**[Виртуальные локальные сети (VLAN)](https://static-course-assets.s3.amazonaws.com/RSE503/ru/index.html" \l "3)**

**и транковые каналы**

**Введение**

Производительность сети является важным фактором эффективности работы организации. Одной из технологий повышения производительности сети является разделение крупных широковещательных доменов на более мелкие. Маршрутизаторы устроены таким образом, что блокируют широковещательный трафик на интерфейсе. При этом маршрутизаторы обычно имеют ограниченное количество интерфейсов LAN. Основная роль маршрутизатора заключается в передаче информации между сетями, а не в предоставлении оконечные устройства доступа к сети.

Предоставление доступа в локальную сеть обычно обеспечивается коммутатором уровня доступа. Для уменьшения размера широковещательных доменов на коммутаторе 2-го уровня, как и на устройстве 3-го уровня, можно создать сеть VLAN. Сети VLAN обычно включаются в проекты сети, для того чтобы сеть облегчала процесс достижения целей организации. Несмотря на то, что сети VLAN в основном используются в коммутируемых локальных сетях, современные реализации VLAN способны функционировать также в муниципальных (MAN) и глобальных (WAN) сетях.

В этой главе рассматриваются различные аспекты конфигурации, управления, поиска и устранения проблем в сетях VLAN и транковых каналах VLAN. Кроме того, в рамках главы вам предстоит изучить вопросы обеспечения безопасности и стратегии, связанные с VLAN и транковыми каналами, а также ознакомиться с практическими рекомендациями по разработке VLAN.

# Работа в аудитории. Телепакет на отпуск

**Телепакет на отпуск**

**Сценарий**

Вы купили трехэтажный дом для отдыха на пляже и планируете сдавать его в аренду. Планировка всех этажей одинакова. На каждом этаже имеется цифровое телевидение.

В соответствии с правилами местного интернет-провайдера в один пакет подписки может входить не более трех станций. Ваша задача — определить, какие телевизионные пакеты вы предложите своим гостям.

* Аудитория делится на группы по три человека в каждой.
* Выберите три различных станции, чтобы приобрести один пакет подписки для каждого этажа вашего доходного дома.
* Заполните PDF-файл для этого упражнения.
* Обсудите ответы вашей группы с классом.

[Работа в аудитории. Телепакет на отпуск](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/3.0.1.2%20Vacation%20Station%20Instructions.pdf)

# Определения виртуальной локальной сети

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.

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).

**Преимущества виртуальных локальных сетей (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, состоит из шести компьютеров и трёх широковещательных доменов: для преподавателей, для учащихся и гостевого домена.
* **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.

# Типы виртуальных локальных сетей

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**

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 команда **show vlan brief** была выполнена на коммутаторе, настроенном по умолчанию. Обратите внимание, что на все порты по умолчанию назначены сети VLAN 1.

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.

**Native 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.

**Управляющая 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 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.

**Голосовые сети VLAN**

Для поддержки передачи голоса по IP (VoIP) требуется отдельная сеть VLAN. Для VoIP-трафика требуется:

* гарантированная полоса пропускания для обеспечения высокого качества голосовой передачи;
* приоритет передачи перед другими типами сетевого трафика;
* возможность маршрутизации в обход перегруженных участков;
* задержка менее 150 мс по всей сети.

Для того чтобы соответствовать этим требованиям, вся сеть должна быть специально спроектирована для поддержки VoIP. В рамках данного курса не рассматриваются особенности настройки сети для поддержки VoIP, однако краткая информация о том, как голосовая VLAN работает между коммутатором, IP-телефоном Cisco и компьютером, будет полезна.

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

# Packet Tracer. Получатели широковещательной рассылки

**Исходные данные/сценарий**

По условиям этого упражнения имеется полностью заполненный 24-портовый коммутатор Catalyst 2960. Все порты используются. Вам необходимо отследить трафик широковещательной рассылки в развёрнутой VLAN и ответить на некоторые вопросы для обсуждения.

[Packet Tracer. Получатели широковещательной рассылки Инструкции](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/3.1.1.5%20Packet%20Tracer%20-%20Who%20Hears%20the%20Broadcast%20Instructions.pdf)

[Packet Tracer. Получатели широковещательной рассылки PKA](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/3.1.1.5%20Packet%20Tracer%20-%20Who%20Hears%20the%20Broadcast.pka)

# Транки виртуальных сетей

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.

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.

# Контроль широковещательных доменов в сетях VLAN

**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 рис. 1 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.

**Сеть с VLAN**

Как показано в анимации на рисунке 2, 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, т.е. из порта F0/3. При получении коммутатором S3 широковещательного кадра через порт F0/3 он пересылает широковещательный кадр из другого порта, настроенного для поддержки сети VLAN 10, т.е. из порта F0/11. Широковещательный кадр прибывает на единственный другой компьютер в сети, настроенный для VLAN 10, т.е. на компьютер для преподавателей PC4.

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.

**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.

**Подробнее о поле тега 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.

# Сети native VLAN и тегирование стандарта 802.1Q

**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.

**Нетегированные кадры в сети native VLAN**

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.

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.

**Тегирование голосовой VLAN**

Не забывайте, что для поддержки VoIP требуется отдельная голосовая 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.

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 рис. 1 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.

**Пример конфигурации**

На рис. 2 приведён пример выходных данных. В рамках данного курса 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).

# Packet Tracer. Исследование методов реализации сети VLAN

**Исходные данные/сценарий**

В этом упражнении необходимо отслеживать пересылку широковещательного трафика через коммутаторы при сконфигурированных и не сконфигурированных VLAN.

[Packet Tracer. Исследование методов реализации сети VLAN. Инструкции](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/3.1.2.7%20Packet%20Tracer%20-%20Investigating%20a%20VLAN%20Implementation%20Instructions.pdf)

[Packet Tracer. Исследование методов реализации сети VLAN. PKA](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/3.1.2.7%20Packet%20Tracer%20-%20Investigating%20a%20VLAN%20Implementation.pka)

**Диапазоны VLAN на коммутаторах Catalyst**

Различные коммутаторы Cisco Catalyst поддерживают разное количество сетей VLAN. Количество поддерживаемых сетей VLAN достаточно велико для удовлетворения потребностей большинства организаций. Например, коммутаторы Catalyst 2960 и 3560 способны поддерживать более 4 тысяч сетей VLAN. Виртуальные локальные сети стандартного диапазона на этих коммутаторах имеют идентификатор от 1 до 1 005, а сети VLAN расширенного диапазона — от 1 006 до 4 094. На этом рисунке показаны доступные VLAN на коммутаторе Catalyst 2960 под управлением Cisco IOS версии 15.x.

**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.

**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.

# Создание виртуальной локальной сети

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.

На рис. 1 показан синтаксис команды Cisco IOS, используемый для добавления сети VLAN к коммутатору и присвоения ей имени. При настройке коммутатора рекомендуется присваивать имя каждой сети VLAN.

На рис. 2 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.

Используйте инструмент проверки синтаксиса на рис. 3 для создания сети VLAN и введите команду **show vlan brief**, для того чтобы отобразить содержимое файла vlan.dat.

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**

# Назначение портов сетям VLAN

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 рис. 1 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.

В примере на рис. 2 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).

Используйте инструмент проверки синтаксиса на рис. 3 для назначения сети VLAN и введите команду **show vlan brief**, чтобы отобразить содержимое файла vlan.dat.

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

# Изменение принадлежности портов виртуальной локальной сети

Существует множество способов изменить принадлежность портов VLAN. На рис. 1 показан синтаксис для изменения принадлежности порта коммутатора сети VLAN 1 с помощью команды режима конфигурации интерфейса **no switchport access vlan**.

Ранее интерфейс F0/18 был назначен сети VLAN 20. Для интерфейса F0/18 нужно ввести команду **no switchport access vlan**. Изучите выходные данные команды **show vlan brief**, которые будут сразу же выведены, как показано на рис. 2. Команда **show vlan brief** показывает назначение VLAN и тип принадлежности для всех портов коммутатора. Команда **show vlan brief** показывает одну строку для каждой VLAN. В выходных данных для каждой VLAN указаны имя, состояние и порты коммутатора VLAN.

Сеть VLAN 20 всё ещё активна, хотя ей не назначены порты. На рис. 3 выходные команды **show interfaces f0/18 switchport** подтверждают, что сеть доступа VLAN для интерфейса F0/18 была сброшена до VLAN 1.

Принадлежность порта VLAN может быть легко изменена. Для того чтобы изменить принадлежность порта VLAN, нет необходимости сначала удалять порт из сети VLAN. При изменении VLAN, к которой принадлежит порт доступа, на другую существующую VLAN, предыдущая принадлежность попросту заменяется на новую. На рис. 4 порт F0/11 назначен сети VLAN 20.

Используйте инструмент проверки синтаксиса на рис. 5, чтобы изменить принадлежность портов VLAN.

# Удаление виртуальных локальных сетей

На рисунке команда режима глобальной конфигурации **no vlan** *vlan-id* используется для удаления сети VLAN 20 из коммутатора. При минимальной настройке коммутатора S1 все порты принадлежат VLAN 1, а неиспользуемая VLAN 20 содержится в базе данных VLAN. Команда **show vlan brief** позволяет убедиться, что после использования команды **no vlan 20** сеть VLAN 20 удалена из файла vlan.dat.

**Внимание!** Перед удалением сети VLAN обязательно переназначьте все порты, которые ей принадлежат, в другие сети VLAN. После удаления VLAN все порты, которые не были перемещены в активную сеть VLAN, не смогут обмениваться данными с другими узлами, пока не будут назначены активной VLAN.

Другой вариант — удалить весь файл vlan.dat с помощью команды привилегированного режима **delete flash:vlan.dat**. Сокращённую версию команды (**delete vlan.dat**) можно использовать в том случае, если в файл vlan.dat не был перемещён из своего расположения по умолчанию. После выполнения этой команды и перезагрузки коммутатора ранее настроенные VLAN будут удалены. Фактически это позволяет восстановить в коммутаторе его заводские конфигурации VLAN.

**Примечание**. Чтобы восстановить заводские настройки в случае с коммутатором Catalyst, перед его перезагрузкой нужно ввести команду **erase startup-config** вместе с командой **delete vlan.dat**.

# Проверка информации о сети VLAN

По завершении настройки сети VLAN её конфигурации можно проверить с помощью команд Cisco IOS **show**.

На рис. 1 показаны параметры команд **show vlan** и **show interfaces**.

В примере на рис. 2 команда **show vlan name student** генерирует выходные данные, которые нелегко интерпретировать. Рекомендуется использовать команду **show vlan brief**. Команда **show vlan summary** отображает список всех настроенных сетей VLAN. В выходных данных на рис. 2 показаны семь сетей VLAN.

Команда **show interfaces vlan** *vlan-id* отображает сведения, которые не рассматриваются в рамках этого курса. Во второй строке на рис. 3 отображена важная информация, которая указывает, что сеть VLAN 20 находится в рабочем состоянии.

Используйте инструмент проверки синтаксиса на рис. 4, чтобы отобразить информацию о VLAN и порте коммутатора, и проверьте назначения и режим VLAN.

# Packet Tracer. Конфигурация сетей VLAN

**Исходные данные/сценарий**

Сети VLAN полезны при администрировании логических групп, поскольку позволяют легко перемещать, изменять или добавлять участников группы. Цель этого задания заключается в создании и присвоении имени сетям VLAN, а также назначении портов доступа конкретным сетям VLAN.

[Packet Tracer. Настройка сетей VLAN. Инструкции](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/3.2.1.7%20Packet%20Tracer%20-%20Configuring%20VLANs%20Instructions.pdf)

[Packet Tracer. Настройка сетей VLAN. PKA](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/3.2.1.7%20Packet%20Tracer%20-%20Configuring%20VLANs.pka)

# Настройка транковых каналов IEEE 802.1Q

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 рис. 1 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*.

На рис. 2 сети VLAN 10, 20 и 30 поддерживают компьютеры для преподавателей, учащихся и гостевой компьютер (PC1, PC2 и PC3). Также необходимо изменить сеть native VLAN с VLAN 1 на другую сеть VLAN, например на VLAN 99. По умолчанию доступ в транковый канал разрешён для всех сетей VLAN. Чтобы ограничить сети VLAN, которым разрешен доступ в транковый канал, можно использовать команду **switchport trunk allowed vlan**.

На рис. 3 порт F0/1 коммутатора S1 настроен как транковый порт, в качестве сети native VLAN назначена VLAN 99, а магистральный канал настроен для передачи трафика только для сетей VLAN 10, 20, 30 и 99.

**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.

# Сброс транкового канала до состояния по умолчанию

На рис. 1 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.

На рис. 2 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.

На рис. 3 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.

# Проверка конфигурации транкового канала

На рис. 1 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.

Используйте инструмент проверки синтаксиса на рис. 2, чтобы настроить сеть native VLAN 99 на транке с поддержкой всех VLAN на интерфейсе F0/1. Проверьте конфигурацию транкового порта с помощью команды **show interfaces f0/1 switchport**.

# Packet Tracer. Конфигурация транковых каналов

**Исходные данные/сценарий**

Для передачи информации VLAN между коммутаторами требуются транковые каналы. Порт коммутатора может работать портом доступа или транковым портом. Порты доступа служат для передачи трафика от определённой VLAN, назначенной конкретному порту. Транковый порт по умолчанию принадлежит всем VLAN. Таким образом, он передаёт трафик во все сети VLAN. Целью данного задания является создание транковых портов и назначение их сети native VLAN, отличной от сети по умолчанию.

[Packet Tracer. Конфигурация транковых каналов. Инструкции](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/3.2.2.4%20Packet%20Tracer%20-%20Configuring%20Trunks%20Instructions.pdf)

[Packet Tracer. Конфигурация транковых каналов. PKA](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/3.2.2.4%20Packet%20Tracer%20-%20Configuring%20Trunks.pka)

**Лабораторная работа. Конфигурация VLAN и транковых каналов**

**В ходе этой лабораторной работы необходимо выполнить следующие задания:**

* Часть 1. Создание сети и настройка базовых параметров устройства
* Часть 2. Создание виртуальных локальных сетей и назначение портов коммутатора
* Часть 3. Поддержка назначения портов VLAN и базы данных VLAN
* Часть 4. Настройка транкового канала стандарта 802.1Q между коммутаторами
* Часть 5. Удаление базы данных VLAN

[Лабораторная работа. Конфигурация VLAN и транковых каналов](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/3.2.2.5%20Lab%20-%20Configuring%20VLANs%20and%20Trunking.pdf)

# Знакомство с 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.

Как показано на рис. 1, 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.

На рис. 2 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.

**Согласованные режимы интерфейса**

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.
* **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.

На рис. 1 показаны результаты параметров конфигурации DTP на противоположных концах транкового канала, подключённого к портам коммутатора Catalyst 2960.

При возможности настраивайте транковые каналы статически. Режим DTP по умолчанию зависит от версии ПО Cisco IOS и от платформы. Чтобы определить текущий режим DTP, введите команду **show dtp interface**, как показано на рис. 2.

Используйте инструмент проверки синтаксиса на рис. 3, чтобы определить режим DTP на интерфейсе F0/1.

**Примечание**. В случае если необходим транковый канал, рекомендуется настроить интерфейс на **trunk** и **nonegotiate**. На каналах, в которых транковая связь не предусмотрена, DTP следует отключить.

# Проблемы с IP-адресацией сети VLAN

Каждой VLAN должна соответствовать уникальная IP-подсеть. Если два устройства в одной сети VLAN имеют разные адреса подсетей, они не могут обмениваться данными. Данное несоответствие является распространённой проблемой, и для её решения нужно выявить ошибку в конфигурации и изменить адрес подсети на правильный.

На рис. 1 компьютер PC1 не может подключиться к указанному серверу Web/TFTP.

Проверка параметров IP-конфигурации на компьютере PC1, показанная на рис. 2, выявляет наиболее распространённую проблему при настройке сетей VLAN — неправильно настроенный IP-адрес. Компьютер PC1 настроен с IP-адресом 172.172.10.21, но правильный IP-адрес — 172.17.10.21.

В диалоговом окне конфигурации Fast Ethernet компьютера PC1 показан обновлённый IP-адрес — 172.17.10.21. На рис. 3 выходные данные снизу отображают, что компьютер PC1 снова подключён к серверу Web/TFTP, расположенному по IP-адресу 172.17.10.30.

# Отсутствующие сети VLAN

Если между устройствами в VLAN по-прежнему нет соединения, но проблемы с IP-адресацией были устранены, обратитесь к рабочей диаграмме на рис. 1, чтобы устранить оставшиеся неполадки:

**Шаг 1.** Примените команду **show vlan**, чтобы убедиться, что порт принадлежит ожидаемой VLAN. Если порт назначен неверной VLAN, используйте команду **switchport access vlan** для корректировки принадлежности VLAN. Используйте команду **show mac address-table** для проверки адресов, полученных на отдельном порте коммутатора и назначенных VLAN этому порту.

**Шаг 2.** Если VLAN, которой назначен порт, удалена, порт становится неактивным. Используйте команду **show vlan** или **show interfaces switchport**.

Для отображения таблицы МАС-адресов используйте команду **show mac-address-table**. На рис. 2 показан пример МАС-адресов, полученных на интерфейсе F0/1. Здесь видно, что MAC-адрес 000c.296a.a21c был получен на интерфейсе F0/1 в сети VLAN 10. Если этот номер не соответствует номеру ожидаемой VLAN, измените принадлежность портов сети VLAN с помощью команды **switchport access vlan**.

Каждый порт коммутатора принадлежит сети VLAN. Если VLAN, которой принадлежит порт, удалена, порт становится неактивным. Все порты, принадлежащие удалённой сети VLAN, не смогут взаимодействовать с другими сегментами сети. Для того чтобы проверить, активен ли порт, используйте команду **show interface f0/1 switchport**. Если порт неактивен, он не будет работать, пока с помощью команды **vlan** *vlan\_id* не будет создана отсутствующая VLAN.

# Введение в поиск и устранение неполадок в транковых каналах

Типичной задачей сетевого администратора является устранение неполадок при создании транкового канала или в каналах, которые некорректно работают в качестве транковых. Иногда порт коммутатора может работать как транковый порт, даже если он не настроен для этого. Например, порт доступа может принимать кадры от сетей VLAN, к которым этот порт не назначен. Это называется утечкой VLAN.

На рис. 1 показана рабочая диаграмма рекомендаций по устранению неполадок в каналах.

Для устранения неполадок при неудачном создании транкового канала или утечке VLAN выполните следующие действия:

**Шаг 1.** Используйте команду **show interfaces trunk**, чтобы проверить, совпадают ли локальная сеть и равноправный узел native VLAN. Если native VLAN не совпадает на обеих сторонах, происходит утечка VLAN.

**Шаг 2.** Используйте команду **show interfaces trunk** для проверки установления транкового канала между коммутаторами. По возможности настраивайте транковые каналы статически. Порты коммутатора Cisco Catalyst по умолчанию используют протокол DTP и пытаются согласовать транковый канал.

Для того чтобы отобразить состояние транка, сети native VLAN, используемой на этом транковом канале, и проверить установку транка, используйте команду **show interfaces trunk**. Пример на рис. 2 показывает, что сеть native VLAN на одной стороне транкового канала была изменена на VLAN 2. Если на одном конце транкового подключения настроена сеть native VLAN 99, а на другом — native VLAN 2, то кадр, отправленный из сети VLAN 99 на одном конце, будет получен в сети VLAN 2 на другом конце. Трафик VLAN 99 попадает в сегмент VLAN 2.

CDP отображает уведомление о несовпадении native VLAN в транковом канале таким сообщением:

\*Mar 1 06:45:26.232: %CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (2), with S2 FastEthernet0/1 (99).

При возникновении несовпадений native VLAN происходят проблемы с подключением в сети. Трафик данных сетей VLAN, кроме двух настроенных сетей native VLAN, успешно проходит по транковому каналу, но данные, связанные с какой-либо из этих двух native VLAN, не проходят по транковому каналу.

Как показано на рис. 2, проблемы несовпадения сети native VLAN не мешает созданию транкового канала. Чтобы решить проблему несоответствия сети native VLAN, настройте сеть native VLAN так, чтобы это была одна и та же VLAN на обеих сторонах канала.

**Распространённые проблемы с транковыми каналами**

Причиной неполадок в транковых каналах обычно является неправильная конфигурация. При настройке сетей VLAN и транковых каналов в коммутируемой инфраструктуре часто случаются следующие типы ошибок конфигурации.

* **Несовпадения native VLAN**: транковые порты настроены с разными сетями native VLAN. При этой ошибке конфигурации генерируются консольные уведомления, а управляющий и административный трафик отправляются в неверном направлении. Это влечёт за собой угрозу безопасности.
* **Несовпадения транкового режима**: для одного транкового порта настроен режим, несоответствующий транковому режиму соответствующего порта с другой стороны. При этой ошибке конфигурации транковый канал перестаёт работать.
* **Разрешённые сети VLAN в транковых каналах**: список сетей VLAN, разрешённых в транке, не был обновлён в соответствии с текущими требованиями VLAN. В этом случае по сети передаётся непредвиденный трафик или же совсем нарушается передача трафика.

Если обнаружена проблема с транковым каналом, а причина неизвестна, начните устранение неполадок с проверки несовпадения транковых каналов для native VLAN. Если причина не в этом, проверьте несовпадения транкового режима, затем проверьте список разрешённых VLAN. На следующих двух страницах показано, как следует решать распространённые проблемы в транковых каналах.

# Несовпадения режимов транковой связи

Транковые каналы обычно настраиваются статически с помощью команды **switchport mode trunk**. Для согласования состояния канала транковые порты коммутатора Cisco Catalyst используют протокол DTP. Когда порт в транковом канале настроен в режиме транка, который несовместим с режимом транкового порта на другой стороне, создание транкового канала между двумя коммутаторами невозможно.

В сценарии, проиллюстрированном на рис. 1, компьютер PC4 не может подключиться к внутреннему веб-серверу. В топологии указана правильная конфигурация. В чём заключается проблема?

Проверьте состояние транковых портов на коммутаторе S1 с помощью команды **show interfaces trunk**. Выходные данные на рис. 2 показывают, что интерфейс Fa0/3 коммутатора S1 в настоящее время находится вне транкового канала. При проверке интерфейса F0/3 выявляется, что порт коммутатора на самом деле находится в динамическом автоматическом режиме. Проверка транков на коммутаторе S3 выявляет, что активные транковые порты отсутствуют. Дальнейшая проверка показывает, что интерфейс Fa0/3 также находится в динамическом автоматическом режиме. Это объясняет, почему транковый канал не работает.

Для того чтобы решить эту проблему, перенастройте транковый режим F0/3 портов на коммутаторах S1 и S3, как показано на рис. 3. После изменения конфигурации выходные данные команды **show interfaces** указывают, что теперь порт коммутатора S1 находится в режиме транка. Выходные данные на компьютере PC4 указывают, что подключение к серверу Web/TFTP по IP-адресу 172.17.10.30 было восстановлено.

# Неверный список виртуальной локальной сети

Для успешной передачи трафика из сети VLAN по транку эта VLAN должна быть разрешена на транковом канале. Для этого используйте команду **switchport trunk allowed vlan** *vlan-id*.

На рис. 1 сеть VLAN 20 (для учащихся) и компьютер PC5 были добавлены в сеть. Документация была обновлена, чтобы показать, что на транке разрешены сети VLAN 10, 20 и 99. В этом сценарии компьютер PC5 не может подключиться к серверу электронной почты для учащихся.

Проверьте транковые порты на коммутаторе S1 с помощью команды **show interfaces trunk**, как показано на рис. 2. Эта команда указывает, что интерфейс F0/3 на коммутаторе S3 был правильно настроен для разрешения сетей VLAN 10, 20 и 99. Проверка интерфейса F0/3 на коммутаторе S1 выявляет, что интерфейсы F0/1 и F0/3 разрешают только сети VLAN 10 и 99. Кто-то обновил документацию, но забыл перенастроить порты на коммутаторе S1.

Перенастройте порты F0/1 и F0/3 на коммутаторе S1 с помощью команды **switchport trunk allowed vlan 10,20,99**, как показано на рис. 3. Выходные данные показывают, что сети VLAN 10, 20 и 99 теперь добавлены к портам F0/1 и F0/3 коммутатора S1. Команда **show interfaces trunk** — это превосходный инструмент для выявления распространённых проблем в транковых каналах. Соединение между компьютером PC5 и сервером электронной почты для учащихся, находящимися по IP-адресу 172.17.20.10, было восстановлено.

# Packet Tracer. Поиск и устранение неполадок при реализации сети VLAN. Сценарий 1

**Исходные данные/сценарий**

В этом задании вам предстоит найти и устранить неполадки с подключением между компьютерами, которые находятся в одной сети VLAN. Задание выполнено, если компьютеры в одной VLAN могут отправлять друг другу эхо-запросы. Любое внедряемое решение должно находиться в соответствии с таблицей адресации.

[Packet Tracer. Поиск и устранение неполадок при реализации сети VLAN. Сценарий 1. Инструкции](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/3.2.4.7%20Packet%20Tracer%20-%20Troubleshooting%20a%20VLAN%20Implementation%20-%20Scenario%201%20Instructions.pdf)

[Packet Tracer. Поиск и устранение неполадок при реализации сети VLAN. Сценарий 1. PKA](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/3.2.4.7%20Packet%20Tracer%20-%20Troubleshooting%20a%20VLAN%20Implementation%20-%20Scenario%201.pka)

# Packet Tracer. Поиск и устранение неполадок при реализации сети VLAN. Сценарий 2

**Исходные данные/сценарий**

В этом задании необходимо найти и устранить неполадки в неверно сконфигурированной среде сети VLAN. Исходная сеть содержит ошибки. Вам необходимо найти и исправить ошибки в конфигурации и установить сквозное подключение. Окончательная конфигурация должна совпадать с топологической схемой и таблицей адресации. Сетью native VLAN для этой топологии является VLAN 56.

[Packet Tracer. Поиск и устранение неполадок при реализации сети VLAN. Сценарий 2. Инструкции](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/3.2.4.8%20Packet%20Tracer%20-%20Troubleshooting%20a%20VLAN%20Implementation%20-%20Scenario%202%20Instructions.pdf)

[Packet Tracer. Поиск и устранение неполадок при реализации сети VLAN. Сценарий 2. PKA](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/3.2.4.8%20Packet%20Tracer%20-%20Troubleshooting%20a%20VLAN%20Implementation%20-%20Scenario%202.pka)

**Лабораторная работа. Поиск и устранение неполадок при реализации сети VLAN**

**В ходе этой лабораторной работы необходимо выполнить следующие задания:**

* Часть 1. Создание сети и настройка базовых параметров устройства
* Часть 2. Поиск и устранение неполадок при реализации сети VLAN 10
* Часть 3. Поиск и устранение неполадок при реализации сети VLAN 20

[Лабораторная работа. Поиск и устранение неполадок при реализации сети VLAN](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/3.2.4.9%20Lab%20-%20Troubleshooting%20VLAN%20Configurations.pdf)

# Спуфинг-атака на коммутатор

В современных коммутируемых сетях существует множество различных типов атак. Архитектура VLAN упрощает обслуживание сети и повышает производительность, однако также даёт злоумышленникам возможность для атаки. Необходимо понимать как принцип действия различных типов атак, так и методы снижения риска атак.

Атака VLAN hopping позволяет посторонней VLAN видеть трафик другой, атакуемой VLAN. Спуфинг коммутатора — это тип атаки сети VLAN, при котором используется неправильно настроенный транковый порт. По умолчанию транковые порты имеют доступ ко всем сетям VLAN и передают трафик для нескольких VLAN через один и тот же физический канал, как правило, между коммутаторами.

На рисунке нажмите кнопку «Воспроизведение», чтобы просмотреть анимацию о спуфинг-атаке коммутатора.

В простом случае спуфинг-атаки коммутатора злоумышленник в своих интересах пользуется тем, что порт коммутатора по умолчанию настроен на динамический автоматический режим. Злоумышленник конфигурирует систему таким образом, чтобы она вела себя как коммутатор. Для такого спуфинга злоумышленник должен уметь имитировать сообщения 802.1Q и DTP. Заставив коммутатор думать, что другой коммутатор пытается создать транковый канал, злоумышленник может получить доступ ко всем сетям VLAN, разрешённым на этом транковом порте.

Лучший способ предотвратить базовую спуфинг-атаку — отключить транковую связь на всех портах, за исключением тех, на которых транковая связь необходима. На нужных транковых портах отключите DTP и вручную включите транковую связь.

# Атака с двойным тегированием

Другой тип атаки сети VLAN — это атака с двойным тегированием (или с двойной инкапсуляцией). Данный вид атаки основан на использовании принципов работы аппаратного обеспечения на большинстве коммутаторов. Большинство коммутаторов выполняют лишь один уровень деинкапсуляции 802.1Q, что позволяет злоумышленнику вставлять в кадр скрытую метку 802.1Q. Метка позволяет пересылать кадр в сеть VLAN, которая не указана первоначальной меткой 802.1Q. Важное свойство атаки с двойной инкапсуляцией заключается в том, что она действует, даже если транковые порты отключены, поскольку обычно узел отправляет кадр в сегменте, который не является транковым каналом.

Атака VLAN hopping с двойным тегированием происходит в три шага:

1. Злоумышленник отправляет на коммутатор кадр с двойным тегированием 802.1Q. Внешний заголовок содержит метку сети VLAN злоумышленника, которая совпадает с native VLAN транкового порта. Предполагается, что коммутатор обрабатывает полученный от злоумышленника кадр, будто он находится на транковом порте или порте с голосовой VLAN (коммутатор не должен получать тегированный кадр Ethernet на порте доступа). В качестве примера представьте, что сетью native VLAN является VLAN 10. Внутренний тег — это VLAN, подверженная атаке. В данном случае — VLAN 20.

2. Кадр прибывает на коммутатор, который проверяет первые 4 байта тега 802.1Q. Коммутатор видит, что кадр предназначен для VLAN 10, которая является сетью native VLAN. Удалив метку VLAN 10, коммутатор пересылает пакет из всех портов сети VLAN 10. На транковом порте удаляется метка сети VLAN 10, но пакет не тегируется заново, поскольку он является частью native VLAN. В это время метка сети VLAN 20 по-прежнему нетронута и не проверяется первым коммутатором.

3. Второй коммутатор проверяет только внутренний тег 802.1Q, отправленный злоумышленником, и видит, что кадр предназначен для сети VLAN 20, являющейся целью злоумышленника. Второй коммутатор отправляет кадр на атакуемый порт или наполняет его лавинной рассылкой в зависимости от того, есть ли в таблице МАС-адресов запись для атакуемого узла.

Этот вид атаки является однонаправленным и работает, только если злоумышленник подключён к порту, находящимся в той же VLAN, что и сеть native VLAN транкового порта. Предотвратить такую атаку не так легко, как остановить обычные атаки VLAN hopping.

Лучший способ снижения вреда от атак с двойным тегированием — удостовериться, что сеть native VLAN транковых портов отличается от VLAN любых пользовательских портов. Согласно практической рекомендации по обеспечению безопасности, рекомендуется использовать фиксированную VLAN, которая отличается от всех пользовательских VLAN в коммутируемой сети, в качестве сети native VLAN для всех транковых каналов 802.1Q.

**Сеть PVLAN периметра**

Некоторые приложения запрещают пересылку трафика на 2-м уровне между портами на одном коммутаторе, чтобы соседнее устройство не могло видеть трафик, генерируемый другим соседним устройством. В таких условиях использование функции граничной частной сети VLAN (PVLAN), которую также называют защищёнными портами, предотвращает обмен одноадресным, широковещательным и многоадресным трафиком между этими портами коммутатора (рис. 1).

Для функции сети PVLAN периметра характерны следующие свойства:

* Защищённый порт не пересылает никакой трафик (одноадресный, многоадресный или широковещательный) на какой-либо другой, защищённый порт, кроме управляющего трафика. Трафик данных нельзя пересылать между защищёнными портами на 2-м уровне.
* Пересылка между защищённым и незащищённым портом происходит в обычном режиме.
* Защищённые порты необходимо настраивать вручную.

Для настройки функции сети PVLAN периметра в режиме конфигурации интерфейса введите команду **switchport protected** (рис. 2). Для того чтобы отключить защищённый порт, используйте команду **no switchport protected** в режиме конфигурации интерфейса. Чтобы проверить конфигурацию функции граничной сети PVLAN, используйте команду режима глобальной конфигурации **show interfaces** *interface-id* **switchport**.

Используйте инструмент проверки синтаксиса на рис. 3, чтобы настроить функцию граничной сети PVLAN на интерфейсе G0/1 и проверить конфигурацию.

# Рекомендации по проектированию виртуальной локальной сети

В заводских настройках коммутаторов Cisco заданы различные сети VLAN для поддержки различных сред и типов протоколов. VLAN 1 является сетью Ethernet VLAN по умолчанию. Наилучший метод обеспечения безопасности — настроить все порты на всех коммутаторах так, чтобы они были связаны с сетями VLAN, исключая сеть VLAN 1. Для этого, как правило, нужно настроить все неиспользуемые порты в сеть VLAN «чёрной дыры», которая никогда не используется в сети. Все используемые порты связаны с сетями VLAN, кроме VLAN 1 и VLAN «чёрной дыры». Для предотвращения несанкционированного доступа рекомендуется отключать неиспользуемые порты коммутатора.

Также для обеспечения безопасности рекомендуется отделять административный трафик от пользовательского. Управляющая VLAN, установленная по умолчанию сетью VLAN 1, следует заменить на другую VLAN. Для удалённого управления коммутатором Cisco коммутатору необходим IP-адрес, настроенный на управляющую VLAN. Пользователи в других сетях VLAN не смогут устанавливать сеансы удалённого доступа с коммутатором, если они не были маршрутизированы в управляющую VLAN с обеспечением дополнительного уровня безопасности. Кроме того, коммутатор следует настроить для приёма только зашифрованных сеансов SSH удалённого управления.

Весь управляющий трафик отправляется на VLAN 1. Поэтому, когда сеть native VLAN изменена на сеть, отличную от VLAN 1, весь управляющий трафик тегируется на транковых каналах IEEE 802.1Q VLAN (тегируется идентификатором VLAN 1). Для обеспечения безопасности рекомендуется изменить сеть native VLAN на сеть, отличную от VLAN 1. Сеть native VLAN также должна отличаться от всех пользовательских сетей VLAN. Убедитесь, что native VLAN для транкового подключения 802.1Q одинакова на обеих сторонах канала.

Протокол DTP предлагает четыре режима порта коммутатора: режим доступа, транковый, динамический автоматический и динамический рекомендуемый. Согласно общей рекомендации, автосогласование следует отключить. Следуя практической рекомендации для обеспечения безопасности, не используйте динамический автоматический или динамический рекомендуемый режимы портов коммутатора.

Наконец, голосовой трафик ограничивается жёсткими требованиями QoS. Если пользовательские компьютеры и IP-телефоны находятся в одной сети VLAN, каждый пытается использовать доступную полосу пропускания, не принимая во внимание другие устройства. Чтобы избежать таких конфликтов, рекомендуется использовать отдельные VLAN для IP-телефонии и трафика данных.

**Лабораторная работа. Реализация средств защиты виртуальной локальной сети**

**В ходе этой лабораторной работы необходимо выполнить следующие задания:**

* Часть 1. Создание сети и настройка базовых параметров устройства
* Часть 2. Внедрение средств обеспечения безопасности VLAN на коммутаторах

[Лабораторная работа. Реализация средств защиты виртуальной локальной сети](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/3.3.2.2%20Lab%20-%20Implementing%20VLAN%20Security.pdf)

**План виртуальной локальной сети**

**План виртуальной локальной сети**

**Сценарий**

Вы разрабатываете сеть с коммутацией VLAN для компании малого или среднего бизнеса.

Ваша компания владеет двумя этажами в высотном здании. Следующие элементы требуют анализа VLAN и доступа к целям планирования:

* Управление
* Финансы
* Продажи
* Отдел кадров
* Сетевой администратор
* Основные посетители вашего делового пространства

Имеется два коммутатора Cisco 3560-24PS.

Используйте текстовый редактор для разработки схемы коммутируемой сети VLAN.

Первый раздел проекта должен включать обычные названия отделов, примерные имена, количество VLAN и порты, которые будут назначены каждой VLAN.

Во втором разделе следует составить список планируемых средств безопасности для этой коммутируемой сети.

По завершении создания плана сети VLAN ответьте на вопросы для обсуждения из PDF-файла для этого задания.

Сохраните результаты работы. Будьте готовы к обсуждению вашего плана VLAN с другой группой или классом.

[Работа в аудитории. План сети VLAN. Инструкции](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/3.4.1.1%20VLAN%20Plan%20Instructions.pdf)

# Packet Tracer. Отработка практических навыков

**Исходные данные/сценарий**

В этом упражнении даны два полностью настроенных коммутатора. На третьем коммутаторе вам необходимо назначить IP-адреса виртуальному интерфейсу коммутатора (Switch Virtual Interface), выполнить настройку сетей VLAN, назначить интерфейсы сетям VLAN, настроить транковую связь и создать базовую защиту коммутаторов.

[Packet Tracer. Отработка практических навыков. Инструкции](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/3.4.1.2%20Skills%20Integration%20Challenge%20Instructions.pdf)

[Packet Tracer. Отработка практических навыков. РКА](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/3.4.1.2%20Skills%20Integration%20Challenge.pka)

**Заключение**

В данной главе мы изучили основы сетей VLAN. Сети VLAN основываются не на физических, а на логических подключениях. Сети VLAN — это механизм, позволяющий сетевым администраторам создавать логические широковещательные домены, которые способны охватывать один или несколько коммутаторов независимо от физического расстояния. Эта функция полезна для уменьшения размера широковещательных доменов или для объединения групп или пользователей, которые не обязательно должны находиться в одном месте.

Существует несколько типов сетей VLAN.

* Сеть VLAN по умолчанию
* Управляющая VLAN
* Native VLAN
* Пользовательская/VLAN для данных
* VLAN «чёрной дыры»
* Голосовая сеть VLAN

В коммутаторе Cisco VLAN 1 является сетью Ethernet VLAN по умолчанию, сетью native VLAN по умолчанию и управляющей VLAN по умолчанию. Согласно практическим рекомендациям, для обеспечения безопасности сети native VLAN и управляющие VLAN должны быть перемещены в другую, отдельную VLAN, а неиспользуемые порты коммутатора должны быть перемещены в сеть VLAN «чёрной дыры».

Команда **switchport access vlan** используется для создания сети VLAN на коммутаторе. Следующий шаг после создания сети VLAN — назначение портов сетям VLAN. Команда **show vlan brief** показывает назначение VLAN и тип принадлежности для всех портов коммутатора. Каждой VLAN должна соответствовать уникальная IP-подсеть.

Примените команду **show vlan**, чтобы убедиться, что порт принадлежит ожидаемой VLAN. Если порт назначен неверной VLAN, используйте команду **switchport access vlan** для корректировки принадлежности VLAN. Используйте команду **show mac address-table** для проверки адресов, полученных на отдельном порте коммутатора и назначенных VLAN этому порту.

Порт коммутатора может работать портом доступа или транковым портом. Порты доступа служат для передачи трафика от определённой VLAN, назначенной конкретному порту. Транковый порт по умолчанию принадлежит всем VLAN. Таким образом, он передаёт трафик во все сети VLAN.

Транковые каналы VLAN упрощают взаимодействие между коммутаторами, передавая трафик, связанный с несколькими VLAN. Тегирование кадров IEEE 802.1Q позволяет различать кадры Ethernet, связанные с определёнными VLAN по мере их прохождения по общим транковым каналам. Для того чтобы включить транковые каналы, используйте команду **switchport mode trunk**. Используйте команду **show interfaces trunk** для проверки установления транкового канала между коммутаторами.

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.

Чтобы вернуть коммутатор к его заводским настройкам с одной сетью VLAN по умолчанию, используйте команду **delete flash:vlan.dat** и **erase startup-config**.

Также в этой главе мы рассмотрели конфигурацию, поиск и устранение неполадок сетей VLAN и транковых каналов с помощью интерфейса командной строки Cisco IOS и изучили основы безопасности и вопросы проектирования в контексте сетей VLAN.