Организация администрирования компьютерных систем

Лекции.

Тема 3. Виртуальные локальные сети (VLAN)

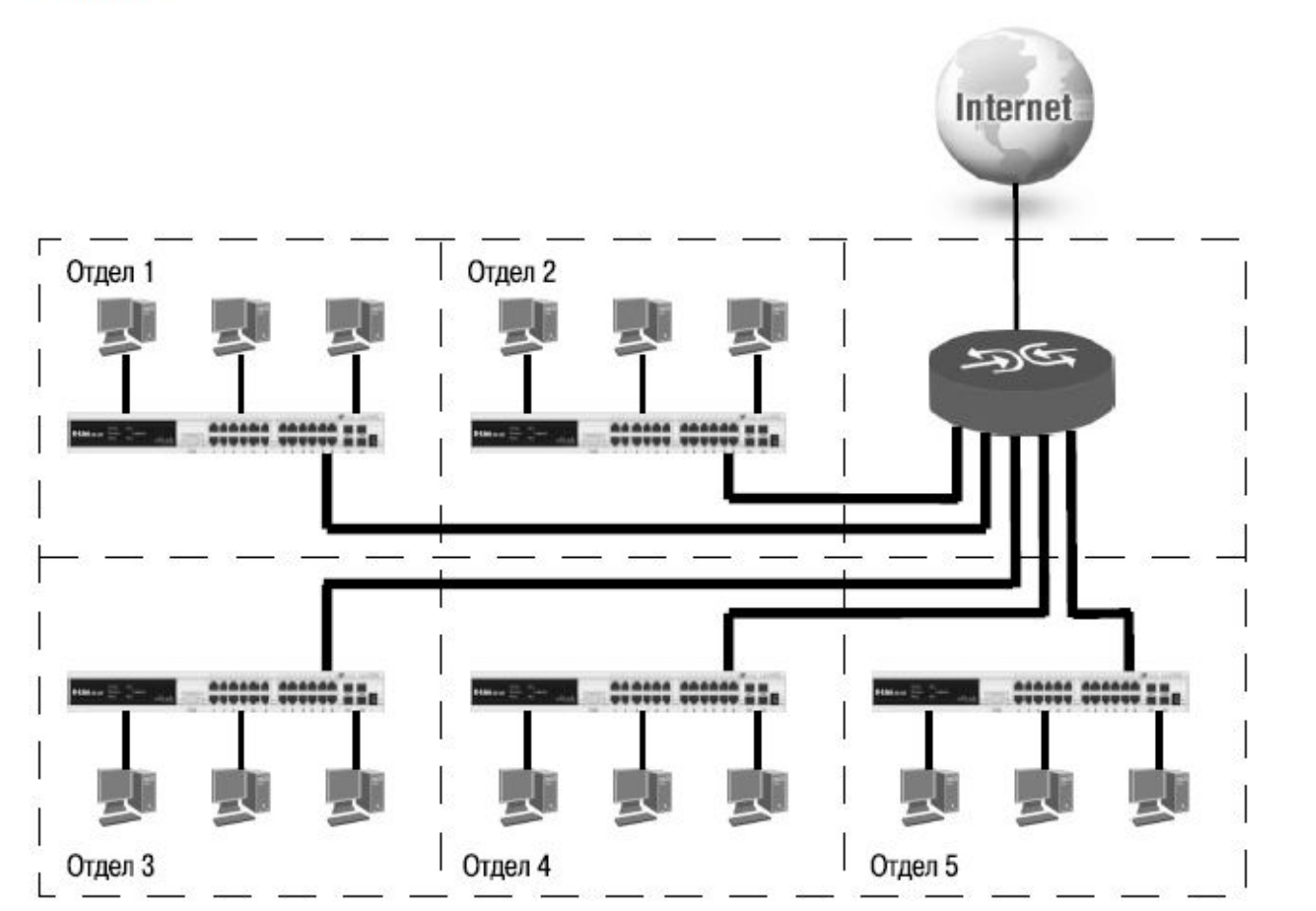
3.1. Понятие VLAN и их типы

- *Широковещательные кадры* — это кадры, передаваемые на все узлы сети. Они необходимы для работы многих сетевых протоколов, таких как ARP, BOOTP или DHCP. С их помощью рабочая станция оповещает другие компьютеры о своем появлении в сети.
- Широковещательные кадры могут привести к нерациональному использованию полосы пропускания, особенно в крупных сетях. Для того чтобы этого не происходило, важно ограничить область распространения широковещательного трафика (эта область называется *широковещательным доменом)* — организовать небольшие широковещательные домены, или виртуальные локальные сети (Virtual LAN, VLAN)
- *Виртуальной локальной сетью* называется логическая группа узлов се ти, 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.

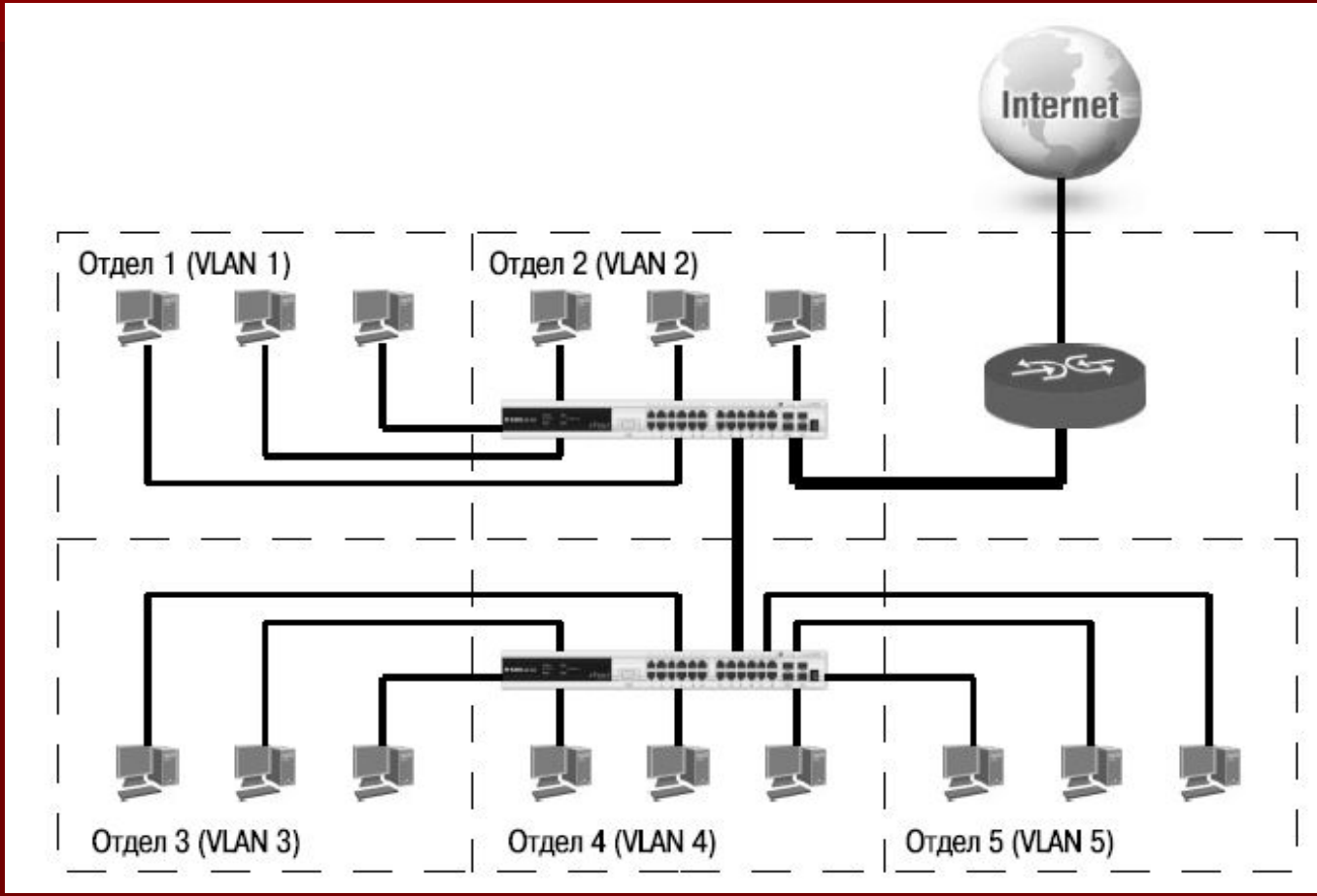
VLAN обладают следующими преимуществами:

- 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.

Физическая сегментация сети



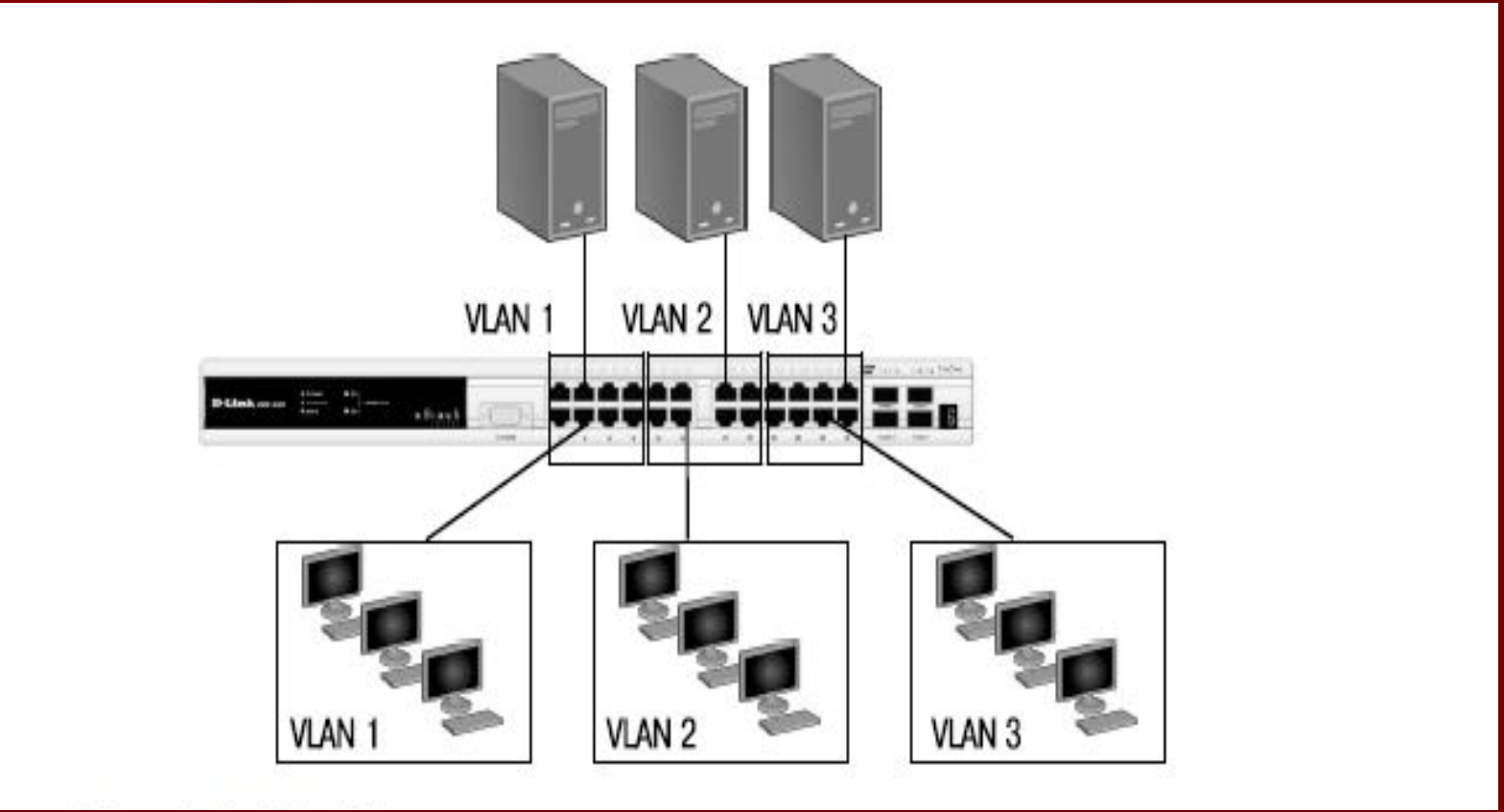
Логическая группировка сетевых пользователей в VLAN



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.

3.3.VLAN на основе портов (Port-based VLAN)



Основные характеристики VLAN на основе портов:

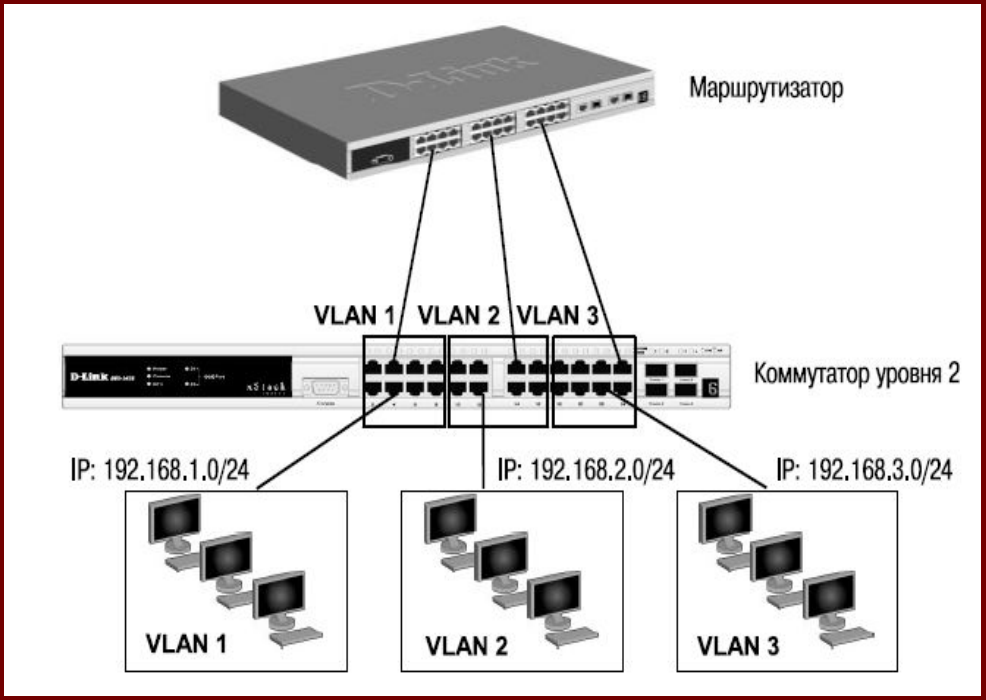
- применяются в пределах одного коммутатора. Если необходимо организовать несколько рабочих групп в пределах небольшой сети на основе одного коммутатора, например, необходимо разнести технический отдел и отдел продаж, то решение VLAN на базе портов оптимально подходит для данной задачи;
- простота настройки. Создание виртуальных сетей на основе груп пирования портов не требует от администратора большого объема ручной работы — достаточно всем портам, помещаемым в одну VLAN, присвоить одинаковый идентификатор VLAN (VLAN ID);

Основные характеристики VLAN на основе портов:

- 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

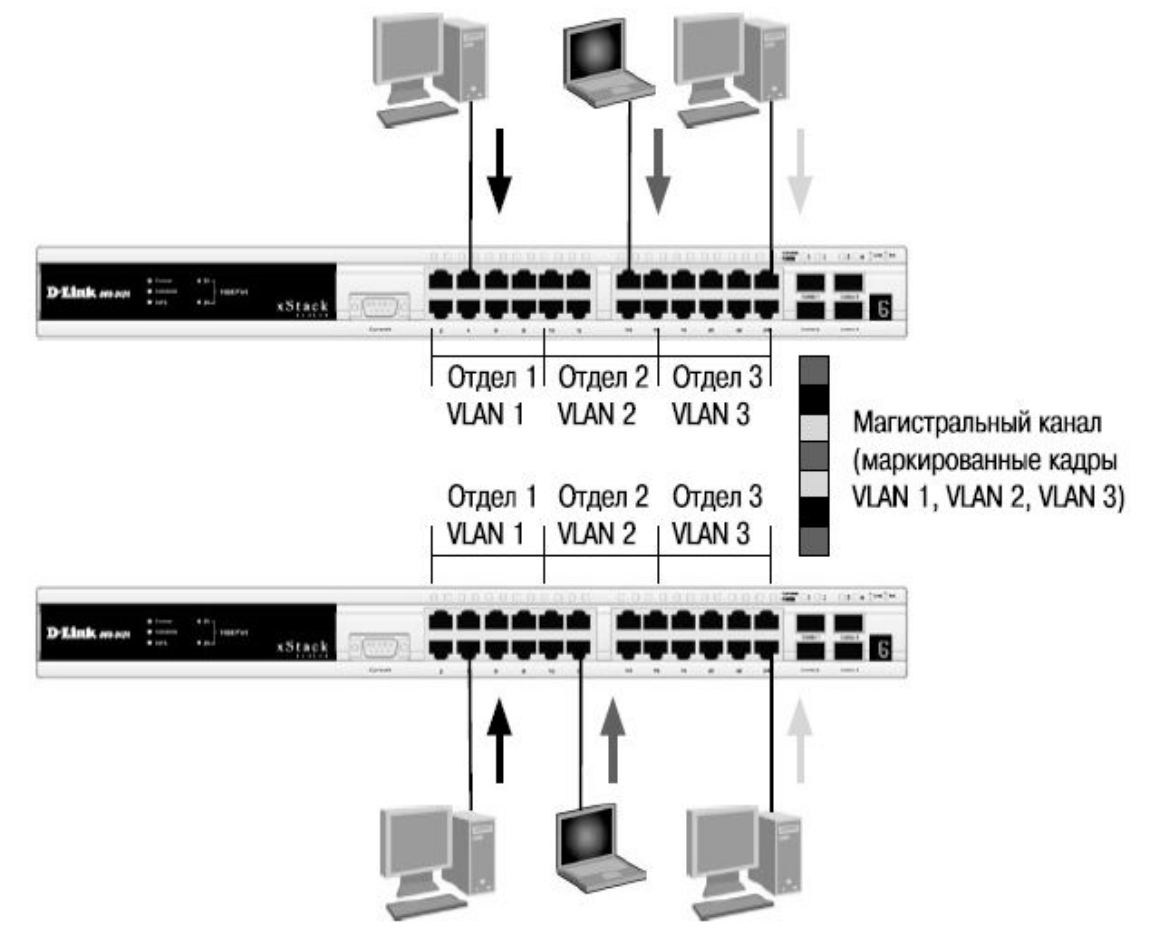
- Недостаток решения - один порт каждой VLAN необходимо подключать к маршрутизатору .
- Решить данную проблему можно двумя способами: использовать коммутаторы, которые на основе фирменного решения позволяют включать порт в несколько VLAN, или использовать коммутаторы уровня 3



3.3. VLAN на основе стандарта IEEE 802.1Q

- 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

Передача кадров разных VLAN по магистральному каналу связи



Преимущества VLAN на основе стандарта IEEE 802.1Q:

- 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 со единению *(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 об разом, 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 возник новение петель в сети;

Преимущества VLAN на основе стандарта IEEE 802.1Q:

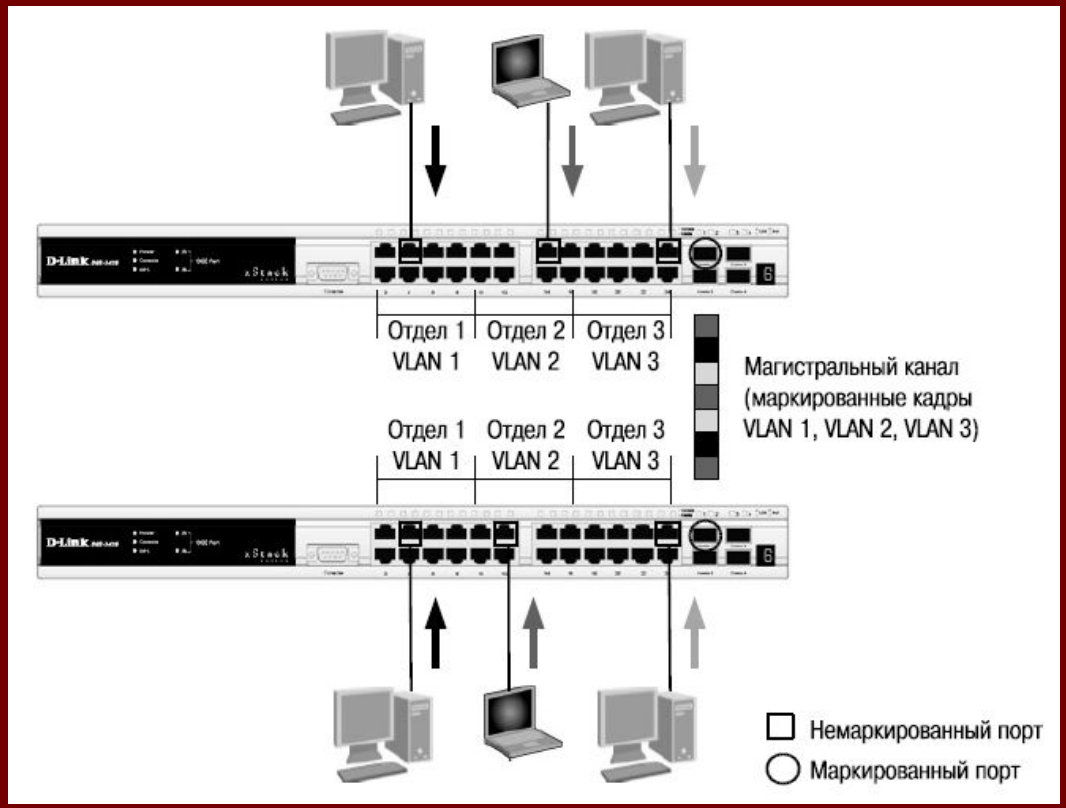
- способность VLAN IEEE 802.1Q добавлять и извлекать теги из заголовков кадров позволяет использовать в сети коммутаторы и сетевые устройства, которые не поддерживают стандарт IEEE 802.1Q;
- устройства разных производителей, поддерживающие стандарт, могут работать вместе, независимо от какого-либо фирменного 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.

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.

Маркированные и немаркированные порты VLAN

- 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

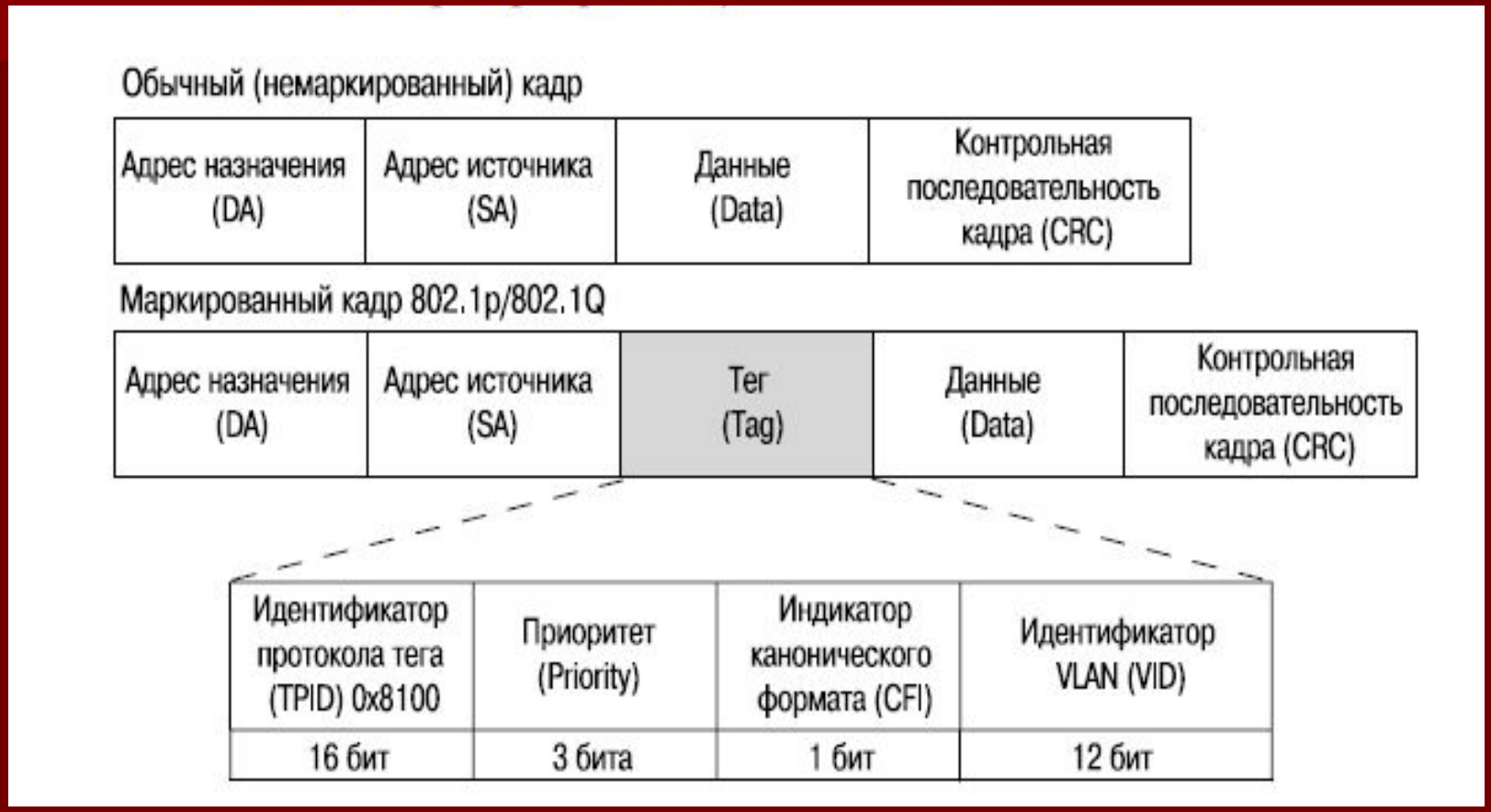


Тег VLAN IEEE 802.1Q

Стандарт IEEE 802.1Q определяет изменения в структуре кадра Ethernet, позволяющие передавать информацию о VLAN по сети. На слайде изображен формат тега 802.1Q VLAN. К кадру Ethernet добавлены 32 бита (4 байта), которые увеличивают его размер до 1522 байт. Первые 2 байта (поле Tag Protocol Identifier, TPID) с фиксированным значением 0x8100 определяют, что кадр содержит тег протокола 802.1Q. Остальные 2 байта содержат следующую информацию:

- *Priority («Приоритет»)* — 3 бита поля приоритета передачи кодируют до восьми уровней приоритета (от 0 до 7, где 7 — наивысший приоритет), которые используются в стандарте 802.1p;
- *Canonical Format Indicator (CFI)* — 1 бит индикатора канонического формата зарезервирован для обозначения кадров сетей других типов (Token Ring, FDDI), передаваемых по магистрали Ethernet;
- *VID (VLAN ID*) — 12-битный идентификатор VLAN определяет, какой VLAN принадлежит трафик. Поскольку под поле VID отведено 12 бит, то можно задать 4094 уникальных VLAN (VID 0 и VID 4095 зарезервированы).

Маркированный кадр Ethernet

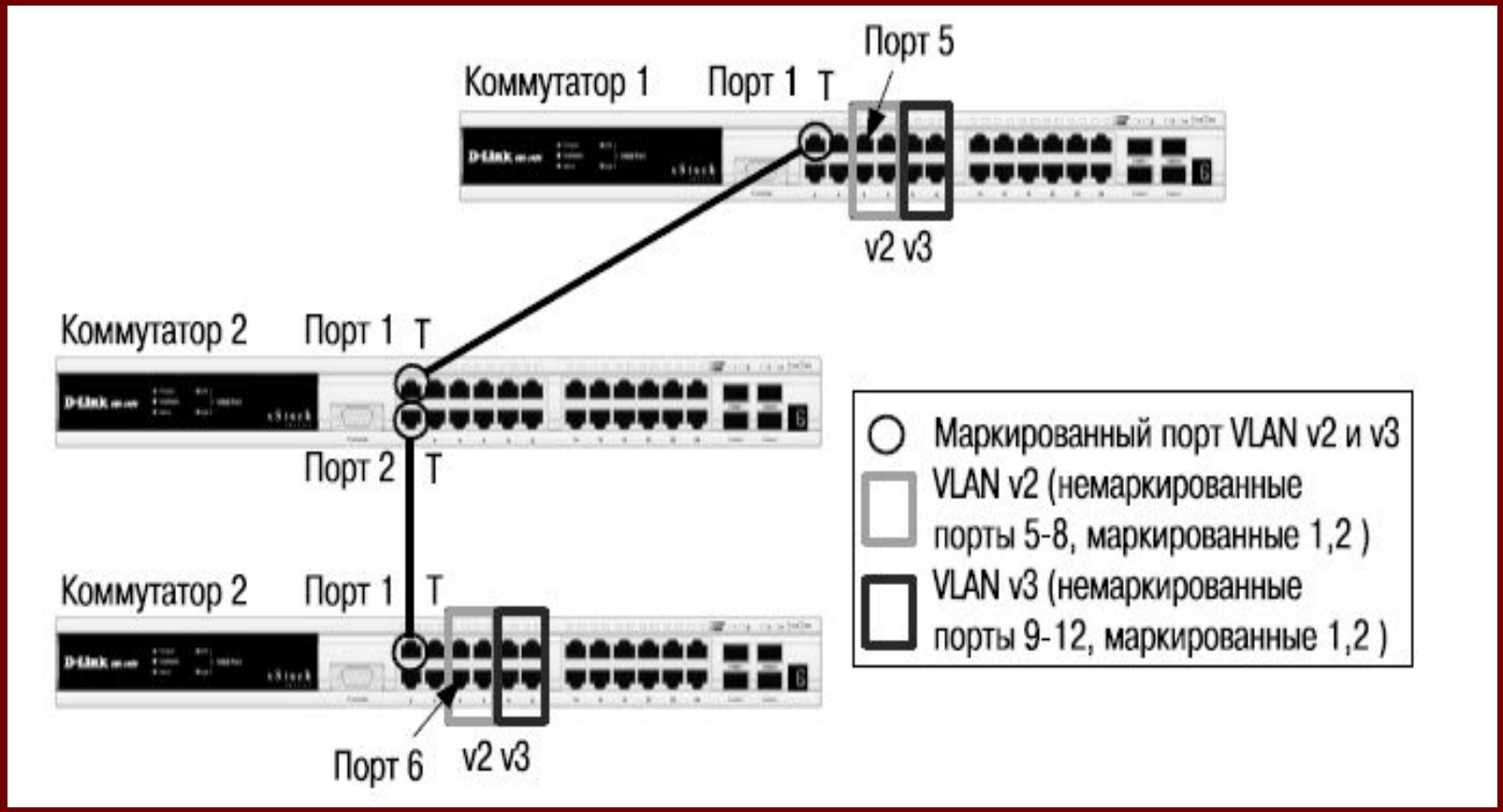


Port VLAN ID

- Каждый физический порт коммутатора имеет параметр, называемый *идентификатор порта VLAN (PVID)*. Этот параметр используется для того, чтобы определить, в какую VLAN коммутатор направит входящий немаркированный кадр с подключенного к порту сегмента, когда кадр нужно передать на другой порт (внутри коммутатора в заголовки всех *немаркированных кадров* добавляется идентификатор VID, равный *PVID* порта, на который они были приняты). Этот механизм позволяет одновременно существовать в одной сети устройствам с поддержкой и без поддержки стандарта IEEE 802.1Q.
- Коммутаторы, поддерживающие протокол IEEE 802.1Q, должны хранить таблицу, связывающую идентификаторы портов PVID с идентификаторами VID сети. При этом каждый порт такого коммутатора может иметь только один PVID и столько идентификаторов VID, сколько поддерживает данная модель коммутатора.
- Если на коммутаторе не настроены VLAN, то все порты по умолчанию входят в одну VLAN с PVID = 1.

Пример настройки VLAN IEEE 802.1Q

(рассмотрим пересылку кадра с порта 5 коммутатора 1 на порт 6 коммутатора 3)



- Порт 5 коммутатора 1 является немаркированным портом VLAN v2 (PVID=2). Поэтому, когда любой немаркированный кадр поступает на порт 5, коммутатор снабжает его тегом 802.1Q со значением VID, равным 2.
- Далее коммутатор 1 проверяет в своей таблице коммутации, через какой порт необходимо передать кадр и принадлежит ли этот порт VLAN v2. Кадр может быть передан через порт 1, т.к. он является маркированным членом VLAN v2. После передачи кадра через порт 1 тег 802.1Q в нем будет сохранен.
- После этого маркированный кадр поступит на порт 1 коммутатора 2. Прежде чем передать кадр дальше, порт 1 проверит, является ли он сам членом VLAN v2. Поскольку порт 1 коммутатора 2 является маркированным членом VLAN v2, он примет кадр и передаст его на порт 2, согласно таблице коммутации. После передачи кадра через порт 2 коммутатора 2 тег 802.1Q в нем будет сохранен, т.к. порт 2 является маркированным портом VLAN v2.
- Порт 1 коммутатора 3 примет поступивший кадр. После проверки на принадлежность к VLAN порт 1 передаст кадр на порт 6, найденный обычным образом в таблице коммутации коммутатора 3. Порт 6 является немаркированным портом VLAN v2, поэтому при выходе кадра через этот порт тег 802.1Q из него будет удален.

Настройка коммутатора 1

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

- **config vlan default delete 1-12**
- **create vlan v2 tag 2**
- **create vlan v3 tag3**

В созданные VLAN добавить порты, для которых необходимо указать, какие из них являются маркированными и немаркиро ванными.

- **config vlan v2 add untagged 5-8**
- **config vlan v2 add tagged 1-2**
- **config vlan v3 add untagged 9-12**
- **config vlan v3 add tagged 1-2**

Настройка коммутатора 2

- **config vlan default delete 1-2**
- **create vlan v2 tag 2**
- **create vlan v3 tag 3**
- **config vlan v2 add tagged 1-2**
- **config vlan v3 add tagged 1-2**

Настройка коммутатора 3

- **config vlan default delete 1-12**
- **create vlan v2 tag 2**
- **create vlan v3 tag 3**
- **config vlan v2 add untagged 5-8**
- **config vlan v2 add tagged 1**
- **config vlan v3 add untagged 9-12**
- **config vlan v3 add tagged 1**

- **Внимание**: заводские установки по умолчанию назначают все порты коммутатора в default VLAN с VID = 1. Перед созданием новой VLAN необходимо удалить из default VLAN все порты, которые требуется сделать немаркированными членами новой VLAN

3.4. Статические и динамические VLAN

Для корректной работы виртуальной локальной сети требуется, чтобы в базе данных фильтрации *(Filtering Database)* содержалась информация о членстве в VLAN. Это необходимо для принятия правильного решения при передаче кадров между портами коммутатора.

Существуют два основных способа установки членство в VLAN:

- статические 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)
- динамические VLAN (членство 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.

3.5. Протокол GVRP

- Определяет способ, посредством которого коммутаторы обмениваются информацией о сети VLAN. Он позволяет динамически создавать и удалять VLAN стандарта IEEE 802.1Q на магистральных портах, автоматически регистрировать и исключать атрибуты 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.

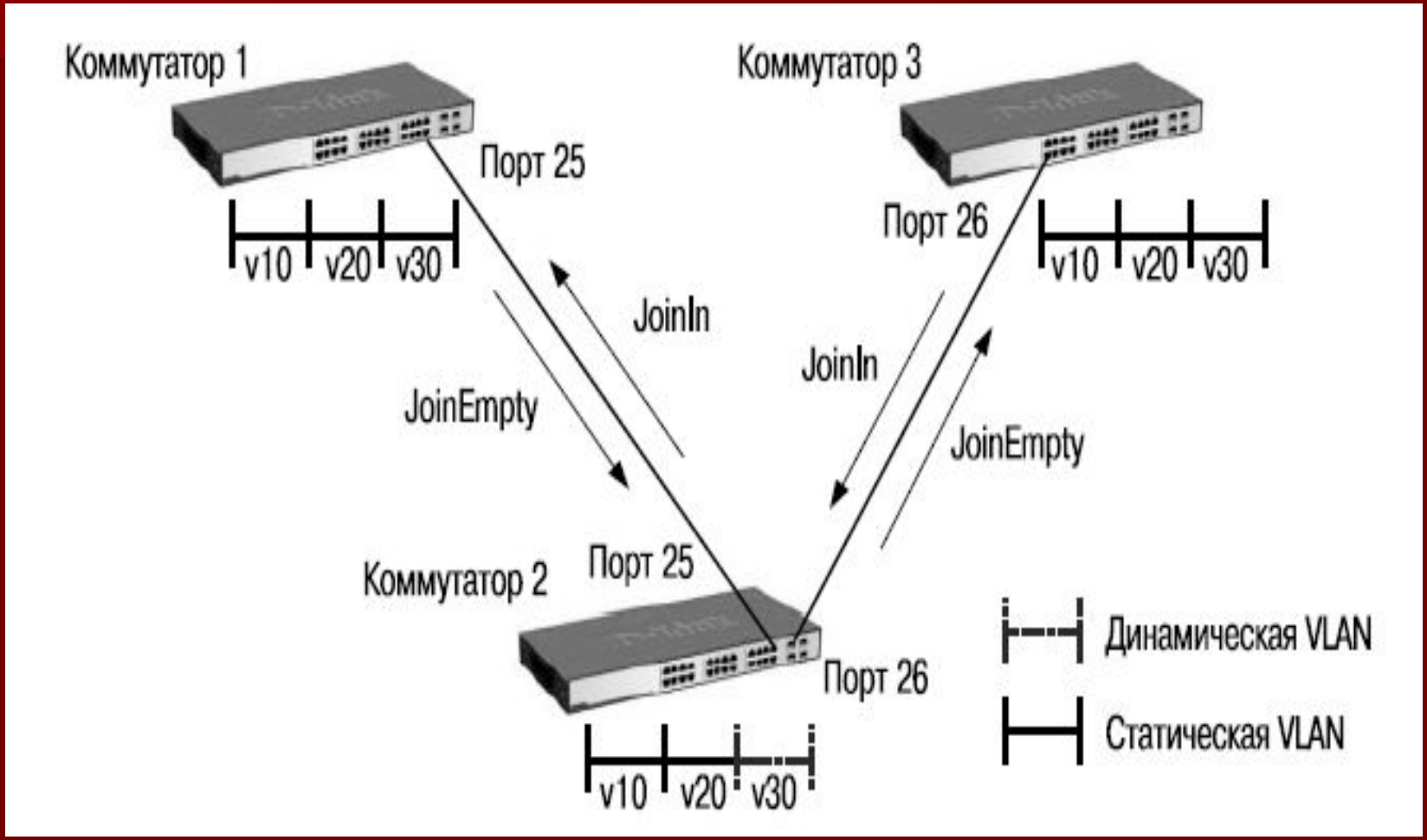
    LeaveEmpty: VLAN на локальном подписчике не настроена;

    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.

Таймеры GVRP

- *Join Timer* — время в миллисекундах (100-100000), через которое отправляются сообщения JoinIn или JoinEmpty. Определяет промежуток времени между моментом получения коммутатором информации о вступлении в VLAN и фактическим моментом вступления в VLAN. По умолчанию установлено значение 200 миллисекунд.
- *Leave Timer* — когда коммутатор получает сообщение об исключении порта из VLAN (Leave message) от другого подписчика GVRP, он ожидает заданный период времени (от 100 до 100000 миллисекунд), определяемый таймером Leave Timer, чтобы убедиться, что информация о данной VLAN больше не существует в сети. Например, когда коммутатор получает сообщение Leave, он не удаляет мгновенно информацию о соответствующей VLAN, а запускает Leave Timer и ждет, когда его время истечет. Если за это время не будет получено сообщение JoinIn с информацией об удаляемой VLAN, то она будет коммутатором удалена. Обычно значение таймера Leave Timer устанавливают в два раза больше значения таймера Join Timer. По умолчанию значение таймера равно 600 мил лисекунд.
- *LeaveAll Timer* — интервал времени в миллисекундах (100-100000), через который отправляется сообщение LeaveAll. Когда коммутатор — подписчик GVRP получает это сообщение, он перезапускает все таймеры, включая LeaveAll Timer. Обычно значение таймера LeaveAll устанавливают в два раза больше значения таймера Leave Timer. По умолчанию значение таймера равно 10000 милли секунд.

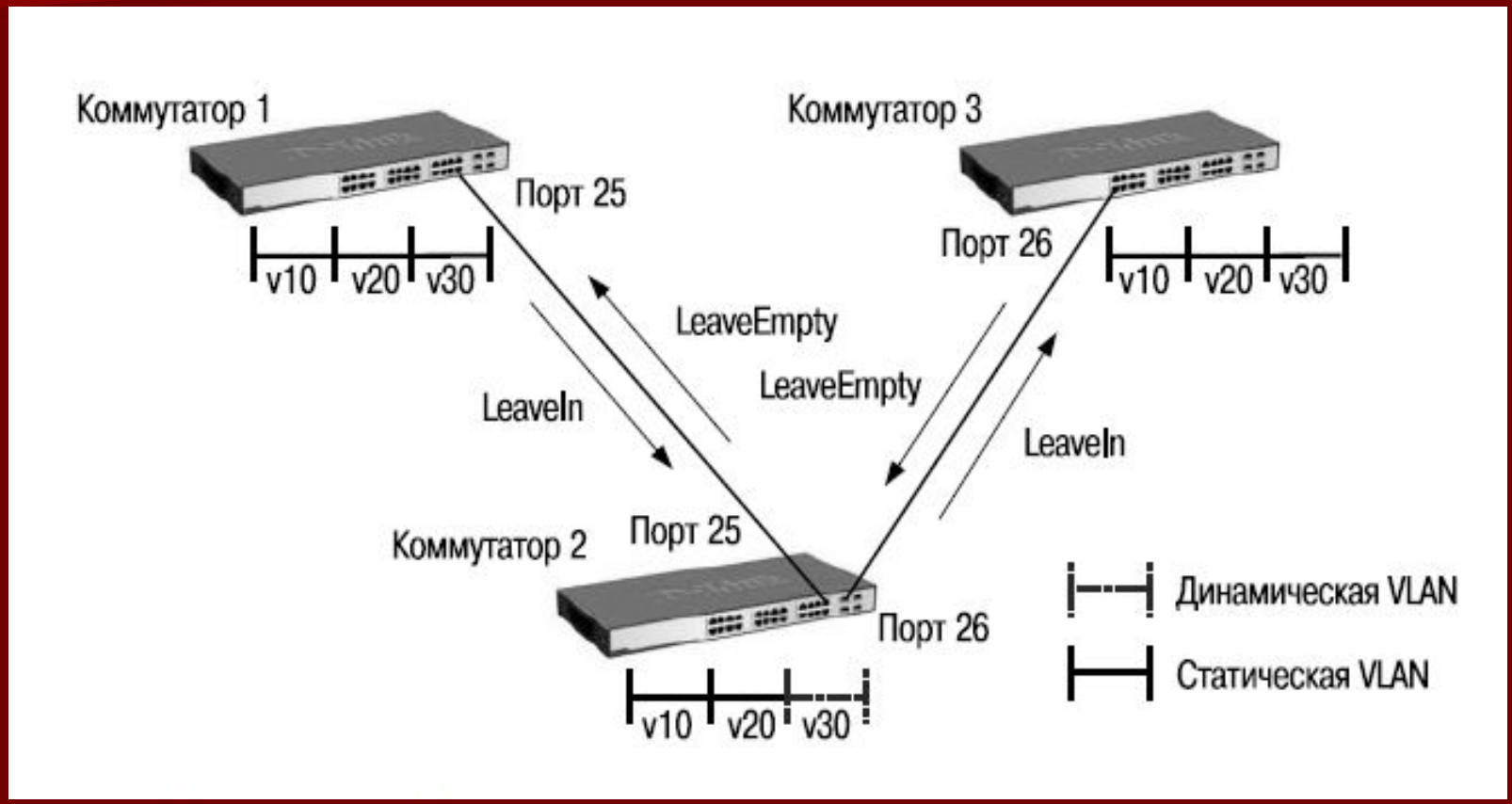
Процесс распространения информации о регистрации VLAN по сети



Процесс распространения информации о регистрации VLAN по сети

- На коммутаторе 1 созданы статические виртуальные сети VLAN v10, v20 и v30. Порт 25 является маркированным членом всех VLAN. Коммутатор 1 отправляет оповещение о VLAN v30 через порт 25 коммутатору 2 (сообщение JoinEmpty). Коммутатор 2 получает это оповещение, динамически создает VLAN v30 и включает в нее порт 25. Порт 26 коммутатора 2 отправляет оповещение о VLAN v30 коммутатору 3 (сообщение JoinEmpty), но сам не становится членом этой VLAN.
- Коммутатор 3 получает оповещение, динамически создает VLAN v30 и включает в нее порт 26. Далее коммутатор 3 изменяет состояние VLAN v30 с динамического на статическое и отправляет через порт 26 сообщение JoinIn о регистрации виртуальной сети. Коммутатор 2 получает это оповещение и регистрирует порт 26 в VLAN v30, которая уже была создана ранее. Сообщение о регистрации VLAN v30 отправляется через порт 25 коммутатору 1. Получив это сообщение, коммутатор 1 перестает рассылать оповещения о VLAN v30.
- ***Внимание***: порт с поддержкой протокола GVRP подключается к сети VLAN только в том случае, если он непосредственно получает оповещение о ней. Если порт с поддержкой протокола GVPR передает оповещение, полученное от другого порта коммутатора, он не подключается к этой сети VLAN.

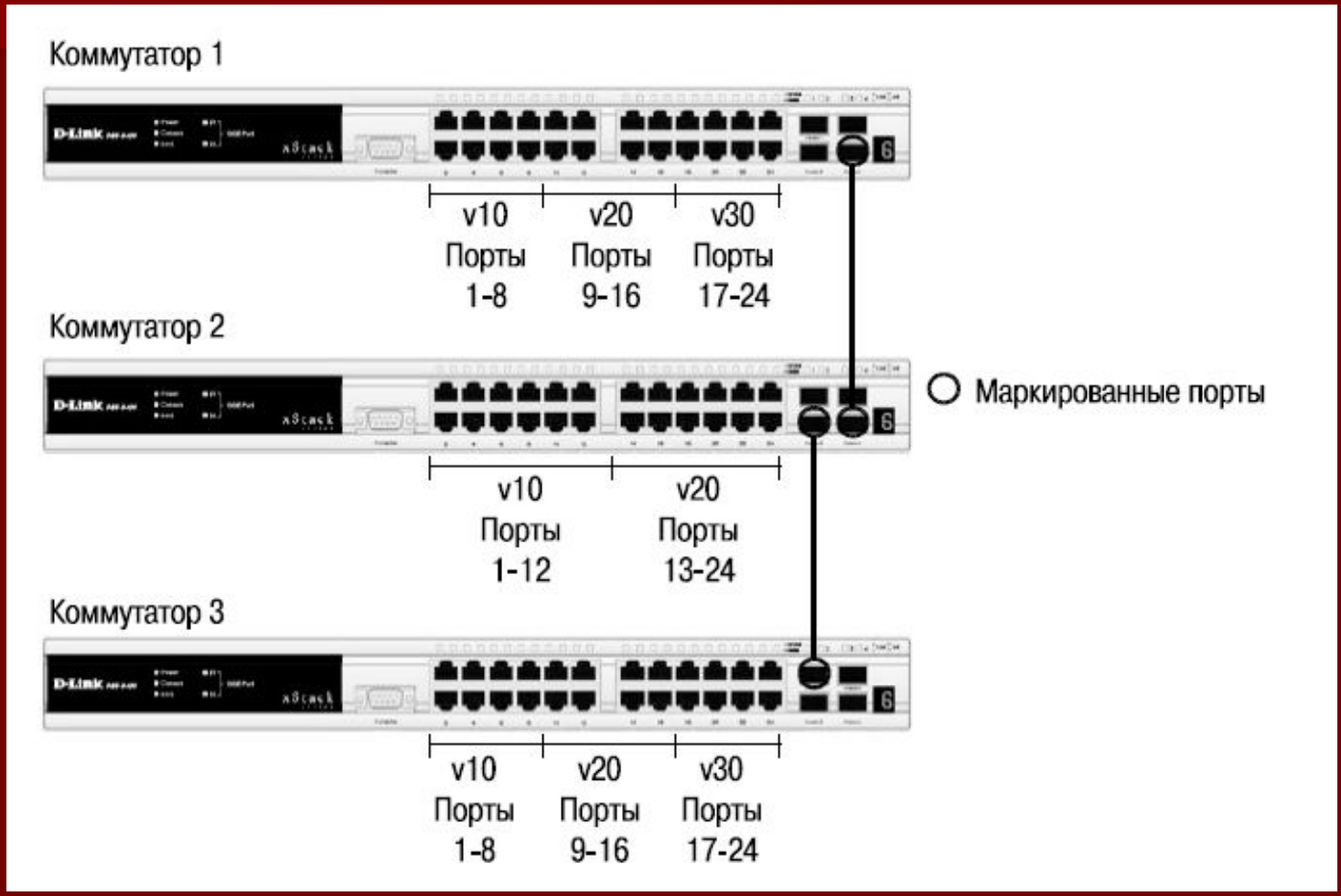
Процесс распространения информации об удалении VLAN по сети



Процесс распространения информации об удалении VLAN по сети

- На коммутаторе 1 удалена статическая VLAN v30, и он отправляет сообщение LeaveIn через порт 25 коммутатору 2. Когда коммутатор 2 получит оповещение об удалении VLAN v30, он исключит порт 25 из этой VLAN и отправит сообщение LeaveIn коммутатору 3 через порт 26.
- Коммутатор 3 получит оповещение об удалении VLAN v30, но удалит ее не сразу, а по истечении периода, установленного таймером Leave Timer. После удаления VLAN v30 коммутатор 3 отправит через порт 26 сообщение LeaveEmpty. После получения этого сообщения коммутатор 2 исключит порт 26 из VLAN v30 и удалит ее по истечении периода, установленного таймером Leave Timer. Через порт 25 будет передано сообщение LeaveEmpty коммутатору 1. Коммутатор 1 исключит свой порт 25 из динамической VLAN v30.

Пример настройки протокола GVRP (требуется настроить возможность динамического распространения по сети информации о VLAN v30)



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 по сети.

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

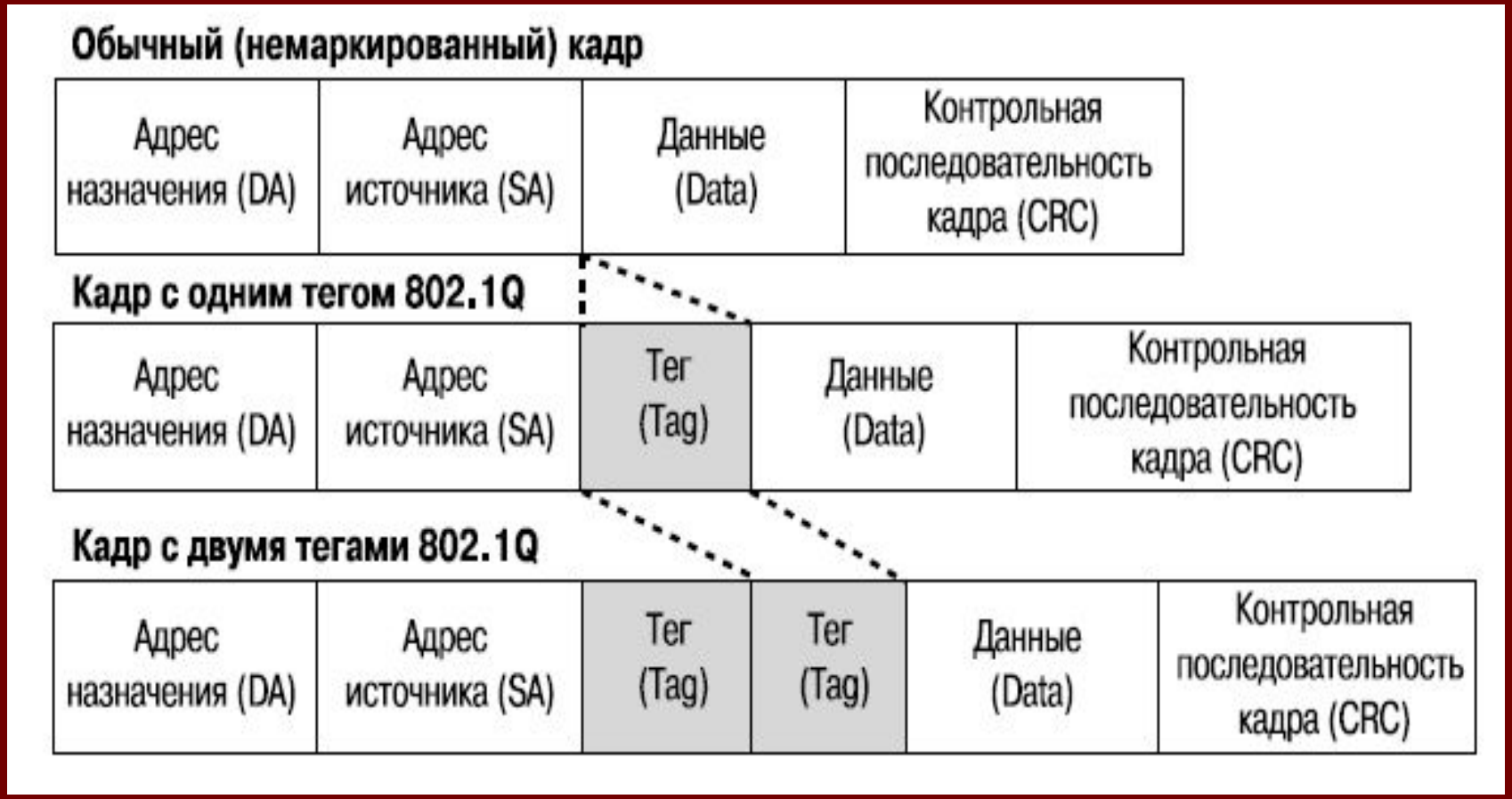
Настройка коммутатора 2

- **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**

3.6. Q-in-Q VLAN

- Функция *Q-in-Q,* также известная как *Double VLAN,* соответствует стандарту IEEE 802.1ad, который является расширением стандарта IEEE 802.1Q. Она позволяет добавлять в маркированные кадры Ethernet второй тег IEEE 802.1Q.
- Благодаря функции Q-in-Q провайдеры могут использовать их собственные уникальные идентификаторы VLAN (называемые Service Provider VLAN ID или *SP-VLANID)* при оказании услуг пользователям, в сетях которых настроено несколько VLAN. Это позволяет сохранить используемые пользователями идентификаторы VLAN (Customer VLAN ID или *CVLAN ID),* избежать их совпадения и изолировать трафик разных клиентов во внутренней сети провайдера.

Формат кадра Ethernet с двумя тегами 802.1Q



Формат кадра Q-in-Q

- На слайде изображены форматы:
  - обычного кадра Ethernet,
  - кадра Ethernet с тегом 802.1Q,
  - кадра Ethernet с двумя тегами 802.1Q.
- Инкапсуляция кадра Ethernet вторым тегом происходит следующим образом: тег, содержащий идентификатор VLAN сети провайдера *(внешний тег),* вставляется перед *внутренним тегом,* содержащим клиентский идентификатор VLAN. Передача кадров в сети провайдера осуществляется только на основе внешнего тега SP-VLAN ID, внутренний тег пользовательской сети CVLAN ID при этом скрыт.
- Функция Q-in-Q позволяет расширить доступное пространство идентификаторов и использовать до 4094 x 4094 = 16 760 836 уникальных виртуальных локальных сетей.

Реализации Q-in-Q

- Две реализации функции Q-in-Q: *Port-based Q-in-Q* и *Selective Q-in-Q.*
- Функция *Port-based Q-in-Q* по умолчанию присваивает любому кадру, поступившему на порт доступа граничного коммутатора провайдера, идентификатор *SP-VLAN,* равный идентификатору PVID порта. Порт маркирует кадр независимо от того, является он маркированным или немаркированным. При поступлении маркированного кадра в него добавляется второй тег с идентификатором, равным *SP-VLAN.* Если на порт пришел немаркированный кадр, в него добавляется только тег с *SP-VLAN* порта.
- Функция *Selective Q-in-Q* является более гибкой по сравнению с *Port-based Q-in-Q.* Она позволяет:
  - маркировать кадры внешними тегами с различными идентификаторами SP-VLAN в зависимости от значений внутренних идентификаторов CVLAN;
  - задавать приоритеты обработки кадров внешних SP-VLAN на основе значений приоритетов внутренних пользовательских CVLAN;
  - добавлять к немаркированным пользовательским кадрам помимо внешнего тега SP-VLAN внутренний тег CVLAN.

Значения TPID в кадрах Q-in-Q

- В теге VLAN имеется поле идентификатора протокола тега (TPID, Tag Protocol IDentifier), который определяет тип протокола тега. По умолчанию значение этого поля для стандарта IEEE 802.1Q равно 0x8100.
- На устройствах разных производителей TPID внешнего тега VLAN кадров Q-in-Q может иметь разные значения по умолчанию. Для того чтобы кадры Q-in-Q могли передаваться по общедоступным сетям через устройства разных производителей, рекомендуется использовать значение TPID внешнего тега равное 0x8 8A8, согласно стандарту IEEE 802.1ad.

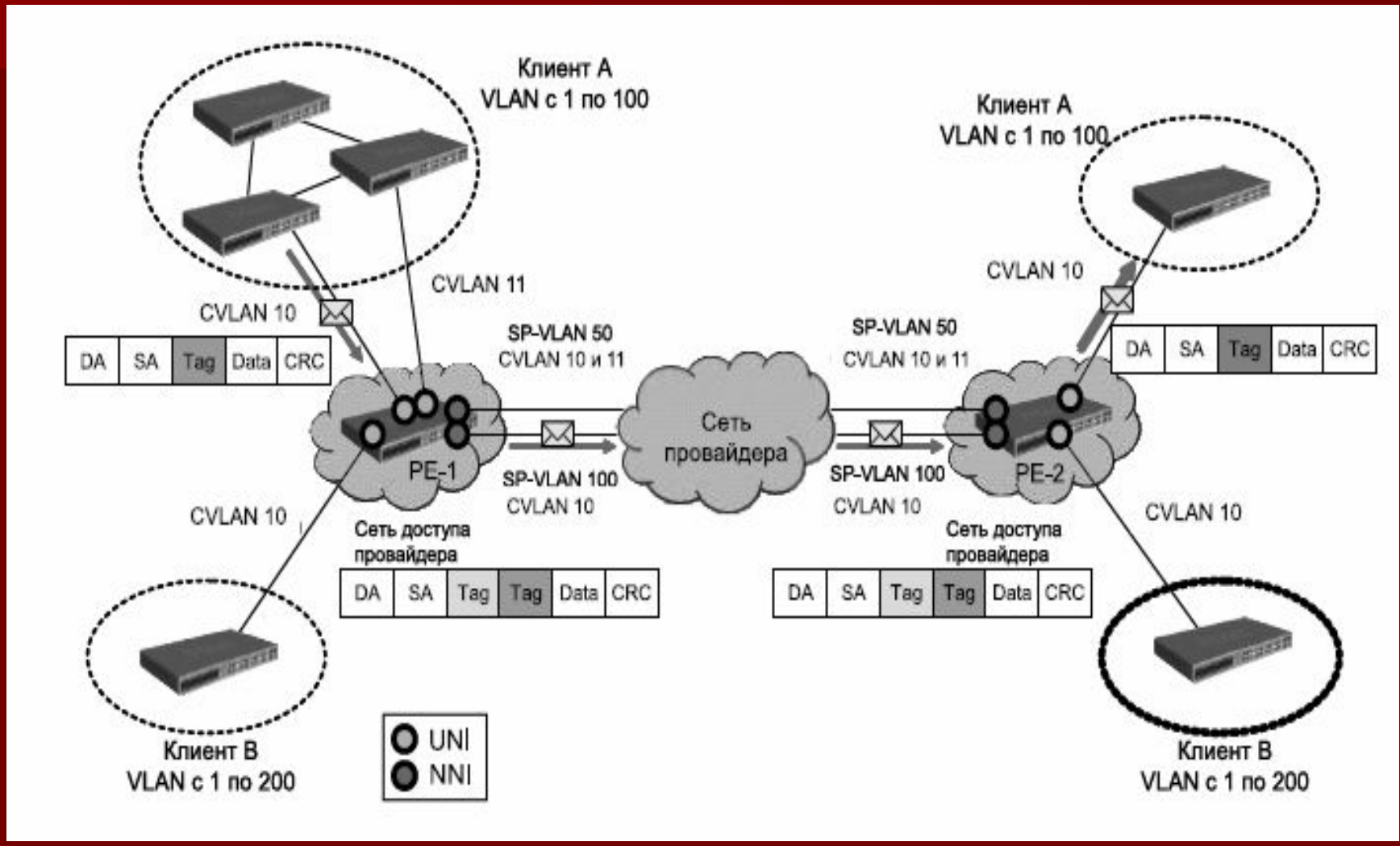
Роли портов в Port-based Q-in-Q и Selective Q-in-Q

- Все порты граничного коммутатора, на котором используются функции Port-based Q-in-Q или Selective Q-in-Q, должны быть настроены как порты доступа (UNI) или Uplink-порты (NNI):
  - *UNI (User-to-Network Interface)* — эта роль назначается портам, через которые будет осуществляться взаимодействие граничного коммутатора провайдера с клиентскими сетями;
  - *NNI (Network-to-Network Interface)* — эта роль назначается портам, которые подключаются к внутренней сети провайдера или другим граничным коммутаторам.

Политики назначения внешнего тега и приоритета в Q-in-Q

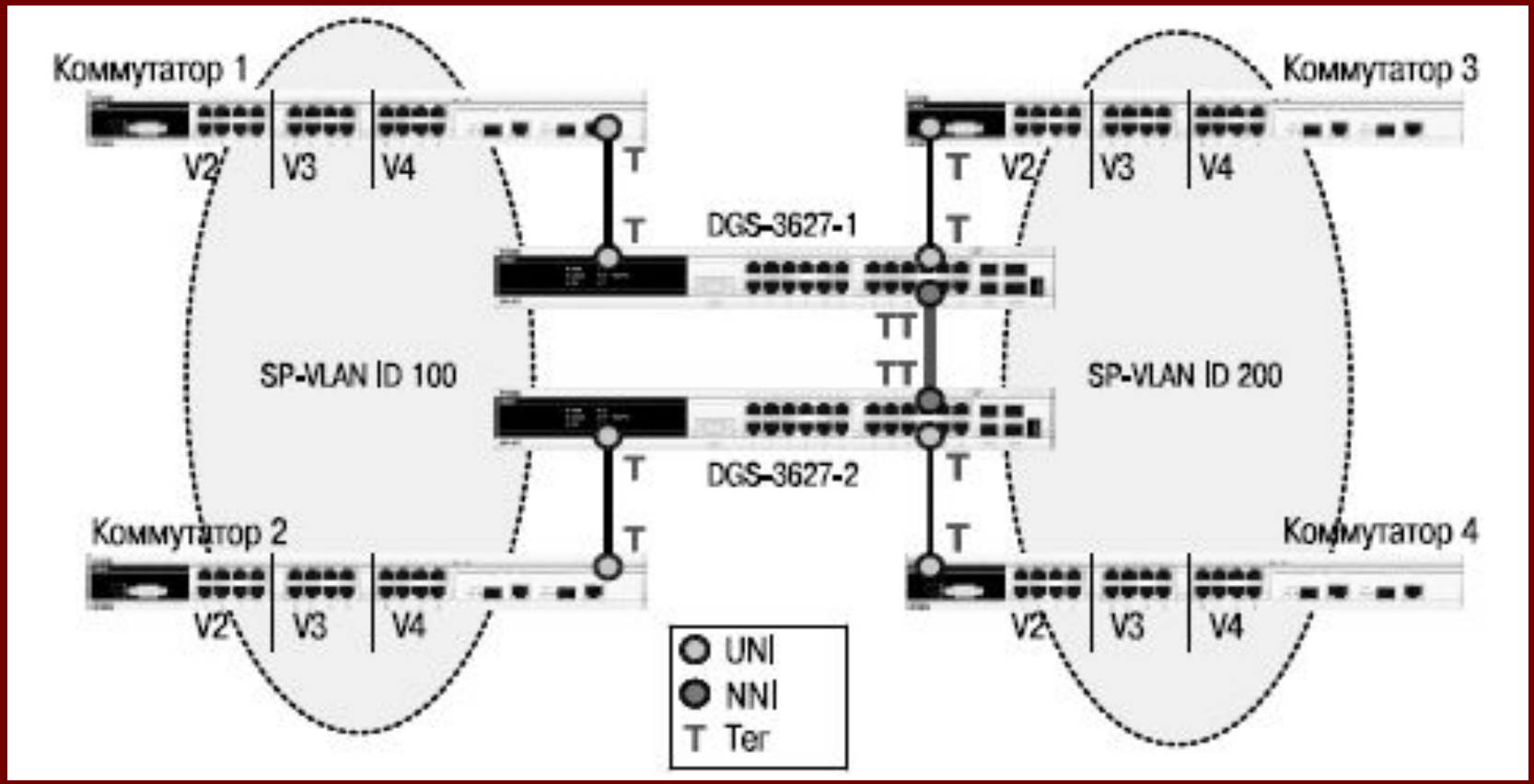
- Функция Selective Q-in-Q позволяет добавлять в кадры различные внешние теги VLAN, основываясь на значениях внутренних тегов. Для этого на портах UNI граничного коммутатора необходимо задать правила соответствия идентификаторов CVLAN идентификаторам SP-VLAN *(vlan translation*).
- Помимо этого, на коммутаторах D-Link с поддержкой функции Q-in-Q, можно активизировать режим Missdrop. При настройке Selective Q-in-Q, включение этого режима позволит отбрасывать кадры, не подходящие ни под одно из правил соответствия идентификаторов. При настройке Port-based Q-in-Q, режим Missdrop надо отключать, чтобы порт коммутатора мог принимать кадры не подходящие ни под одно из правил vlan translation. В этом случае входящим кадрам будет присваиваться внешний тег равный PVID соответствующего порта UNI.
- Значение приоритета внешнего тега по умолчанию равно значению приоритета внутреннего тега, если кадр является маркированным. Если приоритет в полученном кадре отсутствует, то в качестве приоритета вешнего тега будет использоваться приоритет соответствующего входного порта UNI.

Базовая архитектура сети с функцией Port-based Q-in-Q



- Граничные коммутаторы сети провайдера услуг PE-1 и PE-2 позволяют обрабатывать трафик виртуальных локальных сетей двух подключенных к ним клиентских сетей.
- Каждому клиенту провайдером присвоен уникальный идентификатор VLAN: SP-VLAN 50 для клиента A и SP-VLAN 100 для клиента B.
- При передаче кадра из клиентской сети в сеть провайдера, в его заголовок будет добавляться второй тег 802.1Q: для сети A — SP-VLAN 50, для сети B — SP-VLAN 100.
- При передаче кадра из сети провайдера в клиентскую сеть второй тег будет удаляться граничным коммутатором.

Пример настройки функции Port-based Q-in-Q (D-Link, схема подключения двух клиентских VLAN к сети провайдера услуг, граничные коммутаторы - Gigabit Ethernet 3-го уровня. В сети клиента - коммутаторы Fast Ethernet 2-го уровня)



Настройка коммутатора DGS-3627

Внимание: функцию Q-in-Q VLAN необходимо настраивать только на устройствах сети провайдера услуг.

Активизировать функцию Q-in-Q VLAN на коммутаторе.

- **enable qinq**

Удалить соответствующие порты из Q-in-Q VLAN по умолчанию и создать новые VLAN.

- **config vlan default delete 1-24**
- **create vlan d100 tag 100**
- **create vlan d200 tag 200**

Назначить порты доступа в созданных Q-in-Q VLAN.

- **config vlan d100 add untagged 1-12**
- **config vlan d200 add untagged 13-24**

Назначить Uplink-порты в созданных Q-in-Q VLAN.

- **config vlan d100 add tagged 25-27**
- **config vlan d200 add tagged 25-27**

Настроить роли портов доступа в Q-in-Q и отключить режим Missdrop на них.

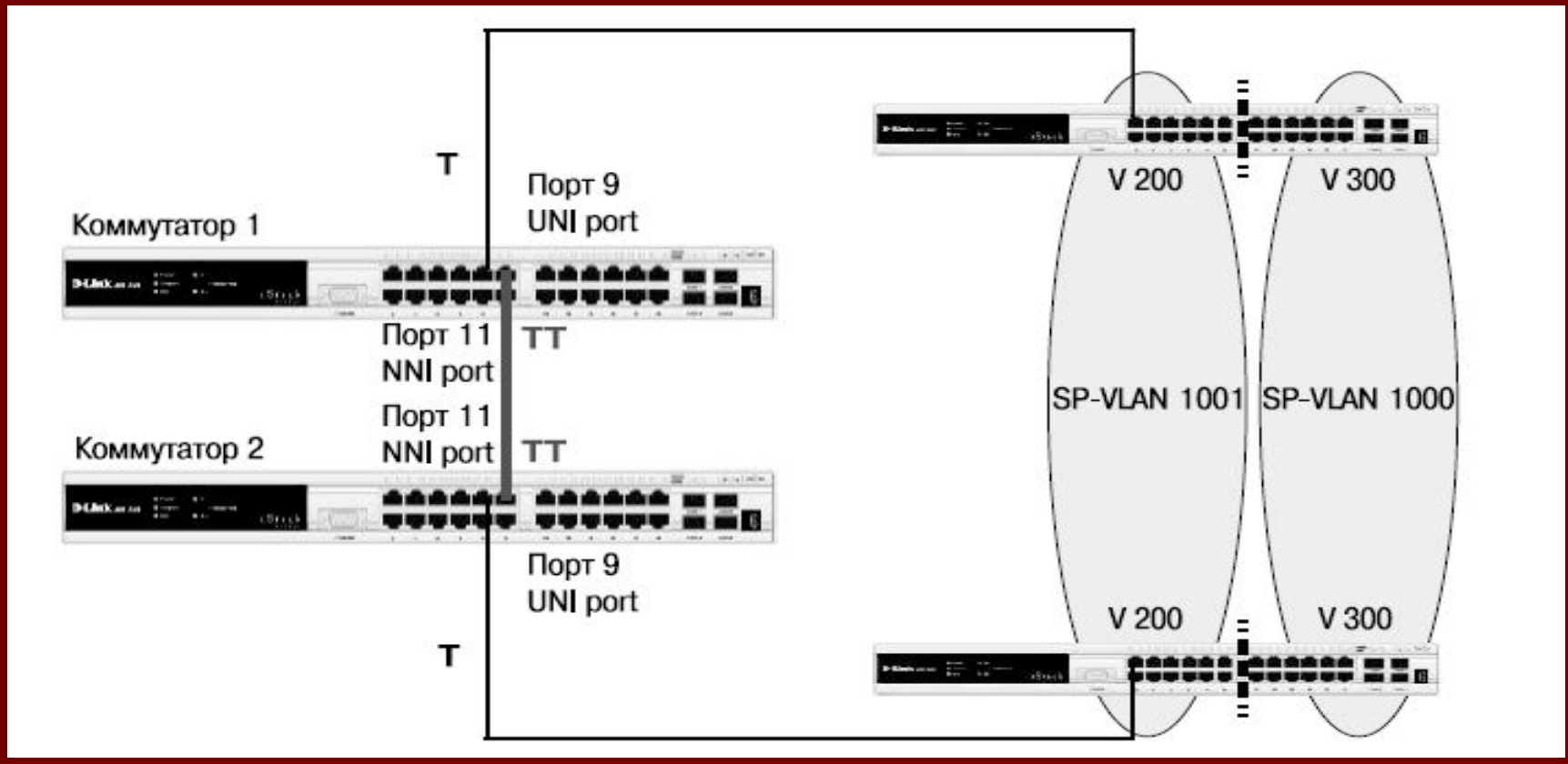
- **config qinq ports 1-24 role uni missdrop disable**

Настройка коммутаторов 1, 2, 3, 4

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

- **config vlan default delete 1-26**
- **create vlan v2 tag 2**
- **create vlan v3 tag 3**
- **create vlan v4 tag 4**
- В созданные VLAN добавить порты, для которых необходимо указать, какие из них являются маркированными и немаркированными.
- **config vlan v2 add untagged 1-8**
- **config vlan v2 add tagged 25-26**
- **config vlan v3 add untagged 9-16**
- **config vlan v3 add tagged 25-26**
- **config vlan v4 add untagged 17-24**
- **config vlan v4 add tagged 25-26**

Пример настройки функции Selective Q-in-Q (двум клиентам провайдером назначен уникальный идентификатор: SP-VLAN 1000 для клиента CVLAN 200 и SP-VLAN 1001 для клиента CVLAN 300. Граничные коммутаторы - Fast Ethernet 2-го уровня. Порты 9 обоих граничных коммутаторов служат для подключения к пользовательским сетям (UNI-порты), передача данных в сеть провайдера осуществляется через порты 11 (NNI-порты))



Настройка коммутаторов 1, 2

Создать требуемые VLAN и добавить порты, для которых необходимо указать, какие из них являются маркированными и немаркированными.

- **create vlan v1000 tag 1000**
- **create vlan v1001 tag 1001**
- **config vlan v1000 add tag 9,11**
- **config vlan v1001 add tag 9,11**

Активизировать функцию Q-in-Q VLAN, указать значения TPID внутреннего и внешнего тега, роли портов и задать правила соответствия идентификаторов CVLAN идентификаторам SP-VLAN.

- **enable qinq**
- **config qinq ports all 0x8100**
- **config qinq ports 9 role uni**
- **create vlan_translation ports 9 cvid 200 add svid 1000**
- **create vlan_translation ports 9 cvid 300 add svid 1001**

3.7. VLAN на основе портов и протоколов - стандарт IEEE 802.1v

Является расширением стандарта IEEE 802.1Q. При определении членства в VLAN стандарт классифицирует *немаркированные* кадры по типу протокола и порту. Формат тега 802.1v аналогичен формату тега 802.1Q

В стандарте IEEE 802.1v определены правила классификации входящих кадров:

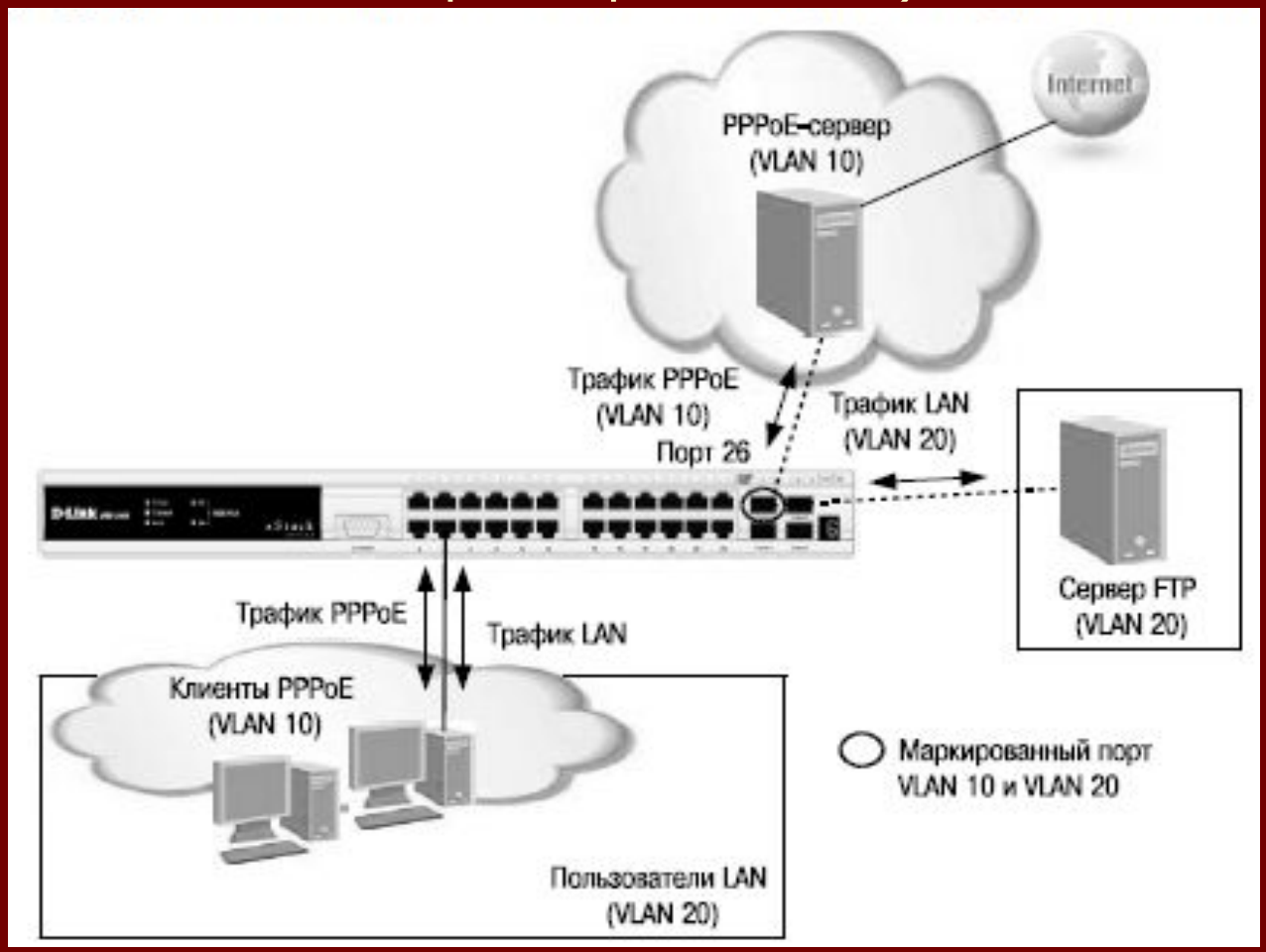
- При поступлении на порт *немаркированного* кадра, коммутатором осуществляется проверка заголовка канального уровня и типа протокола вышележащего уровня. Если тип протокола соответствует типу VLAN 802.1v на этом порте, то в заголовок кадра добавляется тег с идентификатором VID, равным идентификатору соответствующей VLAN 802.1v. Если совпадения не найдены, то в заголовок кадра добавляется тег с идентификатором VID, равным идентификатору входного порта *PVID;*
- При поступлении на порт *маркированного* кадра значение тега VLAN в нем не изменяется.

Внутри коммутатора все кадры являются маркированными. Передача кадров осуществляется на основе таблицы VLAN путем сравнения значений идентификаторов VID. Если порт назначения является членом той же VLAN, что и входной порт, то он передает кадр в подключенный к нему сегмент сети. В противном случае кадр отбрасывается.

Для выходных портов действуют такие же правила, как для стандарта IEEE 802.1Q.

Механизм классификации 802.1v требует, чтобы на коммутаторе были настроены группы протоколов. Каждый протокол в группе определяется типом кадра (Ethernet II, IEEE 802.3 SNAP или IEEE 802.3 LLC) и значением поля идентификации протокола в нем. Порт может быть ассоциирован с несколькими группами протоколов, что позволяет классифицировать поступающие немаркированные кадры по принадлежности к разным VLAN в зависимости от их содержимого. Одна и та же группа протоколов может быть ассоциирована с разными портами коммутатора, при этом на каждом входном порте ей должны быть присвоены уникальные идентификаторы VLAN.

Пример настройки IEEE 802.1v VLAN (пользователи находятся в выделенной VLAN (VLAN 20). Их подключение в Интернет осуществляется через PPPoE- сервер (VLAN 10). Для того, чтобы трафик локальной сети был отделен от трафика PPPoE, на коммутаторе для протокола PPPoE создана VLAN 802.1v с идентификатором VID=10)



Настройка коммутатора

Создание новых VLAN 802.1Q.

- **config vlan default delete 1-28**
- **create vlan pppoe tag 10**
- **config vlan pppoe add untagged 1-24**
- **config vlan pppoe add tagged 26**
- **create vlan base tag 20**
- **config vlan base add tagged 26**
- **config vlan base add untagged 1-24**

Настройка PVID портов, к которым подключены пользователи.

- **config port_vlan 1-24 pvid 20**

Создание VLAN 802.1v для протокола PPPoE (первая группа протоколов настроена для кадров PPPoE, передаваемых на стадии исследования, вторая — для кадров PPPoE установленной сессии).

- **create dot1v_protocol_group group_id 1 group_name pppoe_disc**
- **config dot1v_protocol_group group_id 1 add protocol ethernet_2 8863**
- **create dot1v_protocol_group group_id 2 group_name pppoe_session**
- **config dot1v_protocol_group group_id 2 add protocol ethernet_2 8864**
- **config port dot1v ports 1-24 add protocol_group group_id 1 vlan pppoe**
- **config port dot1v ports 1-24 add protocol_group group_id 2 vlan pppoe**

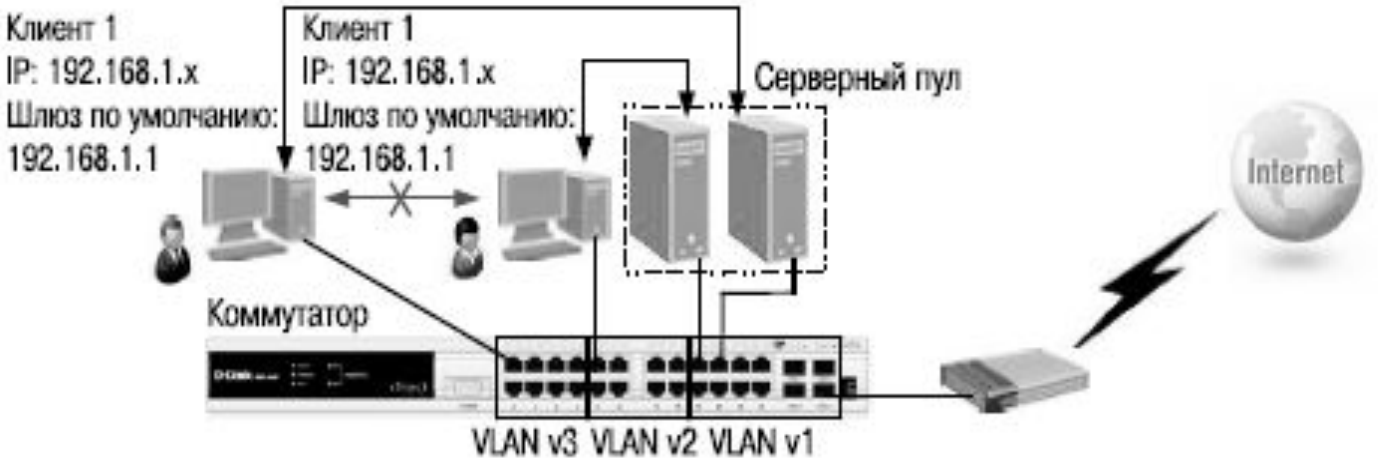
3.8. Асимметричные VLAN

- 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.

3.8. Асимметричные VLAN

- 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.

Пример настройки асимметричных 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)



Коммутатор

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

Настройка коммутатора

- **enable asymmetric_vlan**
- **create vlan v2 tag 2**
- **create vlan v3 tag 3**
- **config vlan v2 add untagged 9-24**
- **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**

3.9. Функция Traffic Segmentation

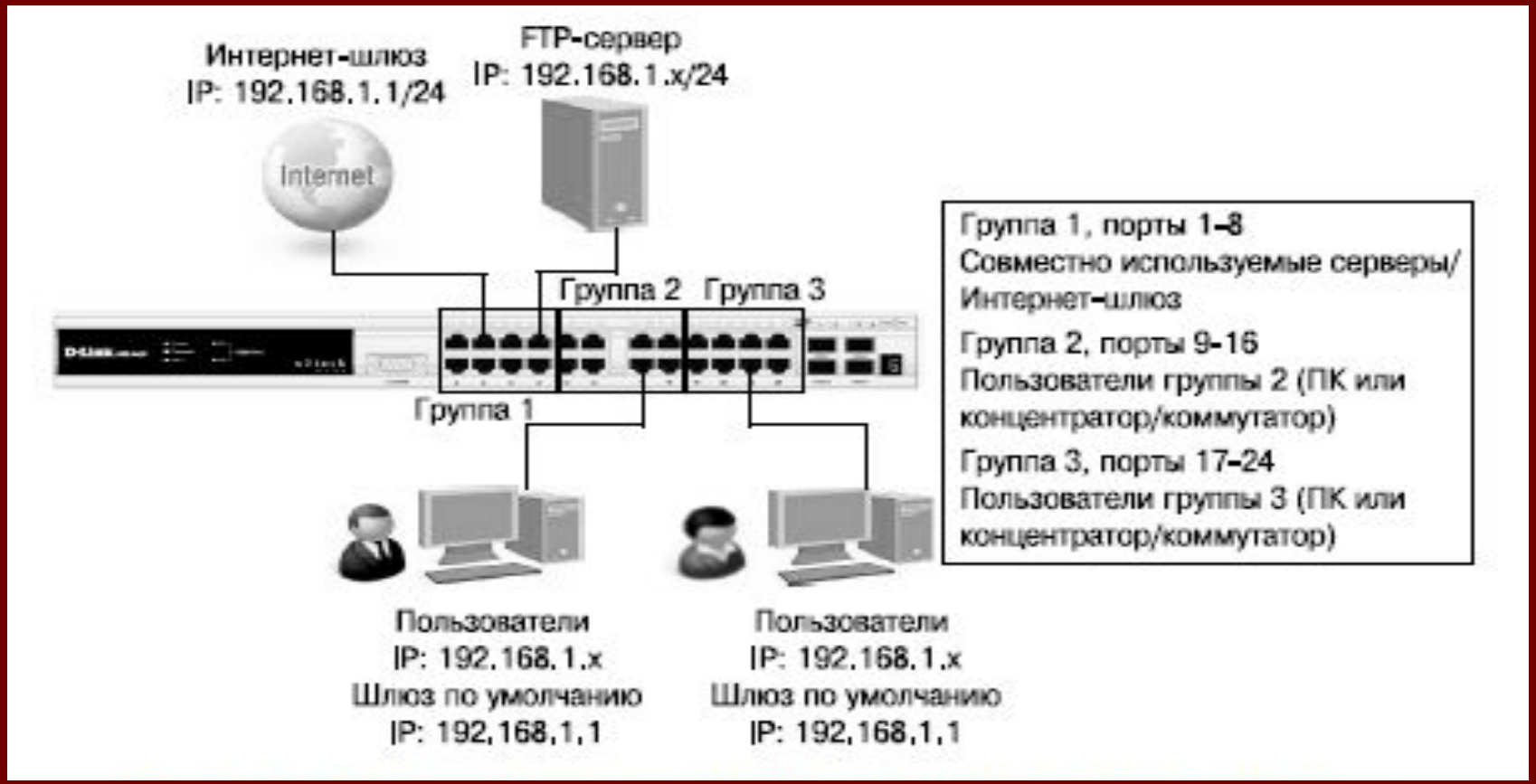
Служит для разграничения доменов на канальном уровне. Порты или группы портов коммутатора изолированы друг от друга, но в то же время имеют доступ к разделяемым портам, используемым для подключения серверов или магистрали сети. Этот метод изоляции трафика аналогичен функции Asymmetric VLAN, но его применение ограничено пределами одного коммутатора или нескольких коммутаторов в стеке.

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 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 и настройки функции Traffic Segmentation (решение задачи совместного использования ресурсов сети разными группами пользователей. Пользователи групп 2 и 3 имеют доступ к совместно используемому FTP-серверу и Интернет-шлюзу, но обмен данными между группами 2 и 3 запрещен)

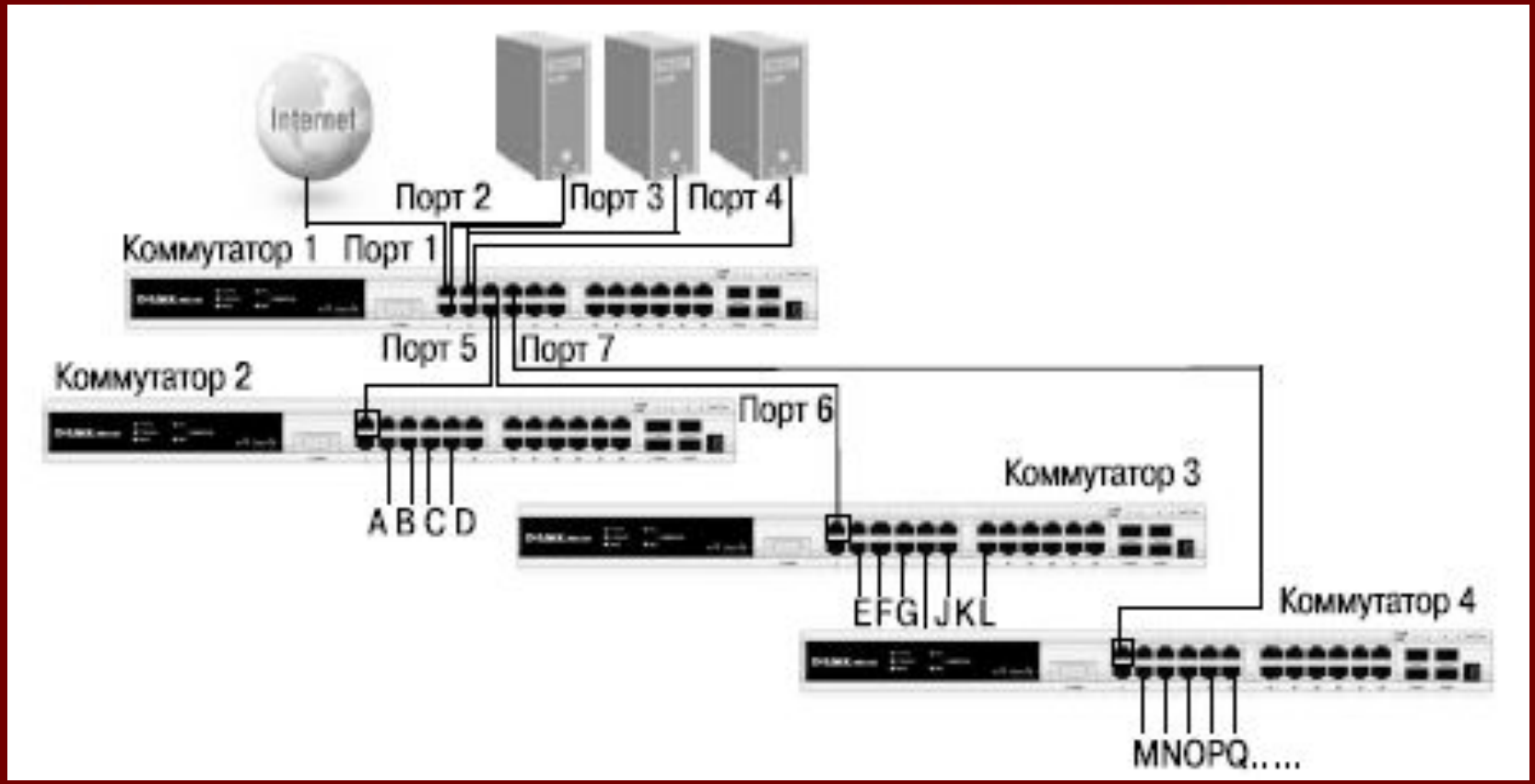


Настройка коммутатора

- **config traffic_segmentation 1-8 forward_list 1-24**
- **config traffic_segmentation 9-16 forward_list 1-16**
- **config traffic_segmentation 17-24 forward_list 1-8,17-24**

Используя возможности построения иерархического дерева функции Traffic Segmentation, можно решать типовые задачи изоляции портов в сетях с многоуровневой структурой.

Пример использования и настройки функции Traffic Segmentation (все компьютеры от A до Q, находящиеся в одной IP-подсети, не могут принимать/отправлять пакеты данных друг другу, но при этом имеют доступ к серверам и Интернету. Все коммутаторы сети поддерживают иерархию Traffic Segmentation)



Настройка коммутатора 1

- **config traffic_segmentation 1-4 forward_list 1-26**
- **config traffic_segmentation 5 forward_list 1-5**
- **config traffic_segmentation 6 forward_list 1-4, 6**
- **config traffic_segmentation 7 forward_list 1-4, 7**

Настройка коммутаторов 2, 3, 4

- **config traffic_segmentation 1 forward_list 1-26**
- **config traffic_segmentation 2-26 forward_list 1**