Виртуальные локальные сети

VLAN

Мищенко П.В.

VLAN (Virtual Local Area Network)

— 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.

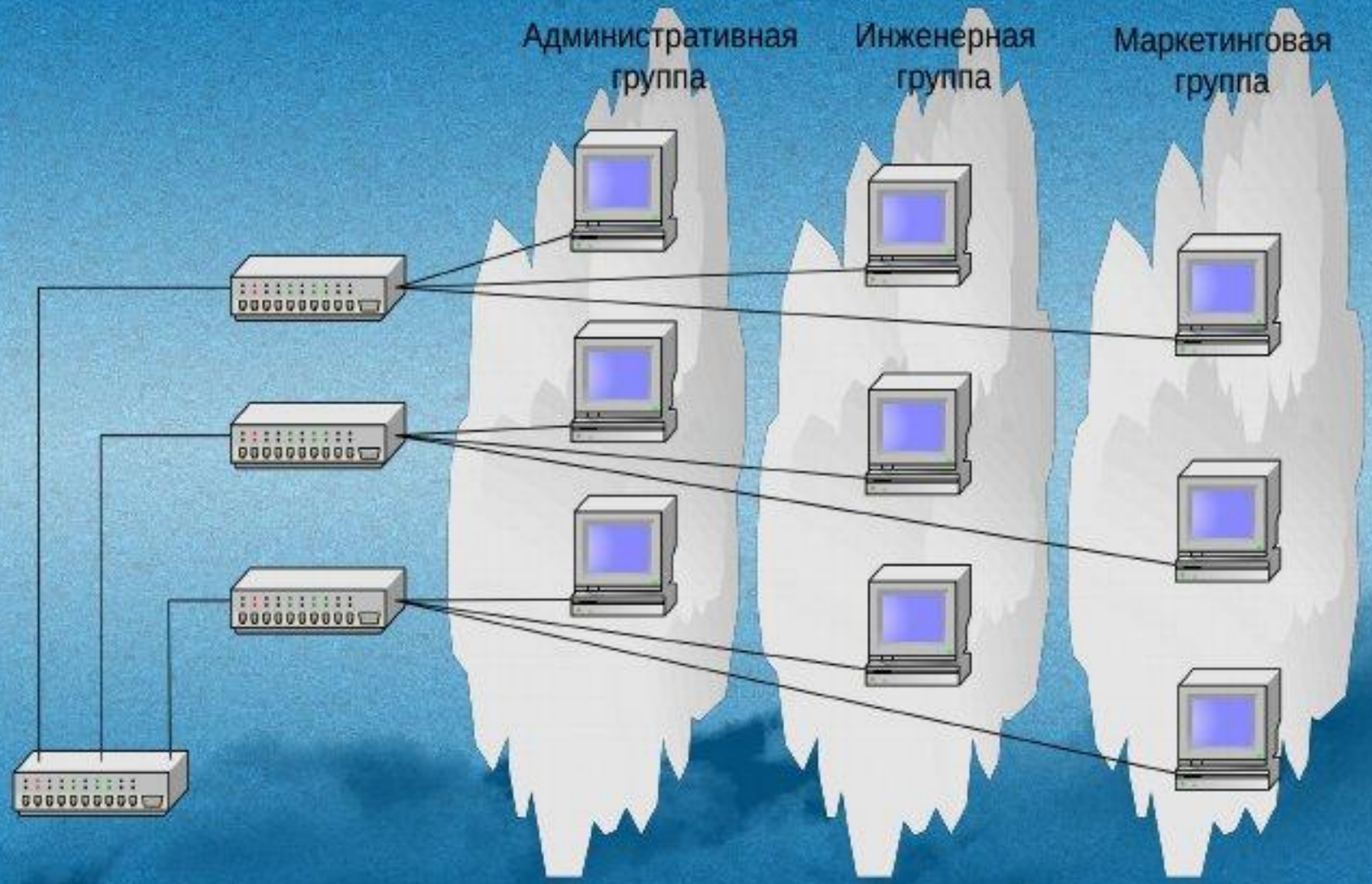
Виртуальной локальной сетью VLAN называется логическая группа узлов сети, трафик которой, в том числе и широковещательный, полностью изолирован от других узлов сети на канальном уровне.

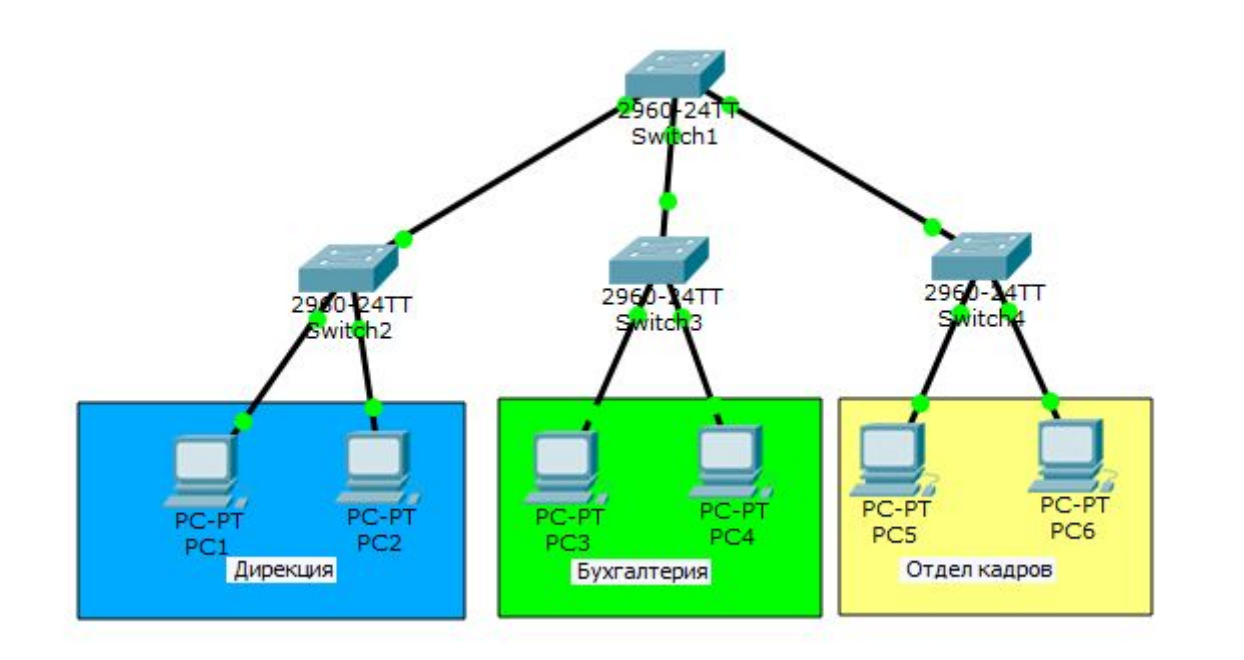
В современных сетях VLAN — главный механизм для создания логической топологии сети, не зависящей от её физической топологии.

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, hopping'ом и тд.

Необходимость введения сегментации сети



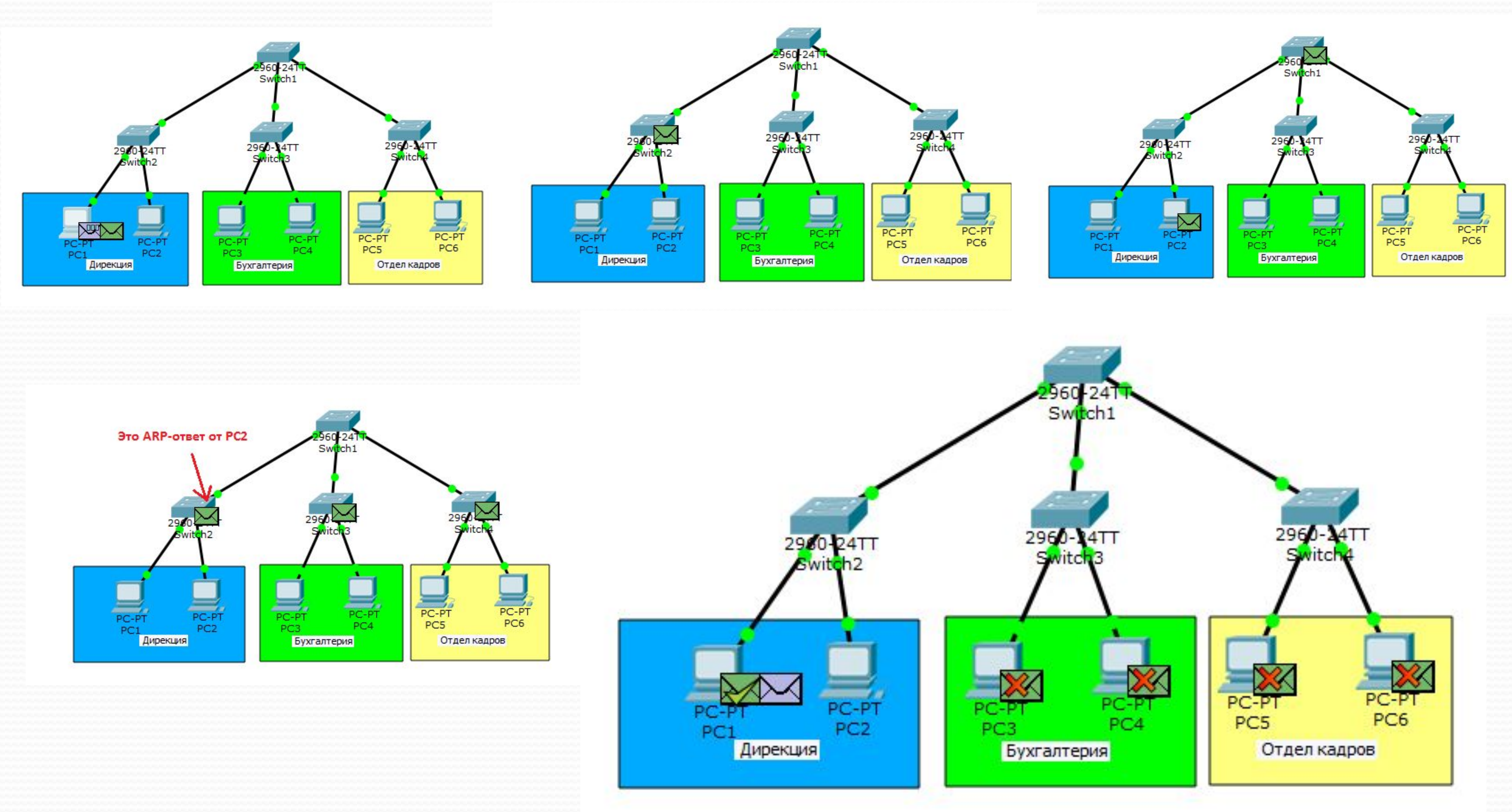


3 отдела: дирекция, бухгалтерия, отдел кадров.

У каждого отдела свой коммутатор и соединены они через центральный верхний.

PC1 – 192.168.1.2/24
PC2 – 192.168.1.3/24
PC3 – 192.168.1.4/24
PC4 – 192.168.1.5/24
PC5 – 192.168.1.6/24
PC6 – 192.168.1.7/24

PC1 отправляет ping на PC2.



Так как PC1 не знает MAC-адрес (или адрес канального уровня) PC2,

то он отправляет ARP-запрос.

Тот приходит на коммутатор, откуда ретранслируется на все активные порты, то есть к PC2 и на центральный коммутатор.

Из центрального коммутатора перейдет на соседние коммутаторы и так далее, пока не дойдет до всех. Вот такой не маленький трафик вызвало одно ARP-сообщение. Его получили все участники сети. Большой и не нужный трафик — это первая проблема.

Вторая проблема — это безопасность. Сообщение дошло даже до бухгалтерии, компьютеры которой вообще не участвовали в этом. Любой злоумышленник, подключившись к любому из коммутаторов, будет иметь доступ ко всей сети. В принципе сети раньше так и работали. Компьютеры находились в одной канальной среде и разделялись только при помощи маршрутизаторов.

ISL (Inter-Switch Link) 802.1q

Шло время и нужно было решать эту проблему на канальном уровне.

Cisco создали свой протокол, который тегировал кадры и определял принадлежность к определенной канальной среде.

Назывался он **ISL (Inter-Switch Link)**. Идея эта понравилась всем и IEEE решили разработать аналогичный открытый стандарт.

Стандарт получил название **802.1q**. Получил он огромное распространение и Cisco решила тоже перейти на него.

И вот как раз технология VLAN основывается на работе протокола 802.1q.

Назначение 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, где нет VLANов, находятся в одном широковещательном домене. Создание VLAN на коммутаторе означает разбиение коммутатора на несколько широковещательных доменов. Если один и тот же VLAN есть 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

- 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.

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

  Существуют проприетарные протоколы, решающие похожие задачи, например, протокол ISL от Cisco Systems, но их популярность значительно ниже.

Коммутатор и VLAN'ы

- VLAN'ы могут быть настроены на коммутаторах, маршрутизаторах, других сетевых устройствах и на хостах. Однако, для объяснения VLAN лучше всего подойдет коммутатор.

- Коммутатор — устройство 2го уровня и изначально все порты коммутатора находятся, как правило, в VLAN 1 и, следовательно, в одном широковещательном сегменте.

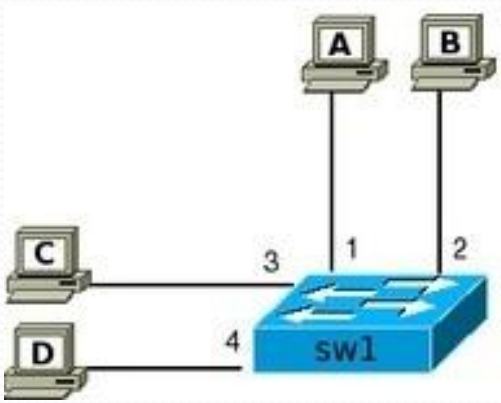
- Это значит, что если один из хостов, подключенных к коммутатору, отправит широковещательный фрейм, то все остальные хосты подключенные к нему также получат его.

Принципы работы коммутатора

- Для того чтобы передавать кадры (фреймы), коммутатор использует таблицу коммутации. Изначально, после включения коммутатора таблица пуста. Заполняет её коммутатор автоматически, при получении кадров от подключенных узлов. Когда коммутатор получает кадр, он сначала передает его в соответствии со своими правилами (описаны ниже), а затем запоминает MAC-адрес отправителя и ставит его в соответствие порту на котором он был получен.

- Например, итоговая таблица коммутации для представленного рисунка будет иметь такой вид:

Порт коммутатора	MAC-адрес хоста
1	A
2	B
3	C
4	D



Когда таблица заполнена, коммутатор знает на каких портах у него находятся какие узлы и передает кадры на соответствующие порты.

Механизмы передачи кадров (фреймов)

Для передачи кадров коммутатор использует три базовых механизма:

- **Flooding** — фрейм, полученный на один из портов, передается на остальные порты коммутатора. Коммутатор выполняет эту операцию в двух случаях:
  - при получении широковещательного или multicast (если не настроена поддержка multicast) фрейма,
  - при получении unknown unicast фрейма. Это позволяет коммутатору доставить фрейм хосту (при условии, что хост достижим и существует), даже когда он не знает, где хост находится.
- **Forwarding** — передача фрейма, полученного на одном порту, через другой порт в соответствии с записью в таблице коммутации.
- **Filtering**— если коммутатор получает фрейм через определенный порт, и MAC-адрес получателя доступен через этот же порт (это указано в таблице коммутации), то коммутатор отбрасывает фрейм. То есть, коммутатор считает, что в этом случае хост уже получил этот фрейм, и не дублирует его.

Два VLAN’а на одном коммутаторе

- Обычно, по умолчанию все порты коммутатора считаются нетегированными членами VLAN 1. В процессе настройки или работы коммутатора они могут перемещаться в другие VLAN'ы.

- На коммутаторе, который изображен на рисунке, настроены два VLAN'а, все порты настроены как нетегированные (access-порты в терминологии Cisco) в соответствующих VLAN.

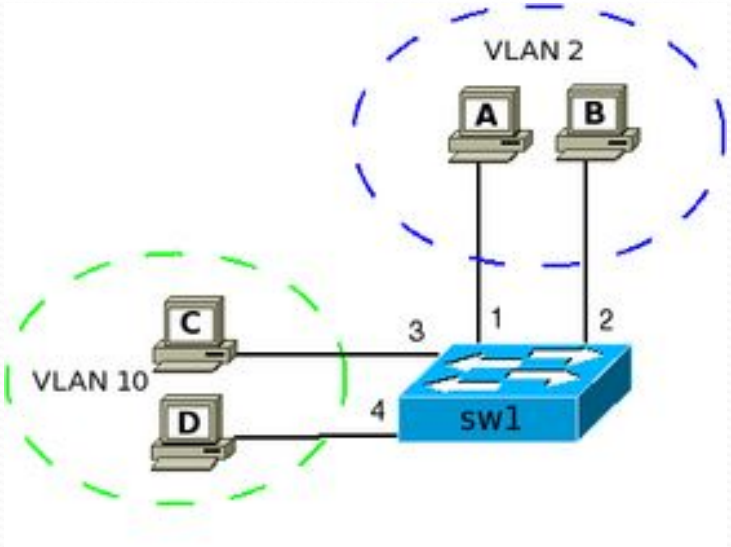
  После этого на коммутаторе существуют две таблицы коммутации.

  Для VLAN'а 2:

Порт коммутатора	MAC-адрес хоста
1	A
2	B

  Для VLAN'а 10:

Порт коммутатора	MAC-адрес хоста
3	C
4	D



- Все базовые механизмы коммутатора остаются точно такими же как и до разделения на VLAN, но они используются только в пределах соответствующего VLAN.

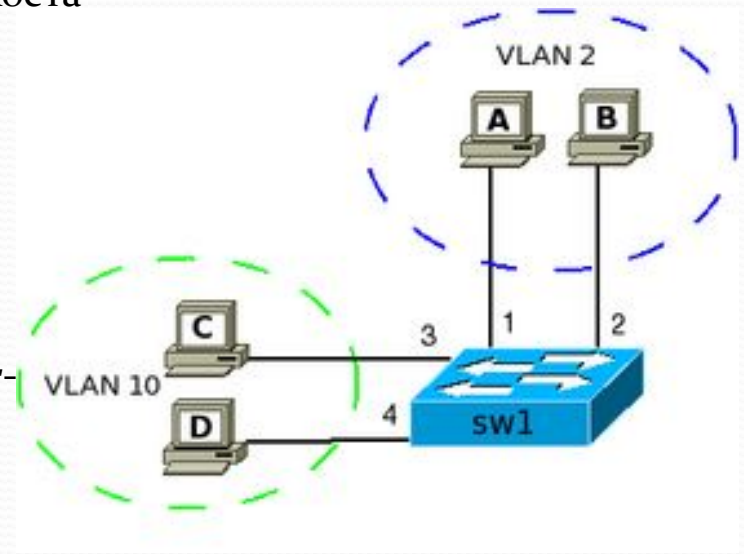
- Например, если хост из VLAN 10 отправляет широковещательный кадр, то он будет отправлен только на порты в этом VLAN'е.

- Получается, что нетегированные порты это "обычные" порты коммутатора. Это просто возможность сообщить коммутатору о том, какому VLAN принадлежат порты. Затем коммутатор использует эту информацию при передаче кадров.

- Как правило, реально в таблице коммутации указывается порт, MAC-адрес и VLAN. То есть, для указанного пример, а таблица коммутации будет такой:

Порт коммутатора	VLAN	MAC-адрес хоста
1	2	A
2	2	B
3	10	C
4	10	D

- Однако, далее для упрощения используется запись таблицы коммутации в виде соответствия между портами и MAC-адресами.



VLAN’ы на нескольких коммутаторах

- К используемому примеру добавлен коммутатор sw2 и два хоста E и F в VLAN 2
- Для указанного примера достаточно добавить на коммутаторе sw1 порт 10 в VLAN 2, а на коммутаторе sw2 порт 9 в VLAN 2. Принадлежность к VLAN указывается настройкой порта нетегированным в VLAN 2 (пока что).

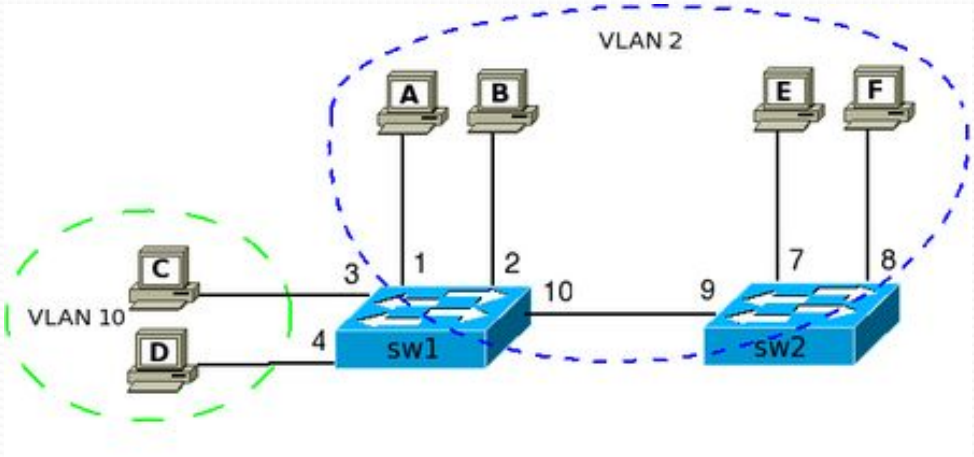
  После этого на коммутаторах в таблицах коммутации добавятся новые порты и соответствующие MAC-адреса хостов. Теперь четыре хоста на разных коммутаторах находятся в одном широковещательном сегменте.

Таблица коммутации sw1 для VLAN'а 2:

Порт коммутатора	MAC-адрес хоста
1	A
2	B
10	E
10	F

Таблица коммутации sw2 для VLAN'а 2:

Порт коммутатора	MAC-адрес хоста
7	E
8	F
9	A
9	B



Тегирование портов

- К используемому примеру добавлен к коммутатору sw2 добавлены два хоста G и H в VLAN 10.

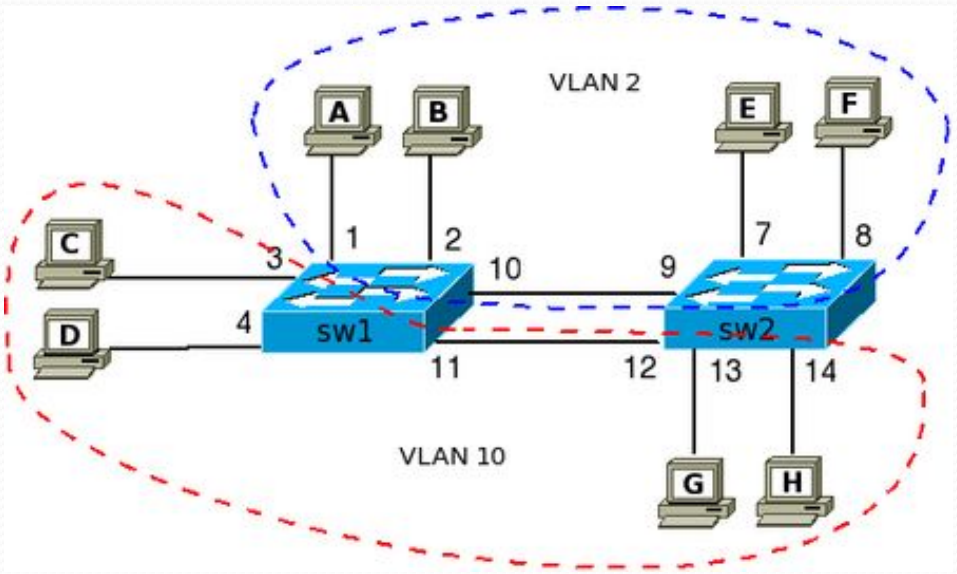
- Для того чтобы хосты C и D в VLAN'е 10 на коммутаторе sw1, могли обмениваться информацией с хостами VLAN'а 10 на коммутаторе sw2 добавлен линк между коммутаторами. Логика аналогична добавлению хостов в VLAN 2.

Таблица коммутации sw1 для VLAN'а 10:

Порт коммутатора	MAC-адрес хоста
3	C
4	D
11	G
11	H

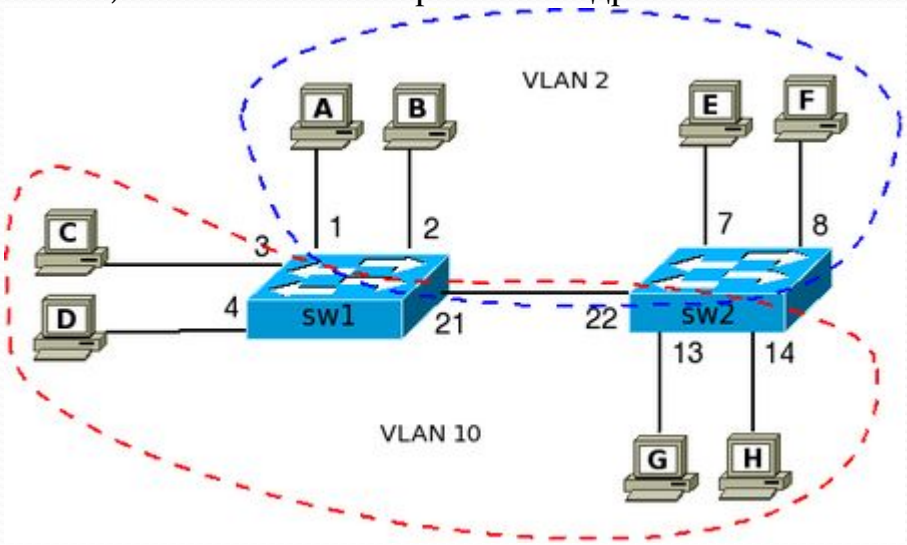
Таблица коммутации sw2 для VLAN'а 10:

Порт коммутатора	MAC-адрес хоста
13	G
14	H
12	C
12	D



Создание тегированного порта между коммутаторами

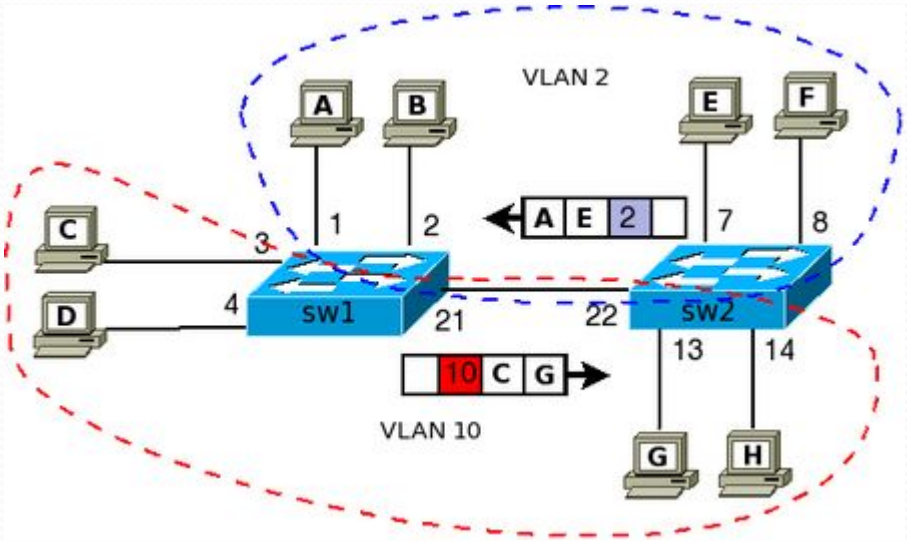
- Когда необходимо передать трафик одного-двух VLAN'ов между коммутаторами, то схема, которая использовалась выше, выглядит нормально. Однако, когда количество VLAN возрастает, то схема явно становится очень неудобной, так как для каждого VLAN надо будет добавлять линк между коммутаторами для того, чтобы объединить хосты в один широковещательный сегмент.
- Для решения этой проблемы используются тегированные порты.
- Тегированный порт позволяет коммутатору передать трафик нескольких VLAN'ов через один порт и сохранить при этом информацию о том, в пределах какого именно VLAN'а передается кадр.
- На коммутаторах sw1 и sw2 порты 21 и 22, соответственно, это тегированные порты.
- Для того, чтобы коммутаторы понимали какому VLAN принадлежит пришедший кадр и использовали соответствующую таблицу коммутации для его обработки, выполняется тегирование кадра.
- Например, если хост E передает фрейм хосту A, то коммутатор sw2 проверяет свою таблицу и видит, что хост A доступен через порт 22. Так как порт настроен как тегированный, то когда кадр выходит с порта 22 в нём проставляется тег, который указывает какому VLAN'у принадлежит этот фрейм. В данном случае проставляется тег с VLAN'ом 2.



- Коммутатор sw1 получает тегированный кадр через тегированный порт 21. Для того чтобы определить на какой порт его передавать далее sw1 использует таблицу коммутации для VLAN 2 (так как этот VLAN был указан в теге). На коммутаторе sw1 порт 21 должен быть настроен как тегированный для того чтобы коммутатор не отбрасывал тегированные фреймы, а считывал информацию тега. И соответственно чтобы он также помечал фрейм тегом, когда будет передаваться трафик коммутатору sw2.

- Остальные порты коммутатора остаются нетегированными. И для хостов операция тегирования, которую выполняют коммутаторы абсолютно прозрачна.
  Хосты ничего не знают о тегах и получают обычные кадры.

- Аналогичные действия выполняются, например, при передаче кадра от хоста C хосту G.



Принадлежность к VLAN

- Порты коммутатора, поддерживающие VLAN'ы, (с некоторыми допущениями) можно разделить на два множества:
- Тегированные порты (или транковые порты, trunk-порты в терминологии Cisco),
- Нетегированные порты (или порты доступа, access-порты в терминологии Cisco);
- Тегированные порты нужны для того, чтобы через один порт была возможность передать несколько VLAN'ов и, соответственно, получать трафик нескольких VLAN'ов на один порт. Информация о принадлежности трафика VLAN'у, как было сказано выше, указывается в специальном теге. Без тега коммутатор не сможет различить трафик различных VLAN'ов.
- Если порт нетегированный в каком-то VLAN'е, то трафик этого VLAN передается без тега. На Cisco нетегированным порт может быть только в одном VLAN, на некоторых других свитчах (например, ZyXEL, D-Link и Planet) данного ограничения нет.
- Если порт тегирован для нескольких VLAN'ов, то в этом случае весь нетегированный трафик будет приниматься специальным родным VLAN'ом (native VLAN). С этим параметром (native, PVID, port VID) возникает больше всего путаницы.
- Например, свитчи Planet для правильной работы untagged порта требуют поместить порт в VLAN, задать режим порта untagged, и прописать этот же номер VLAN в PVID этого порта. HP ProCurve делают наоборот, tagged порт начинает работать как tagged только если поставить его PVID в "None".

- Если порт принадлежит только одному VLAN как нетегированный, то тегированный трафик, приходящий через такой порт, должен удаляться. На деле это поведение обычно настраивается.

- Проще всего это понять, если "забыть" всю внутреннюю структуру коммутатора и отталкиваться только от портов. Допустим, есть VLAN с номером 111, есть два порта которые принадлежат к VLAN 111. Они общаются только между собой, с untagged/access-порта выходит нетегированный трафик, с tagged/trunk-порта выходит трафик тегированный в VLAN 111. Все необходимые преобразования прозрачно внутри себя делает коммутатор.

- Обычно, по умолчанию все порты коммутатора считаются нетегированными членами VLAN 1. В процессе настройки или работы коммутатора они могут перемещаться в другие VLAN'ы.

- Существуют два подхода к назначению порта в определённый VLAN:

- Статическое назначение — когда принадлежность порта VLAN'у задаётся администратором в процессе настройки;

- Динамическое назначение — когда принадлежность порта VLAN'у определяется в ходе работы коммутатора с помощью процедур, описанных в специальных стандартах, таких, например, как 802.1X. При использовании 802.1X для того чтобы получить доступ к порту коммутатора, пользователь проходит аутентификацию на RADIUS-сервере. По результатам аутентификации порт коммутатора размещается в том или ином VLANe (подробнее: 802.1X и RADIUS).

Настройка VLAN на коммутаторах Cisco IOS

Терминология Cisco:

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

- Коммутаторы Cisco ранее поддерживали два протокола 802.1Q и ISL. ISL — проприетарный протокол использующийся в оборудовании Cisco. ISL полностью инкапсулирует фрейм для передачи информации о принадлежности к VLAN'у.

- В современных моделях коммутаторов Cisco ISL не поддерживается.
- Для того чтобы передать через порт трафик нескольких VLAN, порт переводится в режим транка.

Режимы интерфейса

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.

- Dynamic Trunk Protocol (DTP) — проприетарный 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.

Разрешенные VLAN'ы

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

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.