключены.

Примеры настройки асимметричных VLAN

На рис. 6.24 показана схема реализации ассиметричных *VLAN* в пределах одного коммутатора. Пользователи *VLAN* v2 и v3 могут получать доступ к разделяемым серверам и Интернет-шлюзу, находящимся в *VLAN* v1. *Виртуальные локальные сети VLAN* v2 и v3 изолированы друг от друга.

Для реализации этой схемы на коммутаторе D-Link необходимо выполнить следующие настройки:

Настройка коммутатора

```
enable asymmetric_vlan
create vlan v2 tag 2
create vlan v3 tag 3
config vlan v2 add untagged 9-16
config vlan v3 add untagged 1-8,17-24
config gvrp 1-8 pvid 3
config gvrp 9-16 pvid 2
config gvrp 17-24 pvid 1
```

Коммутатор

	VLAN v1 (разделяемая VLAN)	VLAN v2 (пользовательская VLAN)	VLAN v3 (пользовательская VLAN)
Немаркированные порты	17–24	9–16	1–8
Маркированные порты	–	–	–

Функция Traffic Segmentation

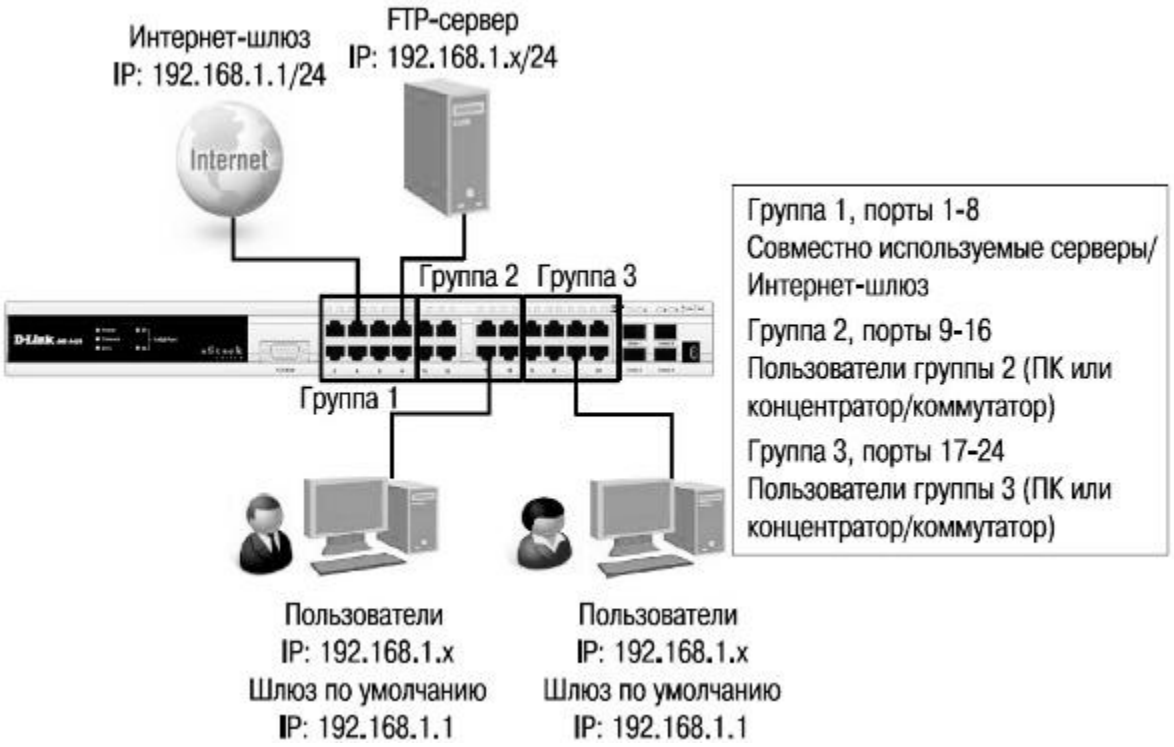
- *Функция Traffic Segmentation* (*сегментация* трафика) служит для разграничения доменов на канальном уровне. Она позволяет настраивать порты или группы портов коммутатора таким образом, чтобы они были полностью изолированы друг от друга, но в то же время имели *доступ* к разделяемым портам, используемым для подключения серверов или магистрали сети. Этот метод изоляции трафика аналогичен функции *Asymmetric VLAN*, но его применение ограничено пределами одного коммутатора или нескольких коммутаторов в стеке, т.к. членство в группе портов не может распространяться *по* сети.

Можно выделить следующие преимущества функции *Traffic Segmentation* *по* сравнению с *Asymmetric VLAN*:

- простота настройки;
- поддерживается работа *IGMP Snooping*;
- функция *Traffic* Segmentation может быть представлена в виде иерархического дерева (при иерархическом подходе разделяемые ресурсы должны быть на "вершине" дерева);
- нет ограничений на создание количества групп портов.
- *Функция* сегментации трафика может использоваться с целью сокращения трафика внутри сетей *VLAN* 802.1Q, позволяя разбивать их на более маленькие группы. При этом правила *VLAN* имеют более высокий приоритет при передаче трафика. Правила *Traffic Segmentation* применяются после них.

Пример использования функции Traffic Segmentation

- Пользователи групп 2 и 3 имеют доступ к совместно используемому FTP-серверу и Интернет-шлюзу, но обмен данными между группами 2 и 3 запрещен.



Подведем итоги

Принципы работы VLAN

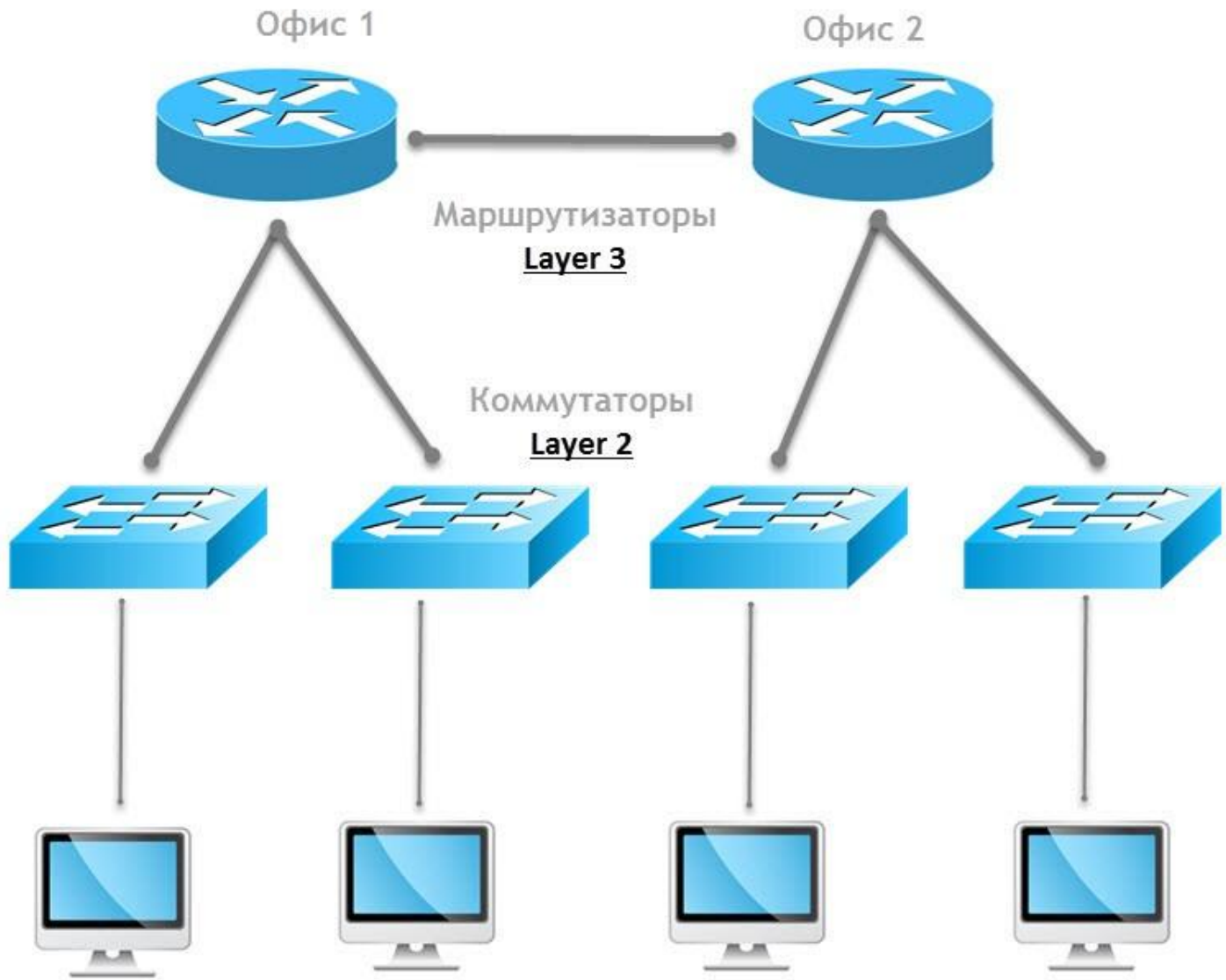
- Компьютеры в локальной сети соединяются между собой с помощью сетевого оборудования — коммутаторов. По умолчанию все устройства, подключённые к портам одного коммутатора, могут взаимодействовать, обмениваясь сетевыми пакетами. Любой компьютер может направить широковещательный пакет, адресованный всем устройствам в этой сети, и все остальные компьютеры, подключённые к коммутатору, получат его. Все слышат всех.
- Большое количество широковещательных пакетов, отправляемых устройствами, приводит к снижению производительности сети, поскольку вместо полезных операций коммутаторы заняты обработкой данных, адресованных сразу всем.

- Чтобы снизить влияние широковещательных рассылок на производительность, сеть разделяют на изолированные сегменты. При этом каждый широковещательный пакет будет распространяться только в пределах сегмента, к которому подключен компьютер-отправитель.
- Добиться такого результата можно, подключив разные сегменты к разным физическим коммутаторам, не соединённым между собой, либо соединить их через маршрутизаторы, которые не пропускают широковещательные рассылки.

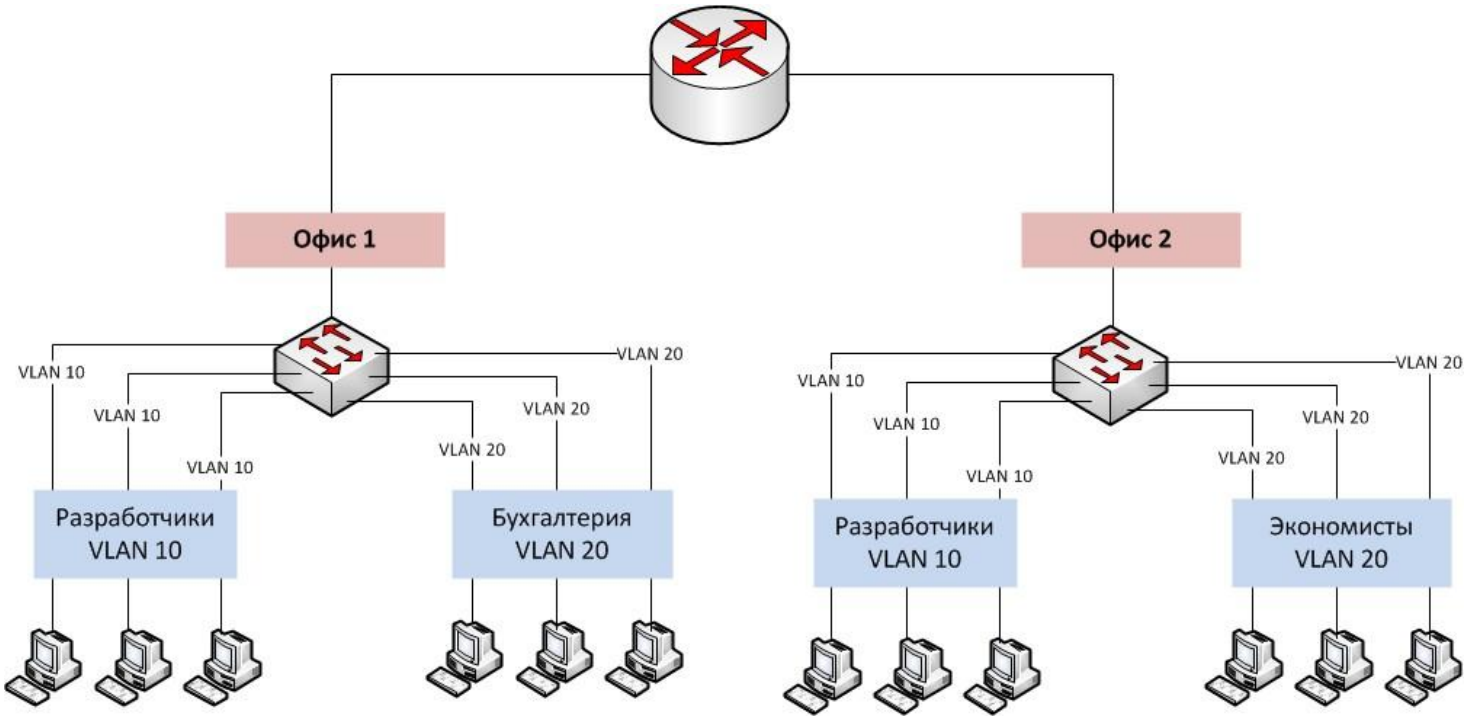
Принципы работы VLAN

- Компьютеры в локальной сети соединяются между собой с помощью сетевого оборудования — коммутаторов. По умолчанию все устройства, подключённые к портам одного коммутатора, могут взаимодействовать, обмениваясь сетевыми пакетами. Любой компьютер может направить широковещательный пакет, адресованный всем устройствам в этой сети, и все остальные компьютеры, подключённые к коммутатору, получат его. Все слышат всех.
- Большое количество широковещательных пакетов, отправляемых устройствами, приводит к снижению производительности сети, поскольку вместо полезных операций коммутаторы заняты обработкой данных, адресованных сразу всем.

- Чтобы снизить влияние широковещательных рассылок на производительность, сеть разделяют на изолированные сегменты. При этом каждый широковещательный пакет будет распространяться только в пределах сегмента, к которому подключен компьютер-отправитель.
- Добиться такого результата можно, подключив разные сегменты к разным физическим коммутаторам, не соединённым между собой, либо соединить их через маршрутизаторы, которые не пропускают широковещательные рассылки.


Офис 1
Офис 2
Маршрутизаторы
Layer 3
Коммутаторы
Layer 2

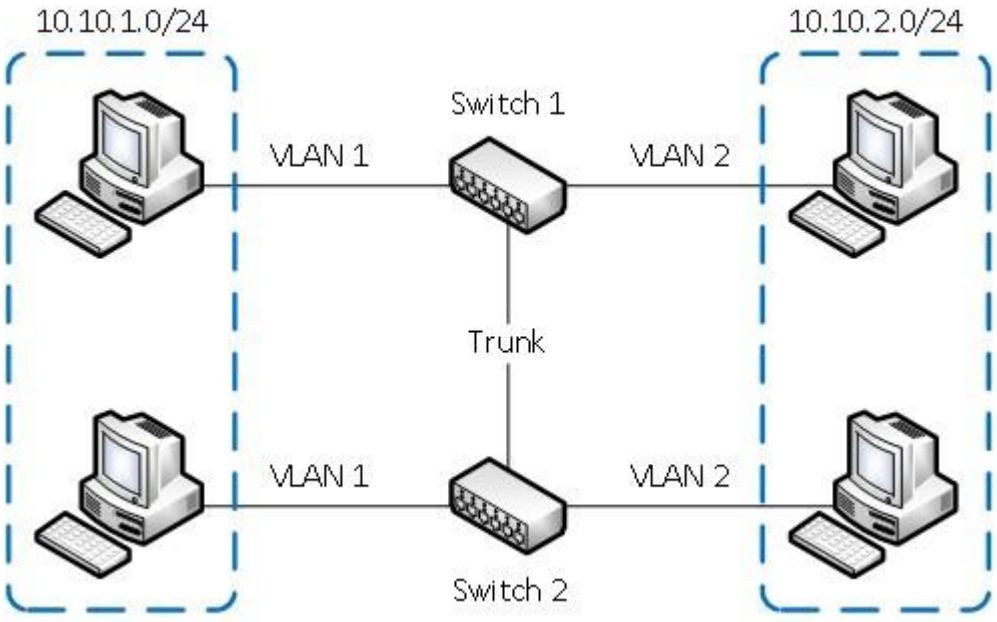
- VLANы позволяют изолировать сегменты сети с помощью одного физического коммутатора. При этом функционально всё будет выглядеть полностью аналогично, но для каждого офиса используется один коммутатор с поддержкой VLAN.



- В основе технологии VLAN лежит стандарт IEEE 802.1Q. Он позволяет добавлять в Ethernet-трафик информацию о принадлежности передаваемых данных к той или иной виртуальной сети — теги VLAN. С их помощью коммутаторы и маршрутизаторы могут выделить из общего потока передаваемых по сети кадров те, что относятся к конкретному сегменту.
- Технология VLAN даёт возможность организовать функциональный эквивалент нескольких LAN-сетей без использования набора из коммутаторов и кабелей, которые понадобились бы для их реализации в физическом виде. Физическое сетевое оборудование заменяется виртуальным. Отсюда термин Virtual LAN.

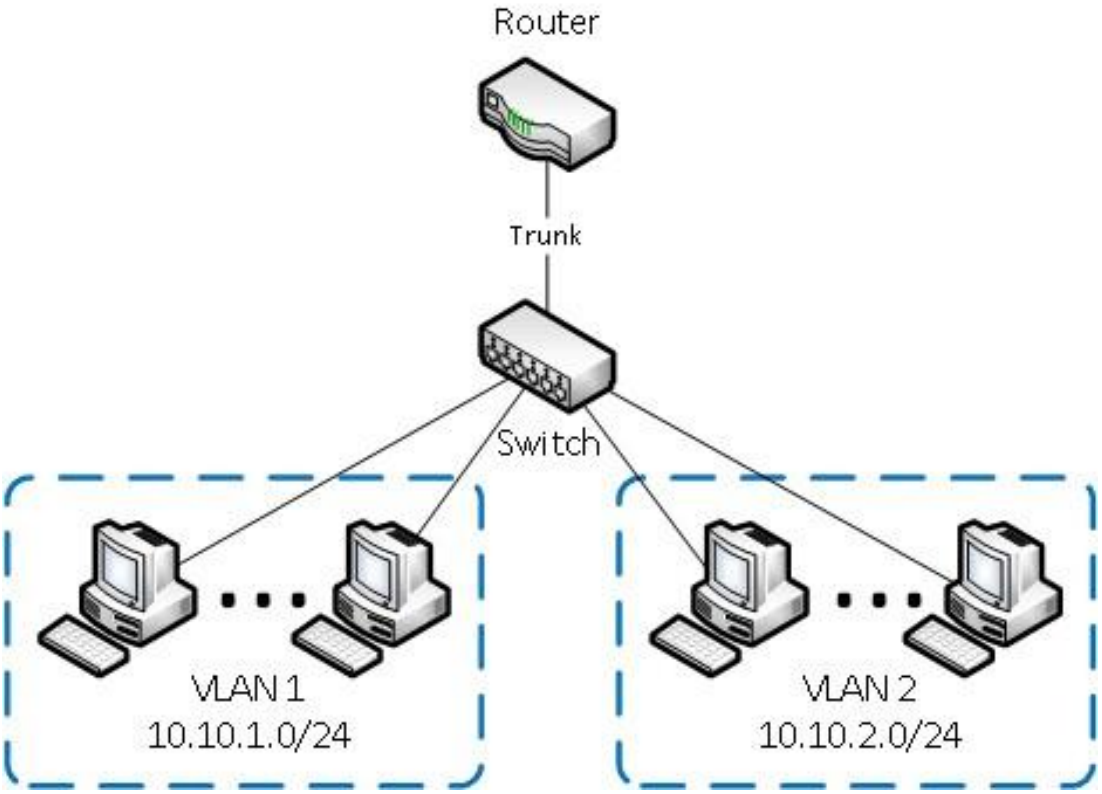
Возможности VLAN (для решения задач):

- **Объединить в единую сеть группы компьютеров, подключённых к разным коммутаторам:**



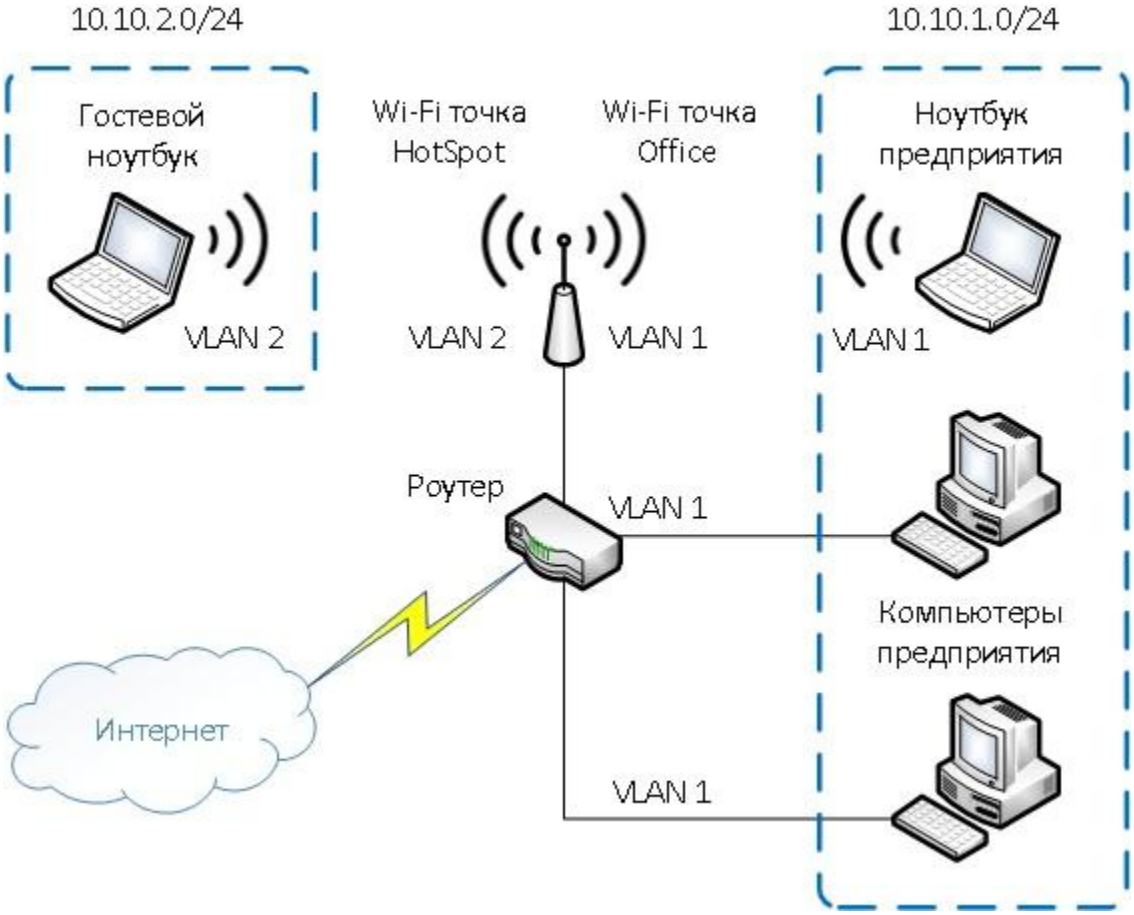
- Компьютеры в VLAN 1 будут взаимодействовать между собой, хотя подключены к разным физическим коммутаторам, при этом сети VLAN 1 и VLAN 2 будут невидимы друг для друга.

- **Разделить на разные сети компьютеры, подключённые к одному коммутатору**



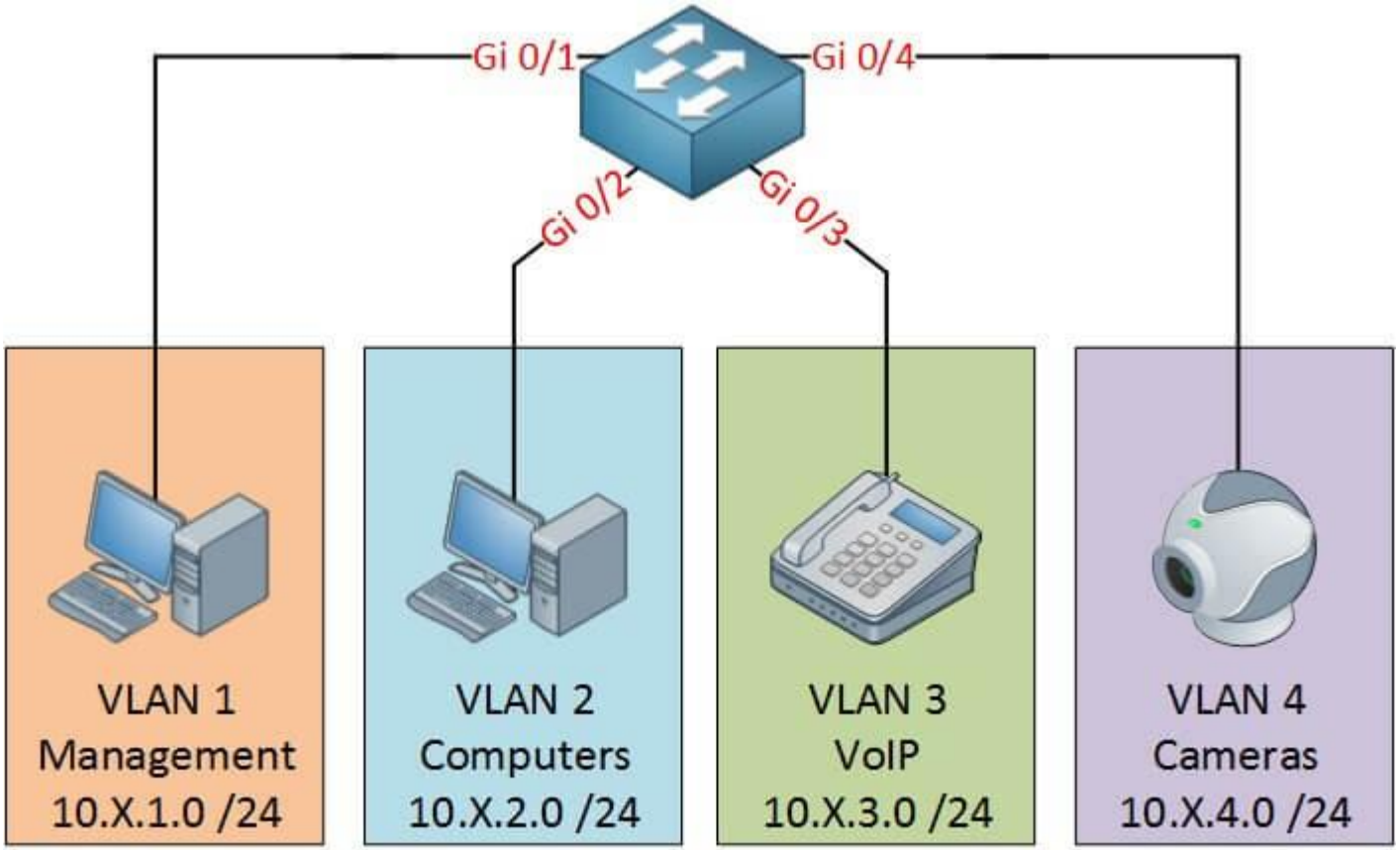
При этом устройства в VLAN 1 и VLAN 2 не смогут взаимодействовать между собой.

- **Разделить гостевую и корпоративную беспроводную сеть компании:**

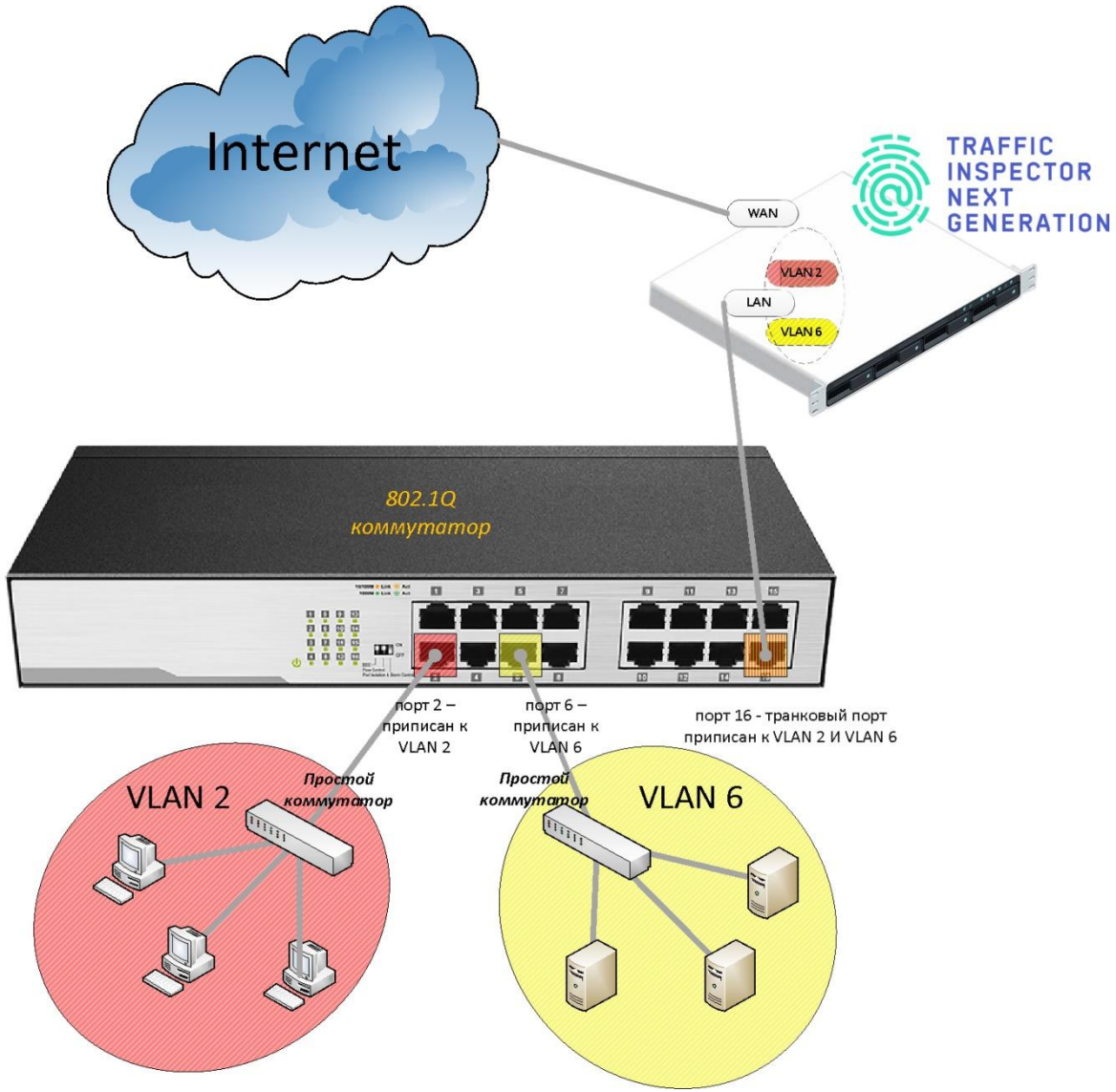


- Гости смогут подключаться к интернету, но не получат доступа к сети компании.

- **Обеспечить взаимодействие территориально распределённых отделов компании как единого целого:**



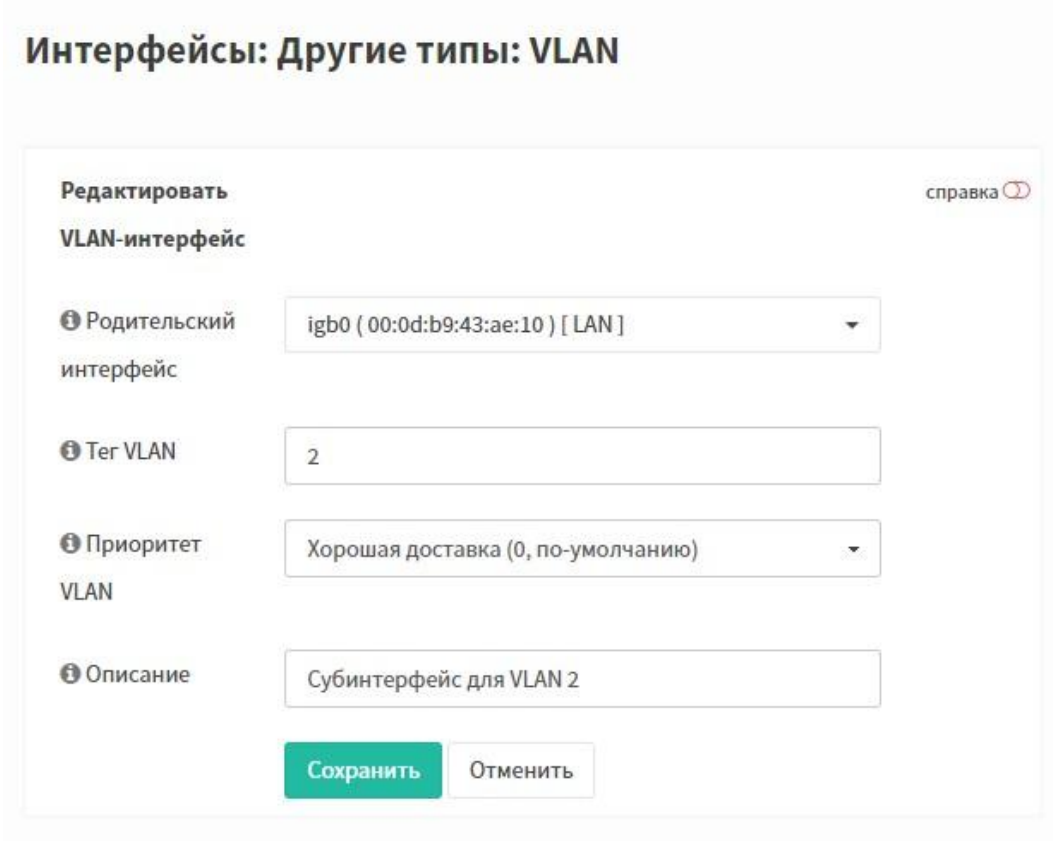
VLAN с Traffic Inspector Next Generation



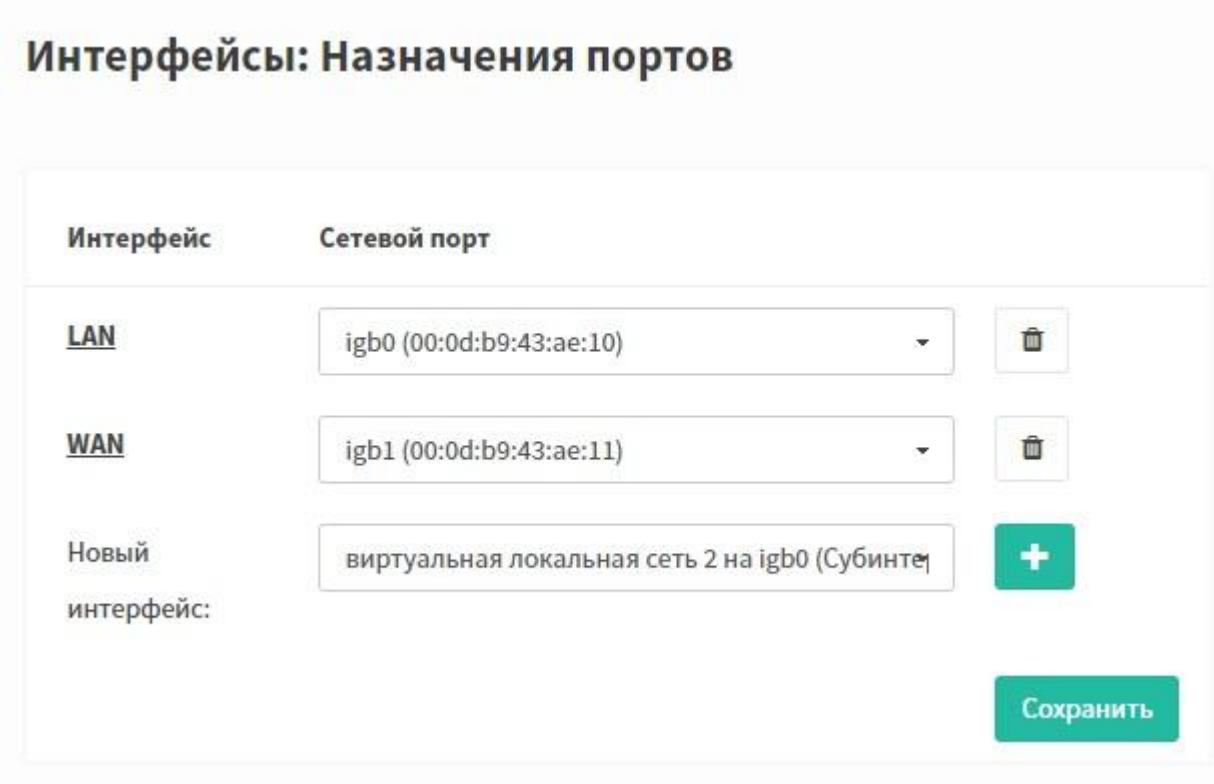
- Технология VLAN позволяет одному устройству Traffic Inspector Next Generation контролировать доступ в интернет для нескольких подразделений, причём для каждого сегмента можно установить свои правила взаимодействия с глобальной сетью.
- На рисунке изображена сеть компании, подключенная к интернет через сервер Traffic Inspector Next Generation. Сеть организована на базе одного коммутатора, на котором создано два виртуальных сегмента — VLAN 2 и VLAN 6. В первом сегменте находятся компьютеры пользователей, во втором — серверы. Устройство Traffic Inspector Next Generation подключено к транковому порту коммутатора — специальному порту, который «слышит» пакеты от всех виртуальных сетей. Трафик, передаваемый или принимаемый на транковый порт, всегда образован тегированными кадрами.

Чтобы управлять работой двух виртуальных сетей на одном устройстве Traffic Inspector Next Generation, достаточно в настройках выполнить следующие операции:

1. Создать VLAN-интерфейсы (Интерфейсы → Другие типы → VLAN)



2. Добавить VLAN-интерфейсы в веб-интерфейс (Интерфейсы → Назначения портов, указать VLAN в поле «Новый интерфейс»)



3. Задать параметры TCP/IP для VLAN-интерфейсов (в разделе «Интерфейсы»)

Включен	Флаг установлен
Описание	VLAN2
Блокировать частные сети	Флаг снят
Блокировать bogon сети	Флаг снят
Тип конфигурации IPv4	Статический IPv4
IPv4 адрес	192.168.2.1/24

4. Сохранить изменения.

Заключение

- Использование VLAN не только упрощает жизнь системным администраторам, позволяя быстро вносить изменения в структуру сети, но и даёт организациям возможность экономить на сетевом оборудовании.
- Администратор Роман, о котором шла речь в начале статьи, обошёлся без покупки дополнительного оборудования, настроив на коммутаторах VLAN для каждого отдела. Это позволило высвободить из старого офиса два коммутатора и использовать их для построения сети в новом офисе. Кроме того, благодаря VLAN решилась проблема с маршрутизацией трафика по WAN-каналу.