D-Link
Building Networks for People

# Лекция 3
# Виртуальные локальные сети (VLAN)

# Лекция 3. Виртуальные локальные сети (VLAN)

- Типы VLAN
- VLAN на основе портов
- VLAN на основе стандарта IEEE 802.1Q
- VLAN на основе портов и протоколов – стандарт IEEE 802.1v
- Private VLAN
- Статические и динамические VLAN
- Протокол GVRP
- Q-in-Q VLAN
- Функция Traffic Segmentation

# Виртуальные локальные сети (VLAN)

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

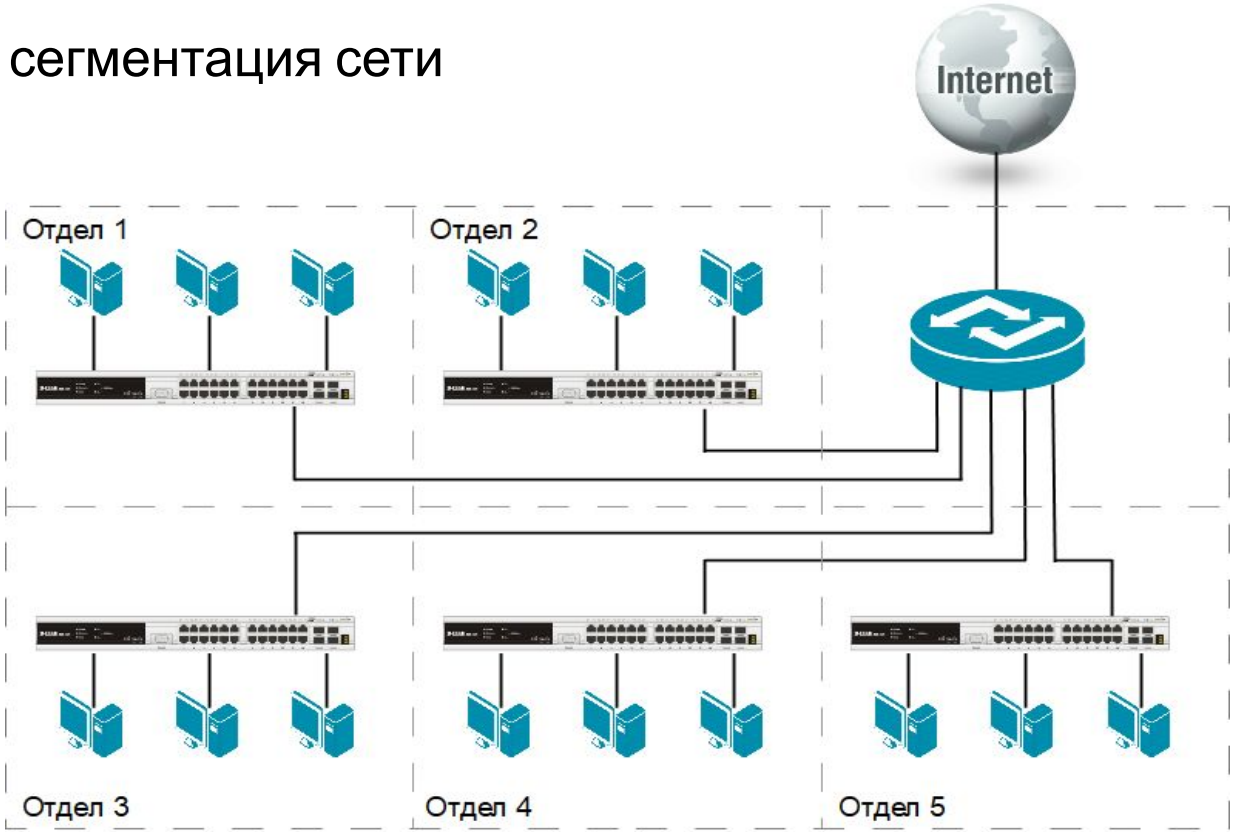
# Виртуальные локальные сети (VLAN)

VLAN обладают следующими преимуществами:

- гибкость внедрения – VLAN являются эффективным способом группировки сетевых пользователей в виртуальные рабочие группы независимо от их физического размещения в сети;
- ограничивают распространение широковещательного трафика, что увеличивает полосу пропускания, доступную для пользователя;
- позволяют повысить безопасность сети, определив с помощью фильтров, настроенных на коммутаторе или маршрутизаторе, политику взаимодействия пользователей из разных виртуальных сетей.

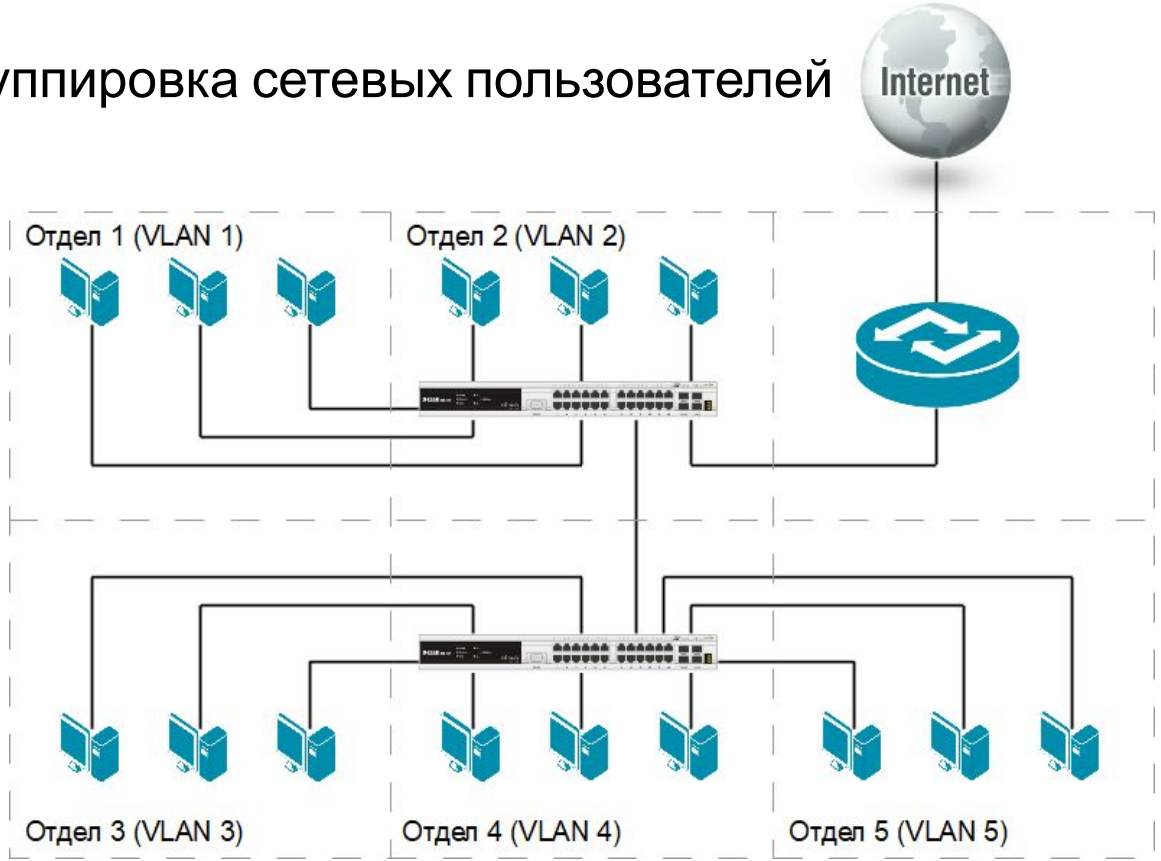
# Виртуальные локальные сети (VLAN)

## Физическая сегментация сети



# Виртуальные локальные сети (VLAN)

Логическая группировка сетевых пользователей в VLAN



# Виртуальные локальные сети (VLAN)

## Типы VLAN

В коммутаторах могут быть реализованы следующие типы VLAN:

- на основе портов (Port-based VLAN);
- на основе стандарта IEEE 802.1Q (IEEE 802.1Q VLAN);
- на основе стандарта IEEE 802.1ad (Q-in-Q VLAN);
- на основе портов и протоколов (IEEE 802.1v VLAN);
- на основе MAC-адресов (MAC-based VLAN);
- частные (Private VLAN);
- для передачи голосовых сообщений (Voice VLAN);
- для передачи видеоданных (Surveillance VLAN);
- асимметричные.

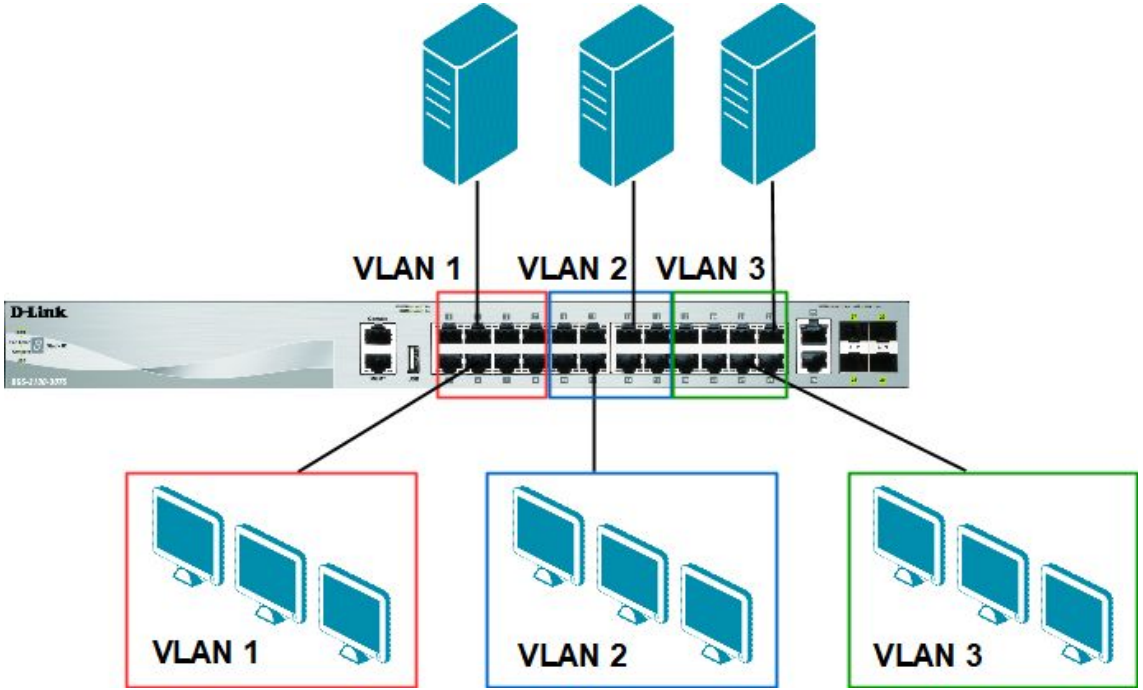
# VLAN на основе портов

## VLAN на основе портов

- При использовании VLAN на основе портов (Port-based VLAN), каждый порт назначается в определенную VLAN, независимо от того, какой компьютер подключен к этому порту.
- Все пользователи, подключенные к этому порту, будут членами одной VLAN.
- Конфигурация портов – статическая и может быть изменена только вручную.

# VLAN на основе портов

## VLAN на основе портов



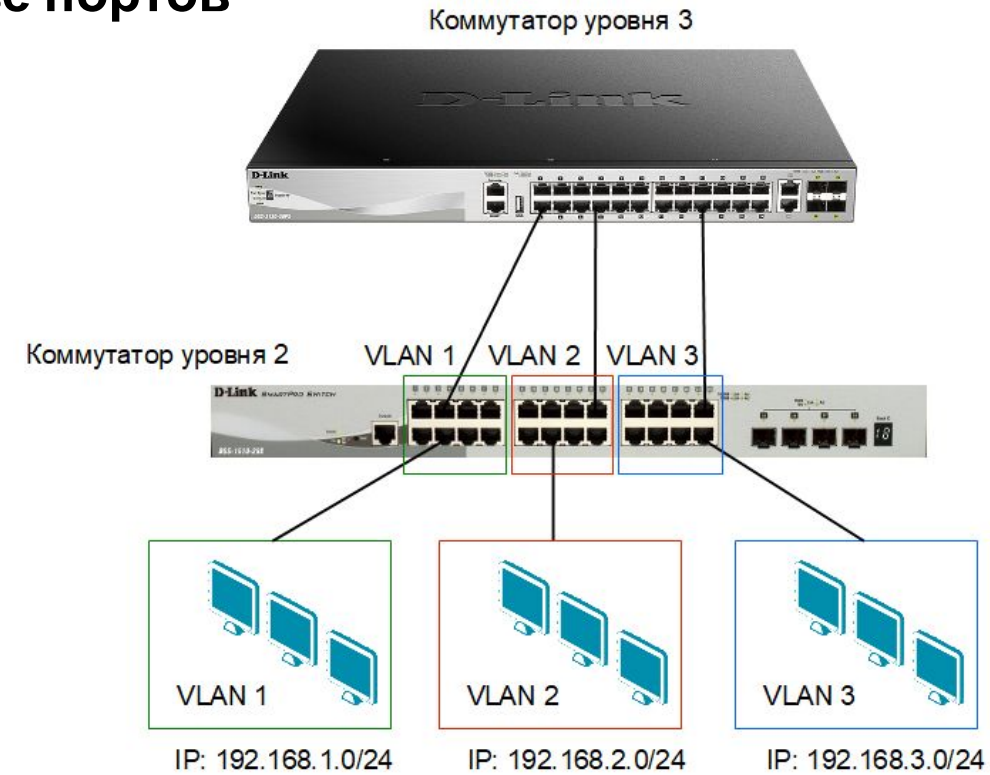
# VLAN на основе портов

## VLAN на основе портов

Для объединения виртуальных подсетей как внутри одного коммутатора, так и между двумя коммутаторами, нужно использовать сетевой уровень OSI-модели.

# VLAN на основе портов

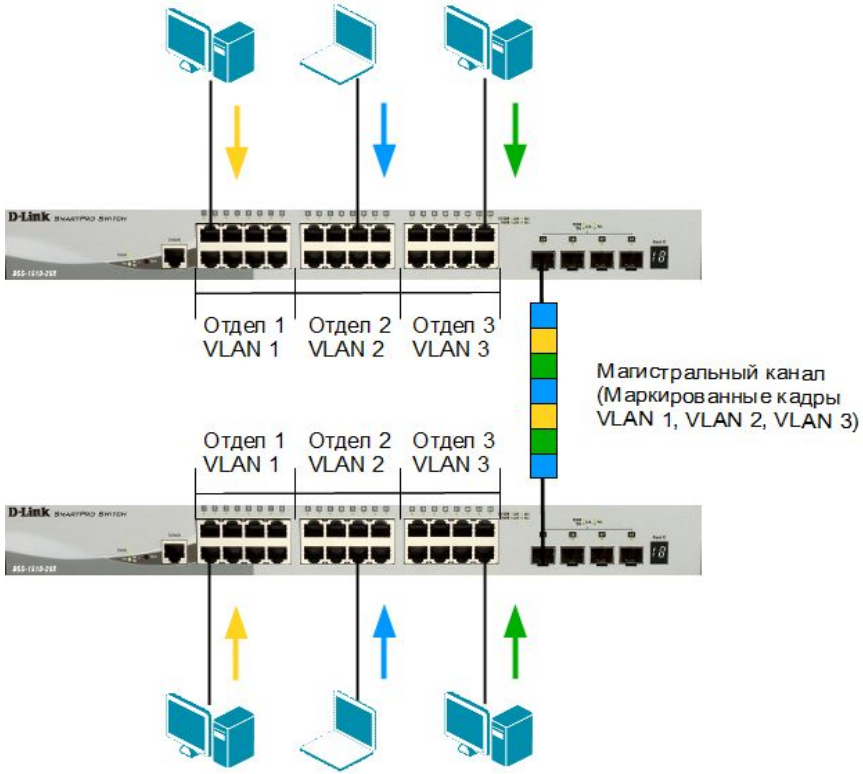
## VLAN на основе портов



## VLAN на основе стандарта IEEE 802.1Q

Виртуальные локальные сети, построенные на основе стандарта IEEE 802.1Q, используют дополнительные поля кадра Ethernet для хранения информации о принадлежности к VLAN при его перемещении по сети.

# VLAN на основе стандарта IEEE 802.1Q



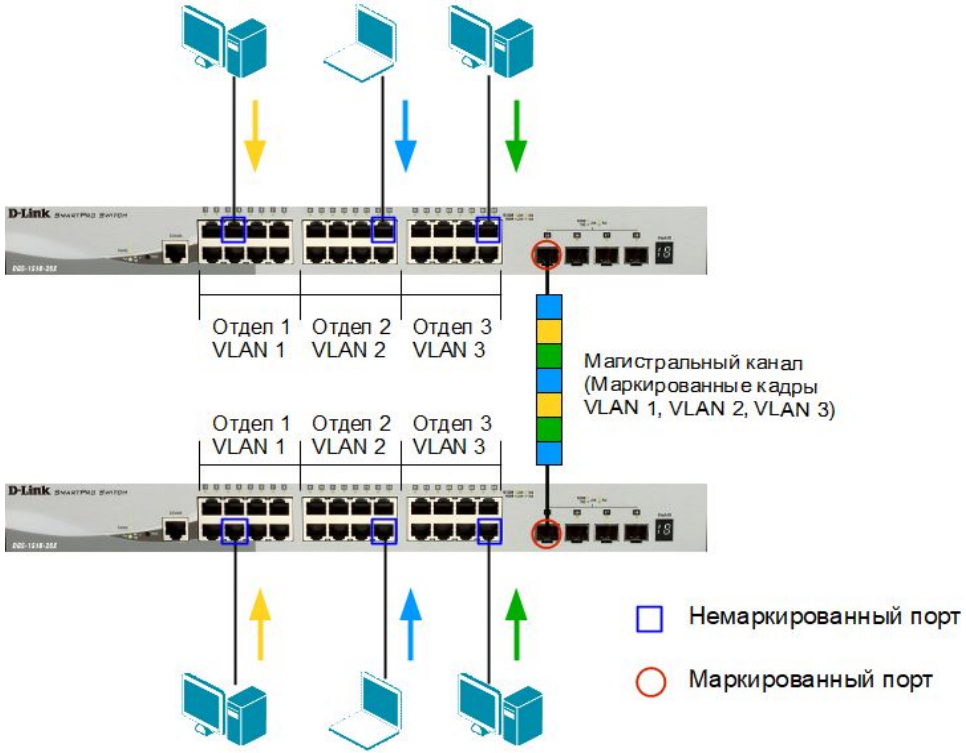
# VLAN на основе стандарта IEEE 802.1Q

## Некоторые определения IEEE 802.1Q

- **Tagging (Маркировка кадра)** – процесс добавления информации о принадлежности к 802.1Q VLAN в заголовок кадра Ethernet.
- **Untagging (Извлечение тега из кадра)** – процесс извлечения информации о принадлежности к 802.1Q VLAN из заголовка кадра Ethernet.
- **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, маршрутизаторы, точки доступа, серверы или рабочие станции, и при этом приниматься решение о маркировке.

# VLAN на основе стандарта IEEE 802.1Q

## Маркированные и немаркированные порты VLAN



# VLAN на основе стандарта IEEE 802.1Q

## Тег VLAN IEEE 802.1Q

**Обычный (немаркированный) кадр**

| Адрес назначения (DA) | Адрес источника (SA) | Длина/тип (Length/Type) | Данные (Data) | Контрольная сумма кадра (FCS) |
|---|---|---|---|---|

**Маркированный кадр 802.1p/802.1Q**

| Адрес назначения (DA) | Адрес источника (SA) | **Тег (Tag)** | Длина/тип (Length/Type) | Данные (Data) | Контрольная сумма кадра (FCS) |
|---|---|---|---|---|---|

| Идентификатор протокола тега (TPID) 0x8100 | Приоритет (Priority) | Индикатор канонического формата (CFI) | **Идентификатор VLAN (VID)** |
|---|---|---|---|
| 16 бит | 3 бита | 1 бит | 12 бит |

# VLAN на основе стандарта IEEE 802.1Q

## Port VLAN ID

- Каждый физический порт коммутатора имеет *идентификатор порта VLAN* (*PVID*).
- PVID используется для определения, 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).
- Коммутаторы, поддерживающие протокол IEEE 802.1Q, должны хранить таблицу, связывающую идентификаторы портов PVID с идентификаторами VID сети.
- Каждый порт 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.

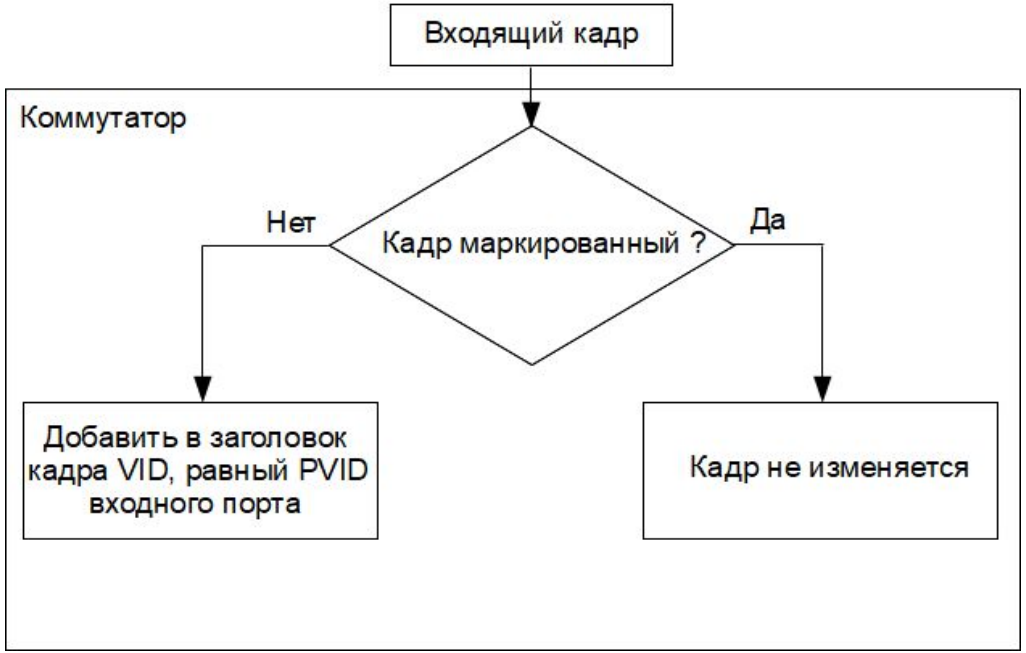
## Продвижение кадров VLAN IEEE 802.1Q

Решение о продвижении кадра внутри виртуальной локальной сети принимается на основе трех следующих правил:

- правила входящего трафика (**ingress rules**) – классификация получаемых кадров относительно принадлежности к VLAN;
- правила продвижения между портами (**forwarding rules**) – принятие решения о продвижении или отбрасывании кадра;
- правила исходящего трафика (**egress rules**) – принятие решения о сохранении или удалении в заголовке кадра тега 802.1Q перед его передачей.

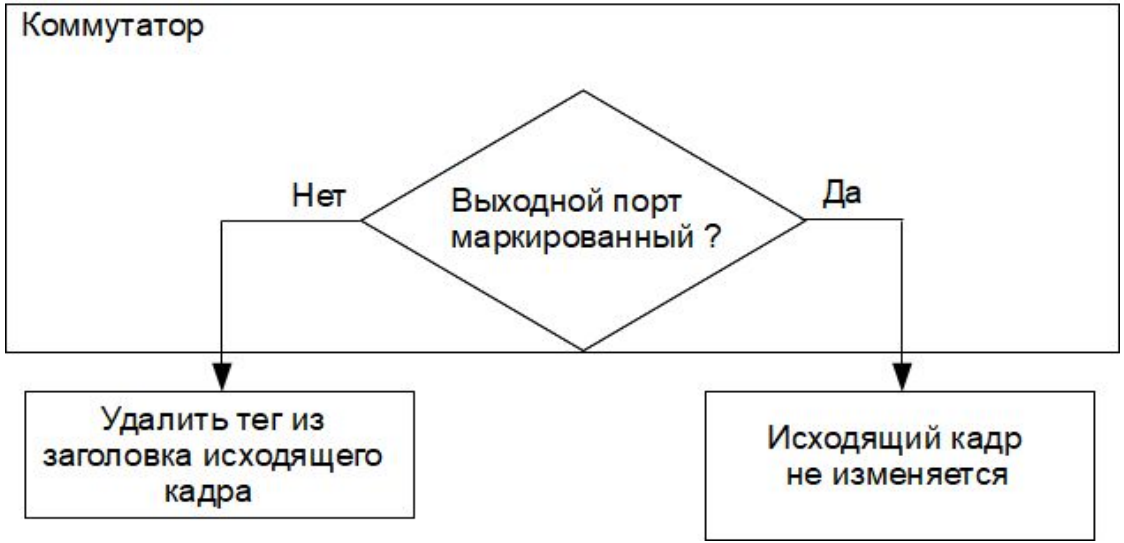
# VLAN на основе стандарта IEEE 802.1Q

## Правила входящего трафика



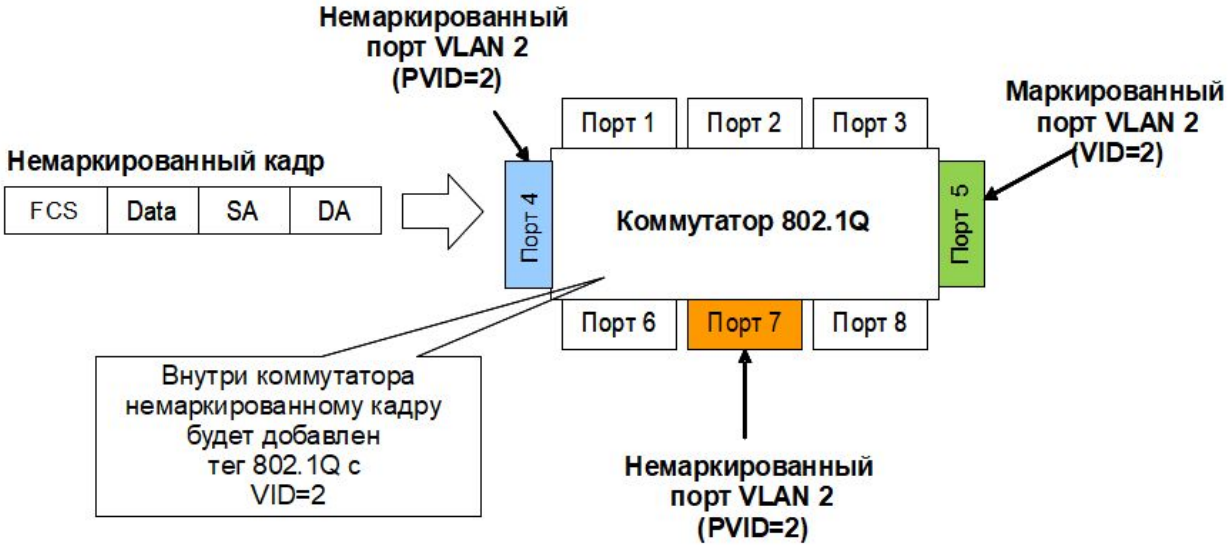
# VLAN на основе стандарта IEEE 802.1Q

## Правила исходящего трафика



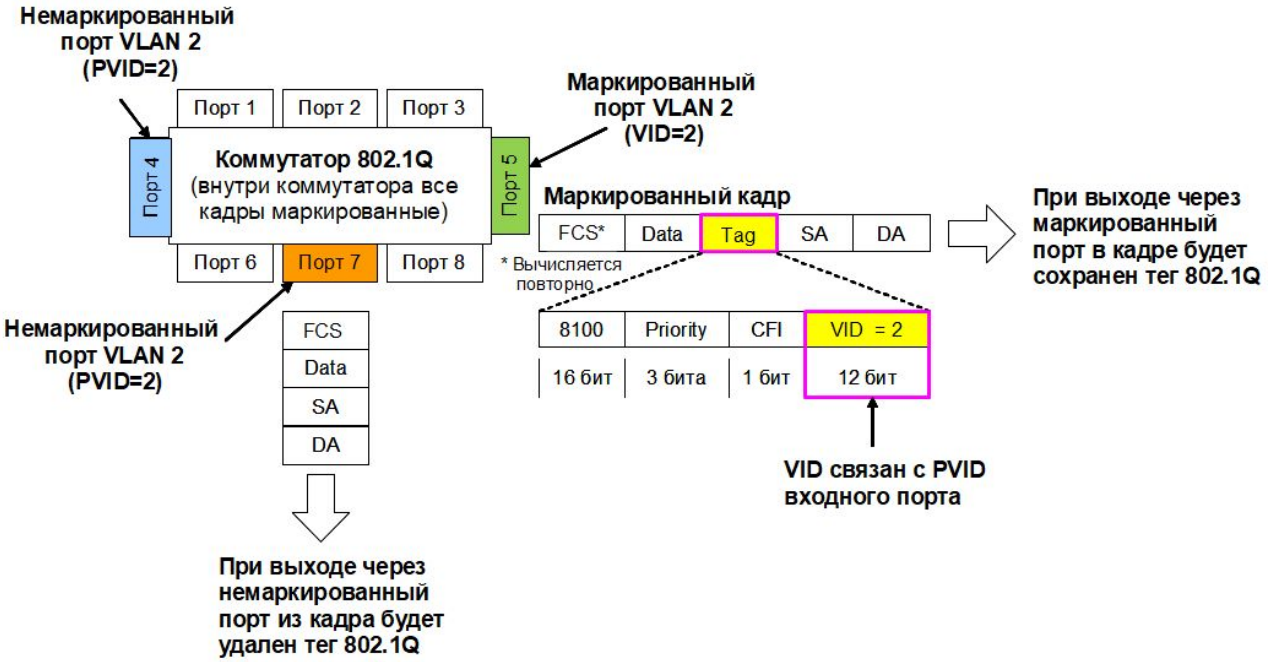
# VLAN на основе стандарта IEEE 802.1Q

## Пример передачи немаркированного кадра



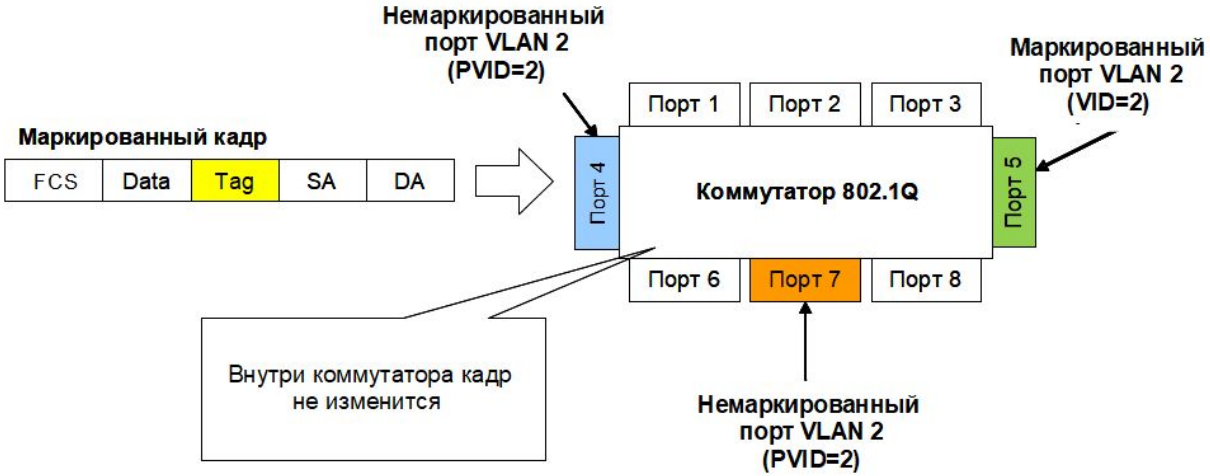
# VLAN на основе стандарта IEEE 802.1Q

## Пример передачи немаркированного кадра



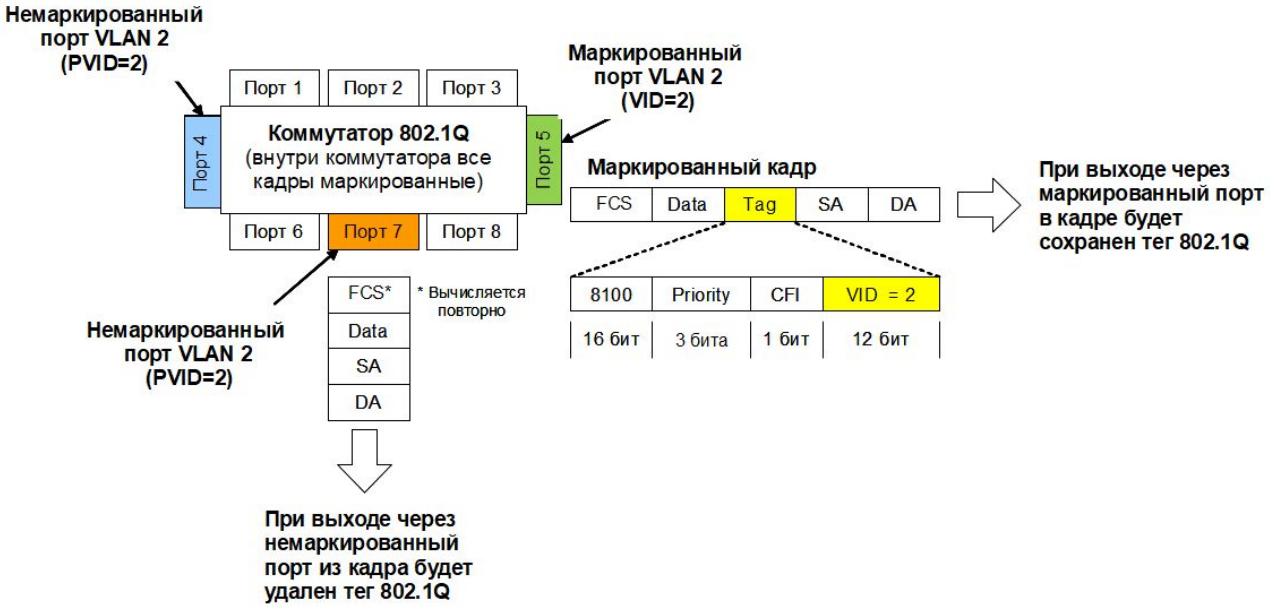
# VLAN на основе стандарта IEEE 802.1Q

## Пример передачи маркированного кадра



# VLAN на основе стандарта IEEE 802.1Q

## Пример передачи маркированного кадра



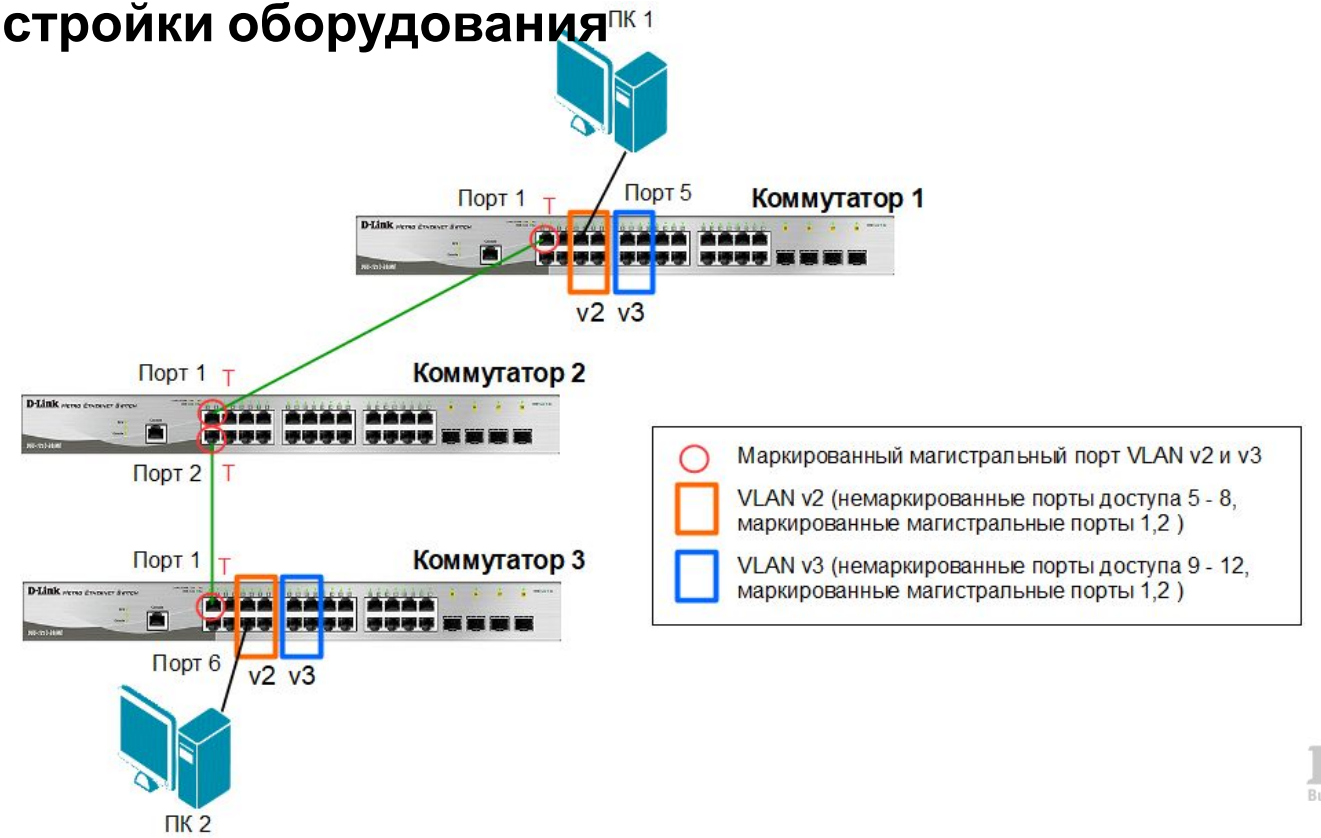
# VLAN на основе стандарта IEEE 802.1Q

## Настройка VLAN IEEE 802.1Q

- По умолчанию все порты коммутатора входят в VLAN 1.
- **VLAN 1** – это VLAN по умолчанию (default VLAN). Она не может быть удалена, но может использоваться.
- Для сегментации сети, надо создать на каждом коммутаторе столько виртуальных сетей, сколько требует конфигурация.
- Порты, входящие в VLAN, должны быть настроены как немаркированные или маркированные.

# VLAN на основе стандарта IEEE 802.1Q

## Пример настройки оборудования



# VLAN на основе стандарта IEEE 802.1Q

## Настройка коммутатора 1

**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 tag 3
```

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

```
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
```

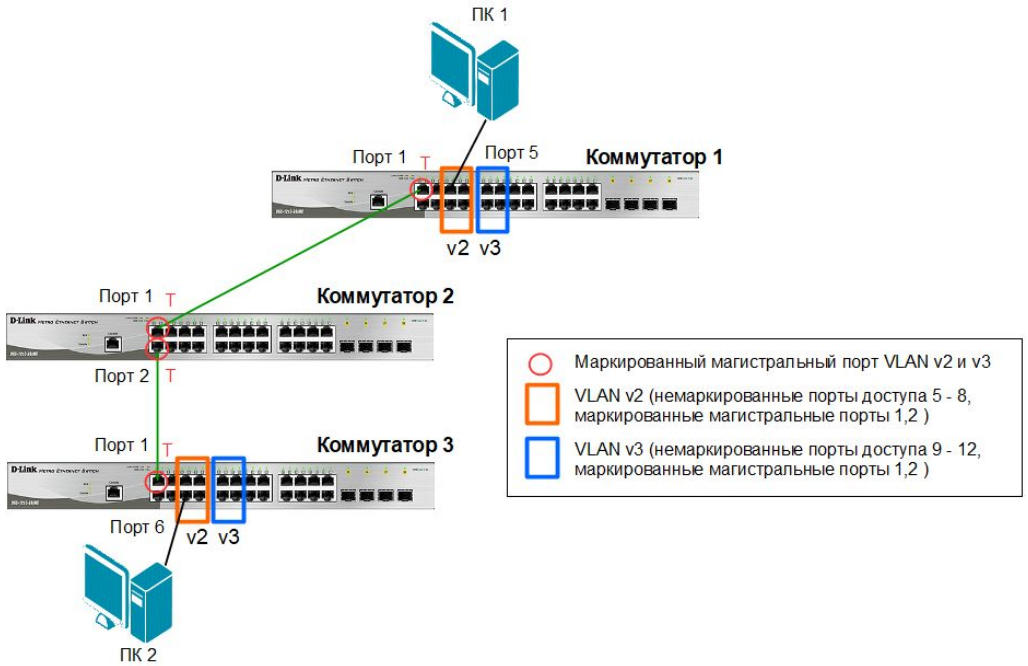
# VLAN на основе стандарта IEEE 802.1Q

## 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
```



# VLAN на основе стандарта IEEE 802.1Q

Результат выполнения команды show vlan на коммутаторе 1:

```
DGS-1210-28/ME:5# show vlan
Command: show vlan

VID               : 1        VLAN NAME      : default
VLAN Type         : Static
VLAN Advertisement : Disabled
Member Ports      : 13-28
Tagged Ports      :
Untagged Ports    : 13-28
Forbidden Ports   :

VID               : 2        VLAN NAME      : v2
VLAN Type         : Static
VLAN Advertisement : Disabled
Member Ports      : 1-2,5-8
Tagged Ports      : 1-2
Untagged Ports    : 5-8
Forbidden Ports   :

VID               : 3        VLAN NAME      : v3
VLAN Type         : Static
VLAN Advertisement : Disabled
Member Ports      : 1-2,9-12
Tagged Ports      : 1-2
Untagged Ports    : 9-12
Forbidden Ports   :



Total Entries  : 3
```

# VLAN на основе стандарта IEEE 802.1Q

Результат выполнения команды show vlan на коммутаторе 2:

```
DGS-1210-28/ME:5# show vlan
Command: show vlan

VID              : 1        VLAN NAME       : default
VLAN Type        : Static
VLAN Advertisement : Disabled
Member Ports     : 3-28
Tagged Ports     :
Untagged Ports   : 3-28
Forbidden Ports  :

VID              : 2        VLAN NAME       : v2
VLAN Type        : Static
VLAN Advertisement : Disabled
Member Ports     : 1-2
Tagged Ports     : 1-2
Untagged Ports   :
Forbidden Ports  :

VID              : 3        VLAN NAME       : v3
VLAN Type        : Static
VLAN Advertisement : Disabled
Member Ports     : 1-2
Tagged Ports     : 1-2
Untagged Ports   :
Forbidden Ports  :



Total Entries  : 3
```

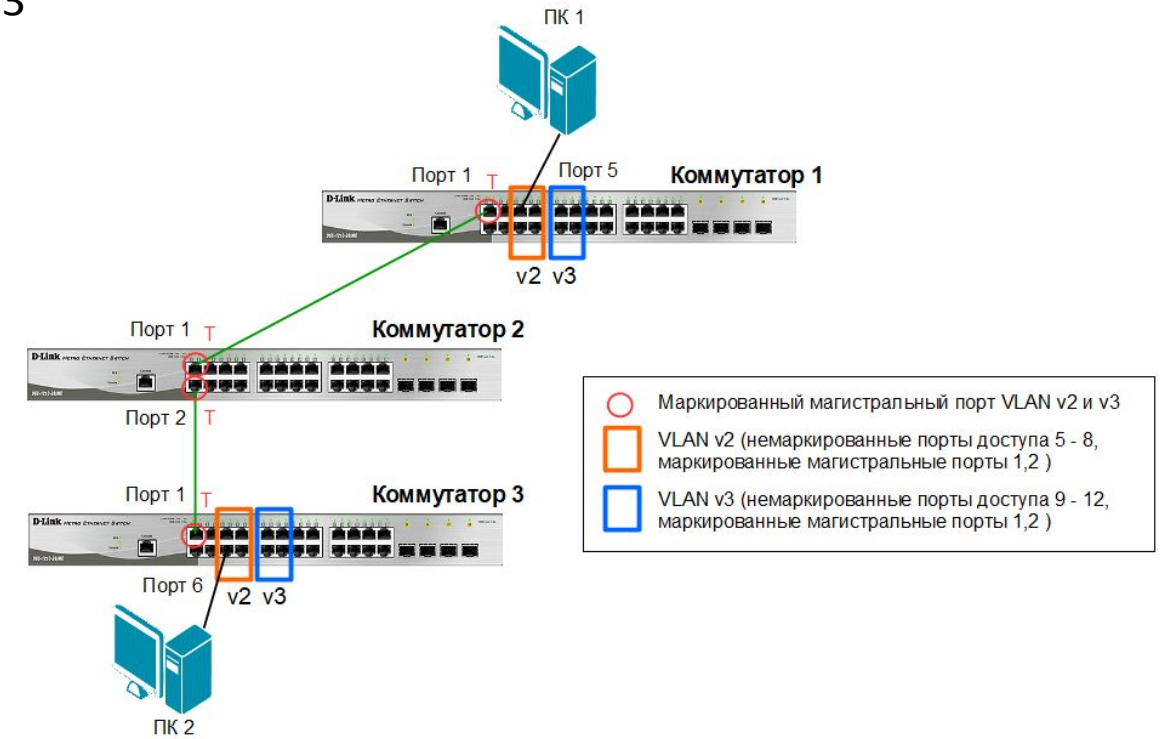
# VLAN на основе стандарта IEEE 802.1Q

Результат выполнения команды show vlan на коммутаторе 3:

```
DGS-1210-28/ME:5# show vlan
Command: show vlan

VID               : 1        VLAN NAME      : default
VLAN Type         : Static
VLAN Advertisement : Disabled
Member Ports      : 13-28
Tagged Ports      :
Untagged Ports    : 13-28
Forbidden Ports   :

VID               : 2        VLAN NAME      : v2
VLAN Type         : Static
VLAN Advertisement : Disabled
Member Ports      : 1,5-8
Tagged Ports      : 1
Untagged Ports    : 5-8
Forbidden Ports   :

VID               : 3        VLAN NAME      : v3
VLAN Type         : Static
VLAN Advertisement : Disabled
Member Ports      : 1,9-12
Tagged Ports      : 1
Untagged Ports    : 9-12
Forbidden Ports   :



Total Entries  : 3
```

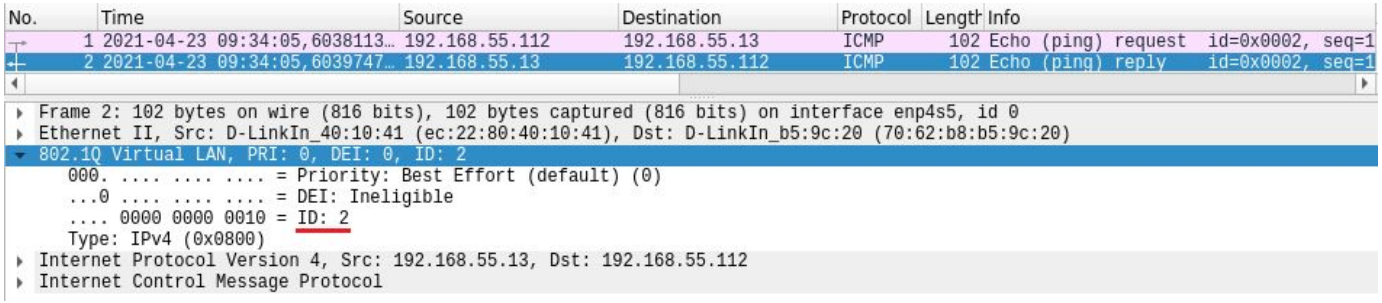
# VLAN на основе стандарта IEEE 802.1Q

Рассмотрим пересылку кадра с порта 5 коммутатора 1 на порт 6 коммутатора 3



# VLAN на основе стандарта IEEE 802.1Q

Порт 5 коммутатора 1 является немаркированным портом VLAN v2 (PVID=2). Когда любой немаркированный кадр поступает на порт 5, коммутатор снабжает его тегом 802.1Q со значением VID равным 2.



# VLAN на основе стандарта IEEE 802.1Q

Таблица коммутации коммутатора 1

```
Command: show fdb

VID  VLAN Name                        MAC Address       Port Type
---- ------------------------------- ----------------- ---- ---------------
1    default                         EC-AD-E0-F8-4A-C0 CPU  Self
2    v2                              48-9E-BD-52-68-26 5    Dynamic
2    v2                              C8-5B-76-B6-81-9D 1    Dynamic

Total Entries  : 3
```

# VLAN на основе стандарта IEEE 802.1Q

Таблица коммутации коммутатора 2

```
Command: show fdb

VID  VLAN Name                        MAC Address       Port Type
---- ------------------------------- ----------------- ---- ---------------
1    default                         18-0F-76-EC-99-66 CPU  Self
2    v2                              48-9E-BD-52-68-26 1    Dynamic
2    v2                              C8-5B-76-B6-81-9D 2    Dynamic

Total Entries  : 3
```

# VLAN на основе стандарта IEEE 802.1Q

Таблица коммутации коммутатора 3

```
Command: show fdb

VID  VLAN Name                        MAC Address       Port Type
---- -------------------------------- ----------------- ---- ---------------
1    default                          6C-19-8F-F3-39-DF CPU  Self
2    v2                               48-9E-BD-52-68-26 1    Dynamic
2    v2                               C8-5B-76-B6-81-9D 6    Dynamic

Total Entries  : 3
```

# VLAN на основе портов и протоколов

- Стандарт IEEE 802.1v-2001 является расширением стандарта IEEE 802.1Q и в настоящее время является частью стандарта IEEE 802.1Q-2018.
- Определяет методы объединения узлов в виртуальные локальные сети на основе поддерживаемых ими протоколов.
- При определении членства в VLAN осуществляется классификация *немаркированных* кадров по типу протокола и порту.
- Формат тега 802.1v аналогичен формату тега 802.1Q.

# VLAN на основе портов и протоколов

## Правила классификации входящих кадров

- При поступлении на порт *немаркированного* кадра коммутатором осуществляется проверка заголовка канального уровня и типа протокола вышележащего уровня инкапсулированного в кадр. 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.

# VLAN на основе портов и протоколов

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 идентификатора протокола в нем.

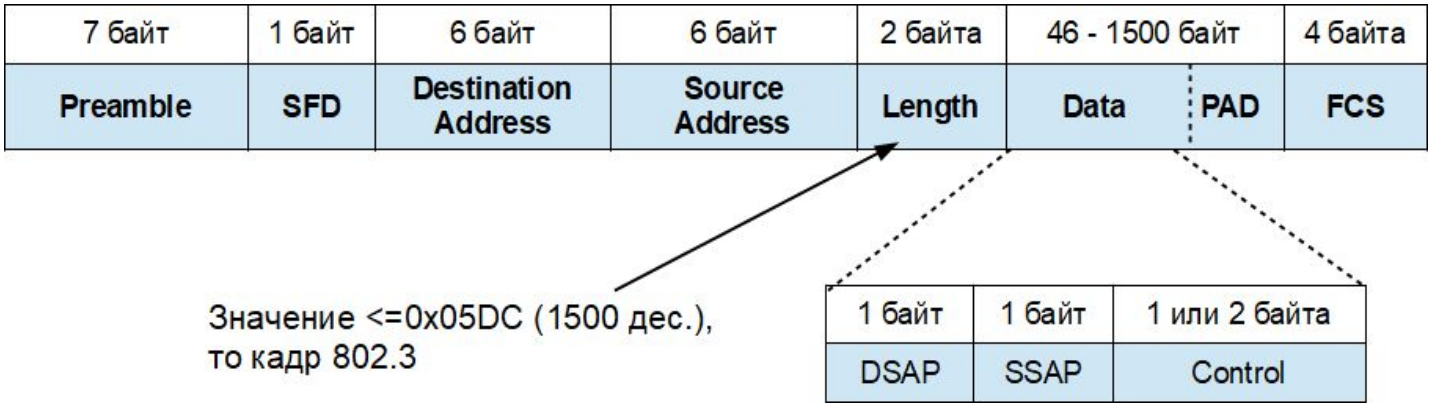
# VLAN на основе портов и протоколов

## Формат кадра IEEE 802.3-2018

| 7 байт | 1 байт | 6 байт | 6 байт | 2 байта | 46-1500, 1504 или 1982 байта | | 4 байта | |
|---|---|---|---|---|---|---|---|---|
| **Preamble** | **SFD** | **Destination Address** | **Source Address** | **Length/ Type** | **Data** | **PAD** | **FCS** | **Extension** |
| | | **64 — 2000 байта** | | | | | | |

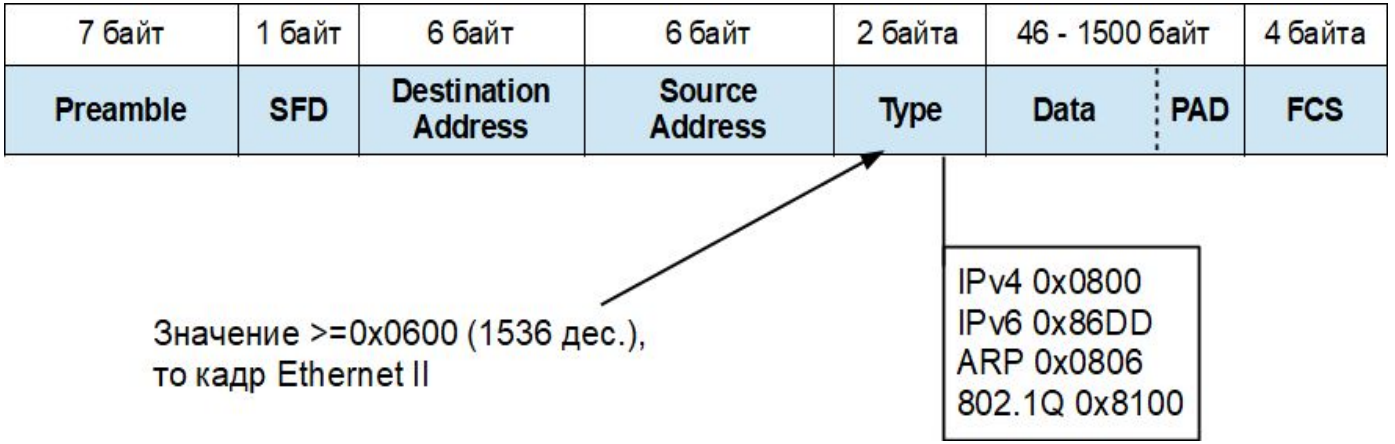
# VLAN на основе портов и протоколов

## Формат кадра IEEE 802.3/LLC



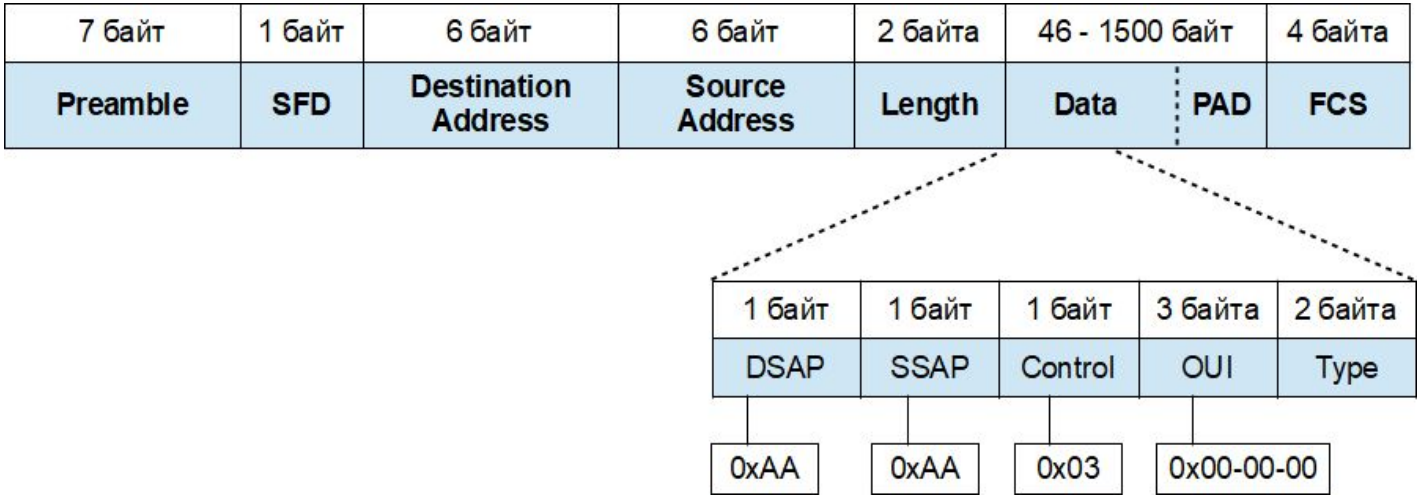
# VLAN на основе портов и протоколов

## Формат кадра Ethernet II



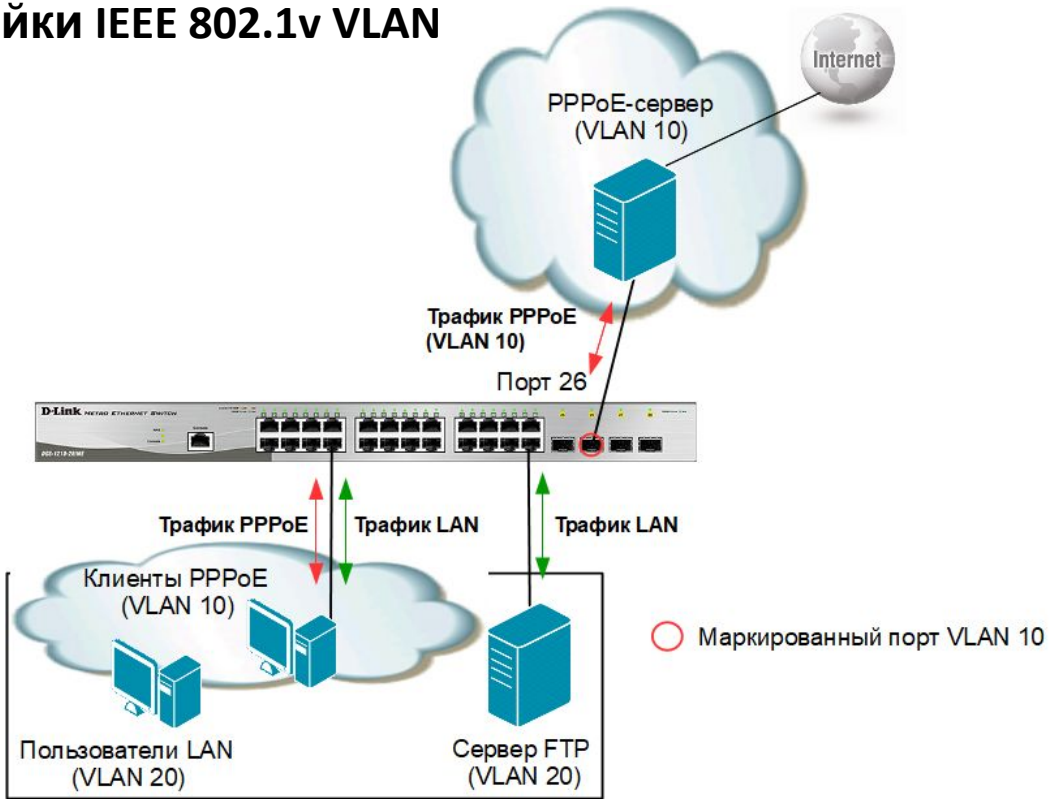
# VLAN на основе портов и протоколов

## Формат кадра Ethernet SNAP



# VLAN на основе портов и протоколов

## Пример настройки IEEE 802.1v VLAN



# VLAN на основе портов и протоколов

## Настройка коммутатора

1. Создание новых VLAN 802.1Q:

```
config vlan default delete 1-26
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 untagged 1-24
```

2. Настройка PVID портов, к которым подключены пользователи:

```
config gvrp 1-24 pvid 20
```

# VLAN на основе портов и протоколов

**3**. 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 0x8863
create dot1v_protocol_group group_id 2 group_name pppoe_session
config dot1v_protocol_group group_id 2 add protocol ethernet_2 0x8864
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
```

# VLAN на основе портов и протоколов

**4.** Проверка выполненных настроек.

**Настройки групп протоколов**

```
DGS-1210-28/ME:5# show dot1v_protocol_group
Command: show dot1v_protocol_group


Group ID Protocol Group Name              Frame Type     Protocol Value
-------- -------------------------------- -------------- --------------
1        pppoe_disc                       EthernetII     8863

2        pppoe_session                    EthernetII     8864
```

# VLAN на основе портов и протоколов

## Настройки классификации VLAN на основе портов и протоколов

```
DGS-1210-28/ME:5# show port dot1v ports 1-3
Command: show port dot1v ports 1-3


Port: 1
Protocol Group ID     VLAN Name
-------------------   ---------------------------------
1                     pppoe
2                     pppoe

Port: 2
Protocol Group ID     VLAN Name
-------------------   ---------------------------------
1                     pppoe
2                     pppoe

Port: 3
Protocol Group ID     VLAN Name
-------------------   ---------------------------------
1                     pppoe
2                     pppoe
```

# Private VLAN

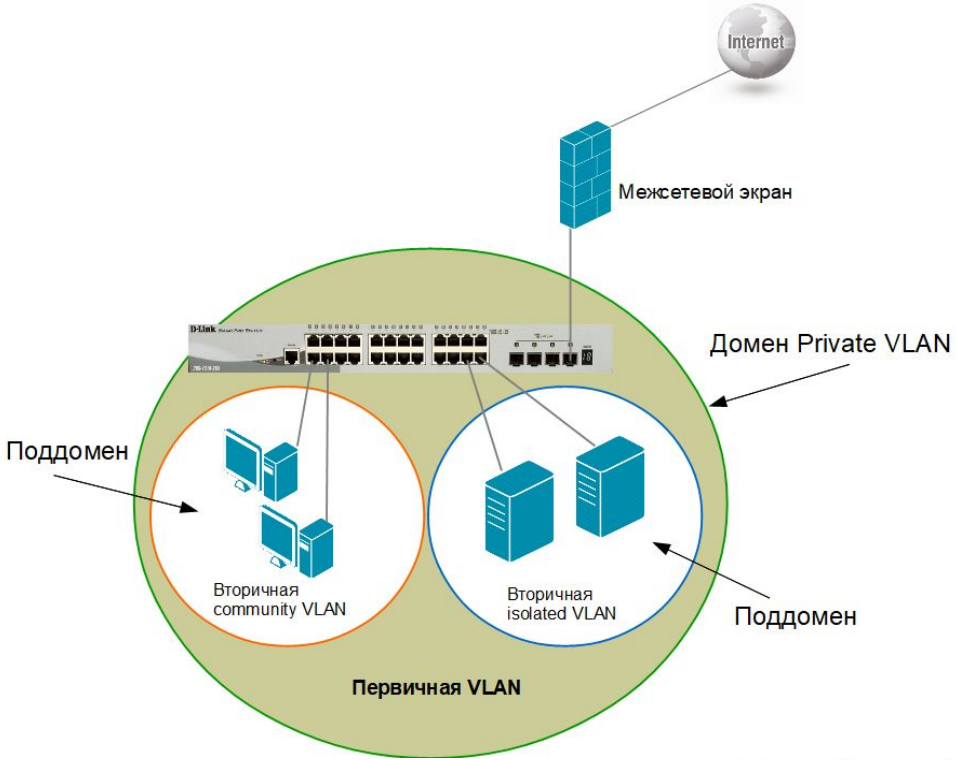
Технология **частных VLAN** (Private VLAN, PVLAN), определенная в RFC 5517, позволяет увеличить количество VLAN, но при этом эффективно использовать идентификаторы VLAN и IP-адреса, повысить безопасность.

Ее можно применять в тех случаях, когда необходимо изолировать трафик разных клиентов или разделить разные типы трафика.

# Private VLAN

Функция Private VLAN делит большой широковещательный домен VLAN на поддомены.

Поддомен представляет собой пару частных VLAN: **первичную VLAN** (primary VLAN) и **вторичную VLAN** (secondary VLAN).



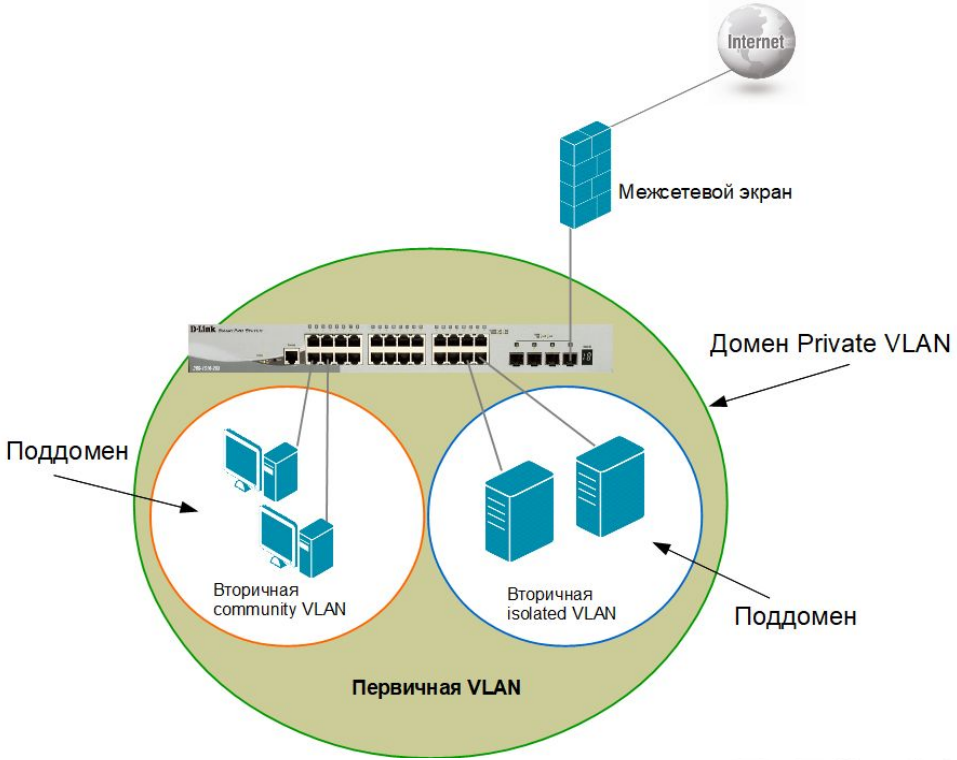
# Private VLAN

- Поддомен не может идентифицироваться с помощью одного VLAN ID.
- Для идентификации поддомена используется пара VLAN ID: идентификатор первичной VLAN (Vp) плюс идентификатор вторичной VLAN (Vs).
- **Первичная VLAN** □ это уникальный и общий идентификатор VLAN для всего домена PVLAN и всех пар его идентификаторов VLAN.
- Идентификаторы вторичных VLAN позволяют отличить один поддомен от другого.

# Private VLAN

Вторичные VLAN могут быть двух типов:

- **isolated** (изолированная) – это вторичная VLAN, у которой все узлы, подключенные к ее портам, изолированы на канальном уровне;
- **community** (VLAN сообщества) – это вторичная VLAN, связанная с группой портов, которые подключены к определенному сообществу конечных устройств с доверительными отношениями.




D-Link
Building Networks for People

# Private VLAN

- В домене PVLAN может быть создана **только одна** изолированная VLAN и несколько VLAN сообществ.
- Вторичные VLAN могут быть ассоциированы **только с одной** первичной VLAN.
- Диапазон идентификаторов для первичной и вторичных VLAN – от 2 до 4094.
- К данным, передаваемым в первичной и вторичных VLAN, добавляется единственный тег в соответствии со стандартом IEEE 802.1Q.

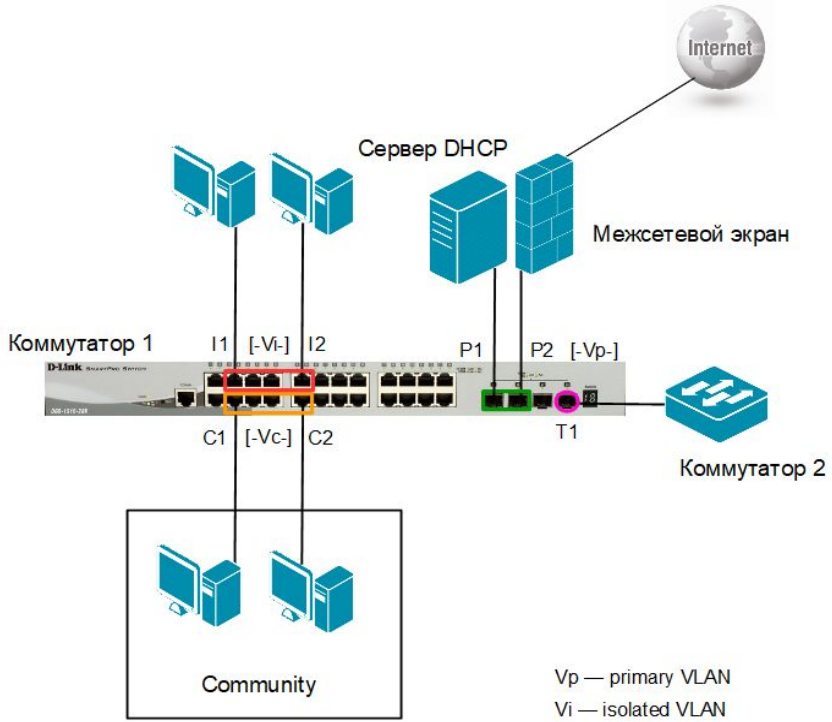
# Private VLAN

- Для маршрутизации между VLAN каждой их них требуется назначить IP-адрес подсети.
- Несмотря на то, что функция Private VLAN увеличивает количество VLAN, для вторичных VLAN не требуются отдельный IP-адрес подсети.
- В домене PVLAN все его члены используют адресное пространство, которое является частью подсети, ассоциированной с первичной VLAN.

# Private VLAN

## Порты Private VLAN

- Каждый тип VLAN (primary, isolated, community) определяется путем присвоения надлежащего обозначения группе портов коммутатора.
- Существует три типа портов.

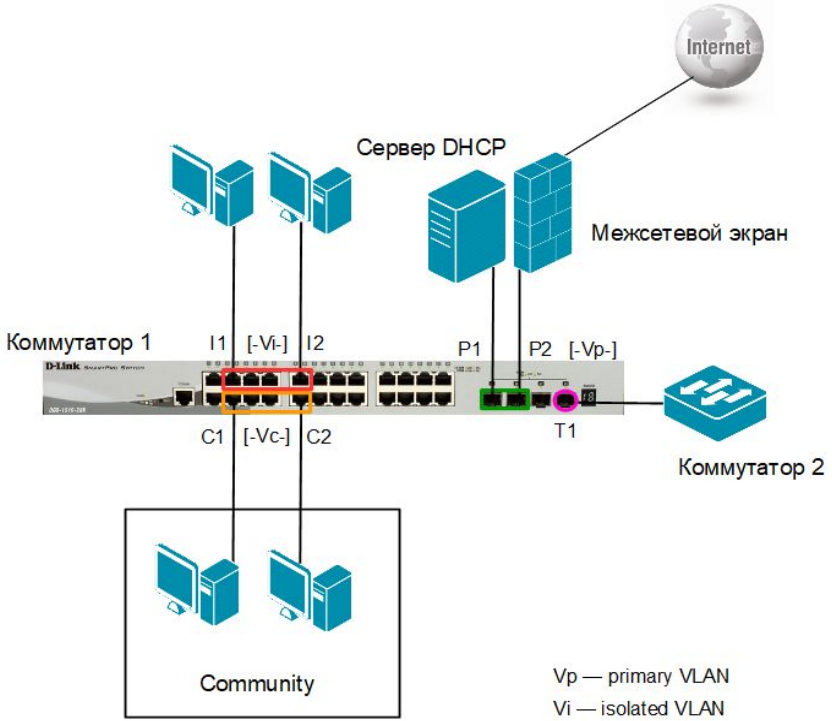



Vp — primary VLAN
Vi — isolated VLAN
Vc — community VLAN
P1, P2 — порты promiscuous коммутатора
I1, I2 — порты isolated коммутатора
C1, C2 — порты community коммутатора
T1 — порт связи между коммутаторами с поддержкой VLAN

# Private VLAN

**Promiscuous** (неразборчивый порт)

- Принадлежит первичной VLAN и может обмениваться данными со всеми интерфейсами, включая изолированные порты и порты сообщества вторичных VLAN, ассоциированных с данной первичной VLAN.
- В одном домене PVLAN можно определить несколько неразборчивых портов.

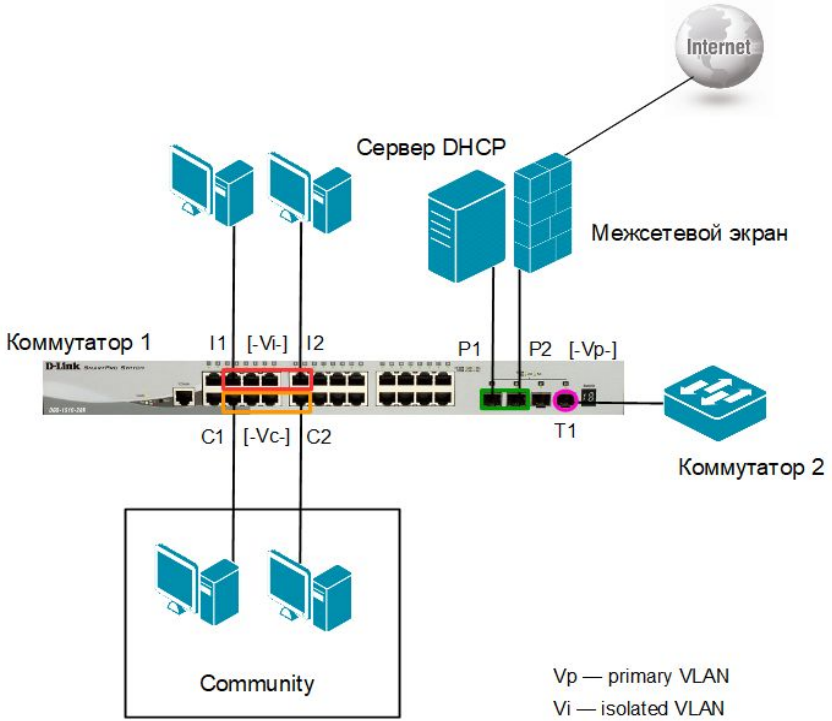



Vp — primary VLAN
Vi — isolated VLAN
Vc — community VLAN
P1, P2 — порты promiscuous коммутатора
I1, I2 — порты isolated коммутатора
C1, C2 — порты community коммутатора
T1 — порт связи между коммутаторами с поддержкой VLAN

# Private VLAN

**Isolated** (изолированный порт)

- Принадлежит вторичной изолированной VLAN.
- Внутри домена PVLAN изолированные порты могут взаимодействовать только с неразборчивыми портами. Изолированным портом обычно является порт доступа, но в некоторых случаях им может быть гибридный/магистральный порт.

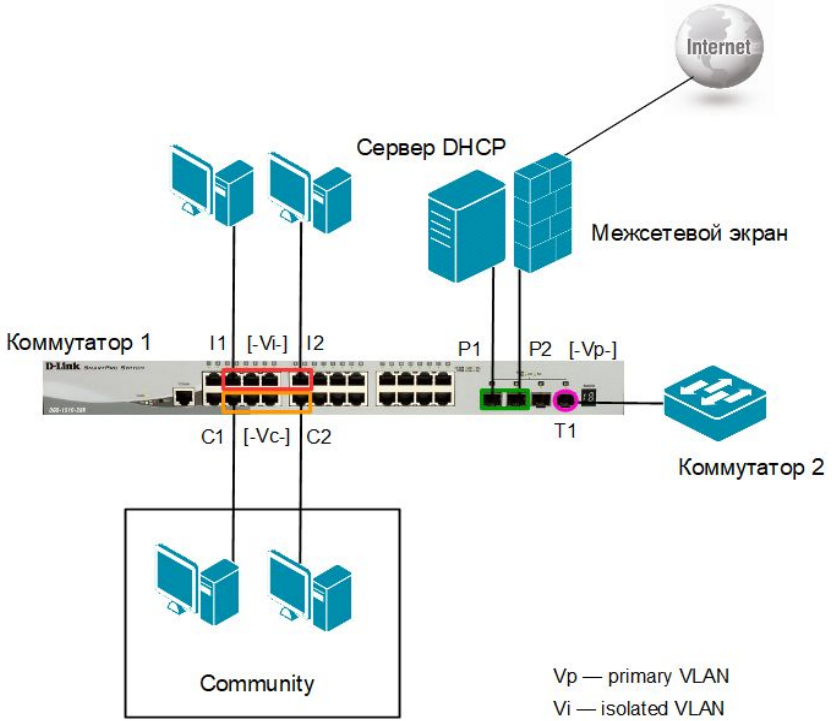



Vp — primary VLAN
Vi — isolated VLAN
Vc — community VLAN
P1, P2 — порты promiscuous коммутатора
I1, I2 — порты isolated коммутатора
C1, C2 — порты community коммутатора
T1 — порт связи между коммутаторами с поддержкой VLAN

# Private VLAN

**Community** (порт сообщества)

- Принадлежит вторичной VLAN сообщества.
- Порты из одной VLAN сообщества могут передавать данные друг другу и взаимодействовать с любым неразборчивым портом.
- Порты сообщества, не могут обмениваться данными с портами из другой VLAN сообщества и с изолированными портами.




Vp — primary VLAN
Vi — isolated VLAN
Vc — community VLAN
P1, P2 — порты promiscuous коммутатора
I1, I2 — порты isolated коммутатора
C1, C2 — порты community коммутатора
T1 — порт связи между коммутаторами с поддержкой VLAN

# Private VLAN

- Private VLAN как и VLAN 802.1Q может быть настроена на разных коммутаторах, если они соединены магистральными каналами. Магистральный порт передает кадры либо из первичной VLAN, либо из вторичной VLAN.
- С PVLAN связаны два типа магистральных портов: *trunk promiscuous* (магистральный неразборчивый) и *trunk secondary* (магистральный вторичный).

# Private VLAN

## Правила настройки функции Private VLAN на коммутаторах с D-Link-like CLI

- Private VLAN может содержать одну isolated VLAN и несколько community VLAN.
- Вторичные VLAN не могут быть ассоциированы с несколькими первичными.
- Немаркированные порты первичной VLAN называются неразборчивыми (promiscuous) портами.
- Маркированные порты первичной VLAN называются магистральными (trunk) портами.
- Неразборчивый (promiscuous) порт одной Private VLAN не может быть неразборчивым портом другой Private VLAN.
- Порт первичной VLAN не может быть одновременно портом вторичной VLAN, и наоборот.
- Вторичные VLAN могут содержать только немаркированные порты.

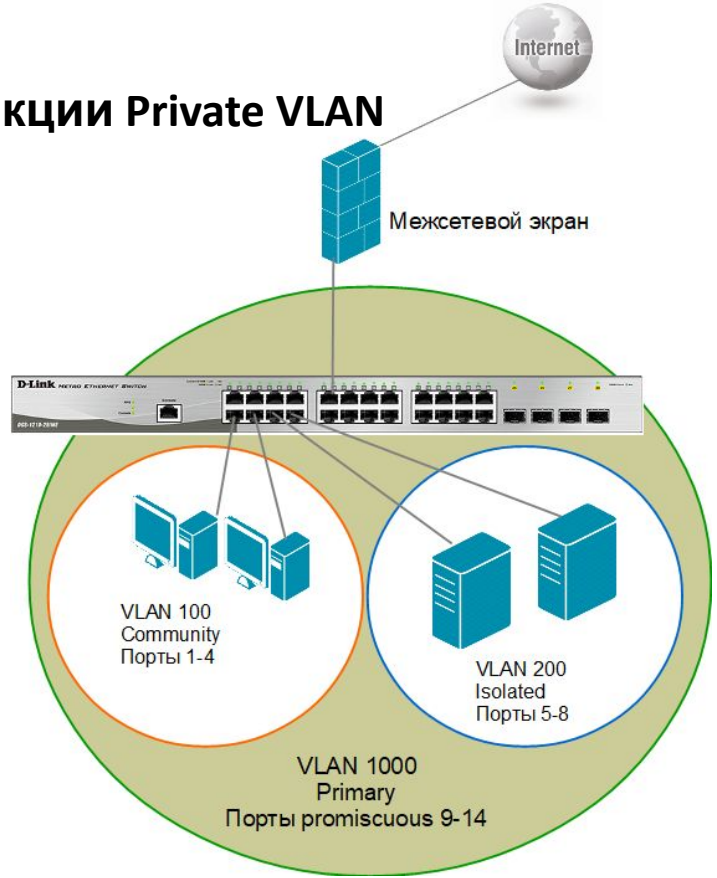
# Private VLAN

## Правила настройки функции Private VLAN на коммутаторах с D-Link-like CLI

- Порт, принадлежащий одной вторичной VLAN, не может одновременно принадлежать другой вторичной VLAN.
- Когда VLAN ассоциирована с первичной как вторичная, неразборчивый порт первичной VLAN ведет себя как немаркированный порт вторичной VLAN, а магистральный порт первичной VLAN – как маркированный порт вторичной VLAN.
- Только первичная VLAN может быть сконфигурирована как L3-интерфейс.
- На портах, принадлежащих private VLAN, не может быть настроена функция сегментации трафика (Traffic segmentation).

# Private VLAN

## Пример настройки функции Private VLAN



# Private VLAN

## Настройка коммутатора

**1**. Удаление соответствующих портов из VLAN по умолчанию (default VLAN), создание вторичных VLAN v100 и v200:

```
config vlan default delete 1-14
create vlan v100 tag 100
create vlan v200 tag 200
```

**2**. Добавить порты во вторичные VLAN как немаркированные: порты 1-4 в VLAN v100, порты 5-8 в v200:

```
config vlan v100 add untagged 1-4
config vlan v200 add untagged 5-8
```

# Private VLAN

**3**. Настройка первичной VLAN 1000 и ассоциация вторичных VLAN с первичной:

```
create vlan vlanid 1000 private_vlan
config private_vlan vlanid 1000 add community v100
config private_vlan vlanid 1000 add isolated v200
```

**4**. Добавить порты 9-14 в первичную VLAN 1000 как немаркированные (promiscuous):

```
config vlan vlanid 100 add untagged 9-14
```

# Private VLAN

**5**. Проверить выполненные настройки.

```
Command: show private_vlan

Trunk Promiscuous Ports:
Trunk Secondary Ports:


Primary Vlan ID: 1000
----------------------------------------
Promiscuous Ports :
Community Ports    : 1-4,9-14    Community VLAN: 100
Isolated Ports     : 5-8         Isolated VLAN : 200



Total Entries   : 1
```

# Статические и динамические VLAN

- Для корректной работы виртуальной локальной сети требуется, чтобы в базе данных фильтрации (*Filtering Database*) содержалась информация о членстве в VLAN.
- Существуют два способа, позволяющих устанавливать членство в VLAN:
  - статические VLAN;
  - динамические VLAN.

# Статические и динамические VLAN

- В статических VLAN установление членства осуществляется вручную администратором.
- 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 и динамические VLAN

- **Статические записи о регистрации в VLAN** (*Static VLAN Registration Entries*) используются для представления информации о статических VLAN в базе данных фильтрации.
- 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).

# Статические и динамические VLAN

**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;
- 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

Протокол GVRP рассылает сообщения GVRP BPDU (GVRP Bridge Protocol Data Units) на многоадресный MAC-адрес 01-80-C2-00-00-21 для оповещения устройств-подписчиков о различных событиях.

# Протокол GVRP

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.

- **LeaveAll 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.

# Протокол GVRP

## Таймеры GVRP

**Join Timer** – время (от 100 до 100 000 мс), 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 мс.

# Протокол GVRP

## Таймеры GVRP

**Leave Timer** – в случае, когда коммутатор получает сообщение об исключении порта из VLAN (Leave message) от другого подписчика GVRP, он ожидает заданный период времени (от 100 до 100 000 мс), определяемый таймером Leave Timer, чтобы убедиться, что информация о данной VLAN больше не существует в сети. Обычно, значение таймера Leave Timer устанавливают в два раза больше значения таймера Join Timer. По умолчанию значение таймера равно 600 мс.

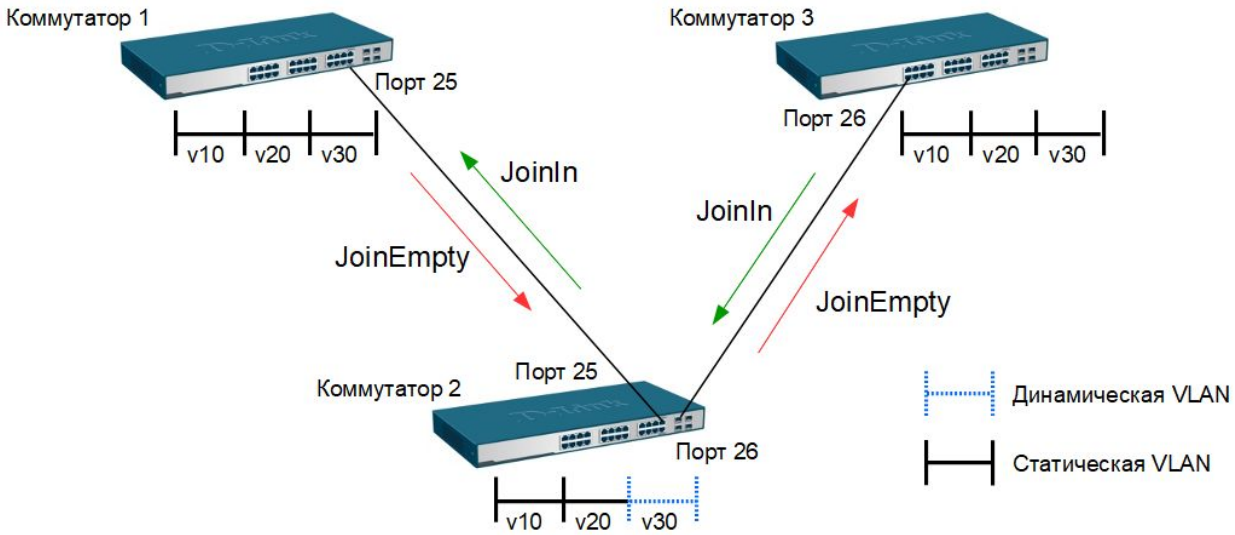
# Протокол GVRP

## Таймеры GVRP

**LeaveAll Timer** – интервал времени (от 100 до 100 000 мс), 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 10 000 мс.

# Протокол GVRP

## Процесс распространения информации о регистрации VLAN по сети



# Протокол GVRP

## Процесс распространения информации о регистрации VLAN по сети

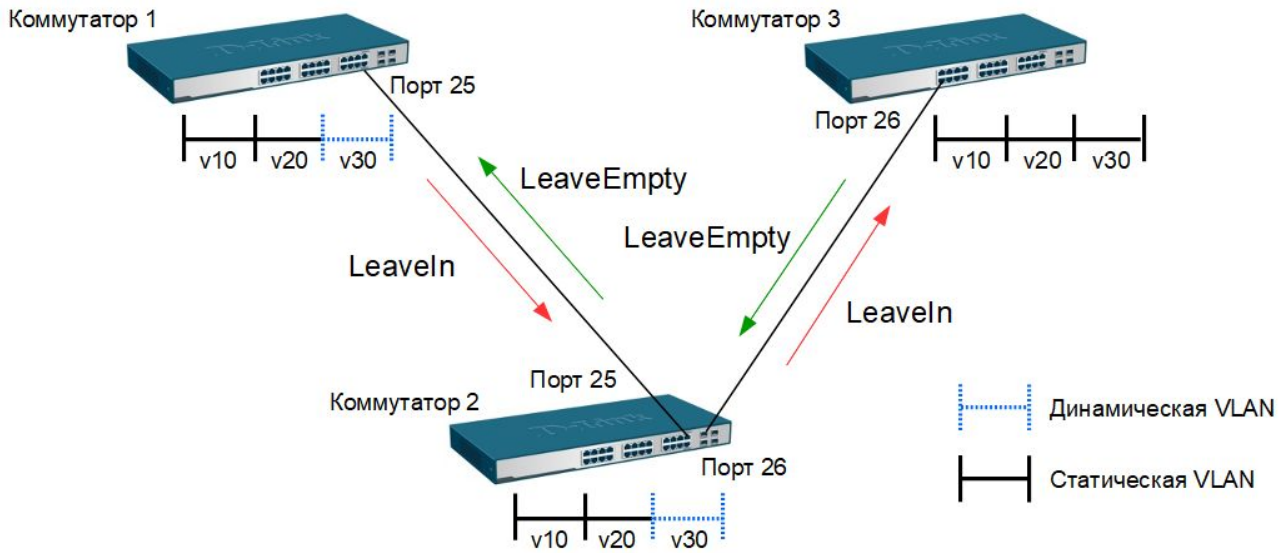
Сообщение JoinEmpty

| | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | D-LinkIn_4e:35:aa | Spanning-tree-(for-bridges)_21 | GVRP | 60 | GVRP |
| 2 | 0.201475 | D-LinkIn_4e:35:aa | Spanning-tree-(for-bridges)_21 | GVRP | 60 | GVRP |

```
Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{2E6C5C36-F74C-4153-B8F2-785EB90EE867}, id 0
IEEE 802.3 Ethernet
Logical-Link Control
GARP VLAN Registration Protocol
   Protocol Identifier: 0x0001 (GARP VLAN Registration Protocol)
 Message 1
      Type: VID (0x01)
 Attribute 1
         Length: 4
         Event: Join Empty (1)
         Value: 30
      End of Mark
   End of Mark
```

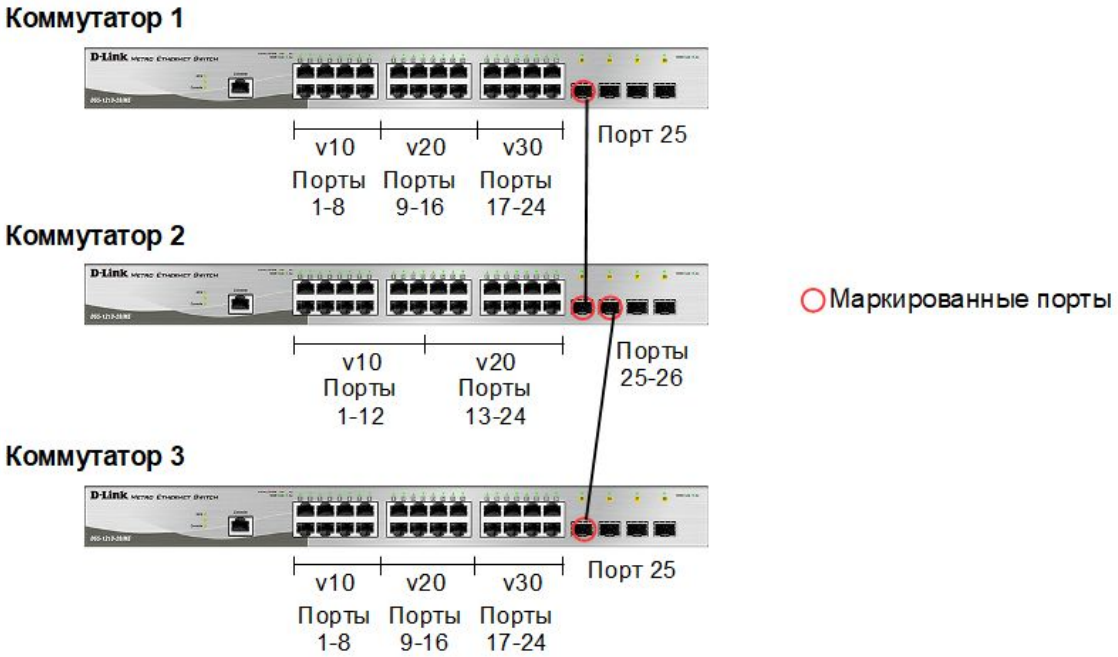
# Протокол GVRP

## Процесс распространения информации об удалении VLAN по сети



# Протокол GVRP

## Настройка протокола GVRP



# Протокол GVRP

**Настройка коммутаторов 1, 3**

1. 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
```

# Протокол GVRP

**2**. 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 tagged 25-26
config vlan v20 add tagged 25-26
```

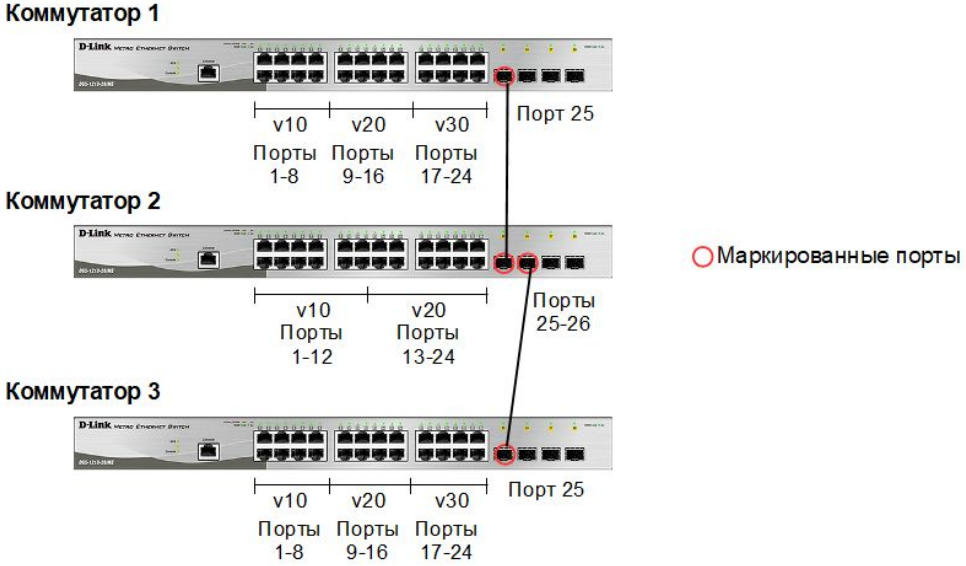
**3**. Активировать протокол GVRP и функцию оповещения о соответствующей VLAN (в данном примере VLAN v30) по сети:

```
config vlan v30 advertisement enable
enable gvrp
config gvrp 25-26 state enable
```

# Протокол GVRP

## 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 gvrp 25-26 state enable
```



# Протокол GVRP

## Настройка протокола GVRP

Посмотреть выполненные настройки можно с помощью команды show gvrp.

# Q-in-Q VLAN

- Функция **Q-in-Q** (также известная как Double VLAN, 802.1Q Tunneling, VLAN Tunneling) соответствует стандарту IEEE 802.1ad, который был разработан как расширение стандарта IEEE 802.1Q-1998 и в настоящее время является частью стандарта IEEE 802.1Q-2018.
- Позволяет добавлять в маркированные кадры Ethernet второй тег IEEE 802.1Q.

# Q-in-Q VLAN

Благодаря функции Q-in-Q провайдеры могут использовать их собственные уникальные идентификаторы VLAN (называемые **Service Provider VLAN ID** или **SP-VLAN ID**) при оказании услуг пользователям, в сетях которых настроено несколько VLAN.

Это позволяет сохранить используемые пользователями идентификаторы VLAN (**Customer VLAN ID** или **C-VLAN ID**), избежать их совпадения и изолировать трафик разных клиентов во внутренней сети провайдера.

# Q-in-Q VLAN

## Формат кадра Q-in-Q

**Обычный (немаркированный) кадр**

| Адрес назначения (DA) | Адрес источника (SA) | Длина/тип (Length/Type) | Данные (Data) | Контрольная сумма кадра (CRC) |
|---|---|---|---|---|

**Кадр с одним тегом 802.1Q**

| Адрес назначения (DA) | Адрес источника (SA) | **Тег (Tag)** | Длина/тип (Length/Type) | Данные (Data) | Контрольная сумма кадра (CRC) |
|---|---|---|---|---|---|

**Кадр с двумя тегами 802.1Q**

| Адрес назначения (DA) | Адрес источника (SA) | **Тег (Tag)** | **Тег (Tag)** | Длина/тип (Length/Type) | Данные (Data) | Контрольная сумма кадра (CRC) |
|---|---|---|---|---|---|---|

# Q-in-Q VLAN

**Реализации Q-in-Q**

Существует два способа реализации функции Q-in-Q:

- Port-based Q-in-Q
- Selective Q-in-Q

# Q-in-Q VLAN

**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.

# Q-in-Q VLAN

**Selective Q-in-Q**

Позволяет:

- маркировать кадры внешними тегами с различными идентификаторами SP-VLAN в зависимости от значений внутренних идентификаторов C-VLAN;
- задавать приоритеты обработки кадров внешних SP-VLAN на основе значений приоритетов внутренних пользовательских C-VLAN;
- добавлять к немаркированным пользовательским кадрам помимо внешнего тега SP-VLAN  внутренний тег C-VLAN.

# Q-in-Q VLAN

**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 0x88A8, согласно стандарту IEEE 802.1ad.

# Q-in-Q VLAN

**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*) назначается портам, через которые будет осуществляться взаимодействие граничного коммутатора провайдера с клиентскими сетями.
- *NNI (Network-to-Network Interface)* назначается портам, которые подключаются к внутренней сети провайдера или другим граничным коммутаторам.

# Q-in-Q VLAN

## 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 C-VLAN идентификаторам SP-VLAN (*vlan translation*).

# Q-in-Q VLAN

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

- ✔ На коммутаторах D-Link с поддержкой функции Q-in-Q, можно активировать режим **Missdrop**, позволяющий 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.

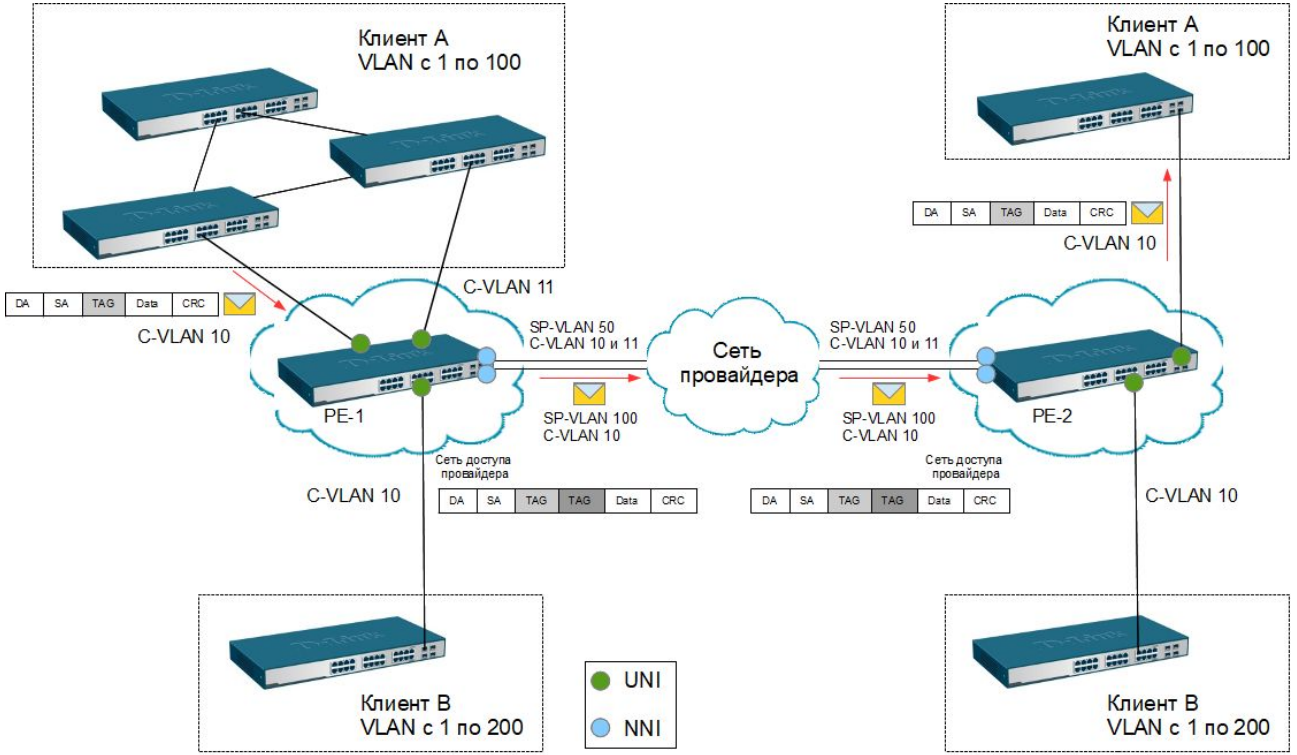
# Q-in-Q VLAN

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

- ✔ Значение приоритета внешнего тега по умолчанию равно значению приоритета внутреннего тега, если кадр является маркированным, или не сделаны соответствующие настройки.
- ✔ Если приоритет в полученном кадре отсутствует, то в качестве приоритета вешнего тега будет использоваться приоритет соответствующего входного порта UNI.

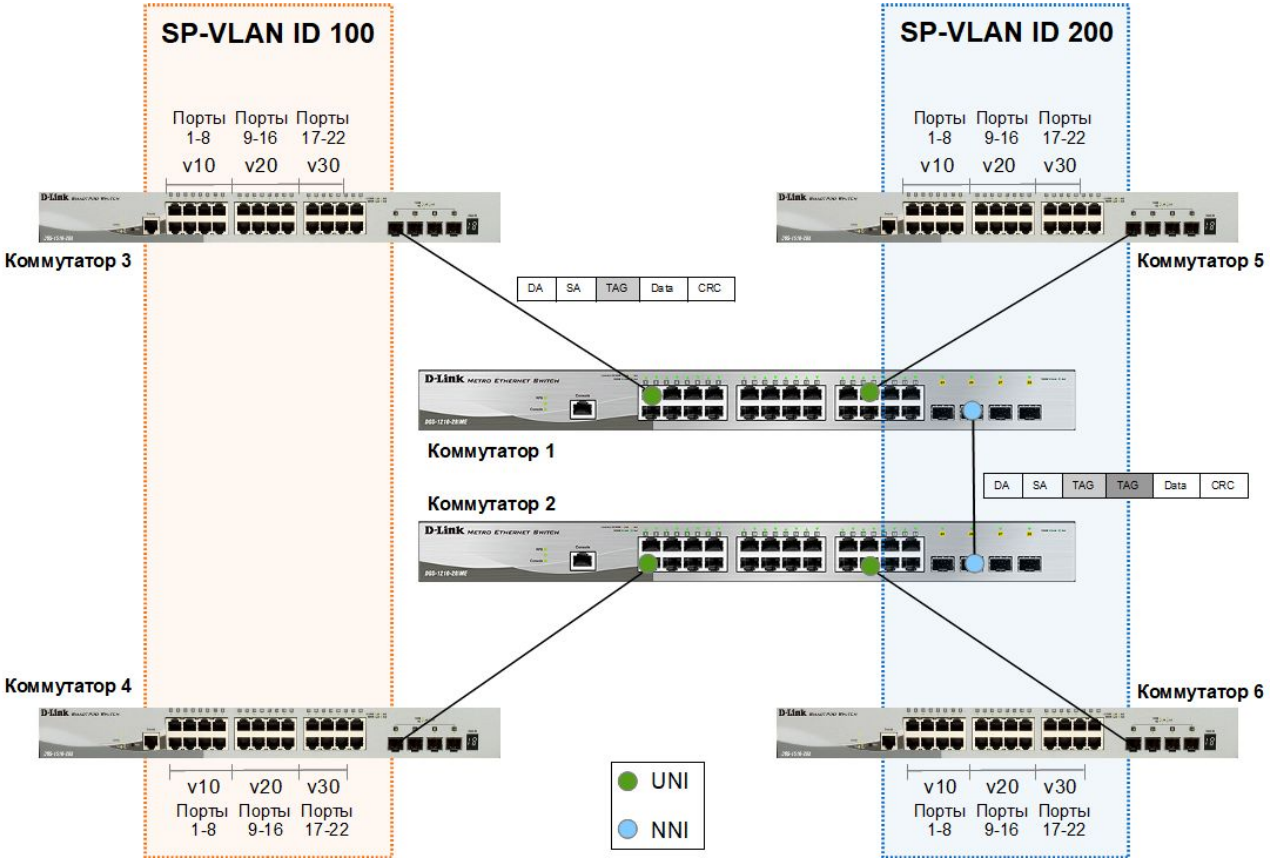
# Q-in-Q VLAN

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



# Q-in-Q VLAN

## Настройка функции Port-based Q-in-Q



# Q-in-Q VLAN

**Настройка коммутаторов 1 и 2**

**1**. Активировать функцию Q-in-Q VLAN на коммутаторе:

```
enable qinq
```

**2**. 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
```

# Q-in-Q VLAN

**3**. Назначить порты доступа в созданных Q-in-Q VLAN:

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

**4.** Назначить Uplink-порты в созданных Q-in-Q VLAN:

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

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

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

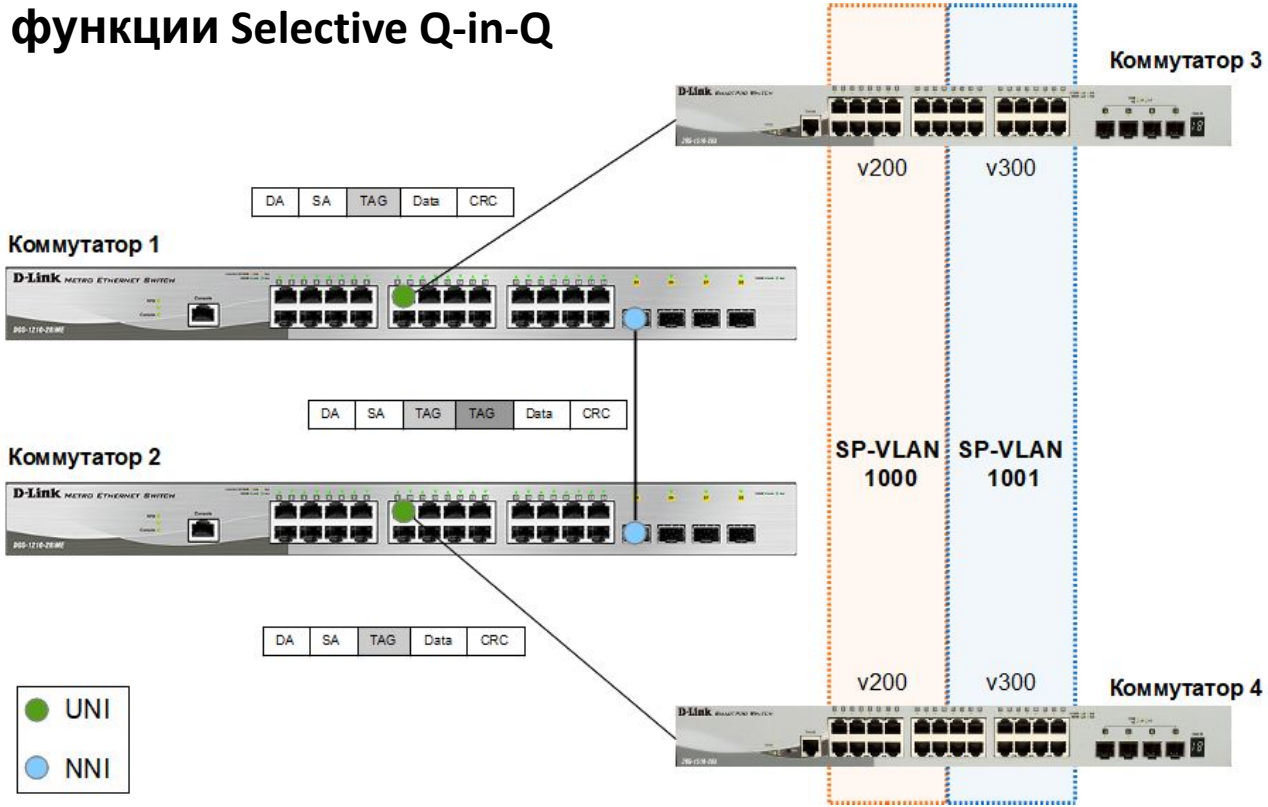
# Q-in-Q VLAN

## Настройка коммутаторов 3, 4, 5, 6

```
config vlan default delete 1-26
create vlan v10 tag 10
create vlan v20 tag 20
create vlan v30 tag 30
config vlan v10 add untagged 1-8
config vlan v10 add tagged 25-26
config vlan v20 add untagged 9-16
config vlan v20 add tagged 25-26
config vlan v30 add untagged 17-22
config vlan v30 add tagged 25-26
```

# Q-in-Q VLAN

## Настройка функции Selective Q-in-Q



# Q-in-Q VLAN

**Настройка коммутаторов 1, 2**

1. 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 9,25
config vlan v1001 add tag 9,25
```

# Q-in-Q VLAN

**2**. Активировать 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 9 role uni
create vlan_translation ports 9 add cvid 200 svid 1000
create vlan_translation ports 9 add cvid 300 svid 1001
```

# Функция Traffic Segmentation

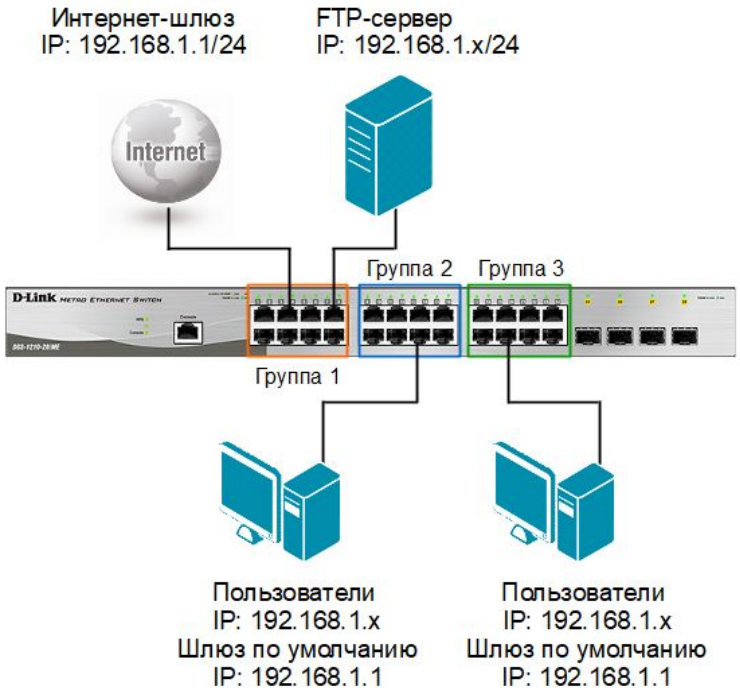
- Функция **Traffic Segmentation** (сегментация трафика) служит для разграничения трафика на канальном уровне.
- Она позволяет настраивать порты или группы портов коммутатора таким образом, чтобы они были полностью изолированы друг от друга, но в то же время имели доступ к разделяемым портам, используемым для подключения серверов или магистрали сети.

# Функция Traffic Segmentation

- 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.

# Функция Traffic Segmentation

## Пример №1 использования и настройки функции Traffic Segmentation




Группа 1, порты 1-8
Совместно используемые серверы/ Интернет-шлюз

Группа 2, порты 9-16
Пользователи группы 2 (ПК или коммутатор)

Группа 3, порты 17-24
Пользователи группы 3 (ПК или коммутатор)

D-Link
Building Networks for People

# Функция Traffic Segmentation

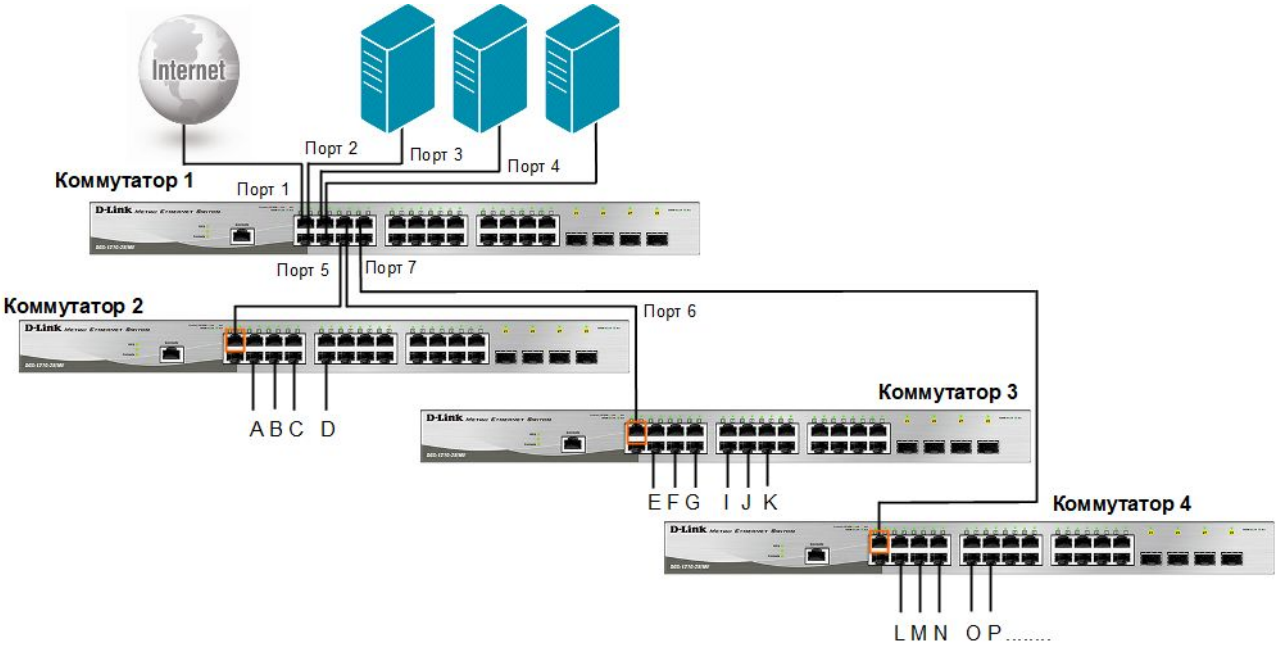
## Пример №1 использования и настройки функции Traffic Segmentation

```
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
```

# Функция Traffic Segmentation

## Пример №2 использования и настройки функции Traffic Segmentation

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



# Функция 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
```

# Спасибо за внимание

D-Link
Building Networks for People