Технологии, применяемые при построении сетей на основе коммутаторов D-Link

Базовый функционал

Зайцев Александр, консультант по проектам

e-mail: azaitsev@dlink.ru

D-Link®
Building Networks for People

Обзор VLAN

Понятие виртуальной локальной сети

- Широковещательный домен
  - Логический сегмент сети.
  - Любое устройство может передавать данные всем устройствам в сегменте.
  - Для отправки кадром 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.

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*.

802.1q – VLAN на базе меток

Термины 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.
- **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

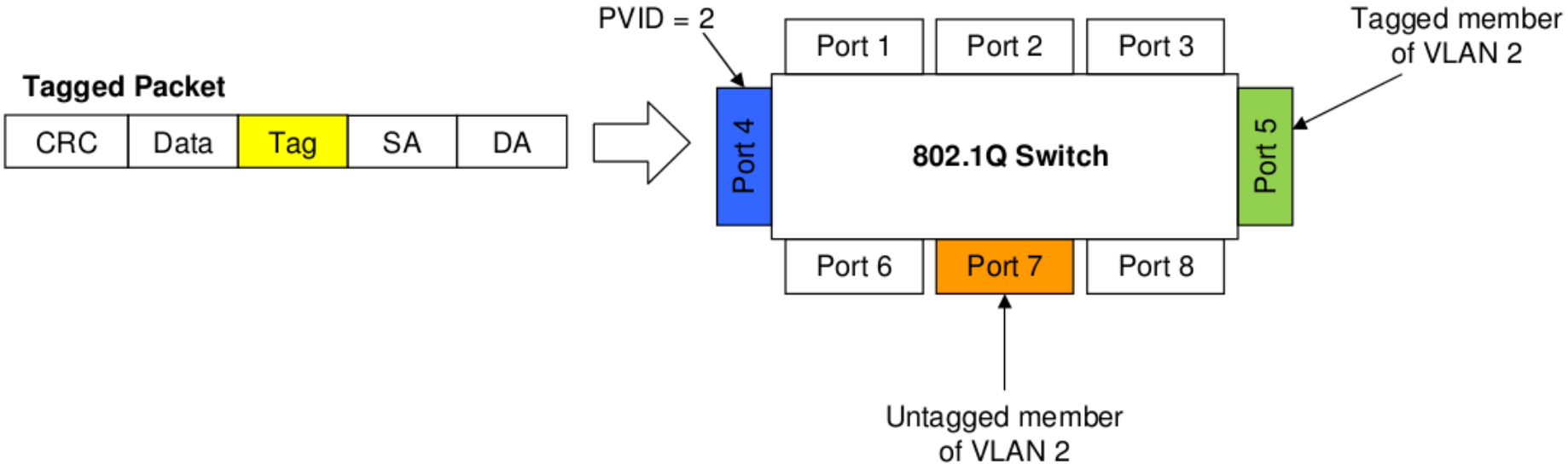
Адрес назначения (DA)	Адрес источника (SA)	Данные (Data)	Контрольная последовательность кадра (CRC)

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

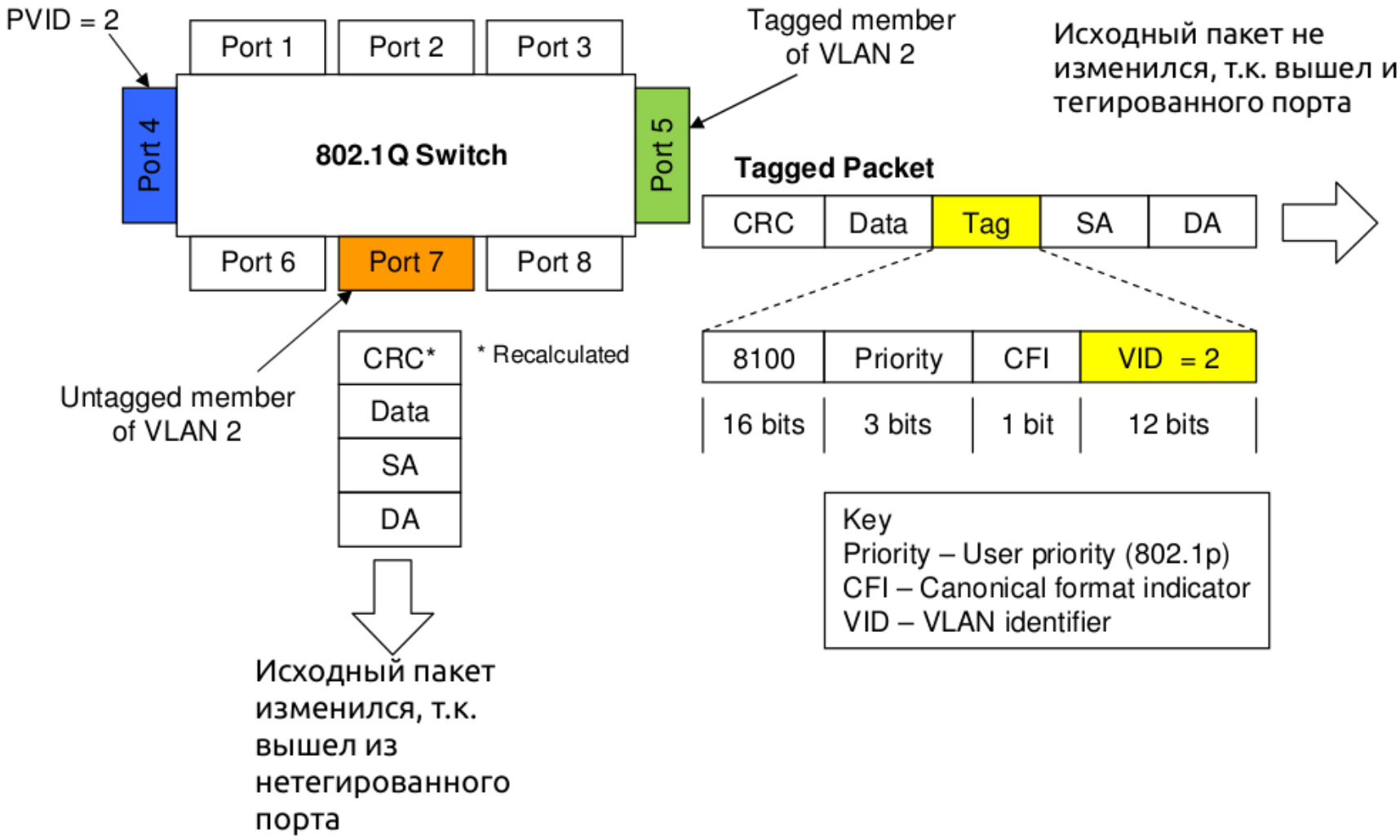
Маркированный входящий пакет



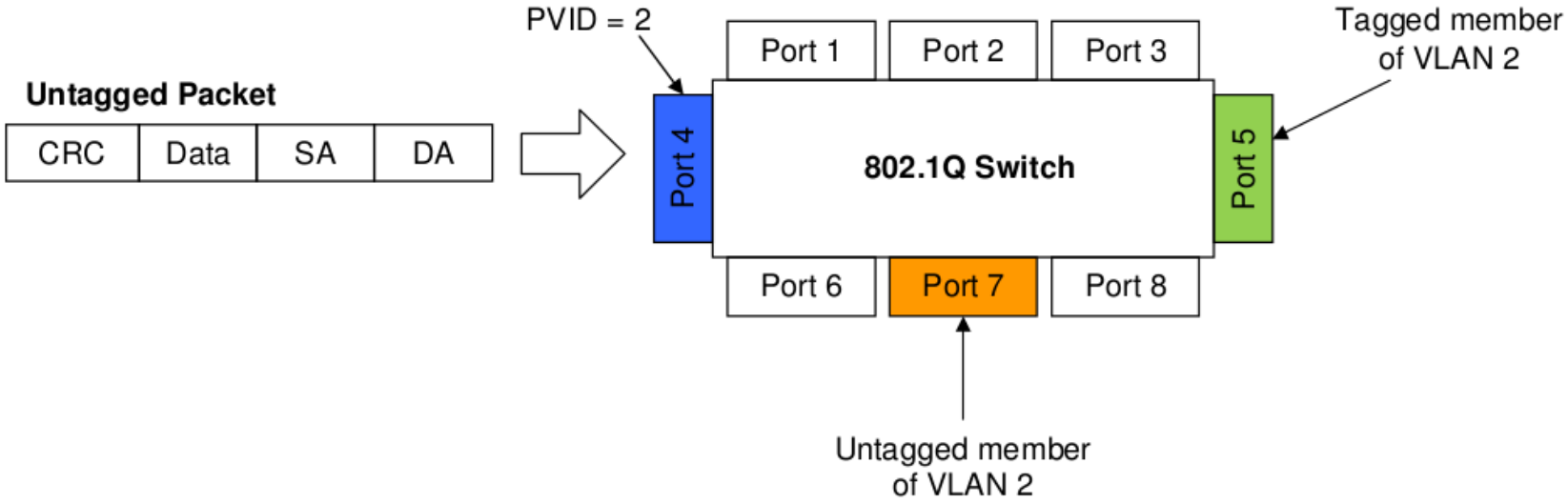
- Входящий пакет назначен для VLAN 2 потому, что в пакете есть маркер принадлежности
- Порт 5 маркирован как Выходящий для VLAN 2
- Порт 7 не маркирован как Выходящий для VLAN 2

- Пакеты перенаправляются на порт 5 с маркером
- Пакеты перенаправляются на порт 7 без маркера

Маркированный входящий пакет



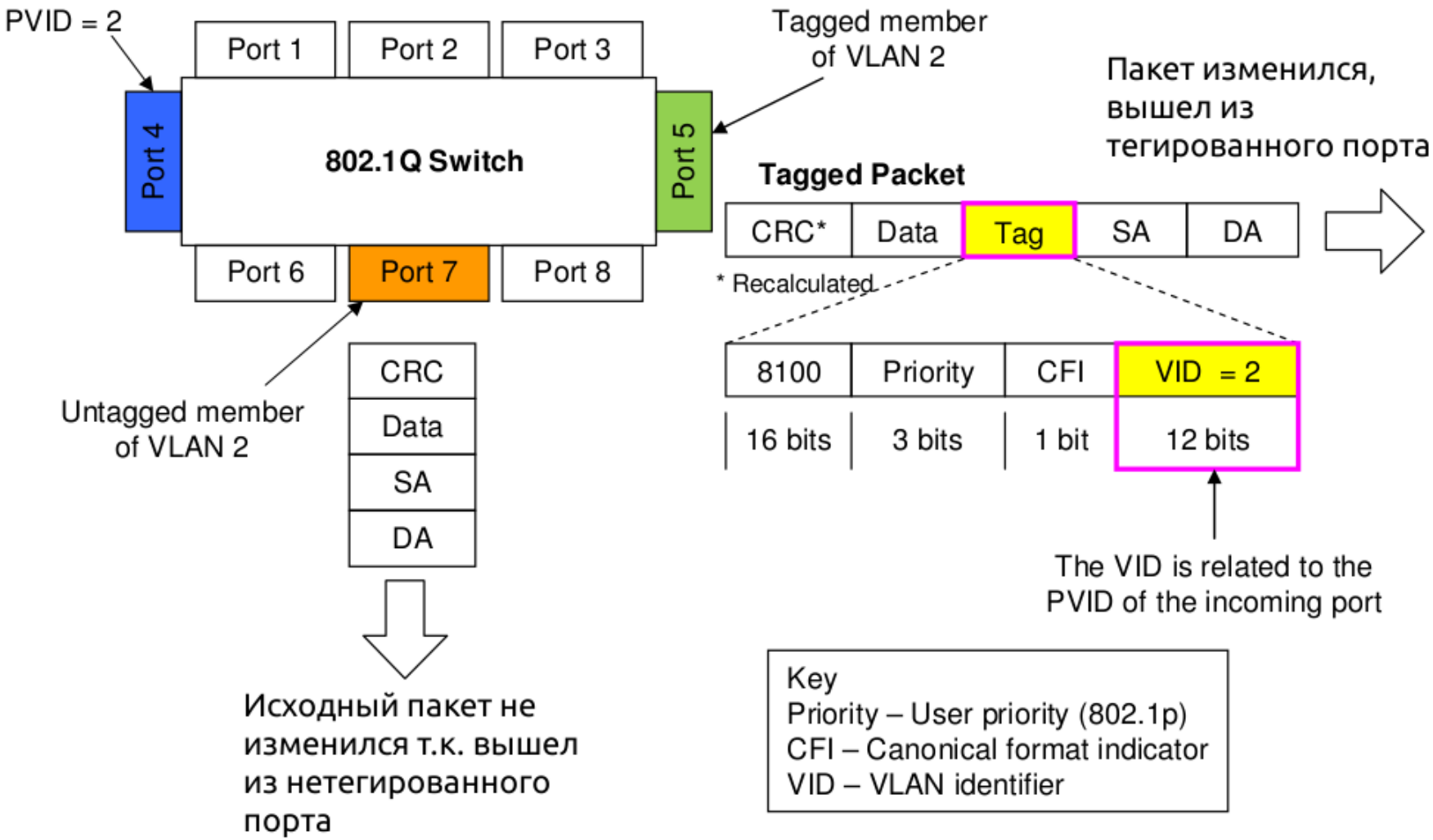
Немаркированный входящий пакет



- PVID порта 4 -> 2
- Входящий немаркированный пакет назначен на VLAN 2
- Порт 5 маркированный Выходящий VLAN 2
- Порт 7 немаркированный Выходящий VLAN 2

- Пакеты с порта 4 перенаправляются на порт5 с маркером
- Пакеты с порта 4 перенаправляются на порт7 без маркера

Немаркированный входящий пакет



Разделение сети, построенной на 2-х коммутаторах на две VLAN

VLAN 1 :

Компьютеры A1, A2, A3, A4

Switch X

VID : 1

Tag: Порт **5**

Untag: Порт **1** и **2**

Порт 1 и 2 PVID = **1**

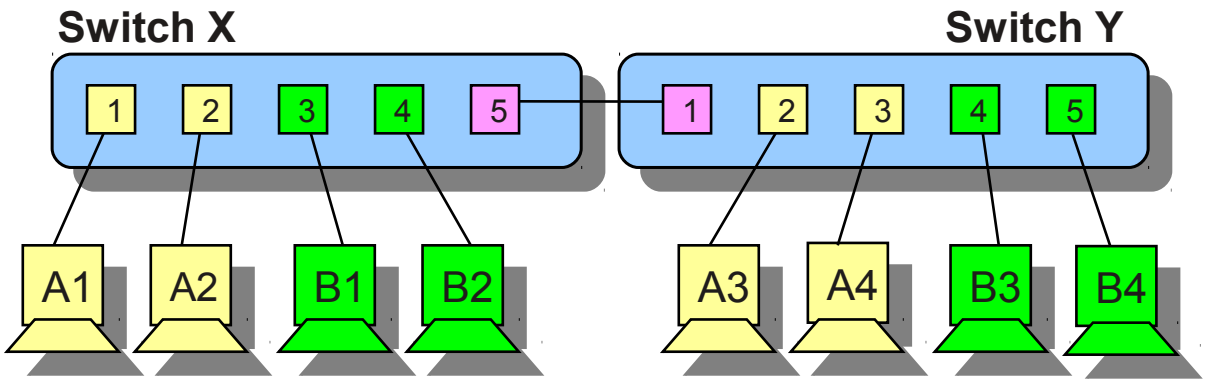
Switch Y

VID : 1

Tag: Порт **1**

Untag: Порт **2** и **3**

Порт 2 и 3 PVID = **1**



VLAN 2 : Компьютеры B1, B2, B3, B4

Switch X

VID : 2

Tag: Порт **5**

Untag: Порт **3 и 4**

Порт 3 и 4 PVID = **2**

Switch Y

VID : 2

Tag: Порт **1**

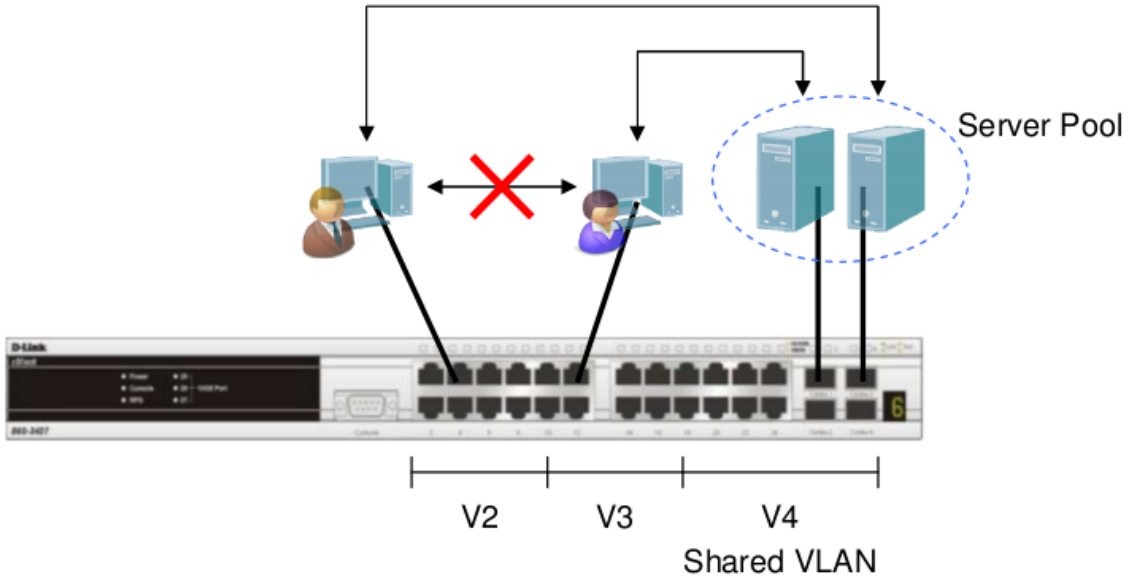
Untag: Порт **4 и 5**

Порт 4 и 5 PVID = **2**

Асимметричные VLAN

для сетевых серверных приложений с использованием коммутатора L2

Сетевые серверные приложения и приложения с доступом в Internet

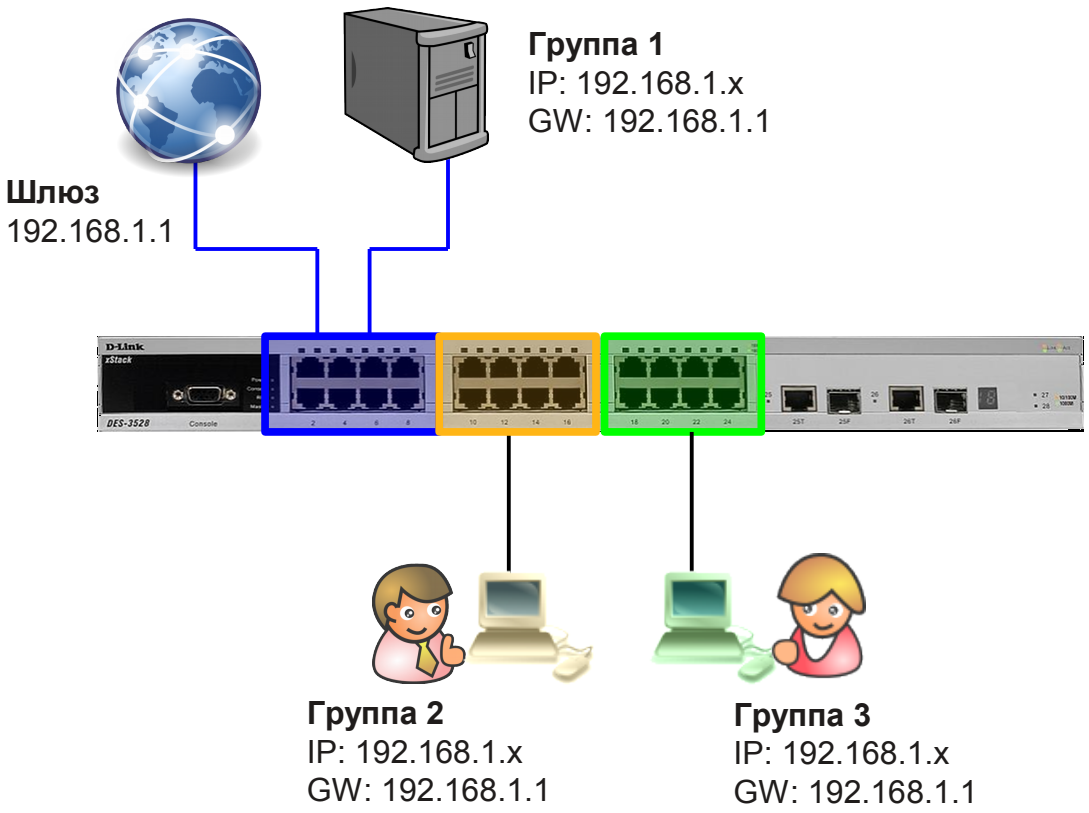


• Общие серверы (Почтовый сервер, файловый сервер, сервера доступа в Internet) должны быть доступны различным группам пользователей, но доступ между группами должен быть закрыт (для повышения производительности или из соображений безопасности)

• Решения на уровне L2: Асимметричные VLAN или сегментация трафика

• Решение на уровне L3: Коммутация L3 + ACL для ограничения доступа между клиентами.

Пример 1: Асимметричные VLAN



V1: порты 1-8, нетегированные
Общий(ие) сервер(ы) или шлюз Internet

V2: порты 9-16, нетегированные
Пользователи VLAN2 (PC или концентратор/коммутатор)

V3: порты 17-24, нетегированные
Пользователи VLAN3 (PC или концентратор/коммутатор)

Задание и требования:

1. V2 и V3 имеют доступ в V1 для обращения к общим серверам (IPX, IP той же подсети, AppleTalk, NetBEUI и т.д.)
2. V2 и V3 имеют возможность обращения к шлюзу Internet для доступа к ресурсам Internet с использованием IP-адресов той же подсети.
3. Не должно быть доступа между V2 и V3.

Пример 1: Асимметричные VLAN

```
enable asymmetric_vlan
create vlan v2 tag 2
create vlan v3 tag 3

config vlan v2 add untagged 1-16
config vlan v3 add untagged 1-8,17-24

config gvrp 1-8 pvid 1
config gvrp 9-16 pvid 2
config gvrp 17-24 pvid 3
save
```

Тест:

1. PC в V2 имеет доступ (ping) к серверам V1 и к сети Internet.
2. PC в V3 имеет доступ (ping) к серверам V1 и к сети Internet.
3. PC в V2 не имеет доступа к PC в V3, и PC в V3 не имеет доступа к PC в V2.

Ограничения асимметричных VLAN

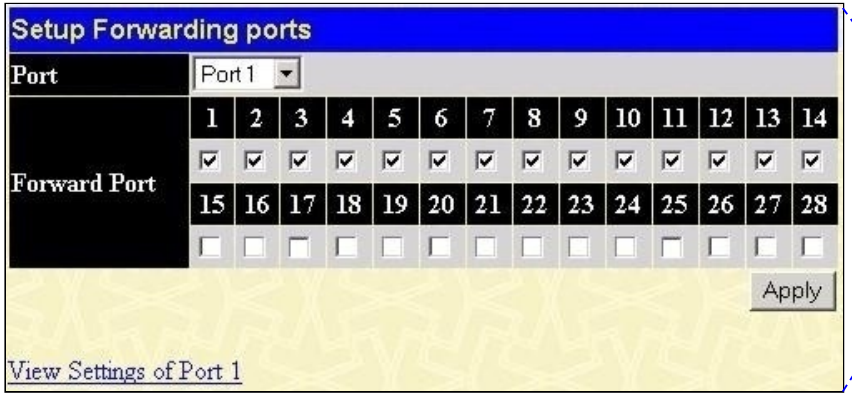
Функция IGMP Snooping не работает при использовании асимметричных VLAN.

Решение: Коммутация L3 + ACL + Протокол маршрутизации групповых сообщений + IGMP snooping

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.

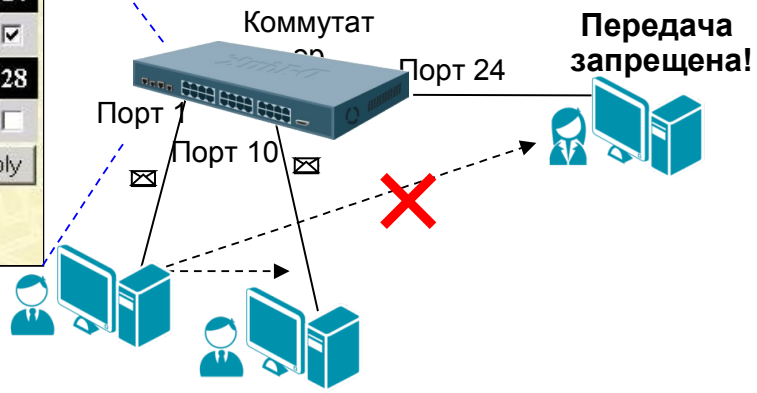
Следующая конфигурация позволяет клиенту, подключенному к порту 1 отправлять/получать трафик от клиентов, подключенных к портам 1-14



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.



Слайд анимирован

Сегментация трафика

Преимущества Traffic Segmentation

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

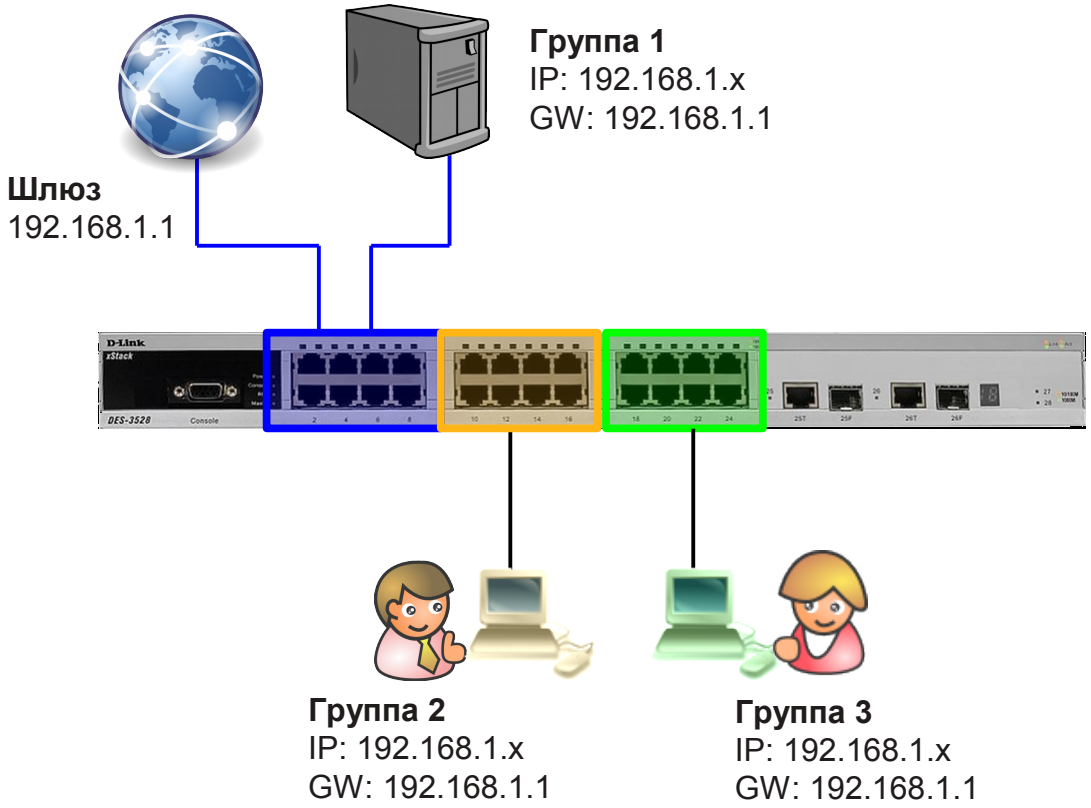
- простота настройки;
- поддерживается работа IGMP Snooping;
- функция Traffic Segmentation может быть представлена в виде иерархического дерева (при иерархическом подходе разделяемые ресурсы должны быть на «вершине» дерева);
- нет ограничений на создание количества групп портов.

- 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.

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



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
```

802.1v – VLAN на базе портов и протоколов

Описание 802.1v

- Стандартизирован IEEE.
- 802.1v это расширение 802.1Q (VLAN на основе портов) для предоставления возможности классификации пакетов не только по принадлежности порту, но также и по типу протокола канального уровня.
- Это означает, что 802.1v VLAN классифицирует пакеты по протоколу и по порту.

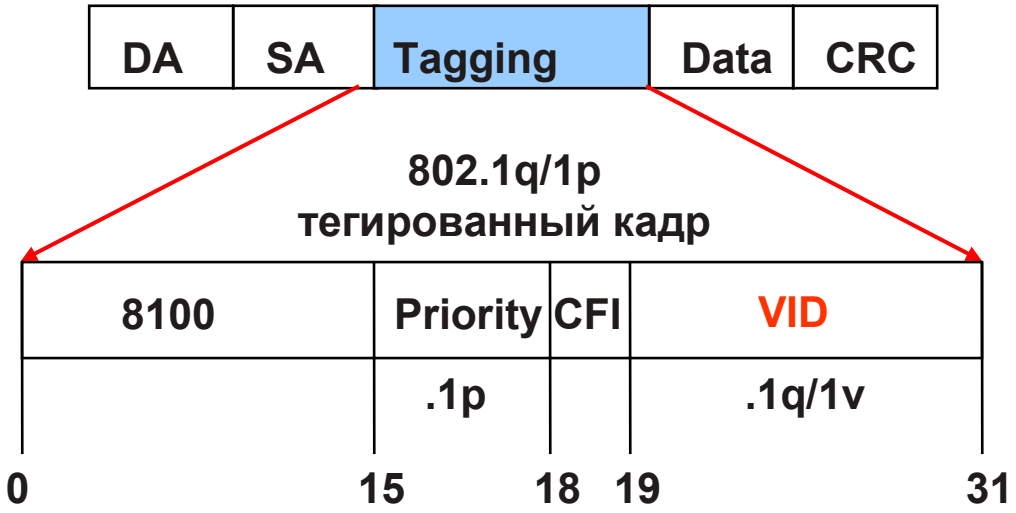
Тегирование кадров 802.1v

Формат тегов кадров 802.1v такой же как и у 802.1q.

Это, 32-х битное поле (VLAN Tag) в заголовке кадра, которое идентифицирует кадр по принадлежности к определенному VLAN или по приоритету.

Максимальный размер тегированного кадра Ethernet - 1522 байтов
(1518 + 4 байта тега)

Обычный (или нетегированный) кадр

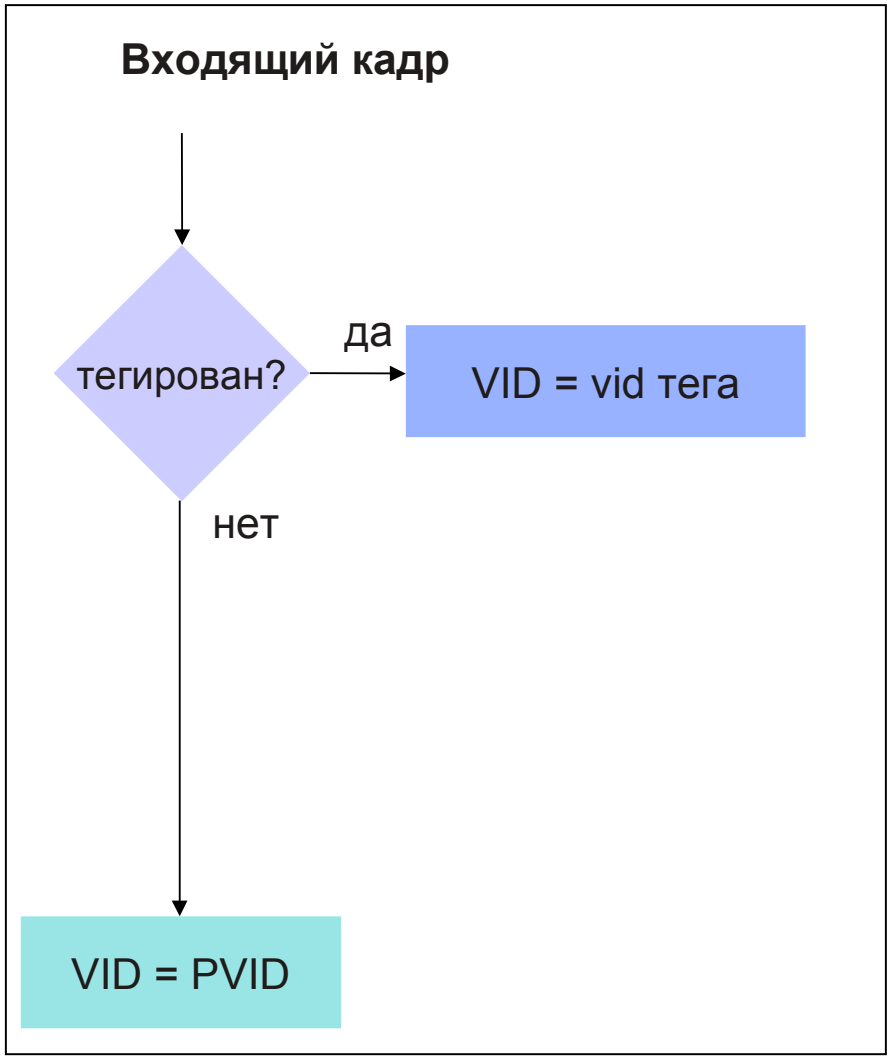


Priority (1p) - 3 бита, 0-7.

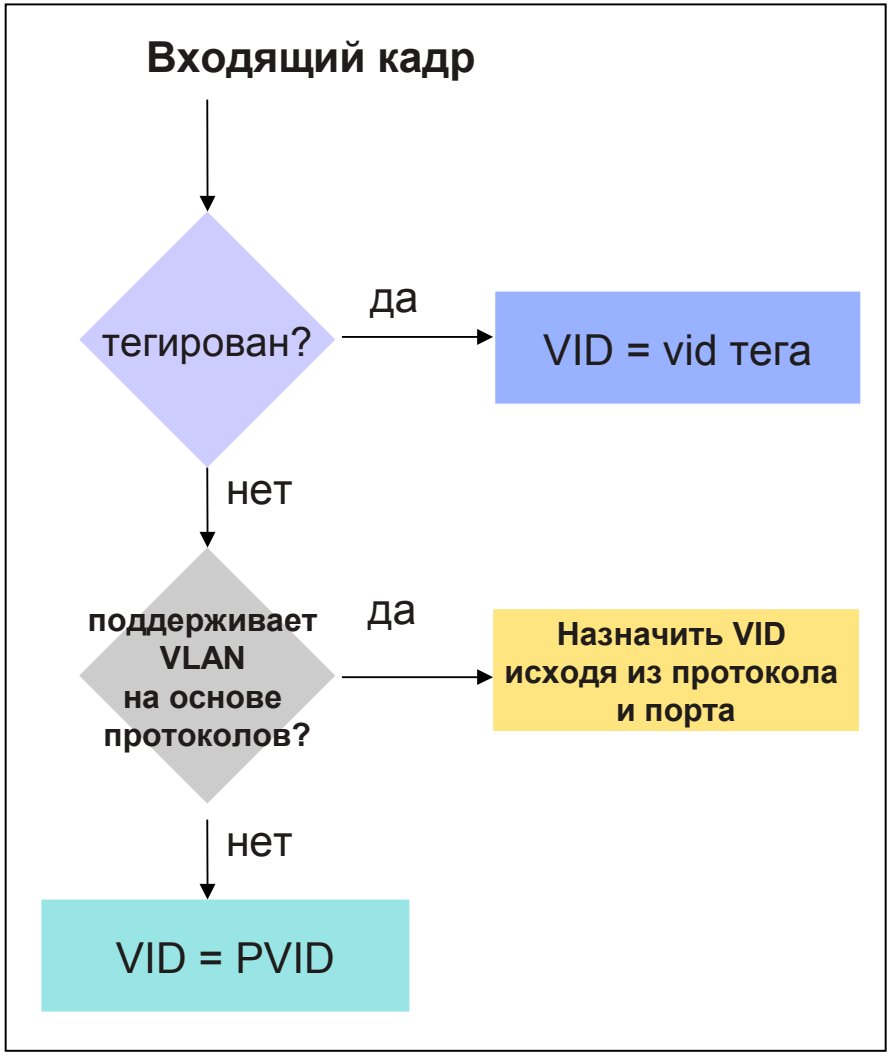
VID (1q/1v) - 12 бит, 0-4095.

Правило классификации VLAN

802.1Q VLAN



802.1v VLAN



Поддерживаемые серией xStack типы протоколов

Коммутатор поддерживает пятнадцать (15) предопределённых протоколов для настройки VLAN на основе протоколов. Пользователь также может выбрать свой протокол (не входящий в эти пятнадцать) сконфигурировав *userDefined* VLAN на основе протоколов. Поддерживаемыми типами протоколов для этих коммутаторов являются: IP, IPX, DEC, DEC LAT, SNAP, NetBIOS, AppleTalk, XNS, SNA, IPv6, RARP и VINES.

Полный список:

protocol-ip,

protocol-ipx802dot3

protocol-ipx802dot2

protocol-ipxSnap

protocol-ipxEthernet2

protocol-appleTalk

protocol-decLat

protocol-decOther

protocol-sna802dot2

protocol-snaEthernet2

protocol-netBios

protocol-xns

protocol-vines

protocol-ipV6

protocol-rarp

protocol-userDefined

Возможна настройка до 7 VLAN на основе протоколов на каждом порту

Пример 2 – Пользователи нескольких протоколов

IP-трафик маршрутизируется между двумя VLAN на базе портов, L3.

Пользователи двух протоколов, IP и IPX
192.168.1.x/24
Шлюз 192.168.1.254

Пользователи протокола IP
192.168.2.x/24
Шлюз 192.168.2.254

Сервер/клиент IPX

Сервер IP,
192.168.4.x/24
Шлюз
192.168.4.254

IPX-трафик проходит через VLAN на основе протокола IPX, L2.

Пример 2 – Пользователи нескольких протоколов

1. Удалить порты из default vlan.

```
config vlan default delete 1:1-1:24
```

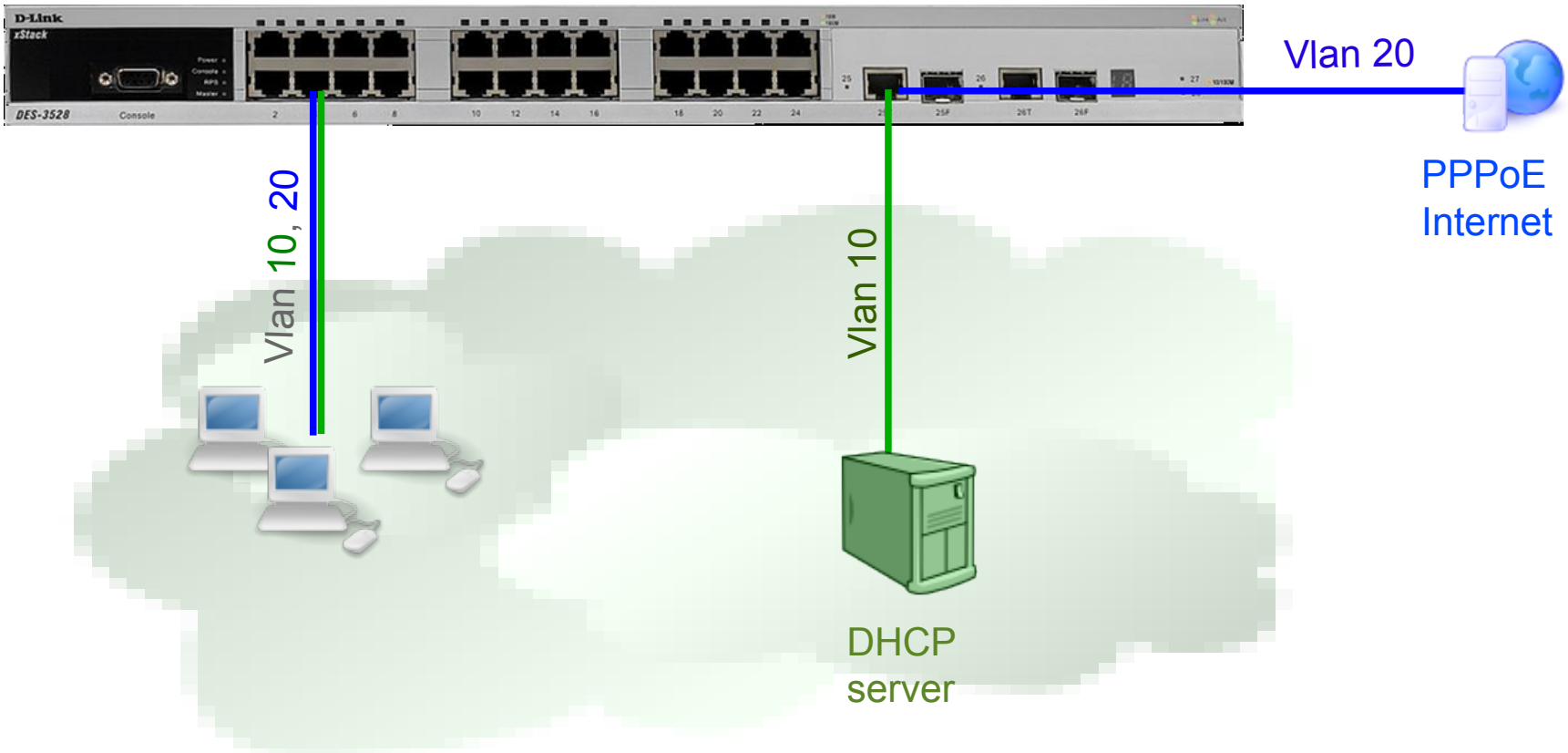
2. Создать VLAN, добавить в него соответствующие порты, а затем создать IP-интерфейс в этом VLAN.

```
create vlan v101 tag 101
config vlan v101 add untagged 1-8
create ipif net1 192.168.1.254/24 v101 state enabled

create vlan v102 tag 102
config vlan v102 add untagged 9-16
create ipif net2 192.168.2.254/24 v102 state enabled

create vlan v104 tag 104
config vlan v104 add untagged 17-24
create ipif net4 192.168.4.254/24 v104 state enabled
```

3. создать VLAN на основе протокола IPX так, чтобы с портов 1-8 пользователи могли обращаться к серверу IPX на порт 24

```
create vlan v200 tag 200 type protocol-ipx802dot3
config vlan v200 add untagged 1-8, 24
```

Пример 3: PPPoE



Пользователи общаются между собой по vlan 10
и имеют доступ в Интеренет через PPPoE сервер, находящийся в vlan 20

Настройки

```
#VLAN
config vlan default delete 1-28
create vlan pppoe tag 20
config vlan pppoe add untagged 1-24
config vlan pppoe add tagged 26
create vlan base tag 10
config vlan base add tagged 26
config vlan base add untagged 1-24
#PVID
config port_vlan 1-24 pvid 10
#DOT1V
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
```

QoS. Качество обслуживания

Качество обслуживания (QoS)

Модели QoS

Можно выделить три модели реализации QoS в сети:

- **Негарантированная доставка данных (Best Effort Service)** – обеспечивает связь между узлами, но не гарантирует надежную доставку данных, время доставки, пропускную способность и определенный приоритет.
- **Интегрированные услуги (Integrated Services, IntServ)** – эта модель описана в RFC 1633 и предполагает предварительное резервирование сетевых ресурсов с целью обеспечения предсказуемого поведения сети для приложений, требующих для нормального функционирования гарантированной выделенной полосы пропускания на всем пути следования трафика.
  - Эту модель также часто называют *жестким QoS* (*hard QoS*) в связи с предъявлением строгих требований к ресурсам сети.
- **Дифференцированное обслуживание (Differentiated Service, DiffServ)** – эта модель описана в RFC 2474, RFC 2475 и предполагает разделение трафика на классы на основе требований к качеству обслуживания.
  - Модель дифференцированного обслуживания занимает промежуточное положение между негарантированной доставкой данных и моделью IntServ и сама по себе не предполагает обеспечение гарантий предоставляемых услуг, поэтому дифференцированное обслуживание часто называют мягким *QoS (soft QoS)*.

Качество обслуживания (QoS)

Приоритезация пакетов

- Для обеспечения QoS на канальном уровне модели OSI коммутаторы поддерживают стандарт IEEE 802.1p.
- Стандарт IEEE 802.1p позволяет задать до 8 уровней приоритетов (от 0 до 7, где 7 – наивысший), определяющих способ обработки кадра, используя 3 бита поля приоритета тега IEEE 802.1Q.

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

Качество обслуживания (QoS)

IEEE 802.1p Приоритет по умолчанию

Используется для того, чтобы добавить тег 802.1p/1q к нетегированному входящему кадру. Приоритет по умолчанию для каждого порта равен 0.

```
DES-3200-26:4# show 802.1p default_priority
Command: show 802.1p default_priority
Port    Priority
------   -------------
1          0
2          0
3          0
…
```

Поменять приоритет по умолчанию на портах можно командой

config 802.1p default_priority <ports> <priority>

QoS в MAN сетях

Трафик в MAN сетях:

1. **VoIP** - **QoS 5**
2. **IPTV** - **QoS 4**
3. **Data**
   a. **Management** - **QoS 7**
   b. **Internet** - **QoS 3**
   c. **Intranet (Local)** - **QoS 0**

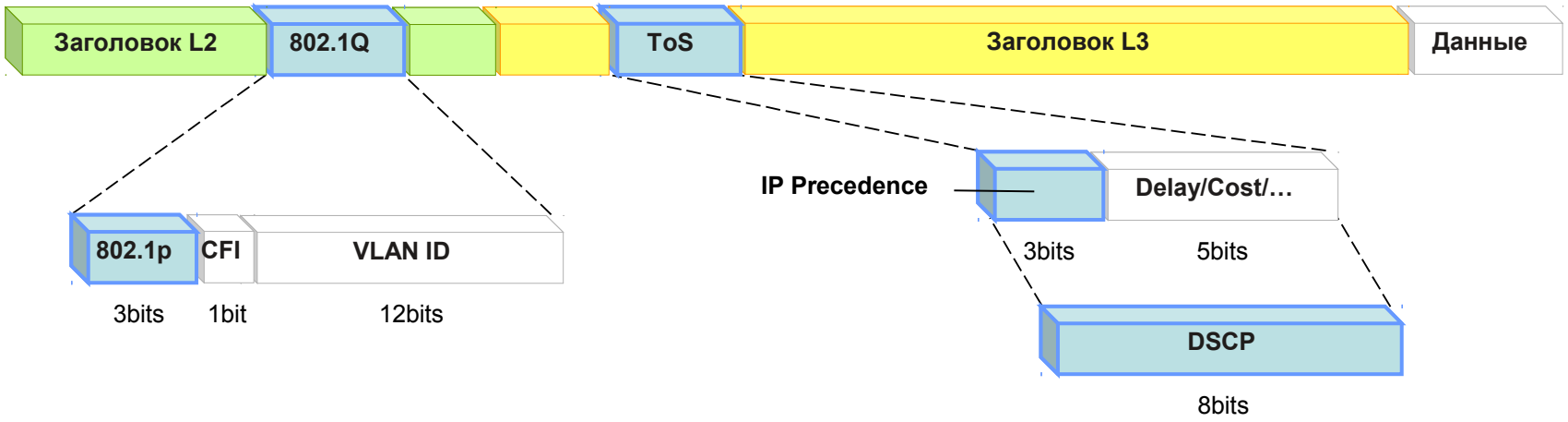
Примечание:

Данная раскраска трафика QoS-ом является рекомендованной, но администратор сети может сам выбрать оптимальный вариант для своей сети.

Качество обслуживания (QoS)

Приоритезация пакетов

- Для обеспечения QoS на сетевом уровне модели OSI в заголовке протокола IPv4 предусмотрено 8-битное поле ToS (Type of Service).
- Этот байт может быть заполнен либо значением приоритета IP Precedence, либо значением DSCP (Differentiated Services Code Point) в зависимости от решаемой задачи:
  - поле IP Precedence имеет размерность 3 бита и может принимать значения от 0 до 7;
  - поле DSCP было стандартизировано IETF с появлением модели DiffServ. Оно занимает 6 старших бит байта ToS и позволяют задать до 64 уровней приоритетов (от 0 до 63).



Качество обслуживания (QoS)

Классификация пакетов

Классификация пакетов (packet classification).- это процесс, позволяющий отнести пакет данных к одному из классов трафика в зависимости от значения одного или нескольких полей его заголовка.

Классификация может осуществляться на основе:

- *приоритета 802.1p;*
- *IP-приоритет или поле DSCP в байте ToS;*
- *MAC-адреса источника и/или приемника;*
- *IP-адреса источника и/или приемника;*
- *номера порта TCP/UDP источника и/или приемника;*
- *тега VLAN и т.п.*

- Программное обеспечение коммутаторов позволяет настраивать карты привязки приоритетов 802.1p, ToS, DSCP к очередям приоритетов каждого порта в соответствии с требованиями пользователей.
- Для классификации пакетов данных на основании различных параметров их заголовков могут использоваться списки управления доступом (Access Control List, ACL).

Качество обслуживания (QoS)

Классификация пакетов

- Для обеспечения дифференцированного обслуживания трафика, коммутаторы поддерживают в зависимости от модели от 4 до 8 аппаратных очередей приоритетов на каждом из своих портов.
- Для обеспечения требуемой очередности передачи пакетов данных в коммутаторе необходимо настроить алгоритм обслуживания очередей и карту привязки приоритетов 802.1p, ToS, DSCP к очередям.
- По умолчанию в коммутаторах D-Link используются следующие карты привязки пользовательских приоритетов 802.1p к аппаратным очередям:

4 очереди приоритетов

Приоритет	Номер очереди
0	Q1
1	Q0
2	Q0
3	Q1
4	Q2
5	Q2
6	Q3
7	Q3

8 очередей приоритетов

Приоритет	Номер очереди
0	Q2
1	Q0
2	Q1
3	Q3
4	Q4
5	Q5
6	Q6
7	Q6

Качество обслуживания (QoS)

Маркировка пакетов

- После процесса классификации коммутатор может осуществить *маркировку пакетов (packet marking)*.
- Маркировка пакетов определяет способ записи/перезаписи значений битов приоритета (DSCP, 802.1p или IP Precedence) входящих пакетов данных.
- Обычно процесс маркировки выполняется на граничных устройствах и позволяет последующим коммутаторам/маршрутизаторам использовать новое значение приоритета пакета для отнесения его к одному из поддерживаемых в сети классов обслуживания.
- Изменить значения битов приоритета в заголовках входящих пакетов

Качество обслуживания (QoS)

Управление перегрузками и механизмы обслуживания очередей

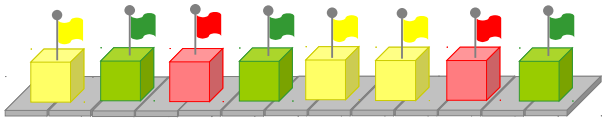
Наиболее часто перегрузка сети возникает в местах соединения коммутаторами сетей с разной полосой пропускания.

В случае возникновения перегрузки сети пакеты начинают буферизироваться и распределяться по очередям.

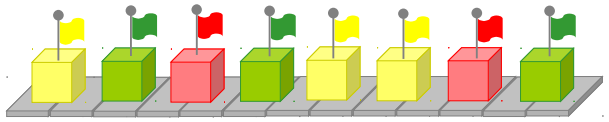
Порядок передачи через выходной интерфейс поставленных в очередь пакетов данных на основе их приоритетов определяется *механизмом обслуживания очередей* (*Queuing mechanism*), который позволяет управлять пропускной способностью сети при возникновении перегрузок.

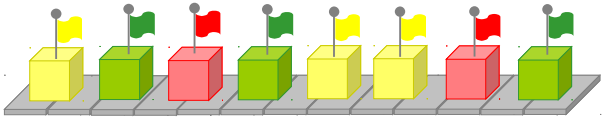
Качество обслуживания (QoS)

Механизм управления перегрузками

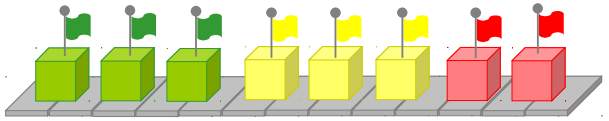


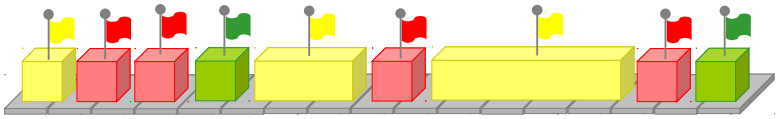
FIFO



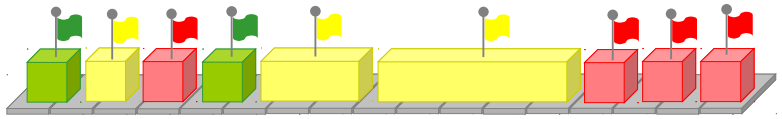


SPQ





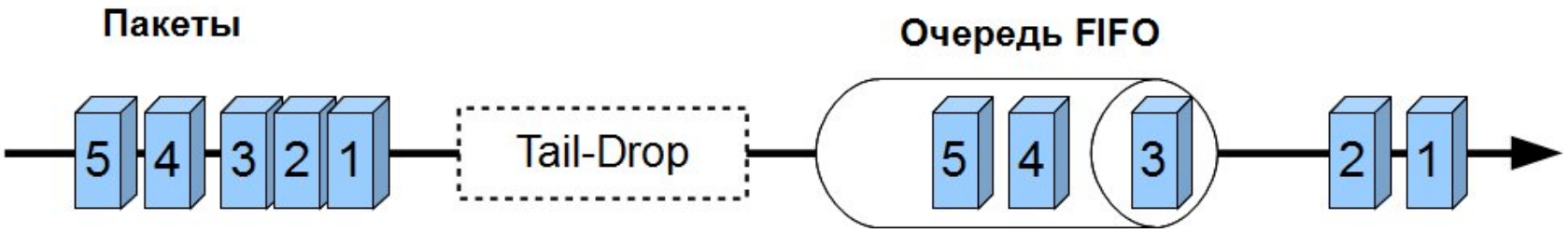
WRR



Качество обслуживания (QoS)

Механизм обслуживания очередей FIFO

Передает пакеты, поставленные в очередь в том порядке, в котором они поступили в нее. Этот механизм не обеспечивает классификации пакетов и рассматривает их как принадлежащие одному классу.



Качество обслуживания (QoS)

Очереди приоритетов со строгим режимом (Strict Priority Queue)

- Предполагают передачу трафика строго в соответствии с приоритетом выходных очередей.
- В этом механизме предусмотрено наличие 4-х очередей – с высоким, средним, обычным и низким приоритетами обслуживания.
- Пакеты, находящиеся в очереди с высоким приоритетом, обрабатываются первыми. Пакеты из следующей по приоритету обслуживания очереди начнут передаваться только после того, как опустеет высокоприоритетная очередь.

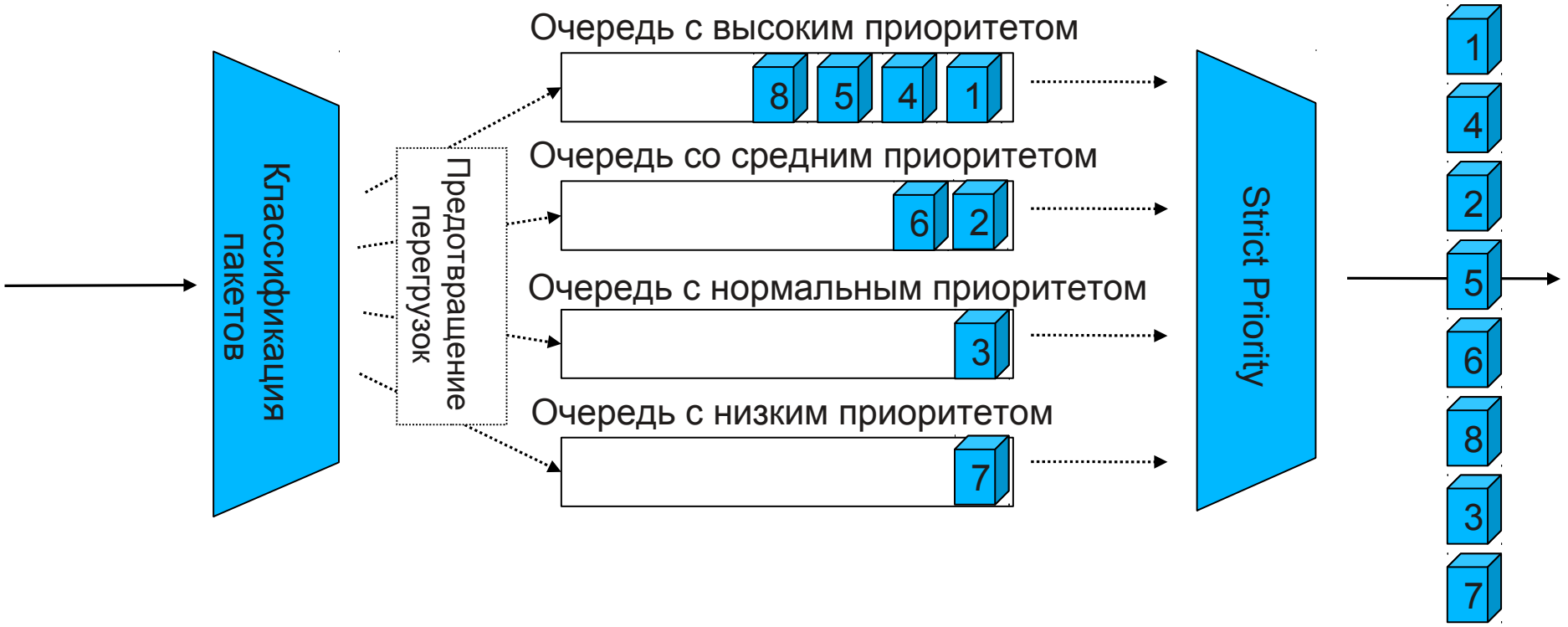
Проблема:

Пакеты из очередей с низким приоритетом могут долго не обрабатываться.

По умолчанию на коммутаторах D-Link настроены очереди приоритетов со строгим режимом.

Качество обслуживания (QoS)

Очереди приоритетов со строгим режимом (Strict Priority Queue)



Слайд анимирован

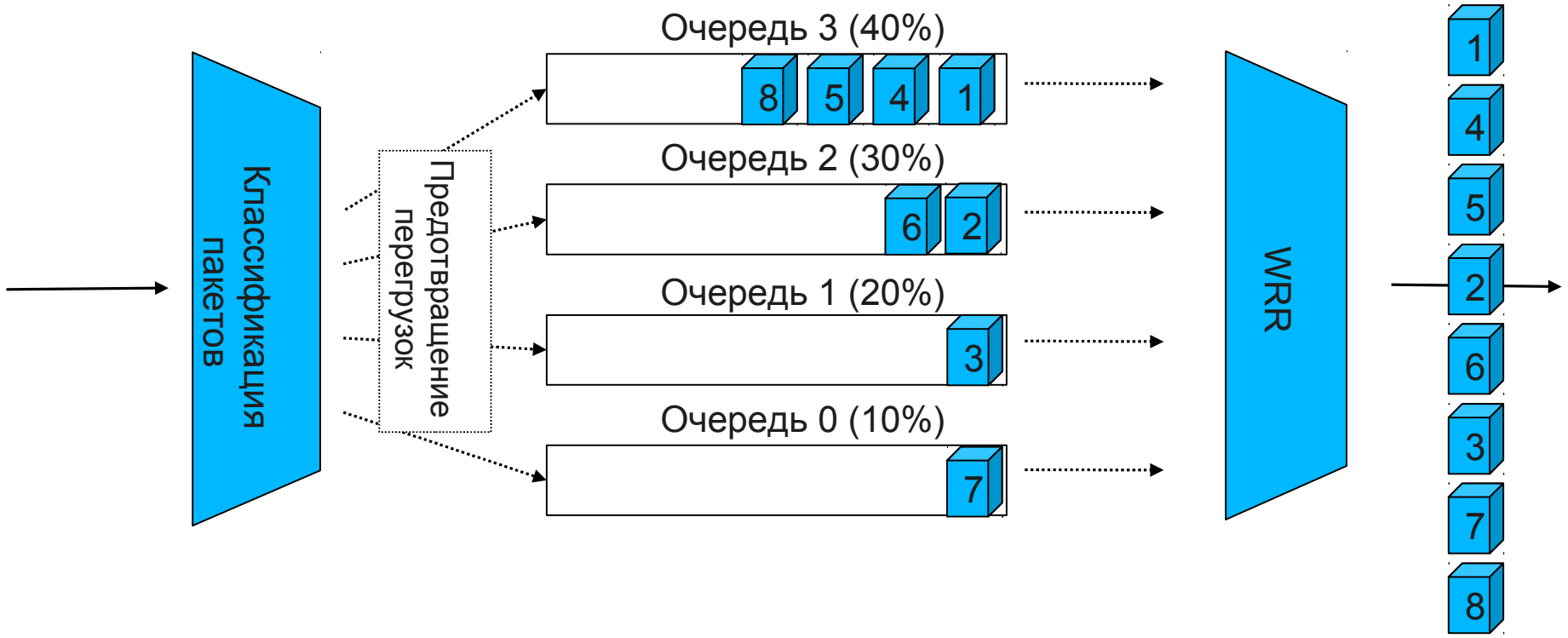
Качество обслуживания (QoS)

Взвешенный алгоритм кругового обслуживания (Weighted Round Robin)

- Этот механизм исключает главный недостаток очередей приоритетов, обеспечивая обработку очередей в соответствии с назначенным им весом и предоставляя полосу пропускания для пакетов из низкоприоритетных очередей.
- Процесс обработки очередей осуществляется по круговому принципу, начиная с самой приоритетной очереди. Из каждой непустой очереди передается некоторый объем трафика, пропорциональный назначенному ей весу, после чего выполняется переход к следующей по убыванию приоритета очереди и т.д. по кругу.

Качество обслуживания (QoS)

Взвешенный алгоритм кругового обслуживания (Weighted Round Robin)



Слайд анимирован

Качество обслуживания (QoS)

Механизм предотвращения перегрузок

Механизм предотвращения перегрузок (*Congestion avoidance*) – это процесс выборочного отбрасывания пакетов с целью избежания перегрузок в сети в случае достижения выходными очередями своей максимальной длины (в пакетах).

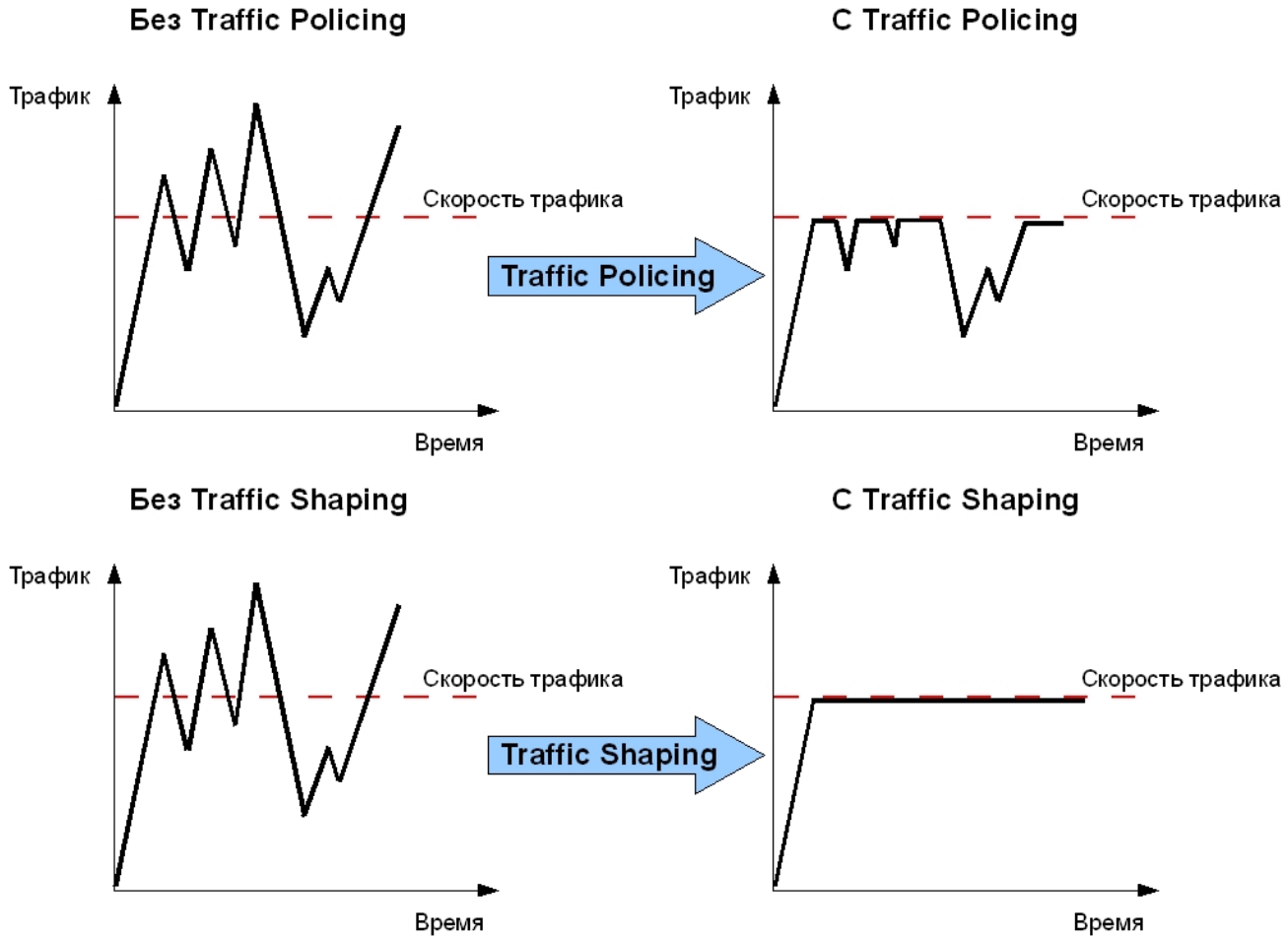
Можно выделить следующие алгоритмы предотвращения перегрузок:

- Алгоритм «отбрасывания хвоста» (Tail-Drop);
- Алгоритм произвольного раннего обнаружения (Random Early Detection, RED);
- Простой алгоритм произвольного раннего обнаружения (Simple Random Early Detection, SRED);
- Взвешенный алгоритм произвольного раннего обнаружения (Weighted Random Early Detection, WRED).

Качество обслуживания (QoS)

Контроль полосы пропускания

Механизмы *Traffic Policing* (ограничение трафика) и *Traffic Shaping* (выравнивание трафика) позволяют регулировать интенсивность трафика с целью обеспечения функций качества обслуживания.



Качество обслуживания (QoS)

Функция Bandwidth control

- Для управления полосой пропускания входящего и исходящего трафика на портах Ethernet коммутаторы D-Link поддерживают функцию *Bandwidth control*, которая использует для ограничения скорости механизм Traffic Policing.

- Администратор может вручную устанавливать требуемую скорость соединения на порте в диапазоне от 64 Кбит/с до максимально поддерживаемой скорости интерфейса с шагом 64 Кбит/с.
- Настройка ограничения скорости до 128 Кбит/с для трафика, передаваемого с интерфейса 5 коммутатора :

```
config bandwidth_control 5 tx_rate 128
```

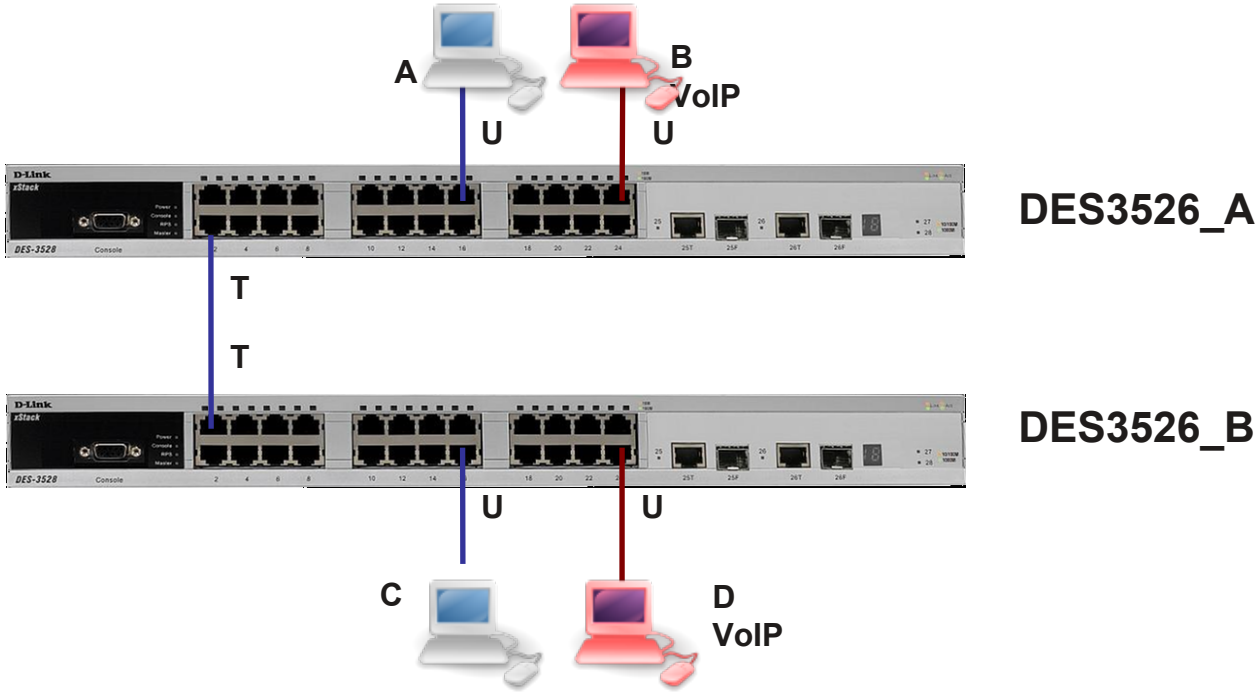
Более гибким решением ограничения полосы пропускания является функция *per-flow Bandwidth control.*

- Эта функция позволяет ограничивать полосу пропускания не всему трафику, получаемому или передаваемому с интерфейса коммутатора, а конкретным потокам данных, определенным администратором сети.
- Функция per-flow Bandwidth control использует механизм списков управления доступом для просмотра определенного типа трафика и ограничения для него полосы пропускания.

Качество обслуживания (QoS)

Пример настройки QoS

Пользователи B и D используют приложения IP-телефонии. Голосовому трафику пользователей B и D требуется обеспечить наивысшее качество обслуживания по сравнению с трафиком других приложений, выполняемых на компьютерах остальных пользователей сети.



Качество обслуживания (QoS)

Настройка коммутаторов

- Для того чтобы внутри коммутатора могла обрабатываться информация о приоритетах 802.1p, состояние портов коммутатора, к которым подключены пользователи необходимо перевести из «немаркированные» в «маркированные».

```
config vlan default add tagged 1
```

- Изменить приоритет порта 24, к которому подключен пользователь B, использующий приложения IP-телефонии с 0 (установлено по умолчанию) на 7. Пакеты с приоритетом 7 будут помещаться в очередь Q6, которая имеет наивысший приоритет обработки.

```
config 802.1p default_priority 24 7
```

Протоколы «покрывающего дерева»
Spanning Tree Protocols

802.1d (STP)
802.1w (RSTP)
802.1s (MSTP)

Протокол Spanning Tree

Зачем нужен протокол Spanning Tree?

- Исключение петель
- Резервные связи

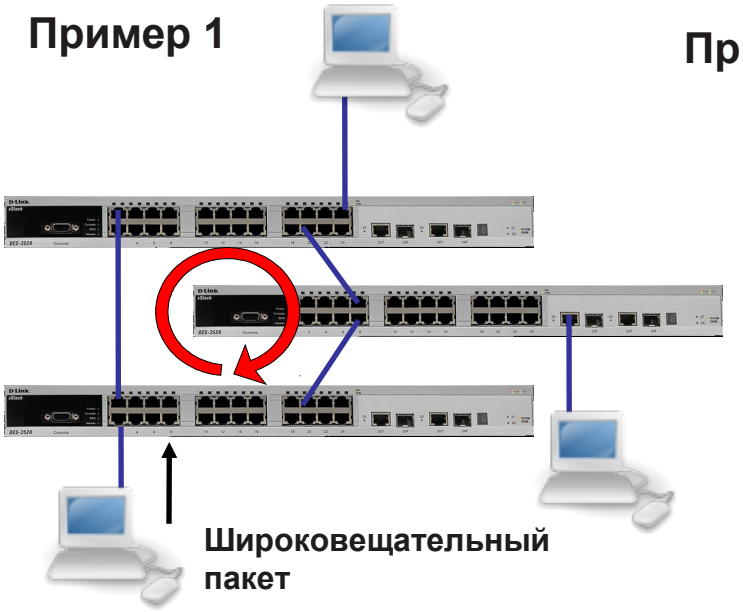
Версии:

- IEEE 802.1d Spanning Tree Protocol, STP
- IEEE 802.1w Rapid Spanning Tree Protocol, RSTP
- IEEE 802.1s Multiple Spanning Tree Protocol, MSTP

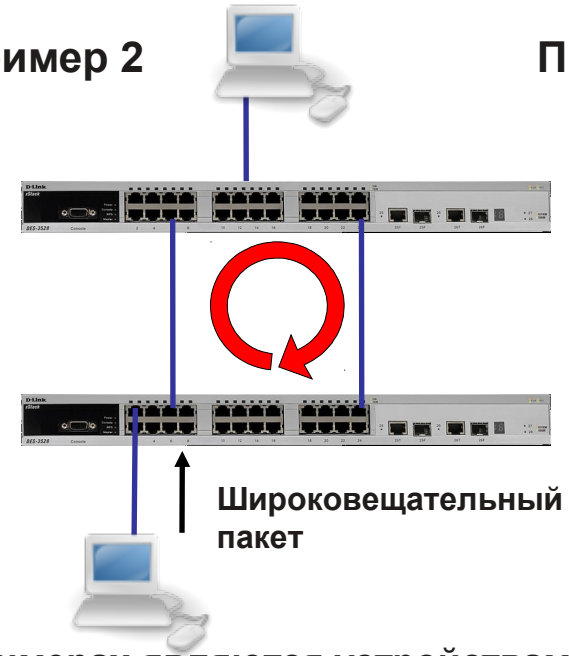
Что такое сетевая петля L2

Коммутаторы (L2), объединённые в кольцо, образуют одну или несколько сетевых петель

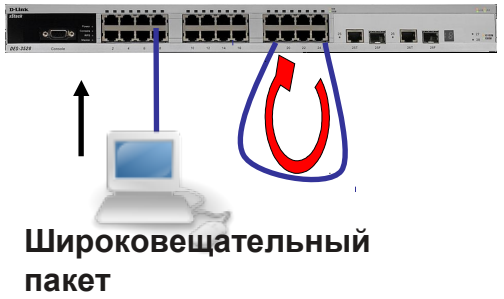
Пример 1



Пример 2



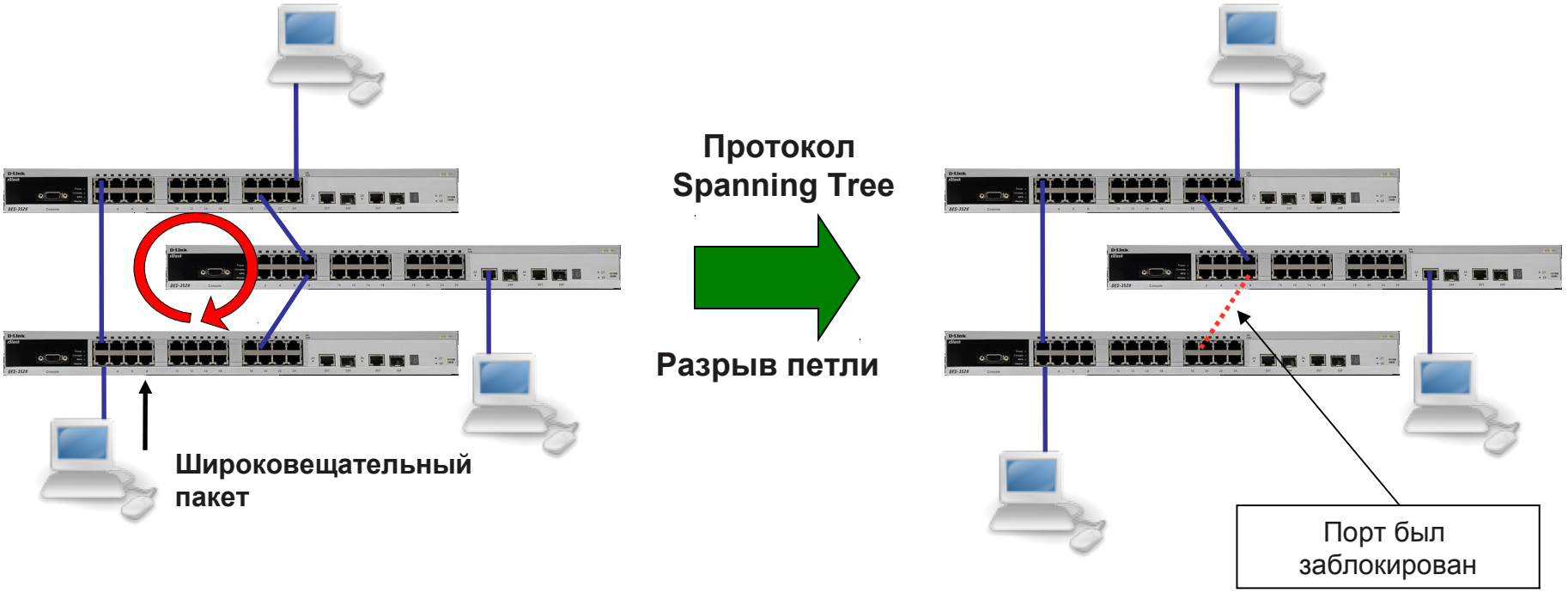
Пример 3



Примечание: Коммутаторы в этих примерах являются устройствами L2, VLAN на них не настроены, и протокол Spanning Tree не включен.

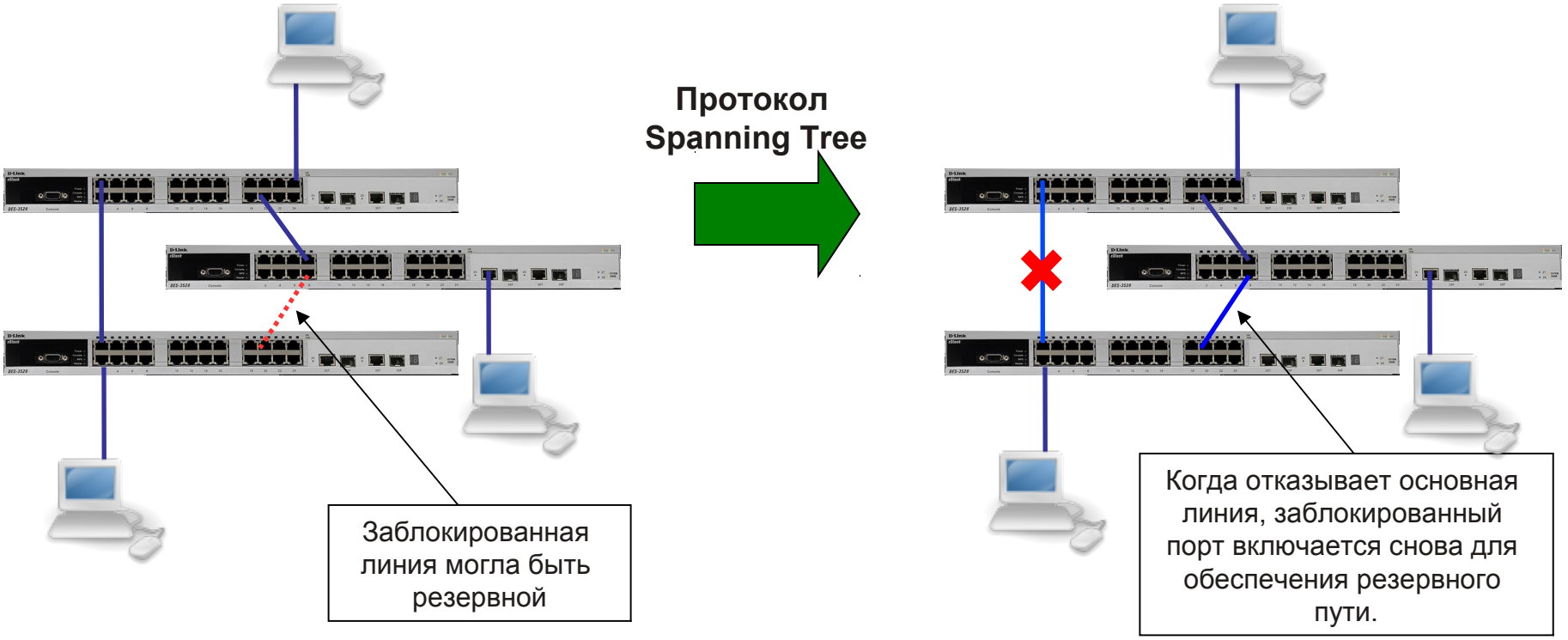
Проблема: В сети L2 Ethernet не допускаются петли. Если они есть, то это может вызвать Широковещательный шторм (Broadcast Storm).

Исключение петель



Решение: Протокол Spanning Tree (STP, RSTP, MSTP) может исключить петлю или петли.

Резервная(ые) связь(и)



Если происходит отказ основной линии, протокол Spanning Tree может включить заблокированный порт для обеспечения резервного пути.

Пакеты BPDU содержат информацию для построения топологии сети без петель

Пакеты BPDU помещаются в поле данных кадров канального уровня, например, кадров Ethernet. Они содержат несколько полей, определяющих работу STP. Среди них наиболее важные:

- Идентификатор коммутатора
- Расстояние до корневого коммутатора
- Идентификатор порта

IEEE 802.1d, STP

Как работает STP (802.1d):

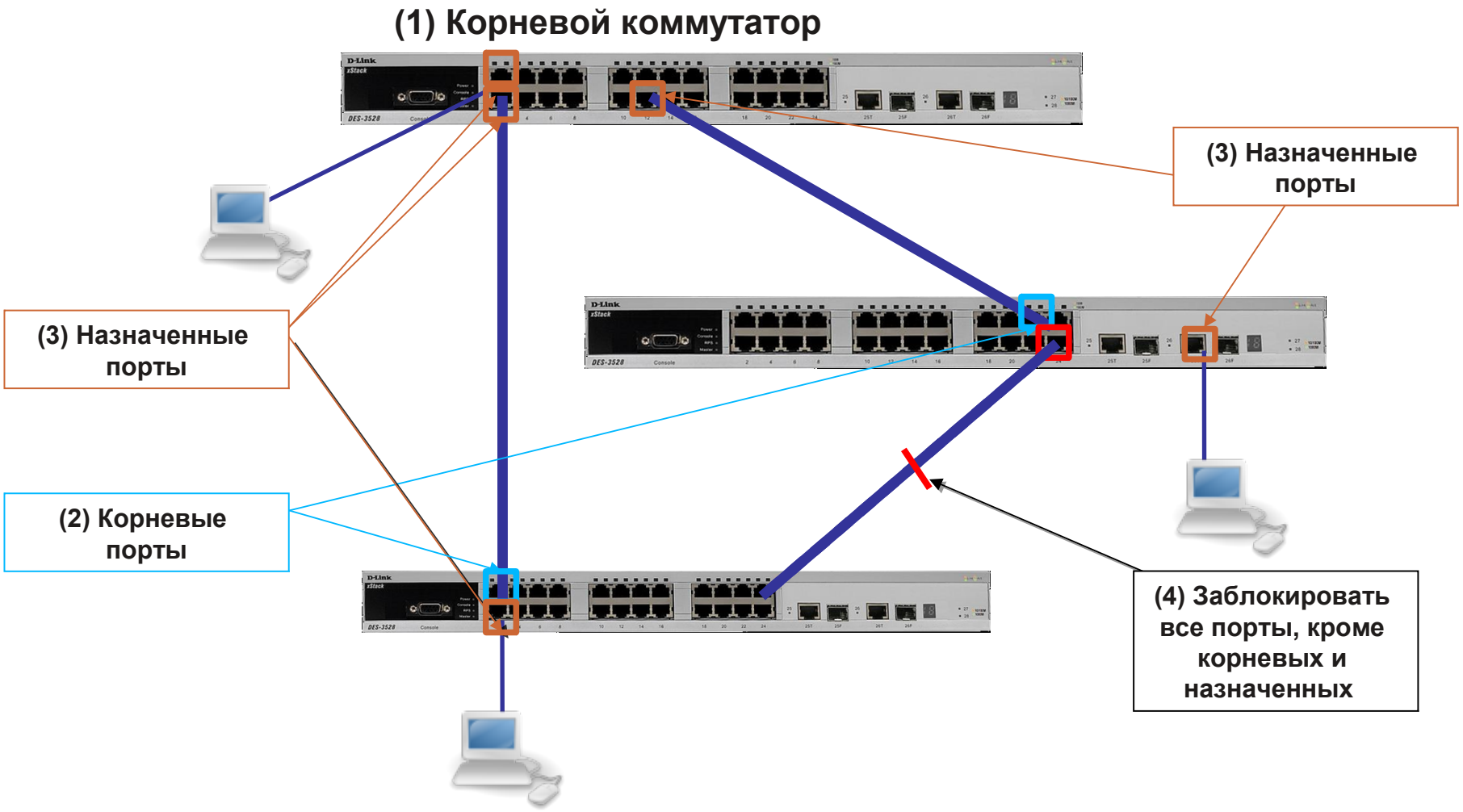
1. Выбирается Корневой коммутатор (*Root Bridge)*. Коммутатор с наименьшим ID становится корневым. Он должен быть один в коммутируемой сети LAN.

2. Определяется Корневой порт (*Root Port)* для каждого коммутатора. Порт коммутатора с наименьшим значением Стоимости пути до корневого коммутатора (Root Path Cost) назначается корневым портом. Он должен быть один у каждого коммутатора.

3. Определяется Назначенный порт (*Designated Port)* для каждого сегмента LAN. Порт, по которому значение стоимости пути до корневого коммутатора для сегмента LAN минимально, выбирается назначенным для данного сегмента. Каждый сегмент LAN иметь только один назначенный порт.

4. Блокируются все порты, не являющиеся корневыми или назначенными.

Как работает STP



Состояния портов в STP

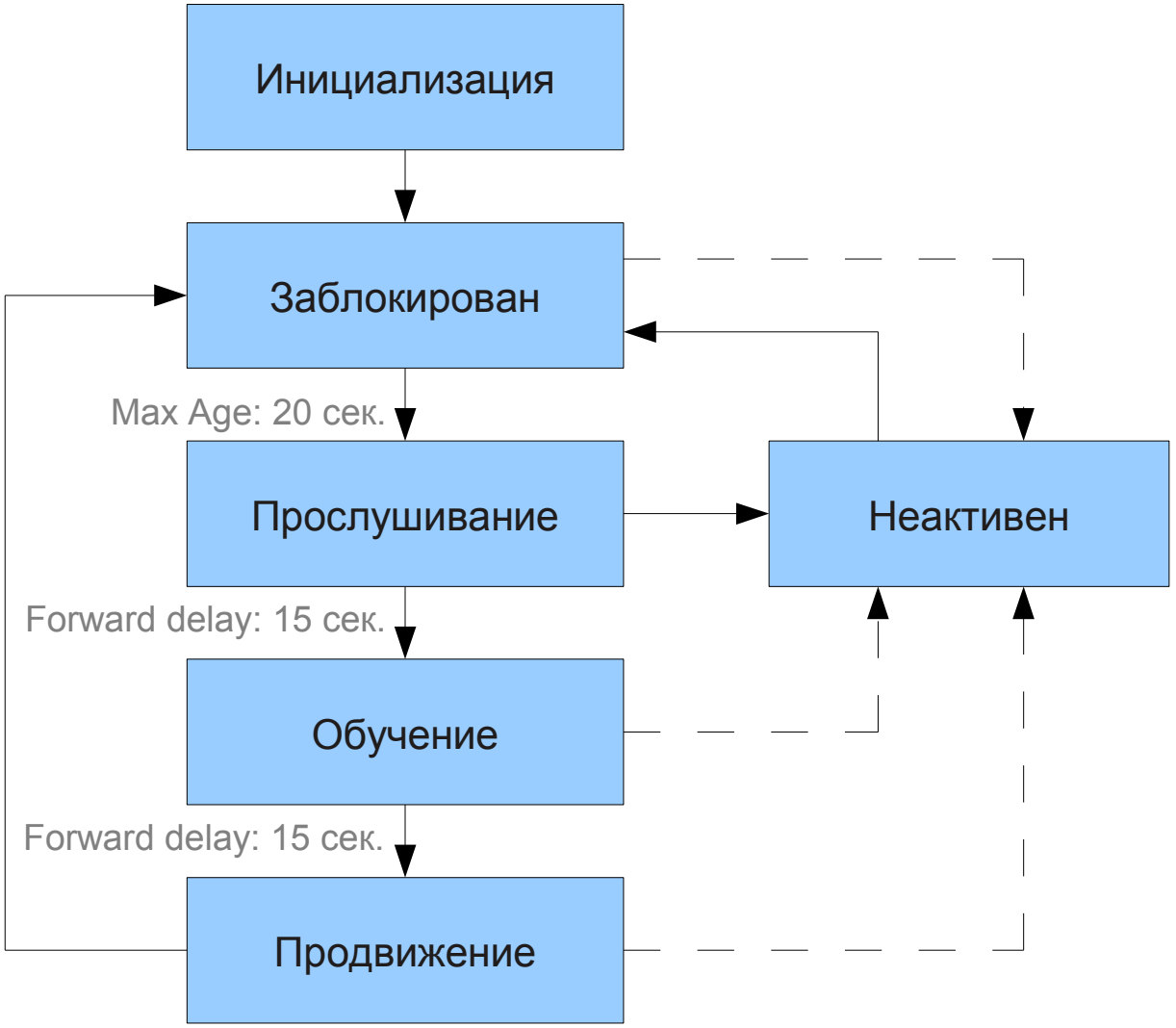
Заблокирован:
Порт принимает BPDU пакеты
Не изучает адреса

Прослушивание:
Определяет Root bridge, корневой порт и назначенные порты

Обучение:
Изучает MAC адреса входящих пакетов, но не передаёт трафик

Продвижение:
Нормальная работа порта

Неактивен:
Не учавствует в построении STP дерева, STP выключен, трафик не передаётся



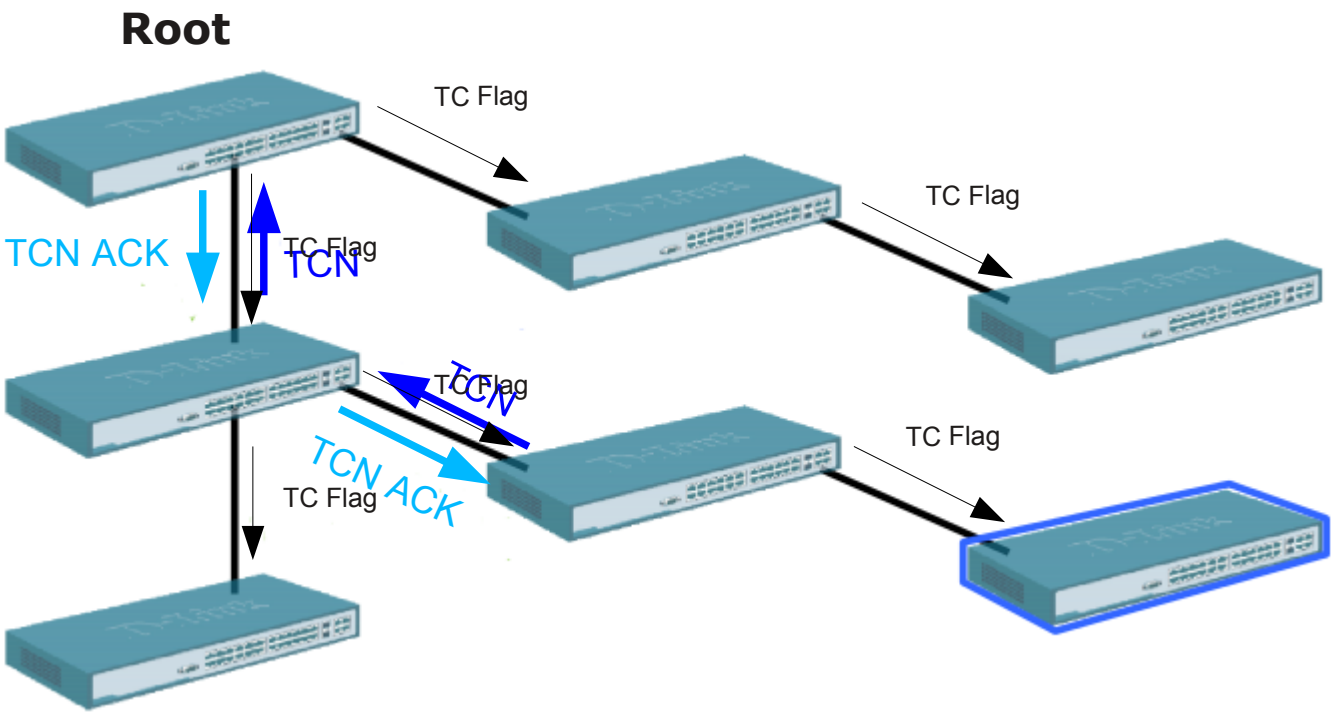
Таймеры протокола STP

Существует несколько таймеров STP:

- **hello:** Интервал hello – это время между Bridge Protocol Data Unit (BPDU), отсылаемыми с портов коммутатора. По умолчанию это 2 секунды, но может быть задан в диапазоне от 1 до 10 секунд.
- **forward delay:** Forward delay (задержка продвижения) это время в двух состояниях – прослушивание и обучение. По умолчанию это 15 секунд, но может быть настроена в диапазоне от 4 до 30 секунд.
- **max age**: Max age (максимальный возраст) – таймер, контролирующий время, в течение которого порт коммутатора хранит информацию о конфигурации BPDU. Это 20 секунд по умолчанию и может быть изменено в диапазоне от 6 до 40 секунд.

Эти три параметра содержатся в каждом BPDU конфигурации. Также есть дополнительный временной параметр в каждой конфигурации BPDU, известный как Возраст сообщения (Message Age). Возраст сообщения это не фиксированная величина. Она представляет собой временной интервал с момента первой посылки BPDU корневым коммутатором. Корневой коммутатор будет посылать все свои BPDU с возрастом сообщения равным нулю, и все другие коммутаторы на пути BPDU будут добавлять к нему 1. В реальности, этот параметр означает как далеко Вы находитесь от корневого коммутатора, получая этот BPDU.

Topology change notification



Корневой коммутатор меняет конфигурационный BPDU

При изменении топологии

- Коммутаторы посылают TCN через корневой порт
- При получении TCN коммутатор отсылает обратно подтверждение получения

Недостатки STP

Основной недостаток 802.1d STP:

Большое время сходимости. Протоколу STP (802.1d) обычно для этого требуется от 30 до 60 секунд.

Решение:

IEEE 802.1w: Протокол Rapid Spanning Tree, RSTP.

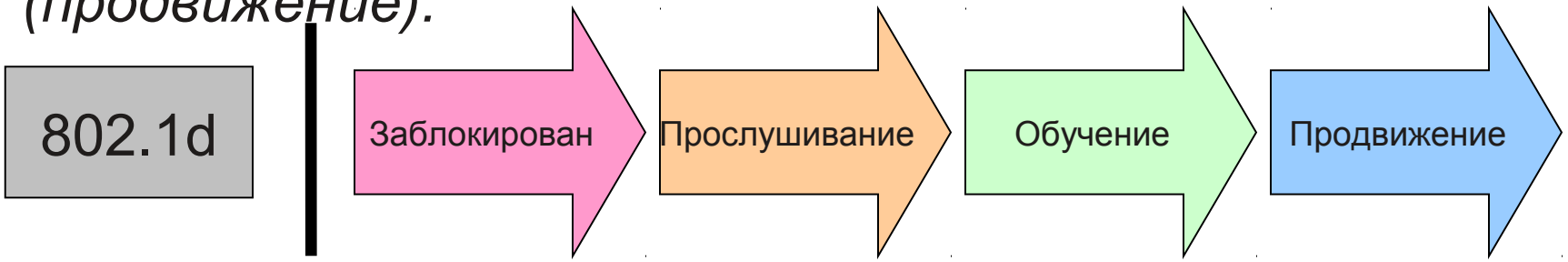
Протокол Rapid Spanning Tree, RSTP

- Стандартизирован IEEE 802.1w

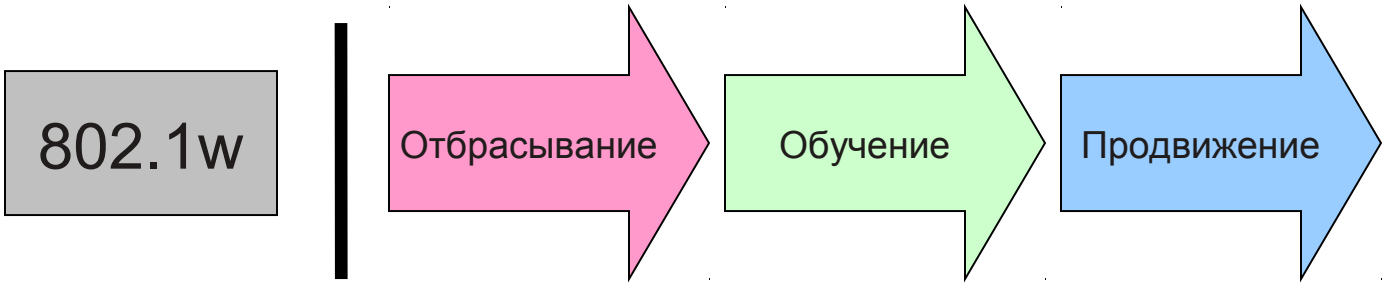
  Обеспечивает серьёзный прирост скорости сходимости коммутируемой сети моментальным переводом корневых и назначенных портов в состояние продвижения кадров

Состояния портов

- В стандарте 802.1d определено 4 различных состояния портов: *blocking (заблокирован), listening (прослушивание), learning (обучение), и forwarding (продвижение).*



- В стандарте 802.1w определено 3 различных состояния портов 802.1w: *discarding (отбрасывание), learning (обучение), и forwarding (продвижение).*



Соответствие состояния портов между 802.1d и 802.1w

STP (802.1d) Состояние порта	RSTP (802.1w) Состояние порта	Порт входит в активную топологию?	Порт изучает MAC-адреса?
Отключён	Отбрасывание	Нет	Нет
Заблокирован	Отбрасывание	Нет	Нет
Прослушивание	Отбрасывание	Нет	Нет
Обучение	Обучение	Нет	Да
Продвижение	Продвижение	Да	Да

Роли портов

- Роли корневых портов
- Роли назначенных портов
- Роли альтернативных портов
- Роли резервных портов

Роли портов

- Роли альтернативных и резервных портов в протоколе RSTP
  - *Альтернативный порт* – порт, который может заменить *корневой порт* при выходе его из строя
  - *Резервный порт* – порт, который может заменить *назначенный порт* при выходе его из строя

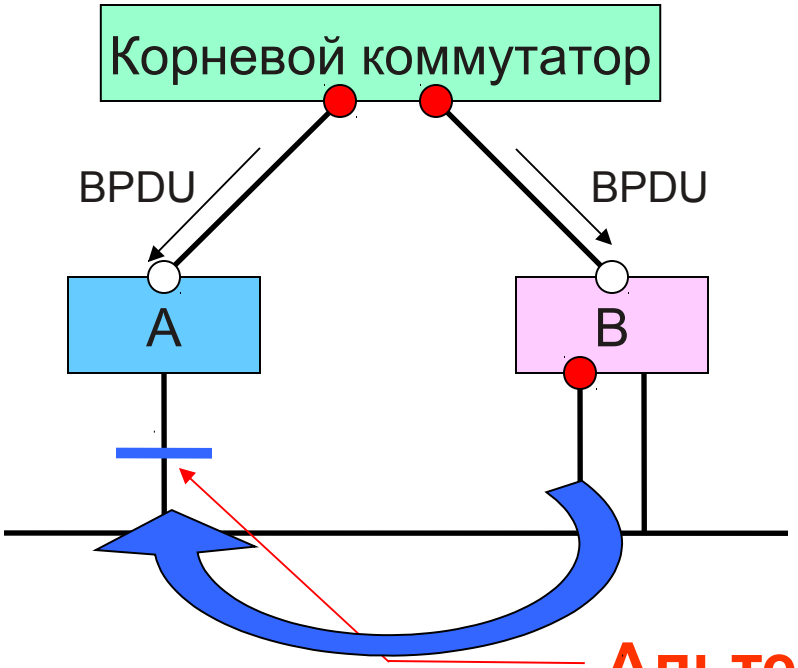
Роли портов

- Роли альтернативных и резервных портов
  - Эти две роли соответствуют заблокированному состоянию по стандарту 802.1d.
  - Для заблокированного порта важнее получать BPDU, чем отсылать их в свой сегмент. Порту необходимо получать BPDU для того, чтобы оставаться заблокированным. В RSTP есть для этого две роли.

Роли портов

- Роли альтернативных портов

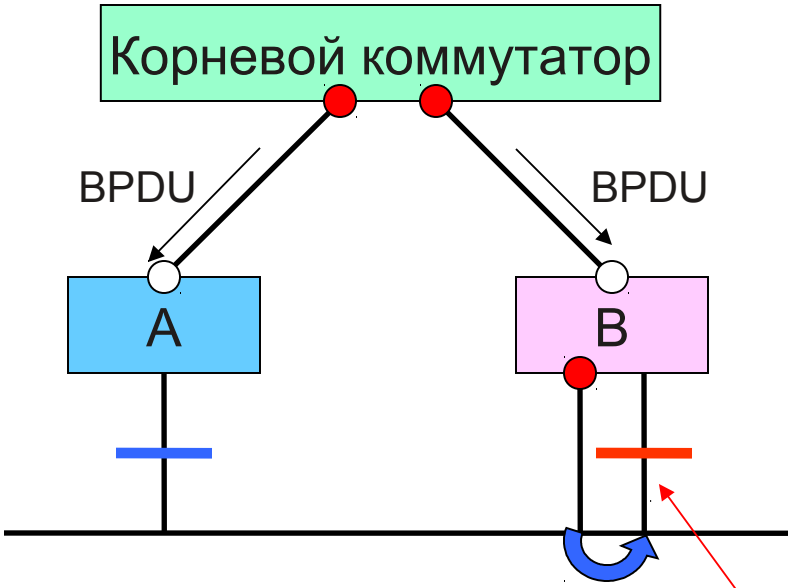
  Альтернативный порт – это порт заблокированный в результате получения более предпочтительных BPDU от другого коммутатора.



Роли портов

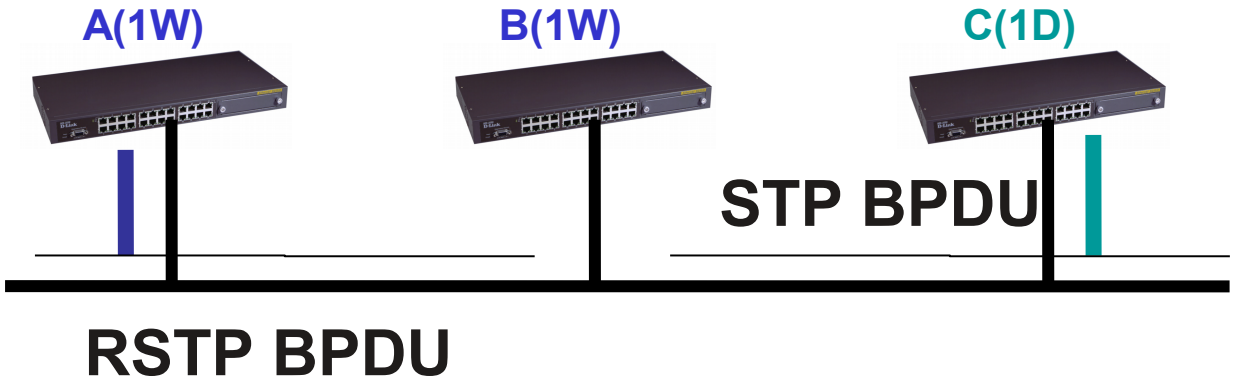
- Роли резервных портов

  Резервный порт – это порт заблокированный в результате получения более предпочтительных BPDU от того же самого коммутатора, которому он принадлежит.



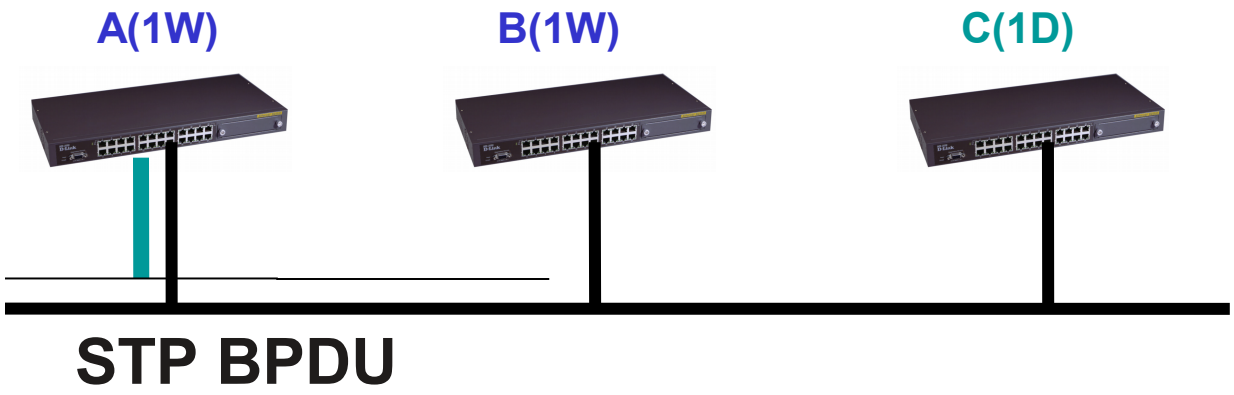
Совместимость с 802.1d

Например, коммутаторы A и B на схеме поддерживают RSTP, и коммутатор A является выделенным для данного сегмента. Устаревший коммутатор C, поддерживающий только STP также присутствует в сети. Так как коммутаторы 802.1d игнорируют RSTP BPDU и отбрасывают их, C считает, что в сегменте нет других коммутаторов и начинает посылать его BPDU формата 802.1d.



Совместимость с 802.1d

Коммутатор A получает эти BPDU и, максимум через два интервала Hello (таймер задержки переключения), изменяет режим на 802.1d только на этом порту. В результате, C может теперь понимать BPDU A и соглашается с тем, что A является выделенным коммутатором для данного сегмента.



Максимальный диаметр сети

Разница между 802.1d и 802.1w заключается в том, как инкрементируется параметр Возраст Сообщения. В 802.1d Возраст Сообщения – это счётчик, поддерживаемый корневым портом коммутатора и инкрементируемый им на 1. В 802.1w, значение инкрементируется на величину большую 1/16 Максимального Возраста но меньшую 1, округлённую до ближайшего целого.

Предельный диаметр сети достигается, когда:
((MessageAge+HelloTime)>=MaxAge)

Например, при умолчальных значениях MaxAge(20 с) и Hello (2 с), максимальный диаметр сети равен 18 переходам от корневого коммутатора, тем самым обеспечивая 37 коммутаторов в цепочке или кольце, при условии, что корневой коммутатор находится в центре.

Общие выводы: STP и RSTP

- Сходимость:

STP, 802.1d: 30 с.
RSTP, 802.1w: 2-3 с.

- Диаметр:

STP, 802.1d: 7 переходов
RSTP, 802.1w: 18 переходов

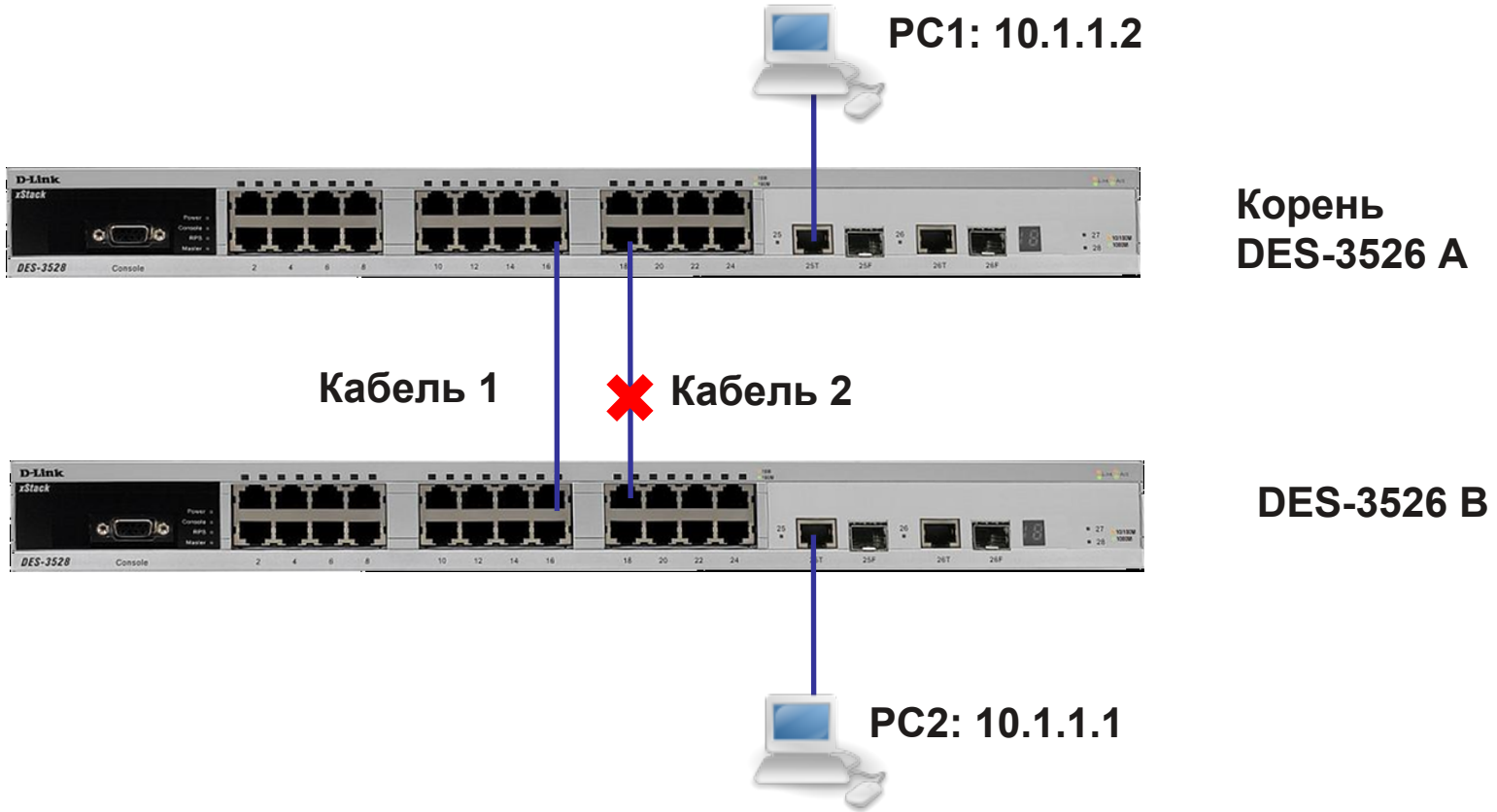
- 802.1w обратно совместим с 802.1d. Тем не менее, преимущество быстрой сходимости будет утеряно.

Пример RSTP

Задачи

- Посмотреть на практике как работает RSTP.
- Посмотреть в динамике состояния подключённых портов, чтобы понять принципы RSTP.
- PC1 пингует PC2 и PC2 пингует PC1 постоянно. Даже при отключении кабеля связность теряется не больше, чем на 1-2 секунды. (Время сходимости)
- Что случится после обратного подключения кабеля?

Пример RSTP



Включить STP на обоих коммутаторах DES-3526. Проверить заблокирован ли один порт DES-3526.
PC1 и PC2 пингуют друг друга постоянно.
Отсоединить кабель 1 и проверить сколько по времени (количество пропущенных ping) будет восстанавливаться связь.
Подсоединить кабель 1 обратно и посмотреть сколько будет восстанавливаться связь.

Настройка RSTP

DES-3526 A:

```
enable stp

# Сделать так, чтобы коммутатор A имел меньшее
значение приоритета для того, чтобы он стал
корневым.
# Приоритет по умолчанию = 32768.

config stp priority 4096 instance_id 1
```

DES-3526 B:

```
enable stp
```

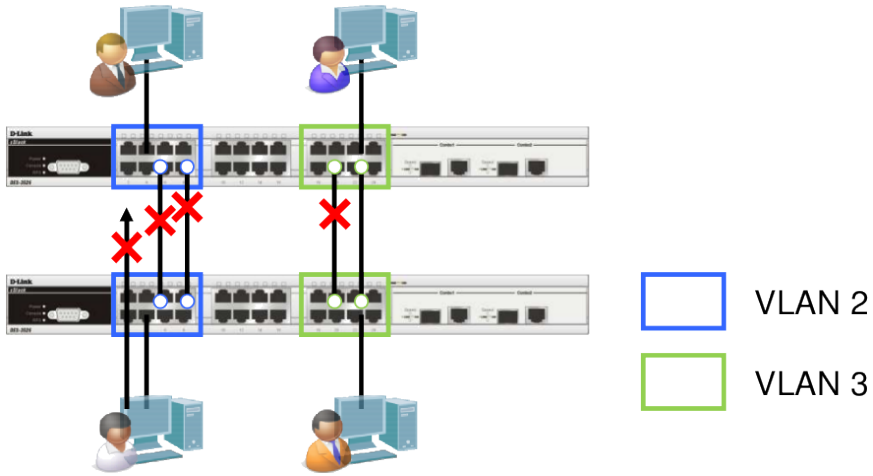
Проверка:

1. PC1 пингует PC2 и PC2 пингует PC1 постоянно.
2. Отключаем кабель 1. Связь может восстановиться через 1-2 с (потеря 1-2 ping) ➔ Время сходимости порядка 1-2 с.
3. Подсоединить кабель 1 обратно. Связь может восстановиться с потерей 1-2 ping.

Ограничение RSTP

Ограничение RSTP:

В сети может быть только одна копия **Spanning Tree** (одно дерево). Если на коммутаторе сконфигурировано несколько VLAN, то все они используют одну копию этого протокола. Это значит, что все VLAN образуют одну логическую топологию, не обладающую достаточной гибкостью. Этот протокол не может поддерживать своё «дерево» для каждого VLAN.



Решение: Протокол Multiple Spanning Tree, MSTP (IEEE 802.1s)

Протокол Multiple Spanning Tree, MSTP

- Стандартизирован IEEE 802.1s.
- MSTP позволяет использовать более одной копии STP в сети с 802.1q VLAN. Он позволяет одни VLAN связать с одной копией STP, а другие с другой, обеспечивая несколько связей между коммутаторами.
- Также MSTP предоставляет возможность распределения нагрузки.
- Каждая копия (покрывающее дерево) MSTP также использует протокол RSTP для более быстрой сходимости сети.

Регионы MSTP

Регион MSTP это связанная группа коммутаторов с поддержкой MSTP с одинаковой конфигурацией MST.

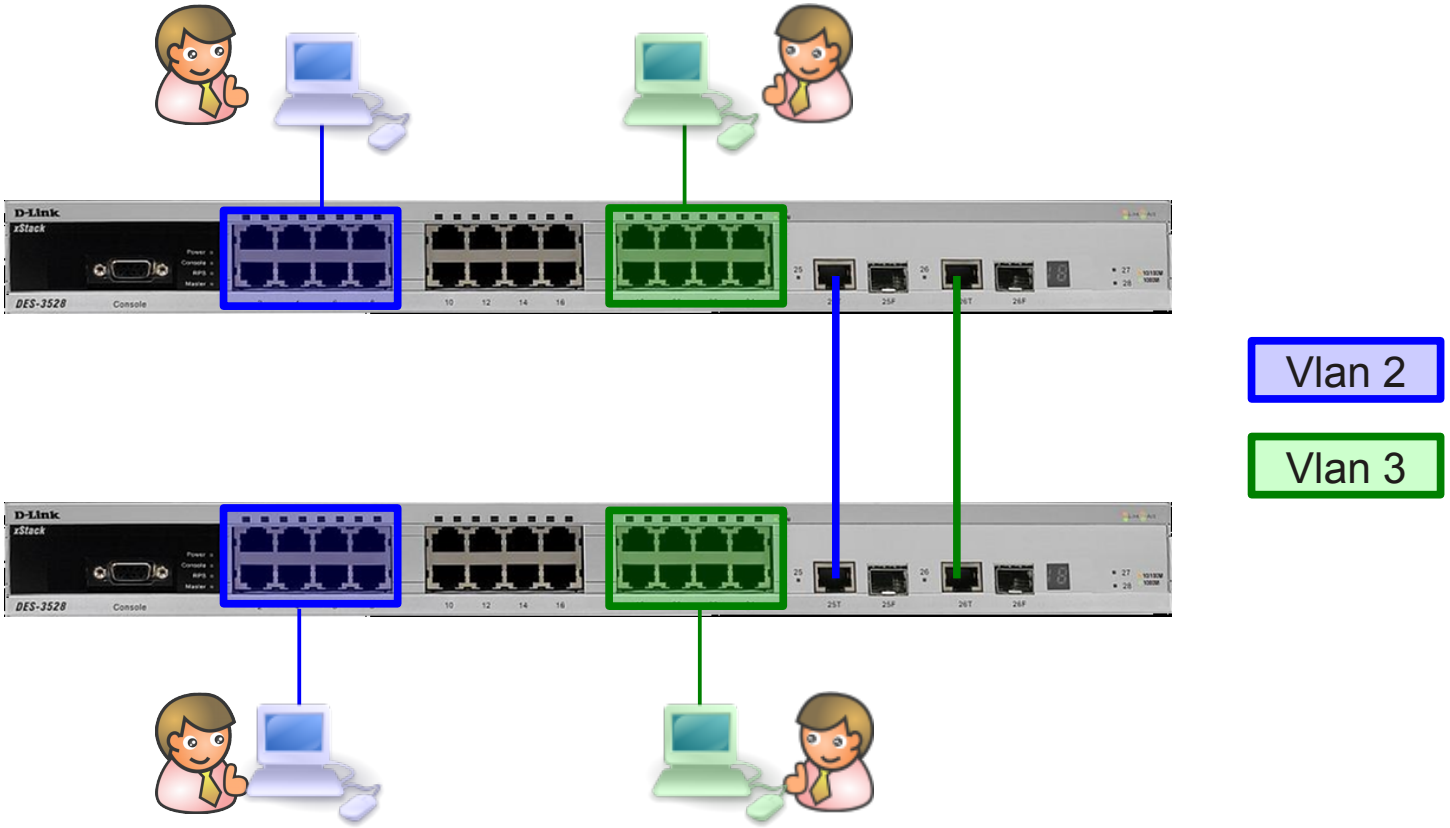
Для того, чтобы добиться одинаковой конфигурации MST нужно задать следующие одинаковые параметры:

- *Конфигурационное имя*
- *Конфигурационный номер ревизии*
- *Карту привязки VLAN к копиям STP*

Преимущества MSTP могут быть использованы только внутри региона. В разных регионах используется только одна копия STP для всех VLAN.

Пример работы MSTP

Распределение нагрузки при помощи MSTP



Порядок настройки MSTP

1. Включить STP на каждом устройстве.
2. Изменить версию STP на MSTP. (По умолчанию RSTP)
3. Задать имя региона MSTP и ревизию.
4. Создать копию и проассоциировать VLAN.
5. Сконфигурировать приоритет STP так, чтобы явно задать корневой коммутатор. По умолчанию это 32768. Чем меньше номер, тем больше приоритет. По умолчанию, чем меньше значение MAC, тем больше вероятность стать корневым коммутатором.
6. Задать приоритеты на портах так, чтобы задать порт в VLAN, который будет заблокирован.
7. Задать пограничный порт.

MSTP Пример 2: Распределение нагрузки

Конфигурация DES-3526_A

```
config vlan default delete 1-24

create vlan v2 tag 2
config vlan v2 add untagged 1-8
config vlan v2 add tagged 25-26
create vlan v3 tag 3
config vlan v3 add untagged 17-24
config vlan v3 add tagged 25-26
enable stp
config stp version mstp
config stp mst_config_id name abc
config stp mst_config_id 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

## Задать приоритет STP так, чтобы коммутатор A стал
корневым.
config stp priority 4096 instance_id 0
config stp priority 4096 instance_id 2
config stp priority 4096 instance_id 3

## Задать приоритеты портов так, чтобы порт 25 стал
активным
## для v2, а порт 26 - для v3.
config stp mst_ports 25 instance_id 2 priority 96
config stp mst_ports 26 instance_id 3 priority 96
config stp ports 1-24 edge true
```

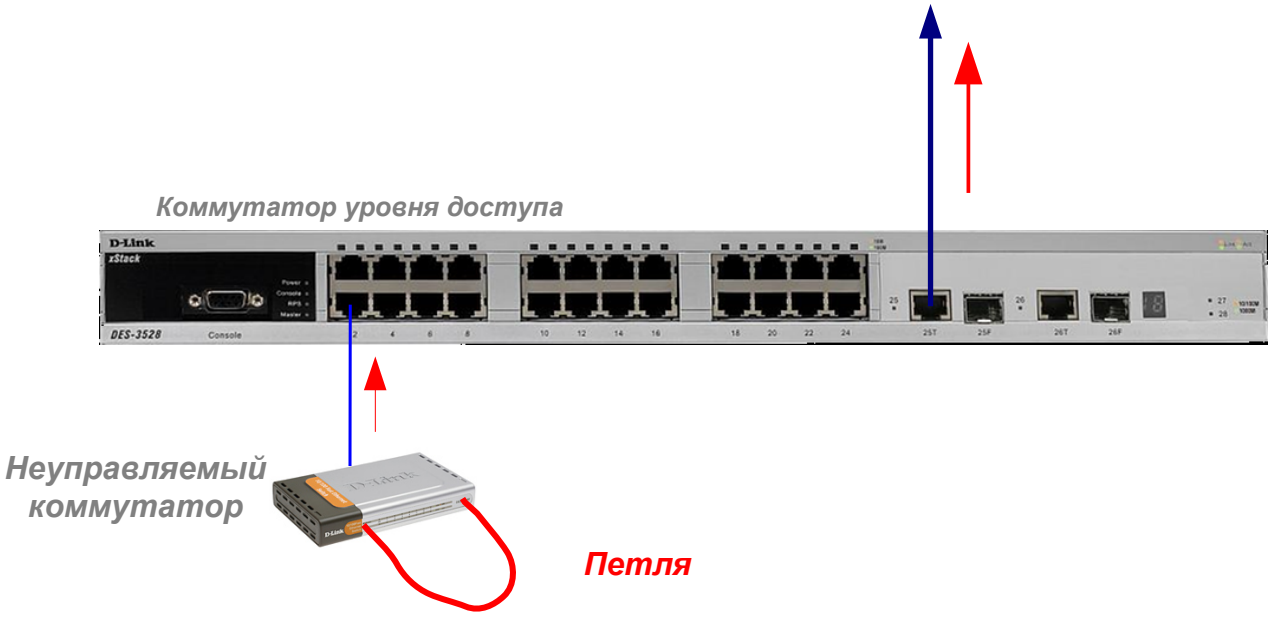
Конфигурация DES-3526_B

```
config vlan default delete 1-24

create vlan v2 tag 2
config vlan v2 add tagged 25-26
config vlan v2 add untagged 1-8

create vlan v3 tag 3
config vlan v3 add tagged 25-26
config vlan v3 add untagged 17-24

enable stp
config stp version mstp
config stp mst_config_id name abc
config stp mst_config_id 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 1-24 edge true
```

```
## Команды отладки для A и B
show stp instance_id
show stp ports
```

Функция LoopBack Detection

Обнаружение «петель» на порту коммутатора: STP LoopBack Detection



Ситуация, показанная на рисунке, вынуждает управляемый коммутатор постоянно перестраивать «дерево» STP при получении своего же собственного BPDU. Новая функция LoopBack Detection отслеживает такие ситуации и блокирует порт, на котором обнаружена петля, тем самым предотвращая проблемы в сети.

LoopBack Detection (пример)

- Задача: Обеспечить на клиентских портах DES-3526 отсутствие петель в неуправляемых сегментах.

  1-ый вариант – петля обнаруживается для порта в целом и блокируется весь порт (режим Port-Based):

- Команды для настройки коммутатора:

  1) **enable loopdetect**

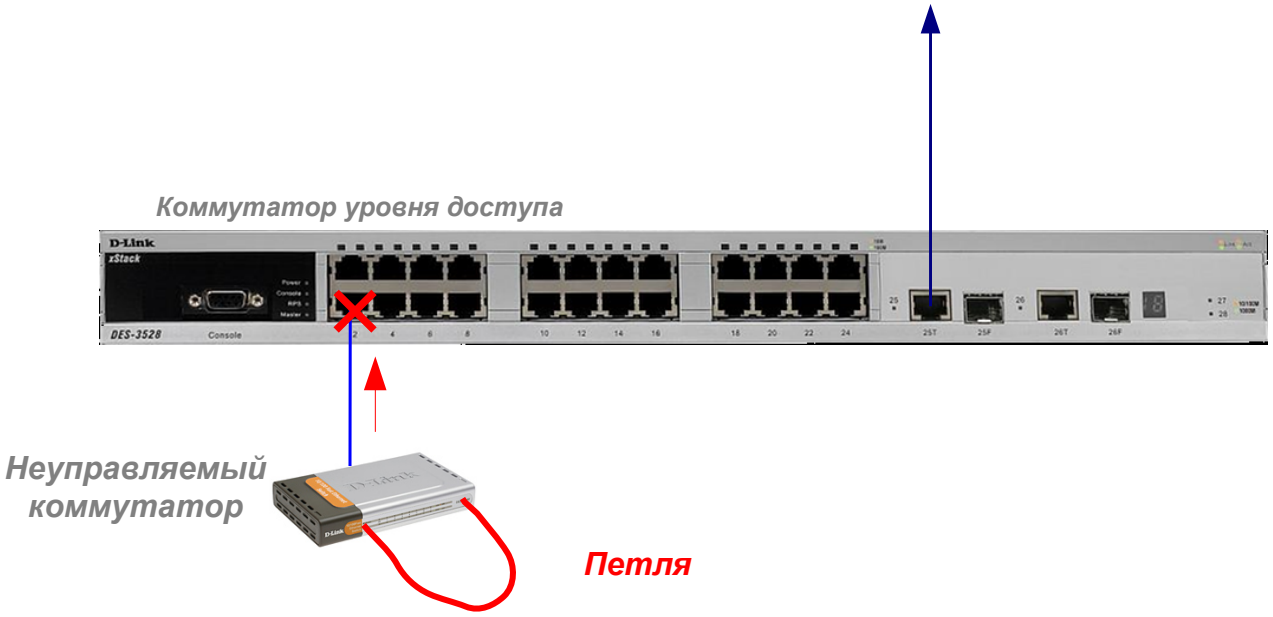
  2) **config loopdetect recover_timer 60** (lbd_recover_timer – время, в течение которого порты будут заблокированы. Оно задаётся глобально на коммутаторе. Если необходимо отключить эту функцию, то следует установить его в 0)

  3) **config loopdetect interval 10** (временной интервал в секундах между отсылаемыми пакетами ECTP (Ethernet Configuration Testing Ptotocol))

  4) **config loopdetect mode port-based** (выбор режима работы функции. При обнаружении петли будет блокироваться весь трафик по порту)

  5) **config loopdetect ports 1-26 state enabled**

Обнаружение «петель» на порту коммутатора: LoopBack Detection



В этой схеме необязательна настройка протокола STP на портах, где необходимо определять наличие петли. В этом случае петля определяется отсылкой с порта специального служебного пакета. При возвращении его по этому же порту порт блокируется на время указанное в таймере. Есть два режима этой функции Port-Based и VLAN-Based.

LoopBack Detection (пример)

- Задача: Обеспечить на клиентских портах DES-3526 отсутствие петель в неуправляемых сегментах.

  2-ой вариант – петля обнаруживается для каждого VLAN-а и блокируется только трафик этого VLAN-а (режим Port-Based):

- Команды для настройки коммутатора:

  1) **enable loopdetect**
  2) **config loopdetect recover_timer 60** (lbd_recover_timer – время, в течение которого порты будут заблокированы. Оно задаётся глобально на коммутаторе. Если необходимо отключить эту функцию, то следует установить его в 0)
  3) **config loopdetect interval 10** (временной интервал в секундах между отсылаемыми пакетами ECTP (Ethernet Configuration Testing Ptotocol))
  4) **config loopdetect mode vlan-based** (выбор режима работы функции. При обнаружении петли в VLAN будет блокироваться трафик по порту только в этом VLAN-е)
  5) **config loopdetect ports 1-26 state enabled**

Агрегирование каналов связи

Агрегирование каналов связи

Типы агрегирования каналов связи

- Статическое:
  - все настройки на коммутаторах выполняются вручную, и они не допускают динамических изменений в агрегированной группе.

- Динамическое, на основе стандарта IEEE 802.3ad (LACP):
  - используется протокол управления агрегированным каналом – Link Aggregation Control Protocol (LACP).

Агрегирование каналов связи

Link Aggregation Control Protocol (LACP)

- Протокол LACP определяет метод управления объединением нескольких физических портов в одну логическую группу и предоставляет сетевым устройствам возможность автосогласования каналов (их добавления или удаления), путем отправки управляющих кадров протокола LACP непосредственно подключенным устройствам с поддержкой LACP.
- Кадры LACP отправляются устройством через все порты, на которых активизирован протокол.
- Порты, на которых активизирован протокол LACP, могут быть настроены для работы в одном из двух режимов:

○ **активном** (*active*):

порты выполняют обработку и рассылку управляющих кадров протокола LACP.

○ **пассивном** (*passive*):

порты выполняют только обработку управляющих кадров LACP.

Агрегирование каналов связи

Ограничения при настройке агрегирования каналов связи

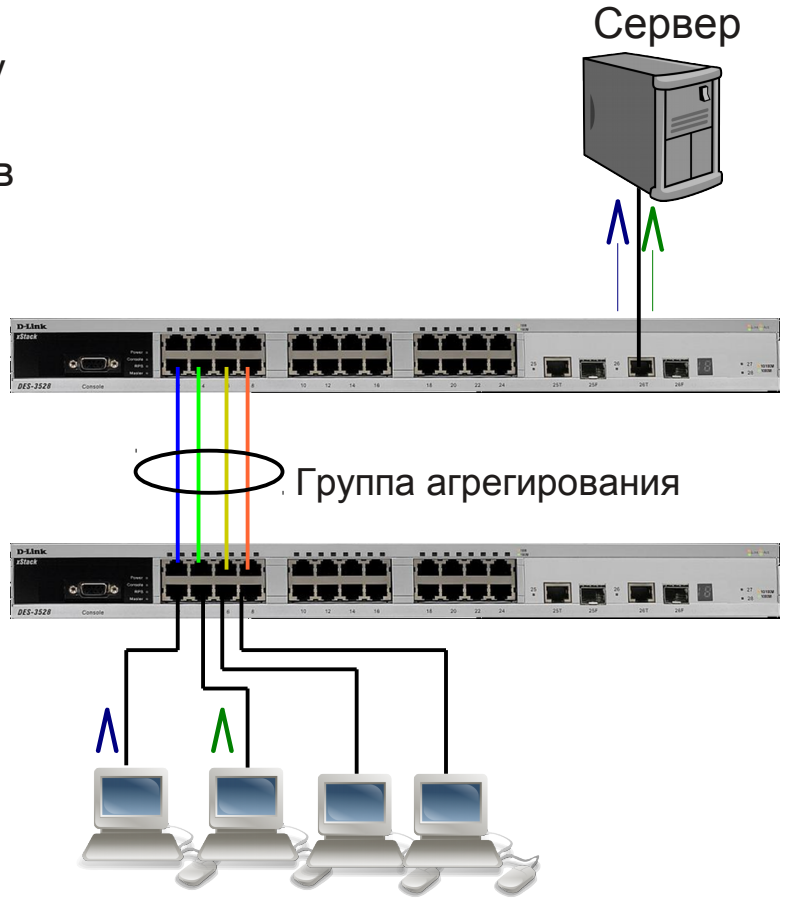
У портов, объединяемых в агрегированный канал, нижеперечисленные характеристики должны иметь одинаковые настройки:

- тип среды передачи;
- скорость;
- режим работы – полный дуплекс;
- метод управления потоком (Flow Control) .

При объединении портов в агрегированный канал на них не должны быть настроены функции аутентификации 802.1X, зеркалирования трафика и блокировки портов.

Агрегирование каналов связи

В сети есть 4 клиентских PC с доступом к общему серверу. Трафик может быть разделён по 4-м агрегированным портам, посредством алгоритмов распределения нагрузки на основе MAC-адресов.



Описание:

Трафик между PC-1 и сервером через первый агрегированный порт.

Трафик между PC-2 и сервером через второй агрегированный порт.
Трафик между PC-3 и сервером через третий агрегированный порт.
Трафик между PC-4 и сервером через четвёртый агрегированный порт.

Статическое агрегирование портов по сравнению с LACP

Протокол управления агрегированным каналом – Link Aggregation Control Protocol IEEE 802.3ad (LACP) используется для организации динамического агрегированного канала между коммутаторам и другим сетевым устройством. Для статических агрегированных каналов (по умолчанию они являются статическими) соединяемые коммутаторы должны быть настроены вручную, и они не допускают динамических изменений в агрегированной группе. Для динамических агрегированных каналов (назначенные LACP-совместимые порты) коммутаторы должны быть совместимы с LACP для автосогласования этих каналов. Динамический агрегированный канал обладает функцией автосогласования, если с одной стороны агрегированная группа настроена как активная (active), а с другой – как пассивная (passive).

Если тип канала явно не указан, то это статическое агрегирование. Агрегированные порты могут быть либо *LACP* либо *Static*. LACP означает, что порты совместимы с LACP, т.е. могут быть подключены только к LACP-совместимому устройству. Порты в статической группе не могут динамически менять конфигурацию, и оба устройства, соединённые посредством такой группы, должны быть настроены вручную, если меняется состав группы и т.д.

Агрегирование каналов связи

Алгоритмы агрегирования портов

Алгоритм агрегирования портов (Link Aggregation Algorithm) на основании некоторых признаков поступающих пакетов закрепляет за определенным портом агрегированного канала поток кадров определенного сеанса между двумя узлами.

В коммутаторах D-Link поддерживается 9 алгоритмов агрегирования портов:

1. ***mac_source*** –MAC-адрес источника;
2. ***mac_destination*** – MAC-адрес назначения;
3. ***mac_source_dest*** – MAC-адрес источника и назначения;
4. ***ip_source*** – IP-адрес источника;
5. ***ip_destination*** – IP-адрес назначения;
6. ***ip_source_dest*** – IP-адрес источника и назначения;
7. ***l4_src_port*** – TCP/UDP-порт источника;
8. ***l4_dest_port*** – TCP/UDP-порт назначения;
9. ***l4_src_dest_port*** – TCP/UDP-порт источника и назначения.

По умолчанию используется алгоритм ***mac_source***

Статическое агрегирование каналов (Пример)

Настройка агрегирования каналов

Для коммутатора A (порты в группе - 2, 4, 6 и 8)

Рекомендации:

1. Создайте группу агрегирования

create link_aggregation group_id 1 type static

config link_aggregation algorithm mac_destination

2. Задайте членов этой группы

config link_aggregation group_id 1 master_port 2 ports 2,4,6,8 state enabled

Для коммутатора B (порты в группе - 1, 3, 5 и 7)

Рекомендации:

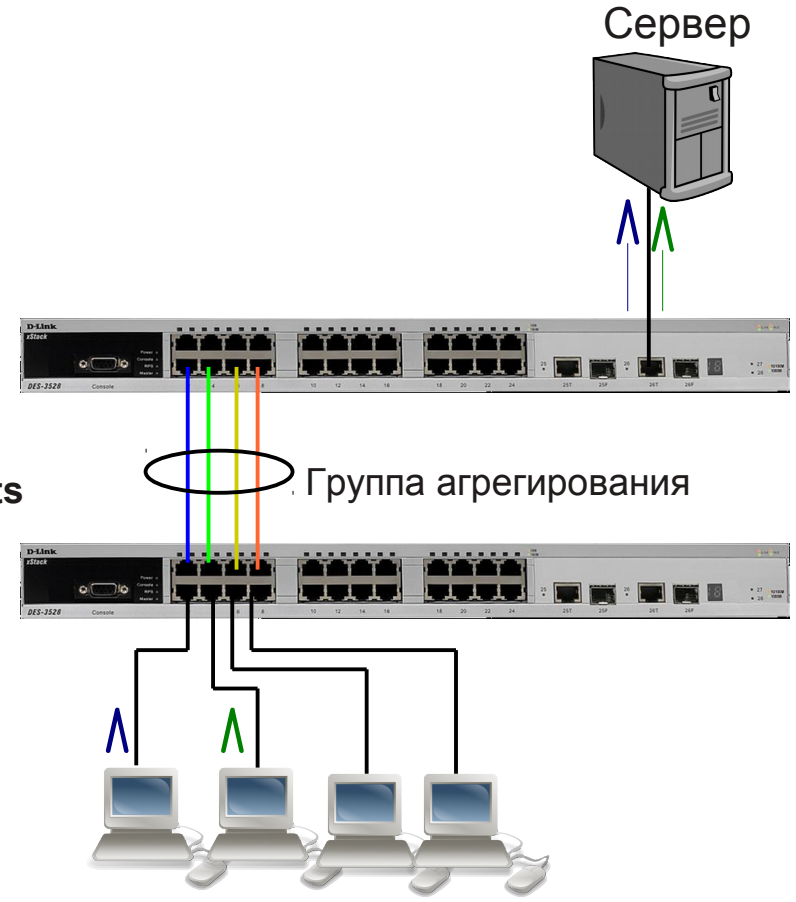
1. Создайте группу агрегирования

create link_aggregation group_id 1

config link_aggregation algorithm mac_source

2. Задайте членов этой группы

config link_aggregation group_id 1 master_port 1 ports 1,3,5,7 state enabled



Агрегирование каналов связи

Настройка агрегирования каналов (LACP)

Настройка коммутатора 1

▪Создать группы агрегирования (тип канала LACP) и задать алгоритм агрегирования.

```
create link_aggregation group_id 1 type lacp
create link_aggregation group_id 2 type lacp
config link_aggregation algorithm mac_destination
```

▪Включить порты 1, 2, 3, 4 в группу 1 и выбрать порт 1 в качестве мастера-порта.

```
config link_aggregation group_id 1 master_port 1
ports 1-4 state enabled
```

▪Включить порты 5, 6, 7, 8 в группу 2 и выбрать порт 5 в качестве мастера-порта.

```
config link_aggregation group_id 2 master_port 5 port
5-8 state enabled
```

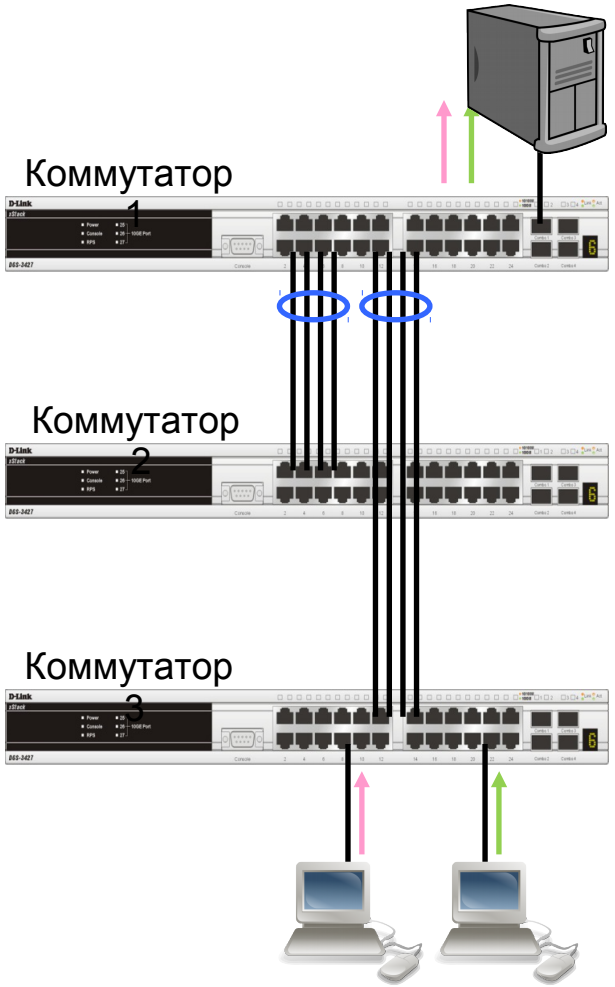
▪Настроить для портов 1-8 активный режим работы.

```
config lacp_port 1-8 mode active
```

Настройка коммутаторов 2 и 3

(на портах 1-4 этих коммутаторов включено автосогласование)

```
create link_aggregation group_id 1 type lacp
config link_aggregation algorithm mac_source
config link_aggregation group_id 1 master_port 1
ports 1-4 state enabled
```



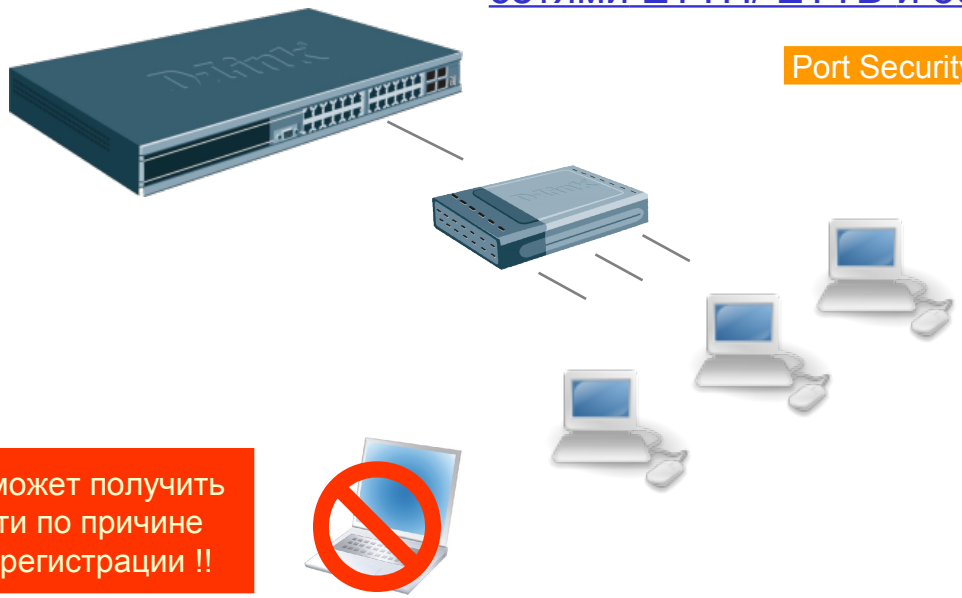
Безопасность на уровне портов и защита от вторжений

Port Security
(безопасность на уровне портов)

Безопасность на уровне портов (Port Security)

Функция *Port Security* в коммутаторах D-Link позволяет регулировать количество компьютеров, которым разрешено подключаться к каждому порту. Более того, она позволяет предоставлять доступ к сети только зарегистрированным компьютерам

Эта функция специально разработана для управления сетями ETTH/ ETTB и офисными сетями



Port Security

Режимы работы функции Port Security

Существует три режима работы функции Port Security:

- *Permanent* (Постоянный) – занесенные в таблицу коммутации MAC-адреса никогда не устаревают, даже если истекло время, установленное таймером FDB Aging Time или коммутатор был перезагружен.

- *Delete on Timeout* (Удалить по истечении времени) – занесенные в таблицу коммутации MAC-адреса устареют после истечения времени, установленного таймером FDB Aging Time и будут удалены.

- *Delete on Reset* (Удалить при сбросе настроек) – занесенные в таблицу коммутации MAC-адреса будут удалены после перезагрузки коммутатора (этот режим используется по умолчанию).

Port Security

Настройка функции Port Security

- На портах 1-3 управляемого коммутатора настроить ограничение по количеству подключаемых пользователей равное 2. MAC-адреса подключаемых пользователей изучаются динамически. Режим работы функции - Delete on Timeout.

```
config port_security ports 1-3 admin_state enabled max_learning_addr 2
   lock_address_mode DeleteOnTimeout
```

- Проверить настройку функции можно с помощью команды:

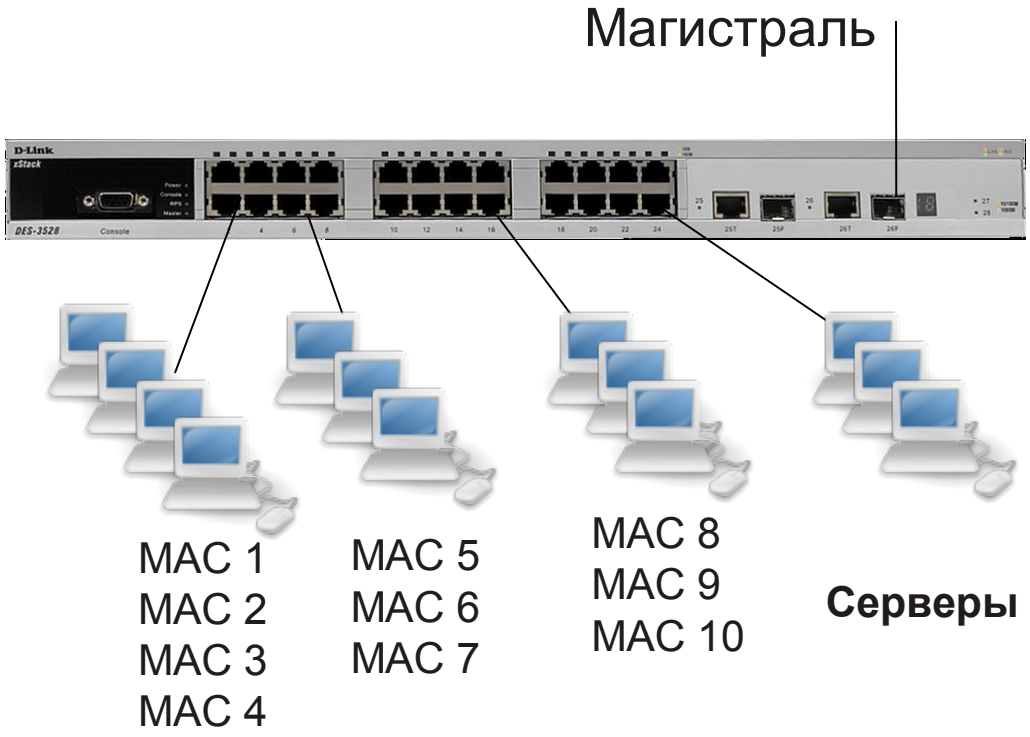
```
show port_security
```

- Если необходимо, чтобы коммутатор отправлял сообщение SNMP Trap или создавал запись в Log-файле при подключении неавторизованного пользователя к порту коммутатора, администратор может настроить выполнение этих действий с помощью команды:

```
enable port_security trap_log
```

Port Security (Пример)

Задача: Незарегистрированные на порту MAC-адреса не могут получить доступ к сети



- Включить Port Security на портах, и установить Max. Learning Addresses = 0 для портов, на которых необходима защита от вторжений
- Добавить нужные MAC-адреса в статическую таблицу MAC-адресов.

Настройка функции Port Security

Используя функцию Port Security можно полностью запретить динамическое изучение MAC-адресов указанными или всеми портами коммутатора. В этом случае доступ к сети получат только те пользователи, MAC-адреса которых указаны в статической таблице коммутации.

Настройка коммутатора

- Активизировать функцию Port Security на соответствующих портах и запретить изучение MAC-адресов (параметр `max_learning_addr` установить равным 0).

```
config port_security ports 1-24 admin_state enabled max_learning_addr 0
```

- Создать записи в статической таблице MAC-адресов (имя VLAN в примере “default”).

```
create fdb default 00-50-ba-00-00-01 port 2
create fdb default 00-50-ba-00-00-02 port 2
create fdb default 00-50-ba-00-00-03 port 2
create fdb default 00-50-ba-00-00-04 port 2
create fdb default 00-50-ba-00-00-05 port 8
....... (аналогично для всех требуемых портов)
```

Функции управления и мониторинга

Начальная настройка коммутатора

Средства управления коммутаторами

К основным средствам управления и мониторинга относятся:

- Web-интерфейс управления;
- Интерфейс командной строки (Command Line Interface, CLI);
- Telnet;
- SNMP-управление.

Начальная настройка коммутатора

Пример присвоения IP-адреса управляющему интерфейсу на коммутаторе DES-3528

```
DES-3528#config ipif System ipaddress 192.168.100.240/24
Command: config ipif System ipaddress 192.168.100.240/24
Success.
```

Проверить правильность настройки IP-адреса коммутатора можно с помощью команды:

```
show ipif
```

Начальная настройка коммутатора

Базовая конфигурация коммутатора

Настройка параметров портов коммутатора.

Для установки параметров портов на коммутаторах D-Link используется команда

config ports

Пример использования команды:

```
DES-3528#config ports 1-3 speed 10_full learning enable state
   enable flow_control enable
Command: config ports 1-3 speed 10_full learning enable state
   enable flow_control enable
Success
```

Проверить настройки параметров портов можно с помощью команды:

show ports *<список портов>*

Начальная настройка коммутатора

Базовая конфигурация коммутатора

Шаг 4. Сохранение текущей конфигурации коммутатора в энергонезависимую память NVRAM.

Активная конфигурация хранится в оперативной памяти SDRAM. При отключении питания, конфигурация, хранимая в этой памяти, будет потеряна.

Для того чтобы сохранить конфигурацию в энергонезависимой памяти NVRAM, необходимо выполнить команду

save

```
DES-3528#save
Command: save
Saving all settings to NV-RAM……Done
```

Начальная настройка коммутатора

Команды «Show»

Команды «**Show**» являются удобным средством проверки состояния и параметров коммутатора, предоставляя информацию, требуемую для мониторинга и поиска неисправностей в работе коммутаторов.

На следующем слайде приведен список наиболее общих команд «Show».

Начальная настройка коммутатора

Команды «Show»

`show config`	эта команда используется для отображения конфигурации, сохраненной в NV RAM или созданной в текущий момент
`show fdb`	эта команда используется для отображения текущей таблицы коммутации
`show switch`	эта команда используется для отображения общей информации о коммутаторе
`show device_status`	эта команда используется для отображения состояния внутреннего и внешнего питания коммутатора
`show error ports`	эта команда используется для отображения статистики об ошибках для заданного диапазона портов
`show firmware information`	эта команда используется для отображения информации о программном обеспечении коммутатора (прошивке)
`show ipif`	эта команда используется для отображения информации о настройках IP-интерфейса на коммутаторе

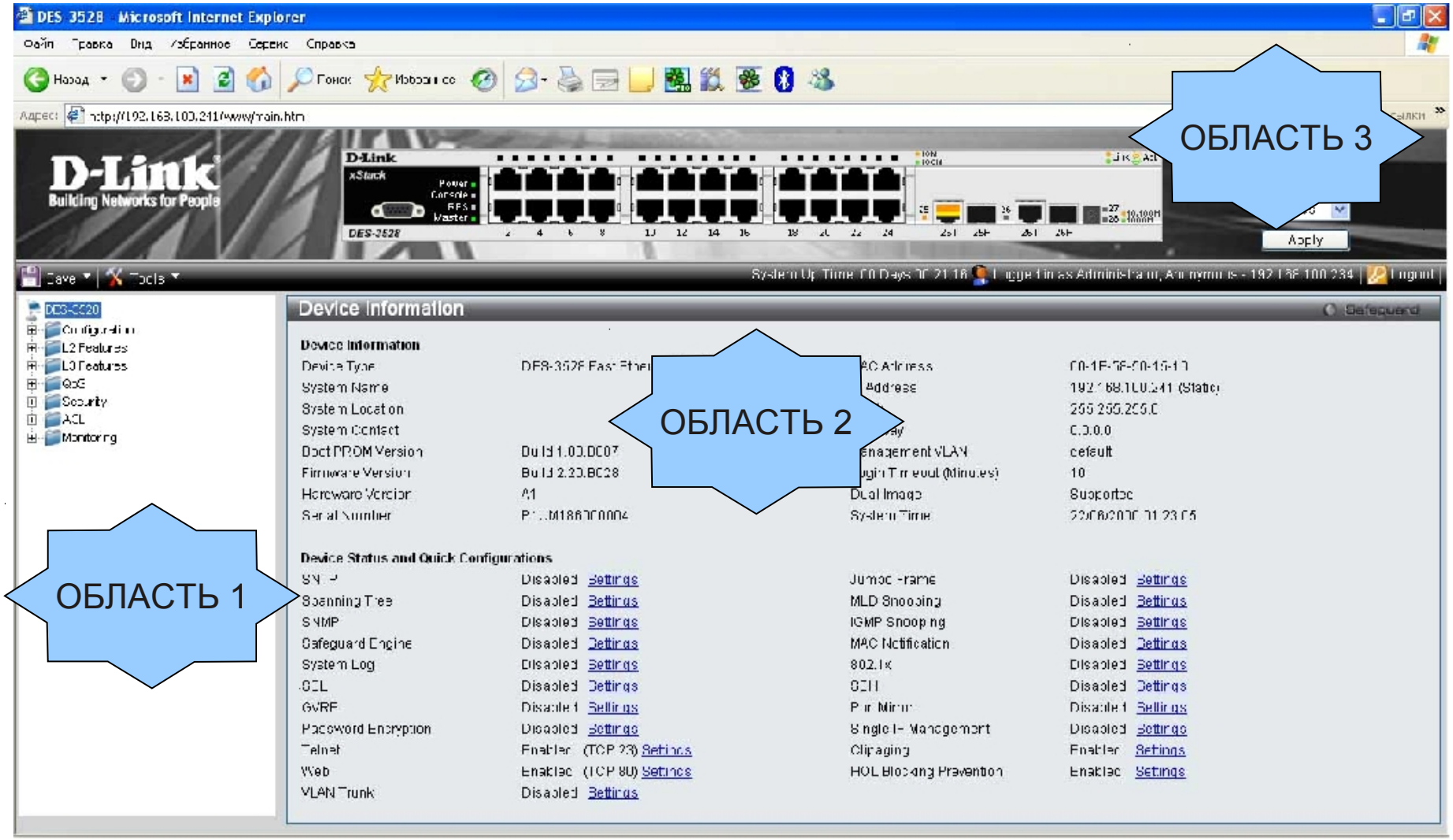
Начальная настройка коммутатора

Команды «Show»

`show packet ports`	эта команда используется для отображения статистики о переданных и полученных портом пакетах
`show log`	эта команда используется для просмотра Log-файла коммутатора

Начальная настройка коммутатора

Web-интерфейс управления



Спасибо

D-Link®
Building Networks for People