Информационные технологии корпоративных сетей

Преподаватель: **ГУБИН Александр Николаевич**

к.т.н., доц.

каф. ИУС (ауд. 631) Тел. 3051278

Информационные технологии корпоративных сетей

Состав курса (9-ый сем):

Лекции - 22 ч.

Лаб.р. - 8 ч.

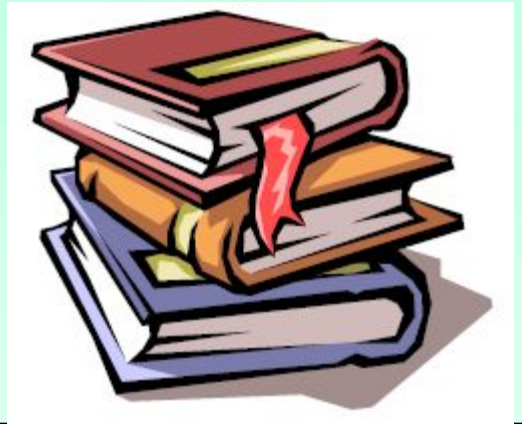
Кпр.

Экзамен

Лекция №2

Литература:

1. Э.Таненбаум, Д.Уэзеролл. Компьютерные сети. 5-е издание, Питер, 2012, 955 с.
2. Ломовицкий В.В. И др. Основы построения систем и сетей передачи информации: Учебное пособие для вузов. М.: Горячая линия-Телеком, 2005.-382с.



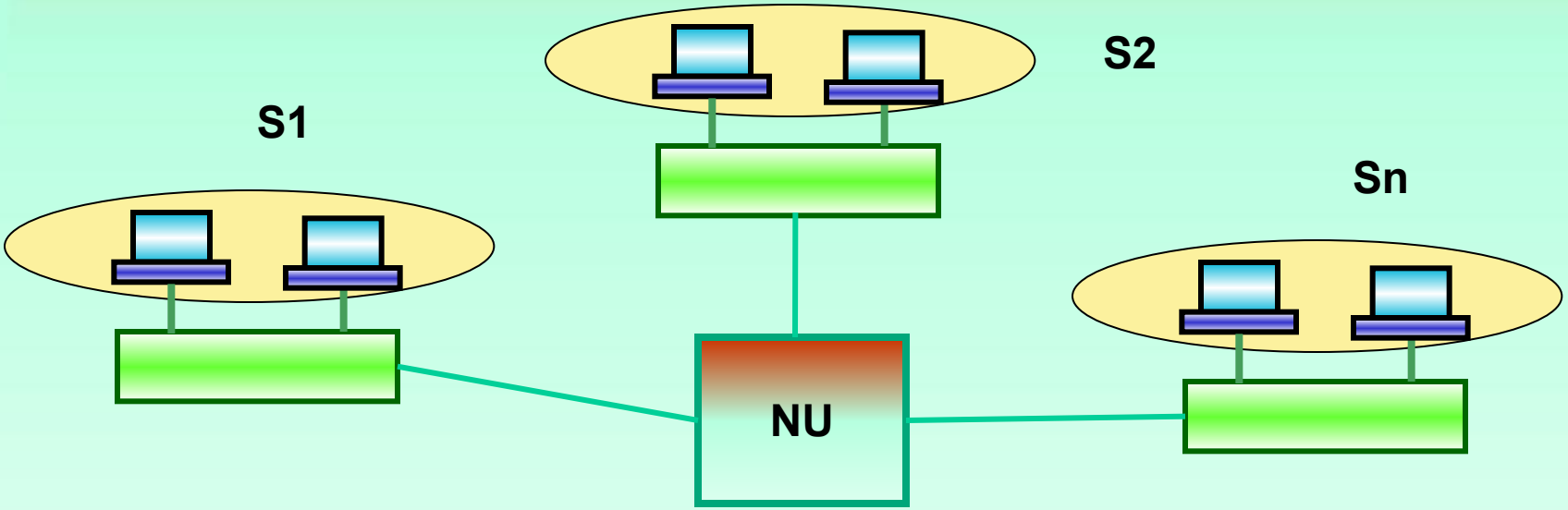
Информационные технологии корпоративных сетей

Лекция № 2 (4 ч)

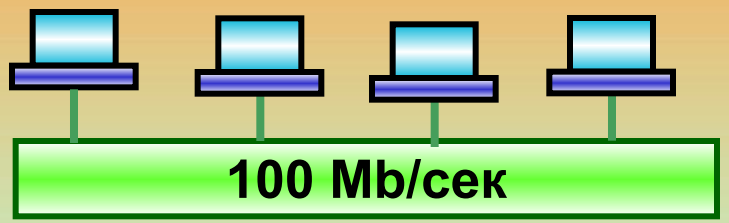
- Основные задачи сегментирования корпоративных сетей.
- Мосты и задачи сегментирования.
- Использование маршрутизаторов для сегментирования КС
- Коммутаторы
- Поддержка виртуальных сетей

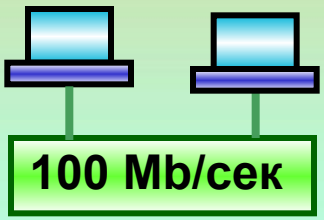
Сегментация КС

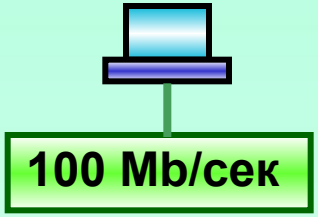
Необходимость сегментирования КС объясняется ростом корпораций (увеличение числа пользователей) и требованиям большей пропускной способности КС. Сегментация предусматривает разделение КС на более мелкие части и соединение этих частей с помощью оборудования межсетевого обмена



Сегментация КС



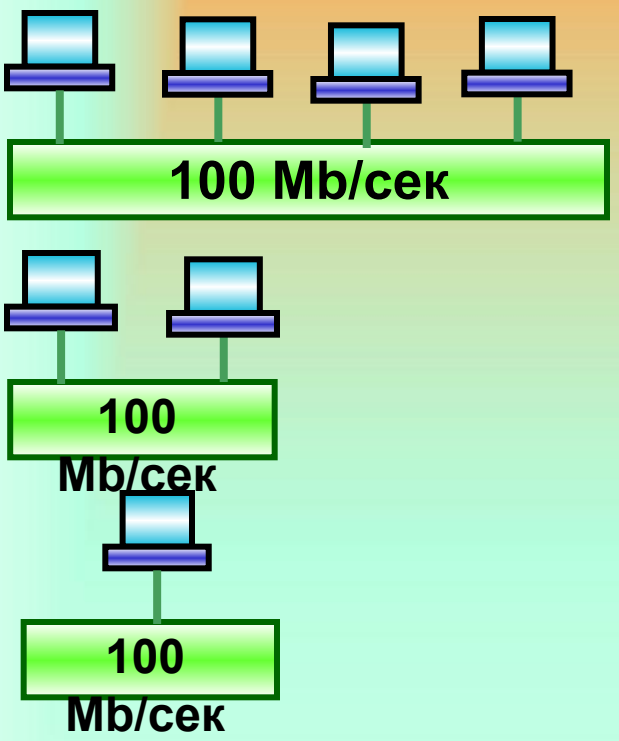




Уменьшение числа пользователей в каждом сегменте КС приводит к увеличению полезной пропускной способности сети на одного пользователя.

(В крайнем случае, когда в сегменте находится один пользователь, он получает полную пропускную способность сети на одного пользователя).

Сегментация КС



Уменьшение числа пользователей в каждом сегменте КС приводит к сокращению количества коллизий (уменьшается вероятность повторных коллизий). Сеть удается отвести от той степени загрузки, когда из-за коллизий ее производительность катастрофически деградирует

С точки зрения локализации трафика, в сегменты следует включать узлы, образующие рабочие группы. Предполагается, что в основном эти узлы обмениваются данными между собой.

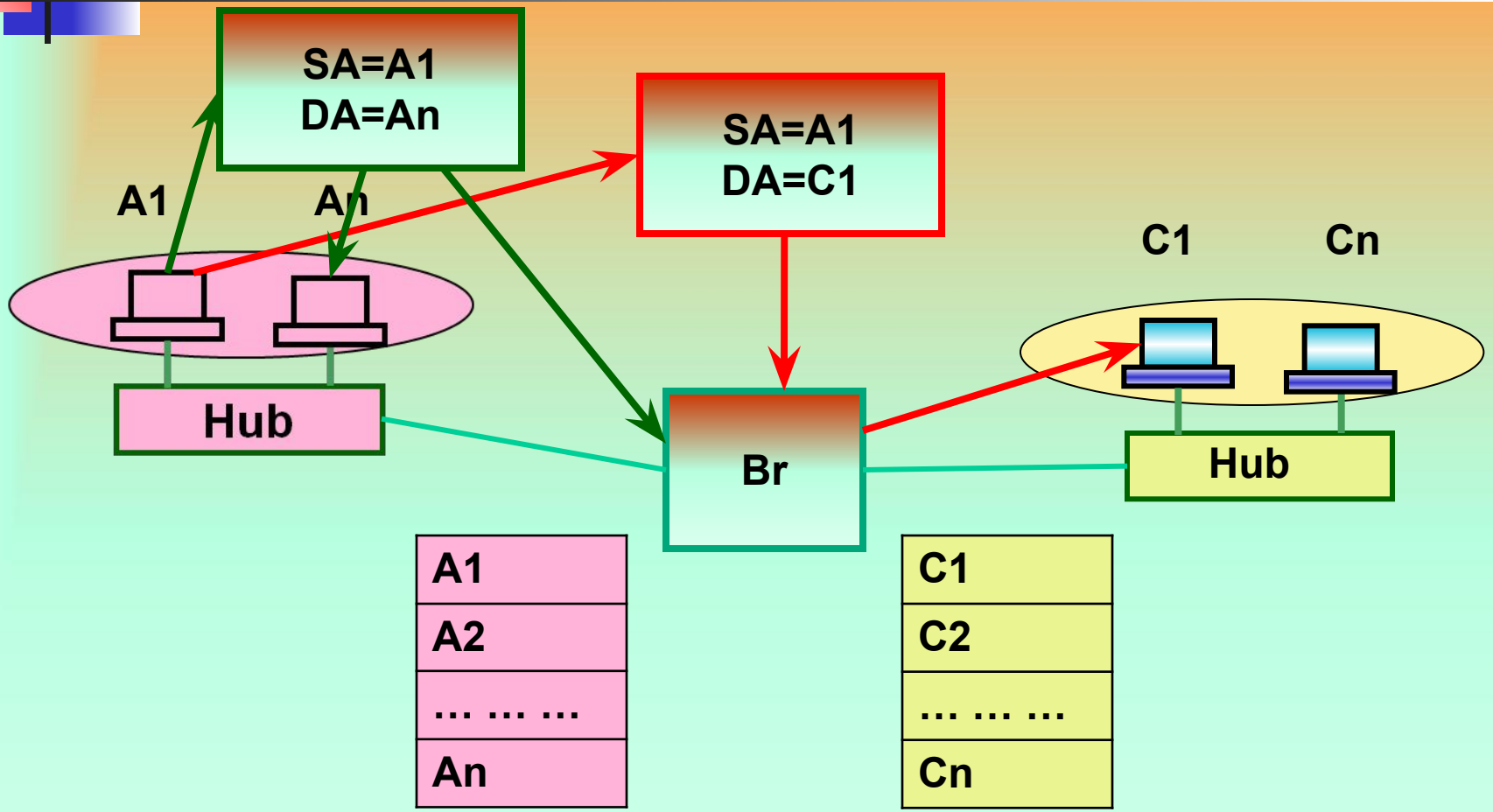
Сегментация КС

Для решения задачи сегментации КС могут быть использованы различные сетевые устройства:

- **Мосты**
- **Маршрутизаторы**
- **Коммутаторы**

Решение проблемы сегментации предусматривает выбор типа устройства межсетевого обмена.

Сегментация КС с помощью мостов



Объединение сегментов КС с помощью мостов предусматривает фильтрацию фреймов (анализ MAC-адресов каждого фрейма)

Сегментация КС с помощью мостов

В технологии Ethernet используется метод называемый прозрачным мостовым соединением (Transparent Bridging).
Согласно этой технологии мост проверяет MAC-адрес получателя фрейма и по результатам проверки определяет надо ли передавать этот фрейм в другой сегмент, или его надо отфильтровать, или передать во все порты.
Мост работает на втором (канальном) уровне модели OSI и следовательно имеет доступ к заголовку фрейма, который содержит информацию о MAC-адресах.

Сегментация КС с помощью мостов

Процесс фильтрации и селективного перенаправления фреймов позволяет сохранить пропускную способность на достаточно высоком уровне в каждом из сегментов КС.

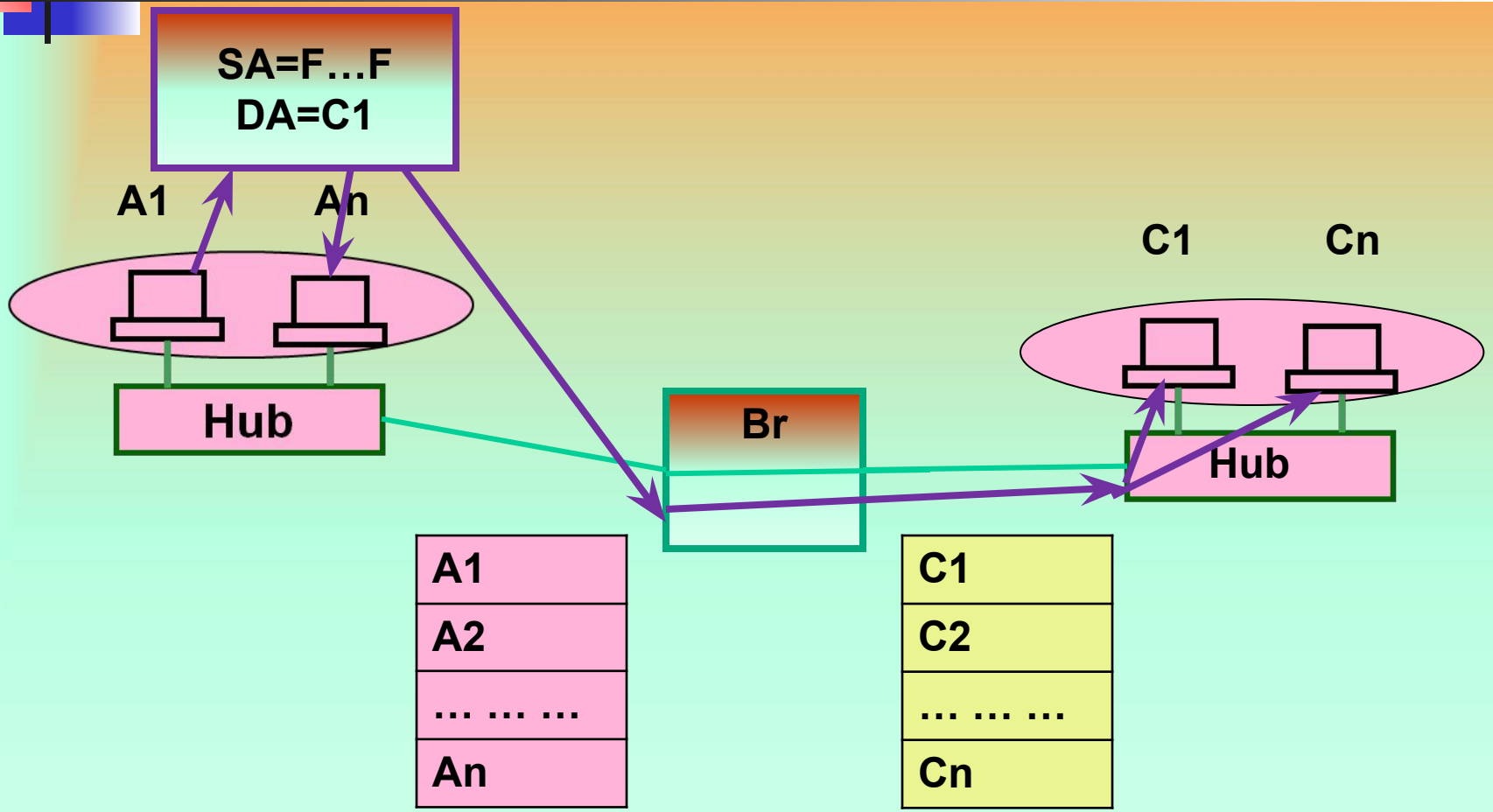
При перенаправлении трафика мосты не меняют содержимого фреймов (адреса 2-го и 3-го уровней остаются без изменений). Можно отметить, что маршрутизаторы вынуждены изменять адреса 2-го уровня.

Фильтрации не подлежат широковещательные фреймы и фреймы групповой рассылки. При получении таких фреймов мост передает их во все интерфейсы.

Сегментация КС с помощью мостов

Поскольку все сегменты КС, подключенные к мосту должны принадлежать одному широковещательному домену (одной IP сети) , то такая КС легко перегружается трафиком широковещательных и групповых сообщений (мультимедиа, видеоконференции и др.). Фреймы посланные участниками конференции распространяются по всем сегментам КС и КС становится одной большой сетью с общим доступом (пропускная способность всей сети становится разделяемой)

Сегментация КС с помощью мостов



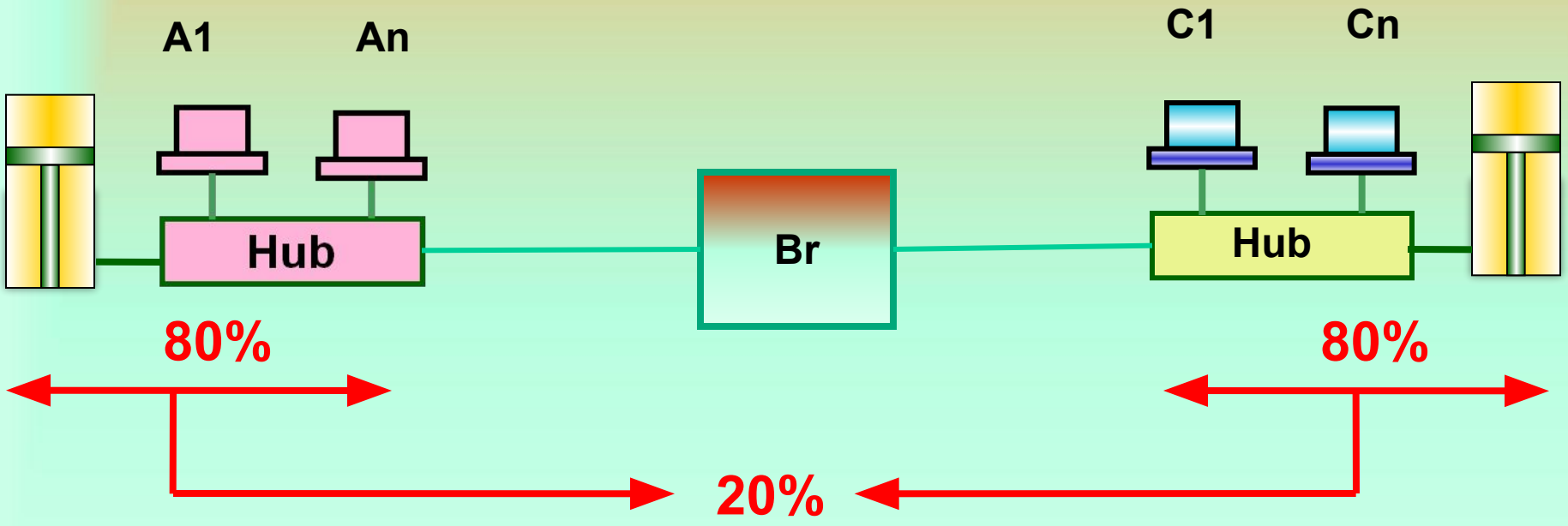
Структура КС при групповом и широковещательном трафике

Сегментация КС с помощью мостов

Существует эмпирическое правило 80/20, которое используется при проектировании сетей с мостами. Согласно этому правилу **использование мостов наиболее эффективно, если 80% трафика сосредоточены в локальном сегменте, а 20% необходимо перенаправлять мостом в другие сегменты**

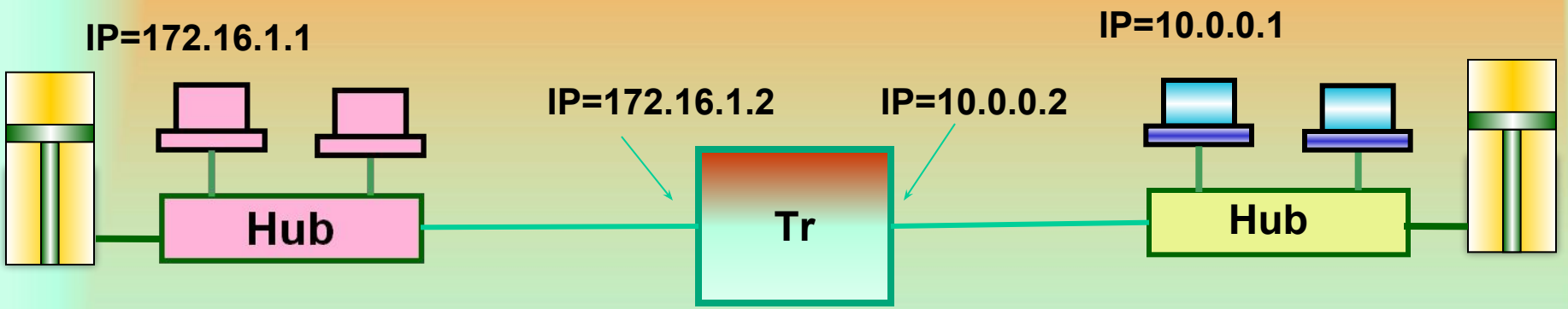
К достоинствам мостов следует отнести их способность не пропускать в другие сегменты фреймы, содержащие ошибки.

Сегментация КС с помощью мостов



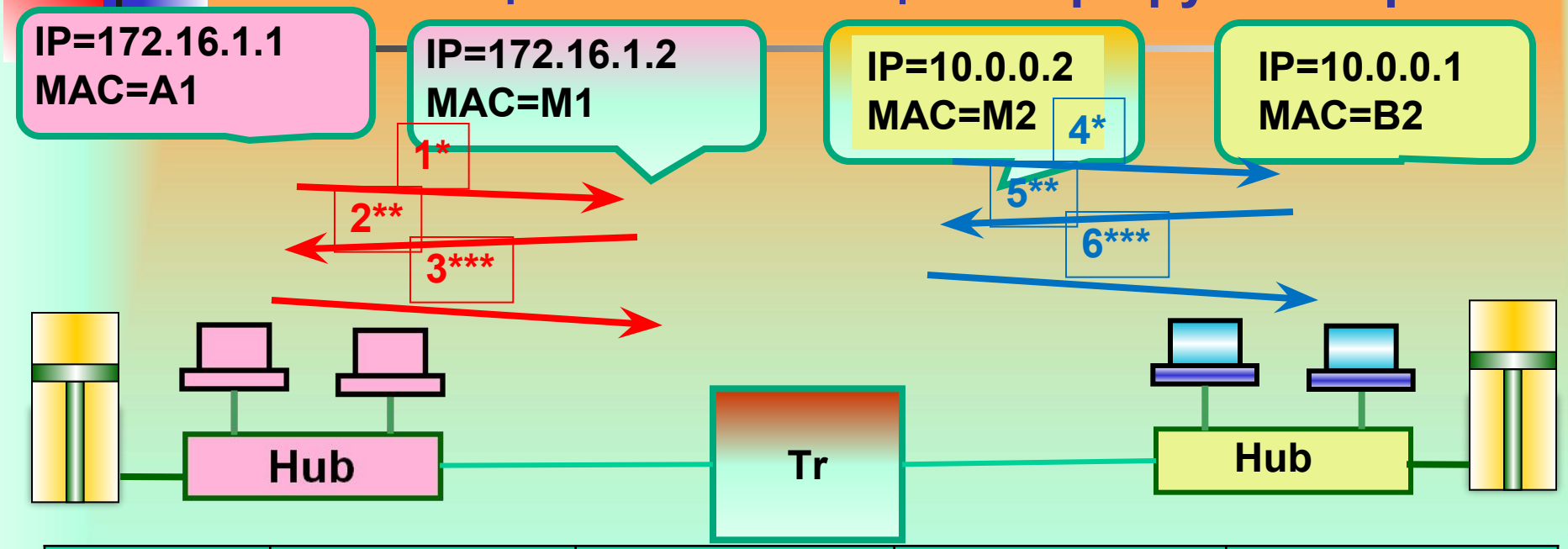
Правило 80/20

Сегментация КС с помощью маршрутизаторов



Маршрутизаторы, при использовании их для сегментации КС ограничивают распространение широковещательных и групповых фреймов. В такой КС каждый сегмент должен принадлежать отдельной подсети

Сегментация КС с помощью маршрутизаторов



№ Фрейма	MAC-получателя	MAC-отправителя	IP- получателя	IP-отправителя
1*(ARP-з)	FF… … … FF	A1	172.16.1.2	172.16.1.1
2**(ARP-о	A1	M1	172.16.1.1	172.16.1.2
3***(д)	M1	A1	10.0.0.1	172.16.1.1
4*	FF… … … FF	M2	10.0.0.1	10.0.0.2
5**	M2	B2	10.0.0.2	10.0.0.1
6***	B2	M2	10.0.0.1	172.16.1.1

Сегментация КС с помощью маршрутизаторов

Когда станции A1 надо обменяться информацией со станцией B2, она сравнивает IP адрес получателя со своим IP адресом и определяет, что получатель находится в другой сети. Следовательно коммутацию необходимо осуществлять через маршрутизатор. IP адрес маршрутизатора задан в конфигурации рабочей станции (default router). Чтобы переслать маршрутизатору информацию отправитель должен адресовать сообщение маршрутизатору на втором уровне с использованием MAC адреса. Для определения MAC адреса маршрутизатора отправитель сначала посылает ARP запрос маршрутизатору (фрейм 1*)

Сегментация КС с помощью маршрутизаторов

Когда фрейм поступает в маршрутизатор, то для станции с MAC=A1 формируется ответ машрутизатора, который содержит MAC-адрес маршрутизатора. На основании этого ответа станция формирует полноценный фрейм с данными который содержит MAC-адрес маршрутизатора. В примере сеть в которой находится получатель напрямую присоединена к маршрутизатору. Маршрутизатор посылает ARP запрос для станции B2. Станция формирует ответ маршрутизатору, который в качестве адреса отправителя содержит MAC адрес станции B2. Получив этот фрейм, маршрутизатор формирует полноценный фрейм данных с MAC адресом получателя B2.

Сегментация КС с помощью маршрутизаторов

Важно отметить, что при прохождении фрейма через маршрутизатор изменяются MAC-адреса (заголовки канального уровня) фреймов. IP –адреса остаются неизменными. Так же как и мосты маршрутизаторы предотвращают прохождение фреймов, содержащих ошибки в сеть получателя.

ARP-протокол разрешения адресов.

Address Resolution Protocol-взаимное преобразование MAC и IP адресов.
Этот протокол обеспечивает формирование (динамически) хостом списки соответствия между MAC и IP адресами хостов. Для получения MAC-адреса узла получателя (в пределах подсети) хост посылает кадр с широковещательным MAC-адресом, в который вкладывает запрос, содержащий IP-адрес получателя. На этот запрос отзовется узел у которого IP-адрес совпадает с соответствующем полем запроса.

ARP-протокол разрешения адресов.

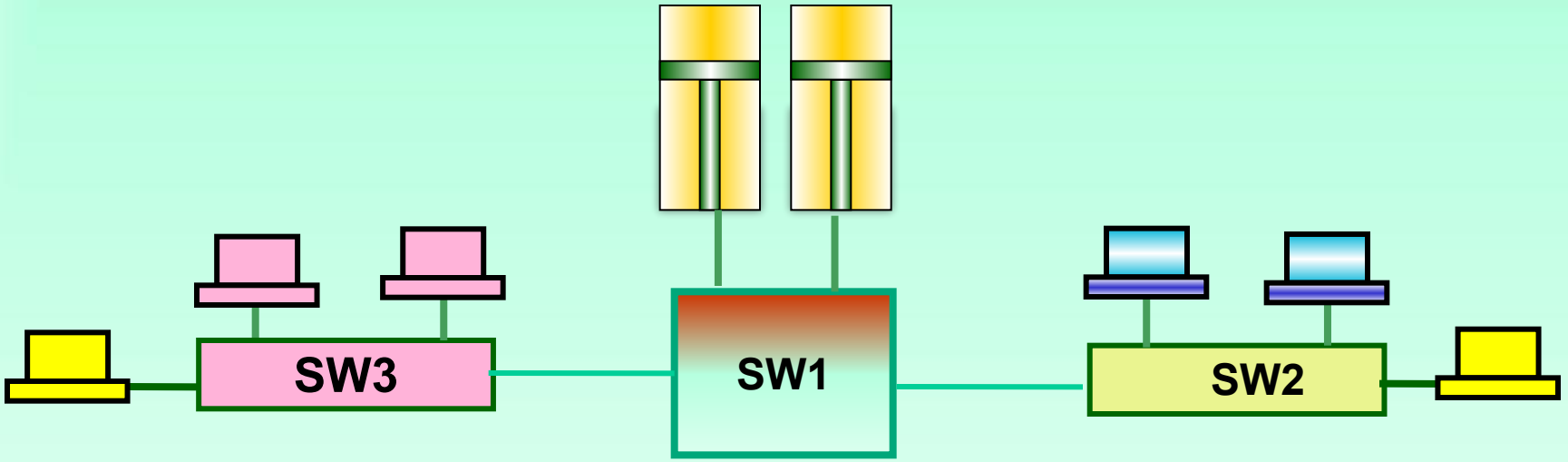
В кадре ответа будет присутствовать искомый MAC-адрес, который и будет занесен в ARP таблицу. ARP –запрос формируется узлом в том случае, когда ему нужно передать пакет по адресу, отсутствующему в его локальной таблице. Если ответ на ARP-запрос не получен, то пакет, который должен быть передан, аннулируется

Сегментация КС с помощью коммутаторов

Коммутаторы (как модернизированные мосты) появились в начале 90-х годов, как результаты работ фирмы Kalpana.
Простые коммутаторы ведут себя как мосты.
Более сложные устройства позволяют сконфигурировать коммутатор так, что различные порты будут принадлежать различным широковещательным доменам. Такая настройка обеспечивает изоляцию широковещательных сообщений. Такие коммутаторы позволяют создавать виртуальные локальные сети (VLAN)

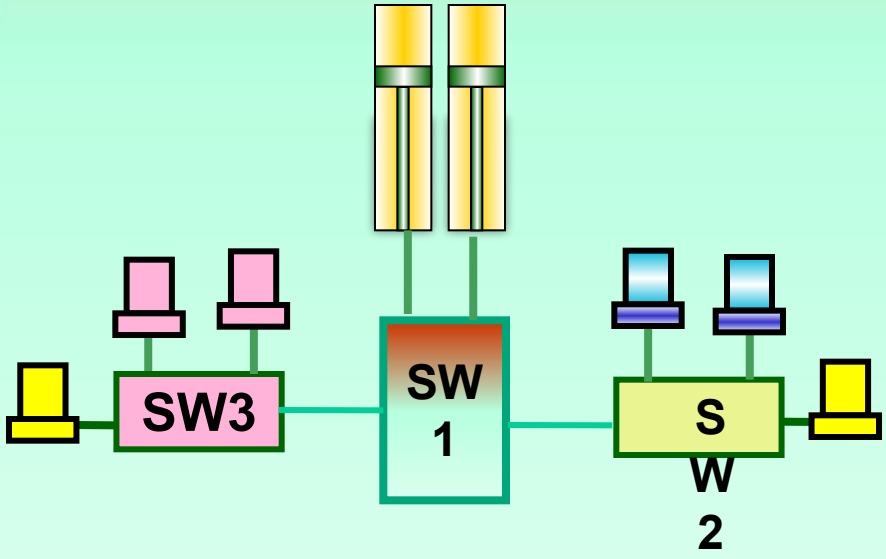
Сегментация КС с помощью коммутаторов

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.



Сегментация КС с помощью коммутаторов

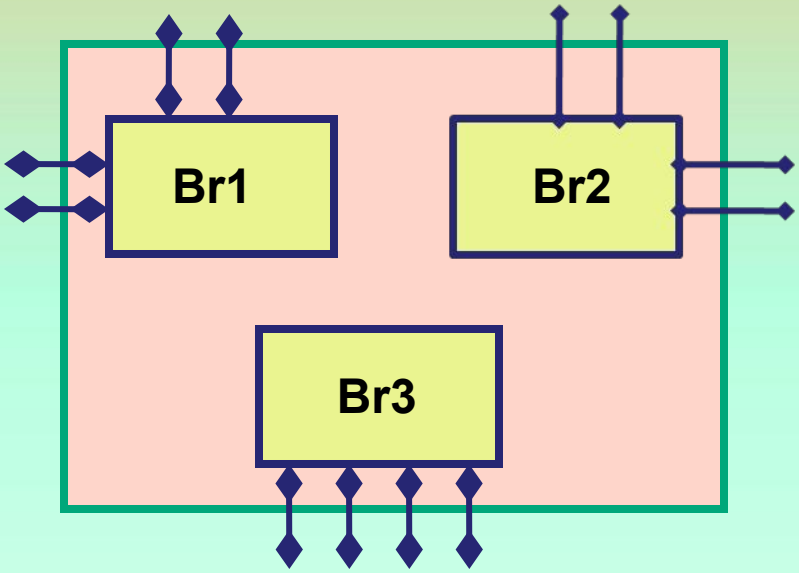
И наоборот, устройства, находящиеся в разных VLAN'ах, невидимы друг для друга на канальном уровне, даже если они подключены к одному коммутатору, и связь между этими устройствами возможна только на сетевом и более высоких уровнях.



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

Сегментация КС с помощью коммутаторов

Коммутатор можно представить как совокупность изолированных друг от друга мостов



При создании VLAN в коммутаторе активизируется соответствующее количество мостов.

Сегментация КС с помощью коммутаторов

Современный подход к построению компьютерных сетей :

«Коммутаторы – по возможности, маршрутизаторы - по необходимости».

Основные цели, которые стараются достичь при построении ВЛВС заключаются в следующем:

- **Повышение полезной пропускной способности за счет локализации широковещательного трафика.**
- **Возможность формирования виртуальных рабочих групп из некомпактно расположенных узлов.**
- **Обеспечение безопасности.**
- **Увеличение соотношения цена/производительность по сравнению с применением маршрутизаторов.**

Сегментация КС с помощью коммутаторов

Основным средством создания ВЛСВ служат интеллектуальные коммутаторы, которые позволяют реализовать следующие подходы к построению ВЛВС:

1. Сеть по портам коммутаторов (port-based VLAN). Каждому порту назначается принадлежность к конкретной VILAN. Это самая простая организация (Layer 1 VLAN). Статическое конфигурирование каждого порта выполняется вручную. Для подключения общедоступного узла (например сервера) необходима возможность назначения одному порту принадлежности нескольким ВЛВС (что позволяют далеко не всякие коммутаторы).

Сегментация КС с помощью коммутаторов

2. Сеть по спискам MAC - адресов (Layer 2 VILAN). Такой вариант обеспечивает большую гибкость, но сложен в первоначальной установке. Перемещение по сети отдельных узлов будет отслеживаться коммутатором автоматически.

3. ВЛВС по типу протокола (802.1Q) - Protocol based VLAN. Принадлежность кадра к определенной ВЛВС определяется значением одного из полей заголовка кадра. (Layer 2 VILAN).

4. ВЛВС, работающие на основе информации третьего уровня (Layer 3 VLAN). Повторяется архитектура с маршрутизаторами.

Сегментация КС с помощью коммутаторов

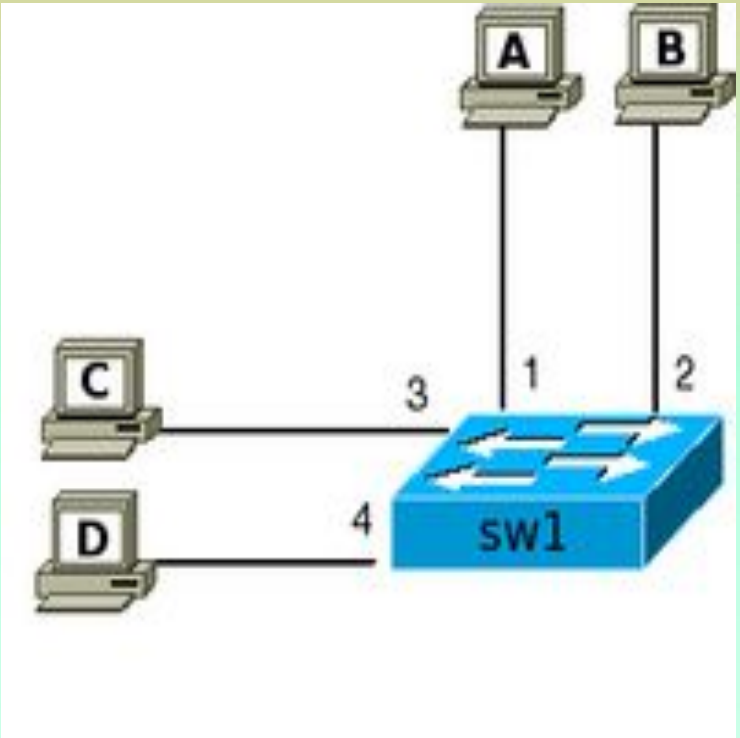
5. ВЛВС для кадров группового трафика на основании протокола IGMP

6. ВЛВС по правилам (Polycy based VILAN). Позволяет комбинировать различные правила организации ВЛВС. Это самый мощный механизм реализации виртуальных сетей.

Сегментация КС с помощью коммутаторов

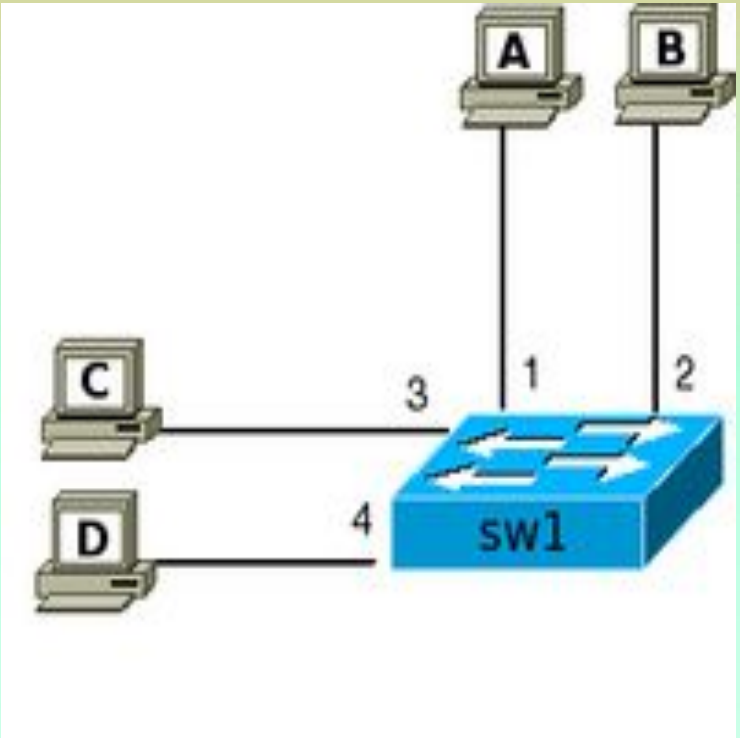
Рассмотрим работу коммутатора.

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.



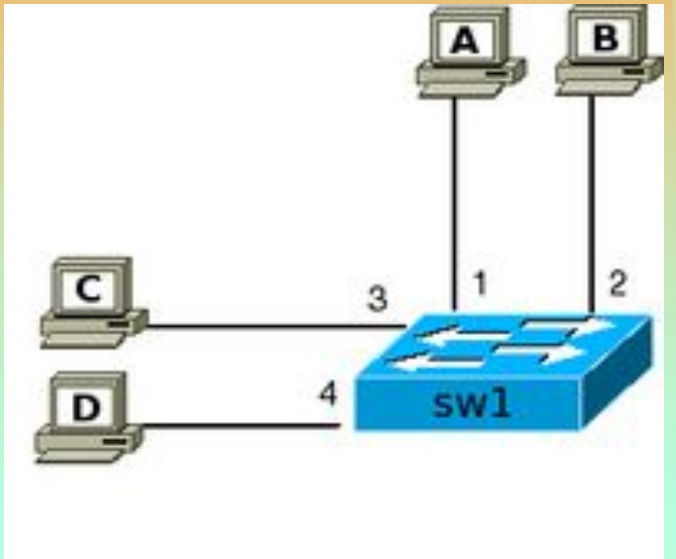
Сегментация КС с помощью коммутаторов

Для того чтобы передавать фреймы, коммутатор использует таблицу коммутации.
Изначально, после включения коммутатора таблица пуста.
Заполняет её коммутатор автоматически, при получении фреймов от хостов.
Когда коммутатор получает фрейм от хоста, он сначала передает его в соответствии со своими правилами, а затем запоминает MAC-адрес отправителя во фрейме и ставит его в соответствие порту на котором он был получен.



Сегментация КС с помощью коммутаторов

Для изображенной схемы, итоговая таблица коммутации будет иметь следующий вид (после того как все хосты передавали какой-то трафик):



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

Сегментация КС с помощью коммутаторов

Механизмы передачи фреймов

Для того чтобы передавать фреймы коммутатор использует три базовых механизма:

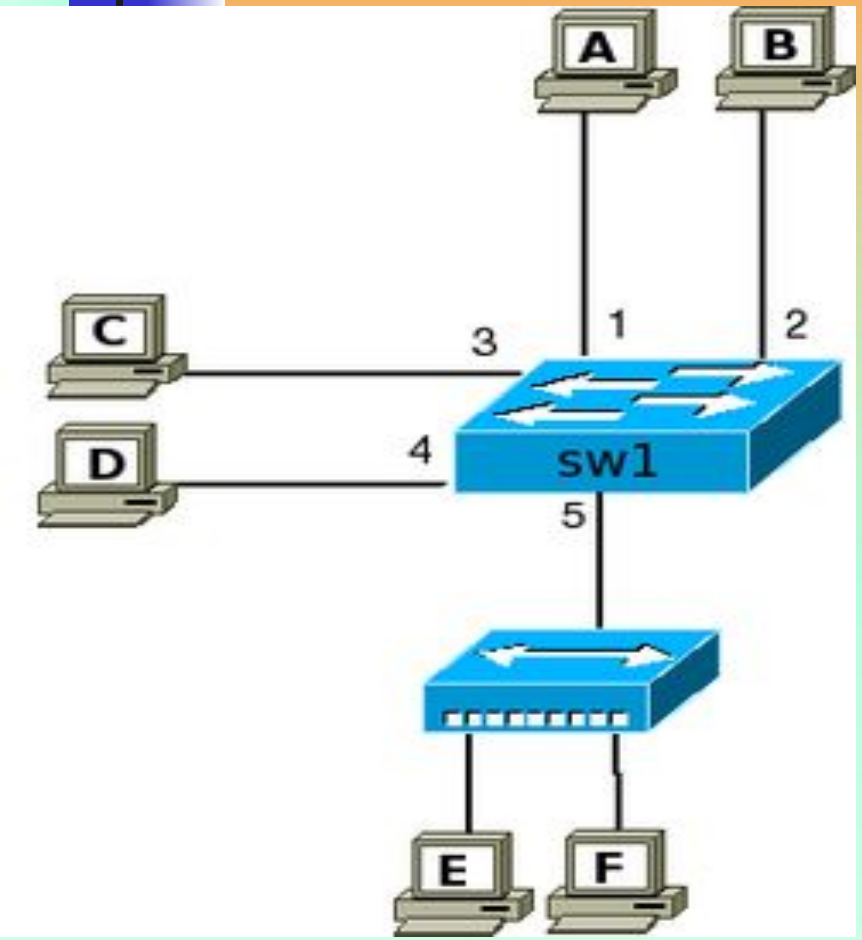
Flooding — фрейм полученный на один из портов передается на остальные порты коммутатора. Коммутатор выполняет эту операцию в двух случаях:

- **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.

Сегментация КС с помощью коммутаторов

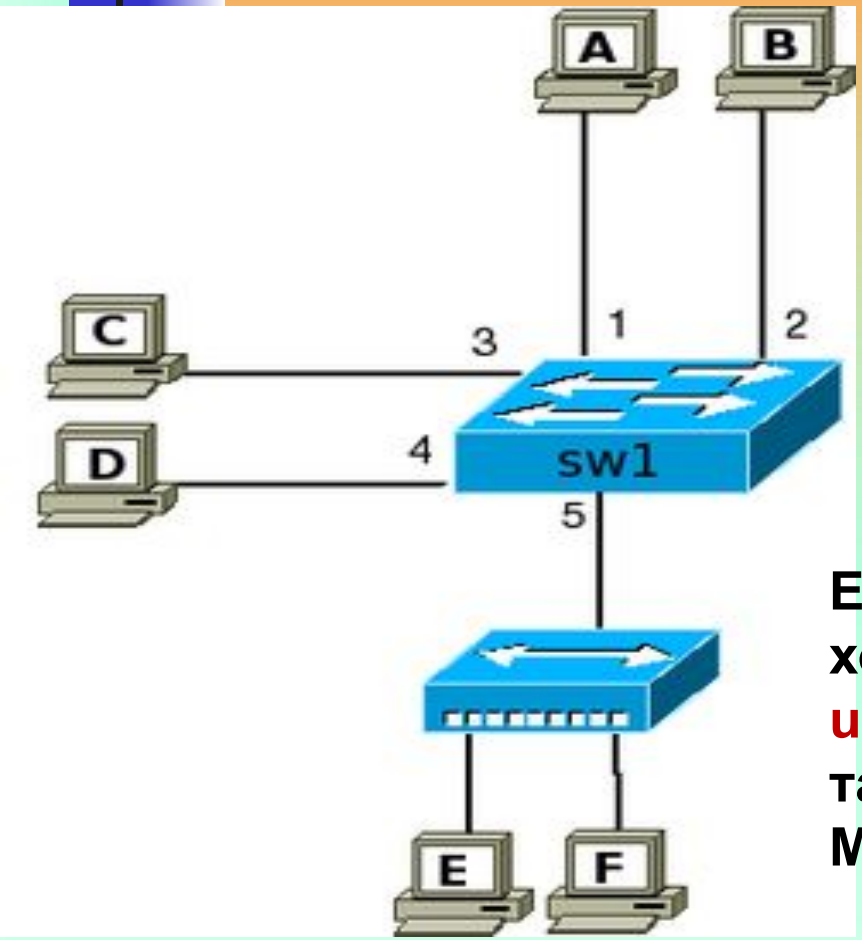


Изначально к коммутатору были подключены три хоста A, B и C. Соответственно у коммутатора будет следующая таблица коммутации:

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

Когда хост A отправляет фрейм хосту B, коммутатор использует механизм forwarding, так как ему известно где находятся оба хоста и хосты находятся на разных портах коммутатора.

Сегментация КС с помощью коммутаторов



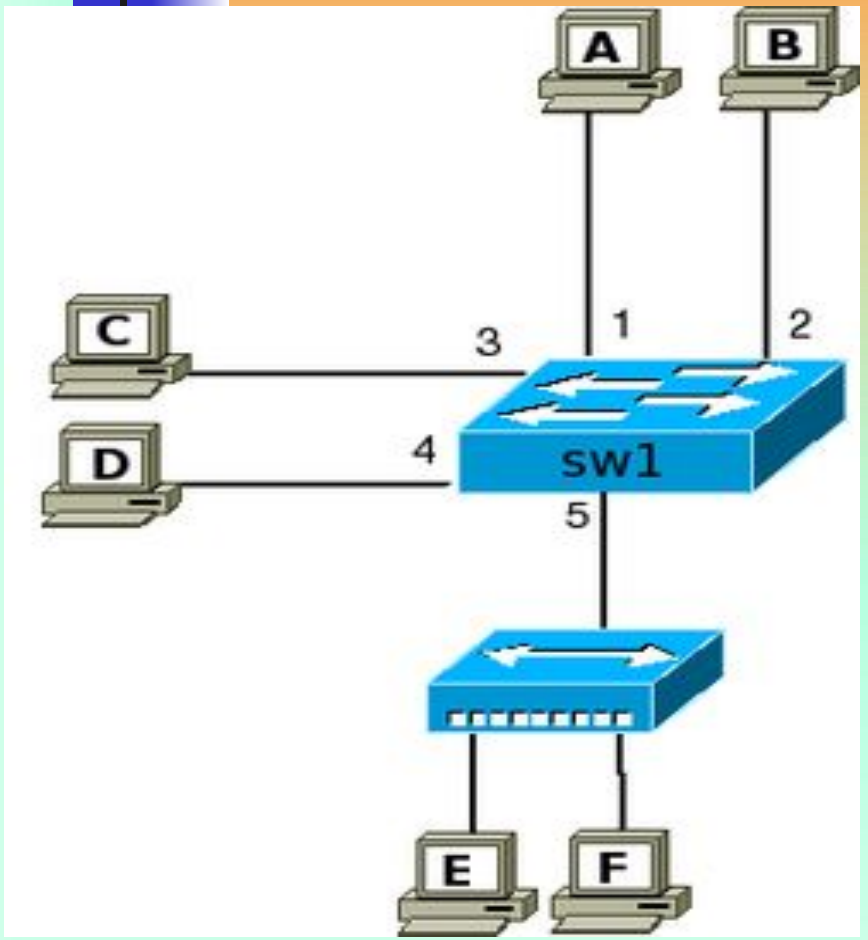
Далее к коммутатору подключили хост D.

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

Если хост A отправляет фрейм хосту D, то для коммутатора это unknown unicast фрейм, так как в таблице коммутации нет записи о MAC-адресе D.

В соответствии со своими правилами коммутатор выполняет flooding и передает фрейм на все порты, кроме 1 (с которого фрейм был получен).

Сегментация КС с помощью коммутаторов

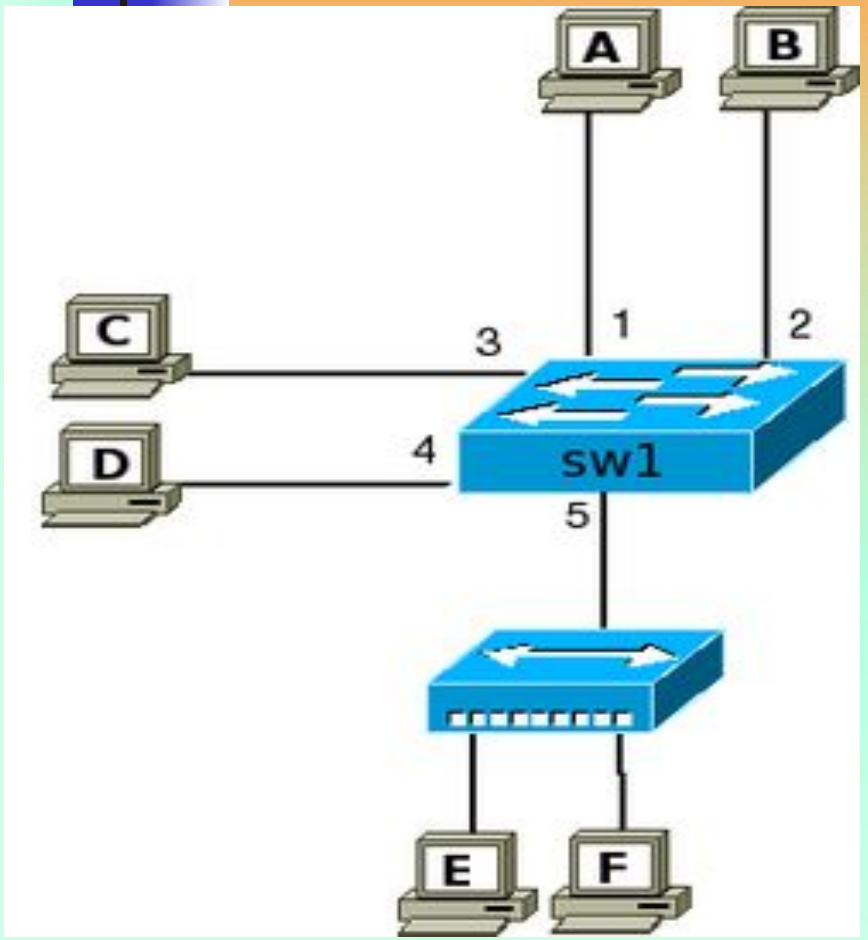


После того как коммутатор получит фрейм от хоста D, он запомнит его адрес и создаст соответствующую запись в таблице коммутации.

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

К коммутатору подключили повторитель с двумя хостами и коммутатор выучил их адреса.

Сегментация КС с помощью коммутаторов

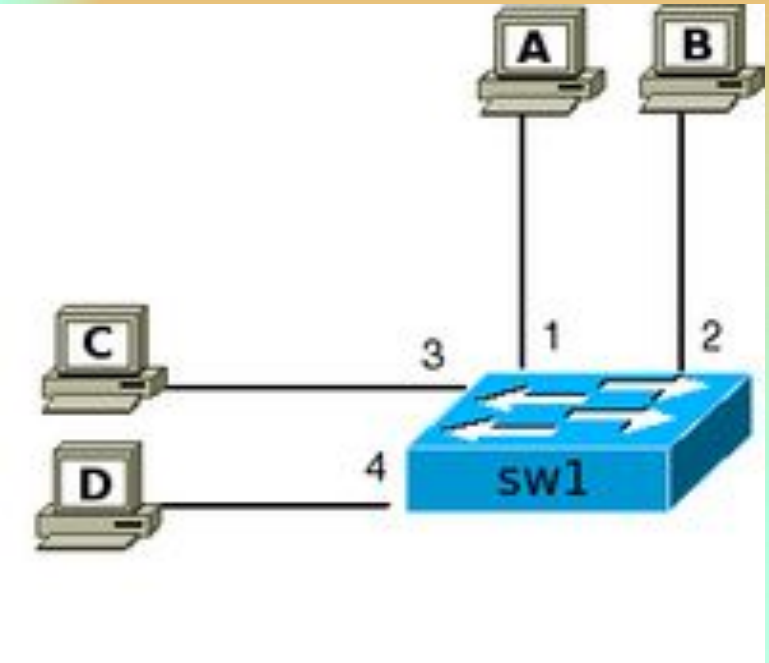


Если после этого хост E будет передавать фрейм хосту F, то коммутатор получит его, но не будет передавать далее.

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

В этой ситуации коммутатор использует механизм filtering, так как MAC-адрес получателя доступен через тот же порт, что и отправитель.

Сегментация КС с помощью коммутаторов

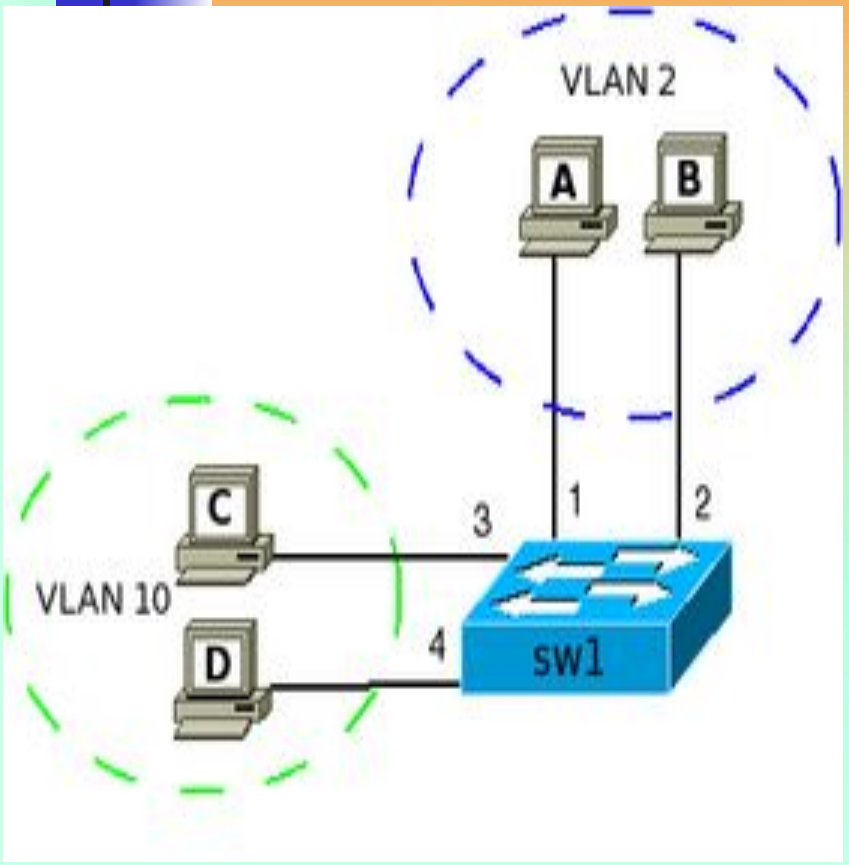


Хосты в одном VLAN на одном коммутаторе

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

К коммутатору подключены 4 хоста. Пусть A, B, C и D это соответствующие MAC-адреса хостов. По умолчанию все порты коммутатора считаются нетегированными членами VLAN 1

Сегментация КС с помощью коммутаторов



Хосты в разных VLAN на одном коммутаторе

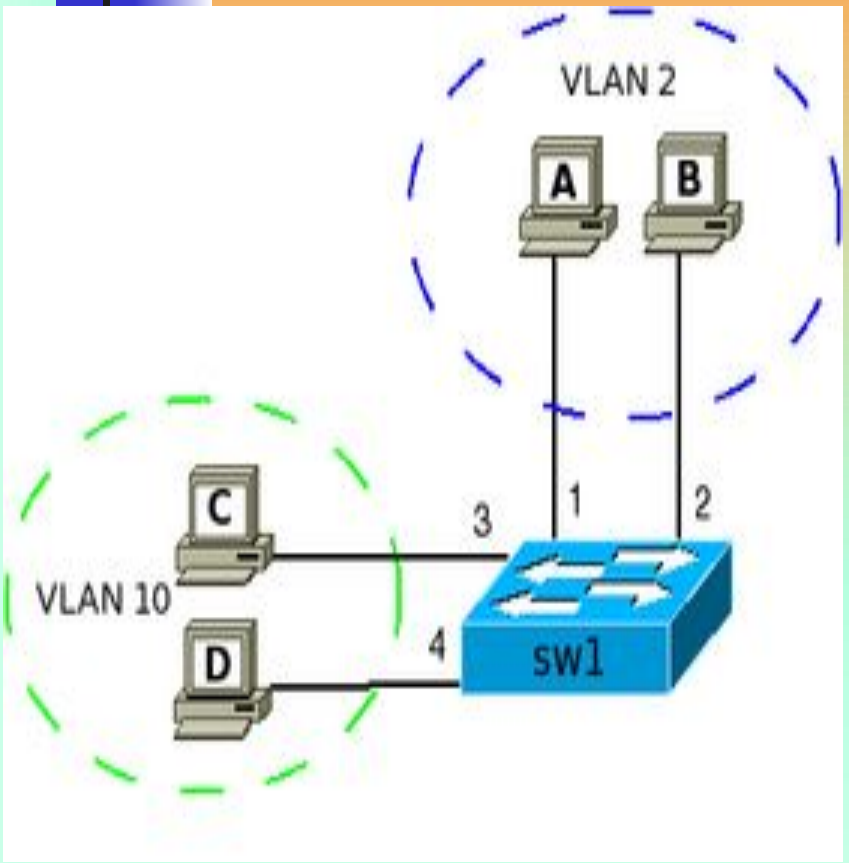
На коммутаторе настроены два VLAN'а, все порты настроены как нетегированные (access-порты в терминологии Cisco) в соответствующих VLAN.

После этого на коммутаторе существуют две таблицы коммутации.

Порт коммутатора	MAC-адрес хоста
1	A
2	B

Порт коммутатора	MAC-адрес хоста
3	C
4	D

Сегментация КС с помощью коммутаторов

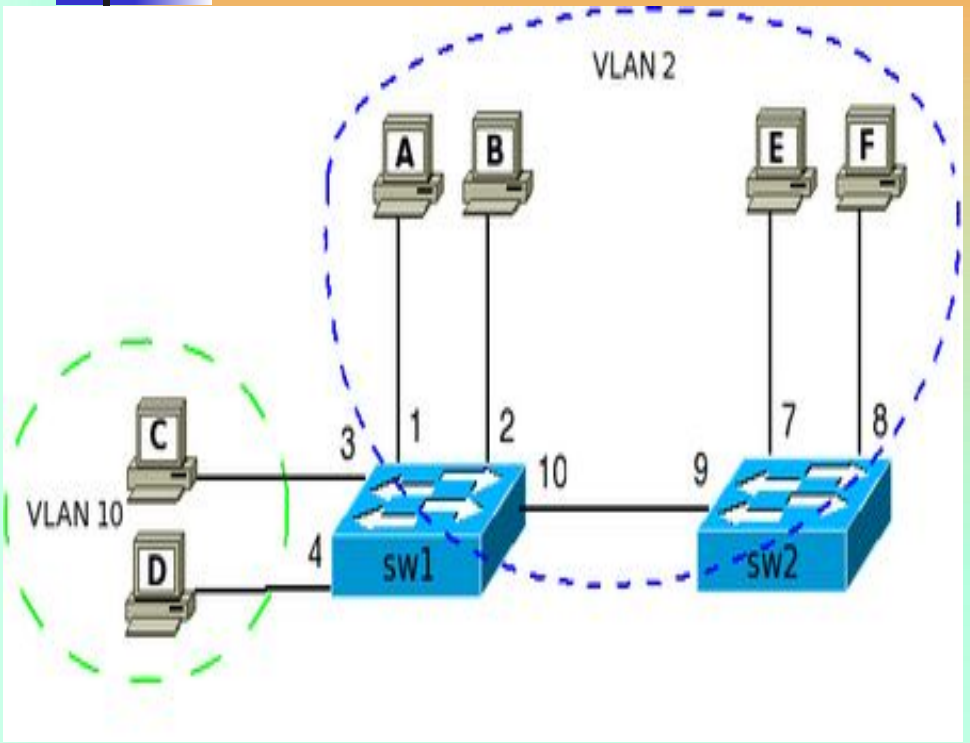


Все базовые механизмы коммутатора остаются точно такими же, как и до разделения на VLAN, но они используются только в пределах соответствующего VLAN.

Например, если хост из VLAN 10 отправляет широковещательный фрейм, то он будет отправлен только на порты в этом VLAN.

Получается, что нетегированные порты это "обычные" порты коммутатора, с возможностью сообщить коммутатору о том, какому VLAN принадлежат порты.
Затем коммутатор использует эту информацию при передаче фреймов.

Сегментация КС с помощью коммутаторов

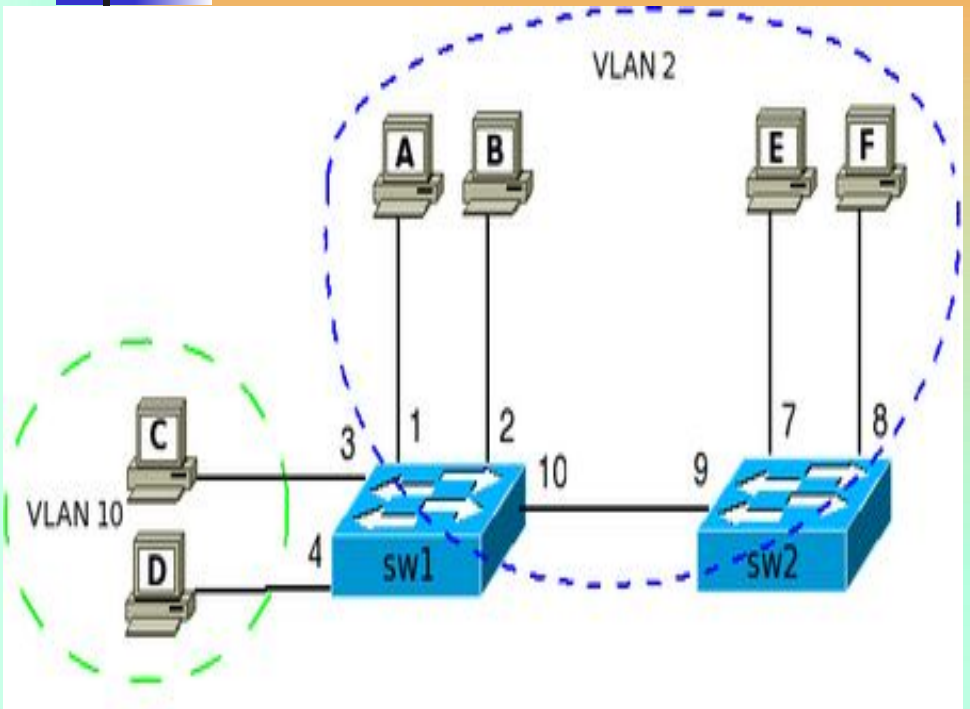


Добавим еще один коммутатор sw2 и два хоста E и F в VLAN 2.
Если рассматривать два коммутатора отдельно, то получается, что на коммутаторе sw1 осталась прежняя таблица коммутации, а на коммутаторе sw2 таблица, пока коммутаторы не соединены, имеет следующий вид:

Порт коммутатора	MAC-адрес хоста
1	A
2	B

Порт коммутатора	MAC-адрес хоста
1	A
2	B

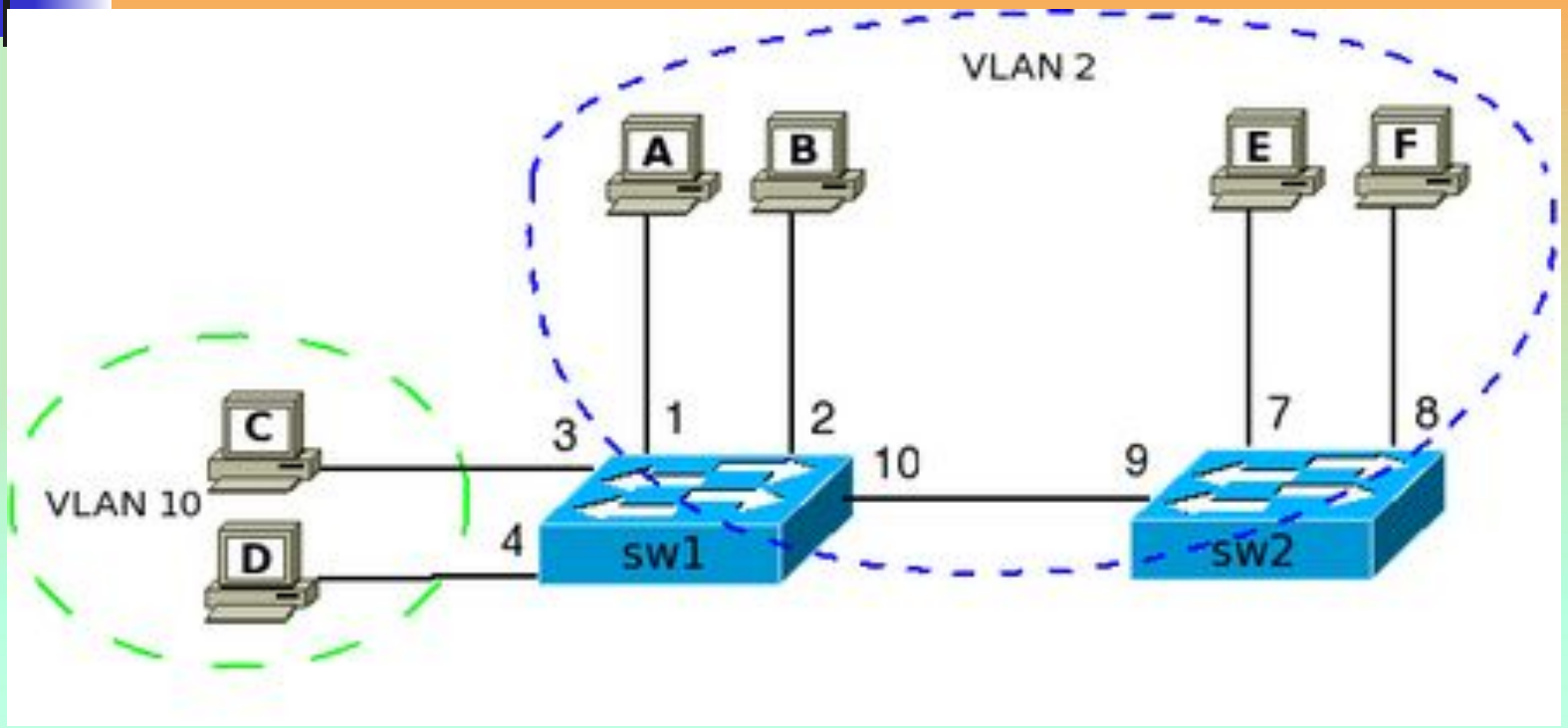
Сегментация КС с помощью коммутаторов



Теперь необходимо чтобы хосты A, B, E, F "увидели" друг друга.
Для этого они должны находиться в одном VLAN.
То есть, необходимо указать коммутатору, что ещё есть хосты в соответствующем VLAN'е.

В нашем случае необходимо 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. 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.

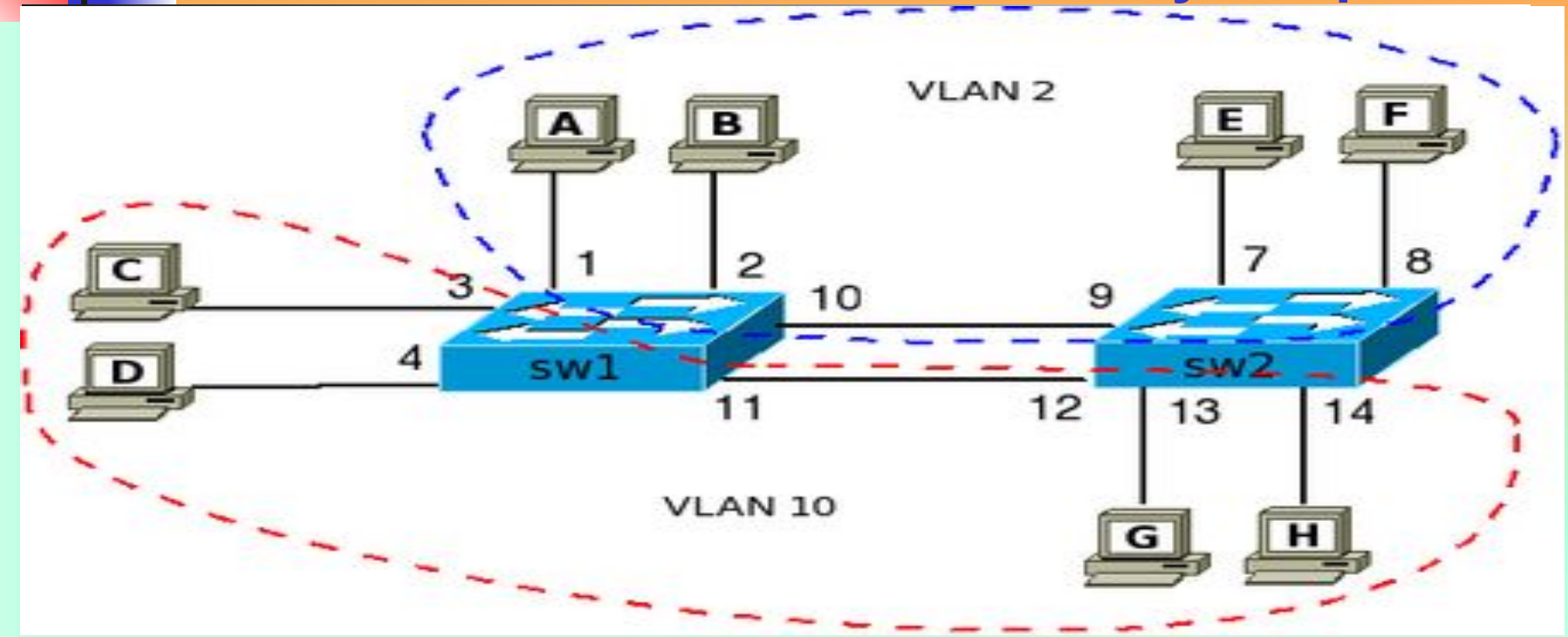
Сегментация КС с помощью коммутаторов



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

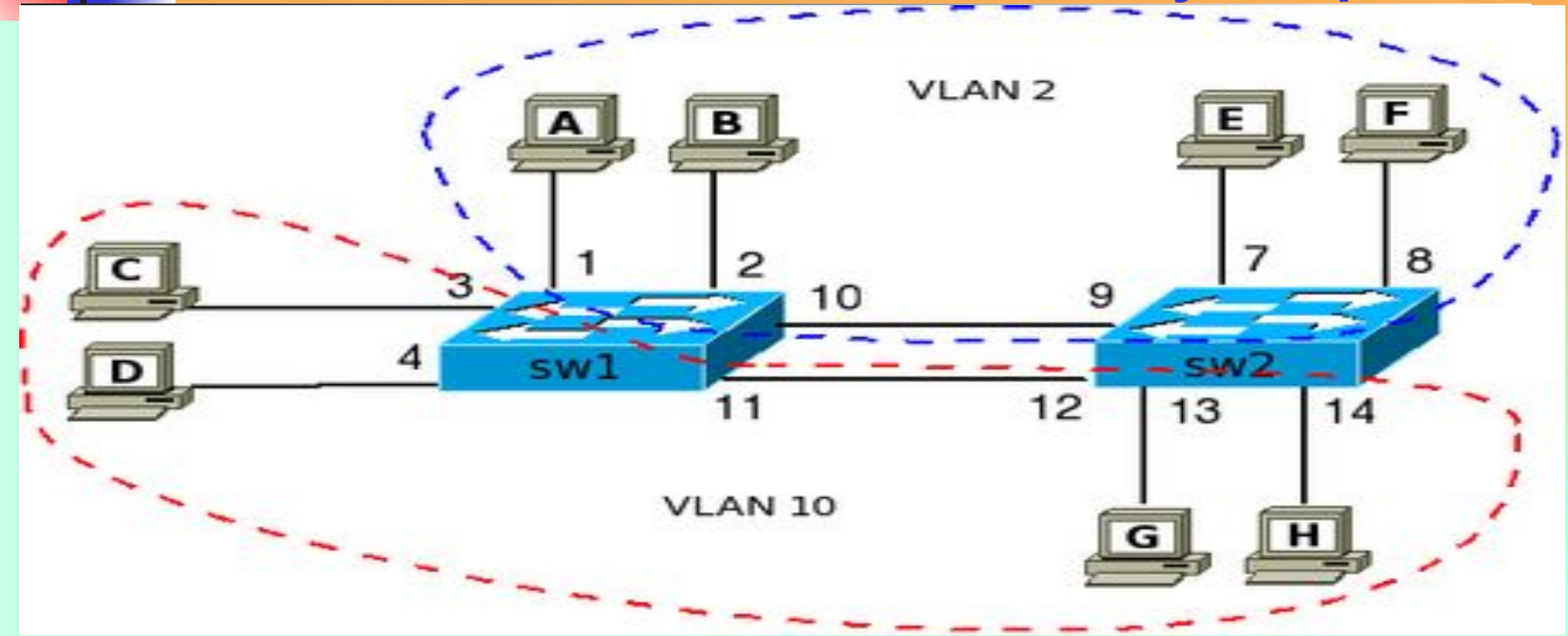
Порт коммутатора	MAC-адрес хоста
7	E
8	F
9	A
9	B

Сегментация КС с помощью коммутаторов



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.

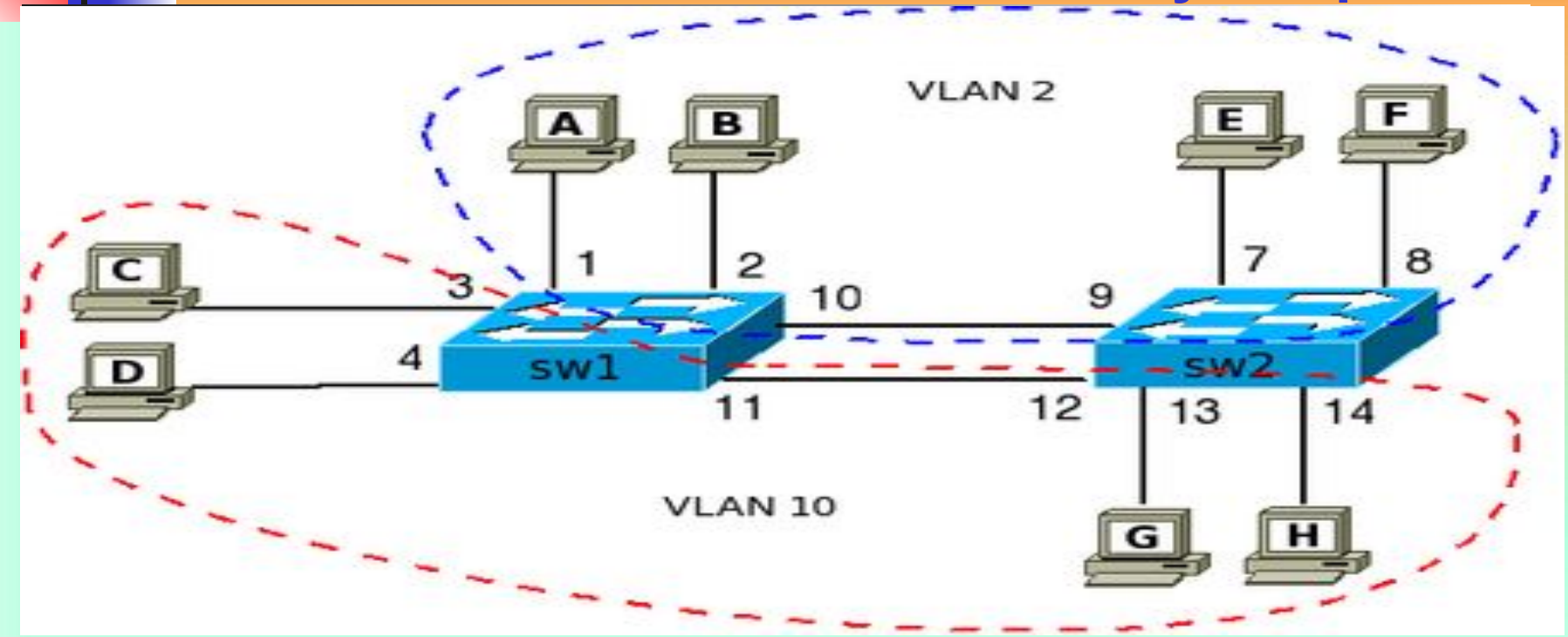
Сегментация КС с помощью коммутаторов



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

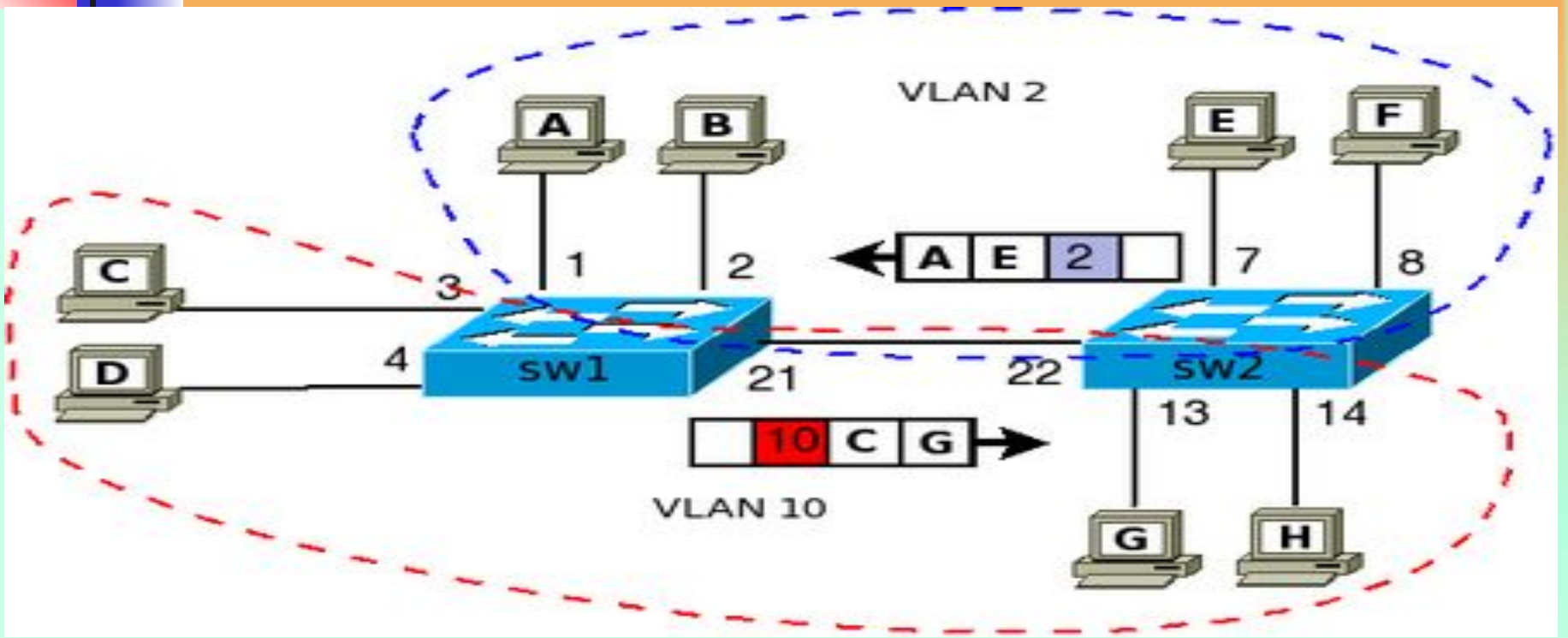
Порт коммутатора	MAC-адрес хоста
13	G
14	H
12	C
12	D

Сегментация КС с помощью коммутаторов



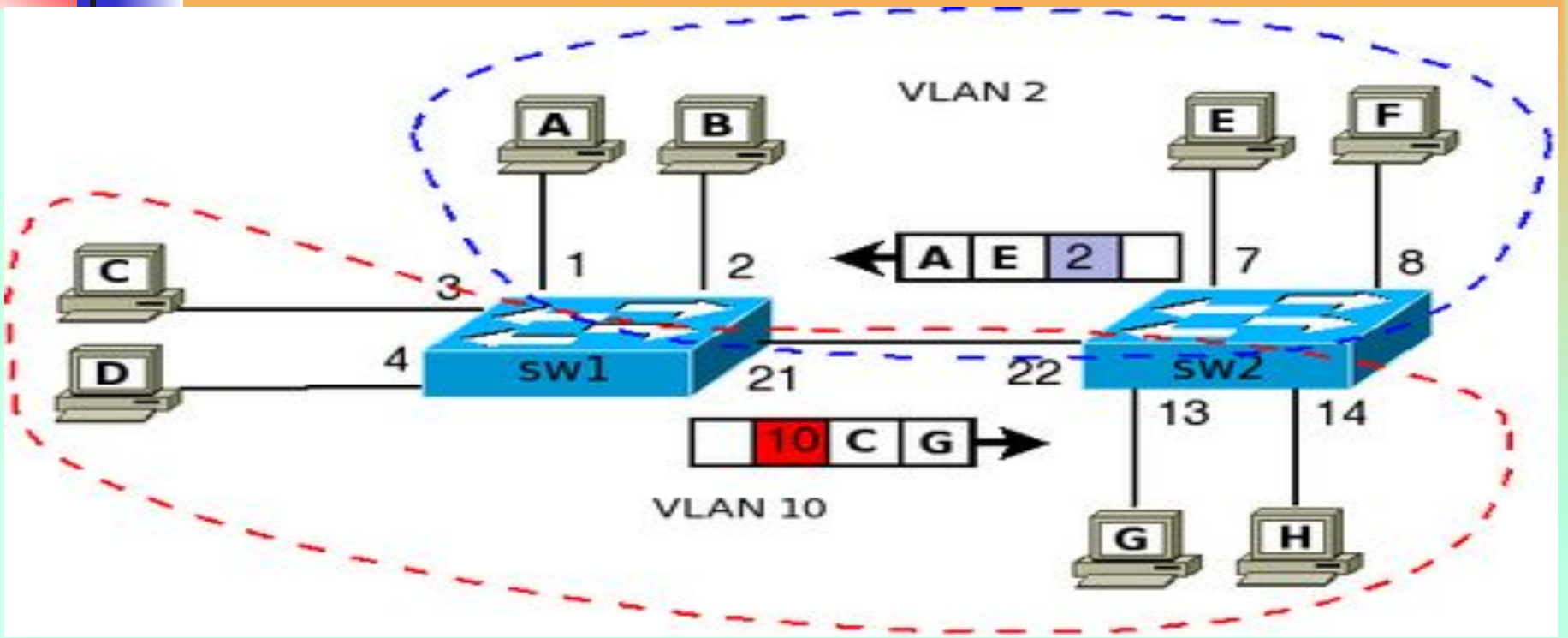
Когда количество VLAN возрастает, то схема становится неудобной, так как для каждого VLAN надо добавлять линк между коммутаторами для того, чтобы объединить хосты в один широковещательный сегмент.

Сегментация КС с помощью коммутаторов



Для устранения избыточности связей используют тегированные порты.
Тегированный порт позволяет коммутатору передать трафик нескольких VLAN'ов через один порт и сохранить при этом информацию о том, какой VLAN принадлежит передаваемый фрейм.

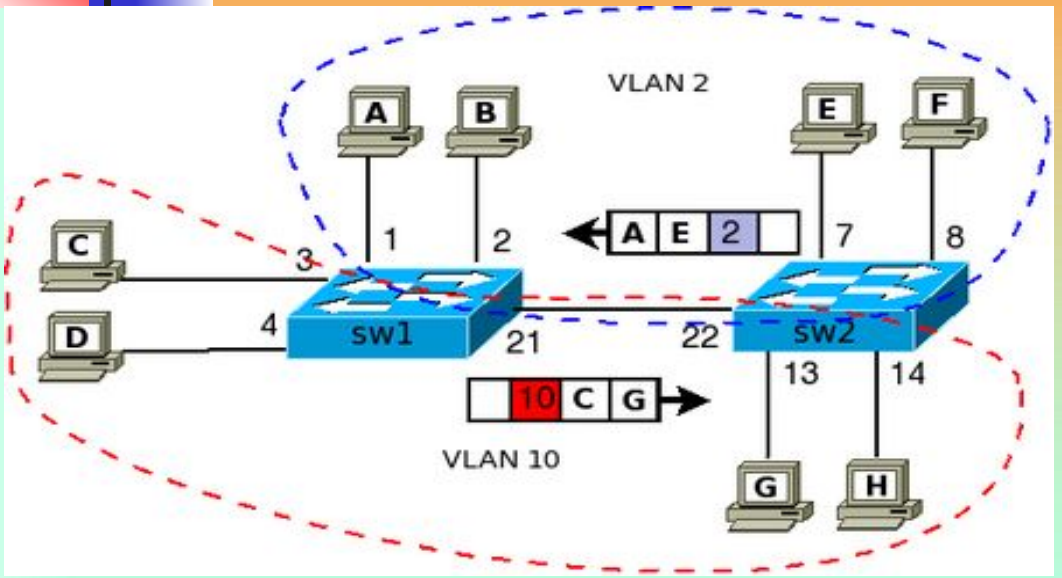
Сегментация КС с помощью коммутаторов



На коммутаторах sw1 и sw2 порты 21 и 22, соответственно, это тегированные порты.

Для того чтобы коммутаторы понимали какому VLAN принадлежит пришедший фрейм и использовали соответствующую таблицу коммутации для его обработки, выполняется тегирование фрейма.

Сегментация КС с помощью коммутаторов



Остальные порты коммутатора остаются нетегированными. Для хостов операция тегирования, которую выполняют коммутаторы абсолютно прозрачна. Хосты ничего не знают о тегах и получают обычные фреймы.
Аналогичные действия выполняются, например, при передаче фрейма от хоста С хосту G

Коммутатор sw1 получает тегированный фрейм 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 считывал информацию тега. И соответственно чтобы он также помечал фрейм тегом, когда будет передаваться трафик коммутатору sw2.

Сегментация КС с помощью коммутаторов

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 свичах (например, ZyXEL, D-Link и Planet) данного ограничения нет.

существуют два подхода к назначению порта в определённый VLAN:

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

— когда принадлежность порта VLAN'у оп*Динамическое назначение*ределяется в ходе работы коммутатора с помощью процедур, описанных в специальных стандартах, таких, например, как 802.1Xределяется 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 RADIUSределяется 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

Настройка VLAN на коммутаторах Cisco

Терминология Cisco:

access port — порт принадлежащий одному VLAN'у и передающий нетегированный трафик

trunk port — порт передающий тегированный трафик одного или нескольких VLAN'ов

Сегментация КС с помощью коммутаторов

Для того чтобы настроить маршрутизацию между сетями разных VLAN на коммутаторе необходимо:

1. Включить ip routing
2. Назначить IP-адреса соответствующим VLAN

Кроме того, необходимо чтобы IP-адреса соответствующих VLAN были указаны как маршруты по умолчанию на хостах.

Включение маршрутизации на коммутаторе:

```
sw(config)# ip routing
```

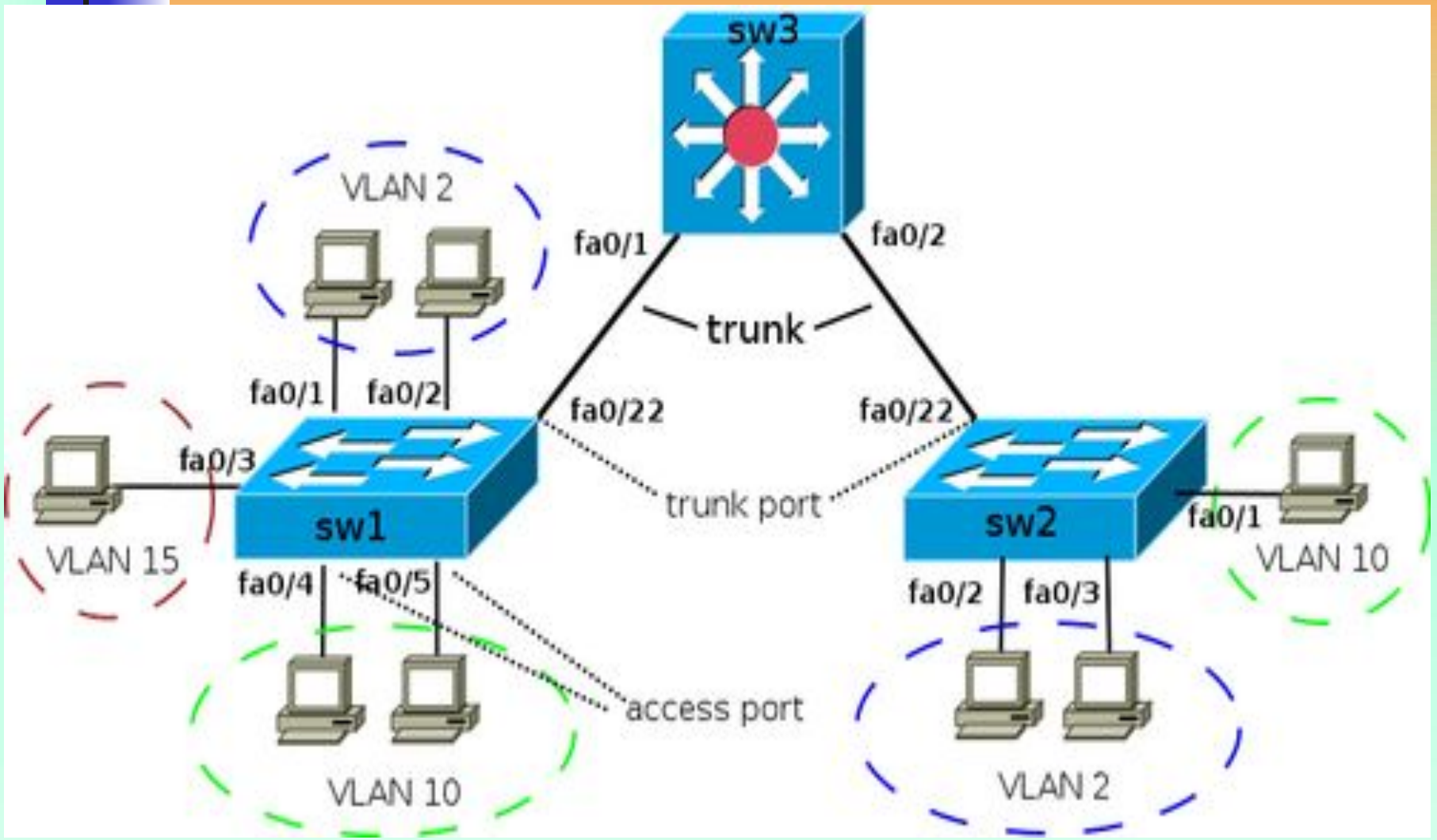
Задание адреса в VLAN. Этот адрес должен быть прописан как маршрут по умолчанию для компьютеров в VLAN 2:

```
sw(config)# vlan 2
sw(vlan-2)# ip address 10.0.2.1/24
```

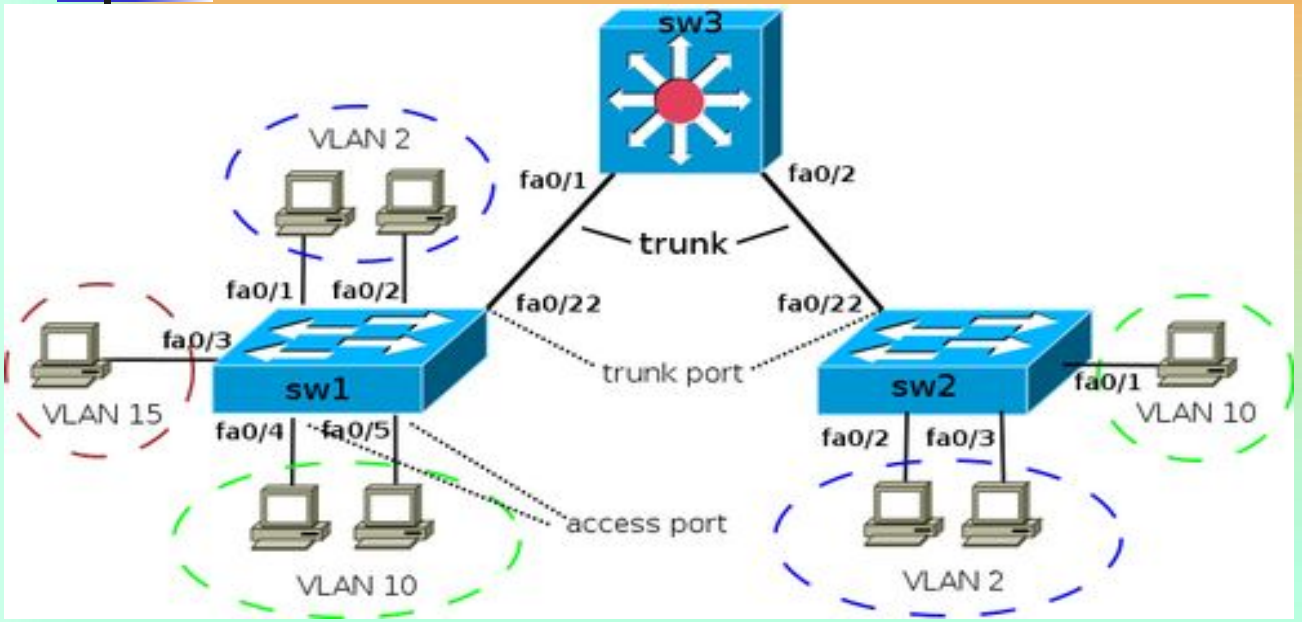
Или, другой формат задания IP-адреса в VLAN:

```
sw(config)# vlan 2 ip address 10.0.2.1/24
```

Настройка VLAN на коммутаторах Cisco



Настройка VLAN на коммутаторах Cisco



Настройка access портов

Назначение порта коммутатора в VLAN:

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

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
```

Настройка VLAN на коммутаторах Cisco

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 VLAN на коммутаторах Cisco

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.

Настройка VLAN на коммутаторах Cisco

Настройка транка (trunk)

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.

Настройка VLAN на коммутаторах Cisco

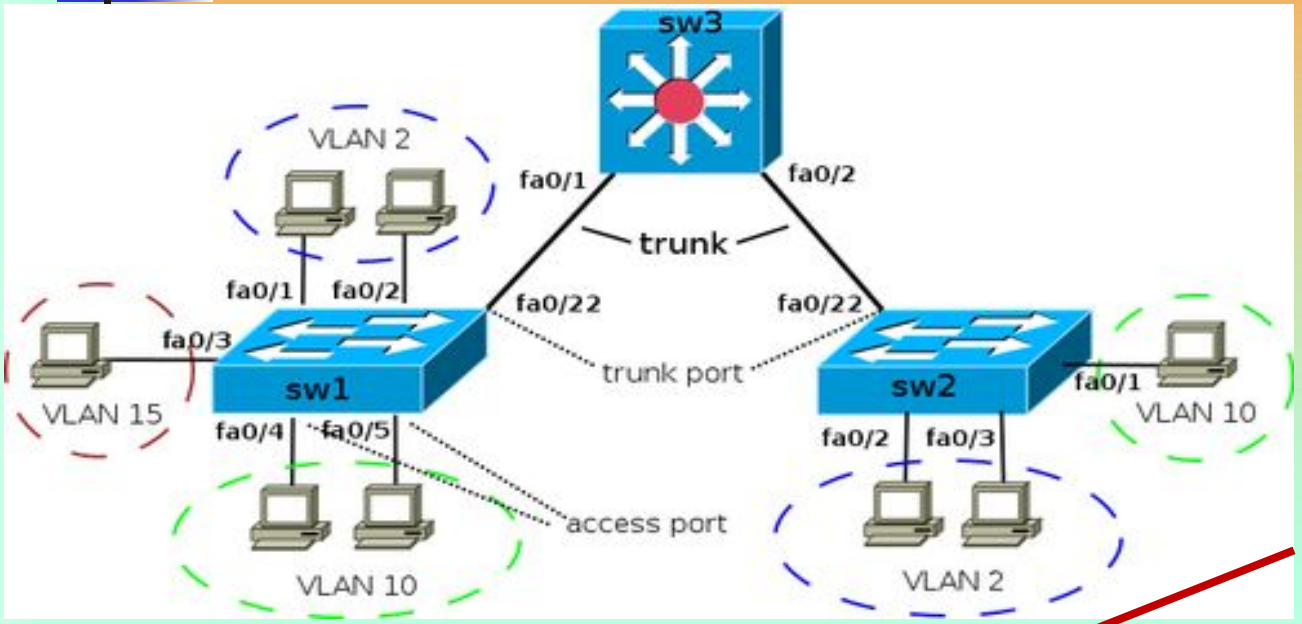
Настройка транка (trunk)

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)

Настройка VLAN на коммутаторах Cisco

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.

Настройка VLAN на коммутаторах Cisco



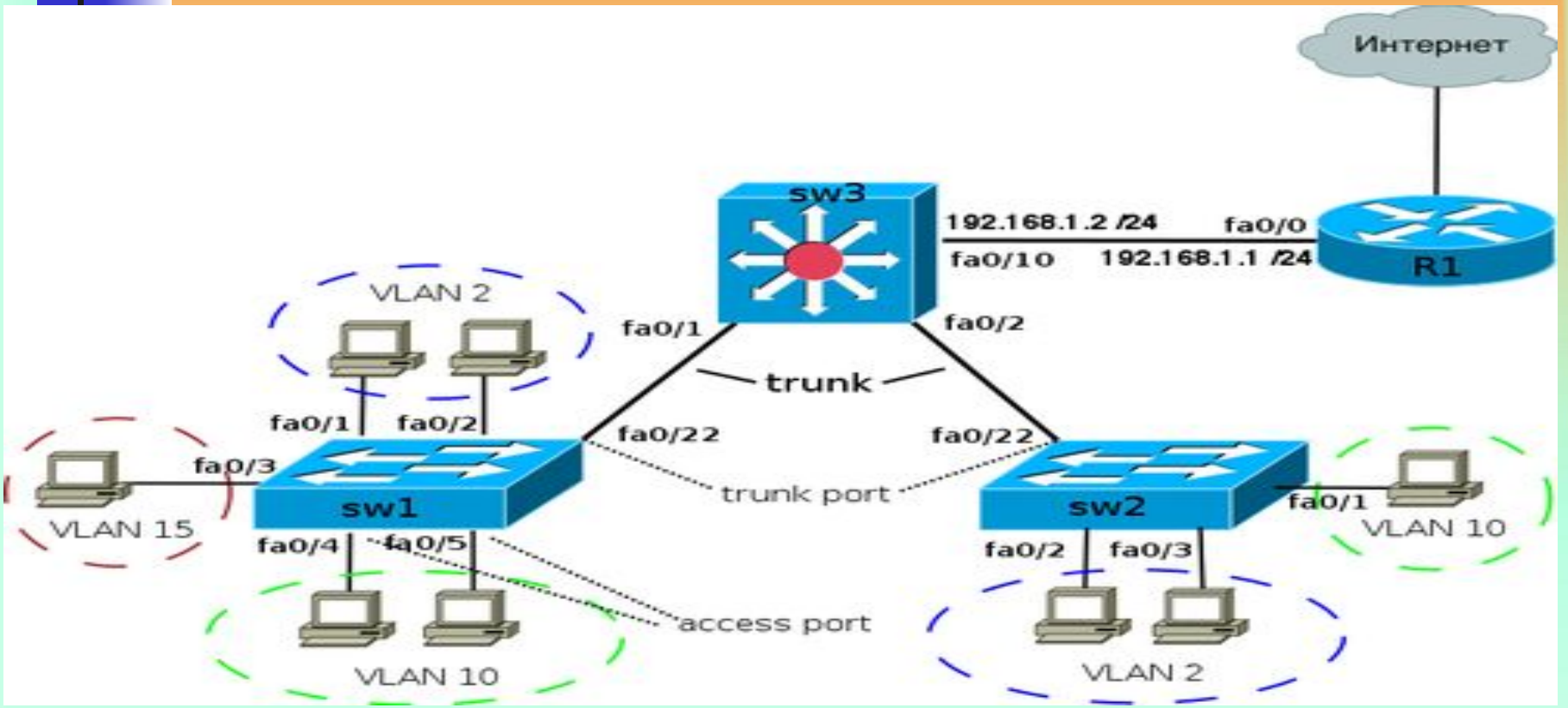
В схеме, на коммутаторах sw1 и sw2, нужные VLAN будут созданы в момент добавления access-портов в соответствующие VLAN.
На коммутаторе sw3 access-портов нет. Поэтому необходимо явно создать все необходимые VLAN:
sw3(config)# vlan 2,10,15

```
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
```

Сегментация КС с помощью коммутаторов

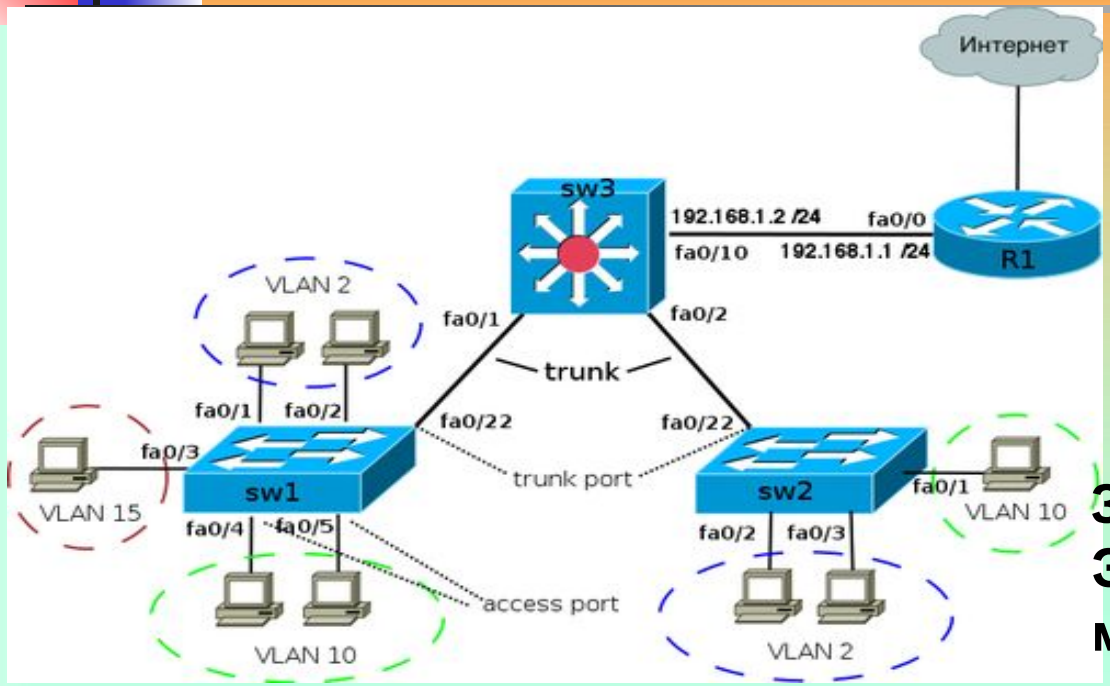
Dynamic Trunk Protocol (DTP) —протокол Cisco, который позволяет коммутаторам динамически распознавать настроен ли соседний коммутатор для поднятия транка и какой протокол использовать (802.1Q или ISL). Включен по умолчанию.

Настройка маршрутизации между VLAN



Все настройки по назначению портов в VLAN, сделанные ранее для sw1, sw2 и sw3, сохраняются. Дальнейшие настройки подразумевают использование sw3 как коммутатора 3 уровня.

Настройка VLAN на коммутаторах Cisco



Включение маршрутизации на коммутаторе:

```
sw3(config)# ip routing
```

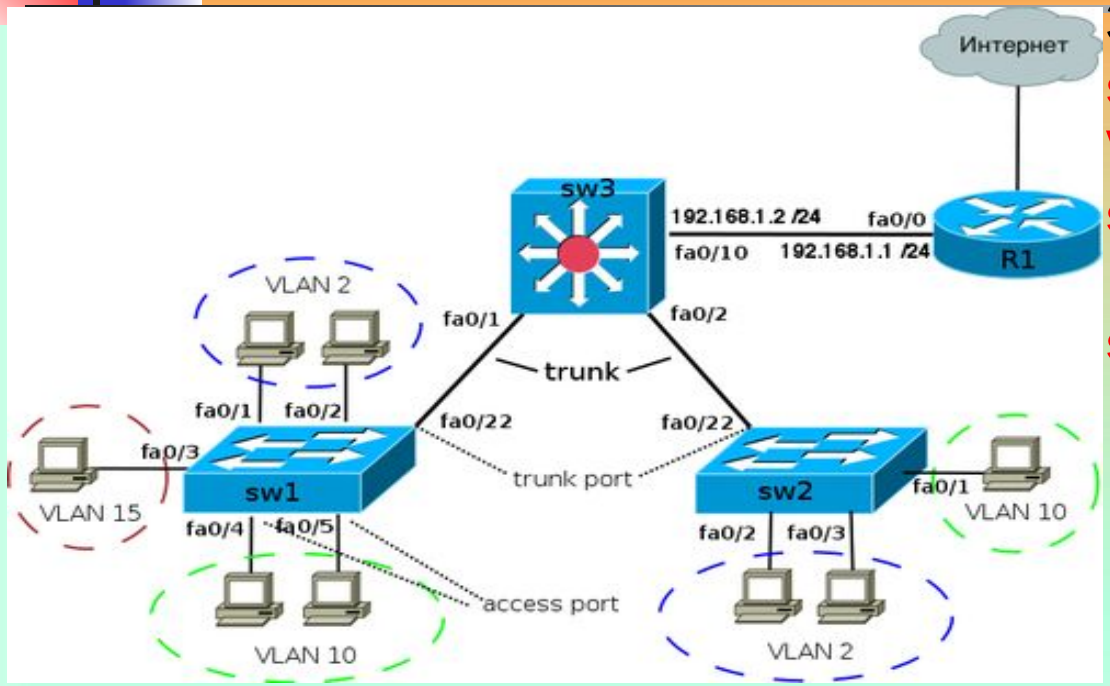
Задание адреса в VLAN. Этот адрес будет маршрутом по умолчанию для компьютеров в VLAN 2:

```
sw3(config)# interface Vlan2
sw3(config-if)# ip address 10.0.2.1 255.255.255.0
sw3(config-if)# no shutdown
```

Настройки на коммутаторе sw3:

VLAN / интерфейс 3го уровня	IP-адрес
VLAN 2	10.0.2.1 /24
VLAN 10	10.0.10.1 /24
VLAN 15	10.0.15.1 /24
Fa 0/10	192.168.1.2 /24

Настройка VLAN на коммутаторах Cisco



Задание адреса в VLAN 10:

```
sw3(config)# interface Vlan10
sw3(config-if)# ip address 10.0.10.1 255.255.255.0
sw3(config-if)# no shutdown
```

Интерфейс fa0/10 соединен с маршрутизатором. Этот интерфейс необходимо перевести в режим 3 уровня. задание IP-адреса:

```
sw3(config)#interface FastEthernet 0/10
sw3(config-if)# no switchport
sw3(config-if)# ip address 192.168.1.2 255.255.255.0
sw3(config-if)# no shutdown
```

Настройки на коммутаторе sw3:

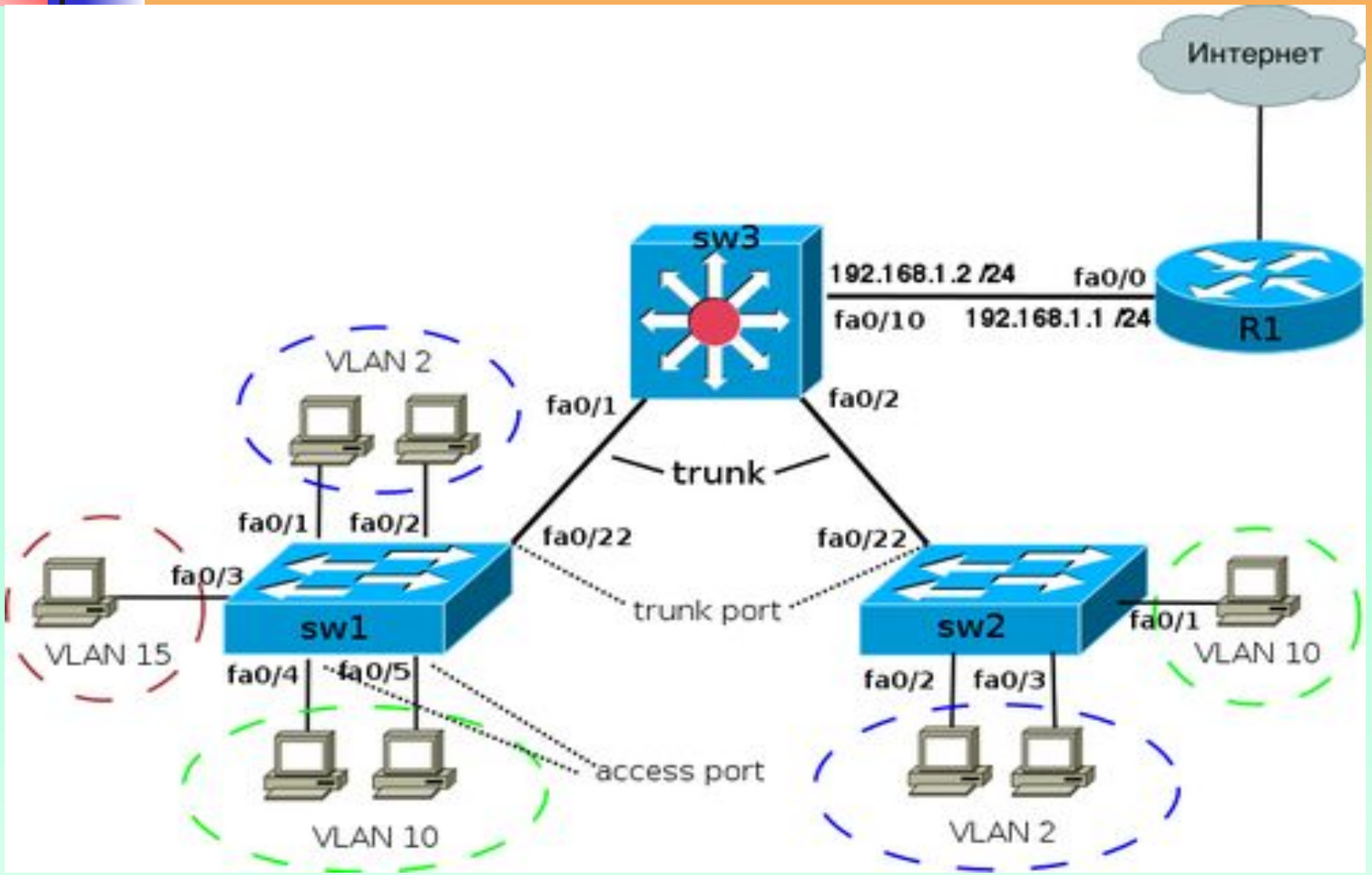
VLAN / интерфейс 3го уровня	IP-адрес
VLAN 2	10.0.2.1 /24
VLAN 10	10.0.10.1 /24
VLAN 15	10.0.15.1 /24
Fa 0/10	192.168.1.2 /24

Настройка VLAN на коммутаторах Cisco

Диапазоны VLAN

VLANs	Диапазон	Использование	Передается VTP
0, 4095	Reserved	Только для системного использования.	--
1	Normal	VLAN по умолчанию. Можно использовать, но нельзя удалить.	Да
2-1001	Normal	Для VLANов Ethernet. Можно создавать, удалять и использовать.	Да
1002-1005	Normal	Для FDDI и Token Ring. Нельзя удалить.	Да
1006-4094	Extended	Только для VLANов Ethernet.	Версия 1 и 2 нет, версия 3 да

Сегментация КС с помощью коммутаторов



Сегментация КС с помощью коммутаторов

Конфигурация sw1:

```
!
interface FastEthernet0/1
 switchport mode access
 switchport access vlan 2
!
interface FastEthernet0/2
 switchport mode access
 switchport access vlan 2
!
interface FastEthernet0/3
 switchport mode access
 switchport access vlan 15
!
interface FastEthernet0/4
 switchport mode access
 switchport access vlan 10
!
interface FastEthernet0/5
 switchport mode access
 switchport access vlan 10
!
interface FastEthernet0/22
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 1,2,10,15
```

На коммутаторе sw3 настроена маршрутизация между VLAN, поэтому в данной схеме хосты могут общаться как в пределах одного VLAN, так и между различными VLAN. Например, хосты на коммутаторе sw1 в VLAN 2 могут взаимодействовать между собой и с хостами в VLAN 2 на коммутаторе sw2. Кроме того, они могут взаимодействовать с хостами в других VLAN на коммутаторах sw1 и sw2.

Сегментация КС с помощью коммутаторов

Конфигурация sw2:

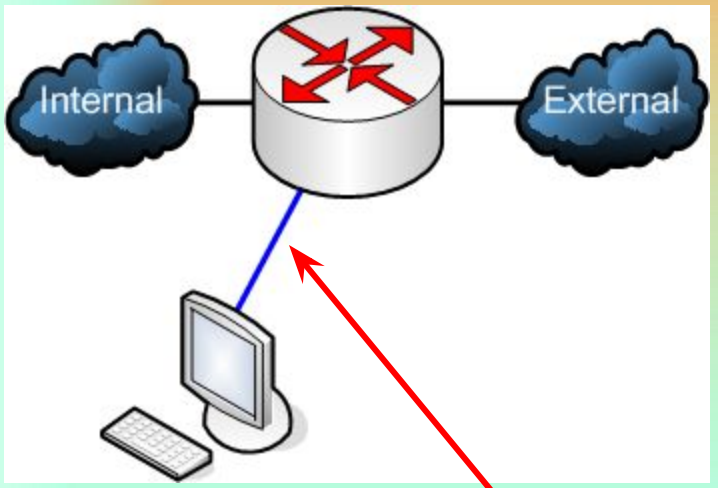
```
!
interface FastEthernet0/1
 switchport mode access
 switchport access vlan 10
!
interface FastEthernet0/2
 switchport mode access
 switchport access vlan 2
!
interface FastEthernet0/3
 switchport mode access
 switchport access vlan 2
!
interface FastEthernet0/22
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 1,2,10
!
```

Сегментация КС с помощью коммутаторов

Конфигурация sw3:

```
!
ip routing
!
vlan 2,10,15
!
interface FastEthernet0/1
 switchport mode trunk
 switchport trunk allowed vlan 1,2,10,15
!
interface FastEthernet0/2
 switchport mode trunk
 switchport trunk allowed vlan 1,2,10
!
interface FastEthernet0/10
 no switchport
 ip address 192.168.1.2 255.255.255.0
!
interface Vlan2
 ip address 10.0.2.1 255.255.255.0
!
interface Vlan10
 ip address 10.0.10.1 255.255.255.0
!
interface Vlan15
 ip address 10.0.15.1 255.255.255.0
!
!ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

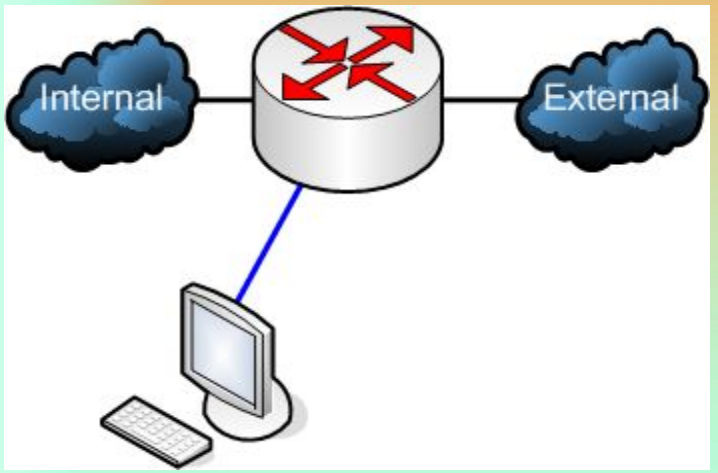
Конфигурирование маршрутизаторов



светло-голубой провод с разъемами RS-232 и RJ-45

Открываем программу-клиент терминального подключения, (PuTTY). В программе указываем порт соединения (COM1) и скорость подключения (9600). Если видно черный экран, мигающий курсор и больше ничего, значит, скорость подключения на роутере выставлена другая. Как правило, это может быть скорость 115200. Если и она не подходит (а это — редкость), то придется подбирать. В любом случае, еще стоит проверить, какой указан COM порт, к которому произведено подключение.

Конфигурирование маршрутизаторов



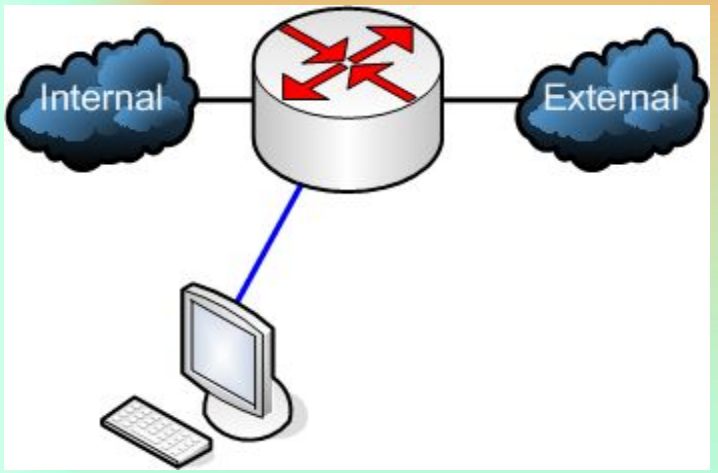
Если все **нормально, то видно приглашение от роутера. По умолчанию оно будет выглядеть так: Router>**

Это значит, что мы находимся в пользовательском режиме. Из этого режима доступно совсем немного команд.

Все эти команды позволяют лишь наблюдать за работой роутера, но не дают возможности вносить изменения в конфигурацию.

Из этого режима можно выполнить, например, команду Ping или show ip interface.

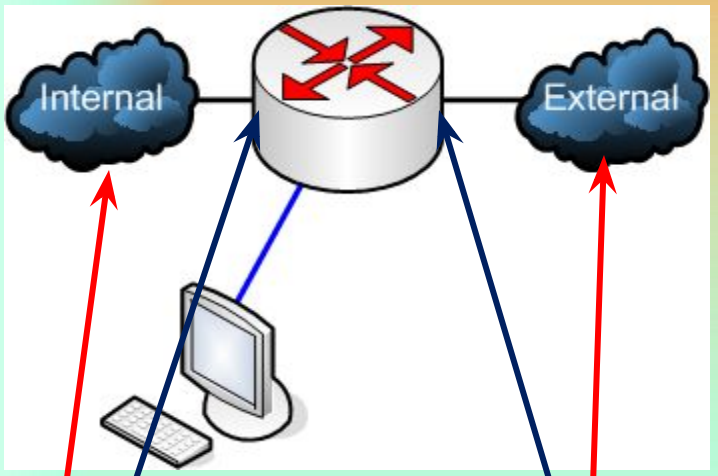
Конфигурирование маршрутизаторов



Для того, чтобы изменять рабочую конфигурацию (настройку) роутера, необходимо войти в привилегированный режим. Привилегированный режим может быть защищен паролем.
Для того чтобы войти в привилегированный режим, нужно набрать команду enable. После этого приглашение командной строки изменится на Router#

Здесь уже доступно намного больше команд. В этом режме можно вносить изменения в рабочую конфигурацию и сохранять измененную конфигурацию в ЗУ.

Конфигурирование маршрутизаторов



192.168.10.1/24,

10.54.0.1

192.168.10.254

10.54.0.0/16,

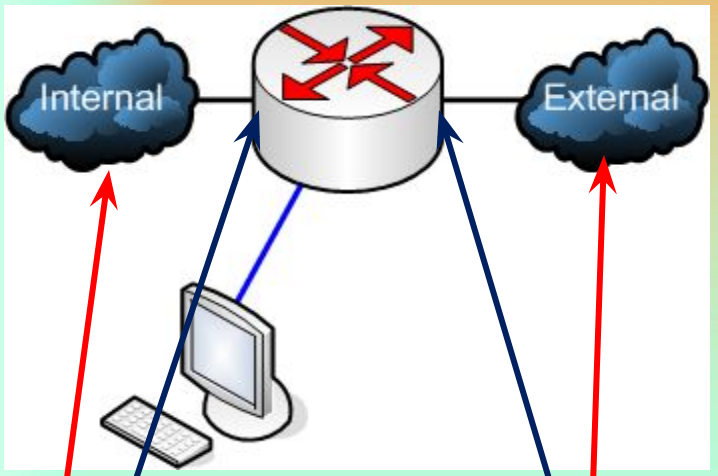
Основная настройка роутера ведется из режима глобальной конфигурации. В него можно попасть из привилегированного режима выполнением команды configure terminal. Приглашение изменится на Router(config)#. (Приглашение командной строки говорит о том, в каком режиме находится маршрутизатор).

Соединим две сети с помощью маршрутизатора.

Сеть Internal имеет диапазон адресов 192.168.10.1/24, адрес роутера в нем — 192.168.10.254, сетевой адаптер — FastEthernet0/0

Сеть External имеет диапазон адресов 10.54.0.0/16, адрес роутера в нем — 10.54.0.1, сетевой адаптер — FastEthernet0/1.

Конфигурирование маршрутизаторов



192.168.10.1/24,

10.54.0.1

192.168.10.254

10.54.0.0/16,

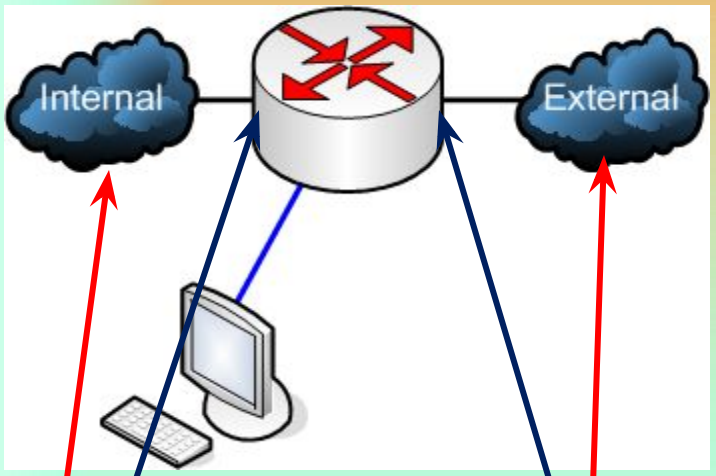
В режиме глобальной конфигурации вводим команду Interface FastEthernet0/0. Приглашение станет таким: Router(config-if)#. Интерфейс по умолчанию не имеет никакого адреса и даже выключен. Сначала введем IP-адрес. Это делается следующей командой: ip address 192.168.10.254 255.255.255.0.

Помните, что интерфейс выключен? Включается он командой no shutdown. Если все хорошо, то пробежит надпись:

```
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
```

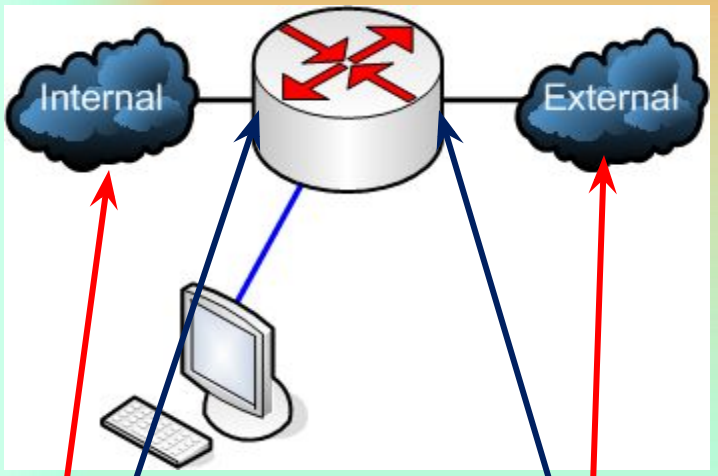
Конфигурирование маршрутизаторов



Первая строка говорит о том, что с сетевым интерфейсом все хорошо с точки зрения физического и канального уровня (сетевой кабель подключен и на другом его конце работает совместимое оборудование). Вторая строка говорит о том, что Сетевой уровень (IP Layer) тоже работает как надо.

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Конфигурирование маршрутизаторов



192.168.10.1/24,

10.54.0.1

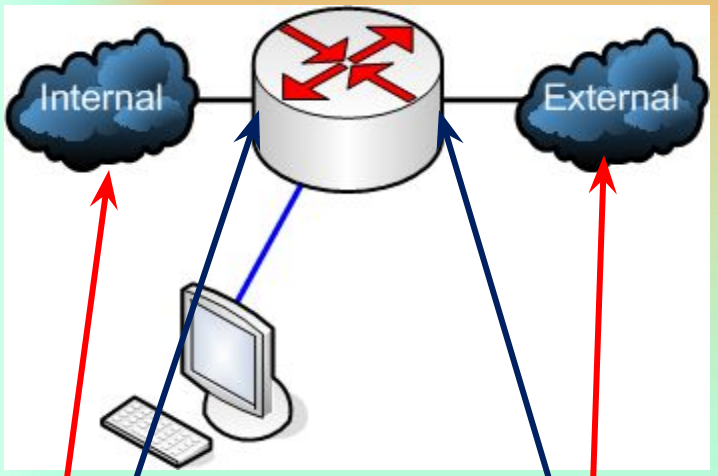
192.168.10.254

10.54.0.0/16,

Проверить, правильно ли все настроено, можно вернувшись в привилегированный режим (команда exit) и выполнив команду show ip interface brief. Она покажет информацию о состоянии сетевых интерфейсов. Вывод команды будет примерно таким:

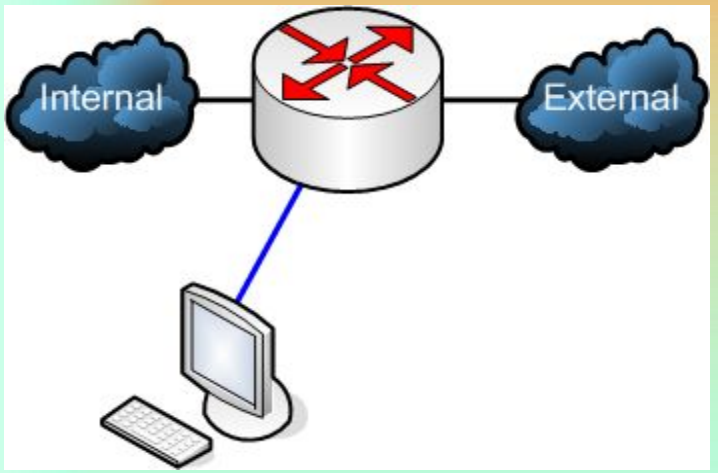
```
Router#show ip interface brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 192.168.10.254 YES manual up up
FastEthernet0/1 10.54.0.1 YES manual up up
```

Конфигурирование маршрутизаторов



Готово! Роутер может передавать пакеты из одной сети в другую и обратно.
Все изменения и настройки, которые внесены, сохранены только в оперативной памяти роутера. Чтобы конфигурация сохранилась и после перезагрузки, ее нужно скопировать в ПЗУ. Для этого из привилегированного режима вводится команда copy running-config startup-config.
Теперь перезагрузка не страшна!

Конфигурирование маршрутизаторов

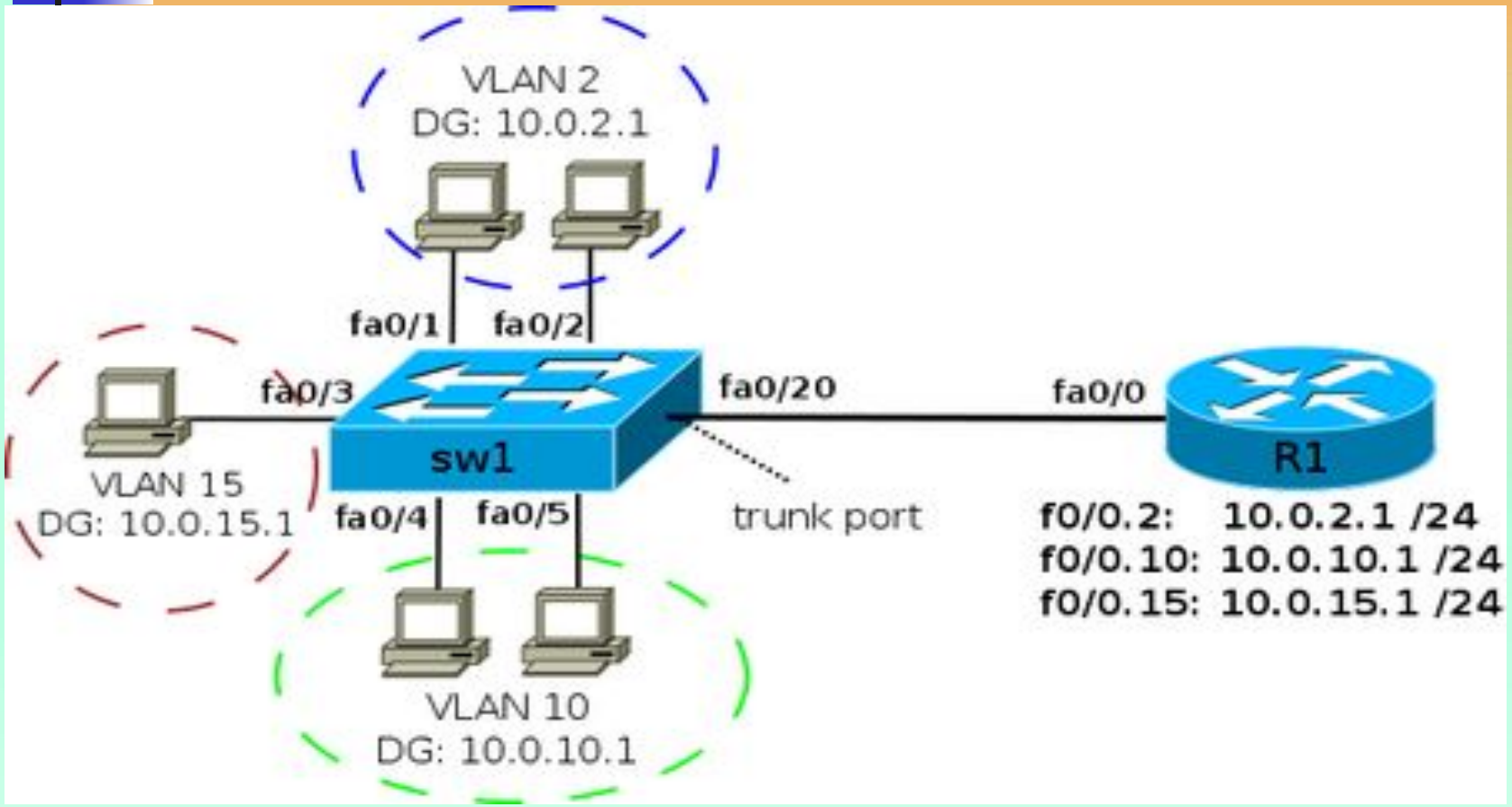


Итого:

Для работы понадобился 4 основных режима конфигурации:

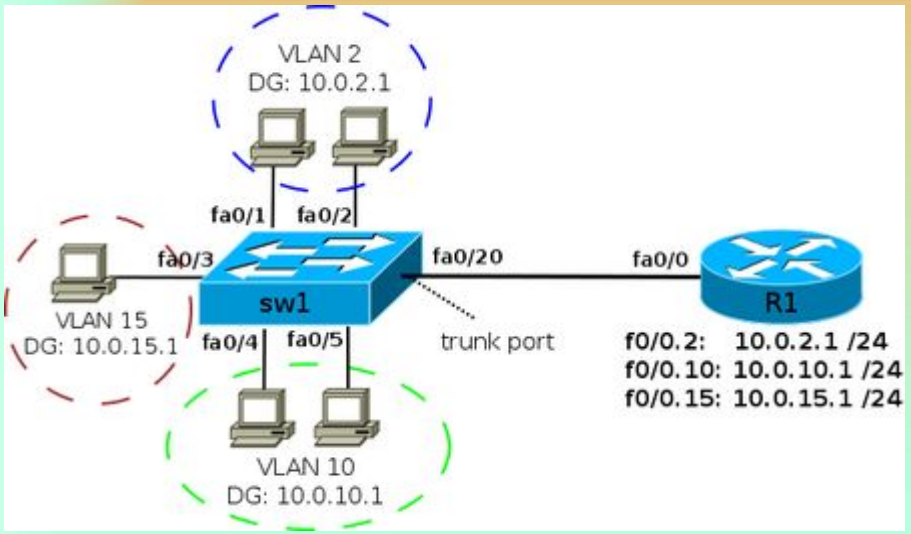
Пользовательский режим: Router>
Привилегированный режим: Router#
Режим глобальной конфигурации: Router(config)#
Режим конфигурации объекта (интерфейса, протокола маршрутизации и т. д.): Router(config-if)#

Настройка VLAN на маршрутизаторах



Передача трафика между VLANами с помощью маршрутизатора

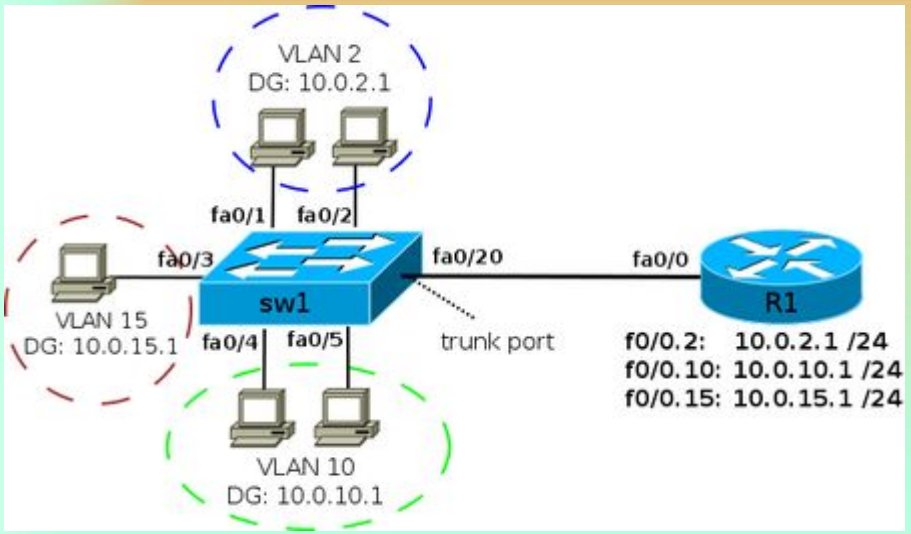
Настройка VLAN на маршрутизаторах



Для того чтобы маршрутизатор мог передавать трафик из одного VLAN в другой (из одной сети в другую), необходимо чтобы в каждой сети у него был интерфейс.

Для того чтобы не выделять под сеть каждого VLAN отдельный физический интерфейс, создаются логические подынтерфейсы на физическом интерфейсе для каждого VLAN.

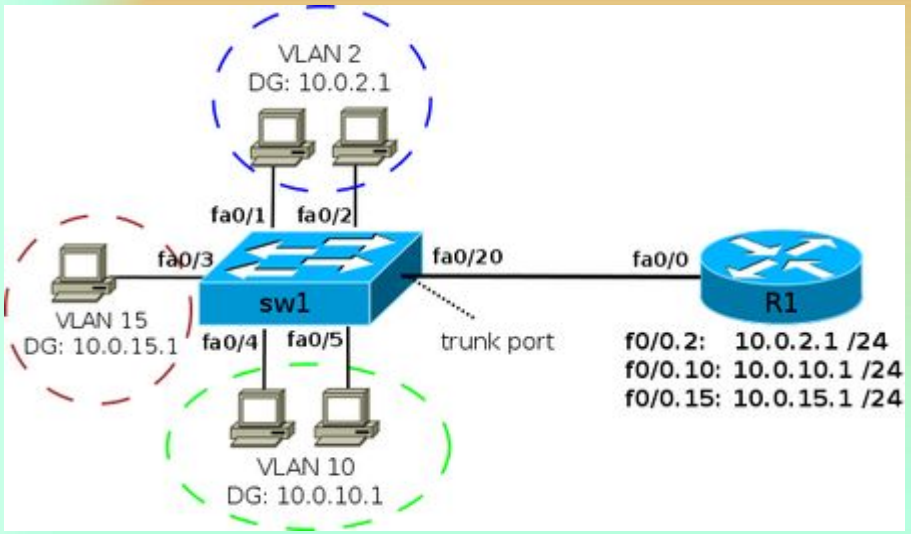
Настройка VLAN на маршрутизаторах



На коммутаторе порт, ведущий к маршрутизатору, должен быть настроен как тегированный порт (в терминах Cisco — транк). Такая схема, в которой маршрутизация между VLAN выполняется на маршрутизаторе, часто называется router on a stick.

Для того чтобы не выделять под сеть каждого VLAN отдельный физический интерфейс, создаются логические подынтерфейсы на физическом интерфейсе для каждого VLAN.

Настройка VLAN на маршрутизаторах



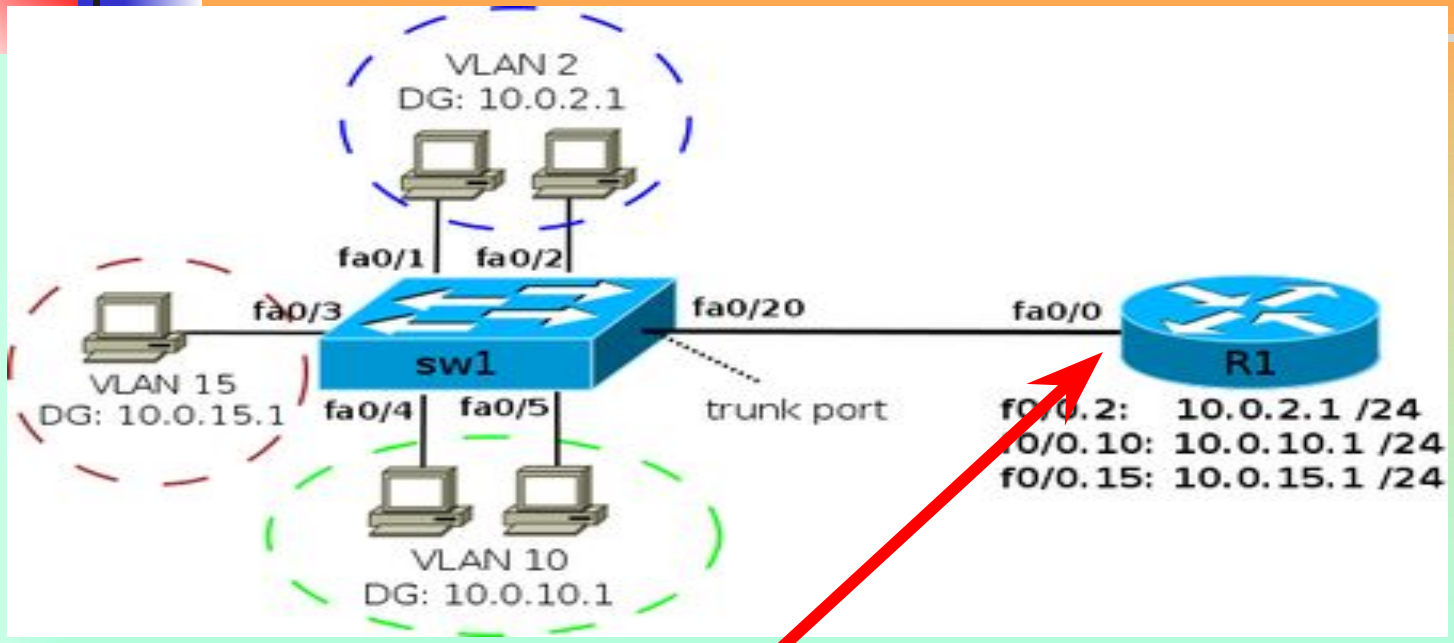
IP-адреса шлюза по умолчанию для VLAN (эти адреса назначаются на подынтерфейсах маршрутизатора R1):

VLAN	IP-адрес
VLAN 2	10.0.2.1 /24
VLAN 10	10.0.10.1 /24
VLAN 15	10.0.15.1 /24

Для логических подынтерфейсов необходимо указывать то, что интерфейс будет получать тегированный трафик и указывать номер VLAN соответствующий этому интерфейсу. Это задается командой в режиме настройки подынтерфейса:

R1(config-if)# encapsulation dot1q <vlan-id>

Настройка VLAN на маршрутизаторах



Создание логического подынтерфейса для VLAN 2:

R1(config)# interface fa0/0.2

R1(config-subif)# encapsulation dot1q 2

R1(config-subif)# ip address 10.0.2.1 255.255.255.0

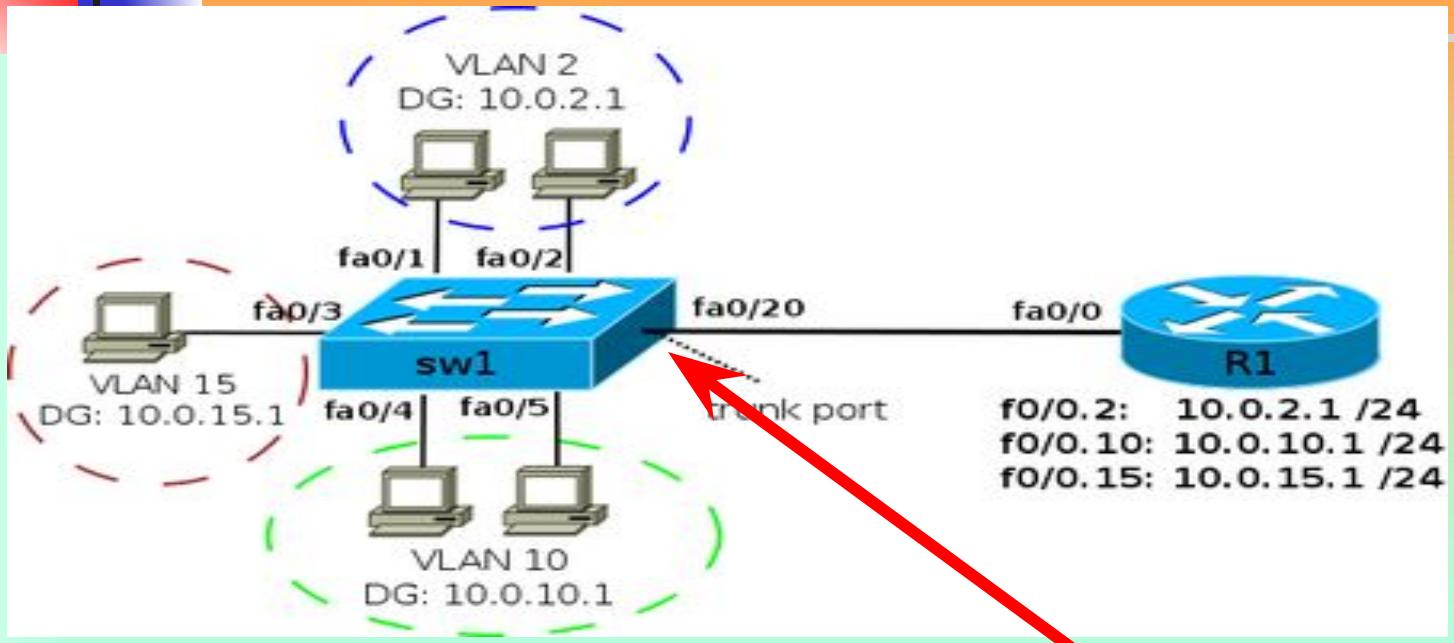
Создание логического подынтерфейса для VLAN 10:

R1(config)# interface fa0/0.10

R1(config-subif)# encapsulation dot1q 10

R1(config-subif)# ip address 10.0.10.1 255.255.255.0

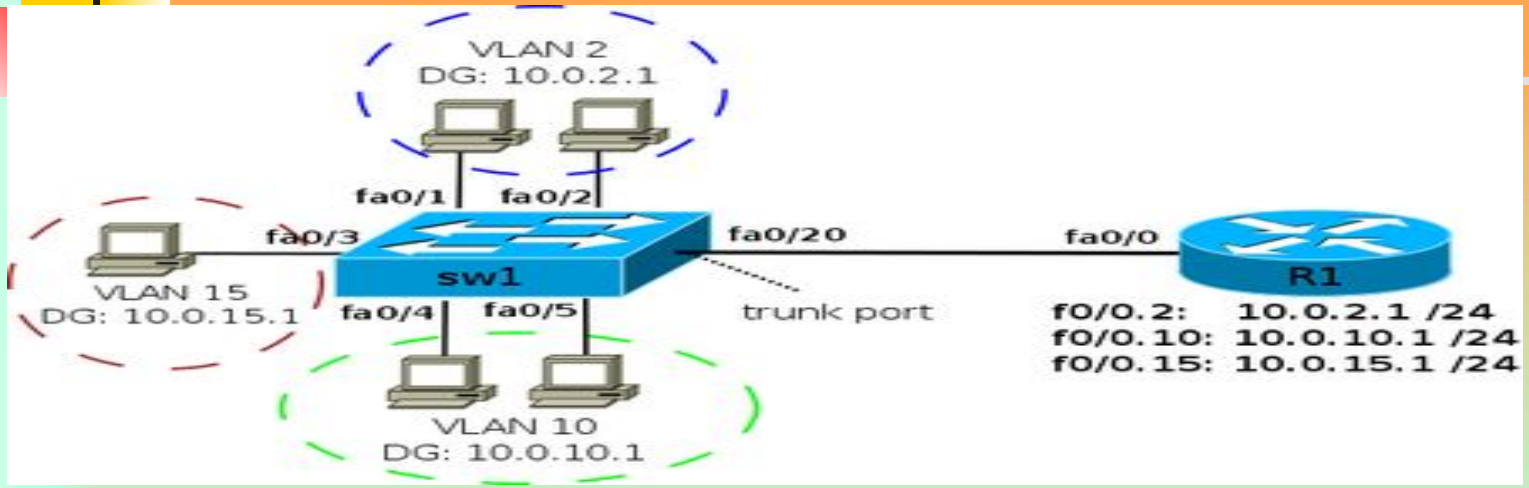
Настройка VLAN на маршрутизаторах



На коммутаторе порт, ведущий к маршрутизатору, должен быть настроен как статический транк:

```
interface FastEthernet0/20
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

Настройка VLAN на маршрутизаторах

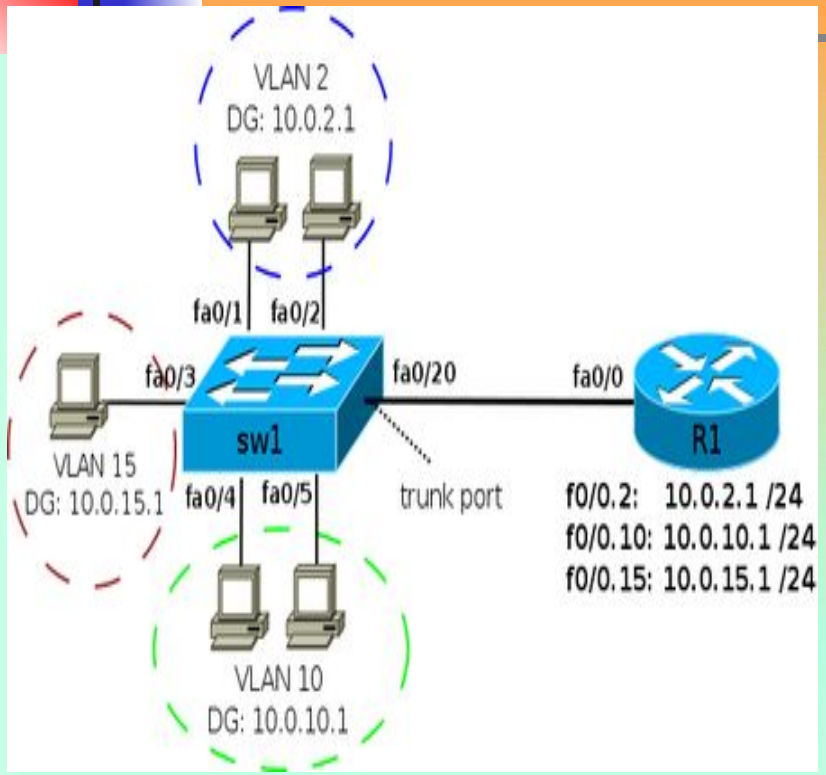


Конфигурационные файлы устройств для схемы в начале

Конфигурация sw1:

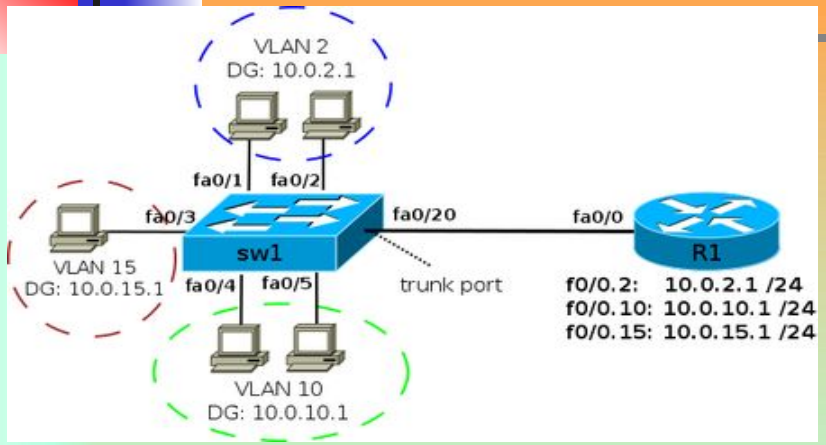
```
!
interface FastEthernet0/1
 switchport mode access
 switchport access vlan 2
!
interface FastEthernet0/2
 switchport mode access
 switchport access vlan 2
!
```

Настройка VLAN на маршрутизаторах




```
interface FastEthernet0/3
 switchport mode access
 switchport access vlan 15
!
interface FastEthernet0/4
 switchport mode access
 switchport access vlan 10
!
interface FastEthernet0/5
 switchport mode access
 switchport access vlan 10
!
```

Настройка VLAN на маршрутизаторах

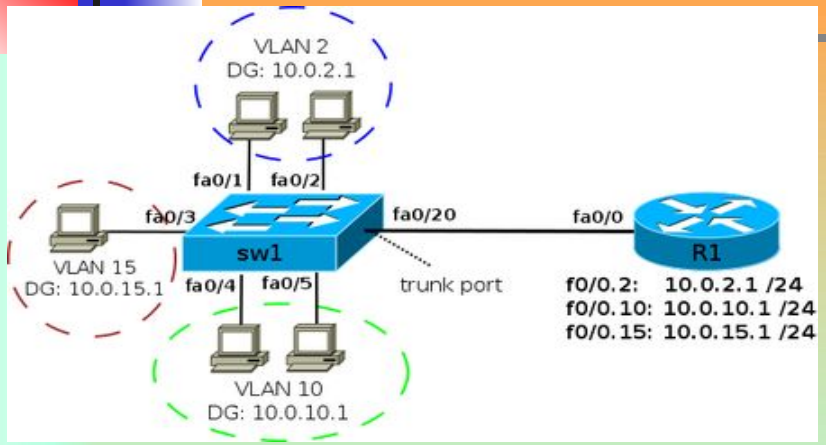



```
interface FastEthernet0/20
 switchport trunk encapsulation
dot1q
 switchport mode trunk
 switchport trunk allowed vlan
2,10,15
!
```

Конфигурация R1:

```
!
interface fa0/0.2
 encapsulation dot1q 2
 ip address 10.0.2.1 255.255.255.0
!
interface fa0/0.10
 encapsulation dot1q 10
 ip address 10.0.10.1 255.255.255.0
!
```

Настройка VLAN на маршрутизаторах

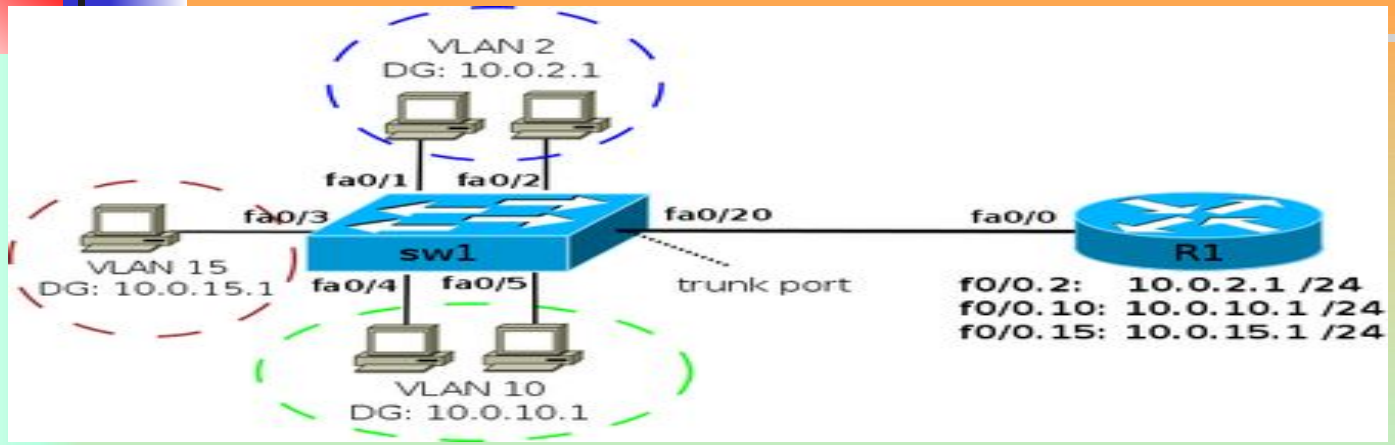



```
interface fa0/0.15
 encapsulation dot1q 15
 ip address 10.0.15.1 255.255.255.0
!
```

Настройка native VLAN

По умолчанию трафик VLAN'а 1 передается не тегированым (то есть, VLAN 1 используется как native), поэтому на физическом интерфейсе маршрутизатора задается адрес из сети VLAN 1.

Настройка VLAN на маршрутизаторах



Задание адреса на физическом интерфейсе:

R1(config)# interface fa0/0

R1(config-if)# ip address 10.0.1.1 255.255.255.0

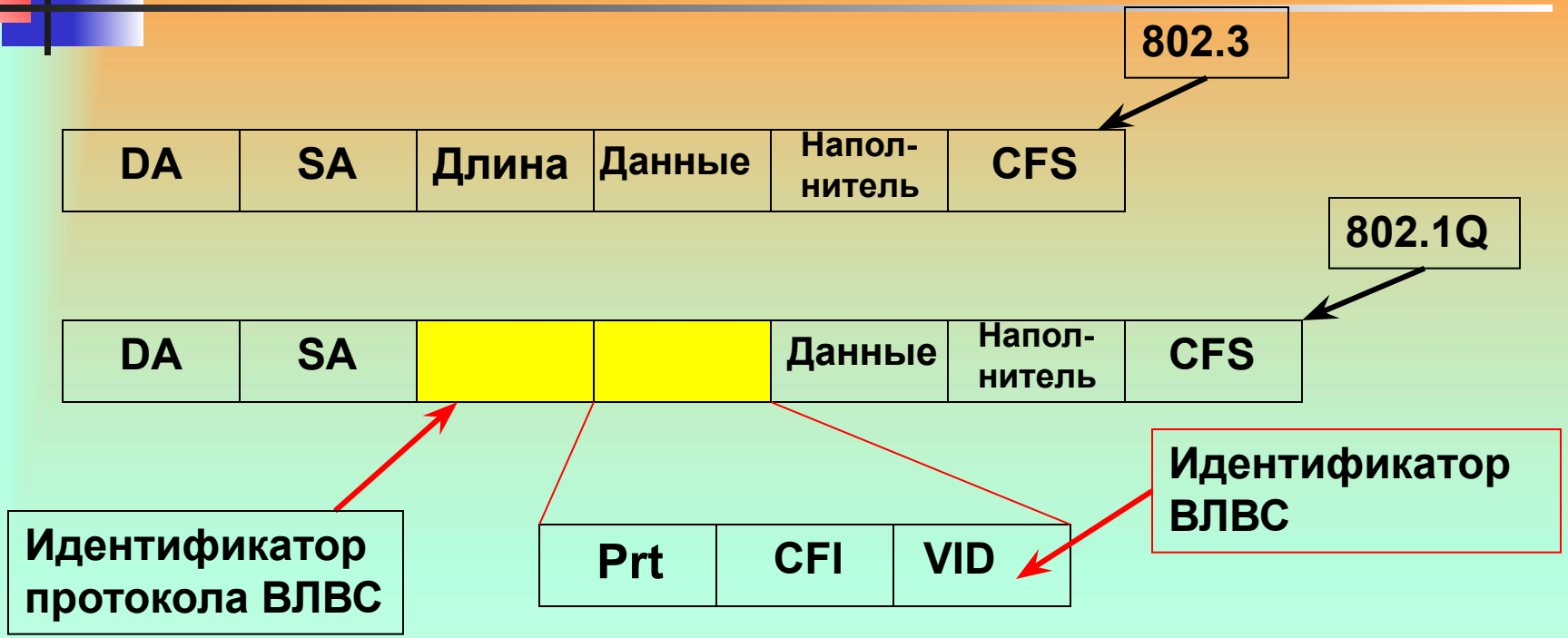
Если необходимо создать подынтерфейс для передачи не тегированного трафика, то в этом подынтерфейсе явно указывается, что он принадлежит native VLAN. Например, если native VLAN 99:

R1(config)# interface fa0/0.99

R1(config-subif)# encapsulation dot1q 99 native

R1(config-subif)# ip address 10.0.99.1 255.255.255.0

Сегментация КС с помощью коммутаторов



Стандарт 802.1Q определяет структуру заголовка для маркированных кадров (Tagged Frames) Ethernet. Тег вставляется в обычный кадр Ethernet после адреса источника. В тег входит 3-х битное поле приоритета кадра (Prt), 12-и битное поле идентификатора ВЛВС (VID – VLAN ID) и бит-идентификатор канонического формата заголовка (CFI –Canonical Format Identifier)

Сегментация КС с помощью коммутаторов

Таким образом 802.1Q отличается от 802.3 добавлением пары двухбайтовых полей. Первое называется идентификатор протокола ВЛВС, оно всегда (для 802.1Q) равно 0x810.

Т.к. это число превышает 1500, то все сетевые карты интерпретируют его как тип кадра, а не как длину. Во втором двухбайтовом поле находятся три вложенных поля.

Главное из них идентификатор ВЛВС, занимает 12 младших бит. Это поле позволяет определить принадлежность кадра к конкретной ВЛВС (до 4096) в пределах коммутируемой сети.

Поле приоритета позволяет различать восемь уровней приоритета фреймов (никакого отношения к виртуальным сетям не имеет).

Сегментация КС с помощью коммутаторов

Поле CFI изначально предназначалось для того, чтобы показывать порядок бит в MAC –адресе.
К VLAN не имеет никакого отношения.

Как работает коммутатор с тегованными кадрами?
Когда кадр с флагом виртуальной сети приходит в ВЛВС совместимый (802.1Q) коммутатор, этот коммутатор использует VID как индекс в таблице, по которой он ищет в какие порты послать пришедший кадр.

Откуда берется таблица?
Если она разрабатывается вручную, то это откат к ручному конфигурированию портов. Достоинством мостов (прозрачность) является их способность к автоматической настройке (построение таблиц коммутации фреймов).

Сегментация КС с помощью коммутаторов

В коммутаторах, поддерживающих ВЛВС удалось сохранить это свойство для их внутренних мостов. Настройка производится по информации содержащейся в заголовках приходящих кадров. Если кадр помеченный как VID=4 приходит на 3 порт, значит одна из машин подключенных к этому порту коммутатора принадлежит виртуальной сети 4.

Все коммутаторы, поддерживающие 802.1Q поставляются в состоянии – простой коммутатор. Для того, чтобы использовать его для создания ВЛВС, коммутатор следует конфигурировать.

Сегментация КС с помощью коммутаторов

Конфигурирование заключается в назначении портам, участвующим в формировании ВЛВС специальных атрибутов.

Каждому порту назначается PVID (Port VLAN Identifier) –идентификатор ВЛВС для всех приходящих в коммутатор немаркированных кадров. Коммутатор маркирует каждый приходящий к нему немаркированный кадр (вставляет номер VLAN, приоритет и пересчитывает FCS). Приходящие маркированные кадры коммутатор оставляет без изменения. Т.о. внутри коммутатора все фреймы будут маркированы.

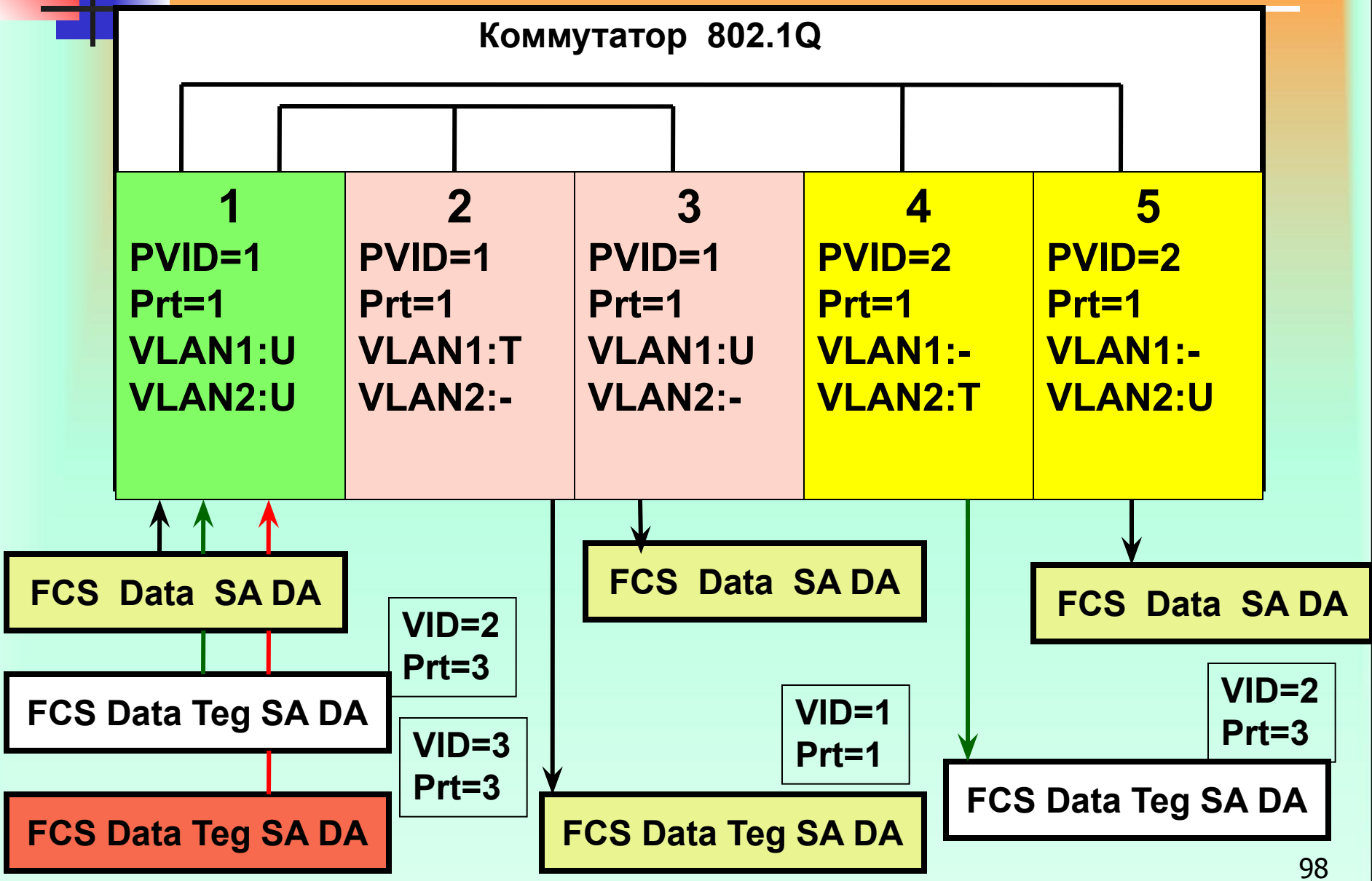
Порты маршрутизатора могут конфигурироваться как маркированные, так и не маркированные члены ВЛВС

Сегментация КС с помощью коммутаторов

Немаркированный порт (член ВЛВС) – Untagged Member все выходящие через него кадры выпускает без тегов (удаляет соответствующие поля и пересчитывает CFS)

Маркированный порт (член ВЛВС) – Tagged Member выпускает все кадры маркированными. Теги берутся либо исходные (если кадр пришел в коммутатор маркированным), либо устанавливаются в соответствии с PID и Prt порта, откуда этот кадр зашел в коммутатор.

Сегментация КС с помощью коммутаторов

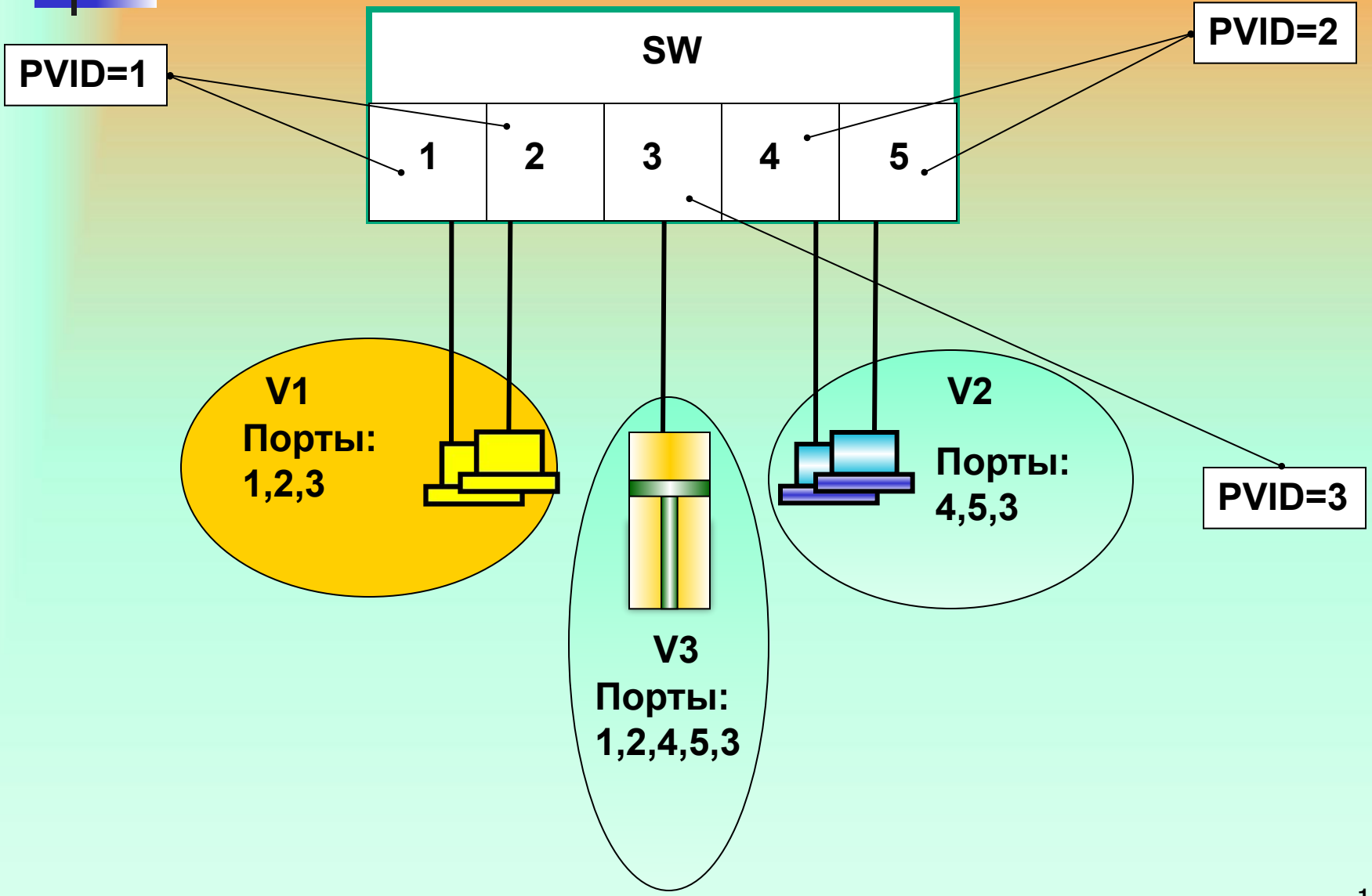


Сегментация КС с помощью коммутаторов

PVID нужны для того, что бы иметь возможность объединять не тегированные порты в несколько VLAN. Что при построении симметричных VLAN не возможно. Как правило, если надо по одному порту гонять трафик из нескольких VLAN, то нужно сделать это порт тегированным, что бы он помечал какой пакет, какому VLAN принадлежит. Что собственно логично.

Таким образом, при помощи этих PVID мы получаем возможность гонять не тегированный трафик за пределами коммутатора и при этом иметь возможность держать несколько VLAN на не тегированном порту.

Сегментация КС с помощью коммутаторов



Сегментация КС с помощью коммутаторов

В первом vlan имеются порты 1,2,3.
Во втором vlan порты 4,5,3.
В третий vlan входят все пять портов, что бы сервер входящий в третий vlan, мот отдавать ответы на все порты.
Допустим. из комп. А, выходит не тегированный фрейм, попадает на первый порт комутатора. Так как у первого порта PVID=1, то фрейму присваивается метка равная 1. Пункт назначения сервер, который висит на третьем порту, так как порт №3 входит в vlan1, наш фрейм может туда попасть. Но не может попасть на 4 и 5 порты, так как они не входят в vlan1, и пакет с меткой 1 отбрасывается. При выходе с порта №3 метка снимается и пакет приходит на сервер.

Сегментация КС с помощью коммутаторов

Далее сервер шлет ответ. От сервера выходит не тегированный фрейм и попадает на третий порт коммутатора, у третьего порта PVID=3, фрейм получает метку 3, так как в vlan3 входит порт №1, то фрейм с ответом свободно попадает в первый порт, при выходе тег снимается и попадает на комп. А.

Такая же схема для работы с сервером, машин из vlan2. Т.е. получается что копы из vlan1 и vlan2 не видят друг друга, но могу общаться с сервером, находящимся в vlan3.
Собственно PVID нужны для того, что бы помечать не тегированные фреймы приходящие на порт коммутатора.

Сегментация КС с помощью коммутаторов

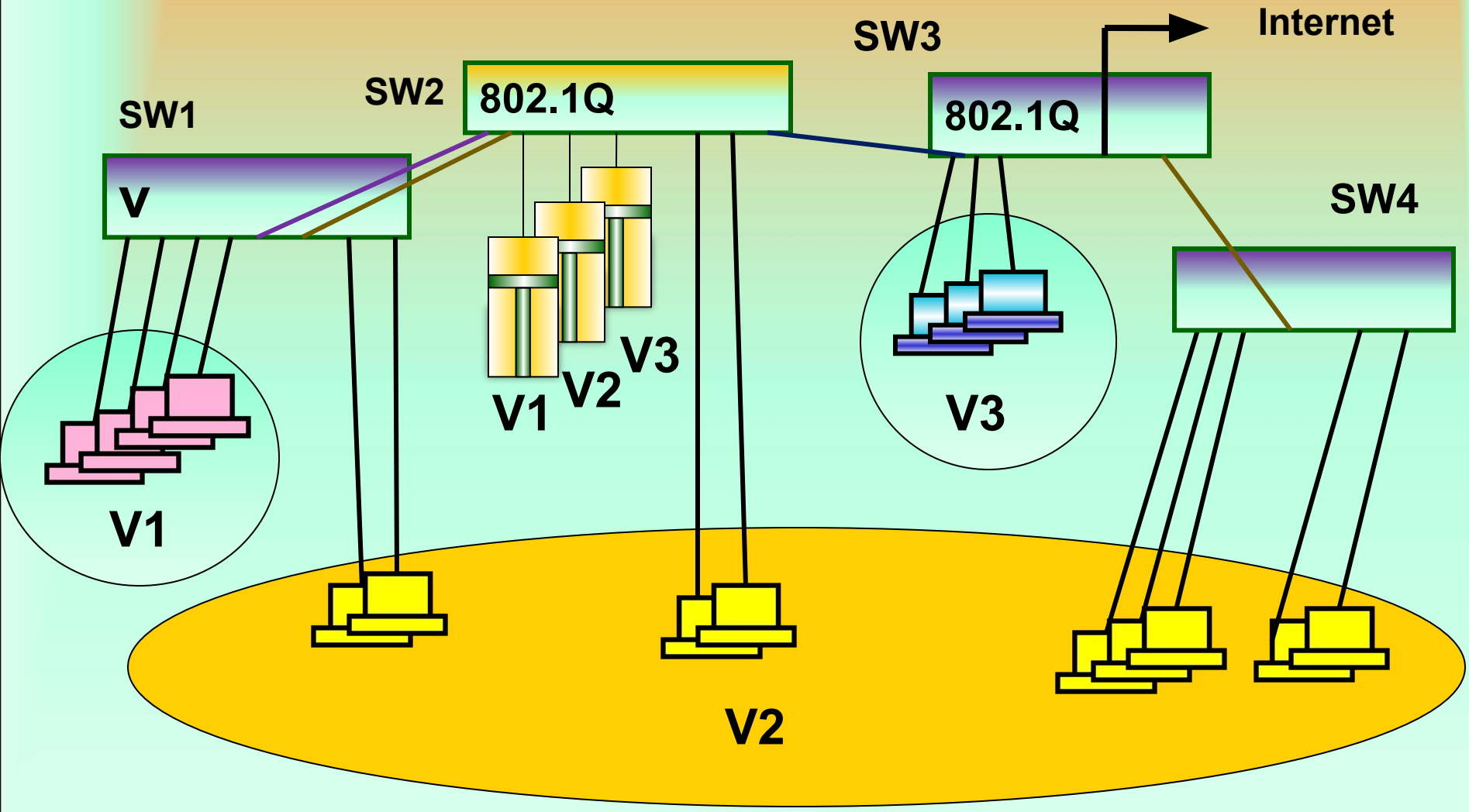
Для каждой ВЛВС определяется список портов, являющихся ее членами. Порт может быть членом одной и более ВЛВС.
Маркированный кадр, пришедший на порт с чужим для порта идентификатором ВЛВС, называется незарегистрированным (Unregistered) и коммутатором игнорируется.

Сегментация КС с помощью коммутаторов

При конфигурировании для каждой ВЛВС каждый порт должен быть объявлен или как немаркированный (U), или как маркированный (T), или как не являющийся членом данной VLAN (-). Каждому порту назначается приоритет (P_prt) и идентификатор ВЛВС (PVID). Если используется запараллеливание портов (port tranking) или резервирование линий (LinkSafe), то с точки зрения ВЛВС запараллеленные порты представляются как единое целое.

Сегментация КС с помощью коммутаторов

Рассмотрим следующую структуру сети , состоящую из различных коммутаторов и конфигурируем порты каждого коммутатора



Сегментация КС с помощью коммутаторов

SW2

802.1Q

1	2	3	4	5	6	7	8
PVID=1 P-prt=1 VLAN1=U VLAN9=- VLAN2=- VLAN3=-	PVID=2 P-prt=1 VLAN2=U VLAN9=U VLAN1=- VLAN3=-	PVID=1 P-prt=1 VLAN1=U VLAN2=- VLAN9=- VLAN3=-	PVID=2 P-prt=1 VLAN2=U VLAN1=- VLAN9=U VLAN3=-	PVID=3 P-prt=1 VLAN3=U VLAN1=- VLAN9=U VLAN2=-	PVID=2 P-prt=1 VLAN2=U VLAN1=- VLAN9=U VLAN3=-	PVID=2 P-prt=1 VLAN2=U VLAN1=- VLAN9=U VLAN3=-	PVID= P-prt=1 VLAN2=T VLAN3=T VLAN9=T

Сегментация КС с помощью коммутаторов

SW2

802.1Q

1	2	3	4	5	6	7	8
PVID=1 P-prt=1 VLAN1=U VLAN9=- VLAN2=- VLAN3=-	PVID=2 P-prt=1 VLAN2=U VLAN9=U VLAN1=- VLAN3=-	PVID=1 P-prt=1 VLAN1=U VLAN2=- VLAN9=- VLAN3=-	PVID=2 P-prt=1 VLAN2=U VLAN1=- VLAN9=U VLAN3=-	PVID=3 P-prt=1 VLAN3=U VLAN1=- VLAN9=U VLAN2=-	PVID=2 P-prt=1 VLAN2=U VLAN1=- VLAN9=U VLAN3=-	PVID=2 P-prt=1 VLAN2=U VLAN1=- VLAN9=U VLAN3=-	PVID= P-prt=1 VLAN2=T VLAN3=T VLAN9=T

Сегментация КС с помощью коммутаторов

SW2

802.1Q

1	2	3	4	5	6	7	8
PVID=1 P-prt=1 VLAN1=U VLAN9=- VLAN2=- VLAN3=-	PVID=2 P-prt=1 VLAN2=U VLAN9=U VLAN1=- VLAN3=-	PVID=1 P-prt=1 VLAN1=U VLAN2=- VLAN9=- VLAN3=-	PVID=2 P-prt=1 VLAN2=U VLAN1=- VLAN9=U VLAN3=-	PVID=3 P-prt=1 VLAN3=U VLAN1=- VLAN9=U VLAN2=-	PVID=2 P-prt=1 VLAN2=U VLAN1=- VLAN9=U VLAN3=-	PVID=9 P-prt=1 VLAN2=U VLAN1=- VLAN9=U VLAN3=-	PVID=2 P-prt=1 VLAN2=T VLAN3=T VLAN9=U VLAN1=-