

**ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ
БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО
ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ**

Кафедра МСИБ

**Методические указания к лабораторной работе
«Настройка асимметричных VLAN и сегментации
трафика»**

Составители: к. т. н., доцент Ермолаев С. Ю.
аспирант Раштвин А. Р

Редактор: д.т.н., профессор Карташевский В. Г.

Рецензент: д.т.н., профессор Васин Н. Н.

Самара, 2013

Цель работы: Ознакомиться с командами настройки асимметричных VLAN, изучить функцию сегментации трафика.

Рекомендуемые источники:

1. Смирнова Е.В., Пролетарский А.В., Баскаков И.В., Федотов Р.А. Управление коммутируемой средой. – М.: РУСАКИ, 2011. – 335 с.
2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2000.

Подготовка к работе

1. Изучить основные данные, касающиеся коммутаторов D-Link, из рекомендованных источников [1, 2].
2. Ознакомиться с содержанием данной методической разработки.
3. Подготовить бланк отчета, который должен содержать:
 - цель работы;
 - схему подключения устройства.

Контрольные вопросы

1. Для чего предназначены асимметричные VLAN?
2. Что происходит с портами коммутатора, на которых настроены асимметричные VLAN?
3. В чем заключаются различия настройки асимметричных VLAN на коммутаторах 2-го и 3-го уровней?
4. Для чего предназначена функция сегментации трафика?
5. Назовите преимущества сегментации трафика по сравнению с асимметричными VLAN.
6. Основное различие между симметричными VLAN и асимметричными VLAN.
7. Расскажите про приоритетность правил Asymmetric VLAN и Traffic Segmentation.
8. Для чего необходимо иерархическое дерево в механизме сегментации трафика?
9. В каком из двух рассмотренных способов обеспечивается поддержка механизма IGMP Snooping?

Содержание отчета

1. Цель работы.
2. Схему подключения.

3. Основные параметры асимметричных VLAN, настроенные в процессе работы.
4. Выводы по проделанной работе.

Задание для выполнения работы

Необходимо:

1. Подключиться к коммутатору.
2. Настроить асимметричные VLAN.
3. Настроить функцию сегментации трафика.

Методические указания к выполнению работы

Основной целью асимметричных VLAN (Asymmetric VLAN) является более эффективное использование разделяемых ресурсов, такие как серверы или Интернет-шлюзы, в коммутируемых сетях. Данная функция реализована в программном обеспечении коммутаторов 2-го уровня D-Link. Асимметричные виртуальные локальные сети позволяют клиентам, принадлежащим разным VLAN и не поддерживающим тегирование 802.1Q взаимодействовать с сервером (или несколькими серверами) через один физический канал связи с коммутатором, не требуя использования внешнего маршрутизатора. Активизация функции Asymmetric VLAN на коммутаторе 2-го уровня позволяет сделать его немаркированные порты членами нескольких виртуальных локальных сетей. При этом рабочие станции остаются полностью изолированными друг от друга. Например, асимметричные VLAN могут быть настроены так, чтобы обеспечить доступ к почтовому серверу всем почтовым клиентам. Клиенты смогут отправлять и получать данные через порт коммутатора, подключенный к почтовому серверу, но прием и передача данных через остальные порты будет для них запрещена.

При активизации асимметричных VLAN каждому порту коммутатора назначается уникальный PVID в соответствии с идентификатором VLAN, членом которой он является. При этом каждый порт может получать кадры от VLAN по умолчанию.

Функция Asymmetric VLAN не поддерживается коммутаторами 3-го уровня. Организация обмена данными между устройствами различных VLAN, не поддерживающих тегирование, реализуется в таких коммутаторах с помощью маршрутизации и списков управления доступом (ACL), ограничивающих доступ устройств к сети.

Основное различие между базовым стандартом 802.1Q VLAN (или симметричными VLAN) и асимметричными VLAN заключается в

том, как выполняется отображение MAC-адресов. Симметричные VLAN используют отдельные адресные таблицы, и, таким образом, не происходит пересечения MAC-адресов между виртуальными локальными сетями. Асимметричные VLAN используют одну общую таблицу MAC-адресов.

При использовании асимметричных VLAN не поддерживается механизм IGMP Snooping (процесс отслеживания сетевого трафика IGMP).

Функция сегментации трафика (Traffic Segmentation) 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 магистральной сети. Этот метод изоляции трафика аналогичен функции Asymmetric VLAN, но его применение ограничено пределами одного коммутатора или нескольких коммутаторов в стеке, т.к. членство в группе портов не может распространяться по сети.

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

- простота настройки (не требуются специальные знания о стандарте 802.1Q);
- поддерживается работа механизма 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 сегментации трафика может использоваться с целью сокращения трафика внутри сетей VLAN 802.1Q, позволяя разбивать их на более маленькие группы. При этом правила VLAN имеют более высокий приоритет при передаче трафика. Правила Traffic Segmentation применяются после них.

1 Подключение к коммутатору

1.1. Подключите компьютер к коммутатору по консольному порту через интерфейс RS-232. После этого на рабочем столе запустите приложение putty.exe. Выберите тип подключения – Serial.

2 Настройка асимметричных VLAN

2.1. После подключения к коммутатору и появления строки приглашения (Command Promt) сбросьте настройки коммутатора к настройкам по умолчанию командой `reset config`.

2.2. Включите функцию асимметричных VLAN командой `enable asymmetric_vlan`.

2.3. Проверьте, все ли порты назначены в VLAN по умолчанию командой `show vlan`.

2.4. Создайте VLAN `net2` и `net3`, добавьте в соответствующие VLAN немаркированные порты следующими командами:

```
create vlan net2 tag 2
create vlan net3 tag 3
config vlan net2 add untagged 1-8
config vlan net3 add untagged 1-4, 9-10
```

2.5. Назначьте PVID немаркированным портам созданных VLAN командами

```
config gvrp 1-4 pvid 1
config gvrp 5-8 pvid 2
config gvrp 9-10 pvid 3
```

2.6. Соберите схему подключения, представленную на рис. 1.

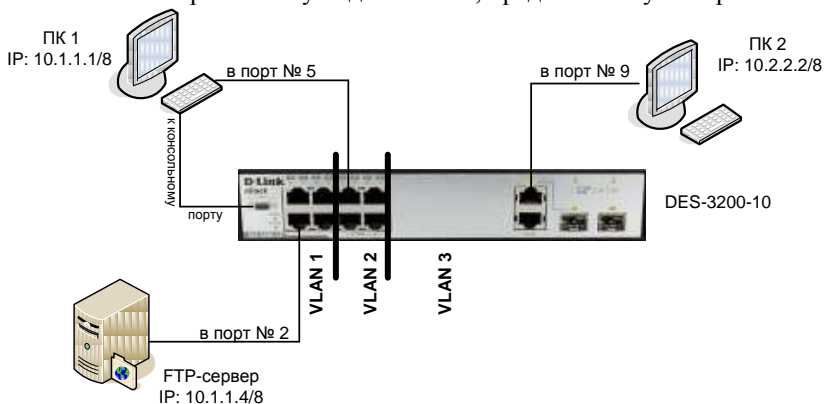


Рисунок 1 – Настройка асимметричных VLAN

2.7. Выполните команду `ping` от ПК1 к FTP-серверу, от ПК2 к FTP-серверу, от ПК1 к ПК2, от ПК2 к ПК1.

2.8. Проверьте состояние PVID на всех портах коммутатора командой `show gvrp`.

Примечание: команда `ping` выполняется в режиме командной строки Windows (Пуск – Выполнить – cmd).

2.9. Разъедините схему, представленную на рис. 6 и сбросьте настройки коммутатора к настройкам по умолчанию командой `reset config`.

2.10. Включите функцию асимметричных VLAN командой `enable asymmetric_vlan`.

2.11. Проверьте, все ли порты назначены в VLAN по умолчанию, командой `show vlan`.

2.12. Создайте VLAN `net2`, `net3`, `net4` и добавьте в соответствующие VLAN немаркированные порты следующими командами:

```
create vlan net2 tag 2
create vlan net3 tag 3
create vlan net4 tag 4
config vlan net2 add untagged 3-4, 7-8
config vlan net3 add untagged 1-2, 5-6
config vlan net4 add untagged 1-4, 7-8
```

2.13. Назначьте PVID немаркированным портам созданных VLAN командами

```
config gvrp 1-2 pvid 1
config gvrp 3-4 pvid 2
config gvrp 5-6 pvid 3
config gvrp 7-8 pvid 4
```

2.14. Соберите схему подключения, представленную на рис. 2.

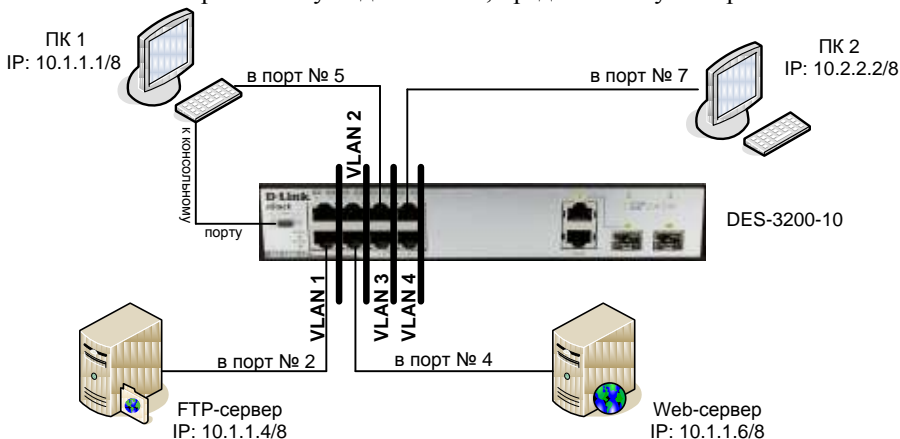


Рисунок 2 – Настройка асимметричных VLAN

2.15. Выполните команду `ping`:

- от ПК1 (VLAN3) к FTP-серверу (VLAN1);
- от ПК2 (VLAN4) к FTP-серверу (VLAN1);
- от ПК1 (VLAN3) к Web-серверу (VLAN2);
- от ПК2 (VLAN4) к Web-серверу (VLAN2);
- от FTP-сервера (VLAN1) к Web-серверу (VLAN2);
- от ПК1 (VLAN3) к ПК2 (VLAN4).

3 Настройка сегментации трафика на одном коммутаторе

В данном задании выполняется настройка сегментации трафика, которая позволит рабочим станциям из групп 2 и 3 получить доступ к серверу из группы 1. При этом обмен данными между устройствами групп 2 и 3 запрещен.

3.1. Разъедините схему, представленную на рис. 7 и сбросьте настройки коммутатора к настройкам по умолчанию командой `reset config`.

3.2. Настройте сегментацию трафика командами
`config traffic_segmentation 1-4 forward_list 1-10`
`config traffic_segmentation 5-8 forward_list 1-8`
`config traffic_segmentation 9-10 forward_list 1-4, 9-10`

3.3. Проверьте внесенные настройки командой `show traffic_segmentation`.

3.4. Соберите схему подключения, представленную на рис. 3.

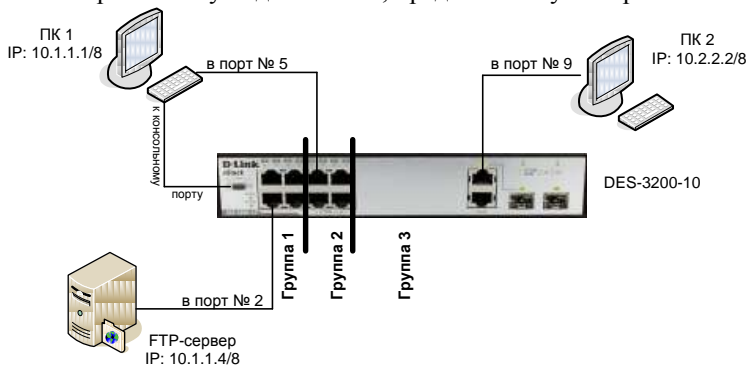


Рисунок 3 – Настройка сегментации трафика на одном коммутаторе

3.5. Выполните команду `ping`:

- от ПК1 (Группа 2) к FTP-серверу (Группа 1);
- от ПК2 (Группа 3) к FTP-серверу (Группа 1);

- от ПК1 (Группа 2) к ПК2 (Группа 3).

4 Настройка сегментации трафика на двух коммутаторах

В данном задании выполняется настройка сегментации трафика на двух коммутаторах, позволяющая разным группам получать доступ к совместно используемому серверу, но запрещающая доступ друг к другу.

4.1. Настройка коммутатора DES-3200-10_A. Сбросьте настройки коммутатора к настройкам по умолчанию командой `reset config`.

4.2. Настройте сегментацию трафика командами

```
config traffic_segmentation 1-3 forward_list 1-10
```

```
config traffic_segmentation 4 forward_list 1-4
```

```
config traffic_segmentation 5-6 forward_list 1-3, 5-6
```

```
config traffic_segmentation 7-10 forward_list 1-3, 7-10
```

4.3. Проверьте внесенные настройки командой `show traffic_segmentation`.

4.4. Настройка коммутатора DES-3200-10_B. Сбросьте настройки коммутатора к настройкам по умолчанию командой `reset config`.

4.5. Настройте сегментацию трафика командами

```
config traffic_segmentation 1 forward_list 1-10
```

```
config traffic_segmentation 2-6 forward_list 1-6
```

```
config traffic_segmentation 7-10 forward_list 1, 7-10
```

4.6. Проверьте внесенные настройки командой `show traffic_segmentation`.

4.7. Соберите схему подключения, представленную на рис. 4.

4.8. Выполните команду `ping`:

- от ПК1 (Группа 2) к FTP-серверу (Группа 1);
- от ПК2 (Группа 3) к FTP-серверу (Группа 1);
- от ПК3 (Группа 4) к FTP-серверу (Группа 1);
- от ПК1 (Группа 2) к ПК2 (Группа 3);
- от ПК2 (Группа 3) к ПК3 (Группа 4);
- от ПК3 (Группа 4) к ПК1 (Группа 2).

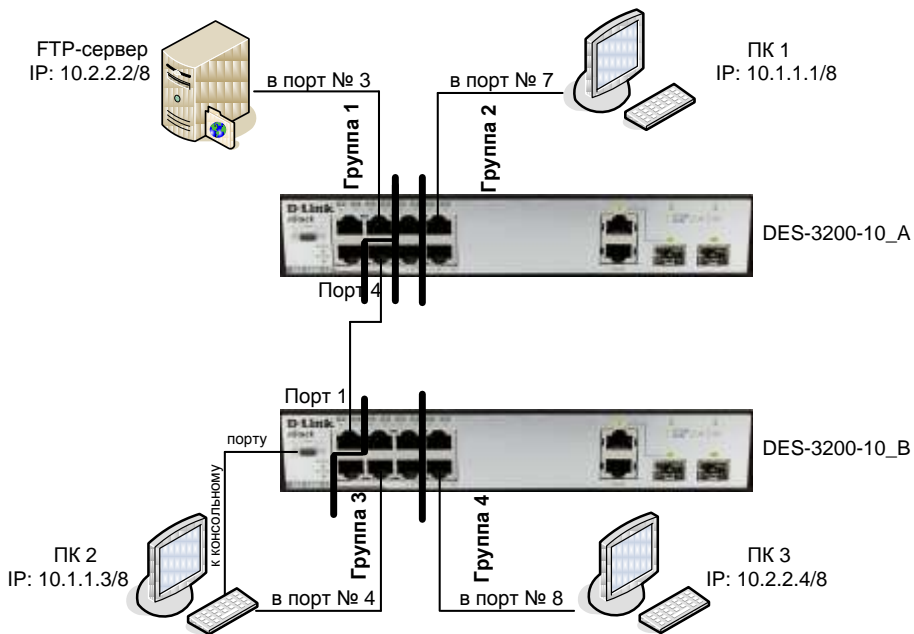


Рисунок 4 – Настройка сегментации трафика на двух коммутаторах