D-Link
Building Networks for People

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

Дёмин Иван, консультант по проектам

idemin@dlink.ru

D-Link
Building Networks for People

Виртуальные Локальные Сети - VLAN

- Дополнительное деление сетевых сегментов для уменьшения трафика и перегрузок
- Логические группы в LAN
- VLAN подобны широковещательным доменам
- Обеспечение безопасности и разделения доступа к ресурсам

Типы VLAN

- VLAN на базе портов
- VLAN на базе меток IEEE 802.1q
- VLAN на базе протоколов IEEE 802.1v

802.1q – VLAN на базе меток

D-Link
Building Networks for People

Преимущества IEEE 802.1q VLAN

- Гибкость и удобство настройки и изменения
- Возможность работы протокола Spanning Tree
- Возможность работы с сетевыми устройствами, которые не распознают метки
- Устройства разных производителей, могут работать вместе
- Не нужно применять маршрутизаторы, чтобы связать подсети

Маркированные кадры-Tagged Frame

- 12-бит VLAN маркер
- Идентифицирует кадр, как принадлежащий VLAN

- Max. Размер маркированного кадра Ethernet 1522 байт
- Немаркированный кадр это кадр без VLAN маркера

VID и PVID

- VID (VLAN Identifier)
- 12-bit часть VLAN маркера
- Указывает какая VLAN
- 12 бит определяет 4096 VLAN’ов
- VID 0 и VID 4095 зарезервированы

- PVID (Port VID)
- Ассоциирует порт с VLAN
- Например,

  Порту с PVID 3, предназначены все немаркированные пакеты VLAN 3

D-Link
Building Networks for People

Правила коммутации маркированных & немаркированных портов (Входящие данные)

- Прием данных с маркером
  - Проверка маркировки VID
  - Коммутация кадра на определенную VLAN группу
- Прием данных без маркера
  - Проверка его PVID
  - Коммутация кадра на определенную VLAN группу

Правила коммутации маркированных & немаркированных портов (Исходящие данные)

- Исходящий порт – маркированный порт
  - Маркировка кадра
  - Для идентификации кадра как принадлежащего VLAN группе
- Исходящий порт – немаркированный порт
  - Удаление маркера

Выходящие (Egress) порты

- Установка портов, передающих трафик в VLAN похожа на маркированные и немаркированные кадры
- Это означает, что VLAN кадры могут передаваться (выходить) через выходящие порты.
- Таким образом, порт, принадлежащий VLAN, должен быть Выходящим (Egress) портом (“E”)

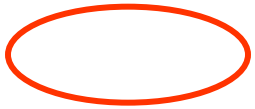
Маркированный входящий пакет (Часть 1)

- 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 (Часть 2)

Немаркированный входящий пакет (Часть 1)

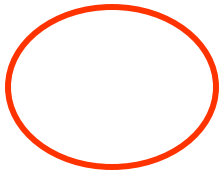


- PVID порта 4 -> 2
- Входящий немаркированный пакет назначен на VLAN 2
- Порт 5 маркированный Выходящий VLAN 2
- Порт 7 немаркированный Выходящий VLAN 2

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

D-Link
Building Networks for People

Немаркированный входящий пакет (Часть 2)



Немаркированный пакет маркируется, т.к.он выходит через маркированный порт

Немаркированный пакет не изменен, т.к. выходит через немаркированный порт.

D-Link
Building Networks for People

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

D-Link
Building Networks for People

Ассиметричные VLAN

для сетевых серверных приложений с использованием коммутатора L2

D-Link
Building Networks for People

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: Ассиметричные VLAN или сегментация трафика
- Решение на уровне L3: Коммутация L3 + ACL для ограничения доступа между .

D-Link
Building Networks for People

Деление сети на две VLAN с предоставлением общего файл-сервера

D-Link
Building Networks for People

Пример 1: Ассиметричные 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.

D-Link
Building Networks for People

Пример 1: Ассиметричные VLAN

Настройки PVID и VLAN:

порты	1-8	9-16	17-24
pvid	1..1	2..2	3..3
VLAN			
default	E..E	E..E	E..E
(V1)	U..U	U..U	U..U
V2	E..E	E..E	-..-
	U..U	U..U	-..-
V3	E..E	-..-	E..E
	U..U	-..-	U..U

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

Ограничения ассиметричных VLAN

Функция IGMP Snooping не работает при использовании ассиметричных VLAN.

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

D-Link
Building Networks for People

802.1v – VLAN на базе портов и протоколов

D-Link
Building Networks for People

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.

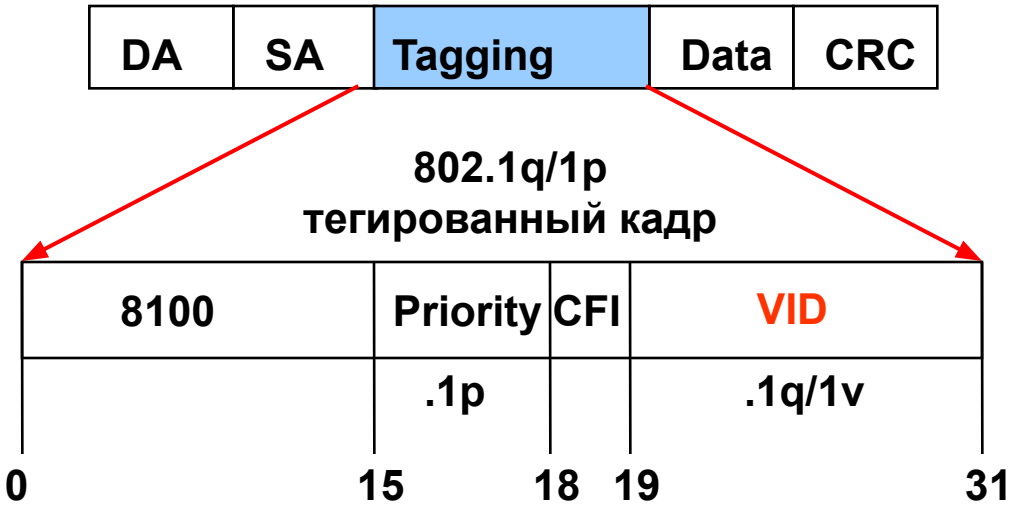
Это, 32-х битное поле (VLAN Tag) в заголовке кадра, которое идентифицирует кадр по принадлежности к определенному VLAN или по приоритету.

Максимальный размер тегированного кадра Ethernet - 1522 байтов

(1518 + 4 байта тега).

Кадр без тега называется нетегированным кадром или просто кадром.

Обычный (или нетегированный) кадр



Priority (1p) - 3 бита, 0-7.

VID (1q/1v) - 12 бит, 0-4095.

D-Link
Building Networks for People

802.1q VLAN на основе портов (выводы)

Ingress (входящий кадр):

- При получении **тегированного** кадра, значения VID/priority не меняются.
- При получении **нетегированного** кадра, добавляется тег с VID=PVID and приоритетом = приоритету по умолчанию 802.1p

Внутри коммутатора (все кадры тегированы)

- Для VLAN, основываясь на VID, свериться с таблицей VLAN и перенаправить кадр только на порты в этом VLAN.
- Для priority, основываясь на заданном классе обслуживания, обработать кадр в соответствии с заданным приоритетом.

Egress (исходящий кадр):

- **Нетегированный** выходной порт: Убрать тег.
- **Тегированный** выходной порт: Не менять информацию в теге так, чтобы информация 1p/1q могла быть передана на следующий, поддерживающий 802.1p/q, коммутатор.

D-Link
Building Networks for People

802.1v VLAN на основе портов и протоколов (выводы)

Ingress (входящий кадр):

- Если получен **тегированный** кадр, значения VID/priority остаются неизменными, в противном случае
- Если получен **нетегированный** кадр
  - Если тип протокола в кадре соответствует типу VLAN на основе протоколов на этом порту, VID= (VID этого VLAN на основе протоколов).
  - Если поля «тип протокола» нет, VID=PVID входящего порта.

Добавить тег с VID и приоритетом по умолчанию 802.1p входного порта к кадру.

Внутри коммутатора (все кадры тегированы)

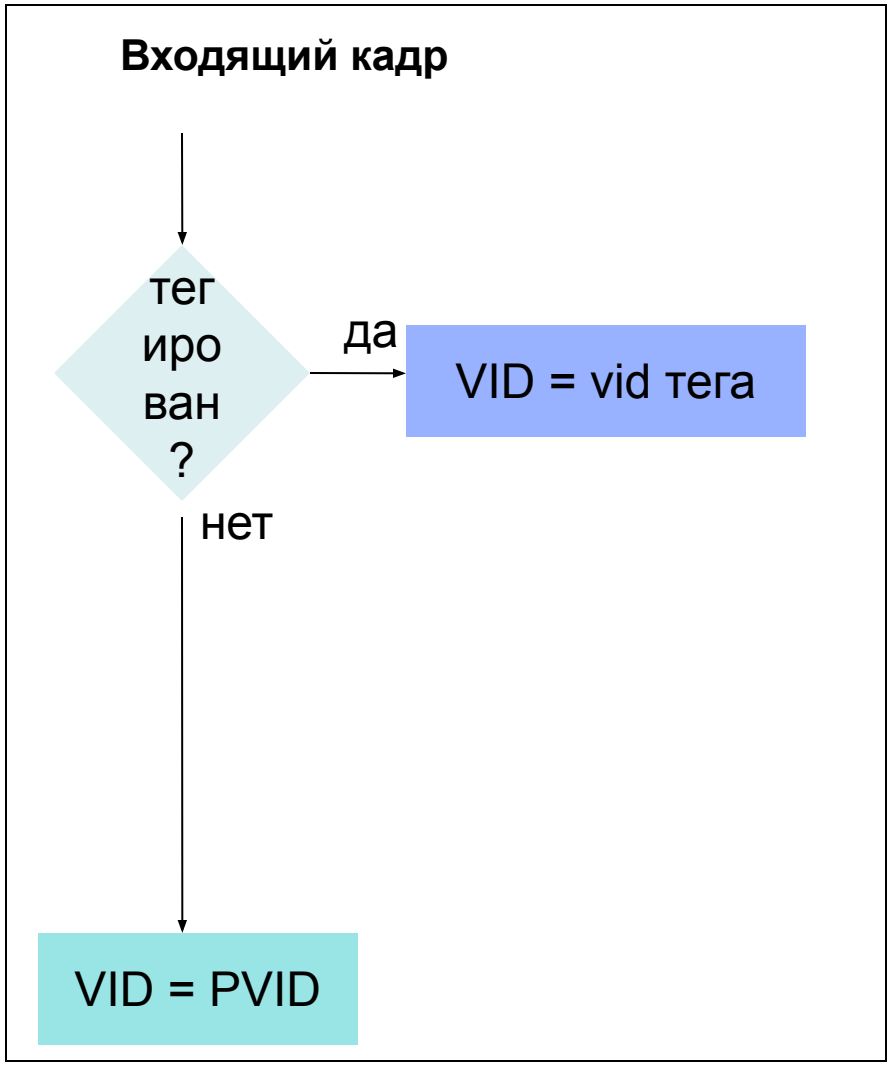
- Для VLAN, основываясь на VID, свериться с таблицей VLAN и перенаправить кадр только на порты в этом VLAN.
- Для priority, основываясь на заданном классе обслуживания, обработать кадр в соответствии с заданным приоритетом.

Egress (исходящий кадр):

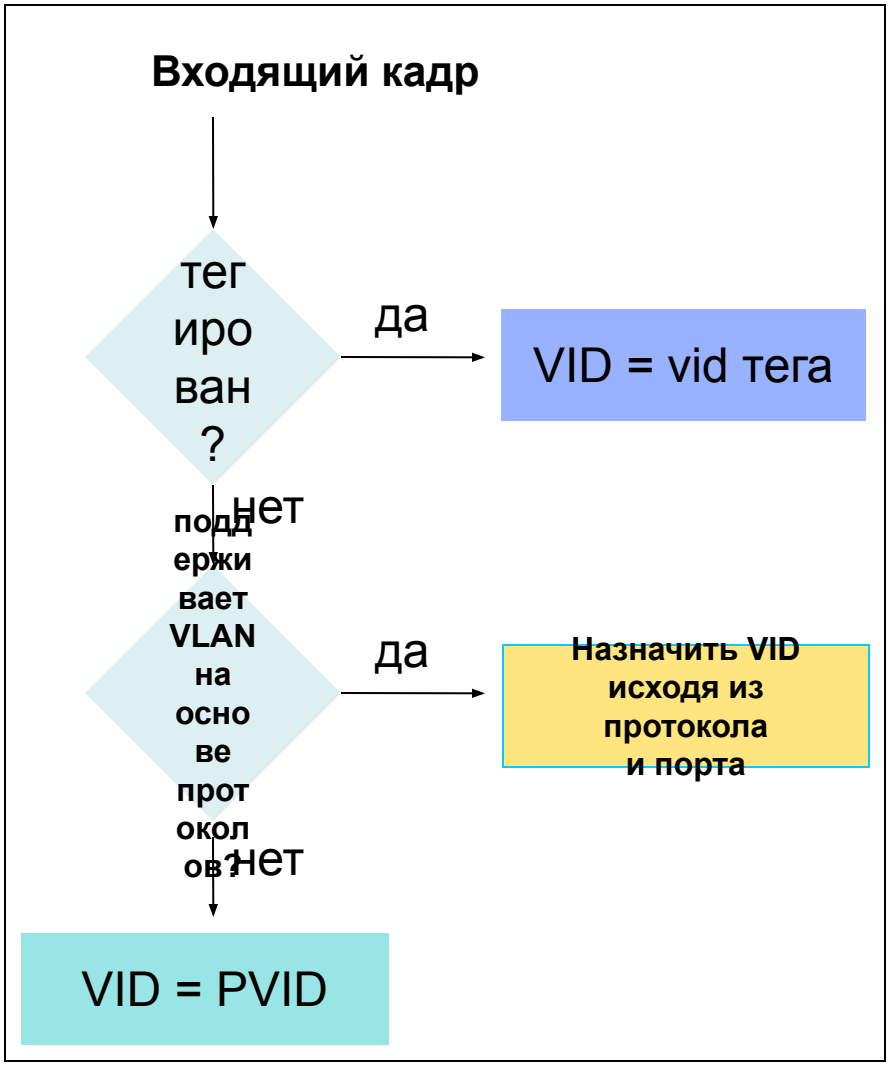
- **Нетегированный** выходной порт: Убрать тег.
- **Тегированный** выходной порт: Не менять информацию в теге так, чтобы информация 1p/1q могла быть передана на следующий, поддерживающий 802.1p/q, коммутатор.

Правило классификации VLAN

802.1Q VLAN на основе портов



802.1v VLAN на основе портов и протоколов



D-Link
Building Networks for People

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:

Возможна настройка до 7 VLAN на основе протоколов на каждом порту

Пример 1 – Выделенный VLAN на основе протоколов

DGS-3324SR

Сервер IP,
192.168.4.x/24
Шлюз
192.168.4.254

IPv6 VLAN на основе протоколов
Пользователи IPv6

Пользователи протокола IP
192.168.2.x/24
Шлюз
192.168.2.254

Задание:

Порты 1-8 – это IPv6 VLAN на основе протоколов. Пользователи в этом VLAN используют протокол IPv6. В этом VLAN должны присутствовать только пакеты IPv6, а пакеты других протоколов, включая IPv4, должны отбрасываться, чем обеспечивается более высокая производительность и уровень безопасности. Пользователи IPv6 НЕ МОГУТ взаимодействовать с другими подсетями.

D-Link
Building Networks for People

Пример 1 – Выделенный VLAN на основе протоколов

На DGS-3324SR

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.

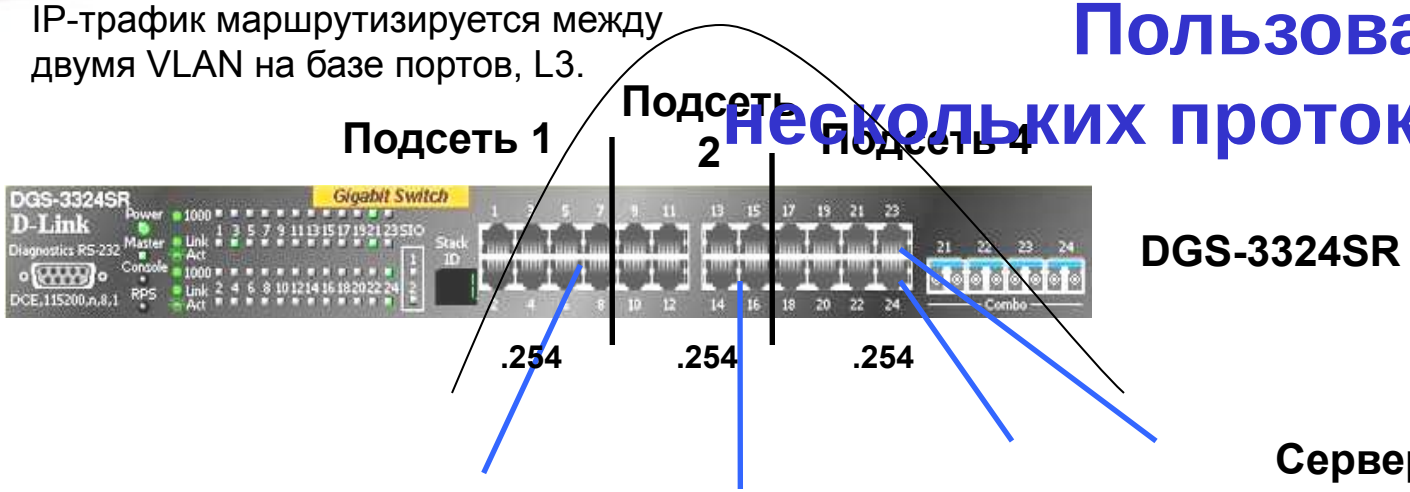
```
create vlan v101 tag 101 type protocol-ipV6
config vlan v101 add untagged 1-8

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
```

На компьютерах пользователей

- **Для пользователей IPv4 подсетей 2 и 4, задать IP-адреса, маску соответствующей IP сети. Шлюз = IP-интерфейс DGS-3324SR.**
- **Пользователи протокола IPv6 в своём VLAN используют конфигурацию IPv6.**

Пример 2 – Пользователи нескольких протоколов

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



DGS-3324SR

Сервер IP,
192.168.4.x/24
Шлюз
192.168.4.254

Сервер/клиент IPX

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

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

Задание:

Пользователи Подсети 1 (порты 1-8) используют два протокола. Пользователь может получить доступ к серверу IP (в Подсети 4) посредством IP-маршрутизации между подсетями (L3) и доступ к серверу IPX (на порту 24) через VLAN на основе протокола IPX (L2).

Пример 2 – Пользователи нескольких протоколов

На DGS-3324SR

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
```

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

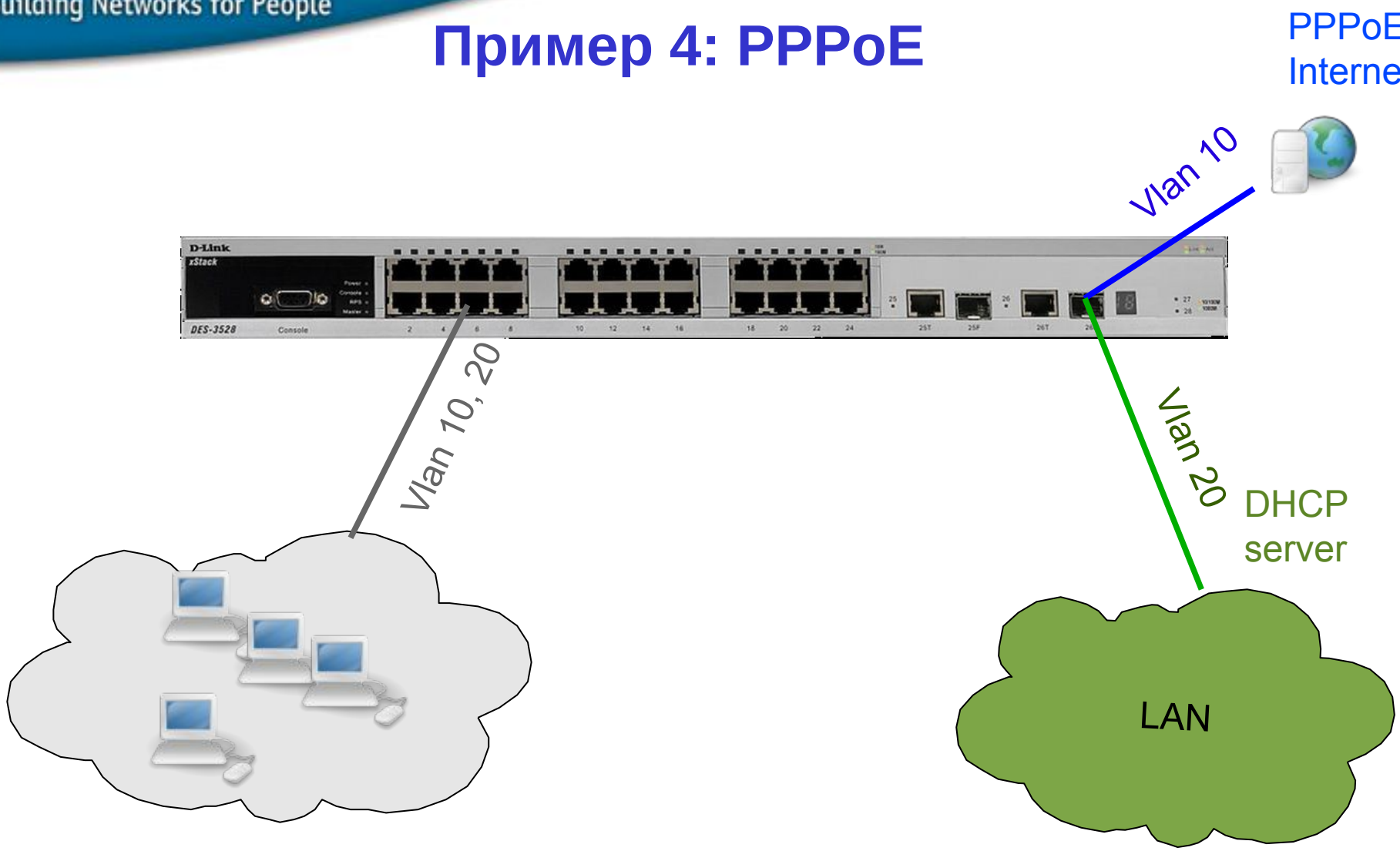
```
create vlan v200 tag 200 type protocol-ipx802dot3
config vlan v200 add untagged 1-8, 24
```

На компьютерах пользователей двух протоколов

1. В ручную задать IP-адрес и маску для соответствующей IP-подсети.
2. Шлюз = IP-интерфейс DGS-3324SR
3. Настройки на сетевой карте, связанные с IPX (разрешить IPX/SPX протокол, режим клиента и т.д.).

D-Link
Building Networks for People

Пример 4: PPPoE



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

D-Link
Building Networks for People

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 20
#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
```

D-Link
Building Networks for People

Приоритеты 802.1p и QoS – качество обслуживания

D-Link
Building Networks for People

Протокол IEEE 802.1P

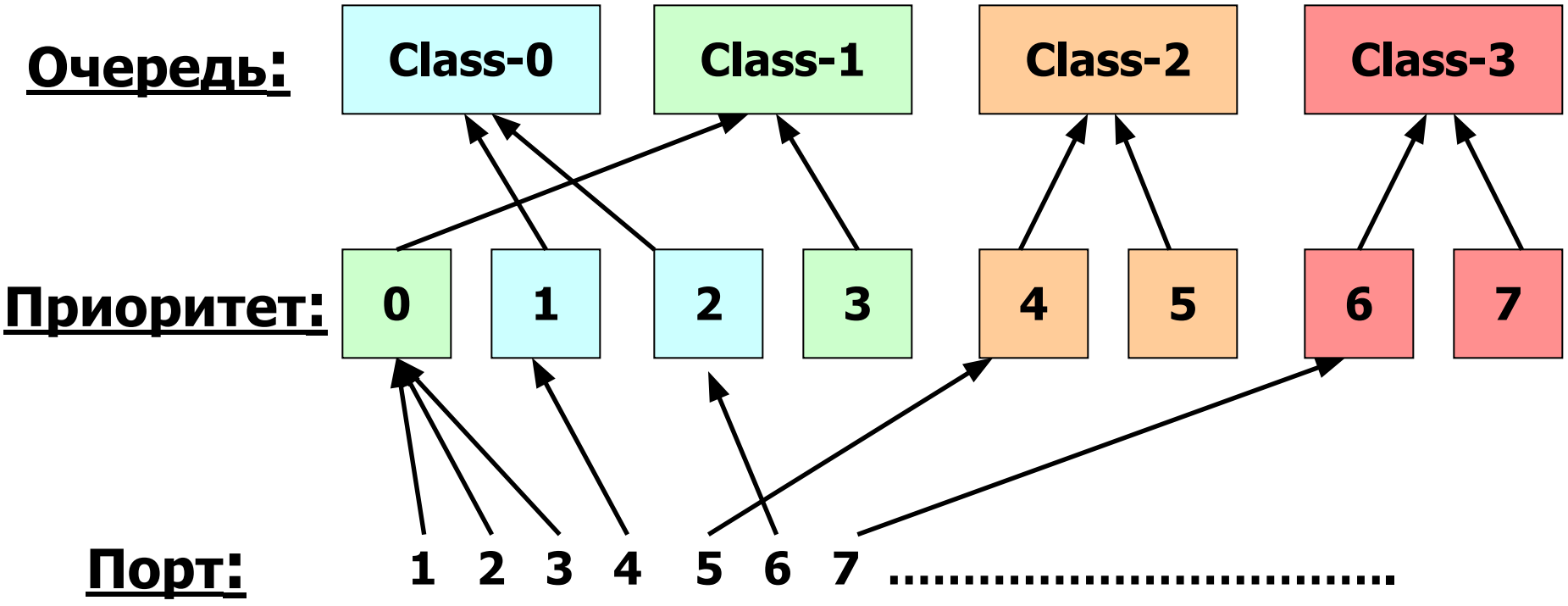
Стандарт IEEE 802.1p определяет приоритет пакета при помощи тэга в его заголовке. Можно задать до 8 уровней приоритета от 0 до 7. Уровень 7 определяет самый высокий приоритет.

Коммутаторы поддерживают 4 очереди Class of Service на каждом порту. Для маркированных пакетов приоритет может быть изменен на одну из четырех очередей CoS. Для немаркированных пакетов приоритет выставляется исходя из приоритета, выставленного на данном порту.

D-Link
Building Networks for People

Как работает 802.1p

4 очереди приоритета



Приоритет по умолчанию 802.1p

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

```
DGS-3324SR:4# show 802.1p default_priority
Command: show 802.1p default_priority
Port  Priority
------- -----------
1:1     0
1:2     0
1:3 0
```

Пример: Поменять приоритет по умолчанию для портов 1-4 на 7:

```
config 802.1p default_priority 1-4  7
```

Пользовательский приоритет 802.1p

Используется для ассоциации пользовательского приоритета 802.1p входящего кадра с одной из аппаратных очередей приоритетов на коммутаторе.

Замечание: 1p = 7 обычно соответствует самой приоритетной очереди, но 1p = 0 не обязательно означает очереди с самым низким приоритетом.

Приоритет кадра внутри коммутатора определяется тем, к какой очереди он приписан, а не приоритетом 1p.

DGS-3324SR:4# show 802.1p user_priority
COS Class of Traffic
Priority-0 -> <Class-2>
Priority-1 -> <Class-0>
Priority-2 -> <Class-1>
Priority-3 -> <Class-3>
Priority-4 -> <Class-4>
Priority-5 -> <Class-5>
Priority-6 -> <Class-6>
Priority-7 -> <Class-6>

DES-3526:4# show 802.1p user_priority
COS Class of Traffic
Priority-0 -> <Class-1>
Priority-1 -> <Class-0>
Priority-2 -> <Class-0>
Priority-3 -> <Class-1>
Priority-4 -> <Class-2>
Priority-5 -> <Class-2>
Priority-6 -> <Class-3>
Priority-7 -> <Class-3>

config 802.1p user_priority <priority 0-7> <class_id 0-6>

D-Link
Building Networks for People

Обработка приоритетов - Строгий режим (Strict Priority)

Обработка приоритетов производится в соответствии с одним из методов, строгий или по весу.

При **строгом** методе, кадры в очередях с высоким приоритетом обрабатываются первыми. Только тогда, когда эти очереди пусты, могут быть обработаны кадры с более низким приоритетом. Кадры с высоким приоритетом всегда получают предпочтение независимо от количества кадров в других очередях в буфере и времени, прошедшего с момента передачи последнего кадра с низким приоритетом. По умолчанию коммутатор настроен как раз на этот режим.

Проблема: Пакеты в очередях с низким приоритетом могут долго не обрабатываться.

Обработка приоритетов – Взвешенный круговой режим (Weighted Round-Robin)

Для использования обработки приоритетов по весу, восемь очередей приоритета в коммутаторе могут быть сконфигурированы в взвешенном круговом режиме (***WRR***) так, чтобы кадры в буфере надолго не задерживались – обработка начинается с очереди с наивысшим приоритетом, потом переходит к более низкому и т.д., а в конце возвращается к наивысшему приоритету, и всё повторяется опять.

Такой режим исключает главный недостаток строгого режима. Очередь с минимальным приоритетом уже не страдают от переполнения, поскольку всем очередям предоставляется часть пропускной способности для передачи. Это достигается заданием максимального числа кадров, которые можно передать из данной очереди приоритетов, перед тем как перейти к следующей. Это устанавливает класс обслуживания (Class of Service (CoS)) для каждой из 8-ми очередей коммутатора.

Команда **config scheduling** может быть использована для настройки взвешенного кругового режима (***WRR***), который сокращает все 8 очередей приоритетов на коммутаторе. Для использования этой схемы, параметры *max_packets* не должны иметь значение *0*. Параметр **max_packet** задаёт максимальное количество кадров в определённой очереди, которое может быть передано за один раз (цикл). Это обеспечивает поддержку CoS, между тем даёт возможность передавать кадры из всех очередей. Это значение можно изменять в диапазоне от 0 до 15 кадров для каждой очереди приоритетов.

config scheduling <class_id 0-6> {max_packet <value 0-15>}

D-Link
Building Networks for People

802.1p Пример 1/2

Задача:

На компьютерах B и D запущены приложения VoIP, и им необходимо более высокое качество обслуживания (QoS) чем другим станциям с обычными приложениями.

Как: Посредством настройки портов, к которым подсоединены компьютеры с VoIP приложениями на приоритет 1p = 7 с умолчальными соответствиями 1p очередям приоритета и режимом обработки приоритетов, входящий кадр VoIP будет соответствовать классу обслуживания 3 и будет иметь более высокий приоритет, чем остальные кадры с других портов (1p = 0, класс 1) на обоих Des3526_1 и Des3526_2.

802.1p Пример 2/2

Конфигурация DES-3526_A

1. Перевести порт, соединяющий Des-3526_1 и 2 из “untagged” в “tagged” так, чтобы приоритеты 1p смогли быть переданы между коммутаторами.

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

1. Поменять приоритет по умолчанию порта 23, к которому подключёно устройство VoIP, с 0 на 7.

```
config 802.1p default_priority ports 23 7
```

1. Пользовательский приоритет и метод обработки остаются по умолчанию.

Конфигурация DES-3526_B

1. Перевести порт, соединяющий Des-3526_1 и 2 из “untagged” в “tagged” так, чтобы приоритеты 1p смогли быть переданы между коммутаторам.

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

1. Поменять приоритет по умолчанию порта 24, к которому подключёно устройство VoIP, с 0 на 7.

config 802.1p default_priority ports 24 7

- Пользовательский приоритет и метод обработки остаются по умолчанию

Сегментация трафика

D-Link
Building Networks for People

Сегментация трафика

Сегментация трафика служит для разграничения доменов на уровне 2.
Данная функция позволяет настраивать порты таким образом, чтобы они были изолированы друг от друга, но в то же время имели доступ к разделяемым портам, используемым для подключения сервером и магистрали сети провайдера. Данная функция может быть использована при построении сетей провайдеров.

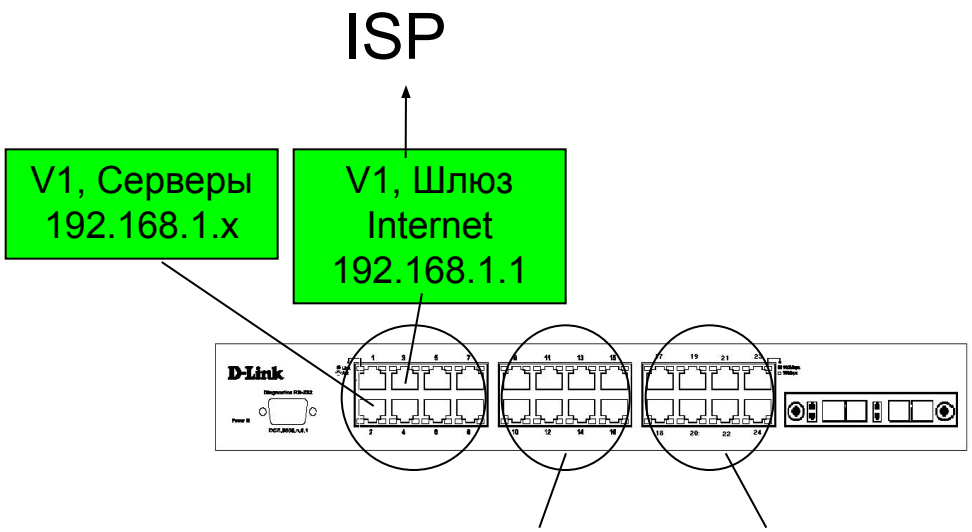
Сегментация трафика

Все компьютеры (ПК 1 – ПК 23) имеют доступ к порту uplink, но не имеют доступа друг к друг на уровне 2

Решение можно использовать для:

- в проектах ETTH для изоляции портов
- для предоставления доступа к общему серверу

Сегментация трафика



V1: порты 1-8
Общий(ие) сервер(ы)

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

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

Задание и требования:

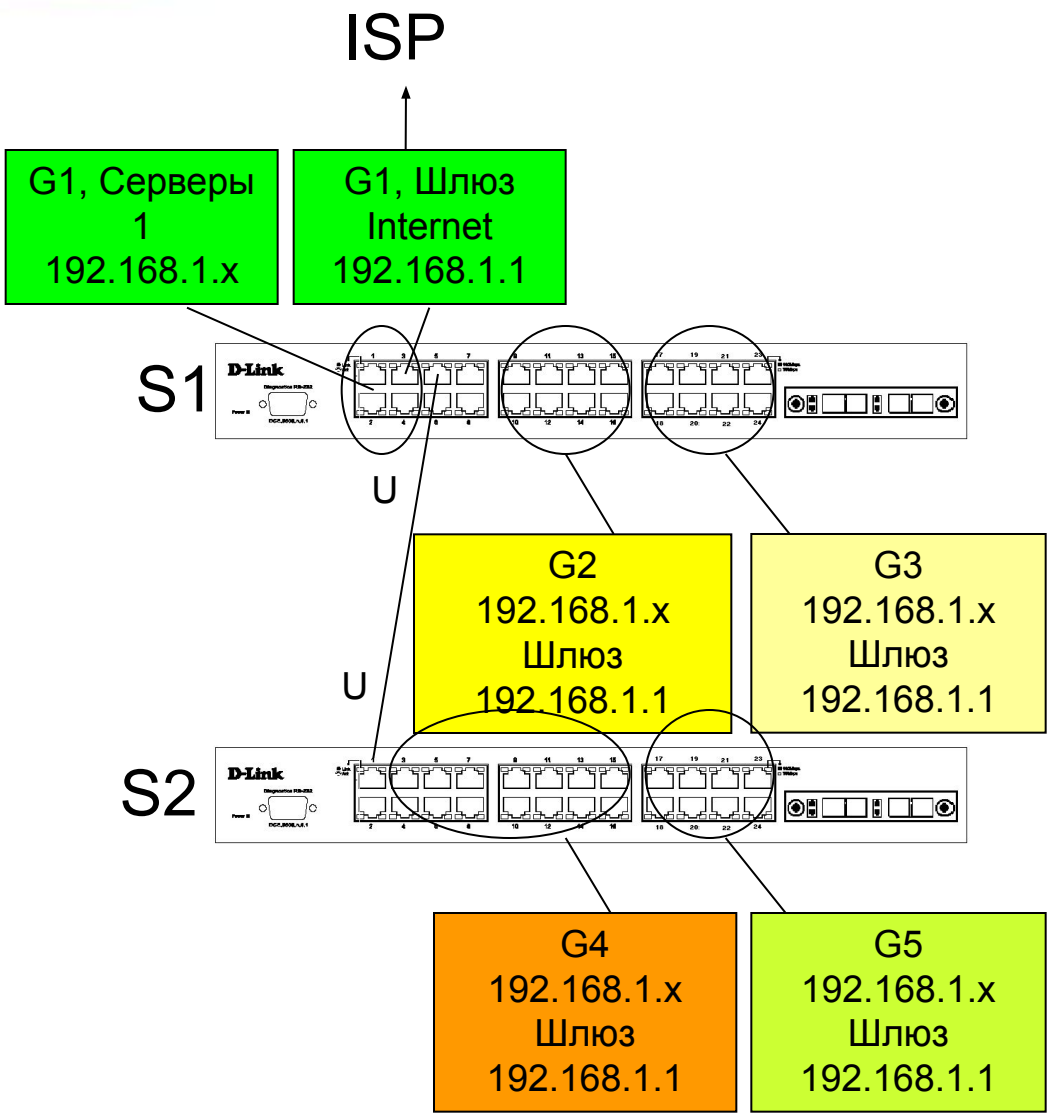
1. V2 и V3 имеют доступ к серверам V1 (IPX, IP той же подсети, AppleTalk, NetBEUI и т.д.)
2. V2 и V3 имеют возможность обращения к шлюзу Internet для доступа к ресурсам Internet с использованием IP-адресов той же подсети.
3. Не должно быть доступа между V2 и V3.

D-Link
Building Networks for People

Конфигурация DES-3526

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

Пример: Сегментация трафика с двухуровневой иерархией



S1 порты 1-4: G1, нетегированные
Общий(ие) сервер(ы) и шлюз Internet
S1 порты 5-8, S2 порты 1-2 , нетегированные
для связи с другими коммутаторами
S1 порты 9-16: G2, нетегированные
Пользователи группы G2 (PC или концентратор/коммутатор)
S1 порты 17-24: G3, нетегированные
Пользователи группы 3 (PC или концентратор/коммутатор)
S2 порт 1: uplink порт
S2 порты 3-16: G4, нетегированные
Пользователи группы 4 (PC или концентратор/коммутатор)
S2 порты 17-24: G5, нетегированные
Пользователи группы 5 (PC или концентратор/коммутатор)

Задачи и требования:

1. Все группы (G2 - G5) имеют доступ к общим серверам shared (IPX, IP, AppleTalk и т.д.) или к шлюзу Internet в G1.

. Не должно быть доступа между G2, G3, G4, G5.

D-Link
Building Networks for People

Конфигурация S1 (Центральный коммутатор)

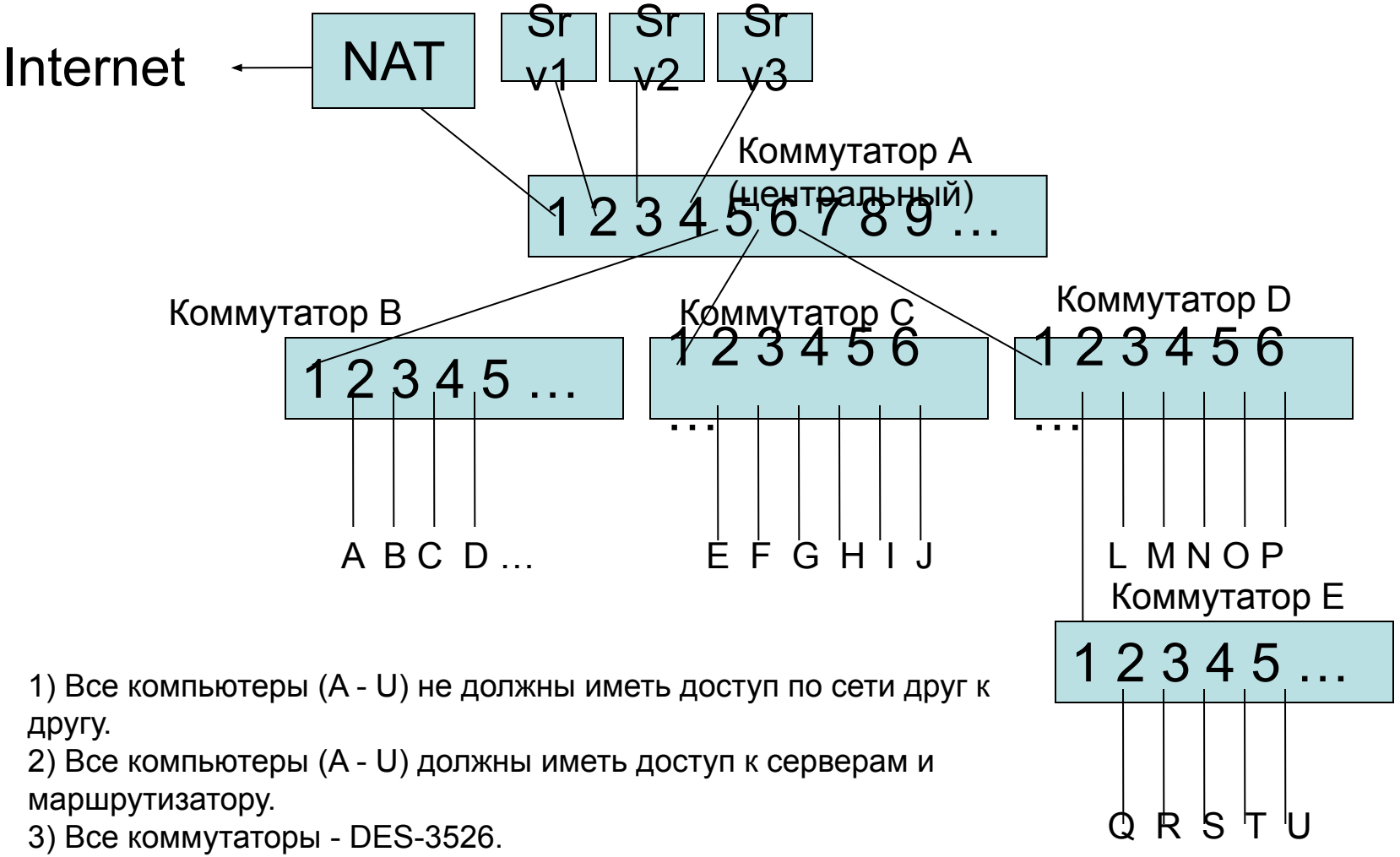
```
config traffic_segmentation 1-4 forwarding_list 1-24
config traffic_segmentation  5 forwarding_list 1-5
config traffic_segmentation  9-16 forwarding_list 1-4, 9-16
config traffic_segmentation  17-24 forwarding_list 1-4, 17-24
```

Конфигурация S2 (Оконечный коммутатор)

```
config traffic_segmentation 1 forwarding_list 1-24
config traffic_segmentation  2-16 forwarding_list 1-16
config traffic_segmentation 17-24 forwarding_list 1,17-24
```

D-Link
Building Networks for People

Иерархическая сегментация трафика для изоляции портов



1) Все компьютеры (A - U) не должны иметь доступ по сети друг к другу.
2) Все компьютеры (A - U) должны иметь доступ к серверам и маршрутизатору.
3) Все коммутаторы - DES-3526.
4) В сети используются IP-адреса из одной подсети (компьютеры, серверы и внутренний интерфейс маршрутизатора).

D-Link
Building Networks for People

Конфигурация

Коммутатор A (центральный)

```
config traffic_segmentation 1-4 forwarding_list 1-26
config traffic_segmentation  5 forwarding_list 1-5
config traffic_segmentation  6 forwarding_list 1-4,6
config traffic_segmentation  7 forwarding_list 1-4,7
```

(повторить для всех портов связи с нижестоящими коммутаторами)

Коммутаторы B, C, D, E,… (другие)

```
config traffic_segmentation 1 forwarding_list 1-26
config traffic_segmentation 2-24 forwarding_list 1
```

D-Link
Building Networks for People

Ассиметричные VLAN по сравнению с сегментацией трафика

Ассиметричные VLAN

- Необходимо глубокое понимание 802.1q VLAN
- Пользователи VLAN могут быть распределены между несколькими устройствами, и сервер может находиться в любом месте.
- Нужна поддержка расширения стандарта 802.1q (перекрывающиеся нетегированные VLAN)
- Может не поддерживать IGMP snooping
- Максимальное количество VLAN ограничено 4094.

Сегментация трафика

- Просто, не нужно знание технологии VLAN.
- Пользователи VLAN не могут быть распределены между устройствами.
- Работает IGMP snooping.
- Сегментация трафика может иметь иерархичную структуру. Нет ограничений на номер VLAN.
- Общие серверы должны быть подключены к центральному коммутатору (при использовании иерархичной структуры)

Протоколы «покрывающего дерева»
Spanning Tree Protocols

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

D-Link
Building Networks for People

Протокол Spanning Tree

Зачем нужен протокол Spanning Tree?

- Исключение петель
- Резервные связи

Версии:

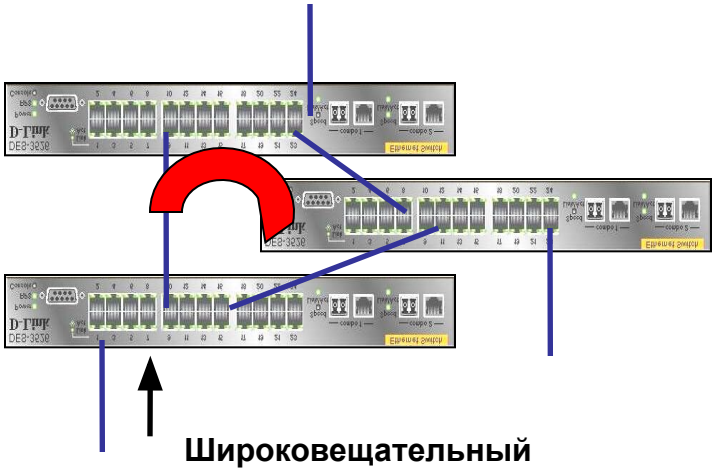
- IEEE 802.1d Spanning Tree Protocol, STP
- IEEE 802.1w Rapid Spanning Tree Protocol, RSTP
- IEEE 802.1s Multiple Spanning Tree Protocol, MSTP

D-Link
Building Networks for People

Что такое сетевая петля L2

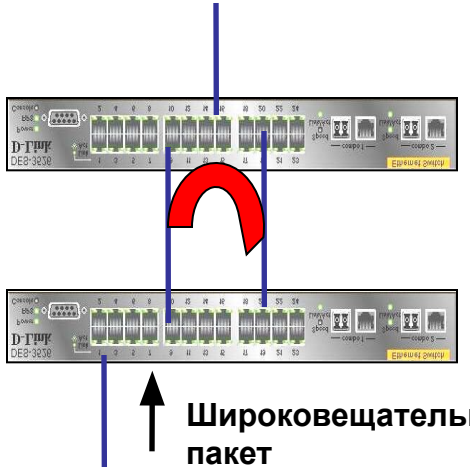
Коммутаторы (L2), объединённые в кольцо, образуют одну или несколько сетевых петель

Пример 1



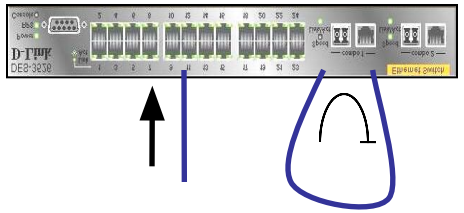
Широковещательный пакет

Пример 2



Широковещательный пакет

Пример 3



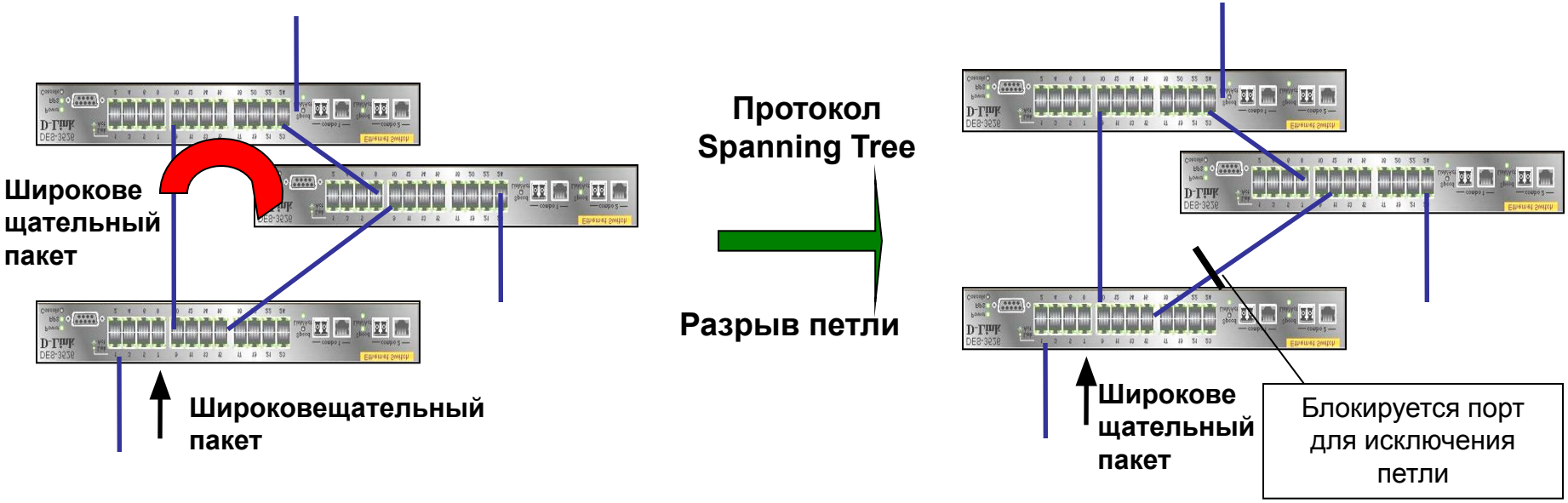
Широковещательный пакет

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).

D-Link
Building Networks for People

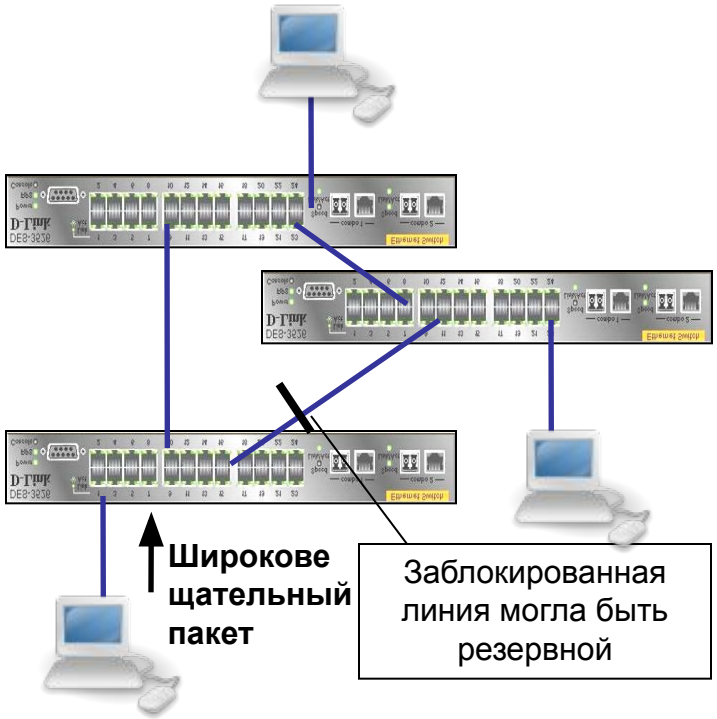
Исключение петель



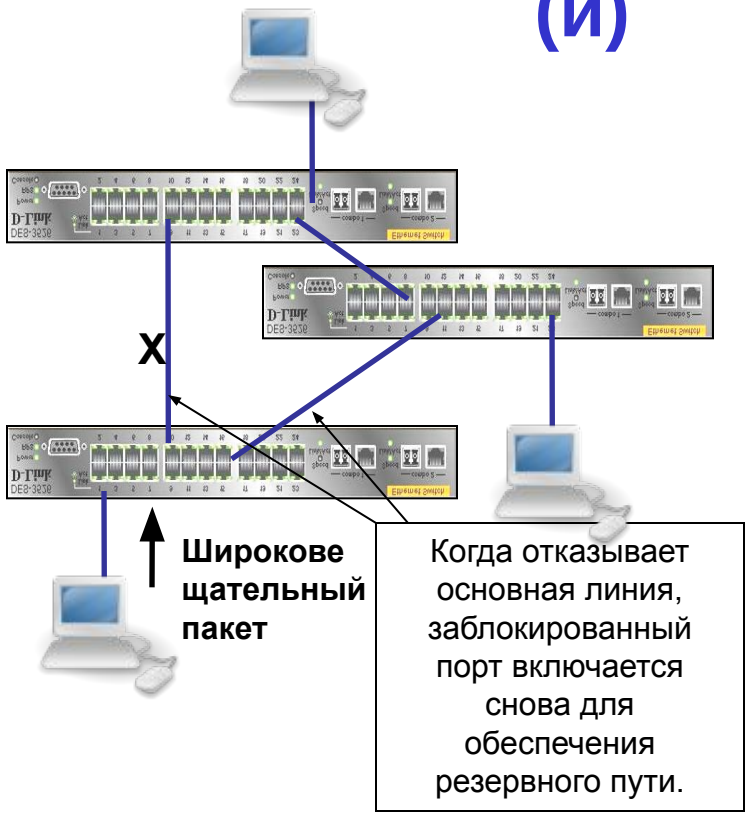
Решение: Протокол Spanning Tree (STP, RSTP, MSTP) может исключить петлю или петли.

D-Link
Building Networks for People

Резервная(ие) связь (и)



Протокол Spanning Tree



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

D-Link
Building Networks for People

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.

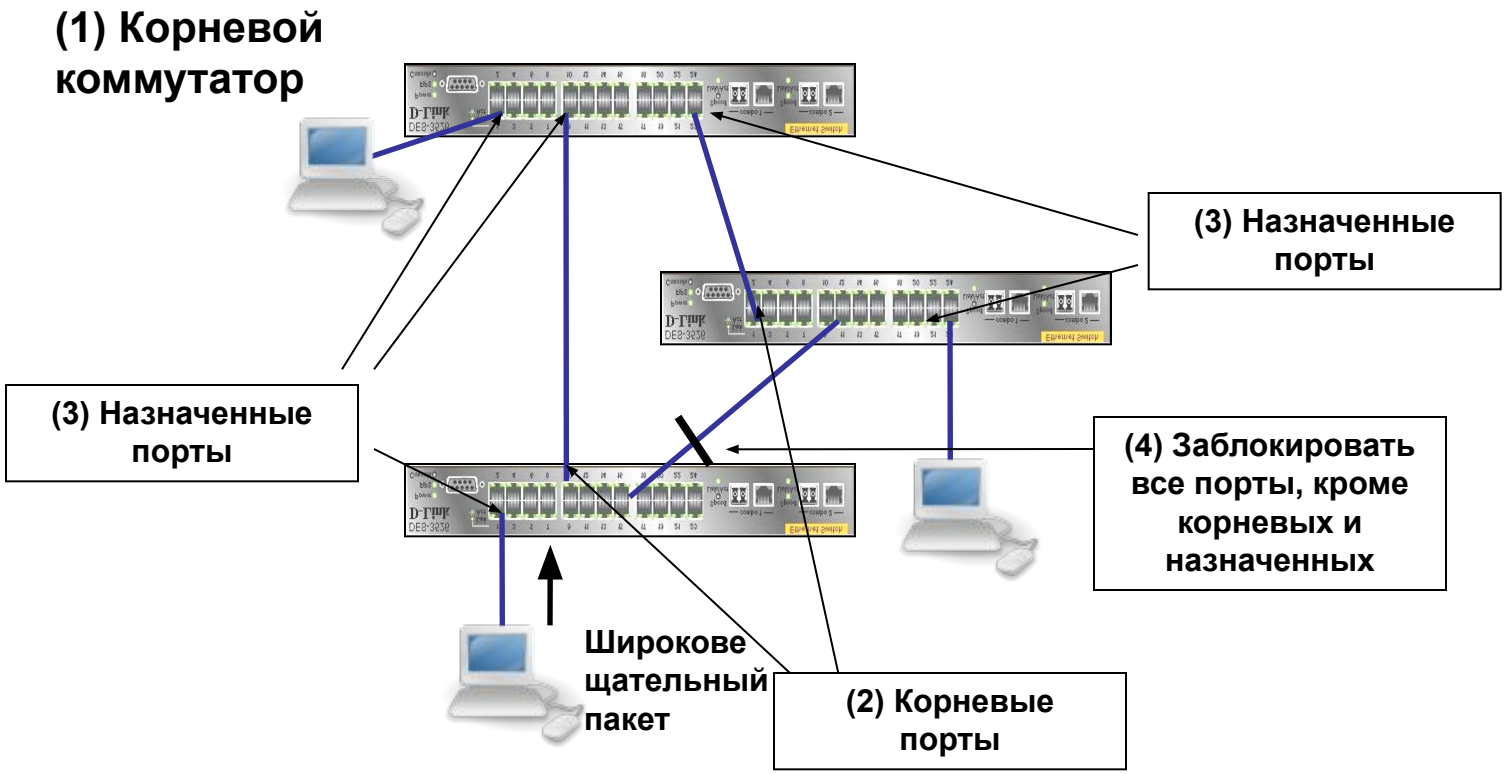
Пакеты BPDU содержат информацию для построения топологии сети без петель

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

D-Link
Building Networks for People

Как работает STP



D-Link
Building Networks for People

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.

D-Link
Building Networks for People

Протокол Rapid Spanning Tree, RSTP

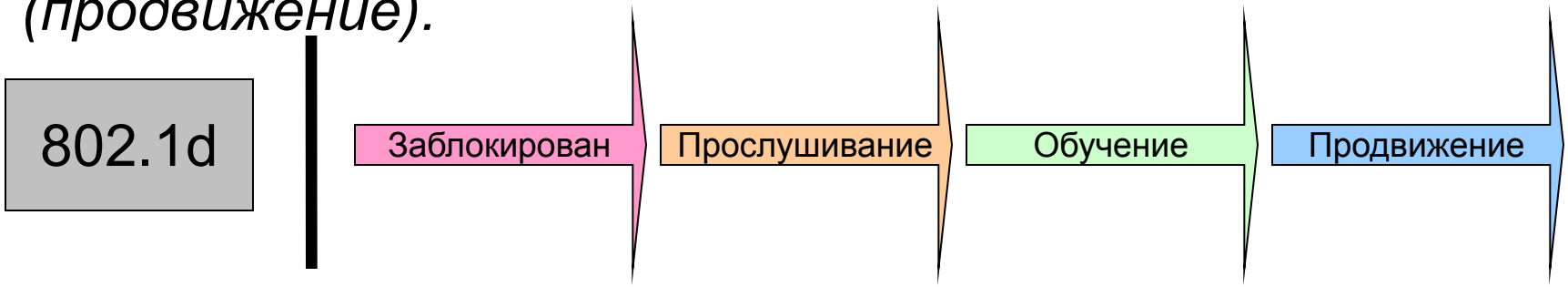
- Стандартизирован IEEE 802.1w

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

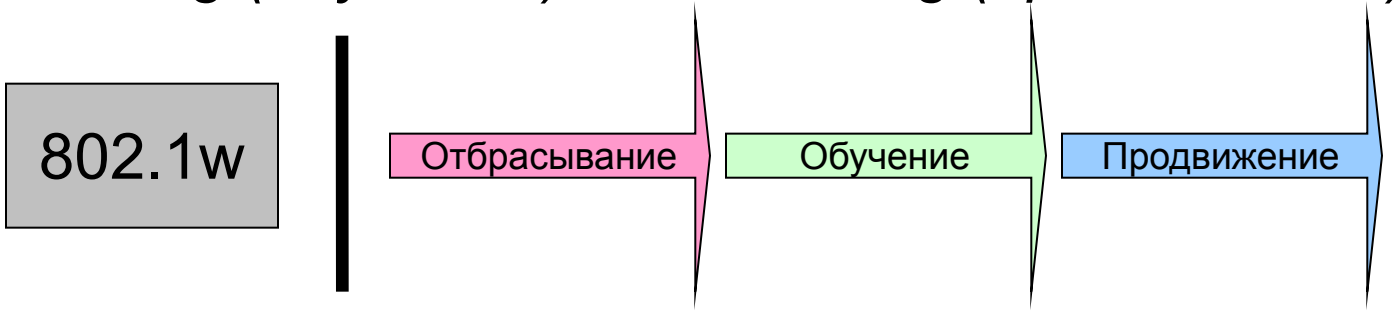
D-Link
Building Networks for People

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).*



D-Link
Building Networks for People

Соответствие состояния портов ме
802.1d и 802

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

D-Link
Building Networks for People

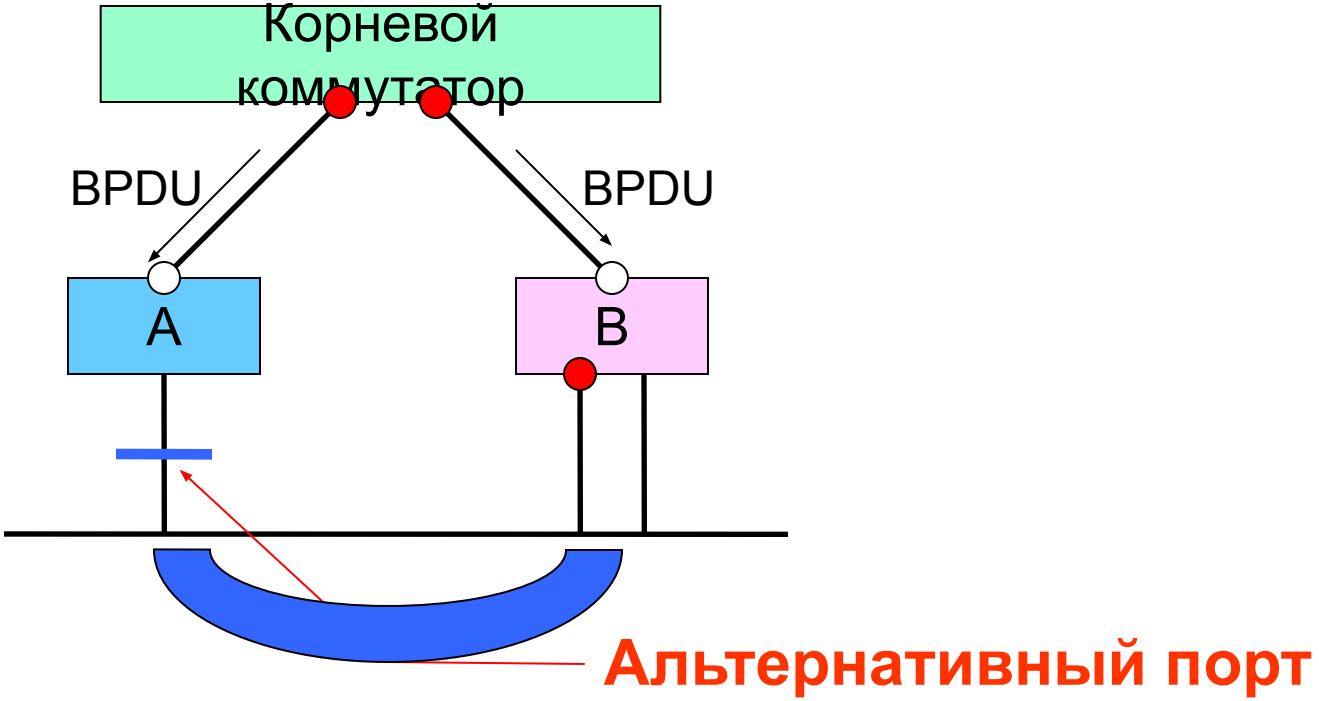
Роли портов

- 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

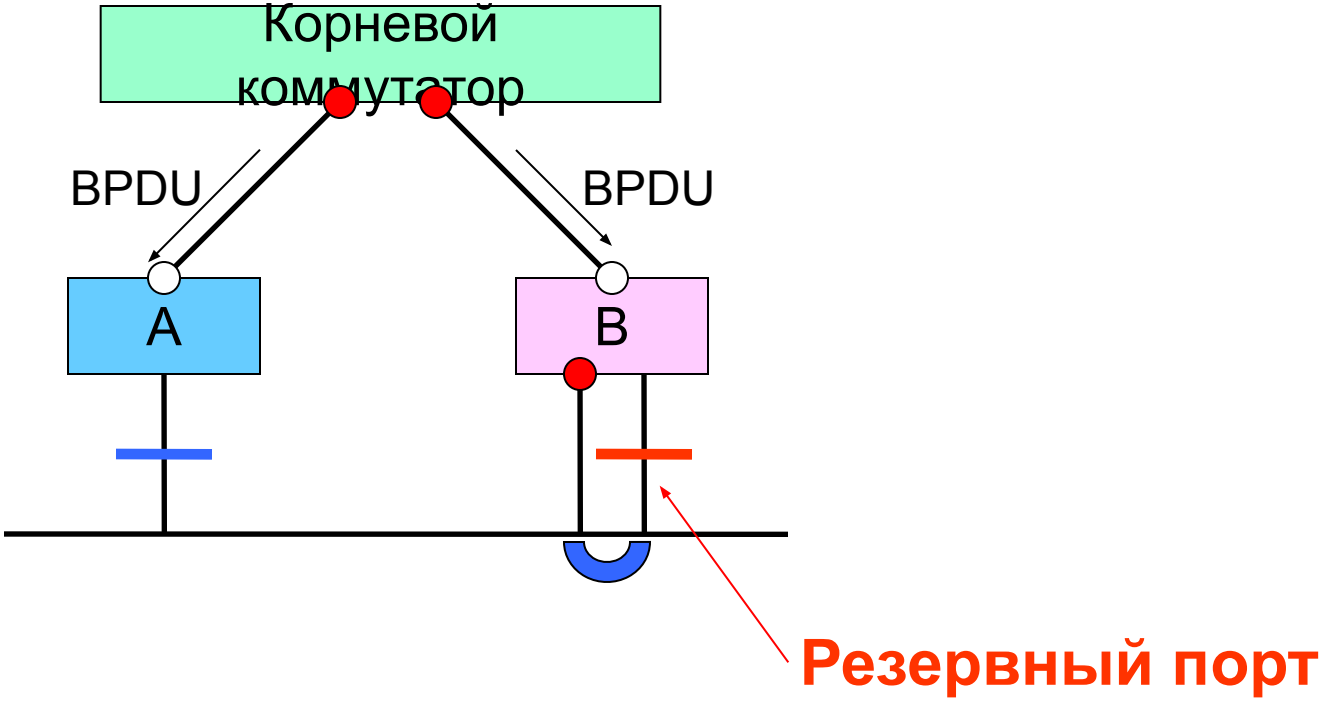
  Альтернативный порт – это порт заблокированный в результате получения более предпочтительных BPDU от другого коммутатора.



Роли портов

- Роли резервных портов

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



D-Link
Building Networks for People

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
  - При отказе корневого порта, RSTP-коммутатор может практически сразу переключить альтернативный порт в корневой порт
  - При выходе из строя назначенного порта, резервный порт может быть также быстро переведён в назначенный

D-Link
Building Networks for People

Быстрый перевод портов в состояние продвижения

Новый протокол RSTP позволяет перевести порт в состояние продвижения кадров без учёта каких-либо таймеров. Таким образом появился реальный механизм обратной связи для совместимых с протоколом RSTP устройств. Для обеспечения быстрой сходимости сети, протокол оперирует двумя понятиями – пограничные порты и тип линии.

1. Пограничные порты

- **Все порты, к которым напрямую подсоединены рабочие станции не могу создать петель в сети и, соответственно, могут быть переведены в состояние продвижения практически сразу без перехода в состояния прослушивания и обучения.**

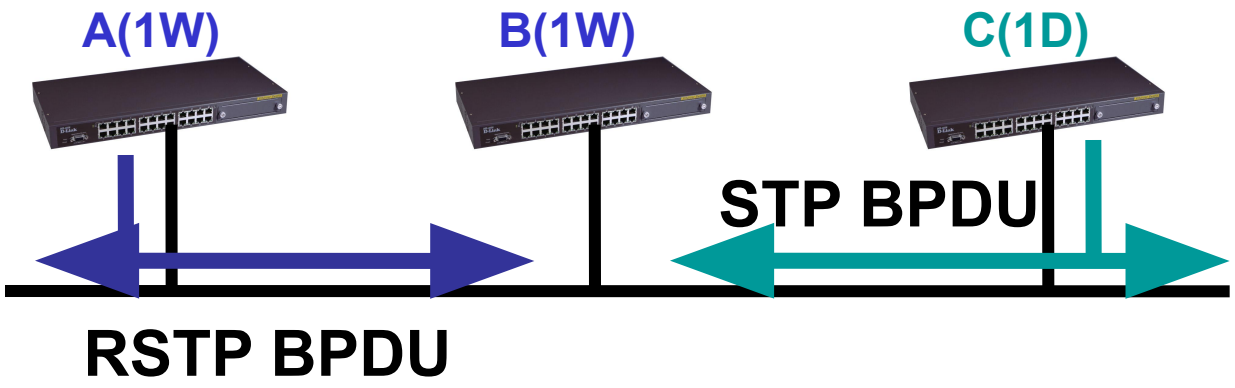
1. Тип линии (точка-точка или разделяемая)

- **Порт функционирующий в режиме полного дуплекса рассматривается как соединение точка-точка.**
- **Порт в режиме полудуплекса воспринимается, по умолчанию, как разделяемое соединение.**
- **Быстрая сходимость сети достигается на соединениях точка-точка.**

D-Link
Building Networks for People

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.



D-Link
Building Networks for People

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.

STP BPDU

D-Link
Building Networks for People

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 (максимальное 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.

D-Link
Building Networks for People

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.

D-Link
Building Networks for People

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.

D-Link
Building Networks for People

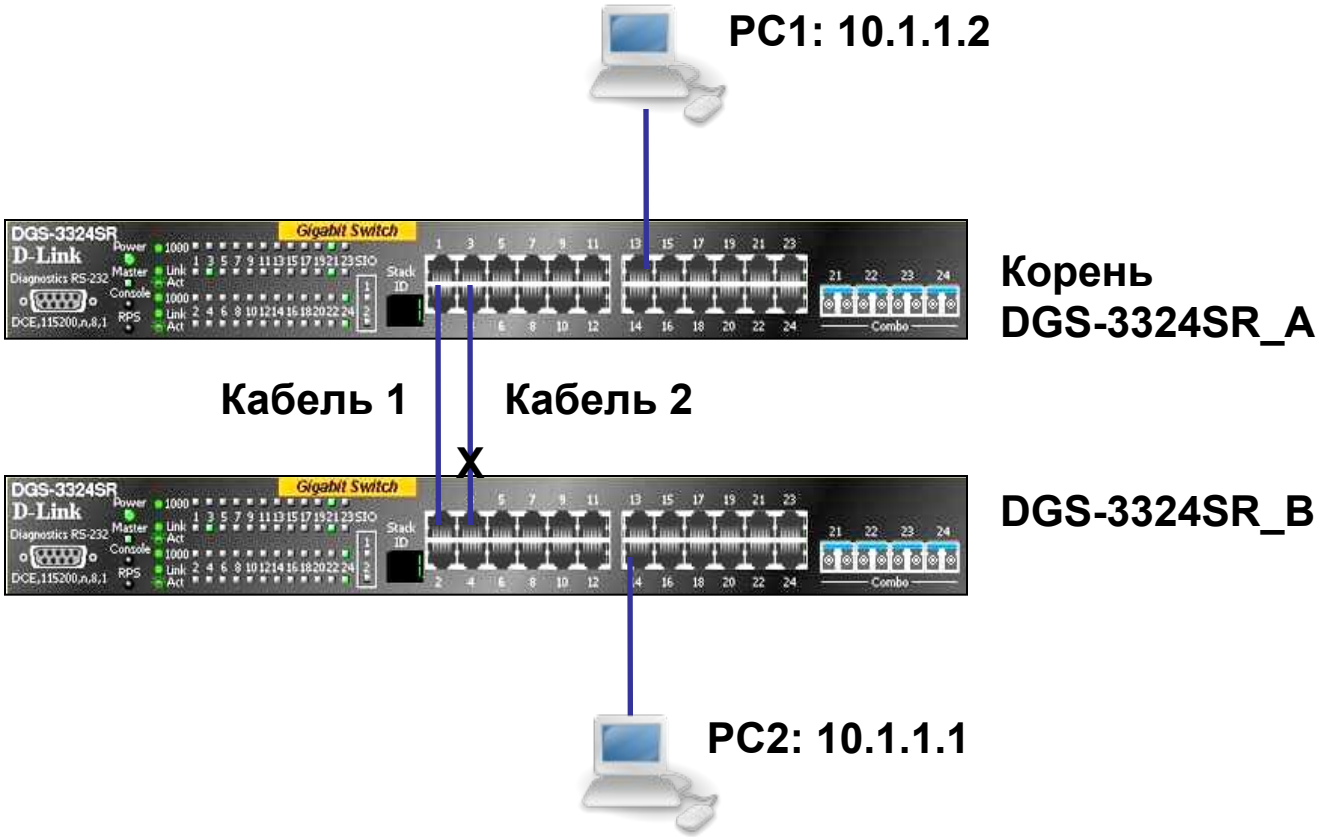
Пример RSTP

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?

D-Link
Building Networks for People

Пример RSTP



Включить STP на обоих коммутаторах DGS-3324SR. Проверить заблокирован ли один порт DGS-3324R.
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-3324SR_A:

```
config ipif System ipaddress 10.1.1.10/8
enable stp
config stp version rstp
```

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

```
config stp priority 4096 instance_id 1
config stp ports 1:5-1:24 edge true
```

DGS-3324SR_B:

```
config ipif System ipaddress 10.1.1.11/8
enable stp
config stp version rstp
config stp ports 1:5-1:24 edge true
```

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.

D-Link
Building Networks for People

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 копия 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)

D-Link
Building Networks for People

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.

D-Link
Building Networks for People

Регионы MSTP

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

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

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

1. Конфигурационное имя
2. Конфигурационный номер ревизии
3. Карту привязки VLAN к копиям STP

D-Link
Building Networks for People

Пример работы MSTP

Сеть состоит из 3 коммутаторов, соединенных между собой.

В сети настроены 2 VLAN с VID 10 и 20.
На коммутаторе 1 VLAN 10 и 20 настроены на разных портах таким образом, что трафик для обоих VLAN 10 и 20 передается по разным соединениям.

На первый взгляд, такая конфигурация достаточно обычна и хорошо подходит для балансировки нагрузки при передаче трафика двух различных VLAN. Однако в сети настроен протокол STP.

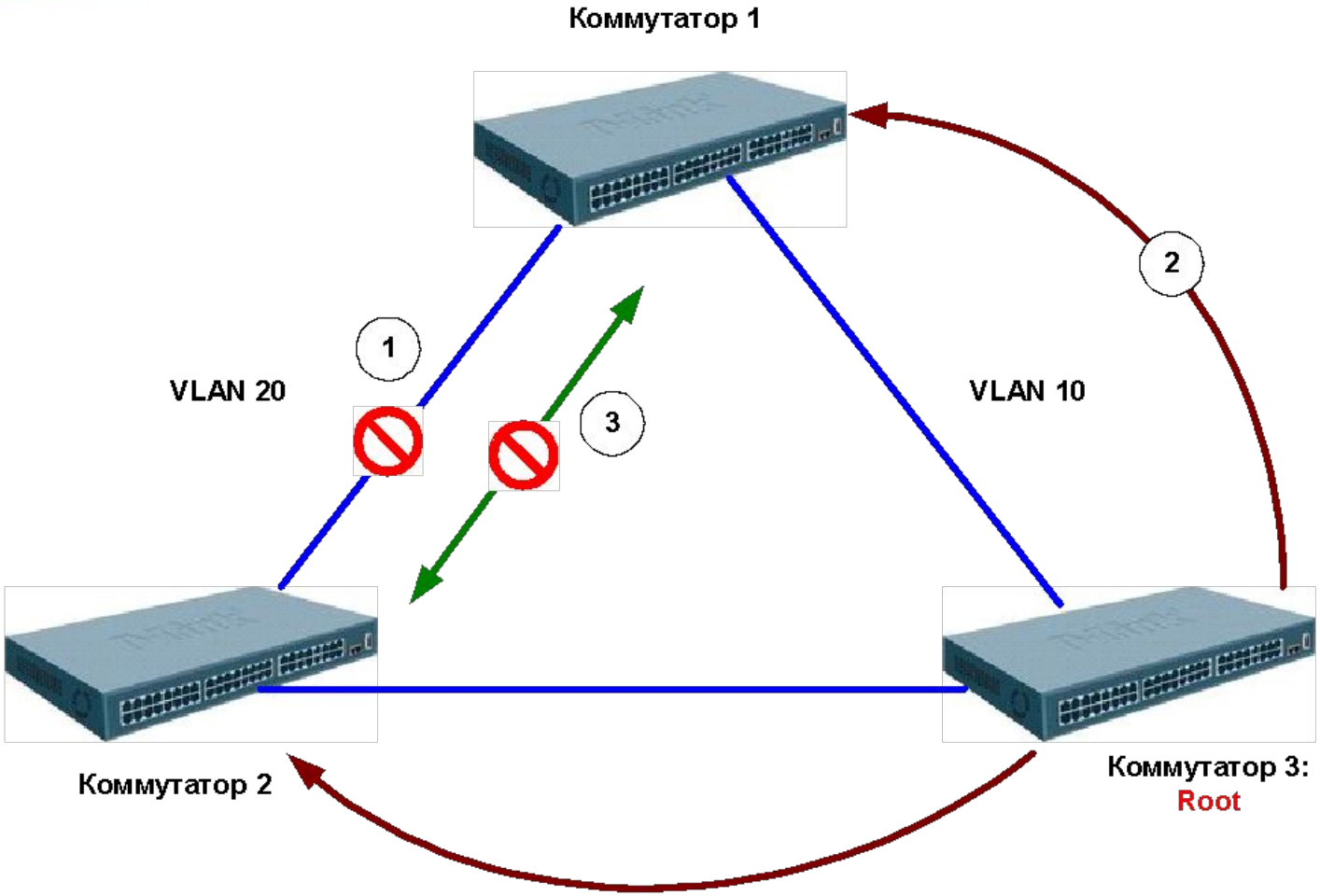
Если коммутатор 3 будет выбран корневым коммутатором для STP, то соединение между коммутаторами 1 и 2 будет заблокировано.

В этом случае трафик из VLAN 20 не сможет передаваться по сети.

Эта проблема возникает потому, что коммутаторы рассматривают VLAN 10 и 20 как независимые сети, в то время как протокол STP рассматривает топологию сети как одну целую сеть.

D-Link
Building Networks for People

Пример работы MSTP



1. В результате работы STP коммутатор 3 выбран корневым, соединение между коммутаторам и 1 и 2 было заблокировано

2. Трафик из VLAN 10 передается между коммутаторами 1 и 3

3. Трафик из VLAN 20 не может быть передан между коммута торами 1 и 2

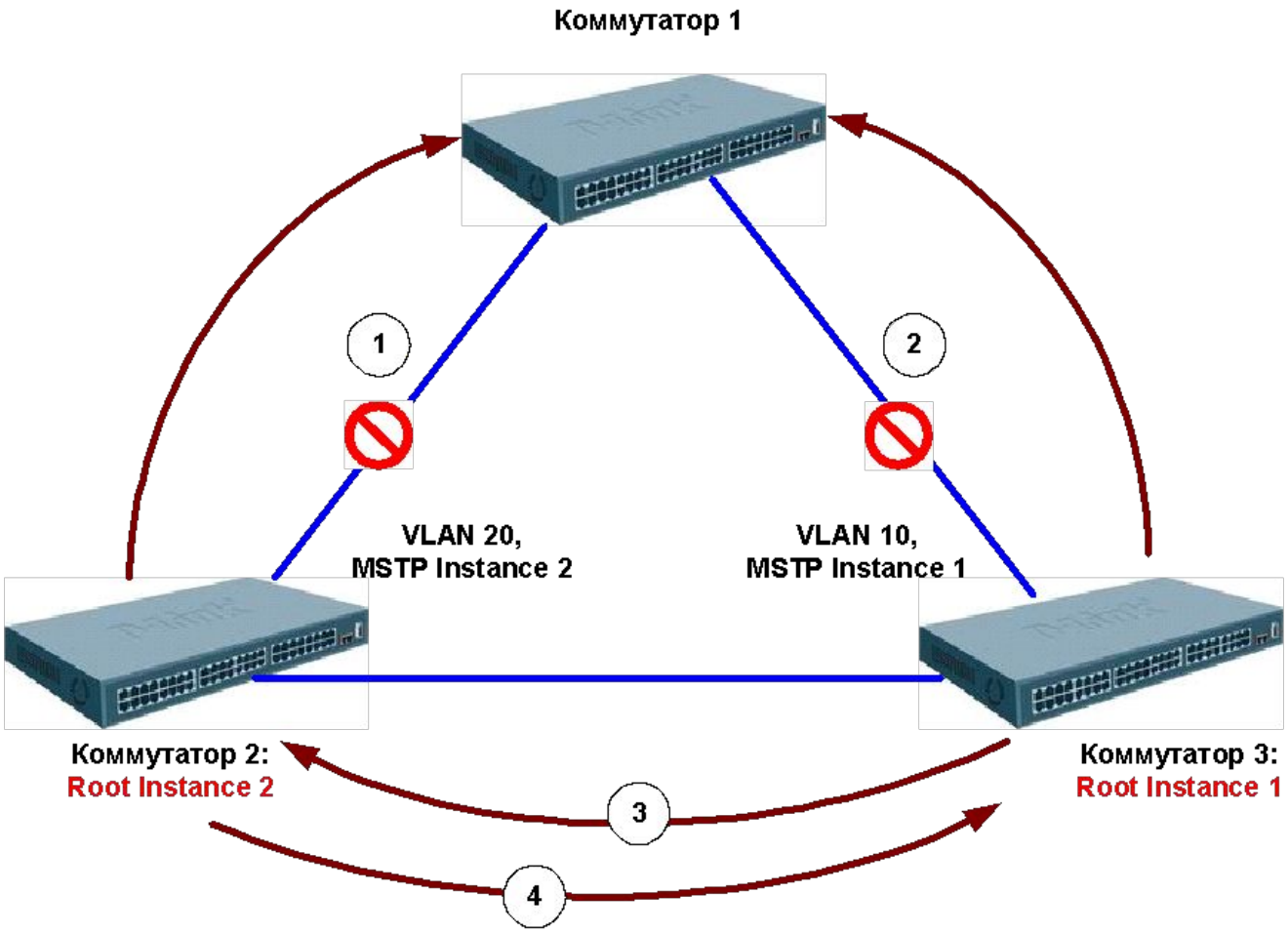
D-Link
Building Networks for People

Пример работы MSTP

- 802.1S решает поставленную задачу:
- Если назначить VLAN 10 на копию MSTP под номером 1, а VLAN 20 сопоставить с копией 2.
- Т.о. получится две независимых топологии дерева STP.
- Коммутатор 3 становится корневым для копии MSTP номер 2 и блокирует прохождение трафика между коммутаторами 1 и 2.
- В отличие от протокола 802.1D STP, это соединение блокируется только для прохождения трафика из VLAN 10.
- Трафик из VLAN 20 будет передаваться по этому соединению.
- Аналогичным образом, копия MSTP под номером 2 выберет коммутатор 2 в качестве корневого и заблокирует соединение между коммутаторами 1 и 3 для трафика из VLAN 20.
- Таким образом, достигается требуемая работа сети: осуществляется баланс нагрузки при передаче трафика нескольких VLAN по разным соединениям и в то же время в сети отсутствуют логические «петли».

D-Link
Building Networks for People

Пример работы MSTP



1. В копии MSTP номер 1 коммутатор 3 выбран корневым, соединение между коммутаторам и 1 и 2 для VLAN 10 было заблокировано
2. В копии MSTP номер 2 коммутатор 2 выбран корневым, соединение между коммутаторам и 1 и 3 для VLAN 20 было заблокировано
3. Трафик из VLAN 10 передается между коммутаторами 1 и 3
4. Трафик из VLAN 20 передается между коммутаторами 1 и 2

D-Link
Building Networks for People

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 1: На каждый VLAN одна копия STP

Задача:

Каждый VLAN образует своё покрывающее дерево. В каждой паре только одна активная линия для каждого VLAN.

Если любая активная линия отказывает, вторая становится активной.

D-Link
Building Networks for People

MSTP Пример 1: На каждый VLAN одна копия STP

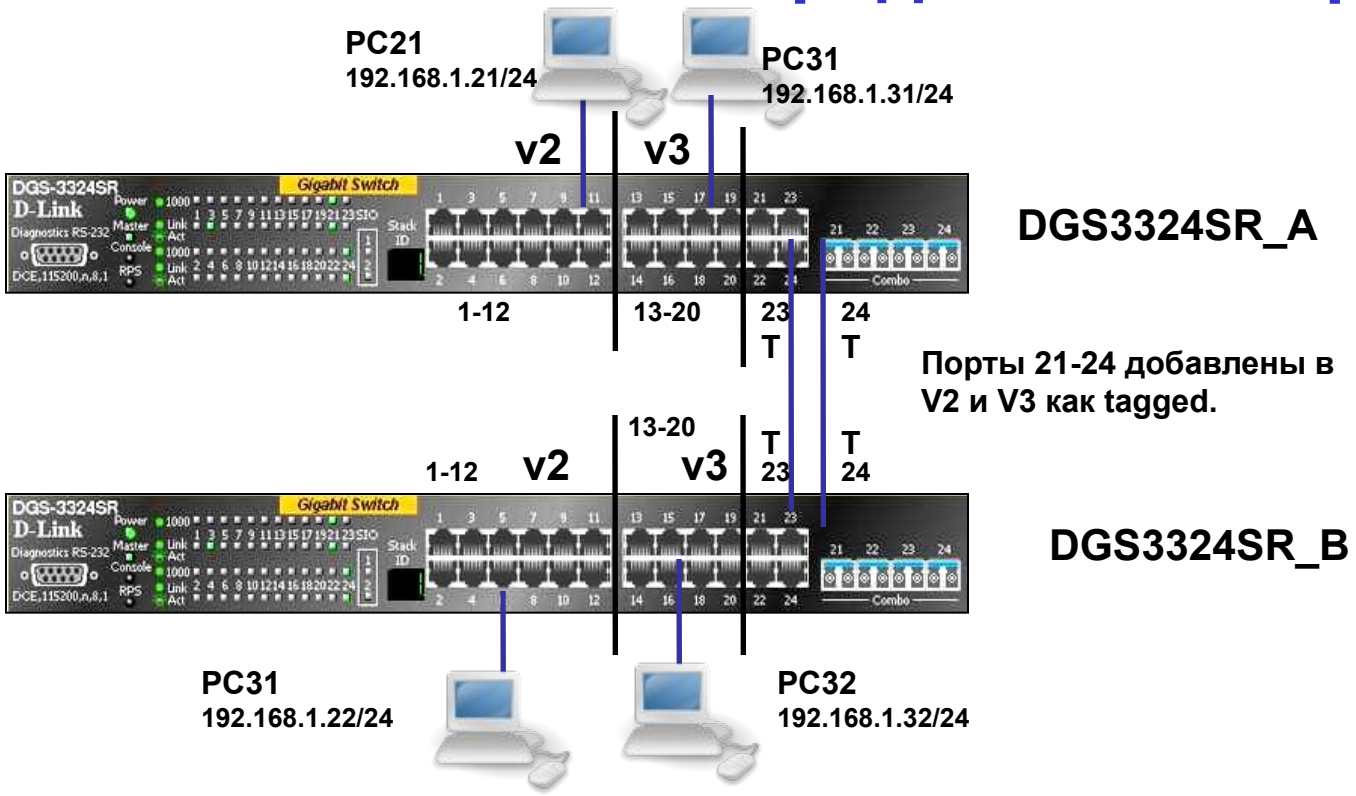
Конфигурация DES3324SR_A

```
config vlan default delete 1-20

create vlan v2 tag 2
config vlan v2 add untagged 1-12
create vlan v3 tag 3
config vlan v3 add untagged 13-20

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.
# Приоритет задаётся по правилу 4096*n, по умолчанию = 32768
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 1 стал активным
## для v2, и порт 13 - для v3.
## приоритет = 16*n, по умолчанию = 128
config stp mst_ports 1 instance_id 2 priority 96
config stp mst_ports 13 instance_id 3 priority 96
config stp ports 3-12 edge true
config stp ports 15-20 edge true
```

Конфигурация DES3324SR_B

```
config vlan default delete 1-20

create vlan v2 tag 2
config vlan v2 add untagged 1-12
create vlan v3 tag 3
config vlan v3 add untagged 13-20

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 3-12 edge true
config stp ports 15-20 edge true
```

MSTP Пример 2: Распределение нагрузки



Задача: Распределение нагрузки.

В V2 и V3 запущены отдельные копии RSTP. Активная линия для V2 - порт 23, а для V3 – 24 с распределением нагрузки. Если одна из линий выходит из строя, V2 и V3 используют оставшуюся в целях обеспечения отказоустойчивости.

D-Link
Building Networks for People

MSTP Пример 2: Распределение нагрузки

Конфигурация DGS3324SR_A

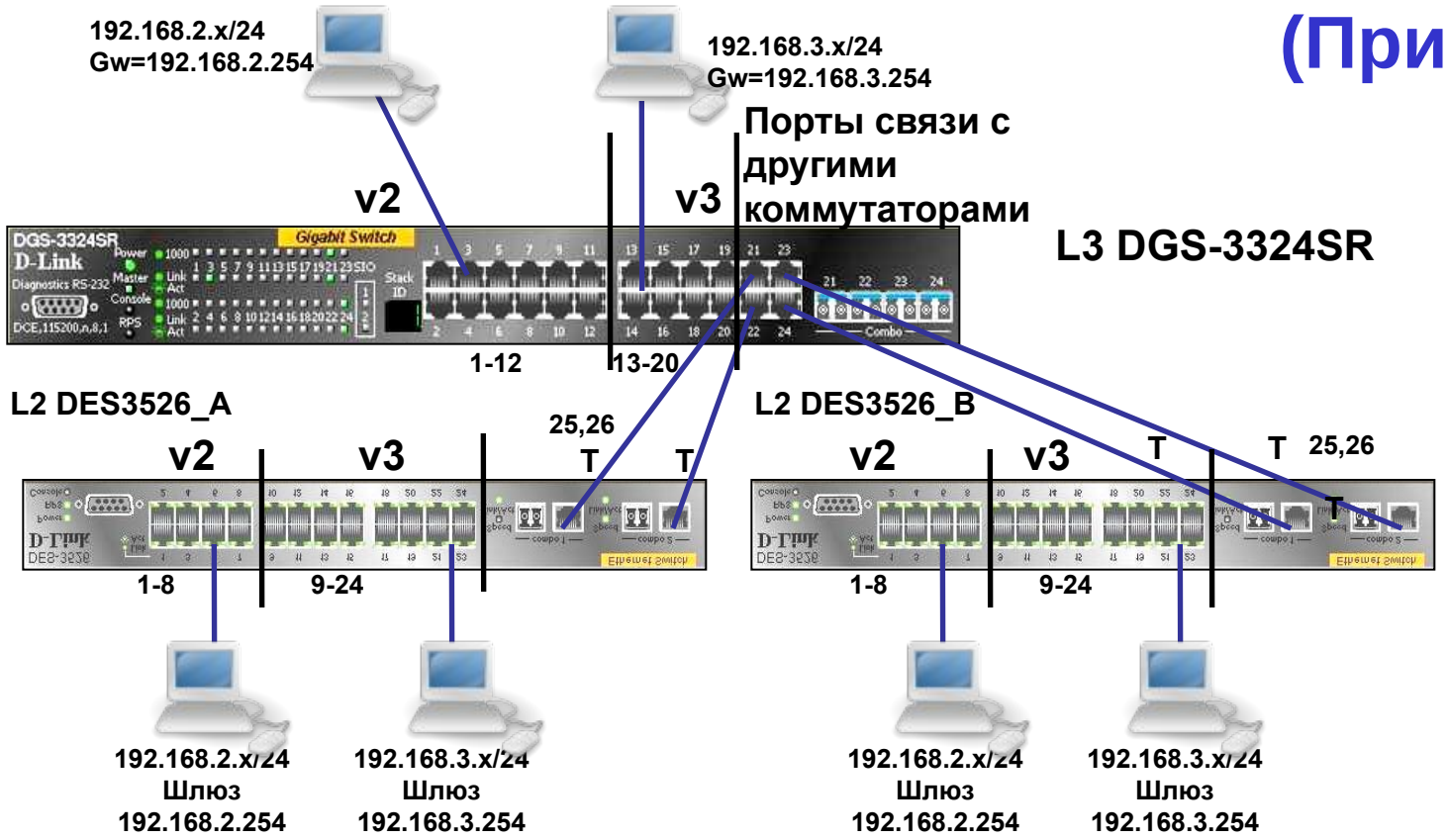
```
config vlan default delete 1-20

create vlan v2 tag 2
config vlan v2 add untagged 1-12
config vlan v2 add tagged 21-24
create vlan v3 tag 3
config vlan v3 add untagged 13-20
config vlan v3 add tagged 21-24

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

## 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 23 стал активным
## для v2, а порт 24 - для v3.
config stp mst_ports 1:23 instance_id 2 priority 96
config stp mst_ports 1:24 instance_id 3 priority 96
config stp ports 1-20 edge true
```

Конфигурация DGS-3324SR_B

```
config vlan default delete 1-20

create vlan v2 tag 2
config vlan v2 add tagged 21-24
config vlan v2 add untagged 1-12

create vlan v3 tag 3
config vlan v3 add tagged 21-24
config vlan v3 add untagged 13-20

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 1-20 edge true
```

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

MSTP в сетях третьего уровня (Пример)



Задача:

Пакеты маршрутизируются коммутатором уровня L3, в то время как MSTP функционирует на уровне L2. В обычном режиме осуществляется распределение нагрузки. Если одна линия отказывает, то используется вторая в качестве резервной.

D-Link
Building Networks for People

Конфигурация DGS3324SR L3

```
config vlan default delete 1-20

create vlan v2 tag 2
config vlan v2 add untagged 1-12
config vlan v2 add tagged 21-24
create ipif ip2 192.168.2.254/24 v2

create vlan v3 tag 3
config vlan v3 add untagged 13-20
config vlan v3 add tagged 21-24
create ipif ip3 192.168.3.254/24 v3

### Конфигурация MSTP
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 1-20 edge true
```

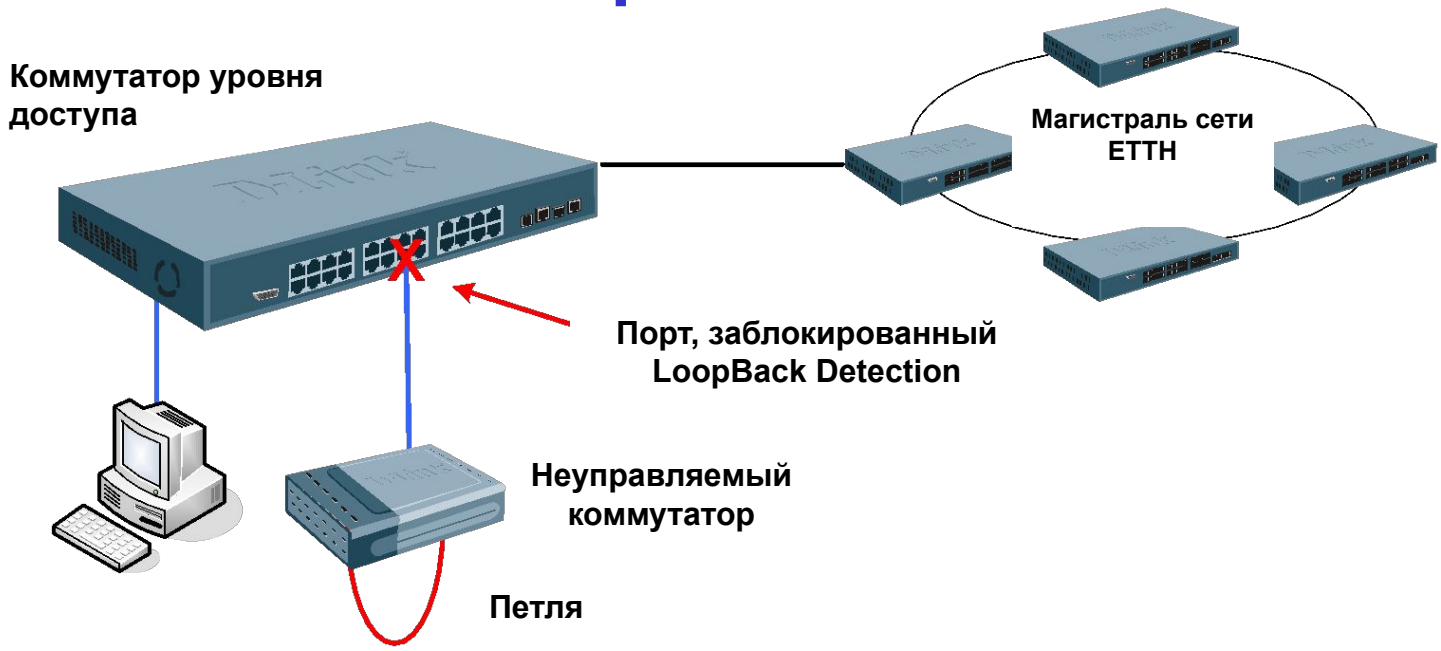
Конфигурации DES3526_A и DES3526_B L2

```
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 9-24
config vlan v3 add tagged 25-26

### Конфигурация MSTP
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
```

D-Link
Building Networks for People

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.

D-Link
Building Networks for People

STP LoopBack Detection (пример)

- Задача: Обеспечить на оконечных портах DES-3526 (edge ports) отсутствие петель в неуправляемых сегментах.

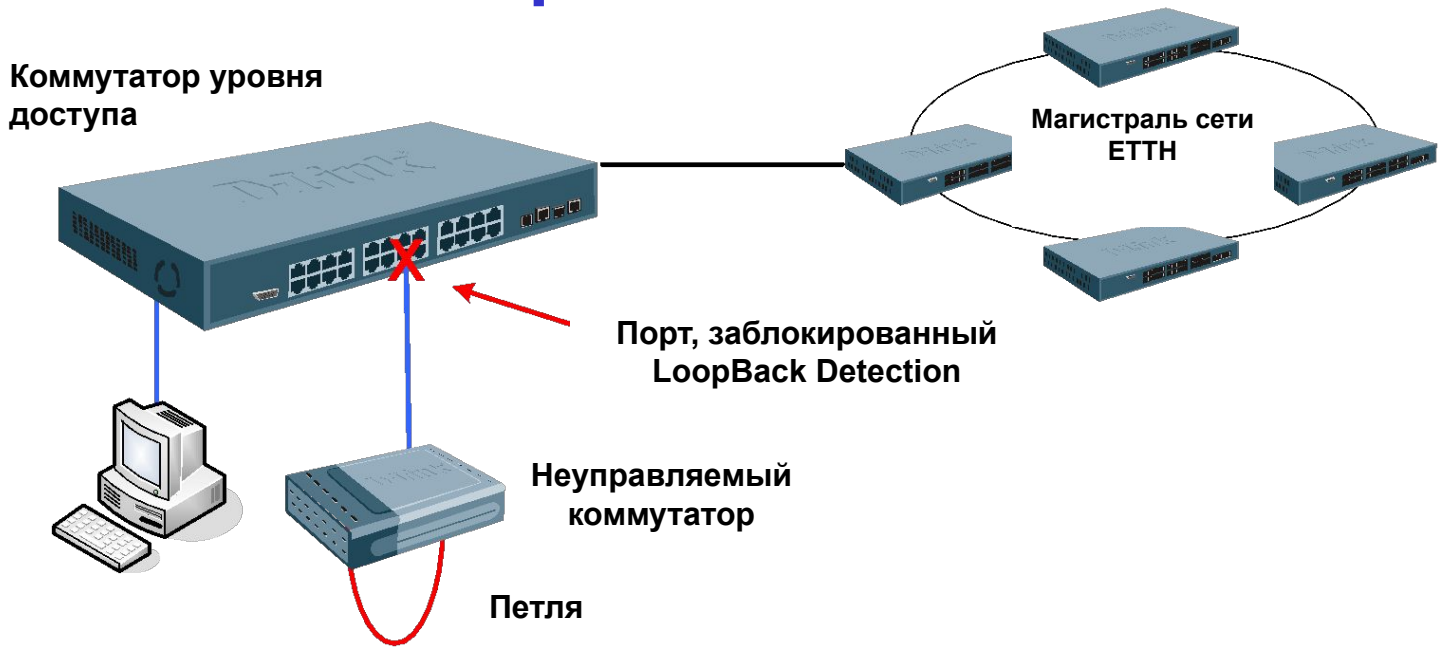
- Команды для настройки коммутатора:

  1) **enable stp** (по умолчанию версия RSTP)

  2) **config stp ports 1-24 state enable edge true lbd enable**

  3) **config stp lbd_recover_timer 60** (lbd_recover_timer – время, в течение которого порты не будут принимать BPDU. Оно задаётся глобально на коммутаторе. Если необходимо отключить эту функцию, то следует установить его в 0)

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.

  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**

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**

D-Link
Building Networks for People

Агрегирование портов

Статическое, 802.3ad LACP

D-Link
Building Networks for People

Агрегирование портов

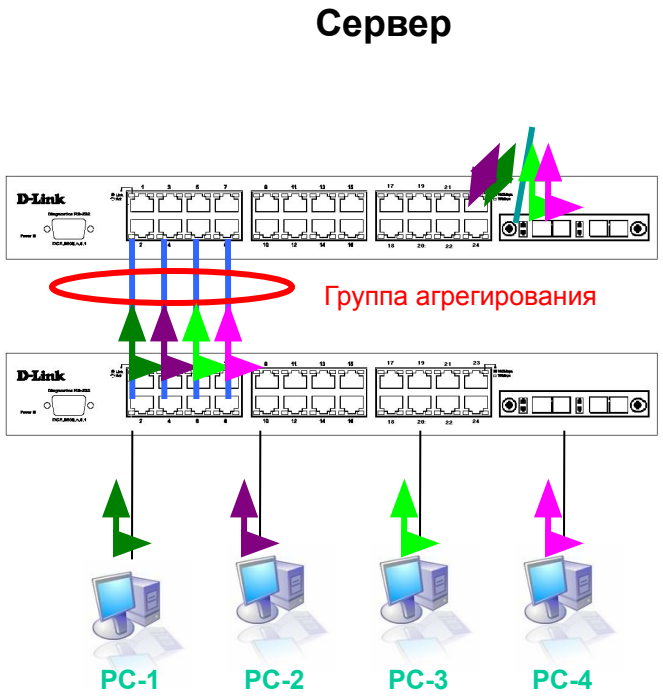
Агрегирование портов используется для объединения некоторого количества портов вместе для организации одного канала с высокой пропускной способностью. Такие порты называются членами группы агрегирования, а один из портов назначается мастером группы (**master port)**.

Так как все порты агрегированной группы должны работать в одном режиме, конфигурация мастера группы распространяется на все порты в группе. Таким образом, при конфигурировании портов в группе агрегирования достаточно настроить мастер-порт.

DES-3226S поддерживает группы агрегирования, каждая из которых может содержать от 2-ух до 8-ми портов, кроме группы агрегирования Gigabit, которая состоит из 2-ух (дополнительных) портов Gigabit Ethernet на модуле расширения.

Агрегирование портов - Пример

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.

Два метода агрегирования портов

1. **Статический**

   (поддерживался первыми коммутаторами D-Link)

1. **IEEE 802.3ad**

   LACP, динамический (новый)

D-Link
Building Networks for People

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.

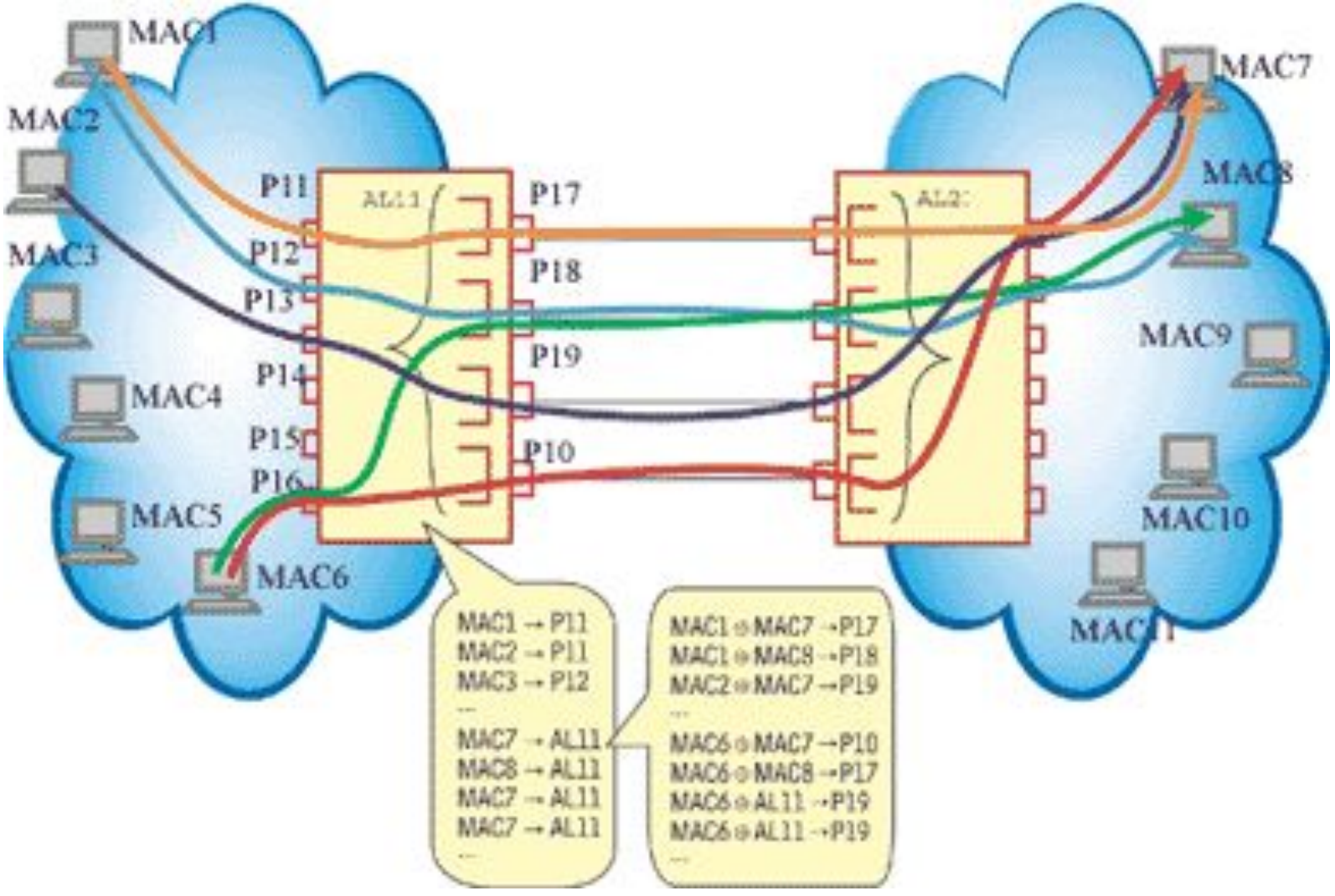
D-Link
Building Networks for People

Алгоритм агрегирования каналов

Этот алгоритм (на каждом устройстве) применяется для определения того, какой порт в группе используется для передачи определённых пакетов. Существует 6 алгоритмов. По умолчанию это MAC-source.

1. mac_source (по MAC-адресу источника)
2. mac_destination (по MAC-адресу назначения)
3. mac_source_dest (по MAC-адресам источника и назначения)
4. ip_source (по IP-адресу источника)
5. ip_destination (по IP-адресу назначения)
6. ip_source_dest (по IP-адресу источника и назначения)

Распределение потоков по каналам транков



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:

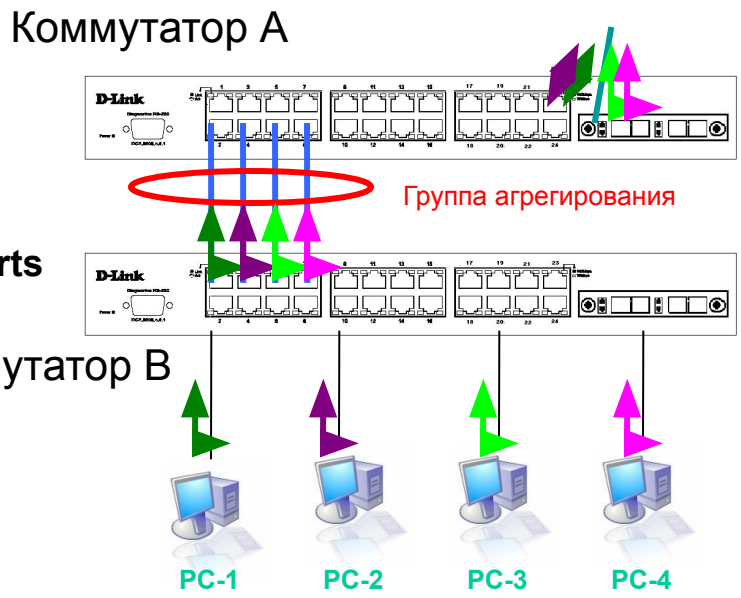
1. Создайте группу агрегирования

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



Динамическое (LACP) агрегирование каналов (Пример)

Для коммутатора A (на портах 1-8 включено автосогласование)

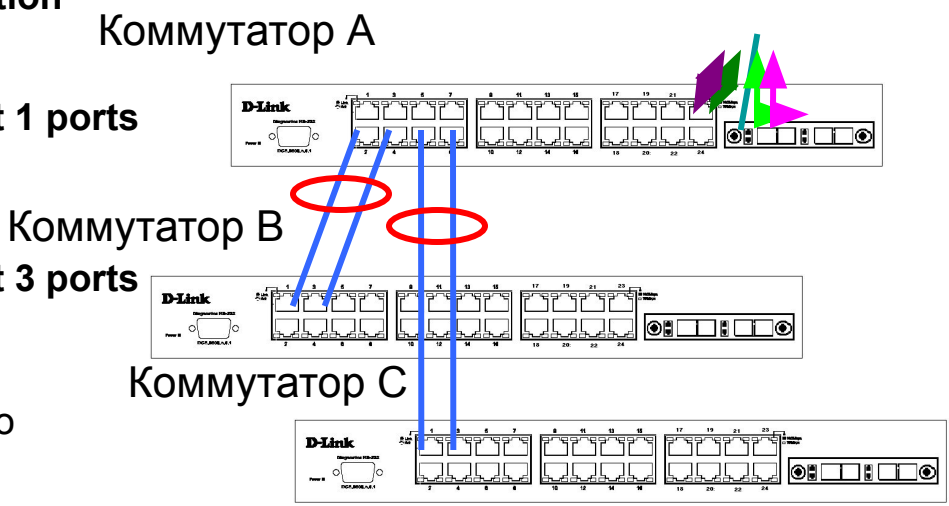
1. Создайте группу агрегирования

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

2. Задайте членов этой группы

config link_aggregation group_id 1 master_port 1 ports 1-2 state enabled
config lacp ports 1-2 mode active

config link_aggregation group_id 2 master_port 3 ports 3-4 state enabled
config lacp ports 3-4 mode active



Для коммутаторов B и C (на портах 1-4 включено автосогласование)

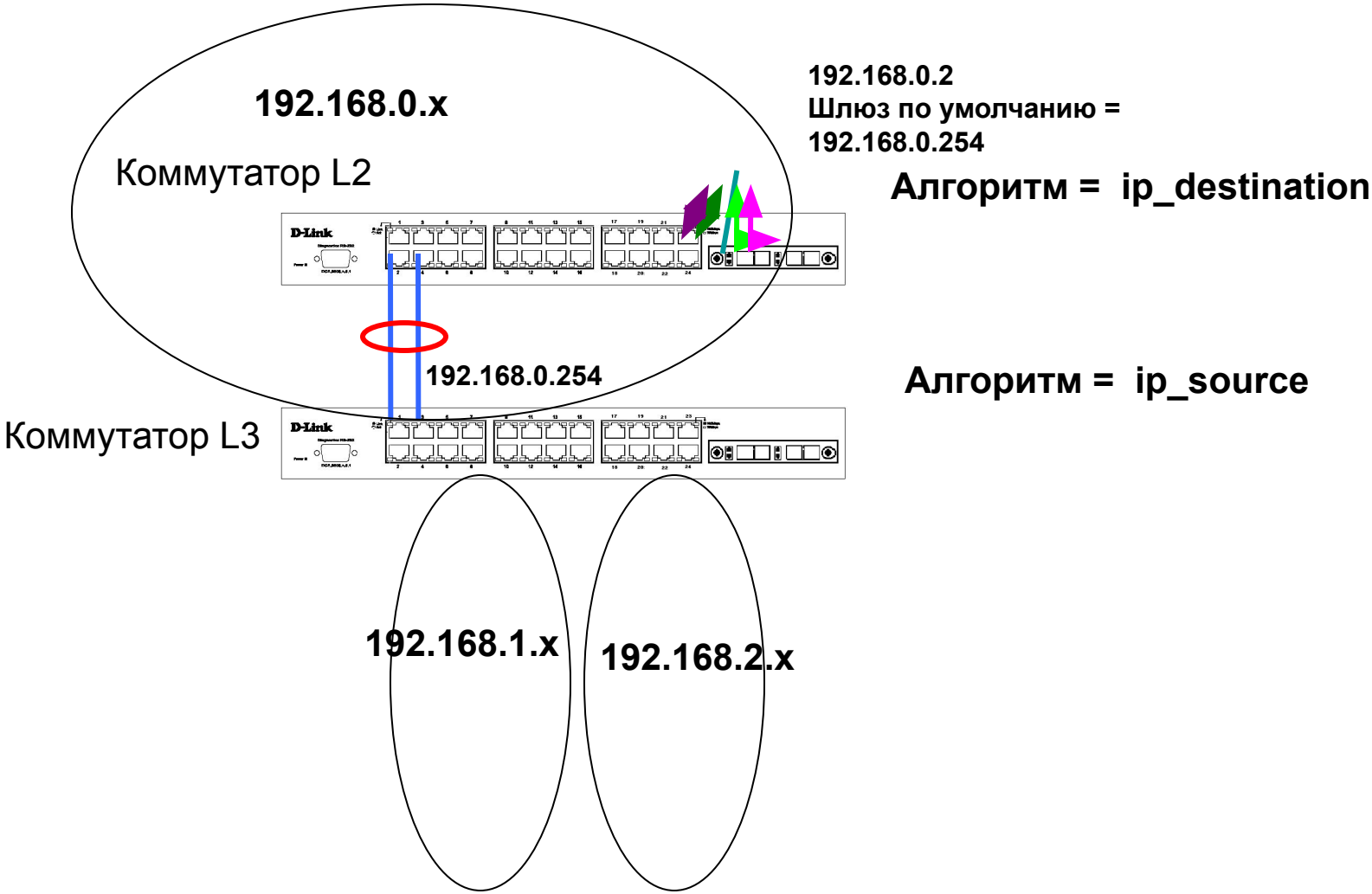
1. Создайте группу агрегирования

create link_aggregation group_id 1 type lacp
config link_aggregation algorithm mac_source

2. Задайте членов этой группы

config link_aggregation group_id 1 master_port 1 ports 1-2 state enabled

Алгоритм агрегирования каналов - IP (Пример)



Замечания:

1. Если на одном конце канала настроен LACP, на втором конце тоже должен быть LACP. Если с одной стороны LACP, а с другой статическая группа – канал работать не будет.
2. Если коммутатор, поддерживающий 802.3ad, должен быть соединён по агрегированному каналу с коммутатором, поддерживающим только статическое агрегирование, он должен быть тоже настроен в статическом режиме.
3. Если устаревший коммутатор D-Link, должен работать по агрегированному каналу с коммутатором Cisco, то коммутатор Cisco должен быть сконфигурирован в режиме “802.1q trunk” (например, Cisco 3600).

D-Link
Building Networks for People

Безопасность на уровне портов и защита от вторжений

D-Link
Building Networks for People

Port Security
(безопасность на уровне портов)

Port Security

- **Проверка подлинности компьютеров в сети**

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

Всё ещё не может получить доступ к сети по причине отсутствия регистрации !!

D-Link
Building Networks for People

Port Security

Команды:

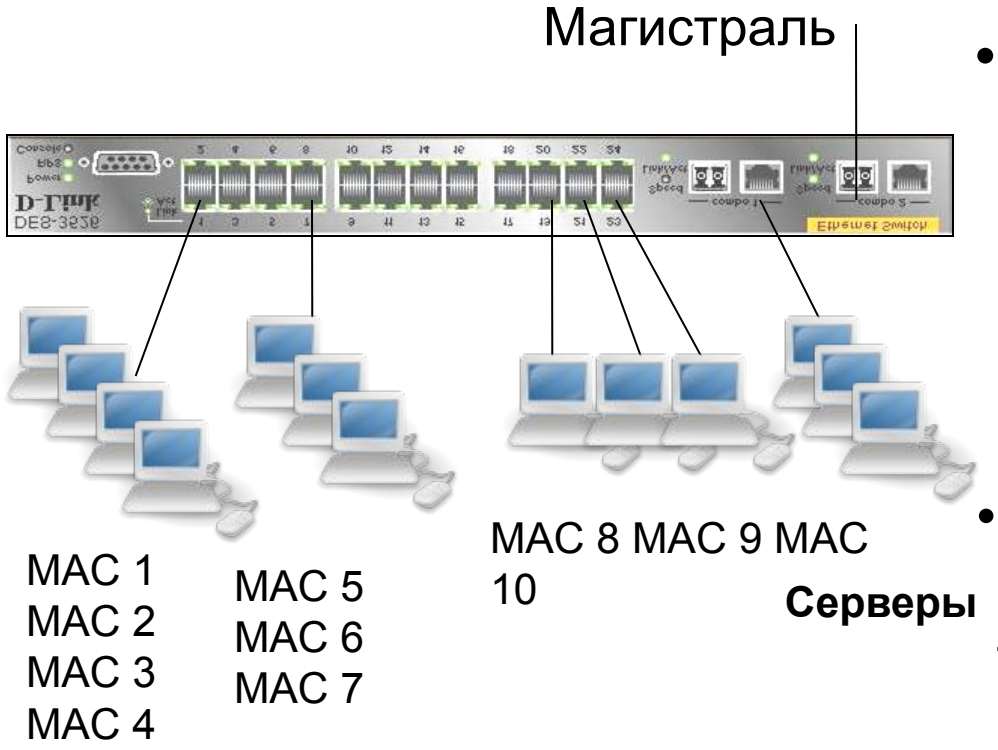
config port_security ports 1-3 admin_state enabled max_learning_addr 2

config port_security ports 4 admin_state enabled max_learning_addr 8

…

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.

D-Link
Building Networks for People

Port Security (пример)

Команды:

config port_security ports 1-24 admin_state enabled max_learning_addr 0
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
create fdb default 00-50-ba-00-00-08 port 20
create fdb default 00-50-ba-00-00-09 port 22
create fdb default 00-50-ba-00-00-10 port 24

(…все остальные разрешённые MAC-адреса)

Port Security для защиты от вторжений

- Режим блокировки адресов - “Непосредственный (permanent)”

  Пример: **config port_security ports 1:1-1:24 lock_address_mode Permanent**

- Возможность включения Port Security на каждом устройстве
- После включения на порту Port Security, выбора режима “Permanent” и задания количество MAC-адресов, которое может быть изучено, эти адреса просто будут добавлены в статическую таблицу MAC-адресов. Даже после включения/выключения, эта таблица всё равно сохраняется. В таблице также содержится время, в течение которого адрес актуален.
- Есть возможность выбора ещё двух режимов – DeleteOnReset и DeleteOnTimeout, которые удаляют заблокированные на портах адреса соответственно после сброса устройства к заводским настройкам и по таймауту
- Для того, чтобы разрешить непосредственно изученный MAC на порту, отключите Port Security на этом порту.

Контроль полосы пропускания

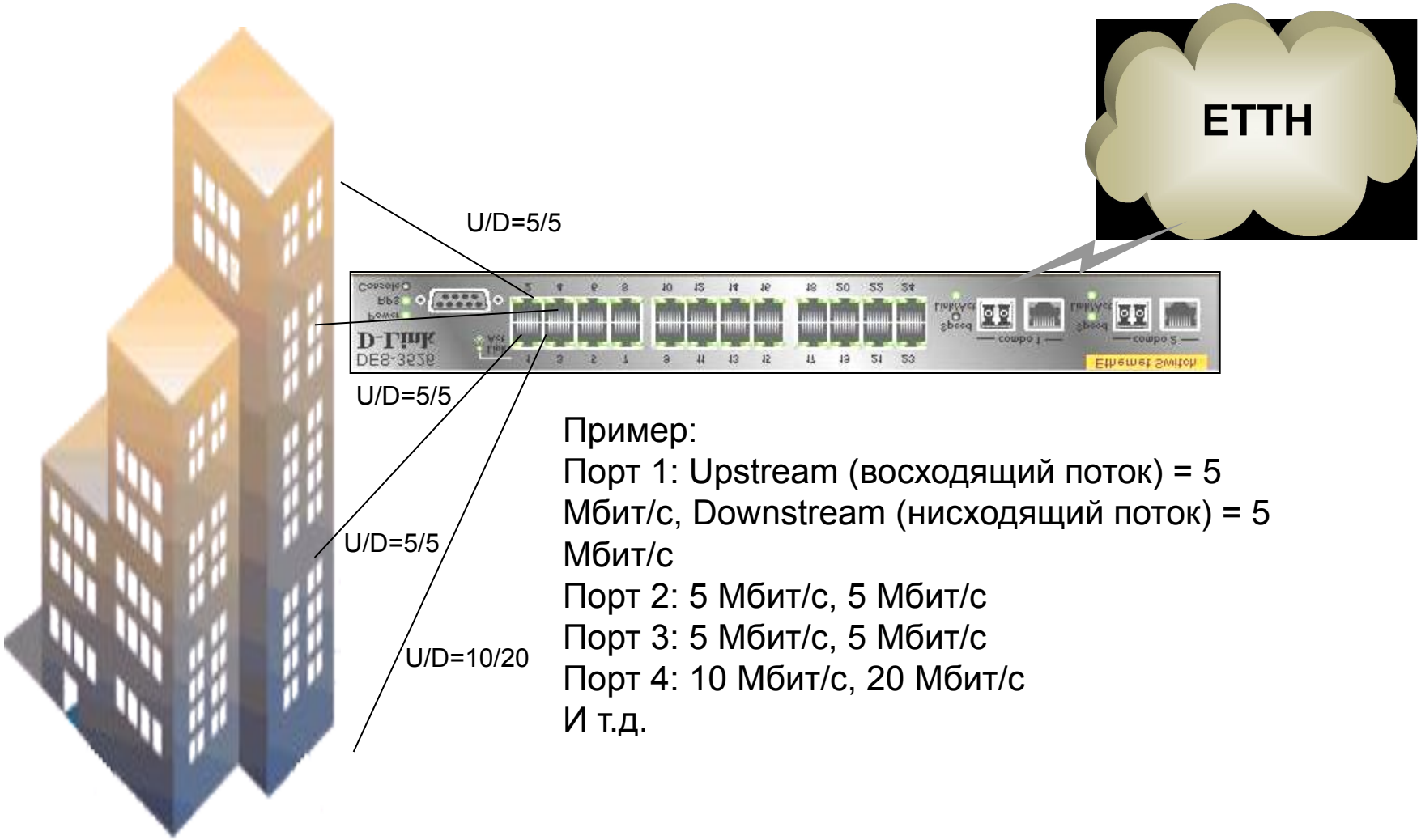
D-Link
Building Networks for People

Шаг настройки полосы пропускания на коммутаторах D-Link

Модель коммутатора	Шаг полосы пропускания на портах 100Base-TX	Шаг полосы пропускания на портах 1000Base-T
 DES-35XX	1 Мбит/с	8 Мбит/с
 DES-38XX, DGS-34XX, DGS-36XX, DES-3028/52, DGS-31XX	64 Кбит/с	64 Кбит/с
 DES-30XX	64 Кбит/с: до 2 Мбит/с 1 Мбит/с: от 2 Мбит/с до 100 Мбит/с	8 Мбит/с

Контроль полосы пропускания

Для каждого порта Ethernet, допускается ограничивать полосу пропускания для входящего и исходящего трафика.



Пример:
Порт 1: Upstream (восходящий поток) = 5 Мбит/с, Downstream (нисходящий поток) = 5 Мбит/с
Порт 2: 5 Мбит/с, 5 Мбит/с
Порт 3: 5 Мбит/с, 5 Мбит/с
Порт 4: 10 Мбит/с, 20 Мбит/с
И т.д.

D-Link
Building Networks for People

Контроль полосы пропускания

Настройка каждого порта
Полоса пропускания для входящего (rx или восходящий поток) или исходящего (tx или нисходящий поток).

config bandwidth_control 1-3 rx_rate 5 tx_rate 5

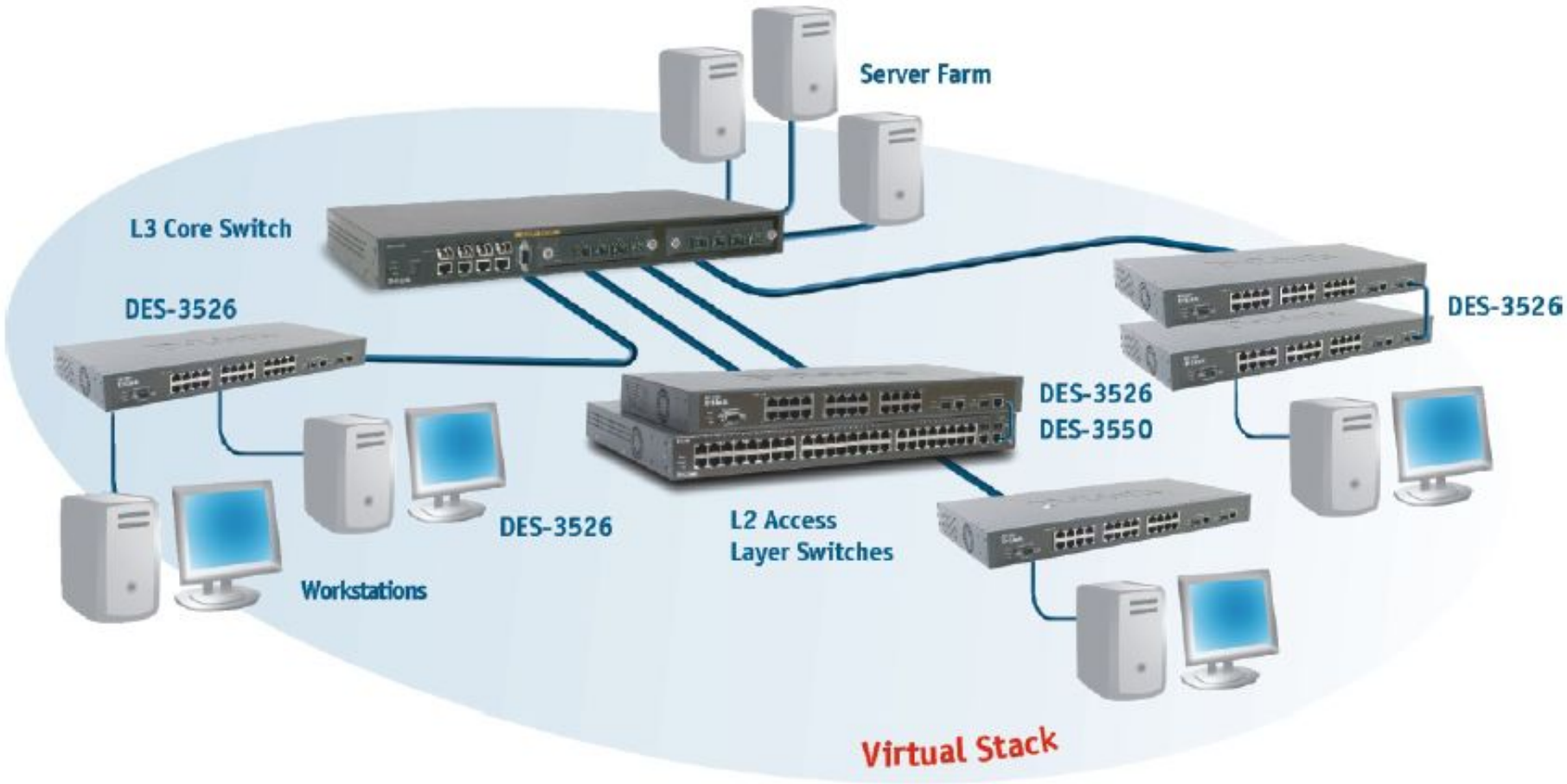
config bandwidth_control 4 rx_rate 10 tx_rate 20

(… для всех других портов, на которых необходим контроль за полосой пропускания)

Функции управления и мониторинга

D-Link
Building Networks for People

Технология Single IP Management: Виртуальный стек



D-Link
Building Networks for People

Преимущества и устройства, поддерживающие SIM

Обеспечивает управление до 32 устройств через один IP адрес.

В отличие от обычного стека, нет ограничения по моделям – в виртуальный стек можно включать любые модели, поддерживающие технологию SIM.

Нет ограничений на расстояние между коммутаторами, нет необходимости в специальных кабелях.

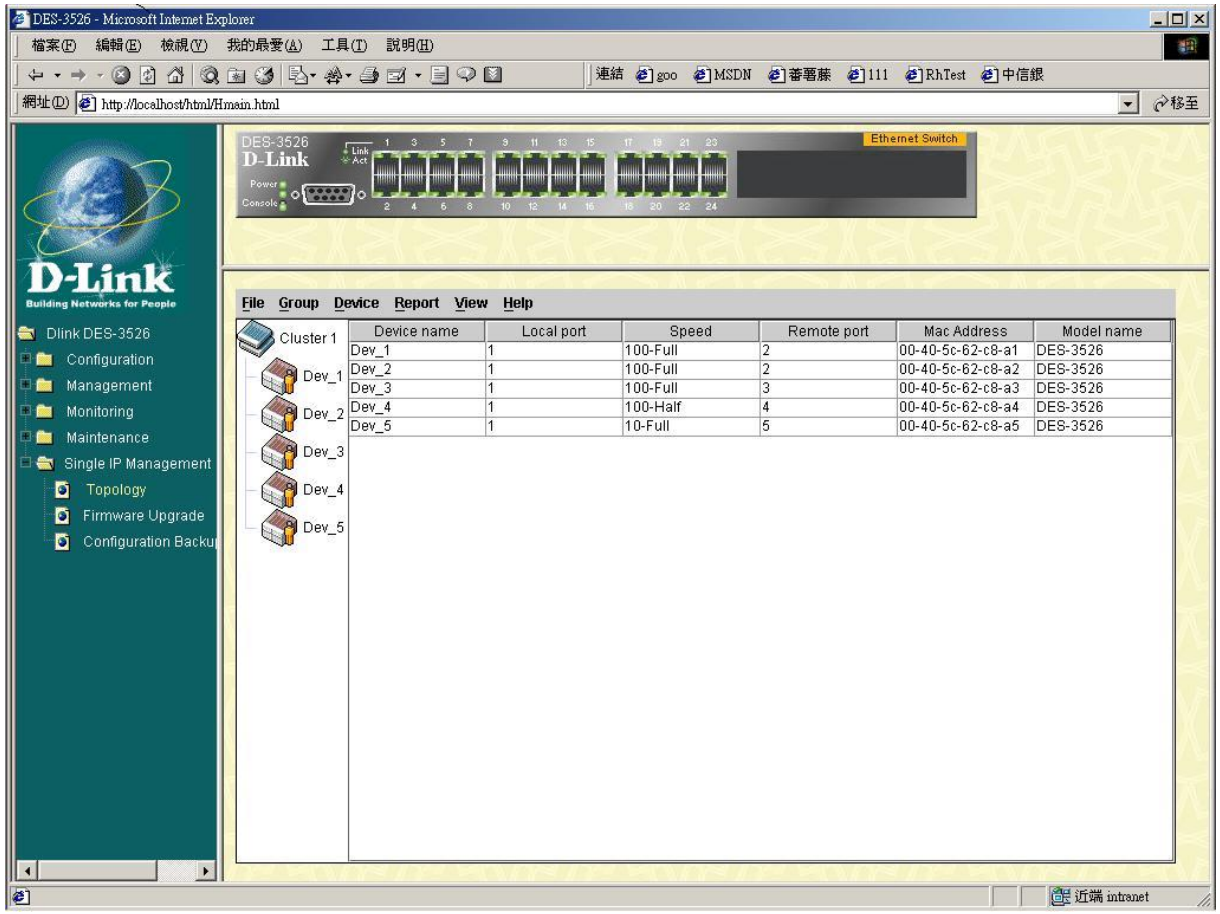
В стек могут быть объединены устройства, расположенные в любом месте сети. Это исключает возможность появления точки единственного отказа (single point of failure).

Коммутаторы DGS-3x12SR, DES-6500, DGS/DXS-33XX, DES-35XX, DES-3828,DGS-34XX, DGS-36XX, DES-30XX, DES-3028/3052 поддерживают SIM

D-Link
Building Networks for People

Как работает D-Link SIM?

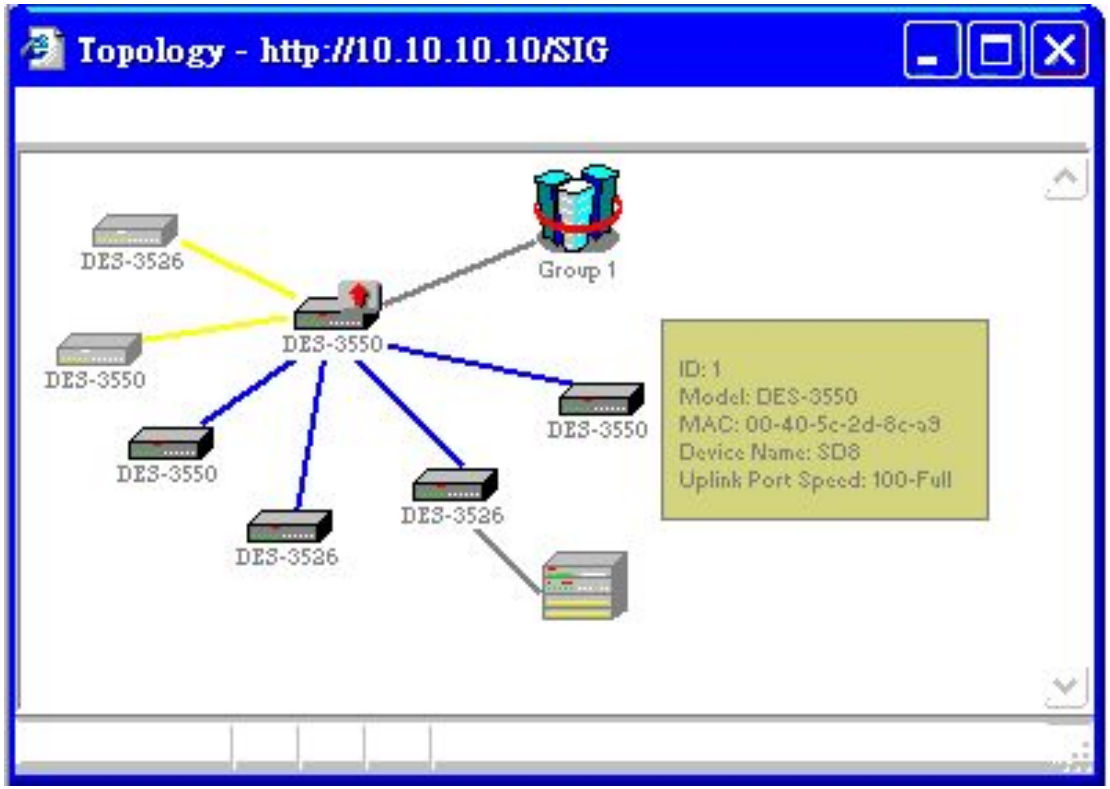
Коммутаторы с поддержкой SIM упрощают задачу управления, т.к. множество коммутаторов могут настраиваться, контролироваться и обслуживаться через один IP-адрес с любой рабочей станции, имеющей Web-браузер. Стек управляется как единый объект.



D-Link
Building Networks for People

Как работает D-Link SIM?

Просмотр топологии и всех устройств сети, входящих в виртуальный стек - в виде дерева (Tree View): отображает карту сети и соединения, месторасположения устройств стека и связи между ними. Это простое и эффективное Web-управление исключает необходимость установки дорогого ПО для SNMP-управления.



D-Link
Building Networks for People

Auto-Configuration - автоконфигурация

D-Link
Building Networks for People

Автоконфигурация

DHCP - сервер / TFTP - сервер

Заранее созданный конфигурационный файл коммутатора, например, test.cfg

Автоконфигурация

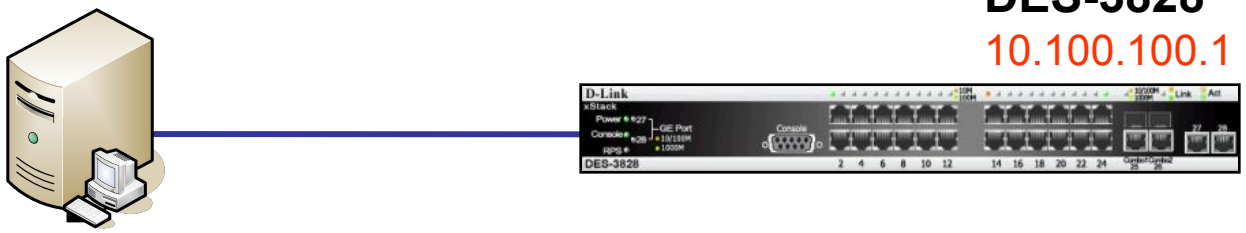
Все коммутаторы расположены в разных местах

При включении функции **auto-configuration**, коммутаторы могут:

- **автоматически получать IP-адрес с DHCP - сервера**
- **загружать созданный заранее и сохранённый конфигурационный файл с удалённого сервера**

Когда функция autoconfig включена на коммутаторе, DHCP – ответ будет содержать имя конфигурационного файла и полный путь к нему. Затем коммутатор запросит файл с TFTP – сервера, указанного в ответе. Если функция autoconfig включена, то коммутатор автоматически становится DHCP – клиентом.

Автоконфигурация: пример



DHCP - сервер / TFTP - сервер

DHCP - сервер:
DHCP : 10.100.100.100

IP Pool: 10.100.100.101 - 10.100.100.200

TFTP - сервер:
Заранее созданный конфигурационный файл коммутатора, например, test.cfg (с созданными 3-мя VLAN-ами)

Настройка функции автоконфигурации по шагам

1. Настройка DHCP и TFTP - серверов

- **Установите или сконфигурируйте службу DHCP сервера**, например, службу Windows 2000 Server DHCP. В этом примере используется DHCP - сервер “haneWin” DHCP Server. На DHCP – сервере, задайте пул IP-адресов, и IP-адрес TFTP сервера и имя конфигурационного файла коммутатора.
- **Запустите TFTP – сервер**.
  В этом примере используется TFTP – сервер D-Link’s TFTP Server.

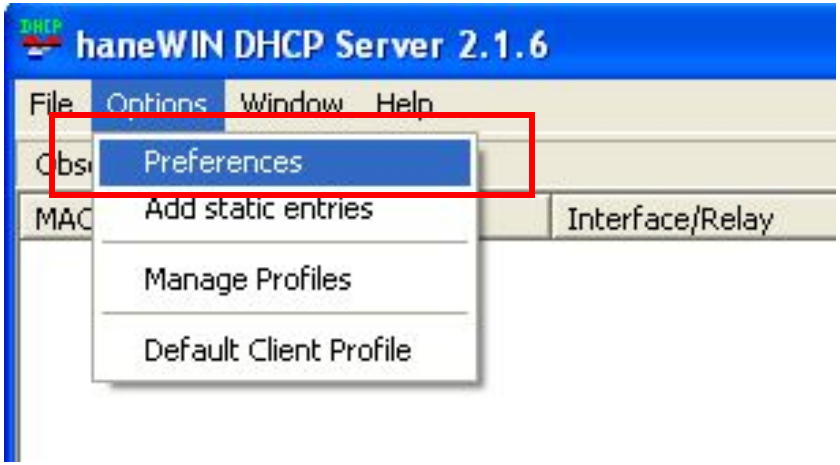
2. Настройка коммутатора

- **Включите функцию “auto-configuration”,** коммутатор автоматически получит IP-адрес и связанные с ним IP-адрес TFTP – сервера и имя конфигурационного файла с DHCP – сервера, сохранит информацию и перезагрузится. После загрузки коммутатора, он обратится к TFTP – серверу для загрузки конфигурационного файла.

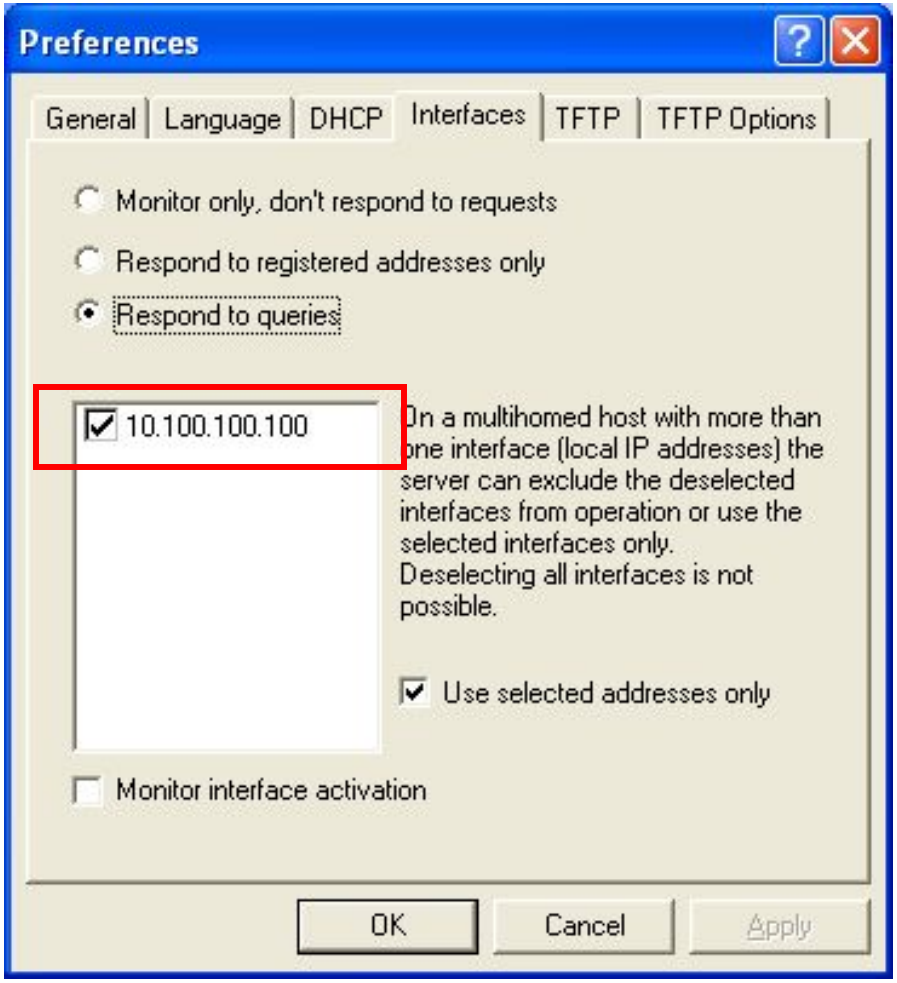
Настройка автоконфигурации - 1

1. Настройка DHCP - сервера (haneWin DHCP Server)

1.1 Выберите Опции Свойства, для того, чтобы настроить DHCP – сервер.



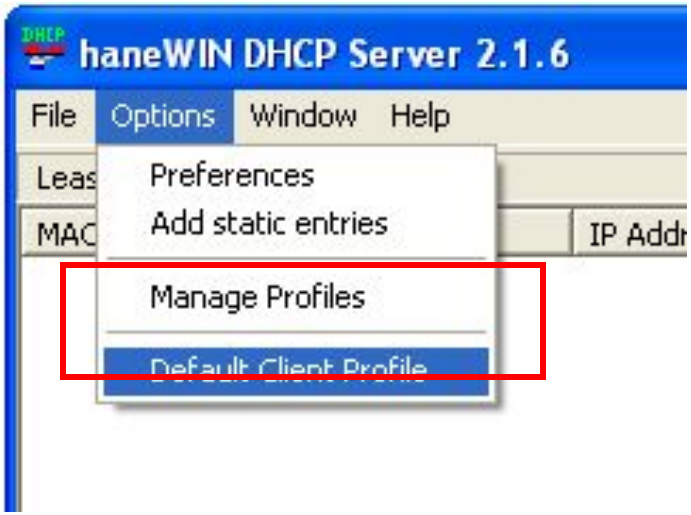
1.2 Выберите 10.100.100.100



Настройка автоконфигурации - 2

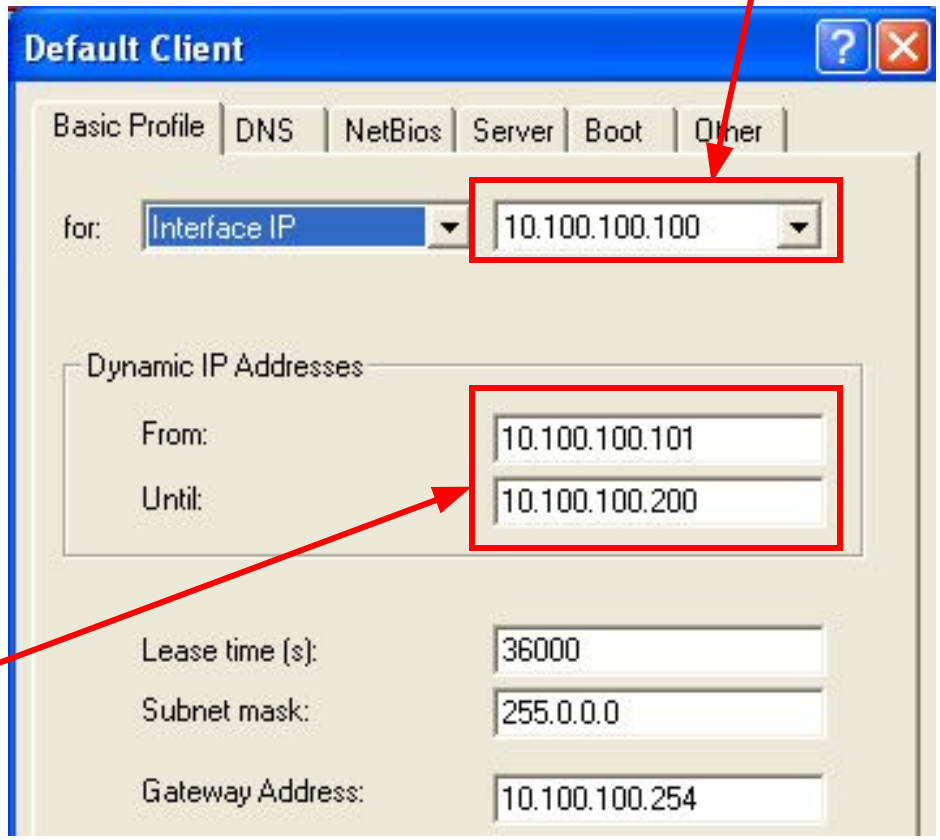
1. Настройка DHCP - сервера (haneWin DHCP Server)

1.3 Выберите Опции Профиль пользователя по умолчанию, для того, чтобы настроить DHCP – сервер.



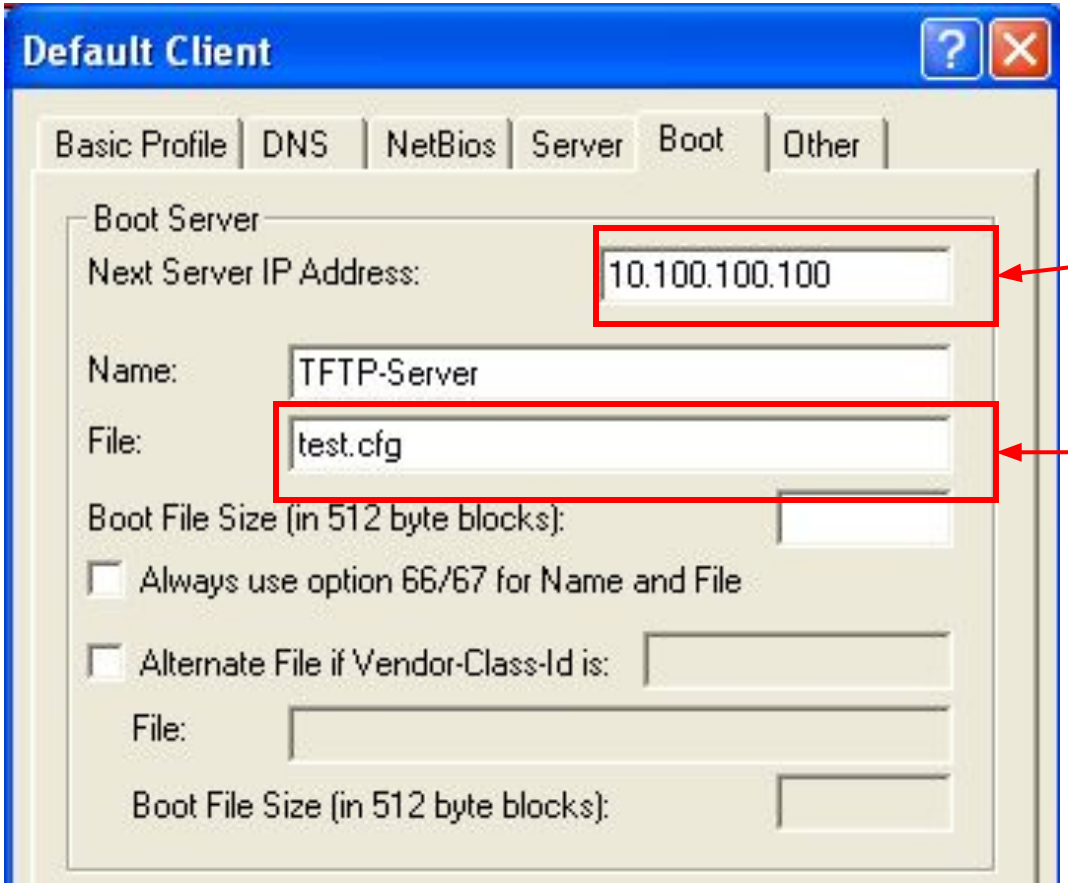
1.4 Задайте пул IP-адресов, маску подсети и т.д.

IP-адрес DHCP - сервера



Пул IP-адресов DHCP

Настройка автоконфигурации - 3



1.5 Задайте IP-адрес TFTP - сервера и имя конфигурационного файла коммутатора.

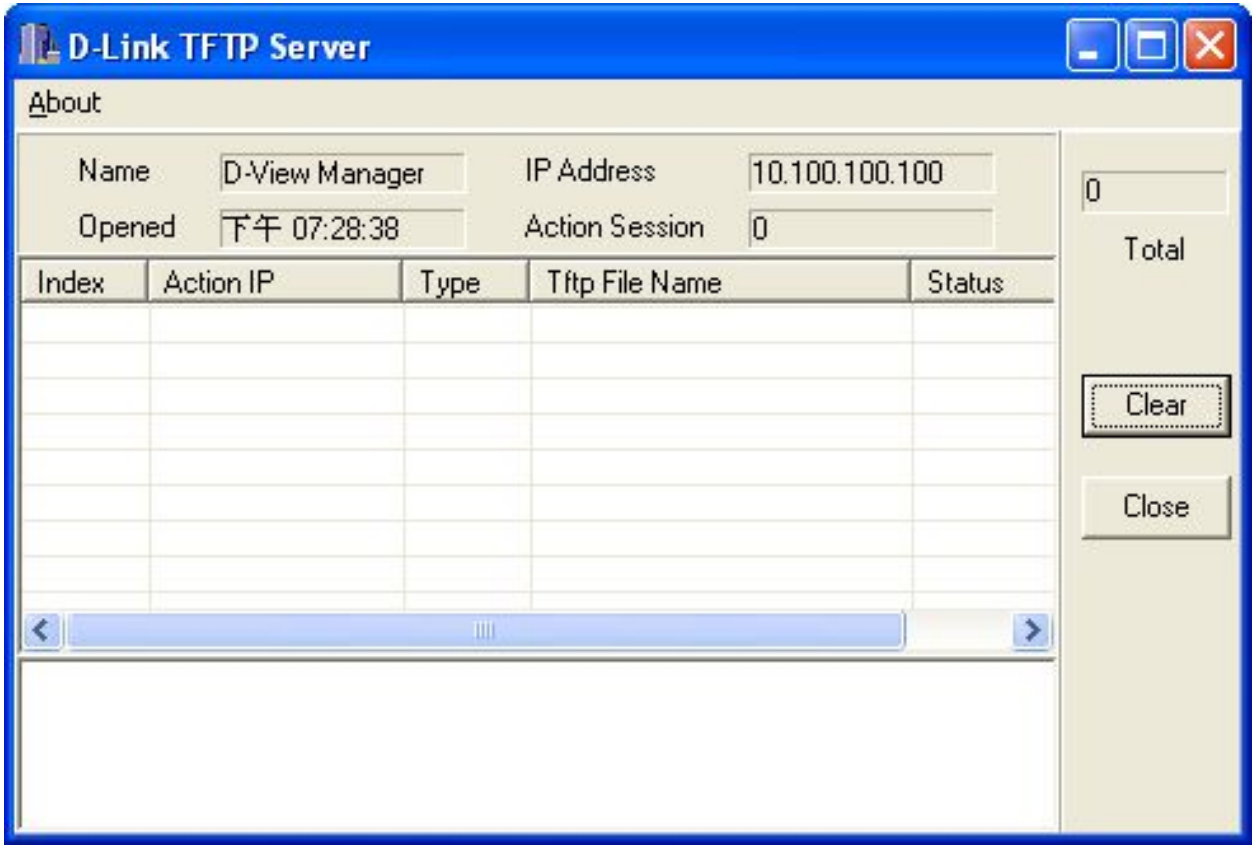
IP-адрес TFTP - сервера

Имя конфигурационного файла

Настройка автоконфигурации - 4

2. Запустите TFTP-сервер D-Link TFTP Server.

Если не указывать путь к файлу в настройках DHCP – сервера, то конфигурационный файл должен находиться в одной папке, что и TFTP – сервер.



Настройка автоконфигурации - 5

3. Конфигурация коммутатора:

3.1 Создание файла конфигурации.

“test.cfg” в этом примере. В нём мы создаём 3 VLAN-а.

3 VLAN-а
1. VLAN Default порты 1-8,25,26
2. VLAN v2 порты 9-16
3. VLAN v3 порты 17-24

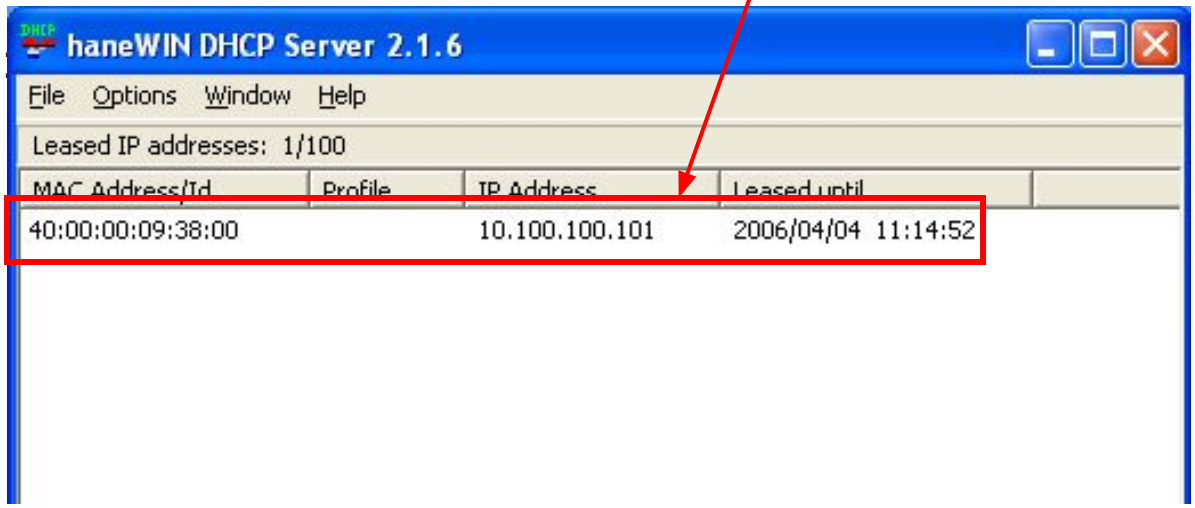
После включения функции “autoconfig”, можно увидеть, как DHCP - сервер выдал IP-адрес коммутатору

3.2 Настройка коммутатора:

enable autoconfig

save

reboot



Результаты автоконфигурации

Результаты:

1. Перед включением функции auto-configuration

DES-3800:4# **show switch**

Command: show switch

Device Type : DES-3828 Fast-Ethernet Switch
MAC Address : 40-00-00-09-38-00
IP Address : 10.90.90.90 (Manual)
Subnet Mask : 255.0.0.0
Default Gateway : 0.0.0.0

2. После включения функции auto-configuration, коммутатор получит IP-адрес автоматически с DHCP – сервера.

DES-3800:4# **show switch**

Command: show switch

Device Type : DES-3828 Fast-Ethernet Switch
MAC Address : 40-00-00-09-38-00
IP Address : 10.100.100.101 (DHCP) **→ IP-адрес поменялся на полученный по DHCP.**
Subnet Mask : 255.0.0.0 **→ Маска подсети поменялась на полученную по DHCP.**
Default Gateway : 10.100.100.254 **→ IP-адрес шлюза по умолчанию поменялся на полученный по DHCP.**

Результаты автоконфигурации

3. Сохраните настройки и перезагрузитесь. После перезагрузки, коммутатор начнёт загружать конфигурационный файл с TFTP – сервера автоматически.

DES-3800:4# **save**
DES-3800:4# **reboot**

После перезагрузки

DES-3800:4# download configuration 10.100.100.100 test.cfg **автоматическая загрузка**
Command: download configuration 10.100.100.100 test.cfg
Connecting to server..... Done.
Download configuration..... Done.
DES-3800:4#
DES-3800:4##---
DES-3800:4## DES-3828P Configuration
DES-3800:4##
DES-3800:4## Firmware: Build 2.00.B18
DES-3800:4## Copyright(C) 2004-2005 D-Link Corporation. All rights reserved.
DES-3800:4##---
DES-3800:4#
.....
.....

Результаты автоконфигурации

4. После успешного завершения загрузки и применения конфигурационного файла, коммутатор перелогинится. Затем Вы увидите, что применена конфигурация из файла test.cfg.

DES-3800:4# **show vlan**
Command: show vlan
VID : 1 VLAN Name : default
VLAN TYPE : static Advertisement : Enabled
Member ports : 1-8,25-28
Static ports : 1-8,25-28
Current Untagged ports : 1-8,25-28
Static Untagged ports : 1-8,25-28
VID : 2 VLAN Name : v2
Member ports : 9-16
Static ports : 9-16
VID : 3 VLAN Name : v3
VLAN TYPE : static Advertisement : Disabled
Member ports : 17-24
……
Total Entries : 3

D-Link®
Building Networks for People

Спасибо!