Семинар 4

Функции защиты от перегрузок CPU. Функции защиты от петель в сетях Ethernet с помощью управляемых коммутаторов L2

Николаев Андрей

г. Красноярск, 2016

D-Link®
Building Networks for People

Функции защиты процессора коммутатора от перегрузок и нежелательного трафика

Функции защиты ЦПУ коммутатора

В коммутаторах D-Link реализованы функции **Safeguard Engine** и **CPU Interface Filtering**, обеспечивающие защиту ЦПУ от обработки нежелательных пакетов и перегрузок.

Повод для использования:

- возникновение в сети многоадресных или широковещательных штормов, вызванных неправильной настройкой оборудования, петлями или сетевыми атаками,
- Неправильно рассчитанная нагрузка на коммутатор и его порты,
- неконтролируемый администратором «флуд» в сети.

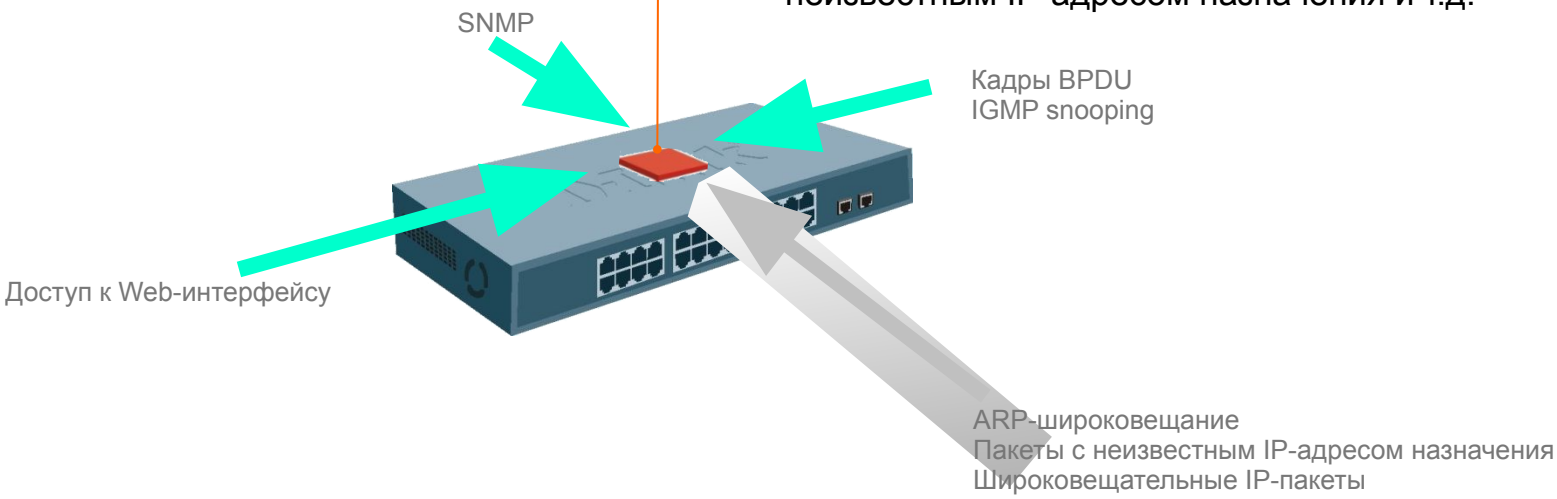
Функция Safeguard Engine

Safeguard Engine - функция для обеспечения возможности снижения загрузки процессора управляемого коммутатора.

ЦПУ коммутатора предназначено для обработки пакетов протоколов STP, SNMP, осуществления доступа к Web-интерфейсу и т.д.

Также для обработки на ЦПУ отправляются некоторые специальные пакеты, такие как широковещательные ARP-пакеты, пакеты с неизвестным IP-адресом назначения и т.д.

ЦПУ испытывает сильную загрузку и не может выполнять такие важные задачи как административный доступ, STP, SNMP и т.д.



Пример настройки функции Safeguard Engine

//Активация функции Safeguard Engine

```
config safeguard_engine state enable
```

//Задание пороговых значений срабатывания и режима работы

```
config safeguard_engine utilization rising 70 falling 50 mode strict
```

Пояснение параметров:

- **Rising Threshold (верхний порог)** – пороговое значение загрузки CPU в процентах, превысив которое, коммутатор войдёт в Exhausted Mode (режим высокой загрузки). Возможный диапазон значений: 20-100;
- **Falling Threshold (нижний порог) – пороговое значение** загрузки CPU в процентах, став ниже которого, коммутатор выйдет из **Exhausted Mode** и механизм Safeguard Engine отключится. Возможный диапазон значений: 20-100;
- **Strict-Mode (строгий режим)** – режим, при котором CPU полностью перестаёт получать ARP-пакеты и широковещательный трафик;
- **Fuzzy-Mode (нестрогий режим)** – режим, при котором CPU полностью перестаёт доступ ARP-пакетов и широковещательного трафика к CPU минимизируется динамически.

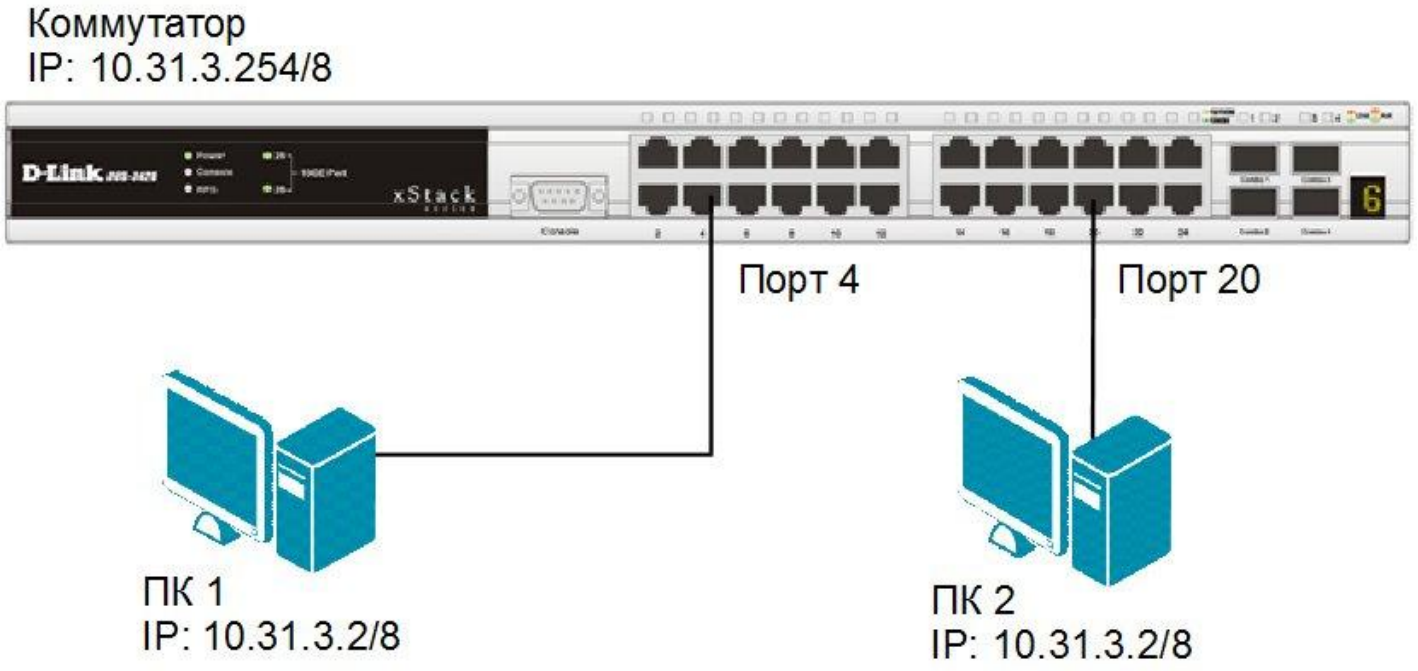
Функция CPU Interface Filtering

CPU Interface Filtering – функция, позволяющая ограничивать пакеты, поступающие для обработки на ЦПУ, путем фильтрации нежелательного трафика на аппаратном уровне.

По своей сути функция CPU Interface Filtering представляет собой списки управления доступом к интерфейсу ЦПУ и обладает аналогичными стандартным ACL принципами работы и конфигурации.

Пример настройки функции CPU Interface Filtering

ТЗ: необходимо настроить коммутатор таким образом, чтобы пакеты ICMP (например, команда Ping), передаваемые компьютером ПК 2, не отправлялись на обработку на ЦПУ, но при этом ПК 2 мог передавать подобные пакеты другим устройствам, например ПК 1.



Пример настройки функции CPU Interface Filtering

//Активация функции CPU Interface Filtering на коммутаторе

```
enable cpu_interface_filtering
```

//Создание профиля доступа для интерфейса ЦПУ

```
create cpu access_profile ip source_ip_mask
255.255.255.255 icmp profile_id 1
```

//Создание правила в профиле доступа

```
config cpu access_profile profile_id 1 add access_id 1
ip source_ip 10.31.3.2 icmp deny
```

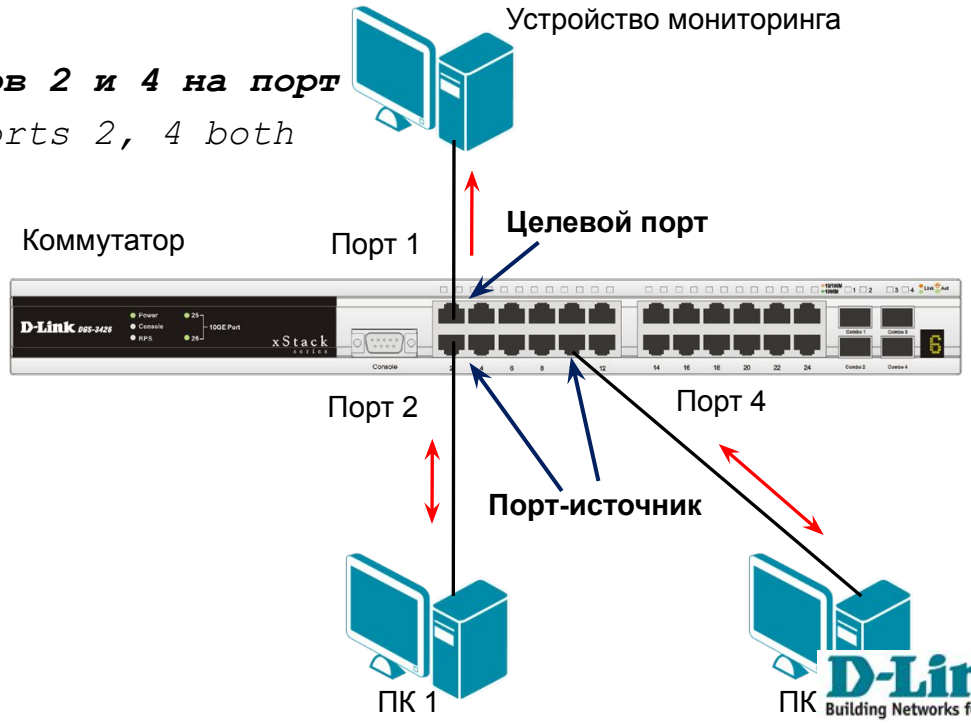
Доп. функция контроля трафика

Функция Port Mirroring

- Функция *Port Mirroring* (Зеркалирование портов) позволяет отображать (копировать) кадры, принимаемые и отправляемые портом-источником (Source port) на целевой порт (Target port) коммутатора, к которому подключено устройство мониторинга с целью анализа проходящих через интересующий порт пакетов.
- Целевой порт и порт-источник должны принадлежать одной VLAN и иметь одинаковую скорость работы.

Настройка коммутатора

```
//Настройка зеркалирования с портов 2 и 4 на порт
config mirror port 1 add source ports 2, 4 both
//Включение зеркалирования
enable mirror
```



Организация многоадресной передачи с помощью управляемых коммутаторов

Типы передачи данных в сетях

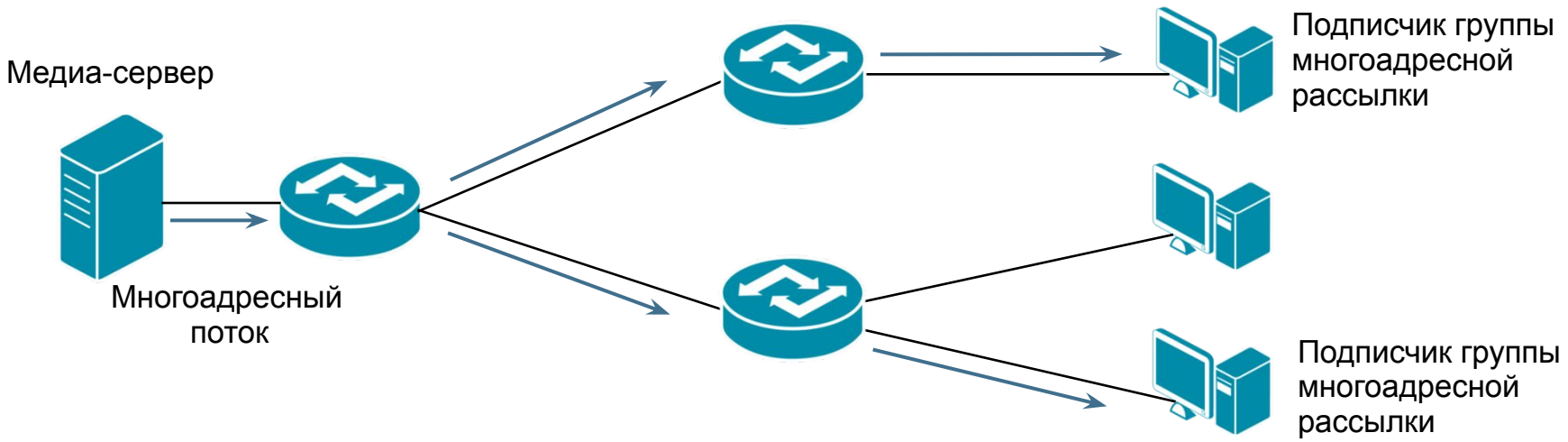
- **Unicast (одноадресная передача)** – поток данных передается от узла-отправителя на индивидуальный *IP-адрес конкретного узла-получателя*;

- **Broadcast (широковещательная передача)** – поток данных передается от узла-отправителя множеству узлов-получателей, подключенных к сети, используя *широковещательный IP-адрес*;

- **Multicast (многоадресная рассылка)** – поток данных передается группе узлов на множество IP-адресов *группы многоадресной рассылки*.

Многоадресная рассылка

- У группы многоадресной рассылки нет географических ограничений: узлы могут находиться в любой точке мира.
- Узлы, которые заинтересованы в получении данных для определенной группы, должны присоединиться к этой группе (подписаться на рассылку) при помощи **протокола IGMP** (Internet Group Management Protocol).
- После подписки узла на группу пакеты многоадресной рассылки IP, будут поступать в том числе и на этот узел.

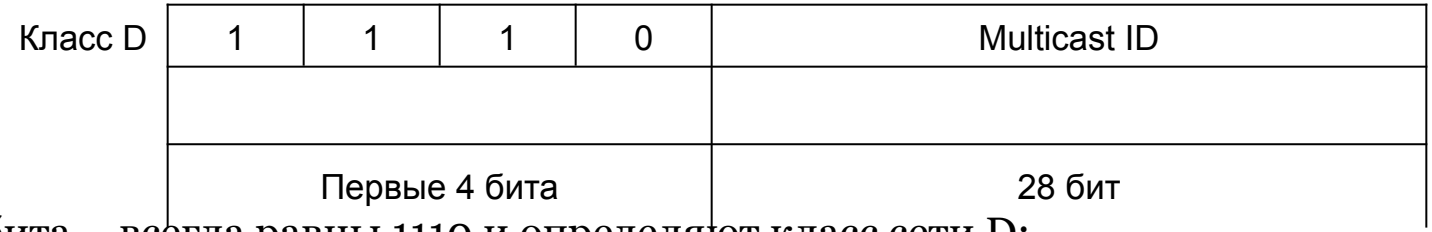


Многоадресная рассылка

Принципы адресации MULTICAST в IPv4

- Источник многоадресного трафика направляет пакеты многоадресной рассылки на групповой IP-адрес.
- Групповые адреса определяют произвольную группу IP-узлов, присоединившихся к этой группе и желающих получать адресованный ей трафик.
- **Агентство IANA** (Internet Assigned Numbers Authority), выделило для многоадресной рассылки адреса IPv4 класса D в диапазоне от 224.0.0.0 до 239.255.255.255.

- Формат IP-адреса **класса D**:

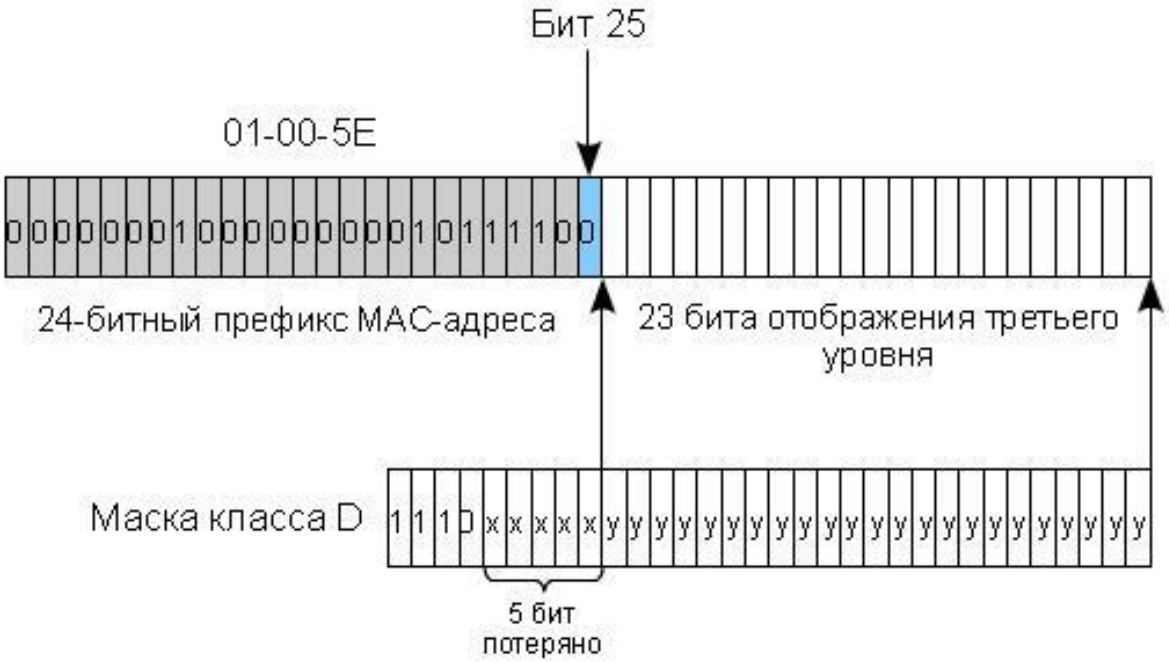


- Первые 4 бита – всегда равны 1110 и определяют класс сети D;
- Остальные 28 бит – используются для идентификации конкретной группы получателей многоадресного трафика.

Многоадресная рассылка

Принципы адресации MULTICAST на канальном уровне

- MAC-адрес групповой рассылки начинается с префикса, состоящего из 24 бит – **01005Eh**. Следующий 25-й бит (или бит высокого порядка) приравнивается к 0. Последние 23 бита MAC-адреса формируются из 23 младших бит группового IP-адреса.
- При преобразовании теряются 5 битов 1-го октета IP-адреса, получившийся адрес не является уникальным.
- Каждому MAC-адресу соответствует 32 IP-адреса групповой рассылки.



Многоадресная рассылка

Подписка и обслуживание групп

- **Протокол IGMP** используется для динамической регистрации отдельных узлов в многоадресной группе локальной сети.

- В настоящее время существуют три версии протокола IGMP:
  - IGMPv1 (RFC 1112), IGMPv2 (RFC 2236), IGMPv3 (RFC 3376).

- Узлы сети определяют принадлежность к группе, посылая IGMP-сообщения на свой локальный многоадресный маршрутизатор. По протоколу IGMP маршрутизаторы (коммутаторы L3) получают IGMP-сообщения и периодически посылают запросы, чтобы определить, какие группы активны или неактивны в данной сети.

- В общем случае протокол IGMP определяет следующие типы сообщений:
  - **запрос о принадлежности к группе** (Membership Query);
  - **ответ о принадлежности к группе** (Membership Report);
  - **сообщение о выходе из группы** (Leave Group Message).

Многоадресная рассылка

IGMP Snooping

Основная проблема – эффект «флудинга» при передаче multicast-трафика коммутатором L2 (передача многоадресного трафика через все порты).

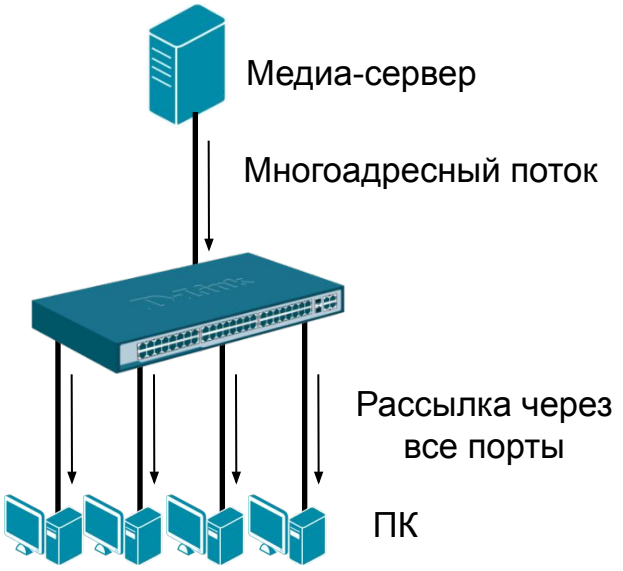
Управление многоадресной рассылкой на коммутаторе L2 может быть выполнено двумя способами:

- Созданием статических записей в таблицах коммутации для портов, к которым не подключены подписчики многоадресных групп;
- Использованием функции **IGMP Snooping** (прослушиванием multicast- трафика).

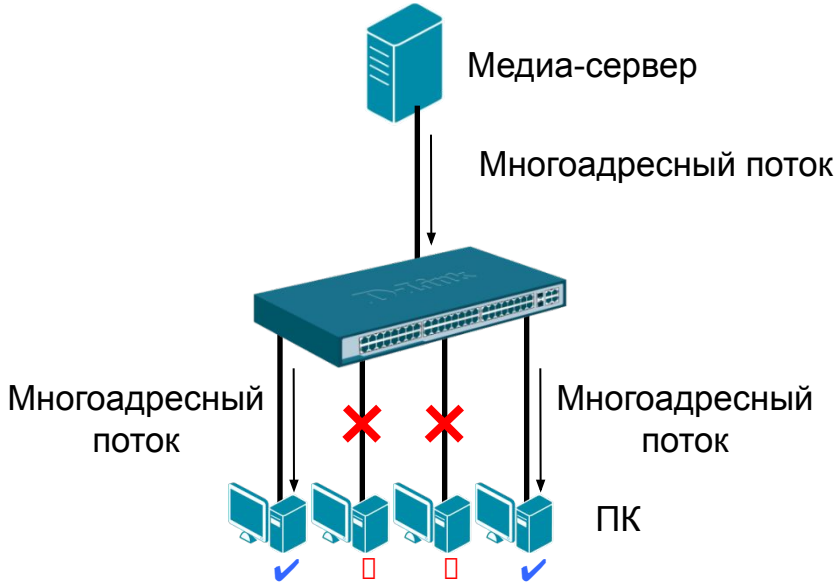
Многоадресная рассылка

Функция IGMP Snooping

- **IGMP Snooping** – это функция, которая позволяет коммутаторам L2 изучать членов многоадресных групп, подключенных к его портам, прослушивая IGMP-сообщения (запросы и ответы), передаваемые между узлами-подписчиками и маршрутизаторами (коммутаторами L3).



Без поддержки IGMP Snooping



С поддержкой IGMP Snooping

Рисунок анимирован

Многоадресная рассылка

Функция IGMP Snooping

1) Когда узел, подключенный к коммутатору, хочет вступить в многоадресную группу или отвечает на IGMP-запрос, полученный от маршрутизатора многоадресной рассылки, он отправляет IGMP-ответ, в котором указан адрес многоадресной группы.
2) Коммутатор просматривает информацию в IGMP-ответе и создает в своей **ассоциативной таблице коммутации IGMP Snooping** запись для этой группы (если она не существует). Эта запись связывает порт, к которому подключен узел-подписчик, порт, к которому подключен маршрутизатор (коммутатор уровня 3) многоадресной рассылки, и MAC-адрес многоадресной группы.
3) Если коммутатор получает IGMP-ответ для этой же группы от другого узла данной VLAN, то он добавляет номер порта в уже существующую запись ассоциативной таблицы коммутации IGMP Snooping.

- Формируя таблицу коммутации многоадресной рассылки, коммутатор осуществляет передачу многоадресного трафика только тем узлам, которые в нем заинтересованы.
- Когда коммутатор получает IGMP-сообщение о выходе узла из группы, он удаляет номер порта, к которому подключен этот узел, из соответствующей записи таблицы коммутации IGMP Snooping.

Многоадресная рассылка

Процесс создания таблицы коммутации IGMP Snooping

Таблица коммутации IGMP Snooping

Номер порта	Многоадресная группа	MAC-адрес многоадресной группы
1, 10, 25	239.192.1.10	01-00-5E-40-01-0A

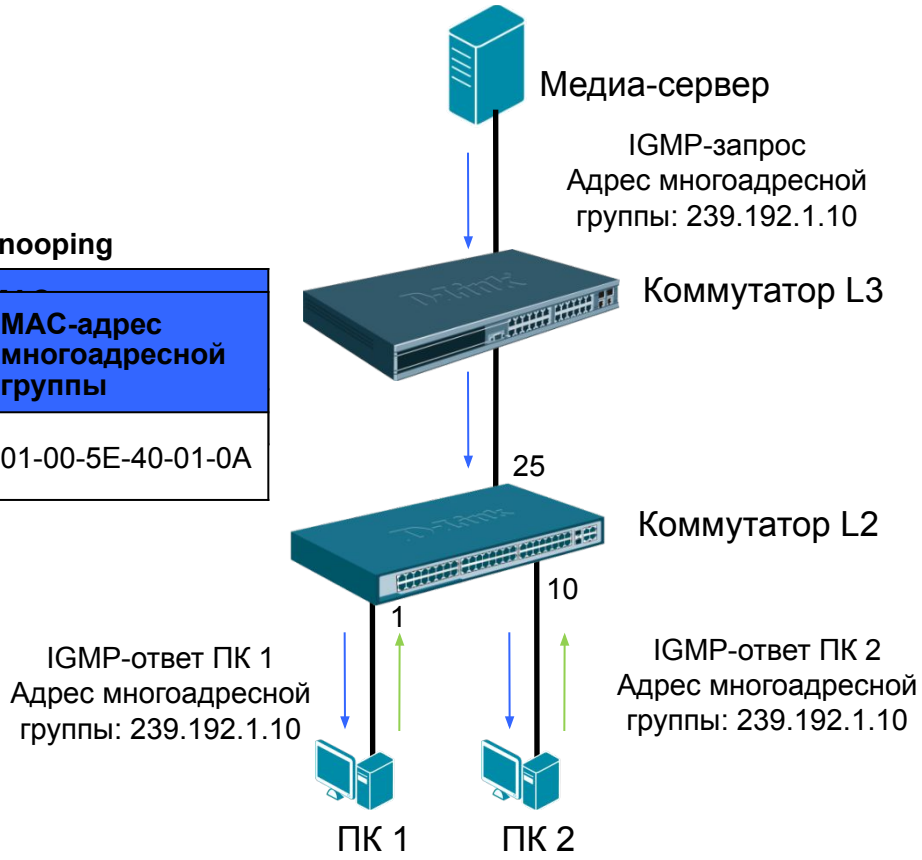
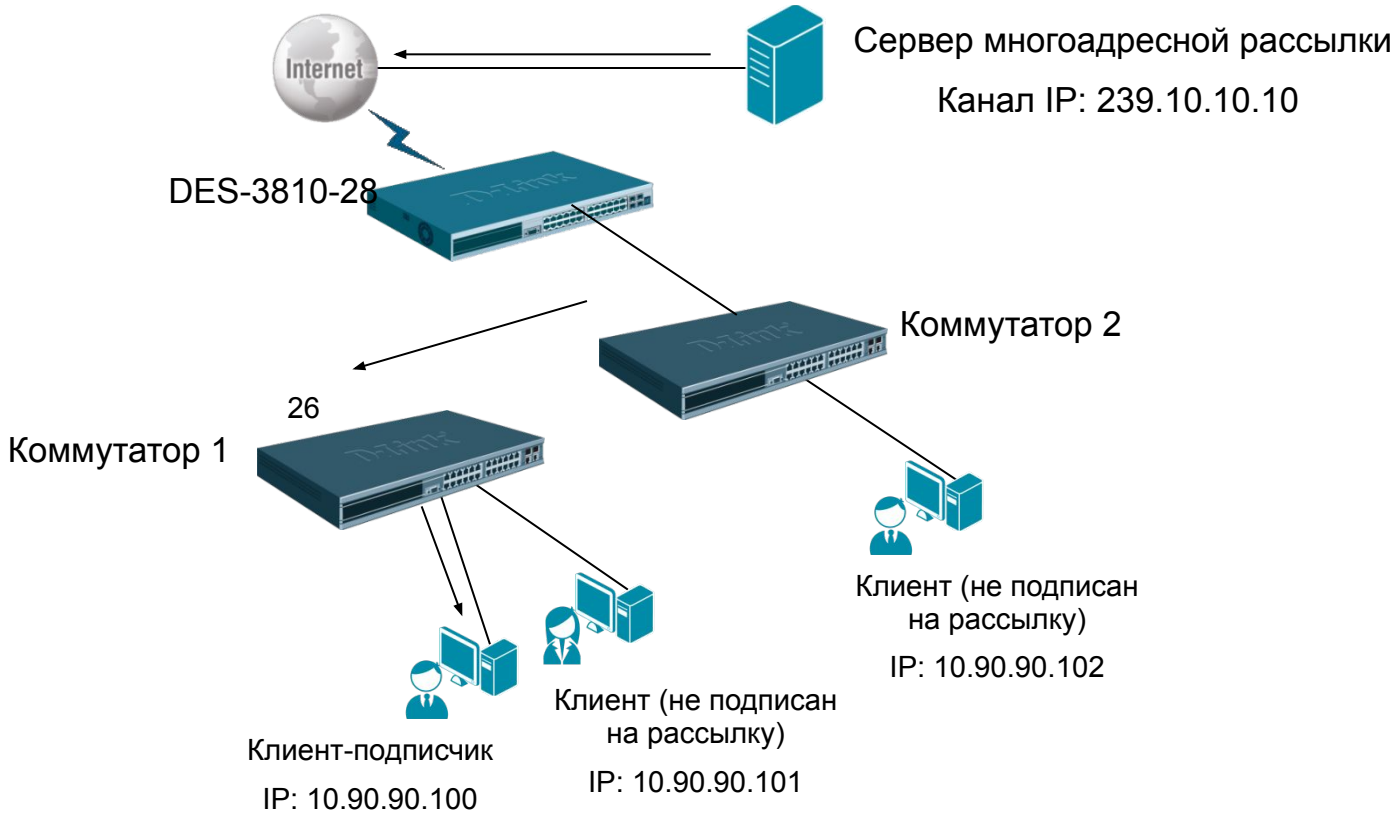


Рисунок анимирован

Многоадресная рассылка

Пример настройки IGMP Snooping



Многоадресная рассылка

Настройка коммутатора 1

//Активизировать функцию IGMP Snooping глобально на //коммутаторе

- `enable igmp_snooping`

//Активизировать функцию IGMP Snooping в указанной VLAN (в //данном примере VLAN по умолчанию)

- `config igmp_snooping vlan default state enable`

//Включить фильтрацию многоадресного трафика, чтобы //избежать его передачи узлам, не являющимся подписчиками //многоадресной рассылки

- `config multicast vlan_filtering_mode vlan default filter_unregistered_groups`

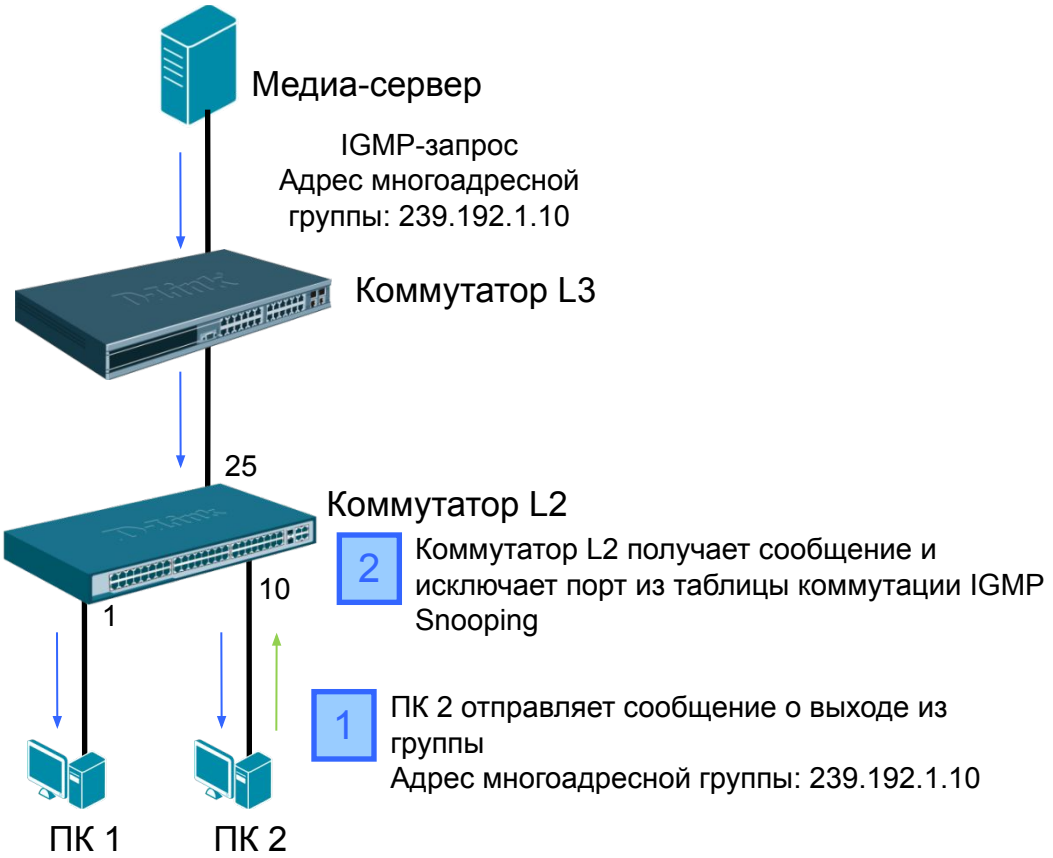
Многоадресная рассылка

Функция IGMP Snooping Fast Leave

- Функция IGMP Snooping Fast Leave, активизированная на коммутаторе, позволяет мгновенно исключить порт из таблицы коммутации IGMP Snooping при получении им сообщения о выходе из группы.
- Порт 25 будет удален из таблицы коммутации IGMP Snooping только в том случае, если к нему не будет подключен ни один узел-подписчик.

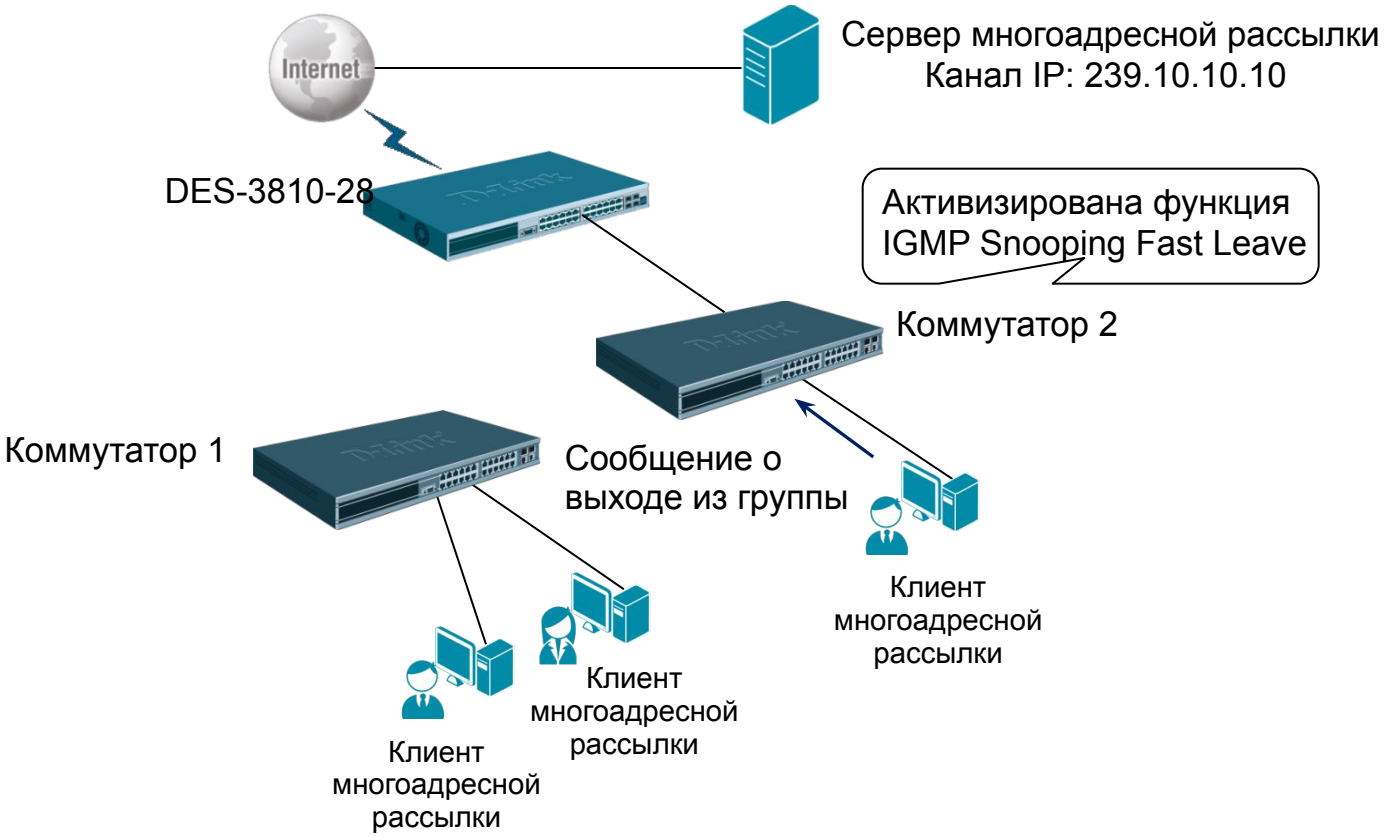
Таблица коммутации IGMP Snooping

Номер порта	Многоадресная группа	MAC-адрес многоадресной группы
1, 25	239.192.1.10	01-00-5E-40-01-0A



Многоадресная рассылка

Пример настройки IGMP Snooping Fast Leave



Многоадресная рассылка

Настройка коммутатора 2

//Активизировать функцию IGMP Snooping глобально на коммутаторе и //в указанной VLAN (в данном примере VLAN по умолчанию). Включить //фильтрацию многоадресного трафика.

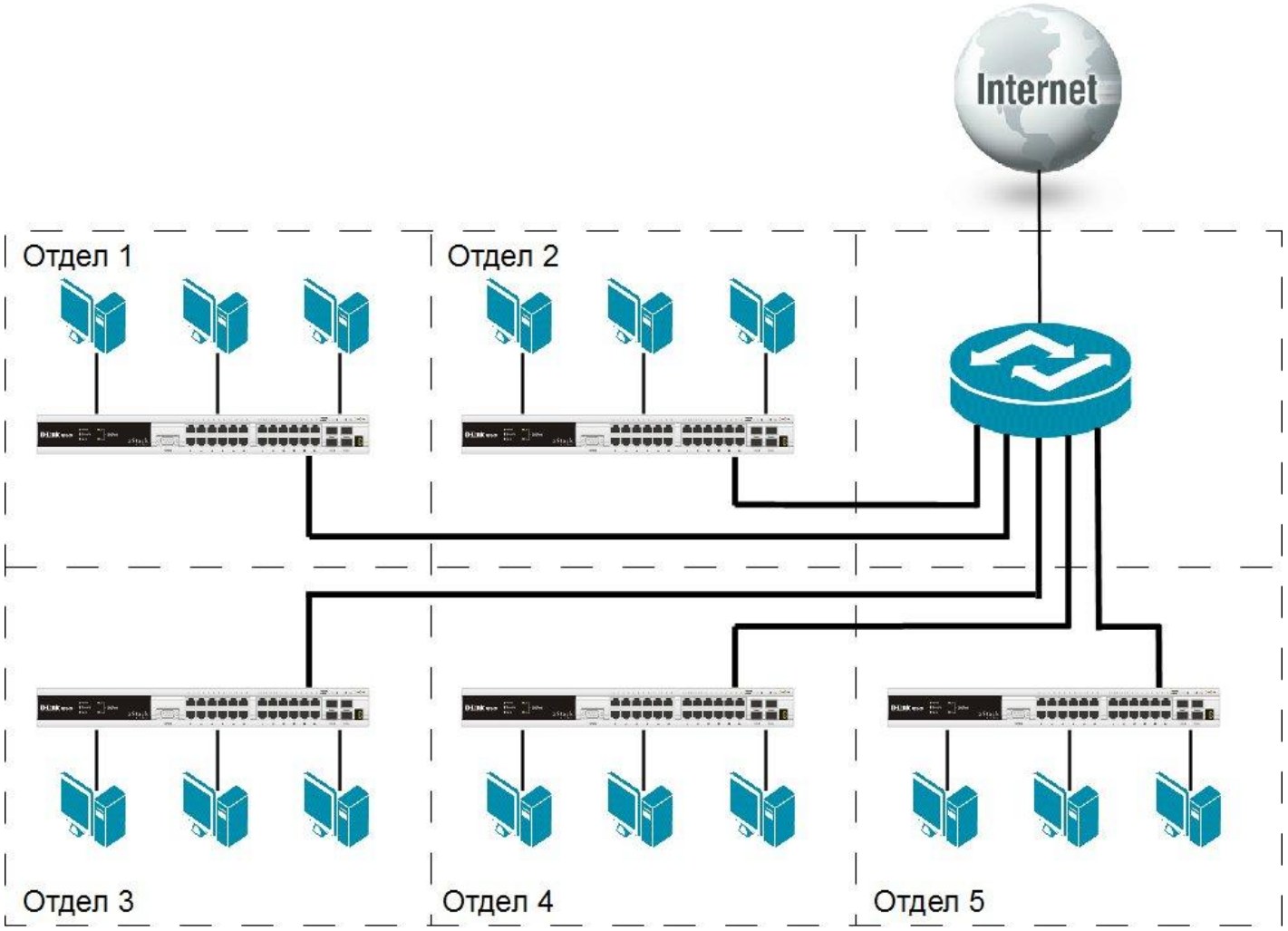
- `enable igmp_snooping`
- `config igmp_snooping vlan default state enable`
- `config multicast vlan_filtering_mode vlan default filter_unregistered_groups`

//Активизировать функцию IGMP Snooping Fast Leave в указанной VLAN.

- `config igmp_snooping vlan default fast_leave enable`

Виртуальные локальные сети (VLAN) и сегментация трафика

Принцип физической сегментации сети



Физическая сегментация сети

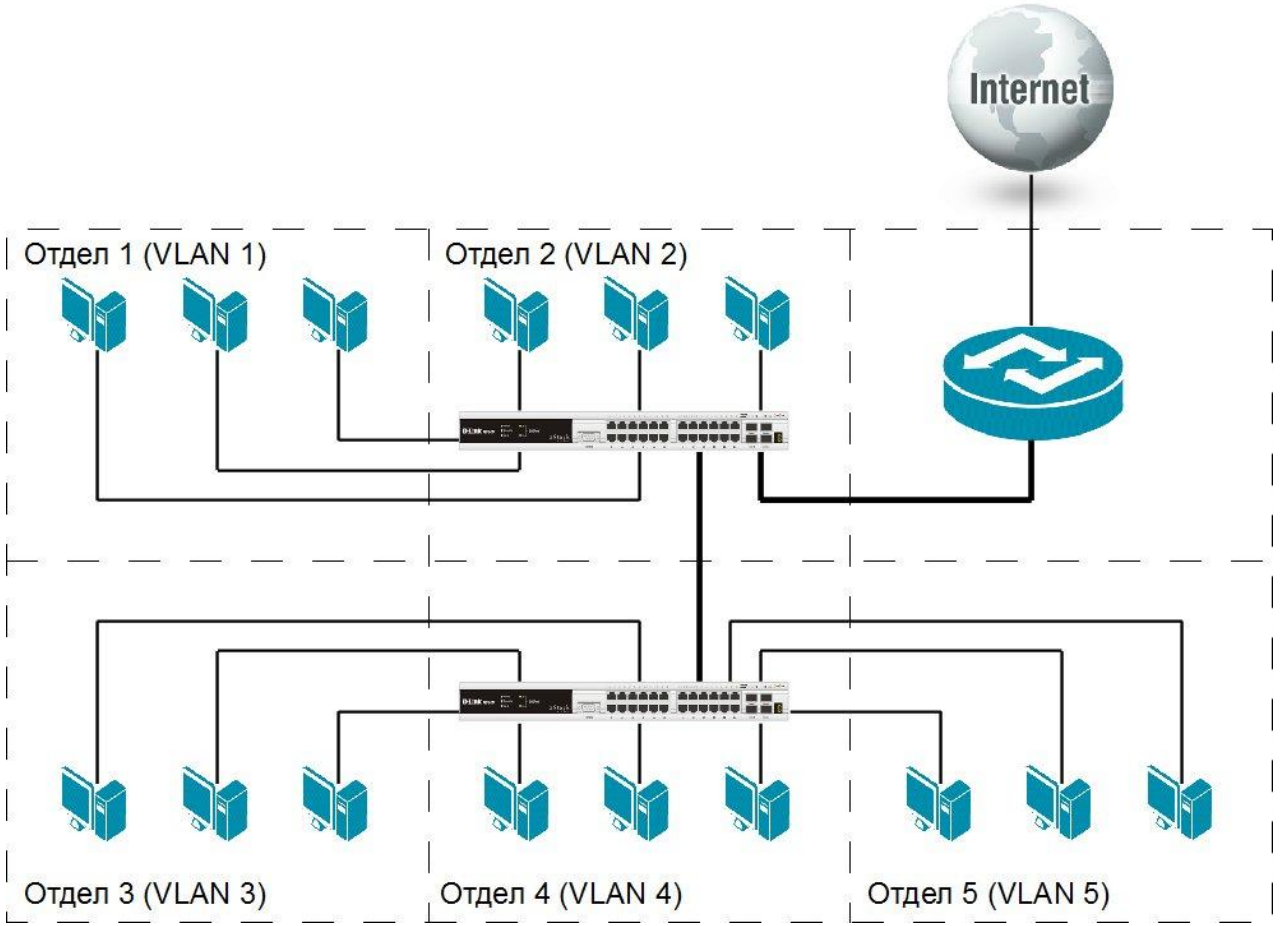
Достоинства:

- Простая и понятная архитектура;
- Возможность масштабирования ЛВС.

Недостатки:

- Неоправданно большие затраты на оборудование и СКС;
- Излишняя избыточность;
- Неиспользование функциональных возможностей оборудования

Принцип логической сегментации сети с помощью VLAN



Понятие VLAN

Виртуальная локальная сеть (Virtual Local Area Network, VLAN) - логическая группа узлов компьютерной сети трафик которой, в том числе и широковещательный, на канальном уровне полностью изолирован от других групп или одиночных узлов сети.

Преимущества использования VLAN:

- Облегчается перемещение, добавление узлов и изменение их соединений друг с другом;
- Достигается большая степень административного контроля над сетевыми узлами и трафиком;
- Повышается безопасность сети;
- Уменьшается потребление полосы пропускания;
- Сокращается неэффективное использование процессора коммутаторов за счет сокращения пересылаемого трафика;
- Предотвращаются широковещательные штормы и сетевые петли.

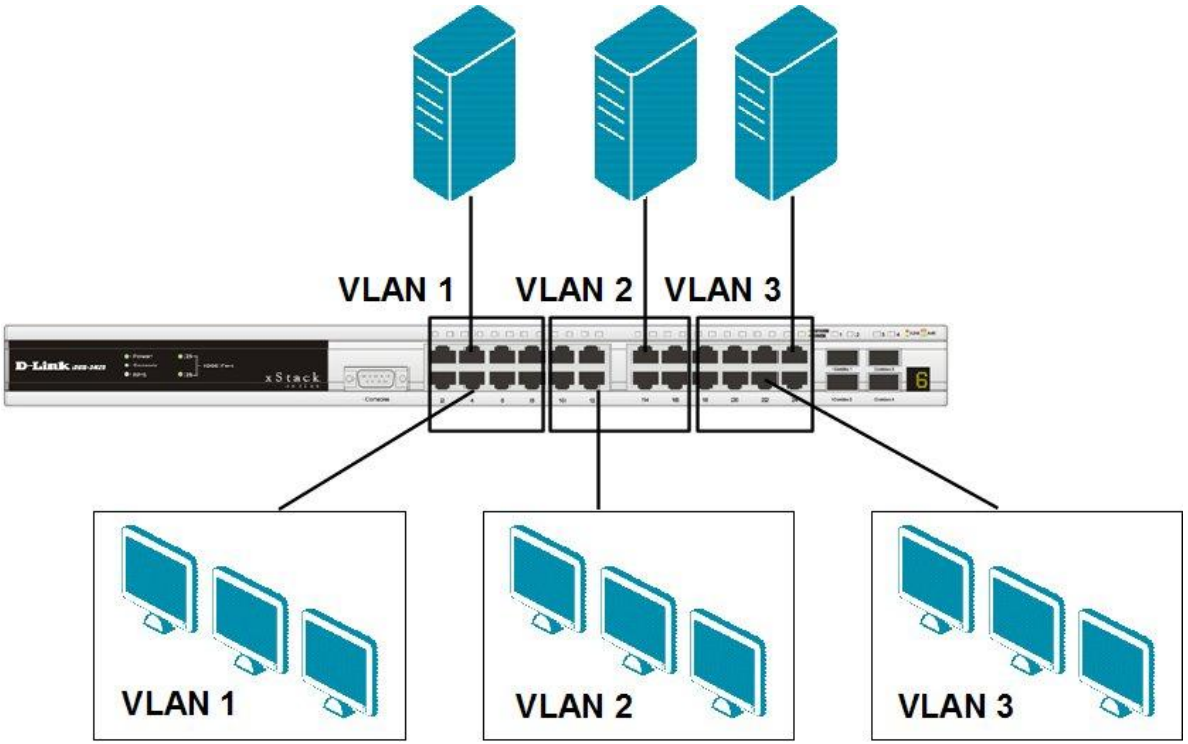
Типы VLAN

В управляемых коммутаторах могут быть VLAN:

- на основе портов;
- на основе стандарта IEEE 802.1q (связан с тегированием трафика);
- на основе стандарта IEEE 802.1ad (связан с двойным тегированием трафика);
- прочие виды VLAN (на основе протоколов, мас-адресов, ассиметричные и др).

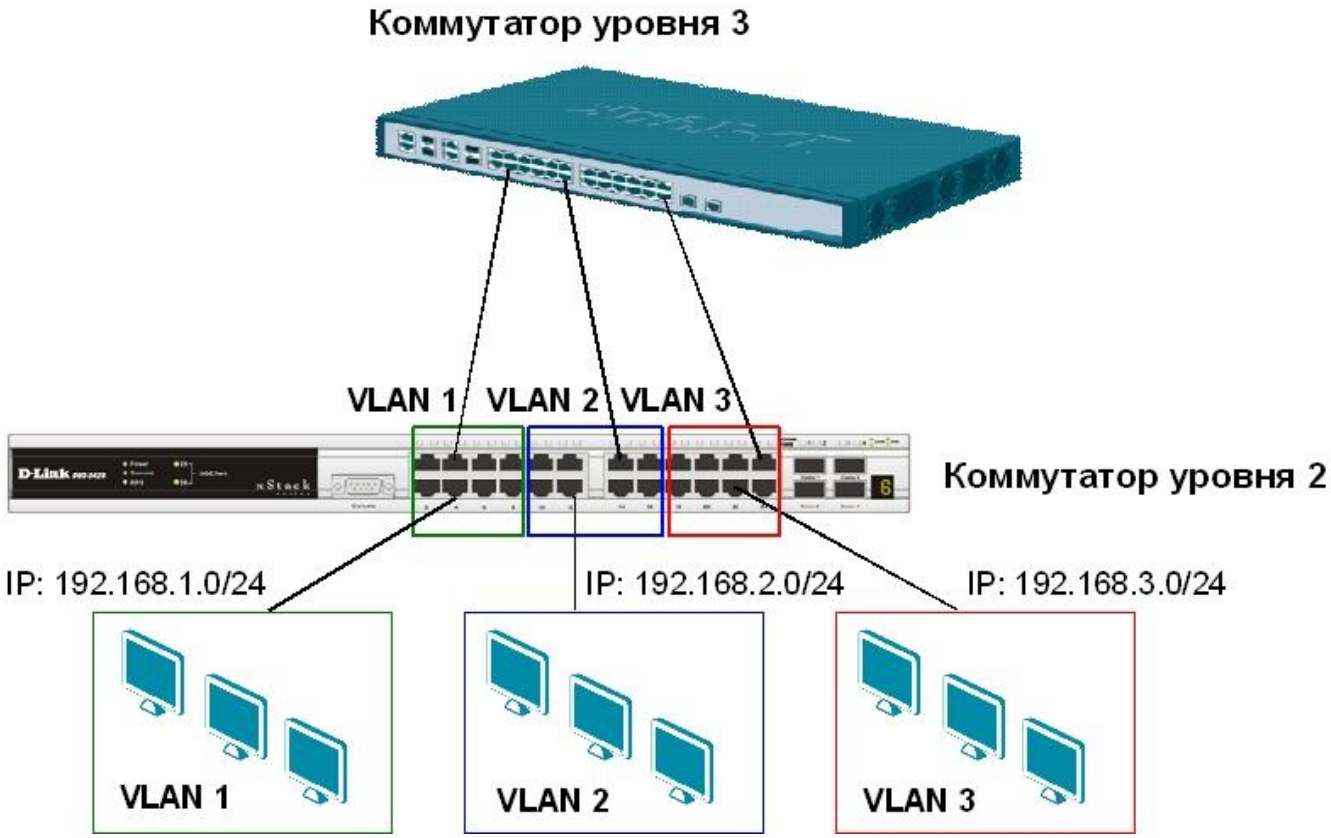
VLAN на основе портов (Port-based VLAN)

- При использовании VLAN на основе портов (Port-based VLAN), каждый порт назначается в определенную VLAN;
- VLAN «привязана» только к одному коммутатору;
- Конфигурация портов статическая и может быть изменена только вручную.



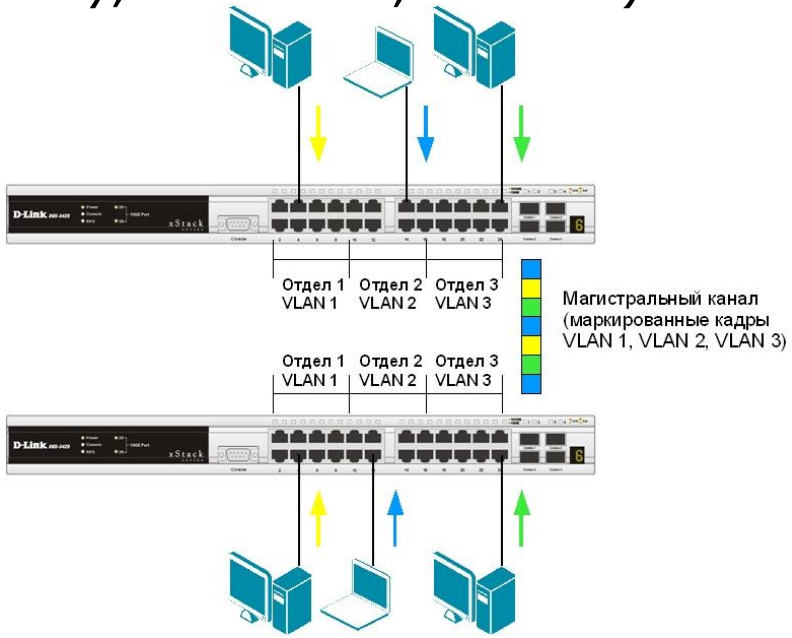
VLAN на основе портов (Port-based VLAN)

При необходимости передавать трафик между разными VLAN можно использовать маршрутизатор или коммутатор L3



VLAN на основе стандарта IEEE 802.1Q

- Стандарт IEEE 802.1q предполагает помечать каждый кадр Ethernet **дополнительным тегом (флагом, меткой, маркером)**;
- Тег должен хранить информацию о принадлежности к VLAN при его перемещении по сети;
- Тегированные кадры возможно передавать через множество 802.1q-совместимых коммутаторов посредством физического соединения (*магистральному каналу, Trunk Link, UPLINK*).



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

Ключевые понятия 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.

VLAN на основе стандарта IEEE 802.1Q

Port VLAN ID

- Каждый физический порт коммутатора имеет параметр, называемый ***идентификатором порта VLAN (PVID)***;
- По сути, PVID определяет идентификатор VLAN, к которой привязан данный порт;
- Все *немаркированные кадры, попадающие на коммутатор* дополняются тегом IEEE 802.1q с VID, равным PVID порта, на который кадры были приняты;
- Внутри коммутатора все кадры являются тегированными;
- Дополнительно, помимо VID, каждой VLAN на коммутаторе можно присвоить имя. Оно исключительно для удобства администратору, и «действует» в рамках одного коммутатора);
- По умолчанию на управляемых коммутаторах D-Link с поддержкой стандарта IEEE 802.1q входят в одну VLAN с **PVID = 1** и с именем **«Default»**.

VLAN на основе стандарта IEEE 802.1Q

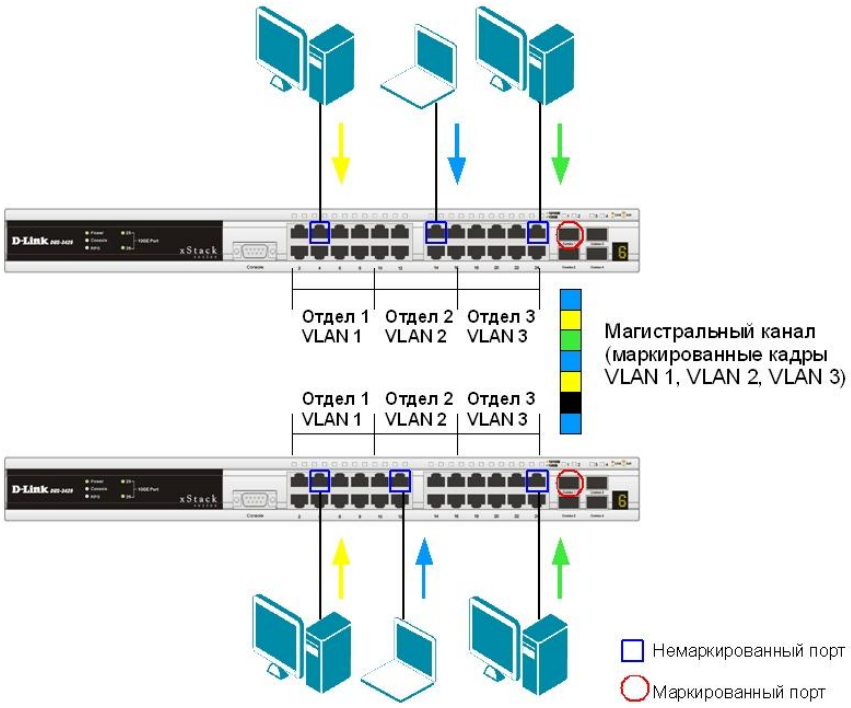
Маркированные и немаркированные порты

Tagged (маркированный) порт – для подключения между собой коммутаторов.

- 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 – для подключения конечных устройств.

- Порт извлекает тег 802.1Q из заголовков всех выходящих через него маркированных кадров.



VLAN на основе стандарта IEEE 802.1Q

ВАЖНЫЕ ЗАМЕЧАНИЯ

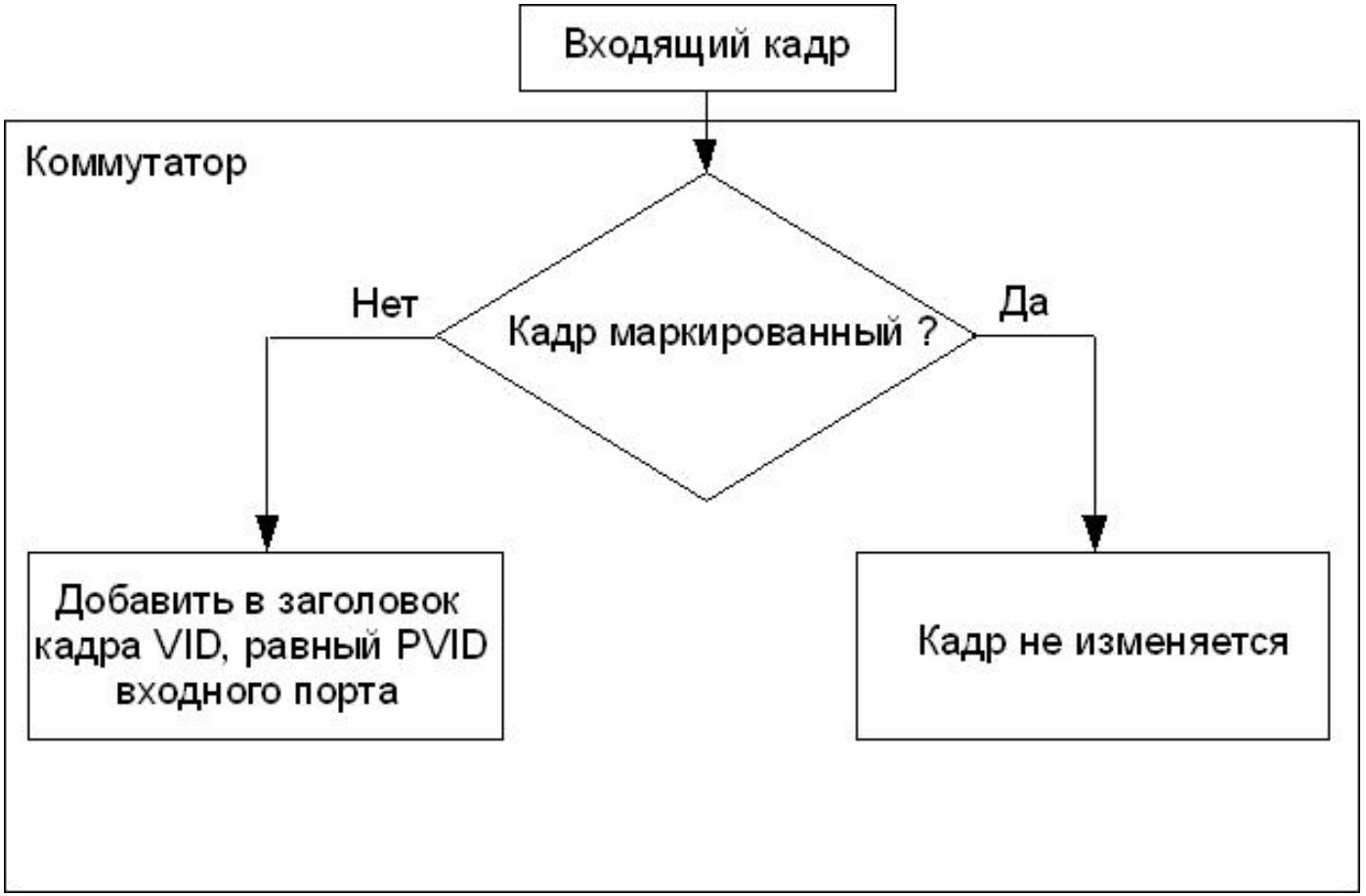
- Поскольку под номер VID в теге отводится 12 бит, максимальное количество VLAN может быть 4094 (номера 0 и 4095 зарезервированы и не используются);

- Нетегированный порт коммутатора может входить только в одну VLAN;

- Тегированный порт коммутатора может входить в несколько VLAN

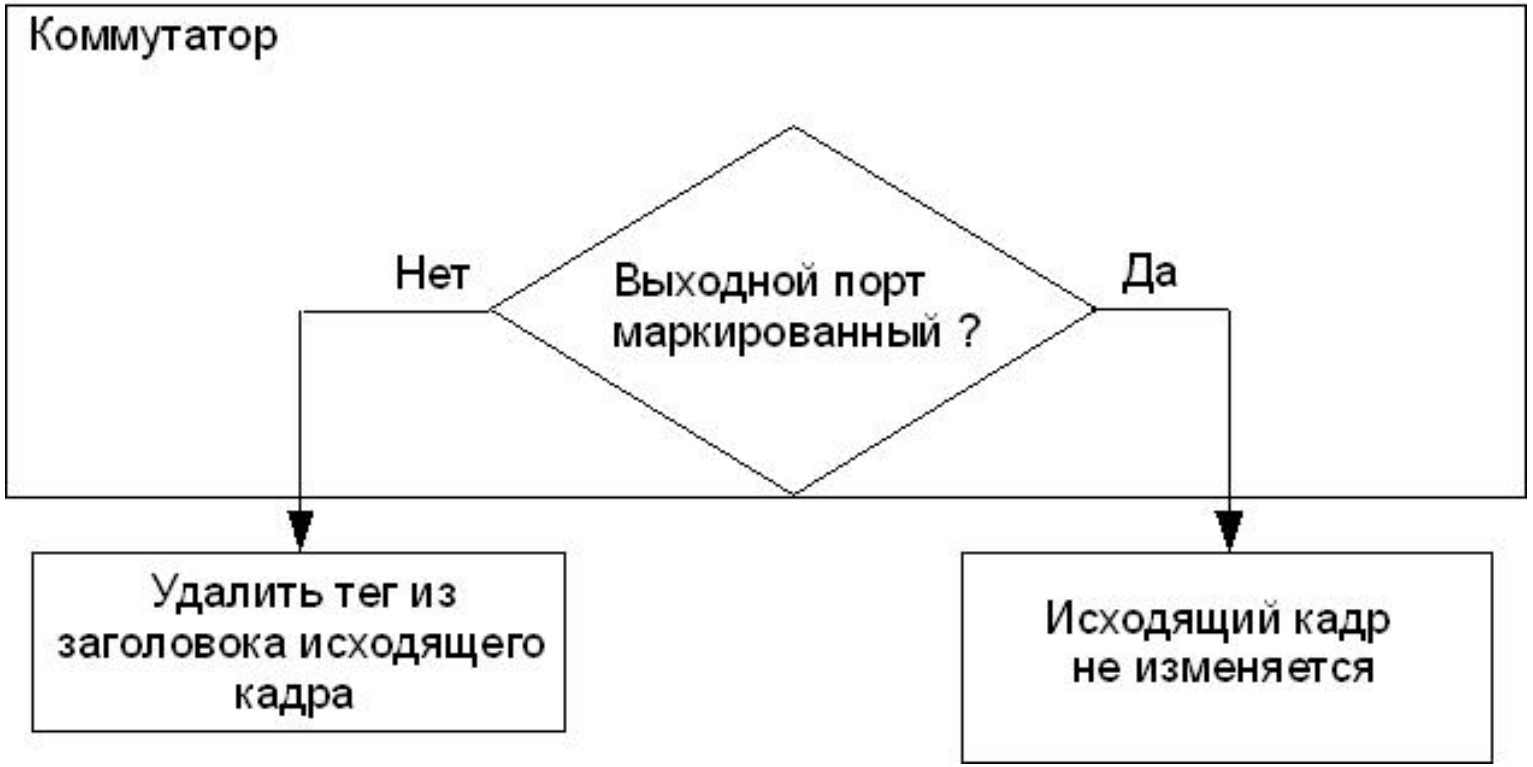
VLAN на основе стандарта IEEE 802.1Q

Правило для входящего трафика



VLAN на основе стандарта IEEE 802.1Q

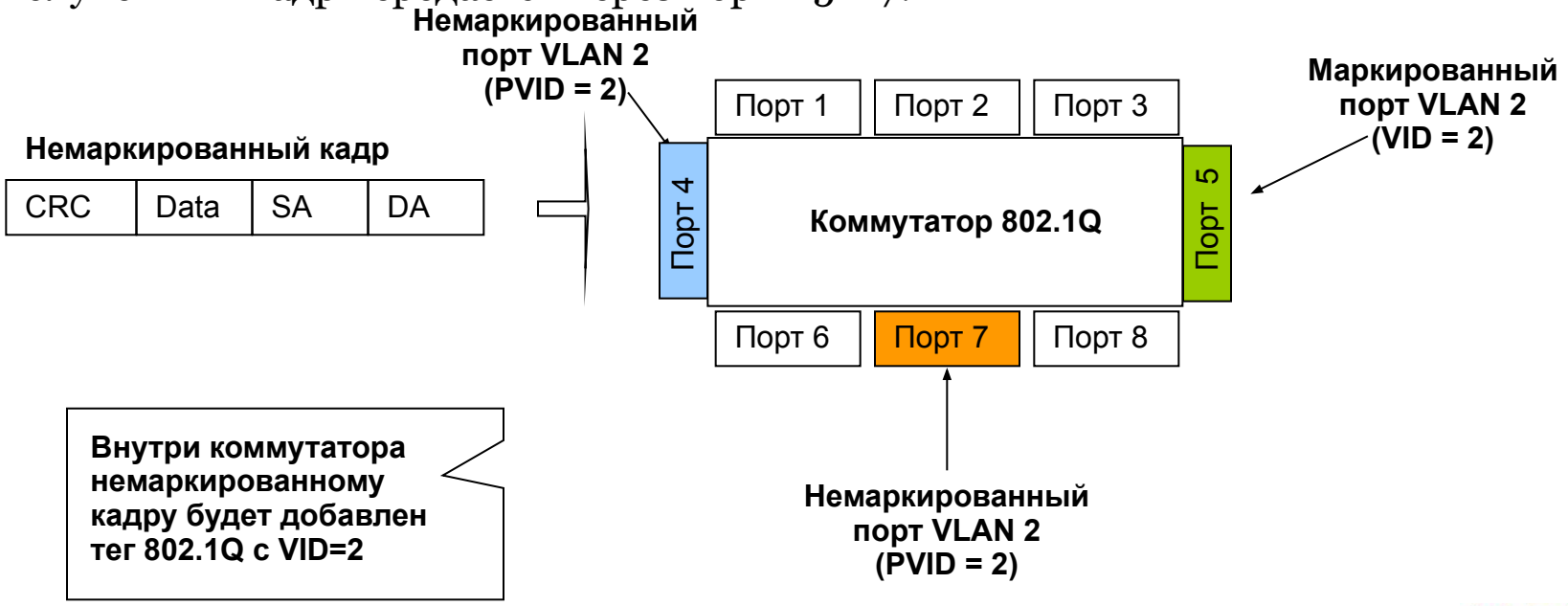
Правило для исходящего трафика



VLAN на основе стандарта IEEE 802.1Q

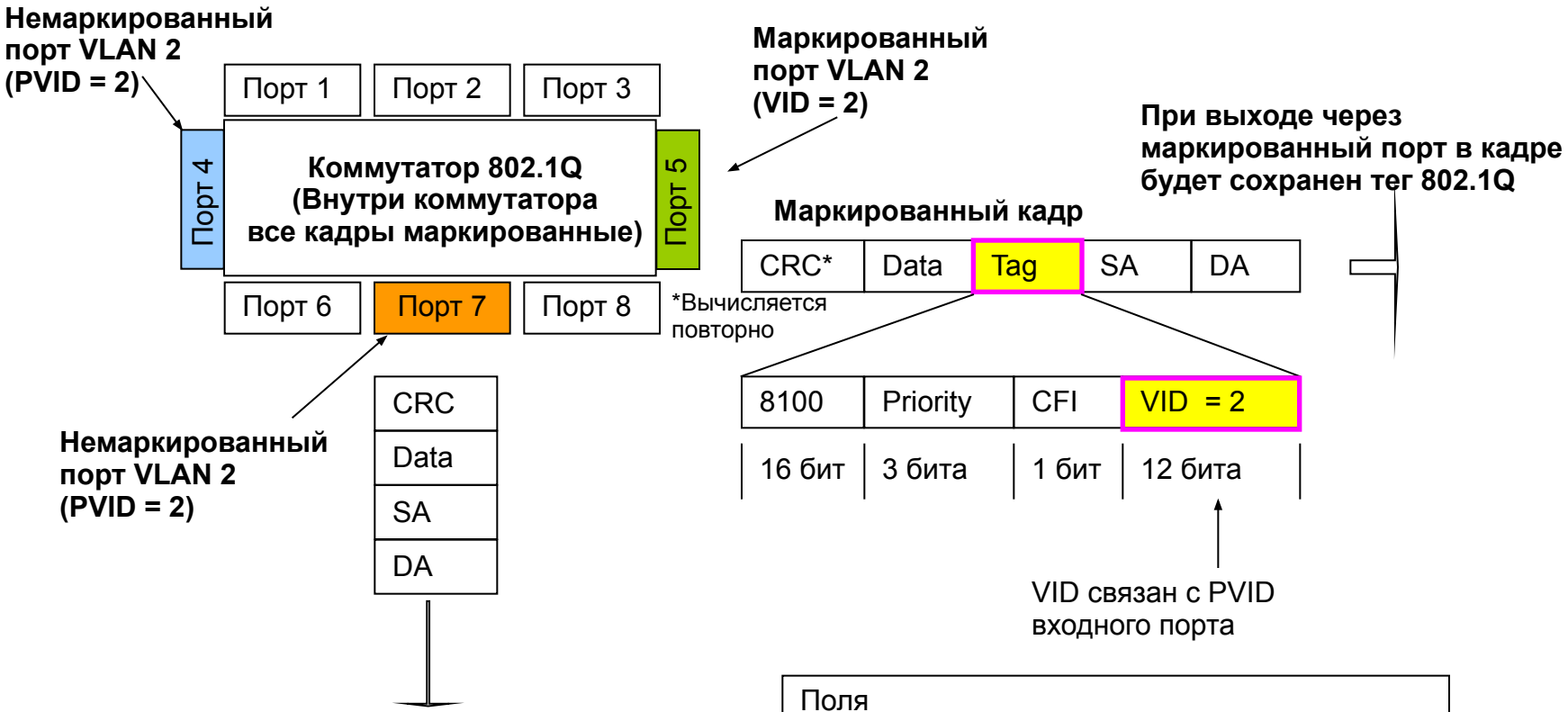
Входящий немаркированный кадр 802.1Q

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



VLAN на основе стандарта IEEE 802.1Q

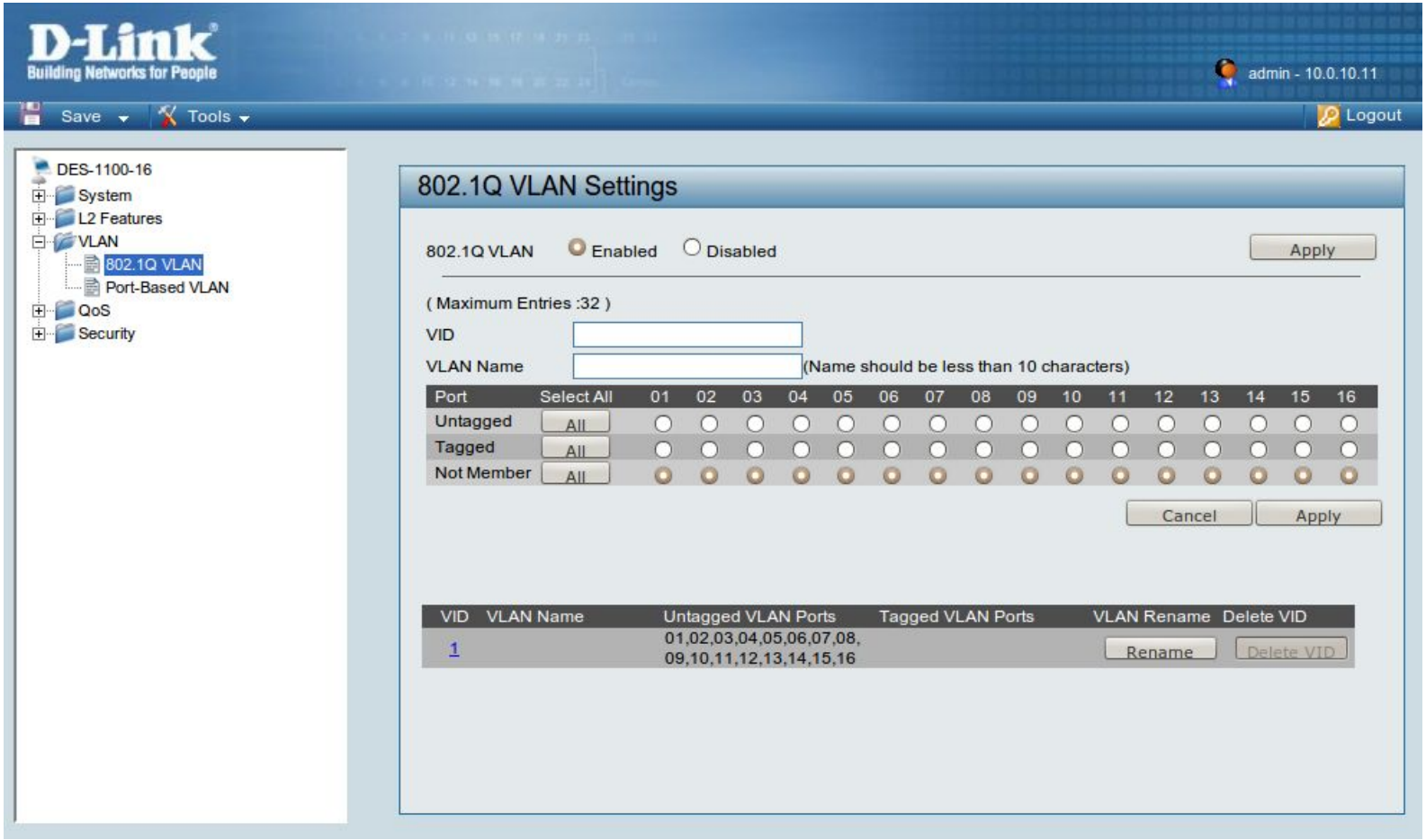
Передача немаркированного кадра через маркированный порт и немаркированный порты



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

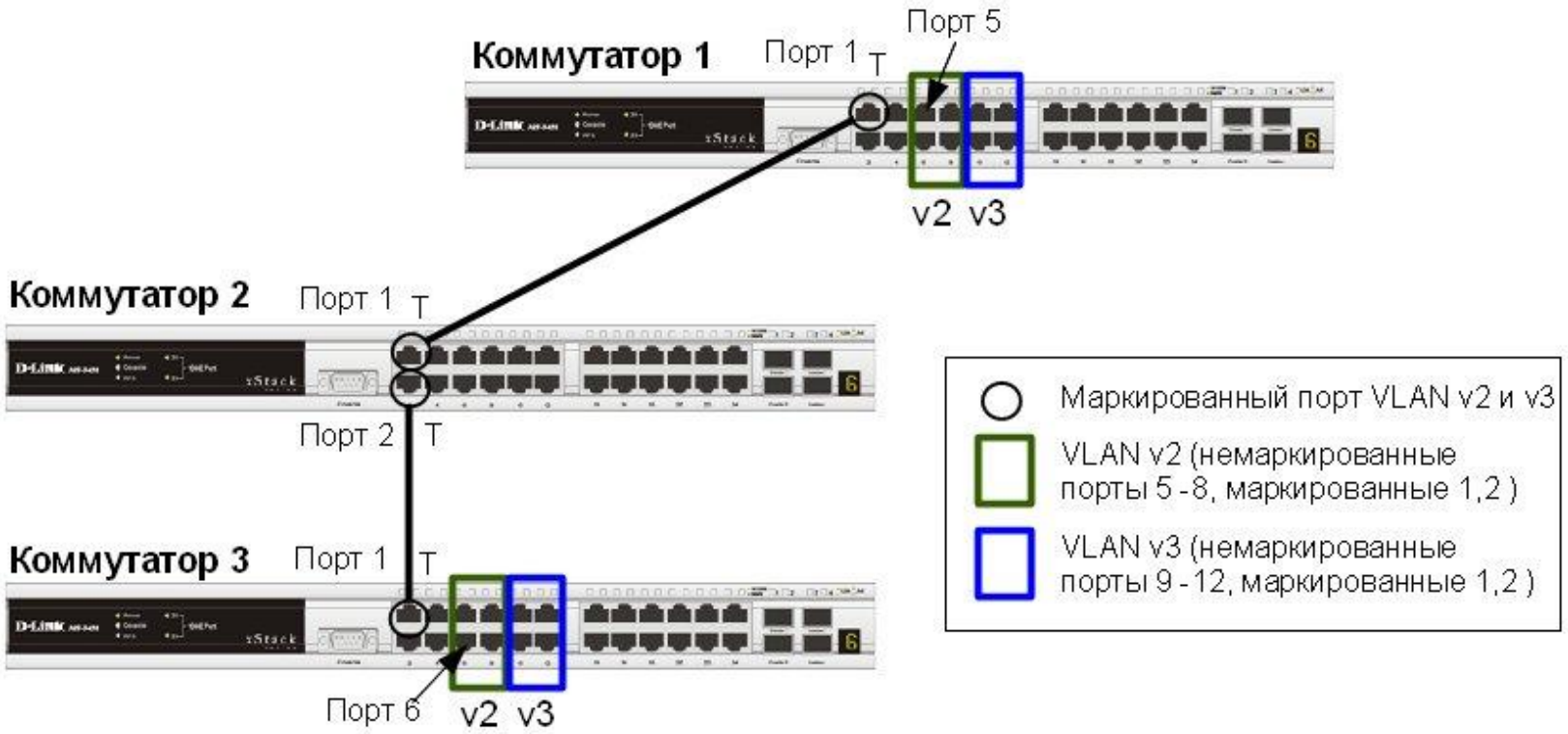
D-Link
Building Networks for People

Настройка VLAN 802.1q через Web-интерфейс на примере DES-1100-16



VLAN на основе стандарта IEEE 802.1Q

Пример настройки VLAN



VLAN на основе стандарта IEEE 802.1Q

Коммутаторы 1 и 3

```
config vlan default delete 1, 5-12
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
```

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
```

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.

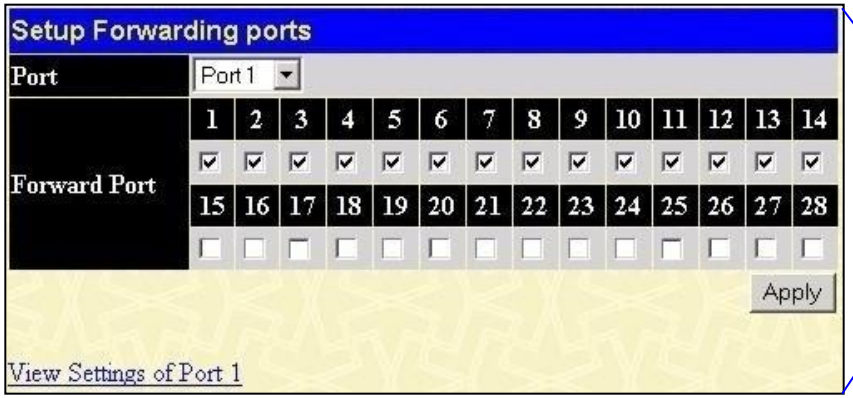
Внимание: заводские установки по умолчанию назначают все порты коммутатора в default VLAN с VID = 1. **Перед созданием новой VLAN необходимо удалить из default VLAN все порты, которые требуется сделать немаркированными членами новой VLAN.**

Функция сегментации трафика

***Traffic Segmentation* (сегментация трафика)** служит для разграничения узлов на канальном уровне в рамках одного коммутатора.

Функция позволяет настраивать порты или группы портов коммутатора таким образом, чтобы они были полностью изолированы друг от друга, но в то же время имели общий доступ к разделяемым портам.

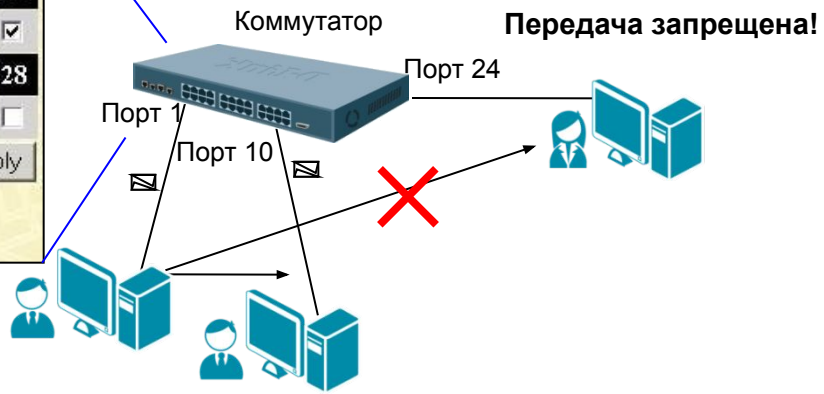
Следующая конфигурация позволяет клиенту, подключенному к порту 1 отправлять/получать трафик от клиентов, подключенных к портам 1-14



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.



Слайд анимирован

Функция сегментации трафика

Преимущества Traffic Segmentation перед VLAN 802.1q

- Простота настройки;
- Свободное группирование портов без ограничений;
- Возможность использования разделяемых ресурсов для изолированных друг от друга групп портов.

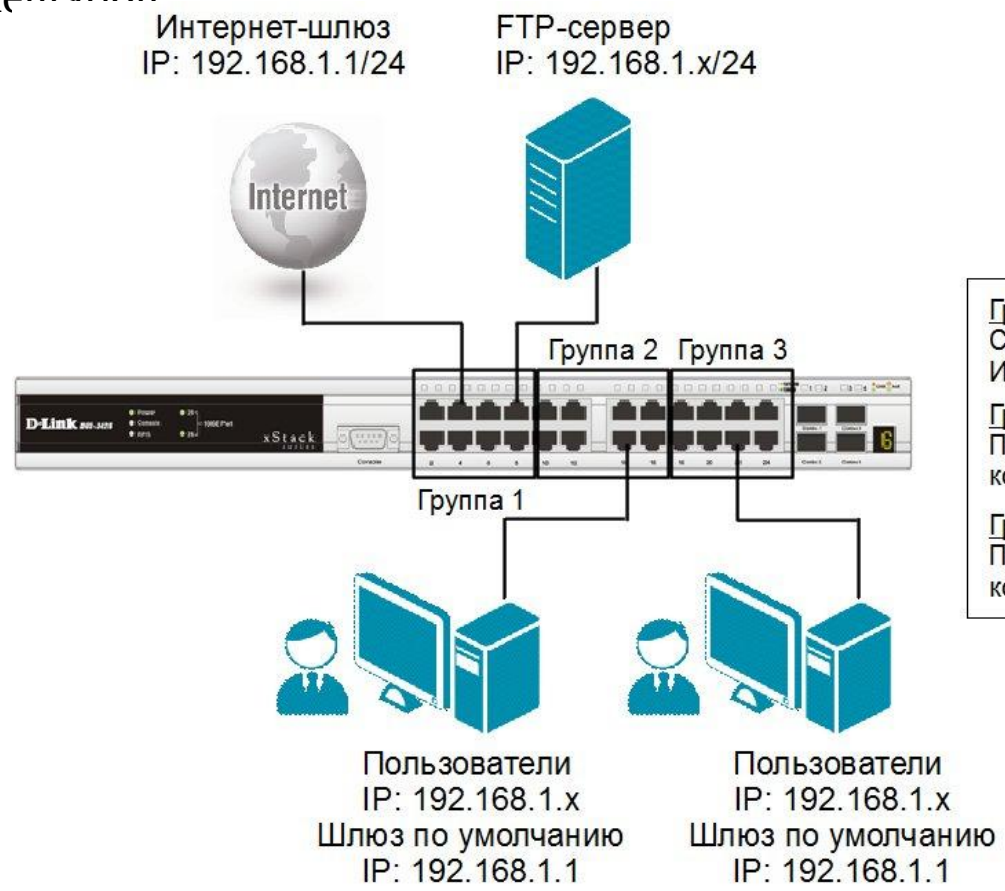
Замечание:

- Функция Traffic Segmentation может использоваться совместно с VLAN 802.1Q с целью сокращения трафика внутри локальной сети, позволяя разбивать ее на более маленькие группы (сегменты);
- При совместном использовании правила VLAN имеют более высокий приоритет. Правила Traffic Segmentation применяются после них.

Функция сегментации 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)

Функция сегментации трафика

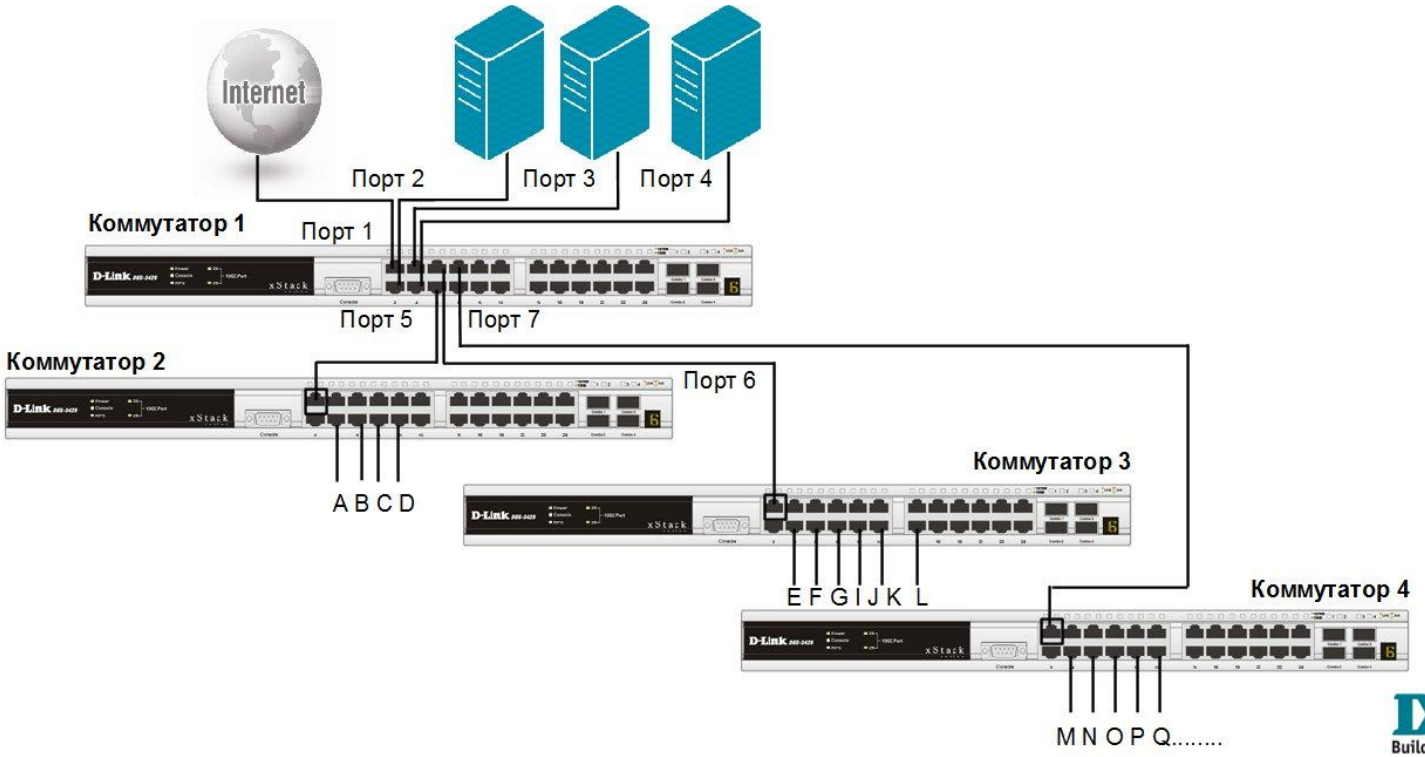
Настройка коммутатора

```
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
```

Функция сегментации 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.



D-Link
Building Networks for People

Функция сегментации 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

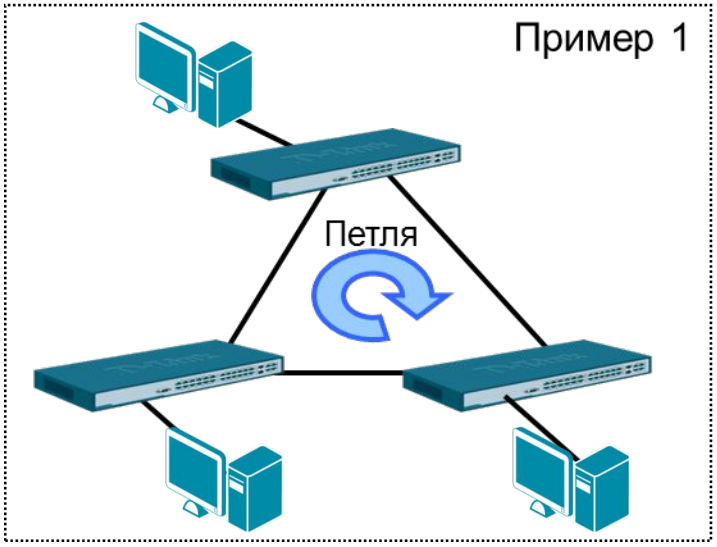
```
config traffic_segmentation 1 forward_list 1-26
config traffic_segmentation 2-26 forward_list 1
```

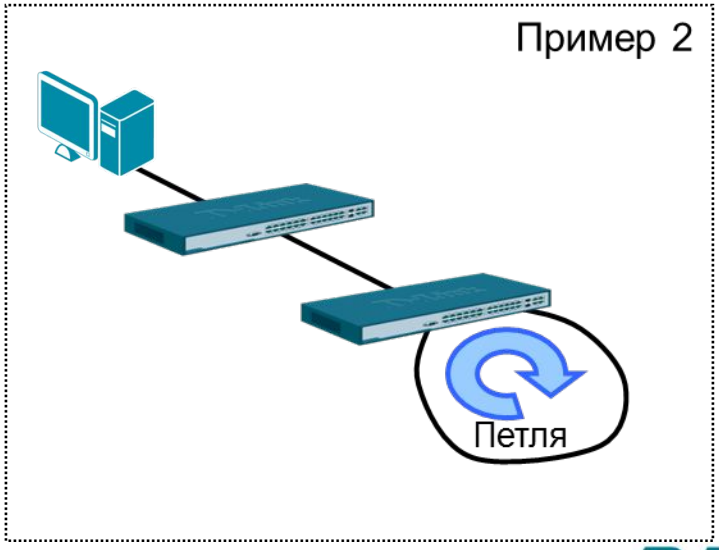
Организация беспетлевых топологий на основе протоколов STP

Ключевые задачи управляемого коммутатора L2

1. Коммутация трафика на канальном уровне;
2. Управление имеющимися подключениями;
3. Управление трафиком.

Для обеспечения надежной работы по всем пунктам в сетевой топологии Ethernet не должно быть петель.





Семейство протоколов STP

STP (**Spanning Tree Protocol**) — семейство сетевых протоколов, предназначенное для автоматического исключения циклов (петель коммутации) из топологии сети на канальном уровне в Ethernet-сетях.

Первоначально протокол STP был разработан в 1985 году Радией Перлман и затем описан в стандарте **IEEE 802.1D** в 1990 году.

Позже появились:

- открытые модификации протокола: **RSTP, MSTP**;
- проприетарные модификации от Cisco: **PVST, PVST+**.

Семейство протоколов STP

Основная задача STP — предотвратить появление петель в сетях Ethernet на канальном уровне путем простого блокирования всех избыточных линков на определенный период времени.

Попутные вопросы:

- какой линк из двух (трех, четырех…) блокировать?
- как определить, что основной линк «упал», и пора включать запасной?
- Как понять, что в сети образовалась петля?

Принцип работы STP

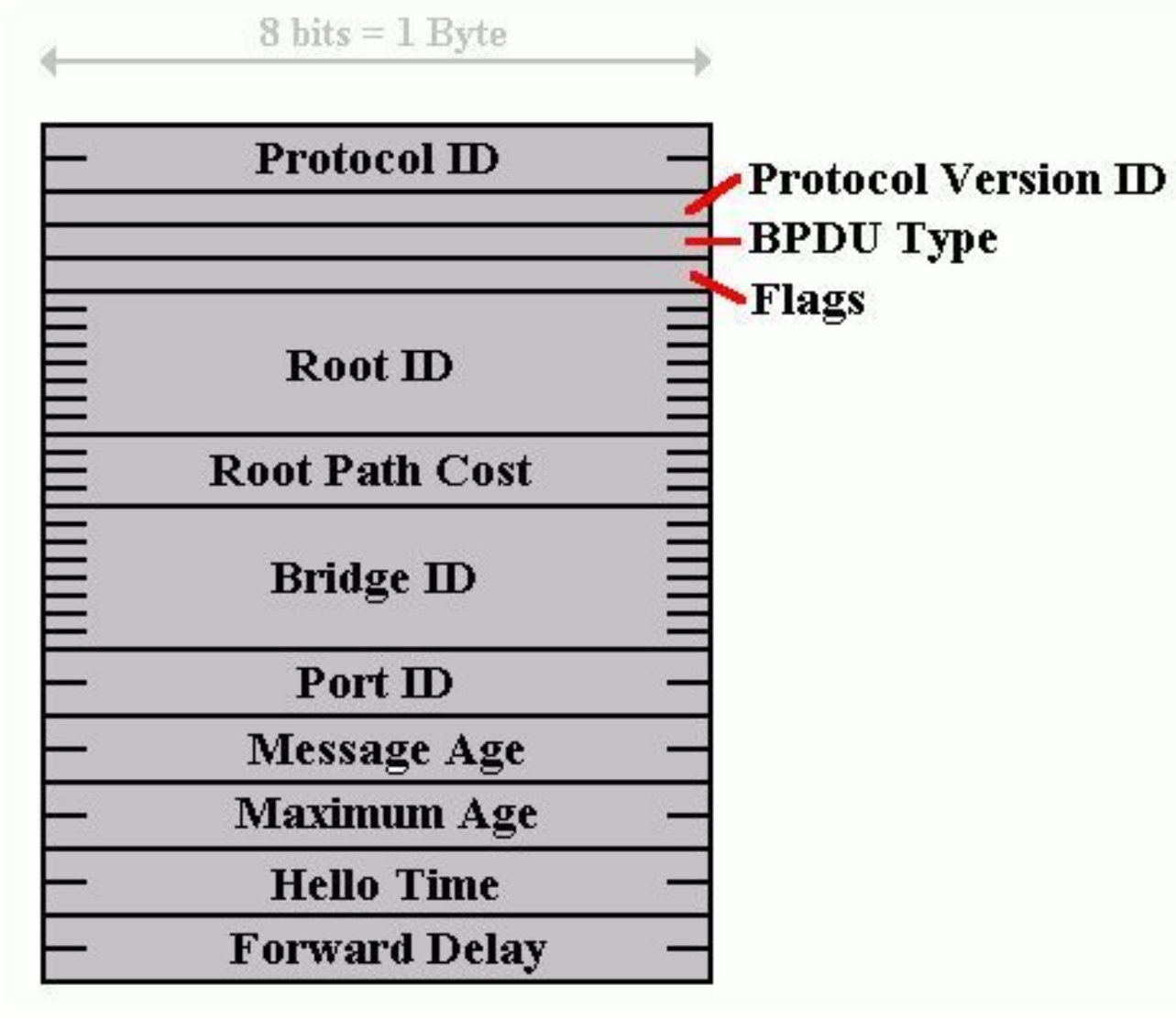
Построение беспетельной топологии между коммутаторами происходит на основе обмена служебными кадрами **BPDU**.

BPDU (Bridge Protocol Data Unit) – Ethernet-кадр, рассылаемый на мультикастовый ethernet-адрес **01-80-c2-00-00-00** каждые 2 секунды (по умолчанию) и прослушиваемый всеми коммутаторами с включенным STP.

Существует три типа кадров BPDU:

- **Configuration BPDU (CBPDU)** – конфигурационный кадр BPDU, который используется для вычисления связующего дерева;
- **Topology Change Notification (TCN)** – уведомление об изменении топологии сети;
- **Topology Change Notification Acknowledgement (TCA)** – подтверждение о получении уведомления об изменении топологии сети.

Формат кадра BPDU



Принцип работы STP

Для построения беспетельной топологии на основе протокола STP необходимо определить роли коммутаторов в сети:

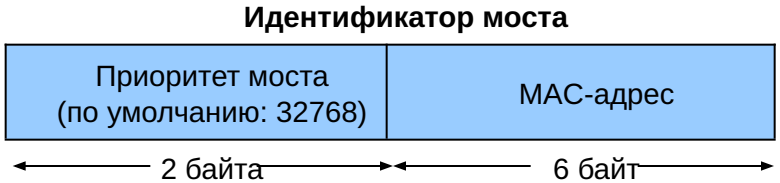
- **Корневой мост** (Root Bridge) - это коммутатор, поддерживающий протокол STP и являющийся «точкой отсчета» топологии;
- **Некорневой мост** – это коммутатор, поддерживающий протокол STP и принимающий участие в построении топологии;
- **Прочие мосты** – это коммутаторы НЕ участвующие в топологии STP.

Принцип работы STP

1. Определение корневого моста

Каждый коммутатор, участвующий в топологии STP, определяет свой *уникальный идентификатор моста (Bridge ID)* и в самом начале построения топологии меряется им с помощью BPDU с другими коммутаторами. Корневым мостом становится устройство **с наименьшим** значением *Bridge ID*.

Идентификатор моста – это 8-байтное поле, которое состоит из 2-х частей:



При определении корневого моста:

- вначале сравниваются приоритеты. Устройство с наименьшим значением приоритета становится корневым мостом;
- если приоритеты равны, сравниваются MAC-адреса. Устройство с наименьшим MAC-адресом становится корневым мостом.

Принцип работы STP

2. Выбор корневого порта у каждого НЕкорневого коммутатора

Корневой порт (Root Bridge Port) - порт на некорневом коммутаторе, который обеспечивает его подключение к корневому коммутатору по кратчайшему пути.

Наилучший путь определяется по стоимости при прохождении кадра BDPU от некорневого коммутатора до корневого и связан с полем кадра “Root Path Cost” по алгоритму:

- Корневой мост посылает BPDU с полем Root Path Cost, равным нулю;
- Каждый последующий некорневой мост при получении кадра BPDU по цепочке «добавляет» к стоимости очередное значение согласно таблице:

Скорость порта	**Стоимость STP (802.1d)**
10 Mbps	100
100 Mbps	19
1 Gbps	4
10 Gbps	2

Принцип работы STP

3. Выбор назначенных портов у КОРНЕВОГО коммутатора

Назначенный порт (**Designated port**) – порт на корневом мосте, которым он соединяется с некорневыми мостами, обеспечивая при этом кратчайший и единственный путь до каждого из них и, тем самым, беспетельную топологию STP.

- Назначенный порт сегмента определяется путем сравнения значений стоимости пути всех маршрутов от данного моста до корневого. Им становится порт, имеющий **наименьшее** значение стоимости, среди всех портов с альтернативными маршрутами.

- Если минимальные значения стоимости пути окажутся одинаковыми у двух или нескольких портов, то для выбора назначенного порта сегмента STP принимает решение на основе последовательного сравнения идентификаторов мостов и идентификаторов портов в кадрах BPDU.

- После выбора корневых и назначенных портов все остальные порты на корневом и всех некорневых коммутаторах сети БЛОКИРУЮТСЯ.

Принцип работы STP

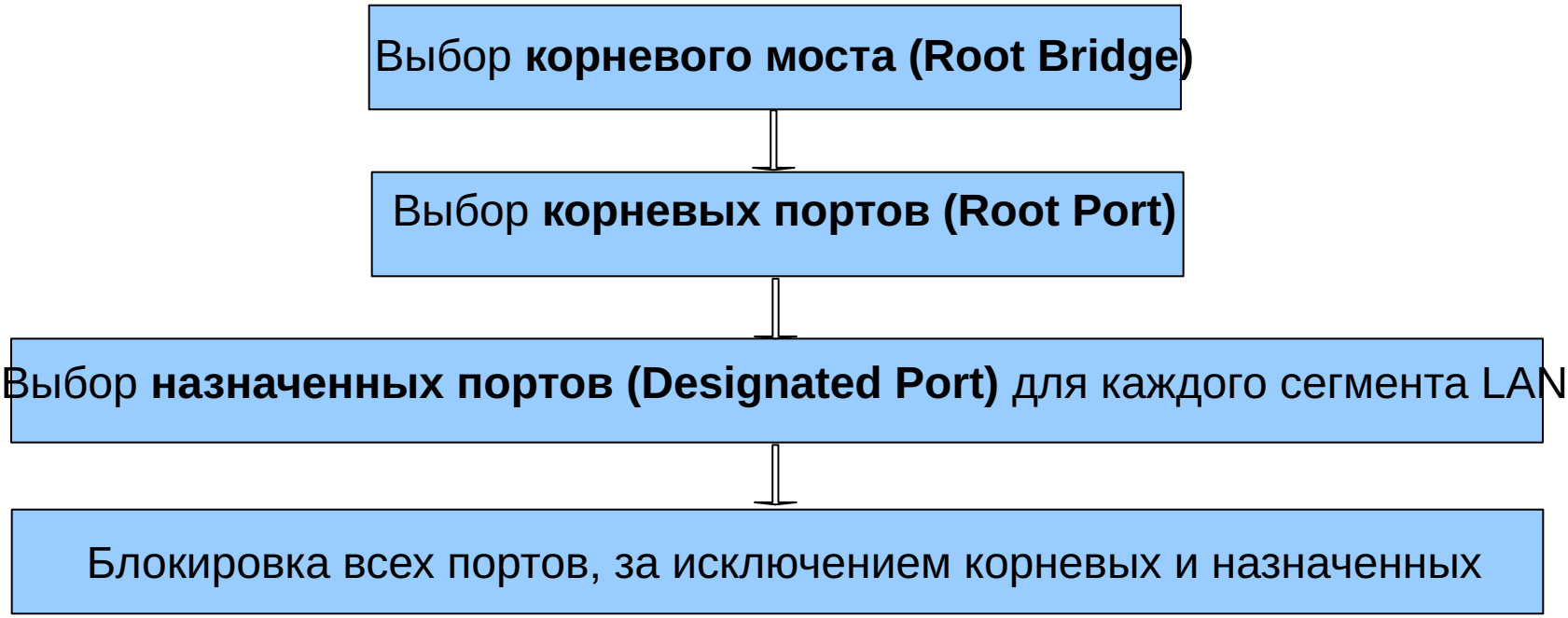
Вопрос. Как быть с портами, к которым подключены конечные узлы?

При настройке STP администратор должен явно указать коммутатору какие именно порты являются граничными (edge-портами) и не участвуют при построении топологии.

Пример:

```
config stp ports 1-24 edge true
```

Обобщенный принцип работы STP на схеме



Принцип работы STP

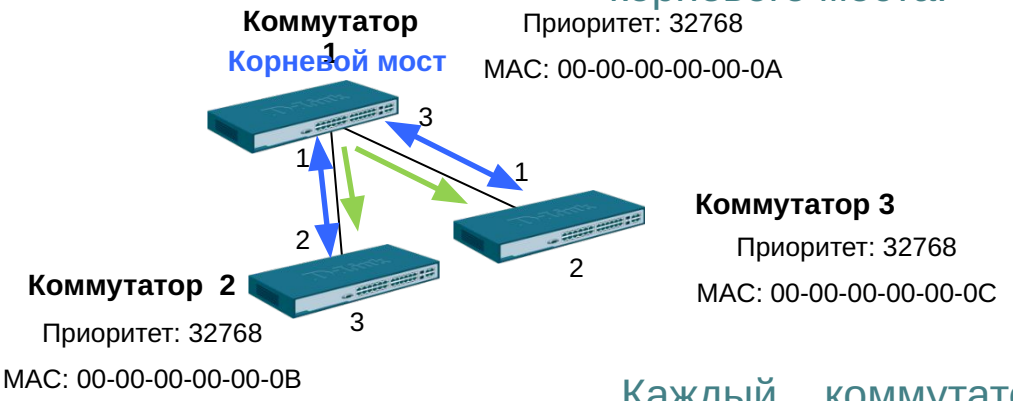
Пример выбора корневого моста

3

После выбора корневого моста, только он рассылает BPDU. Остальные коммутаторы их перенаправляют.

1

В первый момент времени каждый коммутатор считает, что он является корневым мостом и рассылает BPDU, в которых указывает себя в качестве корневого моста.



2

Каждый коммутатор сравнивает свой идентификатор моста с идентификатором корневого моста, указанным в полученном BPDU. Если он меньше, коммутатор заменяет значение идентификатора корневого моста в полученном BPDU на значение своего идентификатора, чтобы быть выбранным в качестве корневого моста.

Слайд анимирован

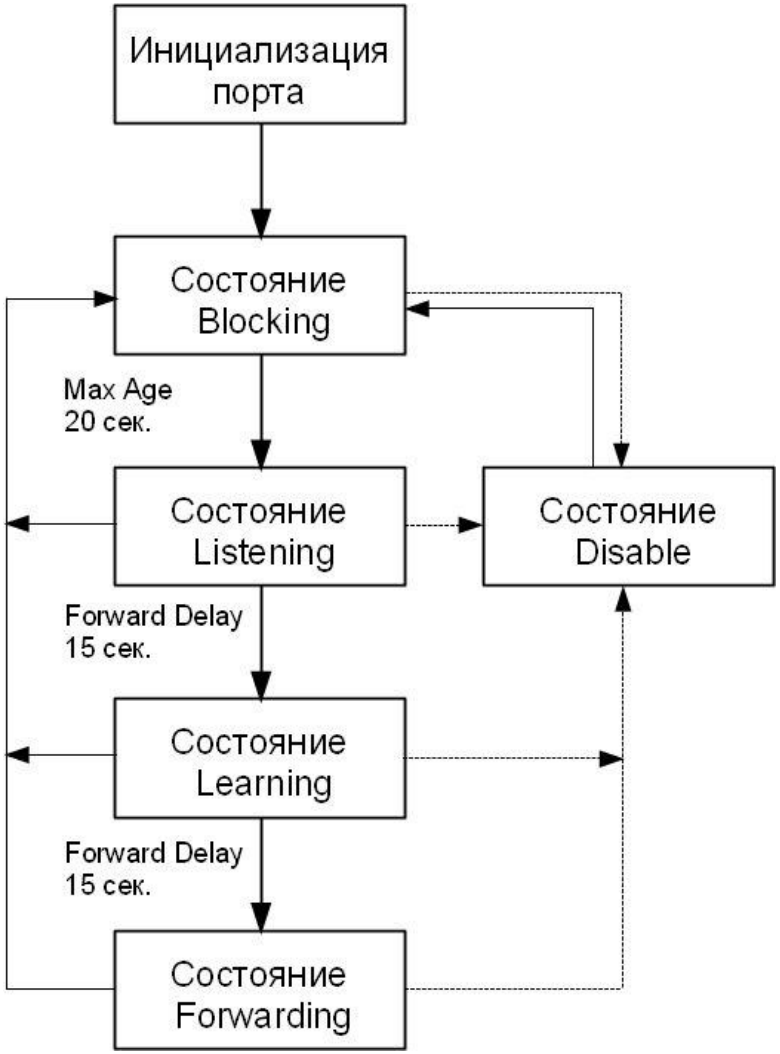
Принцип работы STP

Состояния портов, участвующих в топологии STP

- **Блокировка (blocking):** блокированный порт не шлет ничего. Это состояние предназначено для предотвращения петель в сети. Блокированный порт, тем не менее, слушает BPDU (чтобы быть в курсе событий, это позволяет ему, когда надо, разблокироваться и начать работать);
- **Прослушивание (listening):** порт слушает и сам отправляет BPDU, кадры с обычными данными не перенаправляет;
- **Обучение (learning):** порт слушает, сам отправляет BPDU, а также вносит изменения в свою FDB, но данные не перенаправляет;
- **Перенаправление\пересылка (forwarding):** это обычное состояние рабочего порта (посылает/принимает BPDU, и с данными оперирует, и участвует в поддержании FDB);
- **Отключен (disabled):** состояние administratively down, по факту отключен командой **shutdown**. Понятное дело, ничего делать не может вообще, пока вручную не включат.

Принцип работы STP

Состояния портов STP



Принцип работы STP

Таймеры STP

- **Hello Time** – это интервал времени, через который корневой мост отправляет конфигурационные BPDU. Значение таймера Hello Time **по умолчанию 2 секунды**: диапазон возможных значений от 1 до 10 секунд.
- **Forward Delay** – это интервал времени, в течение которого порт коммутатора находится в состояниях «Прослушивание» и «Обучение». Значение таймера Forward Delay **по умолчанию 15 секунд**: диапазон возможных значений от 4 до 30 секунд.
- **Max Age** – это интервал времени, в течение которого коммутатор хранит параметры текущей конфигурации связующего дерева. Значение таймера Max Age **по умолчанию 20 секунд**: диапазон возможных значений от 6 до 40 секунд.

Принцип работы STP

Пример настройки протокола STP

Настройка коммутатора 1

//Включение STP

- `enable stp`
- `config stp version stp`

//Установка приоритета вручную, чтобы именно коммутатор 1 был выбран корневым мостом

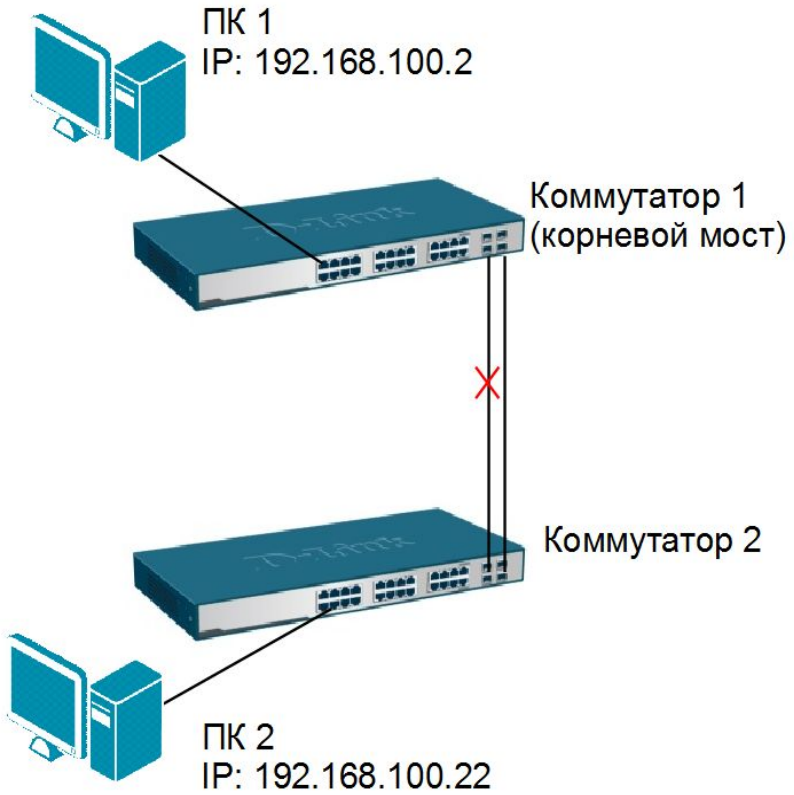
- `config stp priority 4096 instance_id 0`

//Указывание граничных портов, не участвующих при построении топологии STP

- `config stp ports 1-24 edge true`

Настройка коммутатора 2

- `enable stp`
- `config stp version stp`
- `config stp ports 1-24 edge true`



Протокол RSTP

Rapid Spanning Tree Protocol (RSTP) является развитием протокола STP и в настоящее время определен в стандарте **IEEE 802.1D-2004** (ранее был определен в стандарте **IEEE 802.1w-2001**).

ОСНОВНОЕ ПРЕИМУЩЕСТВО ПЕРЕД STP:

- Протокол RSTP значительно ускоряет время построения беспетлевой топологии за счет мгновенного перехода корневых и назначенных портов в состояние продвижения трафика.

STP vs. RSTP

STP (802.1d)	**RSTP (802.1w)**
В уже сложившейся топологии только корневой свич шлет BPDU, остальные ретранслируют	Все свичи шлют BPDU в соответствии с hello-таймером (2 секунды по умолчанию)
Состояния портов	
— блокировка (blocking) — прослушивание (listening) — обучение (learning) — перенаправление\пересылка (forwarding) — отключен (disabled)	— отбрасывание (discarding), заменяет disabled, blocking и listening — learning — forwarding
Роли портов	
— корневой (root), участвует в пересылке данных, ведет к корневому свичу — назначенный (designated), тоже работает, ведет от корневого свича — неназначенный (non-designated), не участвует в пересылке данных	— корневой (root), участвует в пересылке данных — назначенный (designated), тоже работает — дополнительный (alternate), не участвует в пересылке данных — резервный (backup), тоже не участвует

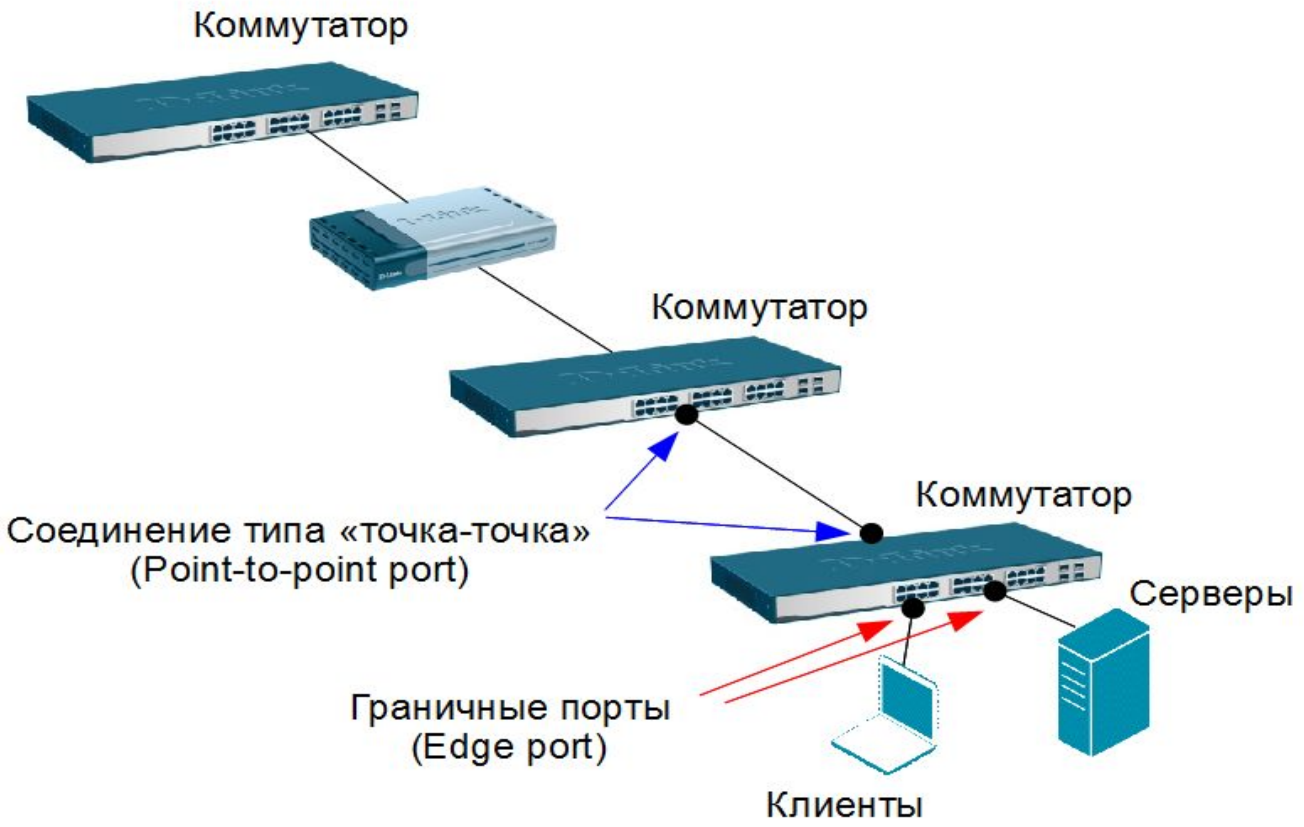
STP vs. RSTP

STP (802.1d)	**RSTP (802.1w)**
Механизмы работы	
Использует таймеры: Hello (2 секунды) Max Age (20 секунд) Forward delay timer (15 секунд)	Использует процесс proposal and agreement (предложение и соглашение)
Свич, обнаруживший изменение топологии, извещает корневой свич, который, в свою очередь, требует от всех остальных очистить их записи о текущей топологии в течение forward delay timer	Обнаружение изменений в топологии влечет немедленную очистку записей
Если не-корневой свич не получает hello- пакеты от корневого в течение Max Age, он начинает новые выборы	Начинает действовать, если не получает BPDU в течение 3 hello-интервалов
Последовательное прохождение порта через состояния Blocking (20 сек) — Listening (15 сек) — Learning (15 сек) — Forwarding	Быстрый переход к Forwarding для p2p и Edge-портов

Протокол RSTP

Протокол RSTP явно определяет тип портов:

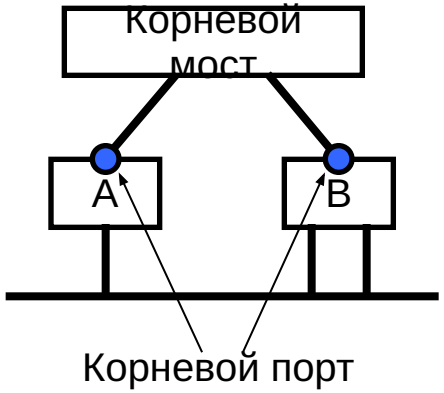
- граничный порт (*edge port*);
- порт «точка-точка» (point-to-point port).

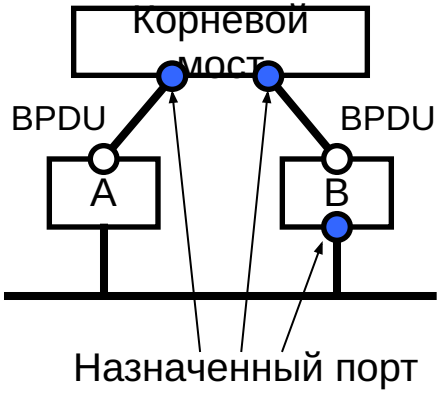


Протокол RSTP

Роли портов типа «точка-точка»

- **Корневой порт (Root Port) -** порт коммутатора, который имеет по сети кратчайшее расстояние (в терминах стоимости пути) до корневого коммутатора;
- **Назначенный порт (Designated Port) -** порт является назначенным, если он посылает BPDU с наилучшими параметрами в тот сегмент, к которому подключен.

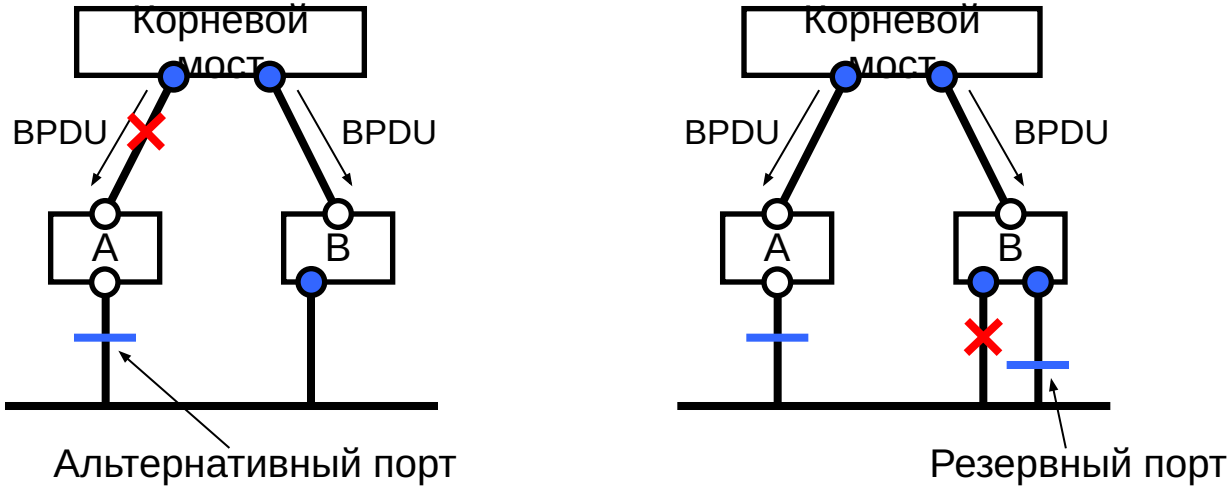




Протокол RSTP

Роли портов RSTP

- **Альтернативный порт (Alternate Port)** – это порт, который предлагает альтернативный основному маршруту путь в направлении корневого моста и может заменить корневой порт в случае выхода его из строя;
- **Резервный порт (Backup Port)** – это порт, который предназначен для резервирования пути, предоставляемого назначенным портом в направлении сегментов сети, НЕ ГАРАНТИРУЕТ альтернативное подключение к корневому мосту.



Протокол RSTP

Состояние портов RSTP

В протоколе MSTP определены состояния, в которых могут находиться порты, аналогичные протоколу RSTP:

- **Learning** («Обучение») – порт может принимать/отправлять кадры BPDU, изучать MAC-адреса и строить таблицу коммутации. Порт в этом состоянии не передает пользовательские кадры;
- **Forwarding** («Продвижение») – в этом состоянии порт может передавать пользовательские кадры, изучать новые MAC-адреса и принимать/отправлять кадры BPDU;
- **Discarding** («Отбрасывание») – в этом состоянии порт может только принимать кадры BPDU, передача пользовательского трафика и изучение MAC-адресов не выполняется.

Протокол RSTP

Стоимости пути в RSTP

Параметр	Скорость канала	Рекомендованное значение	Рекомендованный диапазон	Диапазон значений
Стоимость пути	10 Мбит/с	2 000 000	200 000–20 000 000	1–200 000 000
Стоимость пути	100 Мбит/с	200 000	20 000–2 000 000	1–200 000 000
Стоимость пути	1 Гбит/с	20 000	2 000–200 000	1–200 000 000
Стоимость пути	10 Гбит/с	2 000	200–20 000	1–200 000 000

Протокол RSTP

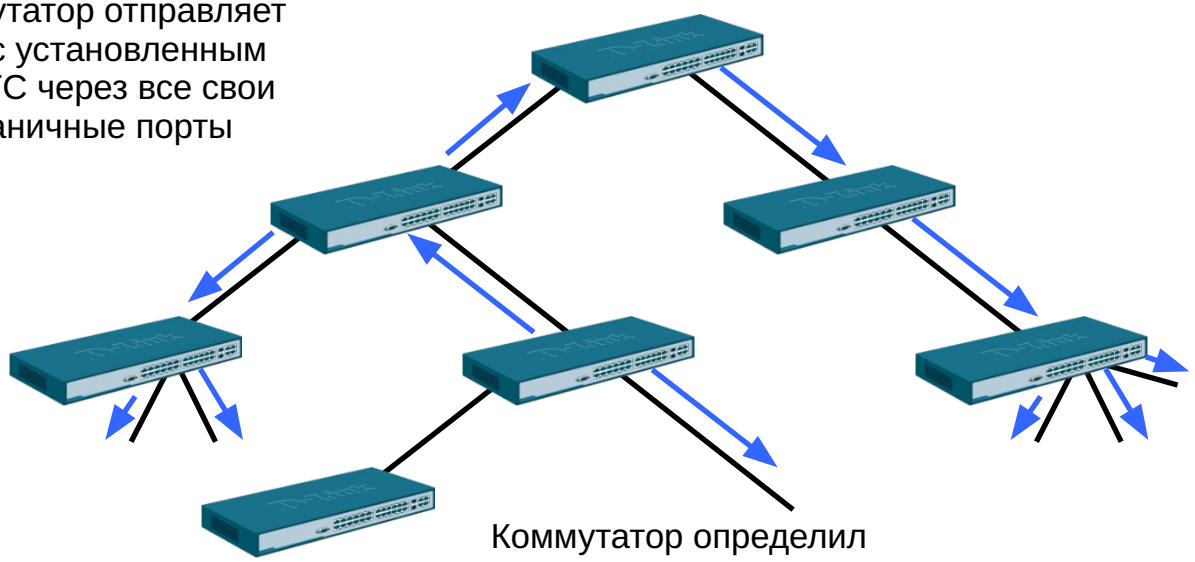
ВЫВОДЫ О РОЛИ ПОРТОВ

- В RSTP остались такие роли портов, как корневой и назначенный;
- Заблокированные порты разделили на две новых роли: Alternate и Backup. Alternate — это резервный корневой порт, а backup — резервный назначенный порт. Как раз в этой концепции резервных портов и кроется одна из причин быстрого переключения в случае отказа;
- Общий принцип RSTP меняет поведение системы в целом: вместо реактивной (которая начинает искать решение проблемы только после того, как она случилась) система становится проактивной, заранее просчитывающей “пути отхода” еще до появления проблемы;
- Для того, чтобы в случае отказа основного переключится на резервный линк, RSTP не нужно заново просчитывать топологию, он просто переключится на запасной, заранее просчитанный.

Протокол RSTP

Пример изменения топологии

2. Коммутатор отправляет BPDU с установленным битом TC через все свои негранничные порты



Коммутатор определил изменение топологии

1. Запускается таймер TC While и удаляются MAC-адреса, ассоциированные со всеми негранничными портами

Слайд анимирован

Принцип работы RSTP

Пример настройки протокола RSTP

Настройка коммутатора 1

//Включение RSTP

- `enable stp`
- `config stp version rstp`

//Установка приоритета вручную, чтобы именно коммутатор 1 был выбран корневым мостом

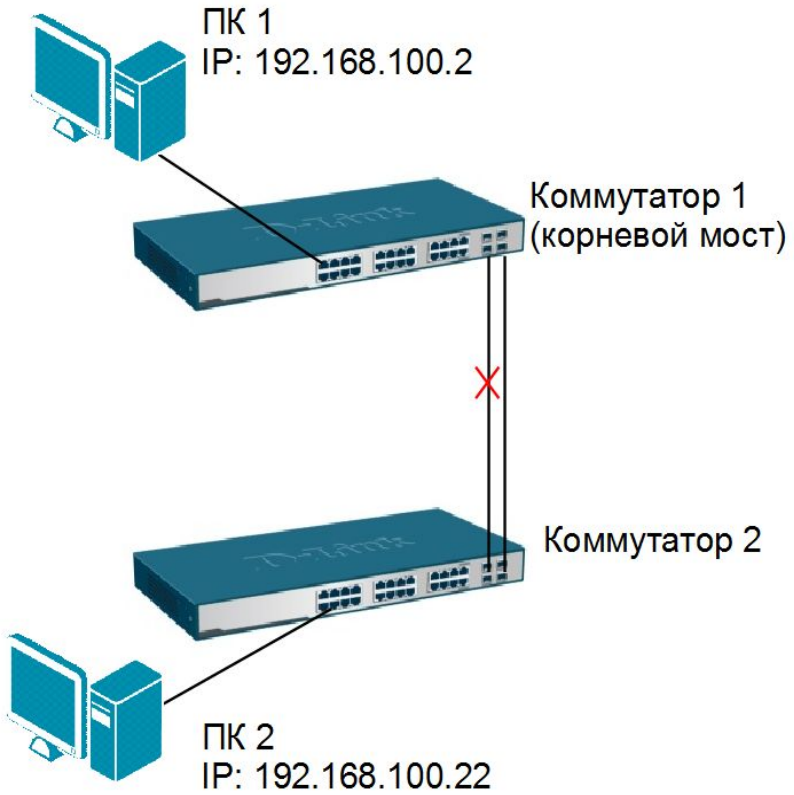
- `config stp priority 4096 instance_id 0`

//Указывание граничных портов, не участвующих при построении топологии RSTP

- `config stp ports 1-24 edge true`

Настройка коммутатора 2

- `enable stp`
- `config stp version rstp`
- `config stp ports 1-24 edge true`



Протокол RSTP

Обратная совместимость с STP

Протокол RSTP может взаимодействовать с оборудованием, поддерживающим STP и автоматически преобразовывать кадры BPDU в формат 802.1D.

При выборе между STP и RSTP следует помнить, что **преимущество быстрой сходимости** явно у протокола RSTP за счет:

- возможности некорневых мостов самостоятельно принимать решение о перестроении конфигурации;
- наличия альтернативных и резервных портов,
- меньшего числа состояний портов и укороченных таймеров.

Протокол MSTP

Multiple Spanning Tree Protocol (MSTP) – расширение протокола RSTP. Первоначально протокол MSTP был определен в стандарте IEEE 802.1s, но позднее был добавлен в стандарт **IEEE 802.1Q-2003**.

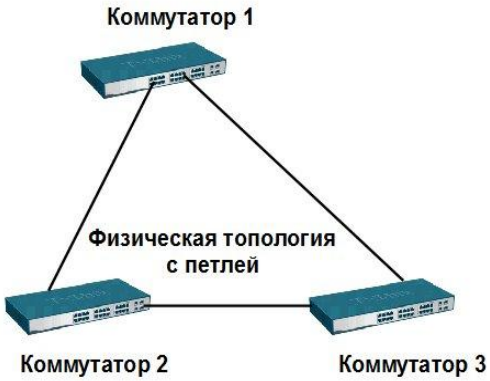
Протокол MSTP обеспечивает быструю сходимость сети и позволяет настраивать отдельное связующее дерево для любой VLAN или группы VLAN, создавая множество маршрутов передачи трафика, и позволяя осуществлять балансировку нагрузки.

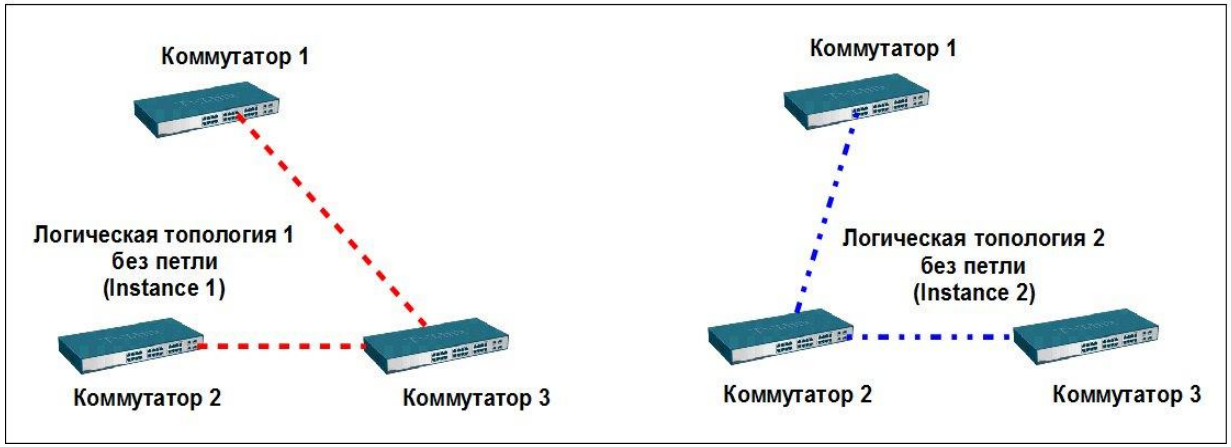
Протокол MSTP обратно совместим с протоколами STP и RSTP.

Протокол MSTP

Понятие региона MST

- Протокол MSTP делит коммутируемую сеть на **регионы MST** (*Multiple Spanning Tree (MST) Region*), представляющие собой набор физически подключенных друг к другу коммутаторов. Каждый из регионов может содержать множество **копий связующих деревьев (*Multiple Spanning Tree Instance, MSTI*)** с независимой друг от друга топологией.



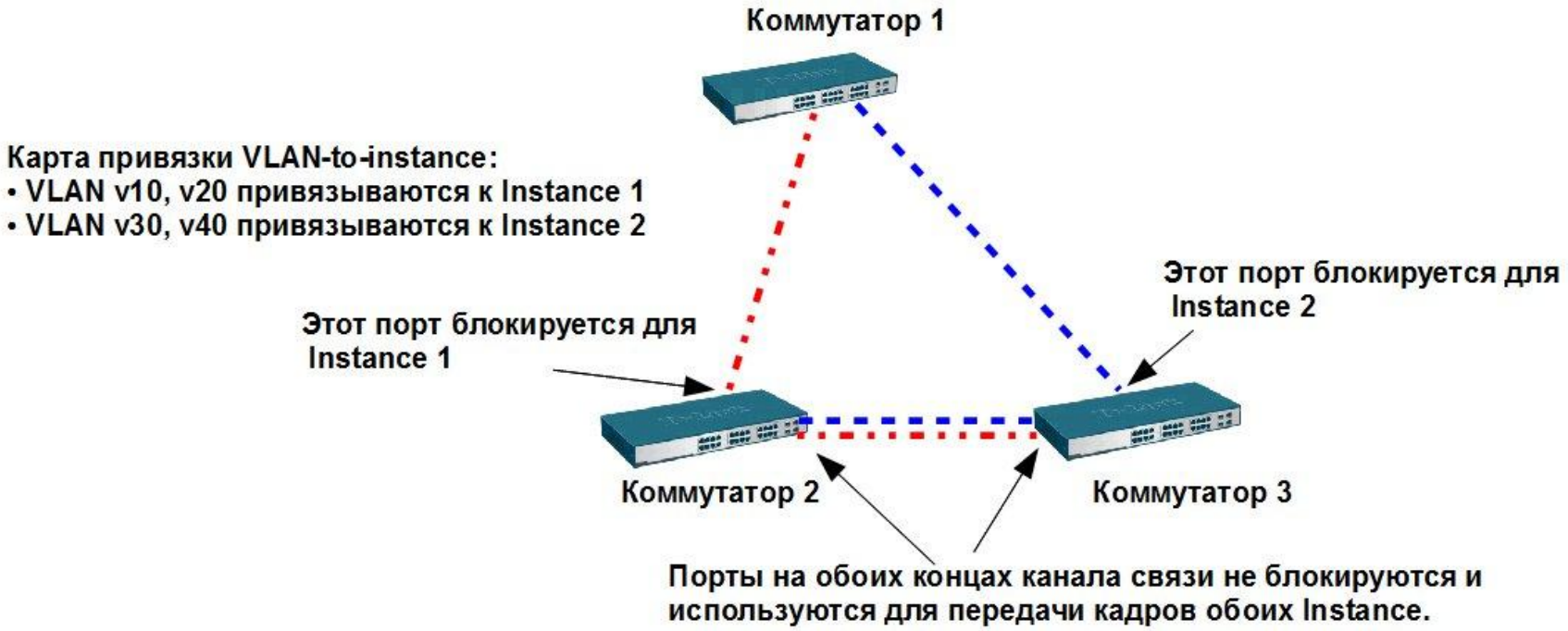


Протокол MSTP

Регион MST

Для того чтобы два и более коммутатора принадлежали одному региону MST, они должны обладать одинаковой конфигурацией MST.

- Конфигурация MST включает:
  - номер ревизии MSTP (*MSTP revision level number*);
  - имя региона (*Region name*);
  - карту привязки VLAN к копии связующего дерева (*VLAN-to-instance mapping*).



Протокол MSTP

Сценарий настройки протокола MSTP на коммутаторах

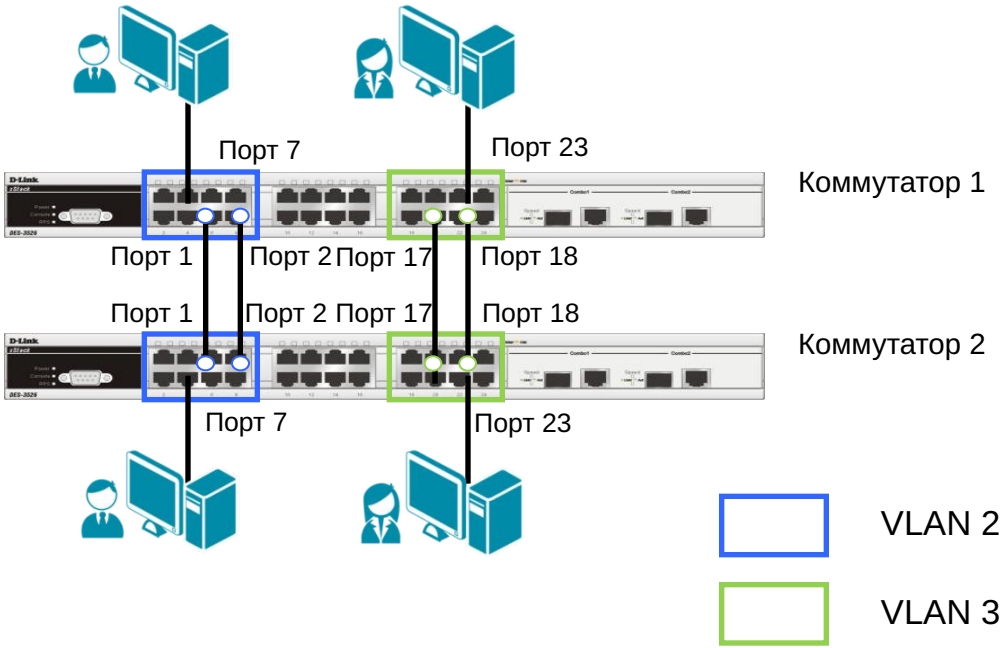
Основные шаги, которые позволяют настроить протокол MSTP на коммутаторах D-Link:

1. Активизировать MSTP на всех устройствах;
2. Настроить граничные порты;
3. Настроить имя MST-региона и ревизию;
4. Создать MSTI и карту привязки VLAN к MSTI;
5. Задать приоритет STP для выбора корневого моста (по умолчанию используется приоритет 32768).

Протокол MSTP

Пример настройки

- В сети созданы две виртуальные локальные сети – VLAN v2 и VLAN v3. Каждая VLAN привязывается к одной копии связующего дерева.



Протокол MSTP

- **Настройка коммутатора 1**
- Создание VLAN

```
config vlan default delete 1-8,17-24
create vlan v2 tag 2
config vlan v2 add untagged 1-8
create vlan v3 tag 3
config vlan v3 add untagged 17-24
```

- Настройка MSTP

```
enable stp
config stp version mstp
config stp mst_config_id name dlink
revision_level 1
create stp instance_id 2
config stp instance_id 2 add_vlan 2
create stp instance_id 3
config stp instance_id 3 add_vlan 3
config stp priority 4096 instance_id 2
config stp priority 4096 instance_id 3
config stp ports 7,23 edge true
```

Настройка коммутатора 2

- Создание VLAN

```
config vlan default delete 1-8,17-24
create vlan v2 tag 2
config vlan v2 add untagged 1-8
create vlan v3 tag 3
config vlan v3 add untagged 17-24
```

- Настройка MSTP

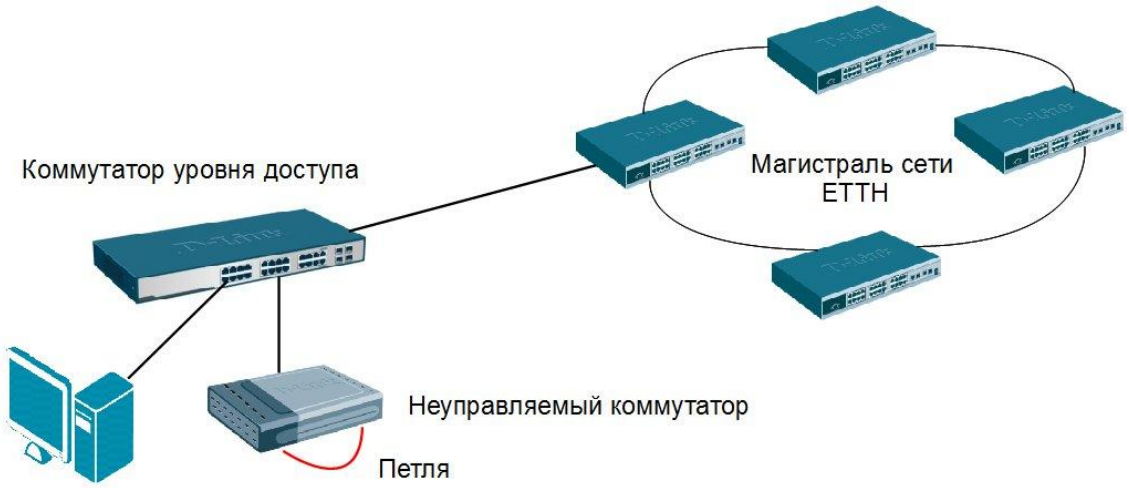
```
enable stp
config stp version mstp
config stp mst_config_id name dlink revision_level
    1
create stp instance_id 2
config stp instance_id 2 add_vlan 2
create stp instance_id 3
config stp instance_id 3 add_vlan 3
config stp ports 7,23 edge true
```

Дополнительные функции защиты от петель

Функции защиты от петель

Функция LoopBack Detection (LBD) обеспечивает дополнительную защиту от образования петель на уровне 2 модели OSI.

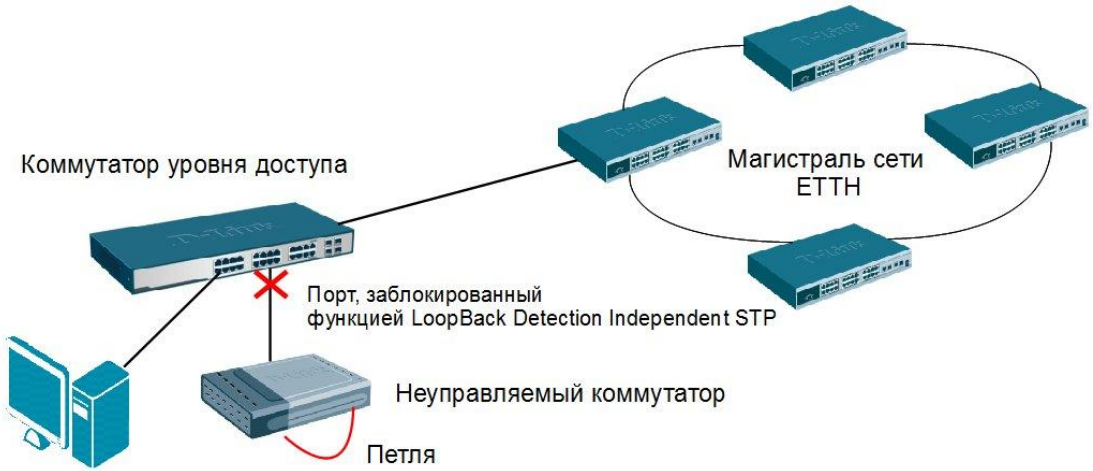
В коммутаторах D-Link функция LBD реализуется под названием LBD LoopBack Detection Independent STP.



Функции защиты от петель

Функция LoopBack Detection Independent STP

- Наличие петли обнаруживается путем отправки портом специального служебного кадра ECTP (Ethernet Configuration Testing Protocol). При получении кадра ECTP этим же портом, он блокируется на указанное в таймере время.
- Функция LoopBack Detection Independent STP версии 4.03 также может определять петли, возникающие между портами одного коммутатора.

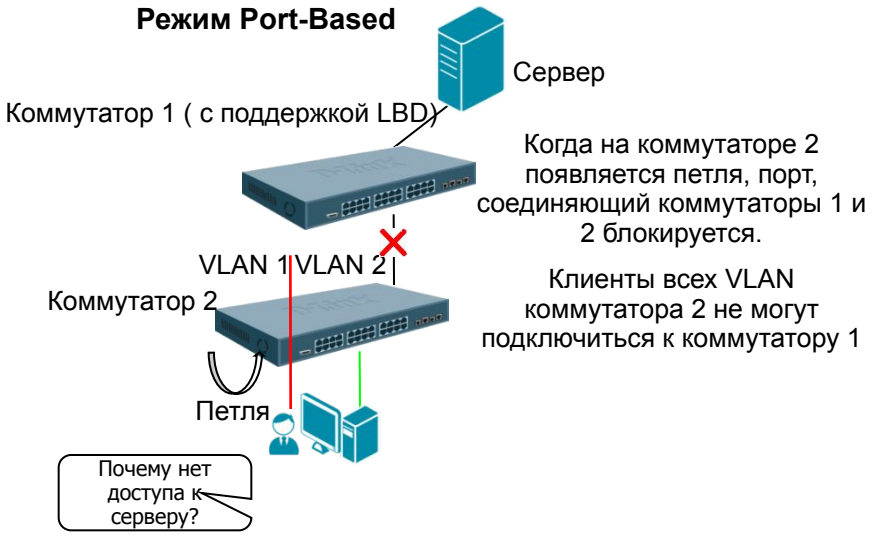


Функции защиты от петель

Функция LoopBack Detection Independent STP

Существуют два режима работы этой функции:

- Port-Based: при обнаружении петли происходит автоматическая блокировка порта, и никакой трафик через него не передается.
- VLAN-Based (начиная с LBD версии v.4.00): порт будет заблокирован для передачи трафика только той VLAN, в которой обнаружена петля. Остальной трафик через этот порт будет передаваться.



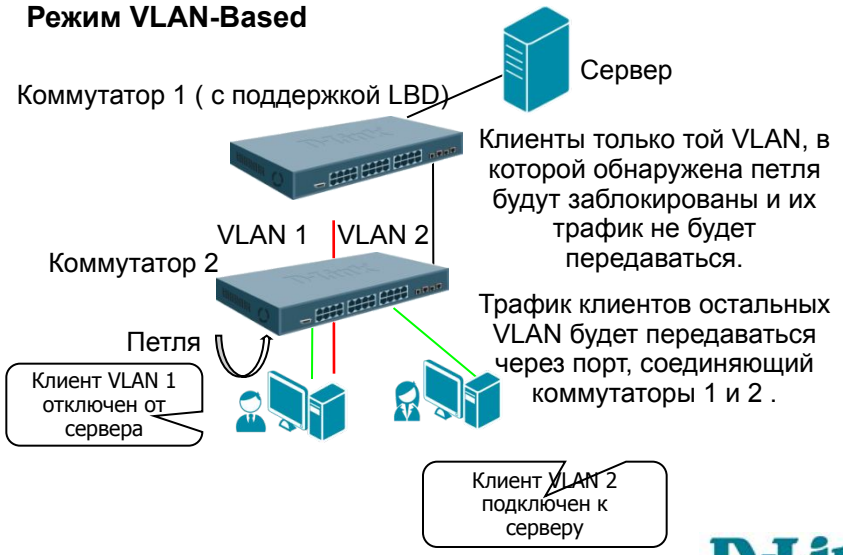


Рисунок анимирован

D-Link
Building Networks for People

Функции защиты от петель

Настройка функции LoopBack Detection Independent STP (Port-Based)

- `enable loopdetect`
- `config loopdetect recover_timer 60`
- `config loopdetect interval 10`
- `config loopdetect mode port-based`
- `config loopdetect ports 1-24 state enabled`

Настройка функции LoopBack Detection Independent STP (VLAN-Based)

- `enable loopdetect`
- `config loopdetect recover_timer 60`
- `config loopdetect interval 10`
- `config loopdetect mode vlan-based`
- `config loopdetect ports 1-24 state enabled`

Важные замечания:
recover_timer – интервал времени в секундах, через который будет проверяться статус заблокированного функцией LBD порта. Если установить значение таймера равным 0, заблокированный порт не сможет быть автоматически разблокирован, и для его восстановления потребуется вмешательство администратора. Значение таймера задается глобально на коммутаторе.
loopdetect interval – временной интервал в секундах между отсылаемыми кадрами ECTP (Ethernet Configuration Testing Protocol).

Ваши вопросы…