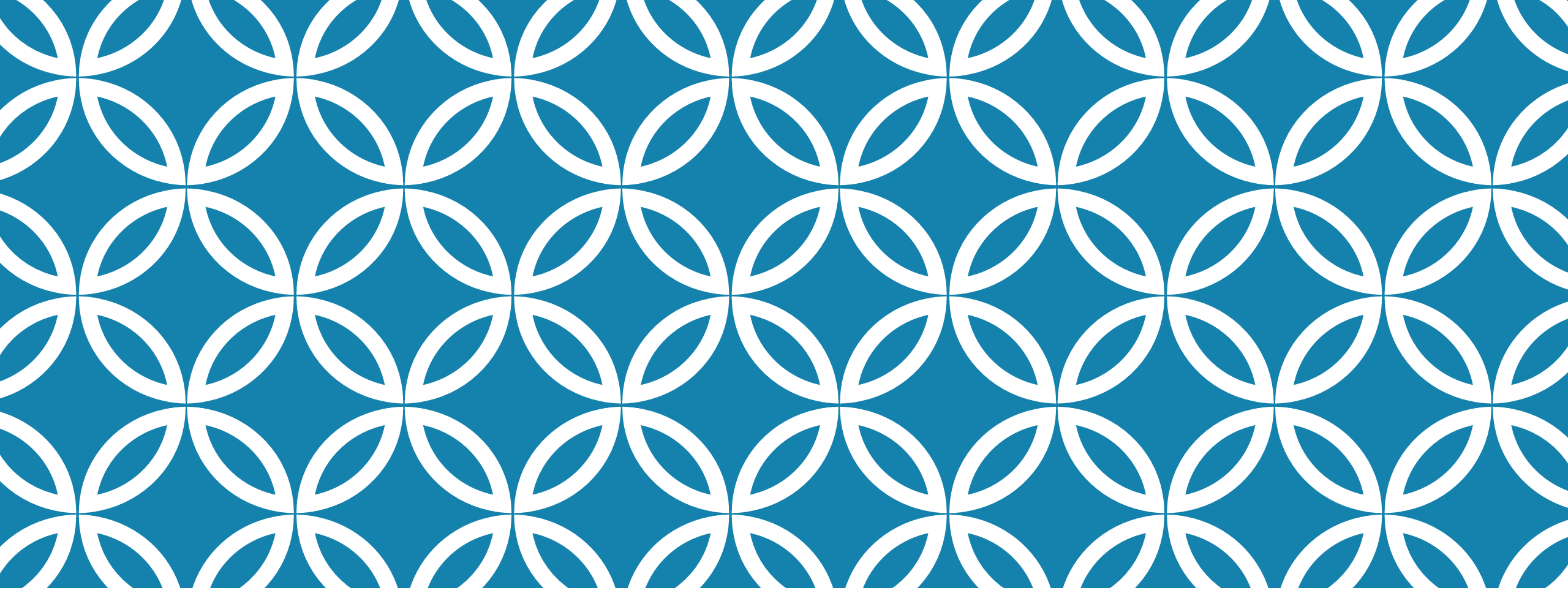


МОДУЛЬ 3. VLAN

КАФЕДРА ТЕЛЕКОММУНИКАЦИЙ

3.1 ОБЗОР ВИРТУАЛЬНЫХ ЛОКАЛЬНЫХ СЕТЕЙ

3.1.1 ОПРЕДЕЛЕНИЕ СЕТИ VLAN

В коммутируемых объединённых сетях сети VLAN обеспечивают гибкость сегментации и организации. Сети VLAN позволяют сгруппировать устройства внутри локальной сети. Группа устройств в пределах сети VLAN взаимодействует так, будто устройства подключены с помощью одного провода. Сети VLAN основываются не на физических, а на логических подключениях.

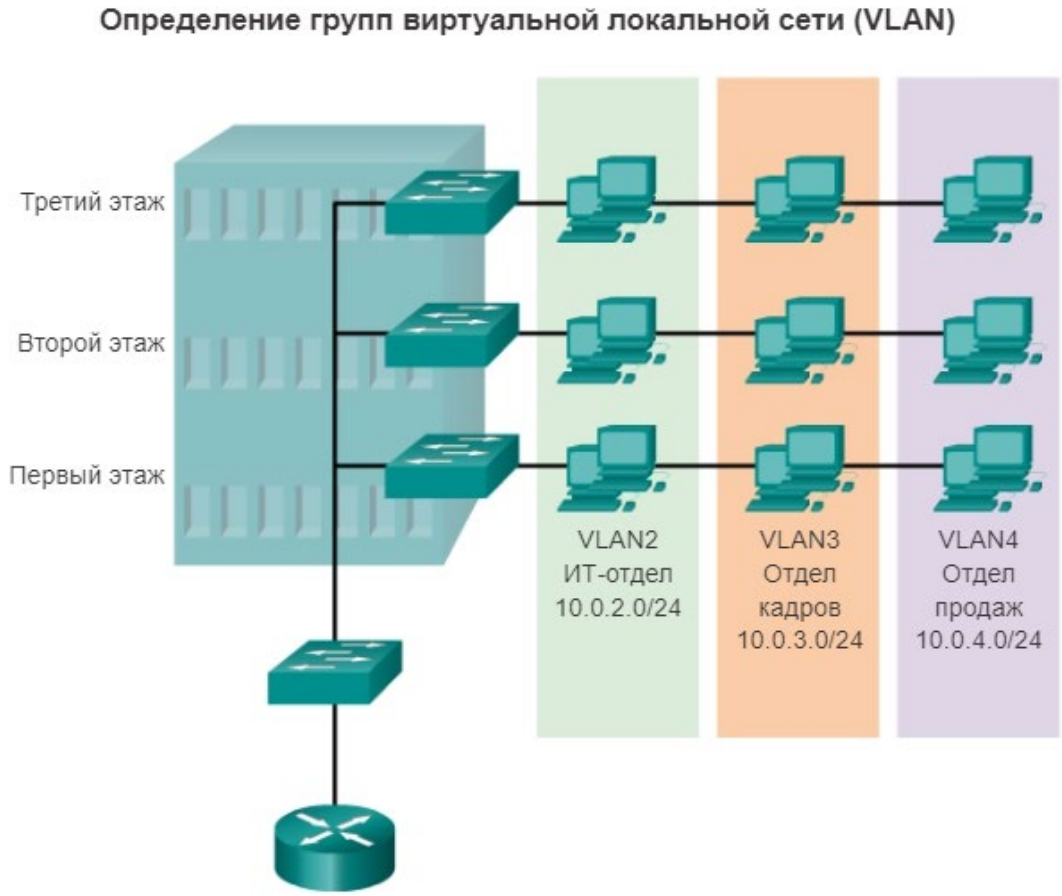
Сети VLAN позволяют администратору производить сегментацию по функциям, проектным группам или областям применения, вне зависимости от физического расположения пользователя или устройства. Устройства в пределах сети VLAN работают таким образом, будто находятся в собственной независимой сети, даже если делят одну общую инфраструктуру с другими VLAN. Любой порт коммутатора может принадлежать сети VLAN.

Одноадресные, широковещательные и многоадресные пакеты пересылаются и рассылаются только к конечным станциям в пределах той сети VLAN, которая является источником этих пакетов. Каждая сеть VLAN считается отдельной логической сетью, и пакеты, адресованные станциям, не принадлежащим данной сети VLAN, должны пересылаться через устройство, поддерживающее маршрутизацию.

3.1.1 ОПРЕДЕЛЕНИЕ СЕТИ VLAN

Сеть VLAN создаёт логический широковещательный домен, который может охватывать несколько физических сегментов LAN. Разделяя крупные широковещательные домены на более мелкие сети, VLAN повышают производительность сети. Если устройство в одной сети VLAN передаёт широковещательный кадр Ethernet, то этот кадр получают все устройства в рамках этой VLAN, устройства же в других сетях VLAN этот кадр не получают.

Сети VLAN позволяют реализовывать политику обеспечения доступа и безопасности, учитывая интересы различных групп пользователей. Каждый порт коммутатора может быть назначен только одной сети VLAN (за исключением порта, подключённого к IP-телефону или к другому коммутатору).



3.1.2 ПРЕИМУЩЕСТВА ИСПОЛЬЗОВАНИЯ VLAN

Производительность пользователей и адаптивность сети играют важную роль в процветании и успехе компании. Сети VLAN облегчают процесс проектирования сети, обеспечивающей помощь в выполнении целей организации. К основным преимуществам использования VLAN относятся:

Безопасность: группы, обладающие уязвимыми данными, отделены от остальной части сети, благодаря чему снижается вероятность утечки конфиденциальной информации. Как показано на рисунке, компьютеры преподавателей находятся в сети VLAN 10 и полностью отделены от трафика данных учащихся и гостей.

Снижение расходов: благодаря экономии на дорогих обновлениях сетевой инфраструктуры и более эффективному использованию имеющейся полосы пропускания и восходящих каналов происходит снижение расходов.

Повышение производительности: разделение однородных сетей 2-го уровня на несколько логических рабочих групп (широковещательных доменов) уменьшает количество лишнего сетевого трафика и повышает производительность.

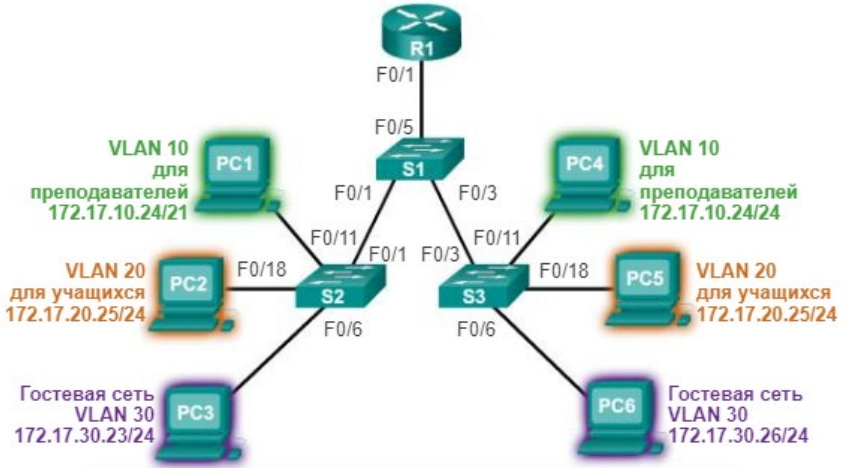
Уменьшенные широковещательные домены: разделение сети на сети VLAN уменьшает количество устройств в широковещательном домене. Сеть, показанная на рисунке на следующем слайде, состоит из шести компьютеров и трёх широковещательных доменов: для преподавателей, для учащихся и гостевого домена.

3.1.2 ПРЕИМУЩЕСТВА ИСПОЛЬЗОВАНИЯ VLAN

Повышение производительности ИТ-отдела: сети VLAN упрощают управление сетью, поскольку пользователи с аналогичными требованиями к сети используют одну и ту же сеть VLAN. При введении в эксплуатацию нового коммутатора на назначенных портах реализуются все правила и процедуры, уже применённые в этой конкретной VLAN. Также ИТ-специалистам легче определять функцию сети VLAN, назначая ей соответствующее имя. На данном рисунке для простой идентификации сеть VLAN 10 была названа «Для преподавателей», VLAN 20 — «Для учащихся» и VLAN 30 — «Гостевая».

Упрощённое управление проектами и приложениями: сети VLAN объединяют пользователей и сетевые устройства для соответствия деловым или географическим требованиям сети. Управление проектом и работа на прикладном уровне упрощены благодаря использованию разделения функций. Пример такой прикладной задачи — платформа разработки приложений для электронного обучения преподавателей.

Каждая VLAN в коммутируемой сети относится к какой-либо IP-сети; таким образом, в проекте VLAN нужно учитывать реализацию иерархической системы сетевой адресации. Иерархическая адресация подразумевает упорядоченное назначение номеров IP-сети сегментам или сетям VLAN с учетом работы сети в целом. Как показано на рисунке, блоки смежных сетевых адресов резервируются и настраиваются на устройствах в определённой области сети.



3.1.3 ТИПЫ СЕТЕЙ VLAN

В современных сетях используется множество различных типов сетей VLAN. Некоторые типы VLAN определяются классами трафика. Другие типы VLAN обусловлены функциями, которые они выполняют.

Виртуальная локальная сеть для данных — это сеть VLAN, которая настроена специально для передачи трафика, генерируемого пользователем. Сеть VLAN, передающая голосовой трафик или трафик управления, не является сетью VLAN для передачи данных. Рекомендуется отделять голосовой и управляющий трафик от трафика данных. VLAN для передачи данных иногда называют пользовательской сетью VLAN. Сети VLAN для данных используются для разделения сети на группы пользователей или устройств.

Сеть VLAN по умолчанию. Все порты коммутатора становятся частью VLAN по умолчанию после первоначальной загрузки коммутатора. Порты коммутатора, находящиеся в сети VLAN по умолчанию, являются частью одного широковещательного домена. Благодаря этому любое устройство, подключённое к любому порту коммутатора, может обмениваться данными с другими устройствами на других портах коммутатора. Сетью VLAN по умолчанию для коммутаторов Cisco установлена VLAN 1. На рисунке на следующем слайде команда **show vlan brief** была выполнена на коммутаторе, настроенном по умолчанию. Обратите внимание, что на все порты по умолчанию назначены сети VLAN 1.

3.1.3 ТИПЫ СЕТЕЙ VLAN

VLAN 1 поддерживает все функции любой сети VLAN, однако её нельзя переименовать или удалить. По умолчанию весь управляющий трафик 2-го уровня связан с сетью VLAN 1.

VLAN 1

```
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
```

- Все порты назначены сети VLAN 1 для пересылки данных по умолчанию.
- Сетью native VLAN по умолчанию является сеть VLAN 1.
- Сетью управления VLAN по умолчанию является сеть VLAN 1.
- VLAN 1 нельзя переименовывать или удалять.

3.1.3 ТИПЫ СЕТЕЙ VLAN

Сеть **native VLAN** назначена транковому порту 802.1Q. Транковые порты — это каналы между коммутаторами, которые поддерживают передачу трафика, связанного с более чем одной сетью VLAN. Транковый порт 802.1Q поддерживает трафик, поступающий от нескольких VLAN (тегированный трафик), а также трафик, который поступает не от VLAN (нетегированный трафик). Тегированным называется трафик, для которого в исходный заголовок кадра Ethernet вставлен 4-байтовый тег, определяющий сеть VLAN, к которой относится этот кадр. Транковый порт 802.1Q размещает нетегированный трафик в сети native VLAN, которой по умолчанию является VLAN 1.

Сети native VLAN определены в спецификации IEEE 802.1Q для обеспечения обратной совместимости с нетегированным трафиком, характерным для устаревших сценариев локальных сетей. Сеть native VLAN служит общим идентификатором на противоположных концах транкового канала.

Рекомендуется настроить native VLAN как неиспользуемую VLAN, отличающуюся от сети VLAN 1 и других VLAN. Фактически принято выделять фиксированную VLAN для выполнения роли сети native VLAN для всех транковых портов в коммутируемом домене.

3.1.3 ТИПЫ СЕТЕЙ VLAN

Управляющая VLAN — это любая сеть VLAN, настроенная для доступа к функциям управления коммутатора. Сеть VLAN 1 по умолчанию является управляющей VLAN. Для создания управляющей VLAN интерфейсу SVI коммутатора данной VLAN назначаются IP-адрес и маска подсети, благодаря чему коммутатором можно управлять через протоколы HTTP, Telnet, SSH или SNMP. Поскольку в исходной настройке коммутатора Cisco VLAN 1 является сетью VLAN по умолчанию, VLAN 1 не следует использовать в качестве управляющей VLAN.

В прошлом управляющая VLAN для коммутатора 2960 была единственным активным интерфейсом SVI. В версиях ОС Cisco IOS 15.x для коммутаторов Catalyst серии 2960 возможна поддержка более одного активного интерфейса SVI. В версиях ОС Cisco IOS 15.x необходимо документировать определённый активный интерфейс SVI, назначенный для удалённого управления. Несмотря на то, что теоретически коммутатор может обладать более чем одной управляющей VLAN, использование нескольких сетей данного типа увеличивает подверженность сетевым атакам.

На рисунке из слада 7 все порты назначены сети VLAN 1 по умолчанию. Ни одна native VLAN не назначена явно, и ни одна другая сеть VLAN не является активной. Таким образом, сети native VLAN и управляющая VLAN совпадают. Подобная настройка считается угрозой безопасности.

3.1.3 ТИПЫ СЕТЕЙ VLAN

Голосовая VLAN. Отдельная VLAN необходима, так как для голосового трафика требуется:

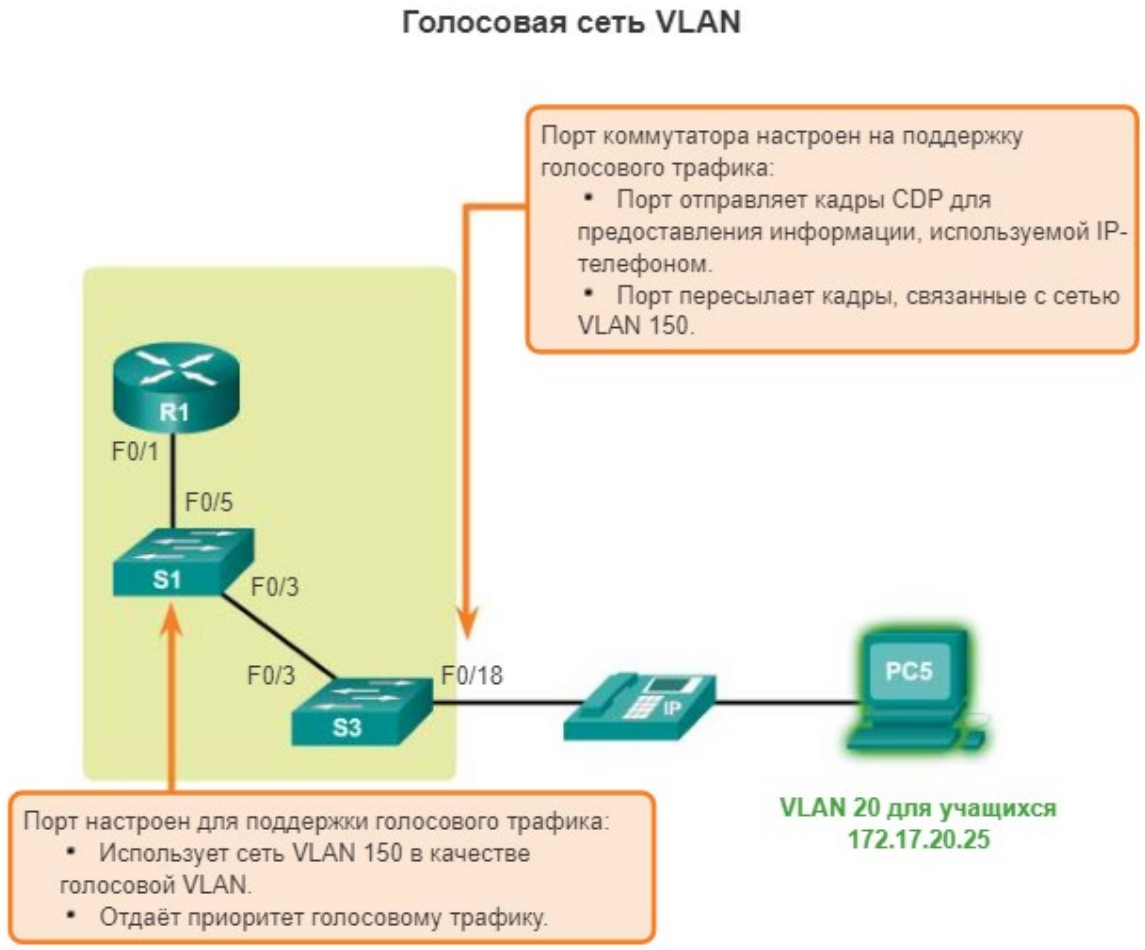
- гарантированная пропускная способность;

- высокий приоритет QoS;

- возможность избежать заторов;

- задержка менее 150 мс от источника к месту назначения.

Вся сеть должна быть спроектирована для поддержки голосовой связи.



3.2 СЕТИ VLAN В СРЕДЕ С НЕСКОЛЬКИМИ КОММУТАТОРАМИ

3.2.1 МАГИСТРАЛИ СЕТЕЙ VLAN

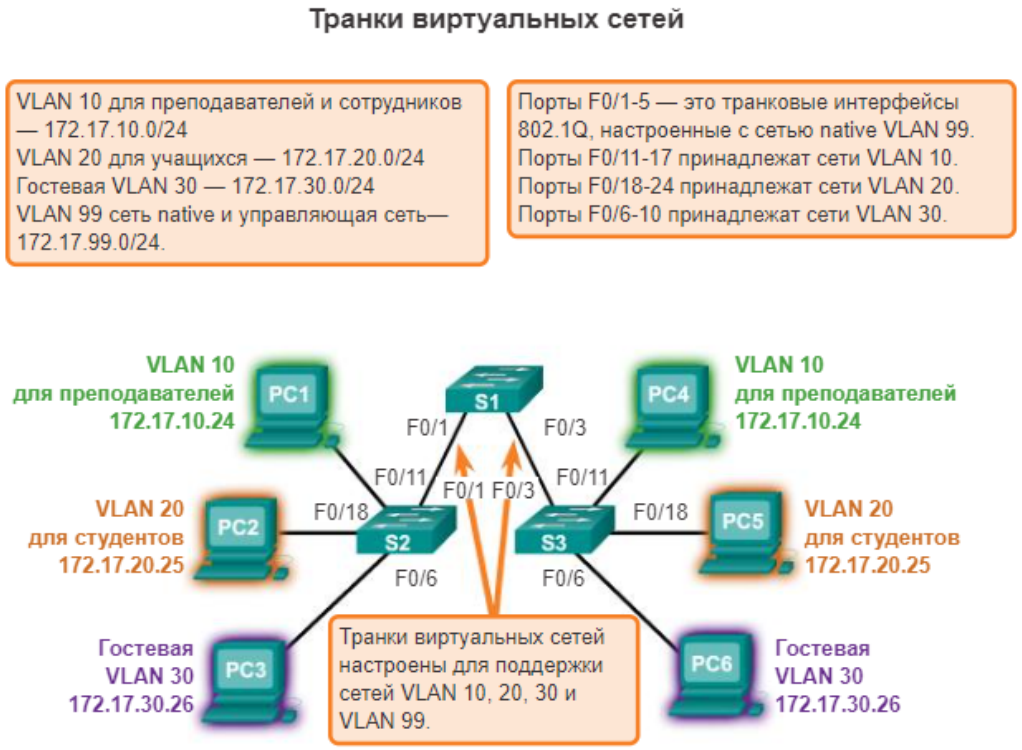
Транк — это канал типа «точка-точка» между двумя сетевыми устройствами, который поддерживает более одной сети VLAN. Транк виртуальных сетей расширяет сети VLAN по всей сети. Cisco поддерживает стандарт IEEE 802.1Q для координации транков в интерфейсах Fast Ethernet, Gigabit Ethernet и 10-Gigabit Ethernet.

Использование сетей VLAN без транковых каналов существенно снижает полезные возможности VLAN. Транки виртуальных сетей обеспечивают распространение всего трафика VLAN между коммутаторами так, чтобы устройства, находящиеся в одной сети VLAN, но подключённые к разным коммутаторам, могли обмениваться данными без вмешательства маршрутизатора.

3.2.1 МАГИСТРАЛИ СЕТЕЙ VLAN

Транк виртуальных сетей не принадлежит какой-либо определённой сети VLAN, а, скорее, является «кабельным каналом» передачи многих VLAN между коммутаторами и маршрутизаторами. Транк может также использоваться между сетевым устройством и сервером или другим устройством, оснащённым соответствующим сетевым адаптером с поддержкой 802.1Q. По умолчанию на транковом порте коммутатора Cisco Catalyst поддерживаются все сети VLAN.

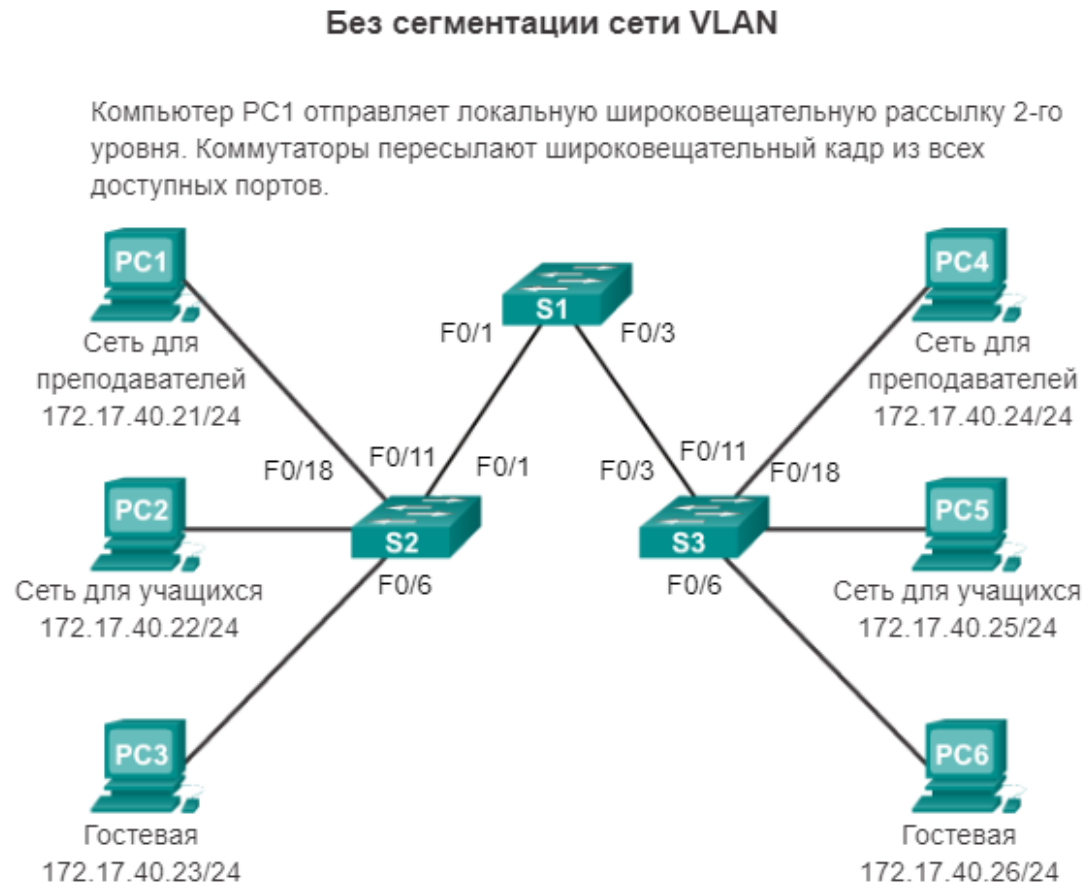
На рисунке каналы между коммутаторами S1 и S2, а также между S1 и S3 настроены для передачи трафика, отправляемого по всей сети от VLAN 10, 20, 30 и 99. Данная сеть не сможет работать без транковых каналов VLAN.



3.2.2 СЕТИ БЕЗ VLAN

При нормальной эксплуатации, когда коммутатор получает широковещательный кадр на одном из своих портов, он пересылает кадр из всех портов, кроме того, на котором он был получен. В анимации на рисунке вся сеть настроена в одной подсети (172.17.40.0/24), сети VLAN не настроены. В результате, когда компьютер преподавателя (PC1) отправляет широковещательный кадр, коммутатор S2 отправляет этот широковещательный кадр из всех своих портов. В конечном итоге вся сеть получает широковещательную рассылку, поскольку сеть является широковещательным доменом.

В случае когда сети VLAN реализованы на коммутаторе, передача одноадресного, многоадресного и широковещательного трафика от узла в определённой VLAN ведется устройствами в пределах этой сети VLAN.

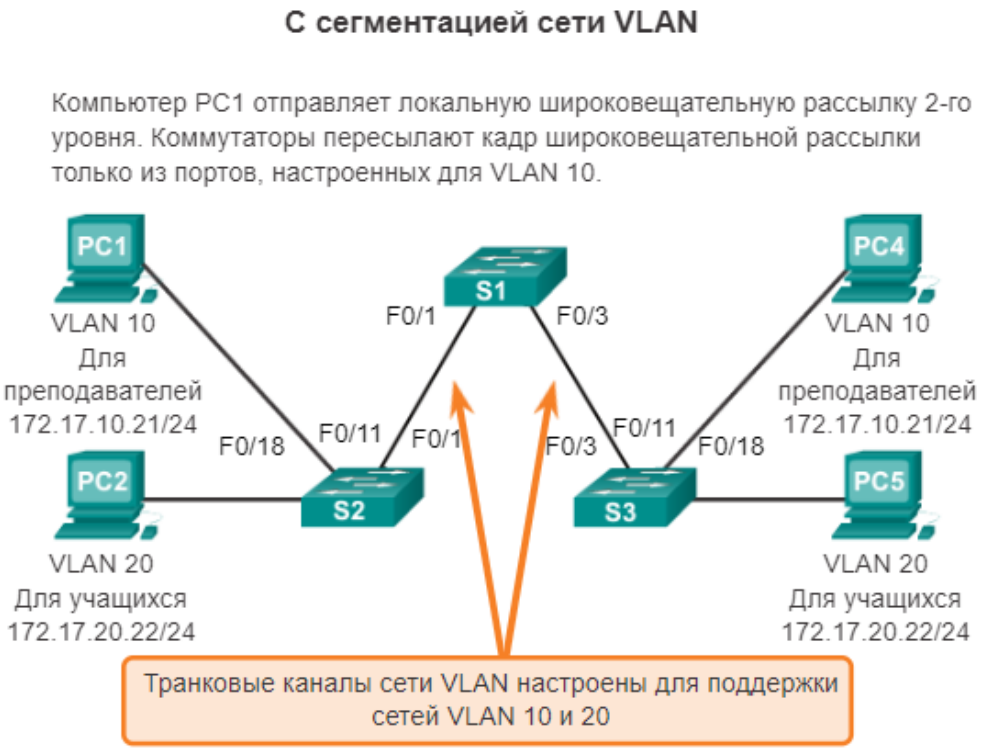


3.2.3 СЕТИ С VLAN

Как показано на рисунке, сеть была разделена на сегменты с помощью двух VLAN. Устройства для преподавателей были назначены сети VLAN 10, а устройства учащихся — сети VLAN 20. Когда из компьютера преподавателя (PC1) отправляется широковещательный кадр на коммутатор S2, коммутатор пересылает кадр только на те порты коммутатора, которые настроены для поддержки VLAN 10.

Порты, обеспечивающие соединение между коммутаторами S1 и S2 (порт F0/1) и между коммутаторами S1 и S3 (порт F0/3), являются транковыми каналами и настроены для поддержки всех VLAN в сети.

Когда коммутатор S1 получает широковещательный кадр через порт F0/1, он пересылает широковещательный кадр из единственного другого порта, настроенного для поддержки сети VLAN 10. При получении коммутатором S3 широковещательного кадра через порт F0/3 он пересылает широковещательный кадр из другого порта, настроенного для поддержки сети VLAN 10. Широковещательный кадр прибывает на единственный другой компьютер в сети, настроенный для VLAN 10.



3.2.4 ТЕГИРОВАНИЕ КАДРОВ ETHERNET ДЛЯ ИДЕНТИФИКАЦИИ СЕТИ VLAN

Коммутаторы серии Catalyst 2960 являются устройствами 2-го уровня. Для пересылки пакетов они используют данные заголовка кадра Ethernet. Они не содержат таблиц маршрутизации. Стандартный заголовок кадра Ethernet не содержит информацию о VLAN, к которой относится кадр. Поэтому, когда кадры Ethernet размещаются в транковом канале, необходимо добавить информацию о сетях VLAN, которым они принадлежат. Этот процесс называется тегированием и выполняется с помощью заголовка IEEE 802.1Q, указанного в стандарте IEEE 802.1Q. Заголовок 802.1Q содержит тег размером 4 байта, который добавляется в оригинальный заголовок кадра Ethernet и идентифицирует VLAN, к которой относится кадр.

Когда коммутатор получает кадр через порт, настроенный в режиме доступа и назначенный сети VLAN, коммутатор добавляет в заголовок кадра метку VLAN, заново вычисляет FCS и отправляет тегированный кадр из транкового порта.

3.2.4 ТЕГИРОВАНИЕ КАДРОВ ETHERNET ДЛЯ ИДЕНТИФИКАЦИИ СЕТИ VLAN

Поле тега VLAN состоит из поля типа, поля приоритета, поля идентификатора канонического формата и поля идентификатора VLAN.

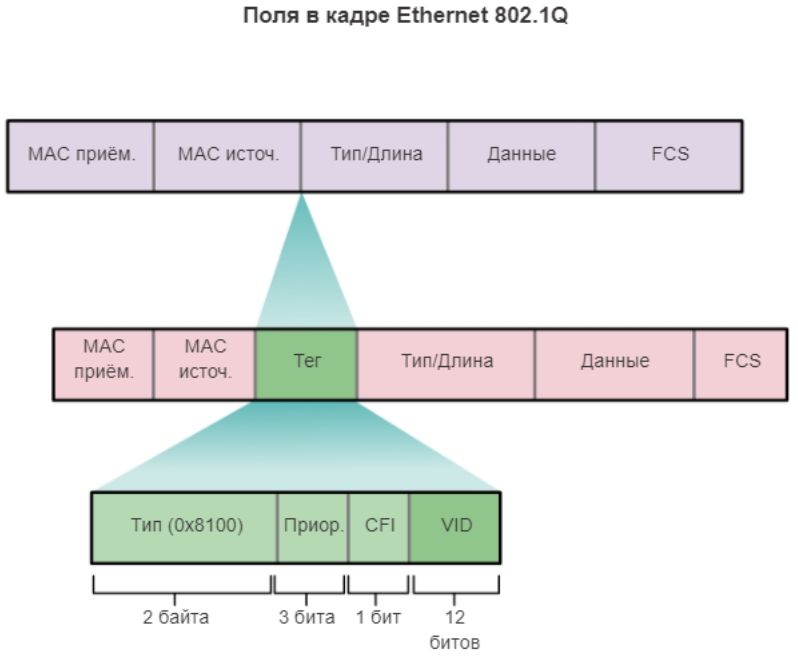
Тип — это 2-байтовое значение, которое называется значением идентификатора протокола тегирования (TPID). Значение для Ethernet имеет вид шестнадцатеричного числа 0x8100.

Приоритет пользователя — это 3-битовое значение, которое поддерживает реализацию уровня или сервиса.

Идентификатор канонического формата (CFI) — это 1-битовый идентификатор, который обеспечивает передачу кадров Token Ring по каналам Ethernet.

VLAN-идентификатор (VID) — это 12-битный идентификационный номер VLAN, который поддерживает до 4096 идентификаторов VLAN.

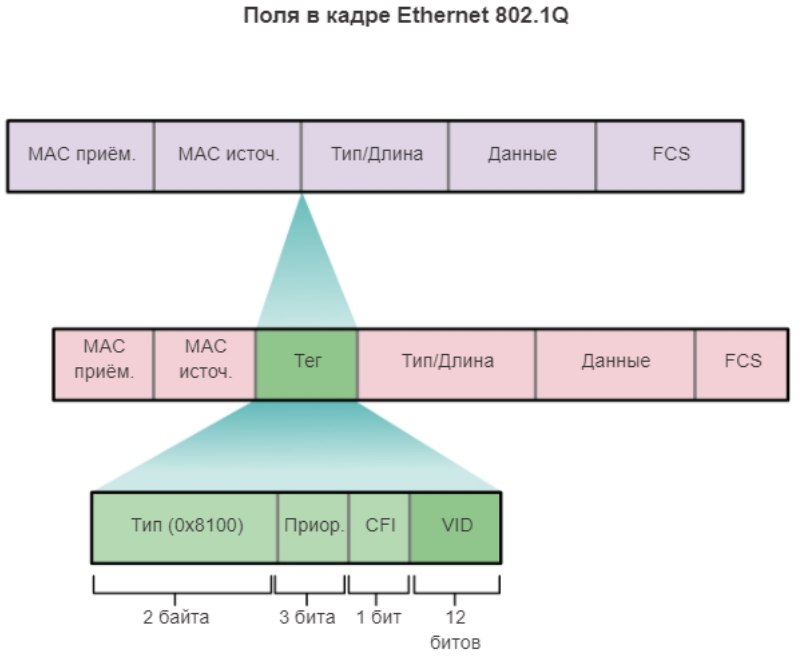
После того как коммутатор добавит поля типа и управляющей информации тега, он пересчитывает значения FCS и добавляет в кадр новое значение FCS.



3.2.4 ТЕГИРОВАНИЕ КАДРОВ ETHERNET ДЛЯ ИДЕНТИФИКАЦИИ СЕТИ VLAN

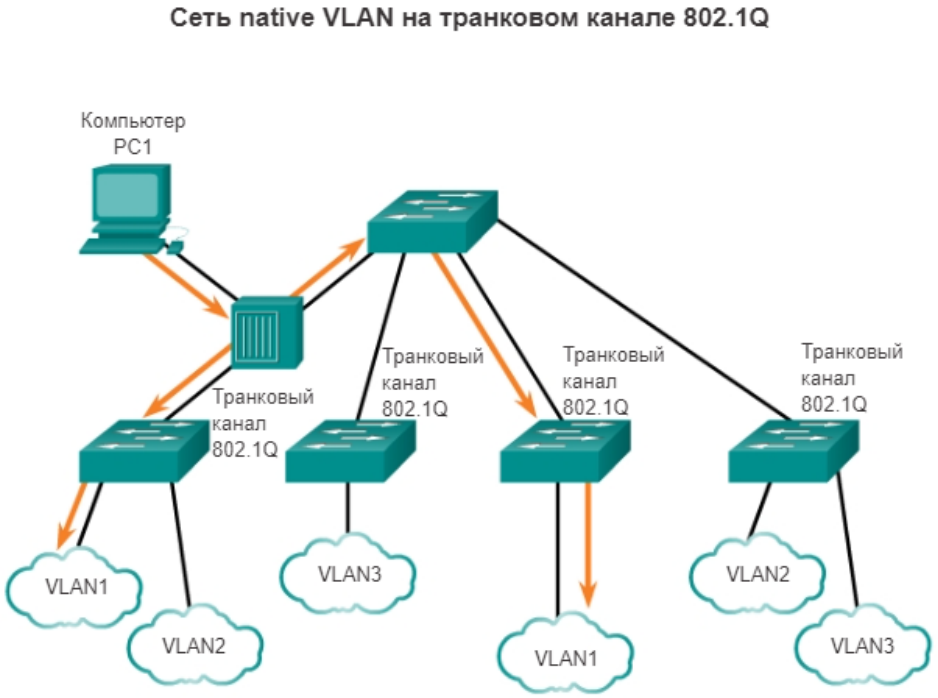
Тегированные кадры в сети native VLAN

Некоторые устройства, поддерживающие транковую связь, добавляют метку в трафик сети native VLAN. Управляющий трафик, отправляемый в сети native VLAN, тегировать не следует. Если транковый порт 802.1Q получает тегированный кадр с таким же идентификатором VLAN, как у сети native VLAN, то он отбрасывает кадр. Следовательно, при настройке порта коммутатора в коммутаторе Cisco настраивайте устройства таким образом, чтобы они не отправляли тегированные кадры по сети native VLAN. К устройствам от других производителей, которые поддерживают тегированные кадры в сети native VLAN, относятся IP-телефоны, серверы, маршрутизаторы и коммутаторы не от Cisco.



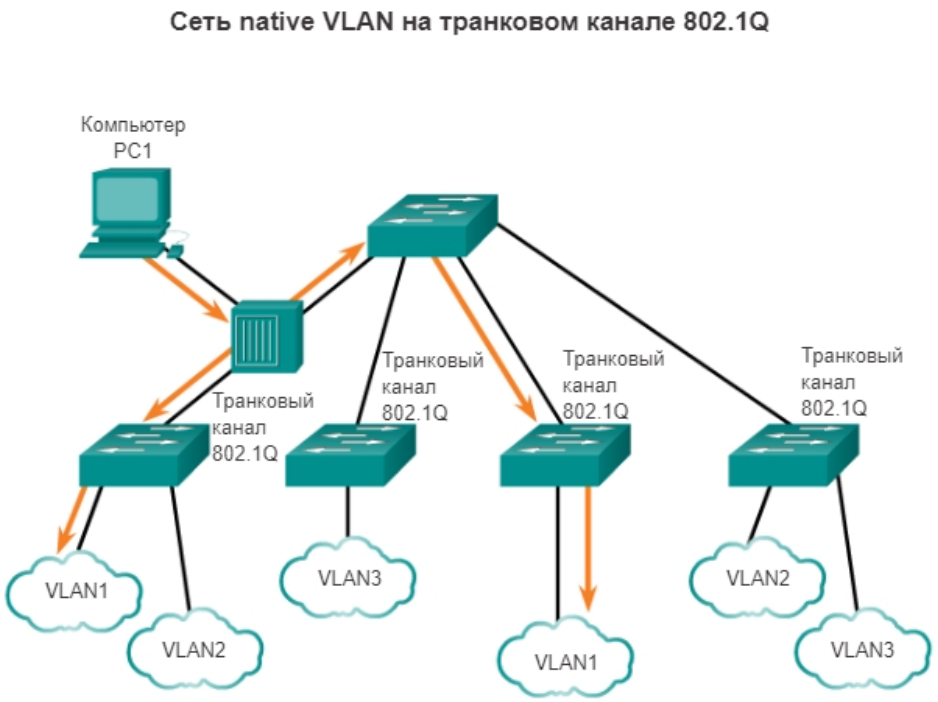
3.2.5 VLAN С НЕТЕГИРОВАННЫМ ТРАФИКОМ И ТЕГИРОВАНИЕ ПО ПРОТОКОЛУ 802.1Q

Когда транковый порт коммутатора Cisco получает нетегированные кадры (которые редко встречаются в хорошо спроектированной сети), он пересылает эти кадры в сеть native VLAN. Если с сетью native VLAN не связаны никакие устройства (что бывает довольно часто), а также нет других транковых портов (что также часто случается), то кадр отбрасывается. Сетью native VLAN по умолчанию является сеть VLAN 1. При настройке транкового порта 802.1Q порту идентификатора VLAN по умолчанию (PVID) присваивают значение идентификатора сети native VLAN. Весь нетегированный трафик, поступающий в порт 802.1Q или из него, пересылается в соответствии со значением PVID. Например, если сеть VLAN 99 настроена в качестве native VLAN, то значение PVID равно 99, а весь нетегированный трафик пересылается в сеть VLAN 99. Если сеть native VLAN не была перенастроена, то значение PVID присваивается равным 1.



3.2.5 VLAN С НЕТЕГИРОВАННЫМ ТРАФИКОМ И ТЕГИРОВАНИЕ ПО ПРОТОКОЛУ 802.1Q

На рисунке компьютер PC1 подключен к транковому каналу 802.1Q с помощью концентратора. PC1 отправляет нетегированный трафик, который коммутаторы связывают с сетью native VLAN, настроенной на транковых портах, и пересылают его соответствующим образом. Тегированный трафик в транковом канале, полученный компьютером PC1, отбрасывается. В этом сценарии сеть является плохо спроектированной по нескольким причинам: в ней используется концентратор, имеется узел, подключённый к транковому каналу, и это означает, что существуют порты доступа коммутаторов, назначенные сети native VLAN. Но в этом сценарии иллюстрируется необходимость в спецификации IEEE 802.1Q для native VLAN как средства обработки устаревших сценариев.



3.2.6 ТЕГИРОВАНИЕ ГОЛОСОВОЙ СЕТИ VLAN

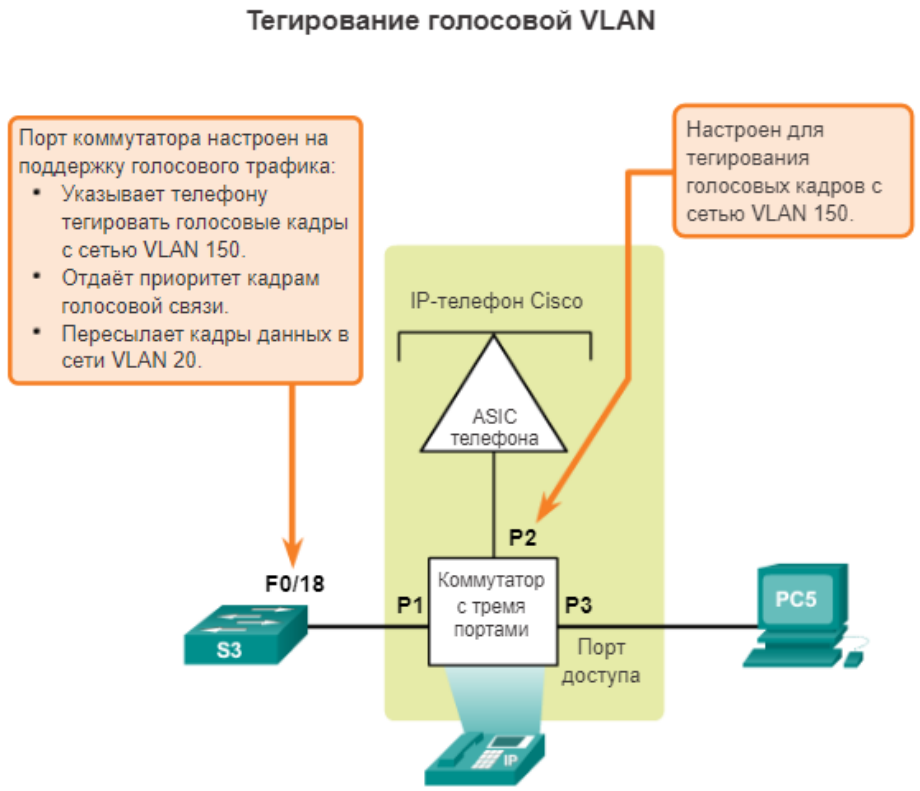
Порт доступа, используемый для подключения IP-телефона Cisco, может быть настроен для использования двух отдельных сетей VLAN: одна сеть VLAN для голосового трафика, а другая сеть VLAN для трафика данных от устройства, подключенного к телефону. Канал между коммутатором и IP-телефоном служит транковым каналом для передачи и голосового трафика, и трафика данных.

IP-телефон Cisco содержит встроенный коммутатор 10/100 на 3 порта. Порты обеспечивают выделенные подключения следующим устройствам:

- порт 1 подключается к коммутатору или другому устройству VoIP;

- порт 2 является внутренним интерфейсом 10/100, через который передаётся трафик IP-телефона;

- порт 3 (порт доступа) подключается к ПК или другому устройству.



3.2.6 ТЕГИРОВАНИЕ ГОЛОСОВОЙ СЕТИ VLAN

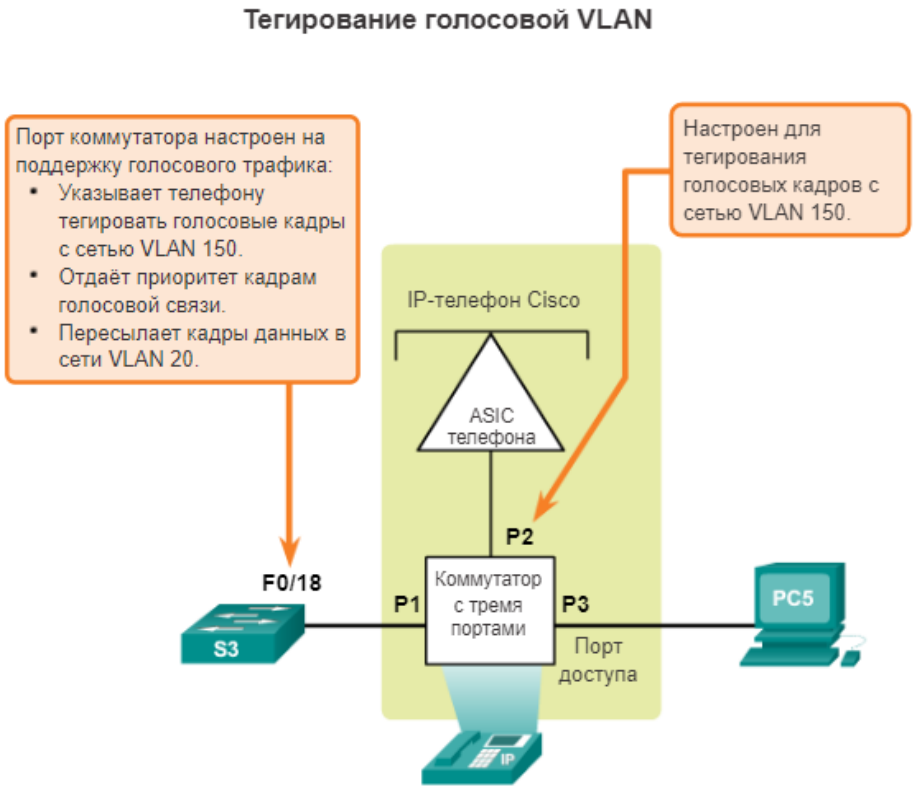
На коммутаторе доступ настроен для отправки пакетов протокола CDP, указывающих подключённому IP-телефону отправлять голосовой трафик на коммутатор одним из трёх способов, в зависимости от типа трафика:

- в голосовой VLAN, тегированной значением приоритета класса обслуживания (CoS) уровня 2;

- в VLAN доступа, тегированной значением приоритета CoS уровня 2;

- в нетегированной VLAN доступа (без значения приоритета CoS уровня 2).

На рисунке компьютер учащегося PC5 подключён к IP-телефону Cisco, а телефон подключён к коммутатору S3. VLAN 150 предназначена для передачи голосового трафика, а PC5 находится в VLAN 20, используемой для данных учащихся.



3.2.6 ТЕГИРОВАНИЕ ГОЛОСОВОЙ СЕТИ VLAN

На рисунке приведён пример выходных данных. В рамках данной темы не рассматриваются команды Cisco IOS голосовой связи, но в выделенных областях в примере выходных данных показан интерфейс F0/18, настроенный с сетью VLAN для данных (VLAN 20) и сетью VLAN для голосовой связи (VLAN 150).

```
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: 20 (student)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 150 (voice)
```

3.3 КОНФИГУРАЦИЯ VLAN
3.3.1 ДИАПАЗОНЫ VLAN НА КОММУТАТОРАХ CATALYST

Виртуальные локальные сети стандартного диапазона

Используются в малых и средних сетях предприятий и организаций.

Определяются идентификатором VLAN от 1 до 1005.

Идентификаторы от 1002 до 1005 зарезервированы для сетей VLAN Token Ring и FDDI.

Идентификаторы 1 и идентификаторы от 1002 до 1005 создаются автоматически и не могут быть удалены.

Конфигурации хранятся в файле базы данных VLAN под именем vlan.dat. Файл vlan.dat расположен во флеш-памяти коммутатора.
Протокол VTP (транковый протокол VLAN), помогающий управлять конфигурациями VLAN между коммутаторами, может распознавать и хранить только сети VLAN стандартного диапазона.

```
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
```

3.3.1 ДИАПАЗОНЫ VLAN НА КОММУТАТОРАХ CATALYST

Сети VLAN расширенного диапазона

Позволяют операторам связи расширять свою инфраструктуру для большого числа клиентов. Некоторым крупным международным корпорациям нужны идентификаторы VLAN расширенного диапазона.

Определяются идентификатором VLAN от 1006 до 4094.

Конфигурации сетей не записываются в файл vlan.dat.

Поддерживают меньше функций VLAN, чем сети VLAN стандартного диапазона.

По умолчанию сохраняются в файл текущей конфигурации.

Протокол VTP не распознаёт сети VLAN расширенного диапазона.

Примечание. 4096 — это максимальное количество VLAN, доступных на коммутаторах Catalyst, поскольку в поле идентификатора VLAN заголовка IEEE 802.1Q насчитывается 12 бит.

3.3.2 КОМАНДЫ СОЗДАНИЯ VLAN

При настройке сетей VLAN стандартного диапазона сведения о конфигурации хранятся во флеш-памяти коммутатора в файле под именем vlan.dat. Флеш-память является постоянной, поэтому не требует выполнения команды **copy running-config startup-config**. Однако, поскольку во время создания сетей VLAN на коммутаторе Cisco часто необходимо настраивать и другие параметры, рекомендуется сохранять изменения текущей конфигурации в начальную загрузочную конфигурацию.

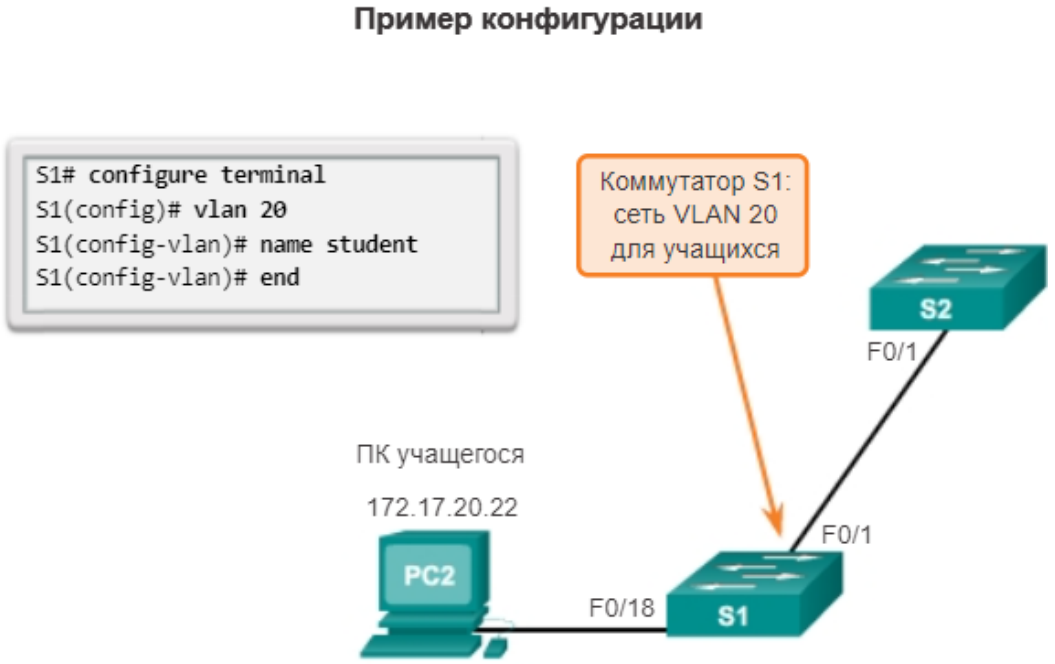
Задача	**Команда IOS**
Войдите в режим глобальной настройки.	Switch# **configure terminal**
Создайте сеть VLAN с допустимым номером идентификатора.	Switch(config)# **vlan** *vlan-id*
Укажите уникальное имя для идентификации сети VLAN.	Switch(config-vlan)# **name** *vlan-name*
Вернитесь в привилегированный режим.	Switch (config-vlan) # **end**
Войдите в режим глобальной настройки.	Switch# **configure terminal**

3.3.2 КОМАНДЫ СОЗДАНИЯ VLAN

На рисунке показано, каким образом на коммутаторе S1 настраивается сеть VLAN для учащихся (VLAN 20). В примере топологии компьютер учащегося (компьютер PC2) не был привязан к сети VLAN, но имеет IP-адрес 172.17.20.22.

Помимо введения одного идентификатора VLAN, можно ввести группу идентификаторов VLAN, разделённых точками, или диапазон идентификаторов VLAN, разделённых дефисами, с помощью команды vlan vlan-id. Например, для создания сетей VLAN 100, 102, 105, 106 и 107 используйте следующую команду:

S1(config)# vlan 100,102,105-107



3.3.3 КОМАНДЫ НАЗНАЧЕНИЯ ПОРТОВVLAN

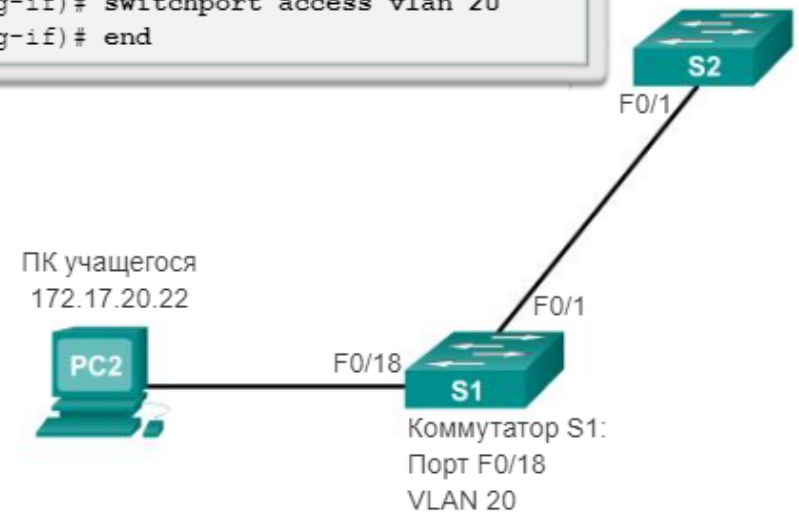
Следующий шаг после создания сети VLAN — назначение портов сетям VLAN. Порт доступа может одновременно принадлежать только одной VLAN. Единственным исключением из этого правила является порт, подключённый к IP-телефону. В этом случае с портом связаны две VLAN: одна для голосовой связи и одна для данных.
На рисунке показан синтаксис для определения порта в качестве порта доступа и назначения его сети VLAN. Выполнять команду **switchport mode access** необязательно, но настоятельно рекомендуется в целях обеспечения безопасности. С помощью этой команды интерфейс переходит в режим постоянного доступа.
Примечание. Используйте команду **interface range**, чтобы одновременно настроить несколько интерфейсов.

Задача	Команда
Войдите в режим глобальной настройки.	Switch# **configure terminal**
Войдите в режим конфигурации интерфейса.	Switch(config)# **interface** *interface-id*
Переведите порт в режим доступа.	Switch(config-if)# **switchport mode access**
Назначьте порт сети VLAN.	Switch(config-if)# **switchport access vlan** *vlan-id*
Вернитесь в привилегированный режим.	Switch(config-if)# **end**

3.3.3 КОМАНДЫ НАЗНАЧЕНИЯ ПОРТОВVLAN

В примере на рисунке VLAN 20 назначена порту F0/18 на коммутаторе S1; таким образом, компьютер учащегося (компьютер PC2) расположен в сети VLAN 20. При настройке VLAN 20 на других коммутаторах сетевой администратор знает, что нужно настроить другие компьютеры учащихся к той же подсети, в которой находится компьютер PC2 (172.17.20.0/24).

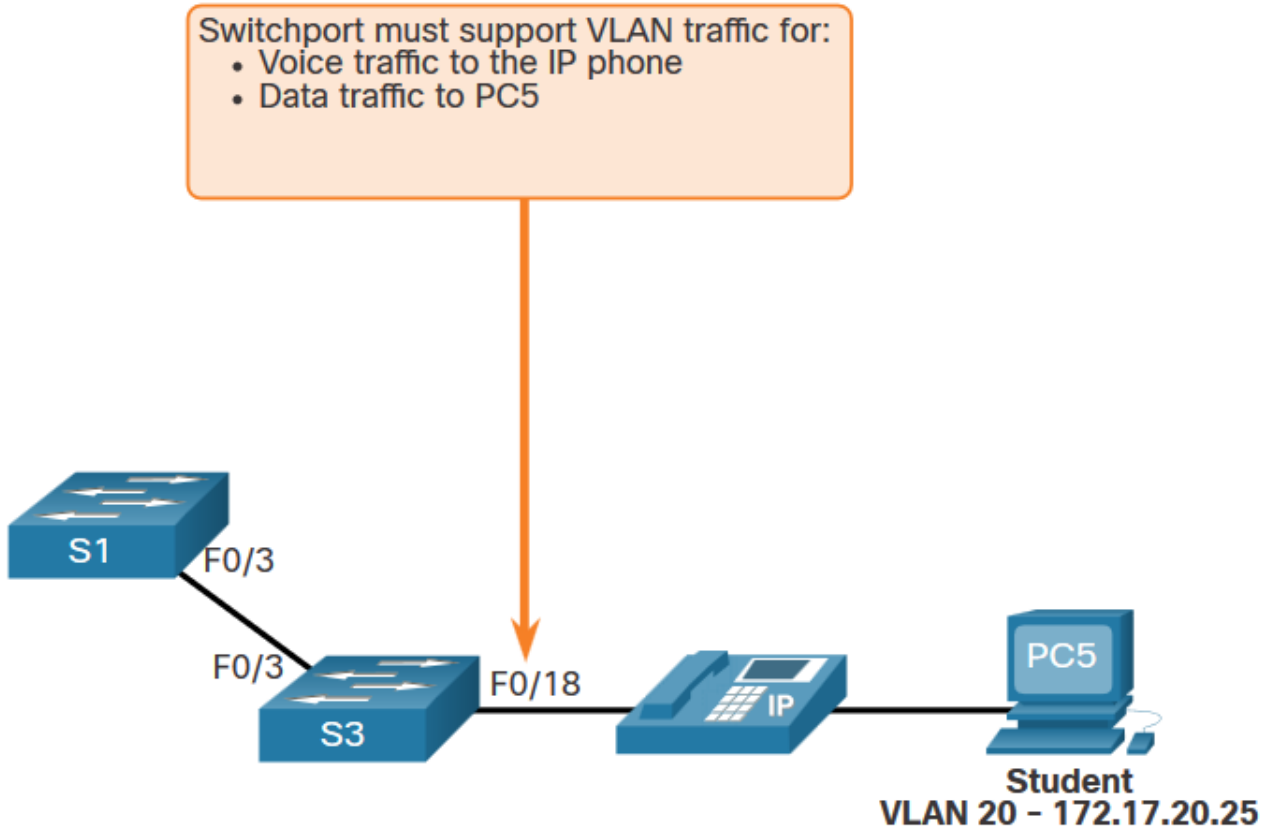
```
s1# configure terminal
s1(config)# interface F0/18
s1(config-if)# switchport mode access
s1(config-if)# switchport access vlan 20
s1(config-if)# end
```



Команда **switchport access vlan** принудительно создаёт VLAN, если таковая ещё не существует на коммутаторе. Например, сеть VLAN 30 отсутствует в выходных данных команды **show vlan brief** на коммутаторе. Если на любом интерфейсе без предыдущей конфигурации ввести команду **switchport access vlan 30**, то коммутатор отобразит следующее:
% Access VLAN does not exist. Creating vlan 30

3.3.4 ДАННЫЕ КОНФИГУРАЦИИ VLAN И ГОЛОСОВЫЕ VLAN

Порт доступа можно назначить только одной сети VLAN. Однако он также может быть назначен одной голосовой VLAN, если телефон и конечное устройство исходят от одного порта коммутатора.



3.3.4 ДАННЫЕ КОНФИГУРАЦИИ VLAN И ГОЛОСОВЫЕ VLAN

Мы хотим создать и назвать голосовую VLAN и VLAN для данных.

Помимо назначения VLAN для данных, мы также назначим голосовую VLAN и включим QoS для голосового трафика к интерфейсу.

Новый коммутатор catalyst автоматически создаст VLAN, если она еще не существует, когда она будет назначена интерфейсу.

Примечание. Реализация QoS выходит за рамки этого курса. Здесь мы показываем использование команды **mls qos trust [cos | устройство cisco-phone | dscp | ip-precedence].**

```
S1(config)# vlan 20
S1(config-vlan)# name student
S1(config-vlan)# vlan 150
S1(config-vlan)# name VOICE
S1(config-vlan)# exit
S1(config)# interface fa0/18
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# mls qos trust cos
S1(config-if)# switchport voice vlan 150
S1(config-if)# end
```

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

3.3.5 ПРОВЕРКА КОНФИГУРАЦИЮ СЕТИ VLAN

Использование команды **show vlan** Полный синтаксис:

show vlan [brief | id vlan-id | name vlan-name | summary]

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

```
S1# show interface vlan 20
Vlan20 is up, line protocol is up
  Hardware is EtherSVI, address is 001f.6ddb.3ec1 (bia 001f.6ddb.3ec1)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set

(Output omitted)
```

Задача	Вариант команды
Отображает имя, состояние и порты VLAN по одной VLAN на строку.	**brief**
Отображает информацию об отдельной VLAN, определяемой по номеру идентификатора VLAN.	**id** *vlan-id*
Отображает информацию об имени одной сети VLAN. *Имя VLAN*— это код ASCII размером от 1 до 32 символов.	**name** *vlan-name*
Отобразите общую информацию о VLAN.	**summary**

3.3.6 ИЗМЕНЕНИЕ НАЗНАЧЕНИЯ ПОРТА VLAN

Существует несколько способов изменить членство в VLAN:

- повторно использовать команду **switchport access vlan vlan-id**;

- использовать команду **no switchport access vlan** для возвращения интерфейса обратно во VLAN 1.

Используйте команды **show vlan brief** или **show interface fa0/18 switchport** для проверки правильности настройки VLAN.

```
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
```

```
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)
```

3.3.7 УДАЛЕНИЕ VLAN

Удалите VLAN с помощью команды **no vlan vlan-id** .

Внимание! Перед удалением сети VLAN необходимо сначала переназначить все ее порты другой сети VLAN.

Удалите все VLAN с помощью команды **delete flash:vlan.dat** или команды **delete vlan.dat**.

Перезагрузите коммутатор после удалении всех VLAN.

Примечание. Чтобы восстановить заводское значение по умолчанию — отключите все кабели для передачи данных, удалите начальную конфигурацию и удалите файл vlan.dat, а затем перезагрузите устройство.

3.4 МАГИСТРАЛИ СЕТИ VLAN
3.4.1 КОМАНДЫ КОНФИГУРАЦИИ ТРАНКА

Транк виртуальной сети — это канал OSI 2-го уровня между двумя коммутаторами, который передаёт трафик во все сети VLAN (если список допустимых сетей VLAN не ограничен вручную или динамически). Для того чтобы активировать транковые каналы, настройте порты на любом конце физического канала с помощью параллельных наборов команд.

Чтобы настроить порт коммутатора на одном конце транкового канала, используйте команду **switchport mode trunk**. С помощью этой команды интерфейс переходит в постоянный транковый режим. На порте начинается согласование протокола DTP для преобразования канала в транковый, даже если интерфейс, подключённый к нему, не соглашается на подобное изменение. Протокол DTP описан в следующем разделе. В данном курсе команда **switchport mode trunk** является единственным способом настройки транкового канала.

На рисунке на следующем слайде показан синтаксис команды Cisco IOS для определения сети native VLAN (кроме VLAN 1).

Для того чтобы определить список сетей VLAN, разрешённых на транковом канале, используйте команду Cisco IOS **switchport trunk native vlan vlan-list**.

3.4.1 КОМАНДЫ КОНФИГУРАЦИИ ТРАНКА

Задача	Команда IOS
Войдите в режим глобальной настройки.	Switch# **configure terminal**
Войдите в режим конфигурации интерфейса.	Switch(config)# **interface** *interface-id*
Установите порт в режим постоянной магистрали.	Switch(config-if)# **switchport mode trunk**
Установите в качестве VLAN с нетегированным трафиком сеть, отличную от VLAN 1.	Switch(config-if)# **switchport trunk native vlan** *vlan-id*
Укажите список сетей VLAN, которым разрешен доступ в магистральный канал.	Switch(config-if)# **switchport trunk allowed vlan** *vlan-list*
Вернитесь в привилегированный режим.	Switch(config-if)# **end**

3.4.1 КОМАНДЫ КОНФИГУРАЦИИ ТРАНКА

К каждой VLAN относятся следующие подсети:

VLAN 10 - Faculty/Staff - 172.17.10.0/24

VLAN 20 - Students - 172.17.20.0/24

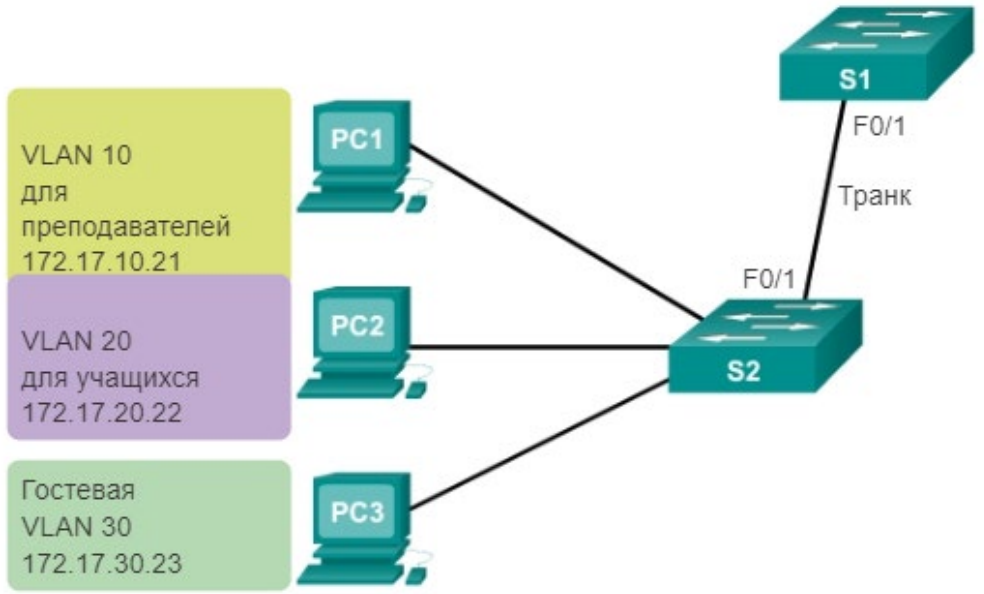
VLAN 30 - Guests - 172.17.30.0/24

VLAN 99 - Native - 172.17.99.0/24

Порт F0/1 на S1 настроен как магистральный порт.

Примечание. Эта конфигурация предполагает применение коммутаторов Cisco Catalyst 2960, которые автоматически используют инкапсуляцию 802.1Q для магистральных каналов. Другие коммутаторы могут потребовать ручной настройки инкапсуляции. Всегда настраивайте оба конца транкового канала с одной и той же сетью native VLAN. Если конфигурация транка 802.1Q на обоих концах различается, то ПО Cisco IOS сообщит об ошибке.

Командная строка	Команда
S1(config)#	Interface fa0/18
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



3.4.2 ПРОВЕРКА НАСТРОЕК ТРАНКА

На рисунке показана конфигурация порта F0/1 на коммутаторе S1. Конфигурацию можно проверить с помощью команды **show interfaces interface-ID switchport.**

В верхней выделенной области показано, что административный режим порта F0/1 настроен на trunk. Порт находится в режиме транка. В следующей выделенной области видно, что сеть native VLAN — это VLAN 99. Далее в нижней выделенной области выходных данных показано, что все VLAN в транковом канале активны.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode trunk
S1(config-if)# no switchport trunk native vlan 99
S1(config-if)# end
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)
```

3.4.3 СБРОС МАГИСТРАЛИ В СОСТОЯНИЕ ПО УМОЛЧАНИЮ

На рисунке показаны команды для удаления разрешённых сетей VLAN и сброса сети native VLAN транка. После сброса до состояния по умолчанию транк разрешает все VLAN и использует VLAN 1 в качестве native VLAN.

Команды коммутатора Cisco под управлением ОС IOS	
Войдите в режим глобальной конфигурации.	`S1# configure terminal`
Войдите в режим конфигурации интерфейса для SVI.	`S1(config)# interface` *`interface_id`*
Разрешите доступ к транковому каналу для всех сетей VLAN.	`S1(config-if)# no switchport trunk allowed vlan`
Сбросьте конфигурацию сети native VLAN до настроек по умолчанию.	`S1(config-if)# no switchport trunk native vlan`
Вернитесь в привилегированный режим.	`S1(config-if)# end`

3.4.3 СБРОС МАГИСТРАЛИ В СОСТОЯНИЕ ПО УМОЛЧАНИЮ

На рисунке показаны команды, используемые для сброса всех параметров транкового интерфейса до параметров по умолчанию. Команда **show interfaces f0/1 switchport** показывает, что транковый канал был восстановлен в состояние 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)
```

3.4.3 СБРОС МАГИСТРАЛИ В СОСТОЯНИЕ ПО УМОЛЧАНИЮ

На рисунке пример выходных данных показывает команды, используемые для удаления транковой функции из порта F0/1 из коммутатора S1. Команда **show interfaces f0/1 switchport** показывает, что теперь интерфейс f0/1 находится в режиме статического доступа.

```
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)
```

3.5 ПРОТОКОЛ ДИНАМИЧЕСКОГО ТРАНКИНГА (DTP)

3.5.1 ОБЩИЕ СВЕДЕНИЯ О DTP

Транковые интерфейсы Ethernet поддерживают различные транковые режимы. Интерфейс может быть установлен в транковый или нетранковый режим либо настроен для согласования транковой связи с соседним интерфейсом. Согласование транкового канала выполняется протоколом динамического создания транкового канала (DTP), который действует только по принципу сквозного подключения между устройствами сети.

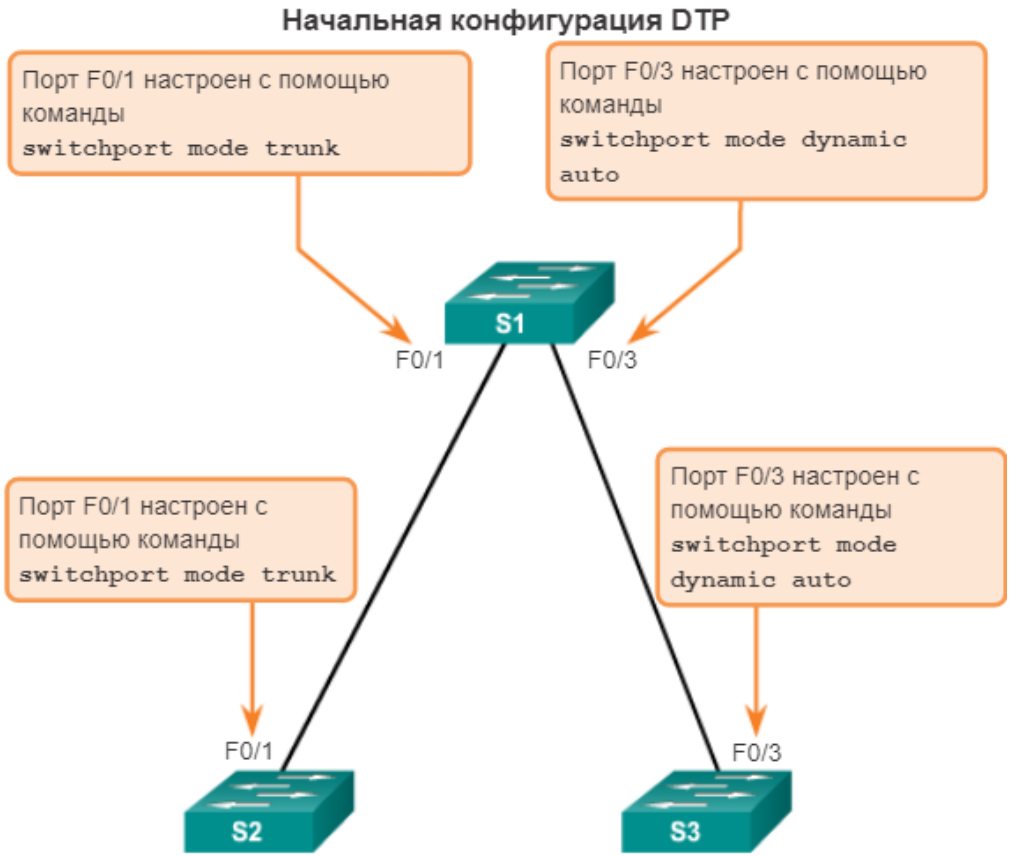
Протокол DTP — это запатентованный протокол Cisco, который автоматически включён на коммутаторах Catalyst 2960 и Catalyst 3560. Коммутаторы других производителей не поддерживают DTP. DTP управляет транковым согласованием только в случае, если порт соседнего коммутатора настроен в режиме транка, который поддерживает DTP.

Внимание! Некоторые межсетевые устройства могут пересылать кадры DTP неправильно, из-за чего могут возникнуть ошибки конфигурации. Чтобы этого избежать, отключите DTP на интерфейсах коммутатора Cisco, который подключён к устройствам, не поддерживающим DTP.

3.5.1 ОБЩИЕ СВЕДЕНИЯ О DTP

Как показано на рисунке, по умолчанию функция DTP для коммутаторов Cisco Catalyst серии 2960 и 3560 настроена на динамический автоматический режим на интерфейсе F0/3 коммутаторов S1 и S3.

Для того чтобы включить транковую связь от коммутатора Cisco к устройству, которое не поддерживает DTP, используйте команды режима конфигурации интерфейса **switchport mode trunk** и **switchport nonegotiate**. Команда преобразует интерфейс в транковый канал, но не позволяет ему создавать кадры DTP.



3.5.1 ОБЩИЕ СВЕДЕНИЯ О DTP

На рисунке канал между коммутаторами S1 и S2 становится транковым, поскольку порты F0/1 на коммутаторах S1 и S2 настроены для игнорирования всех объявлений DTP и перехода в режим транкового порта. Порты F0/3 на коммутаторах S1 и S3 настроены на динамический автоматический режим, поэтому после согласования они будут переведены в состояние режима доступа. Таким образом, создаётся неактивный транковый канал. При настройке порта в транковый режим используйте команду **switchport mode trunk**. Всегда ясно, в каком состоянии находится транк: он всегда в рабочем состоянии. С этой конфигурацией несложно запомнить, в каком состоянии находятся транковые порты. Если порт должен быть транковым, то и режим настроен на транковый.

3.5.2 РЕЖИМЫ ИНТЕРФЕЙСА ДЛЯ СОГЛАСОВАНИЯ

Интерфейсы Ethernet на коммутаторах Catalyst 2960 и Catalyst 3560 поддерживают различные транковые режимы с помощью протокола DTP:

switchport mode access — переводит интерфейс (порт доступа) в постоянный нетранковый режим и сообщает, что канал преобразован в нетранковый канал. Интерфейс становится нетранковым вне зависимости от того, является ли соседний интерфейс транковым или нет.

switchport mode dynamic auto — позволяет интерфейсу преобразовывать канал в транковый канал. Интерфейс становится транковым, если соседний интерфейс переведён в транковый или рекомендуемый режим. Режим порта коммутатора по умолчанию для всех интерфейсов Ethernet — **dynamic auto**.

switchport mode dynamic desirable — предписывает интерфейсу преобразовывать канал в транковый канал. Интерфейс становится транковым, если соседний интерфейс переведён в транковый, рекомендуемый или автоматический режим. Данный режим коммутатора порта используется по умолчанию на старых коммутаторах, например на коммутаторах Catalyst 3550 и 2950.

3.5.2 РЕЖИМЫ ИНТЕРФЕЙСА ДЛЯ СОГЛАСОВАНИЯ

switchport mode trunk — переводит интерфейс в постоянный транковый режим и согласовывает для преобразования соседнего канала в транковый канал. Интерфейс становится транковым, даже если соседний интерфейс не является таковым.

switchport nonegotiate — запрещает интерфейсу создавать кадры DTP. Эту команду можно использовать только в том случае, если режим порта коммутатора интерфейса находится в режиме access или trunk. Чтобы установить транковый канал, необходимо вручную настроить соседний интерфейс в качестве транкового интерфейса.

Параметр	Описание
access	Режим постоянного доступа и согласовывает преобразование соседнего канала в канал доступа
dynamic auto	Будет становиться интерфейсом магистрали, если соседний интерфейс установлен в транк или режим desirable
dynamic desirable	Активно стремится стать магистралью путем переговоров с другими auto или desirable интерфейсами
trunk	режим постоянного транкинга и согласовывает преобразование соседнего канала в trunk

3.5.2 РЕЖИМЫ ИНТЕРФЕЙСА ДЛЯ СОГЛАСОВАНИЯ

Варианты конфигурации DTP являются следующими:

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Ограниченные возможности подключения
Access	Access	Access	Ограниченные возможности подключения	Access

3.5.3 ПРОВЕРКА РЕЖИМА DTP

Конфигурация DTP по умолчанию зависит от версии и платформы Cisco IOS.

Используйте команду **show dtp interface** для определения текущего режима DTP.

В соответствии с рекомендациями рекомендуется установить для интерфейсов режим доступа или транк и отключить DTP.

```
S1# show dtp interface fa0/1
DTP information for FastEthernet0/1:
TOS/TAS/TNS: ACCESS/AUTO/ACCESS
TOT/TAT/TNT: NATIVE/NEGOTIATE/NATIVE
Neighbor address 1: C80084AEF101
Neighbor address 2: 000000000000
Hello timer expiration (sec/state): 11/RUNNING
Access timer expiration (sec/state): never/STOPPED
Negotiation timer expiration (sec/state): never/STOPPED
Multidrop timer expiration (sec/state): never/STOPPED
FSM state: S2:ACCESS
# times multi & trunk 0
Enabled: yes
In STP: no
```