Cisco Packet Tracer
Лабораторная работа №3
Настройка VLAN на коммутаторах Cisco

Теоретическая часть

VLAN (Virtual Local Area Network – Виртуальная локальная вычислительная сеть) – группа устройств, имеющих возможность взаимодействовать между собой напрямую на канальном уровне, хотя физически при этом они могут быть подключены к разным сетевым коммутаторам. И наоборот, устройства, находящиеся в разных VLAN'ах, невидимы друг для друга на канальном уровне, даже если они подключены к одному коммутатору, и связь между этими устройствами возможна только на сетевом и более высоких уровнях.

В современных сетях VLAN – главный механизм для создания логической топологии сети, не зависящей от её физической топологии. VLAN'ы используются для сокращения широковещательного трафика в сети. Имеют большое значение с точки зрения безопасности, в частности как средство борьбы с ARP-spoofing'ом.

Причины использования VLAN

Гибкое разделение устройств на группы

Как правило, одному VLAN соответствует одна подсеть. Устройства, находящиеся в разных VLAN, будут находиться в разных подсетях. Но в то же время VLAN не привязан к местоположению устройств и поэтому устройства, находящиеся на расстоянии друг от друга, все равно могут быть в одном VLAN независимо от местоположения

Уменьшение количества широковещательного трафика в сети

Каждый VLAN – это отдельный широковещательный домен. Например, коммутатор – это устройство 2 уровня модели OSI. Все порты на коммутаторе с лишь одним VLAN находятся в одном широковещательном домене. Создание дополнительных VLAN на коммутаторе означает разбиение коммутатора на несколько широковещательных доменов. Если один и тот же VLAN настроен на разных коммутаторах, то порты разных коммутаторов будут образовывать один широковещательный домен.

Увеличение безопасности и управляемости сети

Когда сеть разбита на VLAN, упрощается задача применения политик и правил безопасности. С VLAN политики можно применять к целым подсетям, а не к отдельному устройству. Кроме того, переход из одного VLAN в другой предполагает прохождение через устройство 3 уровня, на котором, как правило, применяются политики, разрешающие или запрещающие доступ из VLAN в VLAN.

Тегирование трафика VLAN

Если смотреть на VLAN, абстрагируясь от понятия «виртуальные сети», то можно сказать, что VLAN – это просто метка в кадре, который передается по сети. Метка содержит номер VLAN’а (его называют VLAN ID или VID), – на который отводится 12 бит, то есть, VLAN может нумероваться от 0 до 4095. Первый и последний номера зарезервированы, их использовать нельзя.

Компьютер при отправке трафика в сеть даже не догадывается, в каком VLAN'е он размещён. Об этом думает коммутатор. Коммутатор знает, что компьютер, который подключен к определённому порту, находится в соответствующем VLAN'е. Трафик, приходящий на порт определённого VLAN'а, ничем особенным не отличается от трафика другого VLAN'а. Другими словами, никакой информации о принадлежности трафика определённому VLAN'у в нём нет.

Однако, если через порт может прийти трафик разных VLAN'ов, коммутатор должен его как-то различать. Для этого каждый кадр (frame) трафика должен быть помечен каким-то особым образом. Пометка должна говорить о том, какому VLAN'у трафик принадлежит. Без тега коммутатор не сможет различать трафик различных VLAN.

Наиболее распространённый сейчас способ ставить такую пометку описан в открытом стандарте IEEE 802.1Q.

При использовании стандарта Ethernet II 802.1Q вставляет тег перед полем "Тип протокола". Так как кадр изменился, пересчитывается контрольная сумма.

Исходный кадр

Адрес получателя	Адрес отправителя	Тип протокола	Данные	Контрольная сумма

Тегированный кадр

Адрес получателя	Адрес отправителя	Тег	Тип протокола	Данные	Новая контрольная сумма

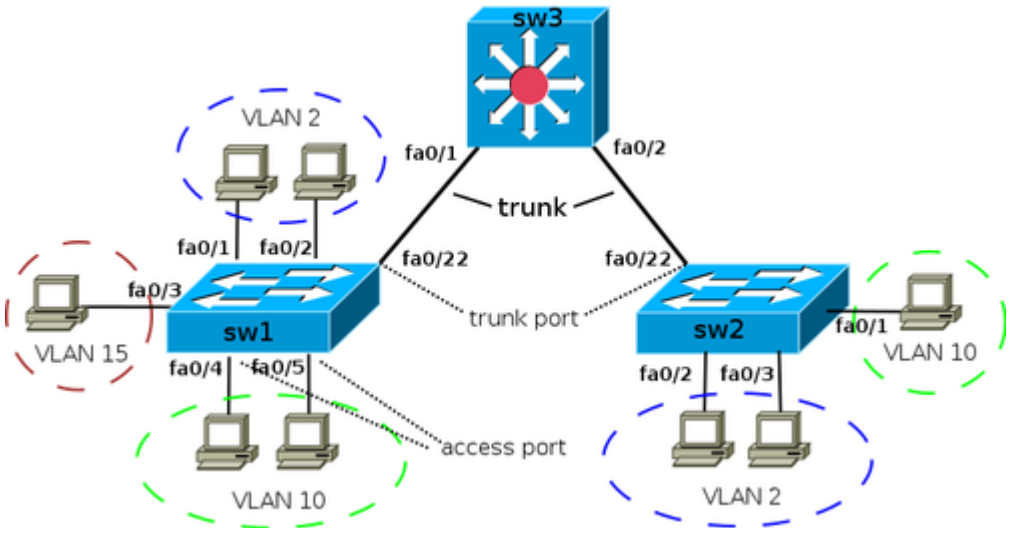
Когда порт должен уметь принимать или отдавать трафик из разных VLAN, то он должен находиться в тегированном или транковом состоянии. Понятия транкового порта и тегированного порта одинаковые. Транковый или тегированный порт может передавать как отдельно указанные VLAN, так и все VLAN по умолчанию, если не указано другое. Если порт нетегирован, то он может передавать только один VLAN (native - родной). Если на порту не указано, в каком он VLAN, то подразумевается, что он в нетегированном состоянии в первом VLAN (VID 1).

Терминология Cisco:

- access port – порт, принадлежащий одному VLAN'у и передающий нетегированный трафик.
- trunk port – порт, передающий тегированный трафик одного или нескольких VLAN'ов.

- **Настройка VLAN на оборудовании Cisco**

- Схема для примера представлена на рис. 1.



- Рис. 1. Схема сети с VLAN

Создание VLAN'а с идентификатором 2 и задание имени test для него:

```
sw1(config)# vlan 2
sw1(config-vlan)# name test
```

Удаление VLAN'а с идентификатором 2:

```
sw1(config)# no vlan 2
```

Настройка access портов

Назначение порта коммутатора в VLAN:

```
sw1(config)# interface fa0/1
sw1(config-if)# switchport mode access
sw1(config-if)# switchport access vlan 2
```

Назначение диапазона портов с fa0/4 до fa0/5 в vlan 10:

```
sw1(config)# interface range fa0/4 - 5
sw1(config-if-range)# switchport mode access
sw1(config-if-range)# switchport access vlan 10
```

Просмотр информации о VLAN'ах:

```
sw1# show vlan brief
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/6, Fa0/7, Fa0/8, Fa0/9,
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13,
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17,
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21,
                                                Fa0/22, Fa0/23, Fa0/24
2    test                             active    Fa0/1, Fa0/2
10   VLAN0010                         active    Fa0/4, Fa0/5
15   VLAN0015                         active    Fa0/3
```

Настройка транка (trunk)

Для того чтобы передать через порт трафик нескольких VLAN, порт переводится в режим транка.

Режимы интерфейса (режим по умолчанию зависит от модели коммутатора):

- **auto** – Порт находится в автоматическом режиме и будет переведён в состояние trunk, только если порт на другом конце находится в режиме on или desirable. Т.е. если порты на обоих концах находятся в режиме "auto", то trunk применяться не будет.
- **desirable** – Порт находится в режиме "готов перейти в состояние trunk"; периодически передает DTP-кадры порту на другом конце, запрашивая удаленный порт перейти в состояние trunk (состояние trunk будет установлено, если порт на другом конце находится в режиме on, desirable, или auto).
- **trunk** – Порт постоянно находится в состоянии trunk, даже если порт на другом конце не поддерживает этот режим.
- **nonegotiate** – Порт готов перейти в режим trunk, но при этом не передает DTP-кадры порту на другом конце. Этот режим используется для предотвращения конфликтов с другим "не-cisco" оборудованием. В этом случае коммутатор на другом конце должен быть вручную настроен на использование trunk'а.

По умолчанию в транке разрешены все VLAN. Для того чтобы через соответствующий VLAN в транке передавались данные, как минимум, необходимо чтобы VLAN был активным. Активным VLAN становится тогда, когда он создан на коммутаторе и в нём есть хотя бы один порт в состоянии up/up.

VLAN можно создать на коммутаторе с помощью команды vlan. Кроме того, VLAN автоматически создается на коммутаторе в момент добавления в него интерфейсов в режиме access.

В схеме, которая используется для демонстрации настроек, на коммутаторах sw1 и sw2, нужные VLAN будут созданы в момент добавления access-портов в соответствующие VLAN:

```
sw1(config)# interface fa0/3
sw1(config-if)# switchport mode access
sw1(config-if)# switchport access vlan 15
% Access VLAN does not exist. Creating vlan 15
```

На коммутаторе sw3 access-портов нет. Поэтому необходимо явно создать все необходимые VLAN:

```
sw3(config)# vlan 2
sw3(config)# vlan 10
sw3(config)# vlan 15
```

Для автоматического создания VLAN на коммутаторах, может использоваться протокол VTP.

Настройка статического транка

Создание статического транка:

```
sw1(config)# interface fa0/22
sw1(config-if)# switchport mode trunk
```

На некоторых моделях коммутаторов (на которых поддерживается ISL) после попытки перевести интерфейс в режим статического транка, может появиться такая ошибка:

```
sw1(config-if)# switchport mode trunk
Command rejected: An interface whose trunk encapsulation is “Auto” can not be configured to “trunk” mode.
```

Это происходит из-за того, что динамическое определение инкапсуляции (ISL или 802.1Q) работает только с динамическими режимами транка. И для того, чтобы настроить статический транк, необходимо инкапсуляцию также настроить статически.

Для таких коммутаторов необходимо явно указать тип инкапсуляции для интерфейса:

```
sw1(config-if)# switchport trunk encapsulation dot1q
```

И после этого снова повторить команду настройки статического транка (switchport mode trunk).

Динамическое создание транков (DTP)

Dynamic Trunk Protocol (DTP) – протокол Cisco, который позволяет коммутаторам динамически распознавать, настроен ли соседний коммутатор для поднятия транка и какой протокол использовать (802.1Q или ISL). Включен по умолчанию.

Режимы DTP на интерфейсе:

- **auto** – Порт находится в автоматическом режиме и будет переведён в состояние trunk, только если порт на другом конце находится в режиме on или desirable. Т.е. если порты на обоих концах находятся в режиме "auto", то trunk применяться не будет.
- **desirable** – Порт находится в режиме "готов перейти в состояние trunk"; периодически передает DTP-кадры порту на другом конце, запрашивая удаленный порт перейти в состояние trunk (состояние trunk будет установлено, если порт на другом конце находится в режиме on, desirable, или auto).
- **nonegotiate** – Порт готов перейти в режим trunk, но при этом не передает DTP-кадры порту на другом конце. Этот режим используется для предотвращения конфликтов с другим "не-cisco" оборудованием. В этом случае коммутатор на другом конце должен быть вручную настроен на использование trunk'a.

Перевести интерфейс в режим auto:

```
sw1(config-if)# switchport mode dynamic auto
```

Перевести интерфейс в режим desirable:

```
sw1(config-if)# switchport mode dynamic desirable
```

Перевести интерфейс в режим nonegotiate:

```
sw1(config-if)# switchport nonegotiate
```

Разрешённые VLAN'ы

По умолчанию в транке разрешены все VLAN. Можно ограничить перечень VLAN, которые могут передаваться через конкретный транк.

Указать перечень разрешенных VLAN для транкового порта fa0/22:

```
sw1(config)# interface fa0/22
sw1(config-if)# switchport trunk allowed vlan 1-2,10,15
```

Добавление разрешенного VLAN с номером 160:

```
sw1(config)# interface fa0/22
sw1(config-if)# switchport trunk allowed vlan add 160
```

Удаление VLAN 160 из списка разрешенных:

```
sw1(config)# interface fa0/22
sw1(config-if)# switchport trunk allowed vlan remove 160
```

Native VLAN

В стандарте 802.1Q существует понятие native VLAN. Трафик этого VLAN передается нетегированным. По умолчанию это VLAN 1. Однако можно изменить это и указать другой VLAN как native.

Настройка VLAN 5 как native:

```
sw1(config-if)# switchport trunk native vlan 5
```

Теперь весь трафик, принадлежащий VLAN'у 5, будет передаваться через транковый интерфейс нетегированным, а весь пришедший на транковый интерфейс нетегированный трафик будет промаркирован как принадлежащий VLAN'у 5 (по умолчанию VLAN 1).

Просмотр информации

Просмотр информации о транке:

```
sw1# show interface trunk

Port        Mode    Encapsulation   Status      Native vlan
Fa0/22        on        802.1q        trunking       1

Port        Vlans allowed on trunk
Fa0/22        1-2,10,15

Port        Vlans allowed and active in management domain
Fa0/22        1-2,10,15

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/22        1-2,10,15
```

Просмотр информации о VLAN'ах:

```
sw1# show vlan brief
VLAN Name                       Status    Ports
---- -------------------------- --------- -------------------------------
1    default                    active    Fa0/6, Fa0/7, Fa0/8, Fa0/9,
                                          Fa0/10, Fa0/11, Fa0/12, Fa0/13,
                                          Fa0/14, Fa0/15, Fa0/16, Fa0/17,
                                          Fa0/18, Fa0/19, Fa0/20, Fa0/21,
                                          Fa0/22, Fa0/23, Fa0/24
2    test                       active    Fa0/1, Fa0/2
10   VLAN0010                   active    Fa0/4, Fa0/5
15   VLAN0015                   active    Fa0/3
```

Диапазоны VLAN

VLANs	Диапазон	Использование
0, 4095	Reserved	Только для системного использования.
1	Normal	VLAN по умолчанию. Можно использовать, но нельзя удалить.
2-1001	Normal	Для VLAN’ов Ethernet. Можно создавать, удалять и использовать.
1002-1005	Normal	Для FDDI и Token Ring. Нельзя удалить.
1006-4094	Extended	Только для VLAN’ов Ethernet.

Практическая часть

Ход работы

1. Зарисовать схему сети согласно варианту.
2. Определить адрес подсети каждого VLAN, какие хосты входят в них, заполнить таблицу.

VLAN	Подсеть	PC, входящие в VLAN
VLAN *V*	10.X.V.0	PC 1, PC 2 и т.д. (например)
…	…	…

X – номер варианта;
V – номер VLAN.

3. Определить IP-адрес для каждого хоста, заполнить таблицу.

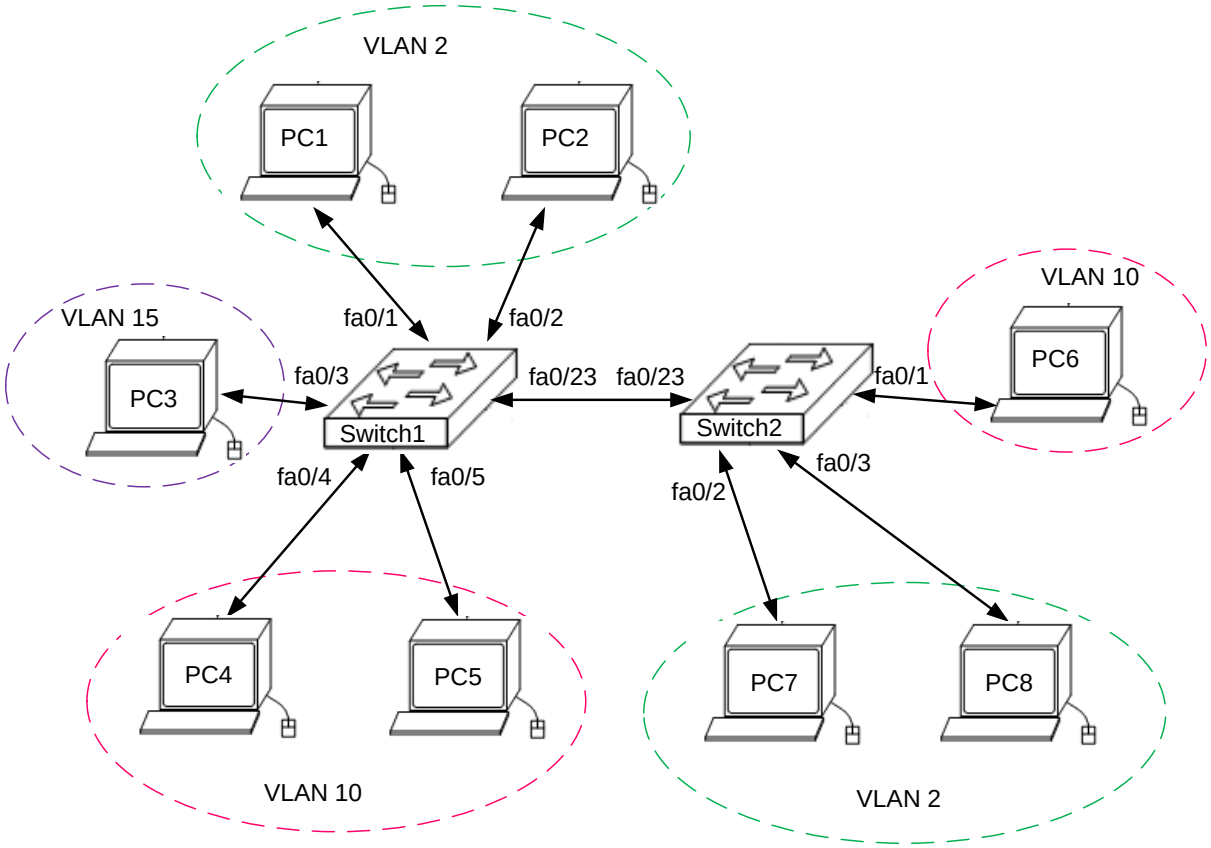
PC	IP-адрес
PC H	10.X.V.H
…	…

H – номер узла (PC).

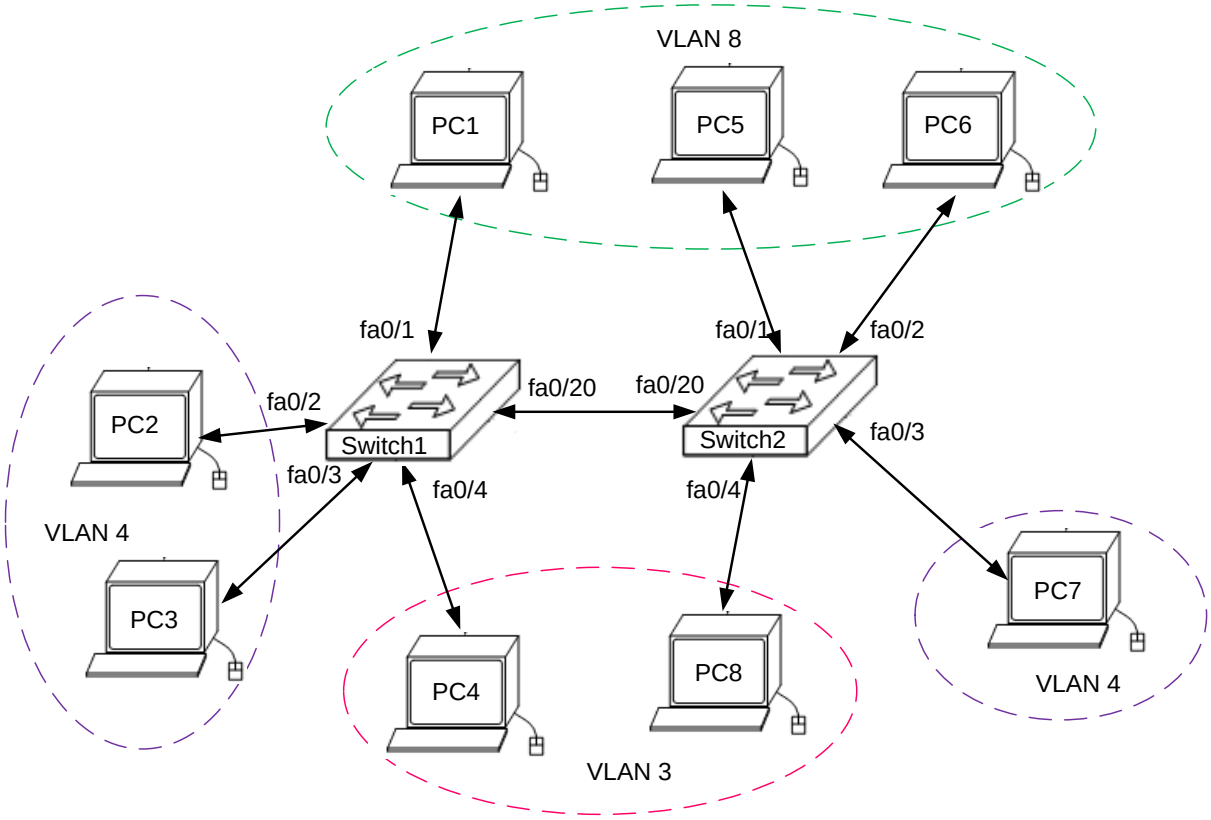
4. Назначить IP-адреса компьютерам на сети.
5. Настроить конфигурацию VLAN на коммутаторах (свитчах) – 5.1.-5.4. Записать используемые для конфигурации команды и реакцию системы, если таковая была.
5.1. Настроить access-порты и назначить их в VLAN согласно заданию и схеме:
5.1.2. Проверить командой ping доступность между PC в одном VLAN в одном сегменте любого коммутатора. Убедиться, что PC в одном VLAN и в разных сегментах друг друга не видят.
5.2. Настроить транковые порты:
5.2.1. Настроить динамический trunk между коммутаторами Switch1 и Switch2.
5.2.2. Убедиться в том, что теперь PC в одном VLAN и в разных сегментах могут пинговать друг друга.
5.2.3. Проверить, что на коммутаторах Switch1 и Switch2 есть все необходимые VLAN, что все они в состоянии active и есть в соответствующем транке.
5.3. Ограничение перечня разрешённых VLAN:
5.3.1. Запретить в транке одного из коммутаторов передачу одного из VLAN, существующих в разных сегментах сети.
5.3.2. Посмотреть, что изменилось в соответствующем транке.
5.3.3. Убедиться, что при этом PC в этом VLAN и в разных сегментах не могут друг друга пинговать.
5.3.4. Вывести информацию о существующем транке.
5.4. Добавление VLAN в перечень разрешённых:
5.4.1. Вернуть VLAN в перечень разрешенных для этого транка.
5.4.2. Проверить, что на коммутаторах Switch1 и Switch2 восстановились предыдущие состояния VLAN в соответствующем транке.

Схемы для лабораторной работы

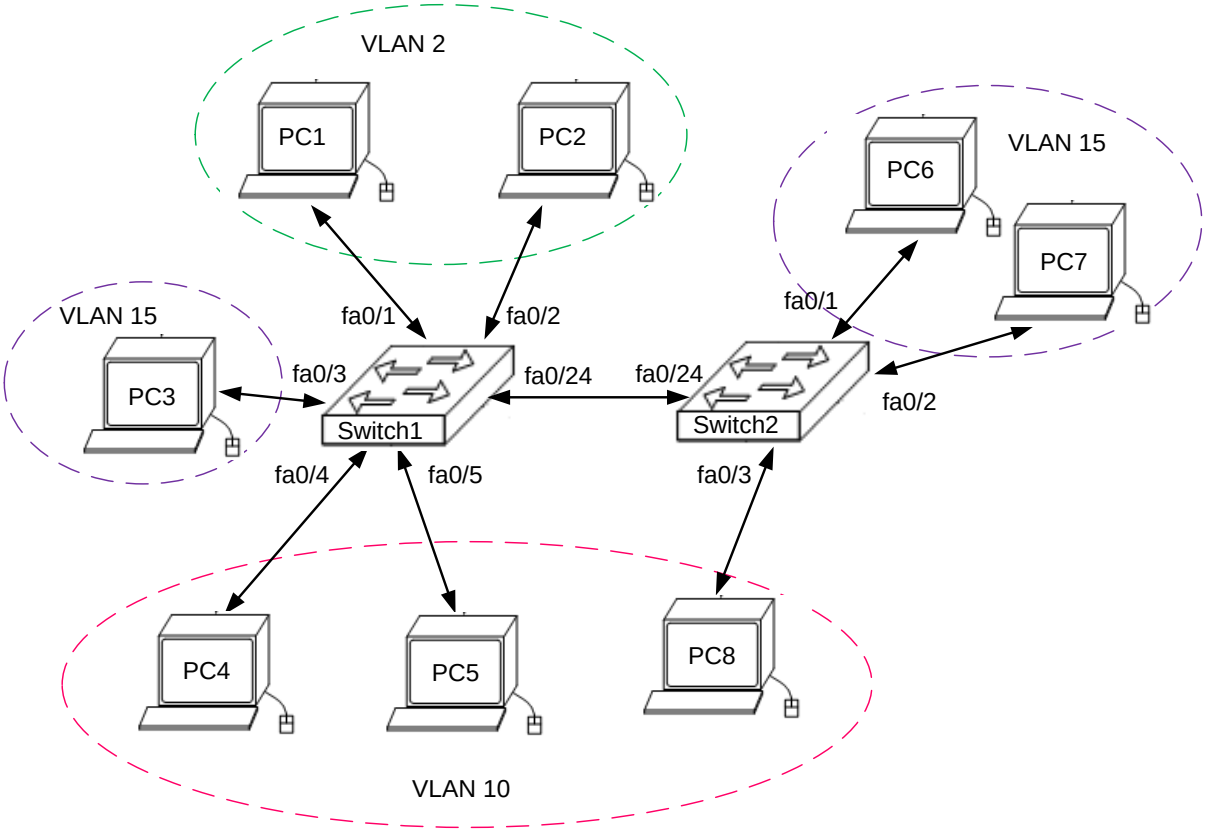
1. Для вариантов 1, 5, 9, 13, 17, 21, 25 и т.д.



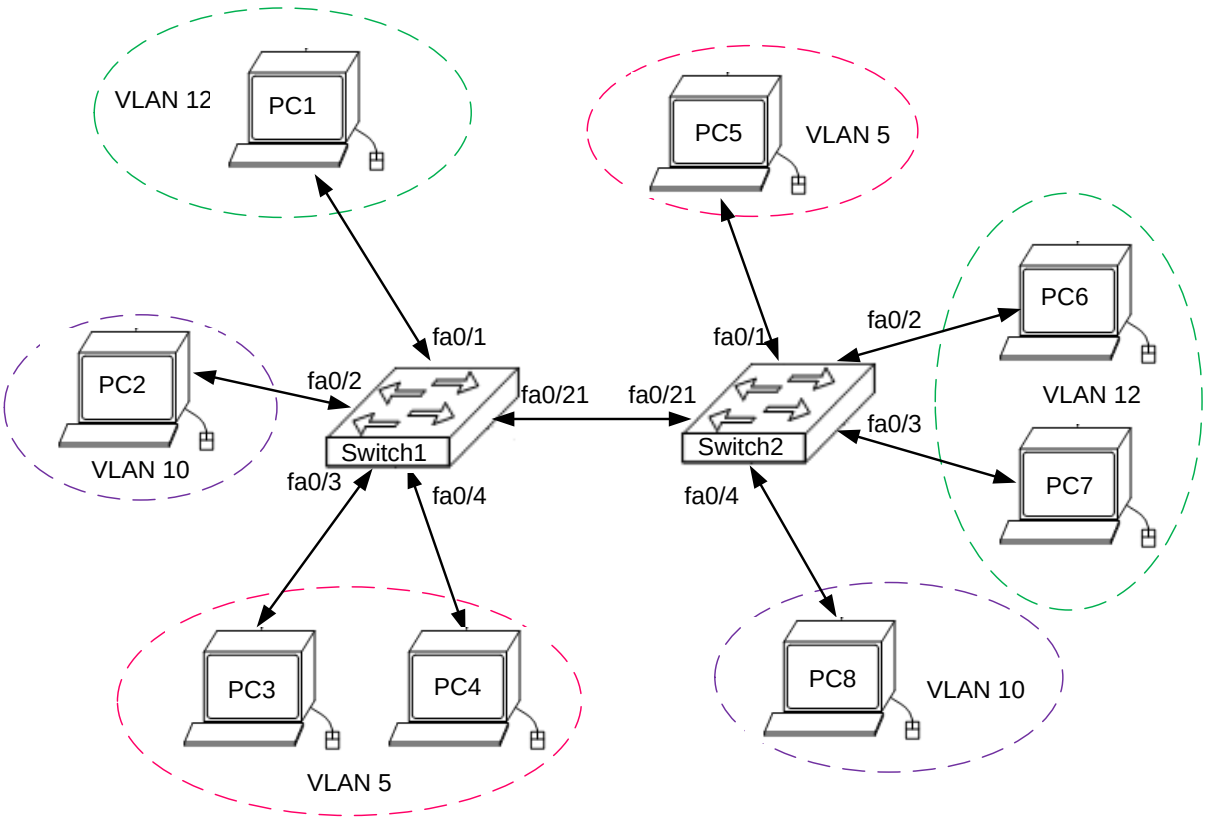
2. Для вариантов 2, 6, 10, 14, 18, 22, 26 и т.д.



3. Для вариантов 3, 7, 11, 15, 19, 23, 27 и т.д.



4. Для вариантов 4, 8, 12, 16, 20, 24, 28 и т.д.



Контрольные вопросы

1. Назовите причины использования VLAN.
2. В чём разница между тегированным и нетегированным трафиком?
3. Сколько бит содержит VID?
4. Какие устройства подключает access-порт?
5. Как называется порт, передающий трафик нескольких VLAN?
6. Какой командой можно посмотреть информацию о настроенных VLAN?
7. Какой командой можно запретить передачу трафика VLAN 70 через транковый порт?
8. Какой командой можно посмотреть информацию о настроенных транковых портах?
9. Будут ли пинговаться устройства одной VLAN, подключенные к разным коммутаторам, между которыми не назначен транковый порт?