VLAN (Virtual Local Area Network)

Описание

VLAN (Virtual Local Area Network) - основа понимания сетей для инженера. Рассказываем, что такое ВЛАН и для чего он нужен

Оглавление

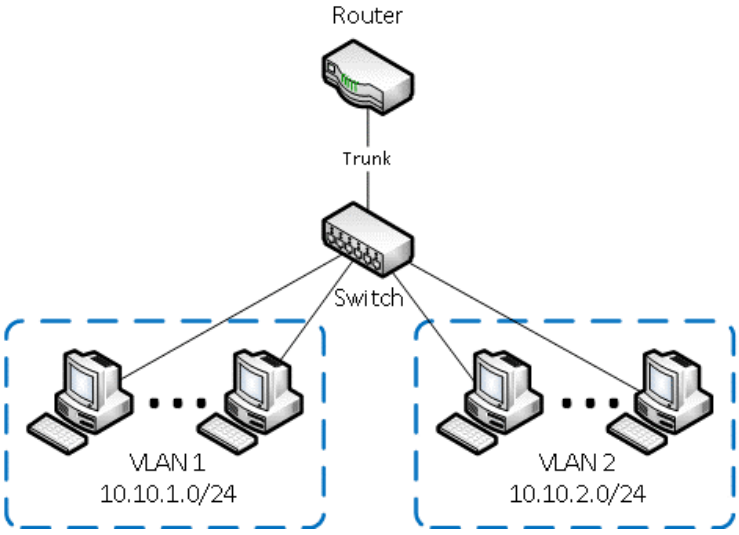
1. Учим основы - что такое VLAN?

Развитие компьютерных сетей проходит ошеломляющими темпами. Обилие устройств в компьютерных сетях порождает ряд проблем, таких, например, как необходимость объединять в отдельные изолированные подсети машины, которые подключены к различным коммутаторам. Иными словами, развитие сетей породило необходимость создания так называемых виртуальных локальных сетей, или VLAN.

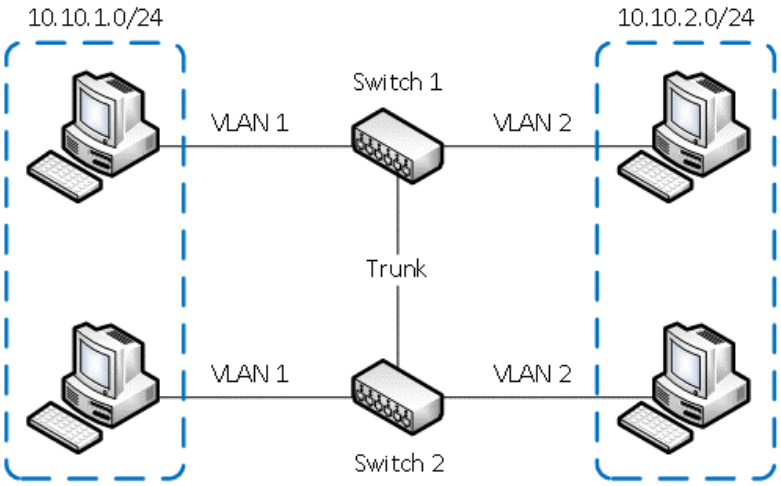
Что же такое виртуальная компьютерная сеть? VLAN дословно расшифровывается как Virtual Local Area Network, или виртуальная локальная сеть. По факту – это функция устройств связи, например, коммутаторов или маршрутизаторов, которая позволяет объединять устройства в одну или несколько виртуальных локальных подсетей в рамках одного физического сетевого интерфейса, такого как Wi-fi или Ethernet. Стоит отметить, что виртуальная логическая топология сети никак не пересекается с физической топологией и, соответственно, не зависит от нее.

НЕСКОЛЬКО ПРИМЕРОВ ИСПОЛЬЗОВАНИЯ ВИРТУАЛЬНОЙ ЛОКАЛЬНОЙ СЕТИ

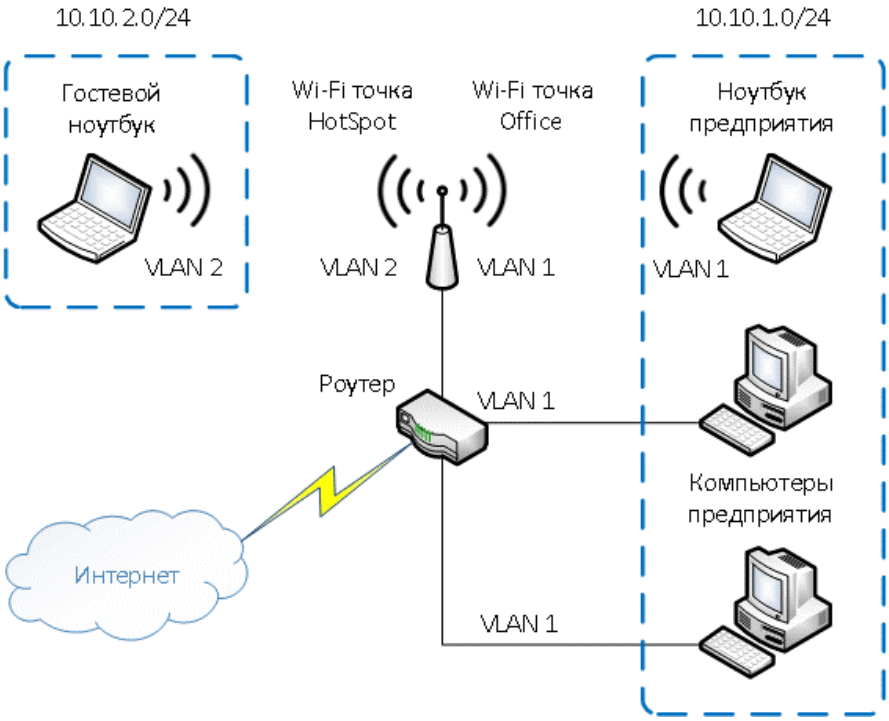
- **Создание отдельных подсетей для групп устройств, подключенных к одному и тому же коммутатору:**
  Если к одному коммутатору или маршрутизатору подключены несколько компьютеров в рамках одного офиса, то их можно разделить на отдельные подсети. Это актуально для малых предприятий, таких как, например, небольшая компания по разработке компьютерных игр. В этом случае будет рациональным объединить в отдельные подсети рабочие станции художников и программистов, поскольку обмен данными между сотрудниками одного отдела в рамках работы будет более эффективным. Специалисты каждого отдела будут видеть компьютеры только своей подгруппы, а руководители отделов, в свою очередь, будут объединены в свою сеть или подсеть, стоящую выше по сетевой иерархии.



- **Создание виртуальной сети для устройств, подключенных к разным коммутаторам:**
  Допустим, во взятой нами за пример компании по разработке компьютерных игр произошло расширение штата – наняли нескольких новых работников – программистов и художников. Их разместили в соседнем кабинете, и, соответственно, выделили им для работы свой коммутатор. В данном случае можно также создать виртуальные сети для отделов организации, в которых появились новые рабочие станции, даже если они физически подключены к другому коммутатору. В этом случае работники разных отделов не будут видеть в сети компьютеры сторонней группы, даже если они физически находятся в одном кабинете.



- **Распределение Wi-fi сети для различных групп пользователей:**
  Пусть в нашей организации стоит роутер, который физически имеет одну точку доступа Wi-fi. VLAN позволяет создать несколько виртуальных точек Wi-fi для разных отделов, в том числе отдельную гостевую точку доступа. Это удобно для руководства предприятия, так как позволяет проконтролировать расход трафика и выяснить, например, что программист Вася, вместо того чтобы писать код, смотрит в соцсетях фото с котиками. Да и для безопасности это также полезно – например, устройства подключаемые через гостевую точку доступа, не будут видеть рабочие компьютеры организации.



ЗАКЛЮЧЕНИЕ

Таким образом, к достоинствам VLAN можно отнести:

- Меньшее количество используемых для создания внутренней сети организации проводов (и меньше головной боли для сетевого администратора);
- Более безопасную и контролируемую связь между устройствами – рабочие станции в рамках одной подсети не будут «видеть» устройства из других подсетей;
- Более эффективное использование трафика в различных подсетях общей сети, за счет возможности управления трафиком в различных подгруппах;
- Повышение эффективности работы отделов через создание новых подгрупп устройств, для чего VLAN предоставляет широчайшие возможности;

2. Настройка VLAN на Cisco – кейсы и история

Давайте окунемся в историю. Начиная с конца 1990-х, все коммутаторы **Cisco** поддерживали проприетарный протокол, который помогал инженерам настраивать одинаковые VLAN-ы на нескольких коммутаторах одновременно, и этот протокол назывался Virtual Trunking Protocol (VTP). Мы не будем погружаться в детали работы VTP, но коснемся того, как различные режимы работы VTP влияют на коммутаторы и настройку VLAN-ов.

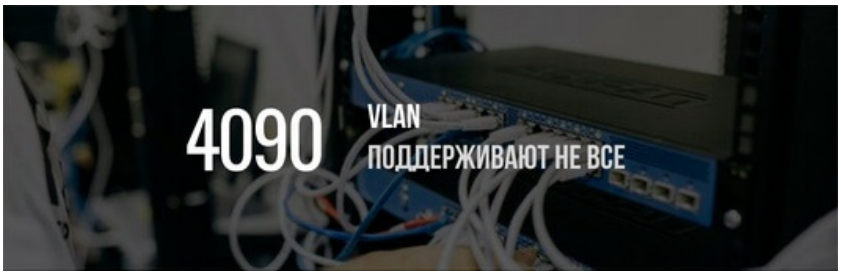
> VLAN (Virtual Local Area Network) – виртуальная локальная сеть, помогает создавать новые бродкастные домены, увеличивает сегментацию и безопасность сети.

Изначально, Cisco поддерживала другой транковый протокол – **Cisco Inter – Switch Link (ISL)**. Так как данный протокол поддерживал только создание VLAN-ов в диапазоне 1-1005, ранние версии VTP также поддерживали только данные VLAN-ы. Это означает, что если вы используете VTP версии 1 или 2 (по умолчанию), у вас будут доступны только VLAN-ы с 1 по 1001 (1002 – 1005 всегда зарезервированы).

Катализатором изменений во многом являлся новый стандарт **IEEE 802.1Q**, а именно, произошло увеличение количества поддерживаемых VLAN-ов до 4 094 штук – за исключением зарезервированных. Такая новость очень пришлась по вкусу инженерам, так как в большой сети возросшее количество VLAN-ов очень помогло в отношении гибкости и удобства. Но при этом третья версия VTP появилась только в 2009 году, поэтому многие привыкли настраивать сеть без использования VTP.

Как это влияет на настройку VLAN-ов, спросите вы? Все коммутаторы Cisco поддерживают стандарт IEEE 802.1Q (некоторые так вообще поддерживают только его), некоторые свитчи поставляются с включенным VTP сервером, что означает, что из коробки они поддерживают только тысячу с небольшим VLAN-ов. Чтобы получить доступ ко всему диапазону VLAN-ов, необходимо настроить VTP версии 3, затем поставить его в прозрачный режим, либо просто выключить VTP целиком.

> Не все коммутаторы Cisco поддерживают 4 090 VLAN-ов. Это ограничение оборудования, как такового.



КОМАНДЫ ДЛЯ НАСТРОЙКИ VLAN

Ниже указаны основные необходимые для создания VLAN-а команды на коммутаторе:

1. **conf t** - вход в режим конфигурации коммутатора;
2. **vlan %номер vlan-a%** - создаие VLAN-а, нужно указать номер;
3. **name %имя vlan-a%** - также VLAN-у можно присвоить имя;

> VLAN не будет создан, пока вы не выйдете из режима настройки VLAN-а.

Однако, существует еще один способ создания VLAN-а – с помощью назначения интерфейса в VLAN.

1. **conf t** - вход в режим конфигурации коммутатора;
2. **interface %номер интерфейса%** - вход в конкретный интерфейс;
3. **switchport access vlan %номер vlan-a%** - присваиваем VLAN интерфейсу, если VLAN не существовал, он будет автоматически создан;

Как удалить VLAN? Об этом ниже:

1. **conf t** - вход в режим конфигурации коммутатора
2. **no vlan %номер vlan-a%** - удаление VLAN-а

Для проверки созданных VLAN-ов, используйте следующие команды:

```
show vlan
show vlan brief
```

Так как VTP по умолчанию настроен в режиме сервера на большинстве коммутаторов, создание VLAN-ов за пределами стандартного диапазона приведут к неудаче (способами, описанными выше). Ошибка вылетит только при выходе из режима конфигурации VLAN-а. Чтобы исправить данную проблему, необходимо переключить версию VTP на третью, или же режим VTP должен быть переключен на **transparent** или полностью выключен. Ниже показаны команды для изменения режима работы VTP.

1. **conf t** - вход в режим конфигурации коммутатора;
2. **vtp mode {server / client / transparent / off}** - настройка режима VTP, для использования расширенного диапазона VLAN-ов, вам нужны transparent или off;

МАЛЕНЬКАЯ КОМПАНИЯ ПЕРЕЕЗЖАЕТ В НОВЫЙ ОФИС?

Теперь приведем пример настройки коммутатора согласно следующему сценарию: организация переезжает в новое здание, причем отдел продаж и отдел разработки будут находиться на одном этаже.
В целях экономии средств и времени, было решено, что все устройства будут подключены через единственный коммутатор. Так как у двух вышеупомянутых отделов должны быть разные права доступа, их необходимо виртуально разделить между собой.

У продавцов будет **VLAN 10**, и все программисты будут находиться в **VLAN 20**. На коммутаторе все рабочие станции продавцов будут подключены к портам Fast Ethernet 0/1 – 0/12, а у программистов к портам 0/13 – 0/24.

Для этого нам необходимо будет настроить каждый интерфейс в соответствии с нужным VLAN-ом. Для этого мы будет использовать команду `interface range`.
Итак, внимание на команды:

1. **conf t** - вход в режим конфигурации коммутатора;
2. **vlan 10** - создаем VLAN для команды продавцов;
3. **vlan 20** - создаем VLAN 20 для команды программистов. Обратите внимание, что даже команда сработала, несмотря на то, что вы были в режиме конфигурации VLAN-а, как будто это был глобальный режим конфигурации;
4. **interface range fastethernet0/1-12** - проваливаемся в режим конфигурации интерфейсов 1 – 12;
5. **switchport access vlan 10** - настраиваем интерфейсы для работы в VLAN 10;
6. **interface range fastethernet0/13-24** - проваливаемся в режим конфигурации интерфейсов 13 – 24;
7. **switchport access vlan 20** - настраиваем интерфейсы для работы в VLAN 20;
8. **do wr** - сохраняем конфиг;

Как только вы поймете основы создания VLAN-ов, вы увидите, что это совсем несложно.
Основными подводными камнями являются различные режимы коммутации, но об этом мы расскажем в следующих статьях.

3. Полное руководство по настройке VLAN

Создание **VLAN**-ов, как и все другие конфигурации на сетевом оборудование, достигается путем ввода соответствующих команд. В этой статье рассматриваются настройка разных типов VLAN на коммутаторах **Cisco**.

Диапазоны VLAN на коммутаторах Catalyst

В зависимости от модели, коммутаторы **Cisco** поддерживает разное число VLAN. Числа поддерживаемых VLAN обычно вполне достаточно для задач большинства компаний. Например, коммутаторы Cisco Catalyst 2960 и 3650 поддерживают больше 4000 виртуальных сетей. Нормальный диапазон VLAN начинается от 1 до 1005, а расширенный – от 1006 до 4094. На выводе внизу можно увидеть VLAN по умолчание на коммутаторе Cisco Catalyst 2960 с Cisco IOS 15 версии.

```
Switch# show vlan brief

VLAN Name              Status    Ports
---- ----------------- -------   --------------------
1    default           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                 Fa0/5, 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
                                 Gi0/1, Gi0/2
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

Нормальный диапазон VLAN

Ниже перечислены основные характеристики нормального диапазона:

- Они используются в малых, средних и больших сетях;
- Нумерация начинается от 1 до 1005;
- Идентификаторы с 1002 до 1005 зарезервированы для устаревших сетей (Token Ring, FDDI);
- Идентификаторы с 1002 до 1005 созданы автоматически и не могут быть удалены;
- Созданные VLAN хранятся в памяти коммутатора в файле базы данных VLAN, именуемого vlan.dat;
- VTP, если настроен, помогает распространять все VLAN между коммутаторами.

Расширенный диапазон

Ниже перечислены основные характеристики расширенного VLAN:

- Используется провайдерами и очень большими компаниями;

- Нумерация начинается с 1006 по 4094;
- По умолчанию, они хранятся в running-config;
- Имеют меньшую функциональность, чем нормальные VLAN;
- Для настройки расширенного VLAN VTP должен работать в режиме transparent.

Примечание: Ограничение количества доступных VLAN продиктовано особенностями заголовка 802.1Q. Полю VLAN ID заголовка 802.1Q IEEE выделено всего 12 бит, поэтому 4096 -- верхняя граница доступных VLAN на коммутаторах Catalyst. А если нужно больше, то можно обратиться к такой технологии как VXLAN.

Команды для создания VLAN

Когда создается VLAN нормального диапазона, как уже было отмечено, эти настройки хранятся в файле `vlan.dat`, то есть не нужно вводить команды `copy running-config startup-config` или `write memory`. Тем не менее, чтобы не потерять изменения сделанные наряду с созданием VLAN, рекомендуется сохранять текущую конфигурацию.

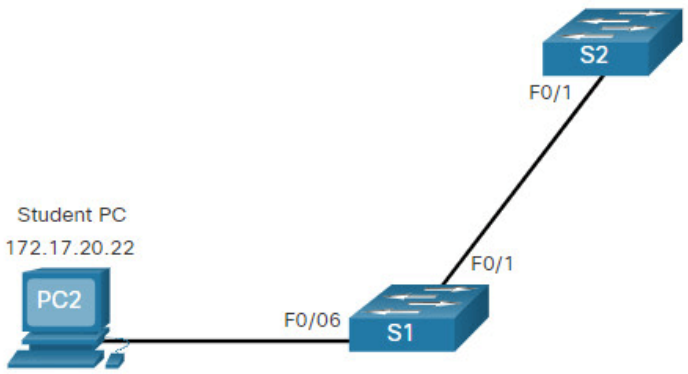
В таблице ниже перечислены команды, которые нужно вводит для создания VLAN и присвоения им названия. Хорошей практикой считается давать VLAN понятные названия, чтобы облегчить поиск и устранение проблем в будущем.

Задача	**IOS команда**
Войти в режим глобальной конфигурации	Switch# configure terminal
Создать VLAN с валидным ID	Switch(config)# vlan vlan-id
Указать уникальное имя для идентификации VLAN	Switch(config-vlan)# name vlan-name
Вернуться в привилегированный режим EXEC	Switch(config-vlan)# end

---

Пример создания VLAN

В топологии ниже, порт к которому подключен ПК Stundent, еще не добавлен ни в один VLAN, но у него есть IP 172.17.20.22, который принадлежит VLAN 20.



Пример ниже демонстрирует настройку VLAN 20 с названием student на коммутаторе S1.

```
S1# configure terminal
S1(config)# vlan 20
S1(config-vlan)# name student
S1(config-vlan)# end
```

Примечание: Кроме создание VLAN-ов по одному, так же есть возможность создания нескольких влан, вводя их идентификаторы через запятые или дефис. Например, команда vlan 100,102,105-107 в режиме конфигурации создаст сразу 5 VLAN-ов с идентификаторами 100, 102, 105, 106, и 107

Добавление портов в VLAN

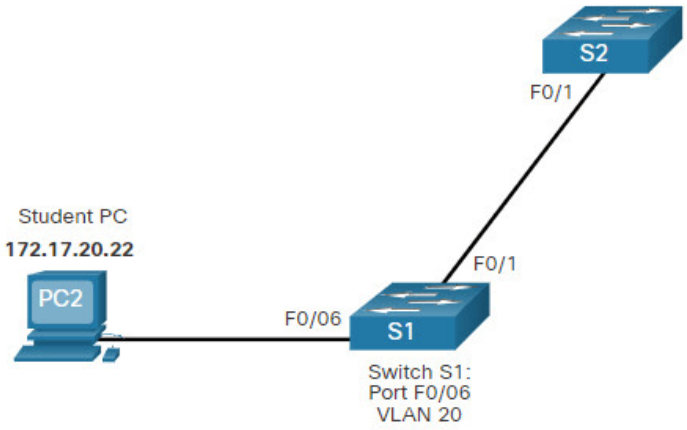
После создания VLAN, следующий шаг – это добавление нужных портов в конкретный VLAN.

В таблице ниже приведены команды для переведения порта в режим **access** и добавления в конкретный VLAN. Команда `switchport mode access` опциональна, но в целях безопасности рекомендуется вводить ее, так как она принудительно переводит порт в режим **access**, что помогает защищаться от атак вроде VLAN Hopping.

Задача	**IOS команда**
Войти в режим глобальной конфигурации	Switch# configure terminal
Войти в режим конфигурации интерфейса	Switch(config)# interface interface-id
Установить порт в режим access	Switch(config-if)# switchport mode access
Присвоить порт VLAN'у.	Switch(config-if)# switchport access vlan vlan-id
Вернуться в привилегированный режим EXEC	Switch(config-if)# end
Примечание: Для одновременной конфигурации нескольких портов можно воспользоваться командой **interface range**.	

Пример присвоения порту VLAN

В топологии ниже порт F0/6 коммутатора S1 настроен в режиме access и добавлен в VLAN 20. Теперь любое устройство, подключенное к данному порту, будет в 20-ом VLAN-е, как и ПК2 в нашем случае.



А ниже приведен пример команд для реализации вышеуказанной цели.

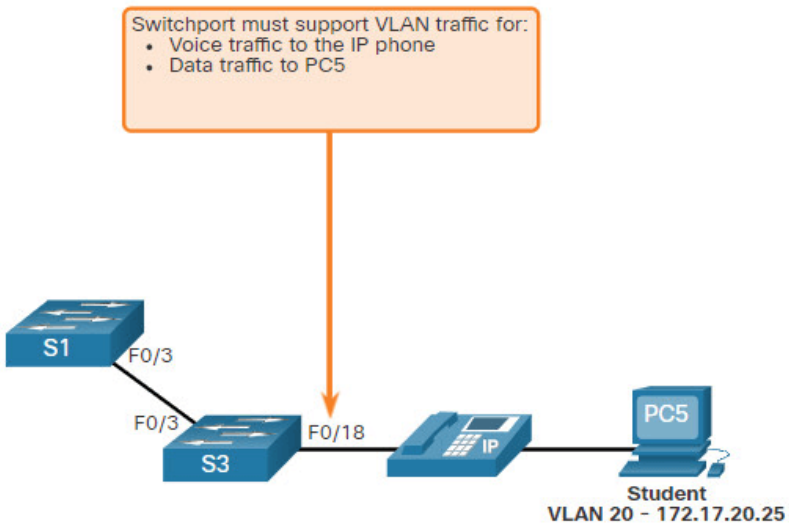
```
S1# configure terminal
S1(config)# interface fa0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# end
```

VLAN настраивается на порту коммутатора, а не на конечном устройстве. ПК2 присвоен IP адреси маска подсети, которая относиться к VLAN 20, а последний указан на порту коммутатора. Если VLAN 20 настроить на другом коммутаторе, администратор сети должен настроить другой компьютер так, чтобы он был в одной подсети с ПК2 (172.17.20.0/24).

VLAN данных и голосовой VLAN

На порту коммутатора в режиме access можно настроить не более одного VLAN-а данных. Тем не менее, на том же порту можно настроить голосовой VLAN. Например, порт к которому подключены IP телефон и конечное устройство, может быть сразу в двух VLAN-ах, - голосовом и VLAN-е данных.

Например, в топологии ниже, ПК5 подключен к IP телефону, который в свою очередь подключен к порту F0/18 коммутатора S3. Для реализации данной идеи созданы VLAN данных и голосовой VLAN.



Пример голосового VLAN и VLAN данных

Чтобы настроить на интерфейсе голосовой VLAN используется команда `switchport voice vlan [vlan-id]` в режиме конфигурации порта на коммутаторе.

В сетях, где поддерживается голосовой трафик, обычно настраиваются различные QoS. Голосовой трафик должен быть маркирован доверенным, как только попадет на интерфейс. Чтобы пометить голосовой трафик как доверенный, а так же указать какое поле пакета используется для классификации трафика, применяется команда `mls qos trust [cos | device cisco-phone | dscp | ip-precedence]` в режиме конфигурации интерфейса.

Конфигурация в примере ниже создаст два VLAN-а и присвоит порту F0/18 коммутатора S3 VLAN данных с идентификатором 20, а также голосовой VLAN 150 и включит QoS, на основе CoS.

```
S3(config)# vlan 20
S3(config-vlan)# name student
S3(config-vlan)# vlan 150
S3(config-vlan)# name VOICE
S3(config-vlan)# exit
S3(config)# interface fa0/18
S3(config-if)# switchport mode access
S3(config-if)# switchport access vlan 20
S3(config-if)# mls qos trust cos
S3(config-if)# switchport voice vlan 150
S3(config-if)# end
```

Если на коммутаторе еще не создан нужный VLAN команда `switchport access vlan` принудительно создаст его. Например, VLAN 30 не выводится при вводе команды `switchport vlan brief`. Но если ввести команду `switchport access vlan 30` без предварительного создания под любым интерфейсом на терминале выведется соответствующее сообщение:

```
% Access VLAN does not exist. Creating vlan 30
```

Проверка настроек VLAN

После настроек VLAN, правильность конфигурации можно проверить с помощью команды `show` с последующим ключевым словом.

Команда `show vlan` выводит список существующих VLAN. Данной команде можно задать разные параметры. Полный синтаксис команды такой: `show vlan [brief | id vlan-id | name vlan-name | summary]`.

В таблице описываются параметры команды `show vlan`.

Задача	**Опция команды**
Отображение имени, статуса и портов VLAN по одной VLAN на строку	brief

Отображение информации об определенном номере VLAN ID. Для vlan-id диапазон от 1 до 4094	id vlan-id
Отображение информации об определенном имени VLAN. Vlan-name - это строка ASCII от 1 до 32 символов.	name vlan-name
Отображение сводной информации о VLAN	summary

Команда `show vlan summary` выводит количество настроенных VLAN на коммутаторе:

```
S1# show vlan summary
Number of existing VLANs              : 7
Number of existing VTP VLANs          : 7
Number of existing extended VLANS     : 0
```

Есть и другие полезные команды вроде `show interfaces interface-id switchport` и `show interfaces vlan vlan-id`. Например, команда `show interfaces fa0/18 switchport` может использоваться для проверки правильно ли присвоен интерфейс F0/18 к голосовому VLAN и VLAN данных.

```
S1# show interfaces fa0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 20 (student)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: 150
Administrative private-vlan host-association: none
(Output omitted)
```

Переназначение VLAN на интерфейсе

Есть несколько вариантов переназначения интерфейсу VLAN-а.

Если неправильно сконфигурировали VLAN на интерфейсе, просто введите команду `switchport access vlan vlan-id` подставив нужный VLAN. Например, представим что порт F0/18 добавлен в VLAN по умолчанию VLAN 1. Чтобы поменять на VLAN 20, достаточно ввести switchport access vlan 20.

Чтобы вернуть обратно в VLAN по умолчанию в режиме конфигурации интерфейса введите команду `no switchport access vlan`.

На выводе ниже можно убедиться, что 18-ый порт коммутатора находится в VLAN по умолчанию.

```
S1(config)# interface fa0/18
S1(config-if)# no switchport access vlan
S1(config-if)# end
S1#
S1# show vlan brief
VLAN Name                 Status    Ports
---- ------------------ --------- -------------------------------
1    default            active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                   Fa0/5, 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
                                   Gi0/1, Gi0/2
20   student            active
1002 fddi-default       act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default    act/unsup
1005 trnet-default      act/unsup
Следует заметить, что 20-ый VLAN все еще активен, несмотря на то, что под ним нет никакого интерфейса.
Чтобы убедиться, что на 18-ый порт в VLAN 1, можно воспользоваться командой show interfaces f0/18 switchport:
S1# show interfaces fa0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
```

Удаление VLAN

Для удаления VLAN используется команда `no vlan vlan-id` в глобальном режиме конфигурации.

Внимание: Прежде чем удалить VLAN убедитесь, что все интерфейсам с данным VLAN назначен другой.

Чтобы удалить весь файл `vlan.dat` введите команду `delete flash:vlan.dat` в привилегированном режиме EXEC. После перезагрузки все настроенные на коммутаторе VLAN удалятся.

> Примечание: Чтобы сбросить коммутаторы Catalyst до заводских настроек отсоедините все кабели кроме кабеля питания и консольного кабеля, от коммутатора. Затем введите `erase startup-config` после него `delete vlan.dat`. После перезагрузки коммутатор сбросится до первоначальных настроек.

Настройка Trunk

После создания и настройки VLAN, пора перейти к конфигурации **Trunk** портов. Trunk это связь на втором уровне OSI между коммутаторами, который пропускает все VLAN (если список разрешенных VLAN явно не указан).

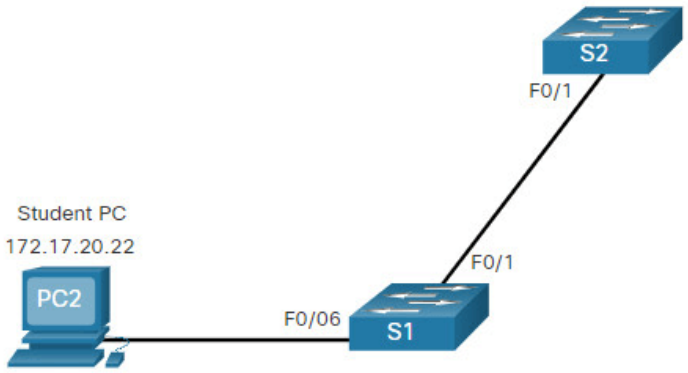
Для настройки интерфейса в режиме Trunk нужно воспользоваться команды, указанные ниже в таблице:

Задача	**IOS команда**
Войти в режим глобальной конфигурации	Switch# configure terminal
Войти в режим конфигурации интерфейса	Switch(config)# interface interface-id
Установите порт в режим постоянного транкинга	Switch(config-if)# switchport mode trunk
Устанавливает для native VLAN значение, отличное от VLAN 1	Switch(config-if)# switchport trunk native vlan vlan-id
Укажите список VLAN, разрешенных для транка	Switch(config-if)# switchport trunk allowed vlan vlan-list

Вернуться в привилегированный режим EXEC	Switch(config-if)# end

Пример настройки Trunk

В топологии ниже VLAN 10, 20 и 30 обслуживают компьютеры Faculty, Student и Guest. Порт F0/1 коммутатора S1 настроек в режиме Trunk и пропускает VLAN-ы 10, 20, 30. VLAN 99 настроен в качестве native (VLAN по умолчанию).



В данном примере показывается настройка порта в режиме trunk, смена VLAN по умолчанию и ограничение разрешенных VLAN.

```
S1(config)# interface fastEthernet 0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan 10,20,30,99
S1(config-if)# end
```

Примечание: В данном примере подразумевается, что используется коммутатор Cisco Catalyst 2960, в котором порты по умолчанию используют 802.1Q. На других коммутаторах может понадобиться ручная настройка режима энкапсуляции на интерфейсе. Так же следует настроить VLAN по умолчанию на обоих концах, иначе коммутатор будет выдавать ошибки.

Проверка настройки Trunk

Вывод ниже демонстрирует настройки интерфейса Fa0/1 коммутатора S1. Данный вывод получен с помощью команды `show interfaces interface-ID switchport`:

```
S1# show interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
(output omitted)
```

Подчеркнутые части показывают режим работы интерфейса и нативный VLAN.

Сброс trunk до настроек по умолчанию

Для сброса настроек транкового интерфейса используйте команды `no switchport trunk allowed vlan` и `no switchport trunk native vlan`. После сброса настроек данный порт будет пропускать все VLAN-ы и VLAN-ом по умолчанию будет VLAN 1.

```
S1(config)# interface fa0/1
S1(config-if)# no switchport trunk allowed vlan
S1(config-if)# no switchport trunk native vlan
S1(config-if)# end
```

Вывод команды `show interfaces f0/1 switchport` показывает, что порт сброшен до настроек по умолчанию:

```
S1# show interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
(output omitted)
```

В вывод ниже показывает команды, которые используются для смены режима работы интерфейс с **trunk** на **access**.

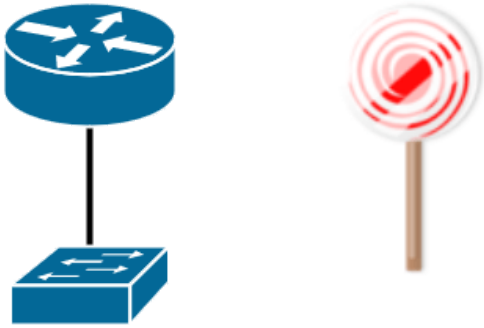
```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# end
S1# show interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
(output omitted)
```

4. Настройка Router-on-a-Stick на Cisco

Router-on-a-stick (роутер на палочке) - это термин, часто используемый для описания схемы, состоящей из маршрутизатора и коммутатора, которые соединены с использованием одного канала Ethernet, настроенного как **802.1Q** транк. Стандарт 802.1Q используется для тегирования трафика, для передачи информации о принадлежности к VLAN. В этой схеме на коммутаторе настроено несколько VLAN и маршрутизатор выполняет всю маршрутизацию между различными сетями или VLAN (**Inter-VLAN routing**).

Хотя некоторые считают, что термин «маршрутизатор на палочке» звучит немного глупо, это очень популярный термин, который широко используется в сетях, где нет коммутатора 3-го уровня.

Также такую схему иногда называют "леденец" – *lollypop*. Находите некоторое сходство?

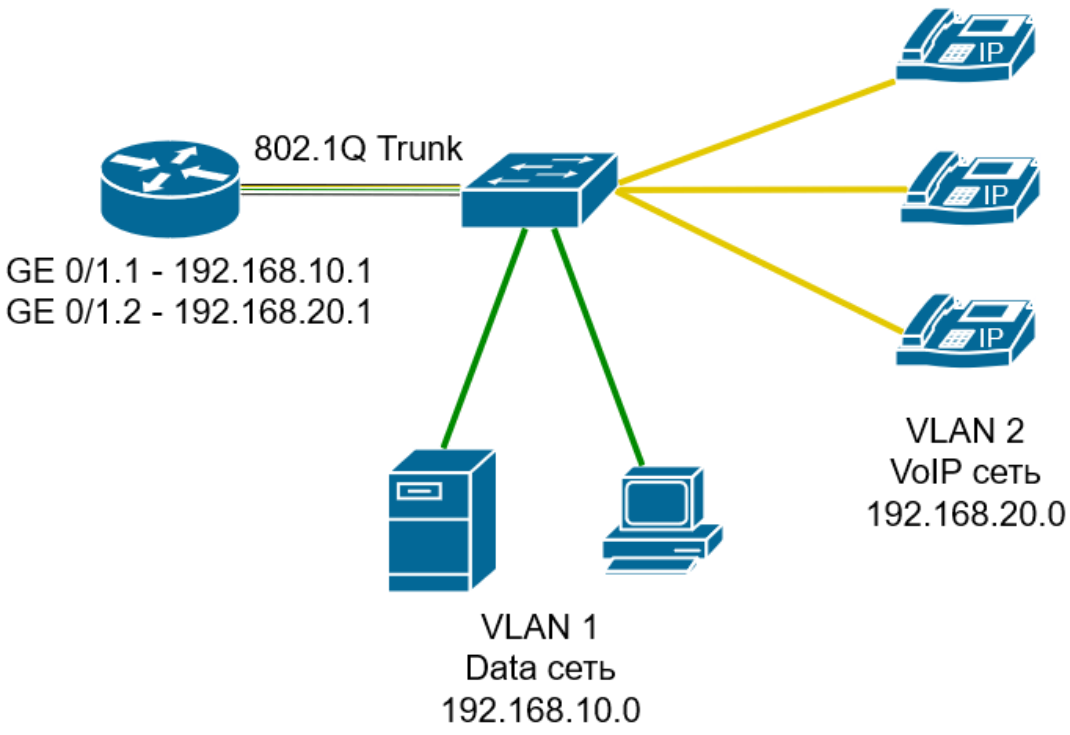


ПРИМЕР

Наш пример основан на сценарии, с которым вы, скорее всего, столкнетесь при работе с сетями **VoIP**. Поскольку реализации VoIP требуют разделения сети передачи данных и сети голоса для маршрутизации пакетов между ними, вам необходим либо коммутатор 3-го уровня, либо маршрутизатор. Эта конфигурация обеспечивает доступность и стабильность VoIP, особенно в часы пик трафика в вашей сети.

Пакеты, передающиеся между VLAN маршрутизируются через один роутер, подключенный к коммутатору, используя один физический порт, настроенный как транк на обоих концах (коммутатор и маршрутизатор).

Этот пример покажет вам, как настроить маршрутизатор и коммутатор **Cisco** для создания между ними 802.1Q транка и маршрутизации пакетов между вашими VLAN.



ШАГ 1 – НАСТРОЙКА КОММУТАТОРА

Первым шагом является создание необходимых двух VLAN на нашем коммутаторе Cisco и настройка их с IP-адресом. Поскольку все коммутаторы Cisco содержат VLAN1 (VLAN по умолчанию), нам нужно только создать VLAN2.

```
Switch# configure terminal
Switch(config)# vlan2
Switch(config-vlan)# name voice
Switch(config-vlan)# exit
Switch(config)# interface vlan1
Switch(config-if)# ip address 192.168.10.2 255.255.255.0
Switch(config-if)# exit
Switch(config)# interface vlan2
Switch(config-if)# ip address 192.168.20.2 255.255.255.0
Switch(config-if)# exit
```

Далее, нам нужно создать транк порт, который будет соединятся с маршрутизатором. Для этой цели мы выберем порт GigabitEthernet 0/1

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# spanning-tree portfast trunk
```

При помощи данных команд мы определили, что транк будет использовать инкапсуляцию 802.1Q, установили порт в режим транка и включили функцию **portfast trunk spanning-tree**, чтобы гарантировать, что порт будет пересылать пакеты немедленно при подключении к устройству, например, маршрутизатору. Внимание: команда spanning-tree portfast trunk не должна использоваться на портах, которые подключаются к другому коммутатору, чтобы избежать петель в сети.

ШАГ 2 – НАСТРОЙКА МАРШРУТИЗАТОРА

Мы закончили с коммутатором и можем переходить к настройке конфигурации нашего маршрутизатора, чтобы обеспечить связь с нашим коммутатором и позволить всему трафику VLAN проходить и маршрутизироваться по мере необходимости.

Создание транка на порте маршрутизатора не сильно отличается от процесса, описанного выше - хотя мы транк на одном физическом интерфейсе, мы должны создать под-интерфейс (**sub-interface**) для каждого VLAN.

```
Router# configure terminal
Router(config)# interface gigabitethernet0/1
Router(config-if)# no ip address
Router(config-if)# duplex auto
Router(config-if)# speed auto
Router(config-if)# interface gigabitethernet0/1.1
Router(config-subif)# encapsulation dot1q 1 native
Router(config-subif)# ip address 192.168.10.1 255.255.255.0
Router(config-subif)# interface gigabitethernet0/1.2
Router(config-subif)# encapsulation dot1q 2
Router(config-subif)# ip address 192.168.20.1 255.255.255.0
```

Чтобы сформировать транк с нашим коммутатором, необходимо создать один под-интерфейс для каждого VLAN, сконфигурированного на нашем коммутаторе. После создания под-интерфейса мы назначаем ему IP-адрес и устанавливаем тип инкапсуляции 802.1Q и указываем номер VLAN, к которому принадлежит под-интерфейс.

Например, команда **encapsulation dot1q 2** определяет инкапсуляцию 802.1Q и устанавливает под-интерфейс на VLAN 2.

Параметр **native** который мы использовали для под-интерфейса gigabitethernet0/1.1, сообщает маршрутизатору, что нативный vlan - это VLAN 1. Это параметр по умолчанию на каждом коммутаторе Cisco и поэтому должен совпадать с маршрутизатором.

Для проверки можно использовать на роутере команду **show vlans**, где будут отображены созданные нами под-интерфейсы, а также при помощи команды **show ip route** в таблице маршрутизации мы должны увидеть наши под-интерфейсы.

Готово! Теперь при помощи роутера мы можем маршрутизировать файлы между разными VLAN.

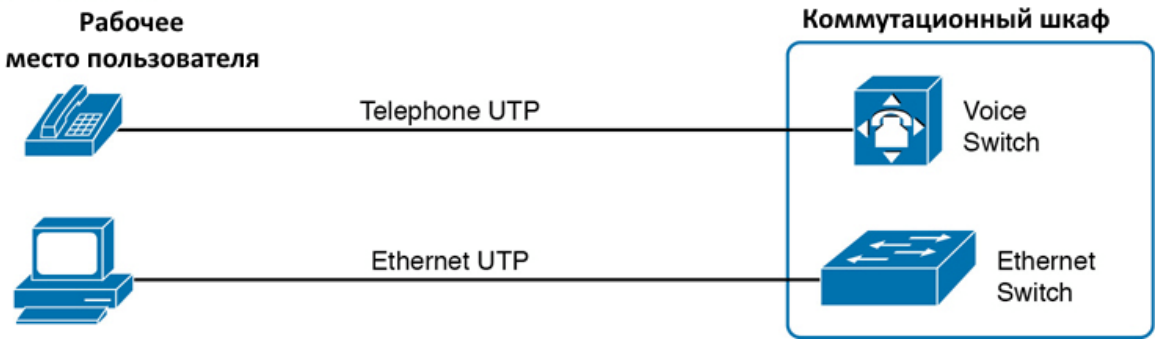
5. IP- телефония и VLAN

В этой статье мы разберем принцип работы и настройку IP-телефонии по Ethernet сетям.

В мире IP-телефонии телефоны используют стандартные порты Ethernet для подключения к сети, и поэтому для отправки и приема голосового трафика, передаваемого посредством IP-пакетов, они используют стек протоколов TCP/IP. Чтобы это работало, необходимо, чтобы порт коммутатора работал как порт доступа, но, в то же время, этот порт работал как магистраль для передачи другого трафика.

ПРИНЦИП РАБОТЫ VLAN ДЛЯ ПЕРЕДАЧИ ДАННЫХ И ГОЛОСА

До IP-телефонии компьютер и телефон располагались на одном рабочем месте. Телефон подключался по специальному телефонному кабелю (телефонный UTP-кабель). Причем этот телефон был подключен к специальному голосовому устройству (часто называемому `voice switch` или частной телефонной станцией `private branch exchange [PBX]`). ПК, конечно же, подключался с помощью Ethernet кабеля (UTP витой пары) к обычному коммутатору локальной сети, который находился в коммутационном шкафу - иногда в том же коммутационном шкафу, что и голосовой коммутатор (`voice switch`). На рисунке показана эта идея.



Предположим, что у нас есть три виртуальные сети VLAN1, VLAN2 и VLAN3. Виртуальные сети VLAN 1 и VLAN 3 содержат по две пары ПК, которые подключаются к коммутатору через отдельные интерфейсы. Для сети VLAN 1 отведены четыре интерфейса "**fa0/12**", "**fa0/11**", "**fa0/22**", и "**fa0/21**" соответственно. Аналогично, 4 интерфейса отведены для сети VLAN 3 - "**fa0/15**", "**fa0/16**", "**fa0/23**", и "**fa0/24**" соответственно. Сеть VLAN 2 состоит из двух ПК, которые подключаются к коммутатору через интерфейсы "**Fa0/13**" и " **Fa0/14**". Два коммутатора соединены между собой через магистраль, и интерфейсы "Gi0/1" и "Gi0/2".

Термин IP-телефония относится к отрасли сети, в которой телефоны используют IP-пакеты для передачи и приема голоса, представленного битами в части данных IP-пакета. Телефоны подключаются к сети, как и большинство других устройств конечных пользователей, используя либо кабель Ethernet, либо Wi-Fi. Новые IP-телефоны не подключаются непосредственно по кабелю к голосовому коммутатору, а подключаются к стандартной IP-сети с помощью кабеля Ethernet и порта Ethernet, встроенного в телефон. После чего телефоны связываются по IP-сети с программным обеспечением, которое заменило операции вызова и другие функции АТС.

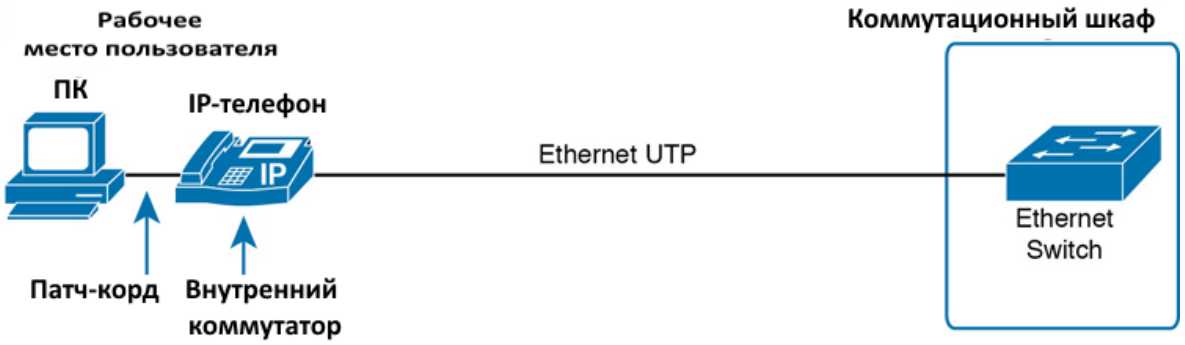
Переход от использования стационарных телефонов, которые работали (некоторые работают по сей день) с использованием телефонных кабелей к новым IP-телефонам (которые нуждались в UTP-кабелях, поддерживающих Ethernet) вызвал некоторые проблемы в офисах.

В частности:

- Старые, не IP-телефоны, использовали категорию UTP-кабелей, у которых частотный диапазон не поддерживал скорость передачи данных в 100-Mbps или 1000-Mbps.
- В большинстве офисов был один кабель UTP, идущий от коммутационного шкафа к каждому столу. Теперь же на два устройства (ПК и IP-телефон) требовалось два кабеля от рабочего стола к коммутационному шкафу.
- Прокладка нового кабеля к каждому рабочему месту вызовет дополнительные финансовые затраты, и плюс потребуется больше портов коммутатора.

Чтобы решить эту проблему, компания Cisco встроила небольшие трехпортовые коммутаторы в каждый телефон.

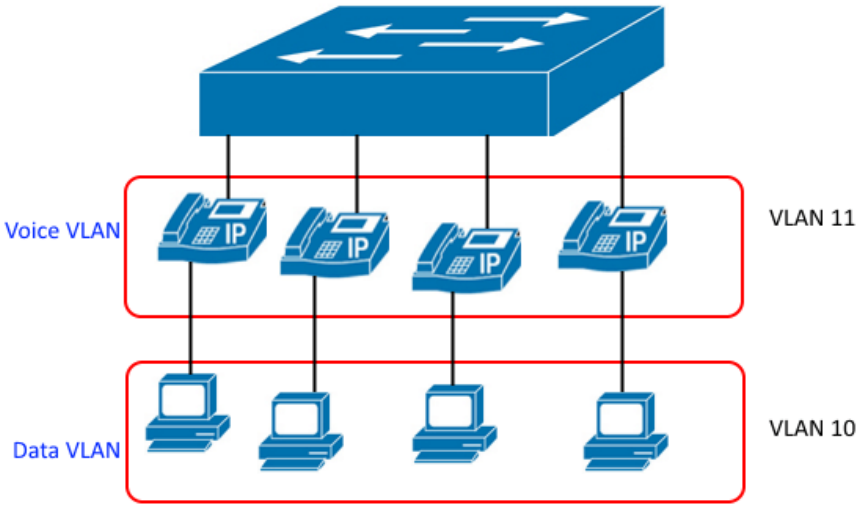
IP-телефоны включают в себя небольшой коммутатор локальной сети, расположенный в нижней части телефона. На рисунке показаны основные кабели, причем кабель коммутационного шкафа подключается напрямую к одному физическому порту встроенного коммутатора телефона, ПК подключается патч-кордом к другому физическому порту телефона, а внутренний процессор телефона подсоединяется к внутреннему порту коммутатора телефона.



Компании, использующие IP-телефонию, теперь могут подключать два устройства к одному порту доступа. Кроме того, лучшие практики Cisco, для проектирования IP-телефонии, советуют поместить телефоны в один VLAN, а ПК в другой VLAN. Чтобы это работало, порт коммутатора действует частично в режиме канала доступа (для трафика ПК) и частично как магистраль (для трафика телефона).

Особенности настройки VLAN'ов на этом порту:

- VLAN передачи данных: та же идея настройки, что и VLAN доступа на access порту, но определенная как VLAN на этом канале для пересылки трафика для устройства, подключенного к телефону на рабочем месте (обычно ПК пользователя).
- Voice VLAN: VLAN для пересылки трафика телефона. Трафик в этой VLAN обычно помечается заголовком 802.1 Q.



На рисунке изображена типичная конструкция локальной сети. Имеется коммутатор, подключенный к двум последовательным уровням сетей, VLAN 11 и VLAN 10, где сеть VLAN 11- Voice VLAN, содержащая 4 IP-телефона, и сеть VLAN 10 - Data VLAN, состоящая из 4 ПК.

НАСТРОЙКА И ПРОВЕРКА РАБОТЫ DATA И VOICE VLAN

Для настройки порта коммутатора, который сможет пропускать голосовой трафик и информационные данные, необходимо применить всего несколько простых команд. Однако разобраться в командах, позволяющих просмотреть настройки режима работы порта, непросто, так как порт действует как access порт во многих отношениях.

Ниже показан пример настройки. В данном примере используются четыре порта коммутатора F0/1F0/4, которые имеют базовые настройки по умолчанию. Затем добавляются соответствующие VLAN'ы: VLAN 10 Data Vlan, VLAN 11- Voice Vlan. Далее все четыре порта настраиваются как порты доступа и определяется VLAN доступа (Vlan 10 Date Vlan). В конце настройки определяем на порт VLAN для передачи голосовых данных (Vlan 11- Voice Vlan). Данный пример иллюстрирует работу сети, изображенную на рисунке:

```
SW-1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-1(config)# vlan 10
SW-1(config-vlan)# vlan 11
SW-1(config-vlan)# interface range FastEthernet0/1 - 4
SW-1(config-if)# switchport mode access
SW-1(config-if)# switchport access vlan 10
SW-1(config-if)# switchport voice vlan 11
SW-1(config-if)#^Z
SW-1#
```

При проверке состояния порта коммутатора, из примера выше, увидим разницу в отображаемой информации выходных данных, по сравнению с настройками по умолчанию порта доступа и магистрального порта. Например, команда `show interfaces switchport` показывает подробные сведения о работе интерфейса, включая сведения о портах доступа. В примере 2 отображены эти детали (подчеркнуты) для порта F0/4 после добавления настроек из первого примера.

```
SW-1# show interfaces FastEthernet0/4 switchport
Name: Fa0/4
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (VLAN0010)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 11 (VLAN0011)
! The rest of the output is omitted for brevity
```

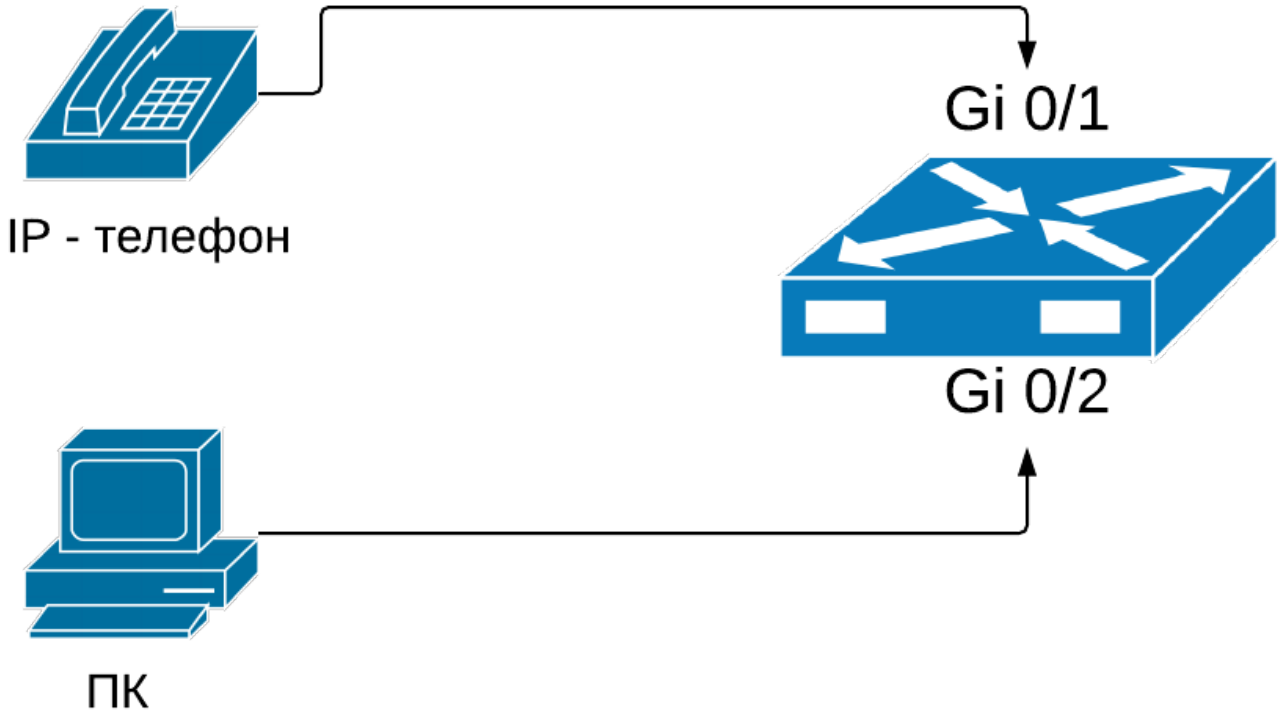
Первые три выделенные строки в выходных данных отображают детали настройки, соответствующие любому порту доступа. Команда `switchport mode access` переводит порт в режим порта доступа. Далее, как показано в третьей выделенной строке, команда `switchport access vlan 10` определила режим доступа VLAN.

Четвертая выделенная строка показывает новый фрагмент информации: идентификатор Voice VLAN, активированная командой `switchport voice vlan 11`. Эта небольшая строка является единственной информацией об изменении состояния порта.

5.1. Настройка voice vlan на Cisco

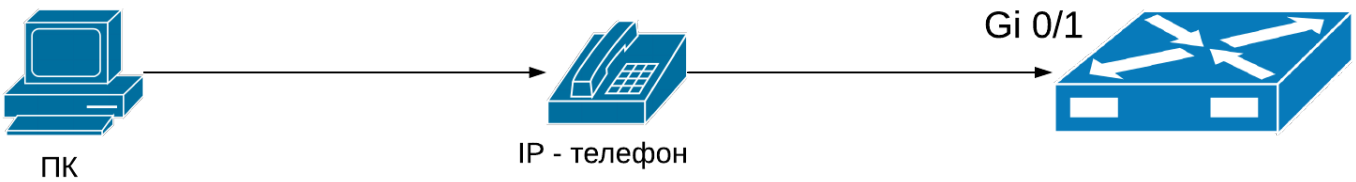
Поговорим про голосовой трафик в классических корпоративных сетях, а именно про его сегрегацию от обычного дата трафика и про включение телефонов в саму КСПД.

Обычно, телефоны находятся на столе рядом с компьютером на рабочем стол, подключаются такой же витой парой (UTP), что и компьютер, и тоже используют протокол **Ethernet**. Для подключения телефона к коммутатору существует две опции – подключение оборудования к свитчу «параллельно», используя два кабеля или же подключив телефон и компьютер «последовательно»:



Первый «параллельный» сценарий заработает, но есть несколько больших недостатков – дополнительный кабель и занятый порт на коммутаторе.

По этой причине в данный момент большинство IP – телефонов, включая **Cisco**, имеют маленький коммутатор на 3 порта внутри IP – телефона:

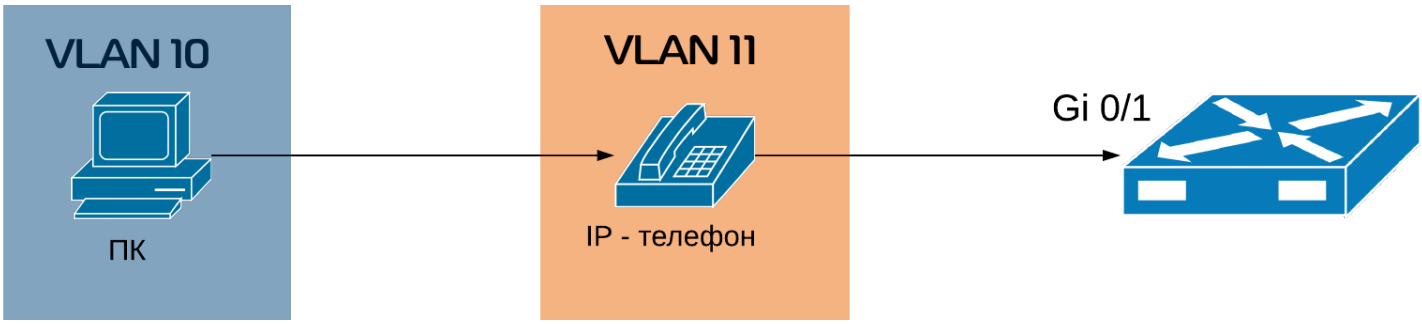


- Первый порт подключается к **коммутатору**;
- Второй порт подключается к **компьютеру**;
- Внутренний порт подключает сам **телефон**;

Теперь поговорим о вопросе разделения голосового трафика от любого другого – и мы можем выполнить данную задачу с помощью голосового VLANa.

Голосовой VLAN также иногда обозначается как AUX VLAN

Посмотрите на схему ниже – это то, как будет выглядеть наше подключение – все компьютеры и обычный трафик будут находиться в VLAN 10, а голосовой трафик мы поместим в VLAN 11.



Как это все работает? Между коммутатором и телефоном у нас есть так называемый "транк". Порт на телефоне, который подключается к компьютеру, является портом доступа. Телефона передает весь трафик с компьютера на коммутатор без каких - либо меток, непомеченным. Трафик с самого телефона всегда будет помечаться, и в транке будут разрешены только два вышеупомянутых VLANa.

НАСТРОЙКА

Если вы уже знакомы с настройкой VLANов, то создание голосового VLANa не составит для вас вообще никакого труда. Давайте настроим порт на коммутаторе, где мы будем использовать VLANы 10 и 11.

Сначала мы создаем данные VLANы:

```
MERION-SW1(config)#vlan 10
MERION-SW1(config-vlan)#name DATA
MERION-SW1(config-vlan)#exit

MERION-SW1(config)#vlan 11
MERION-SW1(config-vlan)#name VOICE
MERION-SW1(config-vlan)#exit
```

Теперь настроим интерфейс:

```
MERION-SW1(config)#interface GigabitEthernet 0/1
MERION-SW1(config-if)#switchport mode access
MERION-SW1(config-if)#switchport access vlan 10
MERION-SW1(config-if)#switchport voice vlan 11
MERION-SW1(config-if)#exit
```

Мы переключили данный порт в режим доступа и настраиваем его для **VLAN 10**. Команда `switchport voice vlan` сообщает коммутатору, чтобы он использовал **VLAN 11** как голосовой VLAN.

Для того, чтобы телефон понял, какой VLAN нужно использовать, используются два протокола – **Cisco Discovery Protocol (CDP)** для телефонов Cisco и **Link Layer Discovery Protocol (LLDP)** для телефонов от других вендоров

ПРОВЕРКА РАБОТОСПОСОБНОСТИ

Для проверки корректности настройки, мы будем использовать команду `show interfaces`

```
MERION-SW1#show interfaces GigabitEthernet 0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (DATA)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 11 (VOICE)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Как видно из вывода выше, VLANы настроились корректно. И теперь посмотрим на статус транка. Вывод скажет нам, что порт не является транком, он покажет какие VLANы в нем используются (то есть, которые мы настроили). Несмотря на то, что он показан как нетранковый, в реальности он все - таки является транком.

```
MERION-SW1#show interfaces GigabitEthernet 0/1 trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi0/1      off              negotiate      not-trunking  1

Port        Vlans allowed on trunk
Gi0/1      10-11

Port        Vlans allowed and active in management domain
Gi0/1      10-11

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/1      10-11
```

На этом настройка завершена – для остальных рабочих станций и телефонов данный шаг нужно выполнить точно также, но на других портах коммутатора. Голосовой трафик будет идти в приоритете перед остальным трафиком и это скажется в лучшую сторону на качестве связи.