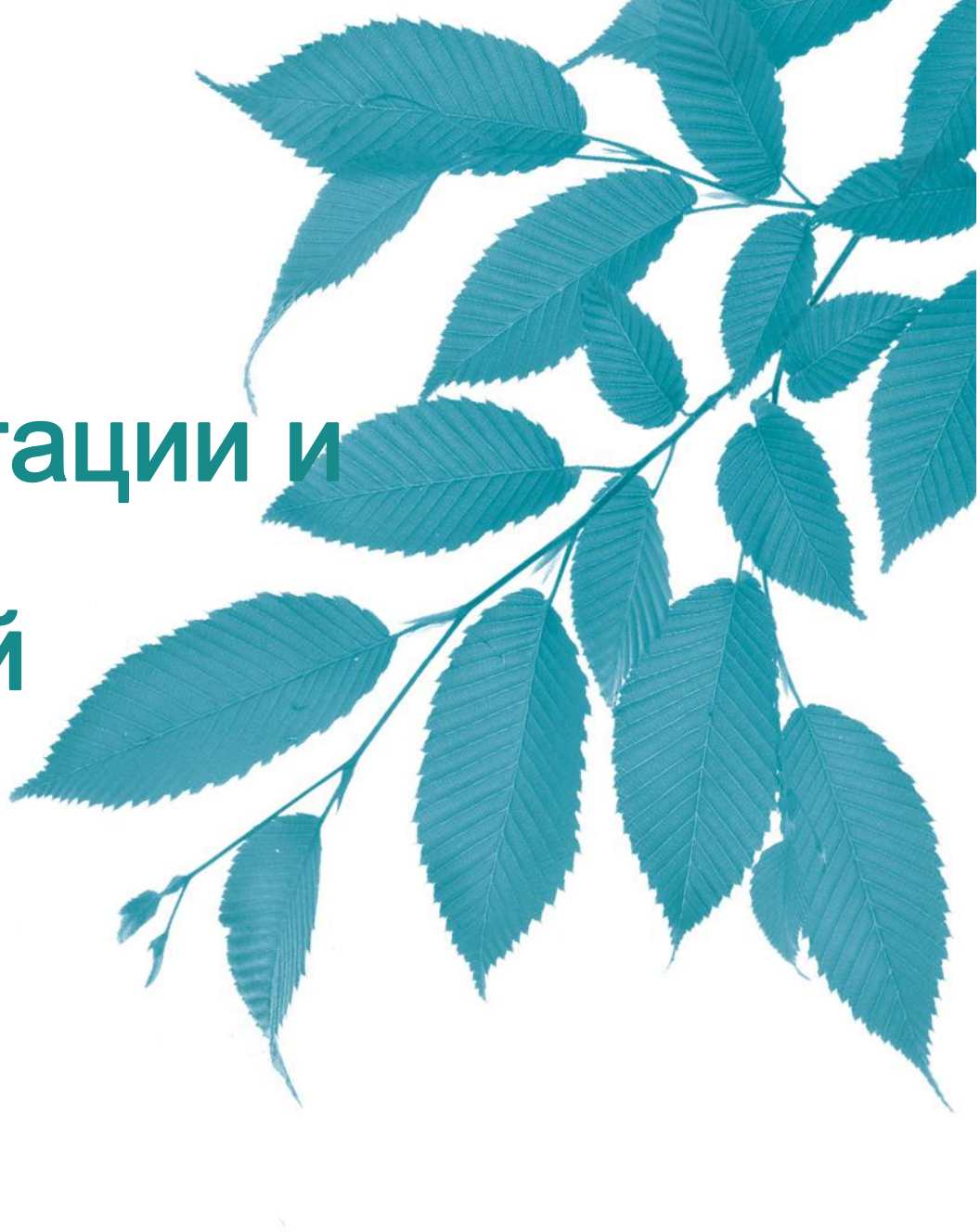


Технологии коммутации и маршрутизации современных сетей Ethernet

Часть 3

Базовый сертификационный курс

Версия 3

D-Link®
Building Networks for People

Сегментация вычислительных сетей

Сегментация вычислительных сетей

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

Обзор VLAN

Понятие виртуальной локальной сети

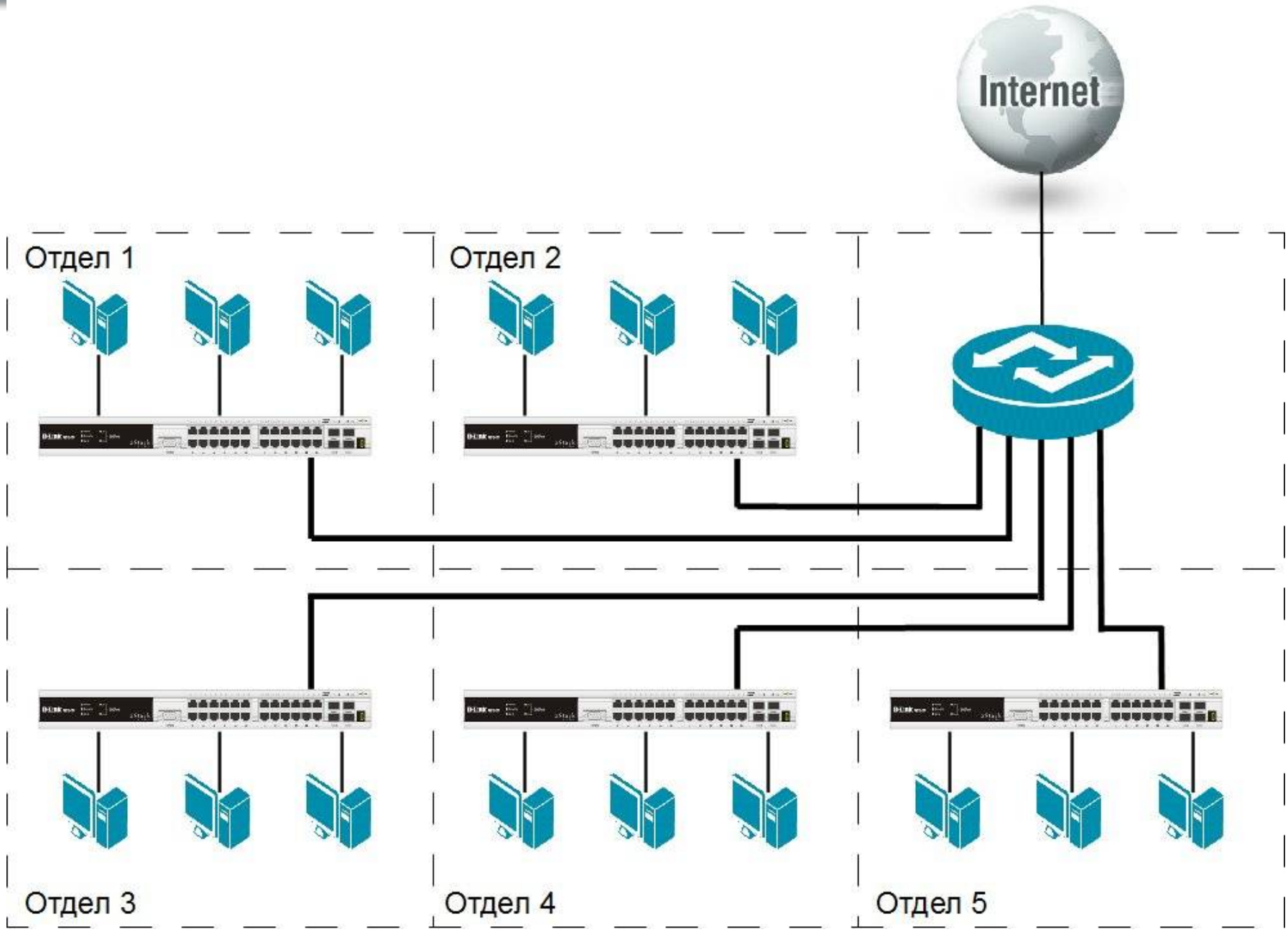
Широковещательный домен

- Логический сегмент сети.
- Любое устройство может передавать данные всем устройствам в сегменте.
- Для отправки кадров всем устройствам, используются широковещательные адреса.

Виртуальная локальная сеть (Virtual Local Area Network, VLAN)

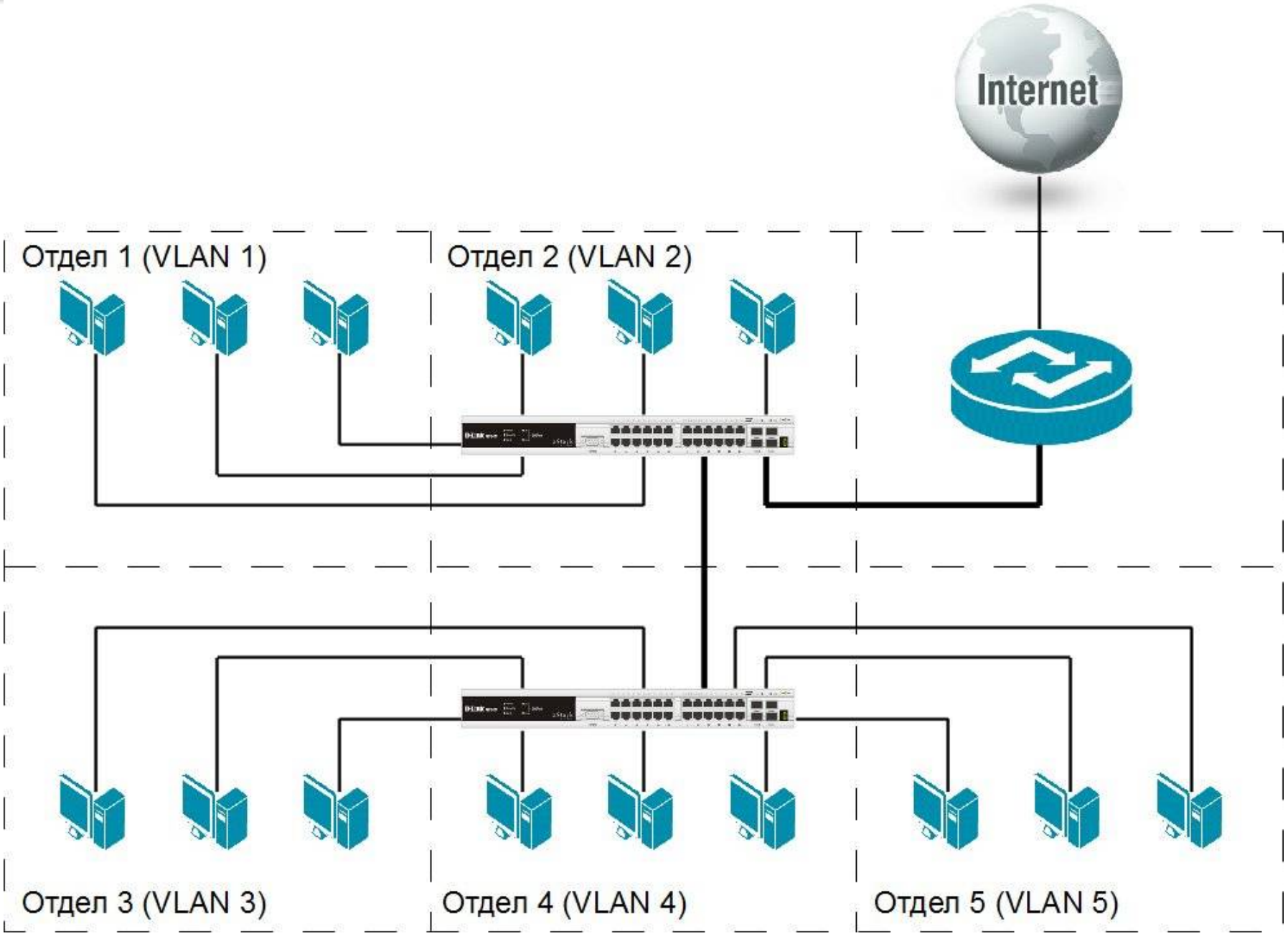
- Логическая группа узлов сети, трафик которой, в том числе и широковещательный, на канальном уровне полностью изолирован от других узлов сети.
- Являются эффективным способом группировки сетевых пользователей в виртуальные рабочие группы, несмотря на их физическое размещение в сети.
- Обеспечивают возможность контроля широковещательных сообщений, что увеличивает полосу пропускания, доступную для пользователя.
- Позволяют повысить безопасность сети.

Обзор VLAN



Физическая сегментация сети

Обзор VLAN



Логическая сегментация сети с помощью VLAN

Типы VLAN

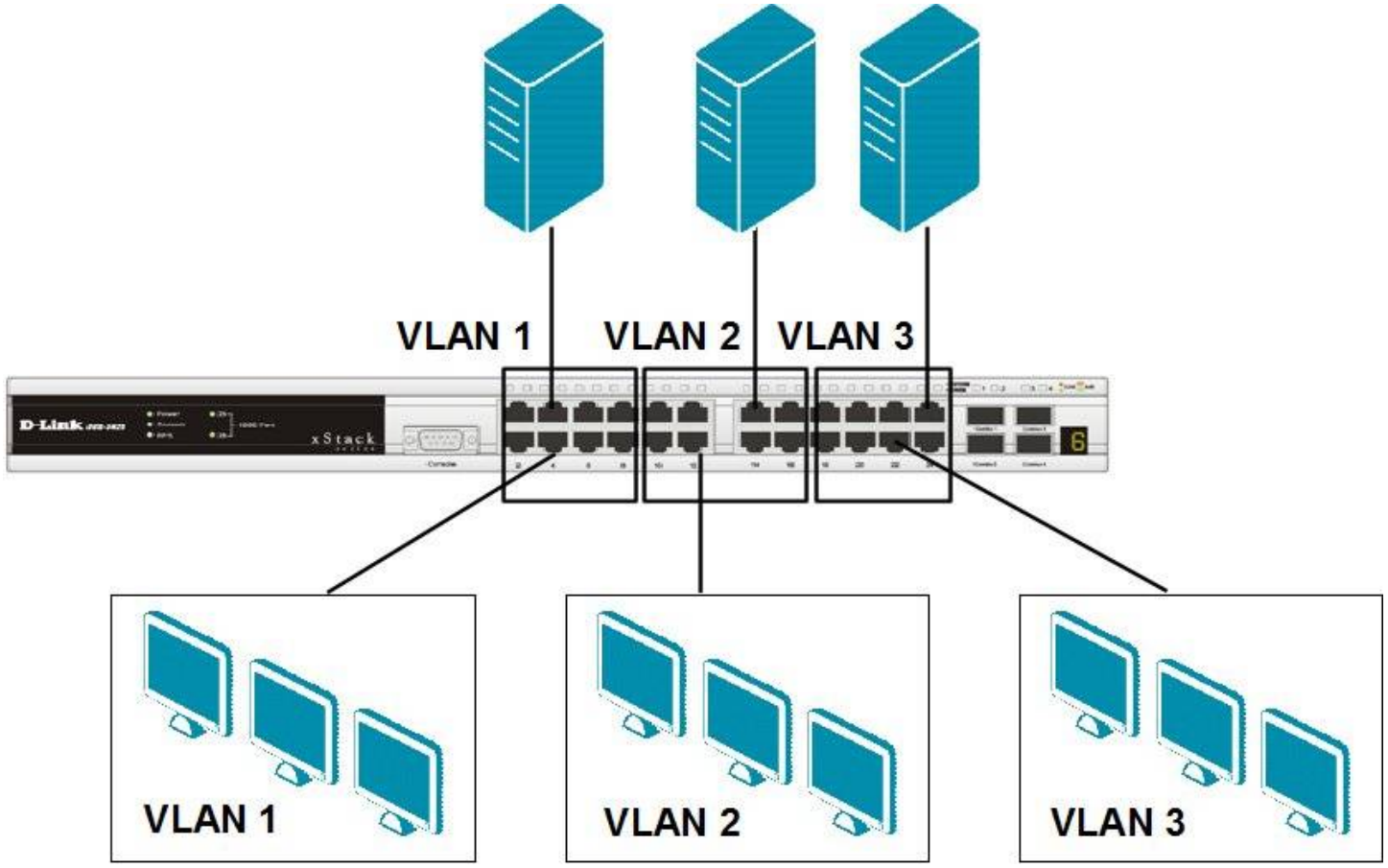
В коммутаторах могут быть реализованы следующие типы VLAN:

- 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.

Также для сегментирования сети на канальном уровне модели OSI в коммутаторах могут использоваться другие функции, например функция *Traffic Segmentation*.

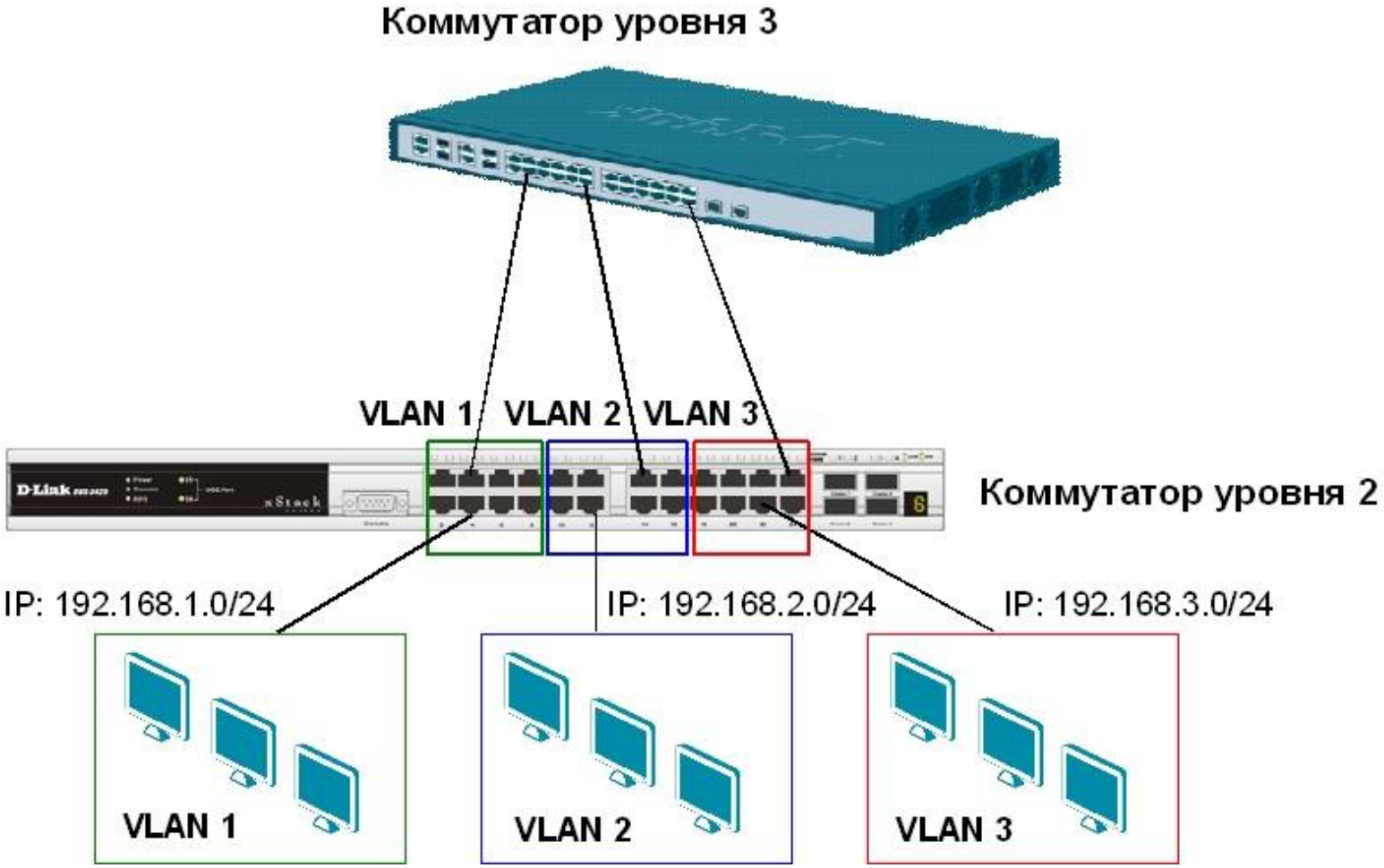
VLAN на основе портов (Port-based VLAN)

- 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.
- Конфигурация портов статическая и может быть изменена только вручную.



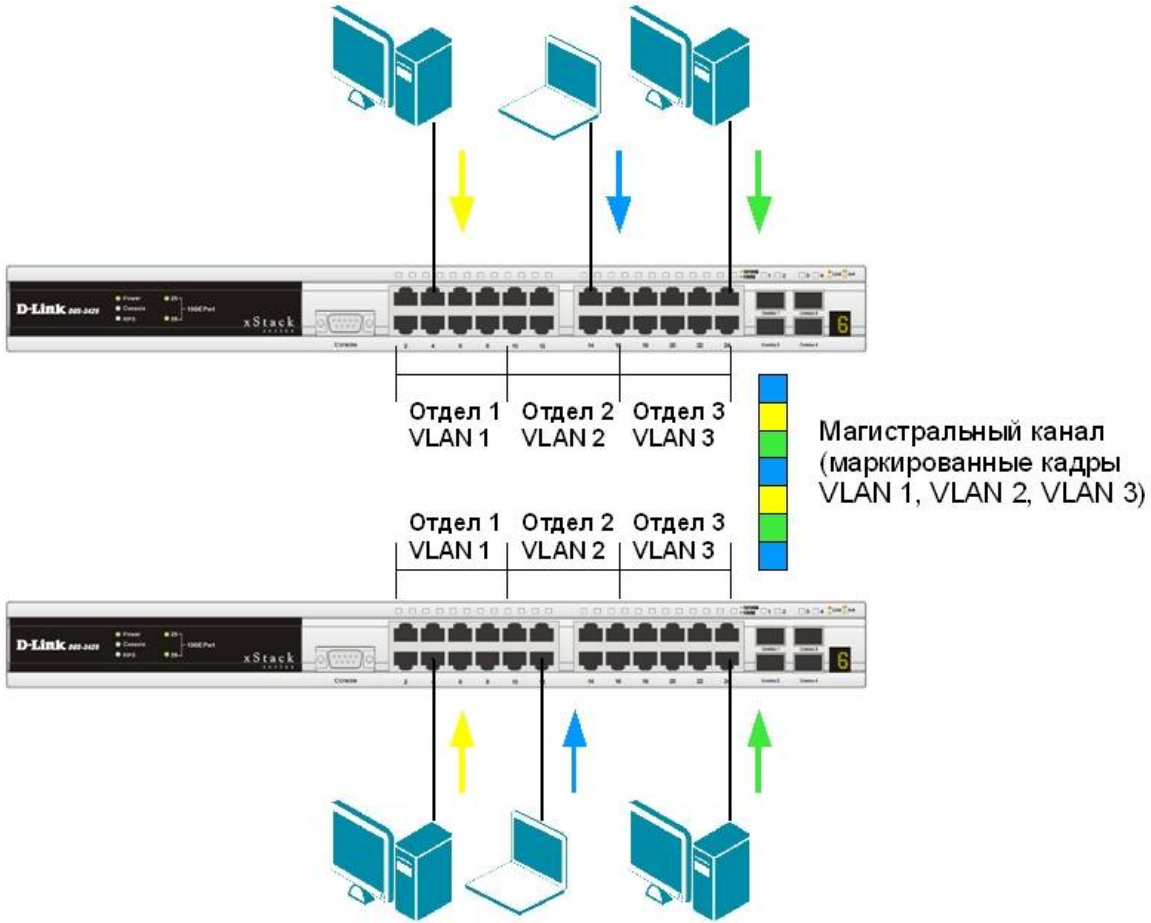
VLAN на основе портов (Port-based VLAN)

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



VLAN на основе стандарта IEEE 802.1Q

- 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.
- Можно создавать необходимые комбинации VLAN как в пределах одного коммутатора, так и между несколькими коммутаторами с поддержкой стандарта IEEE 802.1Q.
- Кадры разных VLAN могут распространяться через множество 802.1Q-совместимых коммутаторов по одному физическому соединению (*магистральному каналу, Trunk Link*).



VLAN на основе стандарта IEEE 802.1Q

Основные 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.

VLAN на основе стандарта IEEE 802.1Q

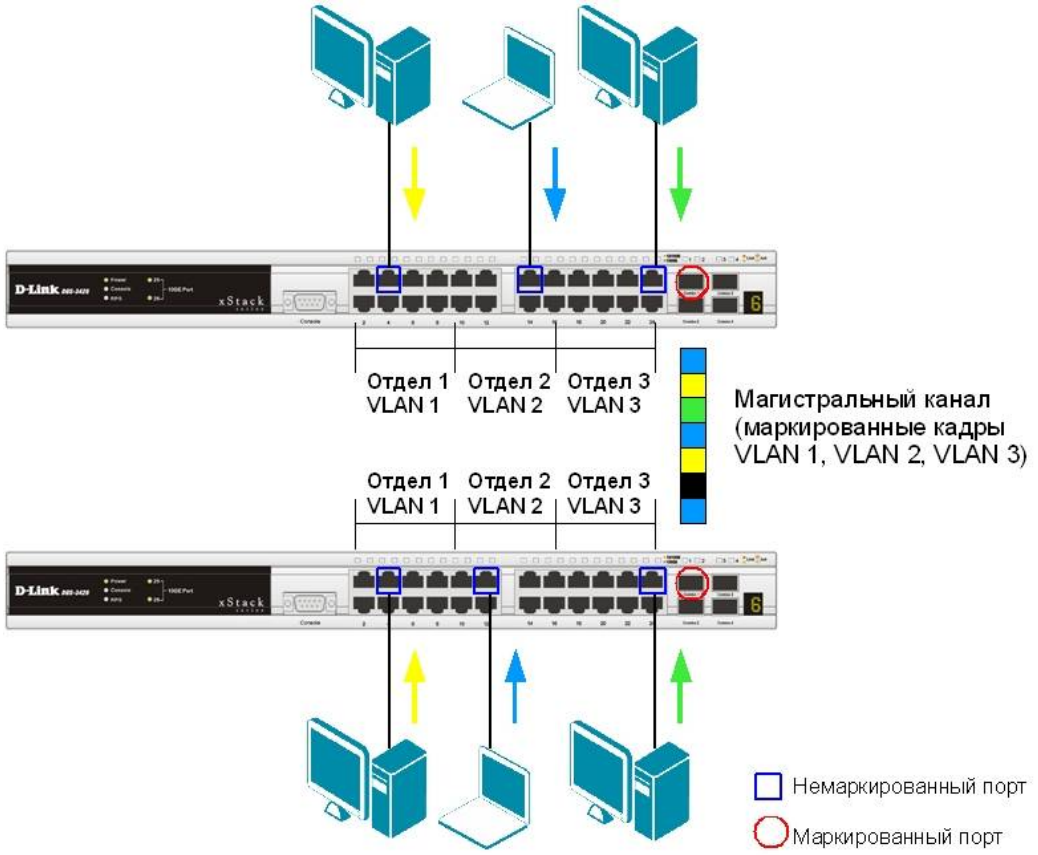
Маркированные и немаркированные порты

Tagged (маркированный) порт:

- сохраняет тег 802.1Q в заголовках всех выходящих через него маркированных кадров и добавляет тег в заголовки всех выходящих через него немаркированных кадров.

Untagged (немаркированный) порт:

- извлекает тег 802.1Q из заголовков всех выходящих через него маркированных кадров;
- обычно используется для подключения конечных устройств.



VLAN на основе стандарта IEEE 802.1Q

Тег VLAN 802.1Q

К кадру Ethernet добавлены 32 бита (4 байта), которые увеличивают его размер до 1522 байт.

VID (VLAN ID):

12-ти битный идентификатор VLAN определяет, какой VLAN принадлежит трафик.

Обычный (немаркированный) кадр

Адрес назначения (DA)	Адрес источника (SA)	Данные (Data)	Контрольная последовательность кадра (CRC)

Маркированный кадр 802.1p/802.1Q

Адрес назначения (DA)	Адрес источника (SA)	**Тег (Tag)**	Данные (Data)	Контрольная последовательность кадра (CRC)

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 параметр, называемый *идентификатор порта VLAN* (*PVID*).
- Идентификатор PVID определяет, в какую VLAN коммутатор направит немаркированный кадр с подключенного к порту сегмента, когда кадр нужно передать на другой порт.
- Всем *немаркированным кадрам* присваивается идентификатор равный *PVID* порта, на который они были приняты.
- Если на коммутаторе не настроены VLAN, то все порты по умолчанию входят в одну VLAN с PVID = 1.

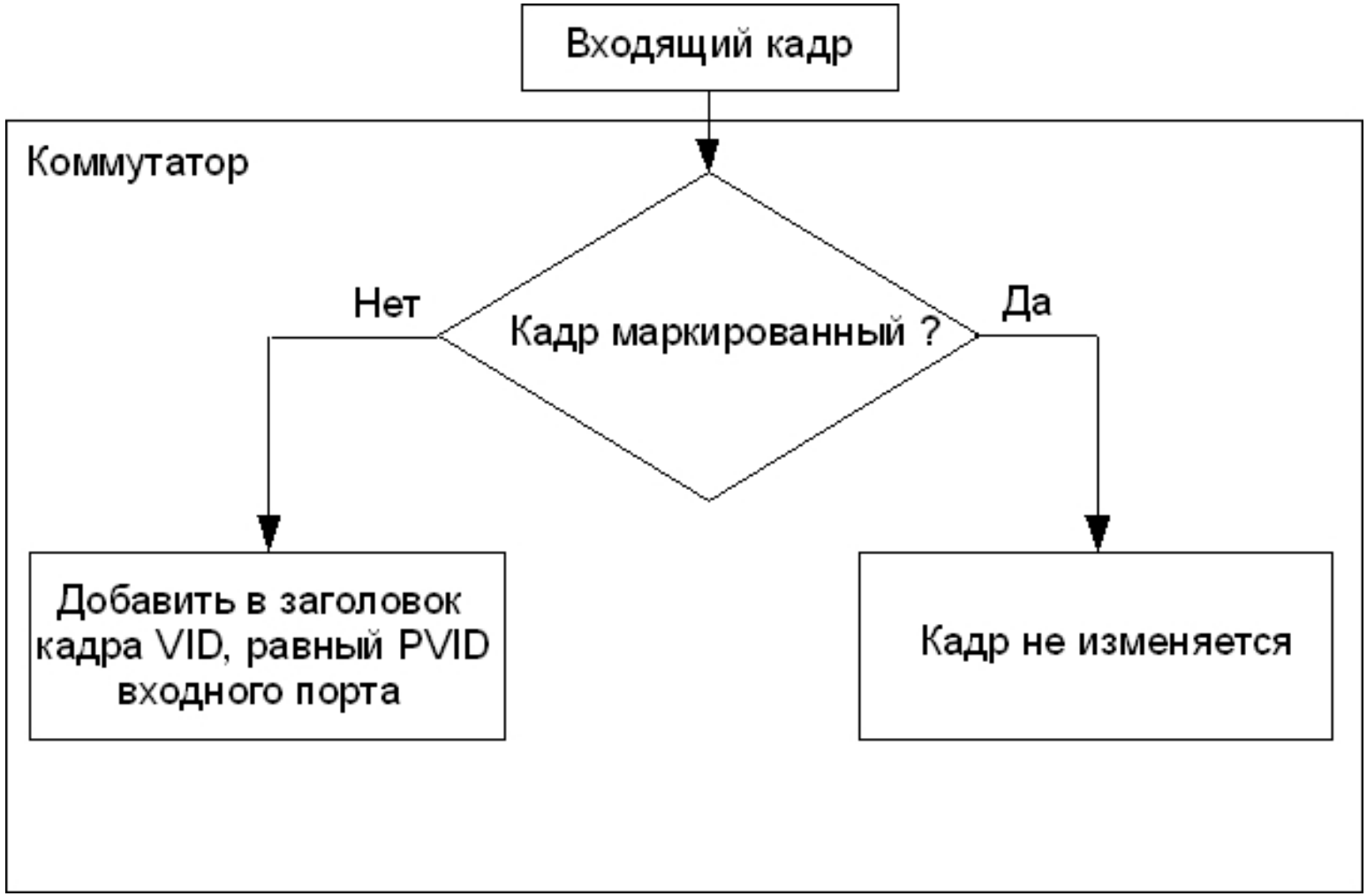
VLAN на основе стандарта IEEE 802.1Q

Продвижение кадров VLAN 802.1Q

- **Правила входящего трафика** (*ingress rules*):
  правила классификации получаемых кадров относительно принадлежности к VLAN.
- **Правила продвижения между портами** (*forwarding rules*): принимается решение о продвижении или отбрасывании кадра.
- **Правила исходящего трафика** (*egress rules*):
  определяется, нужно ли сохранять в заголовке кадра тег 802.1Q перед его передачей или нет.

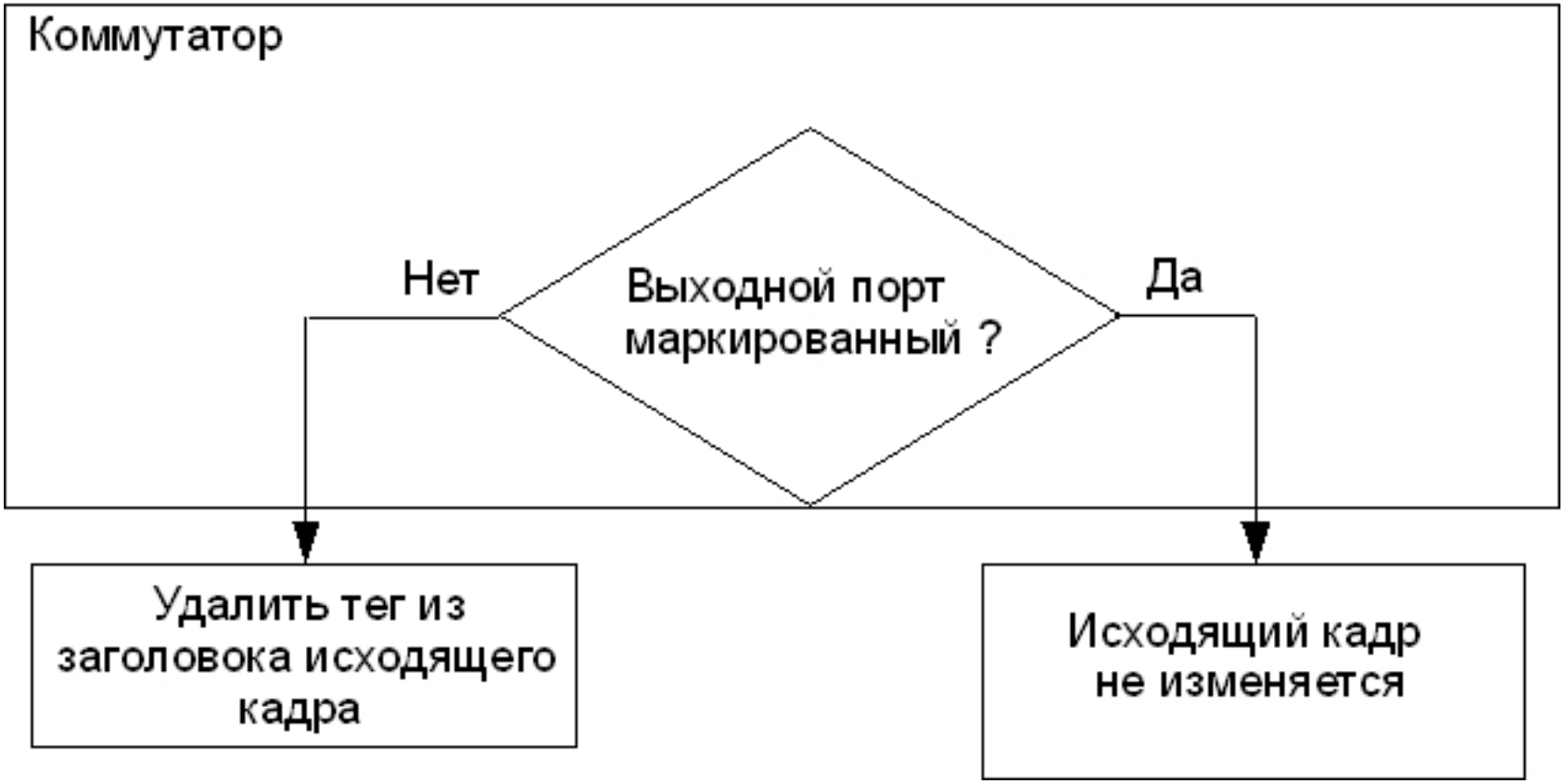
VLAN на основе стандарта IEEE 802.1Q

Правила входящего трафика



VLAN на основе стандарта IEEE 802.1Q

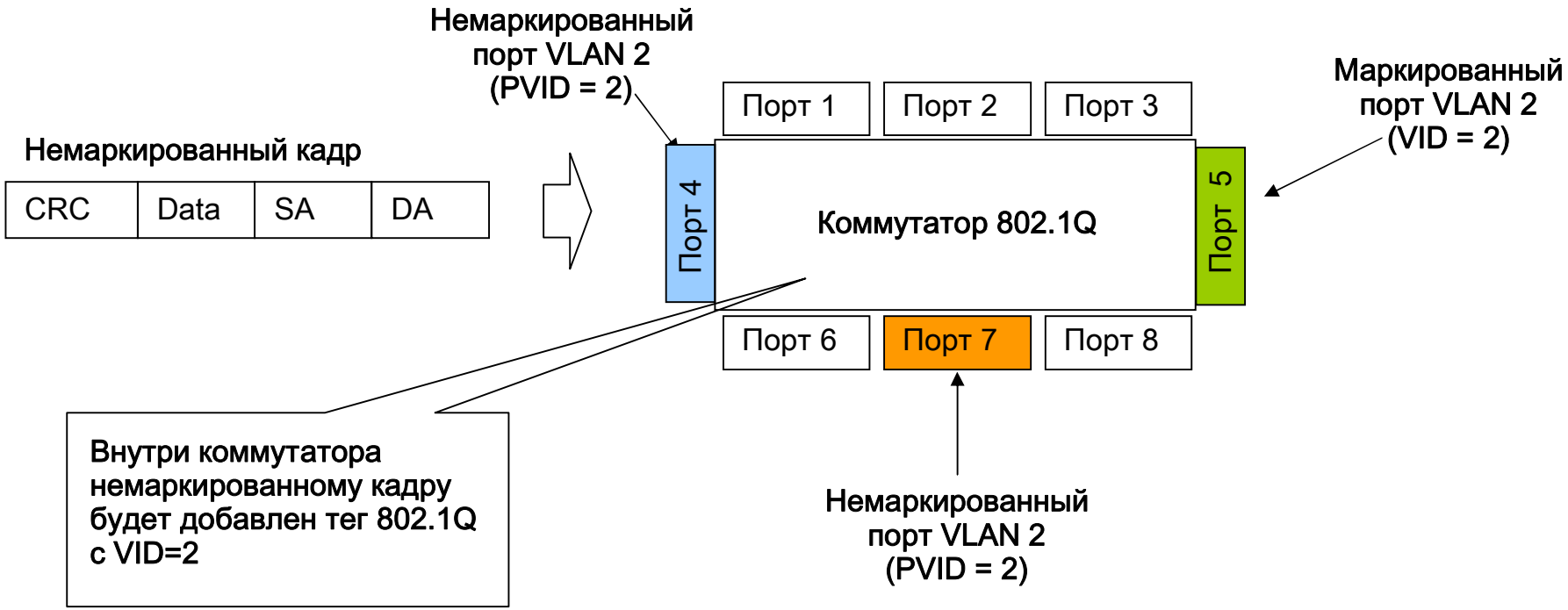
Правила исходящего трафика



VLAN на основе стандарта IEEE 802.1Q

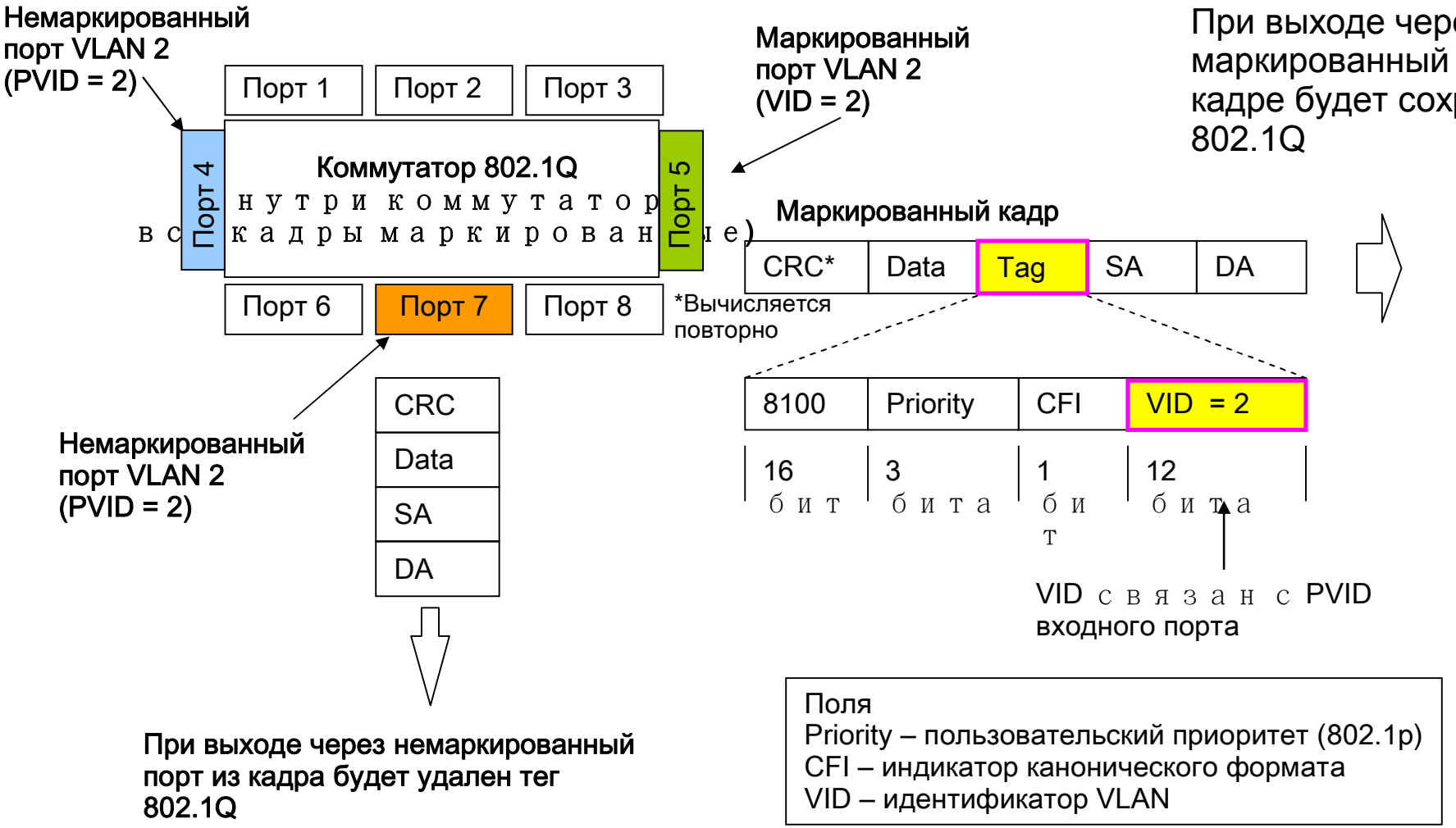
Входящий немаркированный кадр 802.1Q

- Предположим, что PVID порта 4 равен 2.
- Входящему немаркированному кадру будет добавлен тег с VID равным PVID порта 4.
- Порт 5 – маркированный порт VLAN 2.
- Порт 7 – немаркированный порт VLAN 2.
- Полученный кадр передается через порты 5 и 7.



VLAN на основе стандарта IEEE 802.1Q

Передача немаркированного кадра через маркированный порт и немаркированный порты

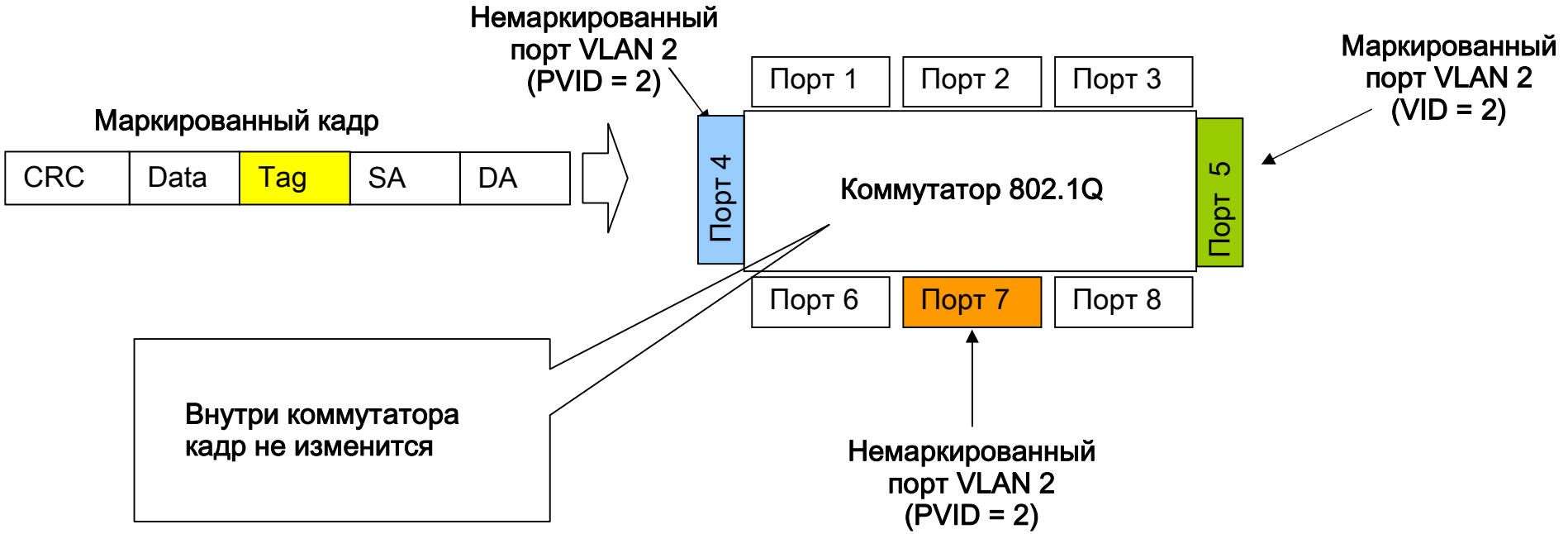


Поля
Priority – пользовательский приоритет (802.1p)
CFI – индикатор канонического формата
VID – идентификатор VLAN

VLAN на основе стандарта IEEE 802.1Q

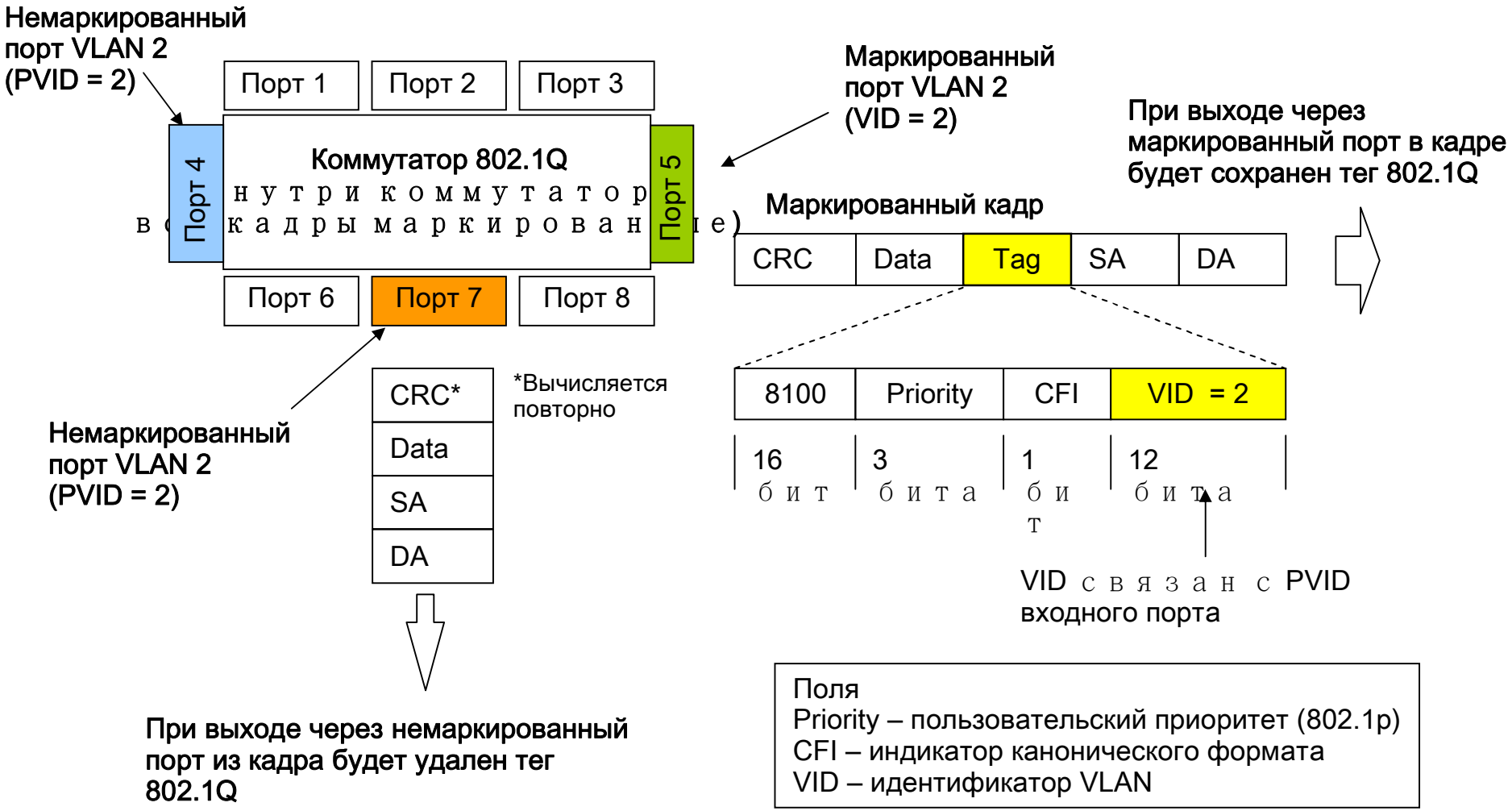
Входящий маркированный кадр 802.1Q

Предположим, что входящий кадр маркированный с VID равным 2.
Порт 5 – маркированный порт VLAN 2.
Порт 7 – немаркированный порт VLAN 2.
Полученный кадр передается через порты 5 и 7.



VLAN на основе стандарта IEEE 802.1Q

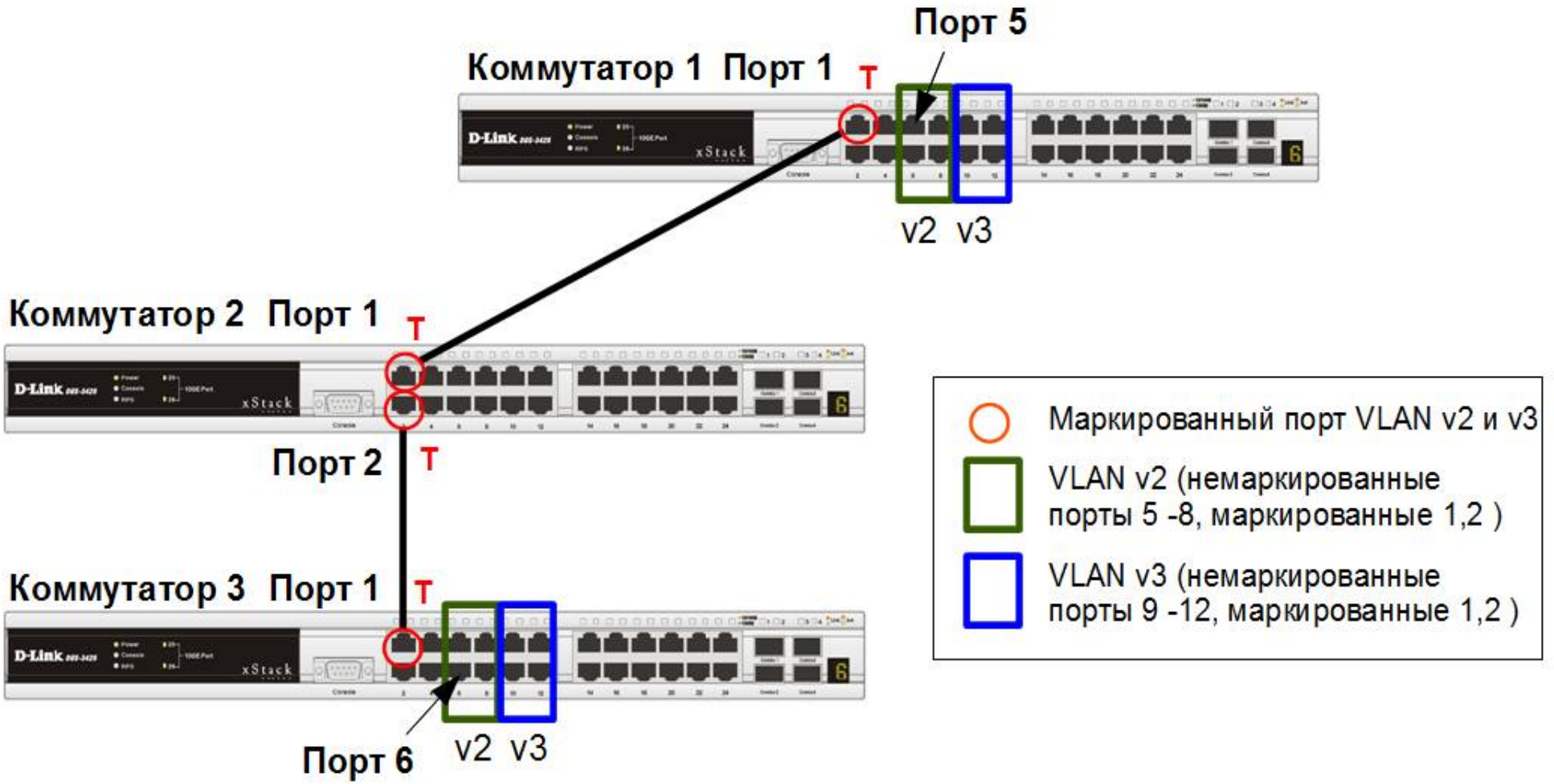
Передача маркированного кадра через маркированный порт и немаркированный порты



Поля
Priority – пользовательский приоритет (802.1p)
CFI – индикатор канонического формата
VID – идентификатор VLAN

VLAN на основе стандарта IEEE 802.1Q

Пример настройки VLAN



VLAN на основе стандарта IEEE 802.1Q

Коммутатор 1

```
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 1-2
config vlan v3 add untagged 9-12
config vlan v3 add tagged 1-2
```

Коммутатор 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
```

Коммутатор 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
```

Порядок настройки:

- Удалить соответствующие порты из VLAN по умолчанию (default VLAN) и создать новые VLAN.
- В созданные VLAN добавить порты и указать, какие из них являются маркированными и немаркированными.

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.**

Статические и динамические VLAN

Существуют два основных способа, позволяющих устанавливать членство в VLAN:

- статические VLAN;
- динамические VLAN.

➢ **Статические VLAN**:

членство устанавливается вручную.

➢ **Динамические VLAN**:

членство устанавливается динамически на основе протокола GVRP (GARP VLAN Registration Protocol) или с помощью процедур, описанных в специальных стандартах, например IEEE 802.1X.

Записи о регистрации в VLAN:

статические, динамические или статические + динамические.

Регистрация VLAN

Статические записи о регистрации VLAN (*Static VLAN Registration Entries*):

- позволяют задавать точные настройки для каждого порта VLAN;
- тип порта (маркированный или немаркированный);
- типы регистрации VLAN:
  - Fixed (порт всегда является членом данной VLAN);
  - Forbidden (порту запрещено регистрироваться как члену данной VLAN);
  - None (обычная регистрация с помощью протокола GVRP).

Динамические записи о регистрации 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.

VLAN на основе портов и протоколов – стандарт IEEE 802.1v

- Стандарт IEEE 802.1v является расширением стандарта IEEE 802.1Q.
- Он позволяет объединять узлы сети в виртуальные локальные сети на основе поддерживаемых ими протоколов.
- При определении членства в VLAN стандарт классифицирует *немаркированные* кадры по типу протокола и порту.
- Формат тега 802.1v аналогичен формату тега 802.1Q.

VLAN на основе портов и протоколов – стандарт IEEE 802.1v

Правила классификации входящих кадров

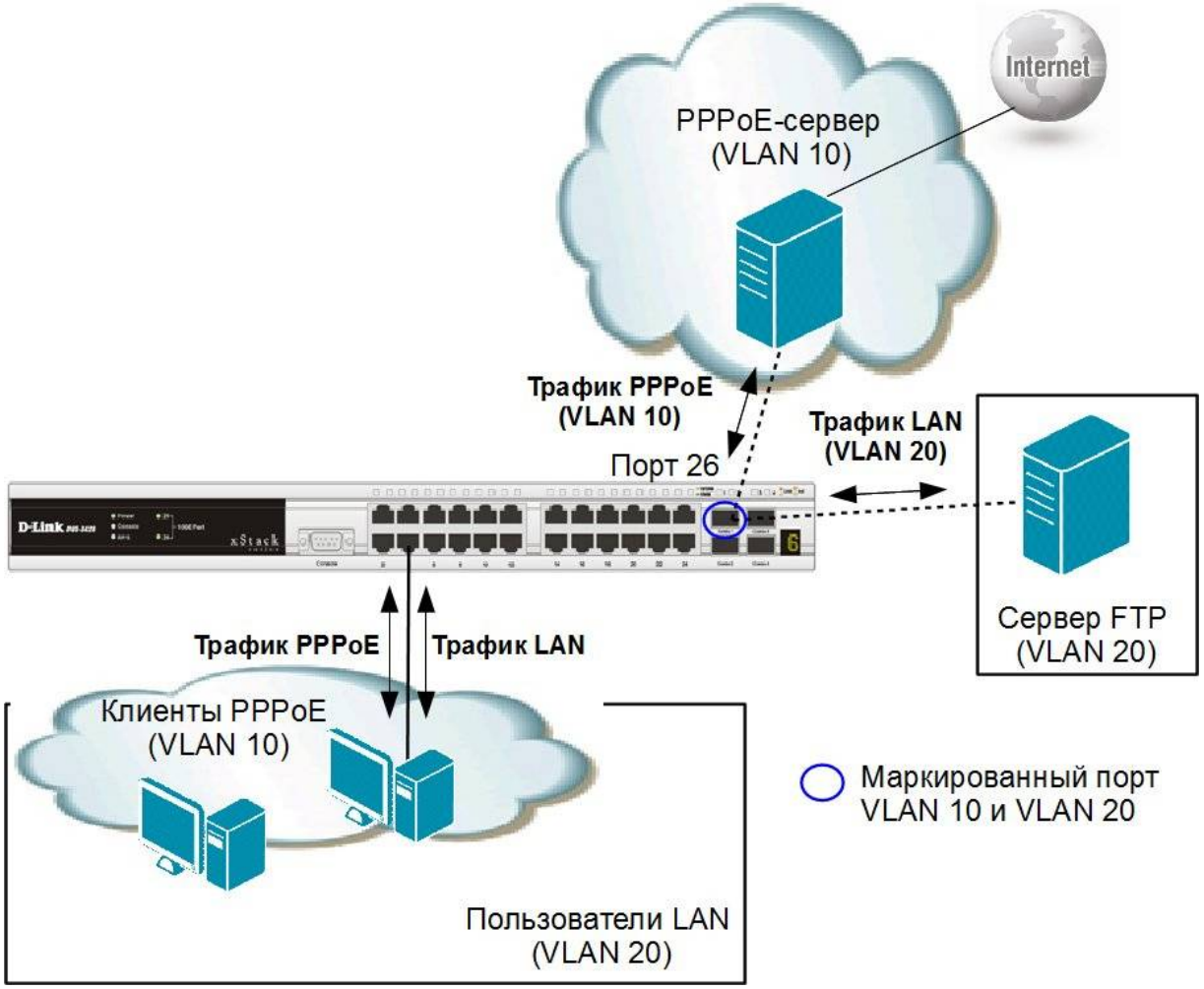
VLAN на основе портов и протоколов – стандарт IEEE 802.1v

- 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.

VLAN на основе портов и протоколов – стандарт IEEE 802.1v

Пример настройки IEEE 802.1v VLAN

Пользователи локальной сети 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.



VLAN на основе портов и протоколов – стандарт IEEE 802.1v

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
```

VLAN на основе портов и протоколов – стандарт IEEE 802.1v

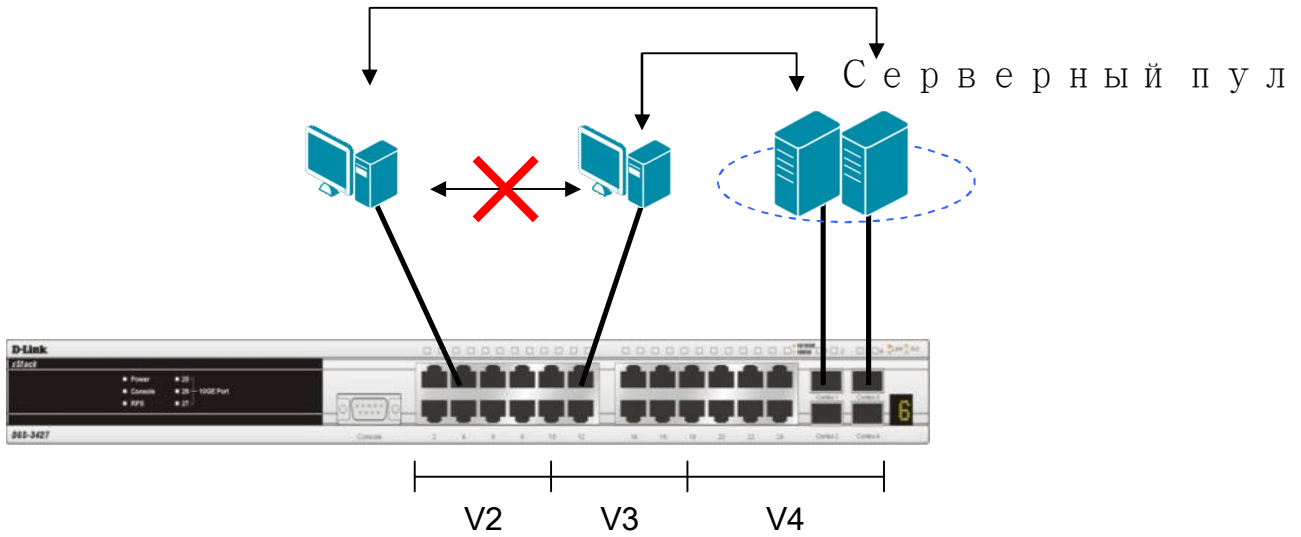
Продолжение настройки коммутатора

- 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
```

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* (асимметричные VLAN).
- Эта функция позволяет клиентам из разных VLAN взаимодействовать с разделяемыми устройствами (например, серверами), *не поддерживающим* 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.



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.

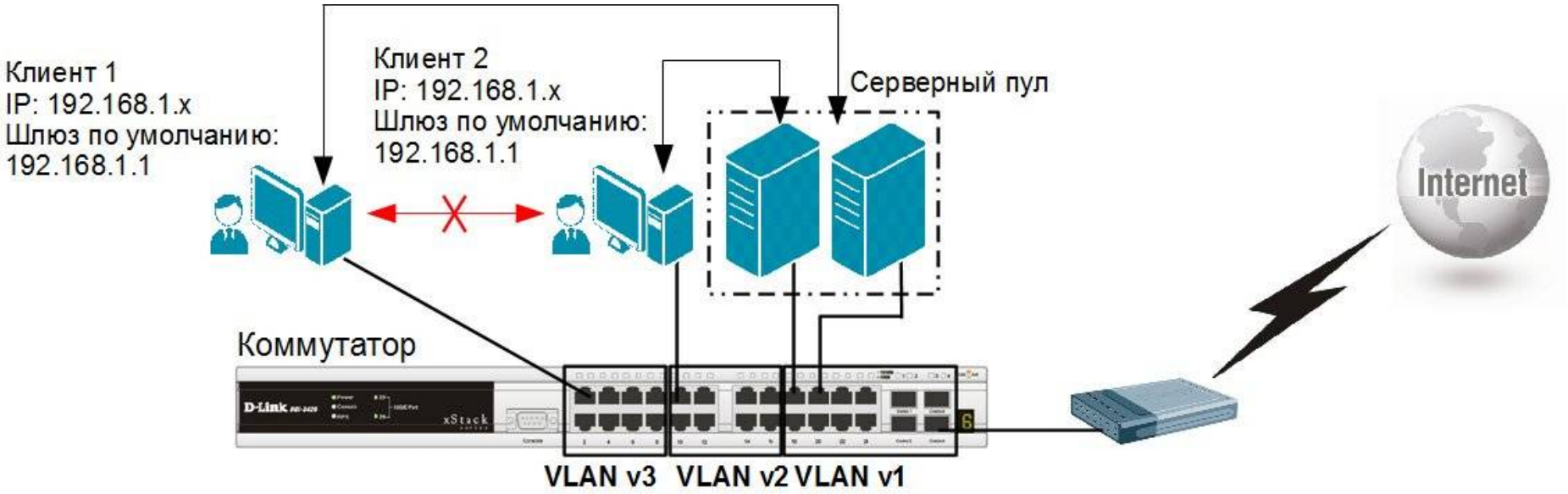
- При использовании асимметричных VLAN существует следующее ограничение: **не функционирует механизм IGMP Snooping**.

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.

Асимметричные VLAN

Настройка асимметричных VLAN

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	-	-	-

Асимметричные VLAN

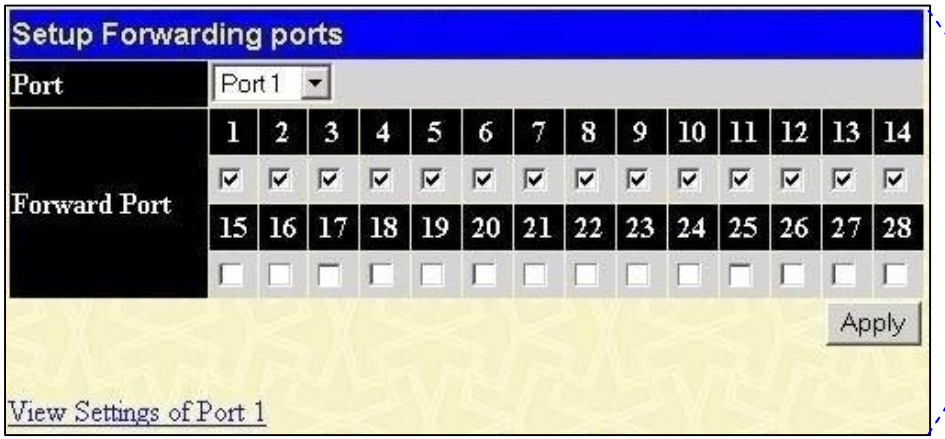
Настройка коммутатора

```
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
```

Сегментация трафика

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.

Следующая конфигурация позволяет клиенту, подключенному к порту 1, отправлять/получать трафик от клиентов, подключенных к портам 1-14



Коммутатор проверяет порт-источник и порт назначения

Порт-источник: 1 → Порт назначения: 10,
Результат: передача трафика через порт назначения.
Порт-источник: 1 → Порт назначения: 24,
Результат: передача трафика запрещена.
Порт-источник: 1 → Порт назначения: 24,
Результат: передача трафика запрещена.

Данные успешно переданы!

Слайд анимирован

Сегментация трафика

Преимущества Traffic Segmentation

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

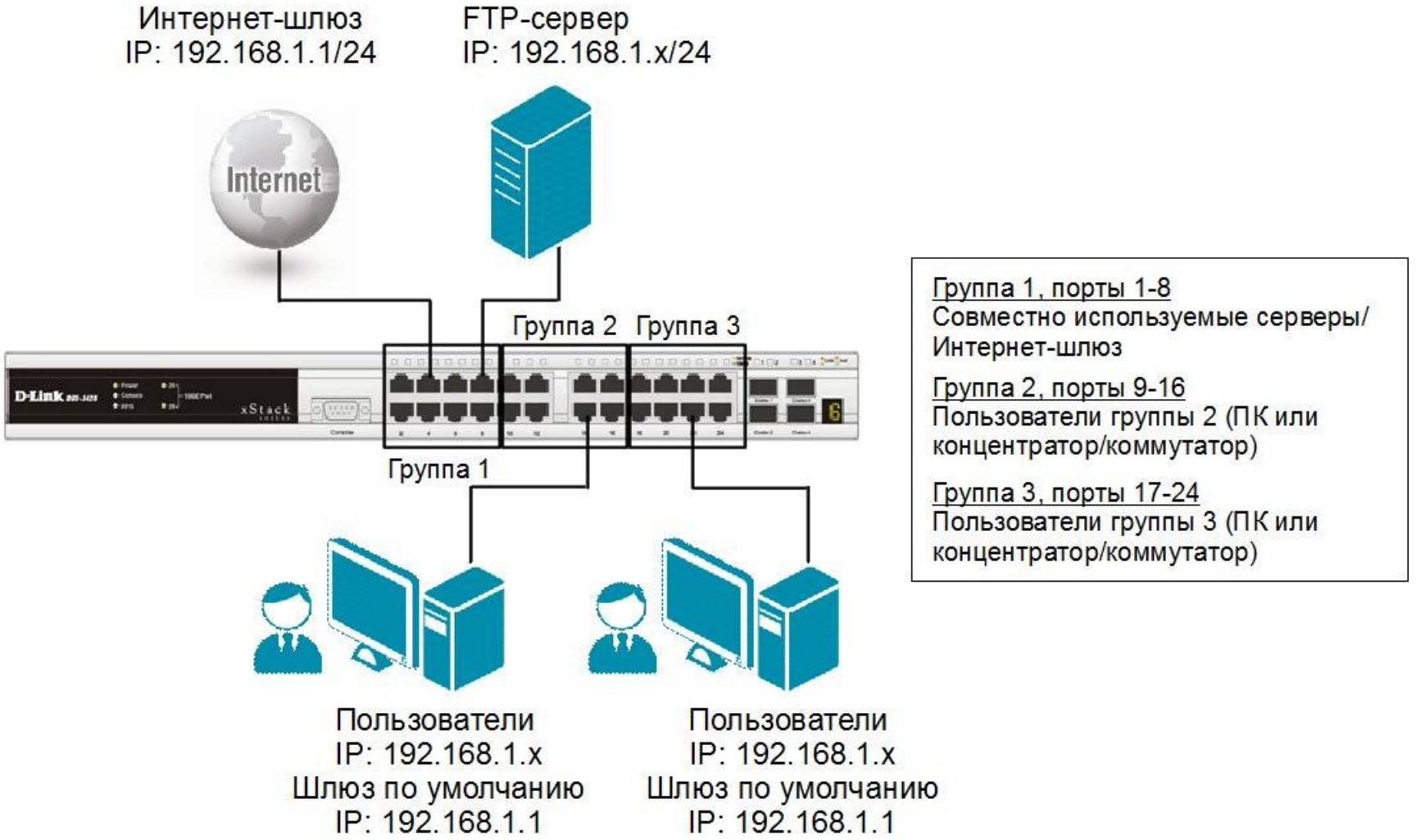
- простота настройки;
- поддерживается работа IGMP Snooping;
- функция Traffic Segmentation может быть представлена в виде иерархического дерева (при иерархическом подходе разделяемые ресурсы должны быть на «вершине» дерева);
- нет ограничений на создание количества групп портов.

❑Функция Traffic Segmentation 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.

Сегментация трафика

Настройка функции Traffic Segmentation. Пример 1

В качестве примера рассмотрим решение задачи совместного использования ресурсов сети разными группами пользователей с использованием функции Traffic Segmentation



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

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

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

Сегментация трафика

Настройка коммутатора

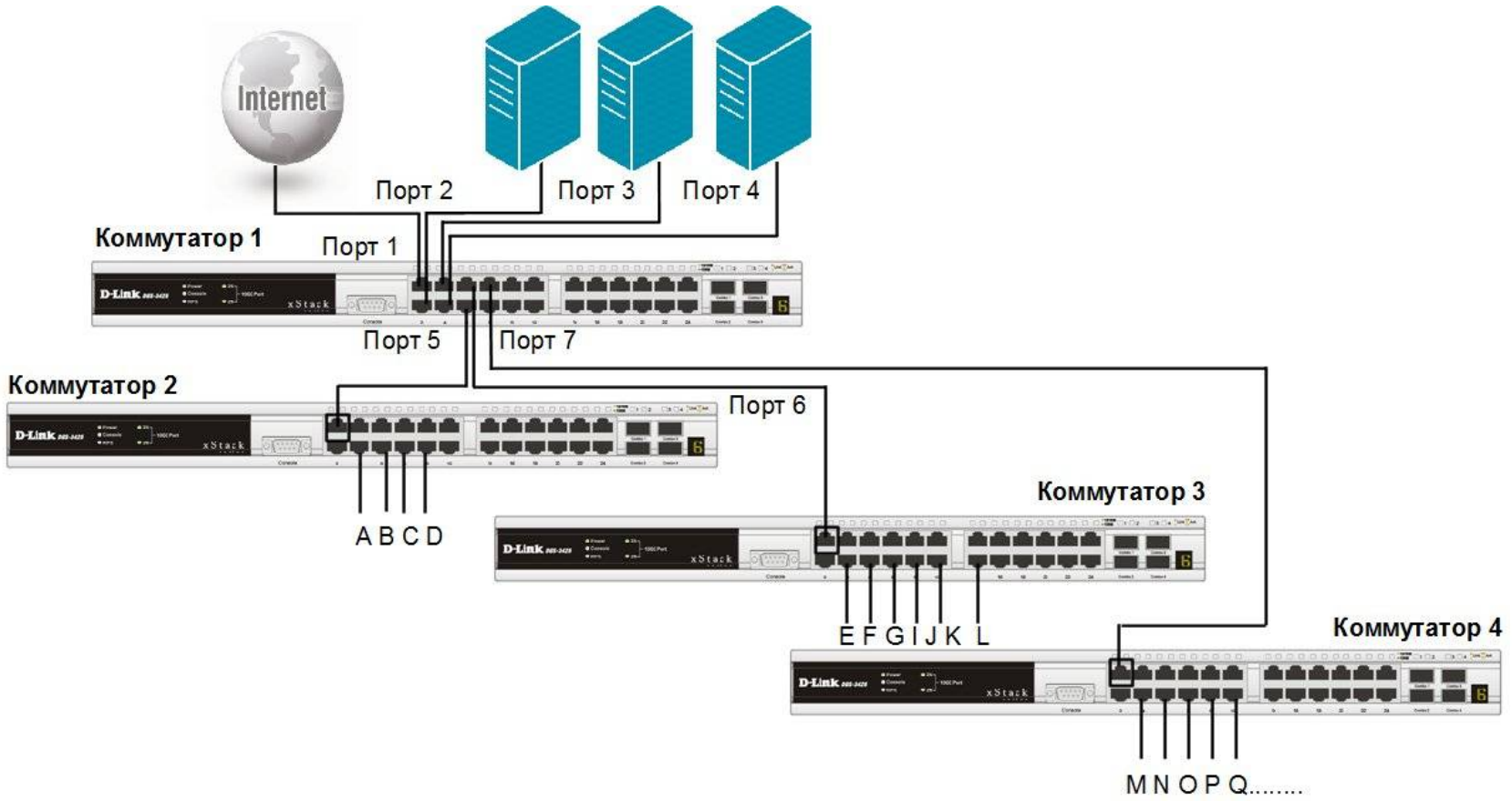
```
config traffic_segmentation 1-8 forward_list 1-24
config traffic_segmentation 9-16 forward_list 1-16
config traffic_segmentation 17-24 forward_list 1-8,17-24
```

Сегментация трафика

Настройка функции Traffic Segmentation. Пример 2

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

В данном примере 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 Интернет. Все коммутаторы сети поддерживают иерархию Traffic Segmentation.



Сегментация трафика

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